院 系 数据科学与计算机学院 学号18308045 姓名 谷正阳

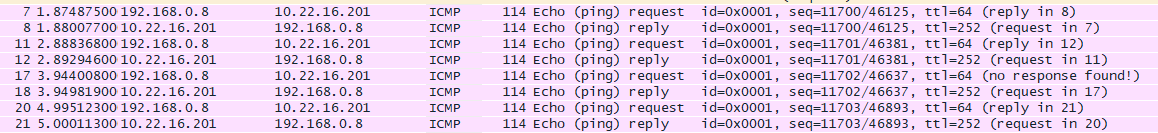
班 级 18

【实验题目】WireShark**实验**

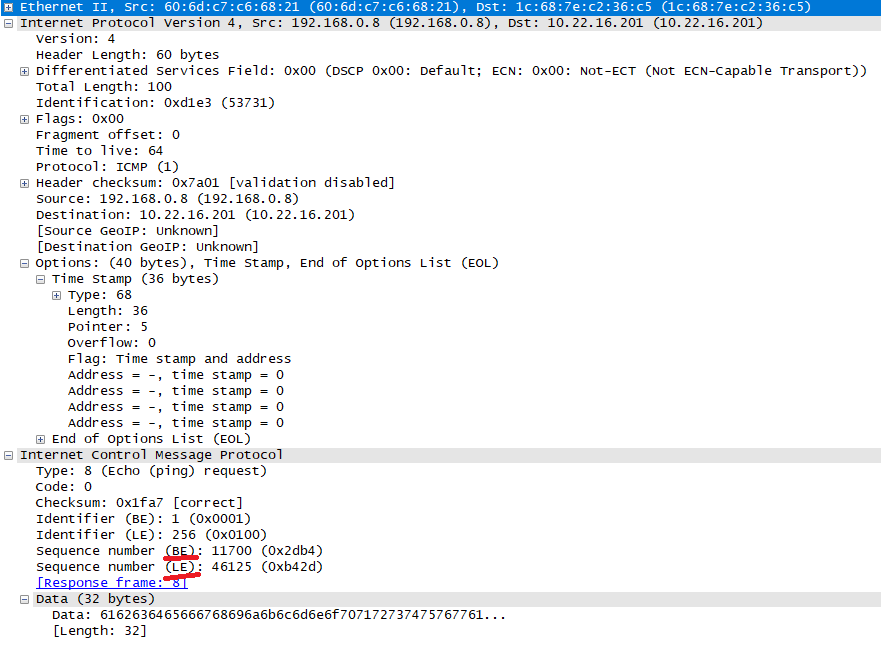
【实验目的】通过WireShark分析IP协议(Option)、ICMP协议、ARP协议、DHCP协议、DNS协议、f协议。

【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）。

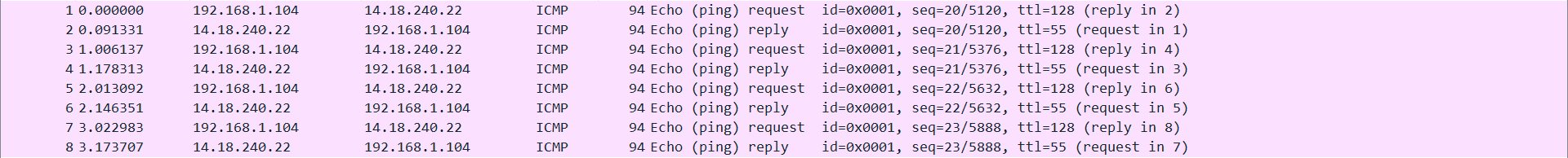
注意每一步都要保存截包文件

【实验任务】

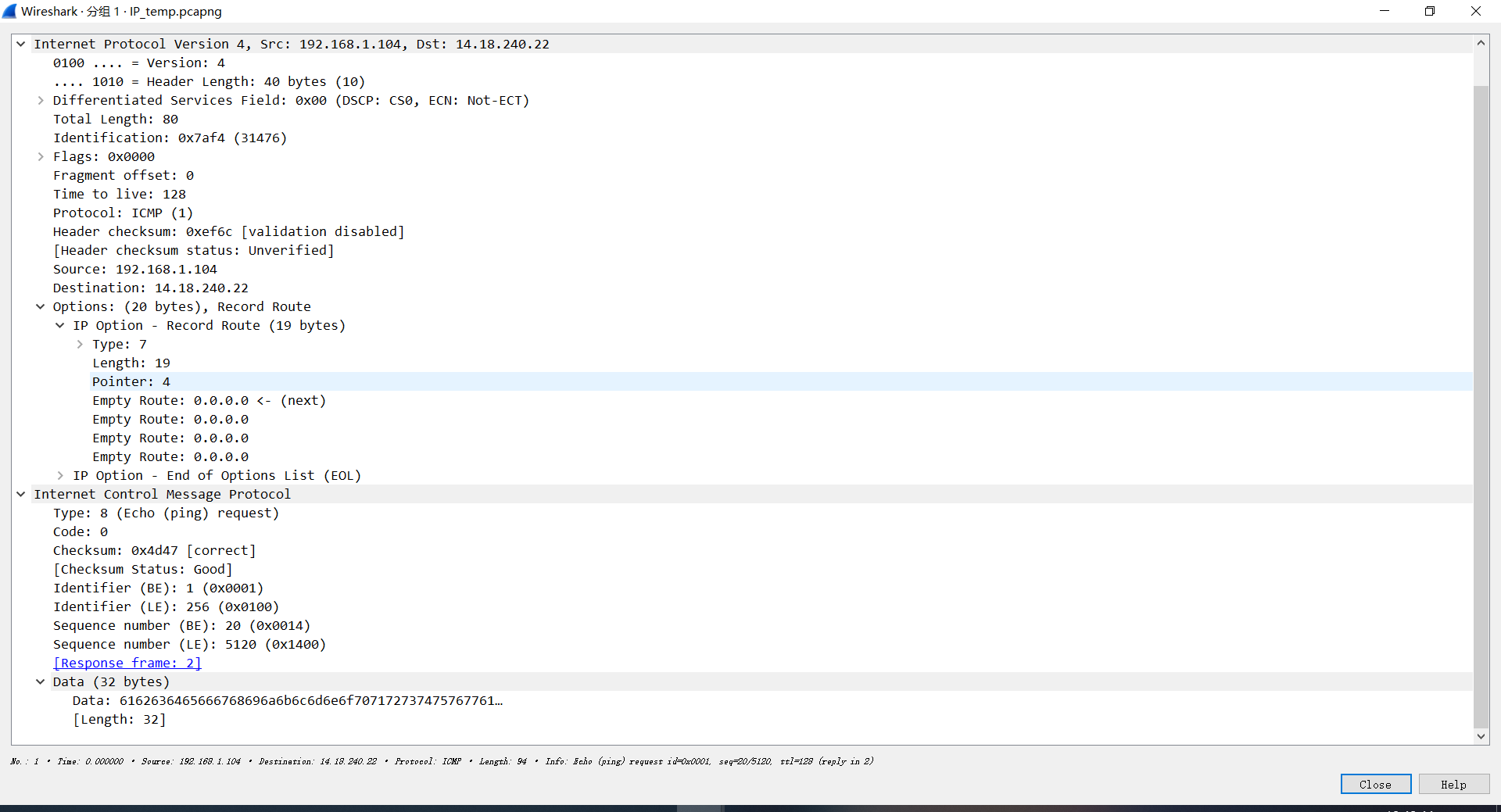
1. (IP.pcapng)IP Option和ICMP协议。

**命令：ping -r 4域名**

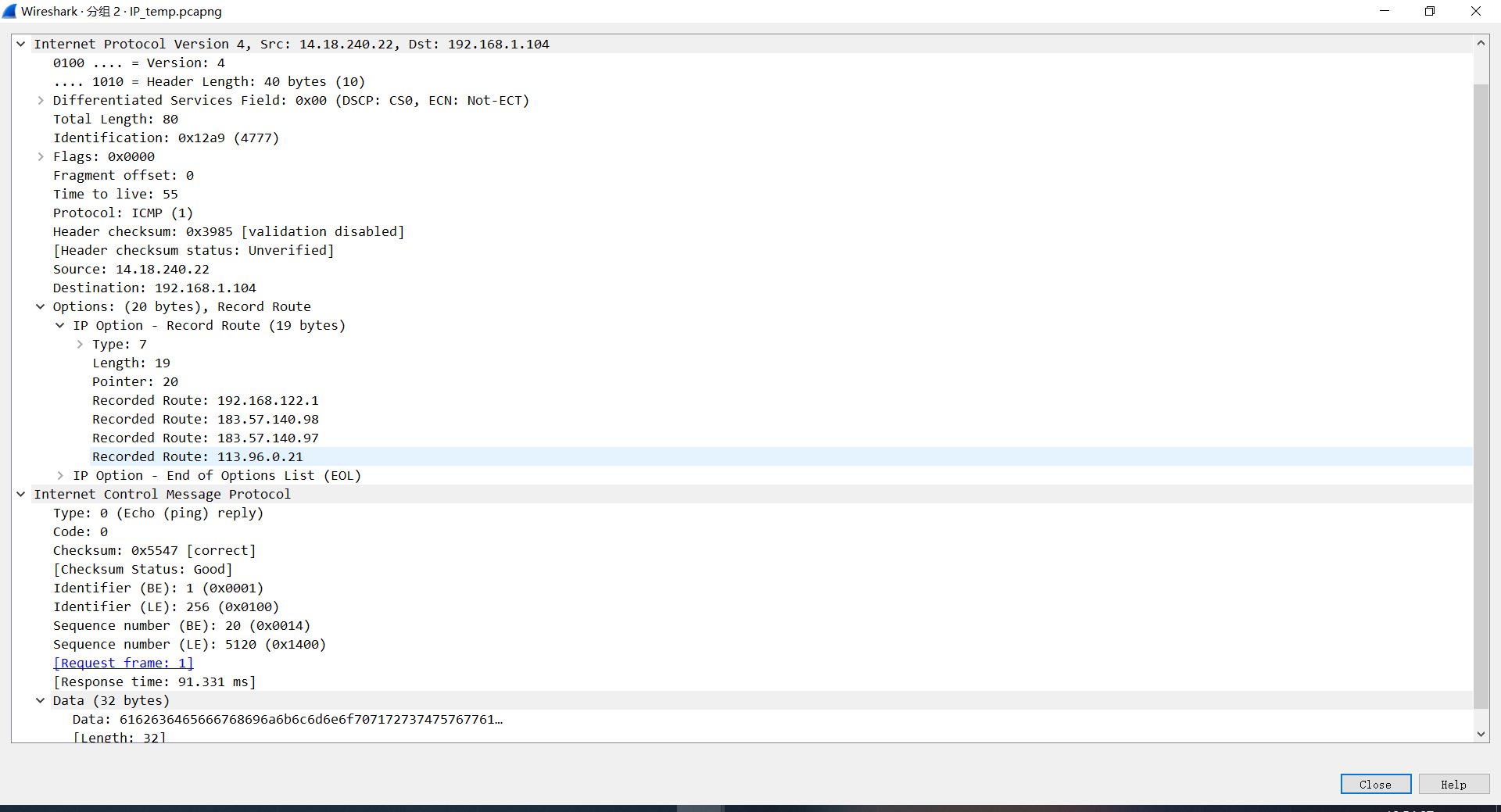
[Ping总图]



[Ping请求包截屏]



[Ping响应包截屏]



[针对于所截包的问题]

