实验 4 ICMP 协议分析

4．1 实验目的

掌握 ICMP 协议的工作原理，理解 ICMP 分组结构。

4．2 实验环境

1．安装科来网络分析系统的连网的 Windows XP 主机两台。

2．实验分组：两名同学一组，轮流进行实验。

4．3 实验内容

用 ping 命令和科来网络分析系统分析 ICMP 包的基本结构以及回显请求与应答消息、目标不可达、超时等消息的 ICMP 报文的异同。

4．4 实验步骤

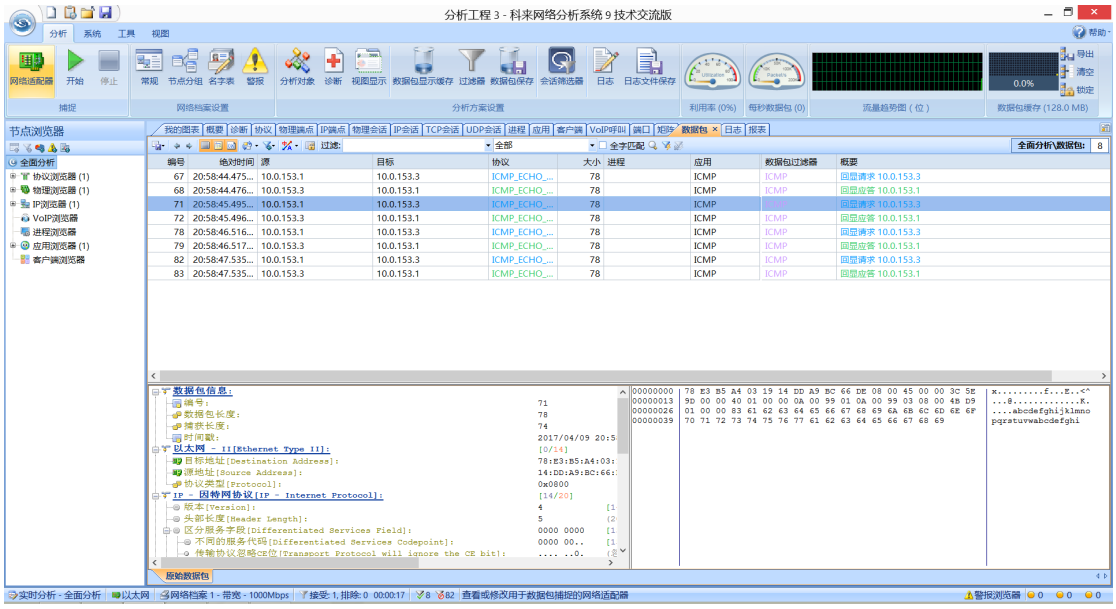
在两台 PC 机上启动科来网络分析系统，开始抓包。

1．回显请求及应答消息。

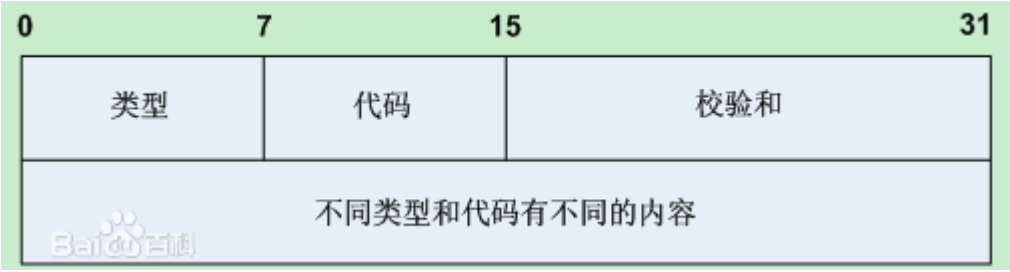
1）在 PC1 上运行命令：ping 临机 IP。

```
C:\WINDOWS\system32>ping 10.0.153.3

正在 Ping 10.0.153.3 具有 32 字节的数据:
来自 10.0.153.3 的回复: 字节=32 时间=1ms TTL=64
来自 10.0.153.3 的回复: 字节=32 时间=1ms TTL=64
来自 10.0.153.3 的回复: 字节=32 时间=1ms TTL=64
来自 10.0.153.3 的回复: 字节=32 时间=1ms TTL=64

10.0.153.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 1ms, 平均 = 1ms
```

