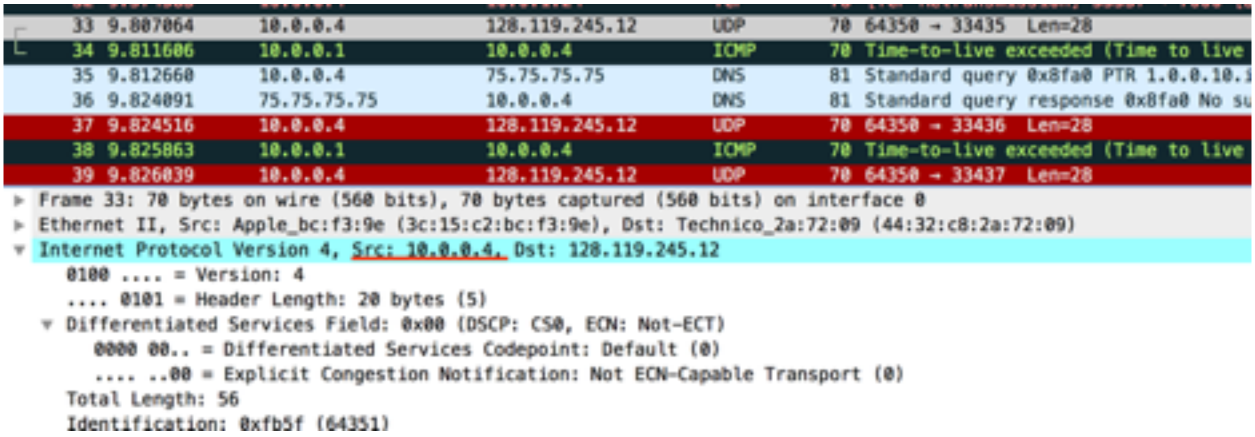
Colleen Minor

CS 372

Lab 3

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?*

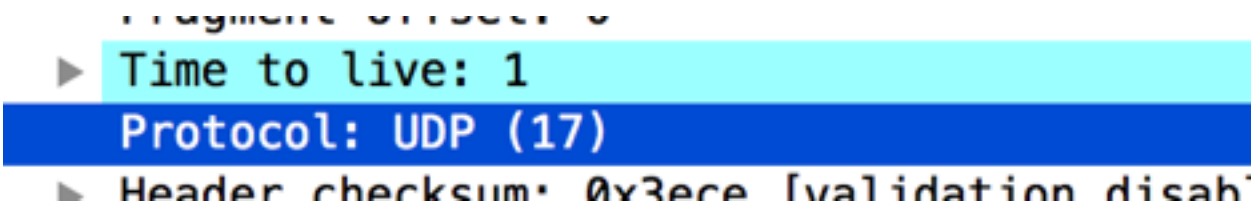
   My IP seems to be listed as 10.0.0.4



```
 33 9.807064   10.0.0.4       128.119.245.12   UDP    70 64350 → 33435  Len=28
 34 9.811606   10.0.0.1       10.0.0.4         ICMP   70 Time-to-live exceeded (Time to live
 35 9.812660   10.0.0.4       75.75.75.75      DNS    81 Standard query 0x8fa0 PTR 1.0.0.10.i
 36 9.824091   75.75.75.75    10.0.0.4         DNS    81 Standard query response 0x8fa0 No su
 37 9.824516   10.0.0.4       128.119.245.12   UDP    70 64350 → 33436  Len=28
 38 9.825863   10.0.0.1       10.0.0.4         ICMP   70 Time-to-live exceeded (Time to live
 39 9.826039   10.0.0.4       128.119.245.12   UDP    70 64350 → 33437  Len=28
▶ Frame 33: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e), Dst: Technico_2a:72:09 (44:32:c8:2a:72:09)
▼ Internet Protocol Version 4, Src: 10.0.0.4, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0xfb5f (64351)
```

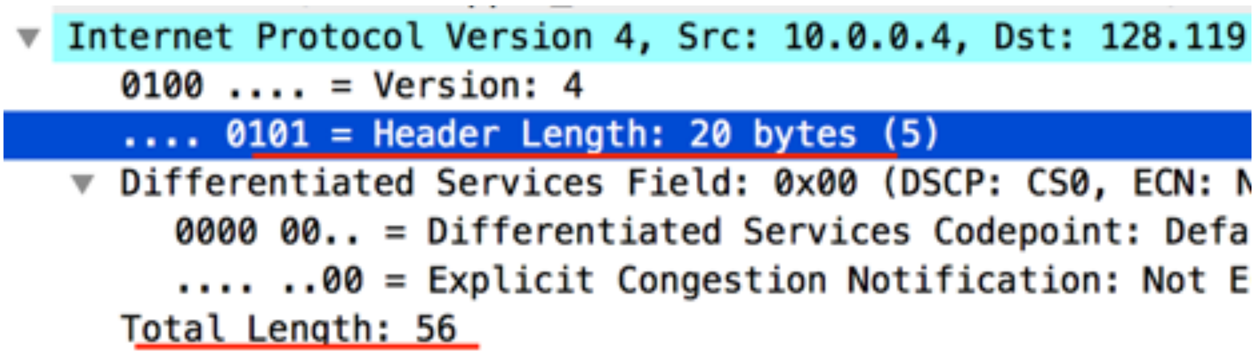
2. *Within the IP packet header, what is the value in the upper layer protocol field?*

   UDP(17)



