

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三　基于PCAP库侦听并分析网络流量**

**班　　级 软件工程2020级数媒班**

**姓　　名 陈鑫蕾**

**学　　号 22920202202877**

**实验时间 2022年11月02日**

**2022年11月02日**

填写说明

1. 本文件为Word模板文件，建议使用Microsoft Word 2019打开，在可填写的区域中如实填写；
2. 填表时勿破坏排版，勿修改字体字号，打印成PDF文件提交；
3. 文件总大小尽量控制在1MB以下，最大勿超过5MB；
4. 应将材料清单上传在代码托管平台上；
5. 在实验课结束14天内，按原文件发送至课程FTP指定位置。

# 实验目的

通过完成实验，理解数据链路层、网络层、传输层和应用层的基本原理。掌

握用 Wireshark 观察网络流量并辅助网络侦听相关的编程；掌握用 Libpcap 或

WinPcap 库侦听并处理以太网帧和 IP 报文的方法；熟悉以太网帧、IP 报文、TCP

段和 FTP 命令的格式概念，掌握 TCP 协议的基本机制；熟悉帧头部或 IP 报文头

部各字段的含义。熟悉 TCP 段和 FTP 数据协议的概念，熟悉段头部各字段和 FTP

控制命令的指令和数据的含义。

# 实验环境

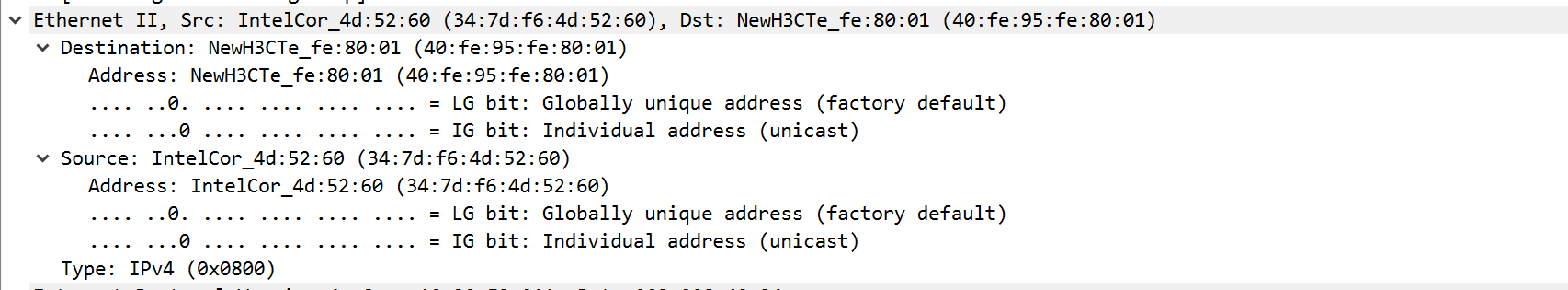
操作系统：Windows

编程语言：C++

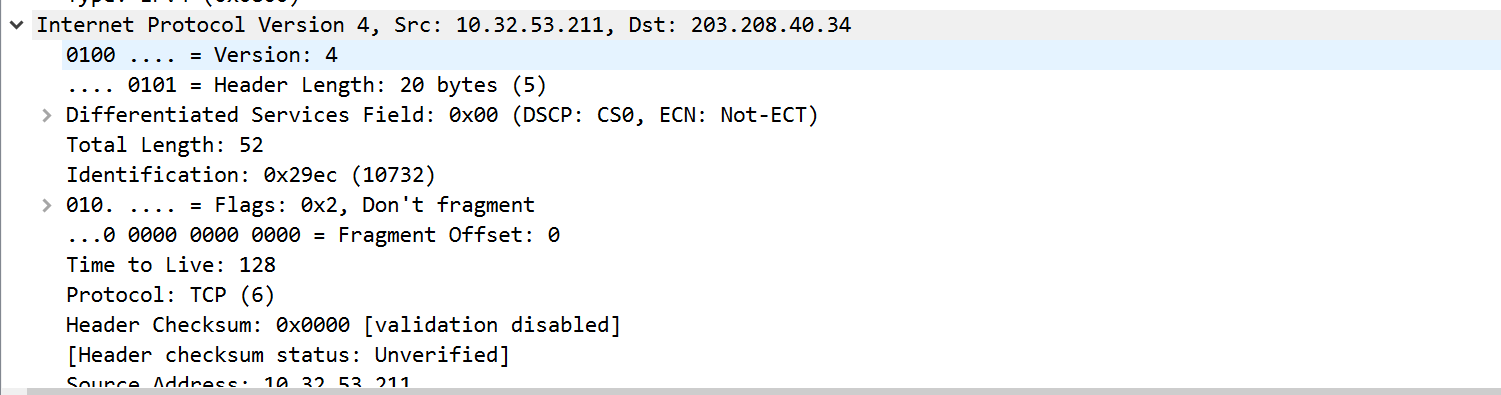
# 实验结果

1. 用侦听解析软件观察数据格式：

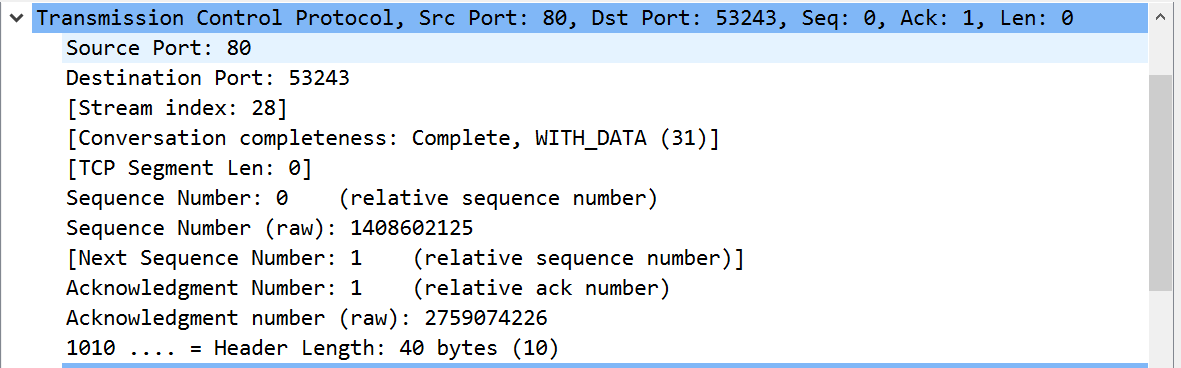
帧头部信息：



IP报包头部信息：



TCP数据段：



Mac地址:

`LE0BP`8[GO5U2(9FGULF]5

IP地址：

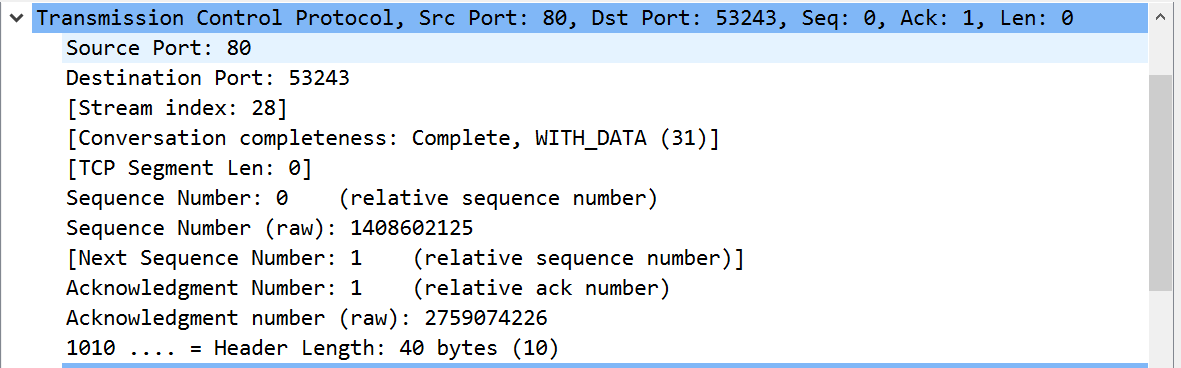
RP5]3R}{6MLC_NA8}]`RG41

TCP端口：

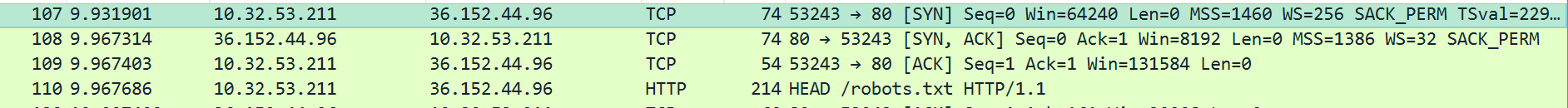
0F}P`T}9L%LAX93IAZHM~B5

1. 用侦听解析软件观察TCP机制

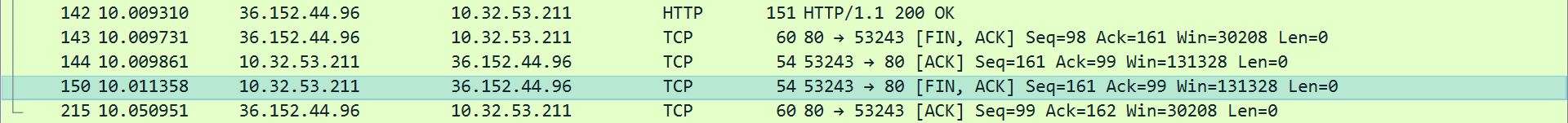
TCP数据段：



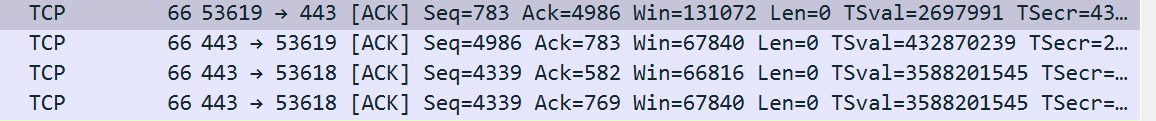
