

****

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 陈渝璇**

**学　　号 24320182203181**

**实验时间 2020年3月25日**

**2020 年 3 月 31 日**

# 实验目的

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。

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。

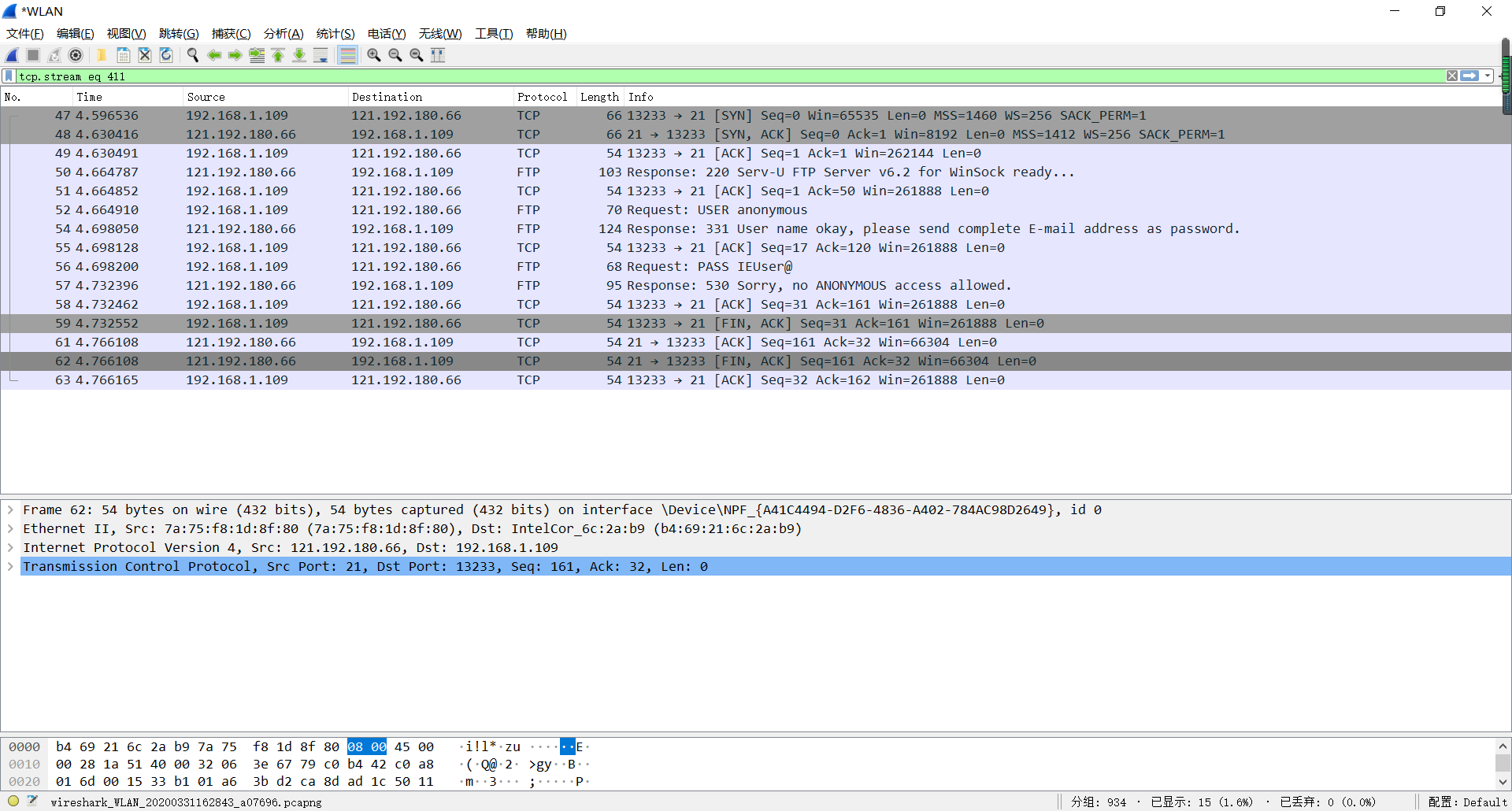
# 实验环境

操作系统：Window10

