

**《计算机网络》实验报告**

(2022~2023 **学年第一学期**)

## 实验名称：IP与ICMP分析

## 学 院：软件学院

## 姓 名：郁万祥

## 学 号：2013852 指导老师：张圣林

### 2022 年 11 月 22

实验名称 (实验 2:IP与ICMP分析)

# 实验目的

IP 和 ICMP 协议是 TCP/IP 协议簇中的网络层协议，在网络寻址定位、数据分组转

发和路由选择等任务中发挥了重要作用。本实验要求熟练使用 Wireshark 软件，观察 IP

数据报的基本结构，分析数据报的分片；掌握基于 ICMP 协议的 ping 和 tracert 命令ࣿ

其工作原理。

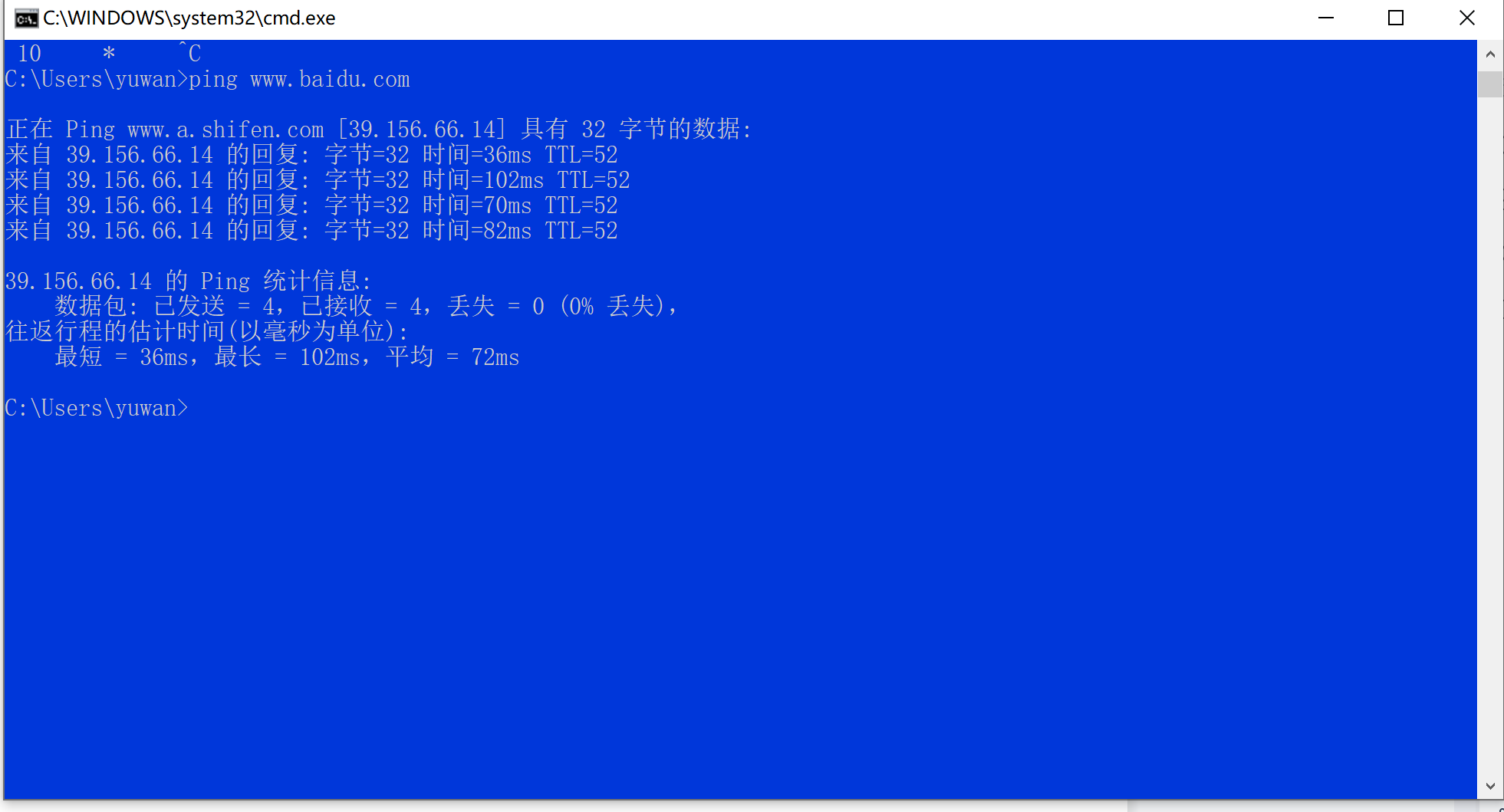
# 实验条件

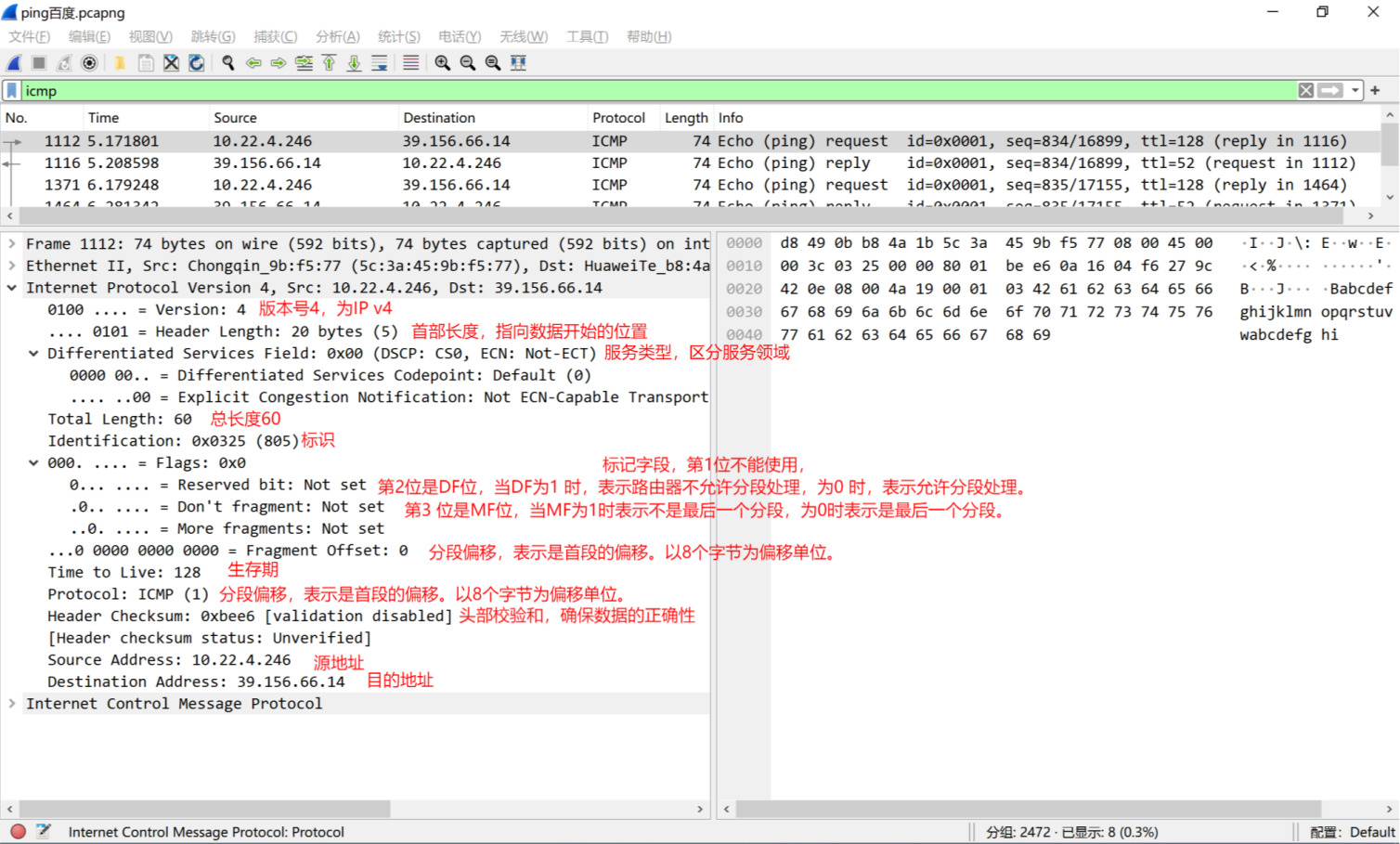
装有 Wireshark 软件的 PC 机一台，处于局域网环境

# 实验报告内容及原理

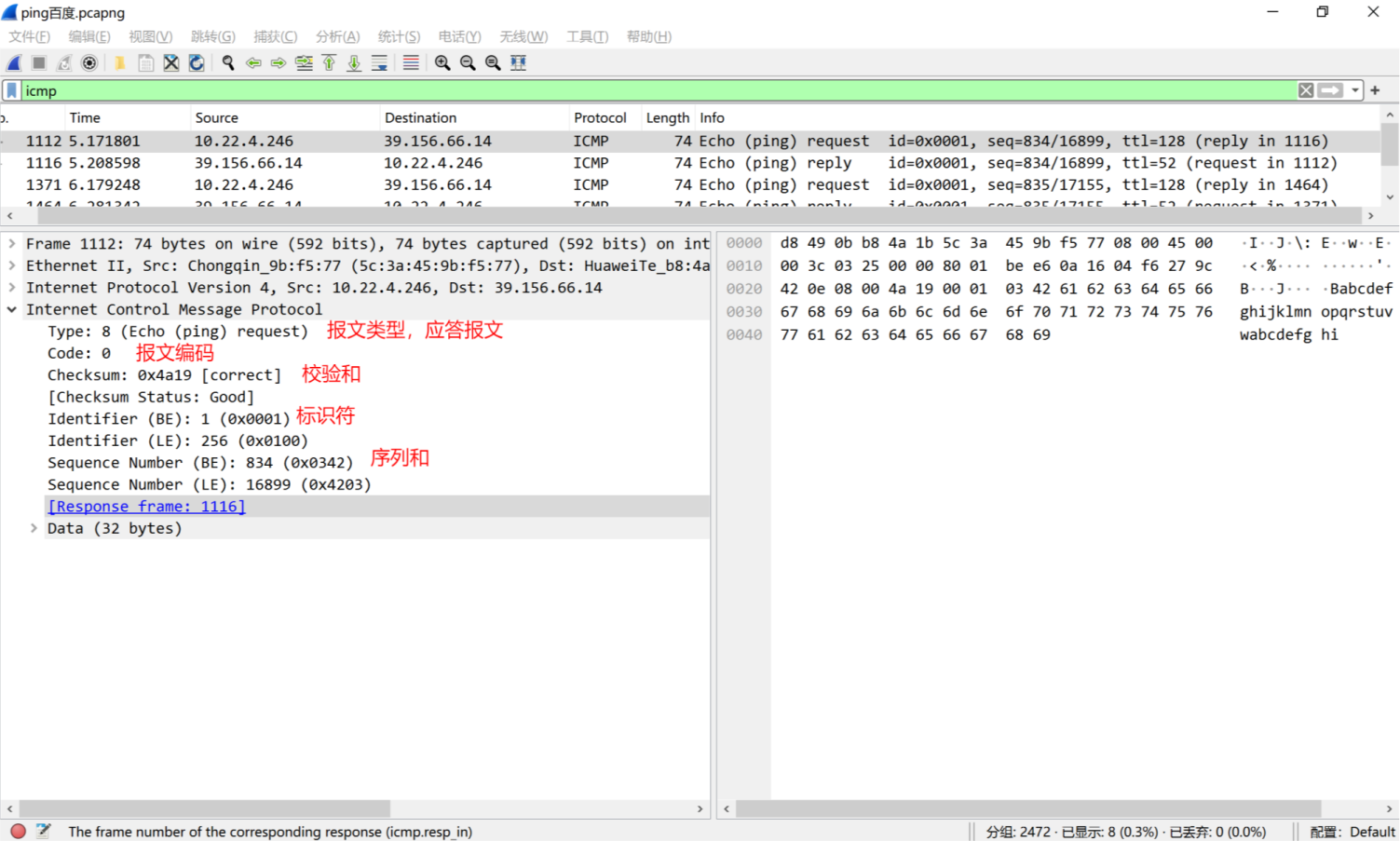
1. **实行ping命令（以ping [www.baidu.com为例），解释任意一个IP数据报的首部。](http://www.baidu.com为例），解释任意一个IP数据报的首部。)**

