院 系 计算机学院 学号　19335262 姓名 张航悦

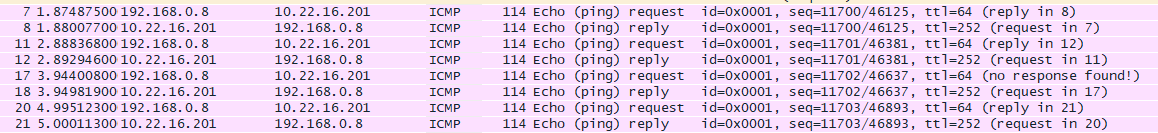
班 级 19

【实验题目】WireShark**实验**

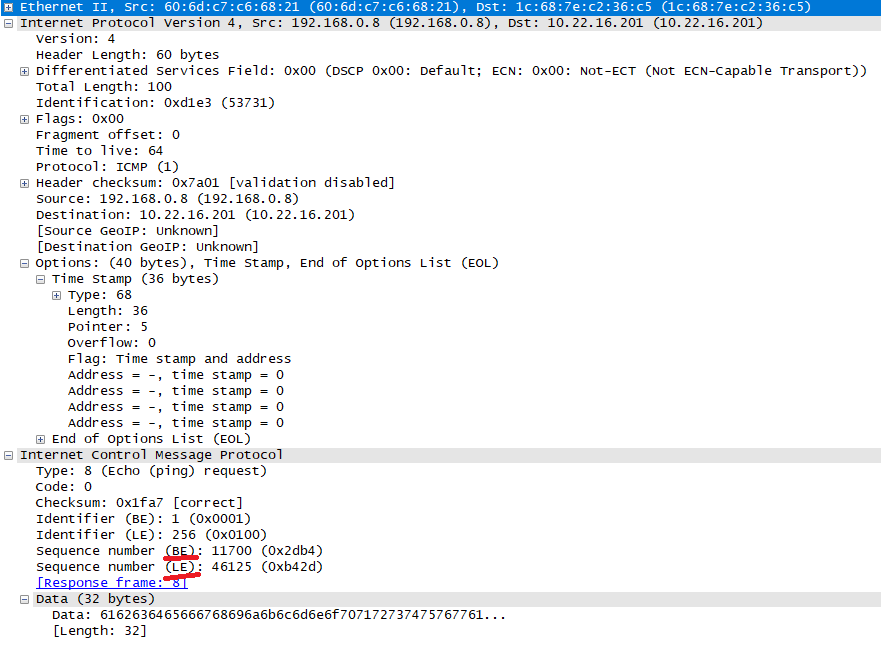
【实验目的】通过WireShark分析IP协议(Option)、ICMP协议、ARP协议、DHCP协议、DNS协议、TCP协议。

【注意事项】

多个包要截一个**总图**（排序或用ICMP作为过滤条件），例如：



所有截包要求展开IP协议和内部协议，如果有多个，只用选择其中一个，例如：



BE = 大端序

LE = 小端序

上面分别用BE和LE表示同一个数，这里是BE有效（本来Intel采用LE，不知道这里为什么是BE有效）。

注意每一步都要保存截包文件

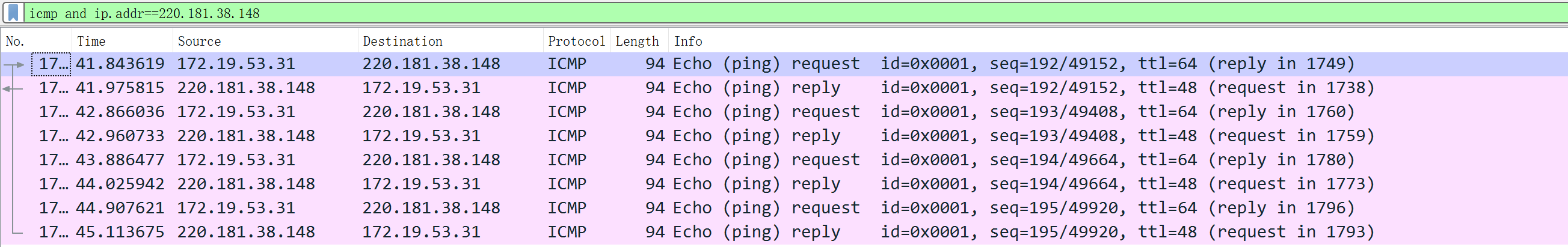
过滤条件：ip.addr == 172.18.187.251 && tcp.port==59161 （具体的可以见WireShark.pdf）

