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)

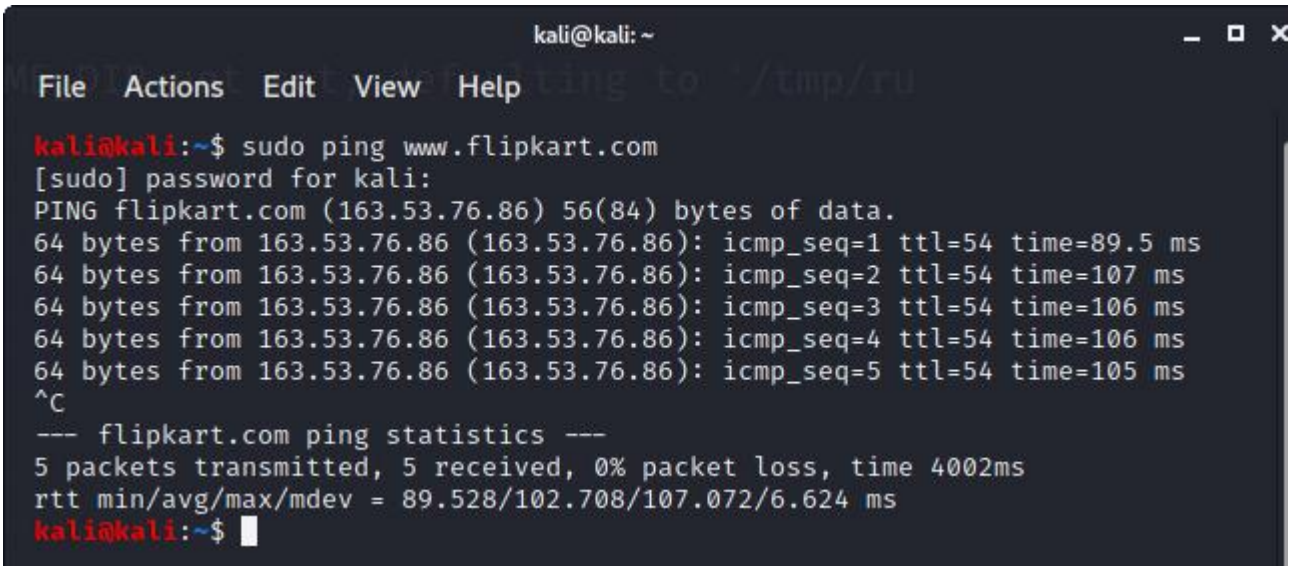
DNS Server: 10.0.2.8 (VM 1)

