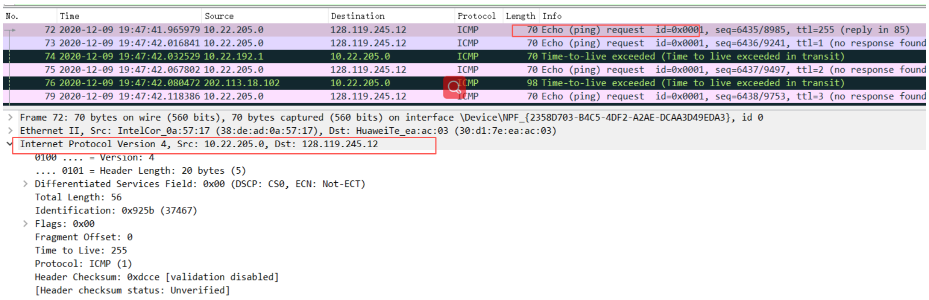
Lab6 Wireshark_IP

- 学号:1813075
- 姓名:刘茵

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?

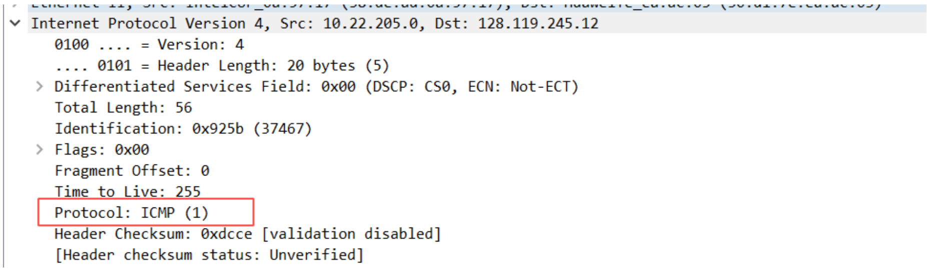


```
No.     Time                       Source          Destination      Protocol  Length Info
    72 2020-12-09 19:47:41.965979 10.22.205.0     128.119.245.12   ICMP        70 Echo (ping) request  id=0x0001, seq=6435/8985, ttl=255 (reply in 85)
    73 2020-12-09 19:47:42.016841 10.22.205.0     128.119.245.12   ICMP        70 Echo (ping) request  id=0x0001, seq=6436/9241, ttl=1 (no response found
    74 2020-12-09 19:47:42.032529 10.22.192.1     10.22.205.0      ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
    75 2020-12-09 19:47:42.067802 10.22.205.0     128.119.245.12   ICMP        70 Echo (ping) request  id=0x0001, seq=6437/9497, ttl=2 (no response found
    76 2020-12-09 19:47:42.080472 202.113.18.102  10.22.205.0      ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
    79 2020-12-09 19:47:42.118386 10.22.205.0     128.119.245.12   ICMP        70 Echo (ping) request  id=0x0001, seq=6438/9753, ttl=3 (no response found

> Frame 72: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{2358D703-B4C5-4DF2-A2AE-DCAA3D49EDA3}, id 0
> Ethernet II, Src: IntelCor_0a:57:17 (38:de:ad:0a:57:17), Dst: HuaweiTe_ea:ac:03 (30:d1:7e:ea:ac:03)
v Internet Protocol Version 4, Src: 10.22.205.0, 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: 0x925b (37467)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xdcce [validation disabled]
    [Header checksum status: Unverified]
```

答：10.22.205.0

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



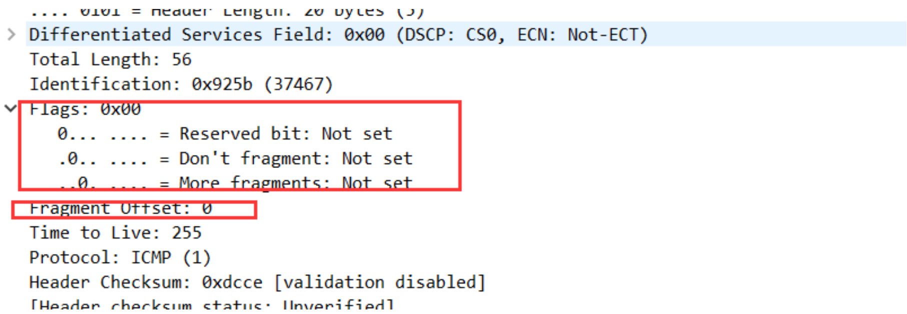
```
> Ethernet II, Src: IntelCor_0a:57:17 (38:de:ad:0a:57:17), Dst: HuaweiTe_ea:ac:03 (30:d1:7e:ea:ac:03)
v Internet Protocol Version 4, Src: 10.22.205.0, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x925b (37467)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xdcce [validation disabled]
    [Header checksum status: Unverified]
```

