院 系 数据科学与计算机学院 学号　　18340161 姓名 田蕊

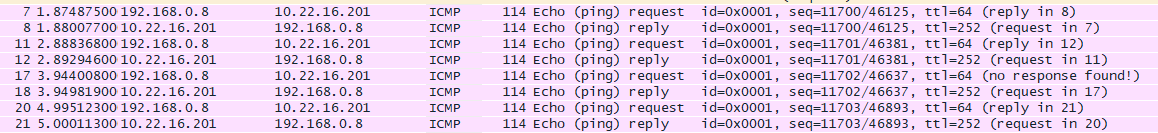
班 级 18

【实验题目】WireShark**实验**

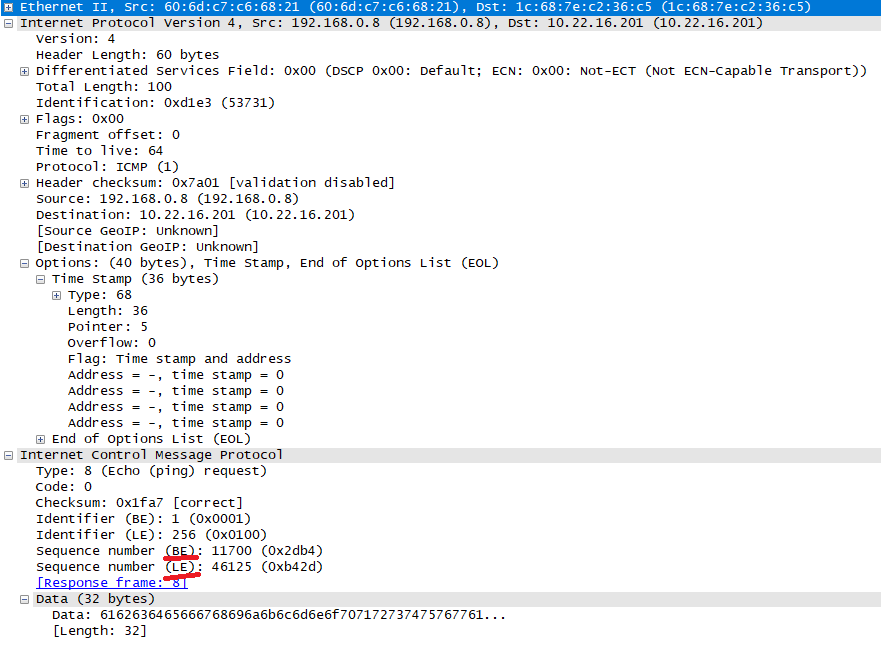
【实验目的】通过WireShark分析IP协议(Option)、ICMP协议、ARP协议、DHCP协议、DNS协议、TCP协议。

【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）。

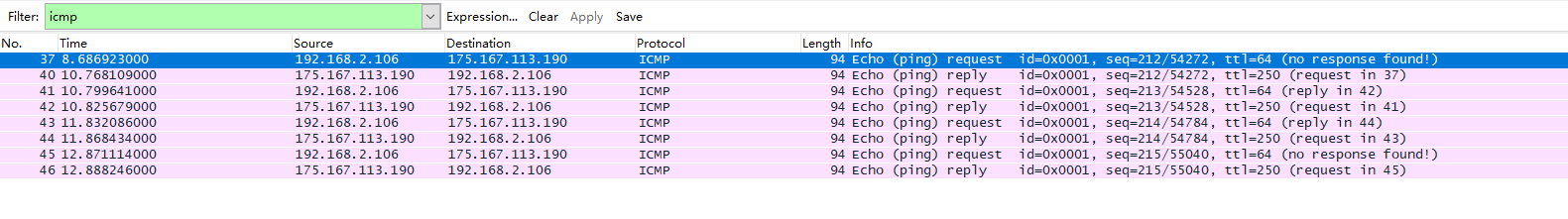
注意每一步都要保存截包文件

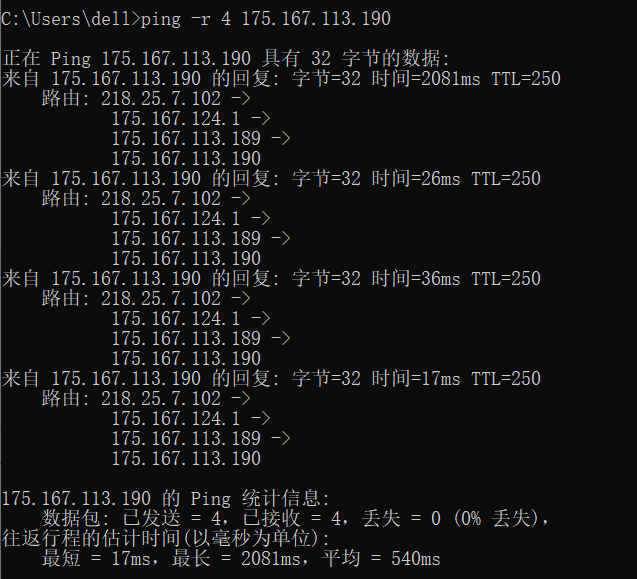
【实验任务】

1. (IP.pcapng)IP Option和ICMP协议。

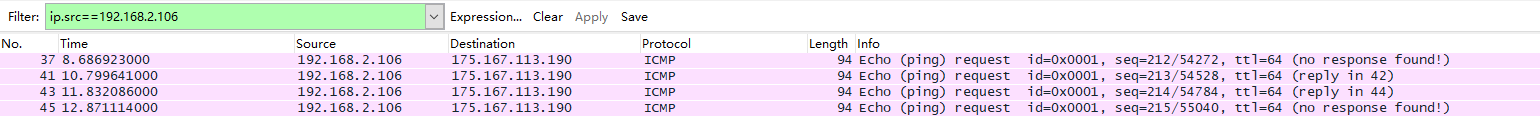
**命令：ping -r 4域名**

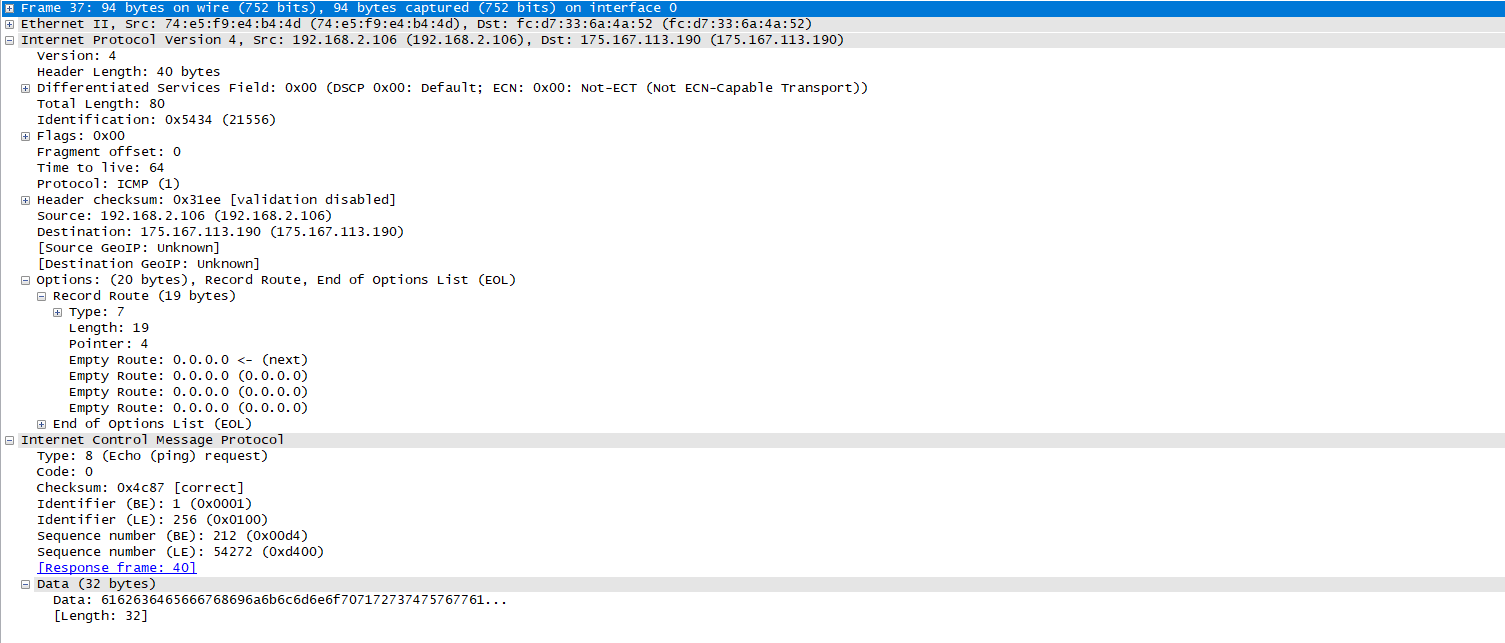
[Ping总图]