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

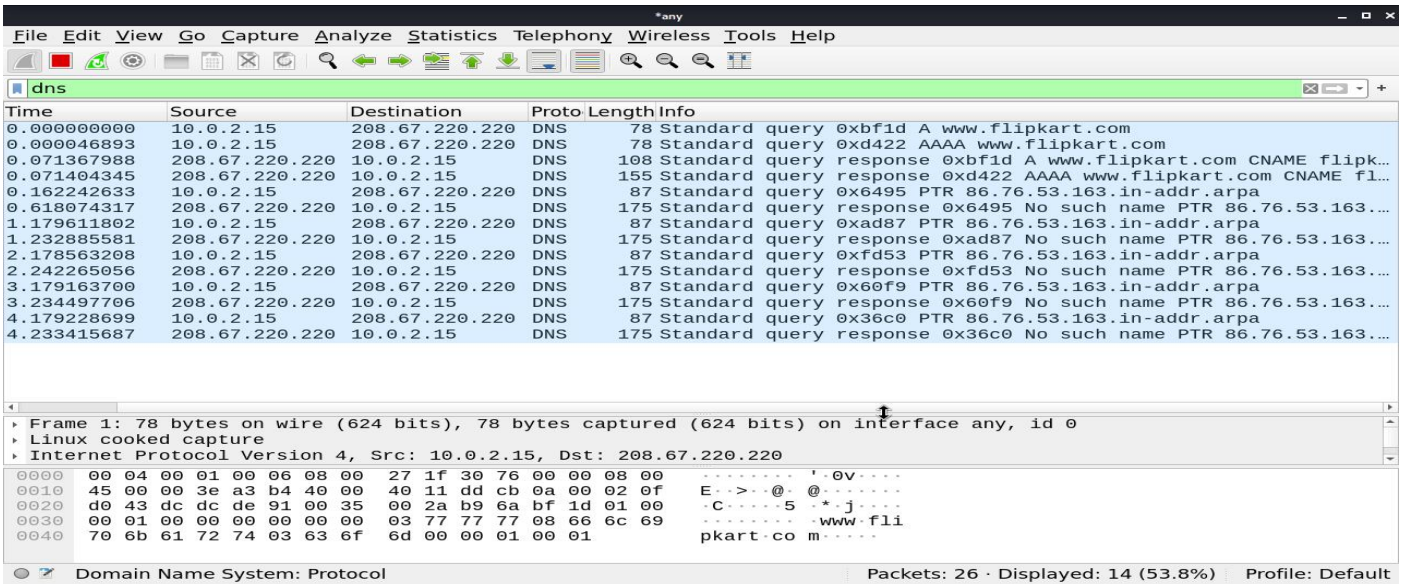
First Test: Pinging using default DNS

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

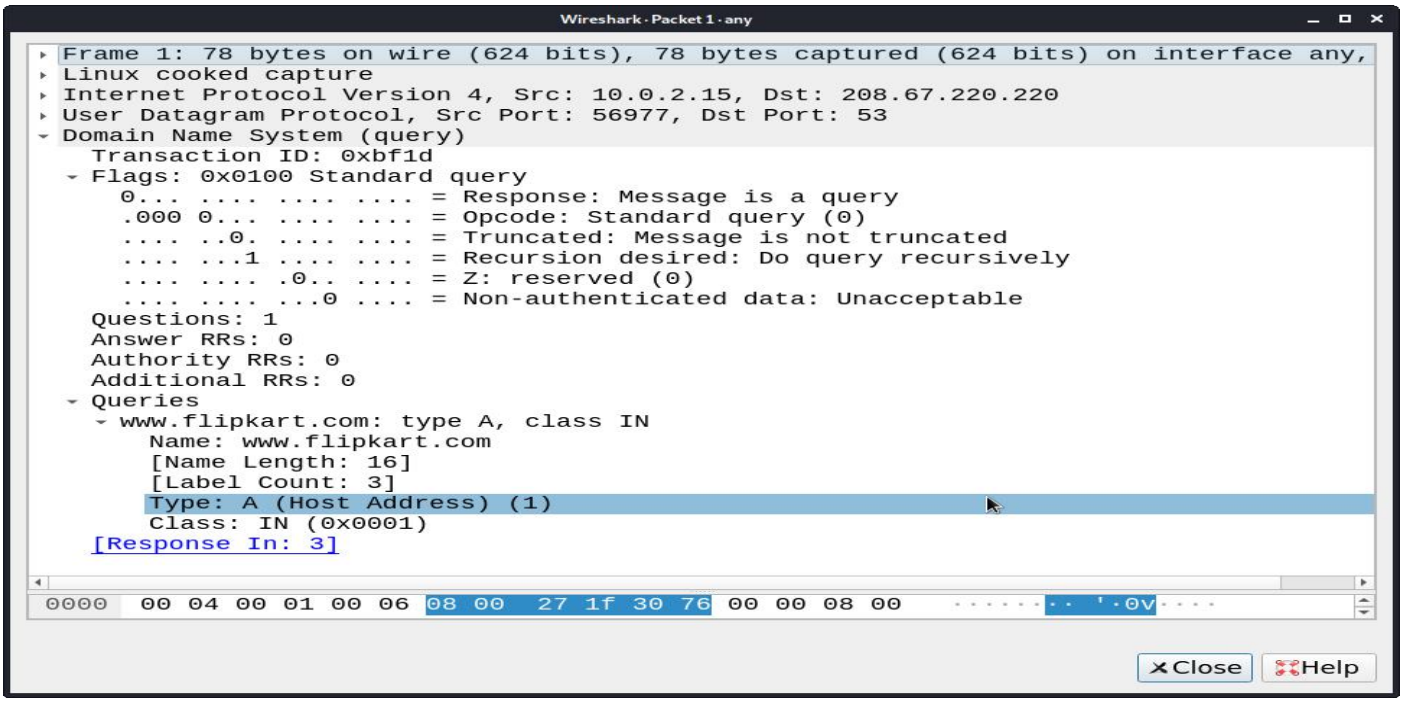
Pinging www.flipkart.com



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

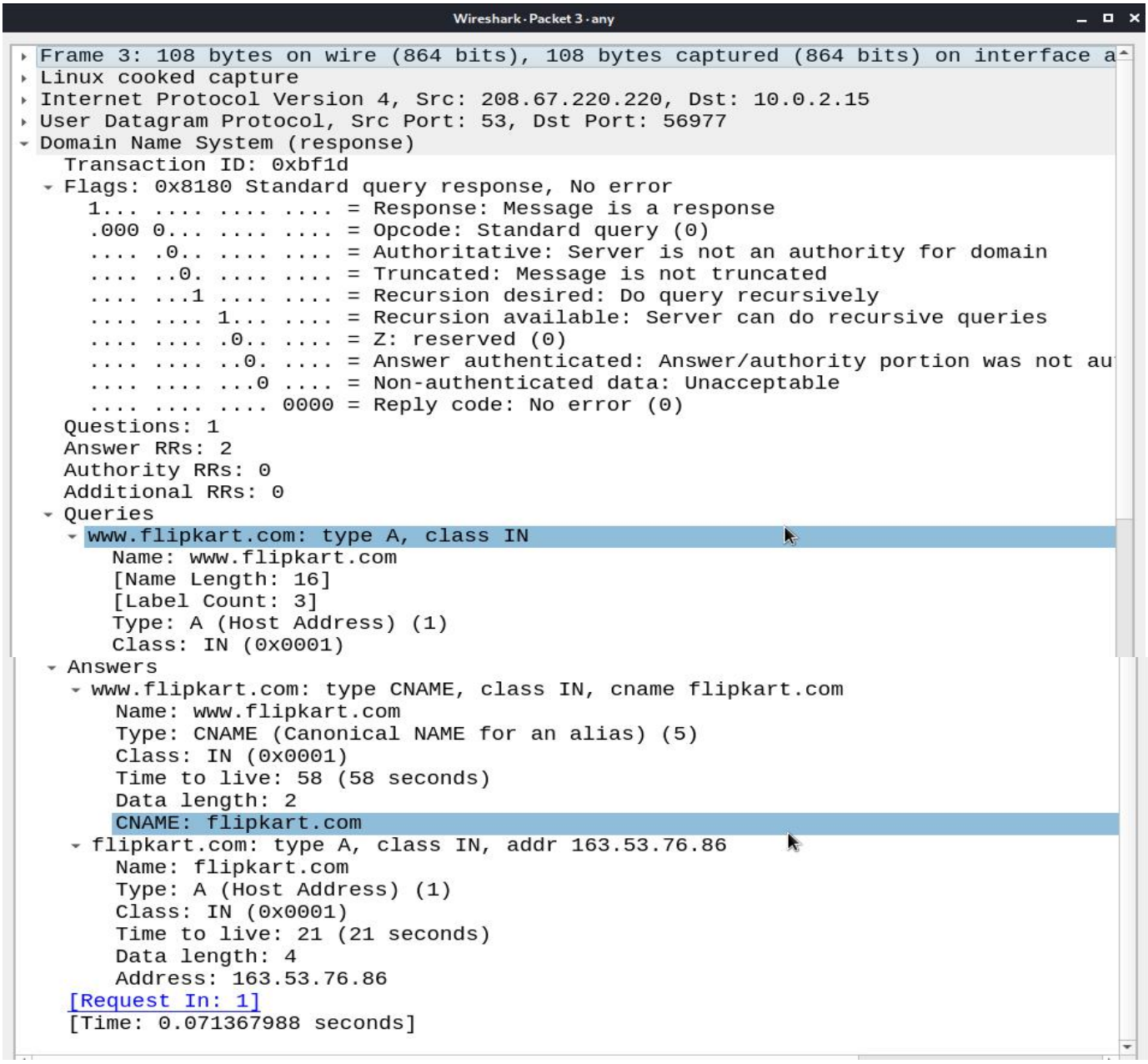


Wireshark Packet Capture



DNS Standard Query

IP address of the website – 163.53.78.110.