IP选项的长度：20 Bytes

ICMP包的Identifier：1

ICMP包的序号：20，20，21，21，22，22，23，23

ICMP包的数据部分长度：32 Bytes

ICMP包的数据部分的内容：

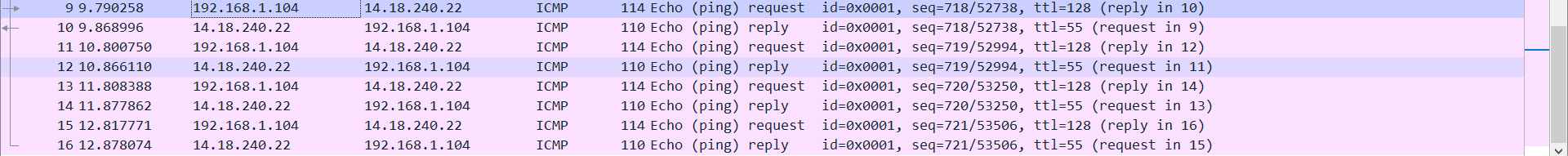
6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

Identifier是什么含义？

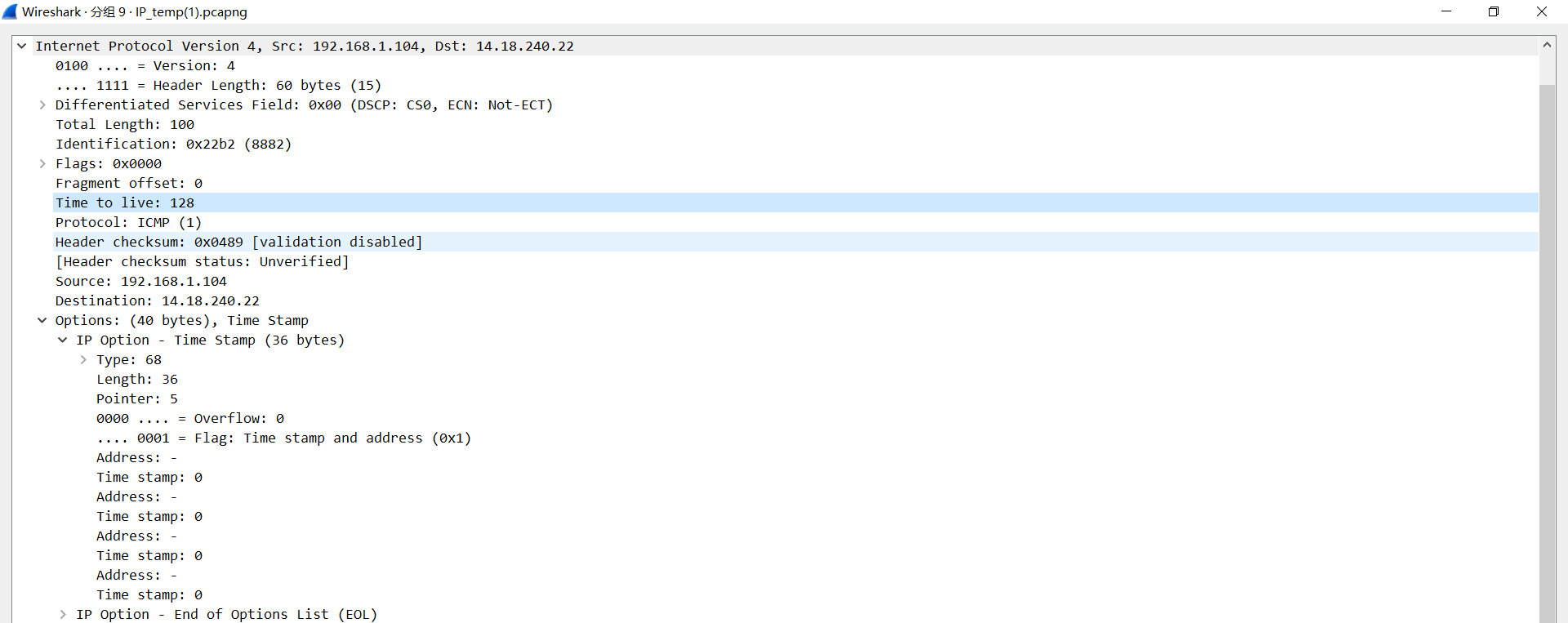
和序号一同用于区分不同的响应，如把进程号记录为标识符，并记录发送序号

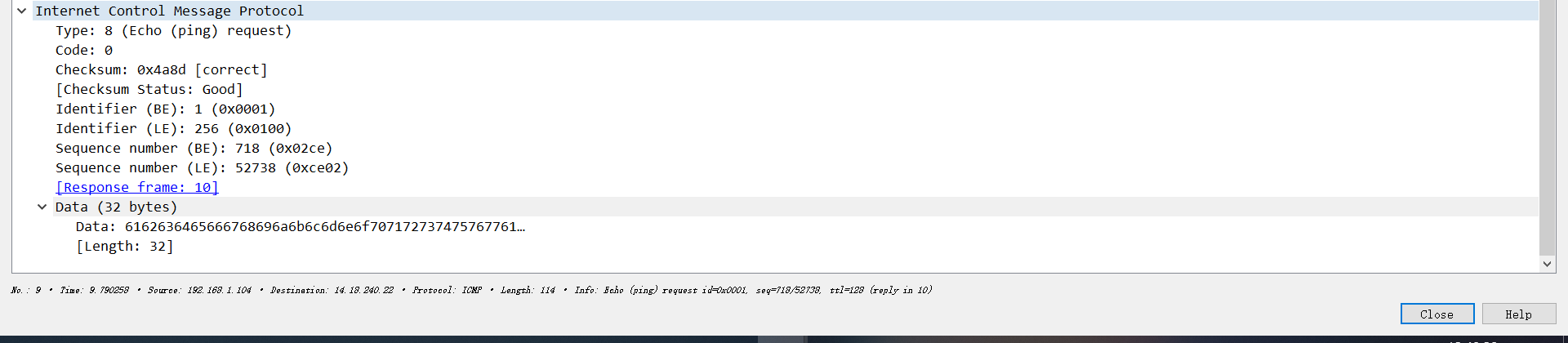
**命令：ping -s 4域名**

[Ping总图]

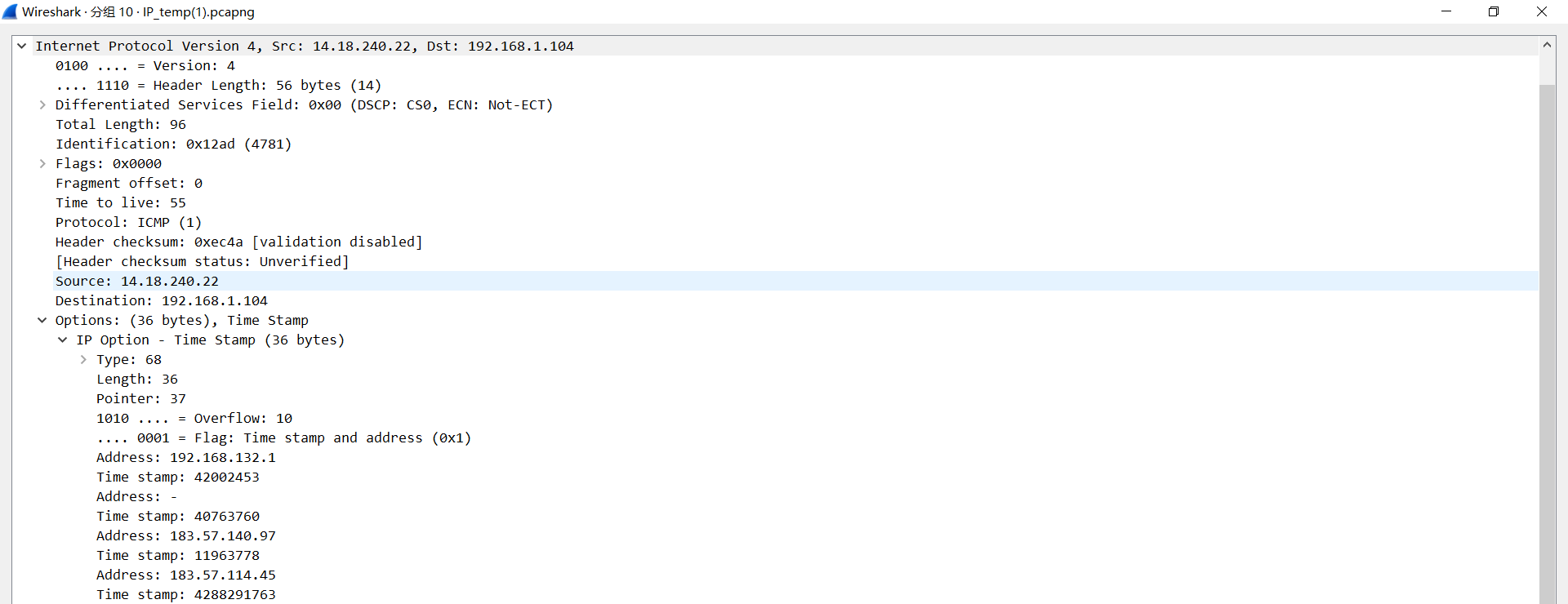


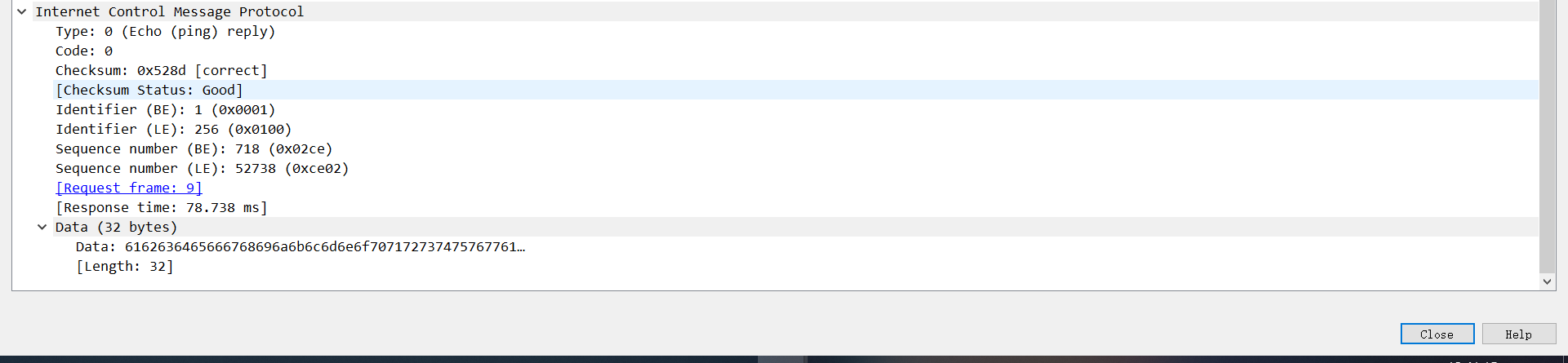
[Ping请求包截屏]





[Ping响应包截屏]





[问题]

