

****

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 詹世彬**

**学　　号 24320182203321**

**实验时间 2020年3月25日**

**2020 年 3 月 25 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

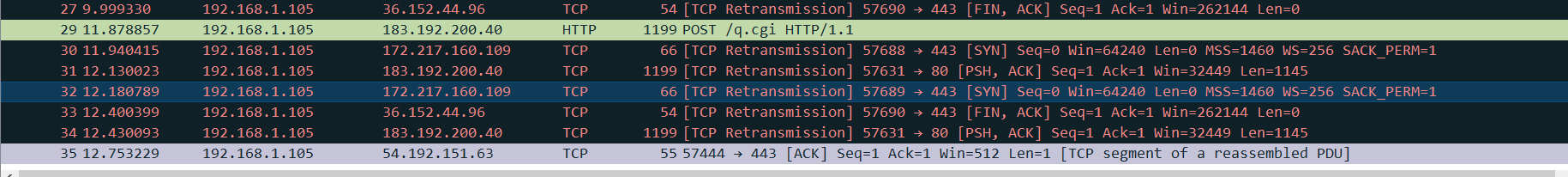
2 用Wireshark侦听并观察FTP数据，分析其用户名密码所在报文的上下文特征，在总结出提取用户名密码的有效办法。基于Winpcap工具包制作程序，实现监听网络上的FTP数据流，解析协议内容并记录与统计。

# 实验环境

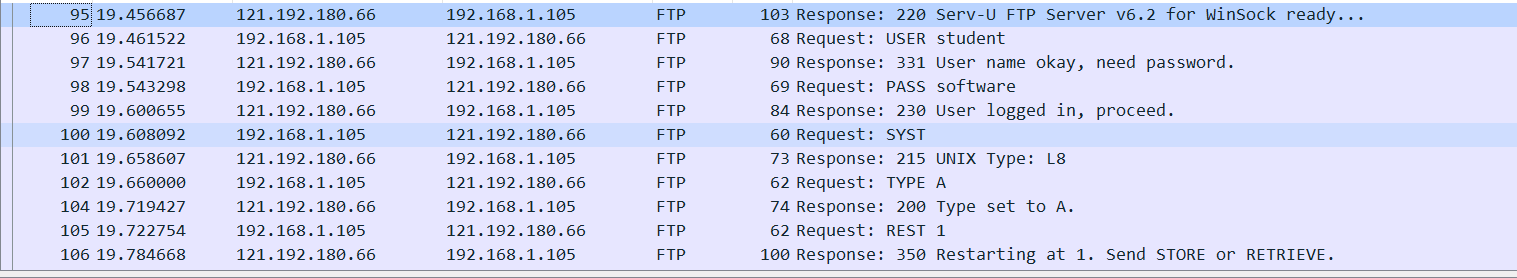
Window 10操作系统、Visual Studio2020、Winpcap

# 实验结果

1. 侦听并观察TCP数据段



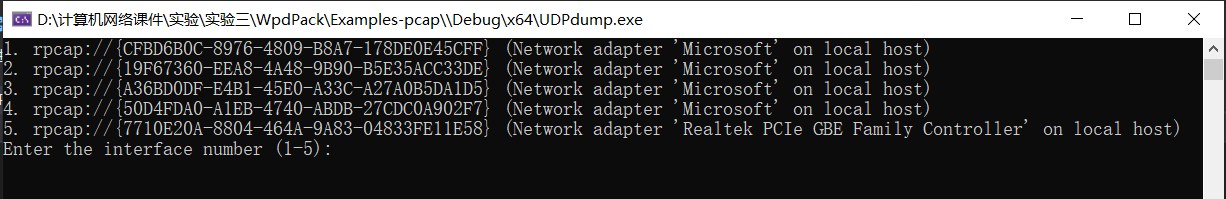
1. 侦听并观察FTP数据



观察得出登录名以‘USER’开头，密码以‘PASS’开头，登录成功以‘230’开头，登录失败以‘530’开头，由此来进行下一步的编程。

1. 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，程序的运行结果如下：

（1）首先选择合适的网卡

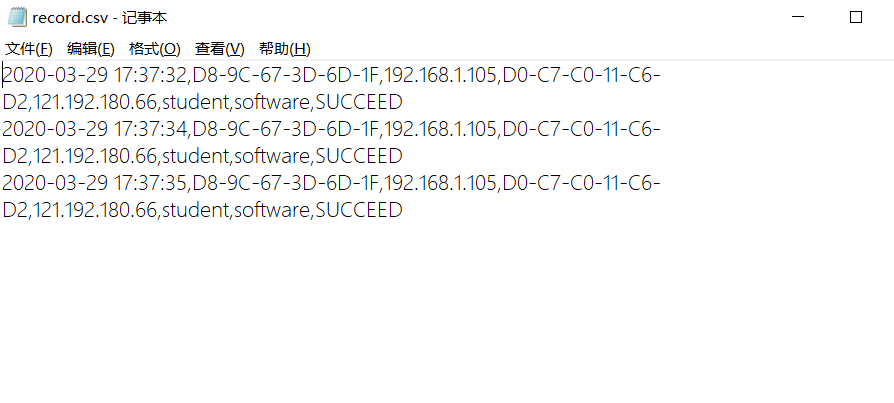


（2）侦听结果如下：

QQ截图20200329173346

格式：时间、源MACA、源IP、目标MAC、目标IP、登录名、口令、成功与否

1. 将结果记录和统计，输出到record.csv文件中



# 实验总结

# 通过这次实验，对Winpcap和Wireshark有了更深刻的了解，对FTP数据和TCP数据有了更深刻的认识，并且通过基于Winpcap工具包制作程序，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。