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 胡曼珑

学　　号 24320182203199

实验时间 2020 年 3 月 18 日

2020 年 3 月 24 日

1 实验目的

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

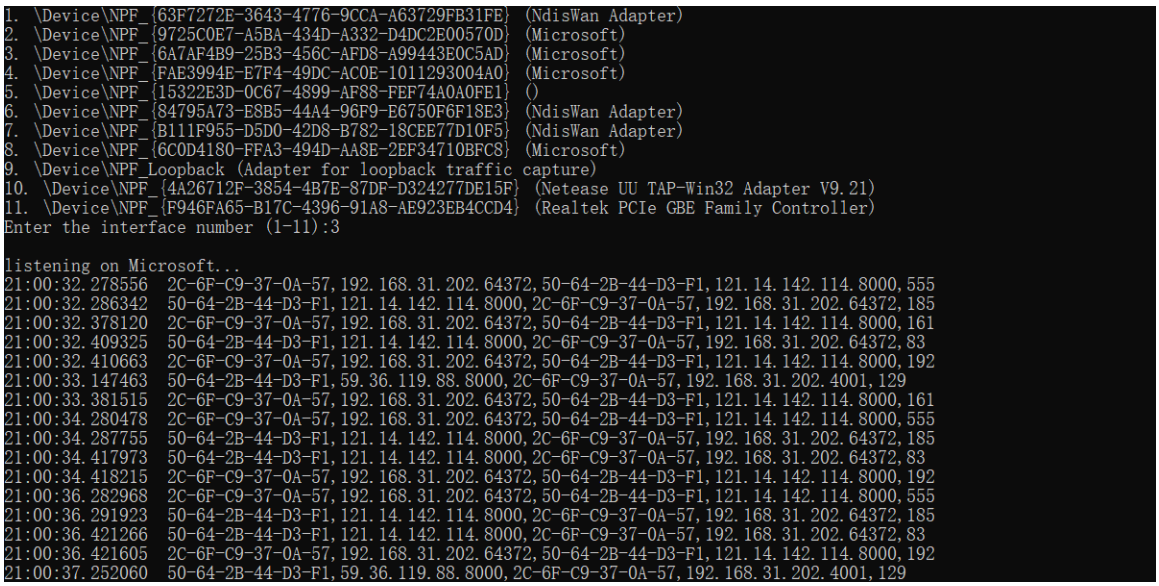
方的 MAC 和 IP 地址，并作记录与统计，对超过给定阈值（如：1MB）的流量进行告

警。

2 实验环境

win10，c，winCap。

3 实验结果



输出结果

```
source:
58-20-59-75-AA-FD,192.168.31.74, len=885
50-64-2B-44-D3-F1,192.168.31.1, len=20244
50-64-2B-44-D3-F1,59.36.119.88, len=2024
50-64-2B-44-D3-F1,121.14.142.114, len=7957
2C-6F-C9-37-0A-57,192.168.31.202, len=28003
dest:
50-64-2B-44-D3-F1,59.36.119.88, len=81
01-00-5E-7F-FF-FA,239.255.255.250, len=876
2C-6F-C9-37-0A-57,239.255.255.250, len=21129
2C-6F-C9-37-0A-57,192.168.31.202, len=9981
50-64-2B-44-D3-F1,121.14.142.114, len=27046
```

一分钟以后的统计结果

```
21:25:20.114962  2C-6F-C9-37-0A-57,192.168.31.202.64372,50-64-2B-44-D3-F1,121.14.142.114.8000,554
超出范围!
```

设阈值为 500 时，超出阈值的输出结果

4 实验总结

1、学习了解 winCap（主要在捕获、分析数据包方面）