Week #4
Implementation of a Local DNS Server and Authoritative NameServer

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.

The objectives of this lab are to understand:

- Install, set up and deploy a local DNS server
- Deploy authoritative nameserver for example.com domain

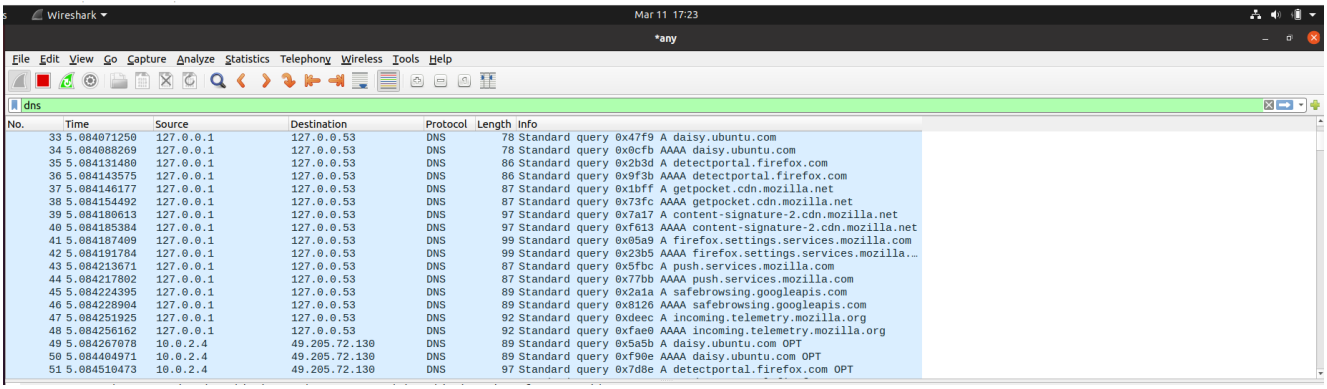
Lab Setup (with Internet Connection)

DNS Server: 10.2.22.184 User/Client: 10.2.22.195 ***Note:***

Use the default IP address provided by PESU LAN.

Observation 1:

Ping a computer such as www.google.com (any domain). Please use Wireshark to show the DNS query triggered by your ping command and DNS response. Describe your observation. (Take a screenshot).



Part 1: Setting Up a Local DNS Server

Task 1: Configure the User/Client Machine

On the client machine 10.2.22.195, we need to use 10.2.22.184 as the local DNS server. This is achieved by changing the resolver configuration file **(/etc/resolv.conf)** of the user machine, so the server 10.2.22.184 is added as the first nameserver entry in the file, i.e., this

server will be used as the primary DNS server. Add the following entry to the **/etc/resolvconf/resolv.conf.d/head** file.

