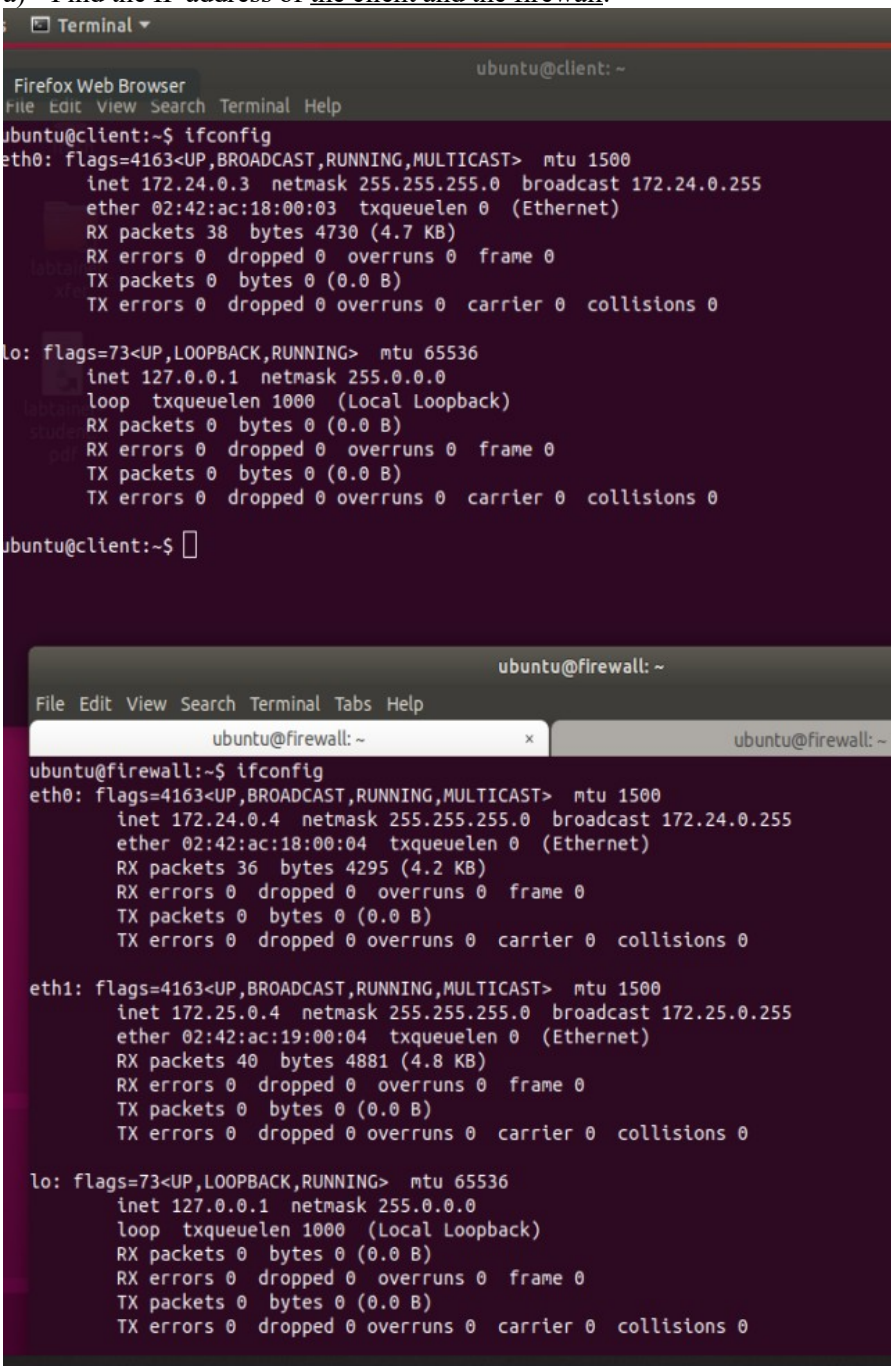
Homework 4 – Linux Firewall

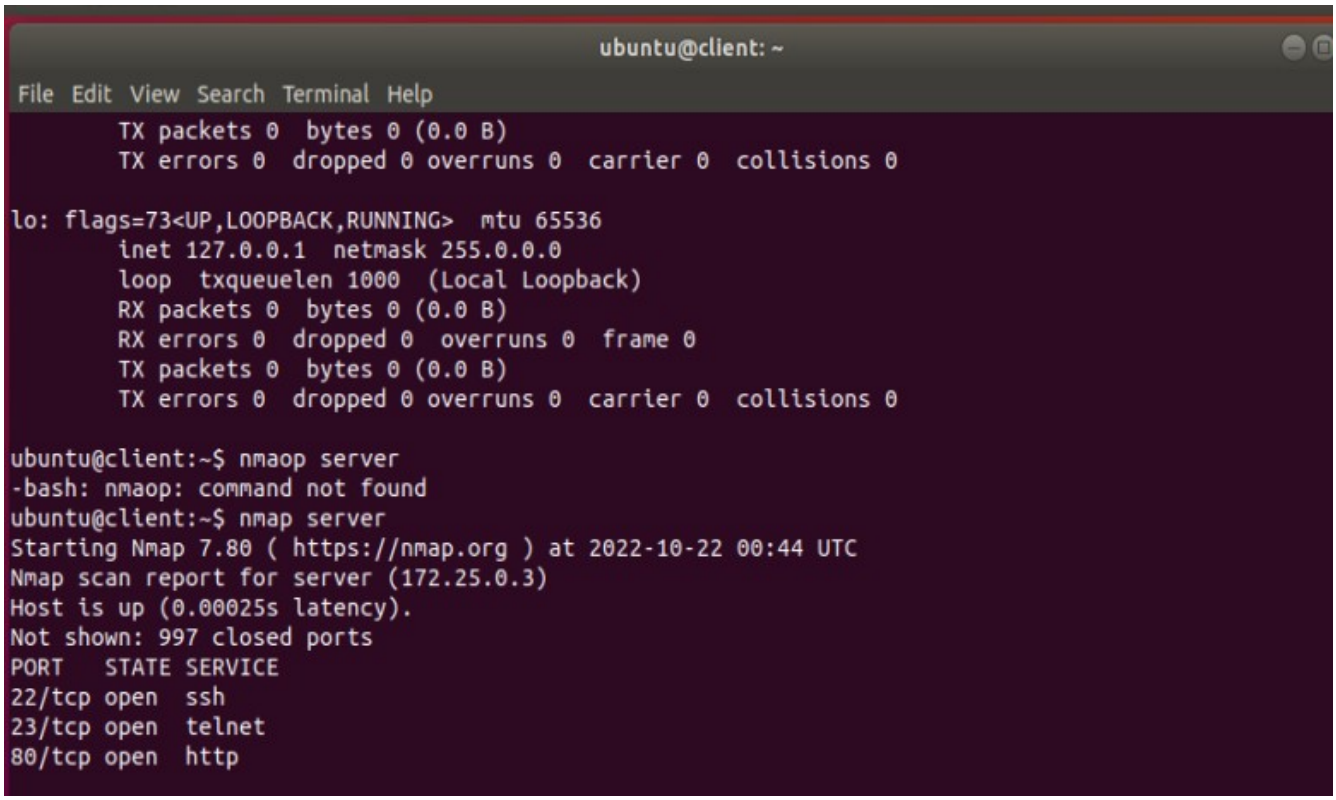
Task 1. Find IP addresses

a) Find the IP address of the client and the firewall.