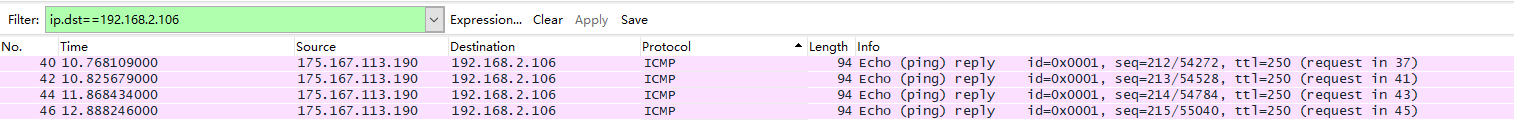


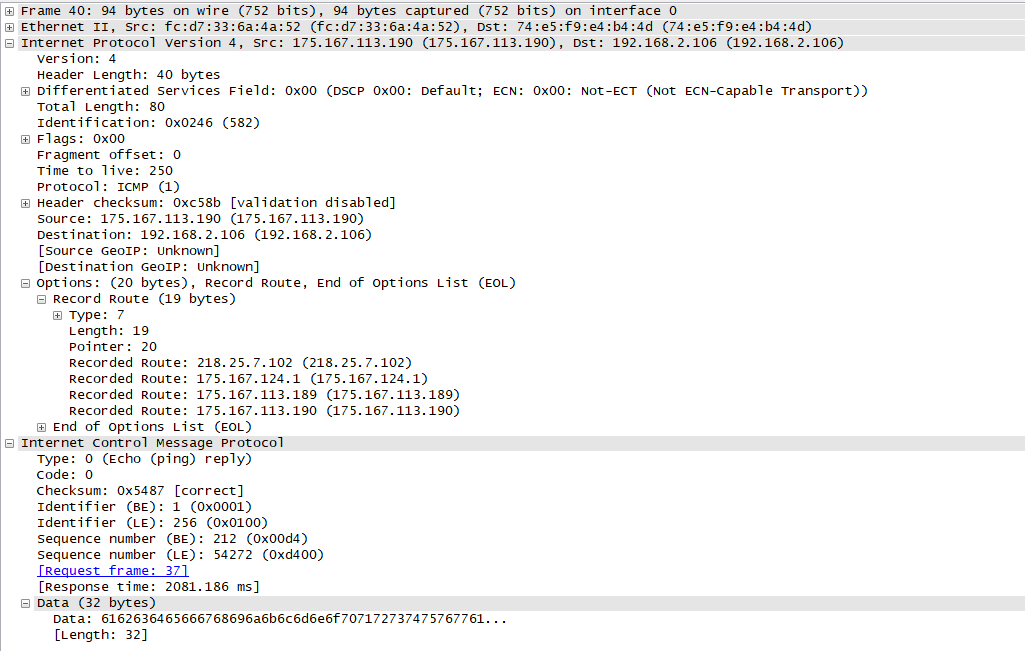
[Ping请求包截屏]





[Ping响应包截屏]





[针对于所截包的问题]

IP选项的长度：20 bytes

ICMP包的Identifier：1

ICMP包的序号：212

ICMP包的数据部分长度：32 bytes

ICMP包的数据部分的内容：



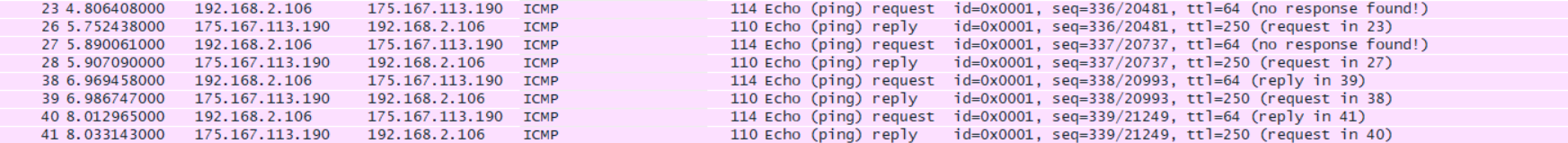
蓝色选中部分就是数据部分内容，左边是十六进制表示的值，右边是字符表示

Identifier是什么含义？

Identifier其实就是根据这个区分不同的PING进程。但是在Windows中icmp Identifier是固定不变的，windows系统不根据Identifier来区别ping进程，它是根据Sequence Number field来区分的。

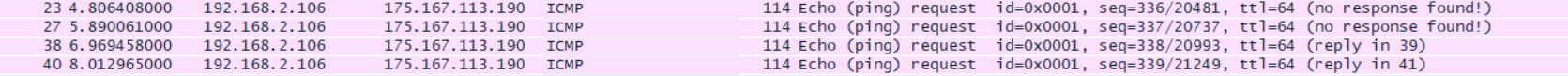
**命令：ping -s 4域名**

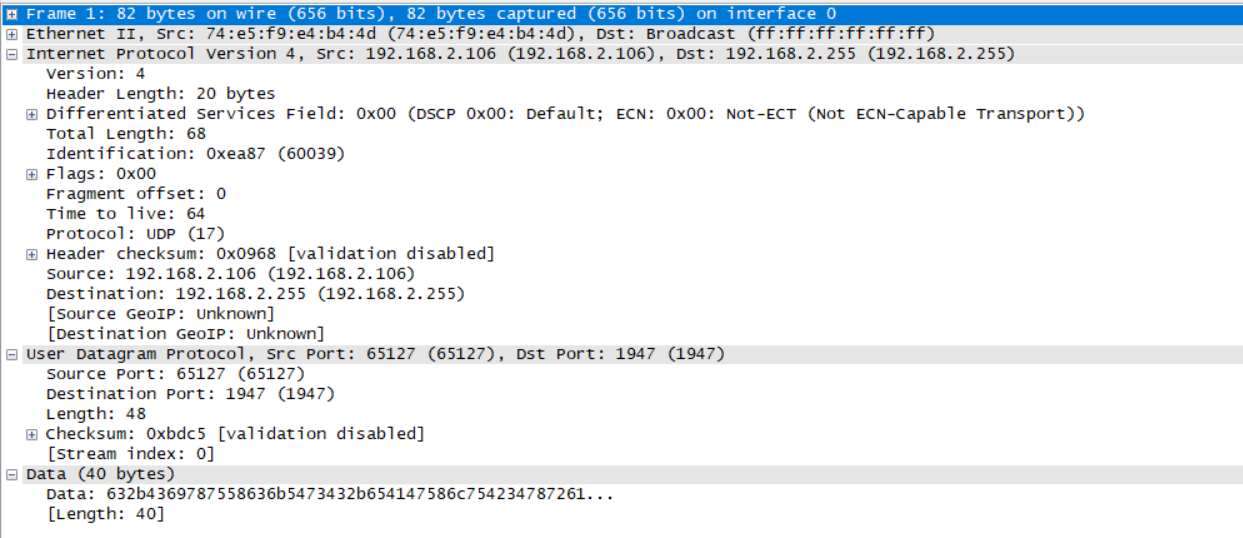
[Ping总图]





