CN Lab Report – Week 4

PES1UG19CS582

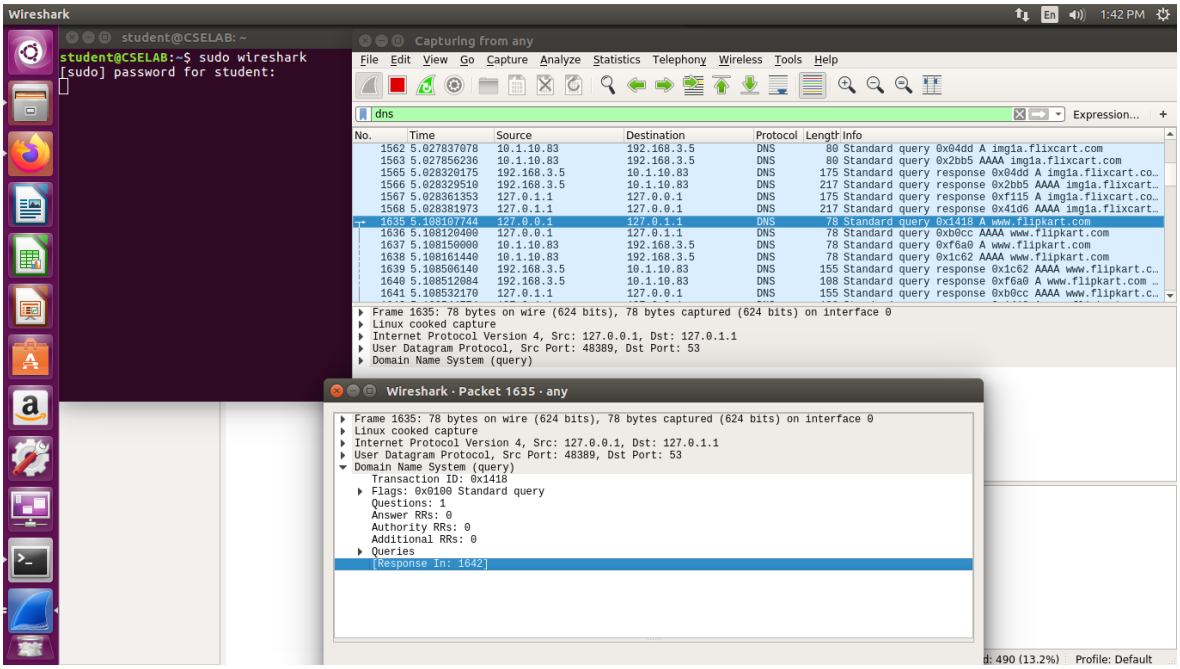
Vridhi Goyal

PES1UG19CS592

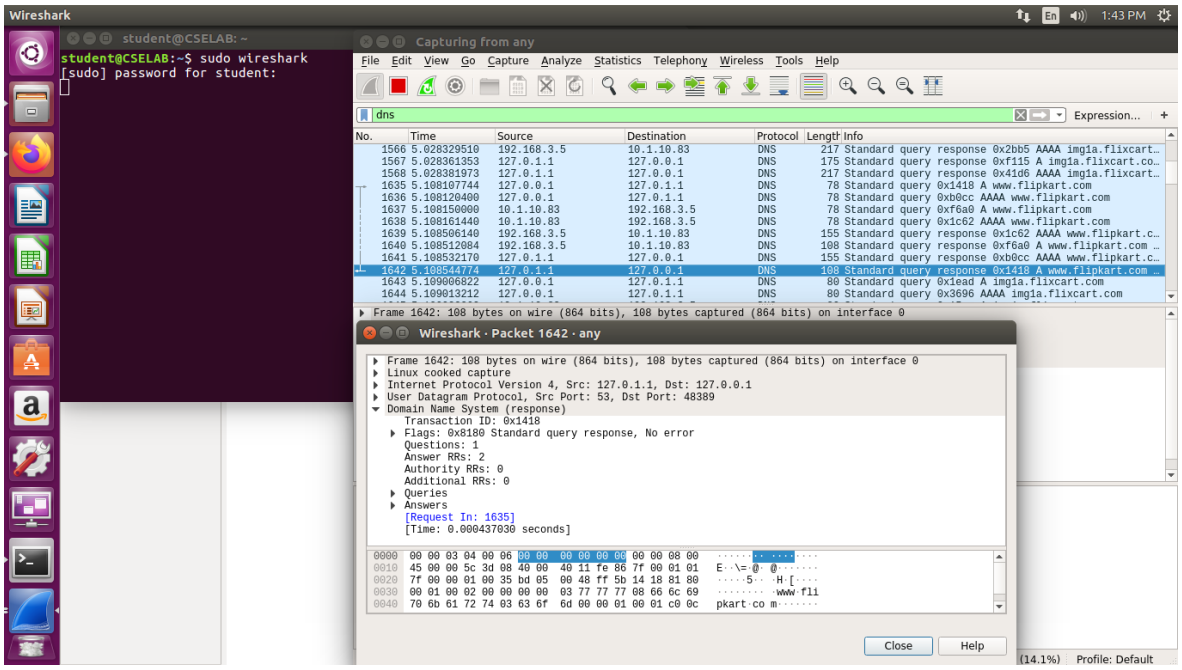
Yashi Chawla

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 **127.0.1.1**.
- 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 – **192.168.3.5**.
- The first query and authoritative response are shown below.



