院 系 数据科学与计算机学院 学号　18340057 姓名

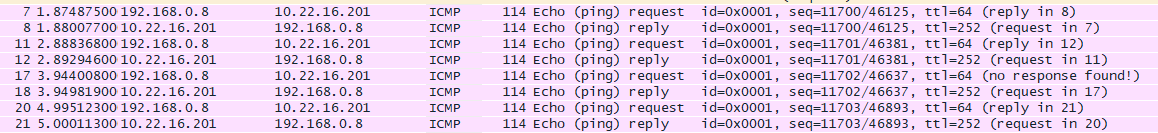
班 级 18级计算机科学二班

【实验题目】WireShark**实验**

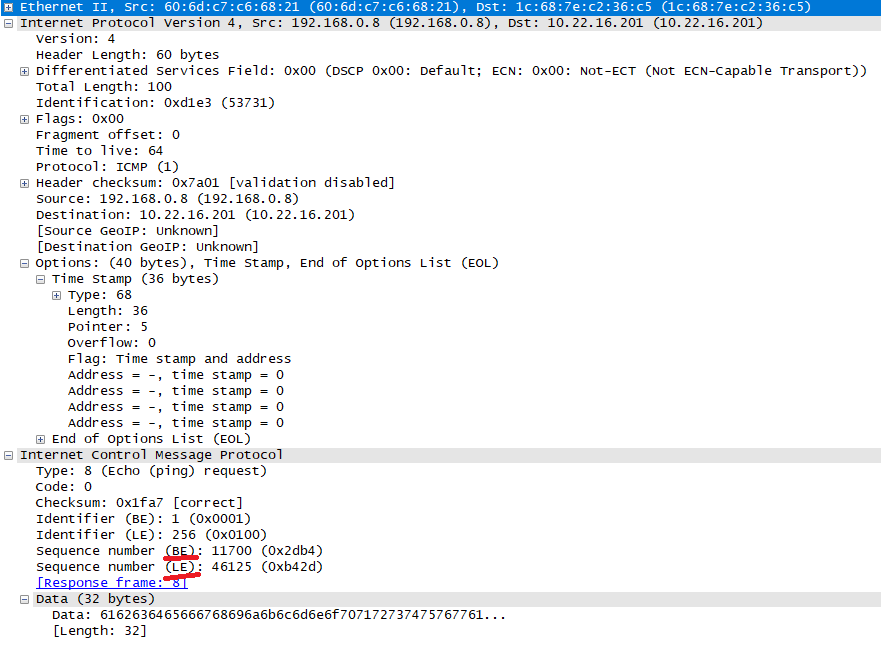
【实验目的】通过WireShark分析IP协议(Option)、ICMP协议、ARP协议、DHCP协议、DNS协议、TCP协议。

