

网络安全实验报告

题 目 捕包软件的使用与实现

专 业 信息安全

学 号 2021111000

学 生 李卓凌

指 导 教 师 王彦

**一、实验目的**

理解捕包程序捕包过程，可以自己编程捕包并从数据包中解析出需要的信息。

# 二、实验内容

1. 熟练使用 sniffer 或 wireshark 软件，对协议进行还原（能够找访问网页的四元组）；只需要写报告，不需要在实验课检查。
2. 利用 libpcap 进行编程，能够对本机的数据包进行捕获分析（比如将本机所有数据包的四元组写到指定文件），按照自己的设想撰写需求分析和详细设计。（实验课检查程序）

# 三、实验过程

**（一）使用 wireshark 软件对协议进行还原**

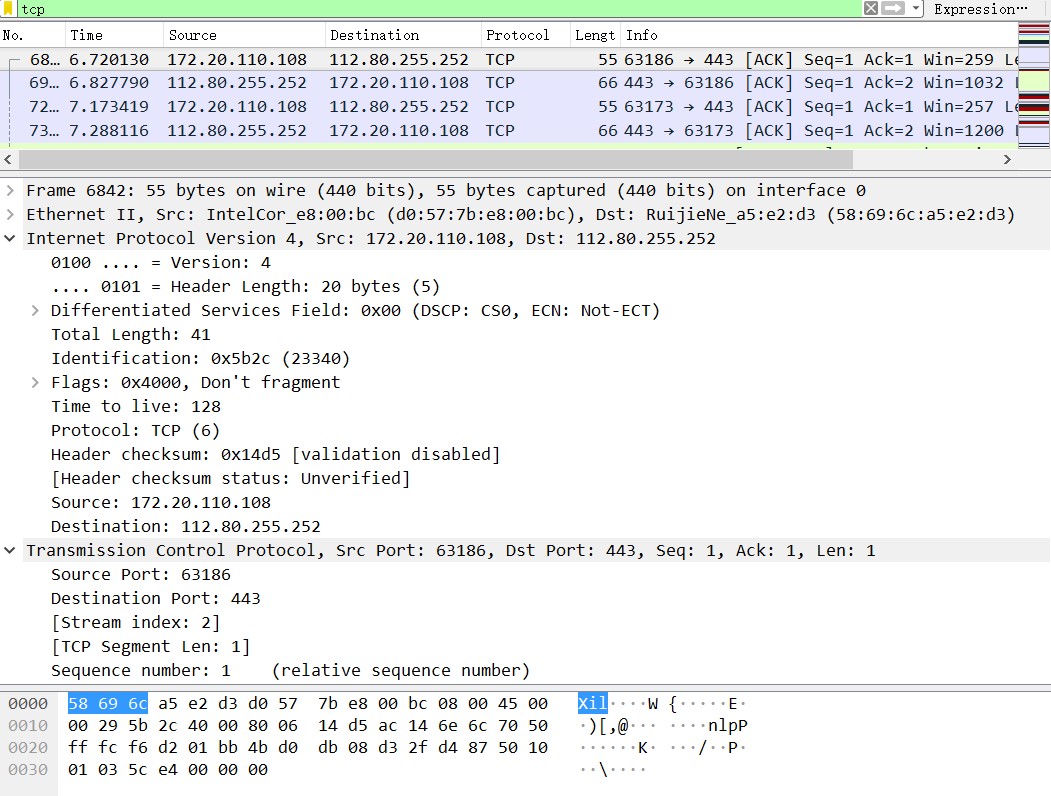
## 实验基本信息：

实验环境：Windows10 x64

WireShark2.6.4

## 1. 捕包并分析四元组

(1) TCP 分析



截图中这个 TCP 数据包，源 IP 为 172.20.110.108，目的 IP 为 112.80.255.252，源

端口为 63186，目的端口为 443。

分析：以太网头部：

前 6 个字节 58 69 6c a5 e2 d3 为目的主机 MAC，往后 6 个字节 d0 57 7b e8 00 bc 为源主机 MAC，

往后 2 个字节为上层协议，0x0800 表示 IPv4 协议；以太网头部结束，现在是 ip 头部：往后 1 个字节 0x45 表示 IP 版本为 4，头部长度为 5，往后 1 个字节为区分服务，0x00 表示默认，

