

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三　侦听以太网和IP报文**

**班　　级 软件工程2018级1班**

**姓　　名 方浩南**

**学　　号 24320182203188**

**实验时间 2020年3月11日**

**2020 年 3 月 25 日**

# 实验目的

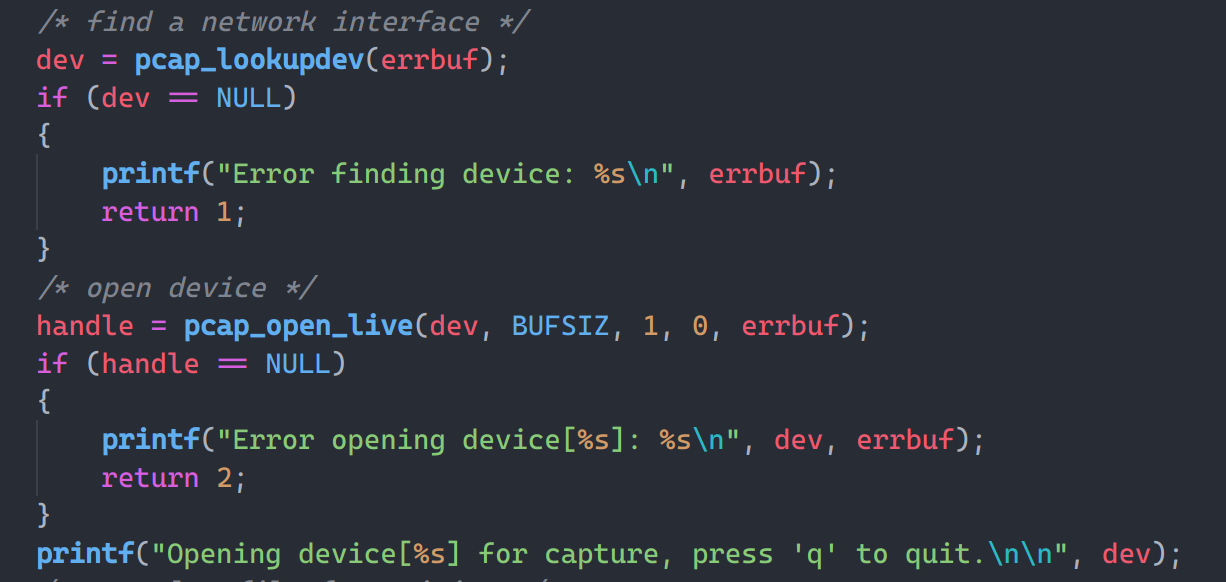
用WinPCAP或libpcap监听并分析以太网的帧，记录目标与源MAC和IP地址。

