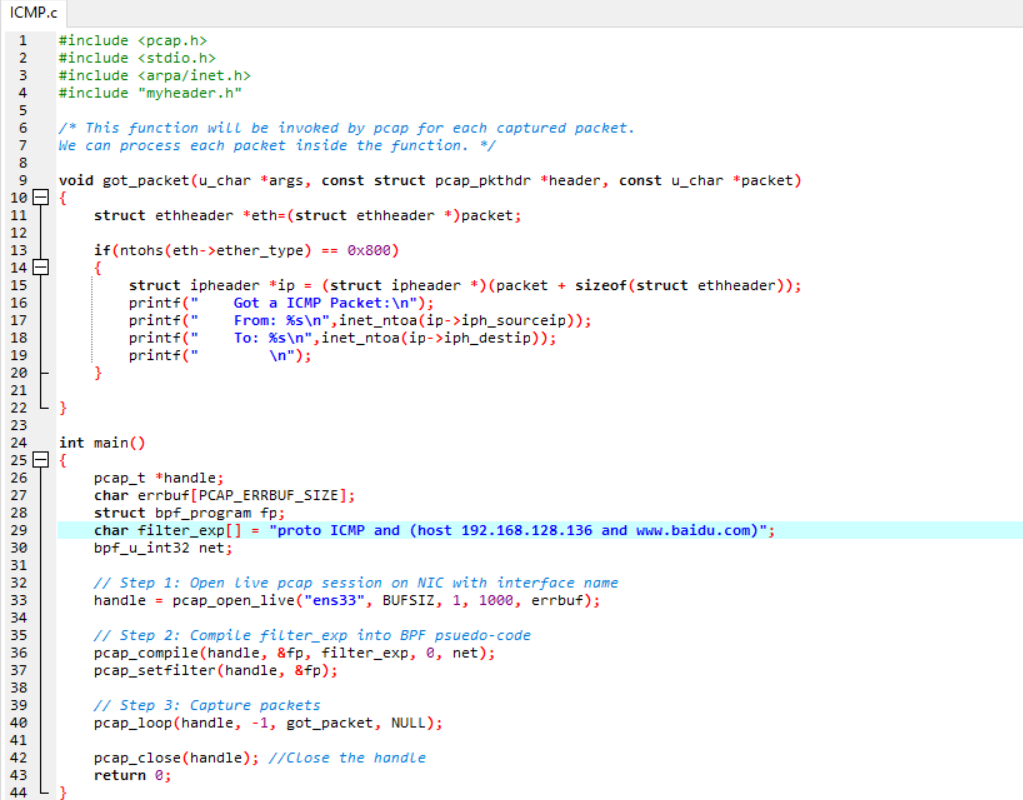
**捕获两个特定主机之间的 ICMP 数据包**

1. eth\_type为0x0800时，上层协议为ip协议，因此作为筛选依据；

同时在主函数中利用BPF规则，构造符合要求的filter\_exp字段并放入pcap\_compile中作为参数，再将网卡设定为虚拟机的ens33；

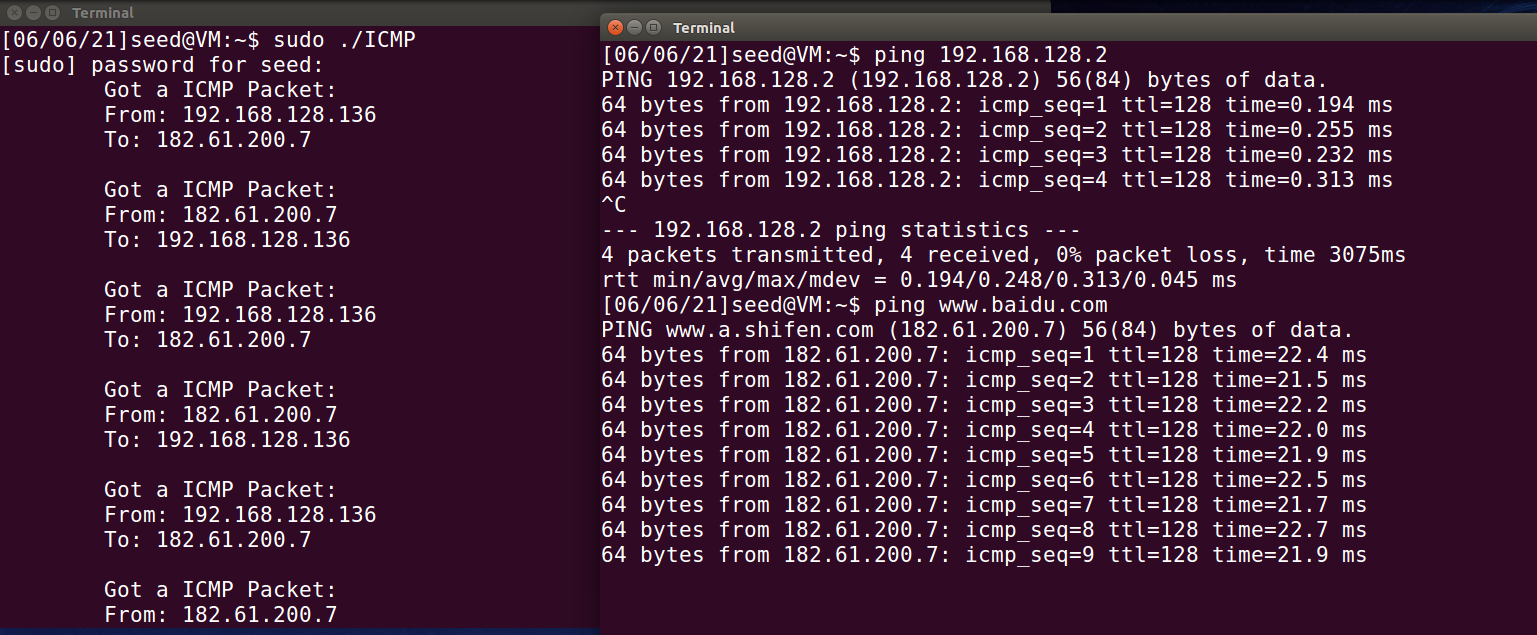
具体代码如下：



1. 完成代码编写后，在虚拟机中编译运行；

通过ping指令来发送ICMP包，此时查看运行窗口反馈，可以看到：

当ping命令不为指定IP时无法得到反馈；  
当ping命令为指定IP时会成功过滤得到指定两个主机之间的ICMP数据包。