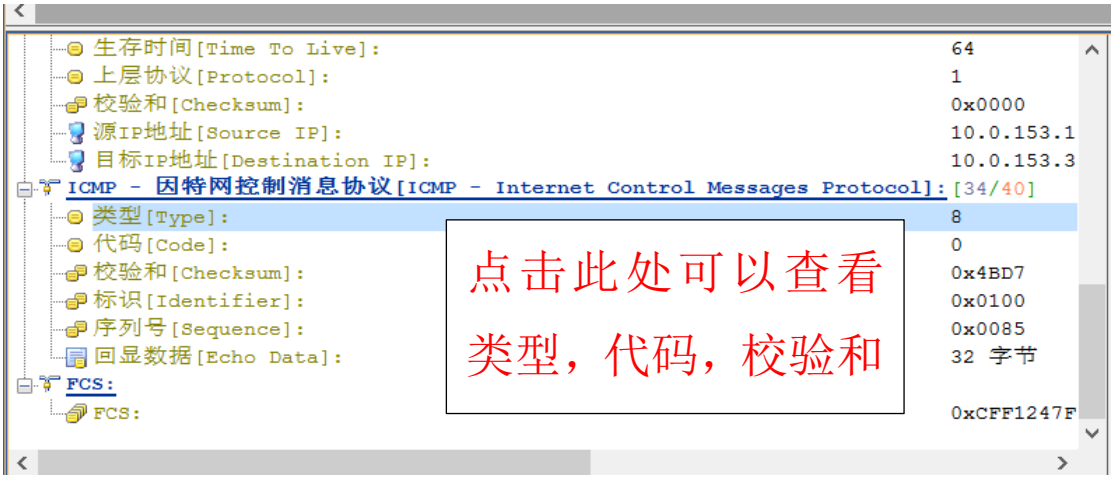
2）命令执行后，停止抓包，分析 ICMP 报文，查看报文结构和首部格式以及首部中各字段的内容。



