**中国科学技术大学计算机学院**

**计算机网络实验报告**

**实验四**

**利用Wireshark观察IP数据报**

**学 号：JL19110004**

**姓 名：徐语林**

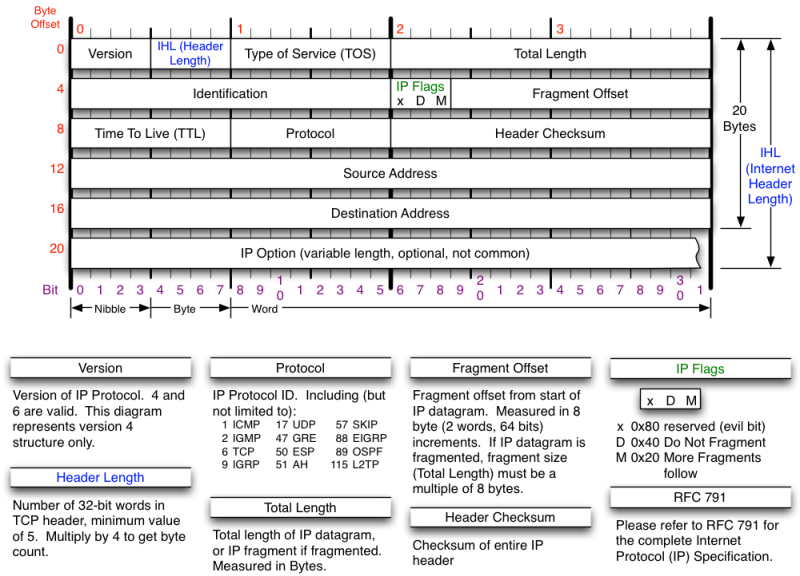
**专 业：计算机科学与技术**

**指导老师：张信明**

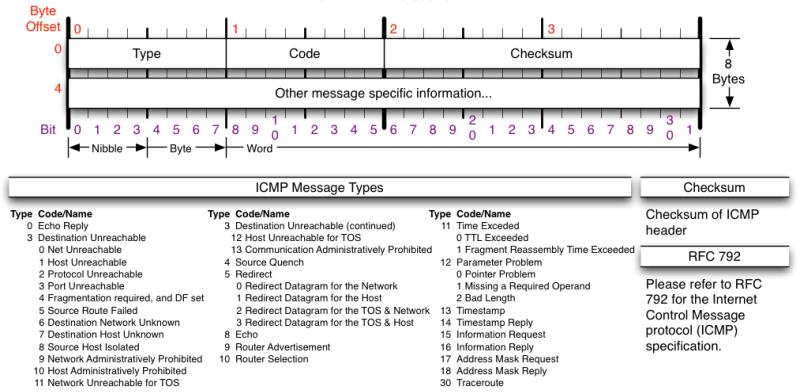
**中国科学技术大学计算机学院**

**2020 年 12 月 10 日**

1. **实验目的**
2. **通过捕获观察并分析IP数据报的结构**
3. **掌握traceroute的使用（Windows下替换为PingPlotter）**
4. **实验原理**
5. Wireshark是一种非常流行的网络封包分析软件，功能十分强大。可以截取各种网络封包，显示网络封包的各种详细信息。Wireshark使用Npcap作为接口，直接与网卡进行数据报文交换，监听共享网络上传送的数据包
6. TTL是IP数据包在计算机网络中可以转发的最大跳数，可以由发送者来设置，每经过一个路由器，路由器就会修改这个TTL字段值，具体的做法就是把该TTL的值减一，再把IP包发送出去。如果在IP包到达目的IP之前，TTL减少为0，路由器将会丢弃这个IP包并向IP包的发送者发送ICMP time exceeded的消息。而traceroute或者是pingplotter也就是设置ttl，通过一次次的重传，与ttl+1来得到到达目的地址的路径上的路由器的信息。
7. IPV4报文：



