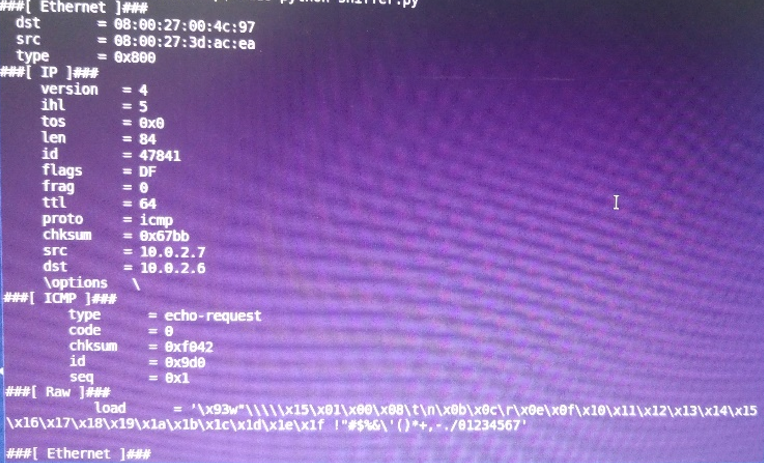
**Lab Task Set 1 – Python**

**A1.1**

Activating the Sniffer plus catching a Packet with Sudo approach

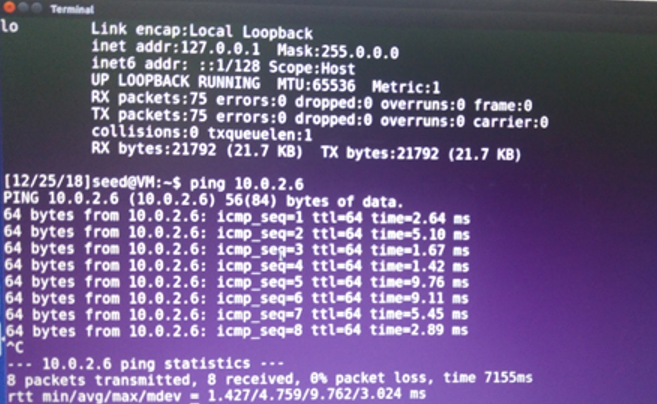


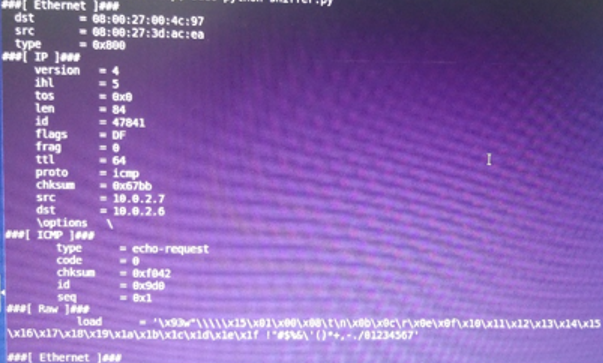
Attempt to run the file without Sudo approach

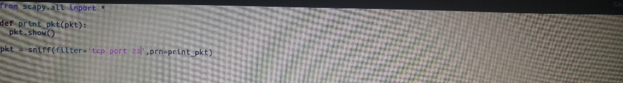


The difference between running with root access ie administrator and normal running is that by administrator access, it will be possible to access the network data for example and manage them which we would not expect any user to access there. so, while running with Sudo approach of manager it will be possible to do things related to management.

**B1.1**

First point - sending a ping from machine number 1 to machine number 2  
 (with the sniffer)

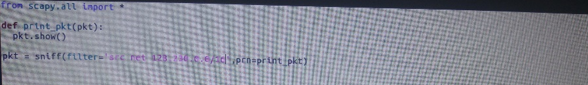
Receiving the ping in machine number 2, caught by the sniper

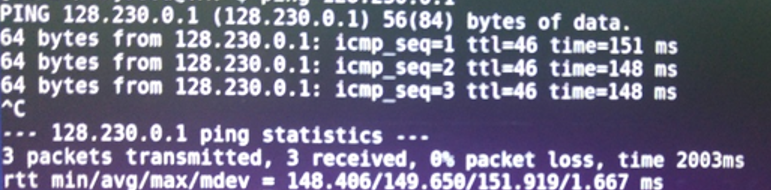
of point two code  


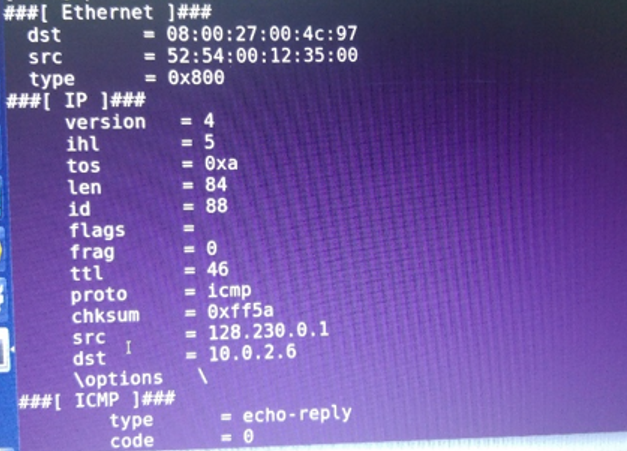
Sending a TCP message through port 23 to machine number 2  
Receive the Packet with the TCP message on machine number 2



