

****

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2019级1班**

**姓　　名 姬颖超**

**学　　号 22920192204218**

**实验时间 2021年4月2日**

**2021 年 4 月 2 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，勿超过5MB；
4. 应将材料清单上传在代码托管平台上；
5. 在学期最后一节课前按要求打包发送至cni21@qq.com。

# 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 10；

编程语言：C++；

软件：Winshark，VS2019+WinPcap。

# 实验结果

3.1 用侦听解析软件观察数据格式

（1）登录FTP时，WinShark捕获的数据

捕获的数据含义：

No.：捕获数据的编号；

Time：捕获数据的相对时间，从开始捕获算为0.000秒；

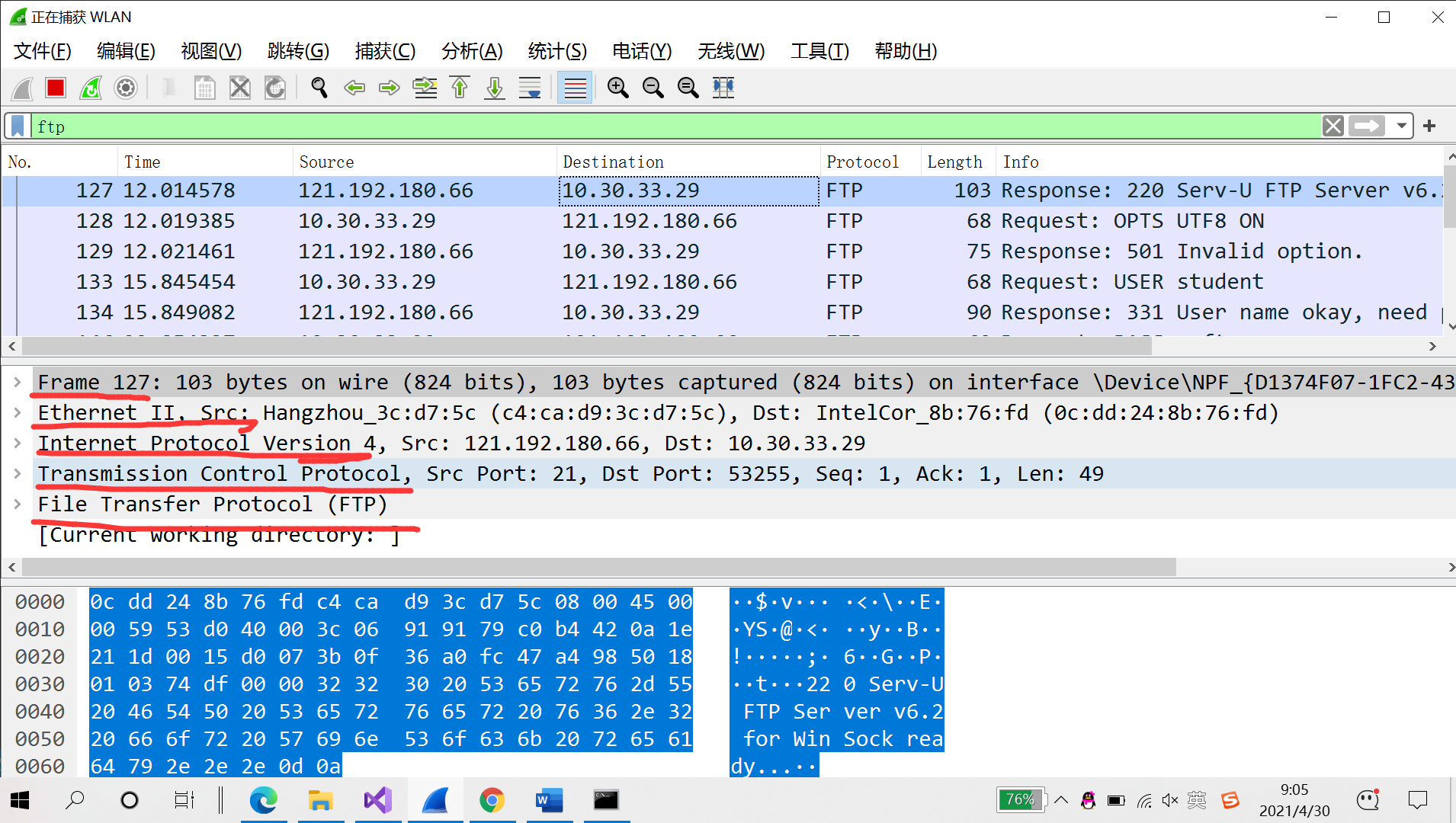
Source：源地址；

Destination：目标地址；

Protocol：协议信息；

Info：数据包的信息。

截图：



Frame：物理层的数据帧概况。

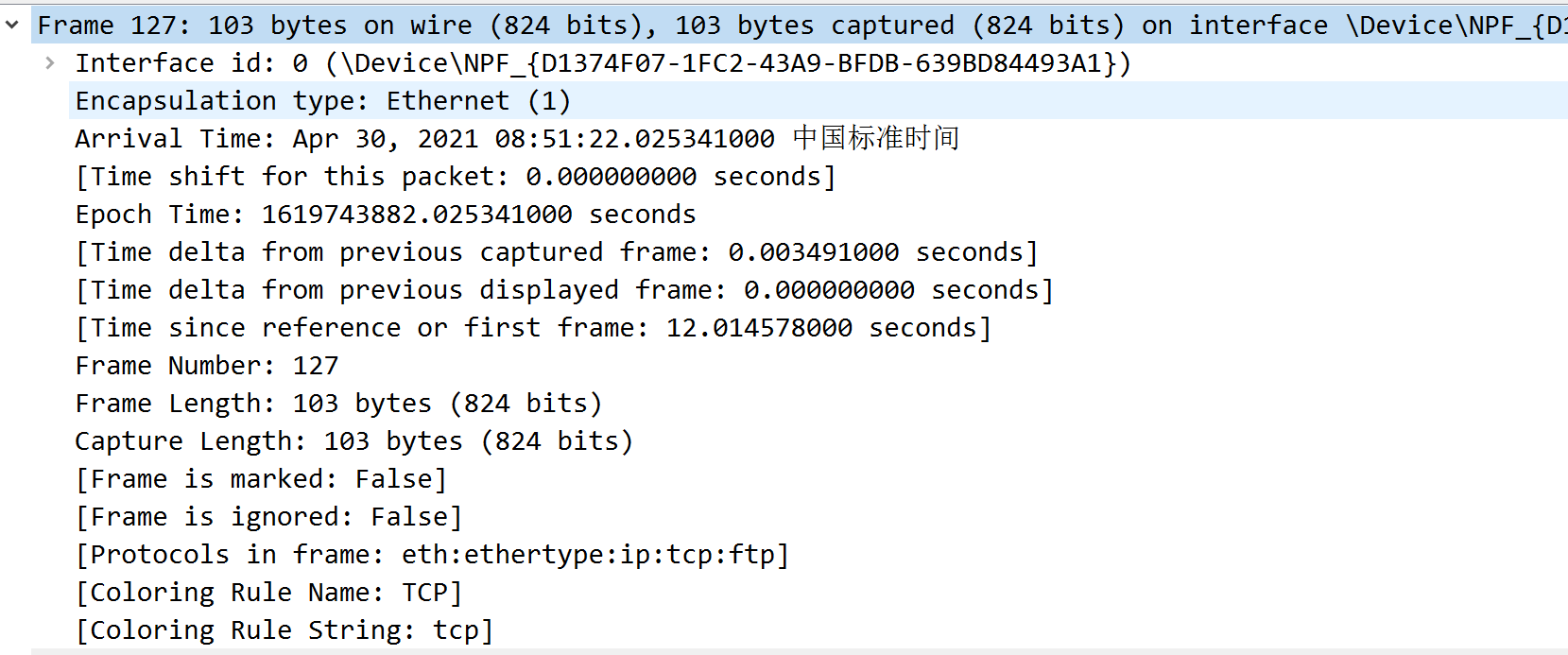
Ethernet II：数据链路层以太网帧头部信息。

Internet Protocol Version 4：互联网层IP包头部信息。

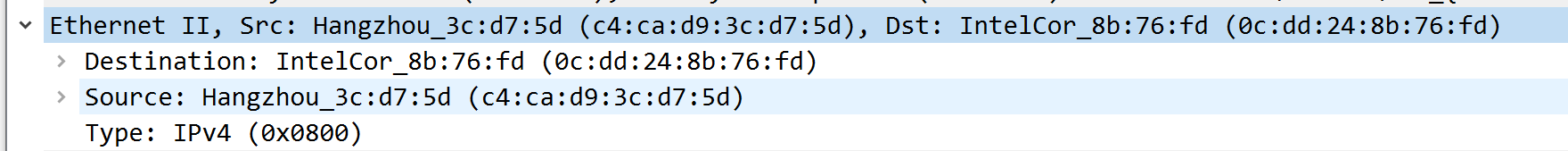
Transmission Control Protocol：传输层的数据段头部信息，此处是TCP协议。

