

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三　用 PCAP 库侦听并分析网络流量**

**班　　级 软件工程2020级卓越班**

**姓　　名 庾晓萍**

**学　　号 20420192201952**

**实验时间 2022年3月23日**

**2022年3月23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，最大勿超过5MB；
4. 应将材料清单上传在代码托管平台上；
5. 在实验课结束14天内，按原文件发送至课程FTP指定位置。

# 实验目的

通过完成实验，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 Wireshark 观察网络流量并辅助网络侦听相关的编程；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、IP 报文、 TCP段和 FTP 命令的格式概念，掌握 TCP 协议的基本机制；熟悉帧头部或 IP 报文头部各字段的含义。熟悉 TCP 段和 FTP 数据协议的概念，熟悉段头部各 字段和 FTP控制命令的指令和数据的含义。

# 实验环境

操作系统：Windows 10；

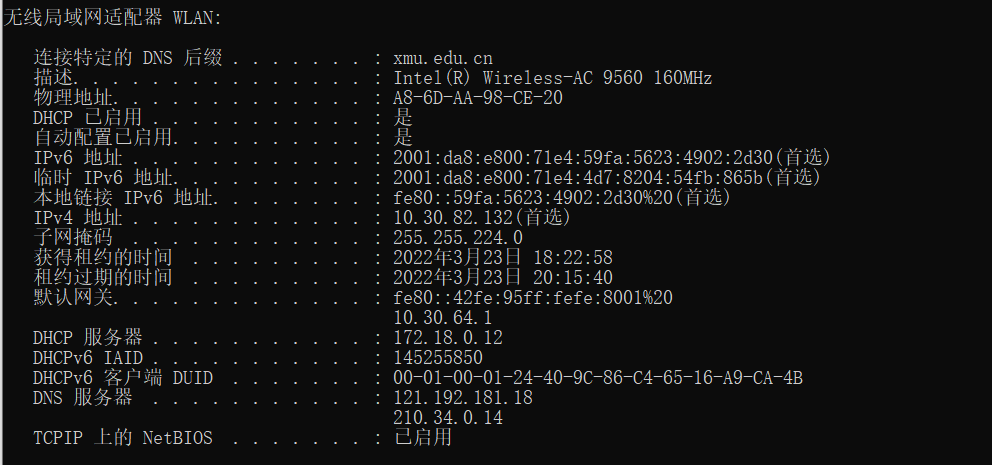
IDE：Visual Studio 2019

编程语言：C++；

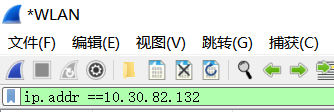