of third point code

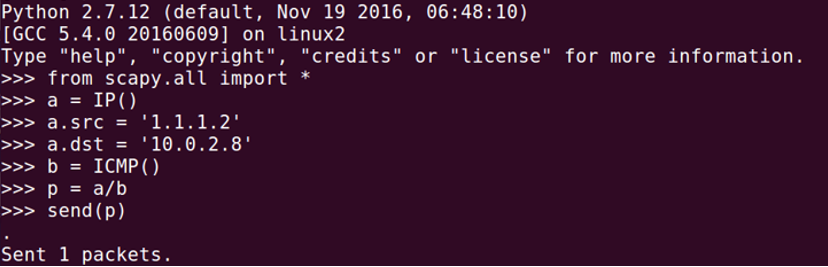


Sending an ICMP message to a subnet machine

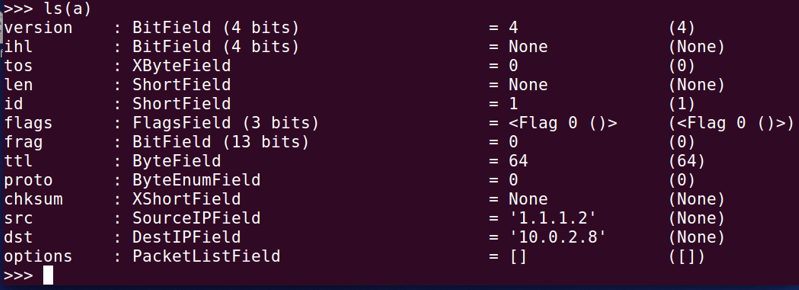
Receive the packet in the machine with the sniffer

**1.2**

Sending a packet to an arbitrary address

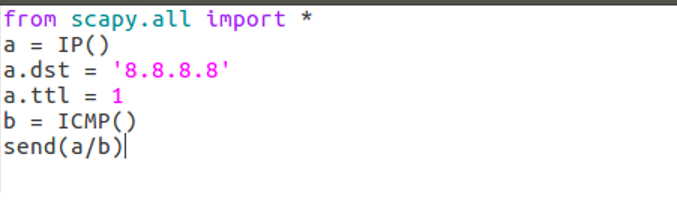


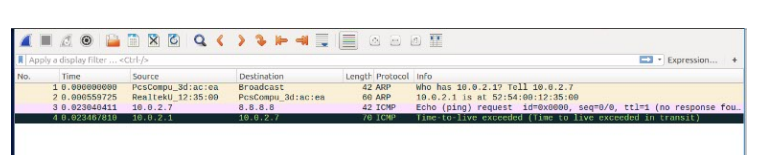
You can see how the packet looks like



**1.3**

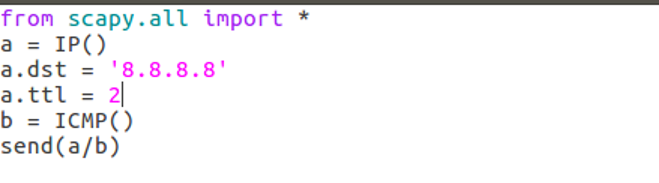
ttl = 1 the code when



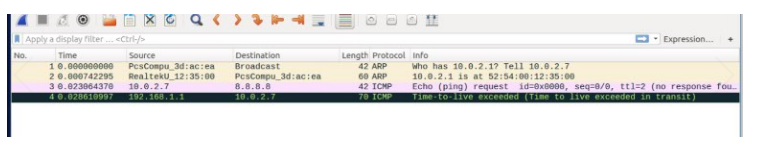
result will be

It can be seen that after the life time of the packet is 1 -> it doesn't reach its destination

