院 系 数据科学与计算机学院 学号　18340013 姓名 陈琮昊

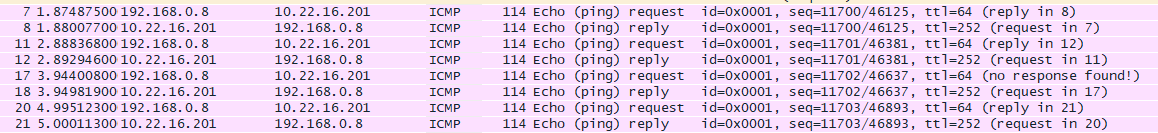
班 级 计科一班

【实验题目】WireShark**实验**

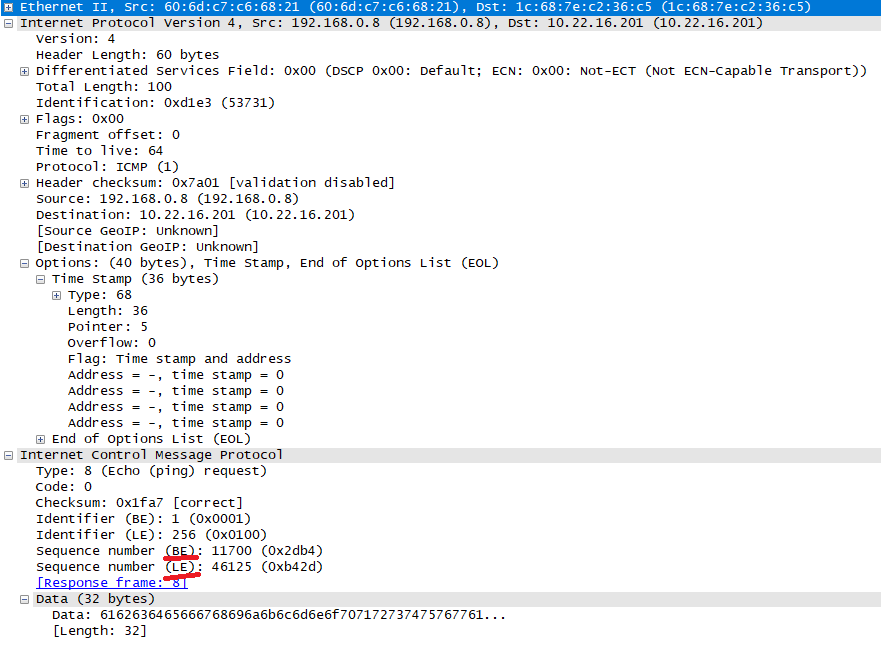
【实验目的】通过WireShark分析IP协议(Option)、ICMP协议、ARP协议、DHCP协议、DNS协议、TCP协议。