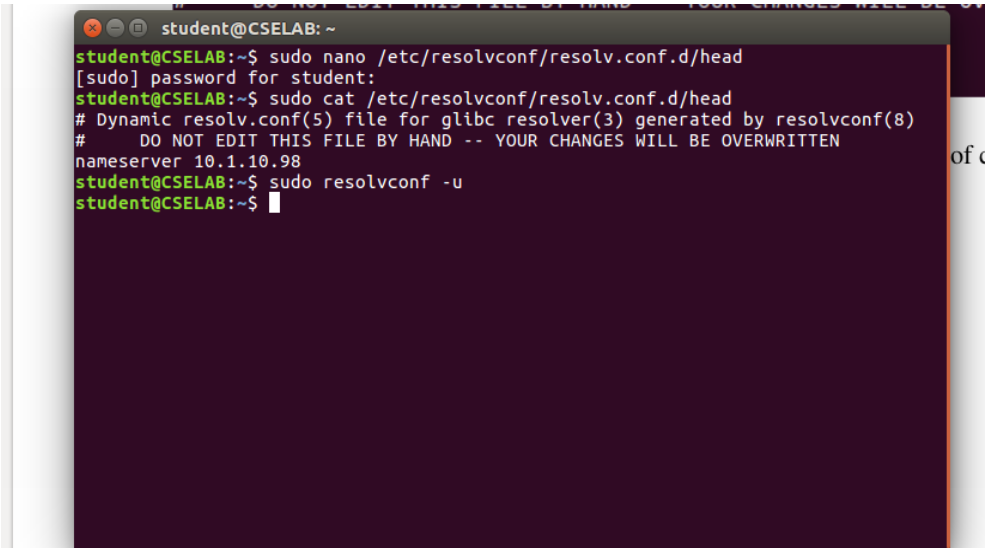
DNS Query



DNS Response

2. Task 1 – Configuring Client Machine

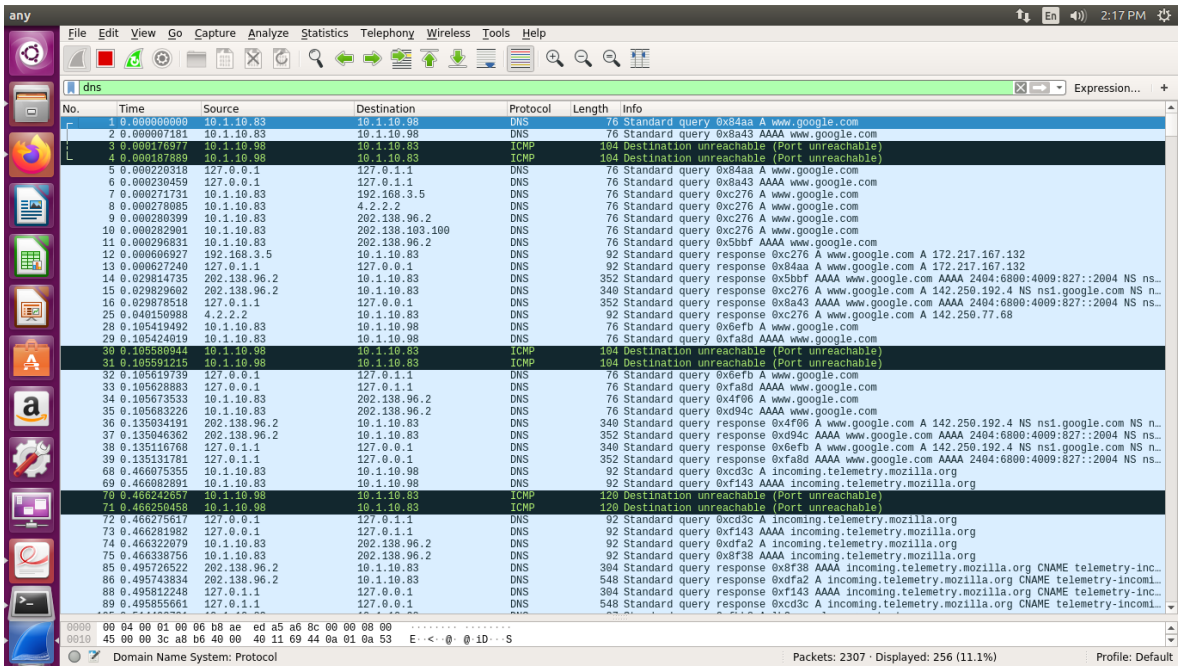
- The IP Address of the client machine is **10.0.10.98** and the IP Address of the server machine is **10.0.10.83**
- We need to add the IP Address of the custom DNS server (**10.0.10.83**) to the client machine.
- This is done by adding the IP address of the server to the file **/etc/resolvconf/resolv.conf.d/head** 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**



