

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三**基于 PCAP 库侦听并分析网络流量

**班　　级 软件工程2019级1班**

**姓　　名 石伟宁**

**学　　号 22920192204269**

**实验时间 2021年4月06日**

**2021 年 4 月 06 日**

填写说明

1. 本文件为Word模板文件，建议使用Microsoft Word 2019打开，在可填写的区域中如实填写；
2. 填表时，勿破坏排版，勿修改字体字号，打印成PDF文件提交；
3. 文件总大小尽量控制在1MB以下，勿超过5MB；
4. 材料清单上传在代码托管平台上；
5. 在学期末将报告按“CNI-E1-00020190000000-张三”的命名后（其中E1是Experiment 1的缩写），压缩为zip文件，作为附件，以“计算机网络-实验报告-00020190000000-张三”发送至cni21@qq.com。

# 实验目的

通过完成项目，理解数据链路层、网络层、传输层和应用层的基本原理。掌握用 Libpcap 或 WinPcap 库侦听并处理以太网帧和 IP 报文的方法；熟悉以太网帧和 IP 报 文的概念，熟悉帧头部或 IP 报文头部各字段的含义。了解 Libpcap 或 WinPcap 库的结 构和基本原理。

# 实验环境

win10，c++语言

# 实验结果

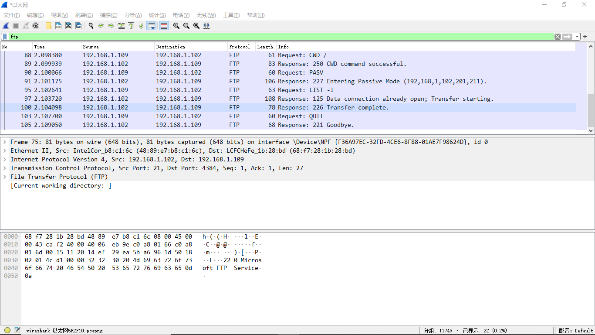
1、用侦听解析软件观察数据格式 用 Wireshark 或 Omnipeek 等网络侦听软件网络上的数据流，验证理论课讲 授的网络协议层次嵌套，验证帧格式、IP 报文格式、TCP 段格式和 FTP 协议命 令和响应的格式，验证 MAC 地址、IP 地址、TCP 端口等协议地址格式。

2、用侦听解析软件观察 TCP 机制 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。

3、用 Libpcap 或 WinPcap 库侦听网络数据 用 Libpcap 或 WinPcap 库侦听网络上的数据流，解析发送方与接收方的 MAC 和 IP 地址，并作记录与统计。

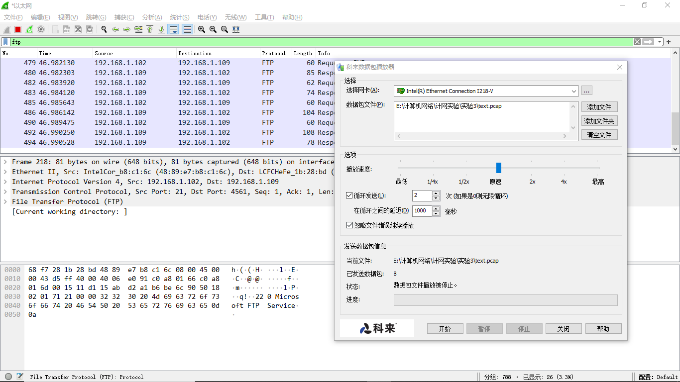
程序在文件上输出形如下列 CSV 格式的日志： 时间、源 MAC、源 IP、目标 MAC、目标 IP、帧长度（以逗号间隔） 2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36- DD-7D-D5-72,192.168.33.2,1536 每隔一段时间（如 1 分钟），程序统计来自不同 MAC 和 IP 地址的通信数 据长度，统计发至不同 MAC 和 IP 地址的通信数据长度。