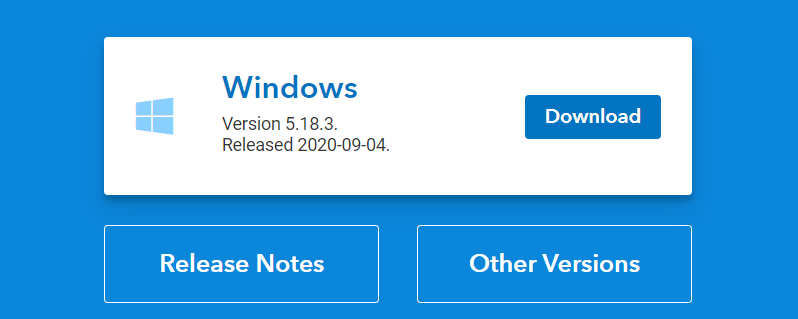
1. ICMP报文：



1. 实验条件

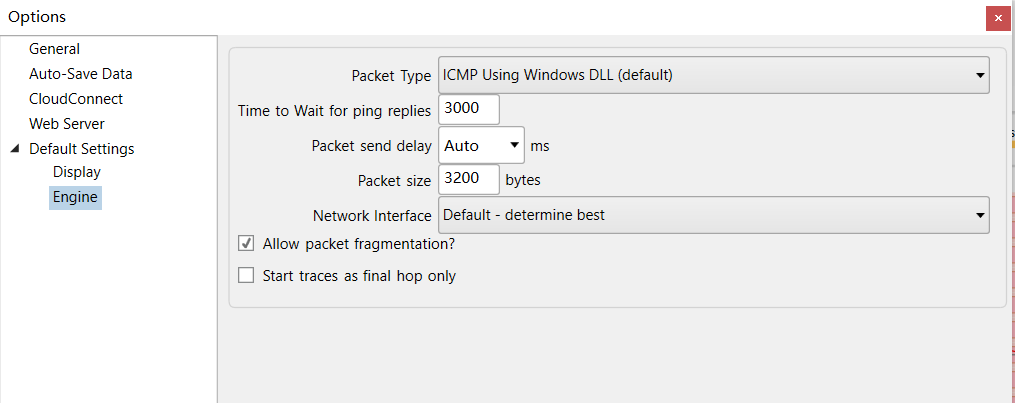
由于是Windows系统，所以利用的是Pingplotter以及之前安装好的wireshark.

1. 实验过程
2. 官网上下载实验要用的Pingplotter:

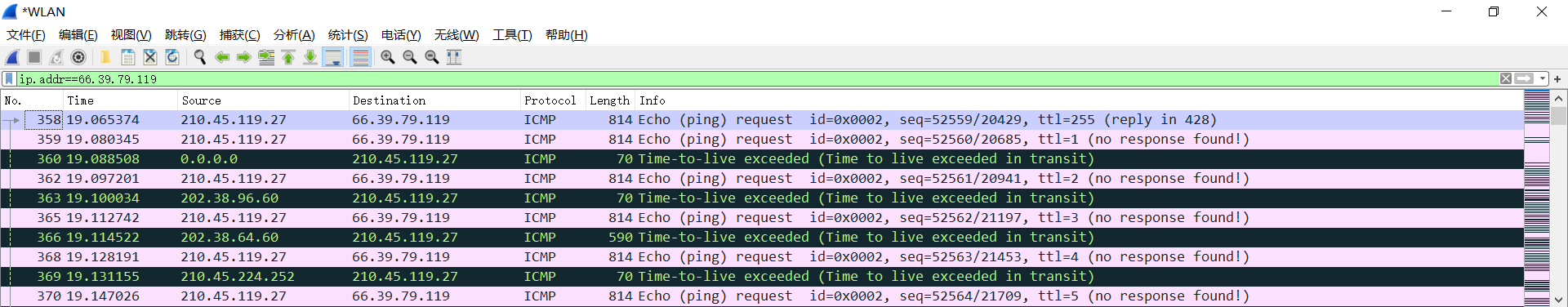


1. 利用PingPlotter发包并用wireshark来捕获查看.用wireshark开始捕获，用PingPlotter发送800，1600,3200的包.

