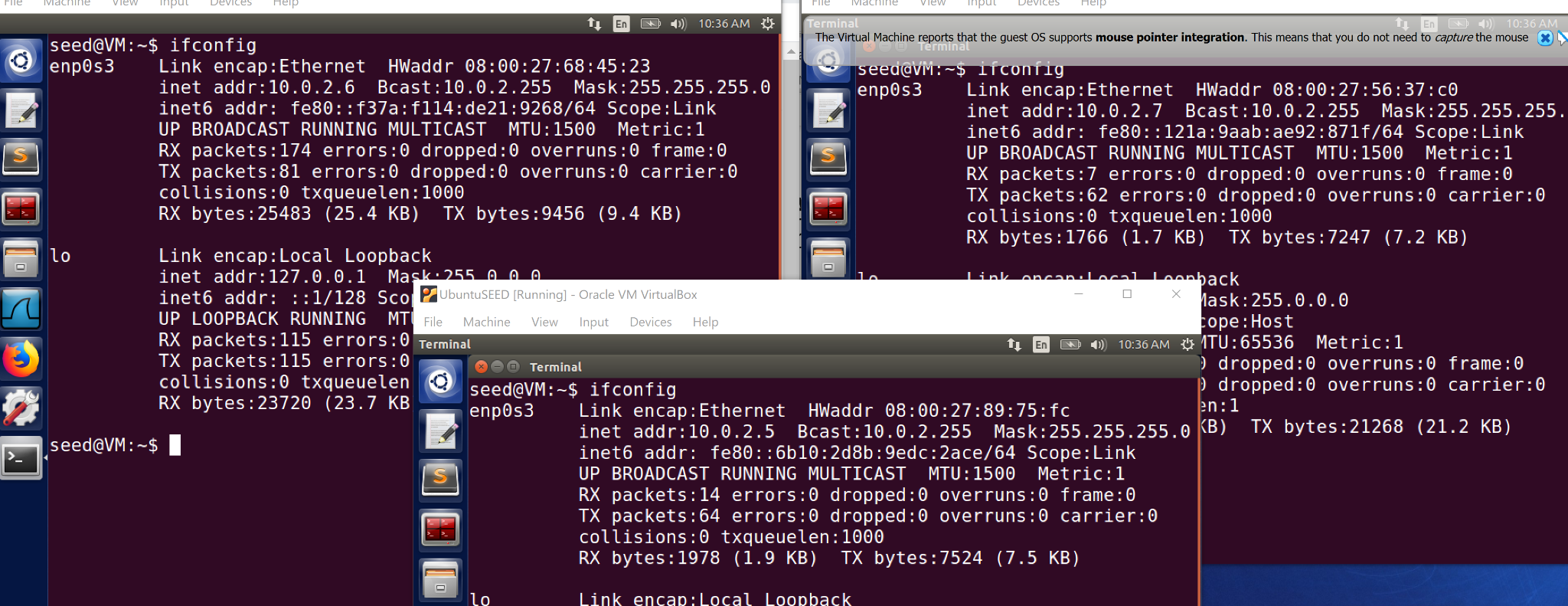
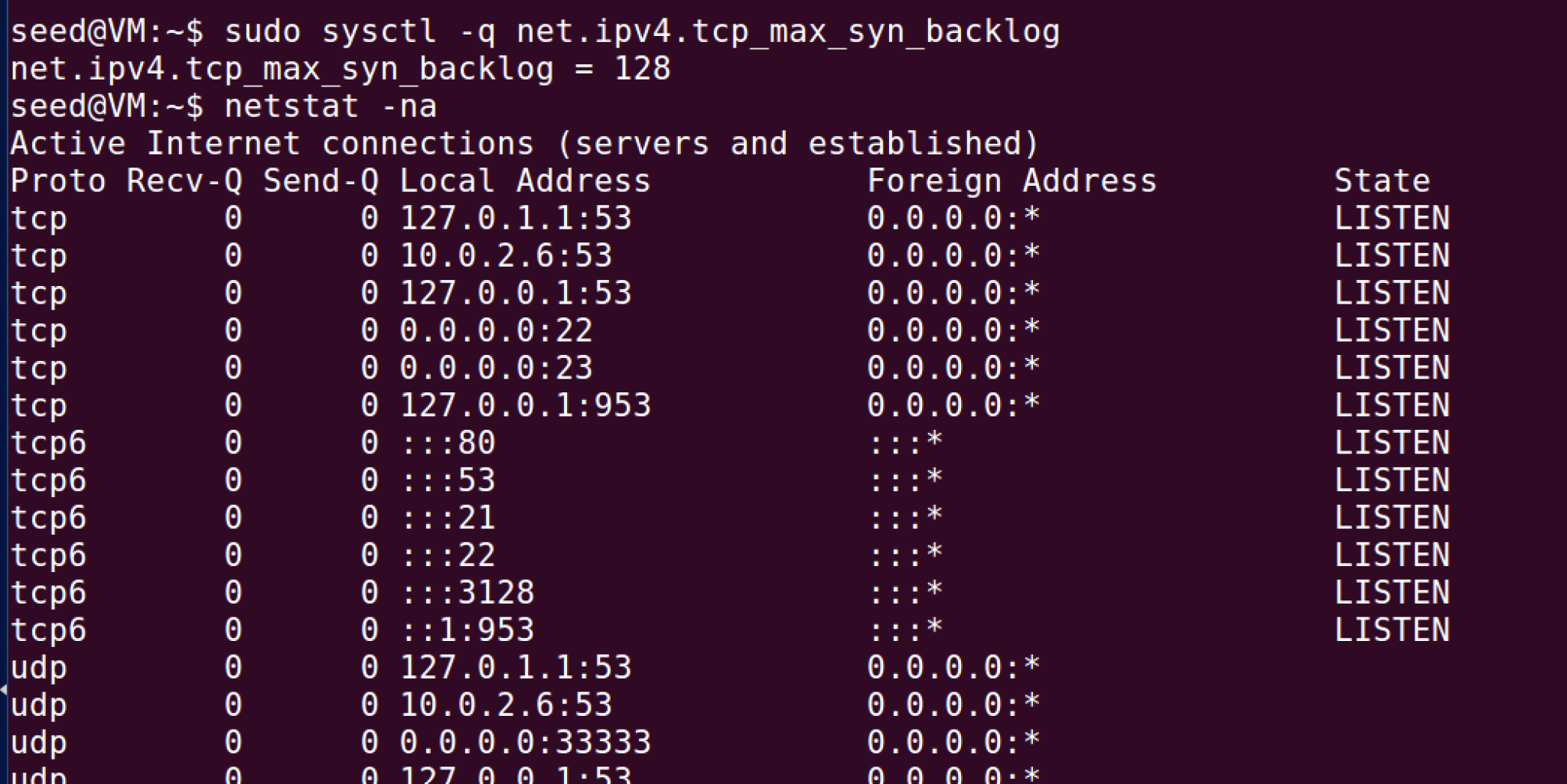
