计算机网络IP实验报告

PB19071535徐昊天

一.实验目的

- 研究IP协议，重点关注IP数据报。
- 了解IP数据报的字段与分片等原理。
- 学习ICMP协议与TTL的作用。

二.实验环境与工具

- windows操作系统。
- wireshark数据包嗅探器。
- traceroute程序pingplotter。

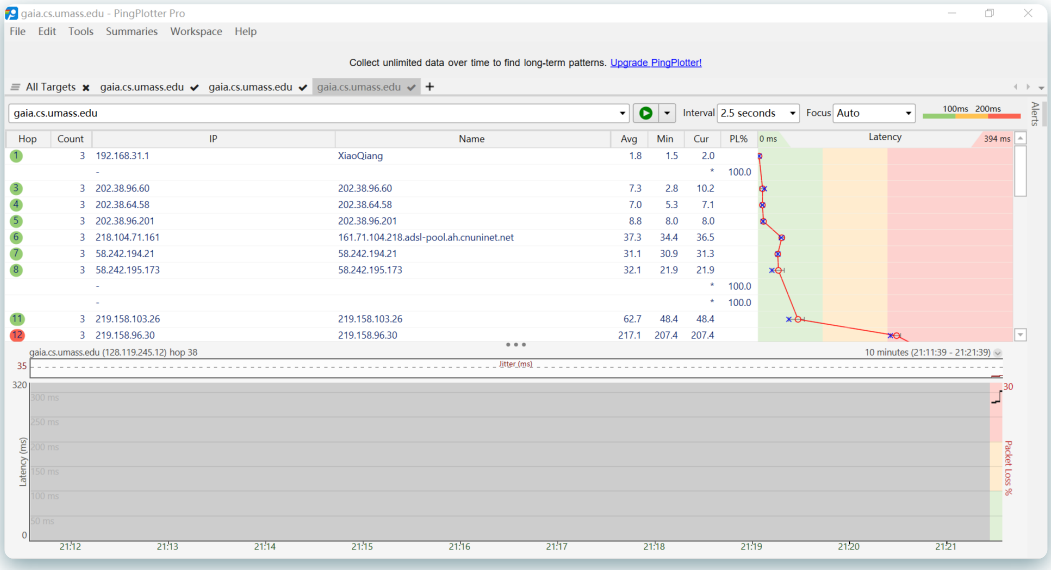
三.实验步骤

1. 在**http://www.pingplotter.com**下载并安装pingplotter。

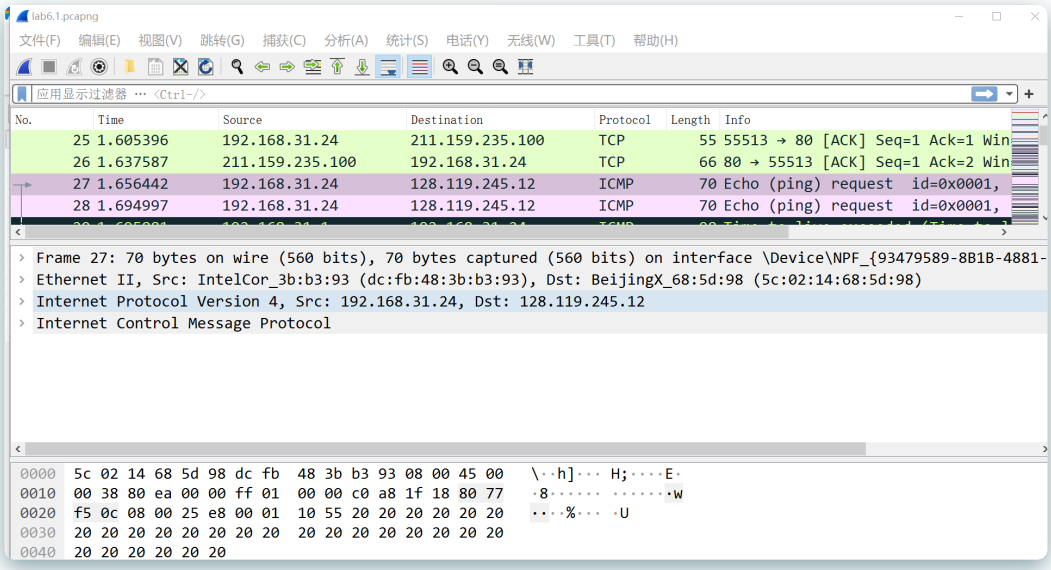
2. 启动wireshark开始数据包捕获。

3. 在pingplotter中调整 `packet size` 为**56**，在 `Address to Trace` 中输入链接 **gaia.cs.umass.edu**，开始跟踪，待count=3时停止跟踪，停止wireshark抓包。

   此时 `pingplotter` 界面如下图所示：



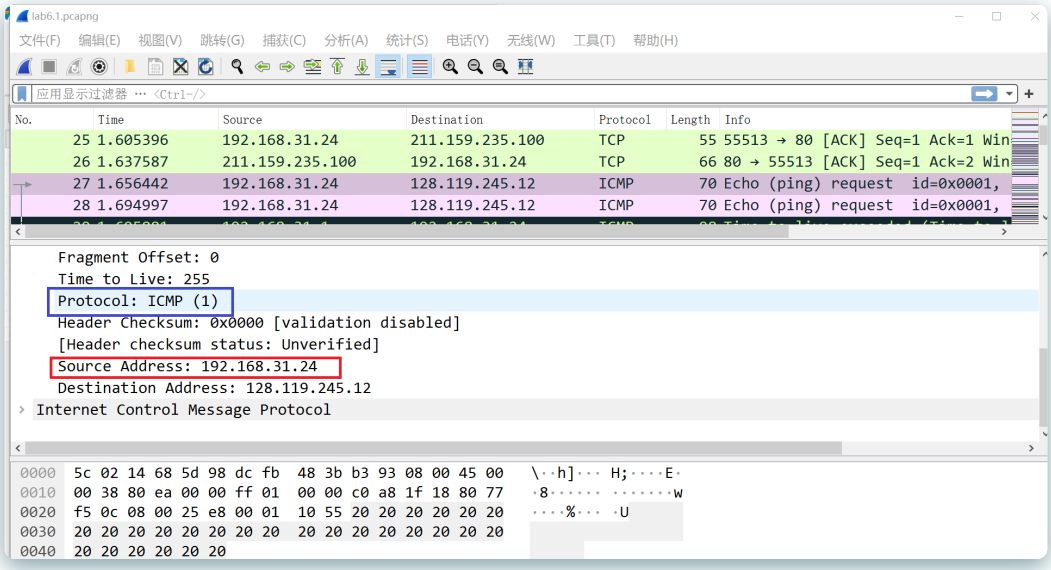
wireshark界面如下图所示：



回答下列问题：

> 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.

