院 系 数据科学与计算机学院 学号　　18340146 姓名 宋渝杰

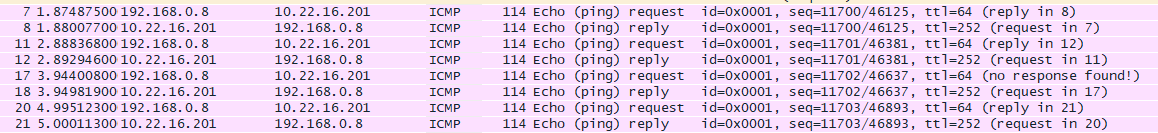
班 级 18

【实验题目】WireShark**实验**

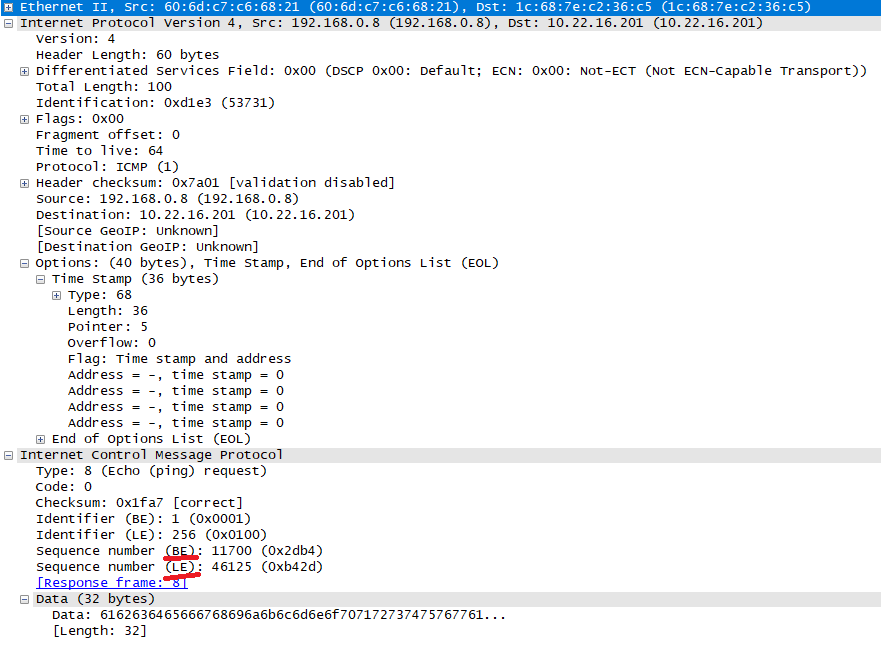
【实验目的】通过WireShark分析IP协议(Option)、ICMP协议、ARP协议、DHCP协议、DNS协议、TCP协议。

【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

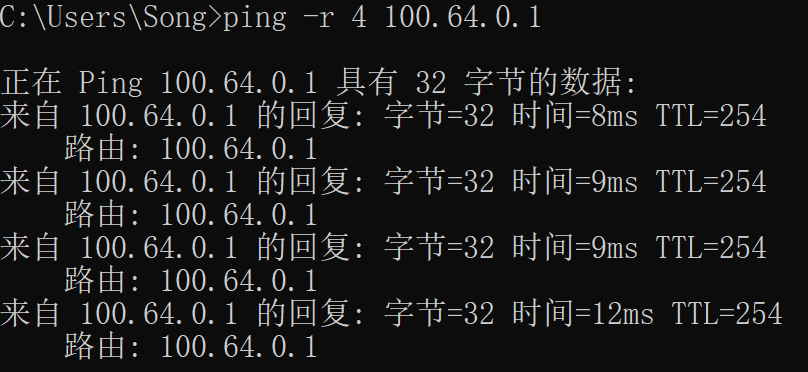
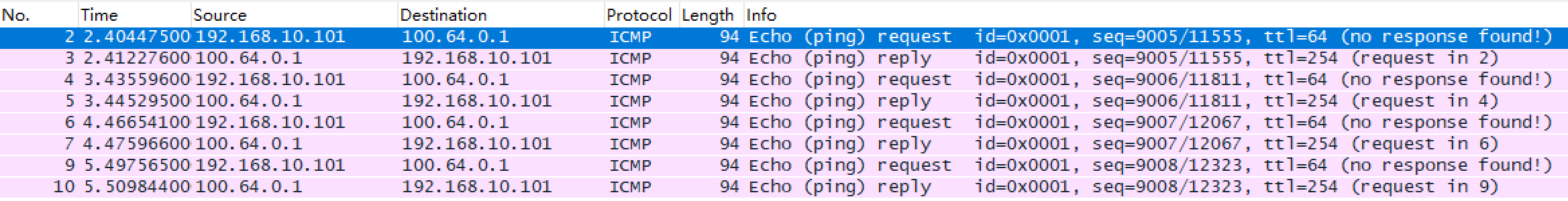
【实验任务】

1. (IP.pcapng)IP Option和ICMP协议。

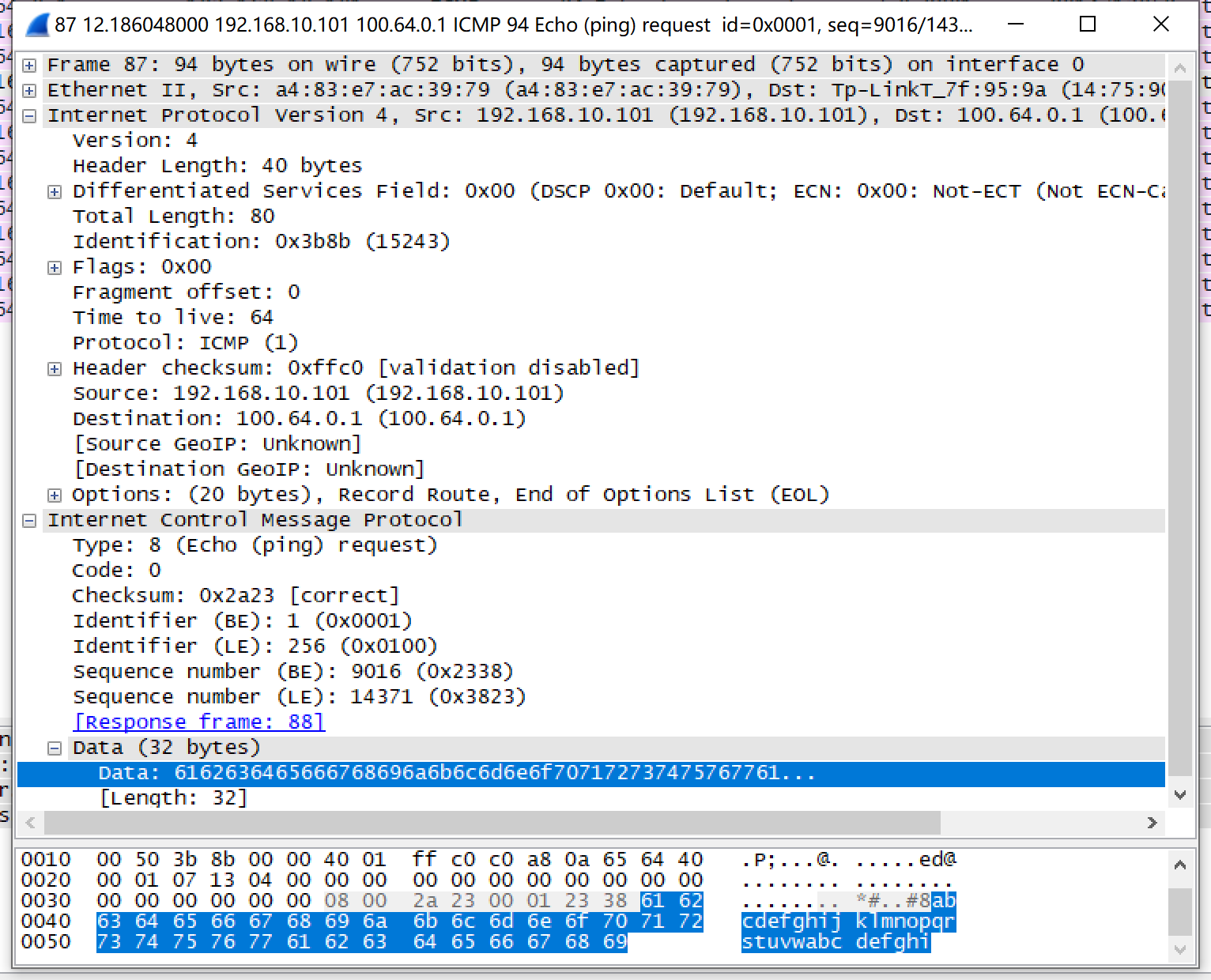
**命令：ping -r 4域名**

[Ping总图] ping -r 4 100.64.0.1

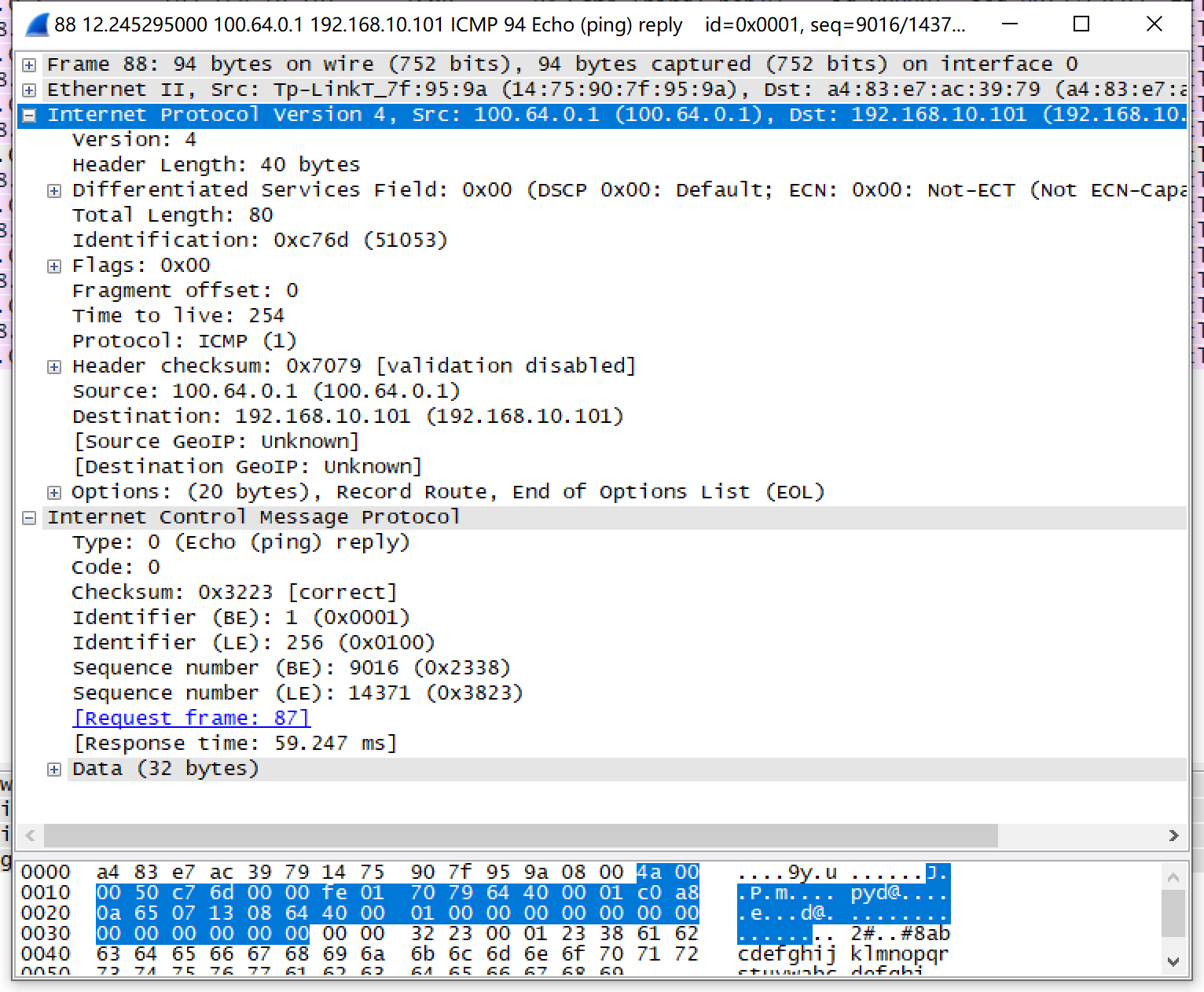
已采用了tracert找到去www.sohu.com路径上的IP地址，依次试一下后只有这一个ip地址可以ping通（这个地址可能是小区路由器出口），因此只能采用ping该地址的方式



