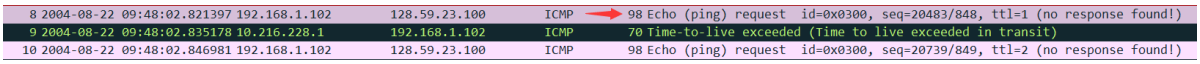
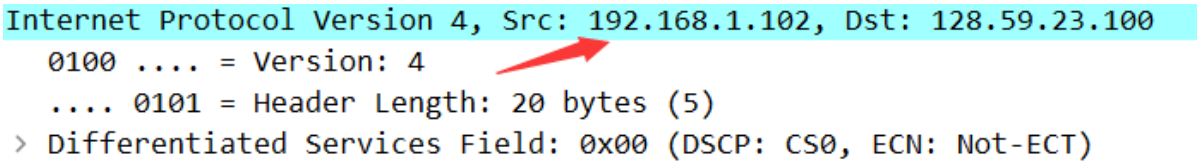
IP实验

Q1

> 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?

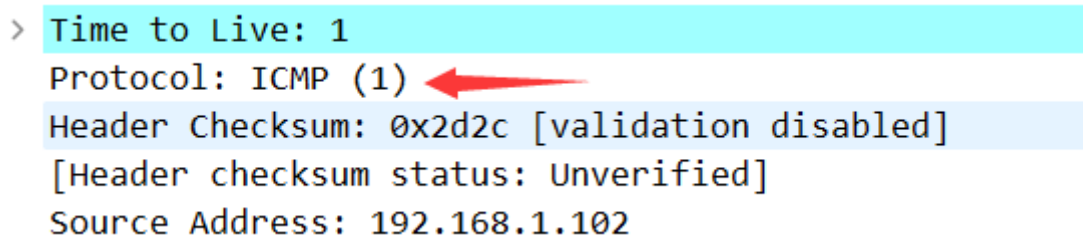




IP为192.168.1.102

Q2

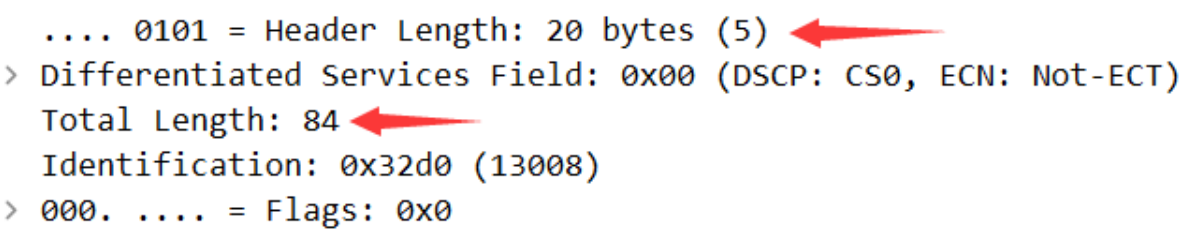
> Within the IP packet header, what is the value in the upper layer protocol field?



ICMP（1）

Q3

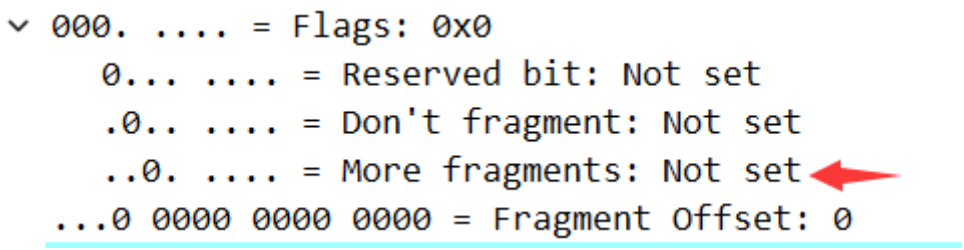
> How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.



