

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三　用 PCAP 库侦听并分析网络流量**

**班　　级 软件工程2019级1班**

**姓　　名 陈栋**

**学　　号 22920192204171**

**实验时间 2021年3月19日**

**2021 年 3 月 19 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

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

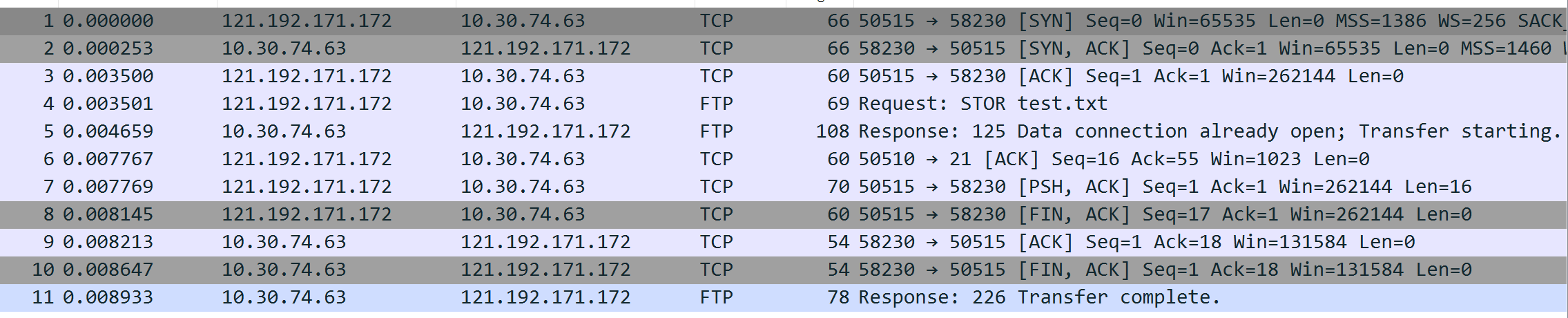
熟悉 TCP 段和 FTP 数据协议的概念，熟悉段头部各字段和 FTP 控制命令的指令和数据的含义