IP选项的长度：40 Bytes，36 Bytes，40 Bytes，36 Bytes，40 Bytes，36 Bytes，40 Bytes，36 Bytes。

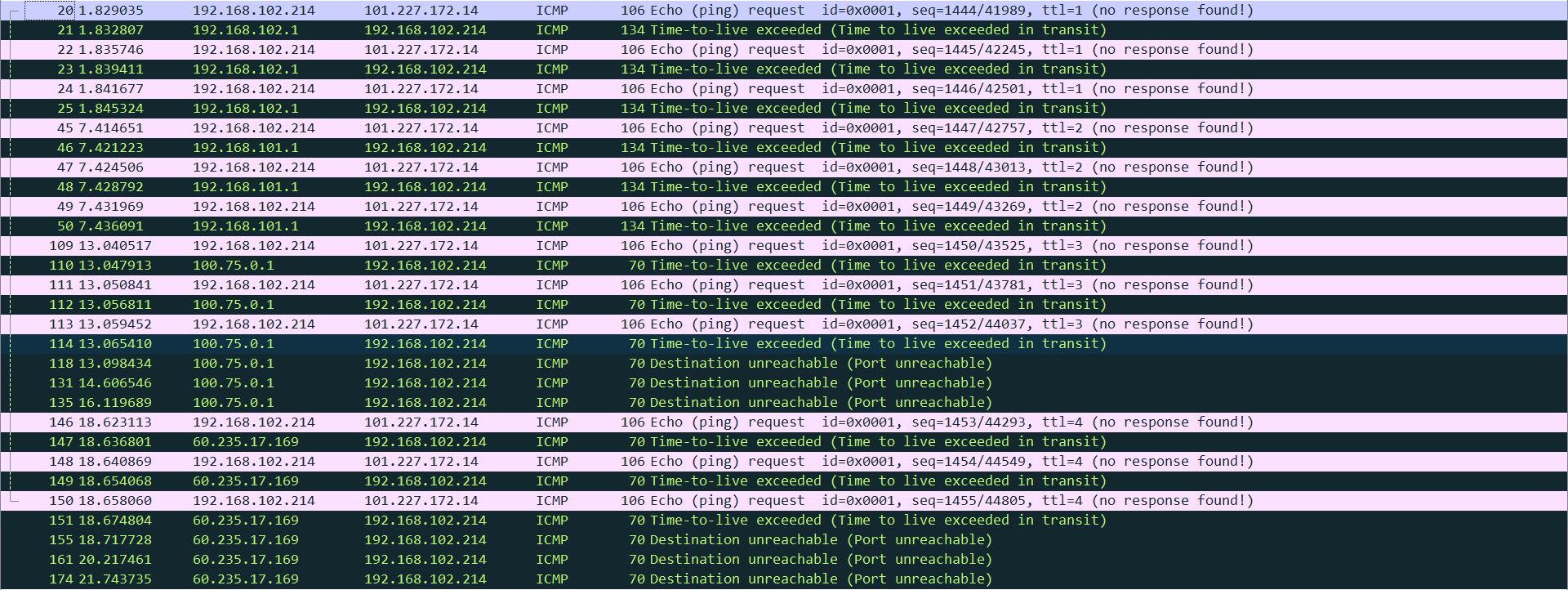
选项中的时间戳是否正确？

正确。

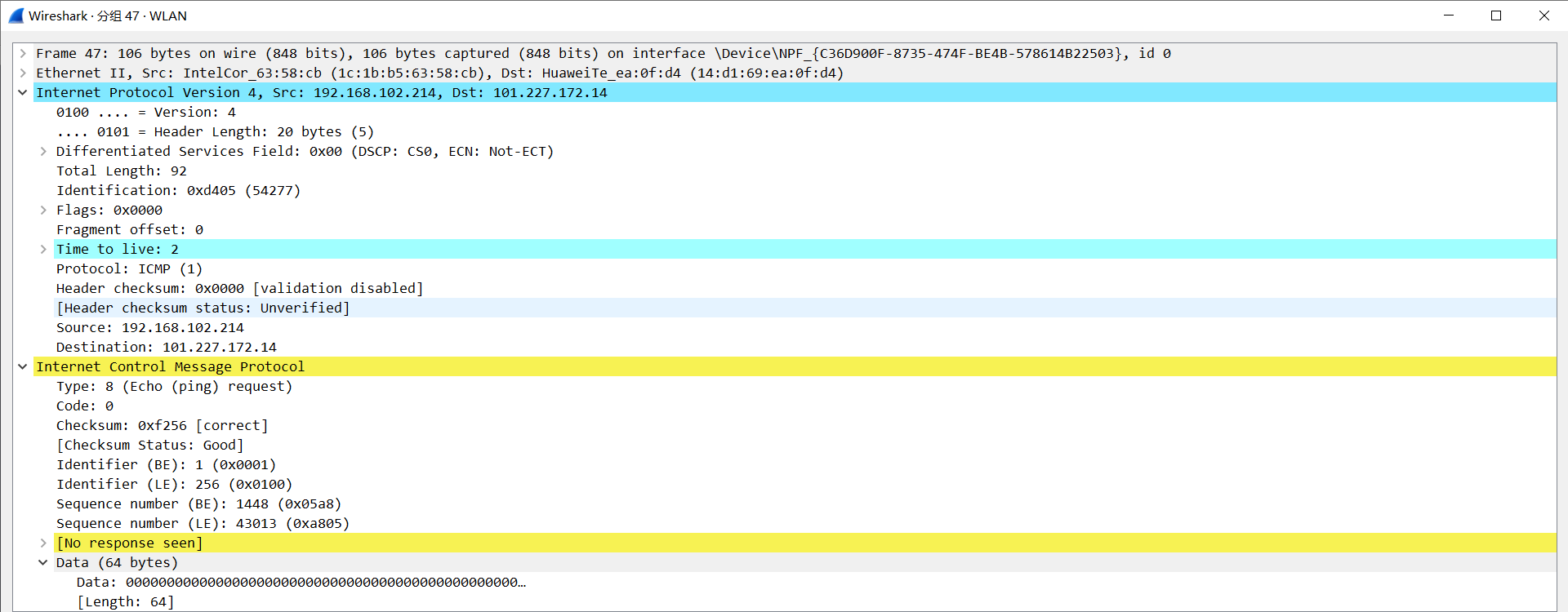
1. (tracert.pcapng) ICMP协议

命令：tracert -h 4 域名

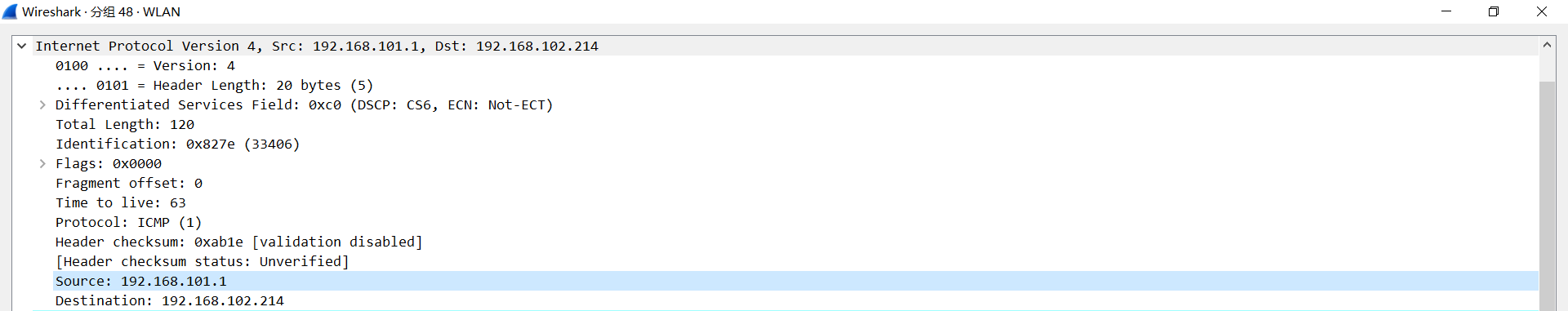
[tracert总图截屏]

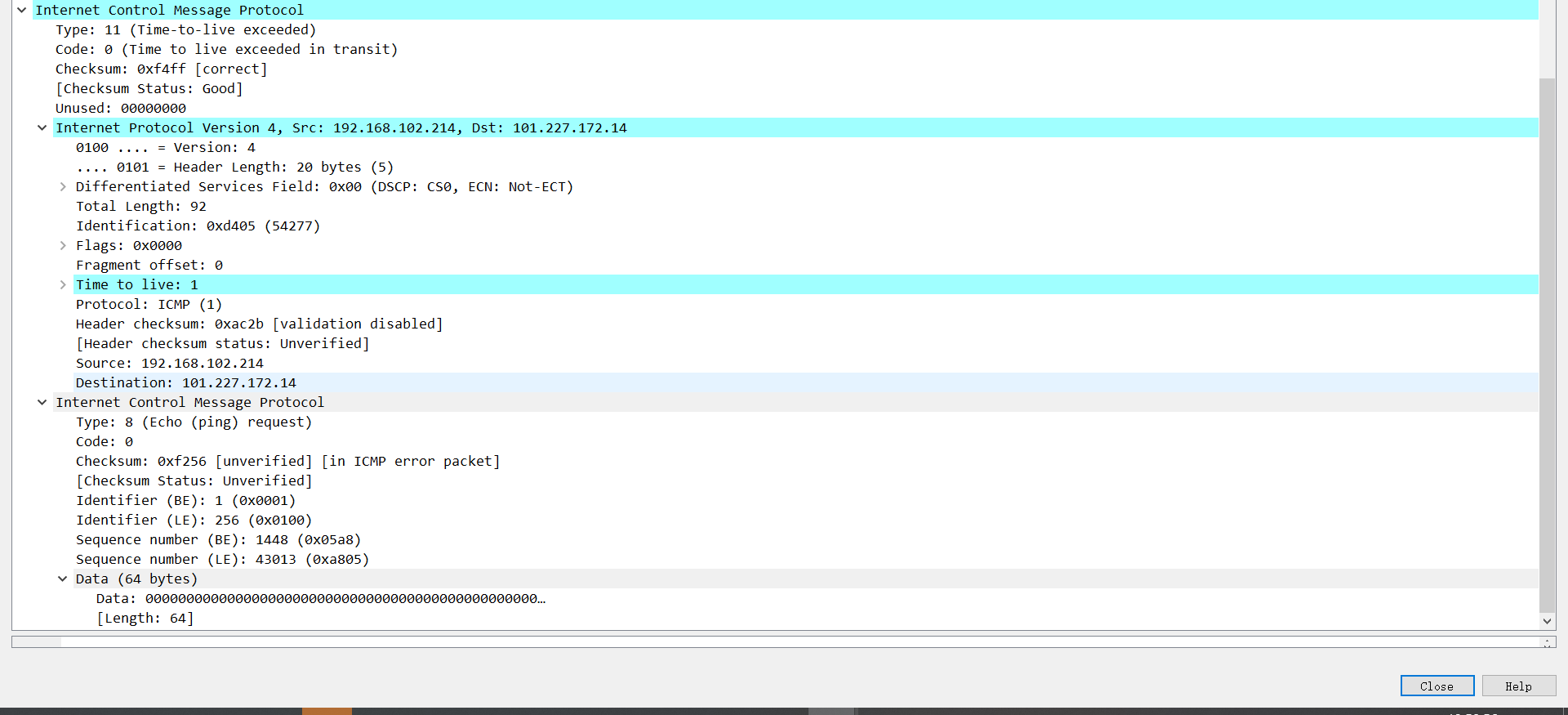


[TTL=2的第二个Ping请求包截屏] \*可以选其他包，但是要修改一下*2和二*



[对应响应包截屏]