【实验任务】

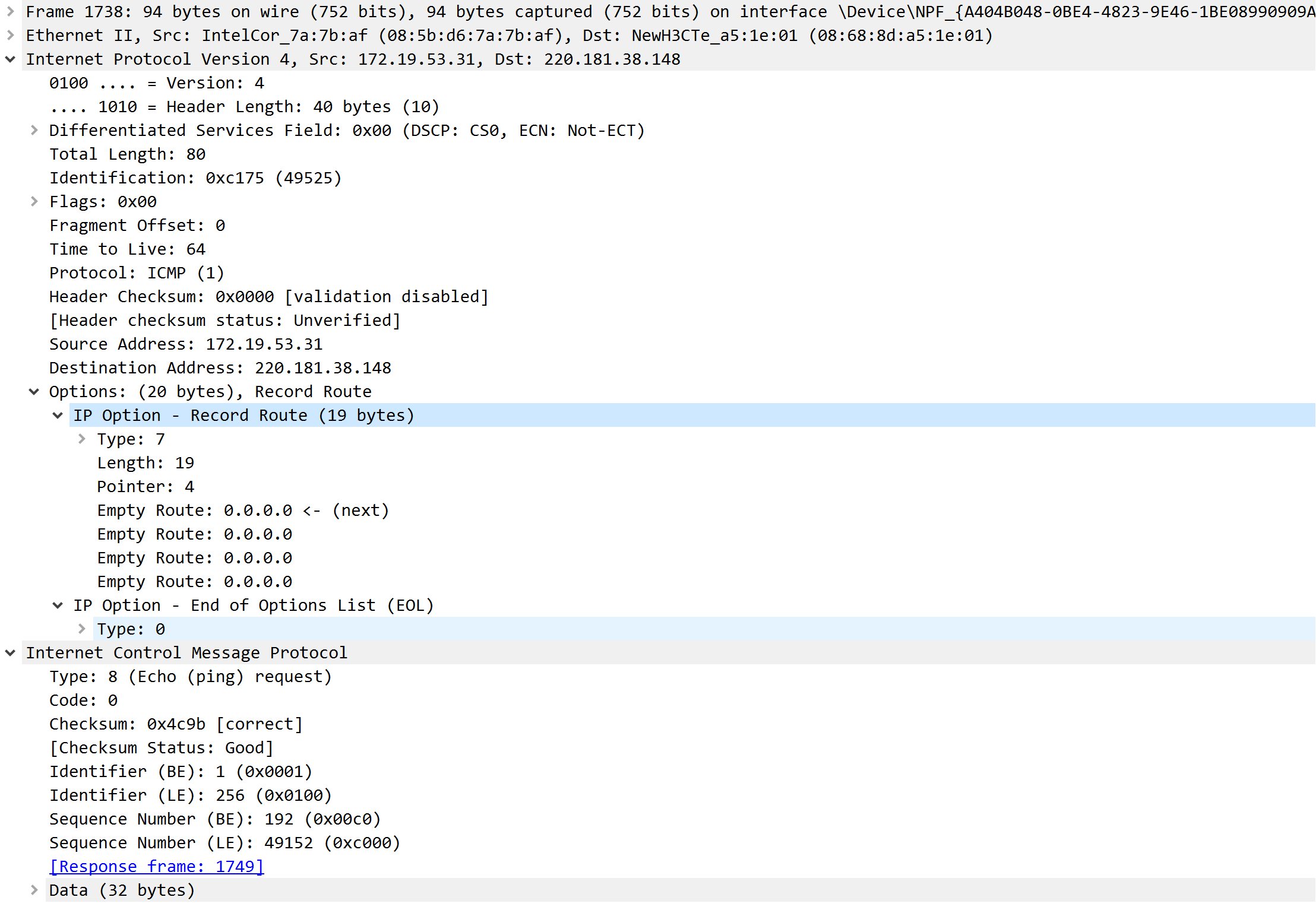
1. (IP.pcapng)IP Option和ICMP协议。

**命令：ping -r 4域名**

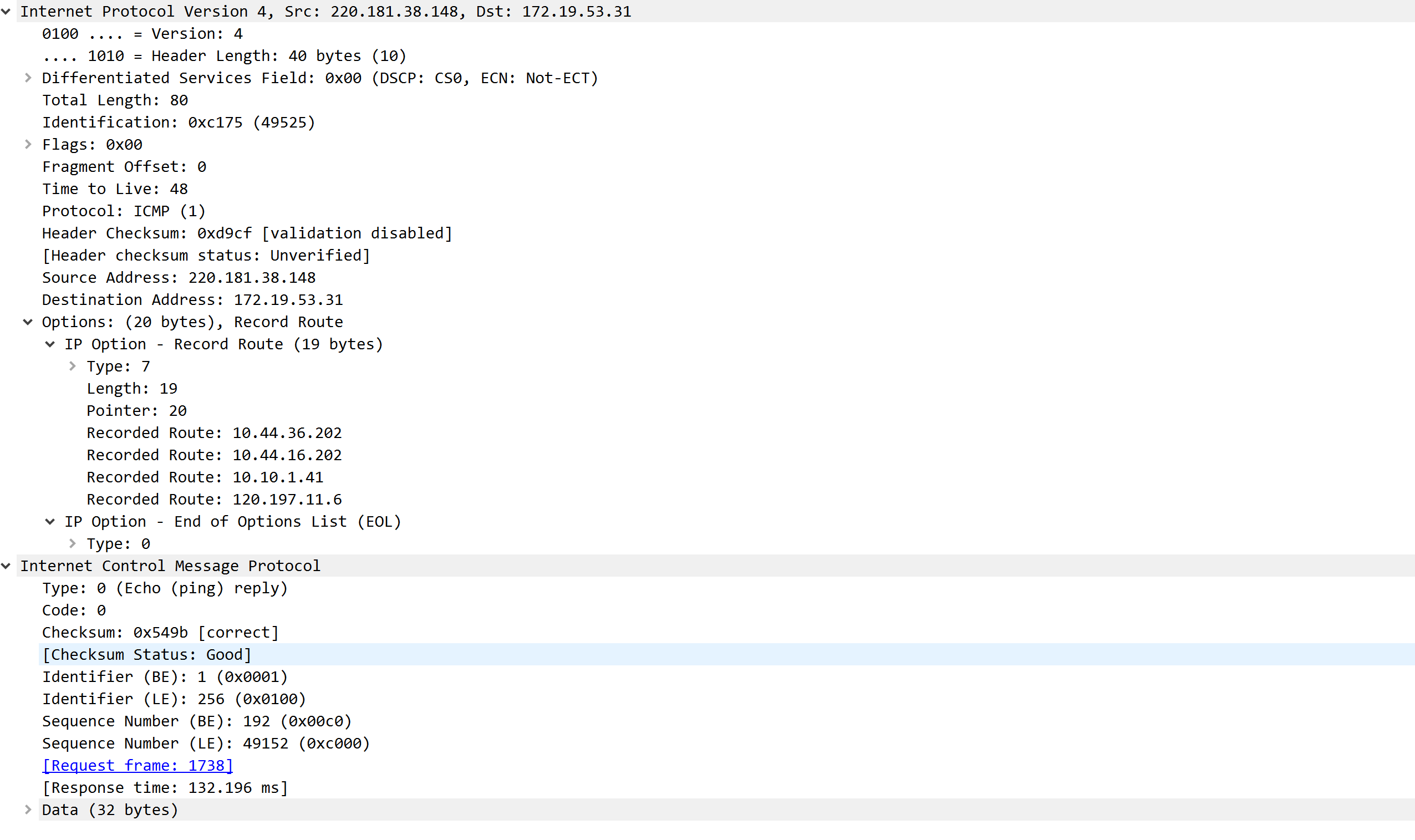
[Ping总图]



[Ping请求包截屏]



[Ping响应包截屏]