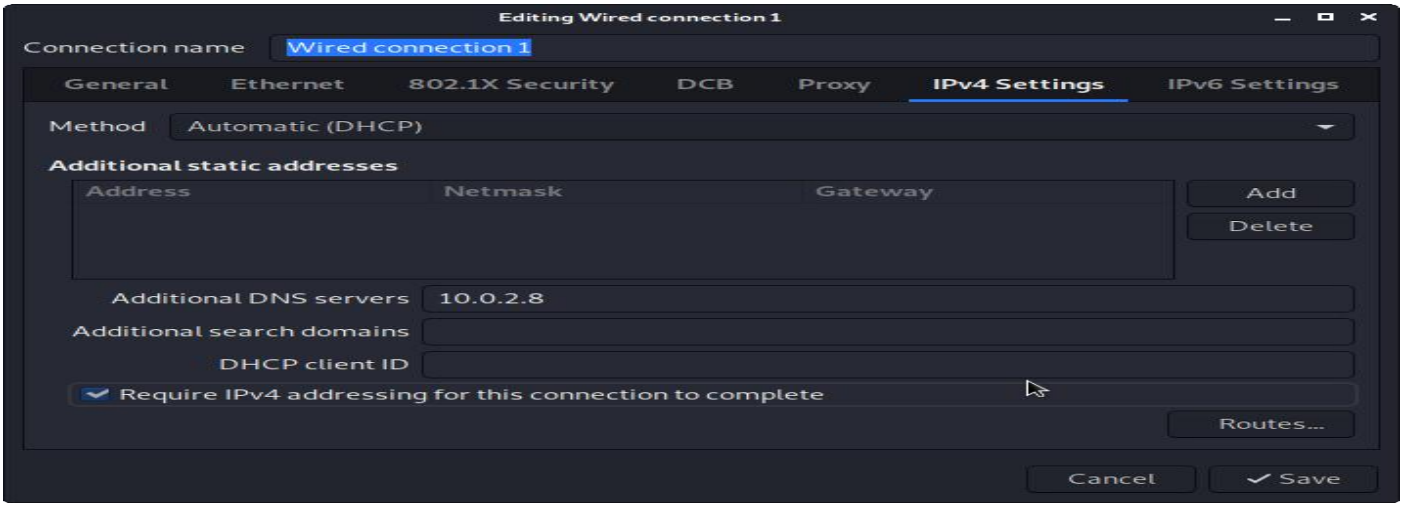


DNS Standard Query Response

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.

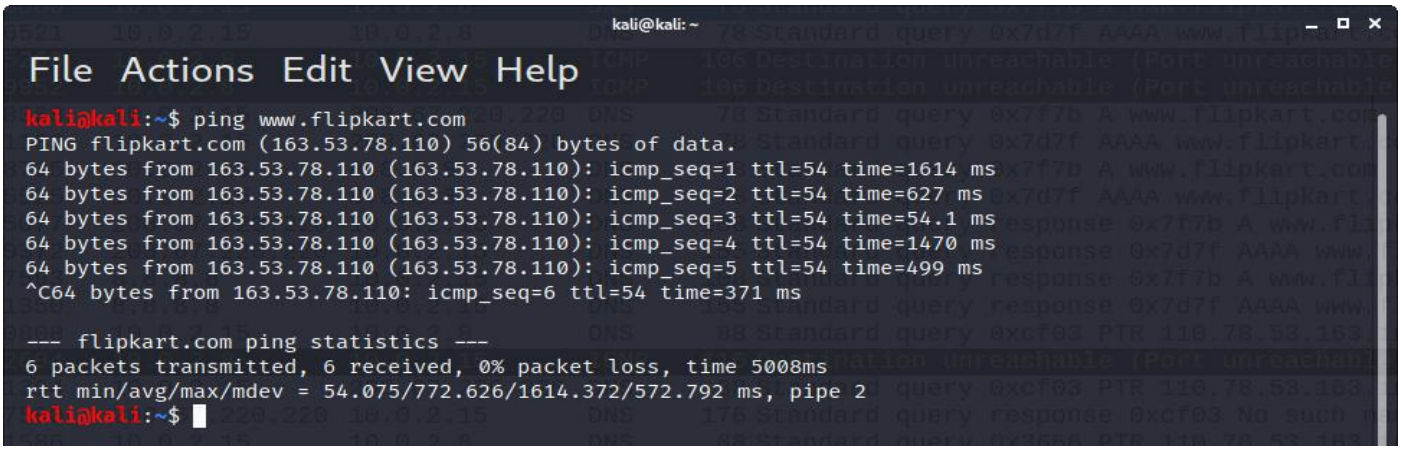
- This ensures that the custom DNS server will be used to resolve names.

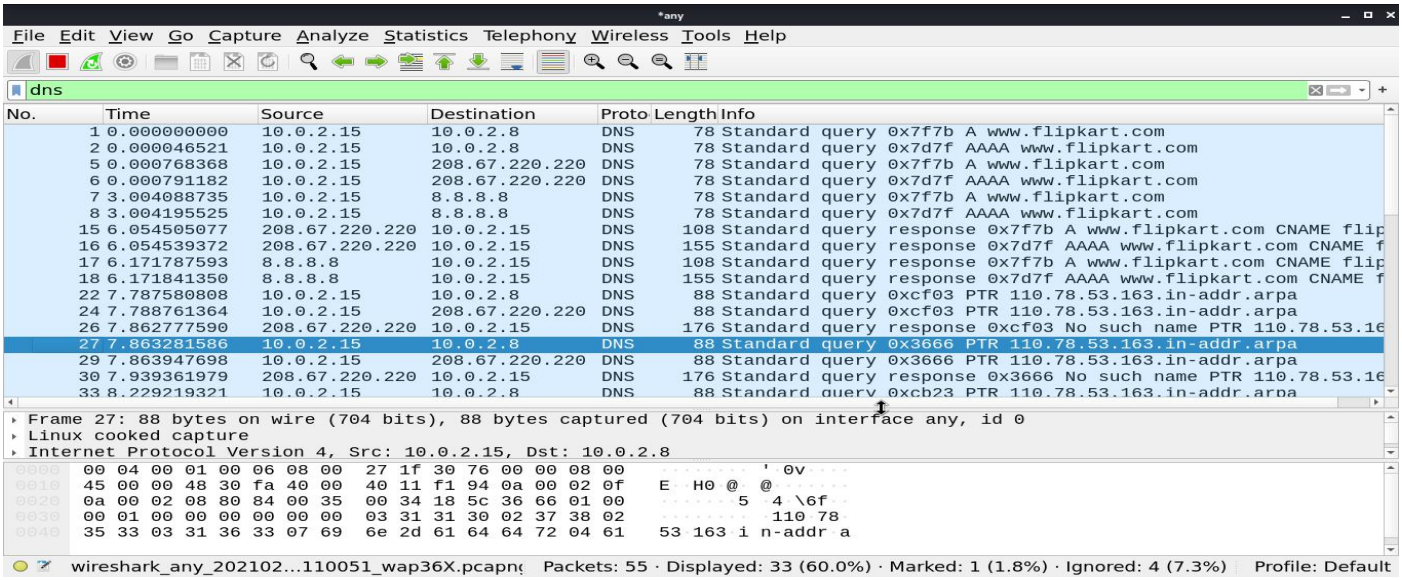
- The changes are applied by using the command sudo resolvconf –u

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).