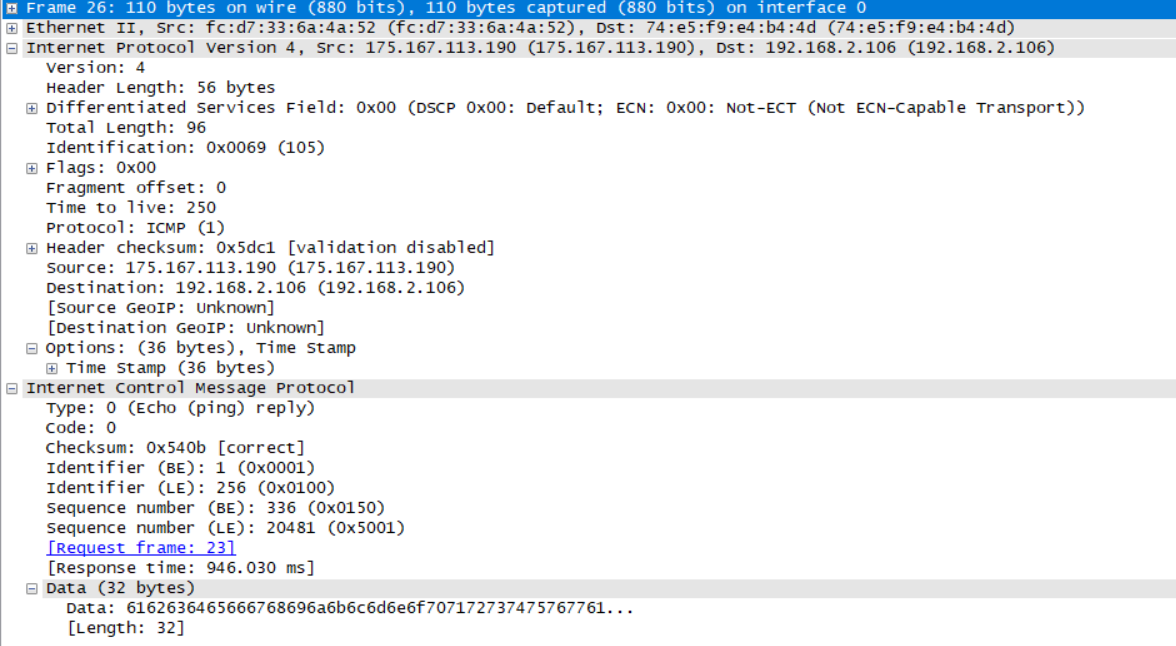
[Ping请求包截屏]





[Ping响应包截屏]



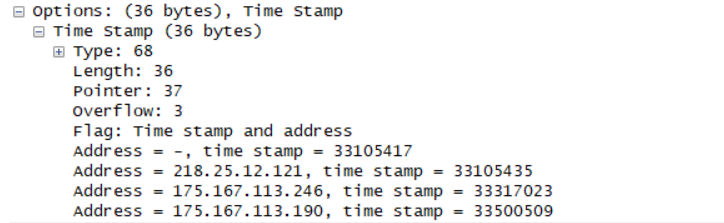


[问题]