【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）。

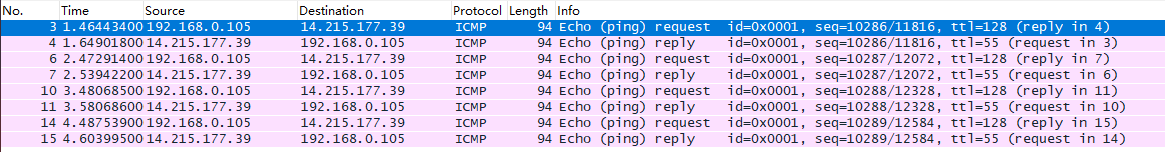
注意每一步都要保存截包文件

【实验任务】

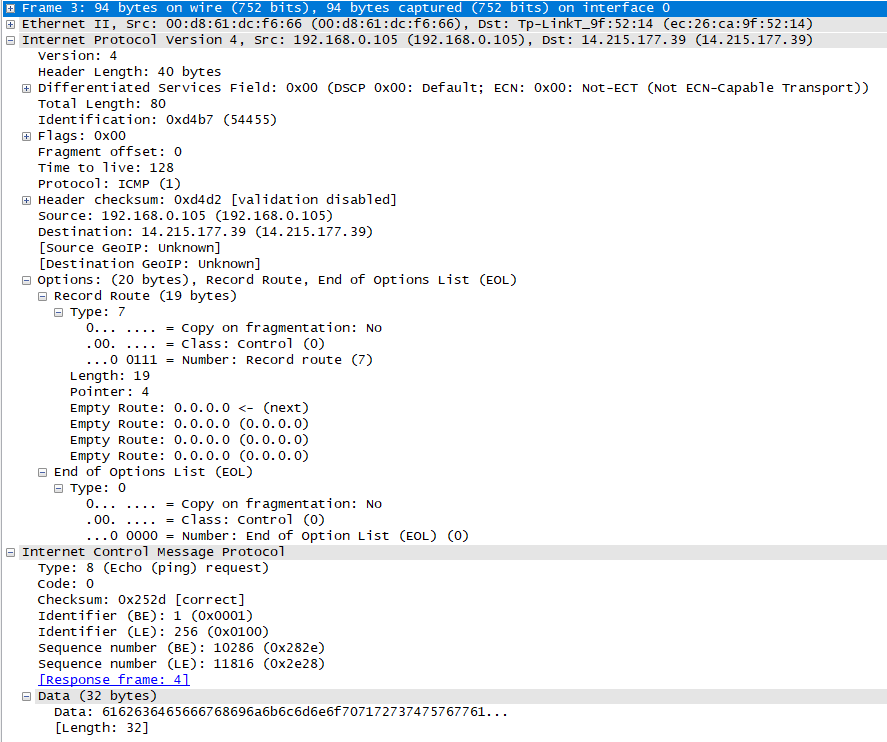
1. (IP.pcapng)IP Option和ICMP协议。

**命令：ping -r 4域名**

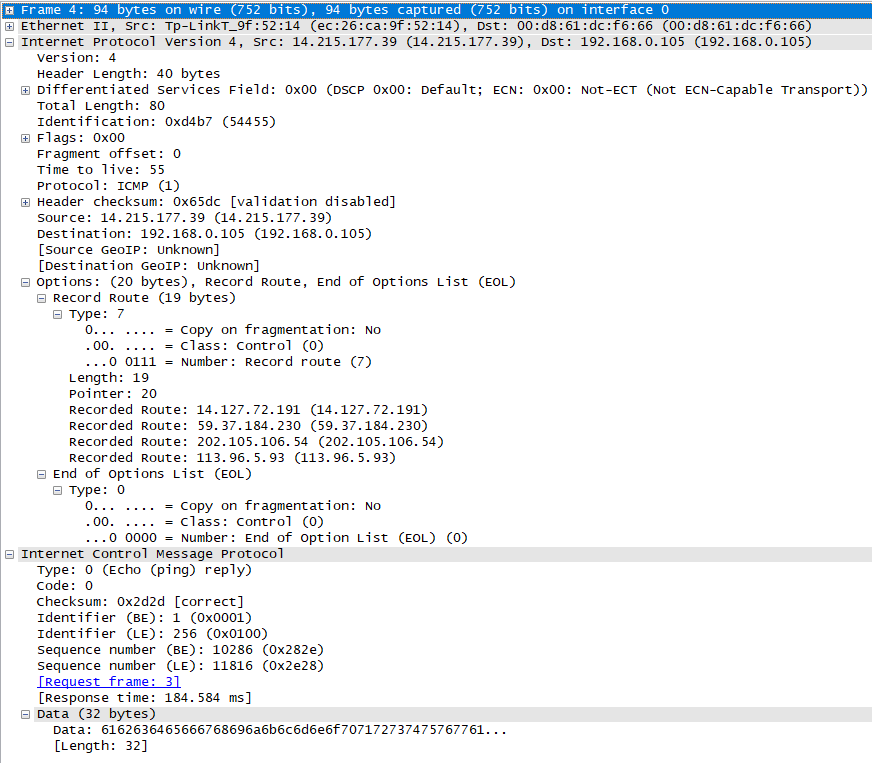
[Ping总图]



[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：20bytes

ICMP包的Identifier：1

ICMP包的序号：10286

ICMP包的数据部分长度：32bytes

ICMP包的数据部分的内容：

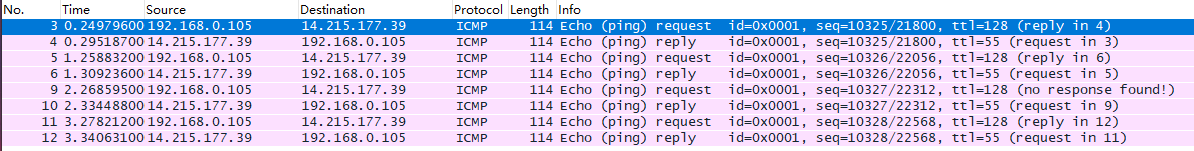
6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

Identifier是什么含义？

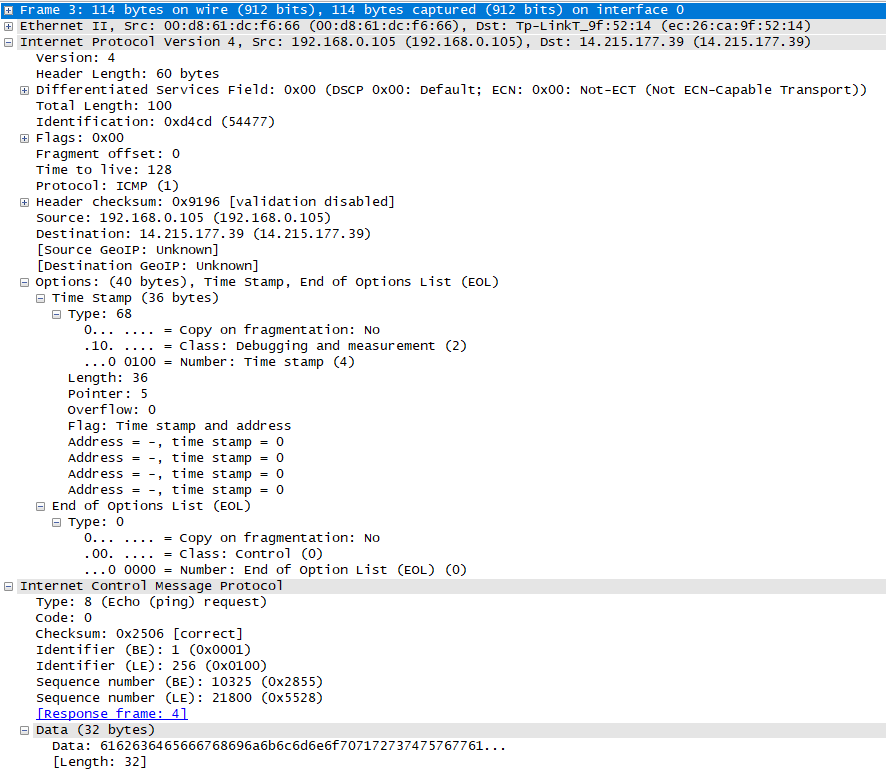
标识符和序列号用于匹配回显应答和回显请求，标识符确定该报文的发送者，序列号关联对应的请求报文和应答报文。

