COMPUTER NETWORKS LABORATORY

By:
Nitish S
PES2201800368
5 'A'

WEEK – 4- Implementation of Local DNS Server
Date: 21/09/2020

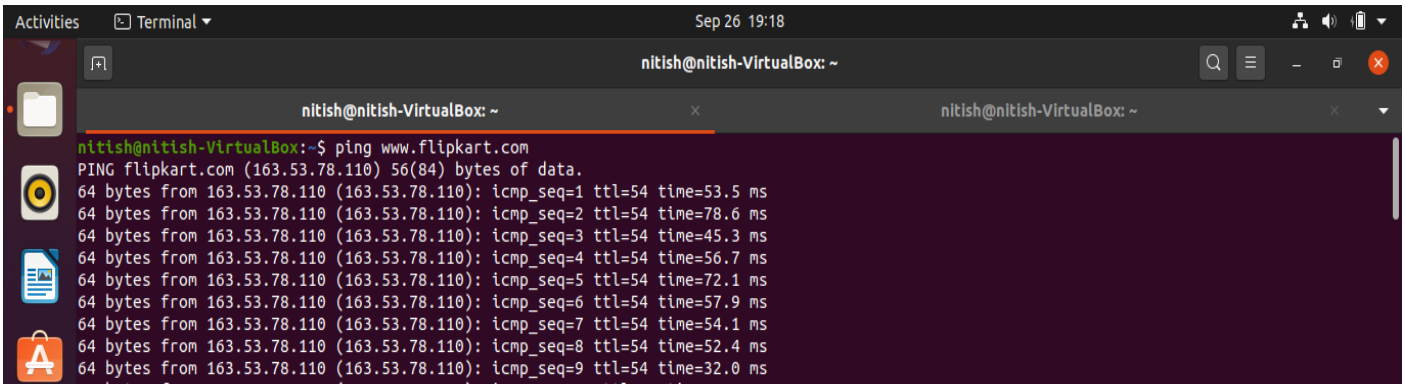
The objectives of this lab are to understand:

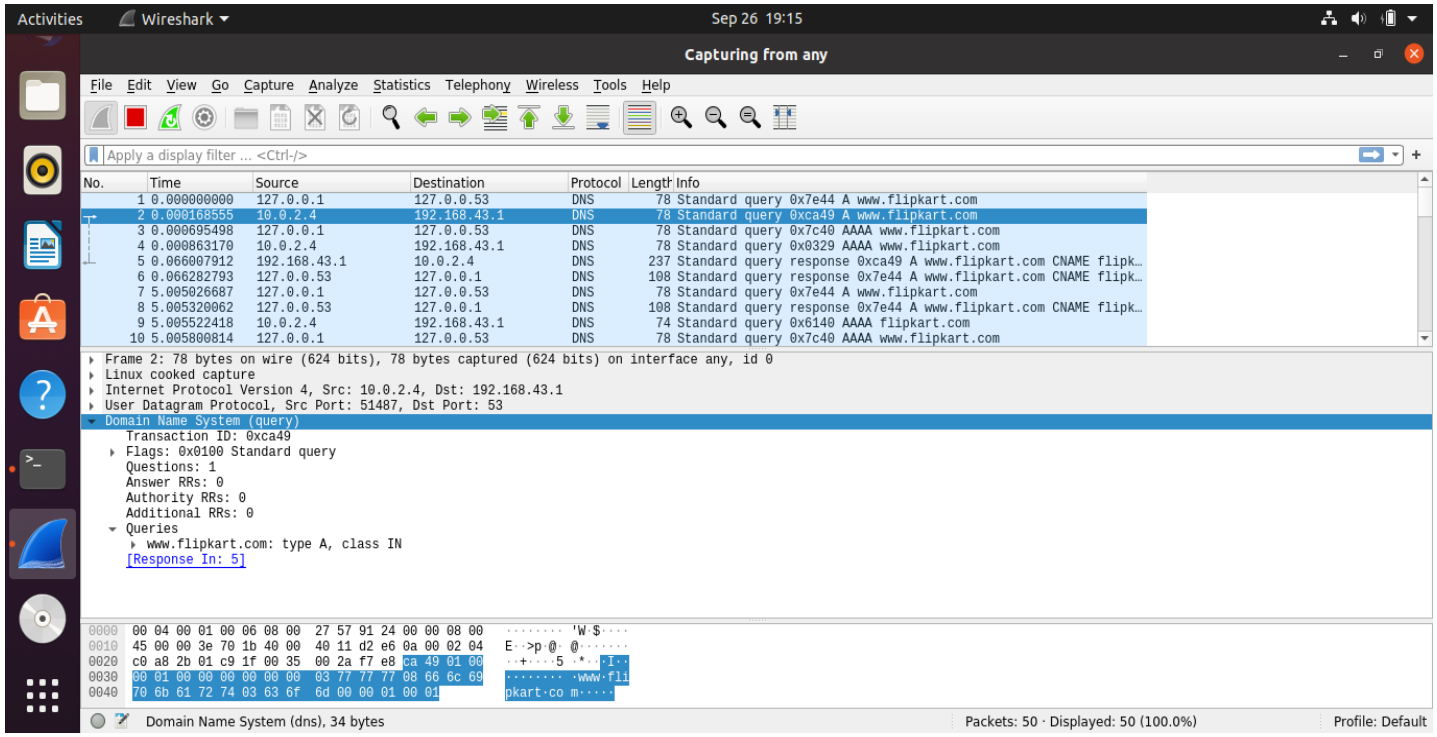
- DNS and how it works
- Install and set up a DNS server
- Functionality and operations

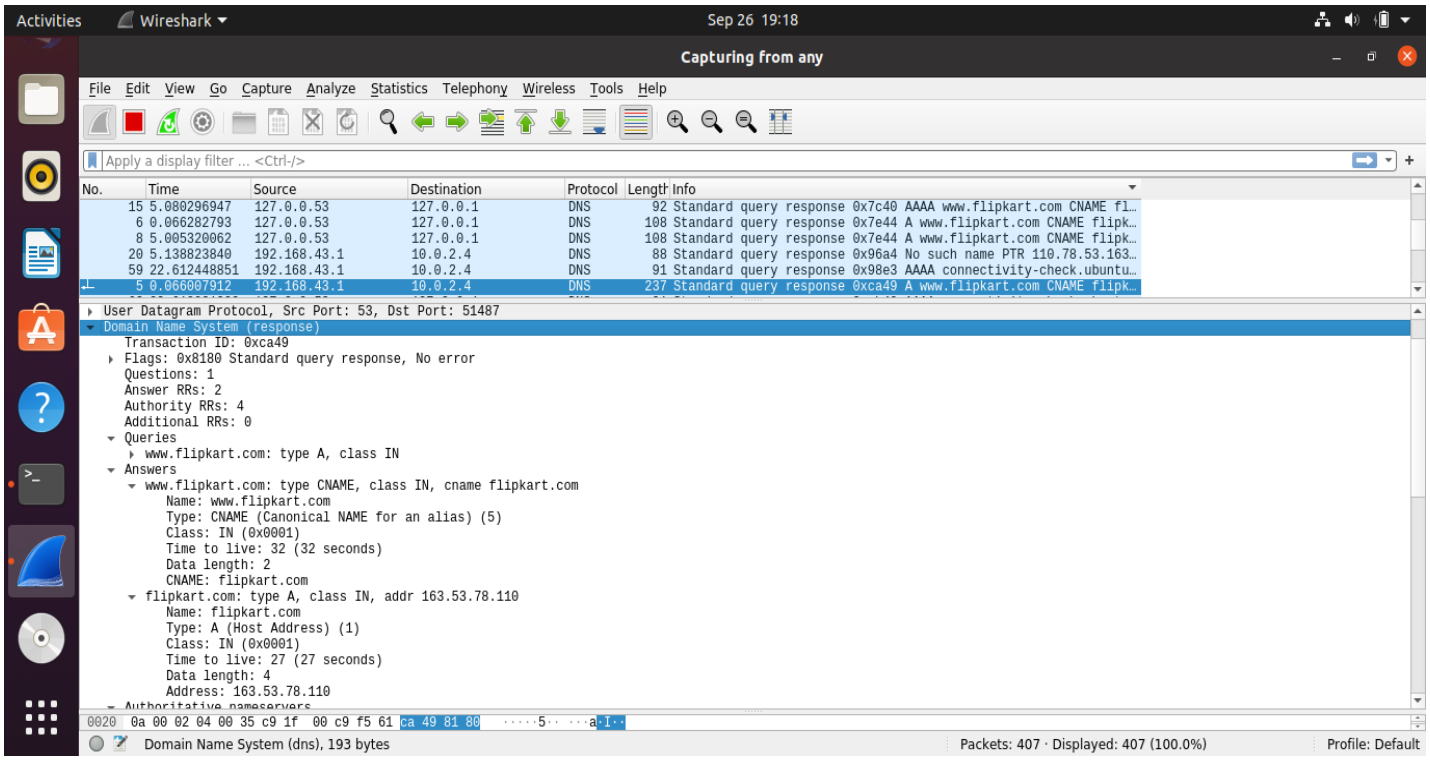
CLIENT MACHINE: 10.0.2.4 **SERVER MACHINE:10.0.2.15**

First 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).