# 实验结果

**1、用侦听解析软件Wireshark观察数据格式。**

① 进入命令窗口之后，输入：ipconfig/all 回车，查看电脑IP详细地址。

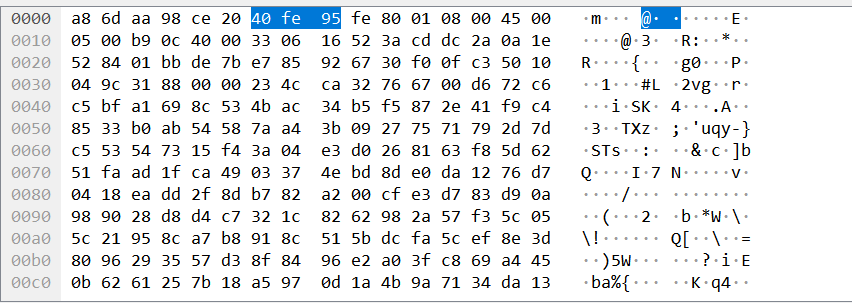


② 将过滤器设为TCP与本地 ip，根据数据包依次获取了帧数、IP 地址、MAC 地址。

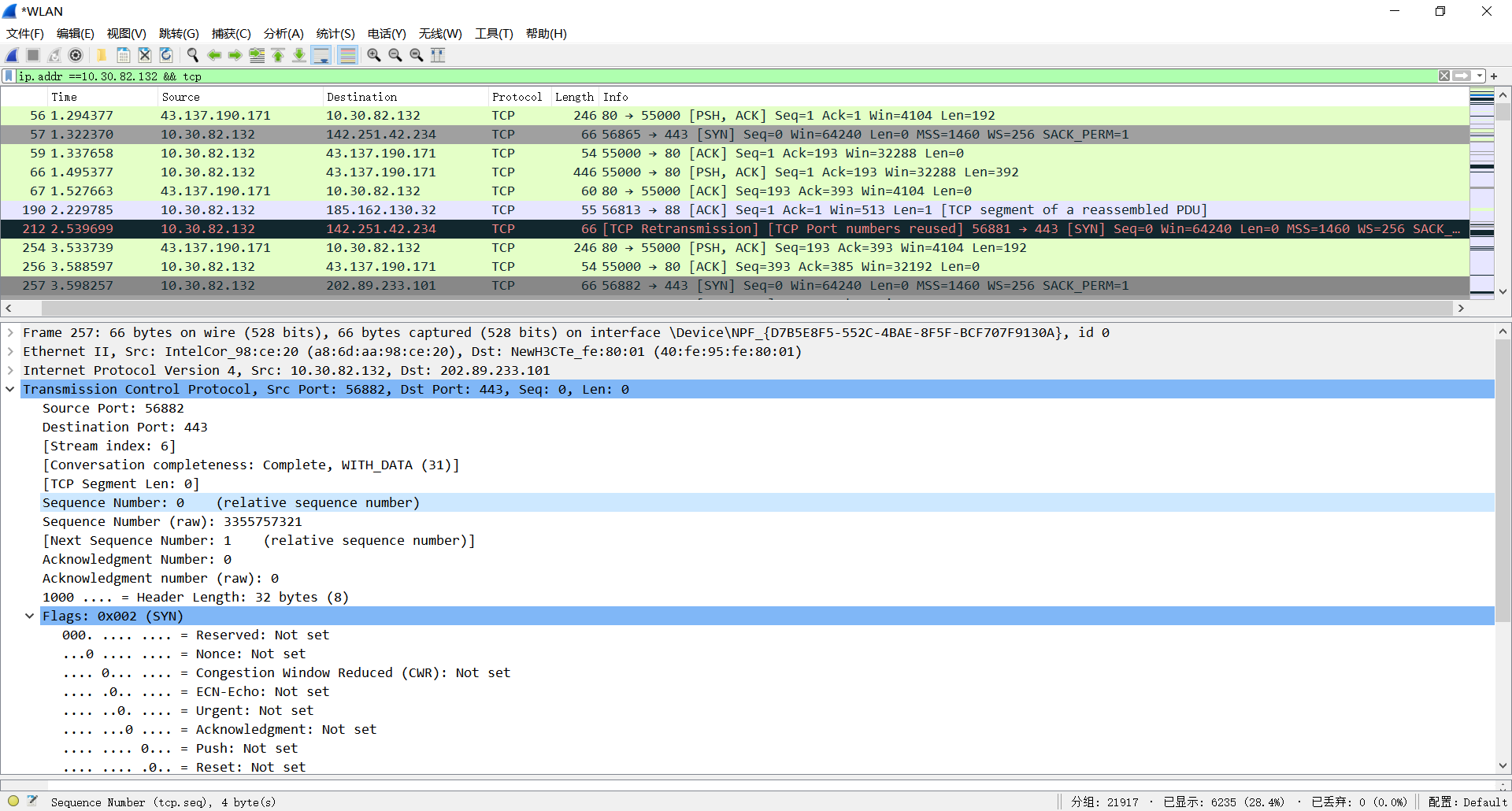






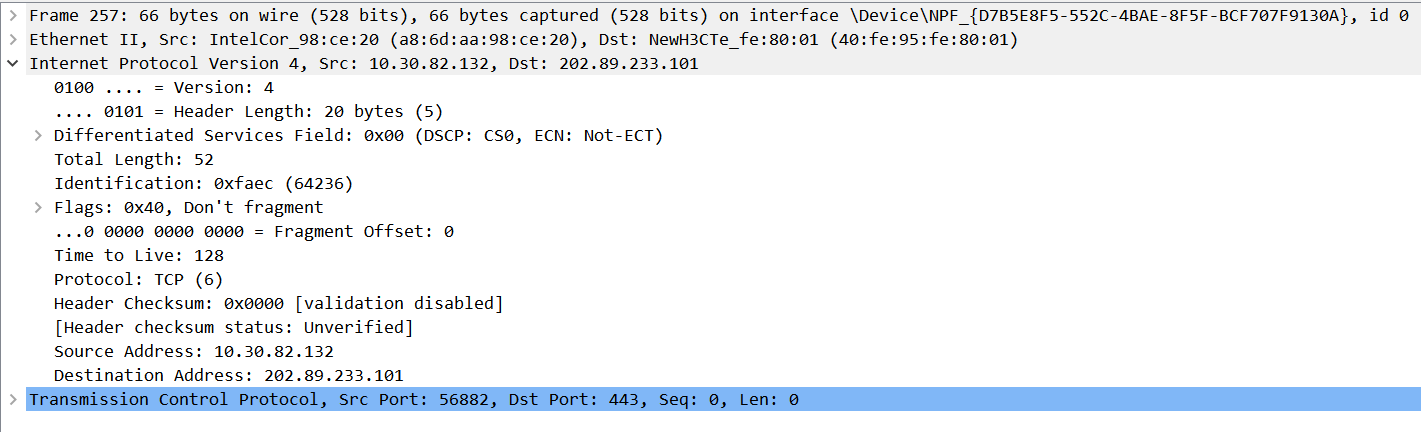


③ 使用 wireshark 分析TCP协议的数据包，其中包含物理层（frame），数据 链路层（Ethernet），网络层（Internet），传输层（Transmission）的信息。



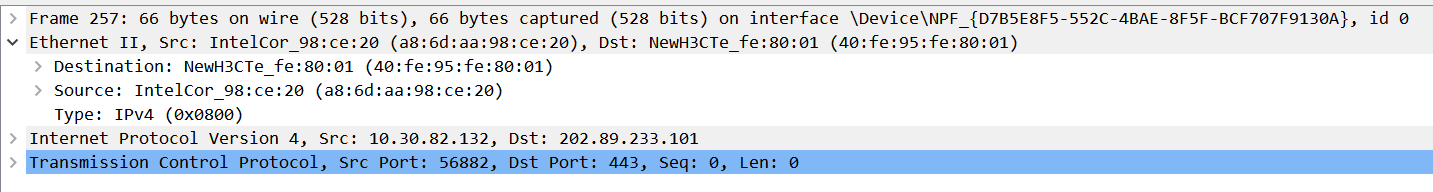
A. 观察IP 报文格式（网络层）：

（1）IP版本号Version：4；（2）：首部长度Header Length：20字节；（3）服务类型Differentiated Service Field：0x00；（4）数据包总长度Total Length：52字节；（5）标识符Identification：0xfaec；（6）标识Flags：不允许分片；（7）分片偏移Fragment offset：0；（8）生存时间Time to Live：数据报的生存周期，可以经过路由器的128条；（9）上层协议Protocol：TCP；（10）校验和：0x0000，未校验；（11）源地址：10.30.82.132；（12）目的地址：202.89.233.101。