**命令：ping -s 4域名**

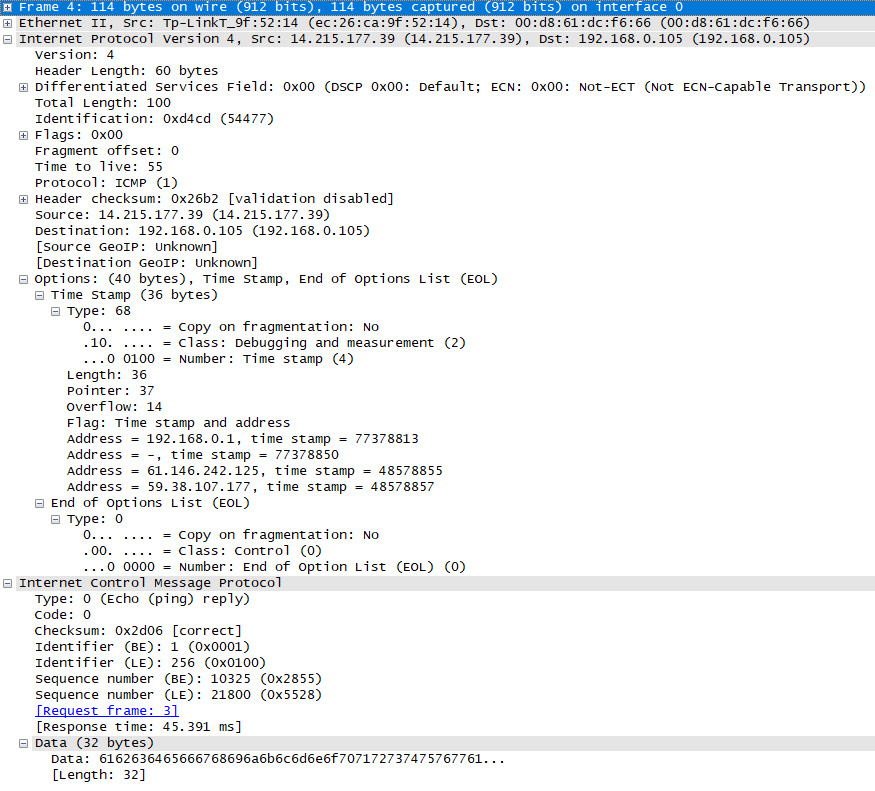
[Ping总图]



[Ping请求包截屏]



[Ping响应包截屏]



[问题]

