

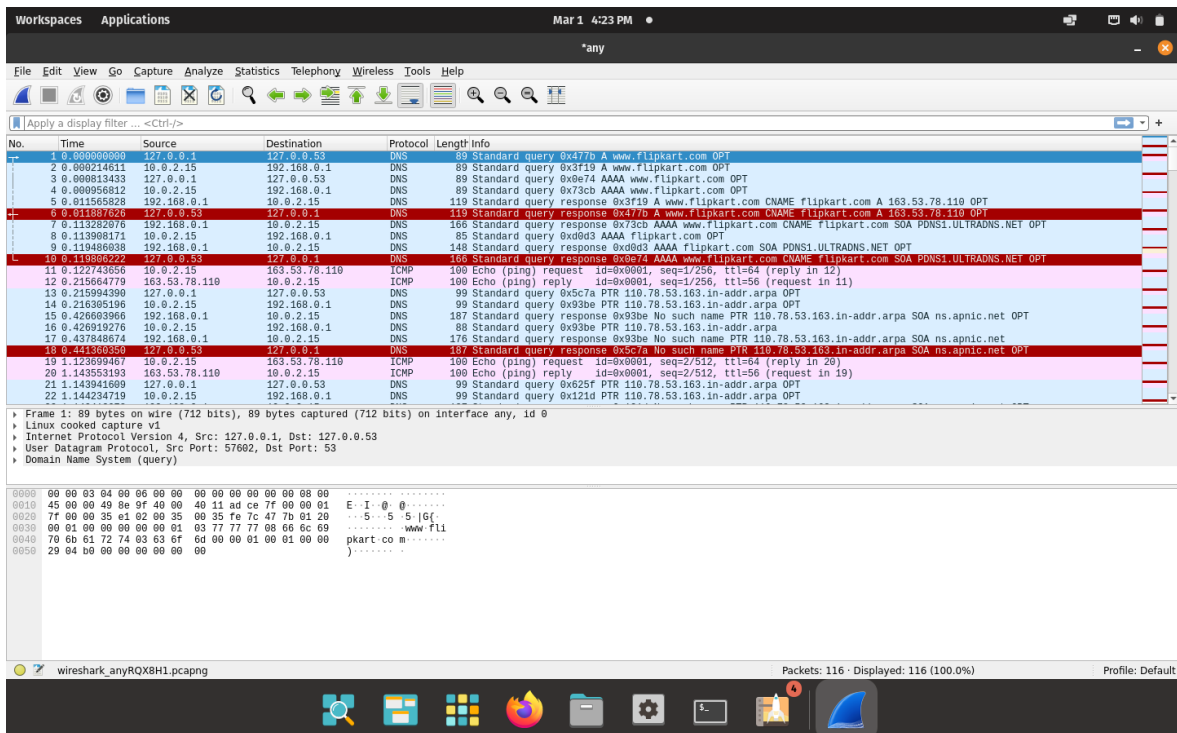
# CN Lab Report – Week 5

PES2UG20CS390

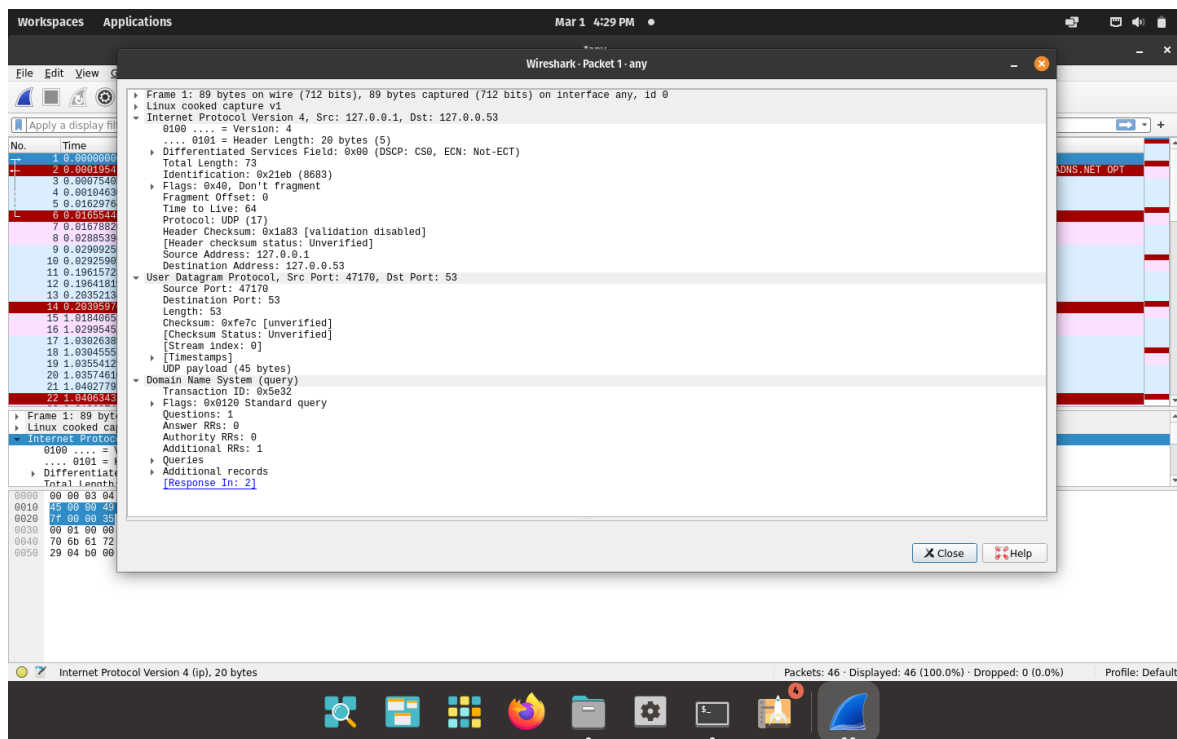
VISHWAS M

## 1. 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 **127.0.0.53**.
- 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**.
- The first query and authoritative response are shown below.



Wireshark Packet Capture



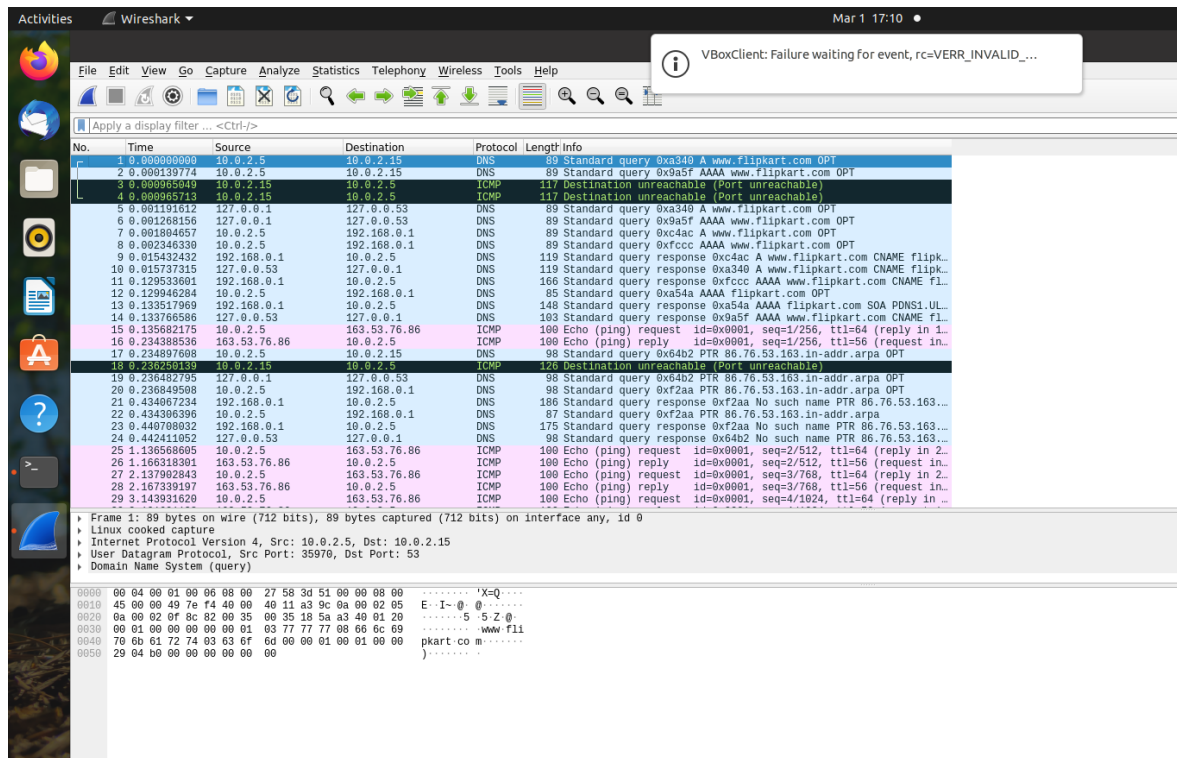
DNS Query

## 2. Task 1 – Configuring Client Machine

- The IP Address of the client machine is **10 . 0 . 2 . 4** and the IP Address of the server machine is **10 . 0 . 2 . 15**.
- We need to add the IP Address of the custom DNS server (**10 . 0 . 2 . 15**) to the client machine.
- 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 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**

