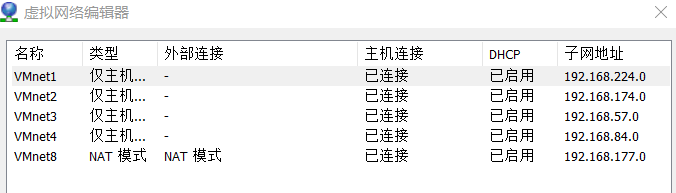
计算机网络实验一

**一．实验目的**

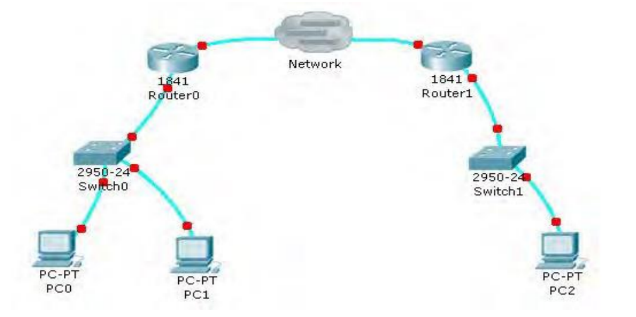
1. 熟悉基本网络工具集的使用
2. 初步了解PDU观测工具Wireshark
3. 加深对子网、子网掩码、网关、路由器、交换机等网络概念的理解
4. 学习路由规则，体会“下一跳”的概念，理解数据包传送过程的转发机制
5. 进一步学习虚拟机、linux平台以及使用命令行

**二．拓扑结构搭建**

VMware Workstation提供了七个虚拟交换机，选取其中的三个vmvet2、vmvet3、vmvet4作为本次实验的虚拟交换机，在设置中给虚拟交换机自动分配了ip如下



然后根据拓扑结构图如下



设net1和net1\_clone为路由器，net2、net2\_clone1、net2\_clone2为终端，设置网络适配器如下图

**三．网络拓扑配置**

|  |  |  |  |
| --- | --- | --- | --- |
| 节点名 | 虚拟设备名 | ip | netmask |
| Router0 | net1 | ens33:192.168.174.1 | 255.255.255.0 |
| ens38:192.168.57.1 | 255.255.255.0 |
| Router1 | net1\_clone | ens33:192.168.174.2 | 255.255.255.0 |
| ens38:192.168.84.1 | 255.255.255.0 |
| PC1 | net2 | ens33:192.168.57.2 | 255.255.255.0 |
| PC2 | net2\_clone1 | ens33:192.168.57.3 | 255.255.255.0 |
| PC3 | net2\_clone2 | ens33:192.168.84.2 | 255.255.255.0 |

三．路由规则配置

（1）通过ifconfig -a|less 查看虚拟机的网络设备

（2）然后设置ip：

net1:

sudo ifconfig ens33 192.168.174.1 netmask 255.255.255.0

sudo ifconfig ens38 192.168.57.1 netmask 255.255.255.0

net1\_clone:

sudo ifconfig ens33 192.168.174.2 netmask 255.255.255.0

sudo ifconfig ens38 192.168.84.1 netmask 255.255.255.0

net2:

sudo ifconfig ens33 192.168.57.2 netmask 255.255.255.0

net2\_clone1:

sudo ifconfig ens33 192.168.57.3 netmask 255.255.255.0

net2\_clone2:

sudo ifconfig ens33 192.168.84.2 netmask 255.255.255.0

（3）其次需要设置终端的网关

net2:

sudo route add default gw 192.168.57.1

net2\_clone1:

sudo route add default gw 192.168.57.1

net2\_clone2:

sudo route add default gw 192.168.84.1

（4)最后设置路由器的路由规则并允许转发

net1:

sudo ip route add 192.168.84.0/24 via 192.168.174.2

sudo su

echo 1 > /proc/sys/net/ipv4/ip\_forward

exit

net1\_clone:

sudo ip route add 192.168.57.0/24 via 192.168.174.1

sudo su

echo 1 > /proc/sys/net/ipv4/ip\_forward

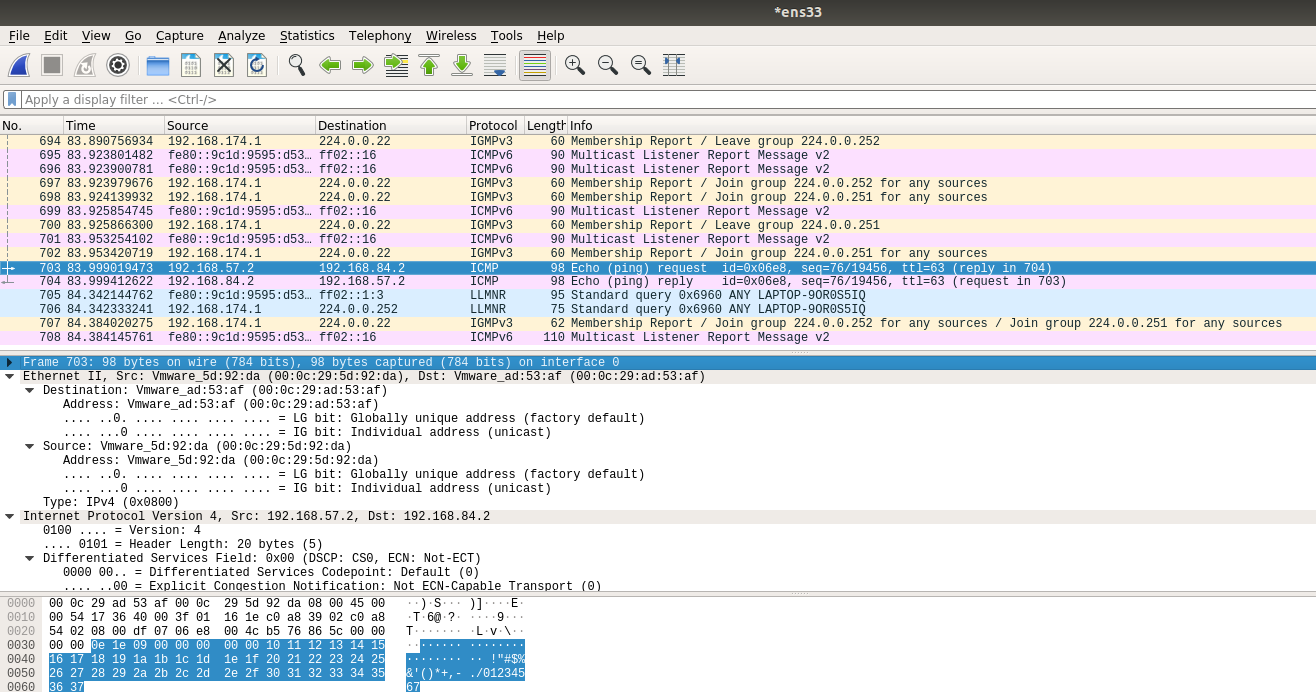
exit

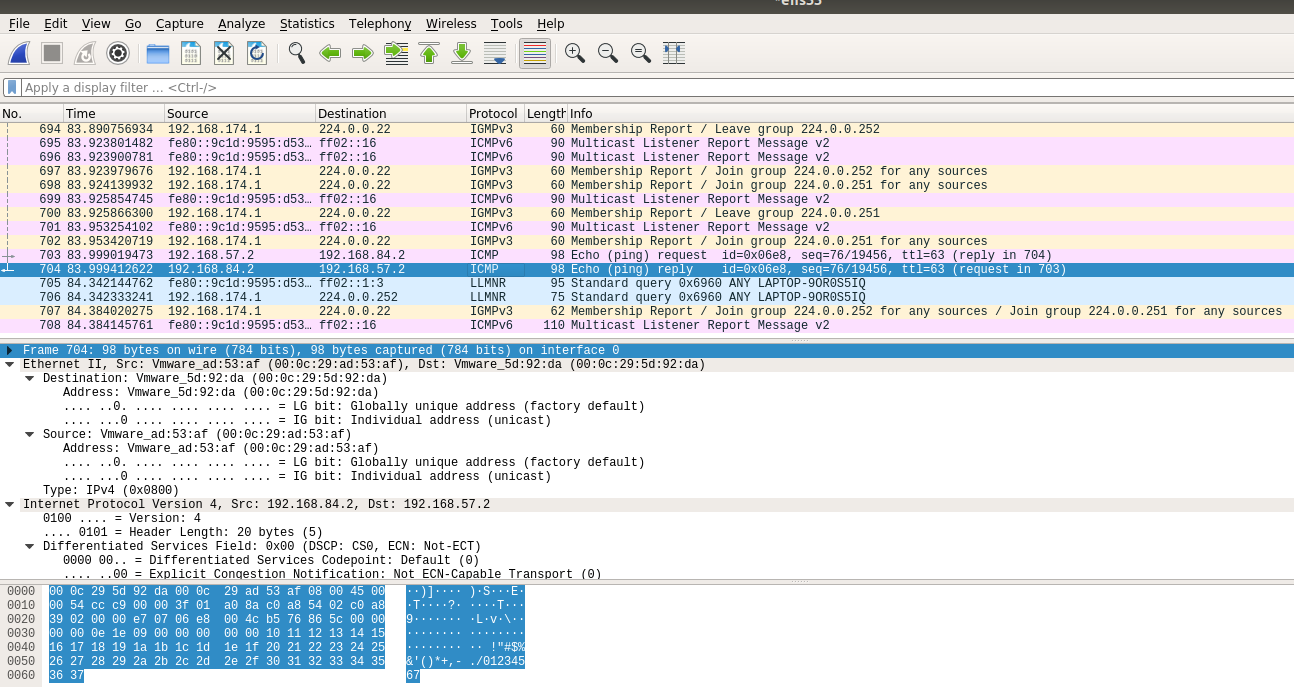
