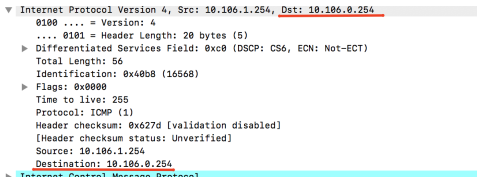
A Look at the Captured Trace

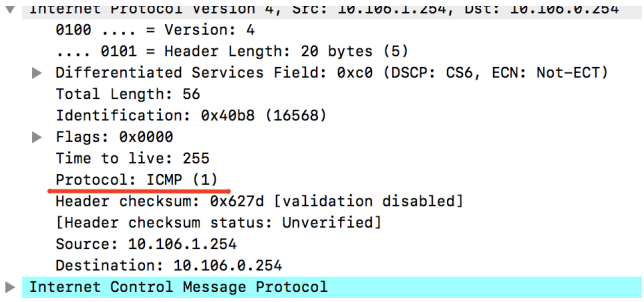
1. Select the first ICMP echo request message sent by your computer and expand the internet protocol part of the packet int he packet detials window. What ist he IP address of your computer?



   - The IP Address of my computer is: 10.106.0.254

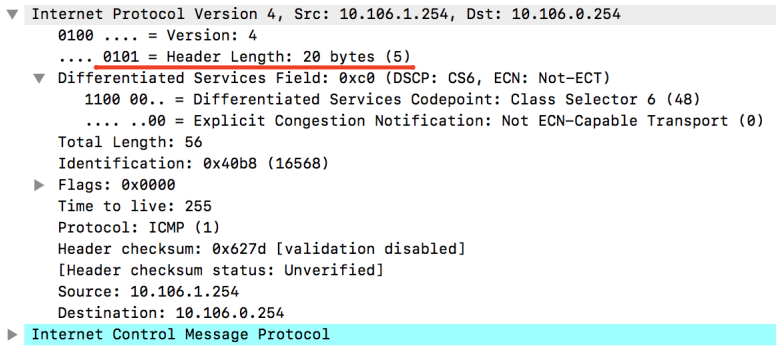
2. Within the IP packet header, what is the value in the upper layer protocol field?

   - The value in the upper layer protocol field is ICMP(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:
     - Size: 20 bytes



   - Payload:
     - The size of the payload is all of the data in the ICMP excluding the header (56 total - 20 header bytes)

```
▼ Internet Protocol Version 4, Src: 10.106.1.254, Dst: 10.106.0.254
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x40b8 (16568)
  ▶ Flags: 0x0000
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x627d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.106.1.254
    Destination: 10.106.0.254
▶ Internet Control Message Protocol
```

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

   - Wireshark tells us fragmentation has occured if the Fragmentation bit is set, or the Fragmentation offset is greater than 0. Our fragmentation bit is set to 0 and our fragmentation offset is also set to 0, so our IP Datagram has not been fragmented.

```
▼ 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: 255
```

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 TTL field, and the Identification field change from packet to packet.
   - Packet A:

```
  Total Length: 56
  Identification: 0x40b8 (16568)
▼ Flags: 0x0000
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not s
    ..0. .... .... .... = More fragments: Not s
    ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 255
```

   - Packet B:

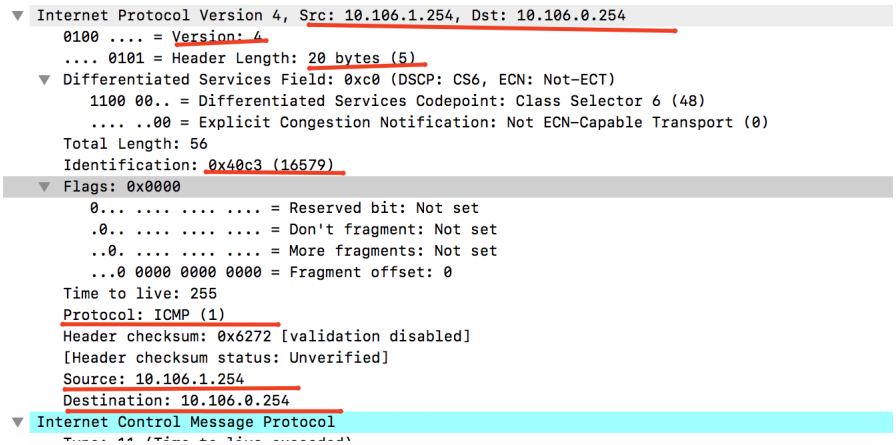
```
  Total Length: 56
  Identification: 0x0595 (1429)
▼ Flags: 0x0000
    0... .... .... .... = Reserved bit: Not se
    .0.. .... .... .... = Don't fragment: Not
    ..0. .... .... .... = More fragments: Not
    ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 63
  Protocol: ICMP (1)
```

