**Week #4**

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

**Team Member 1:**

Name : Laxmikant Bhujang Gurav

SRN : PES1UG20CS658

Roll no.: 55

**Team Member 2:**

Name : Pavan Kumar Nuthi

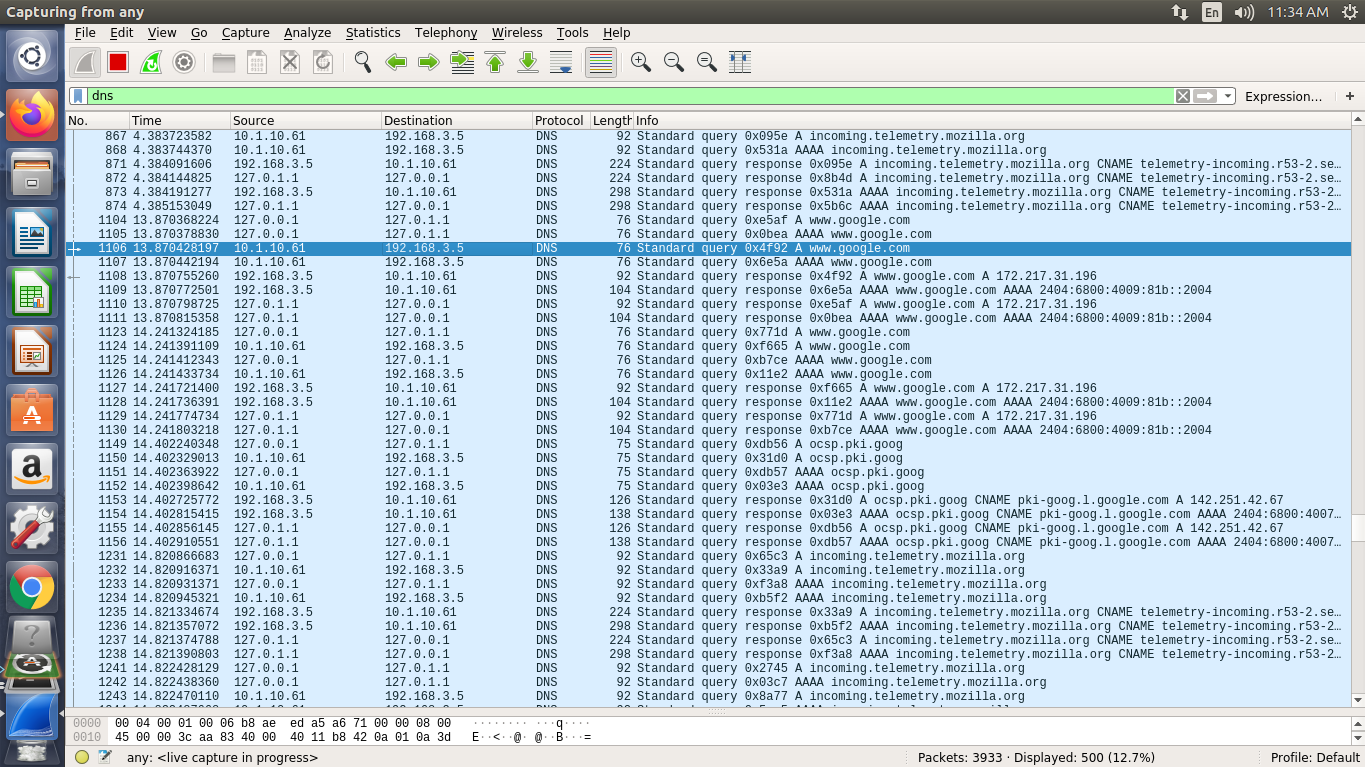
SRN : PES1UG20CS670

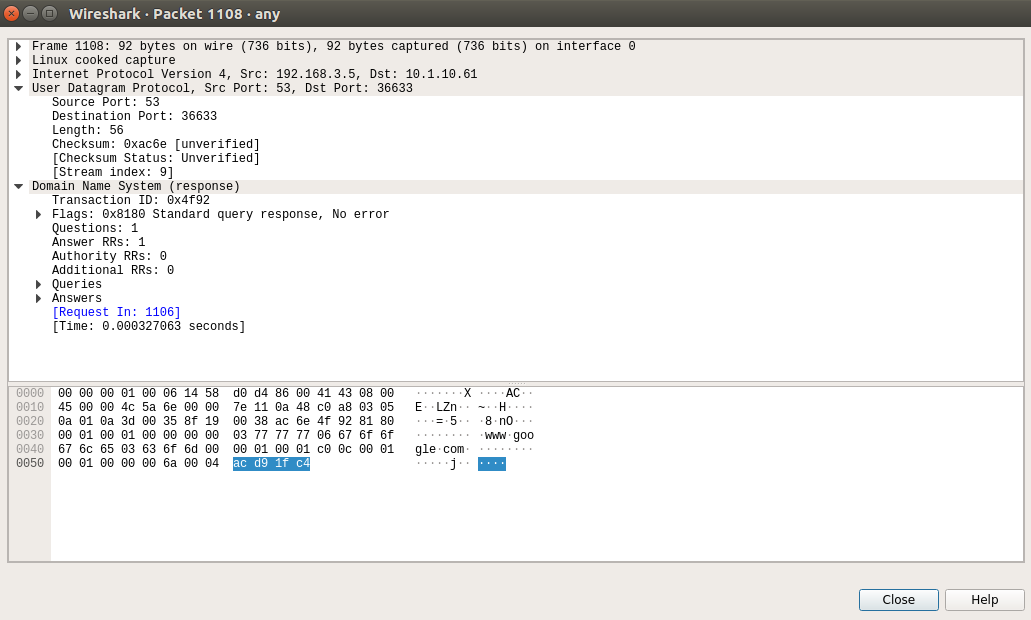
Roll no.: 31

**Observation 1:**

Ping a computer such as www.google.com (any domain). Please use Wireshark to show the DNS query triggered by your ping command and DNS response.

**WIRESHARK CAPTURE**

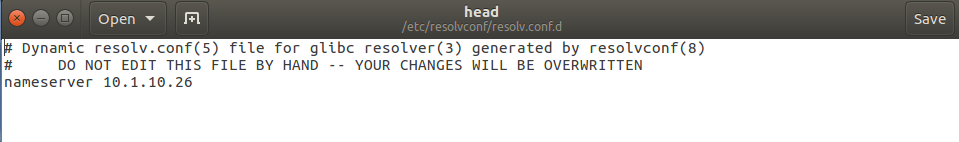


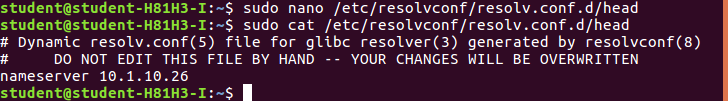


**Part 1: Setting Up a Local DNS Server**

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

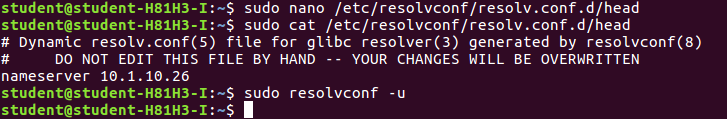
**1.1 Change the resolver configuration file (/etc/resolv.conf):**