答：上层协议是 ICMP，值是 1

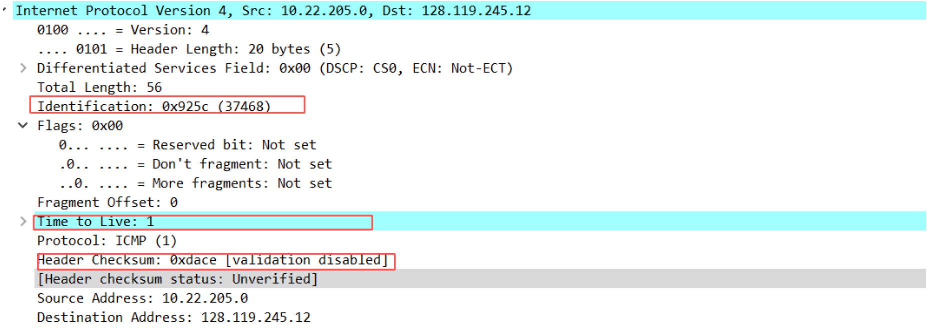
3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

答：从2题图中可以看出 IP 头文件有 20bytes，IP 报的总长度是 56 个 byte，IP 数据长度 （ICMP 协议）就是 36bytes。

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



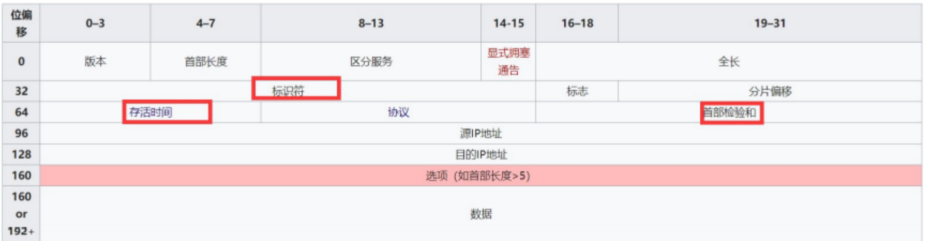
```
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x925b (37467)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xdcce [validation disabled]
    [Header checksum status: Unverified]
```



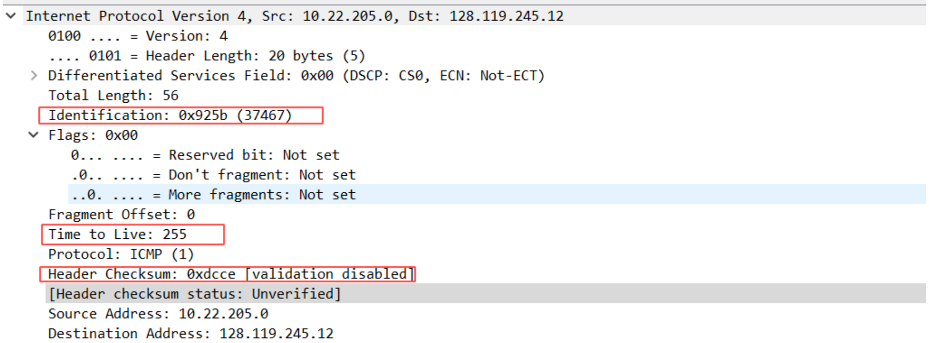
```
v Internet Protocol Version 4, Src: 10.22.205.0, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x925c (37468)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0xdace [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.22.205.0
    Destination Address: 128.119.245.12
```

答：没有被分片，因为flags=0，fragment offset=0，R、DF、MF未设置

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?