## 3. Second Test

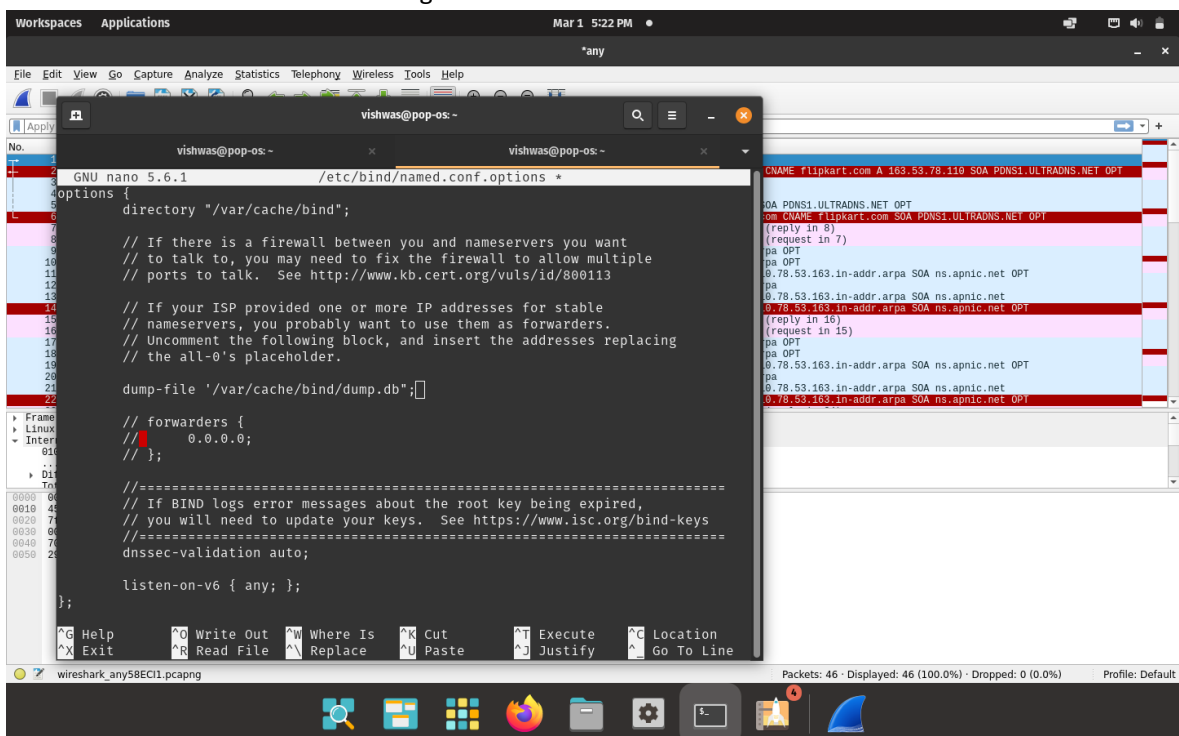
- The Flipkart website is pinged again, and Wireshark is used to capture packets.
- We obtain a `destination unreachable error` in Wireshark as the server machine does not have a DNS server associated with it.
- The client tries to obtain the DNS record from **10 . 0 . 2 . 15** but it does not receive any hence it resorts to using the default DNS server at **127 . 0 . 0 . 53**.



Wireshark Packet Capture

#### 4. Task 2 – Setting Up Local DNS Server

- 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 this server is **/etc/bind/named.conf.options**.
- An entry specifying 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**.





▼ Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0

▶ Interface id: 0 (any)  
 Encapsulation type: Linux cooked-mode capture (25)  
 Arrival Time: Mar 1, 2022 17:31:01.567804692 IST  
 [Time shift for this packet: 0.000000000 seconds]  
 Epoch Time: 1646136061.567804692 seconds  
 [Time delta from previous captured frame: 0.000000000 seconds]  
 [Time delta from previous displayed frame: 0.000000000 seconds]  
 [Time since reference or first frame: 0.000000000 seconds]  
 Frame Number: 1  
 Frame Length: 89 bytes (712 bits)  
 Capture Length: 89 bytes (712 bits)  
 [Frame is marked: False]  
 [Frame is ignored: False]  
 [Protocols in frame: sll:ethertype:ip:udp:dns]  
 [Coloring Rule Name: UDP]  
 [Coloring Rule String: udp]

▼ Linux cooked capture

Packet type: Sent by us (4)  
 Link-layer address type: 1  
 Link-layer address length: 6  
 Source: PcsCompu\_58:3d:51 (08:00:27:58:3d:51)  
 Unused: 0000  
 Protocol: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 10.0.2.5, 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: 73  
 Identification: 0x94e3 (38115)  
 ▶ Flags: 0x4000, Don't fragment  
 Fragment offset: 0  
 Time to live: 64  
 Protocol: UDP (17)  
 Header checksum: 0x8dad [validation disabled]

0000	00 04 00 01 00 06 08 00	27 58 3d 51 00 00 08 00	..... 'X=Q....
0010	45 00 00 49 94 e3 40 00	40 11 8d ad 0a 00 02 05	E..I...@..@.....
0020	0a 00 02 0f d3 5b 00 35	00 35 18 5a 7c 54 01 20	.....[5]5-Z T.
0030	00 01 00 00 00 00 00 01	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 00 00	pkart.co m.....
0050	29 04 b0 00 00 00 00 00	00	).....