Activities
Wireshark
Sep 26 19:15
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 127.0.0.1 127.0.0.53 DNS 78 Standard query 0x7e44 A www.flipkart.com
2 0.000168555 10.0.2.4 192.168.43.1 DNS 78 Standard query 0xca49 A www.flipkart.com
3 0.000695498 127.0.0.1 127.0.0.53 DNS 78 Standard query 0x7c40 AAAA www.flipkart.com
4 0.000863170 10.0.2.4 192.168.43.1 DNS 78 Standard query 0x0329 AAAA www.flipkart.com
5 0.066007912 192.168.43.1 10.0.2.4 DNS 237 Standard query response 0xca49 A www.flipkart.com CNAME flipk…
6 0.066282793 127.0.0.53 127.0.0.1 DNS 108 Standard query response 0x7e44 A www.flipkart.com CNAME flipk…
7 5.005026687 127.0.0.1 127.0.0.53 DNS 78 Standard query 0x7e44 A www.flipkart.com
8 5.005320062 127.0.0.53 127.0.0.1 DNS 108 Standard query response 0x7e44 A www.flipkart.com CNAME flipk…
9 5.005522418 10.0.2.4 192.168.43.1 DNS 74 Standard query 0x6140 AAAA flipkart.com
10 5.005800814 127.0.0.1 127.0.0.53 DNS 78 Standard query 0x7c40 AAAA www.flipkart.com
Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 192.168.43.1
User Datagram Protocol, Src Port: 51487, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xca49
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.flipkart.com: type A, class IN
[Response In: 5]
0000 00 04 00 01 00 06 08 00 27 57 91 24 00 00 08 00
0010 45 00 00 3e 70 1b 40 00 40 11 d2 e6 0a 00 02 04
0020 c0 a8 2b 01 c9 1f 00 35 00 2a f7 e8 ca 49 01 00
0030 00 01 00 00 00 00 00 00 03 77 77 77 08 66 6c 69
0040 70 6b 61 72 74 03 63 6f 6d 00 00 01 00 01
Domain Name System (dns), 34 bytes
Packets: 50 · Displayed: 50 (100.0%)
Profile: Default

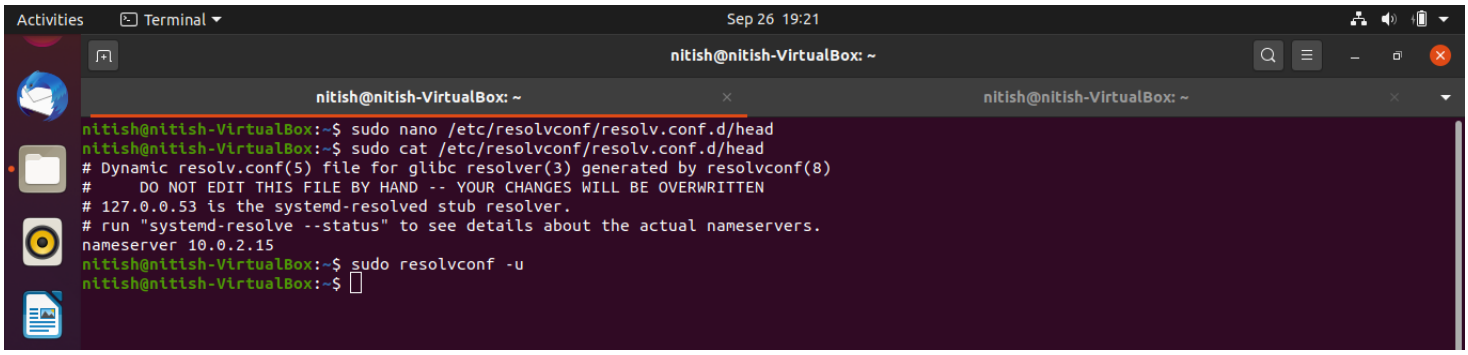

Activities
Wireshark
Sep 26 19:18
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
15 5.080296947 127.0.0.53 127.0.0.1 DNS 92 Standard query response 0x7c40 AAAA www.flipkart.com CNAME fl…
6 0.066282793 127.0.0.53 127.0.0.1 DNS 108 Standard query response 0x7e44 A www.flipkart.com CNAME flipk…
8 5.005320062 127.0.0.53 127.0.0.1 DNS 108 Standard query response 0x7e44 A www.flipkart.com CNAME flipk…
20 5.138823840 192.168.43.1 10.0.2.4 DNS 88 Standard query response 0x96a4 No such name PTR 110.78.53.163…
59 22.612448851 192.168.43.1 10.0.2.4 DNS 91 Standard query response 0x98e3 AAAA connectivity-check.ubuntu…
5 0.066007912 192.168.43.1 10.0.2.4 DNS 237 Standard query response 0xca49 A www.flipkart.com CNAME flipk…
User Datagram Protocol, Src Port: 53, Dst Port: 51487
Domain Name System (response)
Transaction ID: 0xca49
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 4
Additional RRs: 0
Queries
www.flipkart.com: type A, 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: 32 (32 seconds)
Data length: 2
CNAME: flipkart.com
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: 27 (27 seconds)
Data length: 4
Address: 163.53.78.110
Authoritative nameservers
0020 0a 00 02 04 00 35 c9 1f 00 c9 f5 61 ca 49 81 80
Domain Name System (dns), 193 bytes
Packets: 407 · Displayed: 407 (100.0%)
Profile: Default

Observations:-

1) First the source system (10.0.2.4) sends a query to the DNS server(192.168.43.55) requesting a type A RR (resource record) consisting of <hostname,IPv4>. It also sends a type AAAA RR requesting for <hostname,IPv6>.

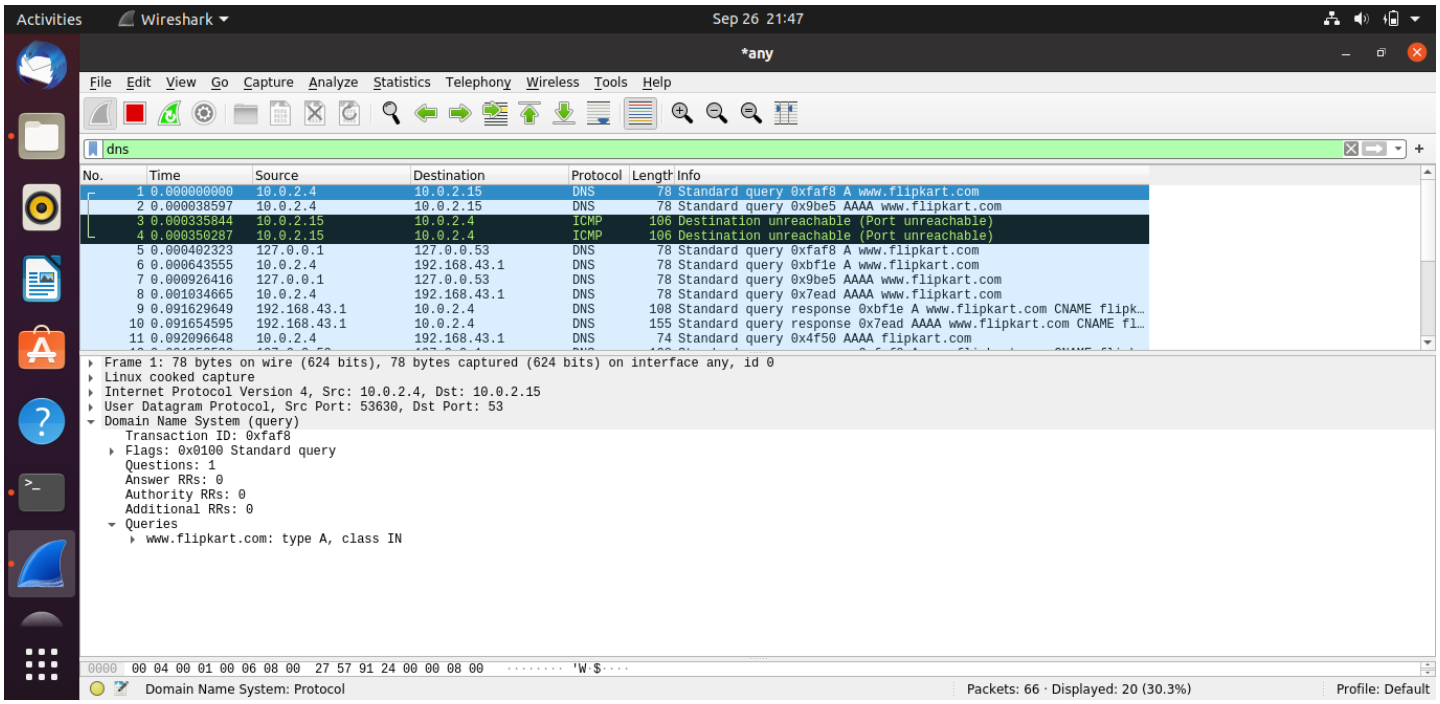
2) The DNS server then responds with 3 Answer RR's, specifying the hostname and IPv4.