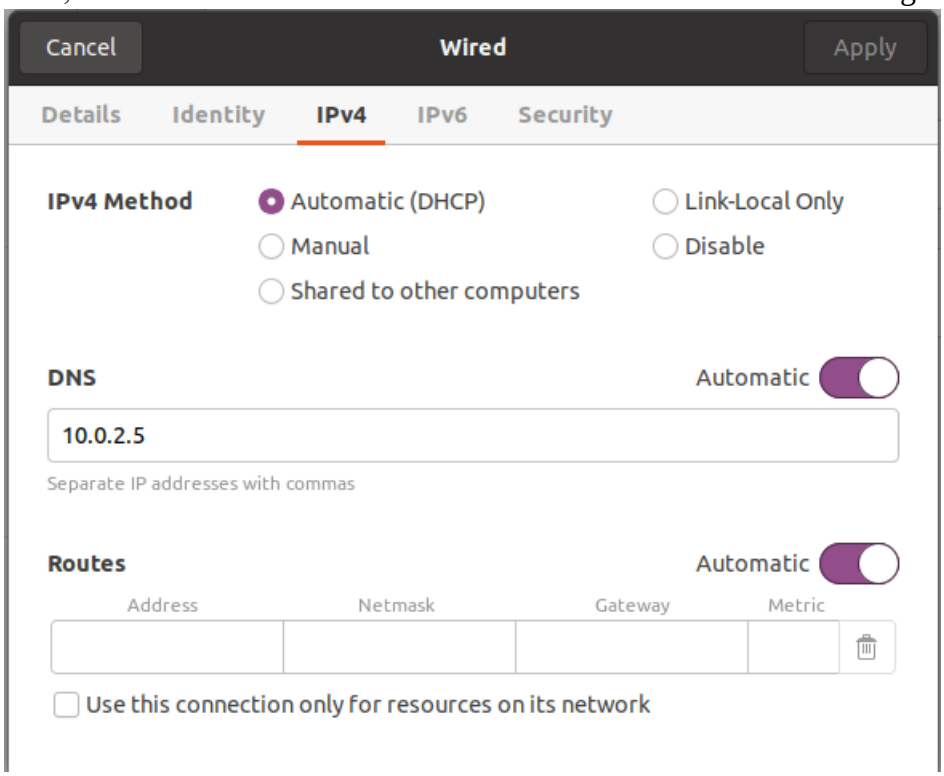
nameserver 10.2.22.184

Run the following command for the change to take effect.
sudo resolvconf -u

The following screenshot shows how to set DNS server on the client machine.

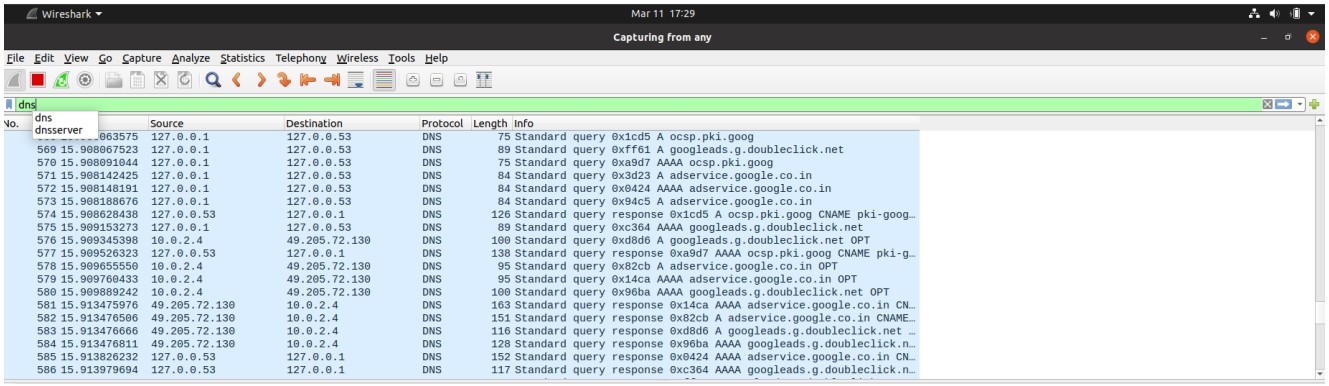
```
gaurav@gaurav-VirtualBox:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
[sudo] password for gaurav:
gaurav@gaurav-VirtualBox:~$ sudo resolvconf -u
gaurav@gaurav-VirtualBox:~$
```

Also, add 10.2.22.184 in 'Additional DNS servers' field in IPv4 settings of client machine.



Observation 2:

Ping a computer such as www.google.com. Please use Wireshark to show the DNS query triggered by your ping command and DNS response. Describe your observation. (Take a screenshot).