DNS Query Packet

```

▼ User Datagram Protocol, Src Port: 53, Dst Port: 54107
  Source Port: 53
  Destination Port: 54107
  Length: 130
  Checksum: 0xd139 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  ▶ [Timestamps]
▼ Domain Name System (response)
  Transaction ID: 0x6b52
  ▼ 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 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: 1
  ▼ Queries
    ▶ www.flipkart.com: type AAAA, class IN
  ▼ 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: 60 (1 minute)
      Data length: 2
      CNAME: flipkart.com
    ▼ Authoritative nameservers
      ▼ flipkart.com: type SOA, class IN, mname PDNS1.ULTRADNS.NET
        Name: flipkart.com
        Type: SOA (Start Of a zone of Authority) (6)
        Class: IN (0x0001)
        Time to live: 60 (1 minute)
        Data length: 51
        Primary name server: PDNS1.ULTRADNS.NET
        Responsible authority's mailbox: sysadmin.flipkart.com
        Serial Number: 2017031805
        Refresh Interval: 10800 (3 hours)
        Retry Interval: 3600 (1 hour)
        Expire limit: 604800 (7 days)
        Minimum TTL: 60 (1 minute)
      ▶ Additional records
        [Request In: 2]
        [Time: 2.683474505 seconds]

```

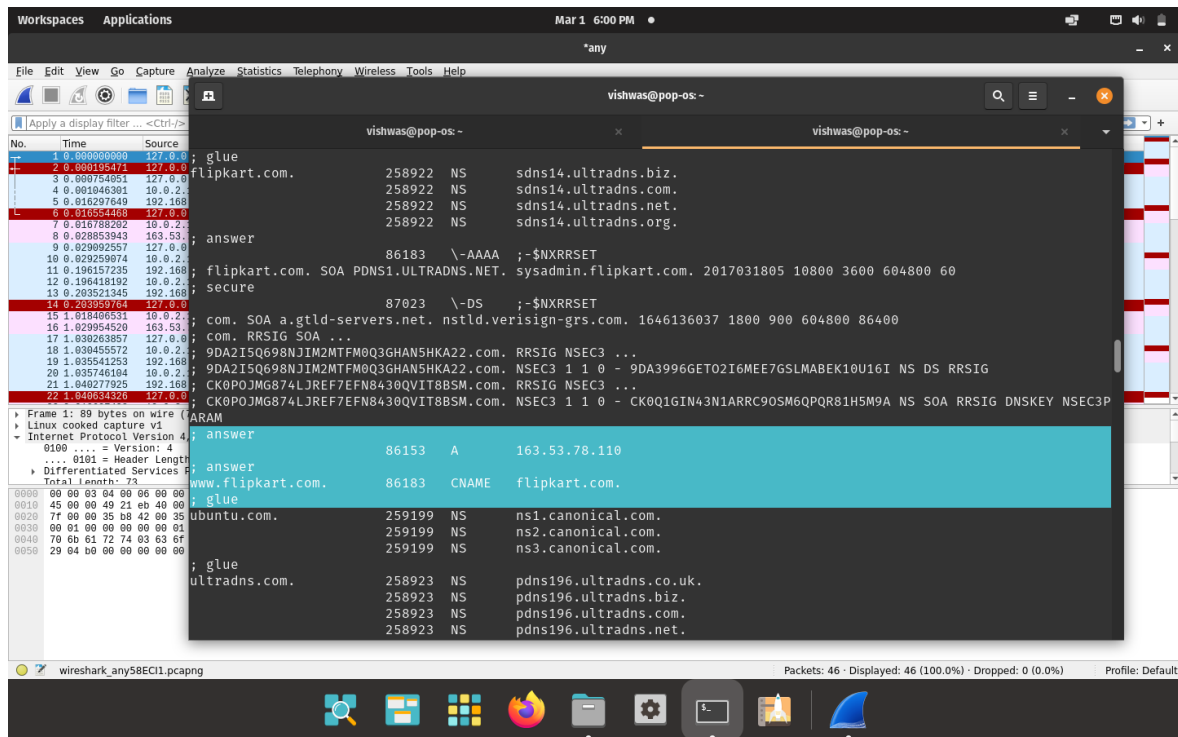
```

0000 00 00 00 01 00 06 08 00 27 d5 ea 90 00 00 08 00 .....!...
0010 45 00 00 96 5a 19 00 00 40 11 08 2b 0a 00 02 0f E...Z...@...+...
0020 0a 00 02 05 00 35 d3 5b 00 82 d1 39 6b 52 81 80 .....5.[...9KR...
0030 00 01 00 01 00 01 00 01 03 77 77 77 08 66 6c 69 .....www·fli
0040 70 6b 61 72 74 03 63 6f 6d 00 00 1c 00 01 c0 0c pkart·co m.....
0050 00 05 00 01 00 00 00 3c 00 02 c0 10 c0 10 00 06 .....<.....