TASK – 1: CONFIGURE THE USER/CLIENT MACHINE:-



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.



Observations:-

1) The DNS query is sent from the user(10.0.2.4) to the local DNS nameserver(10.0.2.15).

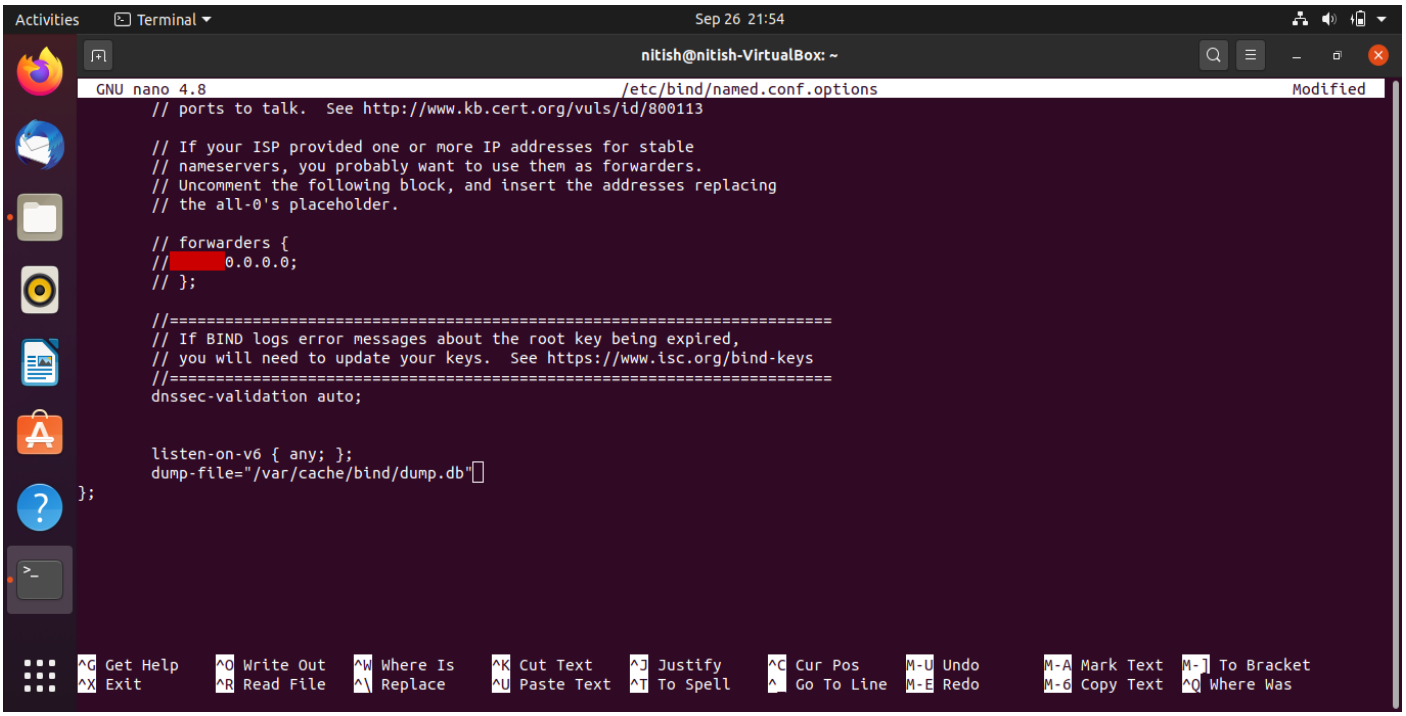
2) The response is not received from the local DNS server as it is still not configured to act as a DNS server. (Hence the 'destination unreachable' message is displayed in the WireShark capture.

TASK – 2: Set Up a Local DNS Server

$ sudo apt-get update

$ sudo apt-get install bind9

Step 1: Configure the BIND9 Server.



Step 2: Start DNS server

We start the DNS server using the command:

$ sudo service bind9 restart

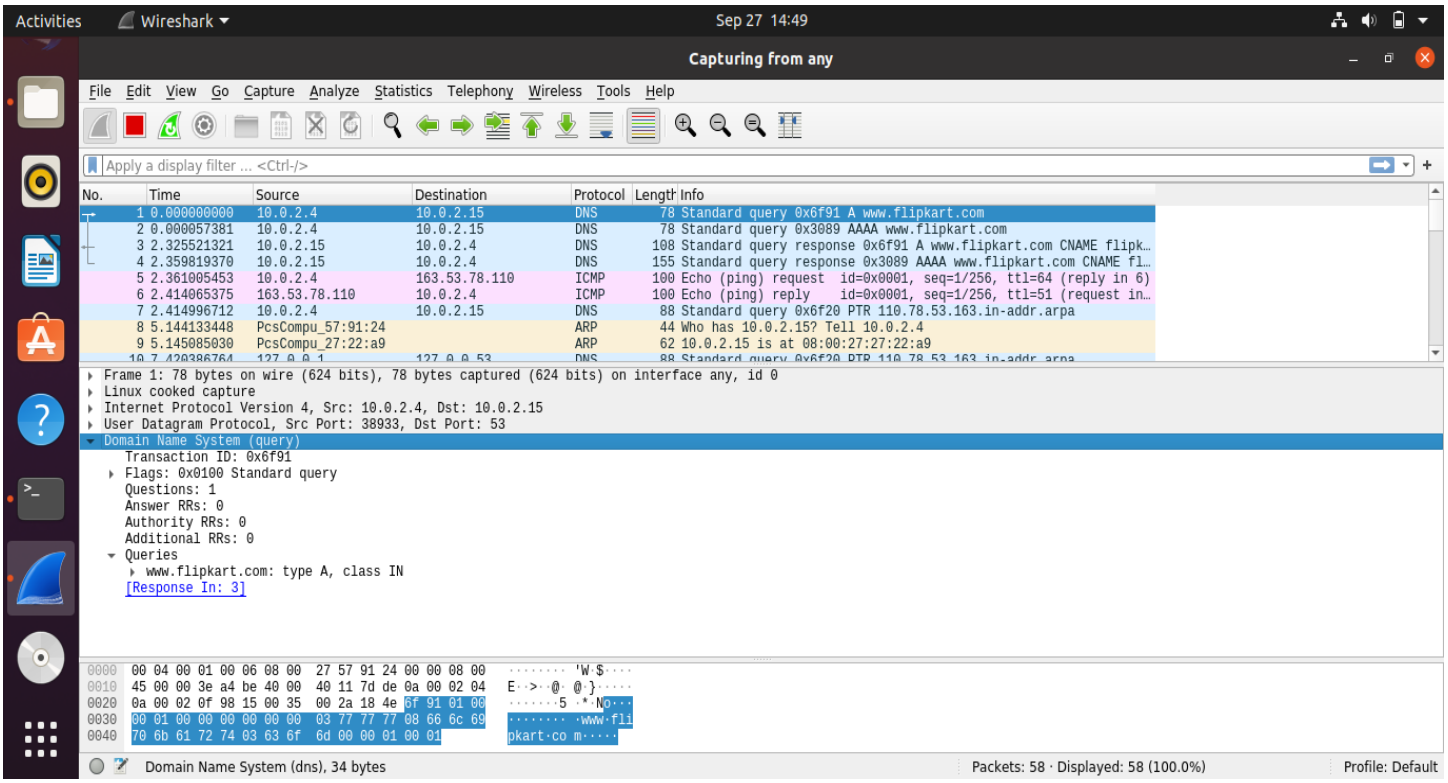
The two commands shown below are related to DNS cache. The first command dumps the content of the cache to the file specified above, and the second command clears the cache.