如下是在PingPlotter界面进行的设置：

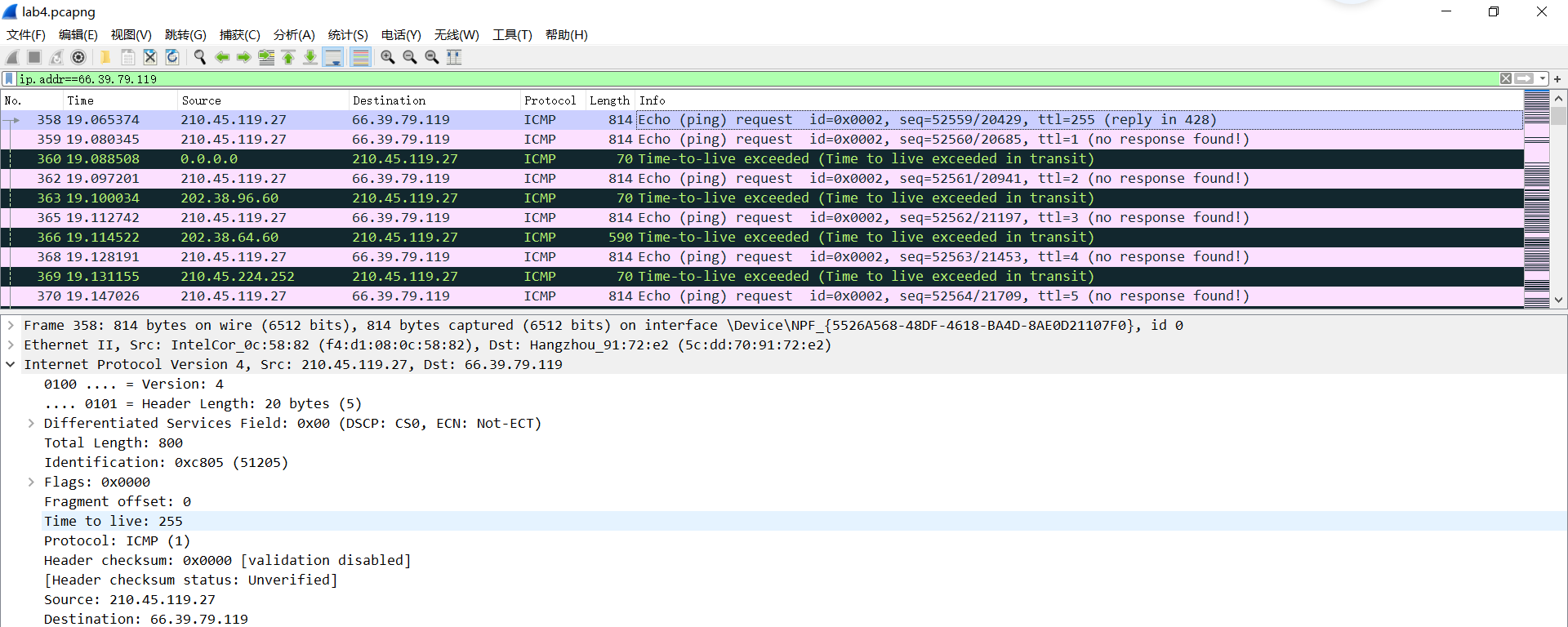


捕获完后在wireshark中写入筛选的条件：

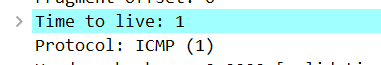


1. 回答问题
2. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

答：我的ip地址为210.45.119.27

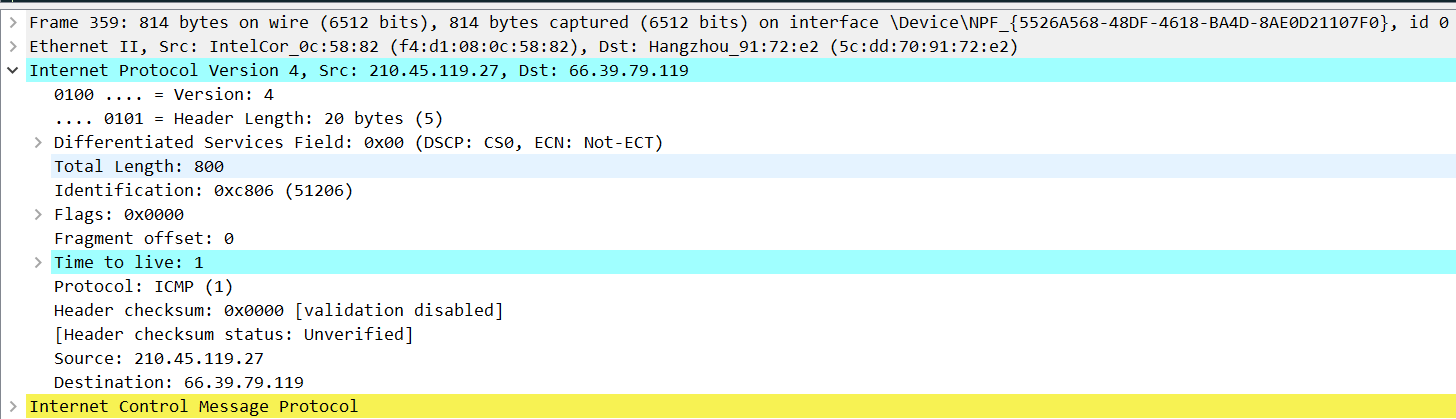


1. Within the IP packet header, what is the value in the upper layer protocol field?