Hypertext Transfer Protocol：应用层的信息，此处是HTTP协议。

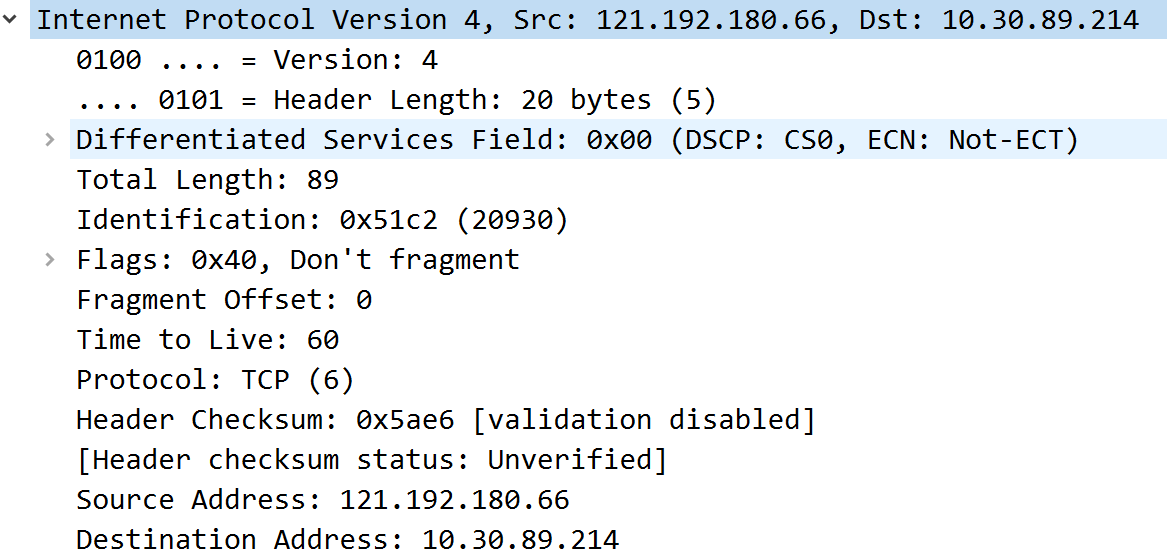
（2）物理层的数据帧头部信息



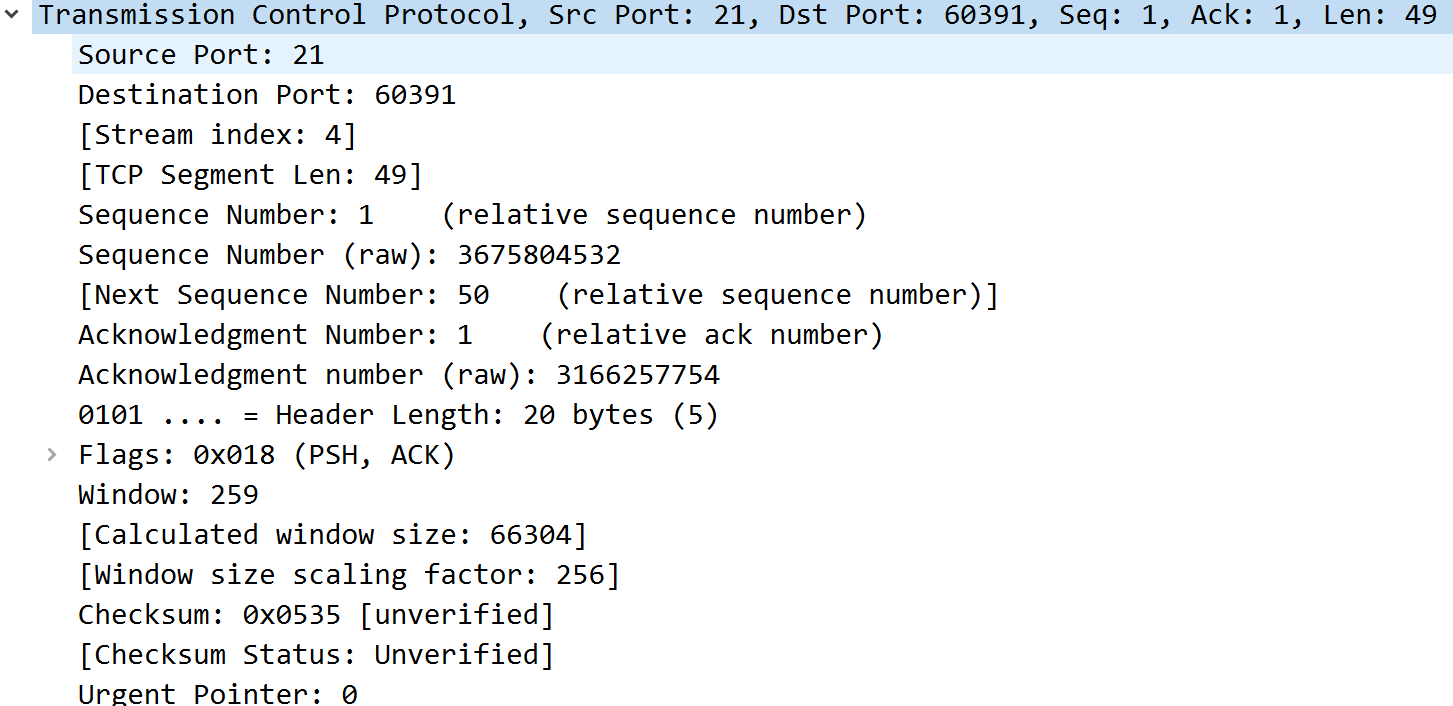
（3）数据链路层的以太网头部信息



（4）网络层Ip头部信息

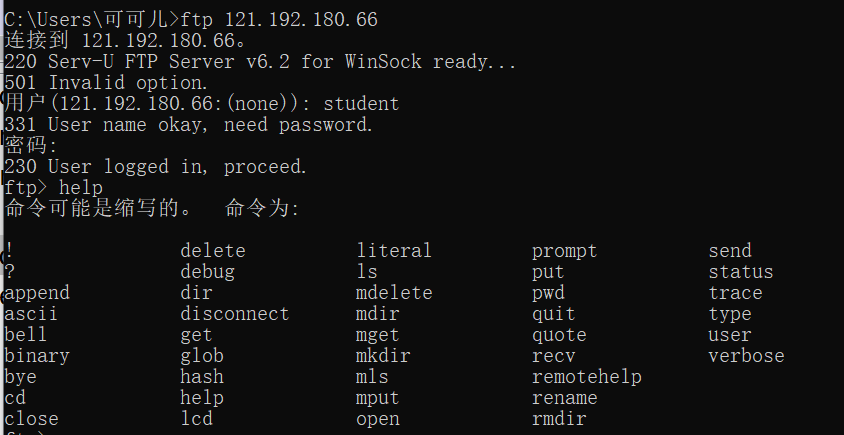


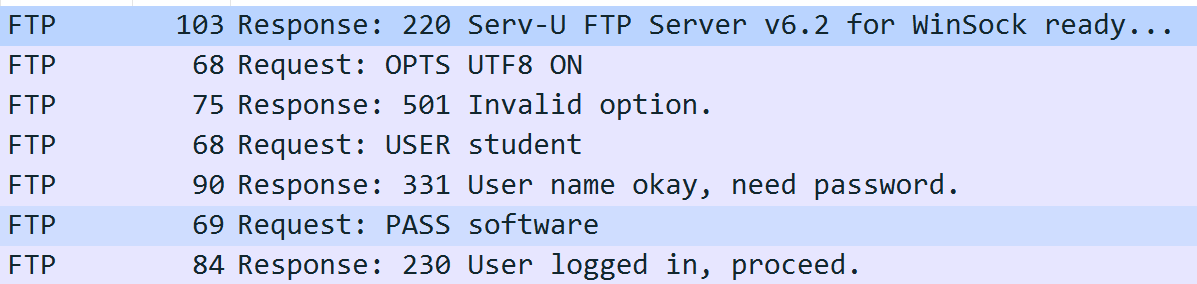
（5）传输层的TCP协议