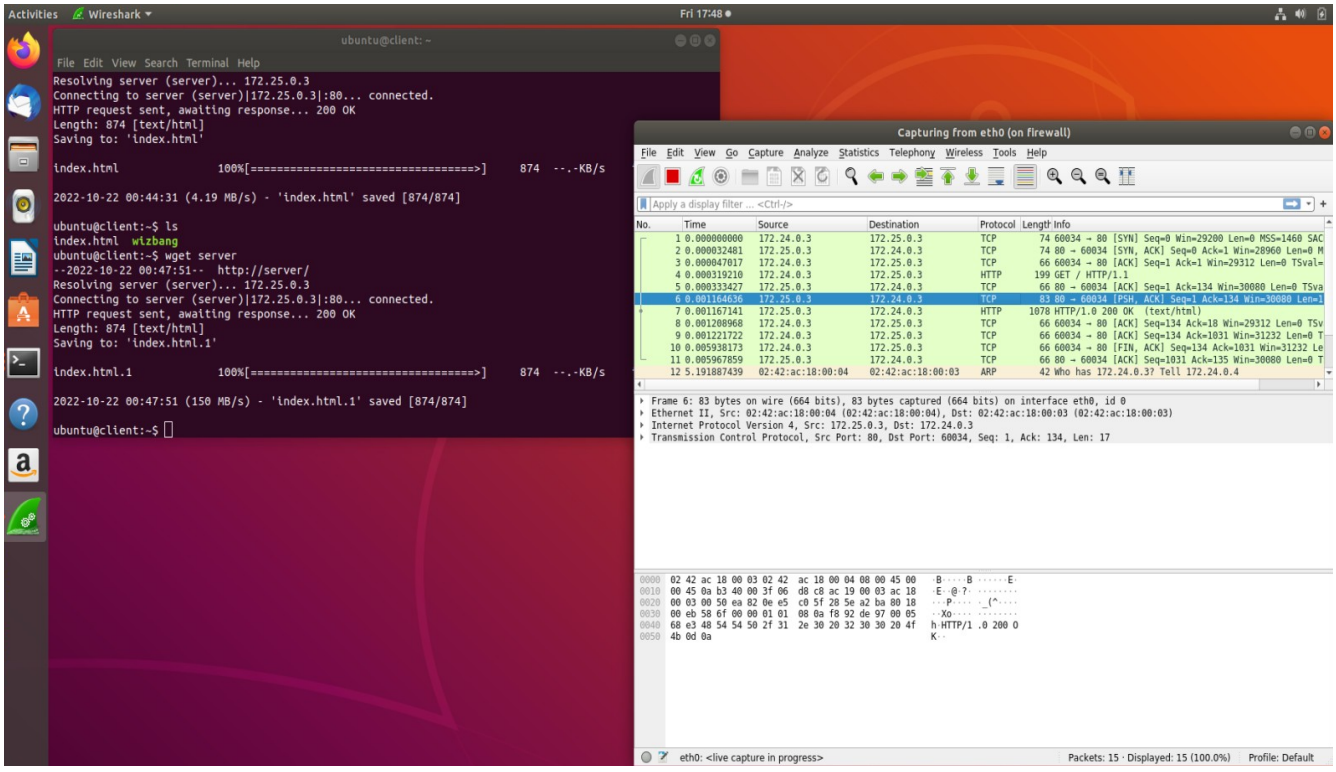


Task 2. Nmap scan

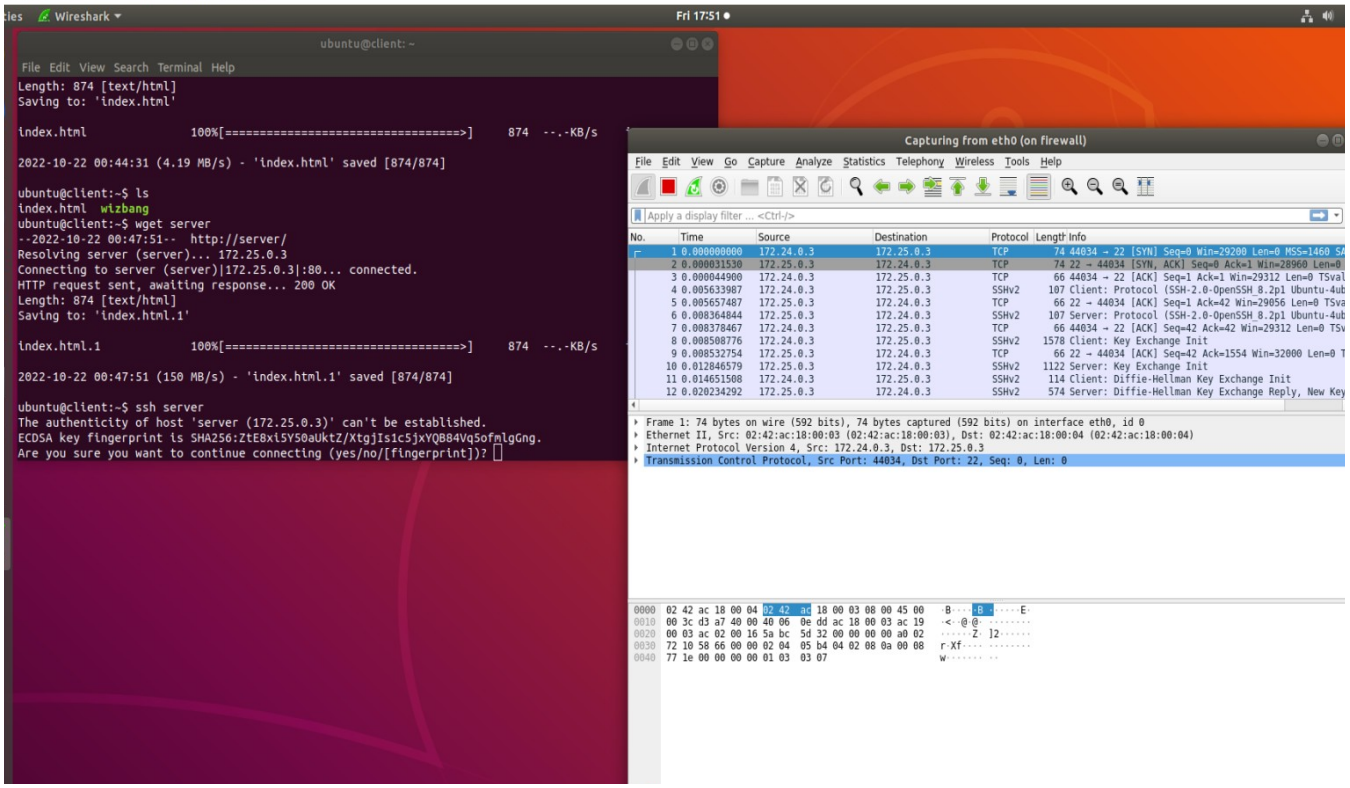
a) Perform a nmap scan on the client for open ports on the server. Show the output in a screenshot.



