**COMPUTER NETWORKS LAB**

**Implementation of a Local DNS Server and Authoritative Nameserver**

**WEEK 5**

**NAME: VISHWA MEHUL MEHTA**

**SRN: PES2UG20CS389**

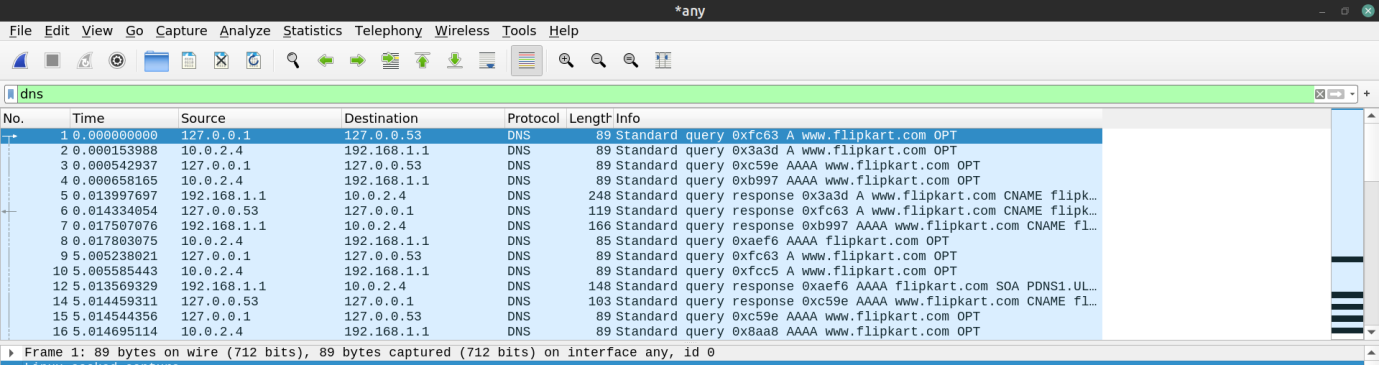
**SECTION: F**

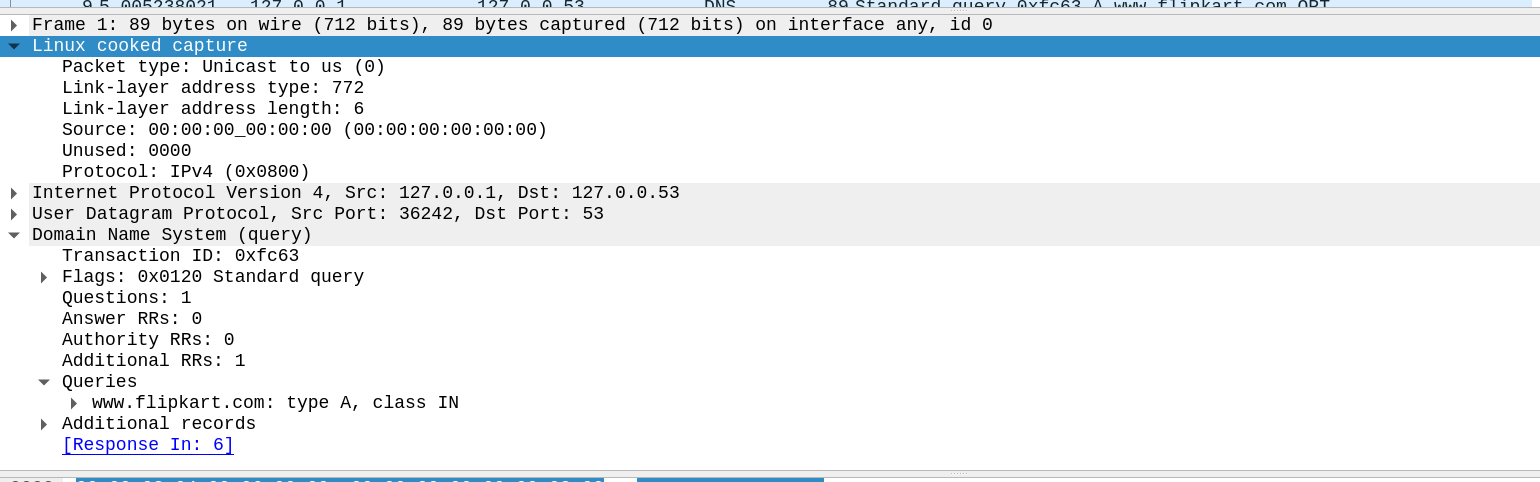
**DATE: 28/02/2022**

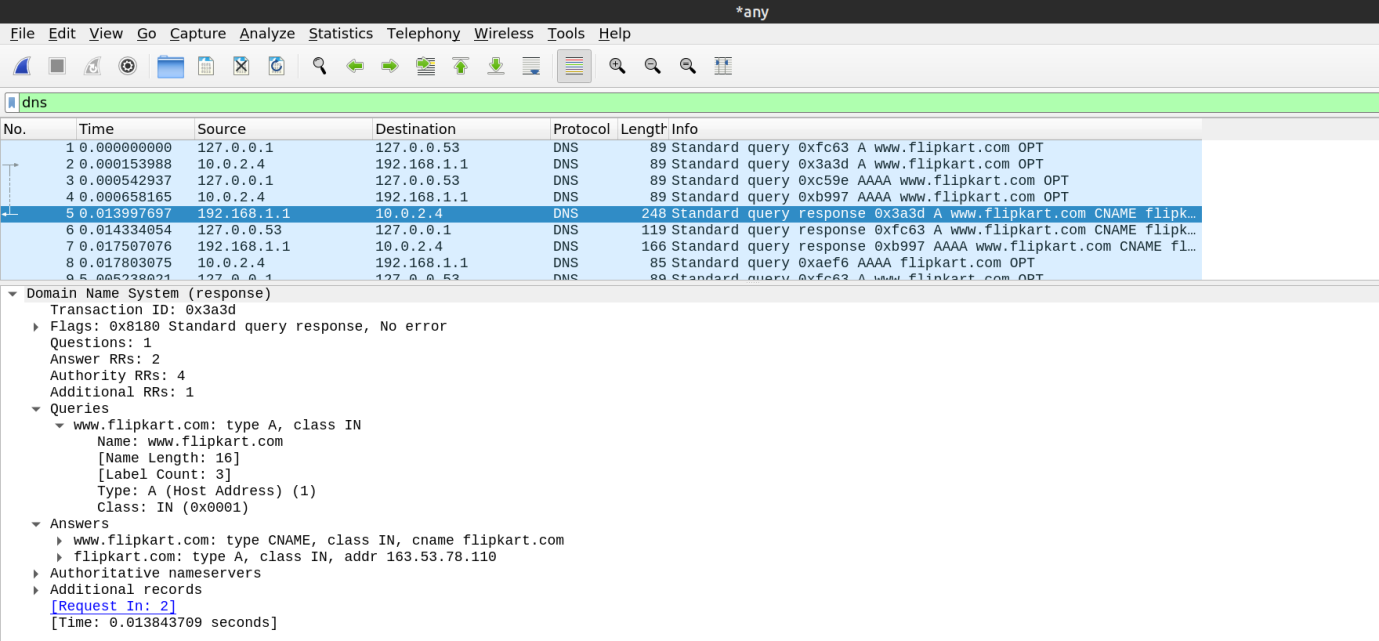
**Part 1: Setting Up a Local DNS Server**

