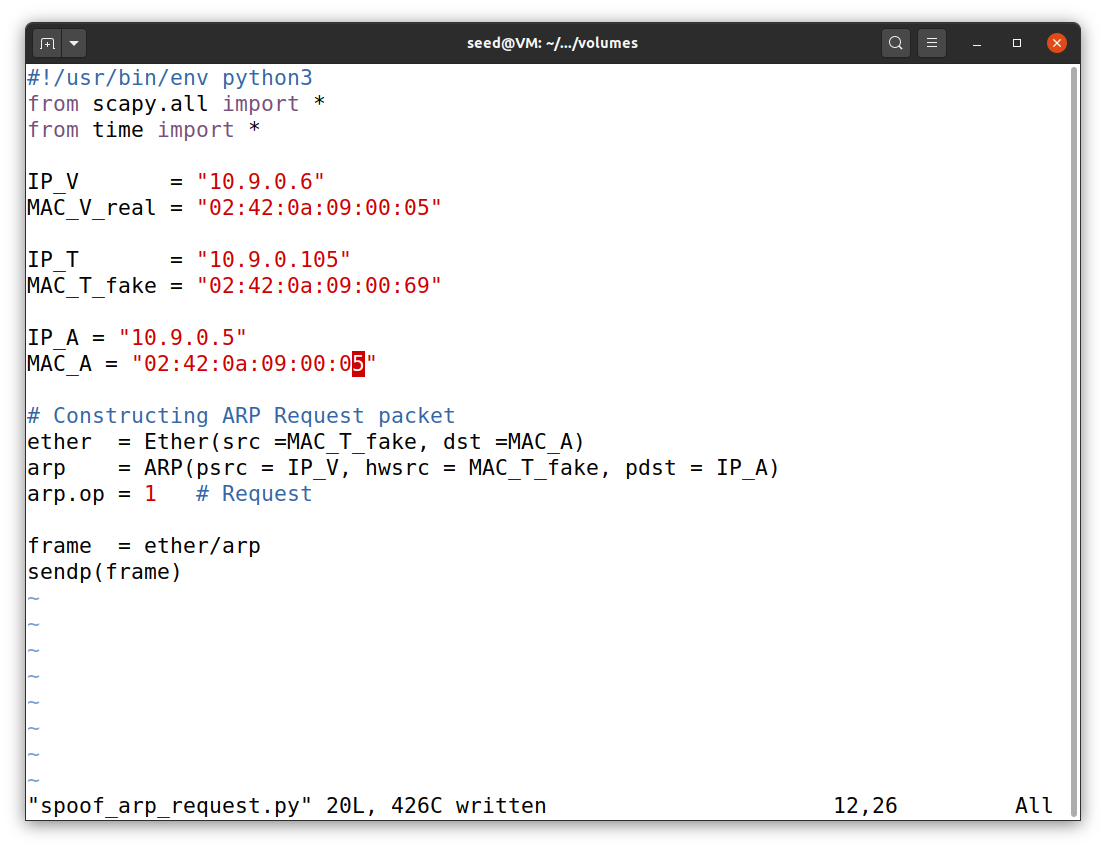
**Lab 3 ARP Cache Poisoning Attack**

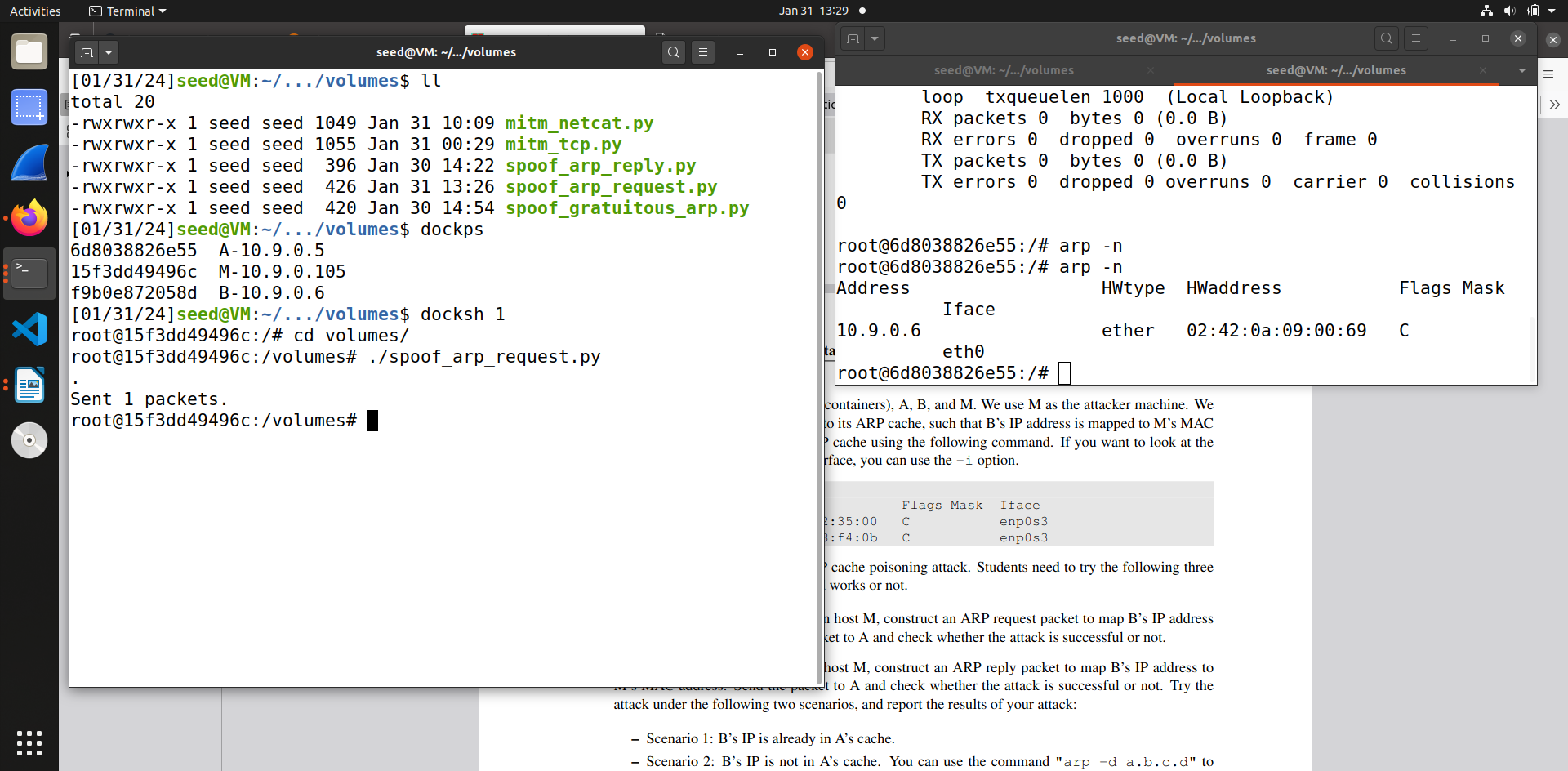
**Task 1. ARP Cache Poisoning**

**Task 1.A Using ARP Request**

In this task, we construct an ARP request packet to map B’s IP address to M’s MAC address.