```

## DNS Response Packet



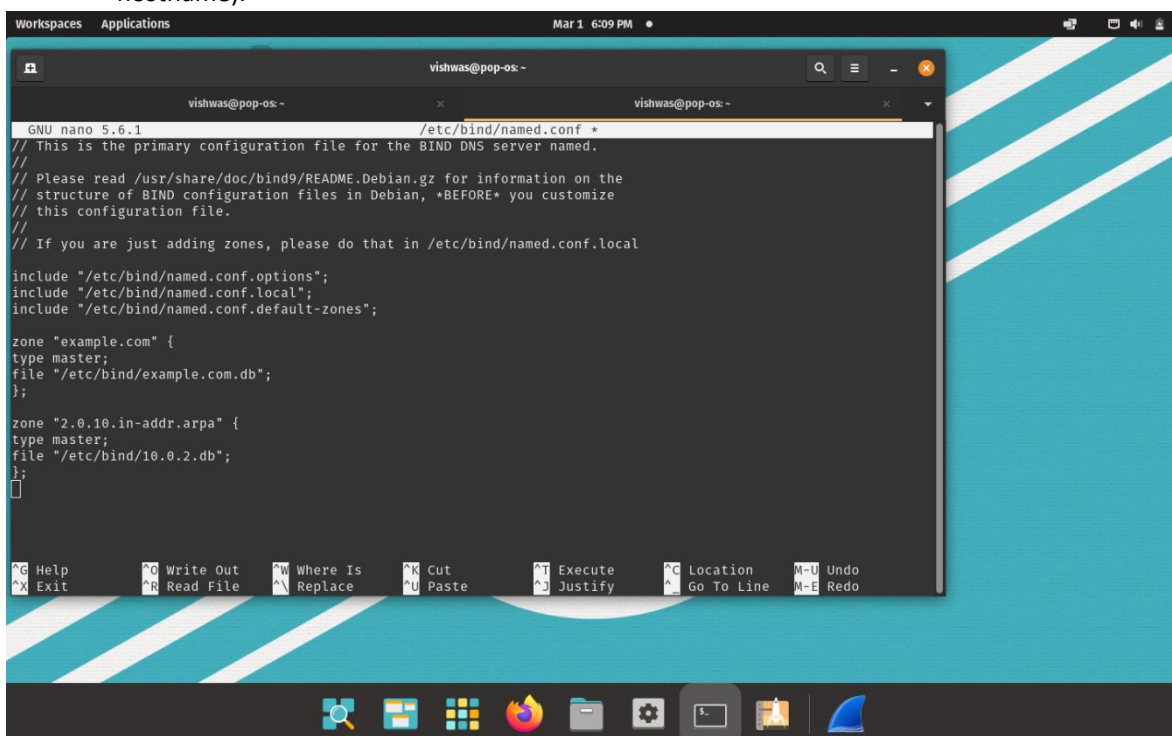


Cache Dumpfile

## 6. Task 3 – Hosting a Zone in the Local DNS Server

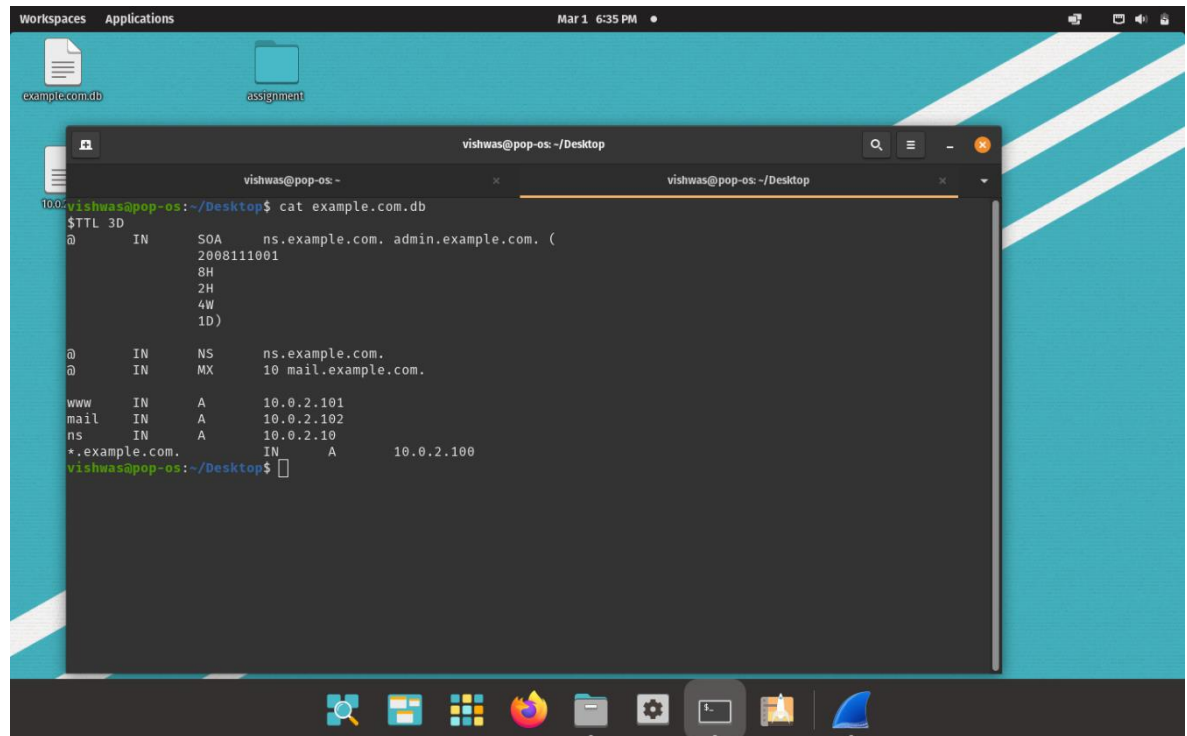
### 6.1 Zone Creation

- 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).