然后在终端如net2：ping 192.168.84.2

然后在路由器net1： sudo wireshark即可抓包

**四．数据包截图**

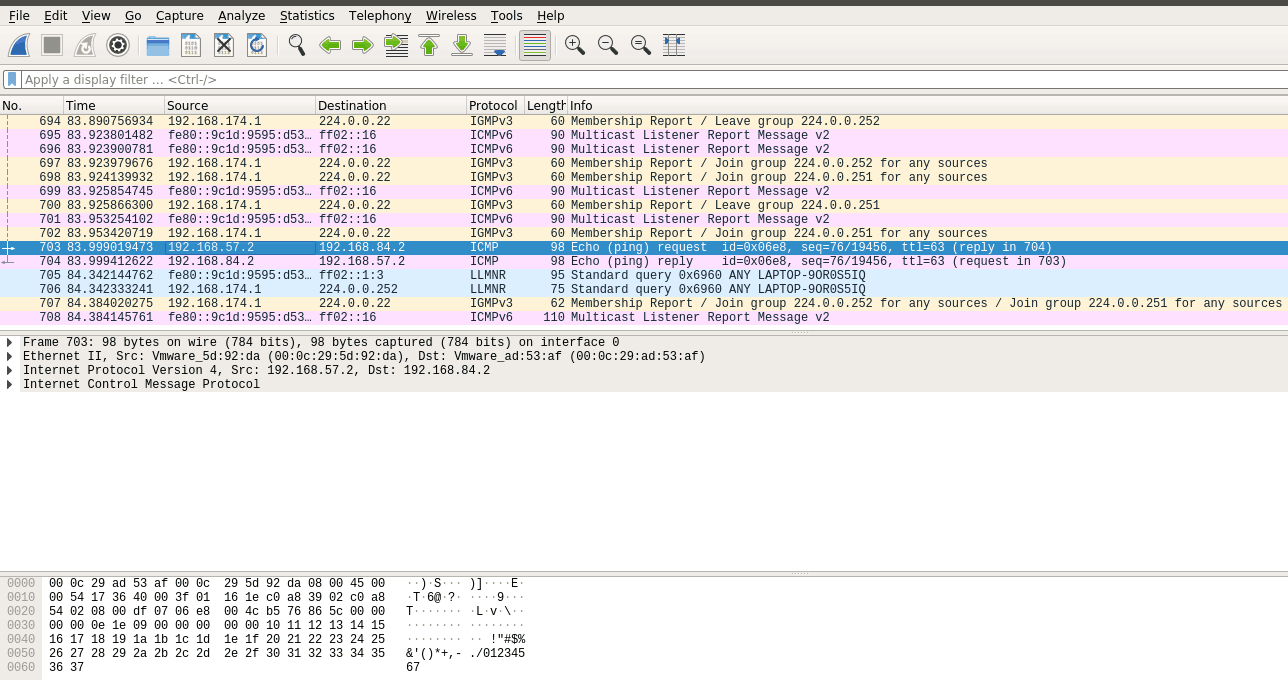
两条记录分别是从net2 发送到net2\_clone2的数据包、从net2\_clone2返回应答的数据包