Task 2: Set Up a Local DNS Server

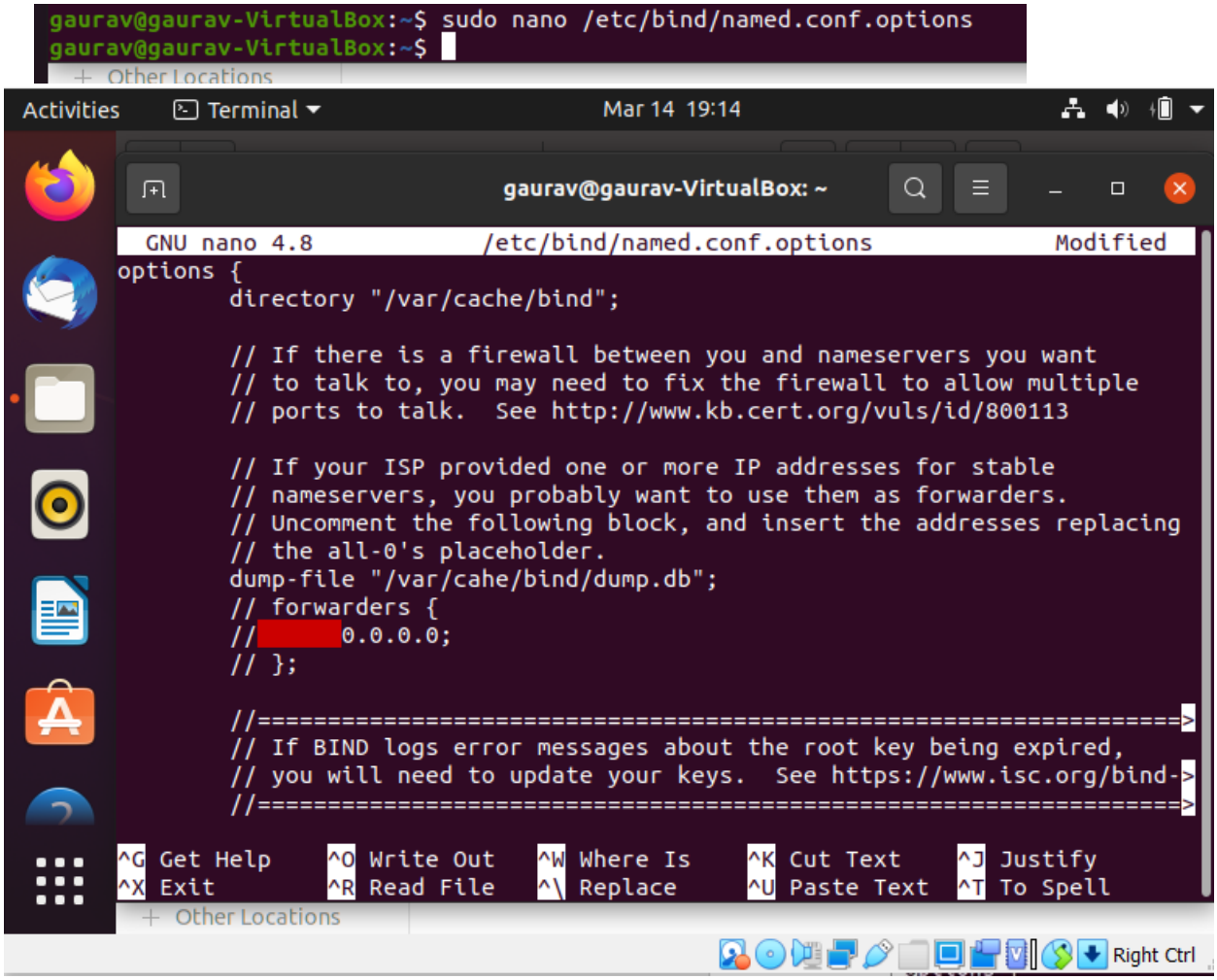
Note: If bind9 server is not already installed, install using the command

$ sudo apt-get update

$ sudo apt-get install bind9

Step 1: Configure the 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. Let us first set up an option related to DNS cache by adding a dump-file entry to the options block. The above option specifies where the cache content should be dumped to if BIND is asked to dump its cache.

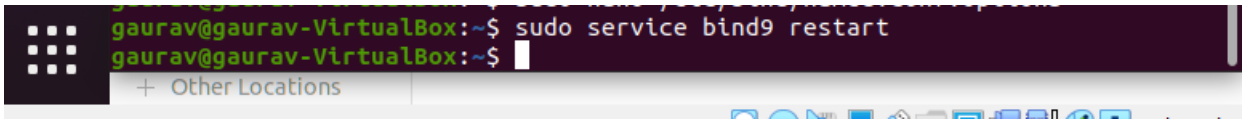


The above option specifies where the cache content should be dumped to if BIND is asked to dump its cache. If this option is not specified, BIND dumps the cache to a default file called **/var/cache/bind/named_dump.db**.