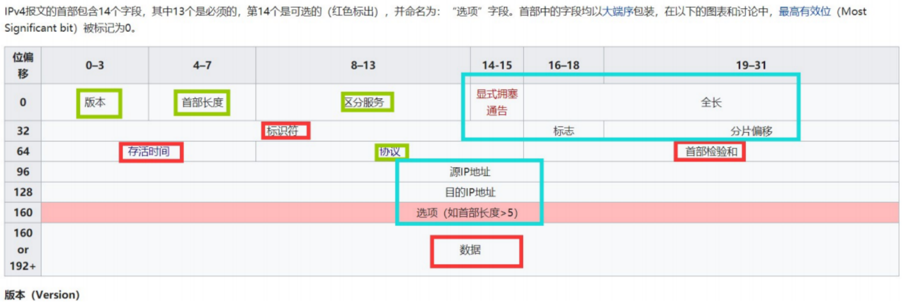
位偏移	0–3	4–7	8–13	14–15	16–18	19–31
0	版本	首部长度	区分服务	显式拥塞通告	全长	
32	标识符				标志	分片偏移
64	存活时间		协议		首部检验和	
96	源IP地址					
128	目的IP地址					
160	选项（如首部长度>5）					
160 or 192+	数据					



```
∨ Internet Protocol Version 4, Src: 10.22.205.0, 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: 0x925b (37467)
  ∨ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xdcce [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.22.205.0
    Destination Address: 128.119.245.12
```

答：首部检验和、TTL、标识都在改变。

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



IPv4报文的首部包含14个字段，其中13个是必须的，第14个是可选的（红色标出），并命名为："选项"字段。首部中的字段均以大端序包装，在以下的图表和讨论中，最高有效位（Most Significant bit）被标记为0。

位偏移	0–3	4–7	8–13	14–15	16–18	19–31
0	版本	首部长度	区分服务	显式拥塞通告	全长	
32	标识符				标志	分片偏移
64	存活时间		协议		首部检验和	
96	源IP地址					
128	目的IP地址					
160	选项（如首部长度>5）					
160 or 192+	数据					

版本（Version）

答：如图蓝色框是保持不变（下次可能改变），绿色框是一定不会改变的（仅指路 由跟踪），红色框是必须改变的。

必须更改是每次路由跟踪（含有多个不同 TTL 的 PING）的序列号，校验值，以及每个 PING 的 TTL。注意每次 PING 也有序列号，校验值，因此数据是一定改变的 （上文说过）。

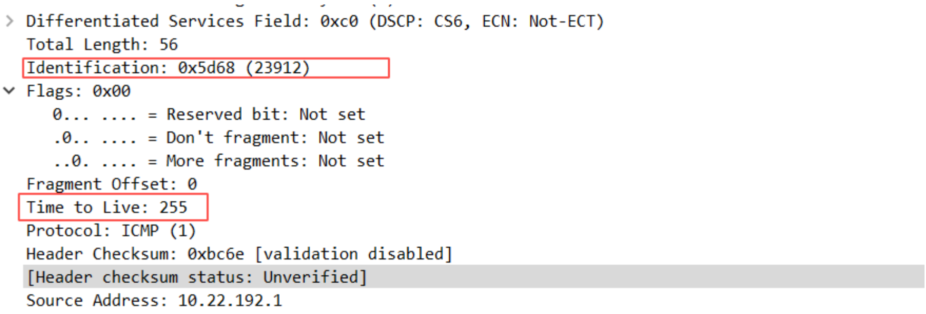
保持不变（下次可能改变）的是你这次路由跟踪，有很多的 PING 的目标数据 长度，目标和本地 IP，可选选项，显式拥塞通告(来自维基百科)，标识符，偏移量这些字段。 但你下次路由跟踪可能会改变目标 IP 和本地 IP，你也会打开一些 IP 的选项， 改变路由跟踪的数据报的大小，造成分片有偏移量这种情况。当然这种情况也可能 不会发生。

必须保持的不变的，也就是我们使用 IPV4 的下的路由跟踪，这些协议和版本都是定死的，你不管什么时候路由跟踪都是这样，所以不会变，因为区分服务已经弃 用，所以也是不会变。

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

答：标识依次增加，如题5图。

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

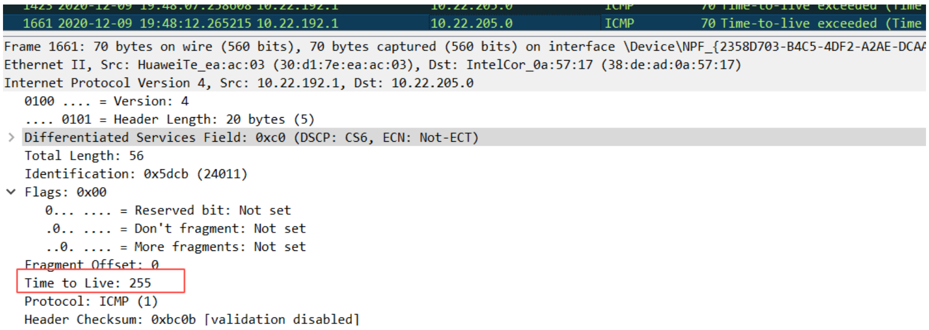


```
> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x5d68 (23912)
v Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment Offset: 0
  Time to Live: 255
  Protocol: ICMP (1)
  Header Checksum: 0xbc6e [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.22.192.1
```

