COMPUTER NETWORKS LAB

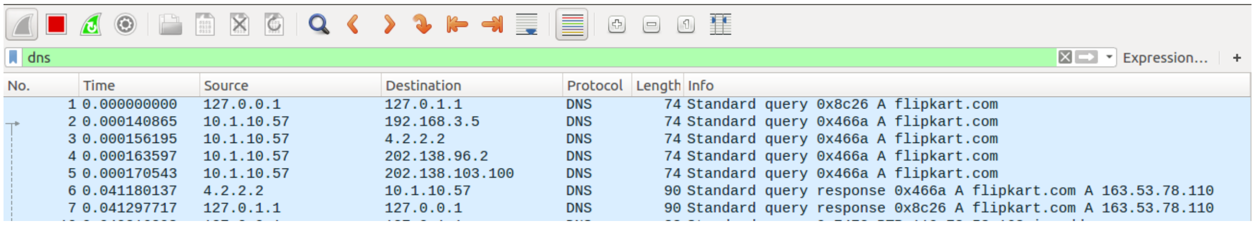
Week 4

Vishal R
PES1UG19CS571
SECTION I

First Test - Pinging using default DNS

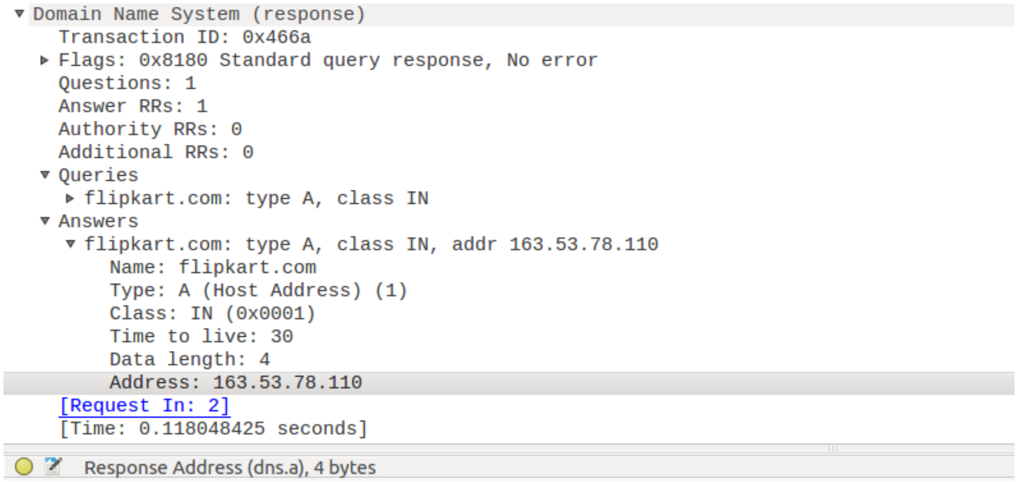
`Wireshark` is used to capture the packets in the background while pinging `www.flipkart.com`.

The IP Address of the Local DNS server is observed to be `127.0.1.1.` 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 – `163.53.78.110`

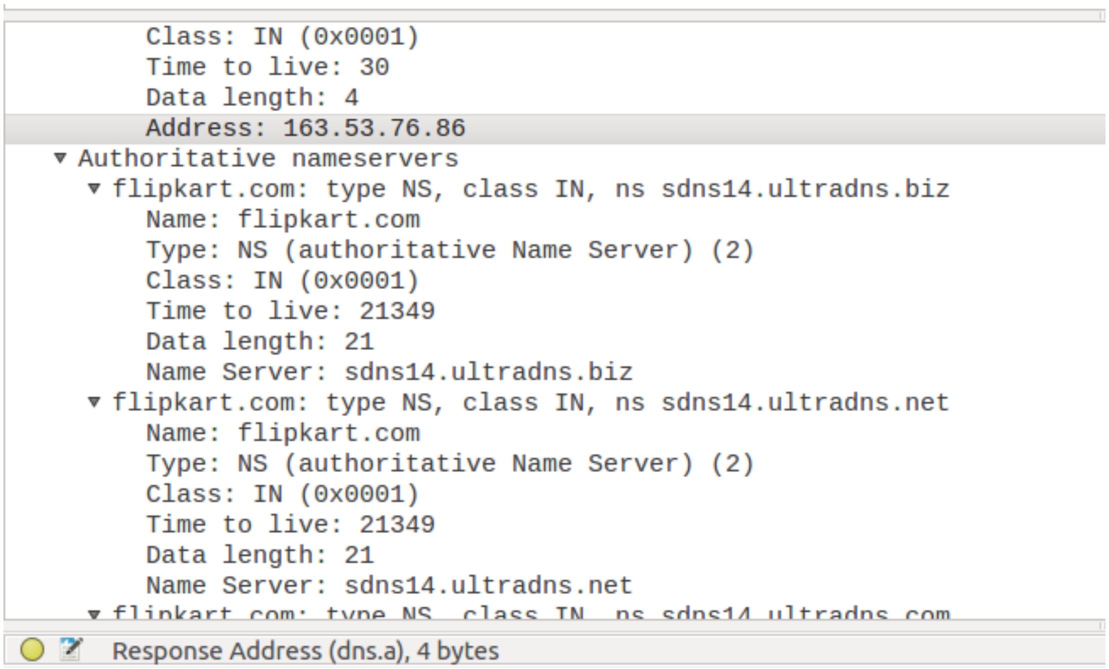


```
No.   Time          Source         Destination       Protocol Length Info
    1 0.000000000   127.0.0.1      127.0.1.1         DNS          74 Standard query 0x8c26 A flipkart.com
    2 0.000140865   10.1.10.57     192.168.3.5       DNS          74 Standard query 0x466a A flipkart.com
    3 0.000156195   10.1.10.57     4.2.2.2           DNS          74 Standard query 0x466a A flipkart.com
    4 0.000163597   10.1.10.57     202.138.96.2      DNS          74 Standard query 0x466a A flipkart.com
    5 0.000170543   10.1.10.57     202.138.103.100   DNS          74 Standard query 0x466a A flipkart.com
    6 0.041180137   4.2.2.2        10.1.10.57        DNS          90 Standard query response 0x466a A flipkart.com A 163.53.78.110
    7 0.041297717   127.0.1.1      127.0.0.1         DNS          90 Standard query response 0x8c26 A flipkart.com A 163.53.78.110
```

The first query and authoritative response are shown below.



```
▼ Domain Name System (response)
    Transaction ID: 0x466a
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ flipkart.com: type A, class IN
  ▼ Answers
    ▼ flipkart.com: type A, class IN, addr 163.53.78.110
        Name: flipkart.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 30
        Data length: 4
        Address: 163.53.78.110
    [Request In: 2]
    [Time: 0.118048425 seconds]
```



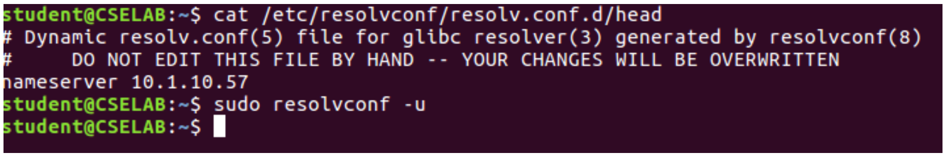
```
        Class: IN (0x0001)
        Time to live: 30
        Data length: 4
        Address: 163.53.76.86
  ▼ Authoritative nameservers
    ▼ flipkart.com: type NS, class IN, ns sdns14.ultradns.biz
        Name: flipkart.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 21349
        Data length: 21
        Name Server: sdns14.ultradns.biz
    ▼ flipkart.com: type NS, class IN, ns sdns14.ultradns.net
        Name: flipkart.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 21349
        Data length: 21
        Name Server: sdns14.ultradns.net
    ▼ flipkart.com: type NS, class IN, ns sdns14.ultradns.com
```