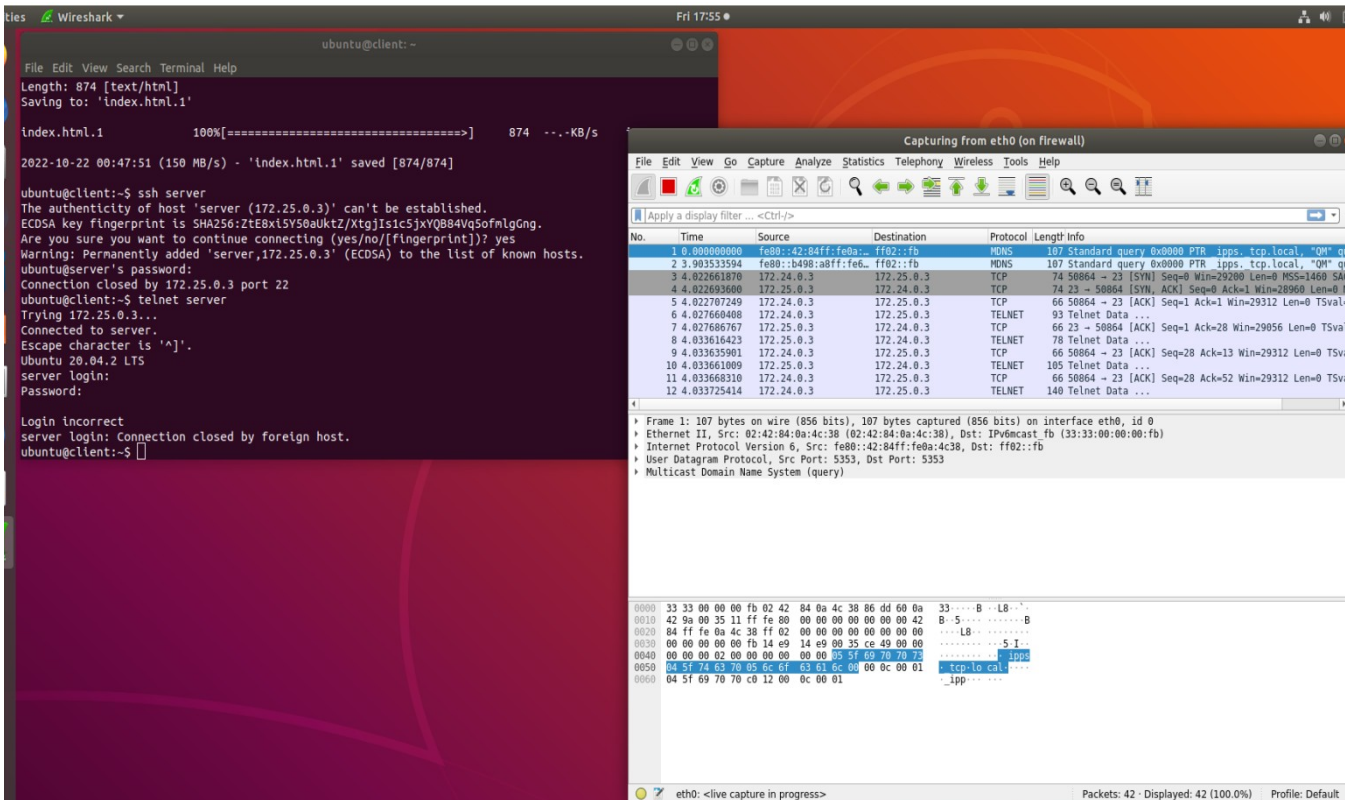
b) Run *wget* and report captured packets on wireshark in a screenshot. To capture packets for a new command, you need to stop/start capturing without exiting wireshark.