（6）应用层的ftp协议

命令和响应：





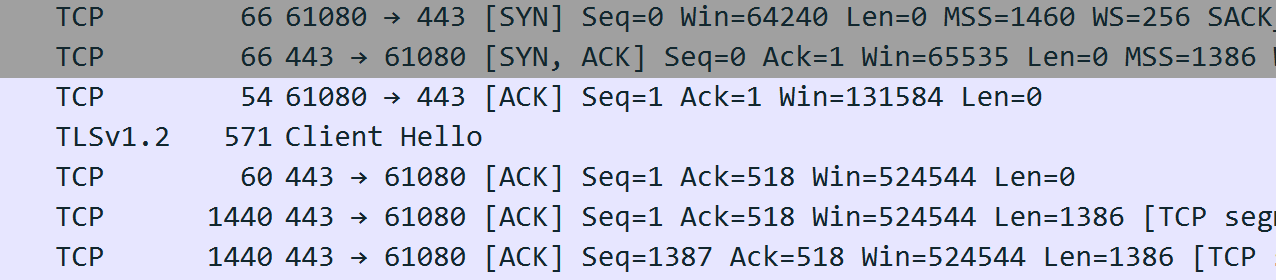
3.2用侦听解析软件观察 TCP 机制

用 Wireshark 侦听并观察 TCP建立和撤除连接的过程

第一次握手数据包：客户端发送一个TCP，标志位为SYN，序列号为0， 代表客户端请求建立连接，如下图所示（第一条）：

第二次握手的数据包：服务器发回确认包, 标志位为 SYN,ACK. 将确认序号(Acknowledgement Number)设置为客户的I S N加1以.即0+1=1，如下图所示（第二条）：