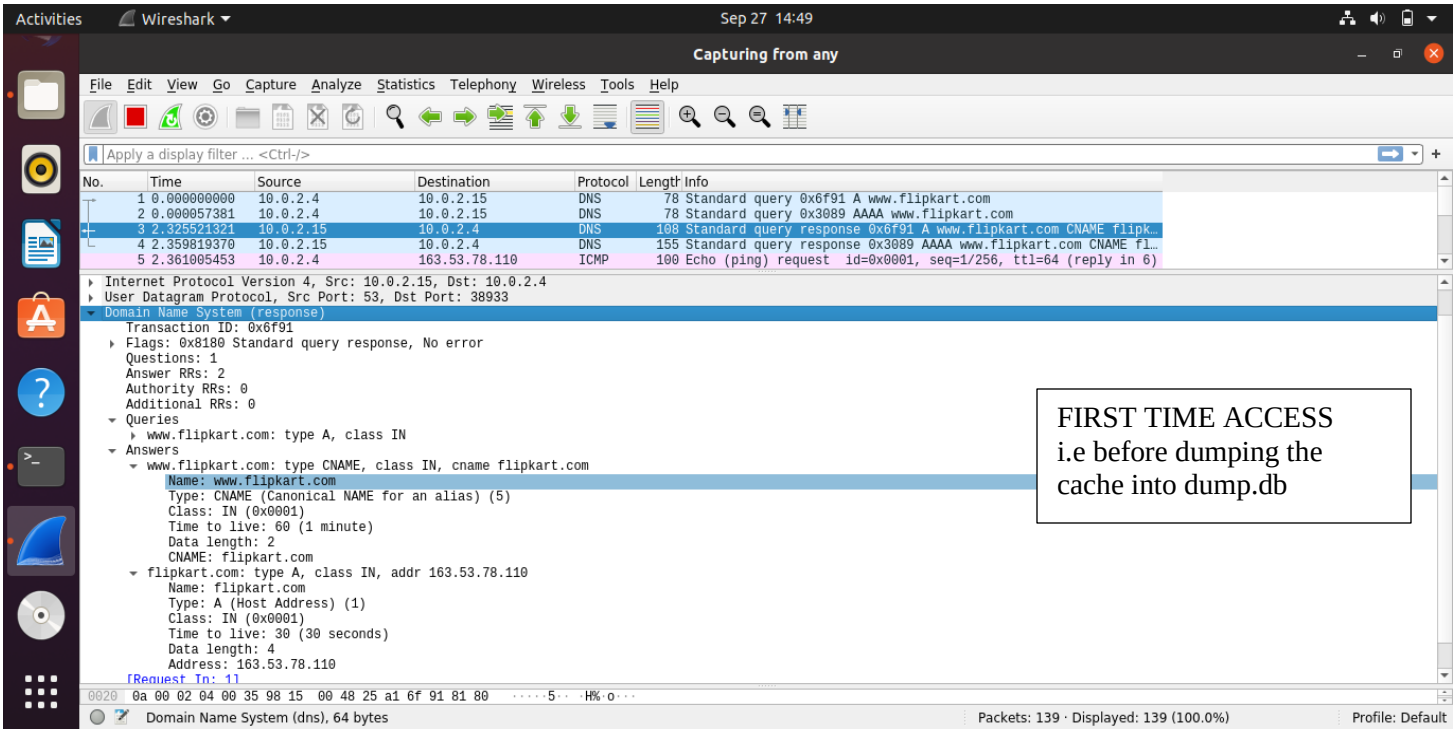
$ sudo rndc dumpdb -cache

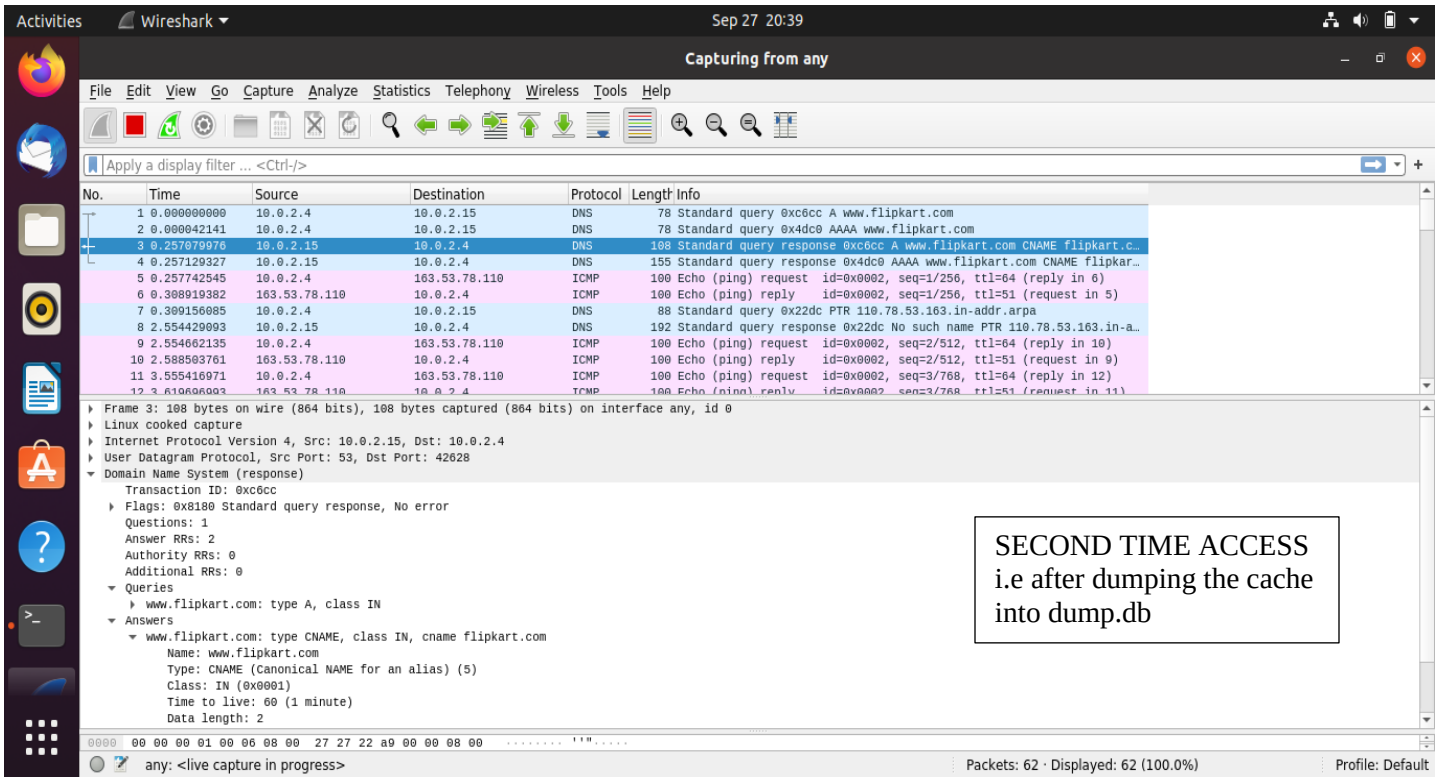
$ sudo rndc flush

Step 3: Use the DNS server
Third Test:

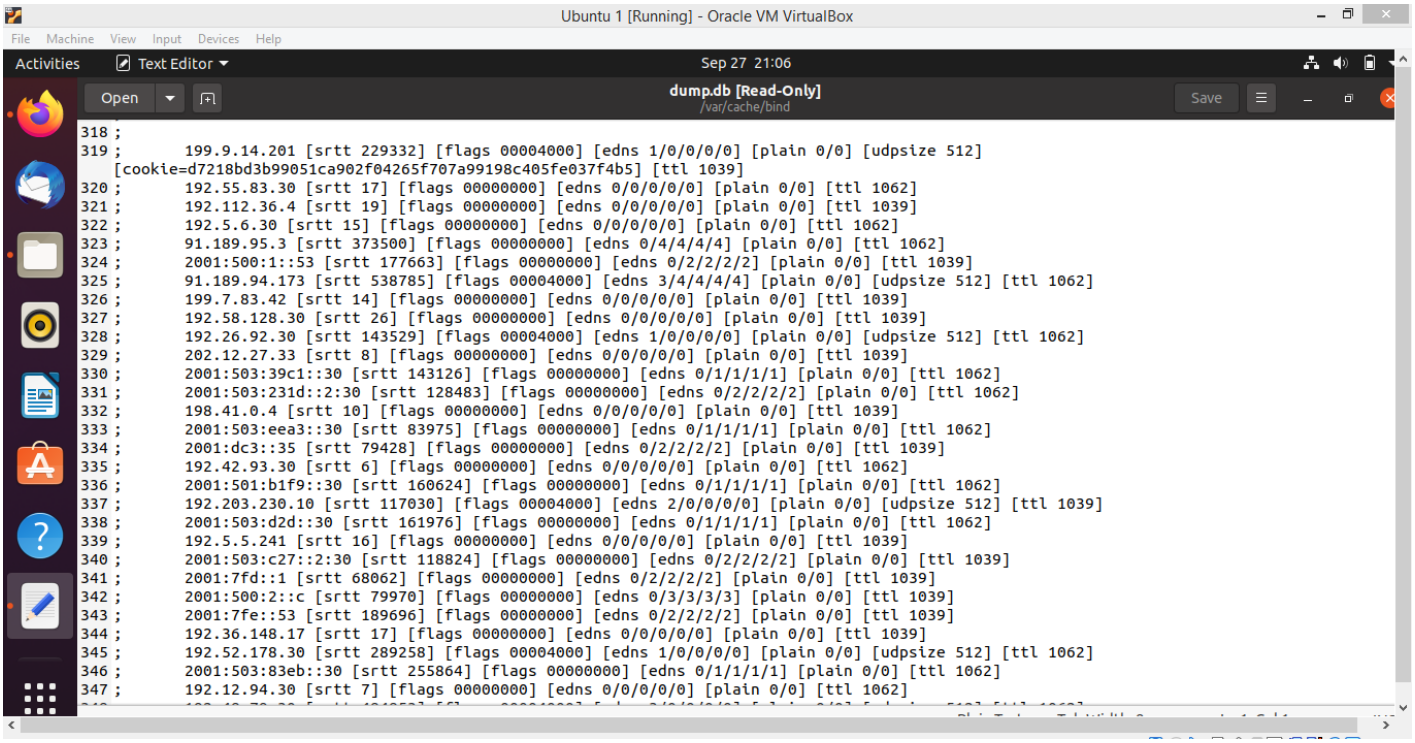
In the user machine (10.0.2.4), and ping a computer such as www.flipkart.com and describe your observation. Please use Wireshark to show the DNS query triggered by your ping command. Please also indicate when the DNS cache is used. (Take a screenshot)







SECOND TIME ACCESS
i.e after dumping the cache into dump.db



OBSERVATIONS:-

1) The DNS query is sent from the client machine 10.0.2.4 to the local DNS server machine 10.0.2.15.

2) We can observe that when the ping command is done for the first time, the time taken to obtain the query response from 10.0.2.15 is **2.3255sec.**

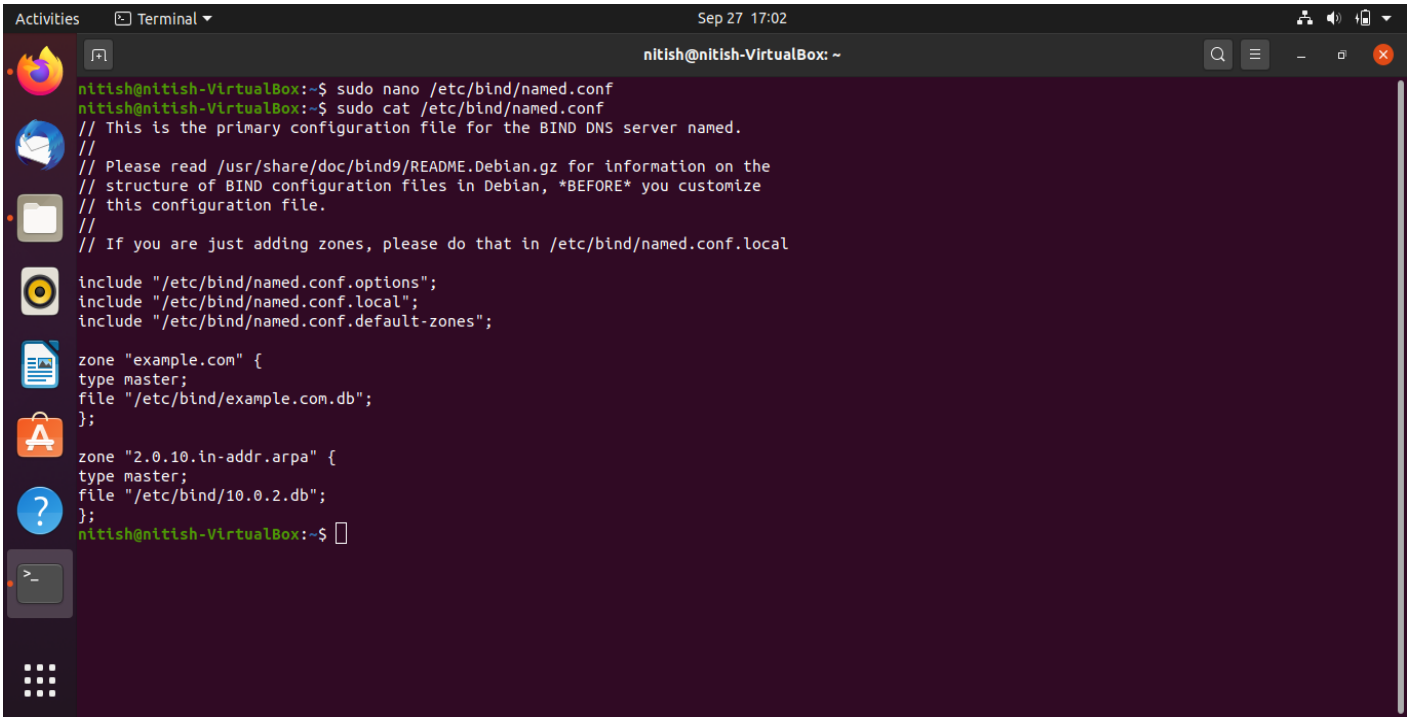
But when the ping command is run from the second time, the time taken to obtain query response from 10.0.2.15 is **0.2570sec.**

The time taken during the second time is less indicating that it is stored in the local cache of the local DNS server machine and hence faster response is obtained.

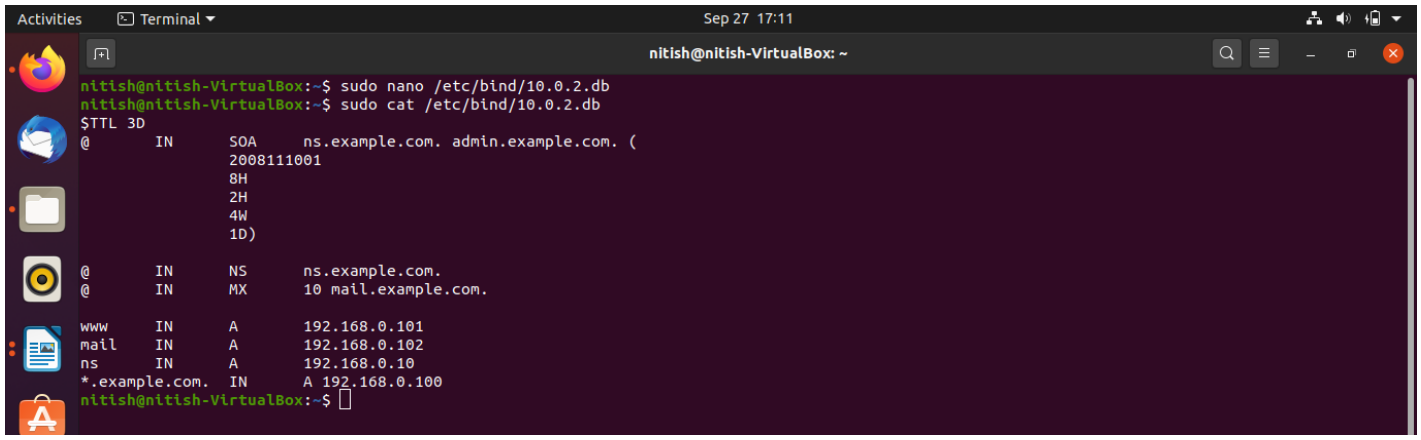
Task 3: Host a Zone in the Local DNS server.

Assume that we own a domain, we will be responsible for providing the definitive answer regarding this domain. We will use our local DNS server as the authoritative nameserver for the domain. In this lab, we will set up an authoritative server for the **example.com** domain.
This domain name is reserved for use in documentation, and is not owned by anybody, so it is safe to use it.

