**计算机网络实验作业4**

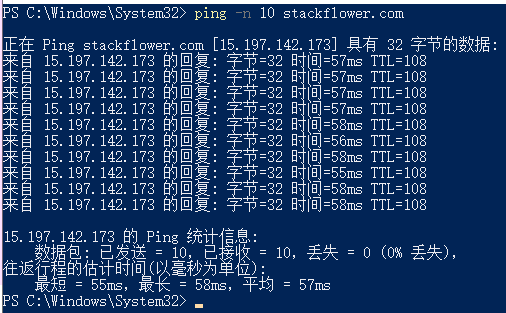
学号：19020011038 姓名：岳宇轩

一．ICMP and Ping

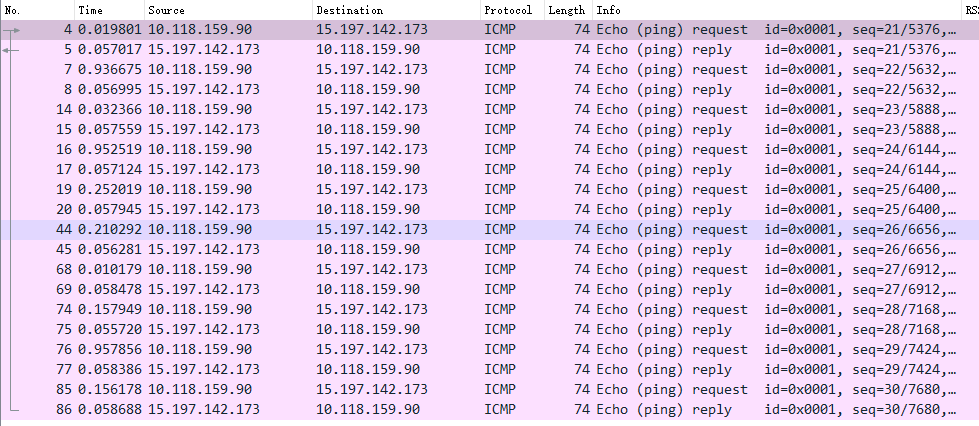
打开wireshark，在C:\Windows\System32下打开windows powershell窗口，键入：

ping -n 10 stackflower.com，

得到下图所示结果：



停止wireshark抓包，查看ICMP分组如下：



1.What is the IP address of your host? What is the lP address of the destination host?

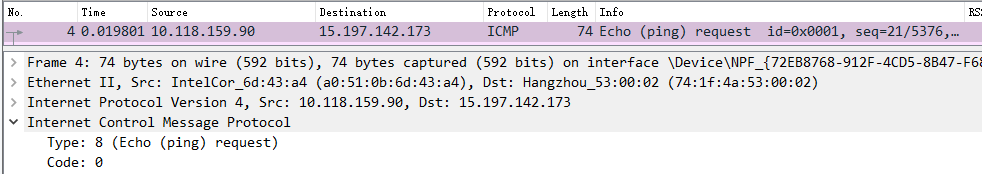


通过wiresharp抓取的包中的source字段和destination字段分析可知，本机IP地址为10.118.159.90,stackflower的IP地址是15.197.142.173

2.Why is it that an ICMP packet does not have source and destination port numbers?

ICMP是IP层的协议，ICMP报文直接封装到IP数据报中，而端口号是运输层才有的,网络层是没有端口，所以ICMP包里没有源地址和目的地址的端口号。

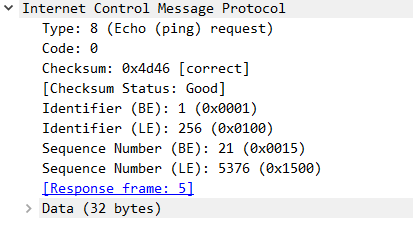
1. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? Howmany bytes are the checksum, sequence number and identifier fields?



ICMP type: 8( Echo(ping)request)

Code:0

ICMP请求分组含有的其他字段:



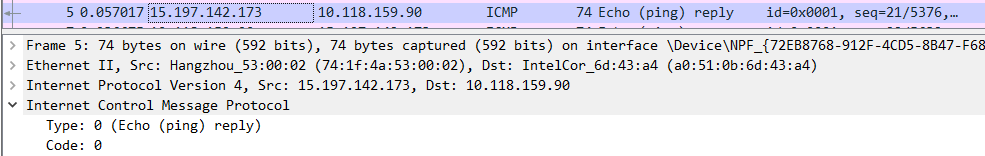
Checksum:校验和 2字节

Idenifier:标识符 2字节

Sequence Number:序列号 2字节

Data:数据 32字节

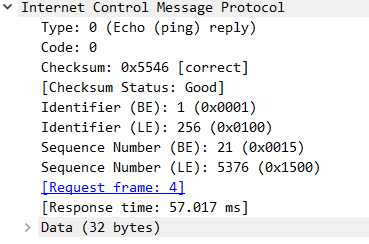
1. Examine the corresponding ping reply packet. What are the ICMP type and codenumbers? What other fields does this ICMP packet have?How many bytes are thechecksum, sequence number and identifier fields?



