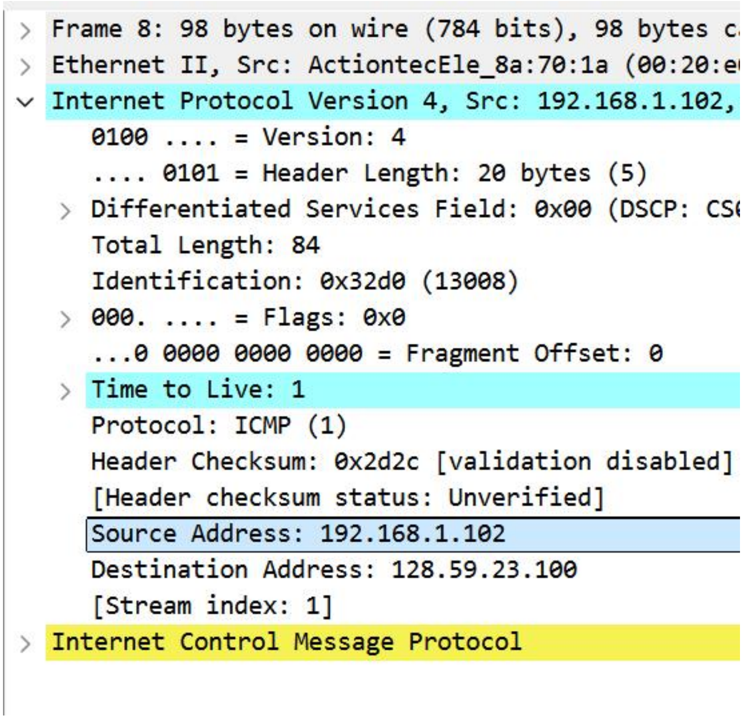
山东大学 计算机科学与技术 学院

新兴网络技术与实践 课程实验报告

学号：202300130183	姓名：宋浩宇	班级：23 级智能班
实验题目：Wireshark Lab: IP v8.0		
实验学时：2	实验日期：2025/4/30	
实验目的：学习 IP		

实验结果：

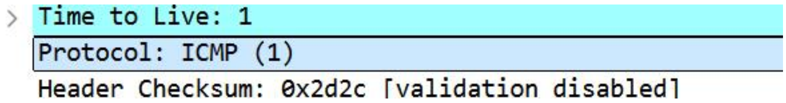
1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window,What is the IP address of your computer?



```
> Frame 8: 98 bytes on wire (784 bits), 98 bytes c
> Ethernet II, Src: ActiontecEle_8a:70:1a (00:20:e
v Internet Protocol Version 4, Src: 192.168.1.102,
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS
     Total Length: 84
     Identification: 0x32d0 (13008)
   > 000. .... = Flags: 0x0
     ...0 0000 0000 0000 = Fragment Offset: 0
   > Time to Live: 1
     Protocol: ICMP (1)
     Header Checksum: 0x2d2c [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 192.168.1.102
     Destination Address: 128.59.23.100
     [Stream index: 1]
> Internet Control Message Protocol
```

如图，地址是 192.168.1.102

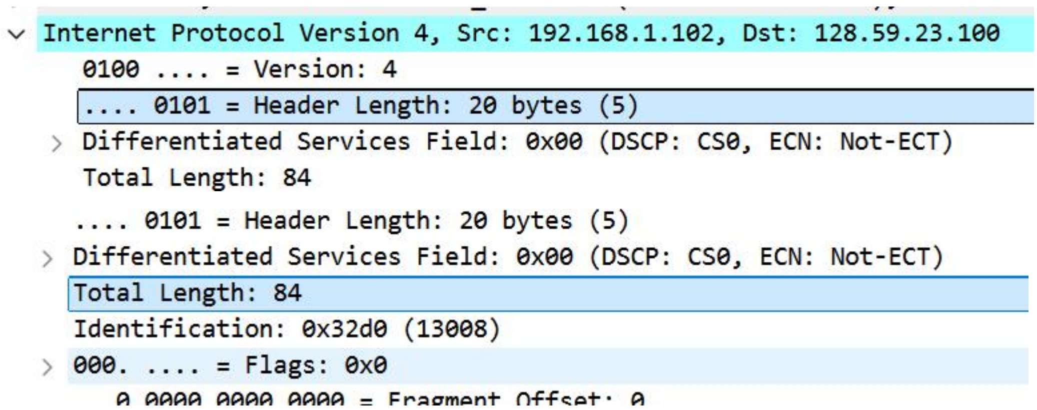
2. Within the IP packet header, what is the value in the upper layer protocol field?



