COMPUTER NETWORKS LAB

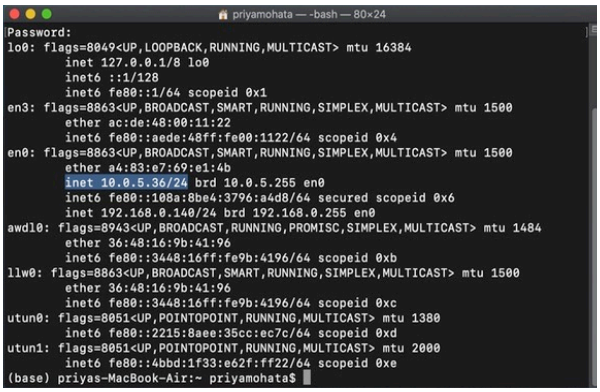
COURSE CODE:UE19CS255

NAME:PRIYA MOHATA SRN:PES2UG19CS301

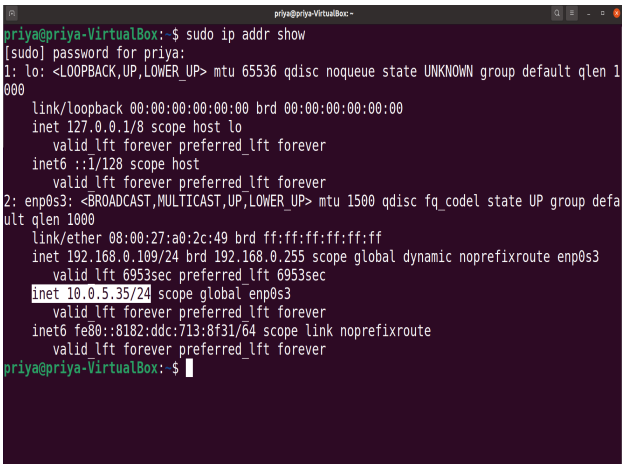
SECTION:E DATE:21/02/2021

EXPERIMENT: DNS (Domain Name System) is the Internet's phone book; it translates hostnames to IP addresses (and vice versa). This translation is through DNS resolution, which happens behind the scene.