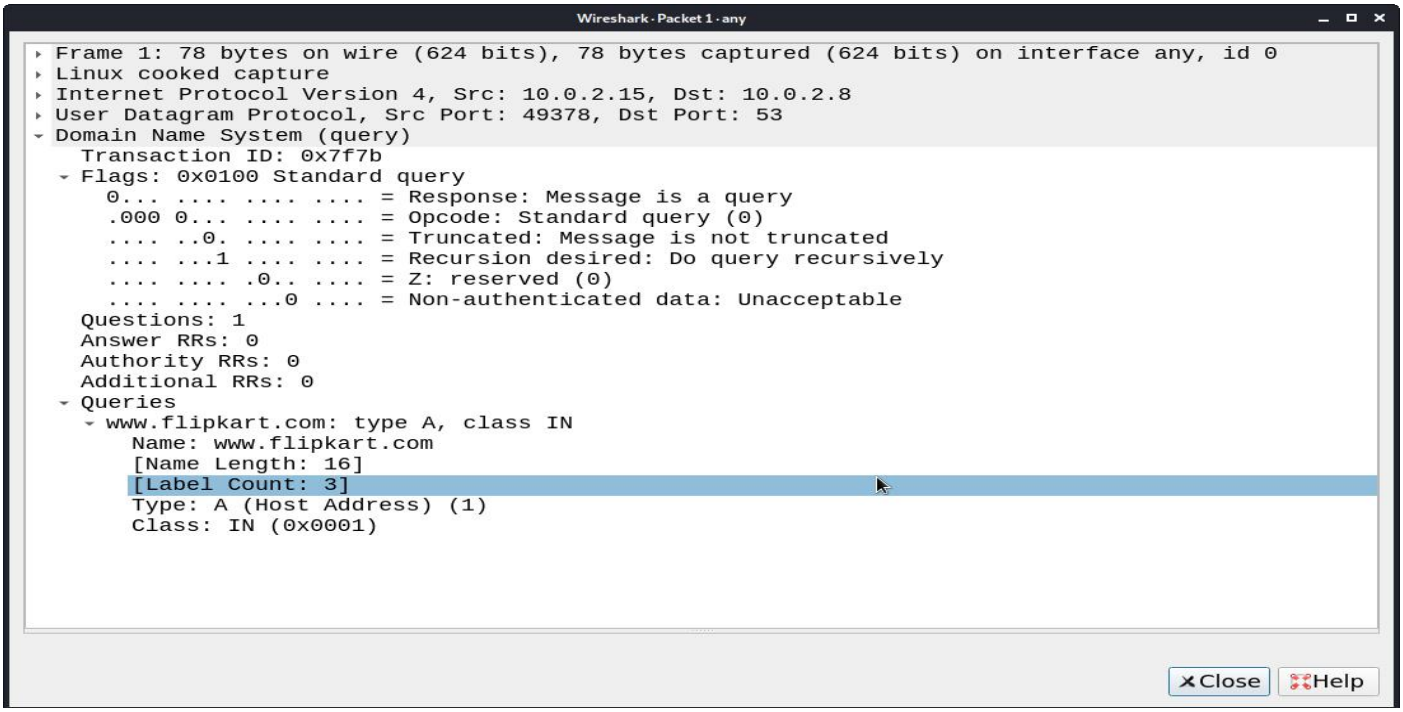
- The Flipkart website is pinged again.





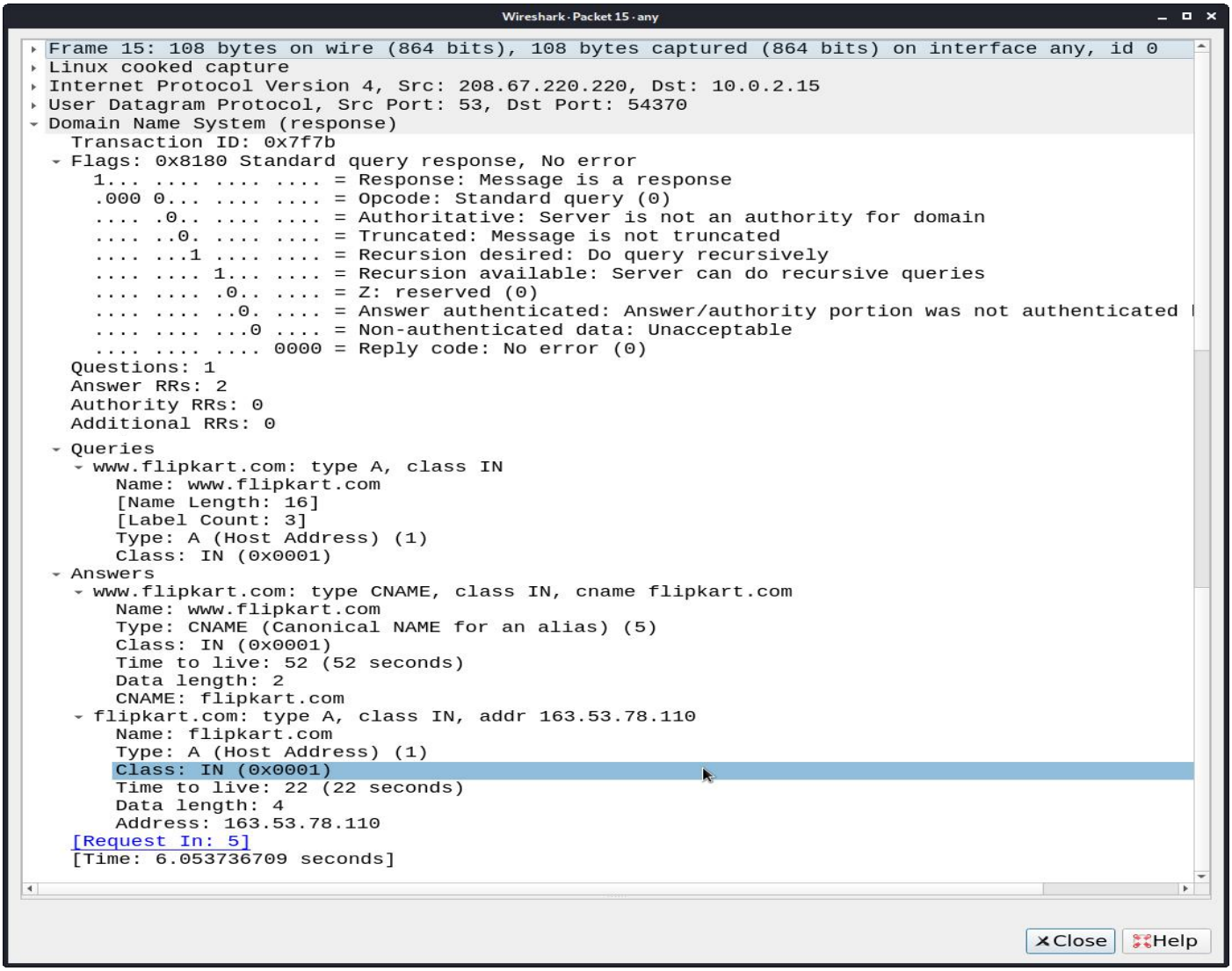
Wireshark Packet Capture

- The client tries to obtain the DNS record from 10.0.2.8



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**

```
kali@kali: ~
File  Actions  Edit  View  Help
  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; };
};

^G Help      ^O Write Out   ^W Where Is    ^K Cut       ^T Execute    ^C Location
^X Exit      ^R Read File   ^\ Replace     ^U Paste     ^J Justify    ^_ Go To Line
```

