院 系 数据科学与计算机学院 学号　18340066　 姓名 黄炜钊

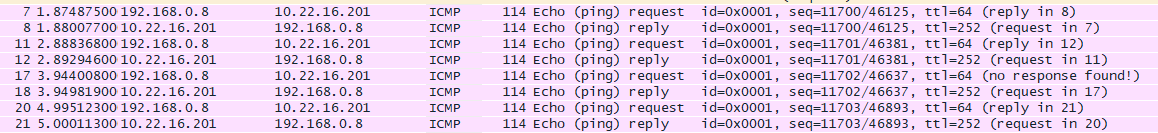
班 级 18

【实验题目】WireShark**实验**

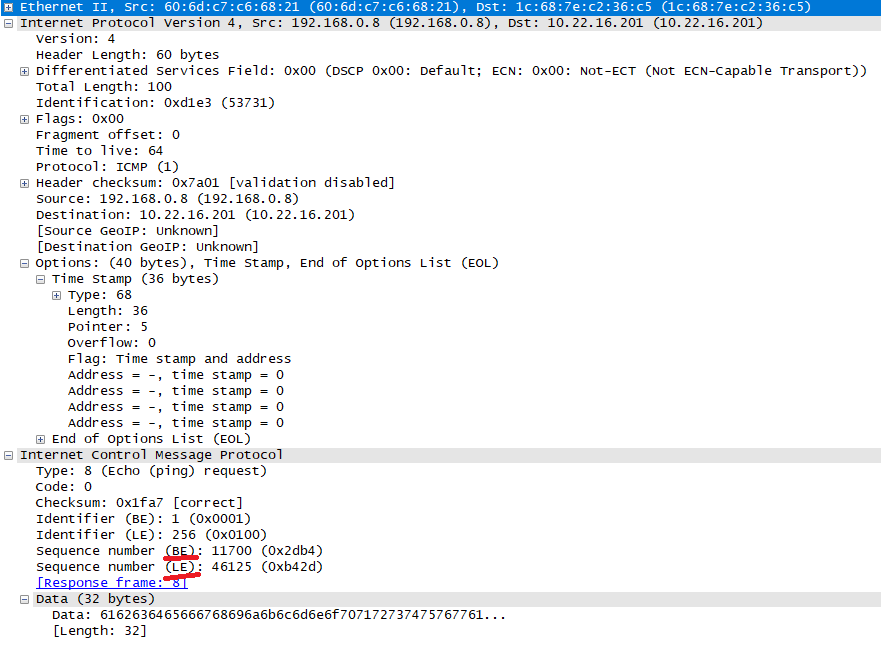
【实验目的】通过WireShark分析IP协议(Option)、ICMP协议、ARP协议、DHCP协议、DNS协议、TCP协议。