[Ping请求包截屏]



[Ping响应包截屏]



[针对于所截包的问题]

IP选项的长度：20

ICMP包的Identifier：1（BE）256（LE）

ICMP包的序号：9008

ICMP包的数据部分长度：32bytes

ICMP包的数据部分的内容：

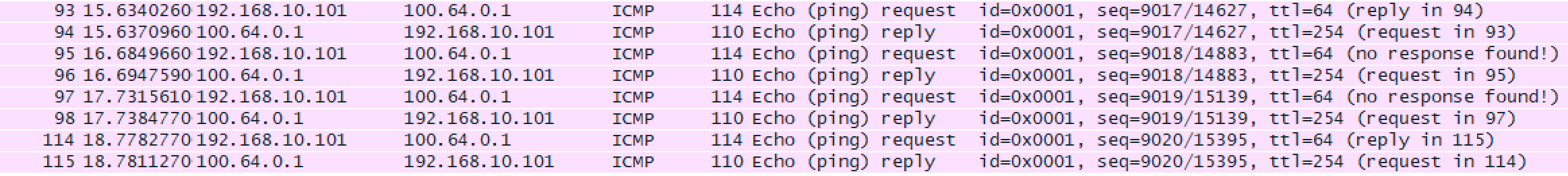
6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

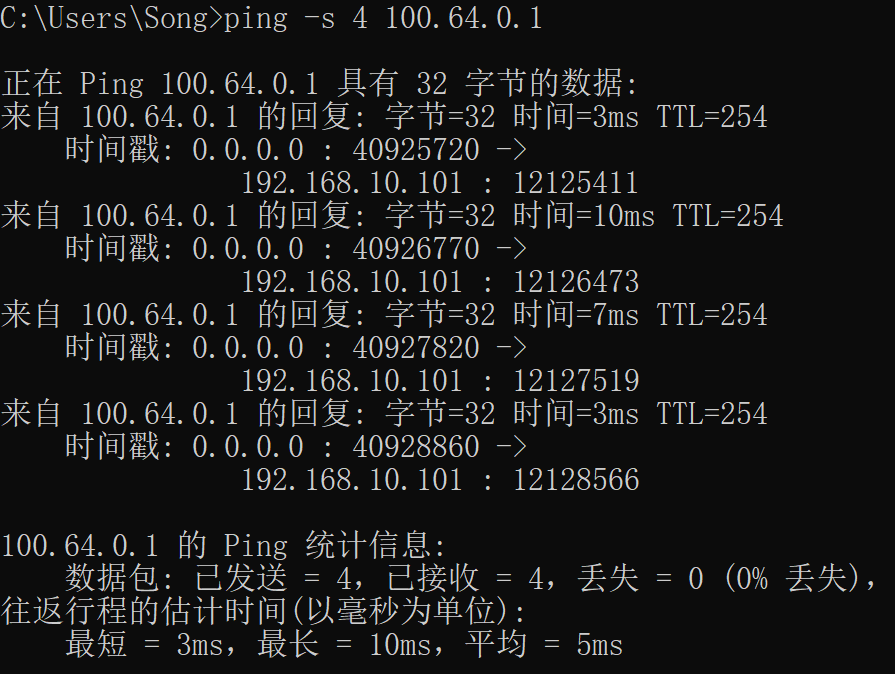
Identifier是什么含义？

icmp Identifier的内容就是ping的进程号，对于windows系统来说，这里代表为Microsoft Windows NT - 256

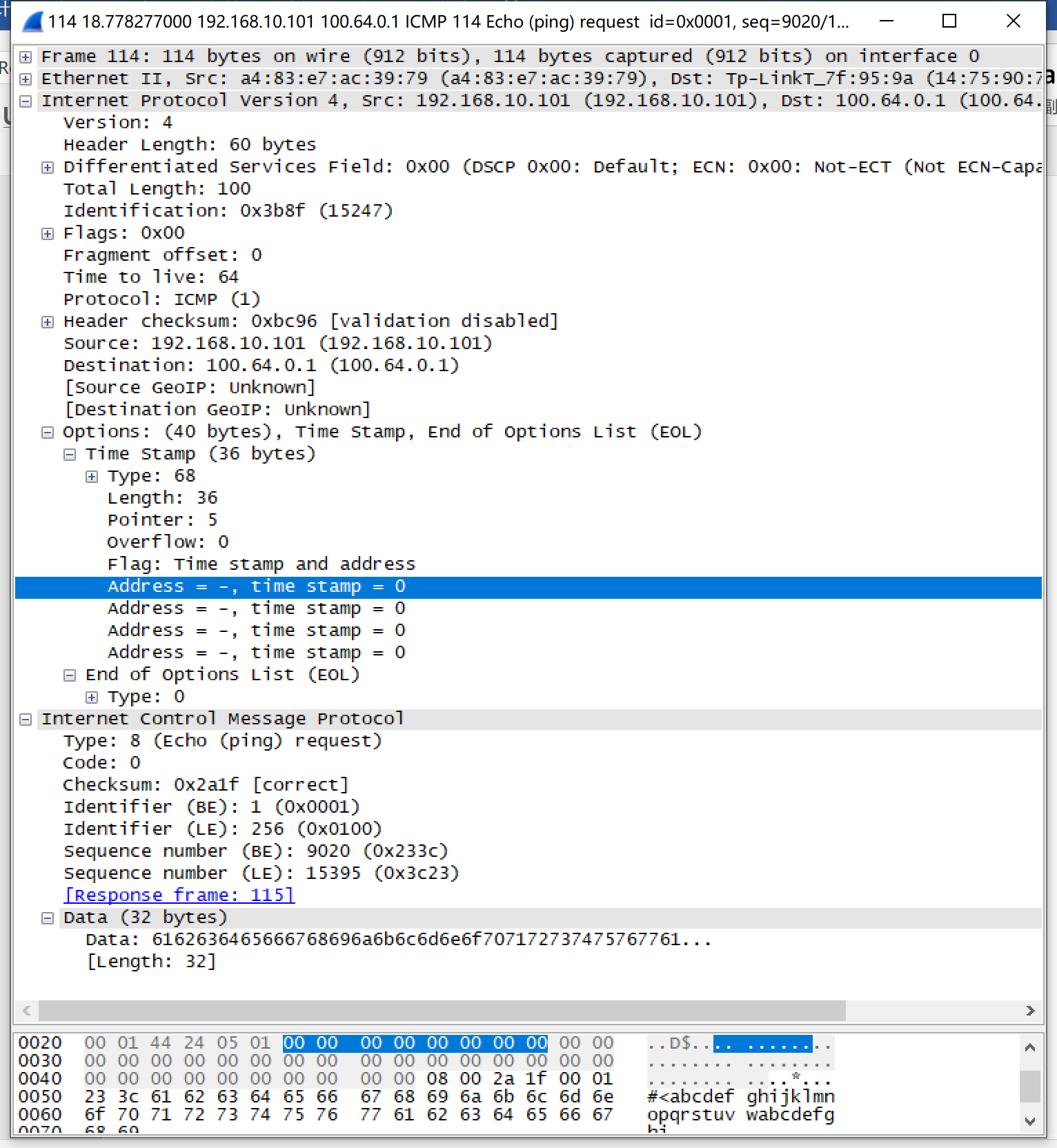
**命令：ping -s 4域名**

[Ping总图] ping -s 4 100.64.0.1

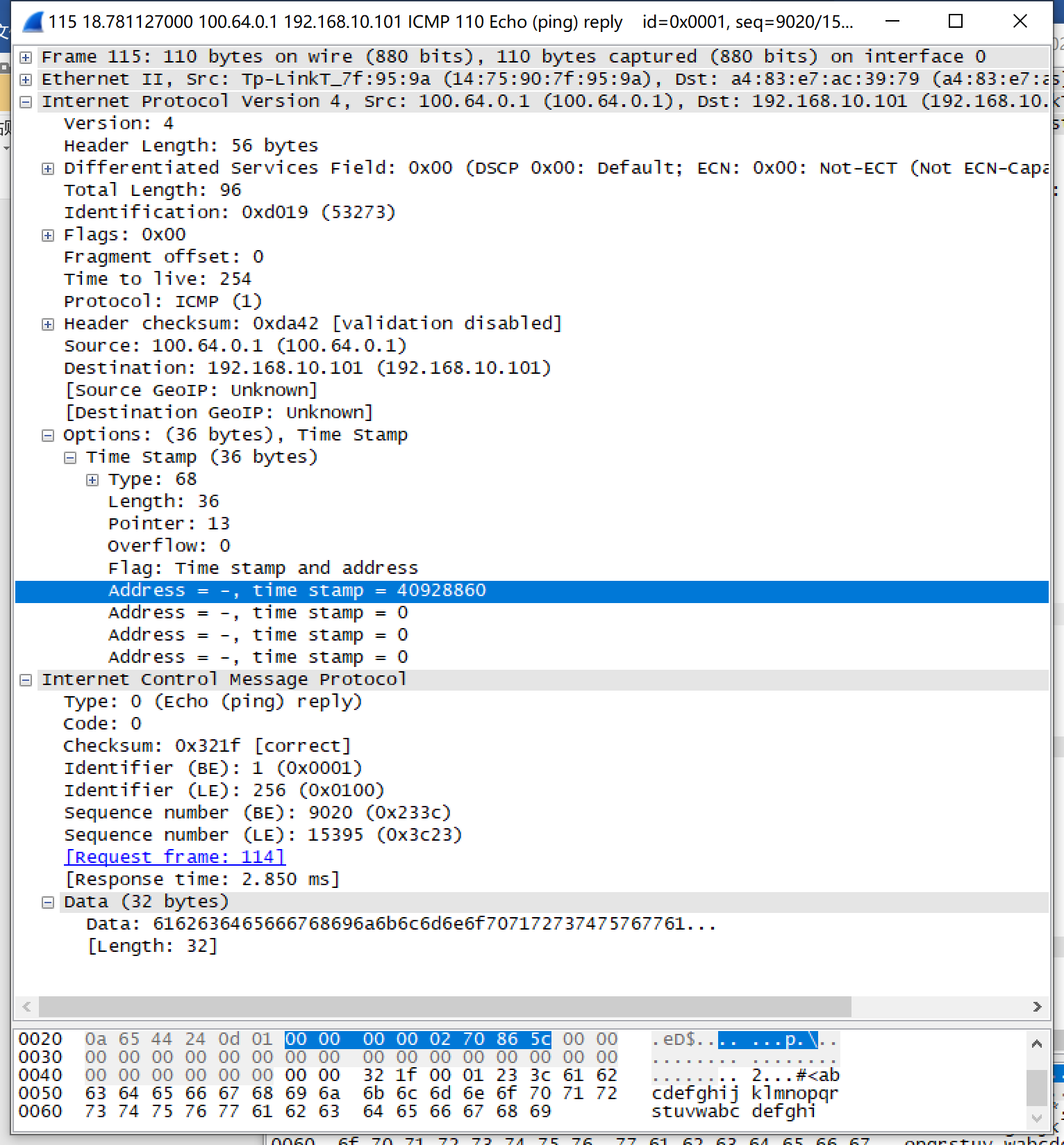




[Ping请求包截屏]