答：

可见上层协议区域的值为ICMP（1）.

1. 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.

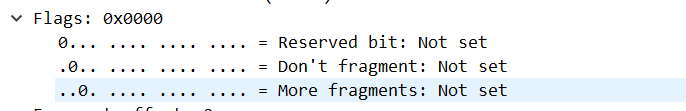
答：

20字节；

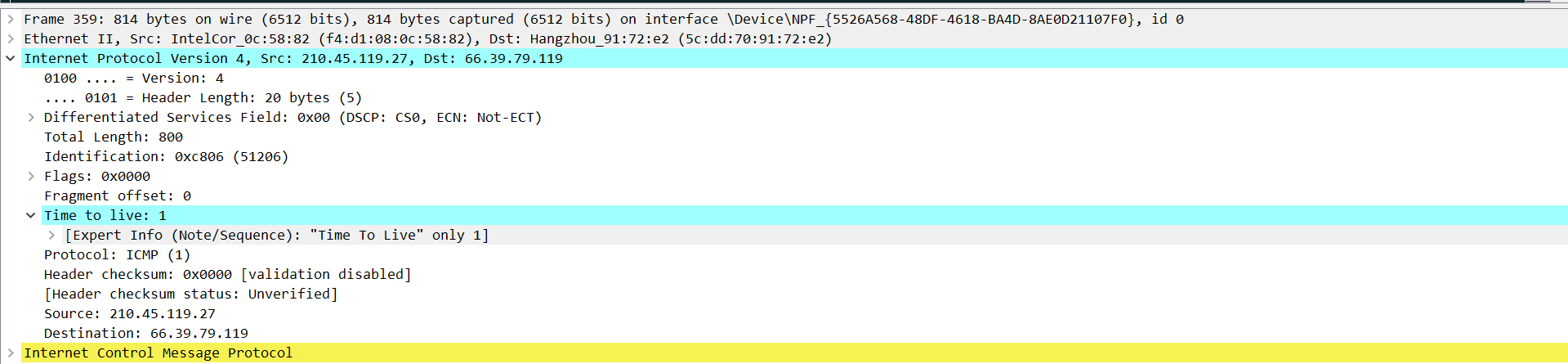
Payload字节数：800-20=780.

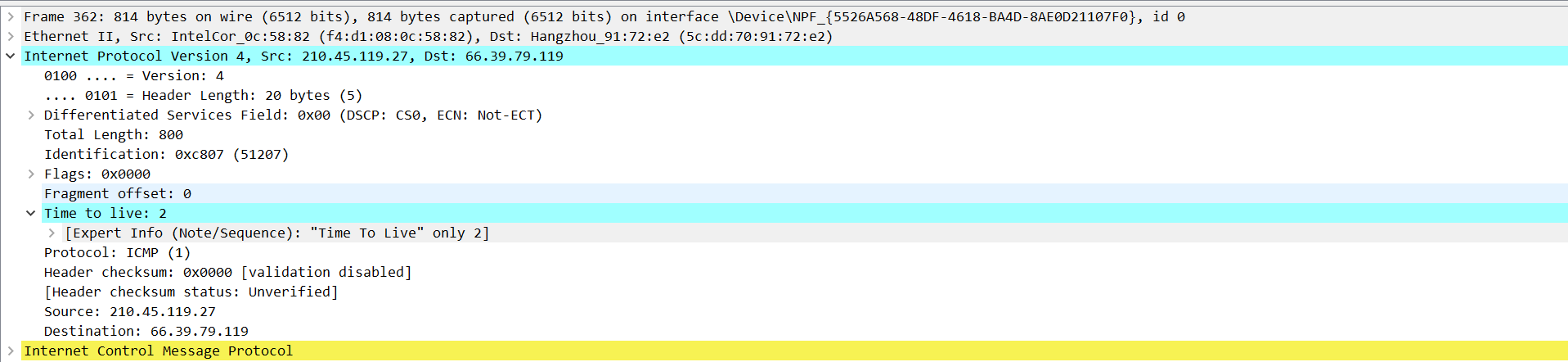
1. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

答：该数据包没有被分割，由于在flags的标记中，more fragments位没有被置为1.



