**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称 数据链路层和网络层协议分析 指导教师 潘冰

实验项目编号 07 实验项目类型 验证型 实验地点 B402

学生姓名 张景曦 学号 2019051098

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 11 月 2 日 下 午～ 11 月 10 日 下 午

1. **实验目的**

1、 理解链路层、网络层主要协议格式，以及协议的工作原理

2、 理解网关和子网掩码概念

3、 学会利用网络嗅探器（如Wireshark）分析协议格式和协议的工作过程

4、 学会使用ping、tracert、arp等命令并使用嗅探器分析其工作过程。

1. **实验内容**

1、 用嗅探器捕获数据包。

2、 分析以太网帧、ARP协议、IP协议、ICMP协议格式

3、 分析PING、TRACERT、ARP命令的工作过程

4、 通过修改主机的网关为指定默认网关、本机IP地址或不设置网关，观察ping的结果，用嗅探器捕获数据包并分析。

**（三）实验器件、仪器和设备**

计算机2台，交换机一台。

**（四）实验原理**

1.实验原理

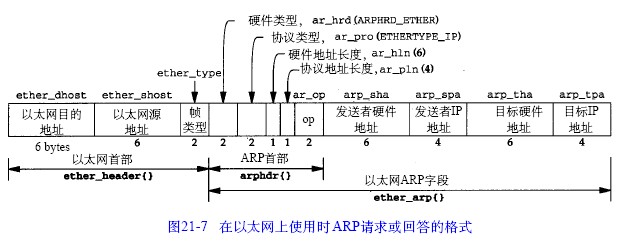
（1）网络嗅探器

Wireshark是一个网络数据包分析软件。通过该软件可以获取网络数据包，并能进行统计分析网络数据包数据。运行Wireshark时需要将网卡设为混合模式。

如果在交换环境里对其他主机进行嗅探，需要对交换机端口进行映射。

（2）协议

以太网上使用的ARP协议格式

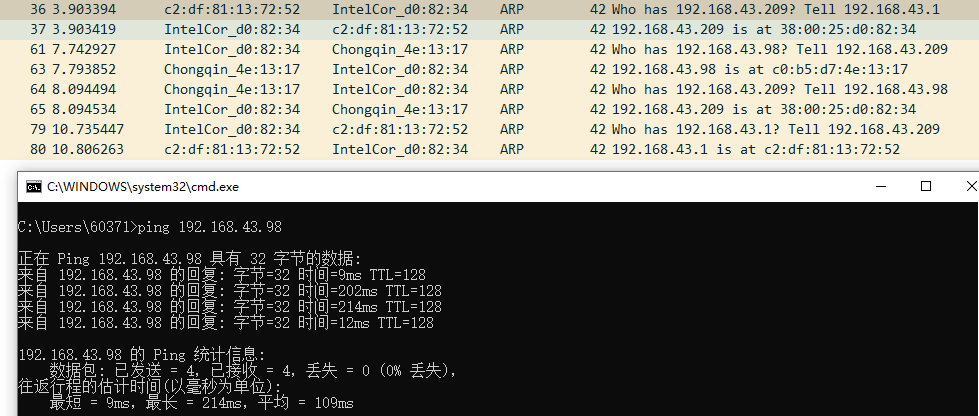


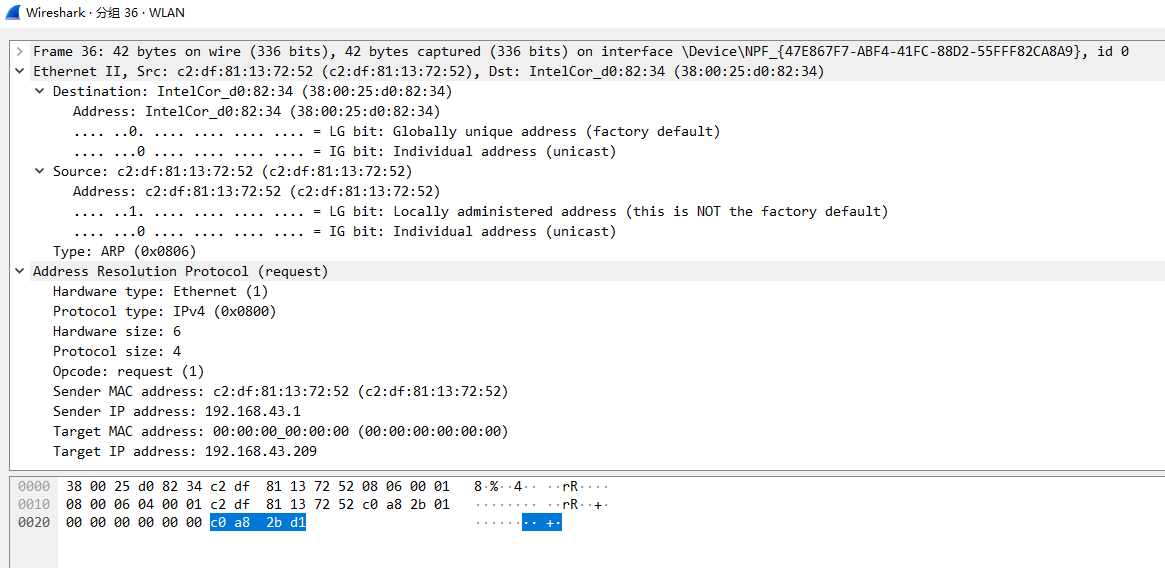
**（五）实验步骤**

1、 安装Wireshark

2、 以太网协议分析

从主机A上向主机B发PING检测报文，捕获以太数据帧，记录并分析MAC帧各字段的含义。





由图可知：

发送者mac地址为：

Sender MAC address: c2:df:81:13:72:52 (c2:df:81:13:72:52)

接收者mac地址为：

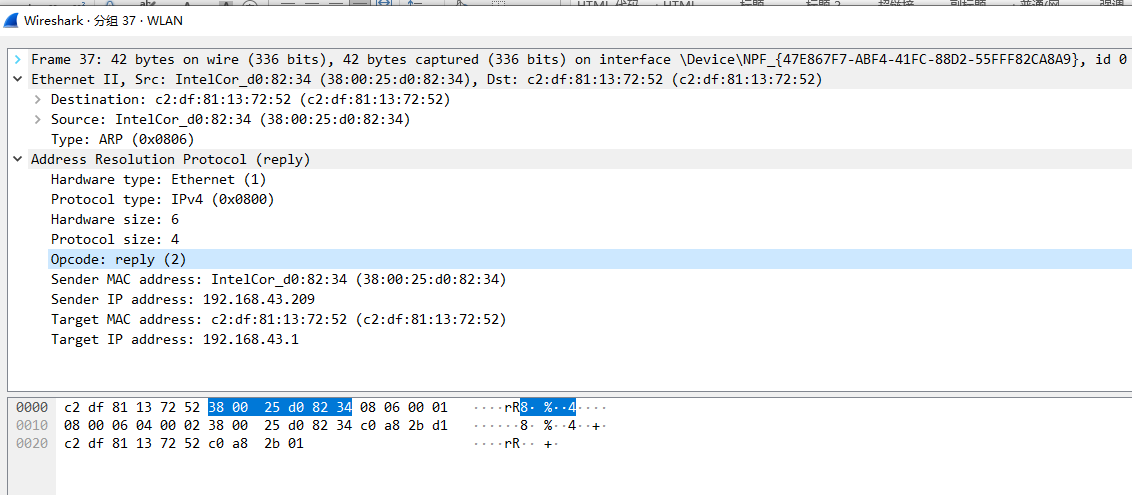
Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)，表示这是一个广播。

