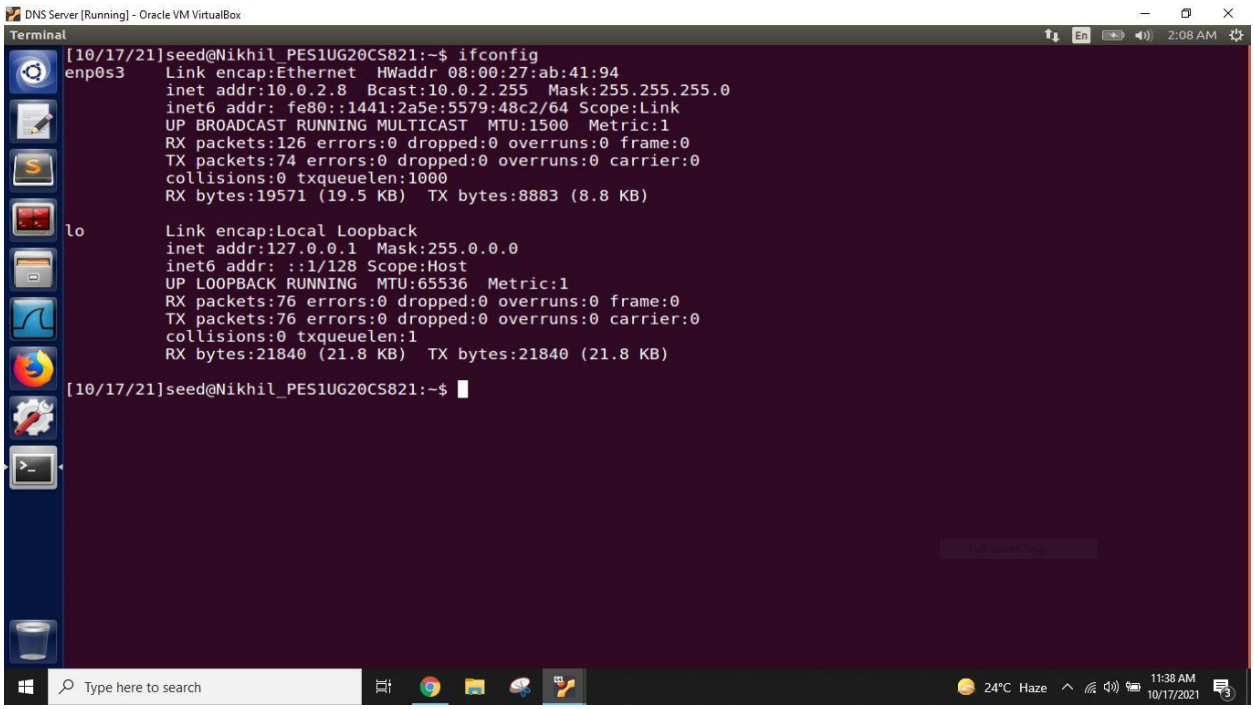
CNS LAB 3
Local DNS Attack

Name: Nikhil T M
SRN:PES1UG20CS821
Section:F

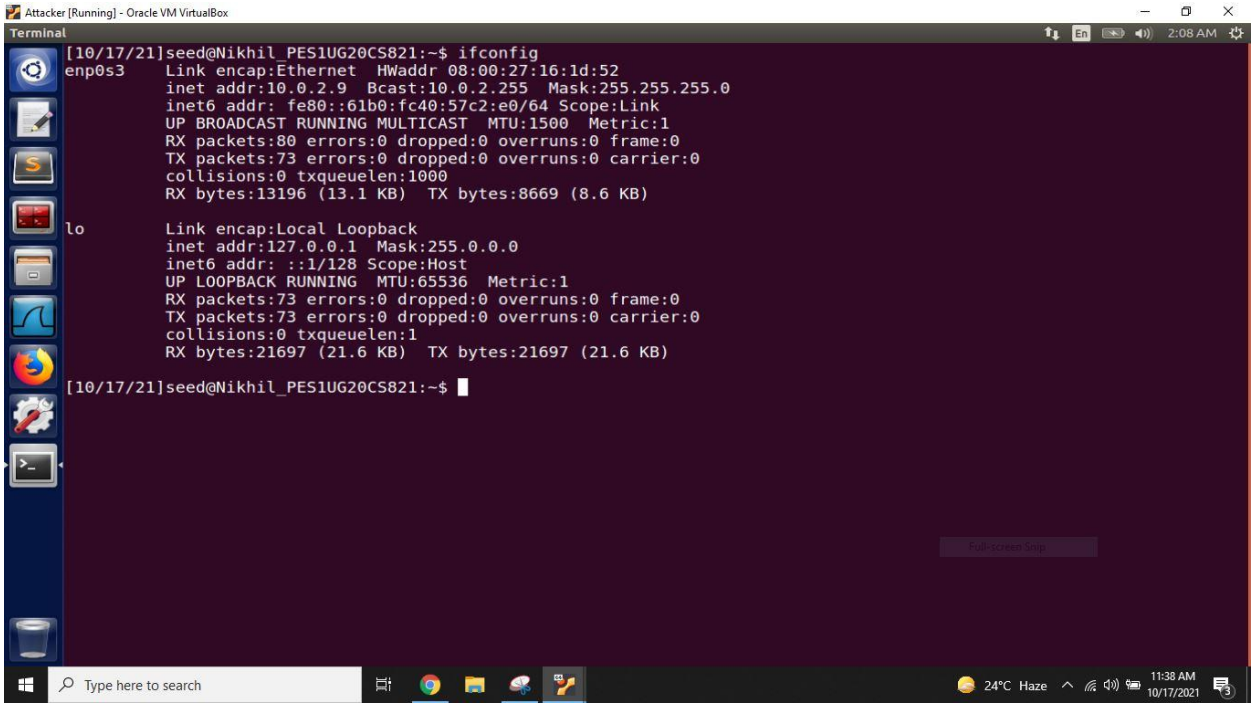
LAB Set Up

DNS Server	10.0.2.8
Attacker	10.0.2.9
Victim	10.0.2.18

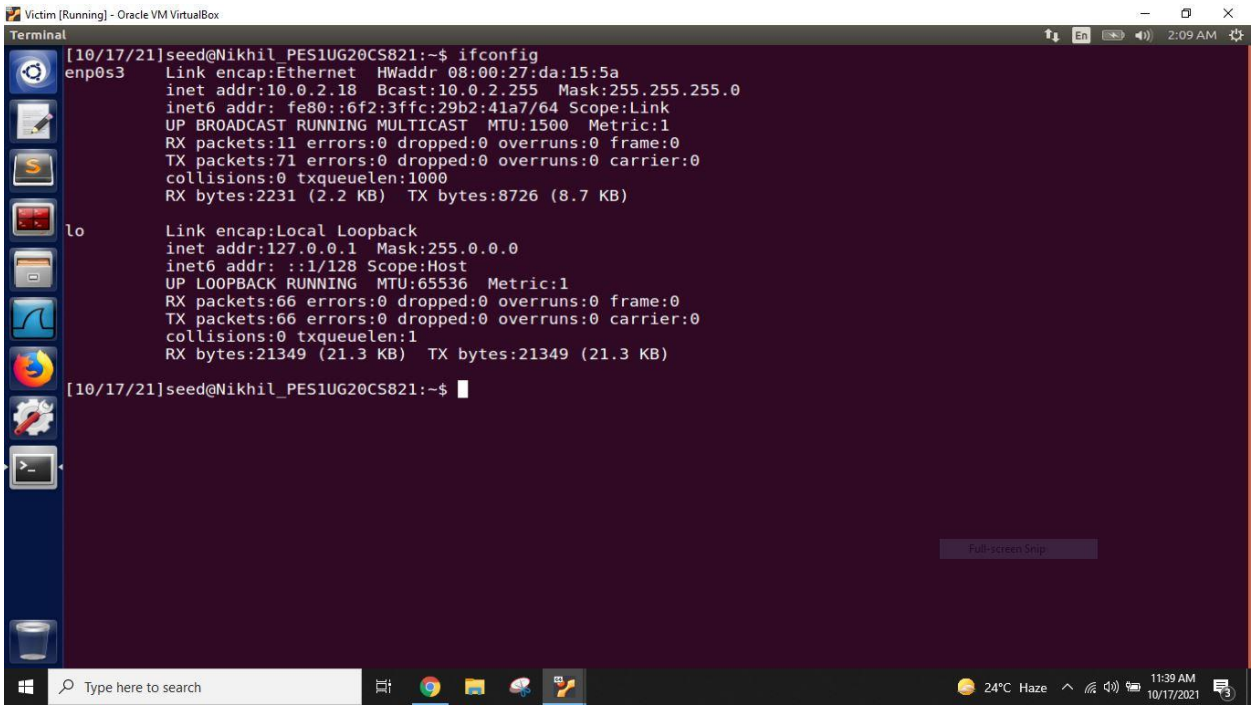
DNS Server



Attacker

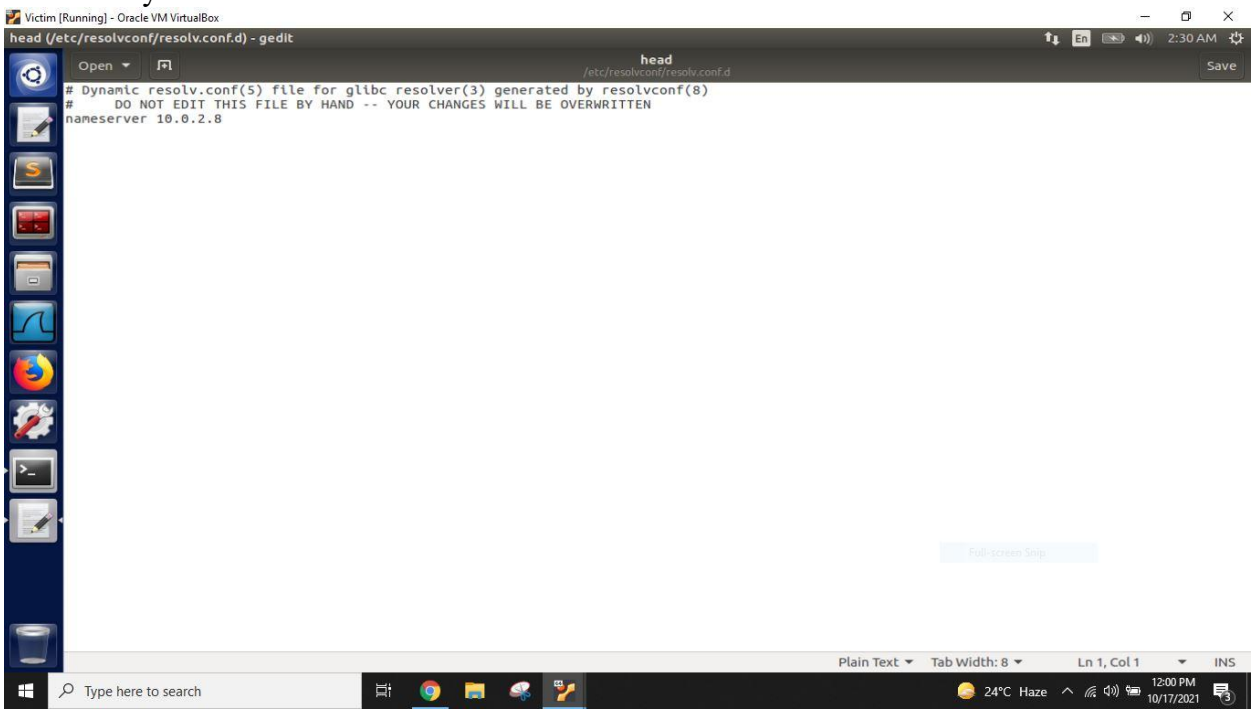


Victim



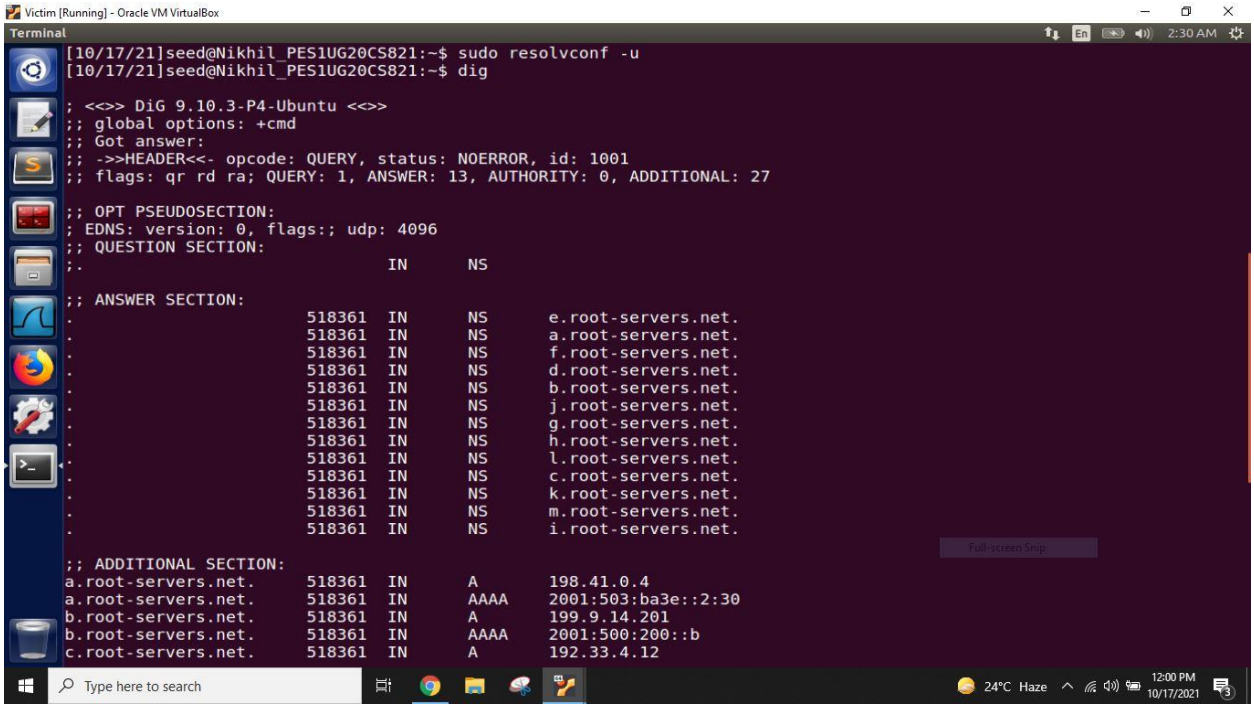
Task 1: Configure the User Machine

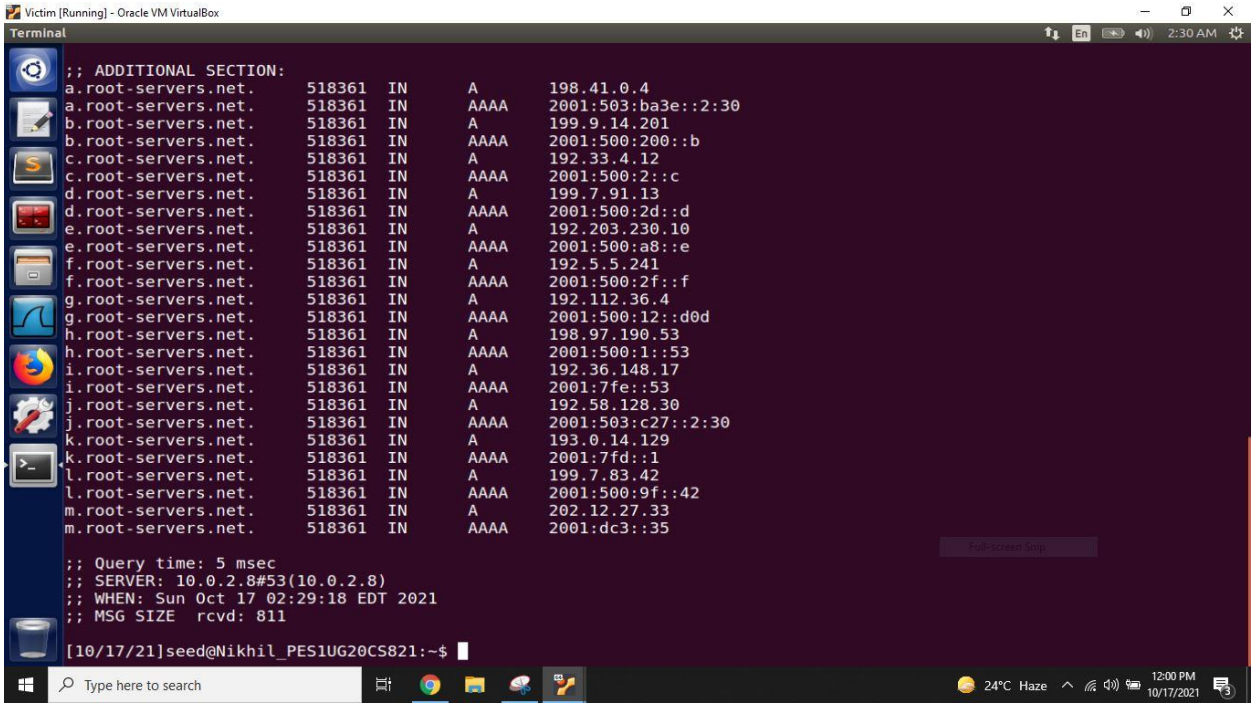
Go to /etc/resolvconf/resolv.conf.d/head file on the victim machine and enter nameserver followed by the DNS Server machine's IP address



