

# 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 库监听并分析以太网的帧

班    级 软件工程 2018 级

姓    名 贺青卓

学    号 34520182201499

实验时间 2020 年 3 月 11 日

2020 年 3 月 11 日

## 1 实验目的

实验 3 是“用 PCAP 库监听并解析 FTP 口令”实验的第一部分。

主要用 WinPCAP 或 libPcap 库监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（如：1MB/s）的流量进行告警。

最终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）

2015-03-14 13:05:16,60-36-DD-7D-D5-21,192.168.33.1,60-36-DD-7D-D5-72,192.168.33.2,1536

对于超过阈值的收发记录在显示器输出：

对于发送：[时间] [源 MAC，源 IP] SEND 长度 bytes out of limit.

对于接收：[时间] [目的 MAC，目的 IP] RECV 长度 bytes out of limit.

[2015-03-14 13:05:16] [60-36-DD-7D-D5-21,192.168.33.1,60] SEND 157106 bytes out of limit.

[2015-03-14 13:05:16] [60-36-DD-7D-D5-21,192.168.33.1,60] RECV 157106

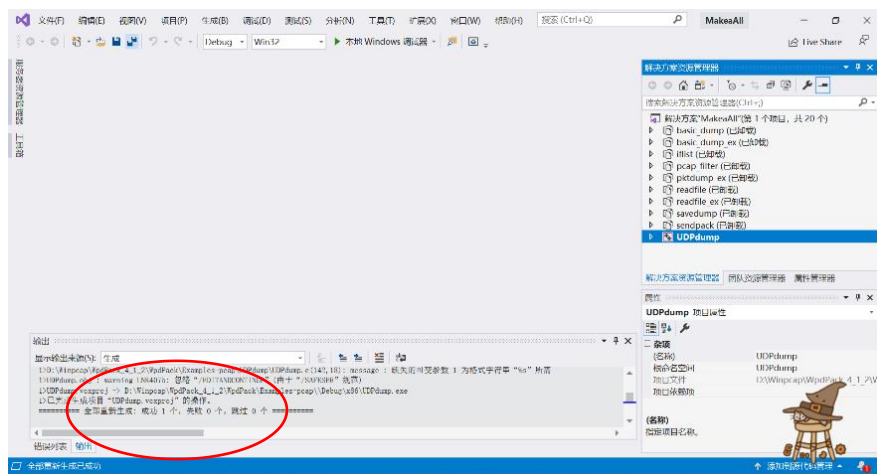
## 2 实验环境

Windows 系统下 VS2019、Winpcap、Wireshark

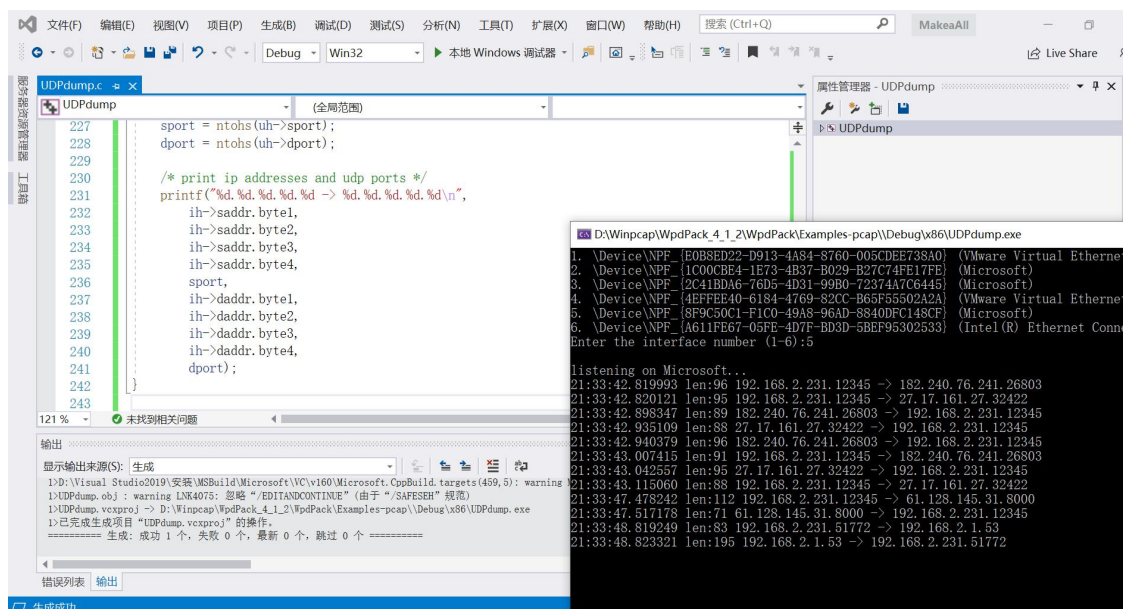
## 3 实验结果

### 一、环境配置

1、下载 Winpcap，运行源代码，并根据提示修正错误，运行成功截图如下

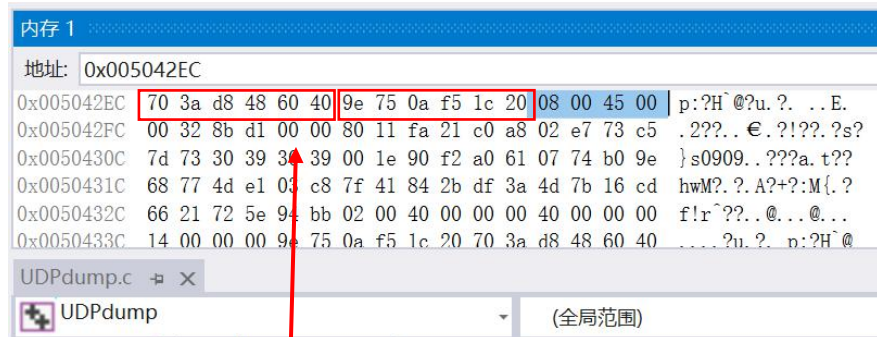


## 2、阅读、运行原本代码如下：



## 二、学习使用测试工具

### 1、在 VS2019 调试中获得 pkt\_data 的首地址，观察内存中的信息如下：



## 运行结果

```

14:30:38.511184 len:339
00 0C 29 73 69 8A 00 50 56 FC 52 95 08 00 45 00
01 45 1D FB 00 00 80 11 8C 56 C0 A8 07 02 C0 A8
07 04 00 35 CB 42
mac_header:
  dest_addr : 00 0C 29 73 69 8A
  src_addr : 00 50 56 FC 52 95
  type : 0800
ip_header
  ver_ihl : 45
  tos : 00
  tlen : 0145
  identification: 1DFB
  flags_fo : 0000
  ttl : 80
  proto : 11
  crc : 8C56
  op_pad : 0035CB42
  saddr : C0 A8 07 02 192.168.7.2
  daddr : C0 A8 07 04 192.168.7.4
  