3）说明 ICMP 报文首部各字段的含义以及所捕获的数据报属于什么报文。

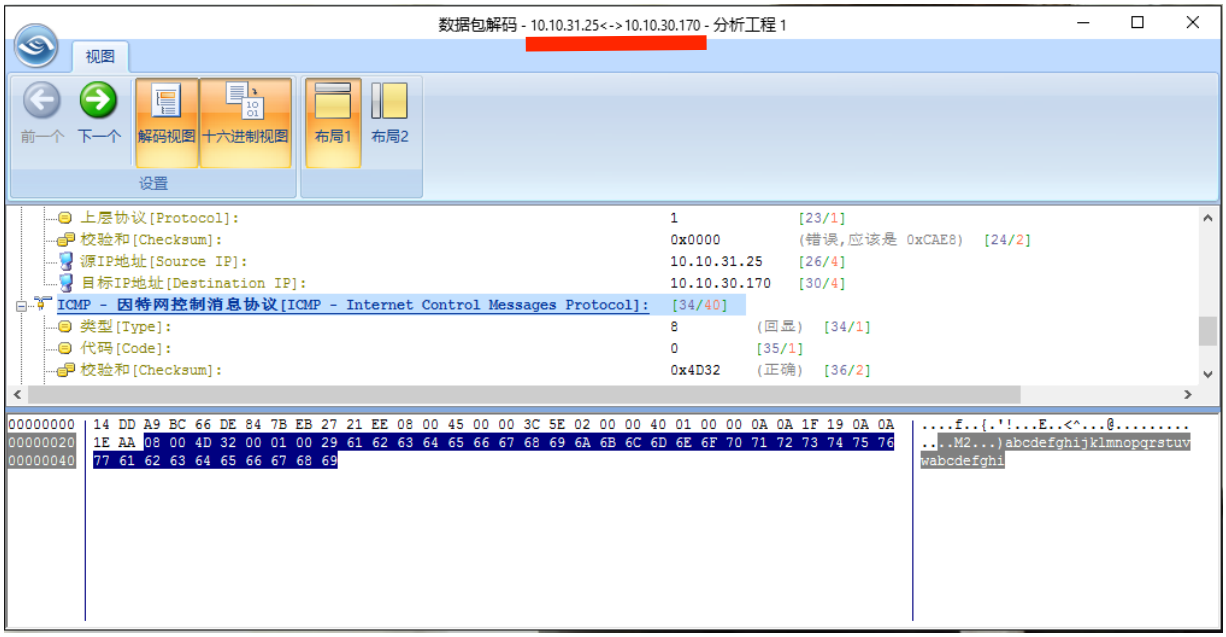


1.类型：占 8 位
2.代码：占 8 位
3.检验和：占 16 位



常用的 ICMP 报文如下表

ICMP 报文种类	类型的值	ICMP 报文的类型
差错报告报文	3	终点不可达
	4	源点抑制（Source quench）
	11	时间超时
	12	参数问题
	5	改变路由（Redirect）
询问报文	8 或 0	会送（Echo）请求或回答
	13 或 14	时间戳（Timestamp）请求或回答



