

****

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2班**

**姓　　名 林晖**

**学　　号 24320182203231**

**实验时间 2020年3月25日**

**2020 年 3 月 30 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

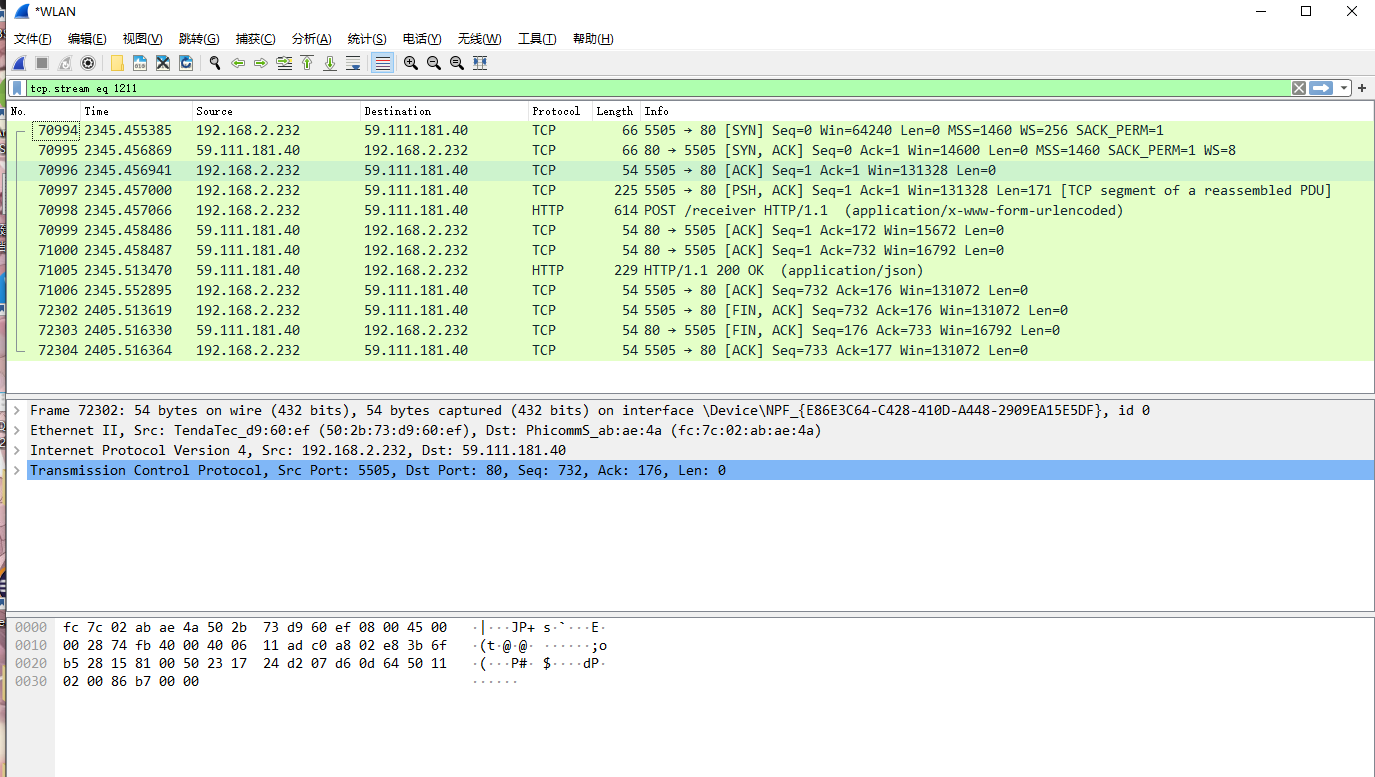
D5-72,192.168.33.2,student,software1,FAILED