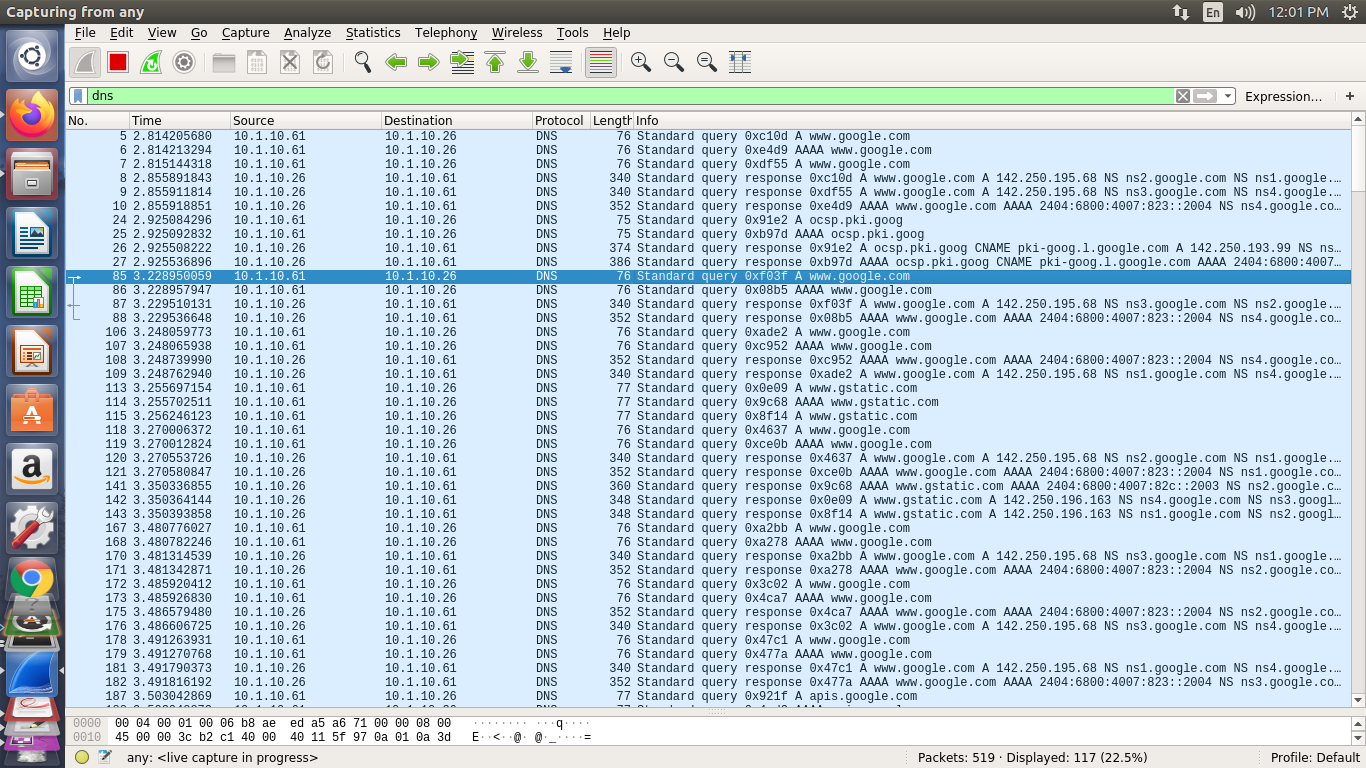
**1.2 Run the following command for the change to take effect.**