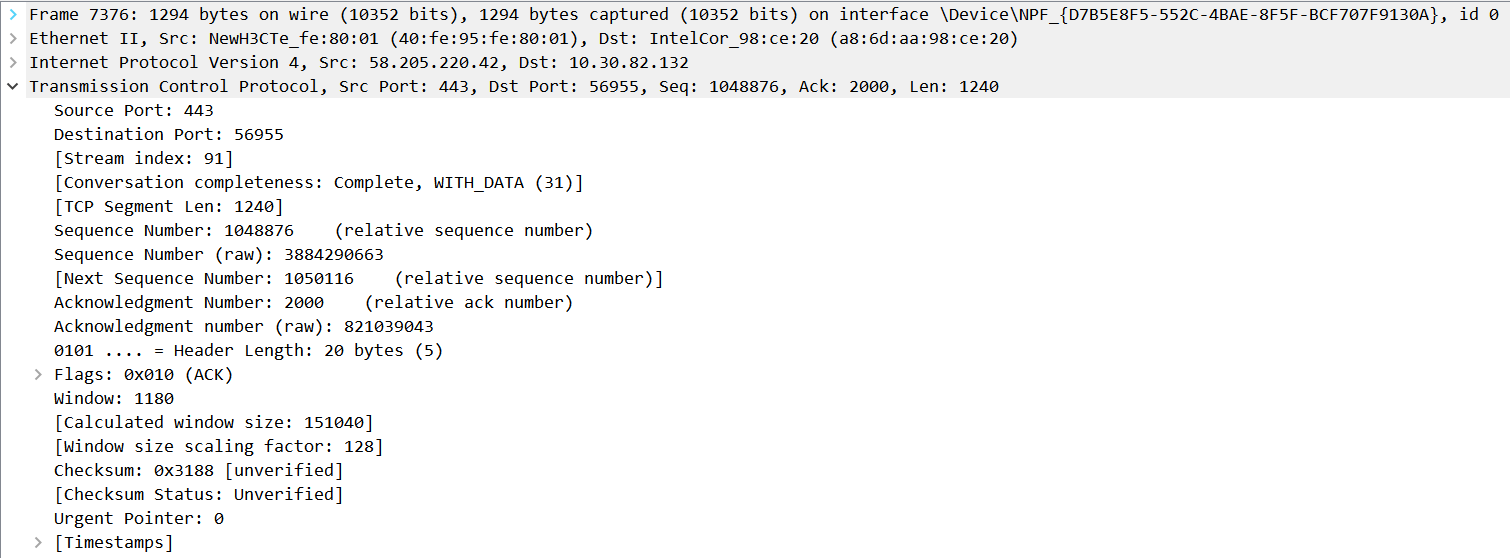
B. 观察帧格式（数据链路层）：

（1）目的地址：40:fe:95:fe:80:01；（2）源地址：a8:6d:aa:98:ce:20；（3）类型：IPv4。

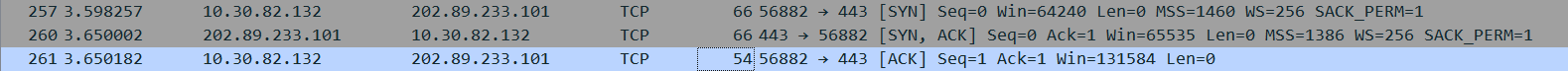


C. 观察TCP格式（传输层）：

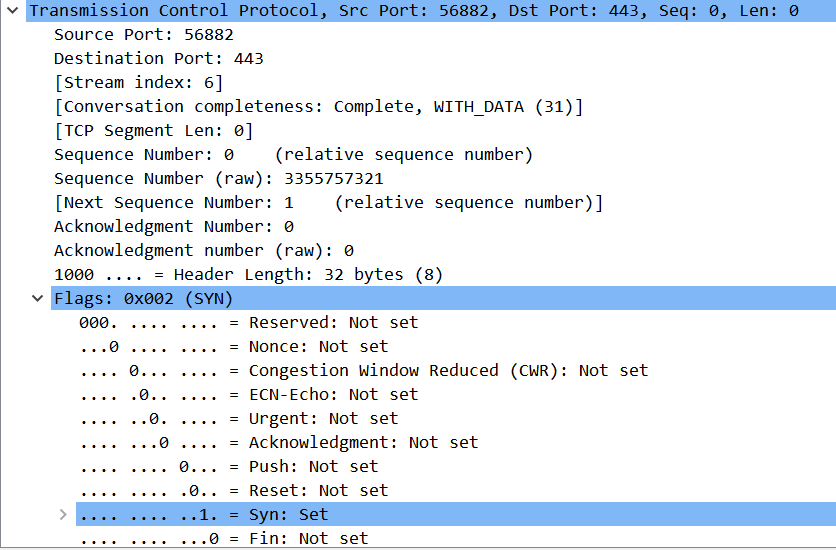
（1）源端口:443； （2）目的端口：56955；（3）序号表示发送的字节流序号是 3884290663；（4） 确认号期待对方发送的字节序号是 821039043；（5）头部长度：20字节；（6）标志位Flags：确认位ACK=1，表示已连接，在连接建立后所有传送的报文段都必须把ACK置为1。（7）窗口大小：1180；（8）校验和：0x3188;（9）紧急指针：0。



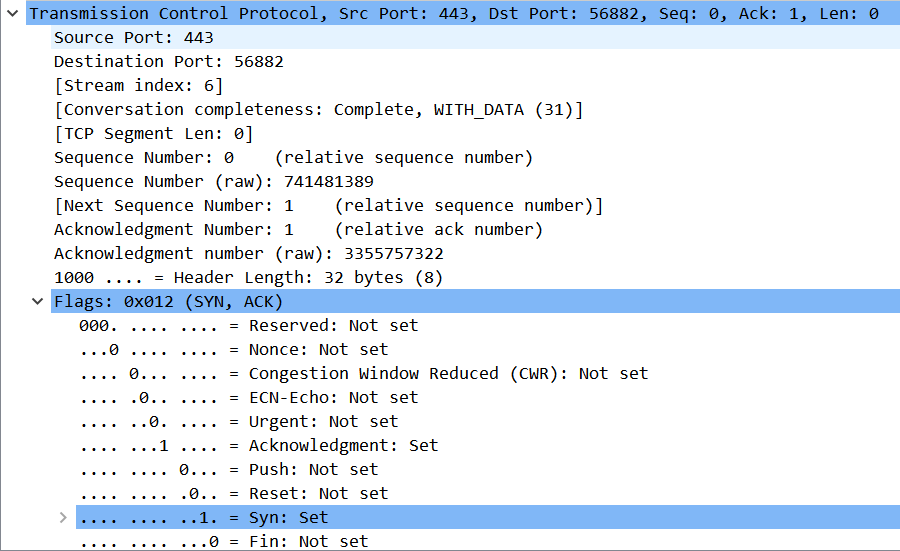
1. **用侦听解析软件观察 TCP 机制（TCP的三次握手、四次挥手）**
2. **TCP三次握手**



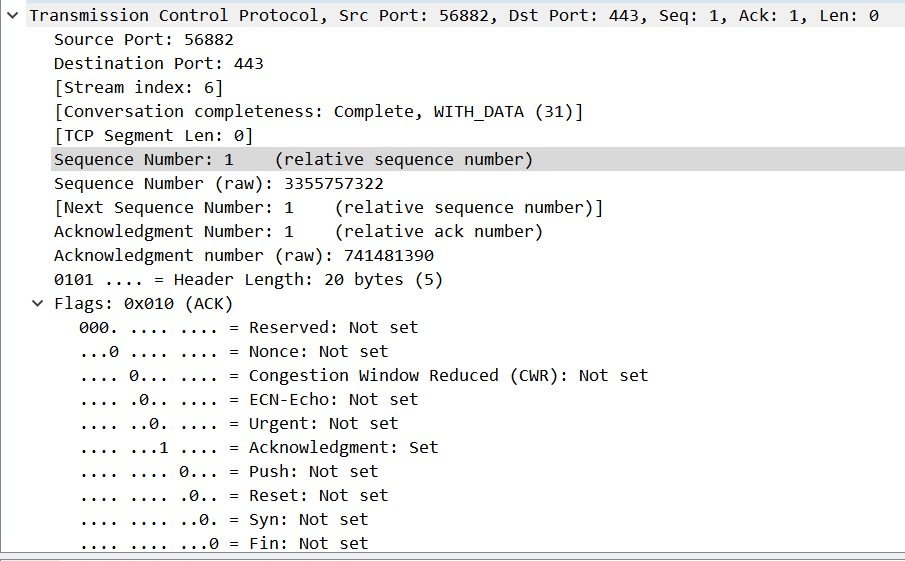
① 第一个握手数据包：客户端发送一个连接请求报文段，无应用层数据，标 志位为同步比特SYN，用来同步序号。序列号seq为0，代表客户端请求建立 连接。



