**COMPUTER NETWORK SECURITY**

**LAB-3**

**ARP CACHE POISONING ATTACK LAB**

NAME: VISHWAS M

SRN: PES2UG20CS390

SEC: F

DATE:17/09/2022

Task 1: ARP Cache Poisoning:

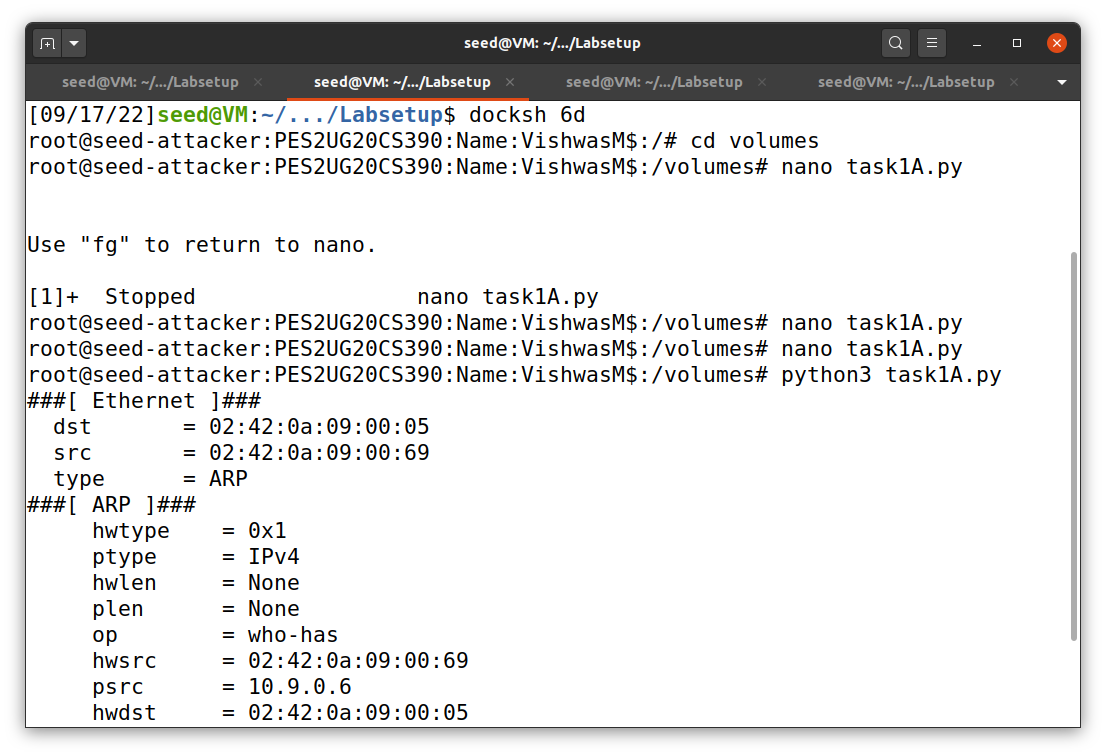
In this task, we have three machines (containers), A, B, and M. We use M as the attackermachine. We would like to cause A to add a fake entry to its ARP cache, such that B’s IP addressis mapped to M’s MAC address. We can check a computer’s ARP cache using the followingcommand. If you want to look at the ARP cache associated with a specific interface, you can usethe -i option.

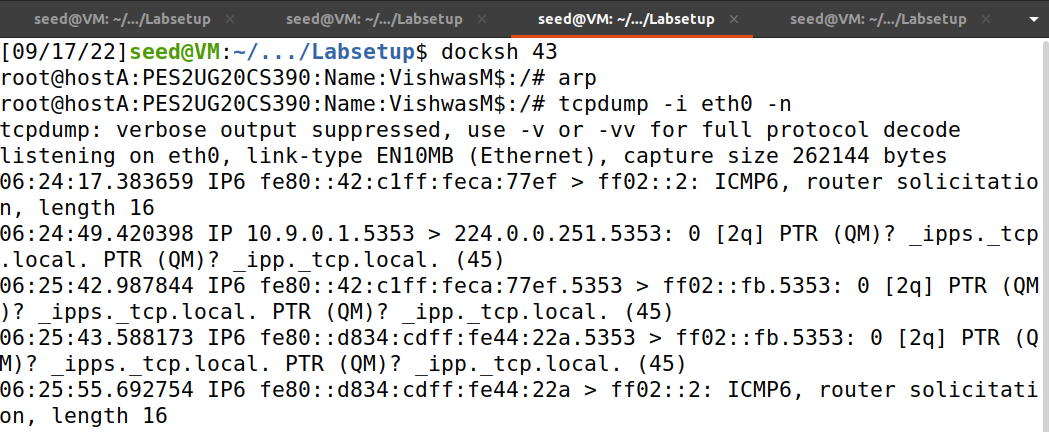
Task 1.A: Using ARP request

On host M, construct an ARP request packet and send it to host A. Check whether M's MAC address is mapped to B's IP address in A's ARP cache

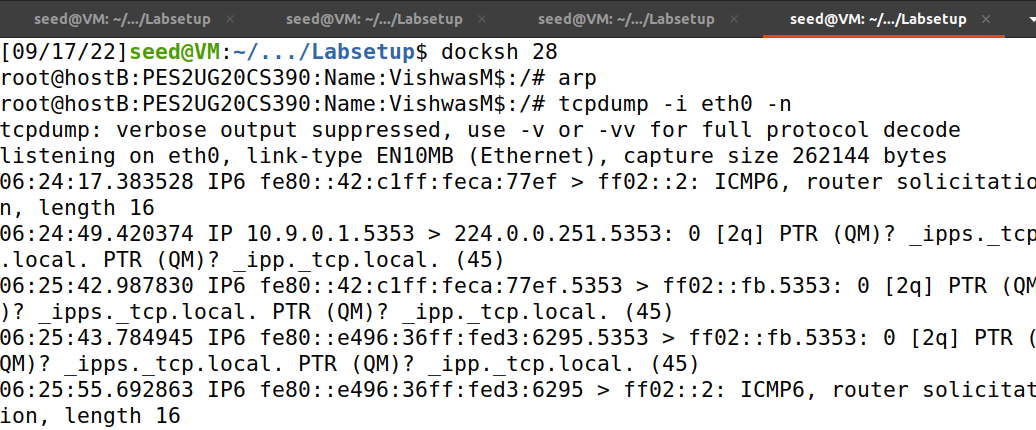
1. Without Ether:

Before running the attack:

Host M:

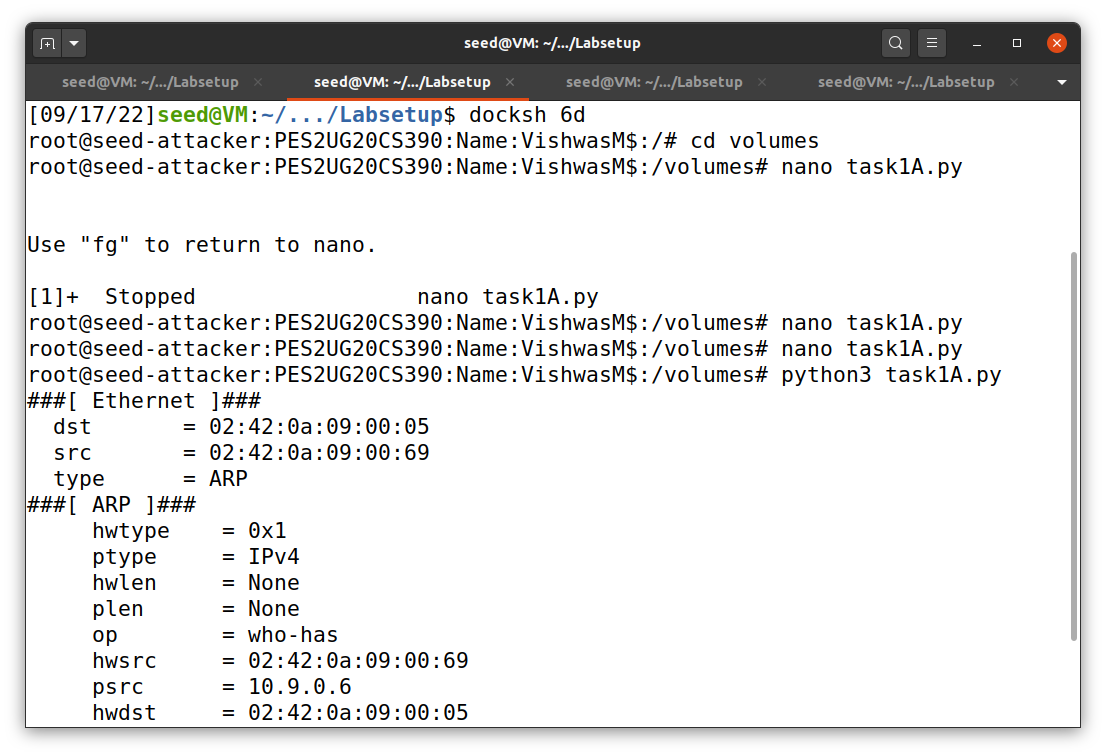
Host A:

Host B:

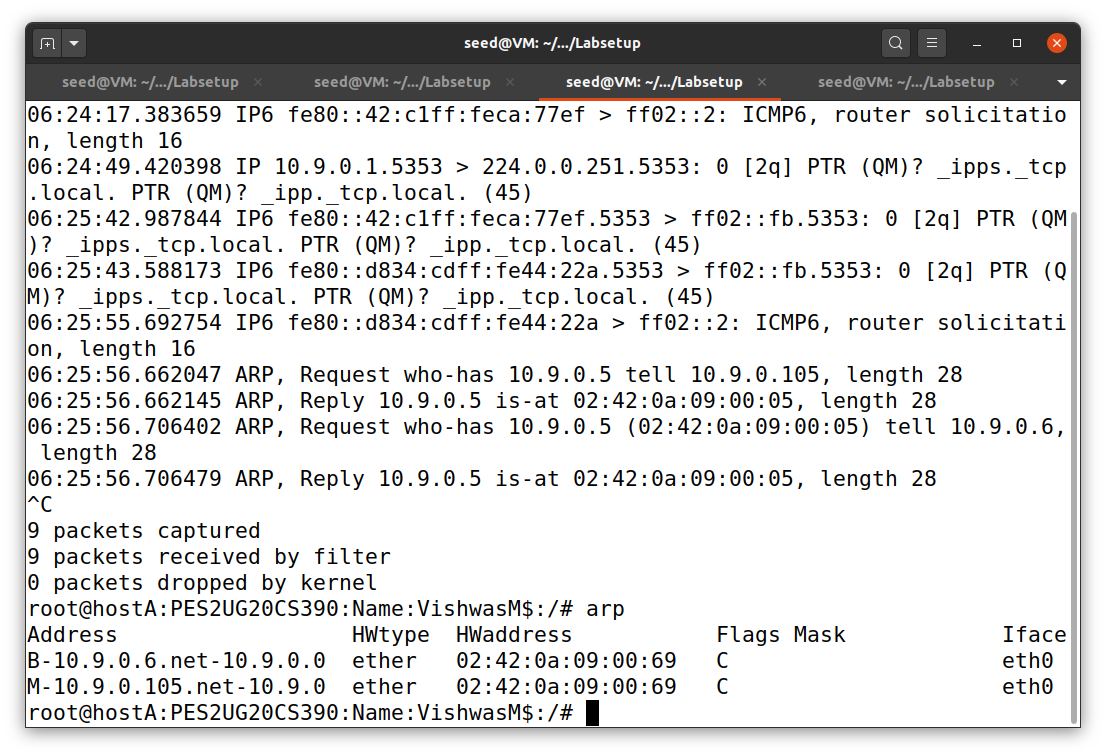
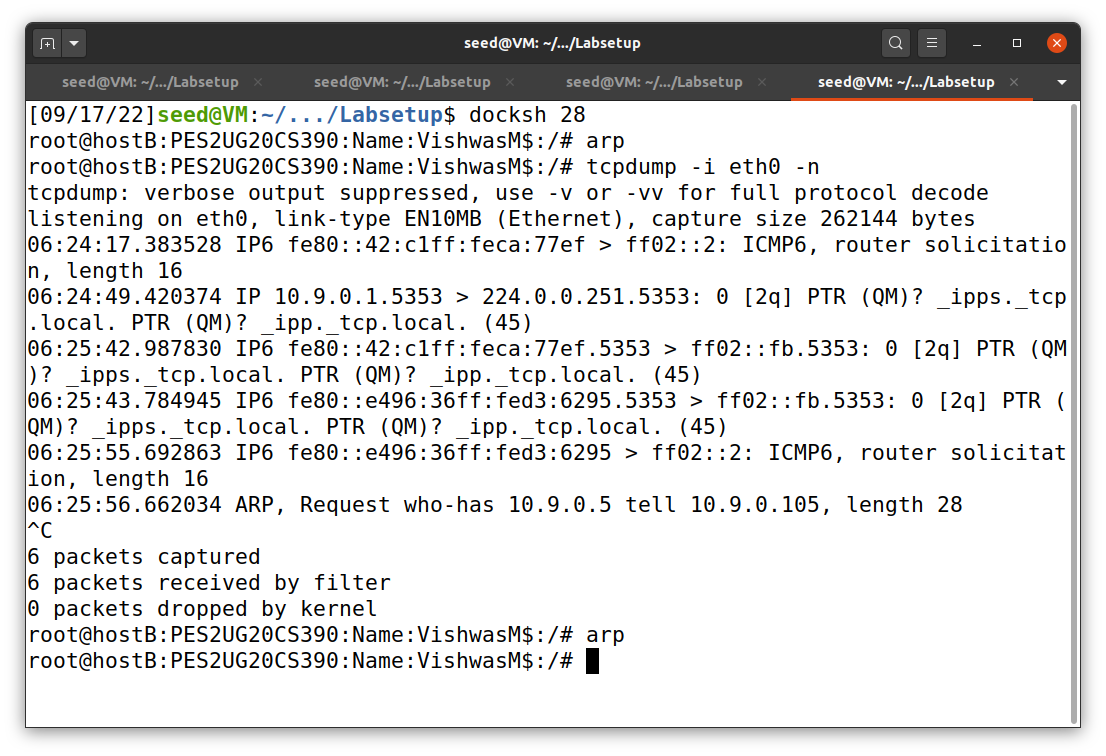


