

# Computer Networks Laboratory

**NAME: PREM SAGAR J S**

**SRN: PES1UG20CS825**

**SEC: 'H'**

## Lab #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:

- DNS and how it works
- Install and set up a DNS server
- Functionality and operations

### Lab Setup (Using Two Virtual Machines)

DNS Server: 10.0.2.8 (VM 1)

User/Client: 10.0.2.15 (default IP) (VM 2)

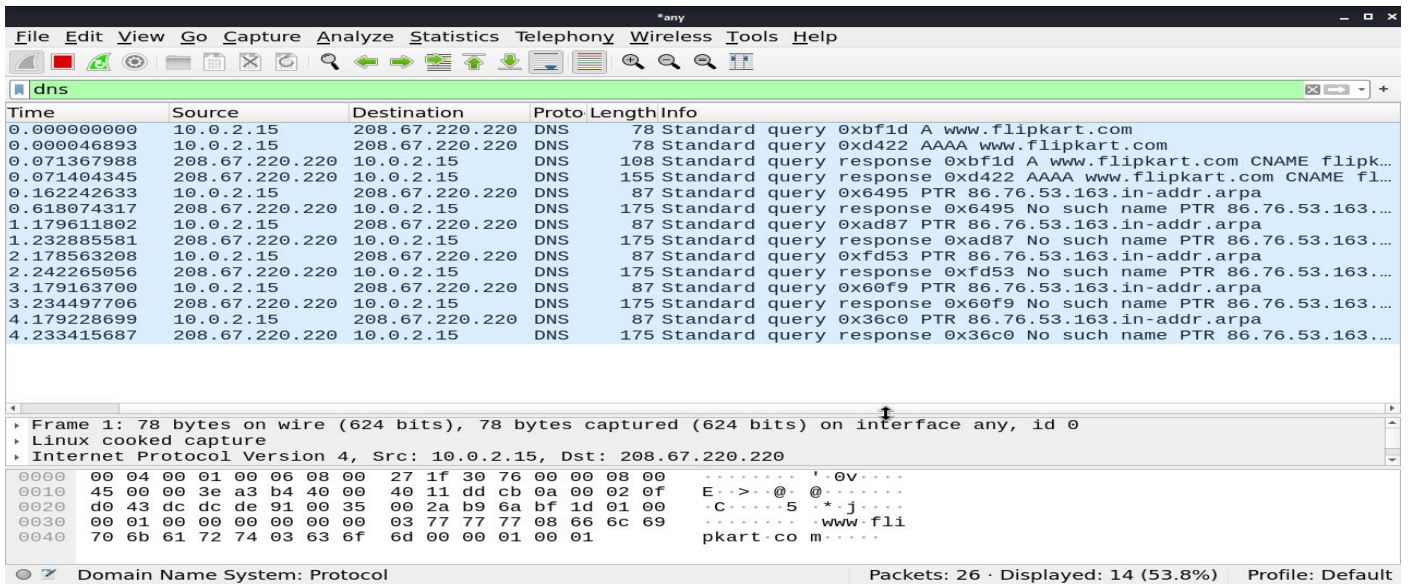
### First Test: Pinging using default DNS

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

Pinging [www.flipkart.com](http://www.flipkart.com)

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo ping www.flipkart.com  
[sudo] password for kali:  
PING flipkart.com (163.53.76.86) 56(84) bytes of data.  
64 bytes from 163.53.76.86 (163.53.76.86): icmp_seq=1 ttl=54 time=89.5 ms  
64 bytes from 163.53.76.86 (163.53.76.86): icmp_seq=2 ttl=54 time=107 ms  
64 bytes from 163.53.76.86 (163.53.76.86): icmp_seq=3 ttl=54 time=106 ms  
64 bytes from 163.53.76.86 (163.53.76.86): icmp_seq=4 ttl=54 time=106 ms  
64 bytes from 163.53.76.86 (163.53.76.86): icmp_seq=5 ttl=54 time=105 ms  
^C  
--- flipkart.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4002ms  
rtt min/avg/max/mdev = 89.528/102.708/107.072/6.624 ms  
kali@kali:~$
```

The IP Address of the DNS server is observed to be 208.67.220.220.



Time	Source	Destination	Proto	Length	Info
0.000000000	10.0.2.15	208.67.220.220	DNS	78	Standard query 0xbfd A www.flipkart.com
0.000046893	10.0.2.15	208.67.220.220	DNS	78	Standard query 0xd422 AAAA www.flipkart.com
0.071367988	208.67.220.220	10.0.2.15	DNS	108	Standard query response 0xbfd A www.flipkart.com CNAME flipk...
0.071404345	208.67.220.220	10.0.2.15	DNS	155	Standard query response 0xd422 AAAA www.flipkart.com CNAME fl...
0.162242633	10.0.2.15	208.67.220.220	DNS	87	Standard query 0x6495 PTR 86.76.53.163.in-addr.arpa
0.618074317	208.67.220.220	10.0.2.15	DNS	175	Standard query response 0x6495 No such name PTR 86.76.53.163....
1.179611802	10.0.2.15	208.67.220.220	DNS	87	Standard query 0xad87 PTR 86.76.53.163.in-addr.arpa
1.232885581	208.67.220.220	10.0.2.15	DNS	175	Standard query response 0xad87 No such name PTR 86.76.53.163....
2.178563208	10.0.2.15	208.67.220.220	DNS	87	Standard query 0xfd53 PTR 86.76.53.163.in-addr.arpa
2.242265050	208.67.220.220	10.0.2.15	DNS	175	Standard query response 0xfd53 No such name PTR 86.76.53.163....
3.179163700	10.0.2.15	208.67.220.220	DNS	87	Standard query 0x60f9 PTR 86.76.53.163.in-addr.arpa
3.234497706	208.67.220.220	10.0.2.15	DNS	175	Standard query response 0x60f9 No such name PTR 86.76.53.163....
4.179228699	10.0.2.15	208.67.220.220	DNS	87	Standard query 0x36c0 PTR 86.76.53.163.in-addr.arpa
4.233415687	208.67.220.220	10.0.2.15	DNS	175	Standard query response 0x36c0 No such name PTR 86.76.53.163....

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0

Linux cooked capture

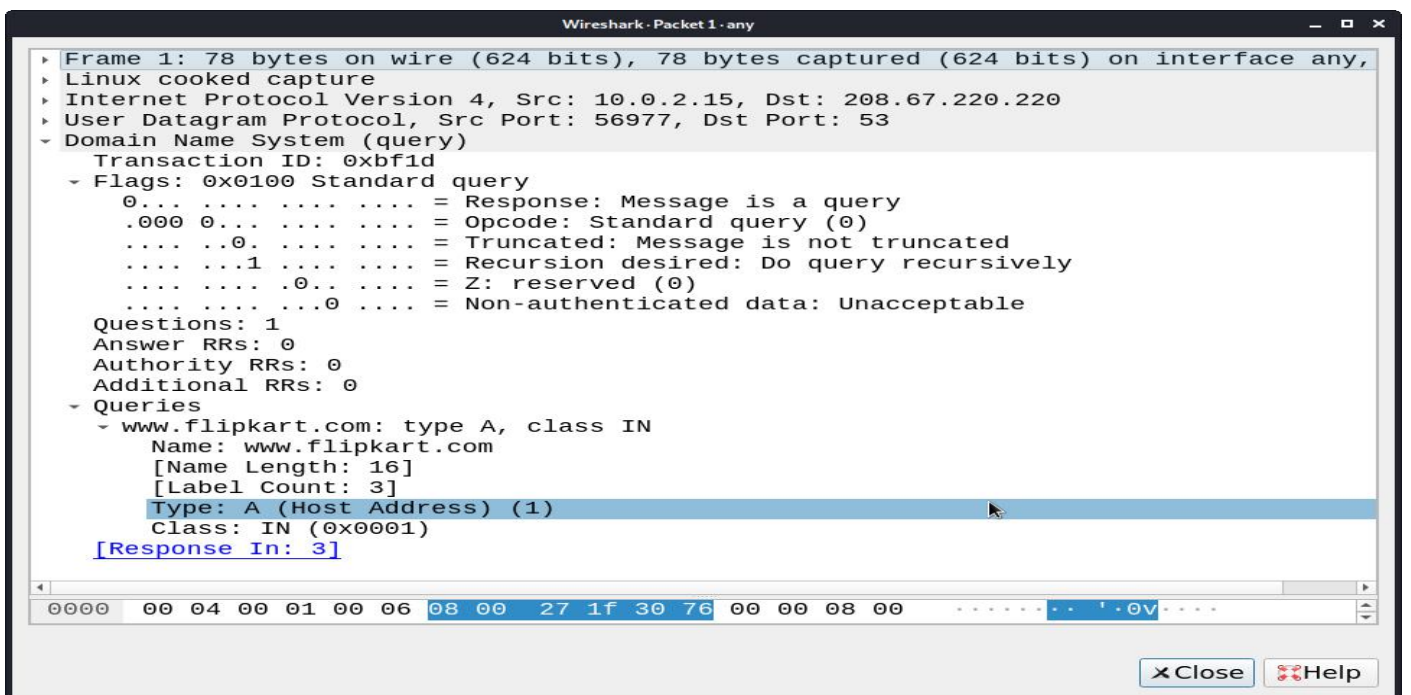
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 208.67.220.220

0000	00 04 00 01 00 06 08 00	27 1f 30 76 00 00 08 00	.....OV.....
0010	45 00 00 3e a3 b4 40 00	40 11 dd cb 0a 00 02 0f	E...@.....
0020	d0 43 dc dc de 91 00 35	00 2a b9 6a bf 1d 01 00	.C...5...*j....
0030	00 01 00 00 00 00 00 00	03 77 77 77 08 66 6c 69	.....www.fli
0040	70 6b 61 72 74 03 63 6f	6d 00 00 01 00 01	pkart.co m....

Domain Name System: Protocol

Packets: 26 · Displayed: 14 (53.8%) Profile: Default

### Wireshark Packet Capture



Wireshark - Packet 1 - any

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any,

Linux cooked capture

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 208.67.220.220

User Datagram Protocol, Src Port: 56977, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xbfd

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.flipkart.com: type A, class IN

Name: www.flipkart.com

[Name Length: 16]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 3]

0000	00 04 00 01 00 06 08 00	27 1f 30 76 00 00 08 00	.....OV.....
------	-------------------------	-------------------------	--------------

Close Help

### DNS Standard Query

IP address of the website – 163.53.78.110.

