中国科学技术大学计算机学院

《计算机网络》实验报告

实验题目：lab4_WireShark Labs(IP)

学生姓名：胡毅翔

学生学号：PB18000290

专业：计算机科学与技术

指导老师：张信明

完成日期：2020 年 12 月 29 日

计算机实验教学中心制

2019 年 09 月

实验目的

1.进一步掌握 Wireshark 网络分析工具。

2.捕获观察 IP 数据报，分析其结构。

3.回答本次实验指导书中的问题。

实验原理

本次实验使用 WireShark 工具。其中，用来观察执行协议实体之间交换的报文的基本工具称为分组嗅探器(packet sniffer)。分组嗅探器被动地拷贝(嗅探)由计算机发送和接收的报文；它也能显示出这些被捕获报文的各个协议字段的内容。分组嗅探器从不发送报文，同时接收到的报文也不会显式地发送到分组嗅探器。它接受的是发送/接收的报文的复制。

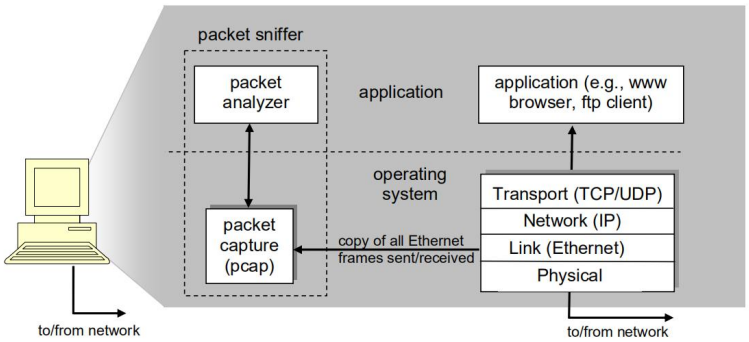

图 1

分组嗅探器的结构如图 1 所示。在图 1 的右边是运行在计算机上的协议和应用。分组嗅探器(图中画虚线框部分)是计算机中的附加软件(区别于上述协议和应用)，它包含两个部分。分组捕获库获取每一个链路层接收/发送的帧。第二部分是分组分析器，其中显示了协议所有字段的内容。为了实现这一目的，分组分析器必须理解所有协议所交换的信息的结构。比如，我们对图 1 中 HTTP 协议的各个字段信息感兴趣。分组分析器理解以太网帧的格式，所以可以从以太网帧中区分出 IP 数据报。同时，它还理解 IP 数据报格式，所以它能从 IP 数据报分离出 TCP 报文段。最后，它还理解 TCP 报文段格式，从中分离出 HTTP 报文。又因它理解 HTTP 协议，所以能在实现 WireShark 中显示 HTTP 协议各字段信息的功能。

实验环境

1.PC 一台

2.Windows 系统

3.WireShark 网络分析工具(版本 3.4.2)

4.Edge 浏览器(版本 86.0.622.56)

5.PingPlotter(版本 5.18.3.8189)

实验过程

WireShark Lab: IP

Capturing packets from an execution of traceroute

实验步骤

1.启动 Wireshark 开始抓包。

2.If you are using a Windows platform, start up pingplotter and enter the name of a target destination in the “Address to Trace Window.” Enter 3 in the “# of times to Trace” field, so you don’t gather too much data. Select the menu item Edit->Advanced Options->Packet Options and enter a value of 800 in the Packet Size field and then press OK. Then press the Trace button. You should see a pingplotter window that looks something like this: 启动 PingPlotter，输入目标地址 128.59.23.100。设置包的大小为 800 字节，开始传输。

3.修改包的大小为 1600 字节重复上述操作。

4.修改包的大小为 3200 字节重复上述操作。

5.停止 WireShark。

A look at the captured trace

实验步骤

1.选择第一个你的计算机发送的 ICMP 响应请求报文，在包详细信息窗口中展开 IP 部分的内容。

2.回答下列问题。

问题

Q1:What is the IP address of your computer?