往后 2 个字节为总长度，0x0029 = 41，往后 2 个字节为 id，值为 0x5b2c（23340），

往后 2 个字节为标志位+片偏移，值为 0x4000，

往后 1 个字节为 ttl，值为 0x80 = 128，

往后 1 个字节为上层协议，0x06 表示 TCP 协议，往后 2 个字节为头部校验和，值为 0x14d5，

往后 4 个字节为源 ip 地址 0xac146e6c，转换为 10 进制就是 172.20.110.108，往后4个字节为目的ip地址0x7050fffc，转换为10进制就是112.80.255.252；

ip 头部结束：现在是 TCP 头部：

往后 2 个字节为源端口 0xf6d2 = 63186，往后 2 个字节为目的端口 0x01bb = 443，往后 4 个字节为 seq 0x4bd0db08，往后 4 个字节为 ack 0xd32fd487，

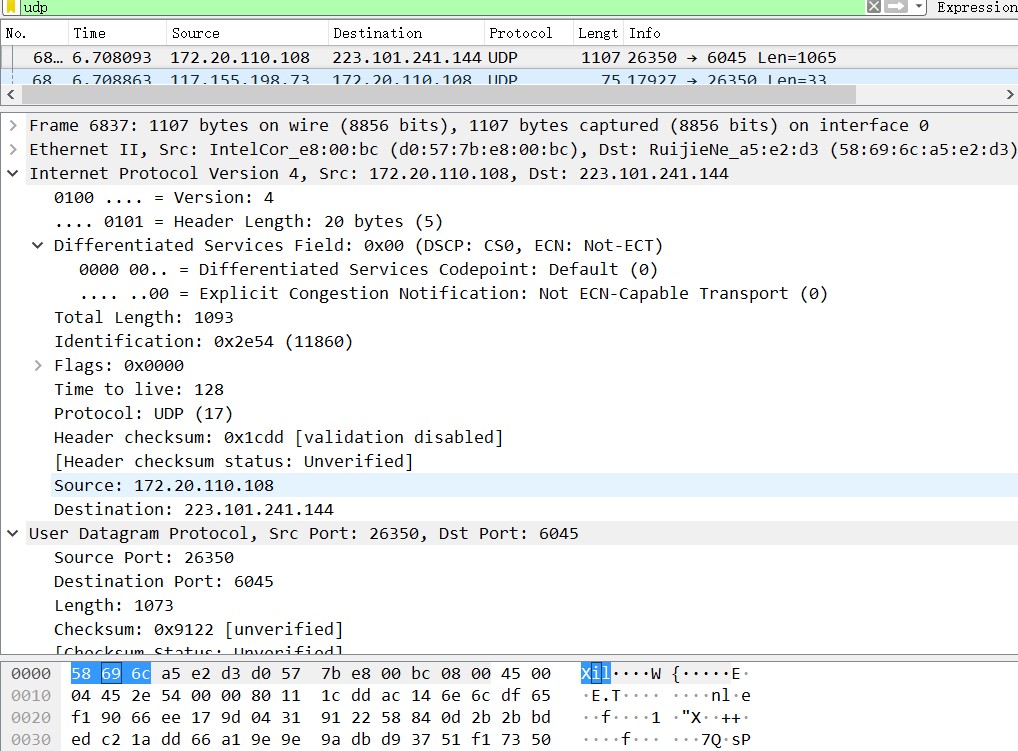
往后 1 个字节为头部长度 0x50 = 80（其实是 4 位），

往后 1 个字节为标志位（其实是 6 位），

往后 2 个字节为窗口大小 0x0103 = 259，往后 2 个字节为校验和 0x5ce4，

往后 2 个字节为紧急指针 0x0000； TCP 头部结束，接下来是数据。

(2) UDP 分析



截图中这个 UDP 数据包，源 IP 为 172.20.110.108，目的 IP 为 223.101.241.144，

源端口为 26350，目的端口为 6045。

分析：

以太网头部和 ip 头部与 TCP 协议基本相同，直接分析 UDP 头部，从第三行第三个字节开始：

2 个字节源端口 0x66ee = 26350，

2 个字节目的端口 0x179d = 6045，

2 个字节总长度 0x0431 = 1073， 2 个字节校验值：0x9122；

后面全都是数据。

**（二）利用 libpcap 编写捕包软件实验基本信息：**

实验环境：Ubuntu22.04 x64

编程语言：C 语言

## 1. 需求分析

本程序需要运用 libpcap 来捕获本机数据包，并获取数据包中的四元组，将其展示给

用户。

程序功能：

(1)捕获本机数据包（可以自定义过滤条件）；

(2)逐层解析数据包，获得 IPv4 数据包的源 ip、目的 ip、源端口、目的端口；

(3)将上述四元组写入文件（每次运行程序都新生成一个文件）。

## 2. 数据结构设计

由于是逐层解析以太网数据帧，所以需要准备至少三种数据结构：以太网数据帧头、

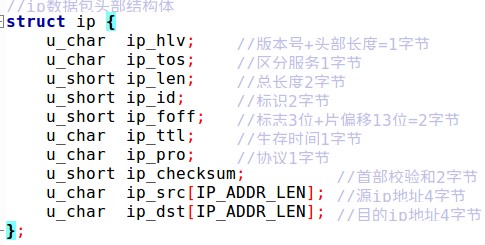
IPv4 数据报头、传输层报文头。具体如下：

数据结构的定义原则：1 字节数据定义为 u\_char，2 字节数据定义为 u\_short，其他 2 的倍数字节的数据（MAC 地址和 IP 地址）定义为 u\_char 数组（TCP 的序列号和 ack 定义为 u\_int，因为它们的表现形式就是一个数字，但地址我们通常是一个一个字节分开解析的）。

