**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 实B401

学生姓名 饶龙悦 学号 2019051101

学院 智能科学与工程 系 计算机 专业 信息安全

实验时间 2021 年 11 月 2 日 上 午～ 11 月 16 日 上 午

**【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。

**【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。

**【实验原理】**

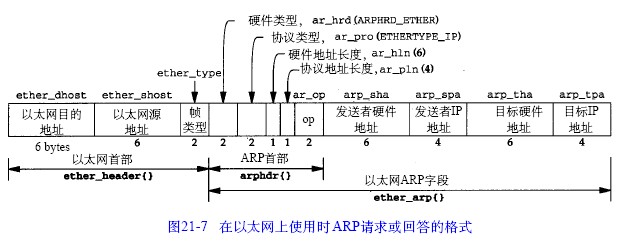
**1、网络嗅探器**

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**



**其他协议数据包格式见教材**。

**【实验环境】**

计算机2台，交换机一台。

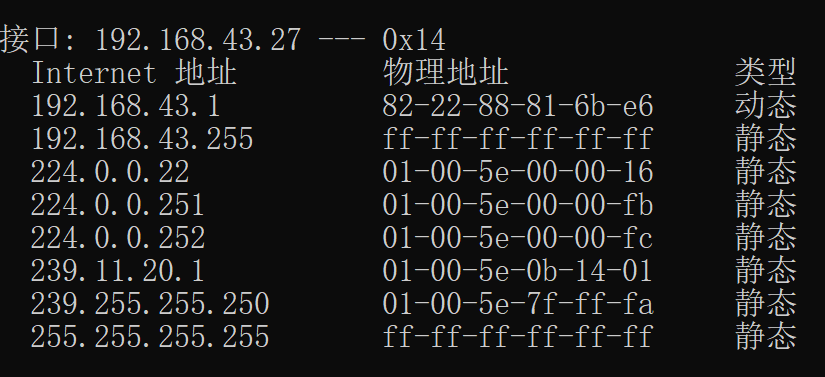
**【实验步骤】**

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。

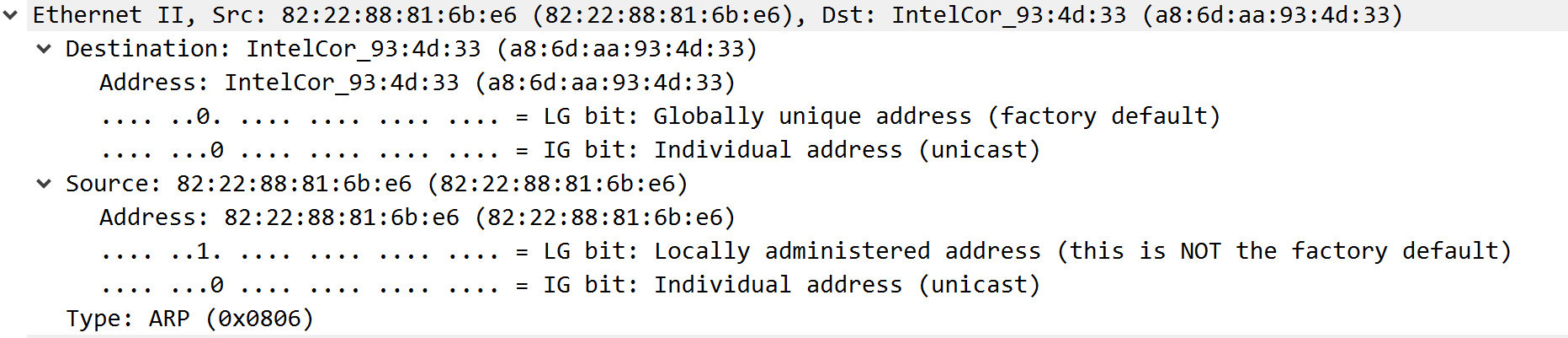
1. ARP协议分析

* 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）；

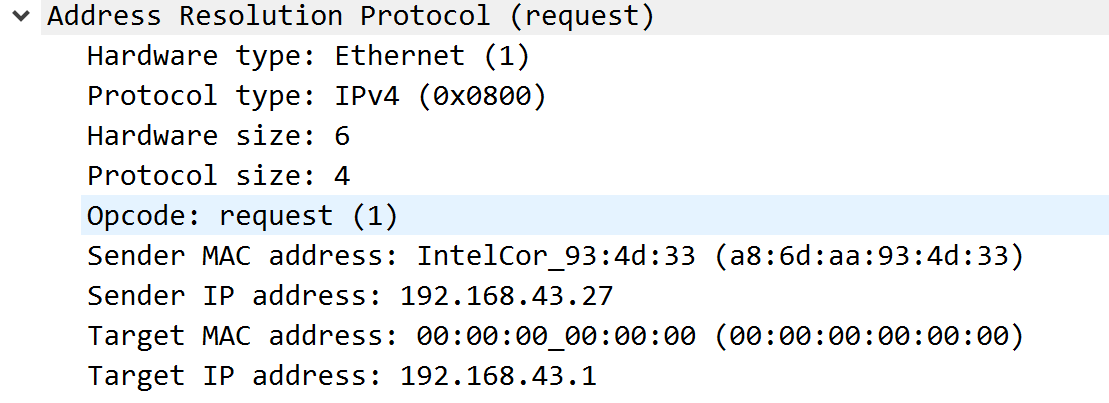


* 运行Wireshark程序；
* 把网线断开1分钟，然后再联网，观察此时是否能捕获ARP报文，如果能，记录并分析各字段的含义；

请求：







网关硬件地址:IntelCor\_93:4d:33(a8:6d:aa:93:4d:33)

硬件类型：Ethernet (1)

协议类型：IPv4(0x0800)

硬件地址长度：6

协议地址长度：4

操作：request(1)

源MAC地址：a8:6d:aa:93:4d:33

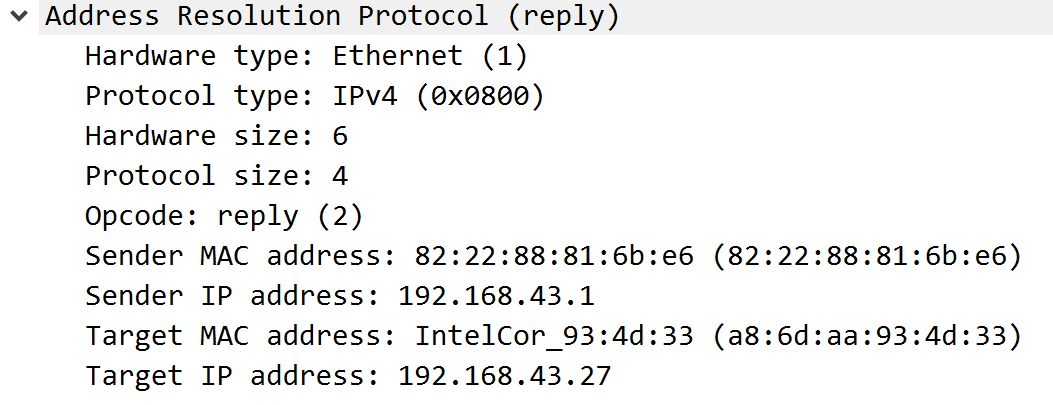
源IP地址：192.168.43.27

目的MAC地址：00:00:00:00:00:00

目的IP地址：192.168.43.1

响应：





硬件类型：Ethernet (1)

协议类型：IPv4(0x0800)

硬件地址长度：6

协议地址长度：4

操作：reply(2)

源MAC地址：82:22:88:81:6b:e6

源IP地址：192.168.43.1

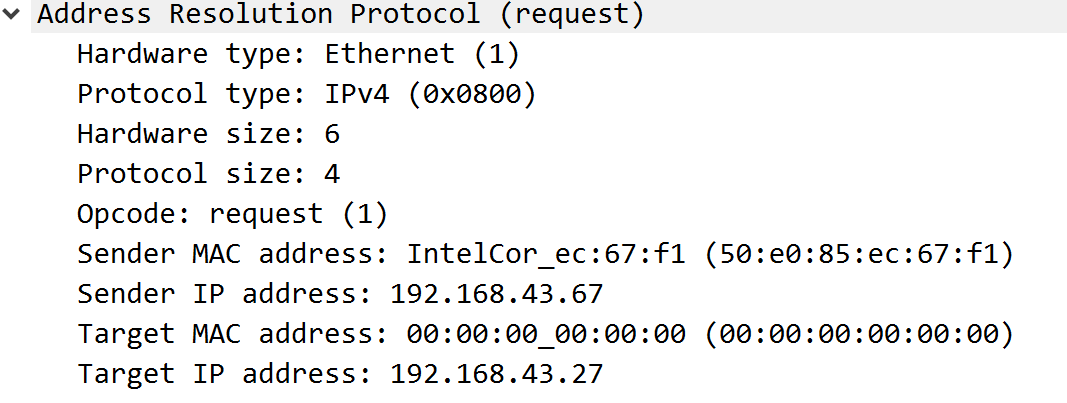
目的MAC地址：a8:6d:aa:93:4d:33

目的IP地址：192.168.43.27

* 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；

请求：





硬件类型：Ethernet (1)

协议类型：IPv4(0x0800)

