# 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 王薪蕾

学　　号 24320182203285

实验时间 2020 年 3 月 11 日

**2020 年　3 月　11 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 WinPCAP 或 libPcap 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，并作记录与统计，对超过给定阈值（如：1MB）的流量进行告警。对 Linux 用户，可以使用 libpcap 编程实现。

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）

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

每隔一段时间（如 1 分钟），程序统计来自不同 MAC 和 IP 地址的通信数据长度，统计发至不同 MAC 和 IP 地址的通信数据长度。

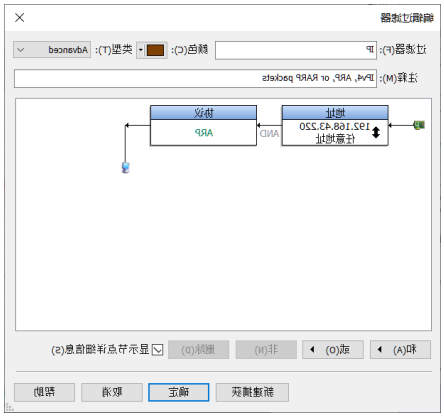
# 2 实验环境

操作系统：windows，编程语言：C++

# 3 实验结果

3.2 使用 OmniPeek 捕获链路数据帧

完成捕获设置：



ping192.168.2.1 结果：

```
C:\Users\adminster>ping 192.168.43.1

正在 Ping 192.168.43.1 具有 32 字节的数据:
来自 192.168.43.1 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.43.1 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.43.1 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.43.1 的回复: 字节=32 时间=4ms TTL=64

192.168.43.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 3ms, 最长 = 4ms, 平均 = 3ms
```

抓包

```
Packet Info
    Packet Number:          1
    Flags:                  0x00000000
    Status:                 0x00000000
    Packet Length:          64
    Timestamp:              15:08:50.290202100 03/14/2020
Ethernet Type 2
    Destination:            98:3B:8F:18:71:A8 [0-5]
    Source:                 96:63:72:60:19:83 [6-11]
    Protocol Type:          0x0806  IP ARP [12-13]
ARP - Address Resolution Protocol
    Hardware:               1  Ethernet (10Mb) [14-15]
    Protocol:               0x0800  IP [16-17]
    Hardware Addr Length:   6 [18]
    Protocol Addr Length:   4 [19]
    Operation:              1  ARP Request [20-21]
    Sender Hardware Addr:   96:63:72:60:19:83 [22-27]
    Sender Internet Addr:   192.168.43.1 [28-31]
    Target Hardware Addr:   00:00:00:00:00:00  Xerox:00:00:00  (ignored) [32-37]
    Target Internet Addr:   192.168.43.220 [38-41]
Extra bytes
    Number of bytes:        (18 bytes) [42-59]
FCS - Frame Check Sequence
```

3.3

连接 ftp

```
:\Users\adminster>ftp 121.192.180.66
连接到 121.192.180.66。
220 Serv-U FTP Server v6.2 for WinSock ready...
501 Invalid option.
用户(121.192.180.66:(none)): student
331 User name okay, need password.
密码:
230 User logged in, proceed.
ftp> bye
221 Goodbye!

:\Users\adminster>
```

握手步骤的四个包

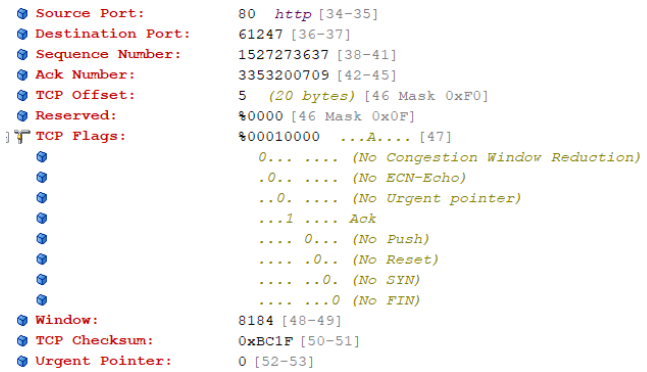
```
TCP Flags:              %00000010  .....S. [47]
    0... .... (No Congestion Window Reduction)
    .0.. .... (No ECN-Echo)
    ..0. .... (No Urgent pointer)
    ...0 .... (No Ack)
    .... 0... (No Push)
    .... .0.. (No Reset)
    .... ..1. SYN
    .... ...0 (No FIN)
Window:                 8192 [48-49]
TCP Checksum:           0x1AAE  Checksum invalid. Should be:  0x90E9 [50-51]
Urgent Pointer:         0 [52-53]
```

```
TCP Flags:              %00010010  ...A..S. [47]
    0... .... (No Congestion Window Reduction)
    .0.. .... (No ECN-Echo)
    ..0. .... (No Urgent pointer)
    ...1 .... Ack
    .... 0... (No Push)
    .... .0.. (No Reset)
    .... ..1. SYN
    .... ...0 (No FIN)
```

