

****

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 数字媒体技术2022级1班**

**姓　　名 魏清晨**

**学　　号 37220222203790**

**实验时间 2024年10月11日**

**2024年10月11日**

填写说明

1. 本文件为Word模板文件，建议使用Microsoft Word 2021打开，在可填写的区域中如实填写；
2. 填表时勿改变字体字号，保持排版工整，打印为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

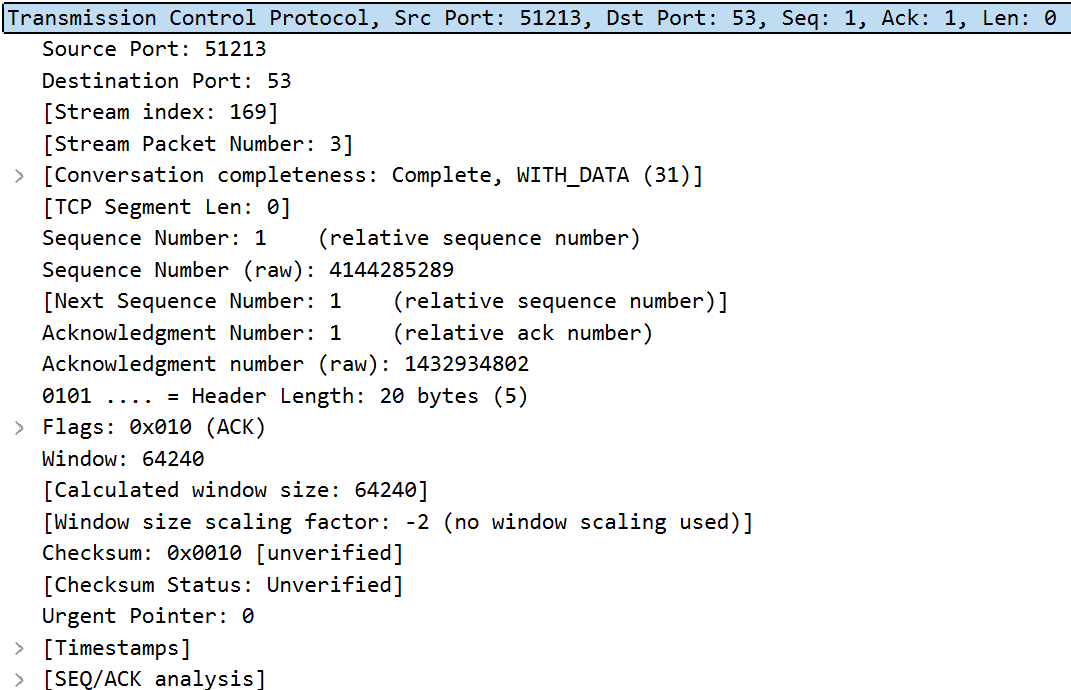
操作系统：Win11 编程语言：C++ 调试软件：CLion2023.2

# 实验结果

1. 用侦听解析软件观察数据格式
2. 网络协议层次嵌套

对于一段数据帧，它包含多个部分，包括上层数据、TCP头部、IP头部、MAC头部，在每一个层级中，每个头部和剩余部分为一个整体，如在应用层只有上层数据，在传输层由TCP头部和上层数据组成**数据段**，在网络层由IP头部和数据段组成**数据包**，在数据链路层由MAC头部和数据包组成**数据帧。**