# 实验环境

操作系统：Windows 10，编程语言：C。

# 实验结果

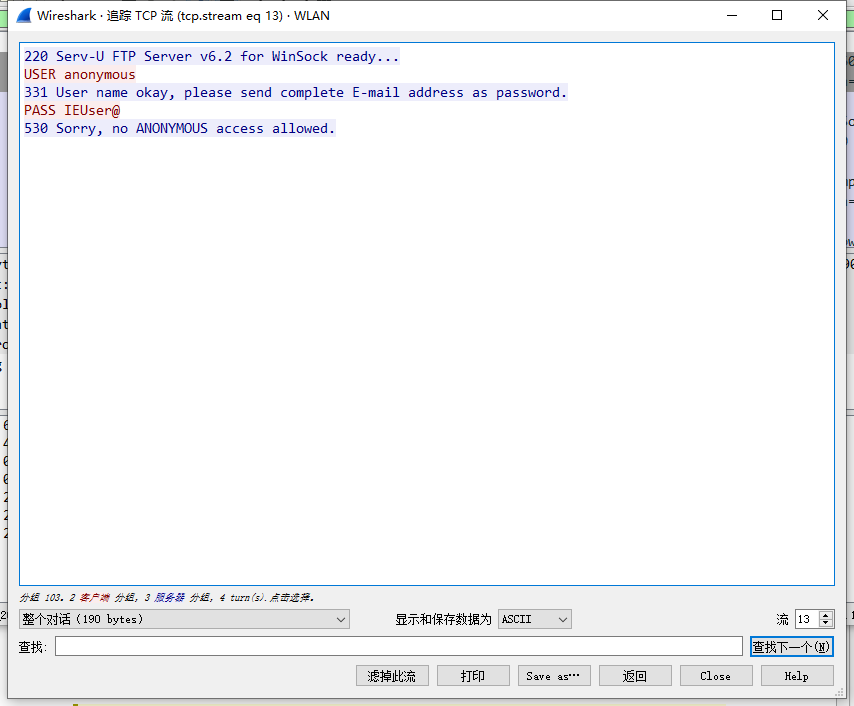
WireShark侦听TCP：



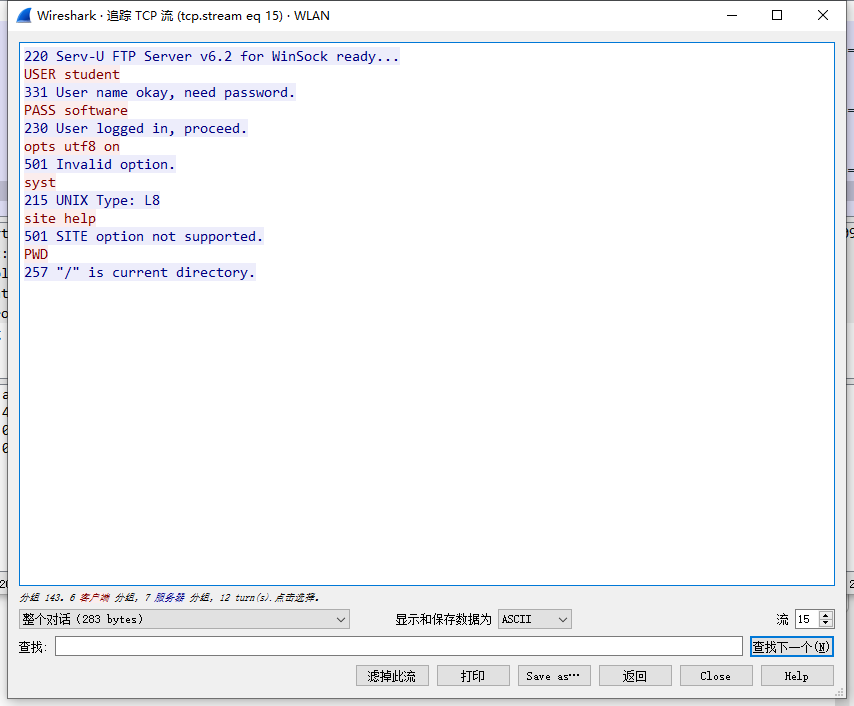