第三次握手的数据包：客户端再次发送确认包(ACK) SYN标志位为0,ACK标志位为1.并且把服务器发来ACK的序号字段+1,放在确定字段中发送给对方。在进过三次握手后和服务器建立了TCP连接，如下图所示（第三条）：



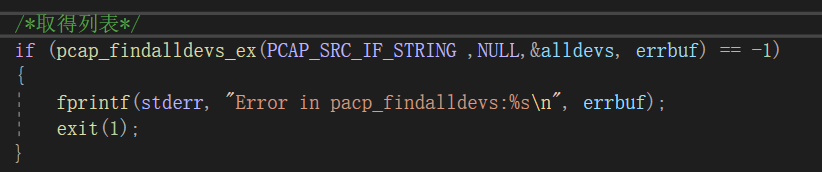
3.3 用 Libpcap 或 WinPcap 库侦听网络数据

（1）VS与WinPcap环境配置

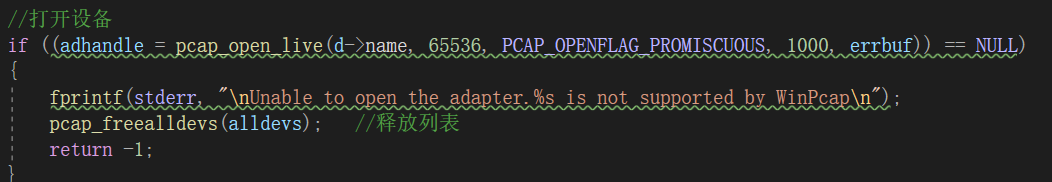
https://blog.csdn.net/qq\_17242957/article/details/50954412

