

****

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 刘明成**

**学　　号 24320182203236**

**实验时间 2020年3月31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撒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

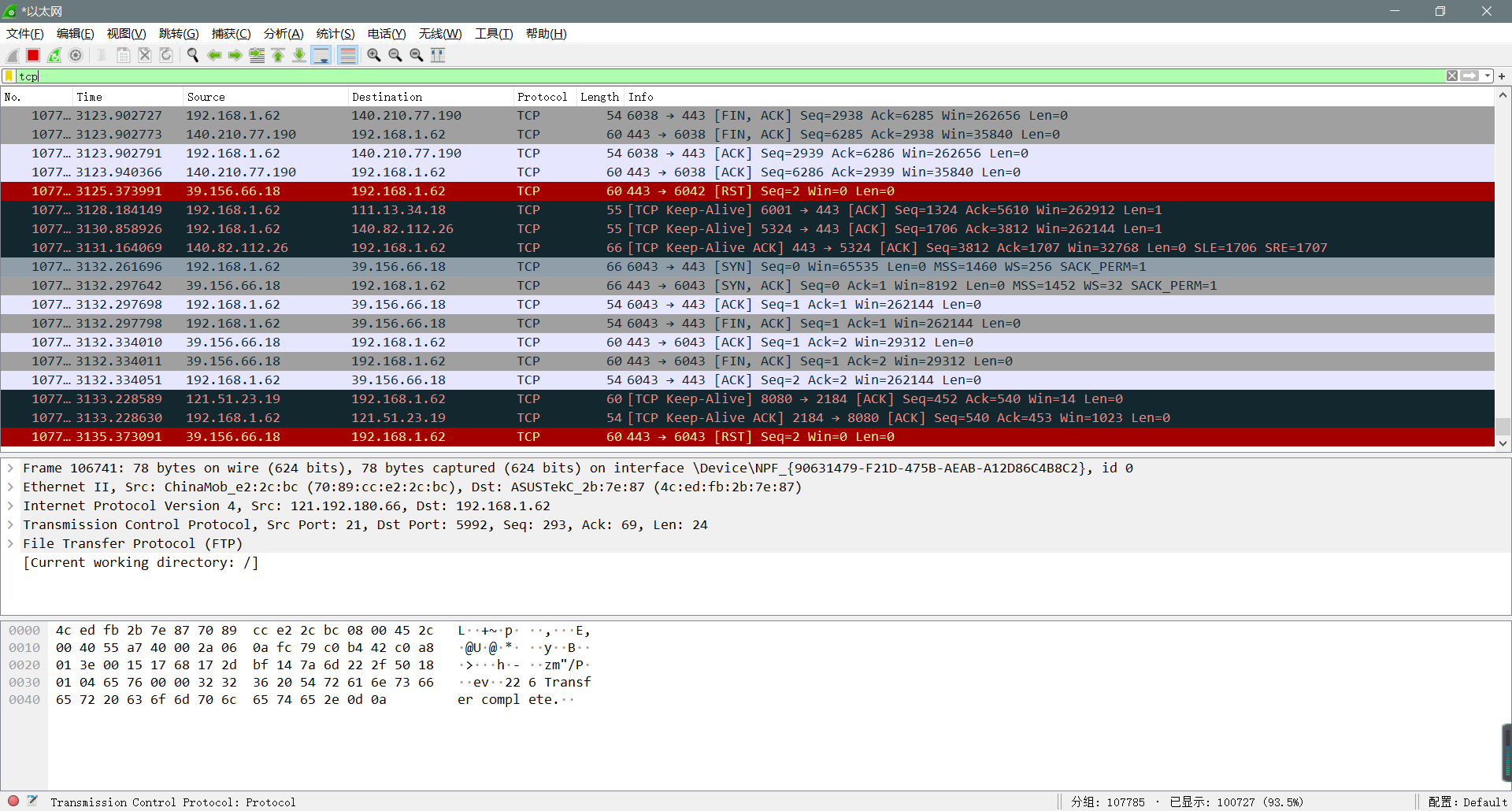
实验机：Windows10 x64位

软件： Visual Studio 2019、Wireshark

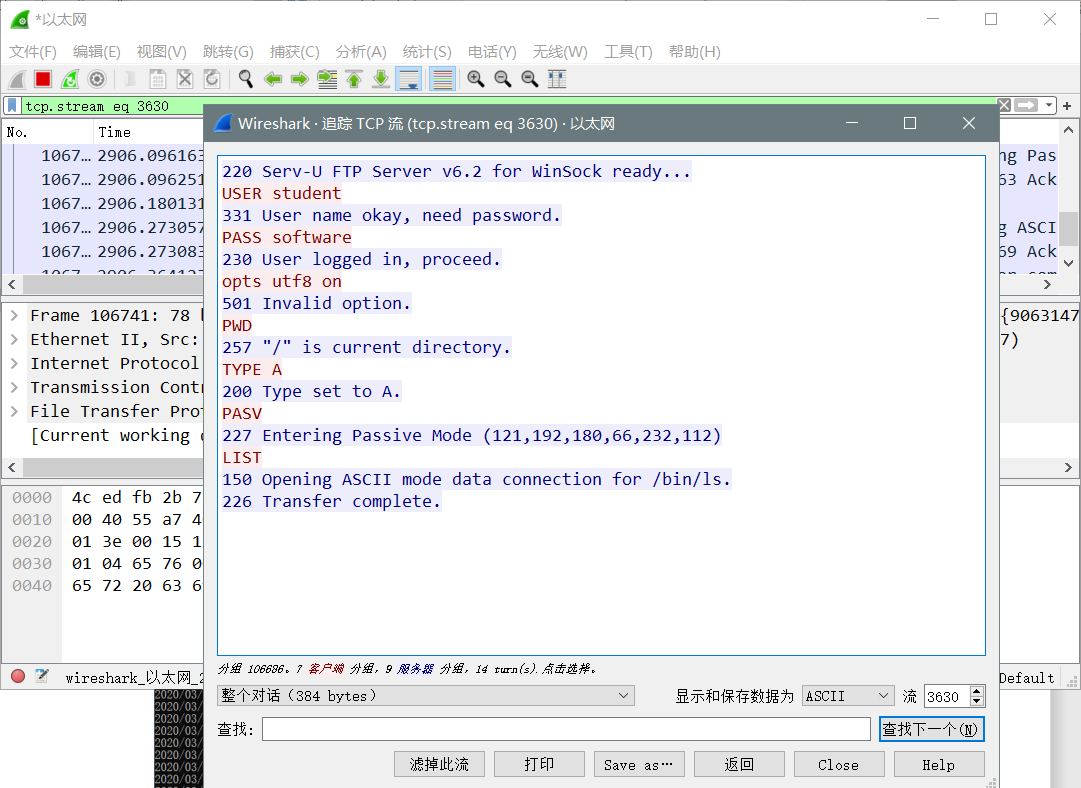
编程语言：C

