

****

软 件 学 院

《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**

**姓　　名 蔡艺敏**

**学　　号 24320182203166**

**班　　级 软件工程2018级1班**

**实验时间 2020年3月25日**

**2020 年 3 月 25 日**

# 实验目的

本实验是“用 PCAP 库侦听并解析 FTP 口令”实验的第二部分。

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。将该过程截图在报告中。

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，

再总结出提取用户名密码的有效方法。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

2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D

D5-72,192.168.33.2,student,software,SUCCEED

2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D

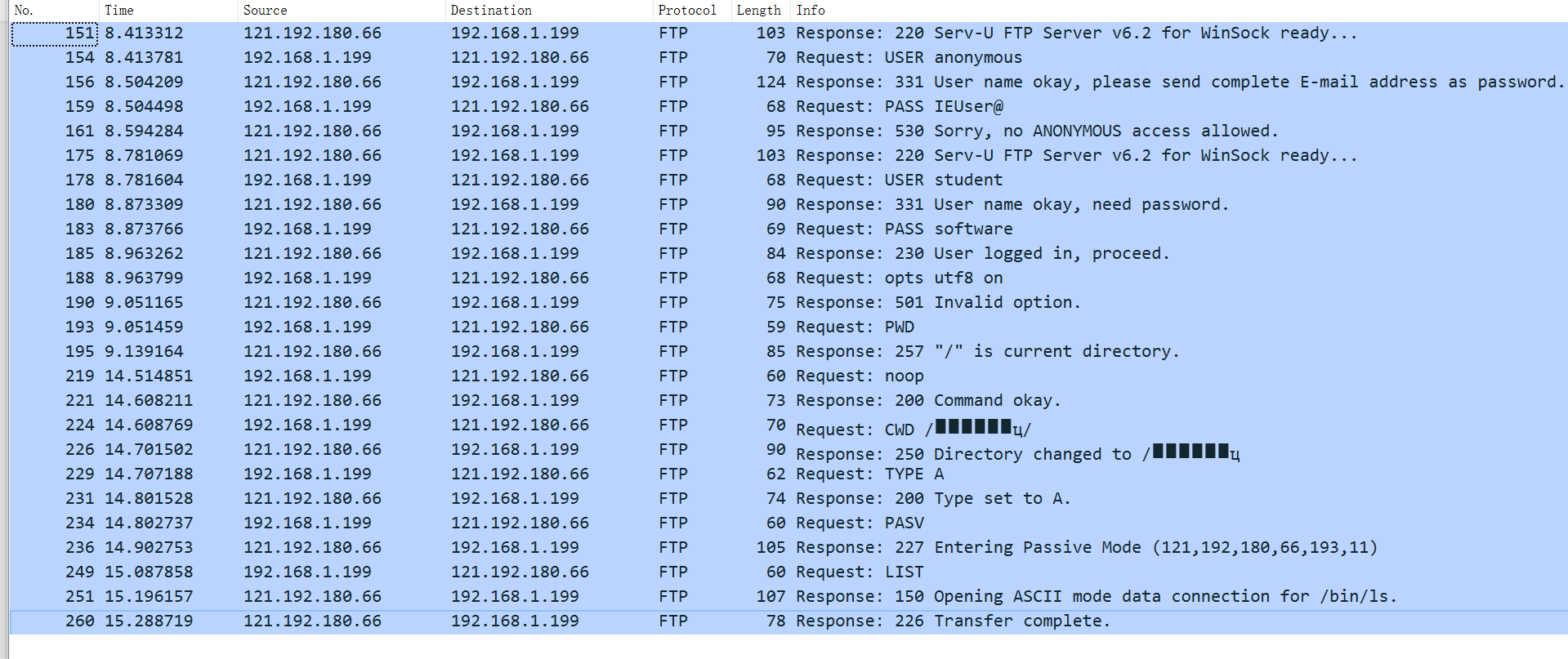
D5-72,192.168.33.2,student,software1,FAILED

