

**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 1 班**

**姓 名 林坚**

**学 号 24320182203232**

**实验时间 2020 年 3 月 26 日**

**2020 年 3 月 26 日**

1. **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

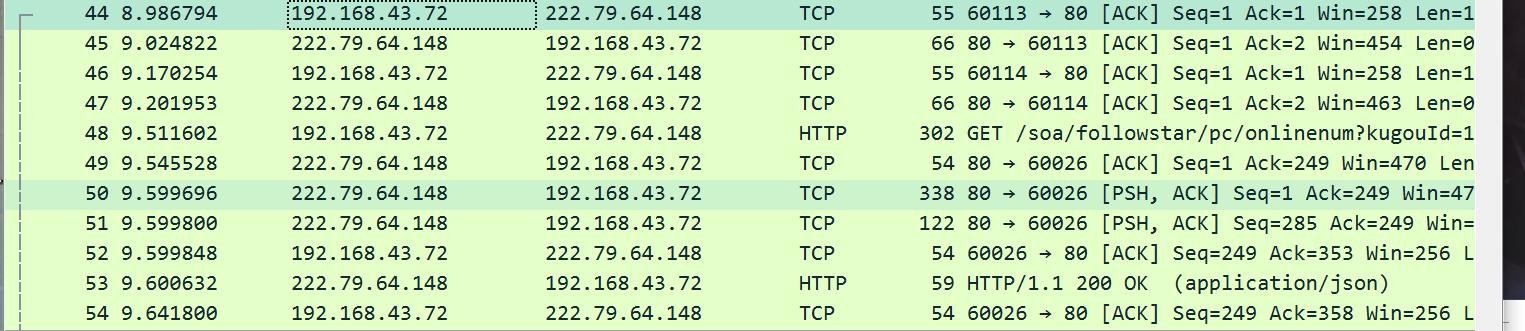
D5-72,192.168.33.2,student,software,SUCCEED

