

# 廈門大學



## 信息学院软件工程系

### 《计算机网络》实验报告

题    目 实验四 观察 TCP 报文段并侦听分析 FTP 协议

班    级 软件工程 2018 级 1 班

姓    名 陈怡心

学    号 24320182203180

实验时间 2020 年 3 月 25 日

2020 年 3 月 30 日

## 1 实验目的

基于 WinPCAP 工具包制作程序，实现监听网络上的 FTP 数据流，解析协议内容，并作记录与统计。对用户登录行为进行记录。

最终在文件上输出形如下列 CSV 格式的日志：

时间、源 MAC、源 IP、目标 MAC、目标 IP、登录名、口令、成功与否。

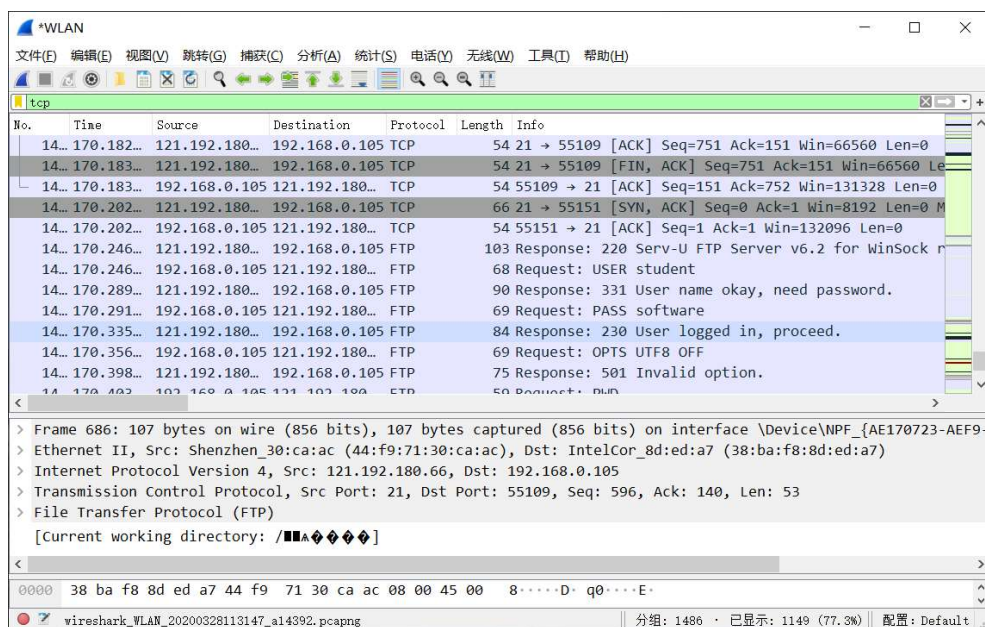
## 2 实验环境

操作系统：Windows 10

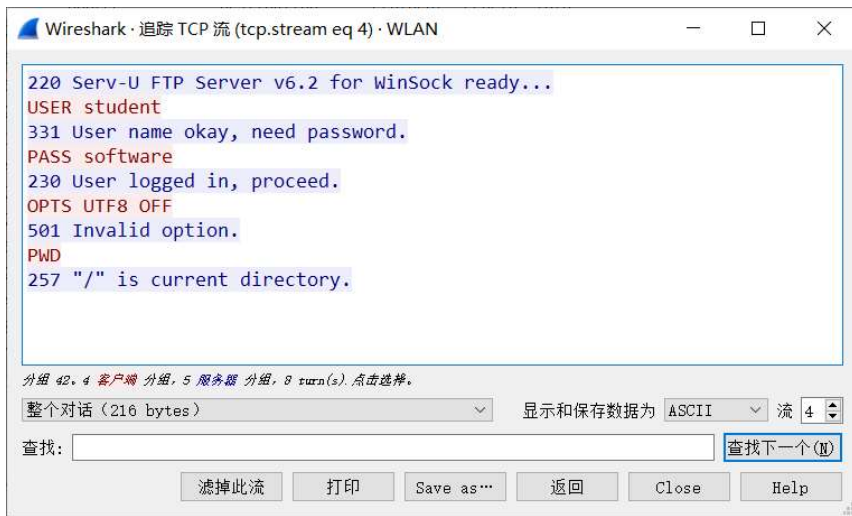
编程语言：C 语言

## 3 实验结果

### 1、使用 TCP 过滤器找到 FTP 包

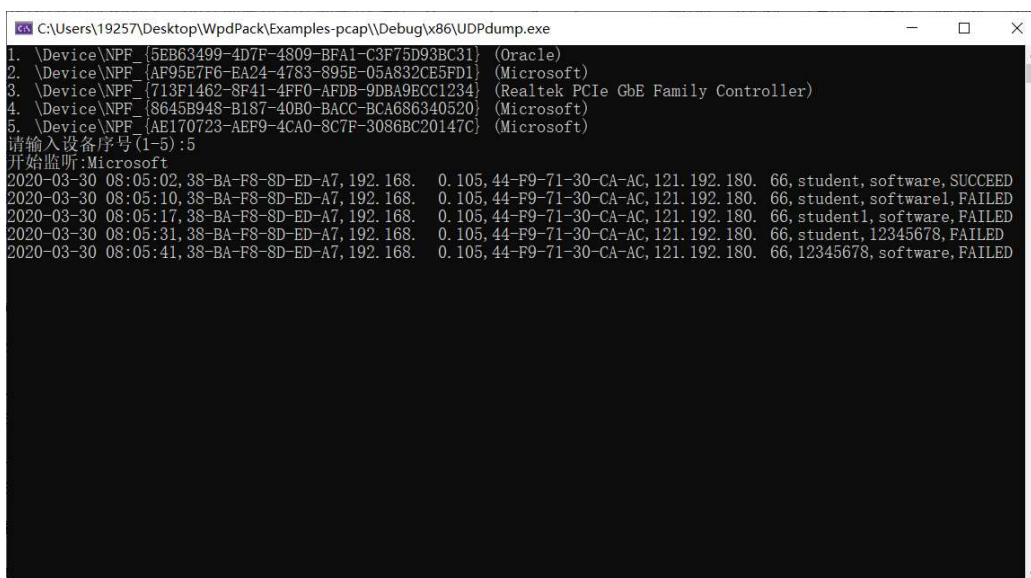


### 2、点击跟踪流了解 FTP 的通信协议的过程



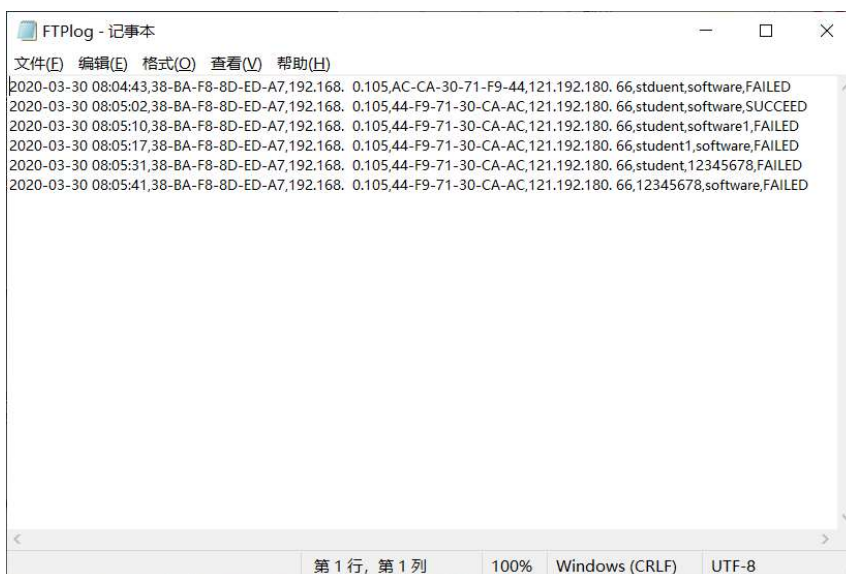
### 3、编写程序监听并记录

运行结果:



```
C:\Users\19257\Desktop\WpdPack\Examples-pcap\Debug\x86\UDPdump.exe
1. \Device\NPF_{5EB63499-4D7F-4809-BFA1-C3F75D93BC31} (Oracle)
2. \Device\NPF_{AF95E7F6-EA24-4783-895E-05A832CE5FD1} (Microsoft)
3. \Device\NPF_{713F1462-SF41-4FF0-AFDB-9DBA9ECC1234} (Realtek PCIe GbE Family Controller)
4. \Device\NPF_{8645B948-B187-40B0-BACC-BCA686340520} (Microsoft)
5. \Device\NPF_{AE170723-AEF9-4CA0-8C7F-3086BC20147C} (Microsoft)
请输入设备序号(1-5):5
开始监听:Microsoft
2020-03-30 08:05:02,38-BA-F8-8D-ED-A7,192.168. 0.105,44-F9-71-30-CA-AC,121.192.180. 66,student,software,SUCCESS
2020-03-30 08:05:10,38-BA-F8-8D-ED-A7,192.168. 0.105,44-F9-71-30-CA-AC,121.192.180. 66,student,software1,FAILED