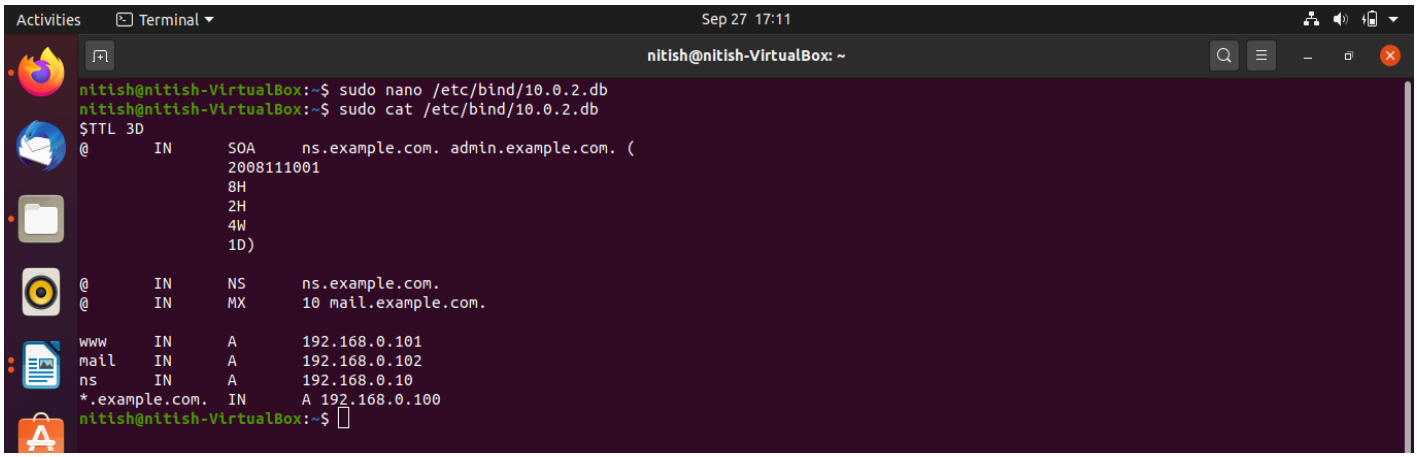
Step 1: Create Zones



Step 2: Setup the forward lookup zone file



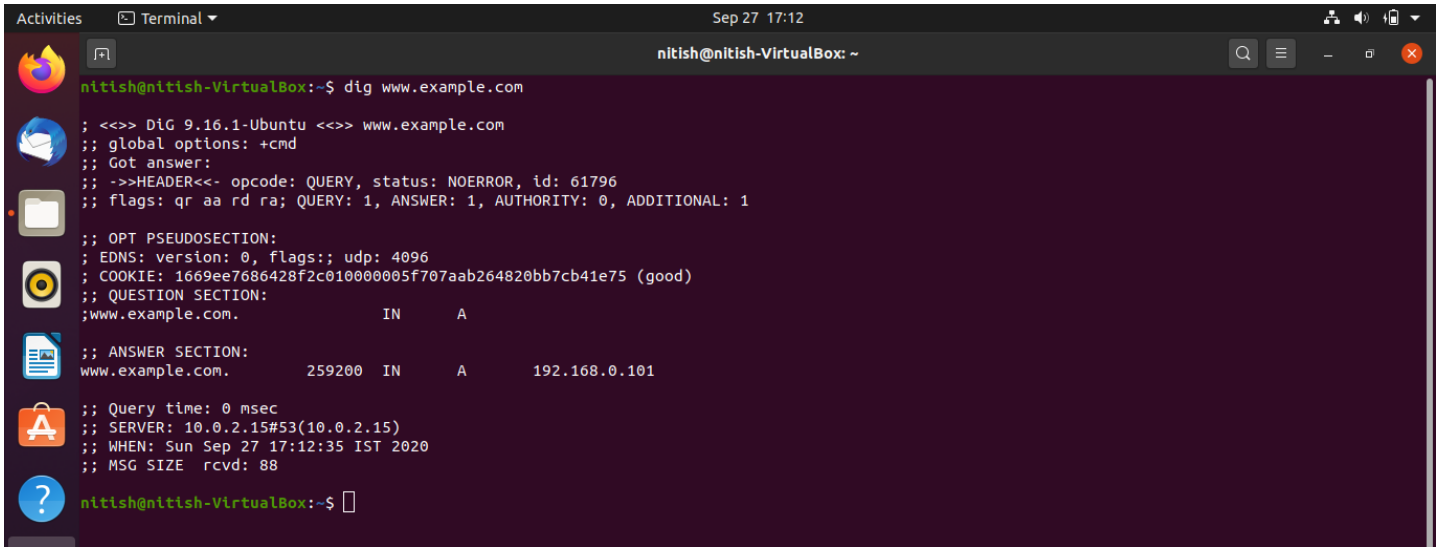
Step 3: Setup the reverse lookup zone file



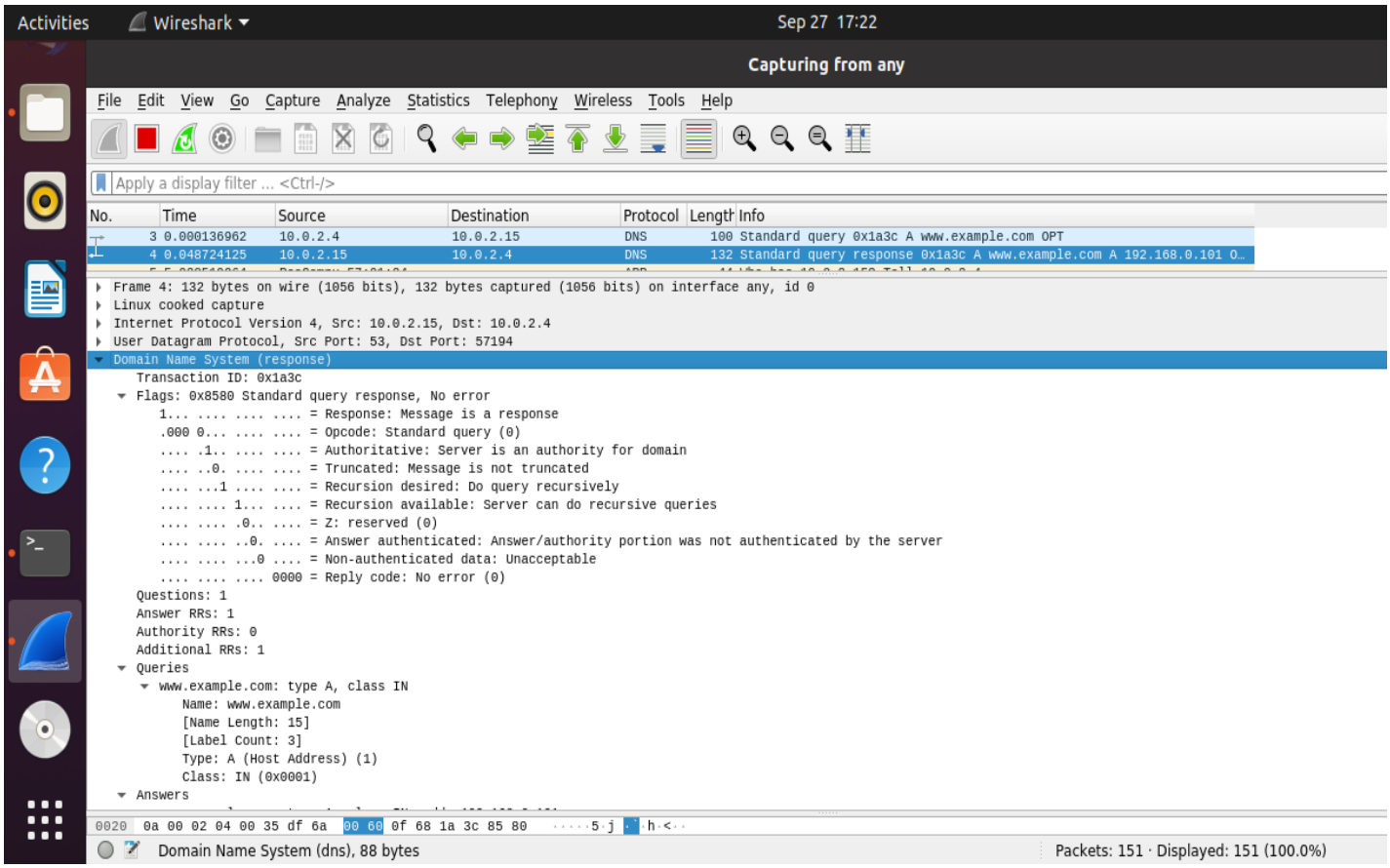
Task 4: Restart the BIND server and test