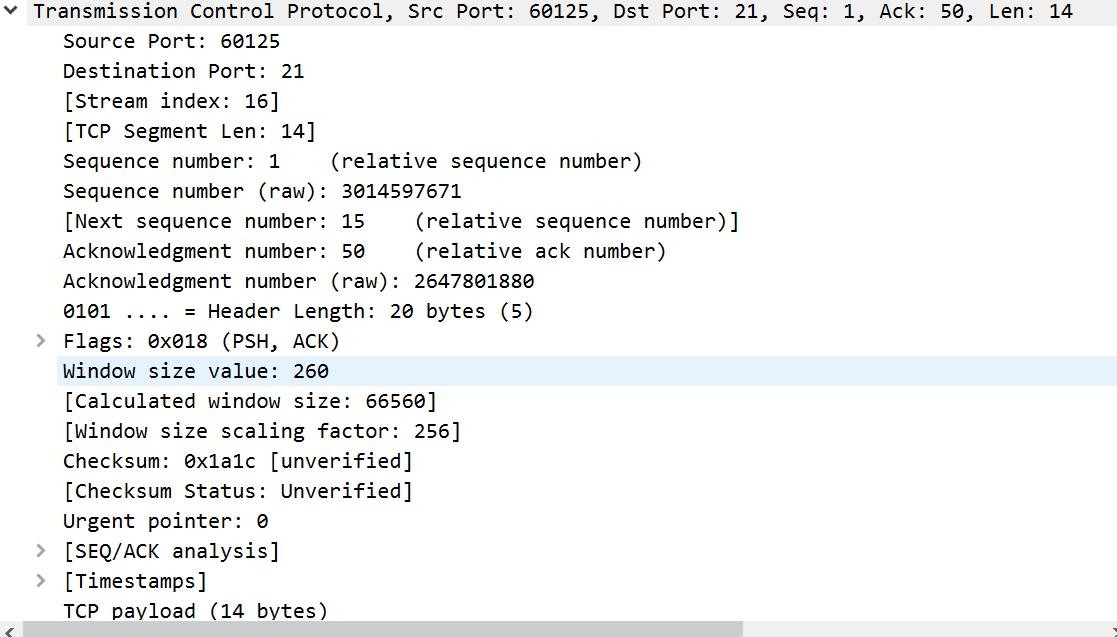
# 实验环境

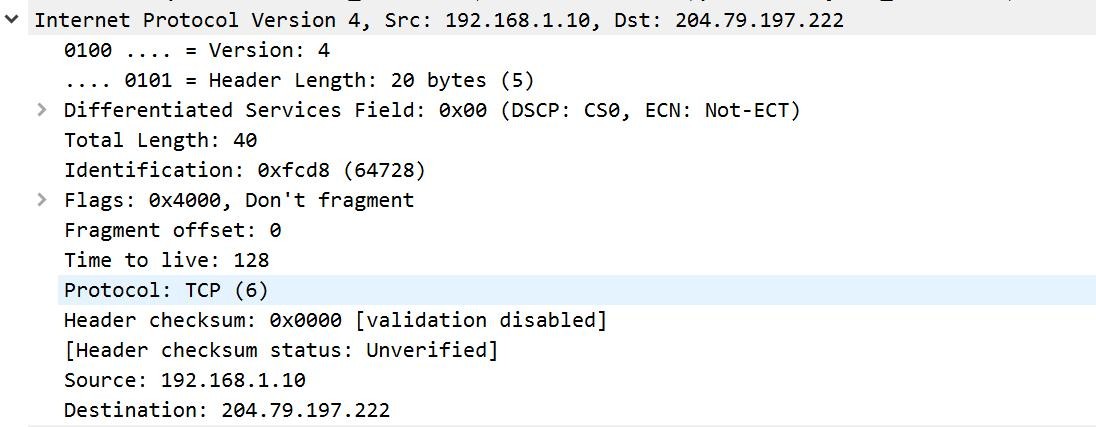
VS2017 ，C++,Winpcap 库

# 实验结果

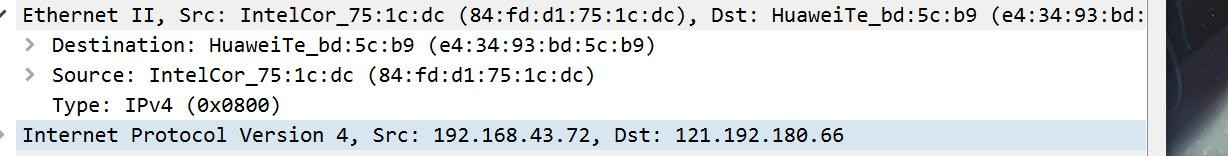
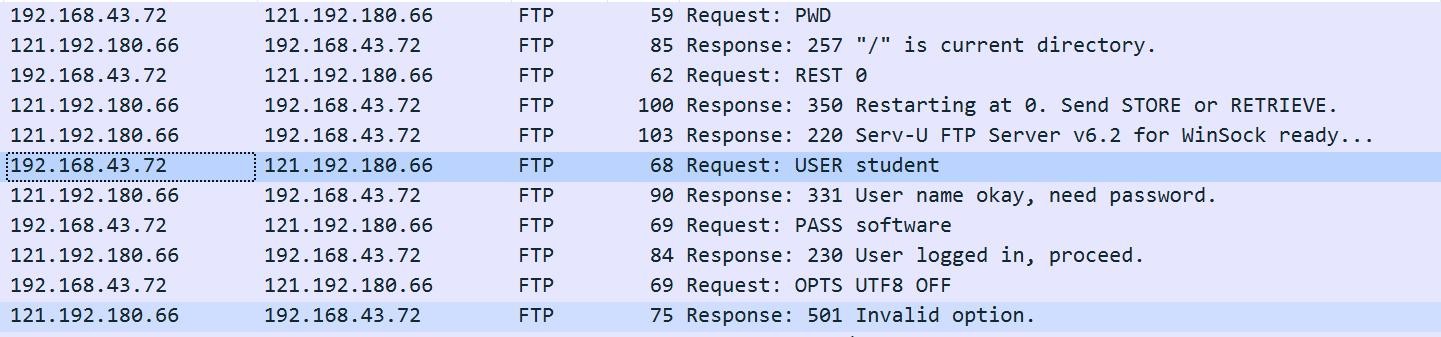
用 Wireshark 侦听并观察 TCP 数据段。观察三次挥手和四次挥手过程

