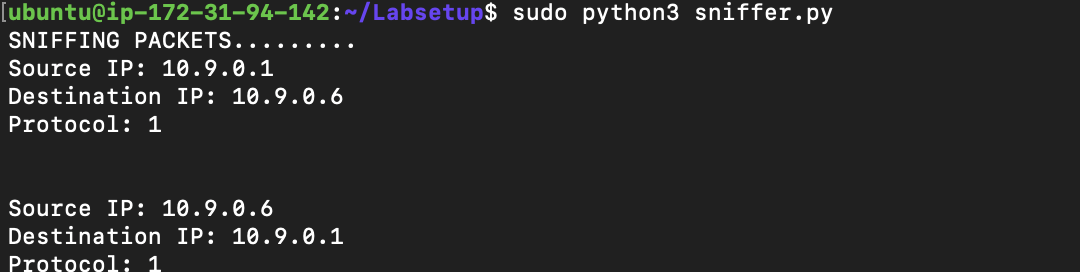
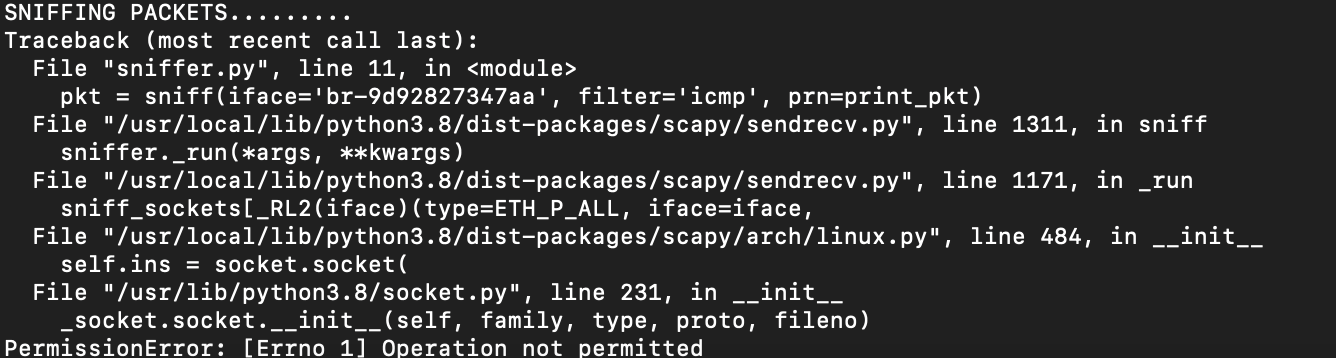
**Task 1.1A:**