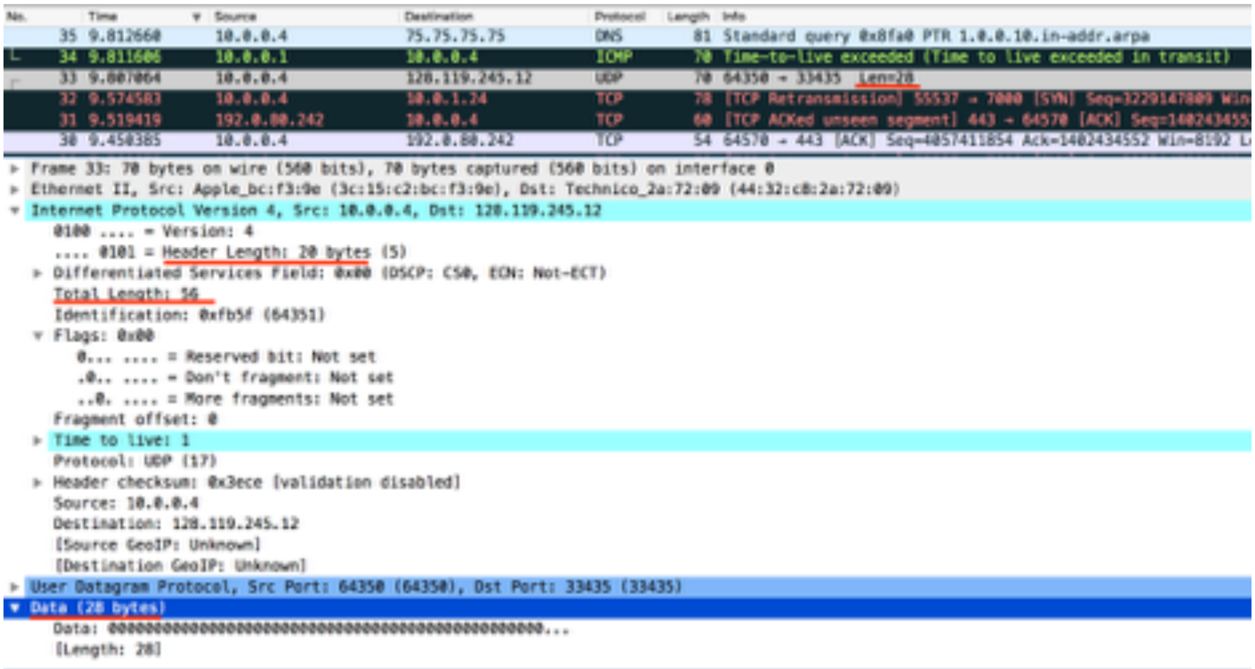
```
▶ Time to live: 1
  Protocol: UDP (17)
▶ Header checksum: 0x3ece [validation disab
```

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.*



```
▼ Internet Protocol Version 4, Src: 10.0.0.4, Dst: 128.119
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: N
      0000 00.. = Differentiated Services Codepoint: Defa
      .... ..00 = Explicit Congestion Notification: Not E
    Total Length: 56
```

The IP header is 20 bytes and the total length is 56 bytes, so to get the payload subtract 20 from 56 = 36 bytes. Except…

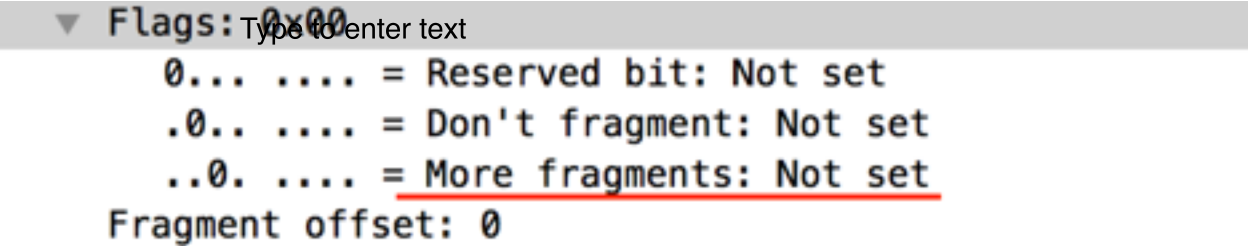


```
No.   Time        Source          Destination       Protocol Length Info
   35 9.812660    10.0.0.4        75.75.75.75       DNS       81 Standard query 0x8fa0 PTR 1.0.0.10.in-addr.arpa
   34 9.811606    10.0.0.1        10.0.0.4          ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   33 9.807064    10.0.0.4        128.119.245.12    UDP       70 64350 → 33435  Len=28
   32 9.574583    10.0.0.4        10.0.1.24         TCP       78 [TCP Retransmission] 55537 → 7000 [SYN] Seq=3229147809 Win
   31 9.519419    192.0.80.242    10.0.0.4          TCP       60 [TCP ACKed unseen segment] 443 → 64570 [ACK] Seq=140243455
   30 9.450385    10.0.0.4        192.0.80.242      TCP       54 64570 → 443 [ACK] Seq=4057411854 Ack=1402434552 Win=8192 L
```

```
▶ Frame 33: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
▶ Ethernet II, Src: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e), Dst: Technico_2a:72:09 (44:32:c8:2a:72:09)
▼ Internet Protocol Version 4, Src: 10.0.0.4, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xfb5f (64351)
  ▼ 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: UDP (17)
  ▶ Header checksum: 0x3ece [validation disabled]
    Source: 10.0.0.4
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▶ User Datagram Protocol, Src Port: 64350 (64350), Dst Port: 33435 (33435)
▼ Data (28 bytes)
    Data: 0000000000000000000000000000000000000000000000000...
    [Length: 28]
```

The data is listed as being of length 28, so I'm not really sure.