【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）。

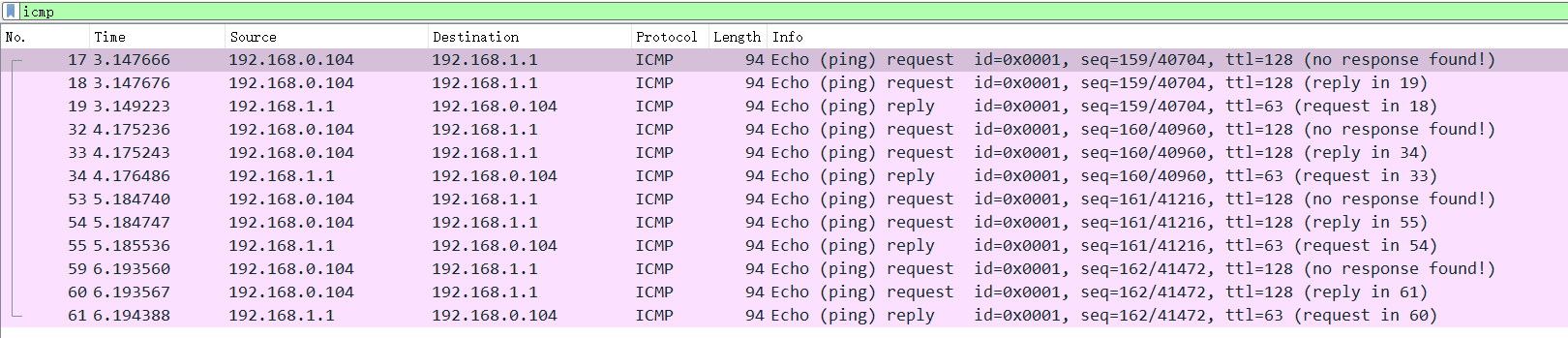
注意每一步都要保存截包文件

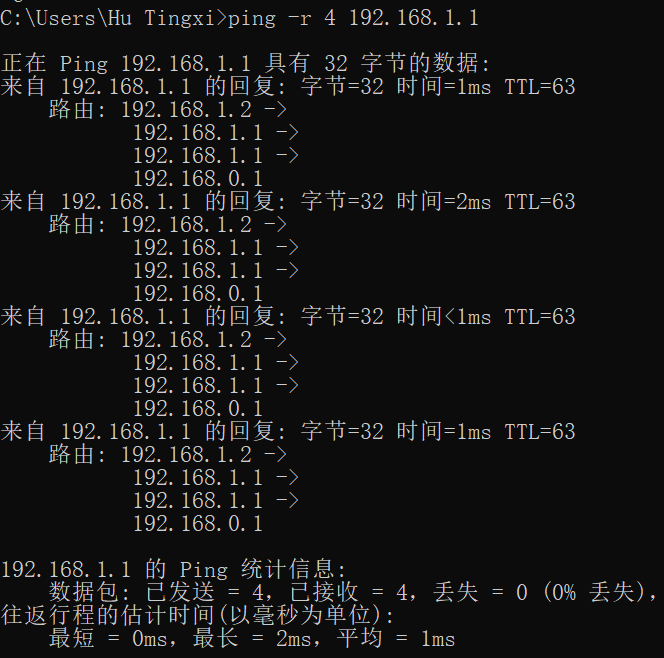
【实验任务】

1. (IP.pcapng)IP Option和ICMP协议。

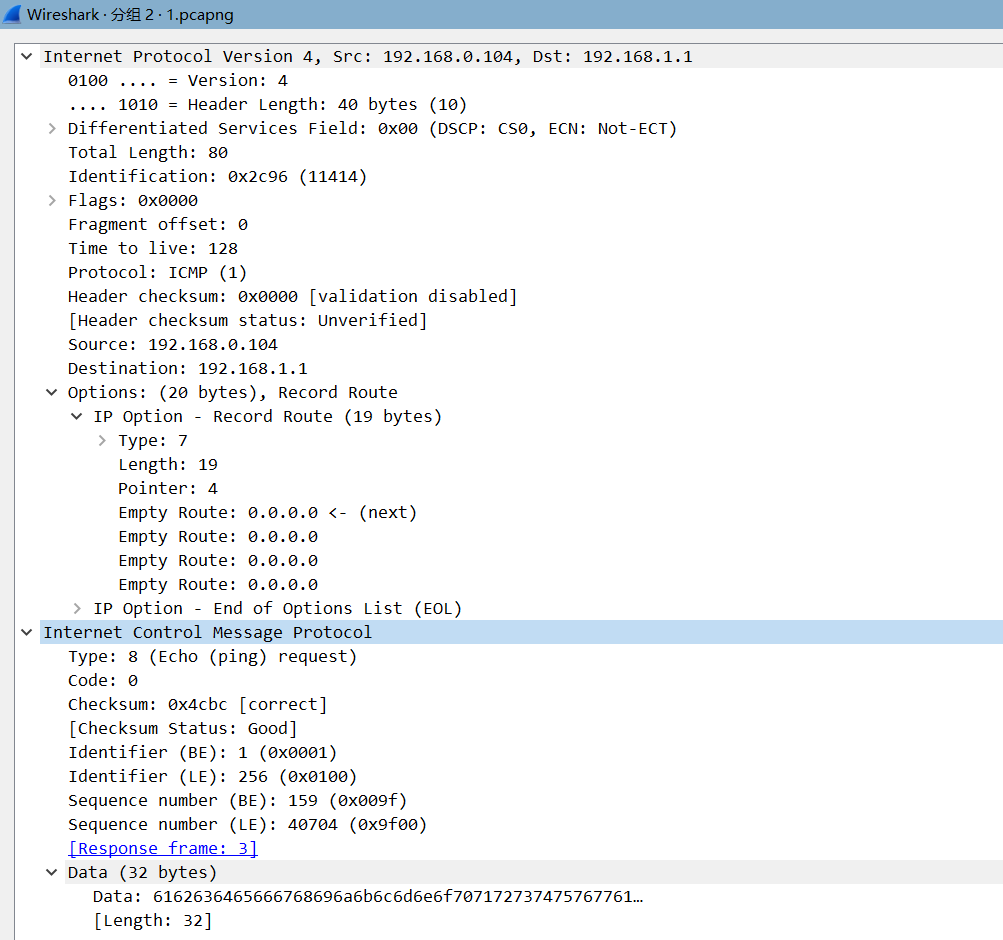
**命令：ping -r 4域名**

[Ping总图] **ping -r 4 192.168.1.1**

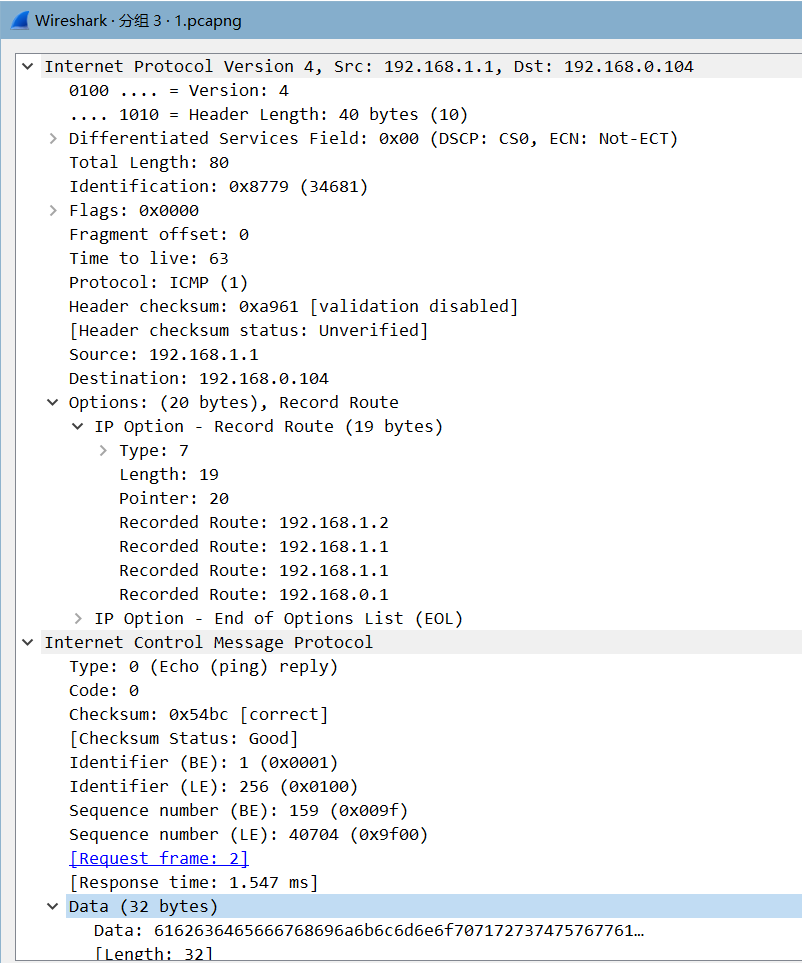




[Ping请求包截屏]



[Ping响应包截屏]



[针对于所截包的问题]

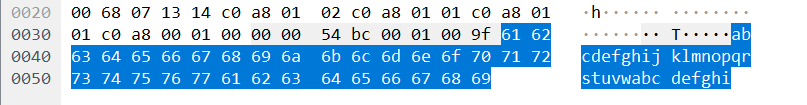
IP选项的长度：20 bytes(19 bytes的路由记录和1 bytes的EOL)