IP选项的长度：40bytes

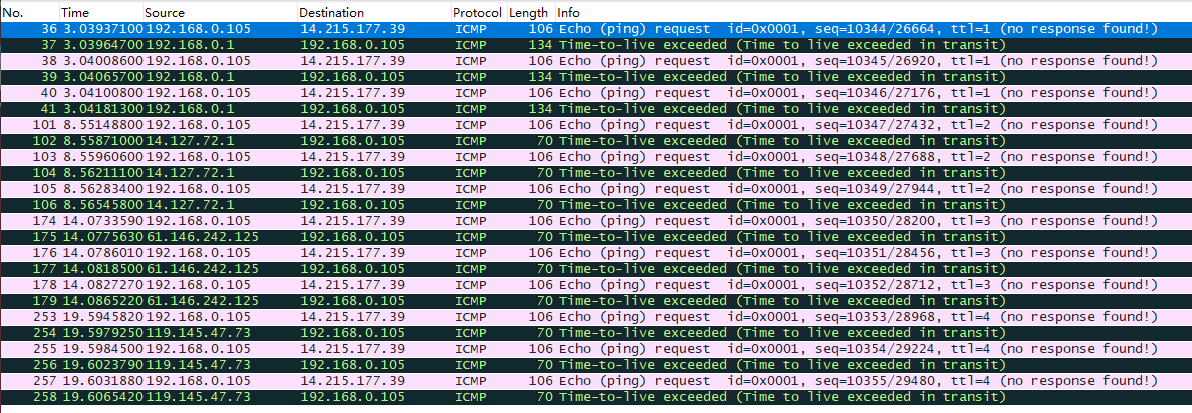
选项中的时间戳是否正确？

错误，77378813转换后是1972-06-14 22:06:53。

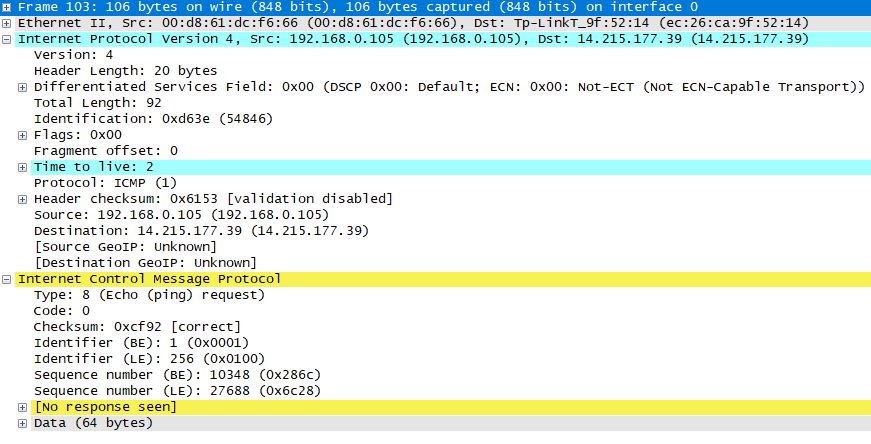
1. (tracert.pcapng) ICMP协议

命令：tracert -h 4 域名

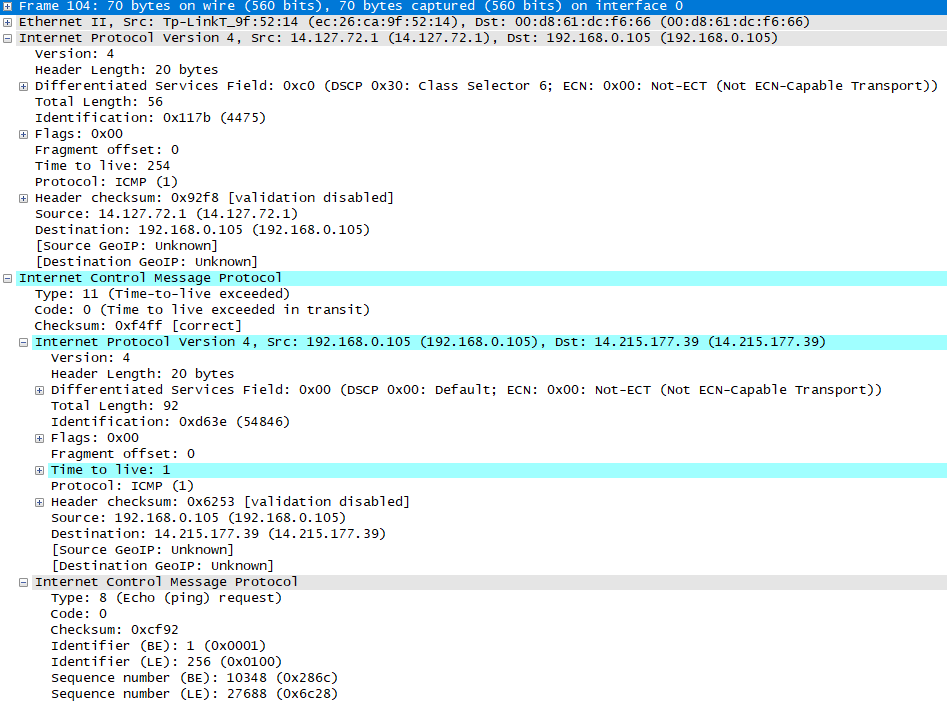
[tracert总图截屏]



[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]



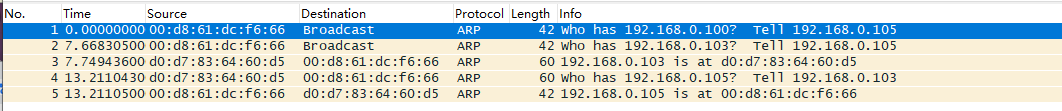
1. (arp.pcapng)ARP协议。

命令：arp –a

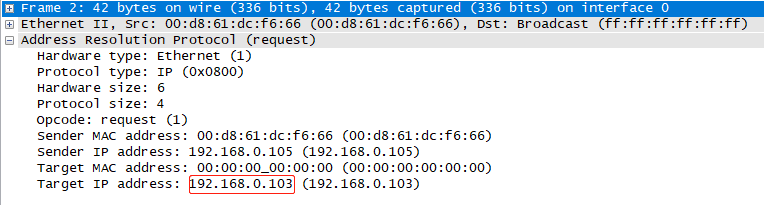
arp –d 192.168.0.14

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

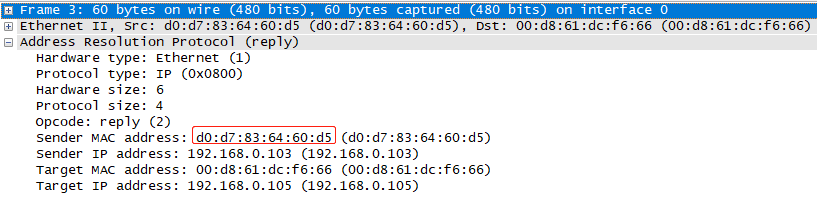
[总图]



[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]