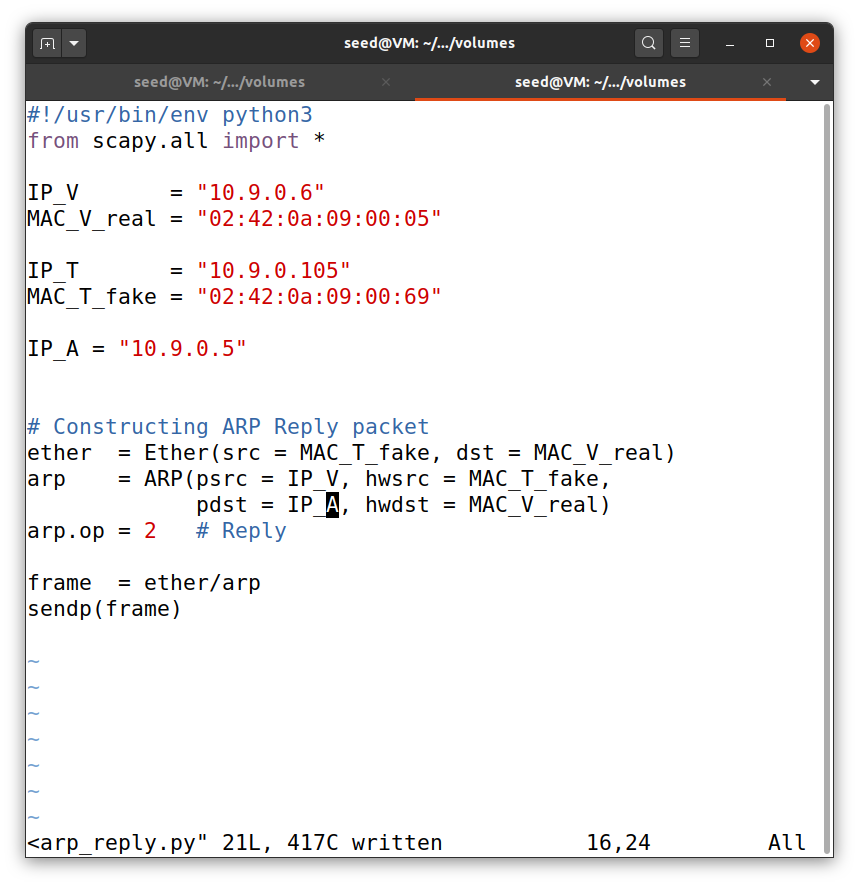


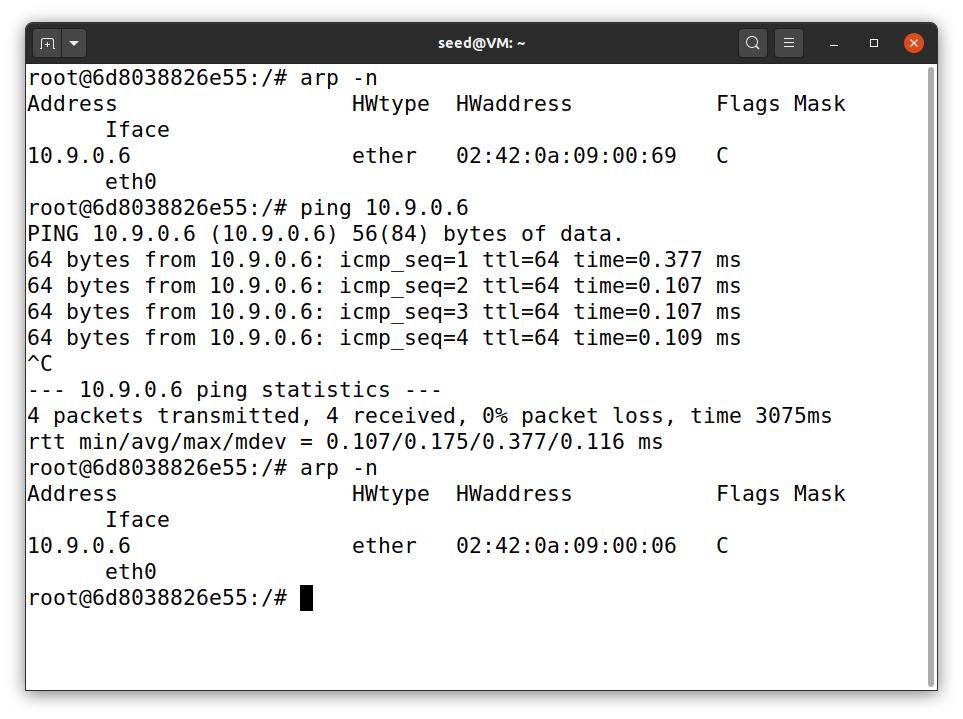
Before sending an ARP attack to A’s machine we have to first check whether it is empty, and after that we run the code to send the packet , and then as shown below in the screen shot we can see that there is B’s IP address mapped with attacker’s MAC address.



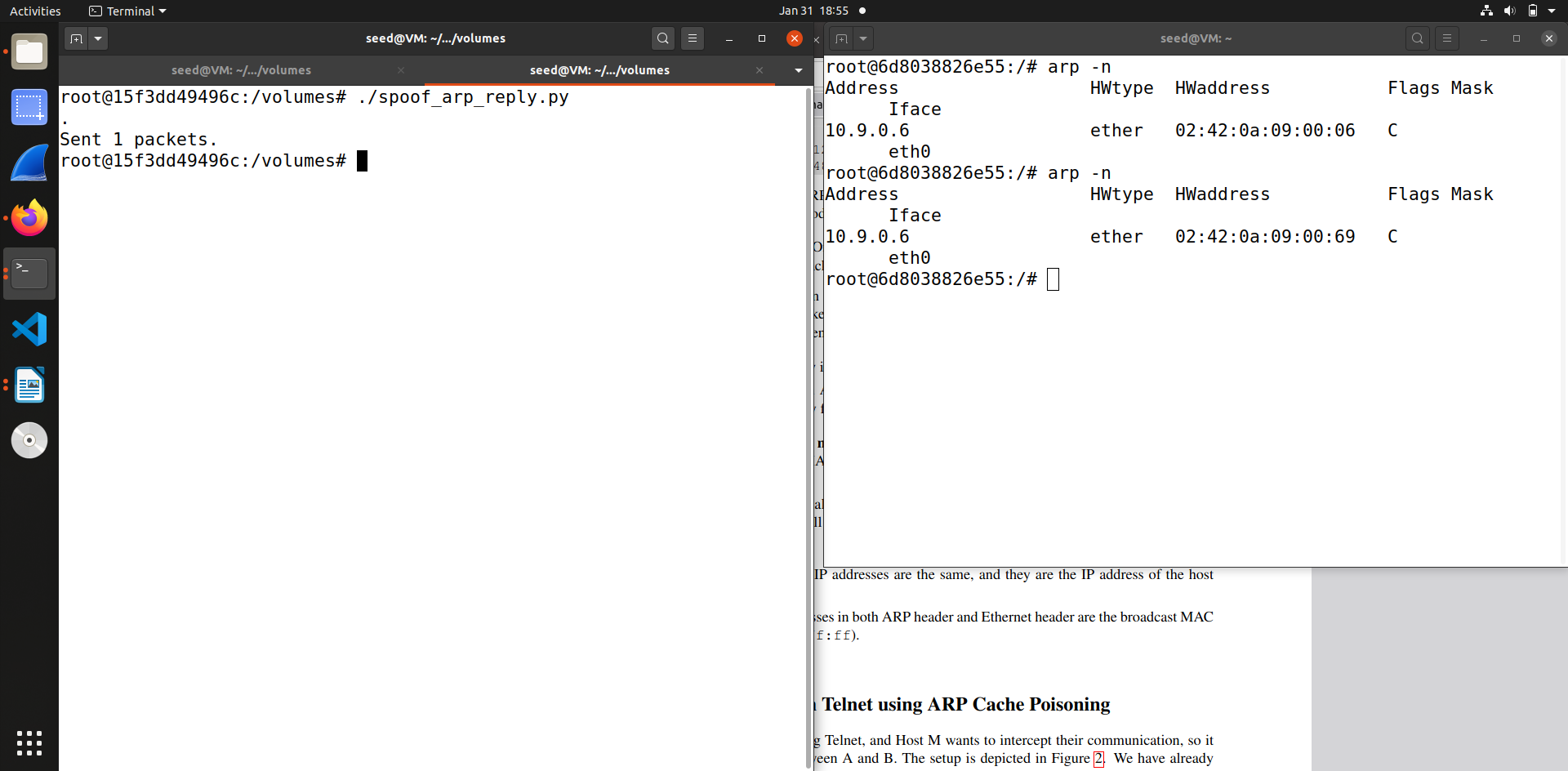
**Task 1.B Using ARP Reply**

In this task, we construct and ARP reply packet to map B’s IP address to M’s MAC address.