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



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

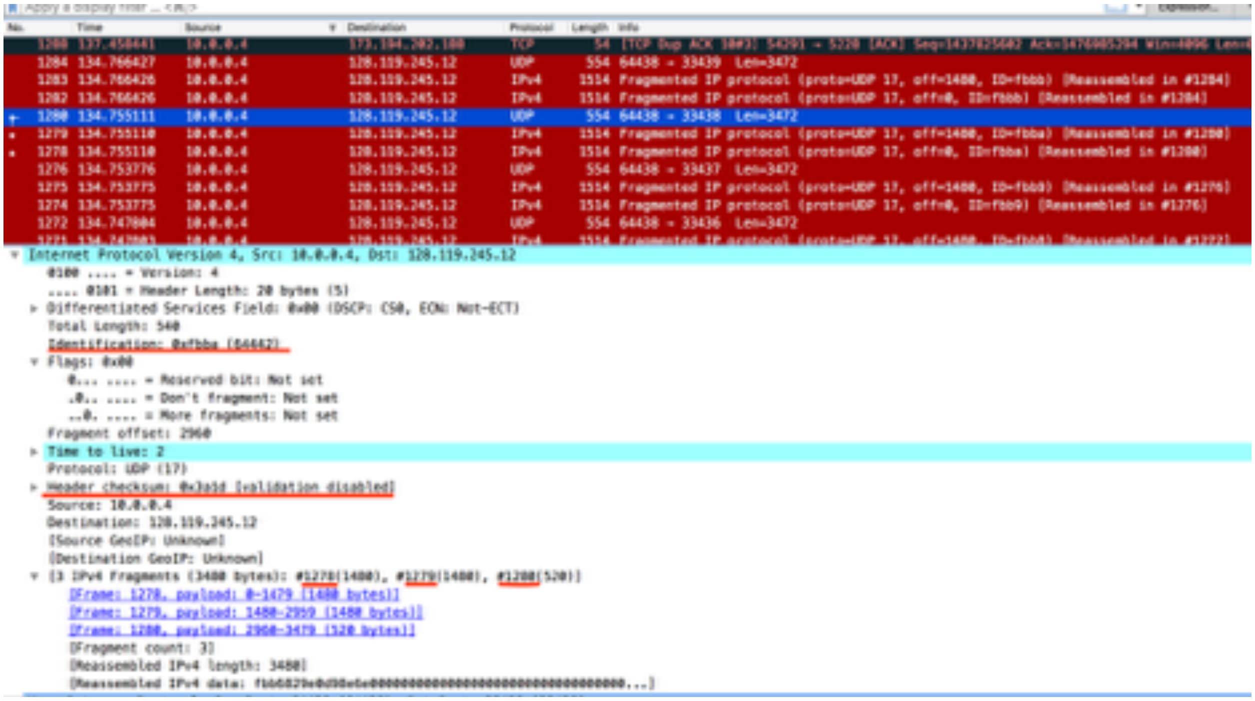
Type to enter text

No it has not. The "more fragments" flag is not set, and that gets set for all fragments except for the last one. Also, the fragment offset flag is 0, meaning there are no previous fragments in this datagram.

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?*

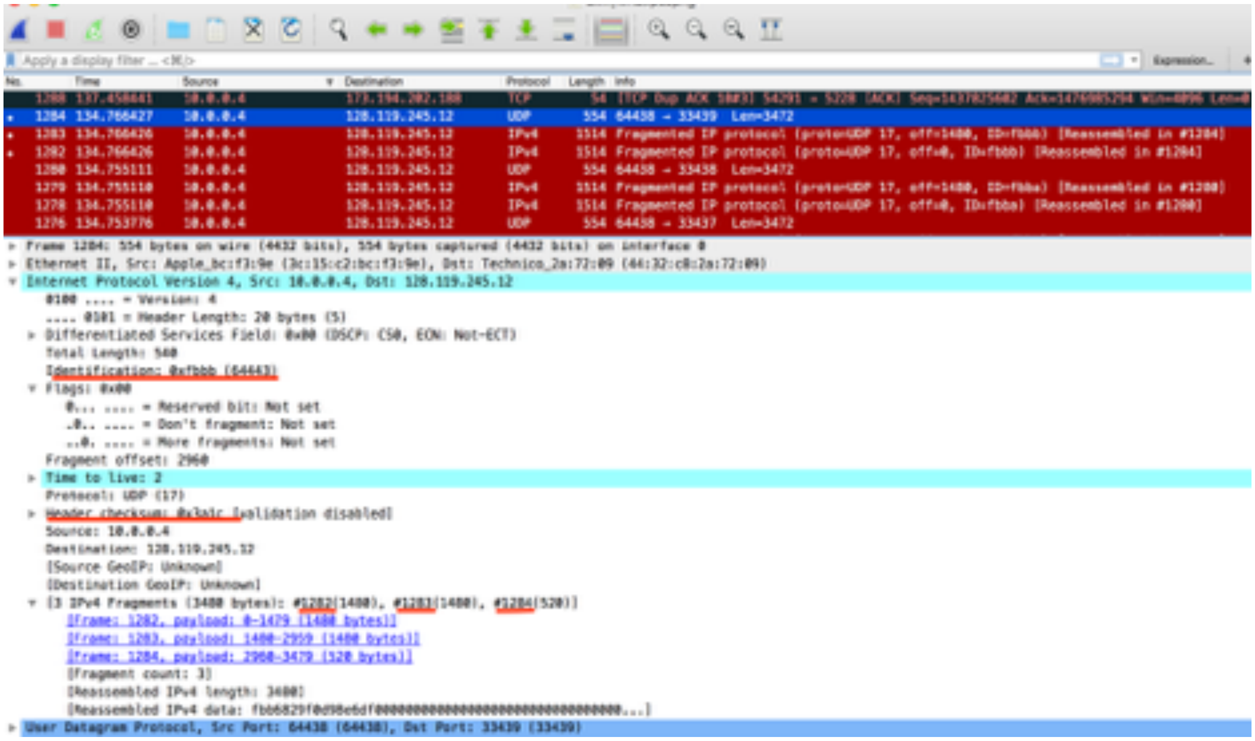
Header checksum, identification, and the frames listed in the (only sometimes visible) ip.fragments field change between each datagram.

Here is an example of these fields changing in subsequent datagrams (id 64442 and 64443):



```
No.   Time        Source     Destination     Protocol Length Info
1288 137.458441  10.0.0.4   173.194.202.188  TCP       54 [TCP Dup ACK 10#3] 54291 → 5228 [ACK] Seq=1437825682 Ack=1476985294 Win=4096 Len=0
1284 134.766427  10.0.0.4   128.119.245.12   UDP      554 64438 → 33439  Len=3472
1283 134.766426  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fbbb) [Reassembled in #1284]
1282 134.766426  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fbbb) [Reassembled in #1284]
1280 134.755111  10.0.0.4   128.119.245.12   UDP      554 64438 → 33438  Len=3472
1279 134.755110  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fbba) [Reassembled in #1280]
1278 134.755110  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fbba) [Reassembled in #1280]
1276 134.753776  10.0.0.4   128.119.245.12   UDP      554 64438 → 33437  Len=3472
1275 134.753775  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fbb9) [Reassembled in #1276]
1274 134.753775  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fbb9) [Reassembled in #1276]
1272 134.747004  10.0.0.4   128.119.245.12   UDP      554 64438 → 33436  Len=3472
1271 134.747003  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fbb8) [Reassembled in #1272]
▼ Internet Protocol Version 4, Src: 10.0.0.4, 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: 540
    Identification: 0xfbba (64442)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 2960
  ▶ Time to live: 2
    Protocol: UDP (17)
  ▶ Header checksum: 0x3a1d [validation disabled]
    Source: 10.0.0.4
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▼ [3 IPv4 Fragments (3480 bytes): #1278(1480), #1279(1480), #1280(520)]
      [Frame: 1278, payload: 0-1479 (1480 bytes)]
      [Frame: 1279, payload: 1480-2959 (1480 bytes)]
      [Frame: 1280, payload: 2960-3479 (520 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 3480]
      [Reassembled IPv4 data: fbb6829e0d98e6e0000000000000000000000000000000000...]
```