答：第一个ICMP Echo Request消息如下图所示：



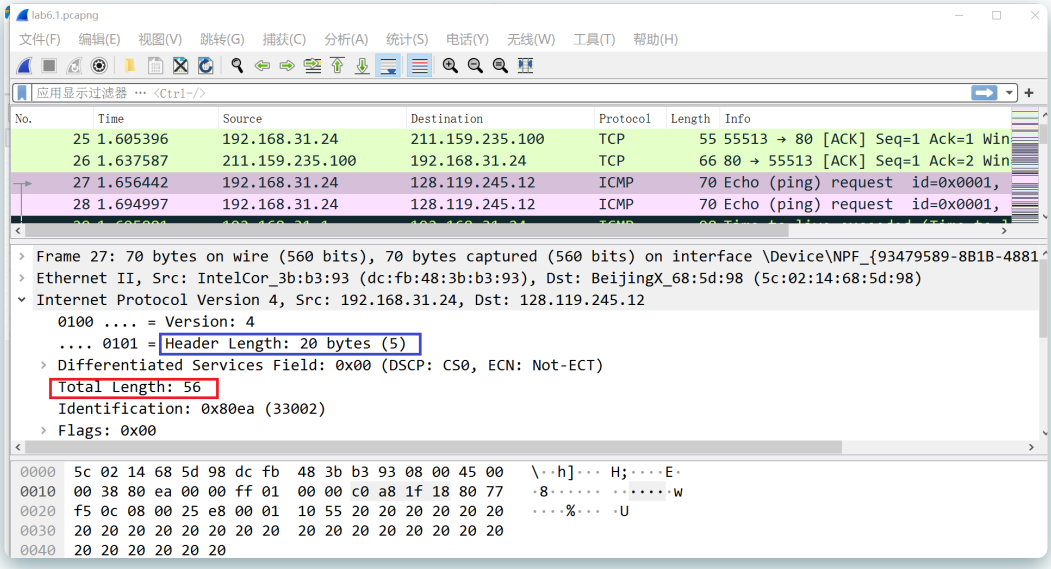
根据红色框中内容，本机IP地址为**192.168.31.24**。

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

答：根据上图中蓝色框中内容，上层协议为ICMP，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.

答：ICMP协议信息如下图所示：

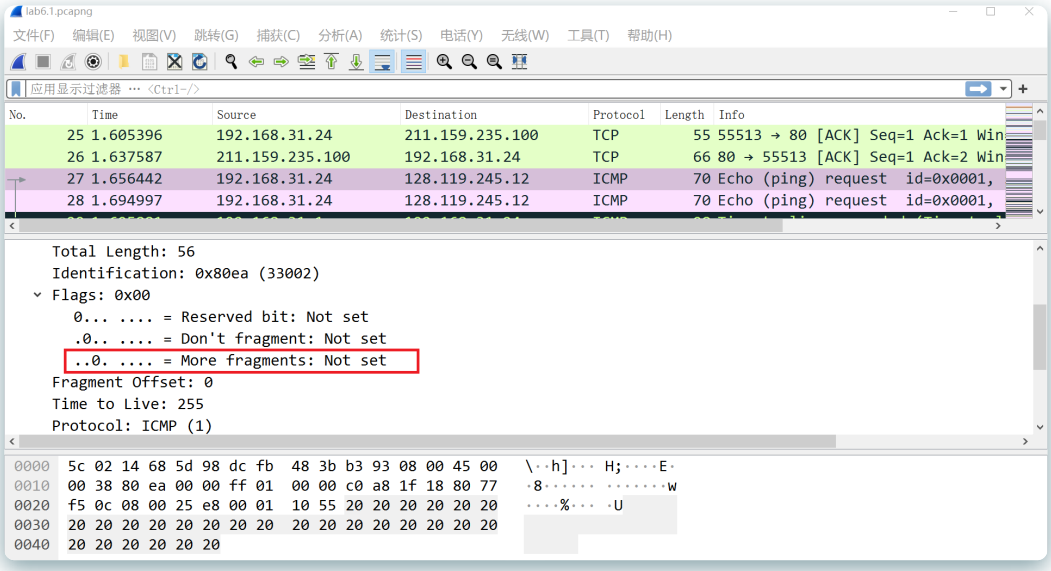


根据上图中蓝色框中内容，IP header长度为20bytes；根据上图红色框中内容，IP数据报总长度为56bytes，故IP datagram的有效负载为56-20=36bytes。

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

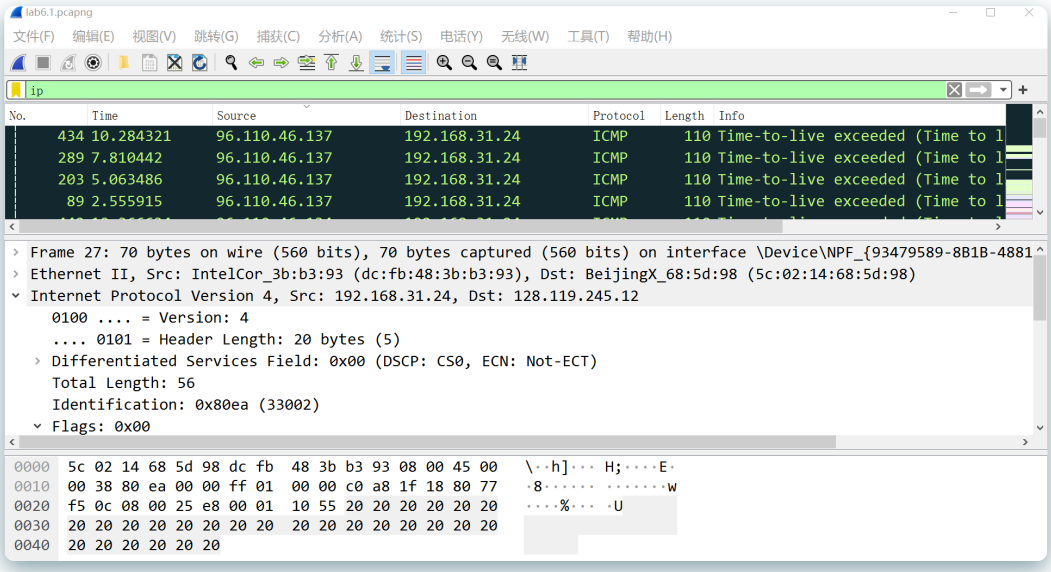
答：未被分段。

IP数据报部分信息如下图所示：



根据上图中红色框中内容，More fragments:not set 可知IP数据报未被分段。

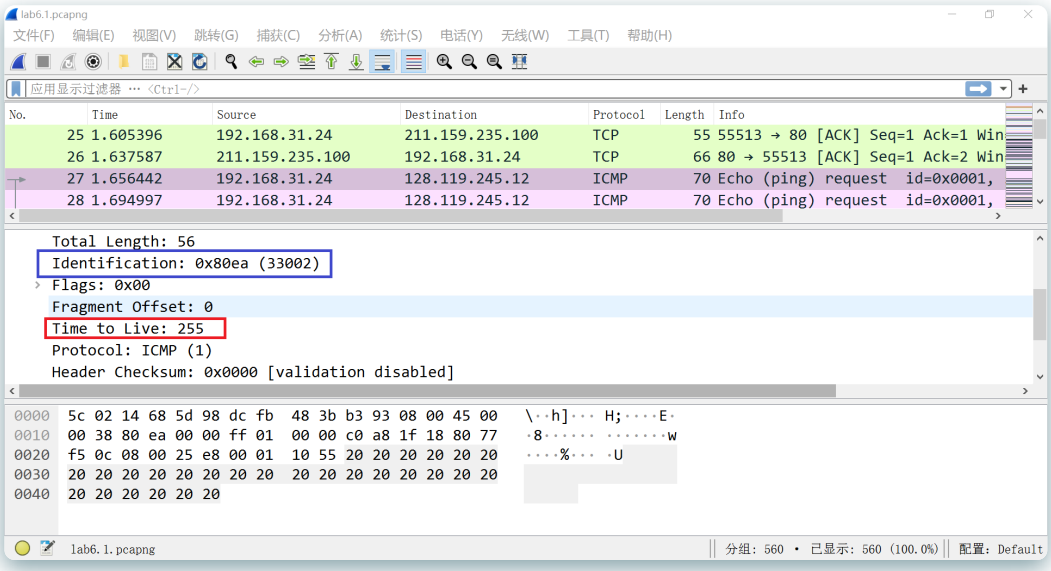
4. 单击Source列标题，根据IP源地址对跟踪的数据包进行排序，使箭头向下，得到wireshark界面如下图所示：