观察TCP报文段接收的三次握手以及断开的四次挥手过程。

同时观察其接收窗口大小，即窗口机制，以及拥塞控制机制等。

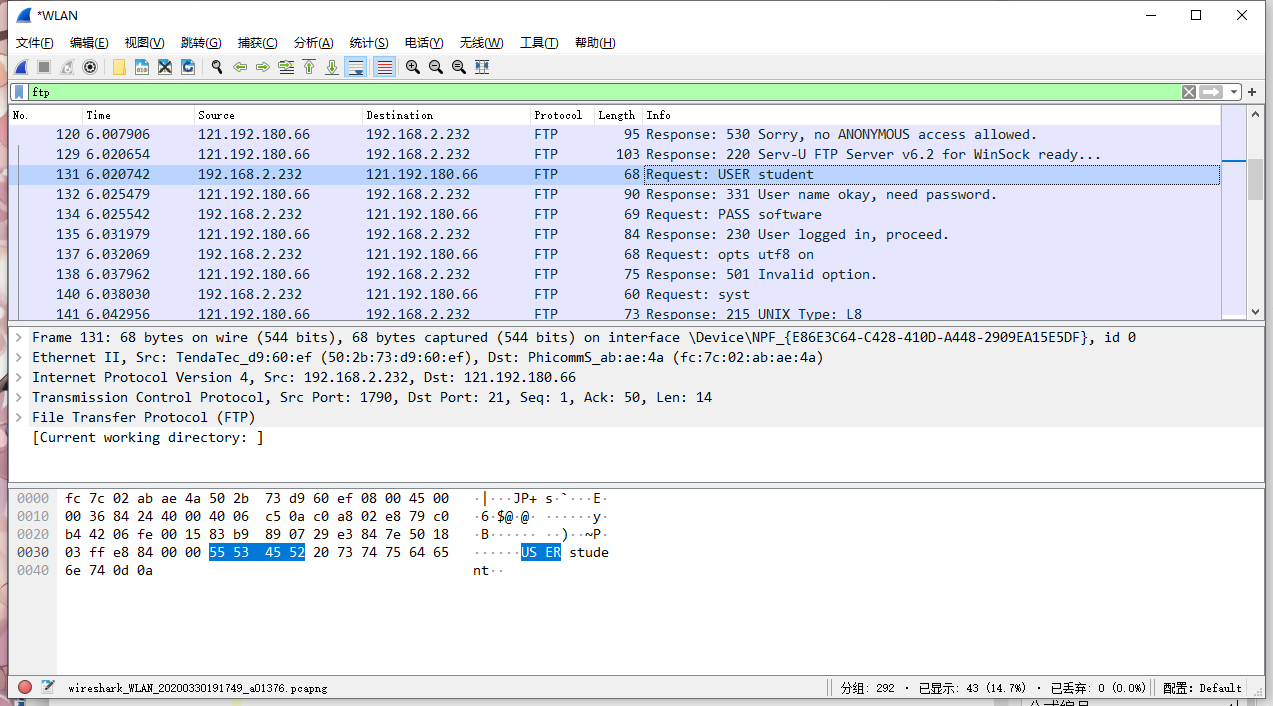
WireShark侦听FTP：

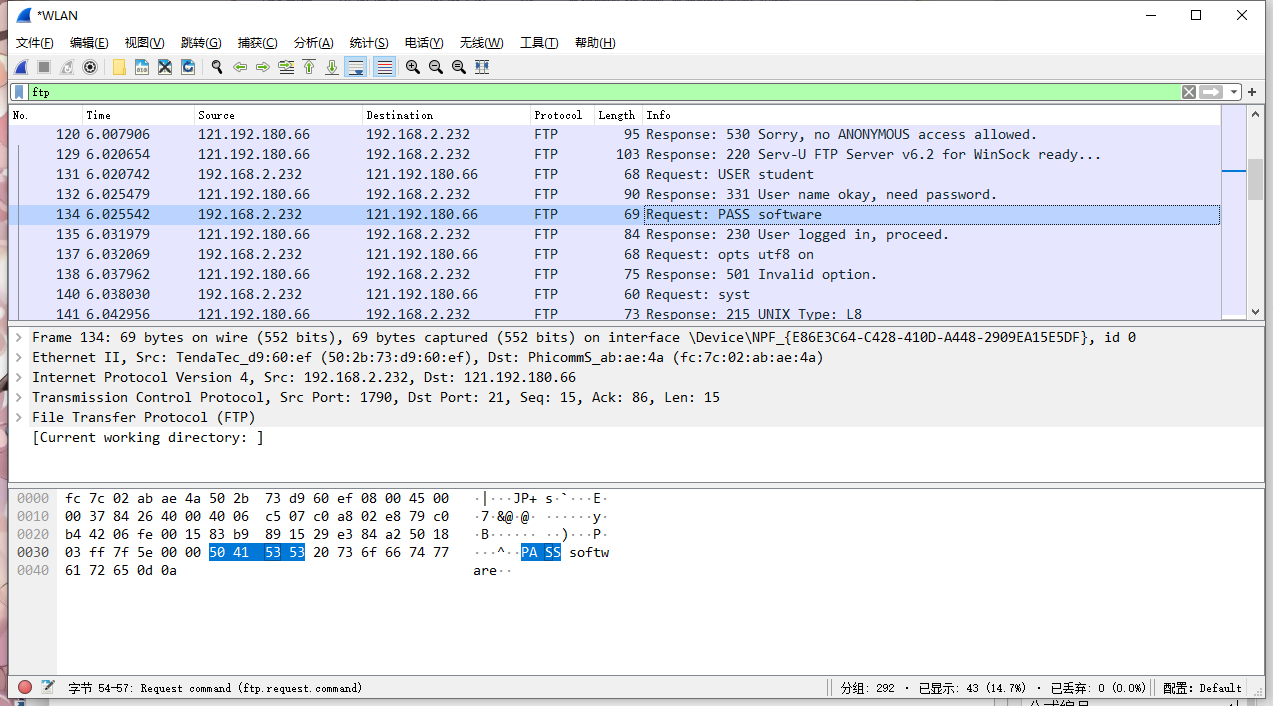