TCP三次握手：

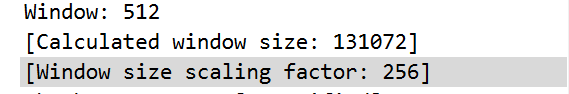


TCP四次挥手：



TCP窗口机制：





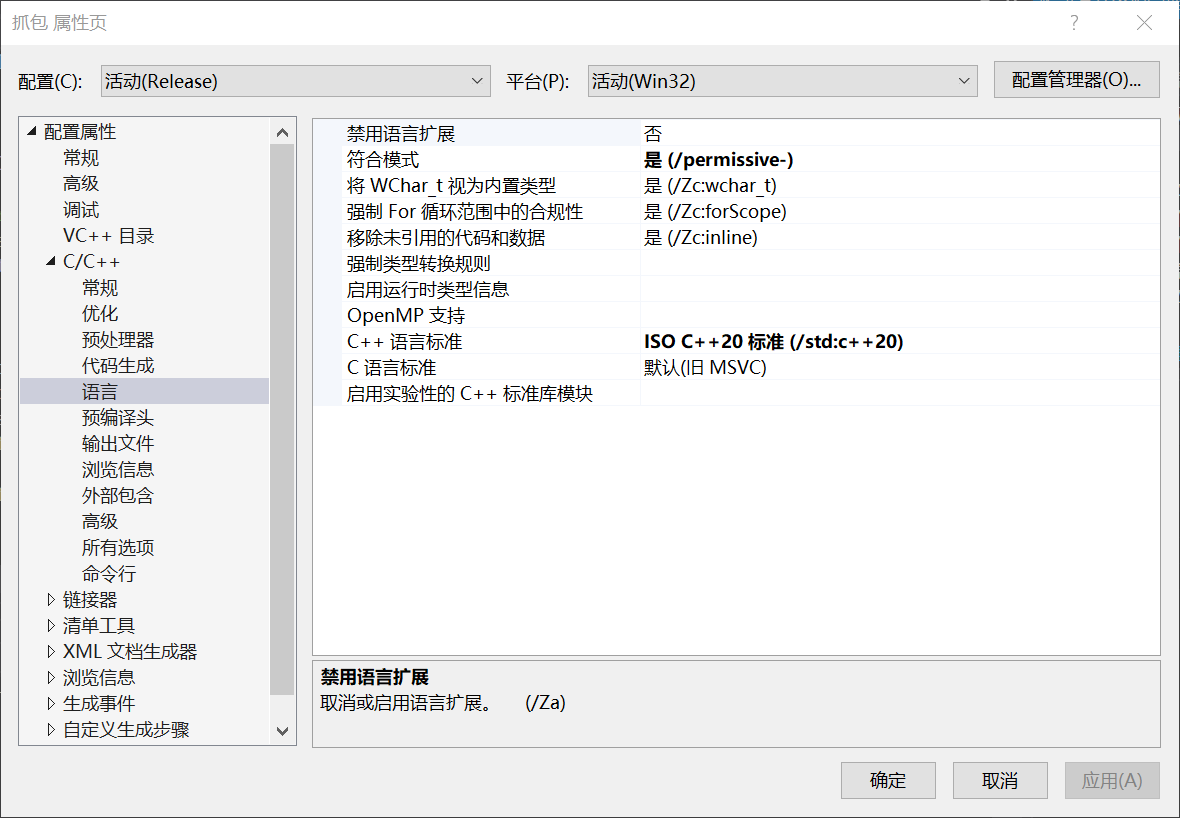
TCP拥塞控制机制：

当接收窗口所设定的速率无法使服务器正常处理数据时即出现拥塞时，能够调整接收窗口大小来减小数据传输速率。通过减小返回给发送端的ACK报文的TCP头窗口大小值来实现。在发生分组丢失的极端情况下，TCP会暂时将窗口大小减为当前值的一半。