报头20字节，总共84字节，所以payload bytes是84-20=64字节

Q4

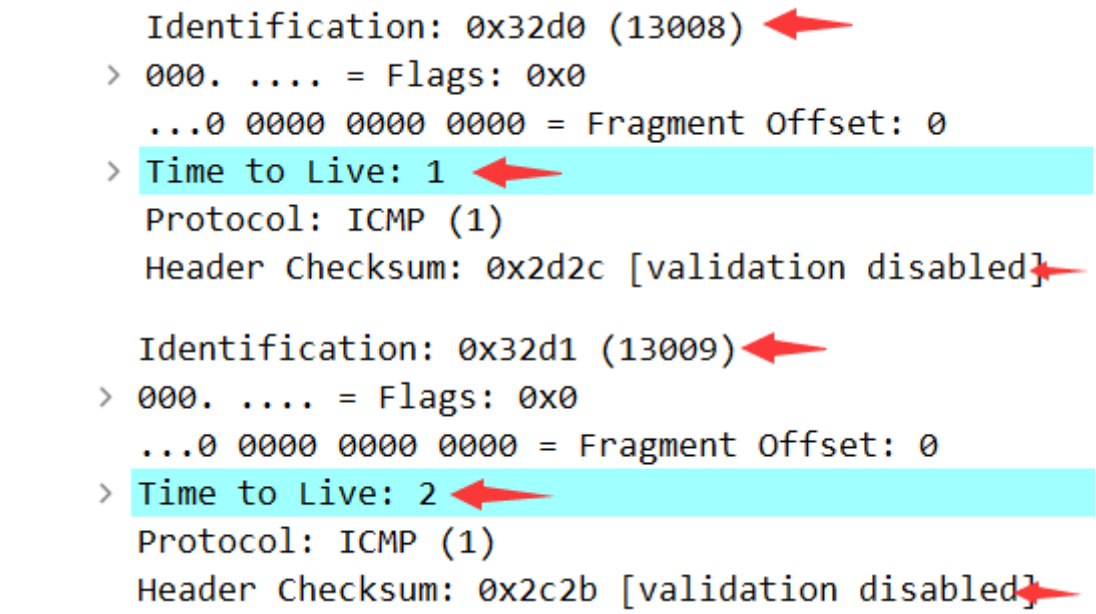
> Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented



flags字段中的More fragments没有置位，为0，所以没有分片

Q5

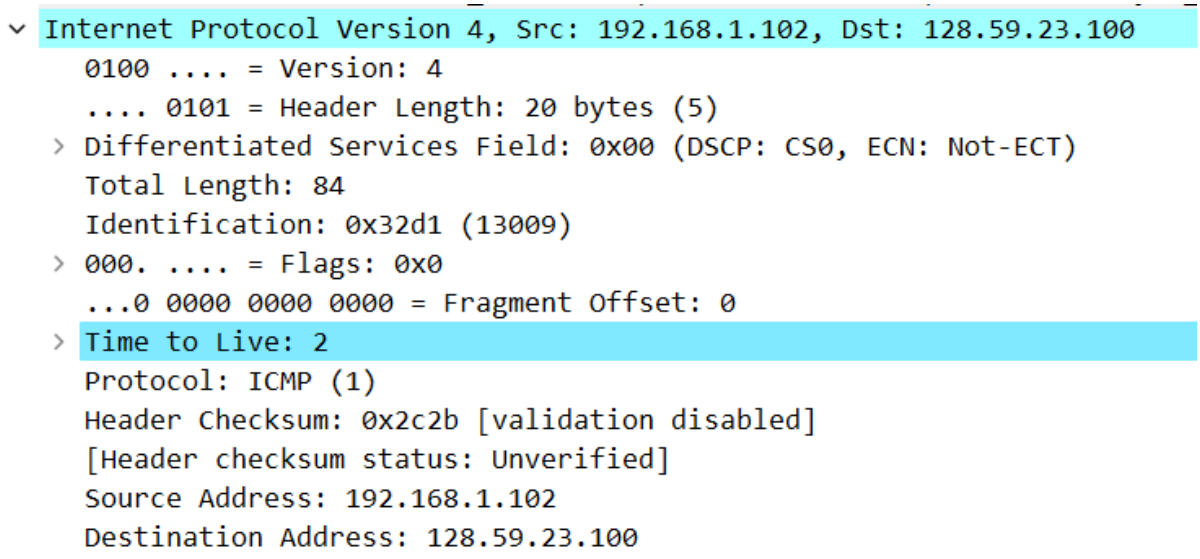
> Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?



identification（标识符）、time to live（存在时间）、header checksum（首部检验和）在改变

Q6

> Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?