Response Address (dns.a), 4 bytes

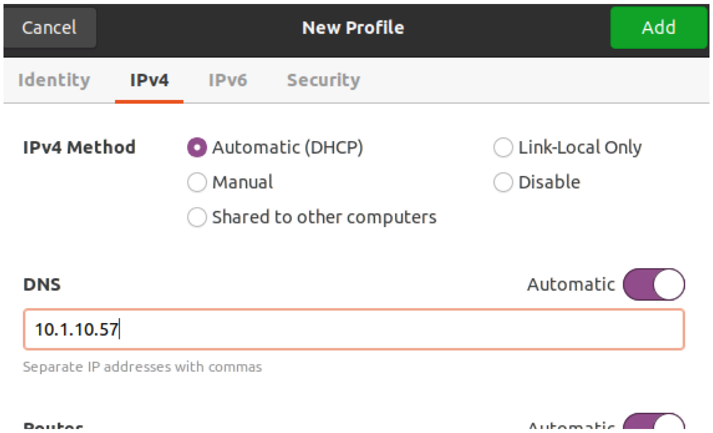
Task 1 - Configuring Client Machine

The IP Address of the client machine is `10.1.10.68` and the IP Address of the server machine is `10.1.10.57`. We need to add the IP Address of the custom DNS server (`10.1.10.57`) in the client machine. We can do this by adding the server's IP address to the file `/etc/resolvconf/resolv.conf.d/head`

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 the IPv4 Network Settings. Finally, the changes can be saved by typing the command `$ sudo resolvconf -u`



```
student@CSELAB:~$ 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
nameserver 10.1.10.57
student@CSELAB:~$ sudo resolvconf -u
student@CSELAB:~$ 
```



IPv4 Method ● Automatic (DHCP) ○ Link-Local Only ○ Manual ○ Disable ○ Shared to other computers

DNS Automatic

10.1.10.57

Separate IP addresses with commas

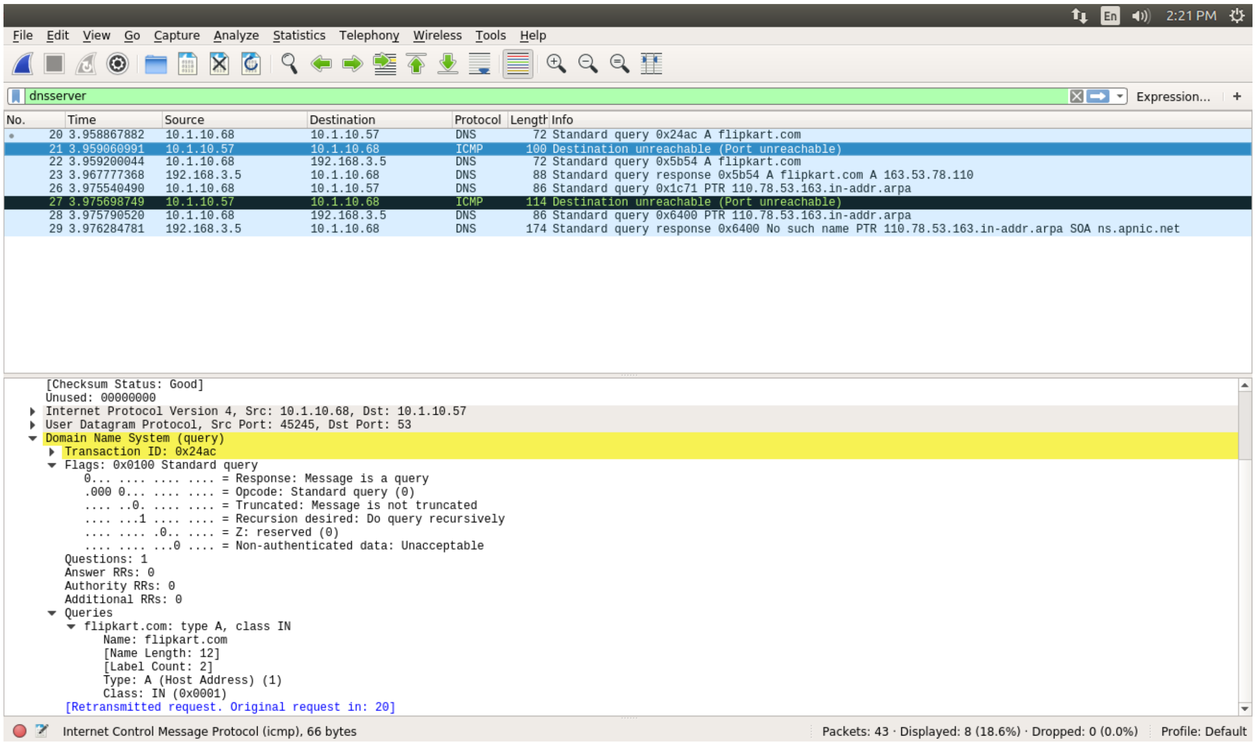
Routes Automatic

Adding `10.1.10.57` in IPv4 settings of client machine.

Second Test

The Flipkart website is pinged again, and Wireshark is used to capture packets.

During packet capture, we get `destination unreachable error` as the server machine does not have a DNS server associated with it. The client tries to obtain the DNS record from `10.1.10.57` but it does not receive any and hence it resorts to using the default DNS server at `127.0.1.1`.



2:21 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dnsserver
Expression…

```
No.   Time         Source        Destination   Protocol Length Info
   20 3.958867882  10.1.10.68    10.1.10.57    DNS       72 Standard query 0x24ac A flipkart.com
   21 3.959060991  10.1.10.57    10.1.10.68    ICMP     100 Destination unreachable (Port unreachable)
   22 3.959200044  10.1.10.68    192.168.3.5   DNS       72 Standard query 0x5b54 A flipkart.com
   23 3.967777368  192.168.3.5   10.1.10.68    DNS       88 Standard query response 0x5b54 A flipkart.com A 163.53.78.110
   26 3.975540490  10.1.10.68    10.1.10.57    DNS       86 Standard query 0x1c71 PTR 110.78.53.163.in-addr.arpa
   27 3.975698749  10.1.10.57    10.1.10.68    ICMP     114 Destination unreachable (Port unreachable)
   28 3.975790520  10.1.10.68    192.168.3.5   DNS       86 Standard query 0x6400 PTR 110.78.53.163.in-addr.arpa
   29 3.976284781  192.168.3.5   10.1.10.68    DNS      174 Standard query response 0x6400 No such name PTR 110.78.53.163.in-addr.arpa SOA ns.apnic.net
```

```
    [Checksum Status: Good]
    Unused: 00000000
  Internet Protocol Version 4, Src: 10.1.10.68, Dst: 10.1.10.57
  User Datagram Protocol, Src Port: 45245, Dst Port: 53
  Domain Name System (query)
      Transaction ID: 0x24ac
      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
          flipkart.com: type A, class IN
              Name: flipkart.com
              [Name Length: 12]
              [Label Count: 2]
              Type: A (Host Address) (1)
              Class: IN (0x0001)
      [Retransmitted request. Original request in: 20]
```

Internet Control Message Protocol (icmp), 66 bytes   Packets: 43 · Displayed: 8 (18.6%) · Dropped: 0 (0.0%)   Profile: Default

