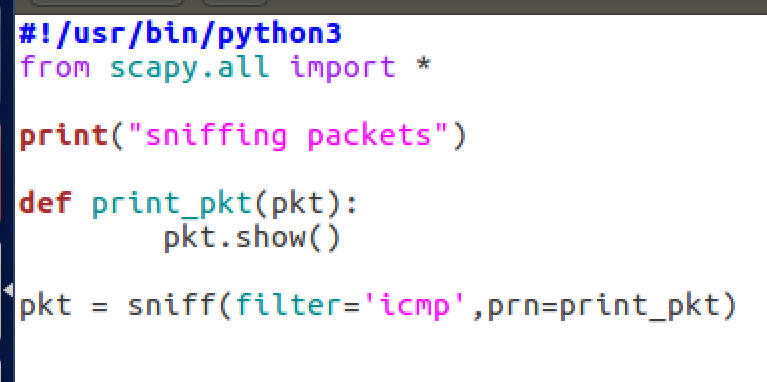
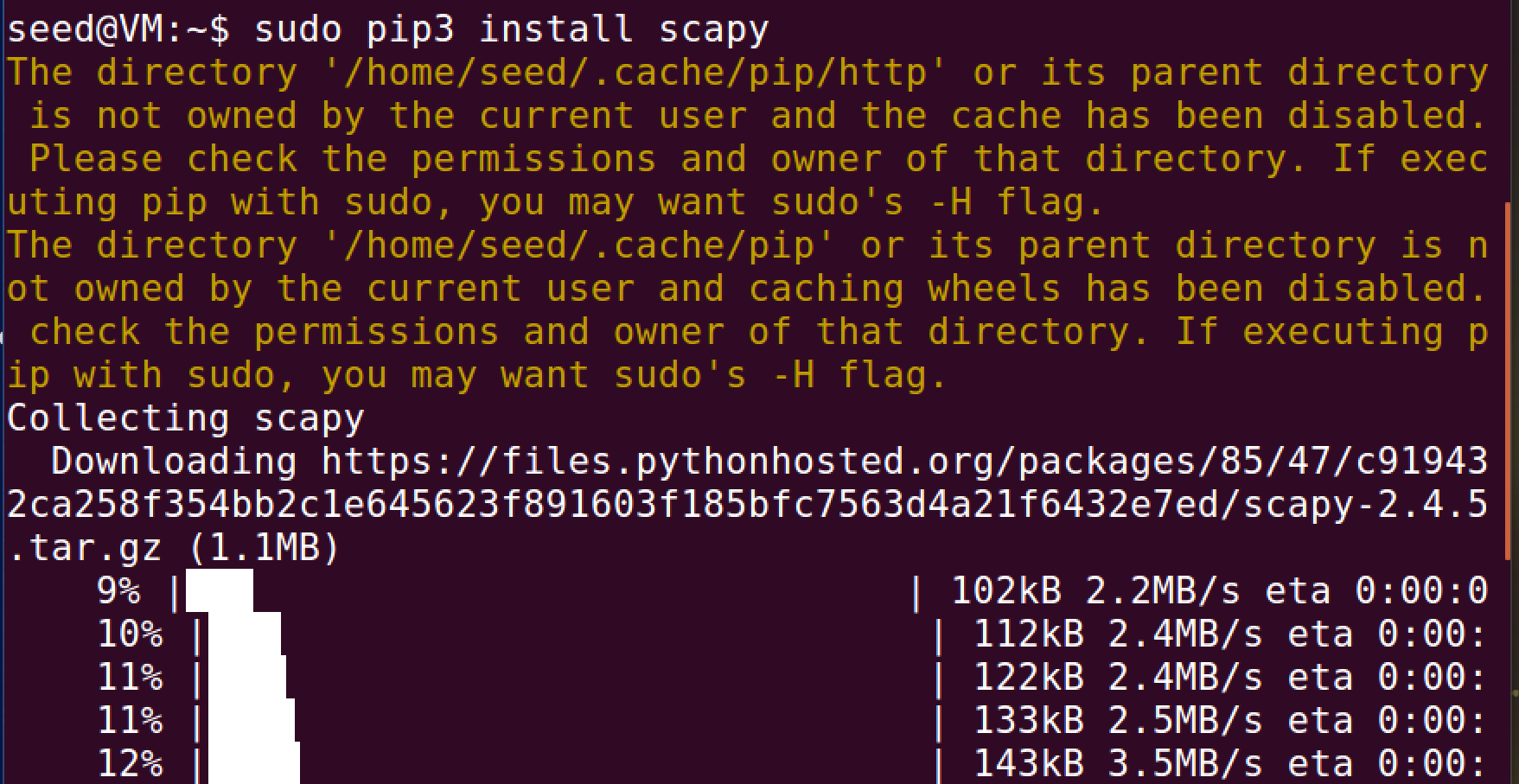
Lab 8

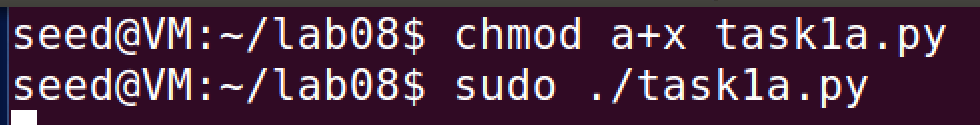
Task 1.1A:

