

廈門大學



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

1 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。

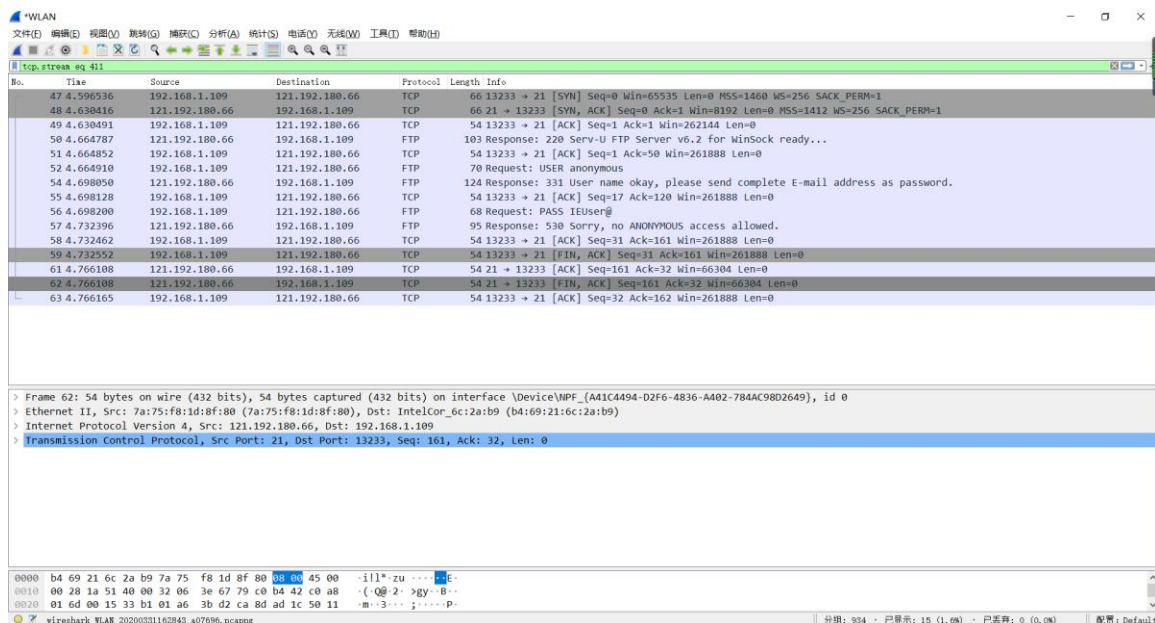
2 实验环境

操作系统：Window10

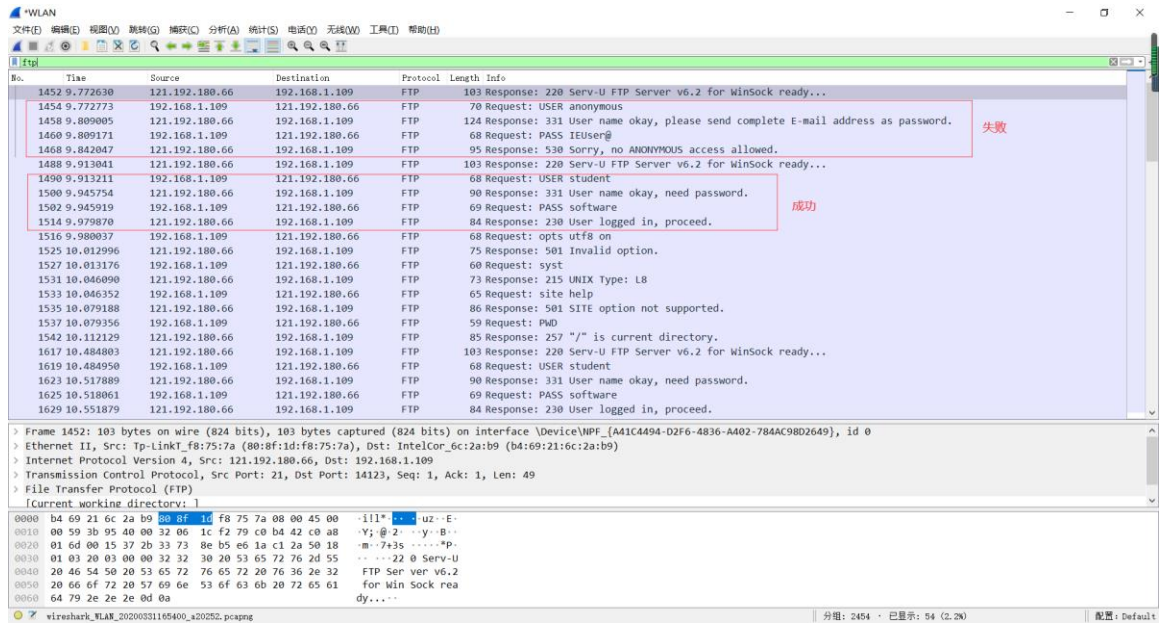
编程语言：c 语言

