厦門大學

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 2018 级 1 班

姓　　名 赖睿朗

学　　号 **243202182203215**

实验时间 **2020 年 3 月 16 日**

2020 年 3 月 16 日

1 实验目的

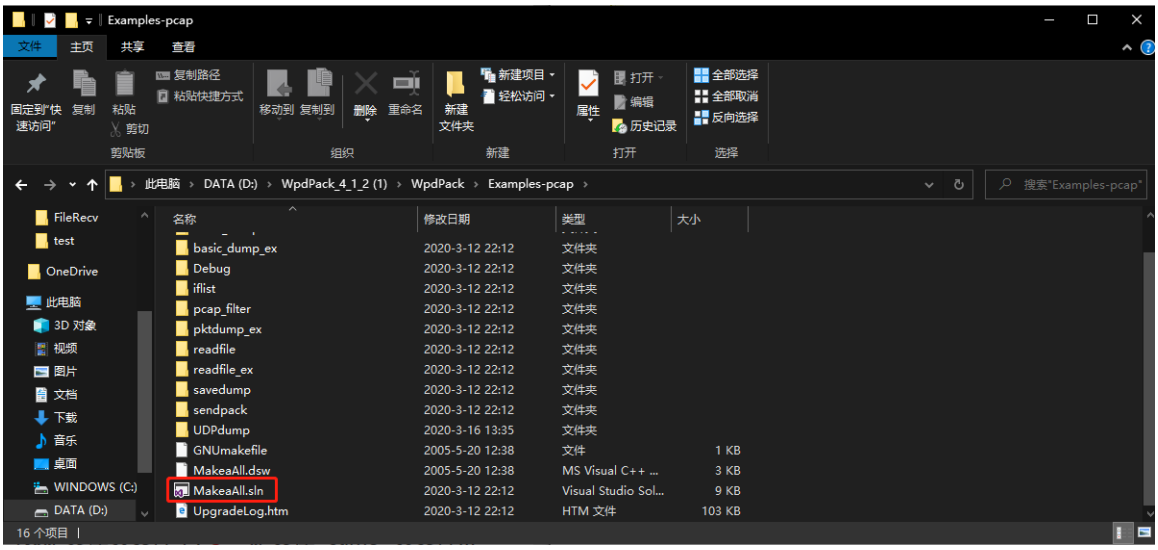
用 WinPCAP 库侦听并分析以太网的帧，记录目标与源 MAC 和 IP 地址。基于 WinPCAP 工具包制作程序，实现侦听网络上的数据流，解析发送方与接收 方的 MAC 和 IP 地址，并作记录与统计，对超过给定阈值（如：1MB）的流量进行告 警。

2 实验环境

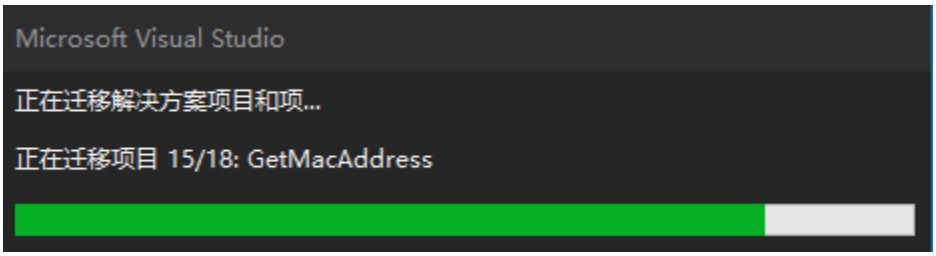
操作系统：Windows10

调用库：WinPCAP

3 实验结果



下载好 WinPCAP，并打开 MakeaAll.sln 工程



等待迁移并且初次运行

```
strftime(timestr, sizeof timestr, "%Y-%m-%d %H:%M:%S", ltime);
```

```
u_char ic[20];
strncpy(ic, pkt_data, 12);
```

```
printf("%02X-%02X-%02X-%02X-%02X-%02X,%d.%d.%d.%d,%02X-%02X-%02X-%02X-%02X-%02X,%d.%d.%d.%d\n",
    ic[tot++], ic[tot++], ic[tot++], ic[tot++], ic[tot++], ic[tot++],
    ih->saddr.byte1,
    ih->saddr.byte2,
    ih->saddr.byte3,
    ih->saddr.byte4,
    ic[tot++], ic[tot++], ic[tot++], ic[tot++], ic[tot++], ic[tot++],
    ih->daddr.byte1,
    ih->daddr.byte2,
    ih->daddr.byte3,
    ih->daddr.byte4
    );
```