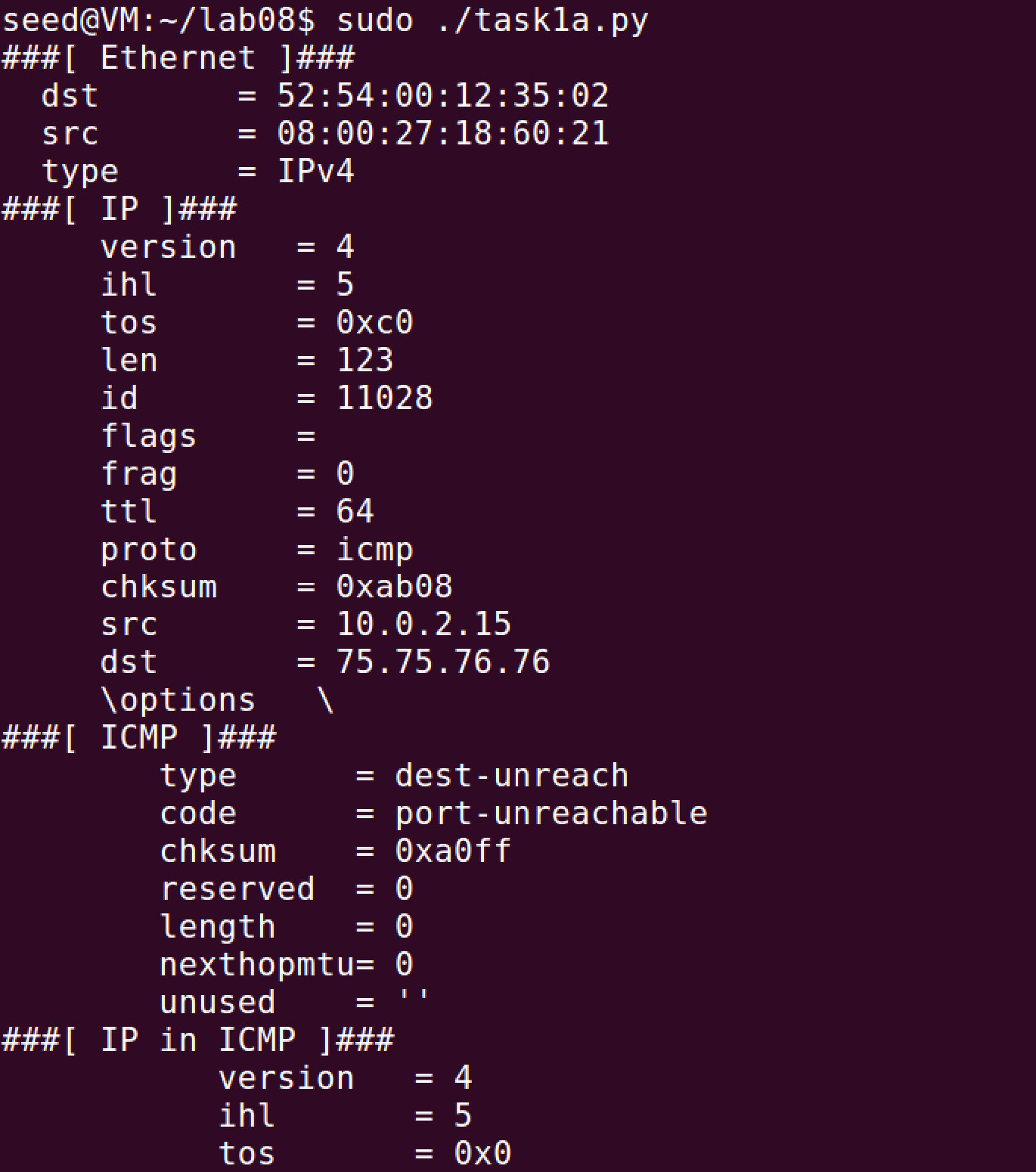
Code Used:

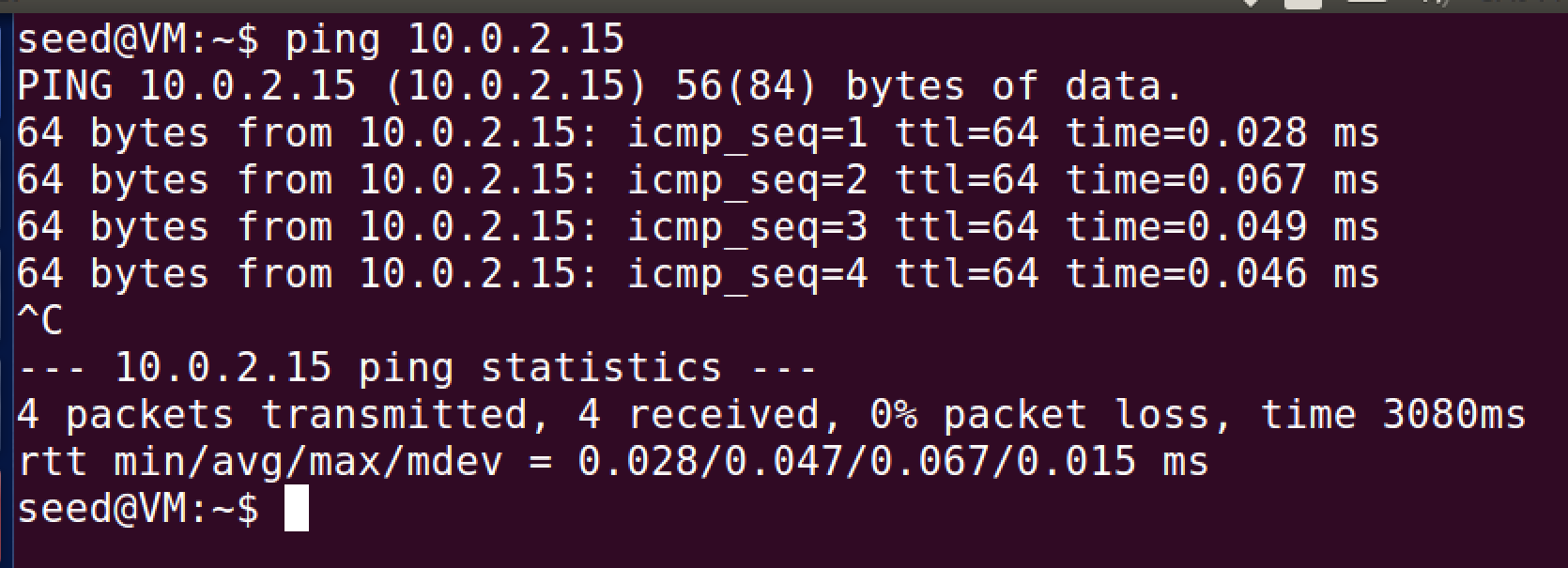


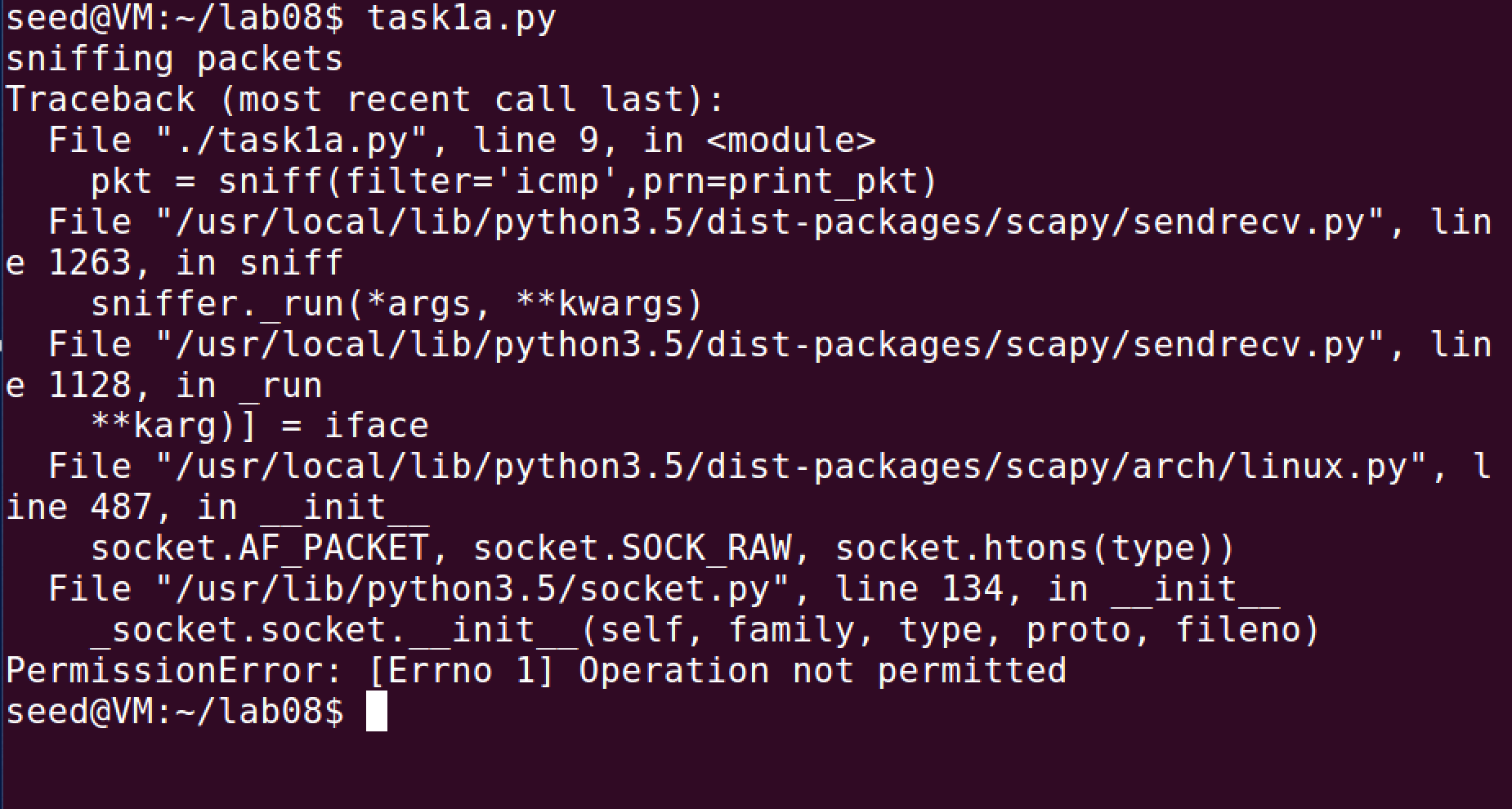
Commands and Results:









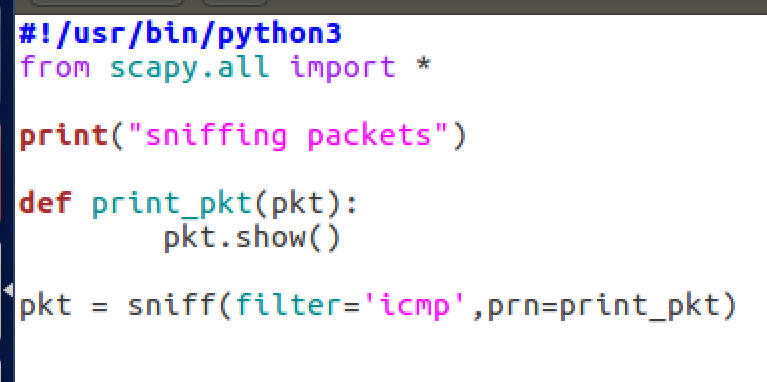


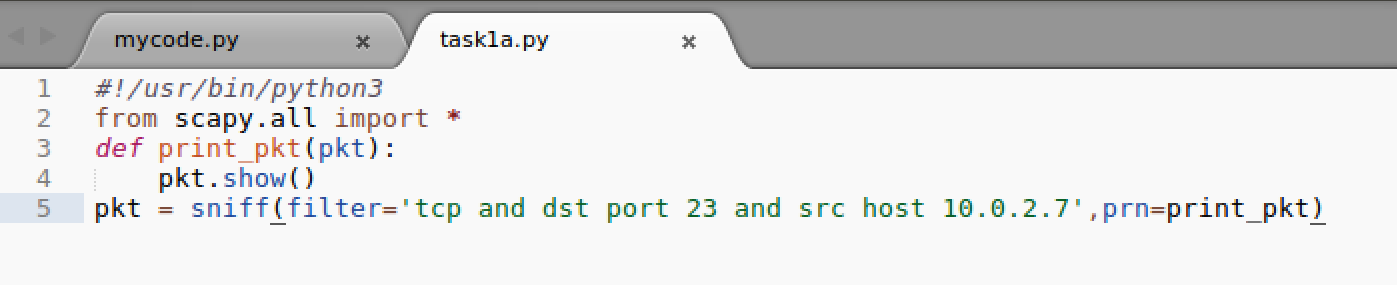
Comments:

First I had to install scapy onto the system to make this able to work. The code is meant to sniff packets from another terminal and print the information to the original terminal. When I ran it with the root privilege it ran no problem, but when I ran it without, it did not work anymore and it said operation not permitted.

