COMPUTER NETWORKS LAB

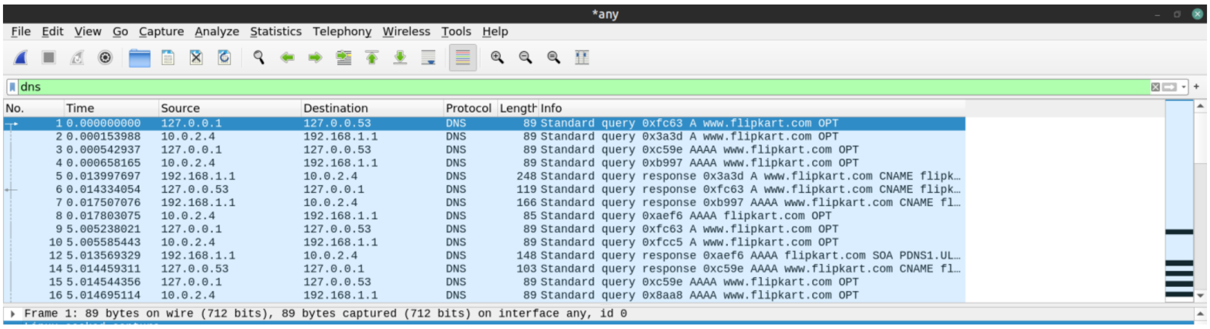
Implementation of a Local DNS Server and Authoritative Nameserver
WEEK 5

NAME: VISHWA MEHUL MEHTA
SRN: PES2UG20CS389
SECTION: F
DATE: 28/02/2022

Part 1: Setting Up a Local DNS Server

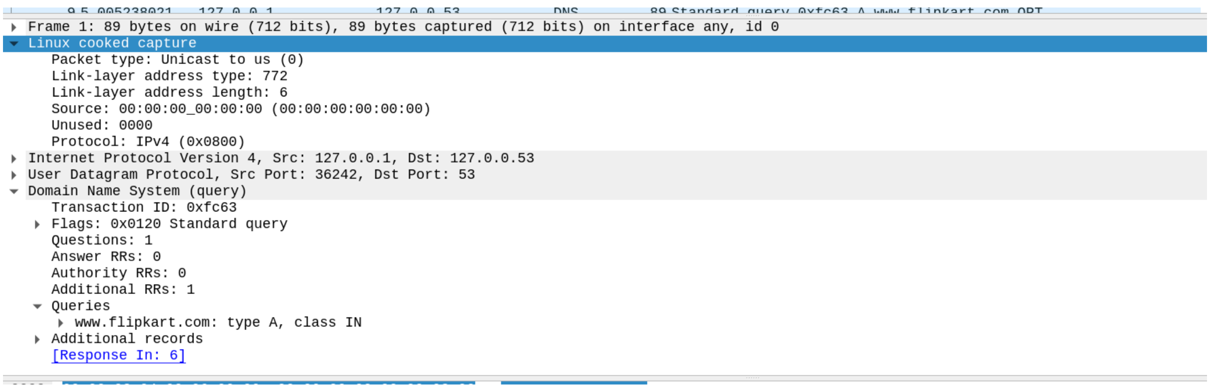
1. Observation 1 – Pinging default DNS:

- **www.flipkart.com** is pinged and the default DNS packets are observed using wireshark.
- Here the default DNS server IP address is **127.0.0.1** and the IP address of destination website is **163.53.78.110**.

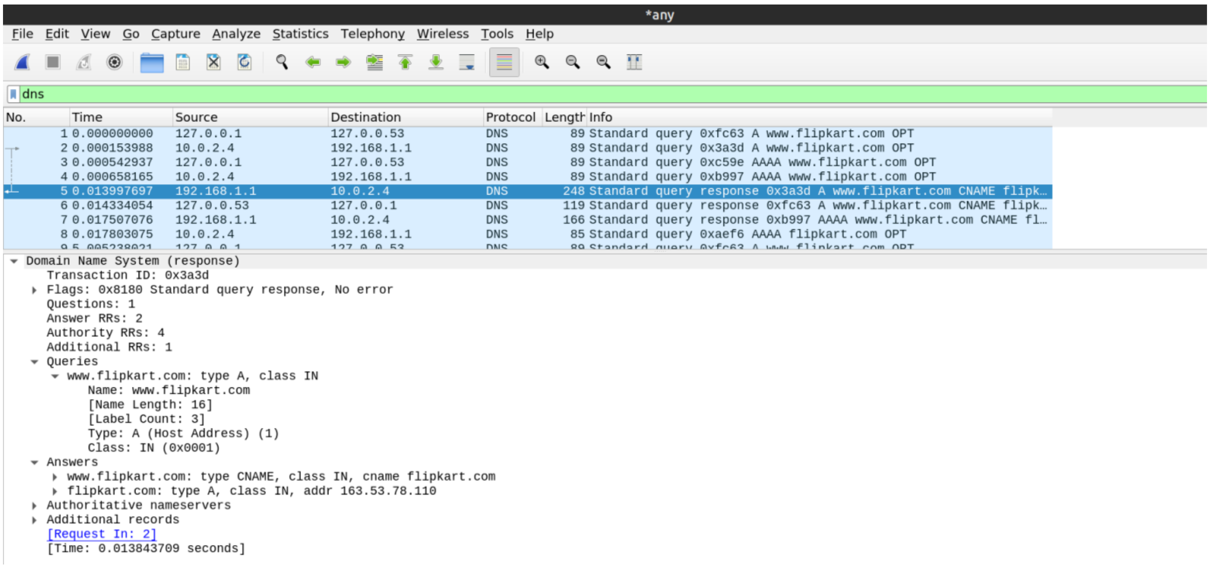


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns
No.  Time         Source        Destination   Protocol Length Info
  1 0.000000000   127.0.0.1     127.0.0.53    DNS       89 Standard query 0xfc63 A www.flipkart.com OPT
  2 0.000153988   10.0.2.4      192.168.1.1   DNS       89 Standard query 0x3a3d A www.flipkart.com OPT
  3 0.000542937   127.0.0.1     127.0.0.53    DNS       89 Standard query 0xc59e AAAA www.flipkart.com OPT
  4 0.000658165   10.0.2.4      192.168.1.1   DNS       89 Standard query 0xb997 AAAA www.flipkart.com OPT
  5 0.013997697   192.168.1.1   10.0.2.4      DNS      248 Standard query response 0x3a3d A www.flipkart.com CNAME flipk…
  6 0.014334054   127.0.0.53    127.0.0.1     DNS      119 Standard query response 0xfc63 A www.flipkart.com CNAME flipk…
  7 0.017507076   192.168.1.1   10.0.2.4      DNS      166 Standard query response 0xb997 AAAA www.flipkart.com CNAME fl…
  8 0.017803075   10.0.2.4      192.168.1.1   DNS       85 Standard query 0xaef6 AAAA flipkart.com OPT
  9 5.005238021   127.0.0.1     127.0.0.53    DNS       89 Standard query 0xfc63 A www.flipkart.com OPT
 10 5.005585443   10.0.2.4      192.168.1.1   DNS       89 Standard query 0xfcc5 A www.flipkart.com OPT
 12 5.013569329   192.168.1.1   10.0.2.4      DNS      148 Standard query response 0xaef6 AAAA flipkart.com SOA PDNS1.UL…
 14 5.014459311   127.0.0.53    127.0.0.1     DNS      103 Standard query response 0xc59e AAAA www.flipkart.com CNAME fl…
 15 5.014544356   127.0.0.1     127.0.0.53    DNS       89 Standard query 0xc59e AAAA www.flipkart.com OPT
 16 5.014695114   10.0.2.4      192.168.1.1   DNS       89 Standard query 0x8aa8 AAAA www.flipkart.com OPT
▸ Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
```



