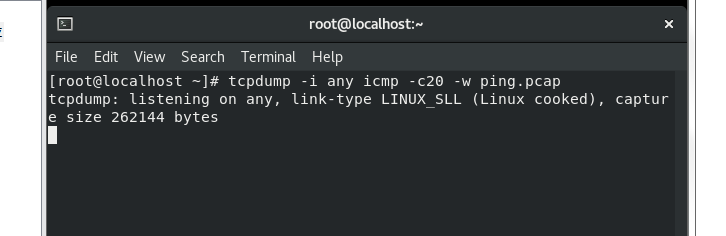
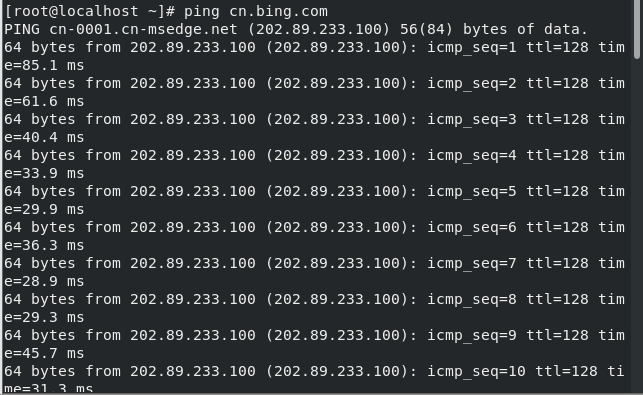
信息安全课程实验二

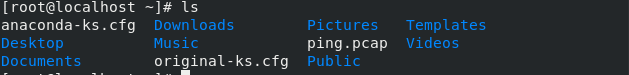
祝天赐 201920201042 19生物3班

实验A

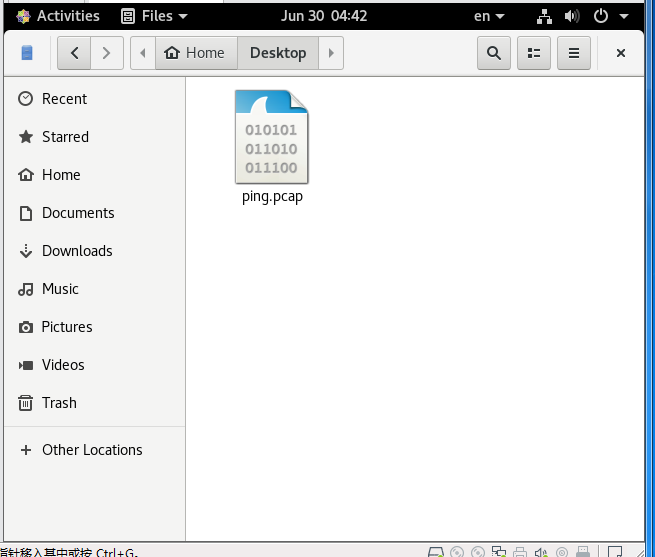
1. 在虚拟机centOS8的终端窗口输入tcpdump命令抓包
2. 在新建终端窗口中ping http：//cn.bing.com