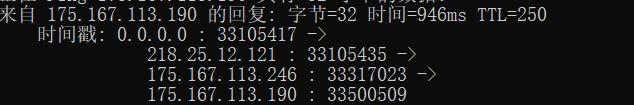
IP选项的长度：36 bytes

选项中的时间戳是否正确？

选项中的时间戳如下所示



控制台中ping后得到的时间戳如下所示

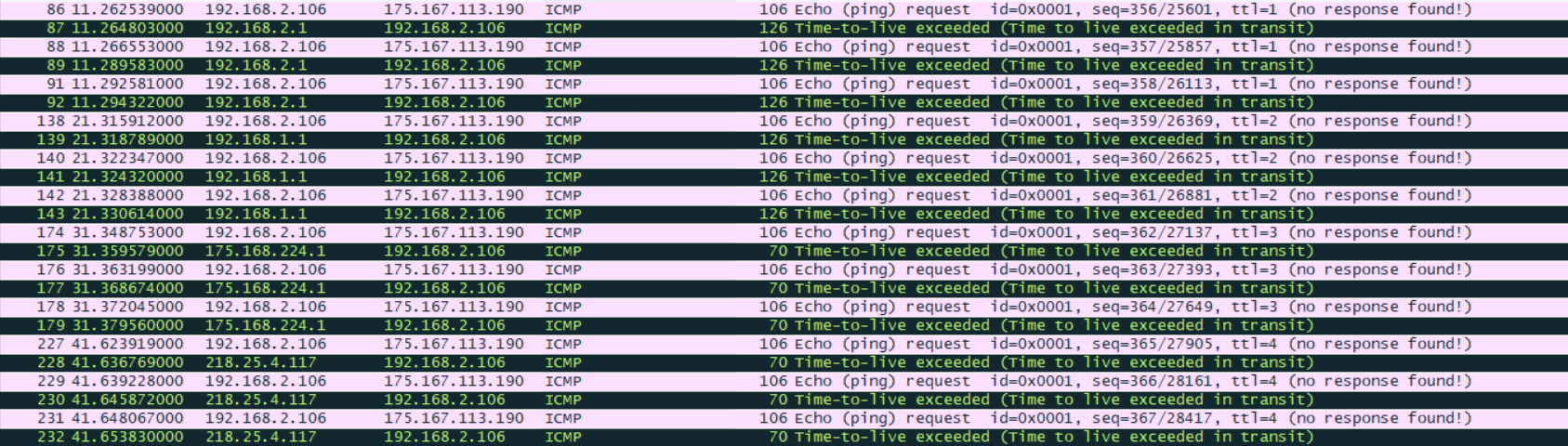


可以看到结果一致，所以时间戳正确。

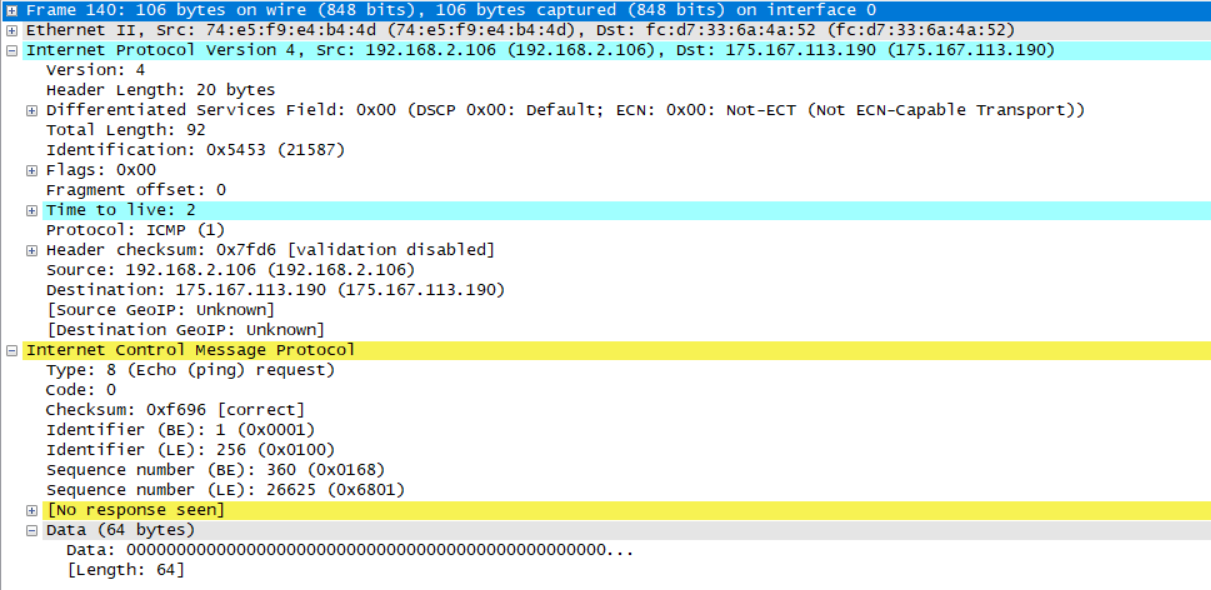
1. (tracert.pcapng) ICMP协议

命令：tracert -h 4 域名

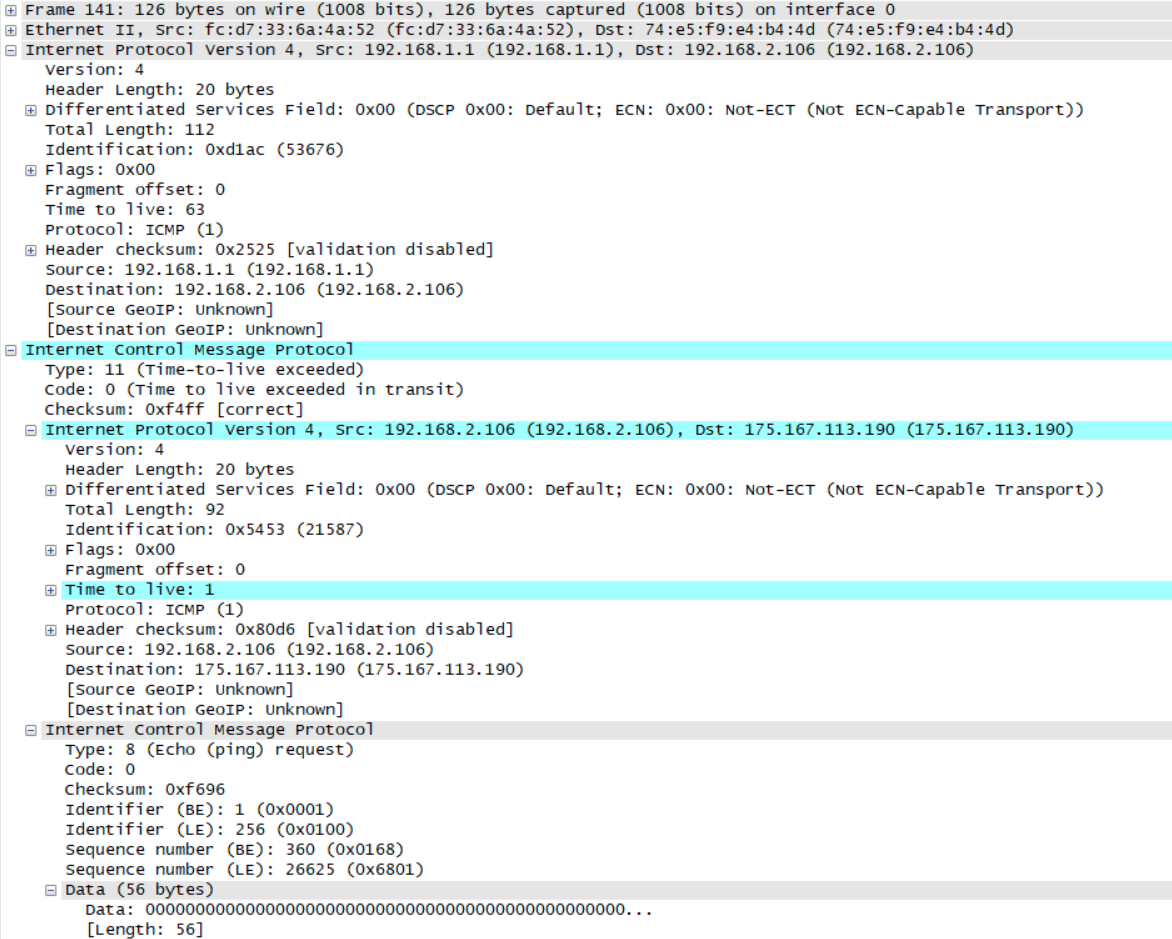
[tracert总图截屏]



[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。

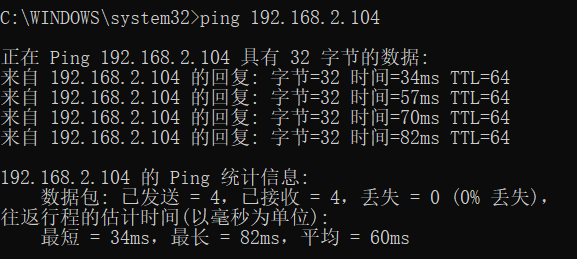
命令：arp –a

arp –d 192.168.0.14

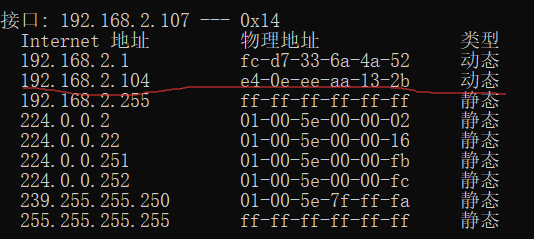
ping家里另一台电脑或手机：先查看ARP缓存，删掉这台电脑的映射，然后启动截包，再ping它

[总图]