Step 2: Start DNS server

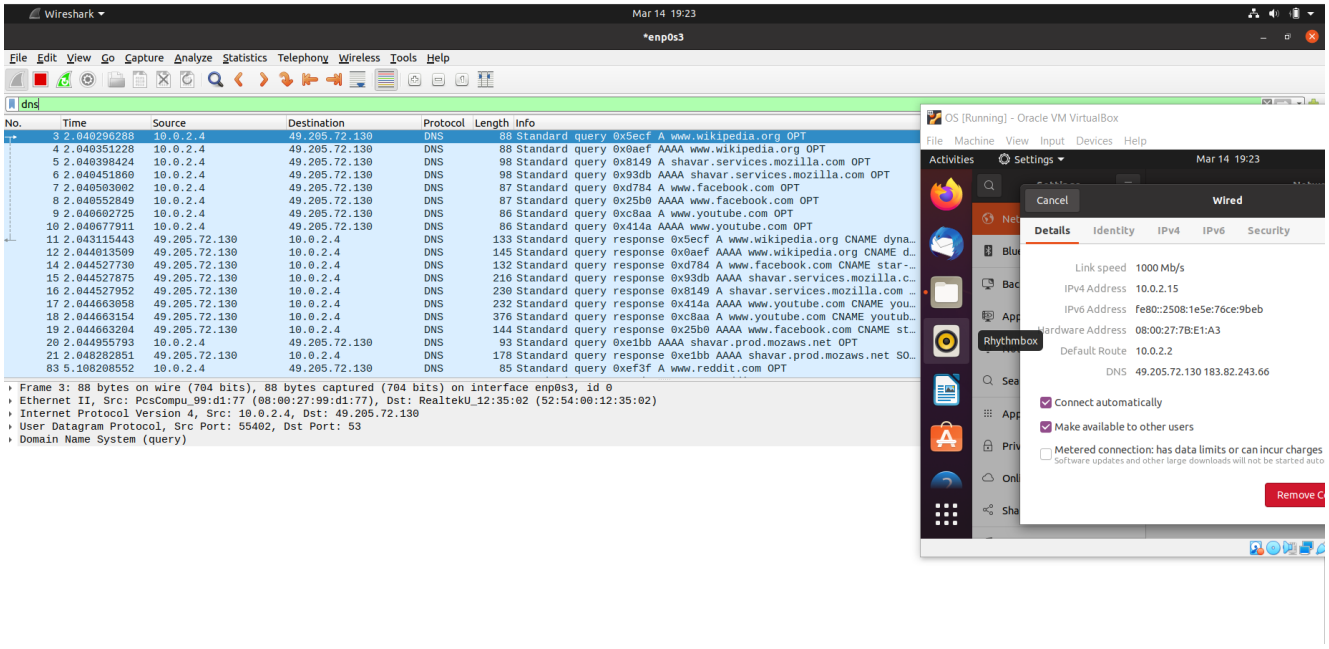
We start the DNS server using the command:

$ sudo service bind9 restart



Observation 3:

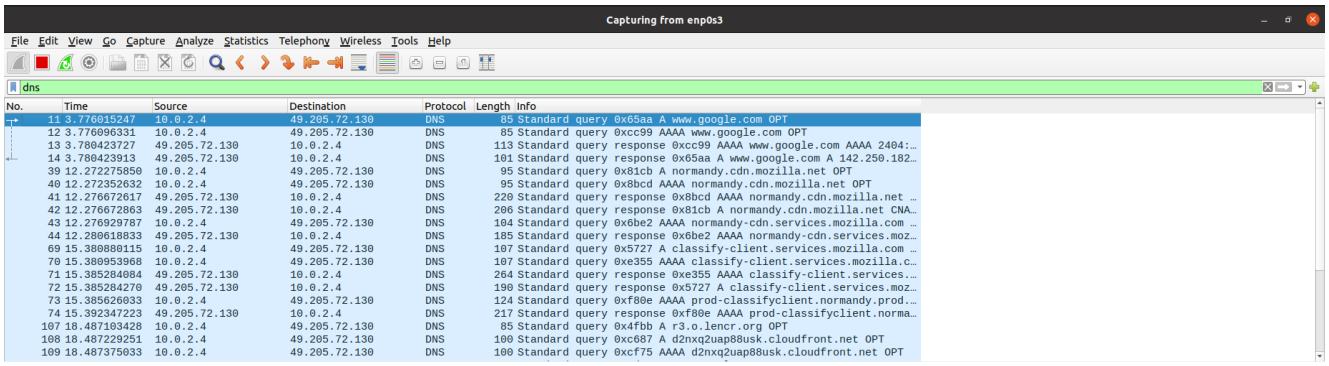
Now, go back to your user machine (10.2.22.195), and ping a computer such as www.google.com and describe your observation. Please use Wireshark to show the DNS query triggered by your ping command. Please also indicate when the DNS cache is used. (Take a screenshot).