【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）。

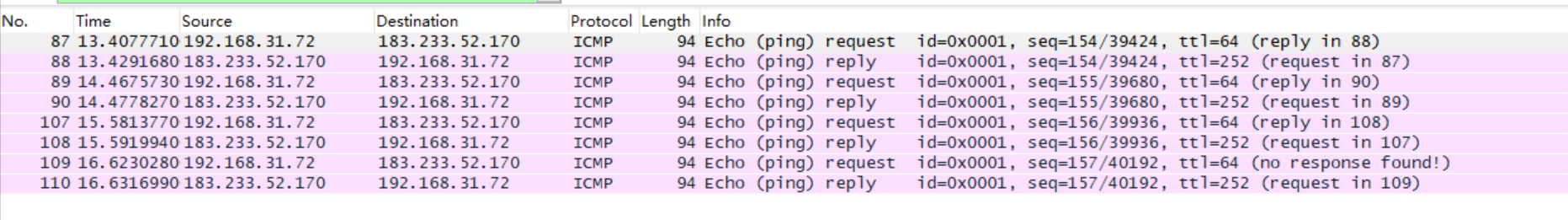
注意每一步都要保存截包文件

【实验任务】

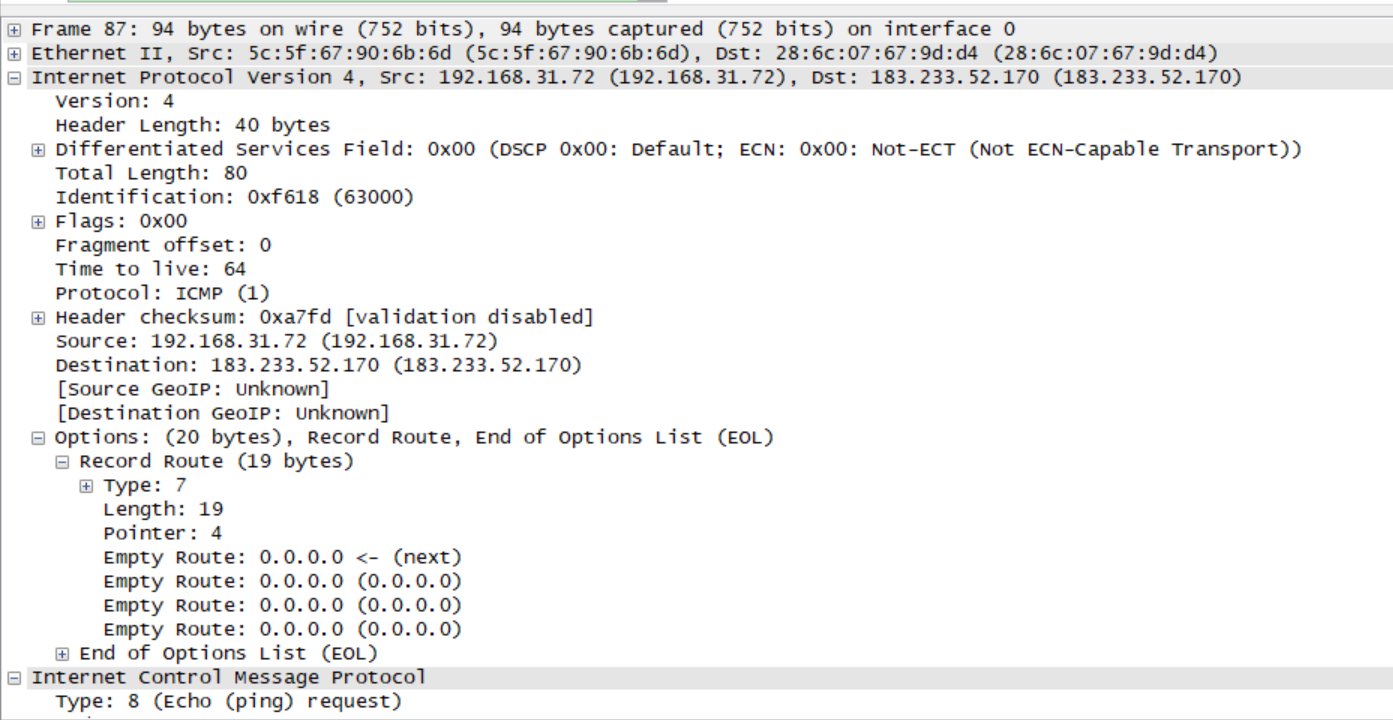
1. (IP.pcapng)IP Option和ICMP协议。

**命令：ping -r 4域名**

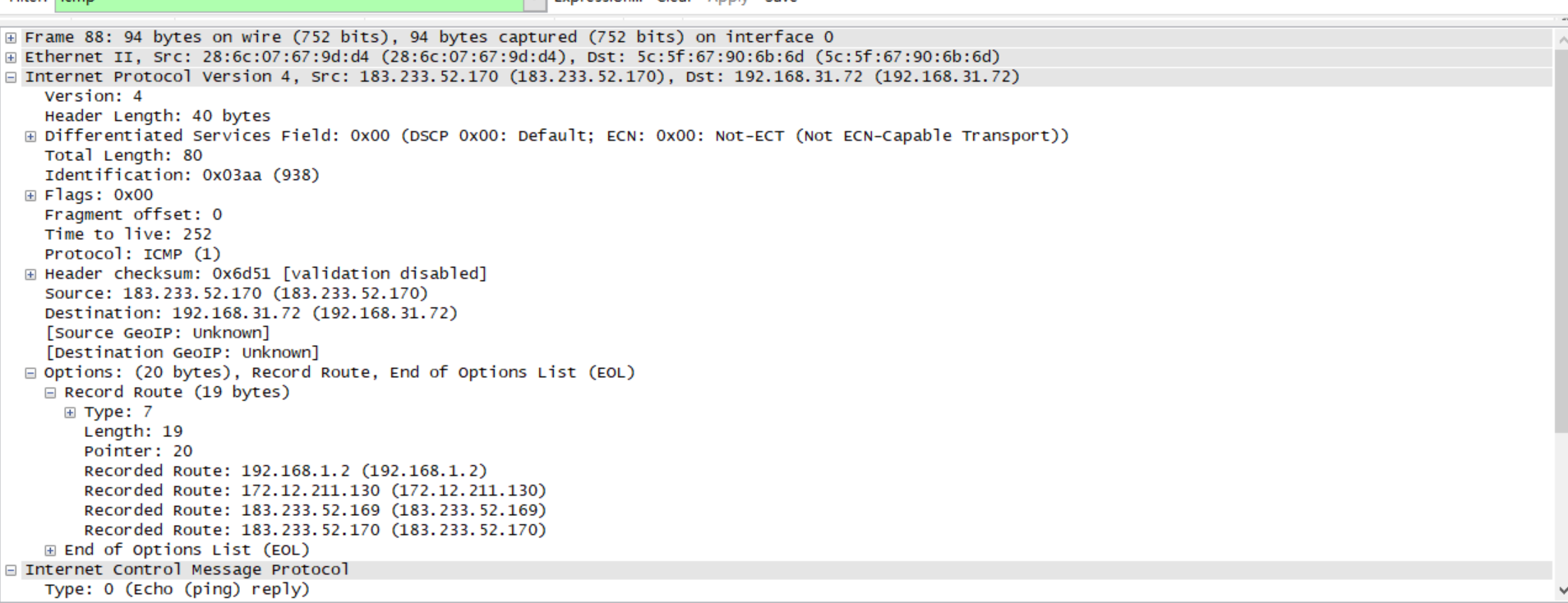
[Ping总图]



[Ping请求包截屏]



[Ping响应包截屏]



[针对于所截包的问题]（响应包）

IP选项的长度：80

ICMP包的Identifier：0x03aa

ICMP包的序号：88

ICMP包的数据部分长度：32bytes

ICMP包的数据部分的内容：

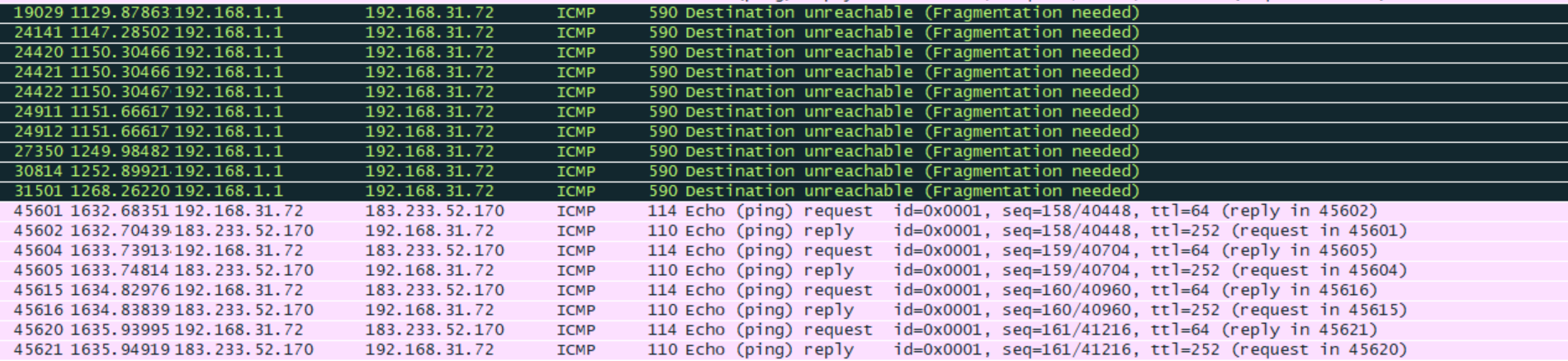
61:62:63:64:65:66:67:68:69:6a:6b:6c:6d:6e:6f:70:71:72:73:74:75:76:77:61:62:63:64:65:66:67:68:69