```
  9 5.005238021   127.0.0.1     127.0.0.53    DNS       89 Standard query 0xfc63 A www.flipkart.com OPT
▸ Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
▾ Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 772
    Link-layer address length: 6
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
▸ User Datagram Protocol, Src Port: 36242, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xfc63
  ▸ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ www.flipkart.com: type A, class IN
  ▸ Additional records
    [Response In: 6]
```

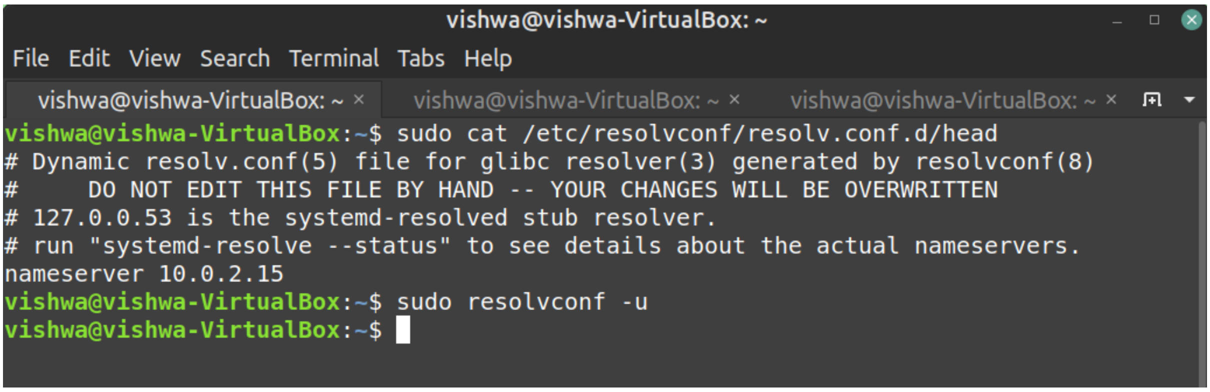

*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time         Source        Destination   Protocol Length Info
    1 0.000000000  127.0.0.1     127.0.0.53    DNS        89 Standard query 0xfc63 A www.flipkart.com OPT
    2 0.000153988  10.0.2.4      192.168.1.1   DNS        89 Standard query 0x3a3d A www.flipkart.com OPT
    3 0.000542937  127.0.0.1     127.0.0.53    DNS        89 Standard query 0xc59e AAAA www.flipkart.com OPT
    4 0.000658165  10.0.2.4      192.168.1.1   DNS        89 Standard query 0xb997 AAAA www.flipkart.com OPT
    5 0.013997697  192.168.1.1   10.0.2.4      DNS       248 Standard query response 0x3a3d A www.flipkart.com CNAME flipk…
    6 0.014334054  127.0.0.53    127.0.0.1     DNS       119 Standard query response 0xfc63 A www.flipkart.com CNAME flipk…
    7 0.017507076  192.168.1.1   10.0.2.4      DNS       166 Standard query response 0xb997 AAAA www.flipkart.com CNAME fl…
    8 0.017803075  10.0.2.4      192.168.1.1   DNS        85 Standard query 0xaef6 AAAA flipkart.com OPT
    9 5.005238021  127.0.0.1     127.0.0.53    DNS        89 Standard query 0xfc63 A www.flipkart.com OPT
```

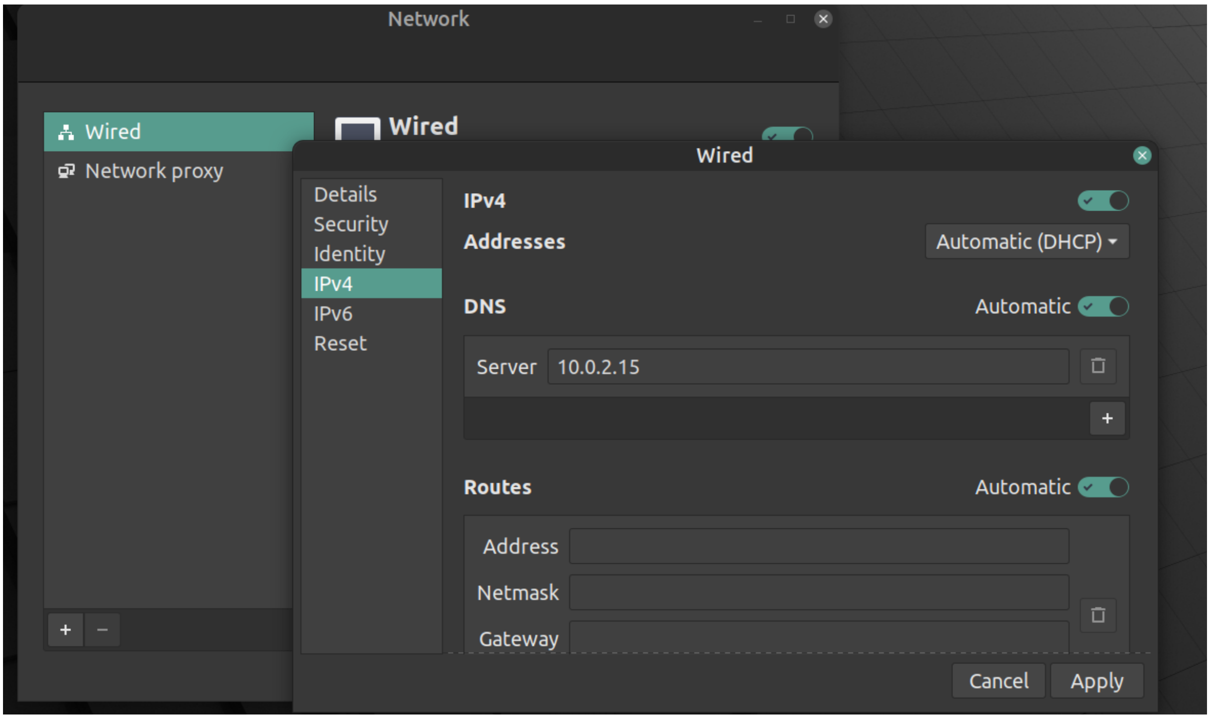
```
▾ Domain Name System (response)
    Transaction ID: 0x3a3d
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 4
    Additional RRs: 1
  ▾ Queries
    ▾ www.flipkart.com: type A, class IN
        Name: www.flipkart.com
        [Name Length: 16]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Answers
    ▸ www.flipkart.com: type CNAME, class IN, cname flipkart.com
    ▸ flipkart.com: type A, class IN, addr 163.53.78.110
  ▸ Authoritative nameservers
  ▸ Additional records
    [Request In: 2]
    [Time: 0.013843709 seconds]
```

2. Task 1: Configure the User/Client Machine

- IP address of the client machine is **10.0.2.4** and the server machine is **10.0.2.15.**
- We need to add the IP address of the custom DNS to the client.
- 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. The custom DNS server will now be used to resolve names.
- The IP Address of the custom DNS server is also added to the DNS menu under the IPv4 Network Settings.
- The changes are applied by using the command **sudo resolvconf –u**


vishwa@vishwa-VirtualBox: ~
File Edit View Search Terminal Tabs Help
vishwa@vishwa-VirtualBox: ~
vishwa@vishwa-VirtualBox: ~
vishwa@vishwa-VirtualBox: ~

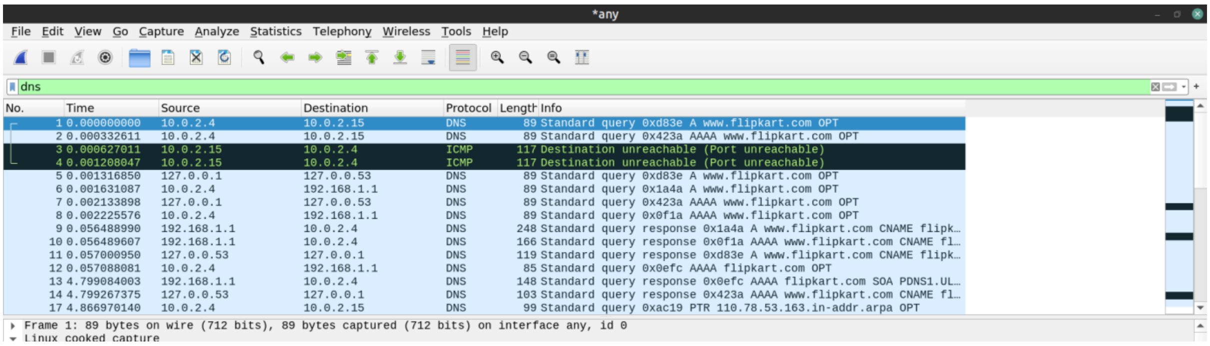
```
vishwa@vishwa-VirtualBox:~$ sudo cat /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 10.0.2.15
vishwa@vishwa-VirtualBox:~$ sudo resolvconf -u
vishwa@vishwa-VirtualBox:~$ 
```



IPv4
Addresses: Automatic (DHCP)
DNS: Automatic
Server: 10.0.2.15
Routes: Automatic
Address
Netmask
Gateway

3. Observation 2: Pinging custom DNS

- www.flipkart.com is pinged again.
- 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 **10.0.2.15** but it does not receive any hence it resorts to using the default DNS server at **127.0.0.53**.