硬件地址长度：6

协议地址长度：4

操作：request(1)

源MAC地址：50:e0:85:ec:67:f1

源IP地址：192.168.43.67

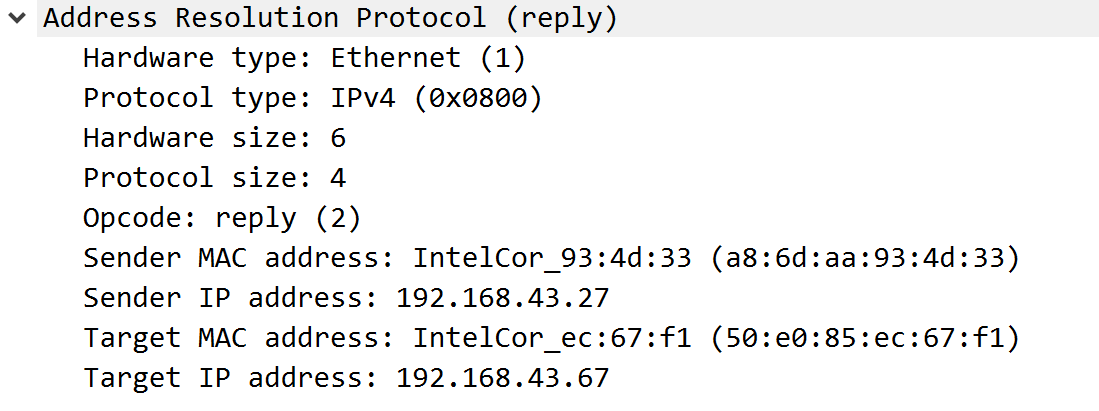
目的MAC地址：00:00:00:00:00:00

目的IP地址：192.168.43.27

广播MAC地址：ff:ff:ff:ff:ff:ff

回答：





硬件类型：Ethernet (1)

协议类型：IPv4(0x0800)

硬件地址长度：6

协议地址长度：4

操作：reply(2)

源MAC地址：a8:6d:aa:93:4d:33

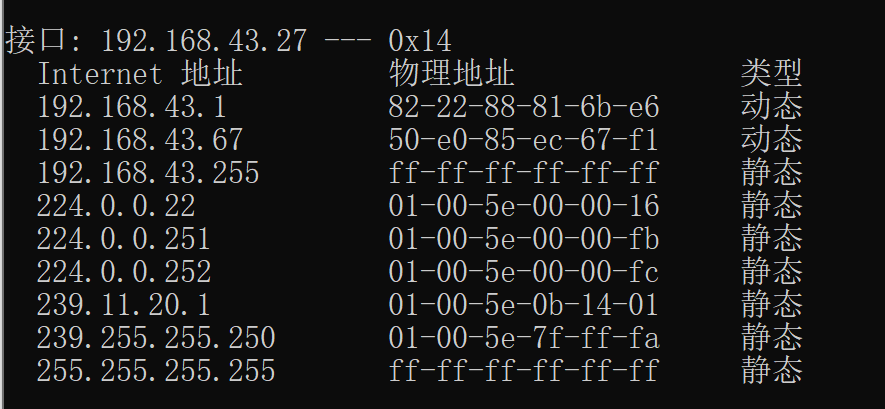
源IP地址：192.168.43.27

目的MAC地址：50:e0:85:ec:67:f1

目的IP地址：192.168.43.67

广播MAC地址：ff:ff:ff:ff:ff:ff

* 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；



Ping通后，多了192.168.43.67这一ip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；

**有报文,与上述报文一致。**

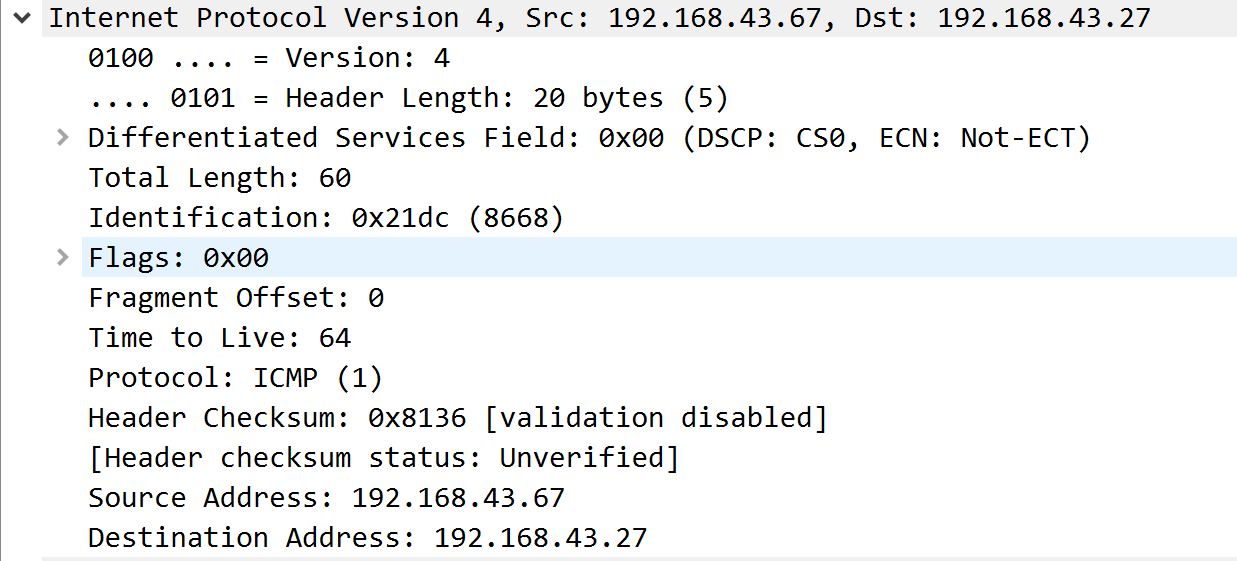
* 主机A上和主机B停止进行任何数据通信，5分钟后再次从A向B发PING检测报文，或者从主机B上向主机A发PING检测报文，观察看此时是否能捕获ARP报文。

**有时有有时没有，有报文时,与上述报文一致。**

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;