ICMP包的Identifier：BE:1，LE:256

ICMP包的序号：BE:159，LE:40704

ICMP包的数据部分长度：32 bytes

ICMP包的数据部分的内容：a到z的字母循环。截图如下：



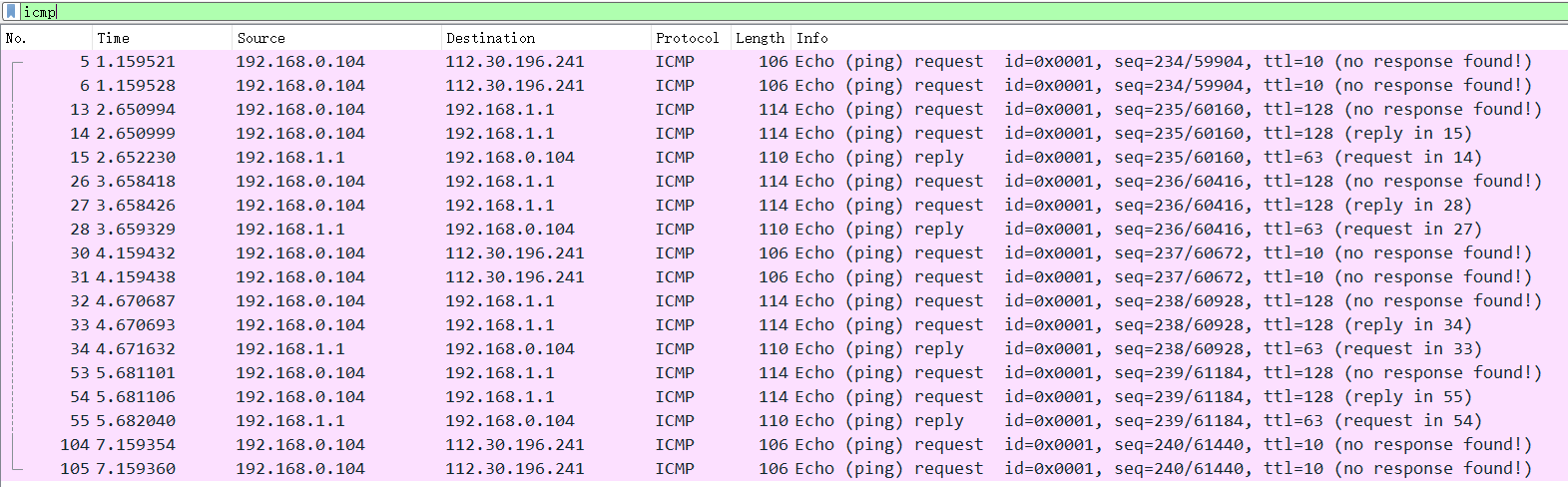
Identifier是什么含义？

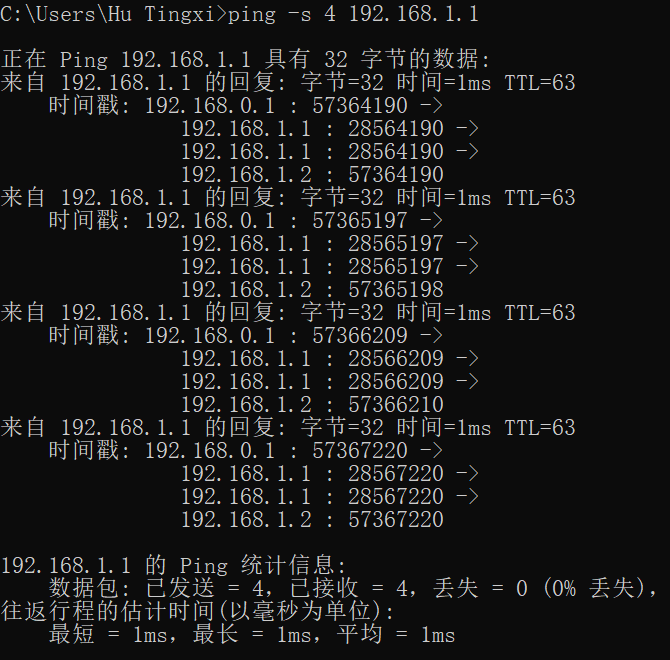
Identifier用于给当前包赋予一个id，使得主机能够区分不同的ping进程。经网上查阅资料，我得知，在linux系统下，icmp包的identifier即为当前进程号，而在windows系统下，identifier是固定的值，因为windows系统不用identifier而是sequence number区分进程。

**命令：ping -s 4域名**

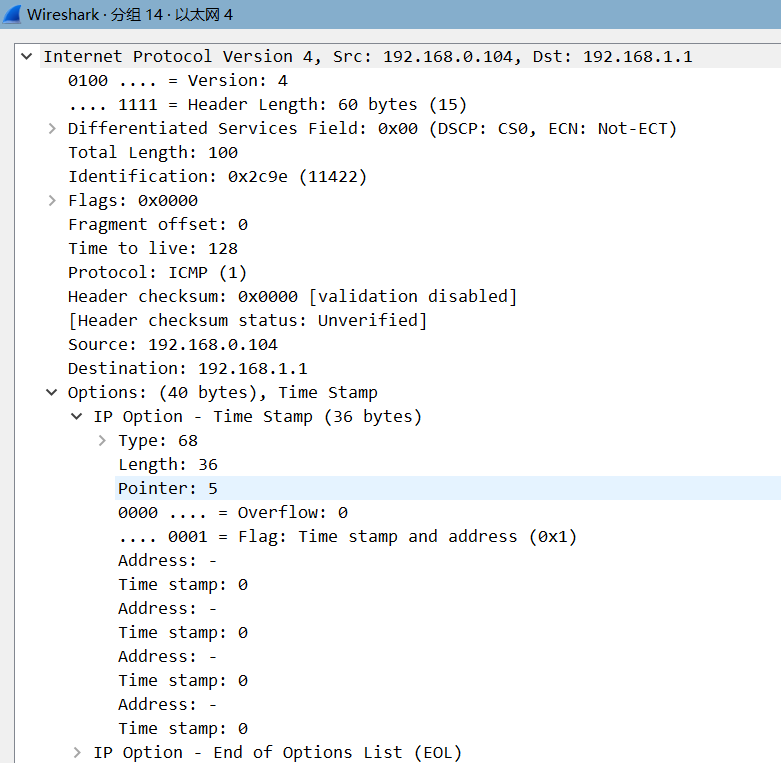
**(这里我另外使用了文件IP2.pcanpg保存)**

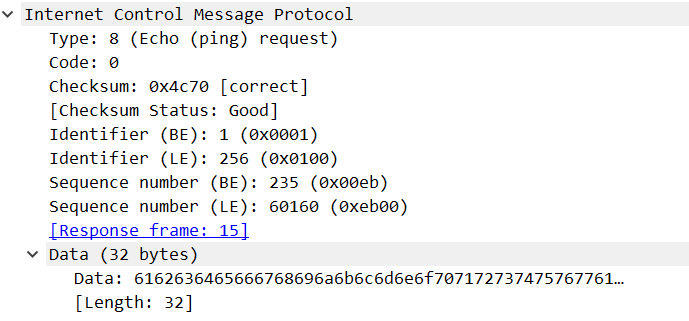
[Ping总图] **ping -s 4 192.168.1.1**



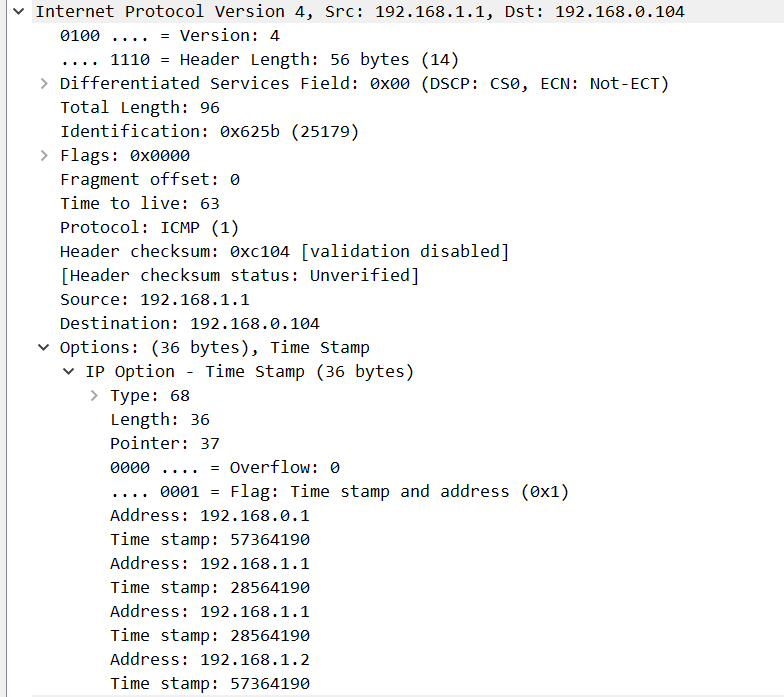


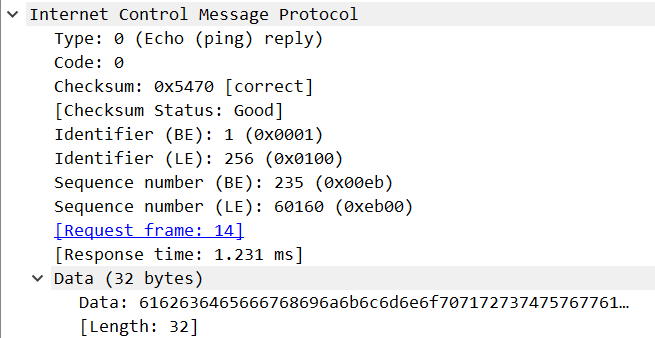
[Ping请求包截屏]





[Ping响应包截屏]





[问题]