文件见 ping百度.pcapng



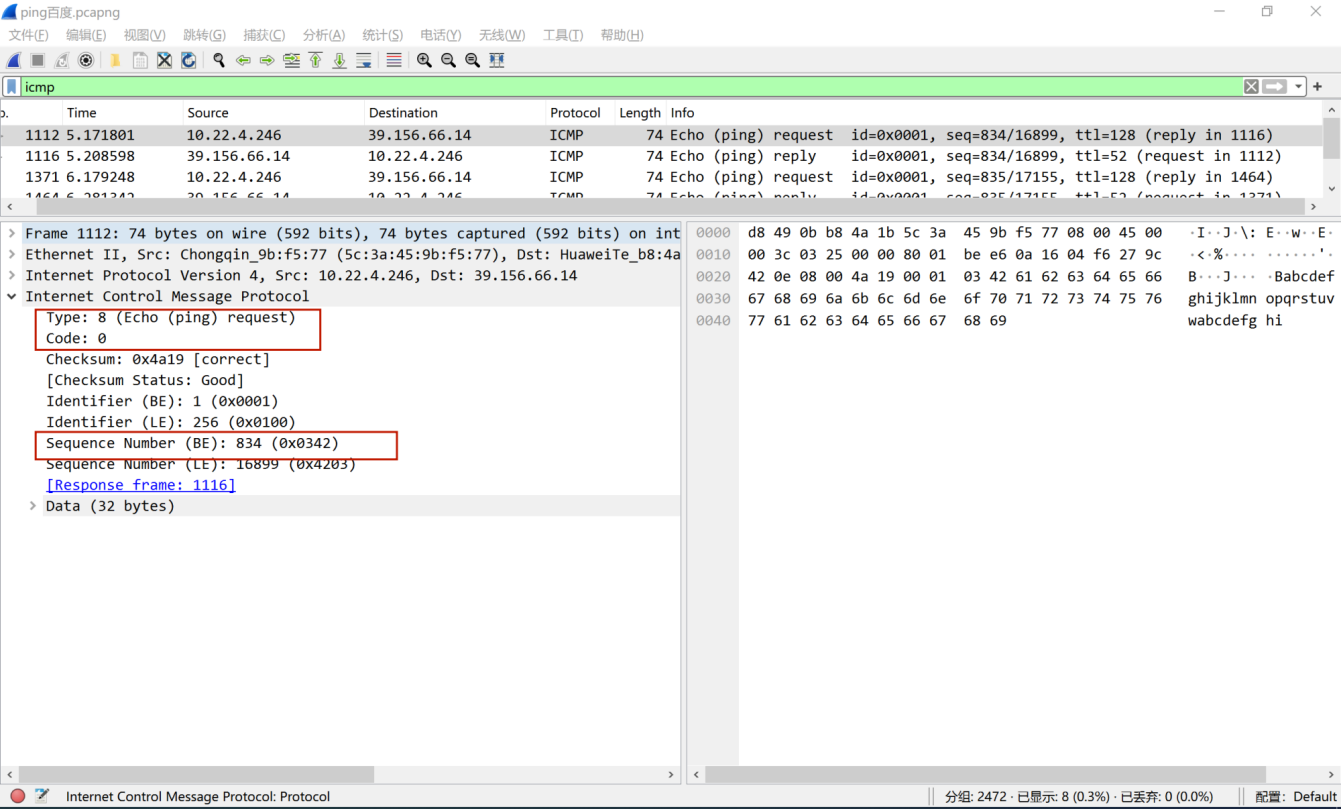


1. **对上述ping命令中的任意一个ICMP协议进行分析。**

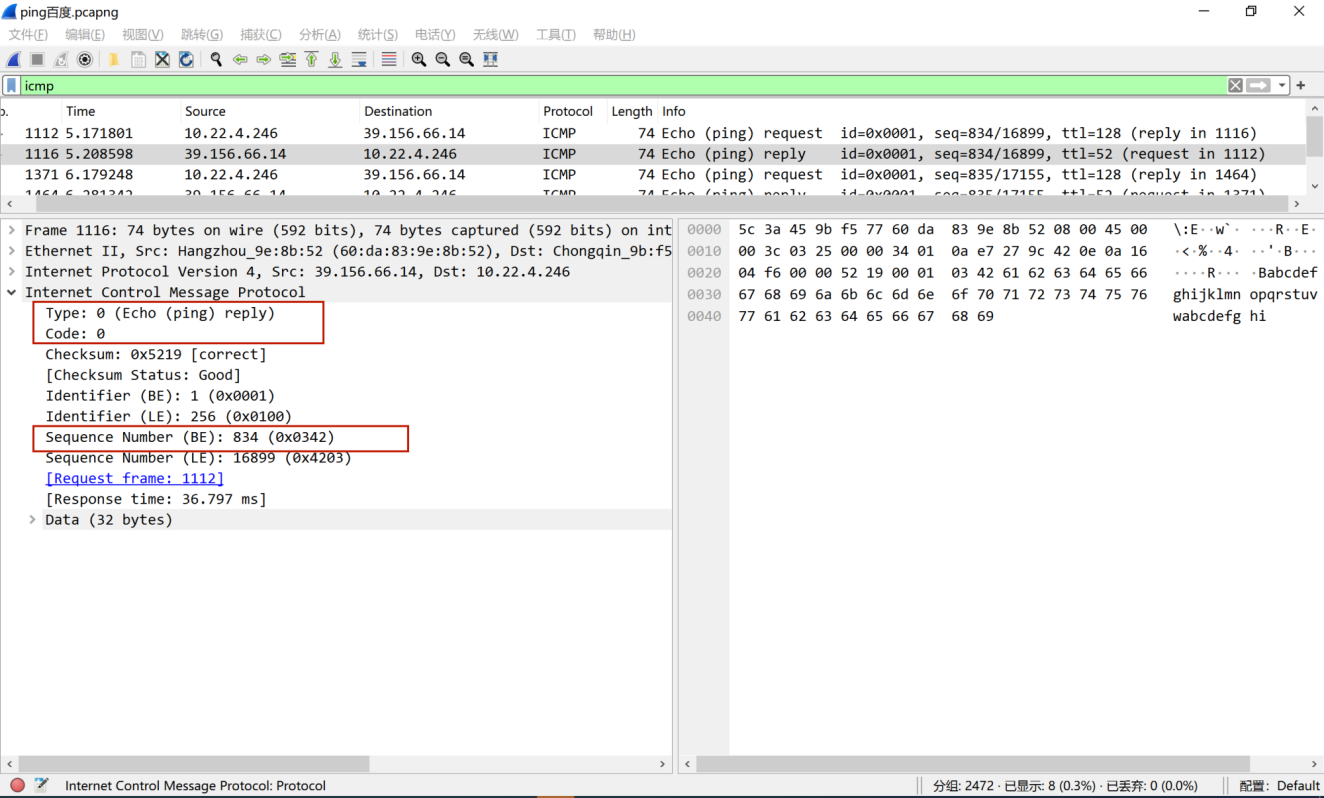


1. **对上述ping命令得到的Echo请求帧和回应帧进行对比。**

请求帧：