**五．协议报文分析**

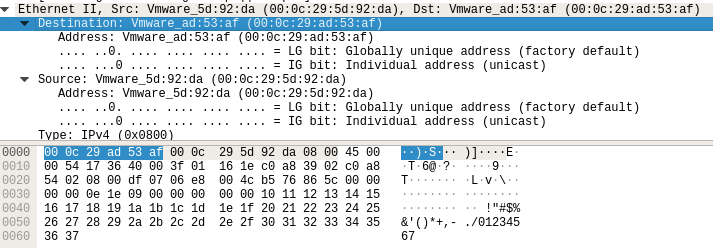
接下来以net2 to net2\_clone2为例，对抓取的数据包进行字段分析：



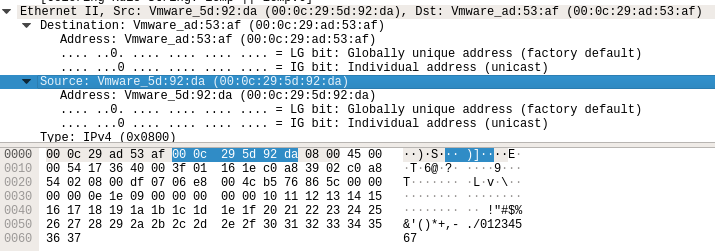
Frame:所抓的包为一个帧，帧号为703，帧大小为98bytes

Ethernet:以太网，有线局域网技术，属于链路层

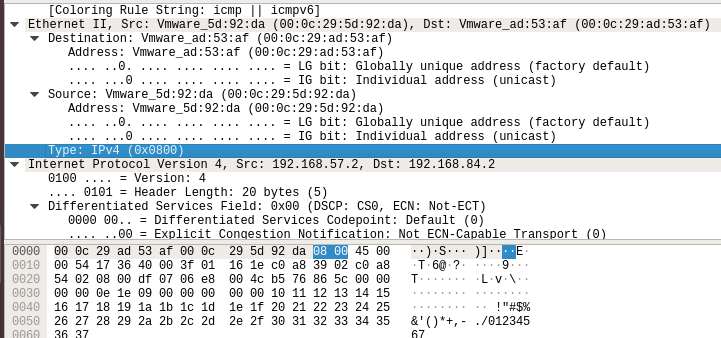
Internet protocol：IP协议，网络层，ipv4，源ip为192.168.57.2，目的ip为192.168.84.2