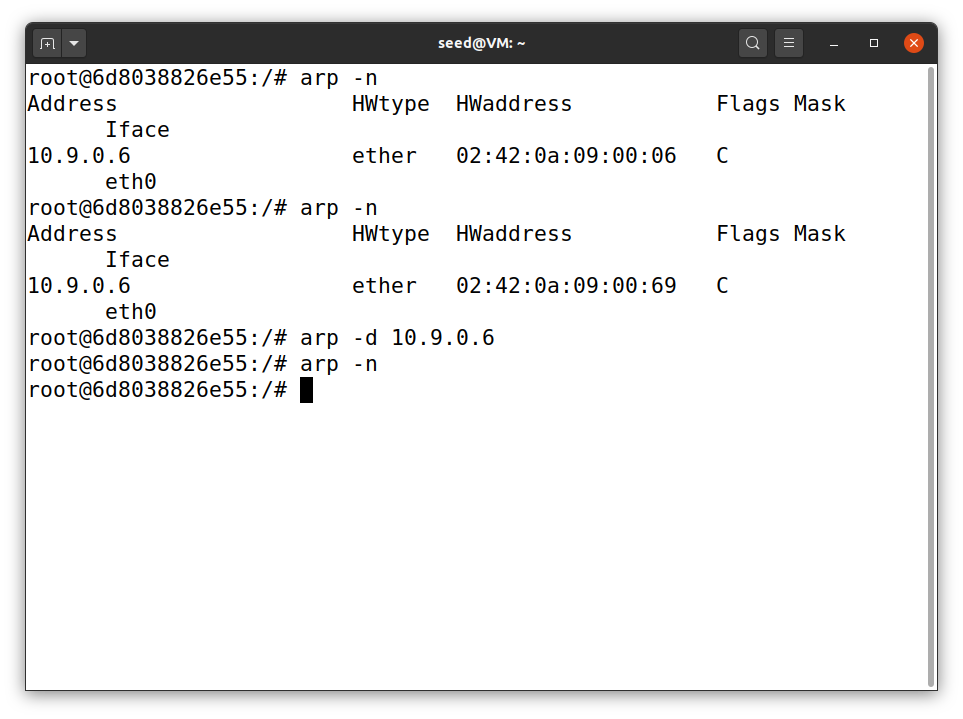


**Scenario 1 - B’s IP is already in A’s cache.**  
  


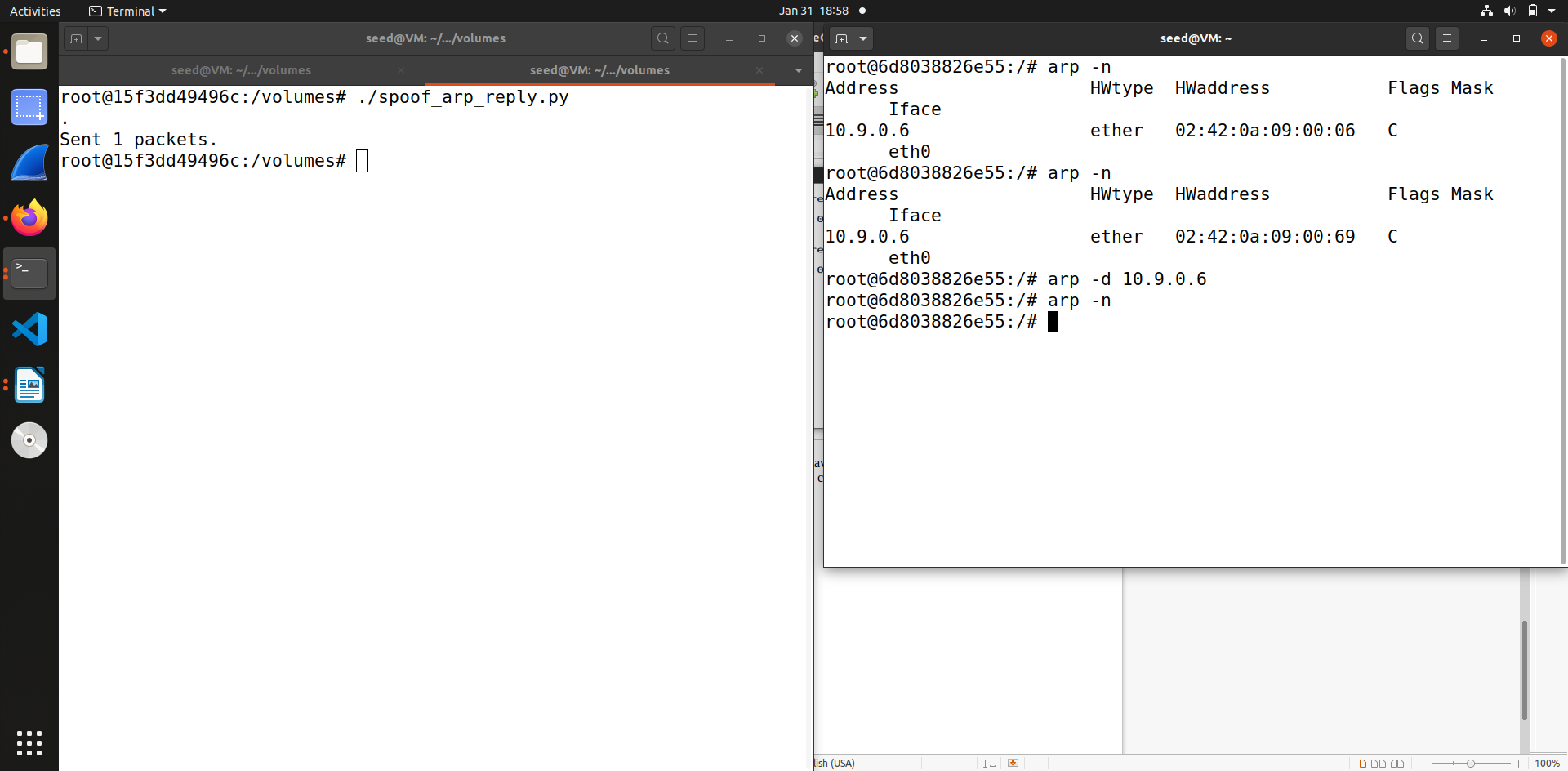
So in this scenario we can see that firstly in A machine ARP cache consists of B’s IP address but it was mapped with attack machine’s MAC address. So when we ping B machine’s IP address the previous entry gets modified with B machine’s IP address and actual MAC address.



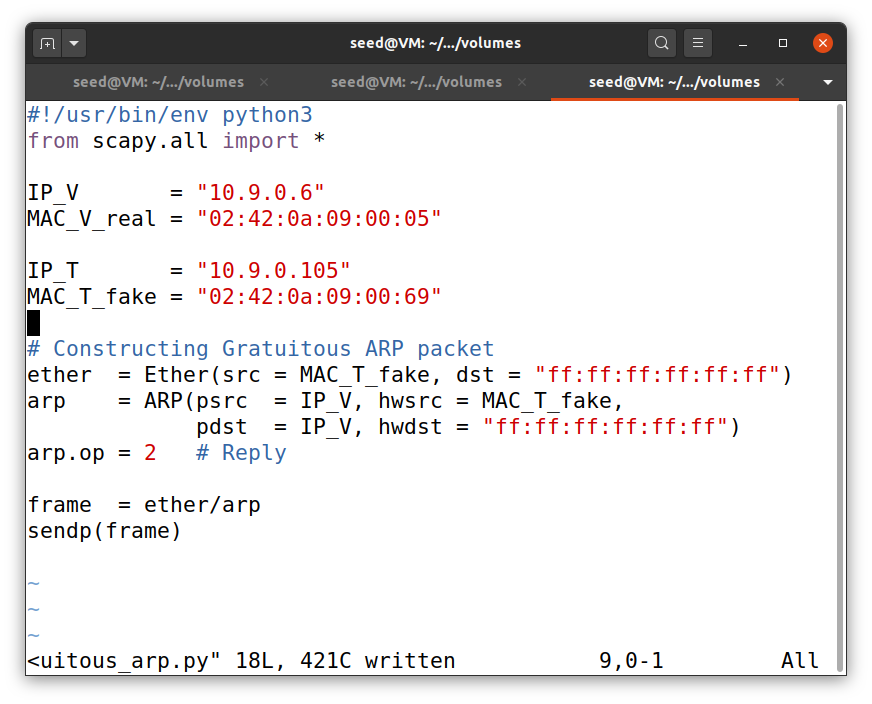
So after that we run the code and send the packet, which then once again modifies the previous entry of B machine’s with IP address of B machine but MAC address of attacker machine, showing attack successful.   
  