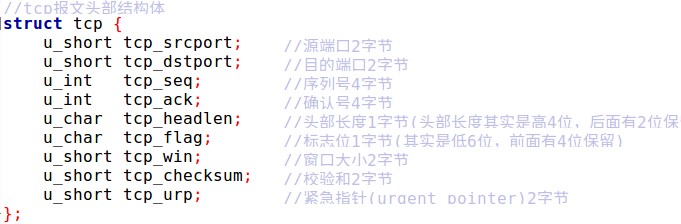
1. 以太网数据帧头



1. IPv4 数据报头



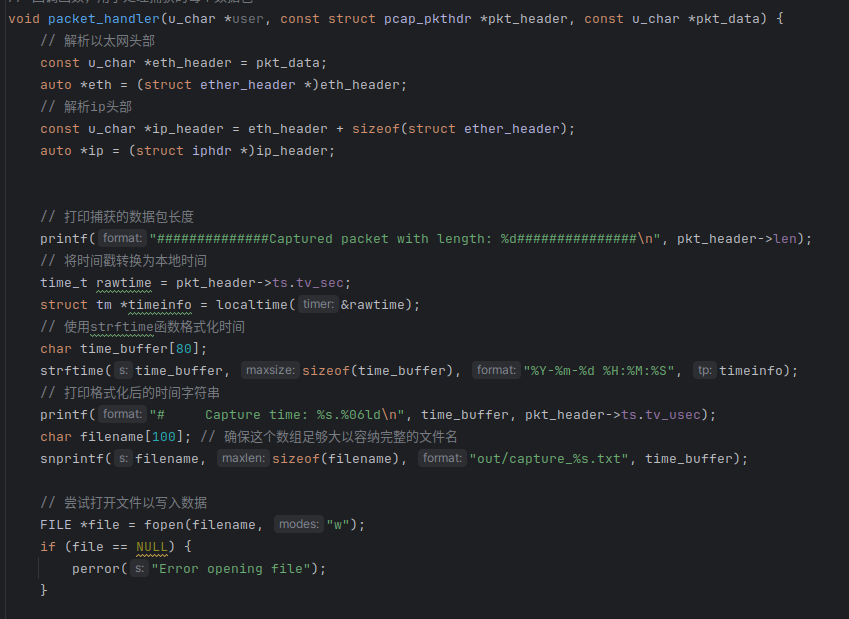
1. TCP 报文头

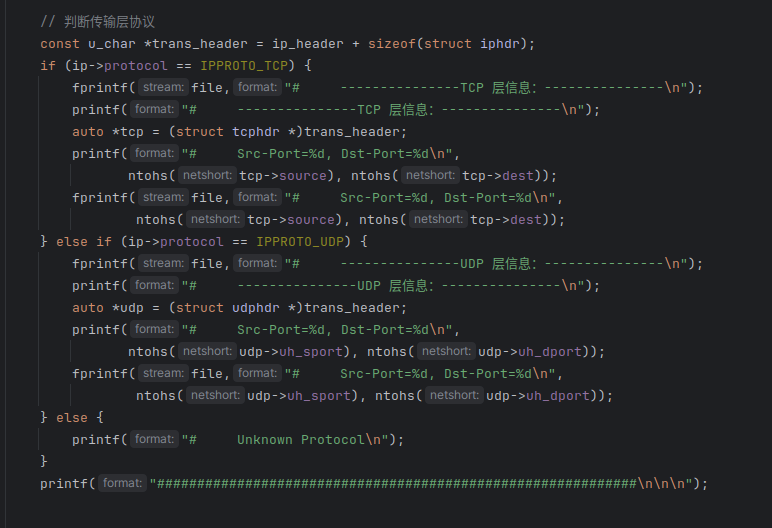


1. UDP 报文头



## 3. 回调函数设计





## 4. 主函数设计



## 6. 编译运行

使用下列命令编译：

gcc pcap.c -Wall -lpcap -o pcap

其中-Wall 参数指打印所有警告信息，-lpcap 用来链接 pcap 库。

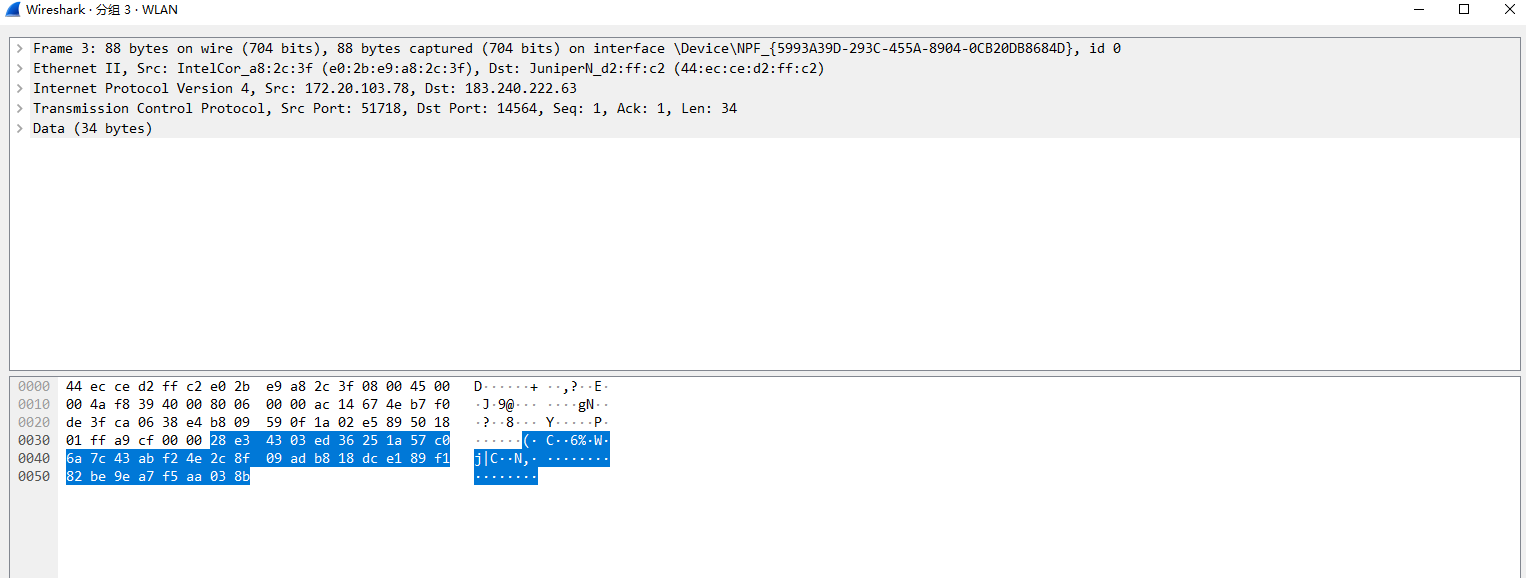