Reconfiguring name server resolution order

3. Second Test

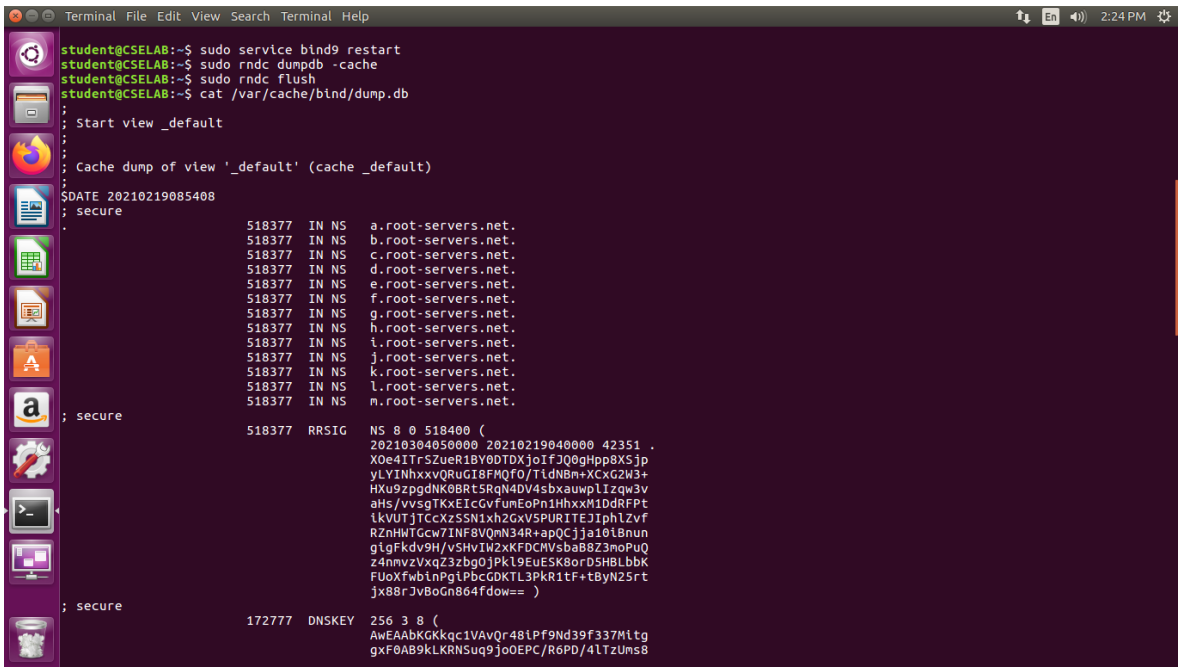
- The Flipkart website is pinged again, and Wireshark is used to capture packets.
- We obtain a destination unreachable error in Wireshark as the server machine does not have a DNS server associated with it.
- The client tries to obtain the DNS record from **10.0.10.83** but it does not receive any hence it resorts to using the default DNS server at **127.0.0.1.**