**3 实验结果**

用Wireshark侦听并观察TCP数据段观察其建立和撒除连接的过程观察段ID、窗口机制和拥塞控制机制等

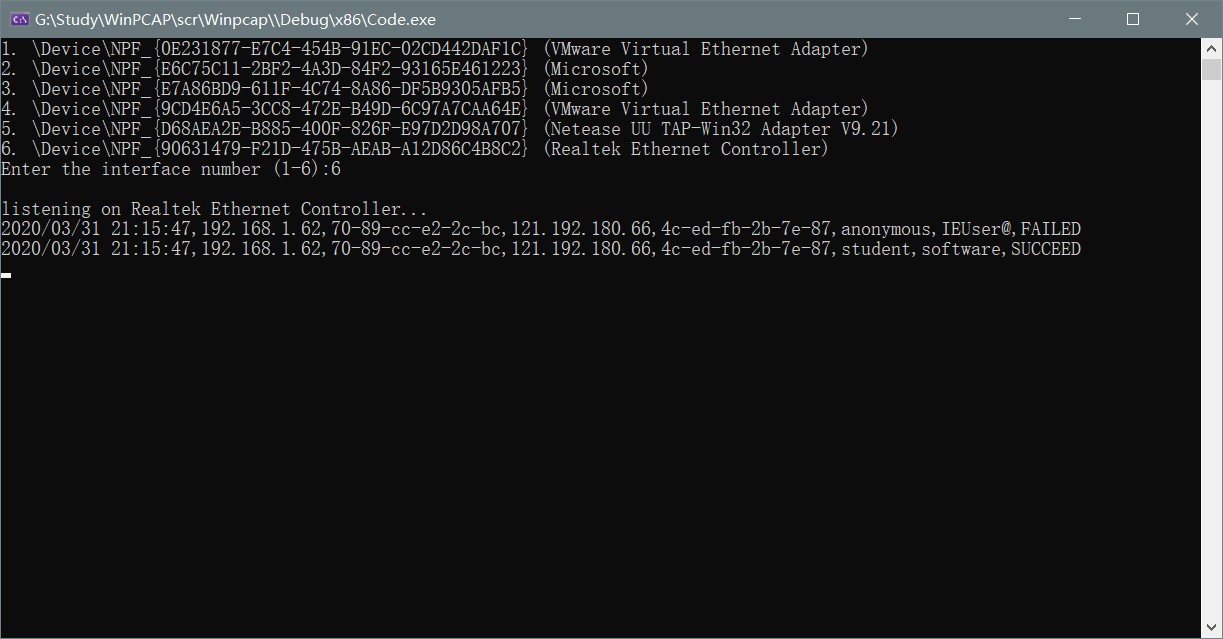


用Wireshark侦听并观察FTP数据，分析其用户名密码所在报文的上下文特征

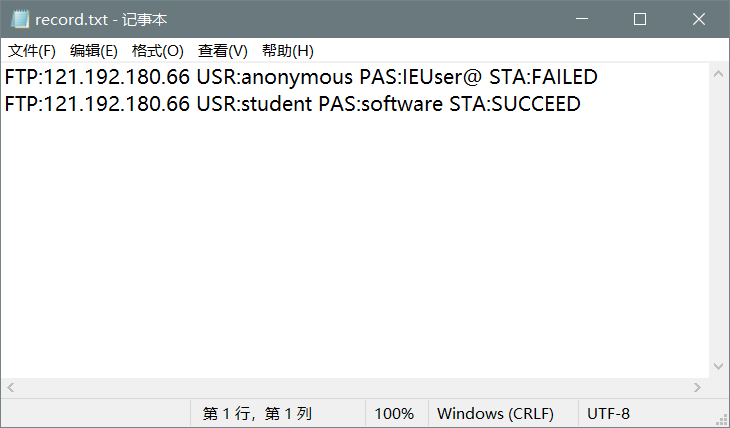


登录报文包括一个头部是USER的包，一个头部是PASS的包，以及头部是230代表成功（530表示登录失败）的包。

监听网络上的FTP数据流，解析协议内容，并作记录与统计：



写入文件：



# 4 实验总结

学习了利用Wireshark侦听并观察TCP与FTP数据段，了解了FTP数据用户名密码所在报文的上下文特征。