c) Run *ssh* and report captured packets on wireshark in a screenshot.

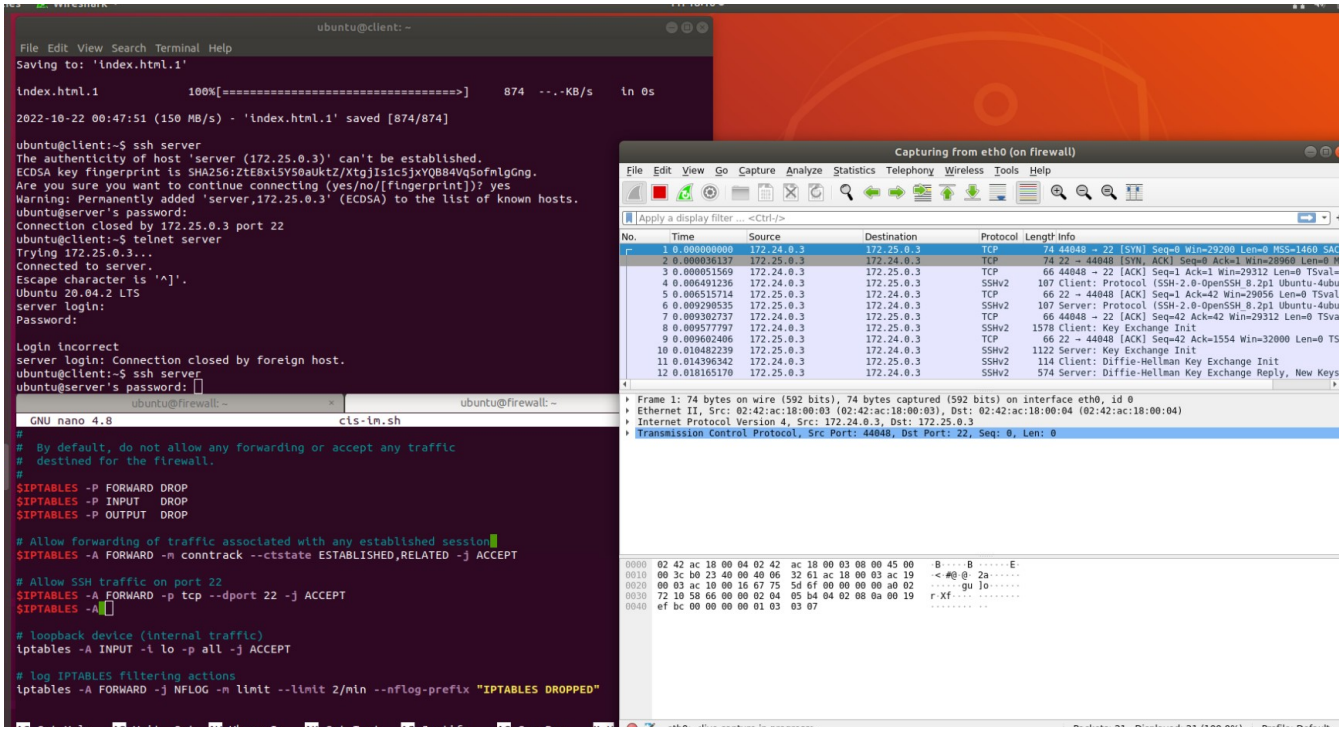


d) Run *telnet* and report captured packets on wireshark in a screenshot.