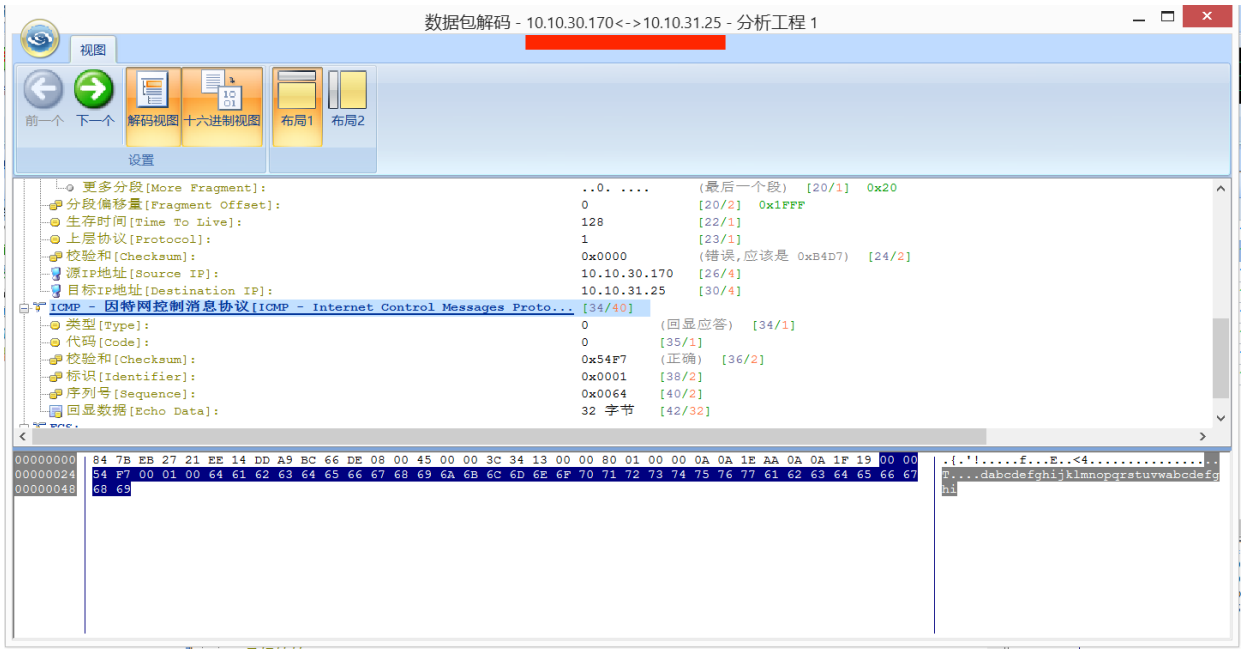
类型：08

代码：00

校验和：4D 32

报文：ICMP 询问报文

4）对 PC2 上捕获到的包进行分析，说明 ICMP 报文首部各字段的含义以及所捕获的数据报属于什么报文。



类型：00

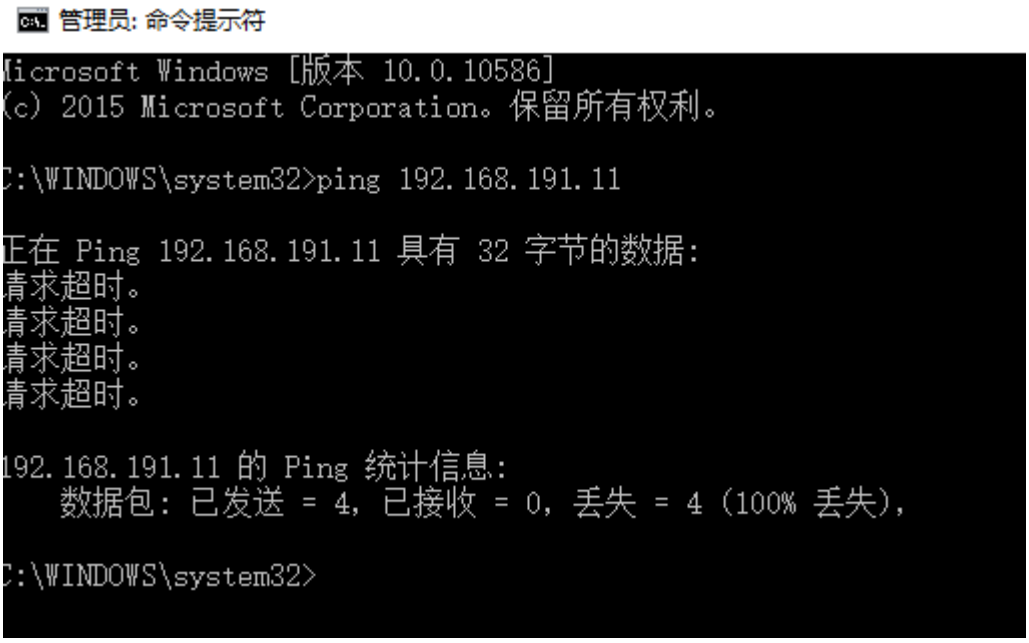
代码：00

校验和：54 F7

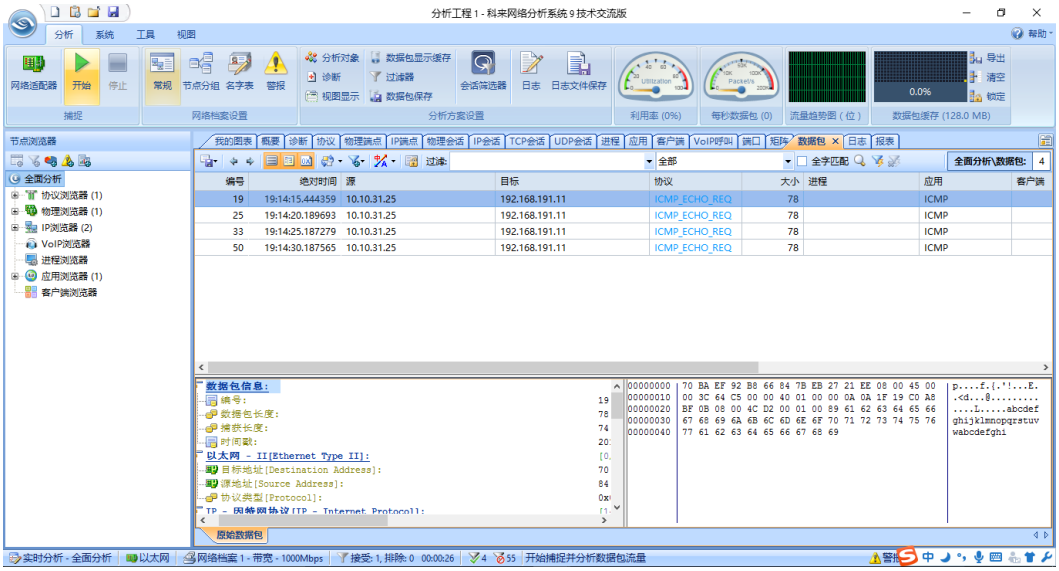
报文：ICMP 询问报文

