

****

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3班**

**姓　　名 饶龙宇**

**学　　号 24320182203256**

**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：

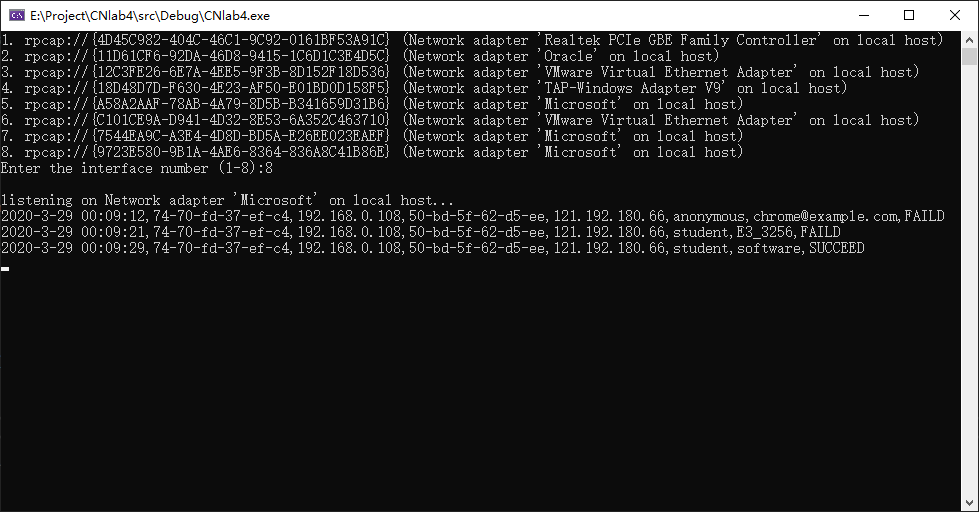
时间、源 MAC、源 IP、目标 MAC、目标 IP、登录名、口令、成功与否

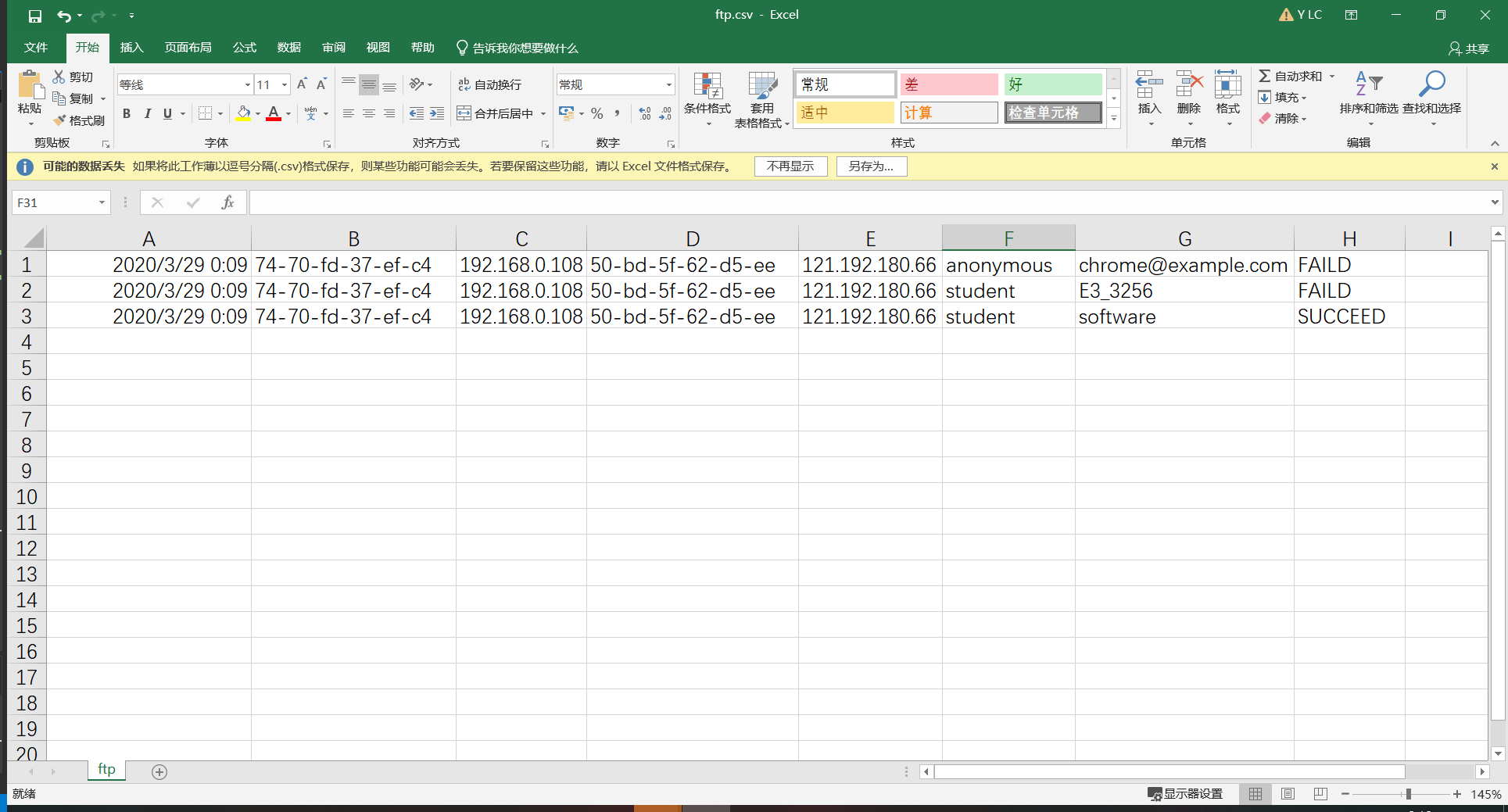
# 实验环境

编程环境：Windows10 Visual Studio 2019

编程语言：C++

# 实验结果

1.控制台输出



2.监听网络上的 FTP 数据流，解析协议内容，并作记录与统计，形成CSV格式的日志。

# 实验总结

通过本次实验，我较实验三对winPcap库的使用有了更深的理解，但是遇到打开本地FTP服务器时无法监听到数据包的问题，只能借助于学院的FTP服务器，还未解决。