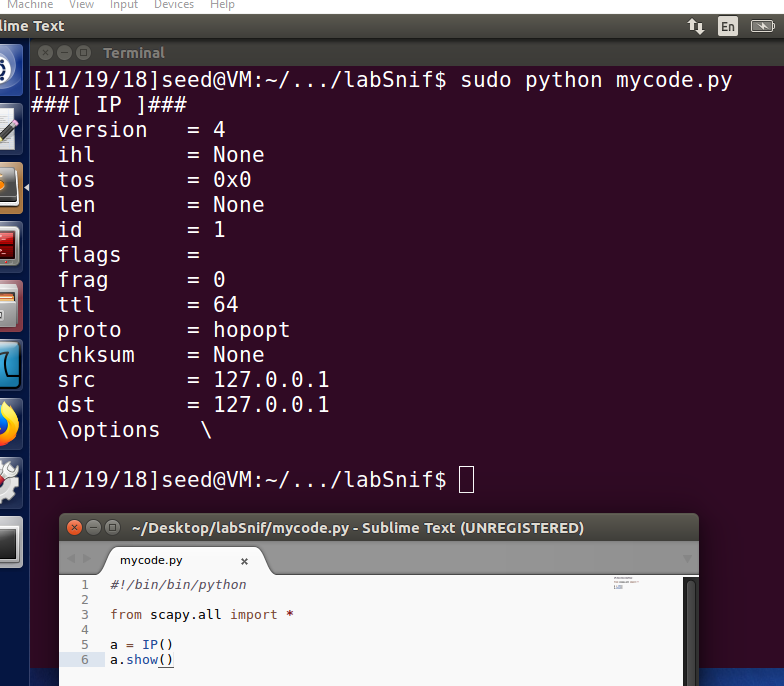
**Name: Alexey Titov**

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