Wireshark Packet Capture

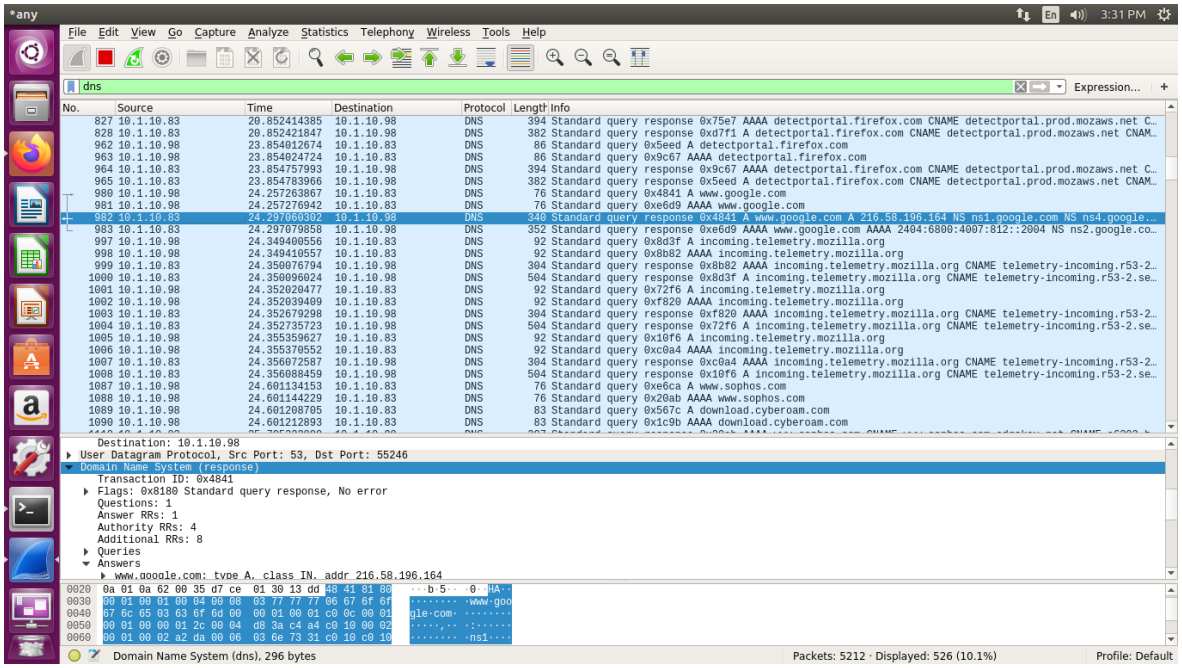
4. Task 2 – Setting Up Local DNS Server

- 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 the 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**.

