

廈門大學



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 何明祥

学 号 24320182203193

实验时间 2020 年 3 月 11 日

2020 年 3 月 11 日

1 实验目的

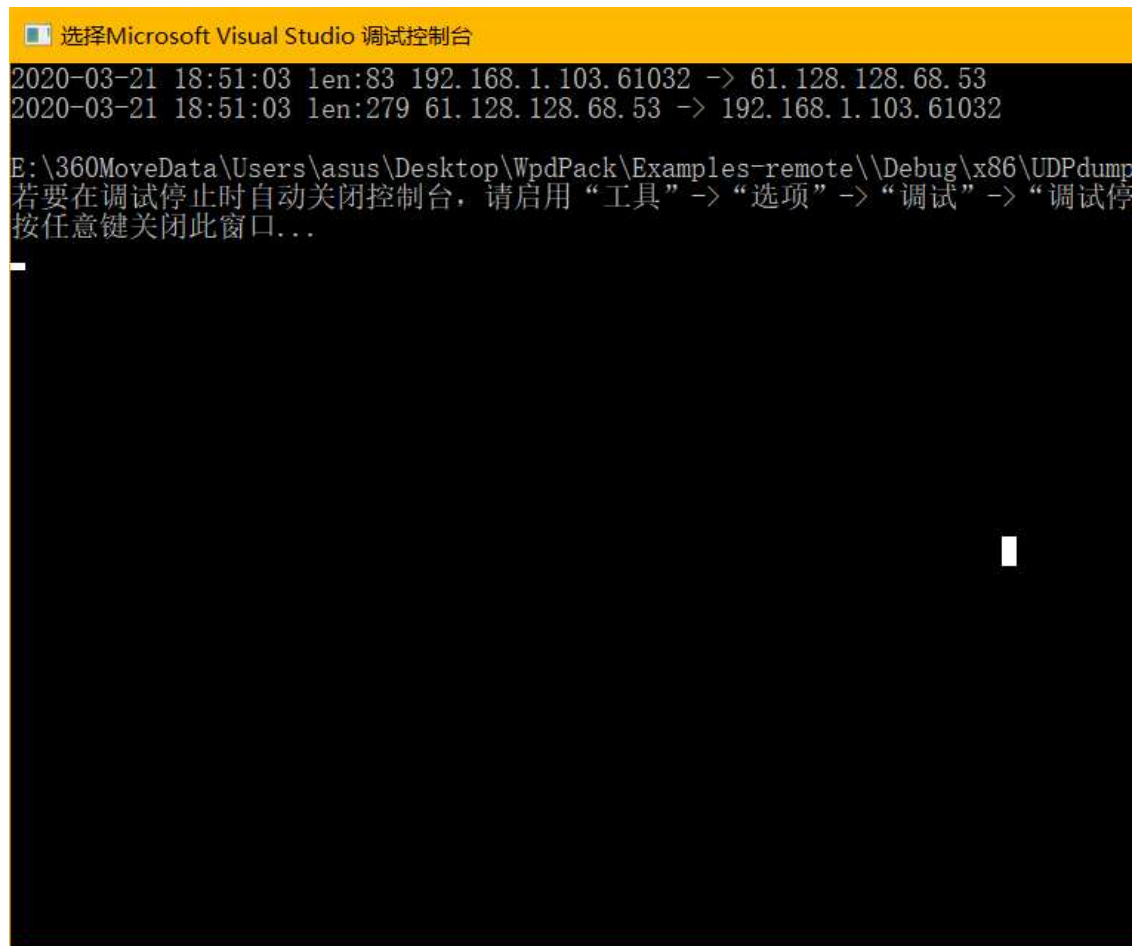
用 PCAP 库侦听并分析网络流量。

2 实验环境

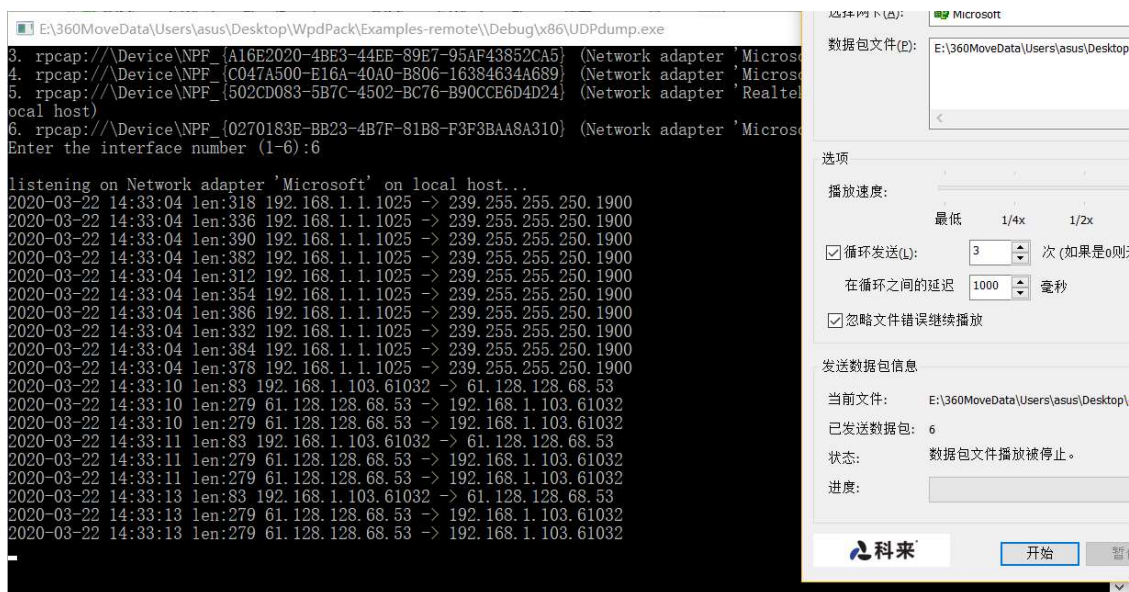
Win10 Visual Studio 2017 WinCAP 库

3 实验结果

调试部分：

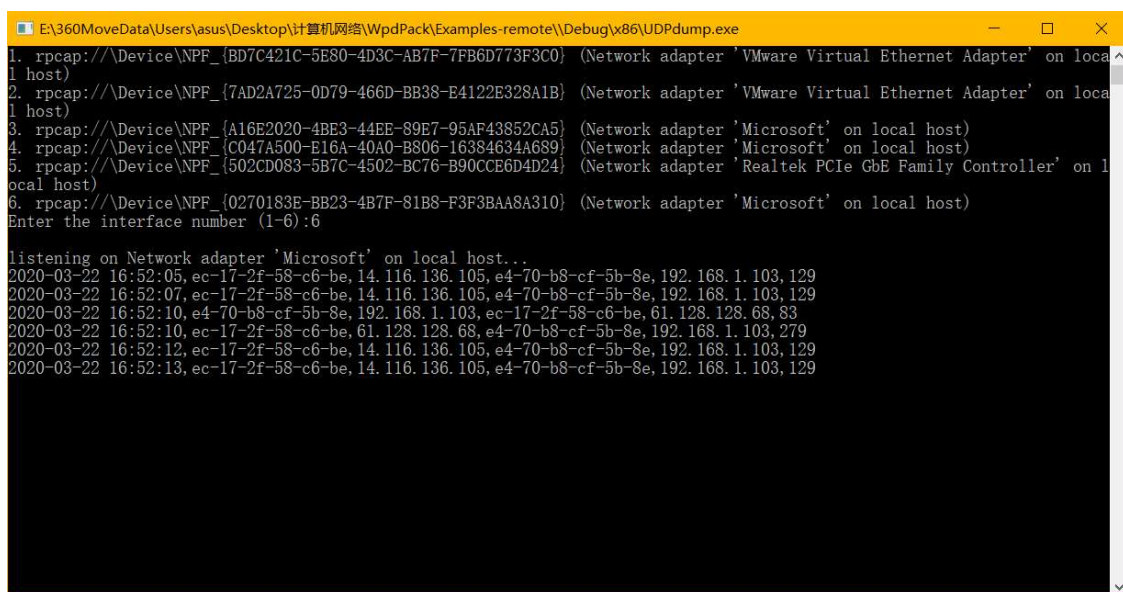


```
选择Microsoft Visual Studio 调试控制台
2020-03-21 18:51:03 len:83 192.168.1.103.61032 -> 61.128.128.68.53
2020-03-21 18:51:03 len:279 61.128.128.68.53 -> 192.168.1.103.61032
E:\360MoveData\Users\asus\Desktop\WpdPack\Examples-remote\Debug\x86\UDPdump
若要在调试停止时自动关闭控制台，请启用“工具”->“选项”->“调试”->“调试停
按任意键关闭此窗口...
```