回应帧：

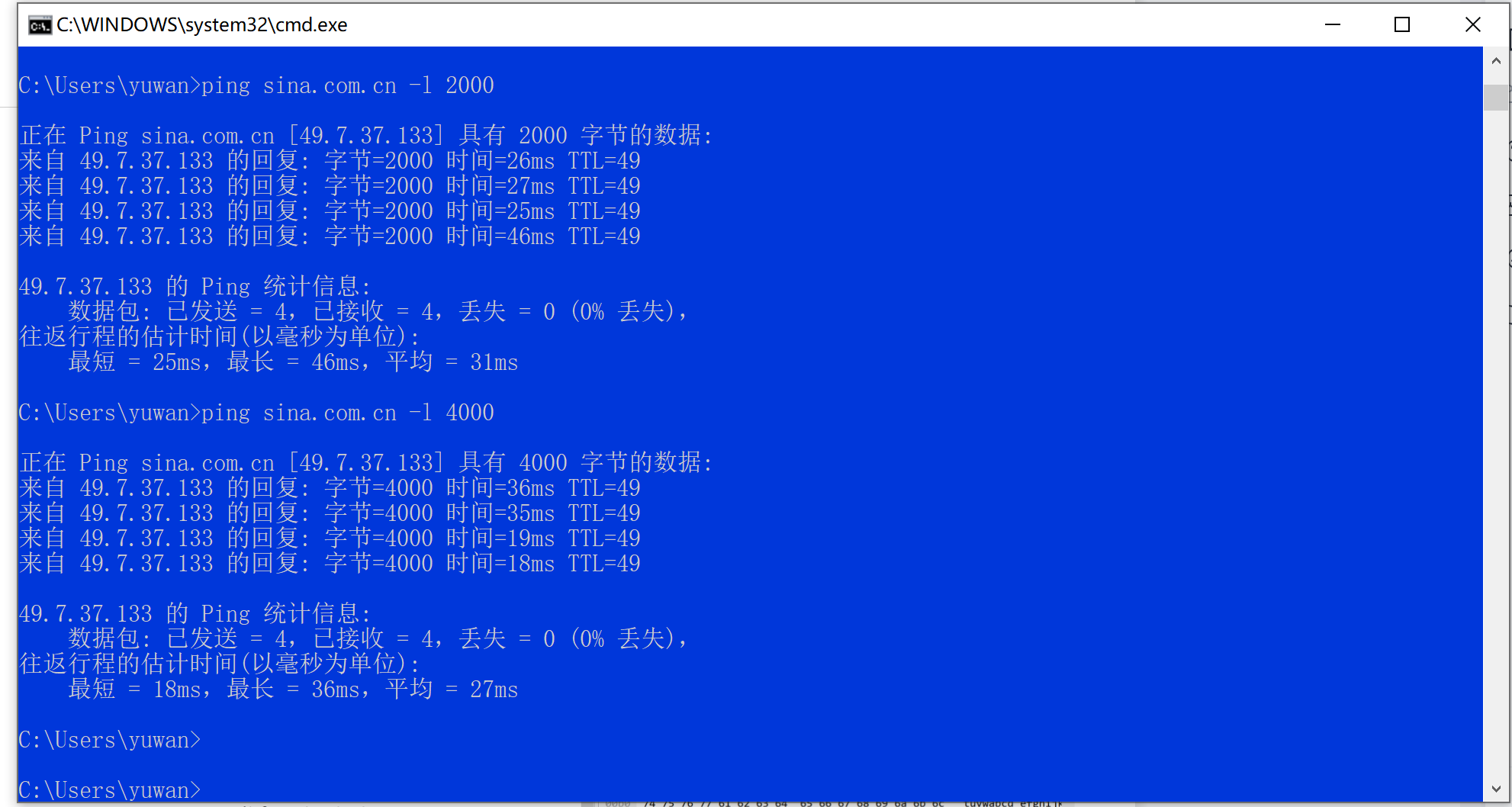


请求类型是8，代码是0，表示请求，回应类型是0，代码是0，表示应答。

回应和请求的Identifier(BE)均834（0x342）,说明该回应是响应的该请求。

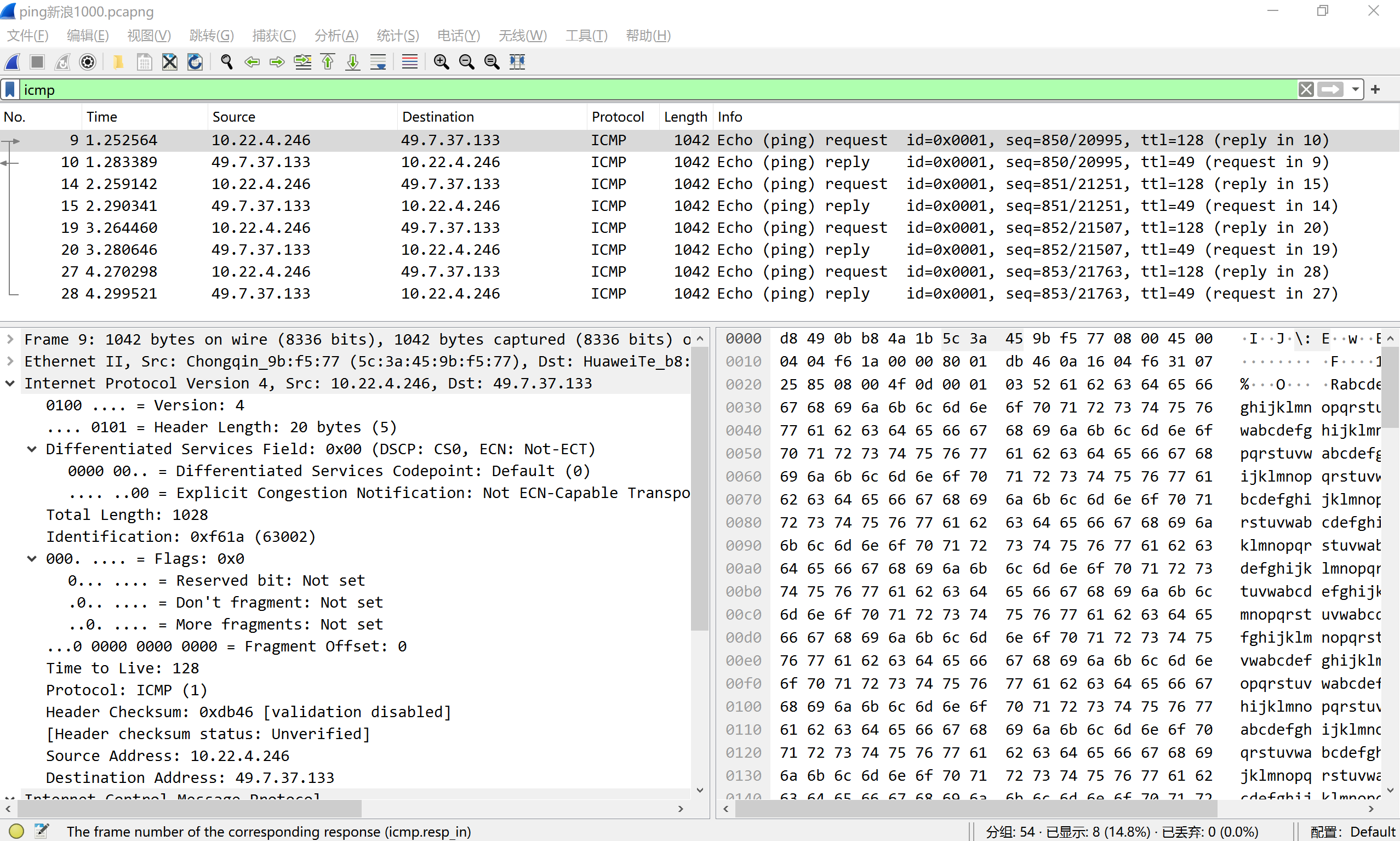
IP头部字段Src和Dst相反，TTL也不同。

