

****

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 王薪蕾**

**学　　号 24320182203285**

**实验时间 2020年3月25日**

**2020 年 3月 25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

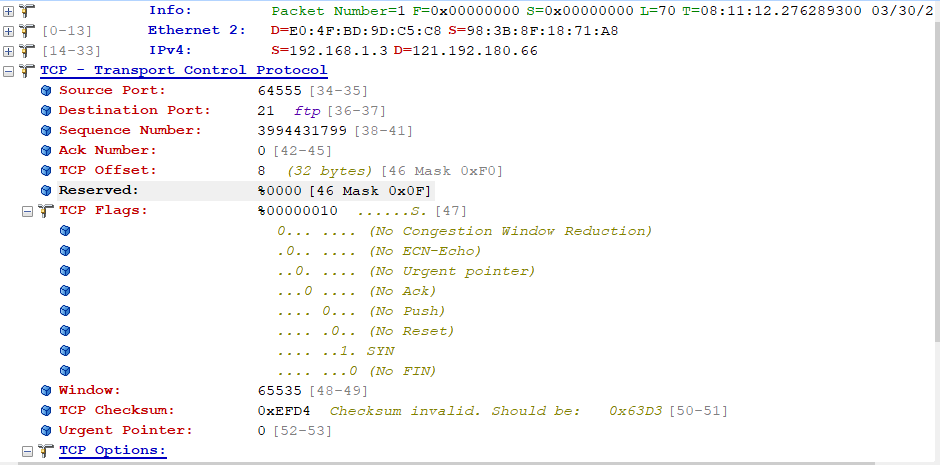
# 实验环境

操作系统：windows，编程语言：C++

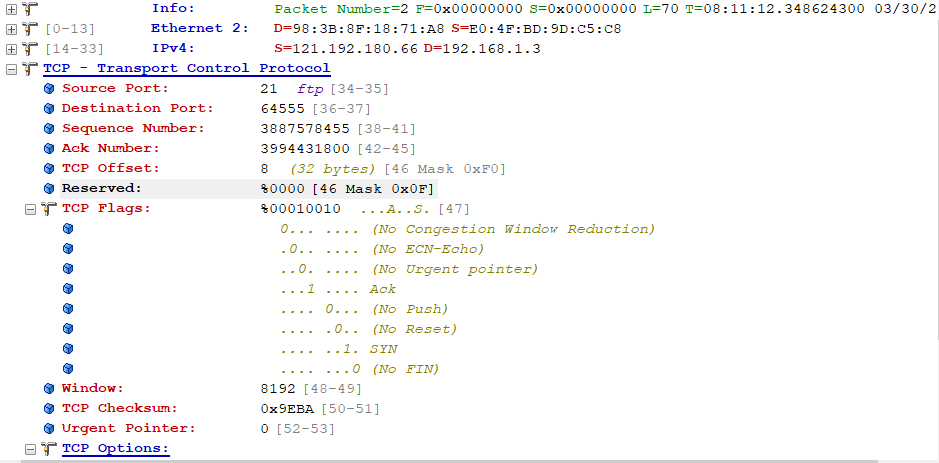
# 实验结果

建立时三次握手

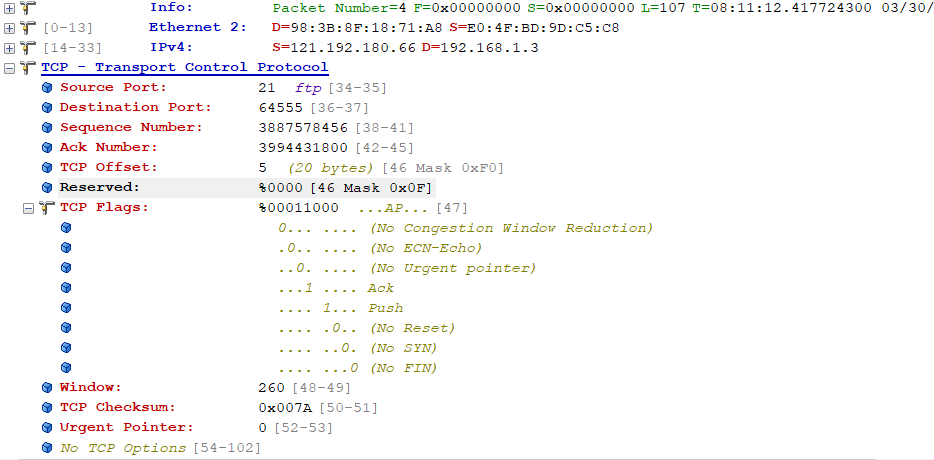
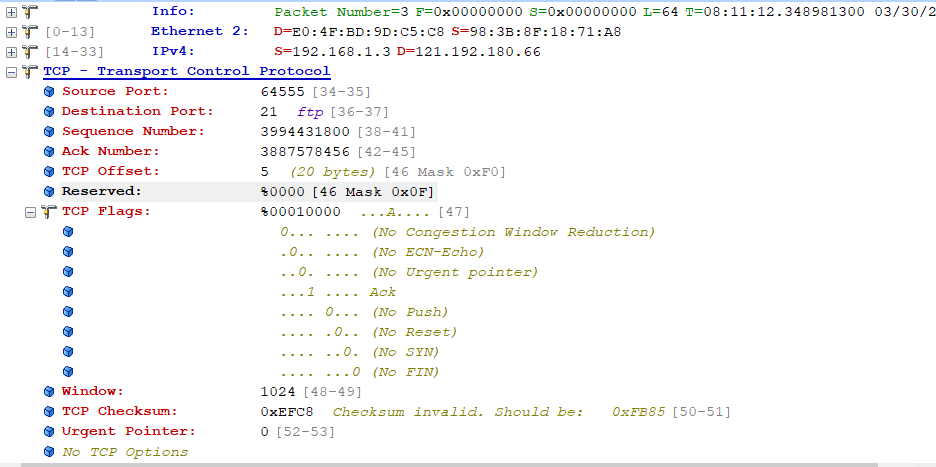
Syn建立🡪ftp