*6442^^*



```
No.   Time        Source     Destination     Protocol Length Info
1288 137.458441  10.0.0.4   173.194.202.188  TCP       54 [TCP Dup ACK 10#3] 54291 → 5228 [ACK] Seq=1437825682 Ack=1476985294 Win=4096 Len=0
1284 134.766427  10.0.0.4   128.119.245.12   UDP      554 64438 → 33439  Len=3472
1283 134.766426  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fbbb) [Reassembled in #1284]
1282 134.766426  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fbbb) [Reassembled in #1284]
1280 134.755111  10.0.0.4   128.119.245.12   UDP      554 64438 → 33438  Len=3472
1279 134.755110  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fbba) [Reassembled in #1280]
1278 134.755110  10.0.0.4   128.119.245.12   IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fbba) [Reassembled in #1280]
1276 134.753776  10.0.0.4   128.119.245.12   UDP      554 64438 → 33437  Len=3472
▶ Frame 1284: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
▶ Ethernet II, Src: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e), Dst: Technico_2a:72:09 (44:32:c8:2a:72:09)
▼ Internet Protocol Version 4, Src: 10.0.0.4, 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: 540
    Identification: 0xfbbb (64443)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 2960
  ▶ Time to live: 2
    Protocol: UDP (17)
  ▶ Header checksum: 0x3a1c [validation disabled]
    Source: 10.0.0.4
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▼ [3 IPv4 Fragments (3480 bytes): #1282(1480), #1283(1480), #1284(520)]
      [Frame: 1282, payload: 0-1479 (1480 bytes)]
      [Frame: 1283, payload: 1480-2959 (1480 bytes)]
      [Frame: 1284, payload: 2960-3479 (520 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 3480]
      [Reassembled IPv4 data: fbb6829f0d98e6df000000000000000000000000000000000...]
▶ User Datagram Protocol, Src Port: 64438 (64438), Dst Port: 33439 (33439)
```

*6443^^*

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

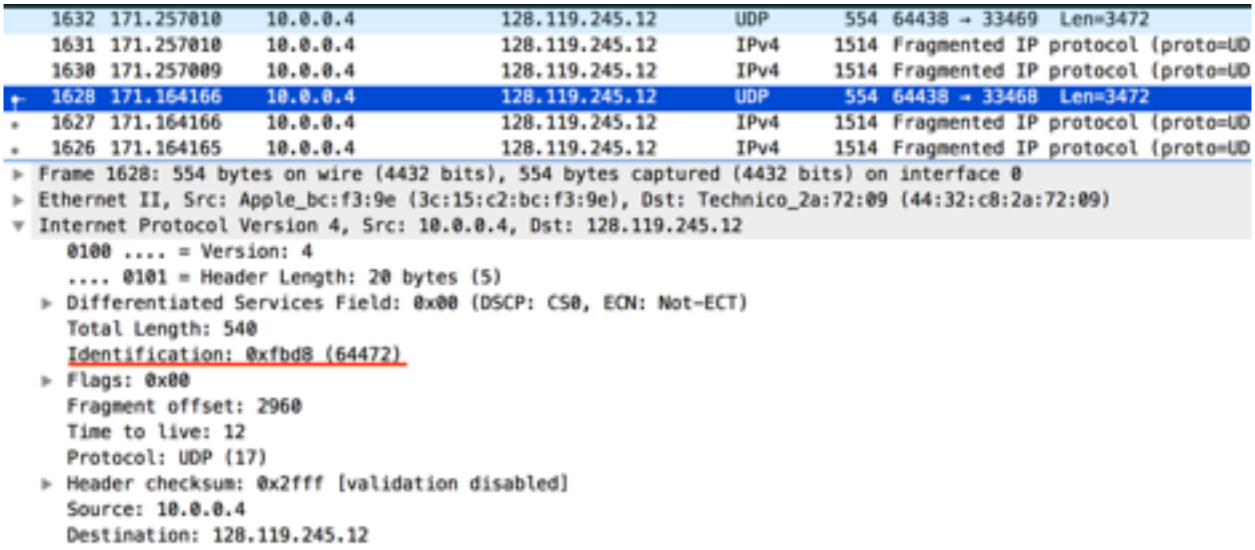
   These are consistent:
   IP Version: 4
   Header length: 20 bytes
   Protocol: UDP(17)
   Differentiated Services Field: 0x00000000
   Source: 10.0.0.4
   Destination: 128.119.245.12

   Which fields must stay constant: The upper-layer protocol (UDP 17), source, and destination must remain constant. The source remains constant because it was sent from my router, and the destination must remain constant so that the datagram is marked with the right address to go to the right destination. The upper-layer protocol remains UDP 17 because 17 is the port being used, and UDP is the transport-layer protocol being used, and it supports data transmission without the need of a handshake.

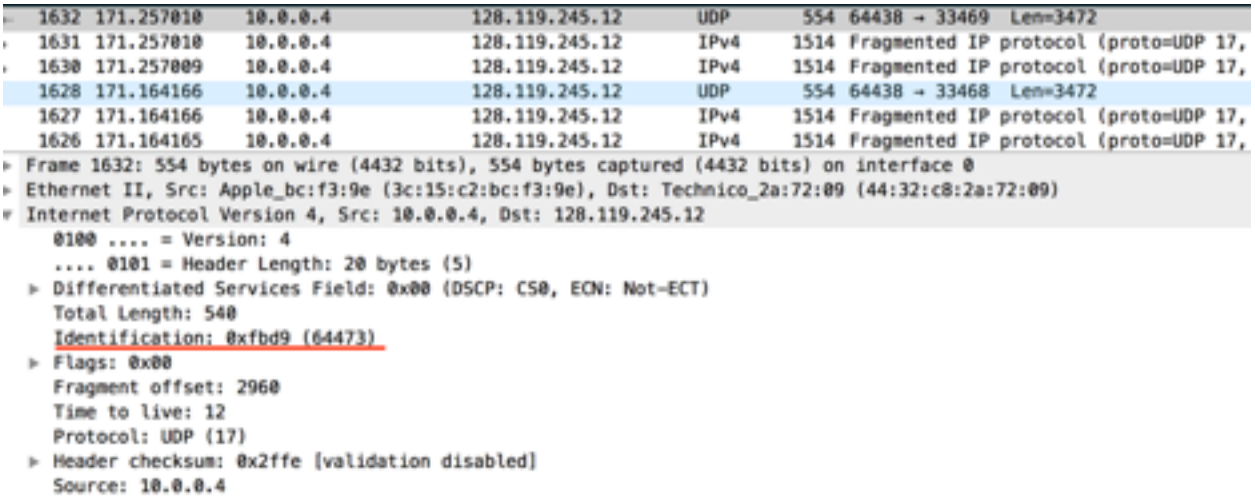
   Which fields must change: The identification field must change because it is used to uniquely identify the group of fragments of a single IP datagram. The header checksum must change because it is a calculation of the ones' complement of the ones' complement sum of the header's 16-bit words, and seeing as the identification field changes each time, it follows that so too will the checksum.