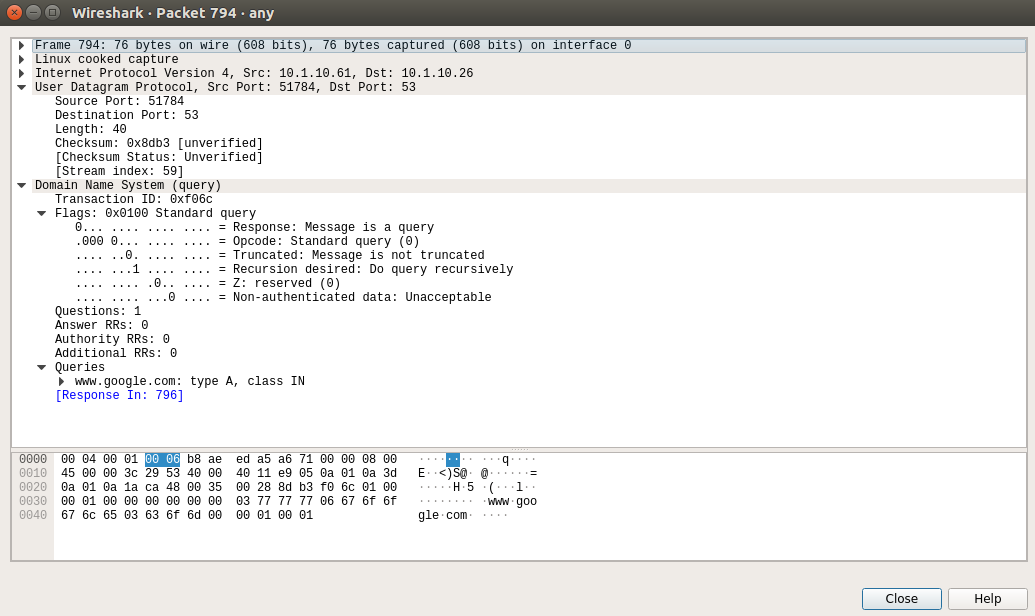
**sudo resolvconf -u**

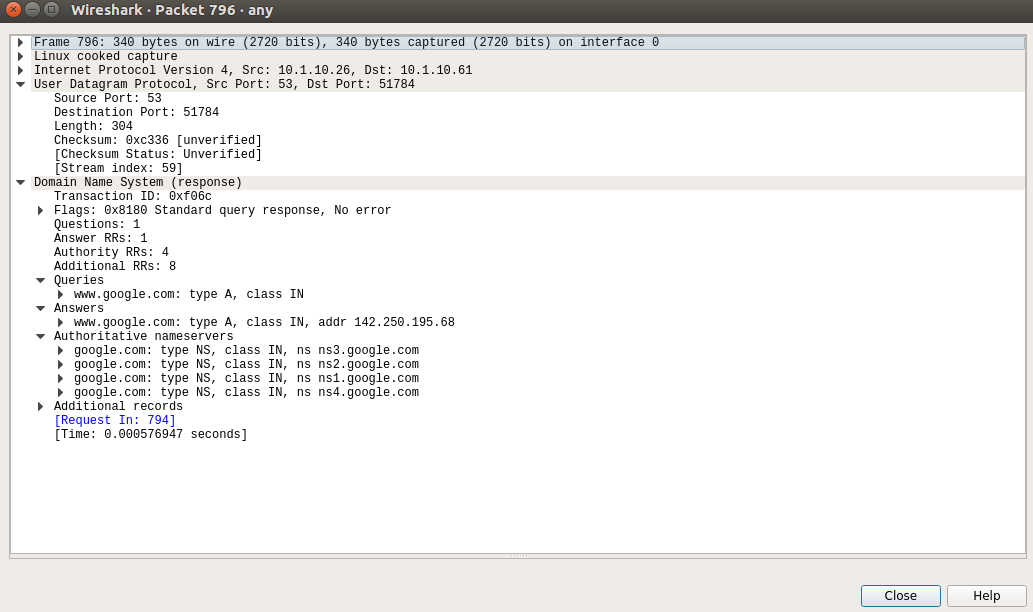


**Observation 2:**

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



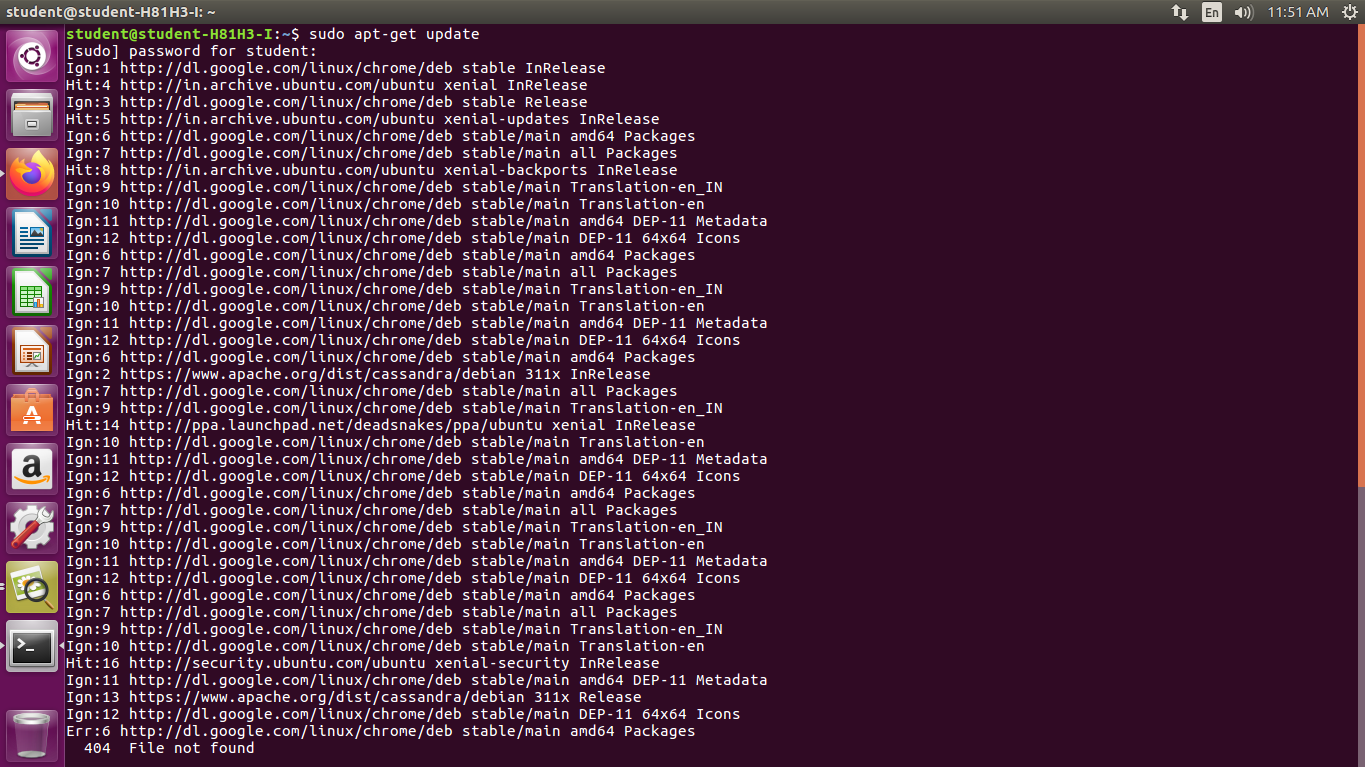




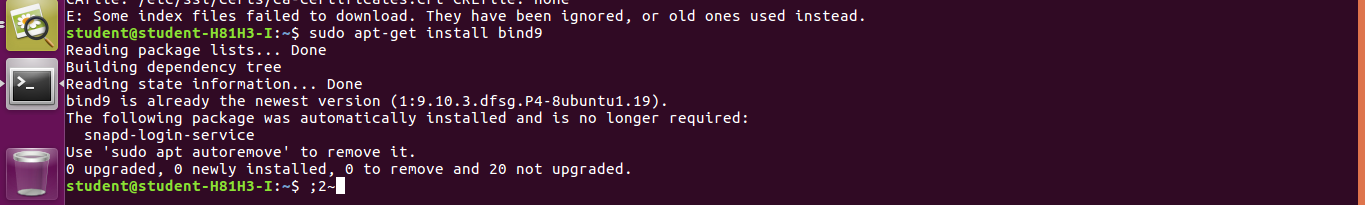
**Task 2: Set Up a Local DNS Server**

**2.1 Note: If bind9 server is not already installed, install using the command**

**$ sudo apt-get update**

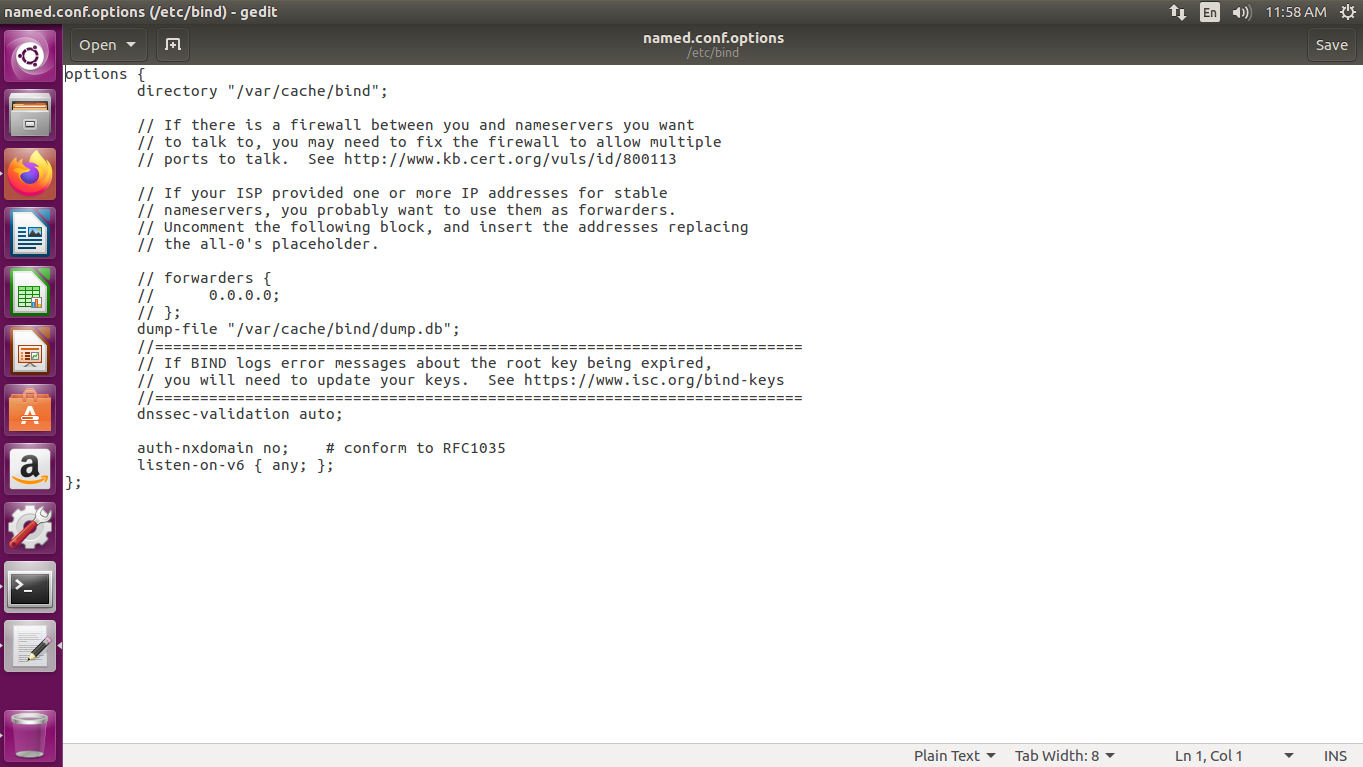