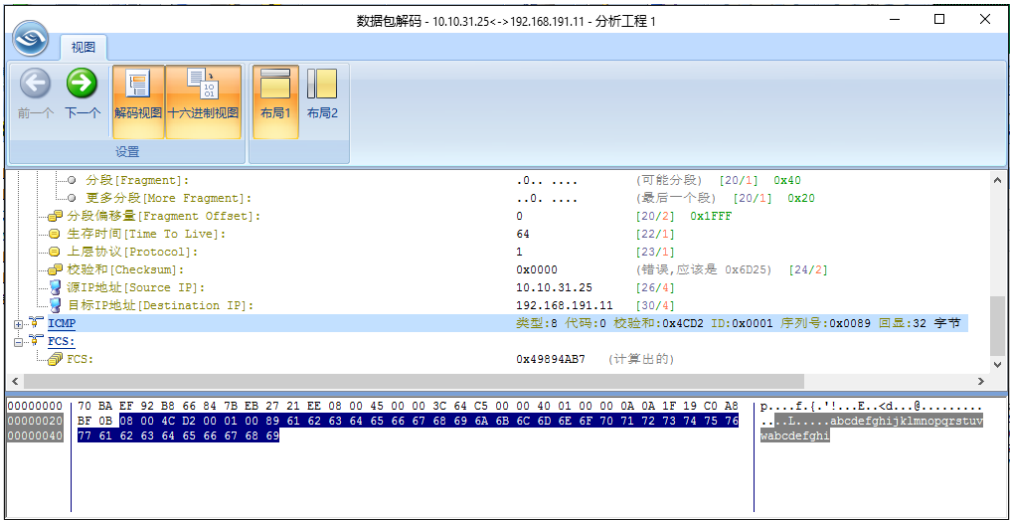
2．超时消息。

1）在 PC1 上运行命令：ping 不存在的或者没有开机的计算机的 IP。



2）停止抓包，分析 ICMP 报文，查看报文结构和首部格式以及首部中各字段的内容。





3）说明 ICMP 报文首部各字段的含义以及所捕获的数据报属于什么报文。

类型：00

代码：00

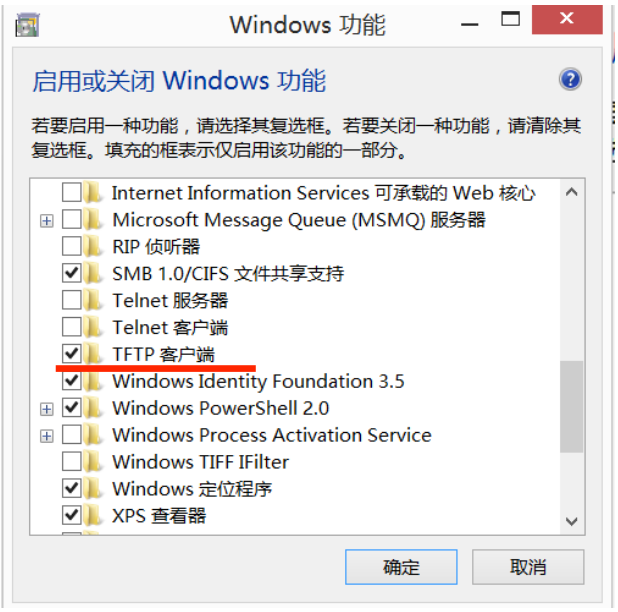
校验和：54 F7

报文：ICMP 询问报

3．端口不可达消息。