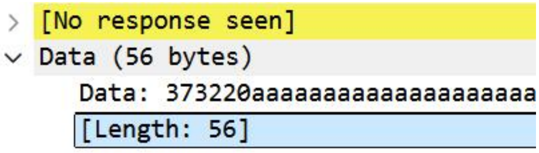
```
> Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0x2d2c [validation disabled]
```

如图，上层协议是 ICMP

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.



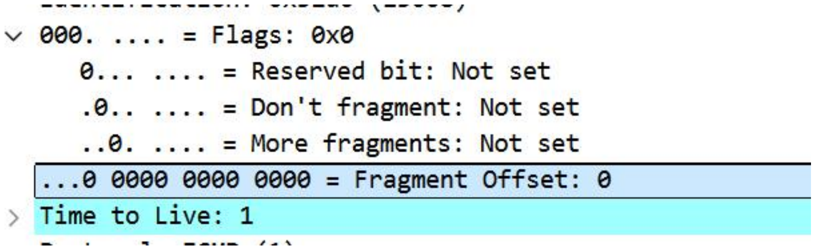
```
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 84
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > 000. .... = Flags: 0x0
        0 0000 0000 0000 = Fragment Offset: 0
```



```
> [No response seen]
v Data (56 bytes)
     Data: 373220aaaaaaaaaaaaaaaaaa
     [Length: 56]
```

IP header 里有 20byte，datagram 段有 56byte，但实际的负载应该是 84-20=64 是根据上图确认的。

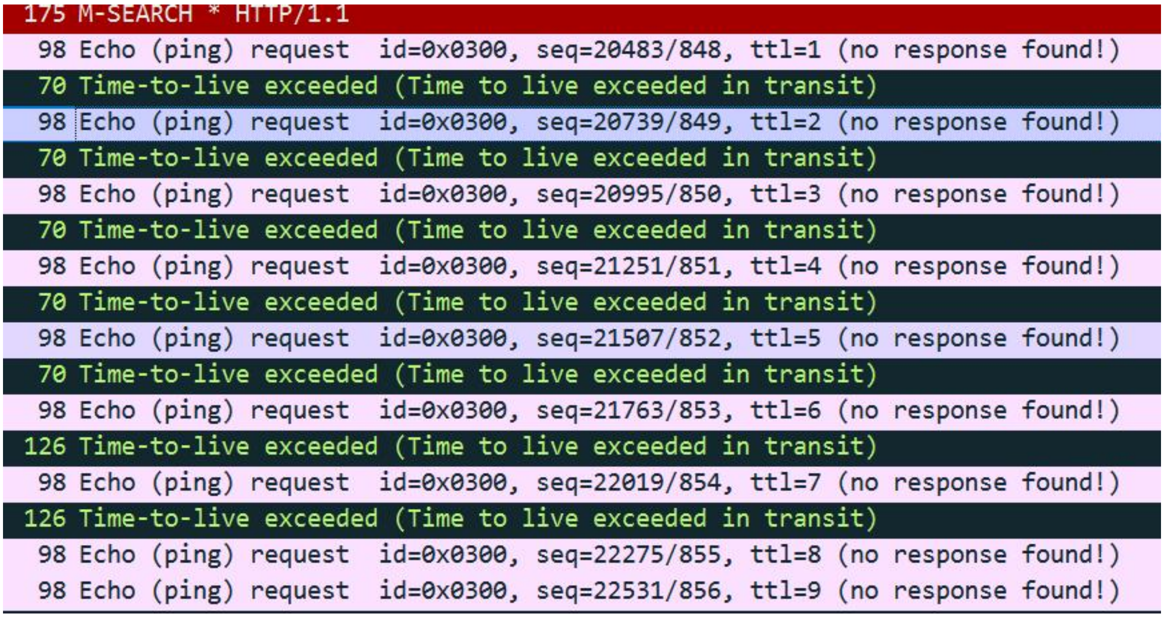
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.



```
v 000. .... = Flags: 0x0
     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: 1
```