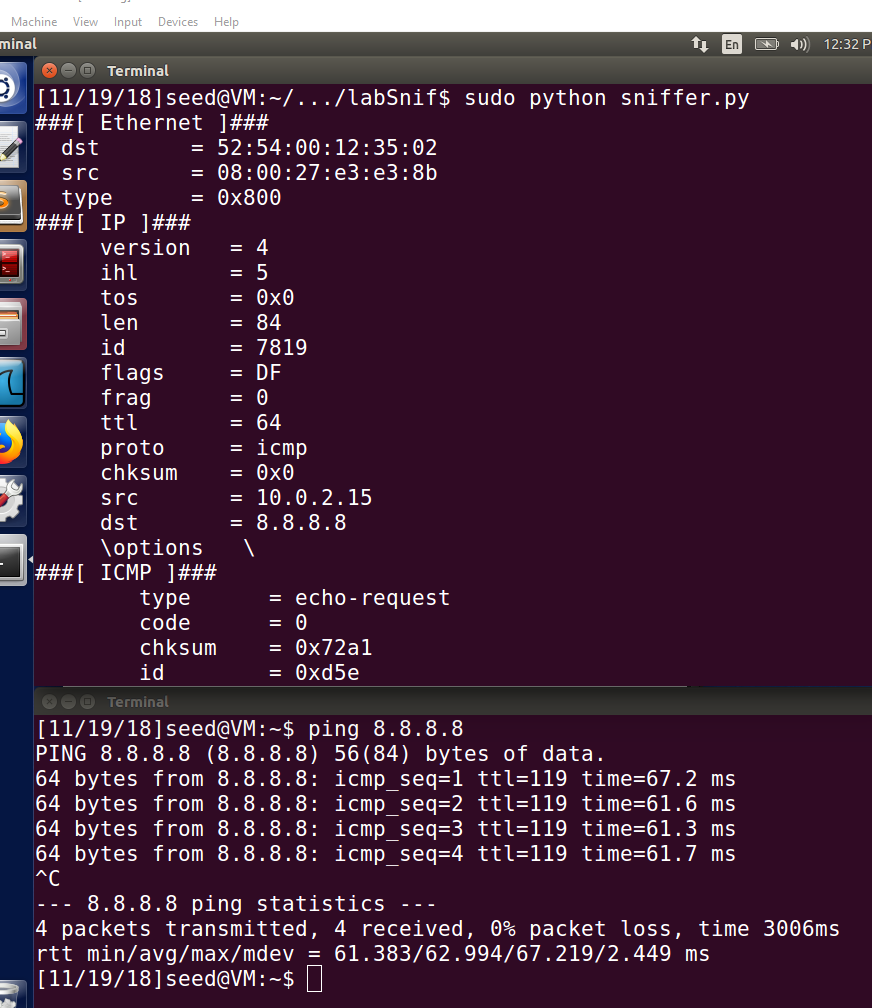


******

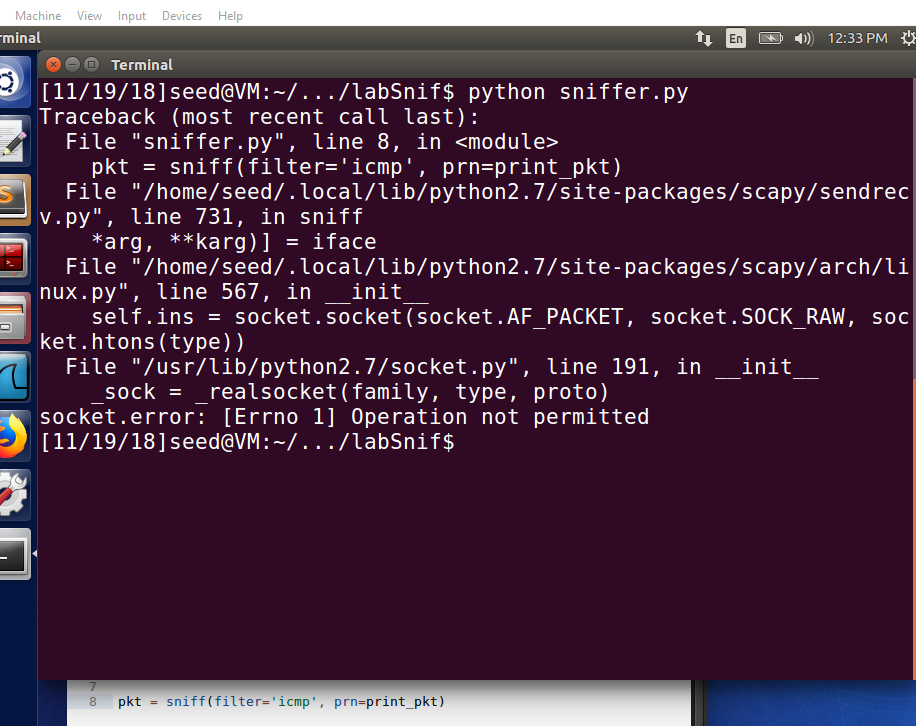
***Task 1.1: Sniffing Packets***

* Task 1.1A.

