

****

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**

# 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。

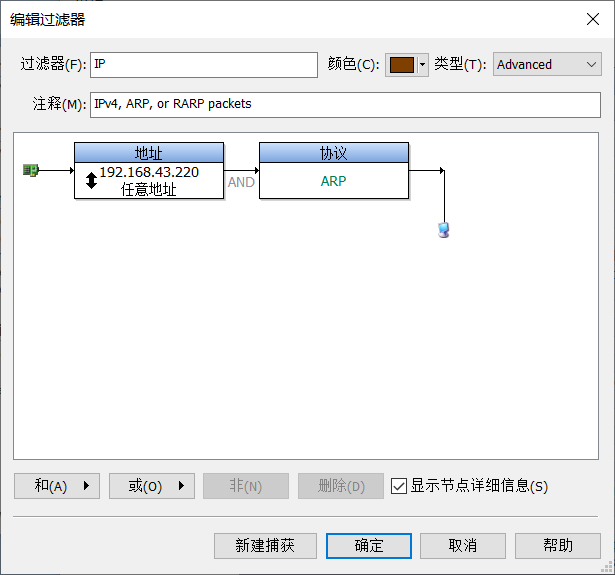
# 实验环境

操作系统：windows，编程语言：C++

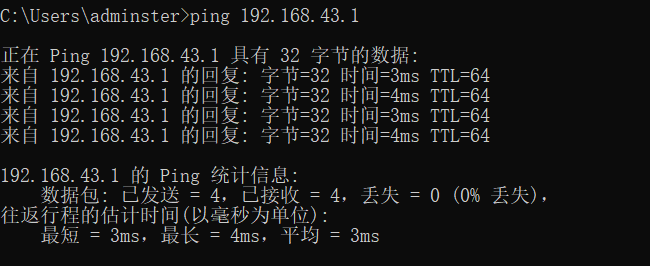
# 实验结果

3.2使用OmniPeek捕获链路数据帧

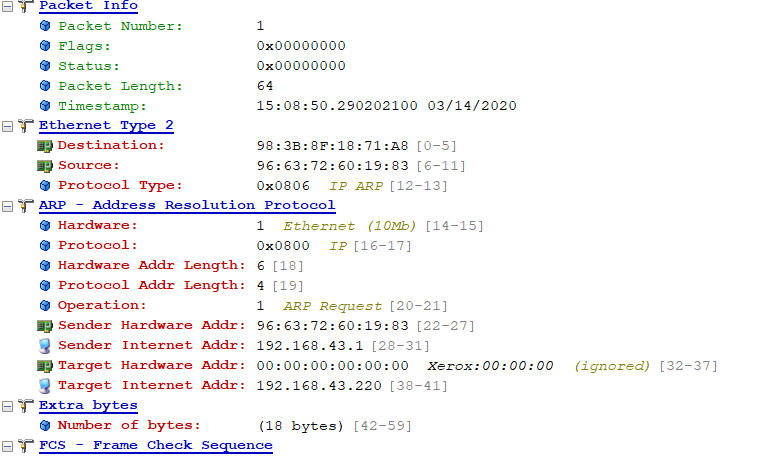
完成捕获设置 ：



ping192.168.2.1结果：

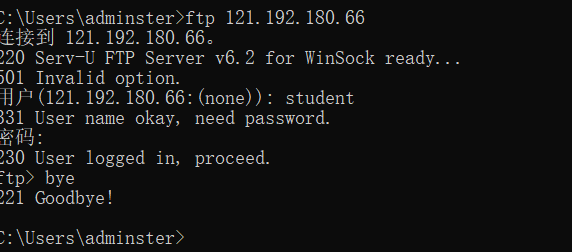


抓包

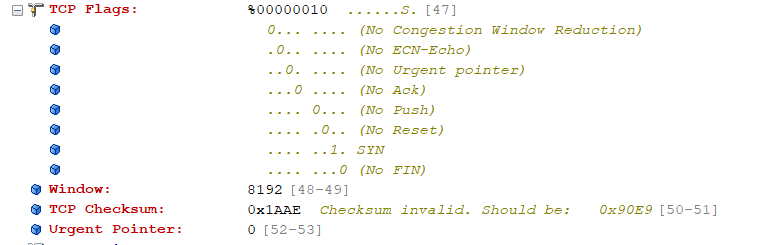
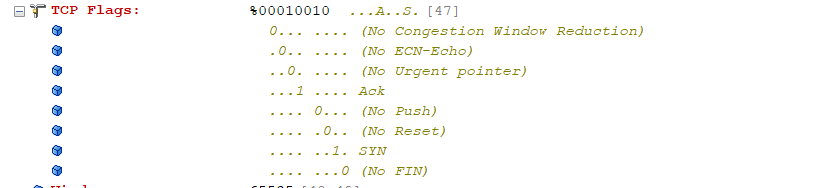
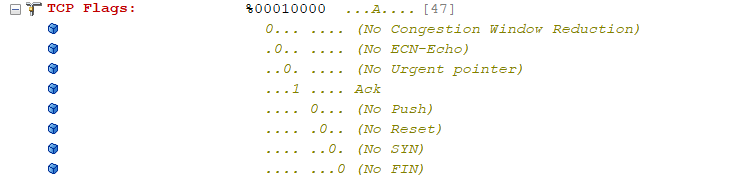
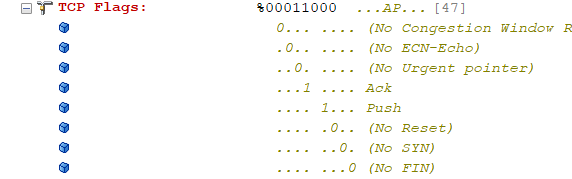