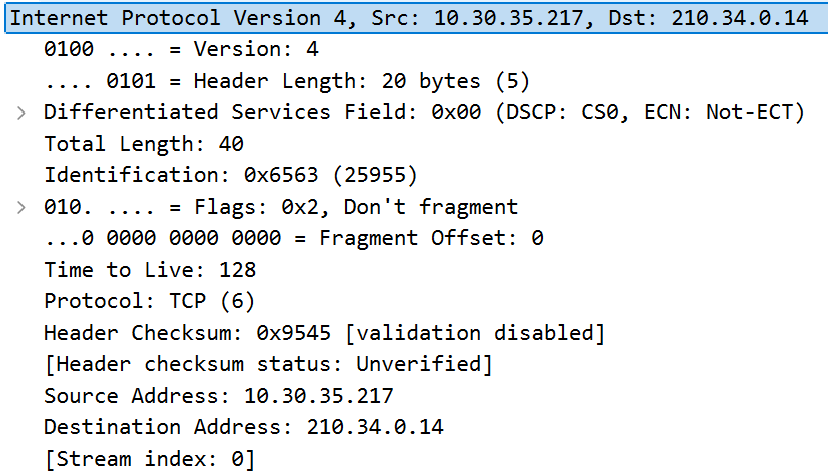
1. TCP段格式



应用层数据前就是TCP，这里TCP头部有20位，具体来讲

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 源端口号 | 目标端口号 | 序列号 | 确认序列号 | TCP头部长度 | 标志位（此处有效的为9个） | 窗口 | 校验和 | 紧急指针 |
| 16位 | 16位 | 32位 | 32位 | 4位 | 12位 | 16位 | 16位 | 16位 |

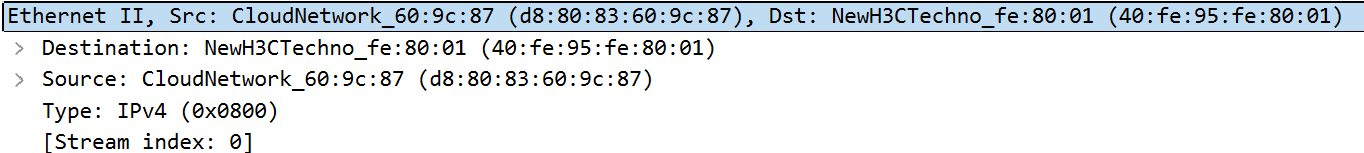
1. IP 报文格式



TCP头部前就是IP头部，有20个字节，具体来讲如下

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 版本 | IP包头部长度 | 差分服务字段 | IP包总长度 | 标识字段 | 标记字段 | 分片偏移 | 存活时间 | 协议 | 校验和 | 目的地址 | 源地址 |
| 4位 | 4位 | 8位 | 16位 | 16位 | 3位 | 13位 | 8位 | 8位 | 16位 | 32位 | 32位 |

1. 帧格式



这部分是以太网帧格式中前头部部分，此处可以看到目的地址Destination: NewH3CTechno\_fe:80:01 (40:fe:95:fe:80:01)，源地址Source: CloudNetwork\_60:9c:87 (d8:80:83:60:9c:87)，类型IPv4。

1. MAC 地址、 IP 地址、 TCP 端口

由上述头部可以得到，**源MAC地址**为 NewH3CTechno\_fe:80:01 (40:fe:95:fe:80:01)，目的MAC地址为 CloudNetwork\_60:9c:87 (d8:80:83:60:9c:87)