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

   They are incremented by 1 with each UDP packet. For example, these subsequent UDP packets with the identification numbers 64472 and 64473:



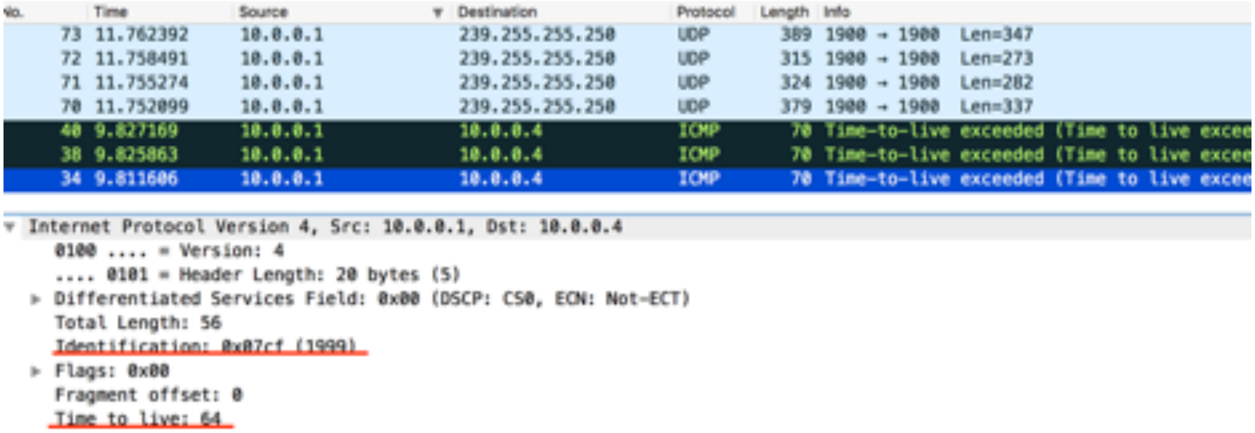
```
   1632 171.257010    10.0.0.4          128.119.245.12     UDP      554 64438 → 33469  Len=3472
   1631 171.257010    10.0.0.4          128.119.245.12     IPv4    1514 Fragmented IP protocol (proto=UD
   1630 171.257009    10.0.0.4          128.119.245.12     IPv4    1514 Fragmented IP protocol (proto=UD
   1628 171.164166    10.0.0.4          128.119.245.12     UDP      554 64438 → 33468  Len=3472
   1627 171.164166    10.0.0.4          128.119.245.12     IPv4    1514 Fragmented IP protocol (proto=UD
   1626 171.164165    10.0.0.4          128.119.245.12     IPv4    1514 Fragmented IP protocol (proto=UD
▶ Frame 1628: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
▶ Ethernet II, Src: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e), Dst: Technico_2a:72:09 (44:32:c8:2a:72:09)
▼ Internet Protocol Version 4, Src: 10.0.0.4, 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: 540
    Identification: 0xfbd8 (64472)
  ▶ Flags: 0x00
    Fragment offset: 2960
    Time to live: 12
    Protocol: UDP (17)
  ▶ Header checksum: 0x2fff [validation disabled]
    Source: 10.0.0.4
    Destination: 128.119.245.12
```



```
1632 171.257010  10.0.0.4       128.119.245.12   UDP     554 64438 → 33469  Len=3472
1631 171.257010  10.0.0.4       128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=UDP 17,
1630 171.257009  10.0.0.4       128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=UDP 17,
1628 171.164166  10.0.0.4       128.119.245.12   UDP     554 64438 → 33468  Len=3472
1627 171.164166  10.0.0.4       128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=UDP 17,
1626 171.164165  10.0.0.4       128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=UDP 17,
▸ Frame 1632: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface 0
▸ Ethernet II, Src: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e), Dst: Technico_2a:72:09 (44:32:c8:2a:72:09)
▾ Internet Protocol Version 4, Src: 10.0.0.4, 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: 540
    Identification: 0xfbd9 (64473)
  ▸ Flags: 0x00
    Fragment offset: 2960
    Time to live: 12
    Protocol: UDP (17)
  ▸ Header checksum: 0x2ffe [validation disabled]
    Source: 10.0.0.4
```

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

8. *What is the value in the Identification field and the TTL field?*
The identification field has a value of 0x07cf (1999) and the TTL field has a value of 64.



```
No.  Time        Source          Destination        Protocol  Length Info
  73 11.762392   10.0.0.1        239.255.255.250    UDP        389 1900 → 1900  Len=347
  72 11.758491   10.0.0.1        239.255.255.250    UDP        315 1900 → 1900  Len=273
  71 11.755274   10.0.0.1        239.255.255.250    UDP        324 1900 → 1900  Len=282
  70 11.752099   10.0.0.1        239.255.255.250    UDP        379 1900 → 1900  Len=337
  40 9.827169    10.0.0.1        10.0.0.4           ICMP        70 Time-to-live exceeded (Time to live excee
  38 9.825863    10.0.0.1        10.0.0.4           ICMP        70 Time-to-live exceeded (Time to live excee
  34 9.811606    10.0.0.1        10.0.0.4           ICMP        70 Time-to-live exceeded (Time to live excee

▾ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x07cf (1999)
  ▸ Flags: 0x00
    Fragment offset: 0
    Time to live: 64
```

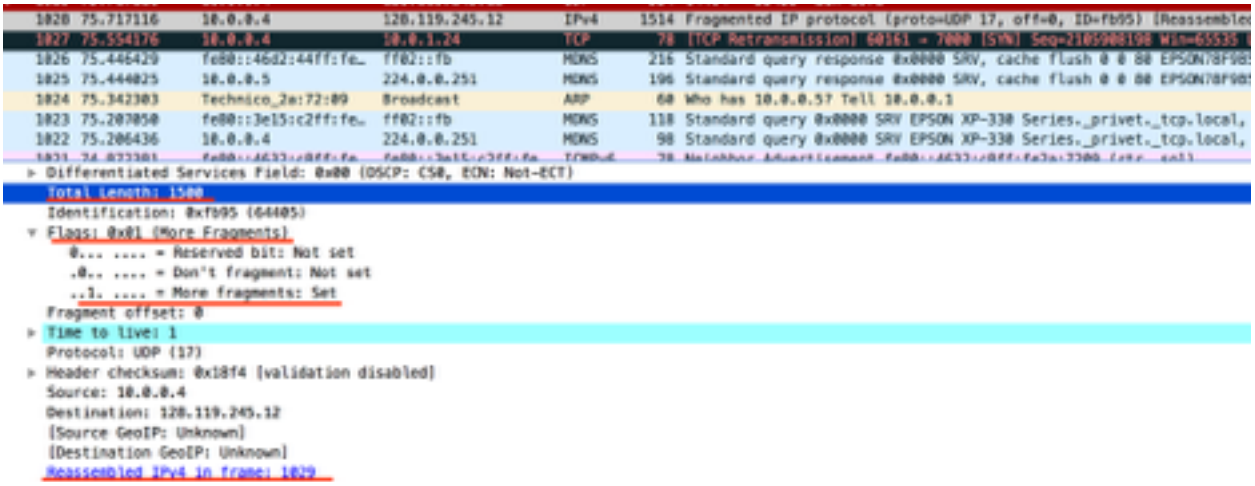
9. *Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?*

   The identification changes each time, because that is a unique identifier, but the Time to Live remains the same because this all refers to the same hop, and 64 is the limit for this particular hop.