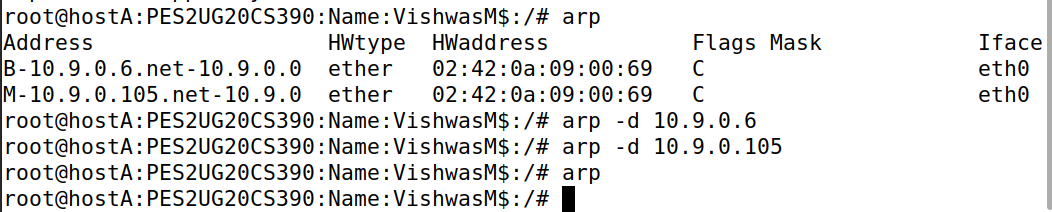
After running the attack:

Host M:



Host A:

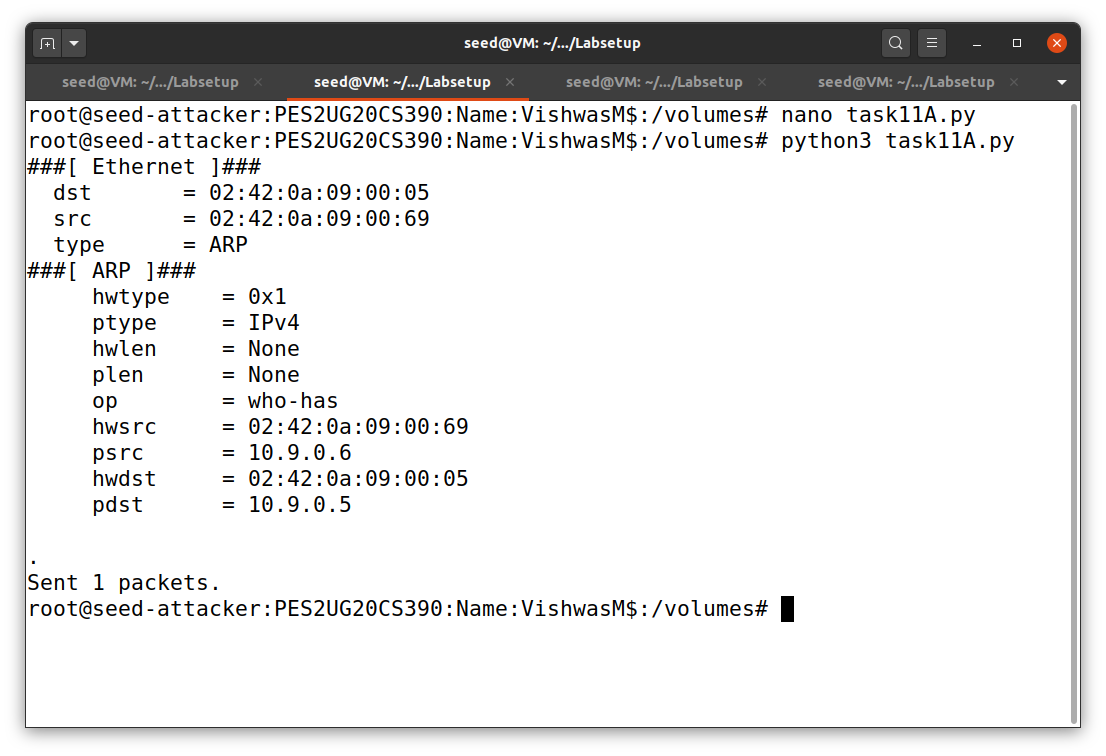
Host B:

Delete the ARP cache:

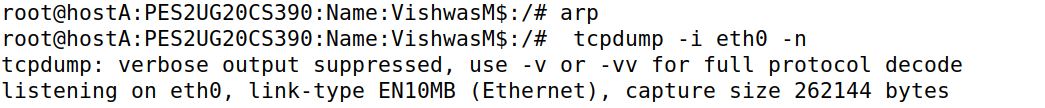
With Ether:

Before the attack:

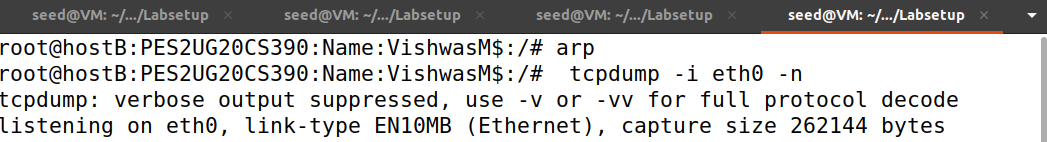
Host M:



Host A:

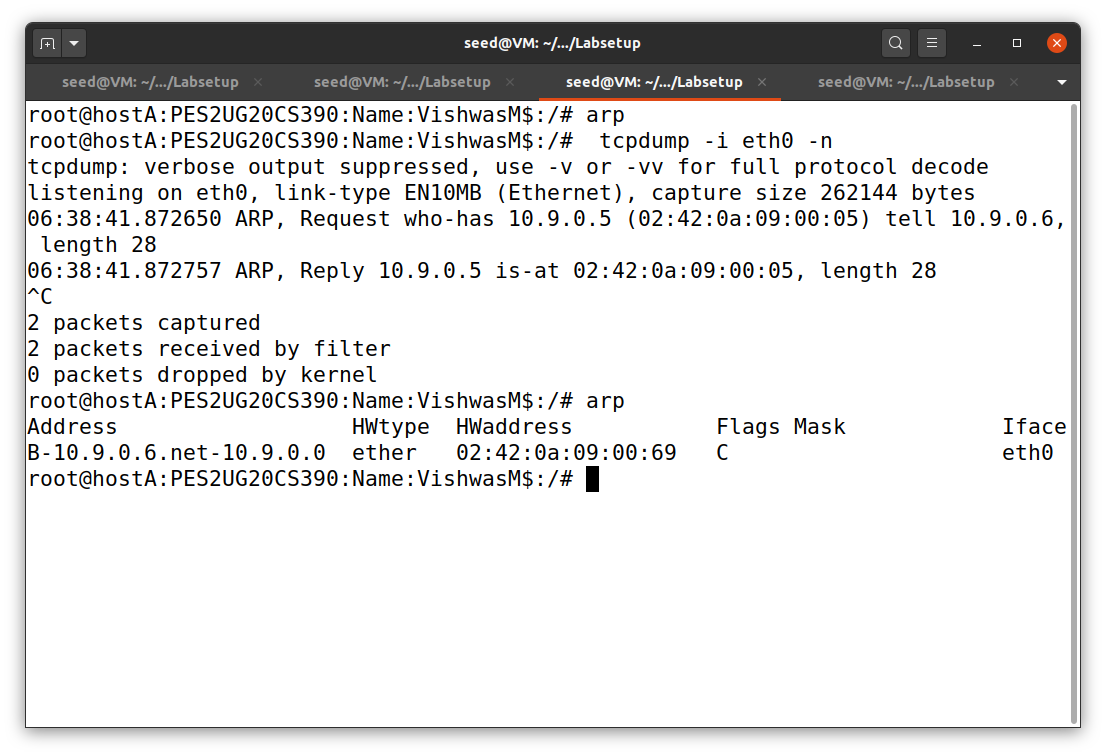


Host B:

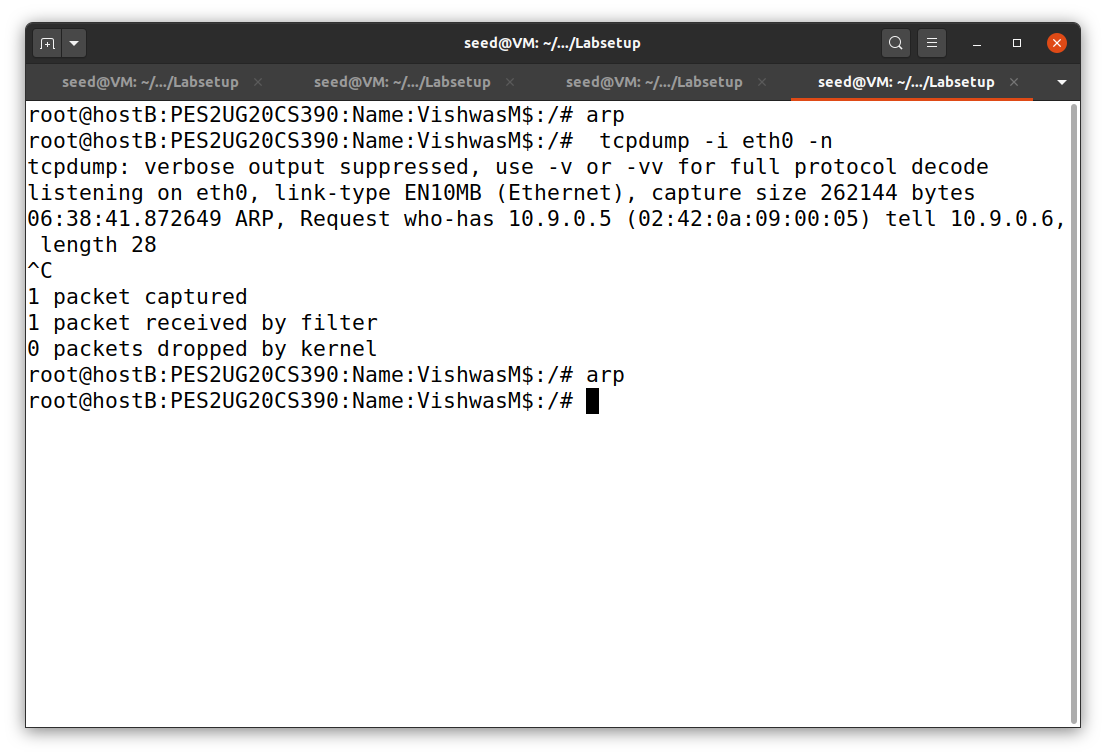


After the attack:

Host A:



Host B:



Questions:

1.What does the ‘op’ in the screenshot of the attacker machine signify? What is its default value?

Ans: Default value will be 1. This op value tells whether this is an ARP request or ARP reply packet.

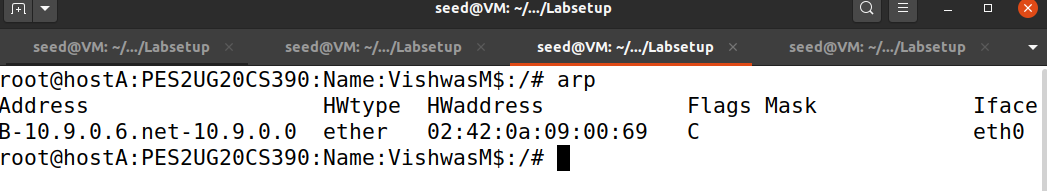
2.What was the difference between the ARP cache results in the above 2 approaches? Why did you observe this difference?

Ans: The cache didn’t get updated in the scenario 2 as IP address was not in the arp cache memory in host A. And ARP cache poisoning is successful when we send ARP reply only when the IP address is in the victim’s ARP cache.

