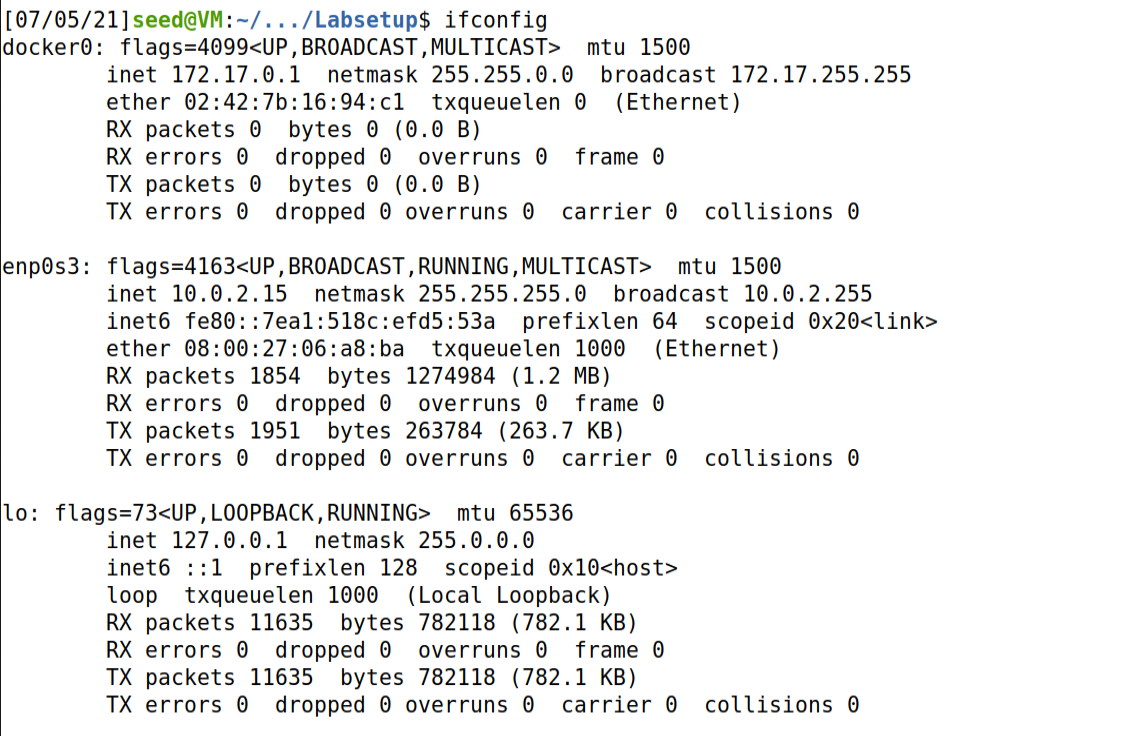
**Lab1-Task1 Packet Sniffing and Spoofing Lab**