\* 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？

使用ARP协议在当前网络中广播ARP分组请求对应IP地址的MAC地址。

ARP协议是否采用了超时重传？

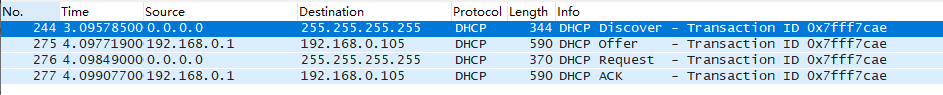
ARP协议没有超时重传机制，超时没有收到响应则丢弃引发ARP查询的IP分组。

Gratuitous ARP包有什么用途？

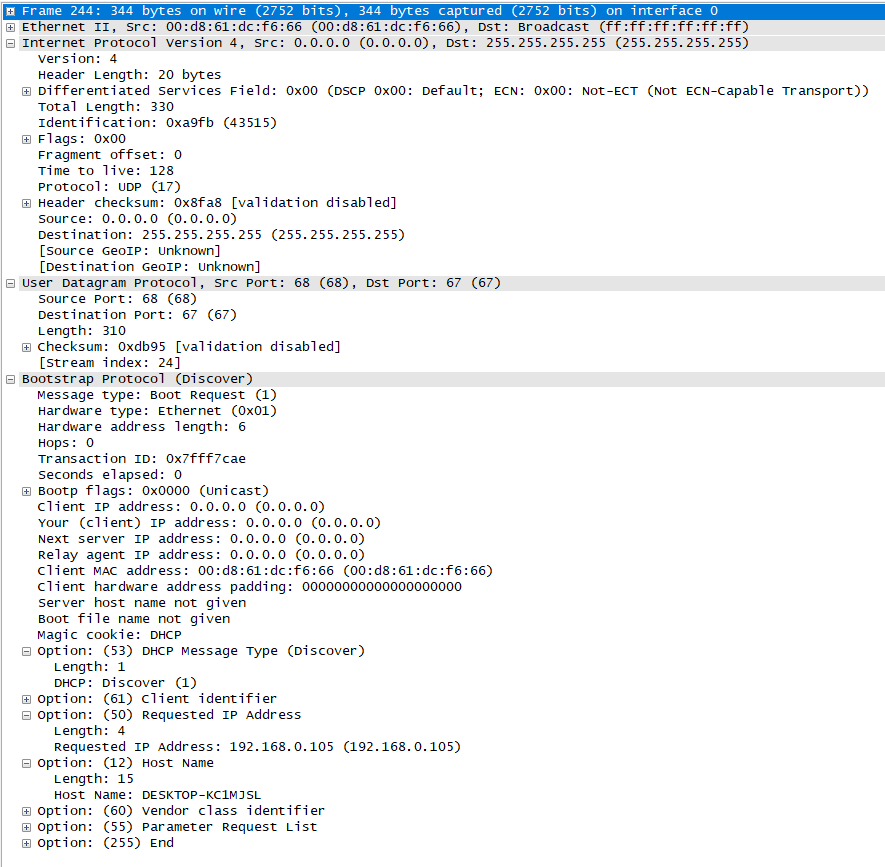
当主机启动的时候，将发送一个Gratuitous ARP请求，请求自己的IP地址的MAC地址。