这里 more fragments 和 fragment offset 都是 0，没有被分片

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?



```
 175 M-SEARCH * HTTP/1.1
  98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
  70 Time-to-live exceeded (Time to live exceeded in transit)
  98 Echo (ping) request  id=0x0300, seq=20739/849, ttl=2 (no response found!)
  70 Time-to-live exceeded (Time to live exceeded in transit)
  98 Echo (ping) request  id=0x0300, seq=20995/850, ttl=3 (no response found!)
  70 Time-to-live exceeded (Time to live exceeded in transit)
  98 Echo (ping) request  id=0x0300, seq=21251/851, ttl=4 (no response found!)
  70 Time-to-live exceeded (Time to live exceeded in transit)
  98 Echo (ping) request  id=0x0300, seq=21507/852, ttl=5 (no response found!)
  70 Time-to-live exceeded (Time to live exceeded in transit)
  98 Echo (ping) request  id=0x0300, seq=21763/853, ttl=6 (no response found!)
 126 Time-to-live exceeded (Time to live exceeded in transit)
  98 Echo (ping) request  id=0x0300, seq=22019/854, ttl=7 (no response found!)
 126 Time-to-live exceeded (Time to live exceeded in transit)
  98 Echo (ping) request  id=0x0300, seq=22275/855, ttl=8 (no response found!)
  98 Echo (ping) request  id=0x0300, seq=22531/856, ttl=9 (no response found!)
```

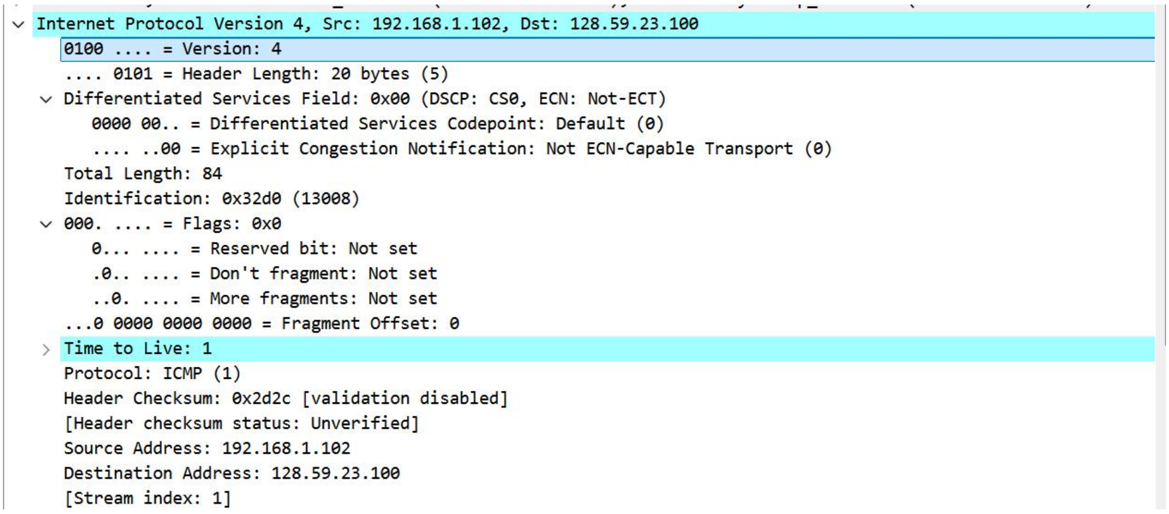
Time to live,seq,header checksum 这几个字段会变