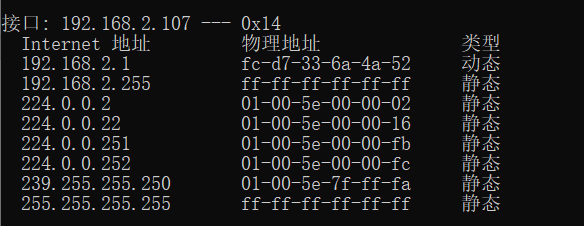
Ping一个手机的IP



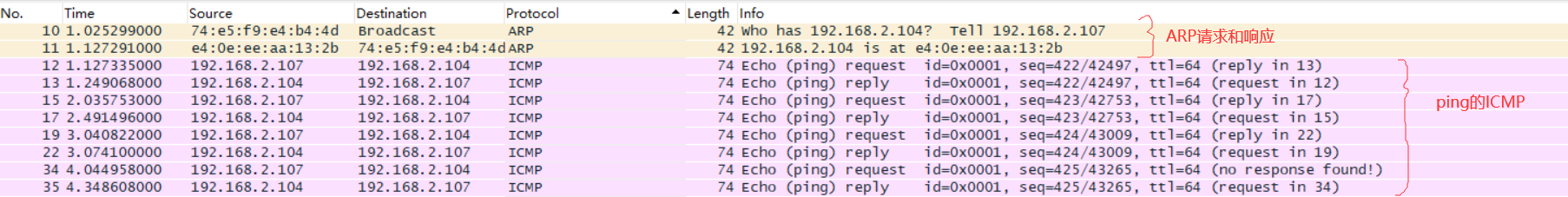
Arp -a查看结果



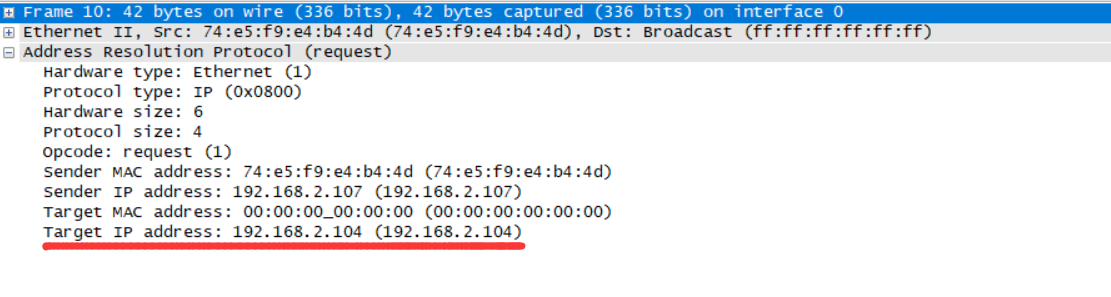
删除后映射不再存在



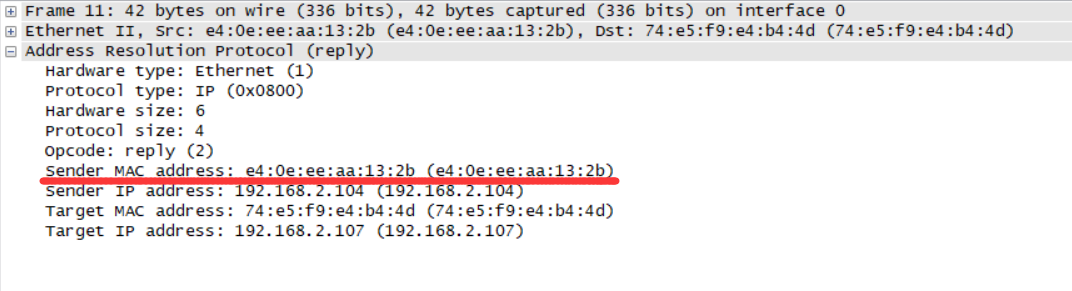
总图：



[ARP请求包截屏] 用红线标出ARP协议中要查询的IP地址

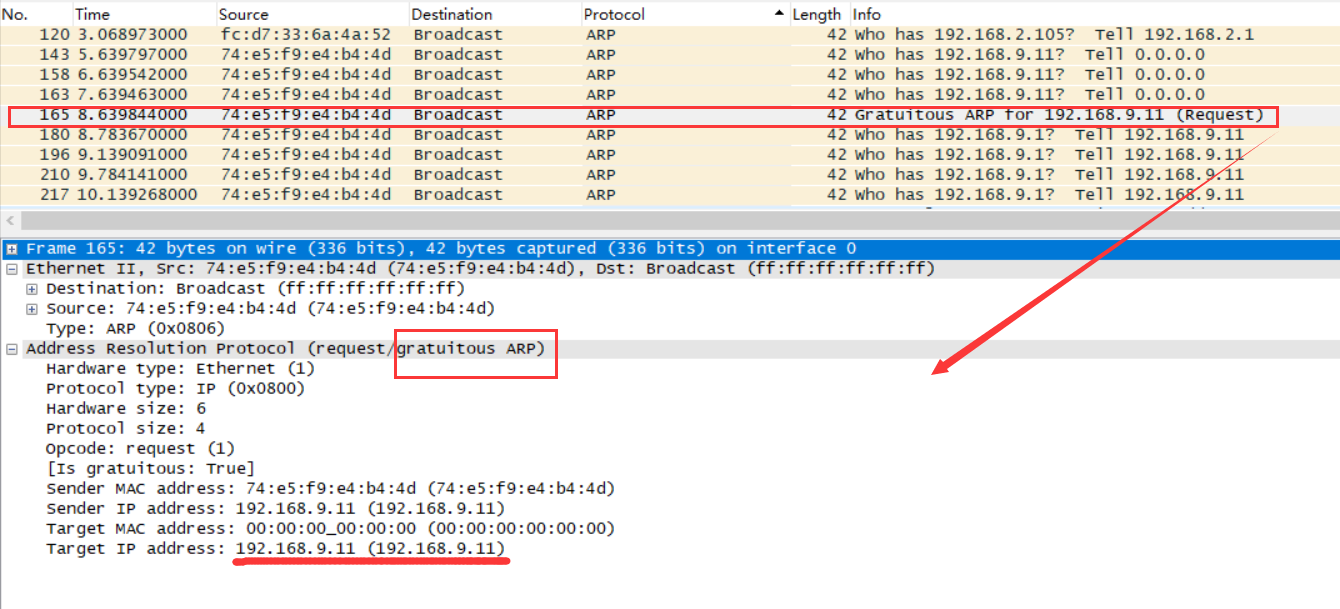


[ARP响应包截屏]用红线标出所查询的IP地址对应的MAC地址



[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？**

先广播一个ARP包查询这个IP地址对应的物理地址的映射

**ARP协议是否采用了超时重传？**

没有采用

**Gratuitous ARP包有什么用途？**

Gratuitous ARP不同于一般的ARP请求，它并非期待得到IP对应的MAC地址，而是当主机启动的时候，将发送一个Gratuitous arp请求，即请求自己的IP地址的MAC地址。

（1）、Gratuitous ARP可以用来验证主机是否冲突

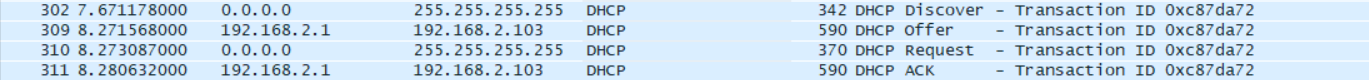
一个主机可以通过它来确定另一个主机是否设置了相同的IP地址。发送主机并不需要一定收到此请求的回答。如果收到一个回答，表示网络中存在与自身IP相同的主机。如果没有收到应答，则表示本机所使用的IP与网络中其它主机并不冲突。