DNS Client : 10.0.5.36

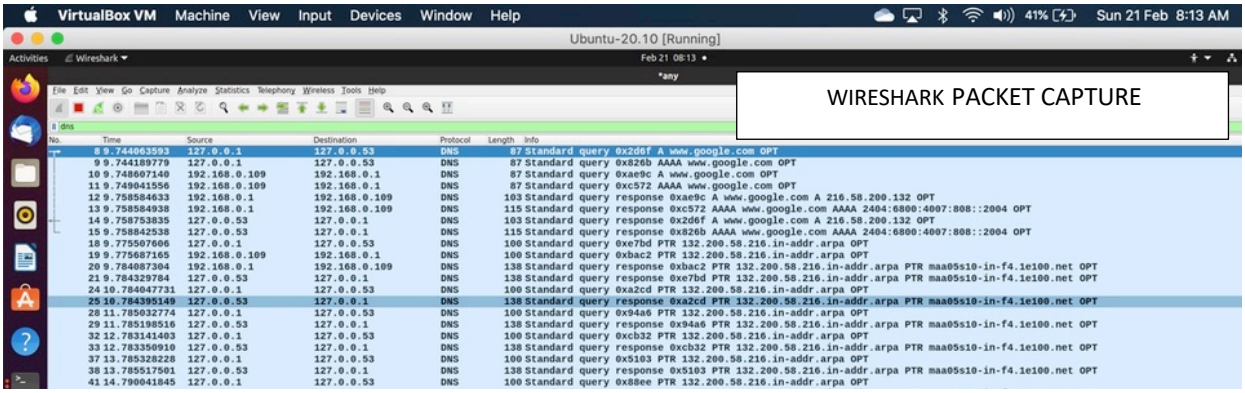


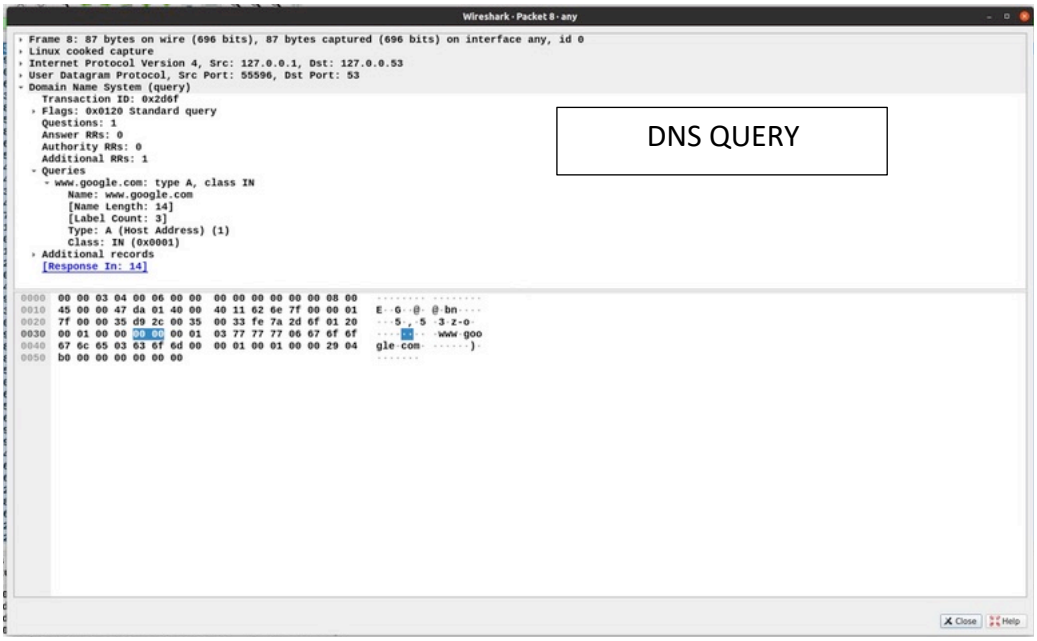
DNS Server : 10.0.5.35

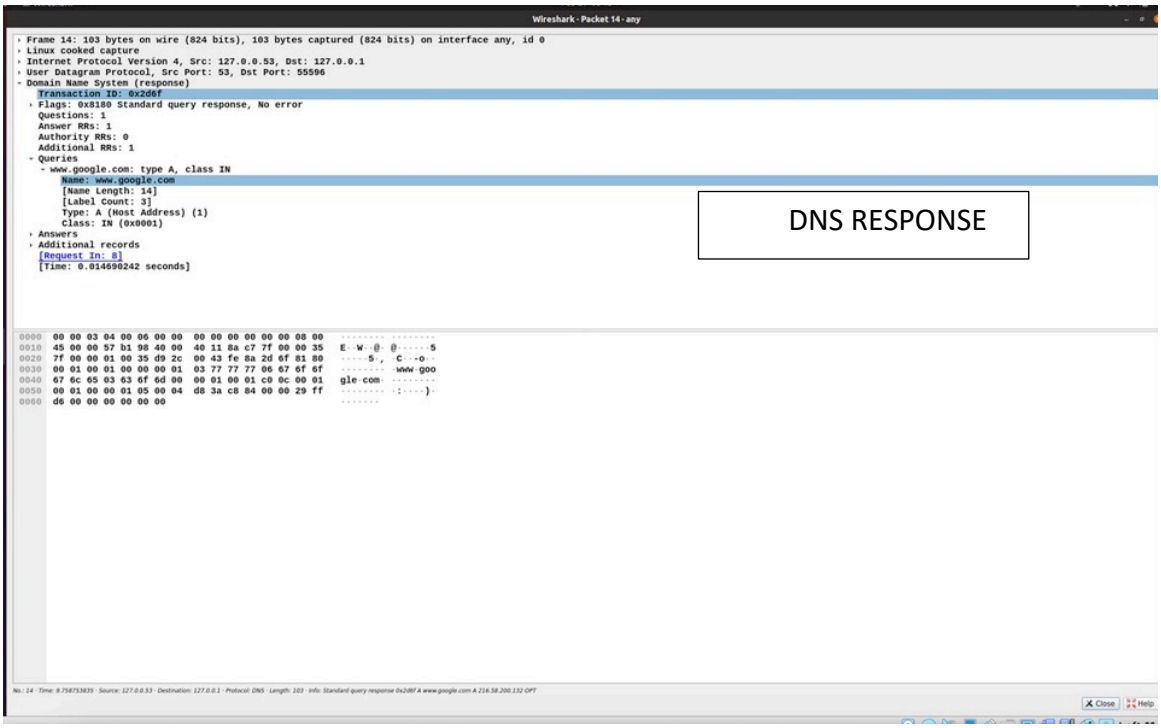


OBSERVATION 1 : First Test – Pinging using default DNS

- Wireshark is used to capture the packets in the background while pinging www.google.com
- The IP Address of the Local DNS server is observed to be 127.0.0.53.
- The query is of type A which stands for authoritative. The answer contains the A type record along with the IP address of the website 142.250.76.36
- The first query and authoritative response are shown below



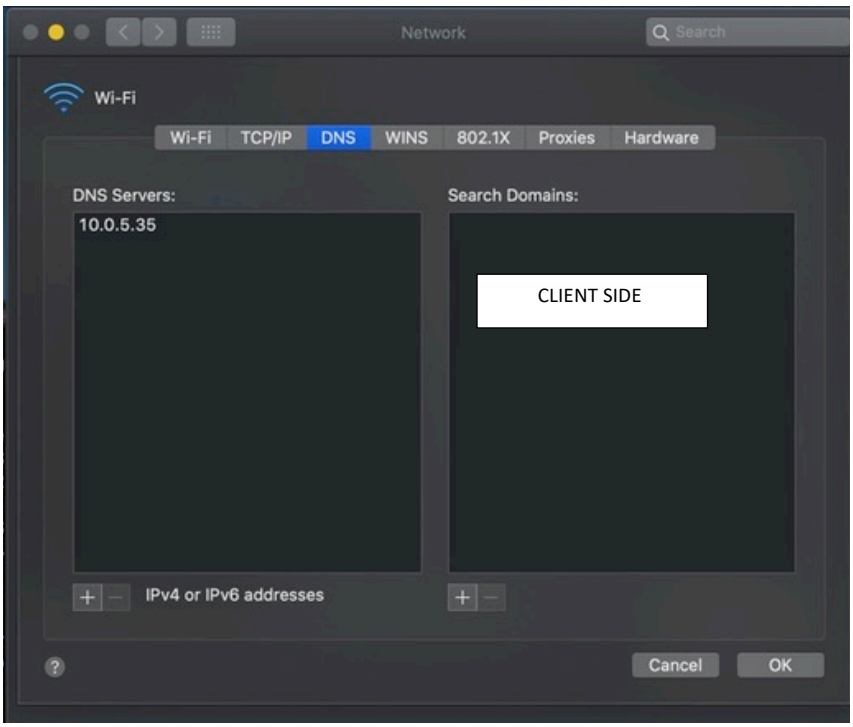




DNS RESPONSE

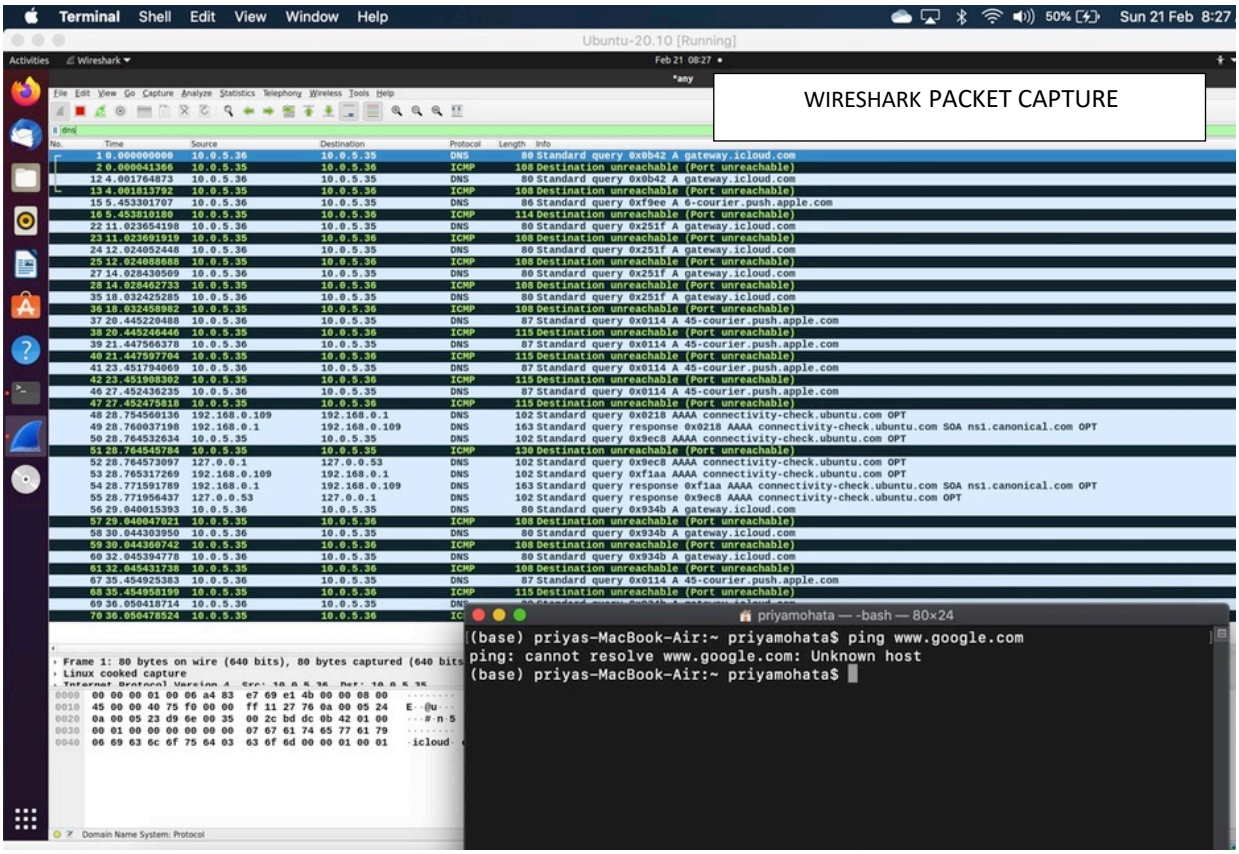
OBSERVATION 2 : Configuring Client Machine

- The IP Address of the client machine is **10.0.5.36** and the IP Address of the server machine is **10.0.5.35**
- We need to add the IP Address of the custom DNS server (10.0.5.35) to the client
- machine.
- This is done by adding the IP address of the server to the file **/etc/resolvconf/resolv.conf.d/head** which stores the order of DNS server resolution. This ensures that the custom DNS server will be used to resolve names.
- The IP Address of the custom DNS server is also added to the DNS menu under theIPv4 Network Settings.
- The changes are applied by using the command **sudo resolvconf -u**