**57118113 蔡义涵**

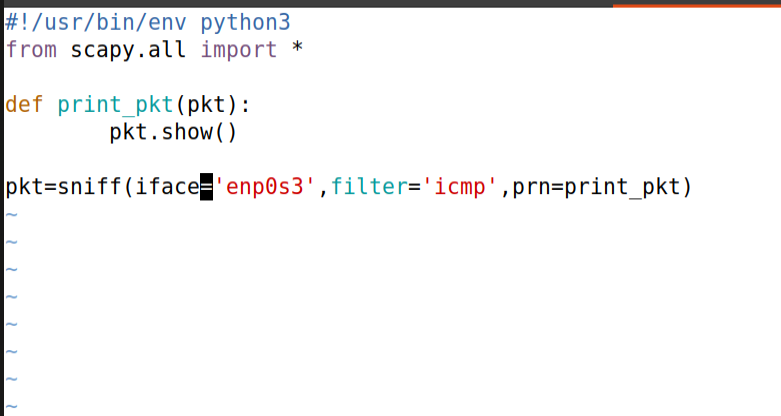
**Task1.1 Sniffing Packets**

**Task1.1A**

首先查看docker对应的接口名称，选择名为’enp0s3’的接口进行实验。

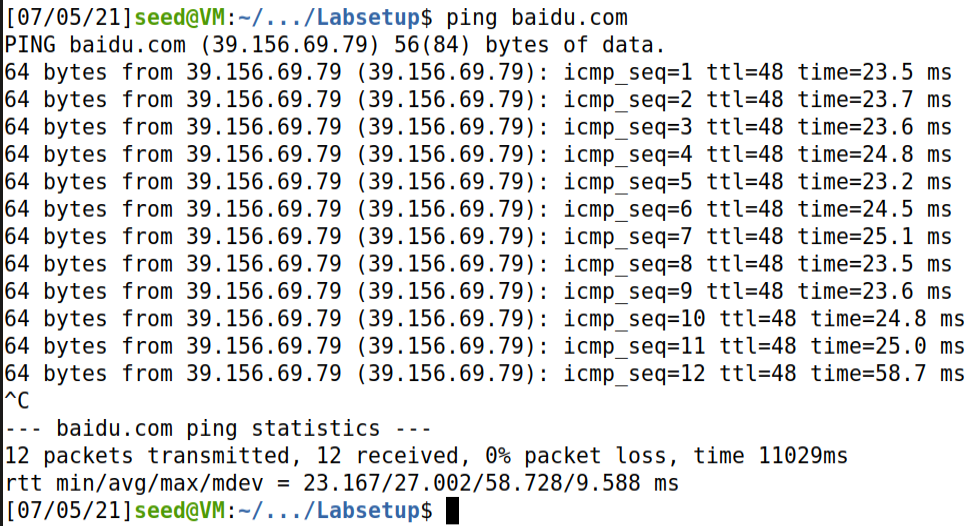


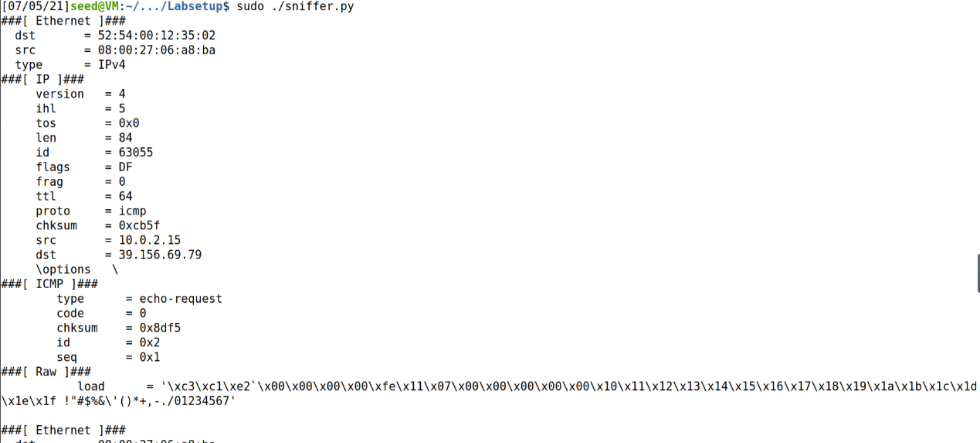
然后根据上述的接口名称写出以下python代码，报文类型设置为icmp。



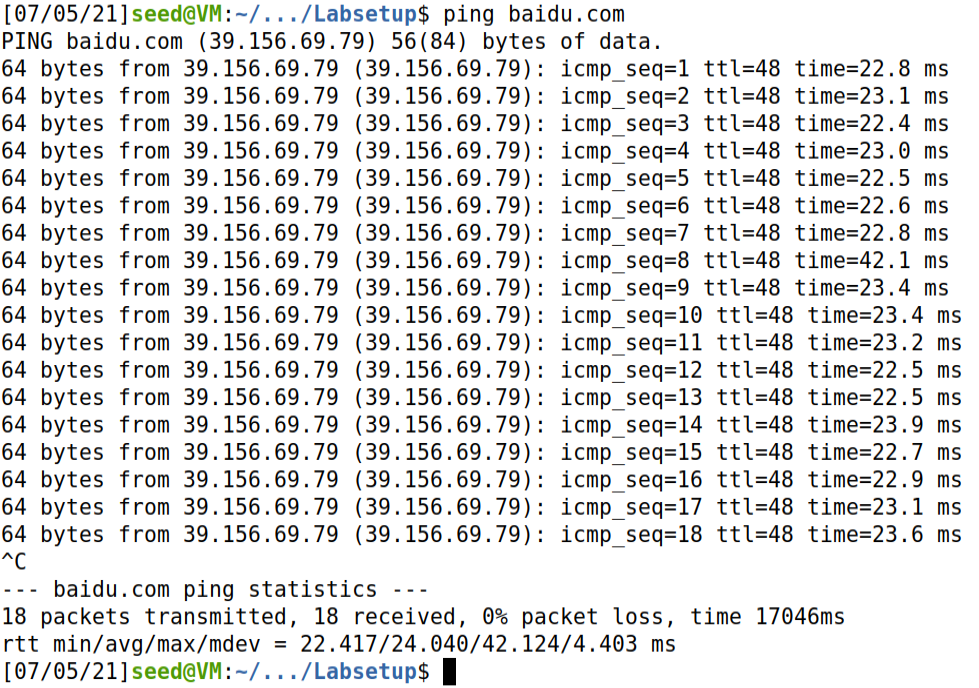
分别以root权限和普通用户权限执行上述程序，同时ping baidu.com，结果如下：