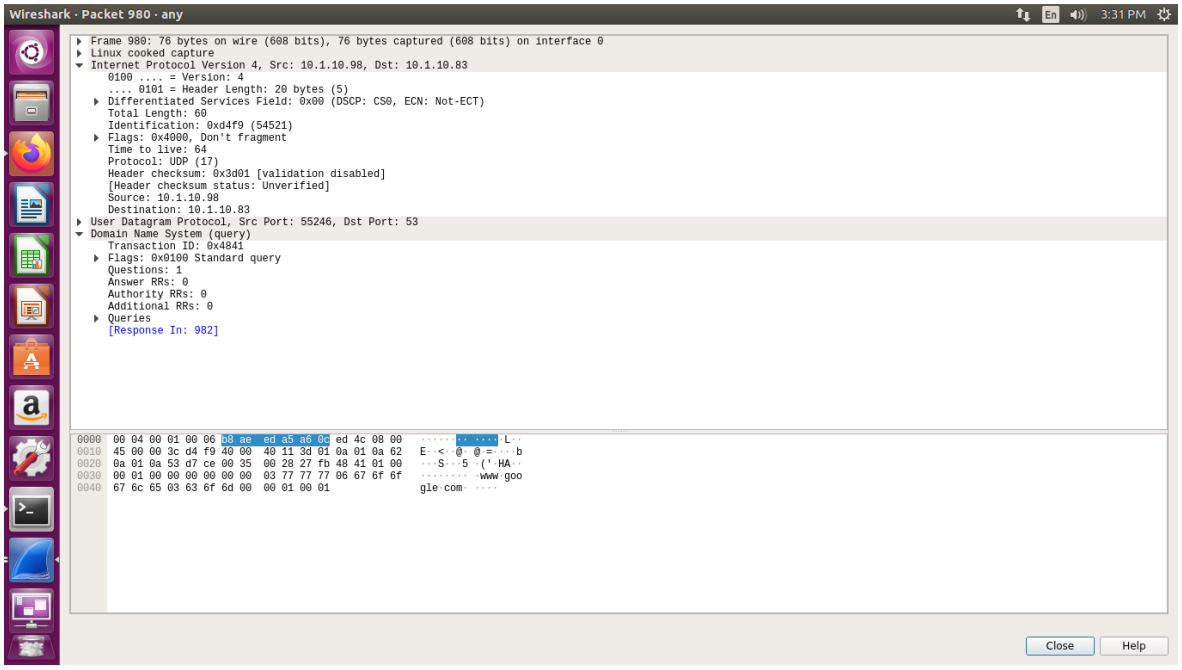


5. Third Test

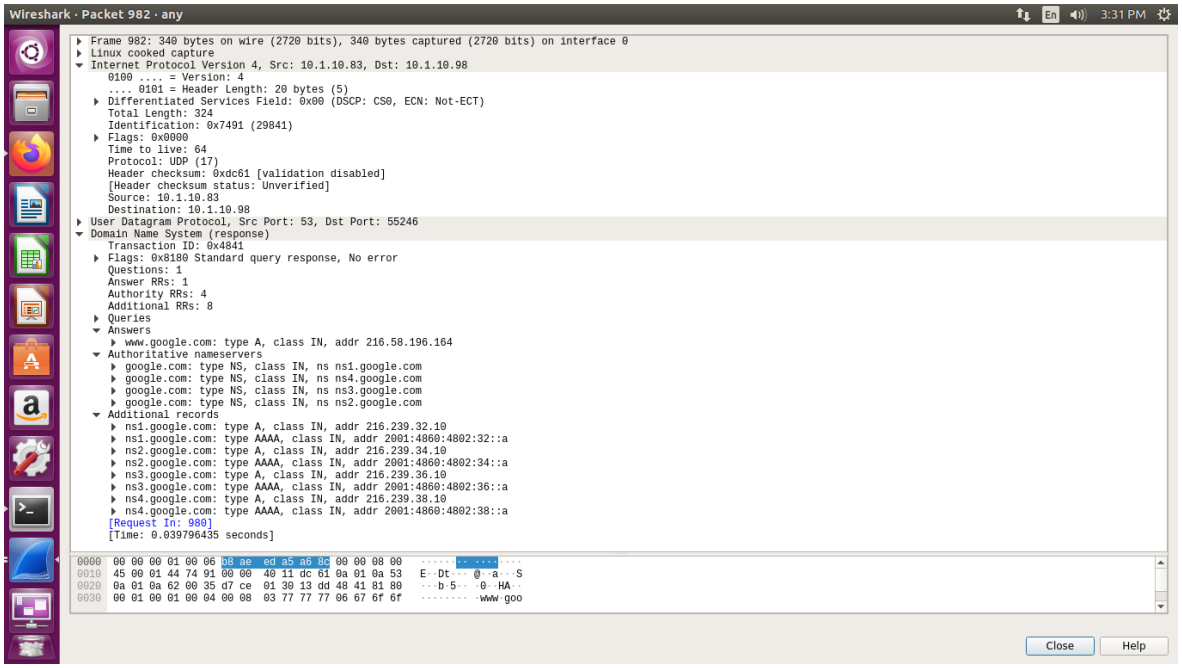
- The Flipkart website is pinged again with Wireshark running in the background.
- The IP Address of the local DNS server is clearly seen in the screenshots below.
- The cache is dumped into the dumpfile so it can be seen.
- The cache file also contains the canonical hostname and the A type records with the IP Address of the Google website.