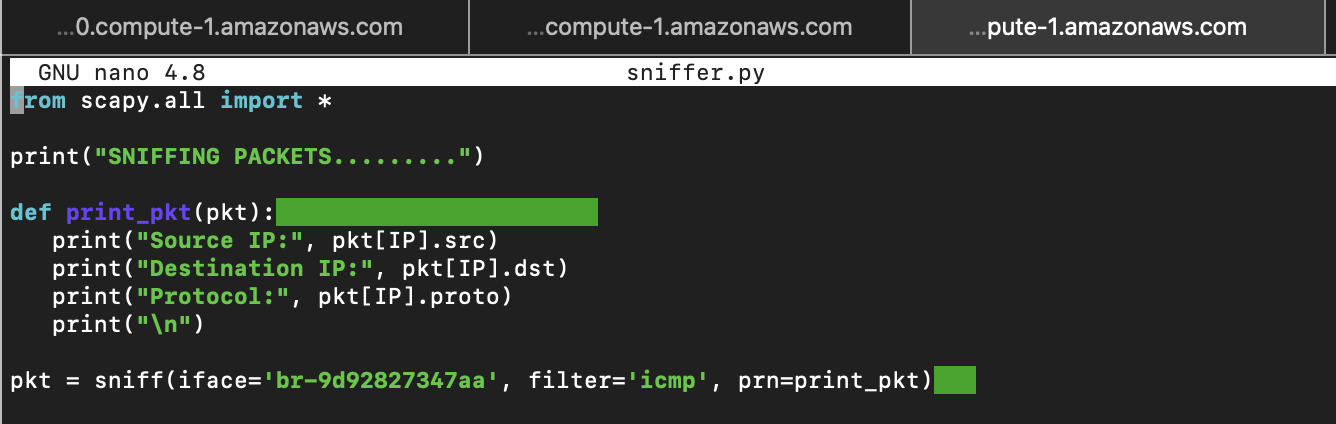
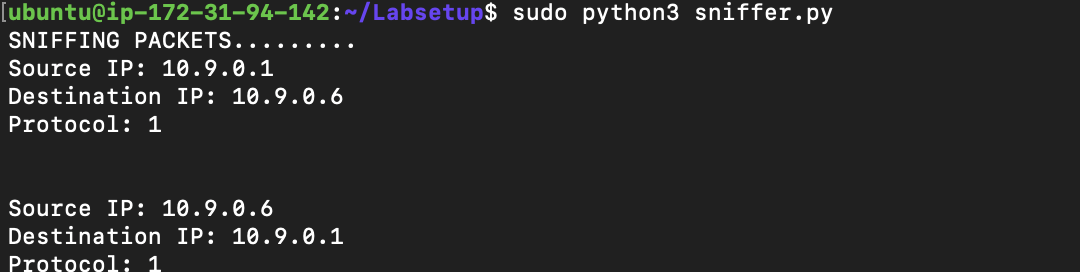
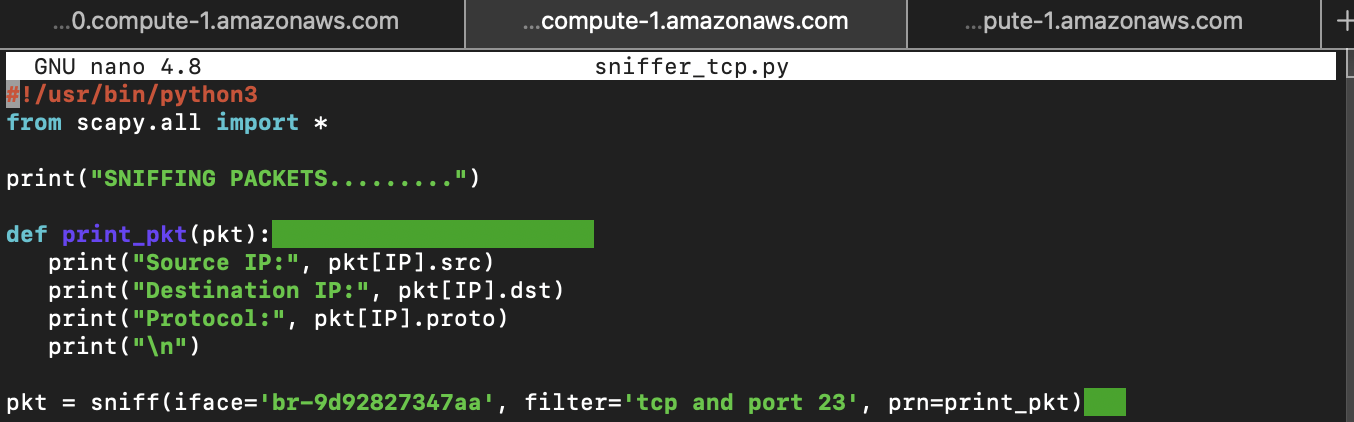
With privilege:

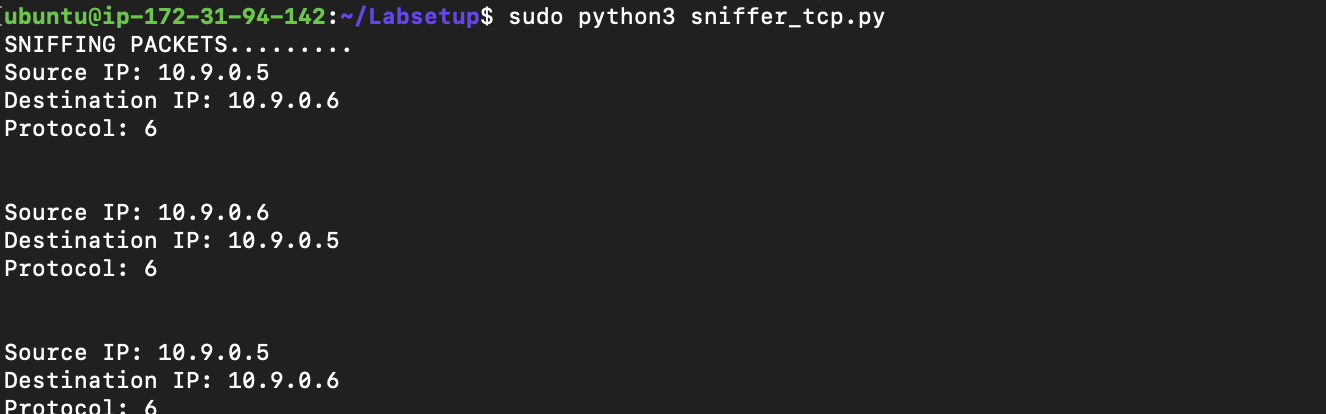


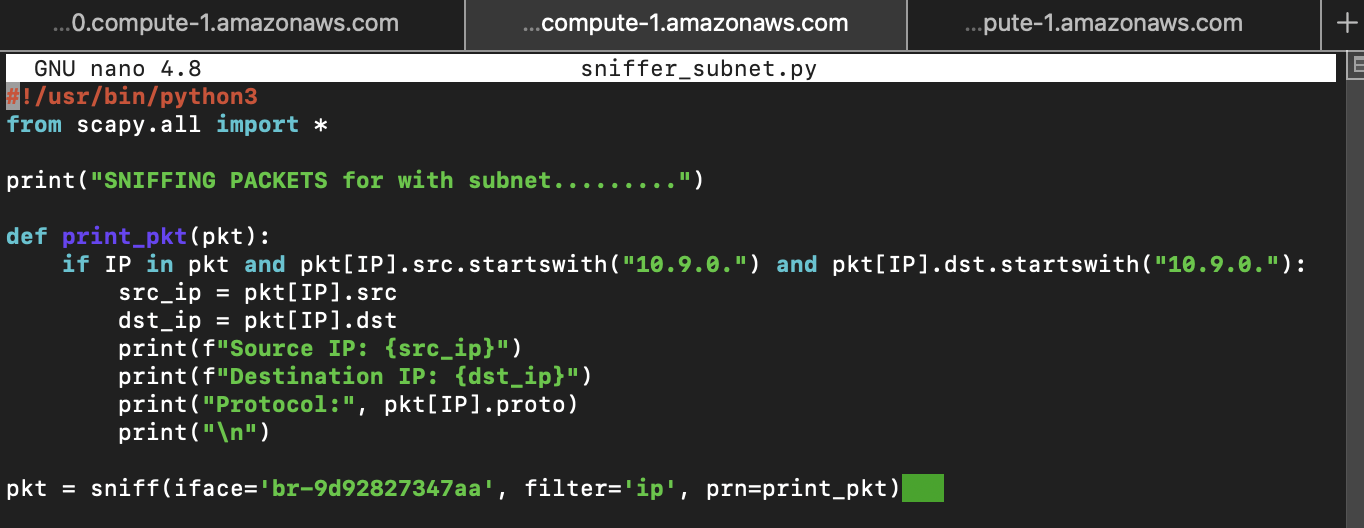
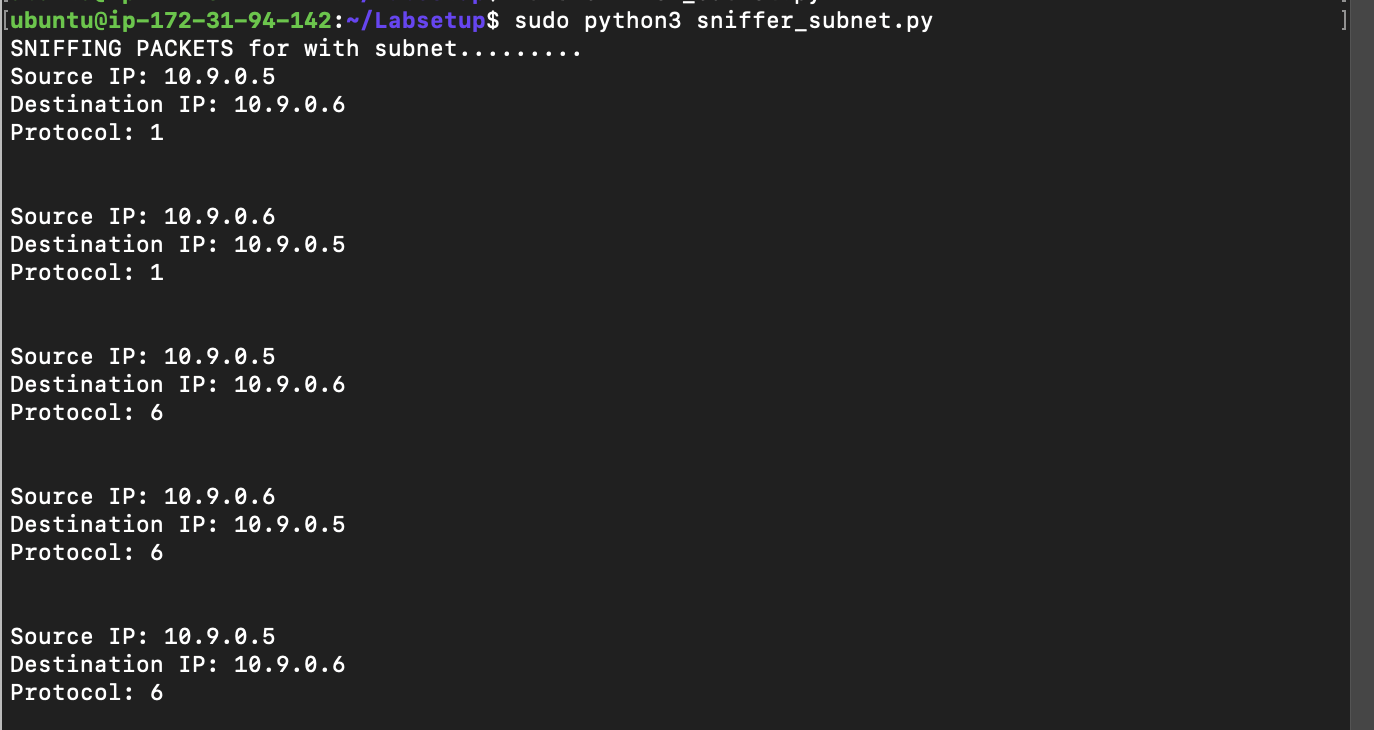
Without privilege: ****