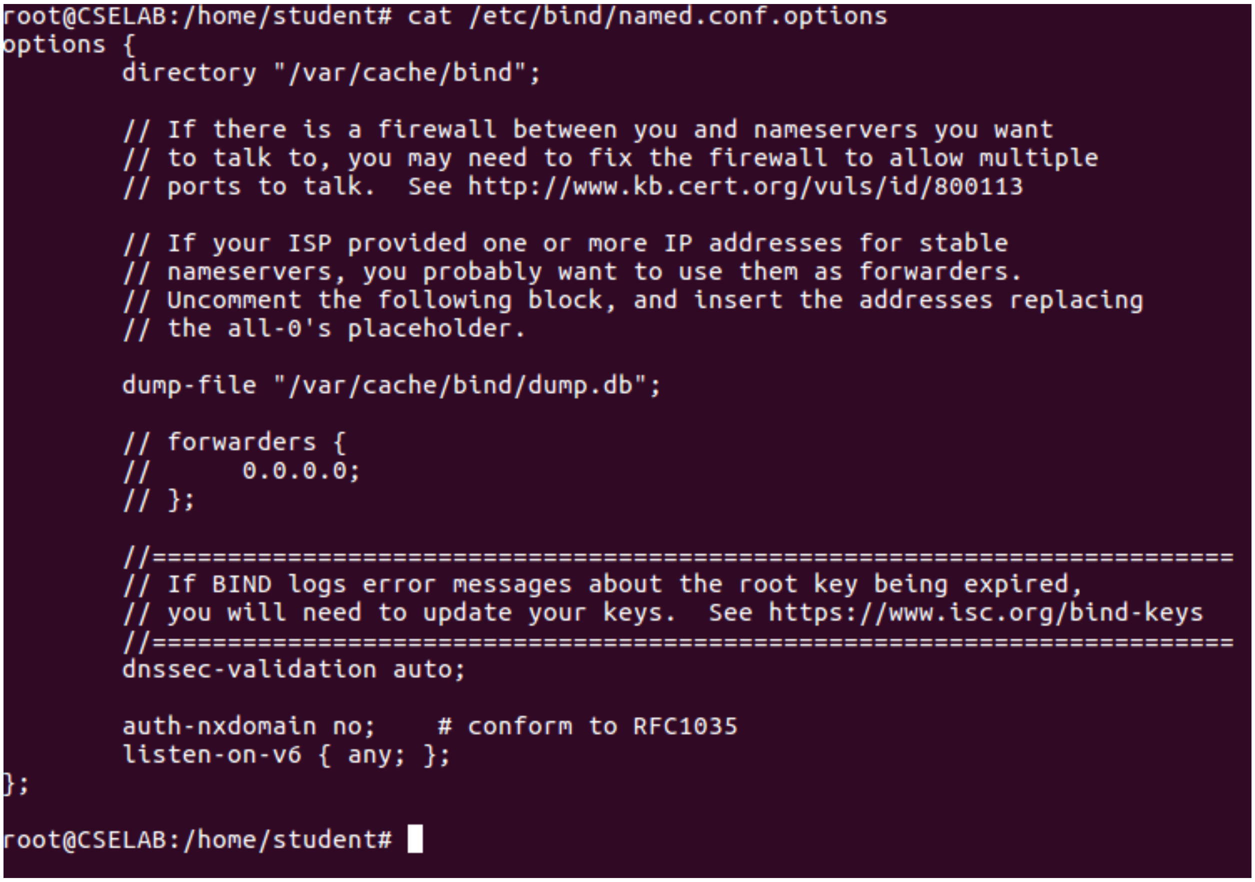
Packet capture in wireshark

Task 2 - Setting Up Local DNS Server

The **bind9** server is used as the DNS server on the server machine. **Bind9** can be installed on the server machine by typing the command $ sudo apt install bind9 in the terminal .

The configuration file for the server is `/etc/bind/named.conf.options`

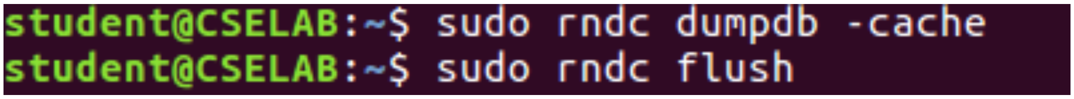
In the configuration file of the server, we need to specify path of the dump file for DNS cache. This can be done by adding the following into /etc/bind/named.conf.options file as shown below.



```
root@CSELAB:/home/student# cat /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // 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;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};

root@CSELAB:/home/student#
```

Adding path to dump-file in bind9 config files

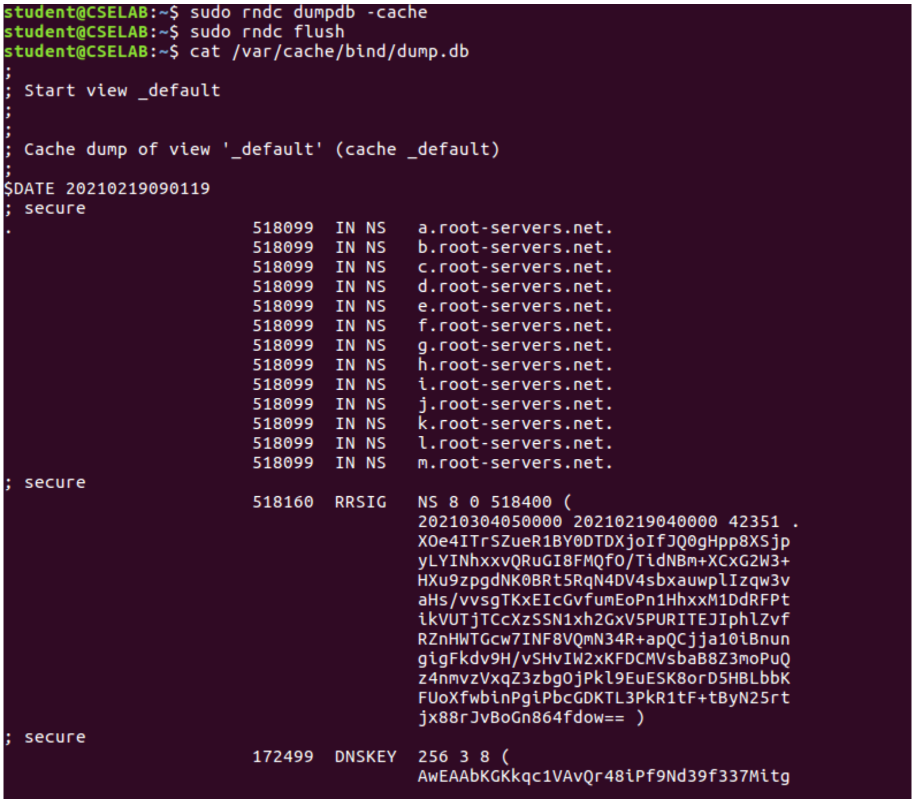
The cache can be dumped into the file using the following command `$ sudo rndc dumpdb -cache` and can be cleared using `$ sudo rndc flush.`



```
student@CSELAB:~$ sudo rndc dumpdb -cache
student@CSELAB:~$ sudo rndc flush
```

We will check the contents of the cache file by typing the command in the terminal.

```
$ cat /var/cache/bind/dump.db
```