（2）、更换物理网卡

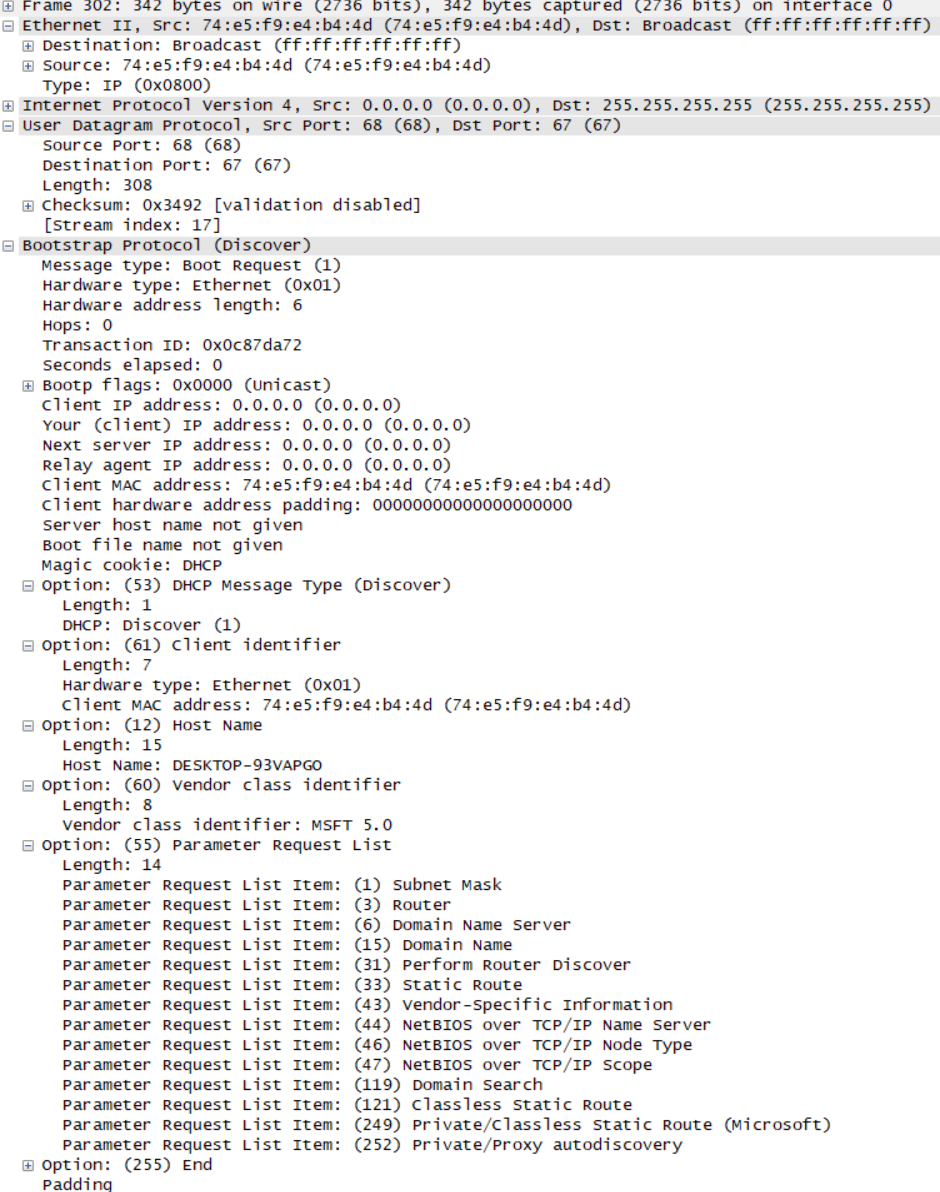
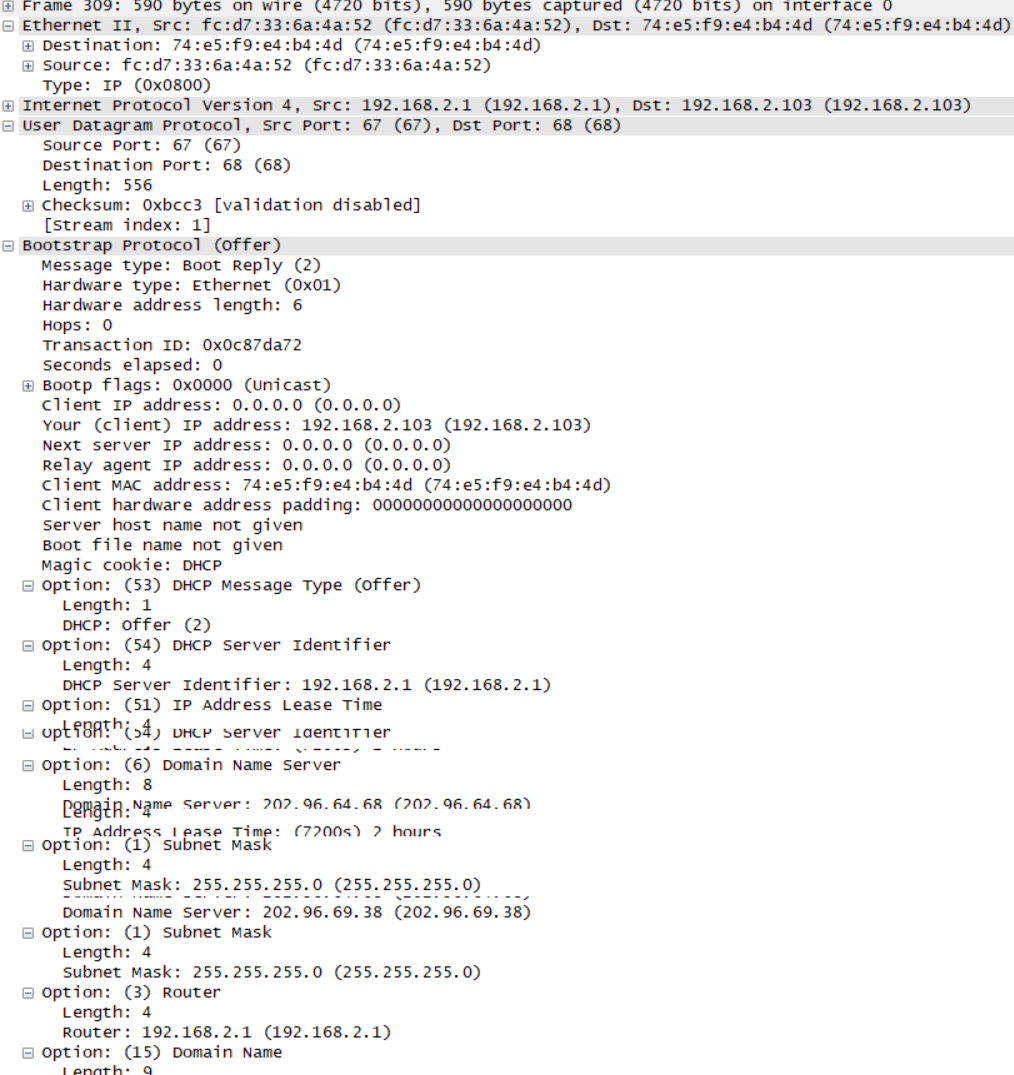
如果发送ARP的主机正好改变了物理地址（如更换物理网卡），可以使用此方法通知网络中其它主机及时更新ARP缓存。