- 图中所示，除了Q5中所改变，其余Version,Header Length,Differentiated Services Field,Total Length,Flags Fragment Offset,Protocol,Source Address,Destination Address保持不变

- 其中必须保持不变的有：Version, Header Length, Differentiated Services Field, Protocol,Source,Address, Destination Address
- 必须改变的是Q5中提到的Identification、Time to Live、Header Checksum，因为Identification用来唯一标识数据报，Time to Live是因为traceroute程序会发送该字段递增的报文，在跳数计数器的作用下来避免报文永远存在，Header Checksum是因为该字段是首部检验和，只要有首部字段发生改变，该字段就会变化

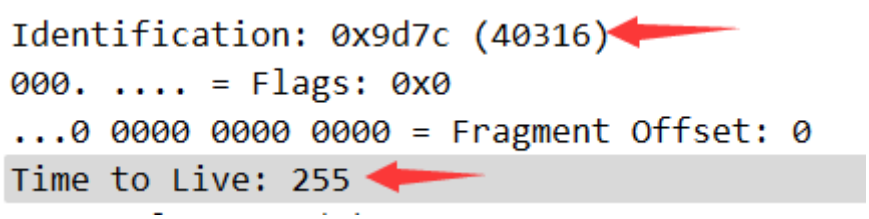
Q7

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

还是Q5中的图可以看出是递增1的

Q8

> What is the value in the Identification field and the TTL field?