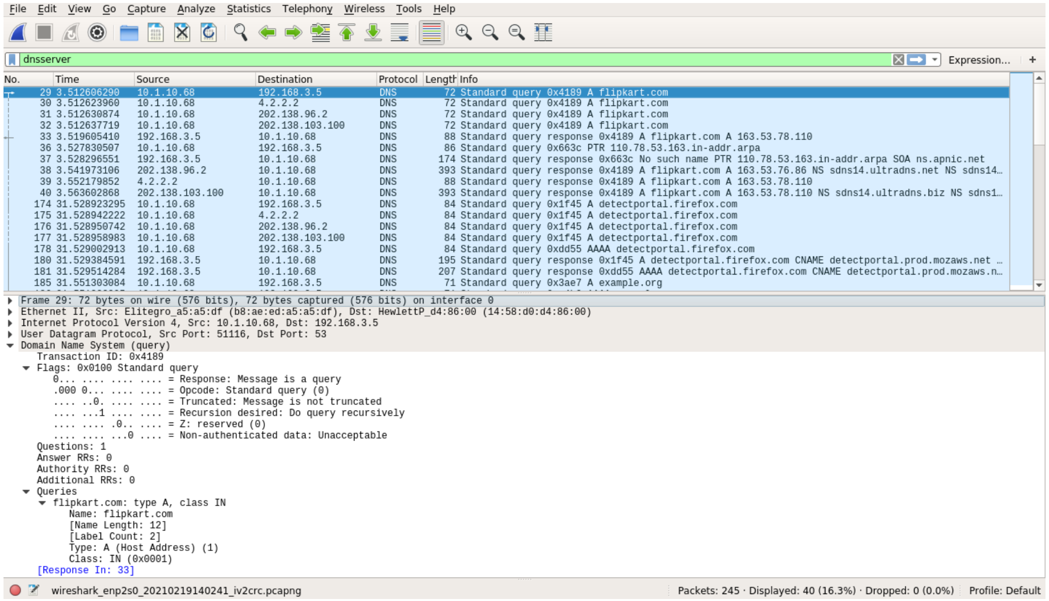
```
student@CSELAB:~$ sudo rndc dumpdb -cache
student@CSELAB:~$ sudo rndc flush
student@CSELAB:~$ cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20210219090119
; secure
.                       518099  IN NS   a.root-servers.net.
                        518099  IN NS   b.root-servers.net.
                        518099  IN NS   c.root-servers.net.
                        518099  IN NS   d.root-servers.net.
                        518099  IN NS   e.root-servers.net.
                        518099  IN NS   f.root-servers.net.
                        518099  IN NS   g.root-servers.net.
                        518099  IN NS   h.root-servers.net.
                        518099  IN NS   i.root-servers.net.
                        518099  IN NS   j.root-servers.net.
                        518099  IN NS   k.root-servers.net.
                        518099  IN NS   l.root-servers.net.
                        518099  IN NS   m.root-servers.net.
; secure
                        518160  RRSIG   NS 8 0 518400 (
                                        20210304050000 20210219040000 42351 .
                                        XOe4ITrSZueR1BY0DTDXjoIfJQ0gHpp8XSjp
                                        yLYINhxxvQRuGI8FMQfO/TidNBm+XCxG2W3+
                                        HXu9zpgdNK0BRt5RqN4DV4sbxauwplIzqw3v
                                        aHs/vvsgTKxEIcGvfumEoPn1HhxxM1DdRFPt
                                        ikVUTjTCcXzSSN1xh2GxV5PURITEJIphlZvf
                                        RZnHWTGcw7INF8VQmN34R+apQCjja10iBnun
                                        gigFkdv9H/vSHvIW2xKFDCMVsbaB8Z3moPuQ
                                        z4nmvzVxqZ3zbgOjPkl9EuESK8orD5HBLbbK
                                        FUoXfwbinPgiPbcGDKTL3PkR1tF+tByN25rt
                                        jx88rJvBoGn864fdow== )
; secure
                        172499  DNSKEY  256 3 8 (
                                        AwEAAbKGKkqc1VAvQr48iPf9Nd39f337Mitg
```

Contents of dump.db

Third Test

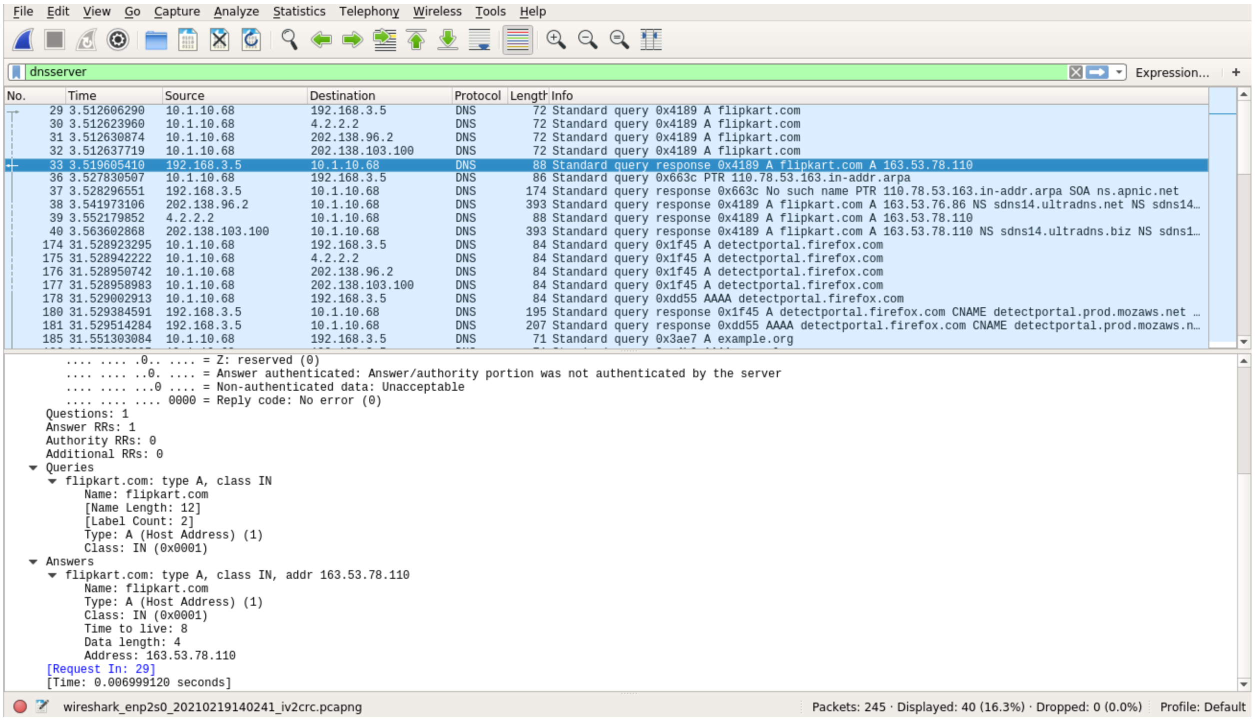
The Flipkart website is pinged again with Wireshark running in the background monitoring ‘any' interface with DNS filter enabled.