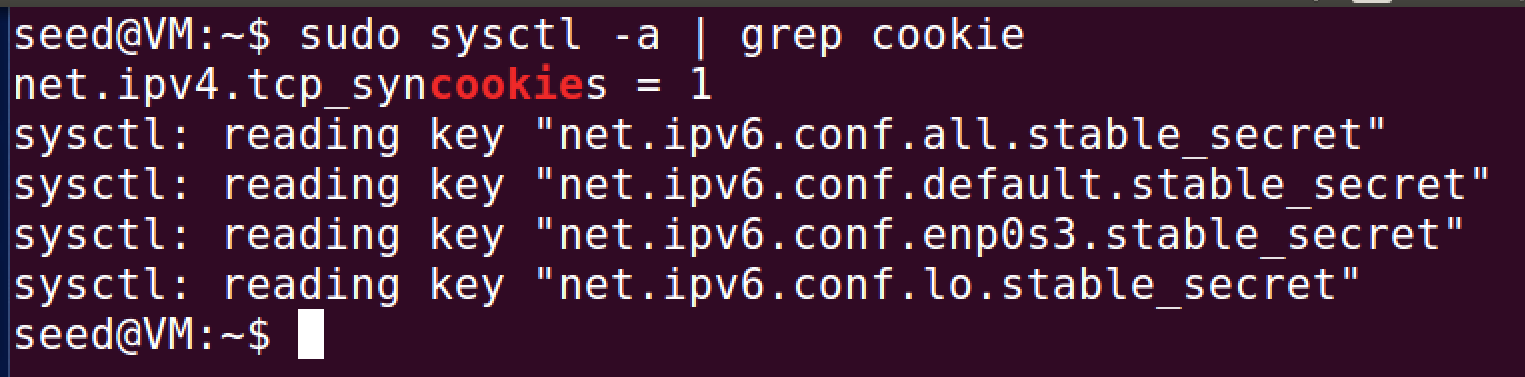
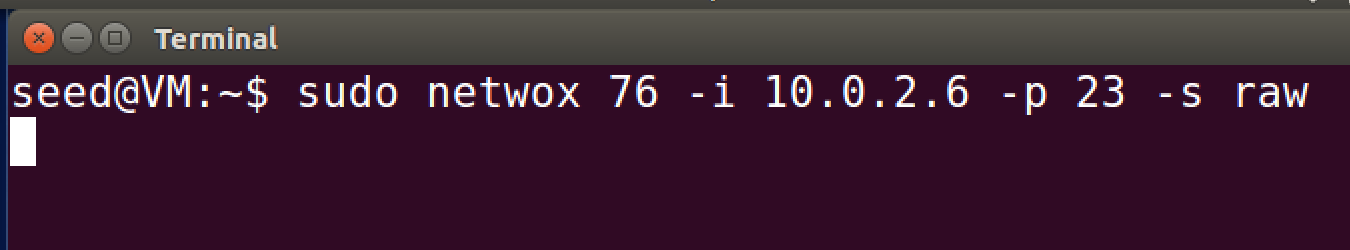
Lab 9