**$ sudo apt-get install bind9**



**2.2 Configure the BIND9 Server :**



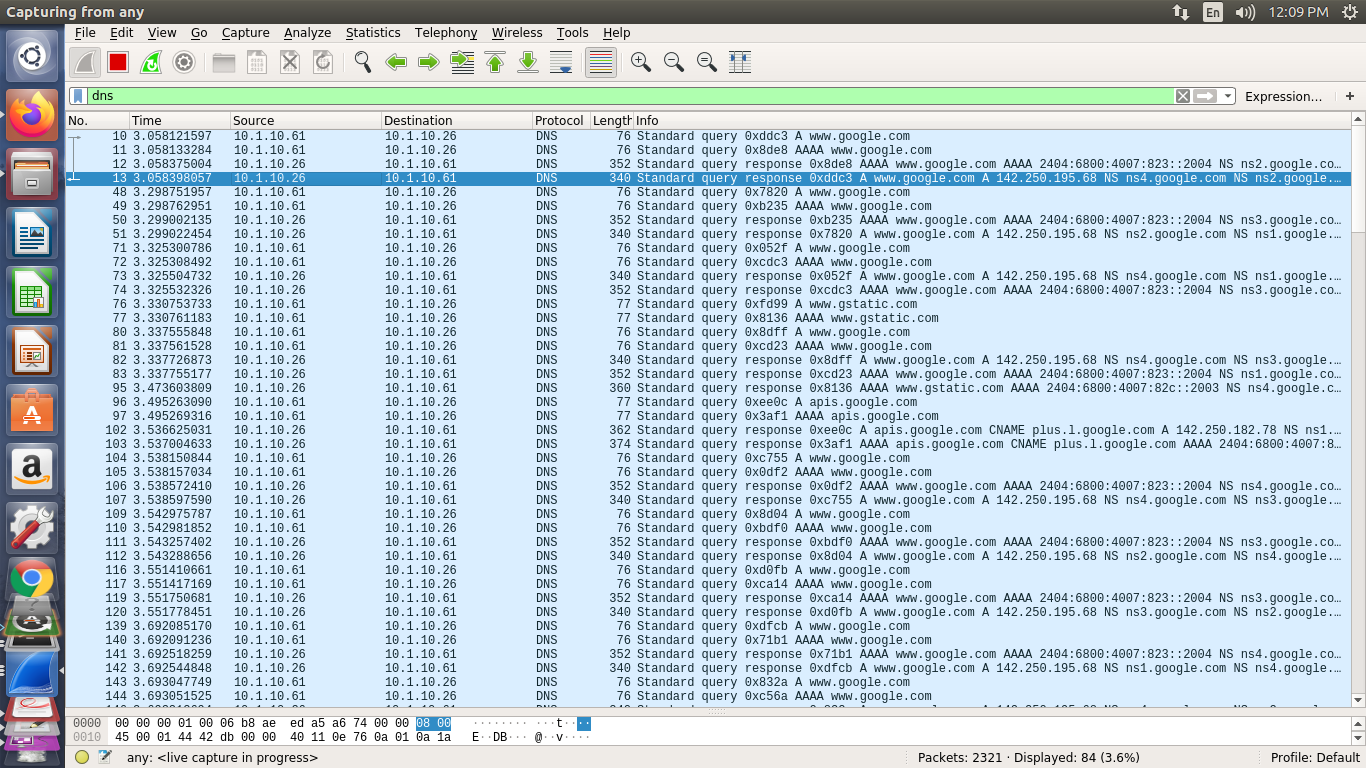


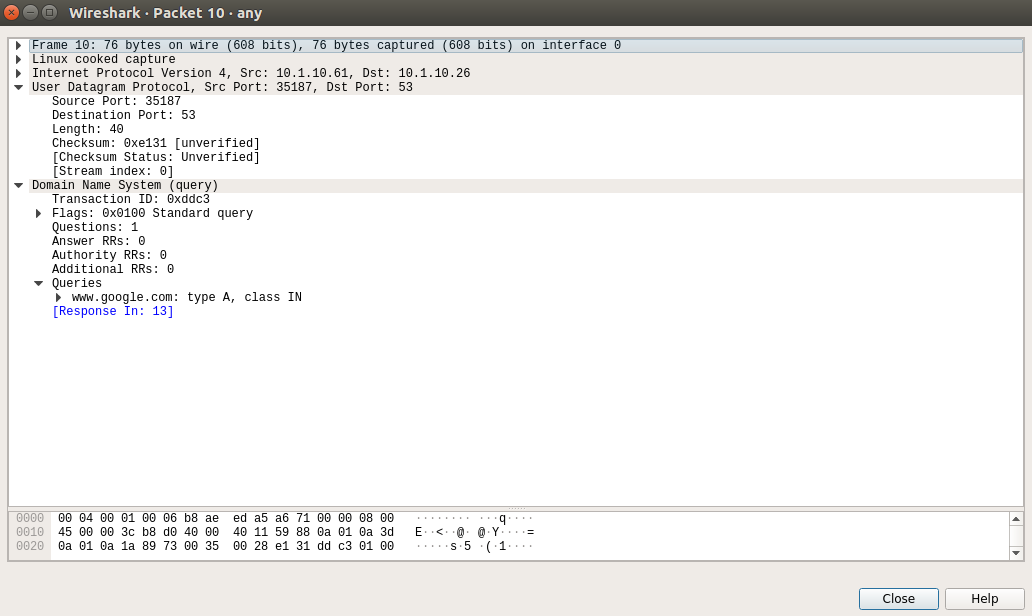
**2.3 Start DNS server :**

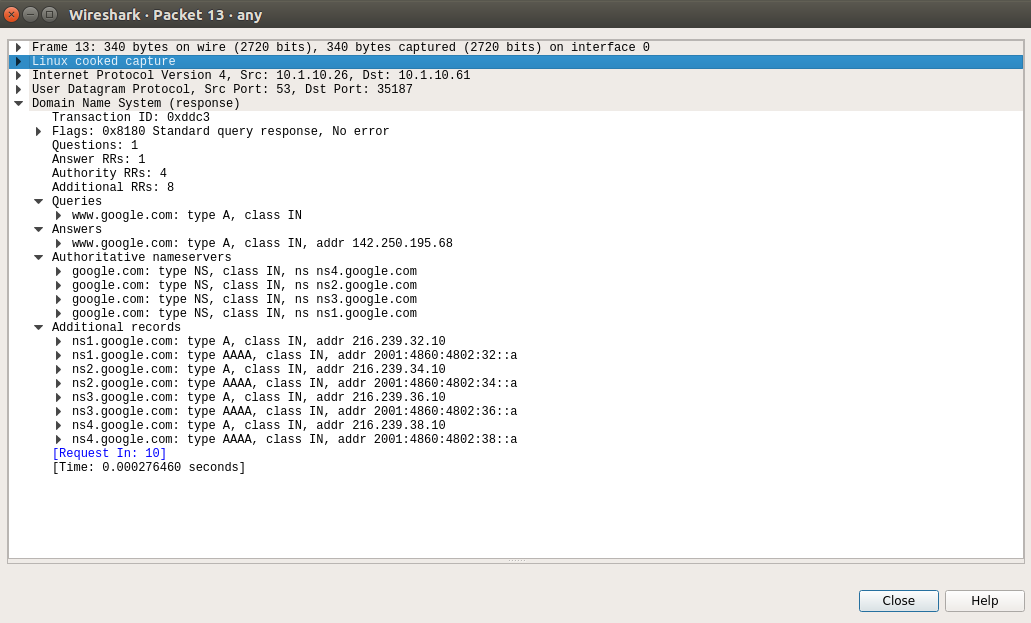


**Observation 3:**

Now, go back to your user machine (10.2.22.195), and ping a computer such as www.google.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).