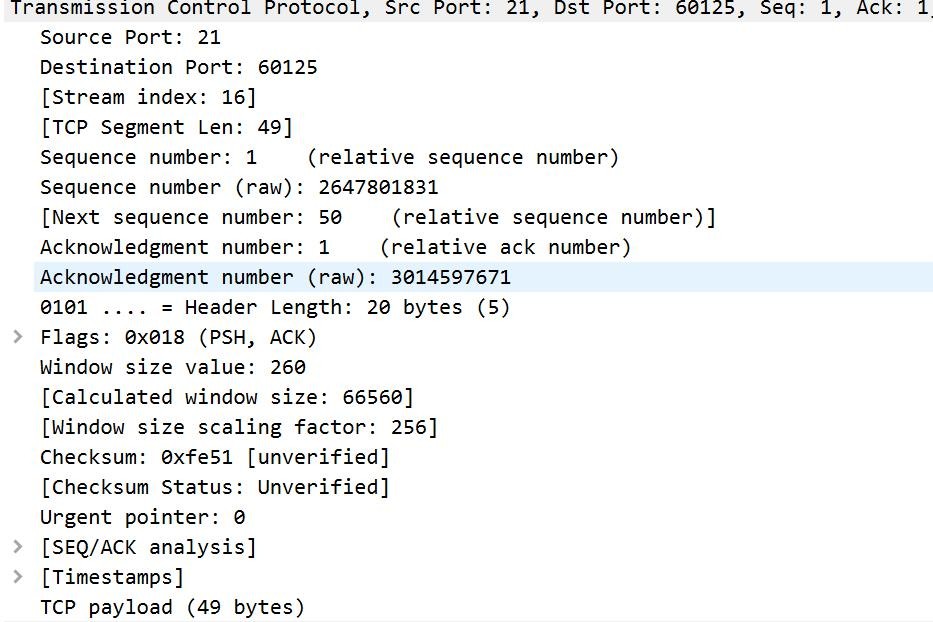


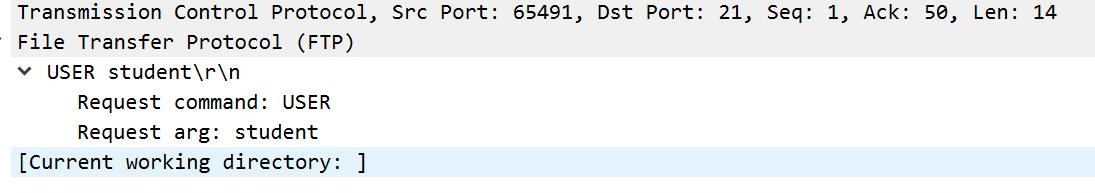




用 Wireshark 侦听并观察 FTP 数据

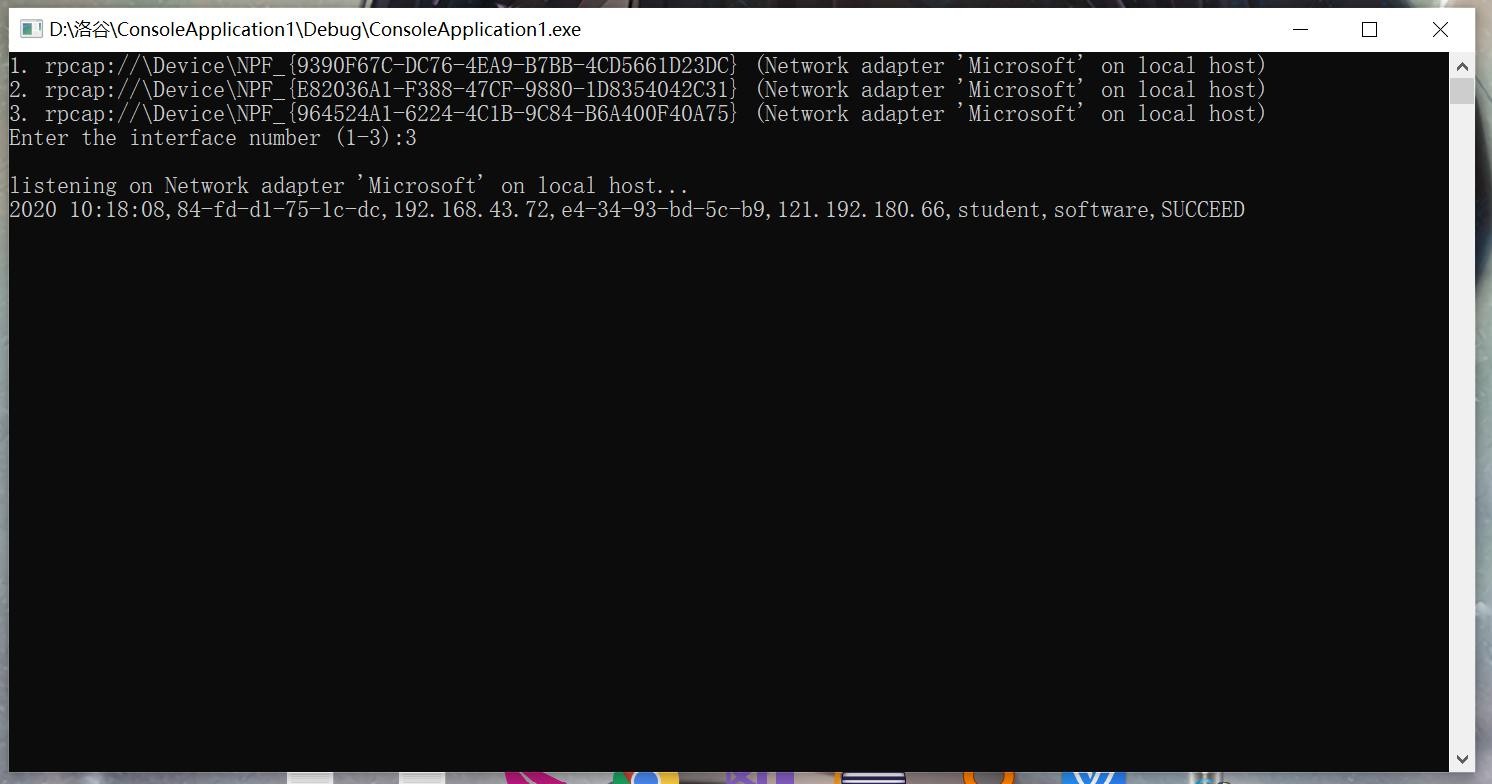




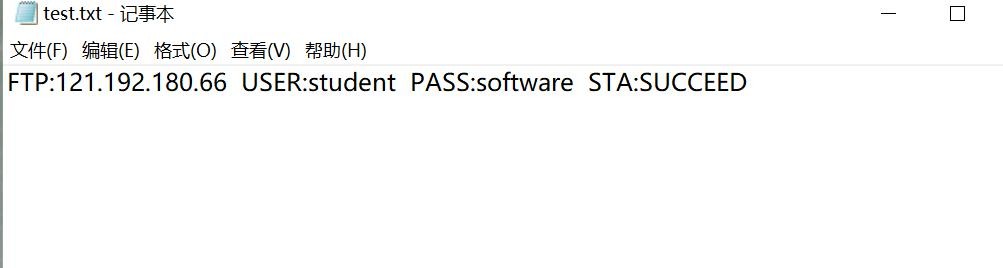


基于 WinPCAP 工具包制作程序，实现监听网

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。



保存到当地 txt 文件里，格式如下



# 实验总结

通过实验的收获，真实总结，勿长篇大论。

总结：对于 FTP 的运作原理有了更深入的认识，对于 TCP 报文握手挥手过程从不了解到大概了解，对于 FTP 登录环节的通信过程有了大概的认识。