for the change to take effect run the command sudo resolvconf -u

And enter the dig command to see the server IP address





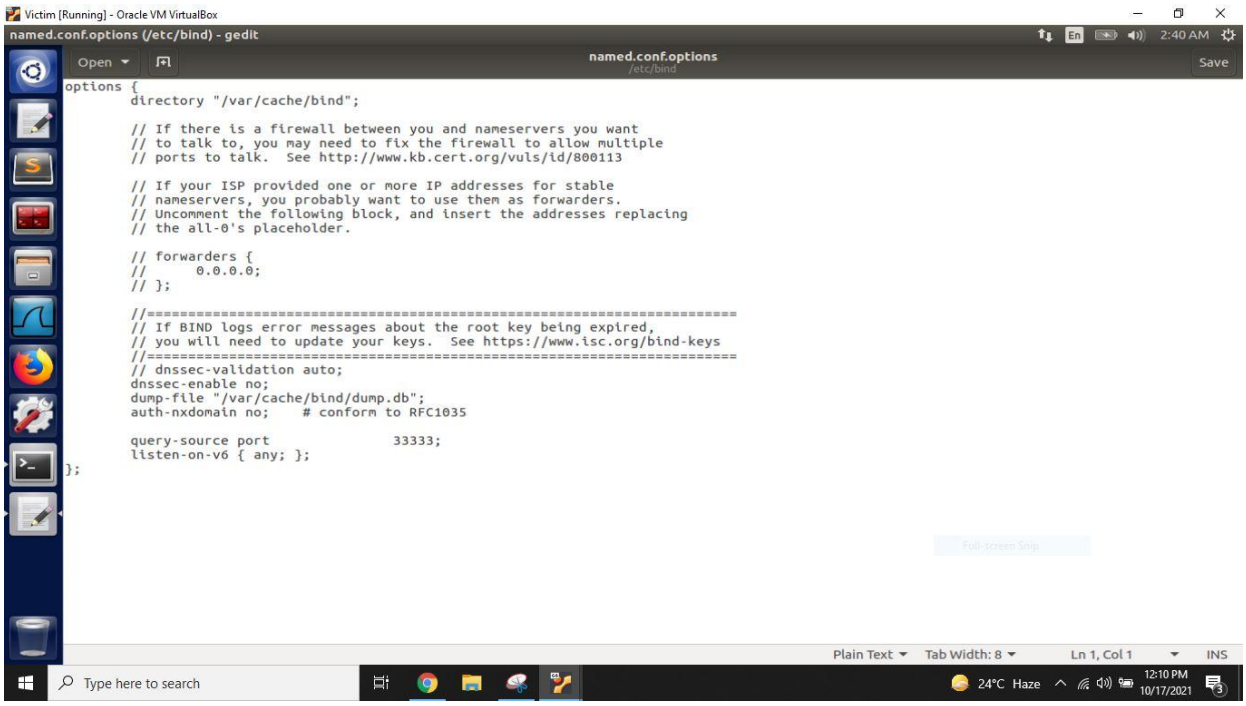
In the above screenshot we can see that the machine with IP address 10.0.2.8 acts as server of port number 53 .

Task 2: Set Up a Local DNS Server

Step 1: Configure the BIND9 Server.

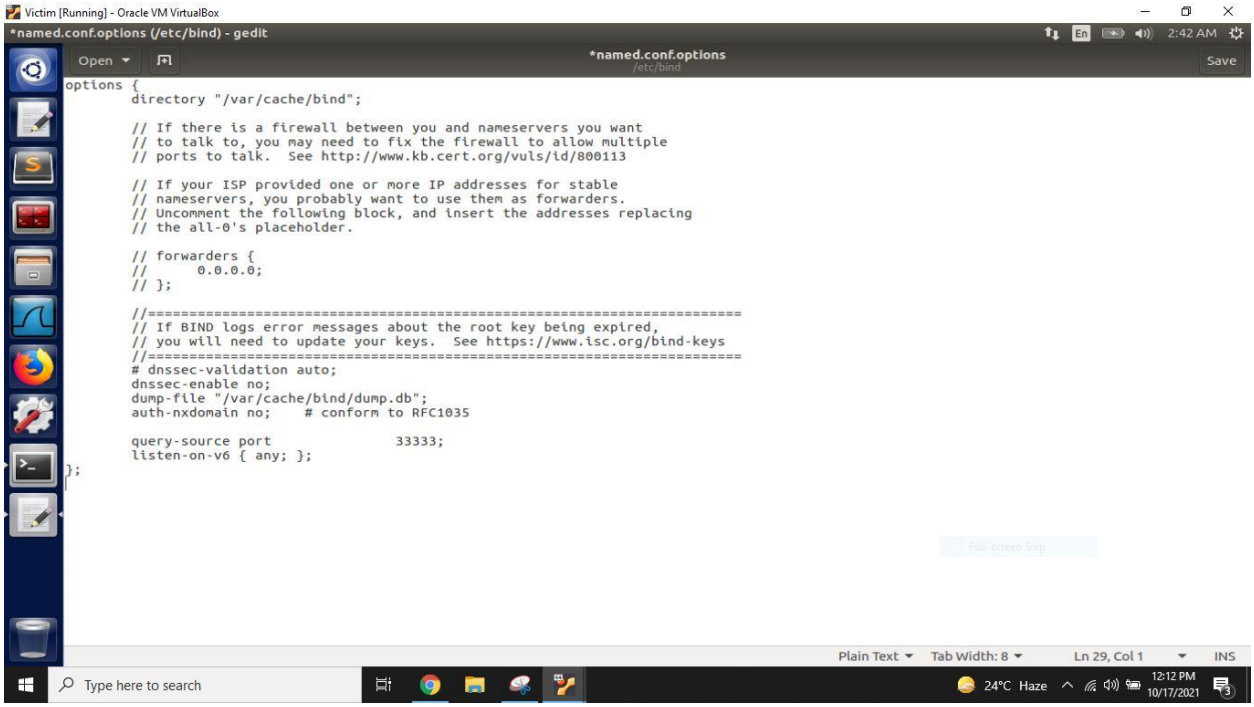
Go to /etc/bind/named.conf.options to edit the configuration of the Bind Server

In the option block set the path where the DNS cache have to be dumped when rndc dumpdb -cache command is used