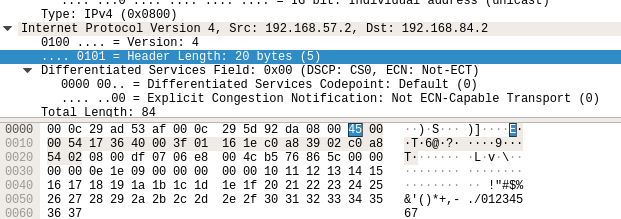
目的地的MAC地址：00：0c:29:ad:53:af



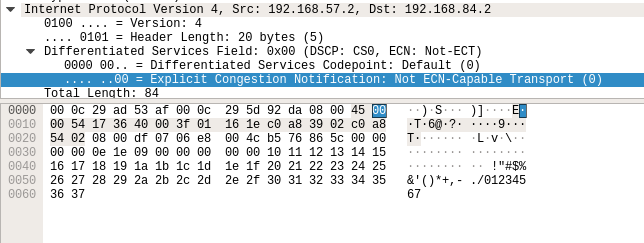
源MAC地址:00：0c:29:5d:92:da



协议类型为ipv4（0x0800）

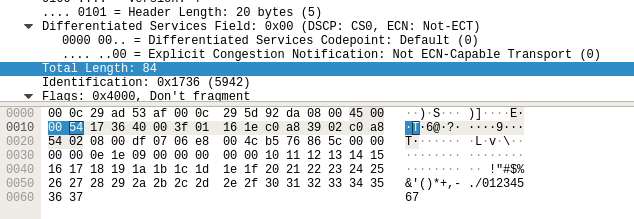


Ip协议版本4，20 bytes(5)

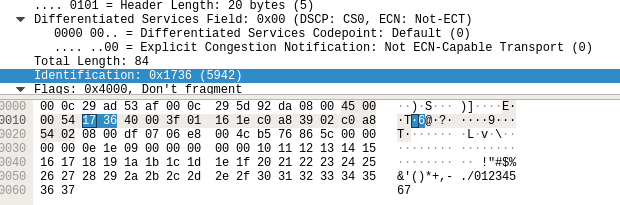


00表示explicit congestion notification:not ecn-capable transport

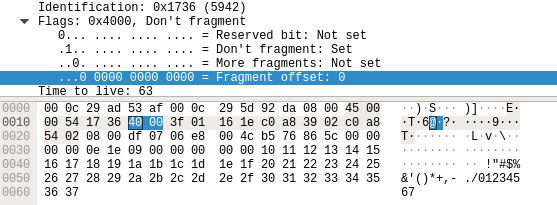
即明确的阻塞指示



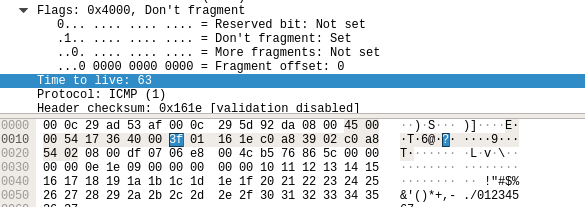
总长度为0x54



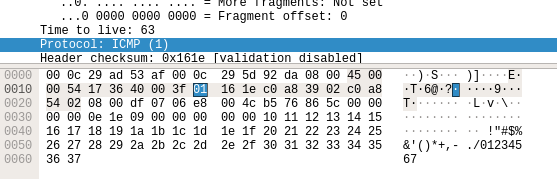
鉴别号0x1736



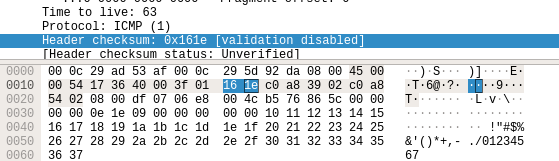
标志flag为0x4000



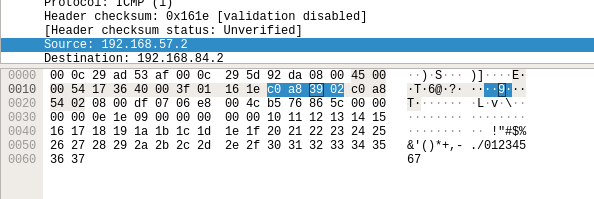
生存期为0x3f



协议名称



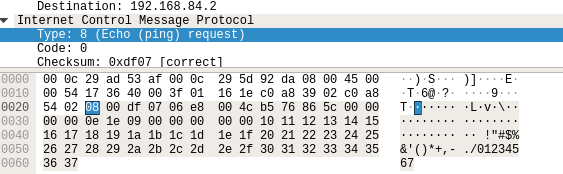
头部校验和校验状态



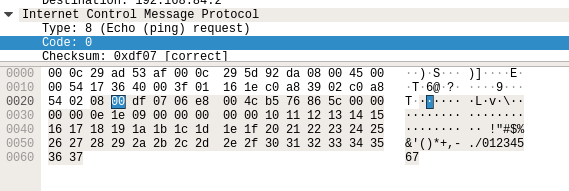
源ip

![C:\Users\吴紫航\AppData\Roaming\Tencent\Users\401986905\QQ\WinTemp\RichOle\L[U](W9K${SA7W]$GM7G7I0.png](data:image/png;base64,)