# 实验环境

Window10 \c语言\java

# 实验结果

1、自己创建ftp，传输数据到ftp上，观察tcp报文机制：

****

**通过学校实验室机房，向本机搭建的ftp上传输文件，学校机房（客户端）端口号以121开头，本机（服务器）端口以10开头**

**1.1tcp三次握手：**

**第一次握手：建立连接时，客户端发送syn包（syn=1）到服务器，并进入syn\_sent状态，等待服务确认；**

****

**第二次握手：服务器收到syn包，必须确认客户的SYN（ack=j+1），同时自己也发送一个SYN包（syn=k），即SYN+ACK包，此时服务器进入SYN\_RECV状态；**

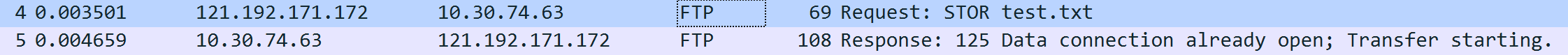
****

**第三次握手：客户端收到服务器的SYN+ACK包，向服务器发送确认包ACK(ack=k+1），此包发送完毕，客户端和服务器进入ESTABLISHED（TCP连接成功）状态，完成三次握手程序监听该报文**

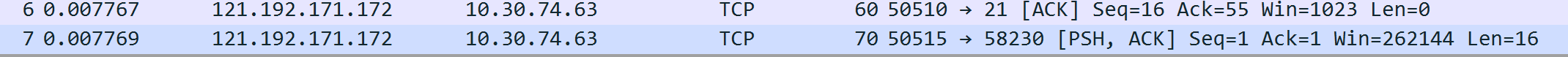
****

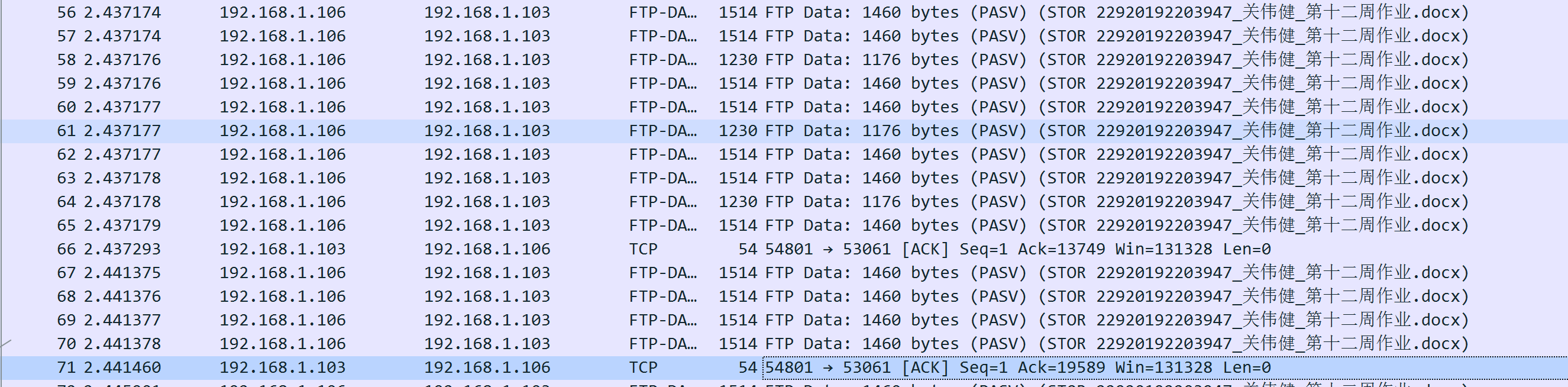
**1.2可靠传输**

**请求传送：**

****

**停等协议：客户端传送一个报文后，会受到一个确认传送确认，然后再进行下一步传送。