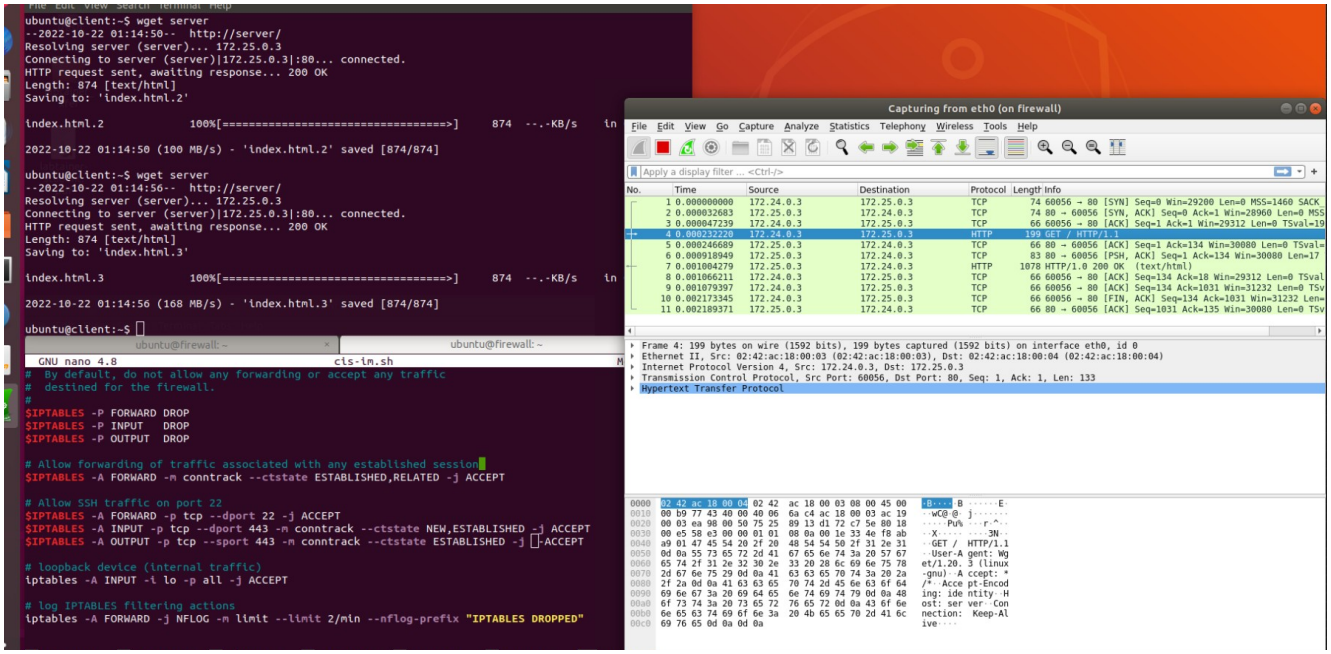


Task 3. Use iptables to limit traffic to the server

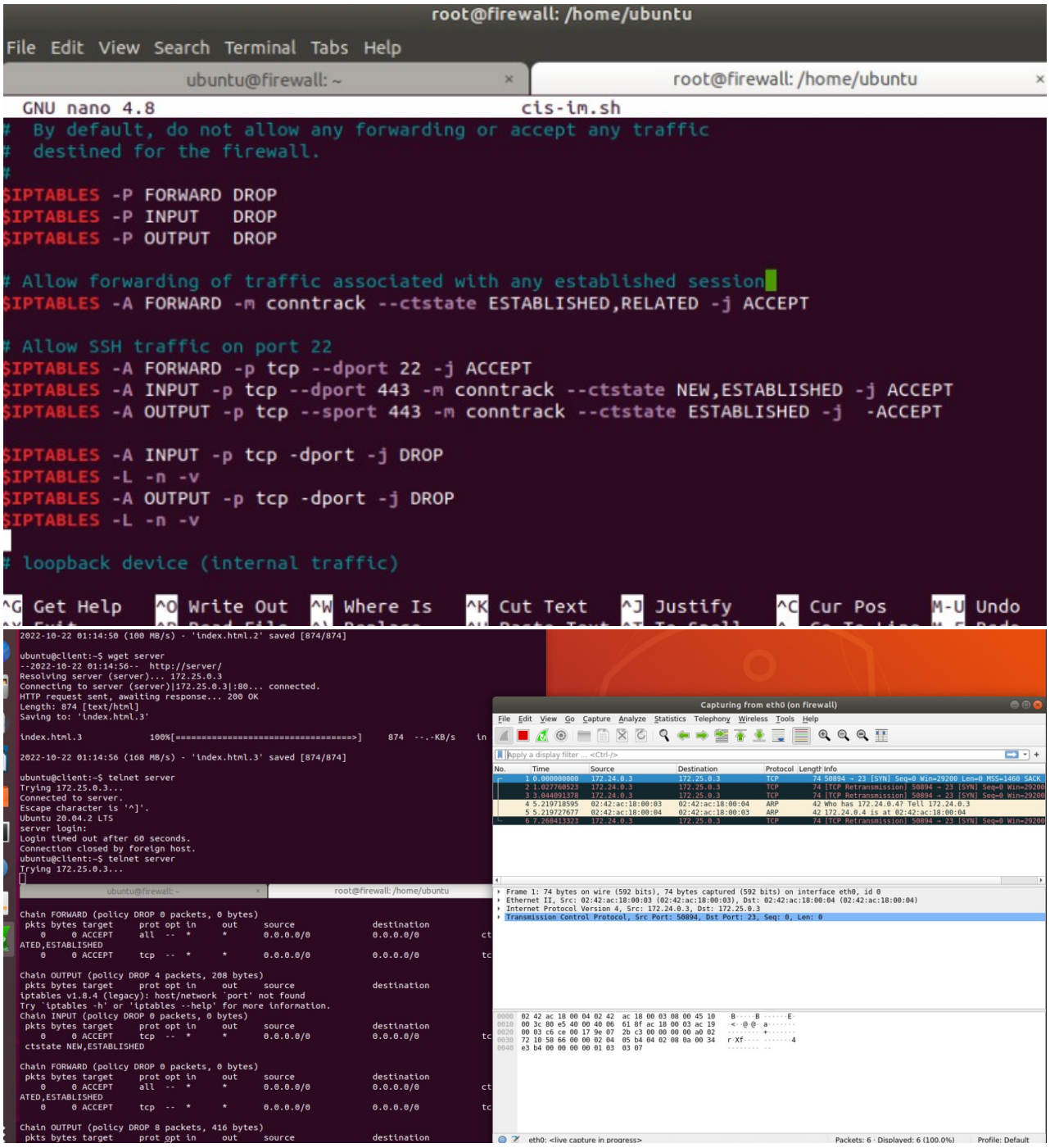
a) Show that ssh traffic is allowed. On the client, run ssh while capturing traffic on the firewall. Report these two activities in two