答：TTL:255

Identification：23912

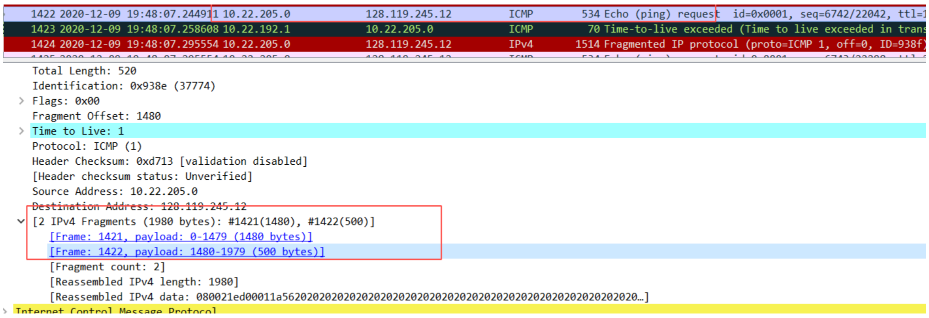
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?



```
  1423 2020-12-09 19:48:07.258608 10.22.192.1        10.22.205.0        ICMP       70 Time-to-live exceeded (Time
  1661 2020-12-09 19:48:12.265215 10.22.192.1        10.22.205.0        ICMP       70 Time-to-live exceeded (Time
Frame 1661: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{2358D703-B4C5-4DF2-A2AE-DCAA
Ethernet II, Src: HuaweiTe_ea:ac:03 (30:d1:7e:ea:ac:03), Dst: IntelCor_0a:57:17 (38:de:ad:0a:57:17)
Internet Protocol Version 4, Src: 10.22.192.1, Dst: 10.22.205.0
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x5dcb (24011)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xbc0b [validation disabled]
```

答：TTL没有改变，因为每一个的路由器都有一个固定的TTL值，ID改变了。（和题8的图对比）

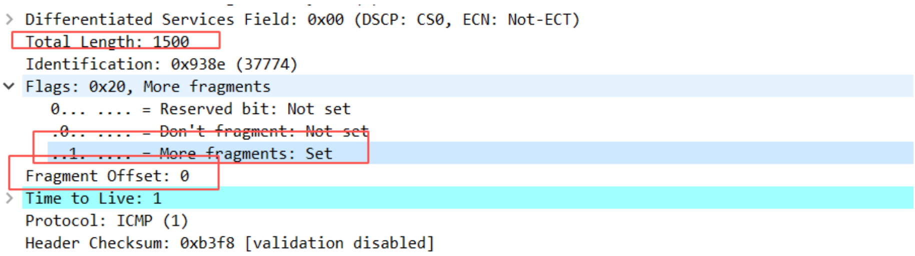
10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?



```
  1422 2020-12-09 19:48:07.244911 10.22.205.0     128.119.245.12    ICMP      534 Echo (ping) request  id=0x0001, seq=6742/22042, ttl=1
  1423 2020-12-09 19:48:07.258608 10.22.192.1     10.22.205.0       ICMP       70 Time-to-live exceeded (Time to live exceeded in trans
  1424 2020-12-09 19:48:07.295554 10.22.205.0     128.119.245.12    IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=938f)
    Total Length: 520
    Identification: 0x938e (37774)
  > Flags: 0x00
    Fragment Offset: 1480
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0xd713 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.22.205.0
    Destination Address: 128.119.245.12
  v [2 IPv4 Fragments (1980 bytes): #1421(1480), #1422(500)]
      [Frame: 1421, payload: 0-1479 (1480 bytes)]
      [Frame: 1422, payload: 1480-1979 (500 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1980]
      [Reassembled IPv4 data: 080021ed00011a5620202020202020202020202020202020202020202020202020202020…]
> Internet Control Message Protocol
```

答：分为两段

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?