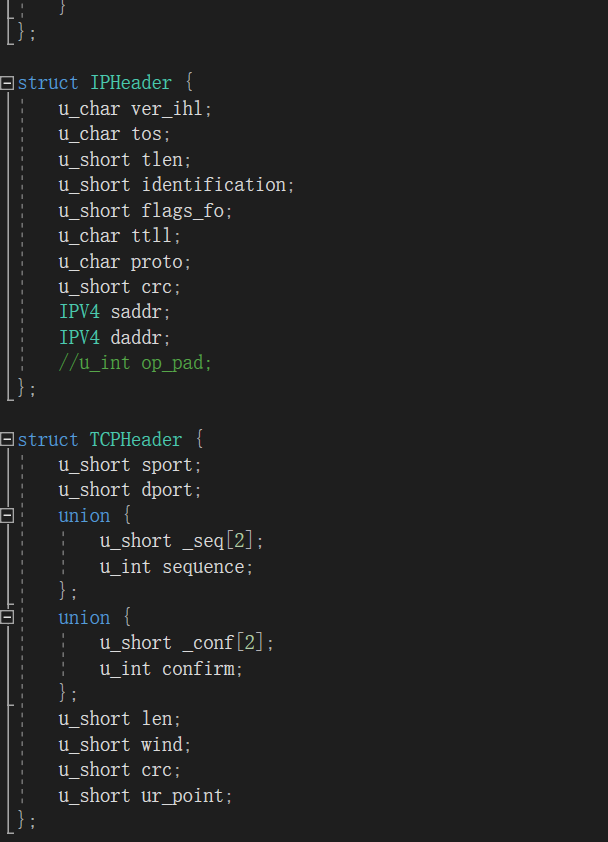
1. 用WinPcap侦听网络数据

环境配置：

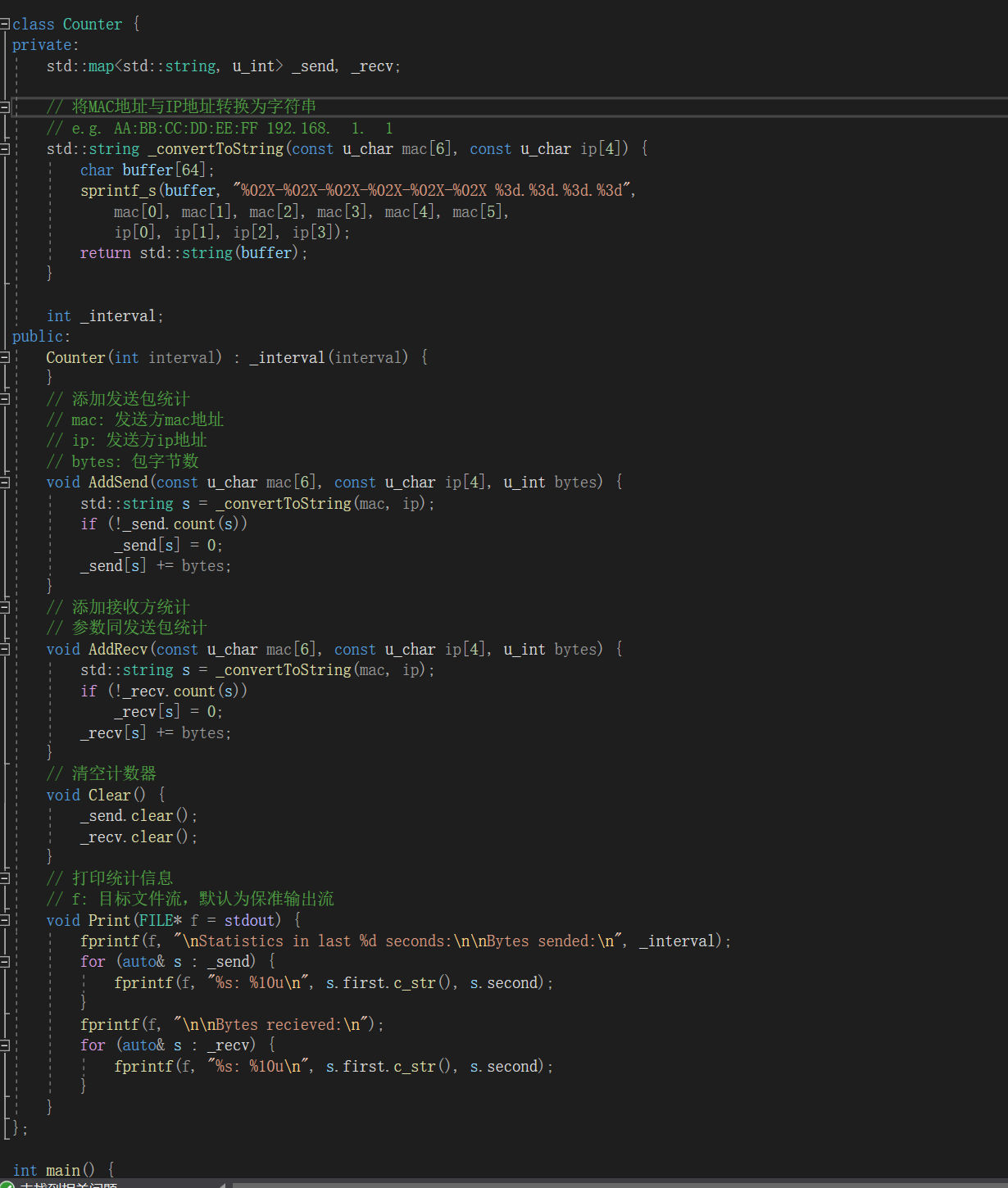
首先先将npcap文件夹下的include和lib连接到项目。记得选择C++语言标准为17版本及以上，否则将会报错。（因为后面采用了一点新标准的语法）