ftp🡪Ack有效syn建立



Ack有效🡪ftp

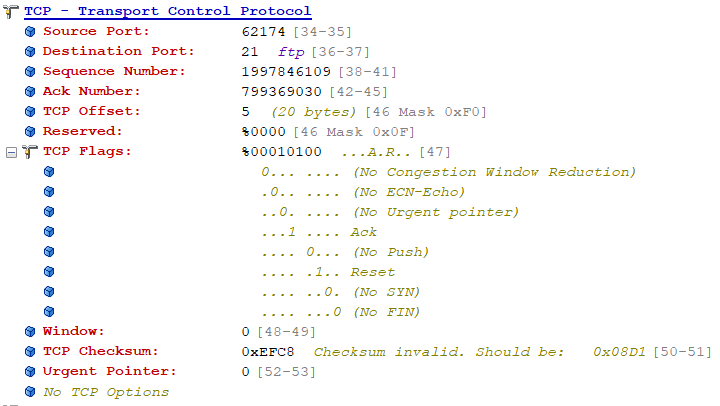


断开时如果直接关闭窗口，WinPcap无法捕捉到包

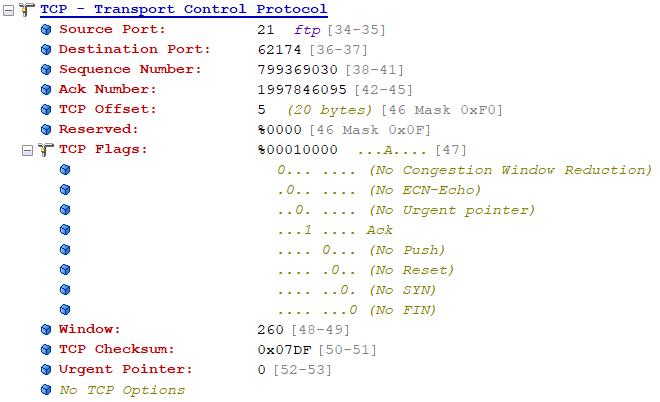
用命令行连接时出现‘远程主机关闭连接’的错误

此时抓到这样的包

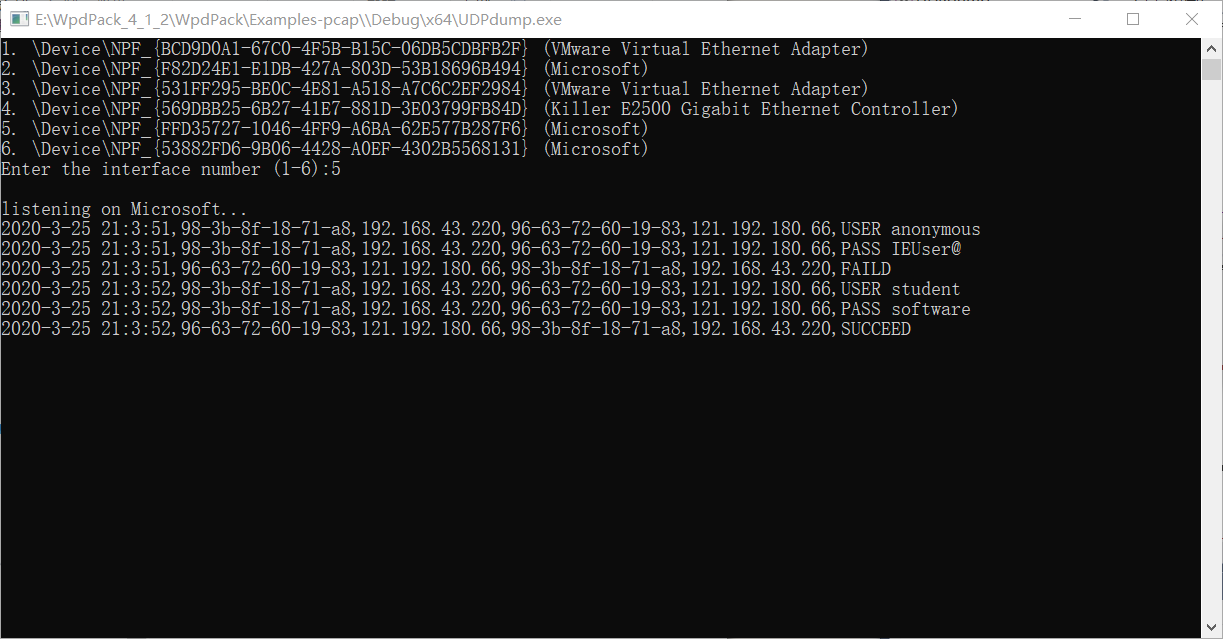
RST 复位TCP连接🡪ftp



ftp🡪ACK



编程的输出图：



# 实验总结

学习了ftp的TCP握手协议，其连接、终止

怎么从包中分析出用户名、密码和是否成功连接