版本：4

首部长度：20byte

区分服务：0x00

总长度：60

标识：0x21dc

标志：0x00

片偏移：0

生存时间：64

协议：ICMP

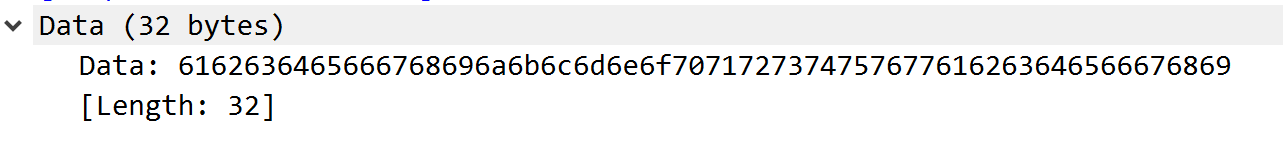
首部检测和：0x8136

源地址：192.168.43.67

目的地址：192.168.43.27

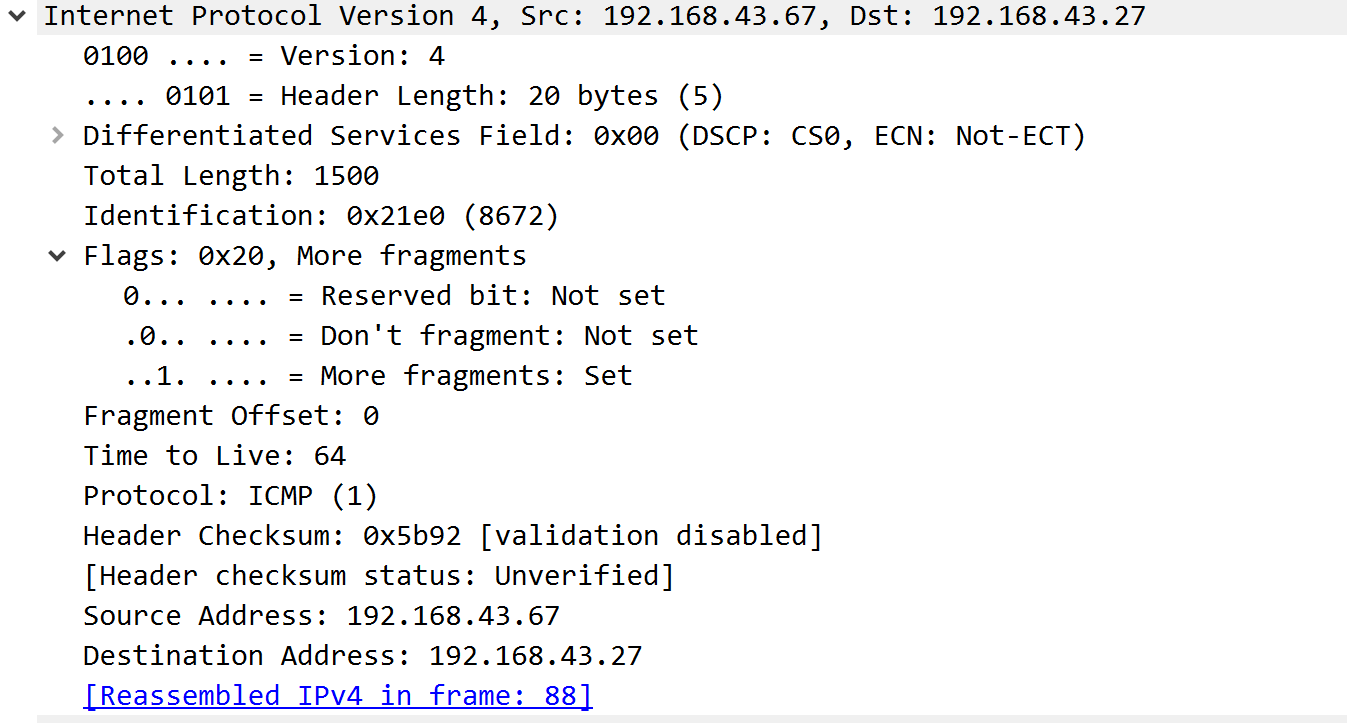
以上为首部。

数据部分：



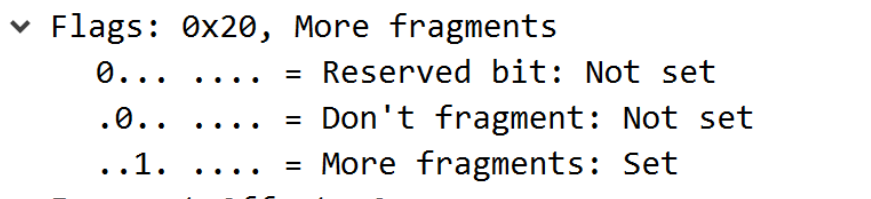
* 使用ping命令，制定数据包长度，如ping -l 2000，使用嗅探器观察IP分片情况，并分析**分片和重组**过程。