1. 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：



从中可以看出TTL,Identification是在改变的。

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

答：保持不变的字段有：Version,Protocol,Header Length,Differentiated Services Field,Source,Destination.

理由：Version：都是IPv4.

Protocol:都是ICMP.

Header Length:都是ICMP，所以不变

Differentiated Services Field:都是ICMP.

Source和Destination:由于在这个过程中源，目的主机并不发生变化，所以这两个也不会改变

必须改变的有：TTL,Identification

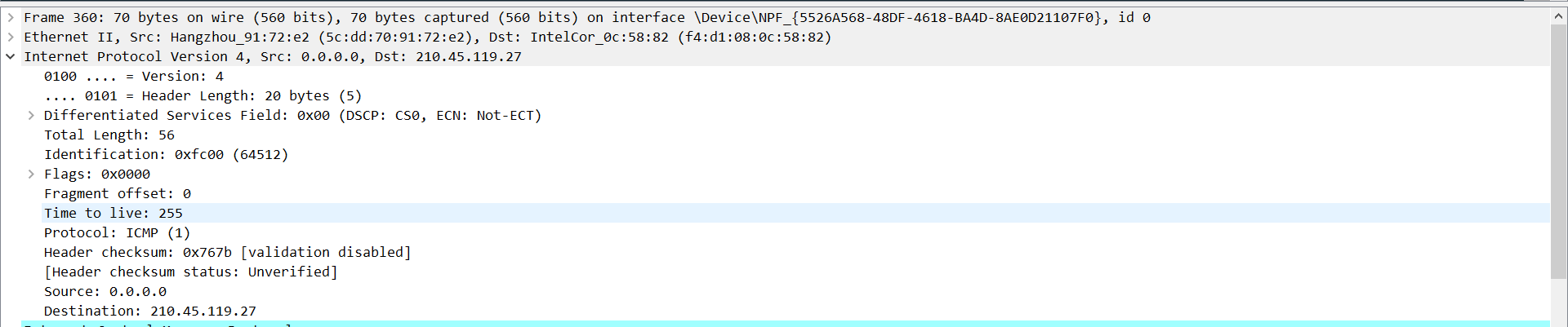
理由：TTL:基于ppt上的原理可知TTL必须改变

Identification:数据报之间的id是不一样的

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

答：可参见第五题的图，id会加一

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

答：

第一跳的：Identification:0xfc00(64512)