Observation 4:

The two commands shown below are related to DNS cache. The first command dumps the content of the cache to the file specified above, and the second command clears the cache. You need extract the DNS cache using 'grep' command and take screenshot of www.google.com DNS cache.

```
gaurav@gaurav-VirtualBox:~$ sudo rndc dumpdb -cache
gaurav@gaurav-VirtualBox:~$ sudo rndc flush
gaurav@gaurav-VirtualBox:~$
```



Note: Compare the above three Wireshark DNS packet capture screenshots taken above.

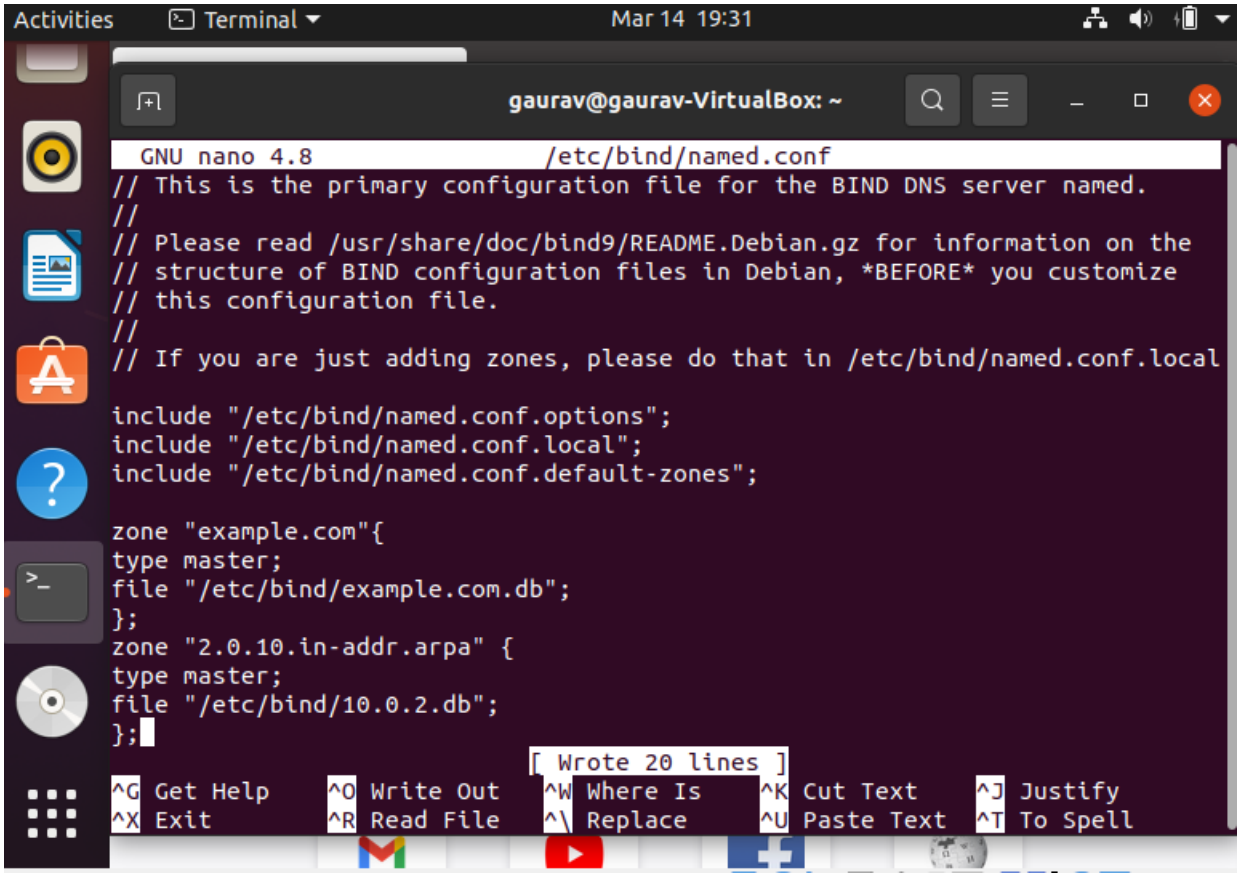
<u>Part 2: Setting Up an Authoritative Nameserver for example.com domain</u>