[Ping响应包截屏]



[问题]

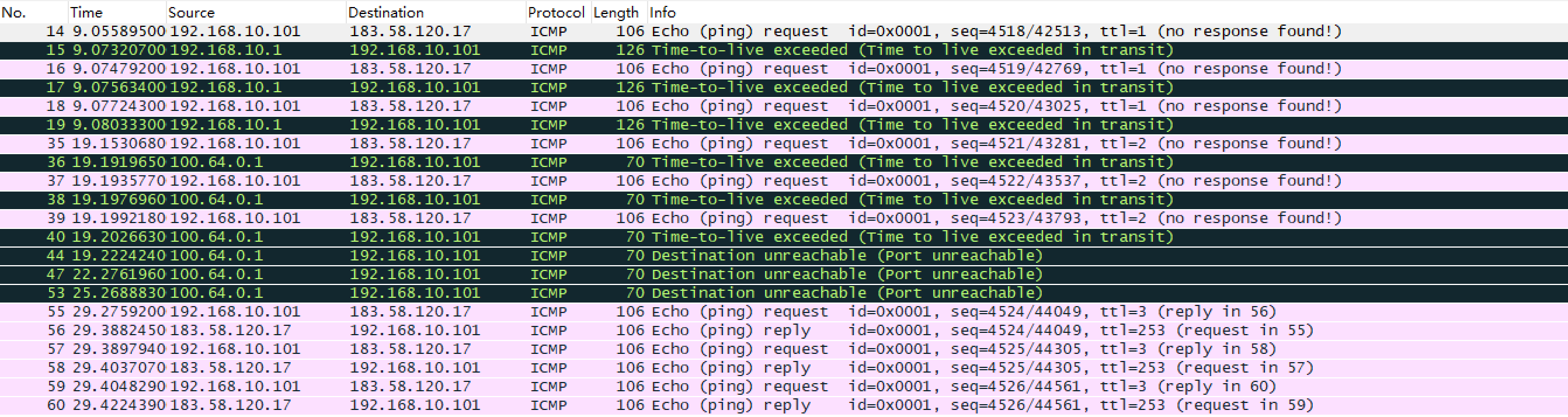
IP选项的长度：请求包为40bytes，响应包为36bytes

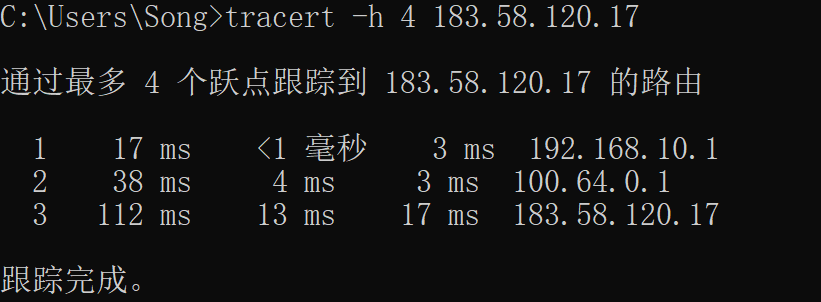
选项中的时间戳是否正确？不完全正确，这个是第4个icmp包，和cmd显示数据不完全一样，少了一个时间戳

1. (tracert.pcapng) ICMP协议

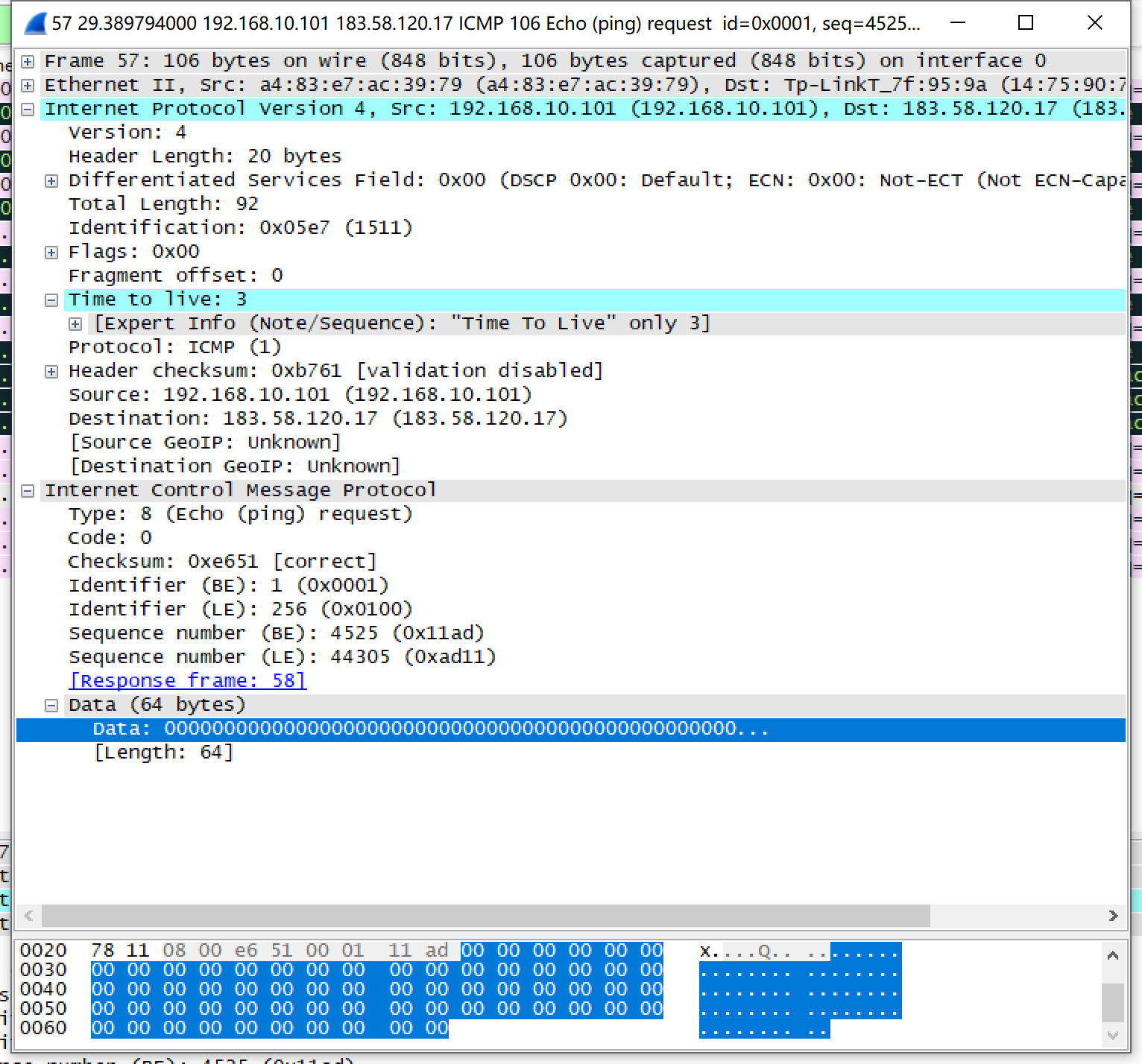
命令：tracert -h 4 域名

[tracert总图截屏] tracert -h 4 183.58.120.17

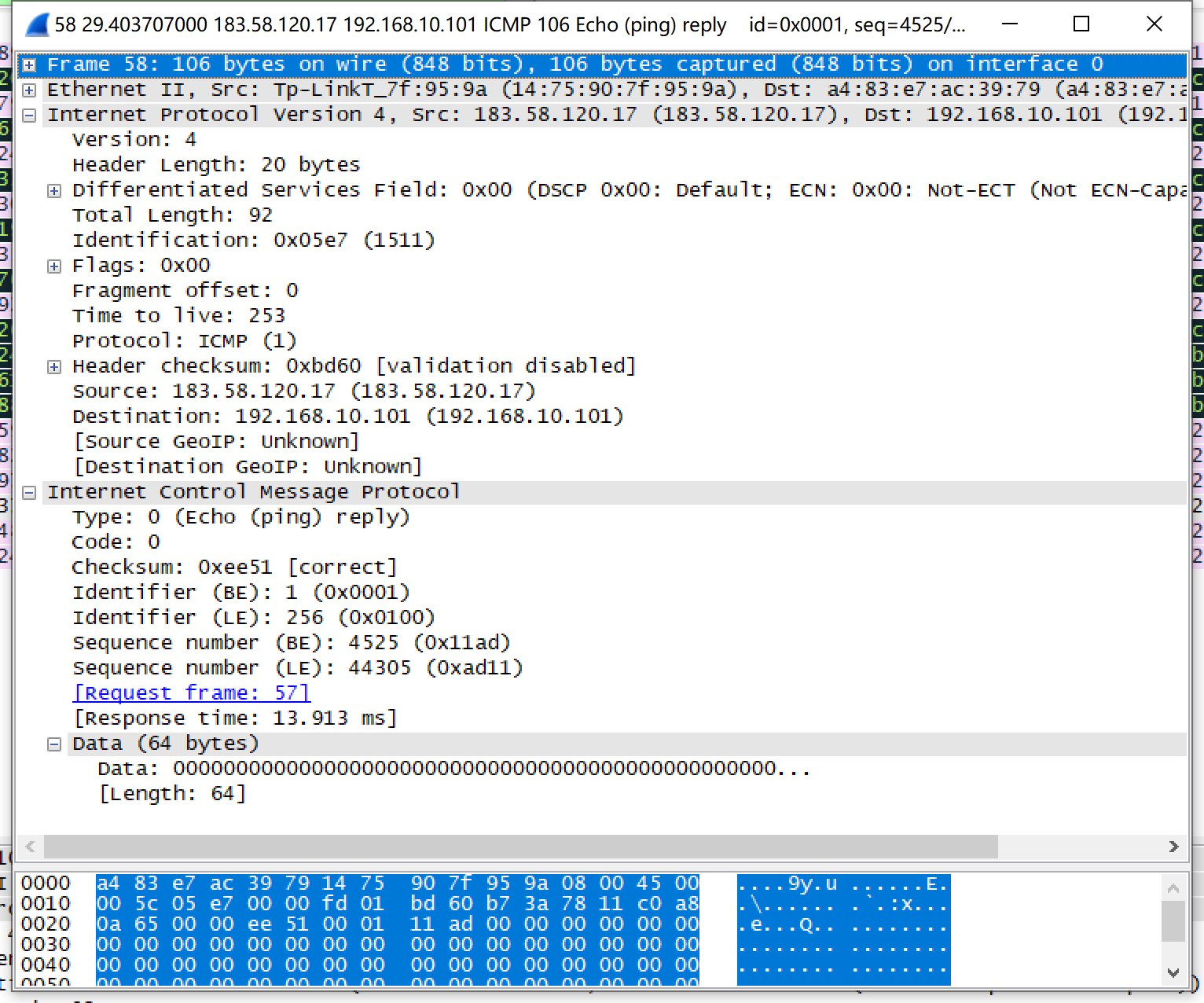




[TTL=3的第二个Ping请求包截屏] \*可以选其他包，但是要修改一下*2和二*



[对应响应包截屏]