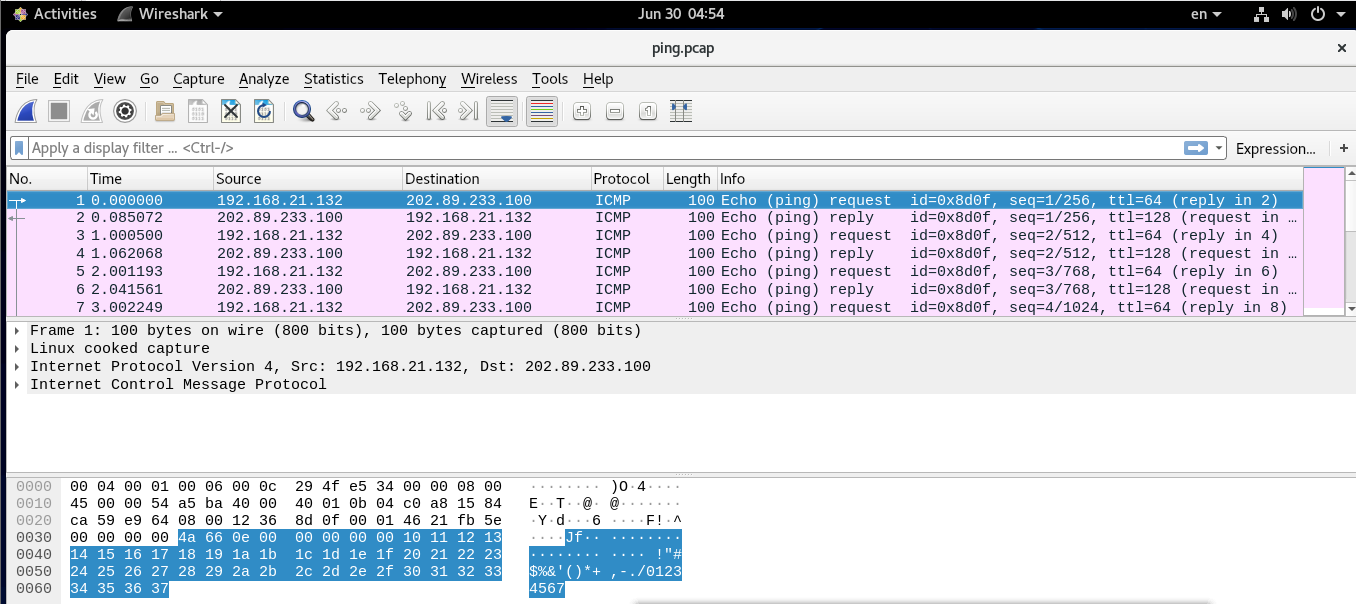
1. 输入ls查看当前目录下有没有ping.pcap文件



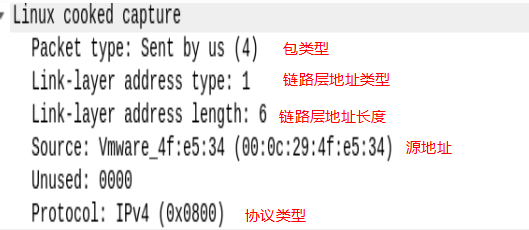
1. 输入mv ./ping.pcap ./Desktop 把文件移动到桌面

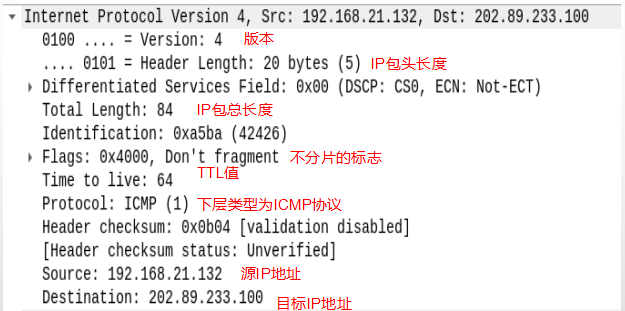
IMG_256

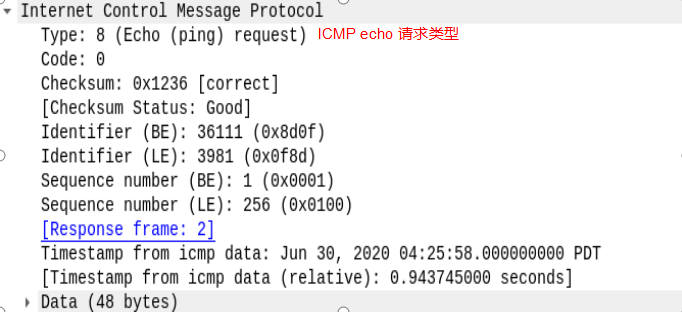
1. 用wireshake打开此文件



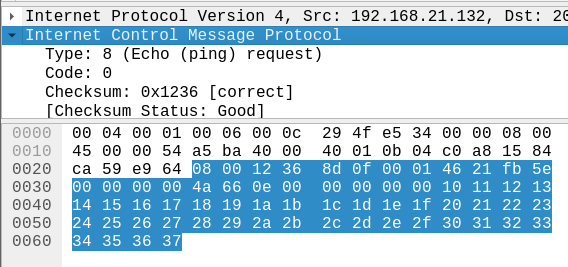
1. 开始标注







1. Checksum值验算



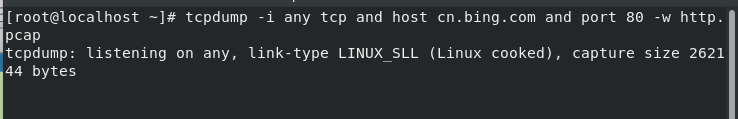
以四个字符为一组，将checksum：1236替换为0000，使用https://zaixianjisuanqi.51240.com/ 十六进制计算器将字符加起来得4edc5.