**Scenario 2: B’s IP is not in A’s cache.**



In this scenario, we have to run the same code but we have to delete B’s IP entry first in A’s cache. To do that we use ‘arp -d 10.9.0.6’, so after executing this command the previous entry of B machine in A’s cache will be deleted.

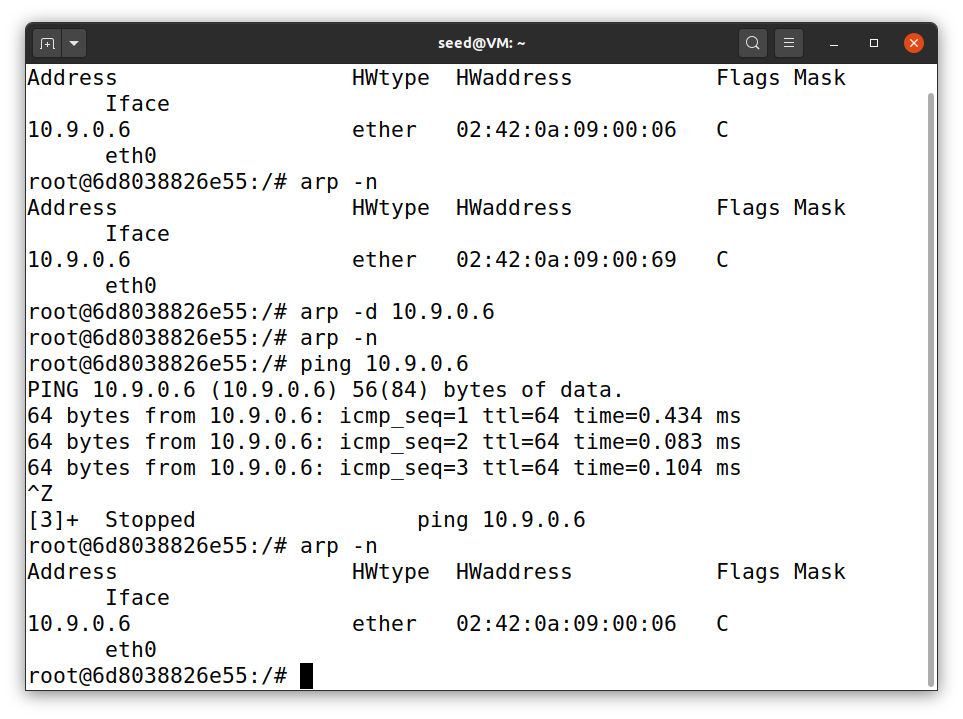
So as we can see from the output above when we delete B machine’s IP cache entry in A machine and then try sending the packet, it is not registered in A machine’s cache, this shows attack has failed.

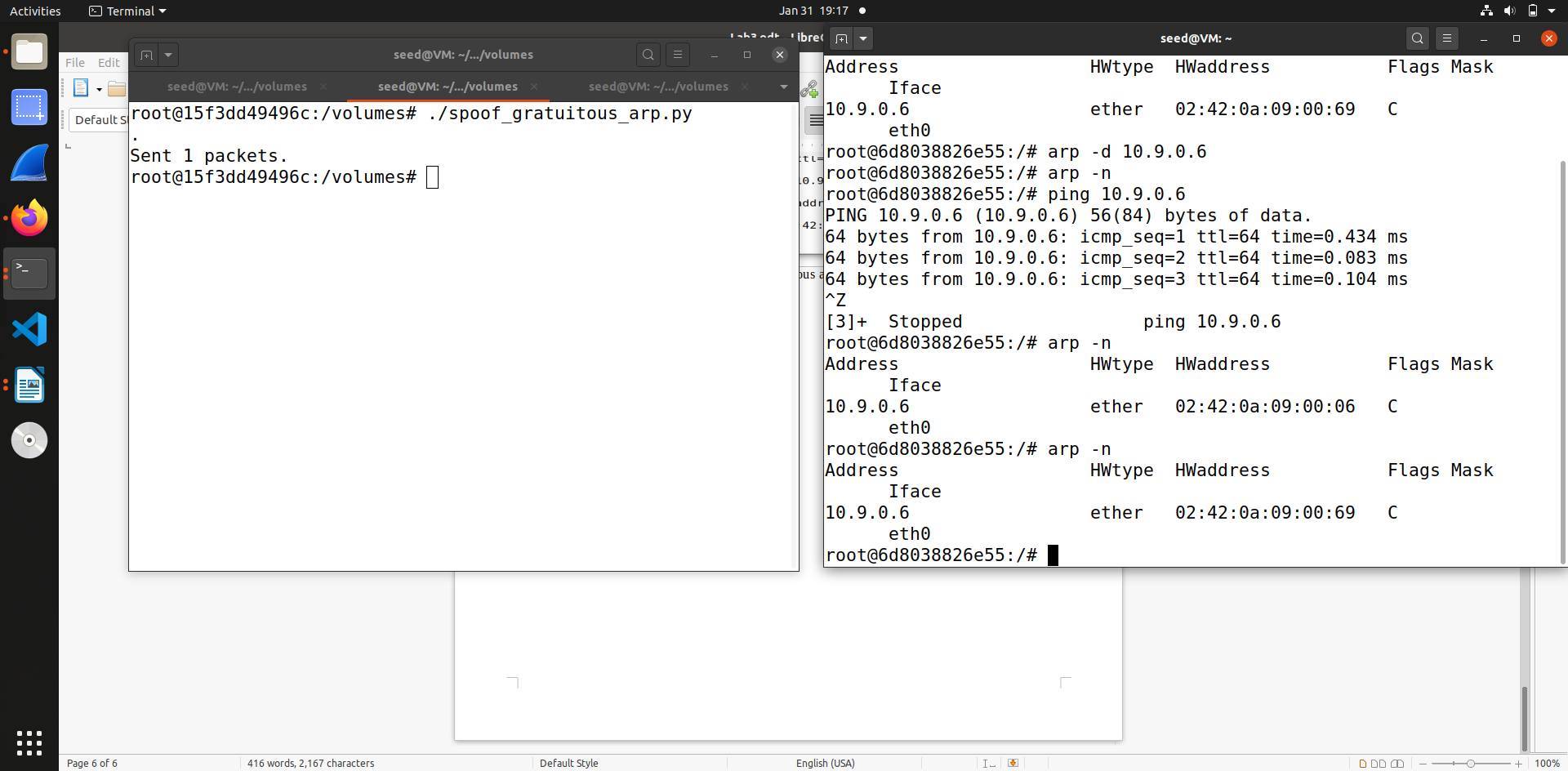
**Task 1.C Using ARP Gratuitous message**

In this task we send an Gratuitous message that is we basically broadcast it. So in this code we keep the source and destination IP address same. The destination MAC address for ARP and Ethernet is broadcasting we write it as “ff : ff : ff : ff : ff : ff” which means “1 : 1 : 1 : 1 : 1 : 1”

In this task also we run the code in 2 scenarios as we did earlier.

