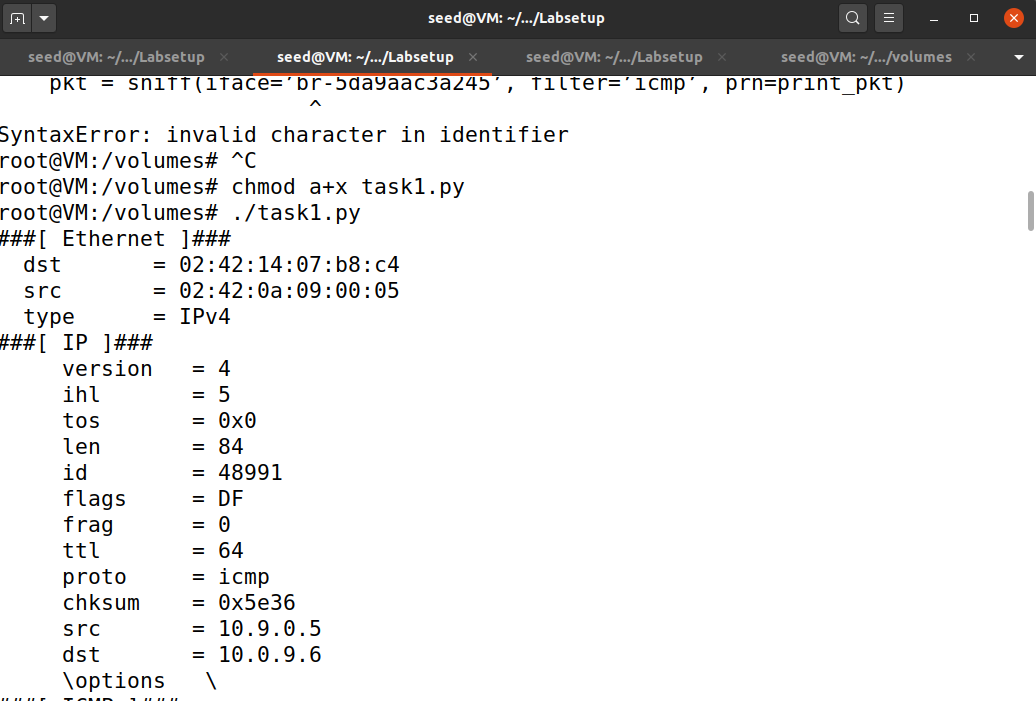
Name: Donghao Li

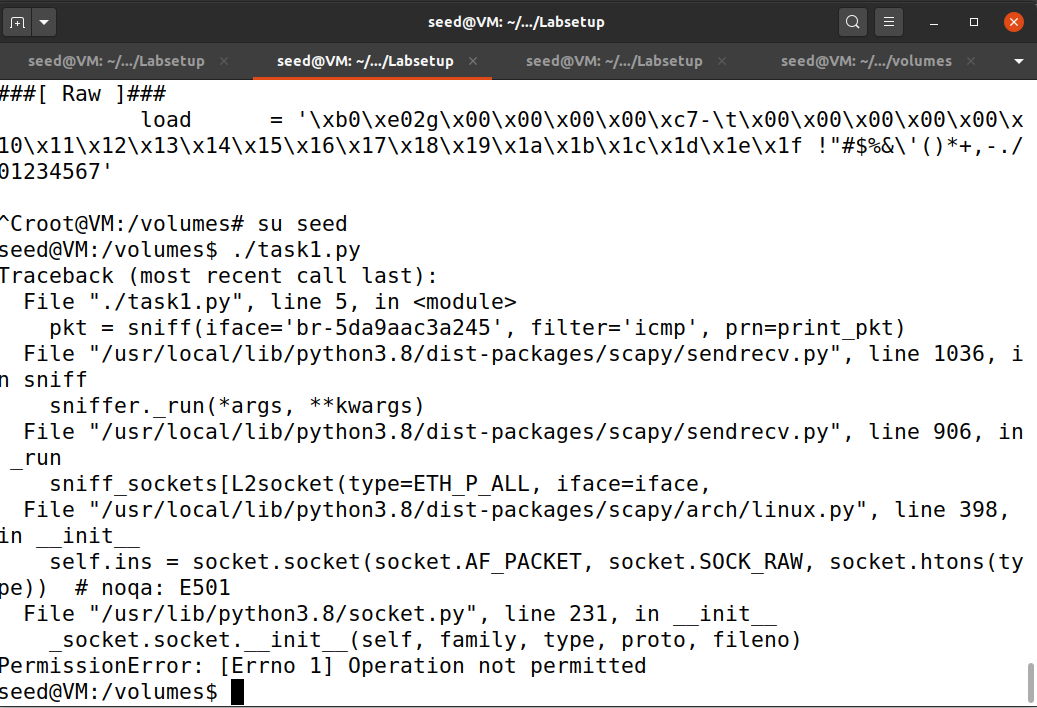
SU email: [dli106@syr.edu](mailto:dli106@syr.edu)