Step 2: Start DNS server

We start the DNS server using the command:

$ sudo service bind9 restart

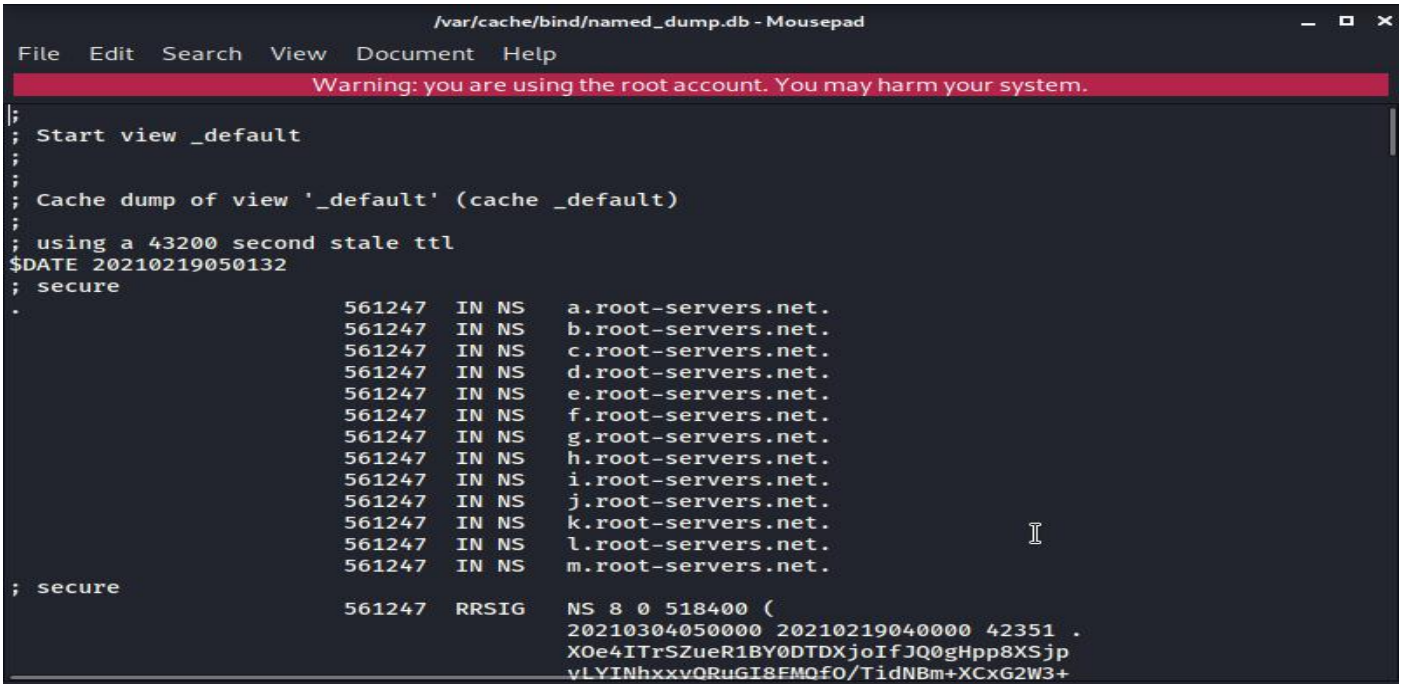
Incase of the Kali Linux OS

$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**.

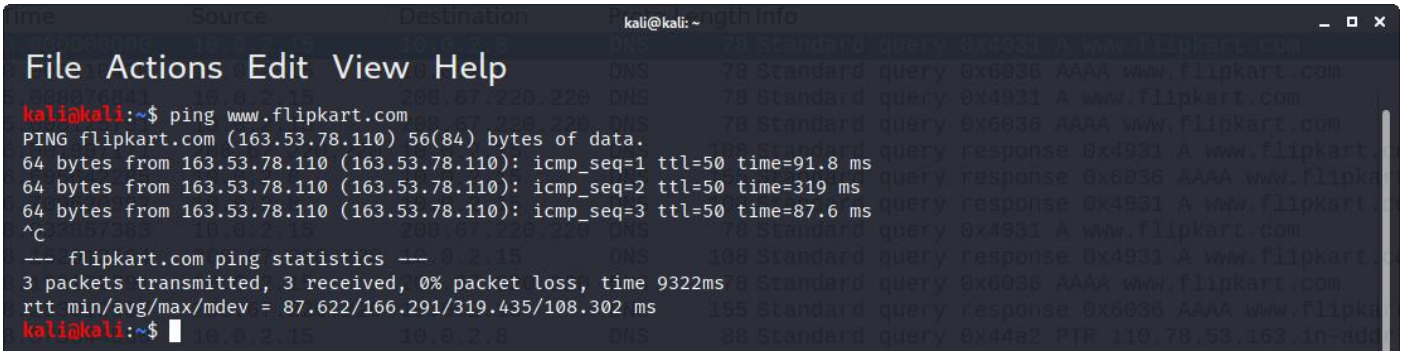
```
kali@kali: ~
File  Actions  Edit  View  Help
kali@kali:~$ sudo rndc dumpdb -cache
kali@kali:~$ sudo mousepad  /var/cache/bind/named_dump.db
kali@kali:~$ sudo rndc flush
kali@kali:~$
```