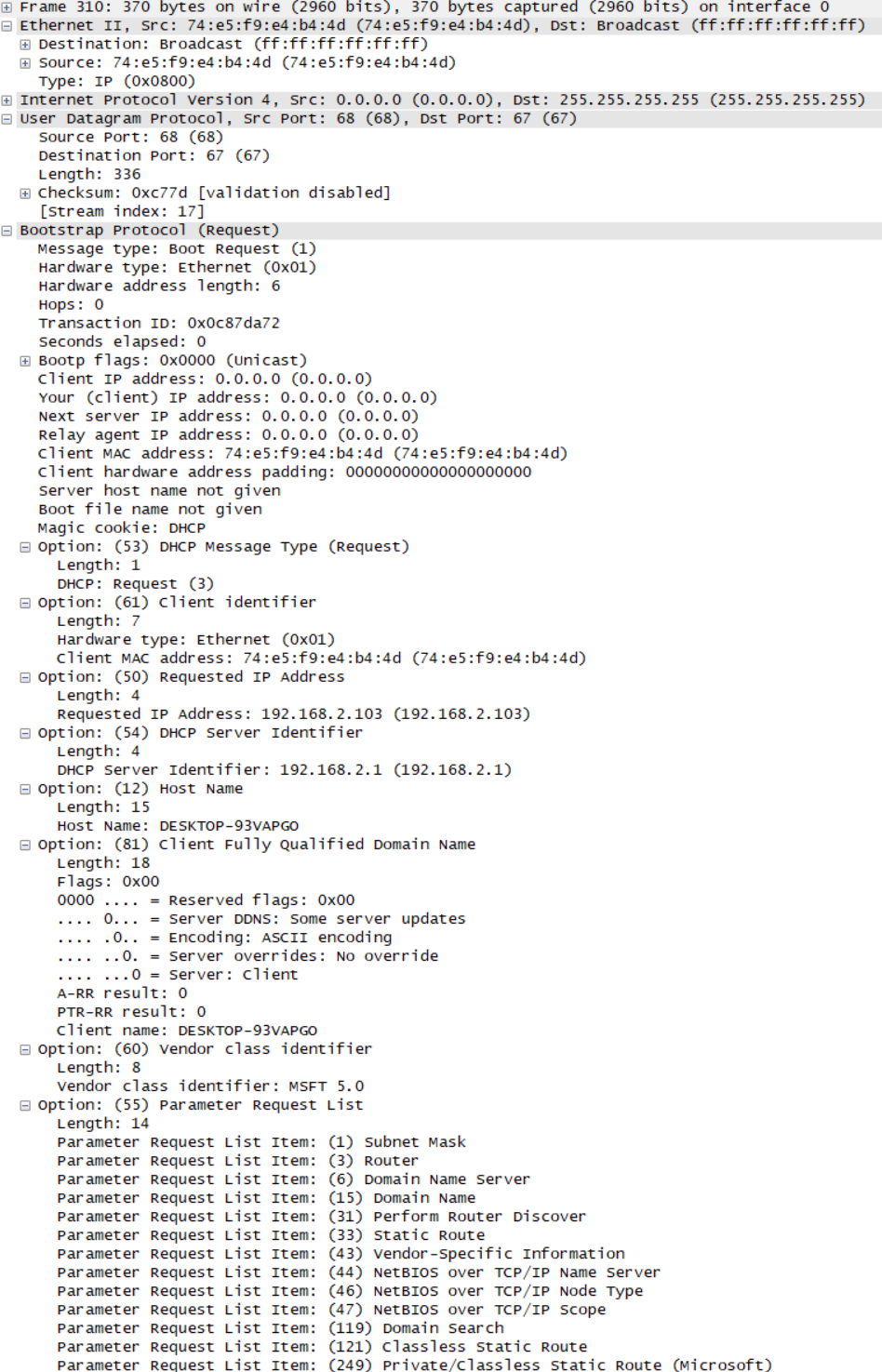
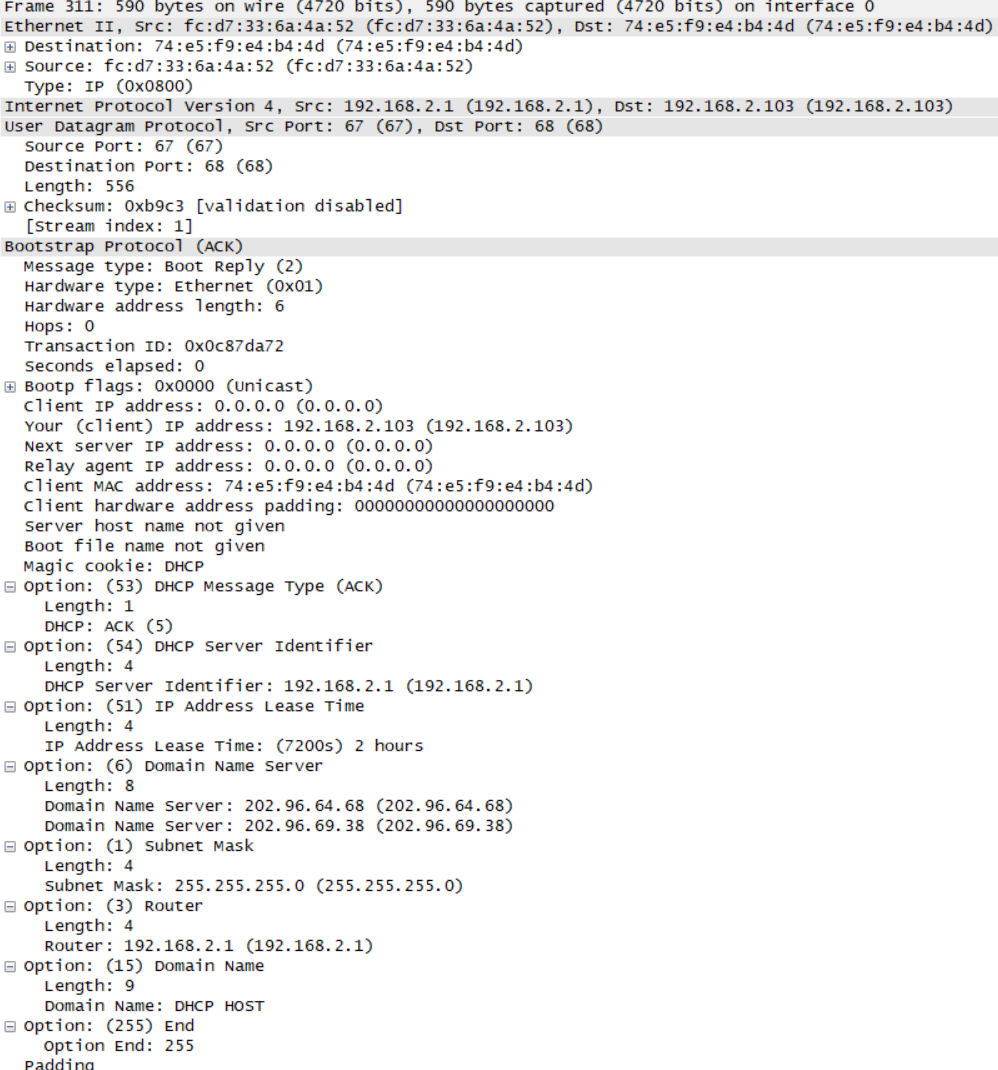
1. (DHCP.pcapng)DHCP协议

[总图]

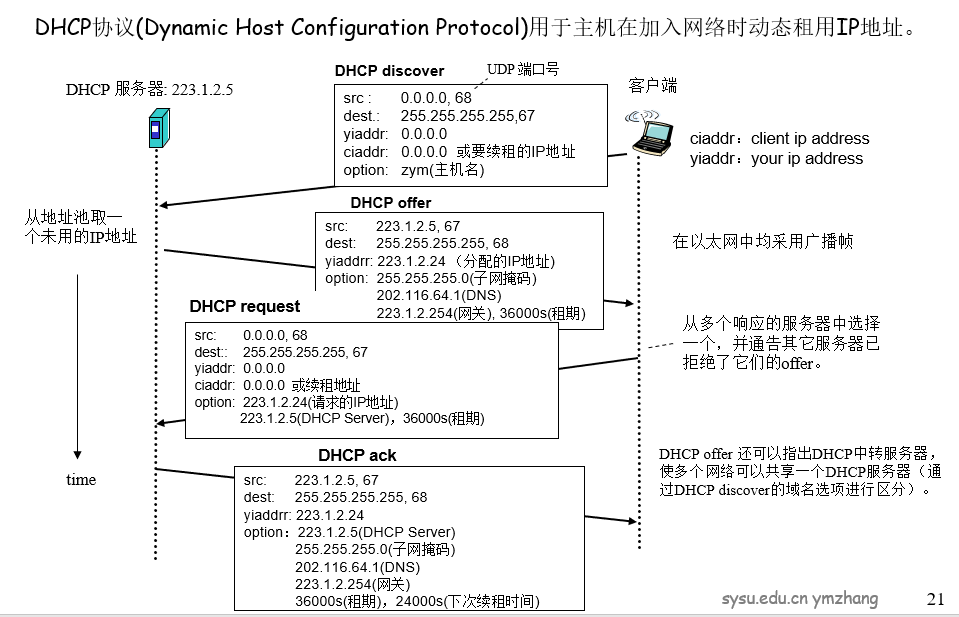


[四个包]

[对照课件]



有没有可以纠正的内容？有的话写出来。

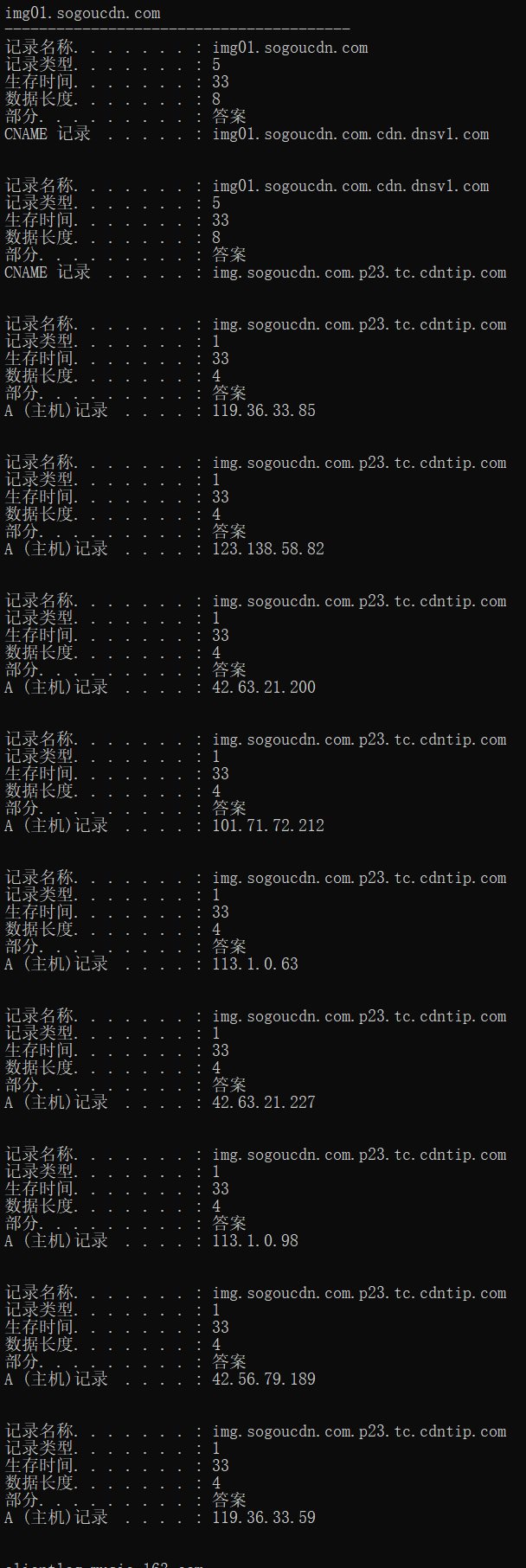
在课件中的DHCP offer中采用的是广播帧，但是在这里我们并没用使用广播而是单播。同时课件上的租期是36000s，而我们这里实际上是7200s.