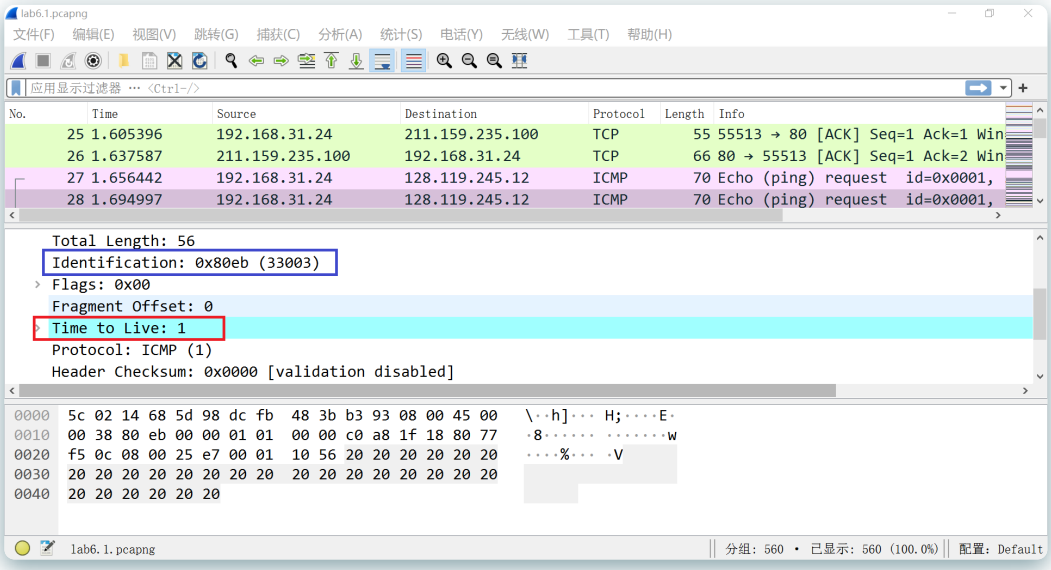


回答下列问题：

> 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?

答：一系列ICMP数据包信息如下图所示：





根据以上两图中蓝色与红色框中内容可知：IP数据报中的标识符和TTL会一直变化。

注：Header Checknum始终为0x0000 ??