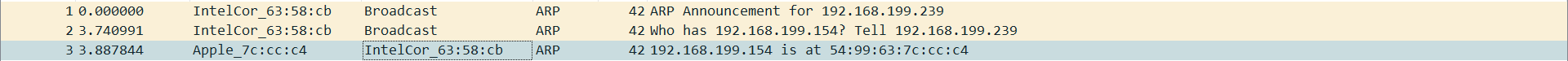
1. (arp.pcapng)ARP协议。

命令：arp –a

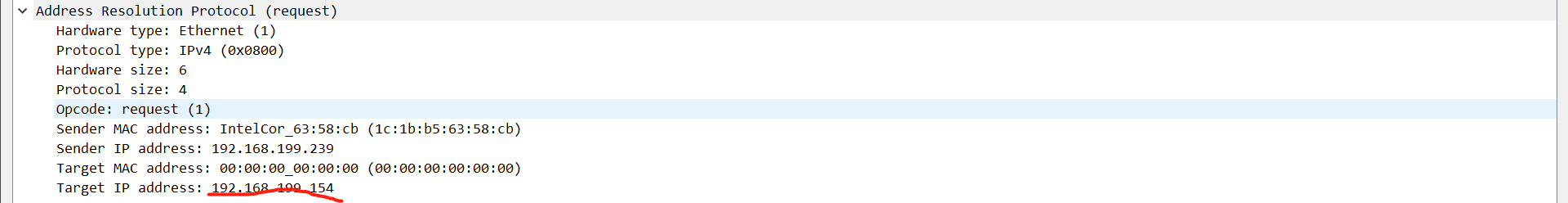
arp –d 192.168.0.14

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

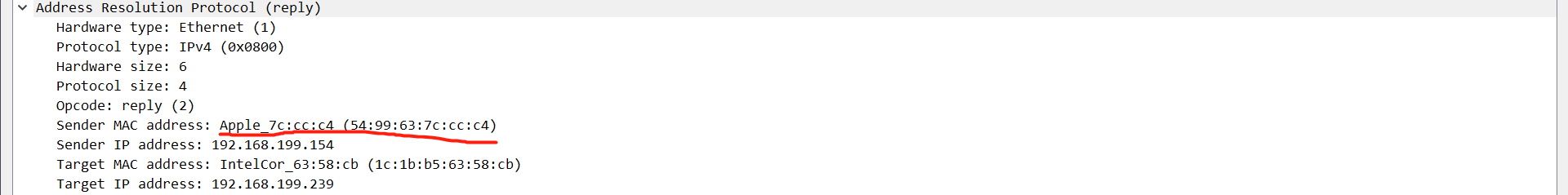
[总图]



[ARP请求包截屏] 用红线标出ARP协议中要查询的IP地址

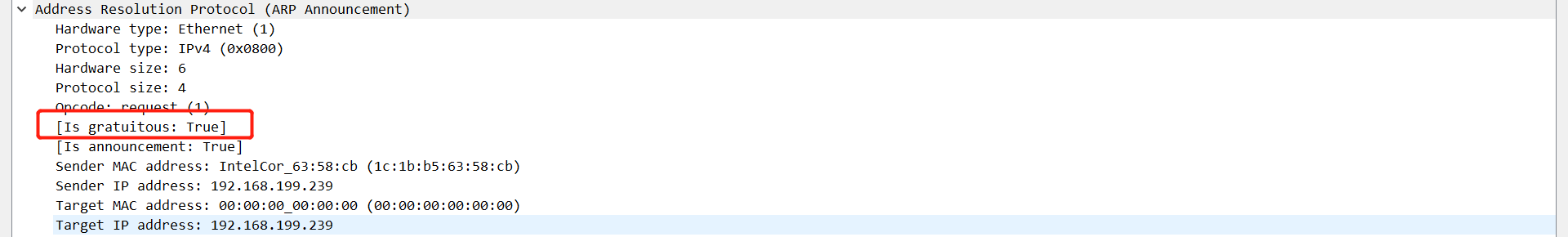


[ARP响应包截屏]用红线标出所查询的IP地址对应的MAC地址



[找到一个Gratuitous ARP包截屏]

