

****

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B班**

**姓　　名 彭书浩**

**学　　号 24320182203251**

**实验时间 2020年3月25日**

**2020 年 3 月 29 日**

# 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。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-7DD5-72,192.168.33.2,student,software,SUCCEED

2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7DD5-72,192.168.33.2,student,software1,FAILED

# 实验环境

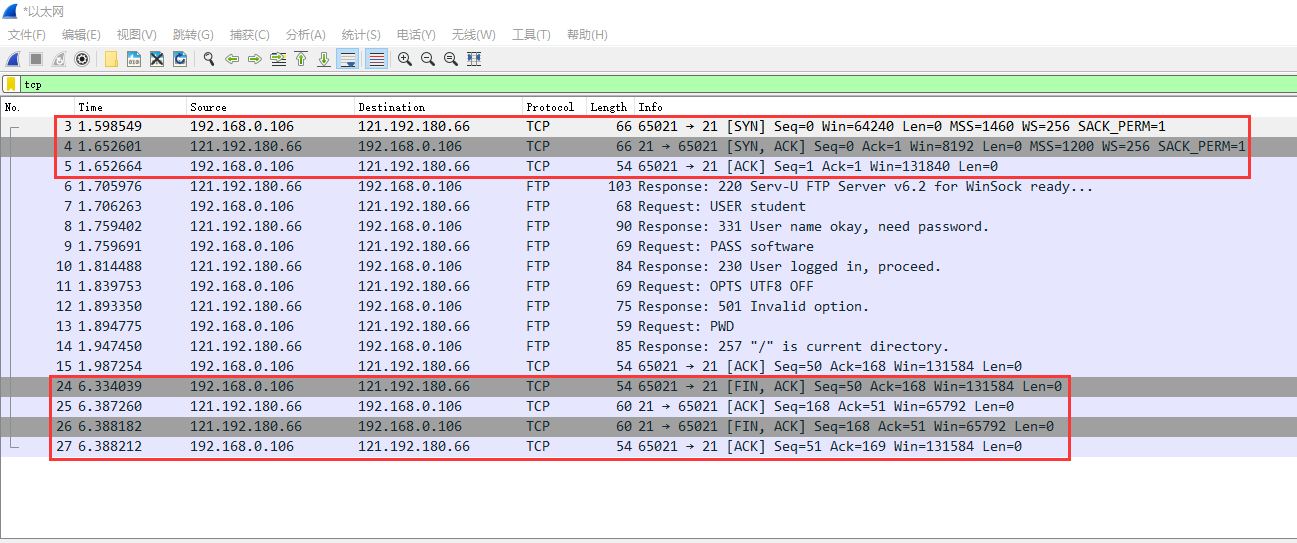
Windows 10操作系统

-WinPCAP；WireShark；科来数据包播放器

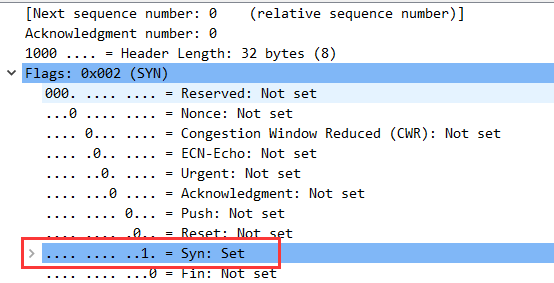