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.4	10.0.2.15	DNS	89	Standard query 0xd83e A www.flipkart.com OPT
2	0.000332611	10.0.2.4	10.0.2.15	DNS	89	Standard query 0x423a AAAA www.flipkart.com OPT
3	0.000627011	10.0.2.15	10.0.2.4	ICMP	117	Destination unreachable (Port unreachable)
4	0.001208047	10.0.2.15	10.0.2.4	ICMP	117	Destination unreachable (Port unreachable)
5	0.001316850	127.0.0.1	127.0.0.53	DNS	89	Standard query 0xd83e A www.flipkart.com OPT
6	0.001631087	10.0.2.4	192.168.1.1	DNS	89	Standard query 0x1a4a A www.flipkart.com OPT
7	0.002133898	127.0.0.1	127.0.0.53	DNS	89	Standard query 0x423a AAAA www.flipkart.com OPT
8	0.002225576	10.0.2.4	192.168.1.1	DNS	89	Standard query 0x0f1a AAAA www.flipkart.com OPT
9	0.056488990	192.168.1.1	10.0.2.4	DNS	248	Standard query response 0x1a4a A www.flipkart.com CNAME flipk…
10	0.056489607	192.168.1.1	10.0.2.4	DNS	166	Standard query response 0x0f1a AAAA www.flipkart.com CNAME fl…
11	0.057000950	127.0.0.53	127.0.0.1	DNS	119	Standard query response 0xd83e A www.flipkart.com CNAME flipk…
12	0.057088081	10.0.2.4	192.168.1.1	DNS	85	Standard query 0x0efc AAAA flipkart.com OPT
13	4.799084003	192.168.1.1	10.0.2.4	DNS	148	Standard query response 0x0efc AAAA flipkart.com SOA PDNS1.UL…
14	4.799267375	127.0.0.53	127.0.0.1	DNS	103	Standard query response 0x423a AAAA www.flipkart.com CNAME fl…
17	4.866970140	10.0.2.4	10.0.2.15	DNS	99	Standard query 0xac19 PTR 110.78.53.163.in-addr.arpa OPT

```
▸ Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
▾ Linux cooked capture
```