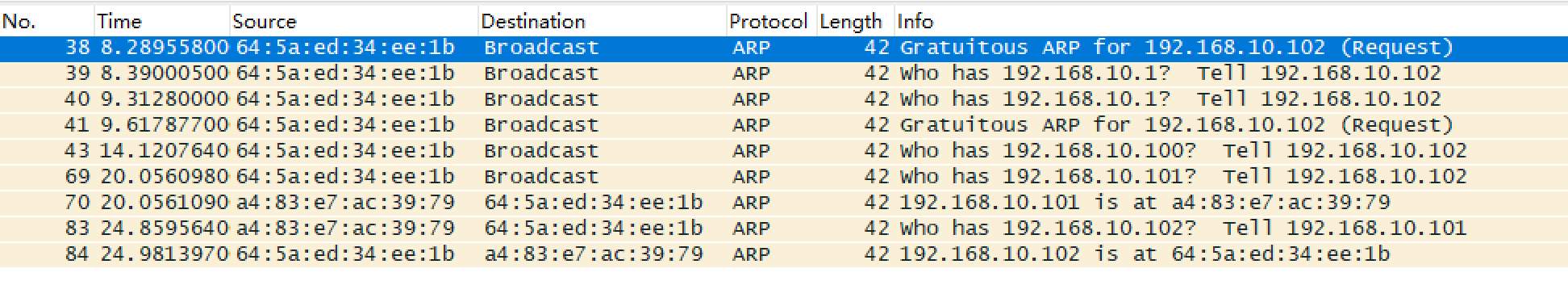
1. (arp.pcapng)ARP协议。

命令：arp –a

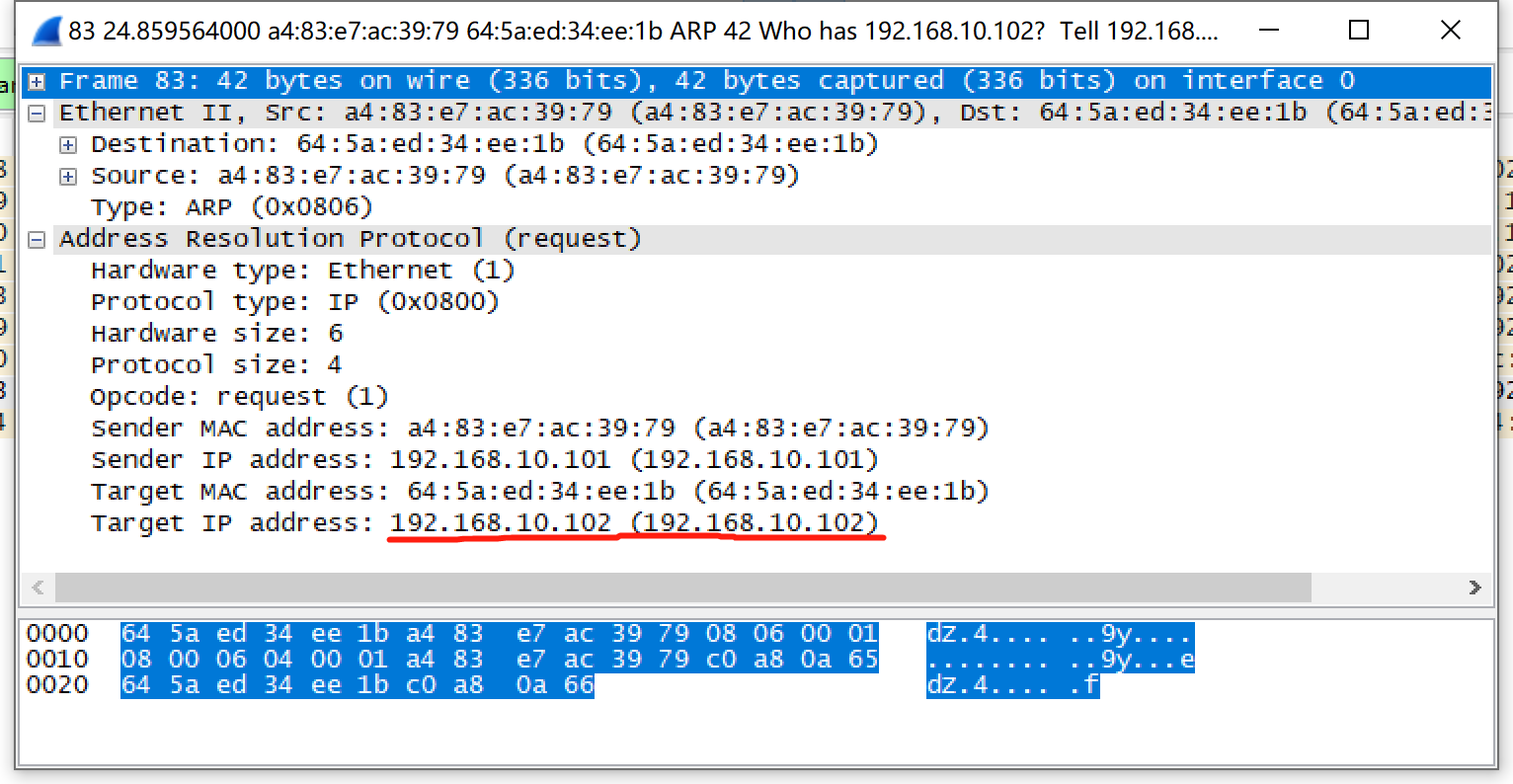
arp –d 192.168.0.14

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

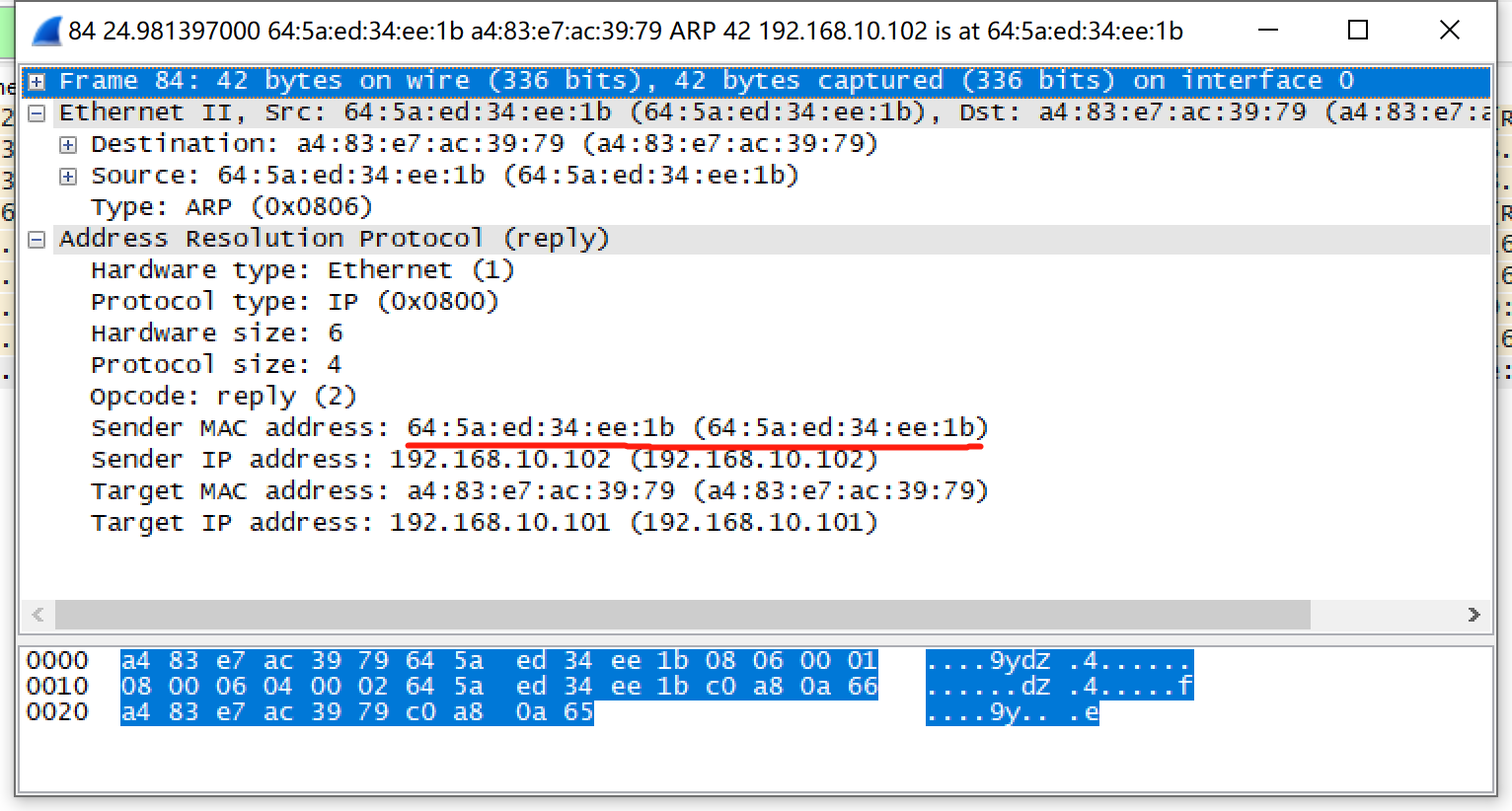
[总图]