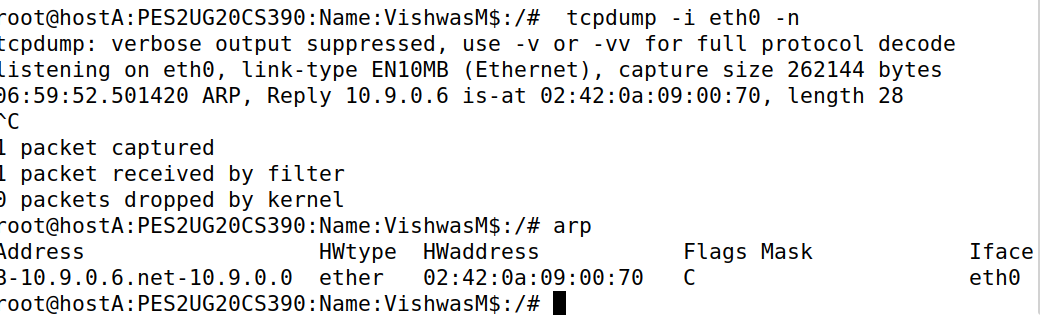
Task 1.B: Using ARP Reply

Scenario 1: B’s IP is already in A’s cache

ARP cache:



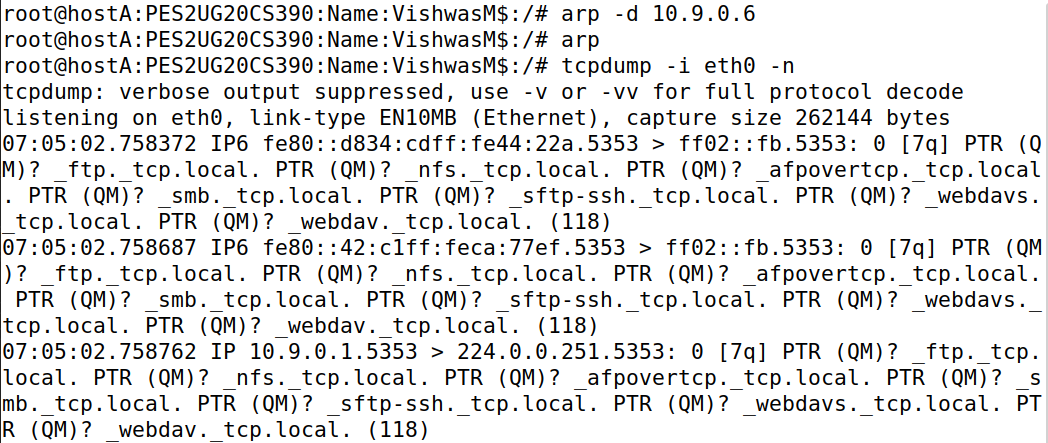
After running the attack:

Host A:

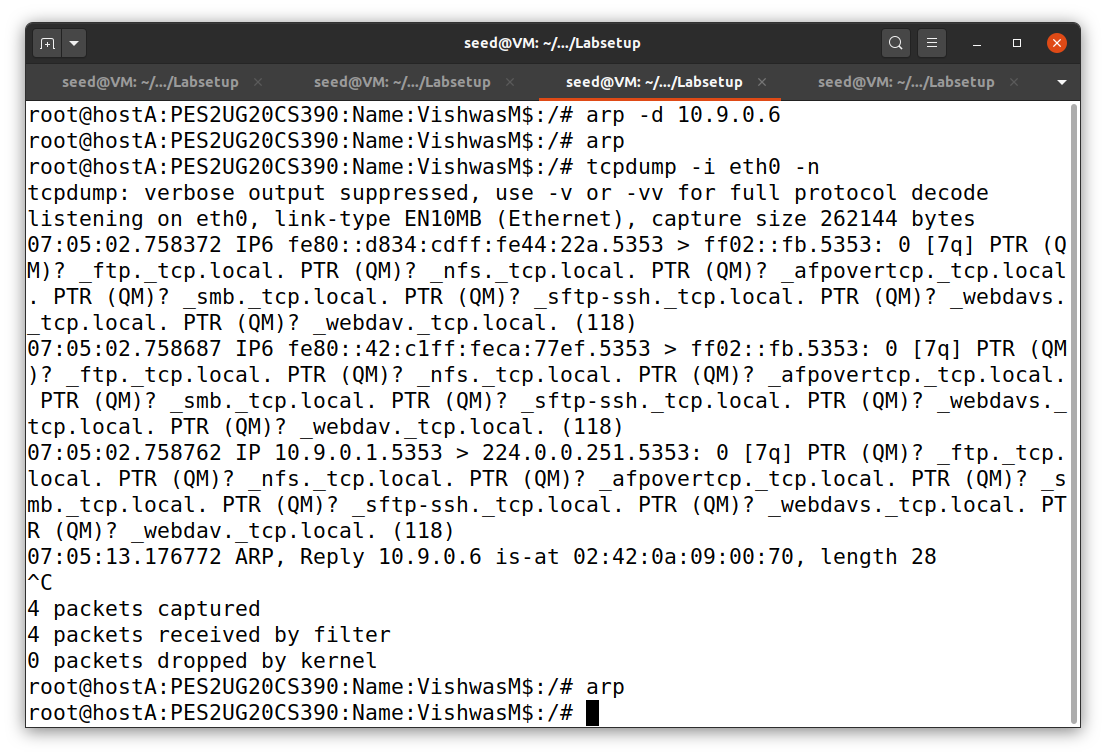
Scenario 2: B’s IP is not in A’s cache

We will clear the arp cache table before performing Scenario 2.

Before:



After:



Question:

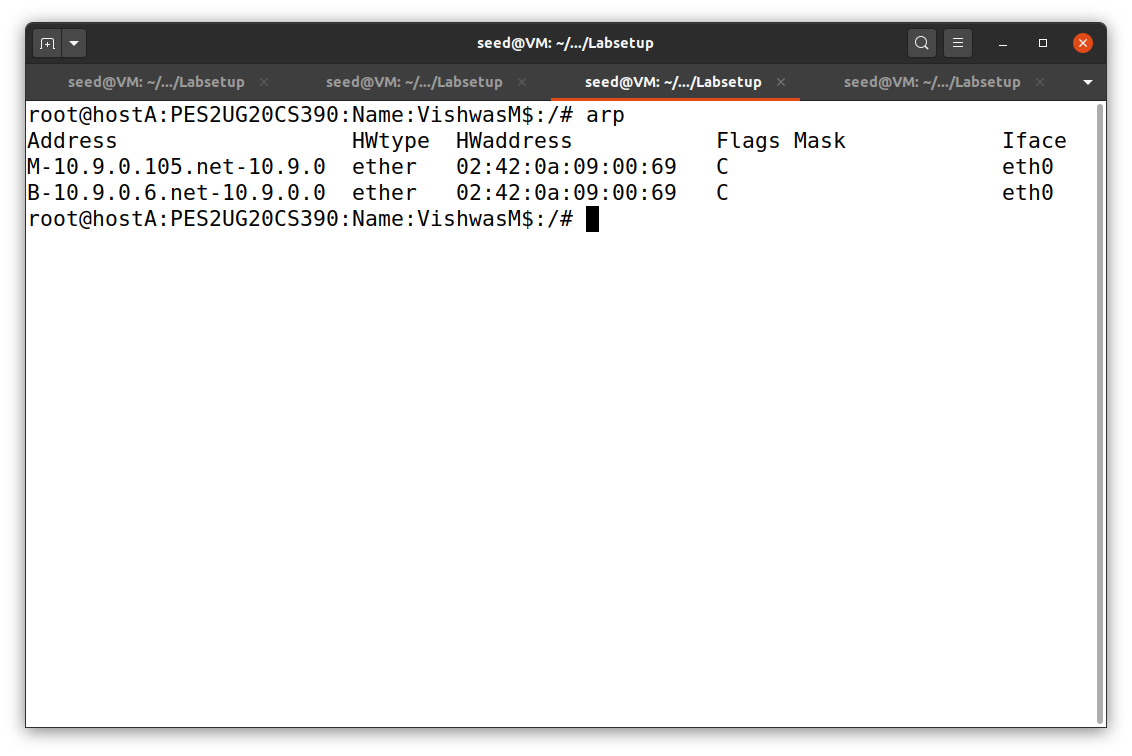
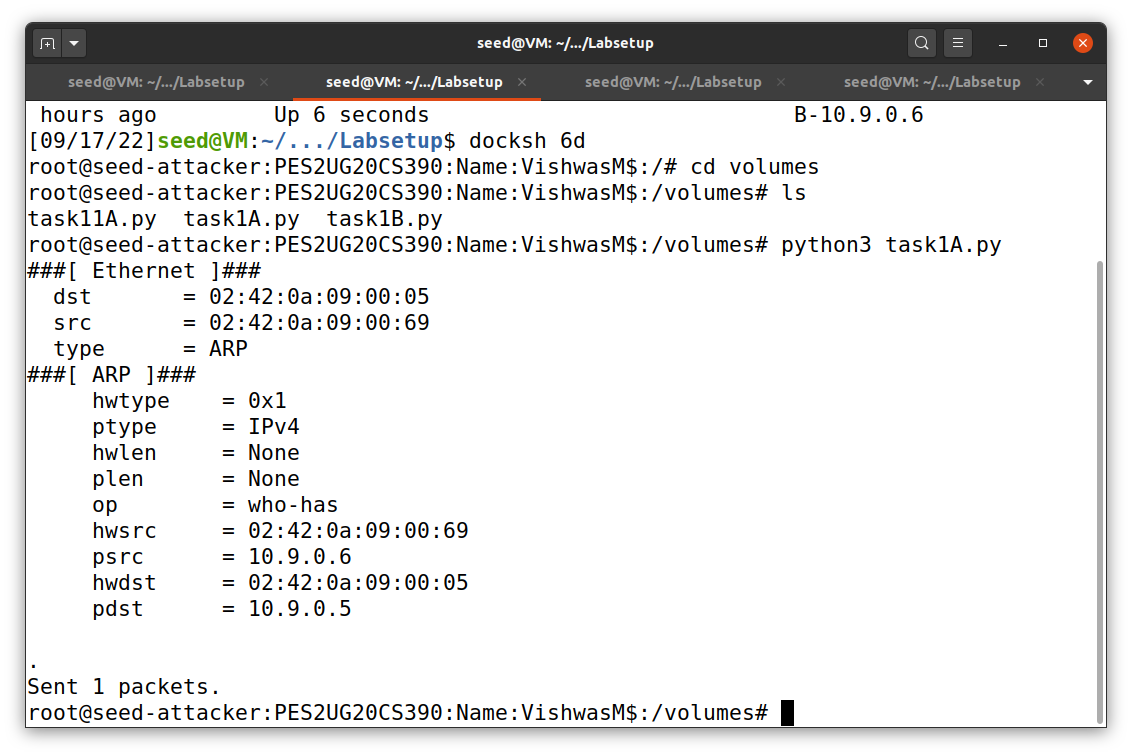
1.What does op=2 mean?

Ans: Op=2 means that the ARP packet is a reply packet.

Task 1.C: Using ARP Gratuitous Message

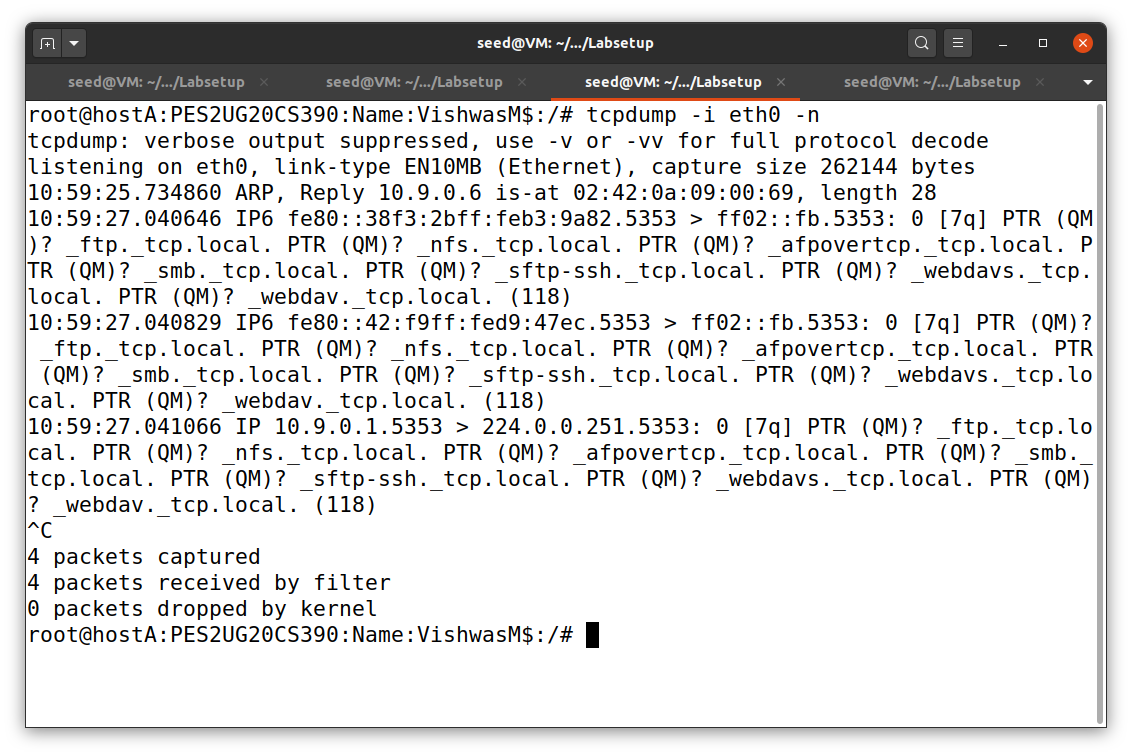
Scenario 1: B’s IP is already in A’s cache

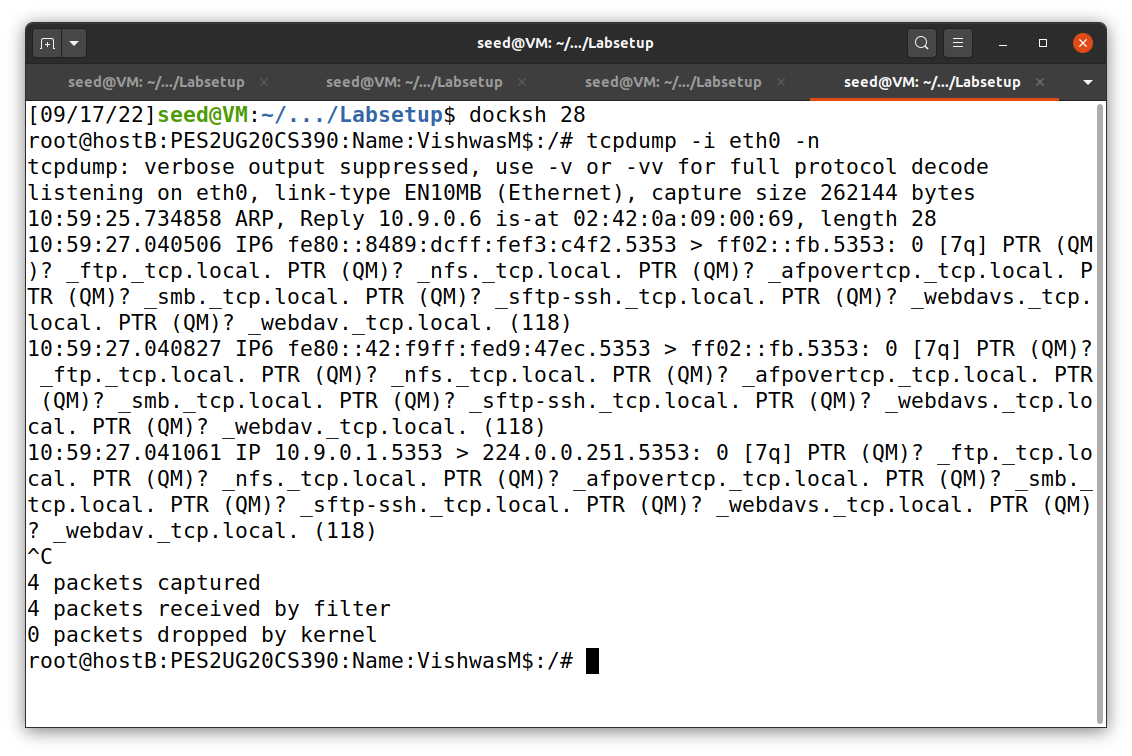
ARP cache:



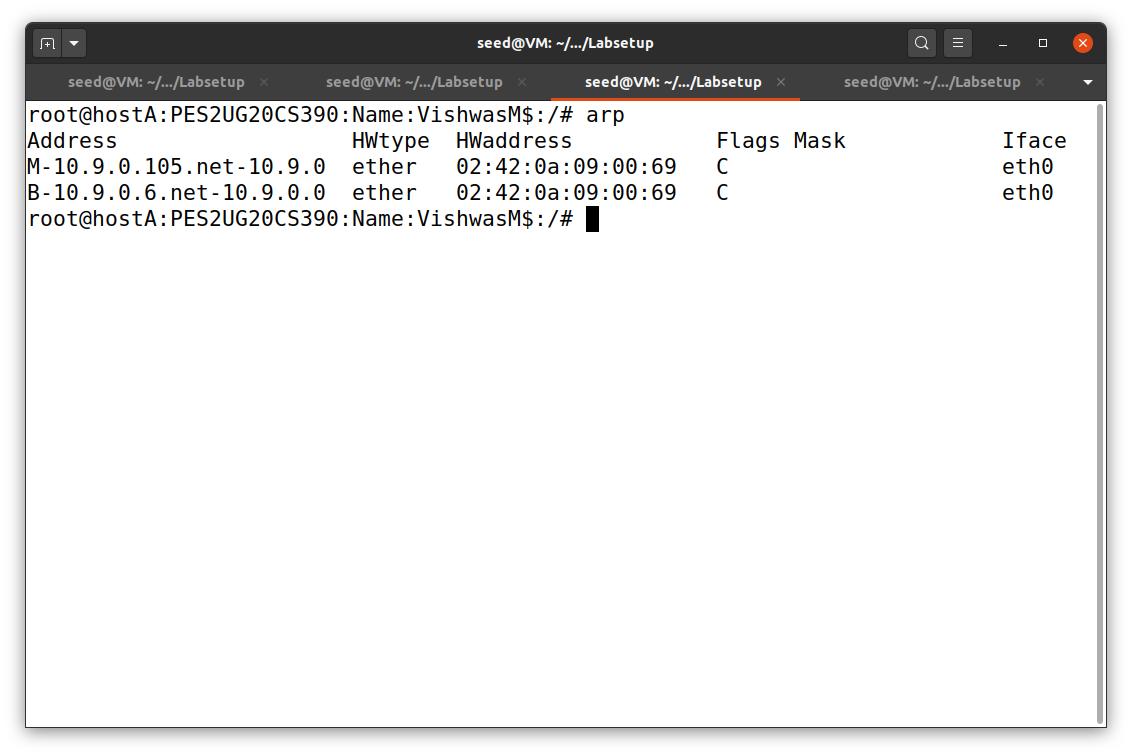
Before:

Host A:



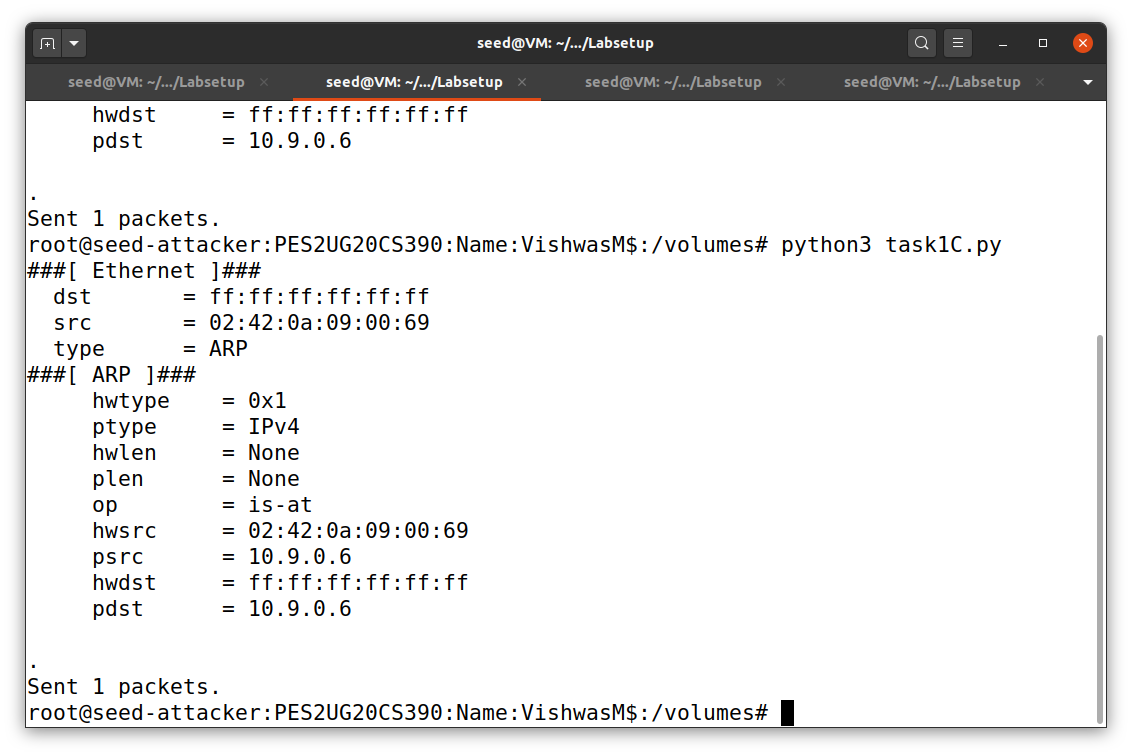
Host B:

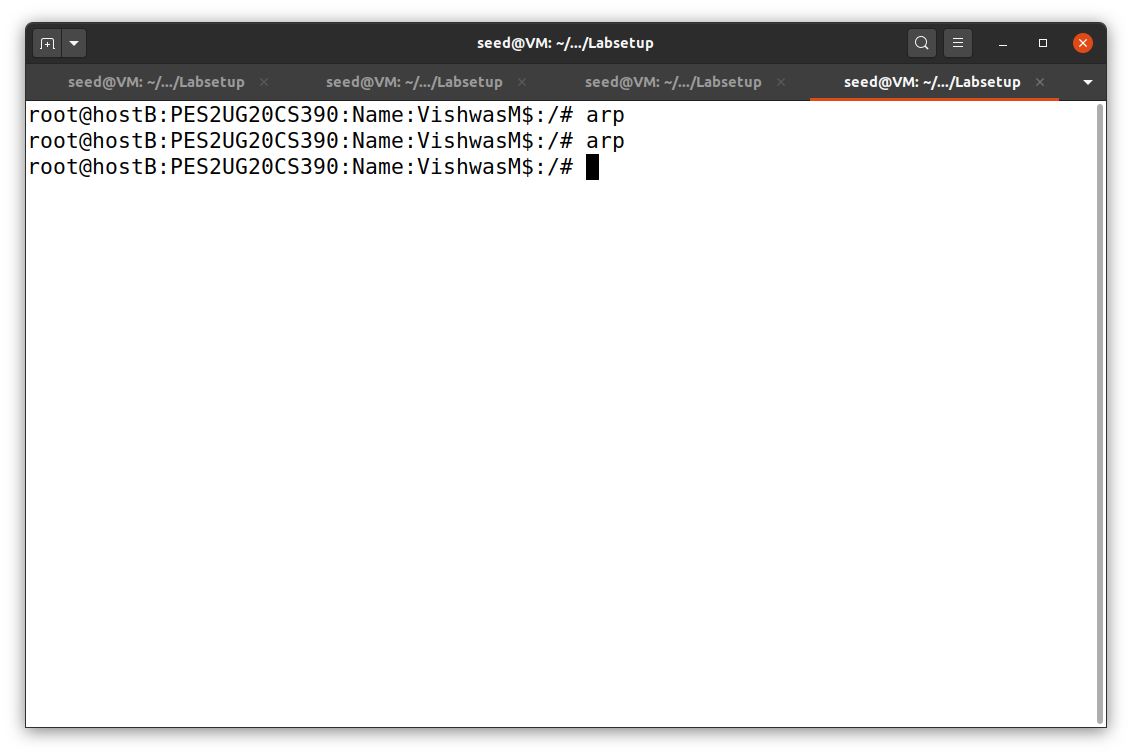
After:

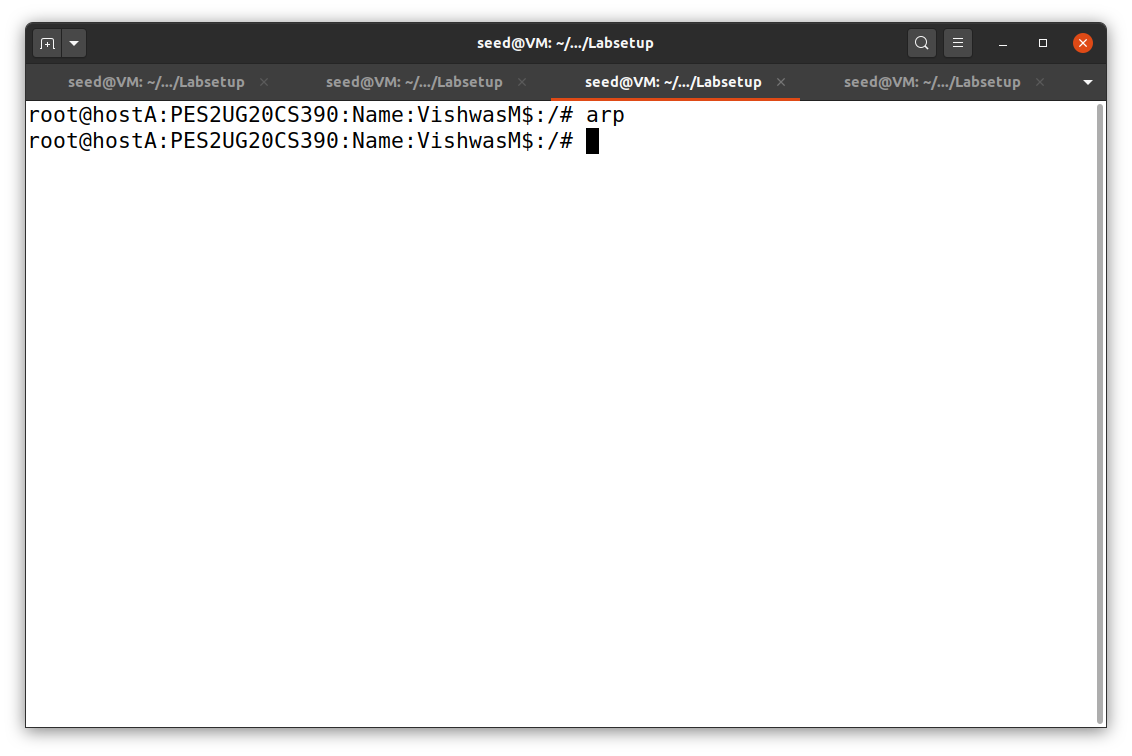


Scenario 2:

We must delete all the entry in the cache before performing scenario 2.