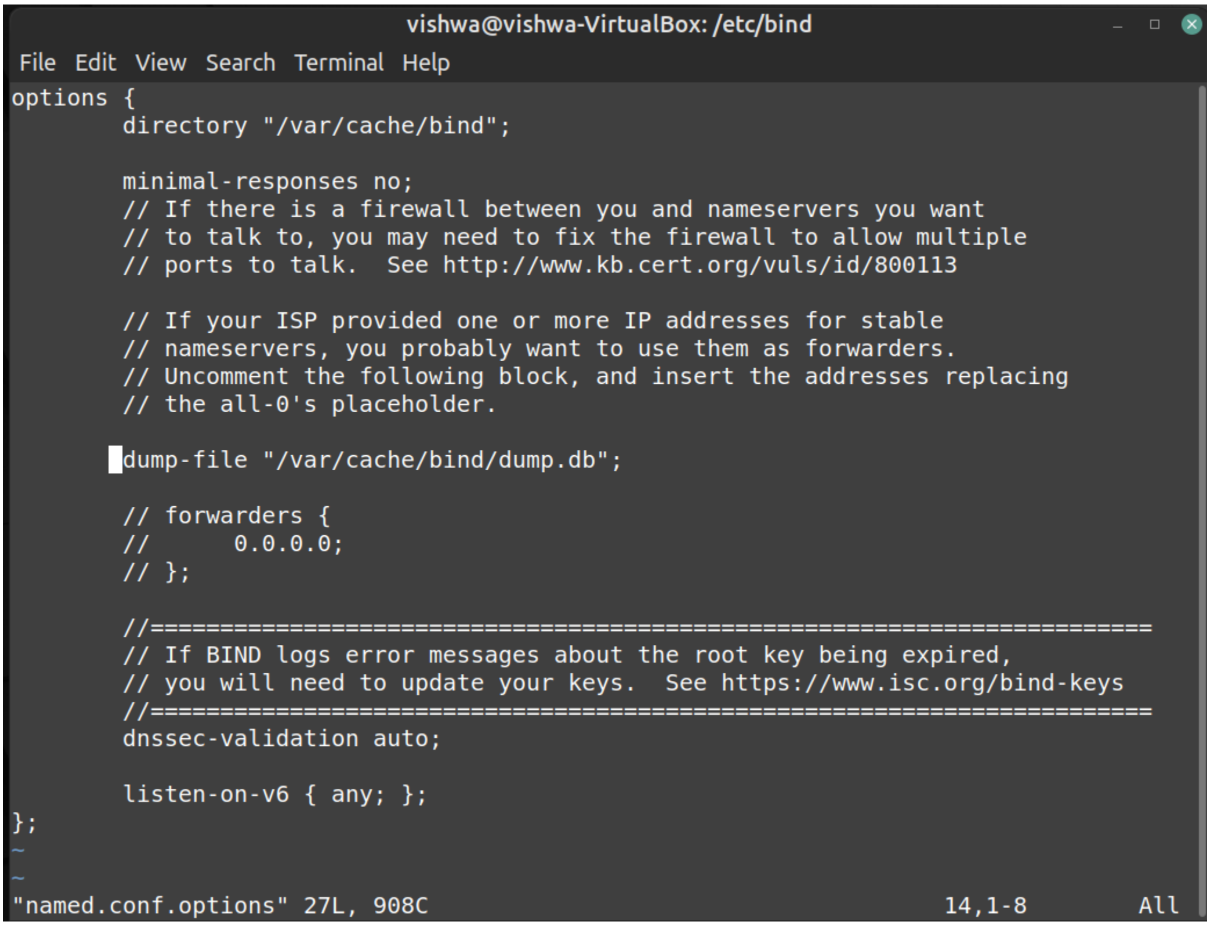
4. Task 2: Setting Up Local DNS Server

a. Set up **bind9 sever:**

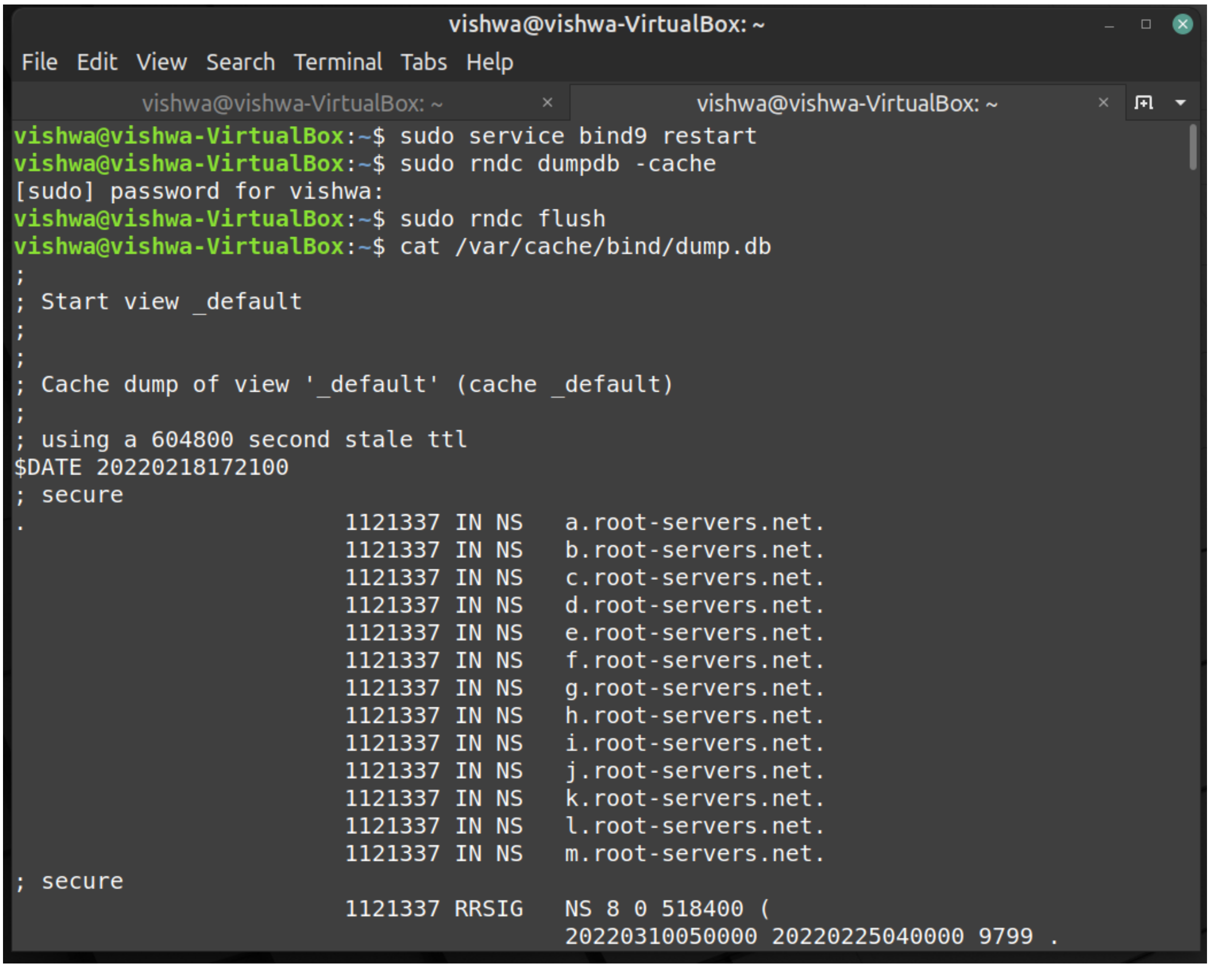
- The **bind9 server** is used as the DNS server on the server machine. It is installed using: **sudo apt install bind9**
- The configuration file for the server is **/etc/bind/named.conf.options.**
- The dump file for the DNS cache is added to the configuration file.
- The cache can be dumped into the file using **sudo rndc dumpdb -cache** and can be cleared or flushed out using **sudo rndc flush.**

b. Start the server:

- We start the DNS server using the command **sudo service bind9 restart.**


vishwa@vishwa-VirtualBox: /etc/bind
File Edit View Search Terminal Help

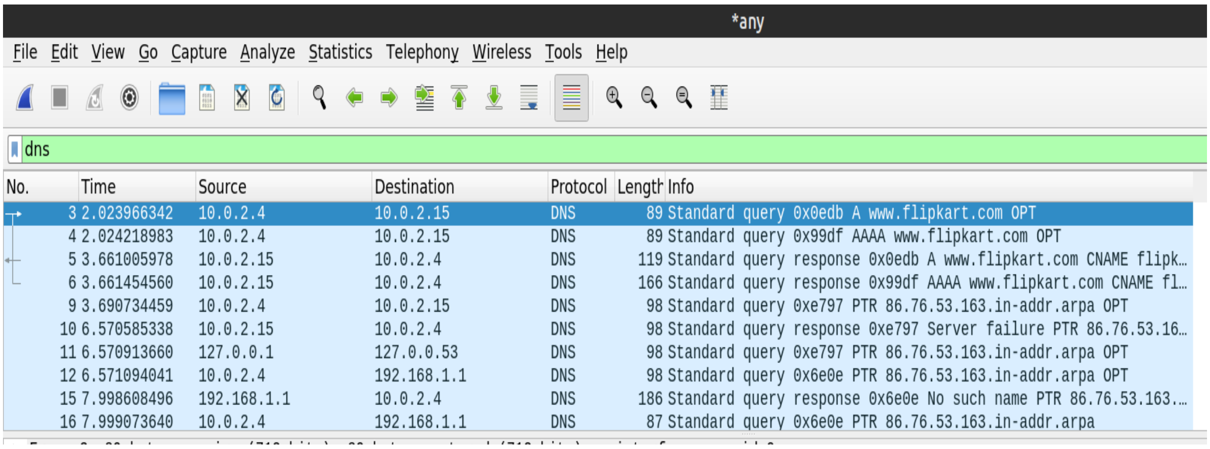
```
options {
        directory "/var/cache/bind";

        minimal-responses no;
        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        dump-file "/var/cache/bind/dump.db";

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
~
~
"named.conf.options" 27L, 908C                                    14,1-8        All
```


vishwa@vishwa-VirtualBox: ~
File Edit View Search Terminal Tabs Help
vishwa@vishwa-VirtualBox: ~
vishwa@vishwa-VirtualBox: ~

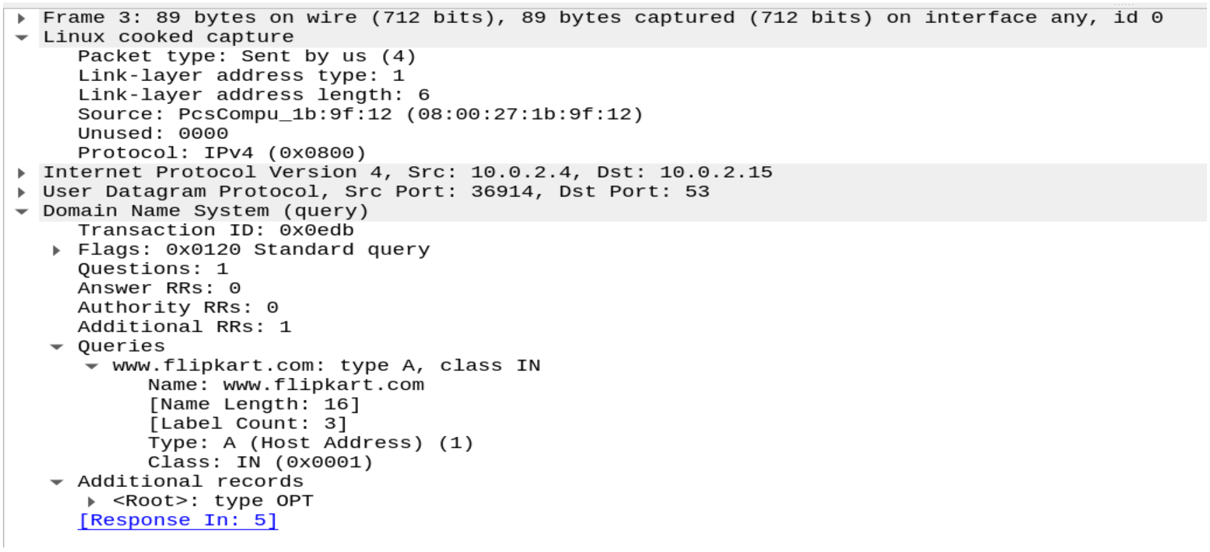
```
vishwa@vishwa-VirtualBox:~$ sudo service bind9 restart
vishwa@vishwa-VirtualBox:~$ sudo rndc dumpdb -cache
[sudo] password for vishwa:
vishwa@vishwa-VirtualBox:~$ sudo rndc flush
vishwa@vishwa-VirtualBox:~$ cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
$DATE 20220218172100
; secure
.                       1121337 IN NS   a.root-servers.net.
                        1121337 IN NS   b.root-servers.net.
                        1121337 IN NS   c.root-servers.net.
                        1121337 IN NS   d.root-servers.net.
                        1121337 IN NS   e.root-servers.net.
                        1121337 IN NS   f.root-servers.net.
                        1121337 IN NS   g.root-servers.net.
                        1121337 IN NS   h.root-servers.net.
                        1121337 IN NS   i.root-servers.net.
                        1121337 IN NS   j.root-servers.net.
                        1121337 IN NS   k.root-servers.net.
                        1121337 IN NS   l.root-servers.net.
                        1121337 IN NS   m.root-servers.net.
; secure
                        1121337 RRSIG   NS 8 0 518400 (
                                        20220310050000 20220225040000 9799 .
```