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

Assume that we own a domain, we will be responsible for providing the definitive answer regarding this domain. 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).



Note: In above screenshot, 10.2.22.0 is the subnet mask of your IP address. This applies to all part of the experiment.

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.

```
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
        2008111001
        8H
        2H
        4W
        1D)

@       IN      NS      ns.example.com.
@       IN      MX      10 mail.example.com.

www     IN      A       10.0.2.22
mail    IN      A       10.0.2.23
ns      IN      A       10.0.2.24
*.example.com.          IN      A       10.0.2.100
```

The symbol '@' is a special notation representing the origin specified in **named.conf** (the string after "**zone**"). Therefore, '@' here stands for **example.com**. This zone file contains 7 resource records (RRs), including a SOA (Start Of Authority) RR, a NS (Name Server) RR, a MX (Mail eXchanger) RR, and 4 A (host Address) RRs.

Step 3: Setup the reverse lookup zone file

We create a reverse DNS lookup file called **10.2.22.db** for the example.net domain to support DNS reverse lookup, i.e., from IP address to hostname in the **/etc/bind/** directory with the following contents.

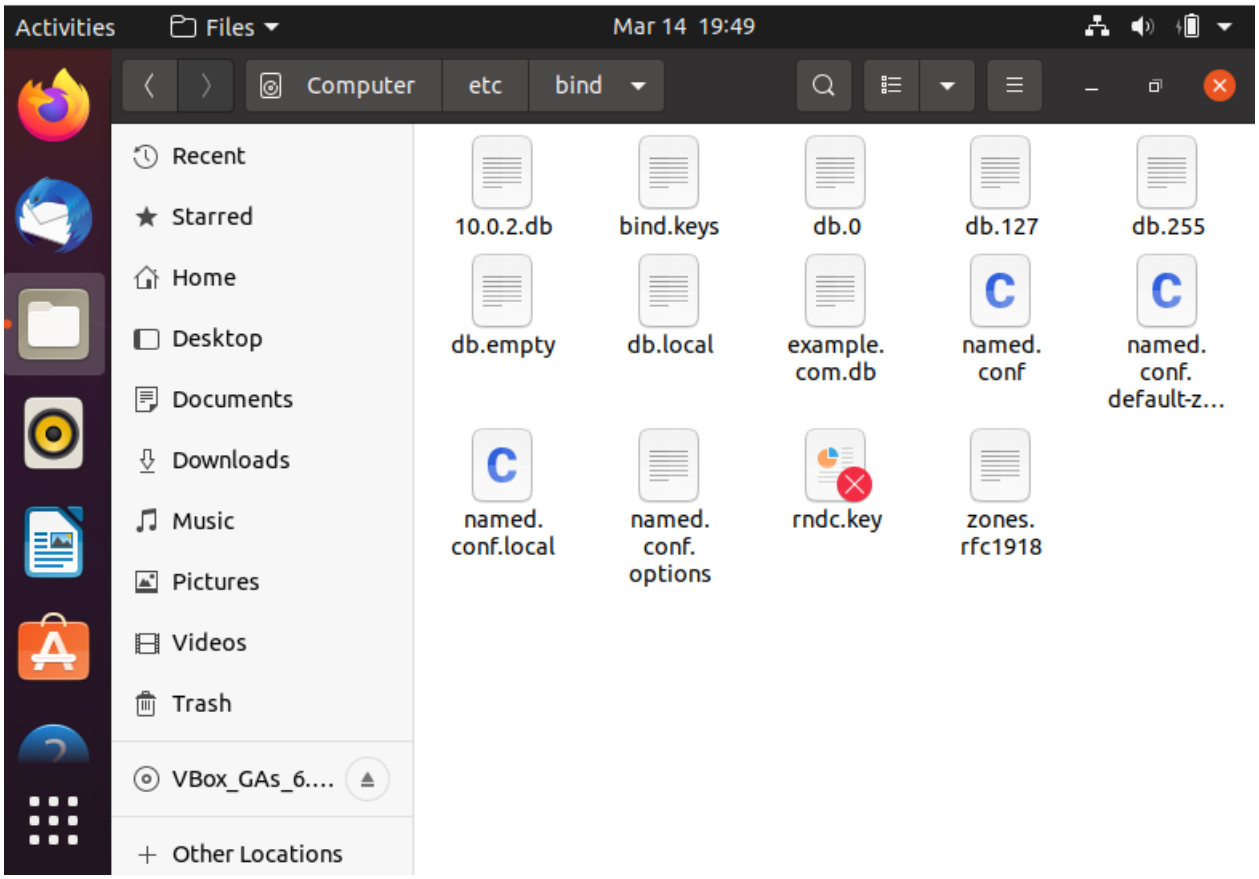
10.0.2.db × example.com.db ×

```
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
        2008111001
        8H
        2H
        4W
        1D)
@       IN      NS      ns.example.com.

101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
10      IN      PTR     ns.example.com.
```