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

答：

①版本、首部长度、区分服务、协议必定保持不变。

原因：固定的字段，无论什么情况都不会改变。

②标志、分片偏移、源IP地址、目的IP地址、选项、全长、显式拥塞通道保持不变。

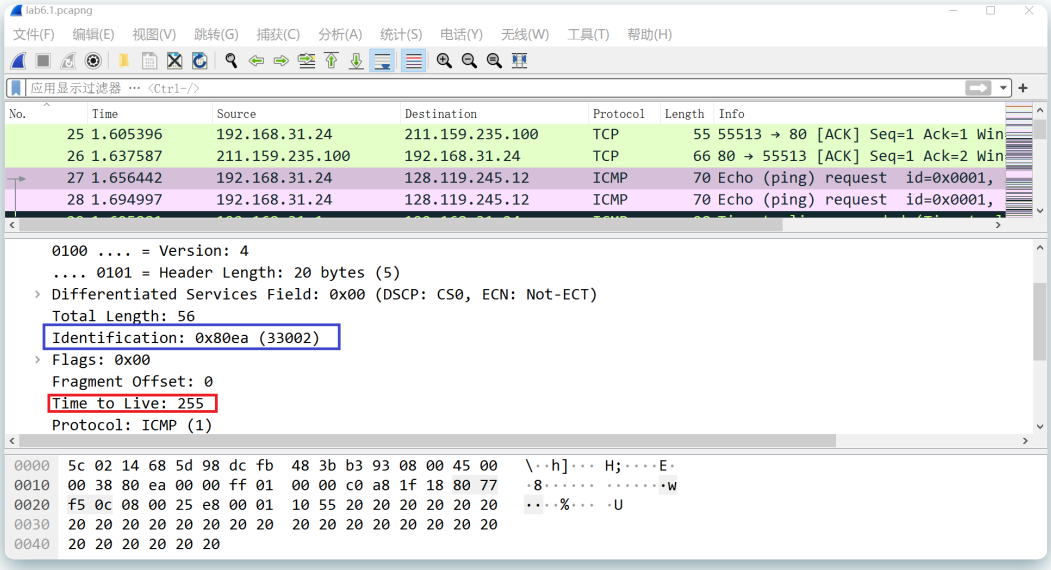
原因：每一次跟踪可能会改变目标IP和本地IP，故上述字段存在改变的可能。

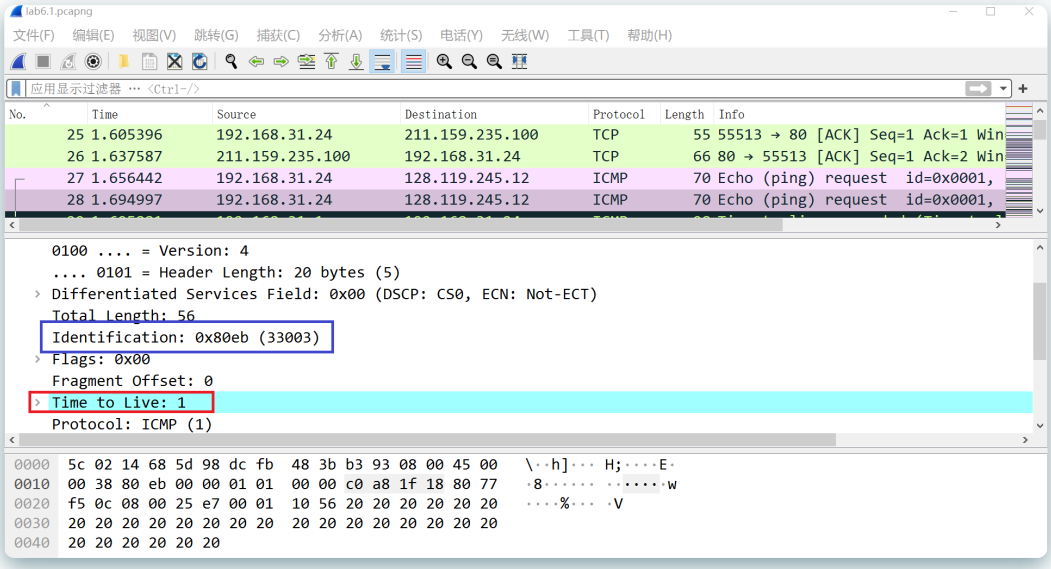
③标识符、TTL、数据必须更改。

原因：这些字段在每一次跟踪都会发生变化。

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

答：部分IP数据报的标识符信息如下图所示：

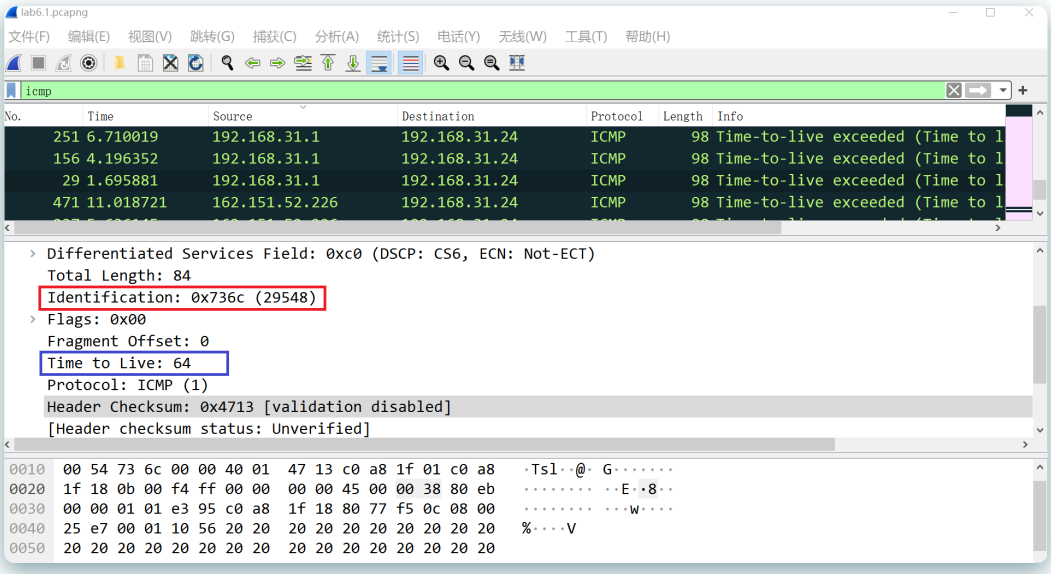




根据蓝色框中内容，可知IP数据报中标识符逐渐递增，每一个IP数据报的标识符都不相同，标识符用于区分IP数据报并处理IP分片。

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

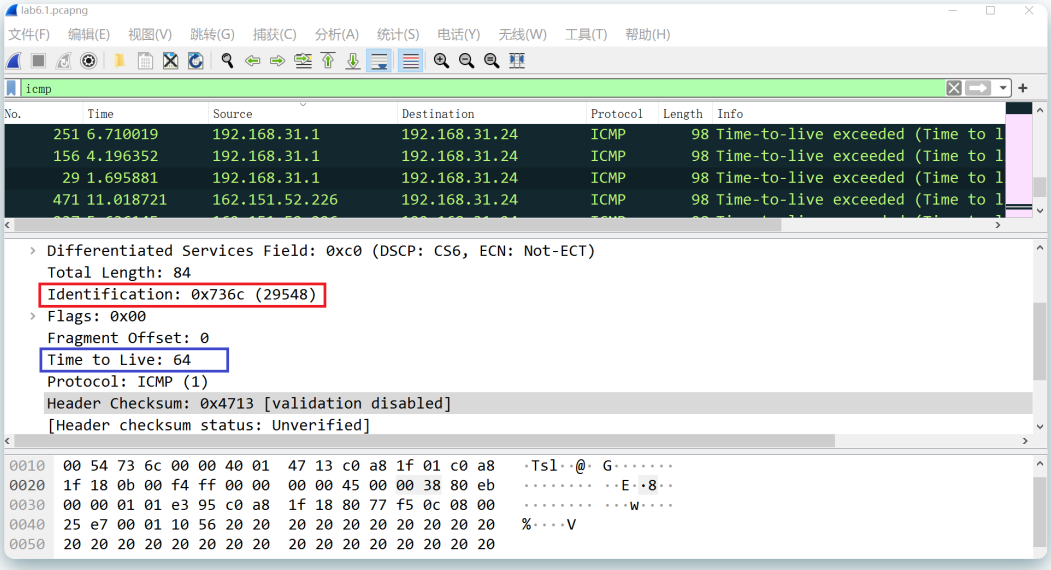
答：第一个ICMP TTL超出的IP数据报信息如下图所示：

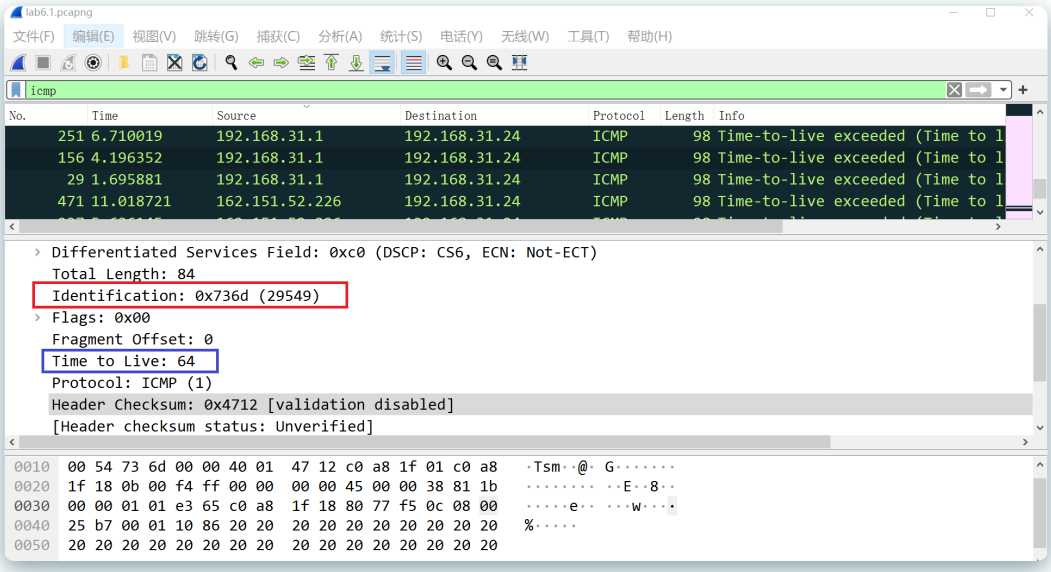


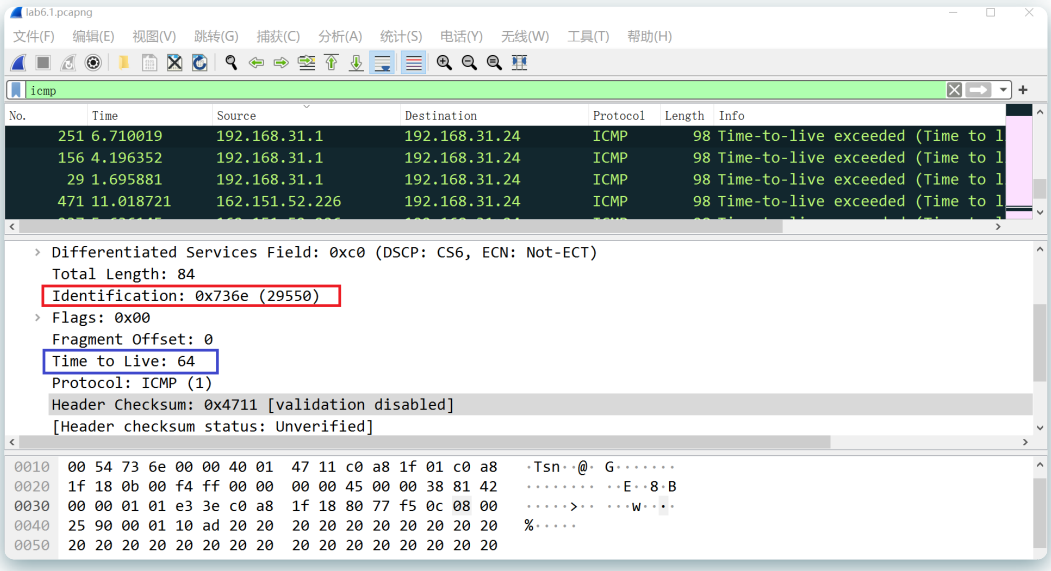
根据上图红色框中内容可知，标识符为**0x736c(29548)**;TTL为**64**。