**源IP地址**为Source Address: 10.30.35.217，目的IP地址为Destination Address: 210.34.0.14

**源TCP端口**为：51212，目的TCP端口为53

1. FTP 协议

此处搭建了一个127.0.0.1的ftp网站

使用cd 1命令后，发送了

响应为



响应格式就是一个响应代码，250就是文件行为完成，后面的info都会被输出到控制台中

此外还有其他响应：

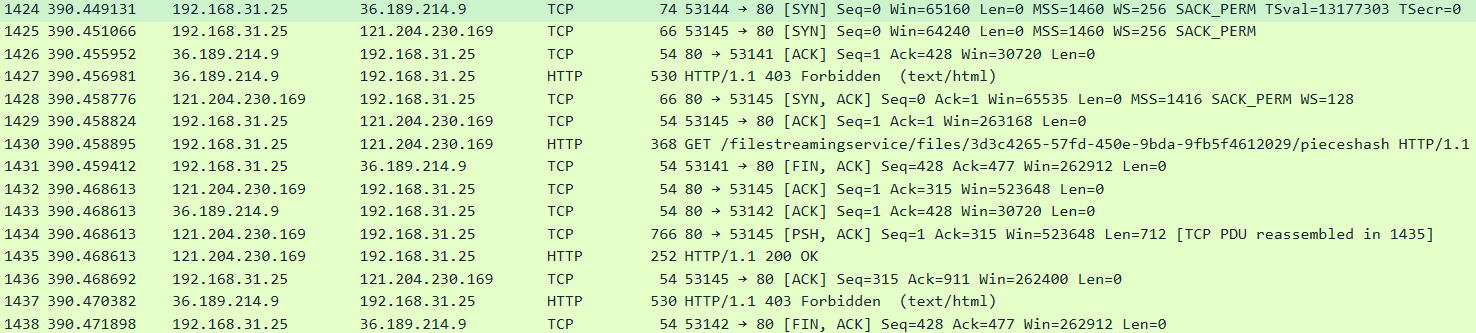








1. 用侦听解析软件观察TCP机制



**关于段ID，涉及到三次握手**

TCP的三次握手，1425、1428、1429就是一次握手的过程，第一次seq=0表示是新的开始，之后第二次收到seq=0，ack=1表示对方要这方从seq=1开始传数据，第三次seq=1响应刚才的包，ack=1表示收到。