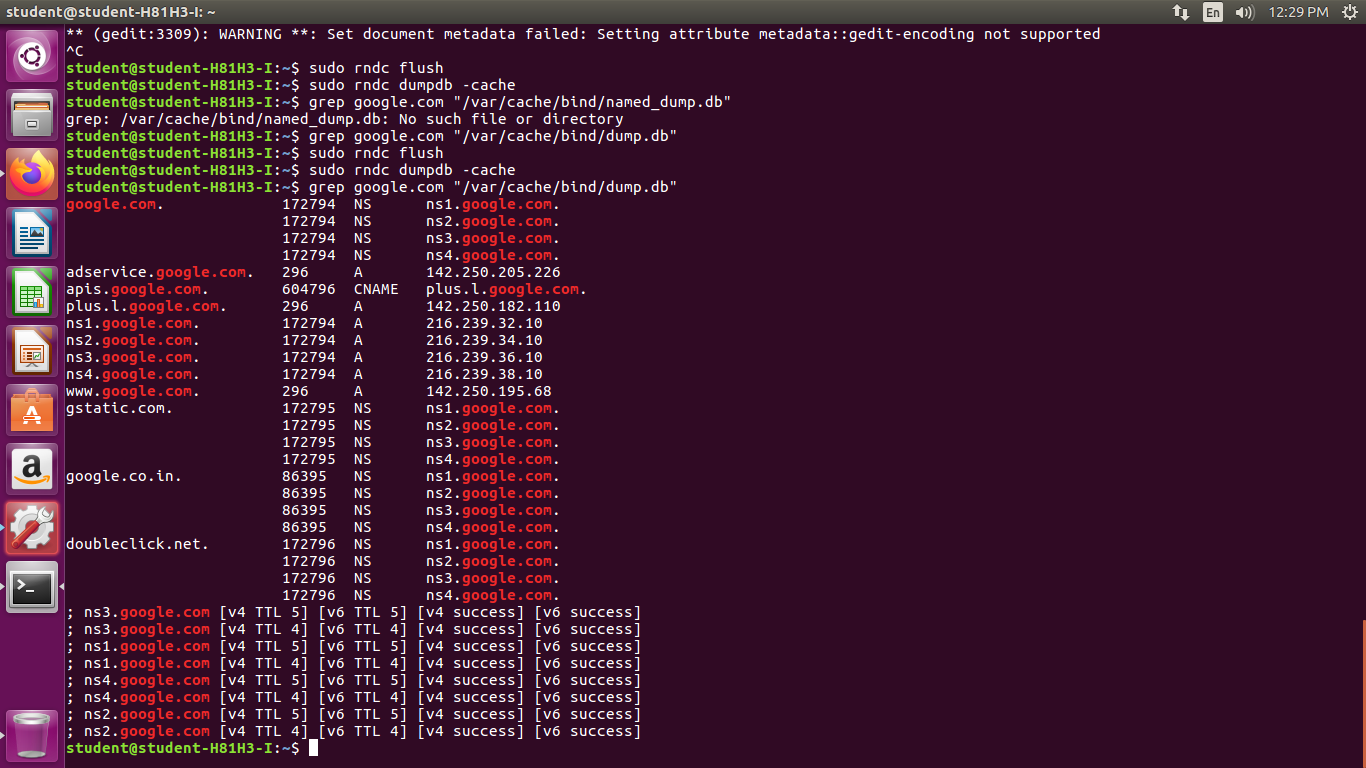


**Observation 4:**

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. You need extract the DNS cache using ‘grep’ command and take screenshot of [www.google.com](http://www.google.com) DNS cache.



