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 罗贤甫

学　　号 24320182203245

实验时间 2020 年 3 月 14 日

2020 年　3　月　4　日

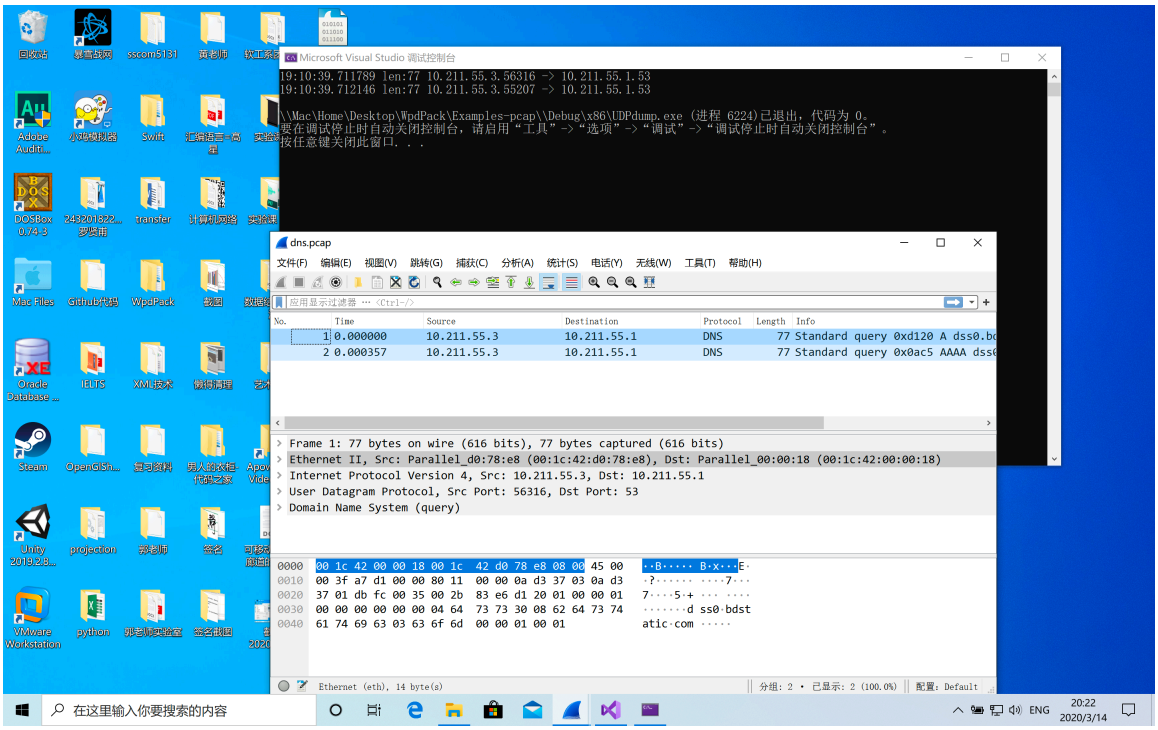
1 实验目的

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，并加以记录与统计，对超过给定阀值的流量进行警告。

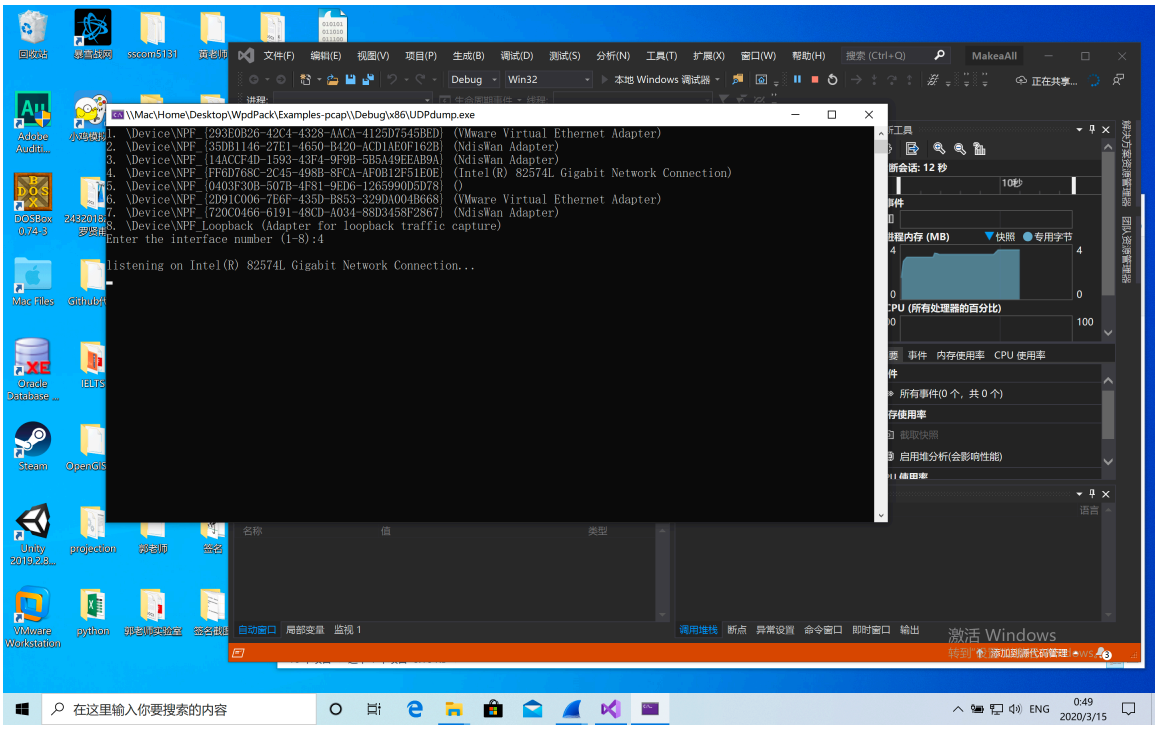
2 实验环境

Win10 系统，Visual Studio 2019，WireShark 软件，C 语言

3 实验结果



通过 WireShark 捕捉并加以实验



选择网卡编号

```
listening on Intel(R) 82574L Gigabit Network Connection...
2020-03-15 13:46:19,00-1C-42-00-00-18,10.211.55.3,58074,00-1C-42-D0-78-E8,10.211.55.1,53,85
2020-03-15 13:46:19,00-1C-42-00-00-18,10.211.55.3,56405,00-1C-42-D0-78-E8,10.211.55.1,53,85
Warning
```

取阀值为 256，在超过 256 时会发出警告，并按照实验手册输出时间，源 MAC、源 IP、目标 MAC、目标 IP、帧长度（以逗号间隔）达到实时监听的功能

```
以太网适配器 以太网:

   连接特定的 DNS 后缀 . . . . . . . : localdomain
   描述. . . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   物理地址. . . . . . . . . . . . . : 00-1C-42-D0-78-E8