**Scenario 1**

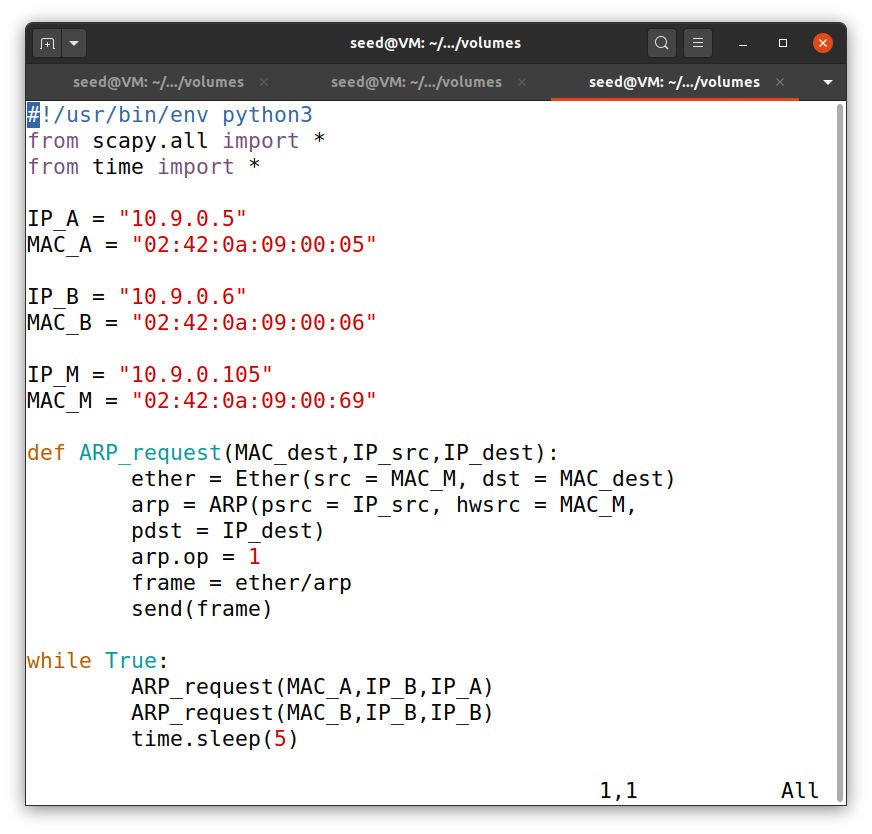
So this is the state of A before we launch the Gratuitous attack on it. We can see it has B machine’s IP address in the cache.

After we run the code we can see that B machine’s cache entry has been modified, it’s IP address is same but the MAC address is mapped to attacker machine, this means the ARP Gratuitous attack was successful.

**Scenario 2**

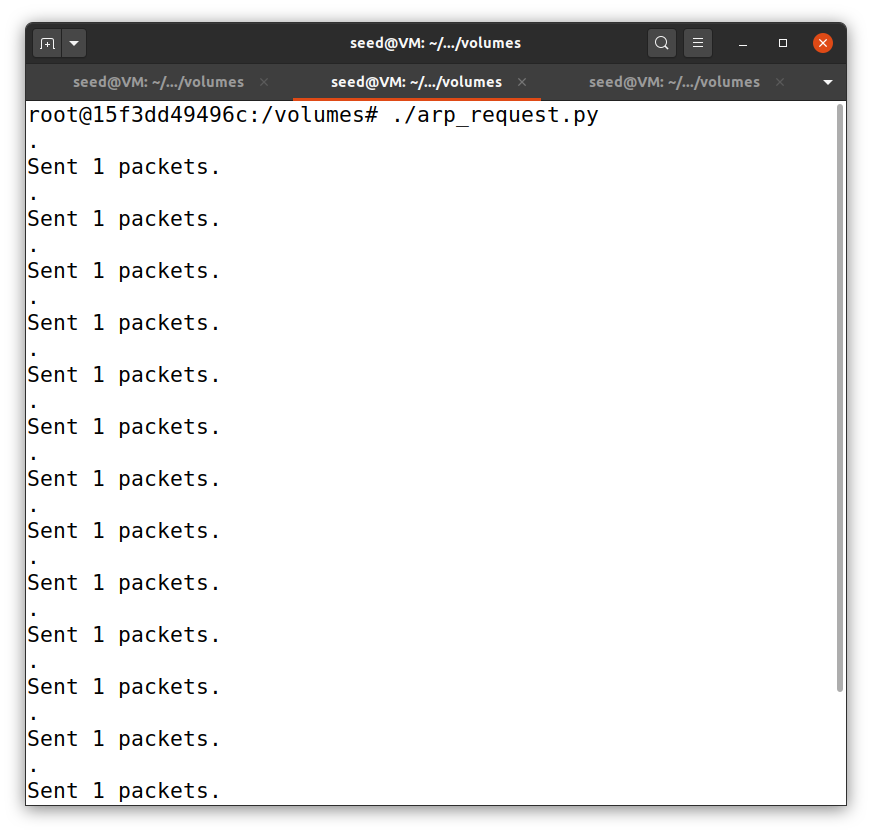
In this scenario we first delete the existing entry of B machine in A machine cache and then run the code , and as above screenshot we can see that the attack fails.

**Task 2 : MITM Attack on Telnet using ARP Cache Poisoning**



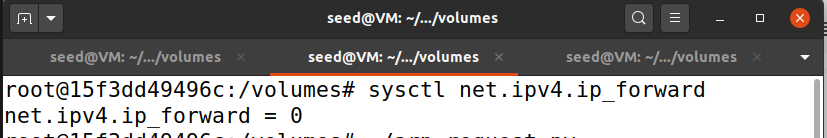
In this task we will carry out Man-In-The-Middle attack using telnet. So firstly we have to make sure that both A and B machine IP addresses are mapped to attacker’s MAC address. Using this above code we will send packets every 5 seconds to both A and B machine to ensure they are mapped to attacker’s MAC address only.

**Step 1 - Launch the ARP cache poisoning attack**

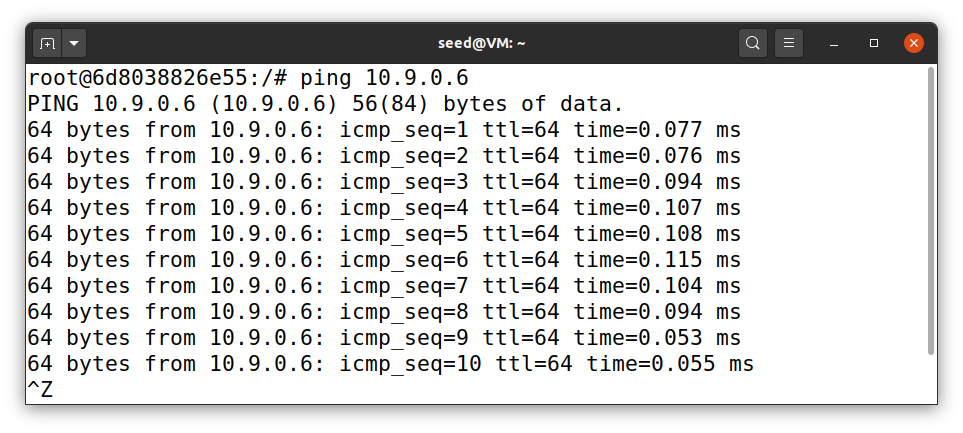


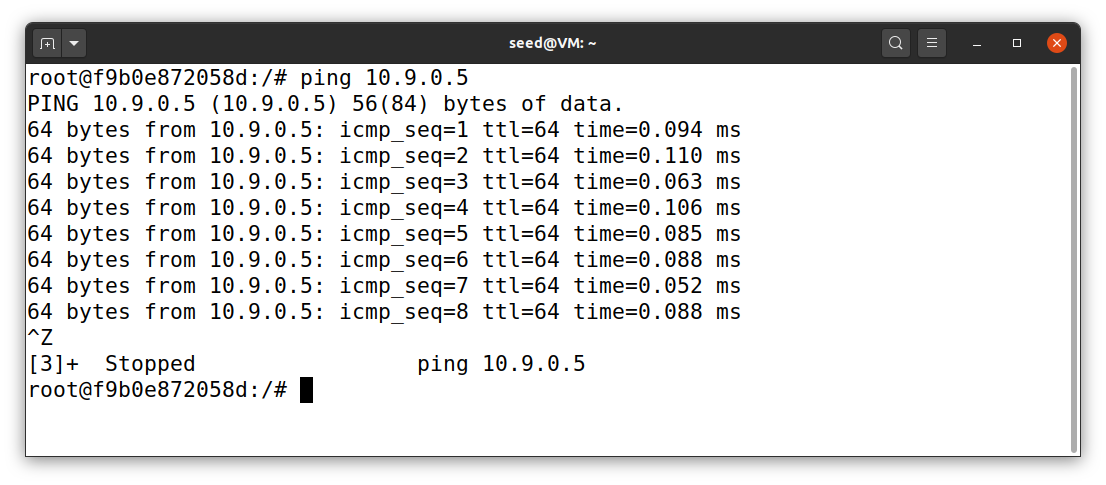
We run the above code of arp\_request so that the attack starts and both machine’s IP address of A and B is mapped to attacker MAC address by sending packets every 5 seconds.