Type: ARP (0x0806)表示上层是一个arp数据报；

Sender IP address: 192.168.43.1

Target IP address: 192.168.43.209

Opcode: request (1)表示请求；



发送者mac地址：

Sender MAC address: IntelCor\_d0:82:34 (38:00:25:d0:82:34)

接收者mac地址为：

Target MAC address: c2:df:81:13:72:52 (c2:df:81:13:72:52)

Type: ARP (0x0806)表示上层是一个arp数据报；

Sender IP address: 192.168.43.209

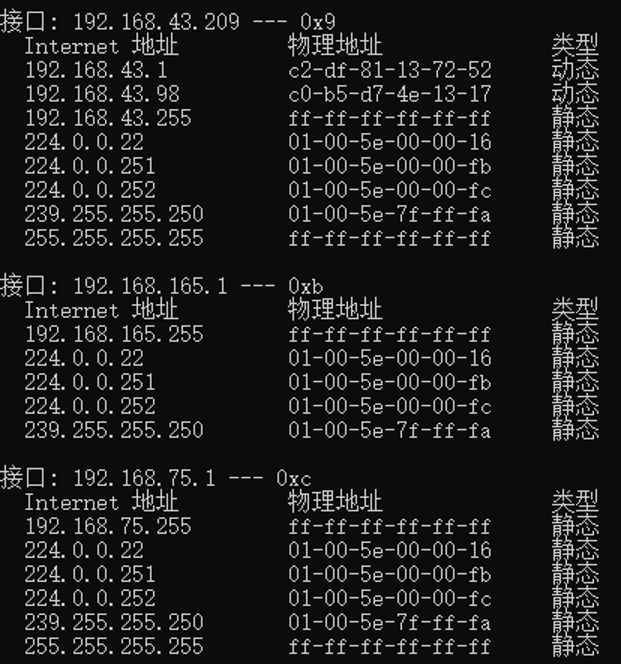
Target IP address: 192.168.43.1

此处mac地址和ip地址均反过来了。

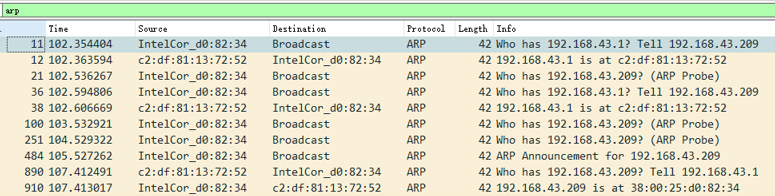
Opcode: reply (2)表示回复；

3.ARP协议分析

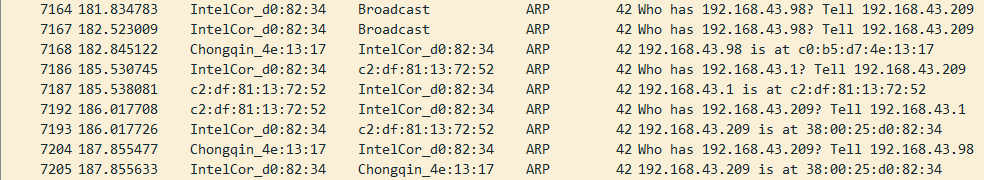
* 进入DOS窗口，用arp – a 查看本机上的ARP表的情况，然后用 arp –d B 删除B的记录（如果有的话）；



* 运行Wireshark程序；
* 把网线断开1分钟，然后再联网，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；



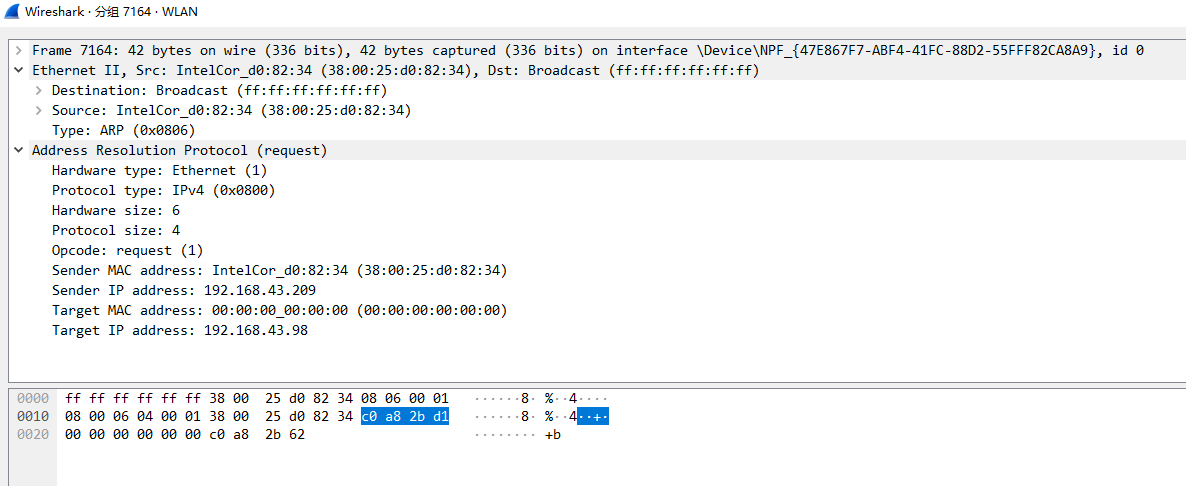
* 从主机A上向主机B发PING检测报文，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；