OBSERVATION 3 : TESTING PING WWW.GOOGLE.COM AGAIN

- The google website is pinged again, and Wireshark is used to capture packets.
- We obtain a destination unreachable error in Wireshark as the server machine does not have a DNS server associated with it
- The client tries to obtain the DNS record from 10.0.5.35 but it does not receive any



OBSERVATION 4 : Setting Up Local DNS Server

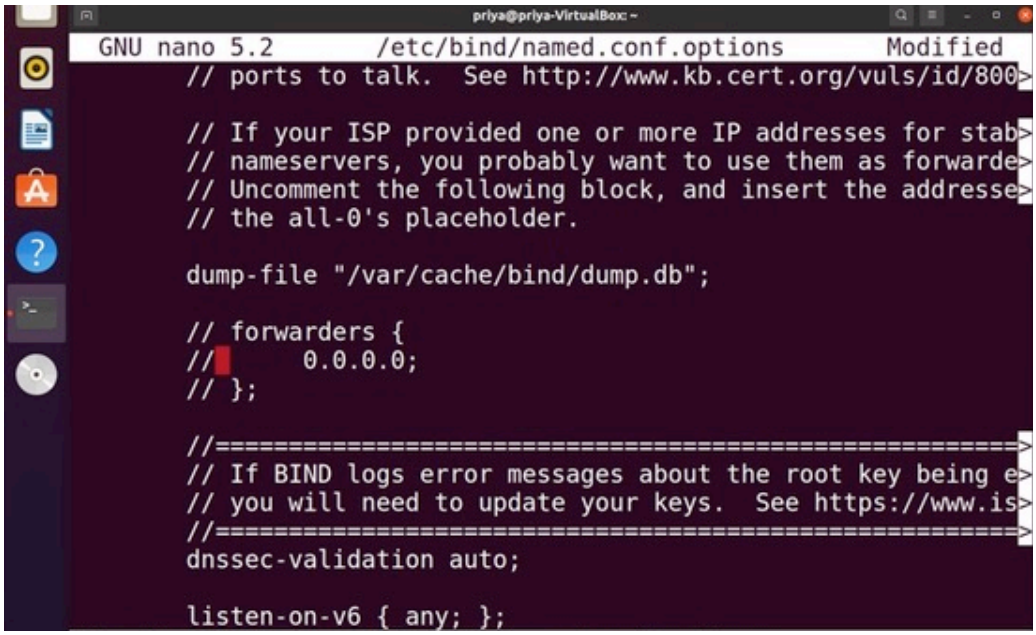
COMMAND USED TO INSTALL BIND9 SERVER

$ sudo apt-get update
$ sudo apt-get install bind9

```
priya@priya-VirtualBox:~$ sudo apt-get install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  bind9-dnsutils bind9-libs bind9-utils python3-ply
Suggested packages:
  bind-doc python-ply-doc
The following NEW packages will be installed:
  bind9 bind9-utils python3-ply
```

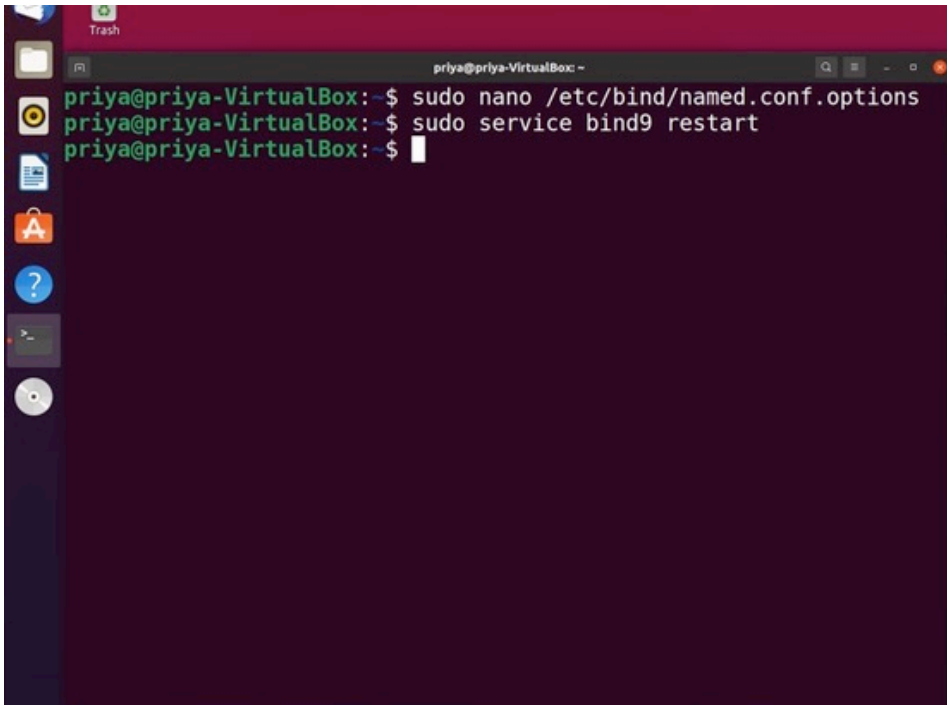
STEP 1 : CONFIGURING BIND9 SERVER

- BIND9 gets its configuration from a file called **/etc/bind/named.conf**. This file is the primary configuration file, and it usually contains several “include” entries
- One of the included files is called **/etc/bind/named.conf.options**
- This is where we typically set up the configuration options.
- BIND dumps the cache to a default file called **/var/cache/bind/dump.db.**