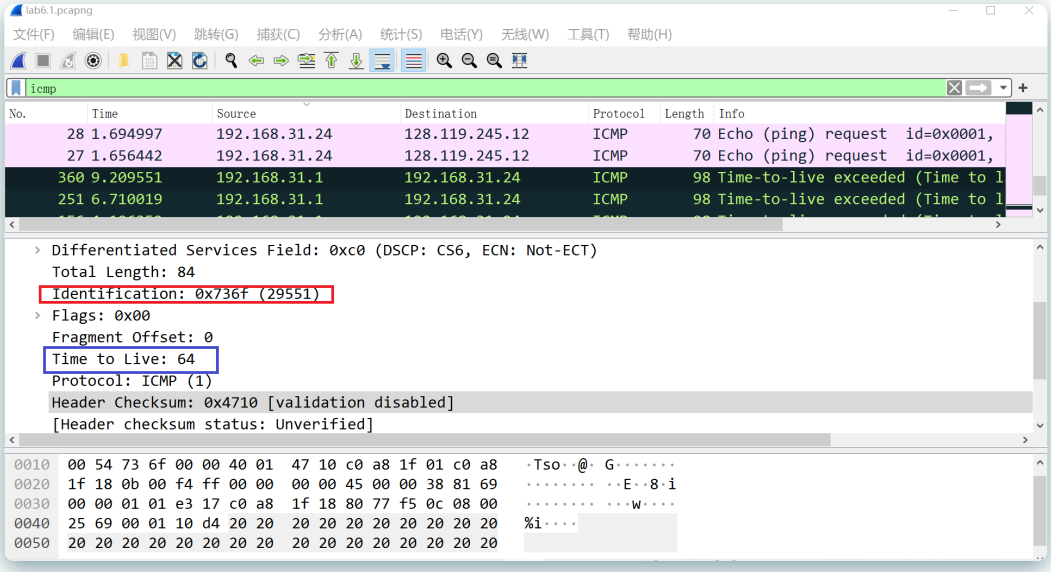
> 9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

答：ICMP TTL超出的所有IP数据报信息如下图所示：







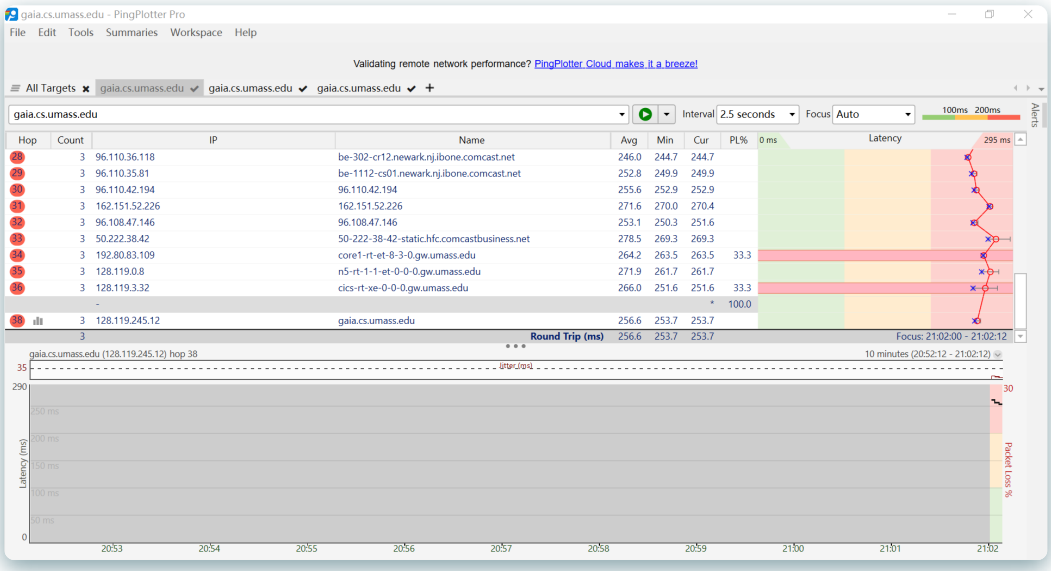


根据以上图中红色框中信息，标识符会发生变化，TTL不会发生变化。

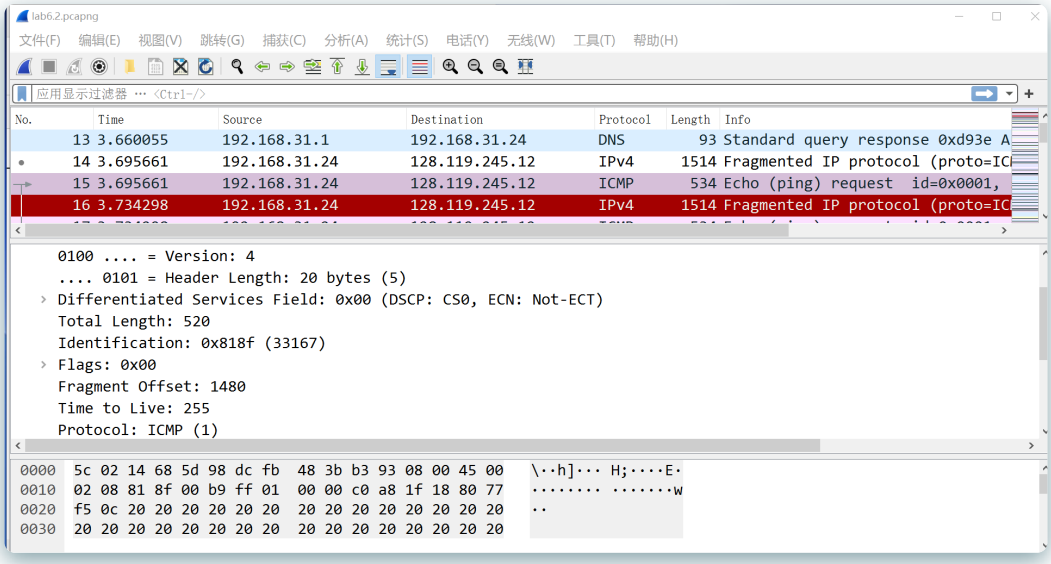
原因：不同IP数据报的标识符必然不同，而同一个路由器发送的所有回复TTL不会发生变化。

5. 启动wireshark进行数据包捕获。

6. 在pingplotter中调整 packet size 为**2000**，在 Address to Trace 中输入链接 **gaia.cs.umass.edu**，开始跟踪，待count=3时停止跟踪，停止wireshark抓包。此时 pingplotter 界面如下图所示：



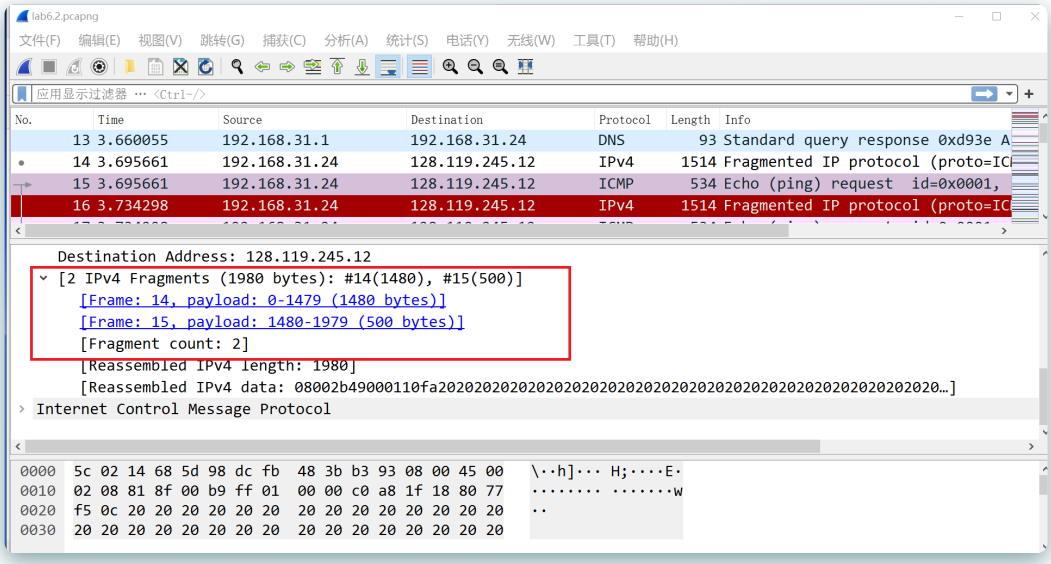
wireshark界面如下图所示：



回答下列问题：

> 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?