The IP Address of the local DNS server is clearly seen in the screenshots below. The cache is dumped into the dump file.



```
dnsserver

No.  Time          Source          Destination      Protocol Length Info
 29  3.512606290   10.1.10.68      192.168.3.5      DNS      72  Standard query 0x4189 A flipkart.com
 30  3.512623960   10.1.10.68      4.2.2.2          DNS      72  Standard query 0x4189 A flipkart.com
 31  3.512630874   10.1.10.68      202.138.96.2     DNS      72  Standard query 0x4189 A flipkart.com
 32  3.512637719   10.1.10.68      202.138.103.100  DNS      72  Standard query 0x4189 A flipkart.com
 33  3.519605410   192.168.3.5     10.1.10.68       DNS      88  Standard query response 0x4189 A flipkart.com A 163.53.78.110
 36  3.527830507   10.1.10.68      192.168.3.5      DNS      86  Standard query 0x663c PTR 110.78.53.163.in-addr.arpa
 37  3.528296551   192.168.3.5     10.1.10.68       DNS     174  Standard query response 0x663c No such name PTR 110.78.53.163.in-addr.arpa SOA ns.apnic.net
 38  3.541973106   202.138.96.2    10.1.10.68       DNS     393  Standard query response 0x4189 A flipkart.com A 163.53.76.86 NS sdns14.ultradns.net NS sdns14…
 39  3.552179852   4.2.2.2         10.1.10.68       DNS      88  Standard query response 0x4189 A flipkart.com A 163.53.78.110
 40  3.563602868   202.138.103.100 10.1.10.68       DNS     393  Standard query response 0x4189 A flipkart.com A 163.53.78.110 NS sdns14.ultradns.biz NS sdns1…
174  31.528923295  10.1.10.68      192.168.3.5      DNS      84  Standard query 0x1f45 A detectportal.firefox.com
175  31.528942222  10.1.10.68      4.2.2.2          DNS      84  Standard query 0x1f45 A detectportal.firefox.com
176  31.528950742  10.1.10.68      202.138.96.2     DNS      84  Standard query 0x1f45 A detectportal.firefox.com
177  31.528958983  10.1.10.68      202.138.103.100  DNS      84  Standard query 0x1f45 A detectportal.firefox.com
178  31.529002913  10.1.10.68      192.168.3.5      DNS      84  Standard query 0xdd55 AAAA detectportal.firefox.com
180  31.529384591  192.168.3.5     10.1.10.68       DNS     195  Standard query response 0x1f45 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net …
181  31.529514284  192.168.3.5     10.1.10.68       DNS     207  Standard query response 0xdd55 AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.n…
185  31.551303084  10.1.10.68      192.168.3.5      DNS      71  Standard query 0x3ae7 A example.org

▶ Frame 29: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
▶ Ethernet II, Src: Elitegro_a5:a5:df (b8:ae:ed:a5:a5:df), Dst: HewlettP_d4:86:00 (14:58:d0:d4:86:00)
▶ Internet Protocol Version 4, Src: 10.1.10.68, Dst: 192.168.3.5
▶ User Datagram Protocol, Src Port: 51116, Dst Port: 53
▼ Domain Name System (query)
    Transaction ID: 0x4189
  ▼ 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
    ▼ flipkart.com: type A, class IN
        Name: flipkart.com
        [Name Length: 12]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 33]

wireshark_enp2s0_20210219140241_iv2crc.pcapng    Packets: 245 · Displayed: 40 (16.3%) · Dropped: 0 (0.0%)    Profile: Default
```

DNS Query packet in Wireshark


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

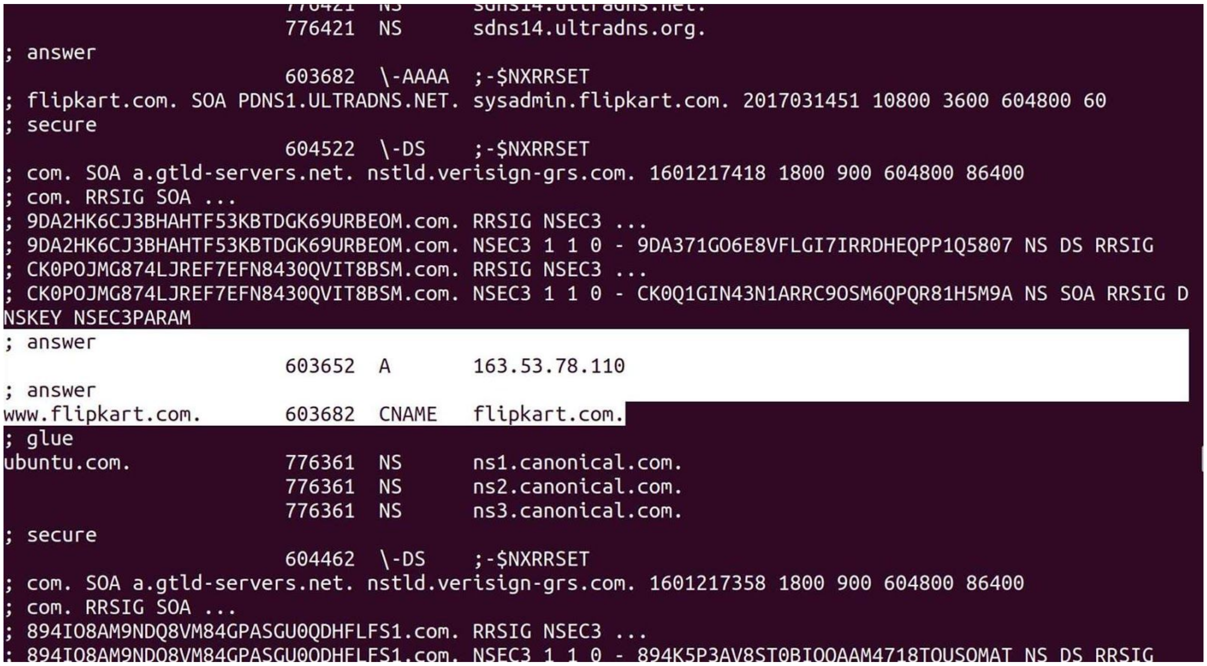
```
dnsserver
```

```
No.   Time          Source           Destination      Protocol Length Info
   29 3.512606290   10.1.10.68       192.168.3.5      DNS        72 Standard query 0x4189 A flipkart.com
   30 3.512623960   10.1.10.68       4.2.2.2          DNS        72 Standard query 0x4189 A flipkart.com
   31 3.512630874   10.1.10.68       202.138.96.2     DNS        72 Standard query 0x4189 A flipkart.com
   32 3.512637719   10.1.10.68       202.138.103.100  DNS        72 Standard query 0x4189 A flipkart.com
   33 3.519605410   192.168.3.5      10.1.10.68       DNS        88 Standard query response 0x4189 A flipkart.com A 163.53.78.110
   36 3.527830507   10.1.10.68       192.168.3.5      DNS        86 Standard query 0x663c PTR 110.78.53.163.in-addr.arpa
   37 3.528296551   192.168.3.5      10.1.10.68       DNS       174 Standard query response 0x663c No such name PTR 110.78.53.163.in-addr.arpa SOA ns.apnic.net
   38 3.541973106   202.138.96.2     10.1.10.68       DNS       393 Standard query response 0x4189 A flipkart.com A 163.53.76.86 NS sdns14.ultradns.net NS sdns14…
   39 3.552179852   4.2.2.2          10.1.10.68       DNS        88 Standard query response 0x4189 A flipkart.com A 163.53.78.110
   40 3.563602868   202.138.103.100  10.1.10.68       DNS       393 Standard query response 0x4189 A flipkart.com A 163.53.78.110 NS sdns14.ultradns.biz NS sdns1…
  174 31.528923295  10.1.10.68       192.168.3.5      DNS        84 Standard query 0x1f45 A detectportal.firefox.com
  175 31.528942222  10.1.10.68       4.2.2.2          DNS        84 Standard query 0x1f45 A detectportal.firefox.com
  176 31.528950742  10.1.10.68       202.138.96.2     DNS        84 Standard query 0x1f45 A detectportal.firefox.com
  177 31.528958983  10.1.10.68       202.138.103.100  DNS        84 Standard query 0x1f45 A detectportal.firefox.com
  178 31.529002913  10.1.10.68       192.168.3.5      DNS        84 Standard query 0xdd55 AAAA detectportal.firefox.com
  180 31.529384591  192.168.3.5      10.1.10.68       DNS       195 Standard query response 0x1f45 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net …
  181 31.529514284  192.168.3.5      10.1.10.68       DNS       207 Standard query response 0xdd55 AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.n…
  185 31.551303084  10.1.10.68       192.168.3.5      DNS        71 Standard query 0x3ae7 A example.org
```

```
      .... .... .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
    ▾ flipkart.com: type A, class IN
        Name: flipkart.com
        [Name Length: 12]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Answers
    ▾ flipkart.com: type A, class IN, addr 163.53.78.110
        Name: flipkart.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 8
        Data length: 4
        Address: 163.53.78.110
    [Request In: 29]
    [Time: 0.006999120 seconds]
```

```
wireshark_enp2s0_20210219140241_iv2crc.pcapng      Packets: 245 · Displayed: 40 (16.3%) · Dropped: 0 (0.0%)   Profile: Default
```