# 实验环境

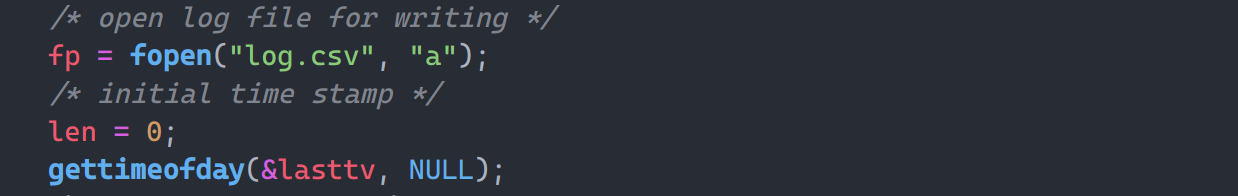
操作系统：Ubuntu 18.04、编程语言：C。

# 实验结果

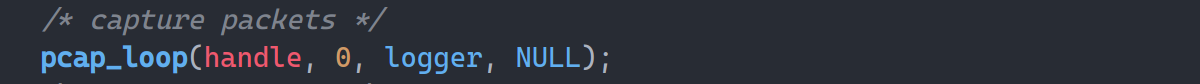
查找并打开一个网卡，名称是字符串而句柄则类似指针。



在开始抓取之前先做其它初始化：设置时间和日志目录。

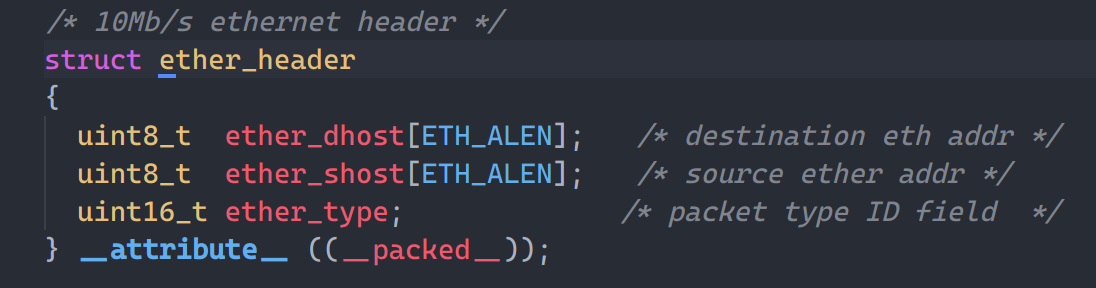


开始抓包：设置为0/-1代表不限个数，每次抓到的包会进入回调函数。

