

****

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 汪文青**

**学　　号 24320182203276**

**实验时间 2020年3月26日**

**2020 年 4 月 7 日**

# 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

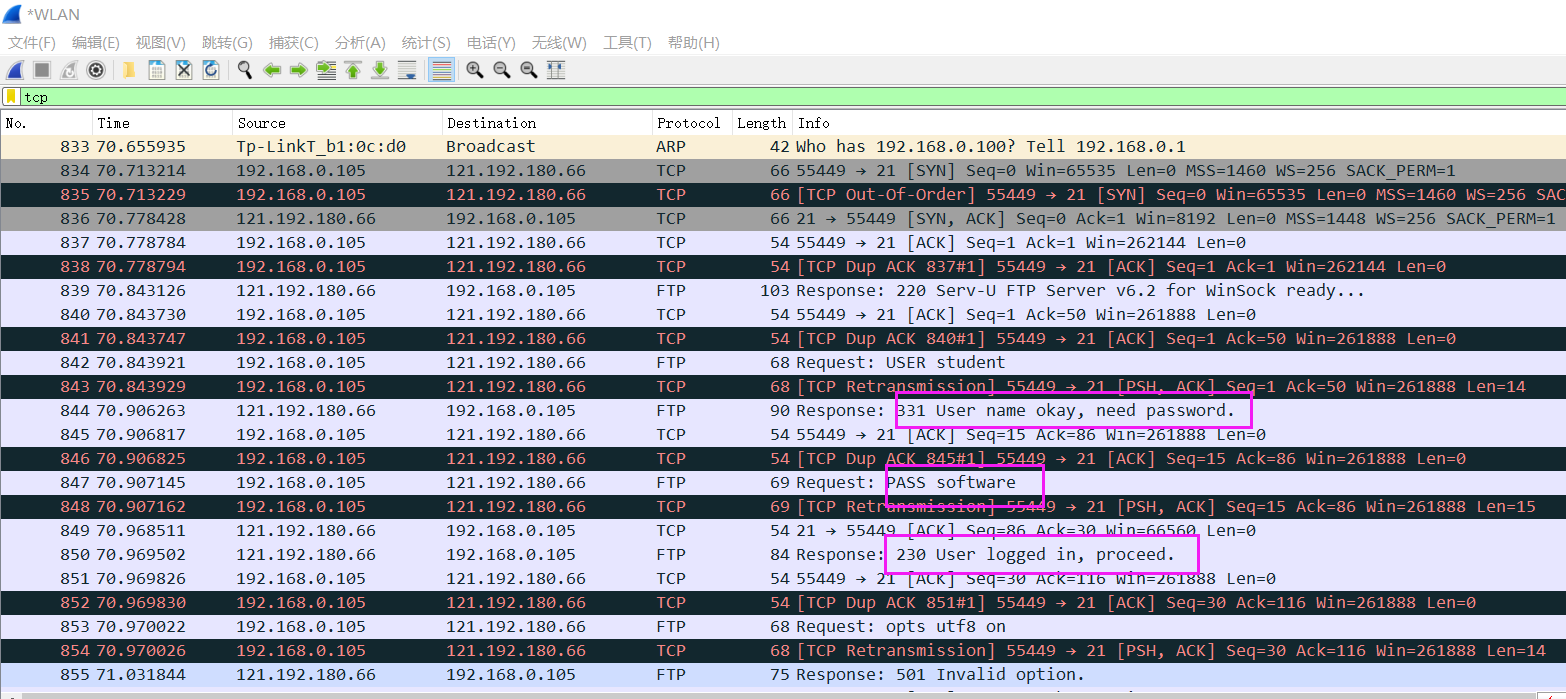
2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D5-72,192.168.33.2,student,software,SUCCEED