将40dc5分成0004和0dc5然后相加得0dc9，然后转化为2进制得0110111001001，

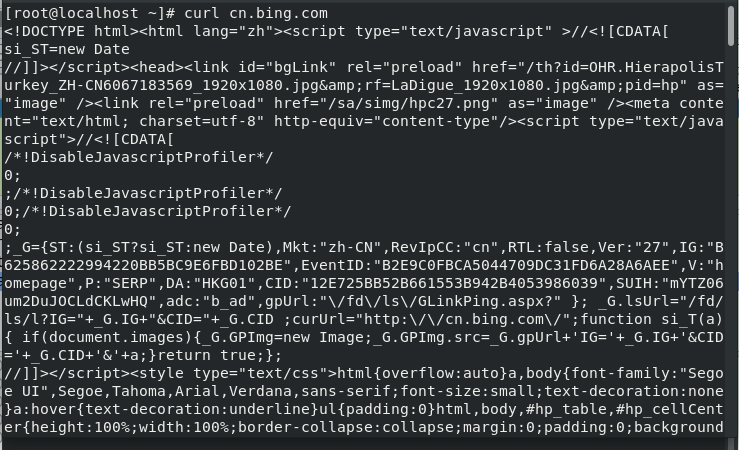
再把checksum值转化为2进制得1001000110110，两者0和1位置完全相反，所以checksum正确。