[针对于所截包的问题]——以请求包为例

IP选项的长度：20B

ICMP包的Identifier：1

ICMP包的序号：192

ICMP包的数据部分长度：32B

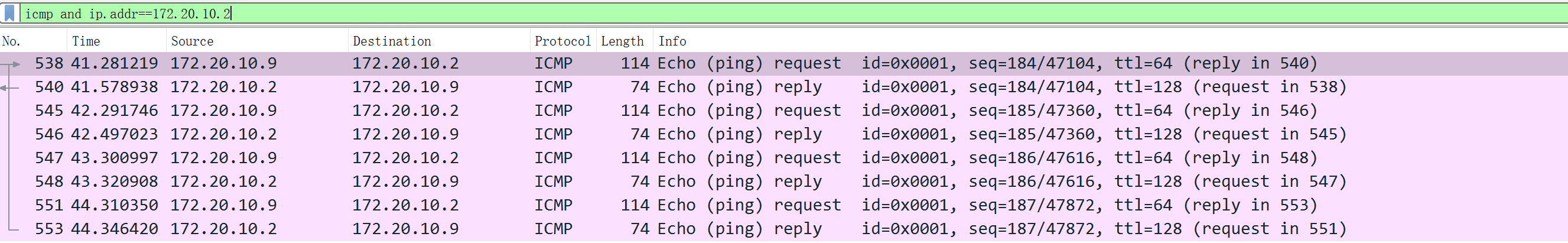
ICMP包的数据部分的内容：

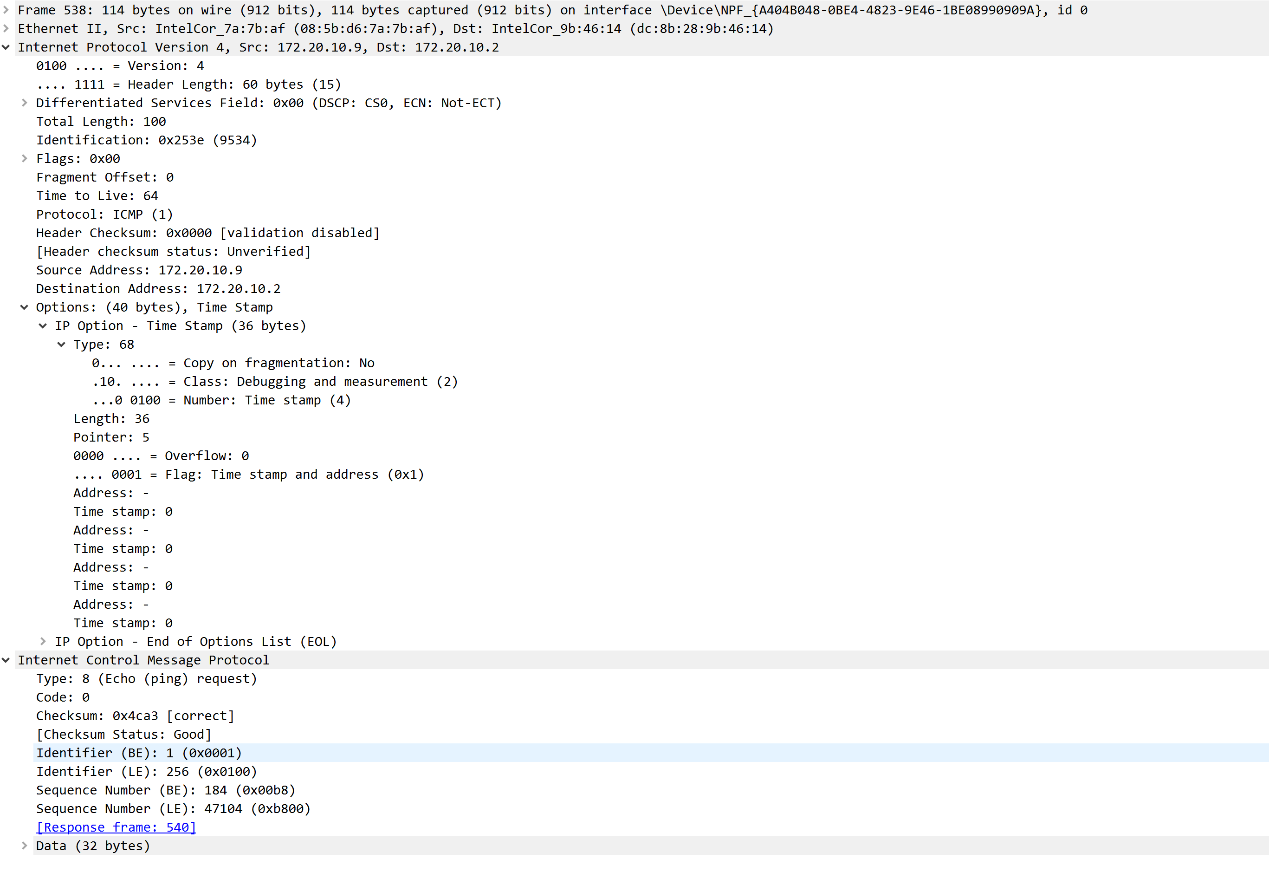


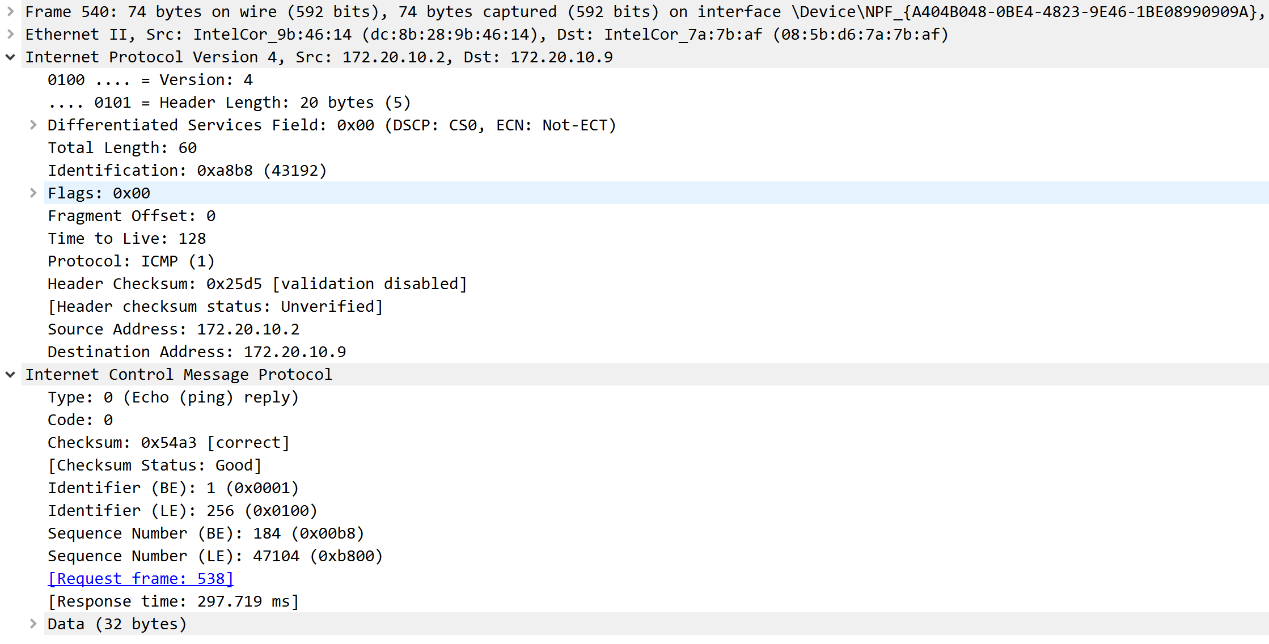
Identifier是什么含义？标识符，标识本进程。当同时与多个目的通信时，通过本字段来区分。

**命令：ping -s 4域名**

[Ping总图]



[Ping请求包截屏]

[Ping响应包截屏]

[问题]——以请求包为例

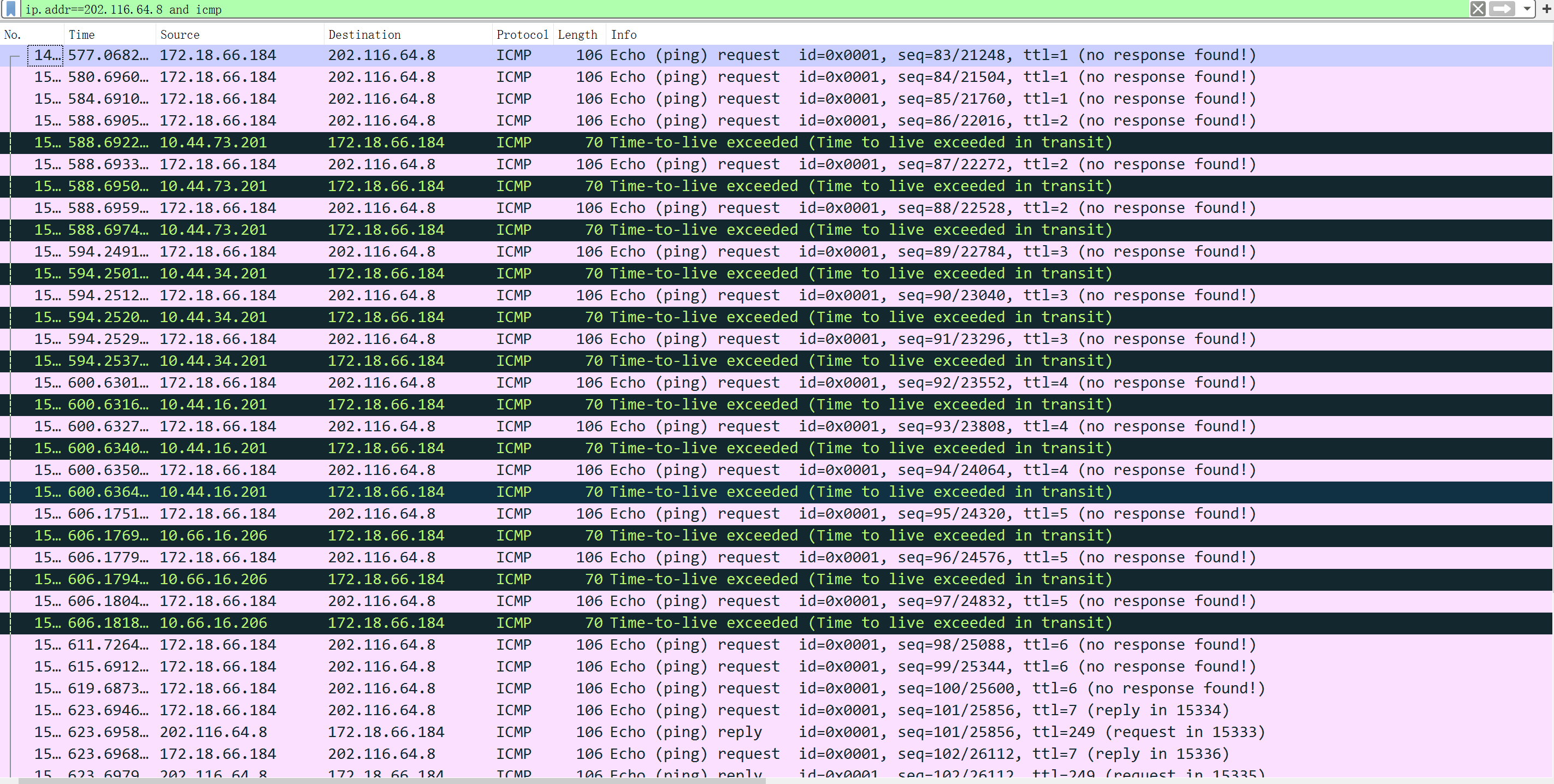
IP选项的长度：40B

选项中的时间戳是否正确？正确。由于ping -s记录计数跃点的时间戳，而我是在同一热点环境下ping的同学的主机，属于同一子网，所以并没有经过路由器，所以返回的ICMP响应类型0，代码为0，即为普通的ping应答。