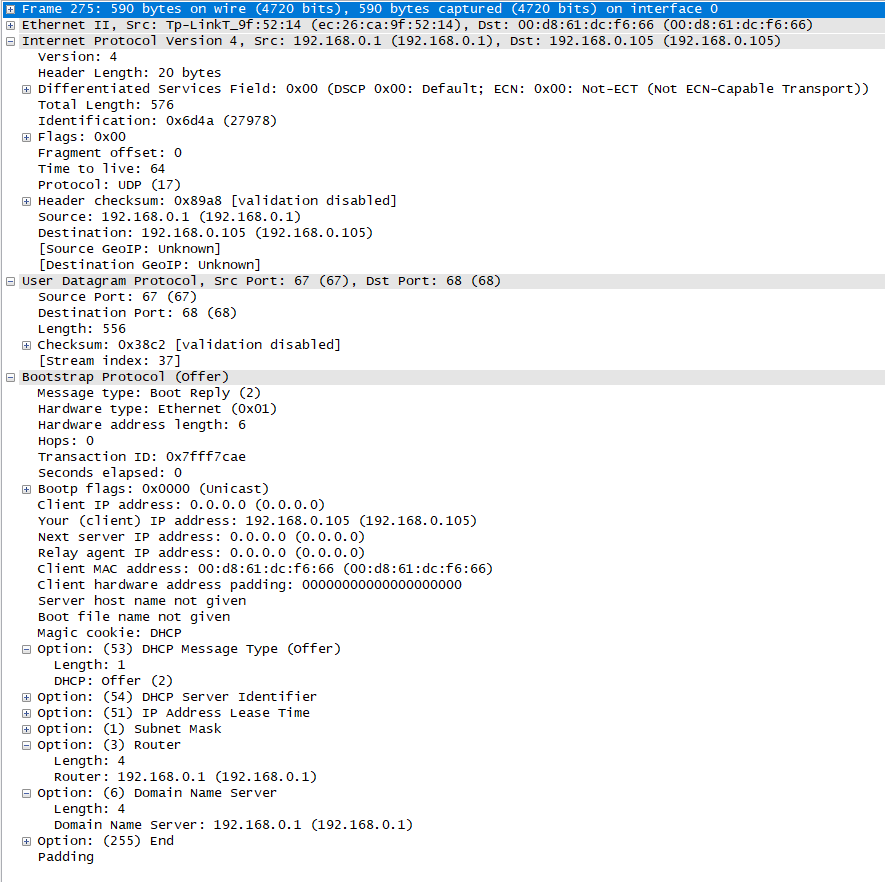
1. (DHCP.pcapng)DHCP协议

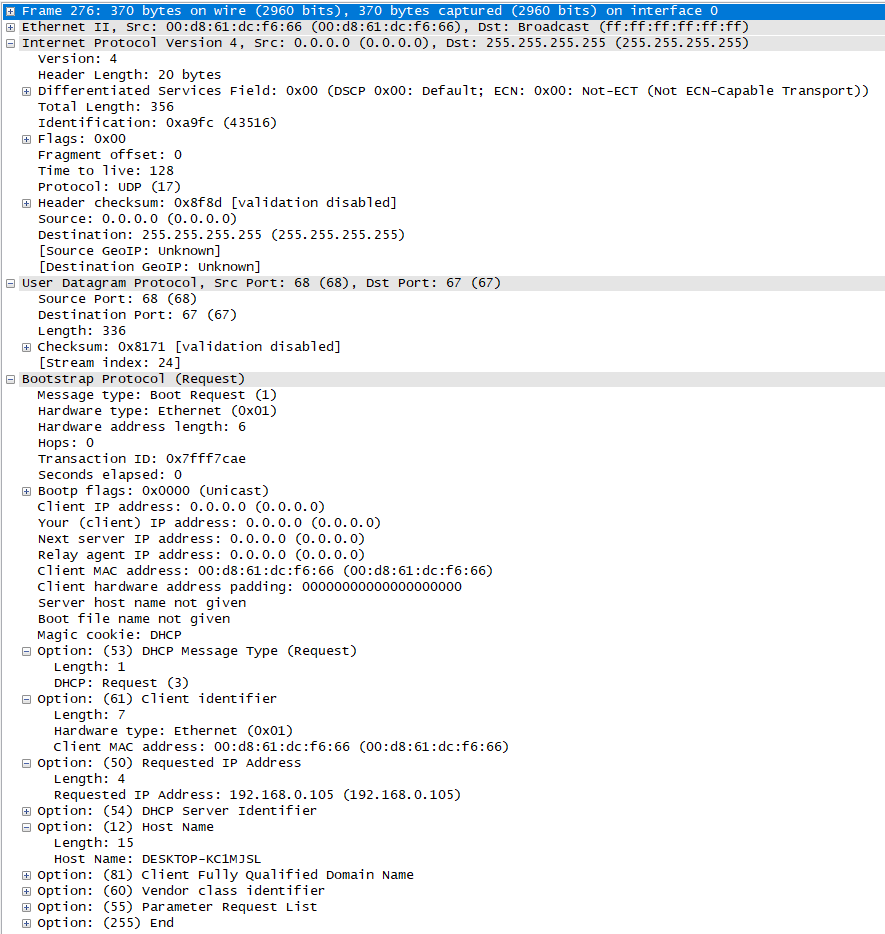
[总图]

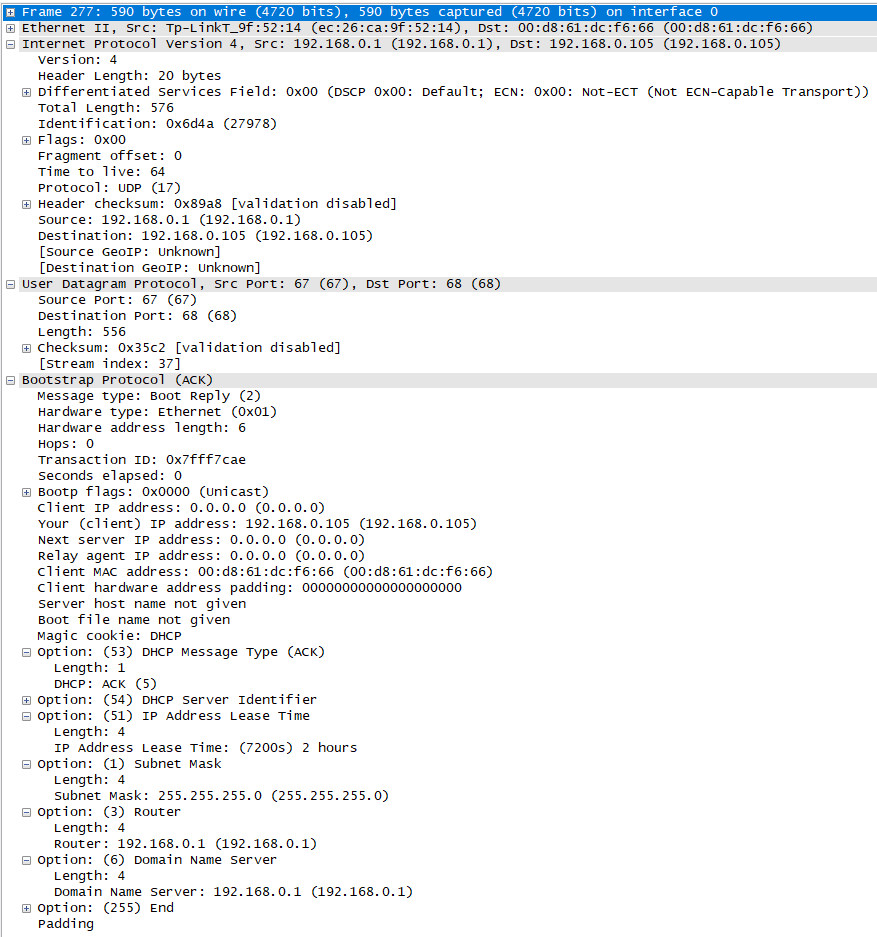


[四个包]