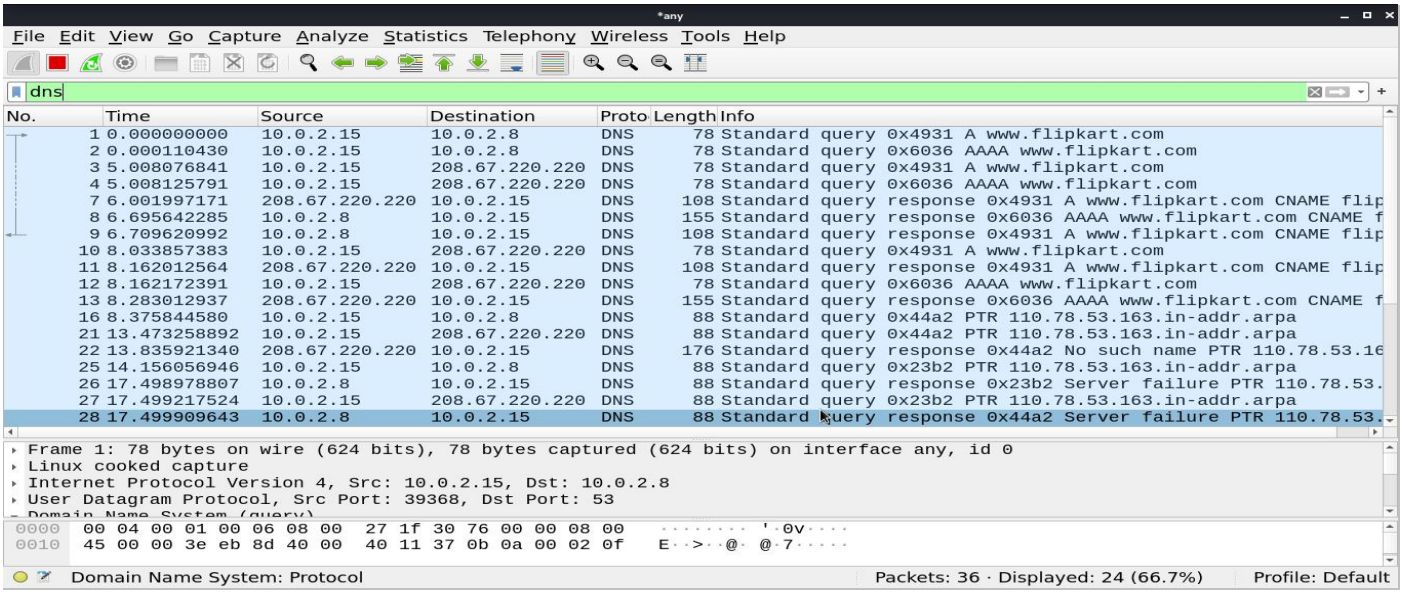
cache dump file

Third Test:

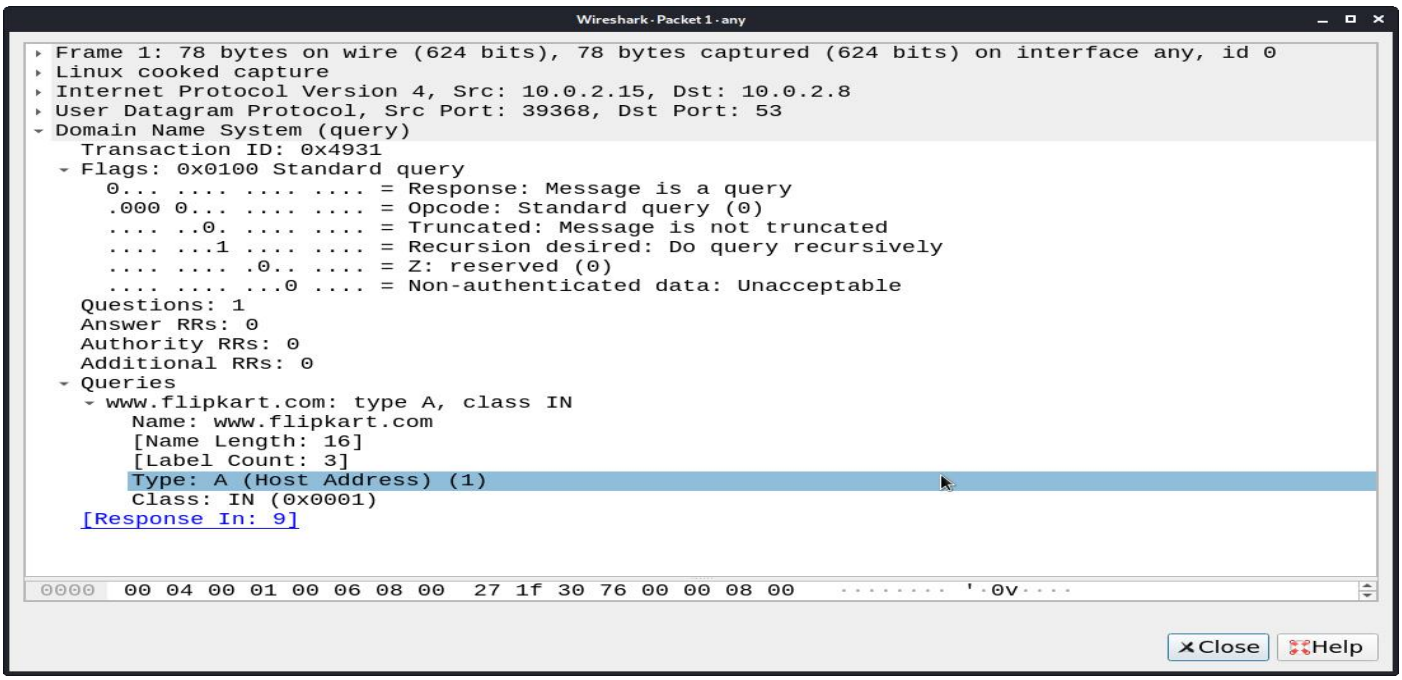
- The Flipkart website is pinged again with Wireshark running in the background.



