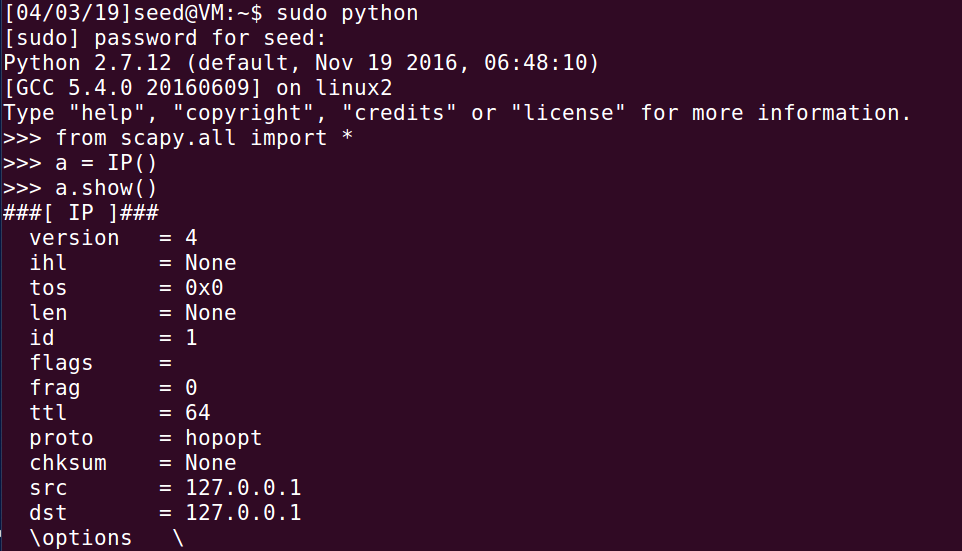
**Packet Sniffing and Spoofing Lab**

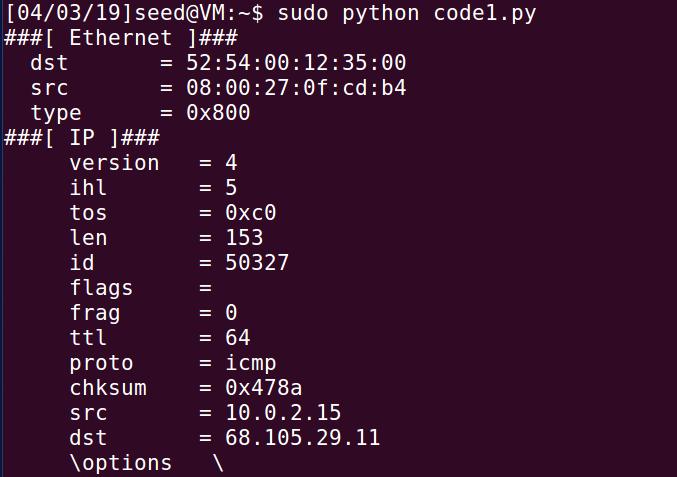
**Lab Task Set 1: Using Tools to Sniff and Spoof Packets**