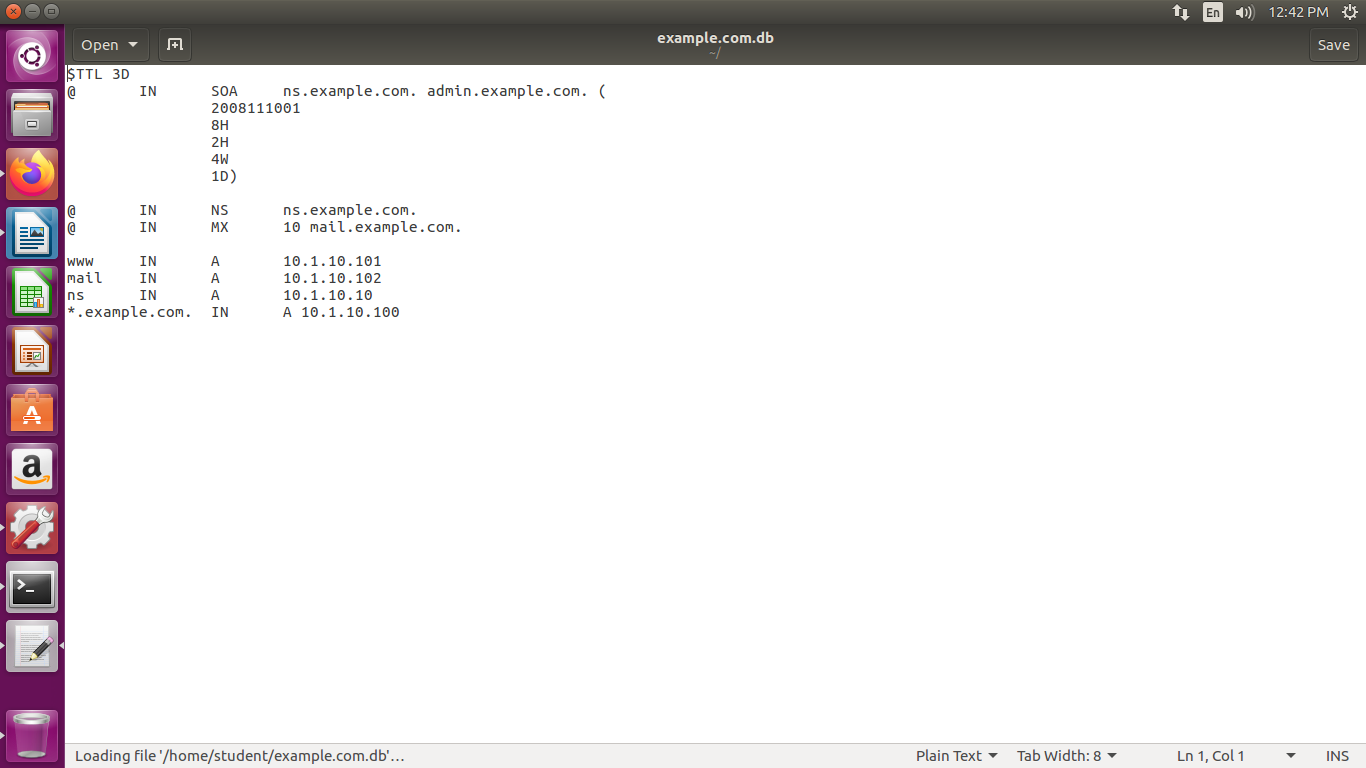
**DNS Cache using ‘grep’ command:**



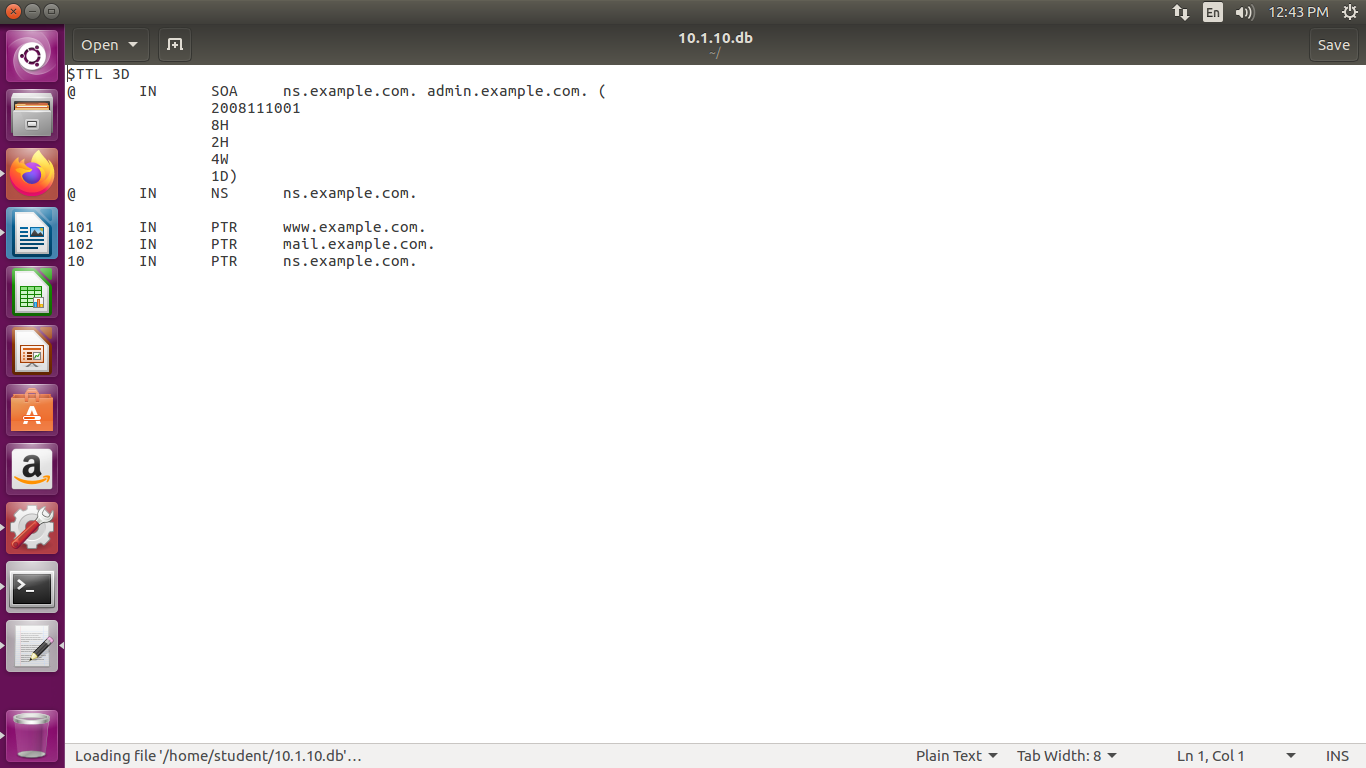
**Part 2: Setting Up an Authoritative Nameserver for example.com domain**

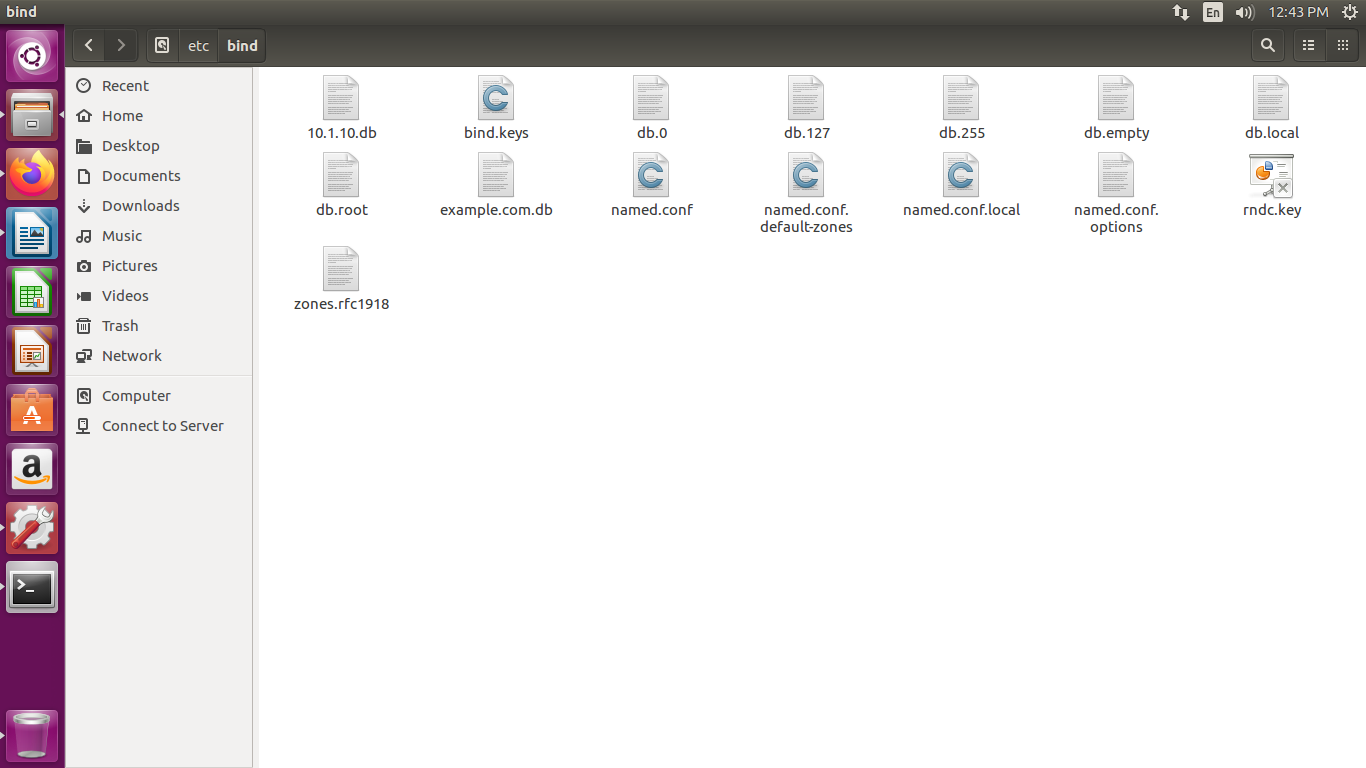
**Task 3: Host a Zone in the Local DNS server.**