② 第二个握手数据包：服务器端为该TCP连接分配缓存和变量，并向客户端 返回确认报文段，允许连接，无应用层数据。标志位为 SYN=1，ACK=1。将确 认序号ack设置为1。

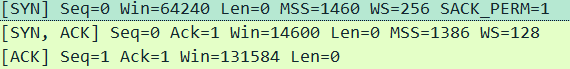


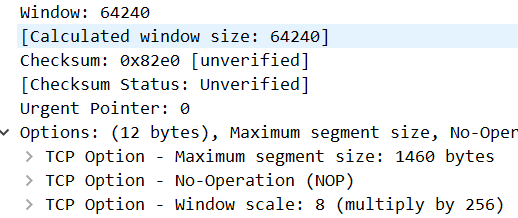
③ 第三个握手数据包：客户端为该TCP连接分配缓存和变量，并向服务器端 再次发送确认包(ACK) ，可以携带数据。SYN 标志位为 0，ACK标志位为1。 并且把服务器发来 ACK 的序号字段+1，放在确定字段中发送给对方。并且在 数据段放写 ISN（Sequence Number）+1。



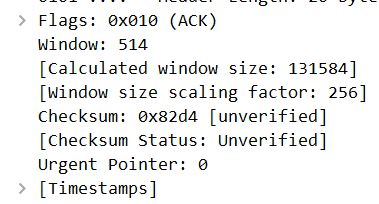
④ 三次握手时窗口滑动

用wireshark抓取TCP连接时的报文发现客户端的Win变大了，这里是使用了 Window Scale来扩张TCP接收窗口，使得接收窗口可以大于131584字节。



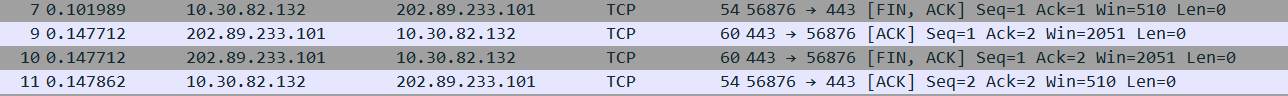


首先1号包是TCP第一次握手连接时客户端的请求包，客户端如果窗口大于64240，那么就先将Window size 设置为64240，表示客户端窗口将大于64240，具体多大，在3号数据包会给出窗口的基数。

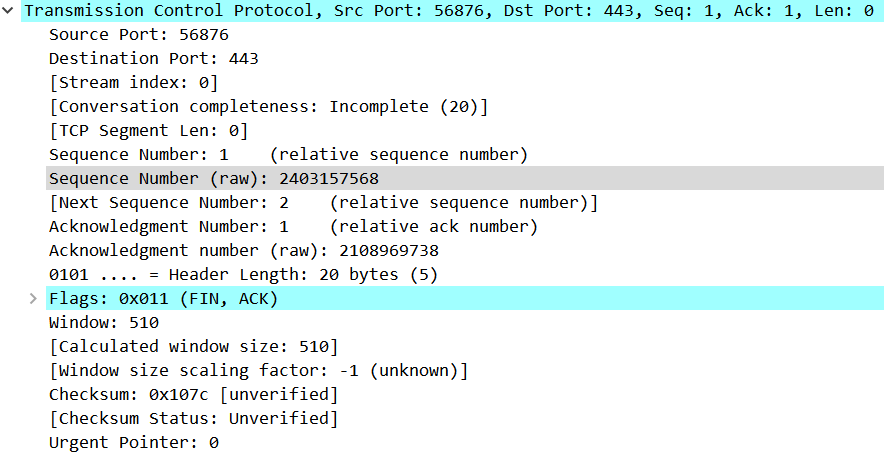


在三号包中，可以看到窗口的基数Window是514，窗口的倍数是2^8=256，那么实际的窗口大小为514\*256=131584Byte。

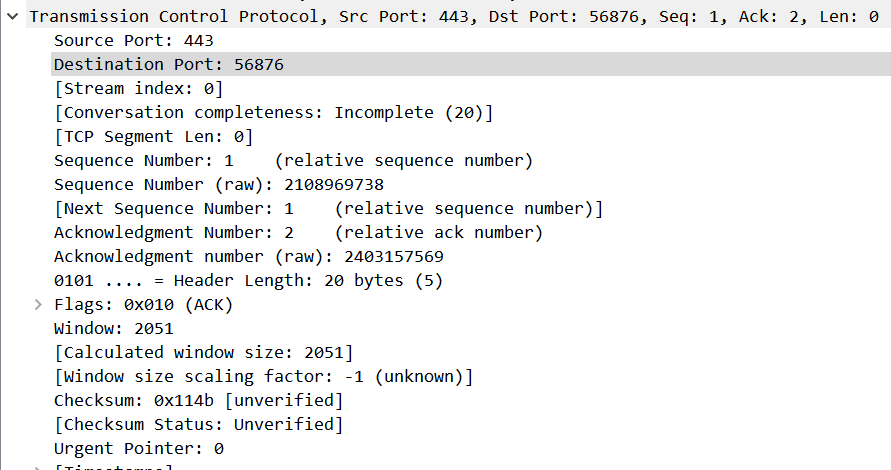
**B. 四次挥手**



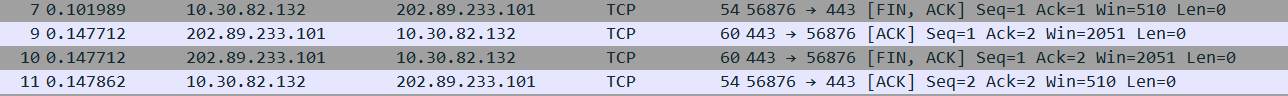
① 第一次挥手：客户端发送连接释放报文段，停止发送数据，主动关闭TCP 连接。FIN = 1，ACK=1。