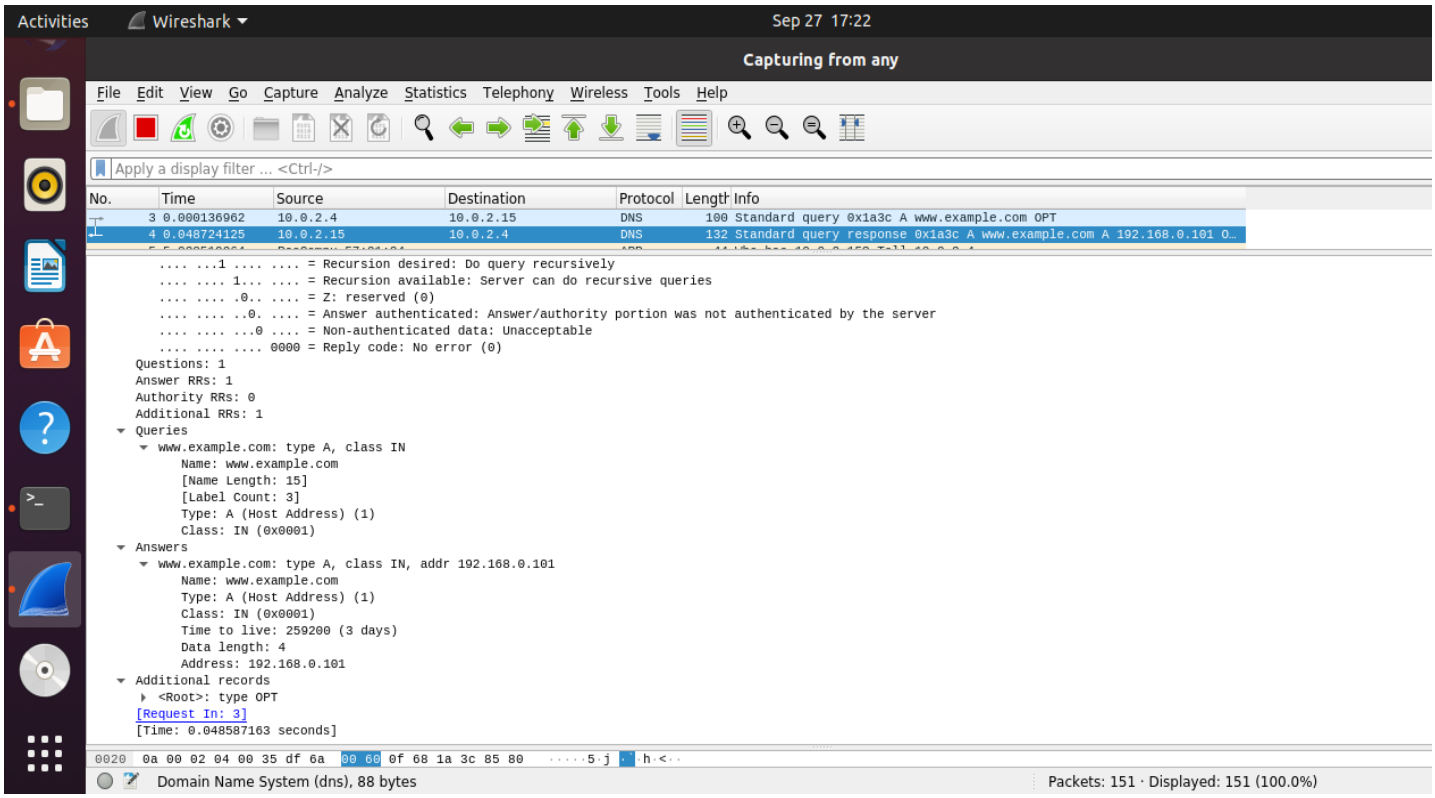
Step – 1:

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.



Step 2: Observe the results in Wireshark capture.



