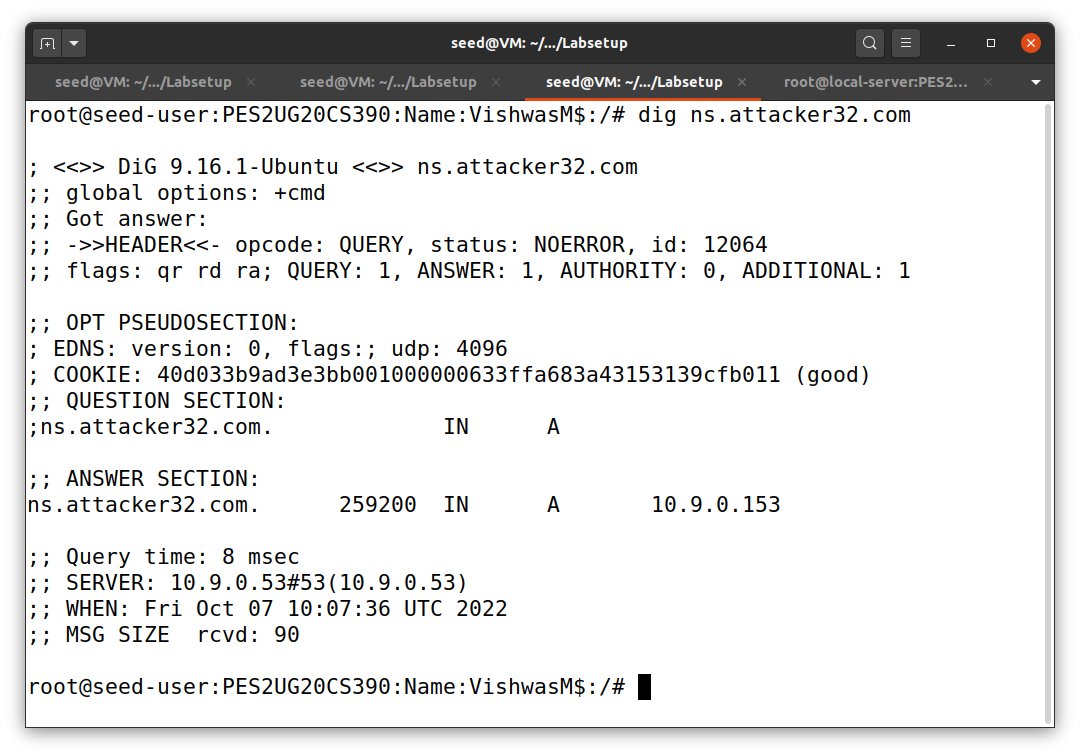
Verification of DNS Server:

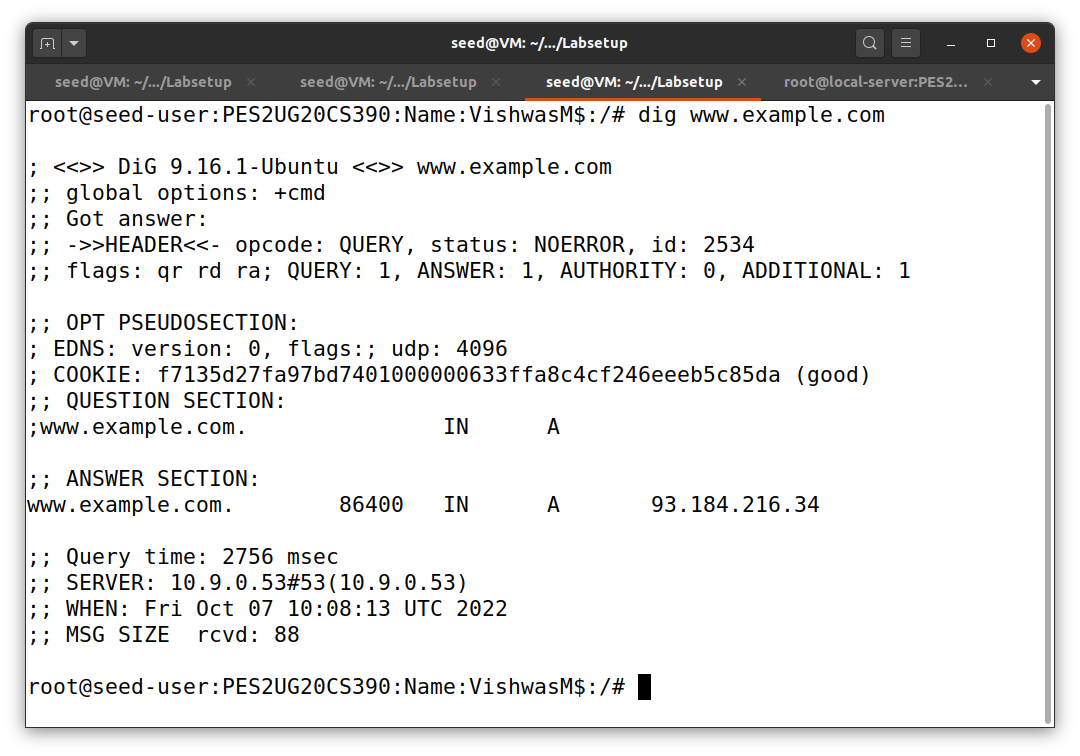
IP address of ns.attacker32.com

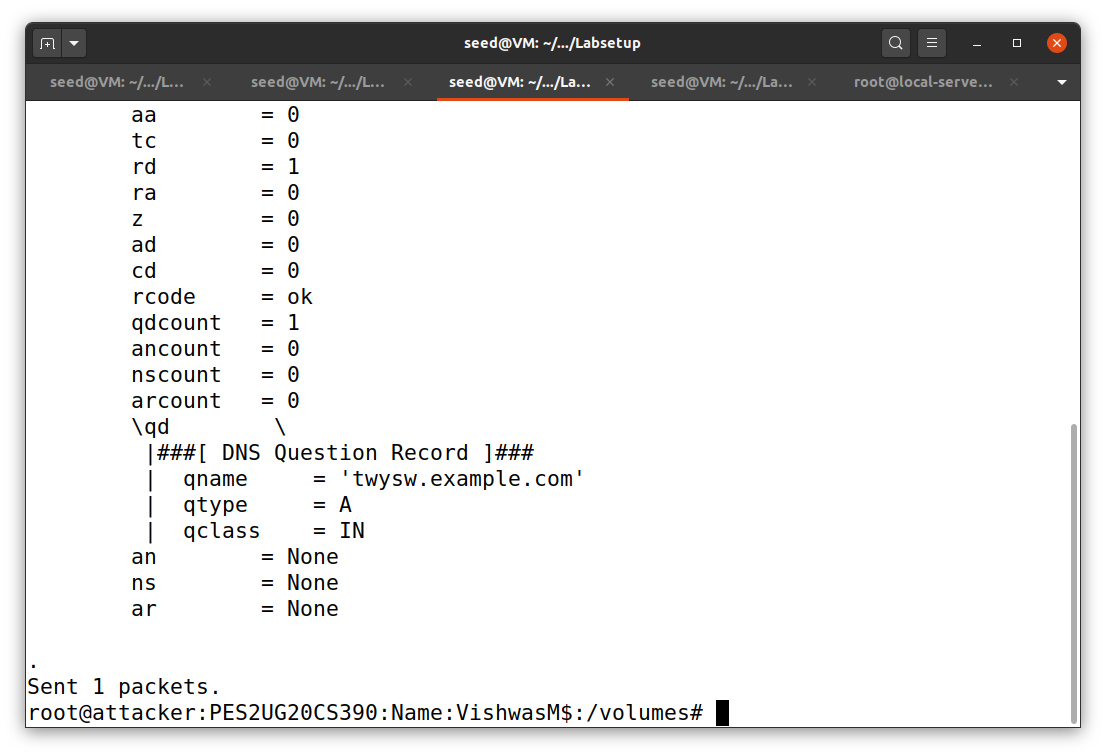


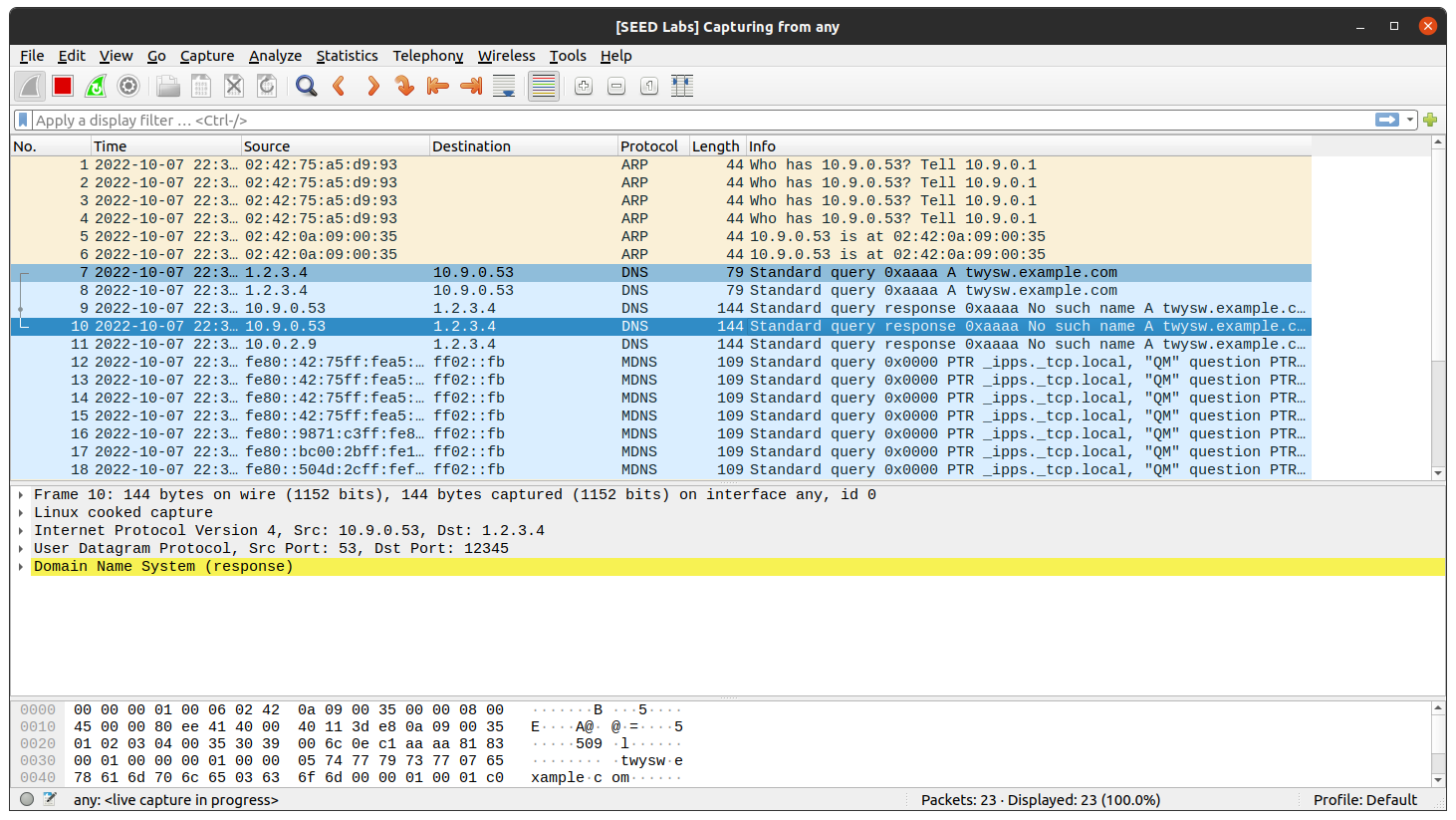
IP address of [www.example.com](http://www.example.com)

Task 1:

We are sending out the DNS queries in order to trigger the DNS server to send DNS requests. We can spoof the DNS reply only if DNS requests are sent out.