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . . : fdb2:2c26:f4e4:0:f80e:6e6:c6eb:d4cf(首选)
   临时 IPv6 地址. . . . . . . . . . : fdb2:2c26:f4e4:0:39f5:3f00:4c4d:ff5f(首选)
   本地链接 IPv6 地址. . . . . . . . : fe80::f80e:6e6:c6eb:d4cf%17(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.211.55.3(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   获得租约的时间  . . . . . . . . . : 2020年3月15日 13:26:20
   租约过期的时间  . . . . . . . . . : 2020年3月15日 14:13:07
   默认网关. . . . . . . . . . . . . : 10.211.55.1
   DHCP 服务器 . . . . . . . . . . . : 10.211.55.1
   DHCPv6 IAID . . . . . . . . . . . : 100670530
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-25-78-28-EE-00-1C-42-D0-78-E8
   DNS 服务器  . . . . . . . . . . . : 10.211.55.1
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

在命令行窗口查看无限局域网 MAC 地址和 IP，与上述结果对照检查，结果正 确

4 实验总结

本次实验利用 WireShark 先捕获部分数据来调试，帮助我更好理解更好阅读本应有难度的代码，而老师的解说视频更是帮助我好好研究。通过这次实验，我对 MAC 地址以及 IP 地址都有了更深层次的理解，也更加理解网卡的运行过程。