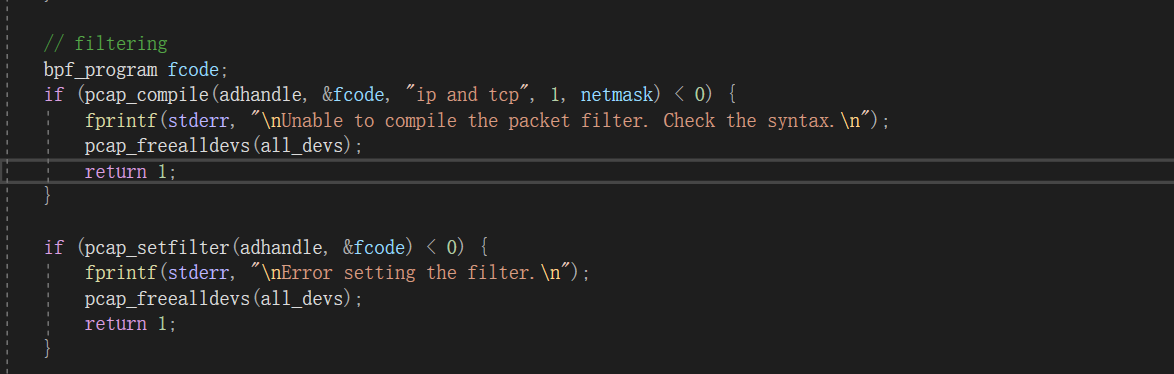


创建以太网报头、IP报头、TCP报头格式

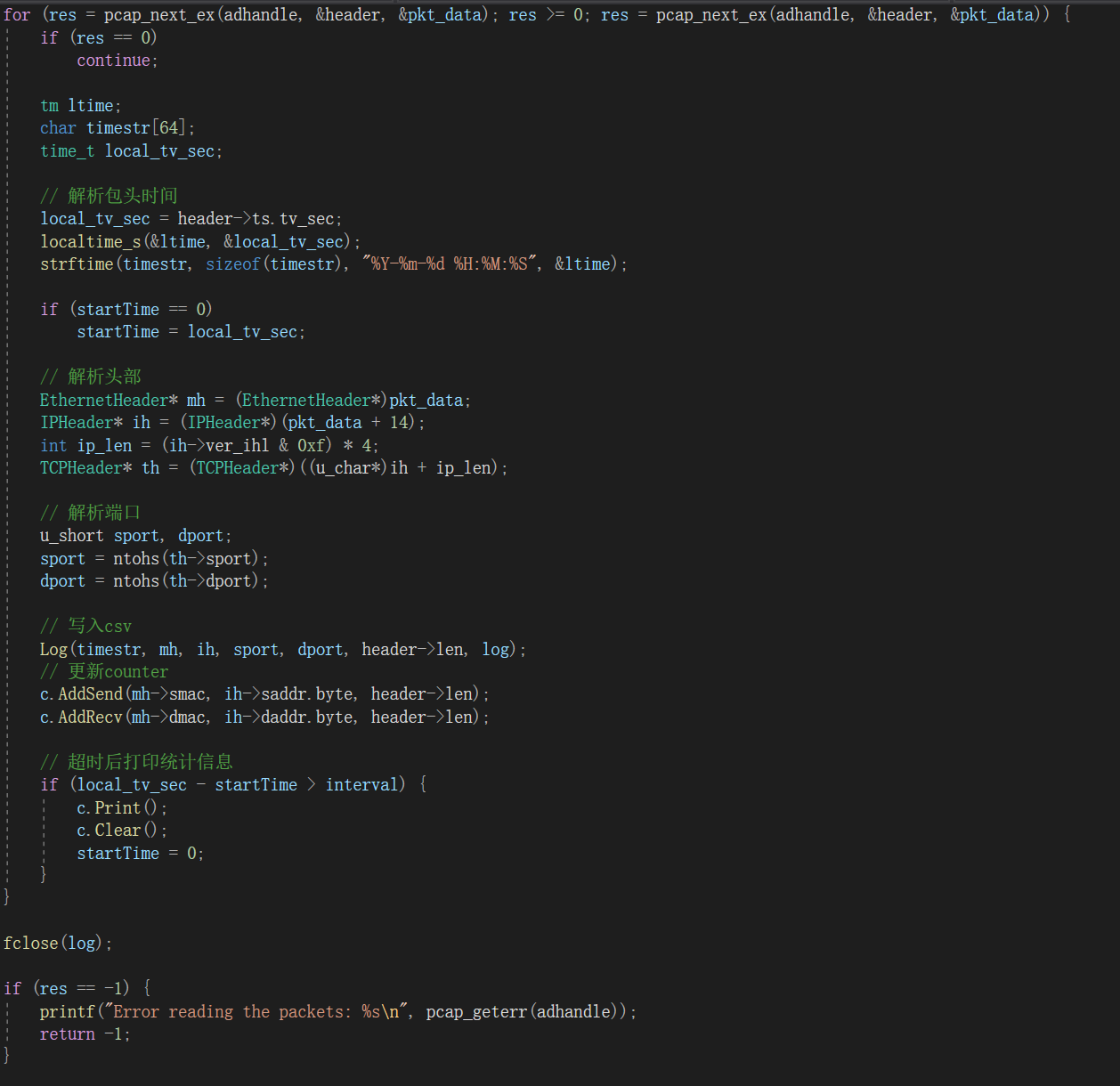


创建计数器类用于统计数据，将MAC地址与IP地址转换为字符串作为map的key用于统计一段时间内来自某一IP的包总长度。分别统计接收方与发送方，接着每五秒将统计信息打印出来。