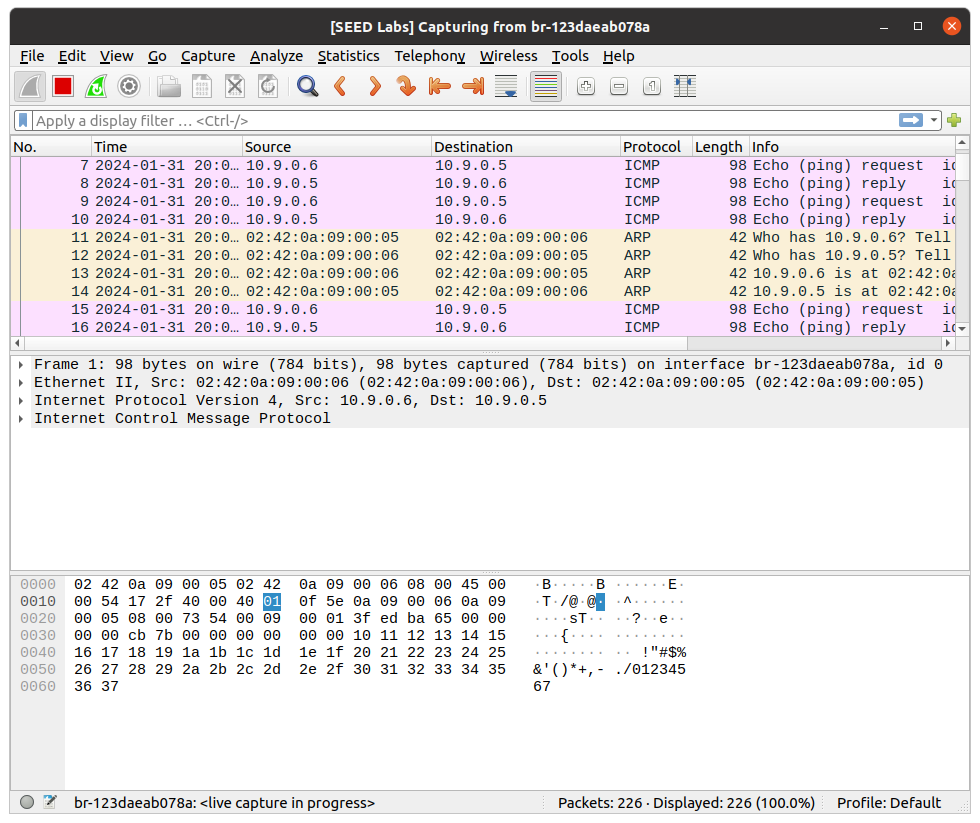
**Step 2 – Testing**

****

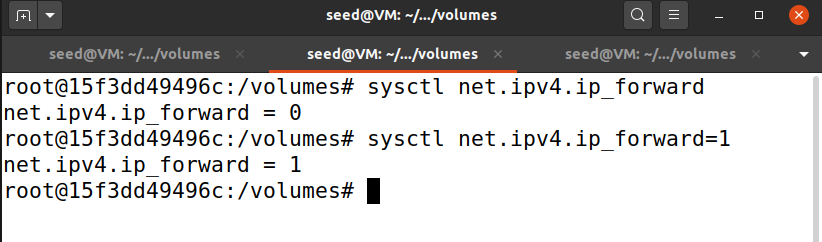
So in this step first we turn off the ip\_forward that is set it to 0.

Then we ping machine B from A

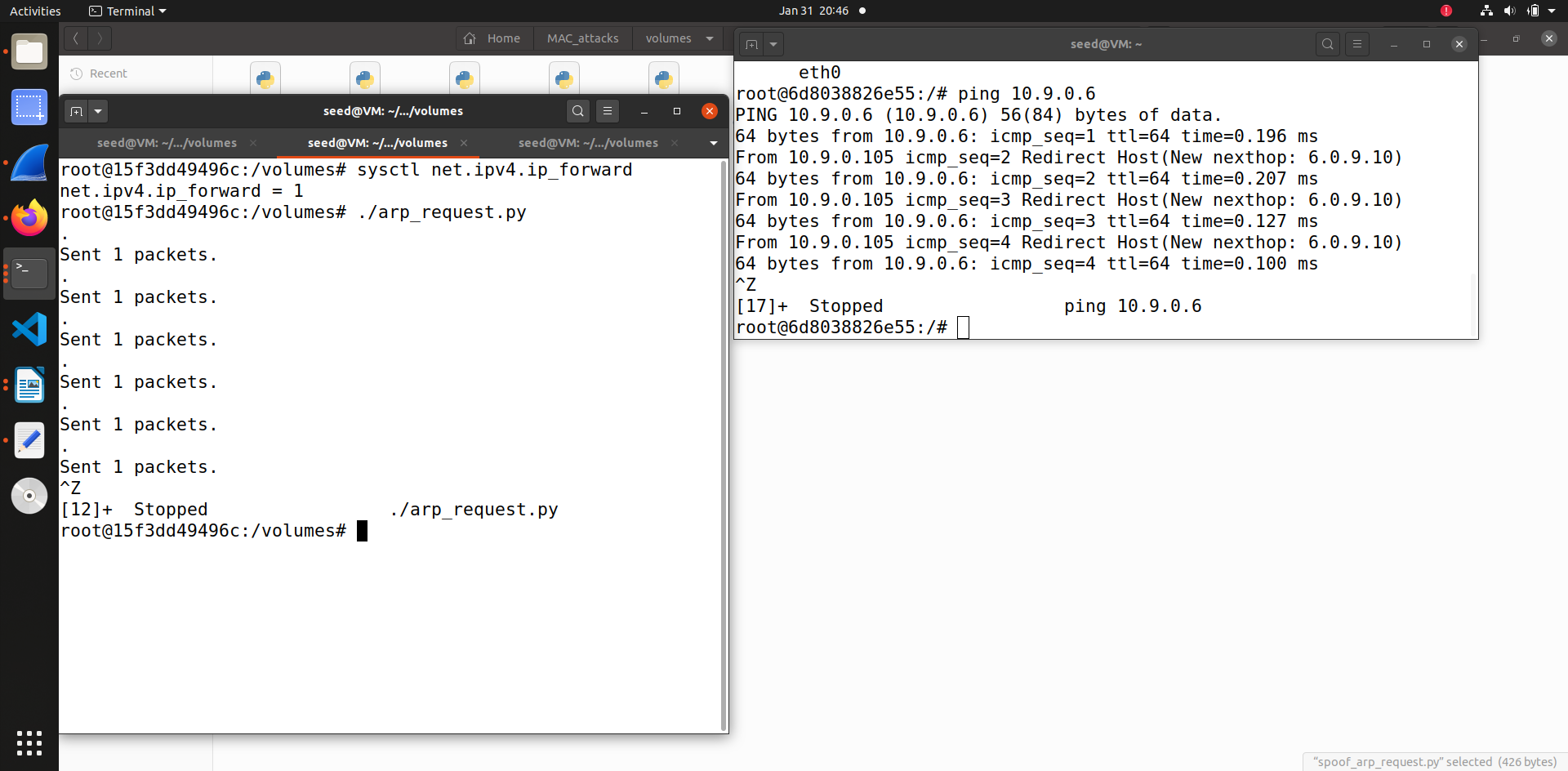
Then we ping machine A from B

This is the what we capture through live Wire shark.