*sudo python sniffer.py*

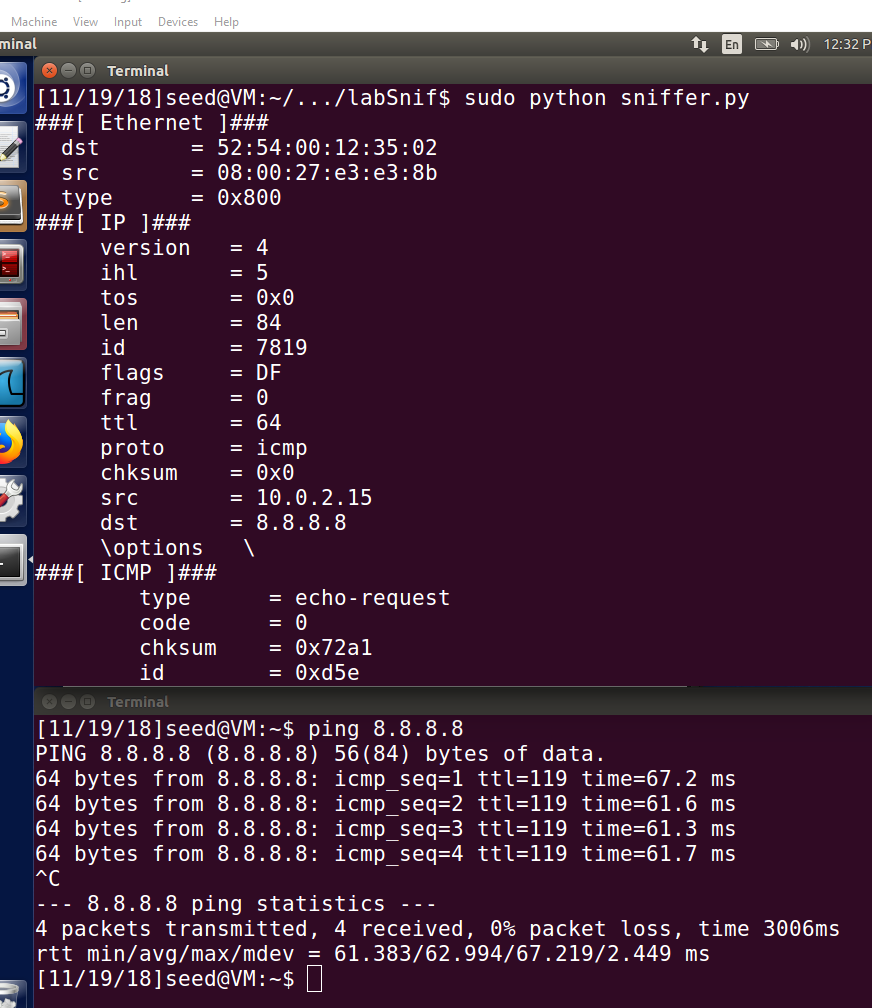


*python sniffer.py*

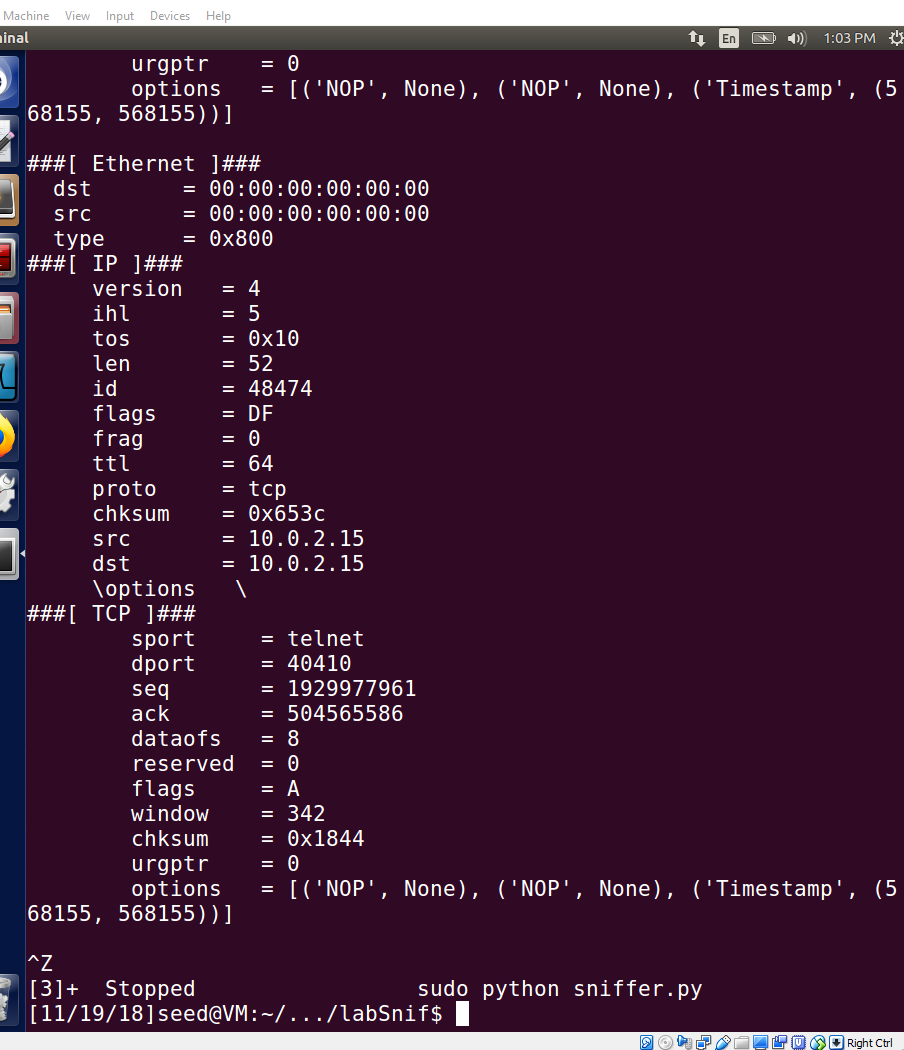


* Task 1.1B.