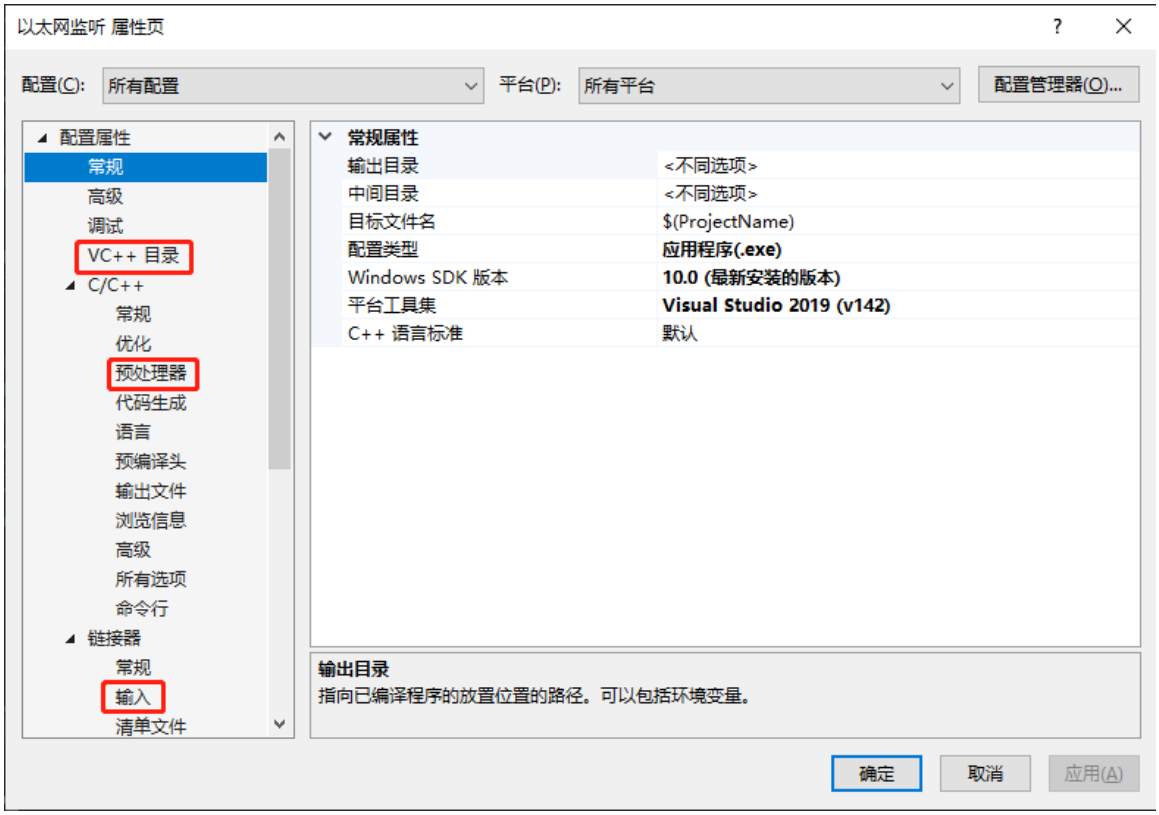
按要求修改代码

```
选择D:\WpdPack_4_1_2 (1)\WpdPack\Examples-pcap\Debug\x86\UDPdump.exe
1. \Device\NPF_{6AA84412-BBBA-467F-95BF-2B77D2433C14} (Microsoft)
2. \Device\NPF_{9DA39D56-2278-4252-B8CA-340C8371AC58} (Realtek PCIe GBE Family Controller)
3. \Device\NPF_{7807A886-992F-4942-B6B0-5AB2E55A44E2} (TAP-Windows Adapter V9)
4. \Device\NPF_{AD71183A-25C6-4BF4-8DC6-34E97D7DABE5} (Microsoft)
选择监听网卡 (1-4):2

正在监听 Realtek PCIe GBE Family Controller...
2020-03-16 13:35:45,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:45,00-00-00-00-00-00,183.232.93.22,9A-87-11-C6-E7-10,192.168.1.4
2020-03-16 13:35:46,00-00-00-00-00-00,183.232.93.22,9A-87-11-C6-E7-10,192.168.1.4
2020-03-16 13:35:46,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:47,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:48,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:49,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:50,00-00-00-00-00-00,183.232.93.22,9A-87-11-C6-E7-10,192.168.1.4
2020-03-16 13:35:50,00-00-00-00-00-00,192.168.1.9,00-00-00-00-00-01,239.255.255.250
2020-03-16 13:35:50,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:51,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:51,00-00-00-00-00-00,192.168.1.202,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:52,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:53,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:54,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:55,00-00-00-00-00-00,192.168.1.9,00-00-00-00-00-01,239.255.255.250
2020-03-16 13:35:55,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:56,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
2020-03-16 13:35:57,9A-87-11-C6-E7-10,192.168.1.4,FF-FF-FF-FF-FF-FF,192.168.1.255
```