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, it has.

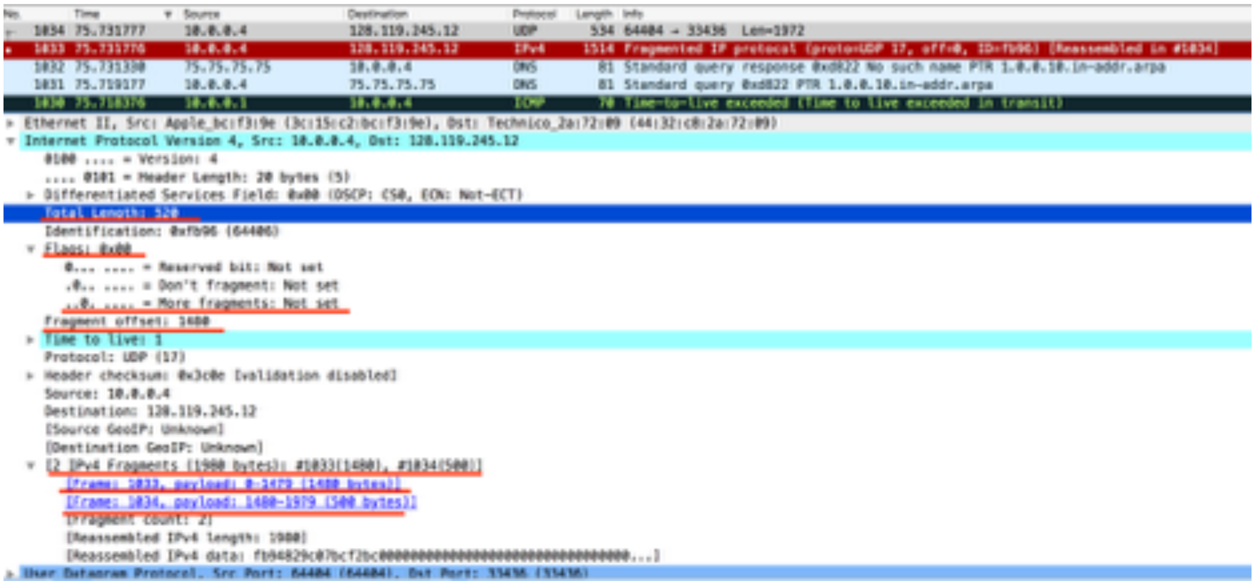
11. *Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?*



```
1028 75.717116   10.0.0.4              128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fb95) [Reassembled
1027 75.554176   10.0.0.4              10.0.1.24        TCP      78 [TCP Retransmission] 60161 → 7000 [SYN] Seq=2105908198 Win=65535
1026 75.446429   fe80::46d2:44ff:fe…   ff02::fb         MDNS    216 Standard query response 0x0000 SRV, cache flush 0 0 80 EPSON78F98
1025 75.444025   10.0.0.5              224.0.0.251      MDNS    196 Standard query response 0x0000 SRV, cache flush 0 0 80 EPSON78F98
1024 75.342303   Technico_2a:72:09     Broadcast        ARP      60 Who has 10.0.0.5? Tell 10.0.0.1
1023 75.207050   fe80::3e15:c2ff:fe…   ff02::fb         MDNS    118 Standard query 0x0000 SRV EPSON XP-330 Series._privet._tcp.local,
1022 75.206436   10.0.0.4              224.0.0.251      MDNS     98 Standard query 0x0000 SRV EPSON XP-330 Series._privet._tcp.local,
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xfb95 (64405)
  ▾ 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: UDP (17)
  ▸ Header checksum: 0x18f4 [validation disabled]
    Source: 10.0.0.4
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 1029
```

The information in the IP address header to indicate that the datagram has been fragmented is the Flags field, which, when opened, shows the "more fragments" flag having been set. The indicator that this is the first fragment is that the fragment offset is set to 0. This IP datagram is 1500 bytes long.

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



```
No.   Time         Source      Destination      Protocol Length Info
1034  75.731777    10.0.0.4    128.119.245.12   UDP       534 64404 → 33436  Len=1972
1033  75.731776    10.0.0.4    128.119.245.12   IPv4     1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fb96) [Reassembled in #1034]
1032  75.731330    75.75.75.75 10.0.0.4         DNS        81 Standard query response 0xd822 No such name PTR 1.0.0.10.in-addr.arpa
1031  75.719177    10.0.0.4    75.75.75.75      DNS        81 Standard query 0xd822 PTR 1.0.0.10.in-addr.arpa
1030  75.718376    10.0.0.1    10.0.0.4         ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
▸ Ethernet II, Src: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e), Dst: Technico_2a:72:09 (44:32:c8:2a:72:09)
▾ Internet Protocol Version 4, Src: 10.0.0.4, 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: 520
    Identification: 0xfb96 (64406)
  ▾ 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: UDP (17)
  ▸ Header checksum: 0x3c0e [validation disabled]
    Source: 10.0.0.4
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▾ [2 IPv4 Fragments (1980 bytes): #1033(1480), #1034(500)]
      [Frame: 1033, payload: 0-1479 (1480 bytes)]
      [Frame: 1034, payload: 1480-1979 (500 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1980]
      [Reassembled IPv4 data: fb94829c07bcf2bc00000000000000000000000000000000...]
▸ User Datagram Protocol, Src Port: 64404 (64404), Dst Port: 33436 (33436)
```

You can tell that this is not the first fragment in the datagram fragment by the fact that the Fragment offset is at 1480 (this was the payload size of the first fragment). There are not more fragments. You can tell this by the fact that the "more fragments" flag is not set, and all fragmented flags except the last have the "more fragments" flag set.