Before:





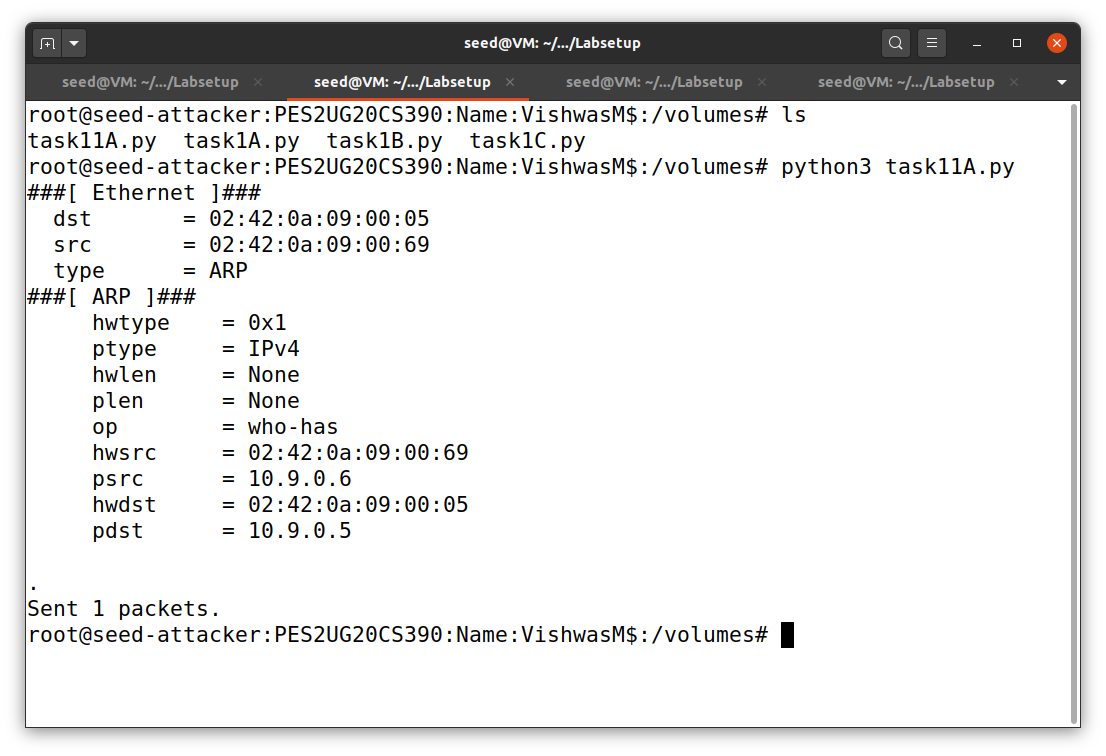
Questions:

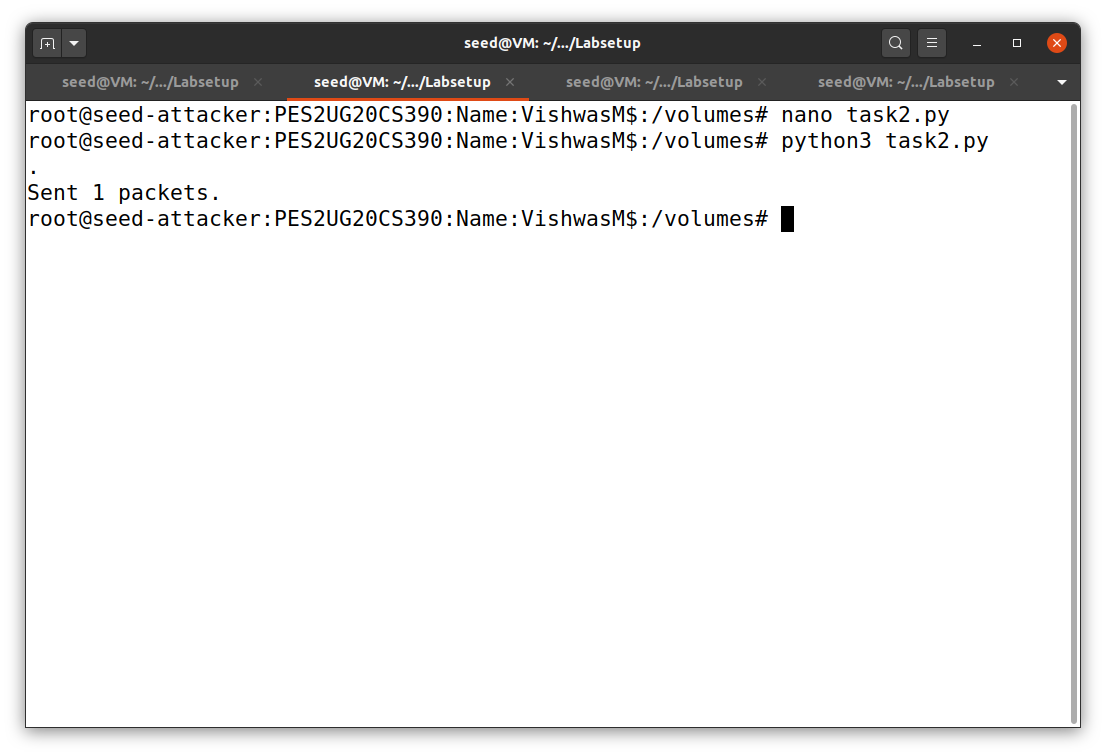
1.Why does VM B’s ARP cache remain unchanged in this approach even though the packet was broadcasted on the network?

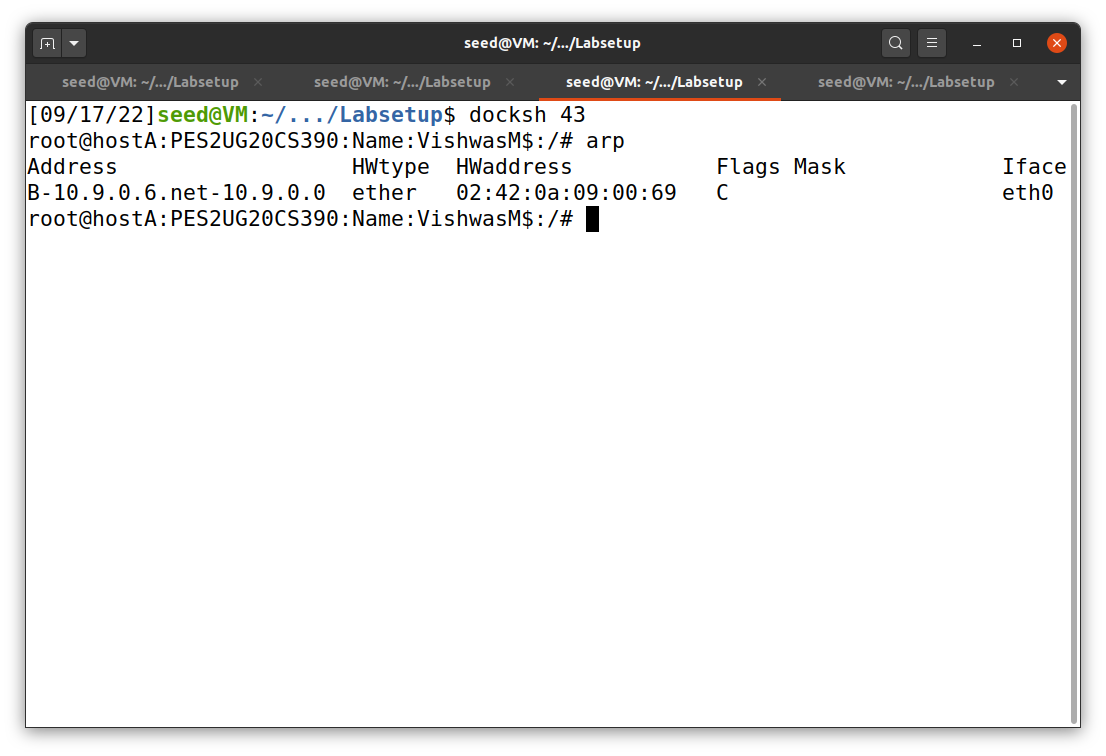
Ans: IP address was not in cache, so the broadcast did not update the IP address.

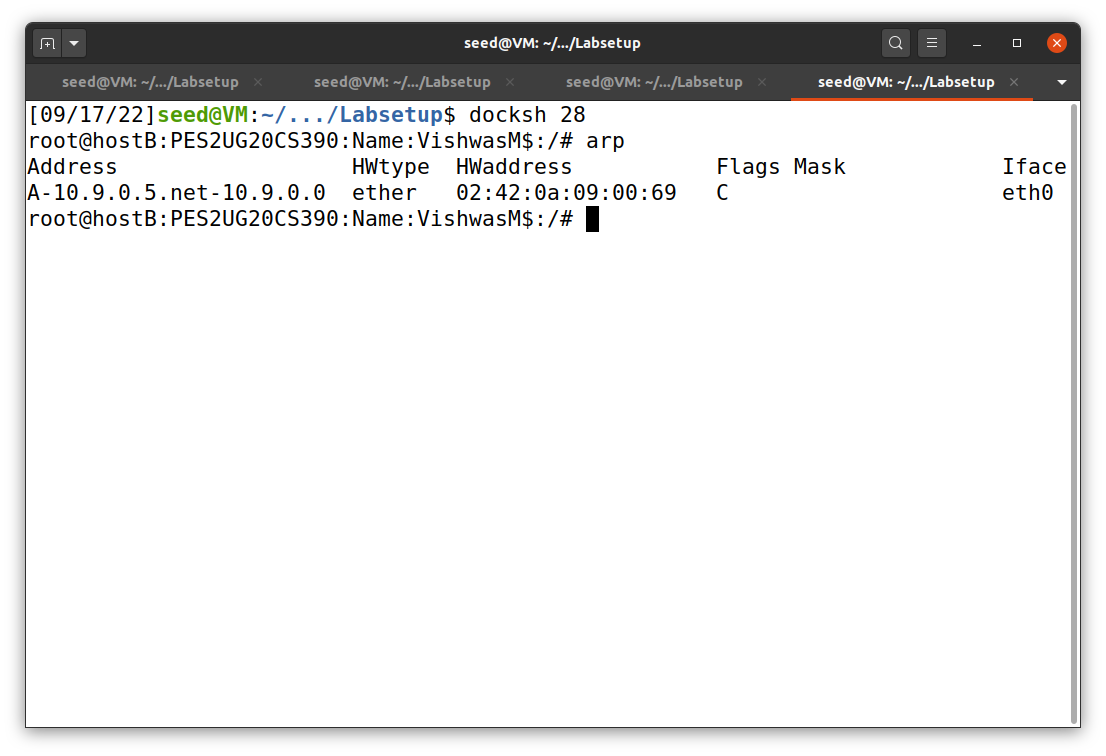
Task 2: MITM Attack on Telnet using ARP Cache Poisoning

Step 1:

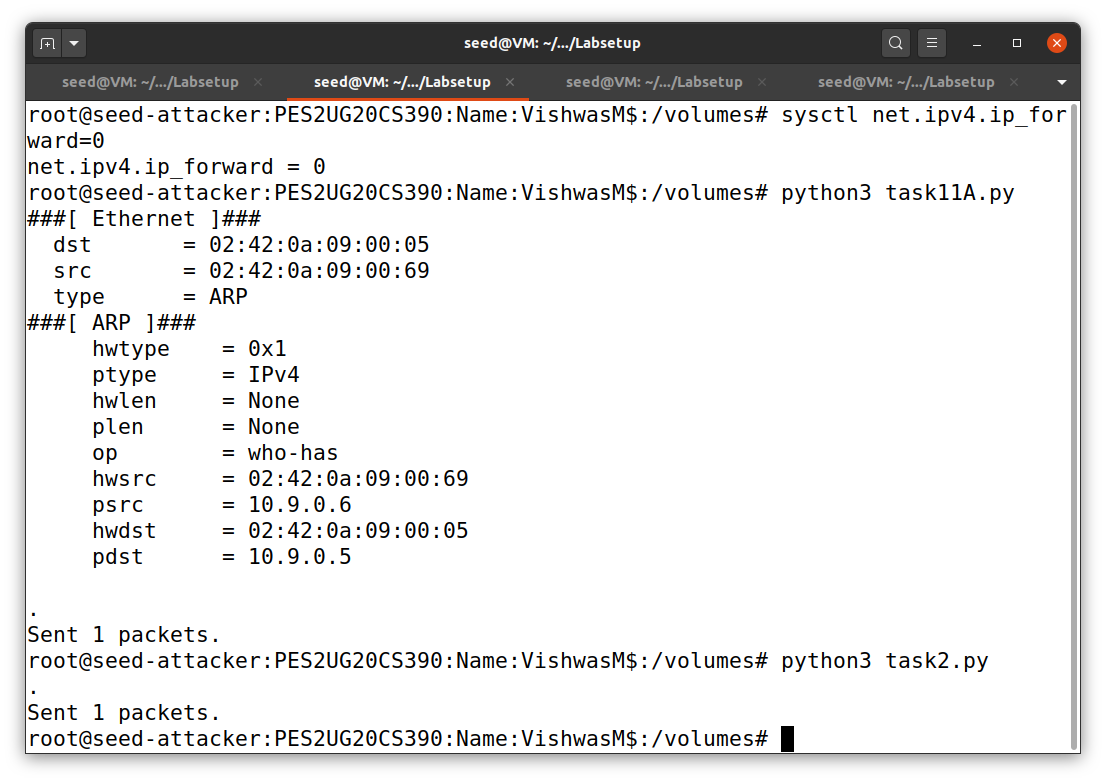
Launch the ARP cache poisoning attack First, Host M conducts an ARP cache poisoning attack on both A and B, such that in A’s ARP cache, B’s IP address maps to M’s MAC address, and in B’s ARP cache, A’s IP address also maps to M’s MAC address. After this step, packets sent between A and B will all be sent to M. We will use the ARP cache poisoning attack from Task 1 to achieve this goal. 