**Lab Task Set 1: Using Scapy to Sniff and Spoof Packets**

**3.1 Task 1.1: Sniffing Packets**

**Task 1.1A.**

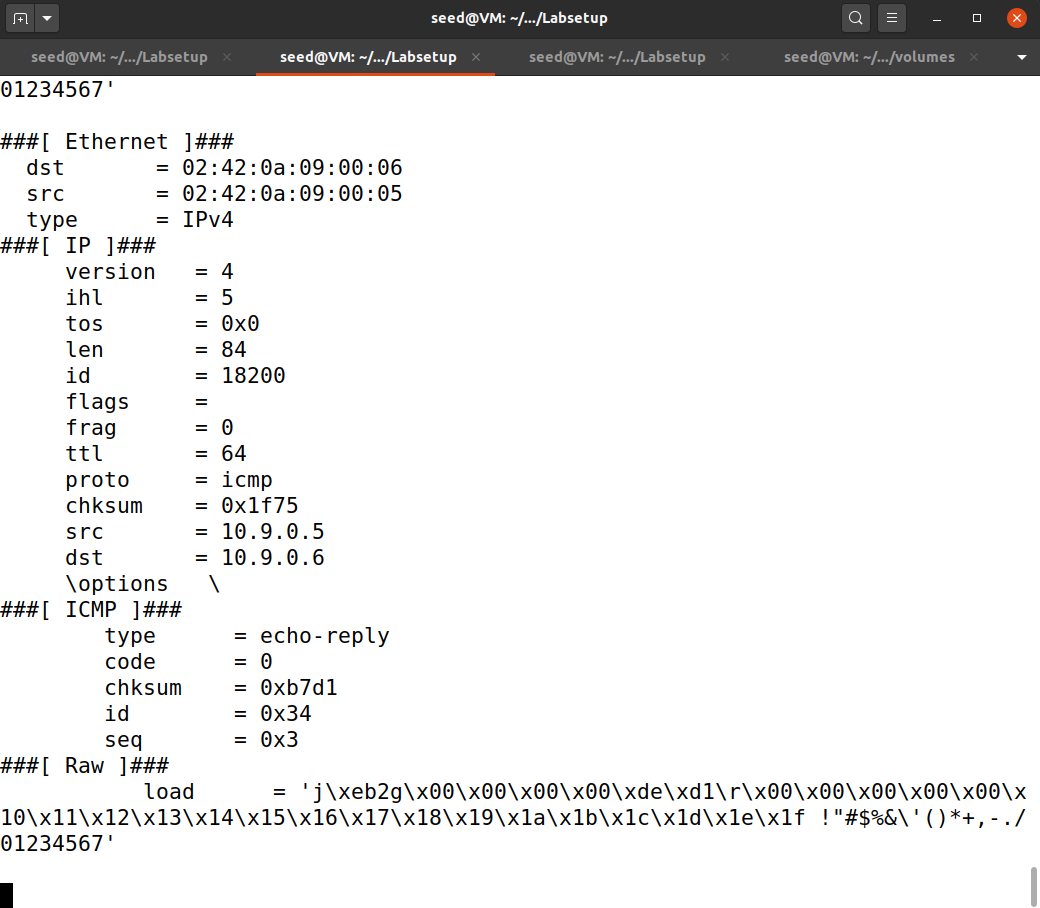
****



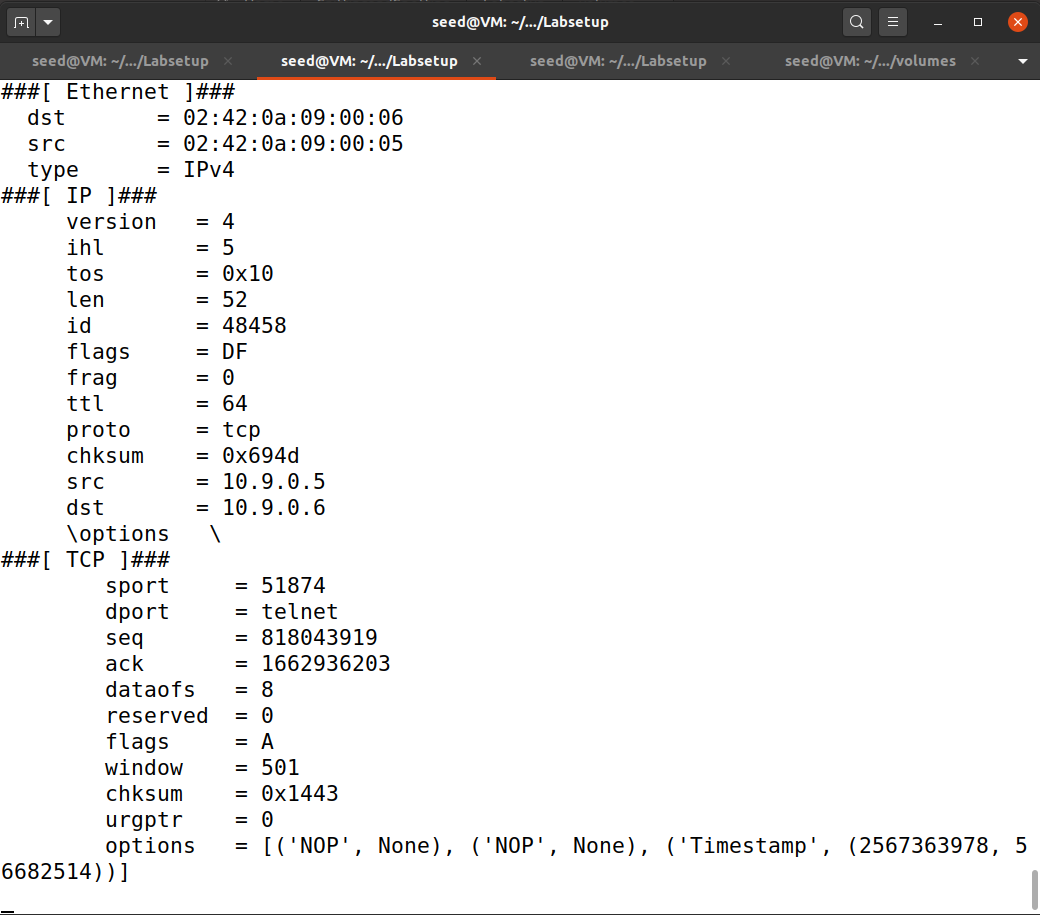
When I use root privilege to run the task1 file, it successfully sniffing the ping message i made from host A to host B, but when i switch to seed privilege, there is a operation not permitted error appeared. This error is thrown because raw access to network interfaces, which is required for sniffing, requires root privileges.