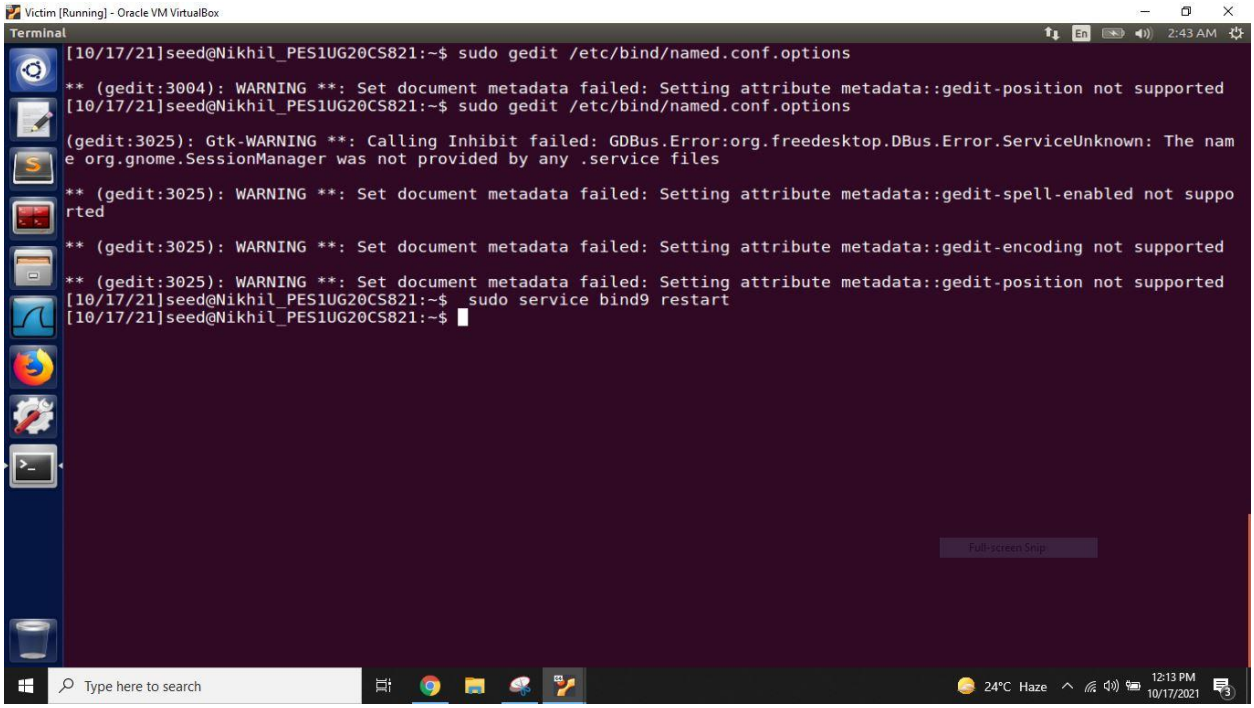
Step 2: Turn off DNSSEC

Comment the dnssec-validation auto and add the line dnssec-enable no which is used to turn off the dnssec



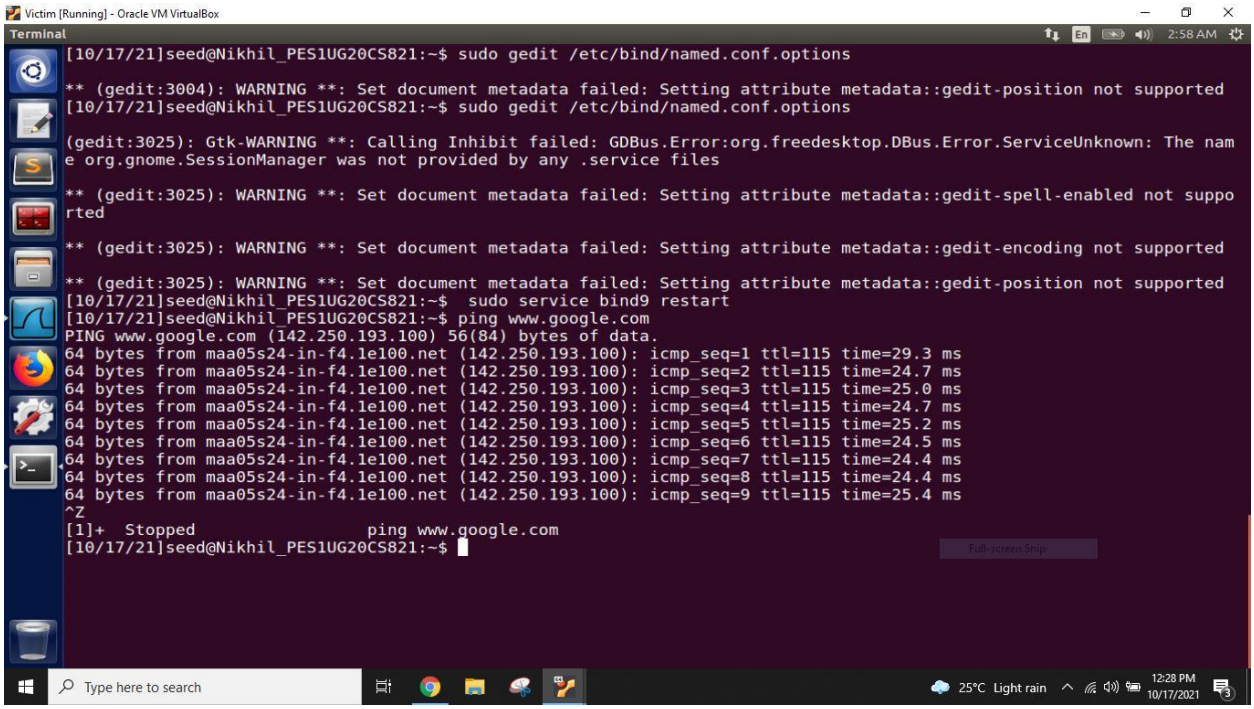
Step 3: Start DNS server

After performing the above changes restart the bind server so that the changes are applied using the command sudo service bind9 restart

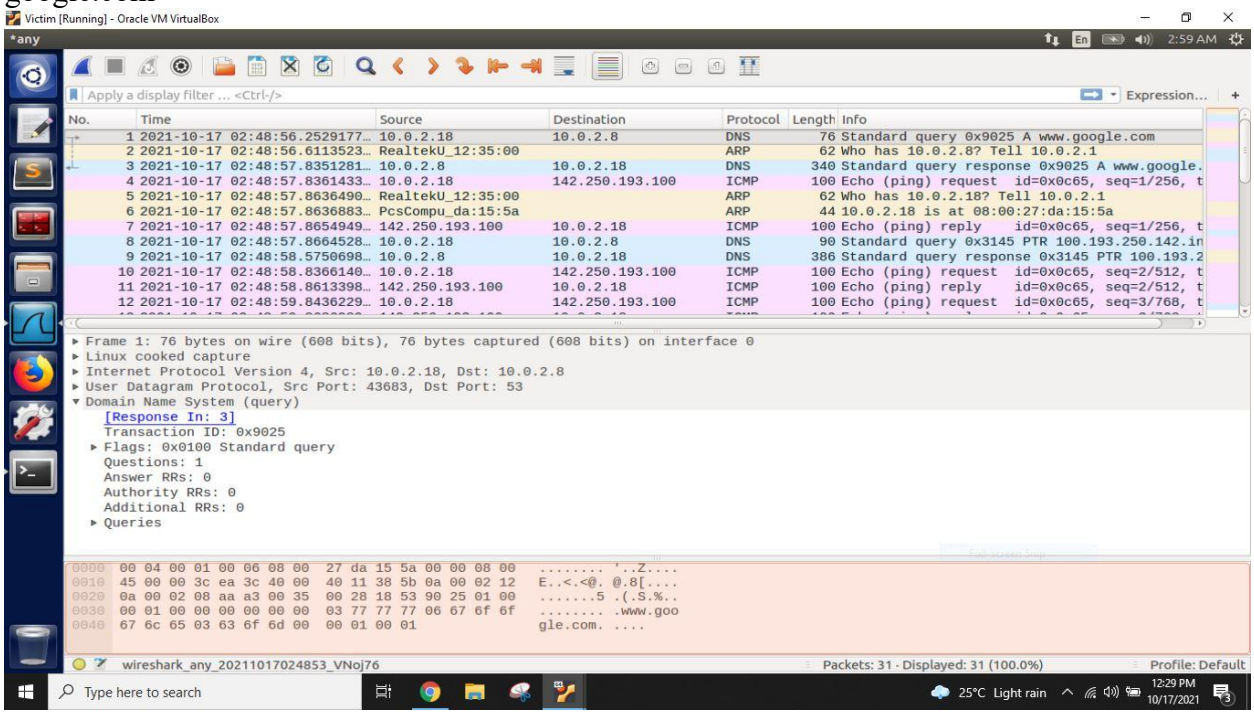


Step 4: Use the DNS server

To make sure that the dns is working ping any of the website and capture the packets using wireshark



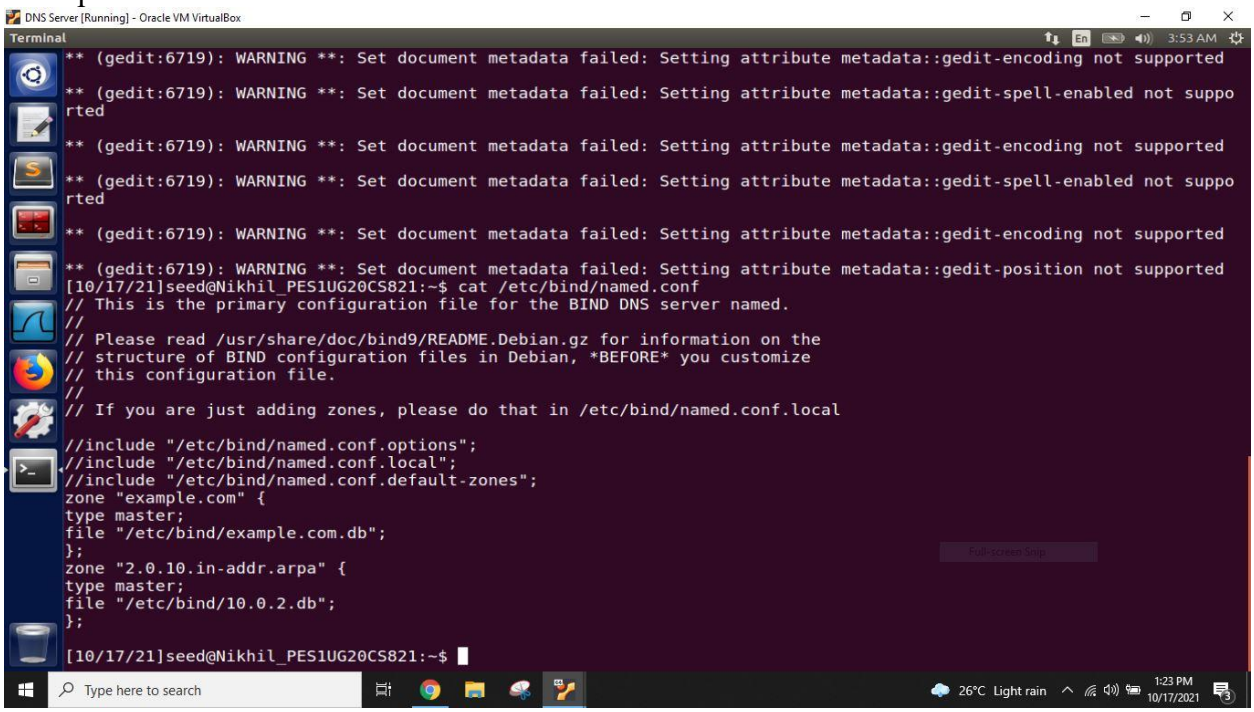
In the below screen shot we can observer that when the victim ping the google.com the request is sent to the dns server 10.0.2.8 later the dns server sends back the reply to the victim which consists of the IP address of the google.com then the victim directly communicate with the google.com



Task 3: Host a Zone in the Local DNS server.

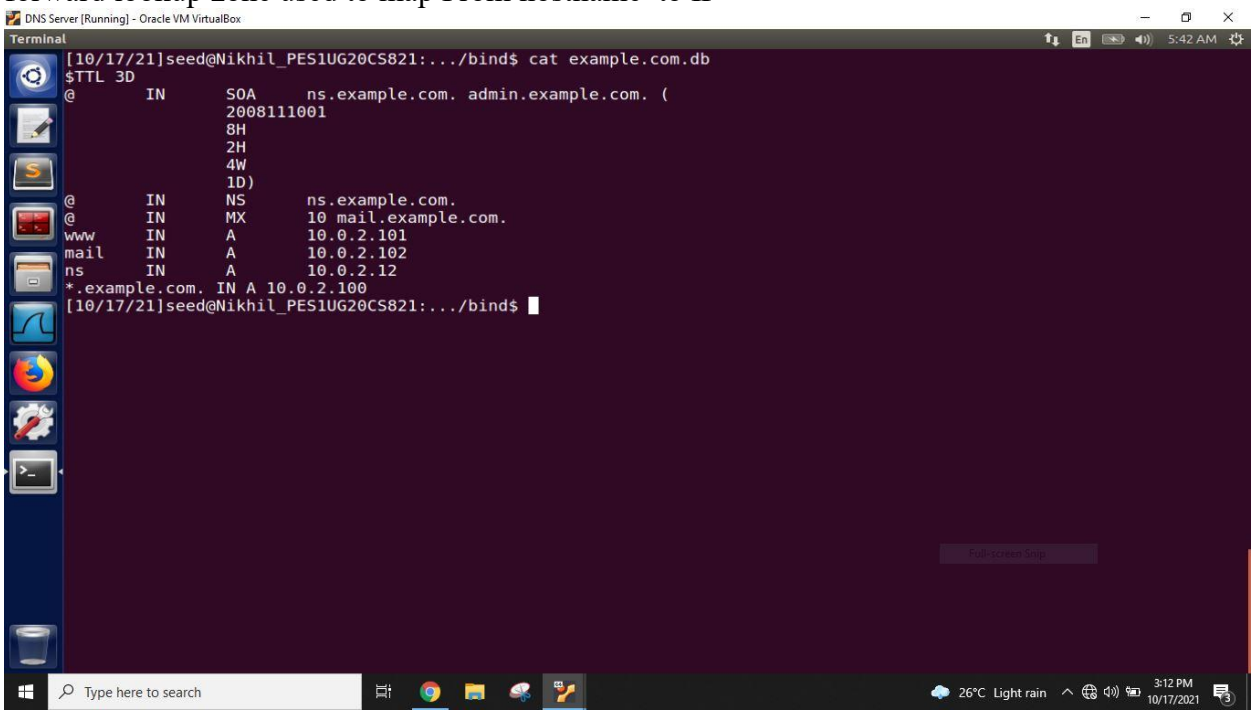
Step 1: Create Zones

We need to create two zone entries in the DNS server by adding the following contents to /etc/bind/named.conf. The first zone is for forward lookup and the second zone is for reverse lookup.