[ARP请求包截屏] 用红线标出ARP协议中要查询的IP地址

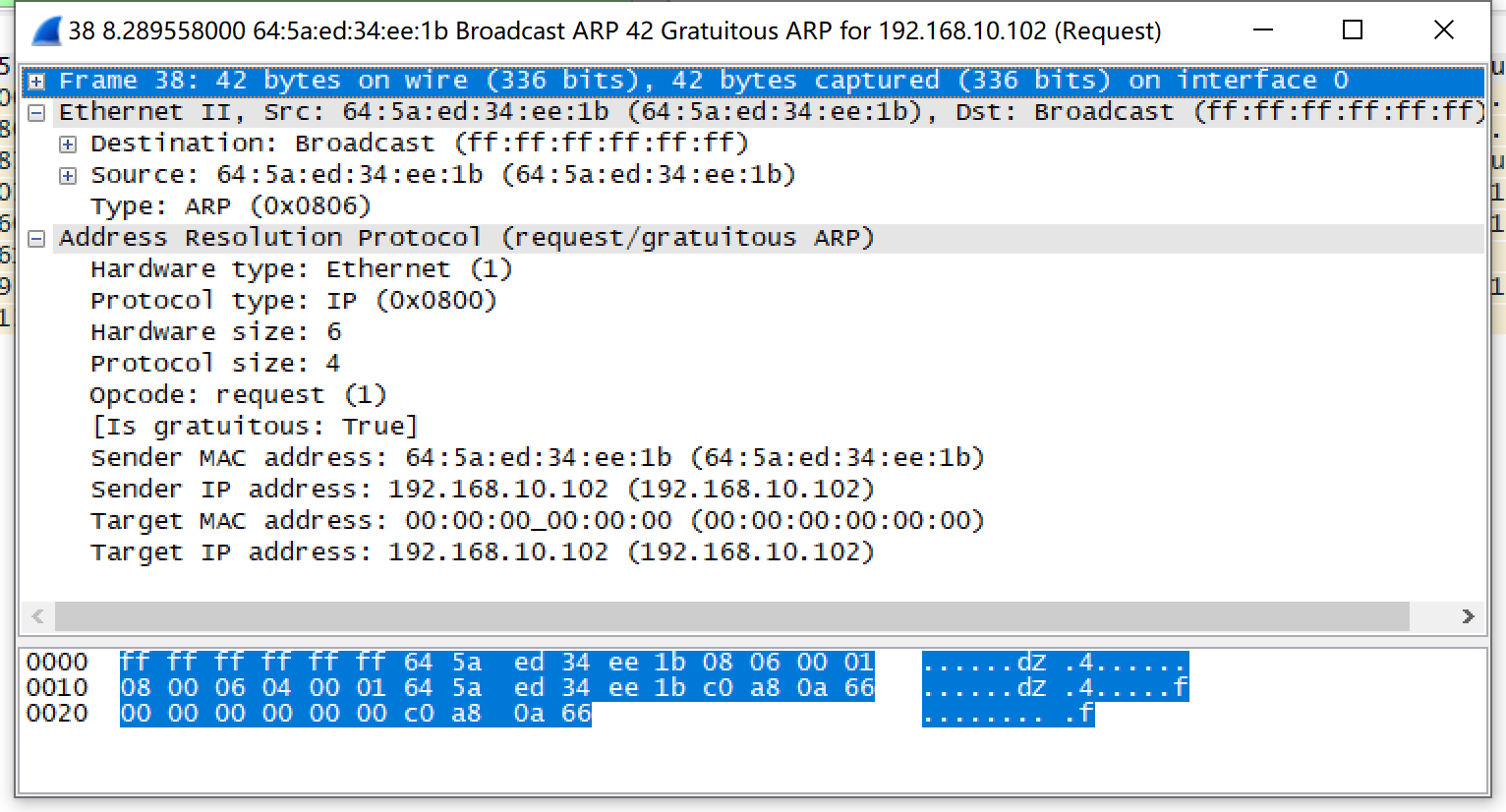


[ARP响应包截屏]用红线标出所查询的IP地址对应的MAC地址



[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]

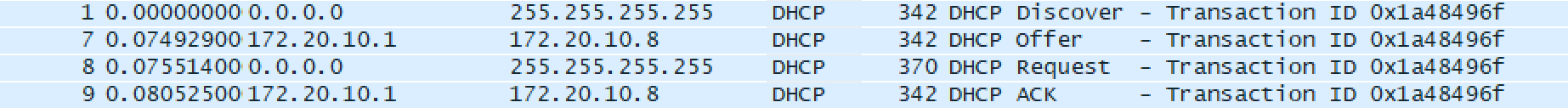
当ARP缓存没有映射时，系统对要发送的IP分组会怎么做？ 进行ARP广播

ARP协议是否采用了超时重传？ ARP无超时重传机制

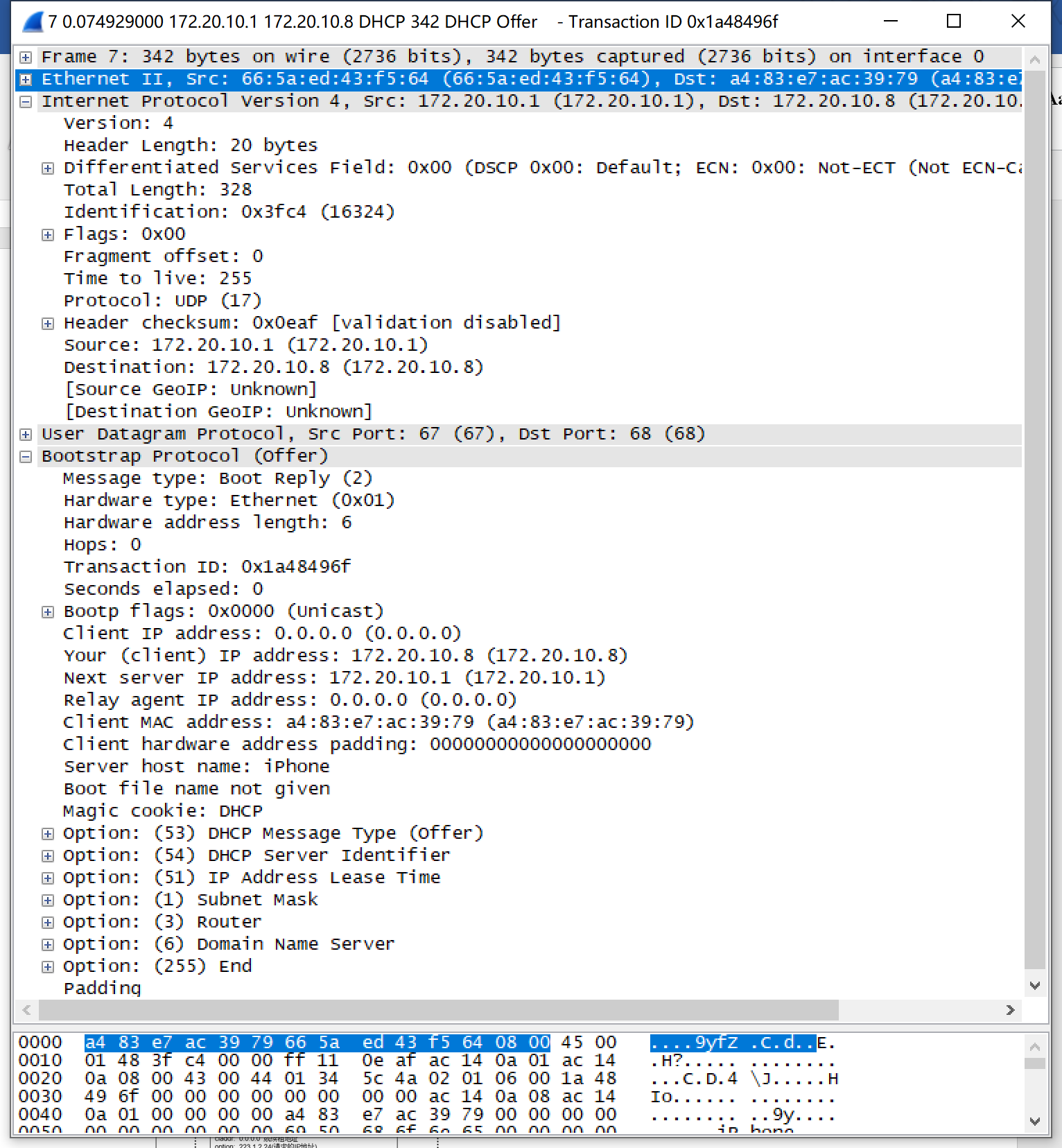
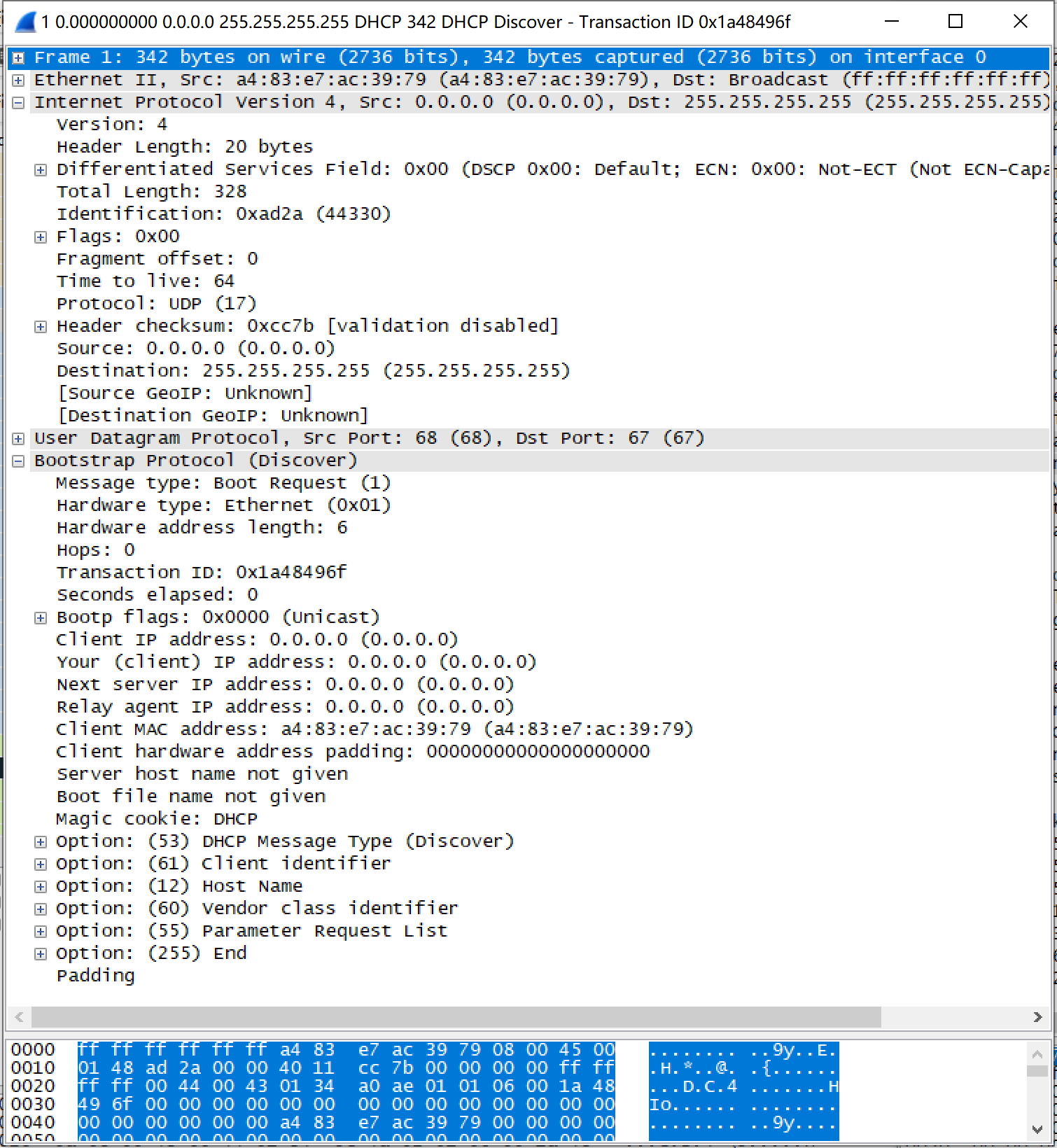
Gratuitous ARP包有什么用途？ 验证ip是否冲突；更新物理网卡时通知其他主机更新ARP缓存