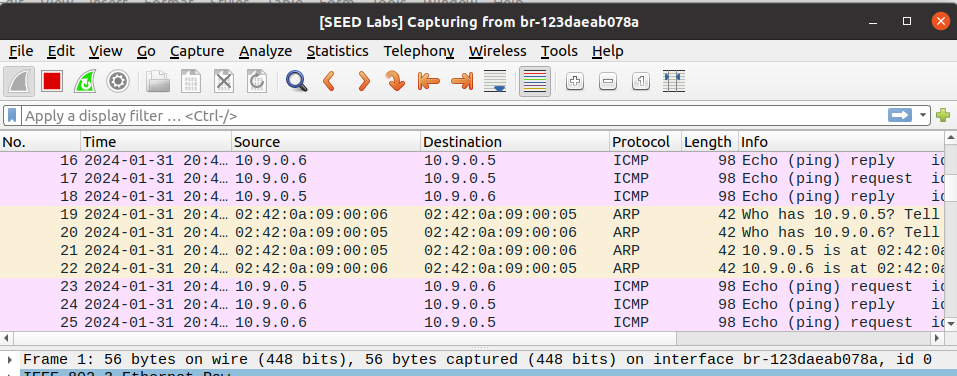
**Step 3 - Turn on IP forwarding**

In this step we turn on the ip\_forward that is set to 1.

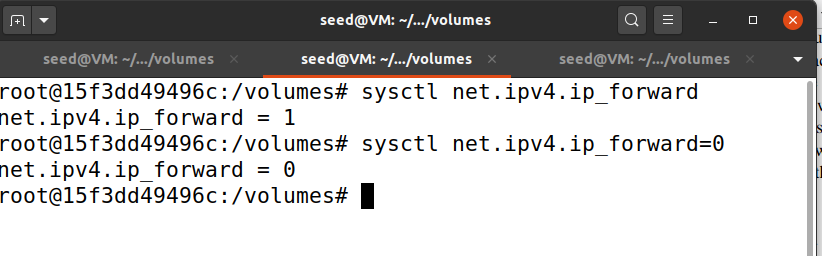
And then repeat step 2.



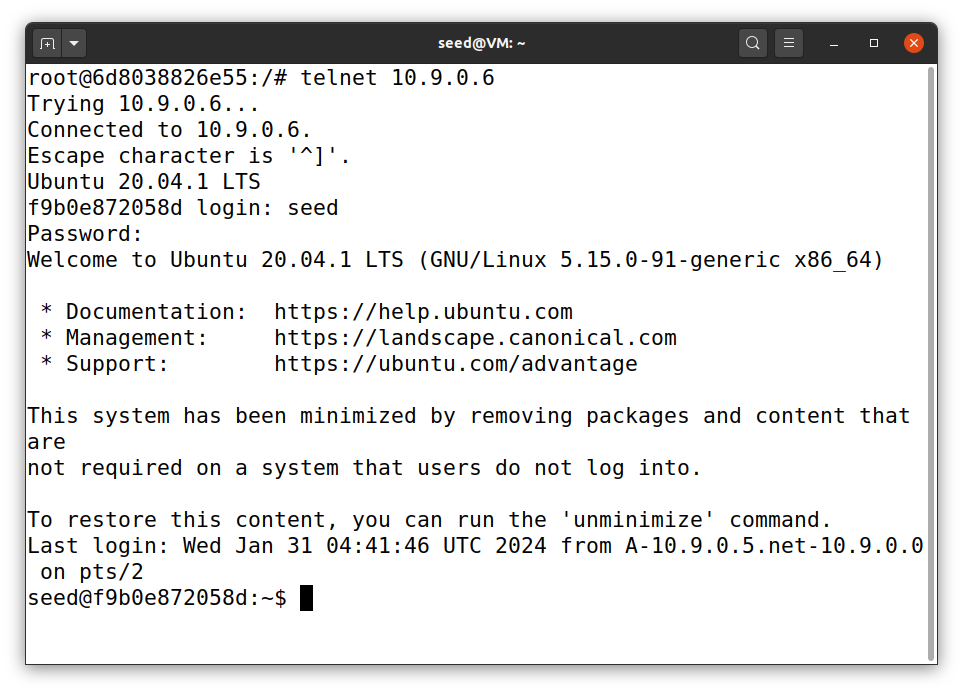
This is same what we did in step 2 , turning on the ip\_forward =1 and then ping machine from A to B and B to A we get this output.