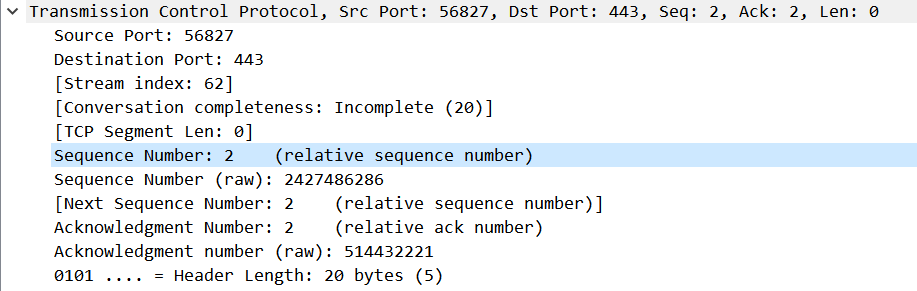
② 第二次挥手：服务器端回送一个确认报文段，客户到服务器这个方向的连接 释放，就是半关闭状态。ACK = 1。序号为1，确认序号为2。



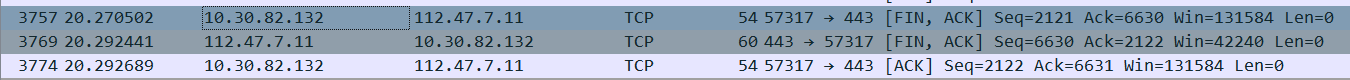
③ 第三次挥手：服务器端发送完数据，就发送连接释放报文段，主动关闭TCP 连接。FIN = 1，ACK = 1。序号为1，确认序号为2。



④ 第四次挥手：客户端回送一个确认报文段，再等到时间等待计时器设置的 最长报文段寿命后，连接彻底关闭。ACK=1，序号为2，确认序号为2。



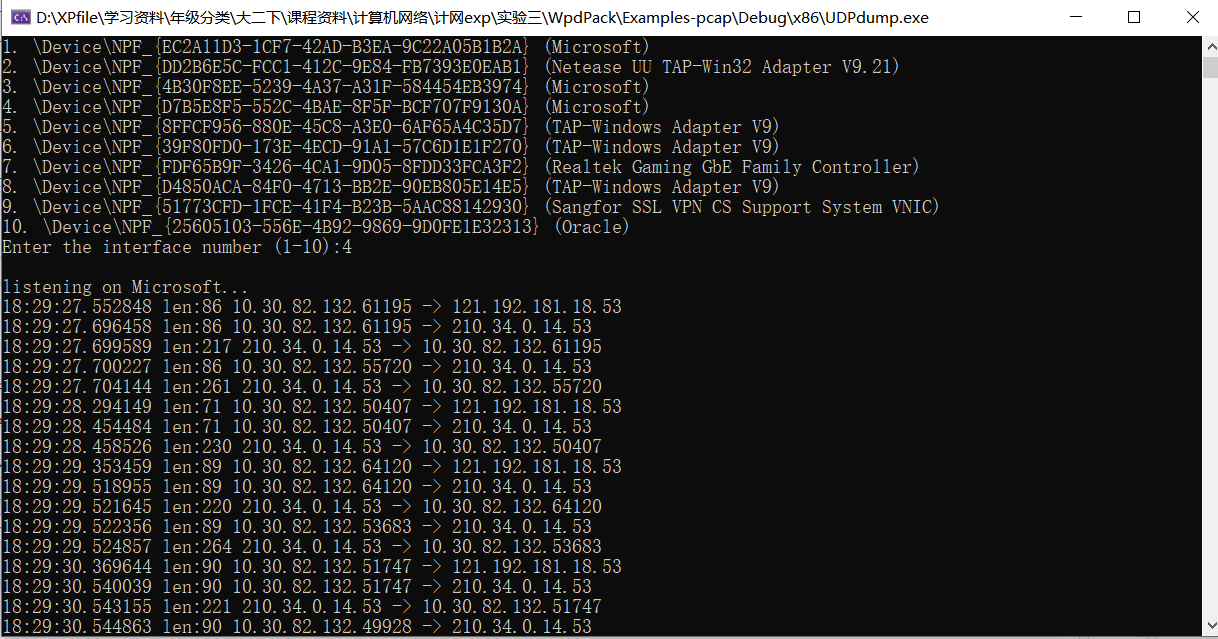
⑤ 问题讨论：执行程序时，发现很多抓到的 TCP 挥手是三次，而不是四次。查阅资料是因为服务器端收到客户端的 FIN 后，服务器端同时也要关闭连接，这样就可以把 ACK 和 FIN 合并到一起发送，节省了一个包，变成了“三次挥手”。而通常情况下，服务器端收到客户端的 FIN 后，很可能还没发送完数据，所以就会先回复客户端一个 ACK 包，稍等一会儿，完成所有数据包的发送后，才会发送 FIN 包，这也就是四次挥手了。