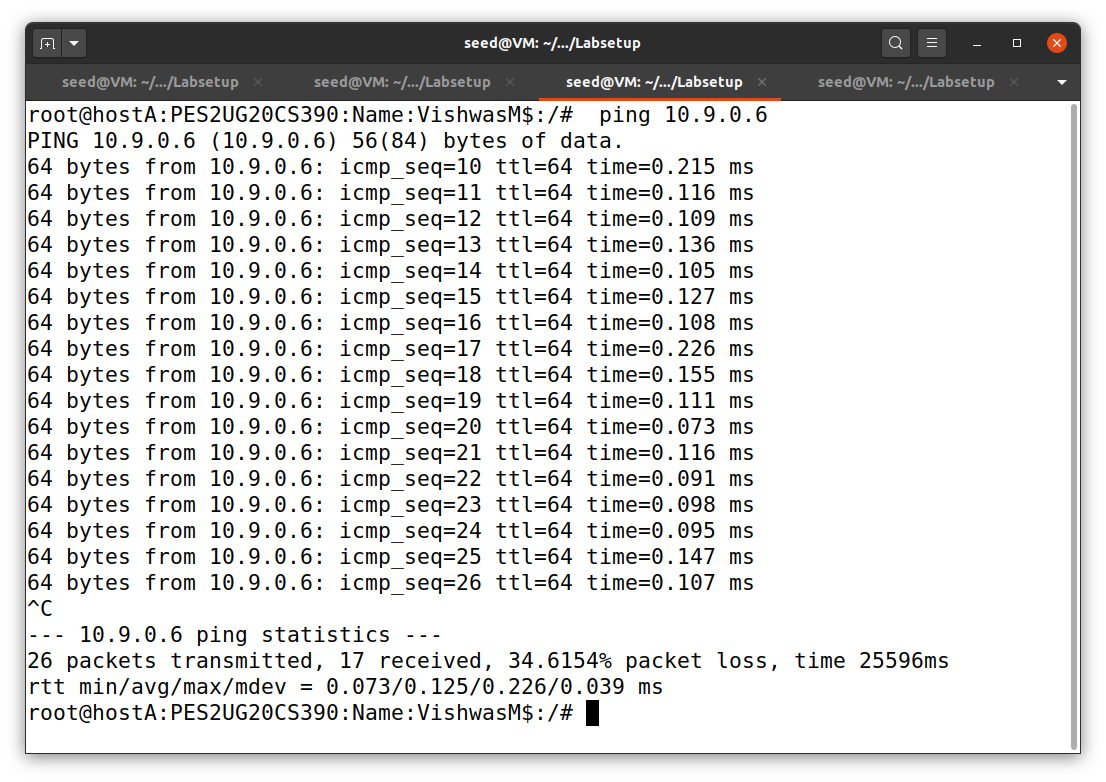


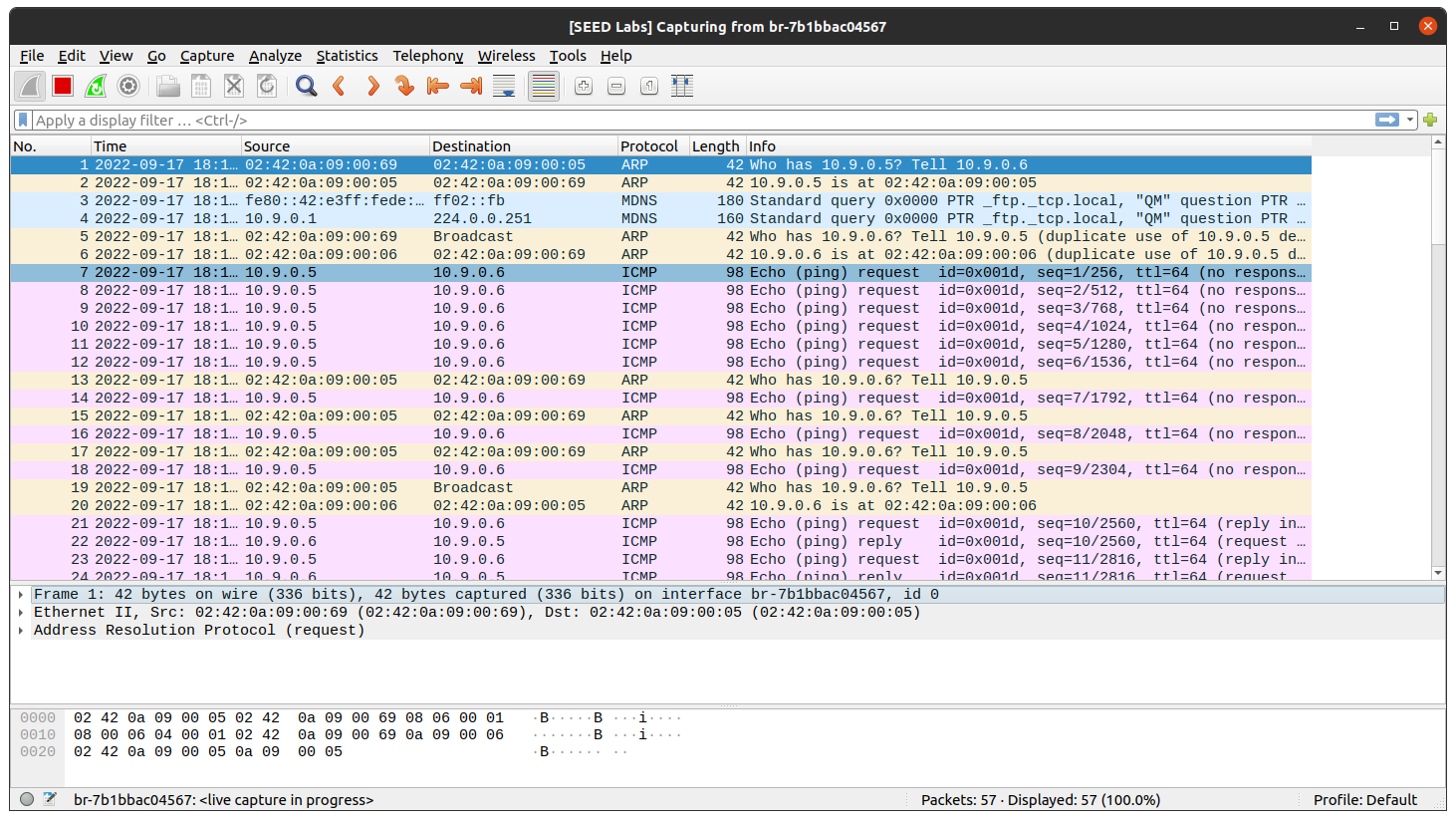




Step 2: Testing





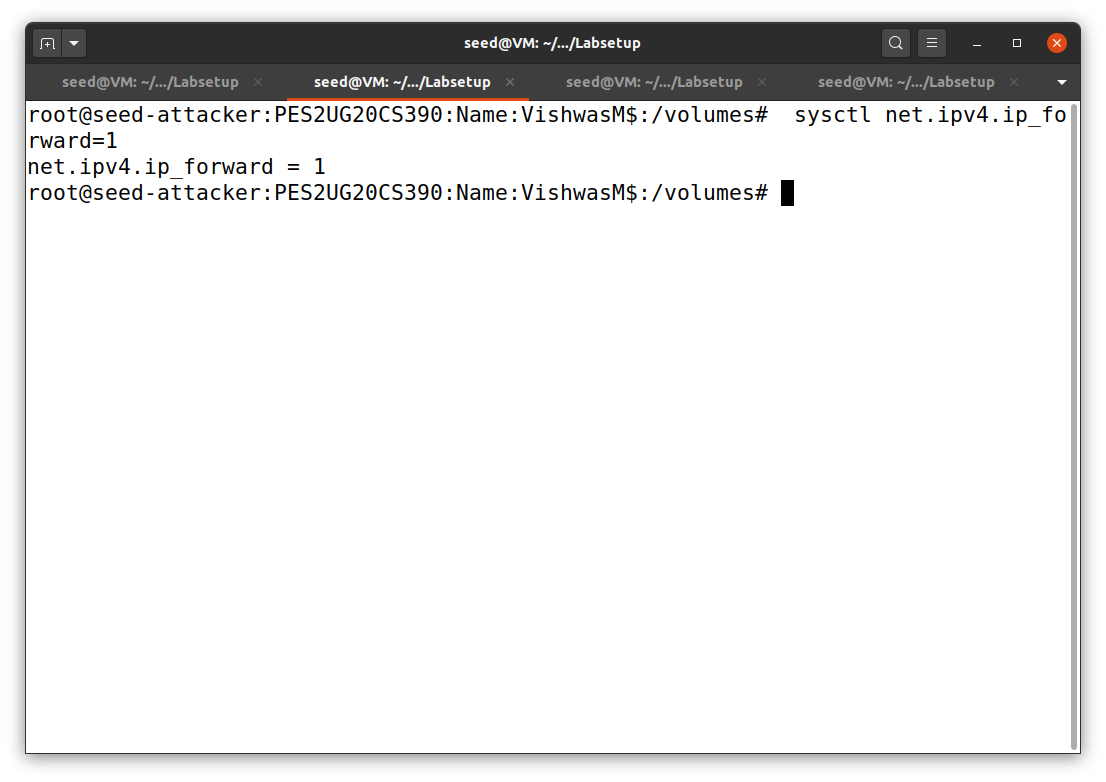


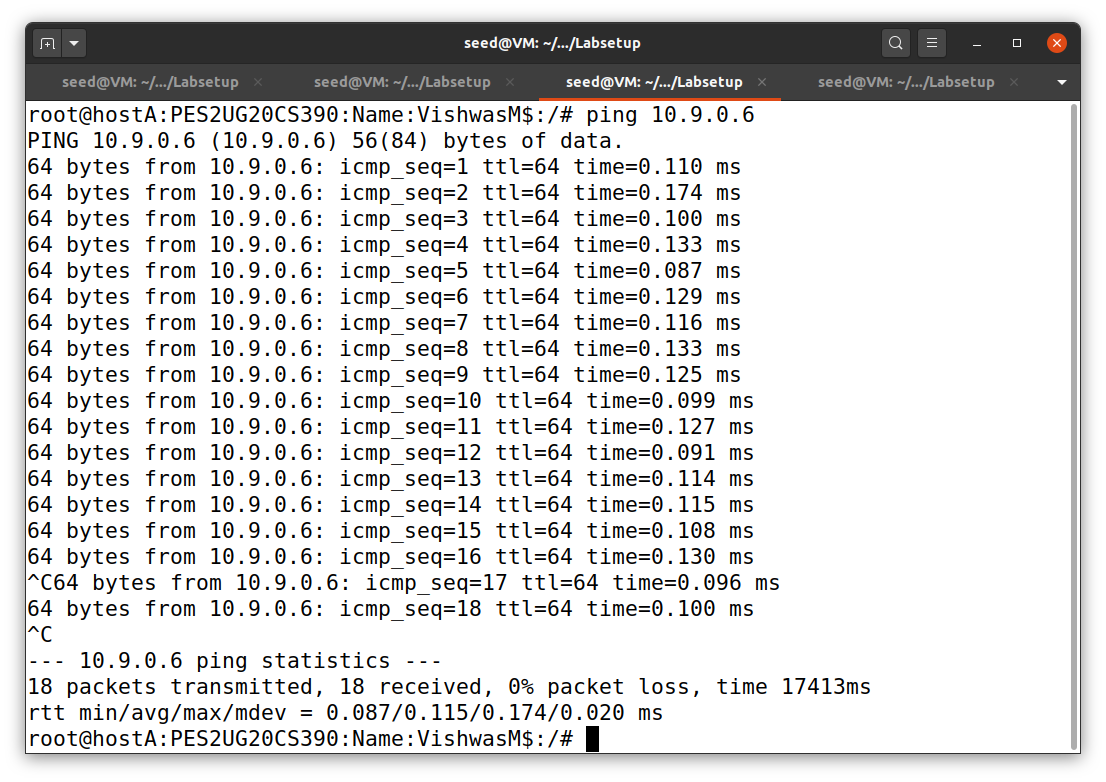
Question:

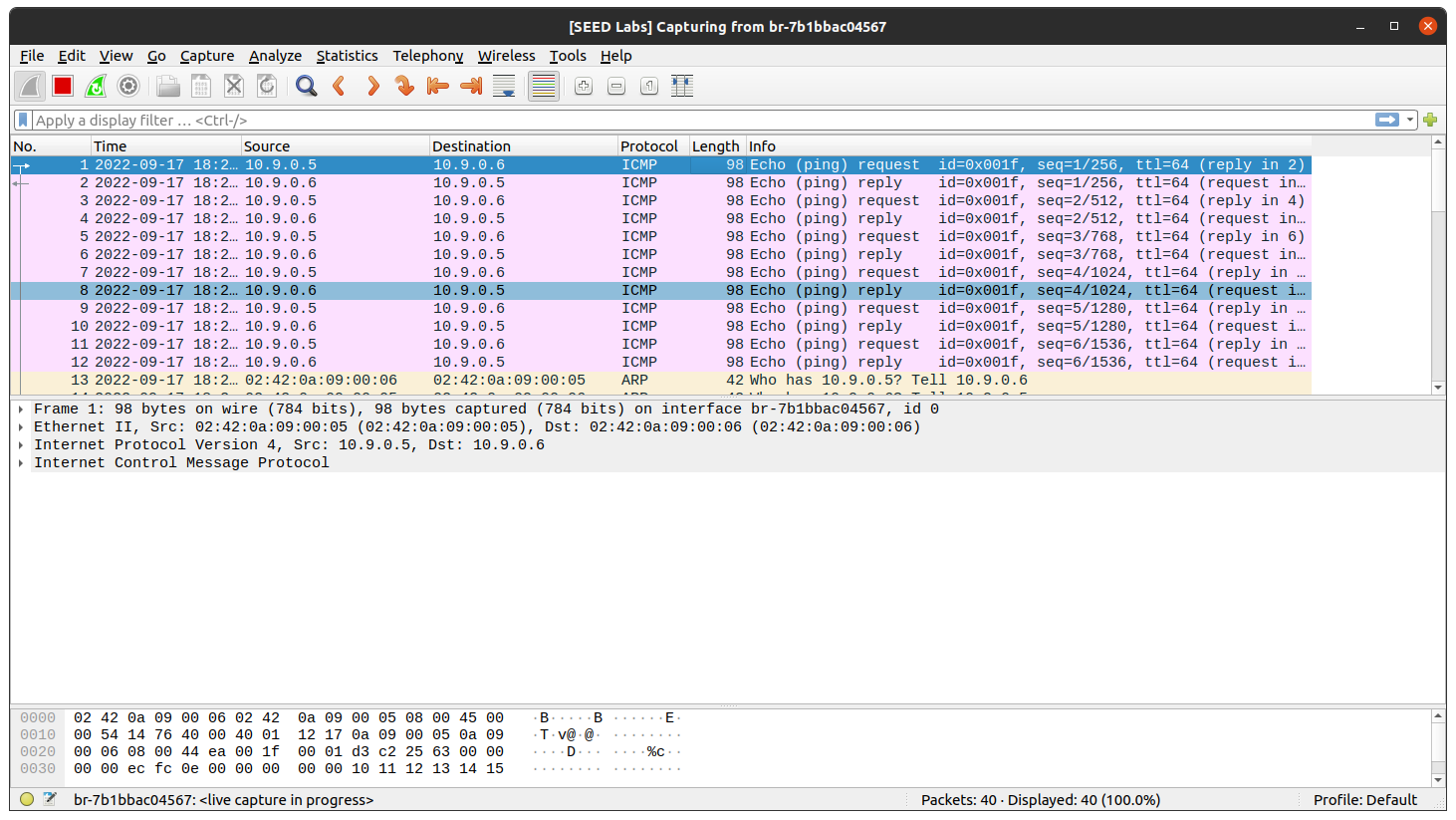
1. What do you observe? Explain

Ans: ARP protocol is observed in the Wireshark.