```
Wireshark - Packet 3 - any
Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface a
Linux cooked capture
Internet Protocol Version 4, Src: 208.67.220.220, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 56977
Domain Name System (response)
  Transaction ID: 0xbfd1d
  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 au
    .... 0... .. = Non-authenticated data: Unacceptable
    .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  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
      Name: www.flipkart.com
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 58 (58 seconds)
      Data length: 2
      CNAME: flipkart.com
    flipkart.com: type A, class IN, addr 163.53.76.86
      Name: flipkart.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 21 (21 seconds)
      Data length: 4
      Address: 163.53.76.86
  [Request In: 1]
  [Time: 0.071367988 seconds]
```

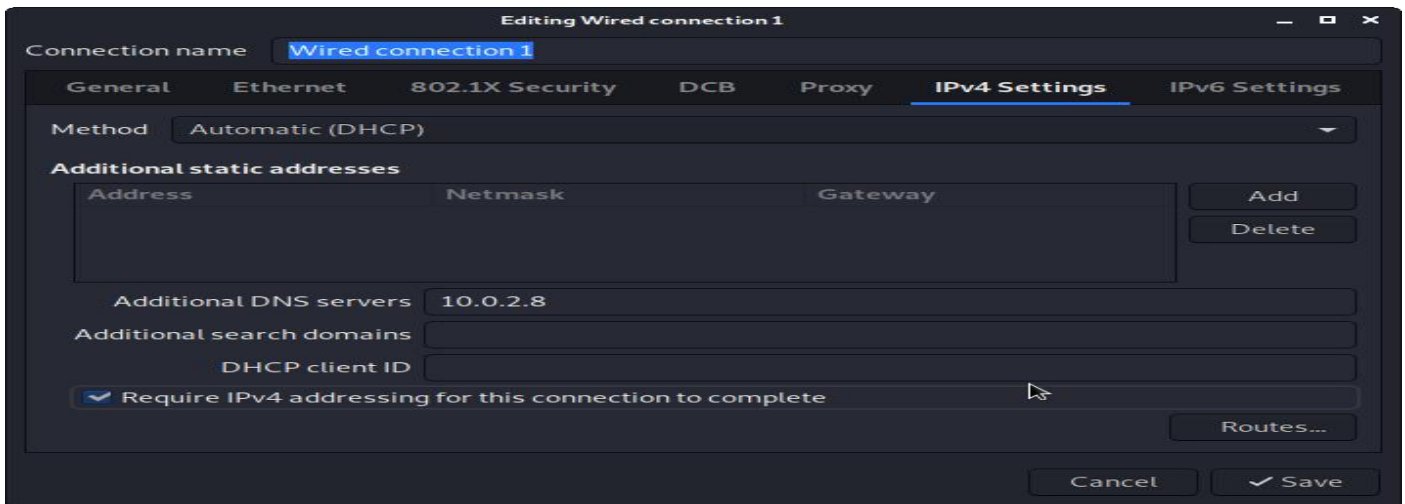
DNS Standard Query Response

## Part 1: Setting Up a Local DNS Server

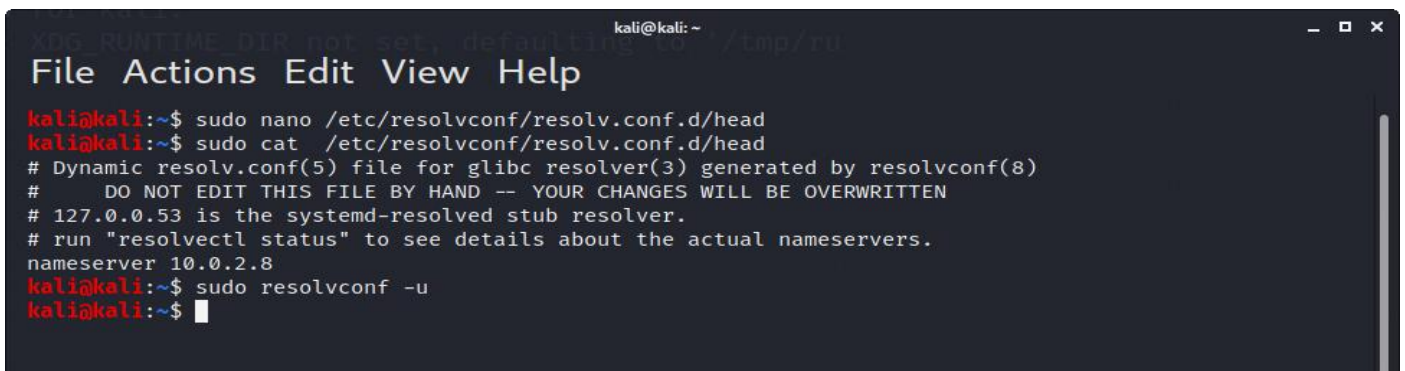
### Task 1: Configure the User Machine

- The IP Address of the client machine is 10.0.2.15.
- The IP Address of the server machine is 10.0.2.8.
- We need to add the IP Address of the custom DNS server (10.0.2.8) to the client machine.
- The IP Address of the custom DNS server is also added to the DNS menu under the IPv4 Network Settings.





- 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.

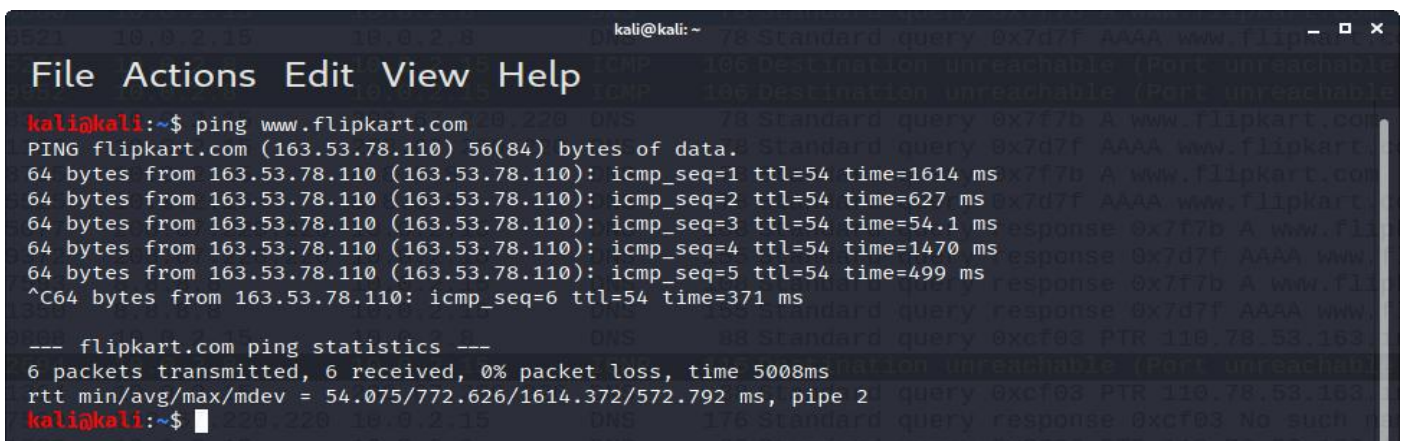


- The changes are applied by using the command `sudo resolvconf -u`

## Second Test:

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

- The Flipkart website is pinged again.



No.	Time	Source	Destination	Proto	Length	Info
1	0.000000000	10.0.2.15	10.0.2.8	DNS	78	Standard query 0x7f7b A www.flipkart.com
2	0.000046521	10.0.2.15	10.0.2.8	DNS	78	Standard query 0x7d7f AAAA www.flipkart.com
5	0.000768368	10.0.2.15	208.67.220.220	DNS	78	Standard query 0x7f7b A www.flipkart.com
6	0.000791182	10.0.2.15	208.67.220.220	DNS	78	Standard query 0x7d7f AAAA www.flipkart.com
7	3.004088735	10.0.2.15	8.8.8.8	DNS	78	Standard query 0x7f7b A www.flipkart.com
8	3.004195525	10.0.2.15	8.8.8.8	DNS	78	Standard query 0x7d7f AAAA www.flipkart.com
15	6.054505077	208.67.220.220	10.0.2.15	DNS	108	Standard query response 0x7f7b A www.flipkart.com CNAME flip
16	6.054539372	208.67.220.220	10.0.2.15	DNS	155	Standard query response 0x7d7f AAAA www.flipkart.com CNAME f
17	6.171787593	8.8.8.8	10.0.2.15	DNS	108	Standard query response 0x7f7b A www.flipkart.com CNAME flip
18	6.171841350	8.8.8.8	10.0.2.15	DNS	155	Standard query response 0x7d7f AAAA www.flipkart.com CNAME f
22	7.787580808	10.0.2.15	10.0.2.8	DNS	88	Standard query 0xcf03 PTR 110.78.53.163.in-addr.arpa
24	7.788761364	10.0.2.15	208.67.220.220	DNS	88	Standard query 0xcf03 PTR 110.78.53.163.in-addr.arpa
26	7.862777590	208.67.220.220	10.0.2.15	DNS	176	Standard query response 0xcf03 No such name PTR 110.78.53.16
27	7.863281586	10.0.2.15	10.0.2.8	DNS	88	Standard query 0x3666 PTR 110.78.53.163.in-addr.arpa
29	7.863947698	10.0.2.15	208.67.220.220	DNS	88	Standard query 0x3666 PTR 110.78.53.163.in-addr.arpa
30	7.939361979	208.67.220.220	10.0.2.15	DNS	176	Standard query response 0x3666 No such name PTR 110.78.53.16
33	8.229219321	10.0.2.15	10.0.2.8	DNS	88	Standard query 0xcb23 PTR 110.78.53.163.in-addr.arpa

Frame 27: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface any, id 0

Linux cooked capture

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.8