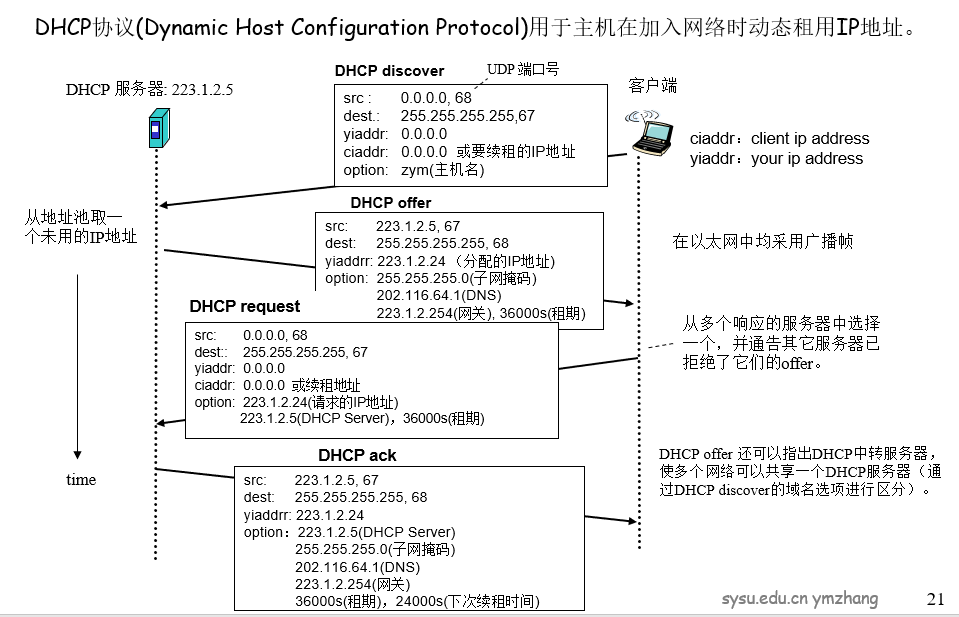








[对照课件]



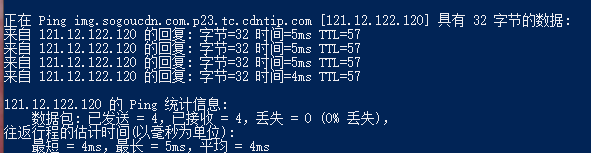
有没有可以纠正的内容？有的话写出来。

OFFER分组中的

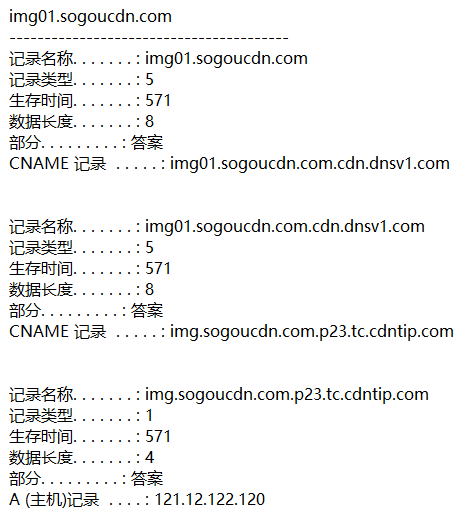
由DHCP服务器发送的offer分组的目标ip地址不是255.255.255.255，而是DHCP服务器分配的用户ip地址192.168.0.105。

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：

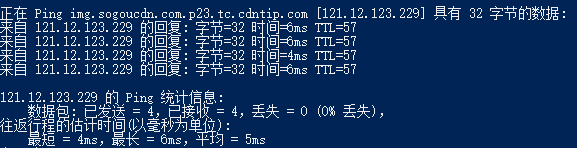


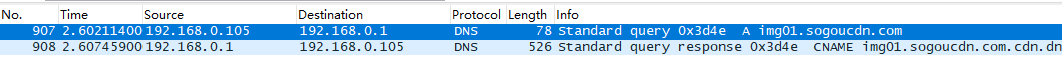
解释其中内容（说明如何可以从DNS记录中得到img01.sogoucdn.com的IP地址）：