Note: You can download the above two db files from Edmodo. Indent spacing is essential.

Step 4: Copy the above files into **/etc/bind** location.

```
gaurav@gaurav-VirtualBox:~$ sudo cp 10.0.2.db /etc/bind
[sudo] password for gaurav:
gaurav@gaurav-VirtualBox:~$ sudo cp example.com.db /etc/bind
Show Applications rtualBox:~$
```



Task 4: 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

```
isfcr@isfcr-H110M-H:~$ sudo service bind9 restart
isfcr@isfcr-H110M-H:~$
```

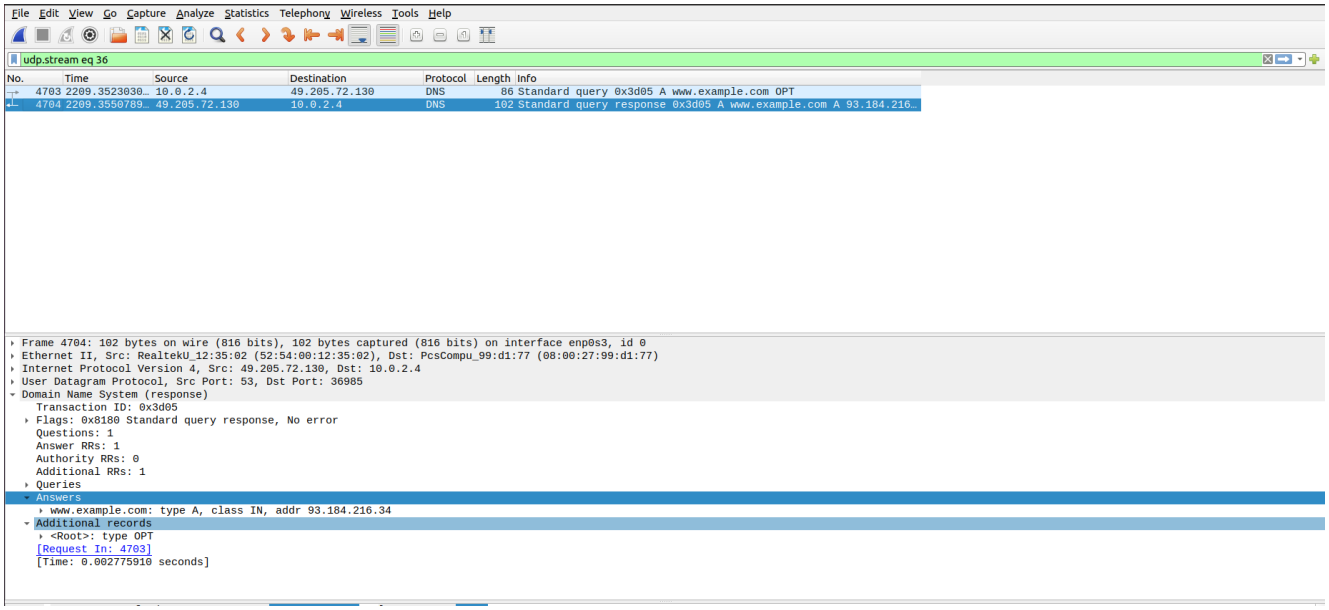
Step 2: Now, go back to the client machine and ask the local DNS server for the IP address of www.example.com using the dig command.