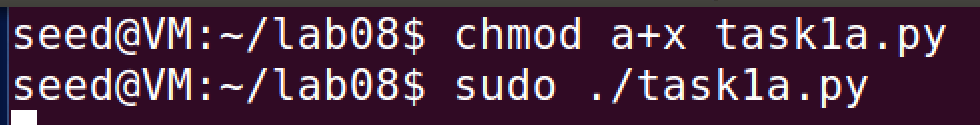
Task 1.1B:

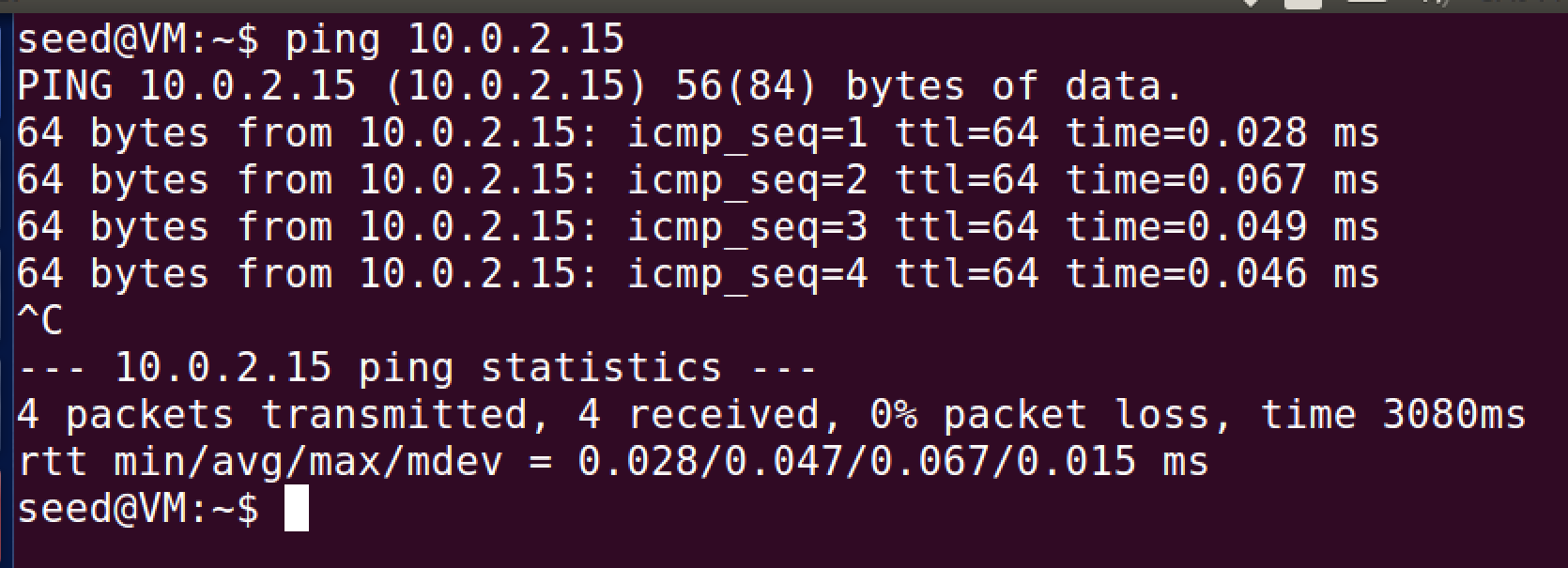
Code Used:

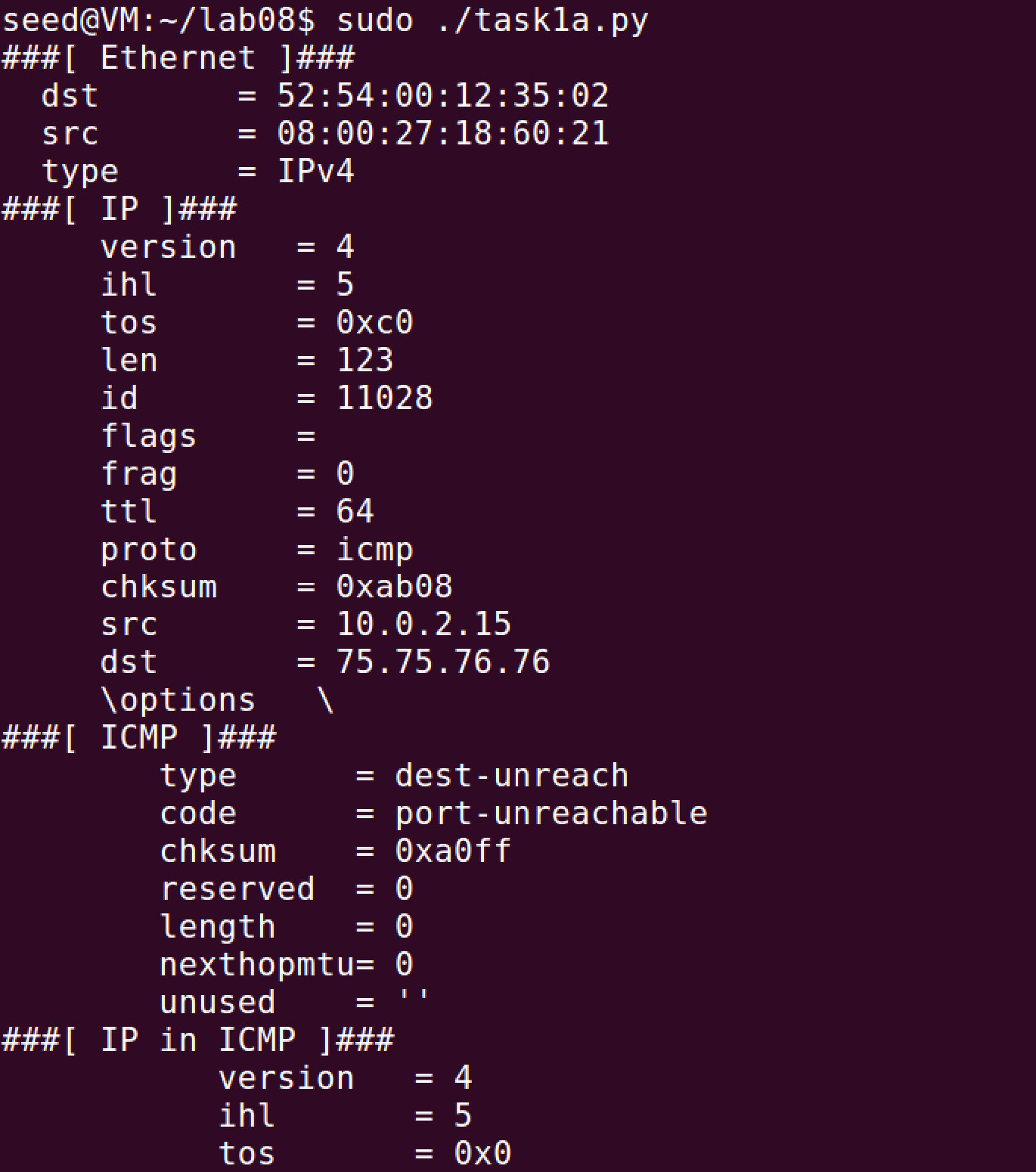


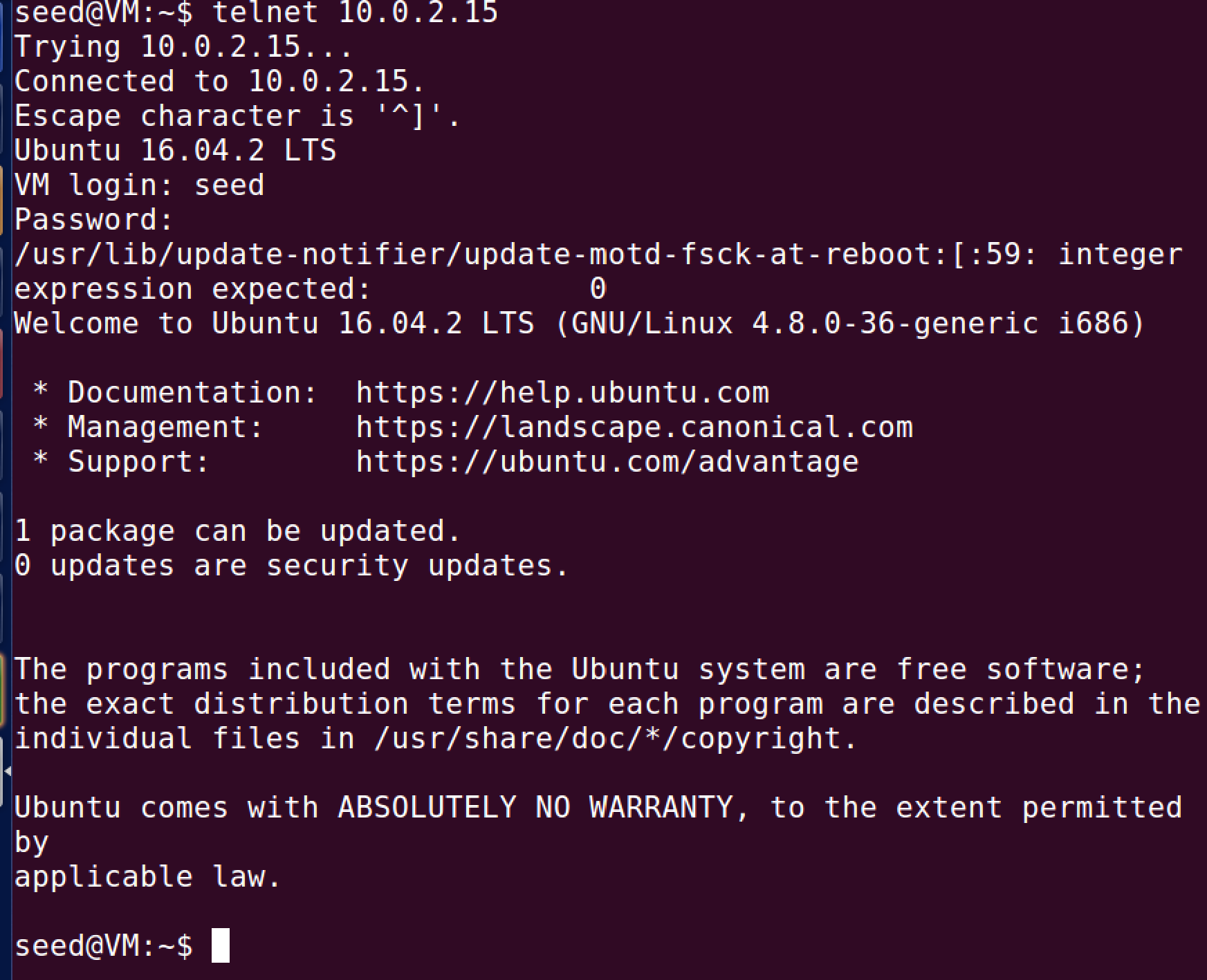