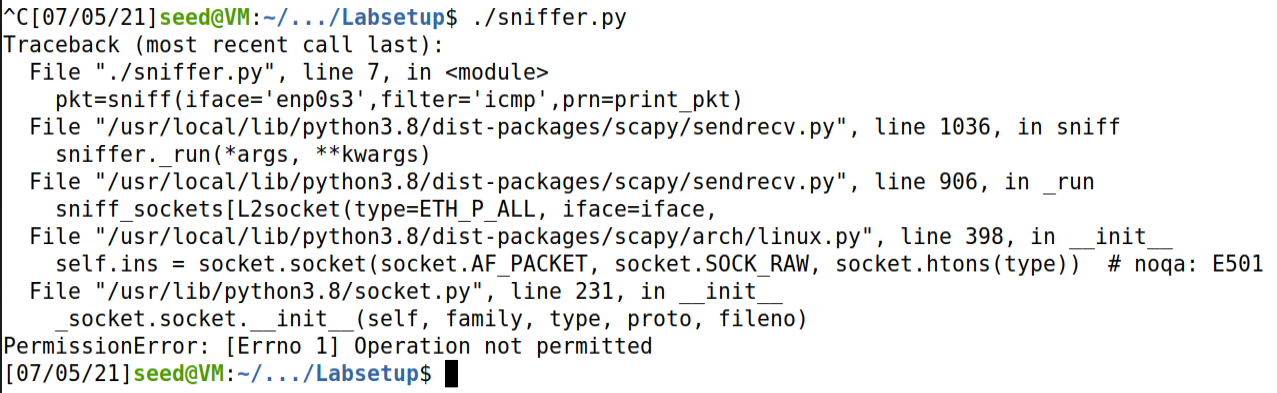
**root权限**





**普通用户权限**



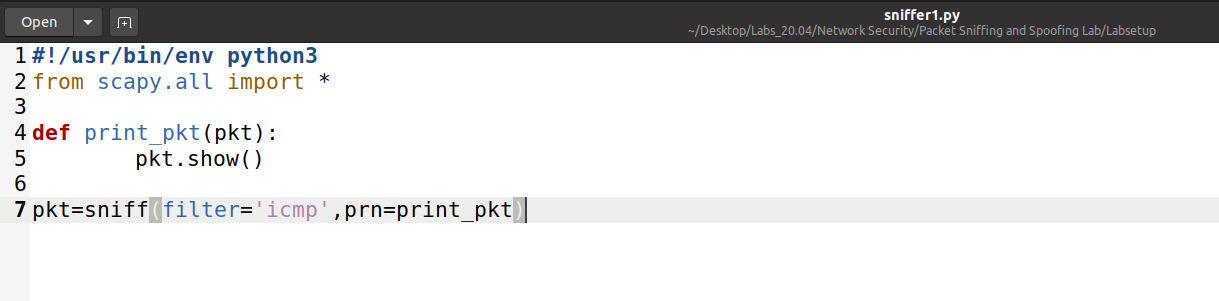


**总结**：可以观察到使用root权限可以正常抓包，而普通用户权限则显示权限不够。

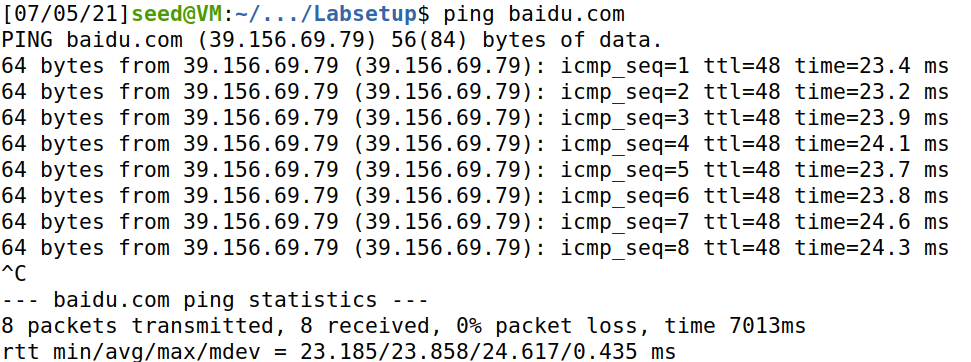
**Task1.1B**

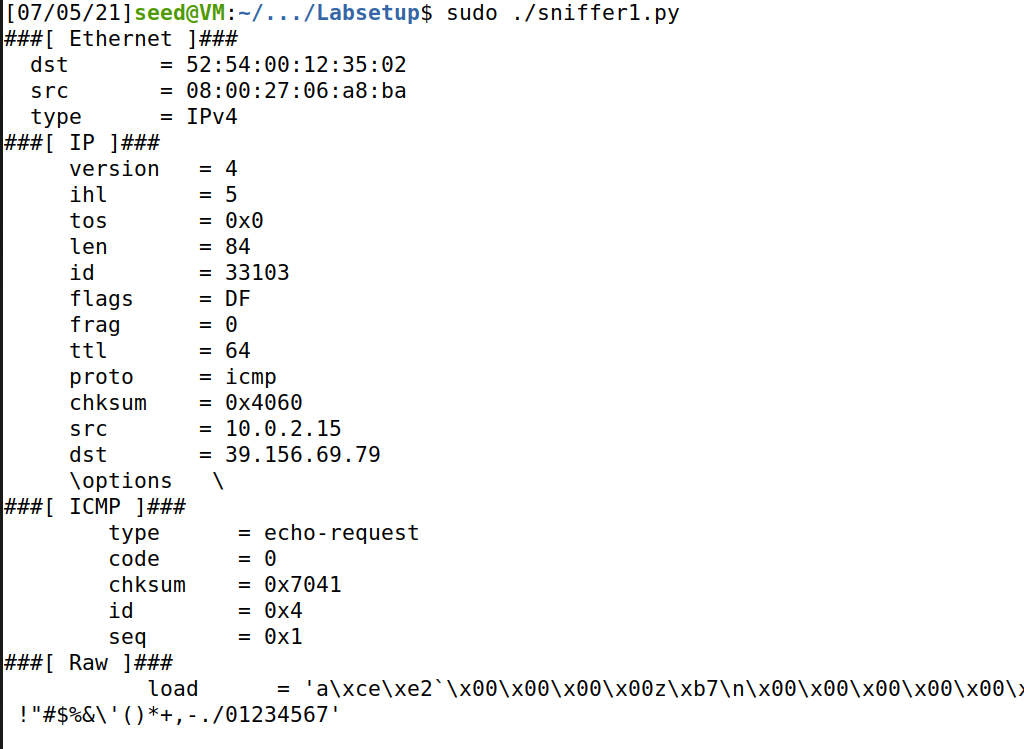
**Capture only the ICMP packet：**

执行以下程序，同时ping baidu.com：