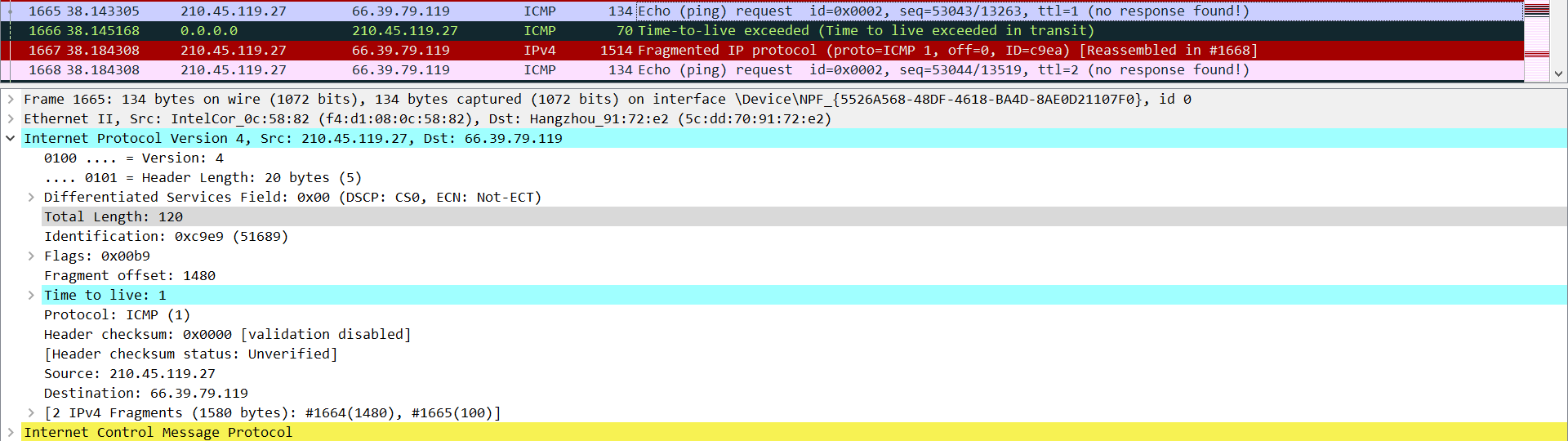
TTL:255

1. 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：id变化.id需要独立，但是ttl不会发生变化，电脑的第一条路由是不会发生变化的，ttl初始值被设置为了255，便不会再发生改变。

1. 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 ip-ethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation. 3 ]

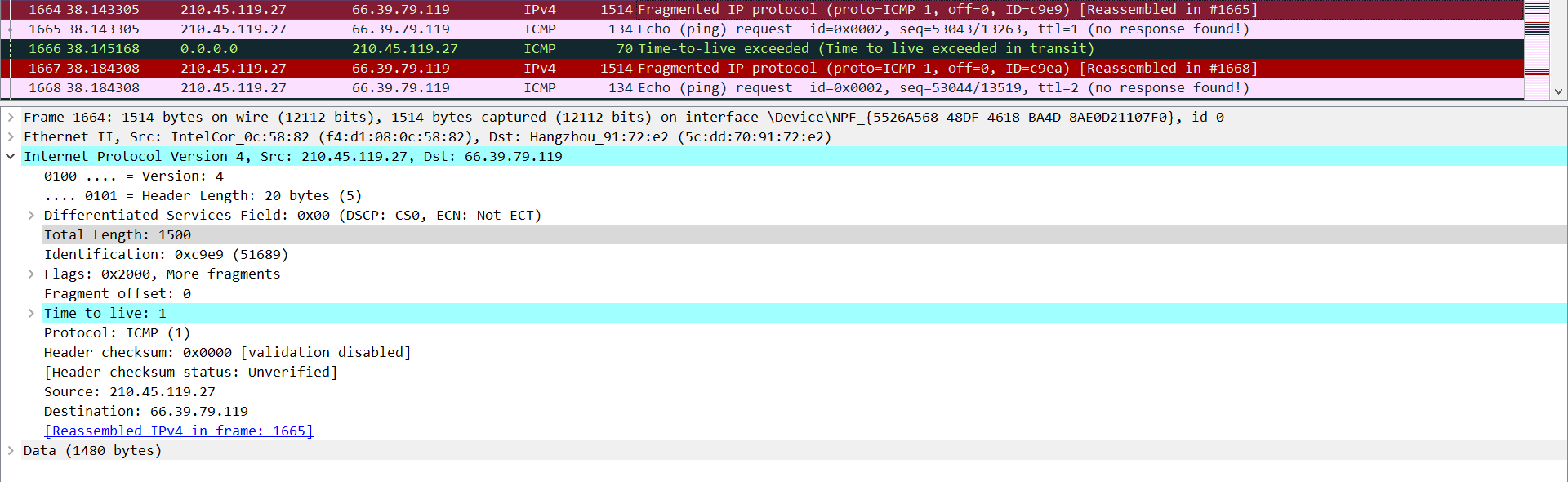
答：如图：



被分成了两个fragment.

1. 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?