打开Anouncement即有：



说明是Gratuitous ARP包。

[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？

将该IP地址填入Target IP address，广播ARP请求包。

ARP协议是否采用了超时重传？

否。

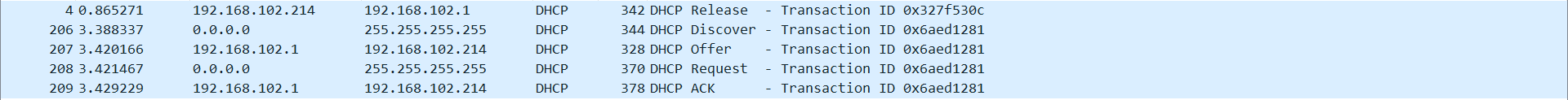
Gratuitous ARP包有什么用途？

1.验证IP是否冲突

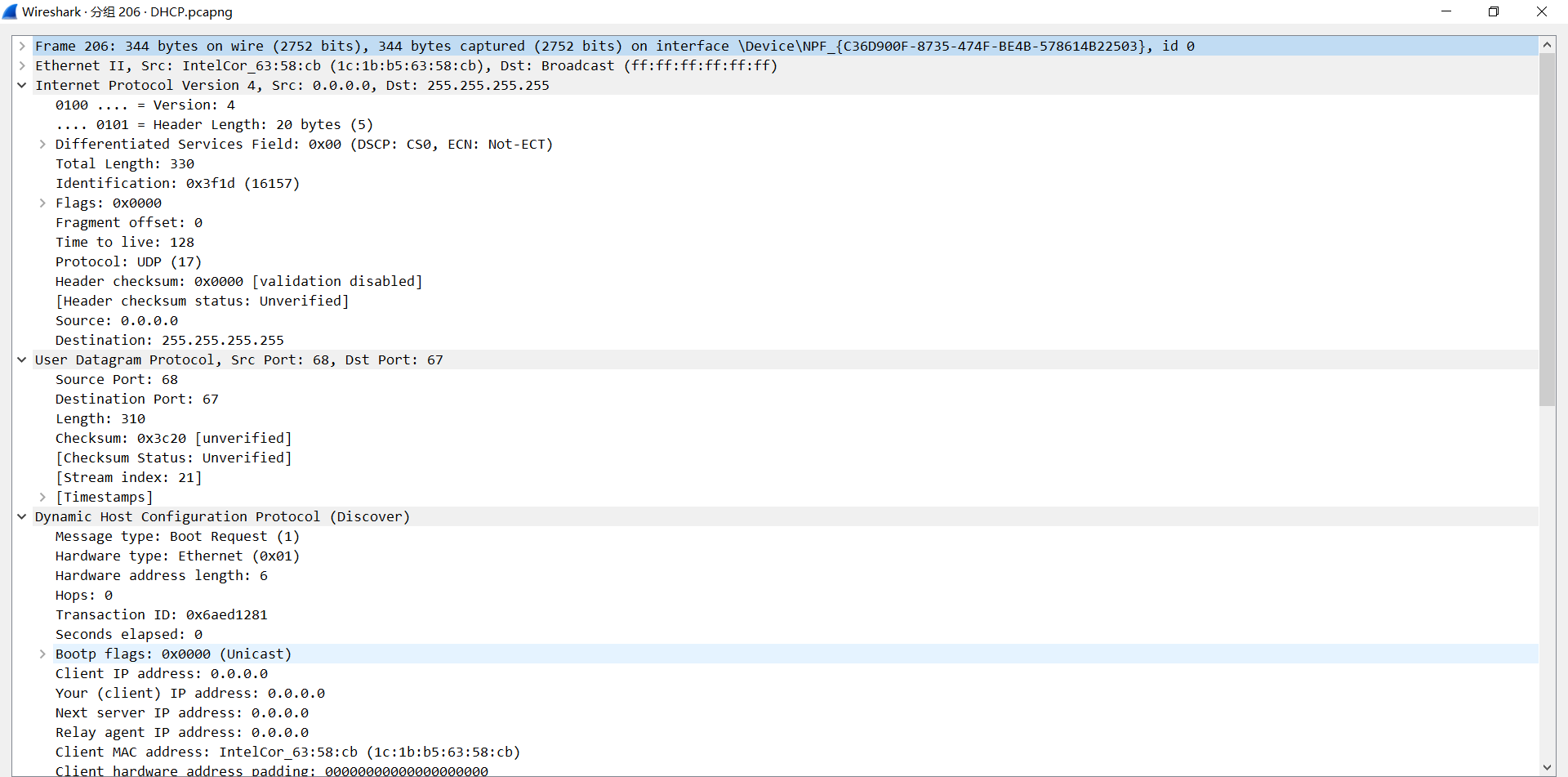
2.更换物理网卡

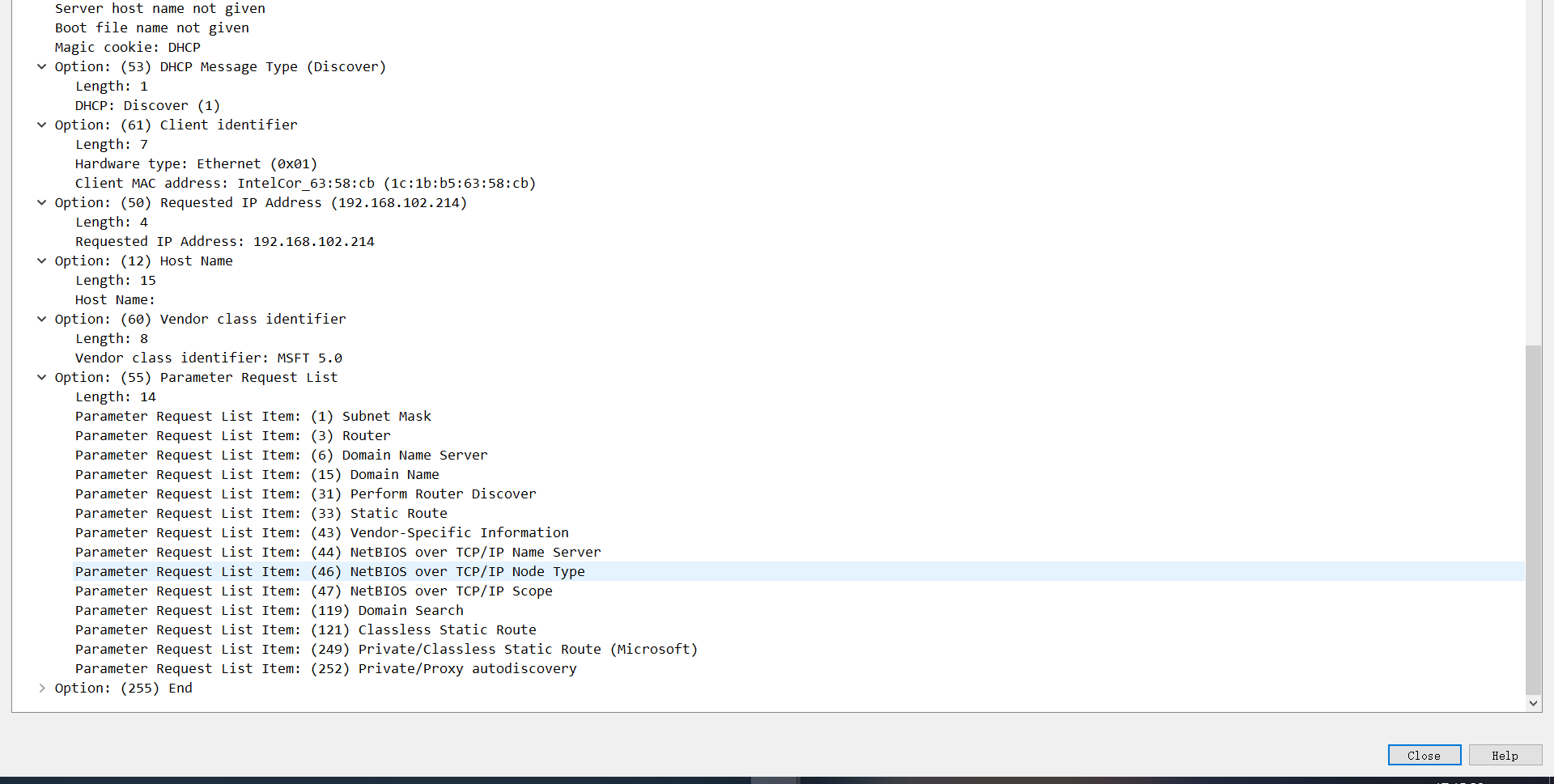
1. (DHCP.pcapng)DHCP协议

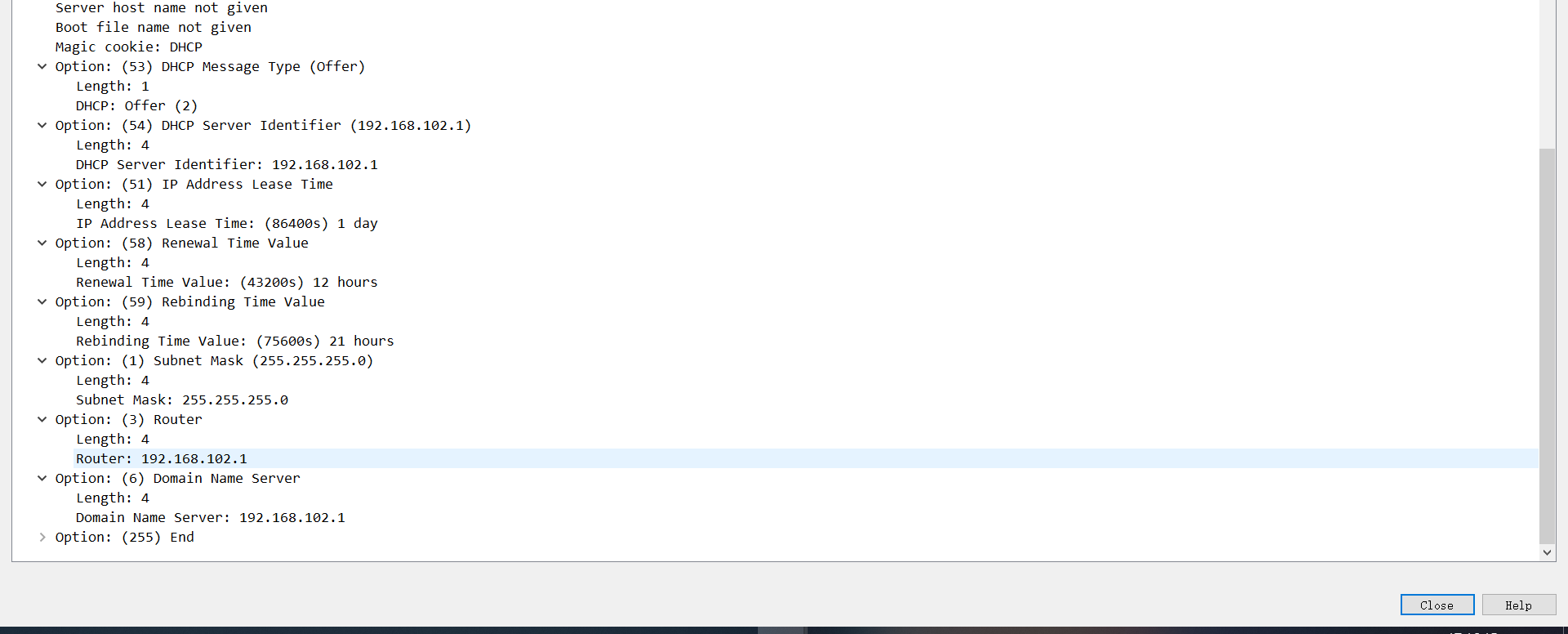
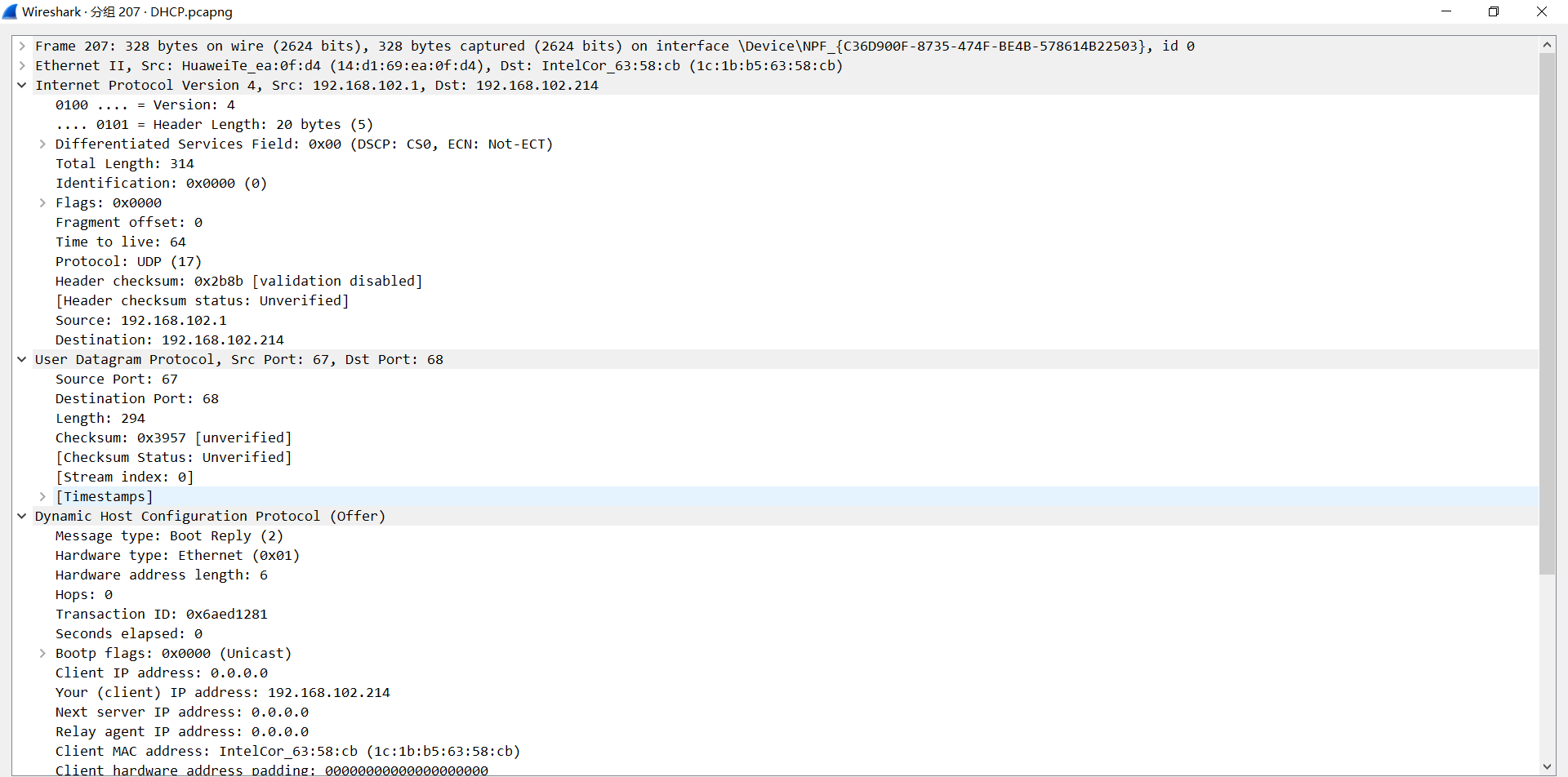
[总图]