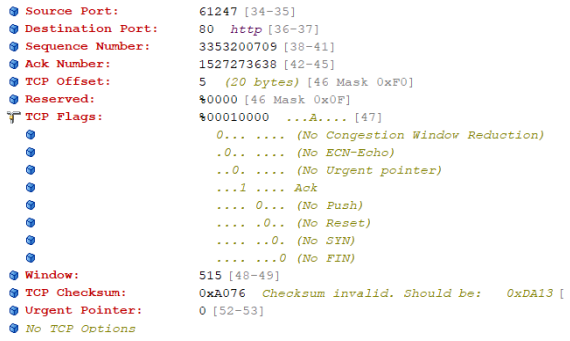
```
TCP Flags:              %00010000  ...A.... [47]
    0... .... (No Congestion Window Reduction)
    .0.. .... (No ECN-Echo)
    ..0. .... (No Urgent pointer)
    ...1 .... Ack
    .... 0... (No Push)
    .... .0.. (No Reset)
    .... ..0. (No SYN)
    .... ...0 (No FIN)
```

```
TCP Flags:              %00011000  ...AP... [47]
    0... .... (No Congestion Window R
    .0.. .... (No ECN-Echo)
    ..0. .... (No Urgent pointer)
    ...1 .... Ack
    .... 1... Push
    .... .0.. (No Reset)
    .... ..0. (No SYN)
    .... ...0 (No FIN)
```

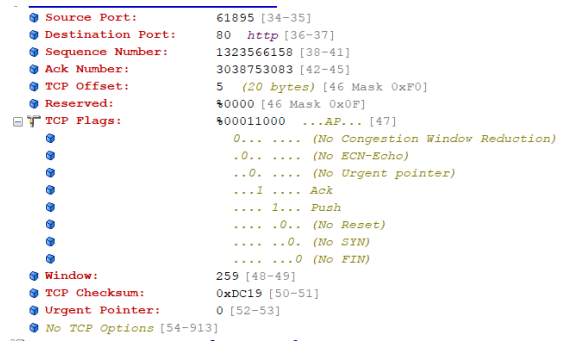
连接 http



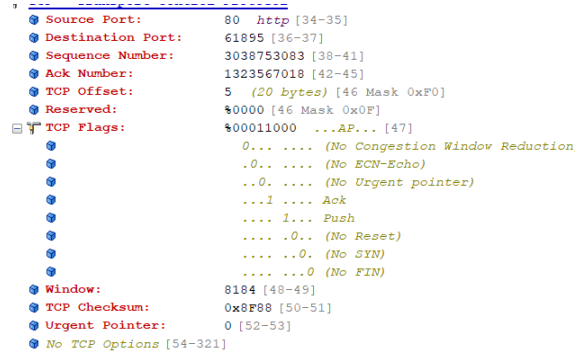

网站向本机发来 ACK




本机向网站发送 ACK

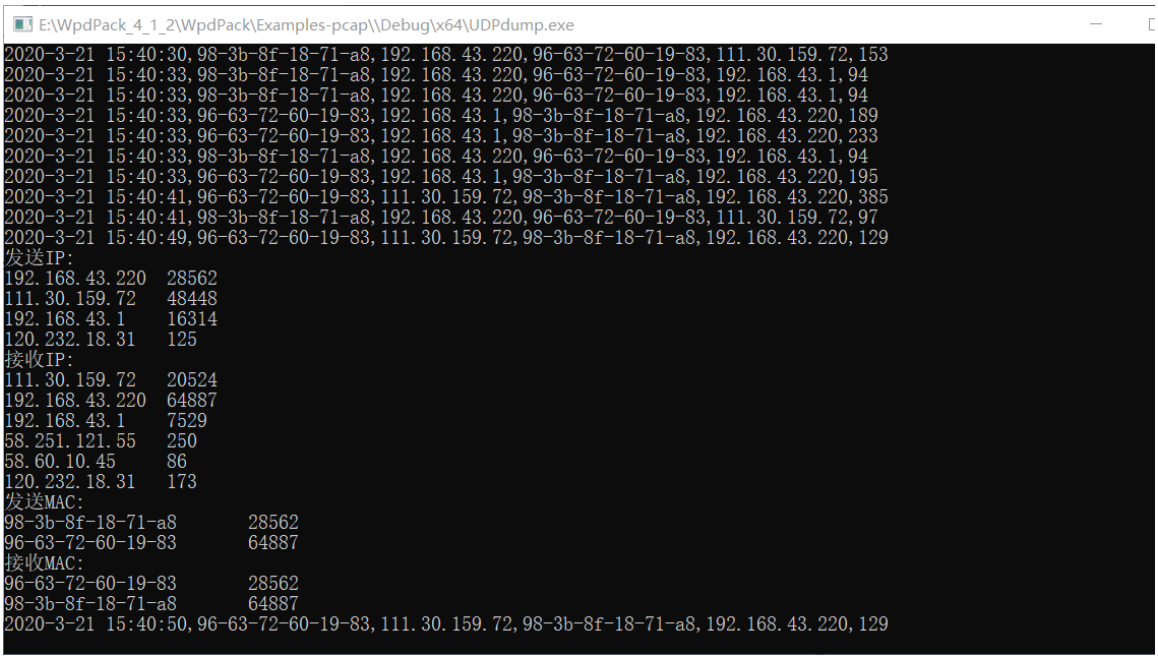



本机发送 发送位 PUSH




网站发送 发送位 PUSH

## 3.4 每一分钟统计一次




# 4 实验总结

更了解了数据包的组成，学会简单编写分析数据包。