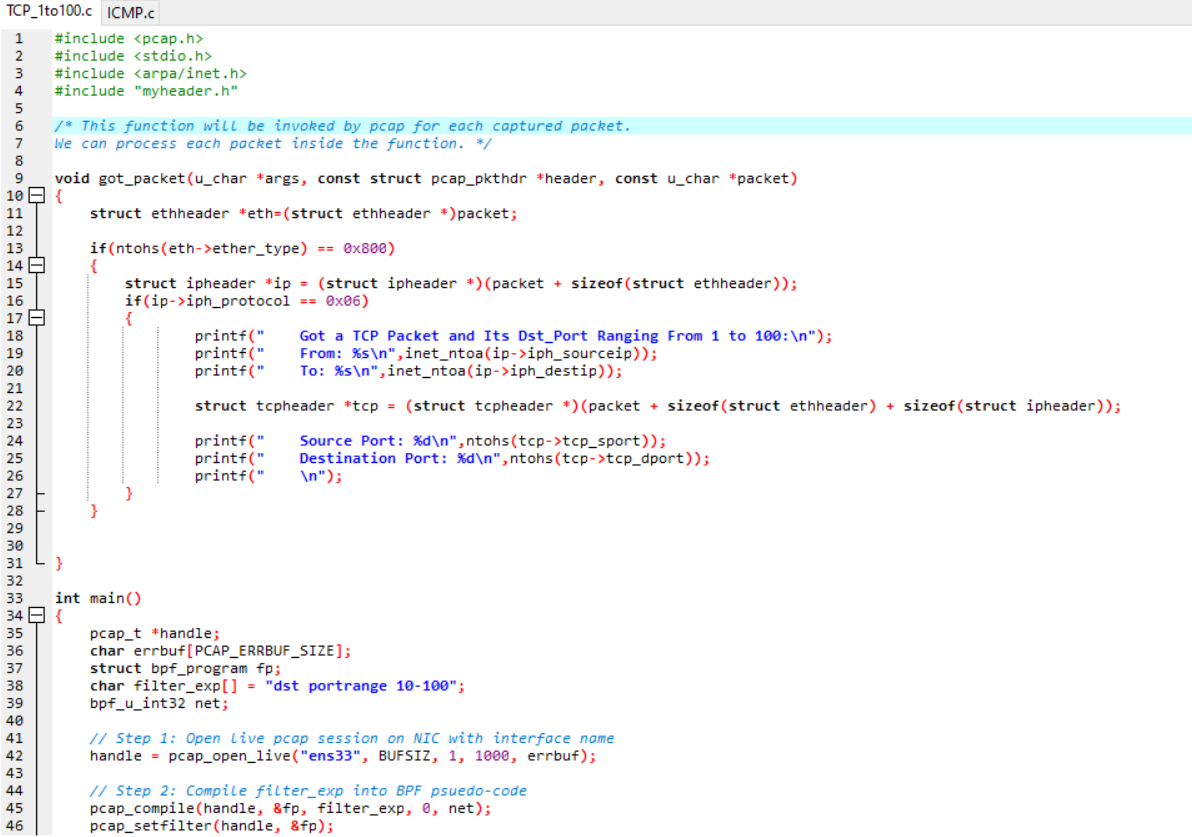
**捕获目标端口号在 10 到 100 范围内的 TCP 数据包**

1. eth\_type为0x0800时，上层协议为ip协议，同时查阅资料可知iph\_protocol为0x0600时为tcp协议，将这两者作为筛选依据



同时在主函数中利用BPF规则，构造仅接受目标端口为10-100数据包的filter\_exp字段并放入pcap\_compile中作为参数，再将网卡设定为虚拟机的ens33；

代码如下



1. 完成代码编写后，在虚拟机中编译运行；

同时打开浏览器——访问网页使用的是http协议，进行内容交互之前需要进行tcp三次握手；

查看运行窗口反馈，可以看到成功过滤得到目标端口为10-100的tcp数据包