DNS Response Packet



```
                        776421  NS      sdns14.ultradns.net.
                        776421  NS      sdns14.ultradns.org.
; answer
                        603682  \-AAAA  ;-$NXRRSET
; flipkart.com. SOA PDNS1.ULTRADNS.NET. sysadmin.flipkart.com. 2017031451 10800 3600 604800 60
; secure
                        604522  \-DS    ;-$NXRRSET
; com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1601217418 1800 900 604800 86400
; com. RRSIG SOA ...
; 9DA2HK6CJ3BHAHTF53KBTDGK69URBEOM.com. RRSIG NSEC3 ...
; 9DA2HK6CJ3BHAHTF53KBTDGK69URBEOM.com. NSEC3 1 1 0 - 9DA371GO6E8VFLGI7IRRDHEQPP1Q5807 NS DS RRSIG
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. RRSIG NSEC3 ...
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6QPQR81H5M9A NS SOA RRSIG D
NSKEY NSEC3PARAM
; answer
                        603652  A       163.53.78.110
; answer
www.flipkart.com.       603682  CNAME   flipkart.com.
; glue
ubuntu.com.             776361  NS      ns1.canonical.com.
                        776361  NS      ns2.canonical.com.
                        776361  NS      ns3.canonical.com.
; secure
                        604462  \-DS    ;-$NXRRSET
; com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1601217358 1800 900 604800 86400
; com. RRSIG SOA ...
; 894I08AM9NDQ8VM84GPASGU0QDHFLFS1.com. RRSIG NSEC3 ...
; 894I08AM9NDQ8VM84GPASGU0QDHFLFS1.com. NSEC3 1 1 0 - 894K5P3AV8ST0BIQOAAM4718TQUSOMAT NS DS RRSIG
```

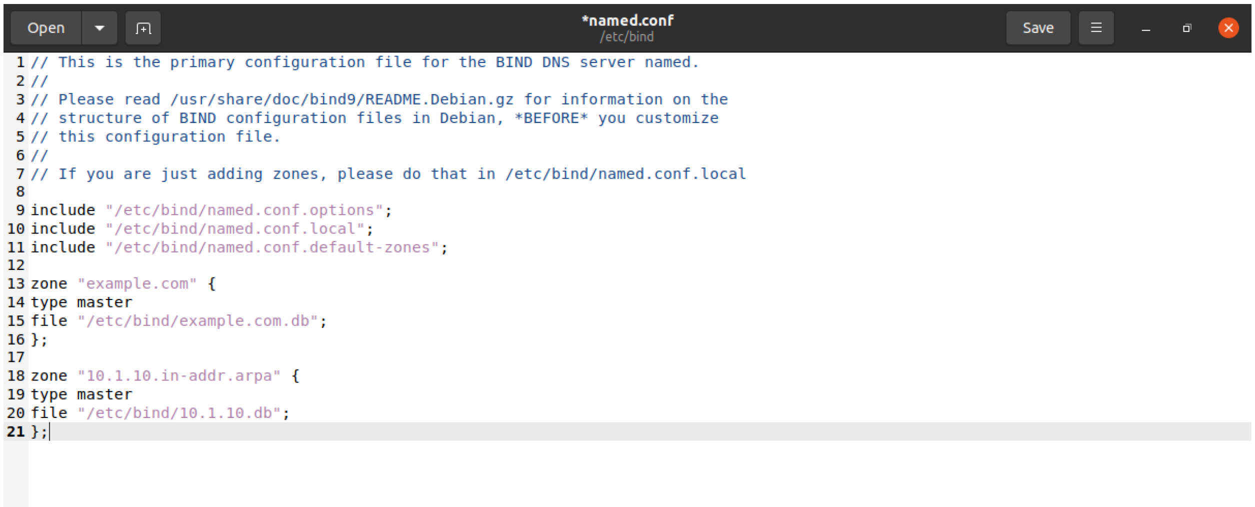
Cache in Dumpfile

Task 3 - Hosting a Zone in the Local DNS Server

Creating a zone

The two zones corresponding to the domain www.example.com must be added to the /etc/bind/named.conf file in the server.

The first zone corresponds to the forward lookup (translation from hostname to IP Address) and the second zone is for the reverse lookup (translation from IP Address to hostname).



```
// 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 "10.1.10.in-addr.arpa" {
type master
file "/etc/bind/10.1.10.db";
};
```

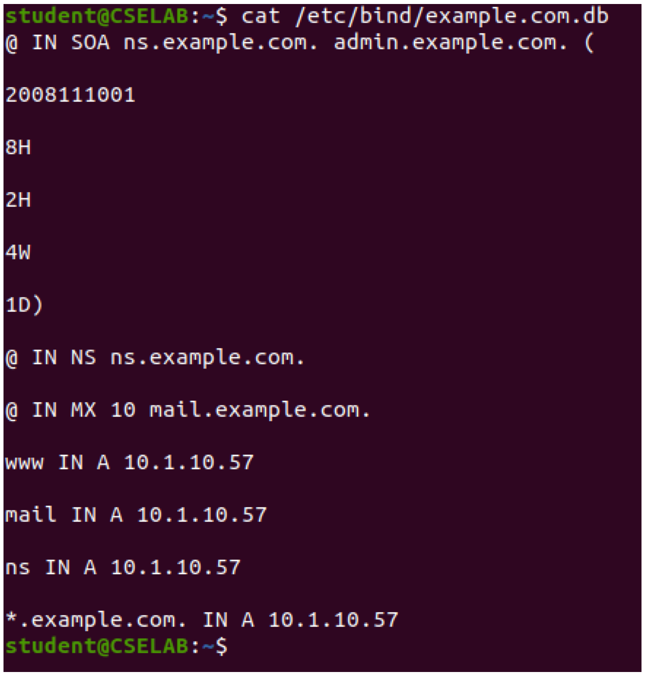
Creating Zones in named.conf file

Forward and Reverse Lookup

The forward lookup file is located at `/etc/bind/example.com.db`. The symbol @ is used to indicate the origin specified, in this case `www.example.com`.

There are 7 records in the lookup file, an SOA record, a nameserver, a mail server and 4 authoritative records.

The TTL field tells the server how long this record should stay in the cache before being removed. In this case the local DNS server requests for a fresh entry from the name server.