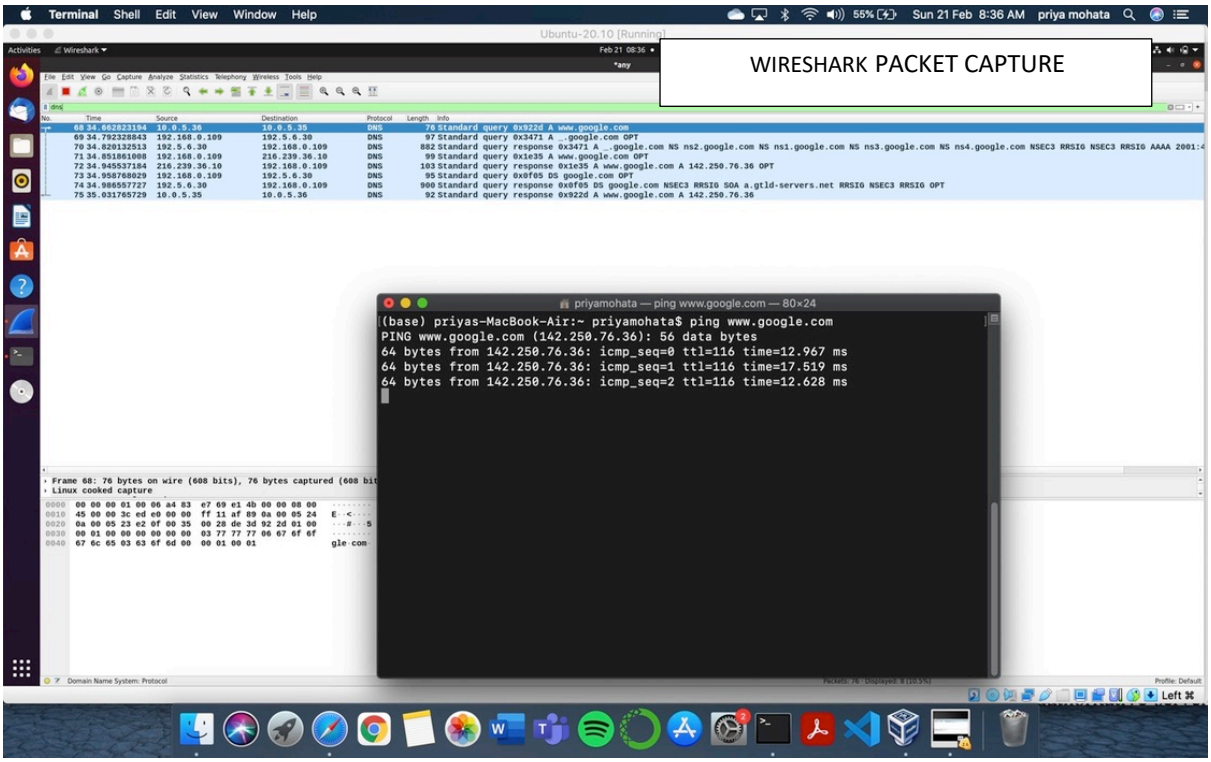


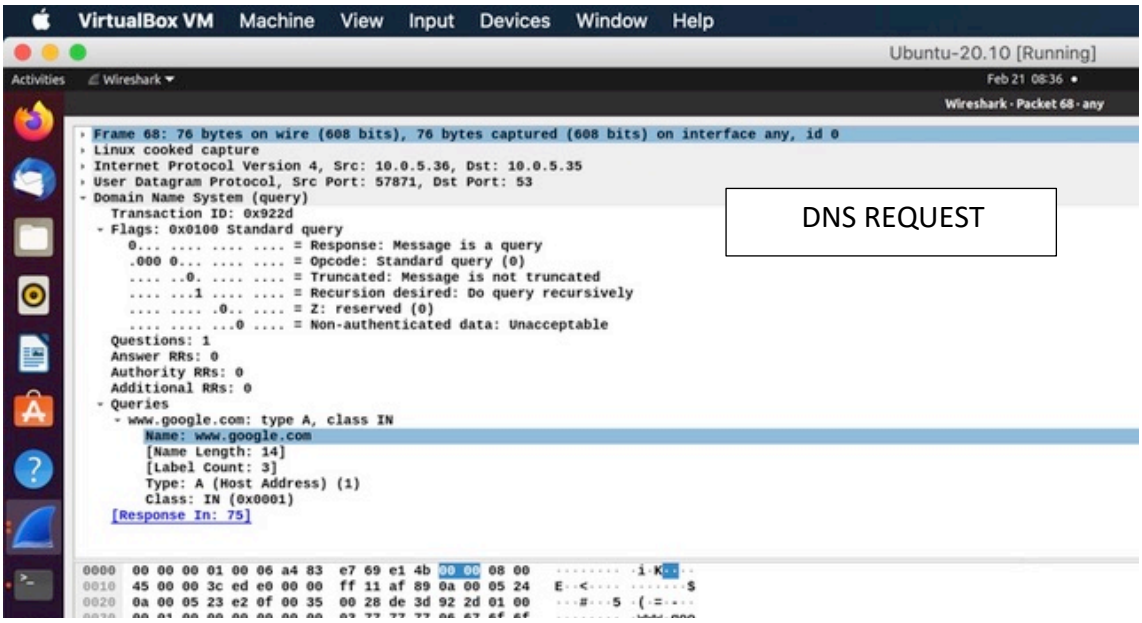
We start the DNS server using the command:

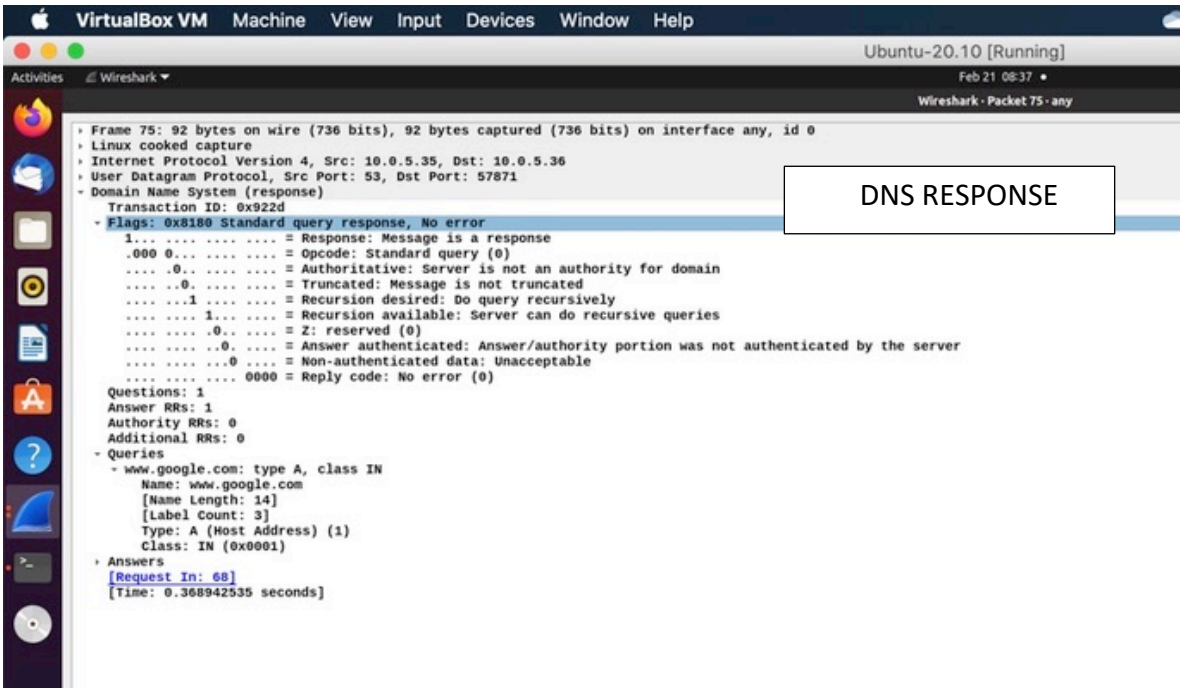
$ sudo service bind9 restart



We go back to your user machine (10.0.5.36), and ping a computer such as www.google.com