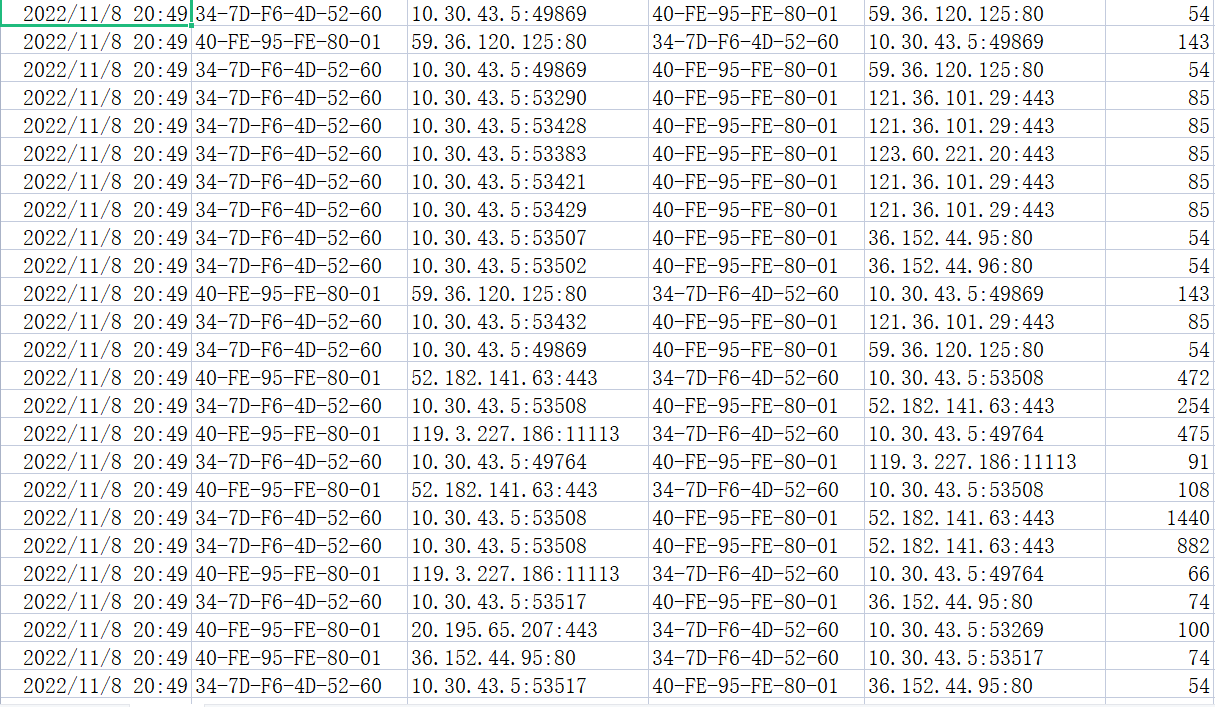
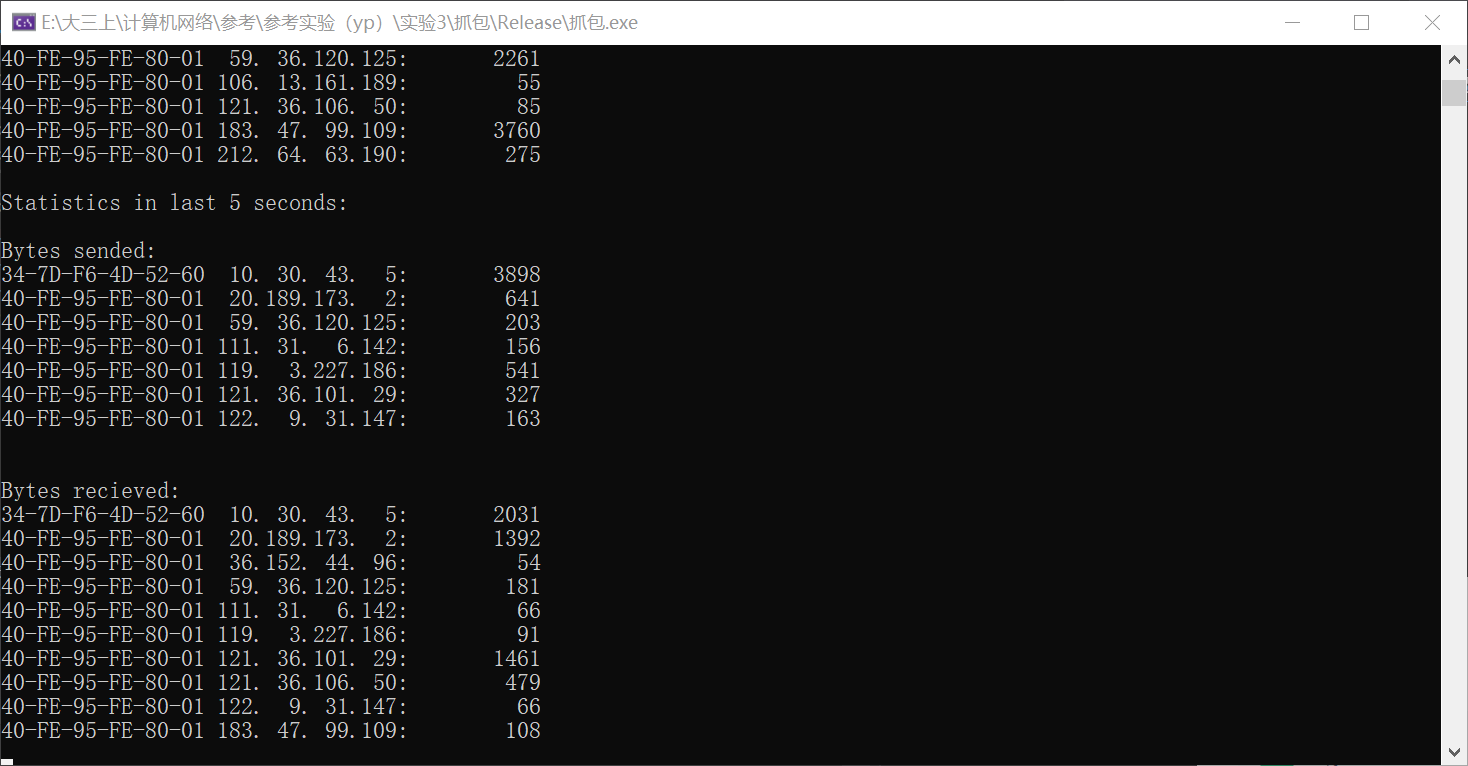