```

0000  00 04 00 01 00 06 08 00 27 1f 30 76 00 00 08 00  ...v...
0010  45 00 00 48 30 fa 40 00 40 11 f1 94 0a 00 02 0f  E..H.@.@
0020  0a 00 02 08 80 84 00 35 00 34 18 5c 36 66 01 00  ...4\6f...
0030  00 01 00 00 00 00 00 00 03 31 31 30 02 37 38 02  ...110 78...
0040  35 33 03 31 36 33 07 69 6e 2d 61 64 64 72 04 61  53 163 1 n-addr a

```

wireshark\_any\_202102...110051\_wap36X.pcapng Packets: 55 · Displayed: 33 (60.0%) · Marked: 1 (1.8%) · Ignored: 4 (7.3%) · Profile: Default

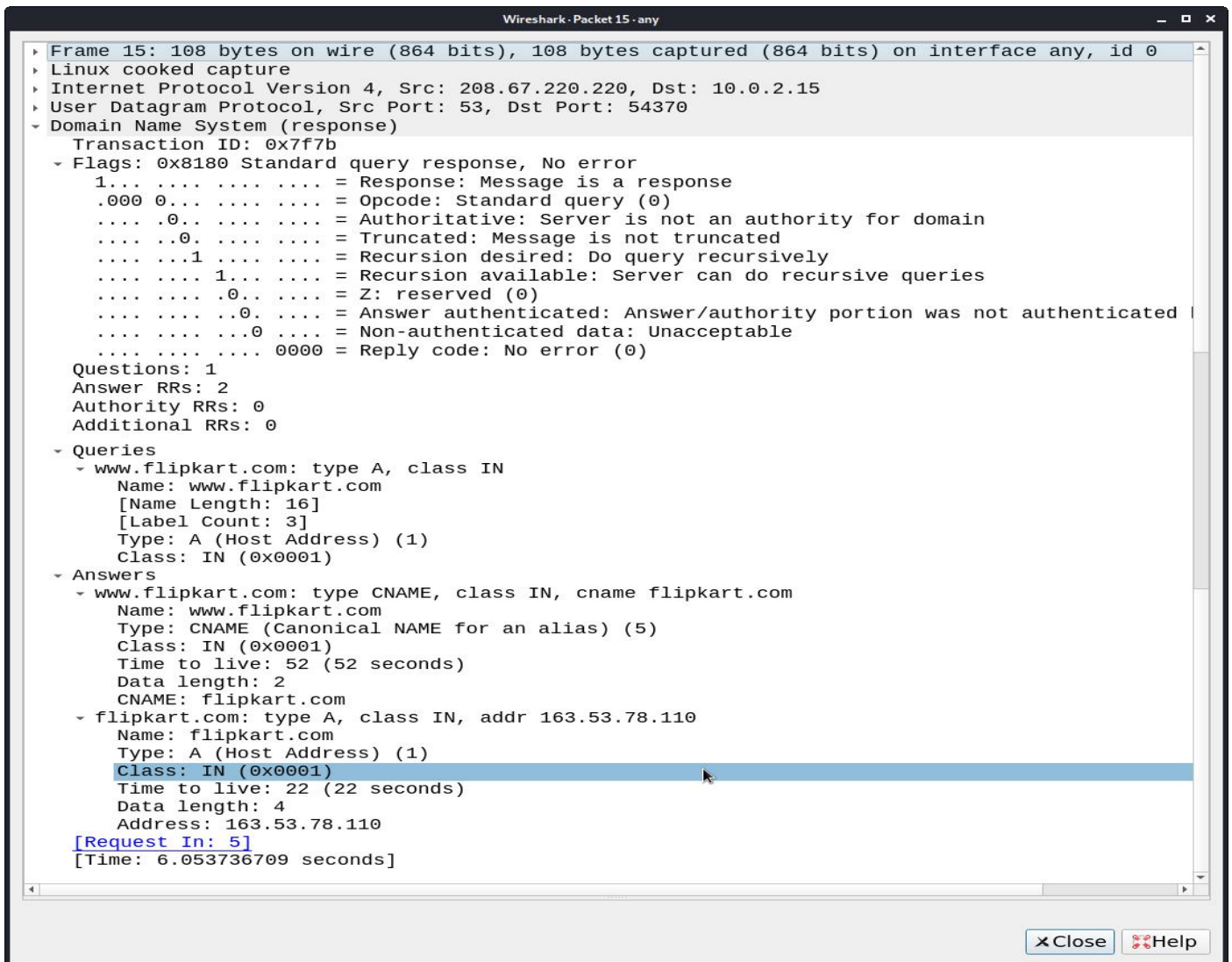
## Wireshark Packet Capture

- The client tries to obtain the DNS record from 10.0.2.8

Wireshark - Packet 1 - any	
<p>Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0</p> <p>Linux cooked capture</p> <p>Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.8</p> <p>User Datagram Protocol, Src Port: 49378, Dst Port: 53</p> <p>Domain Name System (query)</p> <p>Transaction ID: 0x7f7b</p> <p>Flags: 0x0100 Standard query</p> <p>0... .. = Response: Message is a query</p> <p>.000 0... .. = Opcode: Standard query (0)</p> <p>... .. = Truncated: Message is not truncated</p> <p>... ..1... .. = Recursion desired: Do query recursively</p> <p>... ..0... .. = Z: reserved (0)</p> <p>... ..0... .. = Non-authenticated data: Unacceptable</p> <p>Questions: 1</p> <p>Answer RRs: 0</p> <p>Authority RRs: 0</p> <p>Additional RRs: 0</p> <p>Queries</p> <p>www.flipkart.com: type A, class IN</p> <p>Name: www.flipkart.com</p> <p>[Name Length: 16]</p> <p>[Label Count: 3]</p> <p>Type: A (Host Address) (1)</p> <p>Class: IN (0x0001)</p>	
<p>Close Help</p>	

## DNS Standard Query

Hence client received the response from the IP 208.67.220.220.



DNS Standard Query Response

## Task 2: Set Up a Local DNS Server

- The bind9 server is used as the DNS server on the server machine. It is installed using

`sudo apt install bind9.`

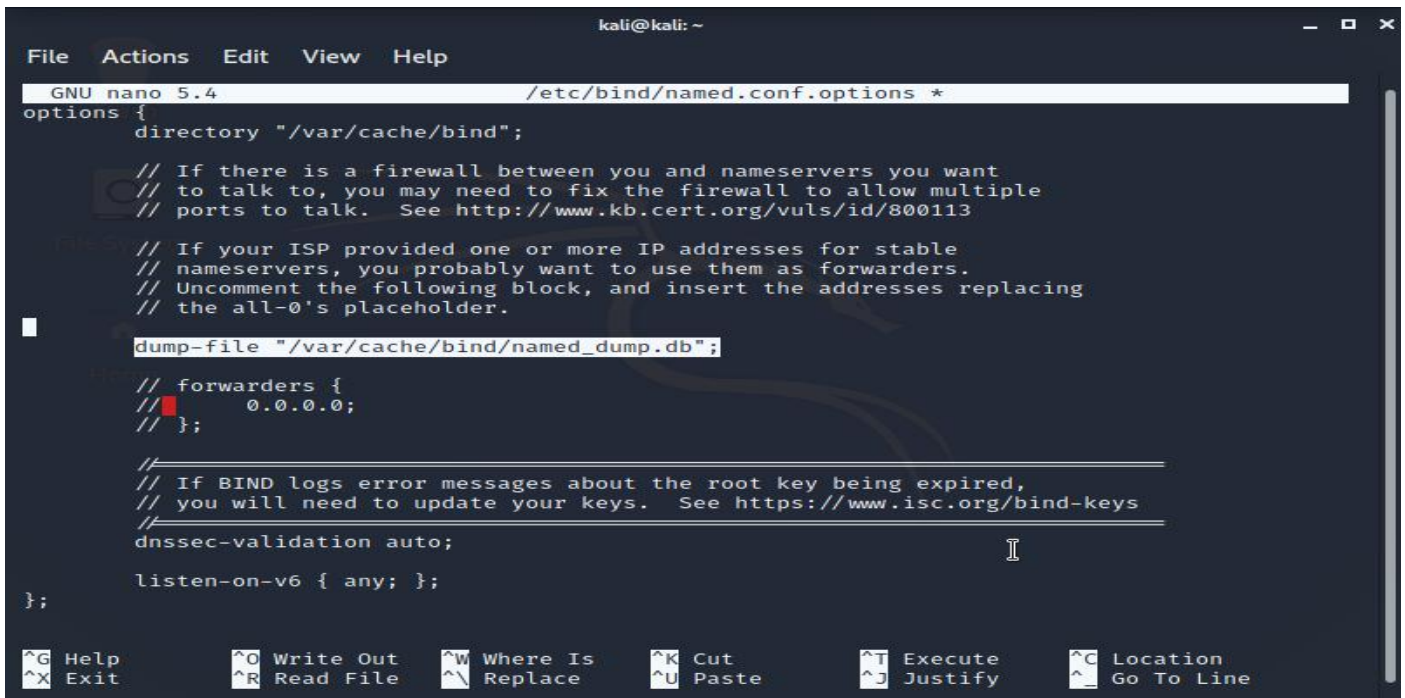
### Step 1: Configure the BIND9 Server

- 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**
- 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