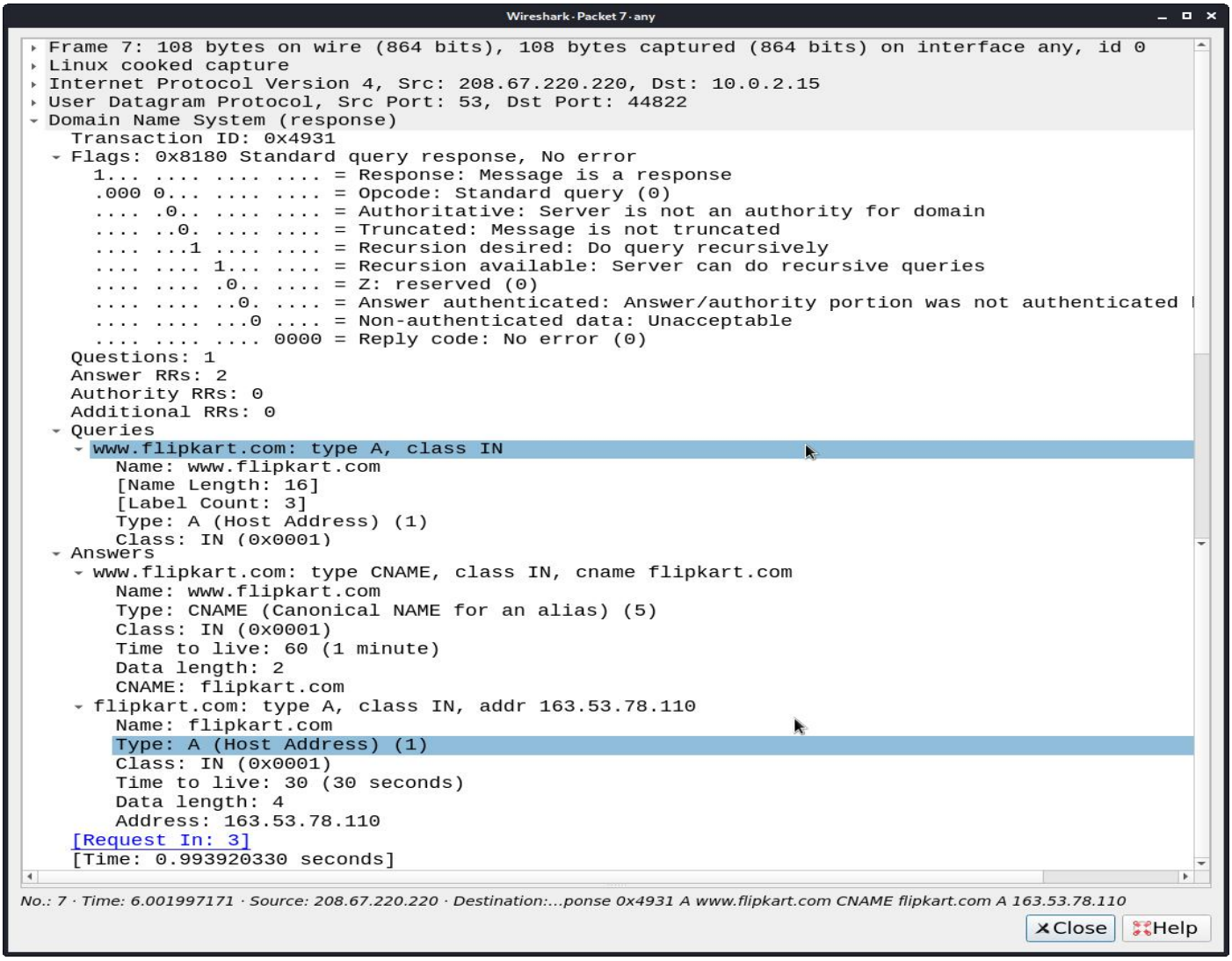
- The IP Address of the local DNS server is 10.0.2.8.