**Task 1.1B:**

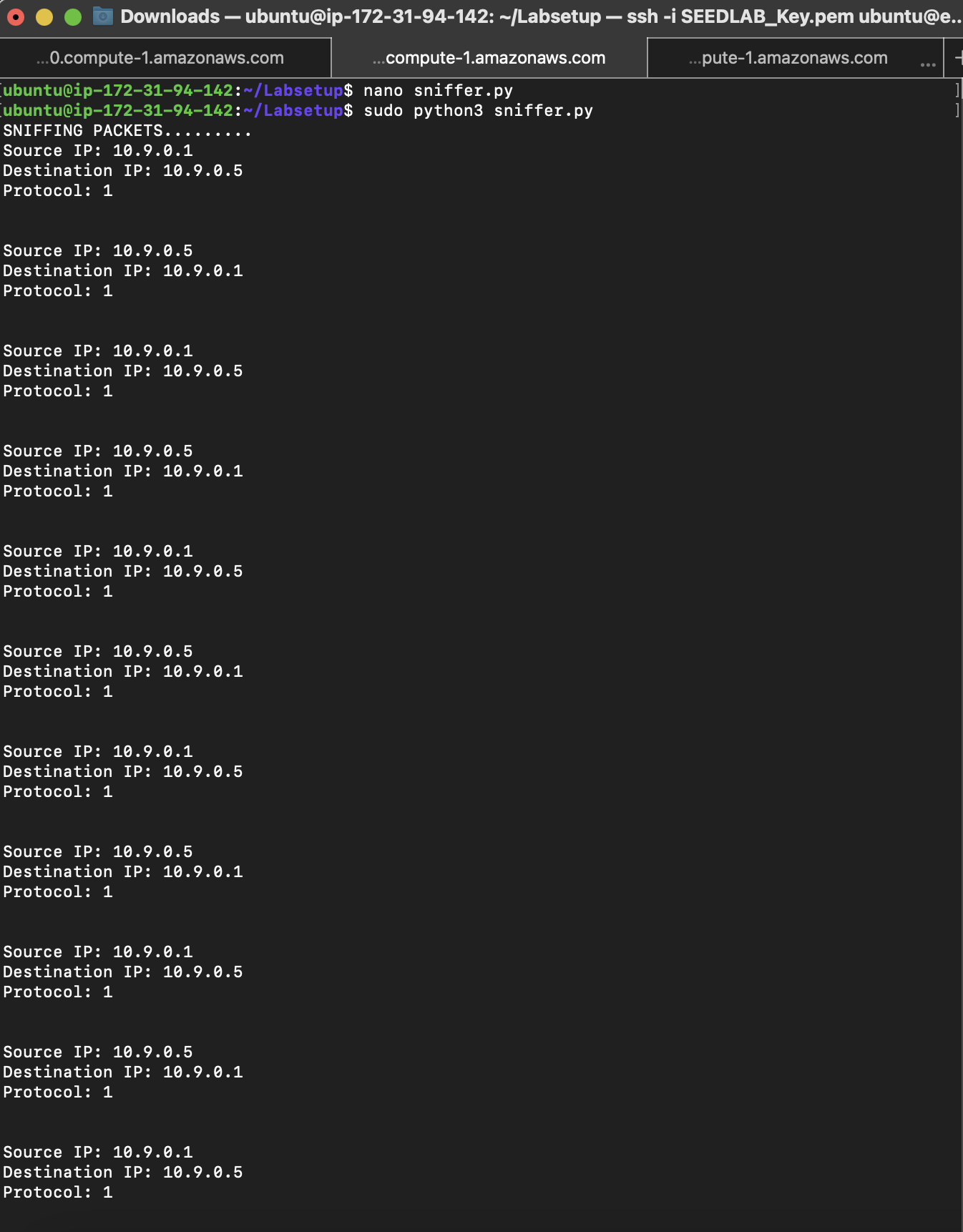
I have used this code for sending dummy packets:

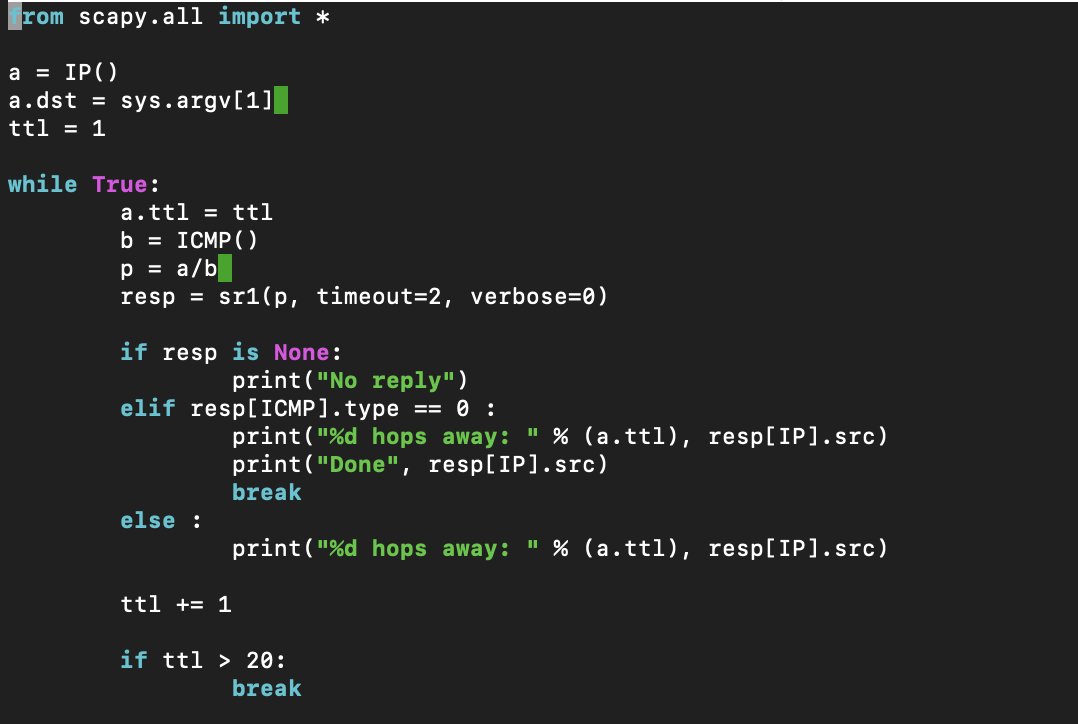
* Using ifconfig command, I get the interface that I have put in the code. The code sniffs icmp packets like ping requests and prints source, destination and protocol id.
* For port 23 I have to check the tcp protocol using the code change in the filter for tcp with port:

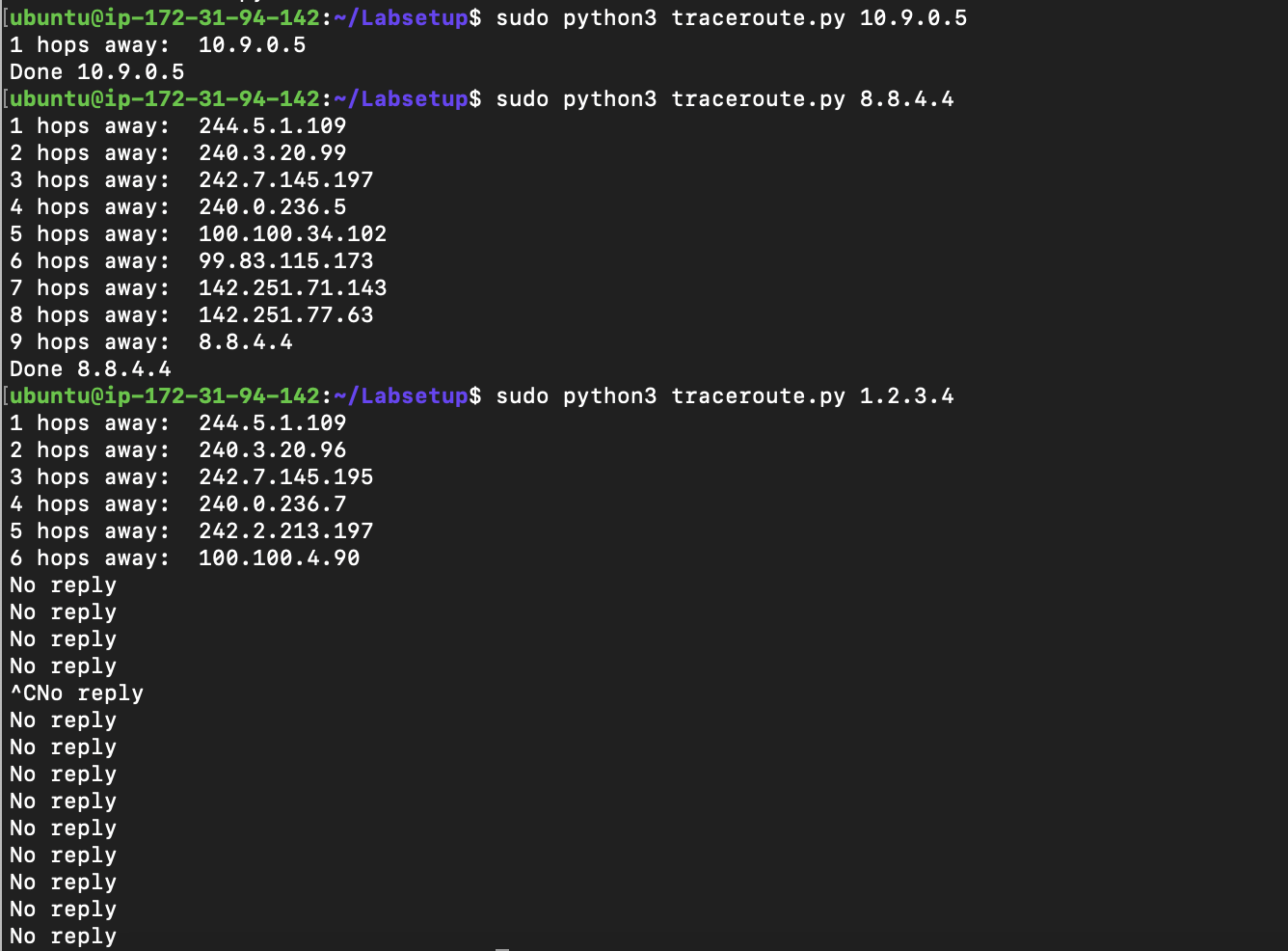
I get the result:

* For subnet, which in my case was 10.9.0.0/24. I checked the ip address and filtered the ip addresses starting with ‘10.9.0’ as it includes all the ip addresses in the subnet.  
  Using code:  
    
  I get:  
  

**Task 1.2**

The code from Task 1.1 for icmp can be used for sniffing icmp packets. We will be using ping which sends ICMP request and i get result for pinging 10.9.0.5 from 10.9.0.1:  


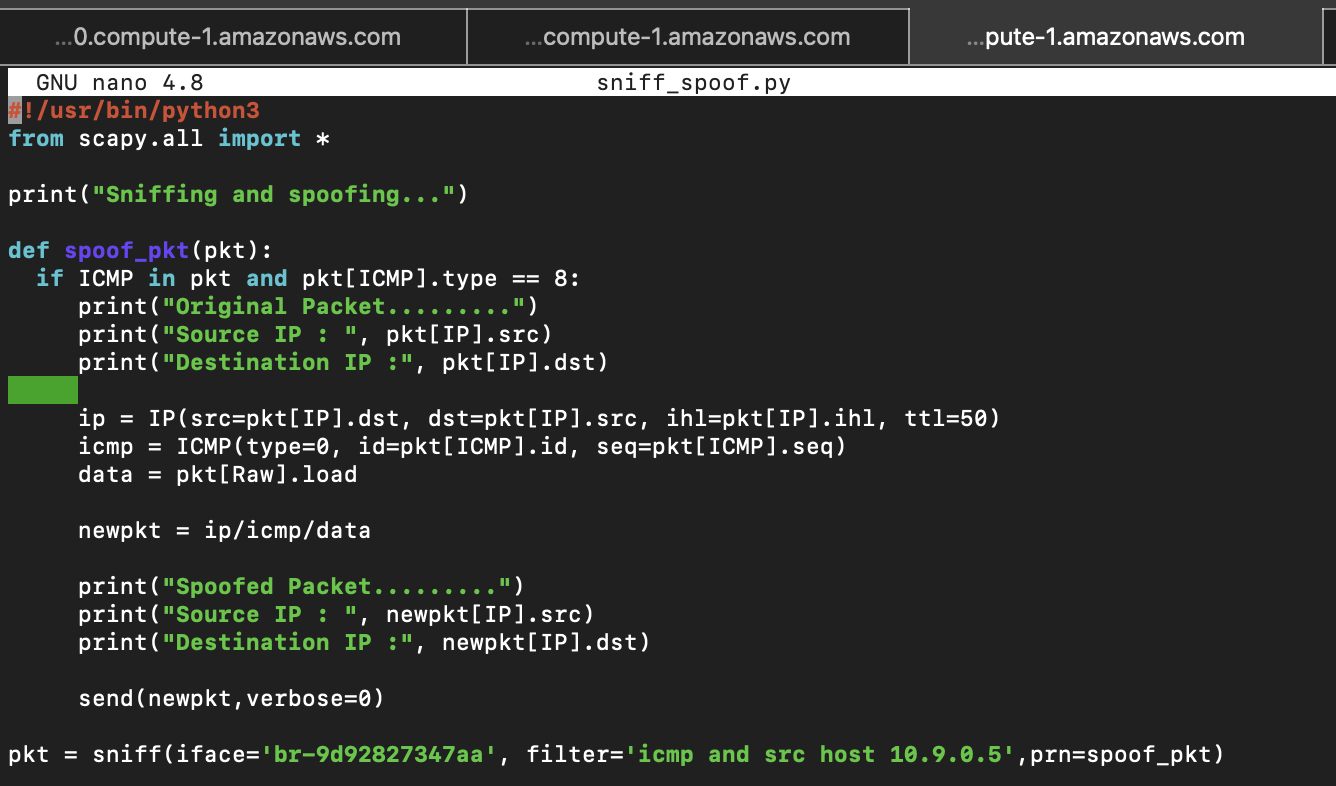
**Task 1.3:**  
Code:  