Step 3 - Turn on IP Forwarding





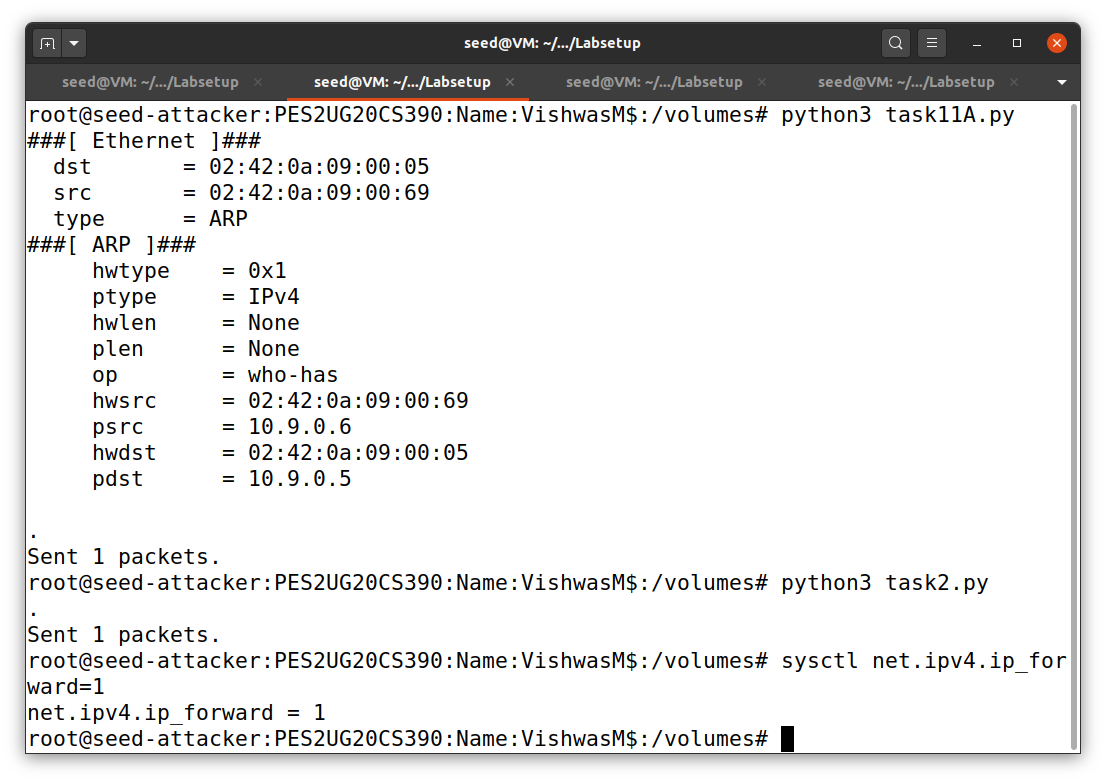


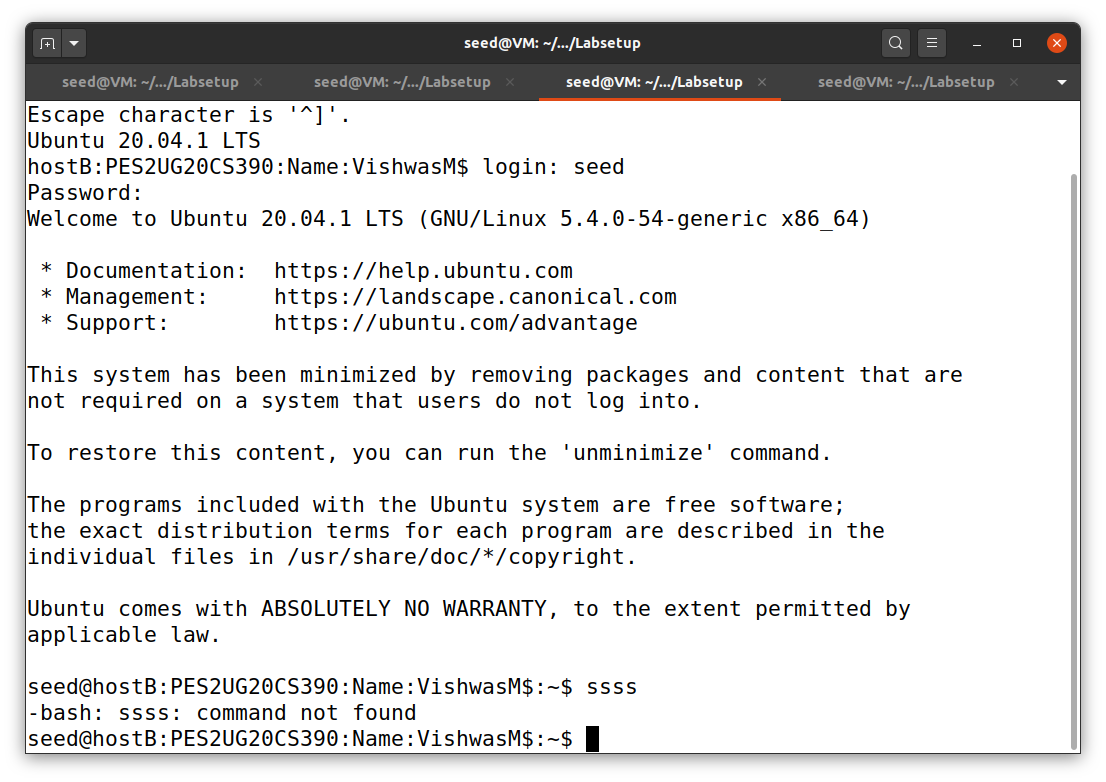
Question:

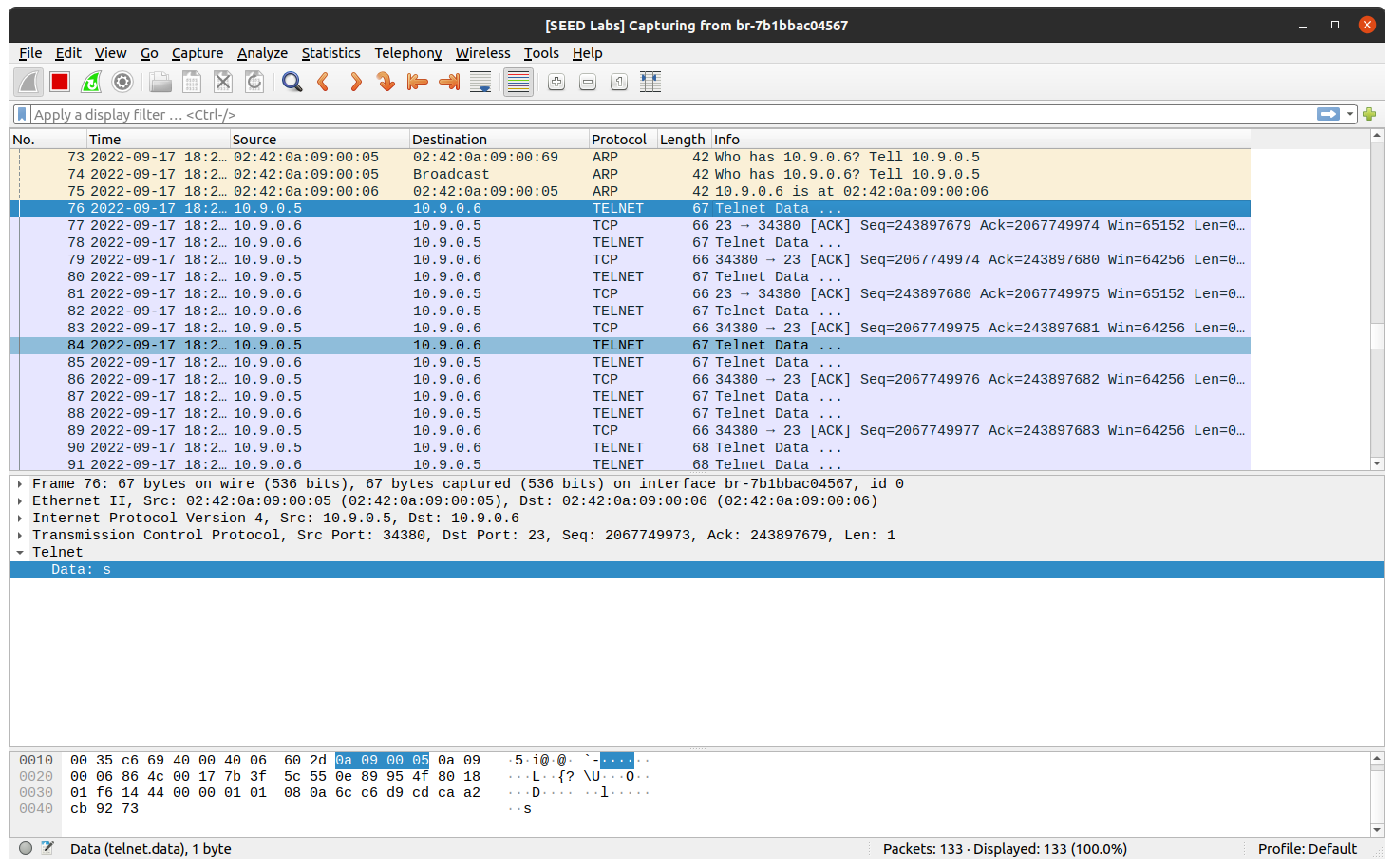
1.Compare the results between the above two steps.

Ans: In the second scenario we have no ARP packets sent. We can just see the ICMP packets travelling across two hosts.