## 6.2 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 mailserver and 4 authoritative records.



The screenshot shows a terminal window titled "vishwas@pop-os: ~/Desktop". The user has executed the command `cat example.com.db`. The output displays the following DNS records:

```
$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.

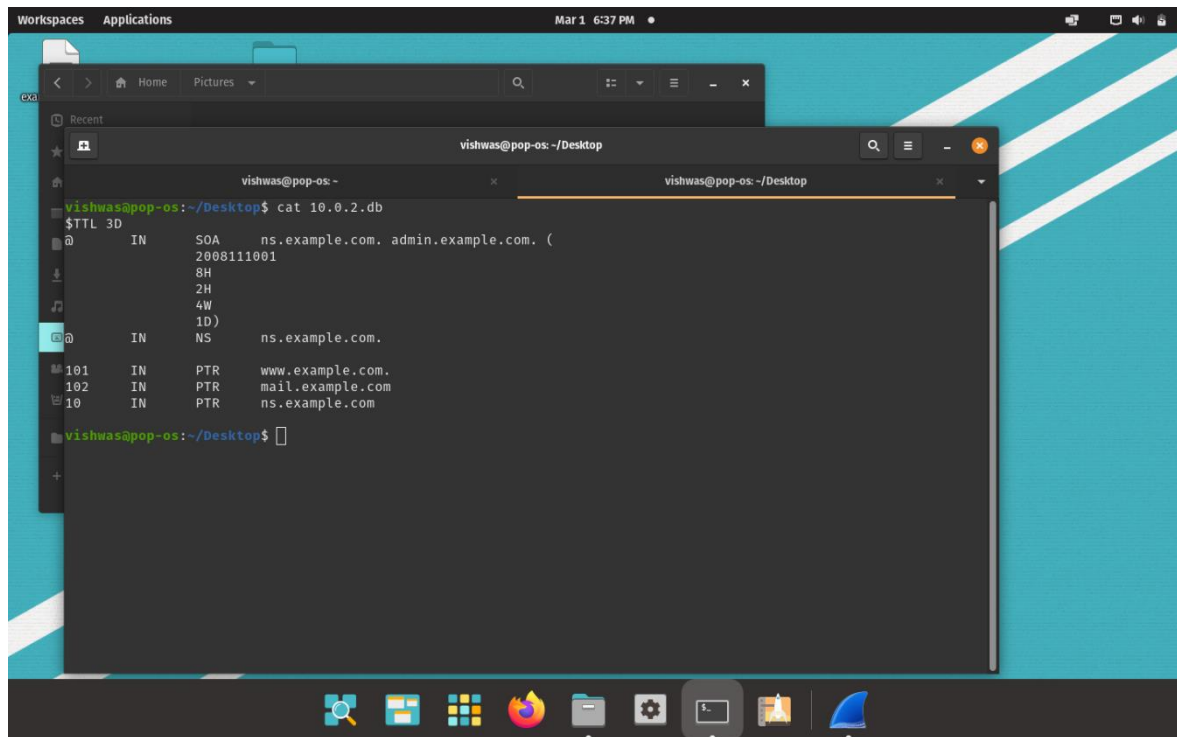
www    IN      A       10.0.2.101
mail   IN      A       10.0.2.102
ns     IN      A       10.0.2.10
*.example.com. IN A       10.0.2.100
```

- 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.

### Forward Lookup file

- The reverse lookup file is stored at `/etc/bind/10.0.2.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.