**Task 1.1B**

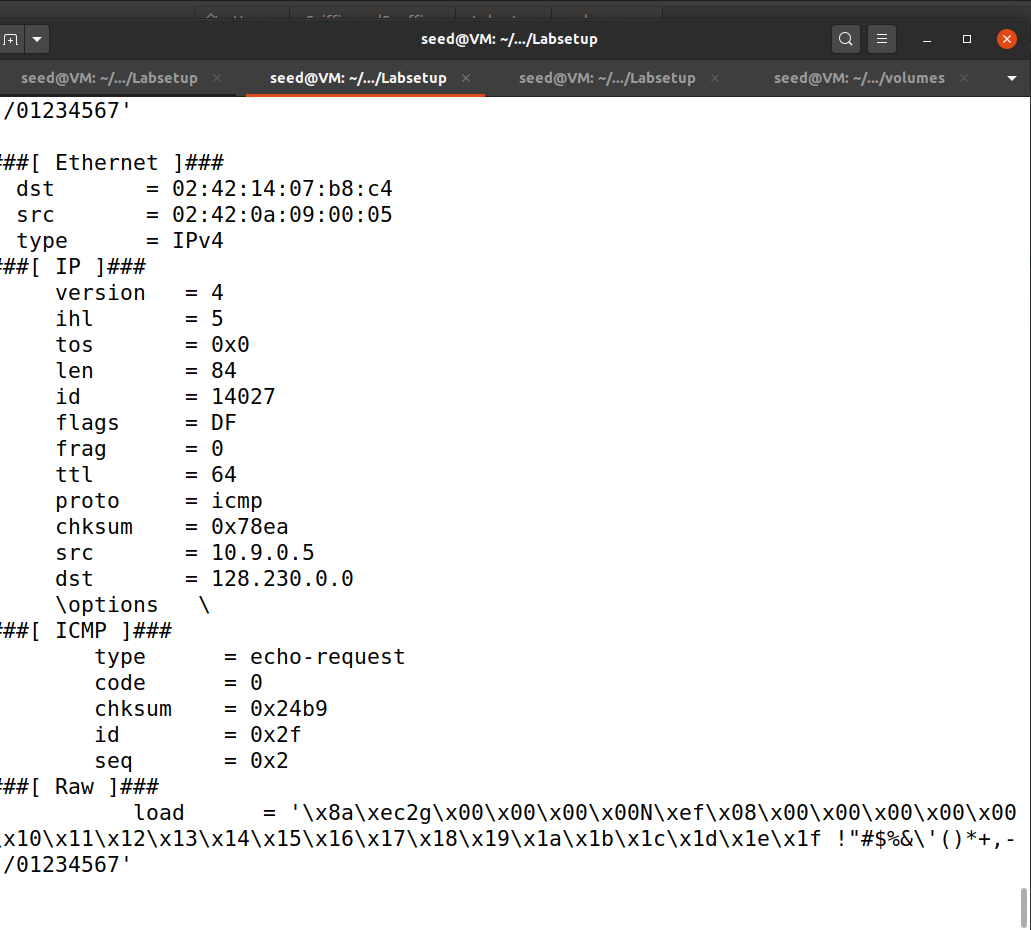
icmp

****

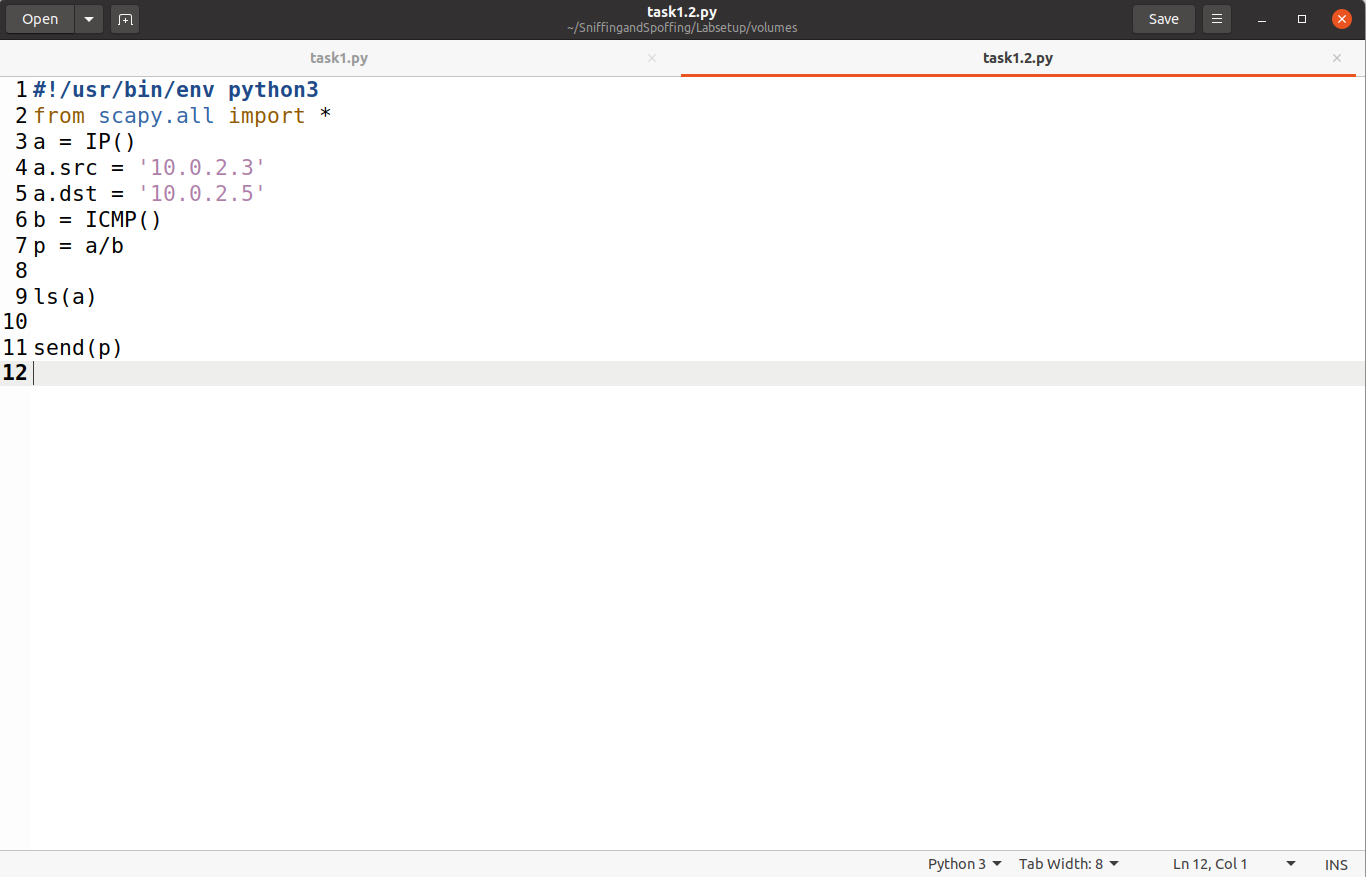
tcp && src host 10.9.0.5 && dst port 23

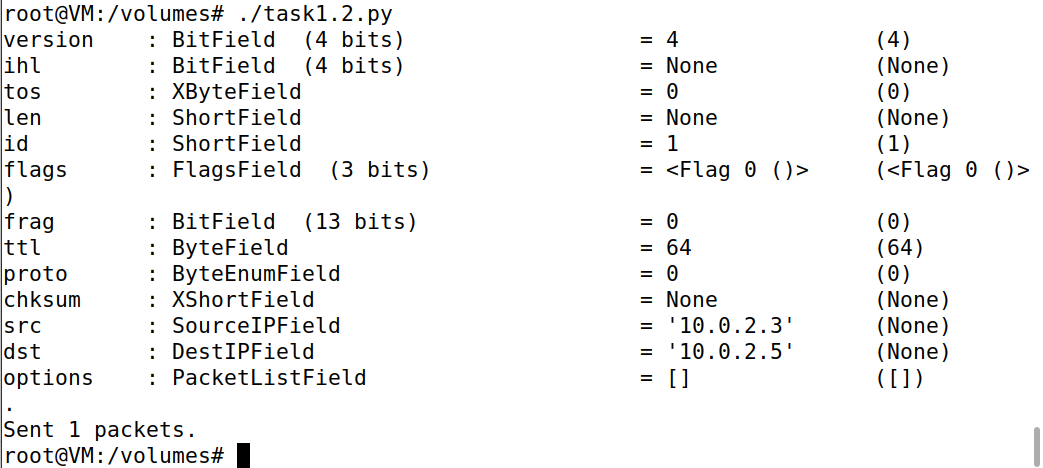


