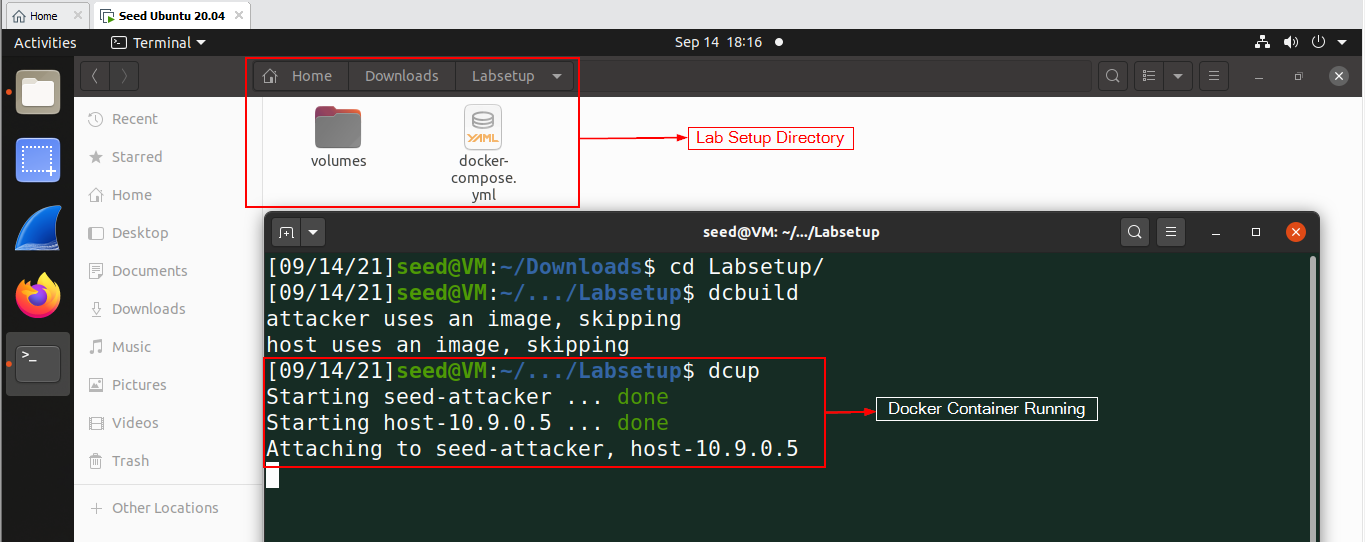
Lab 2 Report - Packet Sniffing and Spoofing Lab