得到结果如下：

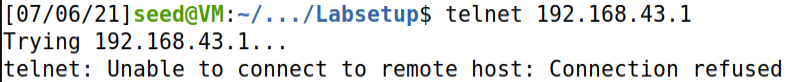




**Capture any TCP packet that comes from a particular IP and with a destination port number 23**

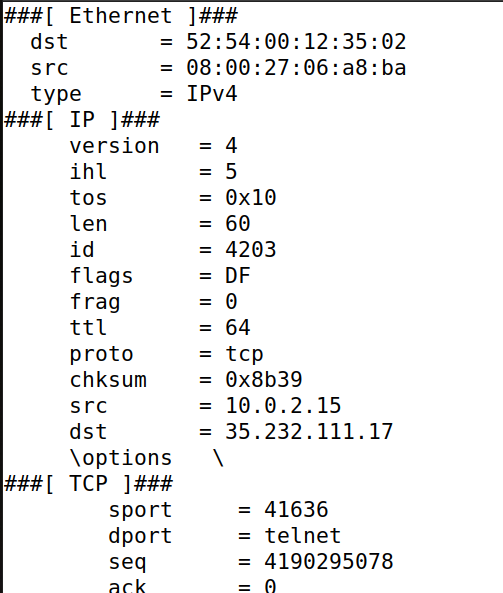
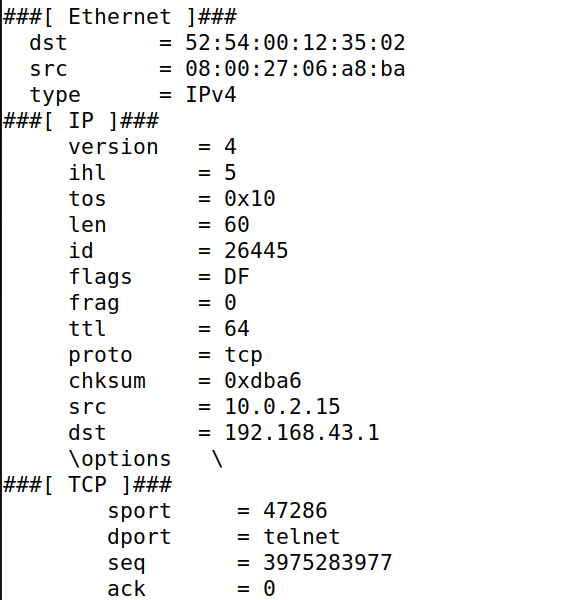
执行以下程序，同时向192.168.43.1发起telnet请求：