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

在 IP 数据报中，版本、首部长度（若无选项字段）、标识（对于分片数据报）、源和目的 IP 地

址通常保持不变；分片时总长度、片偏移、标志字段（More Fragments）必须变化，traceroute 中 TTL 也必须变化，以确保数据报正确传输、转发、重新组装和路由探测，而服务类型（TOS）、协议字段和首部校验和可能变化，其中首部校验和变化是为了适应网络中的动态调整，如 TTL 减少或分片处理。

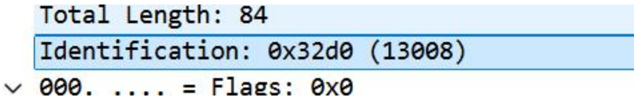
7. Describe the pattern you see in the values in the Identification field of the IP datagram



```
∨ 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)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x32d0 (13008)
  ∨ 000. .... = Flags: 0x0
      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: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Stream index: 1]
```

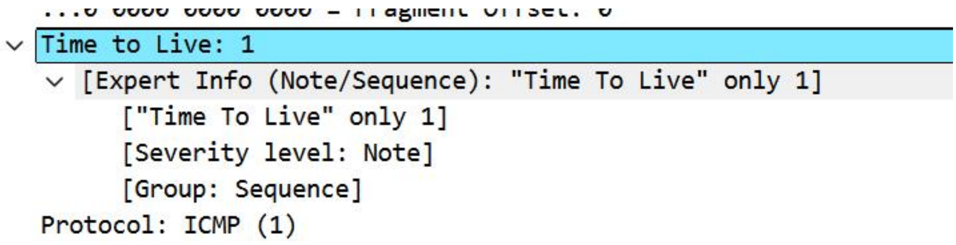
模式是一个 16 位字段

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



```
    Total Length: 84
    Identification: 0x32d0 (13008)
  ∨ 000. .... = Flags: 0x0
```

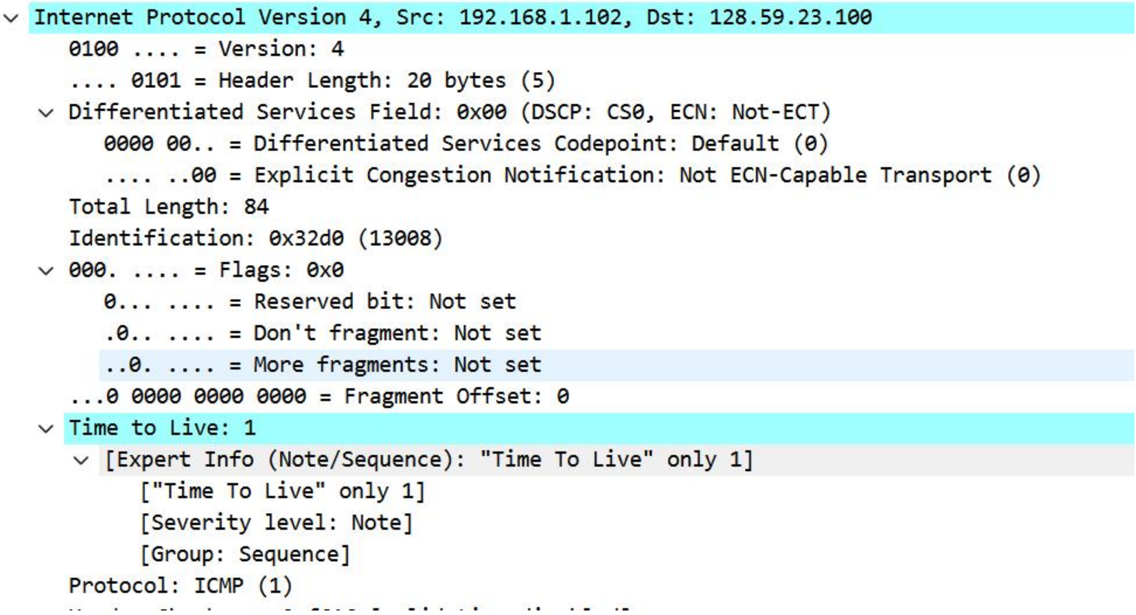
如图，Identification 是 0x32d0(13008)



```
  ...0 0000 0000 0000 = Fragment Offset: 0
∨ Time to Live: 1
  ∨ [Expert Info (Note/Sequence): "Time To Live" only 1]
      ["Time To Live" only 1]
      [Severity level: Note]
      [Group: Sequence]
  Protocol: ICMP (1)
```