IP选项的长度：请求包40bytes，响应包36bytes，时间戳各占36bytes。

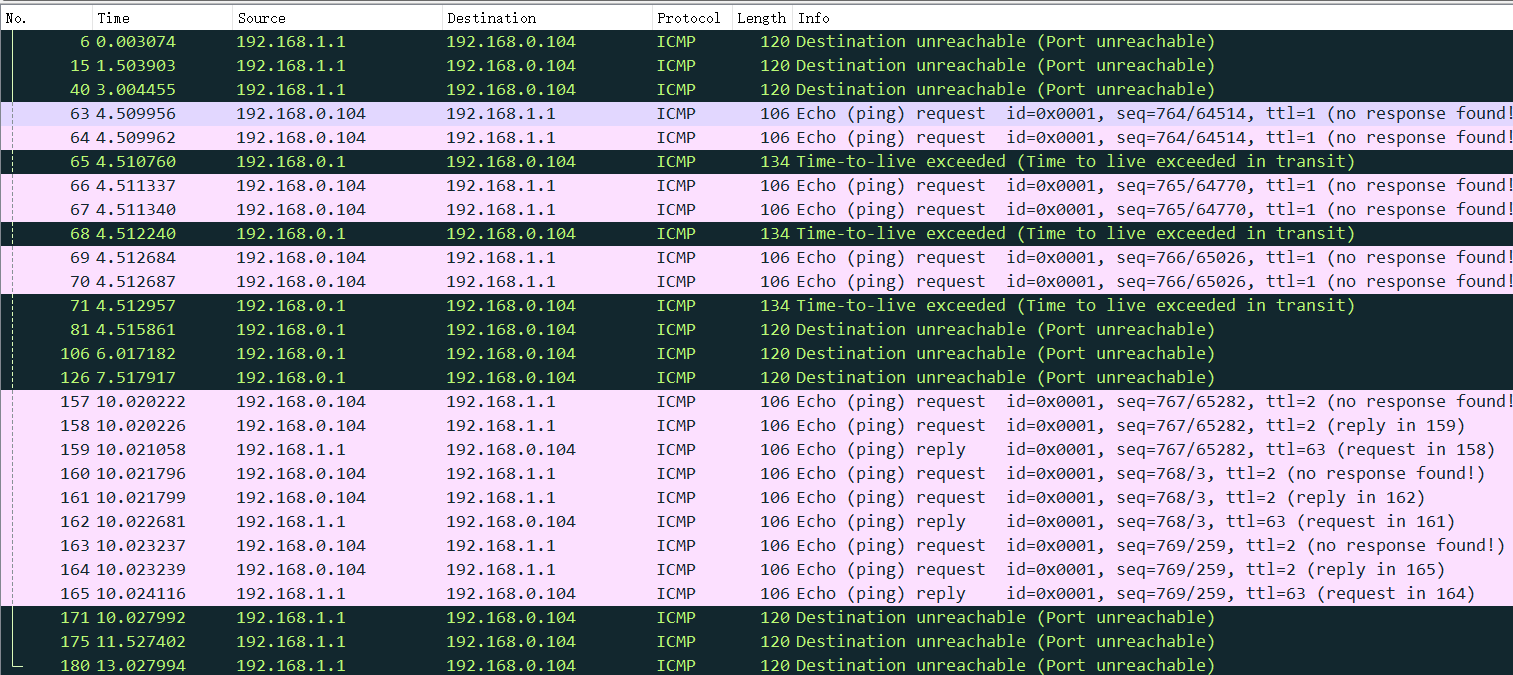
选项中的时间戳是否正确？正确

1. (tracert.pcapng) ICMP协议

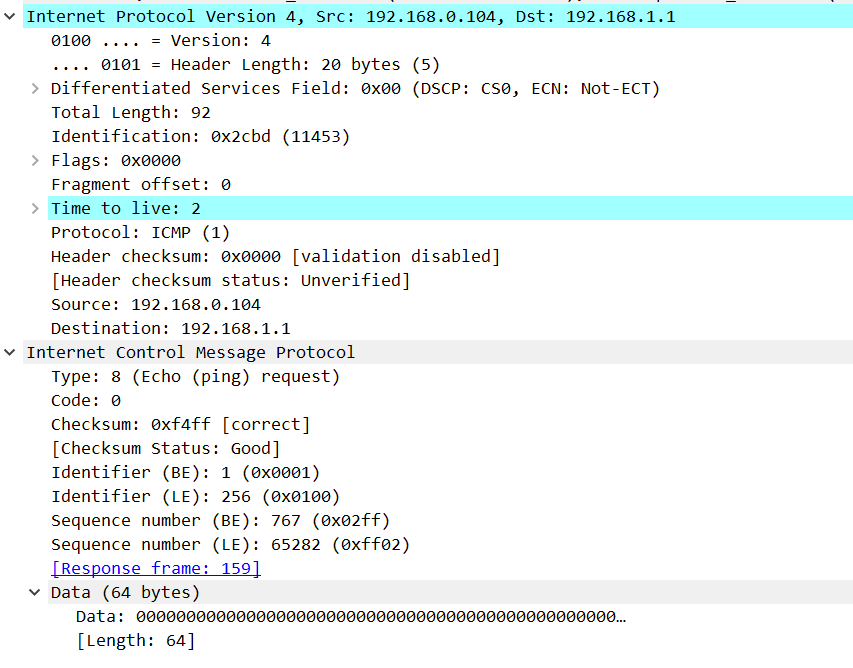
命令：tracert -h 4 域名

tracert -h 4 192.168.1.1

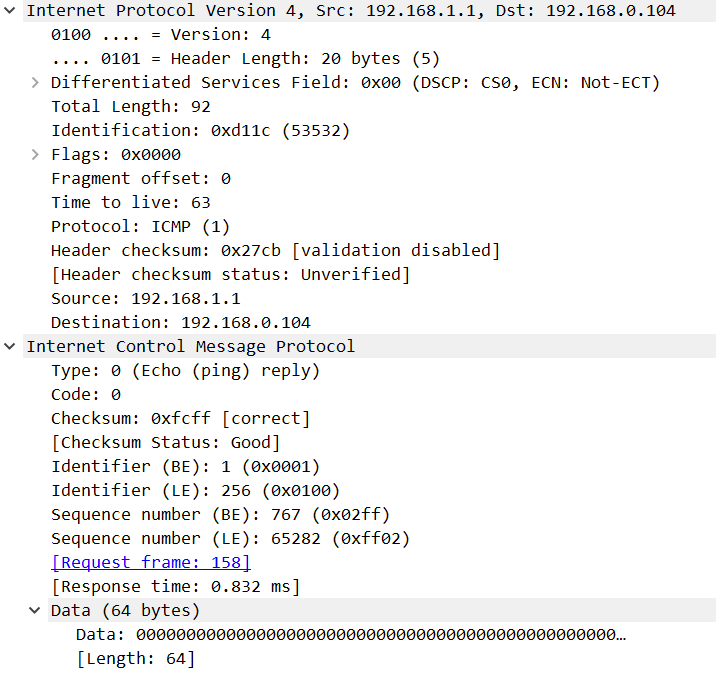
[tracert总图截屏]



[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]