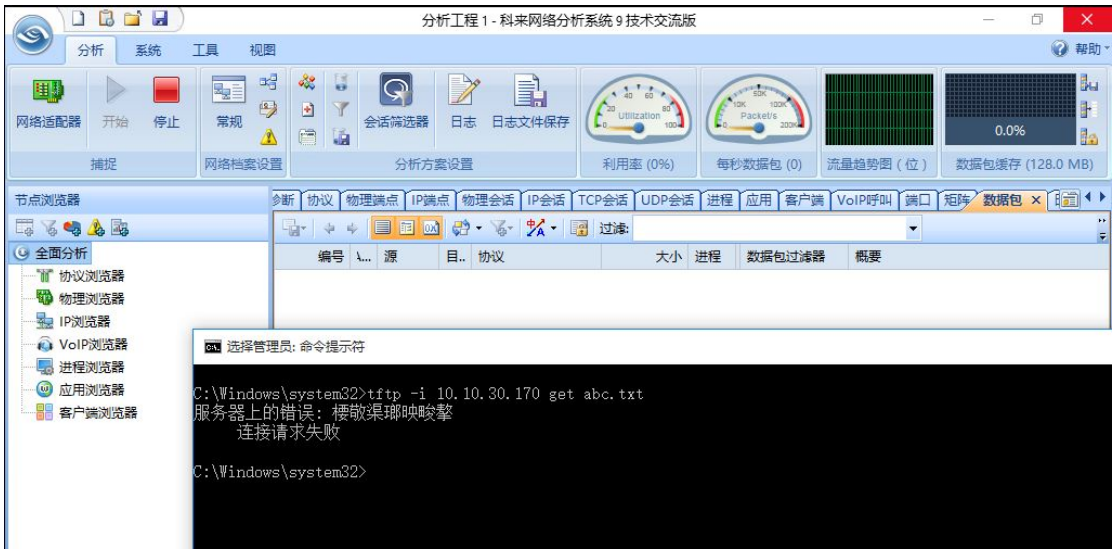
在 PC2 上启动 TFTP 服务器软件。

控制面板——程序——启动或关闭 windows 功能



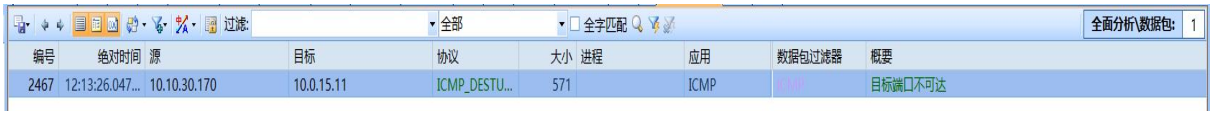
在 PC1 上启动科来网络分析系统，开始抓包。

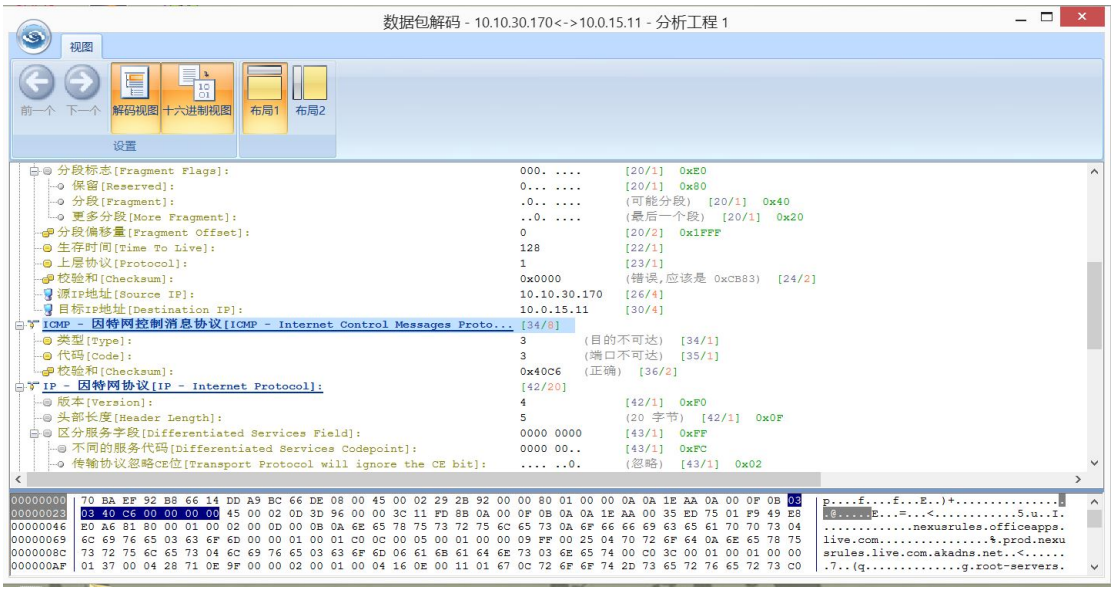
在 PC1 的命令窗口运行命令：tftp –I PC2 的 IP get 文件名（该文件可能不存在）；停止抓包可以看到如图所示结果：