第一个字段是表示广播寻找主机B：192.168.43.98.第二个字段同理。

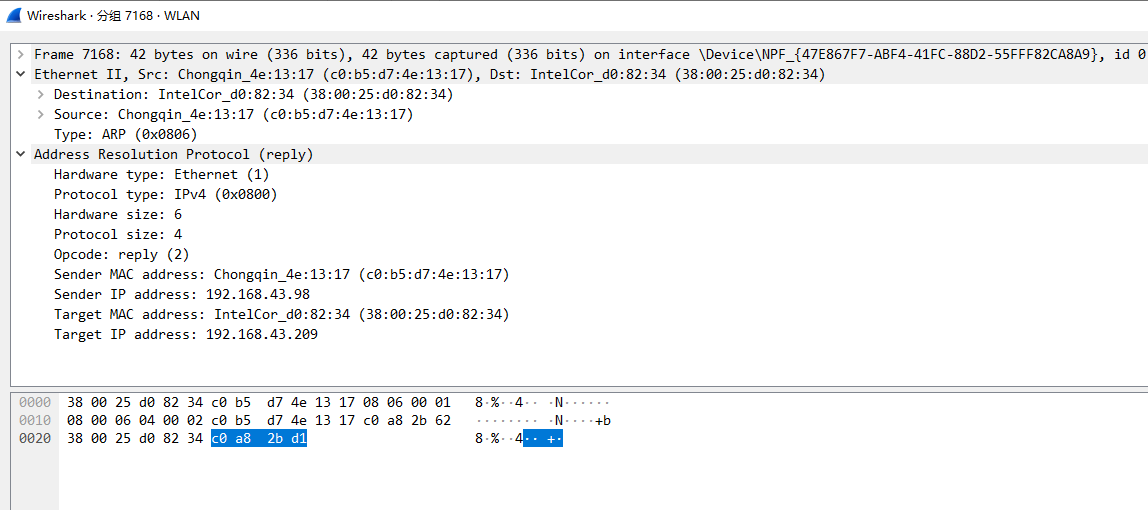
第三个字段表示回复主机B的mac地址。后面同理。

第一个字段的分组信息：



Destination:Broadcast表示这是广播信息。

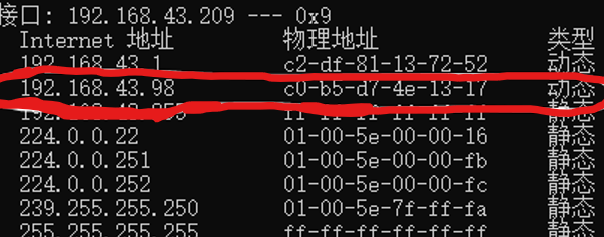
第三个字段的分组信息：



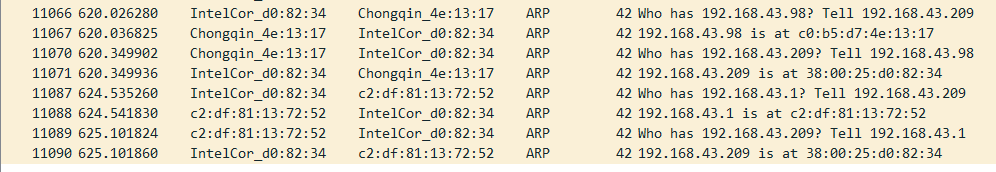
第三个字段的含义同理前文mac报分析。

* 通过arp - a 查看ARP表的更新情况，记录此时能否看到B对应的MAC地址；

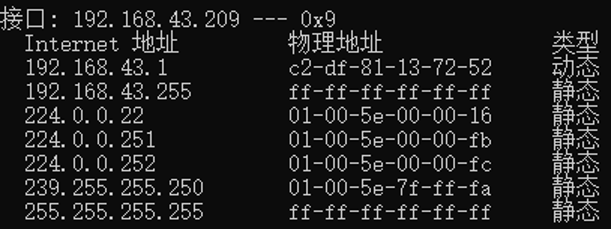
可以看到B的MAC地址：



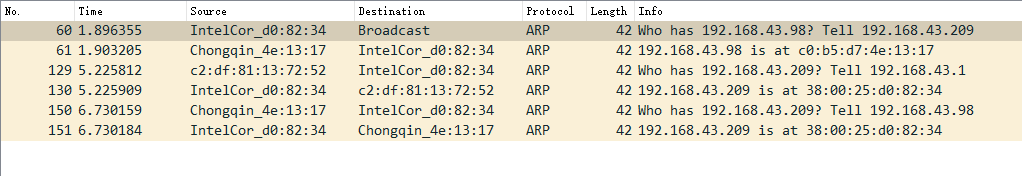
* 再次从主机A上向主机B发PING检测报文，或者再次从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文；能捕获：



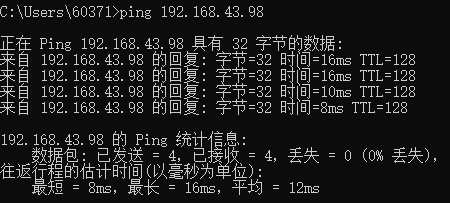
* 主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。