screenshots. Explain how you know ssh traffic is allowed.



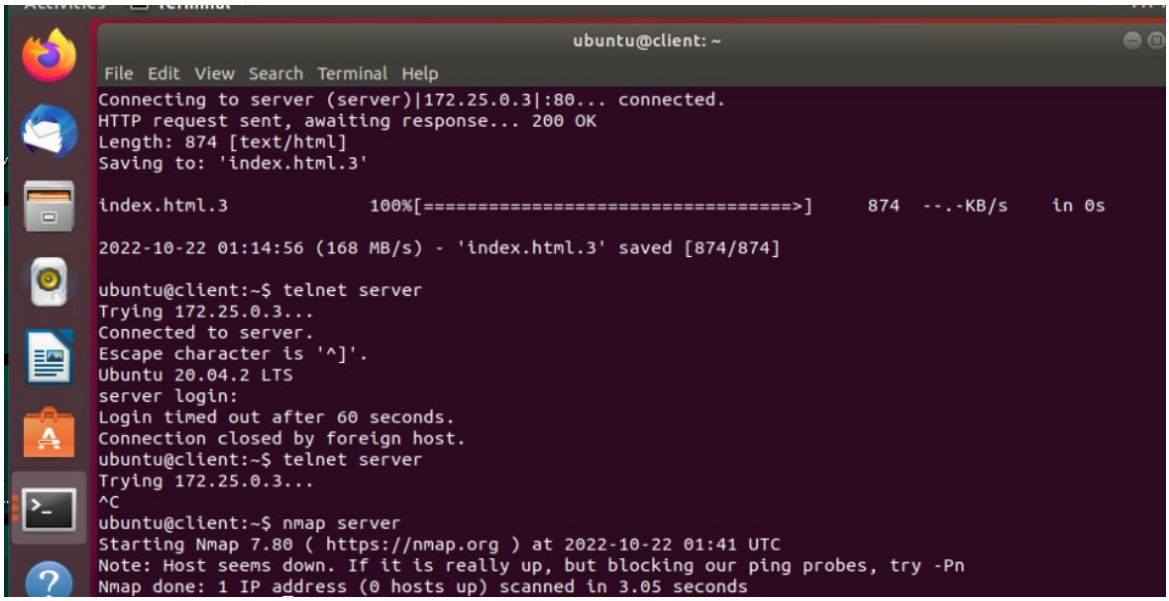
b) Show that HTTP traffic is allowed. Report the same as you did for ssh traffic.



c) Show that telnet traffic is blocked. Report the same as you did for ssh traffic.