net 128.230.0.0/16



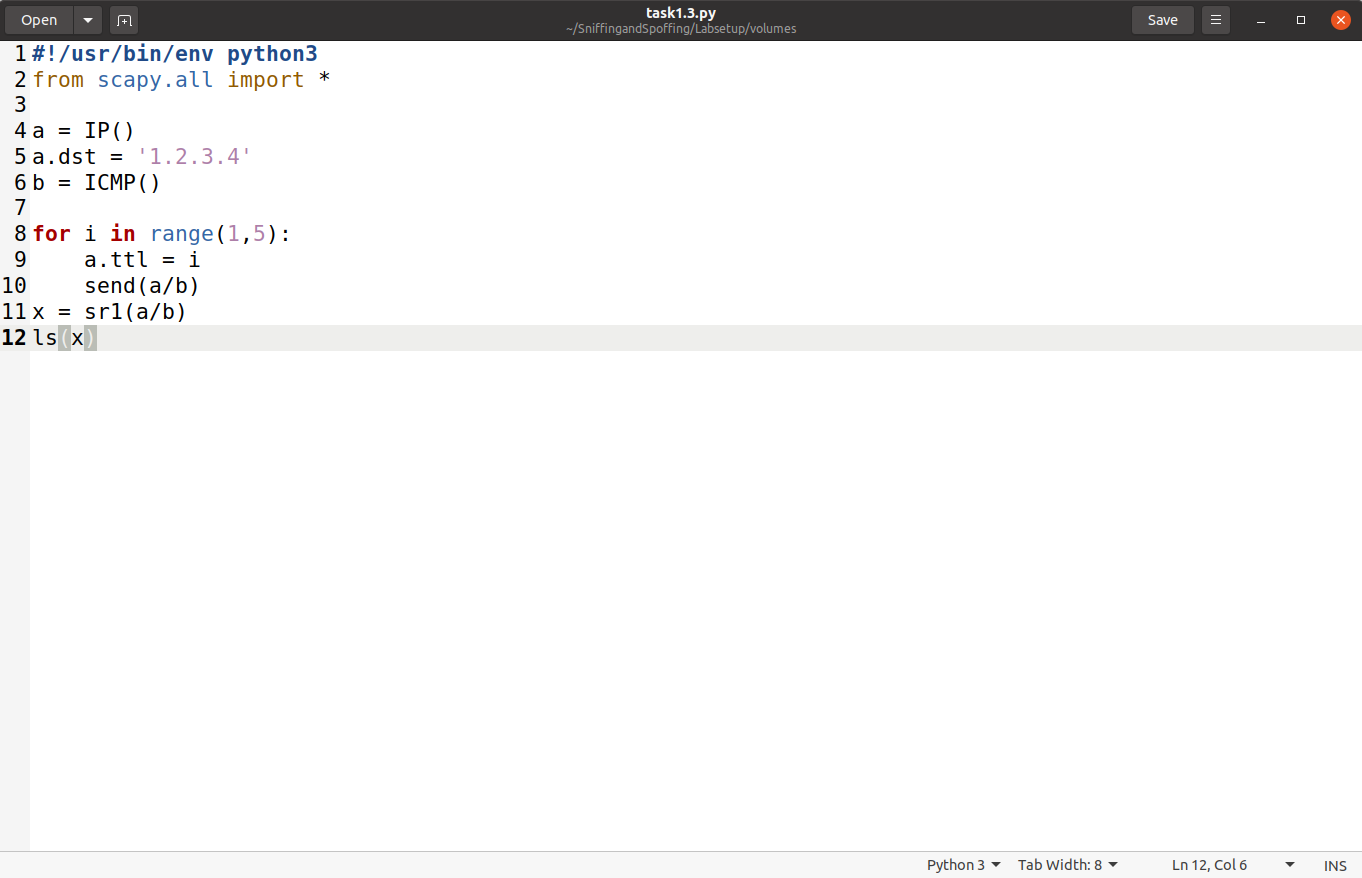
**3.2 Task 1.2: Spoofing ICMP Packets**

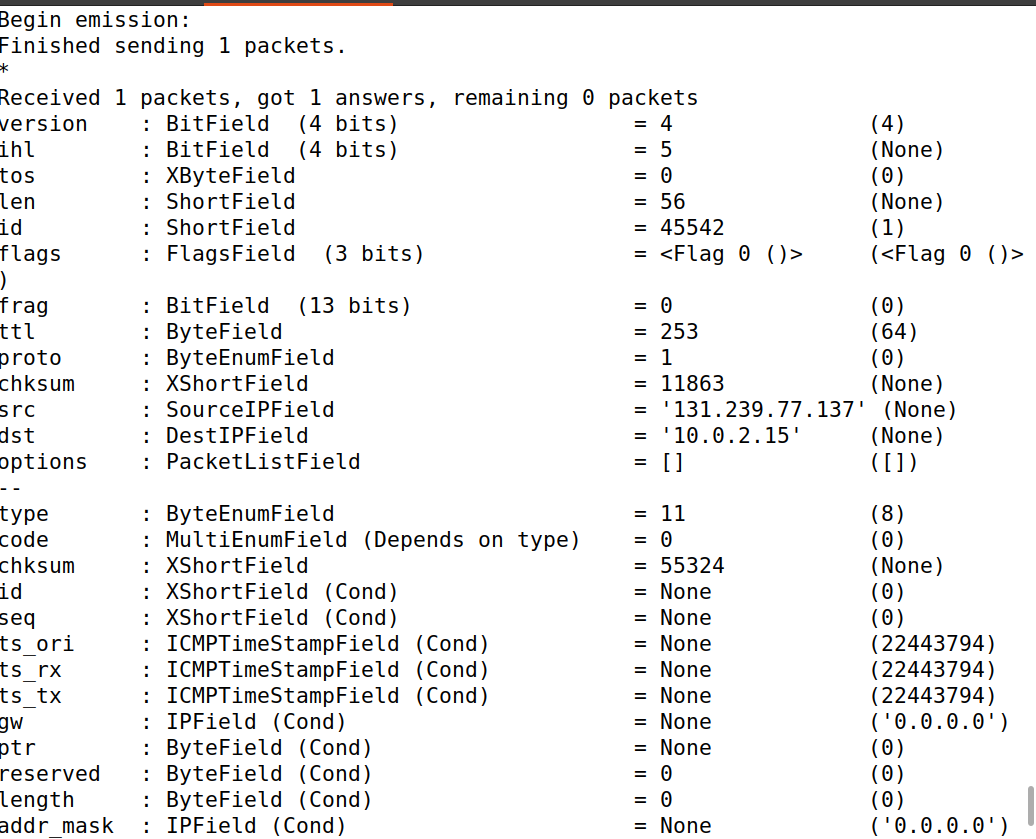
****



As you can see I set the source of a be 10.0.2.3 and the destination be 10.0.2.5. So that the code can be used to spoof IP address 10.0.2.3 when sending an ICMP packet to 10.0.2.5.