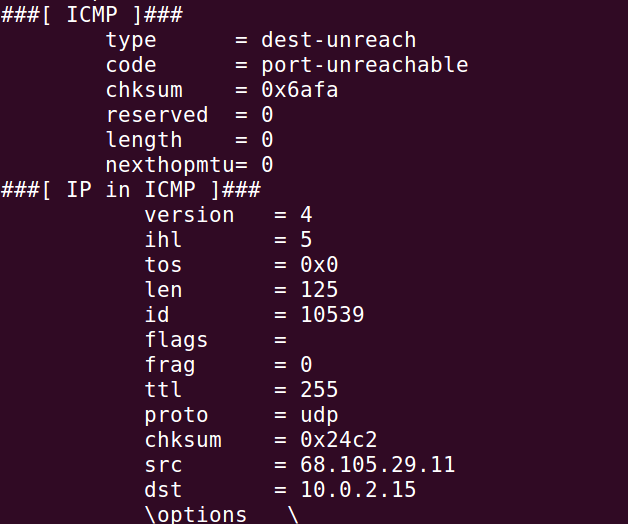


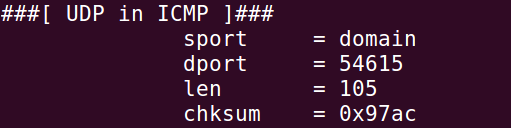
**Task 1.1: Sniffing Packets**

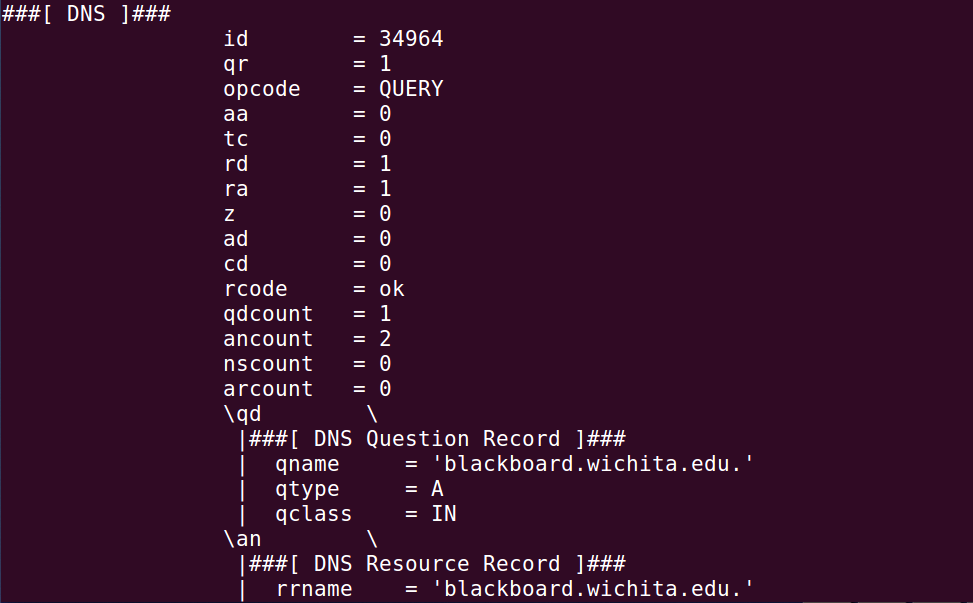
**Task 1.1A**

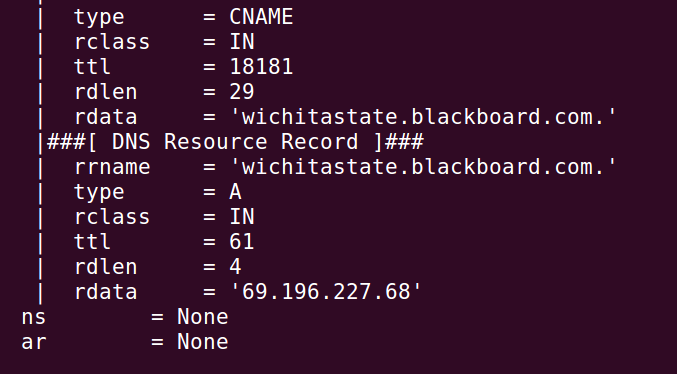
**// Running the program with the root privilege:**