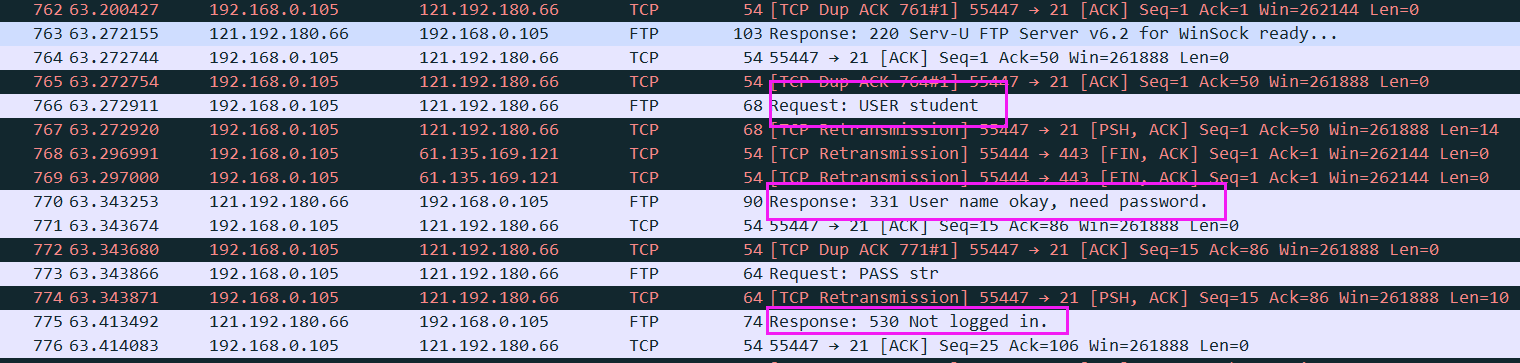
2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D5-72,192.168.33.2,student,software1,FAILED。