2020-03-30 08:05:17,38-BA-F8-8D-ED-A7,192.168. 0.105,44-F9-71-30-CA-AC,121.192.180. 66,student1,software,FAILED
2020-03-30 08:05:31,38-BA-F8-8D-ED-A7,192.168. 0.105,44-F9-71-30-CA-AC,121.192.180. 66,student,12345678,FAILED
2020-03-30 08:05:41,38-BA-F8-8D-ED-A7,192.168. 0.105,44-F9-71-30-CA-AC,121.192.180. 66,12345678,software,FAILED
```

输出 csv 日志:



```
FTPLog - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
2020-03-30 08:04:43,38-BA-F8-8D-ED-A7,192.168. 0.105,AC-CA-30-71-F9-44,121.192.180. 66,student,software,FAILED
2020-03-30 08:05:02,38-BA-F8-8D-ED-A7,192.168. 0.105,44-F9-71-30-CA-AC,121.192.180. 66,student,software,SUCCESS
2020-03-30 08:05:10,38-BA-F8-8D-ED-A7,192.168. 0.105,44-F9-71-30-CA-AC,121.192.180. 66,student,software1,FAILED
2020-03-30 08:05:17,38-BA-F8-8D-ED-A7,192.168. 0.105,44-F9-71-30-CA-AC,121.192.180. 66,student1,software,FAILED
2020-03-30 08:05:31,38-BA-F8-8D-ED-A7,192.168. 0.105,44-F9-71-30-CA-AC,121.192.180. 66,student,12345678,FAILED
2020-03-30 08:05:41,38-BA-F8-8D-ED-A7,192.168. 0.105,44-F9-71-30-CA-AC,121.192.180. 66,12345678,software,FAILED
```

## 4 实验总结

通过这次实验，用 Wireshark 侦听并观察 TCP 数据段，更加了解了数据包的格式，了解段 ID、窗口机制和拥塞控制机，了解 FTP 数据包用户名、密码等信息的格式。