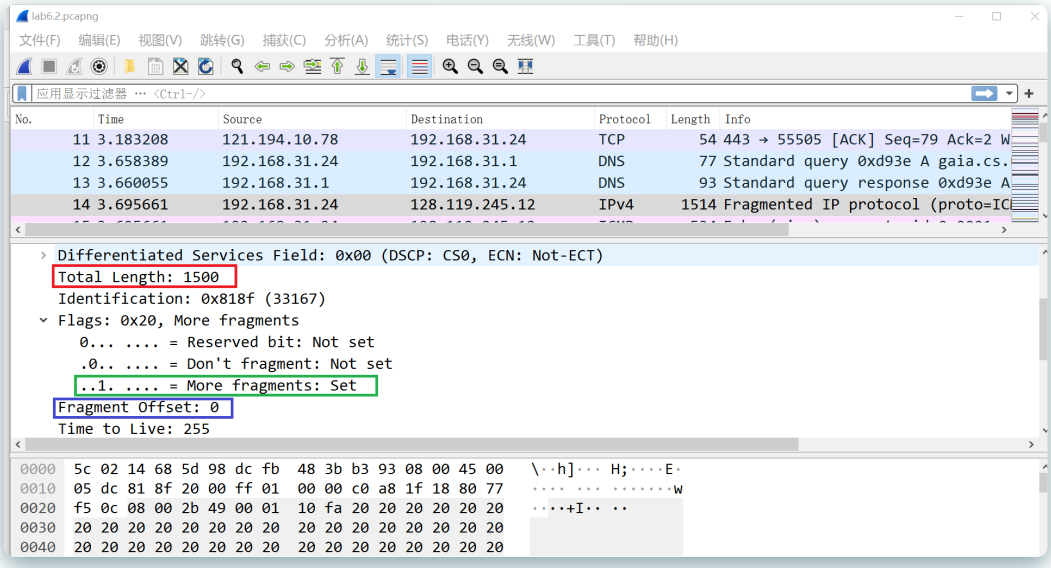
答：第一个 ICMP Echo Request 消息如下图所示：



根据上图红色框中内容，该消息碎片化为两个IP数据包。

> 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?

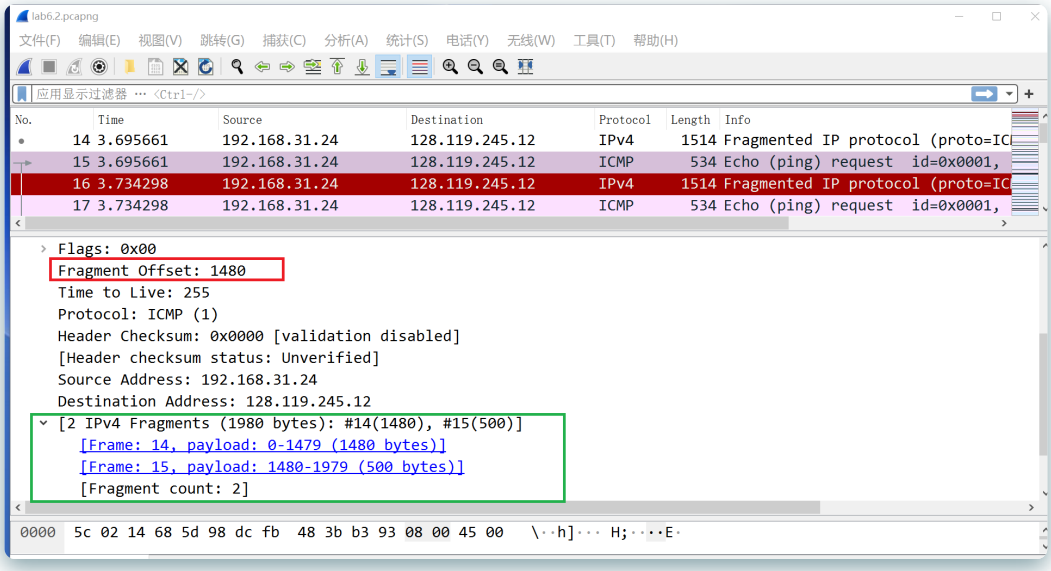
答：IP数据报的第一个片段如下图所示：



根据绿色框中内容，该信息表明数据报碎片化；根据蓝色框中内容，偏移量为0，表明这是第一个片段；根据红色框中内容，这个IP数据报长度为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?