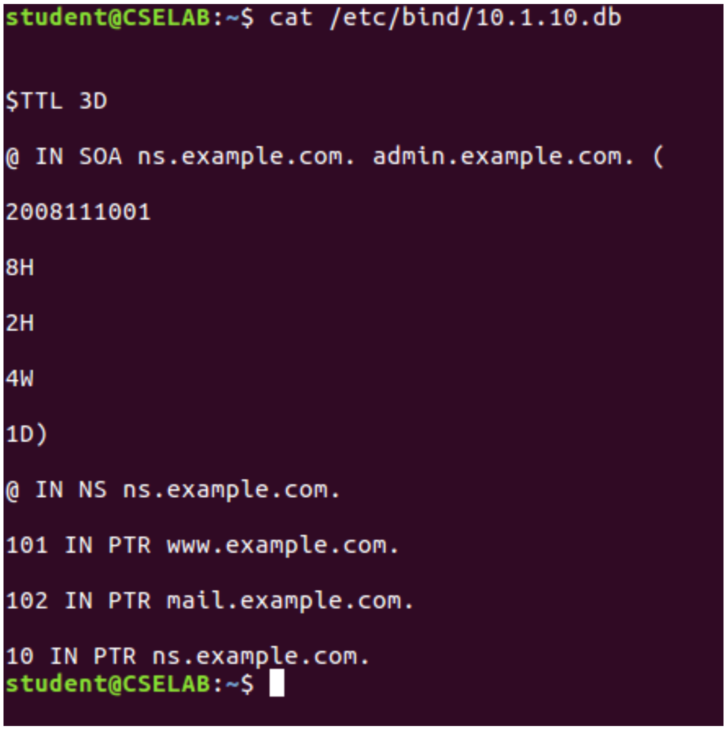


```
student@CSELAB:~$ cat /etc/bind/example.com.db
@ IN SOA ns.example.com. admin.example.com. (

2008111001

8H

2H

4W

1D)

@ IN NS ns.example.com.

@ IN MX 10 mail.example.com.

www IN A 10.1.10.57

mail IN A 10.1.10.57

ns IN A 10.1.10.57

*.example.com. IN A 10.1.10.57
student@CSELAB:~$
```

Forward Lookup File

The reverse lookup file is stored at **/etc/bind/10.1.10.db** and is used to translate IP Addresses to hostnames for the given domain, in this case example.com.

For each IP Address defined in the forward lookup file, a corresponding hostname is referenced here. The record type here is PTR or DNS Pointer Record.



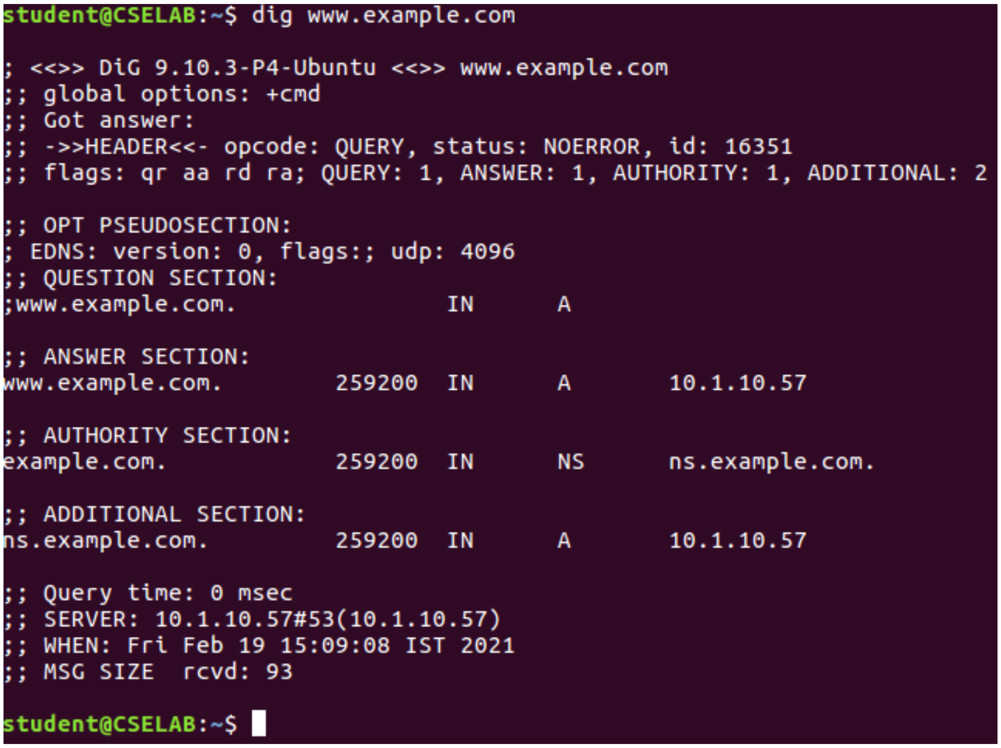
```
student@CSELAB:~$ cat /etc/bind/10.1.10.db


$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.
student@CSELAB:~$
```

Reverse Lookup File

Fourth Test – Testing www.example.com

The dig command is used to lookup name servers specified in the file `/etc/resolv.conf.`

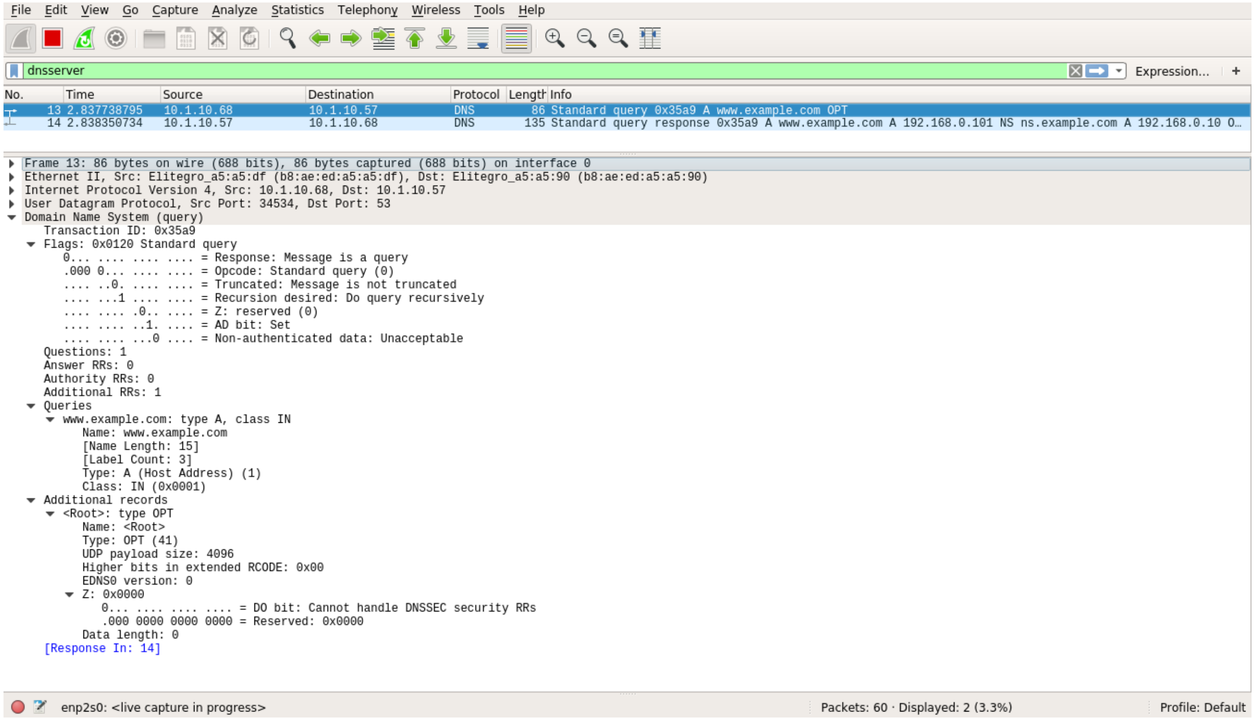
Wireshark is used to capture the packets while running the command `$ dig www.example.com`. The IP Address of the DNS Server and the returned IP Address of the domain set by us can be seen in the query and response packets.



```
student@CSELAB:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16351
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.1.10.57

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       10.1.10.57

;; Query time: 0 msec
;; SERVER: 10.1.10.57#53(10.1.10.57)
;; WHEN: Fri Feb 19 15:09:08 IST 2021
;; MSG SIZE  rcvd: 93

student@CSELAB:~$ 
```