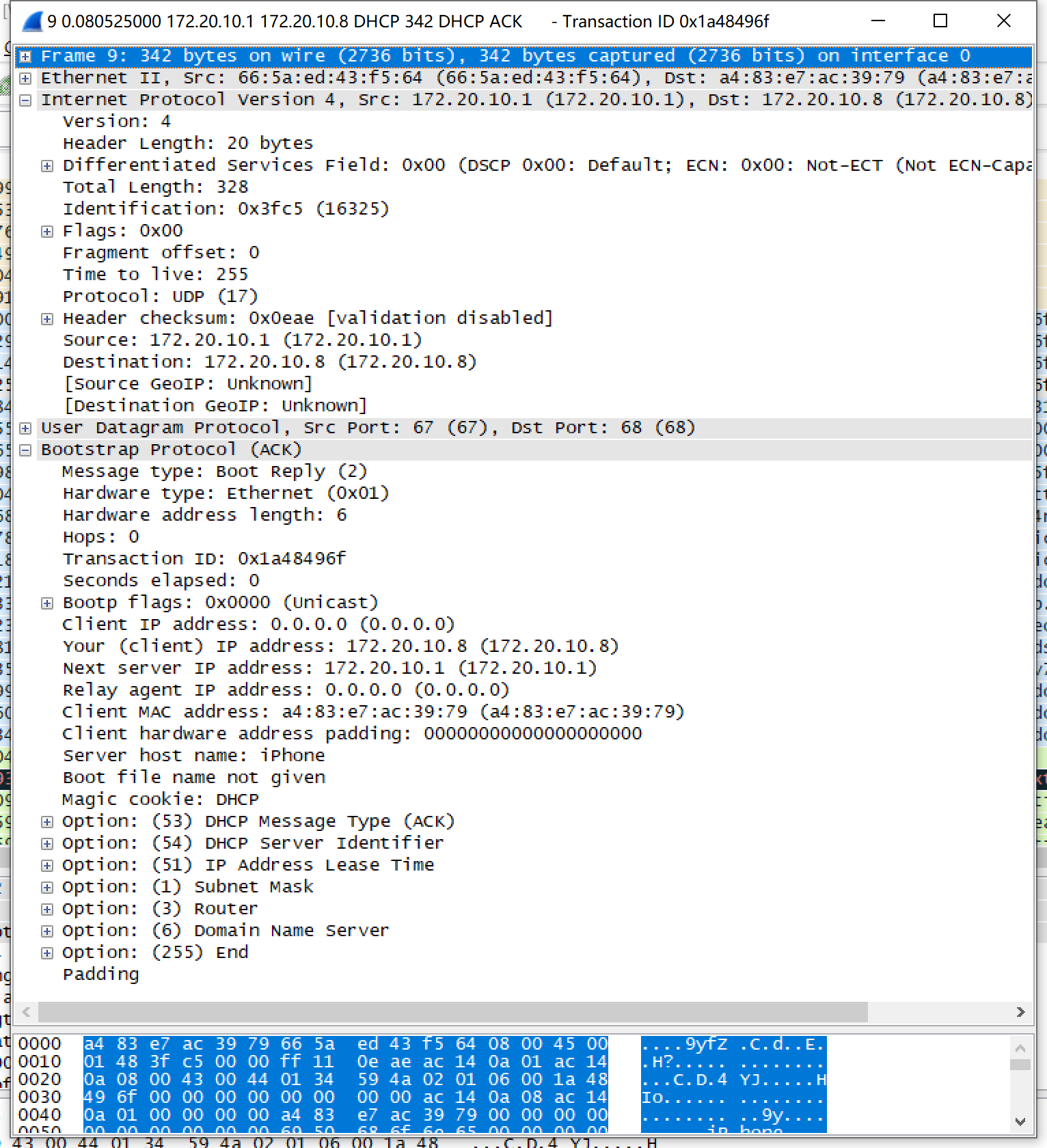
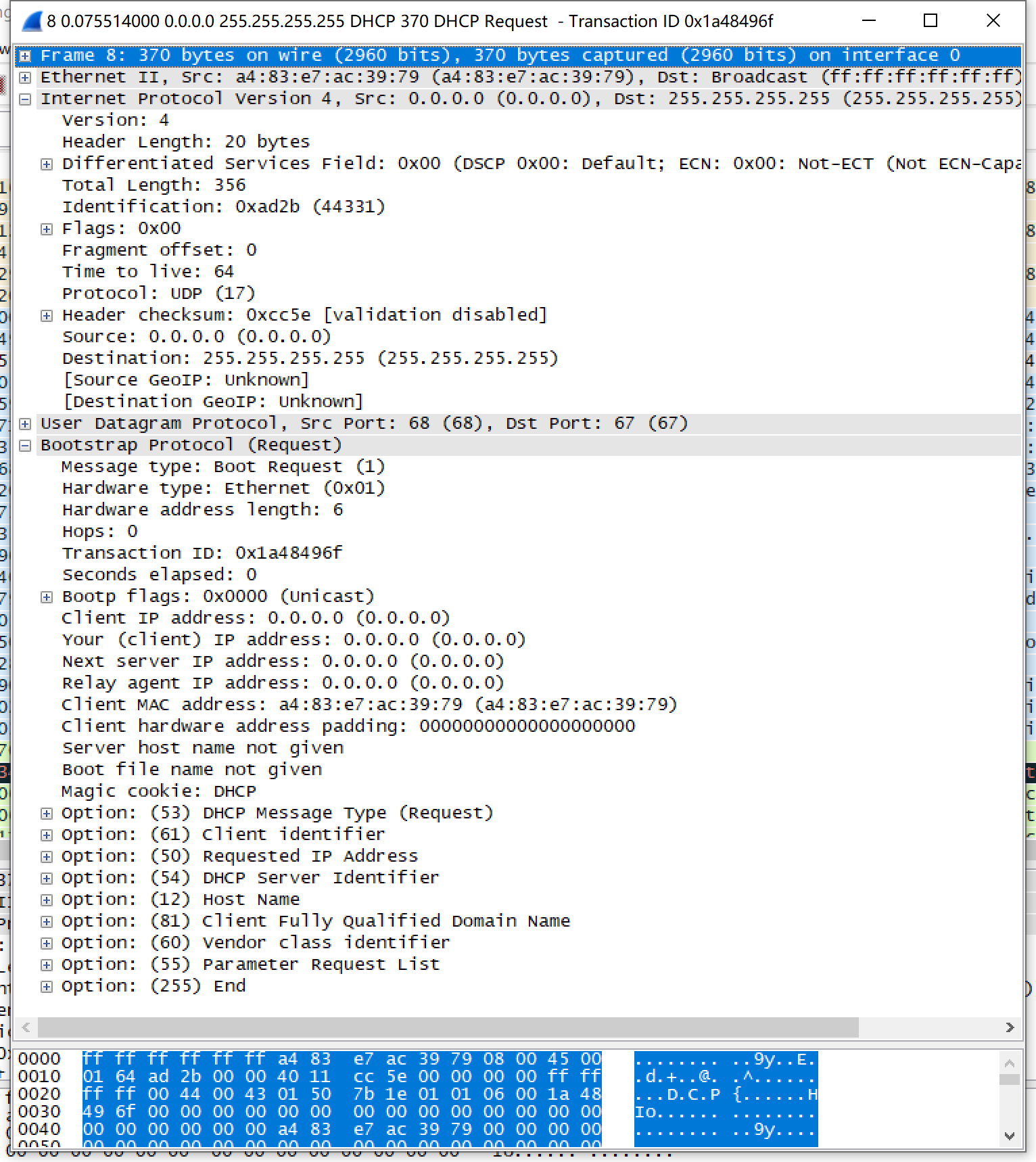
1. (DHCP.pcapng)DHCP协议

[总图]

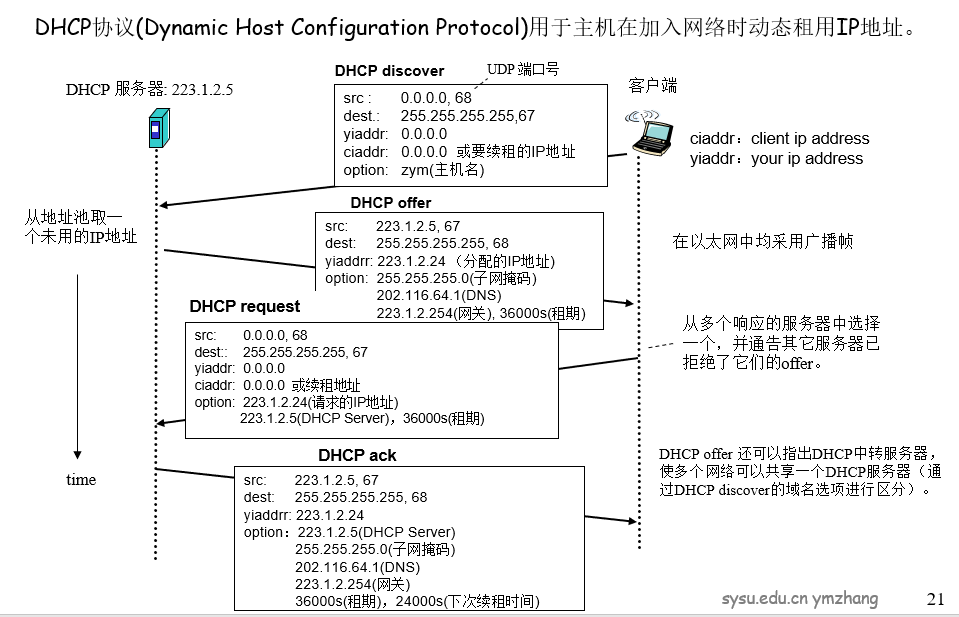


[四个包]





[对照课件]