A1:客户端的 IP 地址是 114.214.255.208，如图 2。

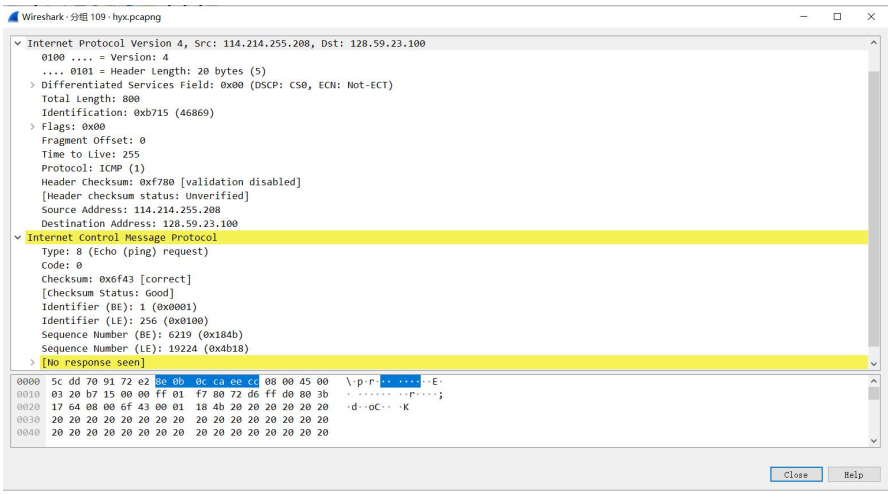

图 2

Q2:Within the IP packet header, what is the value in the upper layer protocol field?

A2:值为 1，如图 3。

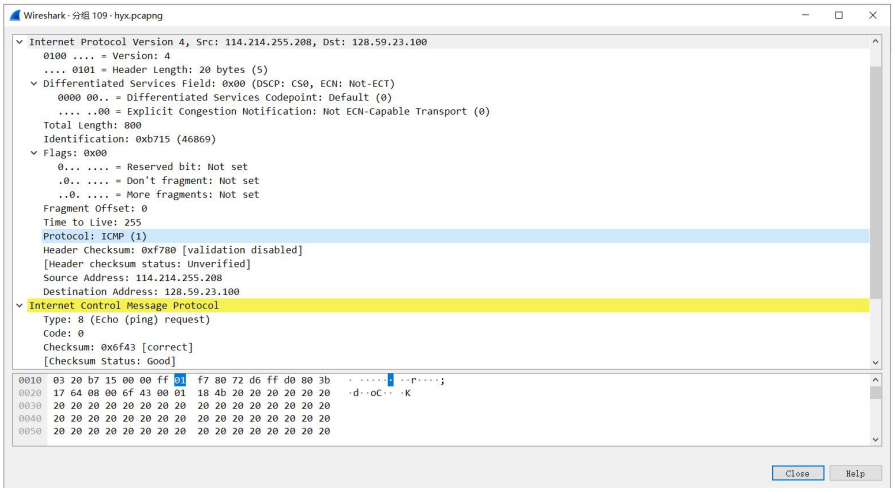

图 3

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.

A3:IP 数据报报头的长度为 20 字节，如图 3 中 Header Length 所示。IP 数据报的有效载荷为 780 字节。由图 3 中的 Total Length 可知 IP 数据报总长为 800 字节，去掉报头 20 字节，800-20=780。

Q4: Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

A4:IP 数据报没有分片，由图 3 中的 More fragments 为 0 和 Fragment Offset 为 0 可知，这是第一个分片且之后没有分片了。

Next, sort the traced packets according to IP source address by clicking on the Source column header; a small downward pointing arrow should appear next to the word Source. If the arrow points up, click on the Source column header again. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the “details of selected packet header” window. In the “listing of captured packets” window, you should see all of the subsequent ICMP messages (perhaps with additional interspersed packets sent by other protocols running on your computer) below this first ICMP. Use the down arrow on your keyboard to move through the ICMP messages sent by your computer.

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?