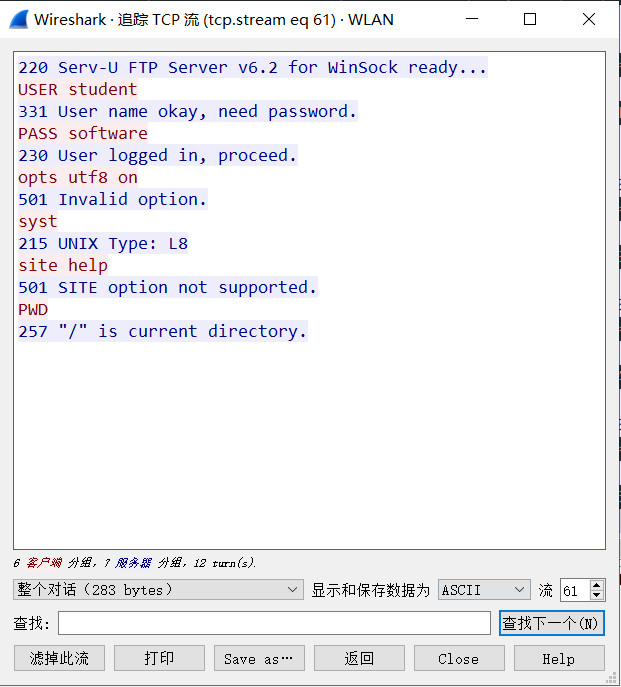
# 实验环境

Windows 10 , visual studio 2019 , 编程语言 c, WinPCAP 工具包

# 实验结果

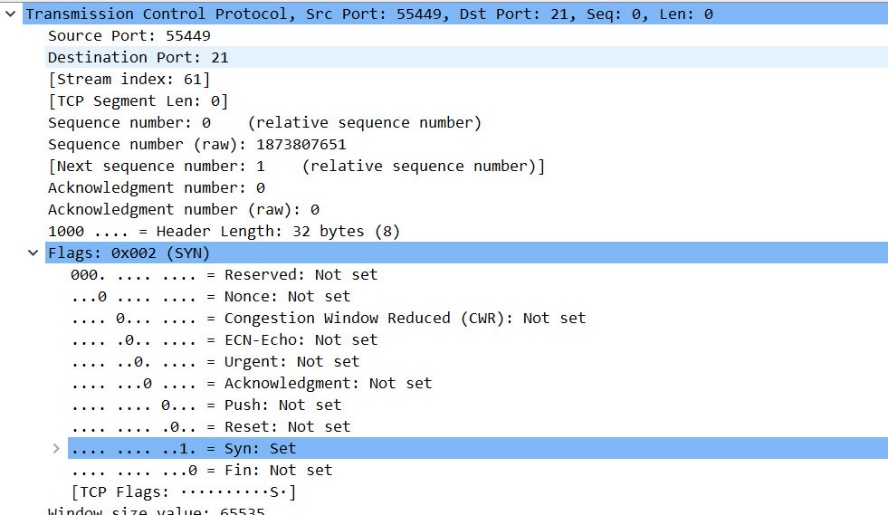






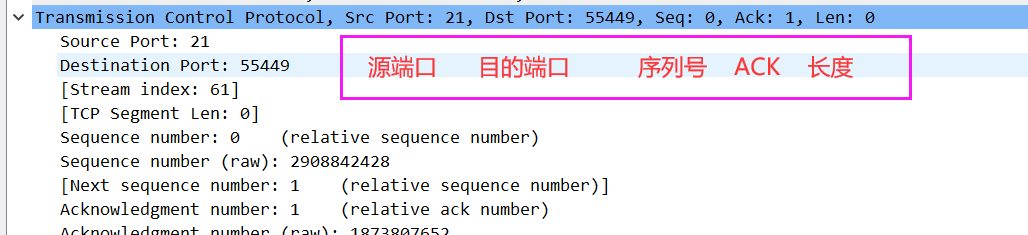
1. 观察第一个TCP报文段:客户端想服务器发送的请求连接包。

重要的数据,SYN=1, seq=0 (sequence number),表示连接请求。



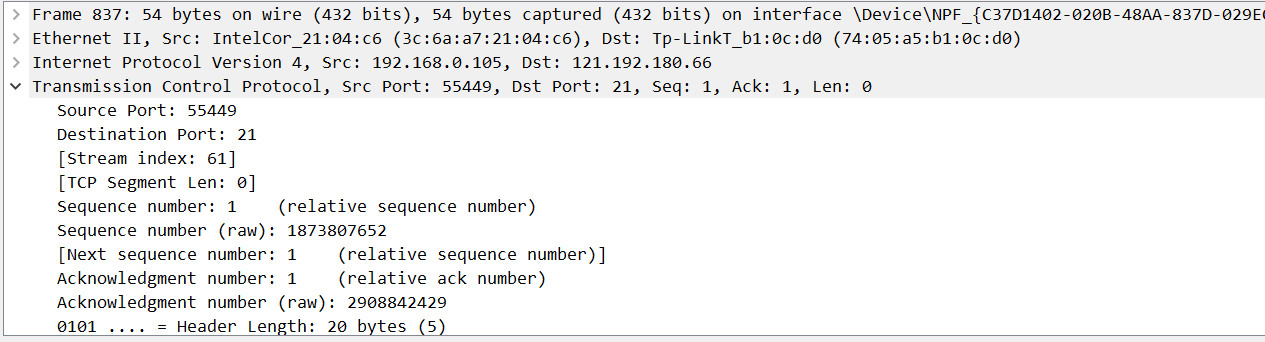
1. 第二个TCP报文段:服务器向客户端发送的确认报文段。

重要数据,SYN=1,seq=0,ACK=1(并不ACK number,值为1时,表示确认字段 有效),ACK number=1(这个才是确认号,表示期望收到对方下一段报文段的 第一个数据字节的序号sequence number,也就是说希望下一段的seq=1,这个也表示1之前的数据包已经接受了)