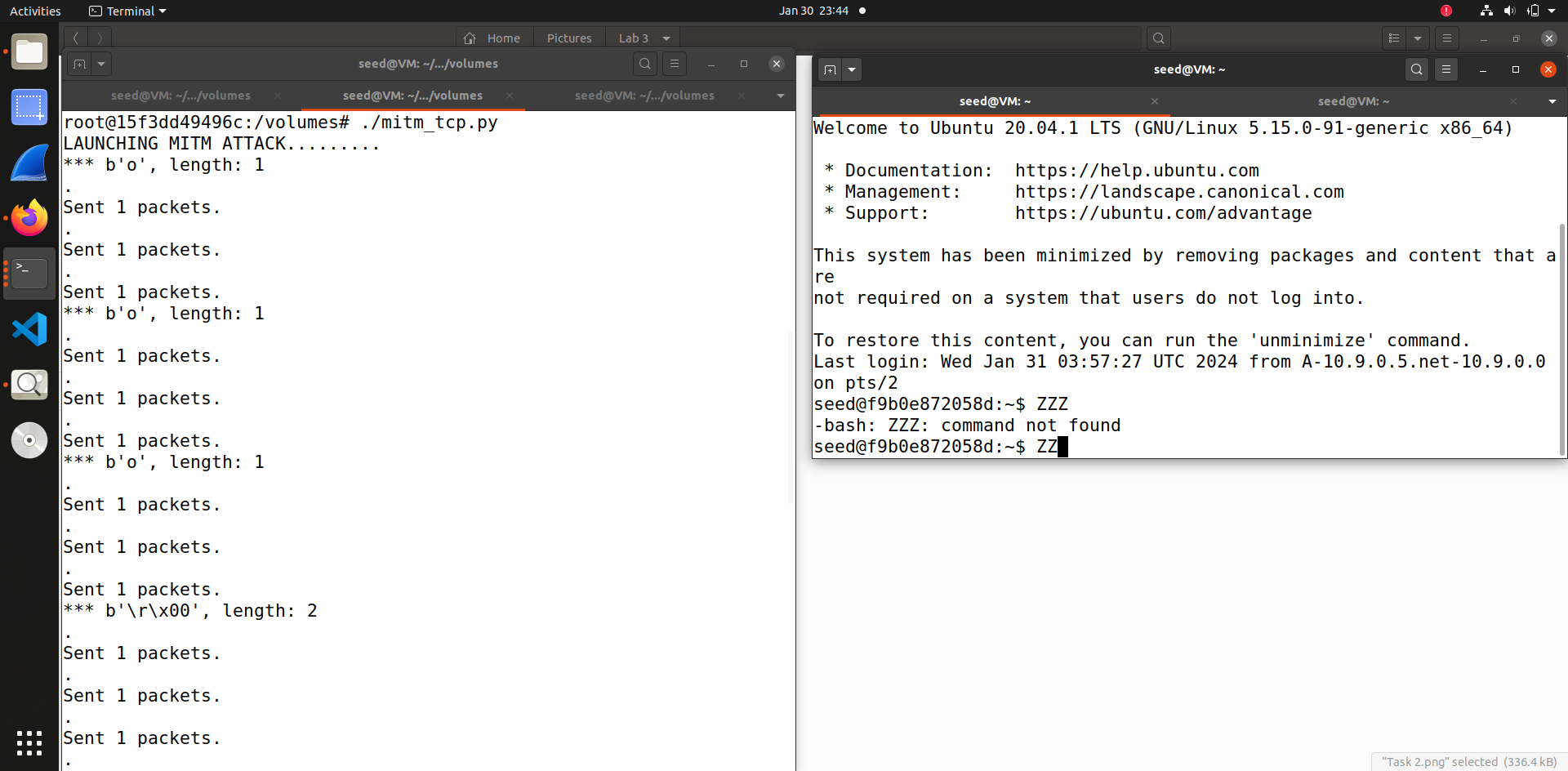
**Step 4 - Launch the MITM attack**

****

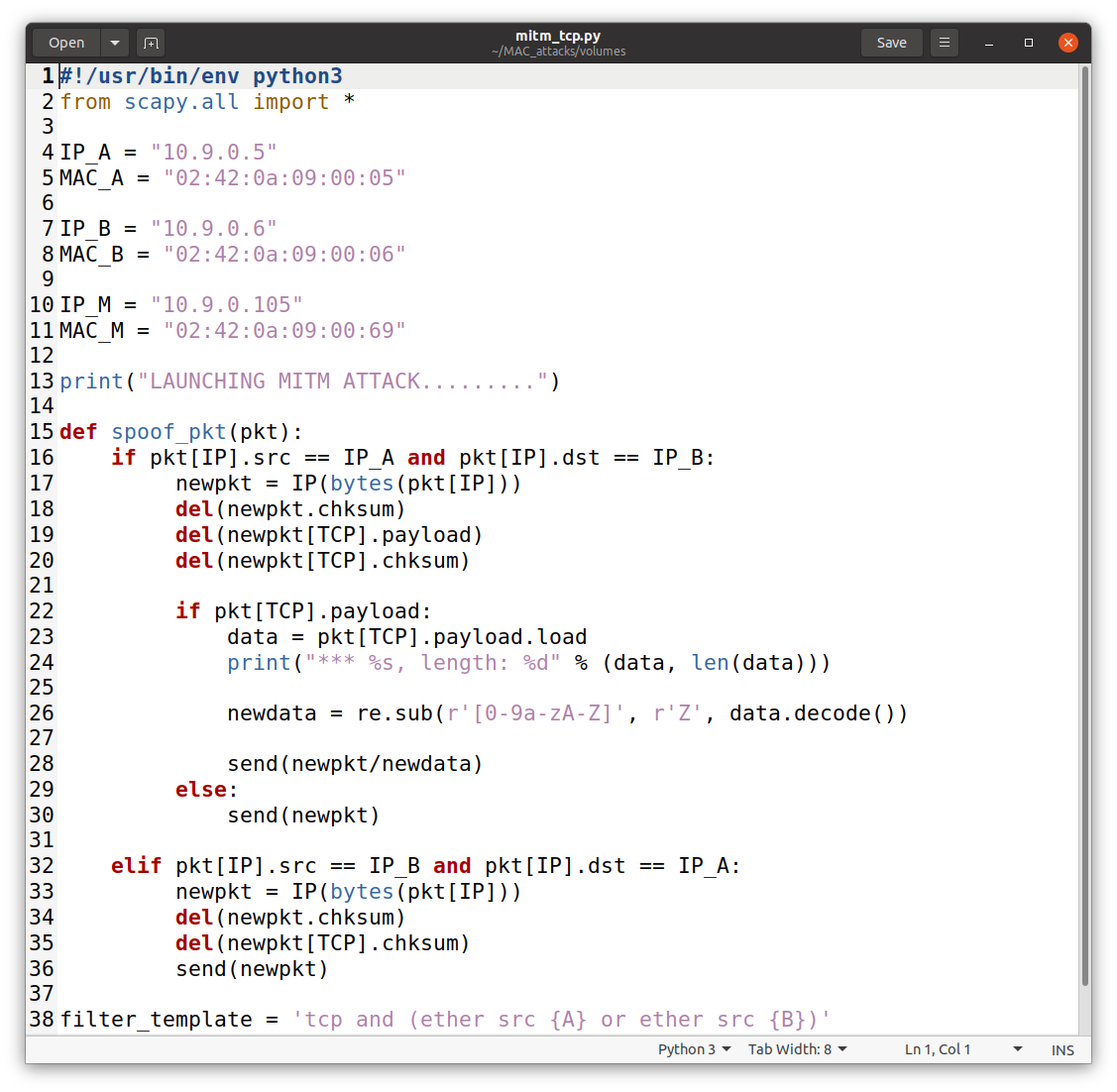
This is the step where we launch the attack so first of all we turn of the ip\_forward that is set it 0.



Then we telnet data between A and B. Assume that A is the telnet and B is the Telnet Server. So we connect to telnet server.

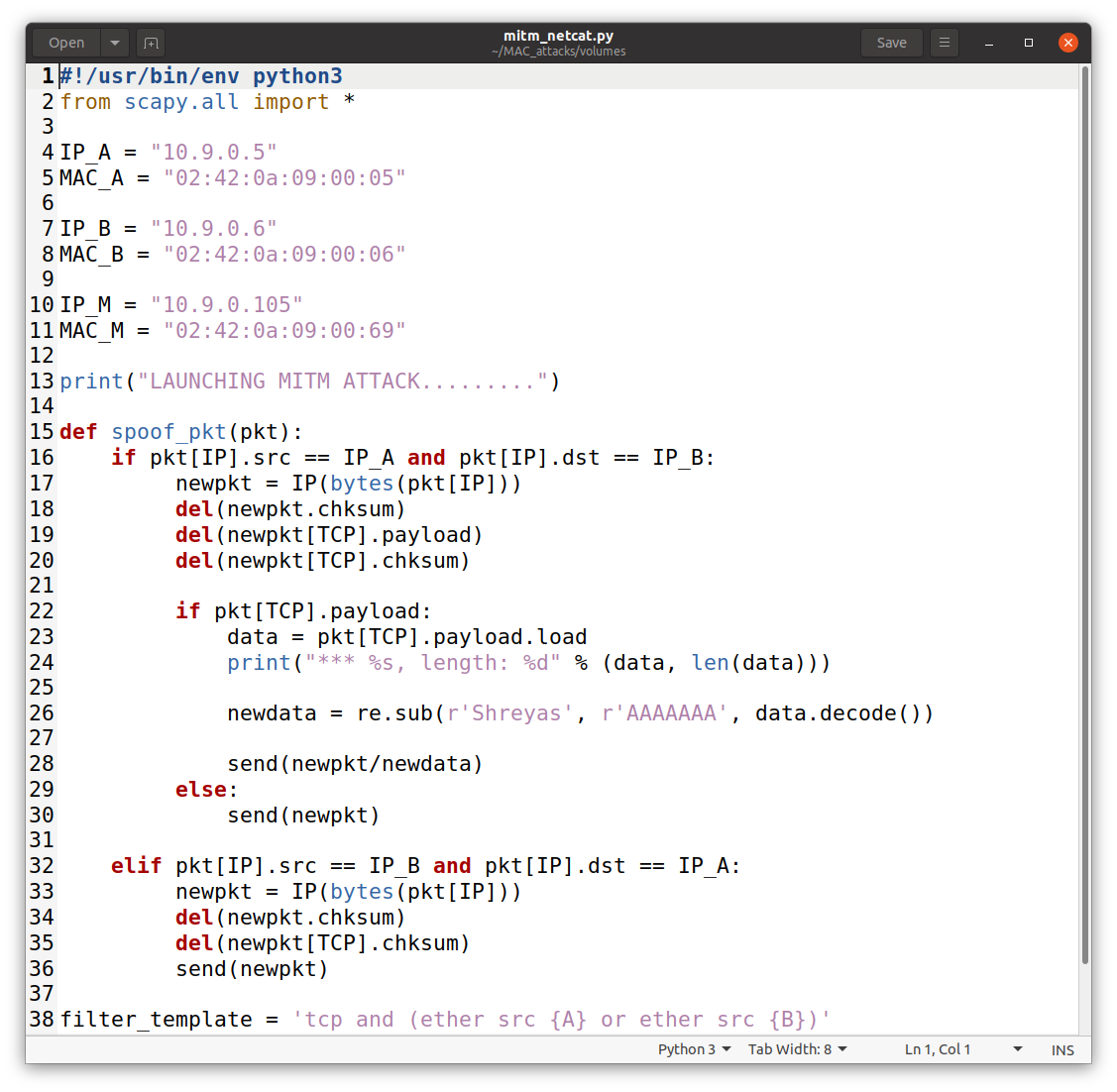


As you can see from the screenshot above when we try to type anything on A’s machine it is been replaced with ZZZ. Thus the attacker keeps intercepting packets send from A to B and replaces them.

This is the code to replace every key we try to type in A machine will be replaced by Z

**Task 3 : MITM Attack on Netcat using ARP Cache Poisoning**

This task is similar to previous task, but in this task we make the communication between A and B using netcat instead of telnet. Also in this task we replace the all letter of first name with that many number of A’s. The code for it is below -



In the screenshot below you can see that first I run the above code in Attacker machine and then send make connection between Machine A and Machine B using netcat. After that as my first name is Shreyas, you can see that it is been replaced by series of A only that name is being replaced other messages are received as it is on B machine. Thus through this we can conclude that the attack was successful.