然后，1430这一行是客户端发起http的请求，这一帧的长度为314

1432这里服务端发回Ack=314+1=315表示接收成功，但没有数据传回

1434带上了PSH标志字，表示有 DATA数据传输，由ACK可知还是对1430的回复，这时数据长度为712

1435服务端又发了一个http，而且PSH也是1，把把剩下的数据发过来，长度为198

1436表示收到了服务端的数据，应答ACK=911=1+712+198表示前两个数据都收到了

**关于窗口机制**

可以看到WIN字段，这里有的包使用了窗口大小因子对窗口大小进行了放缩，所以WIN的数值很大。

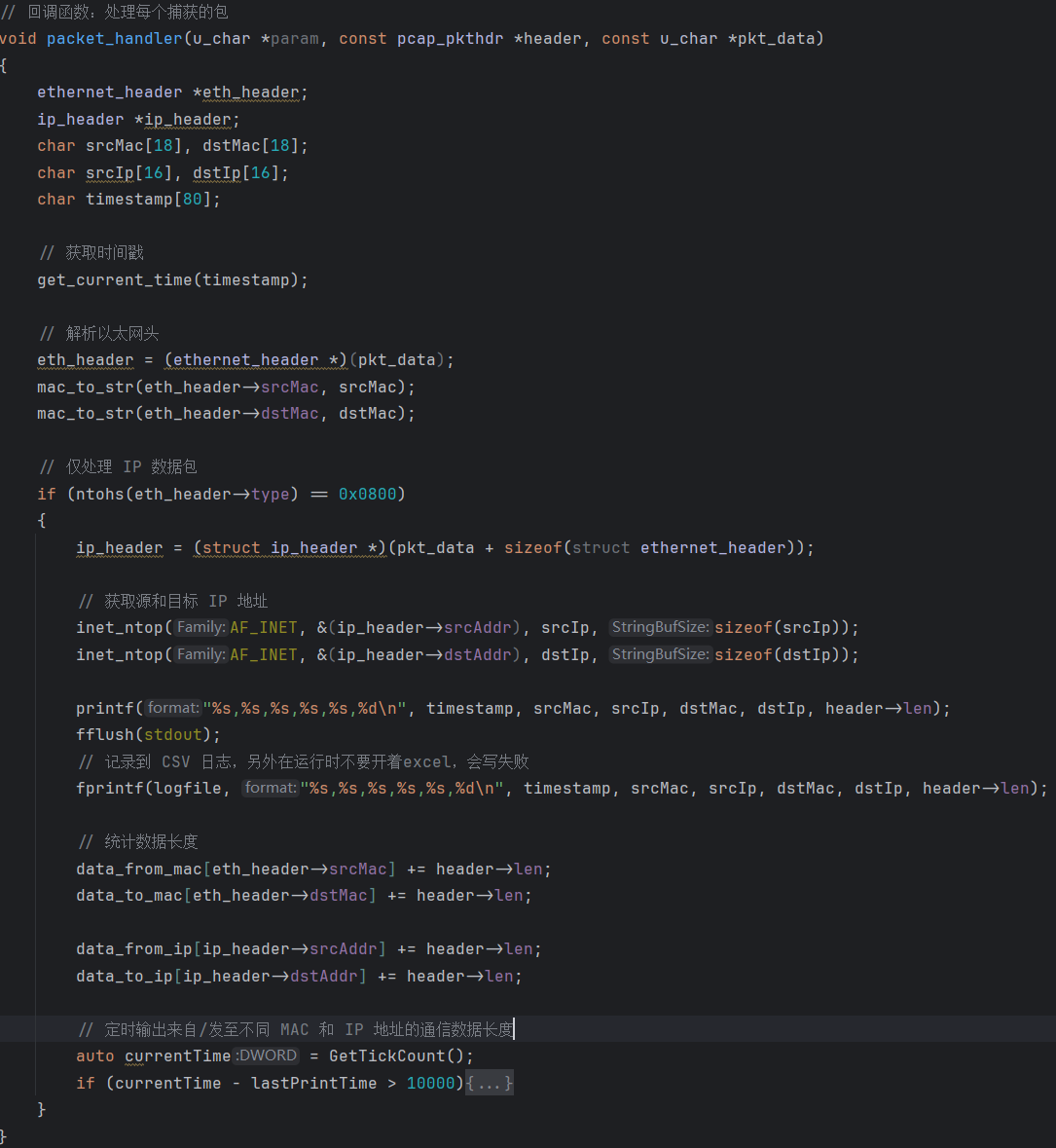
WIN表示发送该TCP报文的接受窗口还可以接受多少字节的数据量，如果已满，就不会再发送，而且就算窗口中间有发送的包获得了回复，也不能移动窗口，只能从两端进行操作