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

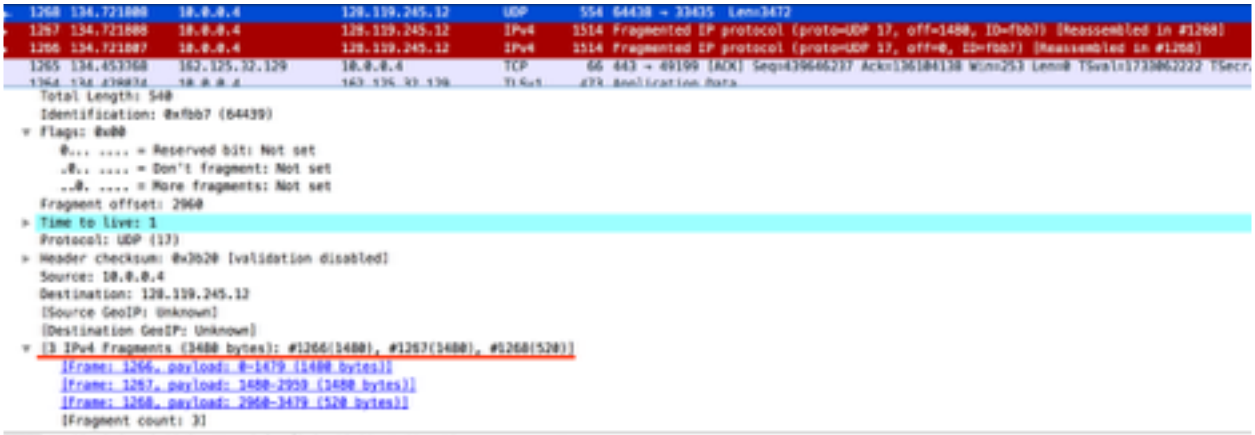
In the second fragment, frame 1034, there is a field called ip.fragments with the description:
2 IPv4 Fragments (1980 bytes): #1033(1480), #1034(500)
Frame: 1033, payload: 0-1479 (1480 bytes)
Frame: 1034, payload: 1480-1979 (500 bytes)

This is missing from the first fragment, frame 1033.

Some other differences:
-The fragment offset in frame 1033 is 0, and in frame 1034 is 1480.
-The total length field in frame 1033 is 1500, and in 1034 is 520.
-The header checksum field in 1033 is 0x18f3 and in 1034 is 0x3c0e.
-The Flags field in 1033 is 0x01 and in 1034 is 0x00.

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

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

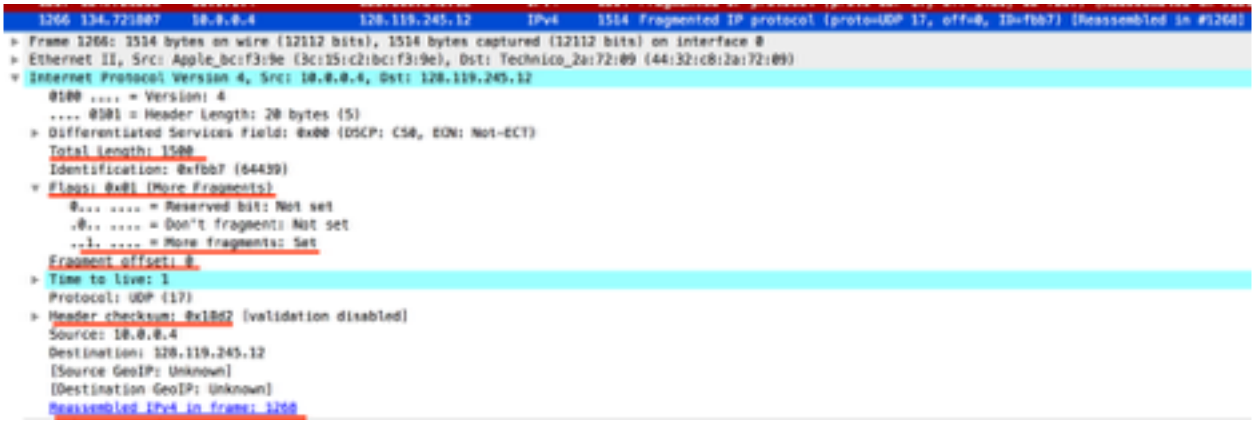


```
1268 134.721888   10.0.0.4         128.119.245.12   UDP     554  64438 → 33435  Len=3472
1267 134.721888   10.0.0.4         128.119.245.12   IPv4   1514  Fragmented IP protocol (proto=UDP 17, off=1480, ID=fbb7) [Reassembled in #1268]
1266 134.721887   10.0.0.4         128.119.245.12   IPv4   1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=fbb7) [Reassembled in #1268]
1265 134.453768   162.125.32.129   10.0.0.4         TCP      66  443 → 49199 [ACK] Seq=439646237 Ack=136184138 Win=253 Len=0 TSval=1733062222 TSecr
1264 134.439874   10.0.0.4         162.125.32.129   TLSv1   473  Application Data
    Total Length: 540
    Identification: 0xfbb7 (64439)
  ▾ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 2960
  ▸ Time to live: 1
    Protocol: UDP (17)
  ▸ Header checksum: 0x3b20 [validation disabled]
    Source: 10.0.0.4
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▾ [3 IPv4 Fragments (3480 bytes): #1266(1480), #1267(1480), #1268(520)]
      [Frame: 1266, payload: 0-1479 (1480 bytes)]
      [Frame: 1267, payload: 1480-2959 (1480 bytes)]
      [Frame: 1268, payload: 2960-3479 (520 bytes)]
      [Fragment count: 3]
```

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

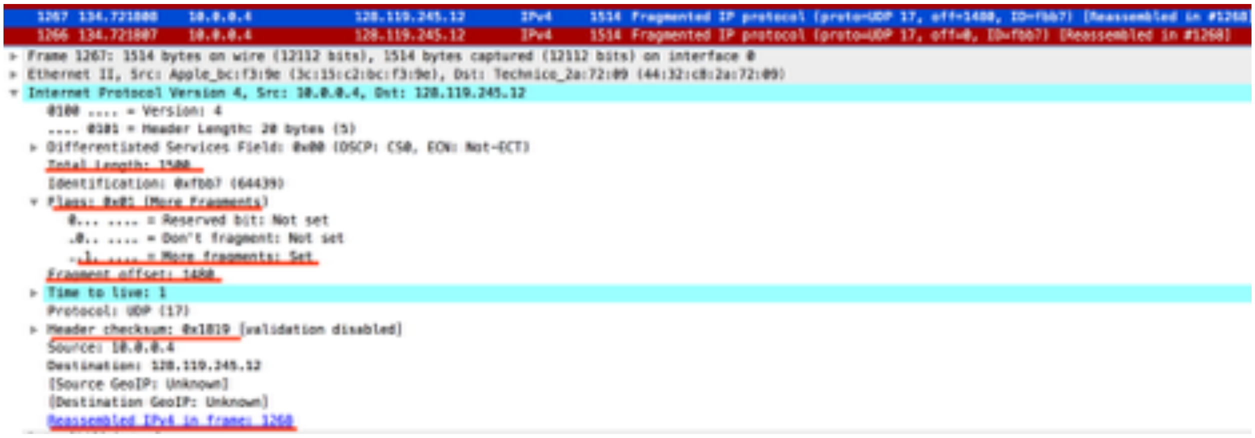
In the first fragment, frame 1266, the Fragment Offset field is 0, then it is 1480 in the second (frame 1267), then it is 2960 in the third (frame 1268).
The Total Length field of the first two is 1500, and in the third it is 540.
The Header Checksum is different for all three.
The flags are set to 0x01 (more fragments) for the first two, and 0x00 for the third.
The first two have a field ip.reassembled_in which has the value1268 for both, and the last has a field ip.fragments which has a very long value and a description of 3 IPv4 Fragments (3480 bytes): #1266(1480), #1267(1480), #1268(520).