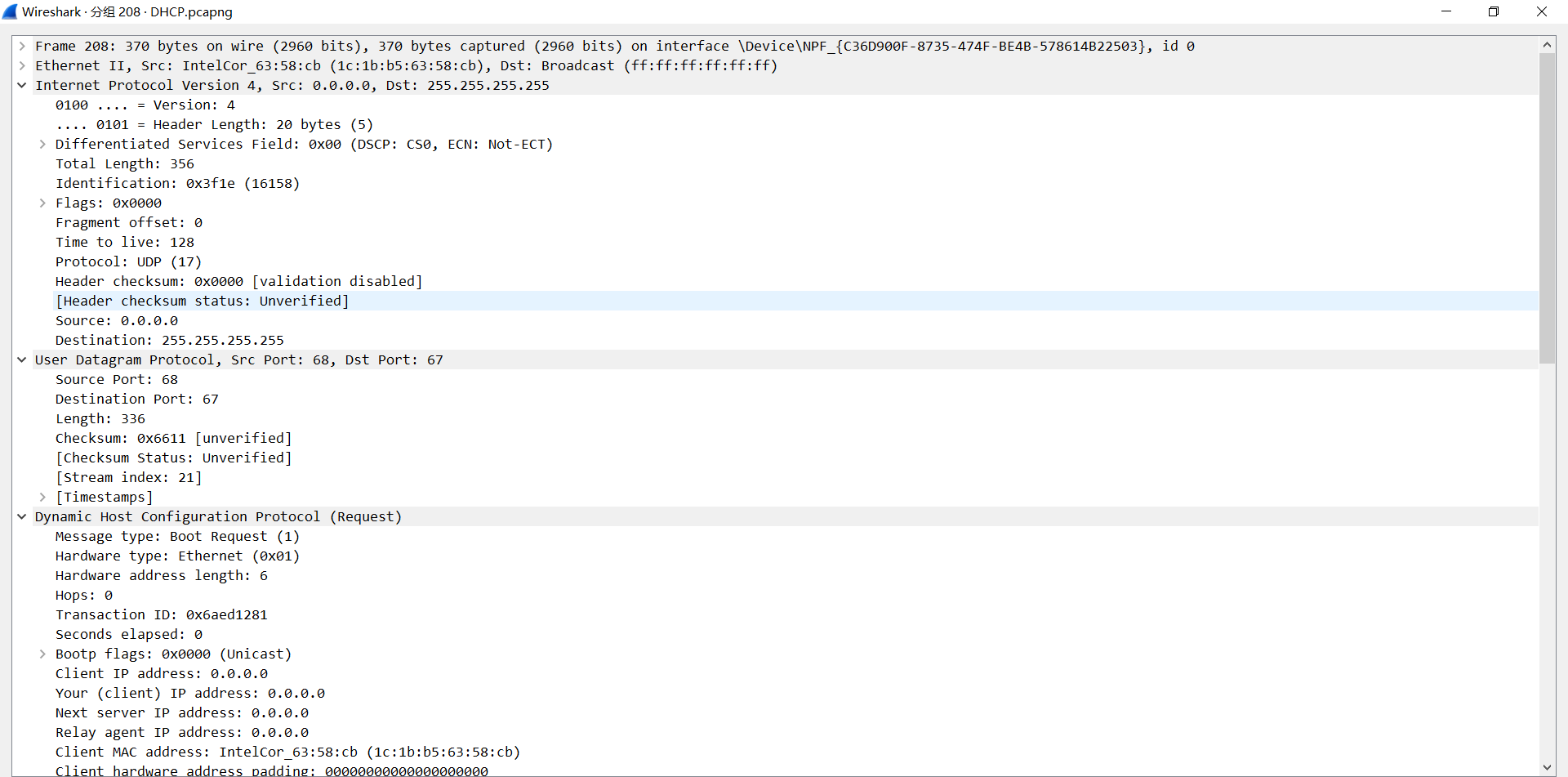


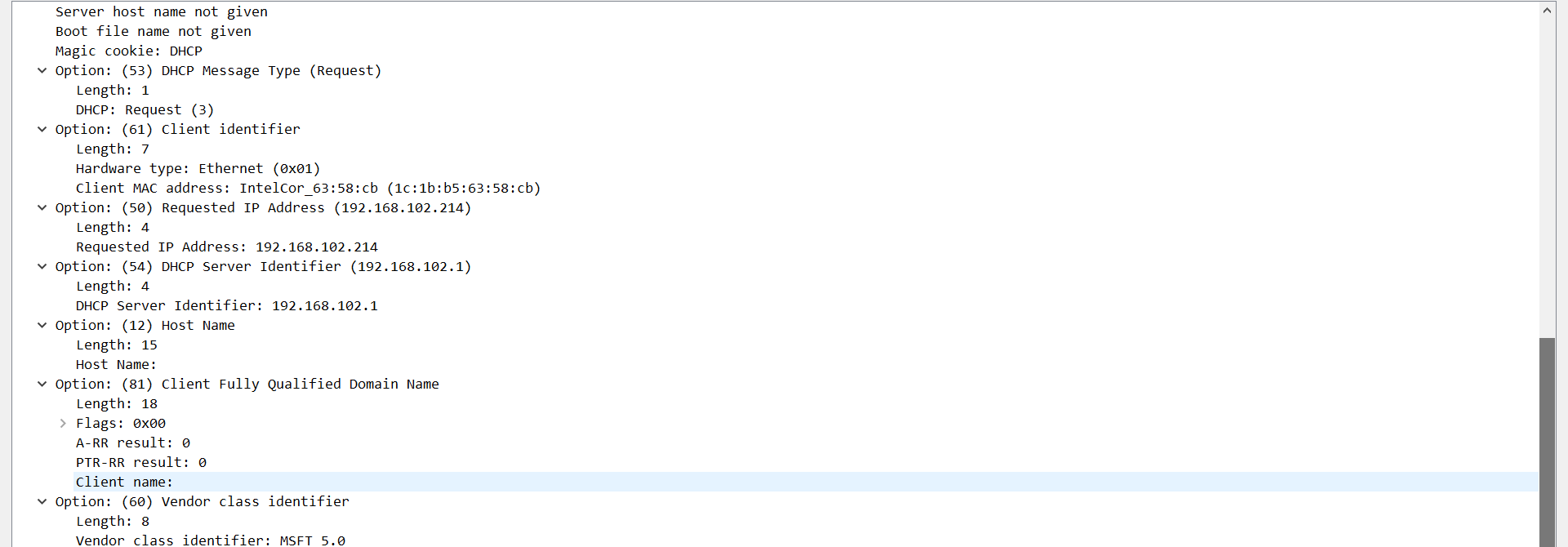
[四个包]

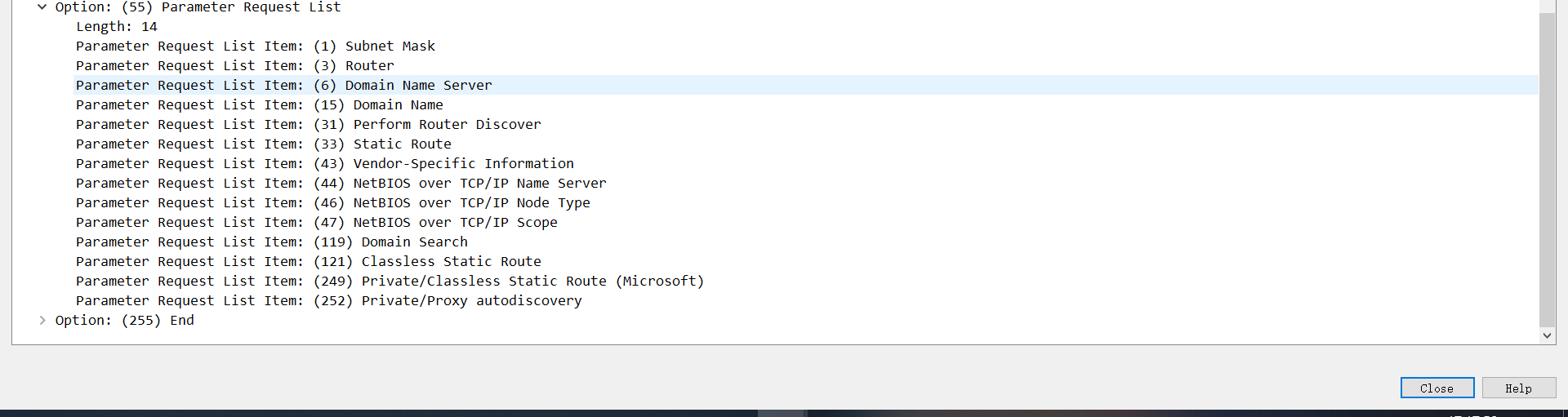


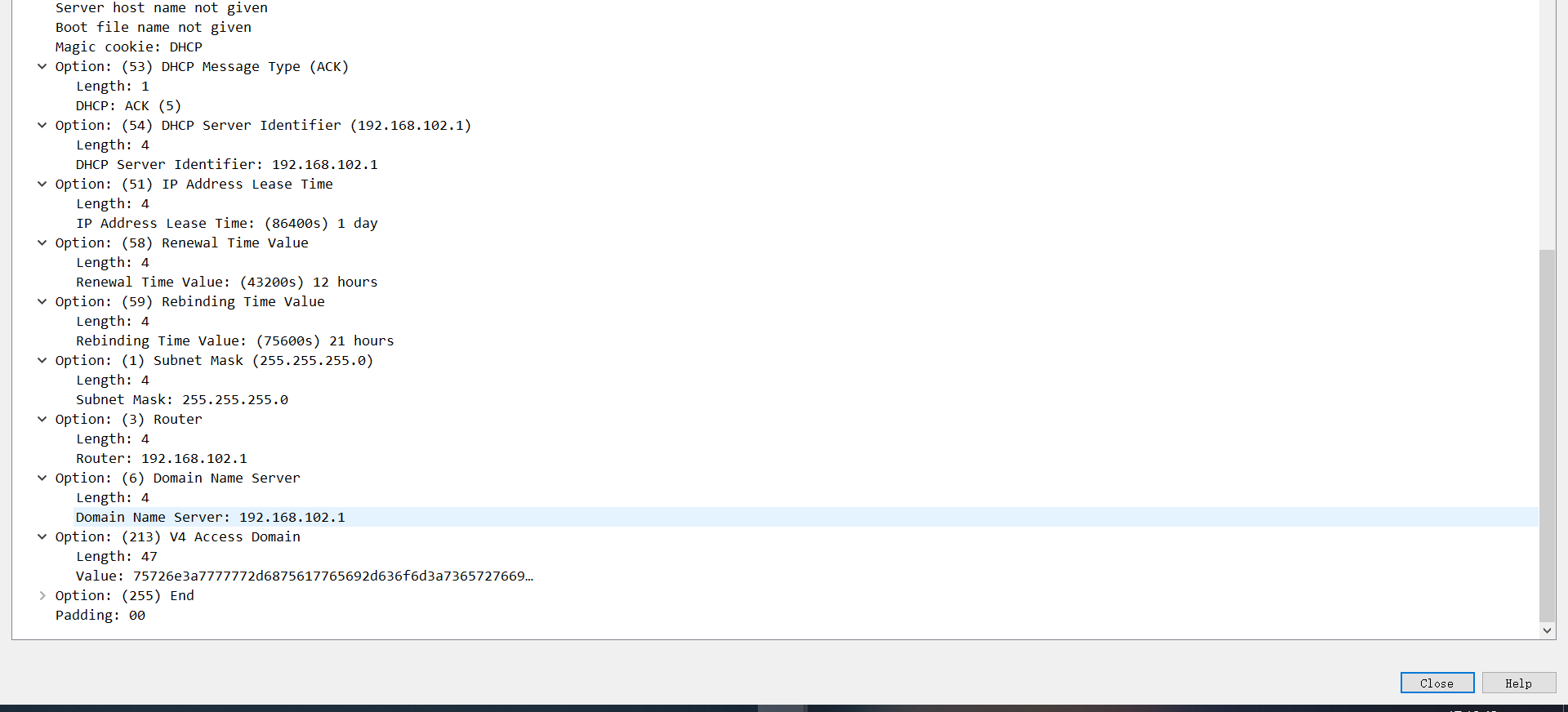
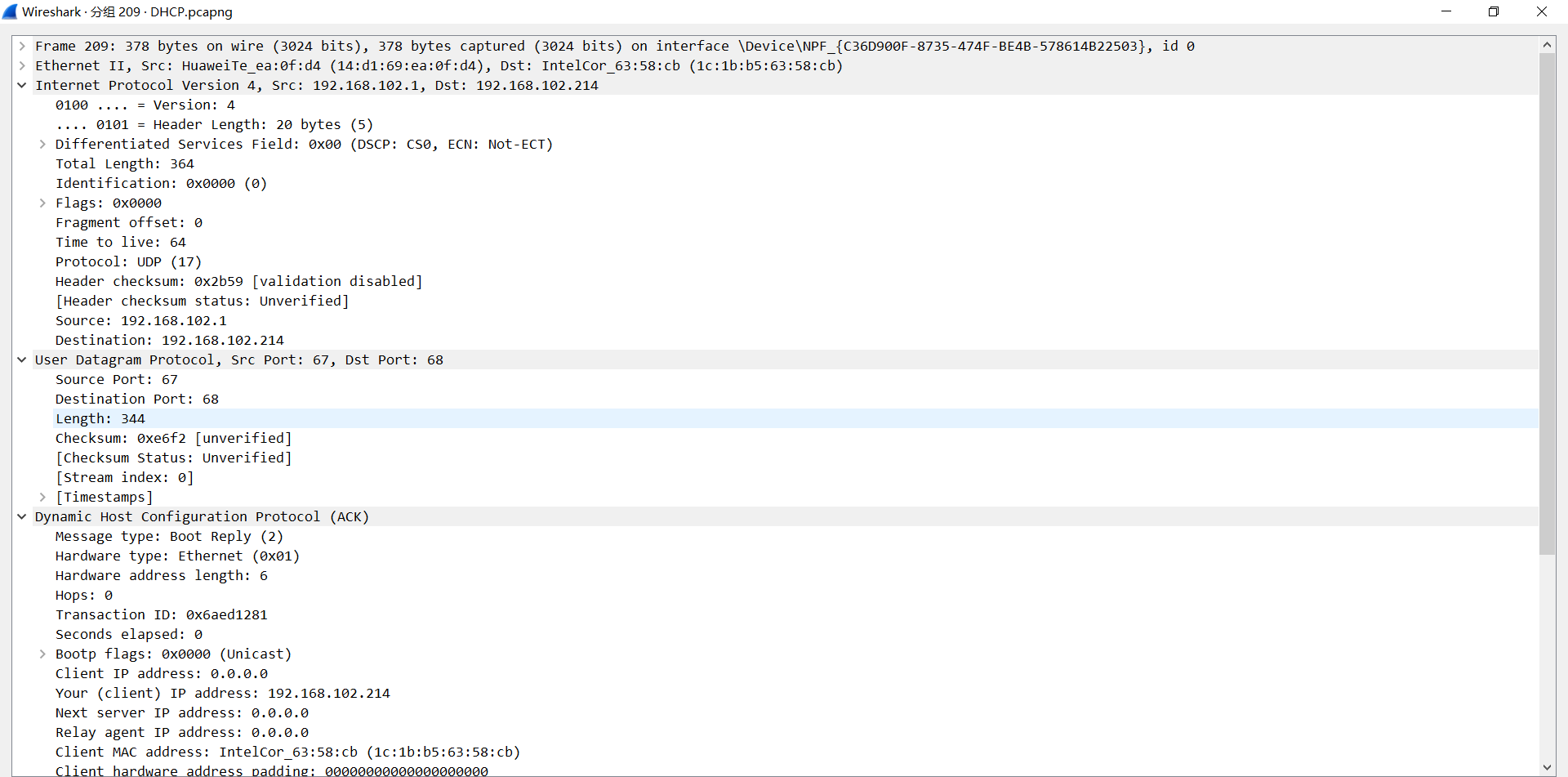