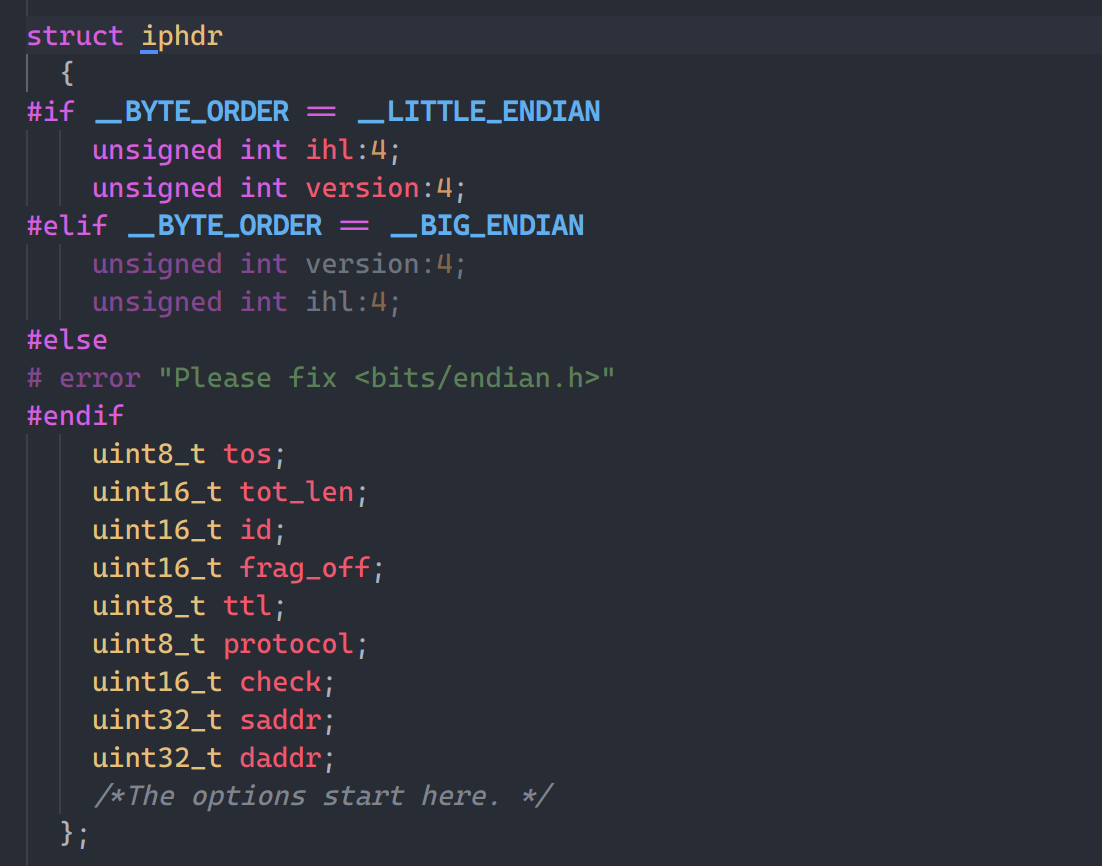


利用C语言的结构体和指针可以很方便转换和读取以太网的帧。

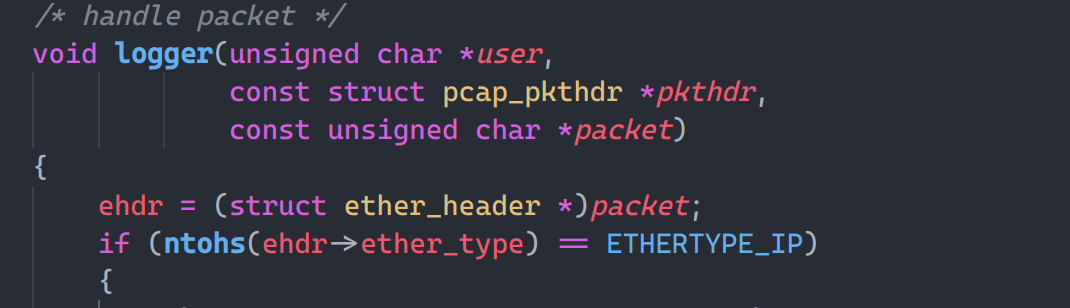
以太网报头：6字节目的MAC、6字节源MAC、2字节类型。



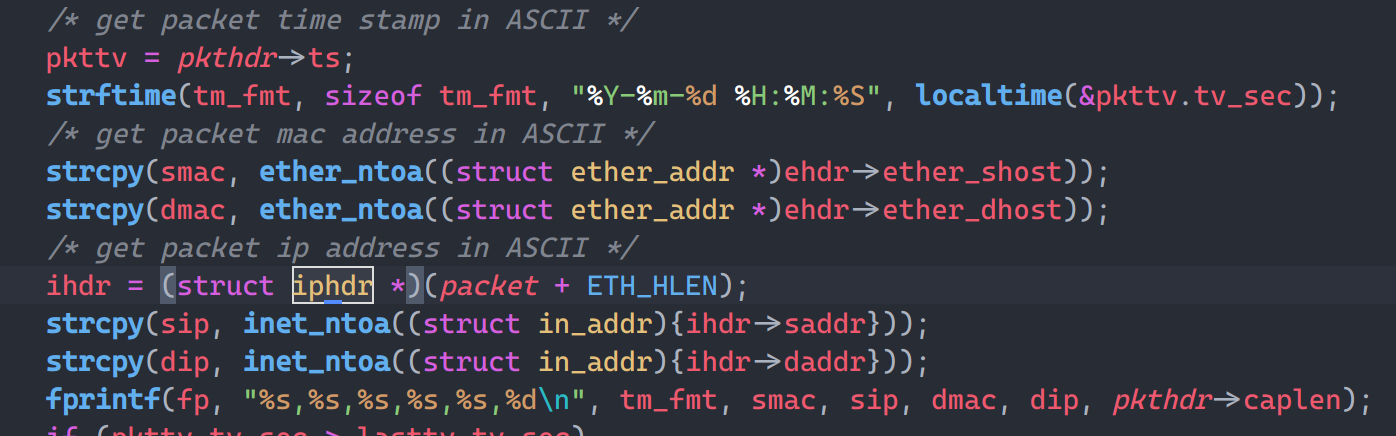
在以太网的数据段开始有IP报头：



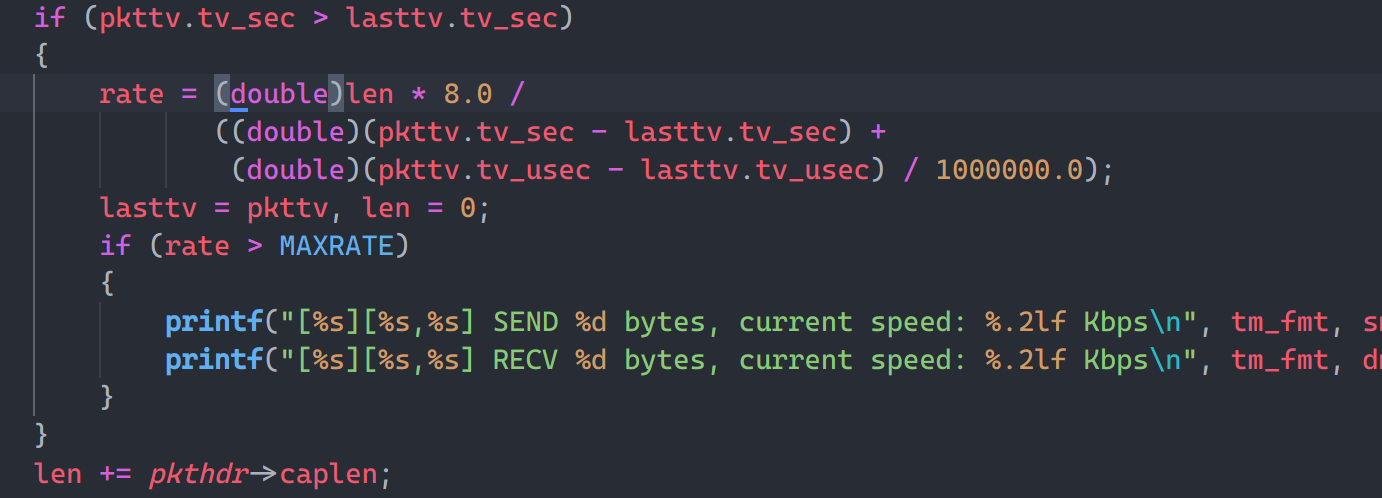
回调函数的定义：如果类型是IP包则记录。