ICMP type: 0 (Echo(ping) reply)

Code:0

ICMP应答分组含有的其他字段：



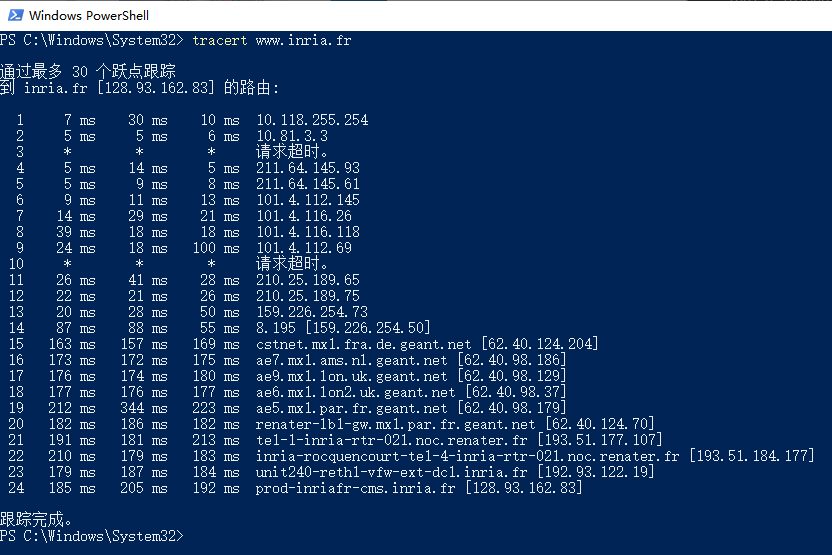
Checksum:校验和 2字节

Identifier:标识符 2字节

Sequence Number:序列号 2字节

Data:数据 32字节

1. ICMP and Traceroute



1. What is the IP address of your host? What is the IP address of the target destination host?



my host: 10.118.159.90

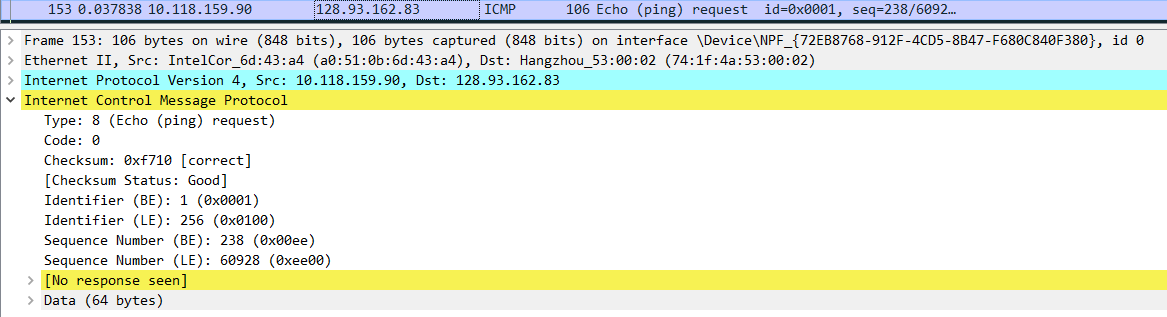
target destination host: 128.93.162.83

6.If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

有不同的协议号

如果ICMP发送UDP数据报,IP协议号应该为0x11.十进制为17,表明交给UDP。

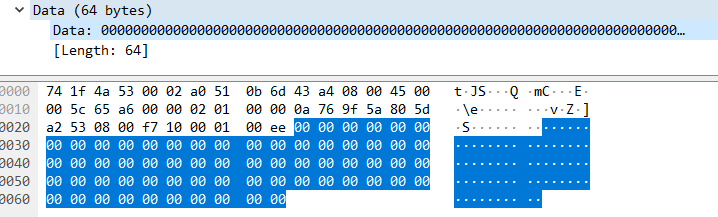
7.Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?



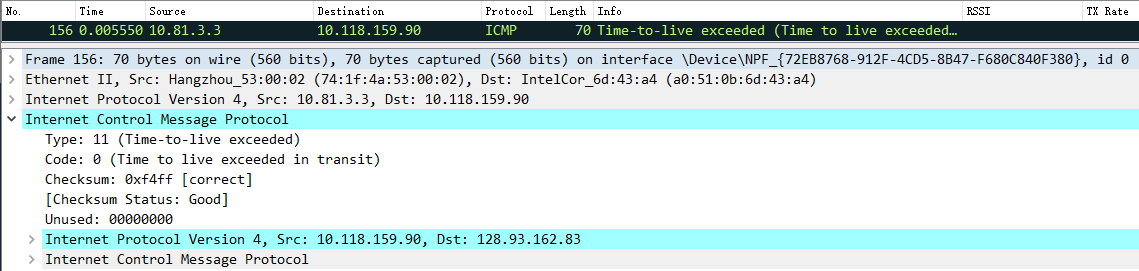
字段是一致的，包内容是不同的

ICMP报文的格式为1个字节的type，1个字节的code,2个字节的checksum，4个字节的由类型决定的部分option，以及剩下的数据部分data。由于type是8/0，那么由类型决定的部分就是2个字节的identifier和2个字节的sequence。所以只要协议类型相同，那么包包含的字段就是相同的。