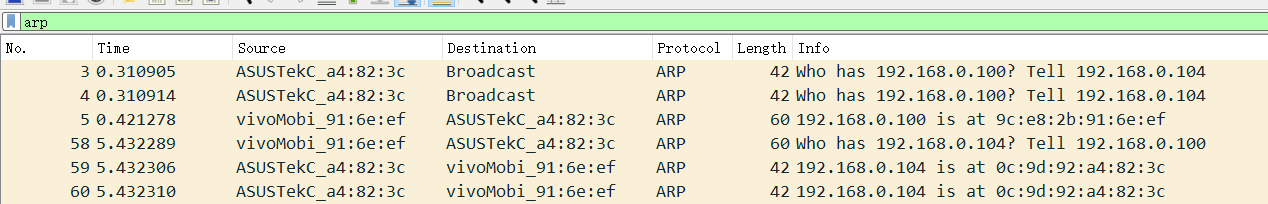
1. (arp.pcapng)ARP协议。

命令：arp –a

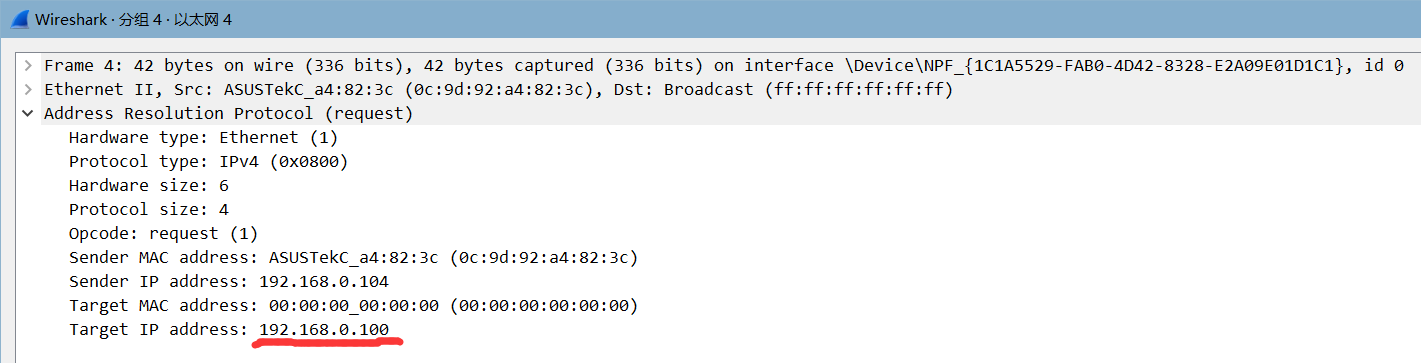
arp –d 192.168.0.14

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

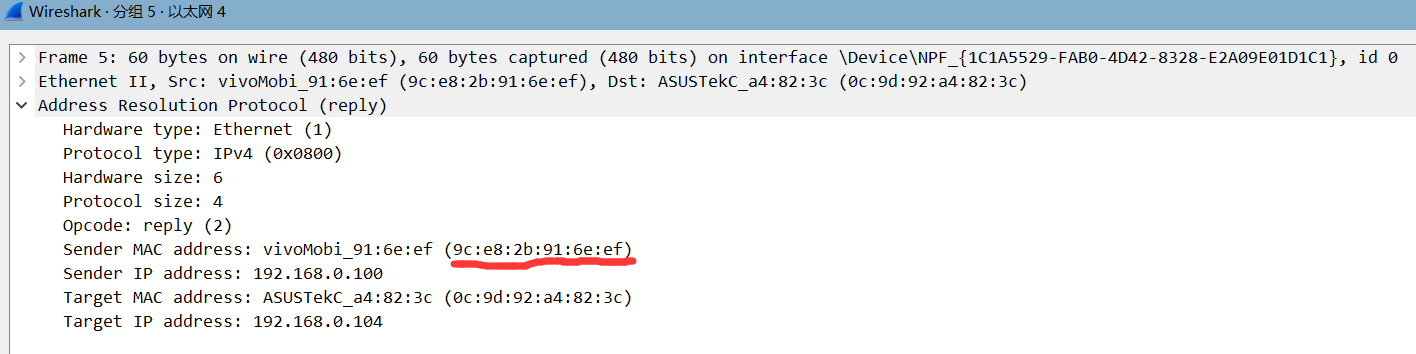
[总图]



[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？

系统会发送arp包询问要发送的ip分组的设备的mac地址。

ARP协议是否采用了超时重传？

采用了。

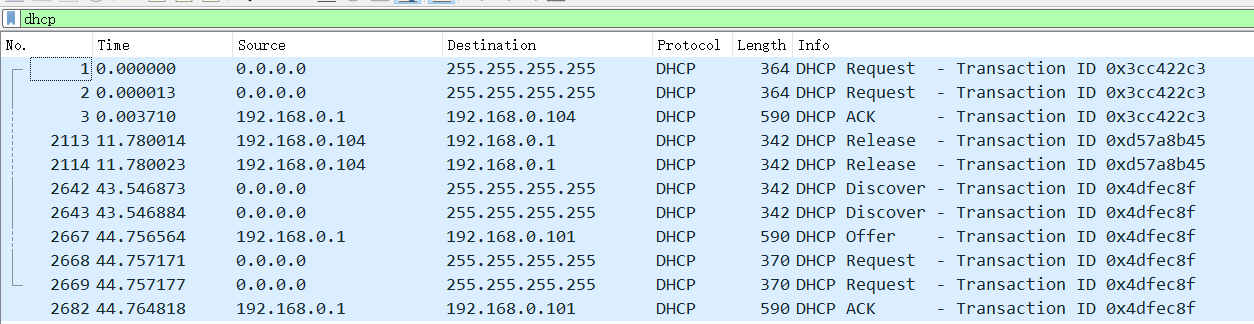
Gratuitous ARP包有什么用途？

Gratuitous ARP包会请求自己的ip的mac地址，以此确定是否还有其他主机设置了相同的ip地址，同时如果发送Gratuitous ARP包的主机的mac地址改变了，还可以更新其他主机中的arp缓存。

1. (DHCP.pcapng)DHCP协议

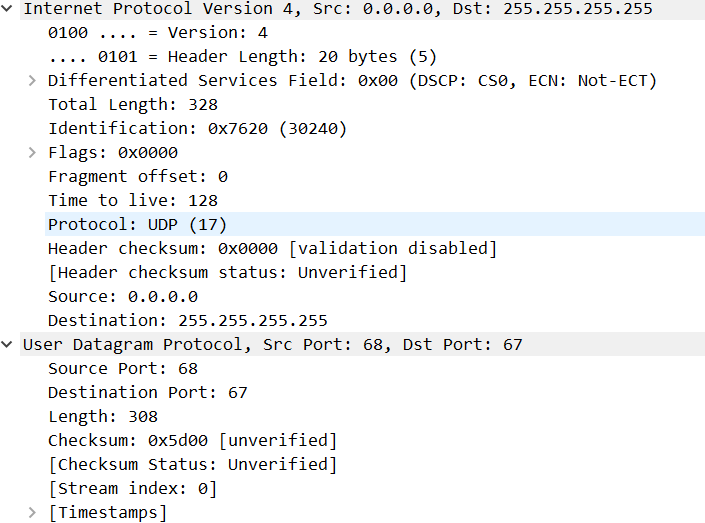
特别说明：每次联网时我的主机会因为有之前的连接记录，会直接发送request包。因此我在连接后使用ipconfig/release命令释放连接，并重新连接网络。下图在release包后面的四种包才是本步骤需要获得的包。

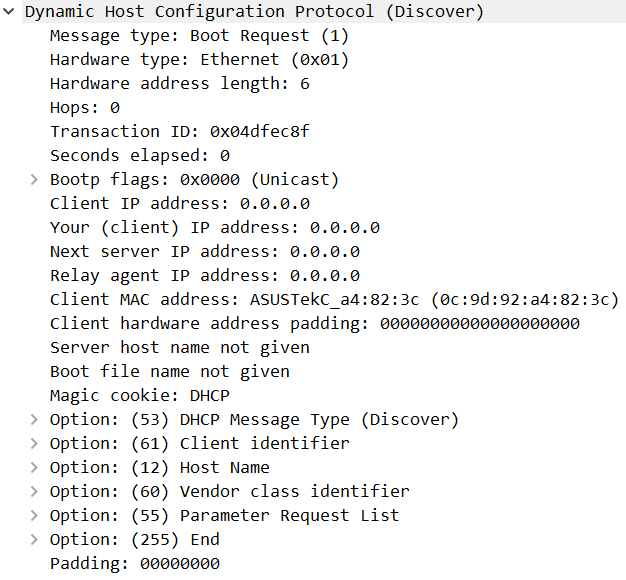
[总图]