**1. Observation 1 – Pinging default DNS:**

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

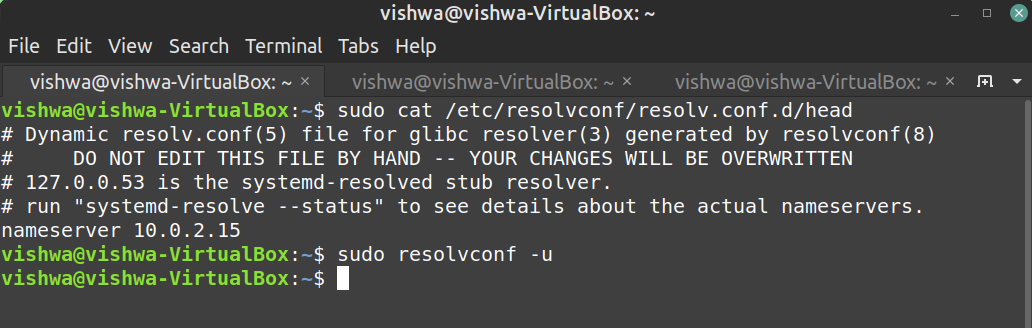


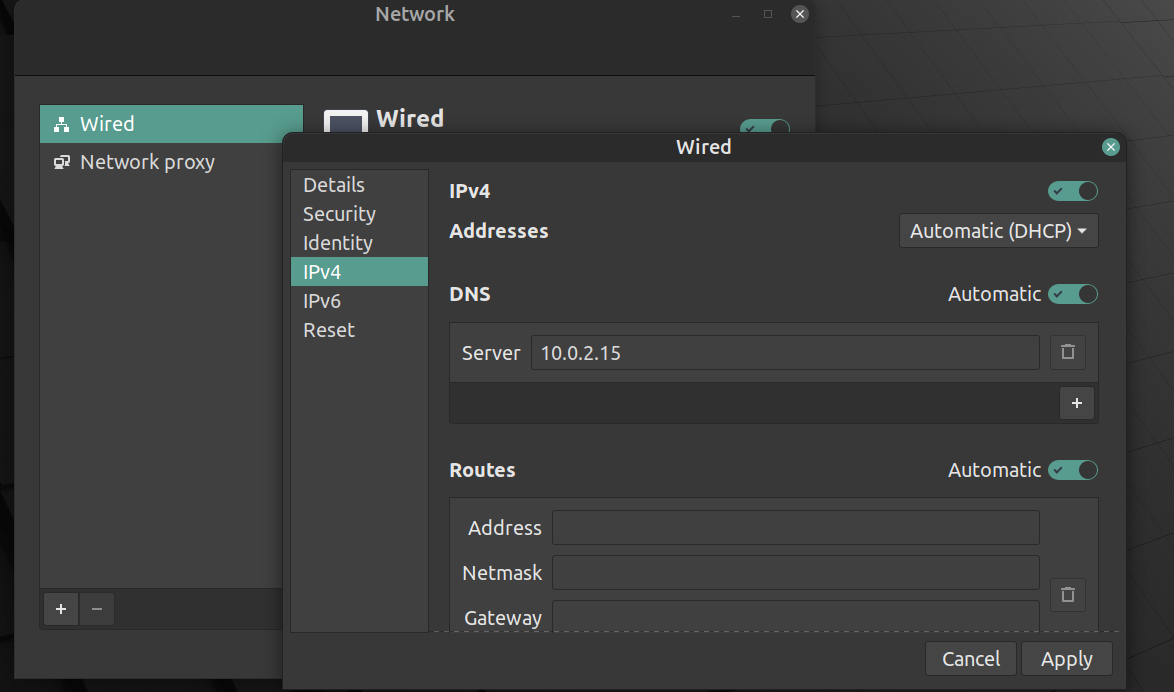




**2. Task 1: Configure the User/Client Machine**

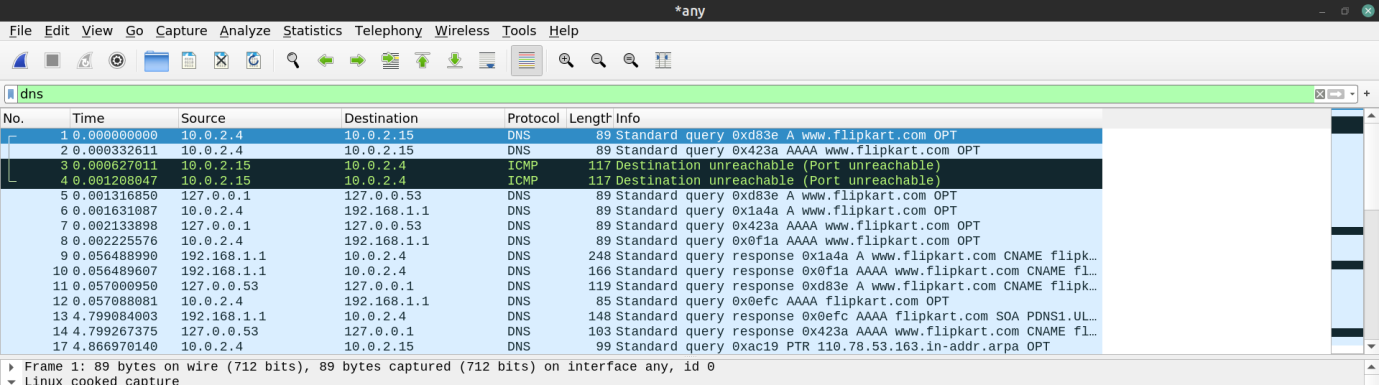
* IP address of the client machine is **10.0.2.4** and the server machine is **10.0.2.15.**
* We need to add the IP address of the custom DNS to the client.
* This is done by adding the IP address of the server to the file **/etc/resolvconf/resolv.conf.d/head** which stores the order of DNS server resolution. The custom DNS server will now be used to resolve names.