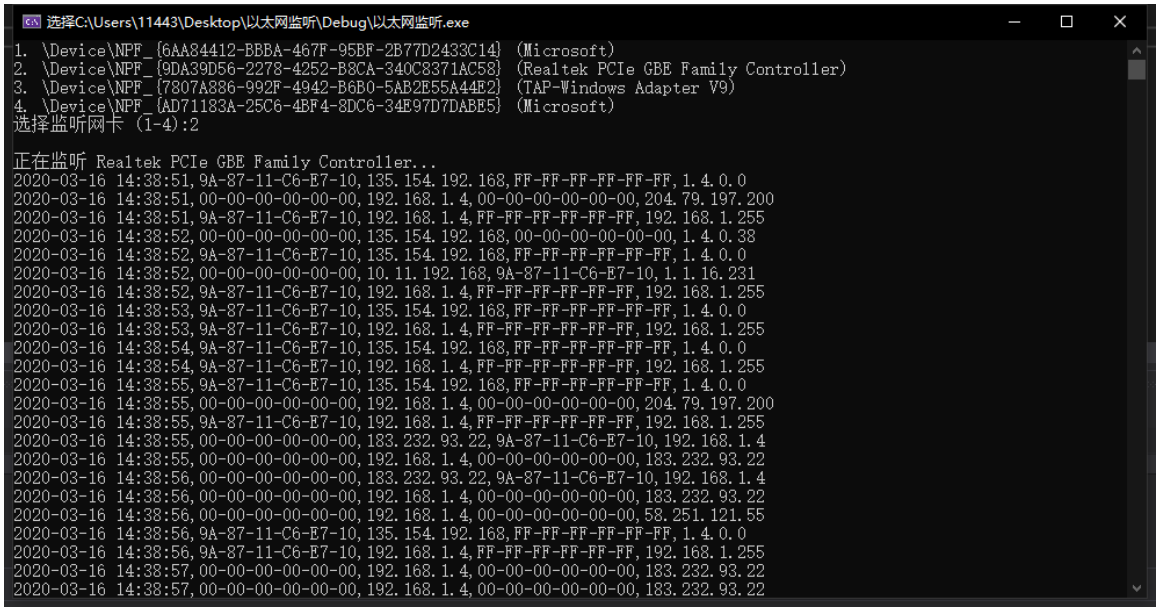
监听结果

初步尝试后可以自己动手实现自己的监听以太网工程了



首先配置好 WinPCAP 库到新建的工程

编程实现实验并运行，工程项目在附件中



监听结果

4 实验总结

渐渐克服了对接手大工程代码的恐惧感，对网卡的工作方式有更进一步的理解。