1. **改变ping的长度参数（1000、2000、4000），(以ping sina.com.cn为例)解释IP数据包的 分片情况。**



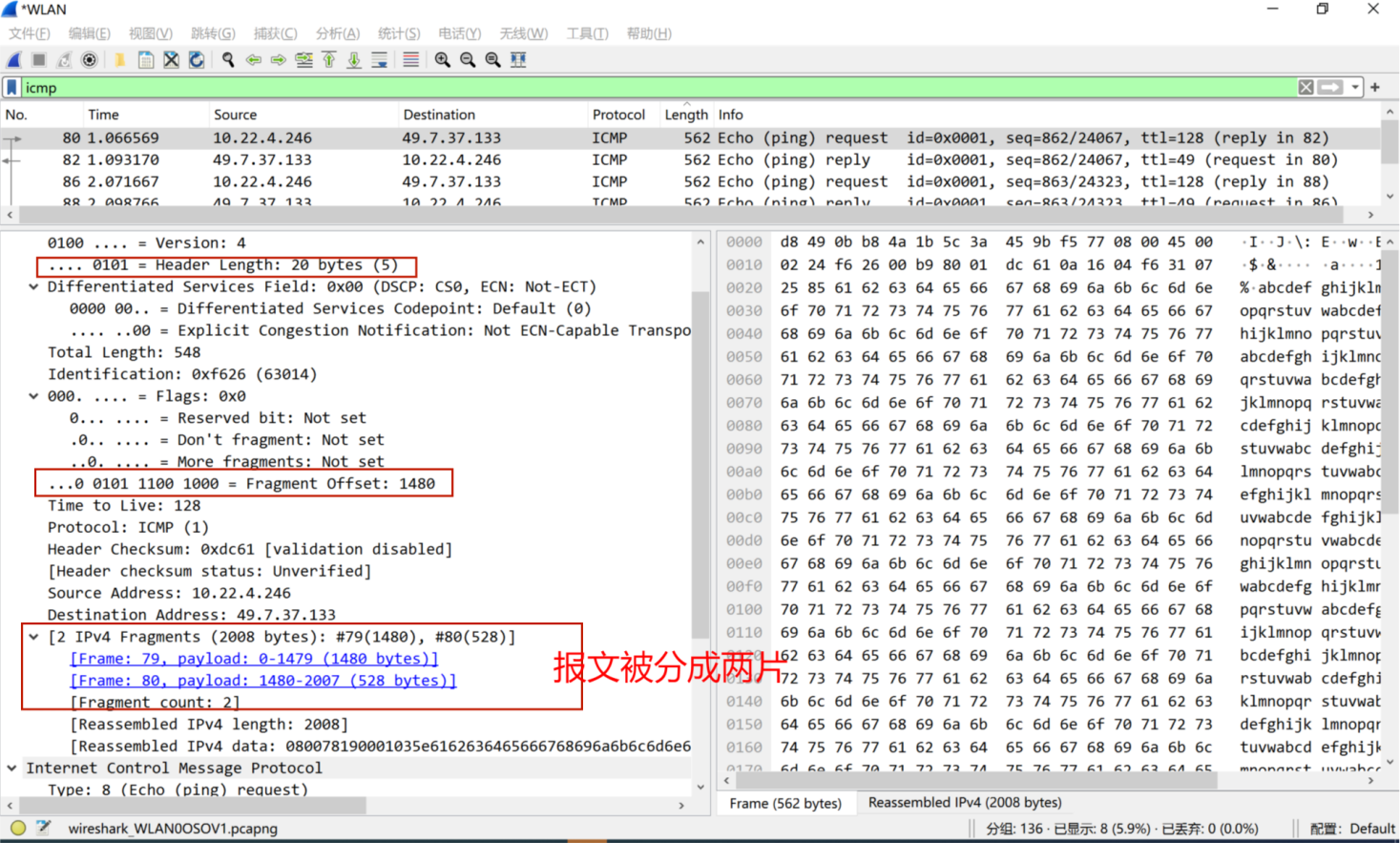
文件见 ping新浪1000.pcapng、ping新浪2000.pcapng、ping新浪4000.pcapng

