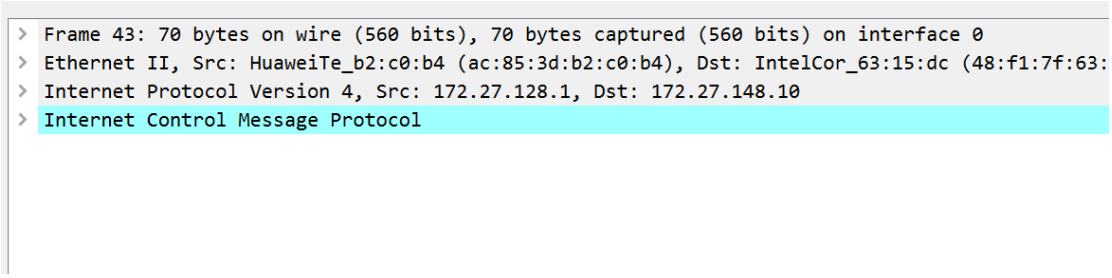
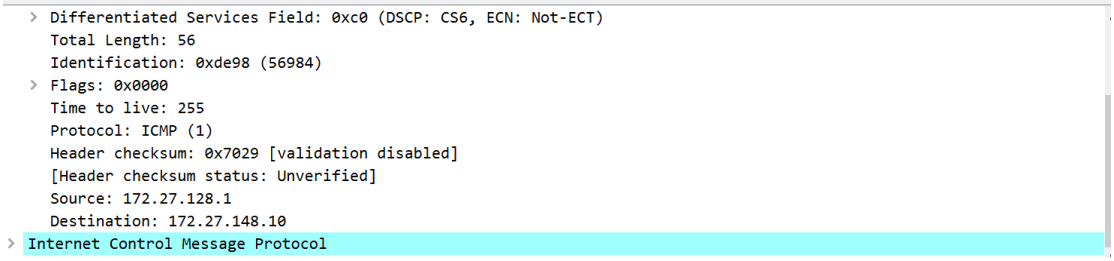
Wireshark Lab: IP v7.0

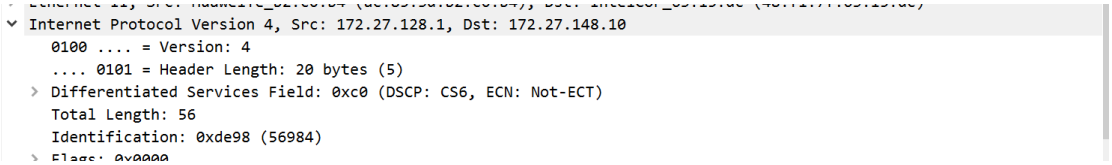
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?
   IP: 172.27.128.1



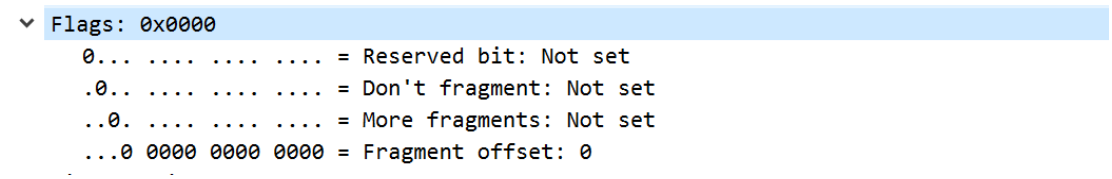
2. Within the IP packet header, what is the value in the upper layer protocol field?
   为 ICMP 协议，值为 1



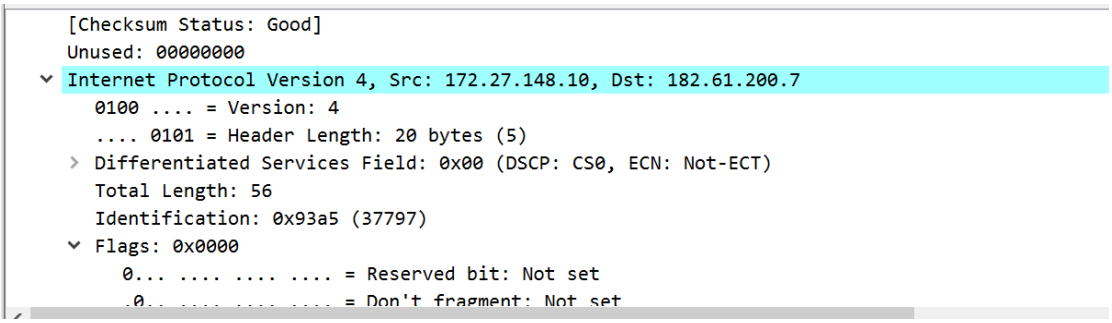
3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
   头部有 20Bytes，一共有 56Bytes，IP 数据报有 36Bytes