**

****

****

**窗口机制：**

**报文没有捕捉到，出现报文丢失**

****

**拥塞控制：**

**重复应答：#前表示报文到哪个序号丢失，#后面是第几次丢失**

****

**1.3四次挥手**

**客户端发送一个FIN，用来关闭客户端到服务器的数据传送**

****

**服务器受到FIN后，发回一个ACK**

****

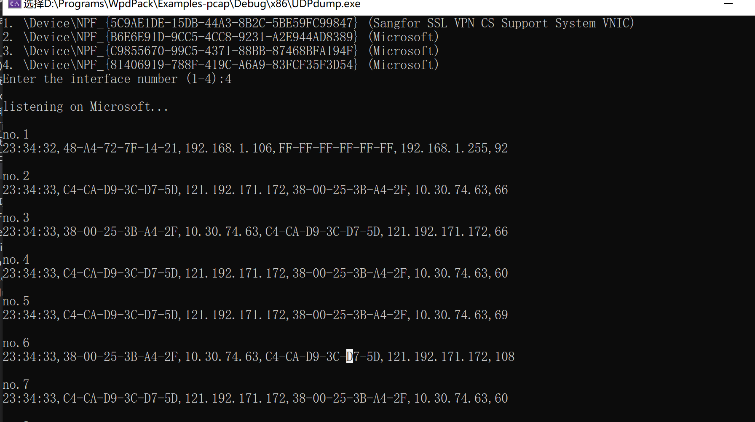
**服务器关闭与客户端的连接，发送一个FIN给客户端**

****

**客户端回答ACK报文确认**

****

**使用程序监听到的报文数据：**

****

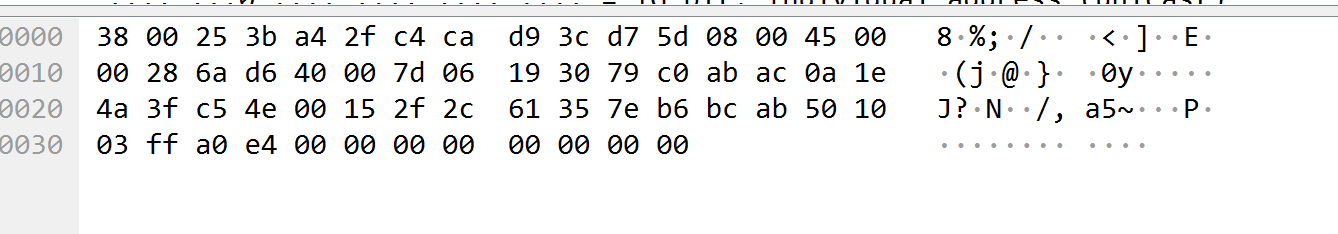
2、**报文分析：**

**2.1数据层报文：**

蓝色：以太网报文头14位