**3、用 WinPcap 库侦听网络数据**

一、WinPcap 库侦听网络数据

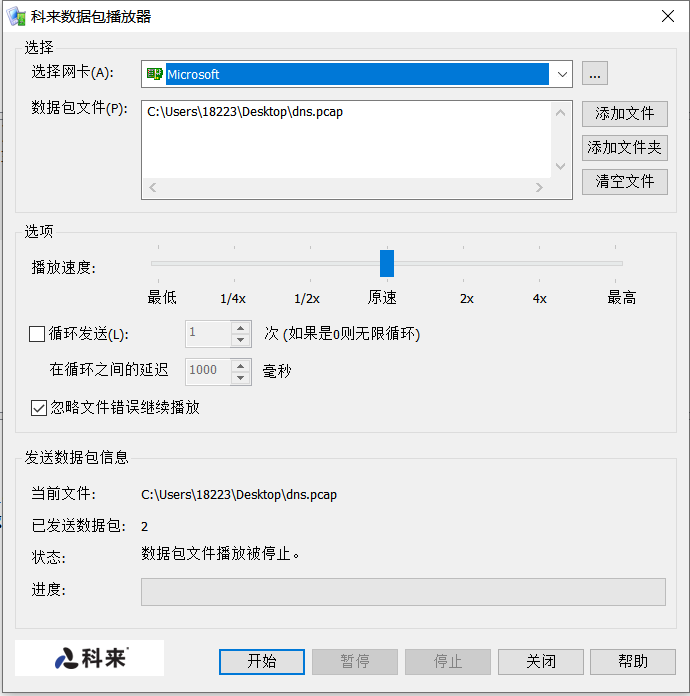
① 下载WinPcap文件，卸载其他项目后成功运行。

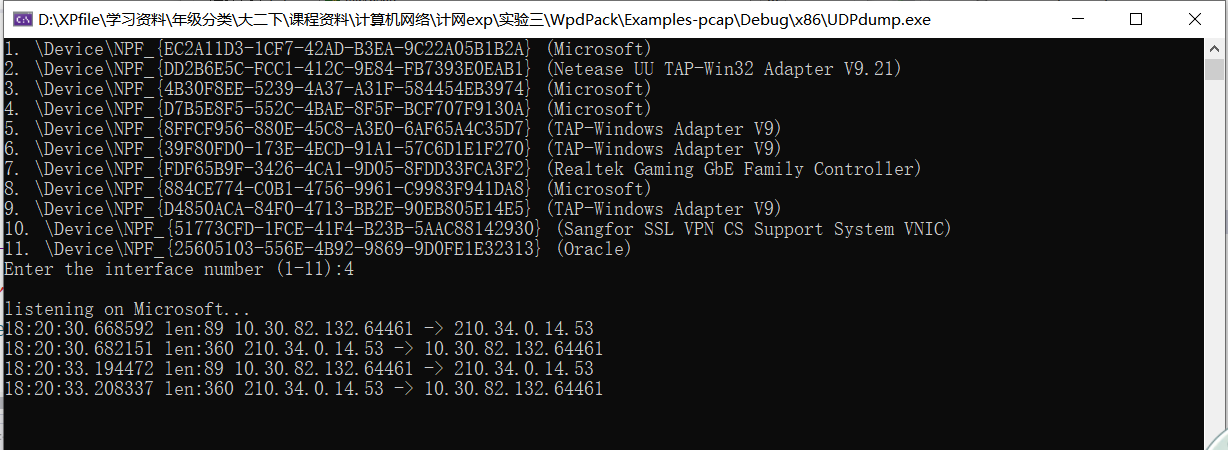


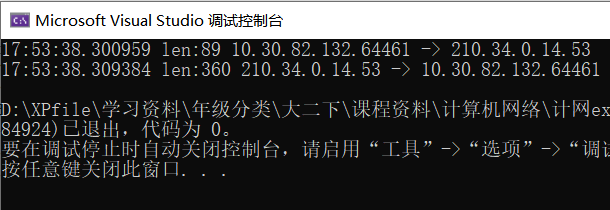
② WinPcap库侦听数据

（1）使用WirShark捕获WLAN上的数据包。在左上角输入dns可以过滤出 dns。选 中两个记录，导出特定分组，命名为dns.pcap

（2）在高级防火墙中新建出站规则，阻止其他一切连接。使用科来数据包播放 器单独播放dns.pcap，调试成功。



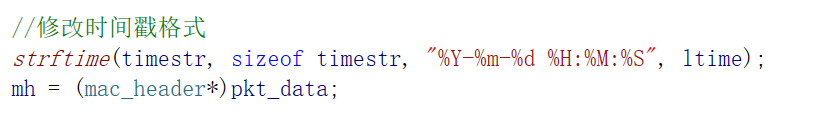


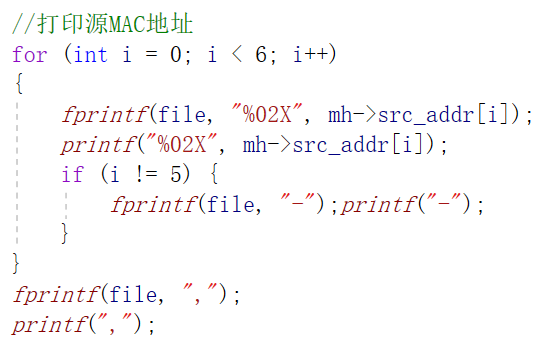
（3）修改UDPdump项目的代码，根据同一文件目录下的readfile工程的文件 的读取pcap文件的代码段，使得UDPdump项目可以读取pcap文件。 

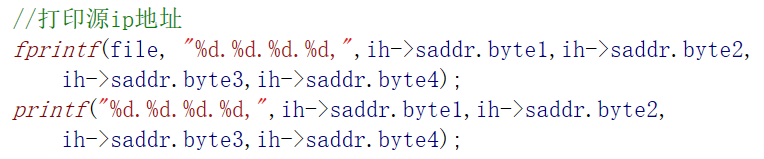
1. 解析MAC和 IP 地址，记录统计（在 winpcap 自带的工程上进行更新）
2. 核心代码

