实践作业5

作业要求：提交word格式作业

作业内容：

1 ）编程实现ICMPping

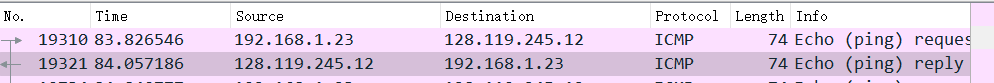
2）Wireshark实验：考察在 ping和 Traceroute命令中 ICMP协议的使用

（1）捕获 Ping 程序生成的数据包 ，回答：

1 您的主机的 IP 地址是多少? 目标主机的 IP 地址是多少?

主机IP地址：192.168.1.23

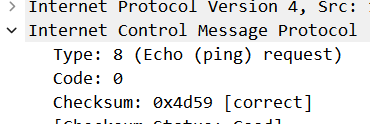
目标主机IP地址：128.119.245.12



2 为什么 ICMP 数据包没有源端口号和目的端口号?

因为**ICMP是网络层的协议，它不需要传输层TCP或者UDP的承载**，直接使用IP数据报承载，因此不需要源端口号和目的端口号，只要源地址和目的地址即可。

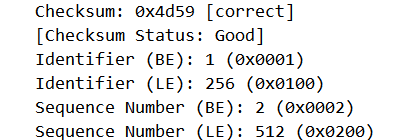
3 查看任意的请求 ICMP 数据包， ICMP 类型和代码是什么?



ICMP类型：8

代码：0

4 该 ICMP 数据包 还有哪些其他字段? 校验和，序列号和标识符字段有多少字节?



如图还有还有Checksum、Checksum Status、Indetifier(BE)，Indentifier (LE)、Sequence number(BE)，Sequence number(LE)

校验和(Checksum)：4个字节

序列号(Sequence)：4个字节

标识符(Identifier)：4个字节

（2）捕获 Traceroute 程序生成的数据包 。

在 Unix / Linux 中，路由跟踪 traceroute 使用 发送不可到达(无使用的)端口的 UDP 包来实现，在 Windows 中，路由跟踪 tracert 仅使用 ICMP 数据包来实现

回答：

1 发送了 UDP 数据包(如在 Unix / Linux 中)，那么探测数据包的 IP 协议号仍然是 01 吗? 如果没有，它会是什么?

发送请求路由跟踪的数据包是 UDP 数据包，因此 IP 承载上层协议号时 17。

2 检查ICMP 响应数据包。 这与本实验的前半部分中的 ICMP ping 查询数据包不同吗? 如果不同，请解释为什么?

不同，这里的 ICMP 报文时 \*\*TTL 报文(类型 11 编码 0)，这个是在 Traceroute 程序中，路由器检查到 Traceroute 发出的 IP 数据报中 TTL 正好过期，因此路由器就需要丢包并且发送该警告报文返回源主机。这个与 Ping 程序中所要达成的目的不同，Ping 程序是为了请求响应。

3 检查源主机收到的最后三个 ICMP 数据包。 这些数据包与 ICMP 错误数据 包有何不同? 他们为什么不同?

这个是目的主机返回的回显应答报文，因为 tracert 程序的原理是发送 TTL 增加的数据包，当 TTL = 1 的包达到路由器，该路由器会将该包丢弃，并且发送 ICMP 错误给请求的机器。而最后一组 3 个数据报时可以到达目的主机的，这时由于是被目的主机接收，目的主机不会丢包，而是确确实实收到的这个探测的数据报并进行了响应.