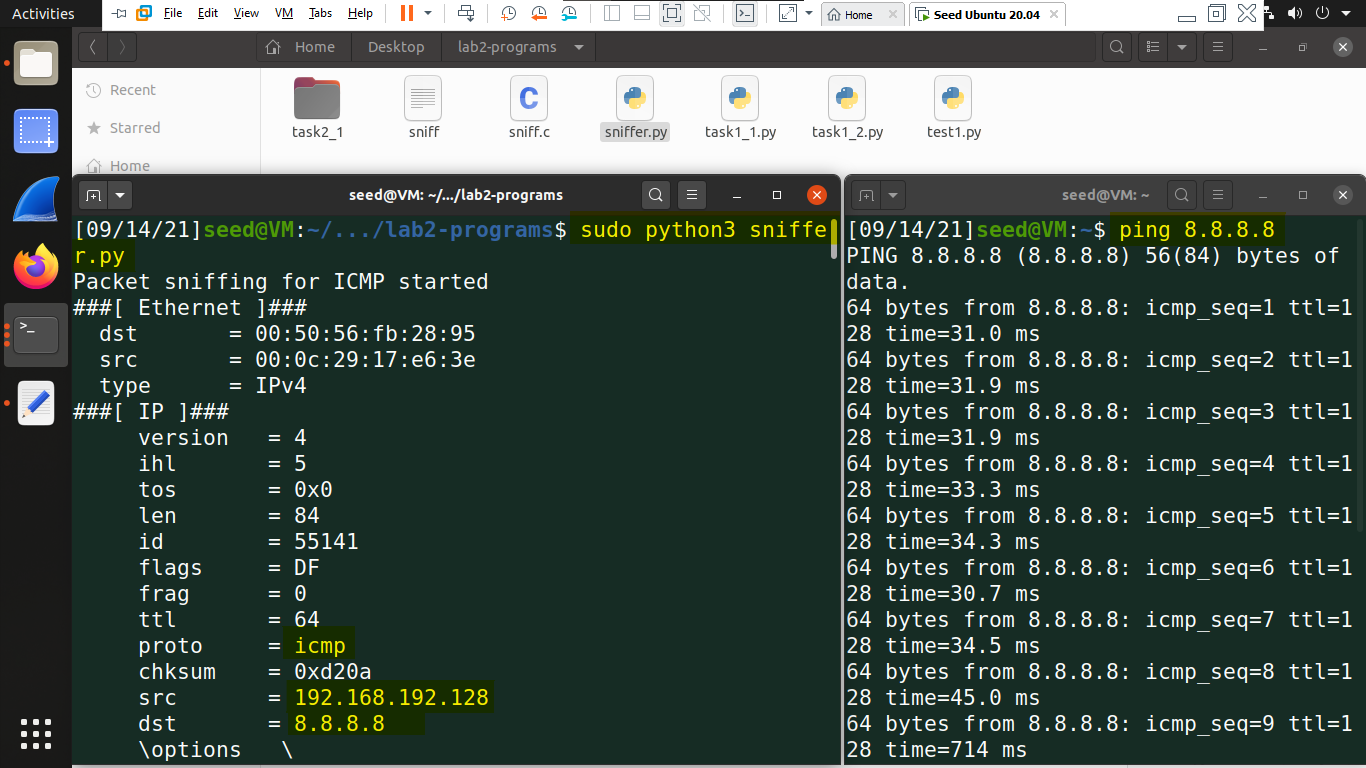
**Name: Shrikant Kale - #700727822**

1. **Task 1.1A: Lab Environment Setup**

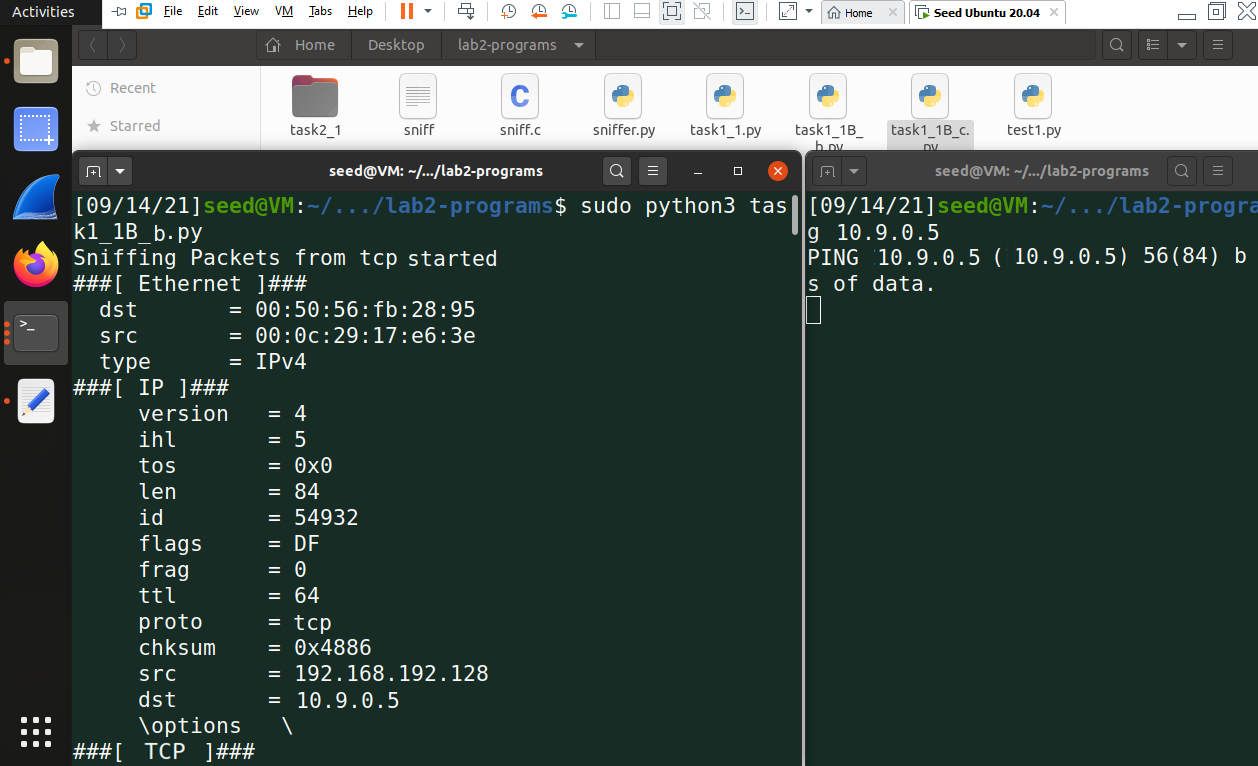
* Created Lab environment using docker containers.
* To execute docker container, I have used docker-compose commands.
  + dcbuild (docker-compose build) – to build the docker container image
  + dcup (docker-compose up) – to run the docker container
  + dcdown (docker-compose down) – to shut down the container