Identifier是什么含义？

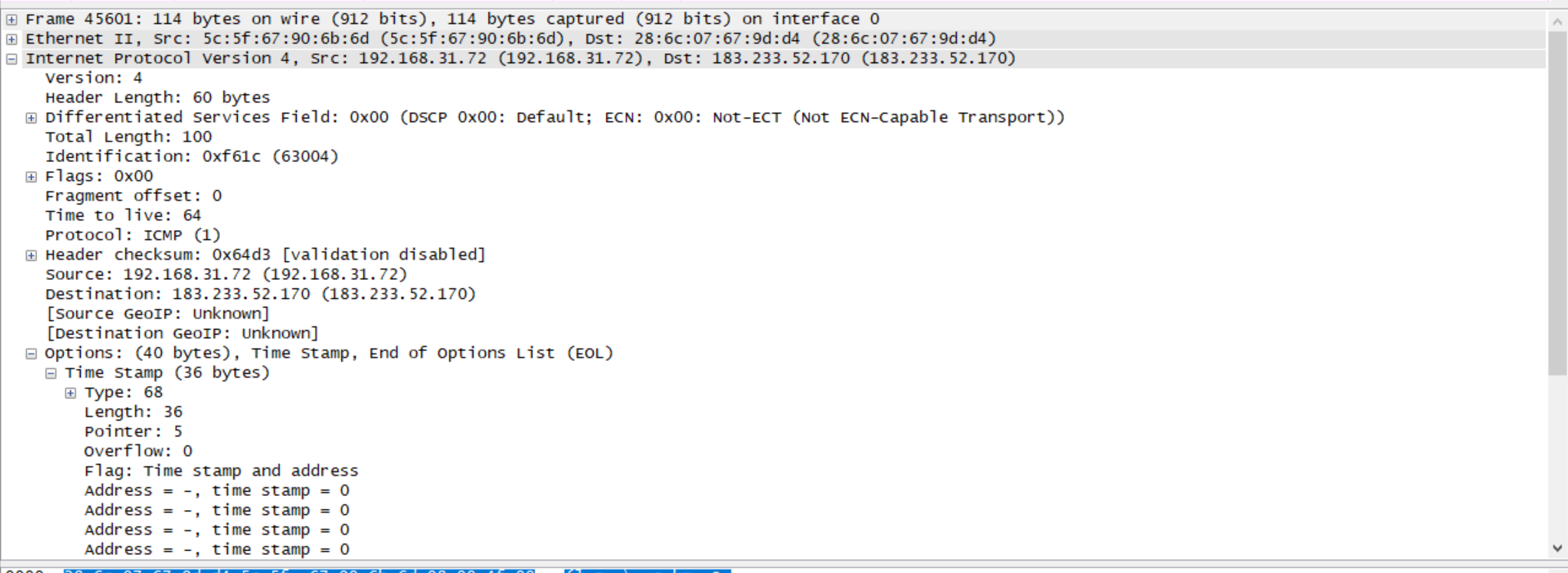
标识符

**命令：ping -s 4域名**

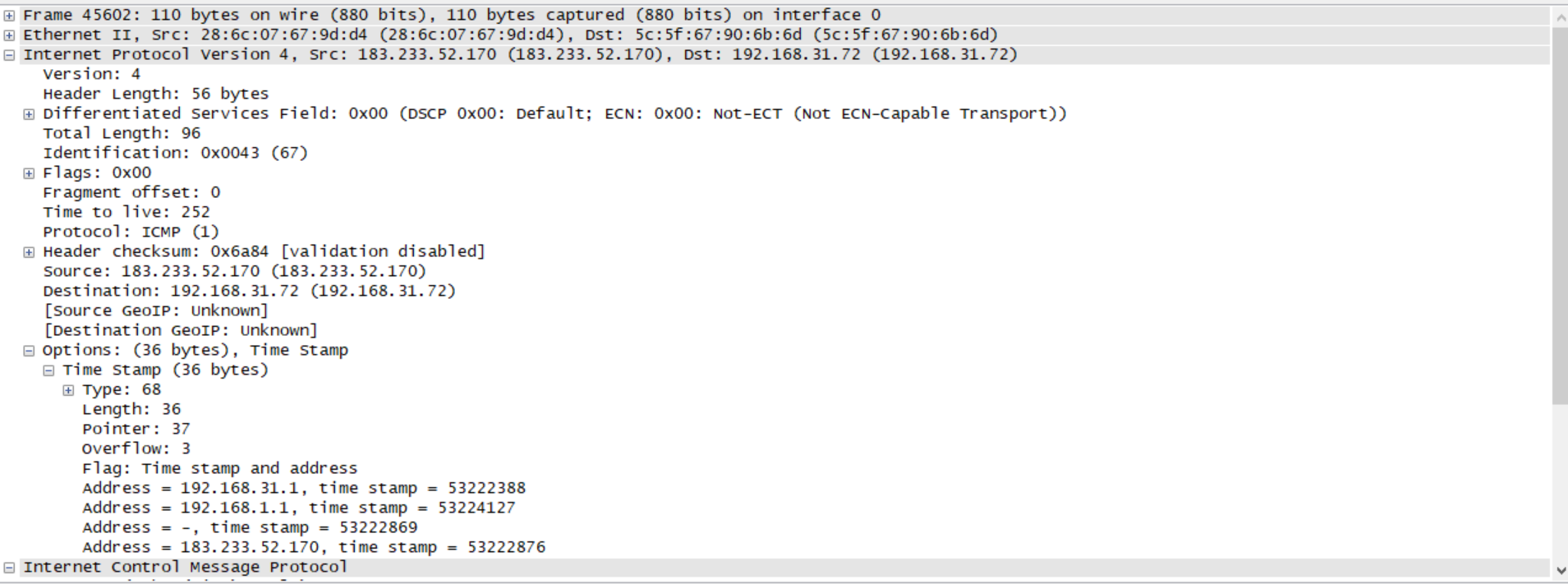
[Ping总图]



[Ping请求包截屏]



[Ping响应包截屏]



[问题]

