

**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 报文段并监听分析FTP 协议**

**班 级 软件工程 2018 级 3 班**

**姓 名 沈黄隽**

**学 号 24320182203260**

**实验时间 2020 年 3 月 23 日**

**2020 年 4 月 7 日**

1. **实验目的**

先用 Omnipeek 或 Wireshark 侦听并观察 TCP 报文段。观察其建立和撤除连

接的过程，观察其报文段 ID、窗口机制和拥塞控制机制等。将其过程截图在报告中。

用 Omnipeek 或 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-

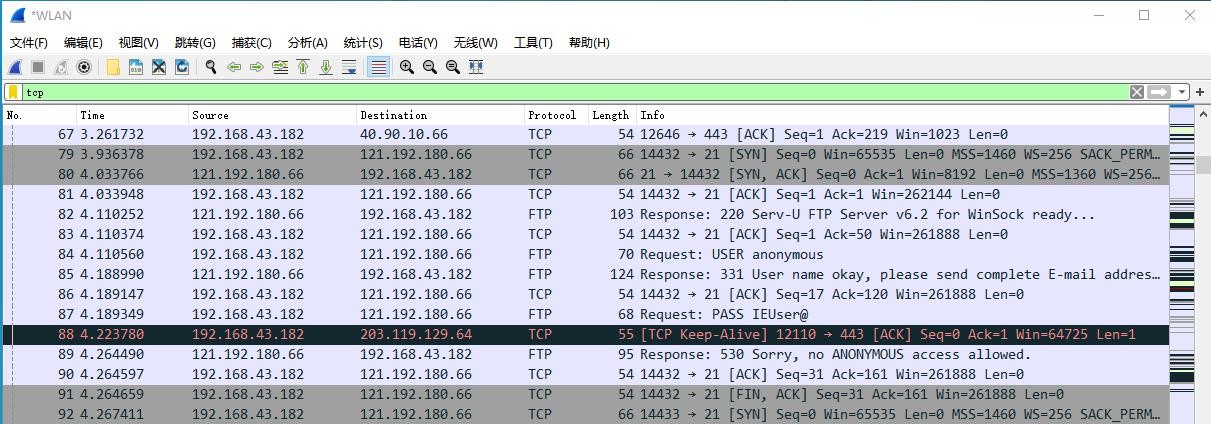
DD-7D-D5-72,192.168.33.2,student,software1,FAILED

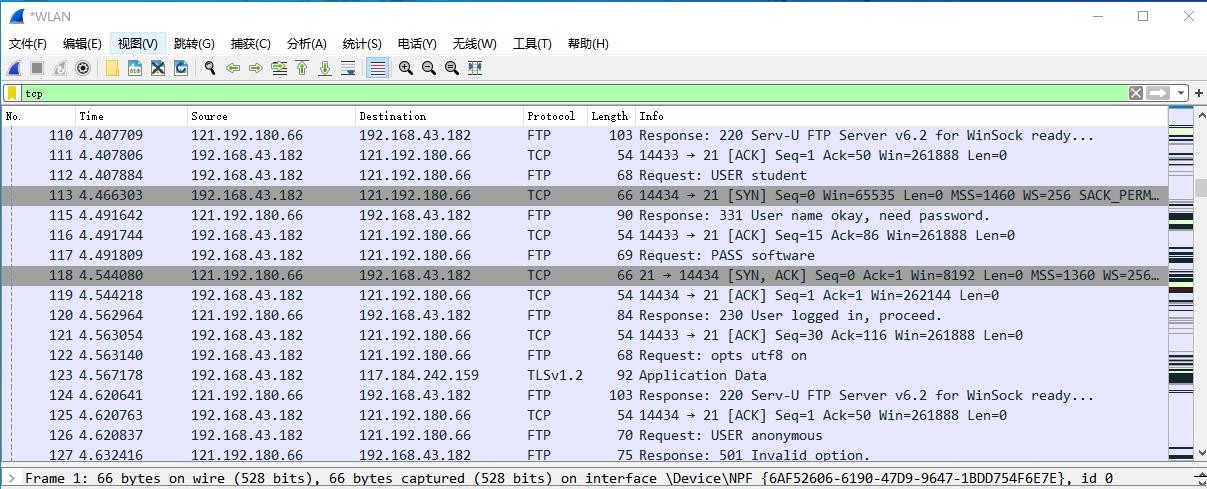
# 实验环境

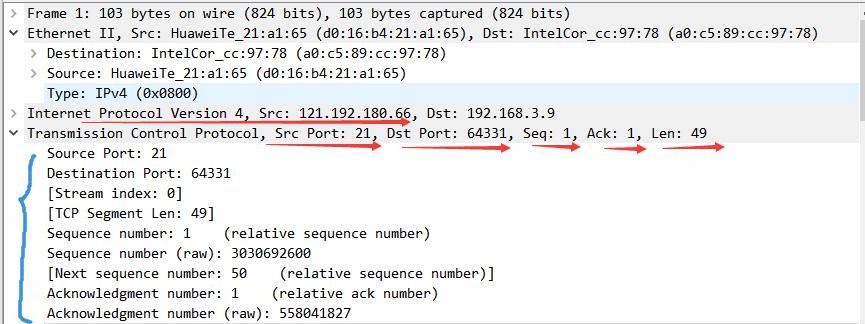
操作环境：Visual Studio 2019、WpdPack、Wireshark