```

有时候在这里还有PPPoE头

注意：MAC地址合理。

注意：IP Ver应为4

注意：IP地址合理。

2020-02-29 厦门大学信息学院软件工程系 黄炜 28

对照课件了解内容

## 2、学习使用 Wireshark 观察报文

## 三、根据实验要求编程，得到符合格式要求的输出

```

UDPdump.c
UDPdump
(全局范围) packet_handler(u_char *param, const pcap_

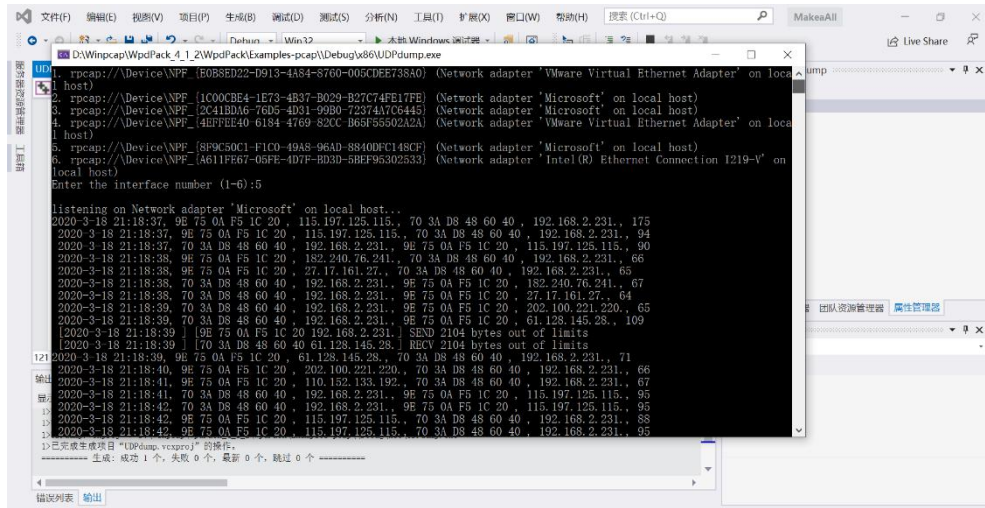
183 local_tv_sec = header->ts.tv_sec;
184 ltime = localtime(&local_tv_sec);
185 strftime(timestr, sizeof timestr, "%H:%M:%S", ltime);
186 printf("%s, ", timestr);
187
188 int length = sizeof(mac_header) + sizeof(ip_header);
189 mh = (mac_header*)pkt_data;
190 ih = (ip_header*)(pkt_data + sizeof(mac_header));
191
192 for (int i = 0; i < 6; i++) {
193     printf("%02X ", mh->dest_addr[i]);
194 }
195 printf(", ");
196 for (int i = 0; i < 4; i++) {
197     printf("%d.", ih->saddr[i]);
198 }
199 printf(", ");
  
```

(小部分代码截图)

1、输出形如下列 CSV 格式的日志：

时间、源 MAC、源 IP、目标 MAC、目标 IP、帧长度并对照步骤“二”中内容，判断显示正确，截图如下

```
2020-3-18 21:30:39, 70 3A D8 48 60 40, 192.168.2.231., 9E 75 0A F5 1C 20, 182.240.76.241., 201
2020-3-18 21:30:39, 70 3A D8 48 60 40, 192.168.2.231., 9E 75 0A F5 1C 20, 27.17.161.27., 200
2020-3-18 21:30:39, 70 3A D8 48 60 40, 192.168.2.231., 9E 75 0A F5 1C 20, 115.197.165.176., 199
2020-3-18 21:30:39, 70 3A D8 48 60 40, 192.168.2.231., 9E 75 0A F5 1C 20, 115.197.125.115., 198
2020-3-18 21:30:39, 70 3A D8 48 60 40, 192.168.2.231., 9E 75 0A F5 1C 20, 202.100.221.220., 201
```



2、对于超过阈值的收发记录在显示器输出：

对于发送：[时间][源 MAC，源 IP] SEND 长度 bytes out of limit.

对于接收：[时间][目的 MAC，目的 IP] RECV 长度 bytes out of limit.截图如下

```
[2020-3-18 21:30:26 ] [70 3A D8 48 60 40 110.152.133.192.] SEND 10160 bytes out of limits
[2020-3-18 21:30:26 ] [9E 75 0A F5 1C 20 192.168.2.231.] RECV 10160 bytes out of limits
```

## 4 实验总结

对网络信息传输有了更直接的体验和了解，学习了 WINPCAP 和 WIRESHARK.学习了如何在调试中观察内存，查看有关 MAC 地址、IP 报文的内容