IP选项的长度：96

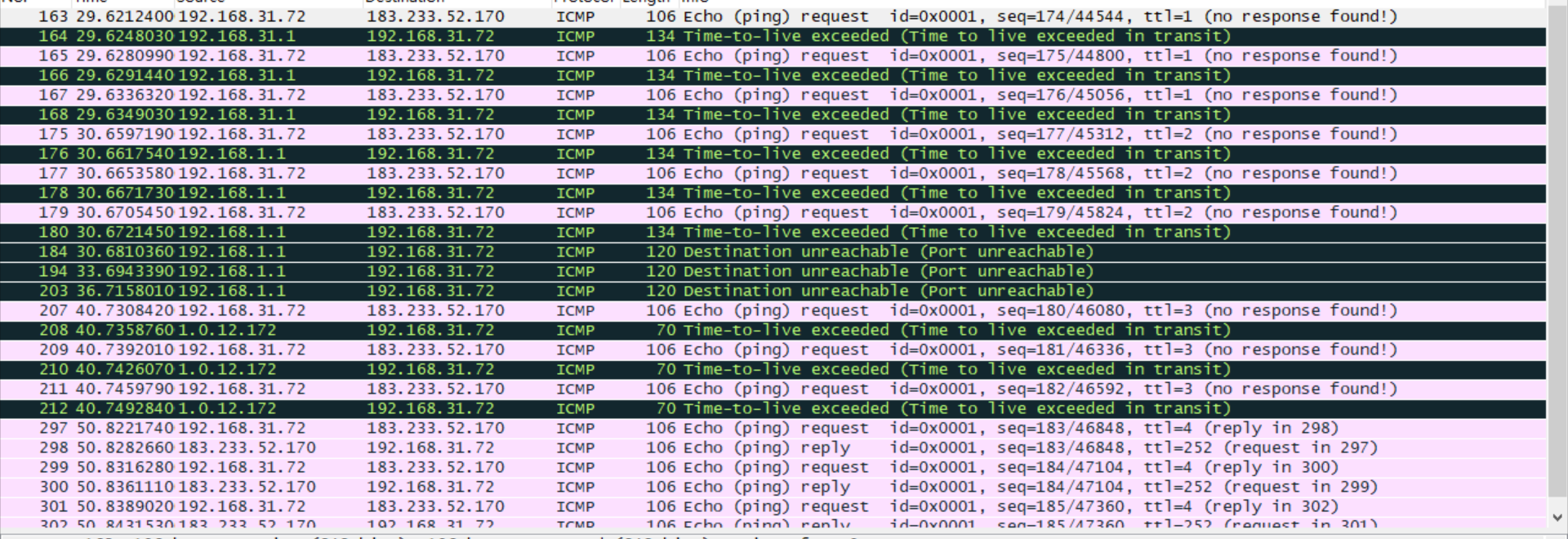
选项中的时间戳是否正确？

正确

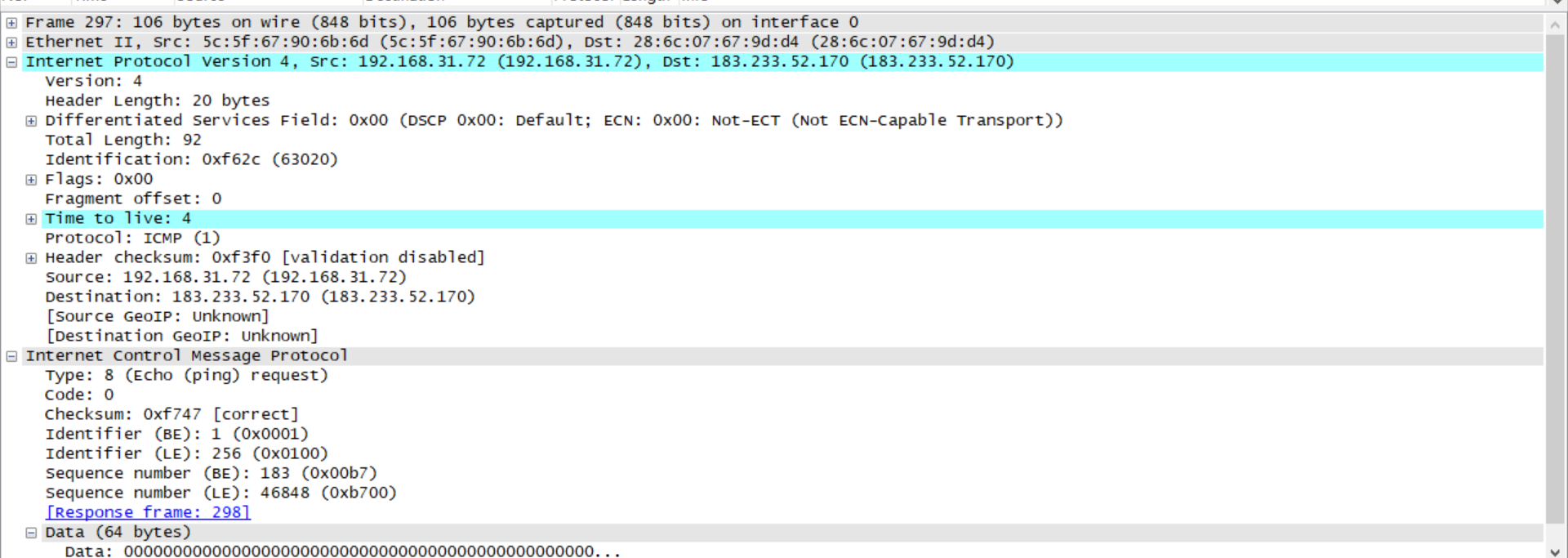
1. (tracert.pcapng) ICMP协议

命令：tracert -h 4 域名

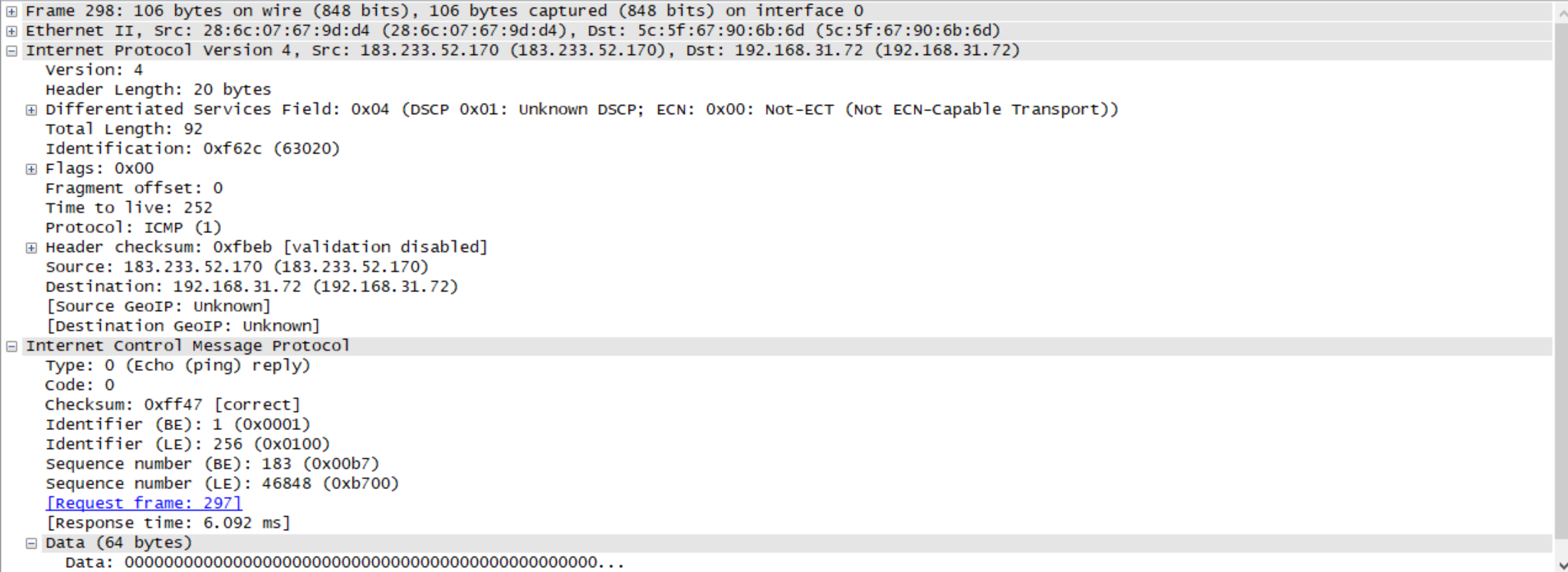
[tracert总图截屏]



[TTL=4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]