5. Observation 3-4: Pinging custom DNS(wireshark output and cache dump file contents)

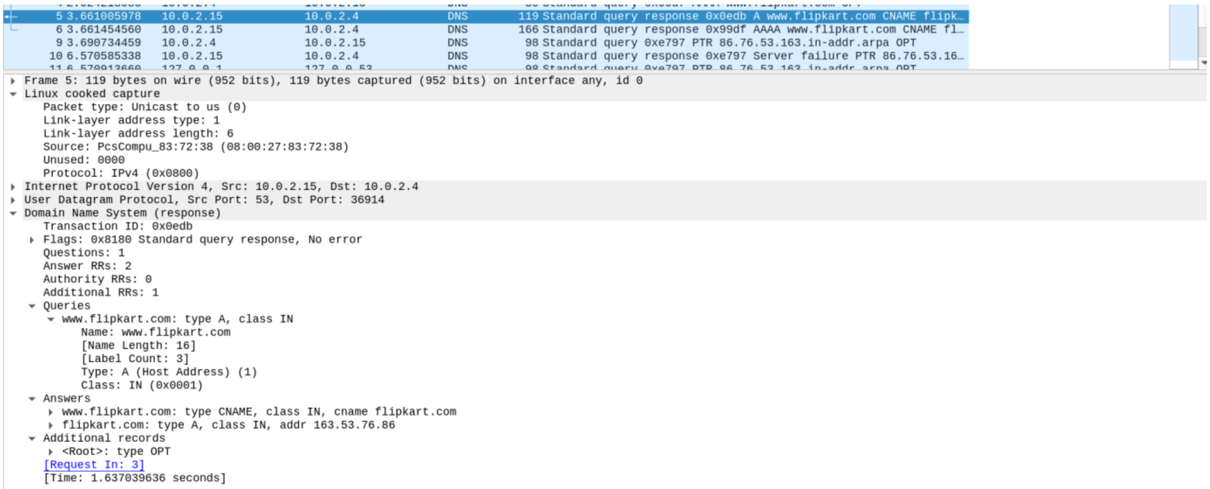
Client:


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

No.	Time	Source	Destination	Protocol	Length	Info
3	2.023966342	10.0.2.4	10.0.2.15	DNS	89	Standard query 0x0edb A www.flipkart.com OPT
4	2.024218983	10.0.2.4	10.0.2.15	DNS	89	Standard query 0x99df AAAA www.flipkart.com OPT
5	3.661005978	10.0.2.15	10.0.2.4	DNS	119	Standard query response 0x0edb A www.flipkart.com CNAME flipk…
6	3.661454560	10.0.2.15	10.0.2.4	DNS	166	Standard query response 0x99df AAAA www.flipkart.com CNAME fl…
9	3.690734459	10.0.2.4	10.0.2.15	DNS	98	Standard query 0xe797 PTR 86.76.53.163.in-addr.arpa OPT
10	6.570585338	10.0.2.15	10.0.2.4	DNS	98	Standard query response 0xe797 Server failure PTR 86.76.53.16…
11	6.570913660	127.0.0.1	127.0.0.53	DNS	98	Standard query 0xe797 PTR 86.76.53.163.in-addr.arpa OPT
12	6.571094041	10.0.2.4	192.168.1.1	DNS	98	Standard query 0x6e0e PTR 86.76.53.163.in-addr.arpa OPT
15	7.998608496	192.168.1.1	10.0.2.4	DNS	186	Standard query response 0x6e0e No such name PTR 86.76.53.163.…
16	7.999073640	10.0.2.4	192.168.1.1	DNS	87	Standard query 0x6e0e PTR 86.76.53.163.in-addr.arpa



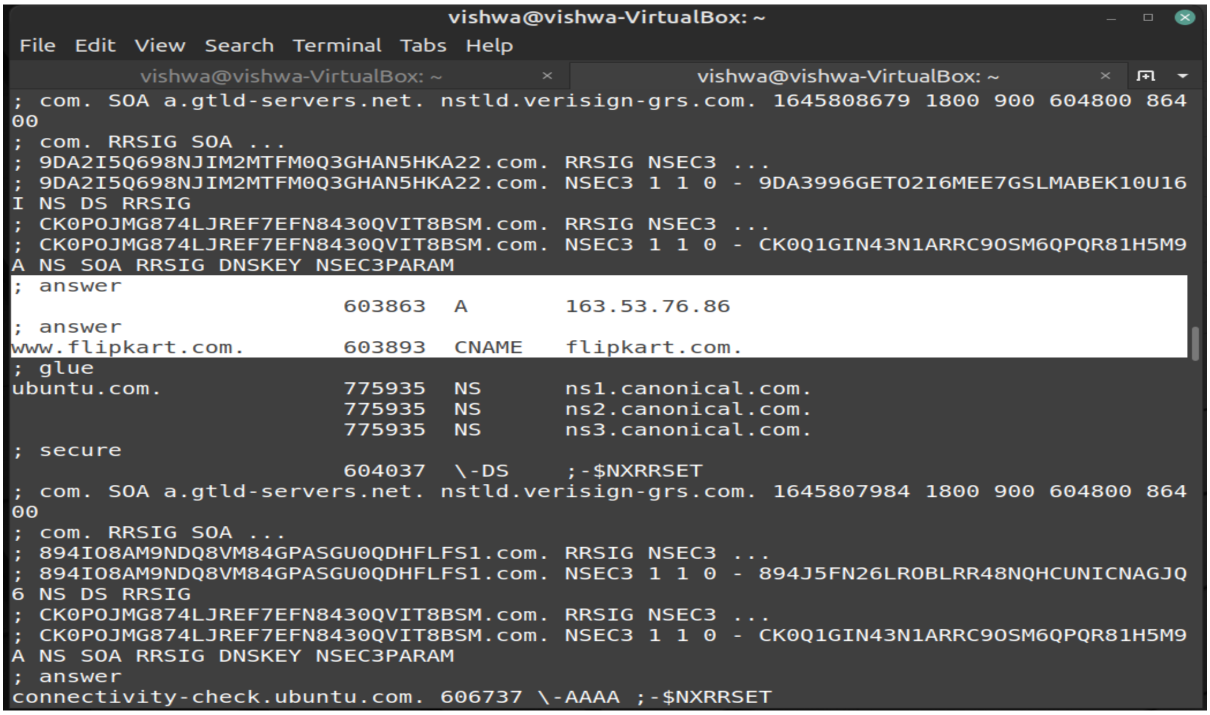
```
▸ Frame 3: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
▾ Linux cooked capture
     Packet type: Sent by us (4)
     Link-layer address type: 1
     Link-layer address length: 6
     Source: PcsCompu_1b:9f:12 (08:00:27:1b:9f:12)
     Unused: 0000
     Protocol: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 36914, Dst Port: 53
▾ Domain Name System (query)
     Transaction ID: 0x0edb
   ▸ Flags: 0x0120 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 1
   ▾ Queries
      ▾ www.flipkart.com: type A, class IN
           Name: www.flipkart.com
           [Name Length: 16]
           [Label Count: 3]
           Type: A (Host Address) (1)
           Class: IN (0x0001)
   ▾ Additional records
      ▸ <Root>: type OPT
     [Response In: 5]
```



```
  5 3.661005978   10.0.2.15   10.0.2.4    DNS   119 Standard query response 0x0edb A www.flipkart.com CNAME flipk…
  6 3.661454560   10.0.2.15   10.0.2.4    DNS   166 Standard query response 0x99df AAAA www.flipkart.com CNAME fl…
  9 3.690734459   10.0.2.4    10.0.2.15   DNS    98 Standard query 0xe797 PTR 86.76.53.163.in-addr.arpa OPT
 10 6.570585338   10.0.2.15   10.0.2.4    DNS    98 Standard query response 0xe797 Server failure PTR 86.76.53.16…
```

```
▸ Frame 5: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on interface any, id 0
▾ Linux cooked capture
     Packet type: Unicast to us (0)
     Link-layer address type: 1
     Link-layer address length: 6
     Source: PcsCompu_83:72:38 (08:00:27:83:72:38)
     Unused: 0000
     Protocol: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4
▸ User Datagram Protocol, Src Port: 53, Dst Port: 36914
▾ Domain Name System (response)
     Transaction ID: 0x0edb
   ▸ Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 2
     Authority RRs: 0
     Additional RRs: 1
   ▾ Queries
      ▾ www.flipkart.com: type A, class IN
           Name: www.flipkart.com
           [Name Length: 16]
           [Label Count: 3]
           Type: A (Host Address) (1)
           Class: IN (0x0001)
   ▾ Answers
      ▸ www.flipkart.com: type CNAME, class IN, cname flipkart.com
      ▸ flipkart.com: type A, class IN, addr 163.53.76.86
   ▾ Additional records
      ▸ <Root>: type OPT
     [Request In: 3]
     [Time: 1.637039636 seconds]
```