IP报文总长度：1500

标识位：0x21e0



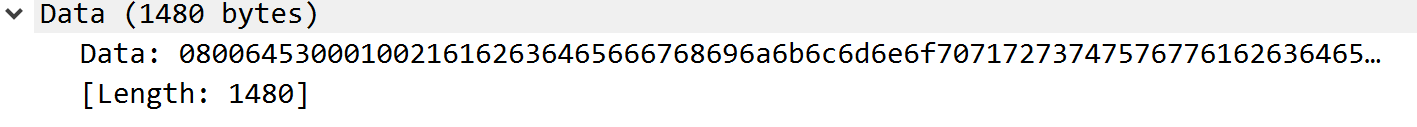
DF=0：能分片

DF=1：还有分片

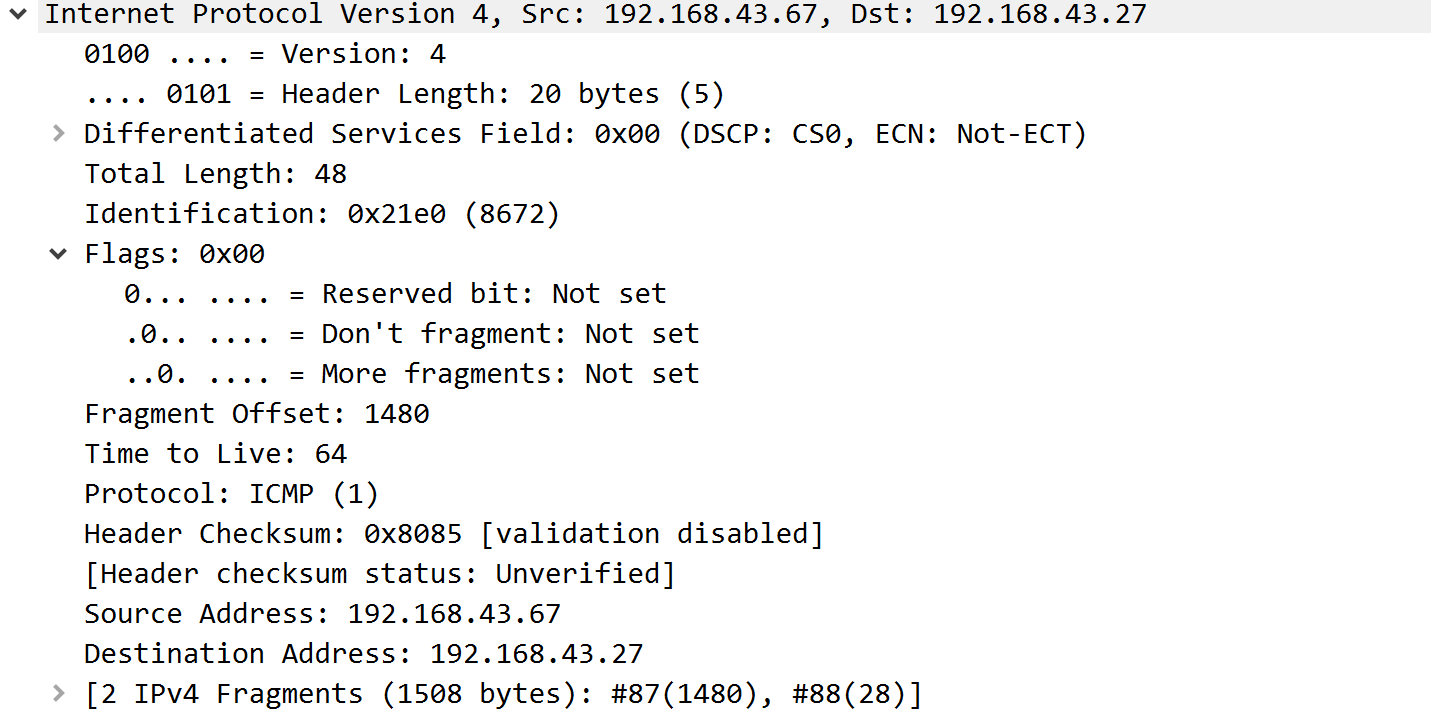


在88号分组重组

第一段 1480个字节：

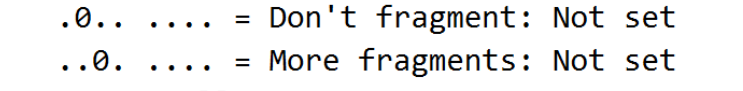




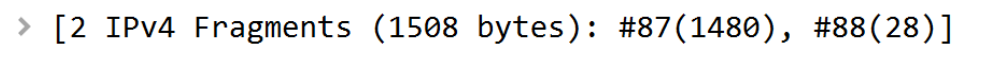


总长度：48=DATA：20+IP head：20+ICMP head：8

标识位：0x21e0



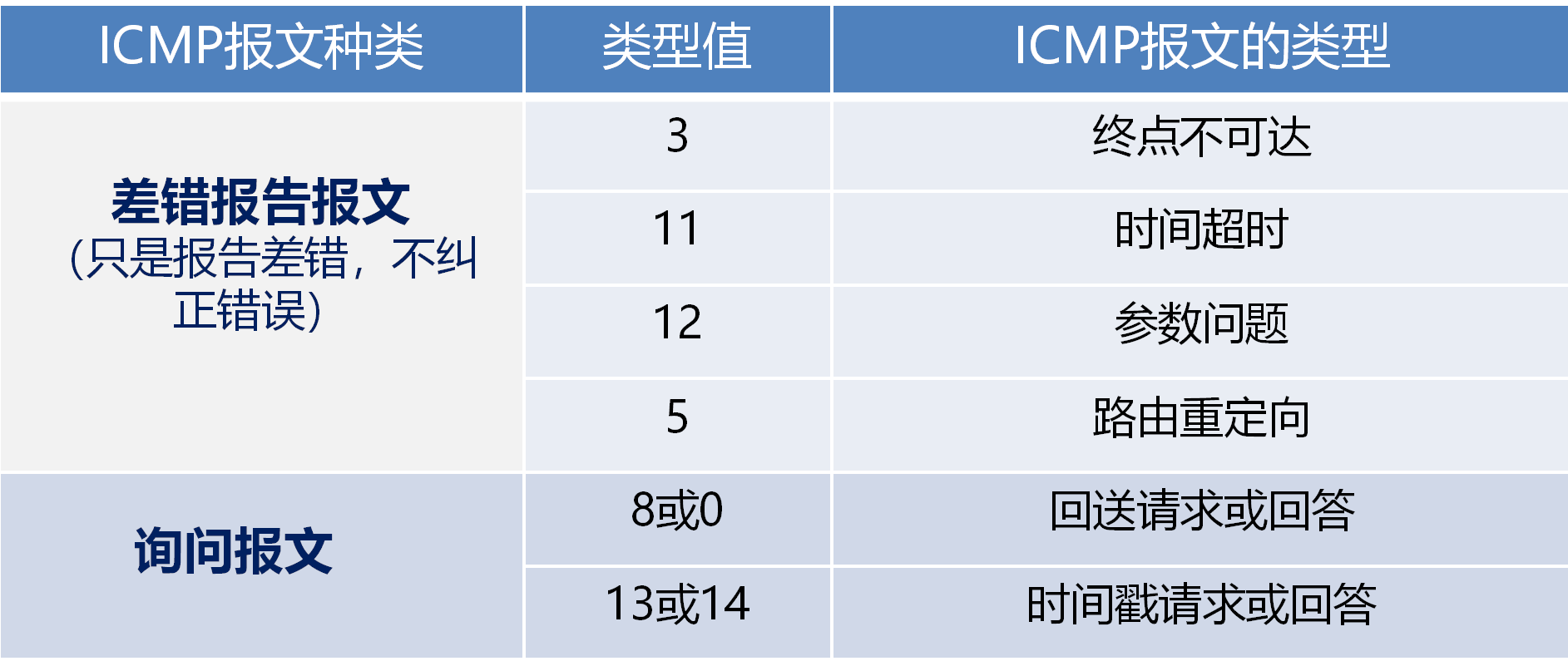
DF=0能分片，MF=0无分片了



重组时多了8个字节，其来自ICMP首部的8个字节

1480+20+8=1508

1. ICMP协议分析

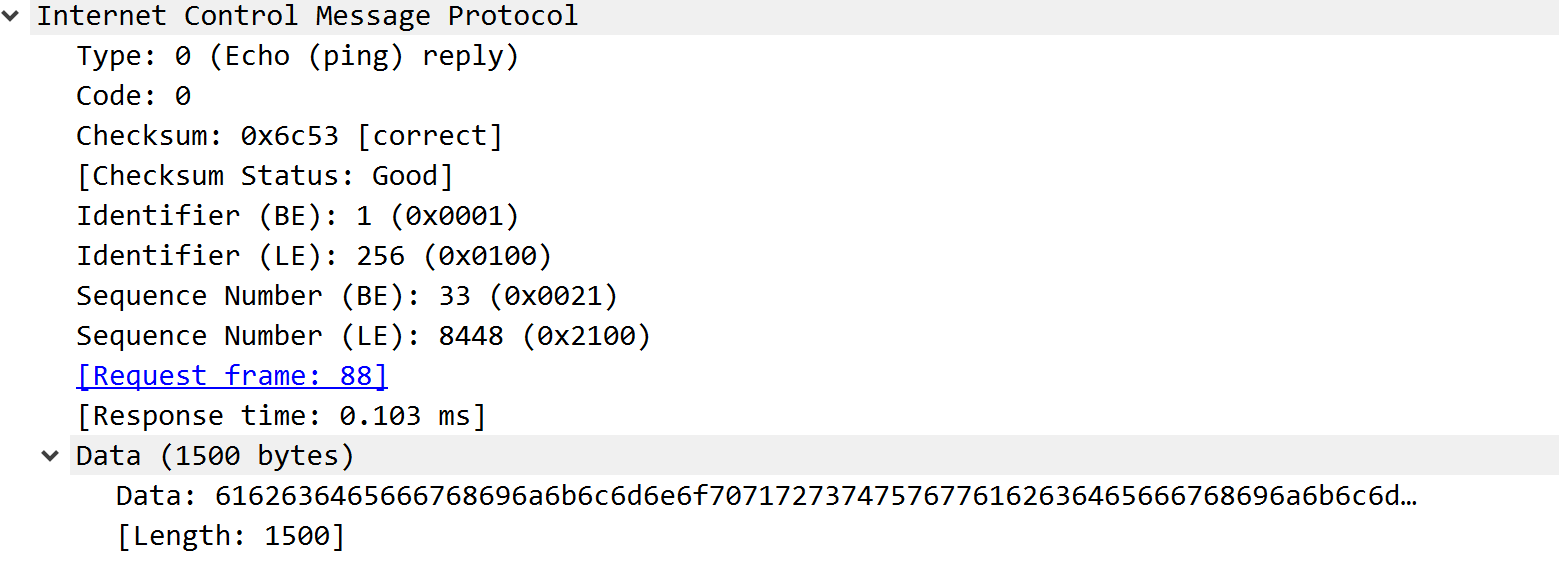


通过ping和tracet命令，了解ICMP协议的使用。

* 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。