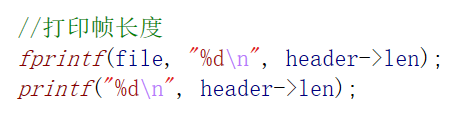
① PART 1：修改输出到csv文件中的格式

（下图展示了修改源MAC地址和修改源IP地址的代码，修改目的地址也是类 似的，不再贴出。）



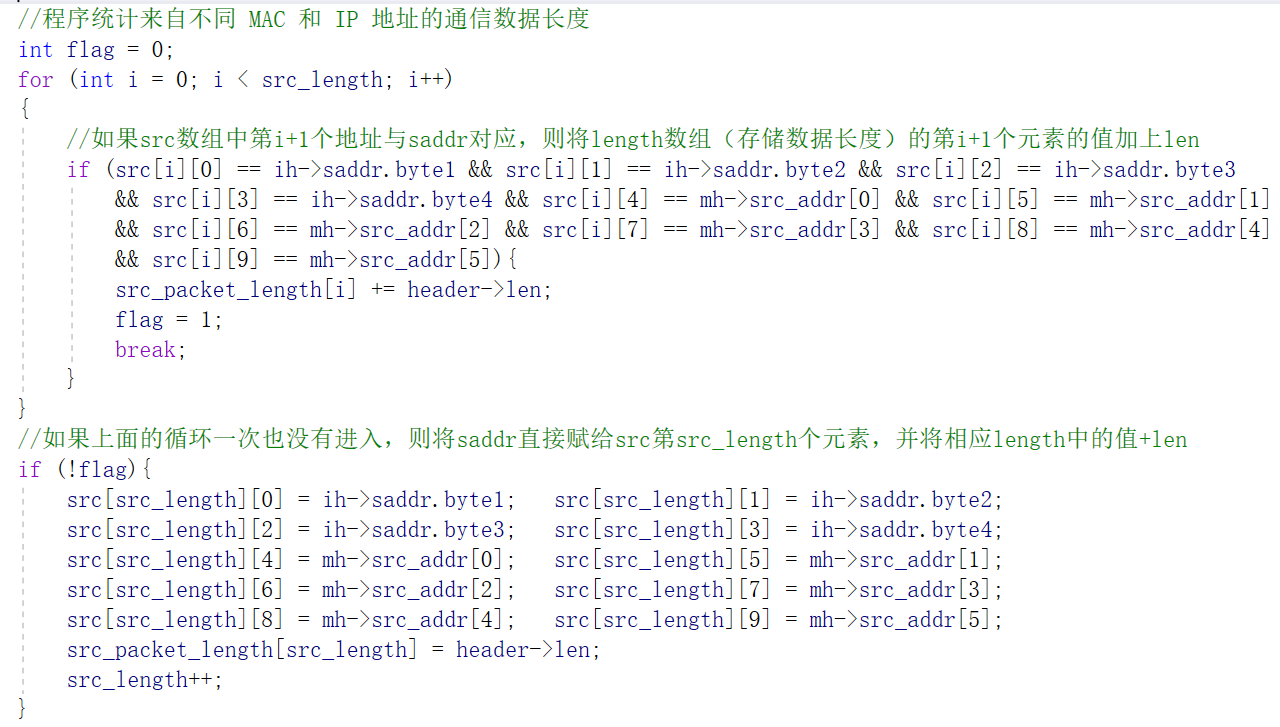


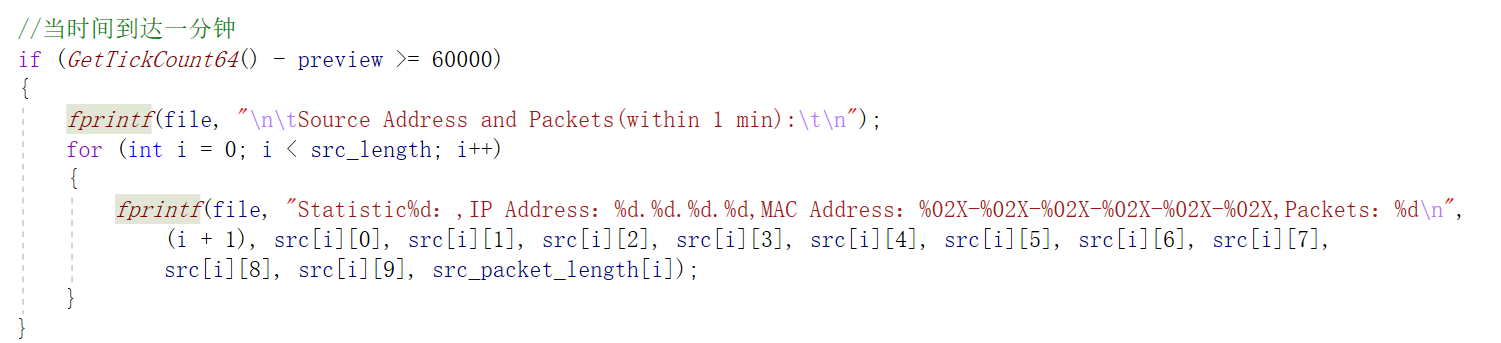




② PART 2：对每分钟数据统计分析

（下图展示了统计来自不同MAC和IP地址的通信数据长度的代码，统计发送 到不同MAC和IP地址的通信数据长度的代码是类似的，不再展示。）

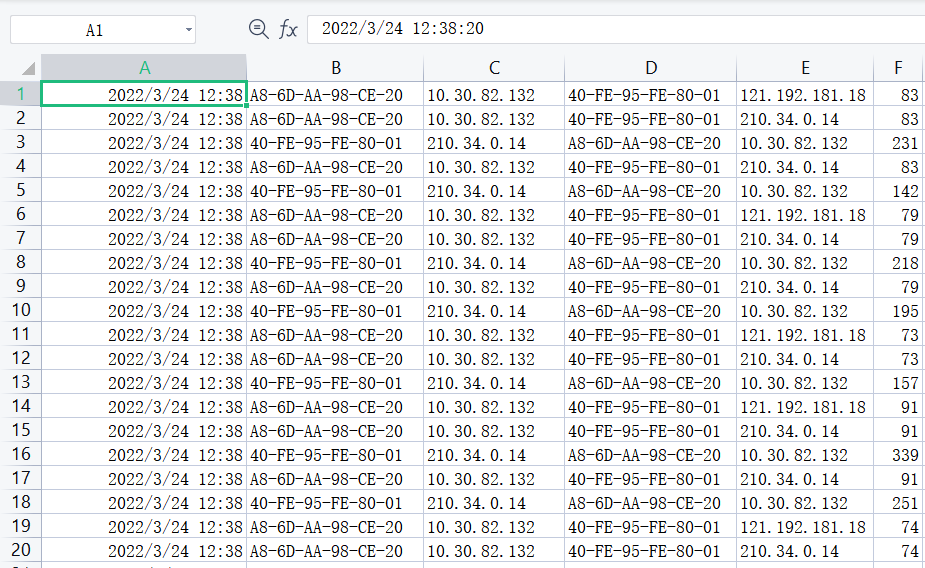


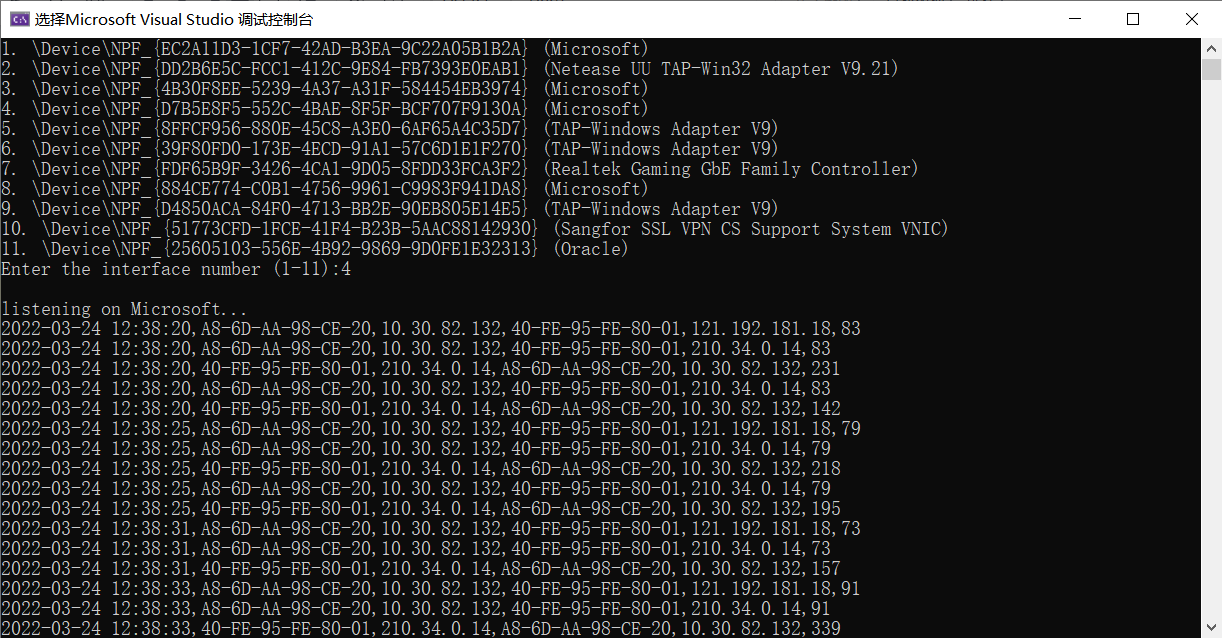


（2）实验结果

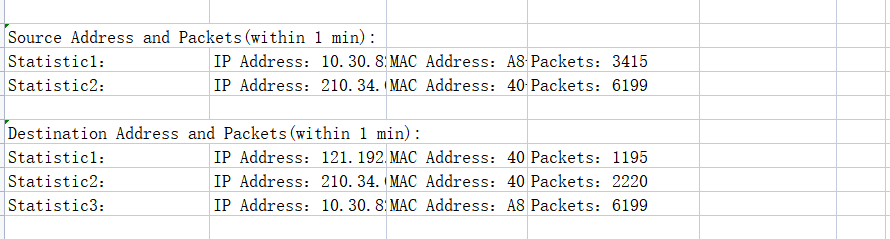
① 程序在文件上输出形如下列 CSV 格式的日志：

时间、源 MAC、源 IP、目标 MAC、目标 IP、帧长度（以逗号间隔）



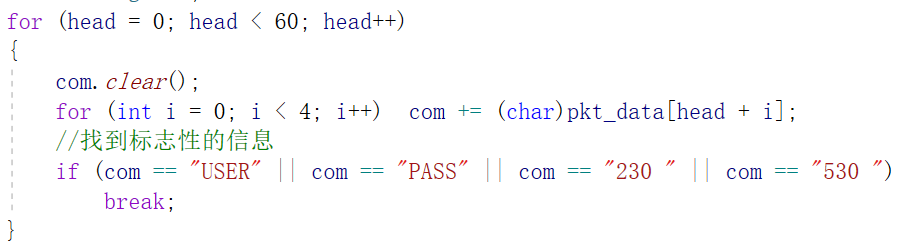


② 每隔一段时间（如 1 分钟），程序统计来自不同 MAC 和 IP 地址的通信 数据长度，统计发至不同 MAC 和 IP 地址的通信数据长度。

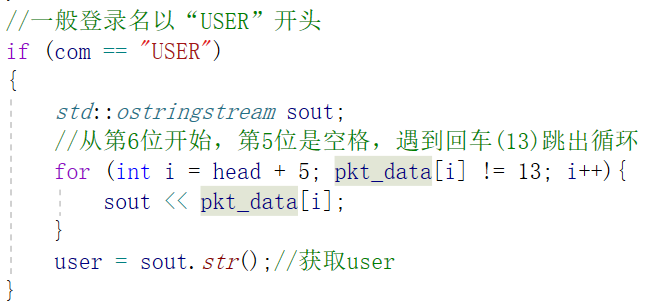


1. 解析侦听到的网络数据（以FTP密码侦听为例）
2. 核心代码

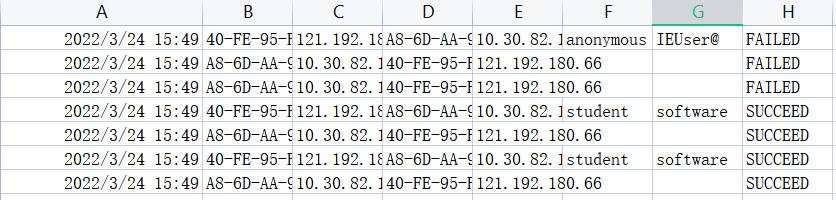