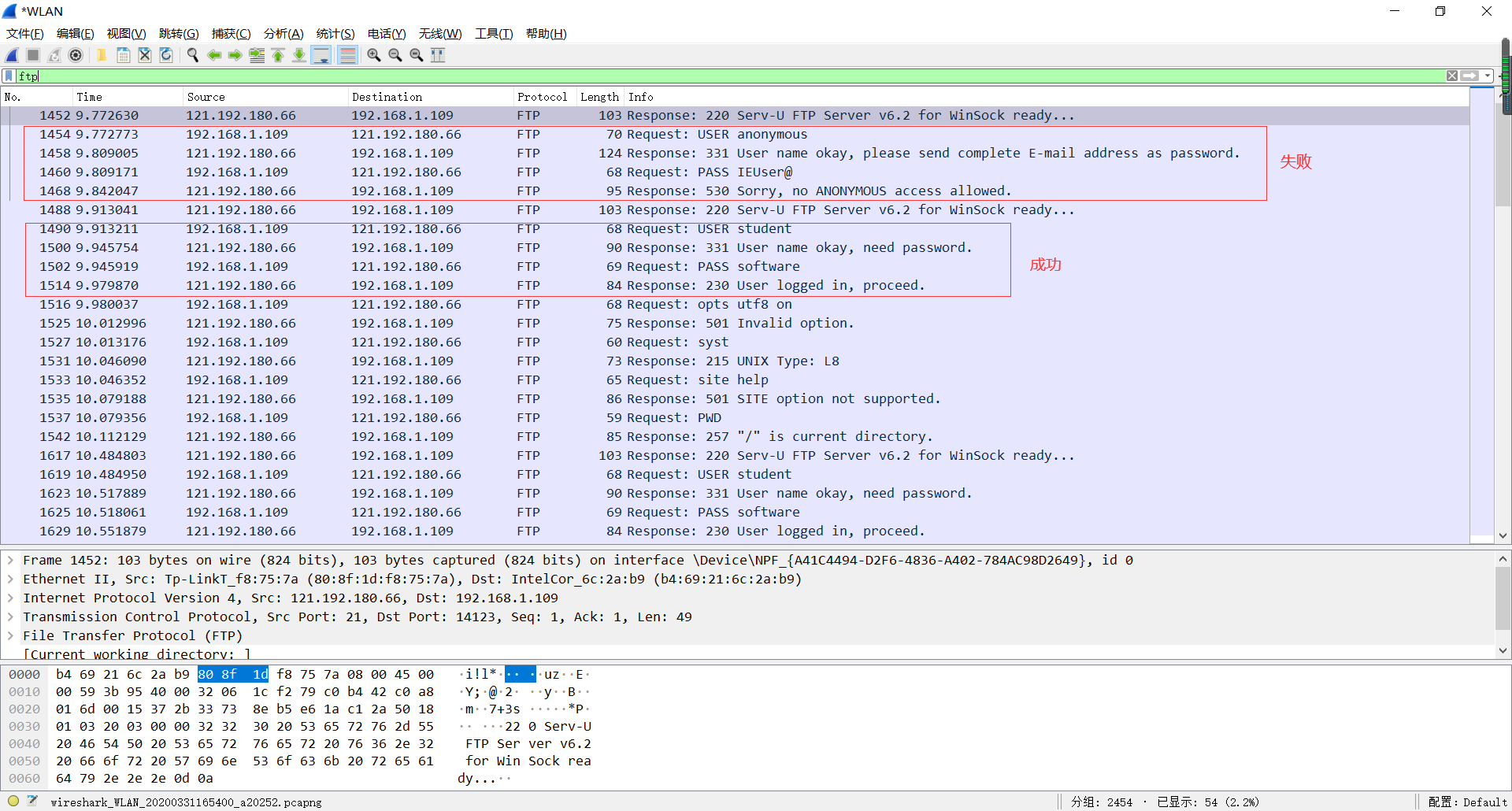
编程语言：c语言

# 实验结果

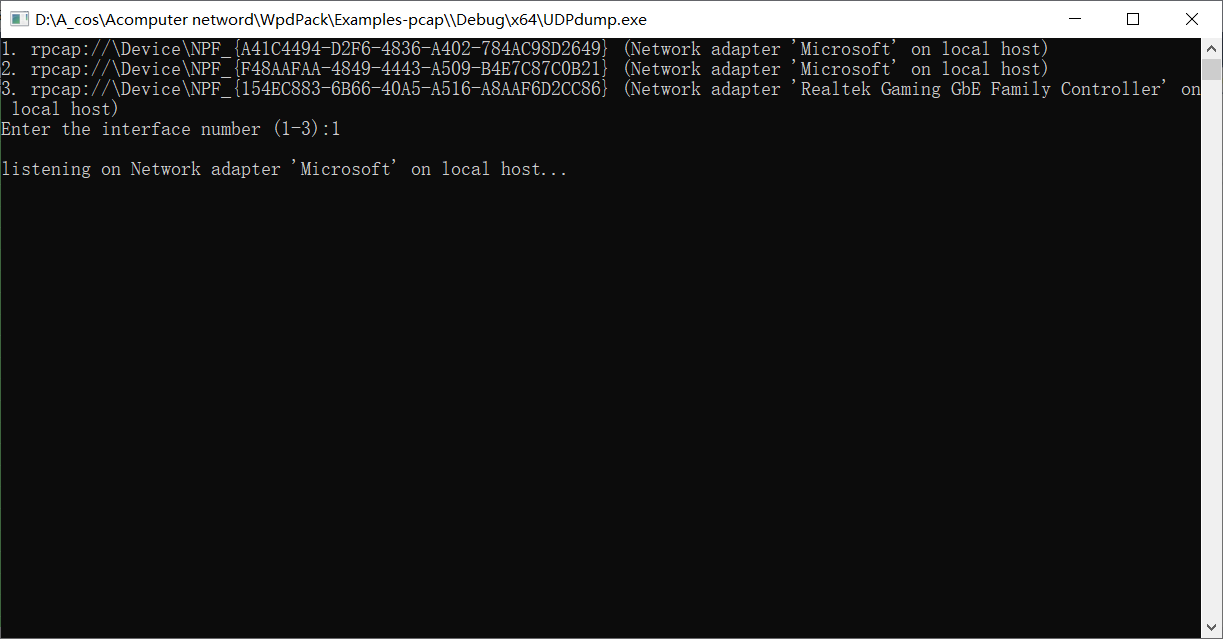
1.侦听ftp:\\121.192.180.66 TCP数据段（前面三次握手，最后四次挥手）