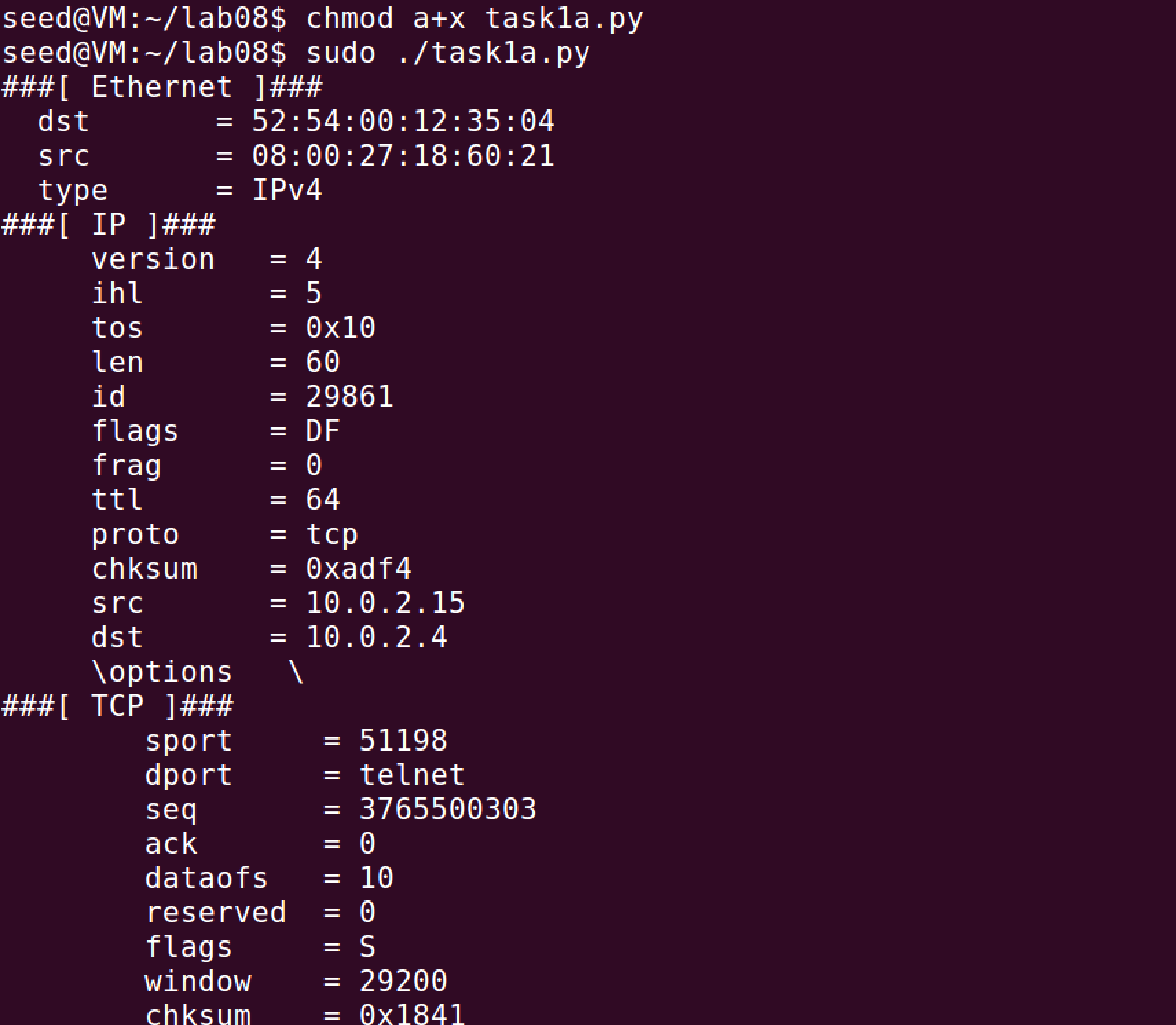
Commands and Results:

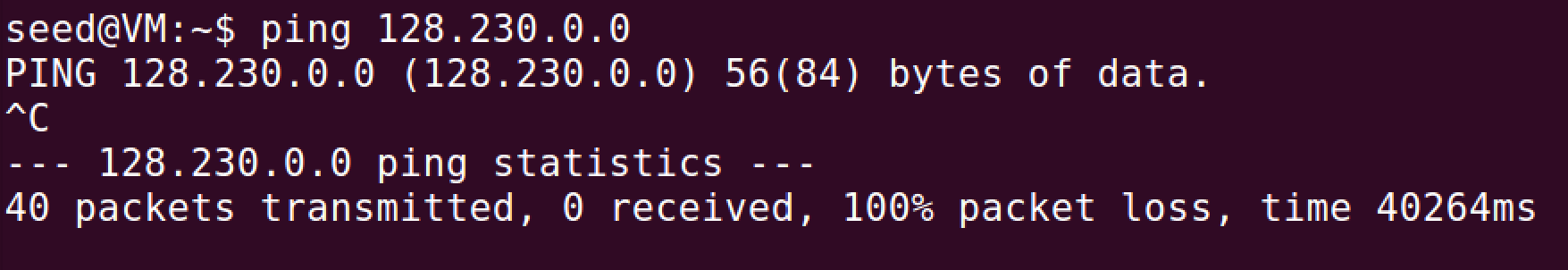


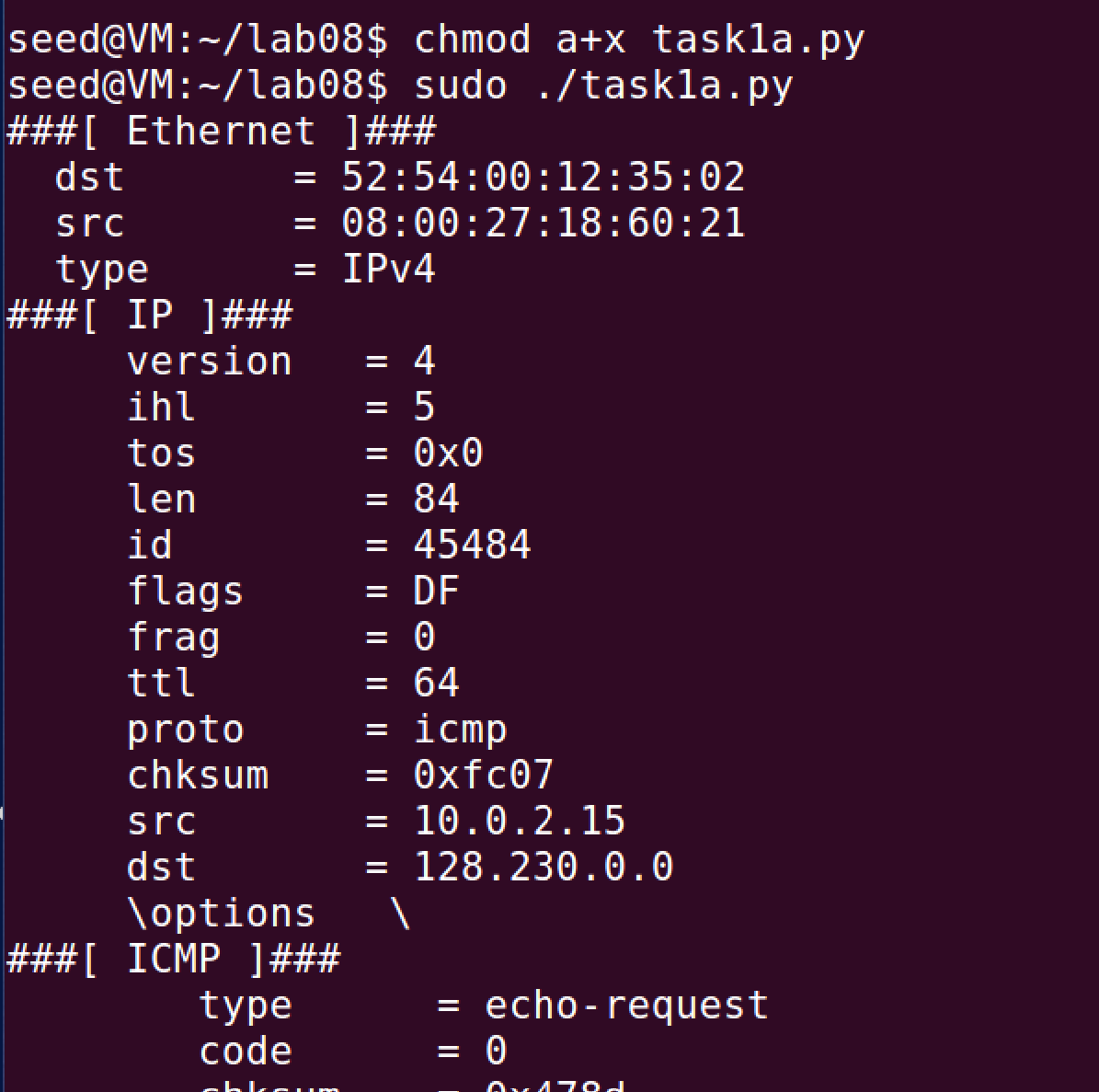












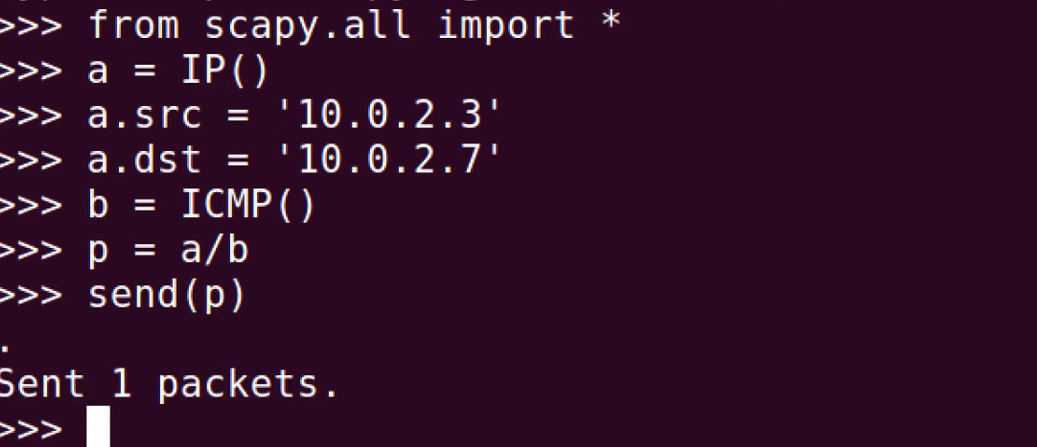
Comments:

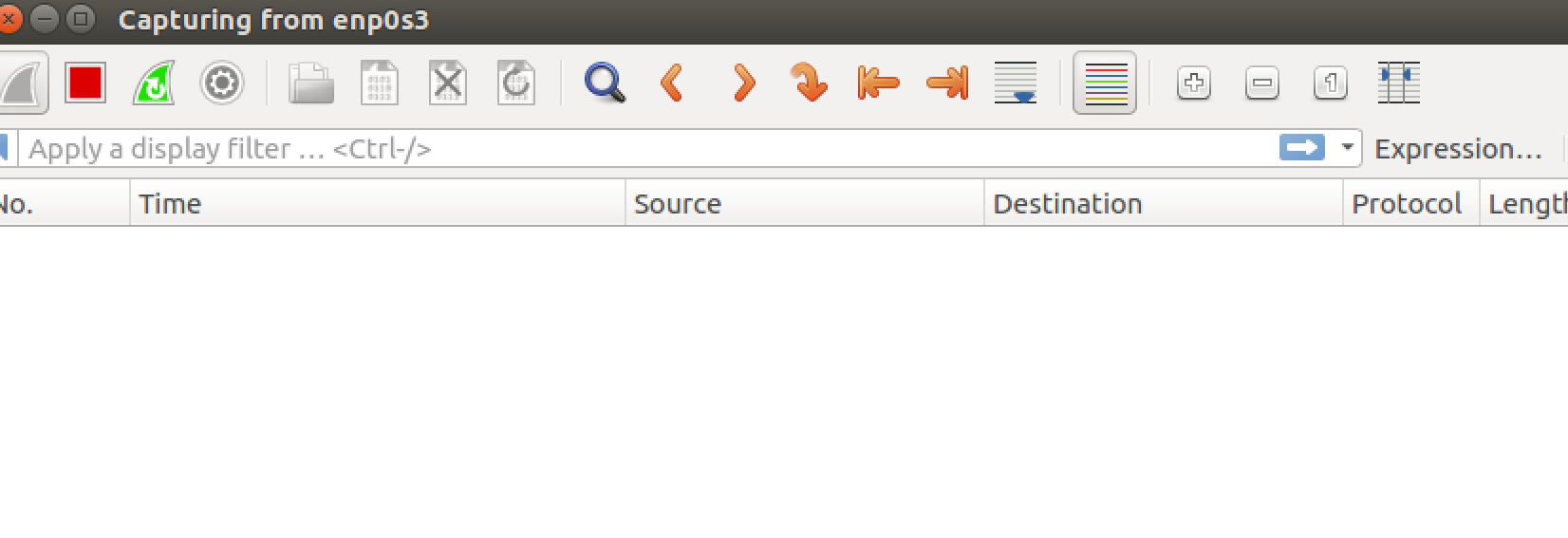
For the ICMP, it was covered in the last task. The tcp connection with the port number 23 worked, and the subnet sniffing worked.

