

**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 库侦听并解析FTP 口令**

**班 级 软件工程 2018 级 3 班**

**姓 名 沈黄隽**

**学 号 24320182203260**

**实验时间 2020 年 3 月 11 日**

**2020 年 3 月 24 日**

1. **实验目的**
   * 本实验是“用 PCAP 库侦听并解析 FTP 口令”实验的第一部分
   * 用 WinPACP 库侦听并分析以太网的帧，记录目标与源 MAC 和 IP 地址

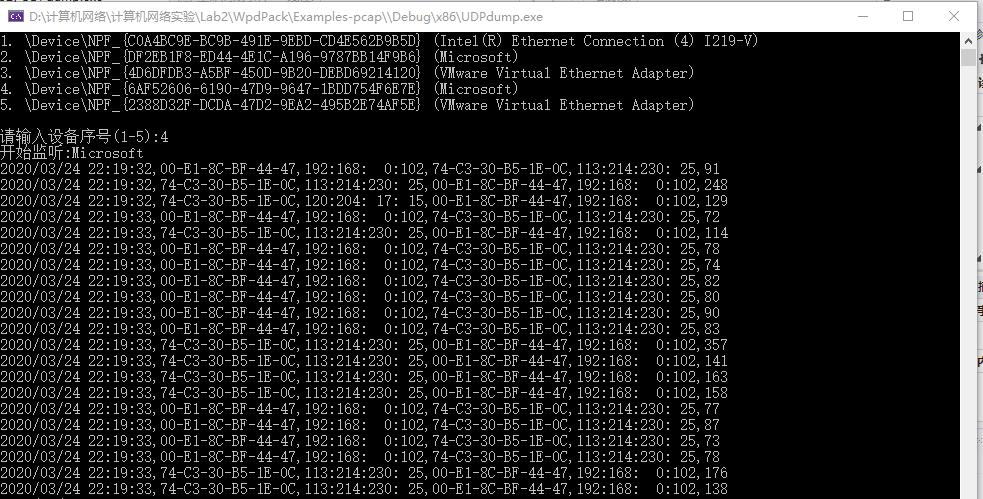
# 实验环境

操作环境：Visual Studio 2019、WpdPack

编程语言：C 语言

# 实验结果

1、基于 WinPCAP 工具包制作程序，实现监听网络上的数据流，解析发送方与接收方的 MAC 和 IP 地址，并作记录与统计，对超过给定阈值的流量进行告警。其中流量阈值为 0.5M，统计数据的时间长度间隔为 20 秒。



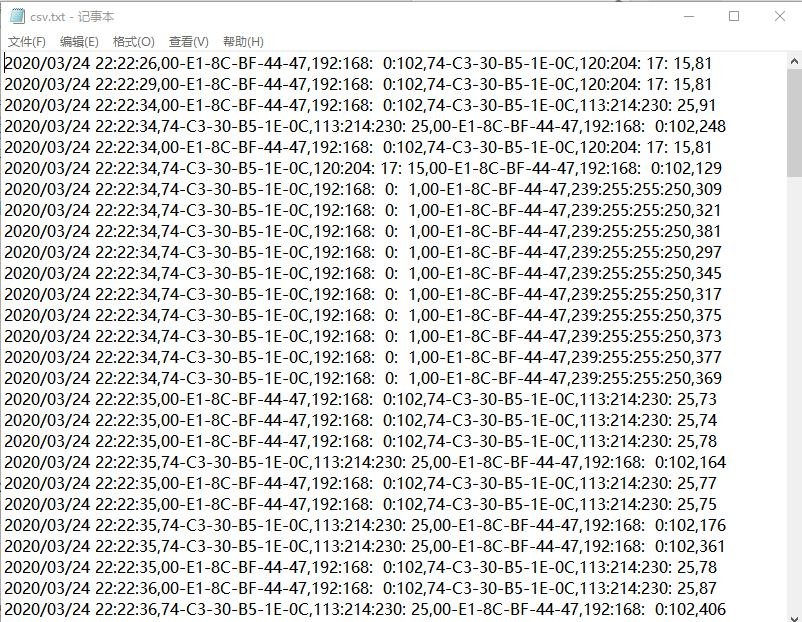
2.每隔一段时间（20s），程序统计来自不同 MAC 和 IP 地址的通信数据长度， 并以“Mac Address ，IP Address ，通信数据长度”的格式显示在输出流显示出来