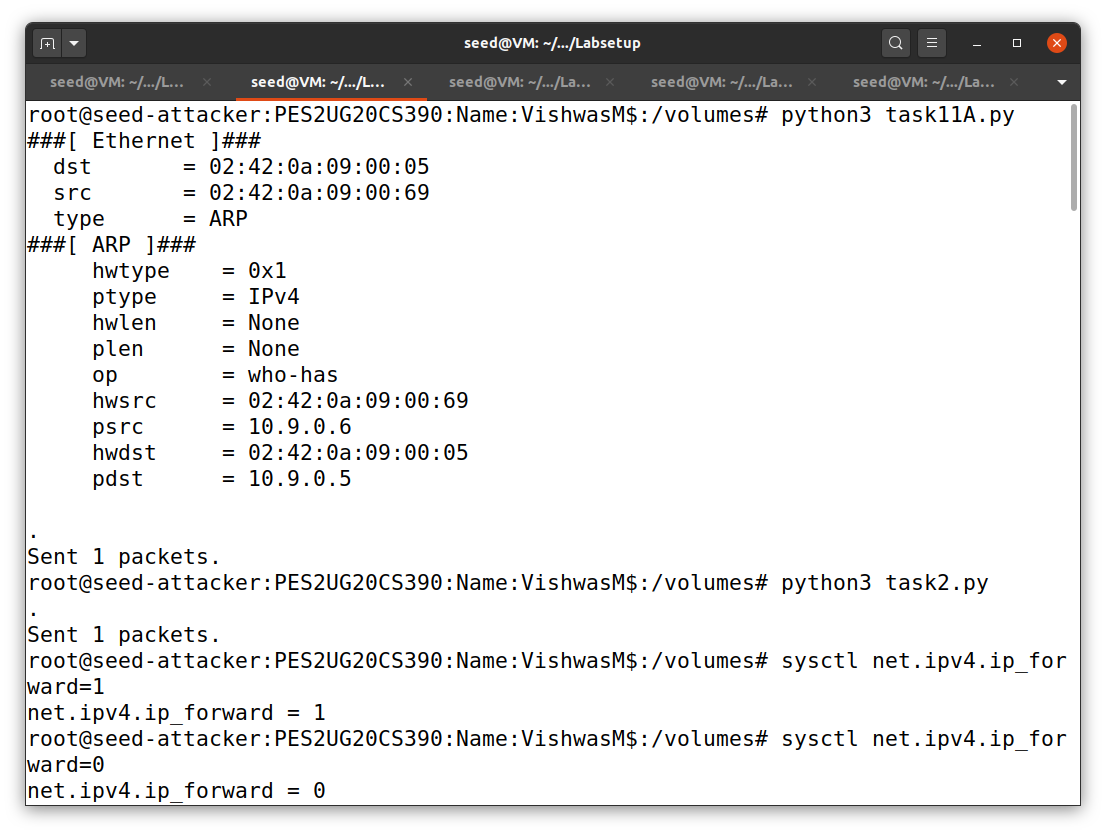
Step 4 - Launch the MITM Attack

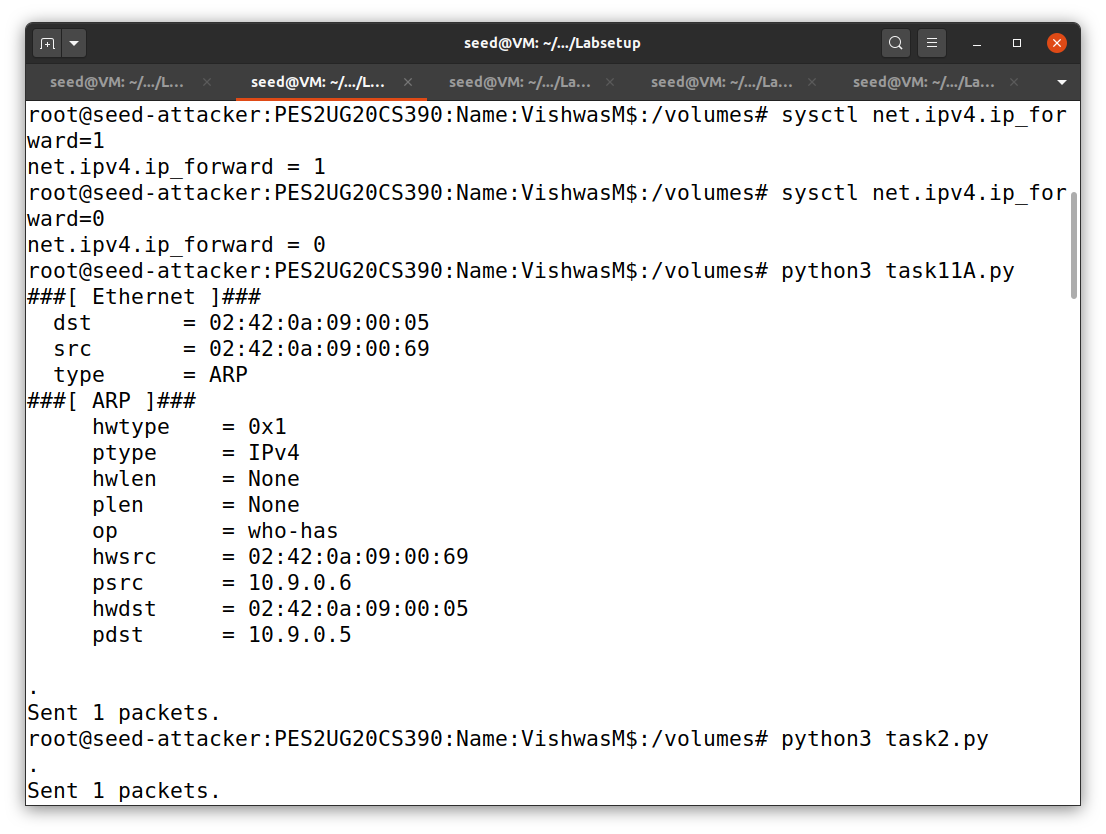


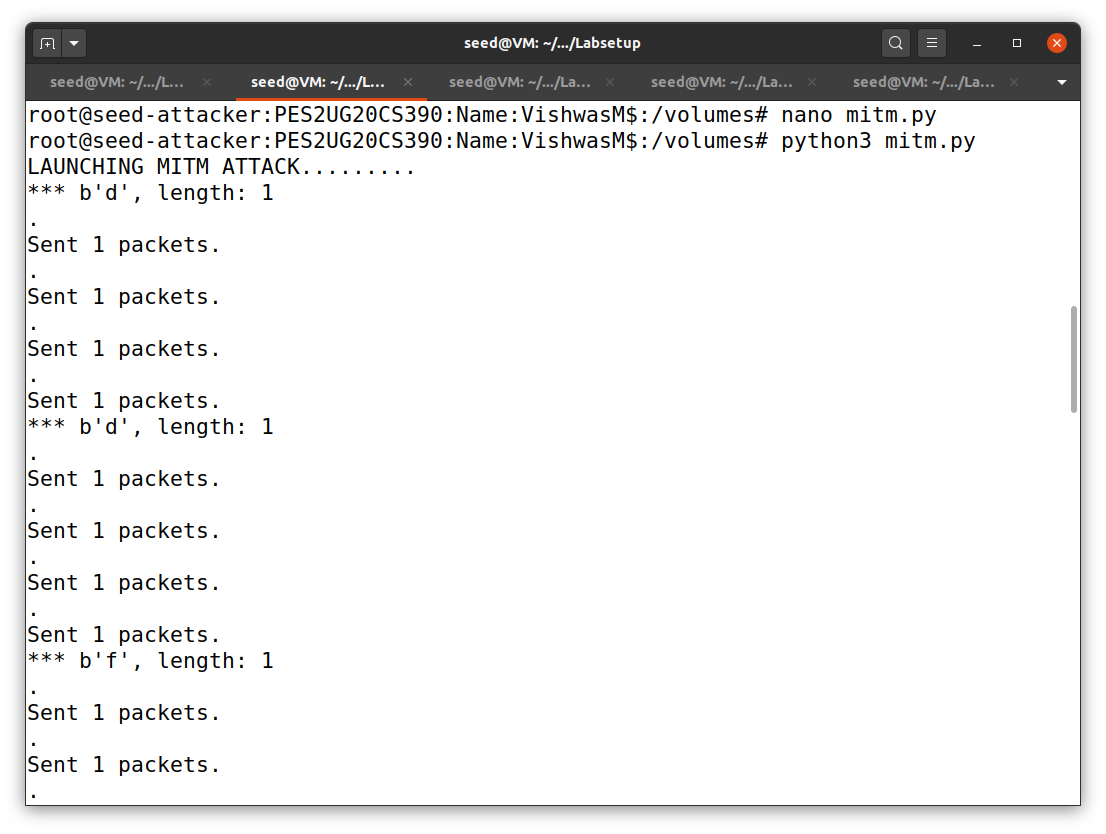


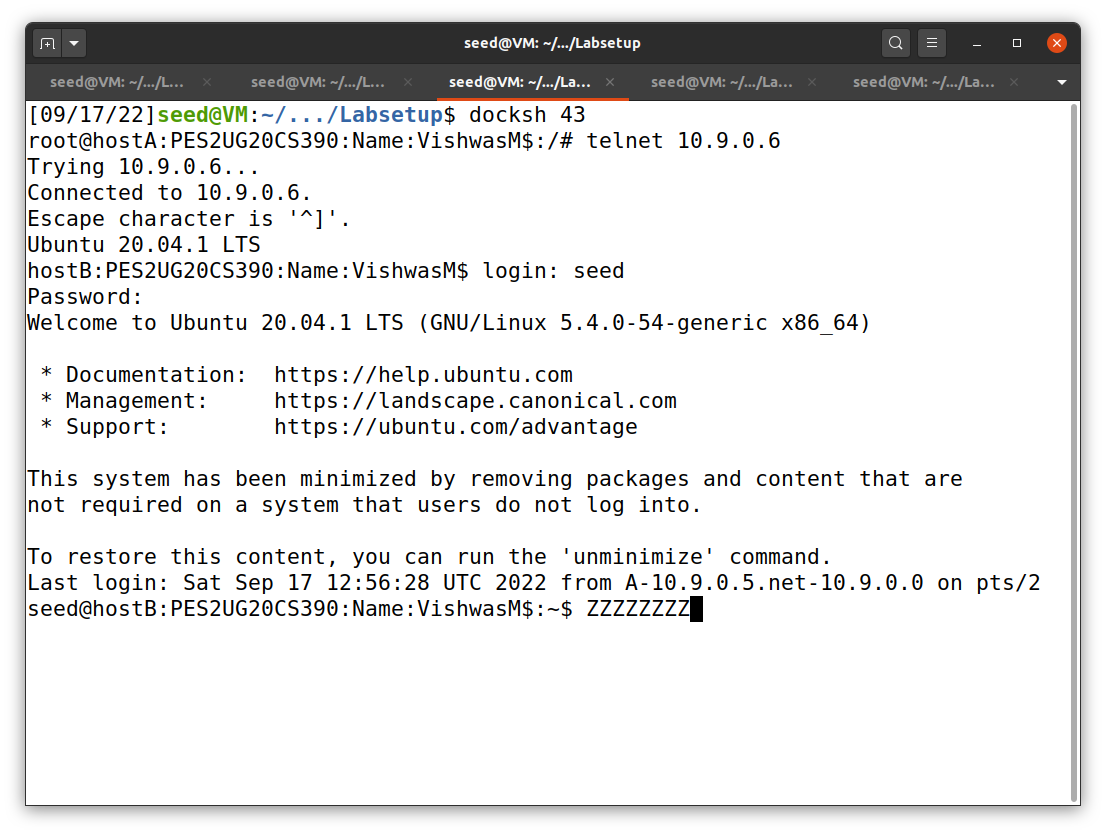


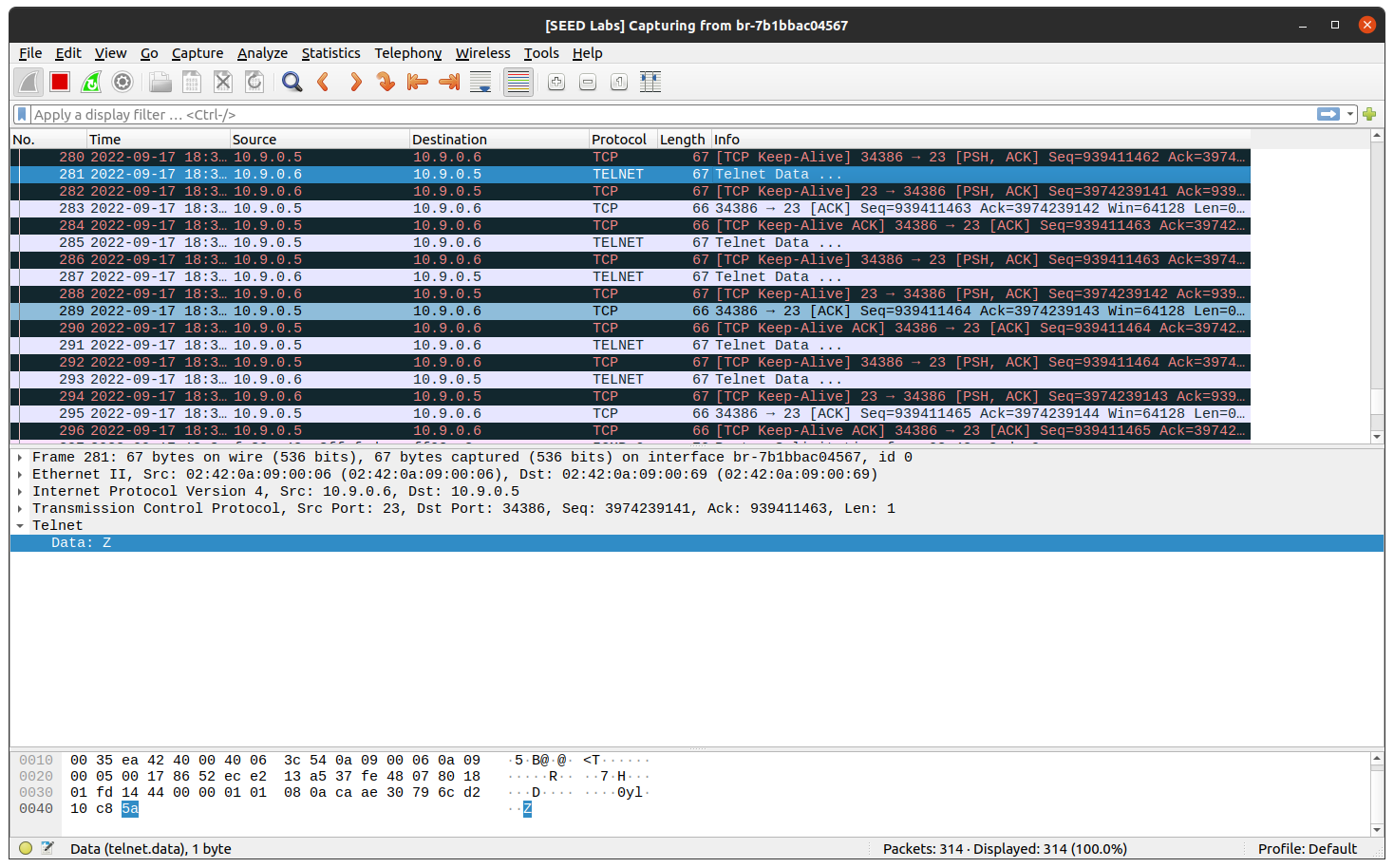
Now to perform the Man in the Middle Attack, we start over and repeat the above steps - for establishing the Telnet connection.











Task 3: MITM Attack on Netcat using ARP Cache Poisoning