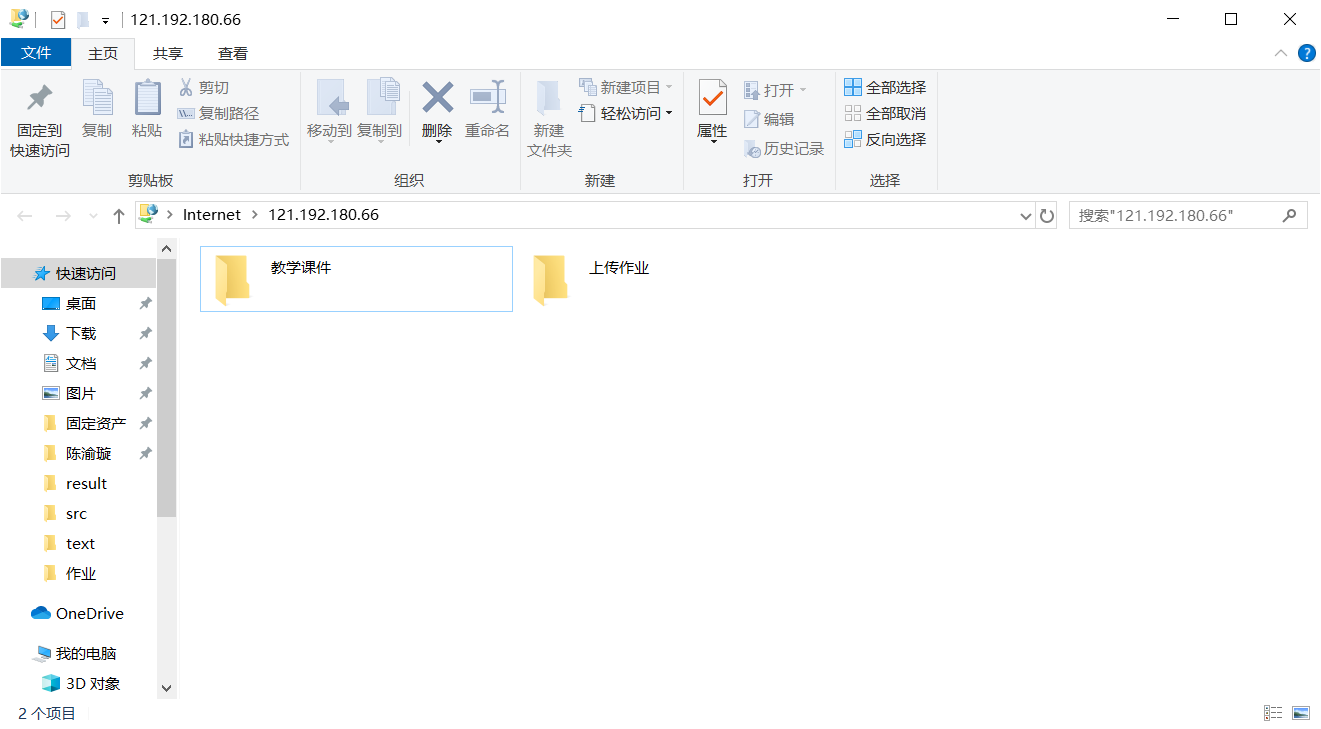
2.侦听并观察 FTP 数据。登录名以USER开头，密码以PASS开头，利用这个获取用户名和密码。成功之后以530开头，失败以230开头。利用这个来判断登录成功与否。