红色：IP报文头20位

黄色：TCP报文头20位



2.2TCP报文：

源端口号（2字节）：21 （00 15） 目的端口号（2字节）：50510（c5 4e）

序号（4字节）：2125905013 （7e b6 bc 75）

确认序号（4）：79143621 （2f 2c 61 35）

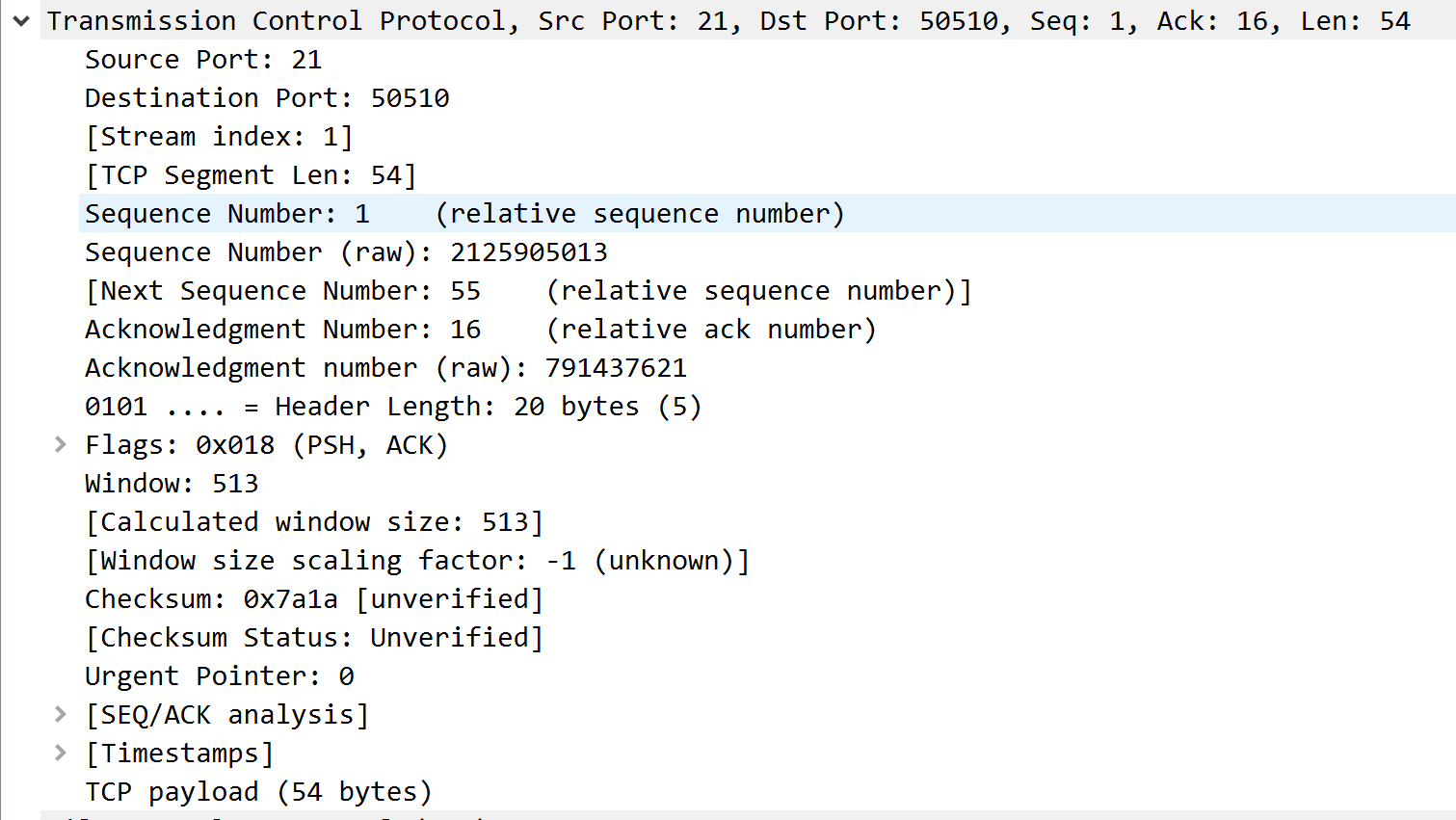
首部长（4）：20

标志位（12）：0x018（50 18）

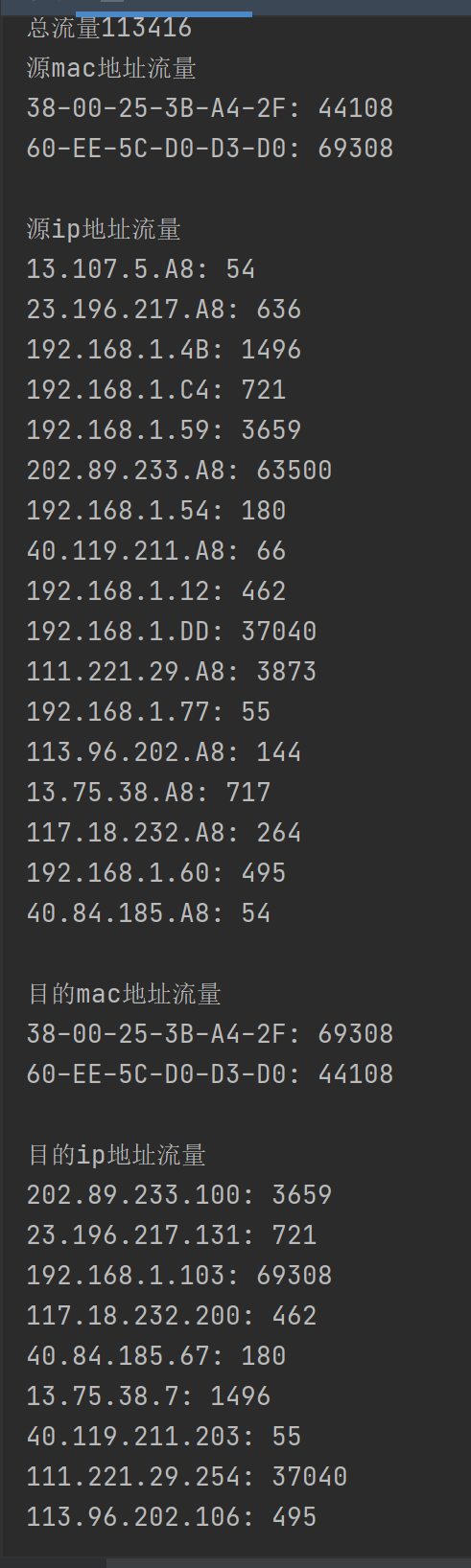
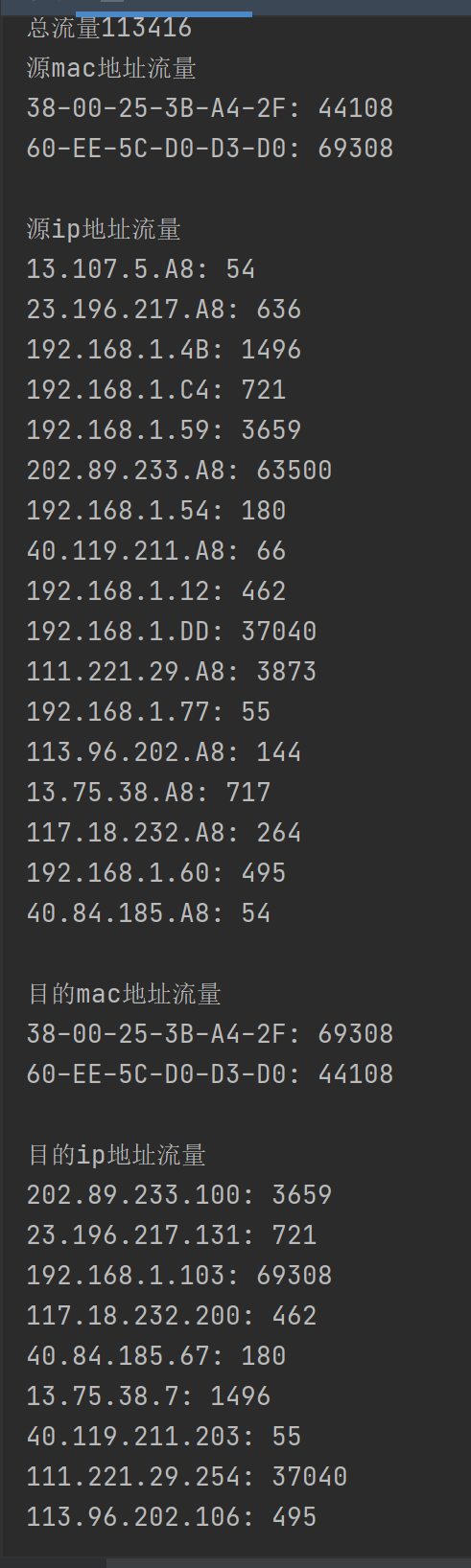
窗口大小（2）：513