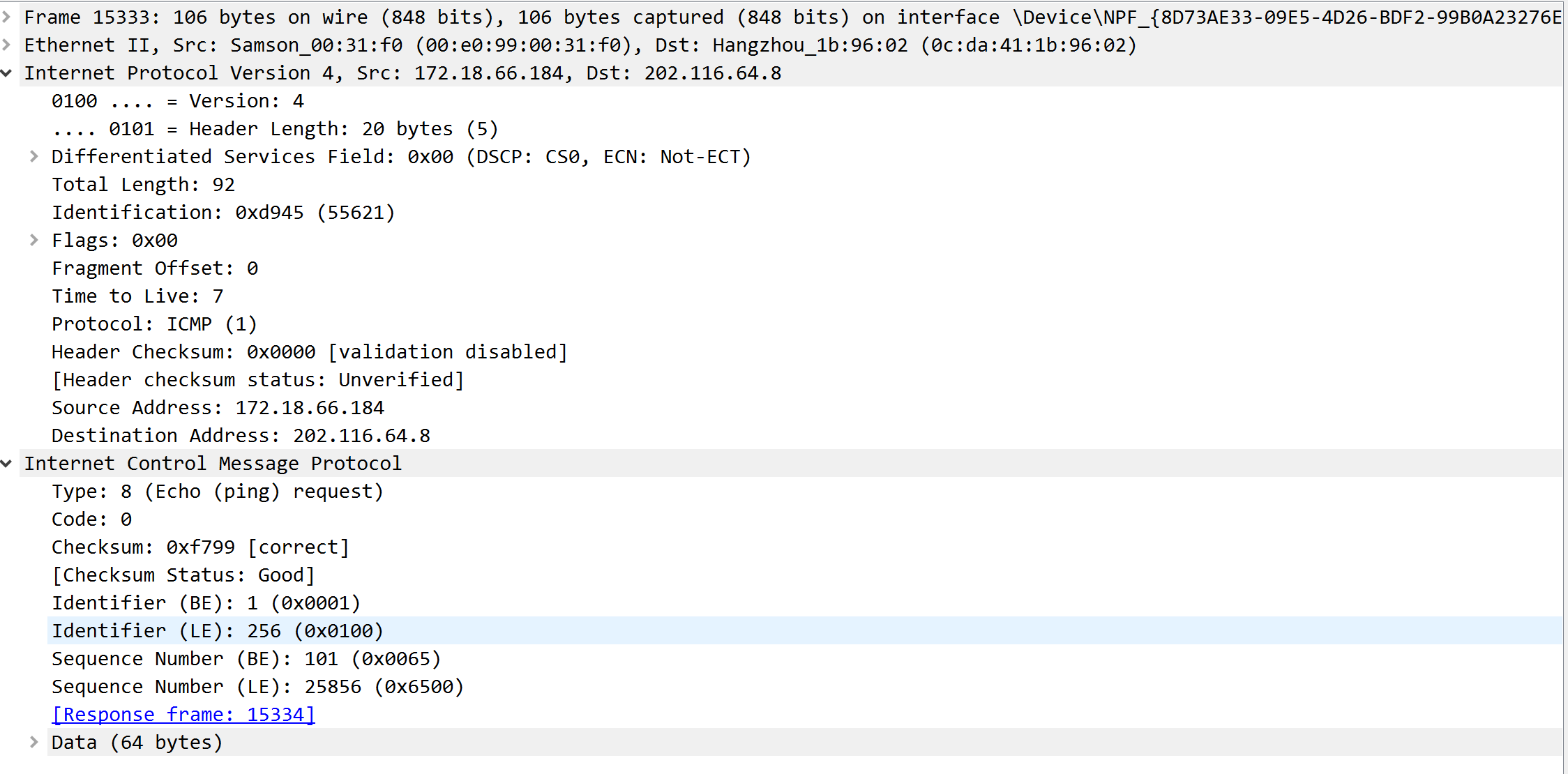
1. (tracert.pcapng) ICMP协议

命令：tracert -h 8 域名 （tracert -h 8 [www.sysu.edu.cn](http://www.sysu.edu.cn)）

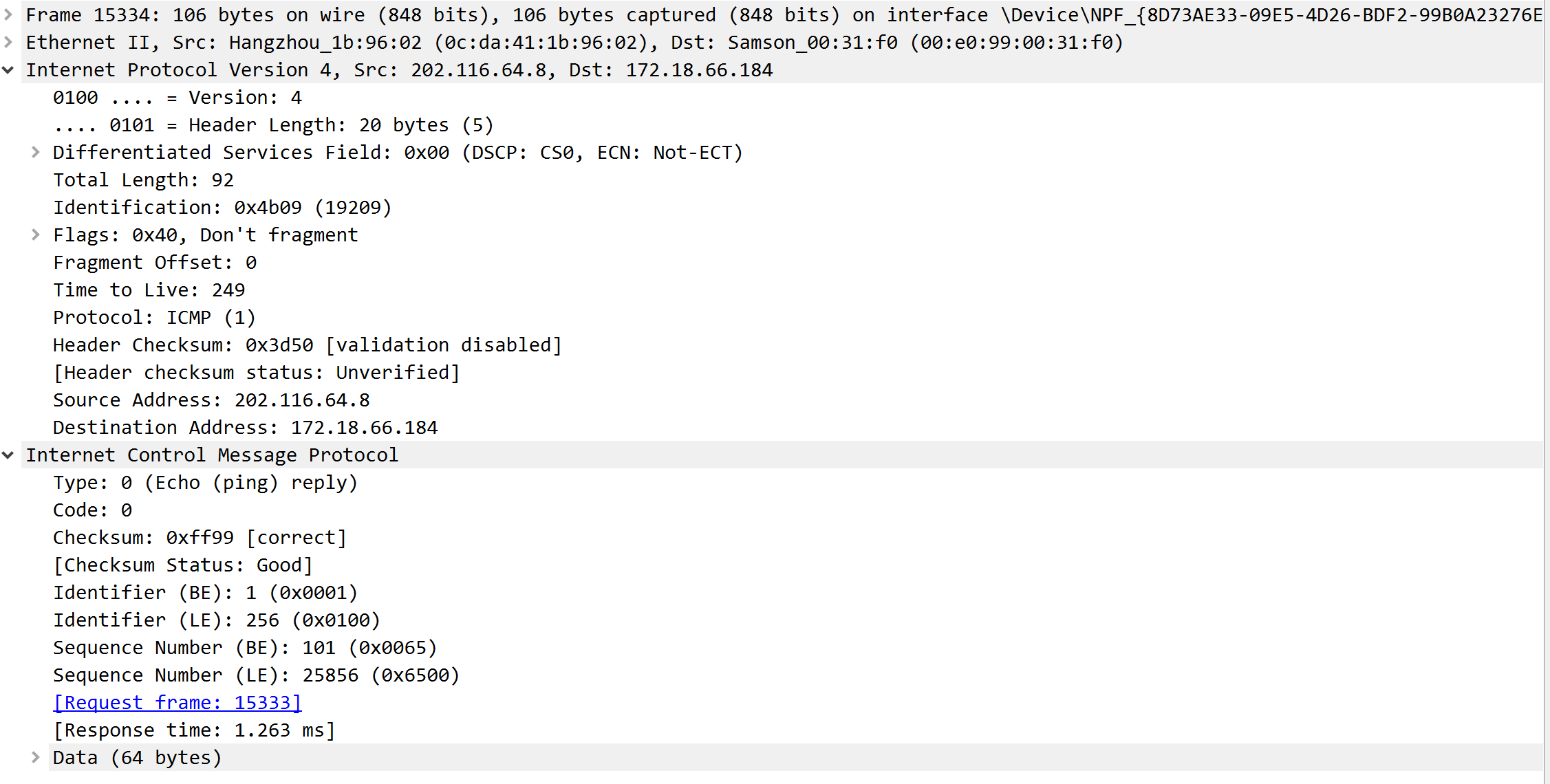
[tracert总图截屏]



[TTL=7的第一个Ping请求包截屏] \*可以选其他包，但是要修改一下*2和二*



[对应响应包截屏]



[说明tracert的基本原理]

tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。

首先，tracert送出一个TTL是1的IP 数据包到目的地，当路径上的第一个路由器收到这个数据包时，它将TTL减1。此时，TTL变为0，所以该路由器会将此数据包丢掉，并送回一个「ICMP time exceeded」消息（包括发IP包的源地址，IP包的所有内容及路由器的IP地址），tracert收到这个消息后，便知道这个路由器存在于这个路径上，接着tracert再送出另一个TTL是2 的数据包，发现第2 个路由器...... tracert每次将送出的数据包的TTL 加1来发现另一个路由器，这个重复的动作一直持续到某个数据包抵达目的地。

tracert 有一个固定的时间等待响应(ICMP TTL到期消息)。如果这个时间过了，它将打印出一系列的\*号表明：在这个路径上，这个设备不能在给定的时间内发出ICMP TTL到期消息的响应。然后，tracert给TTL记数器加1，继续进行。