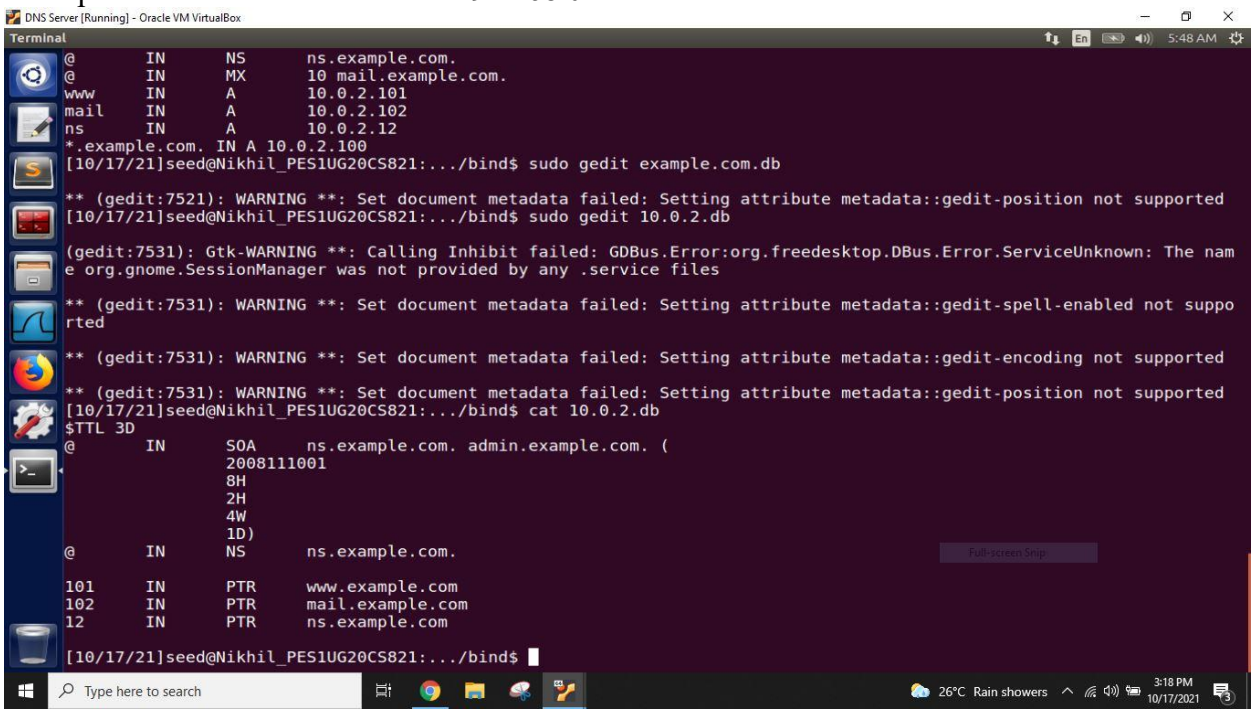
Step 2: Setup the forward lookup zone file

This forward lookup zone file is created with file name example.com.db at the path /etc/bind this forward lookup zone used to map From hostname to IP



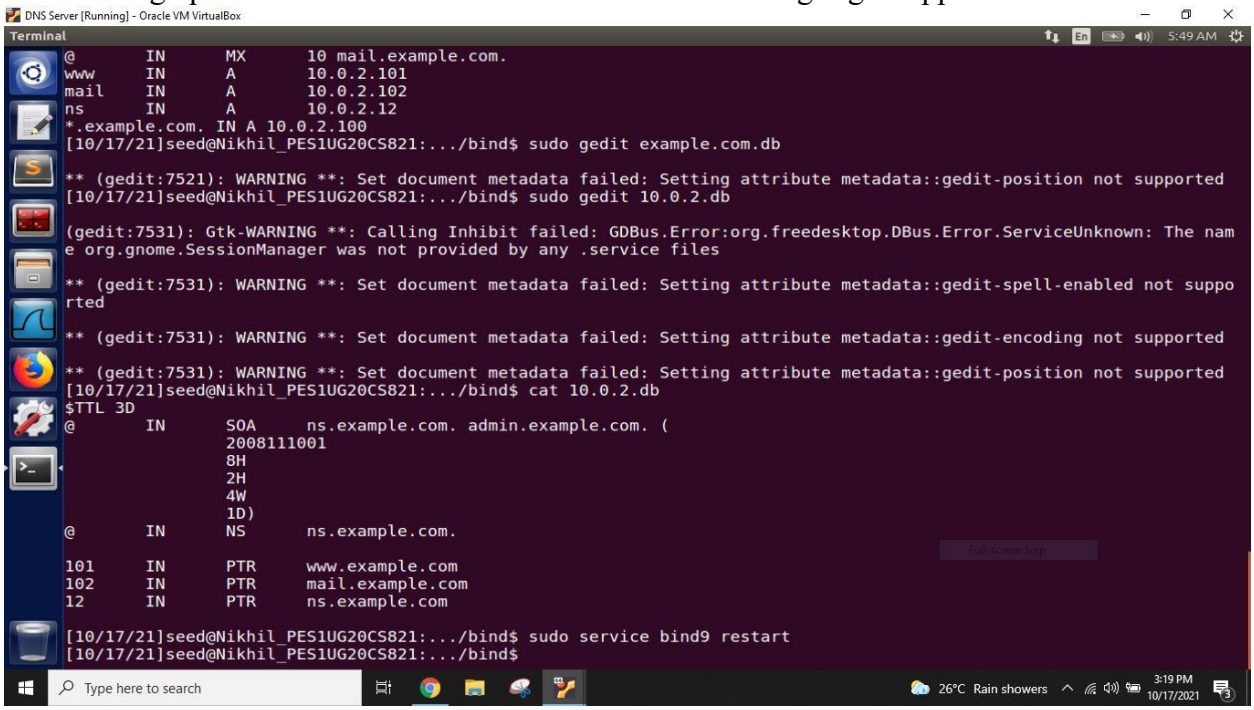
Step 3: Setup the reverse lookup zone file

To support DNS reverse lookup from IP address to hostname, we also create a new DNS reverse lookup file In the /etc/bind/ called 192.168.0.db

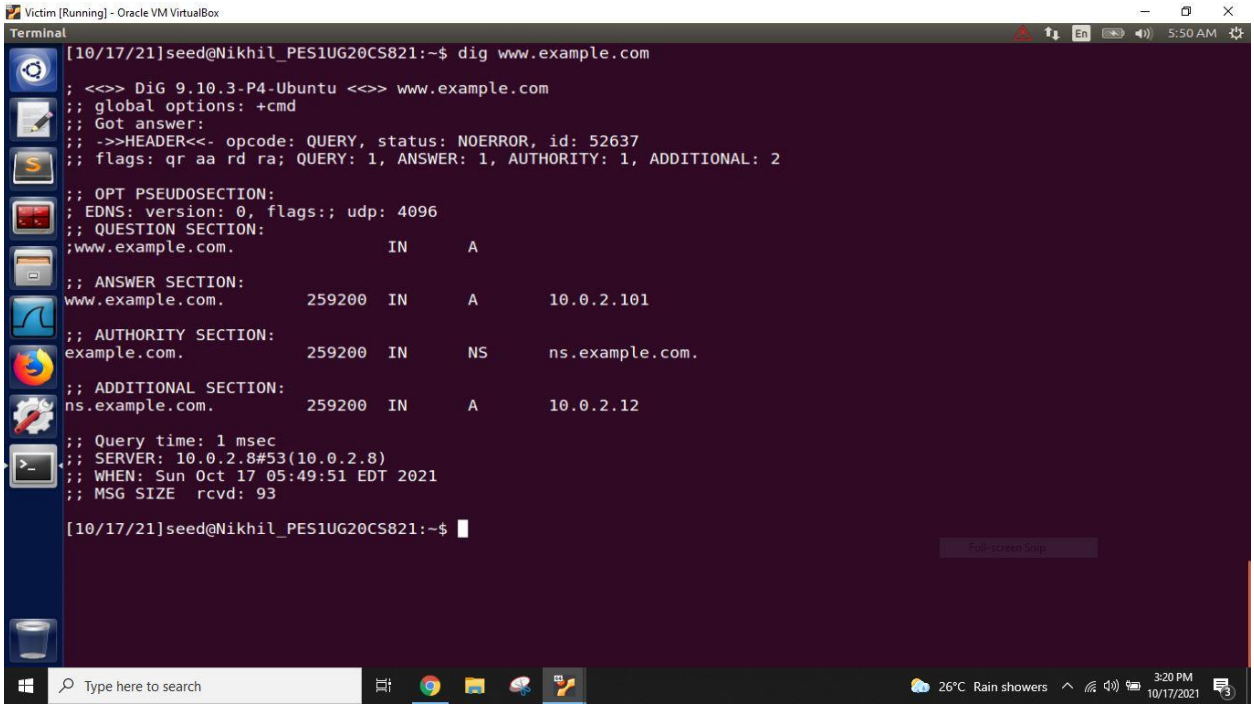


Step 4: Restart the BIND server and test

After setting up the file restart the bind server so that the changes gets applied

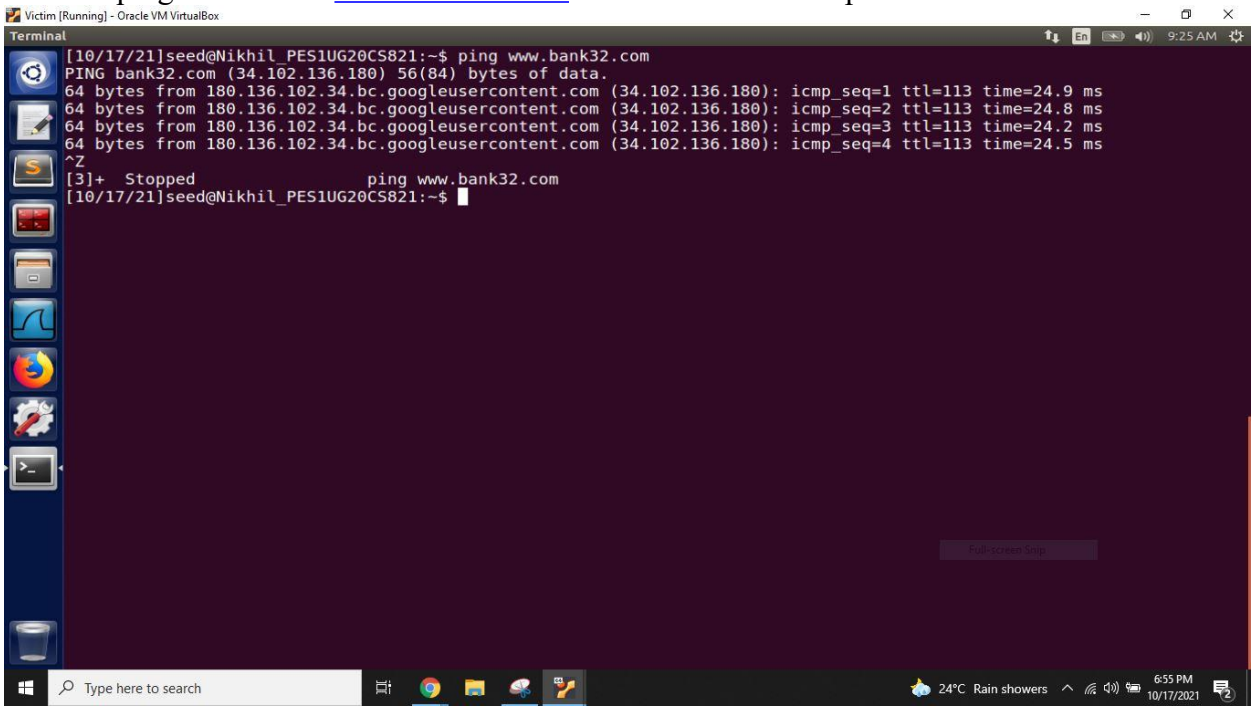


Now dig the www.example.com which contains the ip address we entered in the above file for all the sections