这里的数据部分全部都是0。(checksum, sequence一般每个包都不同，identifier MacOS/Linux和进程号相同, Windows固定)



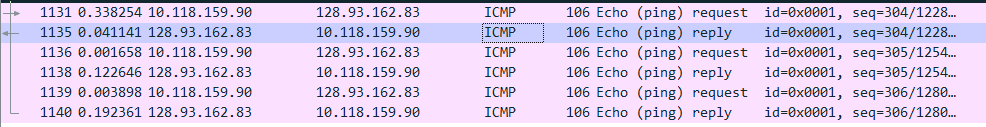
8.Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet.What is included in those fields?

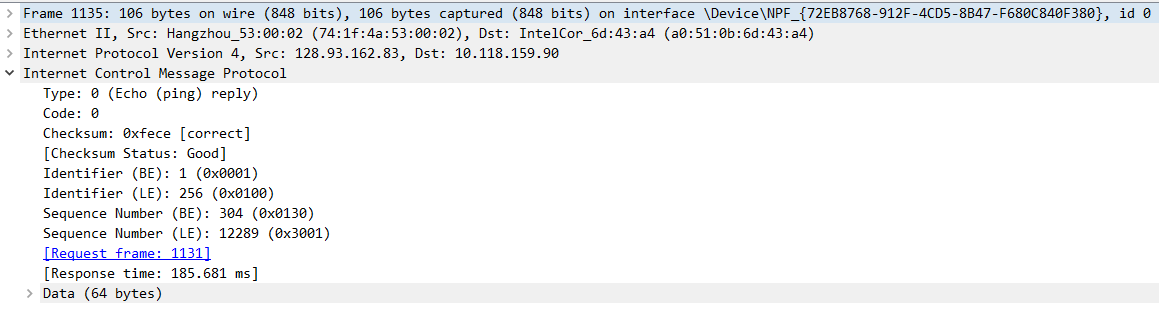


ICMP错误数据报包括;所有IP字段和原来的ICMP字段。

只不过这里的type为11，表示 time-to-live exceeded TTL过期, code是0，由类型决定的部分为全0的填充，数据部分为TTL减至0的那个IP报文的全部。

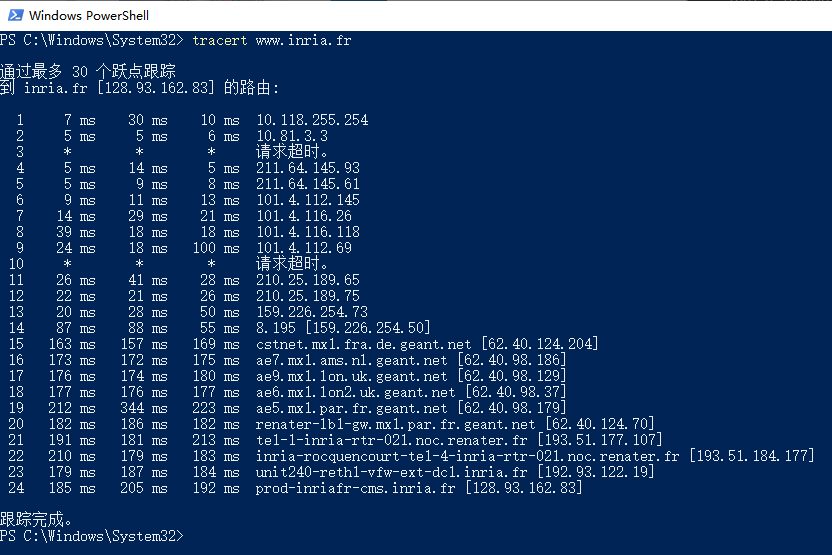
1. Examine the last three ICMP packets received by the source host. How are thesepackets different from the ICMP error packets? Why are they different?





最后三个ICMP reply数据报的Type和Code都是0，表示回显回答，而不是11 (TTL过期)，在TTL为24时恰能把包送到目的地址

1. Within the tracert measurements, is there a link whose delay is significantlylonger than others?Refer to the screenshot in Figure 4, is there a link whosedelay is significantly longer than others? On the basis of the router names, canyou guess the location of the two routers on the end of this link?



从上图可以看出第18跳到第19跳延迟最大

62.40.98.37法国巴黎

62.40.98.179英国

这条链接连接法国巴黎的路由器和英国的路由器