实验B

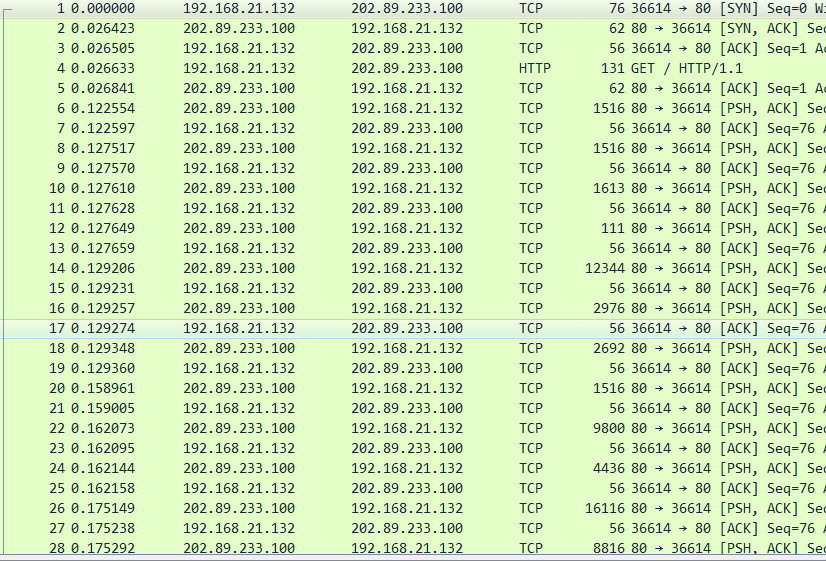
1. 在虚拟机终端执行抓包



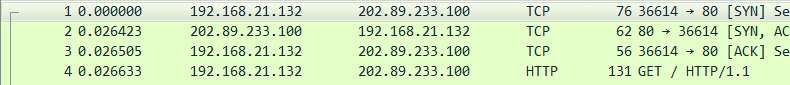
1. 新建客户端执行curl

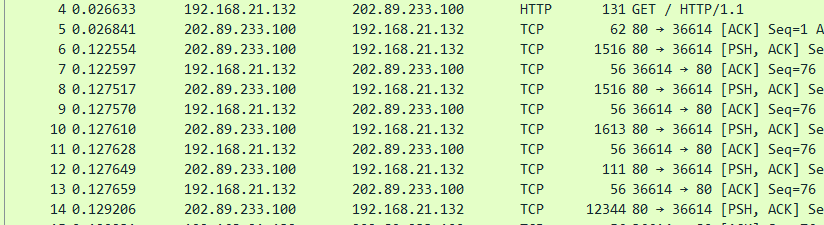


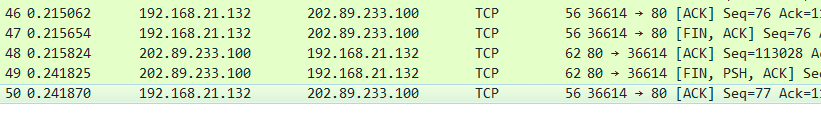
1. 在wireshark中打开http.pcap文件

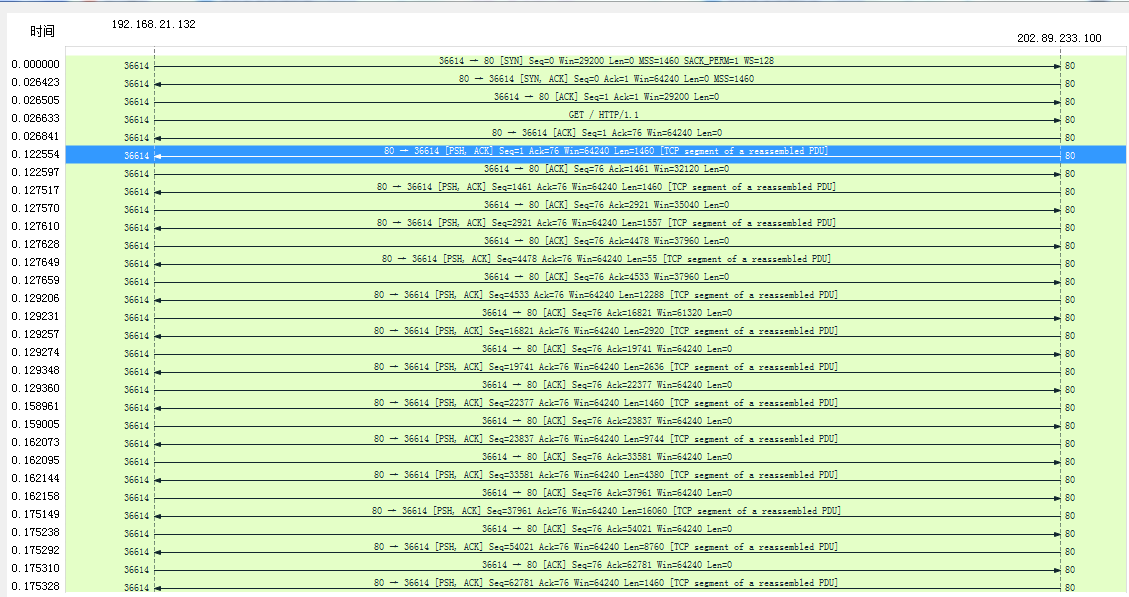


1. 分析

TCP第三次握手，SYN表示同步

HTTP请求和相应，ACK代表确认

TCP三次挥手，FIN表示结束。