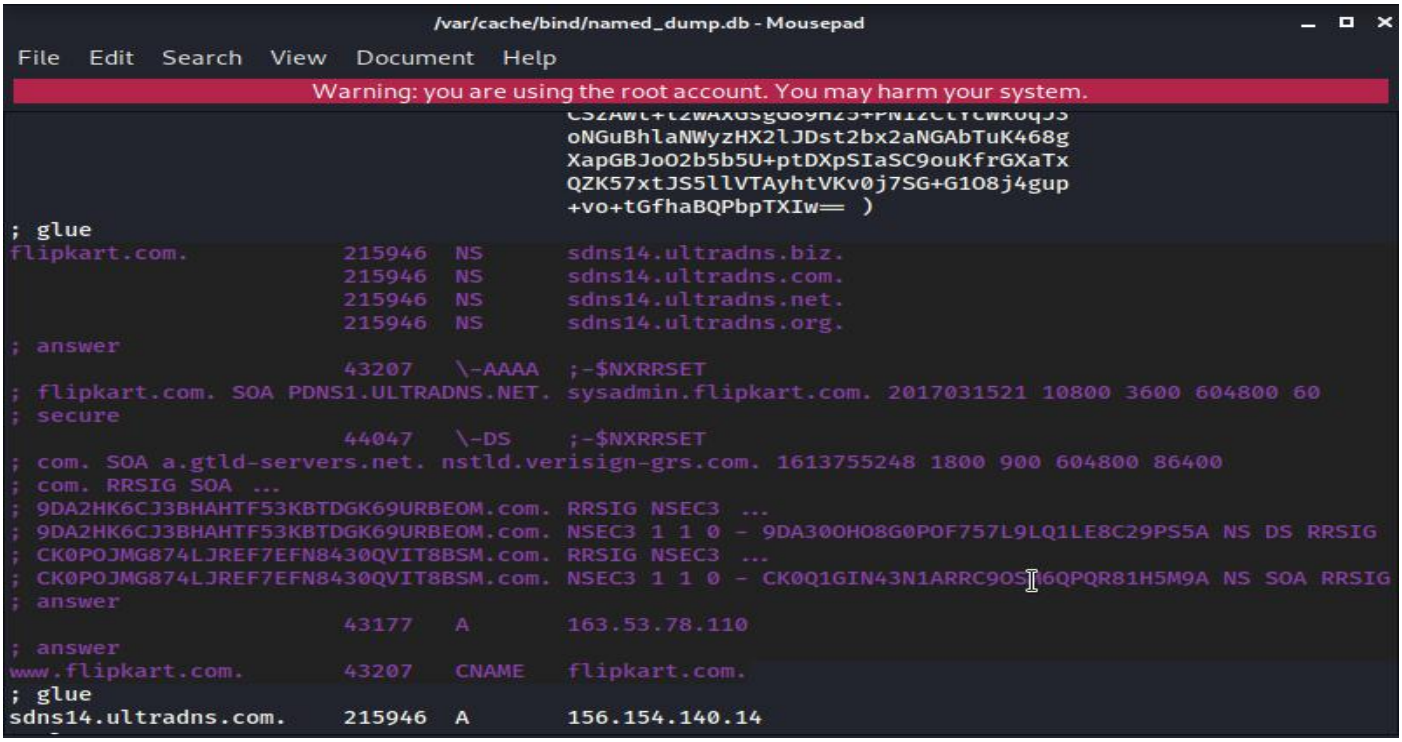
Wireshark Packet Capture



DNS Standard Query



DNS Standard Query response

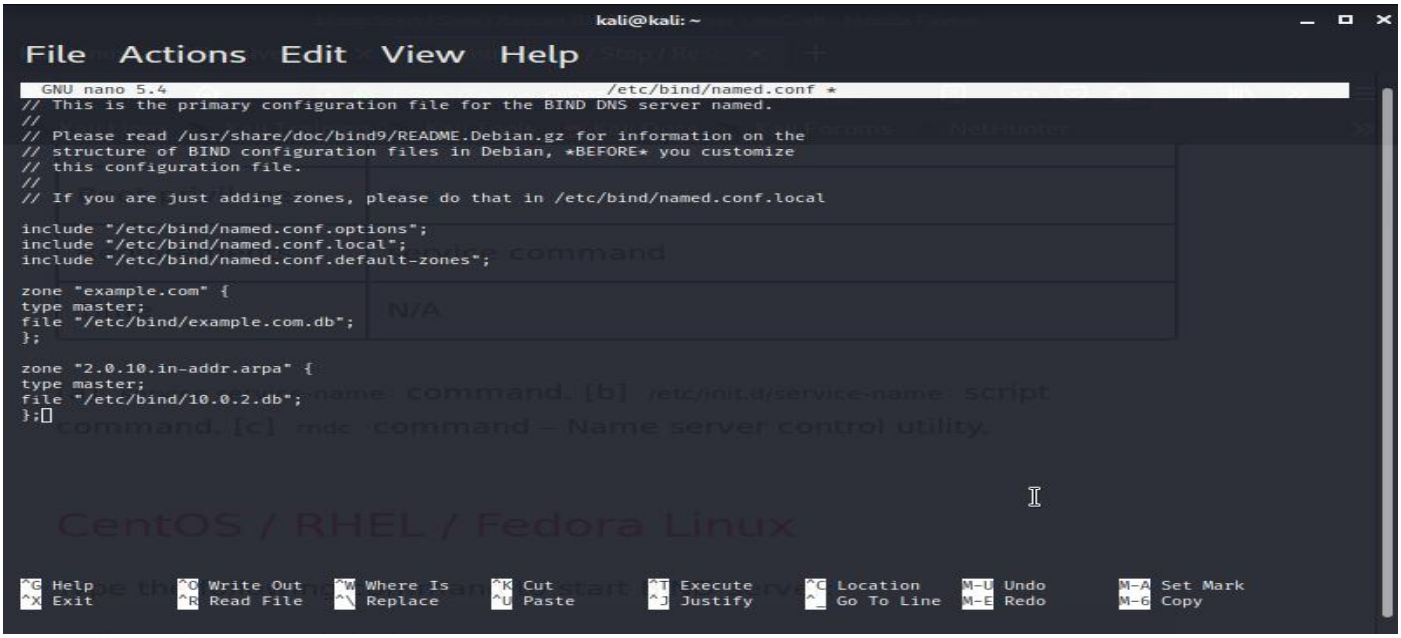


Cache Dumpfile (flipkart.com)

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).



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 **10.2.22.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

```
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: ~
File Actions Edit View Help
kali@kali:~$ dig www.example.com

; <<>> DiG 9.11.5-P4-5.1+b1-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: 84af7c736905beb901000000602fff3cab40b551161c5615 (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

kali@kali:~$
```

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

*any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

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_any_20210219130853_Oq14xC.pcapng Packets: 22 · Displayed: 5 (22.7%) · Ignored: 2 (9.1%) Profile: Default

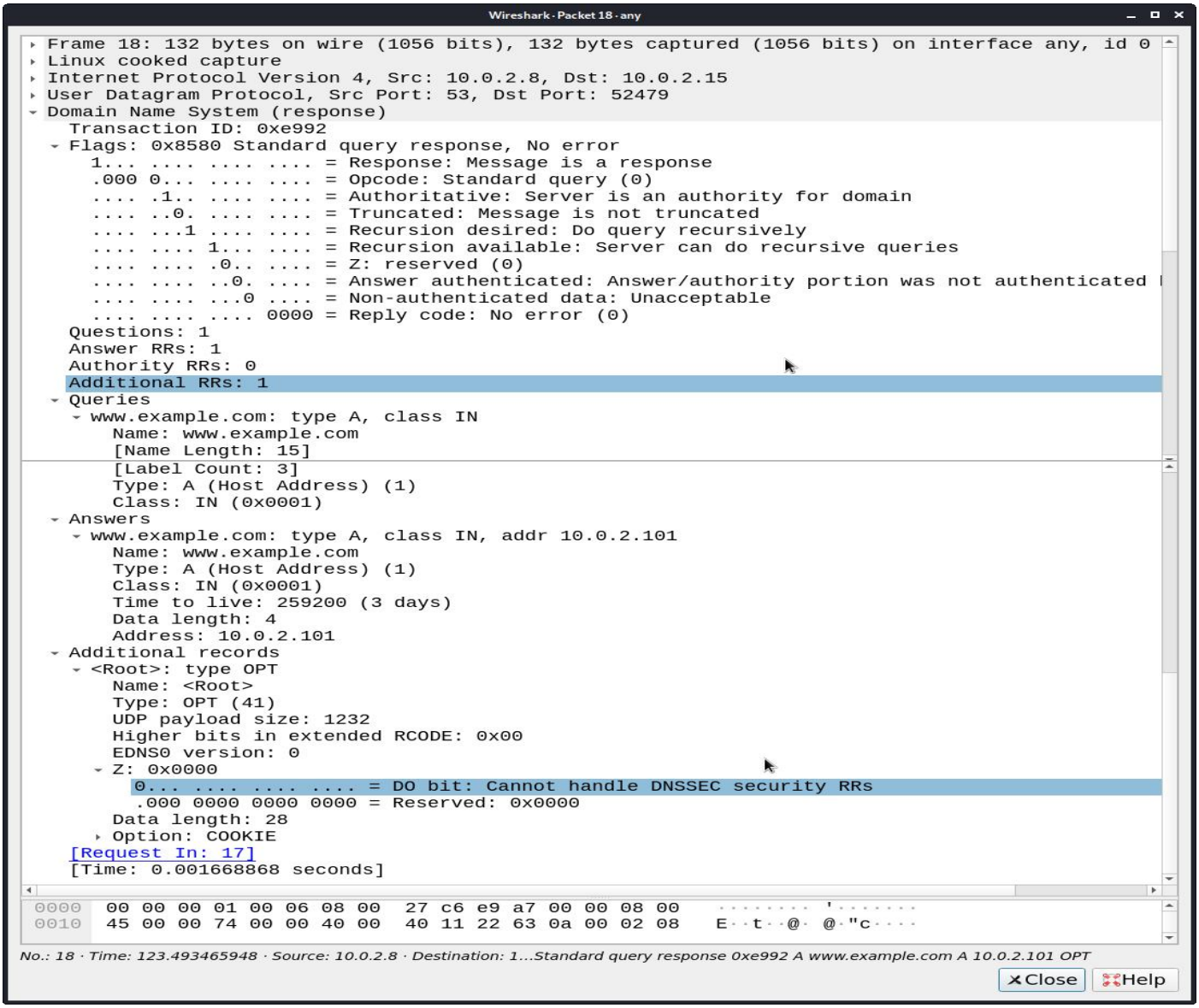
Wireshark Packet Capture

Wireshark · Packet 17 · any

```
▸ 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)
      .... ..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]
```

Close Help

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.