- BIND dumps the cache to a default file called `/var/cache/bind/named_dump.db`



```

GNU nano 5.4 /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/named_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; };
};
  
```

## Step 2: Start DNS server

We start the DNS server using the command:

```
$ sudo service bind9 restart
```

Incase of the Kali Linux OS

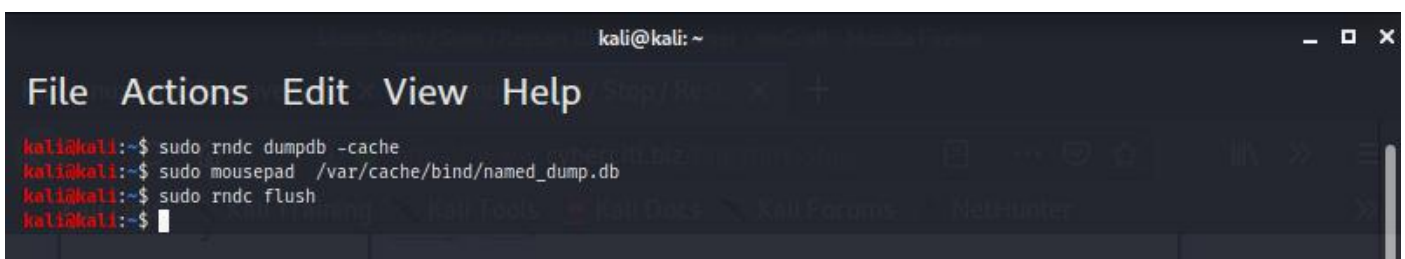
```
$sudo service named restart
```



```

kali@kali: ~
File Actions Edit View Help
kali@kali:~$ sudo nano /etc/bind/named.conf.options
kali@kali:~$ service named restart
kali@kali:~$
  
```

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



```

kali@kali: ~
File Actions Edit View Help
kali@kali:~$ sudo rndc dumpdb -cache
kali@kali:~$ sudo mousepad /var/cache/bind/named_dump.db
kali@kali:~$ sudo rndc flush
kali@kali:~$
  
```

```

/var/cache/bind/named_dump.db - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
;
; Start view _default
;
; Cache dump of view '_default' (cache _default)
; using a 43200 second stale ttl
$DATE 20210219050132
; secure
.
      561247 IN NS      a.root-servers.net.
      561247 IN NS      b.root-servers.net.
      561247 IN NS      c.root-servers.net.
      561247 IN NS      d.root-servers.net.
      561247 IN NS      e.root-servers.net.
      561247 IN NS      f.root-servers.net.
      561247 IN NS      g.root-servers.net.
      561247 IN NS      h.root-servers.net.
      561247 IN NS      i.root-servers.net.
      561247 IN NS      j.root-servers.net.
      561247 IN NS      k.root-servers.net.
      561247 IN NS      l.root-servers.net.
      561247 IN NS      m.root-servers.net.
; secure
      561247 RRSIG      NS 8 0 518400 (
                          20210304050000 20210219040000 42351 .
                          X0e4ITrSZueR1BY0DTDxj0IfJQ0gHpp8XSjp
                          vLYINhxxvQRuGI8FMQfO/TidNBm+XCxG2W3+

```

cache dump file

## Third Test:

- The Flipkart website is pinged again with Wireshark running in the background.