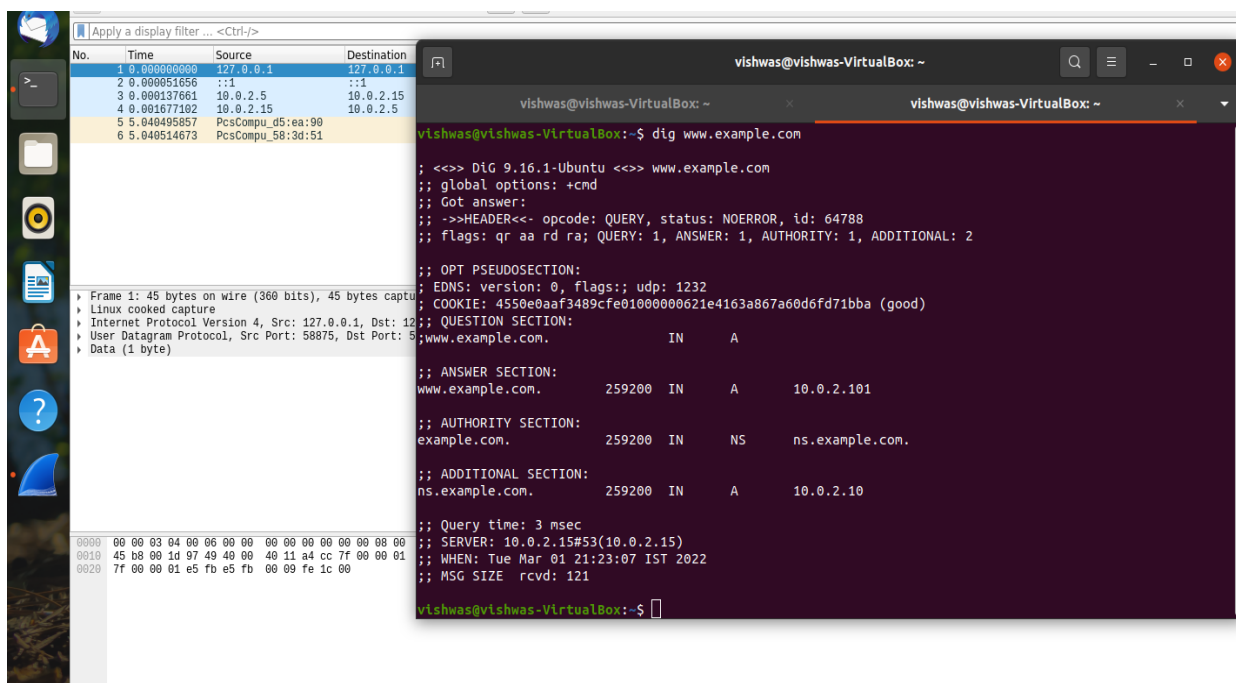




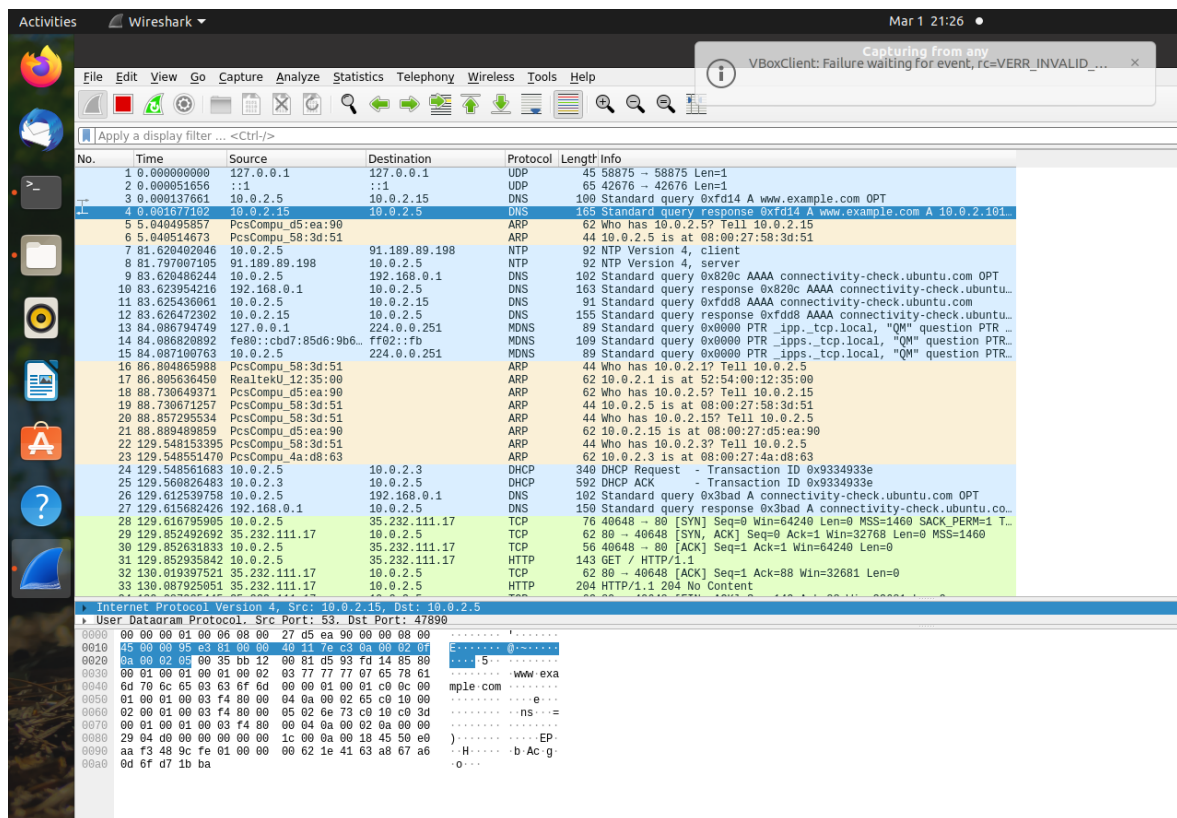
Reverse Lookup file

## 7. Fourth Test – Testing [www.example.com](http://www.example.com)

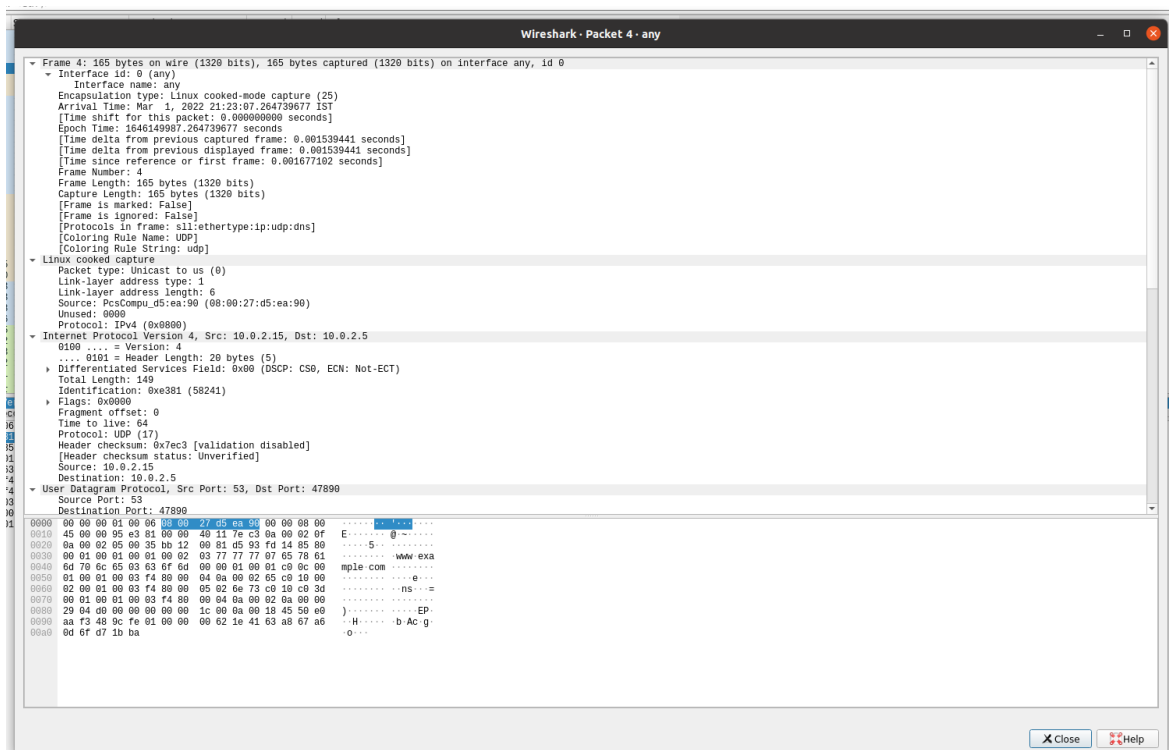
- The dig command is used to lookup name servers specified in the file `/etc/resolv.conf`
- Wireshark is used to capture the packets while running the command dig `www.example.com`
- The IP Address of the DNS Server and the returned IP Address of the domain set by us can be seen in the query and response packets.