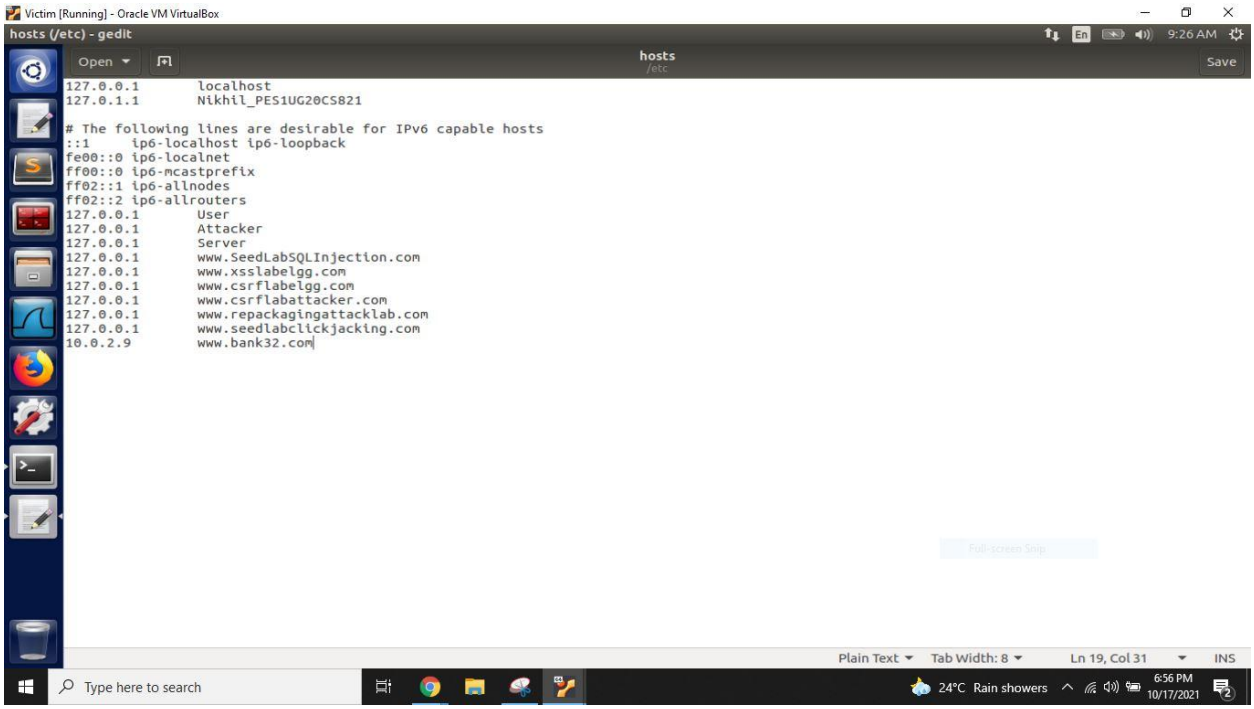


Task 4: Modifying the Host File

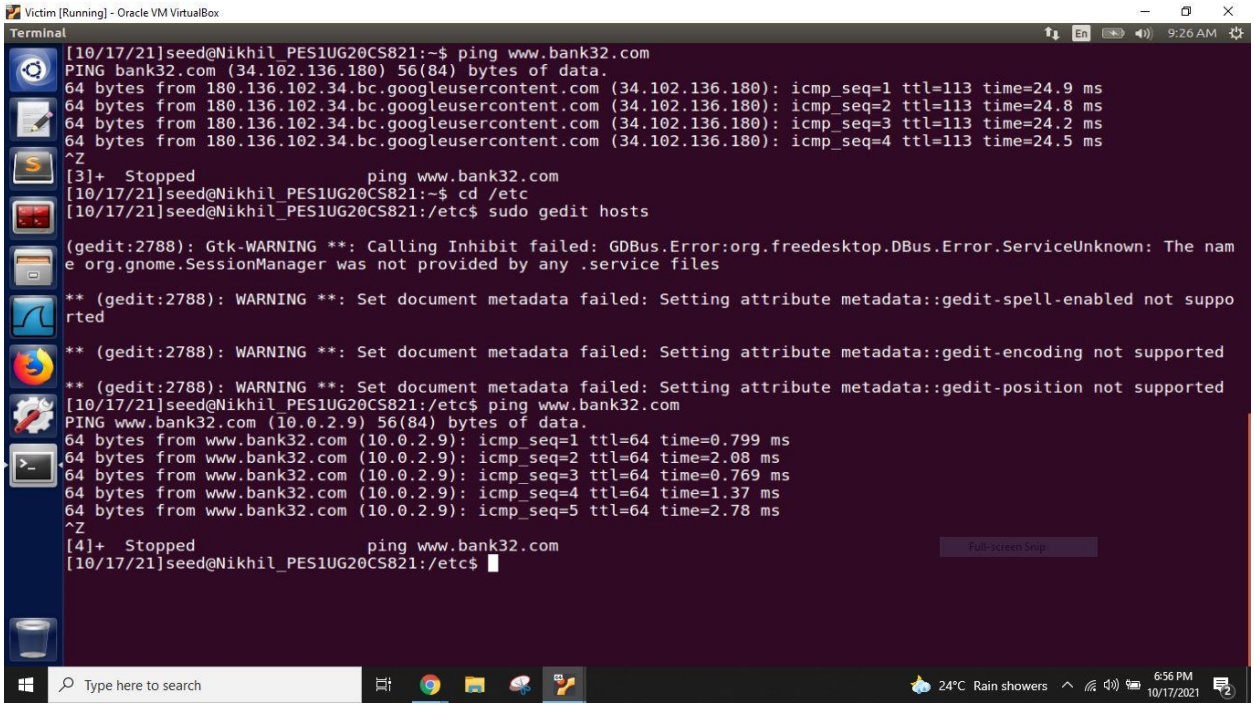
First we ping the website www.bank32.com and noted down the ip address as 34.102.136.180



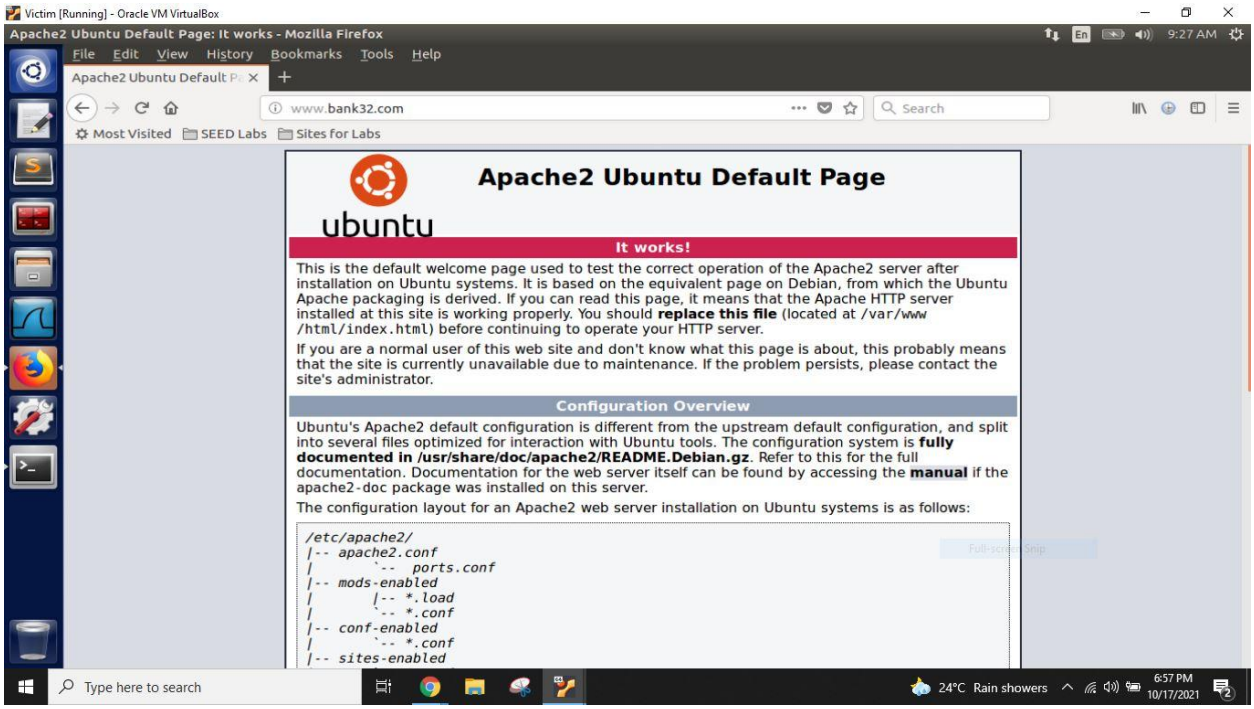
We know the ip address of the site bank32.com is stored in the hosts files in the etc directory
So we edit the hosts file and enter the attacker IP address as 10.0.2.9 followed by the url bank32.com



We can see here when the victim ping the url bank32.com he is getting the response from the attacker ip address 10.0.2.9 by this way the attacker can redirect the user to his requeried ip address so that he can lead the user to the malicious website



When the user visits the same URL through browser he is redirected to the attacker apache server default page

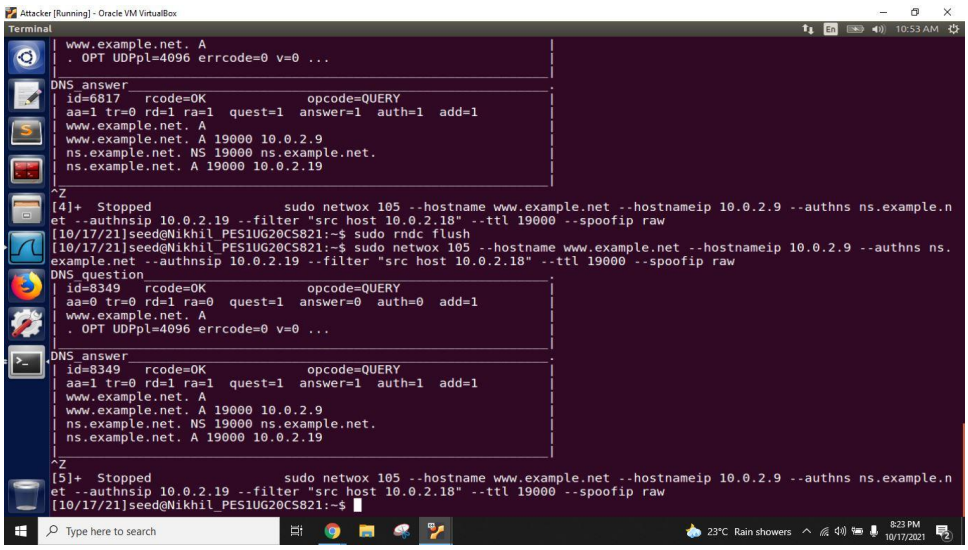


Task 5: Directly Spoofing Response to User

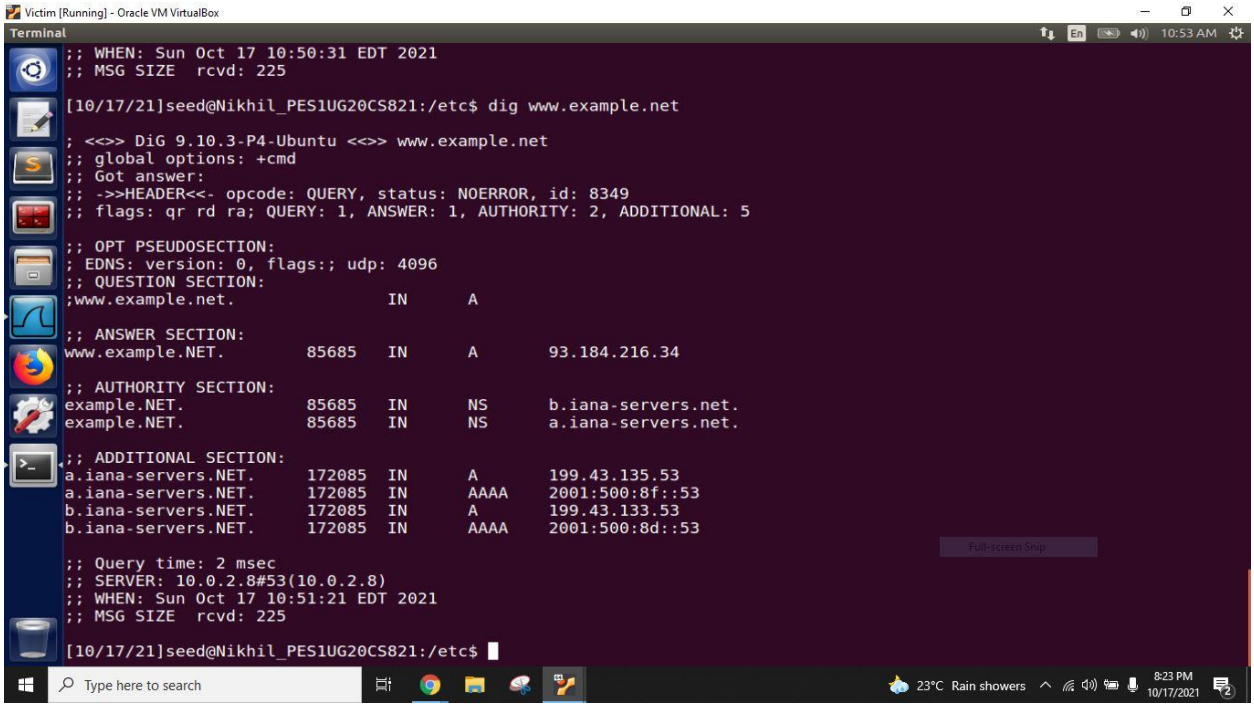
In this attack, the victim's machine has not been compromised, so attackers cannot directly change the DNS query process on the victim's machine.