```

File Actions Edit View Help
kali@kali:~$ ping www.flipkart.com
PING flipkart.com (163.53.78.110) 56(84) bytes of data.
 64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=1 ttl=50 time=91.8 ms
 64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=2 ttl=50 time=319 ms
 64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=3 ttl=50 time=87.6 ms
^C
--- flipkart.com ping statistics ---
 3 packets transmitted, 3 received, 0% packet loss, time 9322ms
 rtt min/avg/max/mdev = 87.622/166.291/319.435/108.302 ms
kali@kali:~$

```

- The IP Address of the local DNS server is 10.0.2.8.

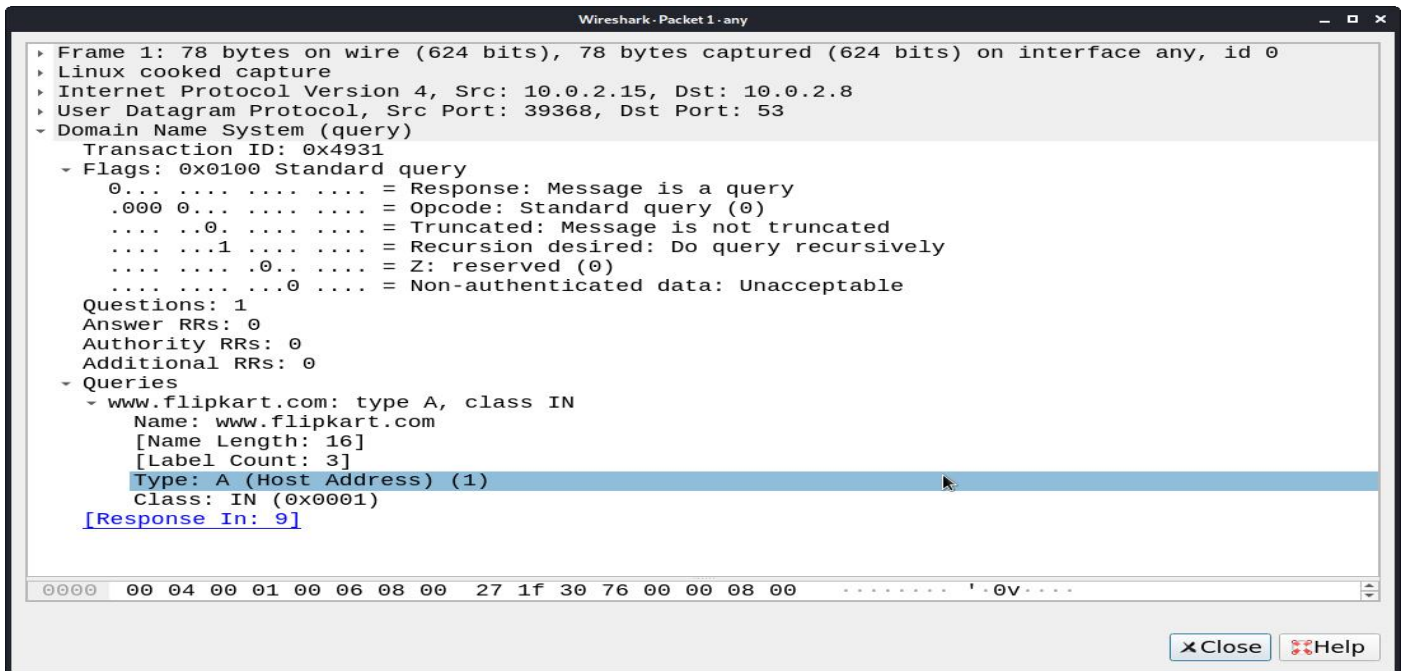
Wireshark packet capture analysis showing DNS traffic. The packet list table is as follows:

No.	Time	Source	Destination	Proto	Length	Info
1	0.000000000	10.0.2.15	10.0.2.8	DNS	78	Standard query 0x4931 A www.flipkart.com
2	0.000110430	10.0.2.15	10.0.2.8	DNS	78	Standard query 0x6036 AAAA www.flipkart.com
3	0.008076841	10.0.2.15	208.67.220.220	DNS	78	Standard query 0x4931 A www.flipkart.com
4	0.008125791	10.0.2.15	208.67.220.220	DNS	78	Standard query 0x6036 AAAA www.flipkart.com
6	0.01997171	208.67.220.220	10.0.2.15	DNS	108	Standard query response 0x4931 A www.flipkart.com CNAME flip
8	0.03857383	10.0.2.8	10.0.2.15	DNS	155	Standard query response 0x6036 AAAA www.flipkart.com CNAME f
9	0.070962092	10.0.2.8	10.0.2.15	DNS	108	Standard query response 0x4931 A www.flipkart.com CNAME flip
10	8.833857383	10.0.2.15	208.67.220.220	DNS	78	Standard query 0x4931 A www.flipkart.com
11	8.162012564	208.67.220.220	10.0.2.15	DNS	108	Standard query response 0x4931 A www.flipkart.com CNAME flip
12	8.162172391	10.0.2.15	208.67.220.220	DNS	78	Standard query 0x6036 AAAA www.flipkart.com
13	8.283012937	208.67.220.220	10.0.2.15	DNS	155	Standard query response 0x6036 AAAA www.flipkart.com CNAME f
16	8.375844580	10.0.2.15	10.0.2.8	DNS	88	Standard query 0x44a2 PTR 110.78.53.163.in-addr.arpa
21	13.473258892	10.0.2.15	208.67.220.220	DNS	88	Standard query 0x44a2 PTR 110.78.53.163.in-addr.arpa
22	13.835921340	208.67.220.220	10.0.2.15	DNS	176	Standard query response 0x44a2 No such name PTR 110.78.53.16
25	14.156056946	10.0.2.15	10.0.2.8	DNS	88	Standard query 0x23b2 PTR 110.78.53.163.in-addr.arpa
26	17.498978807	10.0.2.8	10.0.2.15	DNS	88	Standard query response 0x23b2 Server failure PTR 110.78.53.
27	17.499217524	10.0.2.15	208.67.220.220	DNS	88	Standard query 0x23b2 PTR 110.78.53.163.in-addr.arpa
28	17.499909643	10.0.2.8	10.0.2.15	DNS	88	Standard query response 0x44a2 Server failure PTR 110.78.53.

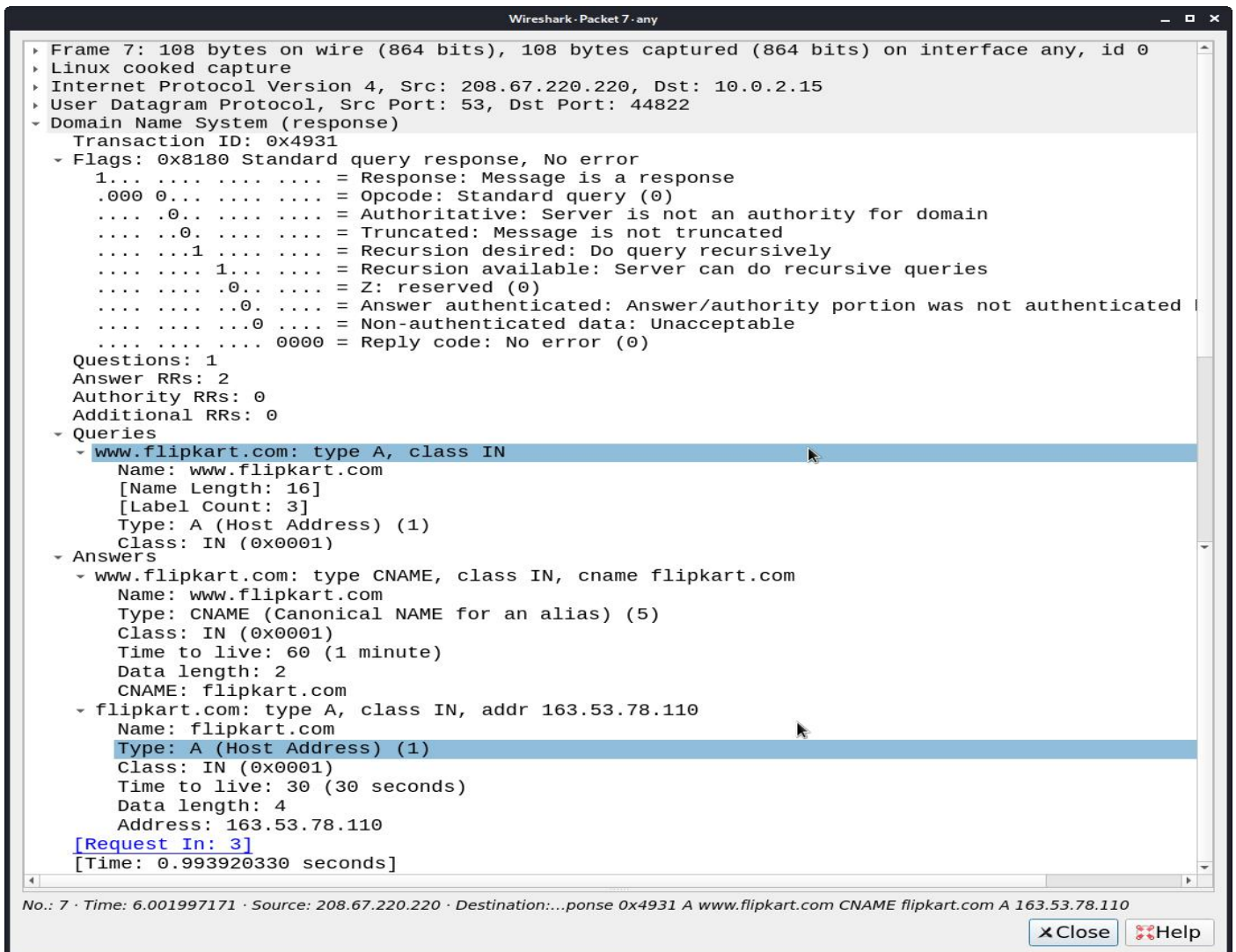
Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0  
Linux cooked capture  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.8  
User Datagram Protocol, Src Port: 39368, Dst Port: 53  
Domain Name System (query)  
0000 00 04 00 01 00 06 00 27 1f 30 76 00 00 08 00 .....V....  
0010 45 00 00 3e eb 8d 40 00 40 11 37 0b 0a 00 02 0f E..>..@. @.7....  
Domain Name System: Protocol  
Packets: 36 · Displayed: 24 (66.7%) Profile: Default



## Wireshark Packet Capture



## DNS Standard Query



## DNS Standard Query response