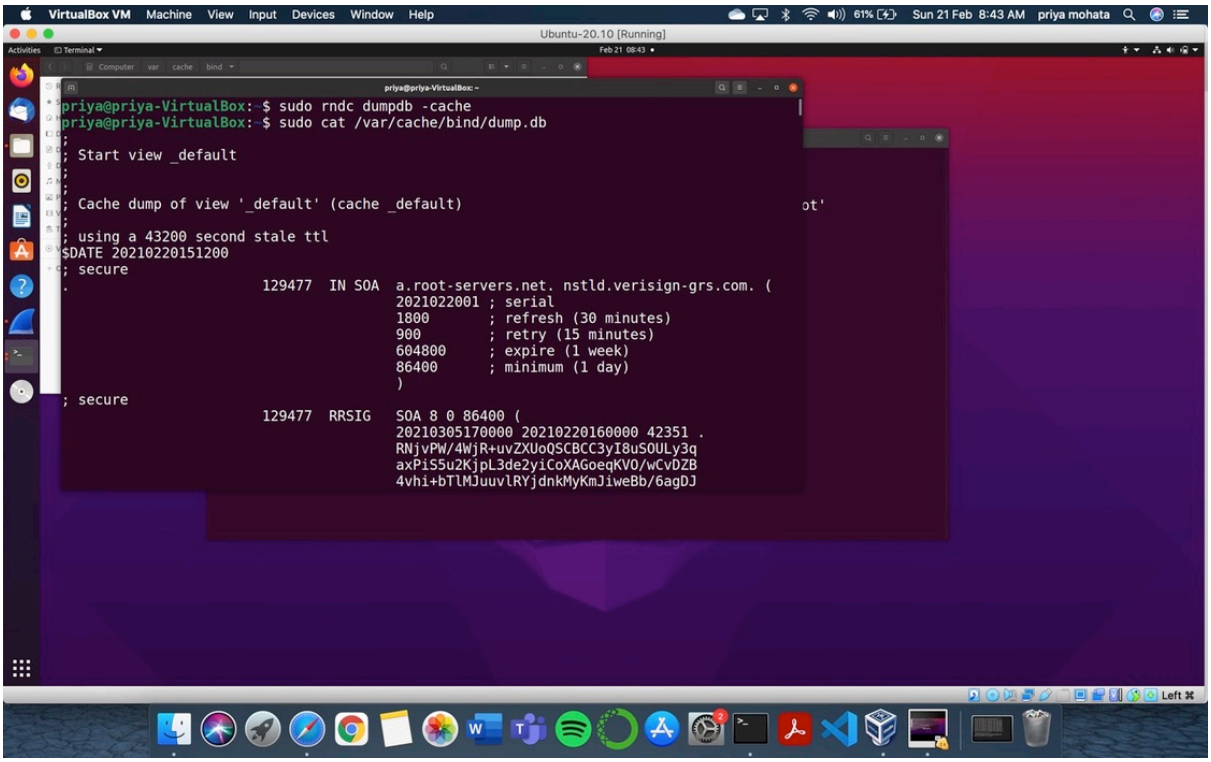



VirtualBox VM Machine View Input Devices Window Help
Ubuntu-20.10 [Running]
Activities Wireshark Feb 21 08:36
Wireshark · Packet 68 · any
Frame 68: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.5.36, Dst: 10.0.5.35
User Datagram Protocol, Src Port: 57871, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x922d
Flags: 0x0100 Standard query
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... .0.. .... = Z: reserved (0)
....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.google.com: type A, class IN
Name: www.google.com
[Name Length: 14]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
[Response In: 75]
0000 00 00 00 01 00 06 a4 83 e7 69 e1 4b 00 00 08 00
0010 45 00 00 3c ed e0 00 00 ff 11 af 89 0a 00 05 24
0020 0a 00 05 23 e2 0f 00 35 00 28 de 3d 92 2d 01 00
DNS REQUEST

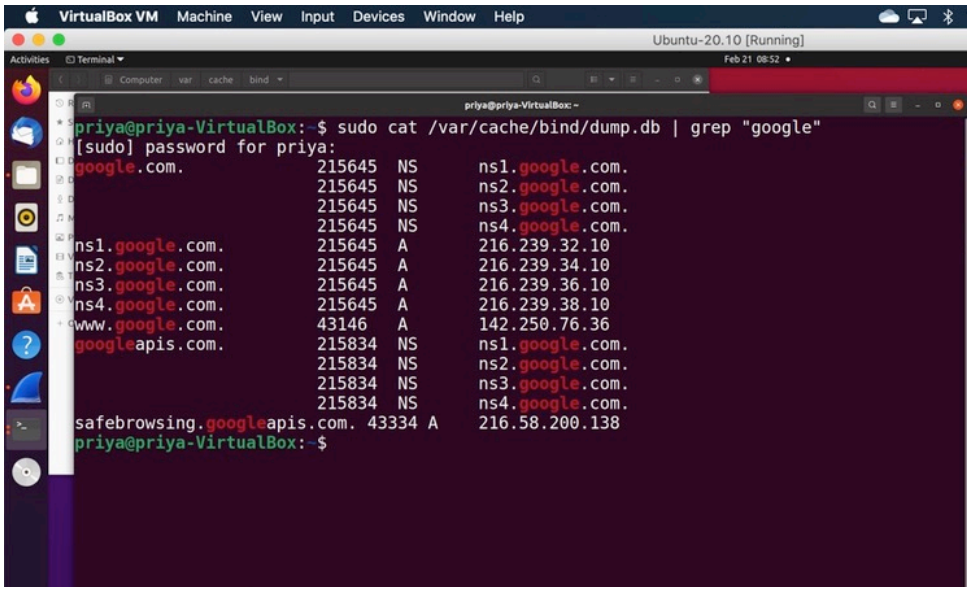

VirtualBox VM Machine View Input Devices Window Help
Ubuntu-20.10 [Running]
Activities Wireshark Feb 21 08:37
Wireshark · Packet 75 · any
Frame 75: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.5.35, Dst: 10.0.5.36
User Datagram Protocol, Src Port: 53, Dst Port: 57871
Domain Name System (response)
Transaction ID: 0x922d
Flags: 0x8180 Standard query response, No error
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
www.google.com: type A, class IN
Name: www.google.com
[Name Length: 14]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
[Request In: 68]
[Time: 0.368942535 seconds]
DNS RESPONSE

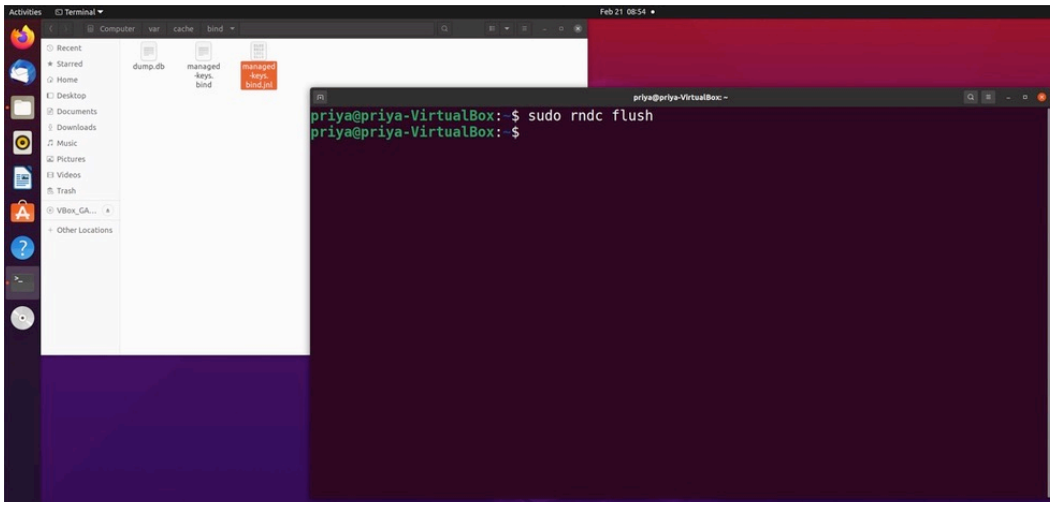
OBSERVATION 5 : Viewing the cache file

- The cache can be dumped into the file using **sudo rndc dumpdb -cache** and can be cleared or flushed out using **sudo rndc flush.**



- The linux command to extract cache for www.google.com from dump.db file,
- **sudo cat /var/cache/bind/dump.db | grep "google"**