如图，TTL 是 1

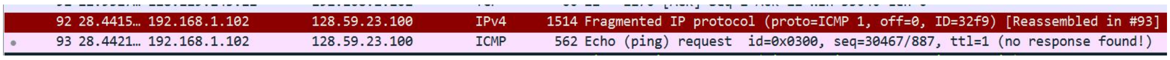
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?



```
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v 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: 84
    Identification: 0x32d0 (13008)
  v 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  v Time to Live: 1
    v [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
    Protocol: ICMP (1)
```

这些值在超时回复中都保持不变了。因为这些值需要标明唯一 IP 数据报和其生命周期。

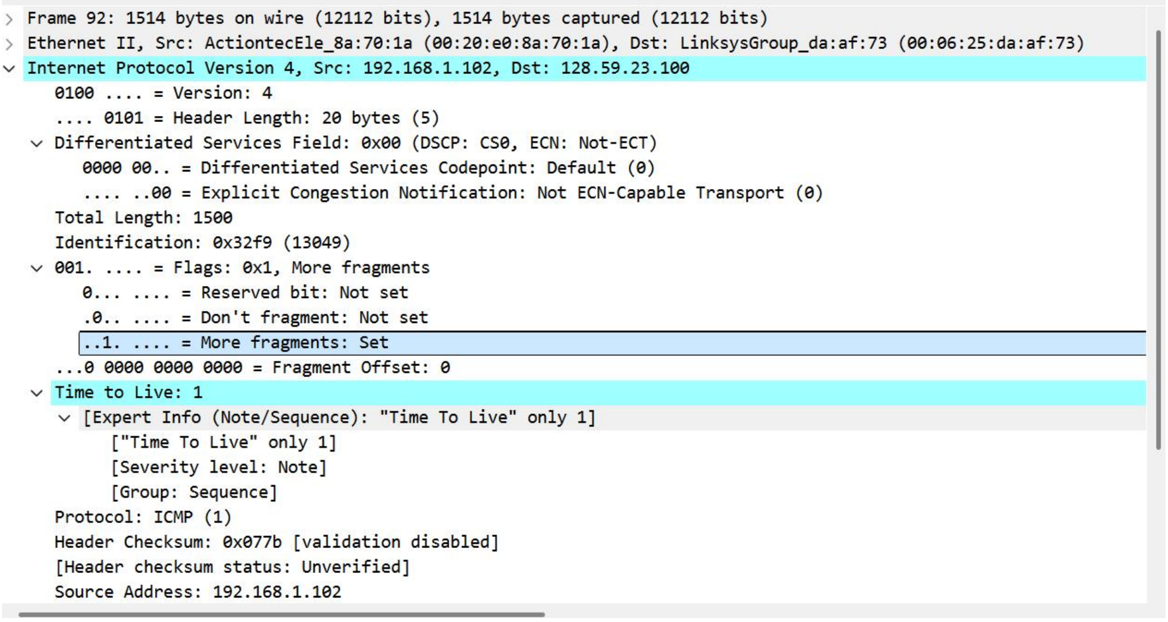
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?



```
92 28.4415… 192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93 28.4421… 192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30467/887, ttl=1 (no response found!)
```

被分片了。

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?