登录失败时：显示530 Sorry, no ANONYMOUS access allowed.



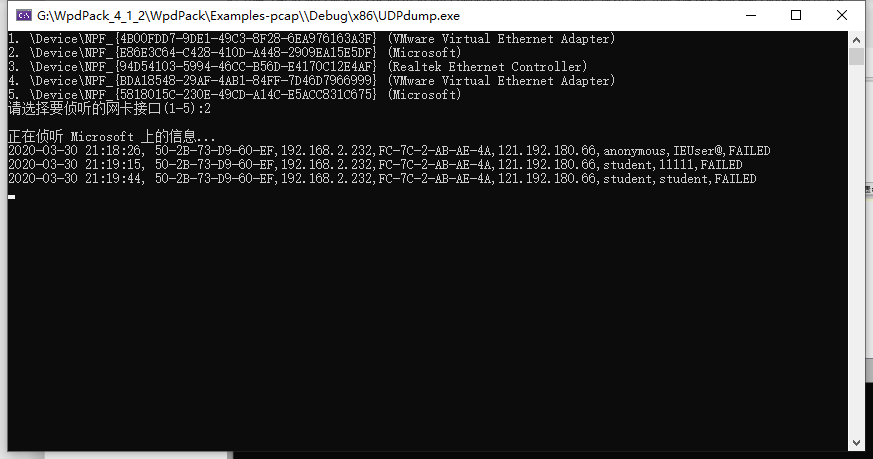
登录成功时：显示230 User logged in, proceed.