3.3

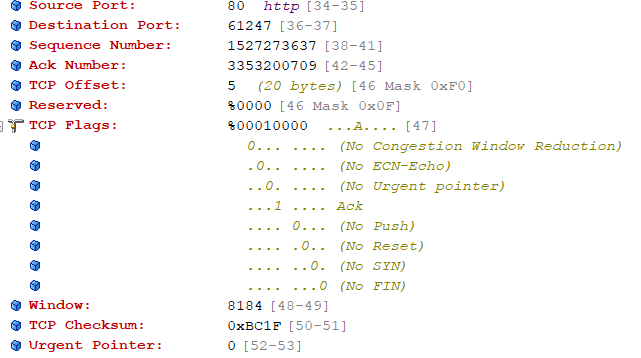
连接ftp

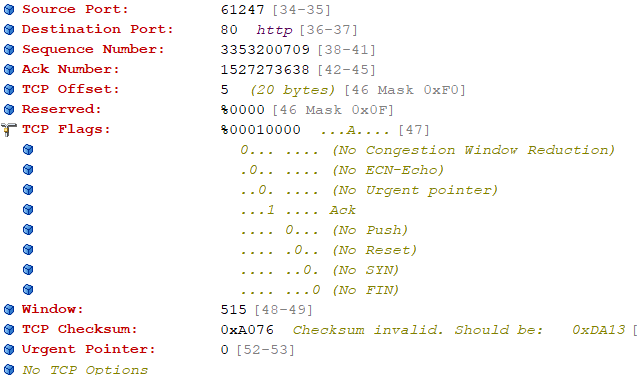


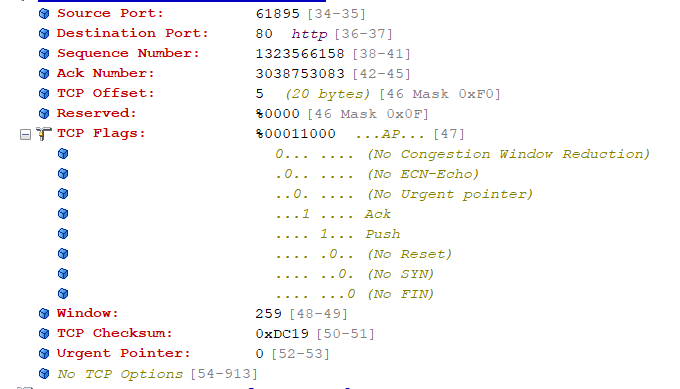
握手步骤的四个包

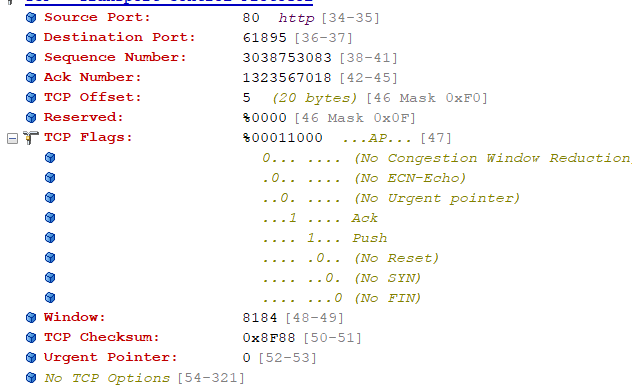
   

连接http

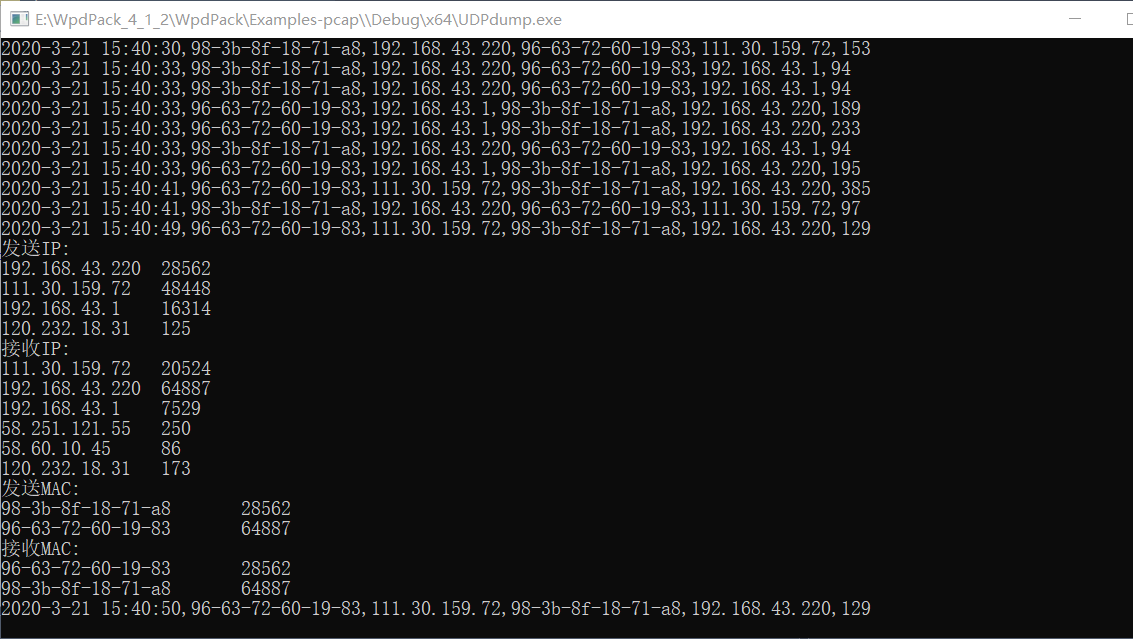
网站向本机发来ACK

 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



# 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。