**3.1 Create Zones :**

**3.2 Setup the forward lookup zone file :**

**3.3 Setup the reverse lookup zone file :**

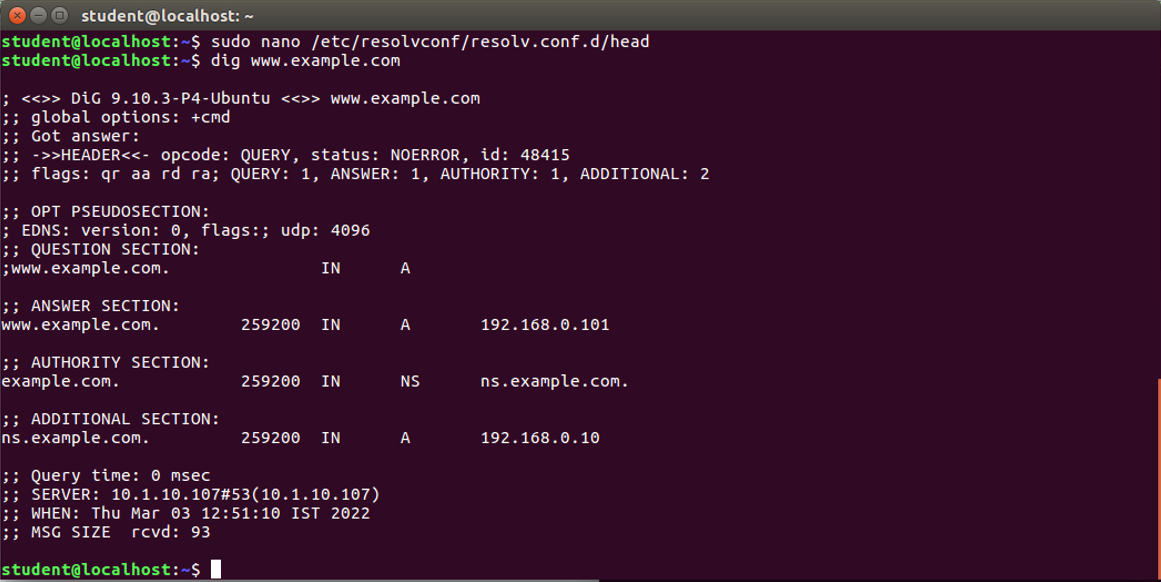




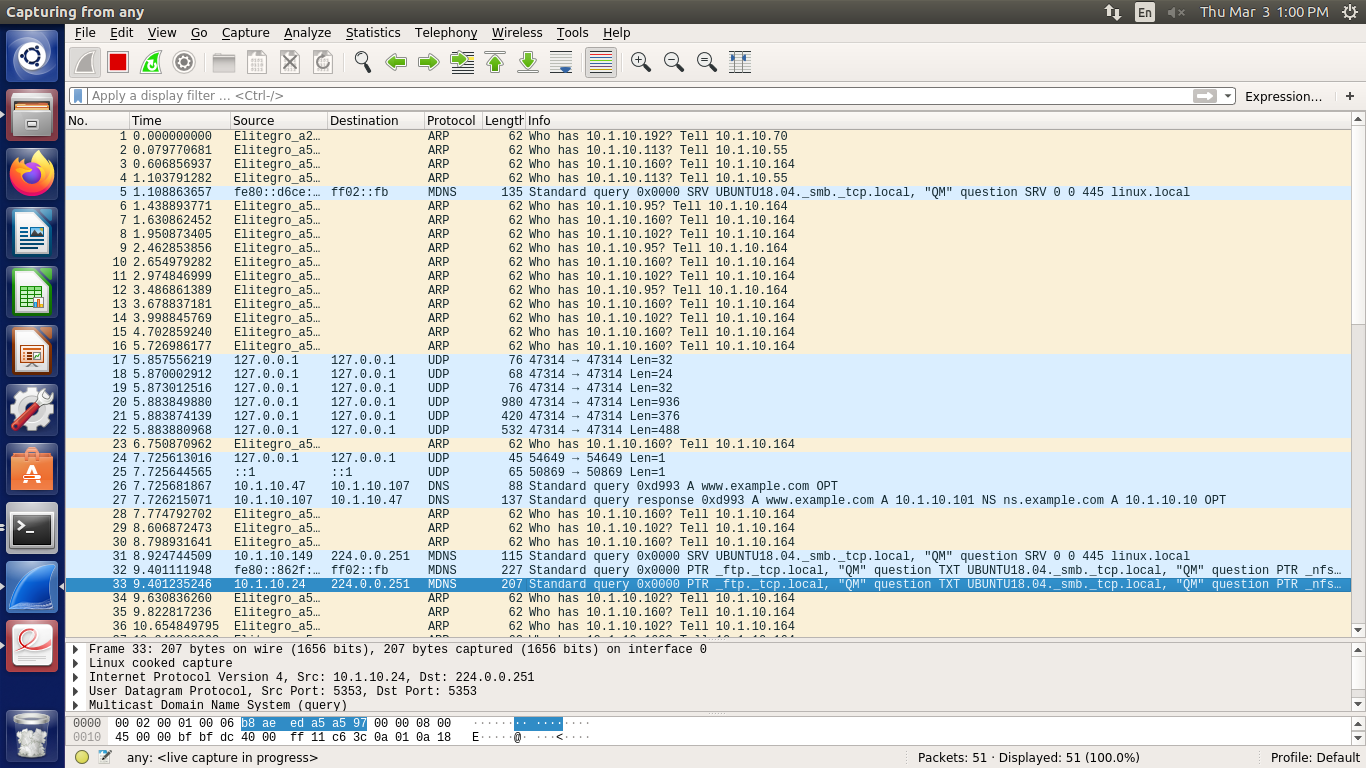
**Task 4: Restart the BIND server and test**

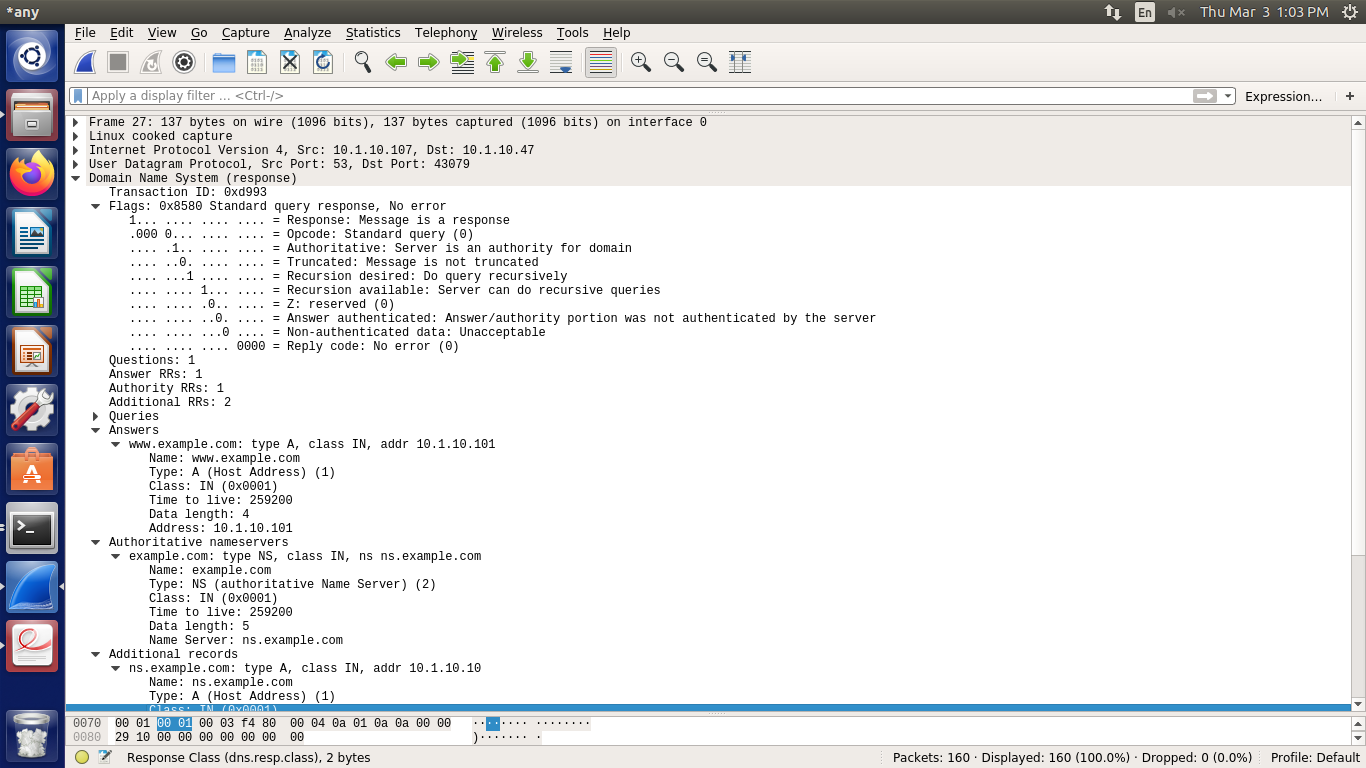
**4.1 When all the changes are made, remember to restart the BIND server. Now we will restart the DNS server using the following command:**