有没有可以纠正的内容？有的话写出来。

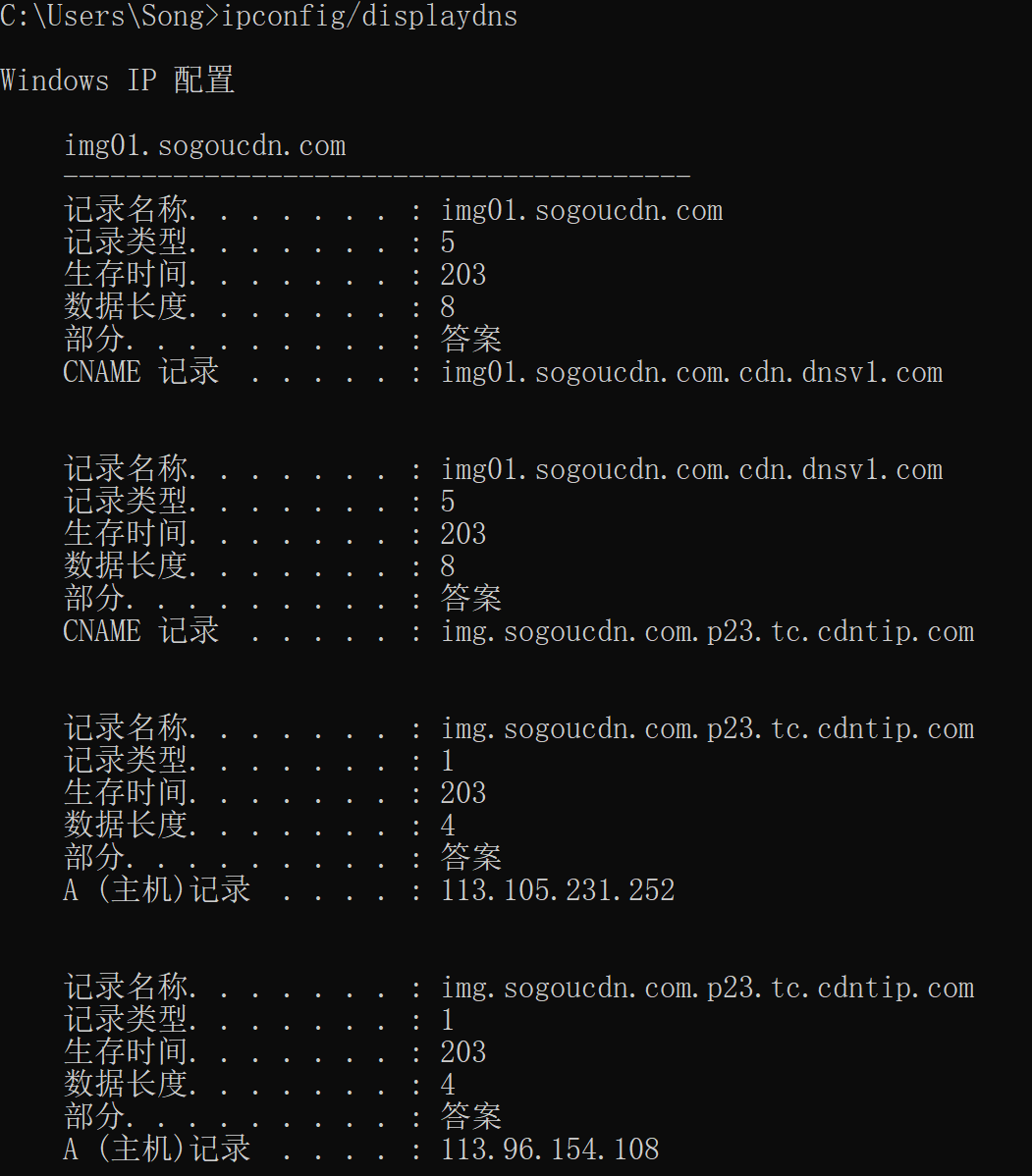
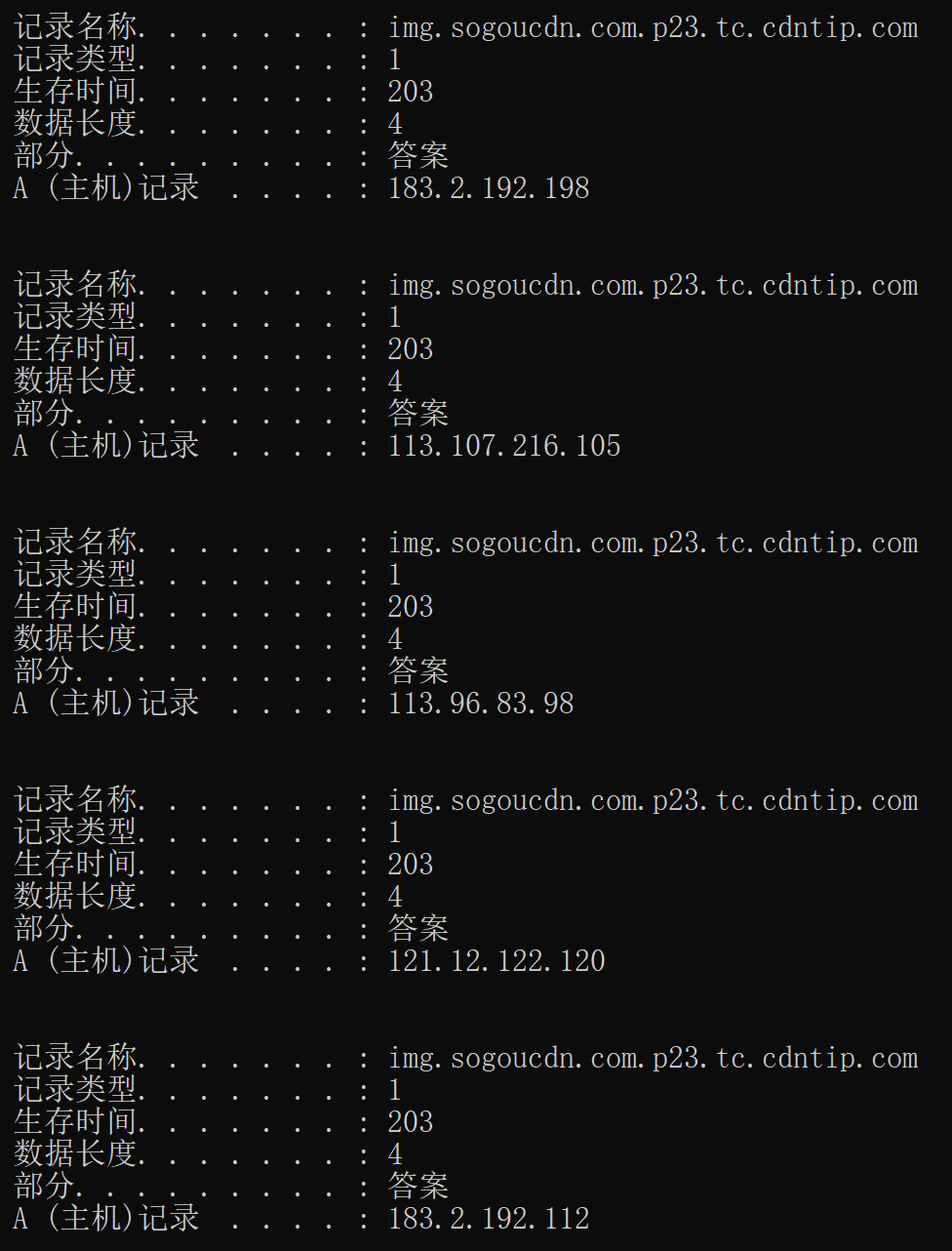
Offer和ack的dest不是255.255.255.255，而好像是分配的ip地址/续租地址

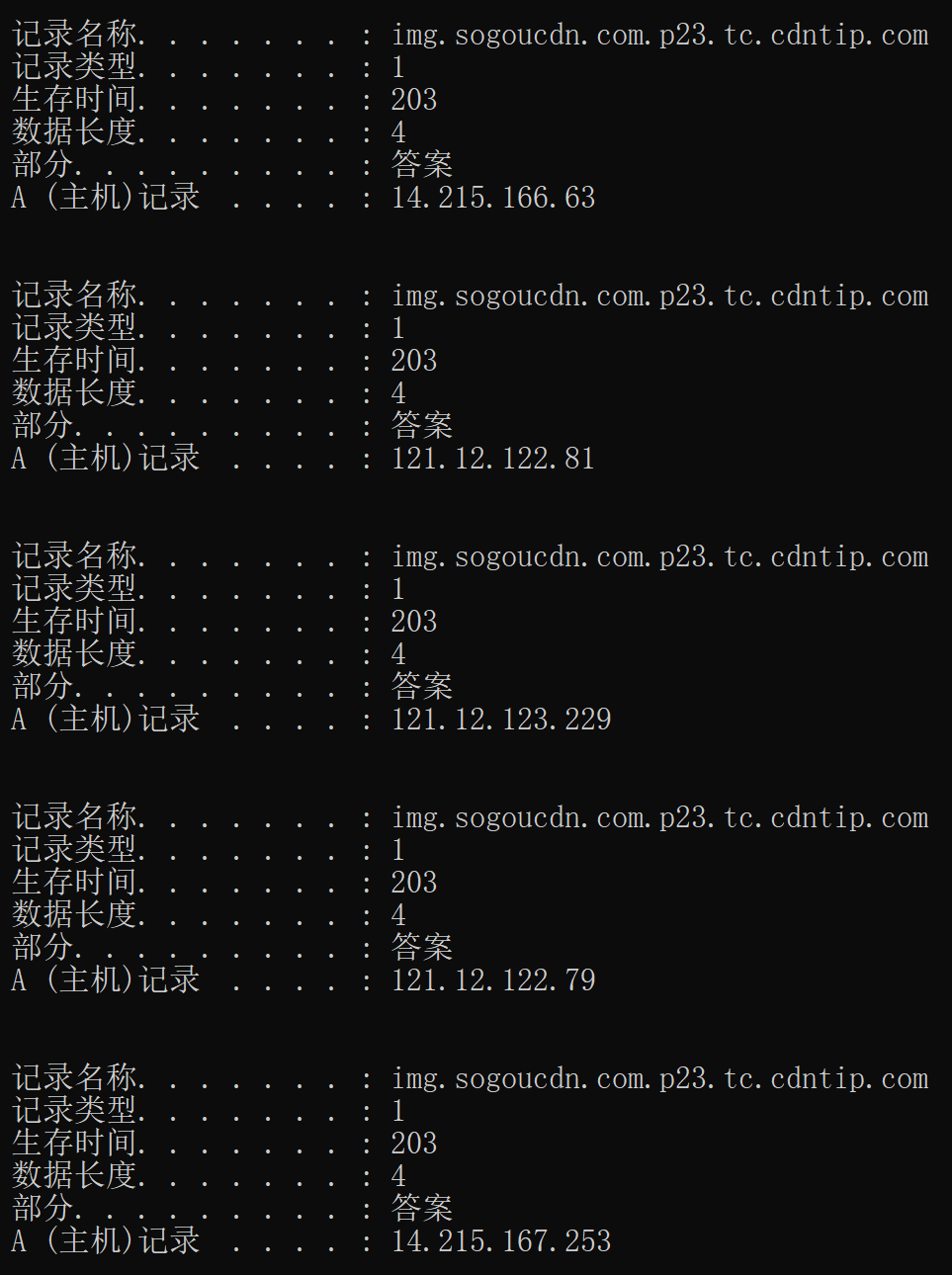
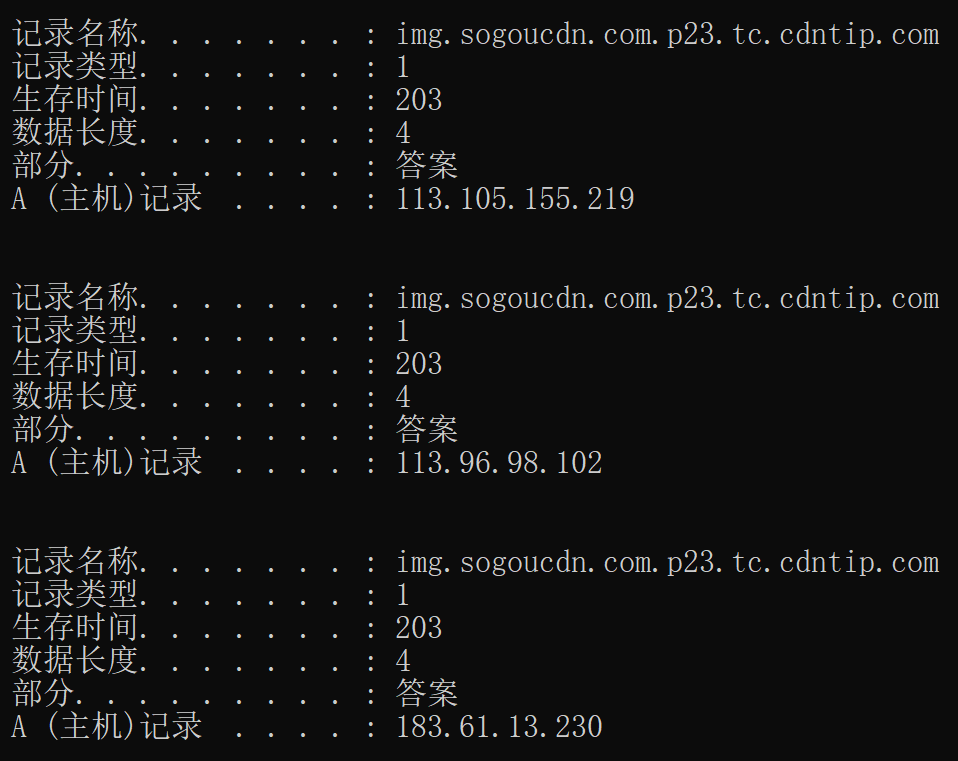
1. (DNS.pcapng)DNS协议