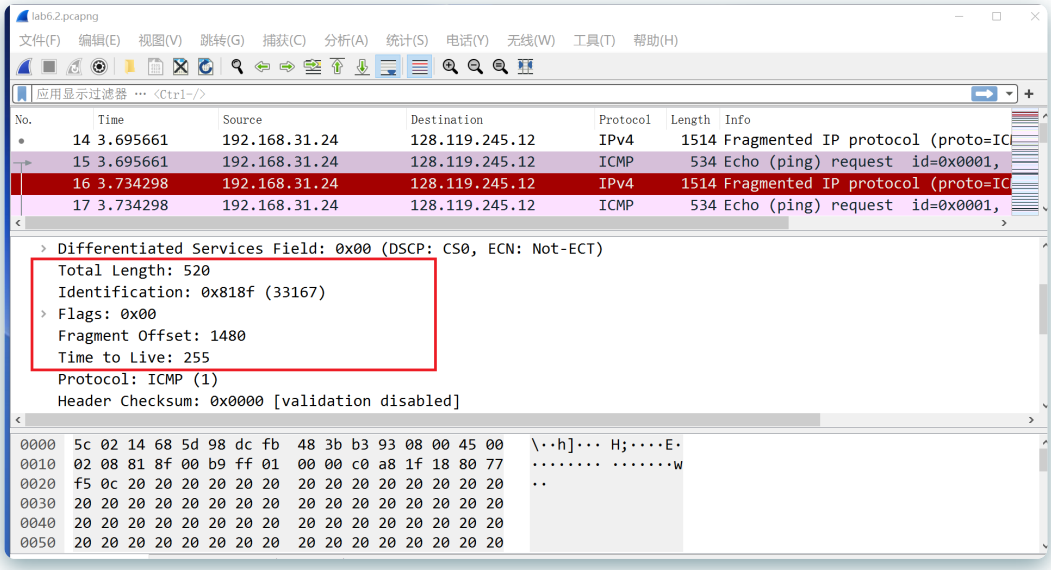
答：IP数据报的第二个片段如下图所示：

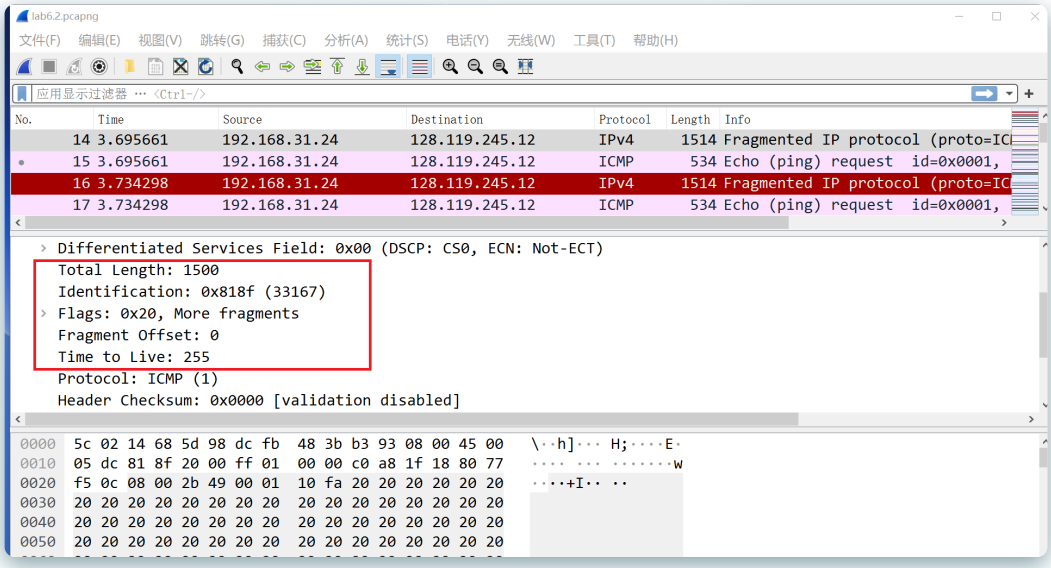


根据红色框中内容，偏移量不为0，故这不是第一个数据报片段；根据绿色框中内容，共有两个数据报，故没有更多的数据报。

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

答：两个IP数据报片段分别如下图所示：



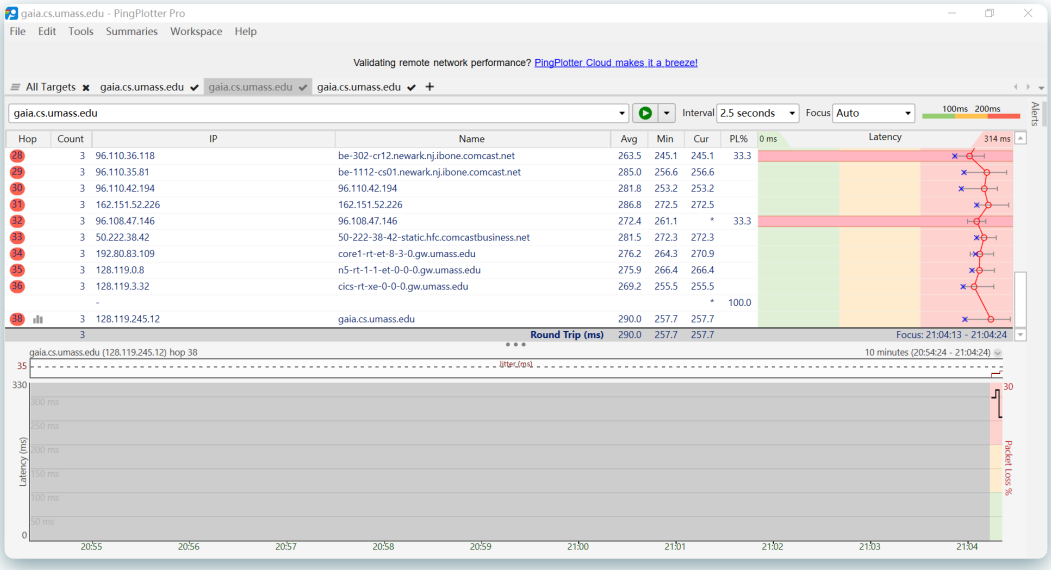


根据上图中红色框中内容，可知数据报长度、偏移量、Flags字段发生了变化。

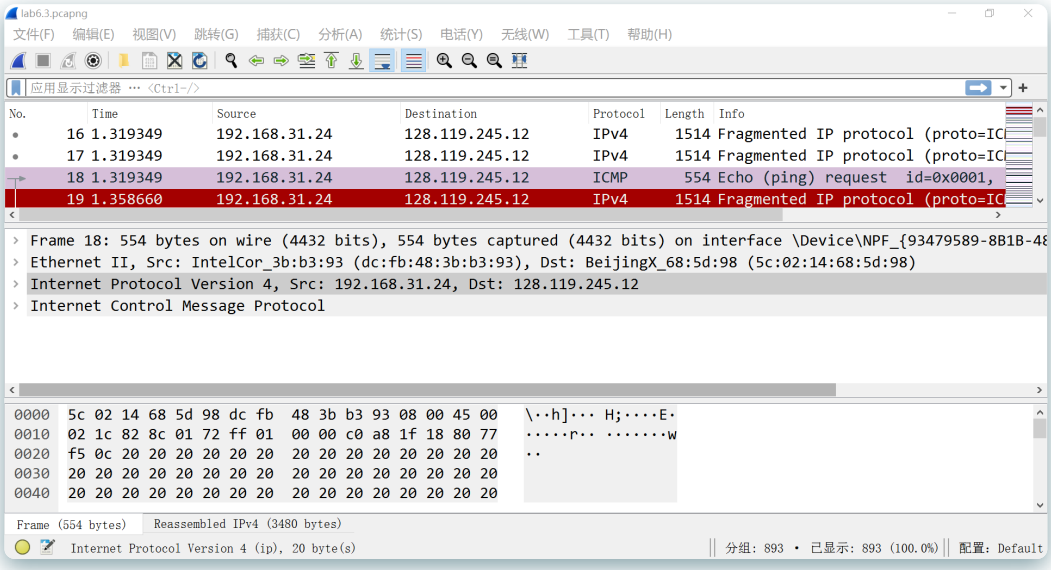
注：Header Checknum始终为0x0000 ??

7. 启动wireshark进行数据包捕获。

8. 在pingplotter中调整 packet size 为**3500**，在 Address to Trace 中输入链接 **gaia.cs.umass.edu**，开始跟踪，待count=3时停止跟踪，停止wireshark抓包。此时 pingplotter 界面如下图所示：