看到没有主机B的地址

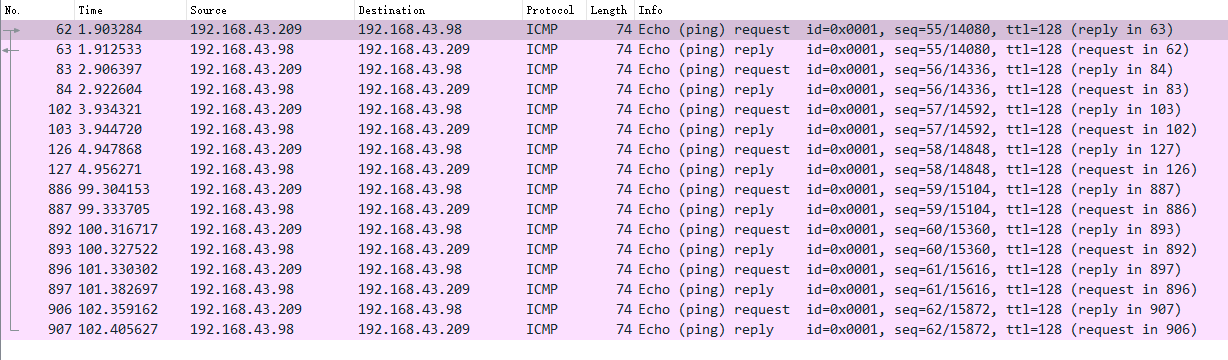


Ping获取arp报文：

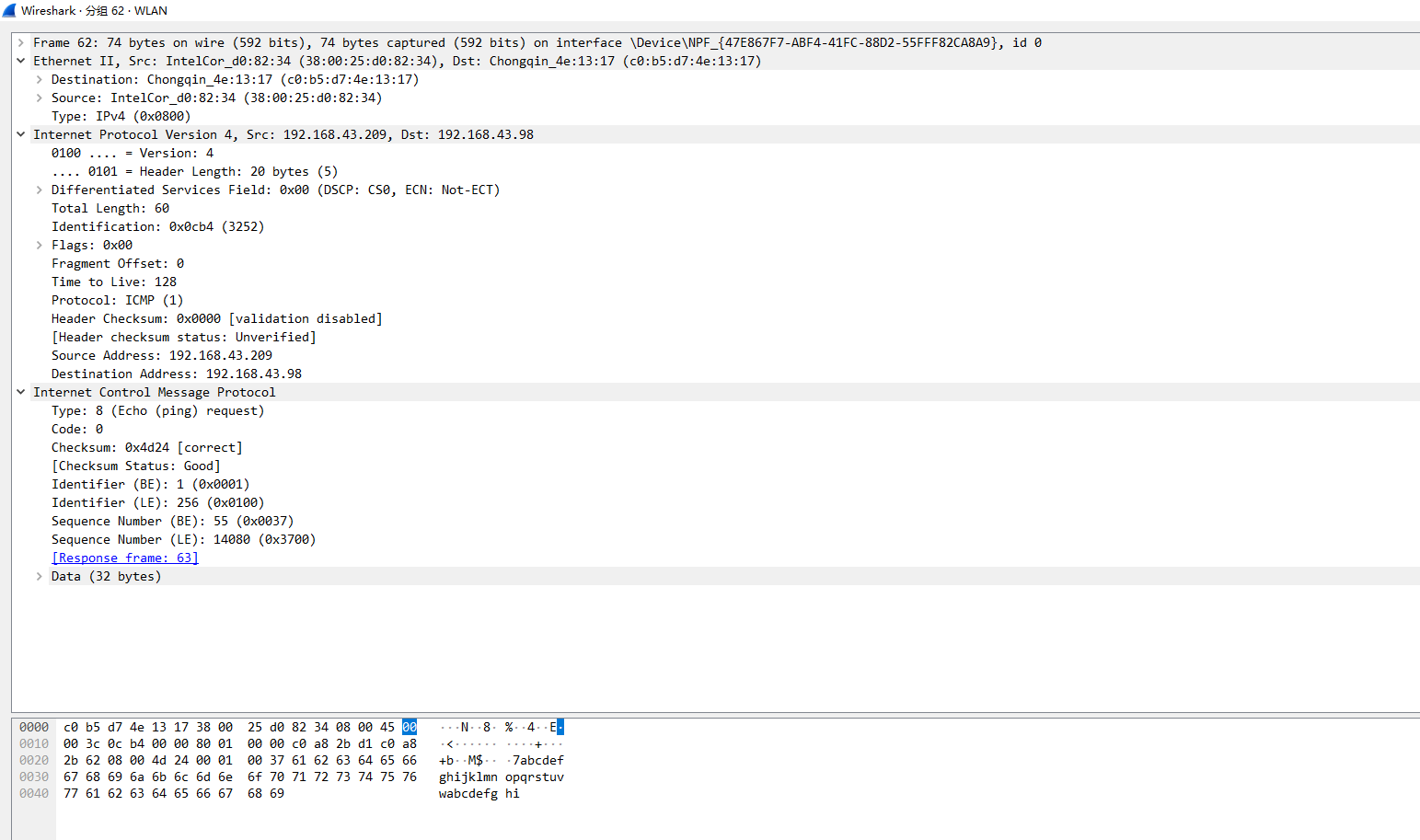


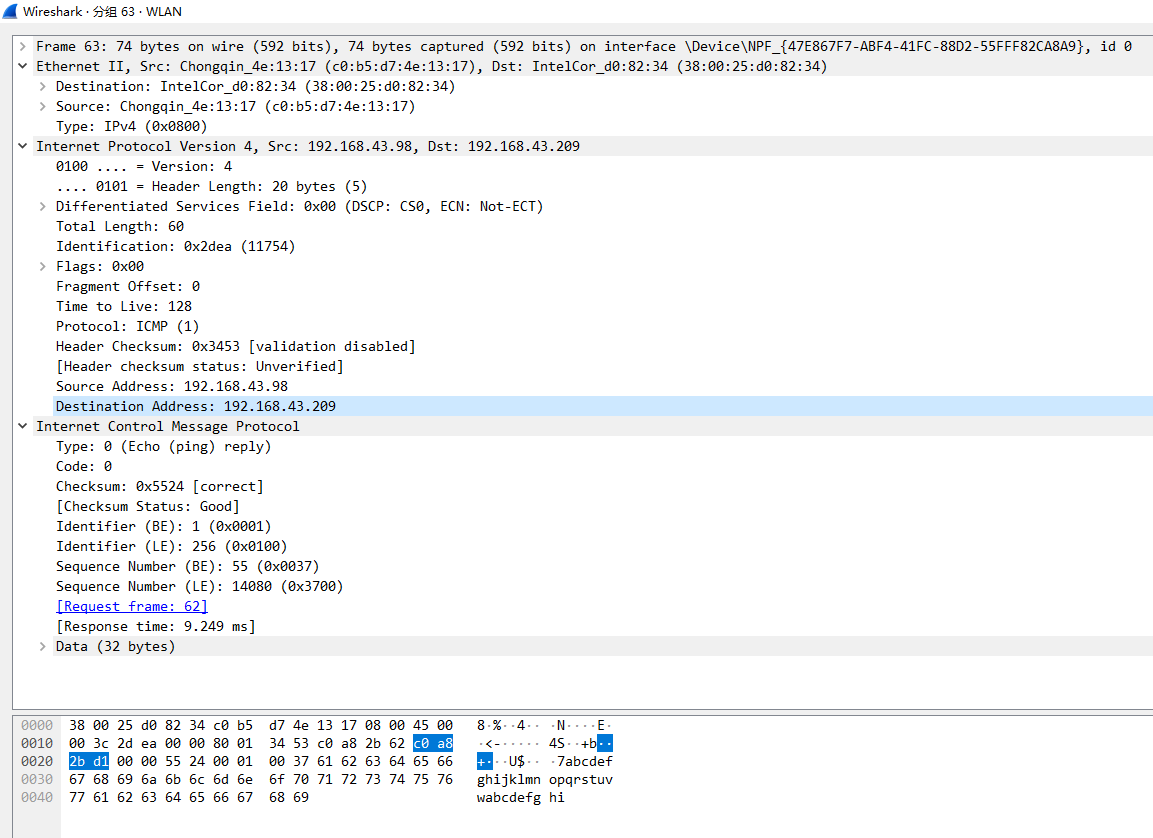
4.IP协议分析

* 从主机A上向主机B发PING检测报文，捕获IP数据包，记录并分析各字段的含义，并与IP数据包格式进行比较;



总共ping了两次，一共发送与接收八个数据包。





版本号：占用4位，表示该IP数据包使用的IP协议版本。

头长度：占用4位，表示整个报头的长度。

服务类型：占用8位，用于规定本数据包的处理方式。

总长度：占用16位，表示整个IP数据包的长度，以字节为单位。

标识：占16位，可以使分片后各数据报片最后能正确地重装成为原来的数据报。

标志：占3位，但目前只有2位有意义. 标志字段中的最低位记为 MF(More Fragment).MF=1即表示后面"还有分片"的数据报.MF=0表示这已是若干数据报片中的最后一个.标志字段中间的一位记为DF(Don't Fragment),意思是"不能分片",只有当 DF=0时才允许分片。

片偏移：占 13位.较长的分组在分片后,某片在原分组中的相对位置.也就是说,相对用户数据字段的起点,该片从何处开始.片偏移以 8个字节为偏移单位,这就是说,每个分片的长度一定是 8字节(64位)的整数倍。

生存时间：占8位，目的是防止无法交付的数据报无限制地在因特网中兜圈子,因而白白消耗网络资源。

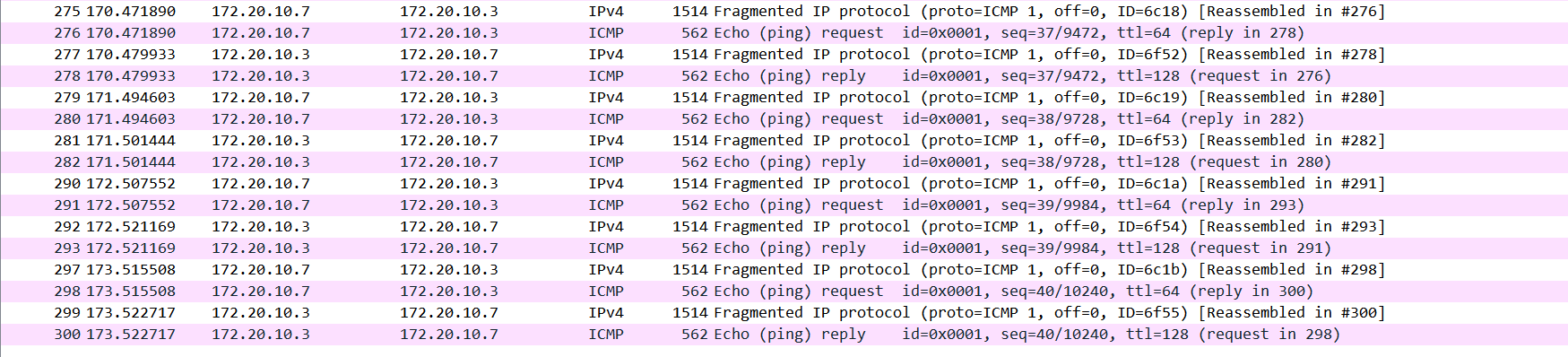
协议：占 8 位.协议字段指出此数据报携带的数据是使用何种协议,以便使目的主机的IP层知道应将数据部分上交给哪个处理过程.详细资料请看文章最后的注释。