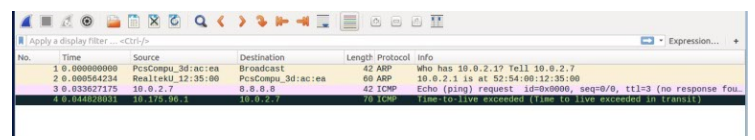
ttl = 2 code, this time,

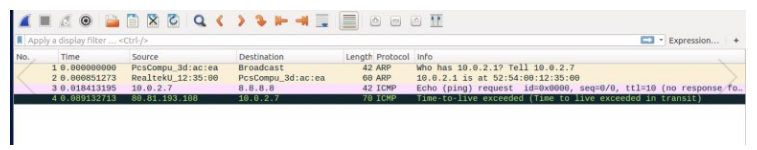


result will be

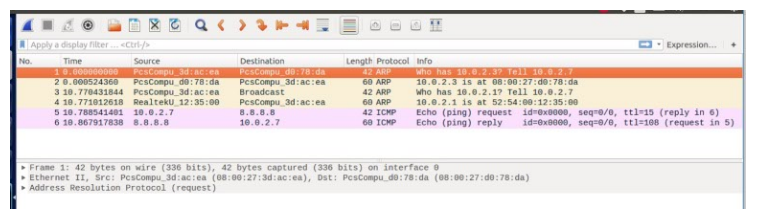


even when ttl=2 the packet it doesn't reach its destination

ttl = 3 

ttl = 10 

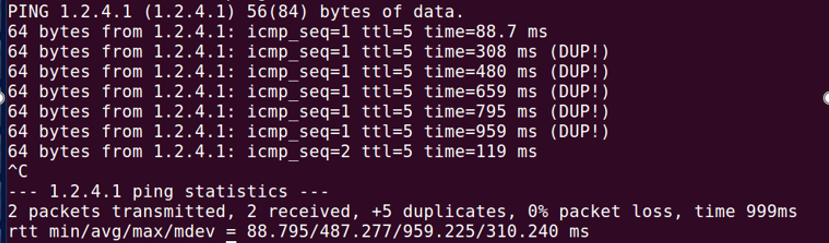
It can be seen that by life time 10 the packet does not reach the destination

ttl = 15 

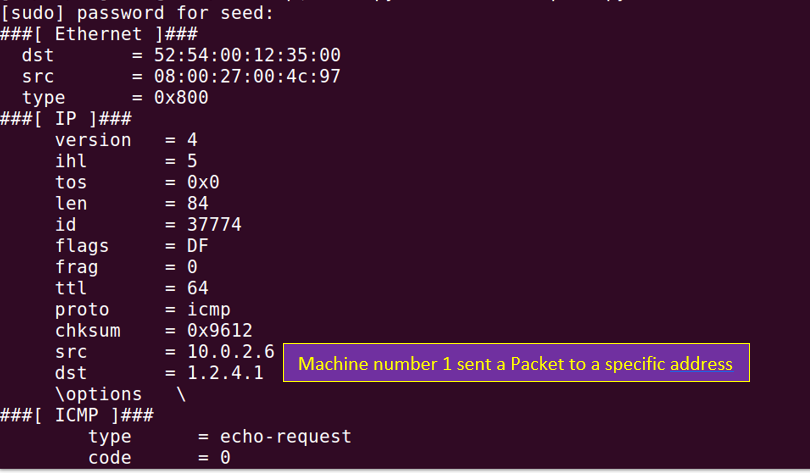
It can be seen that if ttl = 15 **then** the packet reaches the destination.

**1.4**Machine number 1 sends a ping to an arbitrary address.   
machine number 2 sniff the ICMP message and builds a fake message which it returns back to machine number 1 supposedly from the destination that machine 1 expected to receive a response from.

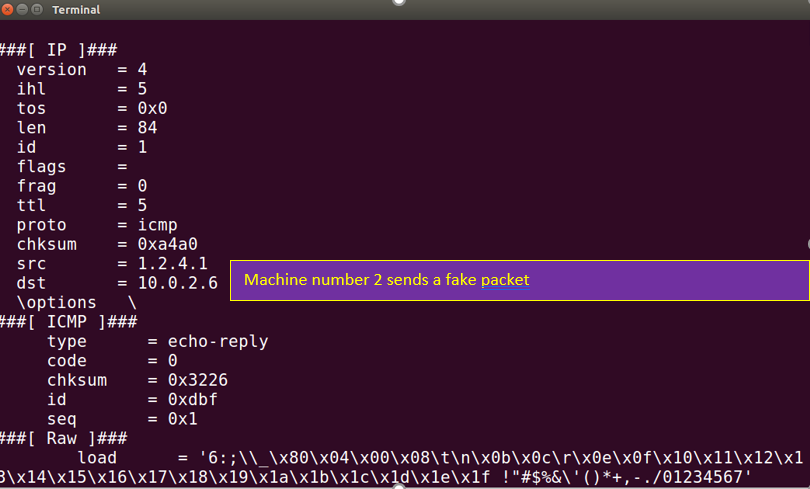
here we can see machine number 1 sending ping



machine number 2 sniff ICMP packets



and then returns fake packet to machine number 1



the code

Creates the header of the new IP and ICMP header and the source of the message is now the destination that machine 1 sent to

here we can see it takes data from the packet that the sniffer has captured and saves it for the new packet we will create

Response

שליחה בחזרה

שם בפקטה החדשה נתונים נוספים כמו אלה