①Ping sina.com.cn -l 1000



因为ping下来的都是长度为1000的数据，而以太网中的MTU为1500，所以不存在分片。

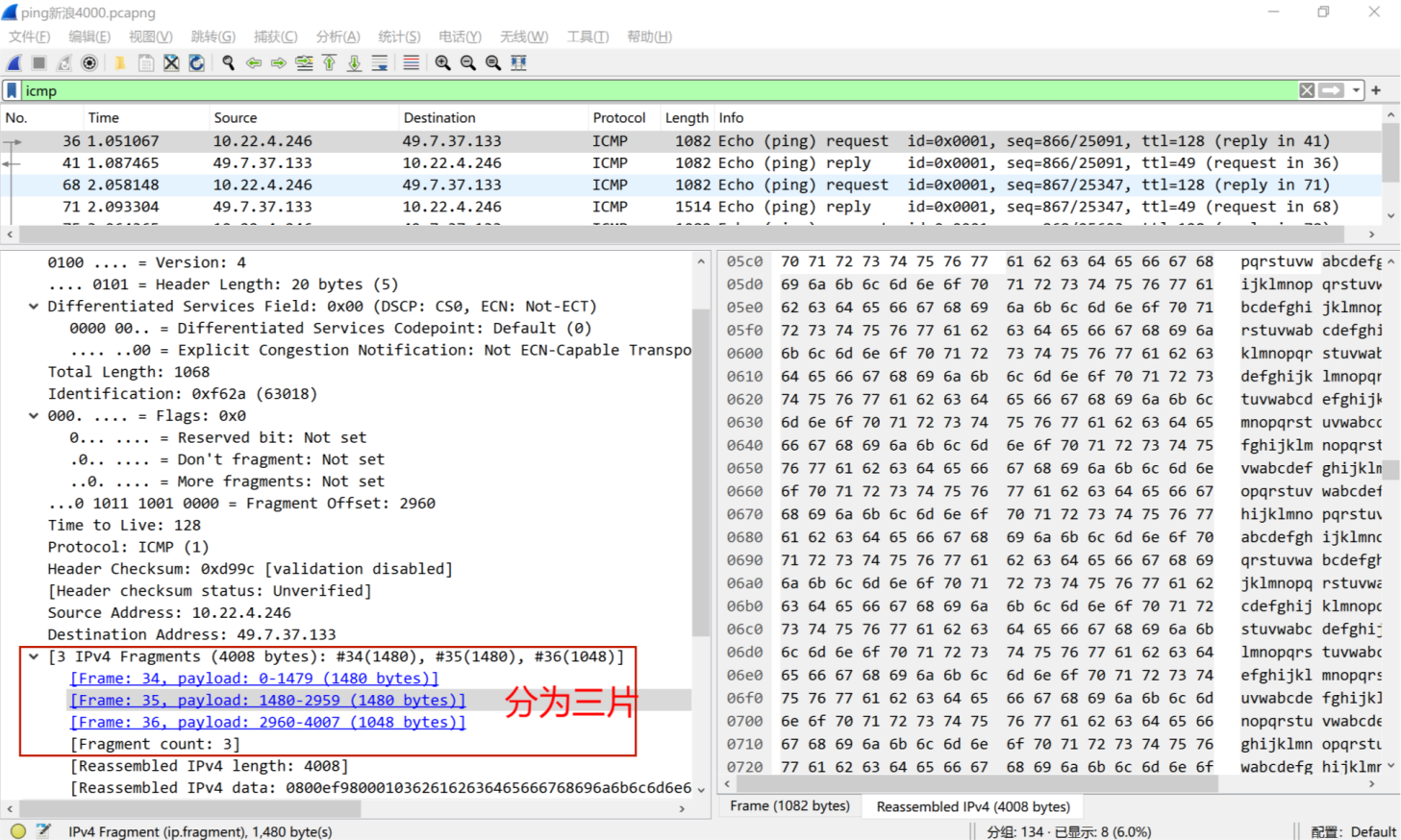
②Ping sina.com.cn -l 2000



MTU计算：我们可以看到，此时分片为2，而分片偏移为1480，再加上头部长度为20，所以说 明第二段的报文头部所在位置为1501，也就是第一片报文长度为1500，也就是MTU。