3 实验结果

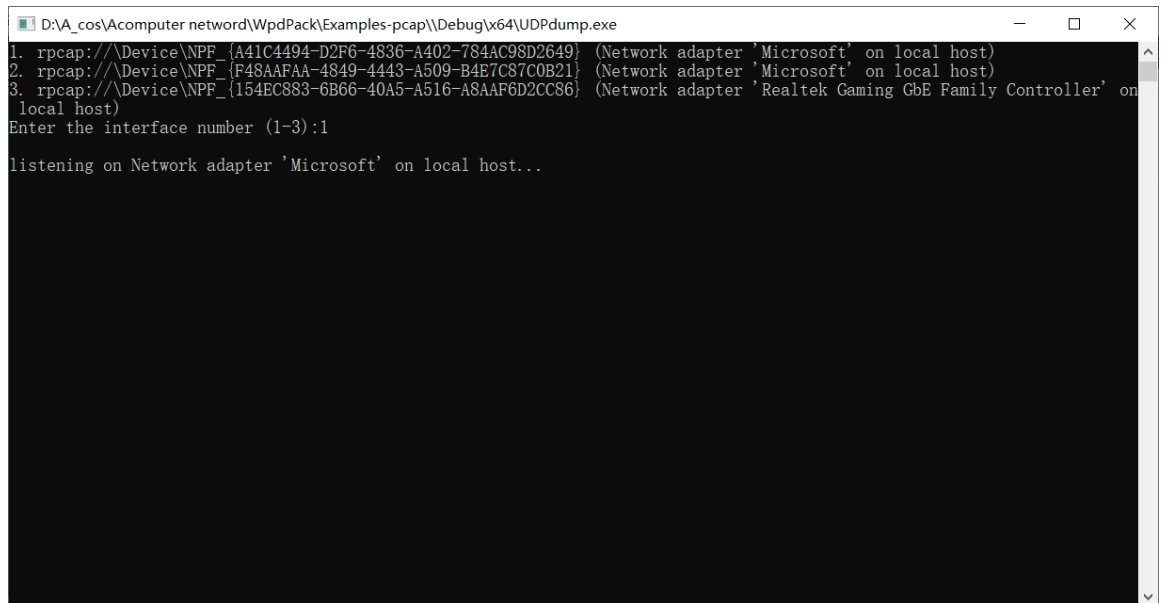
1. 侦听 ftp:\\121.192.180.66 TCP 数据段（前面三次握手，最后四次挥手）



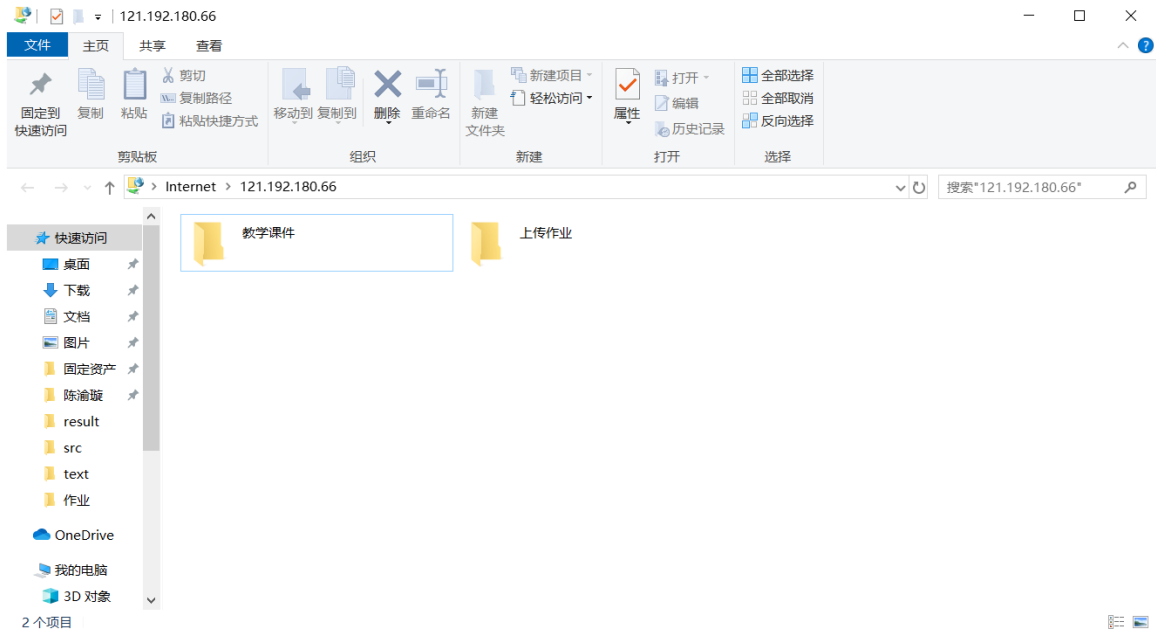
2. 侦听并观察 FTP 数据。登录名以 USER 开头，密码以 PASS 开头，利用这个获取用户名和密码。成功之后以 530 开头，失败以 230 开头。利用这个来判断登录成功与否。