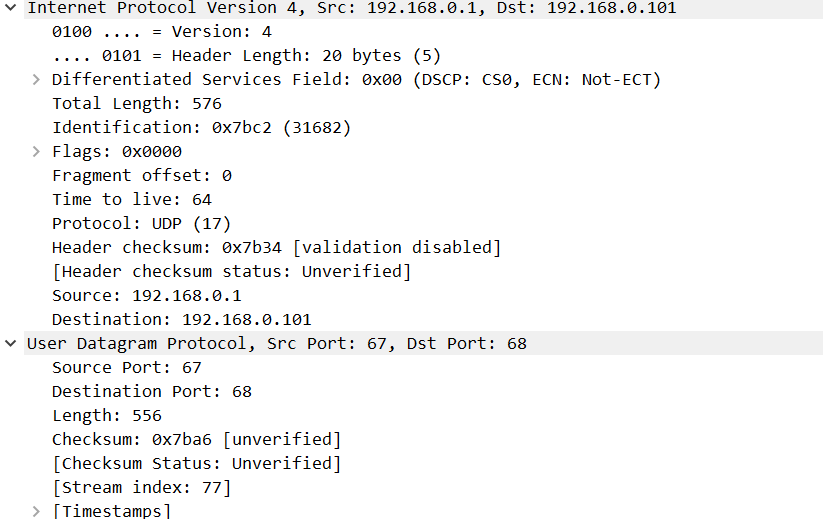
[四个包]

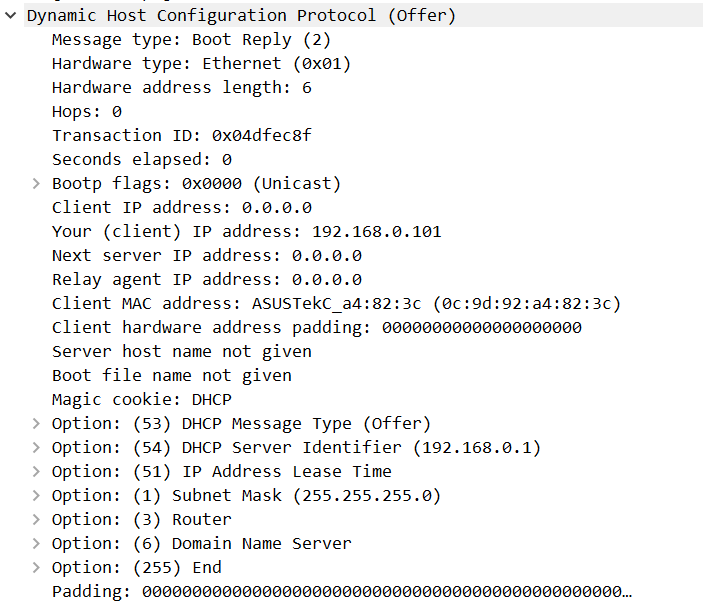
Discover:



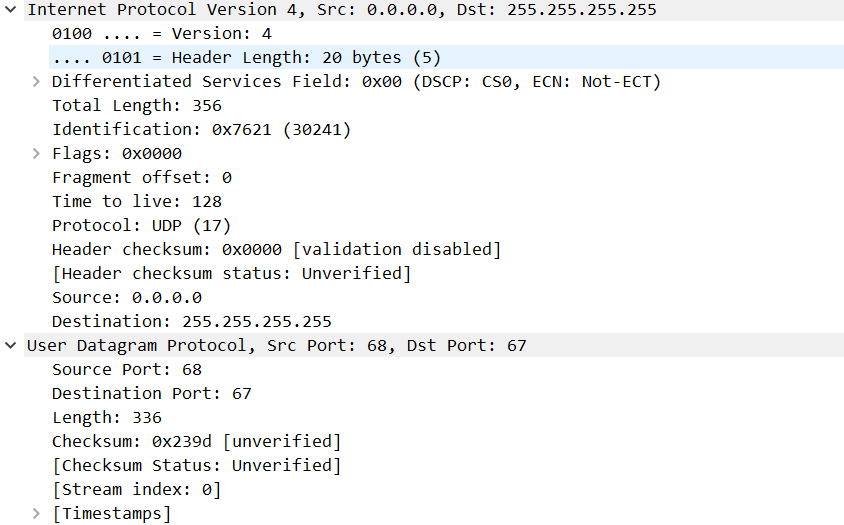


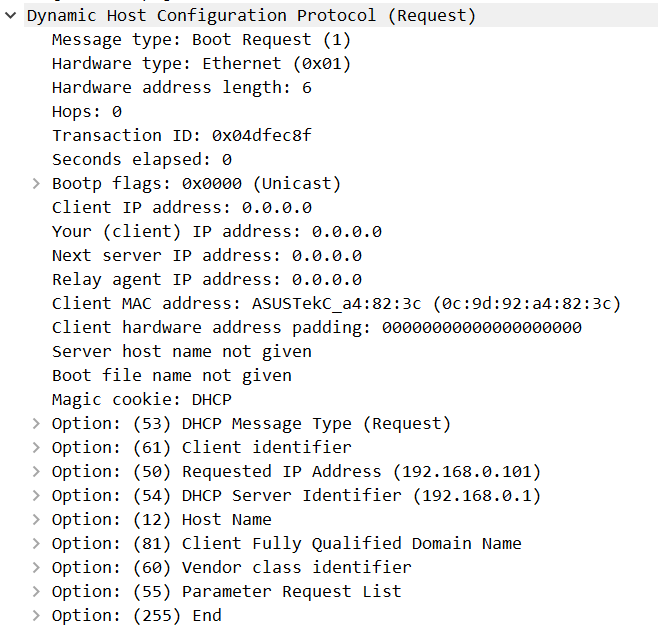
Offer:



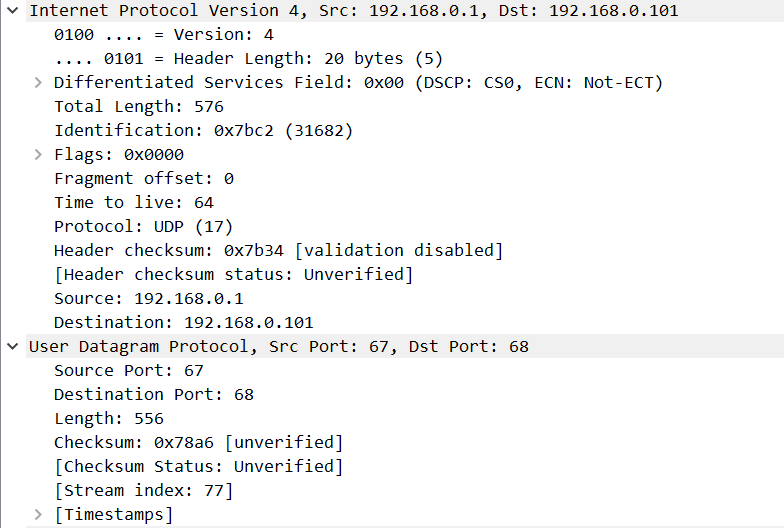


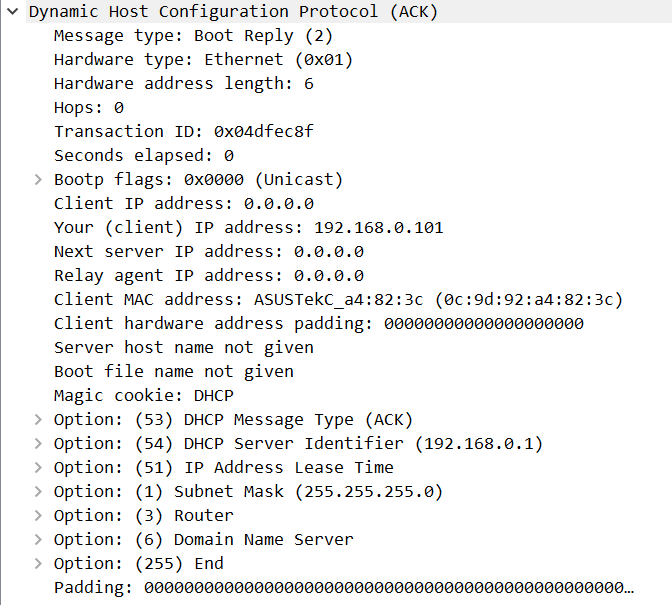
Request:



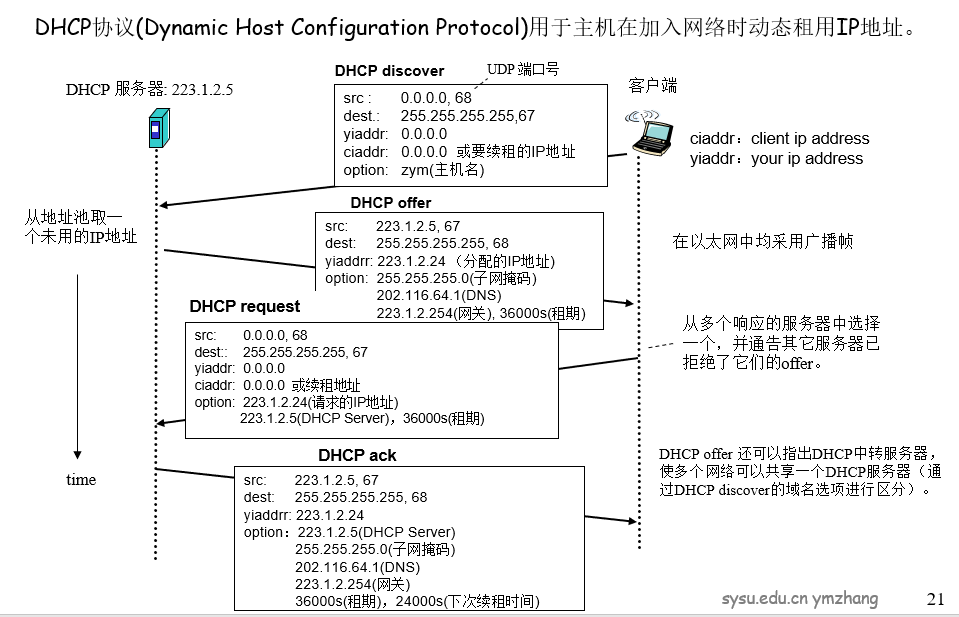


Ack:





[对照课件]



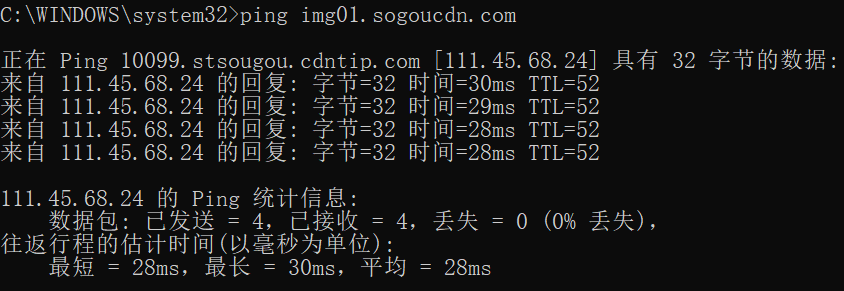
有没有可以纠正的内容？有的话写出来。

由DHCP服务器发给客户端的包中，src是192.168.0.1，即自己的ip地址，而不是课件所给的全零（当然全零也可以表示自己的ip地址），而dest是给客户端分配的ip地址，而不是255.255.255.255。

同时，DHCP包中的ciaddr和yiaddr其实是同一字段，客户端或服务器使用option中的类型判断是ciaddr还是yiaddr。课件中给出的包中同时包含了ciaddr和yiaddr。

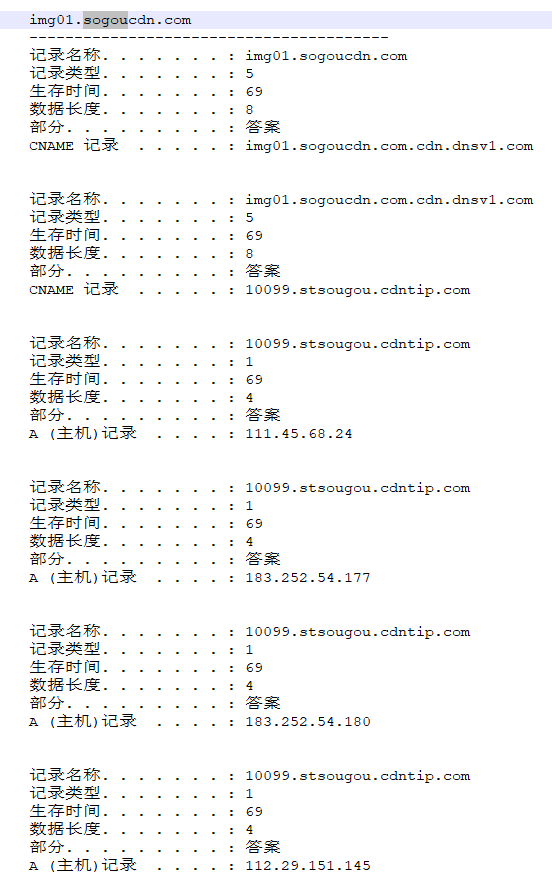
1. (DNS.pcapng)DNS协议

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：

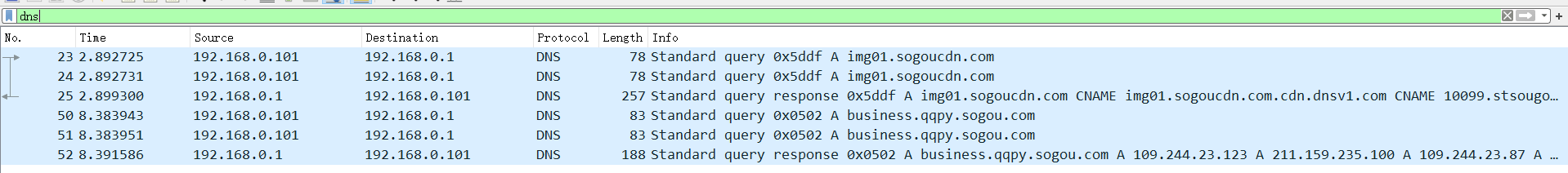
注：ipconfig/displaydns会打印海量数据，难以找到img01.sogoucdn.com的记录。我将输出的内容保存为文本文件后进行搜索，以下是文本文件搜索到的内容的截图：