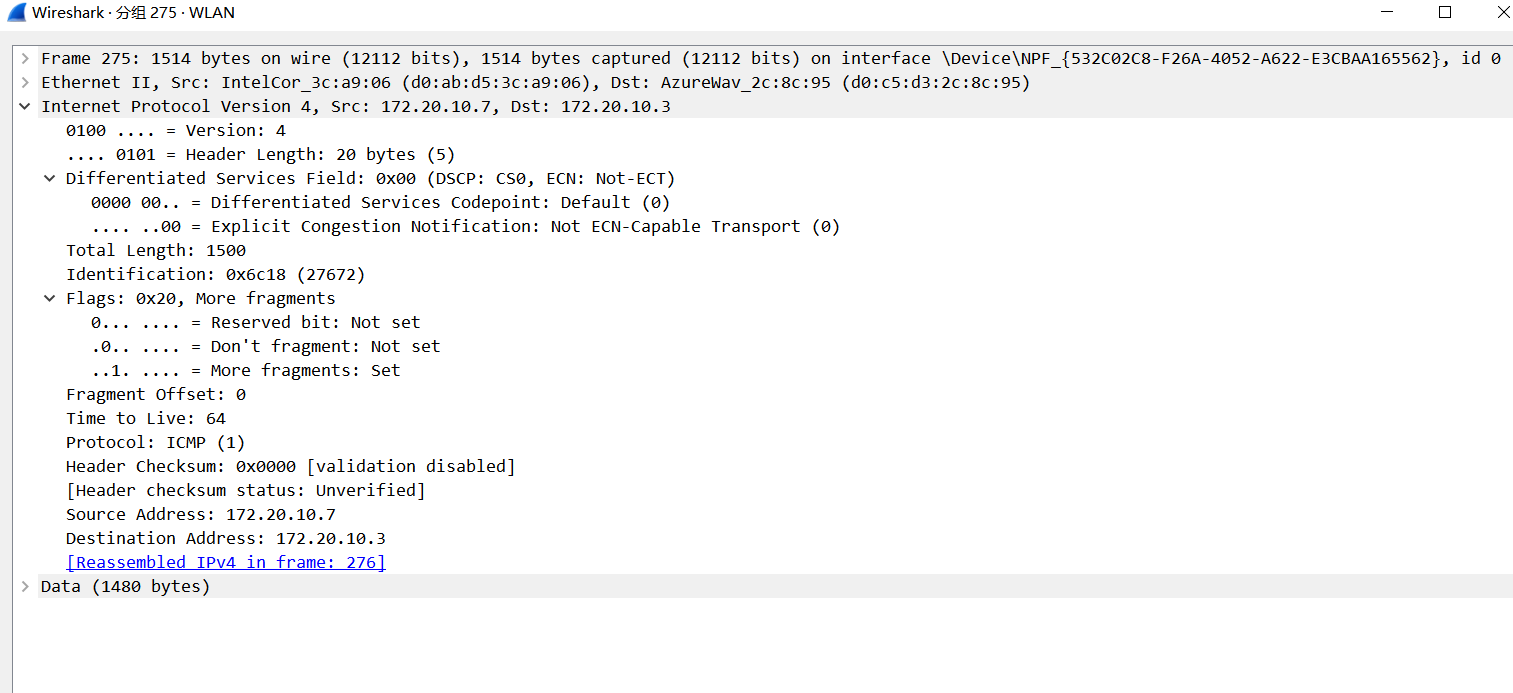
首部检验和：占 16位.这个字段只检验数据报的首部,但不包括数据部分.这是因为数据报每经过一个路由器,都要重新计算一下首都检验和 (一些字段,如生存时间,标志,片偏移等都可能发生变化),不检验数据部分可减少计算的工作量。