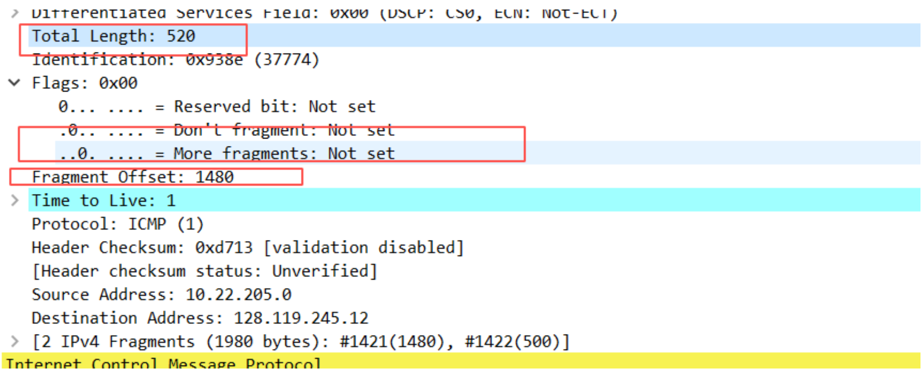


```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1500
  Identification: 0x938e (37774)
v Flags: 0x20, More fragments
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
  Fragment Offset: 0
> Time to Live: 1
  Protocol: ICMP (1)
  Header Checksum: 0xb3f8 [validation disabled]
```

答：MF为 set 标识还有分片，DF为not set可以分片。offset片偏移为0标识这是初始的ip片。

这个数据报的长度：1500bytes

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?



```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 520
  Identification: 0x938e (37774)
v 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: ICMP (1)
  Header Checksum: 0xd713 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.22.205.0
  Destination Address: 128.119.245.12
> [2 IPv4 Fragments (1980 bytes): #1421(1480), #1422(500)]
Internet Control Message Protocol
```

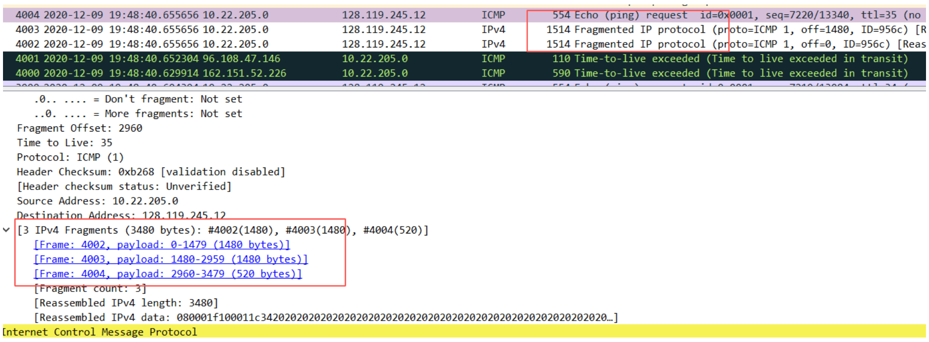
答：Offset为1480表示不为第一个分片，已经有了偏移量。

MF为0表示为最后一个分片。

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

答：Flags, Header checksum，Totol length（参考10，11题图）

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



```
4004 2020-12-09 19:48:40.655656 10.22.205.0      128.119.245.12   ICMP    554 Echo (ping) request  id=0x0001, seq=7220/13340, ttl=35 (no
4003 2020-12-09 19:48:40.655656 10.22.205.0      128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=956c) [R
4002 2020-12-09 19:48:40.655656 10.22.205.0      128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=956c) [Reas
4001 2020-12-09 19:48:40.652304 96.108.47.146    10.22.205.0      ICMP    110 Time-to-live exceeded (Time to live exceeded in transit)
4000 2020-12-09 19:48:40.629914 162.151.52.226   10.22.205.0      ICMP    590 Time-to-live exceeded (Time to live exceeded in transit)
```

```
     .0.. .... = Don't fragment: Not set
     ..0. .... = More fragments: Not set
  Fragment Offset: 2960
  Time to Live: 35
  Protocol: ICMP (1)
  Header Checksum: 0xb268 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.22.205.0
  Destination Address: 128.119.245.12
v [3 IPv4 Fragments (3480 bytes): #4002(1480), #4003(1480), #4004(520)]
     [Frame: 4002, payload: 0-1479 (1480 bytes)]
     [Frame: 4003, payload: 1480-2959 (1480 bytes)]
     [Frame: 4004, payload: 2960-3479 (520 bytes)]
     [Fragment count: 3]
     [Reassembled IPv4 length: 3480]
     [Reassembled IPv4 data: 080001f100011c3420202020202020202020202020202020202020202020202020202020…]
Internet Control Message Protocol
```

答：3个

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

答：Flags, Header checksum，Totol length