**关于拥塞控制机制**

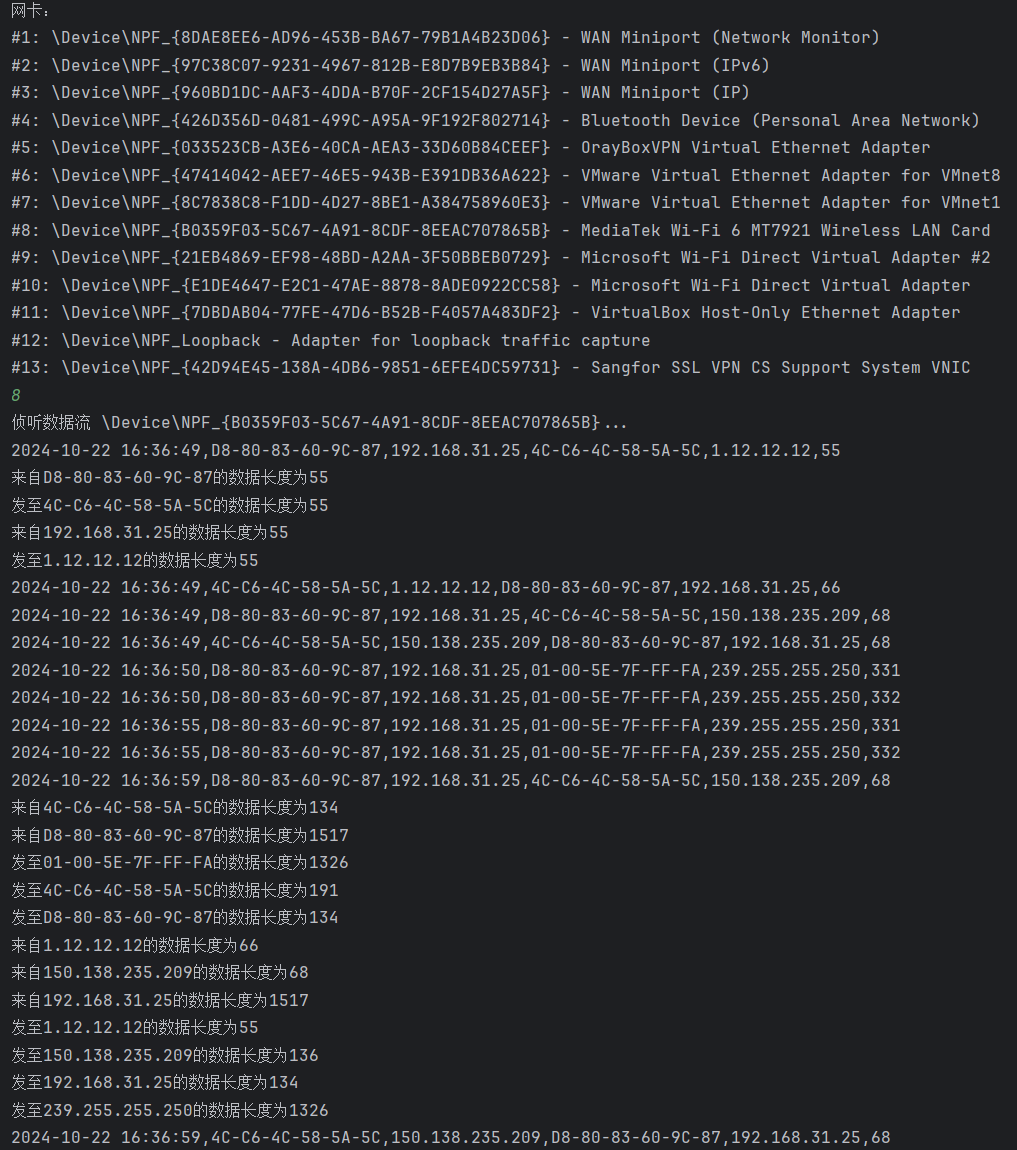
发送方维护cwnd，cwnd不出现在报文中，，使得swnd（发送窗口）等于cwnd，cwnd的维护有两个算法，当cwnd < ssthresh，使用慢开始算法，发送方每收到一个对新报文的确认，使cwnd加一，1到2，2到4，4到8指数增长；当cwnd > ssthresh，使用拥塞避免，限制每个传输轮次，一次只能至多增长1，当发生超时重传时，判断拥塞，令ssthresh的值变为cwnd的一半，所以这个拥塞是动态的拥塞

