# 厦門大學



## 信息学院软件工程系

《计算机网络》实验报告

趔	目	<u> 实验二 用 PCAP 库侦听开分析网络流量</u>
班	级_	软件工程 2018 级 1 班
姓	名.	刘久一
学	号.	24320182203235
实验	时间 _	2020年3月11日

2020年 3月11日

#### 1 实验目的

用 WinPCAP 或 libPcap 库侦听并分析以太网的帧,记录目标与源 MAC 和 IP 地 址。基于 WinPCAP 工具包制作程序,实现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,对超过给定阈值(如:1MB)的流量进行告警。

#### 2 实验环境

Microsoft Windows 10

Microsoft Visual Studio 2019

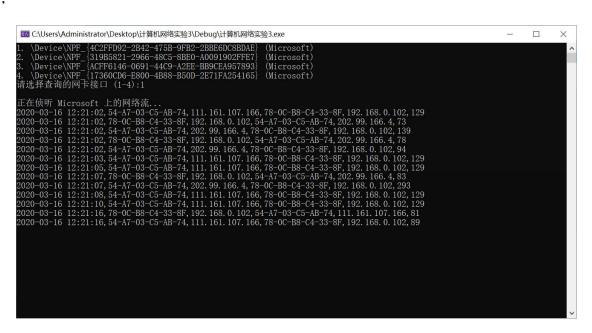
WinPcap V4.1.3

WireShark V3.2.2

#### 3 实验结果

```
Istruct macinfo
u_char dstmac[6];
u_char srcmac[6];
u_char type[2];
macinfo() {}
macinfo(const u_char*src)
    int tot = 0;
    for (int i = 0; i < 6; i++) dstmac
    for (int i = 0; i < 6; i++) srcmac
    for (int i = 0; i < 2; i++) type[:
void printdstmac()
    for (int i = 0; i < 6; i++)
        if (i)printf("-");
        printf("%02X", dstmac[i]);
void printsrcmac()
    for (int i = 0; i < 6; i++)
                                    新建 macinfo 类专门为提取 mac 地址信
```

息;



在每次捕获的数据包中分析出数据包长度, ip 地址, mac 地址即可。

### 4 实验总结

通过这次试验,我初步掌握了 Wincap 库的简单运用,如何正确阅读复用已完备的代码,以及对数字链路层中以太网的帧格式又有了进一步的巩固理解。