```

/var/cache/bind/named_dump.db - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
; glue
flipkart.com.      215946  NS      sdns14.ultradns.biz.
                  215946  NS      sdns14.ultradns.com.
                  215946  NS      sdns14.ultradns.net.
                  215946  NS      sdns14.ultradns.org.
; answer
                  43207   \-AAAA  ;-$NXRRSET
; flipkart.com. SOA PDNS1.ULTRADNS.NET. sysadmin.flipkart.com. 2017031521 10800 3600 604800 60
; secure
                  44047   \-DS      ;-$NXRRSET
; com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1613755248 1800 900 604800 86400
; com. RRSIG SOA ...
; 9DA2HK6CJ3BHAHTF53KBTGK69URBEOM.com. RRSIG NSEC3 ...
; 9DA2HK6CJ3BHAHTF53KBTGK69URBEOM.com. NSEC3 1 1 0 - 9DA300H08G0P0F757L9LQ1LE8C29PS5A NS DS RRSIG
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. RRSIG NSEC3 ...
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. NSEC3 1 1 0 - CK0Q1GIN43N1ARRC90S16QPQR81H5M9A NS SOA RRSIG
; answer
                  43177   A         163.53.78.110
; answer
www.flipkart.com.  43207   CNAME   flipkart.com.
; glue
sdns14.ultradns.com. 215946  A       156.154.140.14

```

Cache Dumpfile (flipkart.com)

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

### Step 1: Create Zones

- We had two zone entries in the DNS server by adding the following contents to `/etc/bind/named.conf`
- The two zones corresponding to the domain **www.example.com** must be added to `/etc/bind/named.conf`
- The first zone is for forward lookup (from hostname to IP), and the second zone is for reverse lookup (from IP to hostname).

```

kali@kali: ~
File Actions Edit View Help
GNU nano 5.4 /etc/bind/named.conf *
// 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";
};

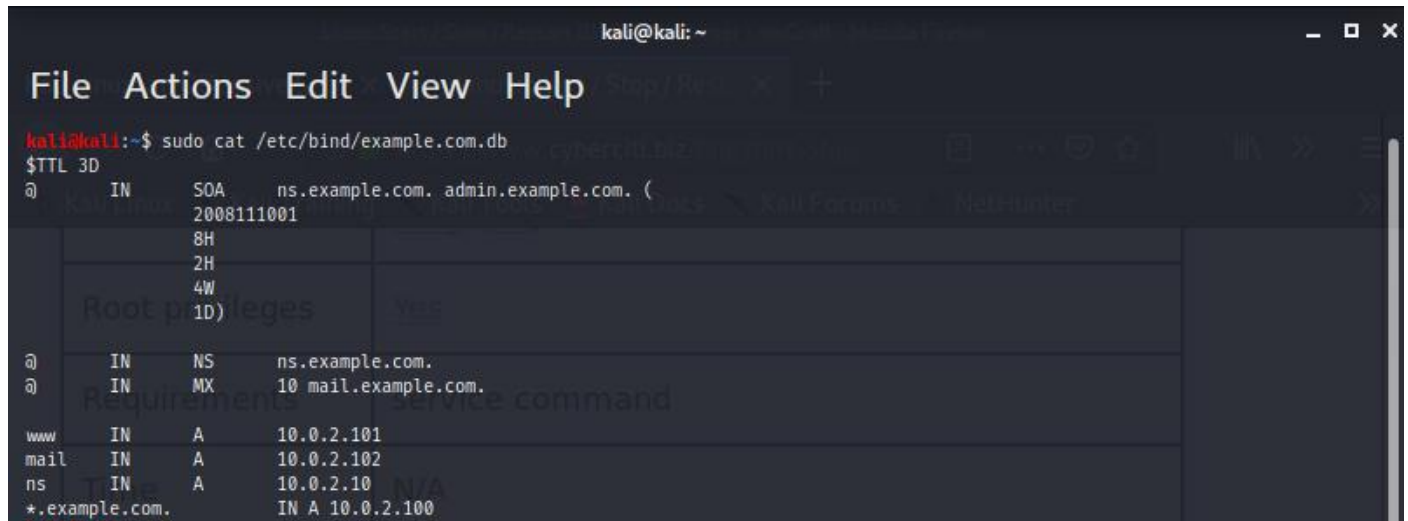
zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/10.0.2.db";
};

```

In above screenshot, 10.0.2.0 is the subnet mask of my IP address

## Step 2: Setup the forward lookup zone file

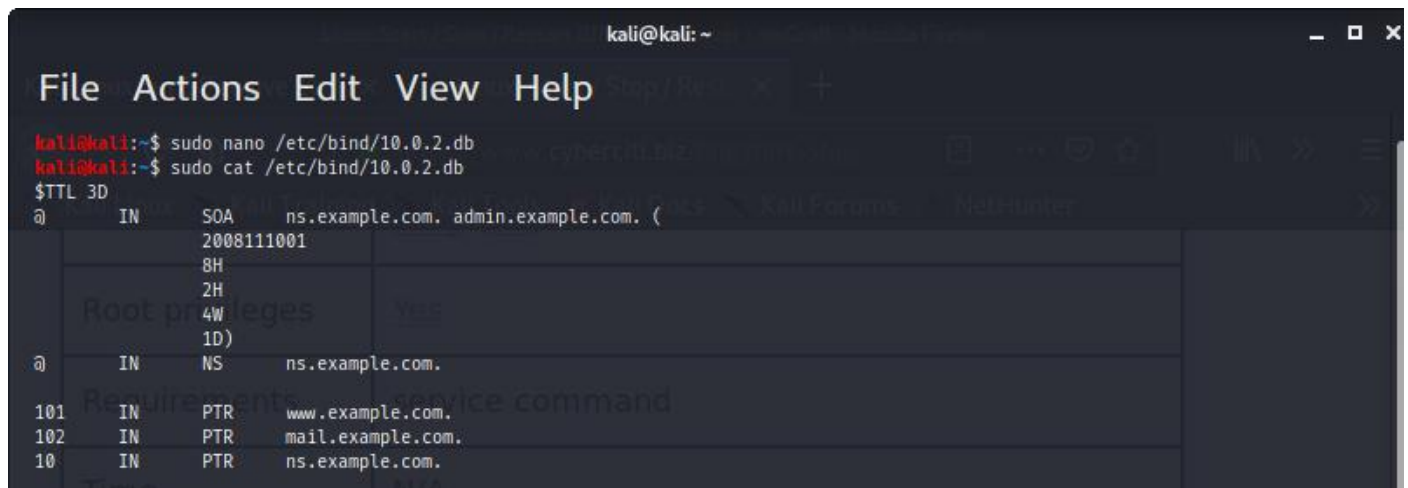
We create **example.com.db** zone file with the following contents in the **/etc/bind/** directory where the actual DNS resolution is stored



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ 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
```