得到结果如下：

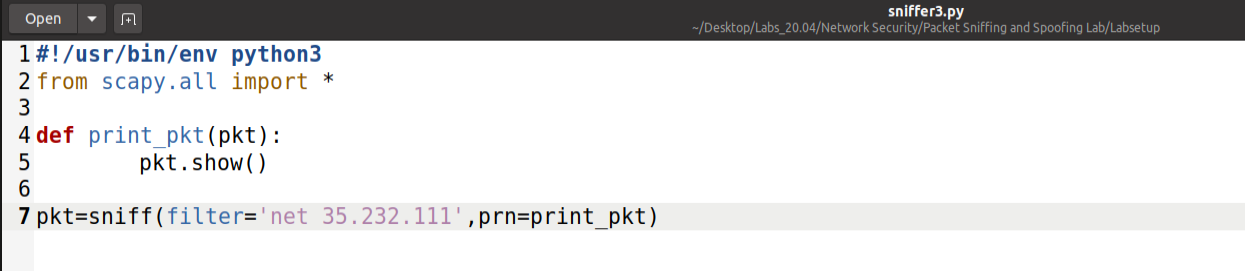




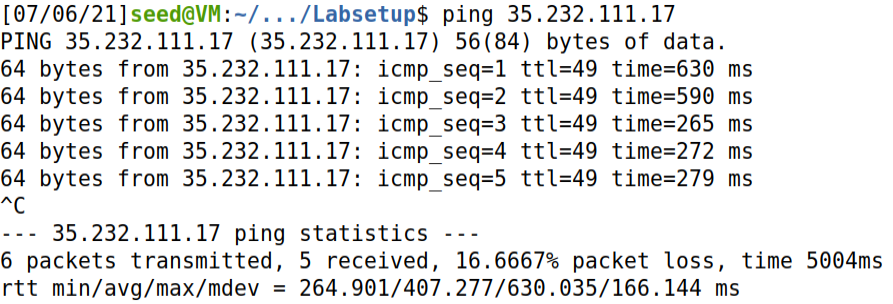
**总结**：23端口是telnet服务端口，此程序能正确接收到来自10.0.2.15的主机的telnet服务报文。

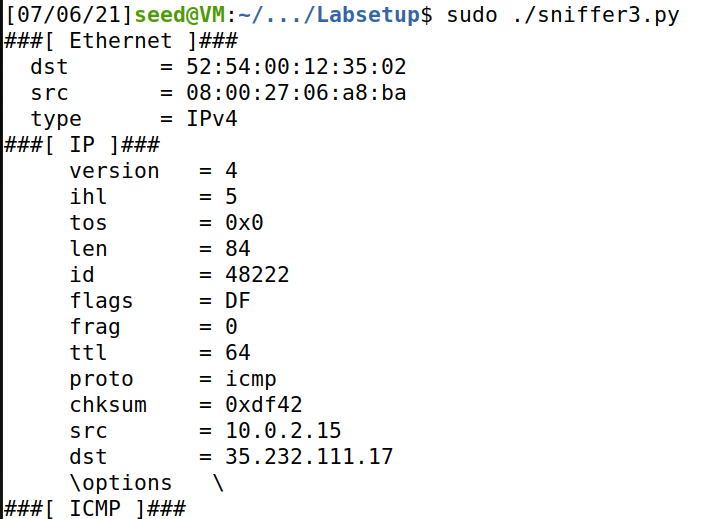
**Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as128.230.0.0/16; you should not pick the subnet that your VM is attached to：**