Server:



vishwa@vishwa-VirtualBox: ~
File Edit View Search Terminal Tabs Help
vishwa@vishwa-VirtualBox: ~
vishwa@vishwa-VirtualBox: ~

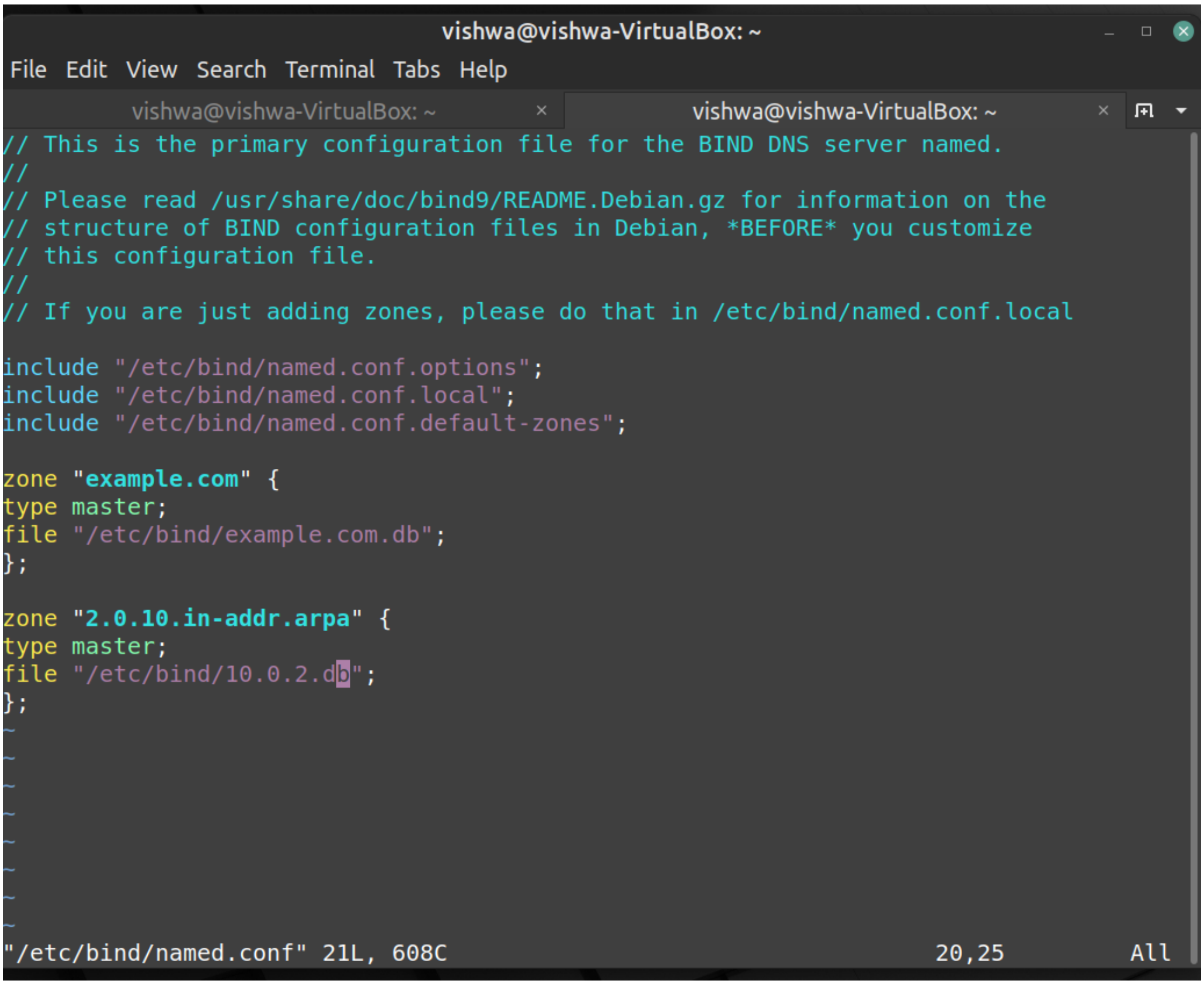
```
; com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1645808679 1800 900 604800 864
00
; com. RRSIG SOA ...
; 9DA2I5Q698NJIM2MTFM0Q3GHAN5HKA22.com. RRSIG NSEC3 ...
; 9DA2I5Q698NJIM2MTFM0Q3GHAN5HKA22.com. NSEC3 1 1 0 - 9DA3996GETO2I6MEE7GSLMABEK10U16
I NS DS RRSIG
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. RRSIG NSEC3 ...
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6QPQR81H5M9
A NS SOA RRSIG DNSKEY NSEC3PARAM
; answer
                                603863  A       163.53.76.86
; answer
www.flipkart.com.               603893  CNAME   flipkart.com.
; glue
ubuntu.com.                     775935  NS      ns1.canonical.com.
                                775935  NS      ns2.canonical.com.
                                775935  NS      ns3.canonical.com.
; secure
                                604037  \-DS    ;-$NXRRSET
; com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1645807984 1800 900 604800 864
00
; com. RRSIG SOA ...
; 894I08AM9NDQ8VM84GPASGU0QDHFLFS1.com. RRSIG NSEC3 ...
; 894I08AM9NDQ8VM84GPASGU0QDHFLFS1.com. NSEC3 1 1 0 - 894J5FN26LROBLRR48NQHCUNICNAGJQ
6 NS DS RRSIG
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. RRSIG NSEC3 ...
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6QPQR81H5M9
A NS SOA RRSIG DNSKEY NSEC3PARAM
; answer
connectivity-check.ubuntu.com. 606737 \-AAAA ;-$NXRRSET
```

Part 2: Setting Up an Authoritative Nameserver for example.com domain

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

a. 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).

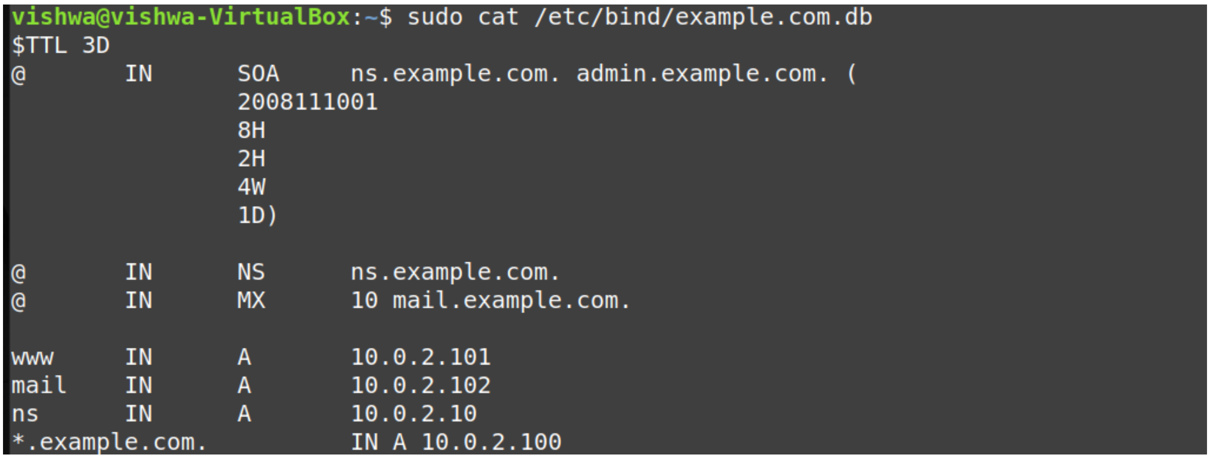

vishwa@vishwa-VirtualBox: ~
File Edit View Search Terminal Tabs Help
vishwa@vishwa-VirtualBox: ~
vishwa@vishwa-VirtualBox: ~