**3.3 Task 1.3: Traceroute**

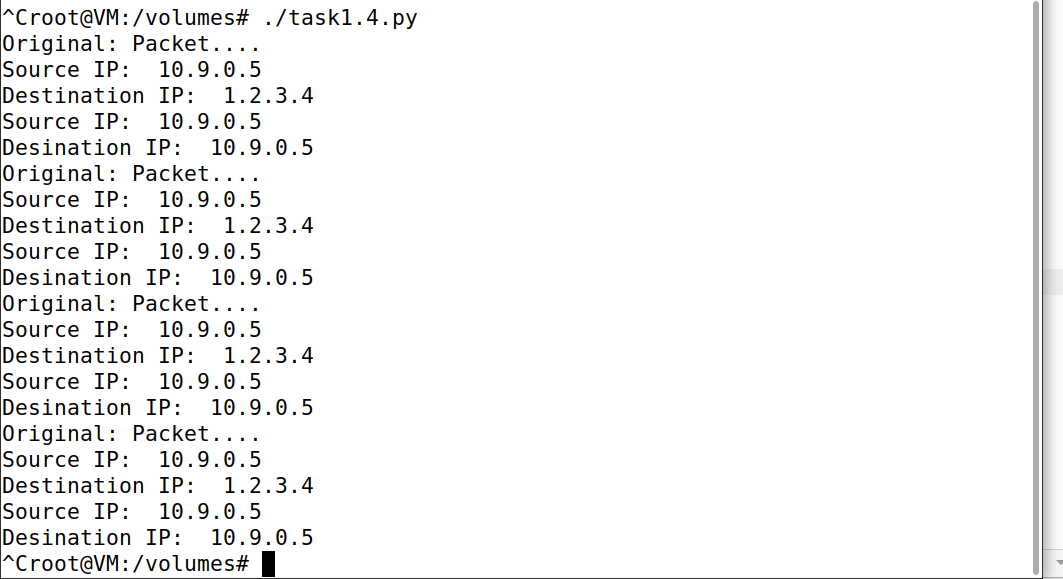
****

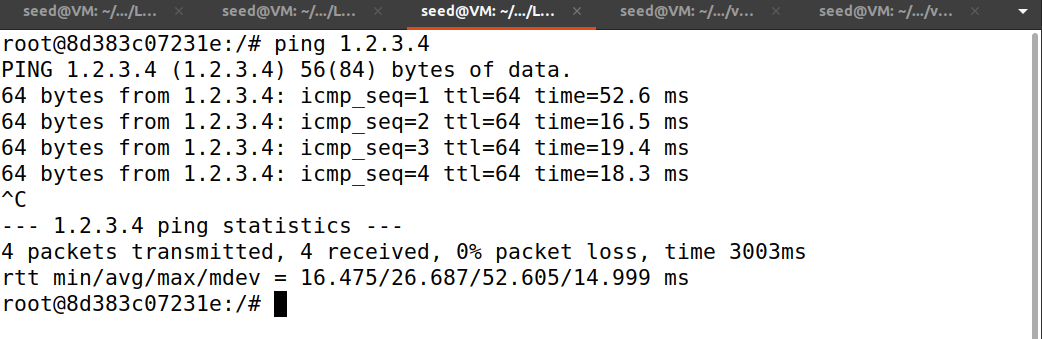


I use a for loop to help me iteratively repeat the procedure, as you can see the result is displayed in the screenshot.

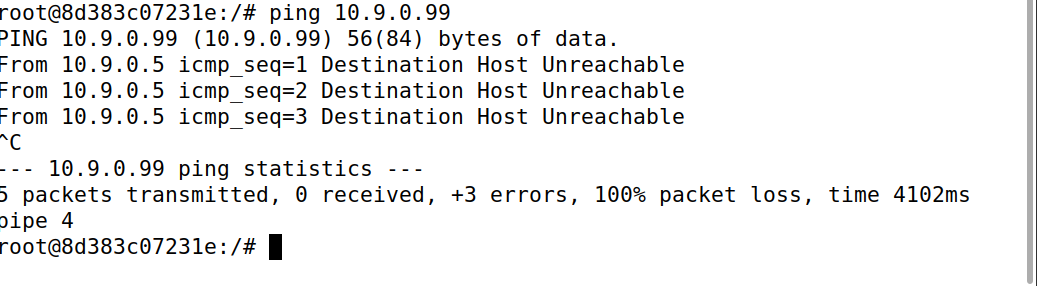
**3.4 Task 1.4: Sniffing and-then Spoofing**