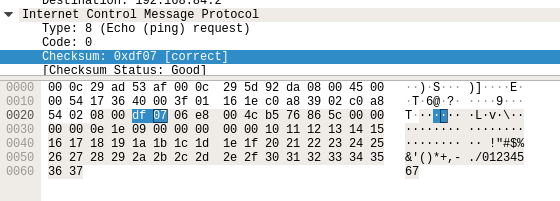
目的ip



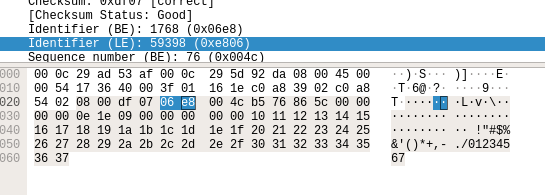
类型：8



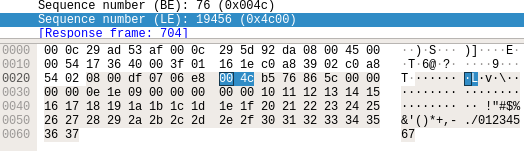
编码：0



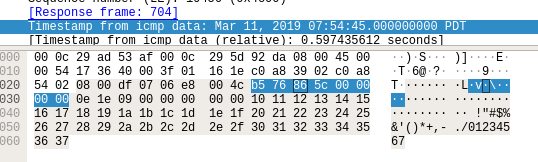
校验和为0xdf07



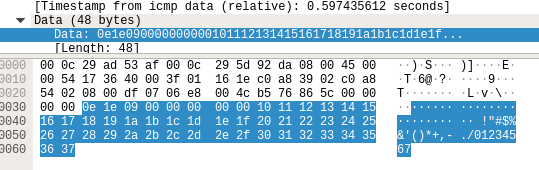
校验者：0xe806



Sequence number：0x4c00



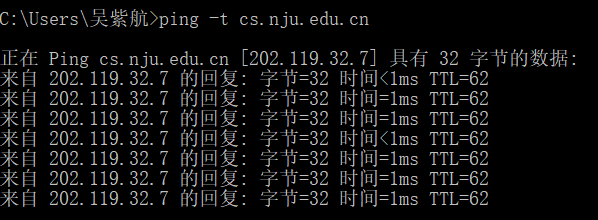
Icmp数据时间标记3月11日，2019年 7点54分45秒

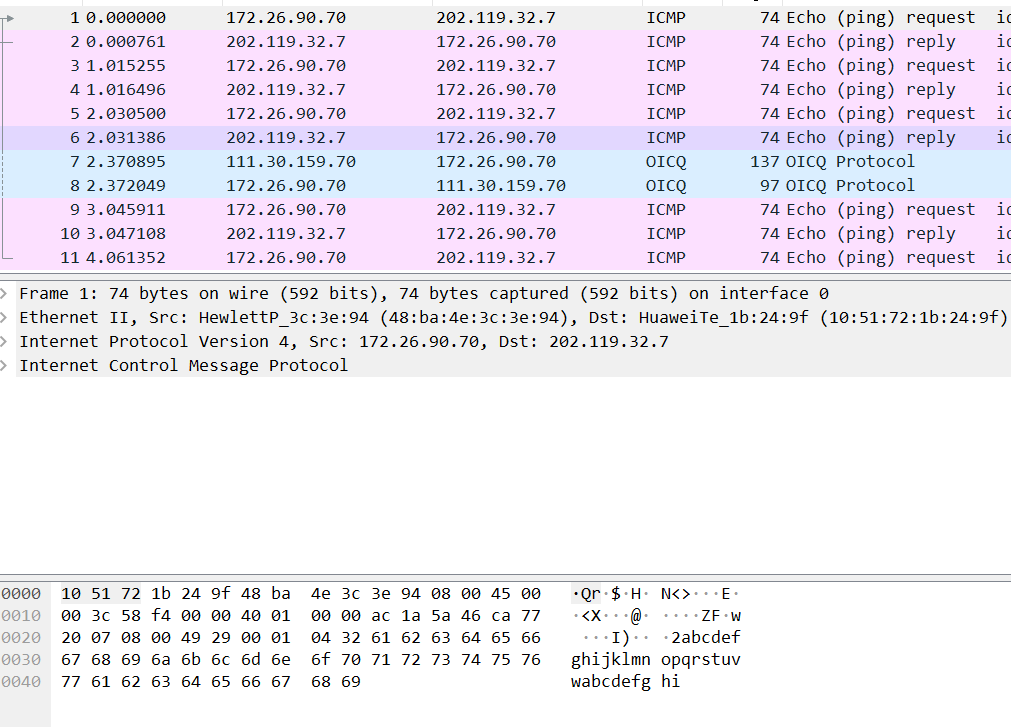