## Step 3: Setup the reverse lookup zone file

We create a reverse DNS lookup file called **10.0.2.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

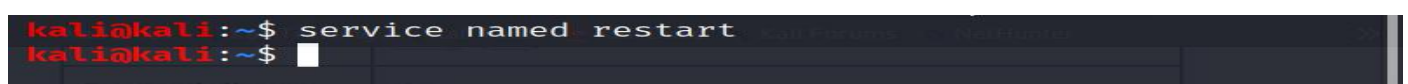


```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ sudo nano /etc/bind/10.0.2.db  
kali@kali:~$ sudo cat /etc/bind/10.0.2.db  
$TTL 3D  
@ IN SOA ns.example.com. admin.example.com. (  
2008111001  
8H  
2H  
4W  
1D)  
@ IN NS ns.example.com.  
101 IN PTR www.example.com.  
102 IN PTR mail.example.com.  
10 IN PTR ns.example.com.
```

## Task 4: Restart the BIND server and test

### Step 1:

Restart bind9 to apply the changes



```
kali@kali:~$ service named restart  
kali@kali:~$
```

### 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



```
kali@kali:~$ dig www.example.com

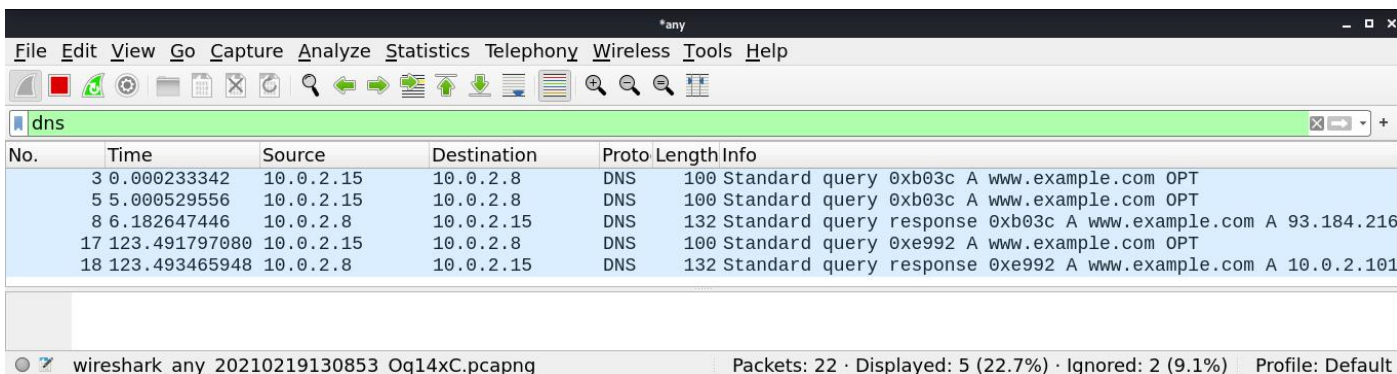
; <<>> DiG 9.11.5-P4-5.1+Debian <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 59794
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 84af7c736905beb901000000602ffff3cab40b551161c5615 (good)
;; QUESTION SECTION:
;www.example.com.                IN      A

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

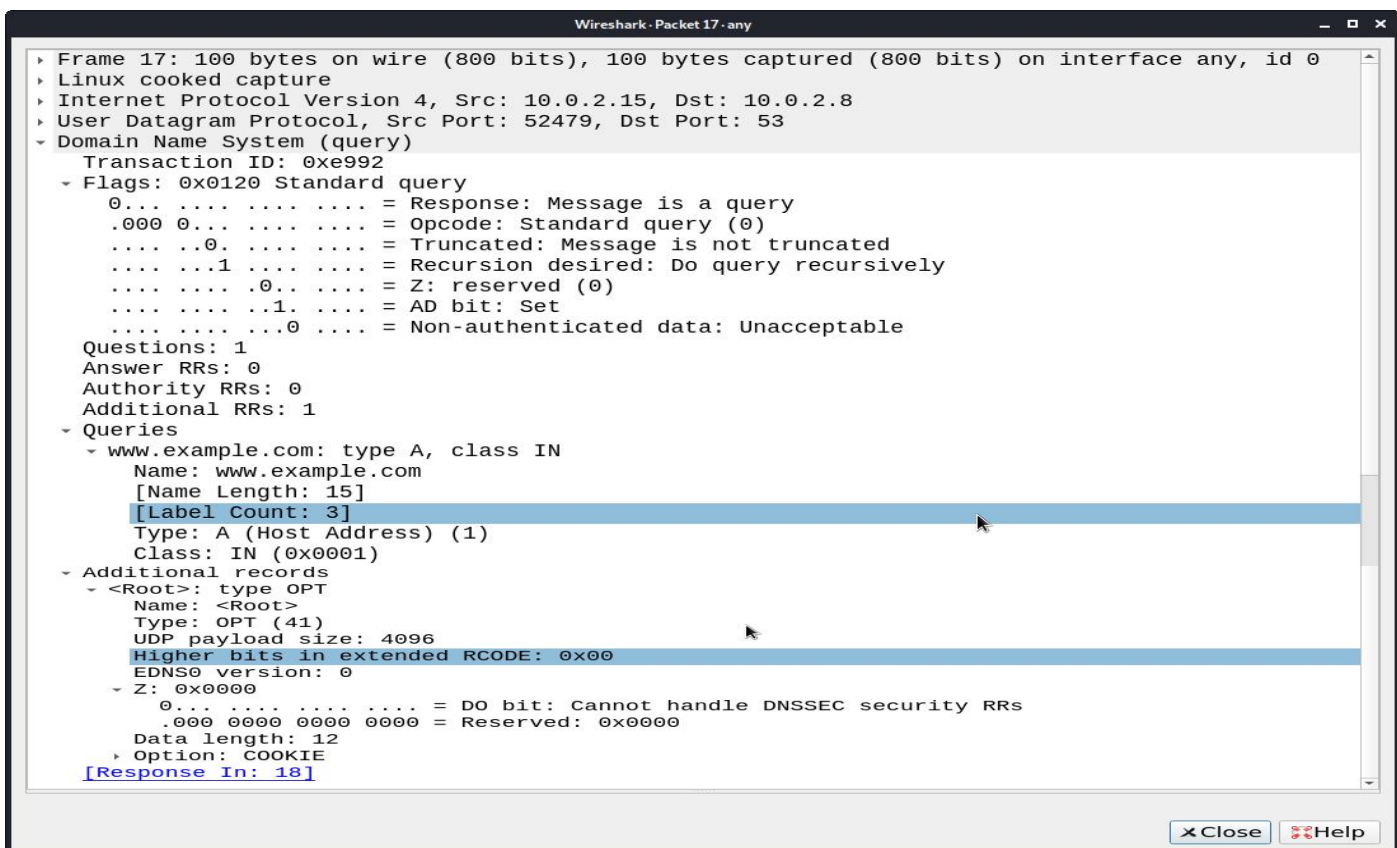
;; Query time: 1 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
;; WHEN: Fri Feb 19 13:11:08 EST 2021
;; MSG SIZE rcvd: 88
```