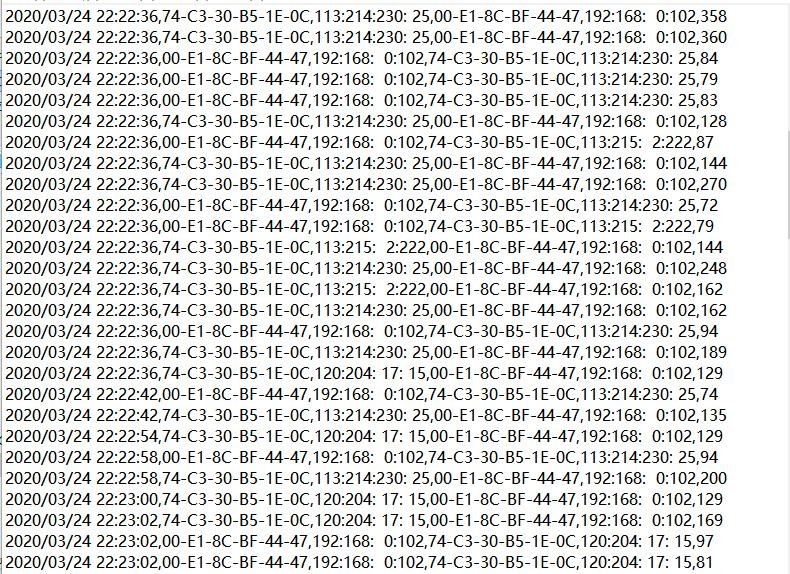


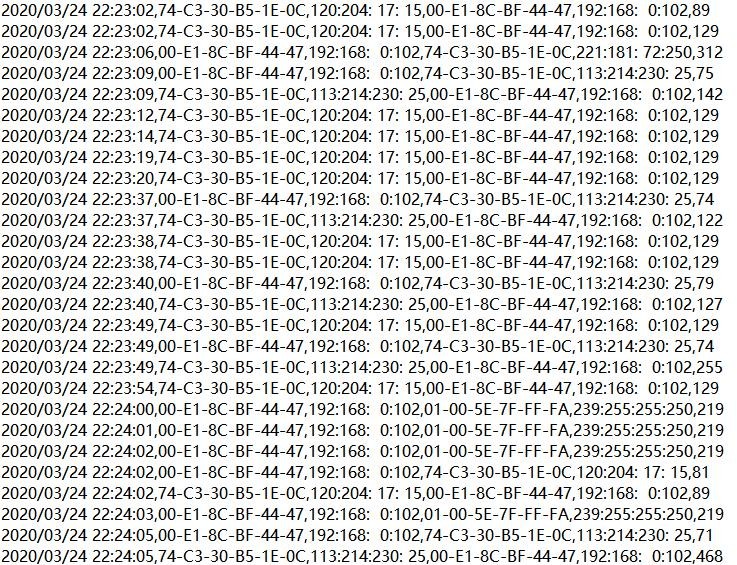


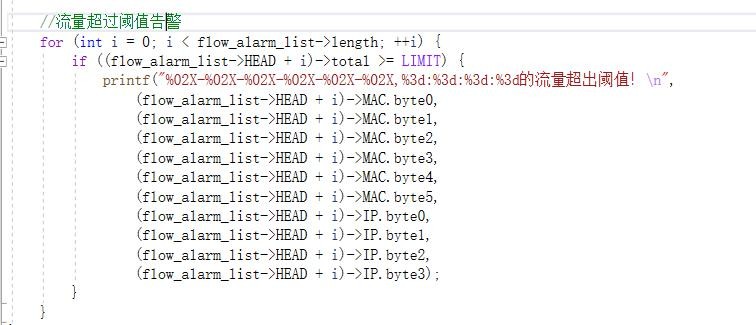


3、程序在文件上输出形如下列 CSV 格式的日志：时间、源 MAC、源 IP、目标MAC、目标 IP、帧长度（以逗号间隔）







4、流量超过阈值（0.5M）告警部分代码示例

# 实验总结

基于 WinPCAP 工具包制作程序，实现监听网络上的数据流，解析发送方与

接收方的 MAC 和 IP 地址，统计来自不同 Mac 和 IP 地址的通信数据长度，对帧监听以及收发有了更深入的了解