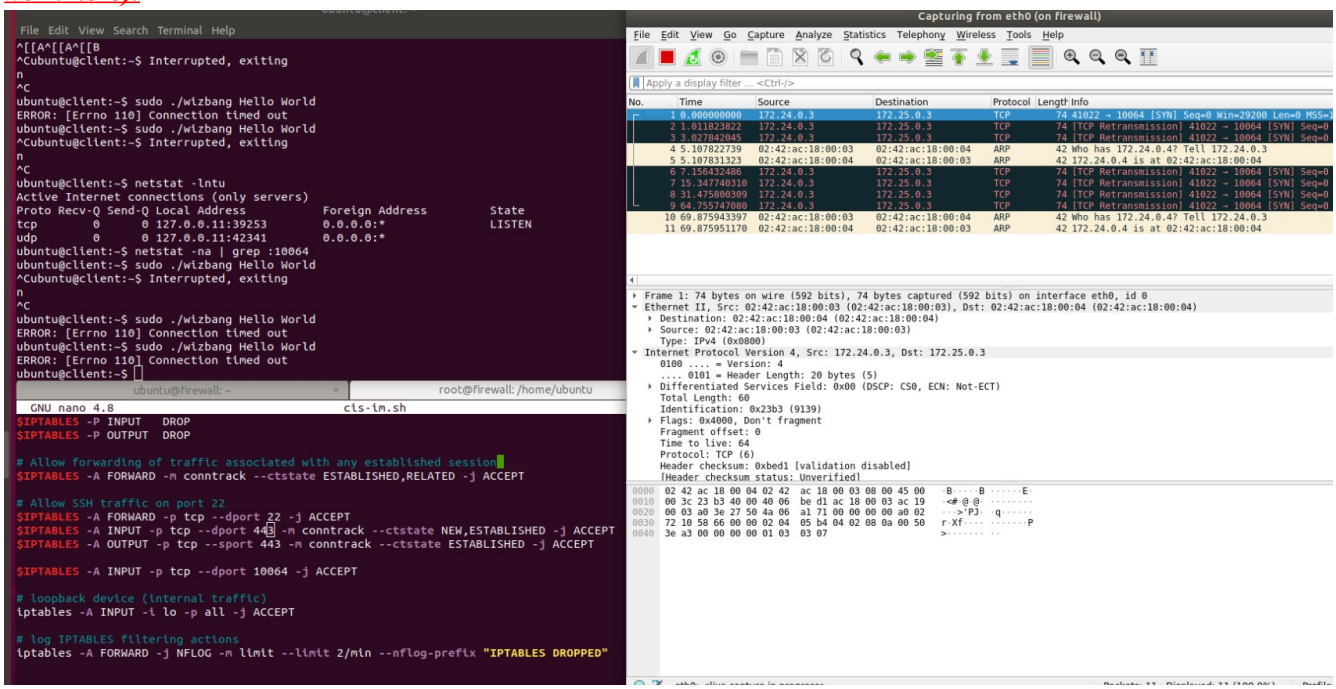


d) At the end, perform a nmap scan on the client for open ports on the server. Show the output in a screenshot. Said the server was down??? (Not sure if that's correct or not from my last rules created for blocking telnet)



Task 4. Open a new service port

a) Show that wizbang traffic is allowed. On the client, run wizbang while capturing traffic on the firewall. Report these two activities in two screenshots. Explain how you know wizbang traffic is allowed. ***I tried to make a rule that opened the port 10064 that it showed on wireshark for the TCP protocol., It wasn't working though. I tried a couple other times to get the port to open but I was still unsuccessful. Not sure what else to do to open the port but I at least wanted to show my attempted work here).***



b) At the end, perform a nmap scan on the client for open ports on the server.

- ***I ran the nmap scan but it came back as "server being down" in the output. I instead ran a netstat scan to show what ports were open, as stated before, I was unsuccessful in opening port 10064 for the wizbang portion of question 4 but I still wanted to shoe my work.***