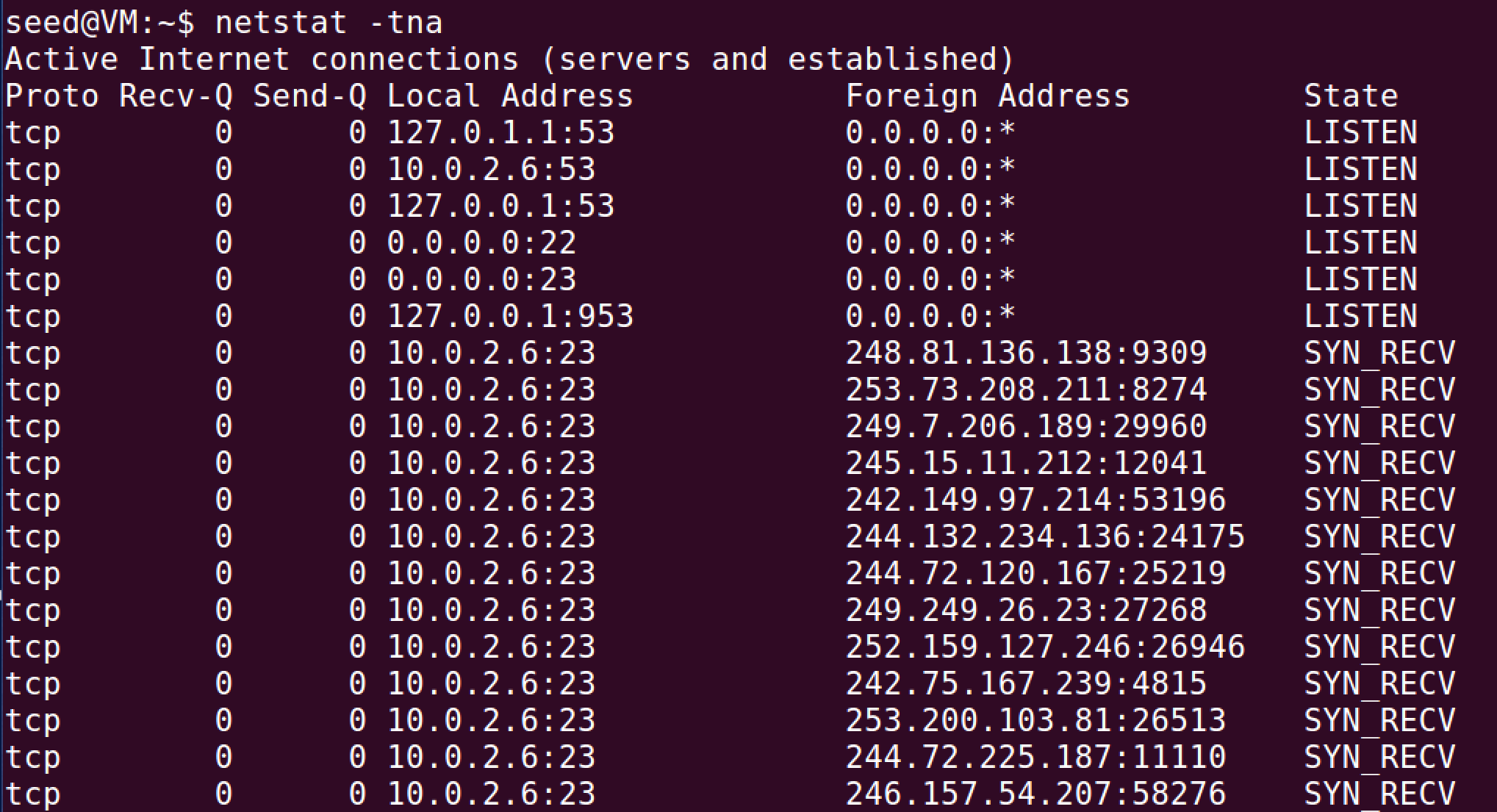
Task 1:

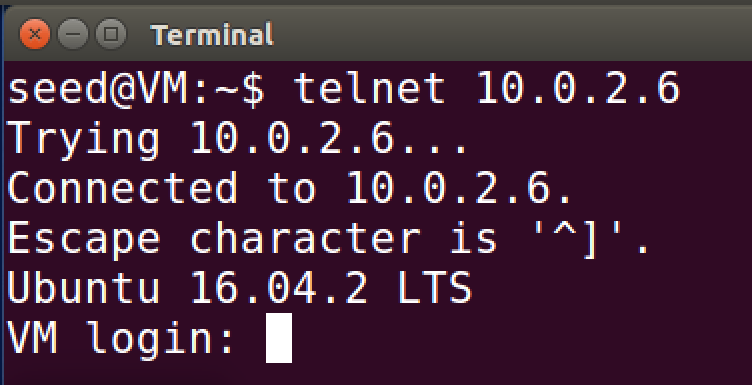






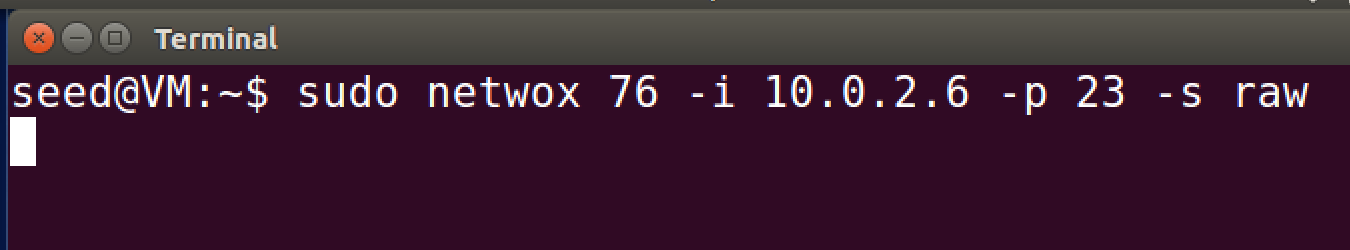


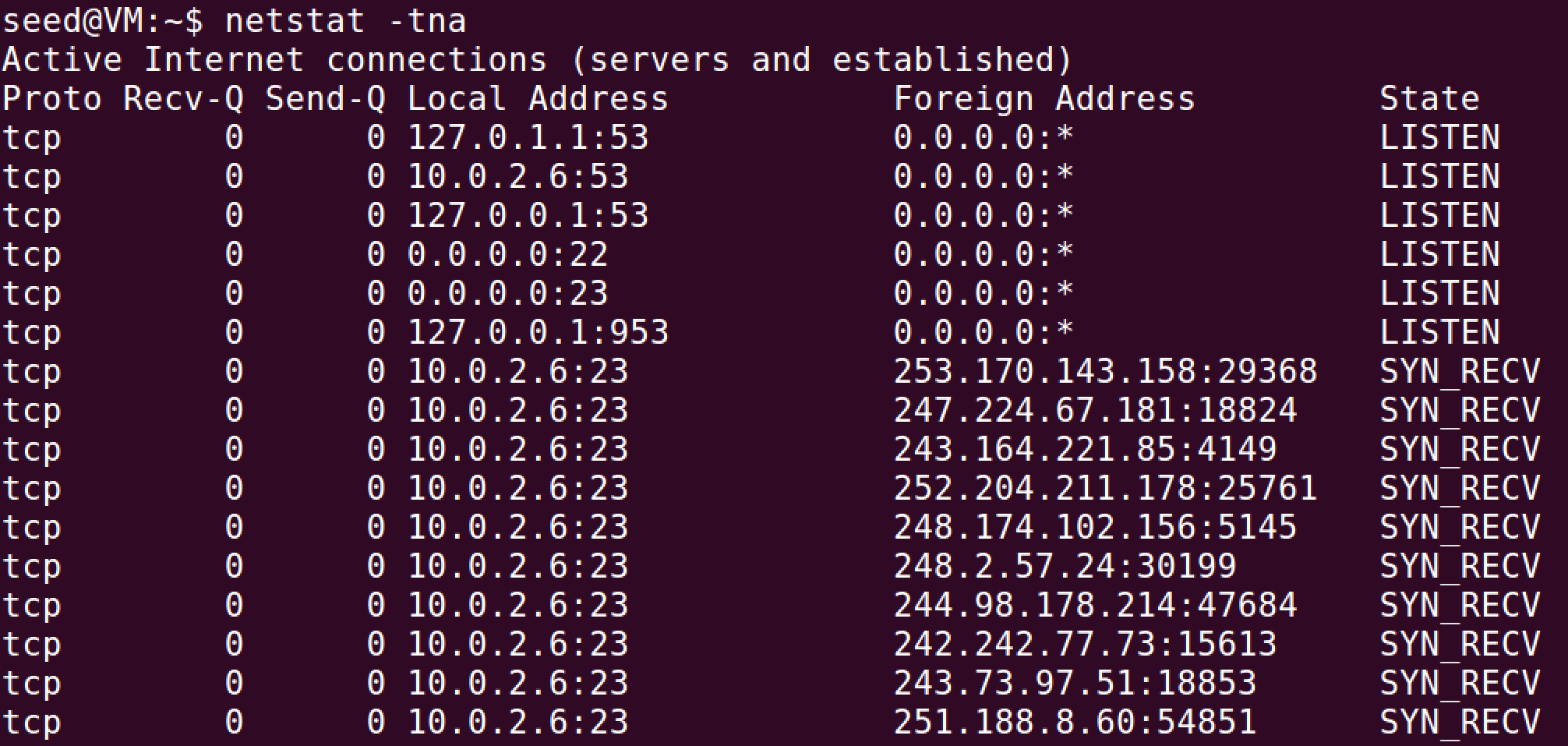


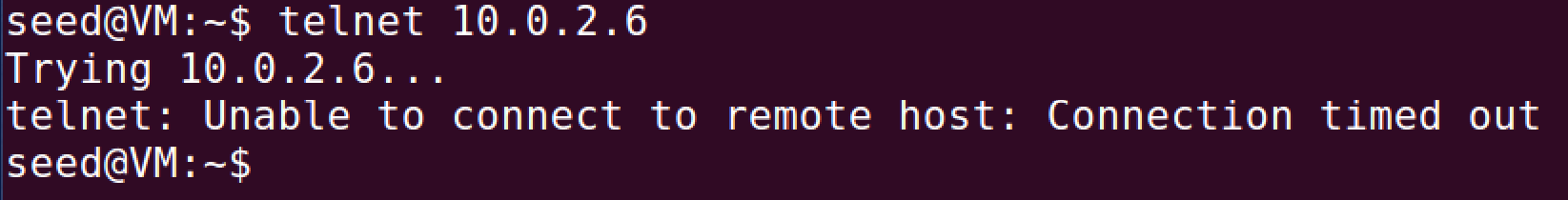


We turn off syncookies by setting it to 0. Then we redo the task.