Running dig www.example.com in terminal

Packet Capture in Wireshark


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

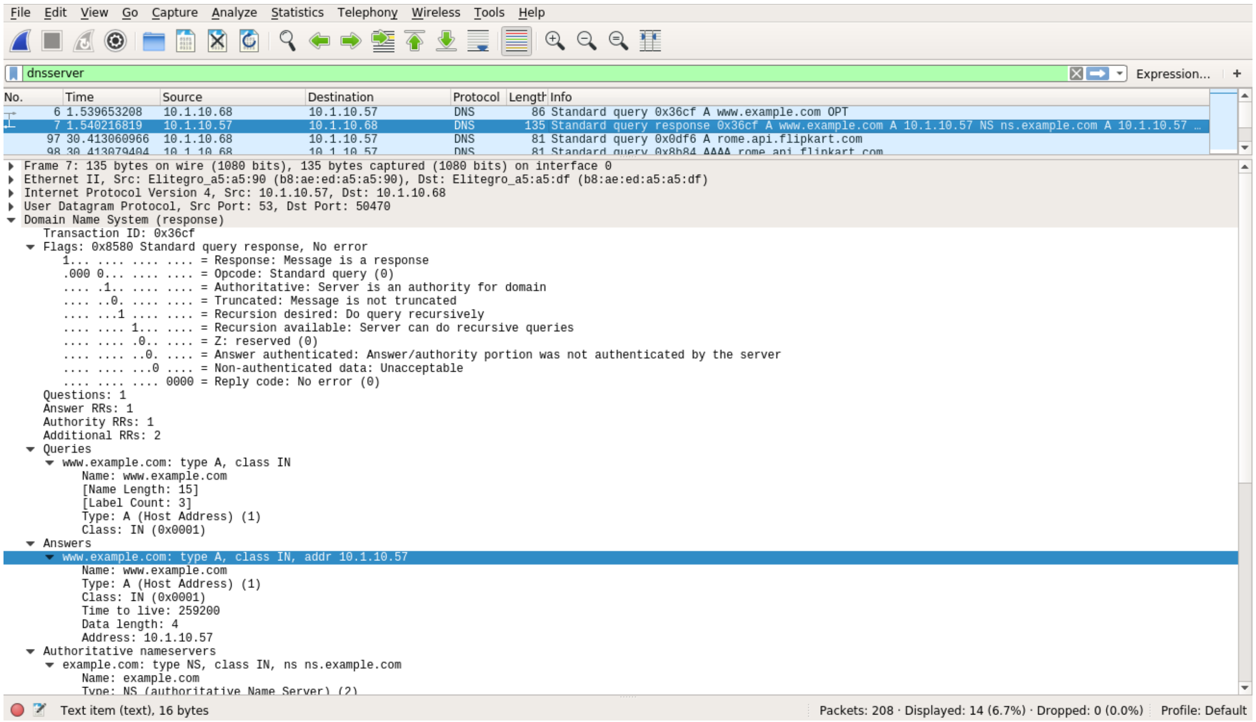
dnsserver

```
No.   Time          Source       Destination  Protocol Length Info
   13 2.837738795   10.1.10.68   10.1.10.57   DNS        86 Standard query 0x35a9 A www.example.com OPT
   14 2.838350734   10.1.10.57   10.1.10.68   DNS       135 Standard query response 0x35a9 A www.example.com A 192.168.0.101 NS ns.example.com A 192.168.0.10 O…
```

```
▸ Frame 13: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
▸ Ethernet II, Src: Elitegro_a5:a5:df (b8:ae:ed:a5:a5:df), Dst: Elitegro_a5:a5:90 (b8:ae:ed:a5:a5:90)
▸ Internet Protocol Version 4, Src: 10.1.10.68, Dst: 10.1.10.57
▸ User Datagram Protocol, Src Port: 34534, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x35a9
  ▾ Flags: 0x0120 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)
      .... .... ..1. .... = AD bit: Set
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ www.example.com: type A, class IN
        Name: www.example.com
        [Name Length: 15]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Additional records
    ▾ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▾ Z: 0x0000
          0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
          .000 0000 0000 0000 = Reserved: 0x0000
        Data length: 0
    [Response In: 14]
```

enp2s0: <live capture in progress>   Packets: 60 · Displayed: 2 (3.3%)   Profile: Default

DNS Query Packet


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

dnsserver

```
No.   Time          Source       Destination  Protocol Length Info
    6 1.539653208   10.1.10.68   10.1.10.57   DNS        86 Standard query 0x36cf A www.example.com OPT
    7 1.540216819   10.1.10.57   10.1.10.68   DNS       135 Standard query response 0x36cf A www.example.com A 10.1.10.57 NS ns.example.com A 10.1.10.57 …
   97 30.413060966  10.1.10.68   10.1.10.57   DNS        81 Standard query 0x0df6 A rome.api.flipkart.com
   98 30.413079404  10.1.10.68   10.1.10.57   DNS        81 Standard query 0x8b84 AAAA rome.api.flipkart.com
```

```
▸ Frame 7: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0
▸ Ethernet II, Src: Elitegro_a5:a5:90 (b8:ae:ed:a5:a5:90), Dst: Elitegro_a5:a5:df (b8:ae:ed:a5:a5:df)
▸ Internet Protocol Version 4, Src: 10.1.10.57, Dst: 10.1.10.68
▸ User Datagram Protocol, Src Port: 53, Dst Port: 50470
▾ Domain Name System (response)
    Transaction ID: 0x36cf
  ▾ Flags: 0x8580 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .1.. .... .... = Authoritative: Server is 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: 1
    Additional RRs: 2
  ▾ Queries
    ▾ www.example.com: type A, class IN
        Name: www.example.com
        [Name Length: 15]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▾ Answers
    ▾ www.example.com: type A, class IN, addr 10.1.10.57
        Name: www.example.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 259200
        Data length: 4
        Address: 10.1.10.57
  ▾ Authoritative nameservers
    ▾ example.com: type NS, class IN, ns ns.example.com
        Name: example.com
        Type: NS (authoritative Name Server) (2)
```

Text item (text), 16 bytes   Packets: 208 · Displayed: 14 (6.7%) · Dropped: 0 (0.0%)   Profile: Default

DNS Response Packet

Questions

Q1. Locate the DNS query and response messages. Are they sent over UDP or TCP?
Answer : The DNS Query and Response messages are visible in the screenshots. They are sent over UDP.

Q2. What is the destination port for the DNS query message? What is the source port of the 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 ifconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
Answer – The DNS query is made to the server at the IP Address 10.2.20.161 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 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.

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.flipkart.com) retrieved from the response message.