# 实验结果

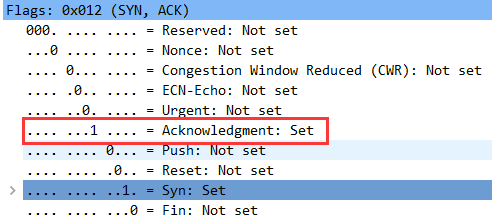
1、用Wireshark侦听并观察TCP/FTP数据段：

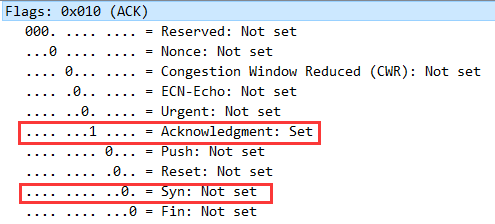
收到开头3次握手数据包、结尾4次握手数据包：



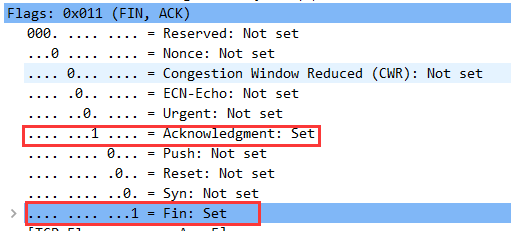
开始3次标志位结果：

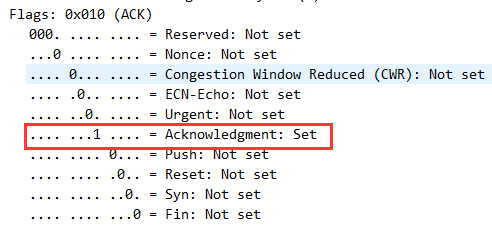






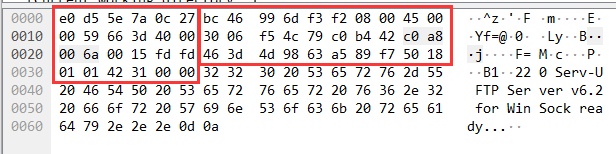
结束两对标志位结果：



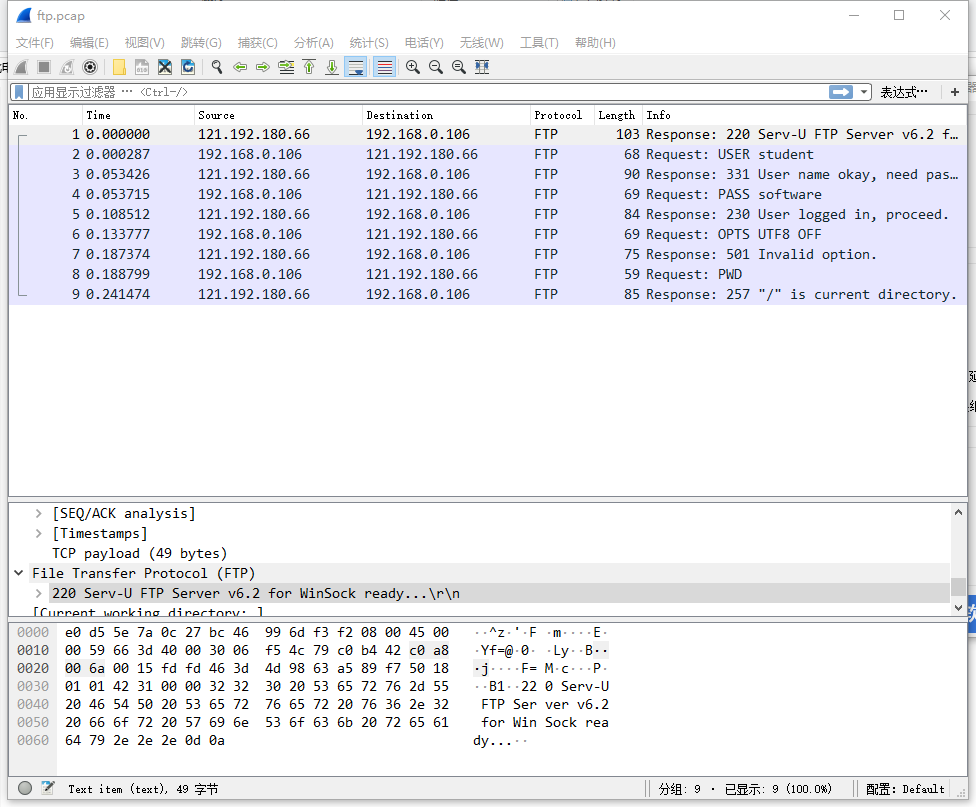


1. 用 Wireshark 侦听并观察 FTP 数据进行分析

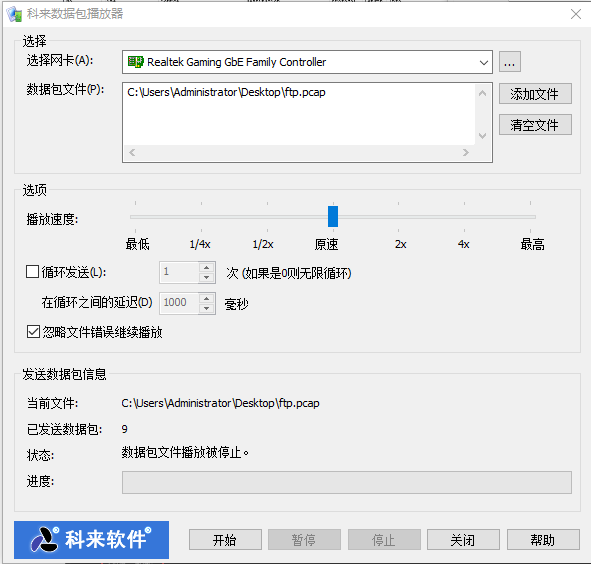
前54字的内容是信息头，后面内容为数据段：



1. WireShark将连接ftp产生的ftp数据包生成pcap文件由程序读取。

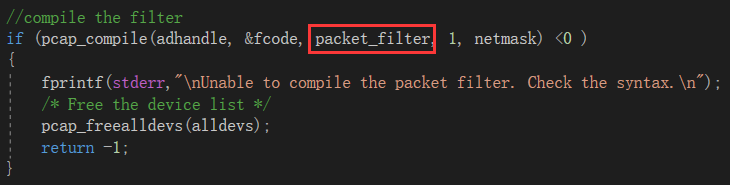


1. 用科来播放器重发pcap文件，由程序网卡接收。