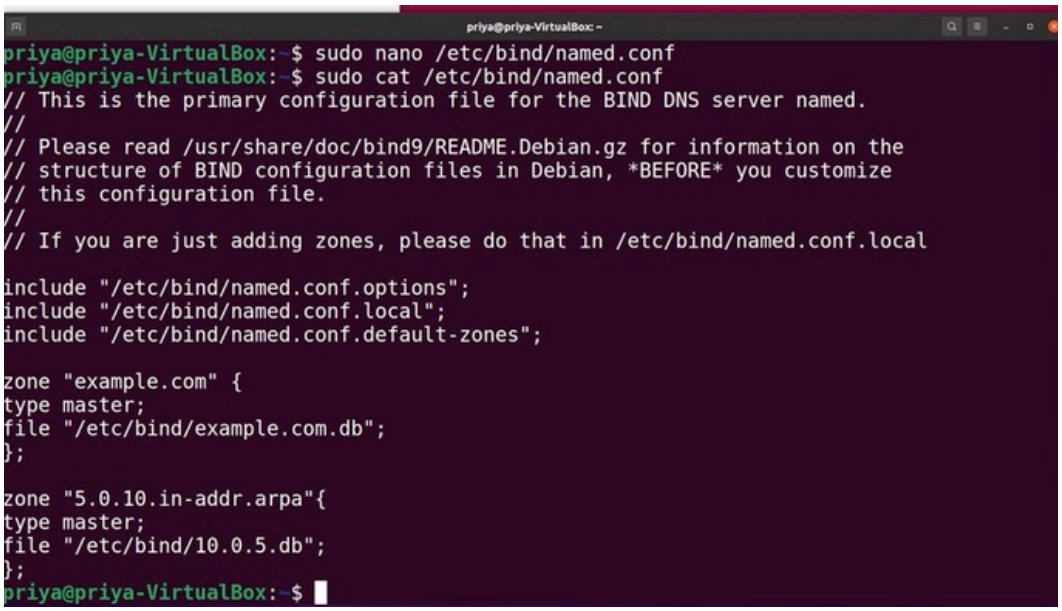

Activities
Terminal
Feb 21 08:54
Computer
var
cache
bind
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
VBox_GA...
Other Locations
dump.db
managed-keys.bind
managed-keys.bind.jnl
priya@priya-VirtualBox: ~
priya@priya-VirtualBox:~$ sudo rndc flush
priya@priya-VirtualBox:~$

OBSERVATION 6 : Host a Zone in the Local DNS server

- We will use our local DNS server as the authoritative nameserver for the domain. In this lab, we will set up an authoritative server for the **example.com** domain. This domain name is reserved for use in documentation, and is not owned by anybody, so it is safe to use it.

Step 1: Create Zones

- We had two zone entries in the DNS server by adding the following contents to **/etc/bind/named.conf** as shown in the below screenshot. The first zone is for forward lookup (from hostname to IP), and the second zone is for reverse lookup (from IP to hostname).