此时ping到的是数据长度为2000的数据报文，然而MTU为1500，所以需要将每一条ICMP报文分 成两片。

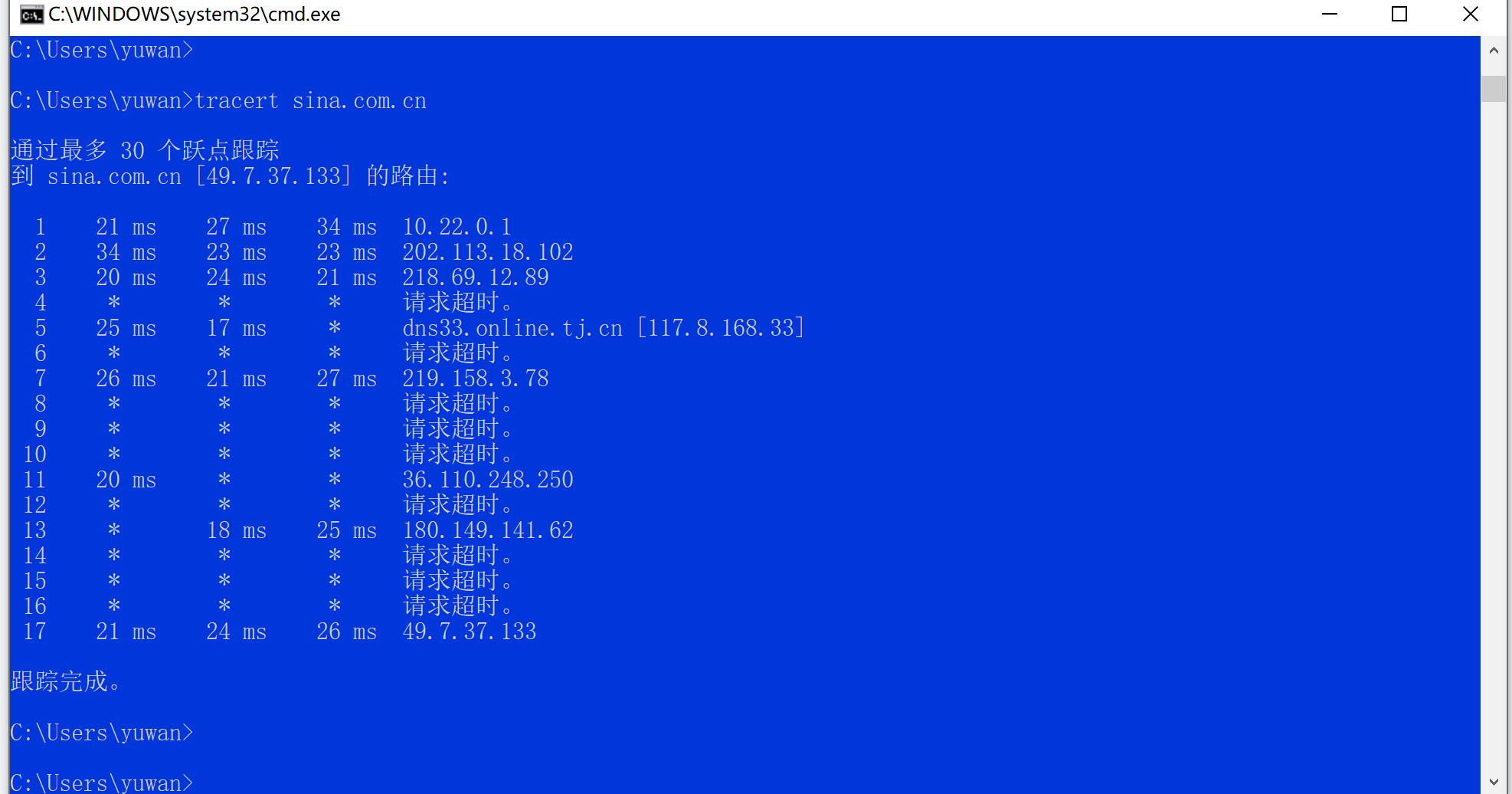
③Ping sina.com.cn -l 4000

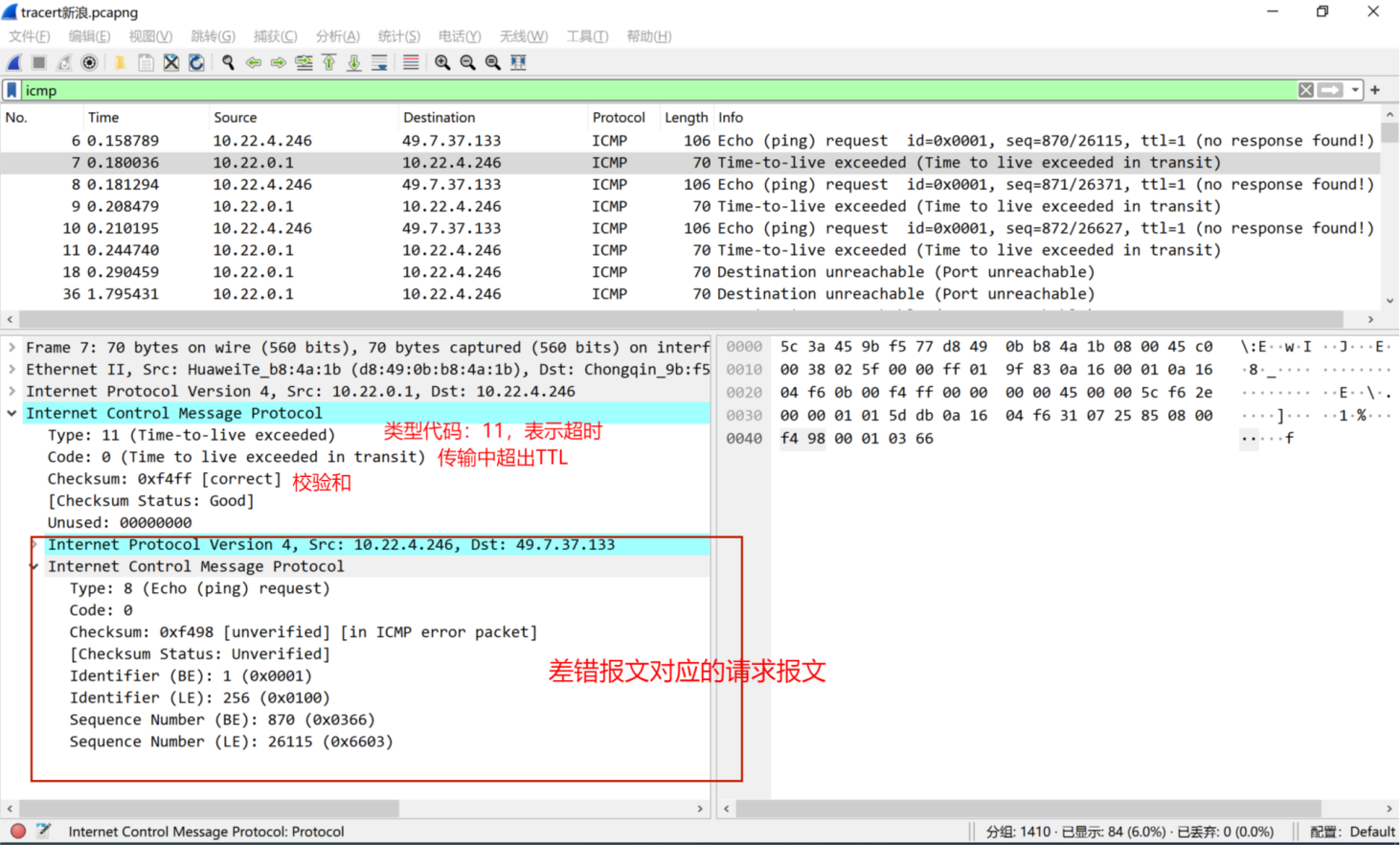


此时ping到的是数据长度为4000的数据报文，然而MTU为1500，所以需要将每一条ICMP报文分 成三片。

1. **实时tracert命令（以tracert [sina.com.com为例），解释任意一个ICMP差错报文的结构。](http://www.baidu.com为例），解释任意一个ICMP差错报文的结构。)**