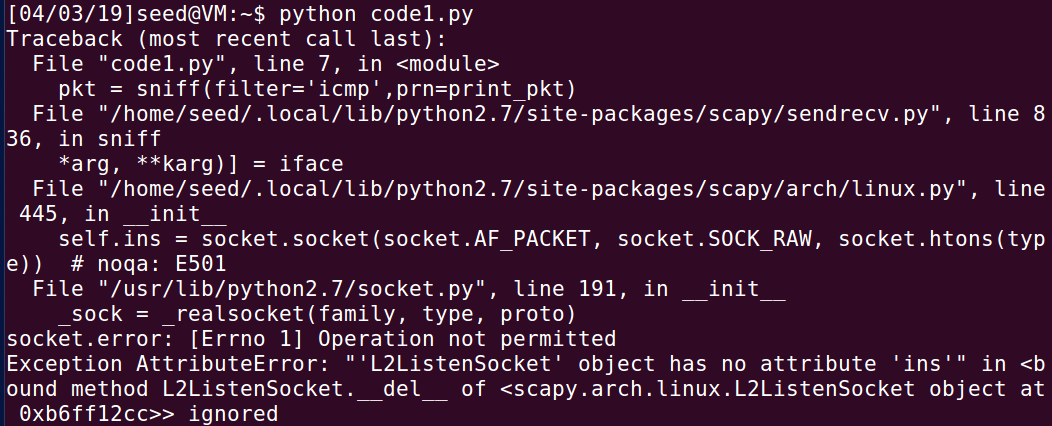








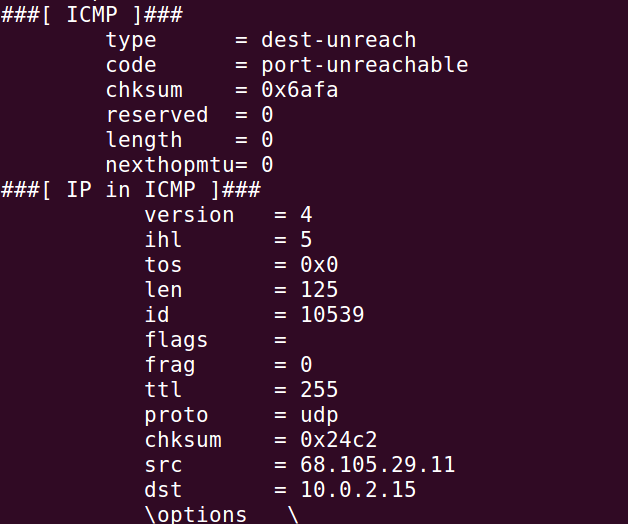
**// Running the task without the root privilege:**



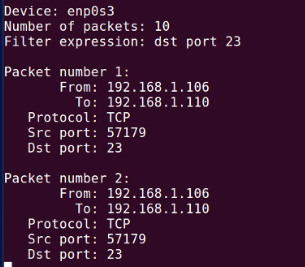
This is a program with root privilege and shows the capturing of packets. Without, the root privilege, it shows an error. In the code, there’s a header that describes what file will be used with the python code. Scapy function is pivotal for sniffing packets.

**Task 1.1B**

**Capture only the ICMP packet**

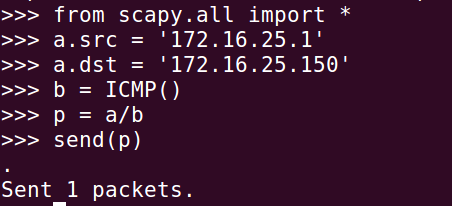


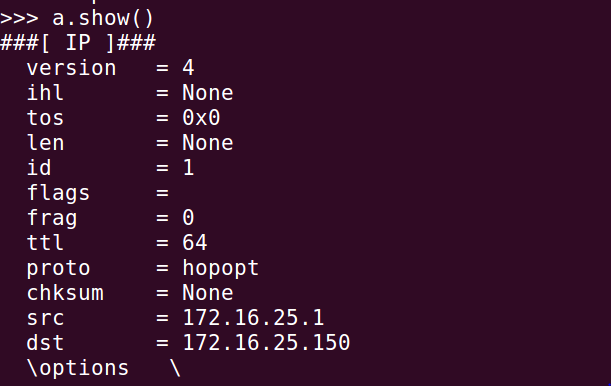
**Capture any TCP packet that comes from a particular IP and with a destination port number 23.**