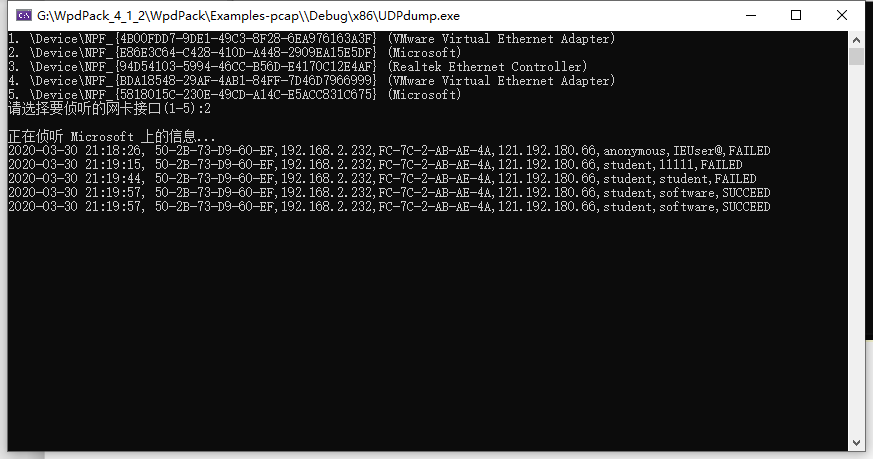


观察发现：存在USER和PASS开始的报文用于登录。

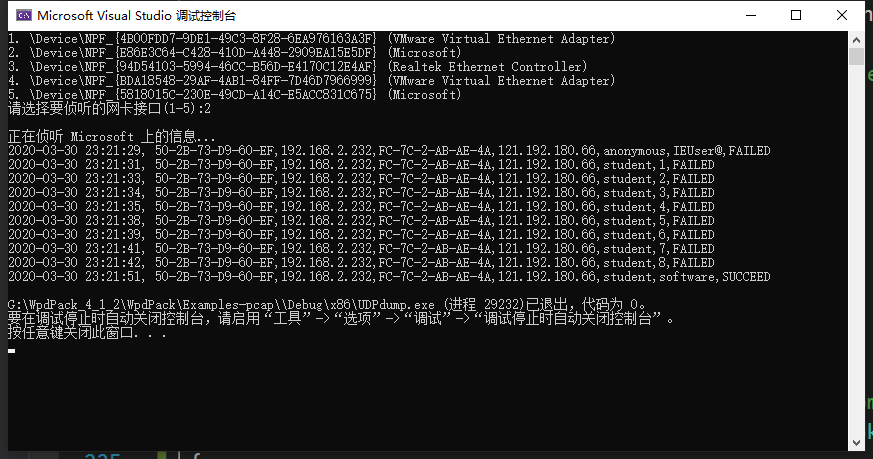
登录FTP：



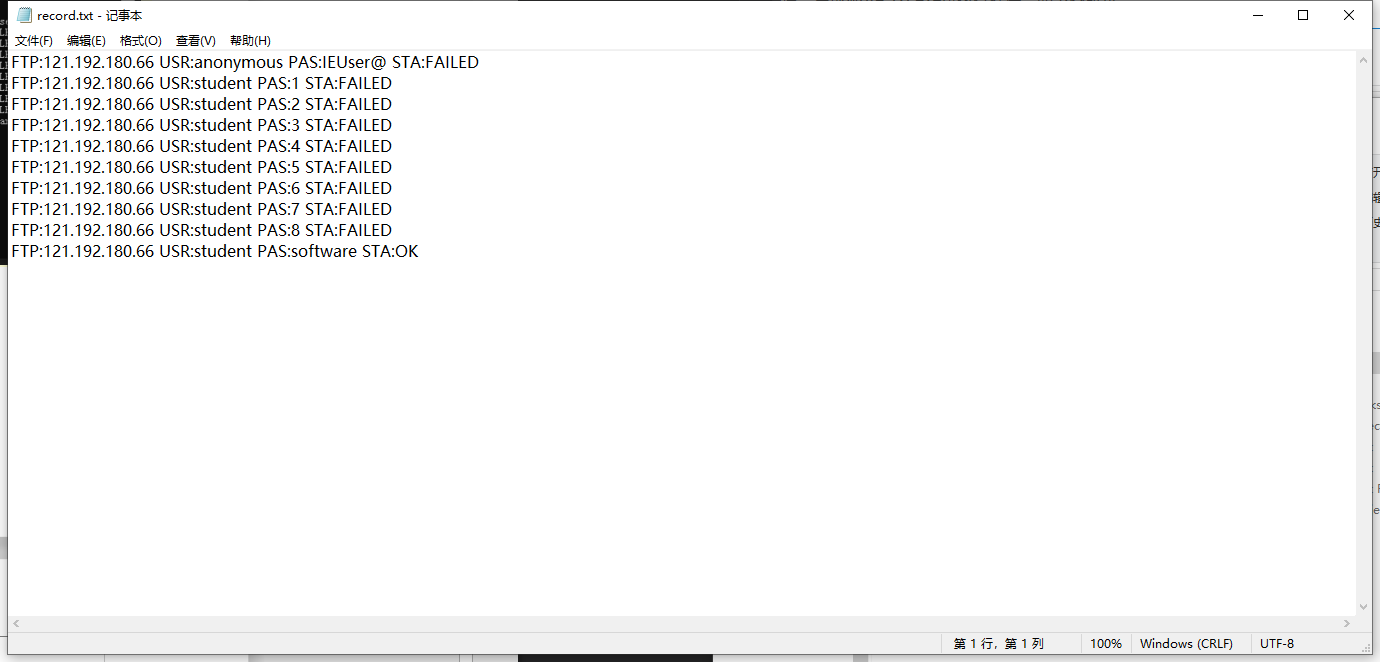
登录失败：显示FAILED



登录成功：显示SUCCEED



读取FTP登录信息，并将其写入文件record.txt



record.txt文件内容

# 实验总结

实际实现了侦听TCP和FTP报文段的功能，观察了TCP握手和挥手的过程，并且实现了搭建FTP服务器，并通过监听FTP通信了解了FTP登录的通信过程，更加熟悉了报文格式。