When a user types the URL www.example.net the user's computer will issue a DNS request to the DNS server to resolve the IP address of the host name. After hearing this DNS request, the attackers can spoof a fake DNS response. The fake DNS response will be accepted by the user's computer

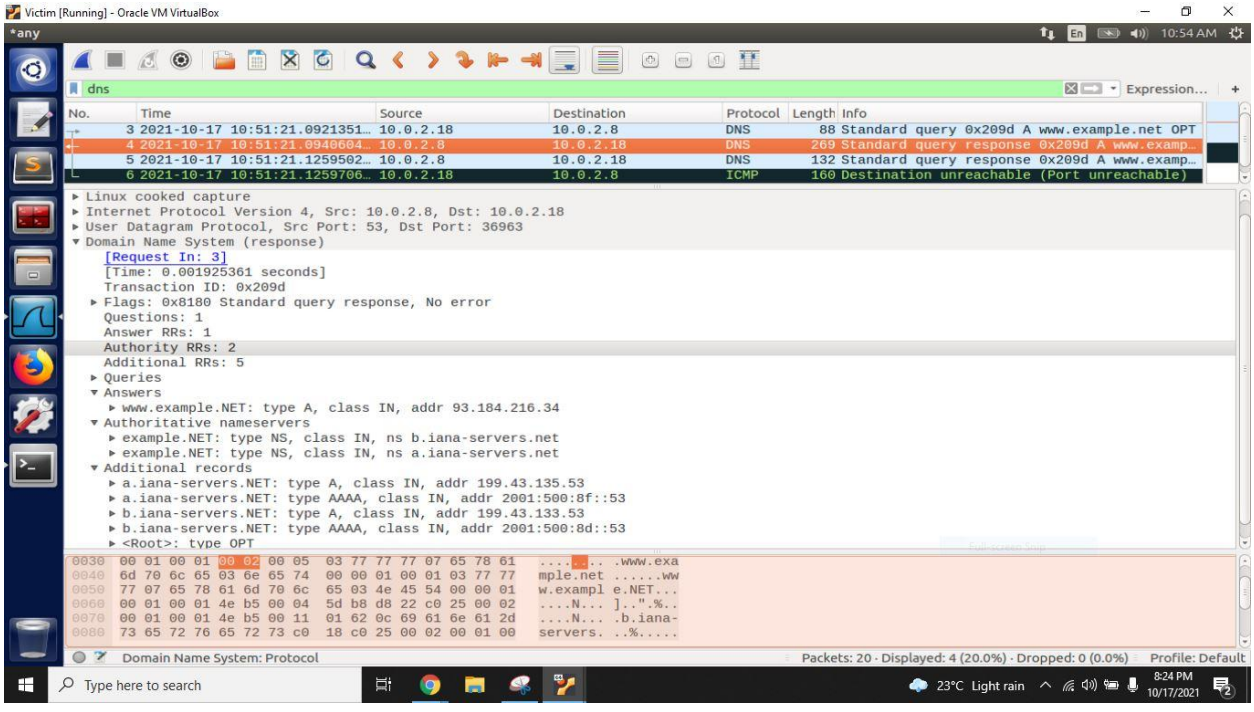
On Attacker machine



On Victim machine

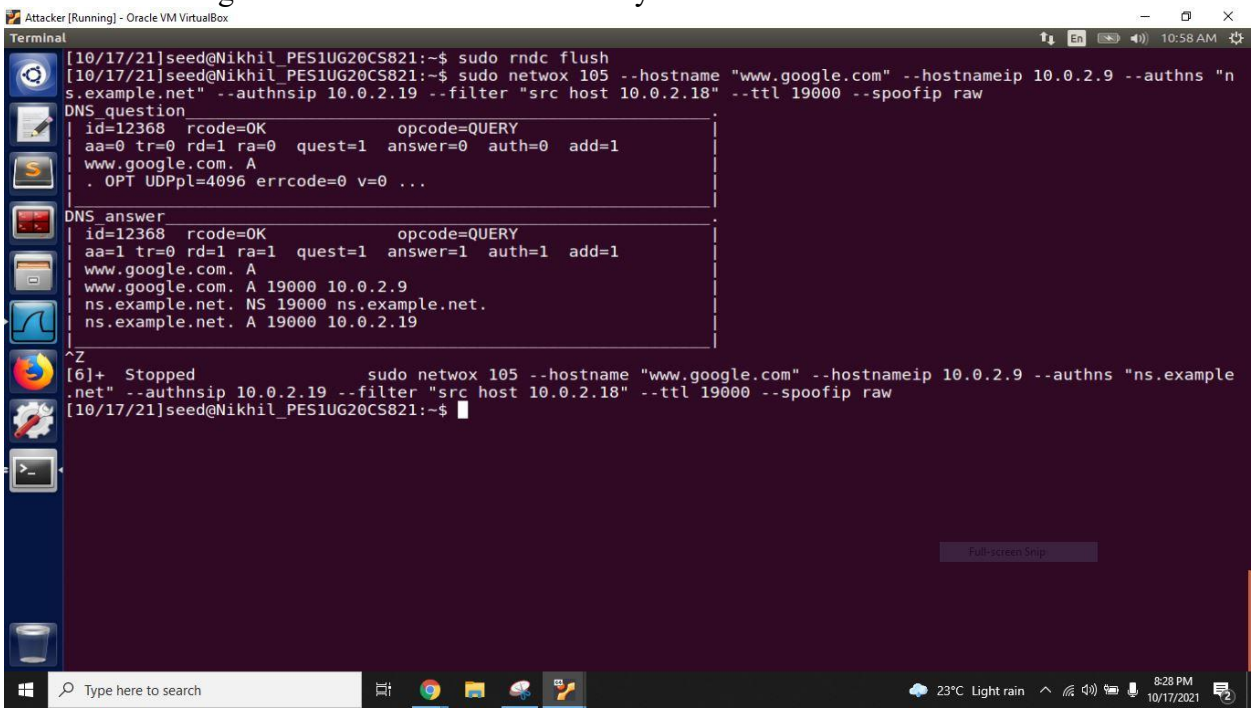


Wireshark observations to show the fake DNS is spoofed by the attacker

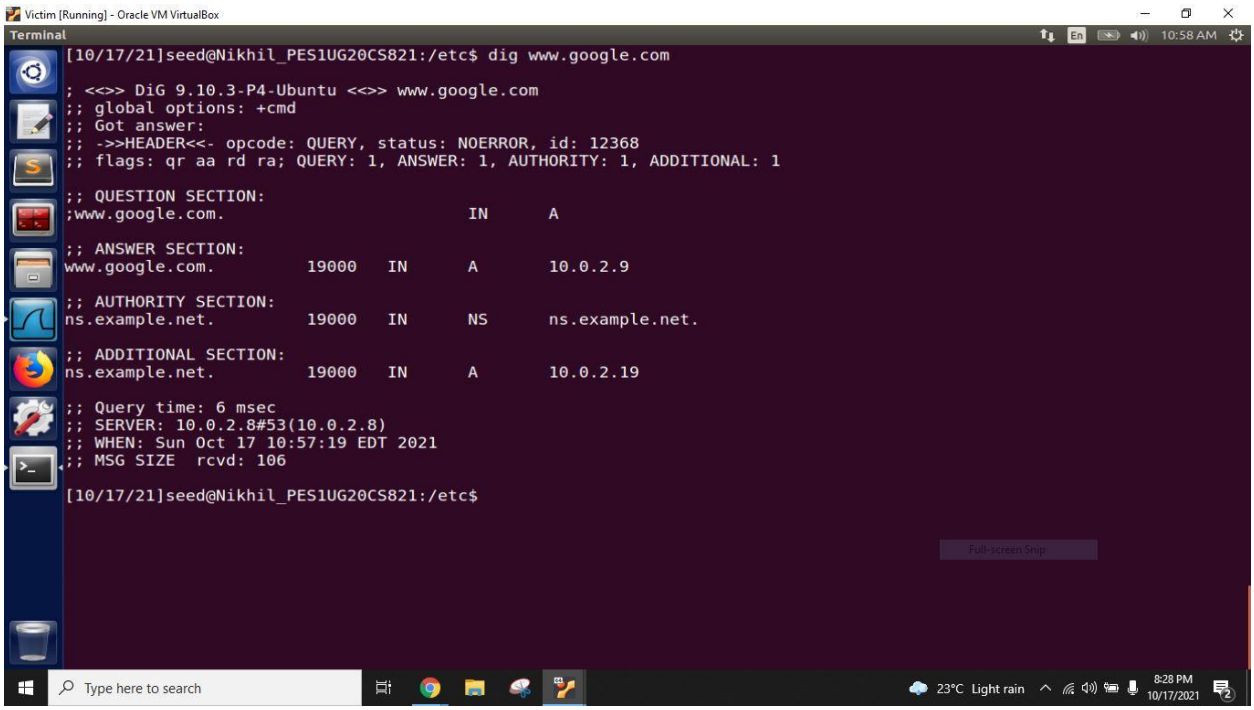


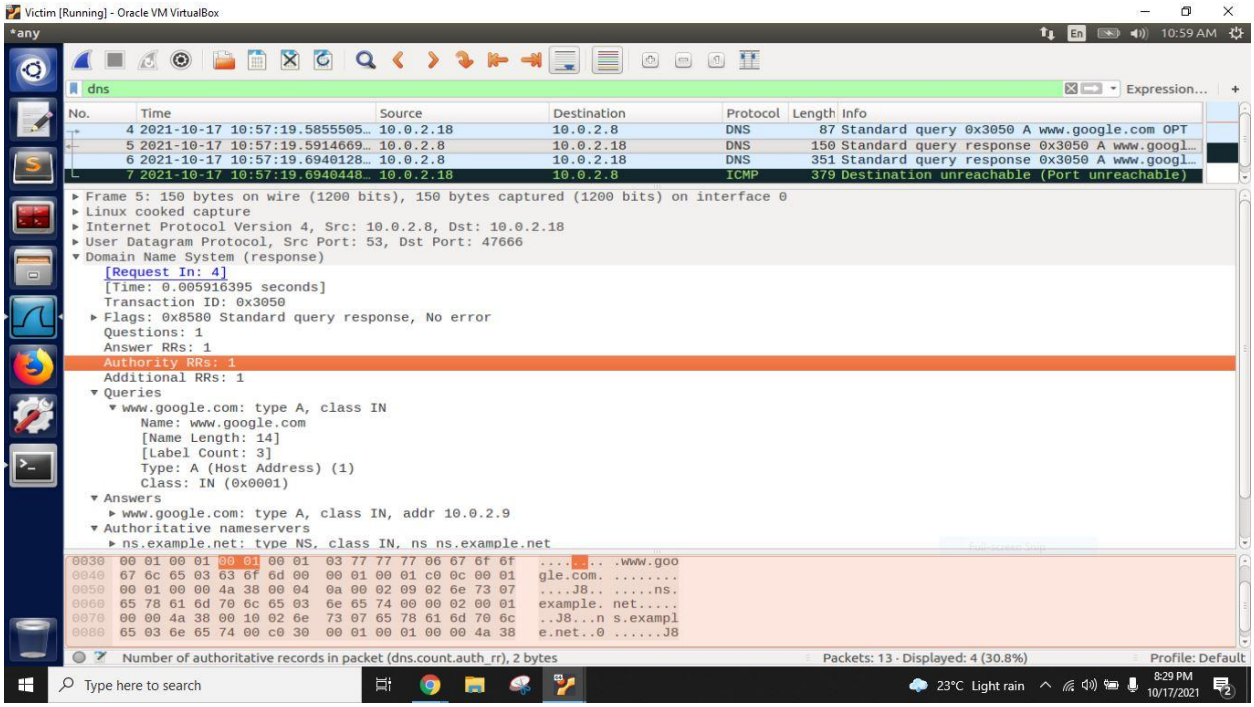
Task 6: DNS Cache Poisoning Attack

In this attack we are spoofing the response to DNS server now, so we set the filter field to "src host 192.168.0.18", which is the IP address of the DNS server. We also use the ttl field to indicate how long we want the fake answer to stay in the DNS server's cache