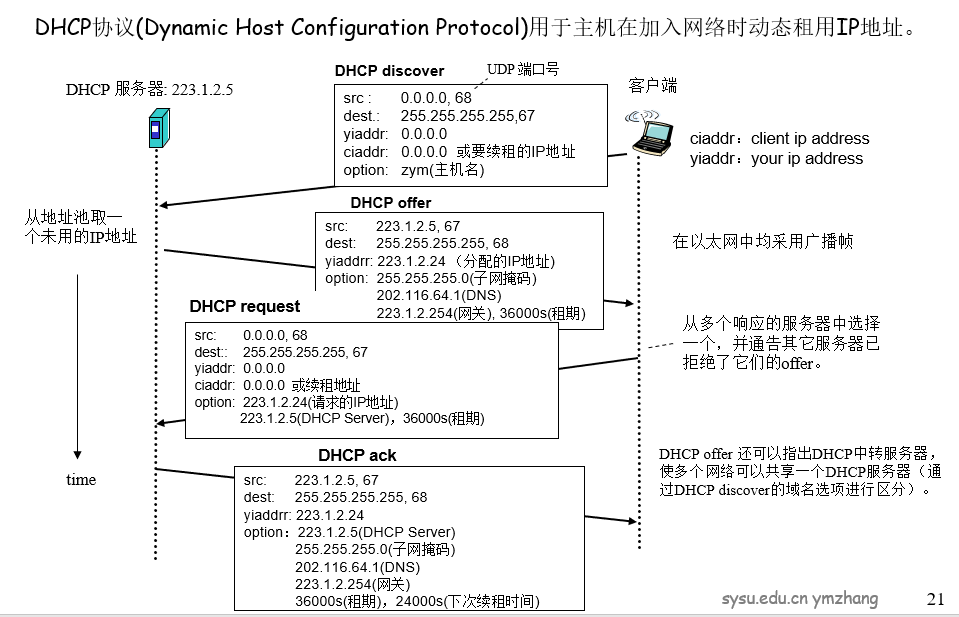








[对照课件]