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

- As Stated earlier the fields that change are:
  - TTL Field: the TTL field increments as seen earlier, this is how the router communicates.
  - Identification Field: Every IP Datagram must have a unique identifier
- The Fields that remeain constant are:
  - The Internet Protocol Version
  - The Header Length
  - Src IP
  - Dst IP
  - Upper Layer Protocol Field
- Packet A:

```
▼ Internet Protocol Version 4, Src: 10.106.1.254, Dst: 10.106.0.254
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▼ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 56
    Identification: 0x40b8 (16568)
  ▼ 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: 255
    Protocol: ICMP (1)
    Header checksum: 0x627d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.106.1.254
    Destination: 10.106.0.254
▼ Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x7db9 [correct]
    [Checksum Status: Good]
  ▼ Internet Protocol Version 4, Src: 10.106.0.254, 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: 1500
      Identification: 0xa06b (41067)
    ▼ Flags: 0x2000, More fragments
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..1. .... .... .... = More fragments: Set
```

- Packet B:

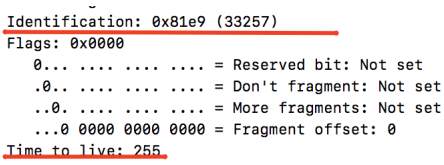


7. Describe the pattern you see in the values in the IDentification field of the IP Datagram

   - The Identification fields appear to be increasing in the Internet Protocol Version 4 field, and in the ICMP fields they appear to be decreasing.

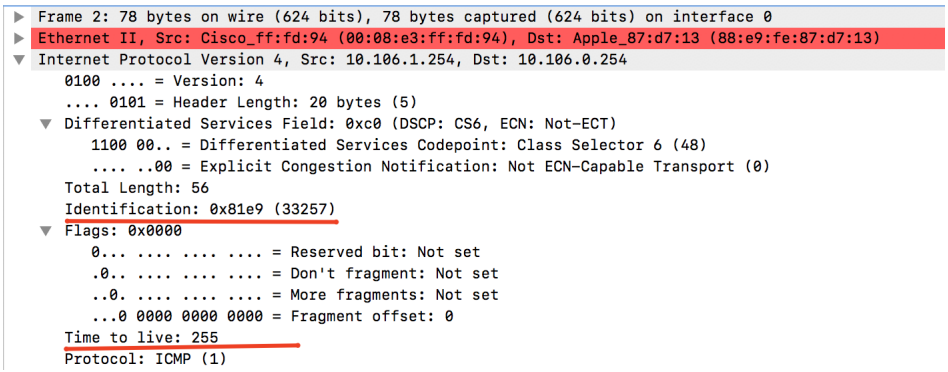
8. What is the value in the Identification field and the TTL field?

   - Identification Field: 0x81e9
   - TTL Field 255

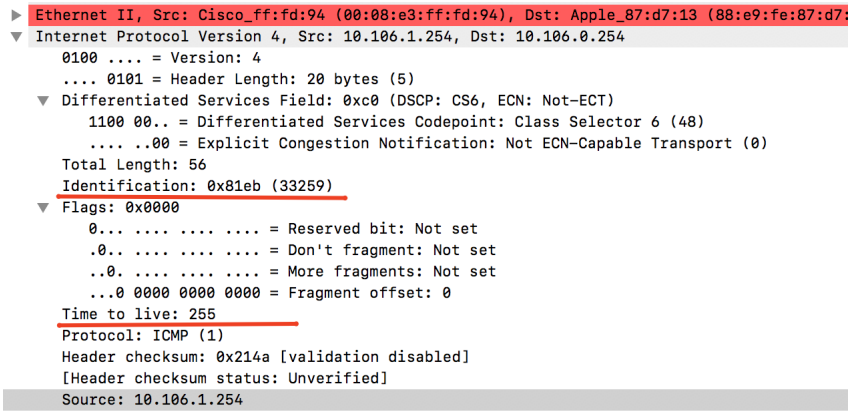


9. Do these values remain uncahnged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

   - The Identification field changes because each packet needs a unique identifier
   - The TTL remains the same because the first hop router hasn't decremented the TTL field yet.
   - Packet A:

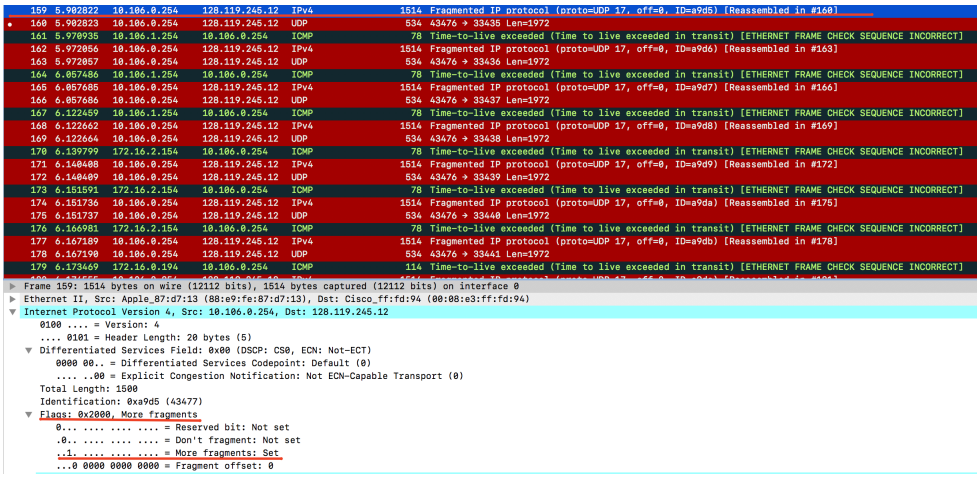


- Packet B:



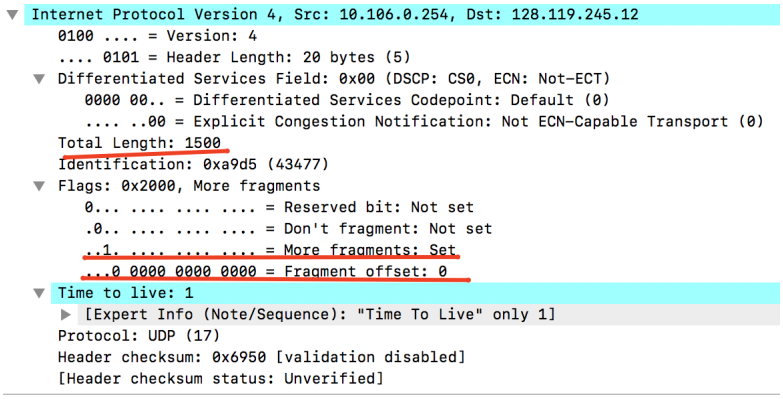
10. Find the first ICMP echo request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000.

    - Yes, the packet has been fragmented across more than one IP Datagram



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

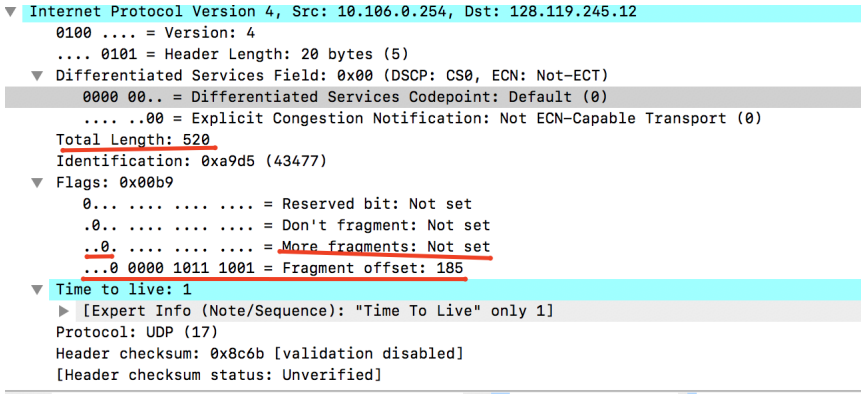
    - As stated above, if the Fragment Offset is > 0 or the Fragmentation Bit is set, we can tell the IP datagram has been fragmented.
    - The 'More Fragments' offset determines the position of the current fragment in the IP datagram, because the fragment offise is zero we are working with the first fragment.
    - The IP datagram is 1500 bytes



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?

    - We know this isn't the first fragmented IP datagram because the Fragment Offset is > 0.