1. **用 Libpcap 或 WinPcap 库侦听网络数据**

**主要处理侦听到的数据的函数部分：**

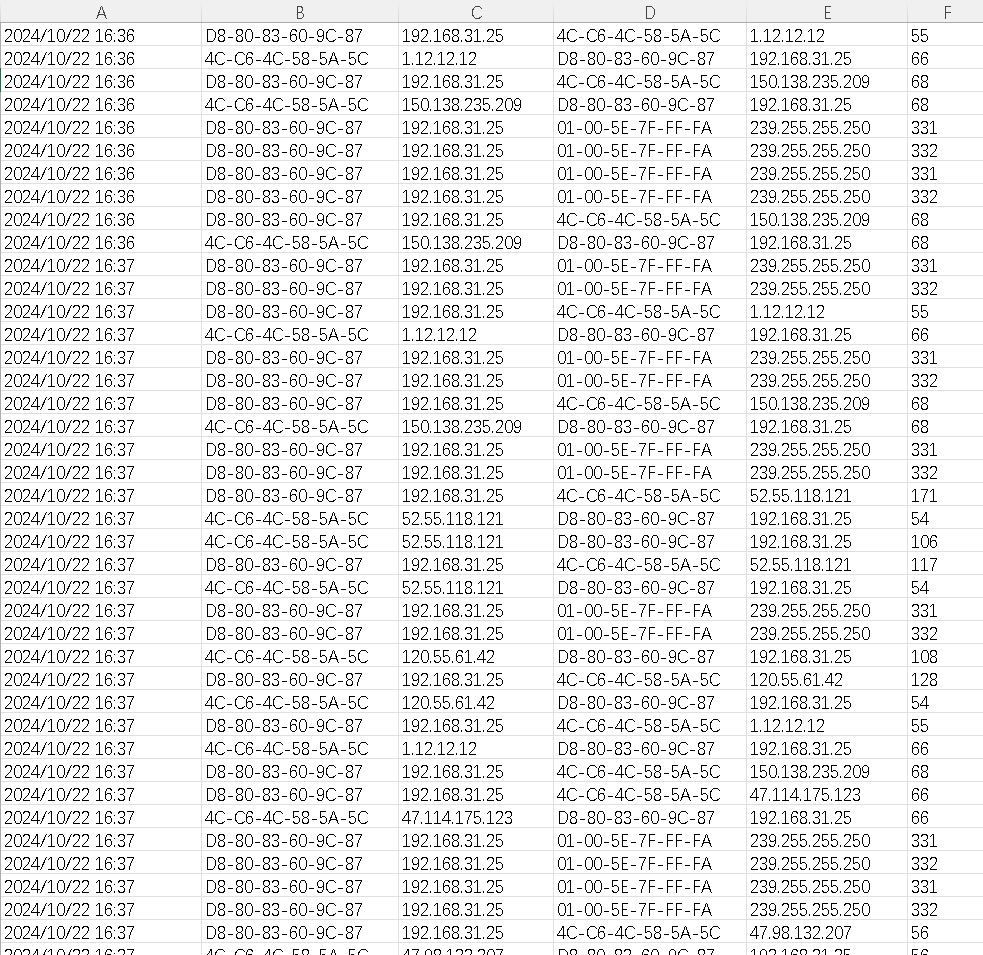


此处设置10秒输出一次统计的收发数据长度



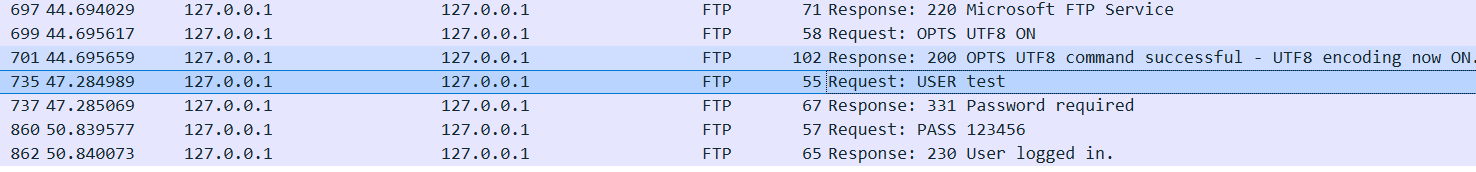
写入csv文件中的数据：

（虽然写入的日期是以“-”相隔，但在csv中不知为何变为了“/”