* The IP Address of the custom DNS server is also added to the DNS menu under the  
  IPv4 Network Settings.
* The changes are applied by using the command **sudo resolvconf –u**





**3. Observation 2: Pinging custom DNS**

* www.flipkart.com is pinged again.
* We obtain a **destination unreachable error** in Wireshark as the server machine does not have a DNS server associated with it.
* The client tries to obtain the DNS record from **10.0.2.15** but it does not receive any hence it resorts to using the default DNS server at **127.0.0.53**.



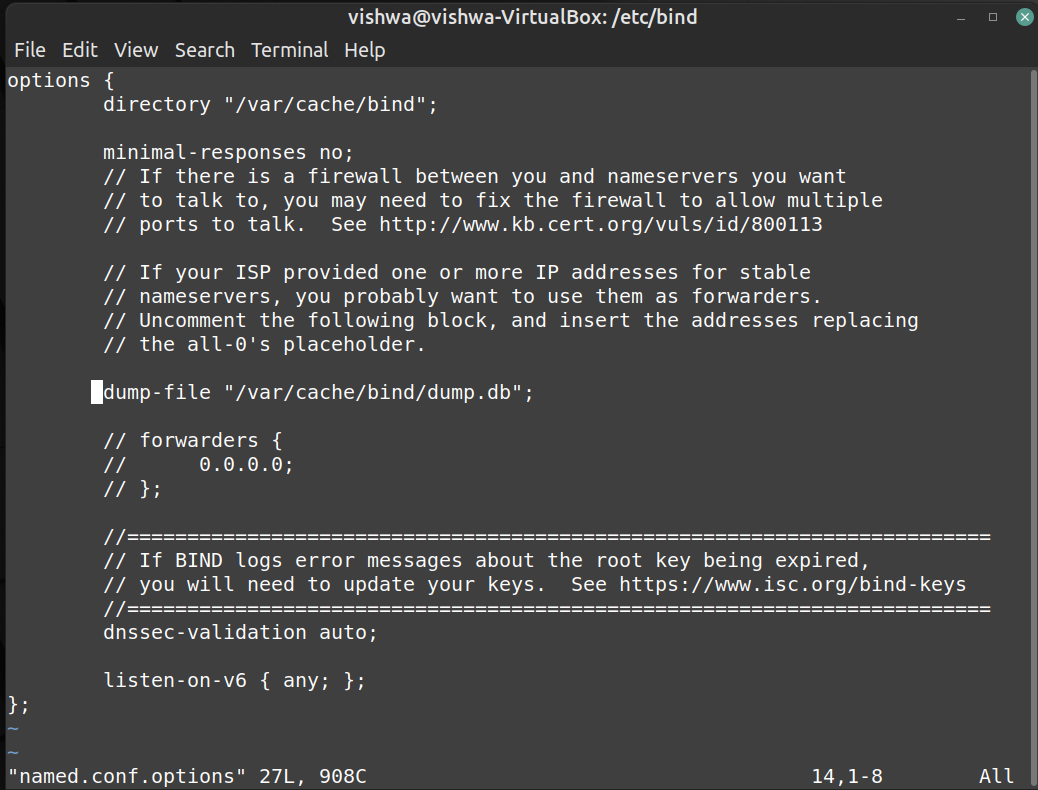
**4. Task 2: Setting Up Local DNS Server**

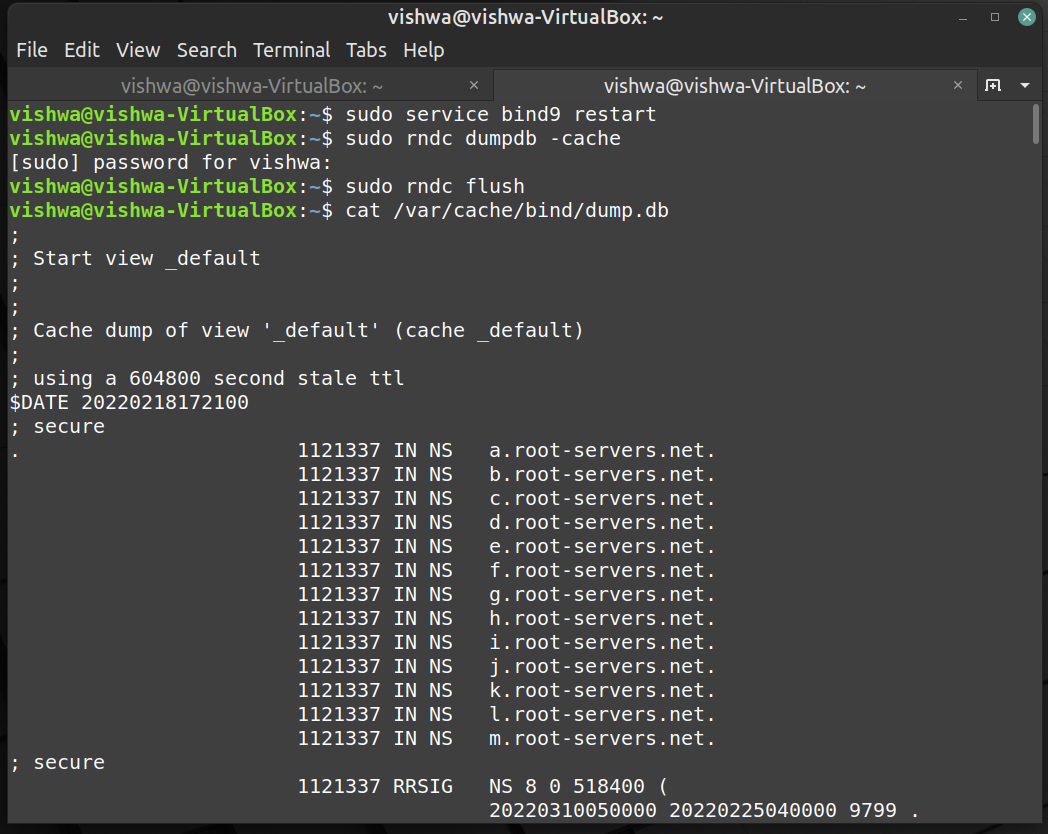
a. Set up **bind9 sever**:

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

b. Start theserver:

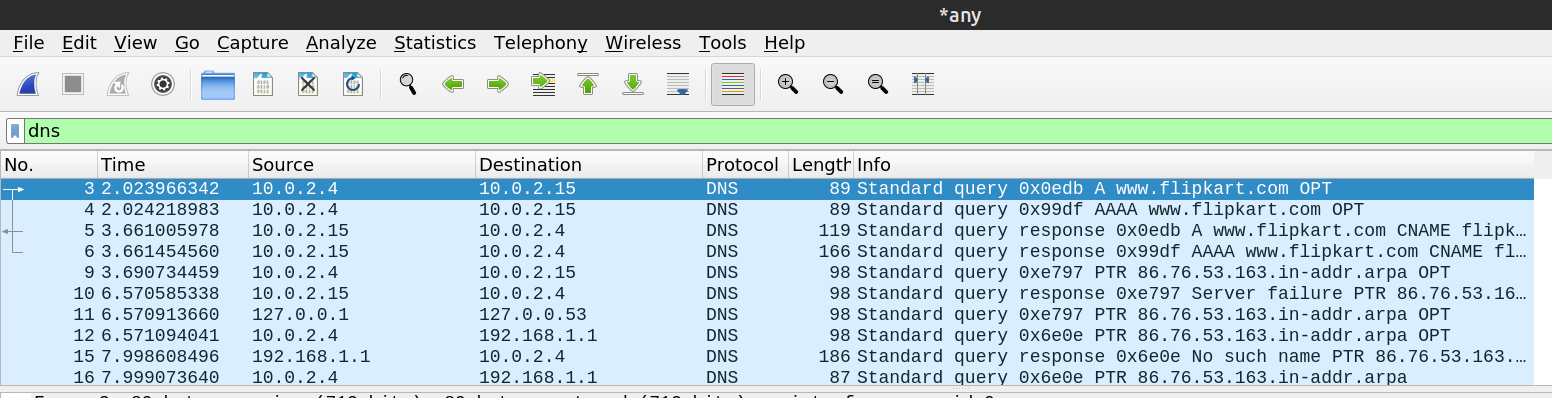
* We start the DNS server using the command **sudo service bind9 restart**.