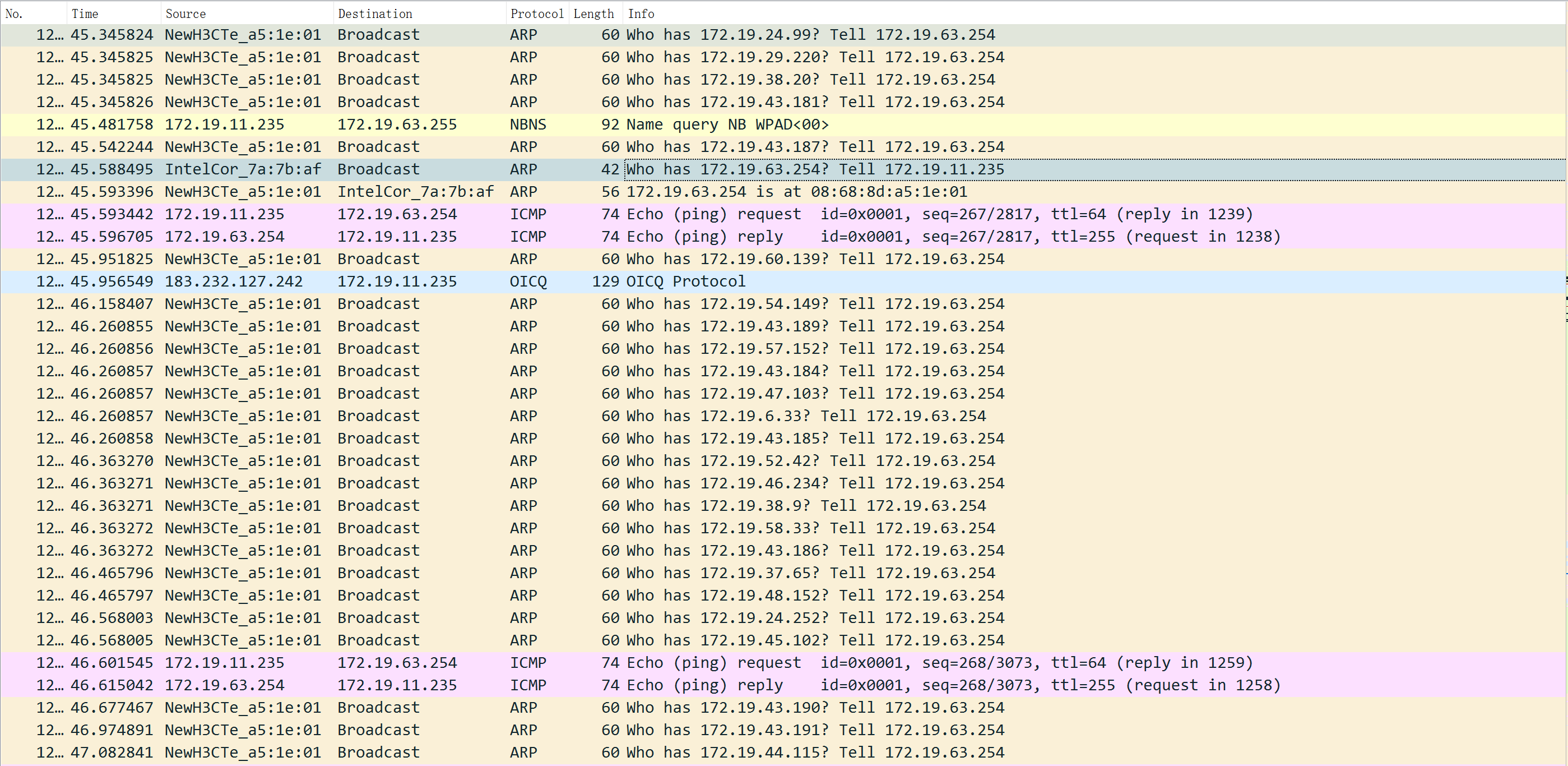
1. (arp.pcapng)ARP协议。

命令：arp –a （查看）

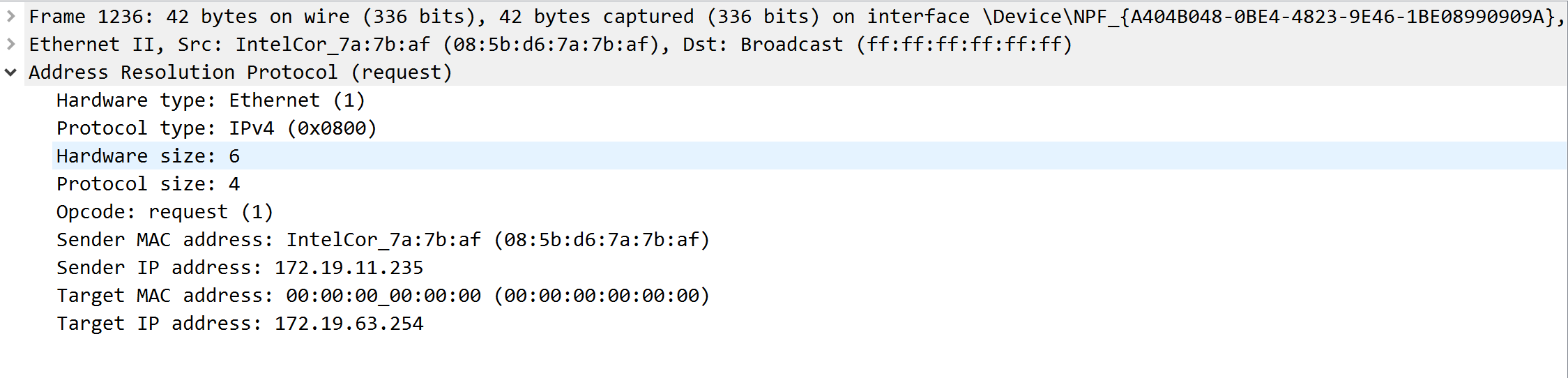
arp –d 192.168.0.14 （删除）

ping默认网关或同学的电脑：先查看ARP缓存，删掉这台电脑的映射，然后启动截包，再ping它

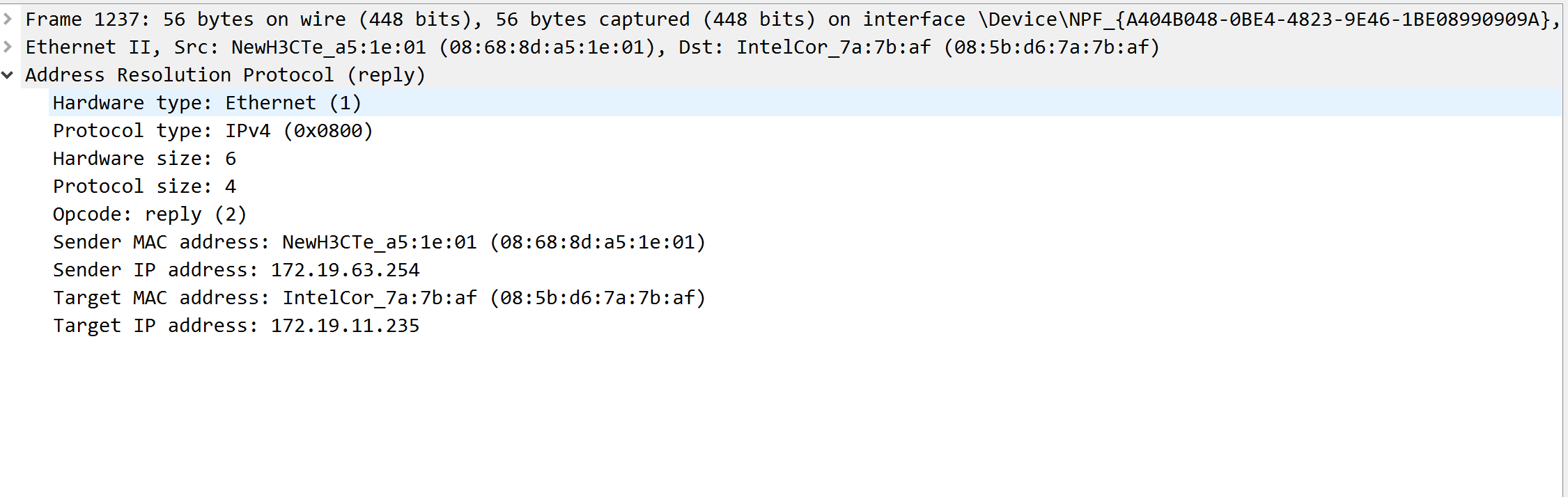
[总图]



[ARP请求包截屏] 用红线标出ARP协议中要查询的IP地址



[ARP响应包截屏]用红线标出所查询的IP地址对应的MAC地址



[找到一个Gratuitous ARP包截屏]

\* 如果没有，可以试一下可以重新配置一个新的IP地址，再找不到就算了。

[问题]

*当ARP缓存没有映射时，系统对要发送的IP分组会怎么做？*

从IP分组中提取出目的地址，根据IP目的地址查询路由表，1）若有下一跳，用下一跳的IP地址广播ARP请求获得对应的MAC地址。2）若即为直连网，则用目的地址IP广播ARP请求，将其对应的映射保存在ARP缓存中。

*ARP协议是否采用了超时重传？*没有*。*

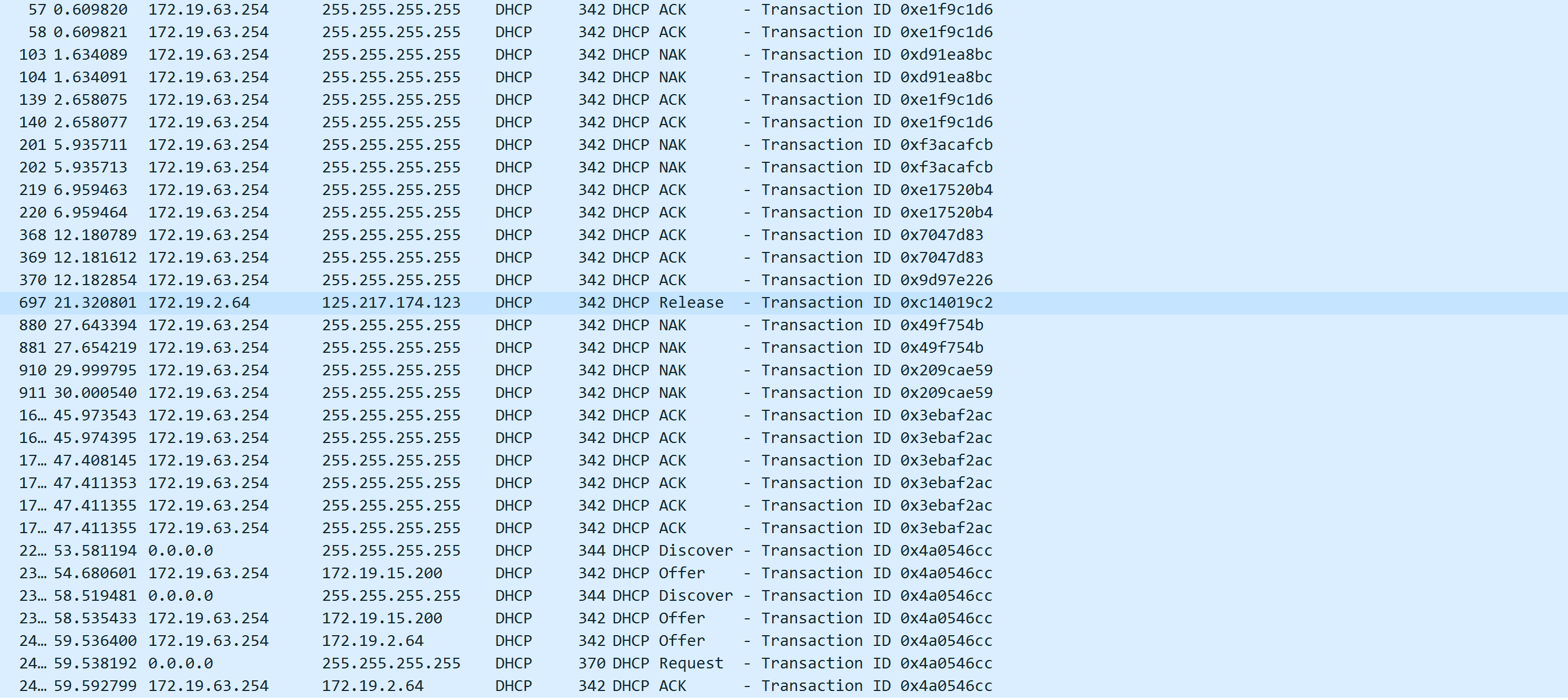
*Gratuitous ARP包有什么用途？*

1) 一个主机可以通过它来确定另一个主机是否设置了相同的I P地址。

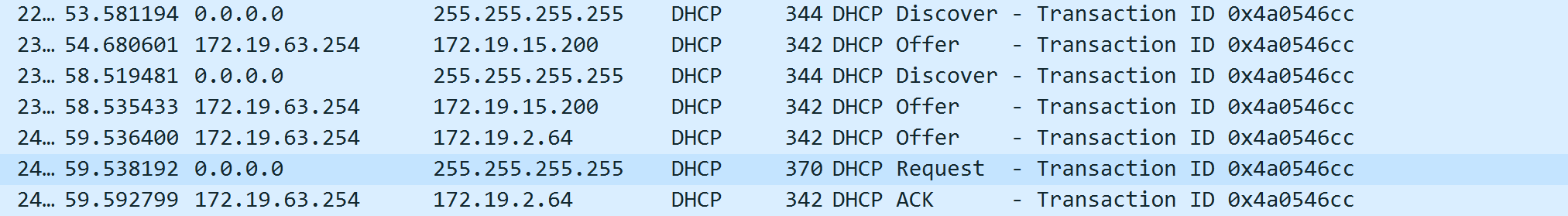
2) 如果发送Gratuitous ARP的主机正好改变了硬件地址（很可能是主机关机了，并换了一块接口卡，然后重新启动），那么这个分组就可以使其他主机高速缓存中旧的硬件地址进行相应的更新。