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "example.com" {
type master;
file "/etc/bind/example.com.db";
};

zone "2.0.10.in-addr.arpa" {
type master;
file "/etc/bind/10.0.2.db";
};
~
~
~
~
~
~
~
~
"/etc/bind/named.conf" 21L, 608C                                  20,25         All
```

b. 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.

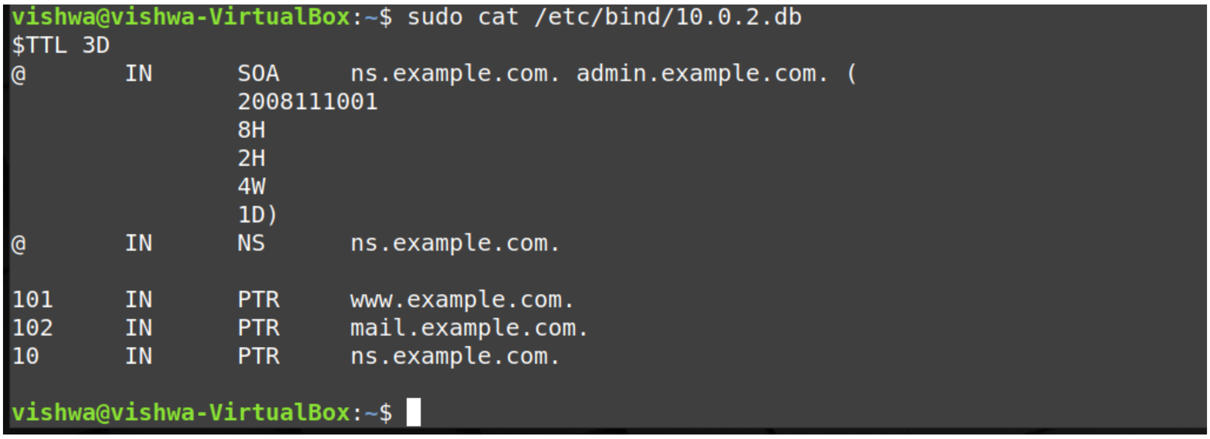
The symbol ‘@’ is a special notation representing the origin specified in named.conf (the string after "zone"). Therefore, ‘@’ here stands for example.com. This zone file contains 7 resource records (RRs), including a SOA (Start Of Authority) RR, a NS (Name Server) RR, a MX (Mail eXchanger) RR, and 4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



```
vishwa@vishwa-VirtualBox:~$ sudo cat /etc/bind/example.com.db
$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       10.0.2.101
mail    IN      A       10.0.2.102
ns      IN      A       10.0.2.10
*.example.com.          IN A 10.0.2.100
```

c. 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.

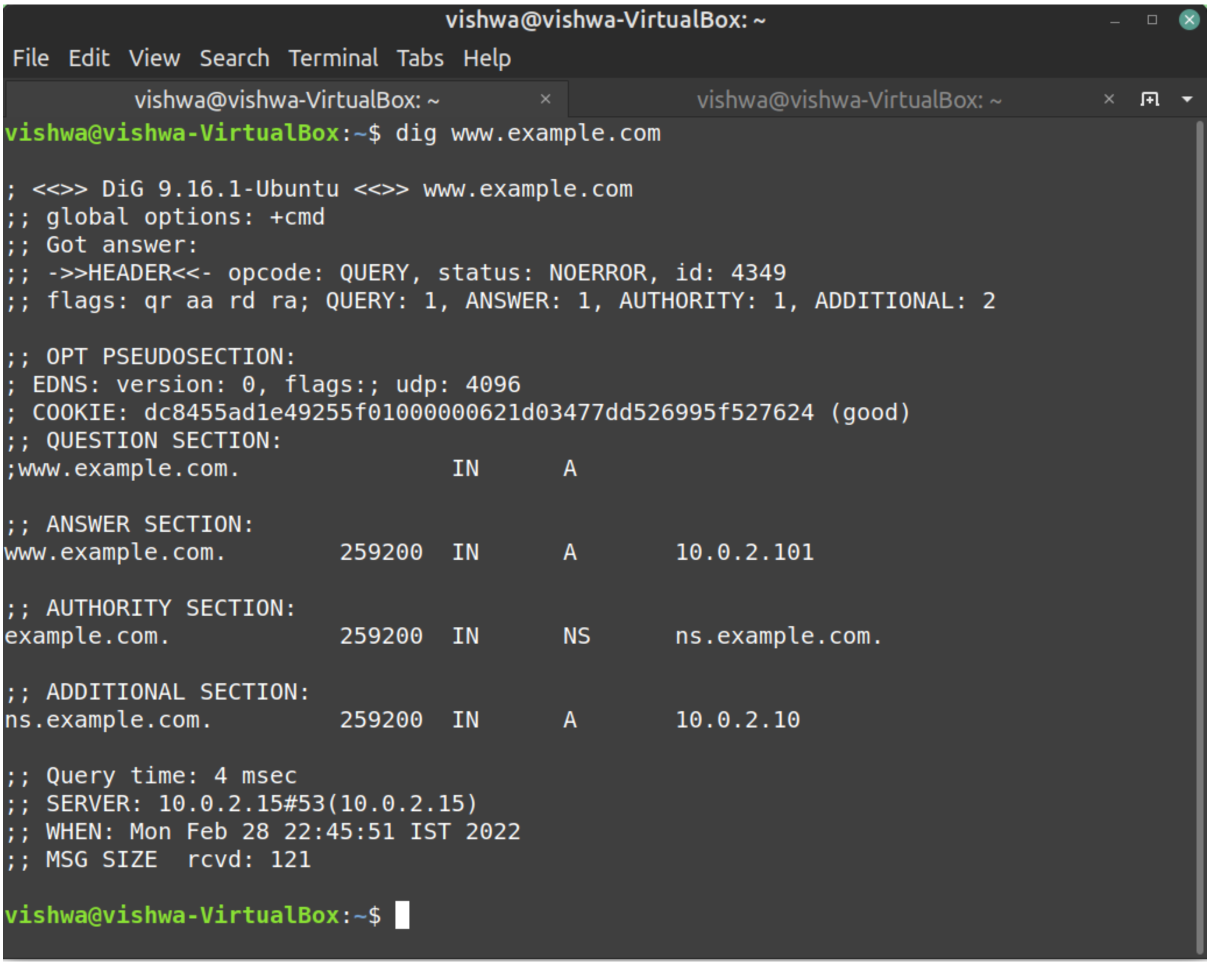


```
vishwa@vishwa-VirtualBox:~$ sudo cat /etc/bind/10.0.2.db
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                2008111001
                8H
                2H
                4W
                1D)
@       IN      NS      ns.example.com.