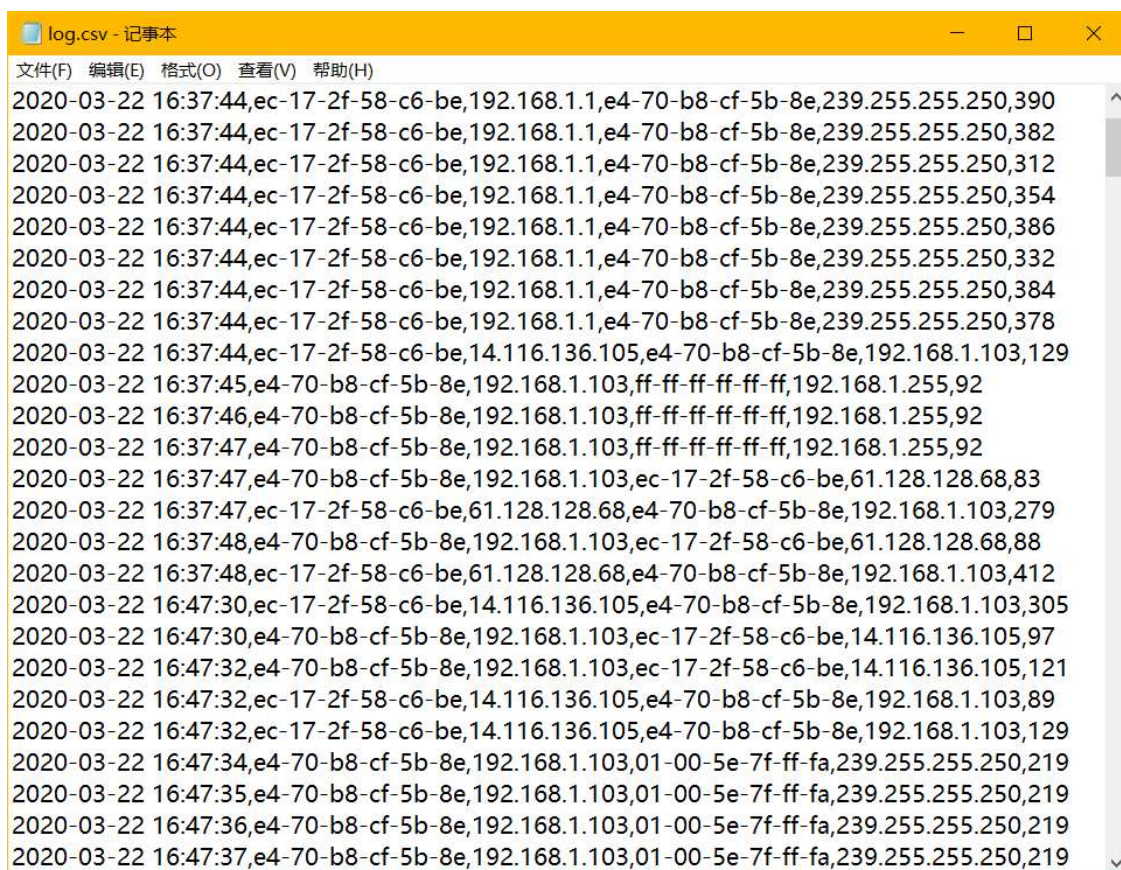


(断网之后 QQ 还能用所以多出许多帧)

修改代码后:



输出到 csv 文件中



```
log.csv - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
2020-03-22 16:37:44,ec-17-2f-58-c6-be,192.168.1.1,e4-70-b8-cf-5b-8e,239.255.255.250,390
2020-03-22 16:37:44,ec-17-2f-58-c6-be,192.168.1.1,e4-70-b8-cf-5b-8e,239.255.255.250,382
2020-03-22 16:37:44,ec-17-2f-58-c6-be,192.168.1.1,e4-70-b8-cf-5b-8e,239.255.255.250,312
2020-03-22 16:37:44,ec-17-2f-58-c6-be,192.168.1.1,e4-70-b8-cf-5b-8e,239.255.255.250,354
2020-03-22 16:37:44,ec-17-2f-58-c6-be,192.168.1.1,e4-70-b8-cf-5b-8e,239.255.255.250,386
2020-03-22 16:37:44,ec-17-2f-58-c6-be,192.168.1.1,e4-70-b8-cf-5b-8e,239.255.255.250,332
2020-03-22 16:37:44,ec-17-2f-58-c6-be,192.168.1.1,e4-70-b8-cf-5b-8e,239.255.255.250,384
2020-03-22 16:37:44,ec-17-2f-58-c6-be,192.168.1.1,e4-70-b8-cf-5b-8e,239.255.255.250,378
2020-03-22 16:37:44,ec-17-2f-58-c6-be,14.116.136.105,e4-70-b8-cf-5b-8e,192.168.1.103,129
2020-03-22 16:37:45,e4-70-b8-cf-5b-8e,192.168.1.103,ff-ff-ff-ff-ff-ff,192.168.1.255,92
2020-03-22 16:37:46,e4-70-b8-cf-5b-8e,192.168.1.103,ff-ff-ff-ff-ff-ff,192.168.1.255,92
2020-03-22 16:37:47,e4-70-b8-cf-5b-8e,192.168.1.103,ff-ff-ff-ff-ff-ff,192.168.1.255,92
2020-03-22 16:37:47,e4-70-b8-cf-5b-8e,192.168.1.103,ec-17-2f-58-c6-be,61.128.128.68,83
2020-03-22 16:37:47,ec-17-2f-58-c6-be,61.128.128.68,e4-70-b8-cf-5b-8e,192.168.1.103,279
2020-03-22 16:37:48,e4-70-b8-cf-5b-8e,192.168.1.103,ec-17-2f-58-c6-be,61.128.128.68,88
2020-03-22 16:37:48,ec-17-2f-58-c6-be,61.128.128.68,e4-70-b8-cf-5b-8e,192.168.1.103,412
2020-03-22 16:47:30,ec-17-2f-58-c6-be,14.116.136.105,e4-70-b8-cf-5b-8e,192.168.1.103,305
2020-03-22 16:47:30,e4-70-b8-cf-5b-8e,192.168.1.103,ec-17-2f-58-c6-be,14.116.136.105,97
2020-03-22 16:47:32,e4-70-b8-cf-5b-8e,192.168.1.103,ec-17-2f-58-c6-be,14.116.136.105,121
2020-03-22 16:47:32,ec-17-2f-58-c6-be,14.116.136.105,e4-70-b8-cf-5b-8e,192.168.1.103,89
2020-03-22 16:47:32,ec-17-2f-58-c6-be,14.116.136.105,e4-70-b8-cf-5b-8e,192.168.1.103,129
2020-03-22 16:47:34,e4-70-b8-cf-5b-8e,192.168.1.103,01-00-5e-7f-ff-fa,239.255.255.250,219
2020-03-22 16:47:35,e4-70-b8-cf-5b-8e,192.168.1.103,01-00-5e-7f-ff-fa,239.255.255.250,219
2020-03-22 16:47:36,e4-70-b8-cf-5b-8e,192.168.1.103,01-00-5e-7f-ff-fa,239.255.255.250,219
2020-03-22 16:47:37,e4-70-b8-cf-5b-8e,192.168.1.103,01-00-5e-7f-ff-fa,239.255.255.250,219
```

4 实验总结

学会了使用 WinCAP 库对网络流量进行侦听并获取其 MAC 地址，IP 地址，以及帧的长度

将实验报告填写完后，通过“Microsoft PDF 打印机”或其它 PDF 打印机，转为 PDF 文件提交。文件总大小尽量控制在 1MB 以下，勿超过 5MB。填表时，勿破坏排版，勿修改字体字号。打印前应将本段说明删除。