（2）关键代码：

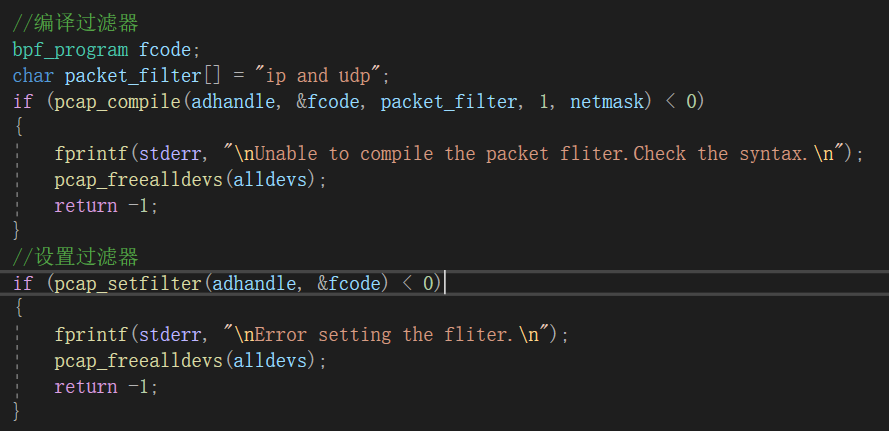
a. 获取设备列表



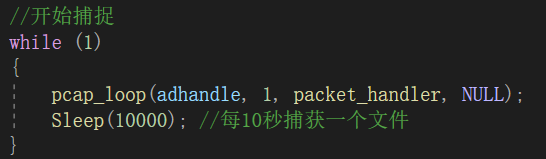
b. 打开设备



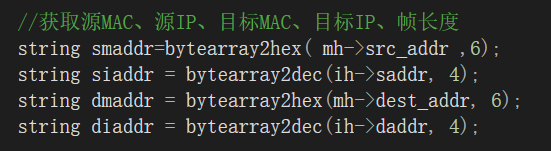
c. 编译设置过滤器



d. 捕获数据

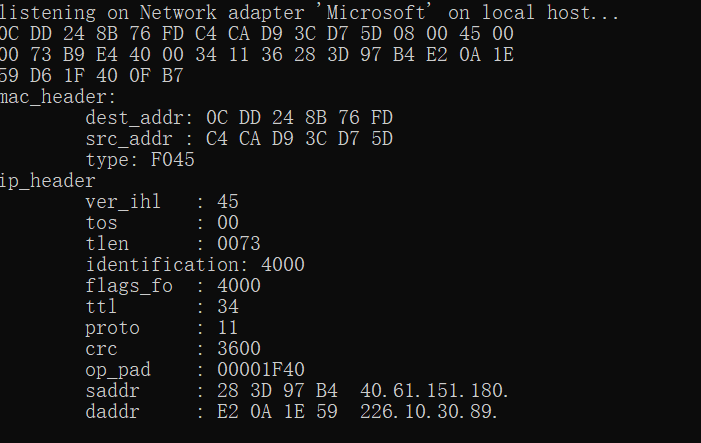


e. 处理数据

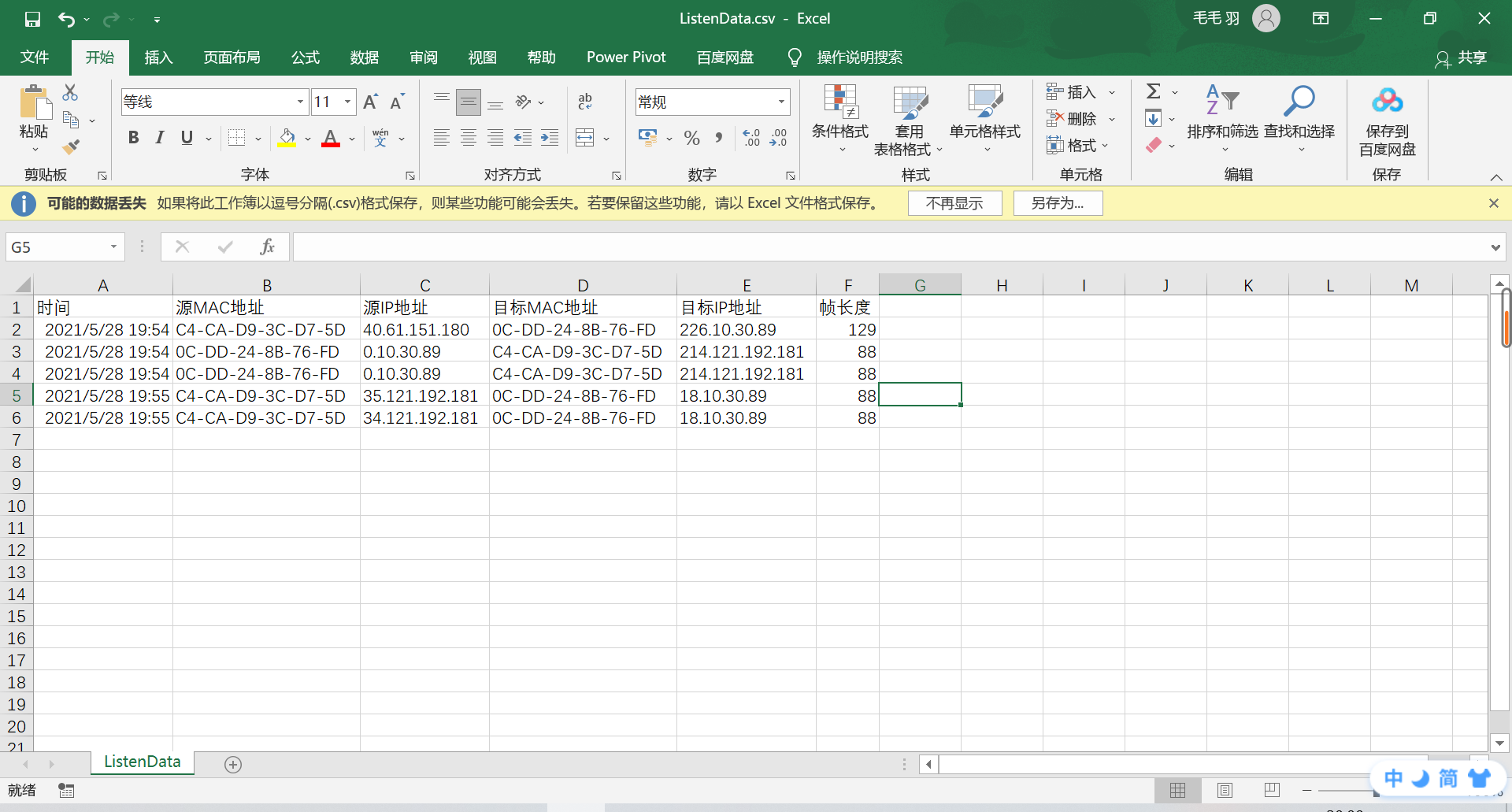


（3）实验结果

控制台的输出数据：



csv文件的数据（每十秒捕获一个包）：



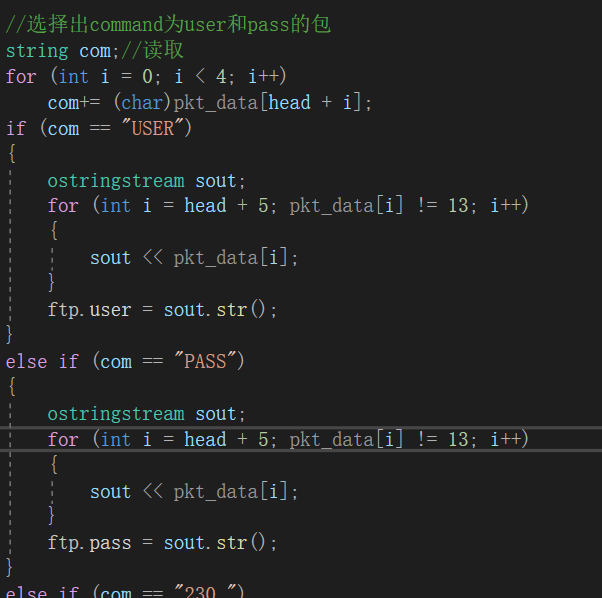