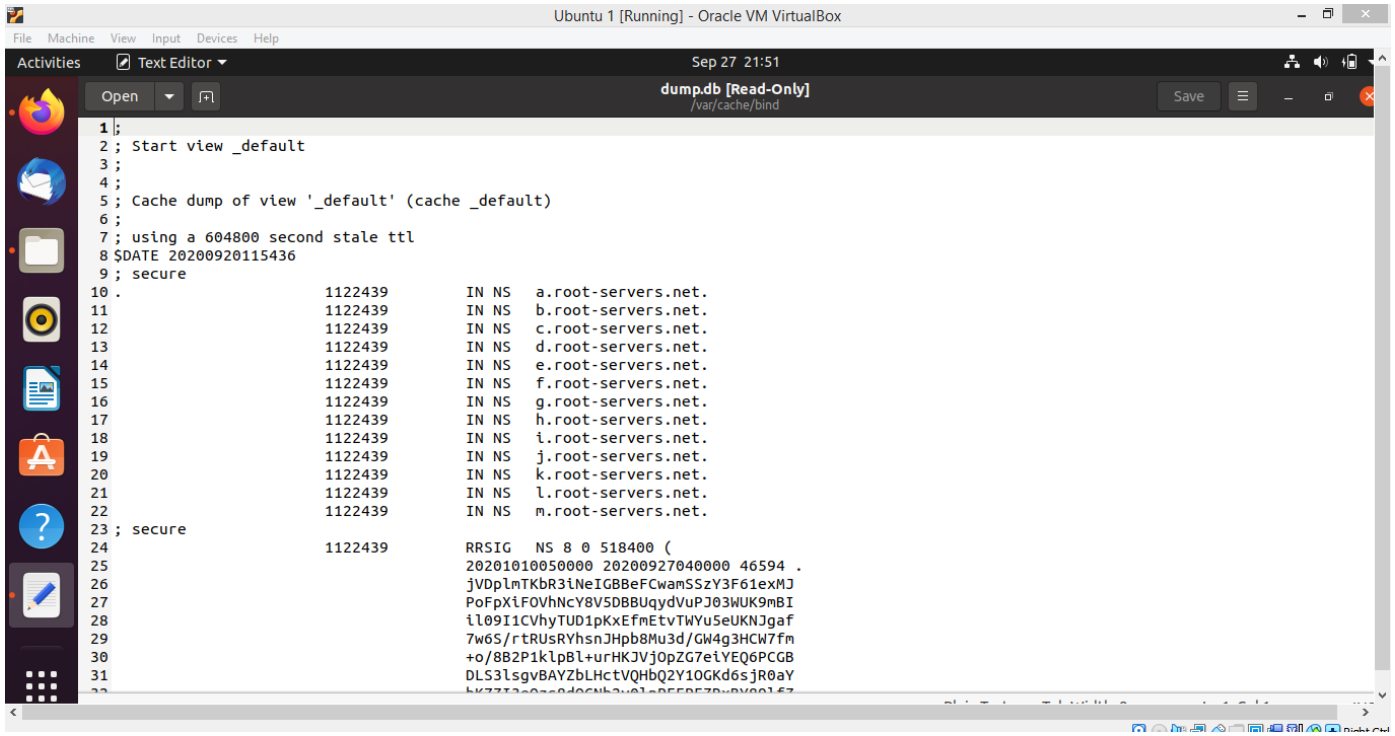


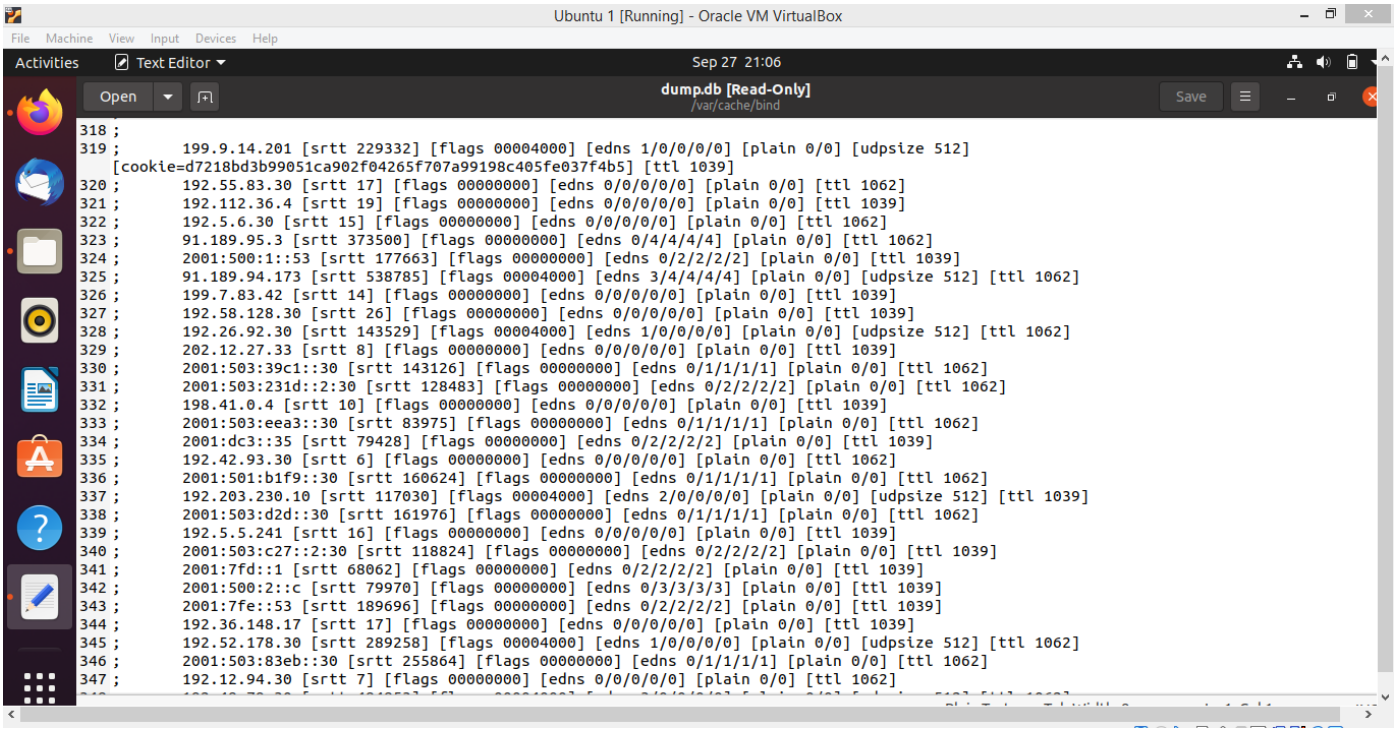
To load and clear DNS cache, use the below commands.

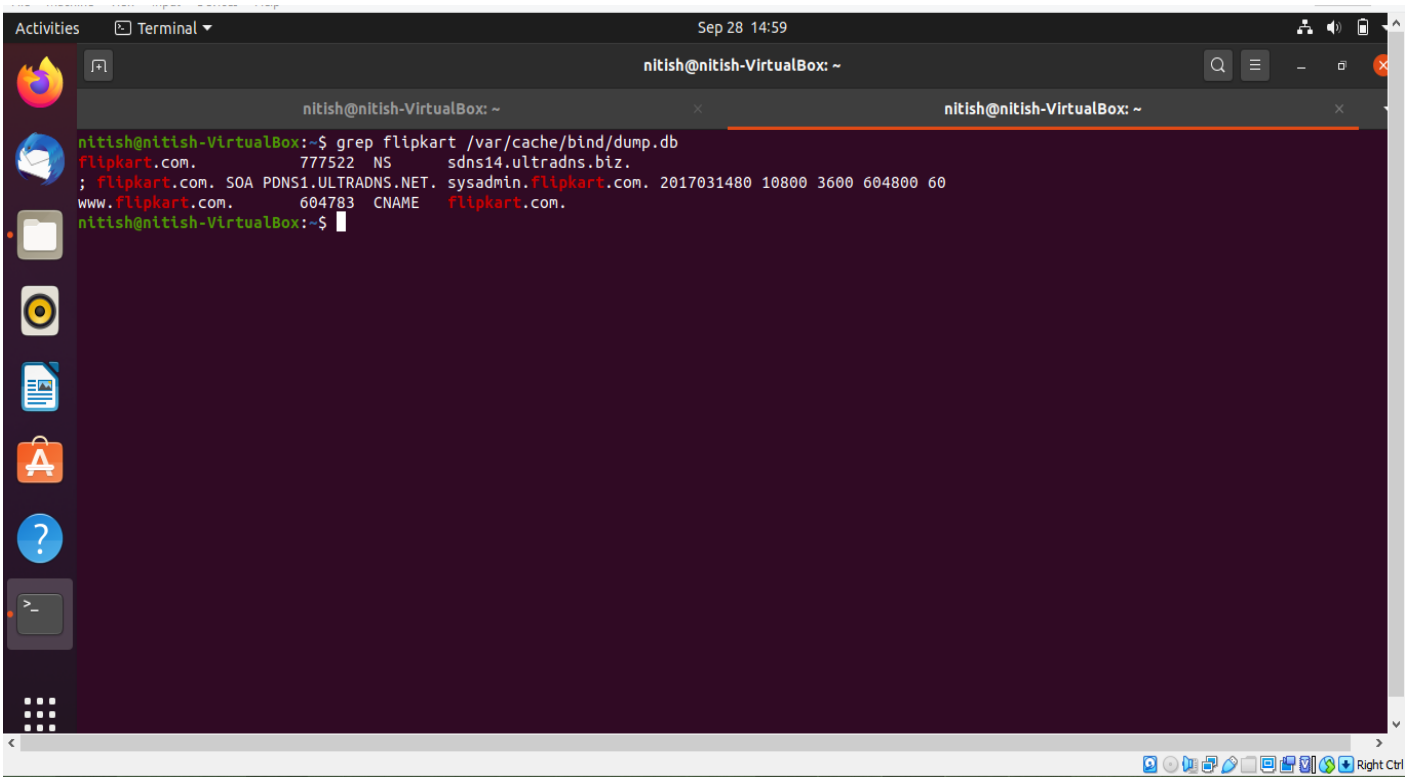
$ sudo rndc dumpdb -cache

$ sudo rndc flush

Local DNS Cache:-







Observation Notebook Requirements:

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

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

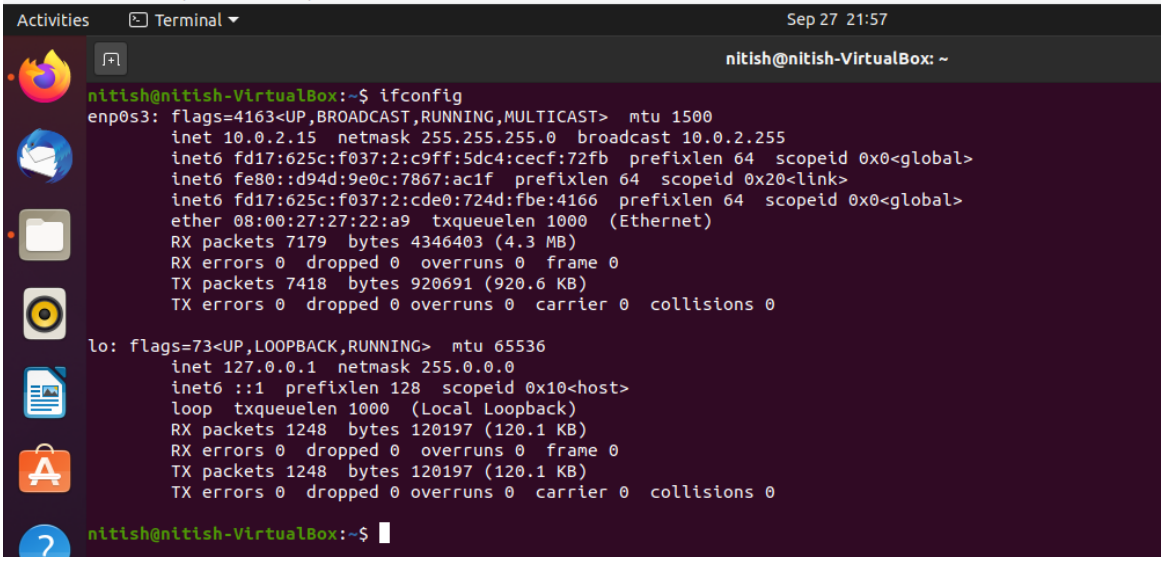
Ans:- The DNS query and response messages are shown above. They are sent over UDP.

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

Ans:- The destination port of the DNS query message is 53. The source port of DNS response message is also 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 message is sent to 10.0.2.15. The IPv4 of the DNS server is also 10.0.2.15. Both are the same.



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

Ans:- The type of DNS query message is **A (for IPv4)** and in some cases **AAAA (for IPv6)** too. The query message does not contain any **Answer RR** 's.

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

Ans:- The number of Answer RR's depends on the particular website.

Each one contains Name, Type, Class, TTL, Data length, Address.

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:- No, the destination IP addresses does not match with any of our IP addresses from DNS response message.