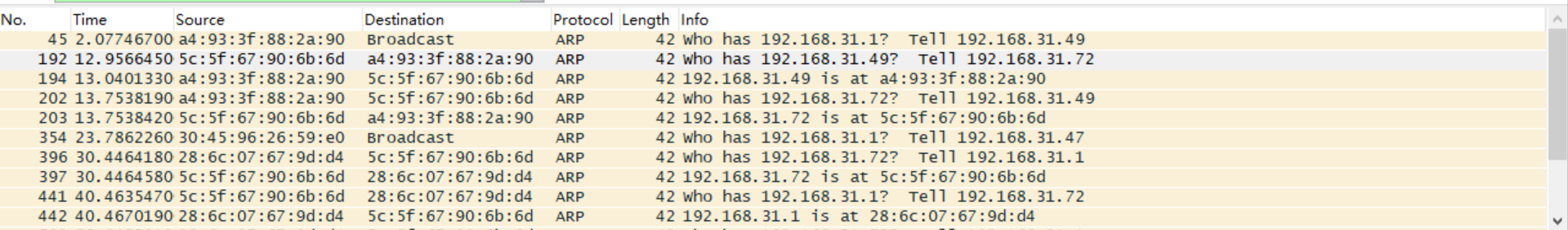
1. (arp.pcapng)ARP协议。

命令：arp –a

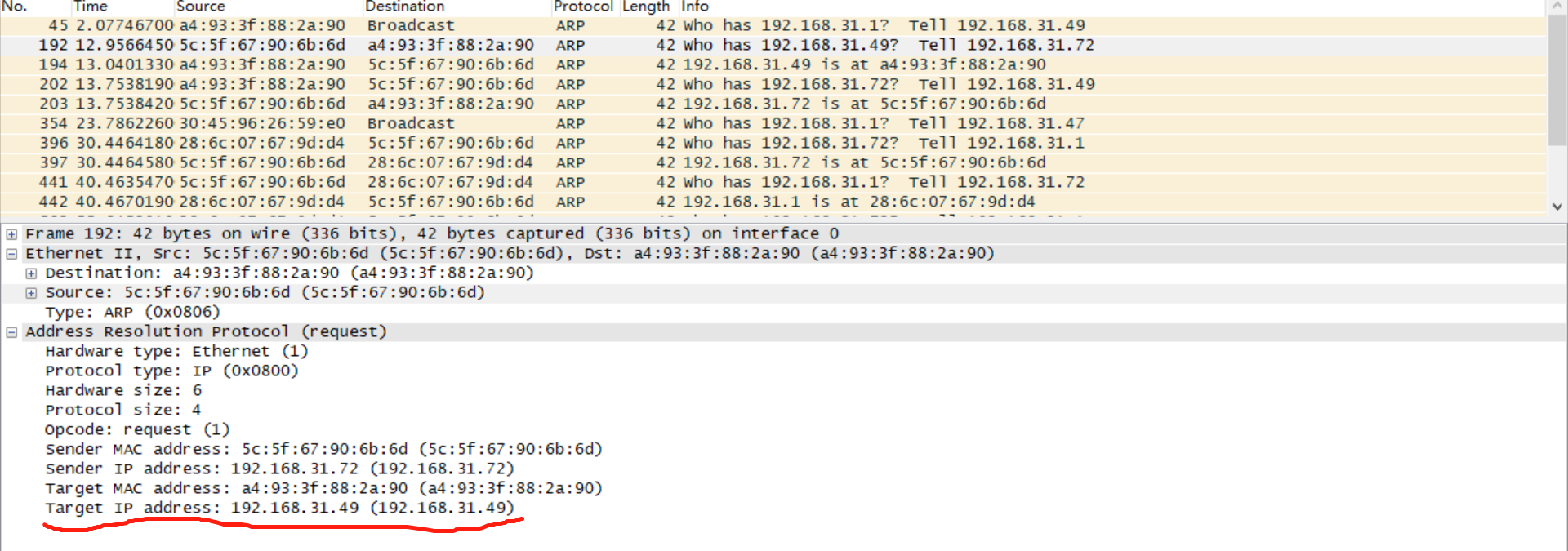
arp –d 192.168.0.14

ping家里另一台电脑或手机：先查看ARP缓存，删掉这台电脑的映射，然后启动截包，再ping它

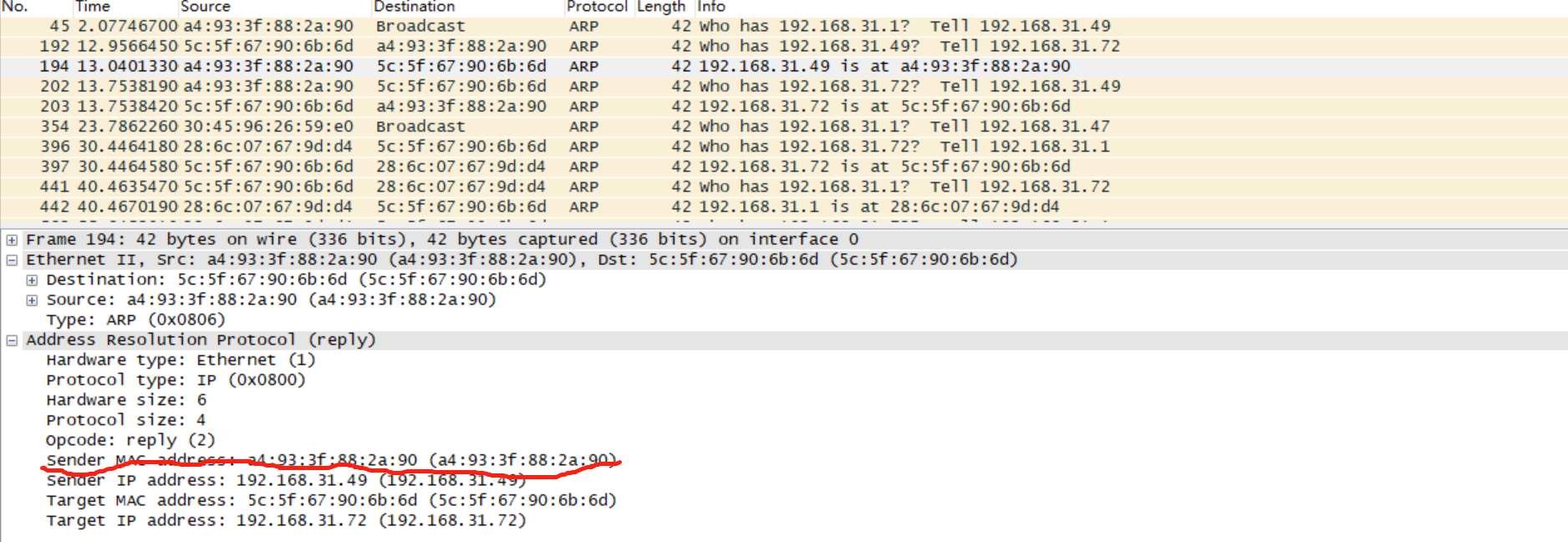
[总图]



[ARP请求包截屏] 用红线标出ARP协议中要查询的IP地址

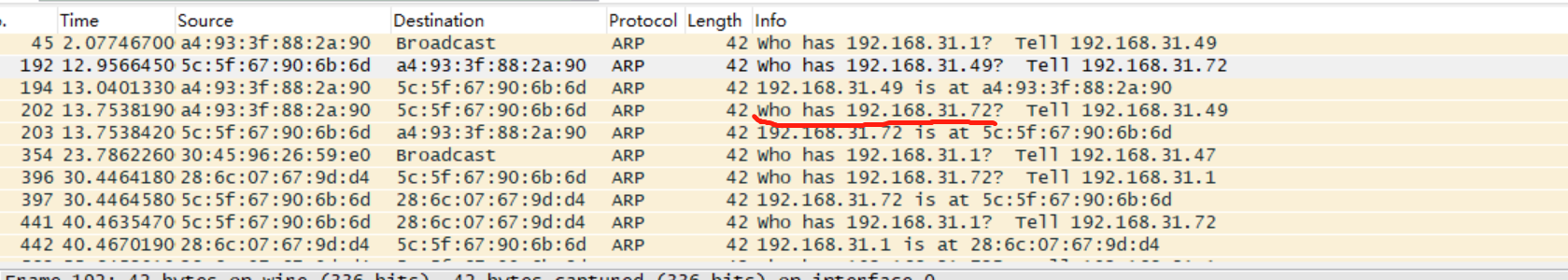


[ARP响应包截屏]用红线标出所查询的IP地址对应的MAC地址



[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？

在网络上用广播方式发送ARP请求分组。

ARP协议是否采用了超时重传？

采用了。

Gratuitous ARP包有什么用途？

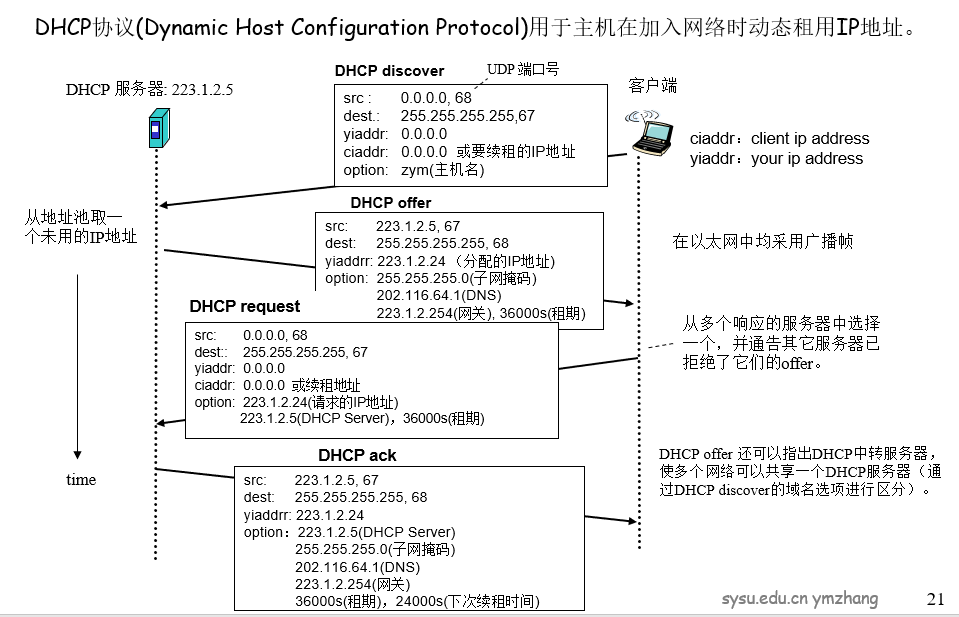
验证ip是否冲突和更换物理网卡。

1. (DHCP.pcapng)DHCP协议

[总图]