使用下列命令运行：

**sudo** ./pcap

捕包程序在运行时需要 root 权限，否则无法正常打开。

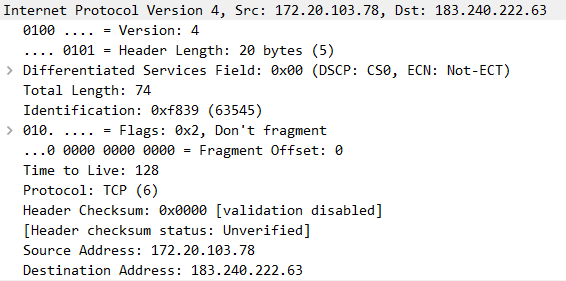
# 四、实验结果

1. **使用 wireshark 软件对协议进行还原**



对这个tcp数据包进行分析：

Ip：

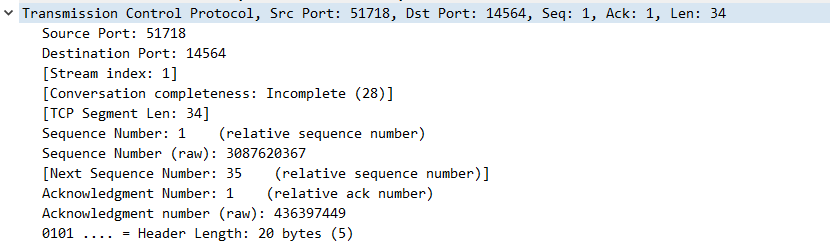


可以看到源ip和目的ip





Tcp：



可以看到源端口和目的端口：





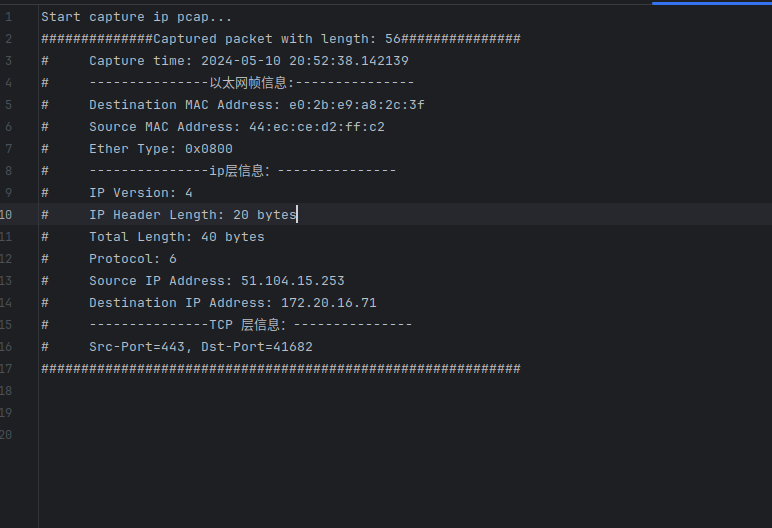
目的主机mac：

源主机mac：

Udp分析类似；

1. **利用 libpcap 编写捕包软件**

以下为捕包时文件中部分输出：



# 五、心得体会

深入理解网络通信：通过分析数据包四元组，不仅仅是在处理数据包，还在深入理解网络通信的基本原理。了解到数据包中包含的重要信息，如源IP、目的IP、源端口和目的端口，这些信息对于理解网络通信的目的和过程至关重要。

提高编程技能：使用libpcap库进行数据包分析是一项高级的编程任务，这需要对网络编程和底层数据包处理有一定的了解。在完成这项任务的过程中，提高了自己的编程技能，尤其是对于C/C++语言和网络编程方面的技能。

加强网络安全意识：通过分析数据包四元组，对网络安全产生更深的认识。可以识别出潜在的网络威胁，如恶意IP地址、异常端口等，并采取相应的防御措施，加强网络安全防护意识。