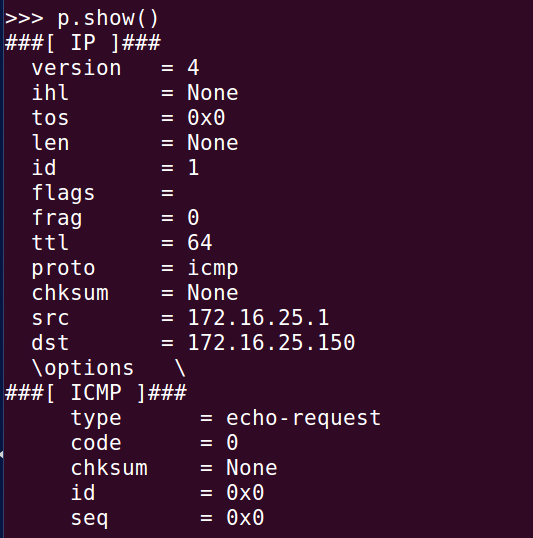


**Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16; you should not pick the subnet that your VM is attached to.**

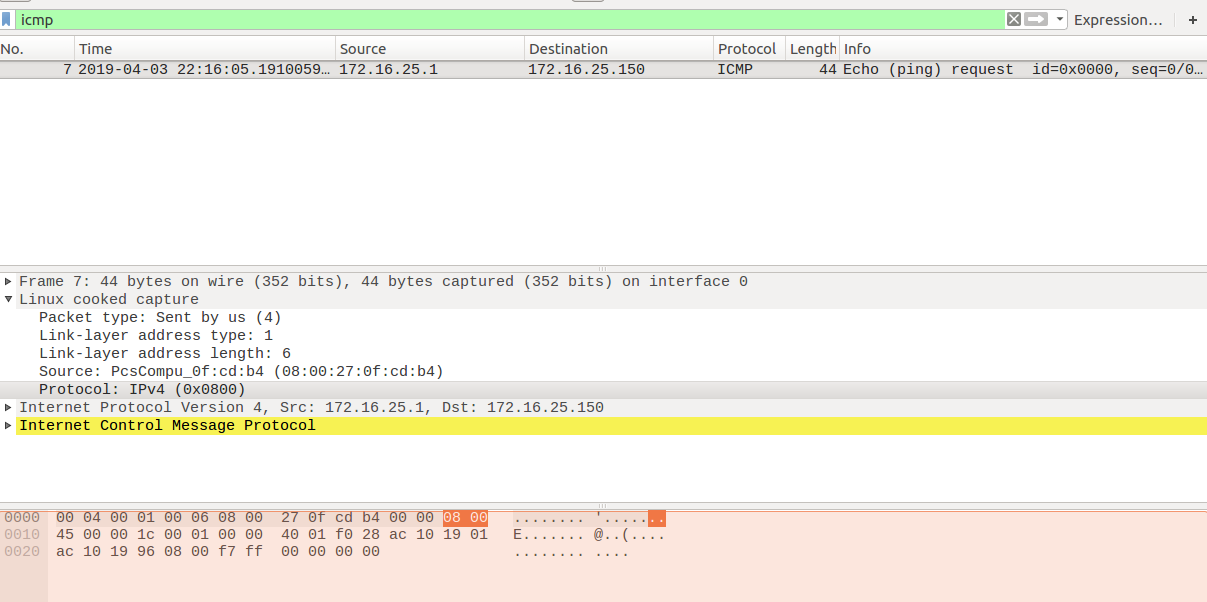
**Task 1.2: Spoofing ICMP Packets**



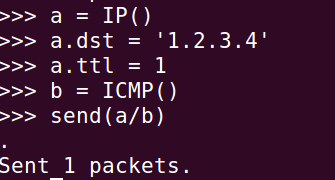