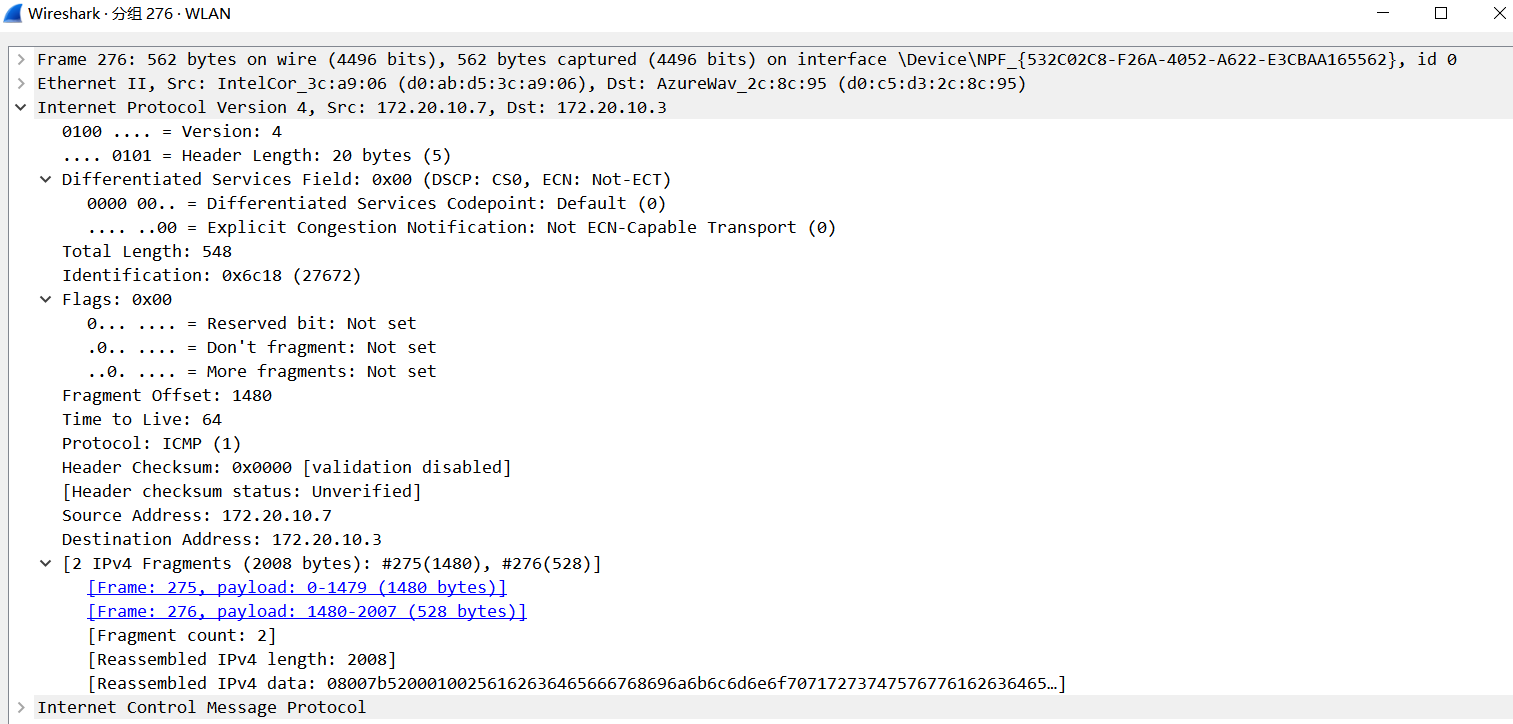
源地址:占32位。

目的地址:占 32位。

* 使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析**分片和重组**过程。







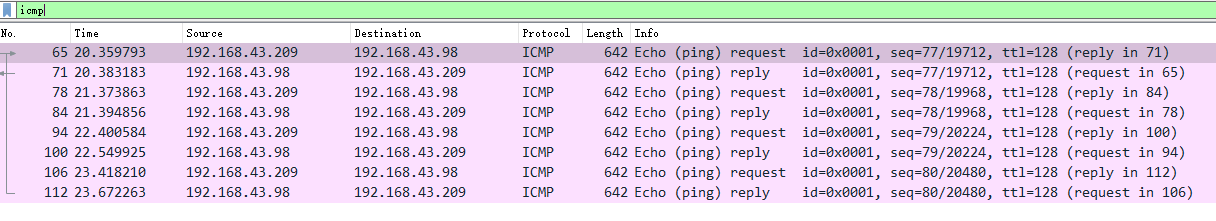
根据图中可以看出一个2000字节的IP数据包被分成了两片，第一片Total length为1500字节，除去首部20字节，数据部分是1480字节；第二片是Total length是548字节，除去IP首部20字节和ICMP首部8字节，数据部分是520字节，两个切片通过相同的标识进行重组，加起来数据刚好是2000字节。

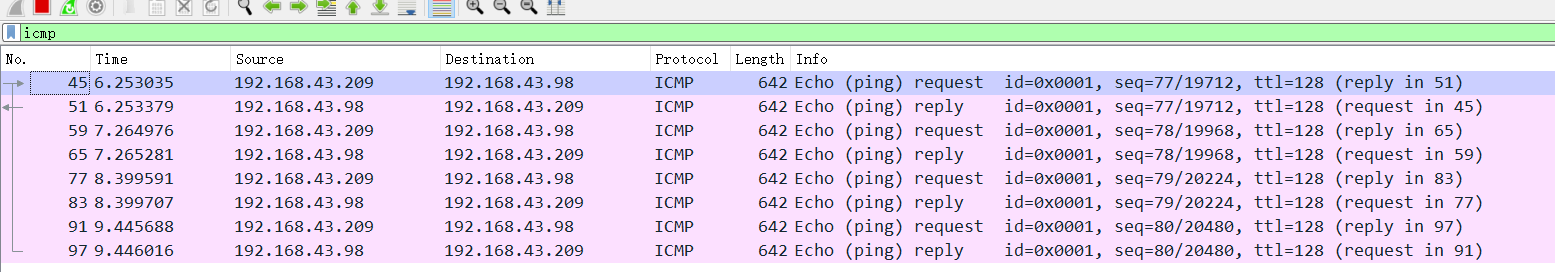
5. ICMP协议分析

通过ping和tracet命令，了解ICMP协议的使用。

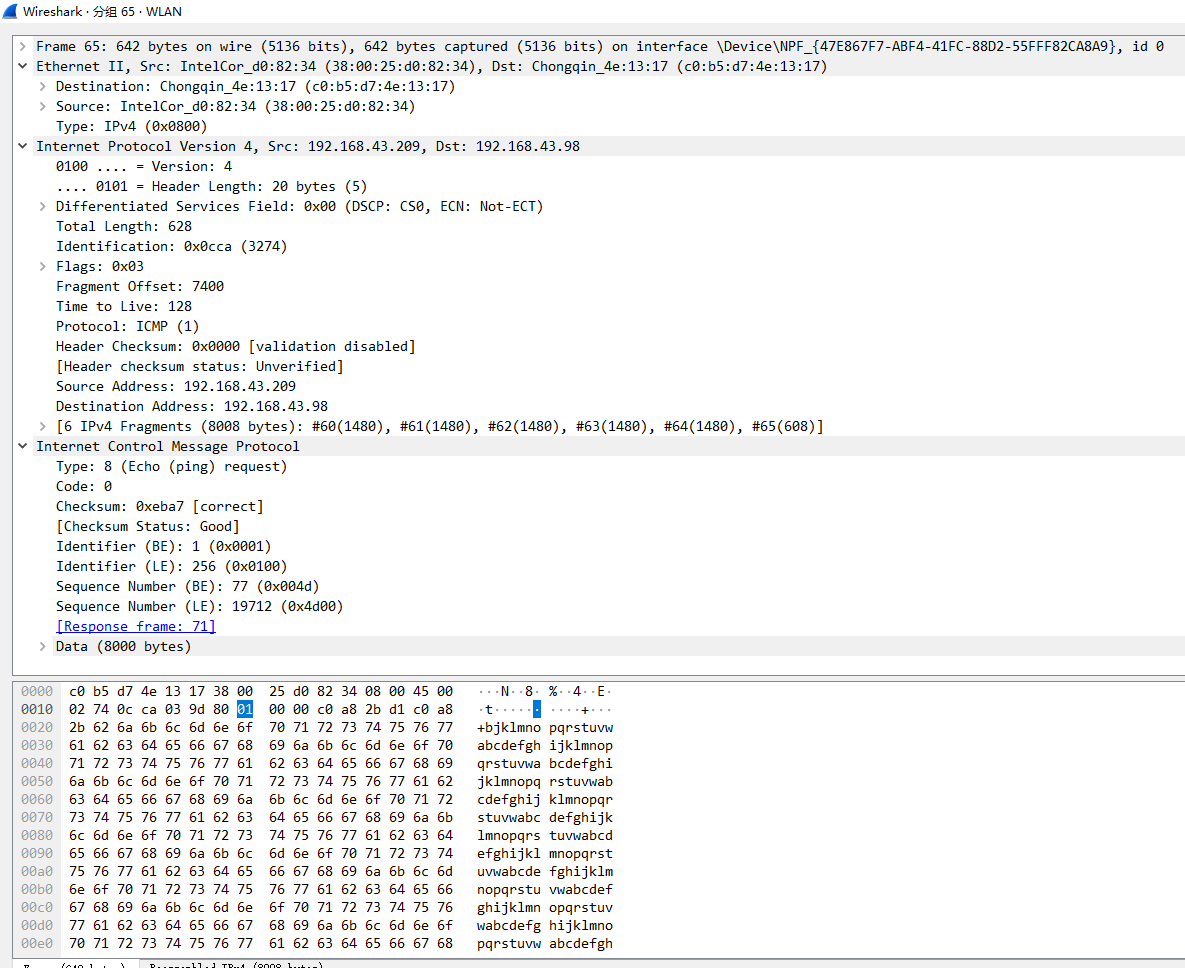
* 从主机A上向主机B发PING检测报文，捕获ICMP请求数据包和应答数据包，记录并分析各字段的含义，并与ICMP数据包格式进行比较；如果返回的差错信息，请分析是由于什么差错引起的。

主机A：

主机B:



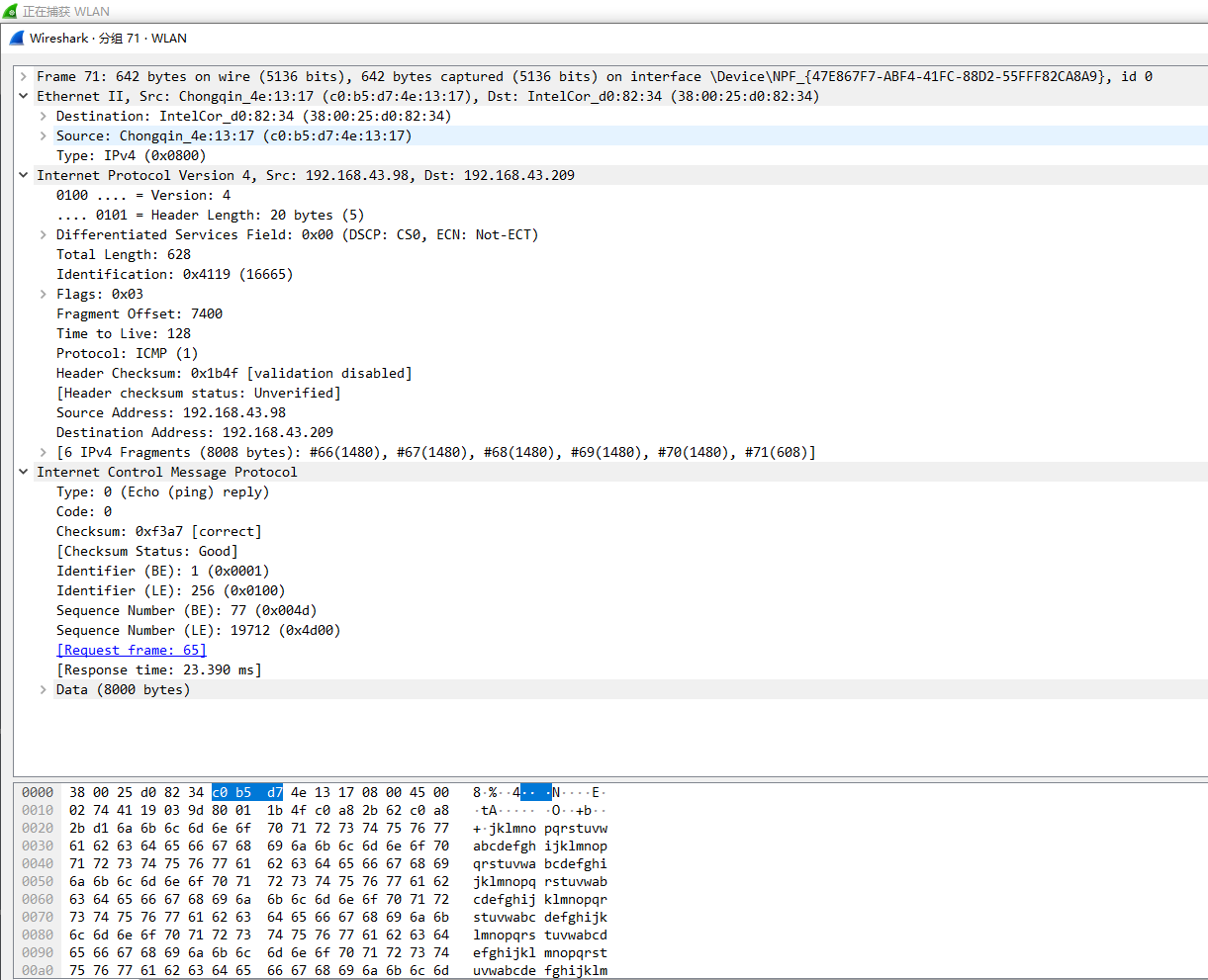
数据没有差错



其中目的主机地址，发送地址等基本信息。无需赘述；

Data（8000bytes）表示报文大小为8000字节，fragment offset表示偏移量为7400。

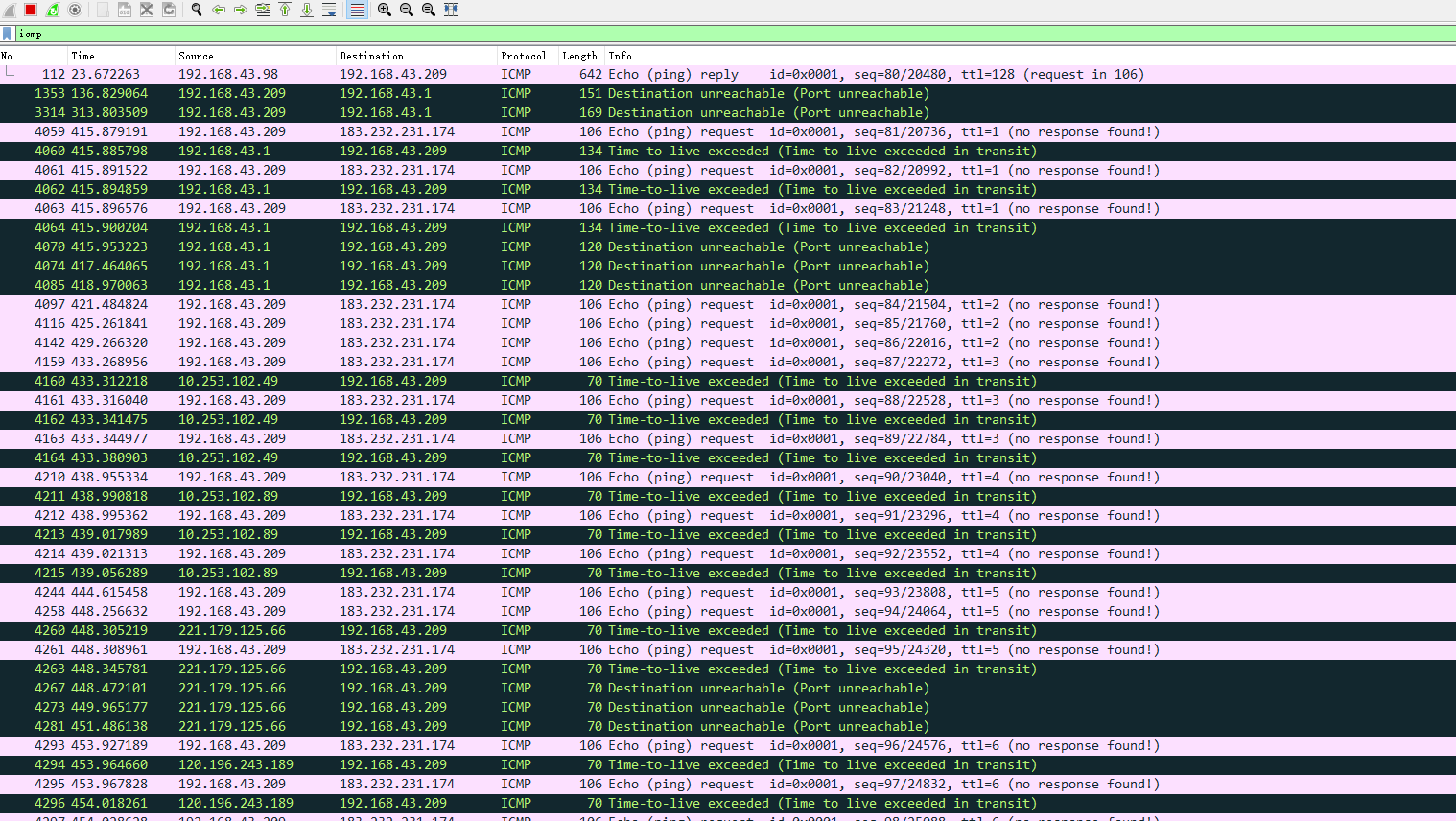
主机A的报文66：

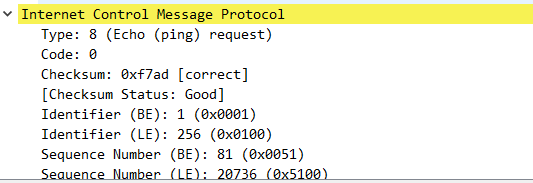


除了地址之外的其他参数基本一致。

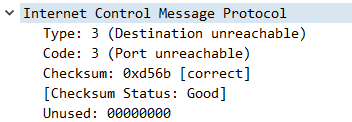
* 使用tracert命令，跟踪某台主机，使用wireshark捕获数据包，分析不同类型ICMP响应数据包格式（如type=8,type=0,type=11）。分析tracert工作原理。