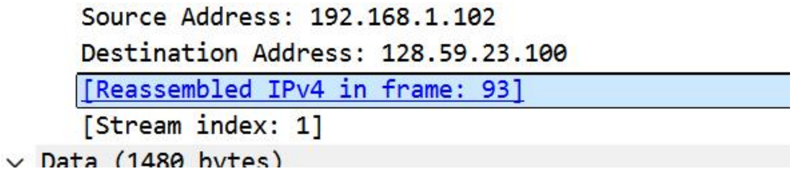
```
> Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: ActiontecEle_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v 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: 0x32f9 (13049)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
  v Time to Live: 1
    v [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
    Protocol: ICMP (1)
    Header Checksum: 0x077b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
```

More Fragments 不为 0，被分片了。

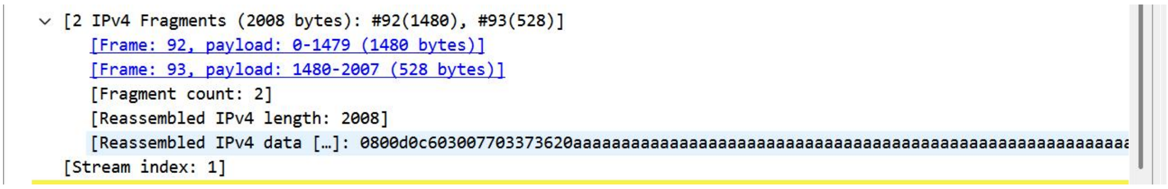
该数据报的长度是 1500byte

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?

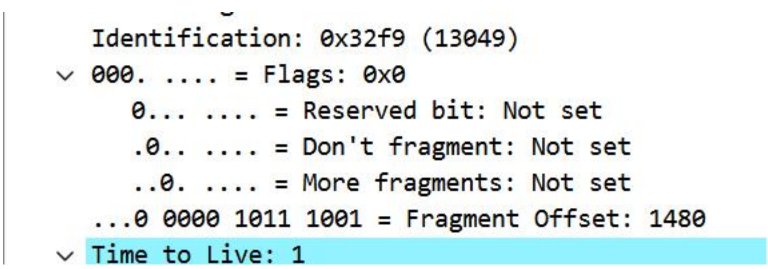


```
        Source Address: 192.168.1.102
        Destination Address: 128.59.23.100
        [Reassembled IPv4 in frame: 93]
        [Stream index: 1]
  Data (1480 bytes)
```



```
    [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
       [Frame: 92, payload: 0-1479 (1480 bytes)]
       [Frame: 93, payload: 1480-2007 (528 bytes)]
       [Fragment count: 2]
       [Reassembled IPv4 length: 2008]
       [Reassembled IPv4 data […]: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
    [Stream index: 1]
```