**文件见tracert新浪.pcapng。**





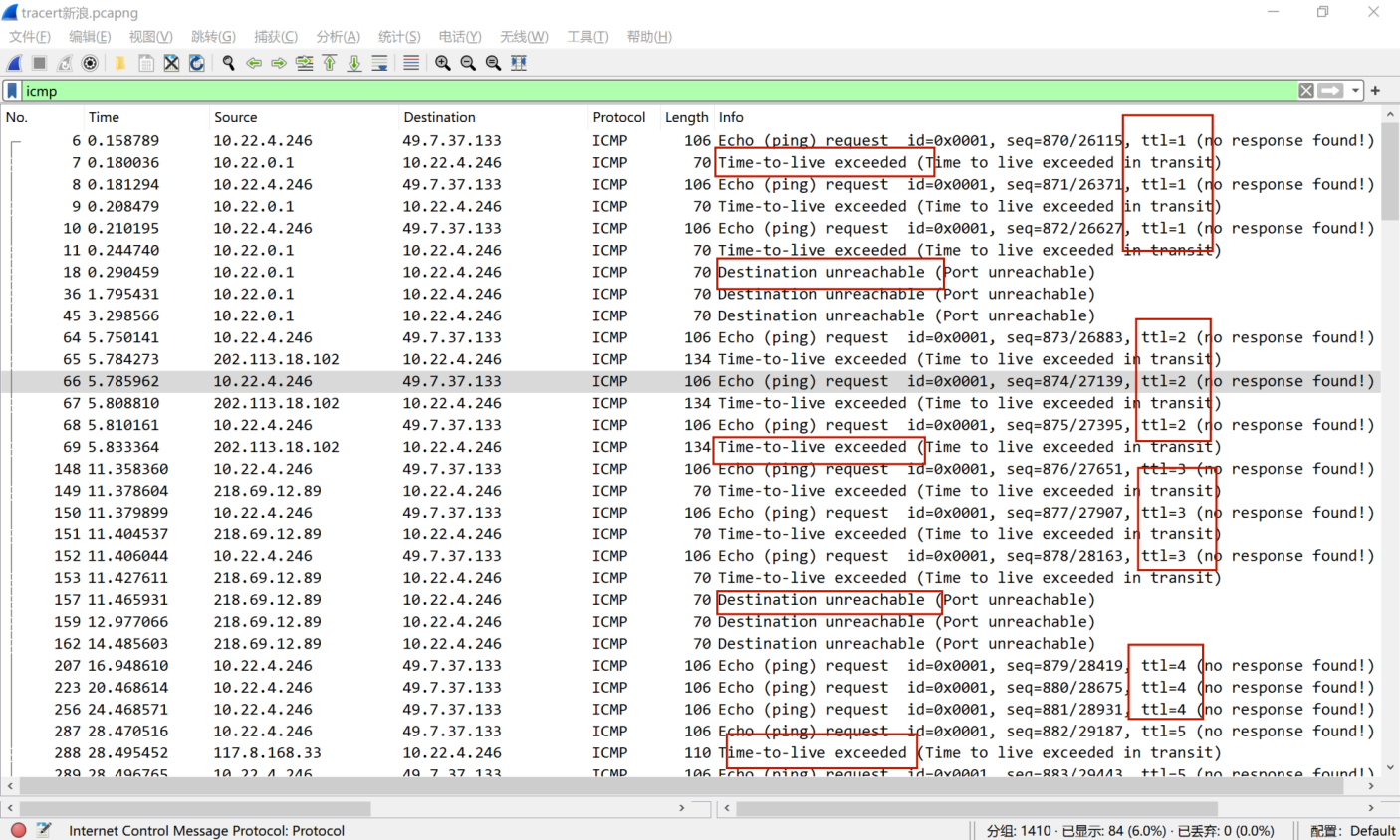
1. **描述tracert工作过程**

Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网 络上其他主机的路由。

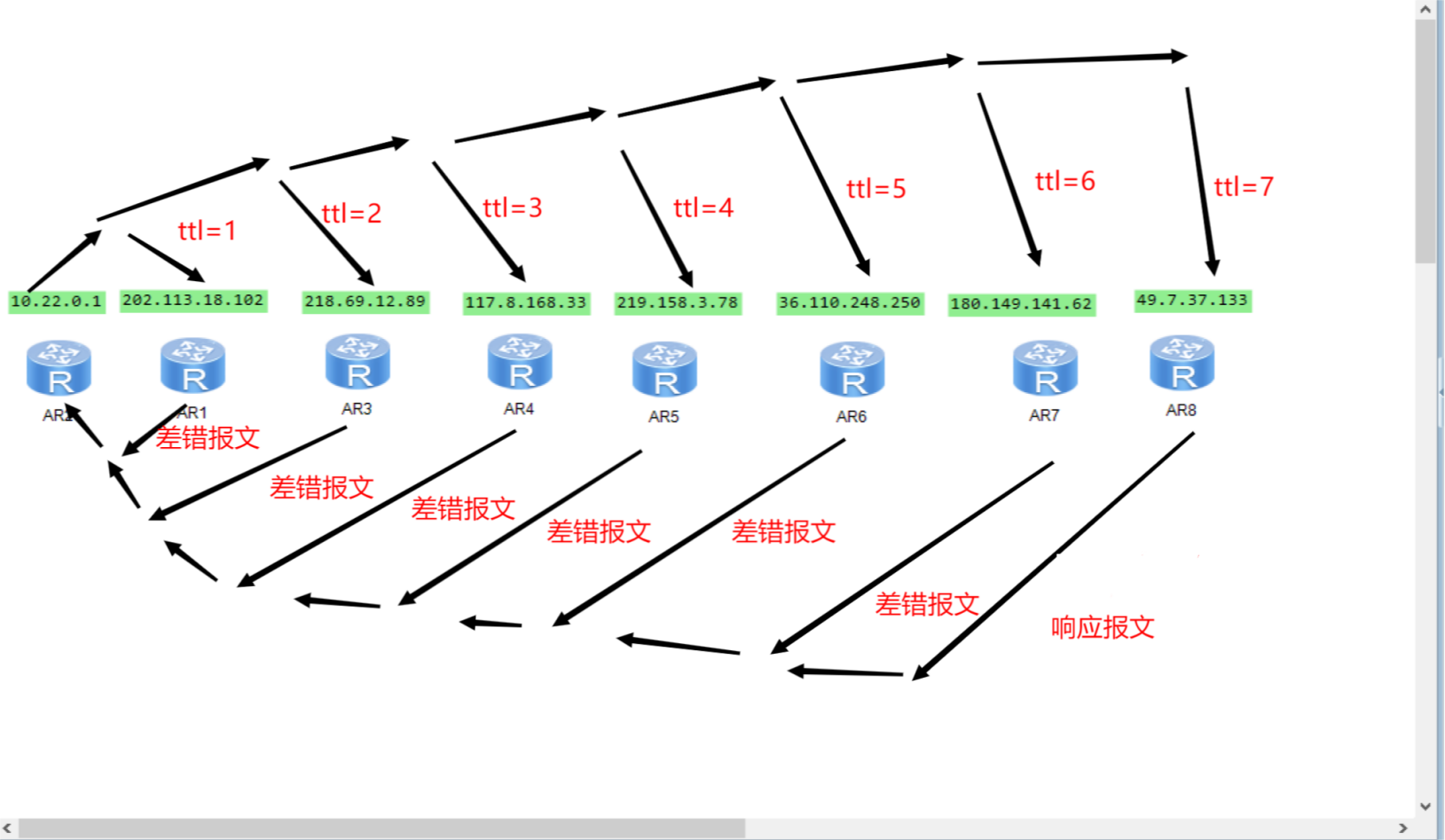
首先，tracert送出一个TTL是1的IP数据包到目的地，当路径上的第一个路由器收到这个数 据包时，它将TTL减1。此时，TTL变为0，所以该路由器会将此数据包丢掉，并送回一个 「ICMP time exceeded」消息（包括发IP包的源地址，IP包的所有内容及路由器的IP地 址），

tracert收到这个消息后，便知道这个路由器存在于这个路径上，接着tracert再送出另一个 TTL是2的数据包，发现第2个路由器......

tracert每次将送出的数据包的TTL加1来发现另一个路由器，这个重复的动作一直持续到某个 数据包抵达目的地。当数据包到达目的地后，该主机则不会送回ICMP time exceeded消息， 一旦到达目的地，由于racert通过UDP数据包向不常见端口(30000以上)发送数据包，因此会 收到「ICMP port unreachable」消息，故可判断到达目的地。



**7、结合上述得到的ICMP报文记录画出数据交互示意。**



# 实验结论及心得体会

1. 经常ping命令会显示timeout：可能是网络问题，可以多ping几次，或者换几个ip地址进行ping命令。
2. 分片的数据包不能够查看，将wireshark首选项里面关掉一个Ipv4的选项，才能显示所有帧的信息。