Result:  


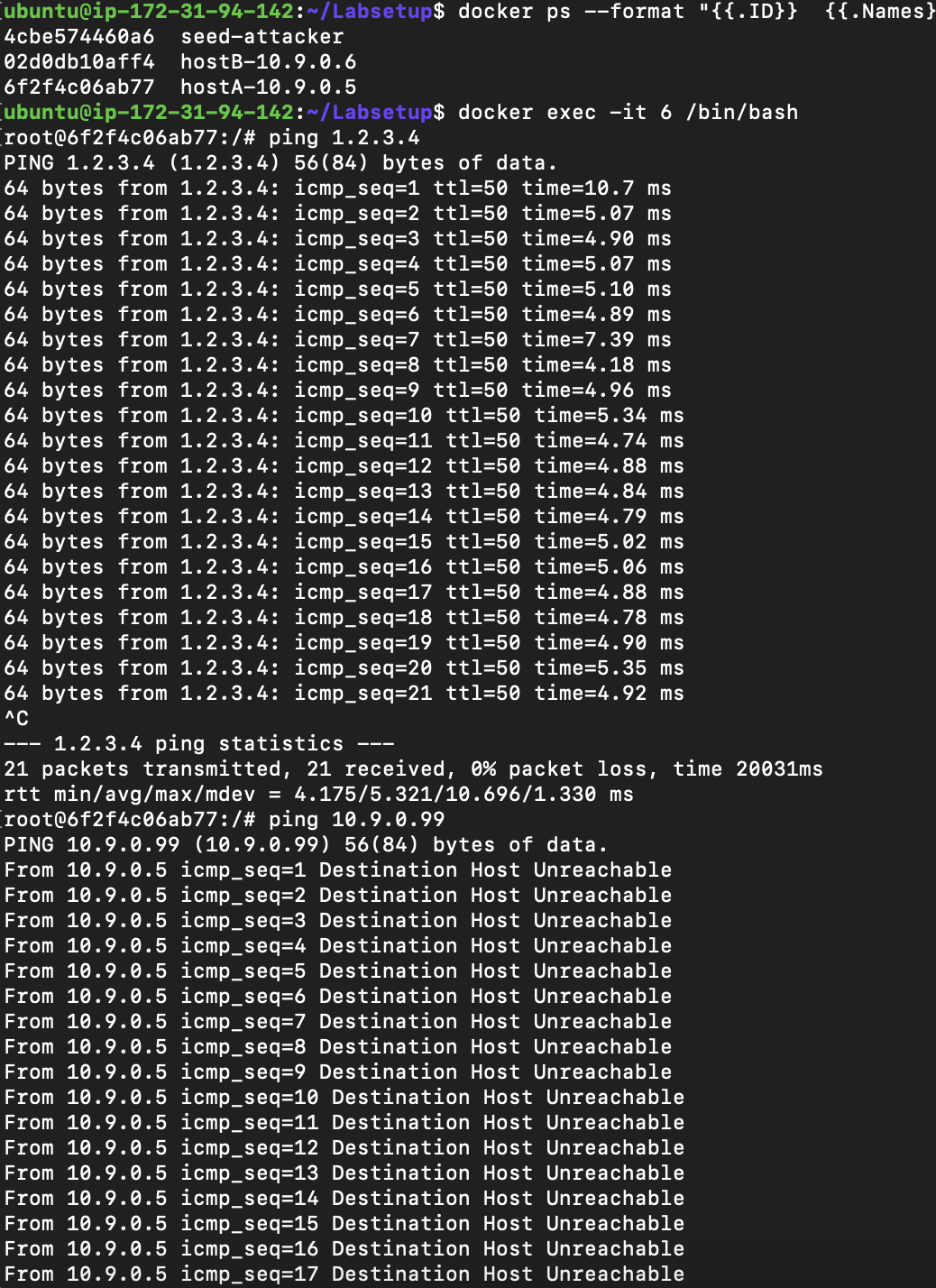
Observations:  
Here we keep on pinging the destination increasing the ttl i.e. number of hops so it can do more hops and stop when the packet reaches its destination and we know how many hops from the ttl. If it does not reach its destination we get no reply.