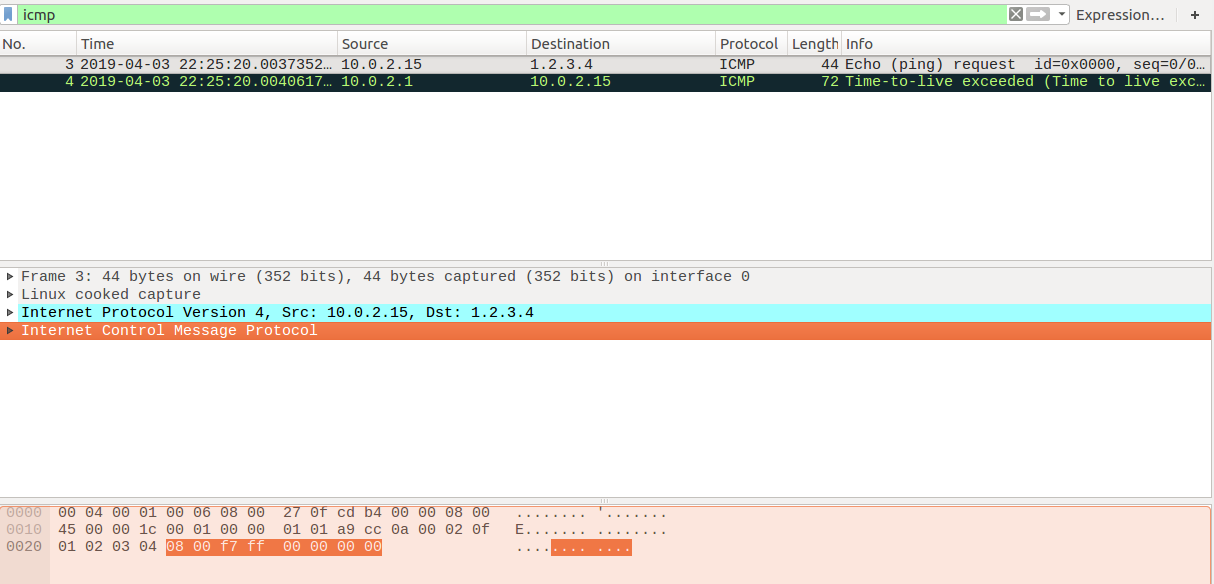


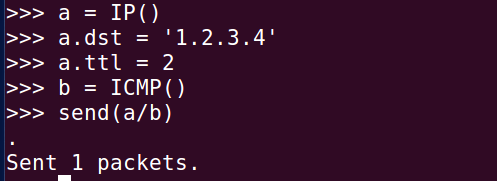
There’s an echo-ping request which clearly shows that I successfully spoofed an ICMP echo request packet with a made up source IP address.