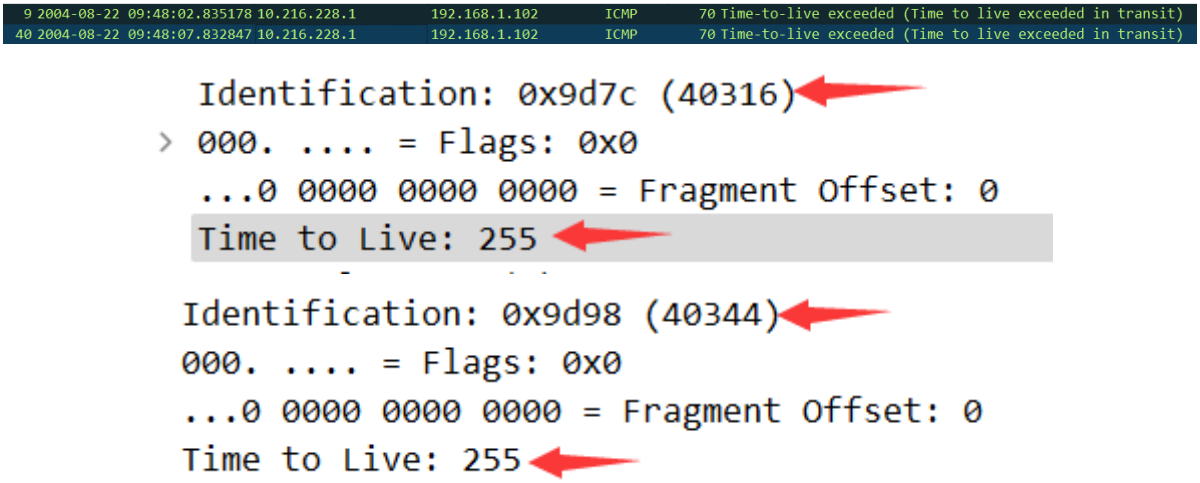


Identification为0x9d7c（40316）

TTL为255

Q9

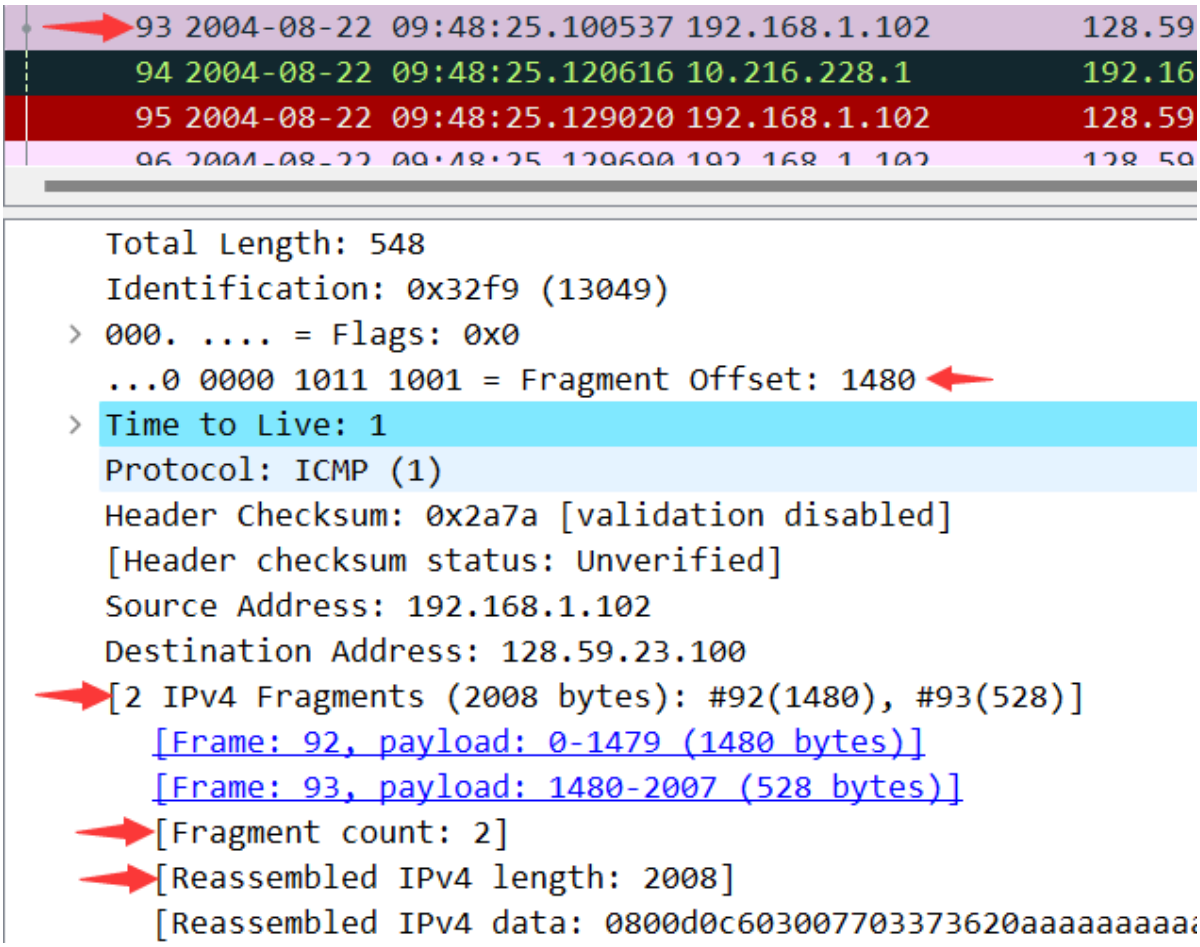
> Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why



ID改变了，TTL没有变，因为ID是对数据报的唯一标识，而TTL不变是因为它们都是第一跳路由器发出的，具有相同的寿命

Q10

> 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?



分为了2片

Q11

> 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

打印结果如下：

```
No.     Time           Source                Destination           Protocol Length Info
     92 28.441511      192.168.1.102         128.59.23.100         IPv4     1514   Fragmented IP protocol
(proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32f9 (13049)
    Flags: 0x20, 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: 1
    Protocol: ICMP (1)
    Header Checksum: 0x077b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 93]
```

More fragments为set说明数据报被分片

Fragment Offset为0说明没有偏移，为第一个分片

数据报长度为1500字节

Q12

> 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?

打印结果如下：

```
No.     Time           Source                Destination           Protocol Length Info
     93 28.442185      192.168.1.102         128.59.23.100         ICMP     562    Echo (ping) request
id=0x0300, seq=30467/887, ttl=1 (no response found!)
Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x32f9 (13049)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2a7a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
Internet Control Message Protocol
```