3.4 解析侦听到的网络数据

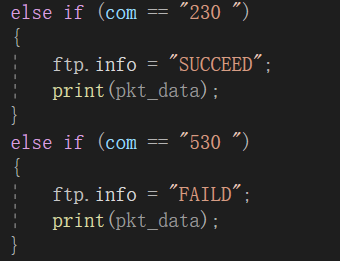
（1）用户名、密码所在报文的特征

一般登录名以“USER”开头，口令以“PASS”开头，登录成功以“230”开头，失败以“530”开头。

（2）关键代码：

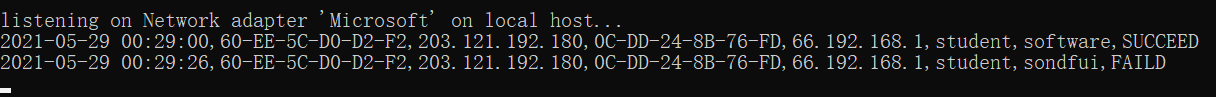
提取用户名和密码以及成功与否的信息：



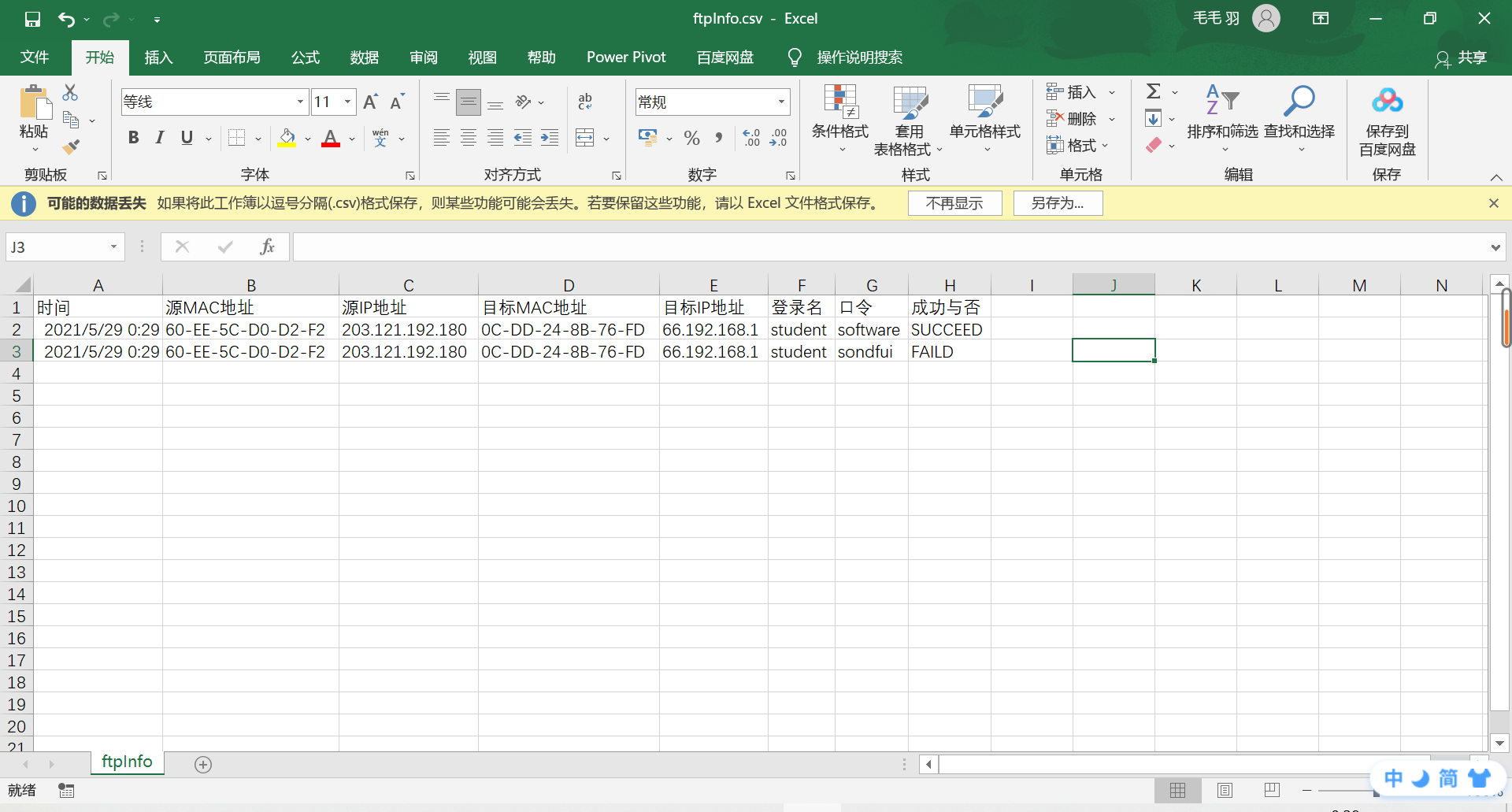


（3）结果

控制台输出：



csv文件：



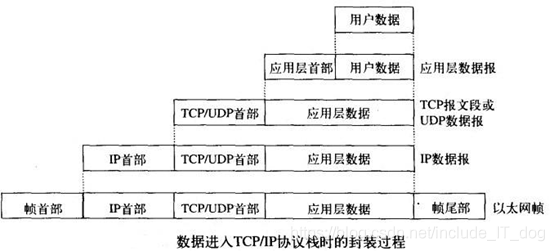
# 实验代码

本次实验的代码已上传于以下代码仓库：