img01.sogoucdn.com -> img01.sogoucdn.com.cdn.dnsv1.com ->

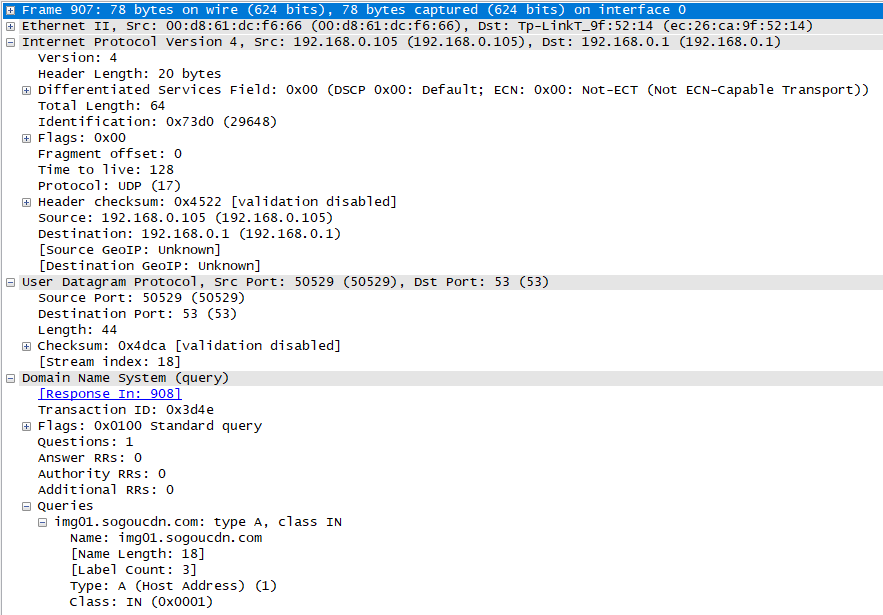
img.sogoucdn.com.p23.tc.cdntip.com -> 121.12.122.120

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

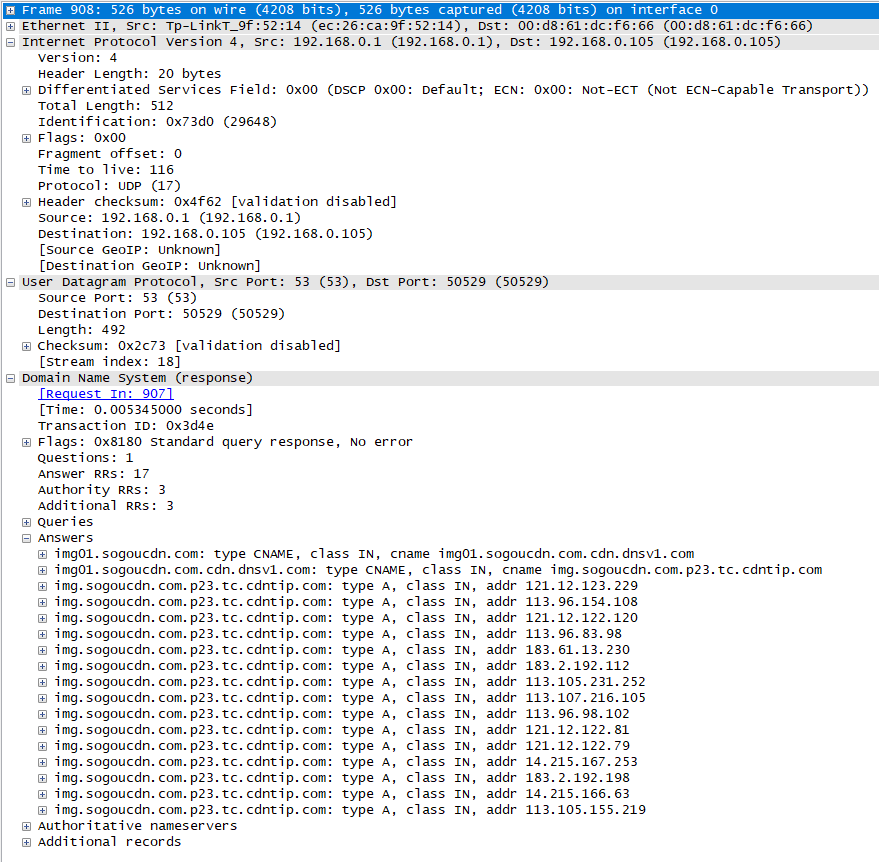




[DNS查询包]



[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：

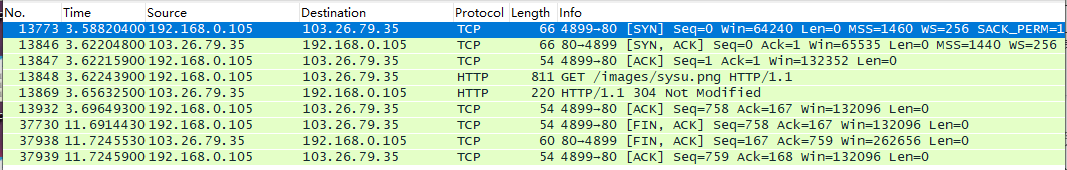
过滤条件：ip.addr==192.168.0.8 and ip.addr==103.26.79.35

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 -> 第一次No.13773:SYN 第二次No.13846:SYN+ACK 第三次No.13847:ACK

四次挥手关闭连接 -> 第一次No.37730:FIN+ACK 第二次和第三次合并No.37938:FIN+ACK

第四次No.37939:ACK

【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】

在WireShark使用过程中有非常多的小问题，例如显示过滤器和抓包过滤器是不同的，在显示过滤器中我们可以使用dhcp之类的关键字，而在抓包过滤器中能够限定的关键字不多，主要还是使用显示过滤器过滤出我们想看的包。此外，ipconfig /displaydns命令所显示的内容较多，我们需要的网址dns映射在命令行窗口中会被覆盖掉，我们可以通过>命令将内容输出到一个.txt文本中，然后再截屏方便操作。

【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）