数据包具体的内容

**六．Ping系主页**

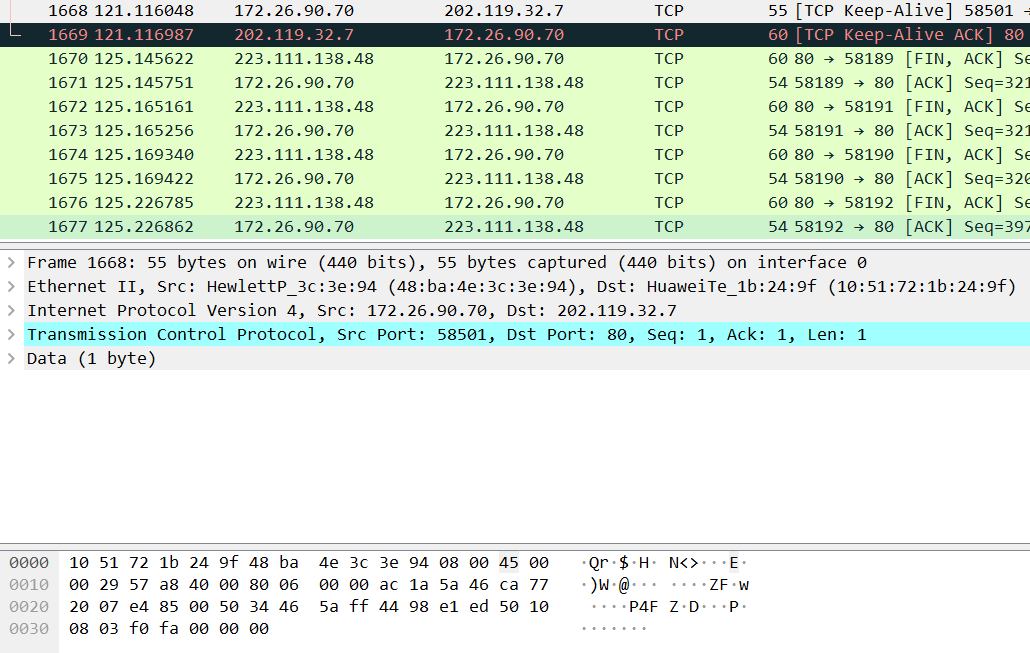
（1）ping cs.nju.edu.cn的抓包截图





简要说明：帧号1,74字节，以太网2，源MAC为48：ba:4e:3c:3e:94,目的MAC为：10：51：72：1b:24:9f,互联网协议版本4，ipv4，源ip：172.26.90.70目的ip：202.119.32.7

（2）登陆[www.nju.edu.cn](http://www.nju.edu.cn)时候的抓包截图



简要说明：帧号1688，55字节，以太网2，源MAC为48：ba:4e:3c:3e:94,目的MAC为：10：51：72：1b:24:9f,互联网协议版本4，ipv4，源ip：172.26.90.70目的ip：202.119.32.7