[四个包]

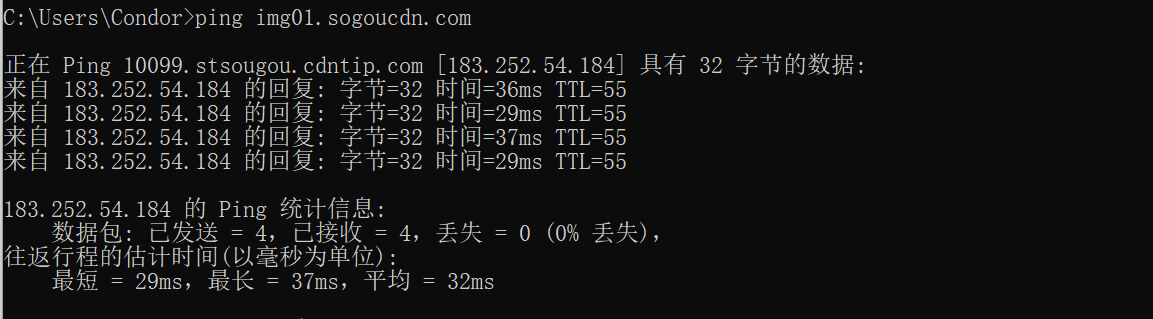
[对照课件]