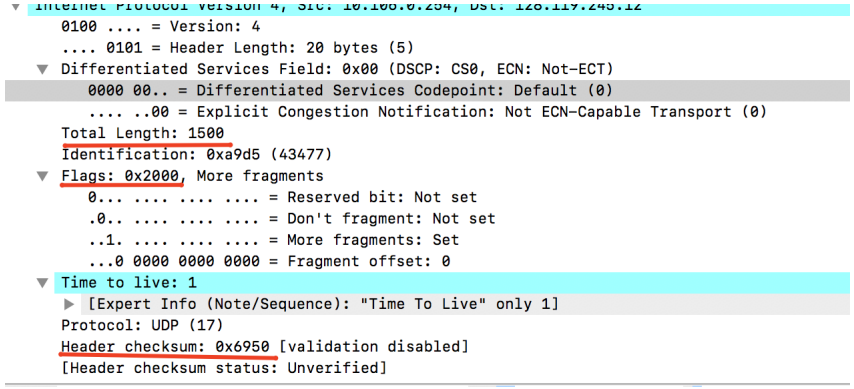
- There are no more fragments following because the 'More Fragments' bit is not set.



-

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

    - The Length of the IP datagram changes
    - The Flags field changes, specifically the Fragmentation Bit, and the Fragmentation Offset subfields
    - The header checksum changes
    - Packet A:



    - Packet B:

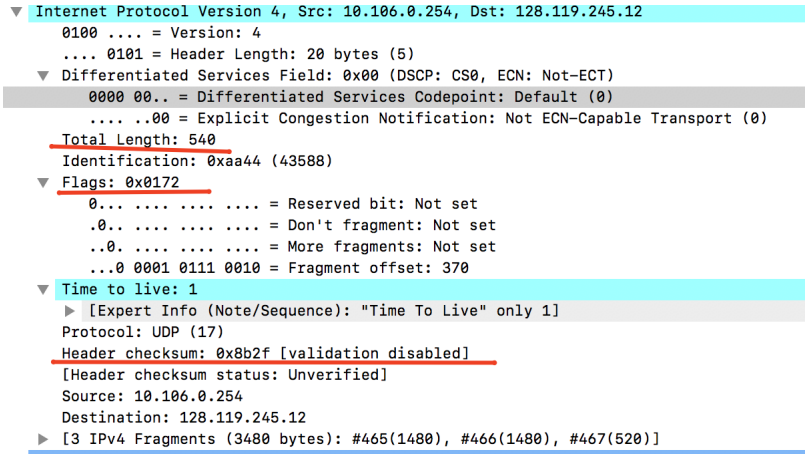
```
▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 520
  Identification: 0xa9d5 (43477)
▼ Flags: 0x00b9
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..0. .... .... .... = More fragments: Not set
    ...0 0000 1011 1001 = Fragment offset: 185
▼ Time to live: 1
  ▶ [Expert Info (Note/Sequence): "Time To Live" only 1]
  Protocol: UDP (17)
  Header checksum: 0x8c6b [validation disabled]
  [Header checksum status: Unverified]
```

14. How many Fragments were created from the original IP datagram?

    - 3 Fragments were created from the original
    -
    ```
    1514  Fragmented IP protocol (proto=UDP 17, off=0, ID=aa44) [Reassembled in #467]
    1514  Fragmented IP protocol (proto=UDP 17, off=1480, ID=aa44) [Reassembled in #467]
     554  43587 → 33435 Len=3472
    ```

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

    - The Length of the IP datagram changes
    - The flags field changes, specifically the fragmentation bit, and the fragmentation offset subfields
    - The header checksum changes
    - Packet A:
    ```
    ▼ Internet Protocol Version 4, Src: 10.106.0.254, 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: 1500
        Identification: 0xaa44 (43588)
      ▼ Flags: 0x20b9, More fragments
          0... .... .... .... = Reserved bit: Not set
          .0.. .... .... .... = Don't fragment: Not set
          ..1. .... .... .... = More fragments: Set
          ...0 0000 1011 1001 = Fragment offset: 185
      ▼ Time to live: 1
        ▶ [Expert Info (Note/Sequence): "Time To Live" only 1]
        Protocol: UDP (17)
        Header checksum: 0x6828 [validation disabled]
        [Header checksum status: Unverified]
        Source: 10.106.0.254
        Destination: 128.119.245.12
        Reassembled IPv4 in frame: 467
    ```
    - Packet B:


Internet Protocol Version 4, Src: 10.106.0.254, 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: 540
Identification: 0xaa44 (43588)
Flags: 0x0172
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0001 0111 0010 = Fragment offset: 370
Time to live: 1
[Expert Info (Note/Sequence): "Time To Live" only 1]
Protocol: UDP (17)
Header checksum: 0x8b2f [validation disabled]
[Header checksum status: Unverified]
Source: 10.106.0.254
Destination: 128.119.245.12
[3 IPv4 Fragments (3480 bytes): #465(1480), #466(1480), #467(520)]