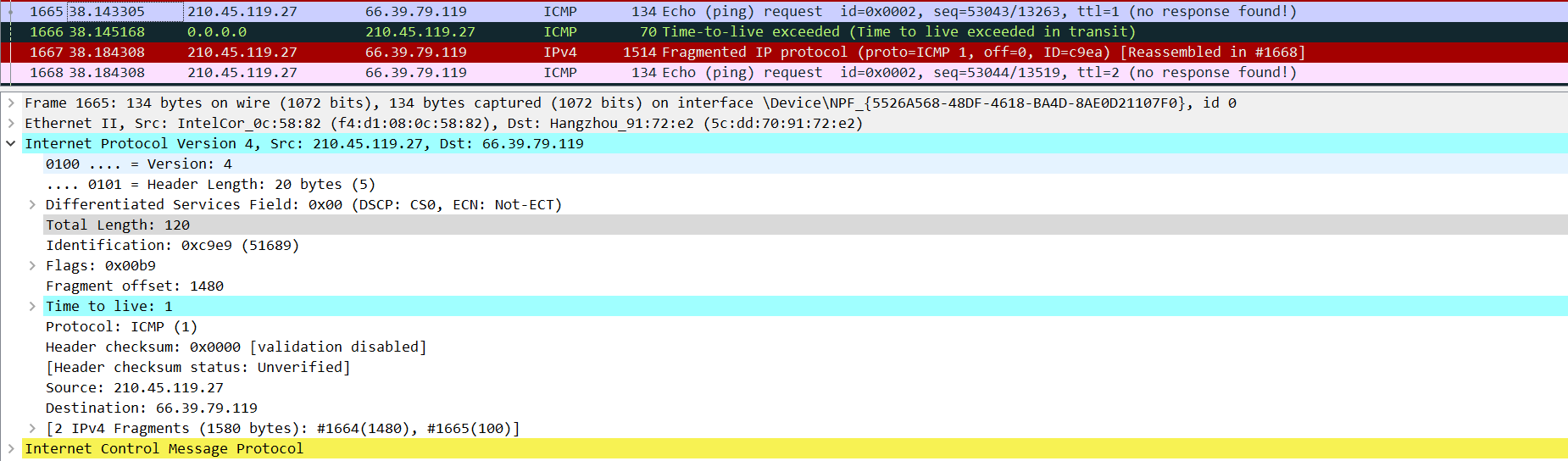
答：



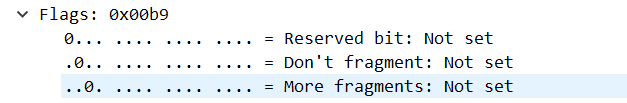
No.1664号frame可以知道其中的more flag被置为了1，Fragment offset为0，整个ip包长度为1500字节

1. 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：找到No.1665号.