Dig stands for (Domain Information Groper) is a network administration command-line tool for querying DNS name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups and displays the answers that are returned from the name server that were queried. dig is part of the BIND domain name server software suite.

```
gaurav@gaurav-VirtualBox:~$ dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41790
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        356     IN      A       93.184.216.34

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Mar 14 20:36:31 IST 2022
;; MSG SIZE  rcvd: 60

gaurav@gaurav-VirtualBox:~$
```

We can see that the ANSWER SECTION contains the DNS mapping. We can see that the IP address of www.example.com is now 10.2.22.101, which is what we have setup in the DNS server.

Step 3: Observe the results in Wireshark capture.



To load and clear DNS cache, use the below commands.

```
gaurav@gaurav-VirtualBox:~$ sudo rndc dumpdb -cache
gaurav@gaurav-VirtualBox:~$ sudo rndc flush
gaurav@gaurav-VirtualBox:~$
```

named dump.db [Read-Only]
/var/cache/bind

```
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
$DATE 20220226133151
; secure
.                       1123046         IN NS   a.root-servers.net.
                        1123046         IN NS   b.root-servers.net.
                        1123046         IN NS   c.root-servers.net.
                        1123046         IN NS   d.root-servers.net.
                        1123046         IN NS   e.root-servers.net.
                        1123046         IN NS   f.root-servers.net.
                        1123046         IN NS   g.root-servers.net.
                        1123046         IN NS   h.root-servers.net.
                        1123046         IN NS   i.root-servers.net.
                        1123046         IN NS   j.root-servers.net.
                        1123046         IN NS   k.root-servers.net.
                        1123046         IN NS   l.root-servers.net.
                        1123046         IN NS   m.root-servers.net.
; secure
                        1123046         RRSIG   NS 8 0 518400 (
                                        20220318050000 20220305040000 9799 .
                                        J+F4rD6WQQWJCFvr+GPQ0GhU9sJkNgdGGEaV
                                        LRMrpufUlqnEJnfhRPhU4tEsJvq/GIcfZw1W
                                        Pv1rIQfem11aeptsQ/mHbn8h2n5pslm6fSvJ
                                        CzXsDHMOO9O4AzcIVrjDZQpcM92aWVUdxRy+
                                        XPzZPyK5Ge+MQXjRB/yV+3IaBdUIEjxmCw0a
                                        arGgvKJ9ufu1ABw29qDGmdMAoPuZk+gno3d4
                                        cQGsBPd6/50XElPA80OxIvufuqCDKJ3HxFLB
                                        VNOwnmMGvtTSU7L3ITEAWKjHK1PJHLTb/ckC
                                        yScTf0XQYiXGozpE+yfdt/tfNvwC/24MDBtR
                                        AI23MVrJAOnNBIJBHQ== )
; secure
                        777446  DNSKEY  256 3 8 (
```

Edmodo Requirements:

1) Wireshark packet capture screenshots (Observations 1-3)
2) DNS cache for www.google.com (Observation 4)
3) **dig www.example.com** command (in Terminal)
4) Wireshark packet capture – **dig www.example.com** command
5) DNS cache on server machine after dig command