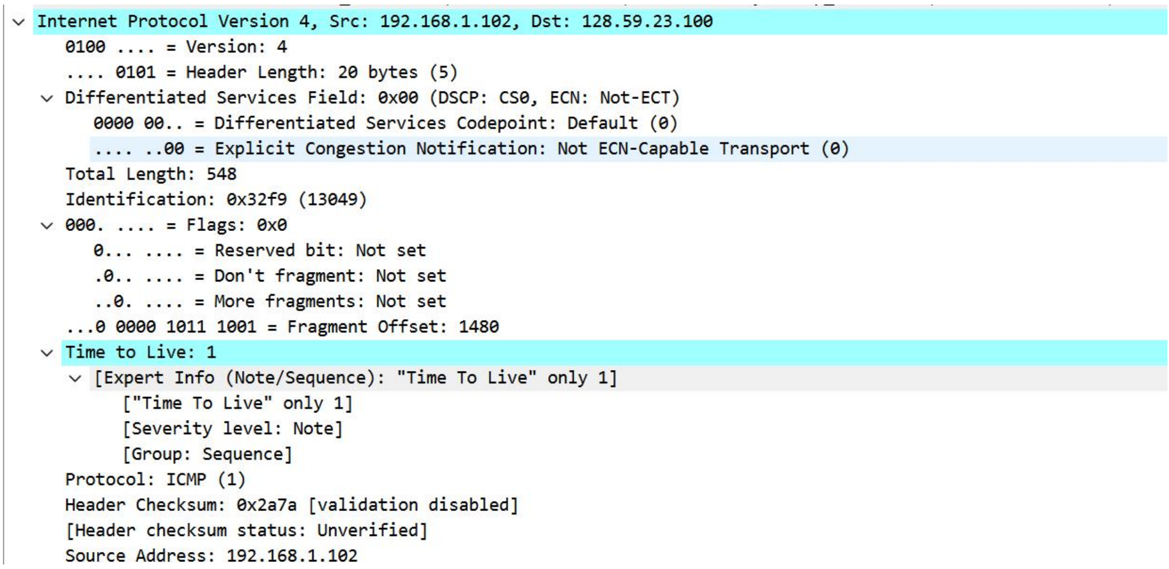
这个地方的 IPv4 Fragments 标明了这不是第一个数据包分片，而 fragment count 字段表示一共只有两个分片，所以没有后续的分片了。还有一个判断依据，



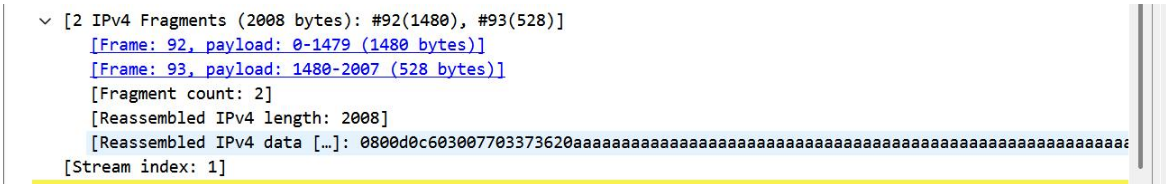
```
      Identification: 0x32f9 (13049)
    000. .... = Flags: 0x0
         0... .... = Reserved bit: Not set
         .0.. .... = Don't fragment: Not set
         ..0. .... = More fragments: Not set
      ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 1
```

这里的 more fragments 为 0.

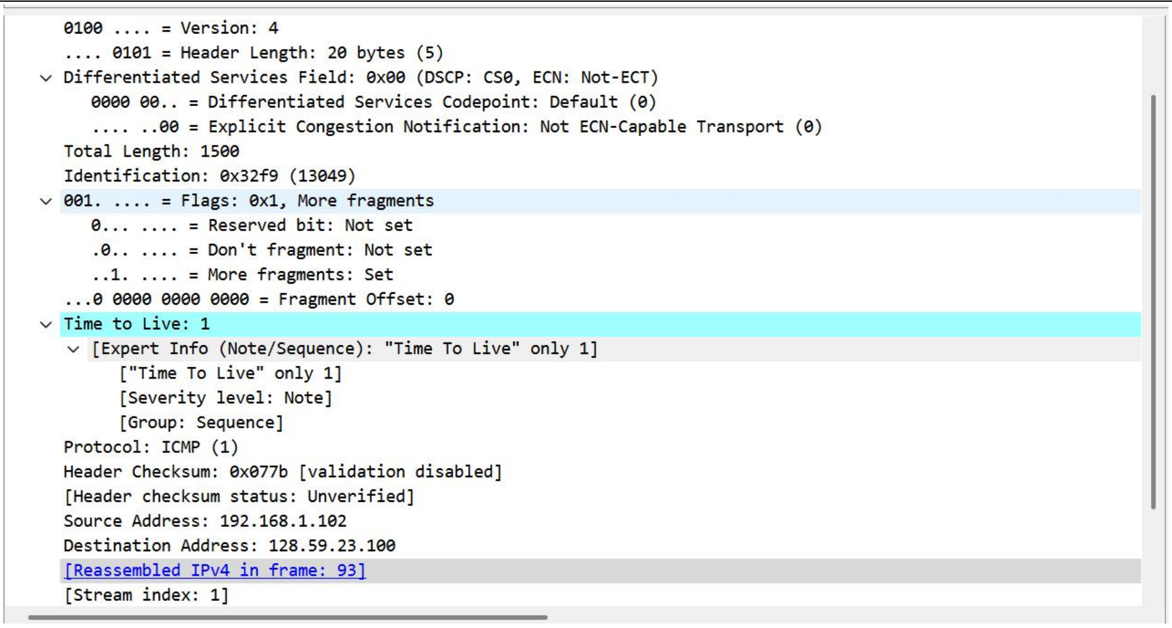
13. What fields change in the IP header between the first and second fragment?



```
  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)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
      Total Length: 548
      Identification: 0x32f9 (13049)
    000. .... = Flags: 0x0
        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
      [Expert Info (Note/Sequence): "Time To Live" only 1]
            ["Time To Live" only 1]
            [Severity level: Note]
            [Group: Sequence]
      Protocol: ICMP (1)
      Header Checksum: 0x2a7a [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.1.102
```