****

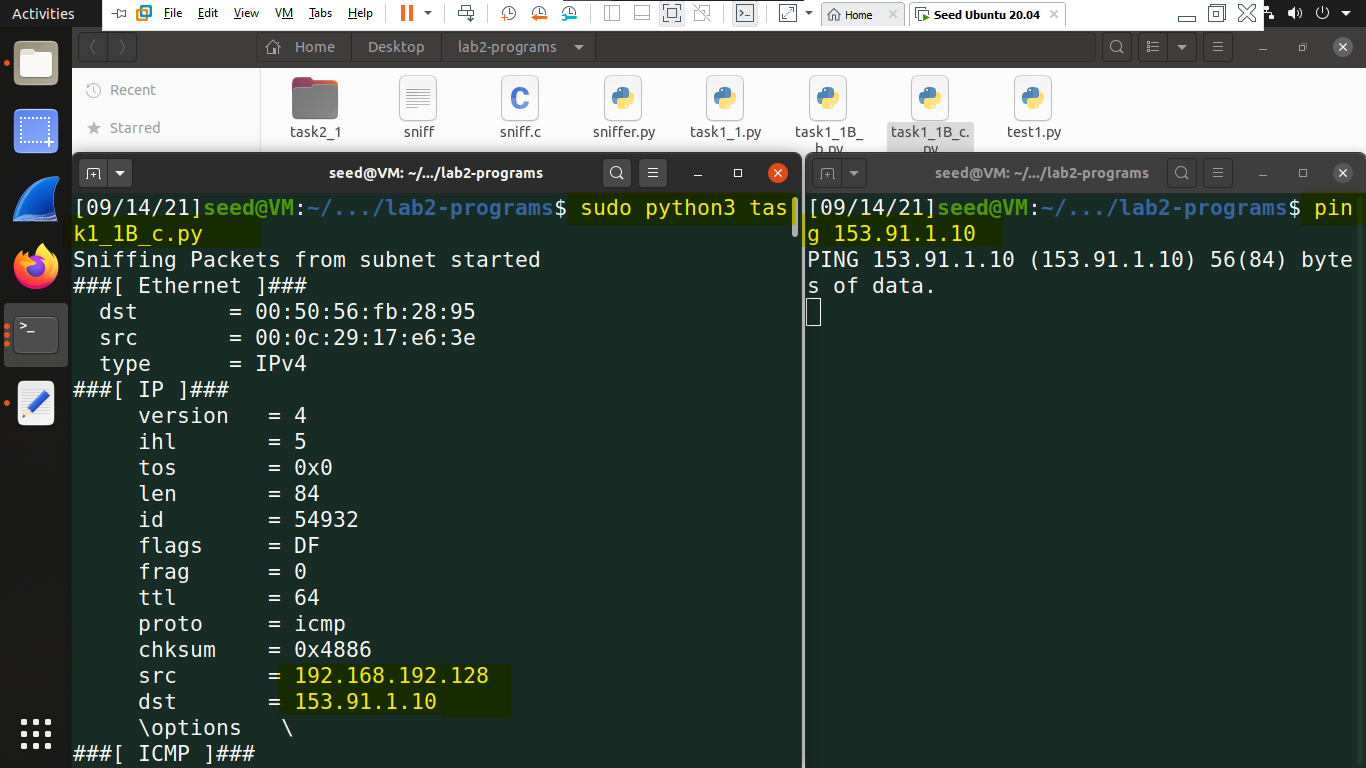
1. **Task 1.1B:** 
   * Capture only the ICMP packet – after setting the filter on your sniff program, try to ping 8.8.8.8
   * Set filter to capture/sniff ICMP packets using python program



* + Capture any TCP packet that comes from a particular IP and with a destination port number 23 – after setting the filter on your sniff program, try to telnet from your host VM to the victim at 10.9.0.5.
  + Captured TCP packets



* + Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16; you should not pick the subnet that your VM is attached to – you can use 153.91.1.0/24 - the subnet belongs to UCM and ping UCM’s web server at 153.91.1.10 after setting the filter on your sniff program
  + Op



1. **Task 2.1A**: On the Host VM (attacker), open Firefox and surf to the Blackboard. Download sniff.c. You only need to modify one line of code based on your VM’s NIC. Compile and run the sniff program using super user privilege. Open another terminal on the Attacker VM and ping 8.8.8.8. You should see the source IP, destination IP and protocol information printed by the sniff program.

* Done sniffing with c programs and printed source and destination.