请求：



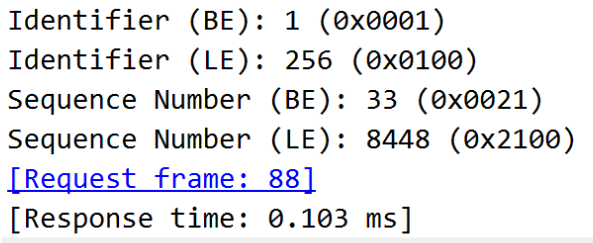


类型：0

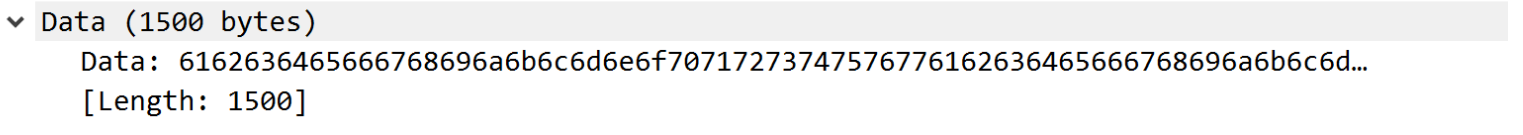
代码：0

检验和：0x6c53

中间部分：

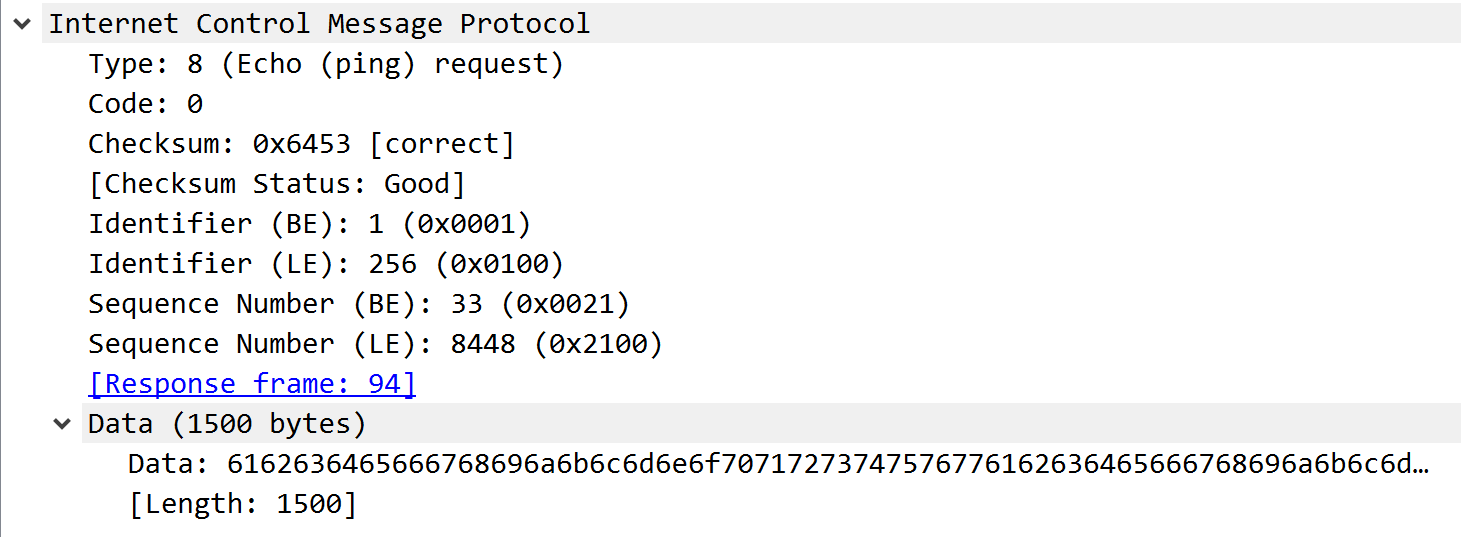


数据部分：



回复：



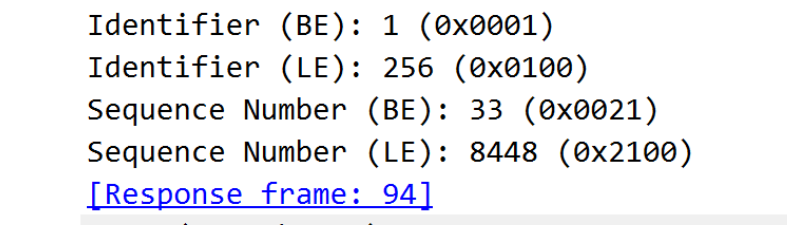


类型：8

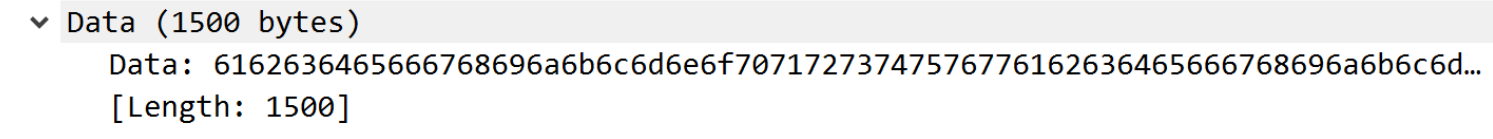
代码：0

检验和：0x6453

中间部分：



数据部分：



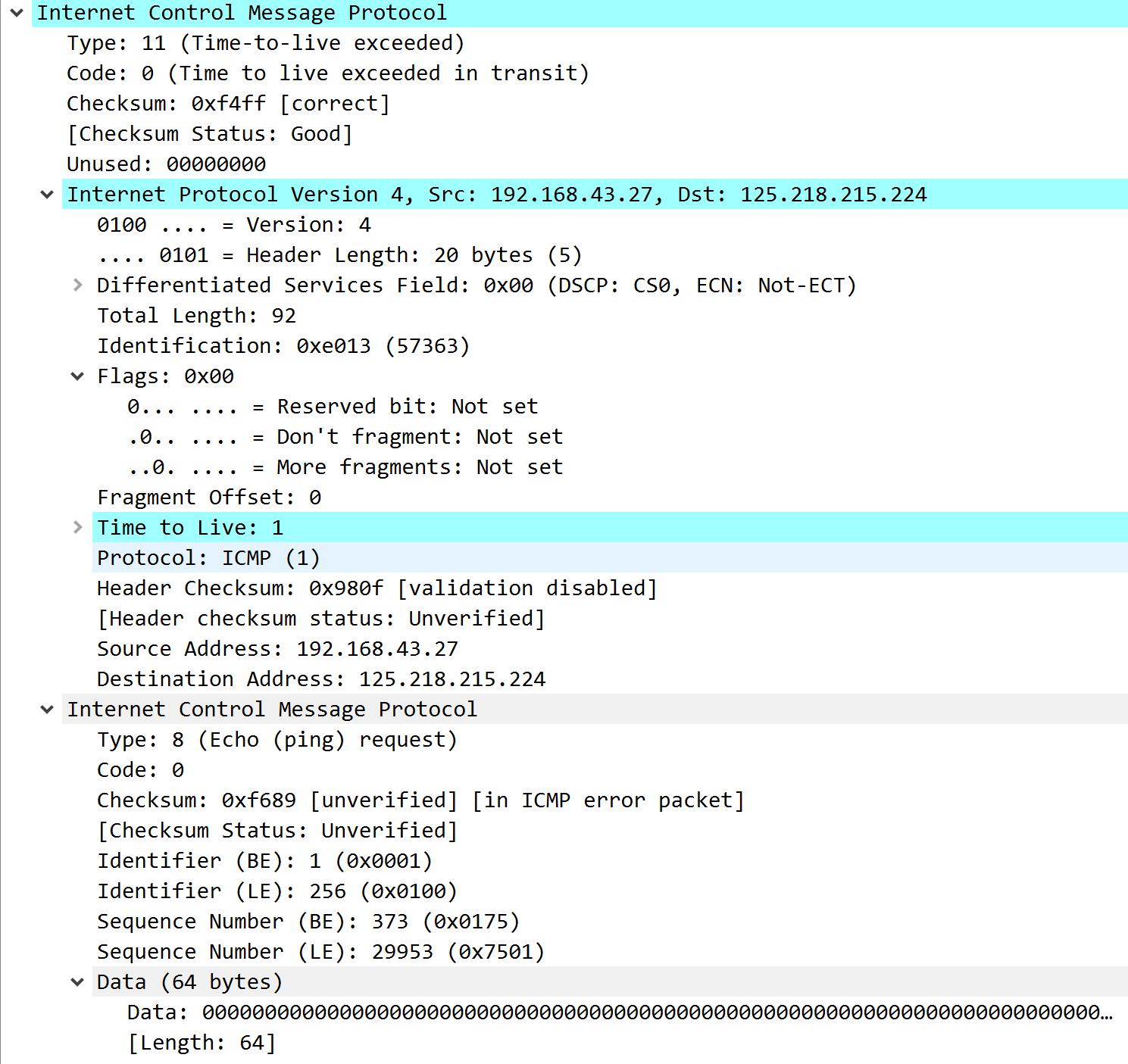
若返回了差错报文，则可能是由：

终点不可达、时间超时、参数问题、路由重定向引起的。

* 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。

类型11：时间超时





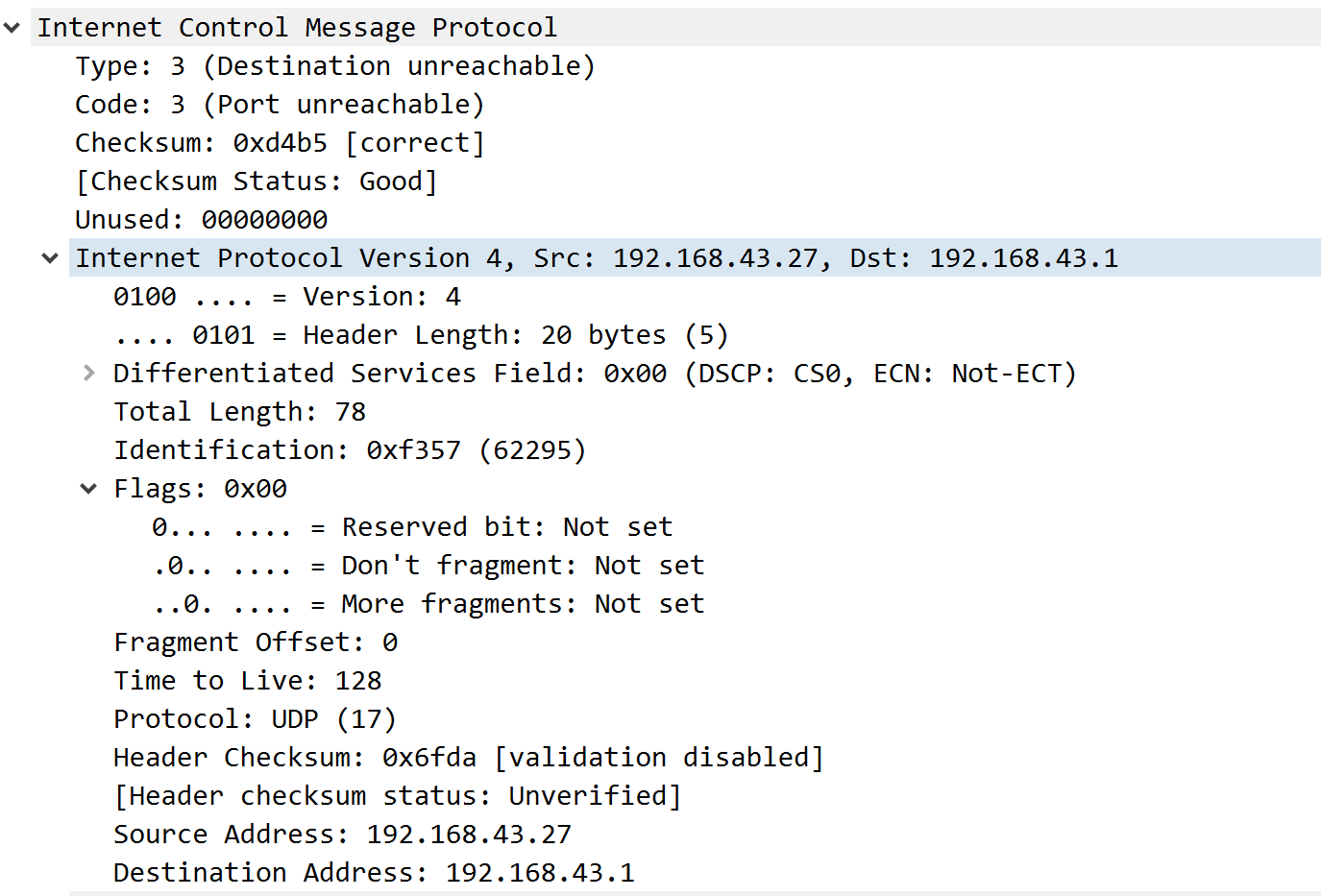
ICMP报文类型:11(请求超时)