1. (DNS.pcapng)DNS协议

先ping img01.sogoucdn.com并截屏：



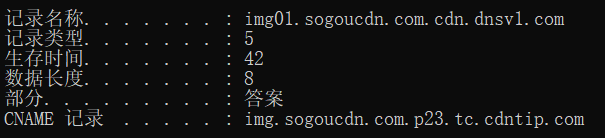
然后，在控制台用C:>ipconfig /displaydns查看DNS缓存，并截屏img01.sogoucdn.com的DNS记录：



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）：



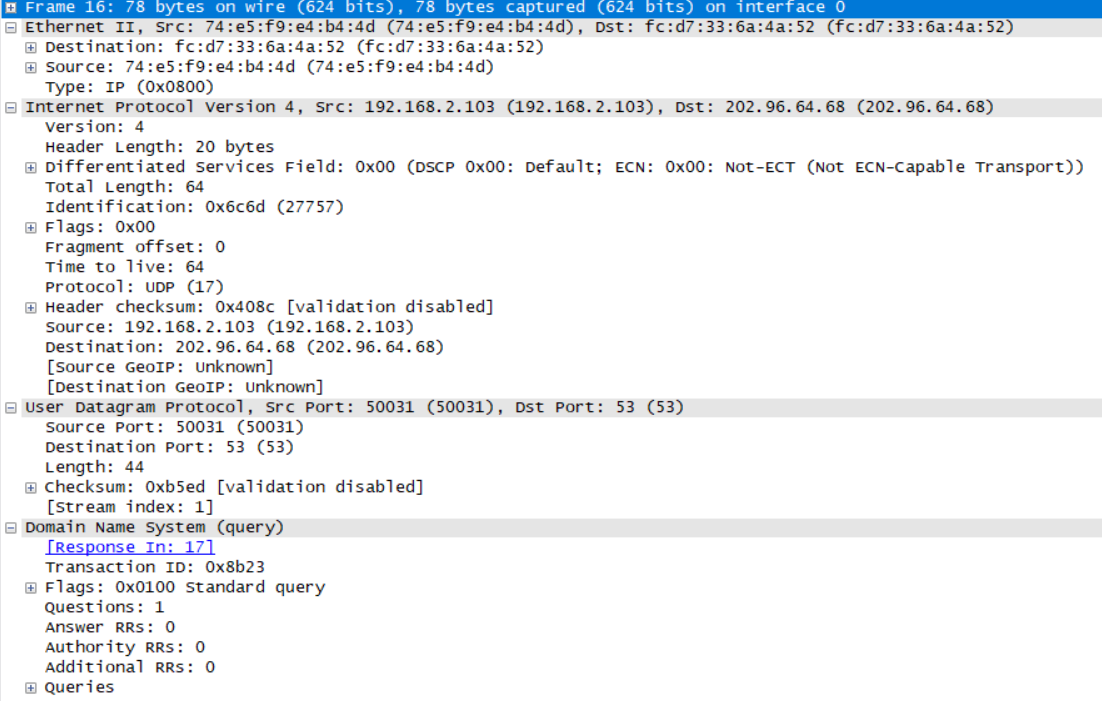
这里说明img01.sogoucdn.com.主机名应该去img01.sogoucdn.com.cdn.dnsv1.com.看，之后的一条记录中



说明DNS查询要到img.sogoucdn.com.p23.tc.cdntip.com这里去查询，接下来的若干条记录就返回了img01.sogoucdn.com的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：

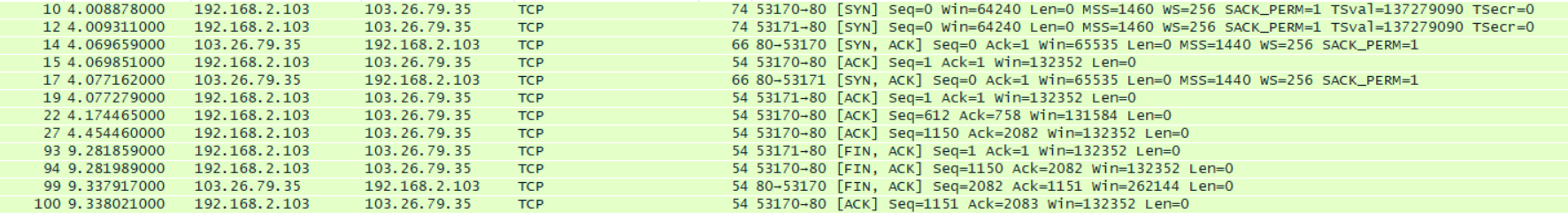
过滤条件：ip.addr==192.168.0.8 and ip.addr==103.26.79.35

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：



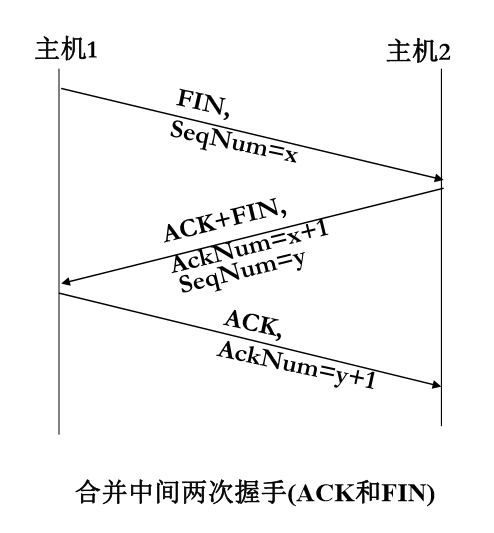
我们可以看到三次握手首先我的电脑IP先发出SYN连接请求，SEQ = 0；

之后103.26.79.35做出响应，SEQ = 0，ACK = 0+1 = 1；

之后第三次握手，我们的电脑IP回应ACK，ACK = 0 + 1 = 1；

四次挥手：

我们这里恰巧变成了三次挥手，就是课件上这样的情况



对应的数据包如下所示



我们可以看见第一个包多了一个ACK，这个ACK是对上面传送的数据的ACK，在这里就直接合并了（我猜测是开启了捎带确认）。

首先192.168.2.103也就是我们的电脑发出FIN报文，SEQ = 1150；（一次挥手）

之后103.26.79.35发出ACK同时也发出FIN报文，ACK= 1150 + 1 = 1151 ，SEQ = 2082；（两次挥手）

最后192.168.2.103发出ACK，ACK = 2082 + 1 = 2083；（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）。

在做DHCP抓包的时候遇到了问题，就是每次手动断开网络连接都只能抓到request和ack包，但是抓不到discover和offer包。查阅资料后采取的策略是在cmd输入“ipconfig/release”指令，这样就会自动断开网络的连接过一段时间再自己连上，但是这个自己连上的时间很长要等很久，所以最后是先在控制台输入指令断开连接，然后再手动连上网络，这下就能抓到四个包了。

【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）