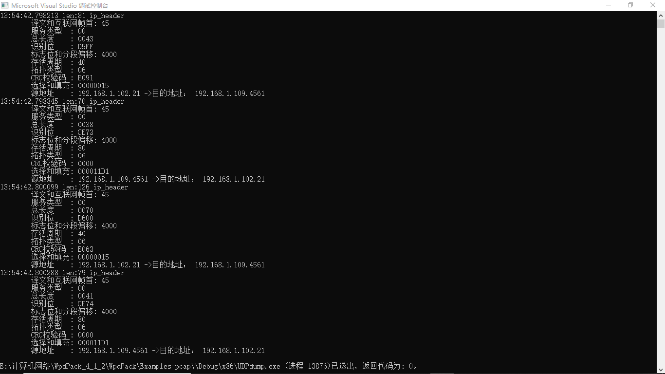
4、解析侦听到的网络数据 用 Wireshark 侦听并观察 FTP 数据，分析其用户名密码所在报文的上下文特 征，再总结出提取用户名密码的有效方法。解析协议内容，并作记录与统计。对 用户登录行为进行记录。程序在文件上输出形如下列 CSV 格式的日志： 时间、源 MAC、源 IP、目标 MAC、目标 IP、登录名、口令、成功与否



(此处为wireshark的截图，实际文件见附录)

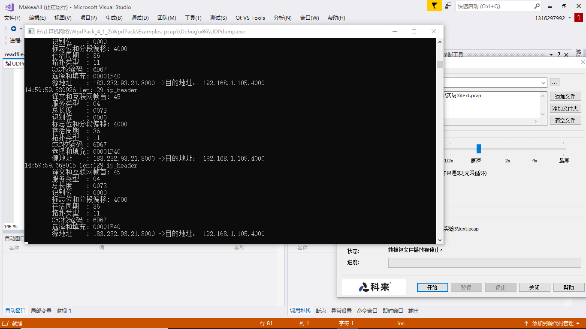
使用克莱播放器播放包进行检测。

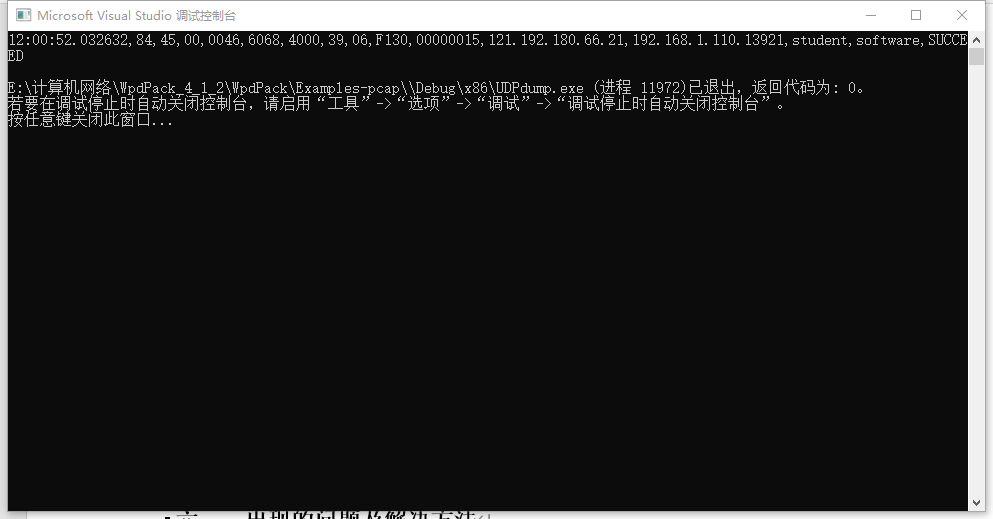




与实验提供的报文相同。

符合预期设置。





最终生成csv文件。

# 实验代码

本次实验的代码已上传于以下代码仓库：https://www.gitee.com/xxx/xxx （注意：建议使用码云，并设置公开权限；本学期暂不推荐使用GitHub；如使用厦门大学私有Git服务，应将whuang@xmu.edu.cn加入项目成员备查，本段话删除。）

# 实验总结

ftp搭建不顺利，原因是防火墙阻碍了访问ftp，使用不同的终端进行处理，最终实现可访问的ftp。

wireshark无法抓取本地报文，解决方法可以使用虚拟机也可以使用别的计算机对ftp进行访问。我和室友两人互相使用对方的ftp完成实验。

对于禁用网卡后仍然会收到很多数据包影响实验数据的整洁性，没有很好的解决方法，通过查阅资料发现可能是应用程序误发包