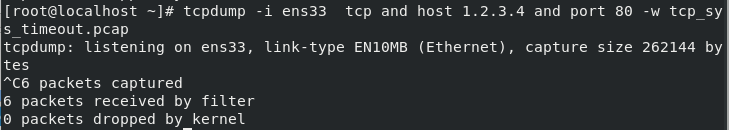
Sequence number是从0开始，然后开始变化

Acknowledgement number是从1开始，然后开始变化

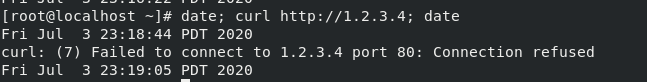
实验C

第一次握手SYN丢包

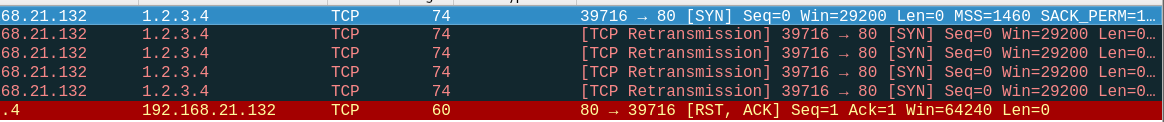
1.运行抓包程序，1.2.3.4为外网ip



2.运行curl



1. wireshark打开包文件



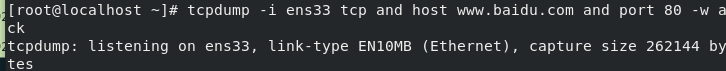
可以看到第一次SYN丢失之后，又进行了4次重发，然后终止了连接。