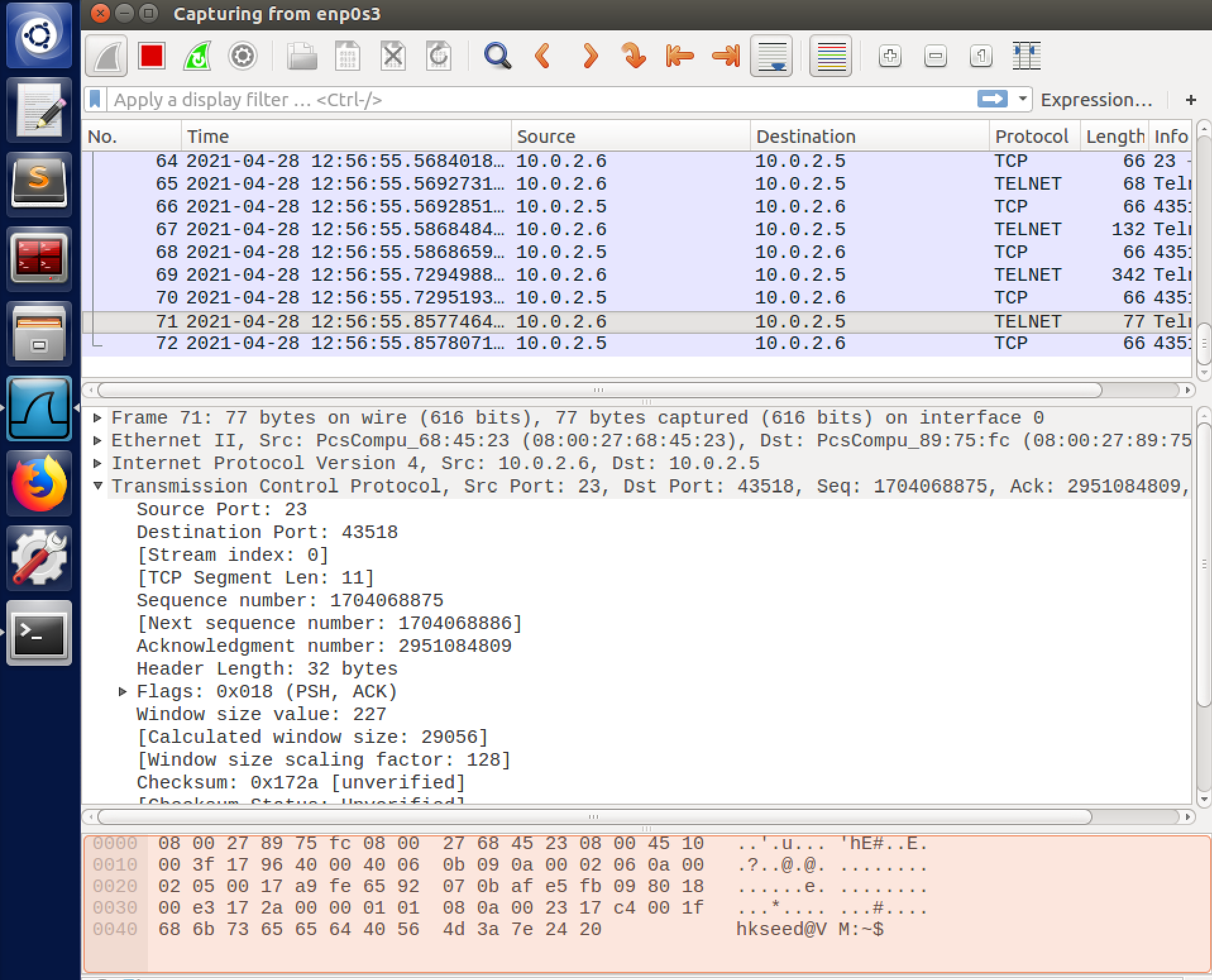


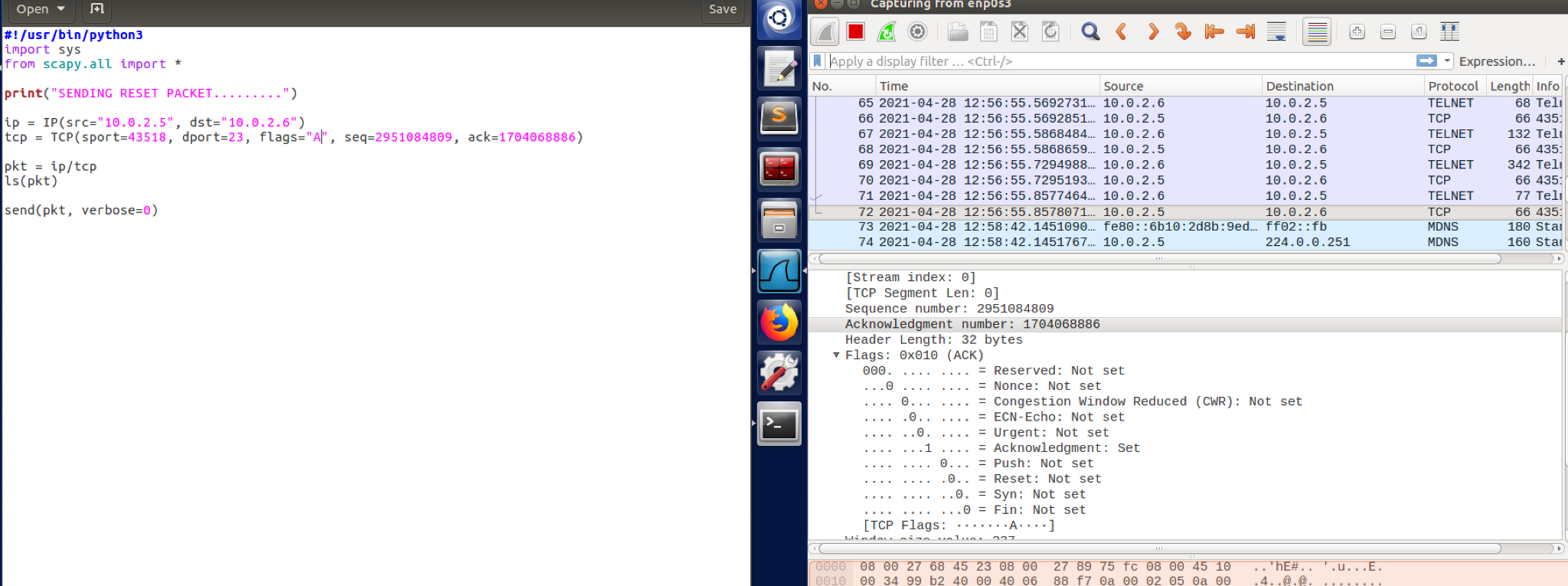


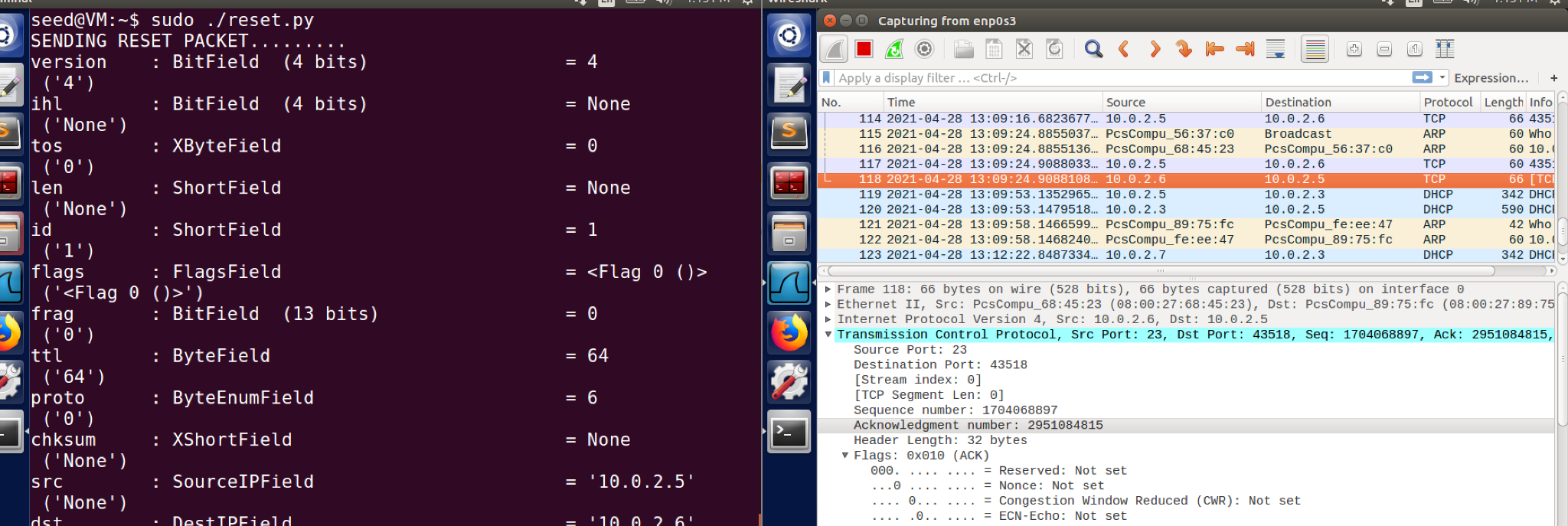
Comments:

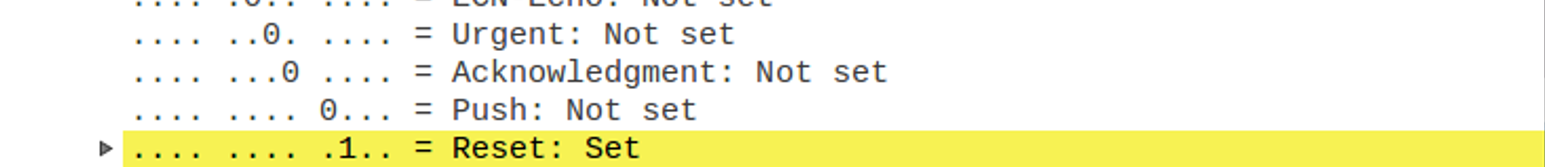
When we test it with the syncookies enabled it still allows us to connect to the server VM because it guards against this kind of attack. When it was disabled it was did not allow connection from the client to the server, further proving that syncookies help protect against this kind of attack.

Task 2:





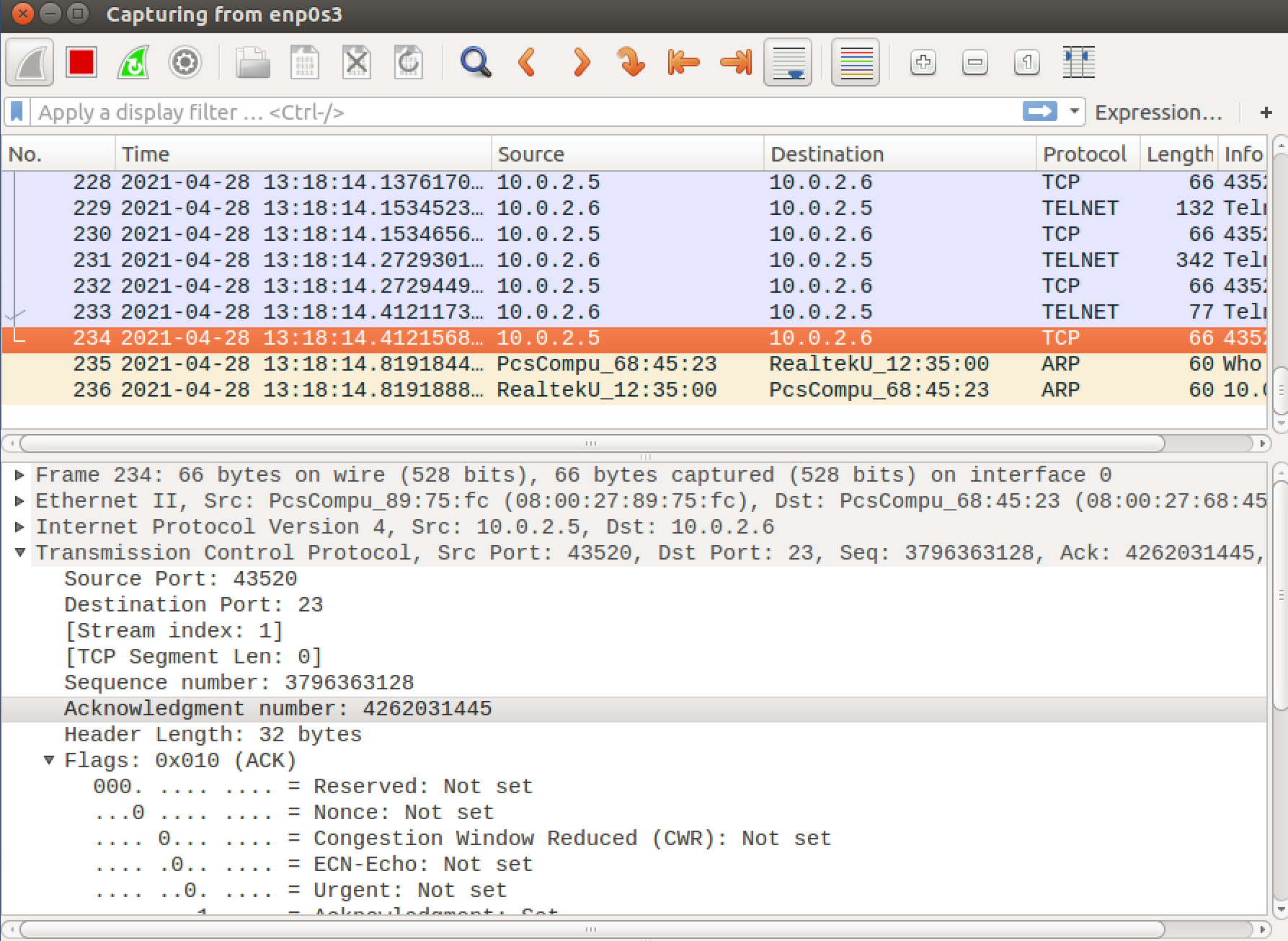


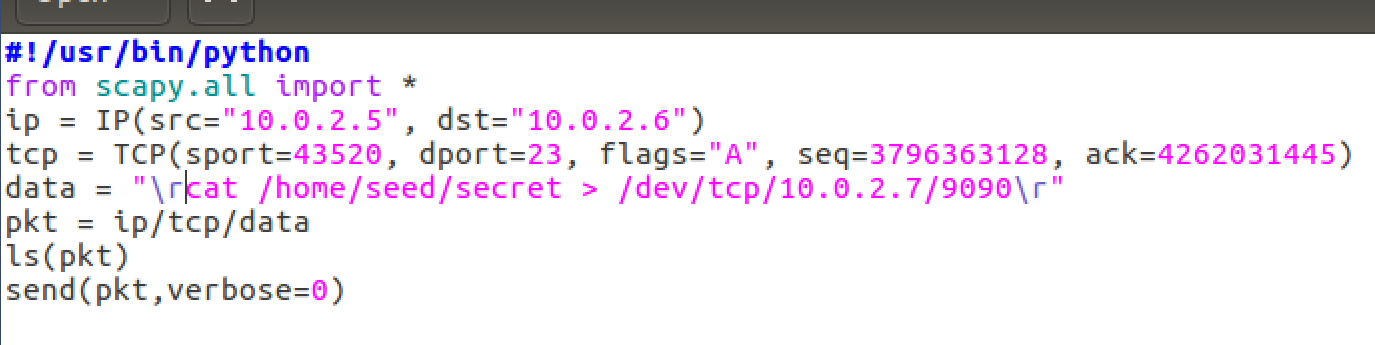


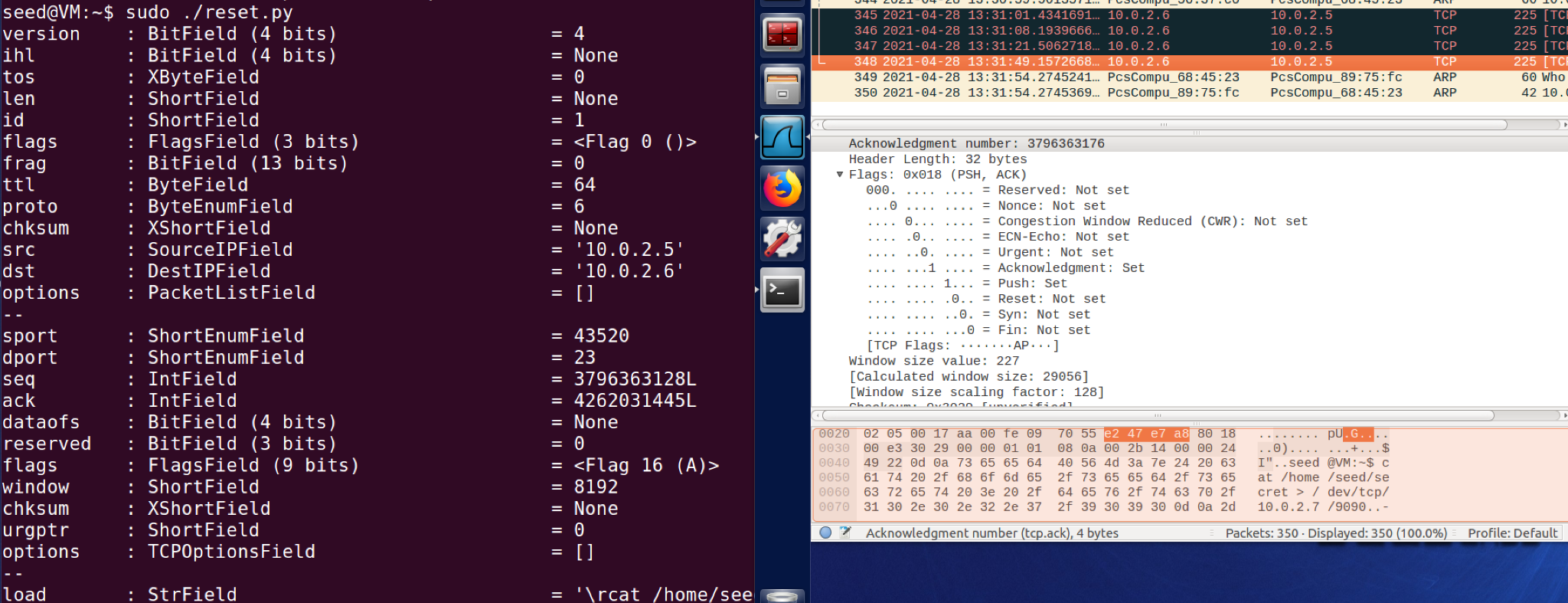
Comments:

So first I had to set the connection between the client and the server and then use the code above to reset the packets that were being sent as shown in the last pic.

Task 4:



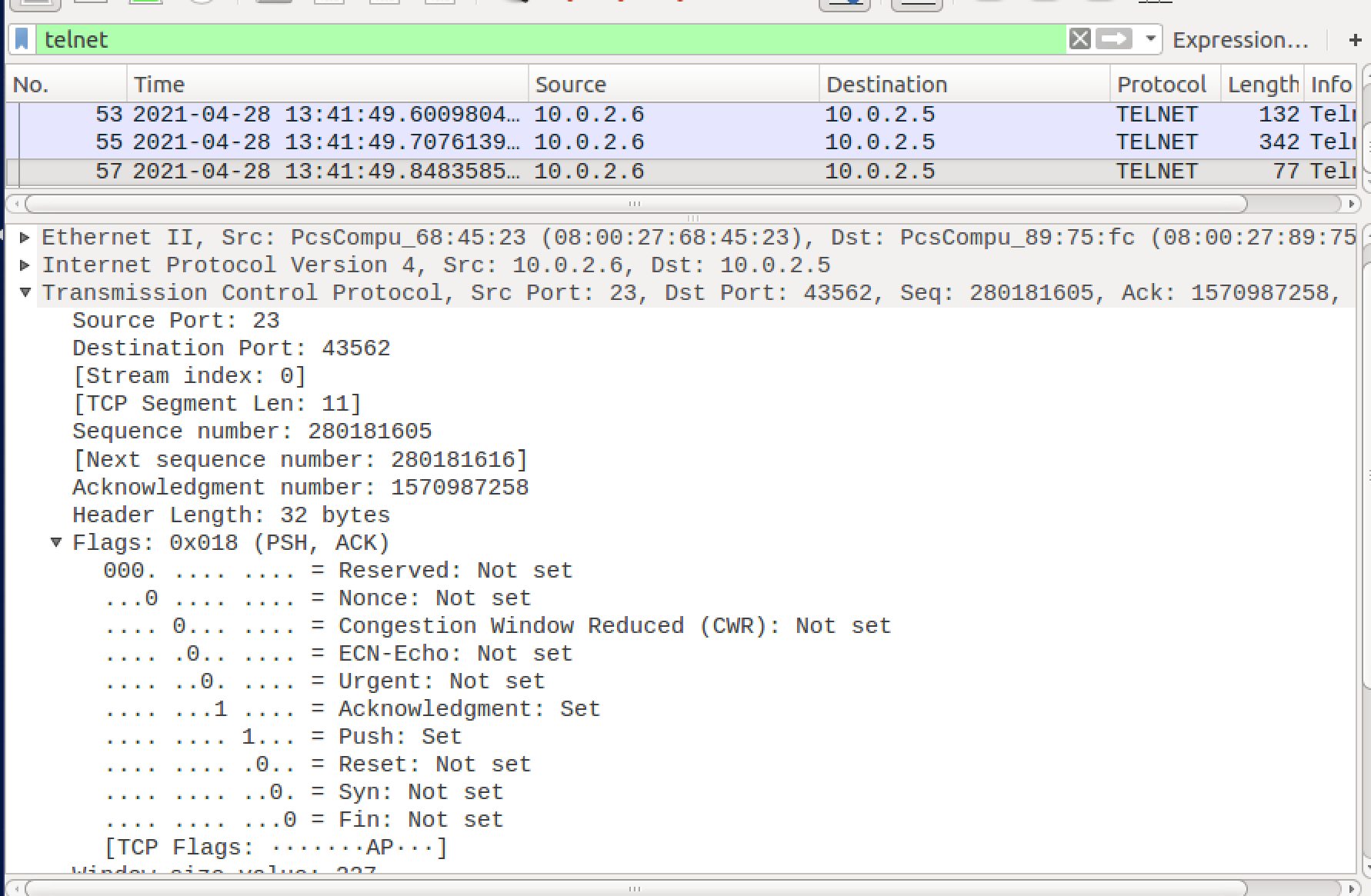


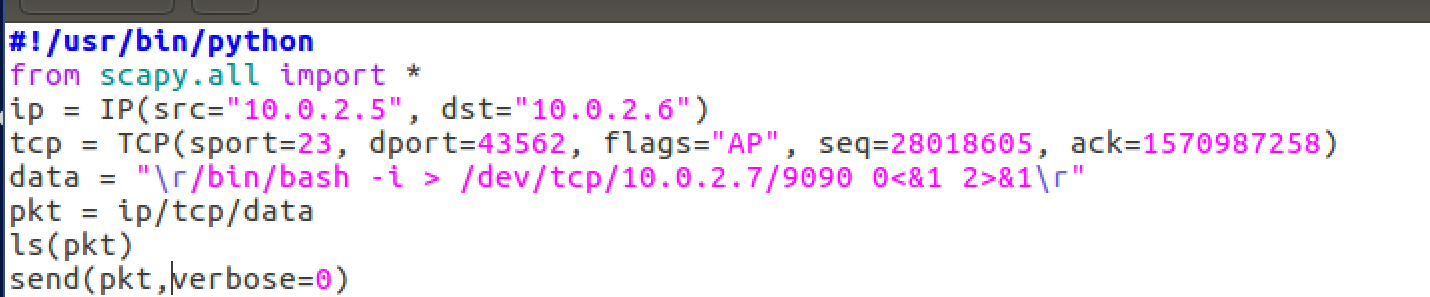


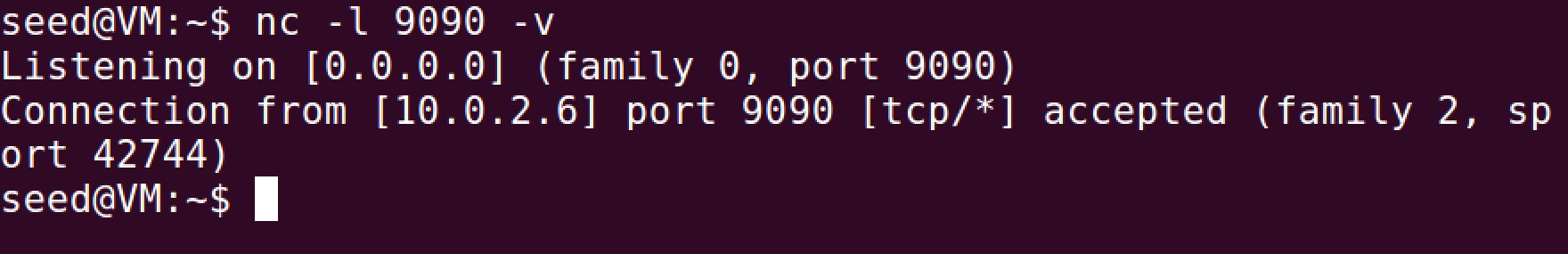
Comments:

First we establish the connection and then get the necessary information to fill into the code. The attacker is listening into the port 9090 so when they run the code it will invoke the server to run the secret program to through the necessary port and allow the attacker to receive said file.

Task 5:







Comment:

With the established connection the code is invoked by the attacker and which runs the reverse shell command to establish the connection through the 9090 port that the attacker is listening in on.