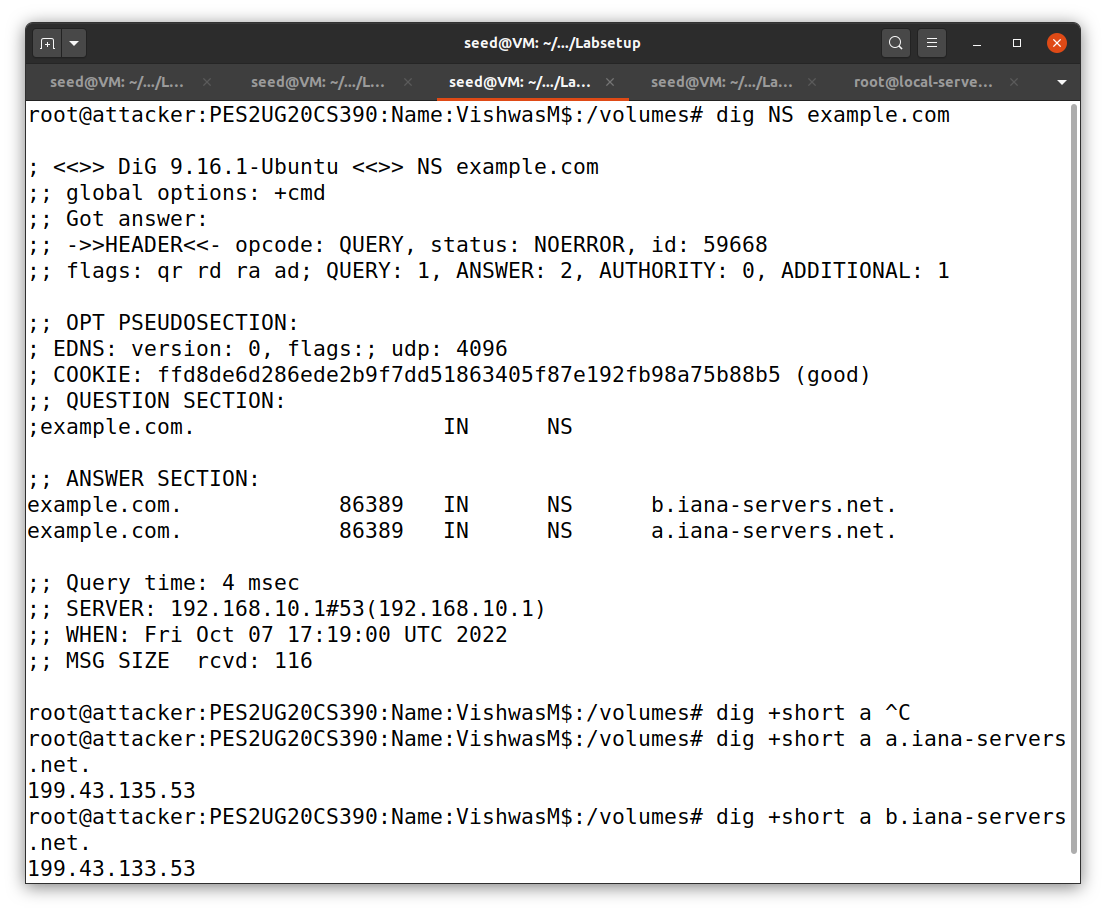


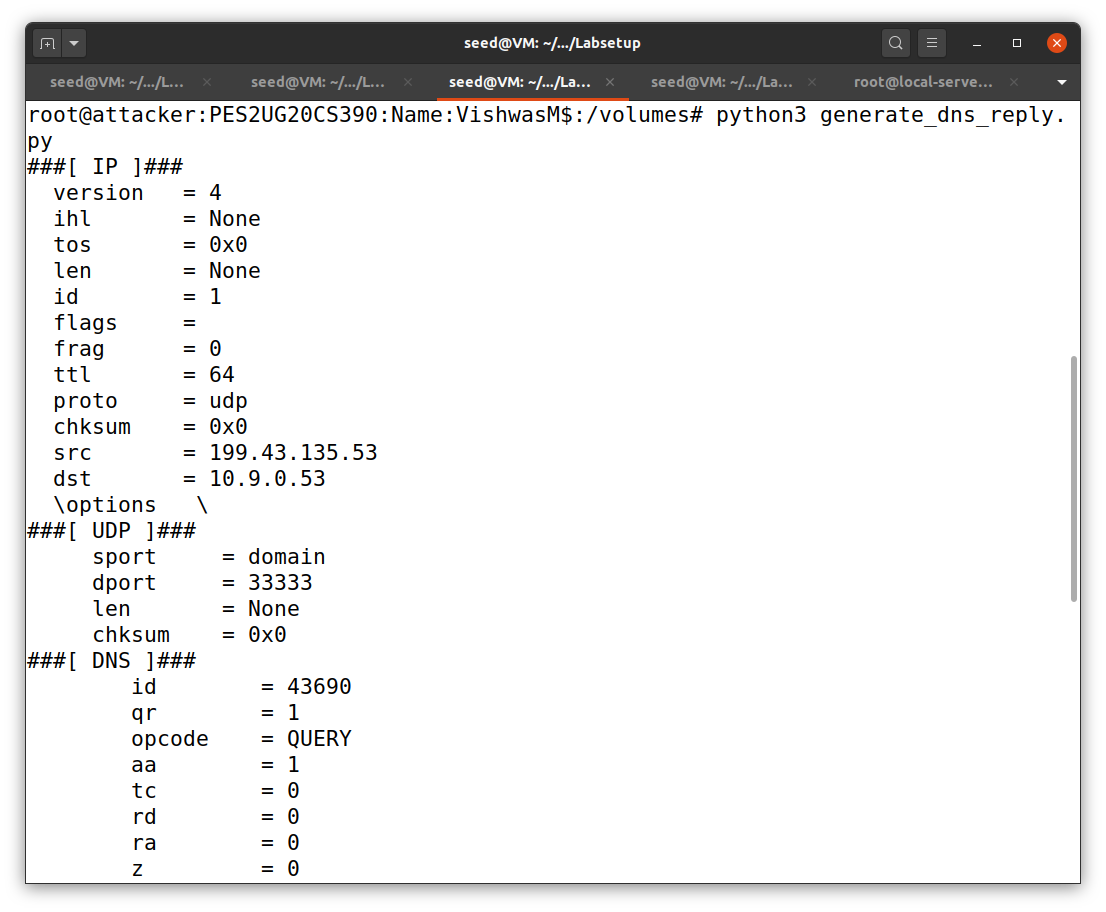
Task 2:

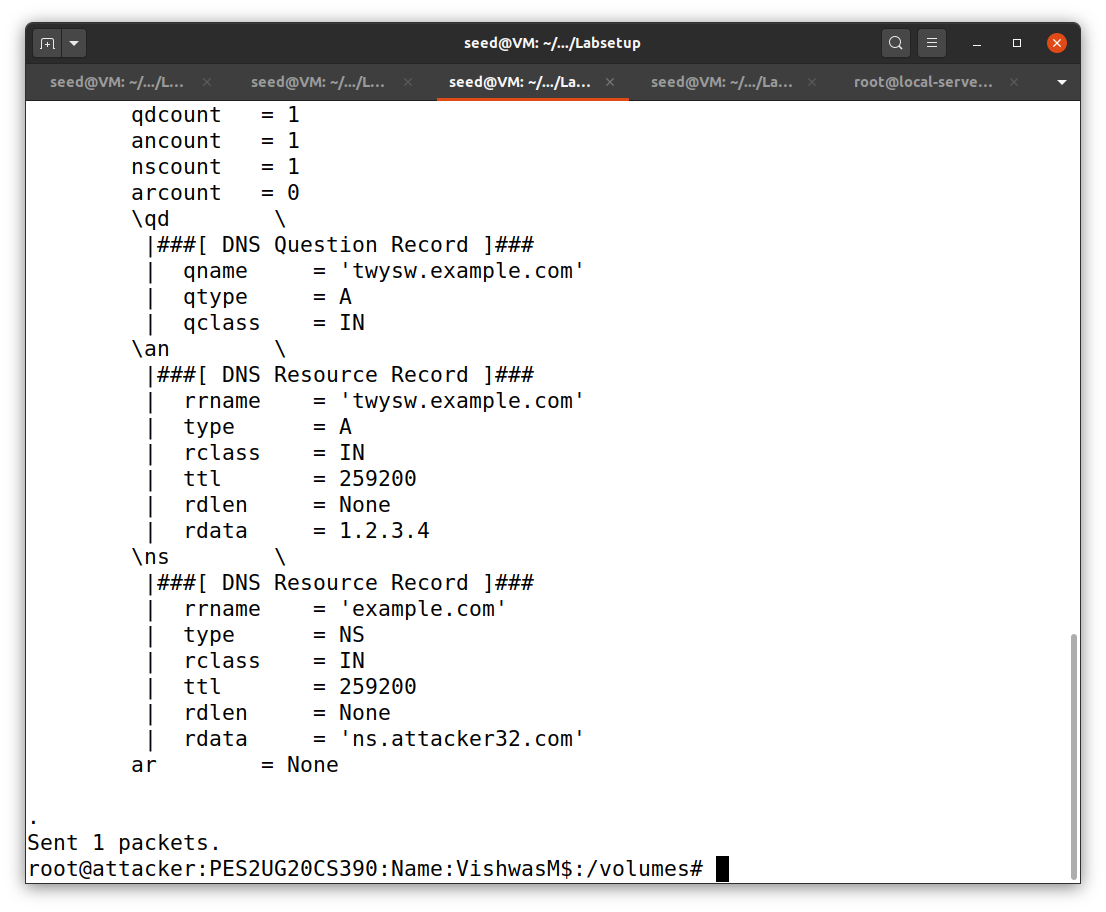
First we need to sniff the replies from the domain’s Name Server and then we have to spoof the DNS replies using Kaminsky attack.

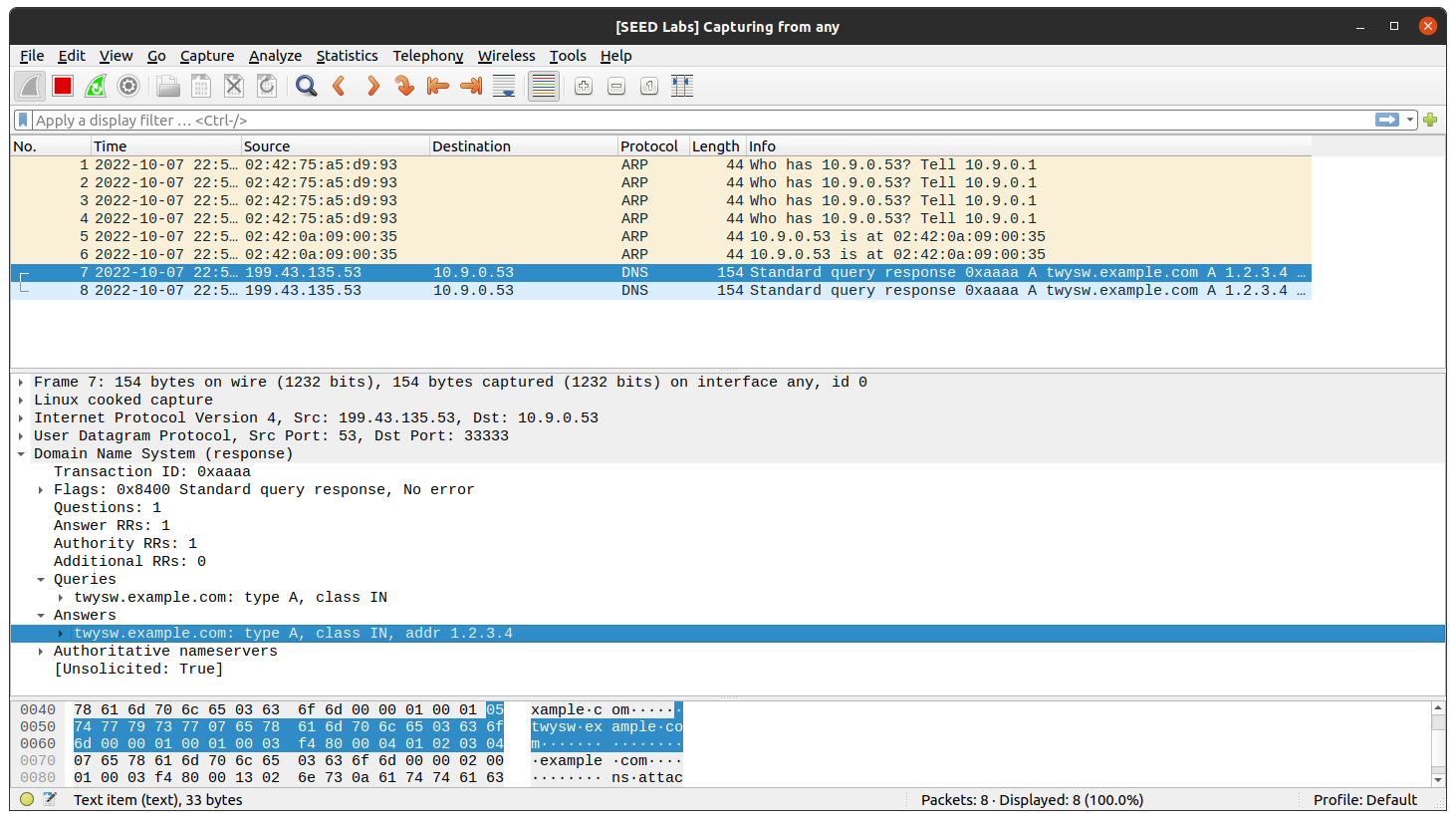
Now we have to get the IP addresses of the name server of the example.com domain.