第二次握手，SYN,ACK丢包

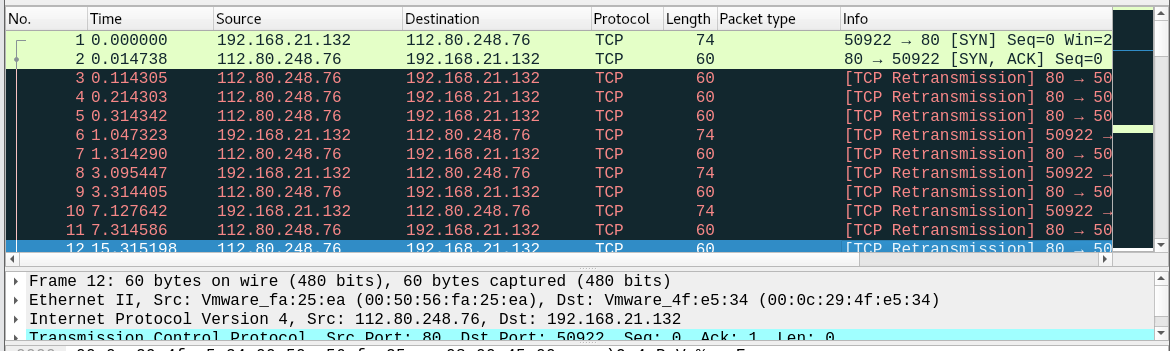
1.建立防火墙

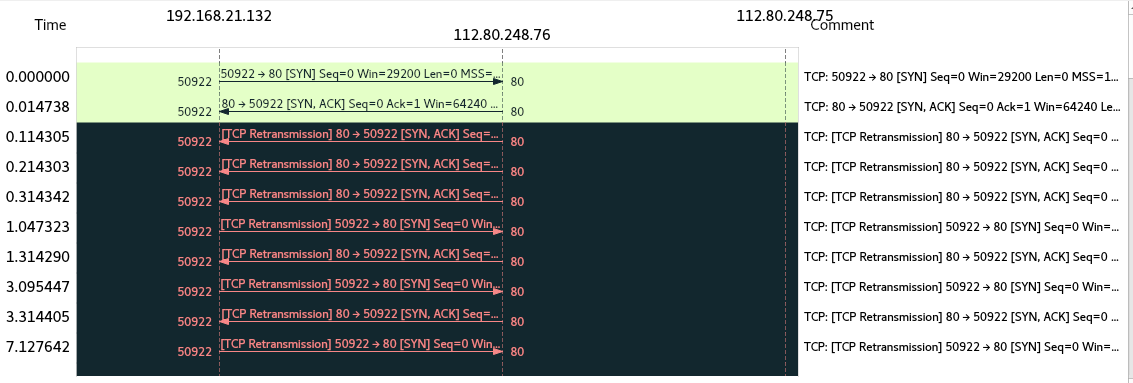
IMG_256

1. 运行抓包程序



1. 运行curl程序
2. wireshark打开所抓的包





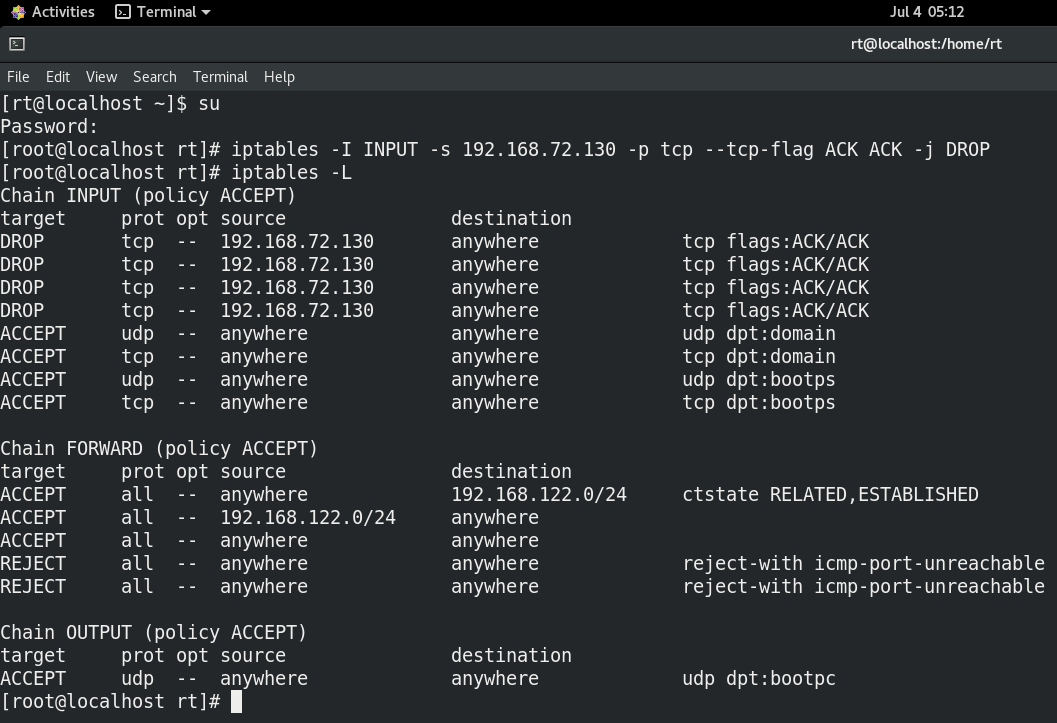
从数据包中可以看出，服务端受到客户端的SYN包后返回了SYN,ACK包，但由于防火墙的拦截导致丢包，所以服务端开始重传SYN,ACK包，而由于客户端一直收不到SYN,ACK包，所以在一定时间后也开始重传SYN包