接着先获取adapters，选择合适的adapters，并设置过滤器为“ip and tcp”，

处理捕获到的TCP包，先解析包头时间，头部，端口。接着将解析的数据写入csv，同时更新counter。添加超时处理。



运行效果：



1. 解析侦听到的网络数据

前面步骤与3同

创建FTPlogin类，用于记录完整的一次FTP登录，包括使用的用户名，密码以及结果。最后将登录信息输出到文件流f。

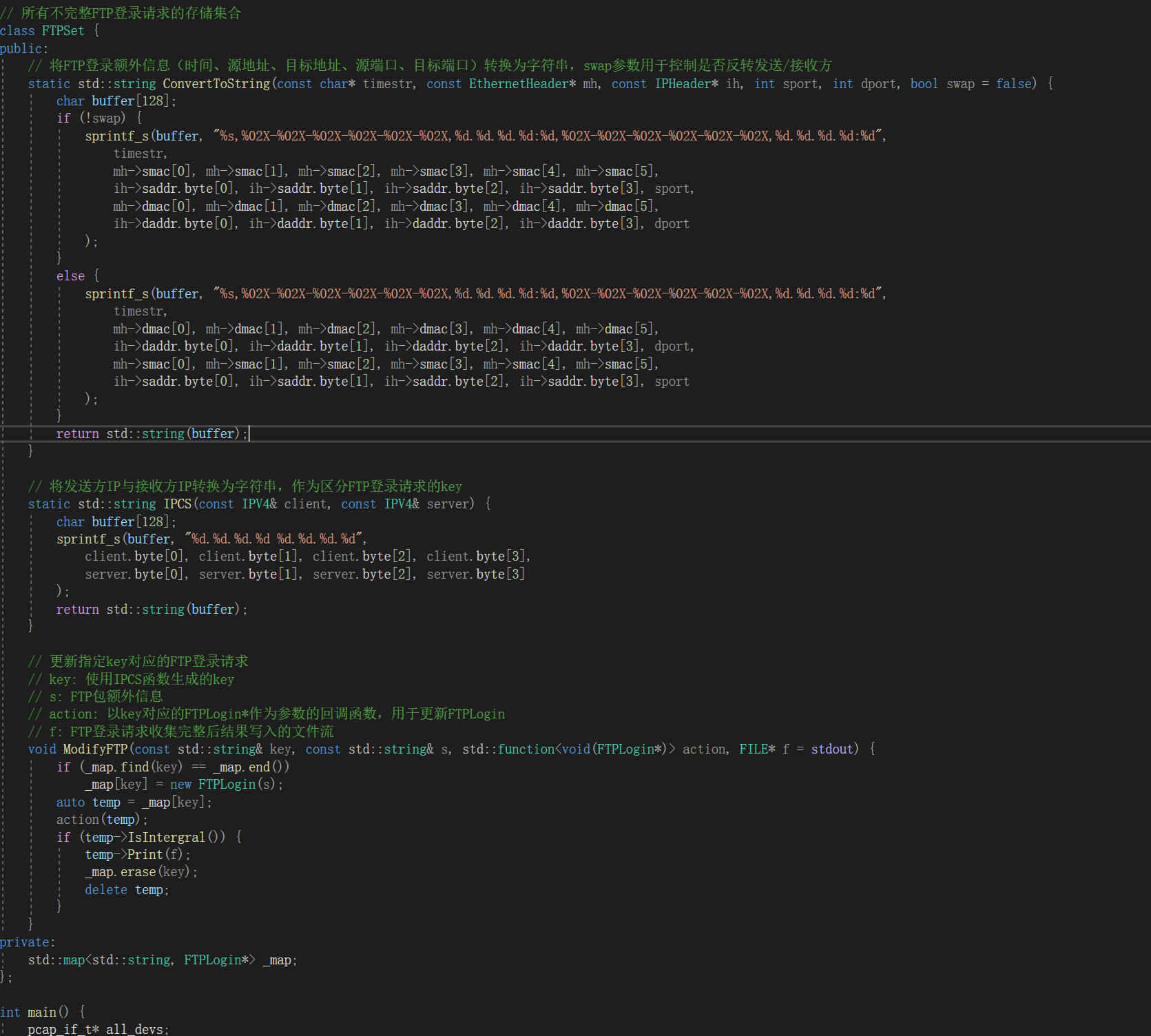


创建FTPSet类记录所有不完整FTP登陆请求的存储集合

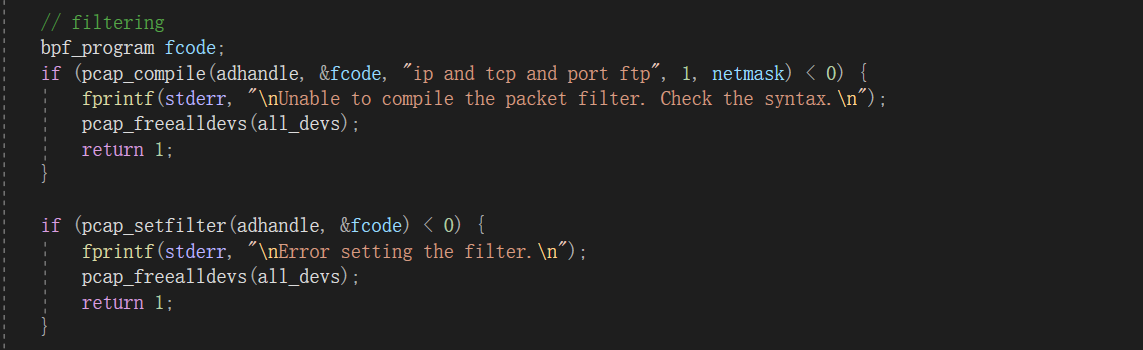
首先将FTP登录额外信息（时间、源地址、目标地址、源端口、目标端口）转换为字符串，swap参数用于控制是否反转发送/接收方

IPCS函数将发送方IP与接收方IP转换为字符串，作为区分FTP登录请求的key