校验和（2）：0x7a1a

紧急指针（2）0



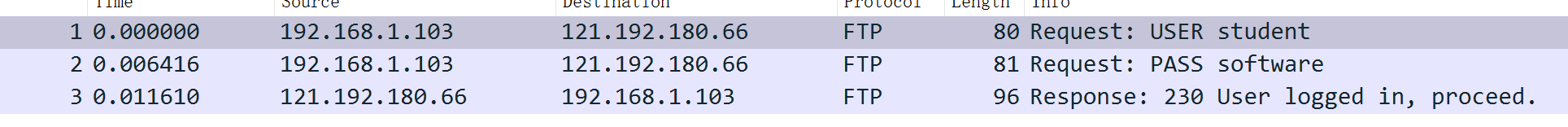
3、计算一分钟内的通信长度：（java计算）



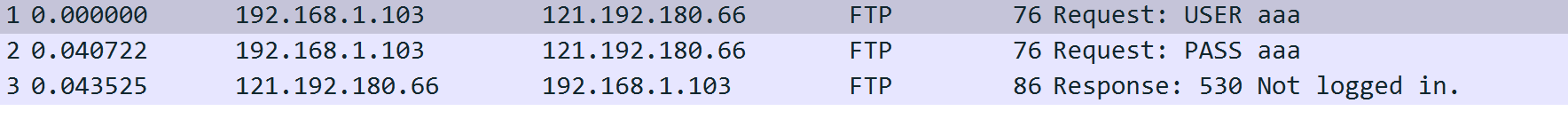
4观察FTP数据

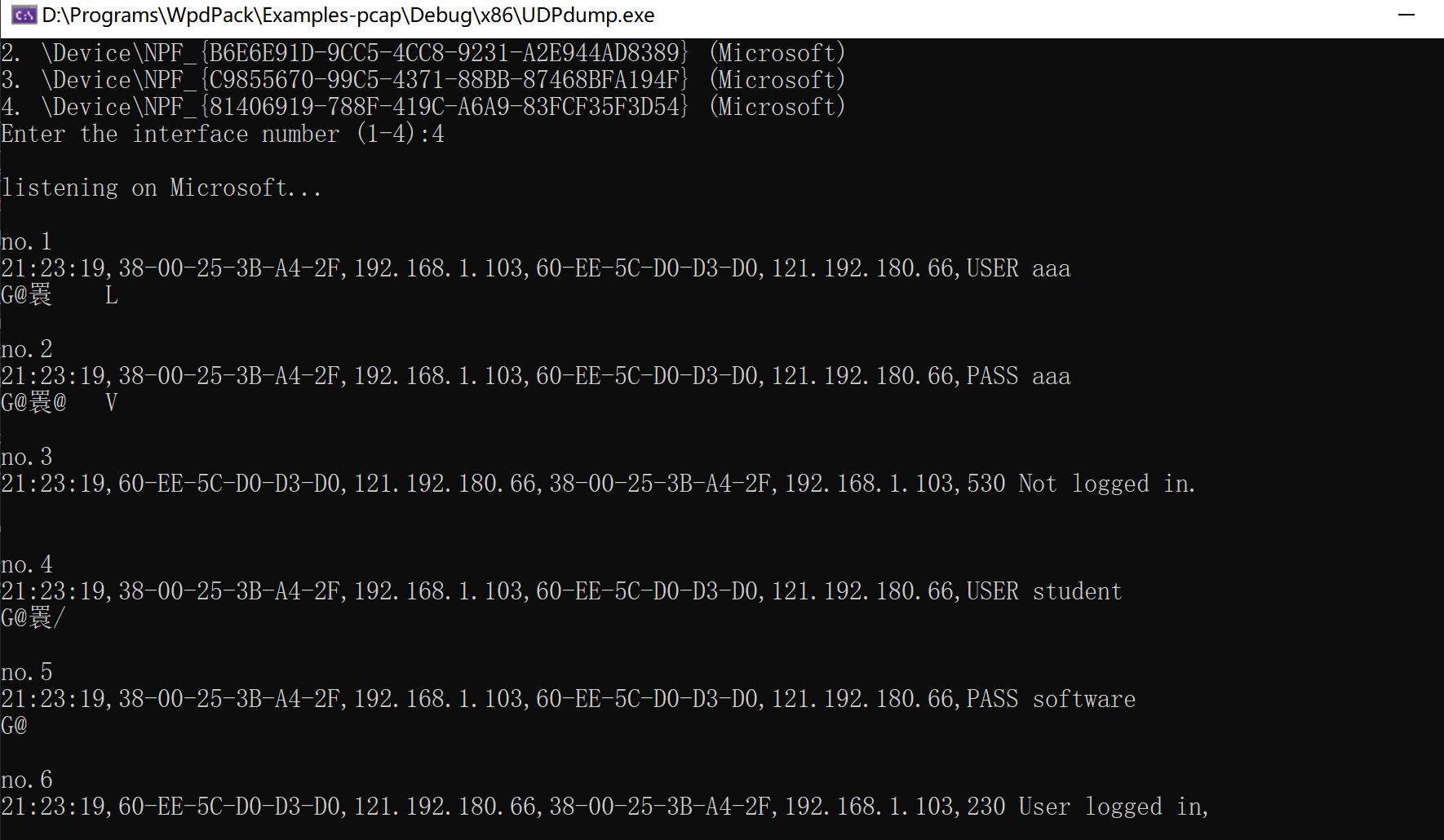
ftp数据报文是利用tcp协议传输的，登陆时所传输的登录信息是放在tcp报文的数据中。以530开头，表示登录失败，以230开头表示登录成功，其中登录信息用户名和密码是分开传送，先认定用户名有效，在认定密码有效。

**登录成功的数据报：**

****

**登录失败的数据报：**

****



# 实验代码

本次实验的代码已上传于以下代码仓库：[cd888888/network: report (github.com)](https://github.com/cd888888/network)

# 实验总结

掌握了tcp报文格式

掌握了ftp登录时的通信过程

掌握了怎么使用wireshark观察网络流量，并辅助进行网络监听相关的编程

掌握了使用winpcap库监听处理以太网帧和ip报文的方法等计算机网络的基础知识和网络编程方法。