第三次握手ACK丢包

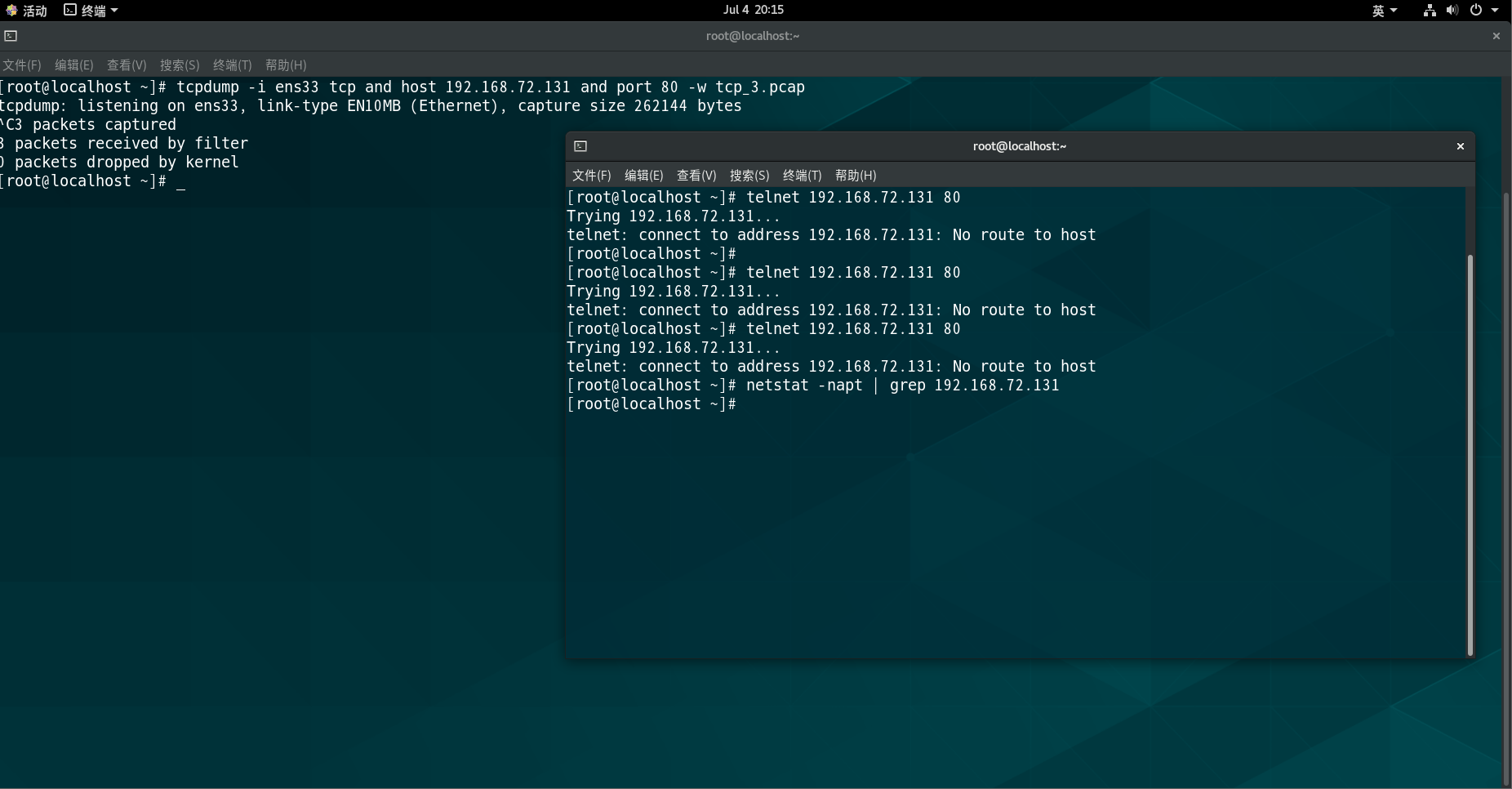
1. 第三次握手实验需在服务端设置防火墙，所以借用朋友的电脑进行实验。

客户端ip：192.168.72.130 服务端ip：192.168.72.131

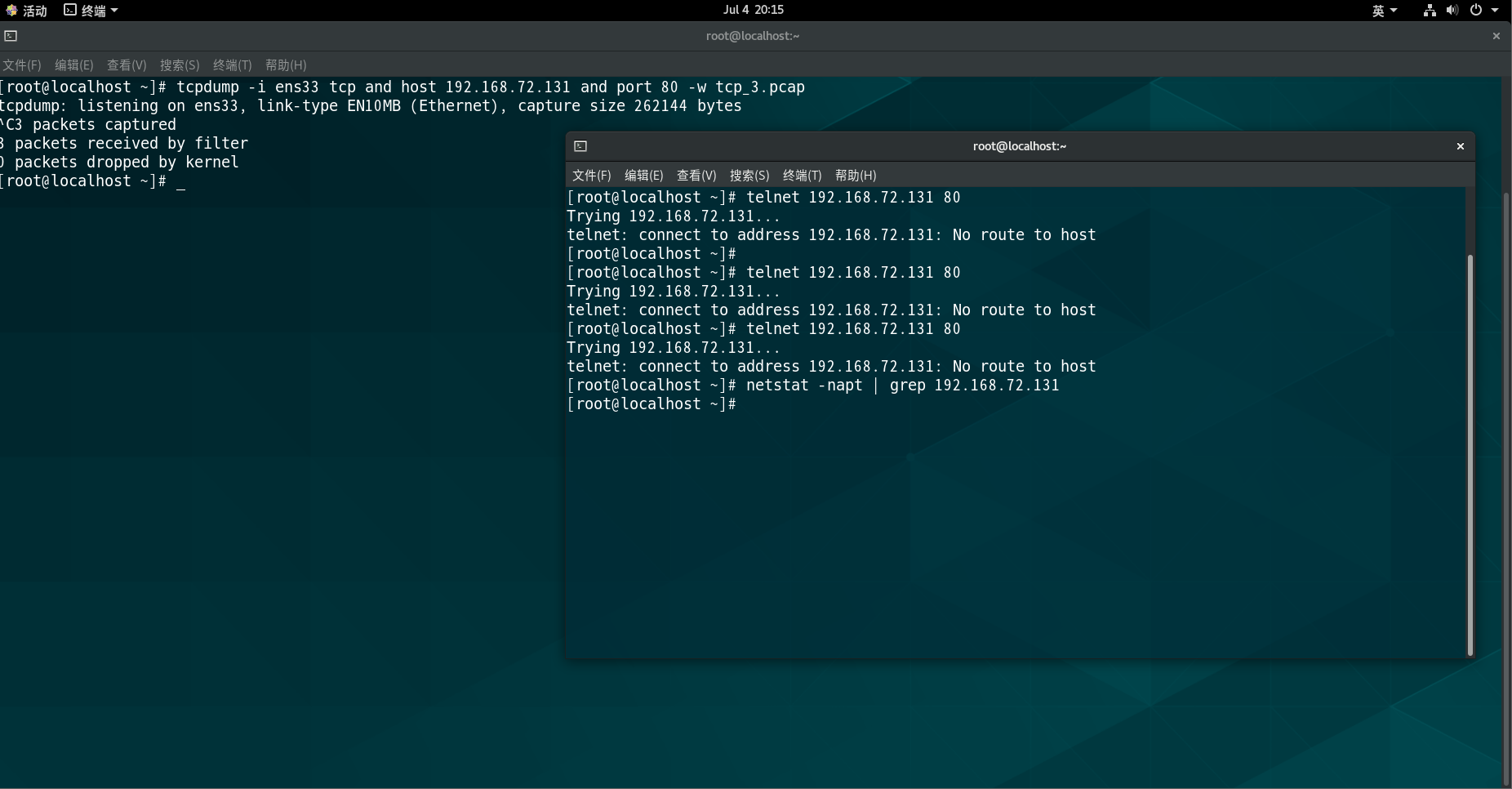
现在服务端输入如下命令设置防火墙



2.客户端输入tcp命令抓包



3.在客户端向服务端发起telnet命令



问题显示No route to host 根据博客[1]