For Name Server a.iana-servers.net. :

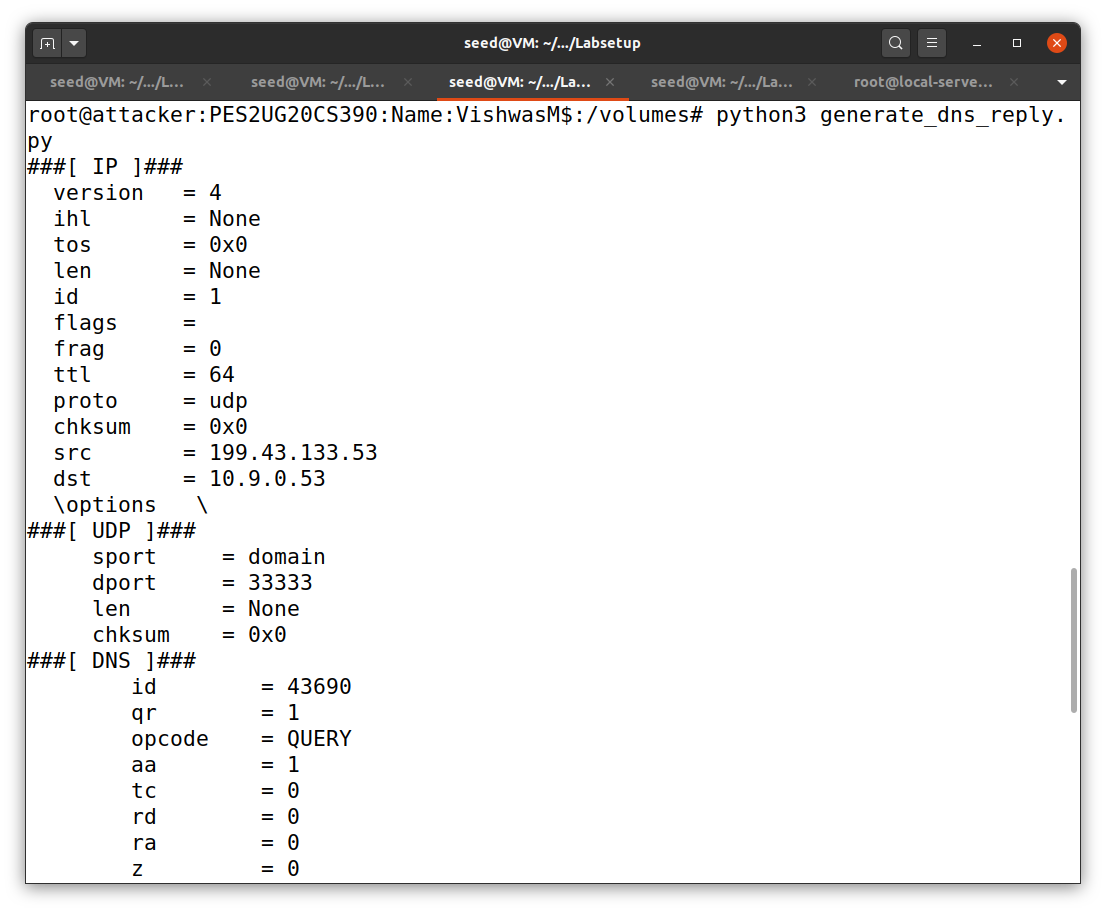


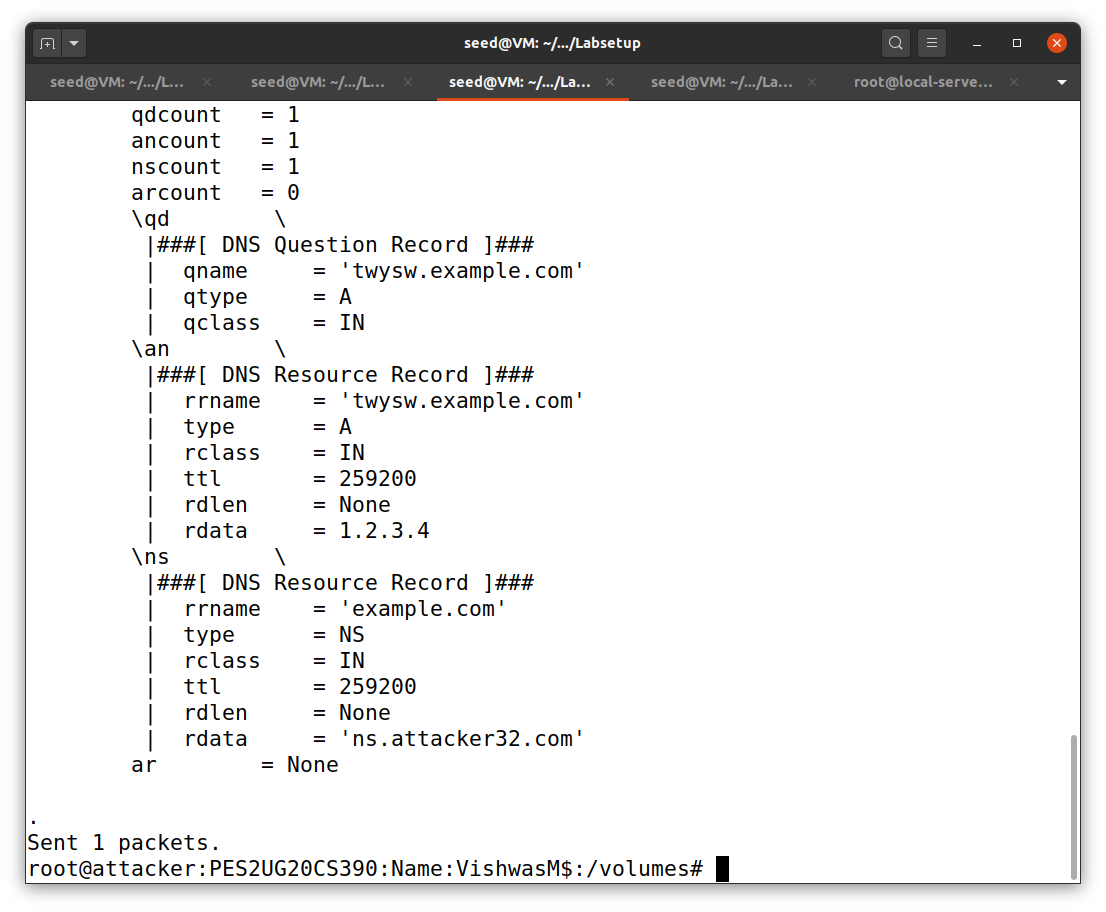