执行以下程序，同时ping 35.232.111.17和192.168.43.1：

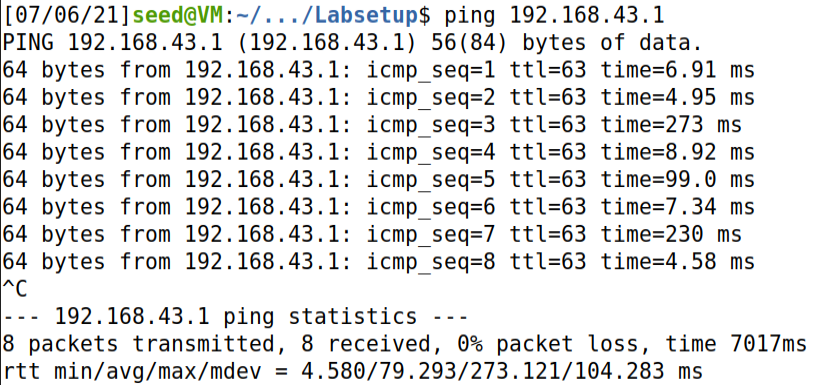


**Ping 35.232.111.17**





**Ping 192.168.43.1**



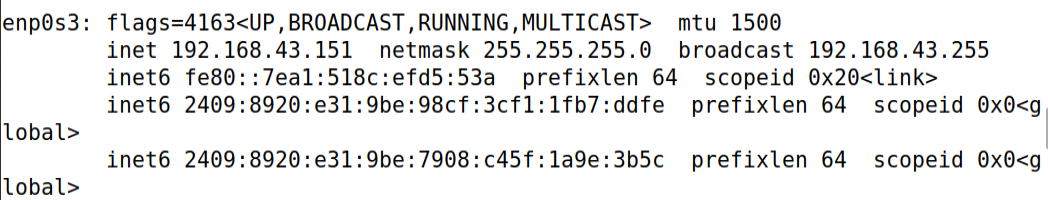


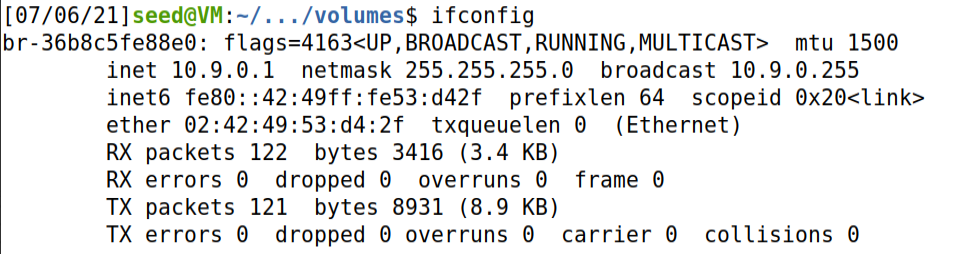
总结：此程序能够得到特定网段的报文，同时过滤掉其他网段的报文。

**Task 1.2: Spoofing ICMP Packets**

我们通过Attacker10.9.0.1向User10.9.0.5发送伪造源地址为192.168.43.151的报文，并观察对应网卡接收到的报文信息。

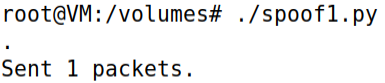
**网卡信息**



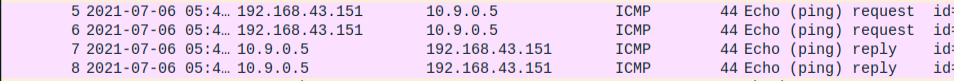