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

vishwa@vishwa-VirtualBox:~$ █
```

7. Observation 5: Testing www.example.com

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.**

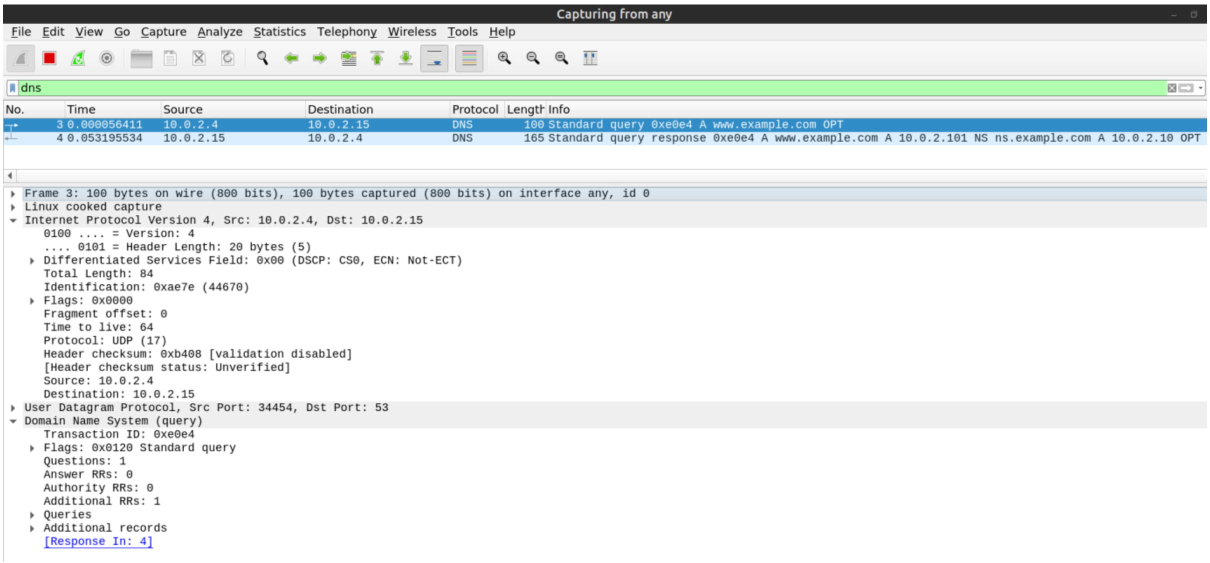
Now, go back to the client machine and ask the local DNS server for the IP address of www.example.com using the dig command. Dig stands for (**Domain Information Groper**) is a network administration command-line tool for querying DNS name servers. It is useful for verifying and troubleshooting DNS problems 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.



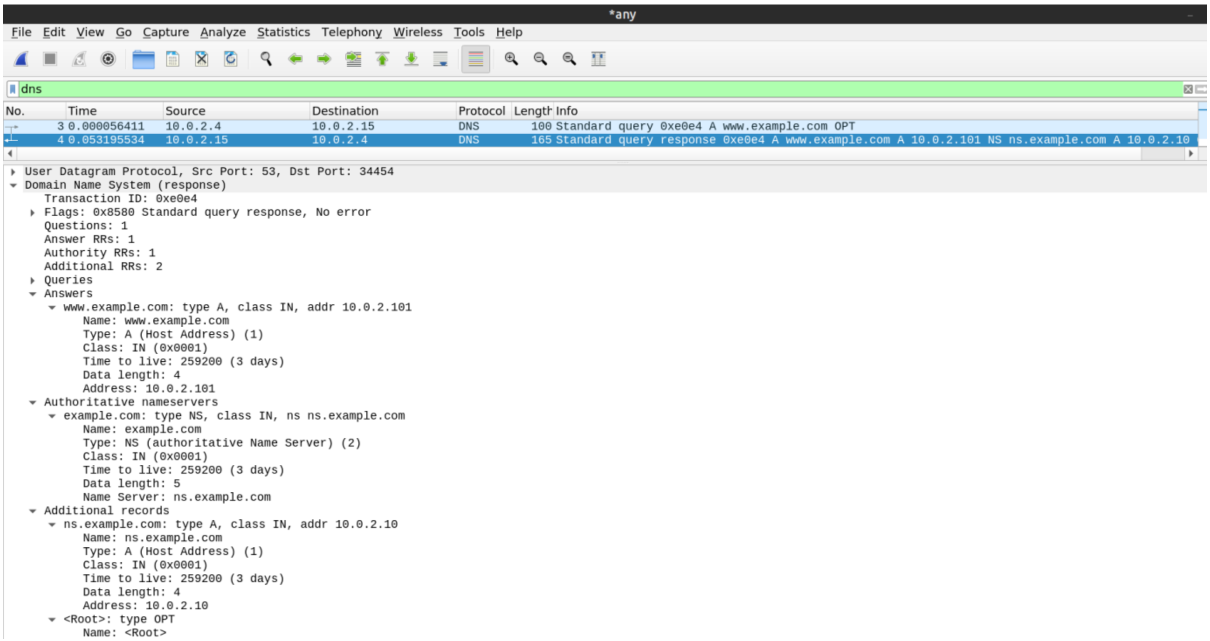
vishwa@vishwa-VirtualBox: ~
File Edit View Search Terminal Tabs Help
vishwa@vishwa-VirtualBox: ~
vishwa@vishwa-VirtualBox: ~

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

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4349
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: dc8455ad1e49255f01000000621d03477dd526995f527624 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.0.2.101

;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       10.0.2.10

;; Query time: 4 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Mon Feb 28 22:45:51 IST 2022
;; MSG SIZE  rcvd: 121

vishwa@vishwa-VirtualBox:~$ 
```

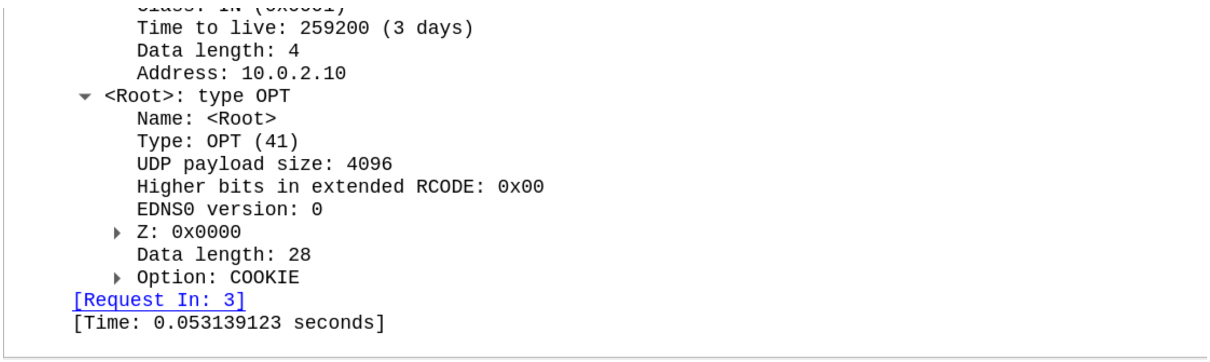
We can see that the ANSWER SECTION contains the DNS mapping. The IP Address of the DNS Server and the returned IP Address of the domain set by us can be seen in the query and response packets.


Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time          Source      Destination  Protocol Length Info
    3 0.000056411   10.0.2.4    10.0.2.15    DNS         100 Standard query 0xe0e4 A www.example.com OPT
    4 0.053195534   10.0.2.15   10.0.2.4     DNS         165 Standard query response 0xe0e4 A www.example.com A 10.0.2.101 NS ns.example.com A 10.0.2.10 OPT

Frame 3: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xae7e (44670)
  Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0xb408 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.4
    Destination: 10.0.2.15
User Datagram Protocol, Src Port: 34454, Dst Port: 53
Domain Name System (query)
    Transaction ID: 0xe0e4
  Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  Queries
  Additional records
    [Response In: 4]
```


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time          Source      Destination  Protocol Length Info
    3 0.000056411   10.0.2.4    10.0.2.15    DNS         100 Standard query 0xe0e4 A www.example.com OPT
    4 0.053195534   10.0.2.15   10.0.2.4     DNS         165 Standard query response 0xe0e4 A www.example.com A 10.0.2.101 NS ns.example.com A 10.0.2.10

User Datagram Protocol, Src Port: 53, Dst Port: 34454
Domain Name System (response)
    Transaction ID: 0xe0e4
  Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 2
  Queries
  Answers
      www.example.com: type A, class IN, addr 10.0.2.101
        Name: www.example.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 259200 (3 days)
        Data length: 4
        Address: 10.0.2.101
  Authoritative nameservers
      example.com: type NS, class IN, ns ns.example.com
        Name: example.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 259200 (3 days)
        Data length: 5
        Name Server: ns.example.com
  Additional records
      ns.example.com: type A, class IN, addr 10.0.2.10
        Name: ns.example.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 259200 (3 days)
        Data length: 4
        Address: 10.0.2.10
      <Root>: type OPT
        Name: <Root>
```



```
        Class: IN (0x0001)
        Time to live: 259200 (3 days)
        Data length: 4
        Address: 10.0.2.10
      <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      Z: 0x0000
        Data length: 28
      Option: COOKIE
    [Request In: 3]
    [Time: 0.053139123 seconds]
```

Observations:

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

The messages are sent over UDP.

2) What is the destination port for the DNS query message? What is the source port of DNS response message?

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

3) 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?

The DNS query is made to server at the IP Address 10.0.2.15. This is the same as the local DNS server configured.

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

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.

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

The answer section of the DNS response message contains two Resource Records.

- CNAME RR: This determines that the hostname flipkart.com refers to the canonical hostname www.flipkart.com.

- A type RR: This provides the IP Address of the canonical hostname.

6) 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?

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