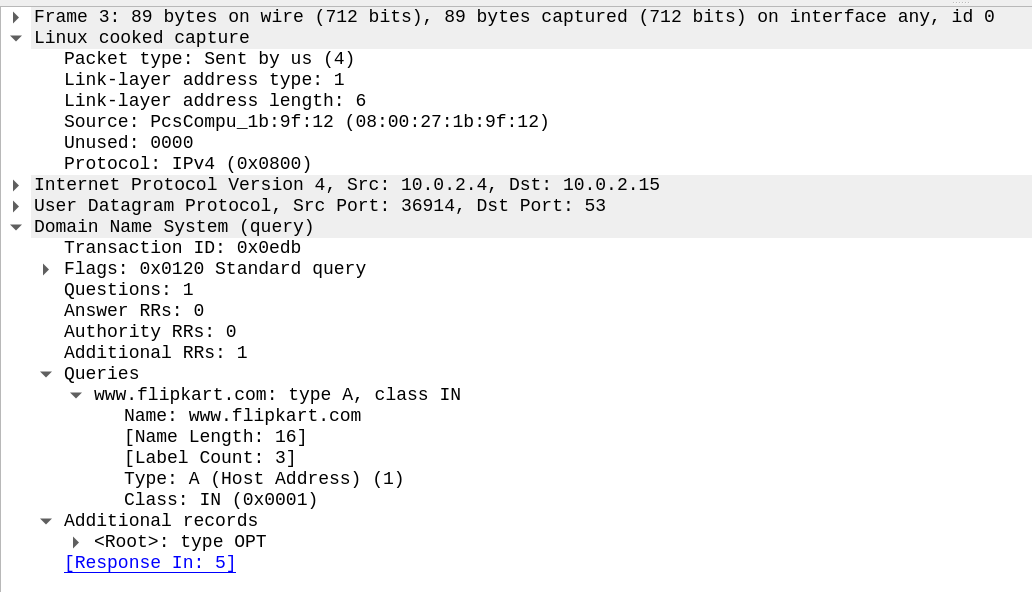


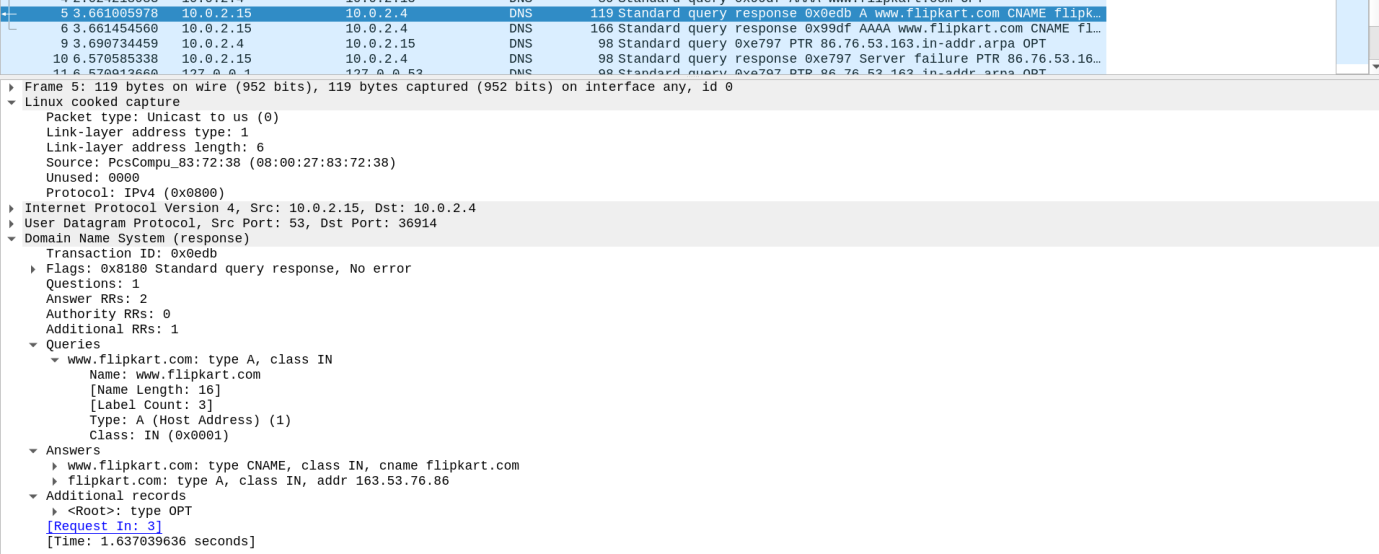


**5. Observation 3-4: Pinging custom DNS(wireshark output and cache dump file contents)**

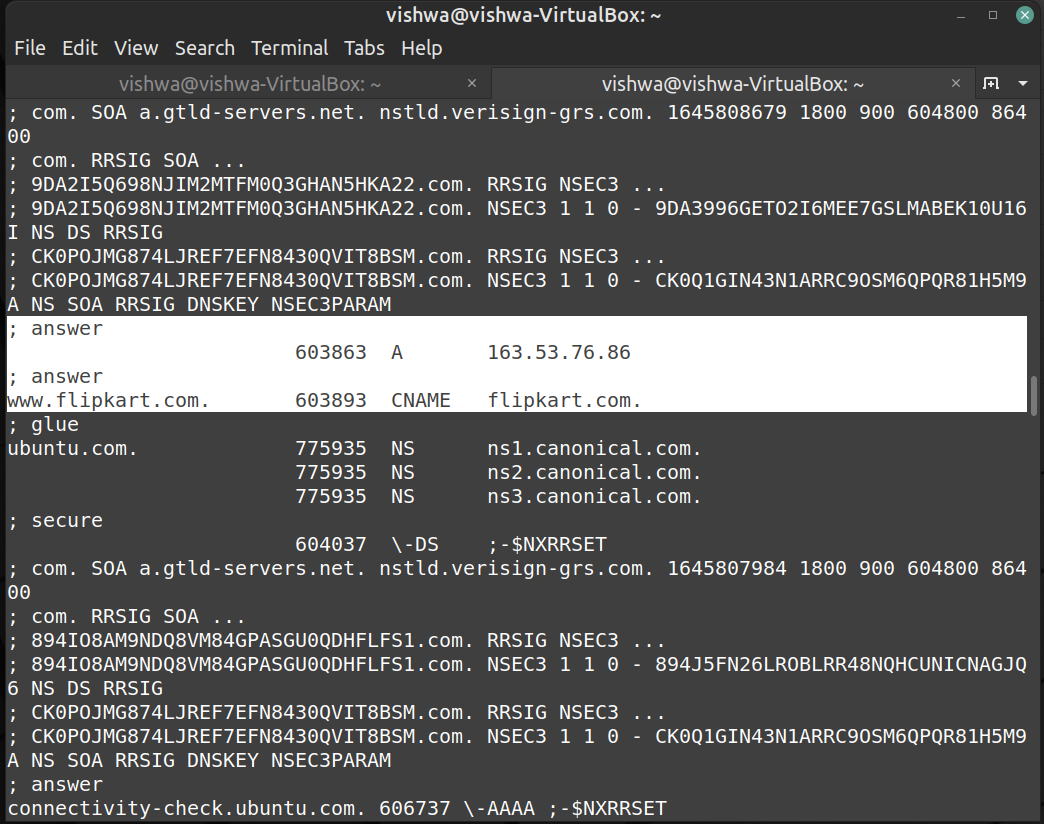
Client:







Server:

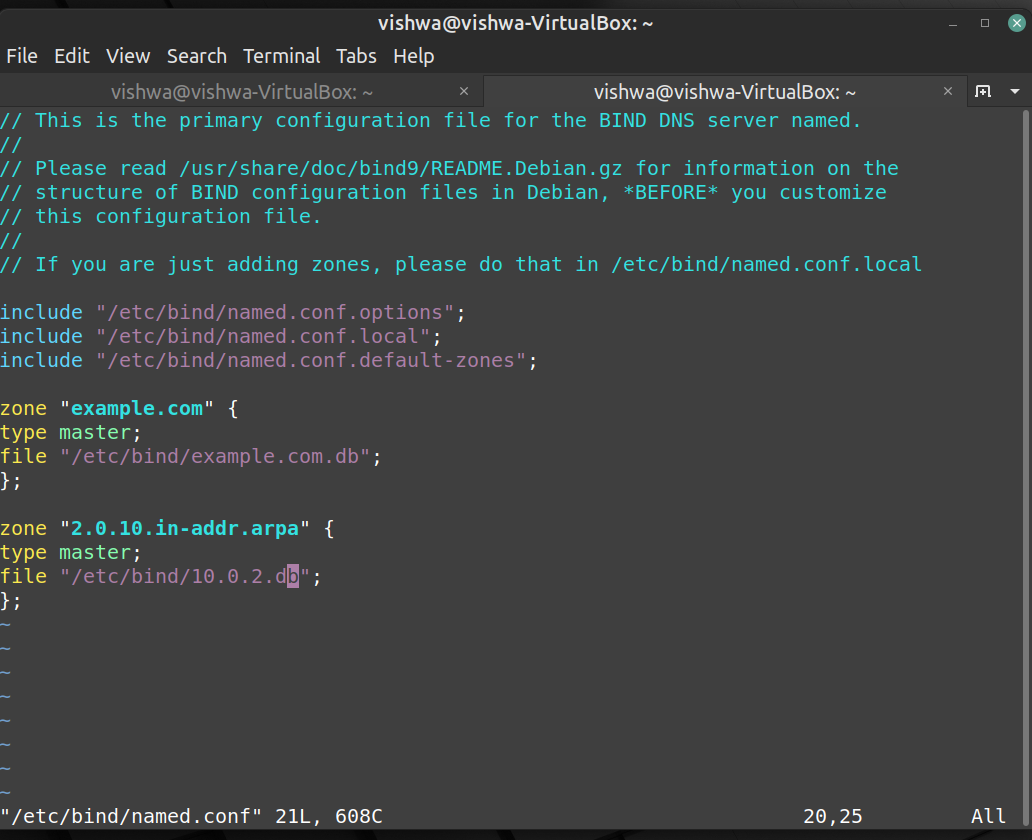


**Part 2: Setting Up an Authoritative Nameserver for example.com domain**

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

1. Create Zones:

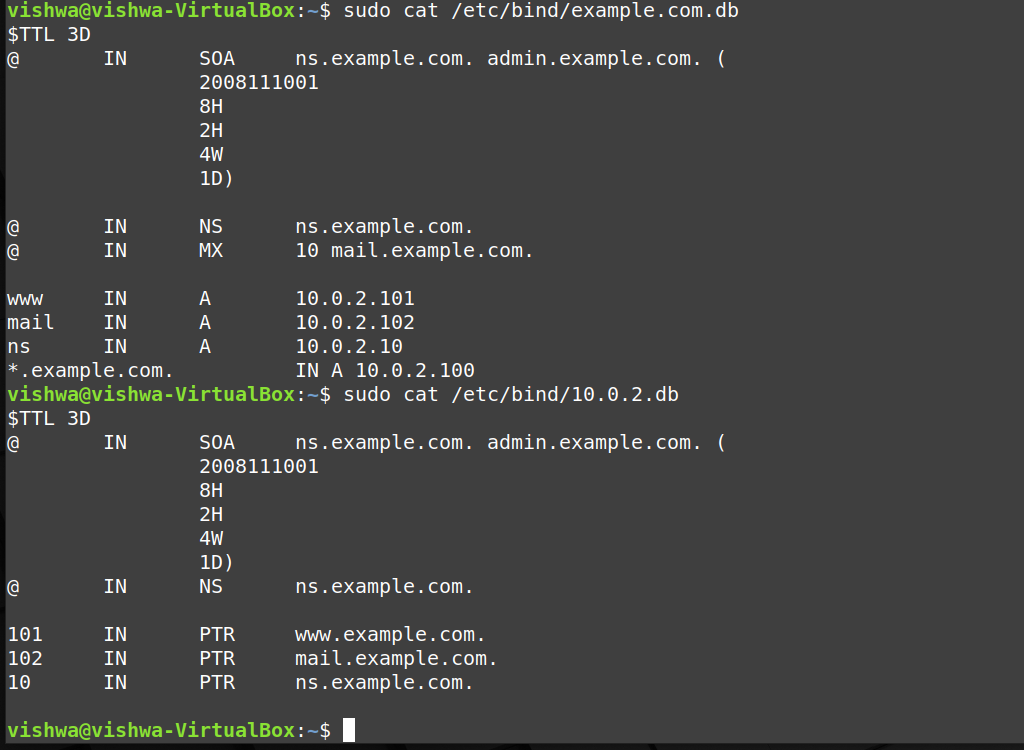
We had two zone entries in the DNS server by adding the following contents to **/etc/bind/named.conf** as shown in the below screenshot. The first zone is for **forward lookup** (from hostname to IP), and the second zone is for **reverse lookup** (from IP to hostname).



1. Setup the forward lookup zone file:

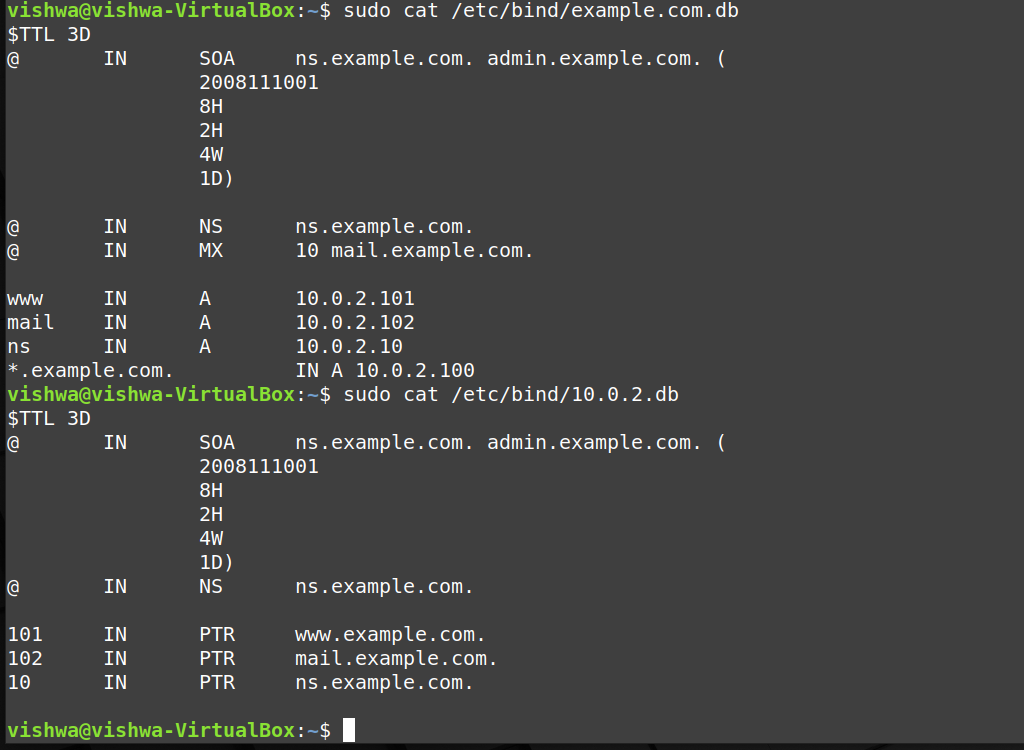
We create **example.com.db** zone file with the following contents in the **/etc/bind/** directory  
where the actual DNS resolution is stored.