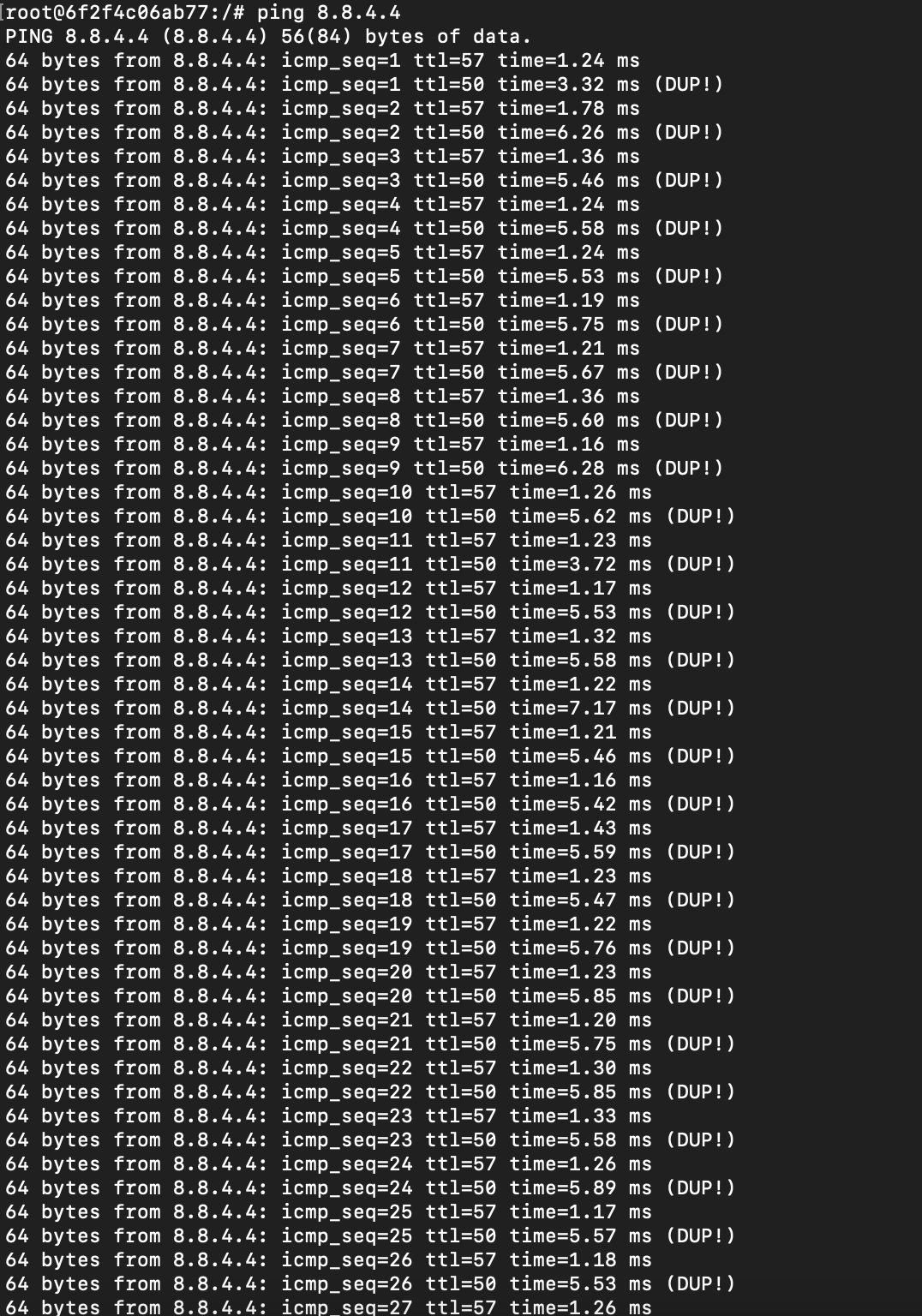
**Task 1.4**

Code:



Result:  
For 1.2.3.4, 10.9.0.99 and 8.8.4.4:





Observations:  
The code does operations for request icmp packet, exchanging source and destination port an keeping ttl to 50 and replying with icmp of same id and sequence. We can see the spoofed reply has TTL as 50.  
For 1.2.3.4, since there is no such ip address we just get one spoofed reply.

For 10.9.0.99, we dont have arp with such ip address so it will show destination host unreachable

For 8.8.4.4, there will be two reply, one spoofed and another from the intended destination device.