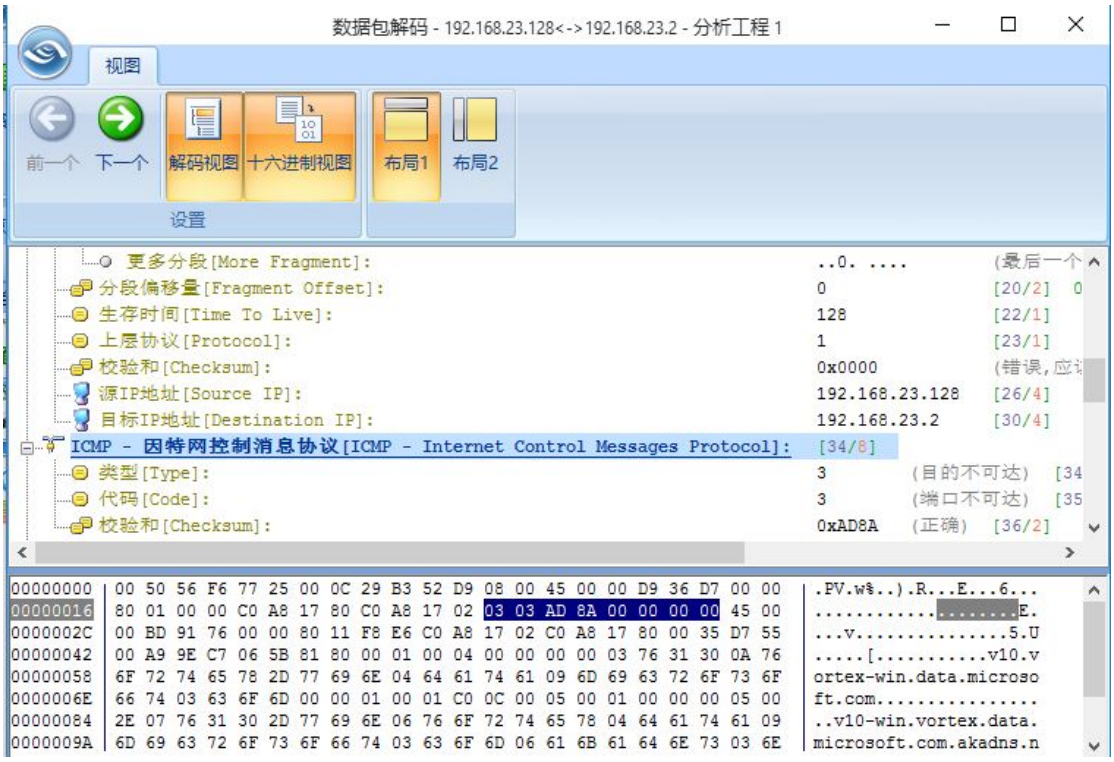
文件存在：

```
C:\WINDOWS\system32>tftp -i 10.10.30.170 put f:\xsw.txt
传输成功: 1 秒 0 字节, 0 字节/秒
```






```
C:\Windows\system32>tftp -i 10.10.30.170 get xsw.txt
传输成功: 1 秒 0 字节, 0 字节/秒
```