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



1. Setup the reverse lookup zone file:

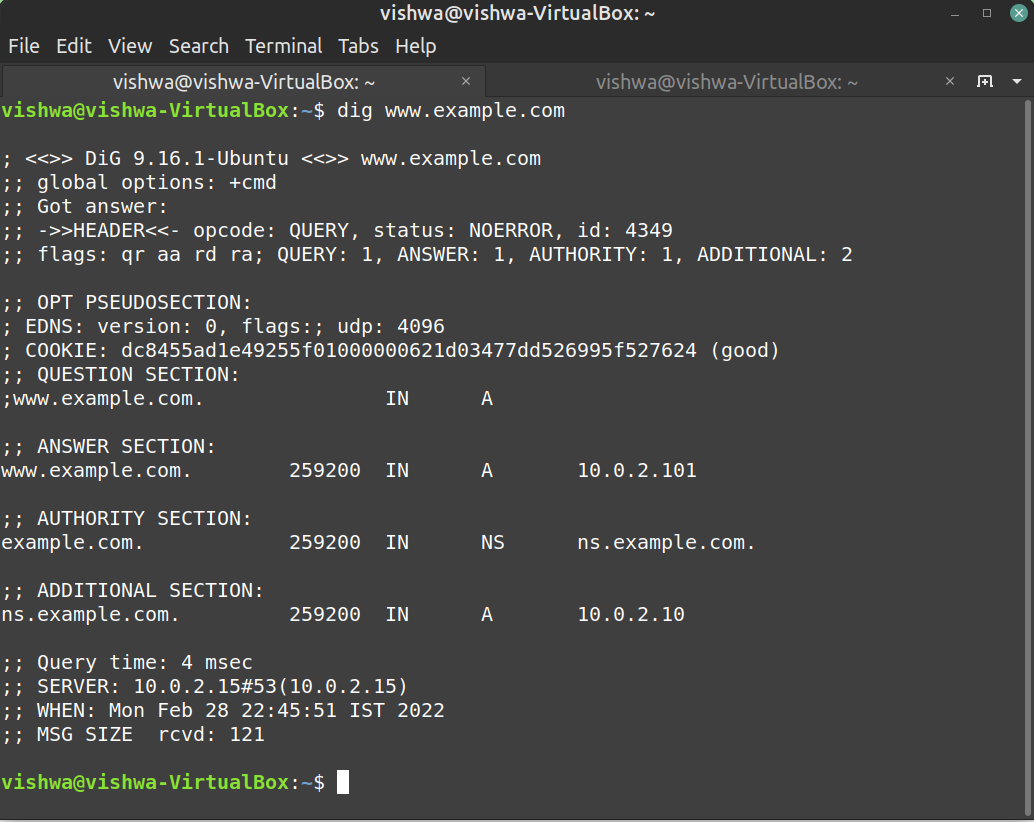
We create a reverse DNS lookup file called **10.2.22.db** for the example.net domain to support  
DNS reverse lookup, i.e., from IP address to hostname in the **/etc/bind/** directory with the following contents.



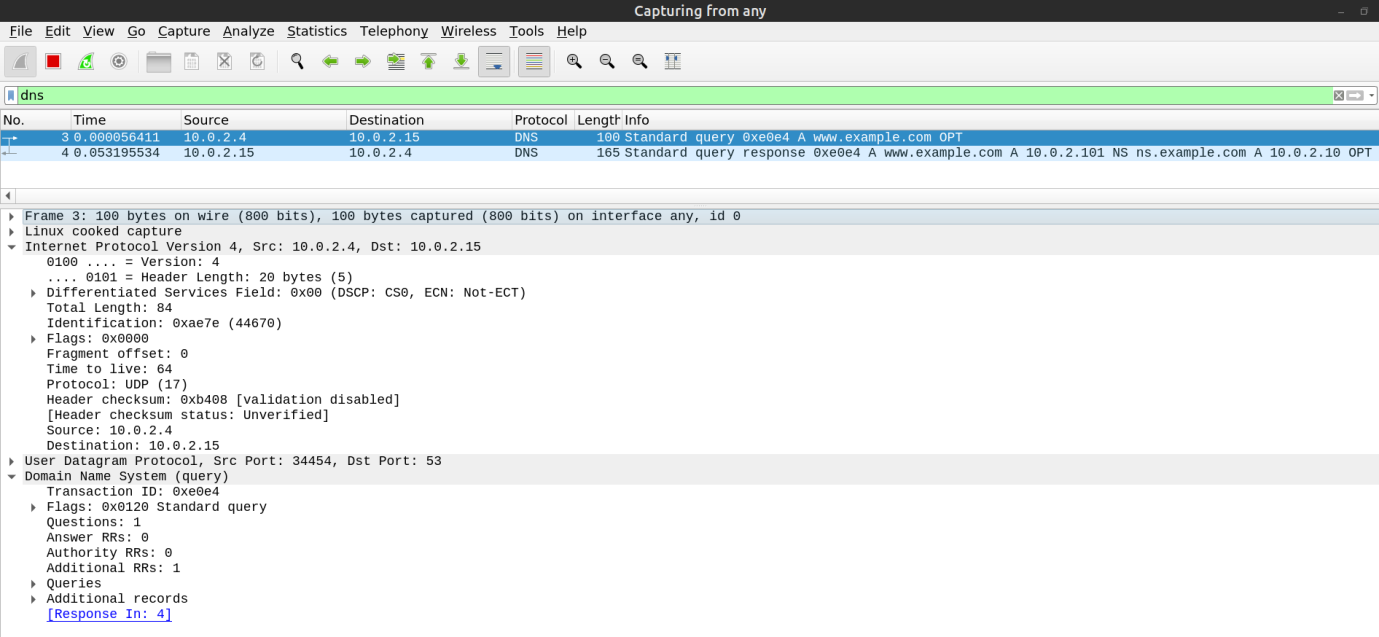
**7. Observation 5: Testing www.example.com**

