

****

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 祖格沄骞**

**学　　号 24320182203339**

**实验时间 2020年3月28日**

**2020 年 3 月 30 日**

# 实验目的

1 用Wireshark侦听并观察TCP数据段，观察其建立和撤除连接的过程，观察段ID、窗口机制和拥塞控制机制等

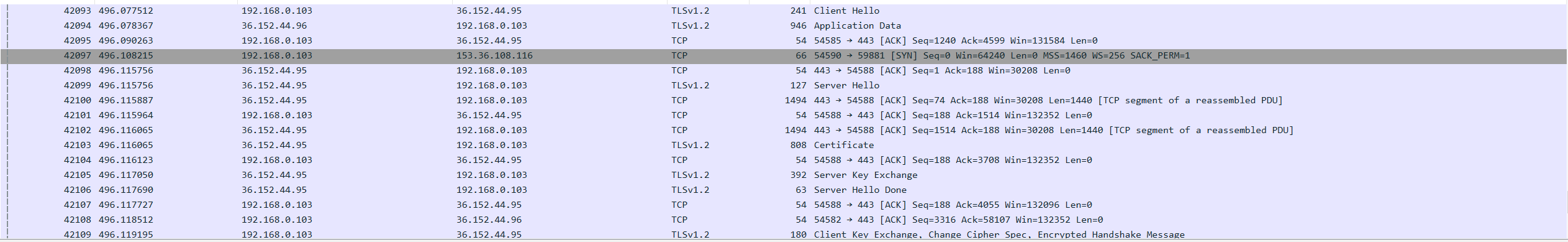
2 用Wireshark侦听并观察FTP数据，分析其用户名密码所在报文的上下文特征，在总结出提取用户名密码的有效办法。基于Winpcap工具包制作程序，实现监听网络上的FTP数据流，解析协议内容并记录与统计。

# 实验环境

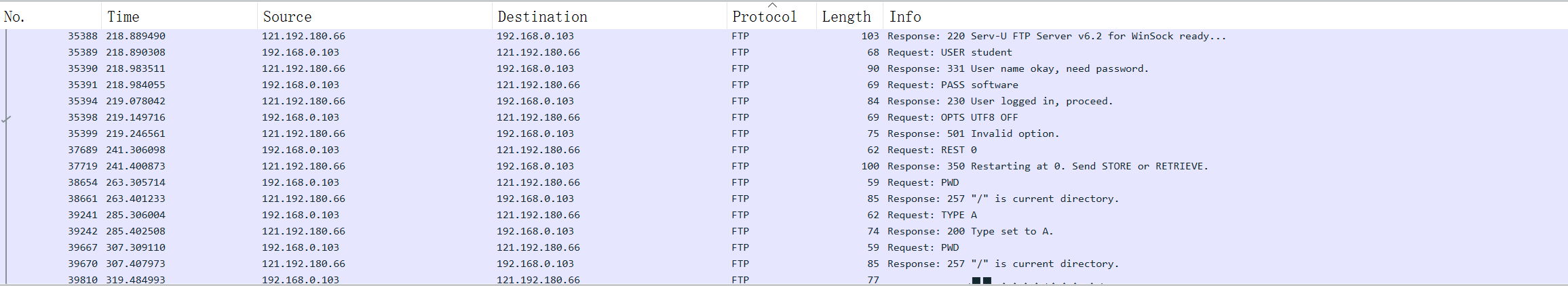
Window 10操作系统、Visual Studio2019、Winpcap

# 实验结果

1. 侦听并观察TCP数据段



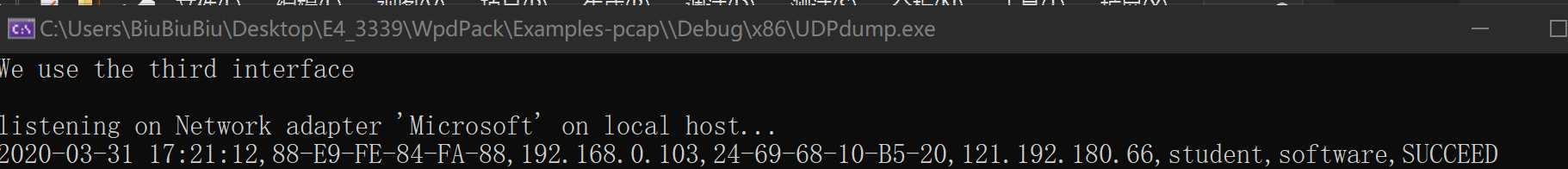
1. 侦听并观察FTP数据



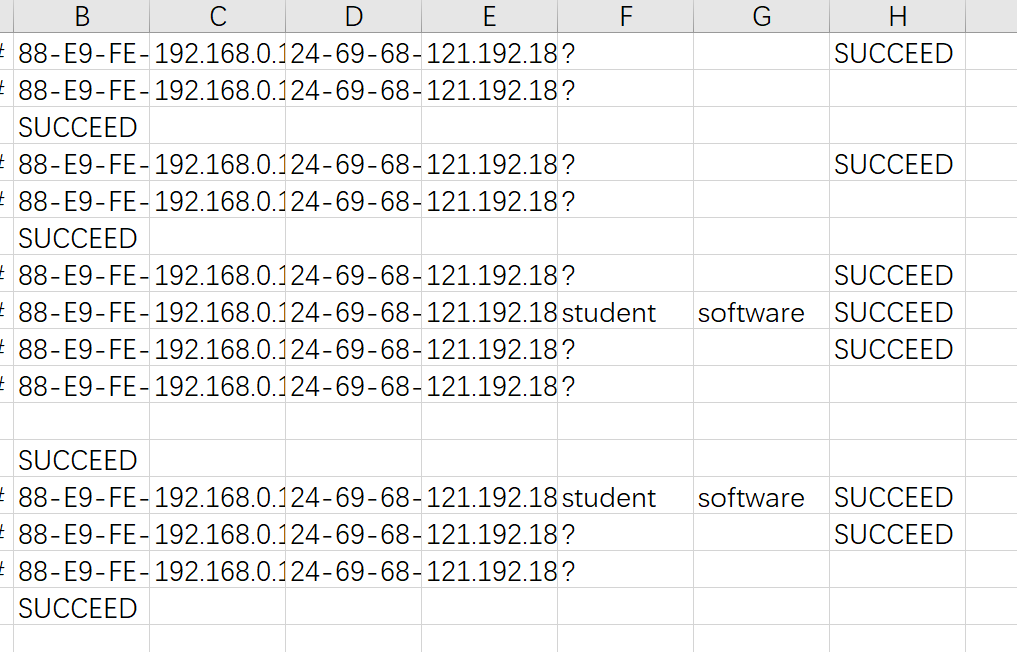
即得出名以“USER”开头，口令以“PASS”开头，登录成功以“230”开头，失败以“530”开头。

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。

侦听结果如下：



记录如下：



# 实验总结

# 通过这次实验，基于wincap库实现对ftp的监听，对Winpcap工具包的使用更加熟悉，提高了自身的代码编辑能力和代码阅读能力。同时也熟悉了wireshark的使用。