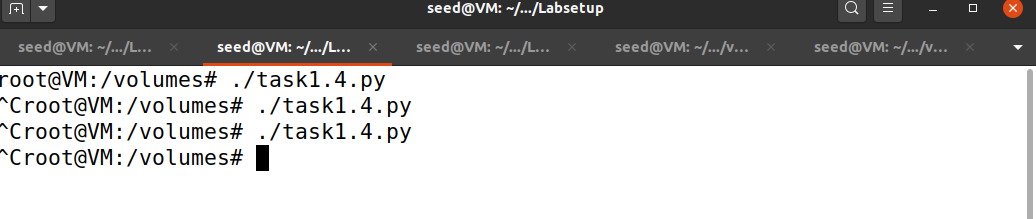
ping 1.2.3.4





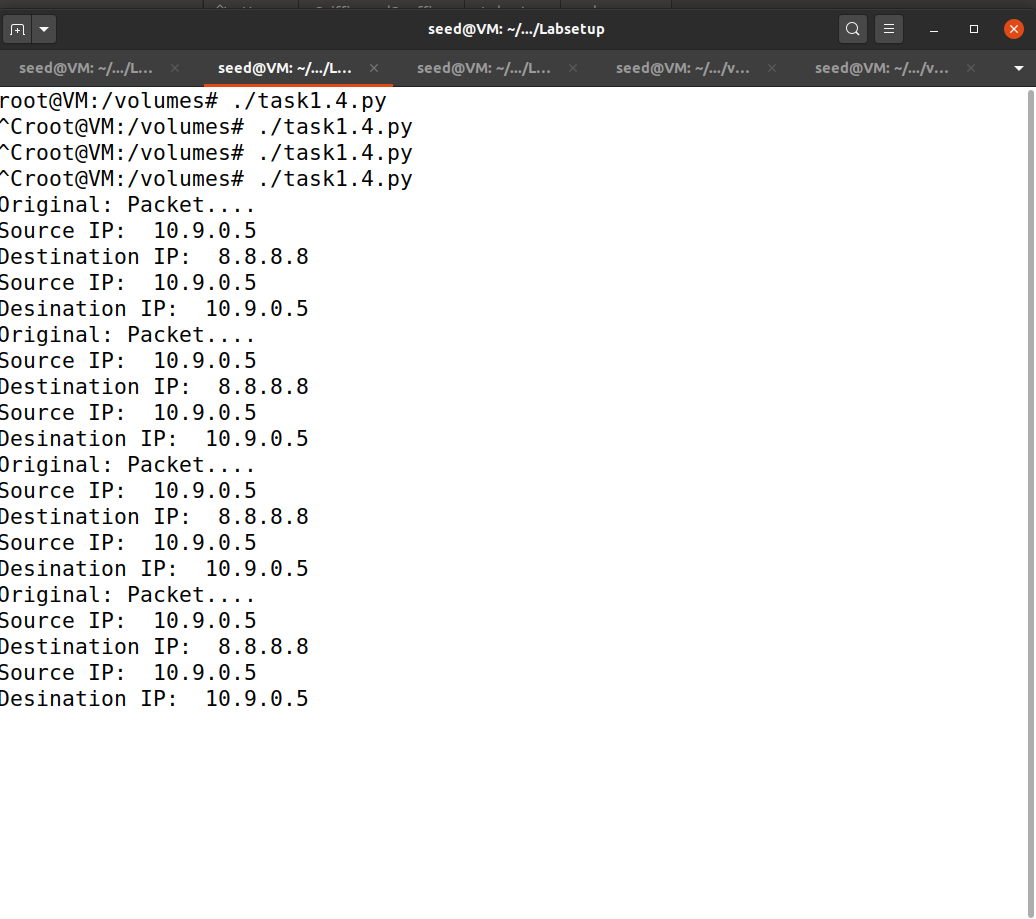
ping 10.9.0.99

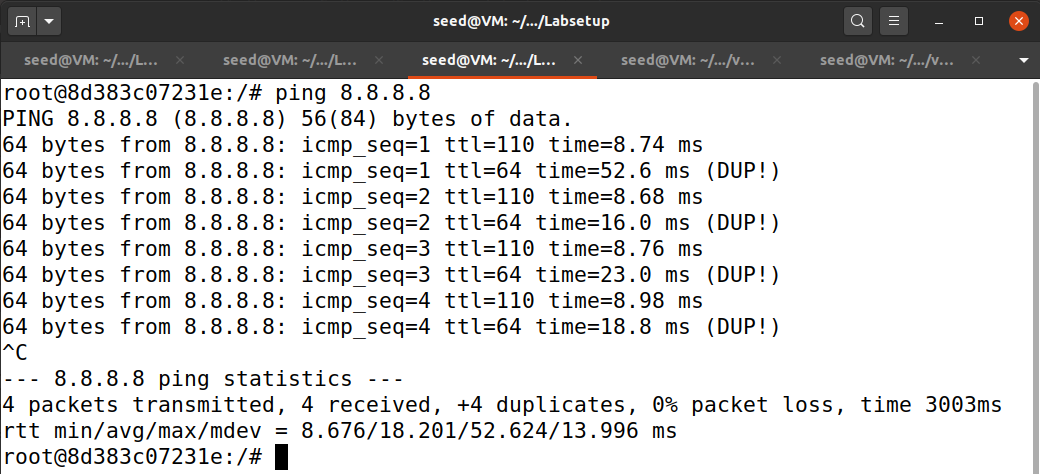




since this address is not existing on LAN which mean there is no record of mapping from record address to this ip address. when we ping this ip, the icmp packet can not create without the mapping so the attacker sniff and spoof nothing

ping 8.8.8.8





with a smaller number in ttl, we get duplicated file. This represent that the spoof file created 4 duplicated file while the real file is pinging. when we check the result of the attack container, it seems also shows this result.