**Spoof程序**



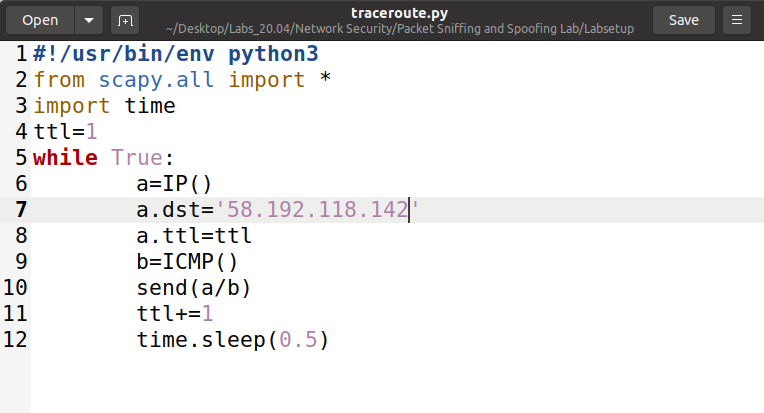


**Wireshark截图如下**

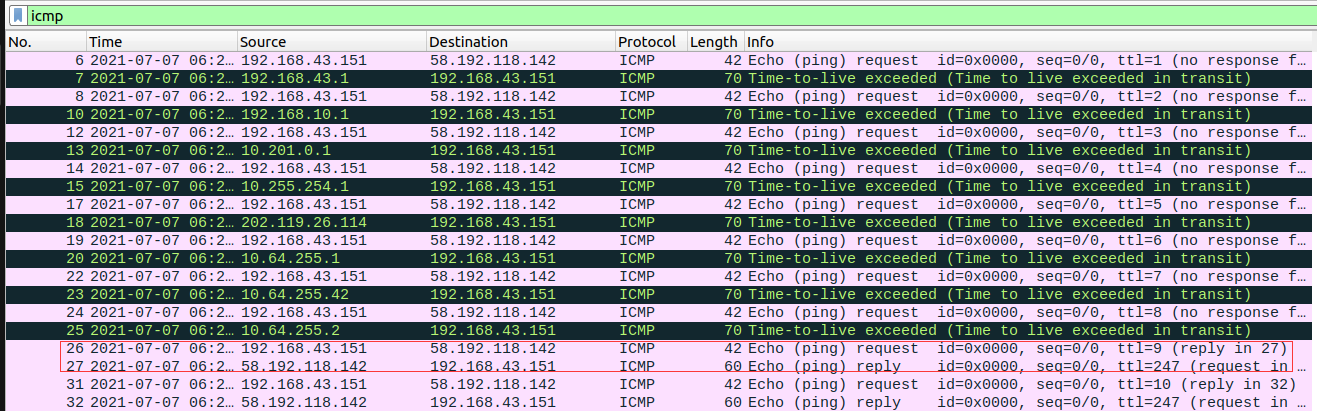


**Task 1.3: Traceroute**

编写以下程序，以寻找与seu.edu.cn路径上的每个路由节点

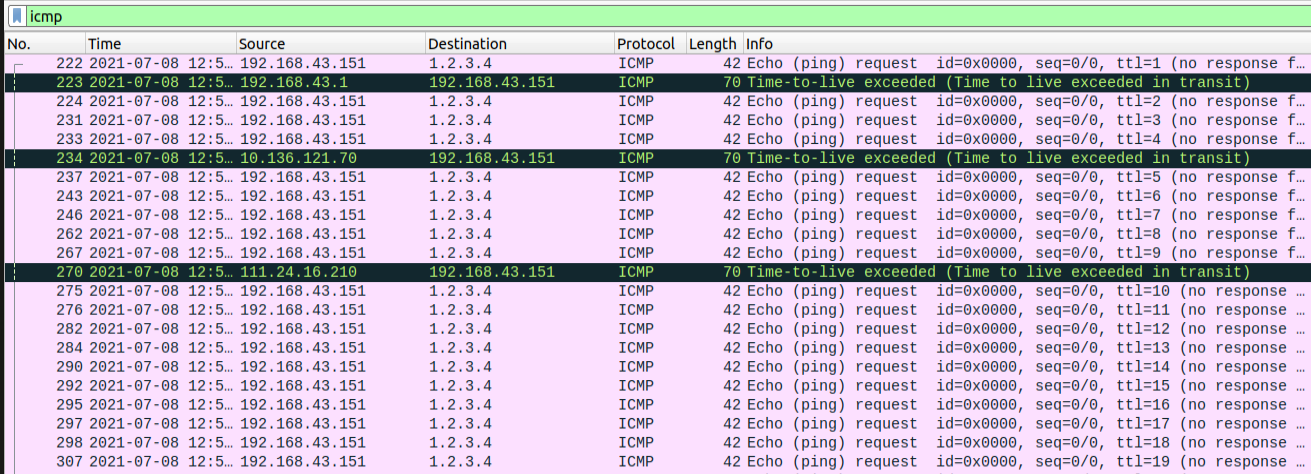


执行此程序，同时使用wireshark抓包观察结果



可以观察到，icmp报文经过9个路由节点后抵达58.192.118.142

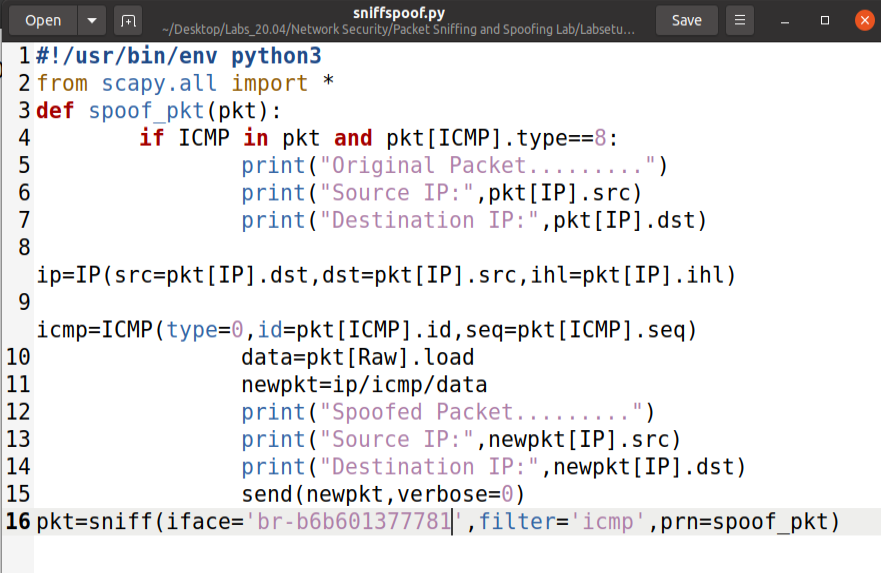
若通过以上方法寻找一个不存在的ip地址1.2.3.4的路径，则会得到以下结果：



可以看到，traceroute报文首先经过192.168.43.1，为VM与主机共享的内网网关，再经过10.136.121.70和111.24.16.210，之后寻址失败。