其中的fragment offset非0这就说明这不是第一个；

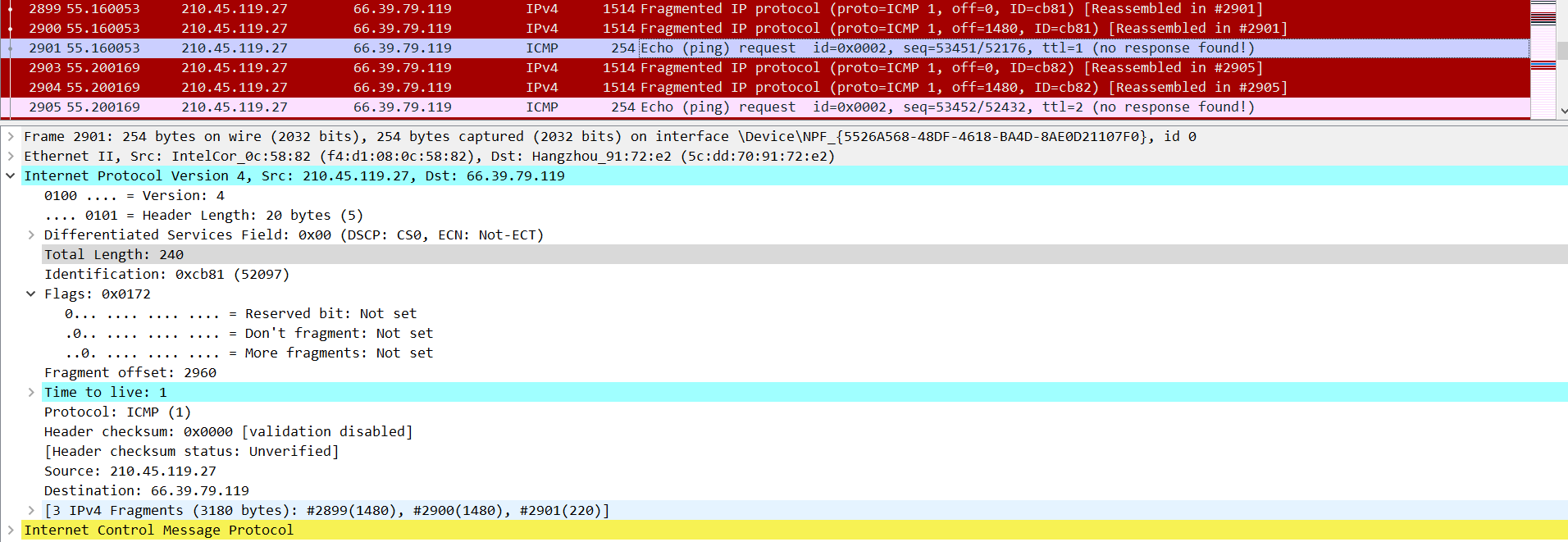


More fragments说明没有更多的片段

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

答：改变的有total length,flags,fragment offset.

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

答：

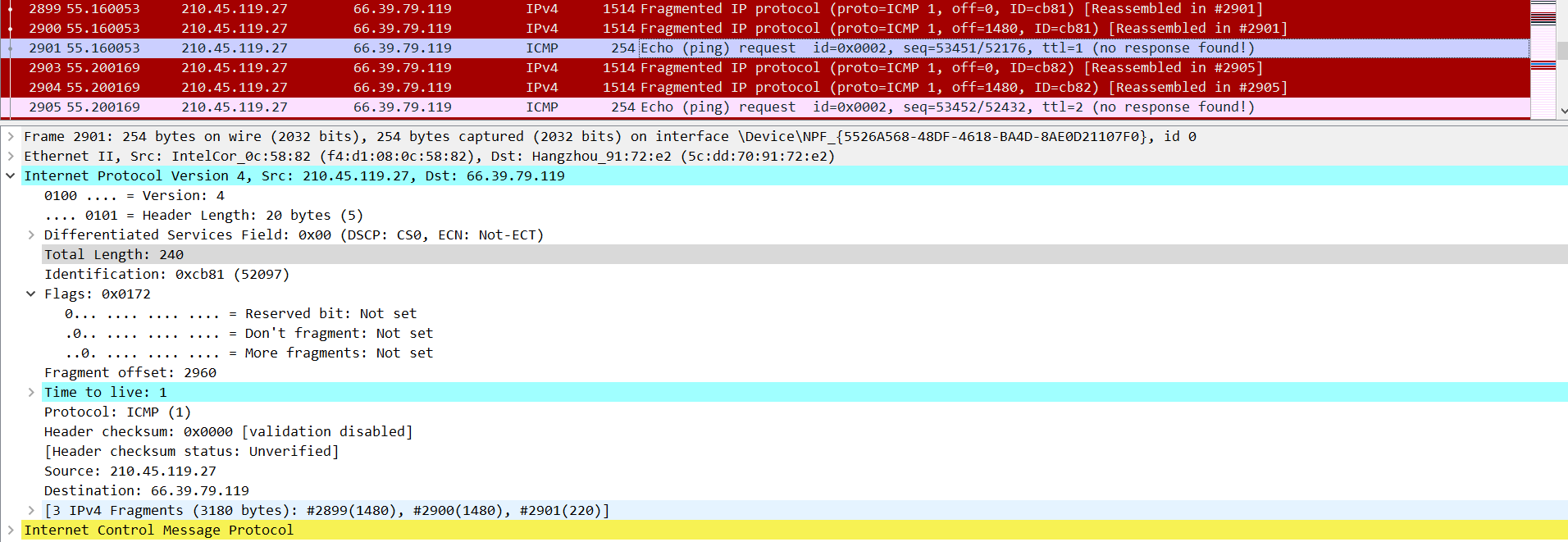
有3个.

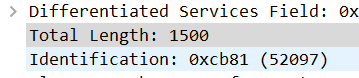
1. What fields change in the IP header among the fragments?

答：第一个和第二个的more fragments位是1，第三个是0；

第一个和第二个payload为1480，第三个为220

对于ppt中报文分片问题的计算，用第14题来做个说明：





1500除开20字节还有1480.第三个的要求是3200，那么只能容纳两个1480的分片，这样1480\*2=2960.3200-2960=240，这是加入了20字节报头的，除开后便是220，所以范围是0-1479,1480-2959,2960-3179.

1. 实验总结

本次实验观察了ip数据报的结构，进一步加深了对ip数据报的理解，以及分片问题的求解，对于理解网络层这一章来说还是有很好的作用.