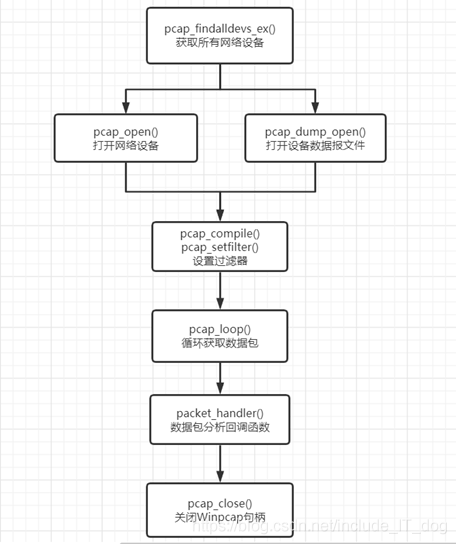
https://github.com/ikekeer/ComputerNetwork/tree/main/E3\_4218

# 实验总结

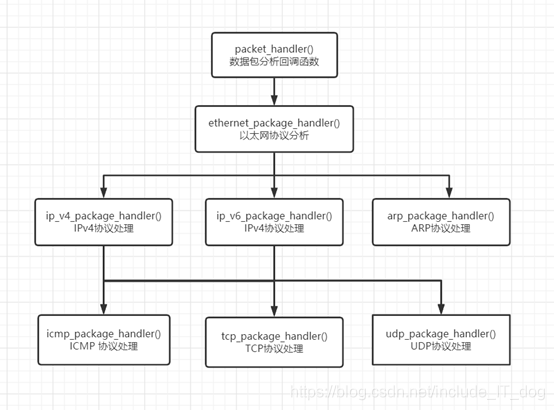
（1）通过使用WinShark捕获数据，进一步熟悉了以太网帧、IP报文、TCP段等头部各字段的含义。理解数据封装过程：



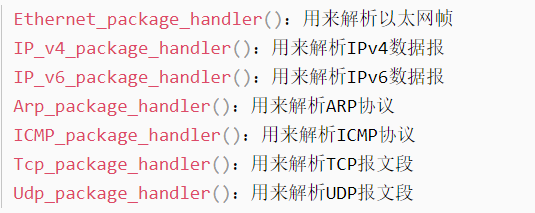
（2）学习了Winpcap系统的处理流程：



协议分析流程：



（3）接触到解析各协议的函数：



（4）编写解析IP报文、TCP报文段、以及FTP报文的程序。