① 找到标志性的信息。一般登录名以“USER”开头，口令以“PASS”开 头，登录成功以“230”开头，失败以“530”开头。



② 获取USER信息，获取PASS信息类似，不再重复。打印时间、源 MAC、 源 IP、目标 MAC、目标 IP与上一个实验项目中的代码相同。



1. 实验结果：侦听得到系FTP的用户名和密码



# 实验代码

本次实验的代码已上传于以下代码仓库：

https://github.com/ryanregal/Exp\_ComputerNetwork

# 实验总结

通过这次实验，我对网络信息传输有了更直接的体验和了解，学习了 WINPCAP 和 WIRESHARK。学习了如何在调试中观察内存，查看有关 MAC地址、IP报文的内容，观察了TCP的三次握手，四次挥手和滑动窗口机制。我还学会了如何在已有的工程项目上进行更改、添加，调试等。过程中遇到了一些问题，比如一开始使用科来数据包生成器找不到网卡适配器，发现是软件本身与Win10系统的兼容性有问题，在更改电脑兼容性并以管理员身份运行后发现可以正常解决。还有比如用Wireshark抓挥手包的时候有的找不到，查阅资料才知道是因为服务器端收到客户端的 FIN 后，服务器端同时也要关闭连接，这样就可以把 ACK 和 FIN 合并到一起发送，节省了一个包，变成了“三次挥手”。另外在进行FTP实验时，出现了The C++ Standard Library forbids macroizing keywords的错误，这是自定义inline导致和系统文件发生冲突，于是预处理器定义中加入“\_XKEYCHECK\_H”，成功运行。