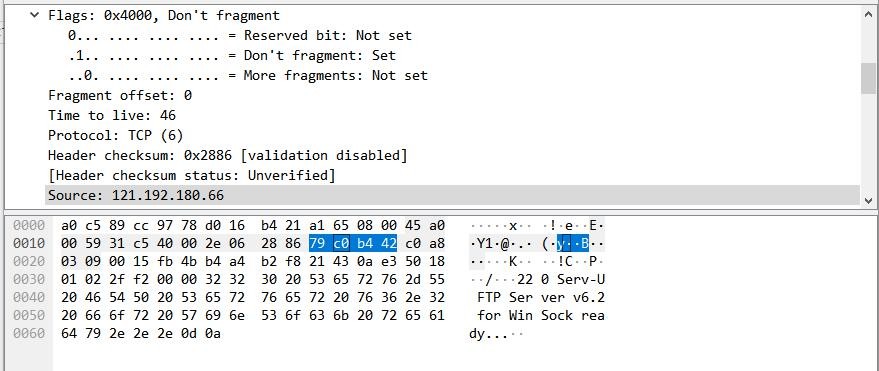
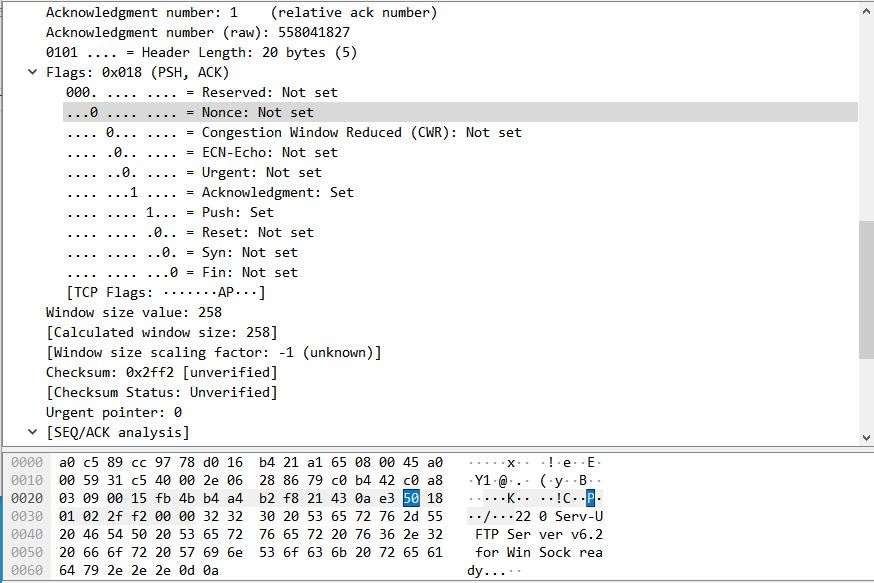
编程语言：C 语言

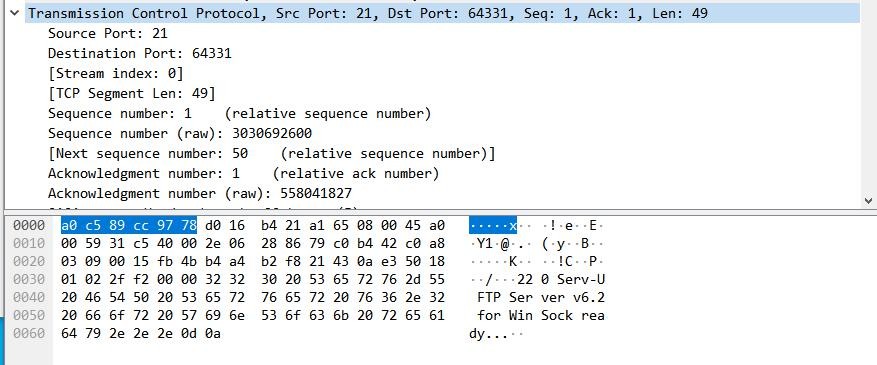
# 实验结果

1、观察 TCP 数据段，观察 Wireshark 对数据的分组形式，观察建立及撤除连接的过程。具体截图如下：

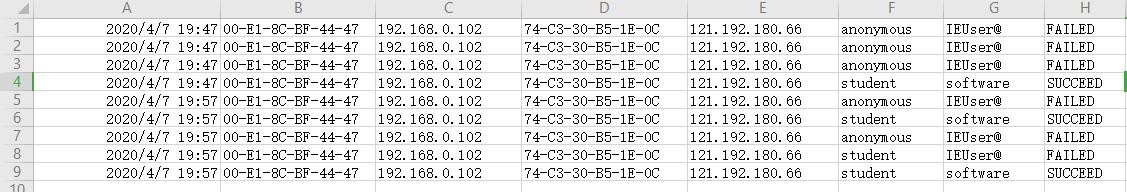


2.观察端口参数，了解 TCP 握手与挥手过程

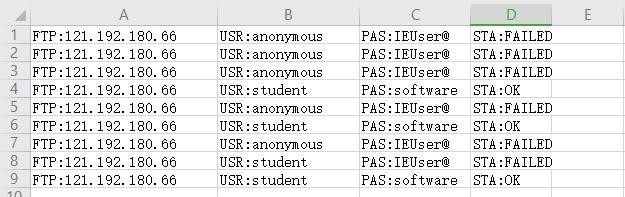




3、最终在文件上输出形如下列 CSV 格式的日志：

时间、源 MAC、源 IP、目标 MAC、目标 IP、登录名、口令、成功与否

表格输出到硬盘的形式如下：



# 实验总结

用 Wireshark 软件对 FTP 通信时的网络分组进行了侦听操作，观察了解TCP 握手和挥手的过程。对 FTP 的通信协议的过程有了更为深入的理解，且在此基础编程能力得到提升。