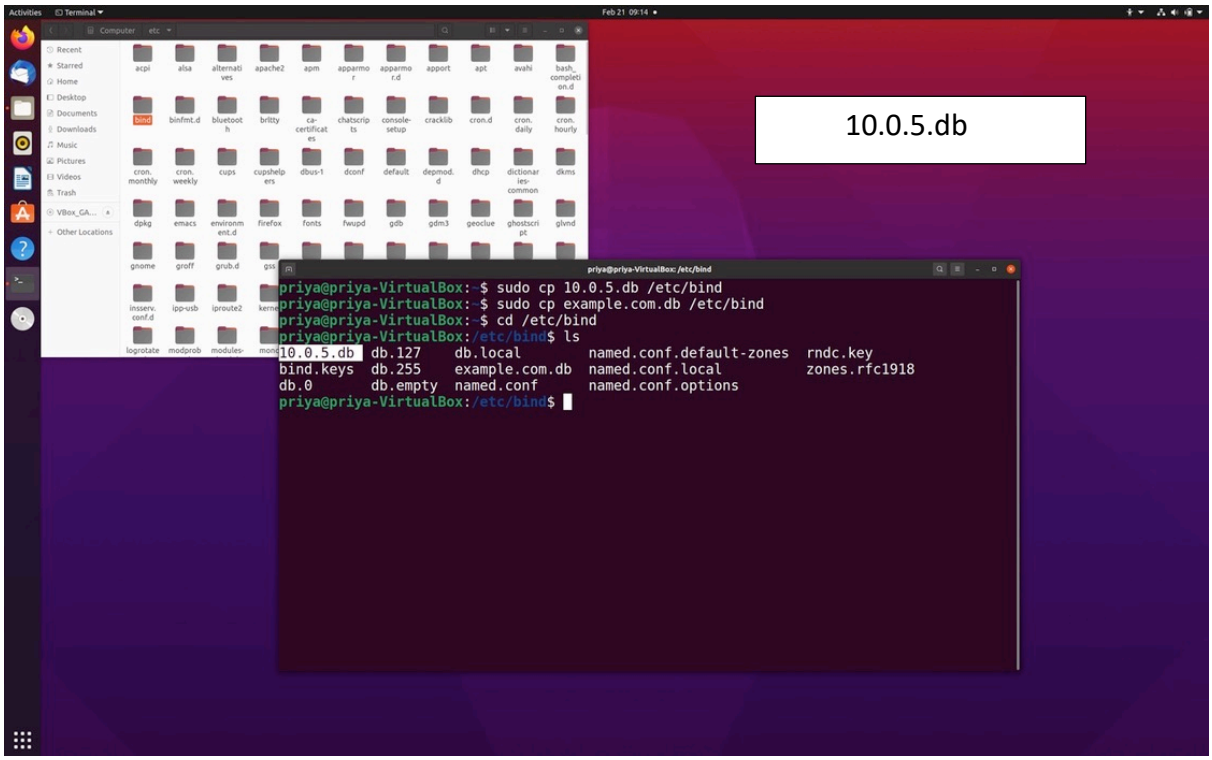


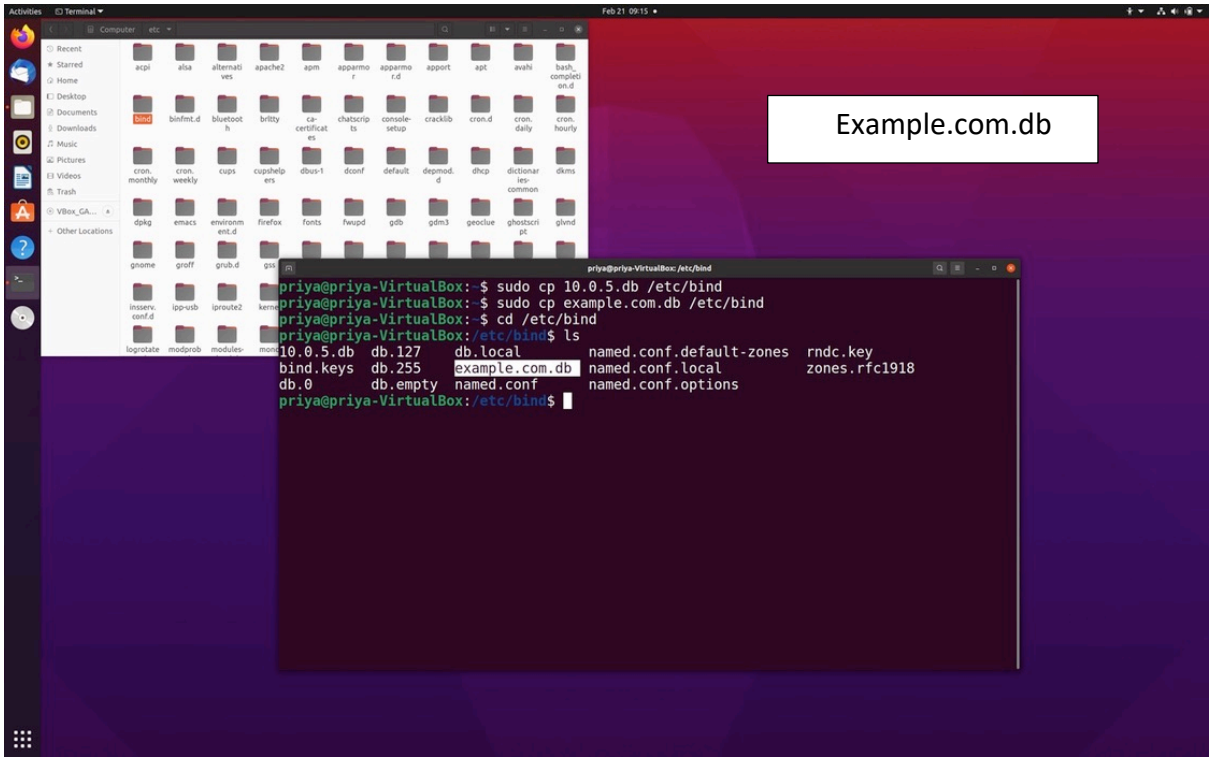
Step 2: Setup the forward lookup zone file

- We create **example.com.db** zone file with the following contents in the **/etc/bind/** directory where the actual DNS resolution is stored.

- We create **10.0.5.db** zone file with the following contents in the **/etc/bind/** directory where the actual DNS resolution is stored.

Step 3: Copy the above files into **/etc/bind** location.


10.0.5.db
priya@priya-VirtualBox: /etc/bind
priya@priya-VirtualBox:~$ sudo cp 10.0.5.db /etc/bind
priya@priya-VirtualBox:~$ sudo cp example.com.db /etc/bind
priya@priya-VirtualBox:~$ cd /etc/bind
priya@priya-VirtualBox:/etc/bind$ ls
10.0.5.db db.127 db.local named.conf.default-zones rndc.key
bind.keys db.255 example.com.db named.conf.local zones.rfc1918
db.0 db.empty named.conf named.conf.options
priya@priya-VirtualBox:/etc/bind$

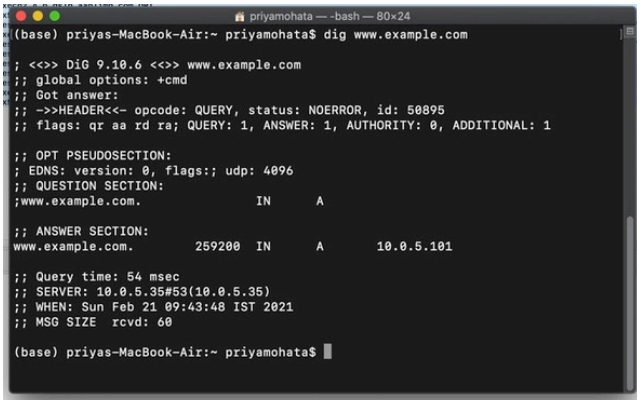

Example.com.db
priya@priya-VirtualBox: /etc/bind
priya@priya-VirtualBox:~$ sudo cp 10.0.5.db /etc/bind
priya@priya-VirtualBox:~$ sudo cp example.com.db /etc/bind
priya@priya-VirtualBox:~$ cd /etc/bind
priya@priya-VirtualBox:/etc/bind$ ls
10.0.5.db db.127 db.local named.conf.default-zones rndc.key
bind.keys db.255 example.com.db named.conf.local zones.rfc1918
db.0 db.empty named.conf named.conf.options
priya@priya-VirtualBox:/etc/bind$

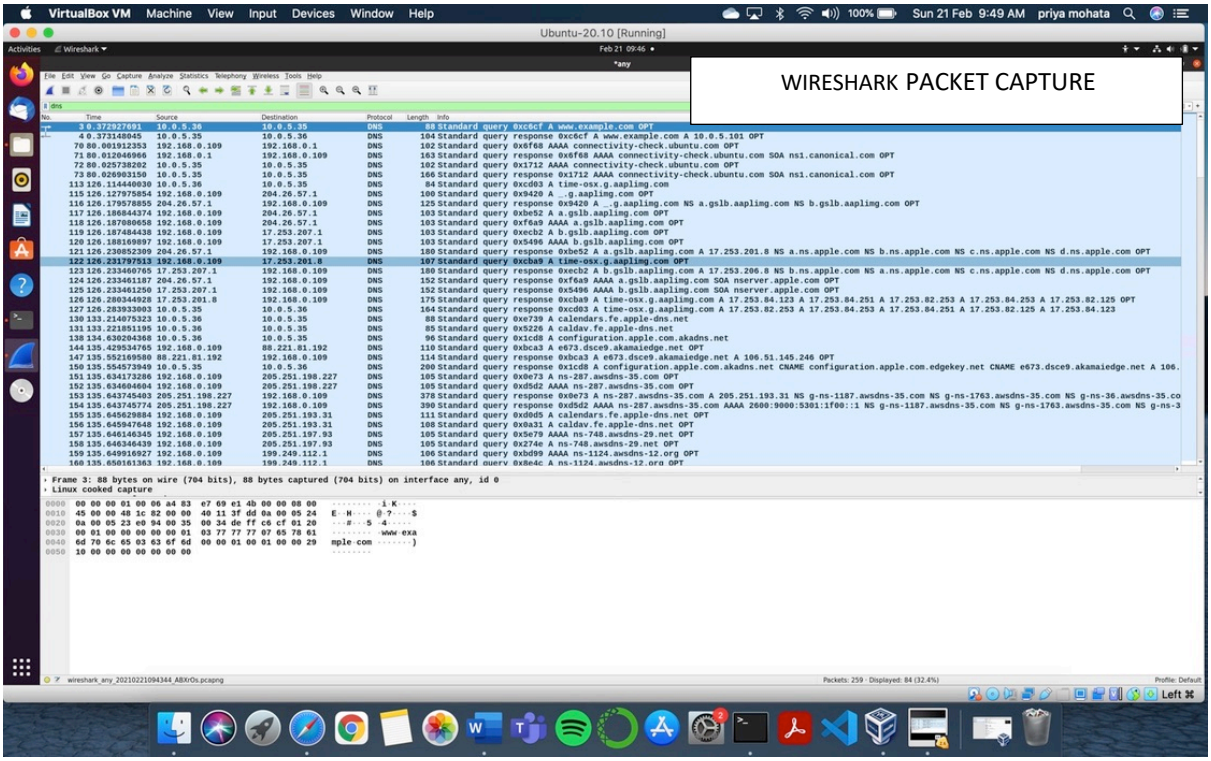
OBSERVATION 7 : Restart the BIND server and test