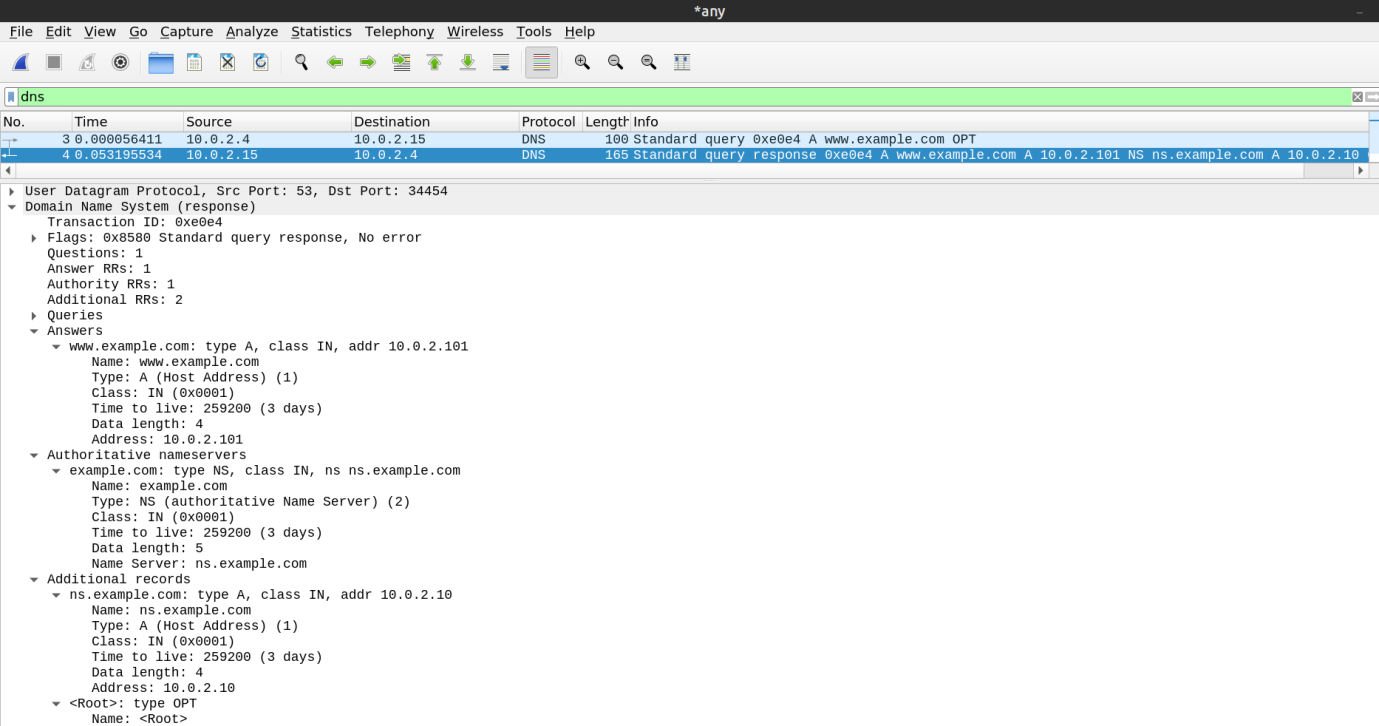
When all the changes are made, remember to restart the BIND server. Now we will restart the DNS server using the following command **sudo service bind9 restart.**

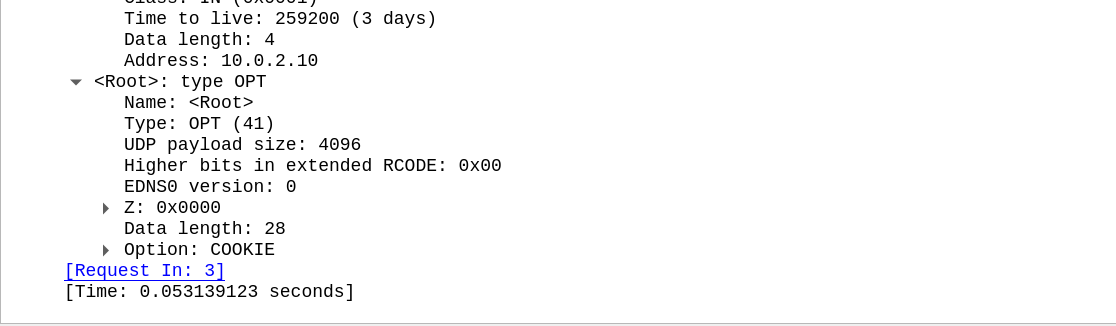
Now, go back to the client machine and ask the local DNS server for the IP address of www.example.com using the dig command. Dig stands for (**Domain Information Groper**) is a network administration command-line tool for querying DNS name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups and displays the answers that are returned from the name server that were queried. **dig** is part of the BIND domain name server software suite.



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







**Observations:**

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

**The messages are sent over UDP.**  
2) What is the destination port for the DNS query message? What is the source port of DNS response message?

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

3) To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

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

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

**The DNS Query is of** type A **since it requests for an authoritative record. The answer section is empty since it does not have any answer.**

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

**The answer section of the DNS response message contains two Resource Records.  
•** CNAME RR**: This determines that the hostname flipkart.com refers to the canonical hostname www.flipkart.com.  
•** A type RR**: This provides the IP Address of the canonical hostname.**

6) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

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