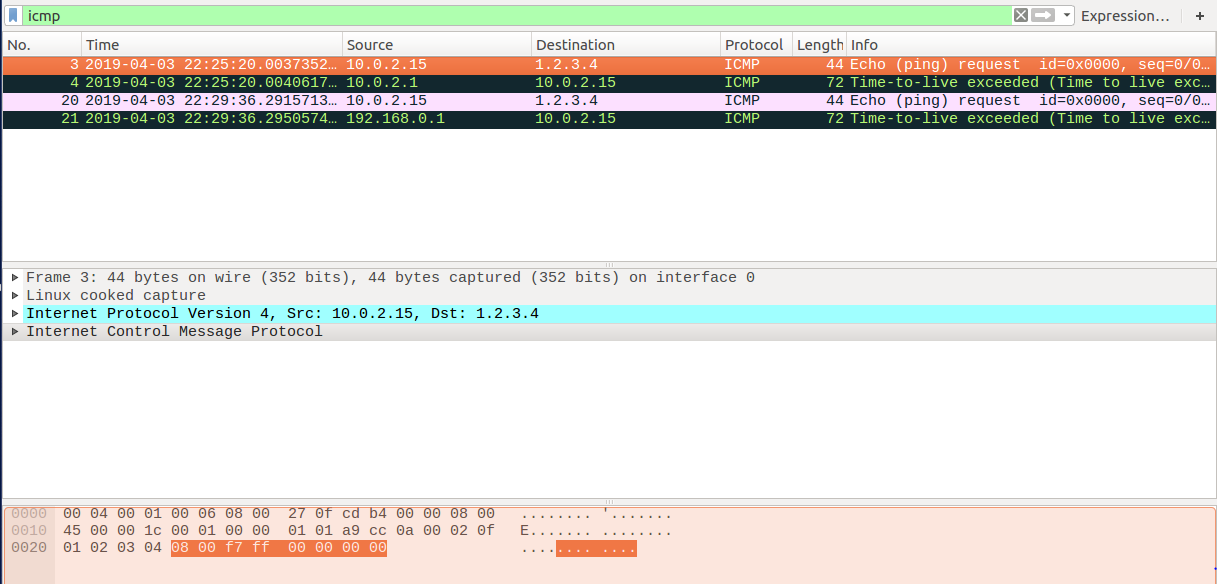


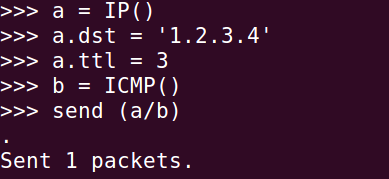
**Task 1.3: Traceroute**

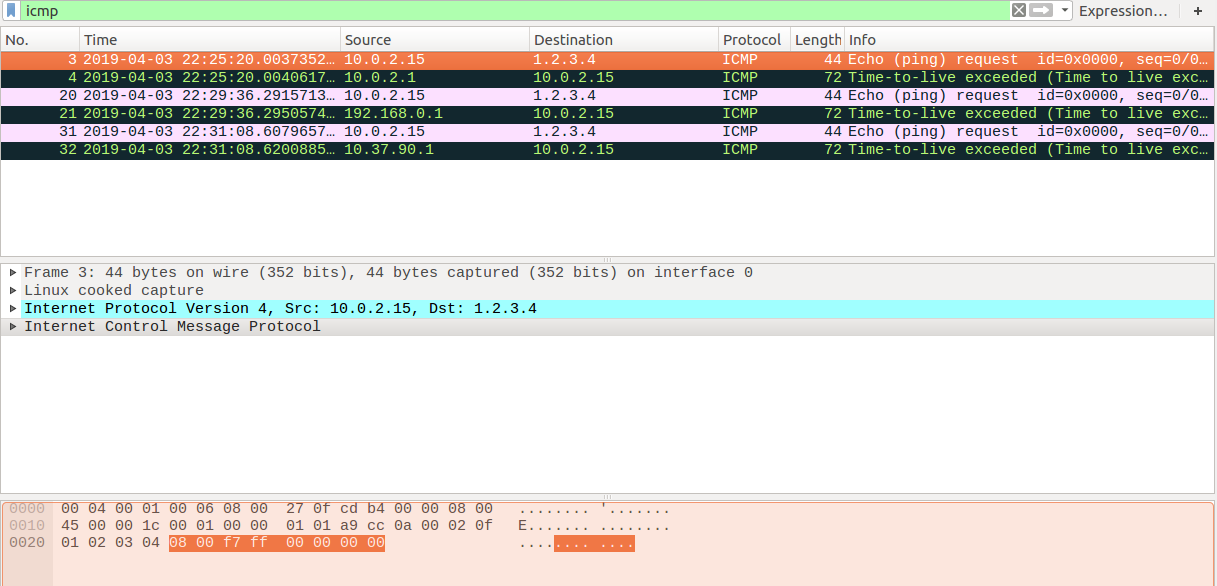




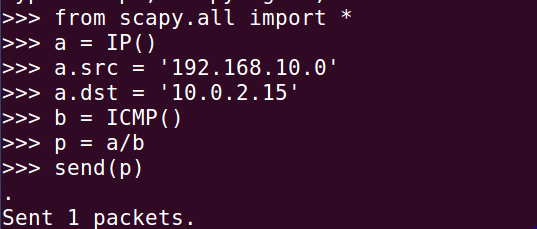


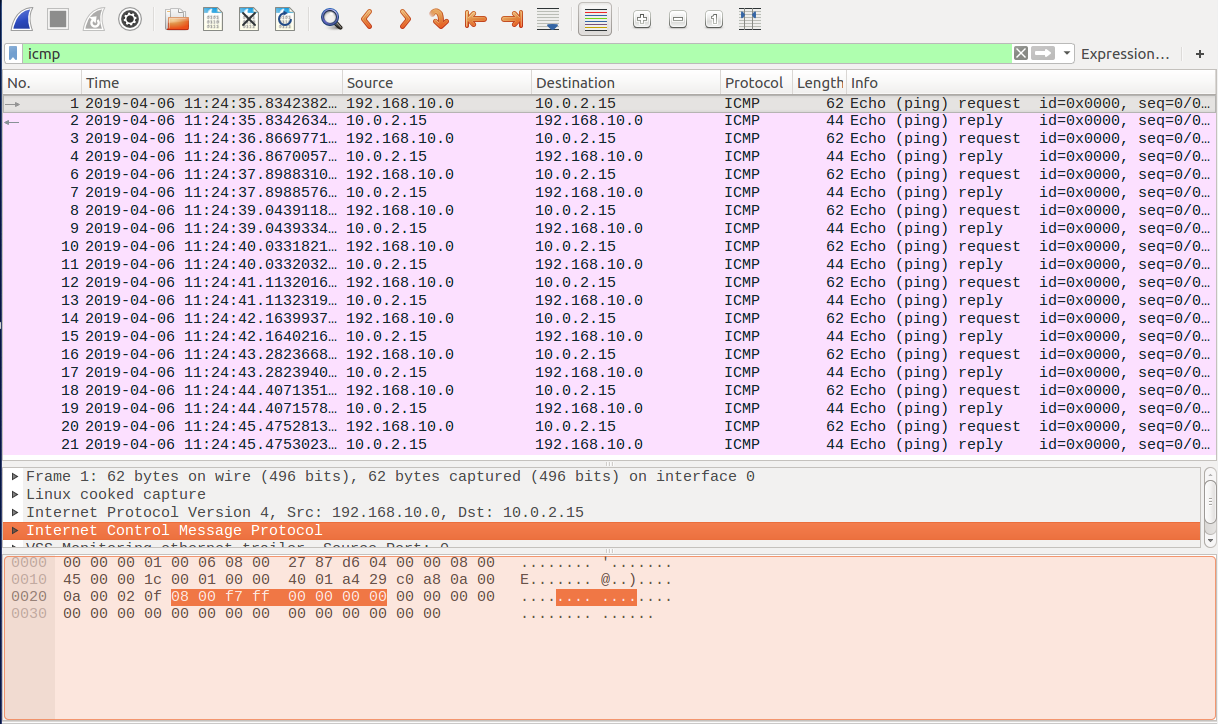






**2.4 Task 1.4: Sniffing and-then Spoofing**





This screenshot shows the ping from the clone VM to the original VM at the Wireshark from original VM to see if there was any ICMP packet echo request and reply. There is an echo-ping request and echo-ping reply which clearly depicts that I successfully spoofed an ICMP echo request packet with a made up source IP address. Whenever the original VM sees an ICMP request regardless of the target IP address, my program immediately sends out an echo-reply packet using the packet spoofing technique.