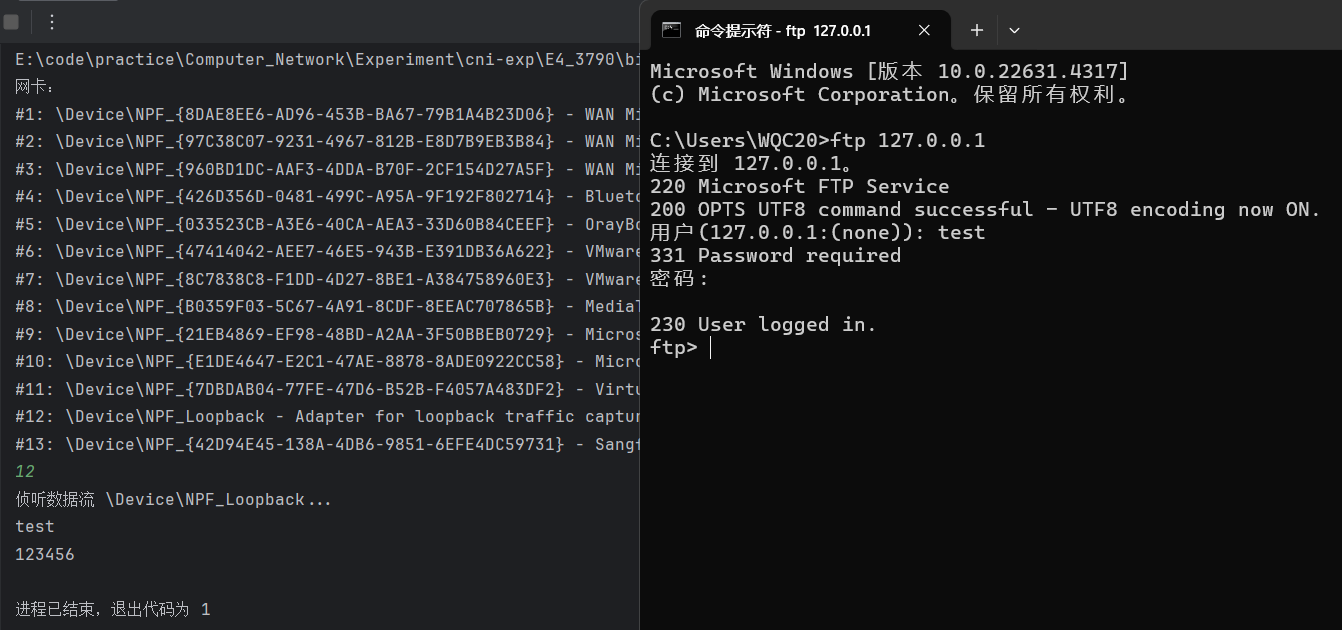


1. 解析侦听到的网络数据

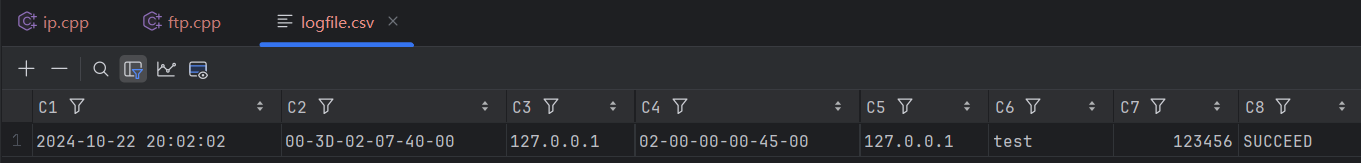
**ftp登录整个流程如下：**



**实验登录ftp流程如下：**

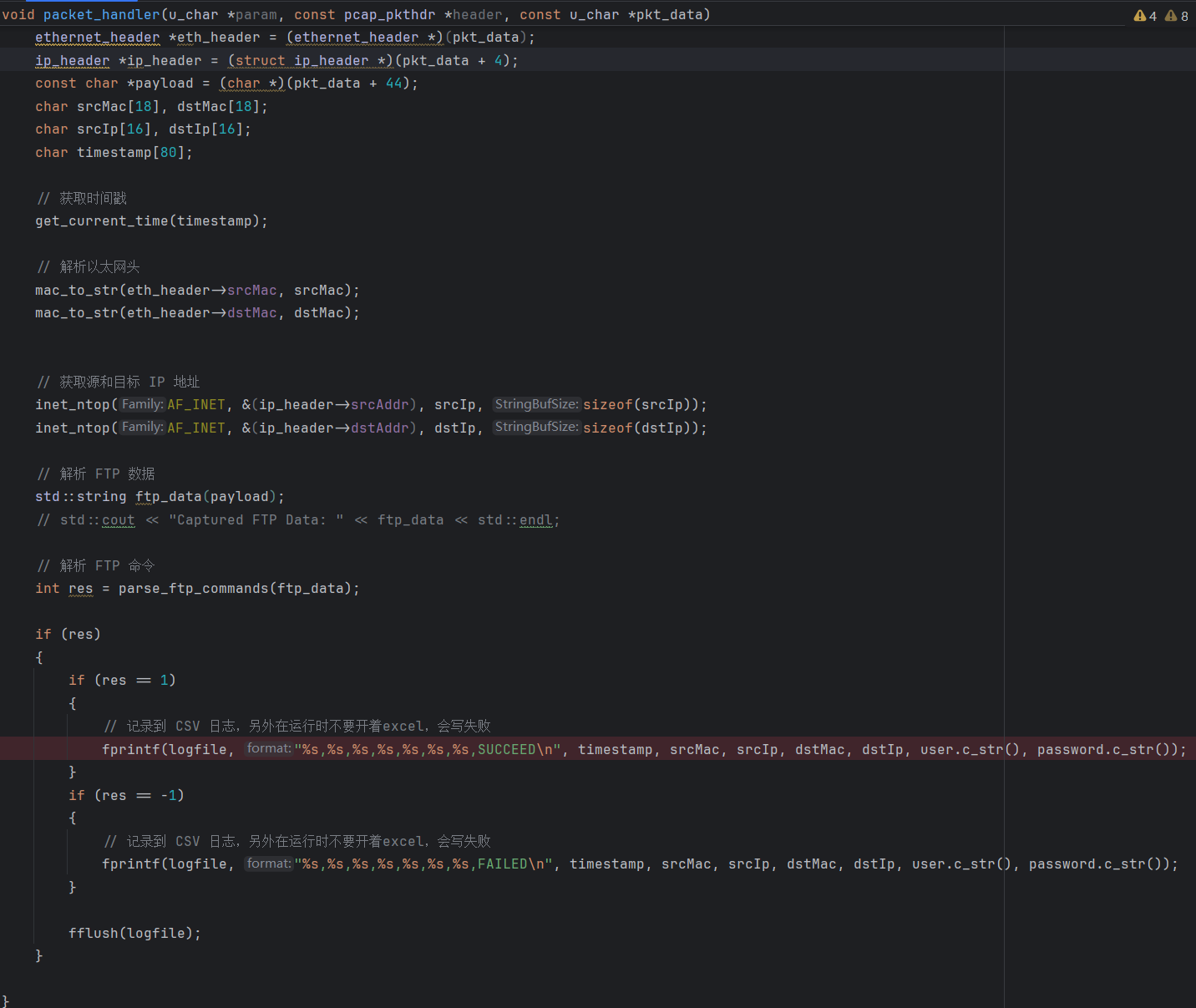


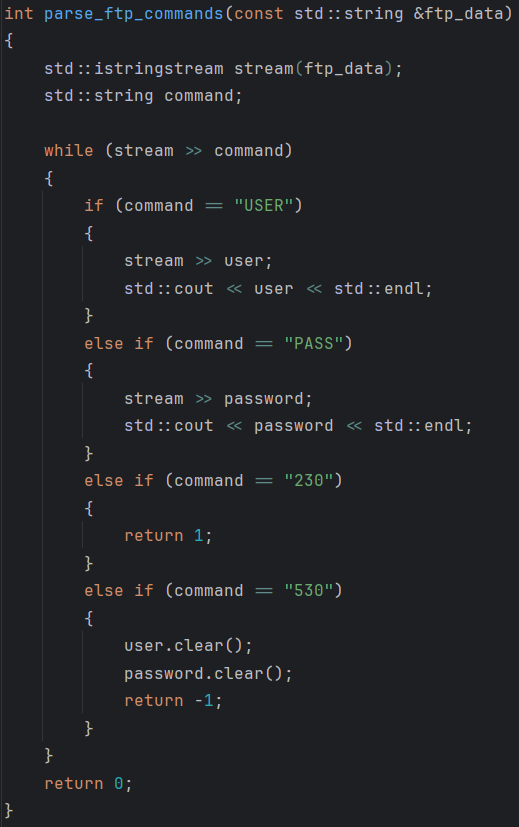
**表格数据：**

****

**主要代码：**

这里以太网帧格式的头部经过wireshark验证只有四个字节，可能是回环数据的原因





# 实验代码

本次实验的代码已上传于以下代码仓库：[CNI-Exp: 厦门大学计算机网络课程实验项目集 (gitee.com)](https://gitee.com/fallingheaven/cni-exp)

# 课后思考题

无课后思考题

# 实验总结

本次实验通过wireshark的使用，一对网络层次协议嵌套有了更好的理解，二对tcp的数据收发机制有了大概的了解，三对ftp的命令格式有了一定的了解

另外，通过npcap库对网络数据的解析，对于接收方解析数据、分析数据有了一定的了解

最后，对于使用本机进行网络上的一些设置，如ftp、防火墙设置等也有了一定的了解。