A5:Time to Live 递增(但在 ttl=1 的 IP 数据报发出前，有一个 ttl=255 的发出，之后按 1，2，3……递增)，还有 Identification，Header Checksum 也在变化，如图 4。

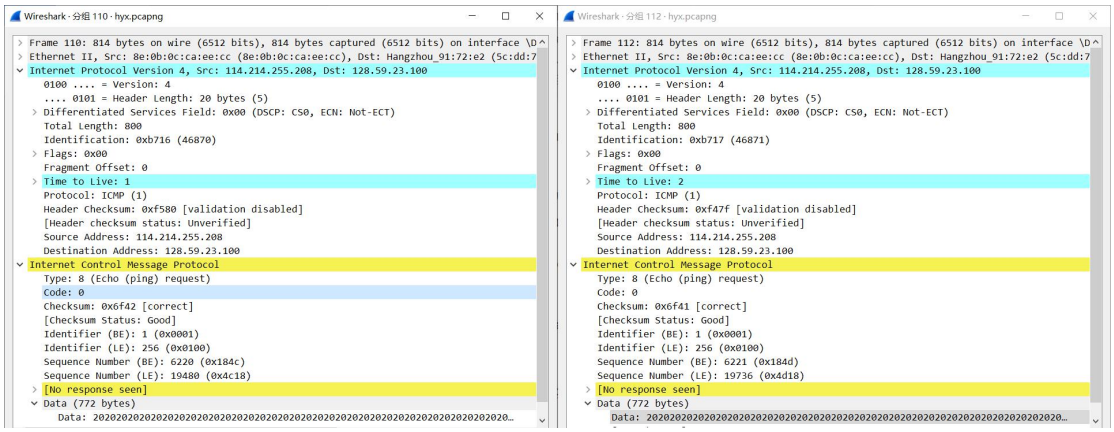

图 4

Q6:Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

A6:Version，Header Length，Total Length，Flags，Fragment Offset，Protocol，Differentiated Services，源 IP 地址及目的 IP 地址等都保持不变。Version，Header Length，Total Length，Flags，Fragment Offset，Protocol，Differentiated Services，源 IP 地址及目的 IP 地址等对于在本次实验中传输的数据报长度为 800 字节的 IP 数据报而言保持不变。但本次实验中必须不变的是 Version (IPv4)，Header Length (20)，Differentiated Services (0x00)，Protocol (ICMP)(1)。其他域可以通过修改地址，数据报长度等进行修改。

Q7:Describe the pattern you see in the values in the Identification field of the IP datagram.

A7:观察可知，Identification 每次递增 1。

Next (with the packets still sorted by source address) find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router.

Q8: What is the value in the Identification field and the TTL field?

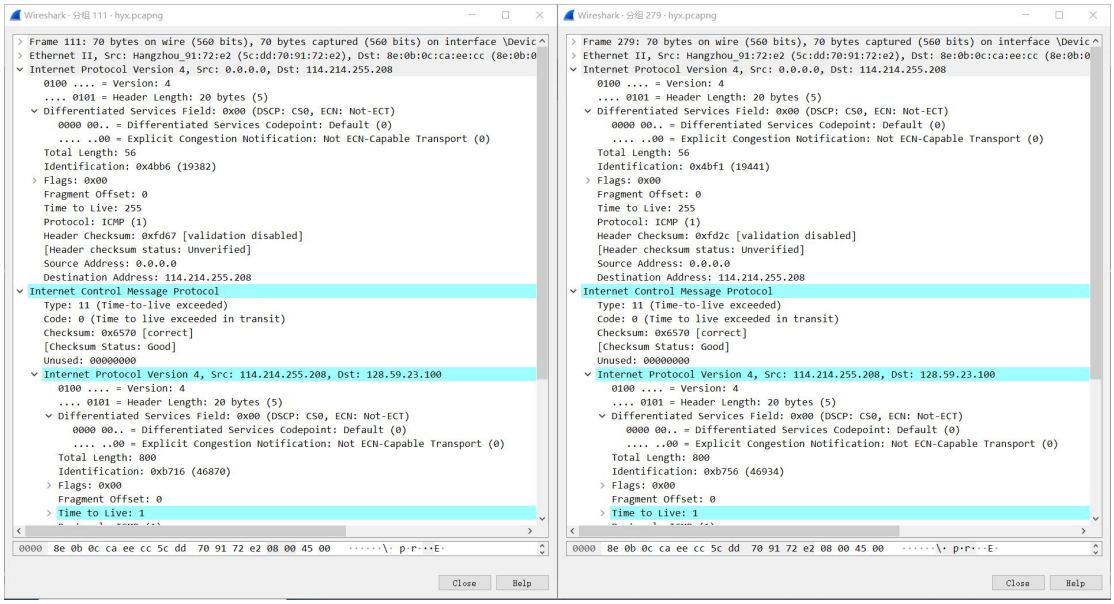

图 5

A8:Identification 域的值为 0x4bb6，TTL 域的值为 255，如图 5 左。

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?