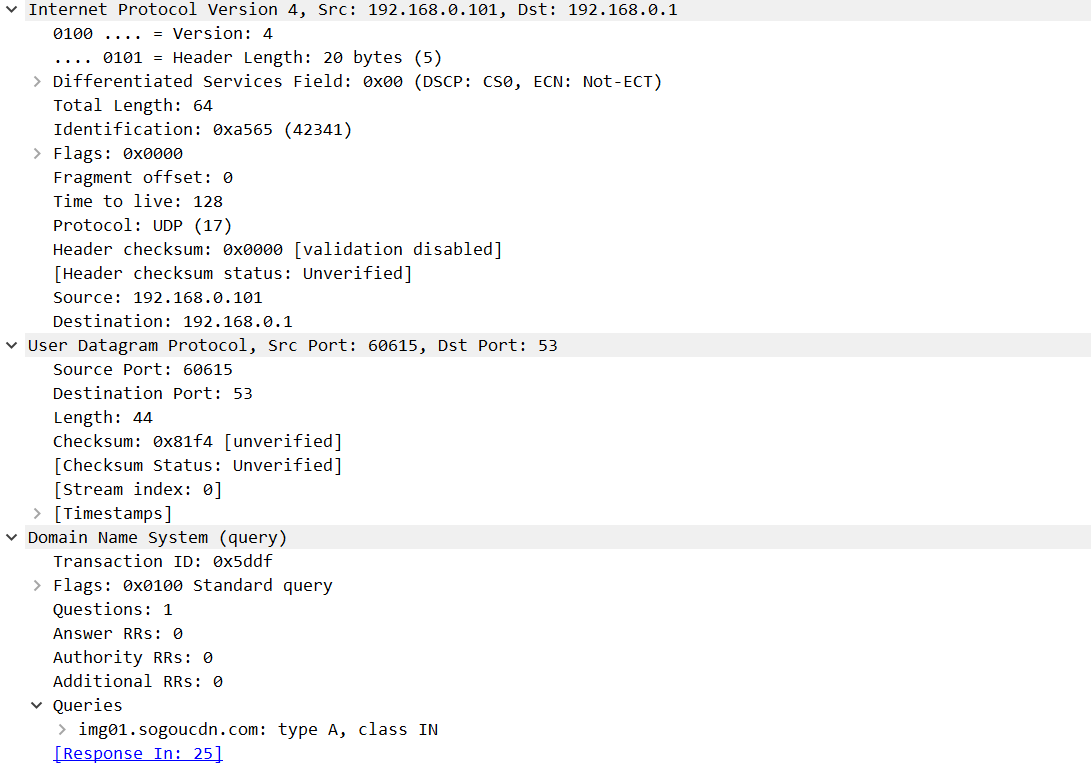
解释其中内容（说明如何可以从DNS记录中得到img01.sogoucdn.com的IP地址）：

第一条记录先获得了img01.sogoucdn.com的CNAME记录，即别名记录。然后根据该别名又找到了新的CNAME记录，最后通过这个CNAME记录找到了主机记录，即ip地址。

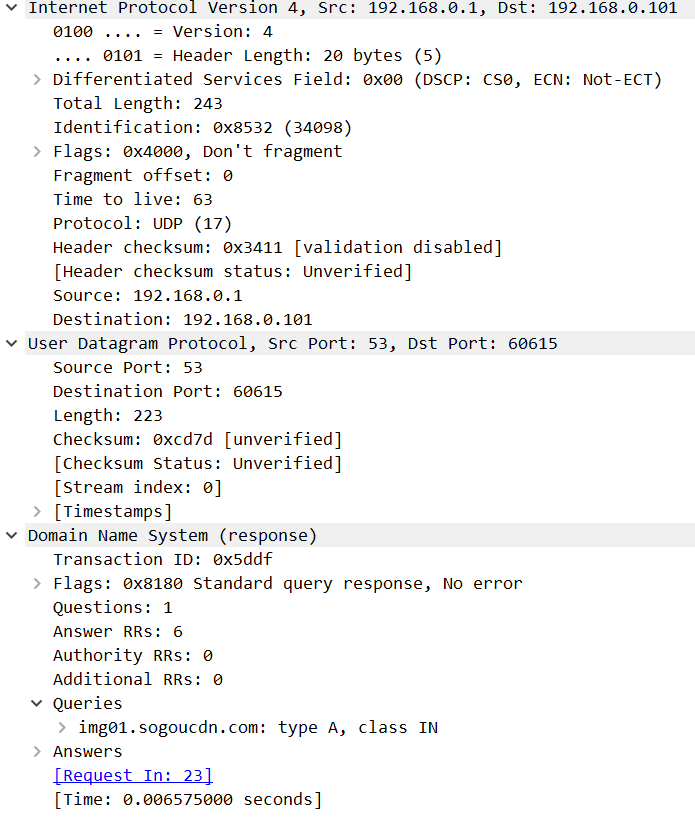
清除DNS记录：C:>ipconfig /flushdns后，再ping img01.sogoucdn.com并截包：



[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：

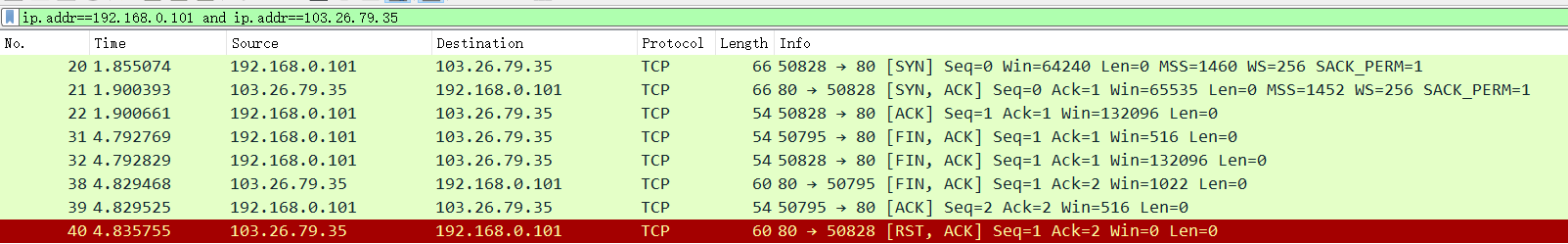
过滤条件：ip.addr==192.168.0.8 and ip.addr==103.26.79.35

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]

前三个包就是三次挥手的包。首先由主机向服务器发送SYN包，Seq=0，请求建立连接，之后服务器向主机发送SYN+ACK的包，Seq=0。从截图中可以看到，Ack=1，即之前的SYN包的Seq+1。最后主机再向服务器发送ACK包表示自己已经收到了SYN+ACK包，Ack=1,即上一个包的Seq+1。

接着四个包就是四次挥手的包。前两个包都是主机发往服务器的FIN+ACK包，可能发生了丢包重传。第三个包是服务器发送给主机的FIN+ACK包，可以看出，主机将四次挥手中的FIN和ACK合并成了一个包发送，ACK为上一个包的Seq+1。最后主机发送ACK包确认收到。

最后一个包是RST包。由服务器强制关闭连接。

【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）。

本次实验中我碰到的问题主要有两个：

首先是DHCP协议实验步骤中，理论上主机连接服务器时会先发送discover包向服务器申请分配ip地址，然而实际实验中，在联网时，我发现截取的包中，主机每次直接发送了request包，服务器收到后发送ack包，四个步骤变成了两步。我估计是每次联网时我的主机会因为有之前的连接记录，会直接发送request包。经网上查阅资料，我得知在连接后使用ipconfig/release命令可以释放连接，通过ipconfig/renew则可以申请重新分配ip。由此我最终得出了四个步骤的包。

其次是在DNS实验步骤中，需要使用ipconfig/displaydns命令查看DNS缓存。输入指令后会打印巨量的数据，完全无法找到需要的项。通过ipconfig/displaydns >c:\out将命令打印内容输出成文本文件，再在文本文件中搜索内容，我才得到了最终要查询的域名。

【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）