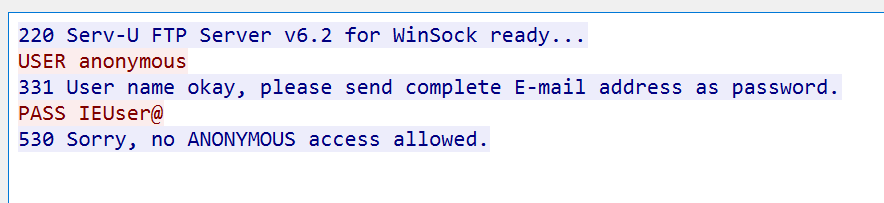
# 实验环境

Win10，VS2015，WinPCAP，科来数据包播放器

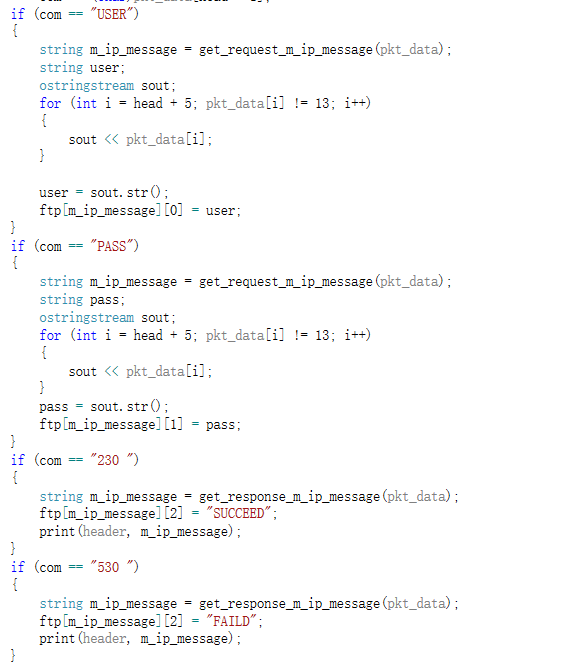
# 实验结果

打开ftp://121.192.180.66/捕捉我们需要的包：

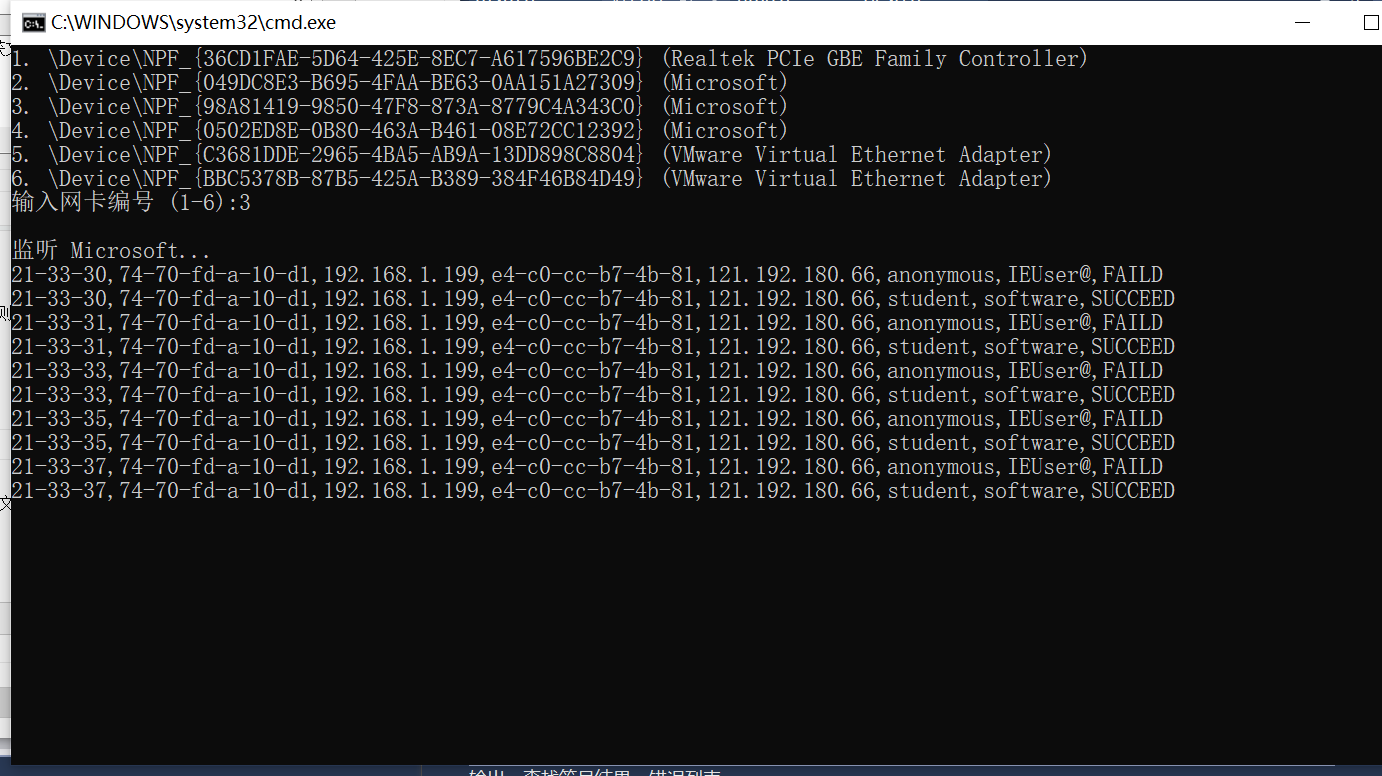




回调函数内登录名、口令和成功与否的判断：



保存数据文件.pcapng，并利用科来多次发送；



# 实验总结

对TCP的三次握手四次挥手有一定的理解，TCP经过三次握手完成连接，经过四次挥手完成连接断开；FTP是基于TCP的应用协议，支持port和pasv两种模式，实验了解了FTP通信协议过程，并对两个端口有一定理解。