1. (DHCP.pcapng)DHCP协议（ipconfig /release 清除网络配置，ipconfig /renew）

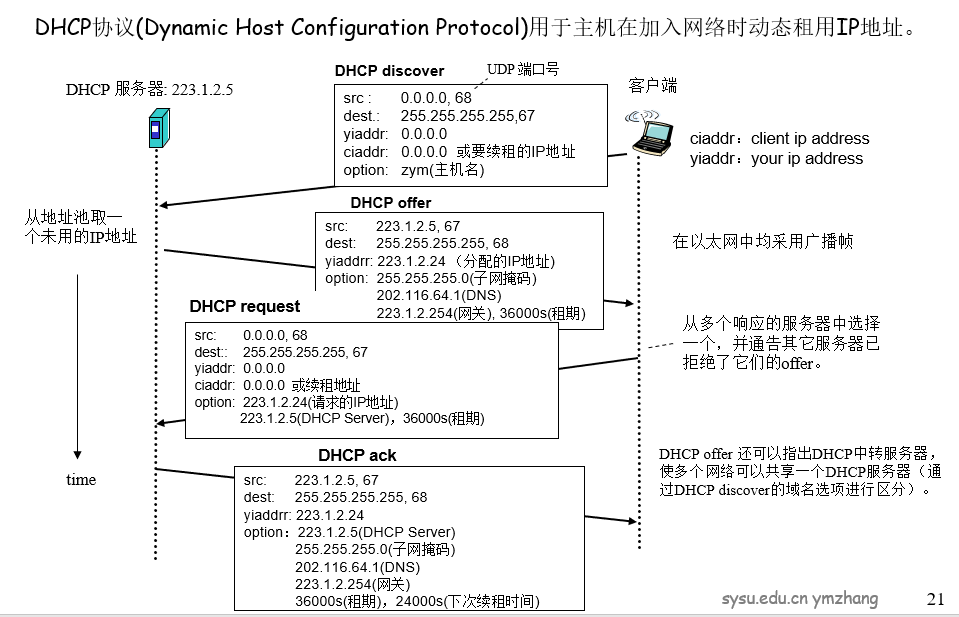
[总图]



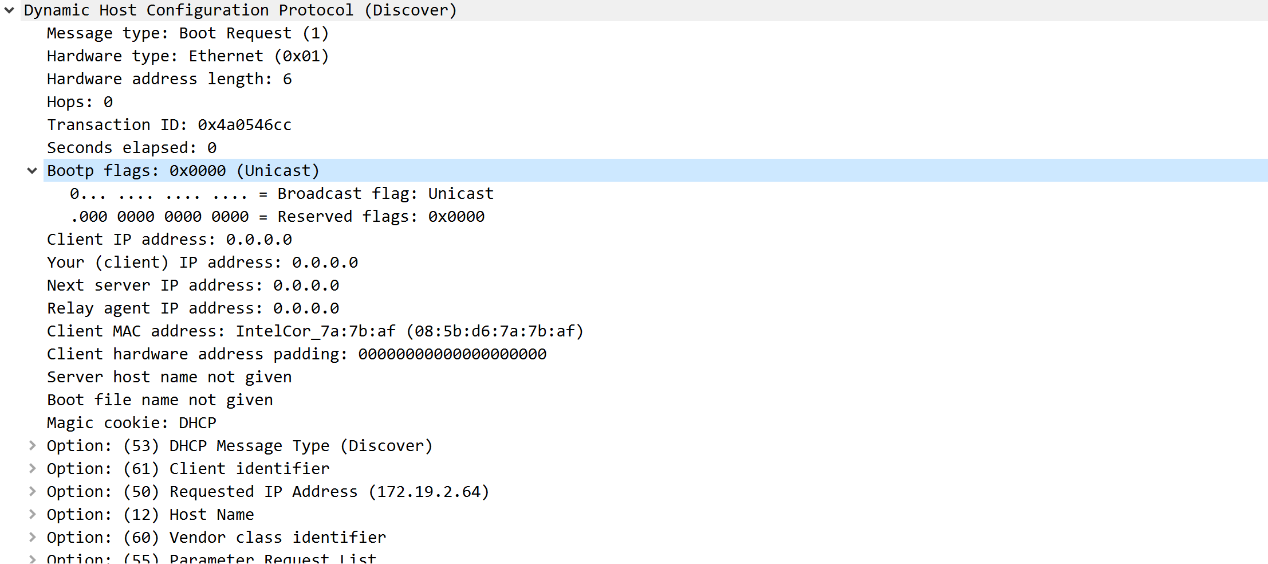
[四个包]



[对照课件]



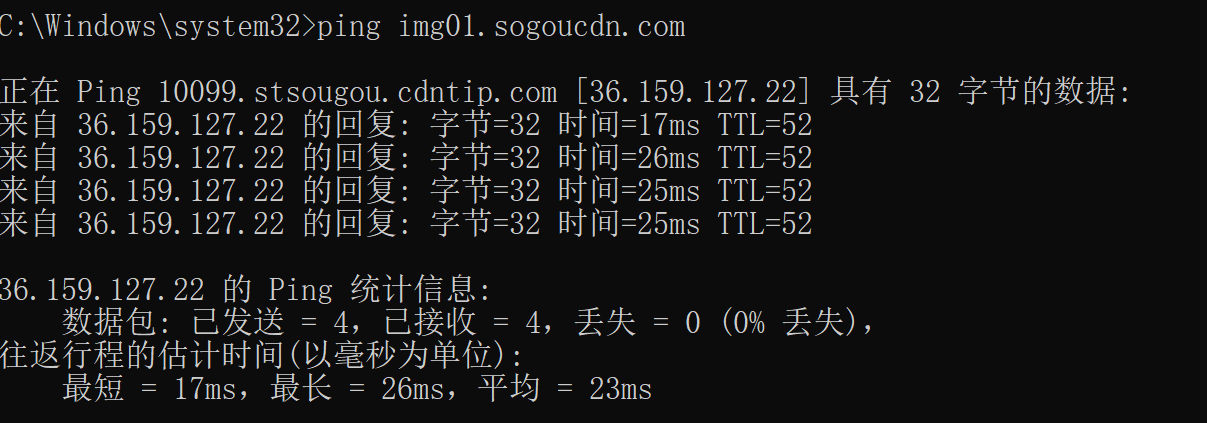
有没有可以纠正的内容？有的话写出来。

对照课件发现DHCP offer的地址非广播地址，而是单播地址。查看DHCP discover包后发现其中DHCP包中的标志位设为了0，表示单播。上网查阅资料了解到，DHCP 服务器使用单播来发送DHCP Offer报文，可以避免打扰其它主机。