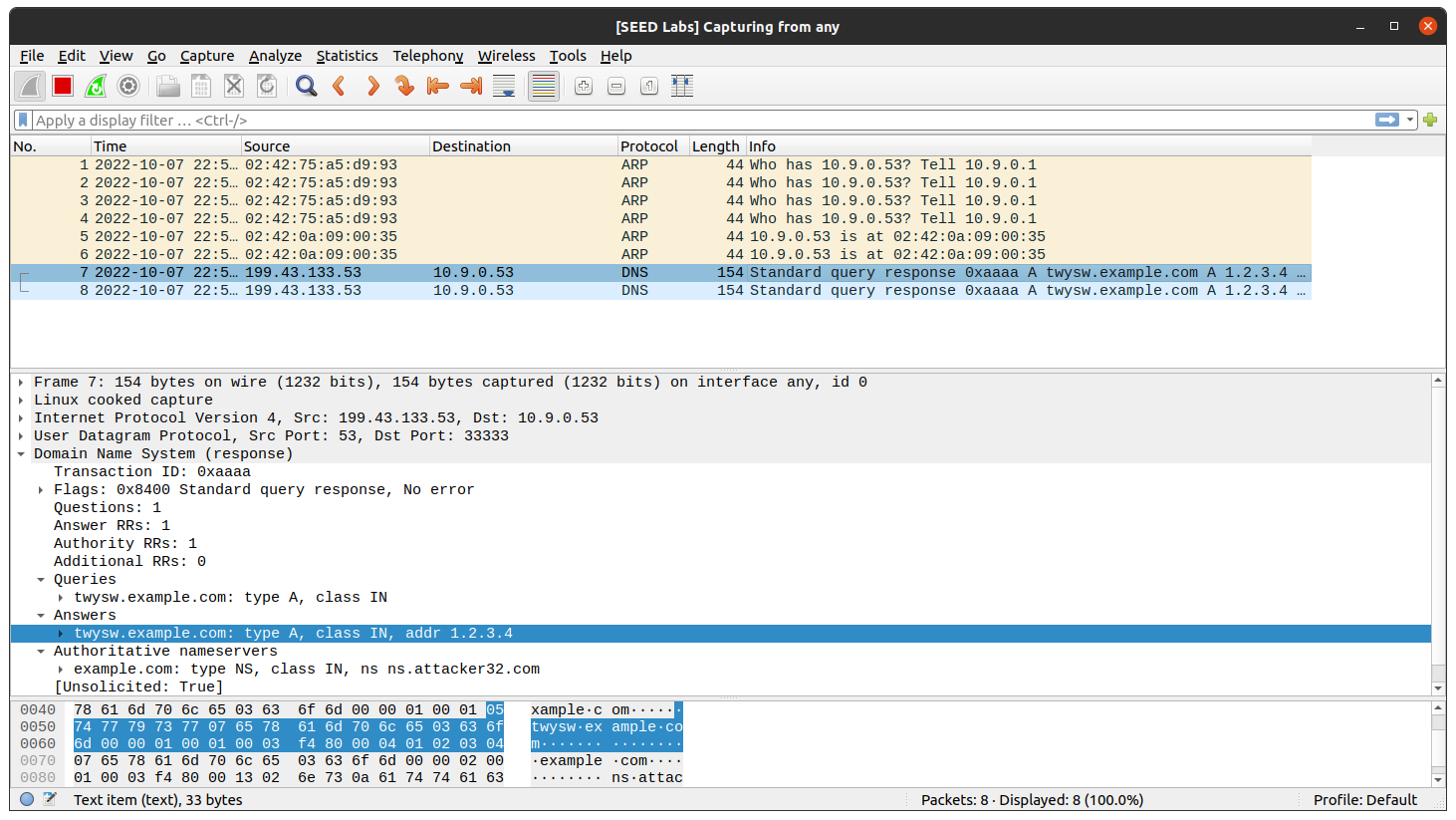




For Name Server b.iana-servers.net. :