A9:TTL 是不变的，但 Identification 是变化的。因为每次最近的路由器发送 TTL-exceeded 回复时，都置 TTL 为 255，但 Identification 标识符是与每条 IP 数据报相关的。

Fragmentation

实验步骤

1.Sort the packet listing according to time again by clicking on the Time column.

问题

Q10: Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 1600. Has that message been fragmented across more than one IP datagram?

A10:是的，出现了分段，由图 6 中 More fragments 等于 1 可知。

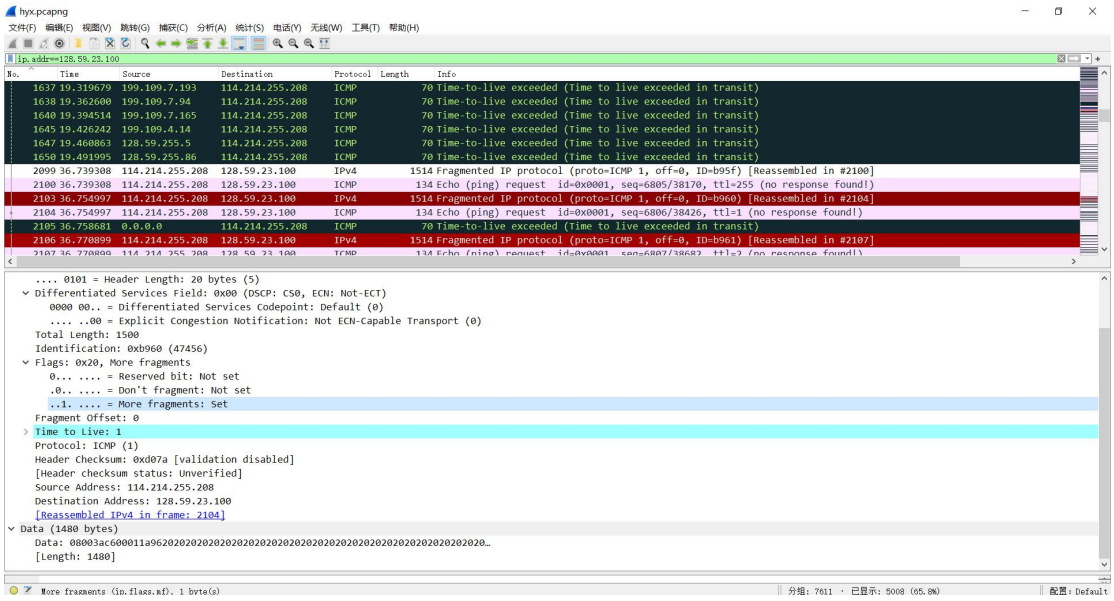

图 6

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?

A11:由图 6 中 More fragments 等于 1 可知被分段了。由图 6 中 Fragment Offset 值为 0，说明这是第一个分片。由 Total Length 知 IP 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?

A12:由图 6 中 Fragment Offset 值为 1480，说明这不是第一个分片。由图 6 中 More fragments 等于 0 可知，没有更多分片。