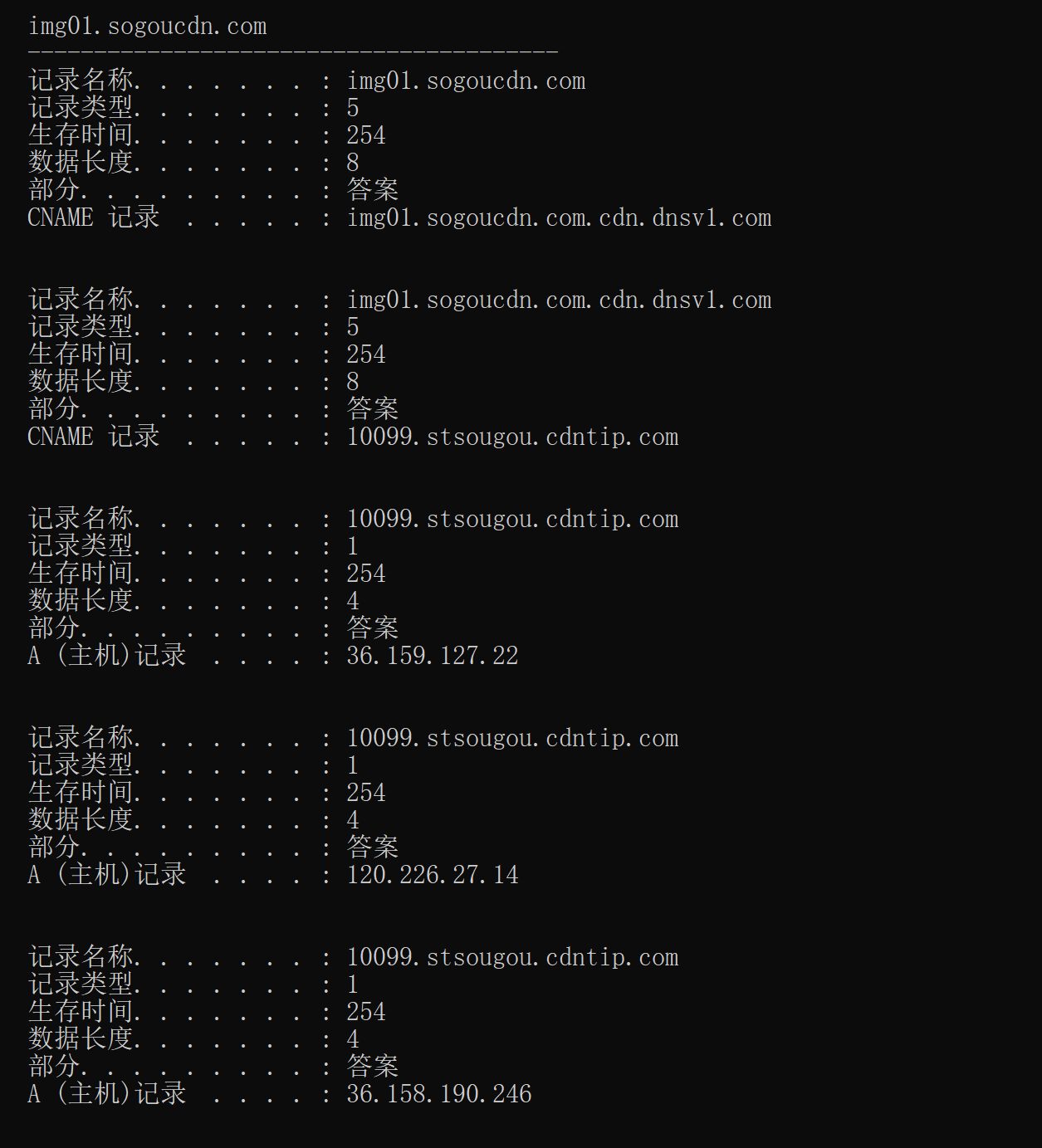
由于此时并没有分配IP地址，所以服务器不是通过ARP协议得知客户端的MAC地址。而是通过DHCP Discover包中的Client MAC address得知的客户端MAC地址，从而能实现单播。

1. (DNS.pcapng)DNS协议

先ping img01.sogoucdn.com并截屏：



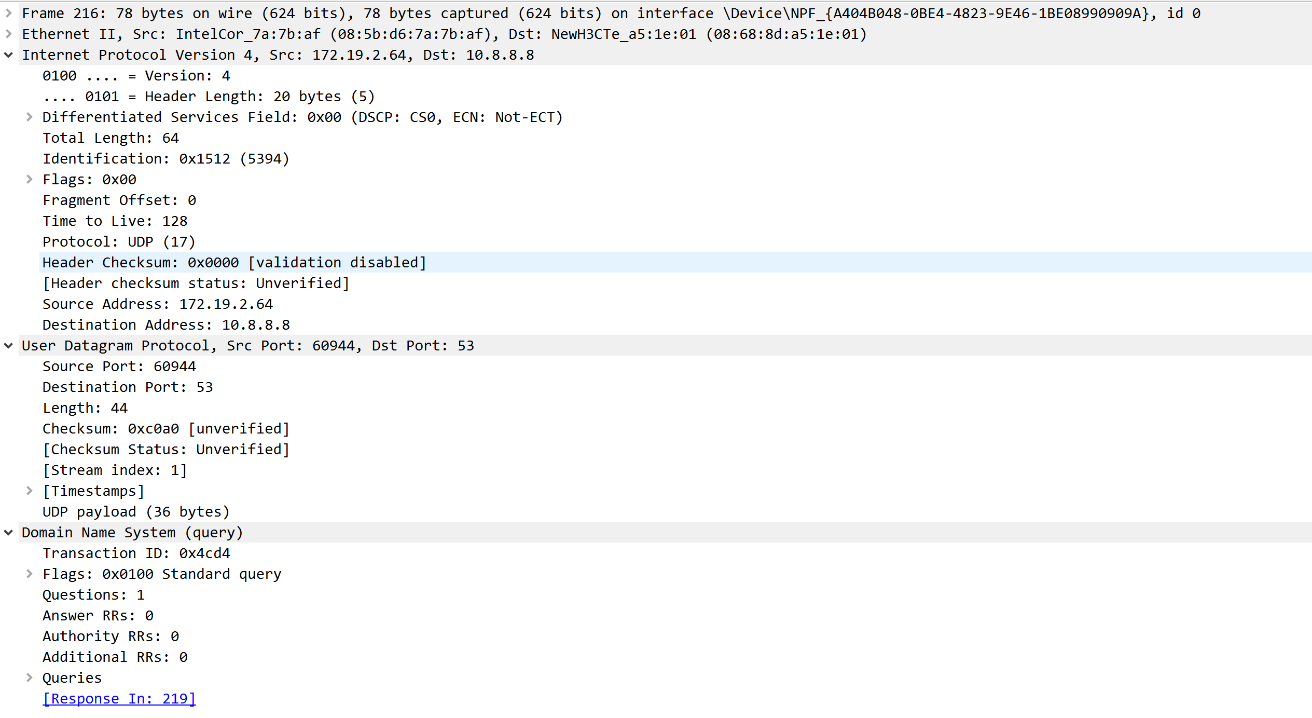
然后，在控制台用C:>ipconfig /displaydns查看DNS缓存，并截屏img01.sogoucdn.com的DNS记录：

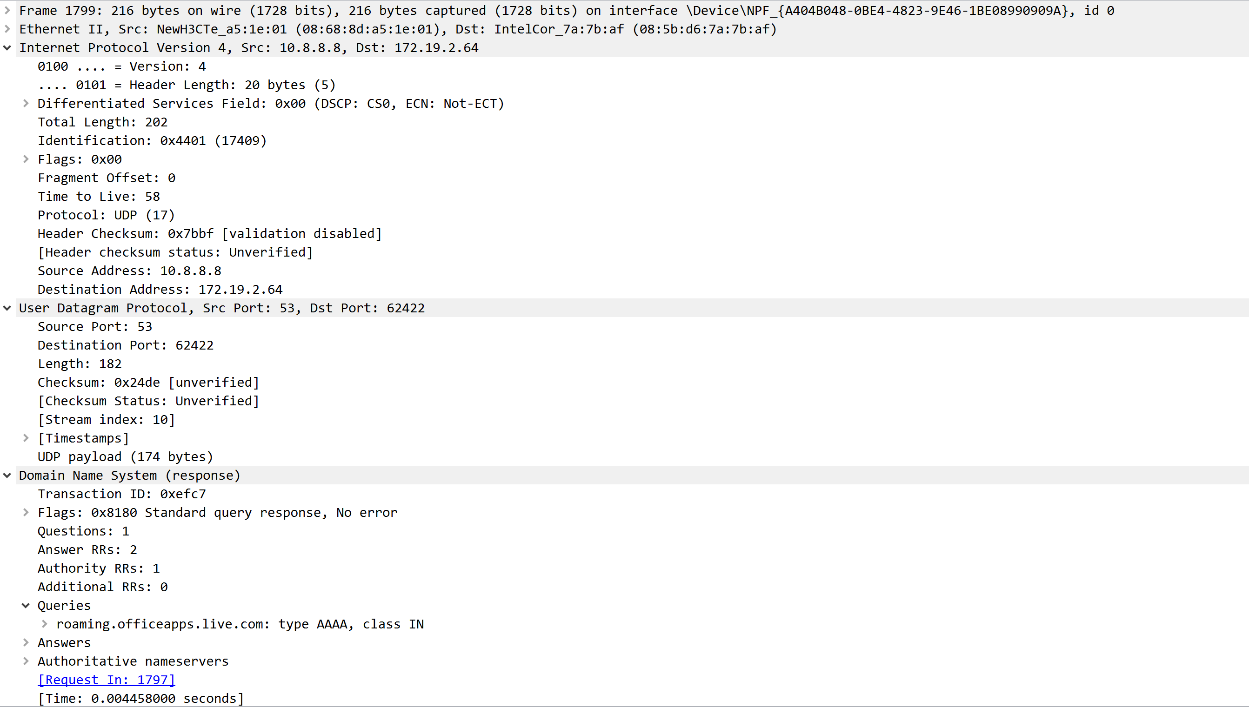


解释其中内容（说明如何可以从DNS记录中得到img01.sogoucdn.com的IP地址）：

CNAME记录也叫别名记录，相当于给域名起别的名字。A记录则是将一个域名映射为一个IP。CANME记录主要应用于CDN加速上。主机先向本地DNS服务器查询img01.sogoucdn.com的IP地址，本地DNS服务器中并没有这对映射关系，于是将域名的解析权交给CNAME指向的CDN专用DNS服务器。CDN的DNS服务器将CDN的全局负载均衡设备IP地址返回给用户。用户向CDN的全局负载均衡设备发起URL访问请求。CDN全局负载均衡设备根据用户IP地址，以及用户请求的URL，选择一台用户所属区域的区域负载均衡设备，并将请求转发到此设备上。基于以下这些条件的综合分析之后，区域负载均衡设备会选择一个最优的缓存服务器节点，并从缓存服务器节点处得到缓存服务器的IP地址，最终将得到的IP地址返回给全局负载均衡设备，再把服务器的IP地址返回给用户。