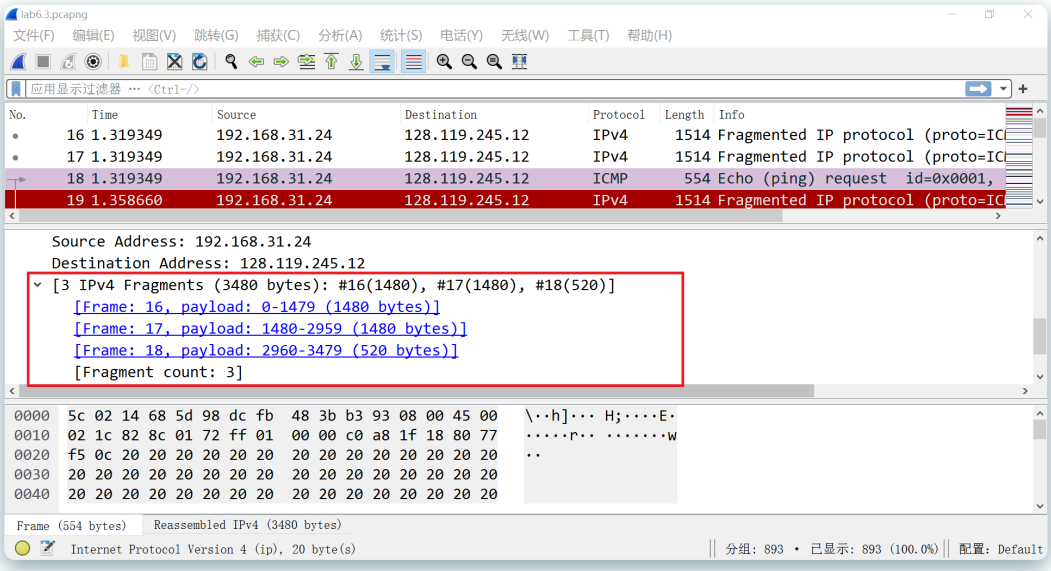
wireshark界面如下图所示：



回答下列问题：

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

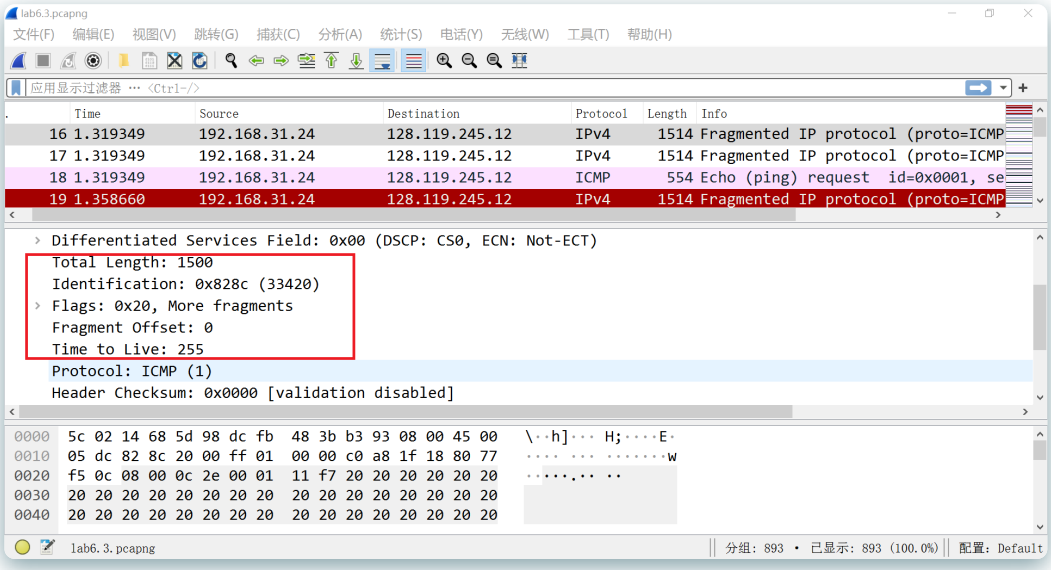
答：第一个 ICMP Echo Request 消息如下图所示：

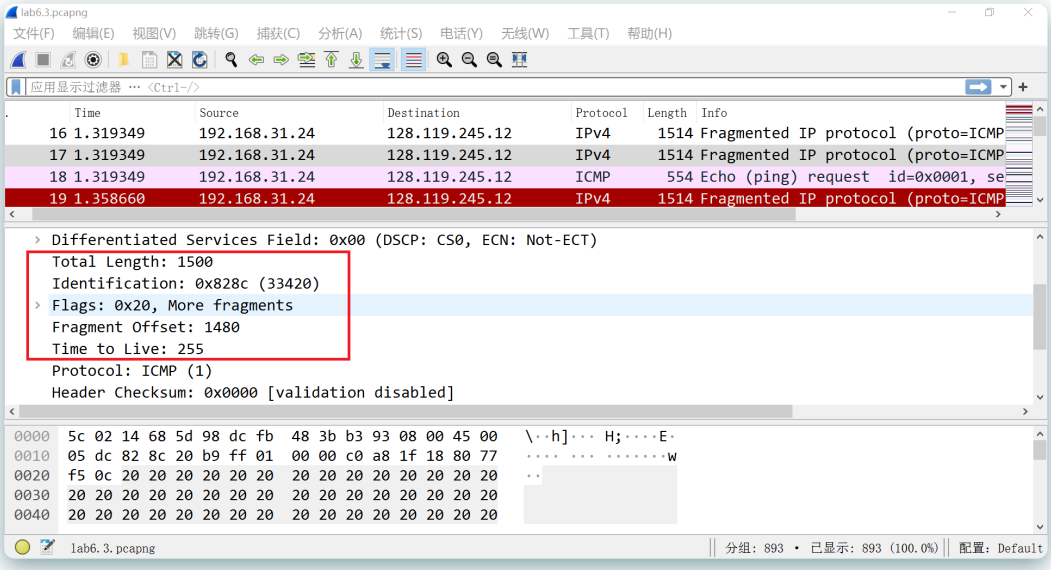


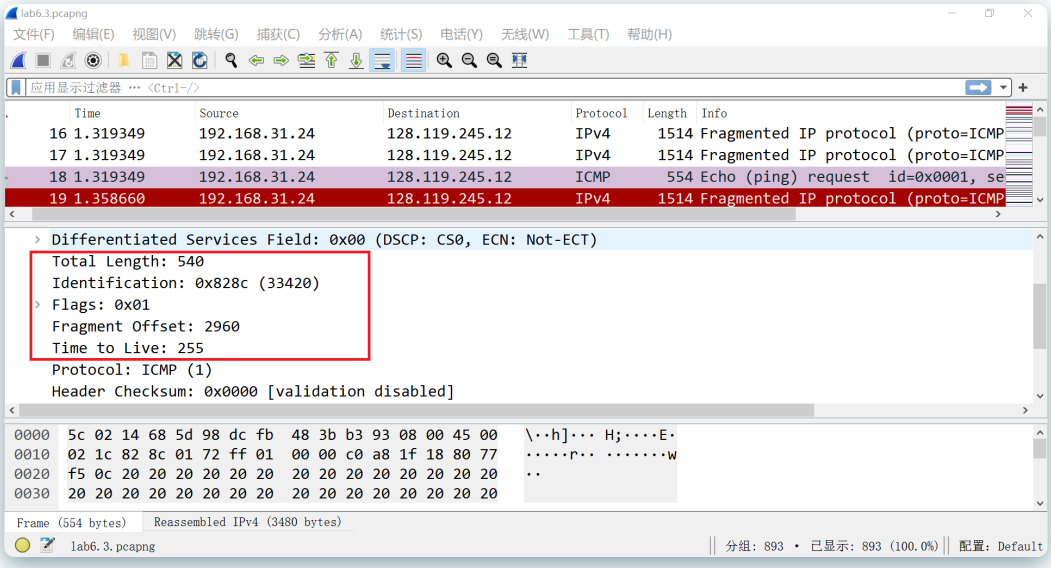
根据红色框中内容，原始数据报创建了3个片段。

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

答：三个数据报片段的信息分别如下图所示：







根据上图中红色框中内容，可知数据报长度、偏移量、Flags字段发生了变化。

注：Header Checknum始终为0x0000 ??

四.实验收获与感想

1. 深入理解了IP协议的工作原理，尤其是IP数据报的原理。
2. 学习了软件 `pingplotter` 的使用，了解了traceroute的执行与测试。
3. 了解了IP数据报的字段与分片原理。
4. 初步认识了ICMP协议与TTL。
5. 加强了对wireshark的了解和运用，了解了更多数据的抓取位置和时序图的使用与观察。