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



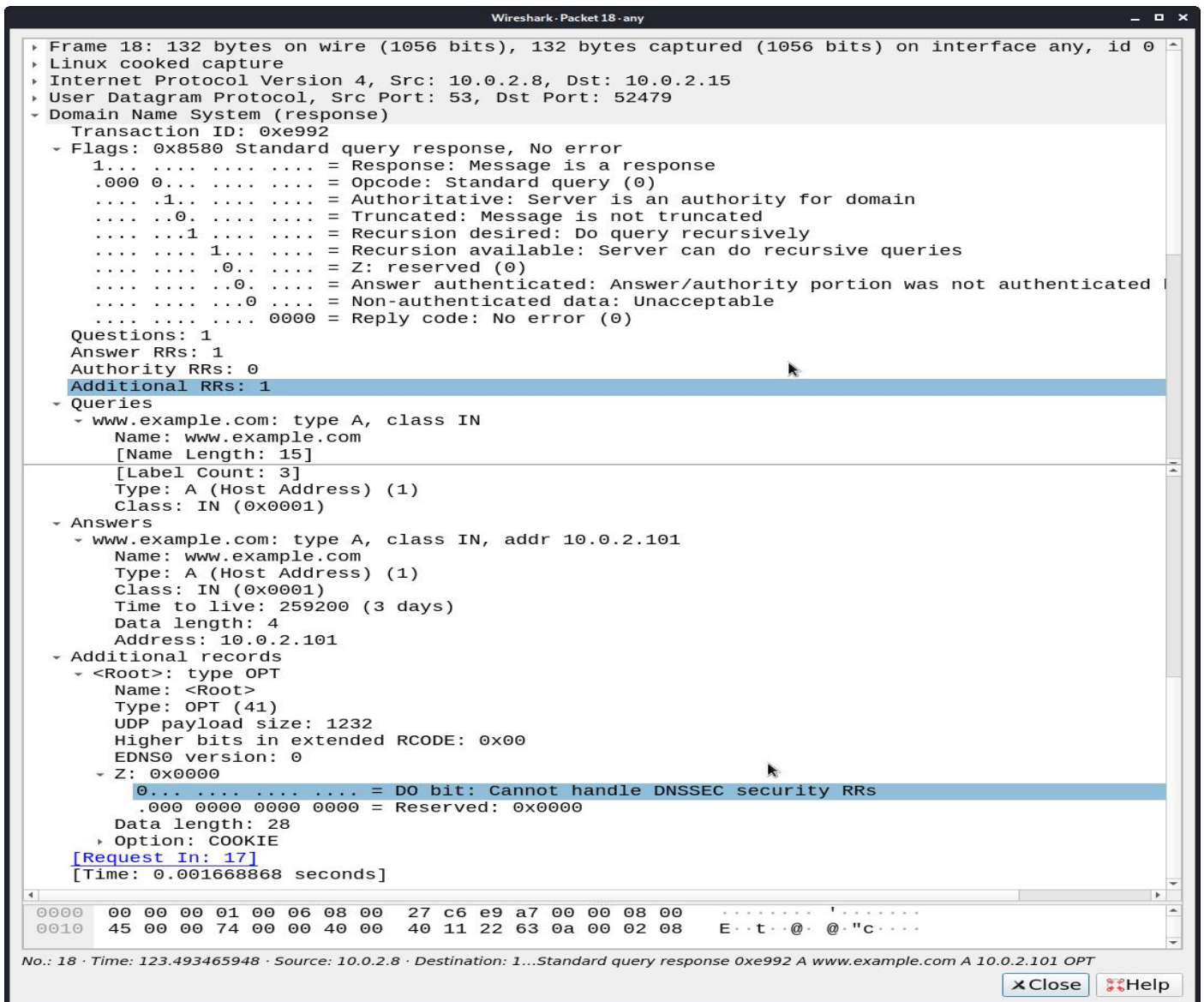
No.	Time	Source	Destination	Proto	Length	Info
3	0.000233342	10.0.2.15	10.0.2.8	DNS	100	Standard query 0xb03c A www.example.com OPT
5	5.000529556	10.0.2.15	10.0.2.8	DNS	100	Standard query 0xb03c A www.example.com OPT
8	6.182647446	10.0.2.8	10.0.2.15	DNS	132	Standard query response 0xb03c A www.example.com A 93.184.216
17	123.491797080	10.0.2.15	10.0.2.8	DNS	100	Standard query 0xe992 A www.example.com OPT
18	123.493465948	10.0.2.8	10.0.2.15	DNS	132	Standard query response 0xe992 A www.example.com A 10.0.2.101

## Wireshark Packet Capture



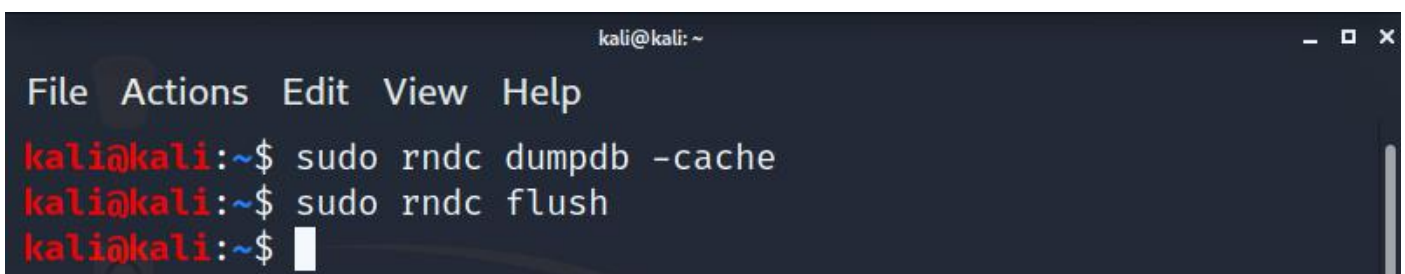
```
Frame 17: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.8
User Datagram Protocol, Src Port: 52479, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0xe992
  Flags: 0x0120 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (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: 12
      Option: COOKIE
      [Response in: 18]
```

## Wireshark Standard Query



## Wireshark Standard Query Response

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



## Observation Questions :

For 'ping **www.flipkart.com**', answer the following questions

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

*ANS :* They are sent over UDP.

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

*ANS :* 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?

*ANS :* The DNS query is made to server at the IP Address 10.0.2.8. 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"?

*ANS :* 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?

*ANS :* 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?

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