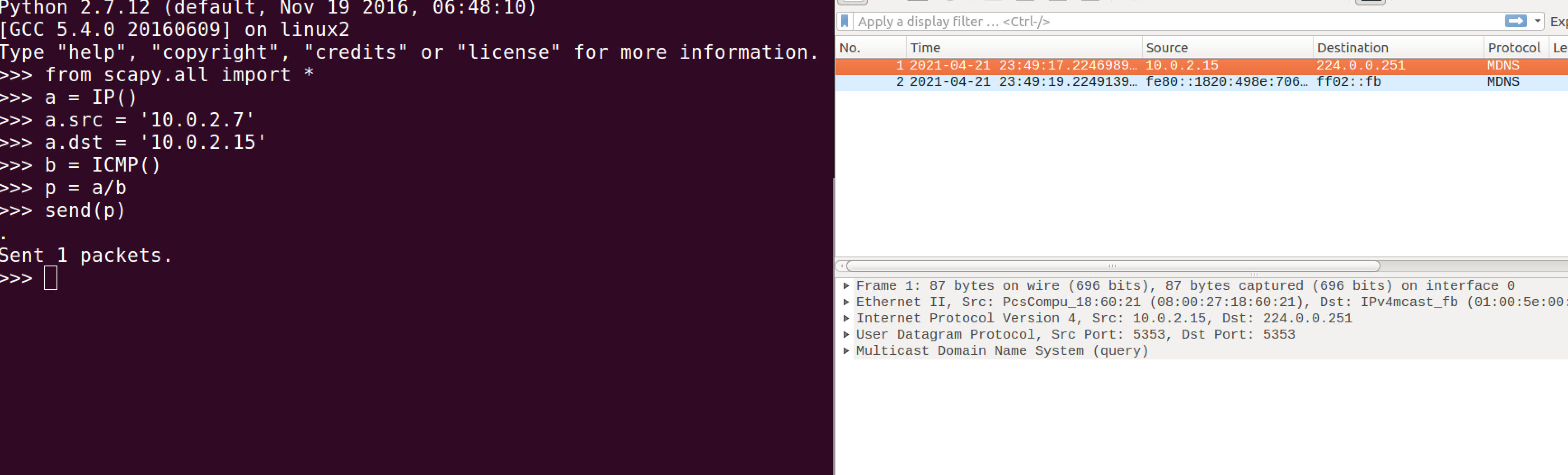
Task 1.2:

Code Used:

Commands and Results:





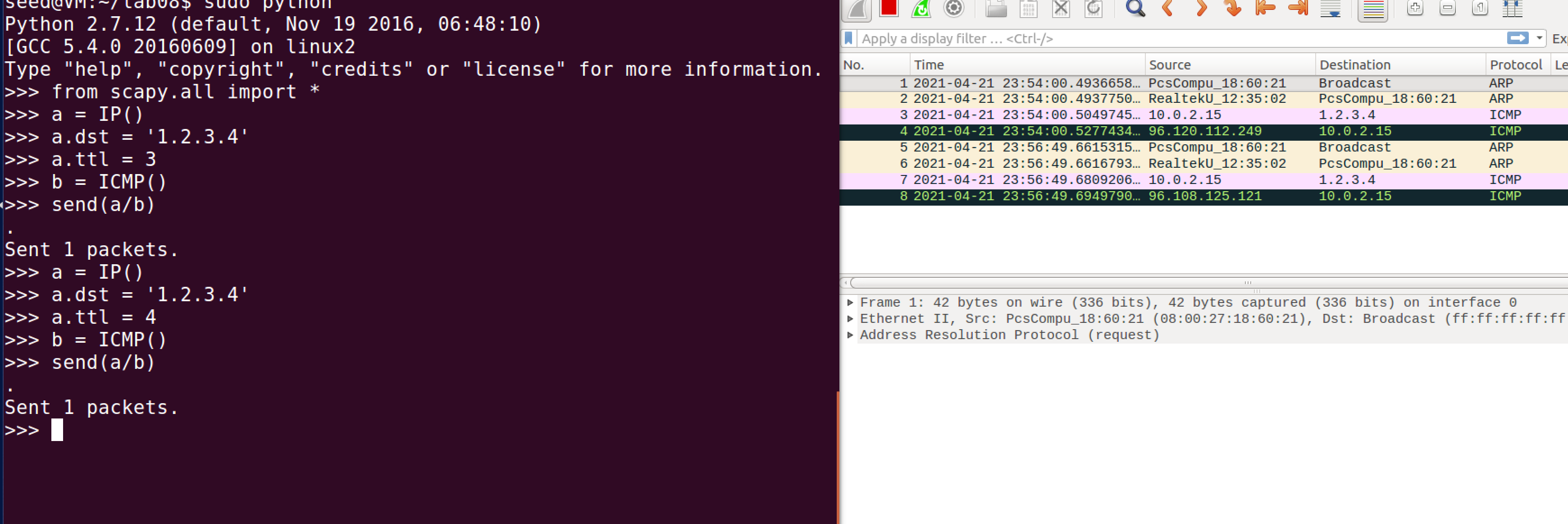


Comments:

Wireshark would not work properly. I don’t think this is correct because it should show that it received the packet and spoofed it. This is how much it would do.

Task 1.3:

Commands and Results:



Comments:

It received the packet from the code from the lab. It keeps changing the source in wireshark whenever the ttl is changed.

Task 1.4:

Code Used:

Commands and Results:

Comments:

I had no clue how to start this or even do this. Sorry