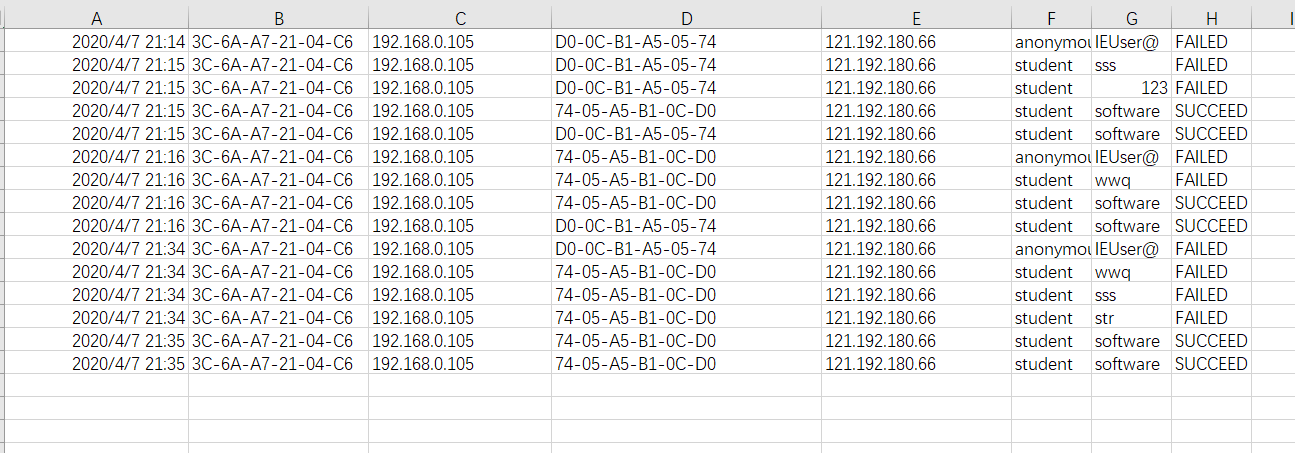
3.第三个TCP报文段:客户端向服务器发送的确认报文段

重要数据,ACK=1, seq=1, ACK number=1

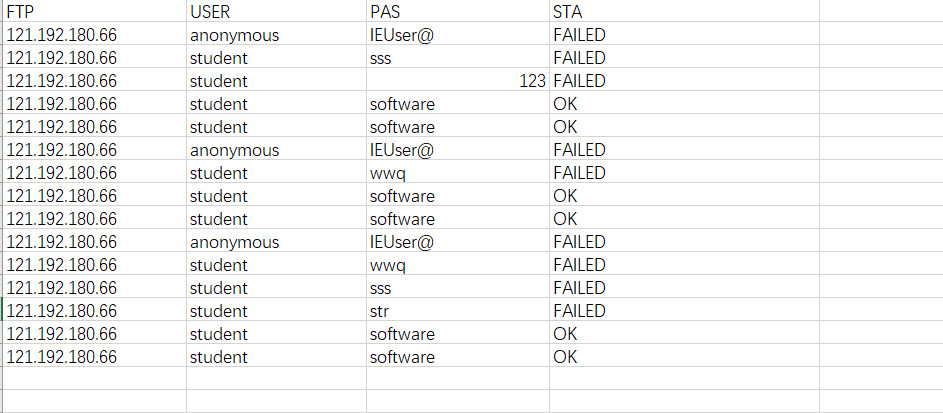


最终在文件上输出形如下列 CSV 格式的日志：

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



多次登陆学院FTP 将监听到的上述信息以表格形式输出到硬盘中。程序输出格式实例如下：



# 实验总结

学习并分析了TCP数据包的结构、含义。分析了TCP连接的建立过程和数据传输过程，观察了TCP 握手和挥手的过程。在wireshark中要注意区分ACK和ACK number。