Wireshark packet capture



Request

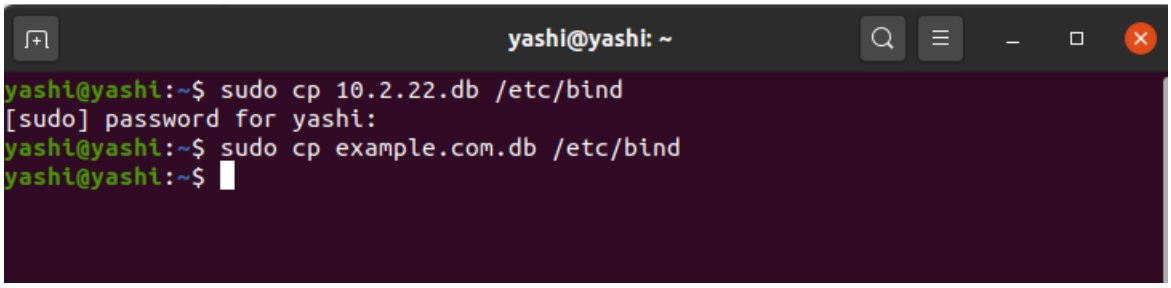


Response

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).



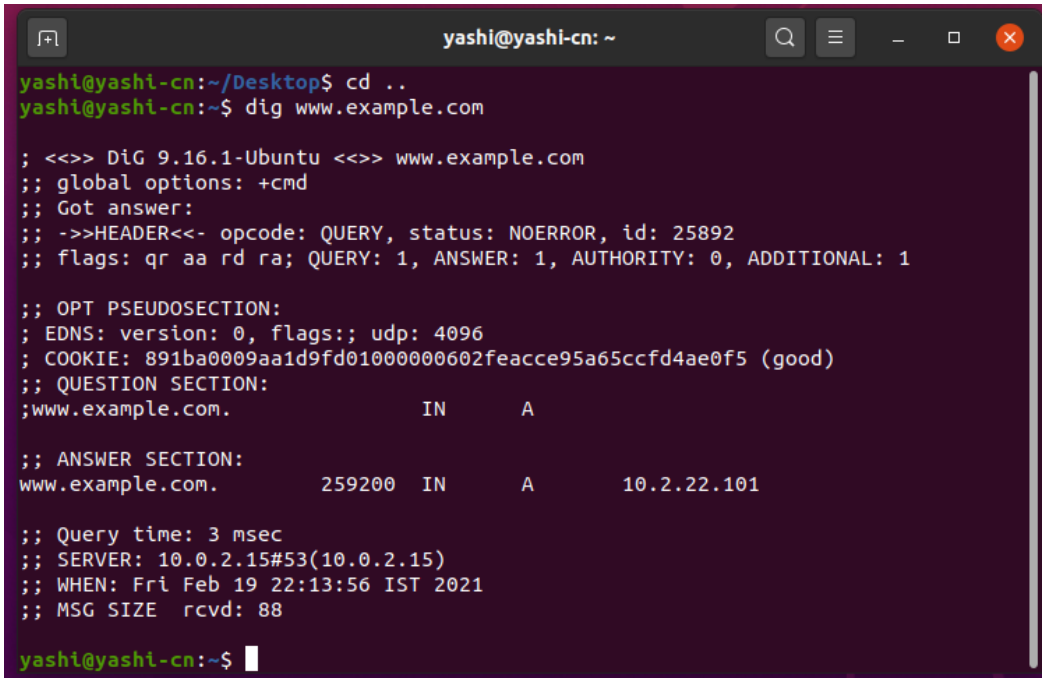
6.2 Forward and Reverse Lookup

- 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 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.