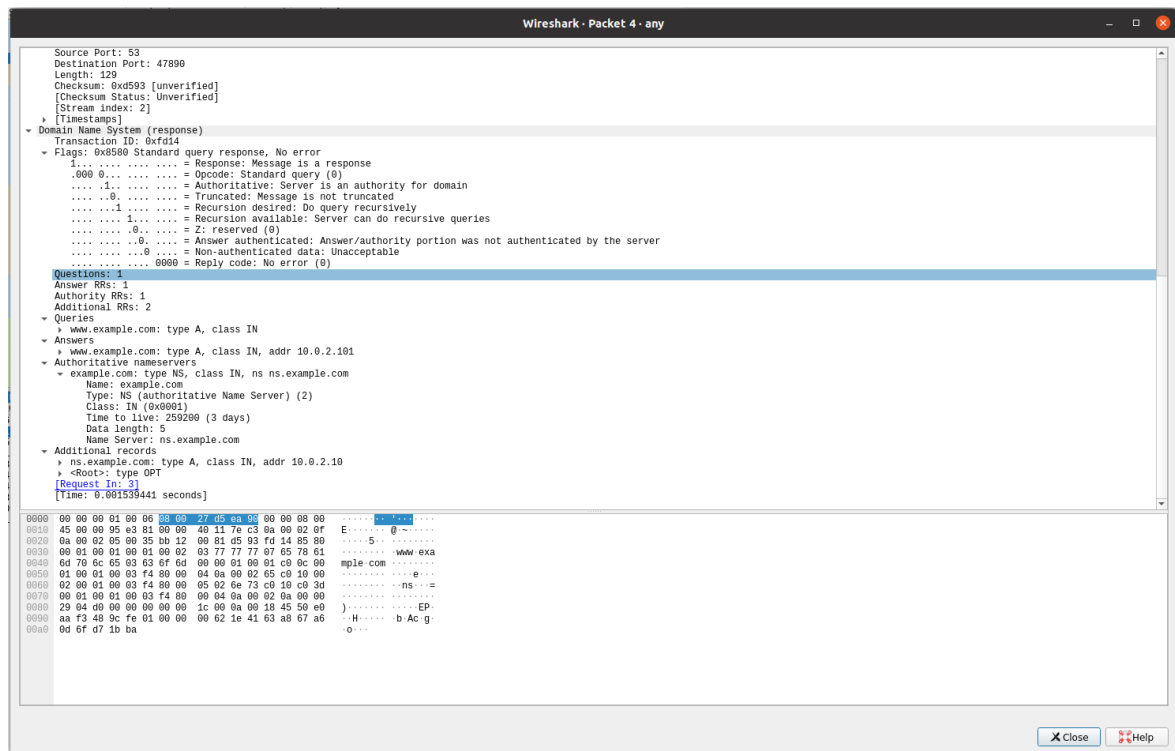
dig `www.example.com`



Wireshark Packet Capture



DNS Response Packet



DNS Response Packet

## 8. Questions

**Q1.** Locate the DNS query and response messages. Are then 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 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 ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

**Answer** – 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.

**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.