总长度92=8（新ICMP首部8字节）+20（IP首部20字节）+8（ICMP报文首部）+56（数据56字节）

其余内容与回复请求ICMP报文一致。

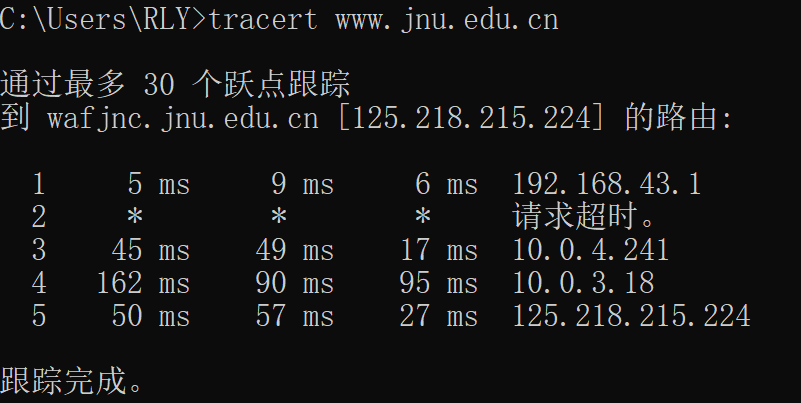
类型3：终点不可达





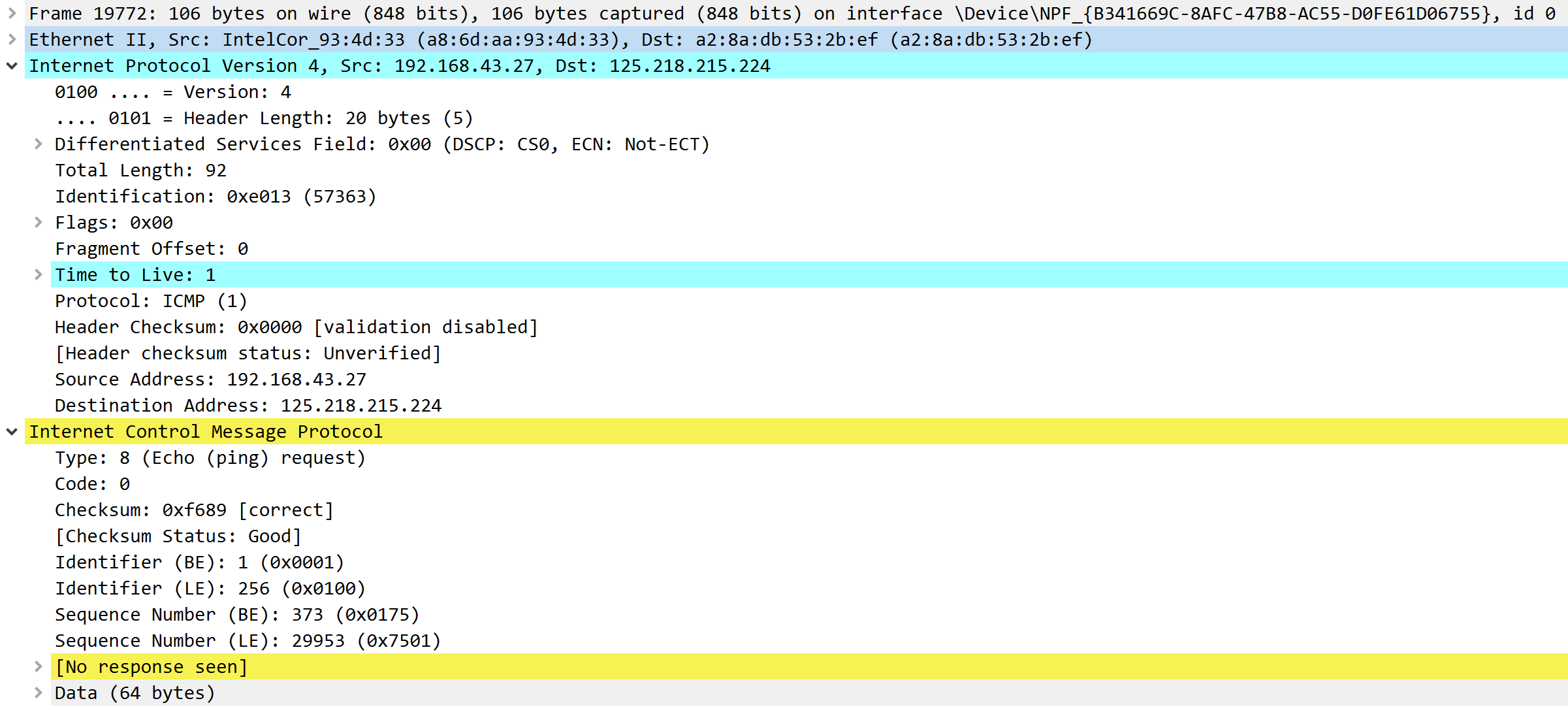
ICMP报文类型:3(终点不可达)