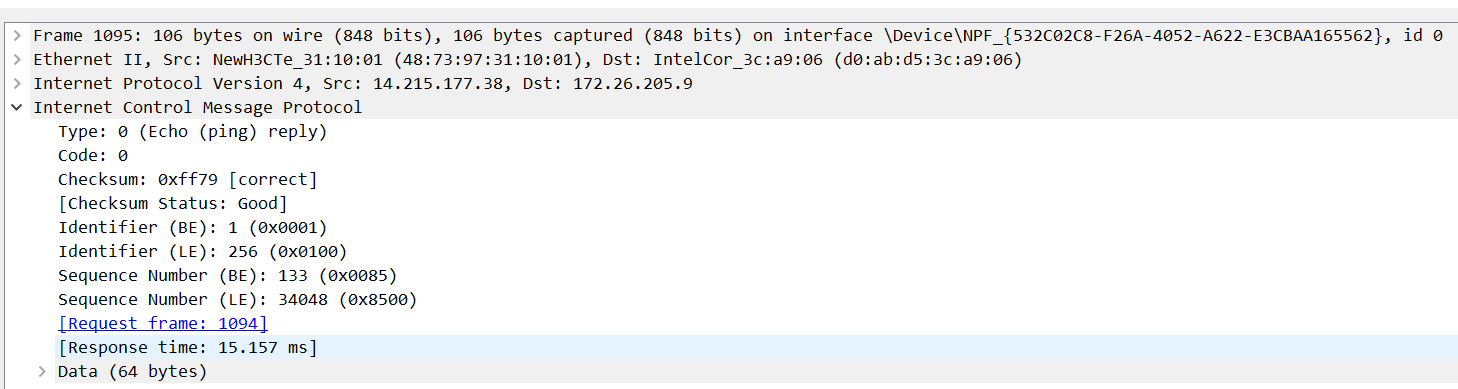




Type为8，Code为0代表ping请求。



Type为3表示无法到达地址，Code为3代表无法到达端口。



Type为0，Code为0代表ping应答。

**（六）实验结果与分析**

思考题：

1、在ARP包分析实验过程中，为什么A有时能捕获ARP报文，有时却不能捕获ARP报文？

这个要看主机A的ARP表中有无目标主机的IP-MAC映射关系，如果没有的话就需要广播ARP包去获取目标主机的MAC地址，就可以捕获到ARP报文；如果有的话就直接从ARP表中获取目标主机的MAC地址，而不需要广播，则捕获不到ARP报文。

2、为什么运行ping 127.0.0.1时，不能捕获到ICMP报文？如果运行ping 本机IP地址能收到报文吗？ 为什么？

Ping127.0.0.1时，属于环回测试，只是检查本地TCP/IP协议是否设置，并不会经过网卡，所以抓不到。Ping本机IP地址也收不到，

数据包没有发到网口。

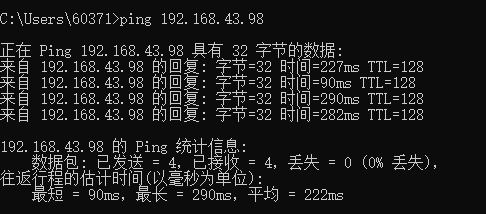
3、在ping 的过程中，返回信息“Request timed out” 和“Destination Host Unreachable”分别是由哪些情况引起的？

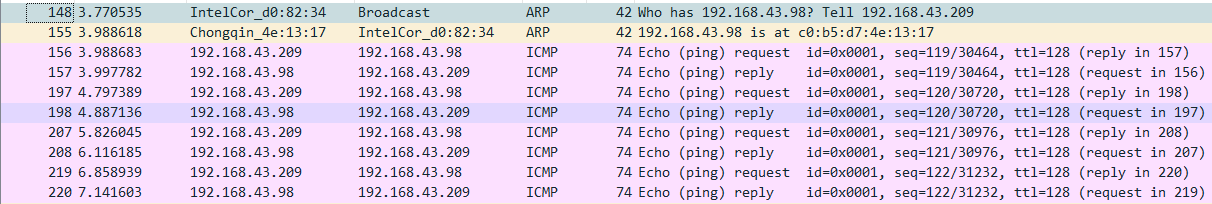
“Destination Host Unreachable” 是本地系统没有到所需目标的路由，或者远程路由器报告它没有到目标的路由。

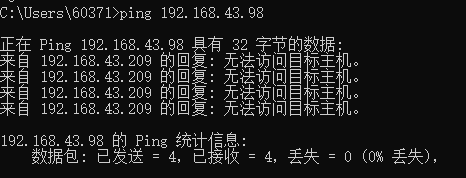
“Request timed out”最常见的情况包括网络拥塞，ARP请求失败，数据包过滤，路由错误或静默丢弃。

4、请通过实验验证：

主机如果不设置“网关”，同一网段内的主机可以相互通信。用ping命令测试，用嗅探器测试可以捕获8个ICMP数据包，2个ARP数据包。不同网段的主机不能通信，用PING命令测试，会显示“ Destination Host Unreachable”，因为没有指明网关，无法发送出去，因此显示“目的主机不可达”，用嗅探器捕获不到任何信息。



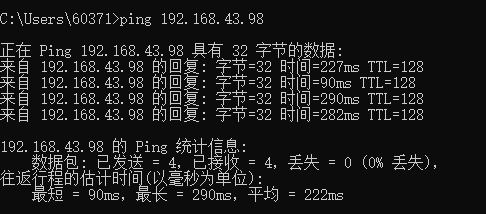


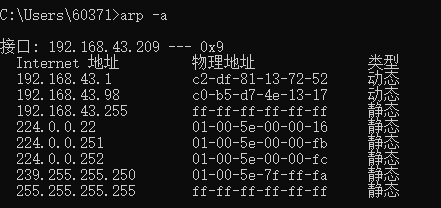


主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。

5.通过下面实验理解网关

假设主机A的IP地址为10.2.2.2/23，主机B的IP地址为10.2.3.3/23，两台主机均不设置网关，用ping命令测试两主机的连通性，用ARP命令查看物理地址。对结果进行分析。





Ping的通，可以看到地址。

假设主机A的IP地址为10.2.2.2/24，主机B的IP地址为10.2.3.3/23，两主机不设置网关，分别在主机A和主机B上用ping测试与对方的连通性，用ARP查看物理地址。对测试结果进行分析。