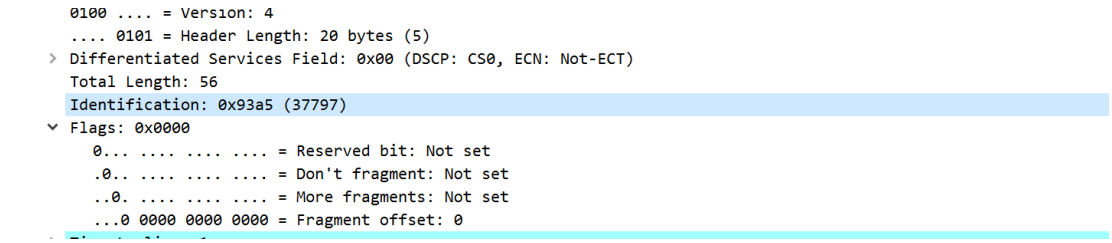
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
   未开启分段，应该没有



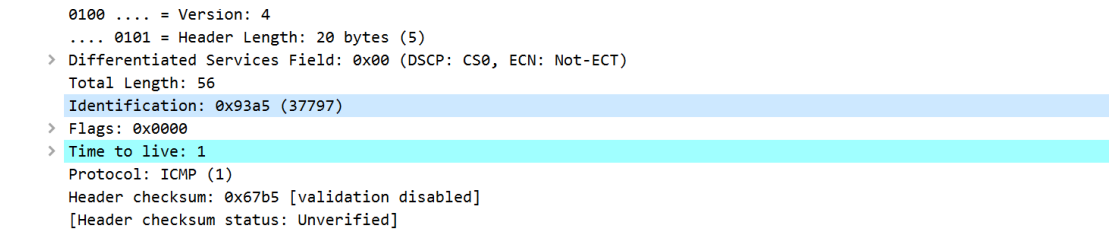
5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?
   标识符、存活时间、IP 头校验码会一直变



6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?
   必须更改每次路由跟踪的序列号、校验值，以及每个 PING 的 TTL。暂时保持不变的是这次路由跟踪，有很多的 PING 的目标数据长度。目标和本地 IP、可选选项、显式拥塞通告、标识符、偏移量、协议和版本这些字段必须保持的不变的。
7. Describe the pattern you see in the values in the Identification field of the IP datagram
   这是 16Bits 标识符



8. What is the value in the Identification field and the TTL field?
   ID 字段：37797，TTL 为 1



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?
   IP 数据报的 ID 字段改变，TTL 字段不变。
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? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3]
    是的，已经分片。

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 520
  Identification: 0x93d7 (37847)
v 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: 255
  Protocol: ICMP (1)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
```

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?
通过 IP 数据头的标志位分段标志可以发现已经被分段，通过偏移量发现这是第一个片段，这个数据报有 1500Byte。

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 520
  Identification: 0x93d7 (37847)
v 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: 255
  Protocol: ICMP (1)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
```

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?
通过观察偏移量。

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 520
  Identification: 0x93d8 (37848)
v 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
  Protocol: ICMP (1)
  Header checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
```

13. What fields change in the IP header between the first and second fragment?
ID、标志位、校验码、偏移量。
14. How many fragments were created from the original datagram?
3 个

```
  Source: 172.27.148.10
  Destination: 182.61.200.7
v [3 IPv4 Fragments (3480 bytes): #1006(1480), #1007(1480), #1008(520)]
    [Frame: 1006, payload: 0-1479 (1480 bytes)]
    [Frame: 1007, payload: 1480-2959 (1480 bytes)]
    [Frame: 1008, payload: 2960-3479 (520 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 3480]
    [Reassembled IPv4 data: 08001d890001009c2020202020202020202020202020202020…]
```

15. What fields change in the IP header among the fragments?
ID、标志位、校验码、偏移量。