清除DNS记录：C:>ipconfig /flushdns后，再ping img01.sogoucdn.com并截包：

[DNS查询包]

[DNS响应包]

1. (TCP.pcapng)截取完整的TCP三次握手建立连接和四次挥手关闭连接的包：

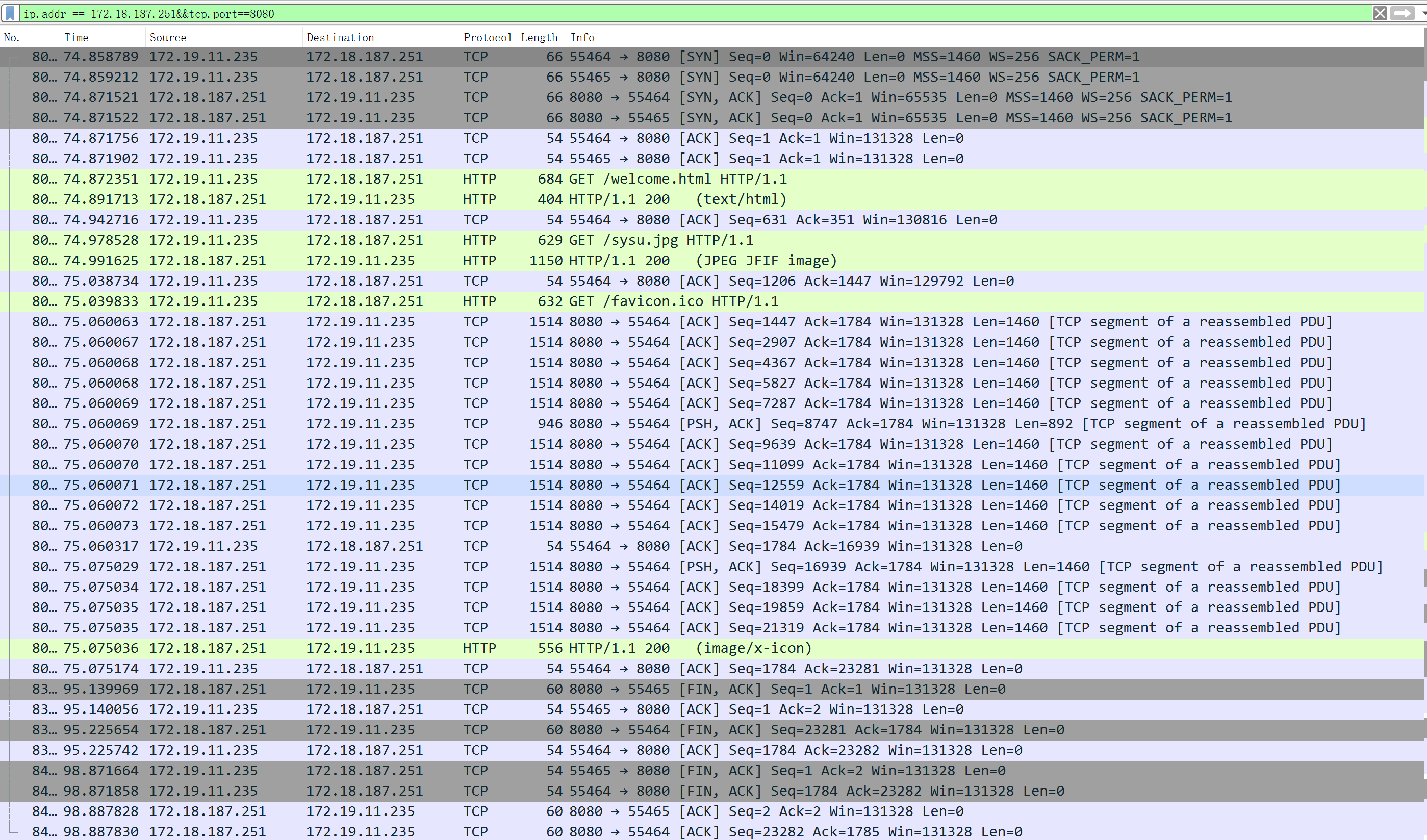
http://172.18.187.251:8080/welcome.html （要等一会）

先用过滤条件：ip.addr == 172.18.187.251

知道端口号后再用过滤条件：ip.addr == 172.18.187.251 && tcp.port==59161

第二遍要刷新一下

[总图]



[分析1]

* 建立连接, 写出标志位、相对序号、相对确认号和长度（数据长度）、选项：

（1）C->S

标志位：SYN=1

相对序号=0

长度=0B

选项：MSS=1460B；Window scale=8；选择性确认

（2）S->C

标志位：SYN=1，ACK=1

相对序号=0

相对确认号=1

长度=0

选项：MSS=1460B；Window scale=8；选择性确认

（3）C->S

标志位：ACK=1

相对序号=1

相对确认号=1

长度=0

选项：MSS=1460B；Window scale=8；选择性确认

* 传送出数据, 写出相对序号，相对确认号，长度，选项以及每一步的作用：

(1)S->C

相对序号=15479

相对确认号=1784

长度=1460

无选项

作用：发送数据

(2)C->S

相对序号=1784

相对确认号=16939

长度=0

无选项

作用：确认

* 释放连接, 写出标志位、相对序号、相对确认号和长度、选项：

（1）S->C

标志位：FIN，ACK

相对序号=23281

相对确认号=1784

无选项

长度=0

（2）C->S

标志位：ACK

相对序号=1784

相对确认号=23282

无选项

长度=0

（3）C->S

标志位：FIN，ACK

相对序号=1784

相对确认号=23282

无选项

长度=0

（4）S->C

标志位：ACK

相对序号=23282

相对确认号=1785

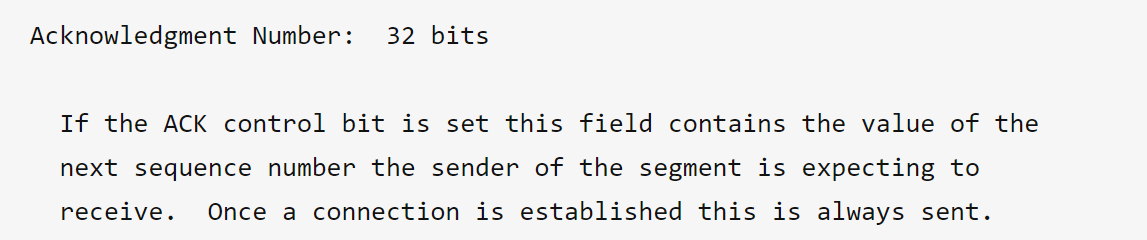
无选项

长度=0

[分析3]

有什么特别的发现？

发现在TCP四次挥手的过程中与上课所讲的不一样。第一次挥手发送的标志位为FIN+ACK，而非上课所讲的FIN标志位。查询TCP协议发现对于ACK有一段这样的描述。

 该规定指出TCP除了主动发起连接的第一个SYN包，ACK=0，其它所有TCP包都设置ACK= 1 标志位。所以才会出现抓包时的现象。

【完成情况】

是否完成以下步骤？(√完成 -未做完 ×未做)

(1) [√] (2) [√] (3) [√] (4) [√] 5[√] 6[√]

【实验体会】

通过本次实验，我复习了以往学过的应用层和网络层协议，抓包分析也让我对各个协议有了更直观的感受。

在实验的过程中，我遇到了一些困难。在ICMP协议的实验中，最初很难ping通网站，经常返回请求超时。后来在班群大家讨论，发现有线校园网比较容易ping通。虽然更改为了有线校园网，但我的ping -s还是ping不通域名。后来在QQ群中了解到，路由器可能会丢弃带有选项的IP数据报，导致ping不通。于是后来我改为了ping同学的主机。

在ARP协议的实验中，最初用cmd执行arp -d默认网关的arp映射时报错，提示“删除失败,请求的操作需要提升”。改用管理员身份运行时，也无法删除。后来我尝试用powershell管理员身份运行该指令，才成功。

在实验的过程中，也发现了一些和理论课有出入的地方。如DHCP协议，上课时说DHCP Offer采用广播帧，但是在抓包的过程中发现，DHCP offer可以采取单播的方式传输，减少带宽的浪费。

其次在TCP协议四次挥手的抓包分析时，我发现第一次挥手实际发送的标志位FIN+ACK，而并非上课所讲的FIN。查询TCP协议了解到，处第一次SYN连接以外，TCP其他所有包ACK标志位均有效。

通过抓包分析，我扩充了对各协议的理解，收获很大。

【交实验报告】

上传网址：<http://172.18.187.251/netdisk/default.aspx?vm=19net>

编程实验

截止日期（不迟于）：2021年7月1日（周四）23:00

上传文件名：学号\_姓名\_WireShark.doc

学号\_姓名\_WireShark.rar （包含所有.pcapng文件）