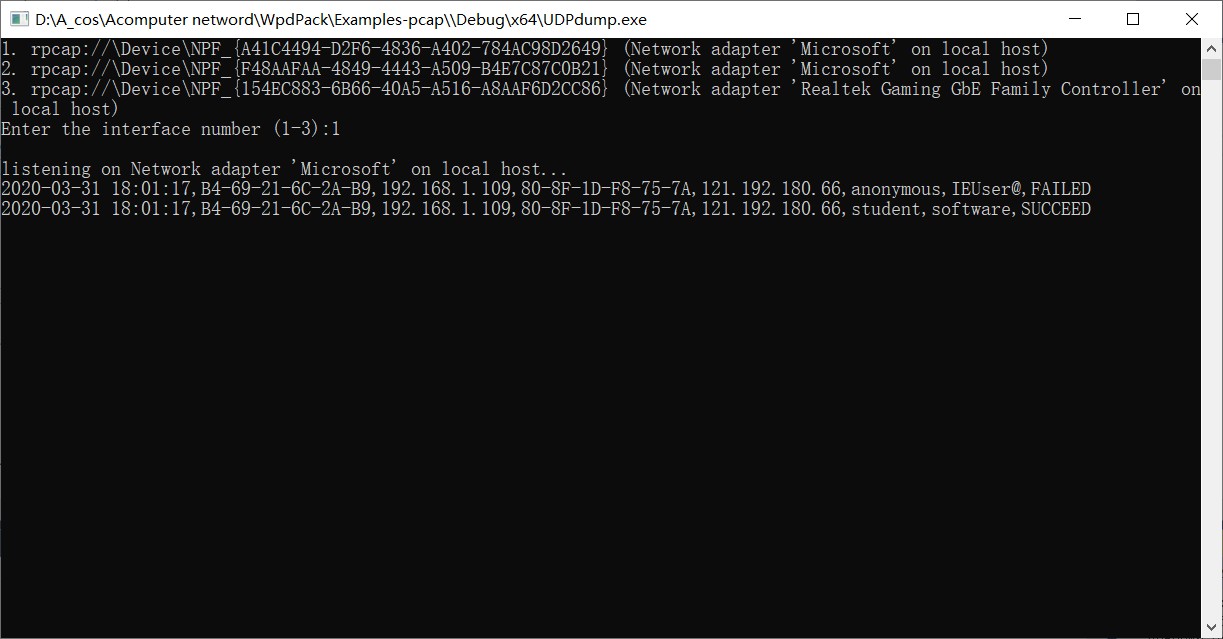
3.运行WinPCAP程序



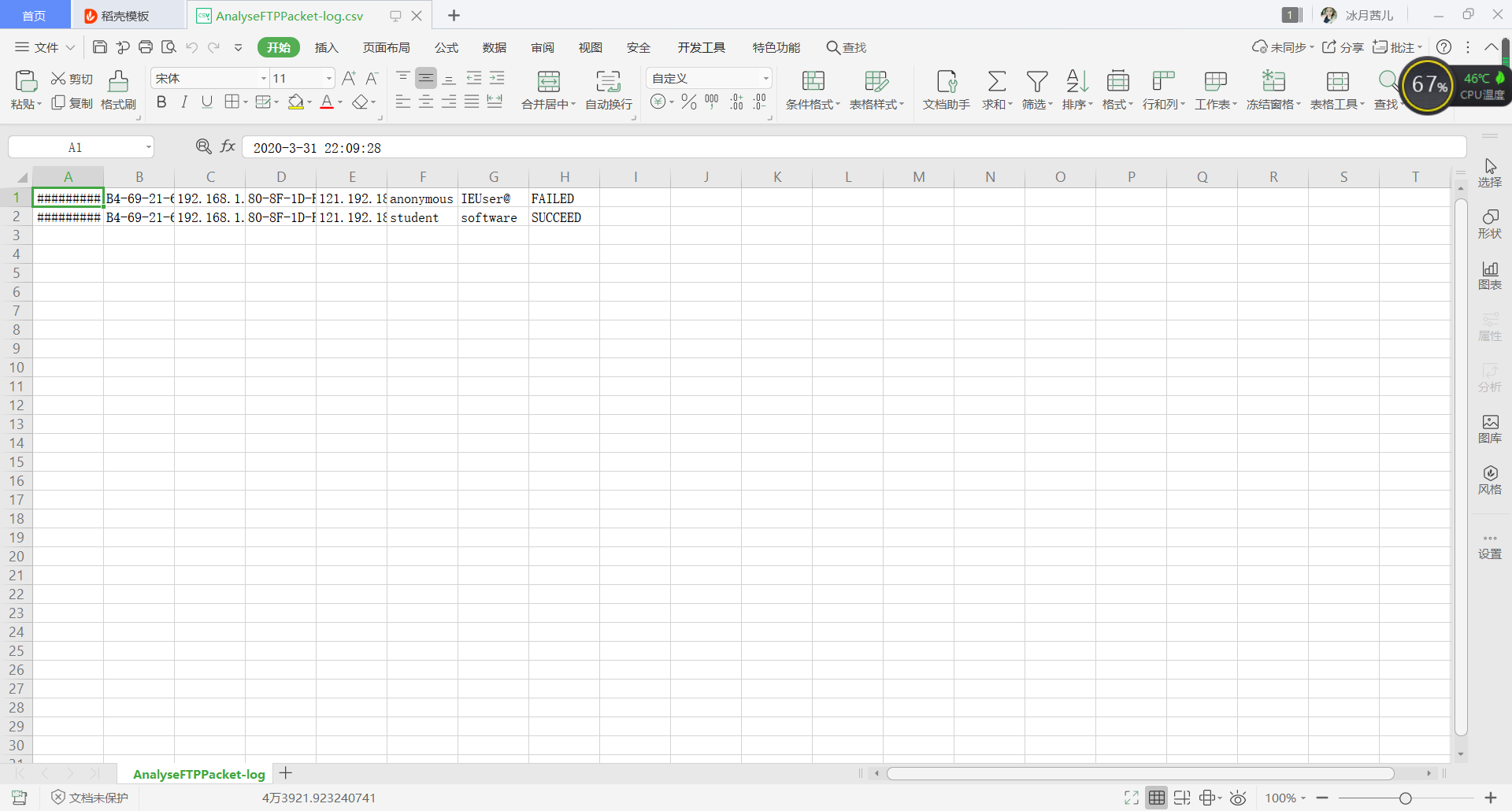
登录ftp



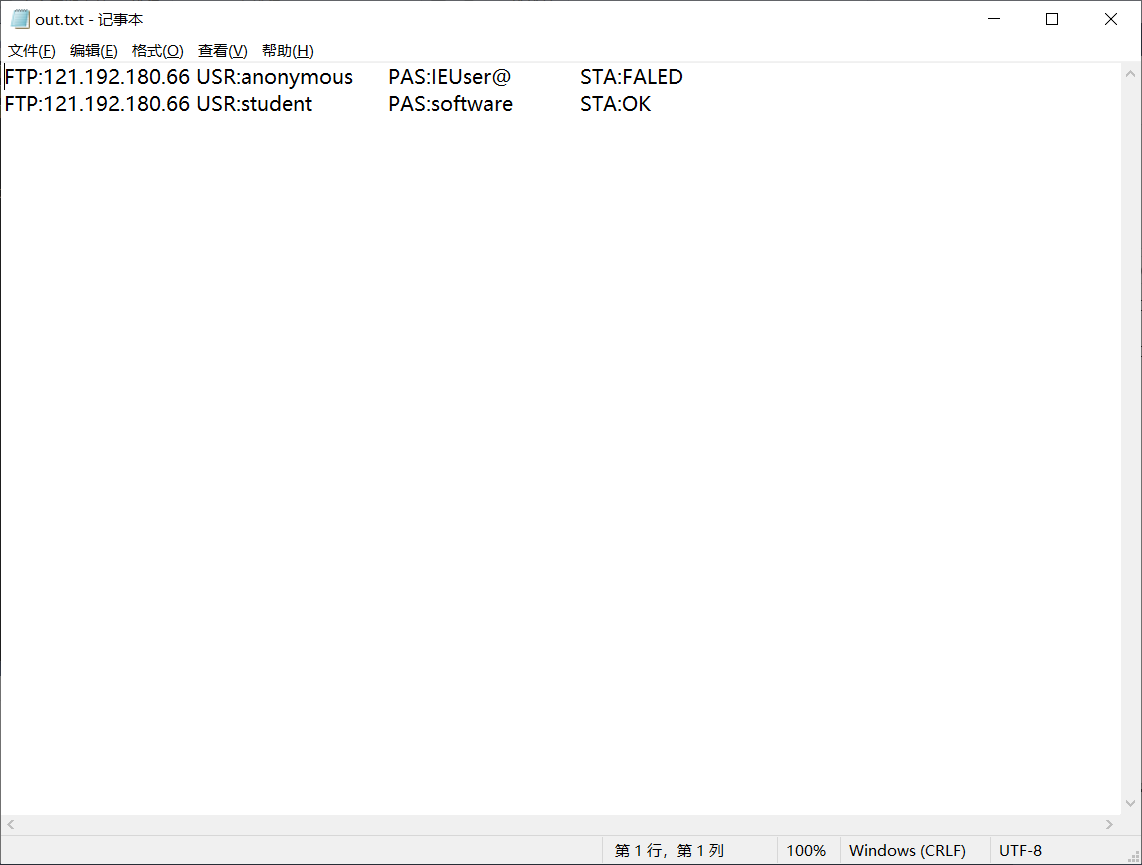
失败与成功连接



输出csv文件



输出文件out.txt



# 实验总结

结合上一次作业所学知识，这次增加了获取ftp的登录用户名与密码的操作。通过Wireshark 侦听并观察 TCP/FTP 数据段，总结用户名与密码的方法。获取user与pass后面的字节至换行符为止，来获取用户名与密码，存储，然后输出。判断是否连接成功来输出成功与否标志。