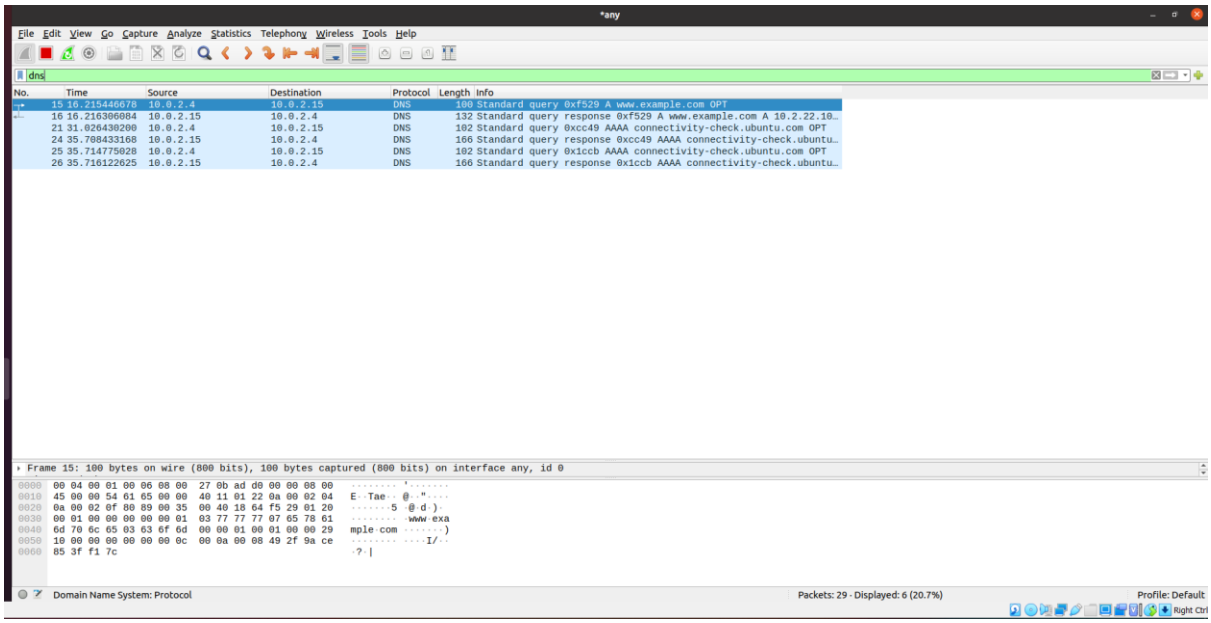
- The reverse lookup file is stored at **/etc/bind/10.0.2.db**and is used to translate IP Addresses to hostnames for the given domain, in this case example.com.
- For each IP Address defined in the forward lookup file, a corresponding hostname is referenced here.
- The record type here is PTR or DNS Pointer Record.