Fragment Offset为1480说明有偏移，则不是第一个分片

More fragments为Not set说明没有更多分片

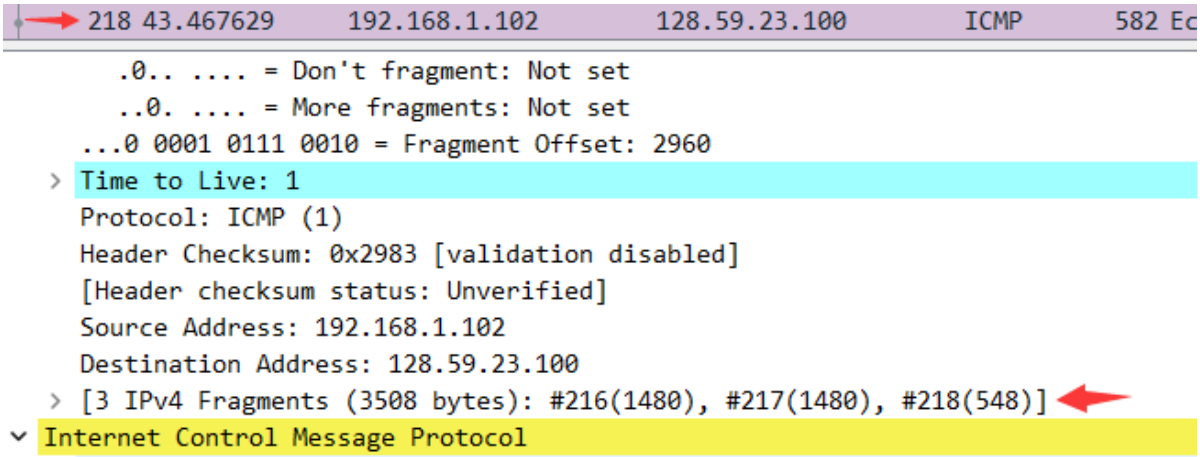
Q13

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

比较上面两题的图即可知道，Total Length,More fragments,Fragment Offset,Header Checksum有变化

Q14

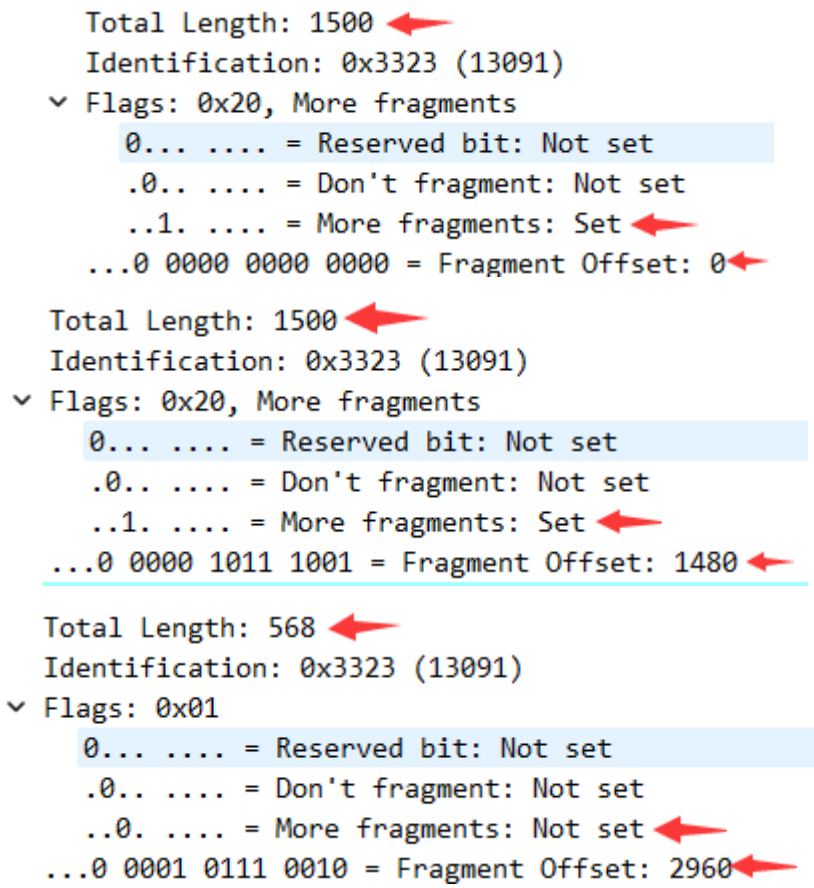
> How many fragments were created from the original datagram?



3个分片

Q15

> What fields change in the IP header among the fragments?



Total Length,More fragments,Fragment Offset变化，所以Header Checksum也会变化