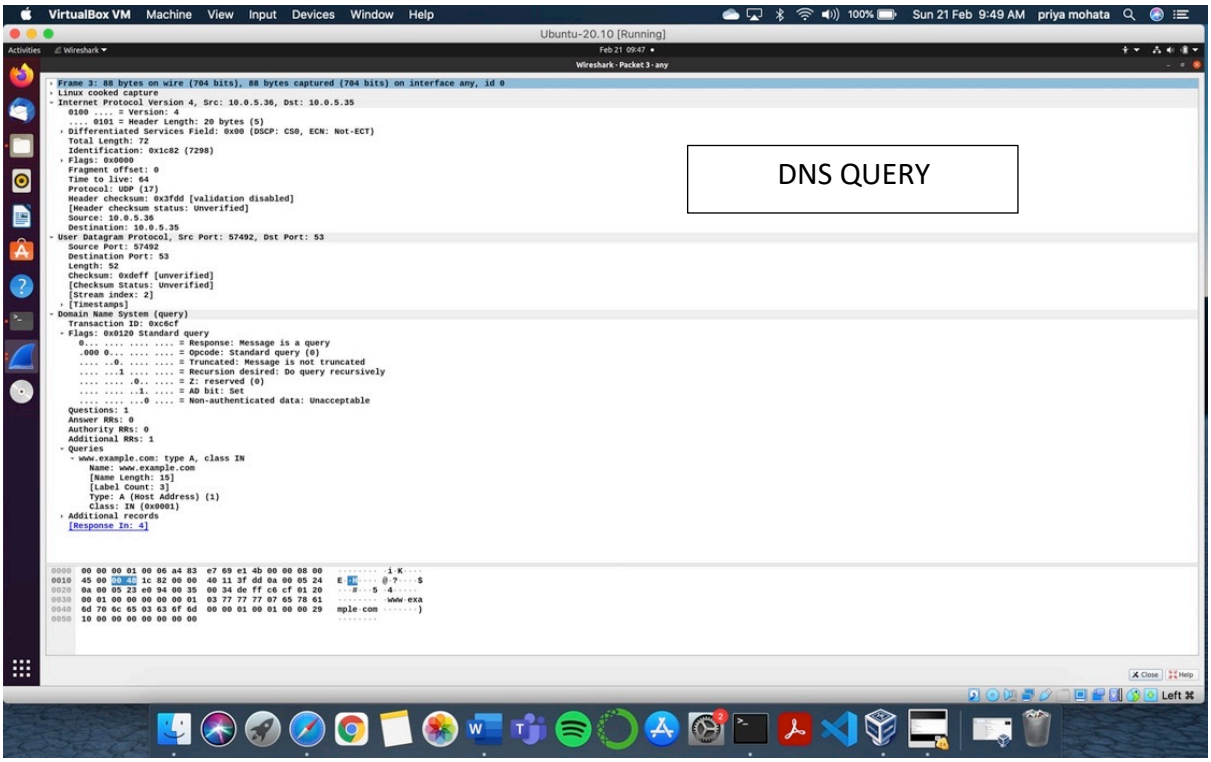
Step 1: When all the changes are made, remember to restart the BIND server. Now we will restart the DNS server using the following command:

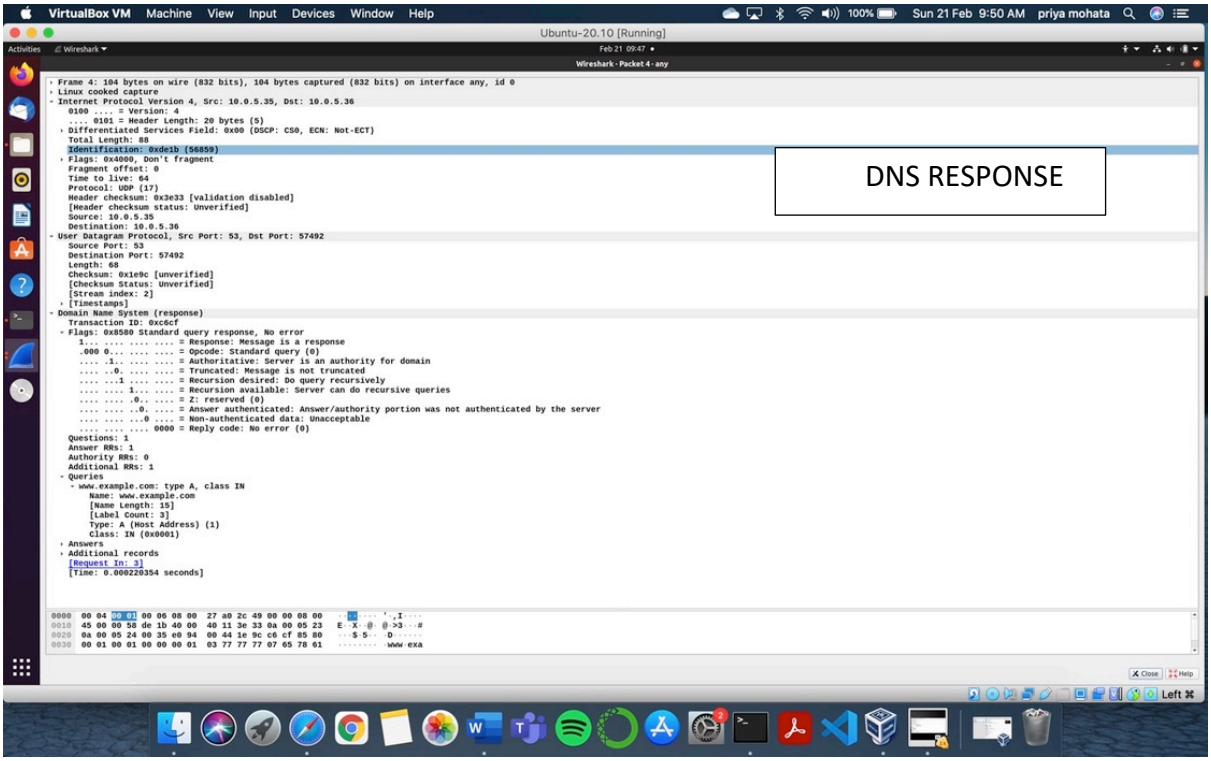
$ sudo service bind9 restart

Step 2: Now, go back to the client machine and ask the local DNS server for the IP address of www.example.com using the dig command.






VirtualBox VM Machine View Input Devices Window Help
Sun 21 Feb 9:49 AM priya mohata
Ubuntu-20.10 [Running]
Wireshark · Packet 3 · any
DNS QUERY


VirtualBox VM Machine View Input Devices Window Help
Sun 21 Feb 9:50 AM priya mohata
Ubuntu-20.10 [Running]
Wireshark · Packet 4 · any
DNS RESPONSE

QUESTIONS

Q1. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Answer : The DNS Query and Response messages are visible in the screenshots. They are sent over UDP(User Datagram Protocol).

Q2. What is the destination port for the DNS query message? What is the source port of DNS response message?

Answer : The destination and source ports of the DNS query and response messages are the same. The port number for DNS protocol is 53.

Q3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Answer : The DNS query is made to server at the IP Address 10.0.5.35. This is the same as the local DNS server configured.

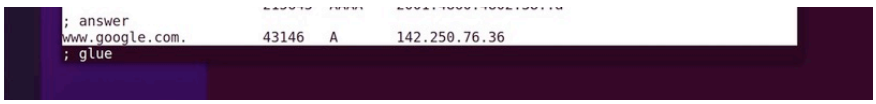
Q4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

Answer :The DNS Query is of type A since it requests for an authoritative record. The answer section is empty since it does not have any answer.

Q5. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

Answer :The answer section of the DNS response message contains one Resource Record.

A type RR: This provides the IP Address of the hostname



Q6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Answer : The destination IP Address of the SYN packet corresponds to the IP Address of hostname (www.google.com) retrieved from the response message.