**Task 1.4:** **Sniffing and-then Spoofing**

编写以下程序并在10.9.0.1上执行：

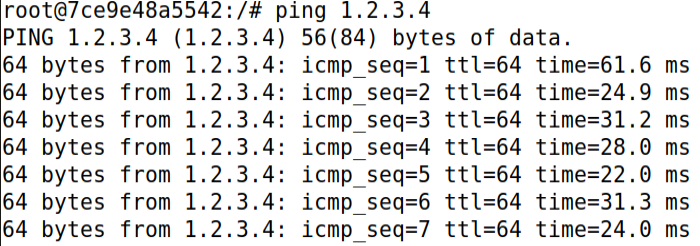


**Ping 1.2.3.4**

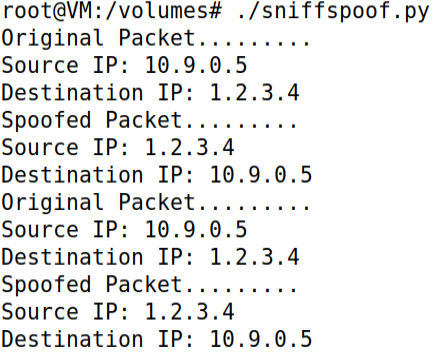
**Ping结果（不执行程序）**

****

**Ping结果（执行程序）**

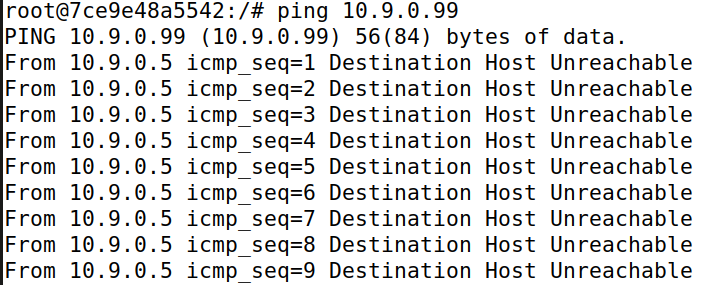


**程序执行结果**

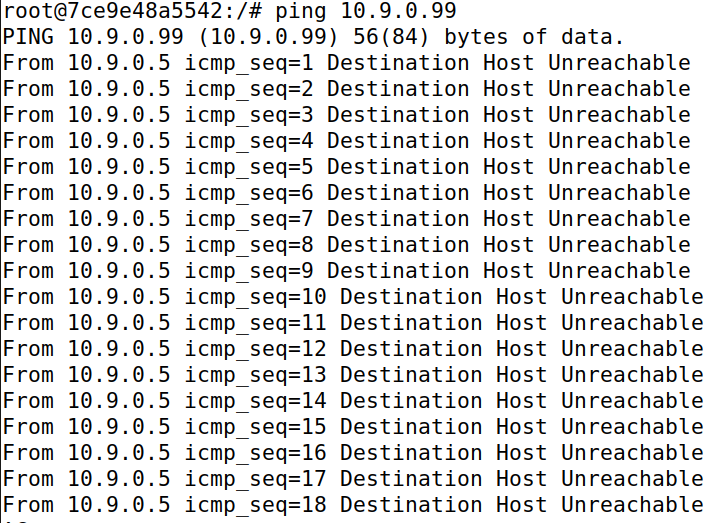


**Ping 10.9.0.99**

**Ping结果（不执行程序）**

****

**Ping结果（执行程序）**

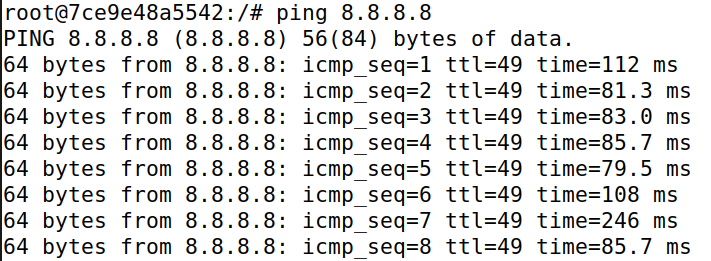


**程序执行结果**

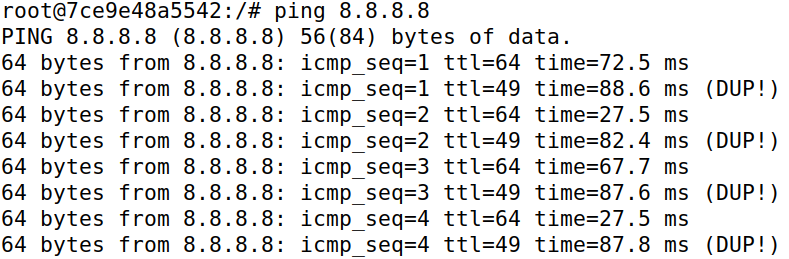


**Ping 8.8.8.8**

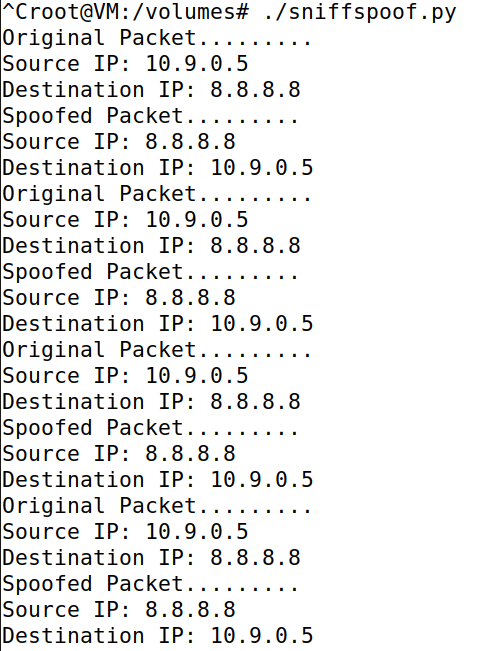
**Ping结果（不执行程序）**



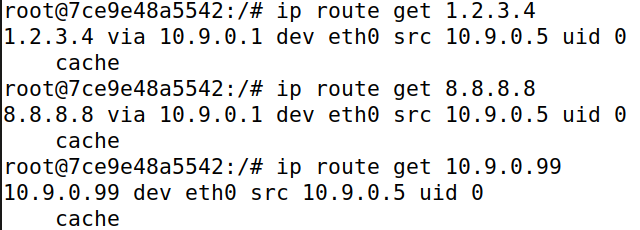
**Ping结果（执行程序）**



**程序执行结果**



**Ip route get**



**总结：**对于在Internet上不存在的主机1.2.3.4，该程序能够欺骗容器10.9.0.5，并接收到返回的报文；对于在LAN上不存在的主机10.9.0.99，该程序无法完成欺骗；对于Internet上真实存在的主机8.8.8.8，该程序能够产生作用，但容器10.9.0.5同时接受到真正的返回报文和虚假的返回报文，且两者时延具有较大的区别。原因是对于LAN上的主机ip地址，容器10.9.0.5不会通过网关10.9.0.1来寻址，而是直接在LAN中寻址，因此10.9.0.1中的程序无法发挥作用。