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：

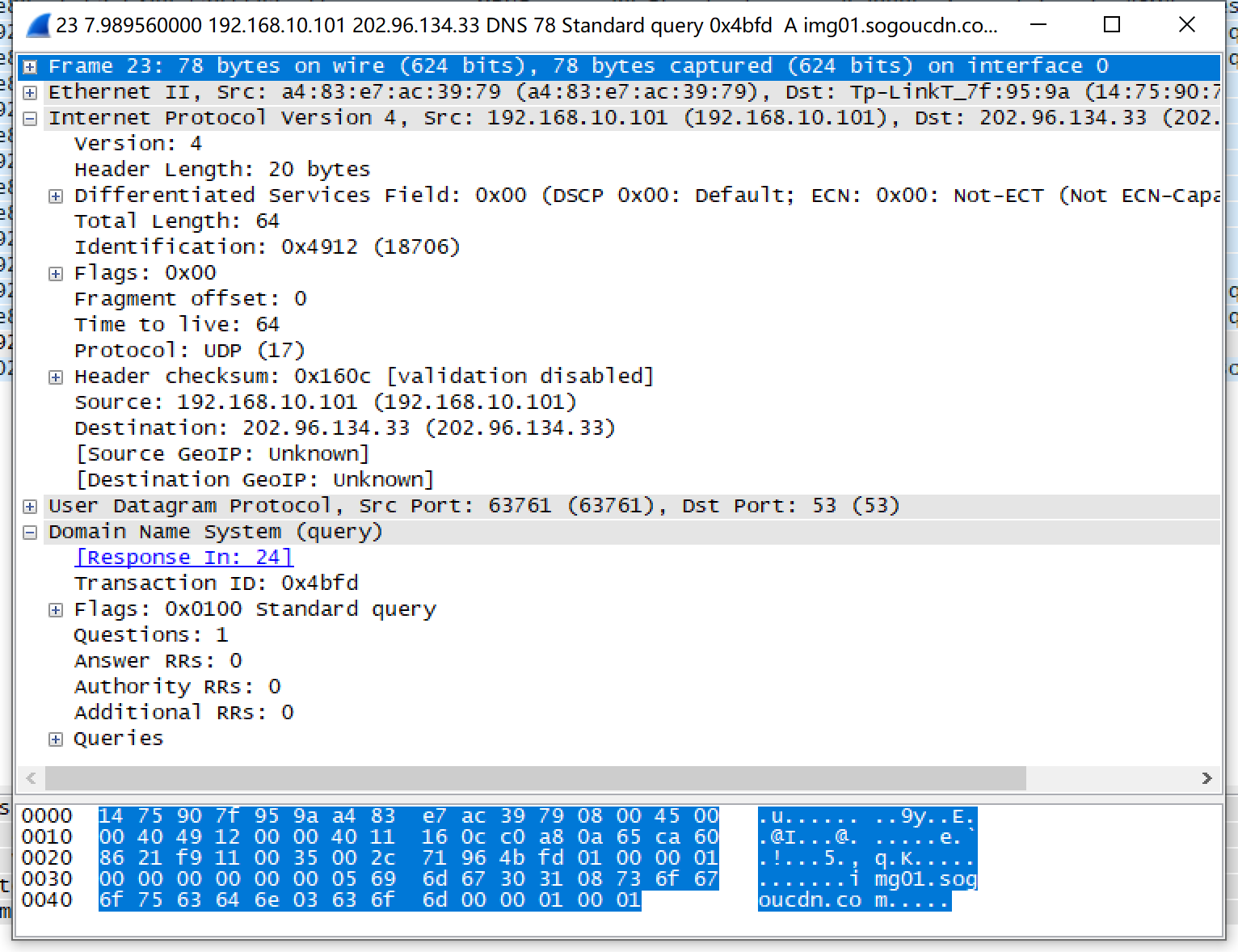
 

解释其中内容（说明如何可以从DNS记录中得到img01.sogoucdn.com的IP地址）：

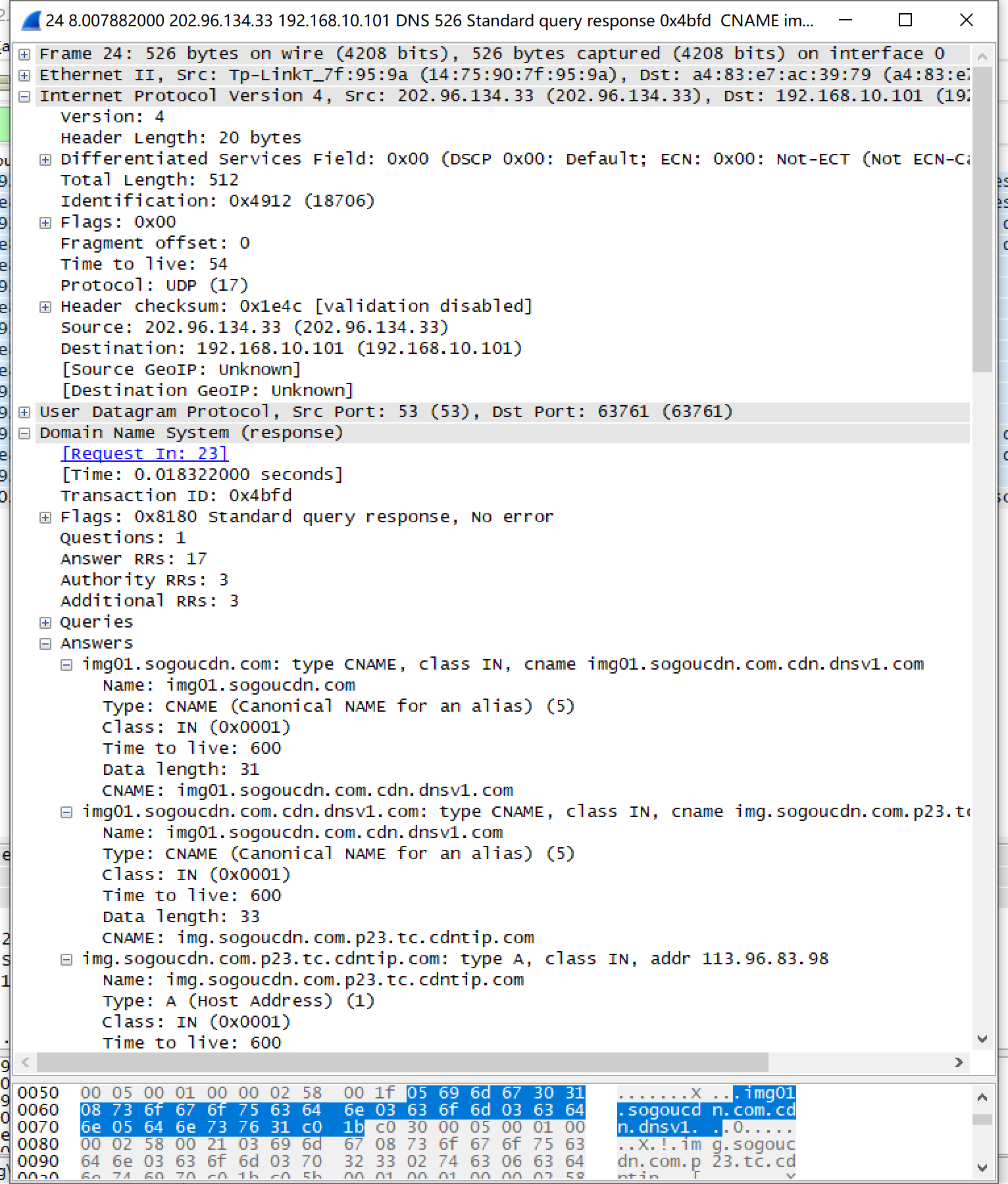
主机会向其域名服务器发出域名解析请求，如果其域名服务器可以解析，则向主机返回解析结果；如果不能解析则将请求转发给更上层的域名服务器知道能够解析为止。

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]Answers过长，只截取一部分



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：

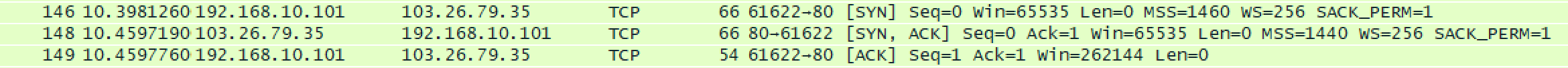
过滤条件：ip.addr==192.168.0.8 and ip.addr==103.26.79.35

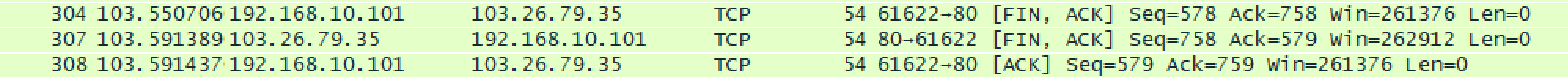
192.168.0.8要用你的电脑的IP地址替换。

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]

主机为：192.168.10.101；客户端为：103.26.79.35

三次握手建立连接：

第一次握手：客户端向主机发送SYN包，以及seq=0；

第二次握手：主机向客户端发送SYN、ACK包，以及seq=0，Ack=1；

第三次握手：客户端向主机发送ACK包，以及Ack=1。

四次挥手关闭连接：

第一次挥手：客户端向主机发送FIN包，以及seq=578；

第二、三次挥手：主机向客户端发送ACK包的同时发送FIN包，Ack=579,seq=758;

第四次挥手：客户端向主机发送ACK包，Ack=759。

【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）。

遇到的问题：

1、步骤一中ping一个地址能ping通，但是加了-r，-s这些参数之后，有些地址就ping不通了，有超时的有主机不可达的

2、步骤三中ping手机的ip地址，需要查看手机的内网地址

3、步骤六中四次挥手需要等一定时间，且这四次之间可能间夹其它TCP的包

解决方法：

1、目前只能通过tracert查询路径之后，ping那些加了-r，-s参数还能ping通的地址来进行实验

2、网上查询资料得，从手机wifi中可以查看手机连上内网之后分配到的ip地址

3、耐心等待，可以通过观察原端口->目的端口来找到四次挥手的包

实验体会：

本次实验复习了许多协议，巩固了许多协议的知识，比如说发包的条件和包的一些具体内容，同时也发现了具体的数据包和课本上的数据有一些不同。

【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）