Images:



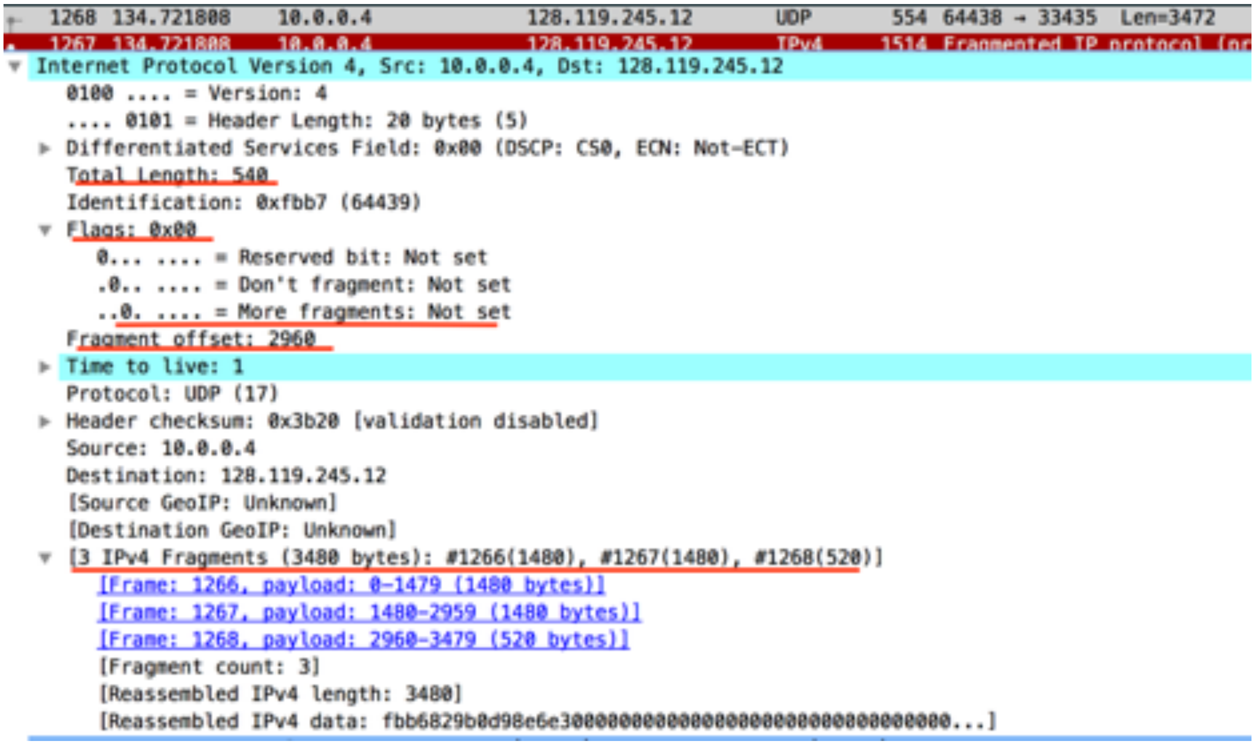
```
1266 134.721807   10.0.0.4        128.119.245.12     IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fbb7) [Reassembled in #1268]
▸ Frame 1266: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▸ Ethernet II, Src: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e), Dst: Technico_2a:72:09 (44:32:c8:2a:72:09)
▾ Internet Protocol Version 4, Src: 10.0.0.4, 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: 0xfbb7 (64439)
  ▾ 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: UDP (17)
  ▸ Header checksum: 0x18d2 [validation disabled]
    Source: 10.0.0.4
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 1268
```

Frame 1266^^



```
1267 134.721808   10.0.0.4        128.119.245.12     IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=fbb7) [Reassembled in #1268]
1266 134.721807   10.0.0.4        128.119.245.12     IPv4    1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=fbb7) [Reassembled in #1268]
▸ Frame 1267: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▸ Ethernet II, Src: Apple_bc:f3:9e (3c:15:c2:bc:f3:9e), Dst: Technico_2a:72:09 (44:32:c8:2a:72:09)
▾ Internet Protocol Version 4, Src: 10.0.0.4, 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: 0xfbb7 (64439)
  ▾ Flags: 0x01 (More Fragments)
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment offset: 1480
  ▸ Time to live: 1
    Protocol: UDP (17)
  ▸ Header checksum: 0x1819 [validation disabled]
    Source: 10.0.0.4
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 1268
```

Frame 1267^^



```
  1268 134.721808    10.0.0.4              128.119.245.12       UDP       554  64438 → 33435   Len=3472
  1267 134.721808    10.0.0.4              128.119.245.12       IPv4      1514 Fragmented IP protocol (pr
▼ Internet Protocol Version 4, Src: 10.0.0.4, 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: 540
    Identification: 0xfbb7 (64439)
  ▼ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 2960
  ▶ Time to live: 1
    Protocol: UDP (17)
  ▶ Header checksum: 0x3b20 [validation disabled]
    Source: 10.0.0.4
    Destination: 128.119.245.12
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ▼ [3 IPv4 Fragments (3480 bytes): #1266(1480), #1267(1480), #1268(520)]
      [Frame: 1266, payload: 0-1479 (1480 bytes)]
      [Frame: 1267, payload: 1480-2959 (1480 bytes)]
      [Frame: 1268, payload: 2960-3479 (520 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 3480]
      [Reassembled IPv4 data: fbb6829b0d98e6e30000000000000000000000000000000000...]
```

Frame 1268^^