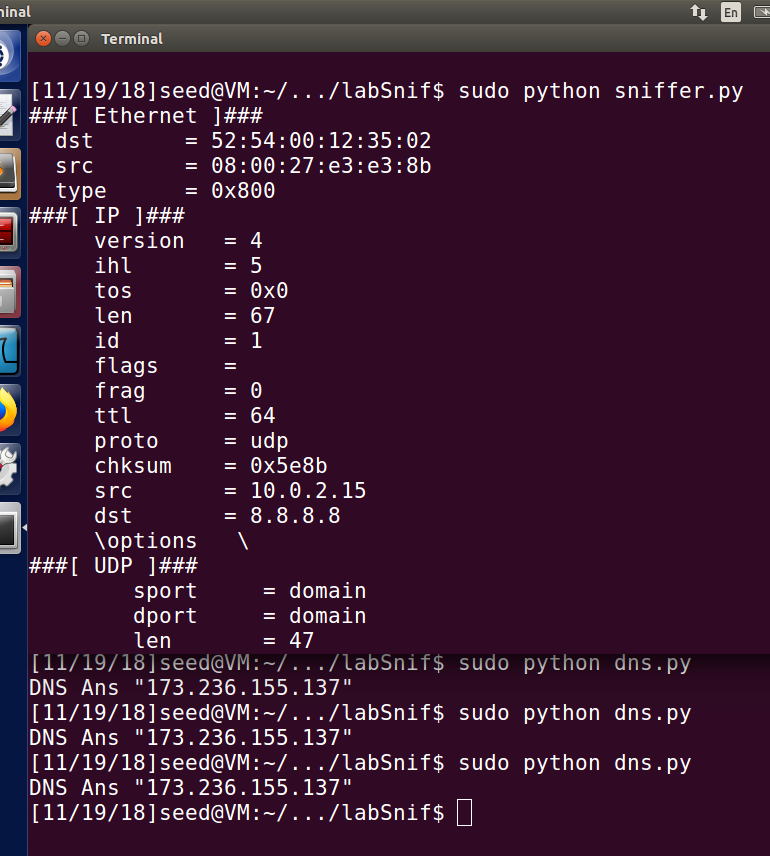
1. Capture only the ICMP packet



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

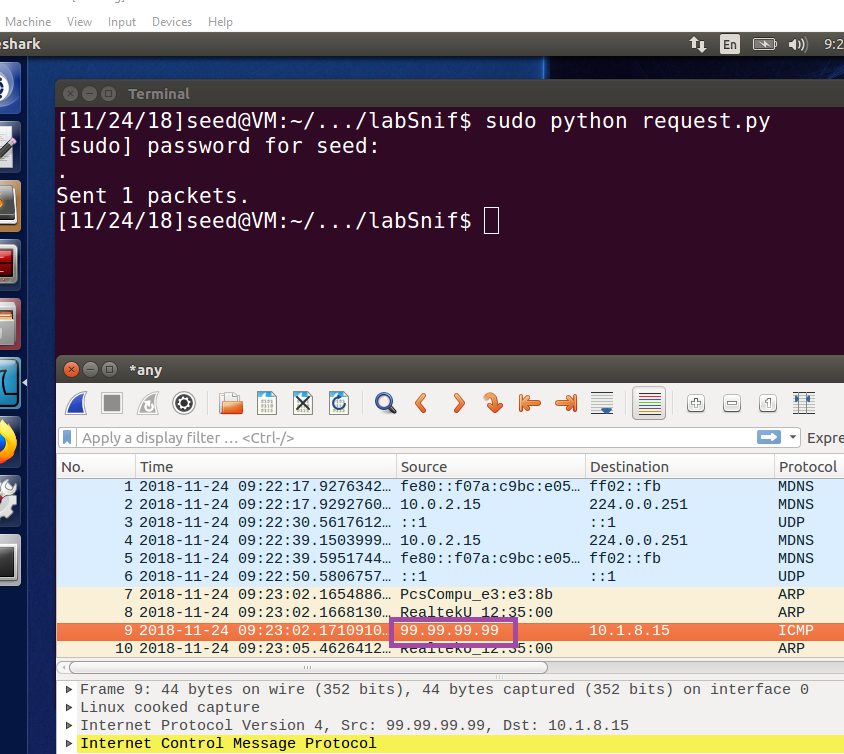


1. Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16; you should not pick the subnet that your VM is attached to.