利用系统相关函数把IP/MAC/时间方便地转为可读形式：

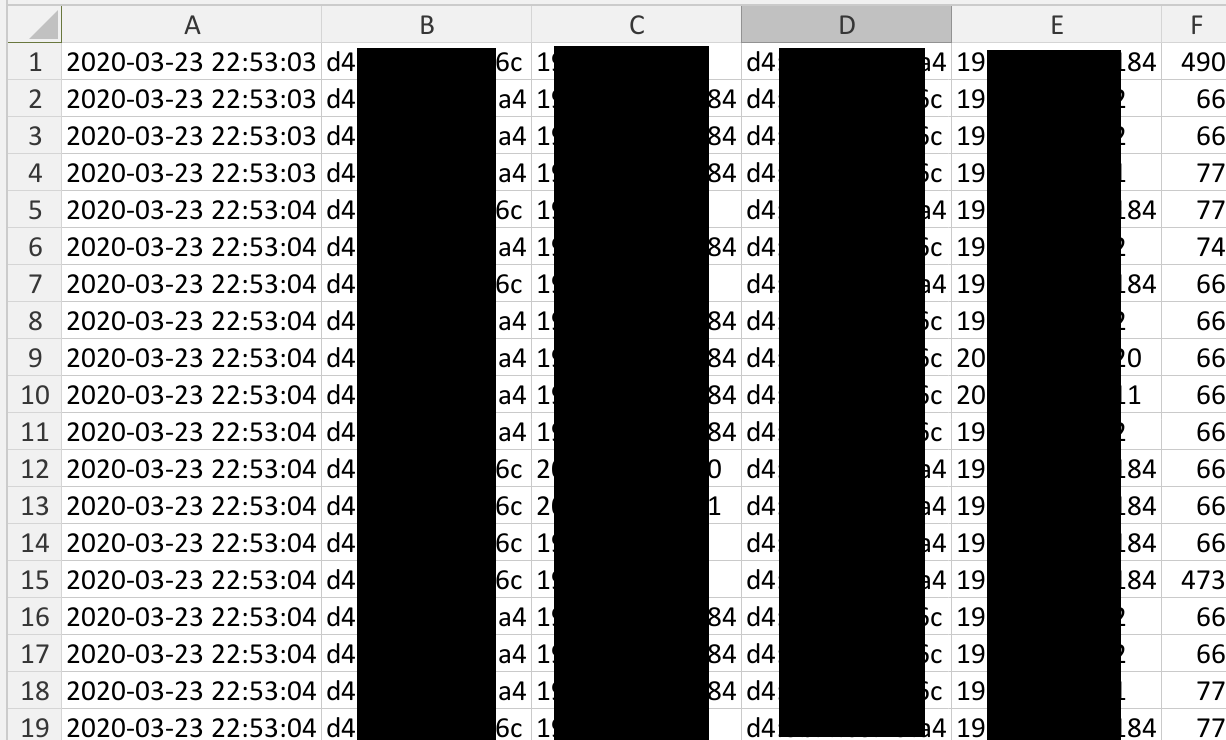
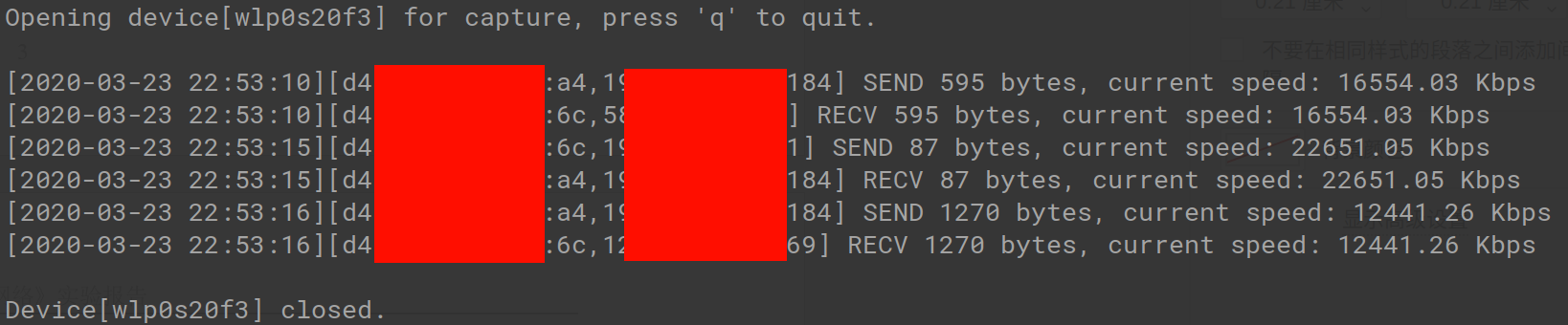


以秒为单位，累加一秒（或若干）的所有包长度并记录时间戳，计算速率。



通过设置非阻塞的终端输入可以在每次回调时检测输入以退出侦听。

运行结果：



# 实验总结

通过这次实验不仅学习了libpcap的使用，更借助结构体切实地理解了以太网的帧格式、报头和地址等等。