7. Fourth Test – Testing www.example.com

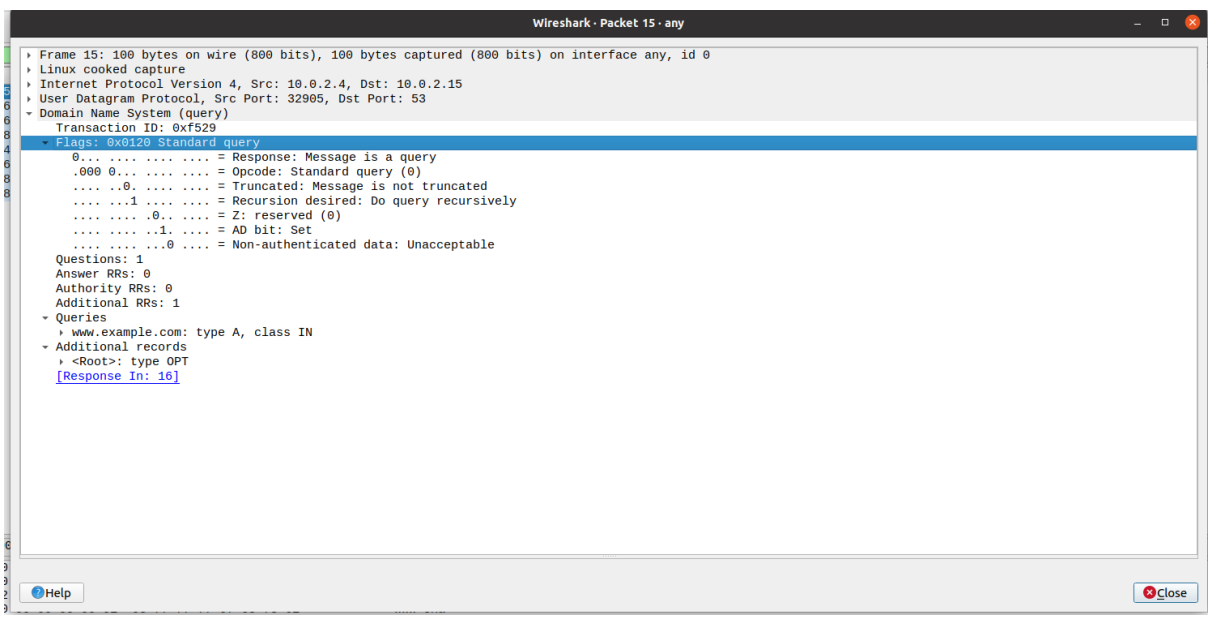
- The dig command is used to lookup name servers specified in the file **/etc/resolv.conf**
- Wireshark is used to capture the packets while running the command dig **www.example.com**
- The IP Address of the DNS Server and the returned IP Address of the domain set by us can be seen in the query and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



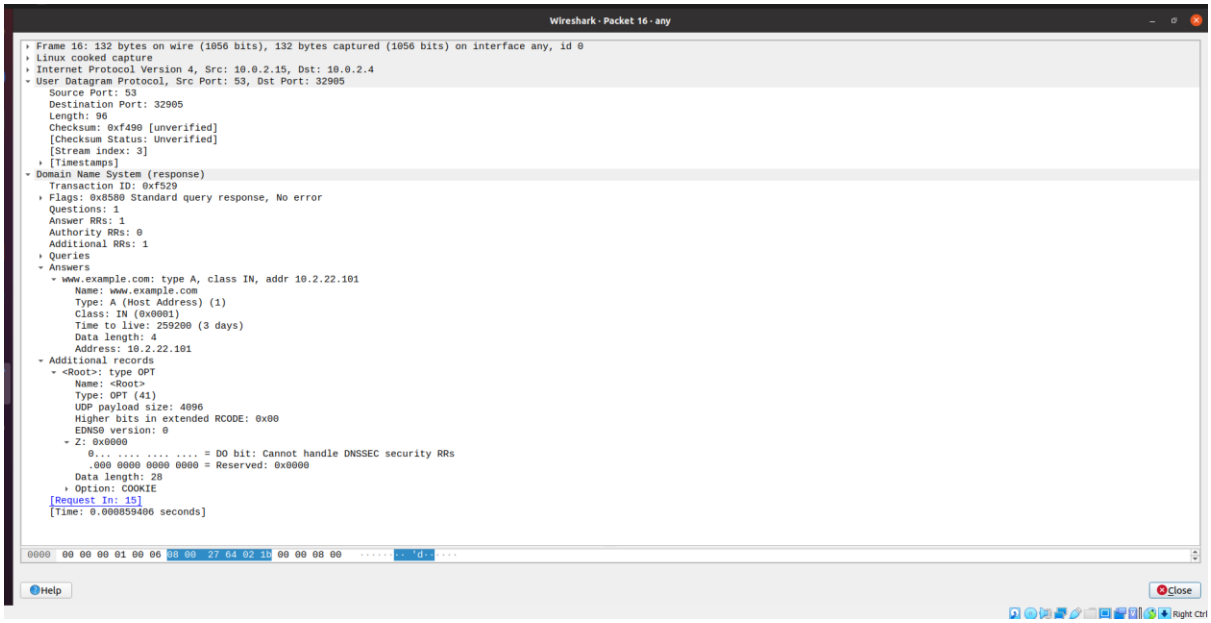
```
dig www.example.com
```



Wireshark Packet Capture



Request



Response

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.