ModifyFTP函数更新指定key对应的FTP登录请求



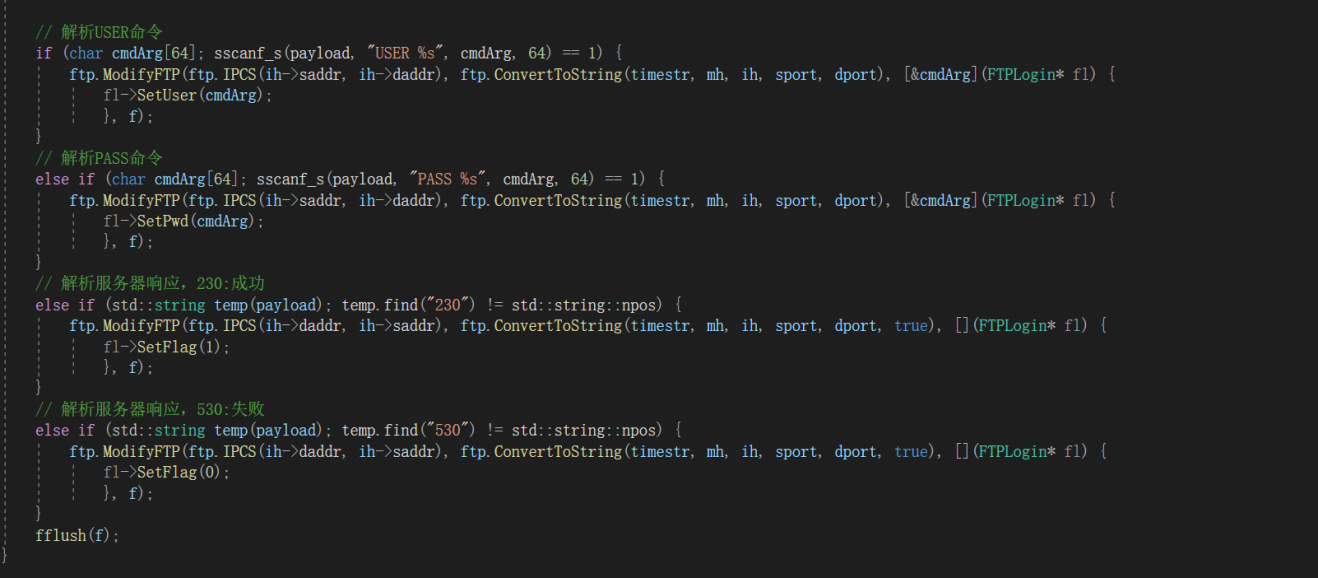
其他步骤与TCP类似，只是需要更改过滤器为“ip and tcp and port ftp”



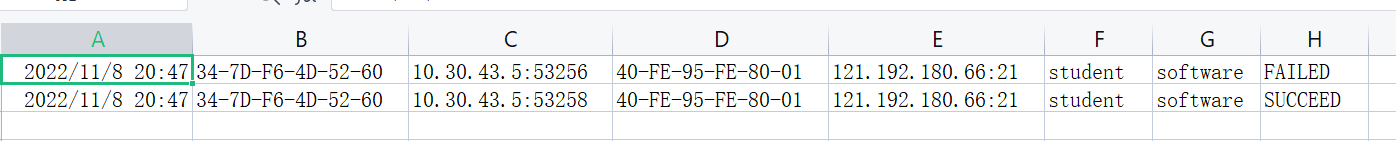
利用包长度、以太报头长度、IP报头长度、TCP报头长度来计算载荷长度

{7`AIN95JK[}IIC__DTM8@4

最后依次解析USER，PASS命令以及服务器响应。此处if语句使用了C++17新语法。



运行结果：



# 实验代码

本次实验的代码已上传于以下代码仓库： https://gitee.com/Cutie\_Chen/computer-network/tree/master/3

# 实验总结

通过捕获并分析以太网帧，分析常见数据包的帧格式，熟悉以太网中常用协议，数据包在网络中的发送方式、各报头的作用；

学会了用Wireshark侦听网络数据。