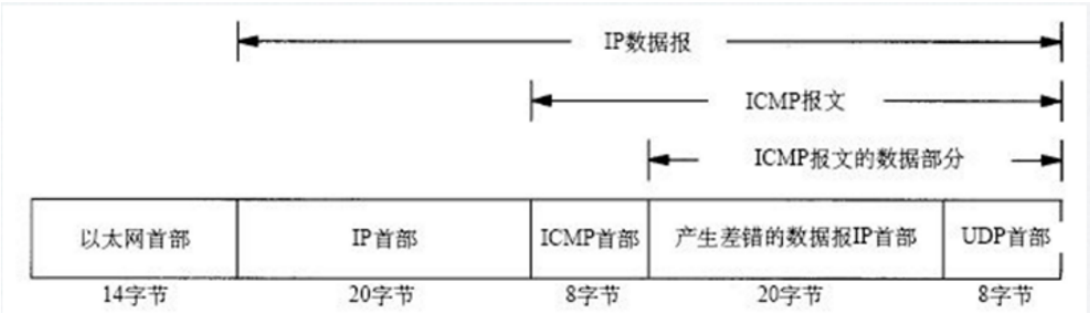


4．5 实验要求

完成本次实验后，通过查找资料，整理并总结 ICMP 报文的各字段的意义，ICMP 各种消息的作用，进一步掌握网络连通性的测试方法。

4．6 思考与讨论

1．通过查资料，请描述协议不可达报文的结构以及首部字段的含义。



2．总结 ICMP 类型与代码，简单描述其含义。

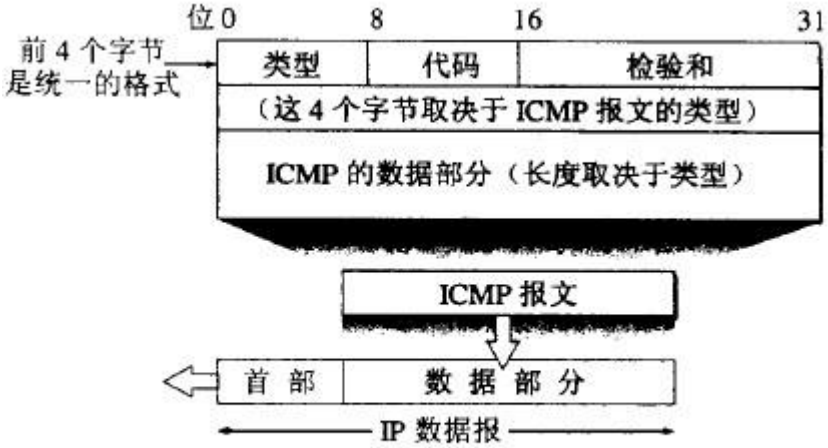


图 4-27　ICMP 报文的格式

Type	Code	类别	含义
0	0	查询	回送应答
	0	差错	网络不可抵达
	1	差错	主机不可抵达
	2	差错	协议不可抵达
	3	差错	端口不可抵达
	4	差错	需要重新分片但设置了不分片比特
	5	差错	源路由失败
3	6	差错	目的网络未知
	7	差错	目的主机未知
	8	差错	源主机被隔离
	9	差错	目的网络被禁止
	10	差错	目的主机被禁止
	11	差错	对所请求的服务类型，网络不可达
	12	差错	对所请求的服务类型，主机不可达
	13	差错	由于过滤，通信被禁止
	14	差错	主机越权
	15	差错	优先级失效
4	0	差错	源端被关闭

5	0	差错	对网络重定向
	1	差错	对主机重定向
	2	差错	对服务类型和网络重定向
	3	差错	对服务类型和主机重定向
8	0	查询	请求回显
9	0	查询	路由器通告
10	0	查询	陆由器请求
11	0	差错	传输期间数据报超时
	1	差错	数据报组装期间超时
12	0	差错	IP报头损坏
	1	差错	缺少必要的选项
13	0	查询	时间戳请求
14	0	查询	时间戳回复
15	0	查询	信息请求（已过时）
16	0	查询	信息回复（已过时）
17	0	查询	地址掩码请求
18	0	查询	地址掩码回复