***Task 1.2: Spoofing ICMP Packets***

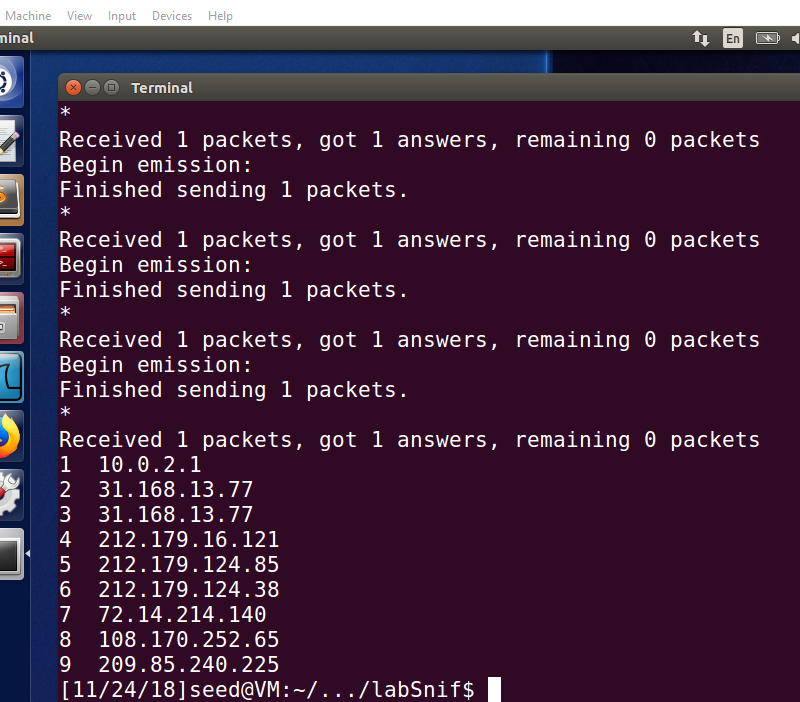




**Observation**: In the screenshots above, we can see that the attacker sends a spoofed ICMP request to a host and the host sends back an ICMP reply which is evident in the Wireshark capture.

**Explanation:** The attacker on 10.0.2.15 creates an ICMP packet with source address as 99.99.99.99 and sends the request to 10.0.2.15.

***Task 1.3: Traceroute***



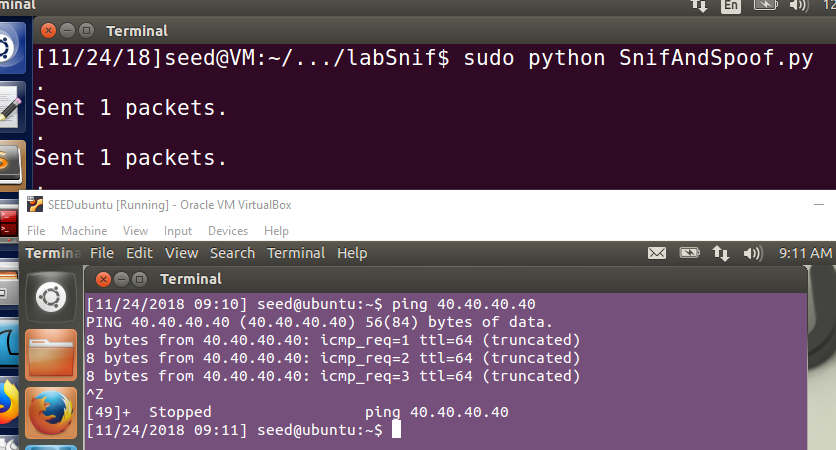
Explanation:

1– this is IP address of the first router.

\* \* \*

9 -this is IP address of the ninth router.

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





**Observation:**

User pings a host 40.40.40.40 on the network, the attacker sniffs the ICMP request, immediately spoofs the ICMP reply to the source of the ICMP request. The user receives the ICMP reply from the attacker.

**Explanation:**

Snoofing is sniffing for the request and immediately sending the reply. The user pings a host 40.40.40.40, the attacker on VM A receives the ICMP packet using pcap which listens to traffic (promiscuous mode on), spoofs an ICMP reply using raw socket by replacing the source ip as the destination ip and the destination ip as the source ip. The fields in the ip header and the icmp header are spoofed by the attacker. When the reply is sent to the User, it seems like he gets a normal reply from the host he pings to.