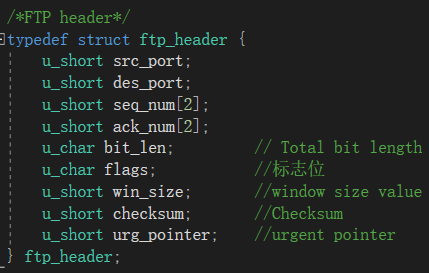


1. 用wincap的过滤器来过滤数据包，只接收ftp数据包。

IMG_256

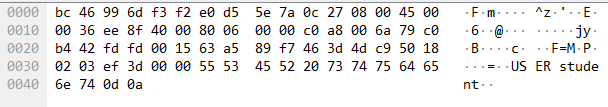


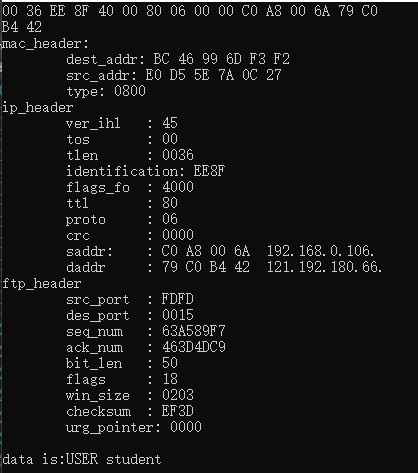
1. 根据ftp数据分析结果，改写程序。



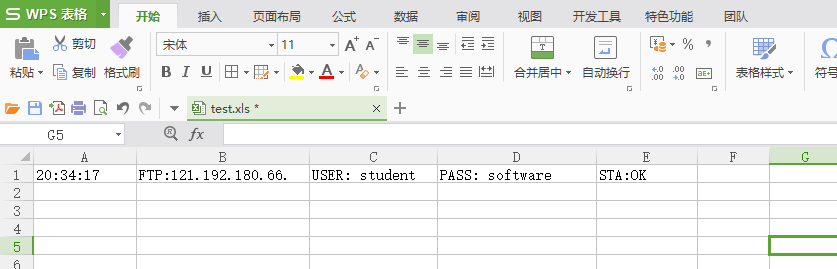
1. 程序运行，通过科来重新发送ftp数据包，输出结果。

以发送用户名的ftp数据包为例：





最后输出到表格中的数据：



# 实验总结

1、代码中采用了一个ntohs（）函数，用于16进制数据的输出。由于数据的储存方式是字节大端序位小端序，故用此函数以原格式输出数据。

2、 FTP协议是TCP/IP协议的一部分，严格意义上来说是应用层协议，它定义了本地登录户机与远程服务器之间的交互过程。采用过滤器过滤时有其特有的格式。

1. ftp数据段的结尾是以/r/n结尾的，输出数据时应把它们排除。
2. 拔除网线后，使用科来数据播放器重新发送数据包时，网卡不会发送与接收任何数据。