Tracert跟踪过程：



①第一个ICMP请求数据包,TTL=1：

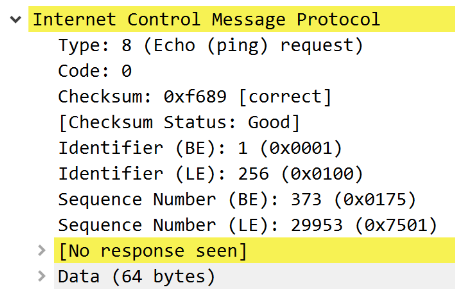




ICMP类型：8

总字节长度92=64（数据长度64字节）+8（ICMP首部8字节）+20（IP首部20字节）

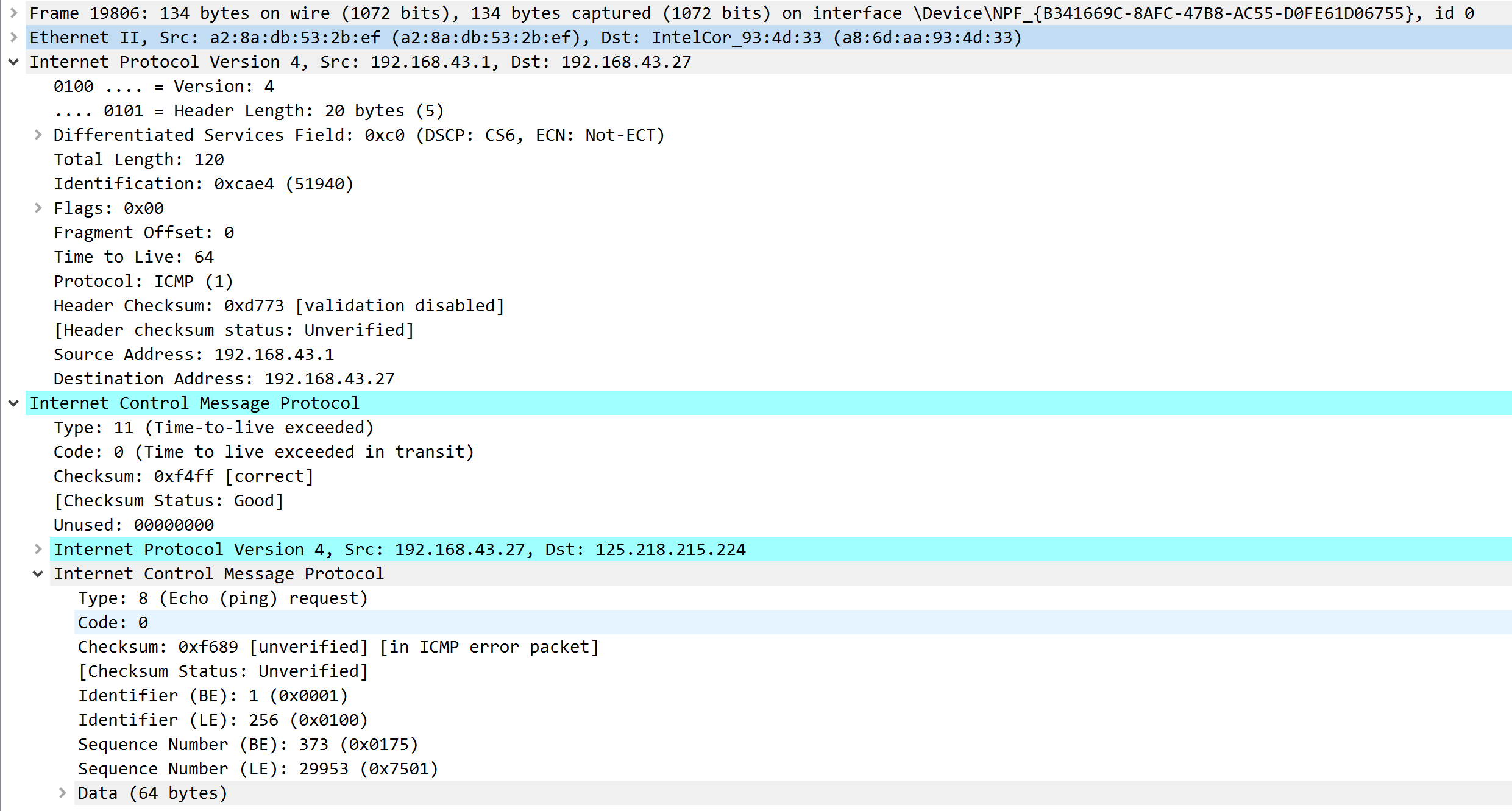
ICMP请求8字节：



Time to Live：1

②第一个TTL=1的ICMP回应数据包





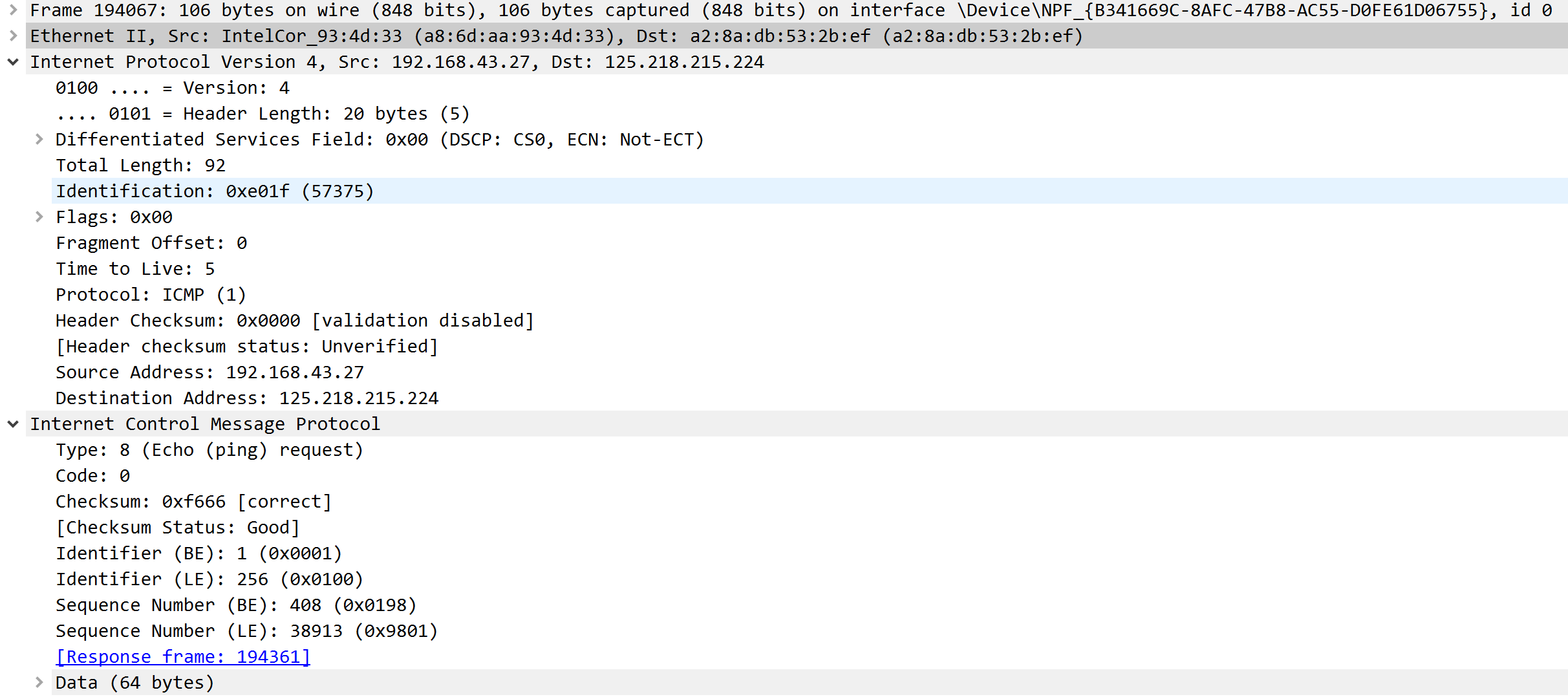
ICMP响应类型：11（请求超时）

总长度92=8（新ICMP首部8字节）+20（IP首部20字节）+8（ICMP报文首部）+56（数据56字节）

其余内容与回复请求ICMP报文一致。

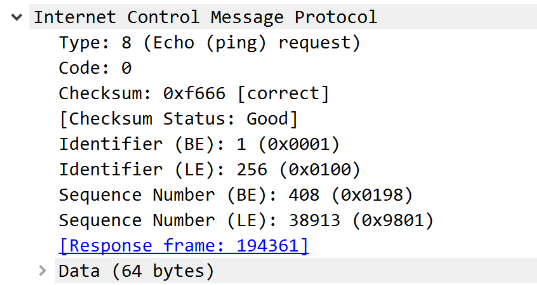
中间还有3个ICMP应答报文，共6个；

③第5个ICMP请求数据包,TTL=5



Time to Live：5

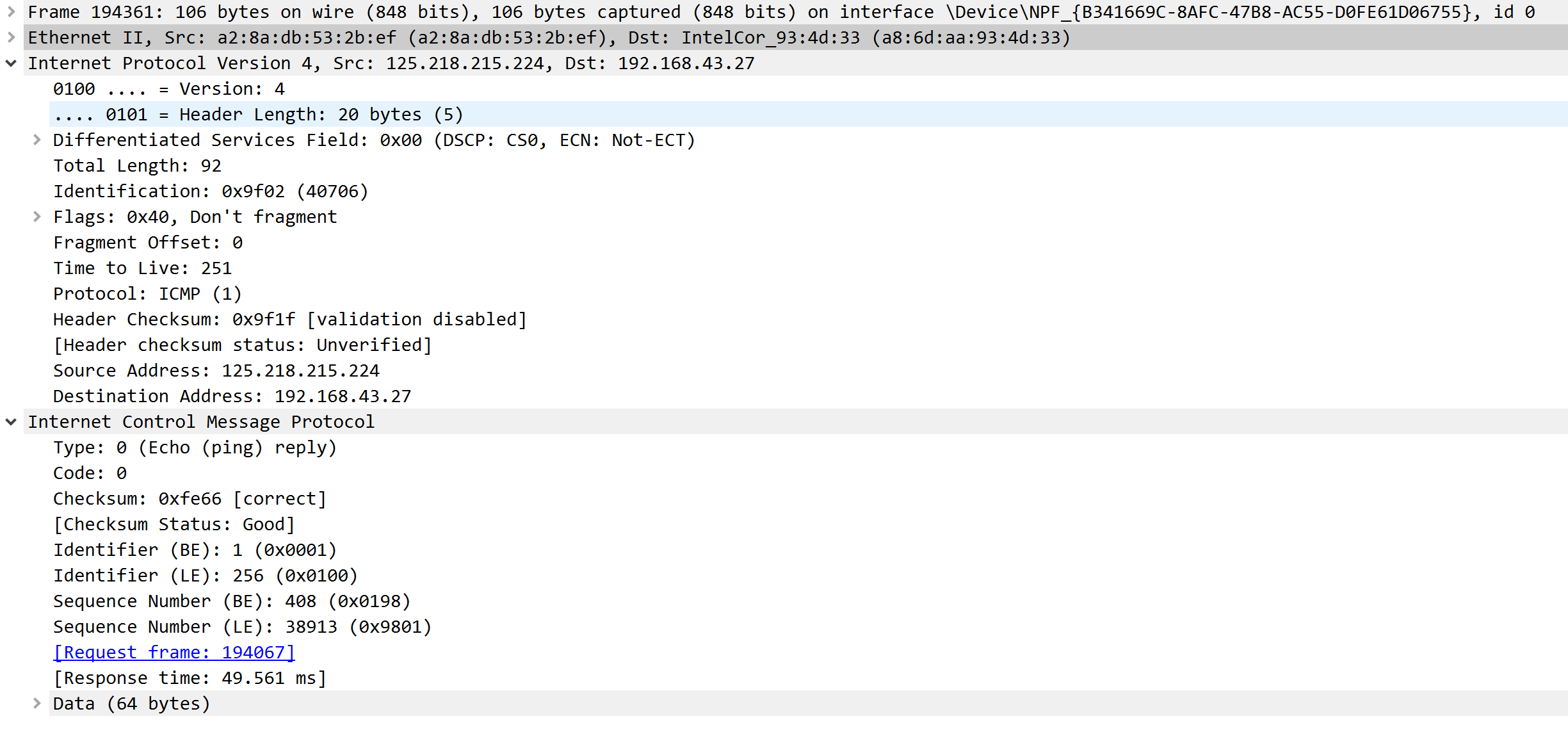
ICMP请求8字节：



目标Ip一直是：125.218.215.224

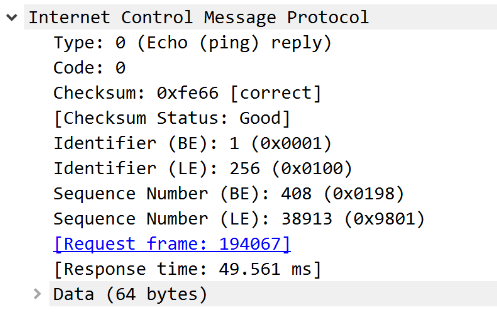
④第5个ICMP请求数据包的回应





类型：0

ICMP请求：



**Tracert的工作原理：**

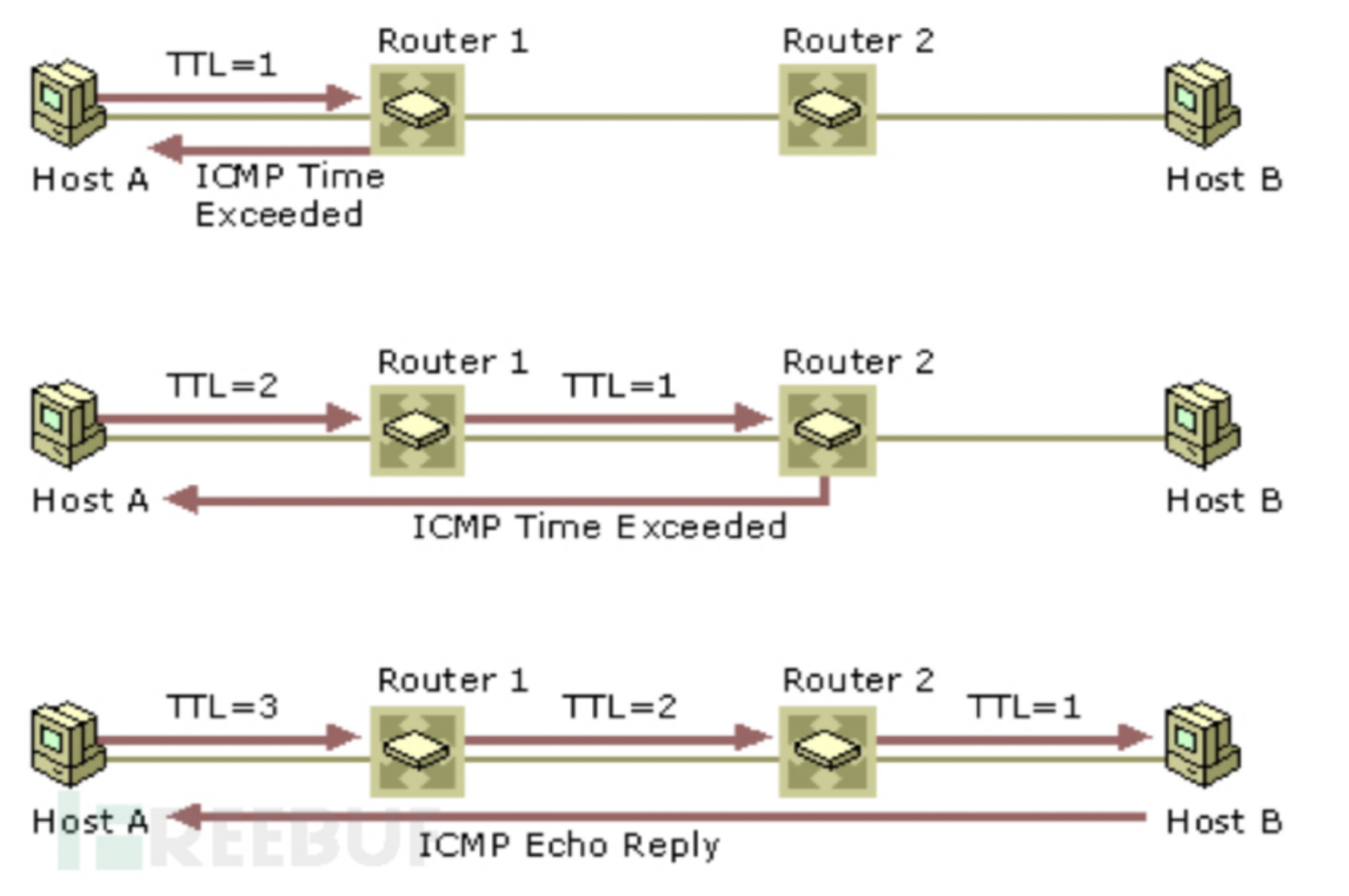
**它利用 IP 数据报中的 TTL 字段和 ICMP 时间超过差错报告报文实现对从源点到终点的路径的跟踪。**

**向目的主机发送一串ICMP回应请求包（type=8），第一个数据包的TTL=1，当经过第一个路由器时，TTL=TTL-1=0，该路由器返回一个ICMP超时差错报文，从而获取该路由器的信息；**

**源主机依次发TTL=2，TTL=3，……的ICMP回应请求包，直到最后一个请求包刚刚到达目的主机时TTL=1，目的主机不执行TTL-1操作，直接发回ICMP请求应答数据包（type=0）。**

**这样通过经过的每个路由器和目的主机返回的信息，获取了源主机到达目的主机的路由信息。**

**每个节点测试3次。**



**【思考题】（分析原因并通过实验验证）**

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？