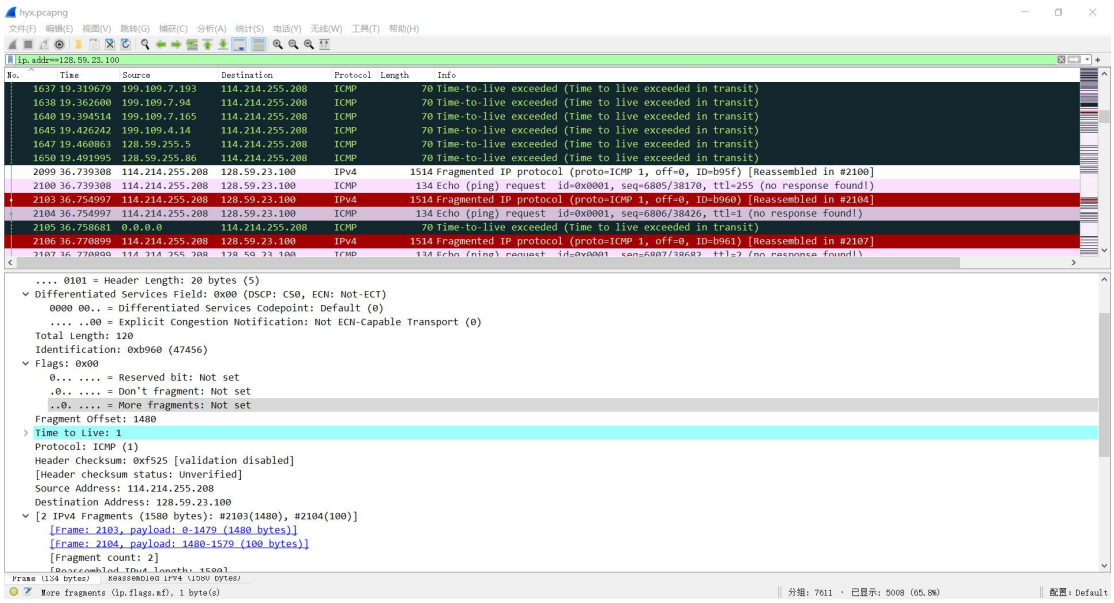

图 7

Q13:What fields change in the IP header between the first and second fragment?

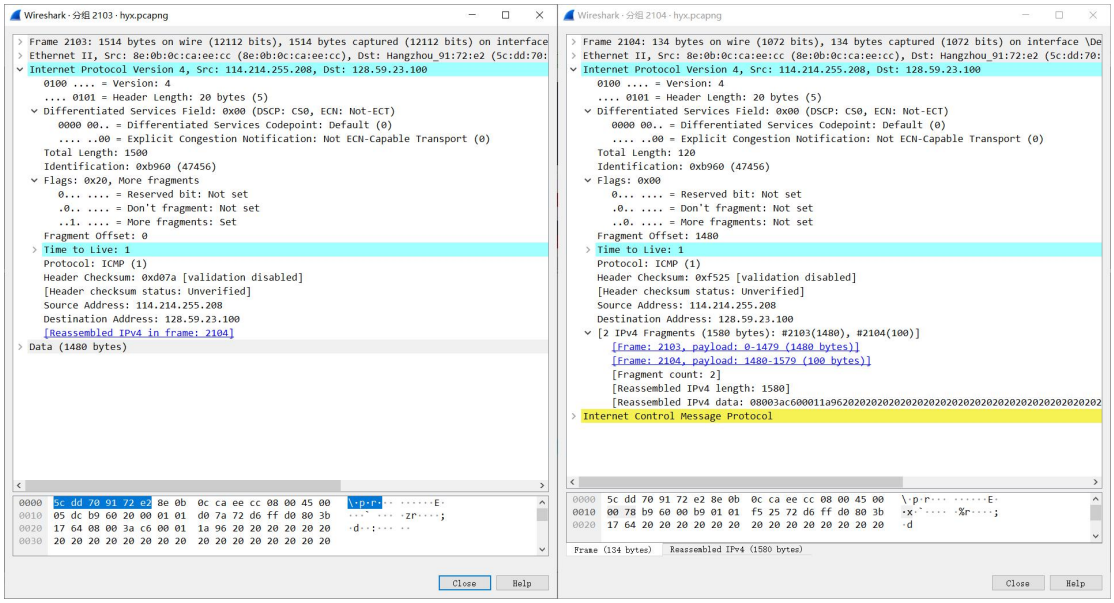

图 8

A13:由图 8 可知 Total Length，More fragments，Fragment Offset，Header Checksum 发生了变化。

Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3200.

Q14:How many fragments were created from the original datagram?