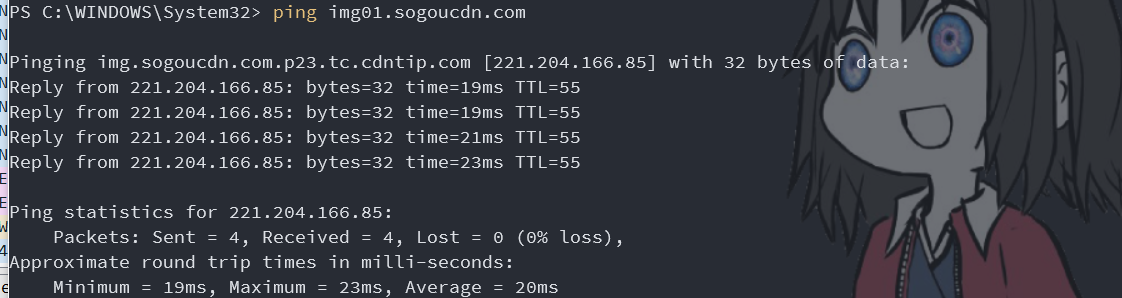
有没有可以纠正的内容？有的话写出来。

1. offer和ack的dest为客户端ip地址，而非广播地址

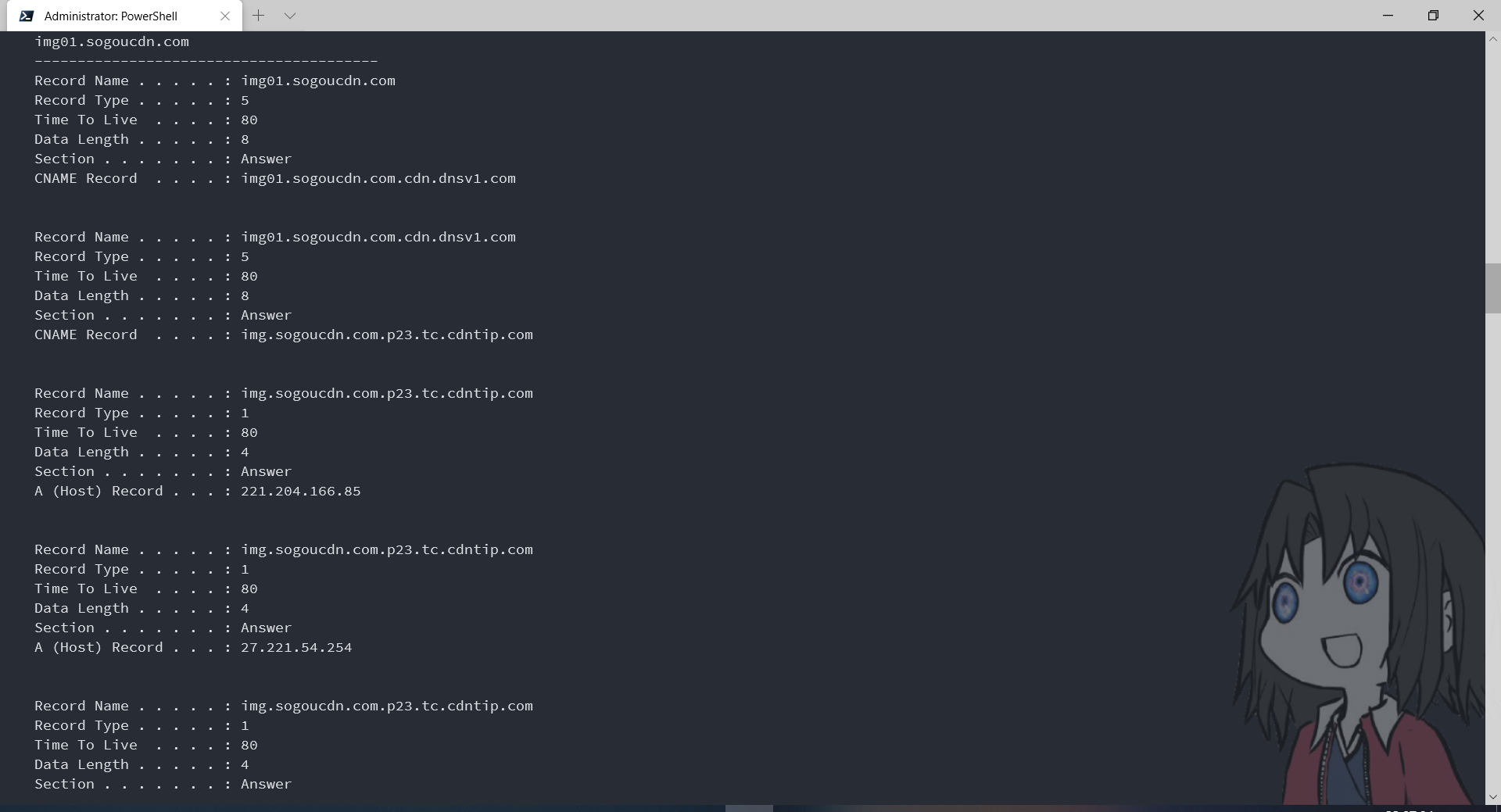
2. request的options里没有租期

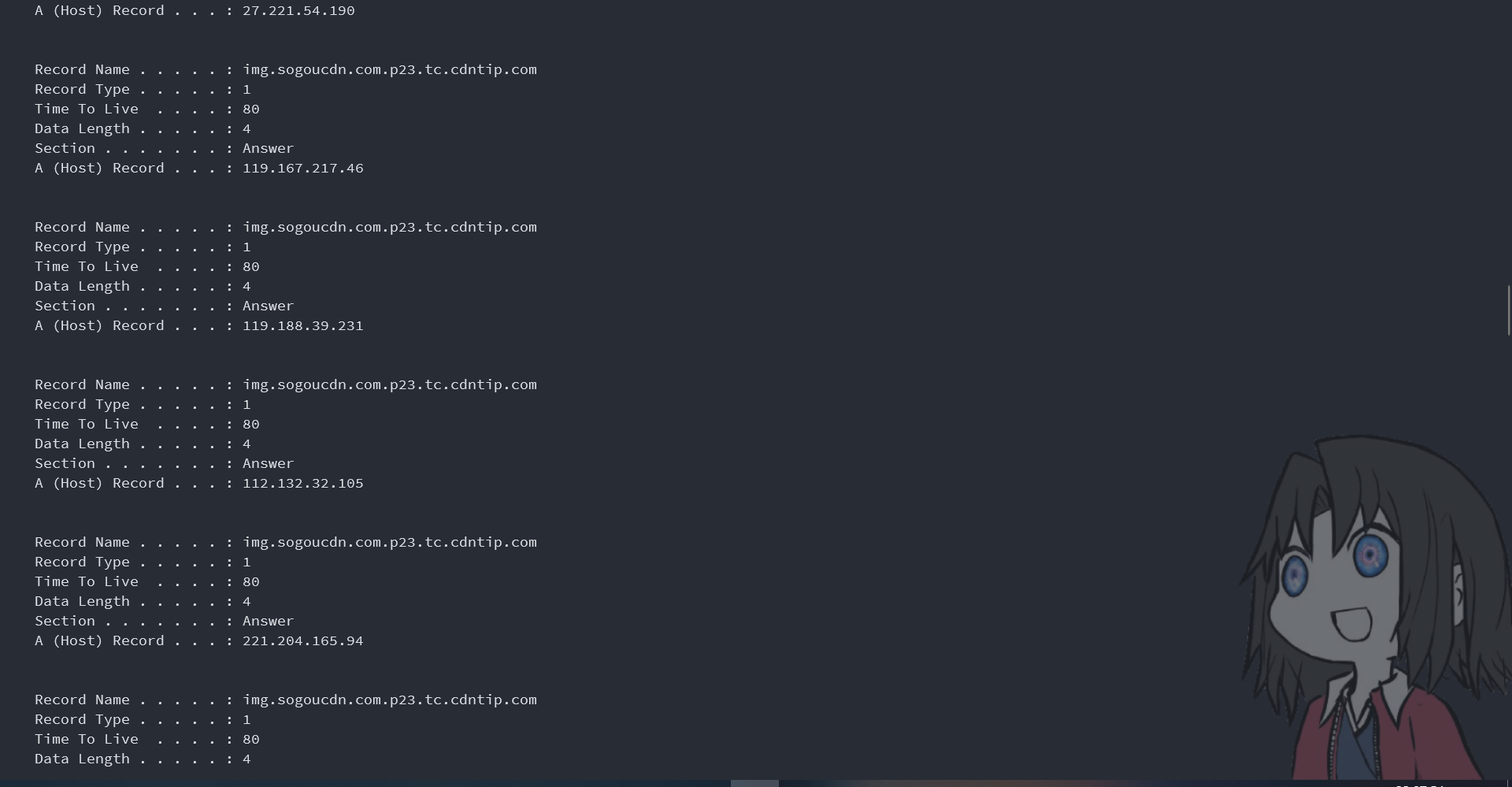
1. (DNS.pcapng)DNS协议

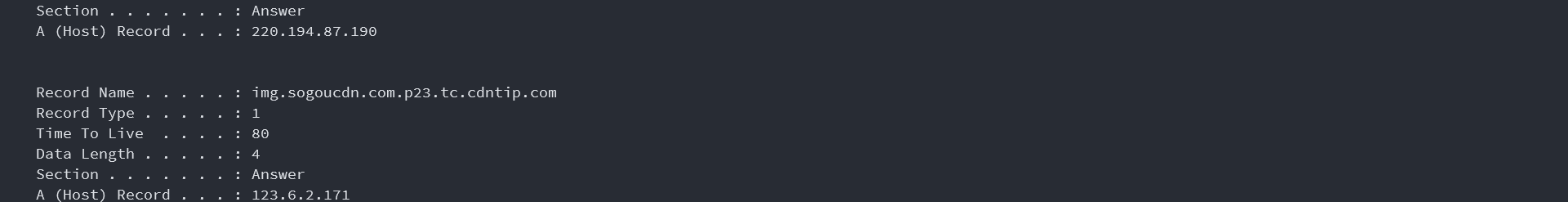
先ping img01.sogoucdn.com并截屏：



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）：

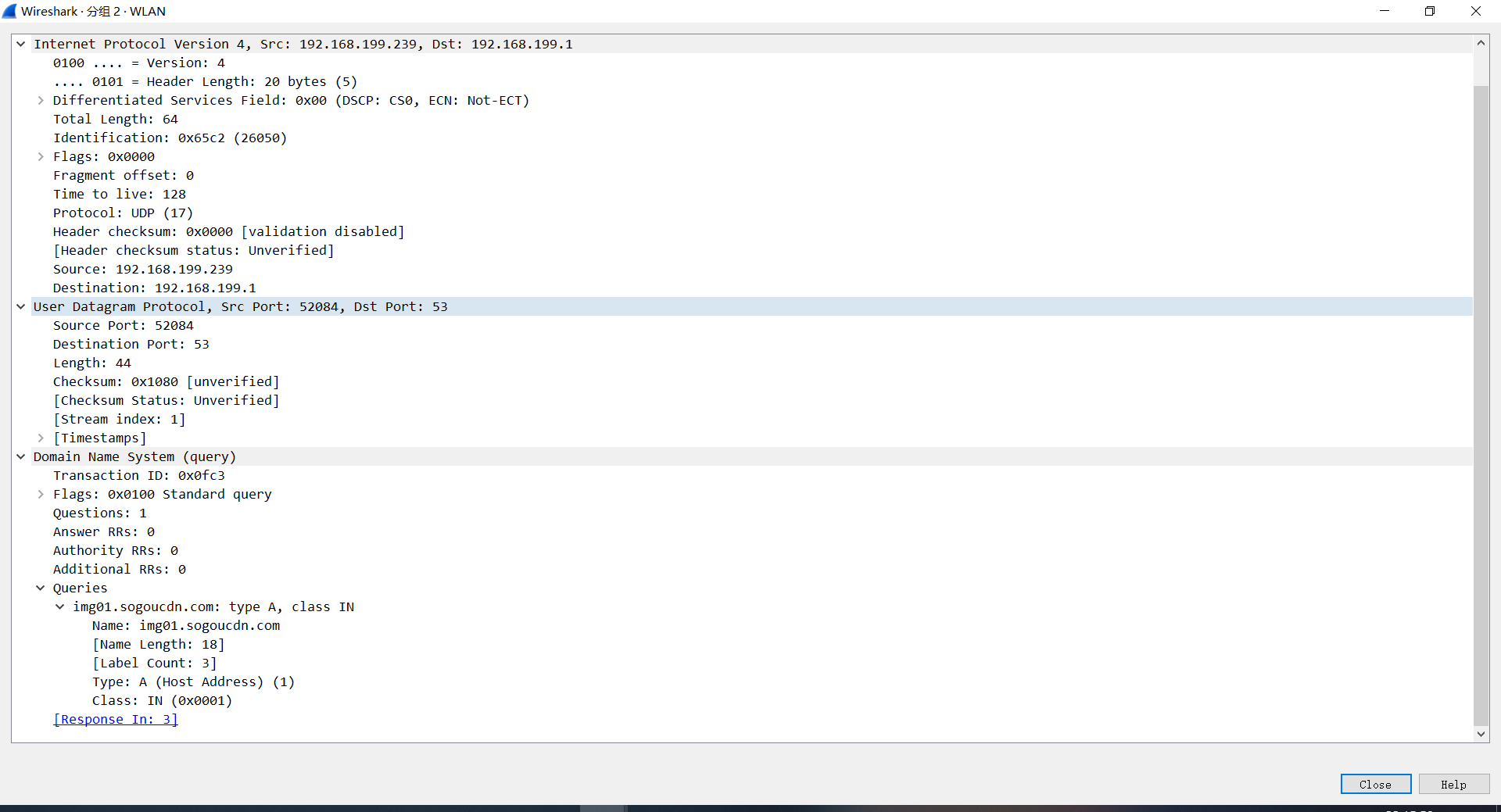
用Record Name索引，或与Record Name比较。

如果是CNAME Record，则映射到另一个域名，最终映射到一个A Record，并映射到相应的IP地址。

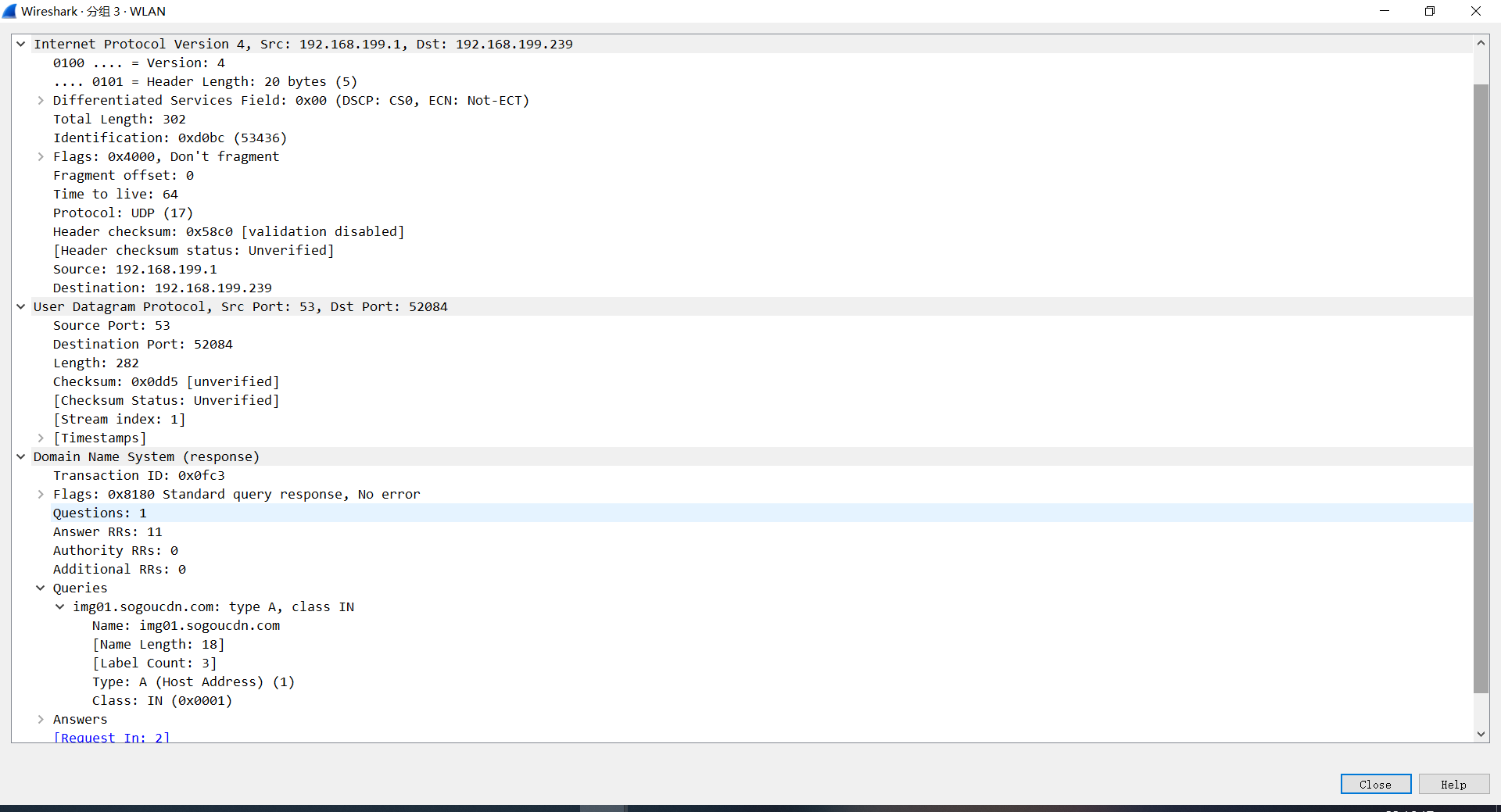
如果是A Record，则直接映射到IP地址。

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：

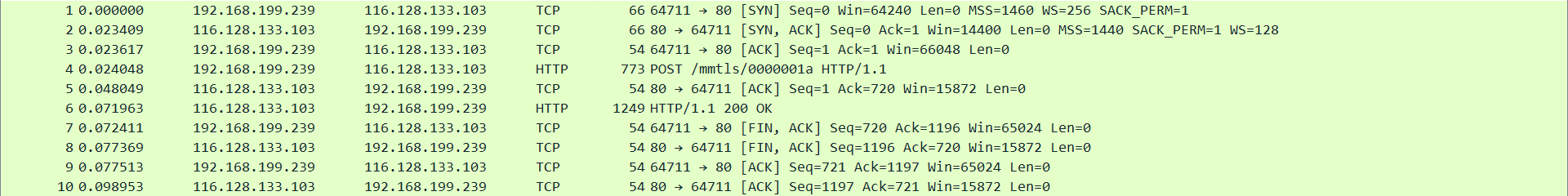
过滤条件：ip.addr==192.168.0.8 and ip.addr==103.26.79.35

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]

三次握手建立连接：

最开始主机1（192.168.199.239:64500）向主机2（116.128.133.102:80）发送SYN，Seq=0。

主机2向主机1发送SYN+ACK，Ack=1=0+1即对上面SYN的确认，Seq=0。

主机1向主机2发送ACK，Ack=1=0+1即对上面SYN+ACK的SYN的确认。

关闭：采用了合并中间两次握手和双方同时发送FIN。

主机1向主机2发送FIN+ACK，Seq=720

主机2向主机1发送FIN+ACK，Seq=1196

主机1向主机2发送ACK，Ack=1197=1196+1即对上面的FIN+ACK的FIN的确认。

主机2向主机1发送ACK，Ack=721=720+1即对最前面的FIN+ACK的FIN的确认。

在三次握手的三个数据包之后，第四个包才是HTTP的， 这说明HTTP的确是使用TCP建立连接的。HTTP下的ACK应该是响应HTTP。

【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】

做ping -r和ping -s的实验时，全都是Timed out。按照老师的说法，可能由于小区出口路由器，后来换用热点不行，咖啡厅的WIFI也不行，最终只得向实验成功的同学索要成功截的包，再加以分析。

做arp实验时，由于平板电脑没有直接的如“ipconfig”，“ifconfig”的命令可以查询其IP地址，在其中安装LibTerm（模拟了部分Linux的指令），然后运行“ifconfig”才得以知晓其IP地址。

做DNS实验时，查询了CNAME Record和A Record的区别。

做TCP实验时，老师给的网址，几次都没有成功截到四次挥手关闭连接，最后用了个拍脑门的办法，开着WireShark上网冲浪，找到看上去比较理想的包并过滤，最后找到了采用了合并中间两次握手和双方同时发送FIN来关闭连接。

【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）