**答：一开始如果A主机的arp表里面没有主机B的MAC地址时，就会通过广播的方式，捕获并添加主机B的MAC地址的ARP报文，再一次通信时，主机A的arp表有B的MAC地址了，所以不需要再发送ARP报文了，所以就可能不能捕获。**

1. 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？

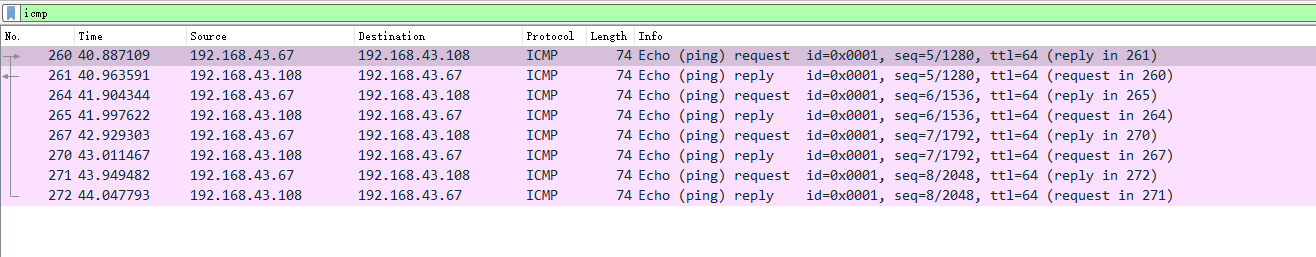
**答：ping127.0.0.1属于环回测试，只是检查本地TCP/IP协议是否设置，并不会经过网卡，所以没有存在通信这一过程，因此不能捕获到ICMP报文。ping本机也不能收到报文，不经过网卡，环回驱动会对它进行处理。**

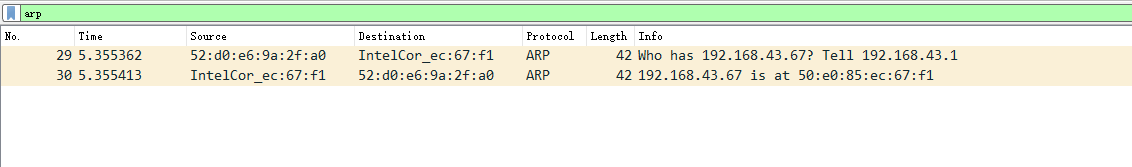
1. 在ping 的过程中，返回信息“Request timed out” 和“Destination Host Unreachable”分别是由哪些情况引起的？

**答：返回信息“Request timed out” 指虽然源主机的路由表具有到达目标的路由，但是由于一些原因无法到达，便会出现请求超时的提示，可能是因为对方防火墙没关，也有可能是对方关机了，或者ip不匹配。“Destination Host Unreachable”表示路由表中没有到达目标的路由。可能是因为双方不在同一片局域网。**

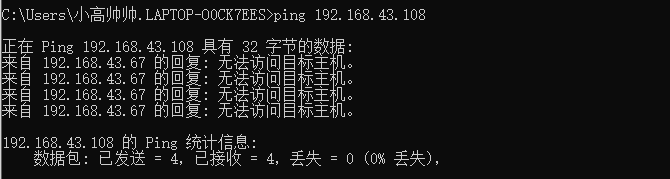
4、请通过实验**验证**：

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。

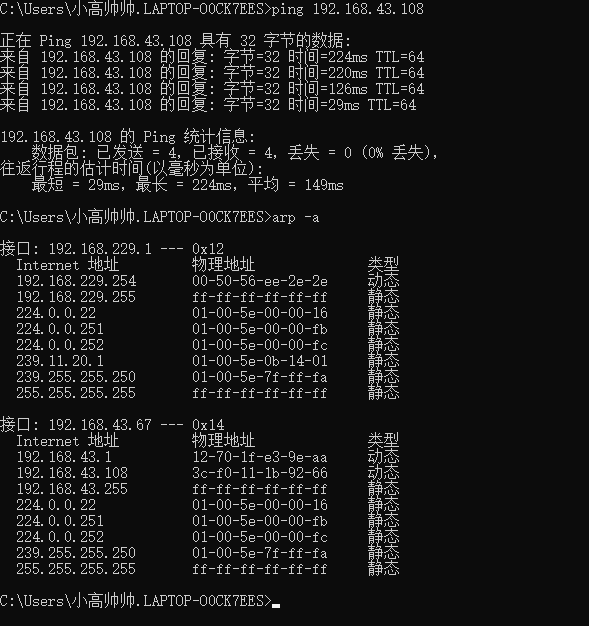




主机如果设置“网关”，同一网段的主机通信不通过网关转发，用ping命令测试，用嗅探器可以捕获所有测试数据包，能看到对方主机的MAC地址。不同网段的主机之间通信需要网关转发，用ping命令测试，能看到网关的MAC地址（包括能通信或不能通信）。

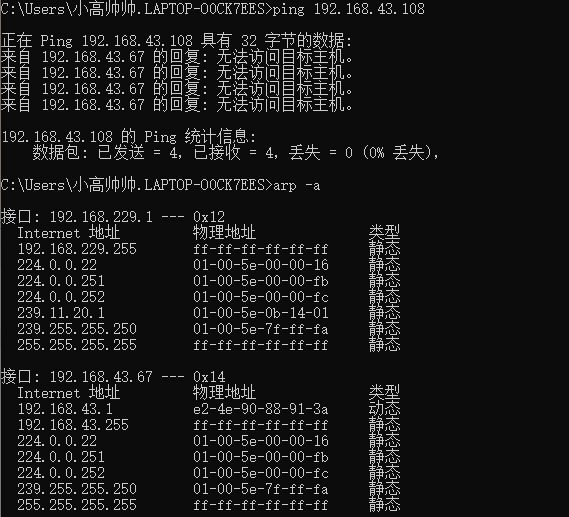
5、通过下面实验**理解网关**

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，能看到对方的物理地址。

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。



ping不同，arp也没有对方的物理地址。