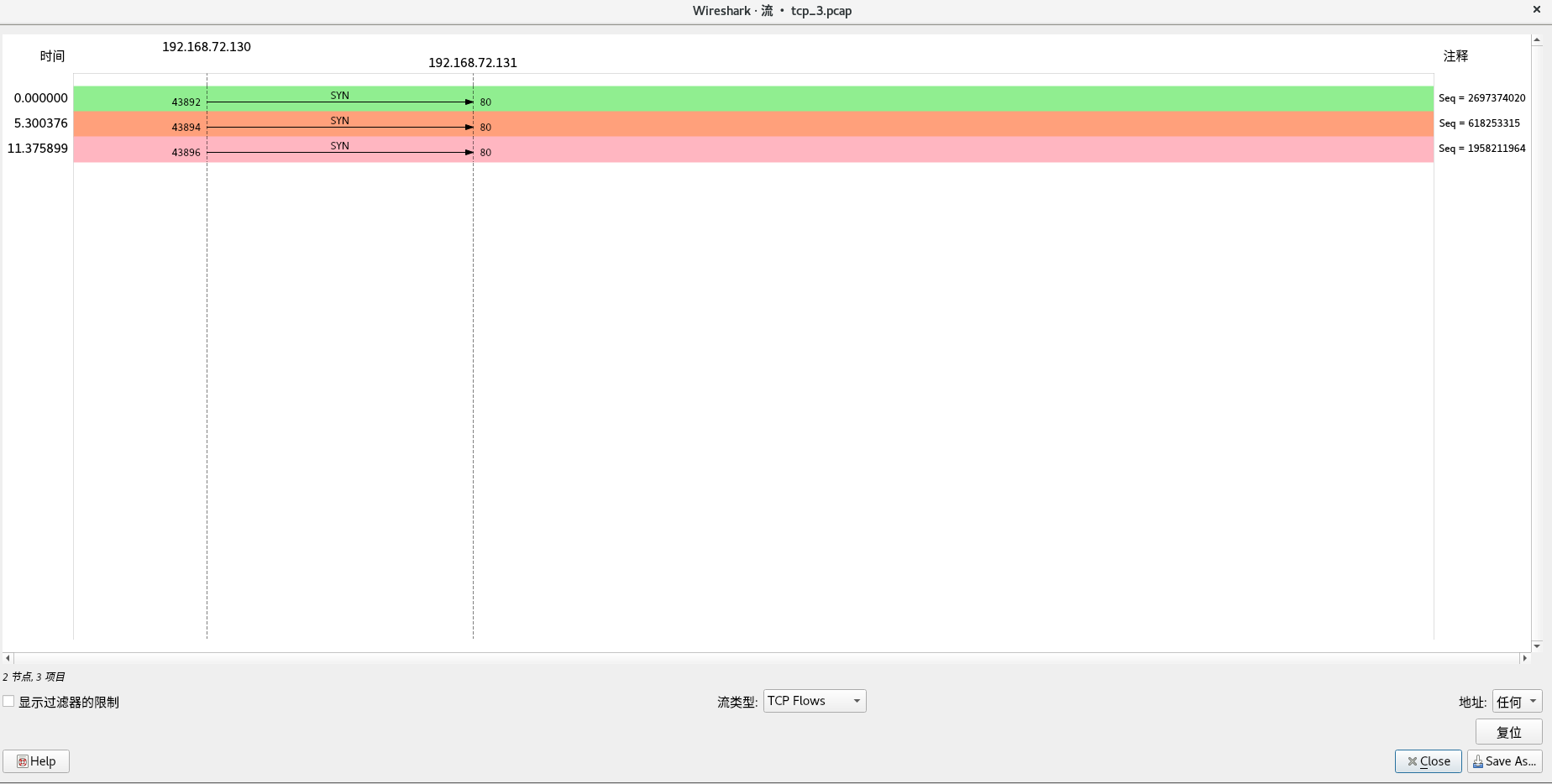
<https://blog.csdn.net/lmb1612977696/article/details/80623814>

所说需清除防火墙设置，这与实验目的相冲突，无法解决。

客户端与服务端均在同一局域网下，但是却达不到目的效果，与

<https://mp.weixin.qq.com/s/UQNVjQ80AVy5GKPZbkI6qw> 中描述不相符，无法找到原因。

Tcp抓包也只能抓到三个SYN包，无法判断哪里出现了问题。

**参考文献**

1. <https://mp.weixin.qq.com/s/UQNVjQ80AVy5GKPZbkI6qw>
2. <https://juejin.im/post/5edb48f4f265da76b4049430>
3. <https://blog.csdn.net/lmb1612977696/article/details/80623814>