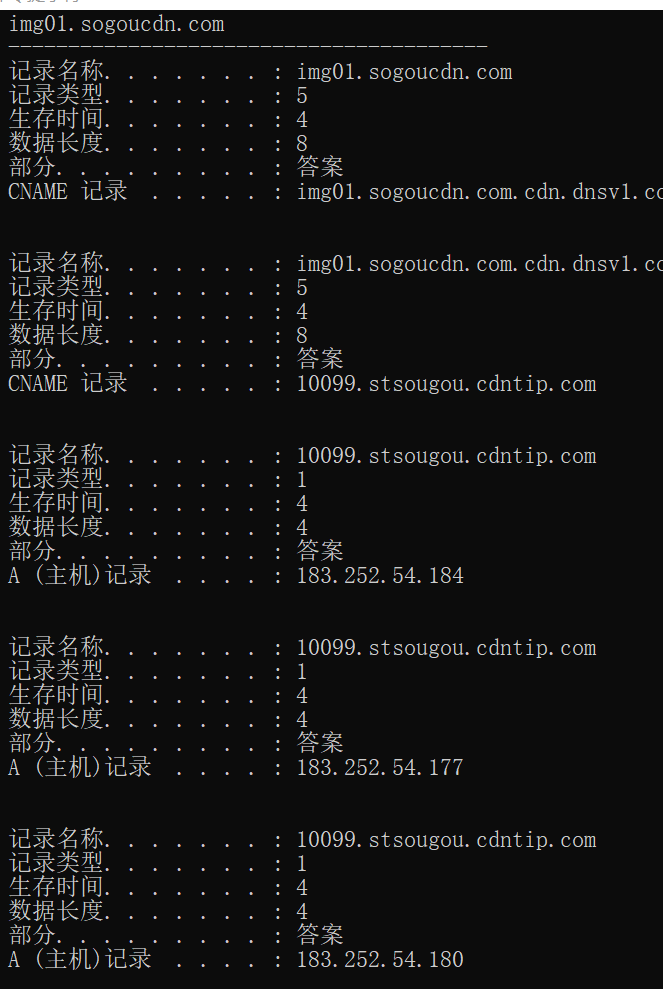
有没有可以纠正的内容？有的话写出来。

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：

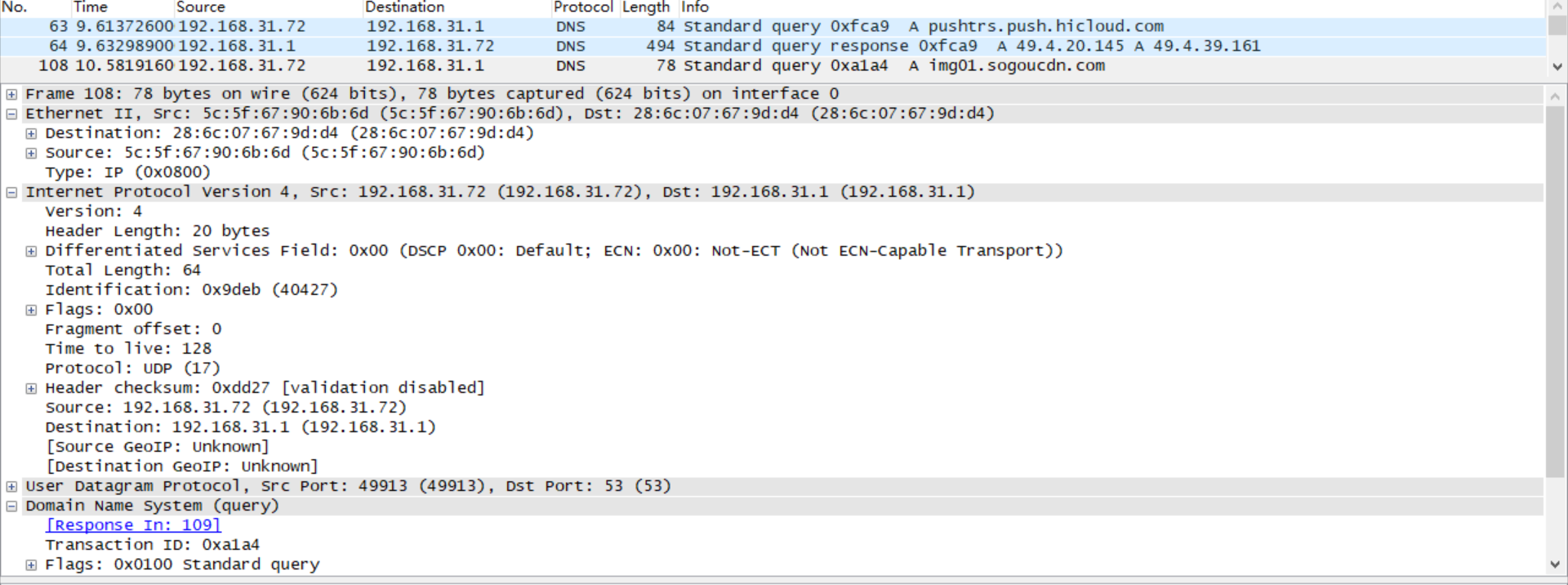


解释其中内容（说明如何可以从DNS记录中得到img01.sogoucdn.com的IP地址）：

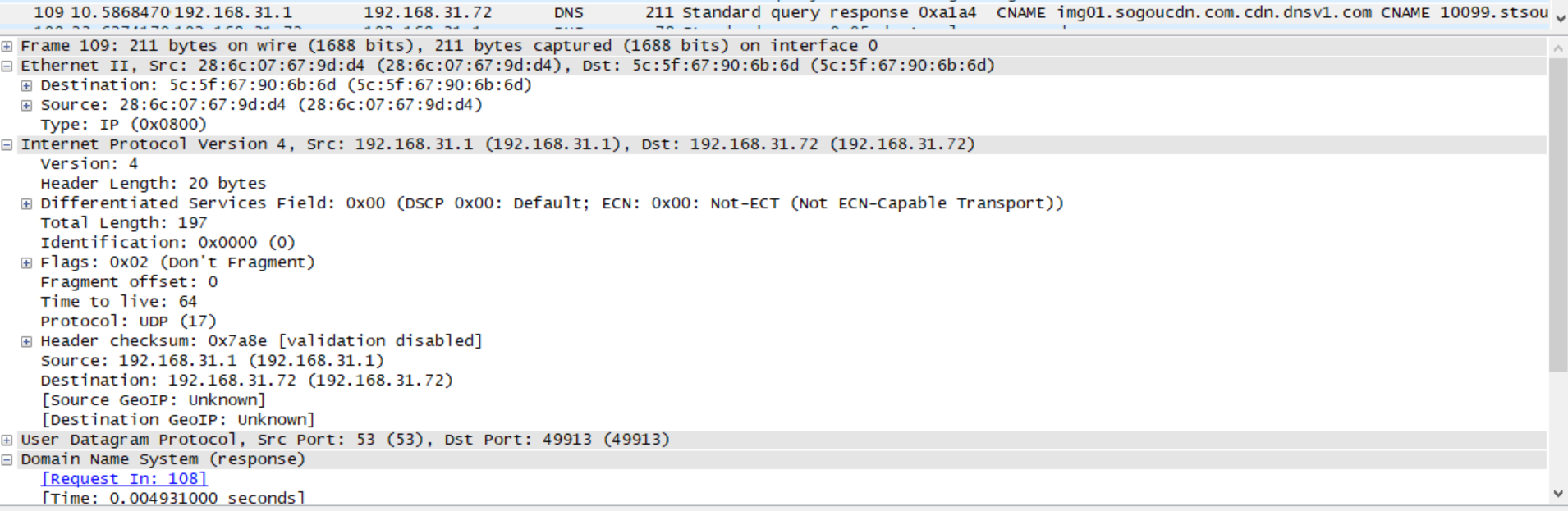
在记录中不断跳转，直到最后获取ip地址。

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：

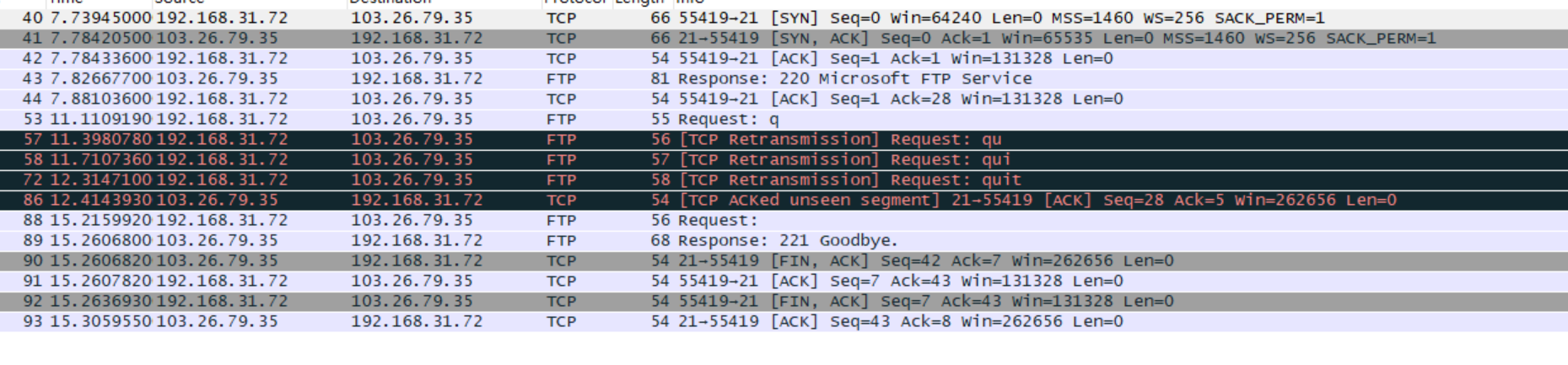
过滤条件：ip.addr==192.168.31.72 and ip.addr==103.26.79.35

192.168.31.72要用你的电脑的IP地址替换。

http://103.26.79.35/images/sysu.png （刷新后要等很久才会关闭连接）

如果需要传送完整的图(第二次开始 304 not modified)，可以采用其他图sysu2.png~sysu24.png

[总图]



[分析]

三次握手：

我的电脑先发送syn包到服务器，并进入SYN\_SENT状态，等待服务器确认；

服务器收到syn包，确认了我的电脑的SYN，同时也发送SYN+ACK到我的电脑，并进入SYN\_RECV状态；

客户端收到了SYN+ACK，向服务器发送确认包ACK，待服务器收到之后，两者进入tcp连接成功状态，完成三次握手。

四次挥手：

服务器发送一个FIN，关闭服务器到我的电脑的数据传输；

我的电脑收到这个FIN，发送一个ACK给服务器；

随即，我的电脑关闭与服务器的链接，发送一个FIN给服务器，关闭我的电脑到服务器的数据传输；

服务器发回ACK确认，完成四次挥手。

【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】

写出实验过程中的问题，思考及解决方法，简述实验体会（如果有的话）。

DHCP部分不知道从何下手。

【交实验报告】

上传网址：<http://103.26.79.35/netdisk/default.aspx?vm=18net>

截止日期（不迟于）：2020年7月23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）