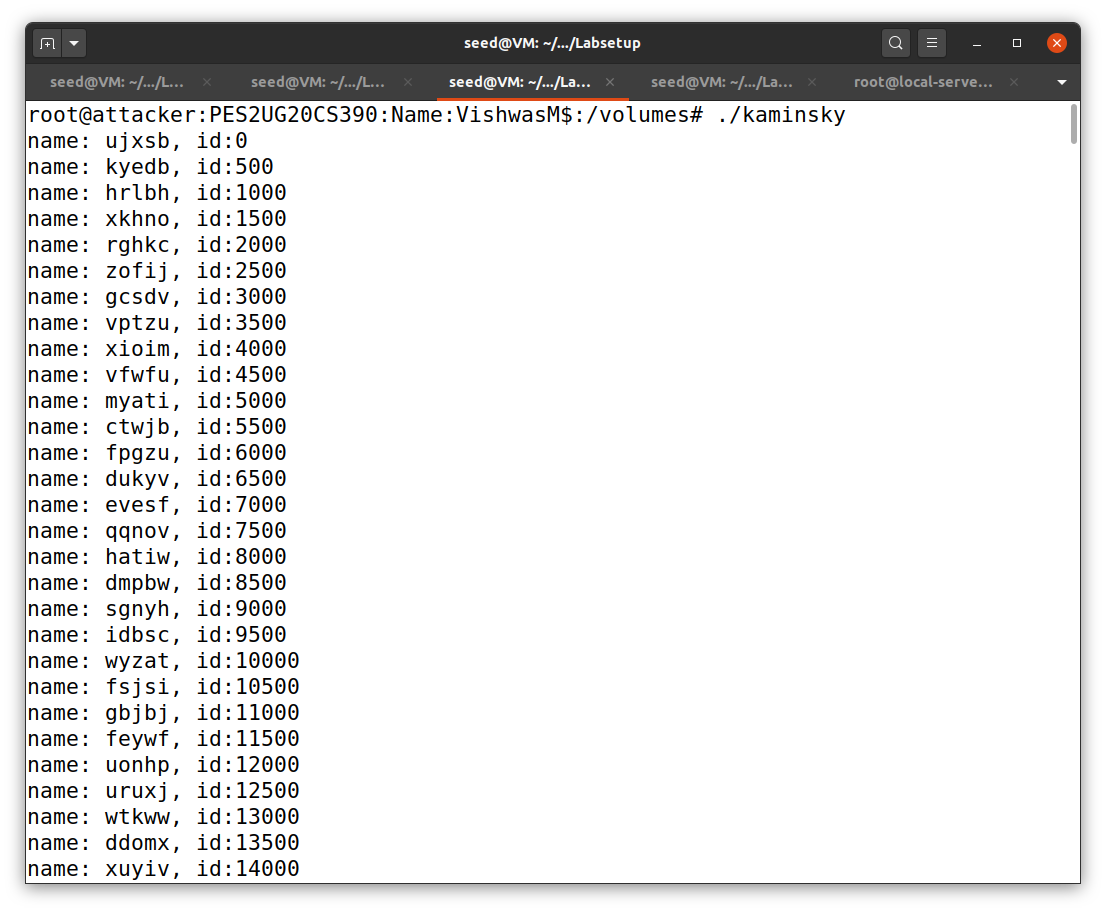




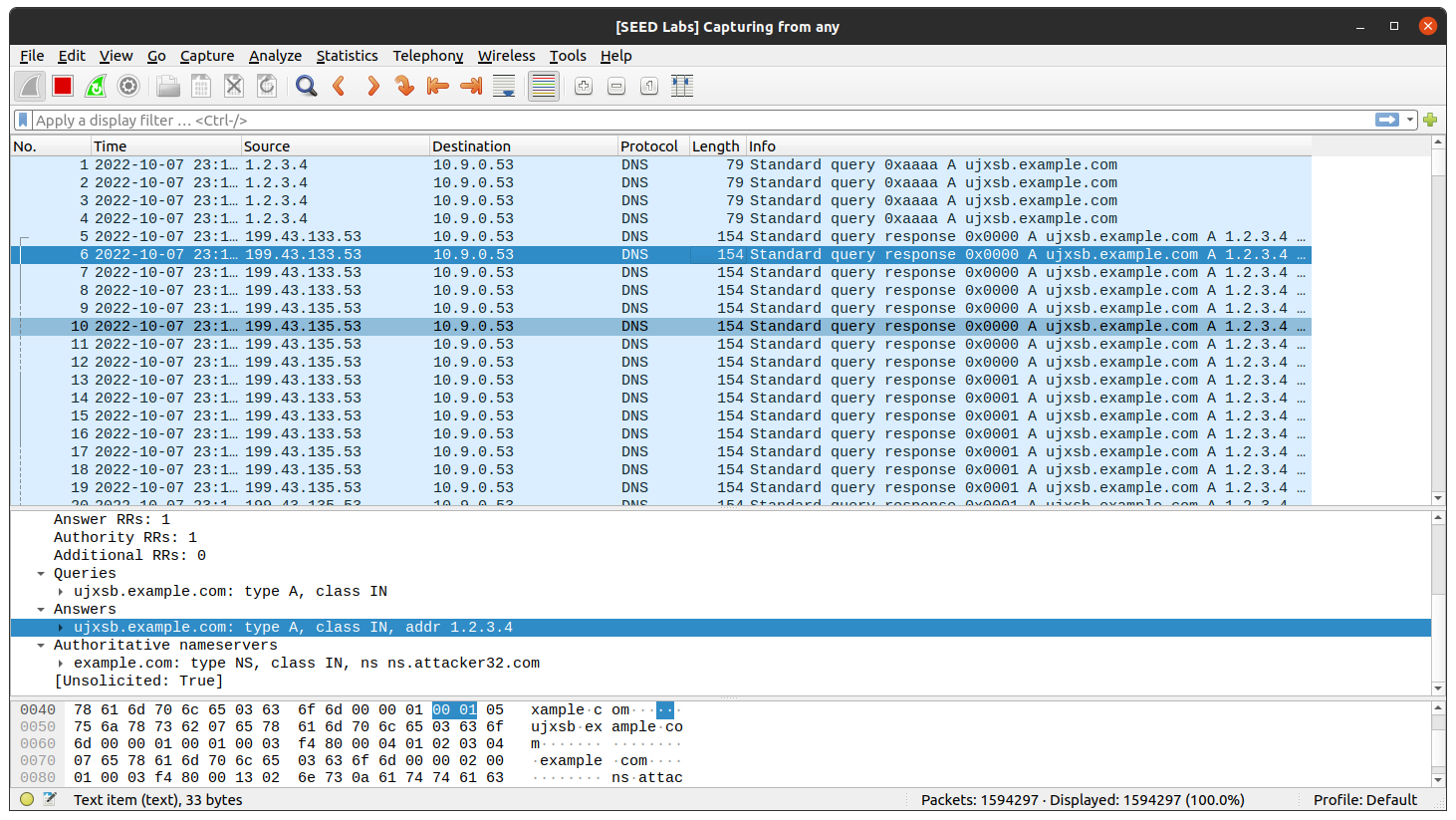
Task 3:

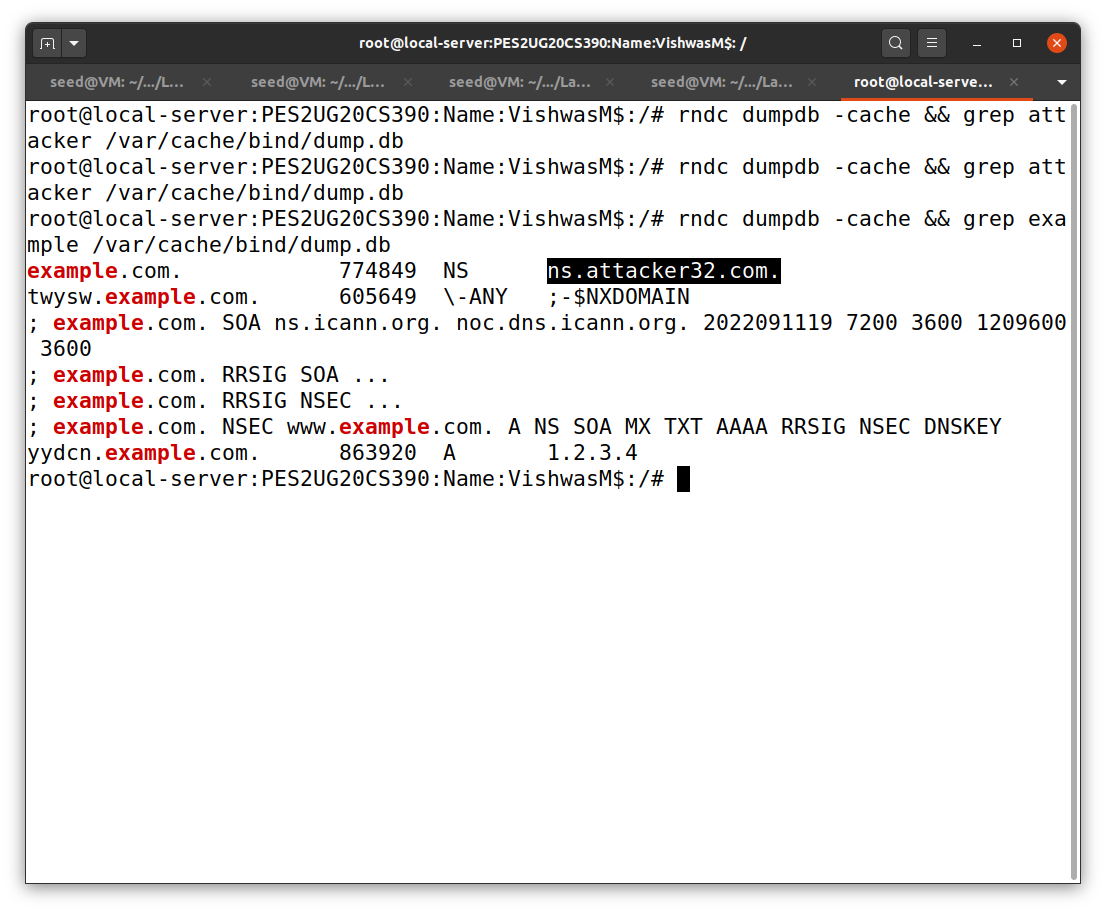
Now we need to send out many spoofed DNS replies, hoping one of them hits the correct transaction number and arrives sooner than the legitimate replies.

Here speed is the key, so more packets are sent out, the higher the success rate. So we have a hybrid approach. We can combine both scapy and C



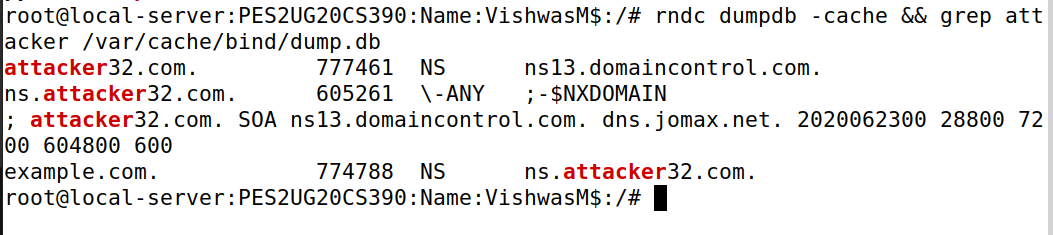
Here we are sending many DNS replies.





Here we can see that the Name Server has been changes to ns.attacker32.com

So from now onwards instead of going to the original Nameserver, it goes to the attacker.



Task 4:

If the attack is successful, in the local DNS server’s DNS cache, the NS record for example.com will become ns.attacker32.com. When this server receives a DNS query for any hostname inside the example.com domain, it will send a query to ns.attacker32.com, instead of sending to the domain’s legitimate nameserver.To verify whether your attack is successful or not, go to the User machine, run the following two dig commands. In the responses, the IP addresses for www.example.com should be the same for both commands, and it should be whatever you have included in the zone file on the Attacker nameserver.