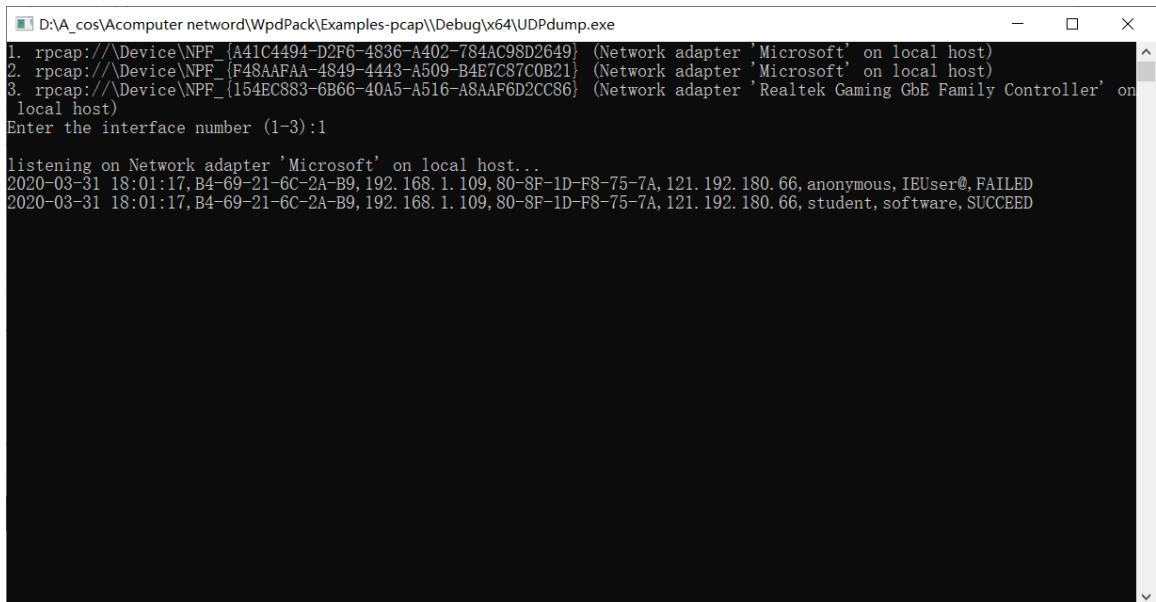
3.运行 WinPCAP 程序



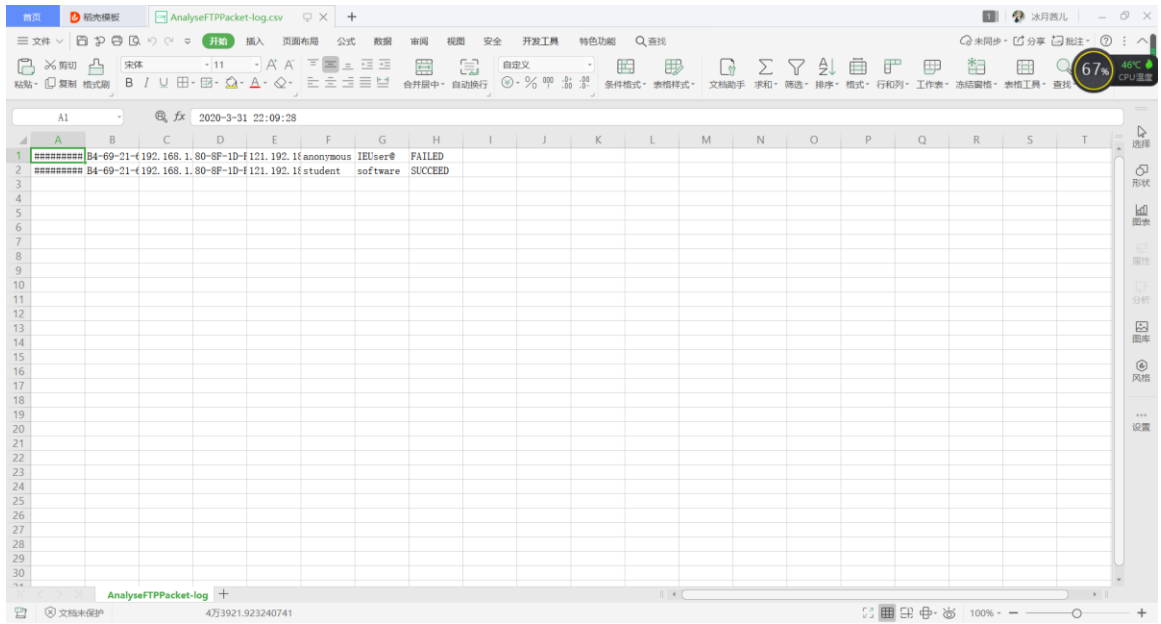
登录 ftp



失败与成功连接



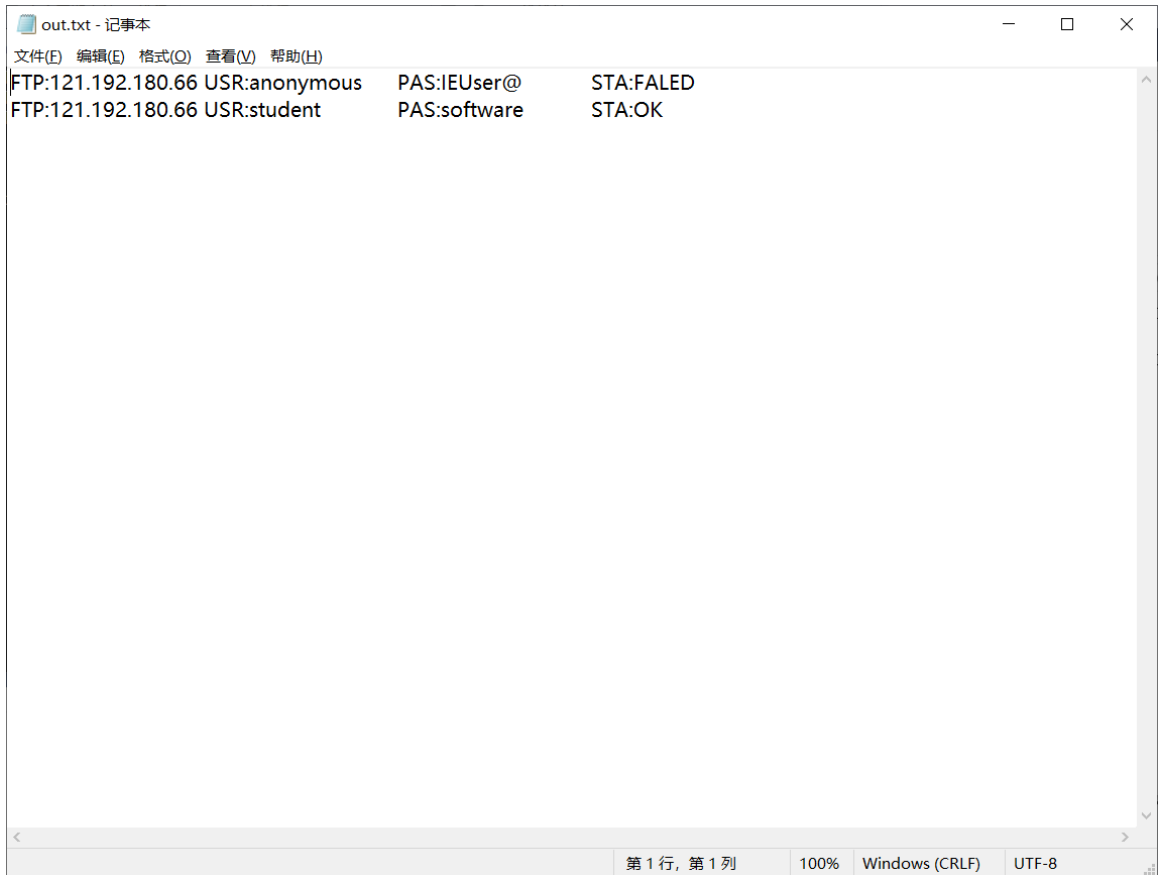
输出 csv 文件



The screenshot shows a WPS spreadsheet titled 'AnalyseFTPPacket-log.csv'. The data is as follows:

	A	B	C	D	E	F	G	H
1	#####	B4-69-21-1	192.168.1.80-8F-1D-F	121.192.1	ifanonymous	IEUser@	FAILED	
2	#####	B4-69-21-1	192.168.1.80-8F-1D-F	121.192.1	ifstudent	software	SUCCESS	

输出文件 out.txt



The screenshot shows a Notepad window titled 'out.txt - 记事本'. The content of the file is:

```
FTP:121.192.180.66 USR:anonymous PAS:IEUser@ STA:FALED
FTP:121.192.180.66 USR:student PAS:software STA:OK
```

4 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。