On victim Machine

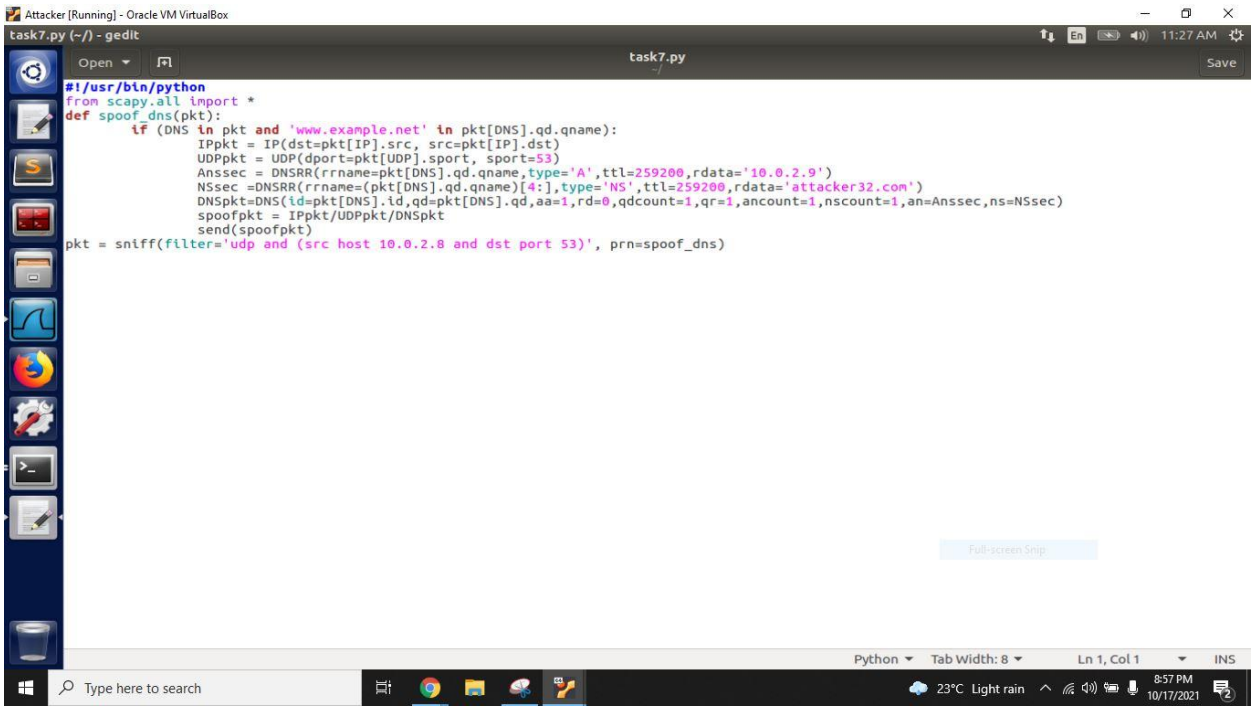




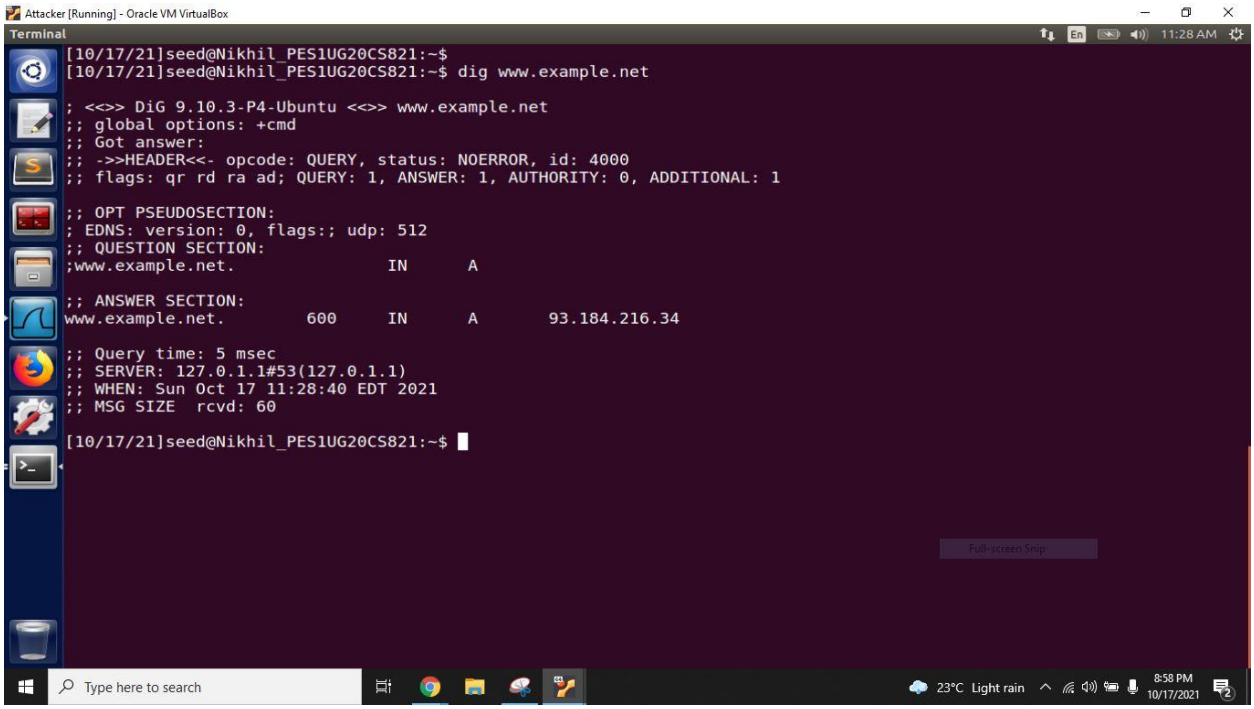
Task 7: DNS Cache Poisoning: Targeting the Authority Section

In this task we perform the DNS cache Poisoning by targeting the authority section

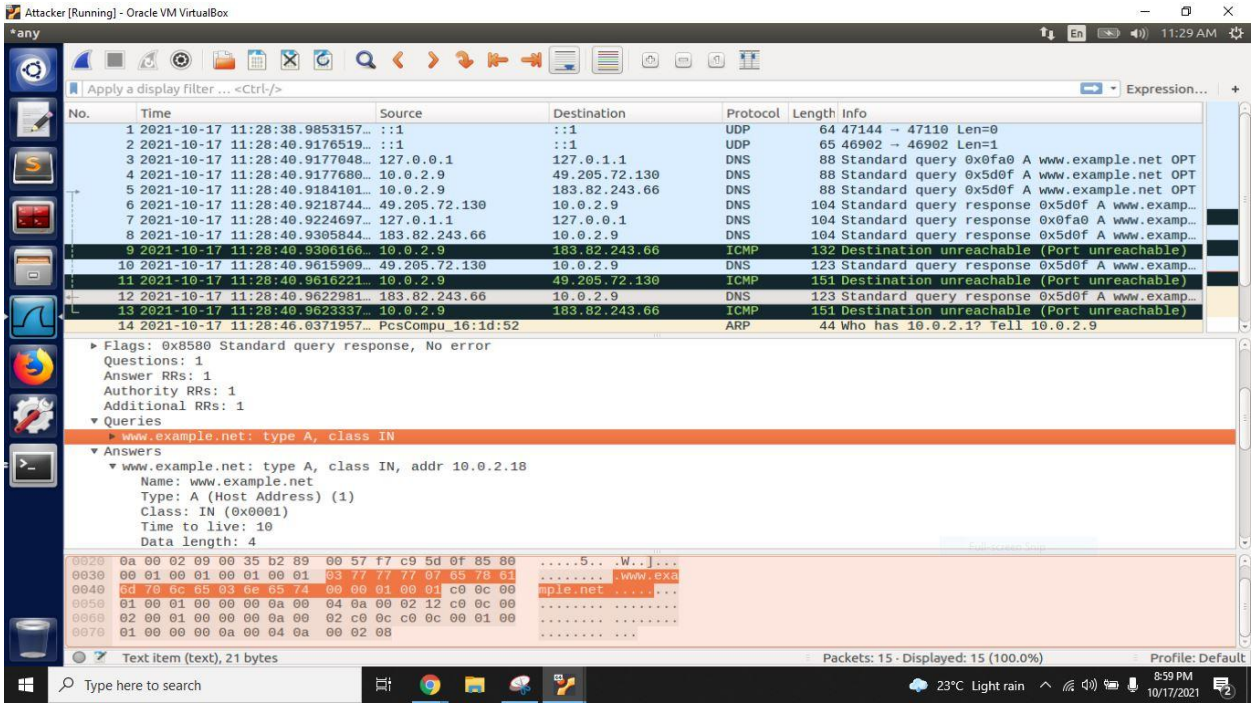
Each DNS Zone has at least one authoritative name server that publishes information about that zone. They are called `authoritative' because they provide original and answers to DNS queries as opposed to obtaining answers from other DNS servers.



The above code is saved and runned in the attacker machine
After the use of dig command