A14:由图 9 可知，分为了 3 个分片。

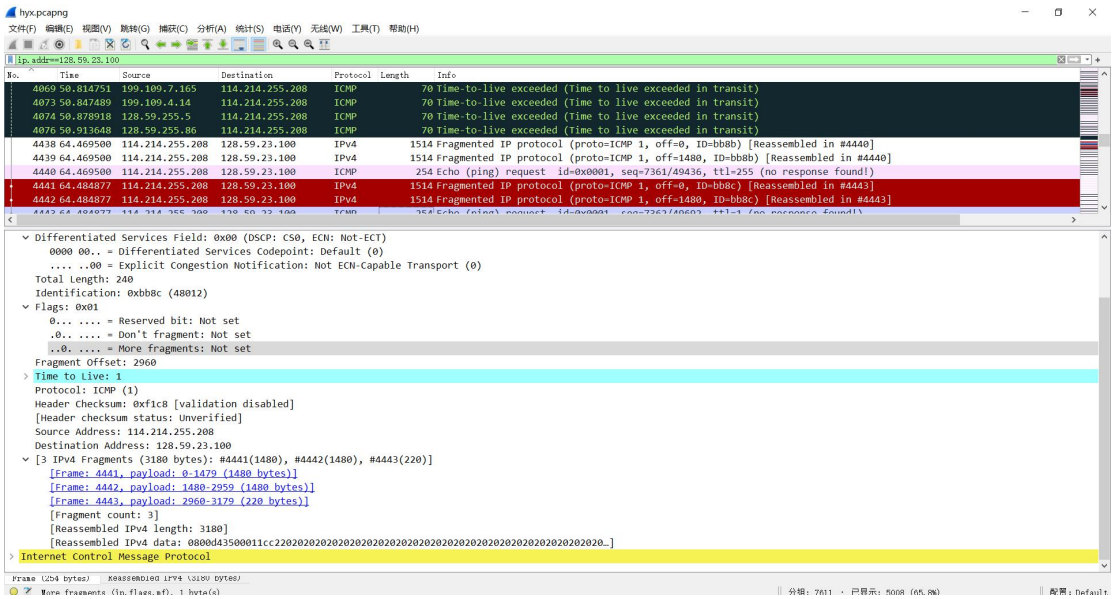

图 9

Q15:What fields change in the IP header among the fragments?

A15:由图 10 可知变化的域有：Total Length，More fragments，Fragment Offset 及 Header Checksum。

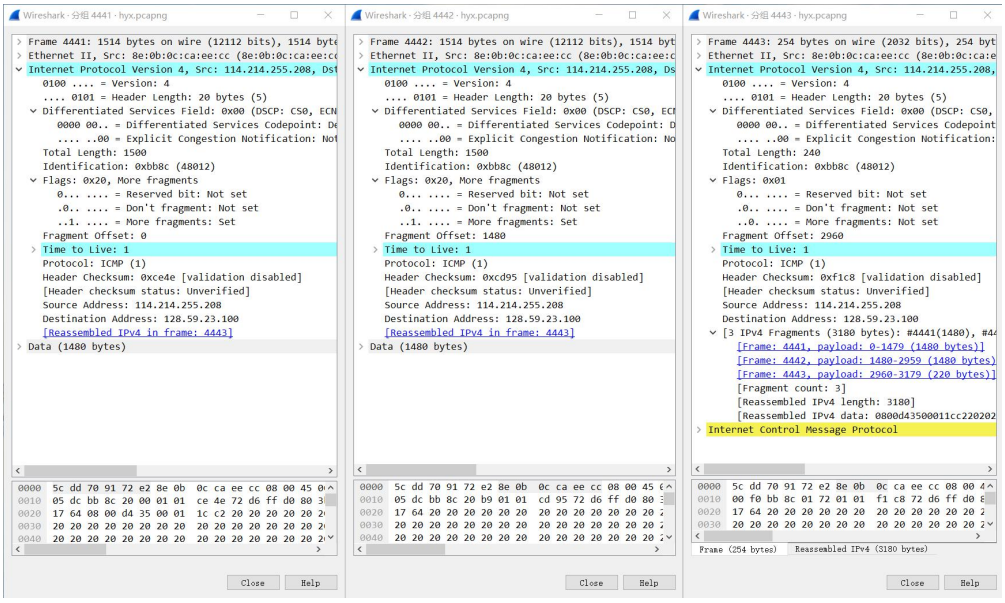

图 10

总结

本次实验通过 WireShark 分组嗅探器捕获并分析 IP 数据报，深入了解了 IP 数据报的结构，对报文中的内容有了深刻的理解，在回顾教材内容的同时又有所提升，进一步加深了对网络层的理解。

附：本次实验使用 WireShark 分组嗅探器获得的数据部分以截图形式体现于实验报告中，完整数据在 Github 仓库。