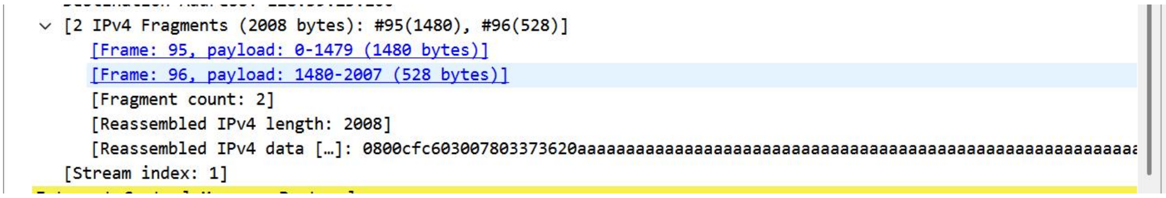
```
    [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
       [Frame: 92, payload: 0-1479 (1480 bytes)]
       [Frame: 93, payload: 1480-2007 (528 bytes)]
       [Fragment count: 2]
       [Reassembled IPv4 length: 2008]
       [Reassembled IPv4 data […]: 0800d0c603007703373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
    [Stream index: 1]
```



```
    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: 0x32f9 (13049)
  ∨ 001. .... = Flags: 0x1, 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
    ∨ [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
    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]
    [Stream index: 1]
```

如图可以看出 Identification 字段不同，headerChecksum 不同，TTL 不同，IPv4 Fragments 不同

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



```
  ∨ [2 IPv4 Fragments (2008 bytes): #95(1480), #96(528)]
      [Frame: 95, payload: 0-1479 (1480 bytes)]
      [Frame: 96, payload: 1480-2007 (528 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 2008]
      [Reassembled IPv4 data […]: 0800cfc603007803373620aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
    [Stream index: 1]
```

原始数据报被分成了 2 个分片。

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

在分片之间，IP 首部中的总长度、片偏移、标志字段（More Fragments 标志位）发生了变化，其中总长度和片偏移随分片位置和大小变化，More Fragments 标志位用于指示是否是最后一个分片。

问题及收获：

通过本次实验，我深入理解了 IP 数据报的结构和分片机制。在实验过程中，我学会了如何使用 Wireshark 捕获和分析网络数据包，并能够准确识别 IP 首部中的各个字段及其含义。通过分析 traceroute 程序生成的 ICMP 数据报,我观察到了 IP 数据报在传输过程中的变化,特别是 TTL 字段的递减和 ICMP TTL 超时消息的生成。此外，我还详细了解了 IP 数据报分片的过程，包括如何识别分片、分片标识字段的作用以及分片过程中各个字段的变化情况。这些知识不仅加深了我对 IP 协议的理解，还提高了我分析和解决网络问题的能力。