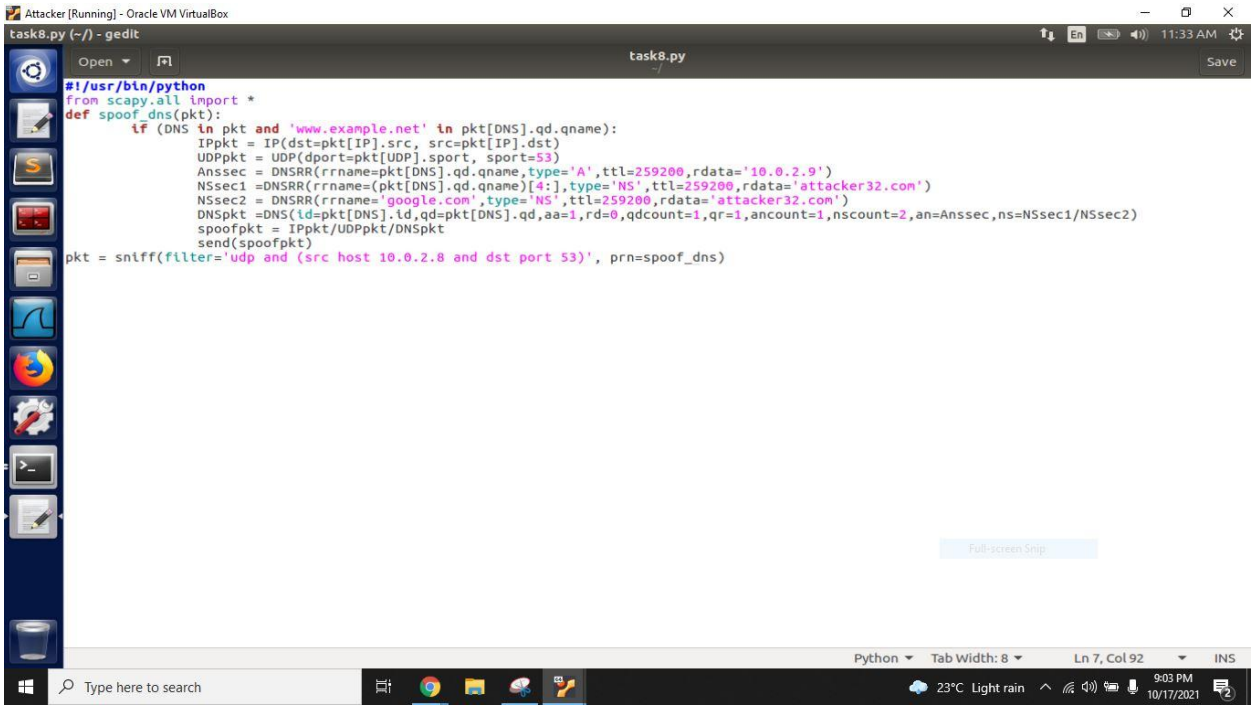


Authority section is successfully DNS cache poisoned

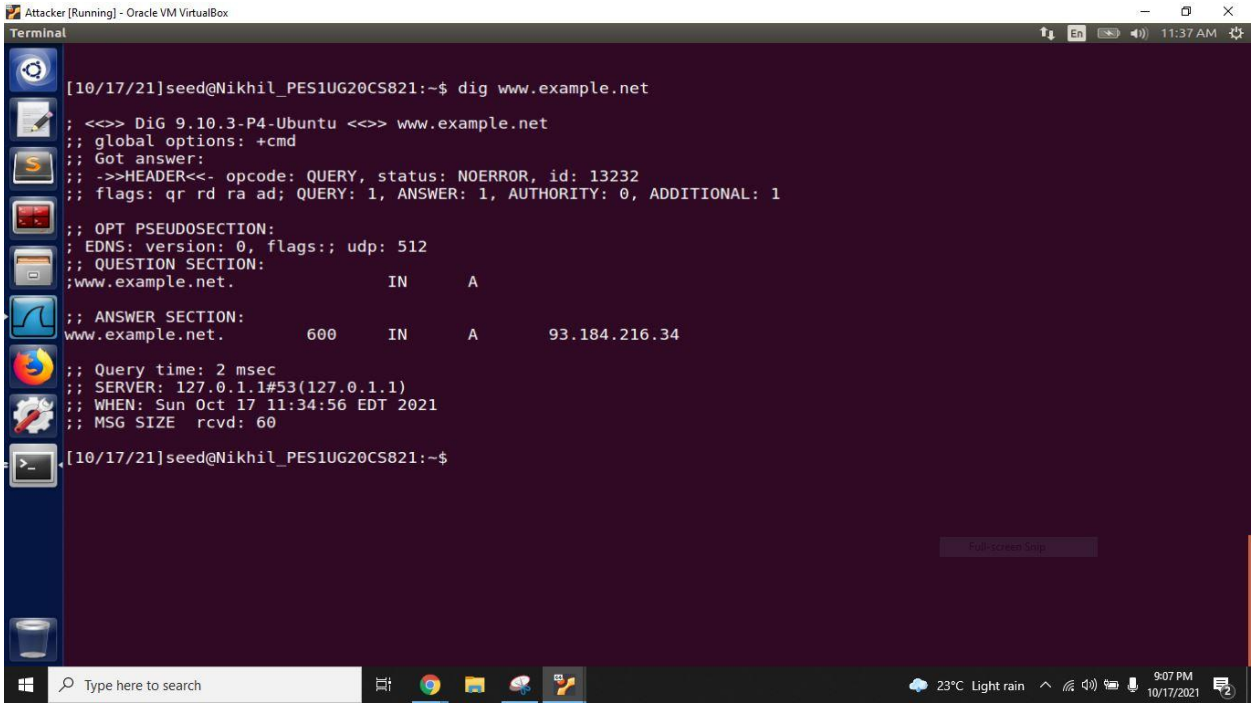


Task 8: Targeting Another Domain

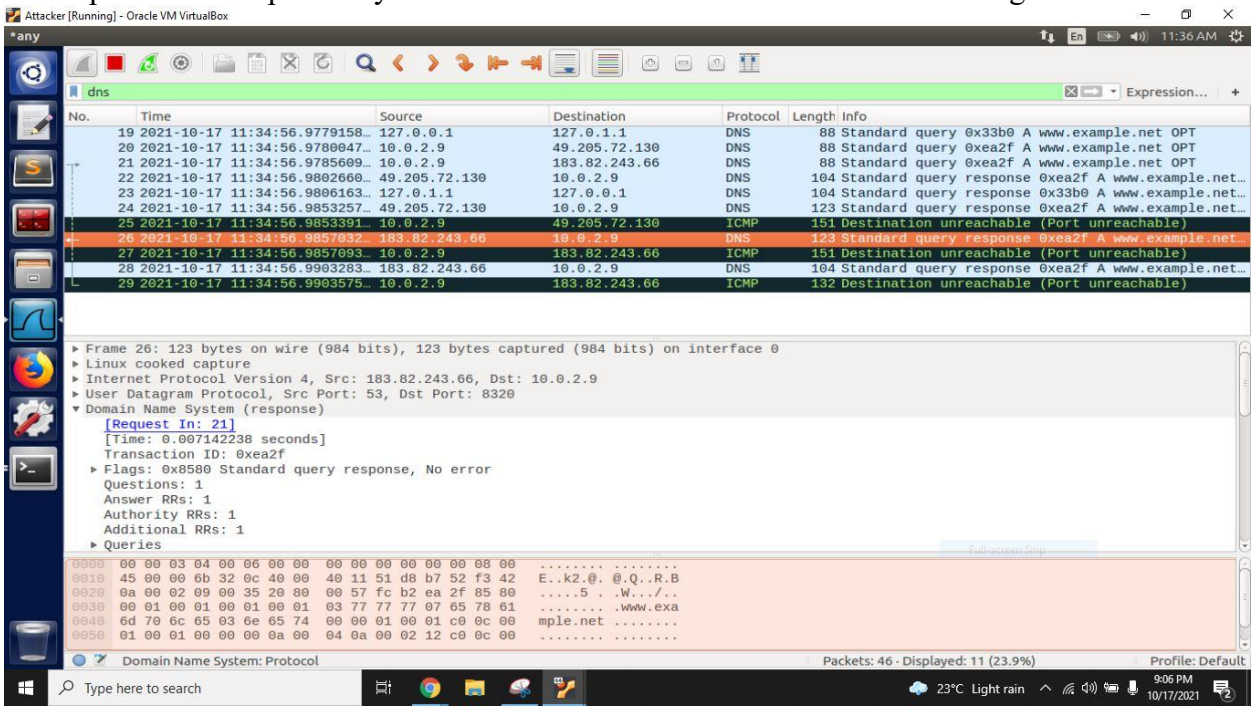
In this task we extend the above attack by targeting the another domain that is atatcker32.com
We run the below code in the attacker machine



After use of dig command the terminal observation s listed below



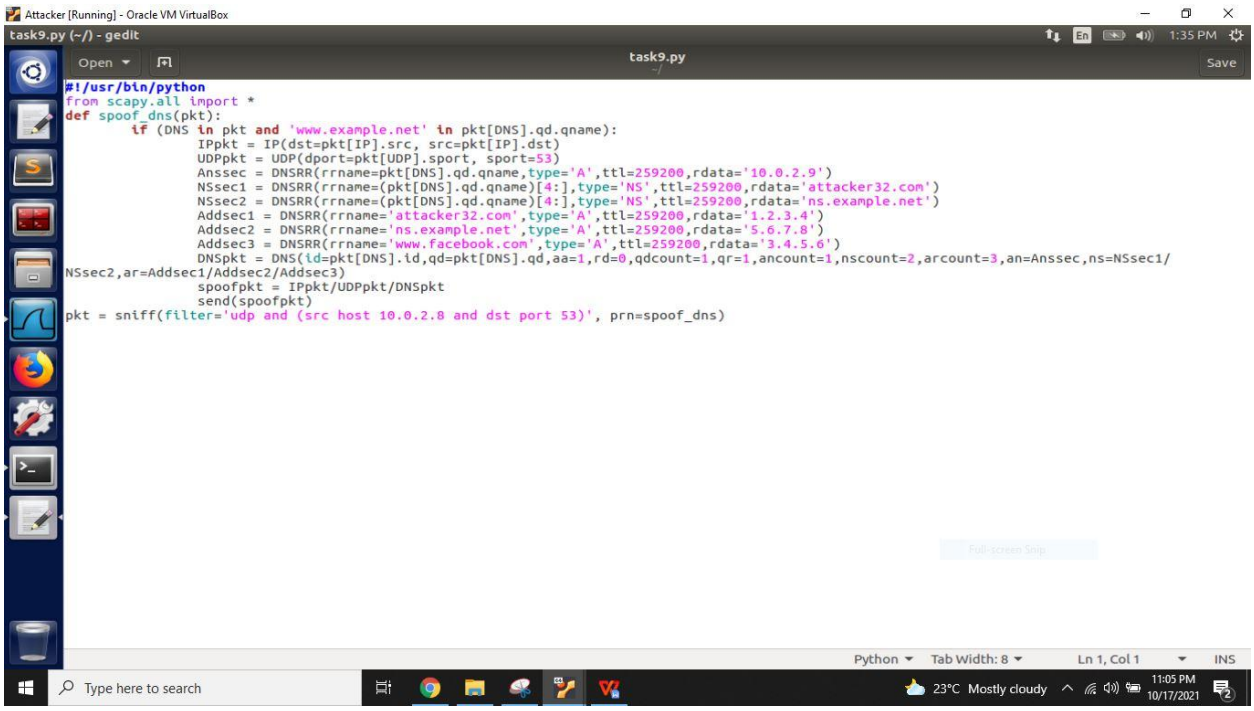
These packets are captured by wireshark and see the attacker32.com is also targeted



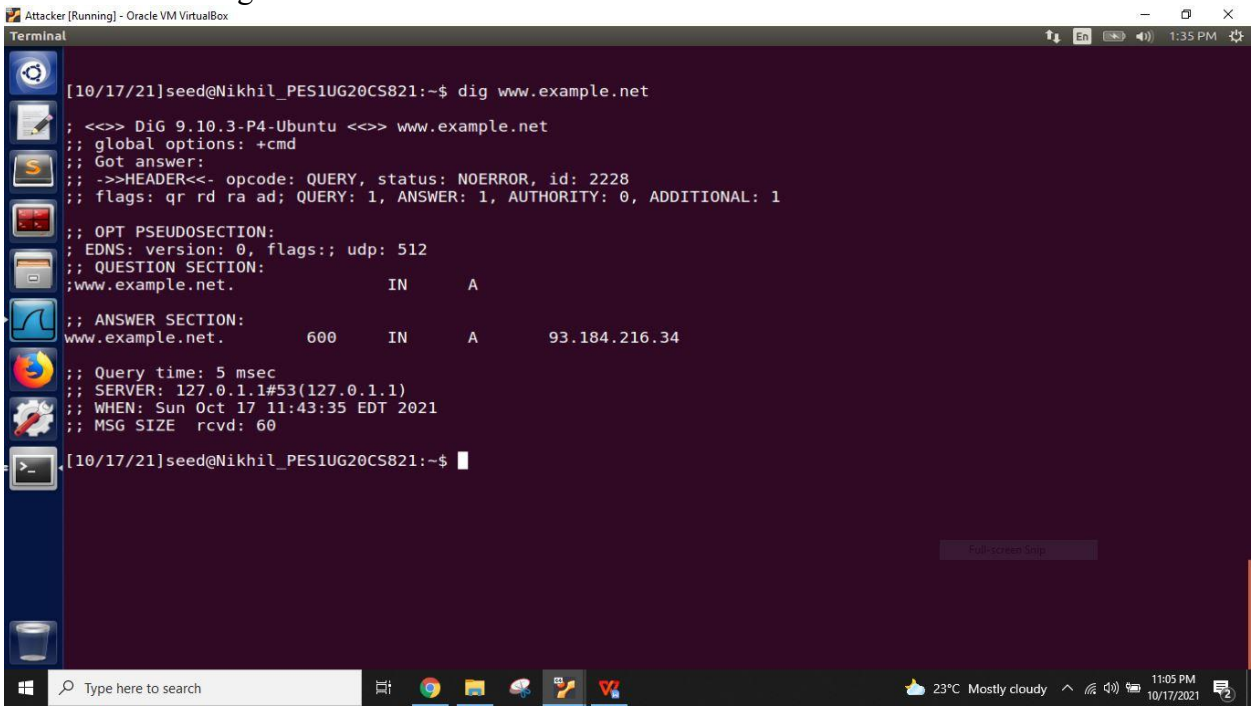
Task 9: Targeting the Additional Section

In DNS replies, there is section called Additional Section, which is used to provide additional information such as ip address especially for those which appears in the Authority section. In this task we spoof some entries in additional section

Run the below code the attacker machine



After the use of dig



Additional section getting spoofed