**4.2 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.**

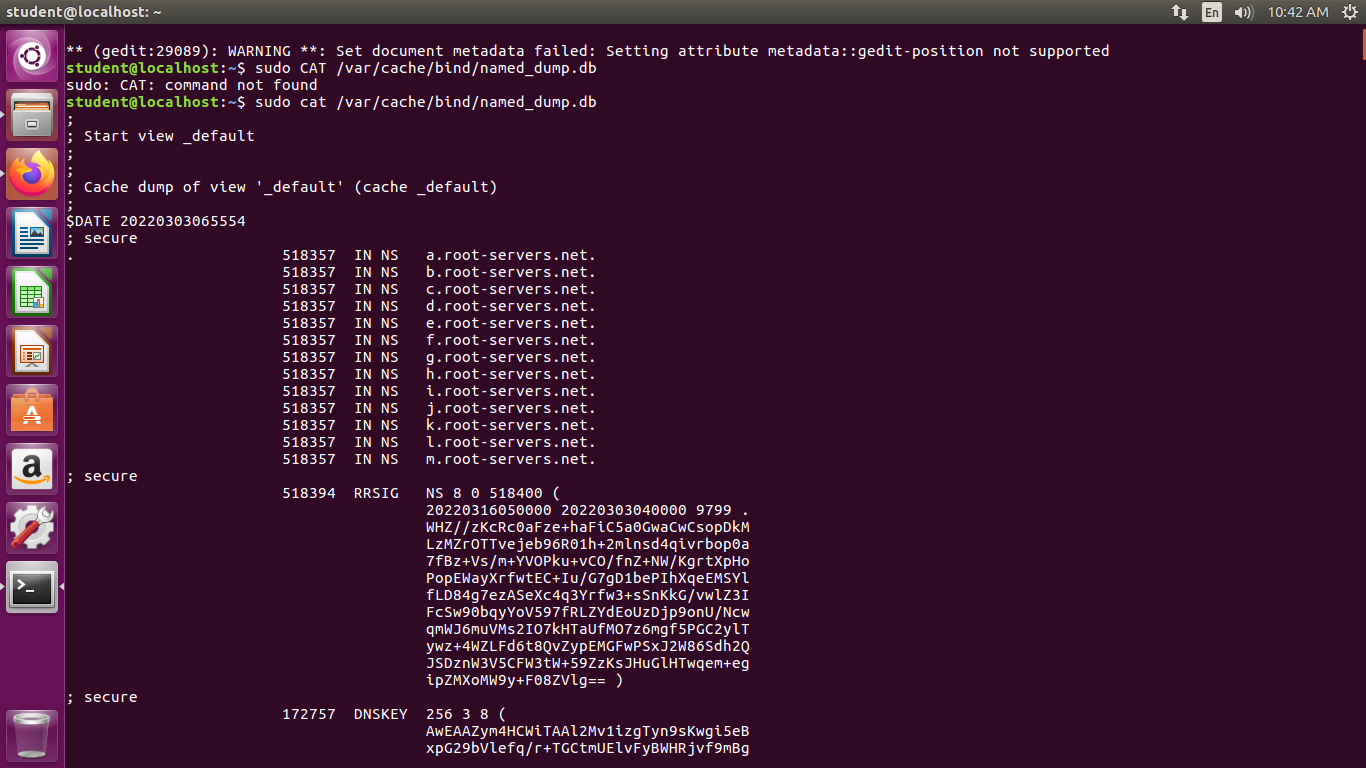


**4.3 Observe the results in Wireshark capture :**





**4.4 DNS cache on server machine after dig command :**

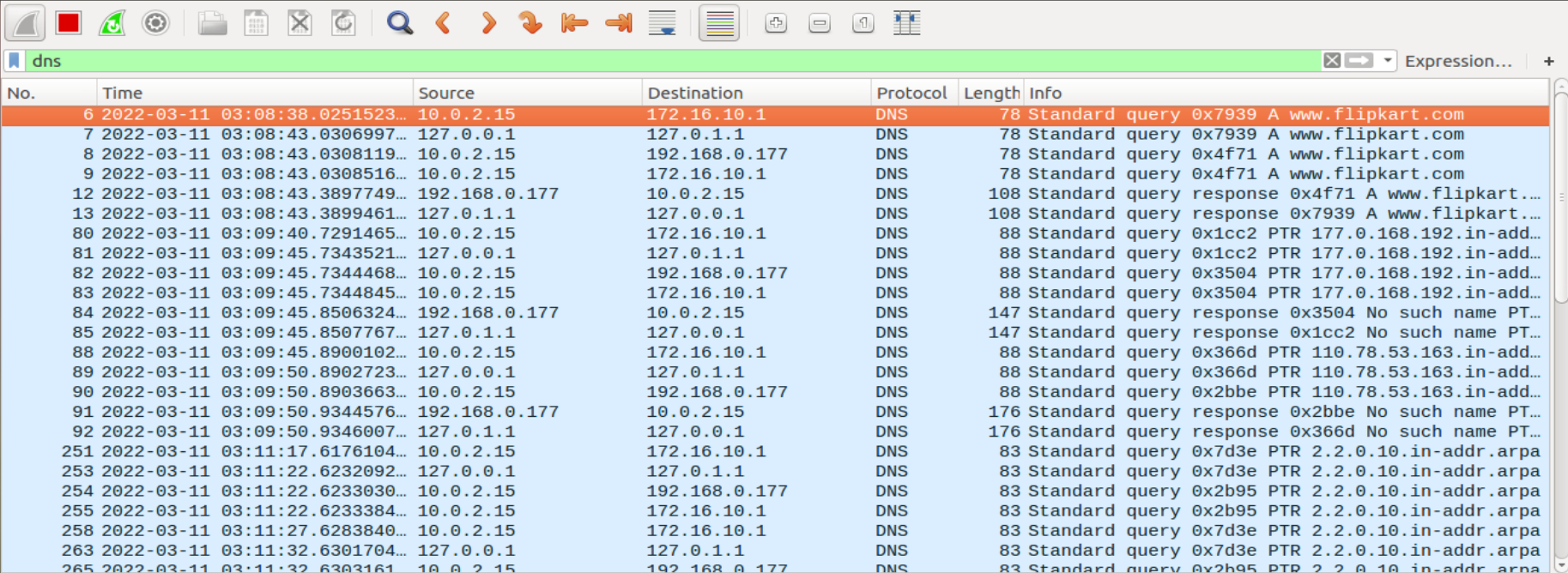


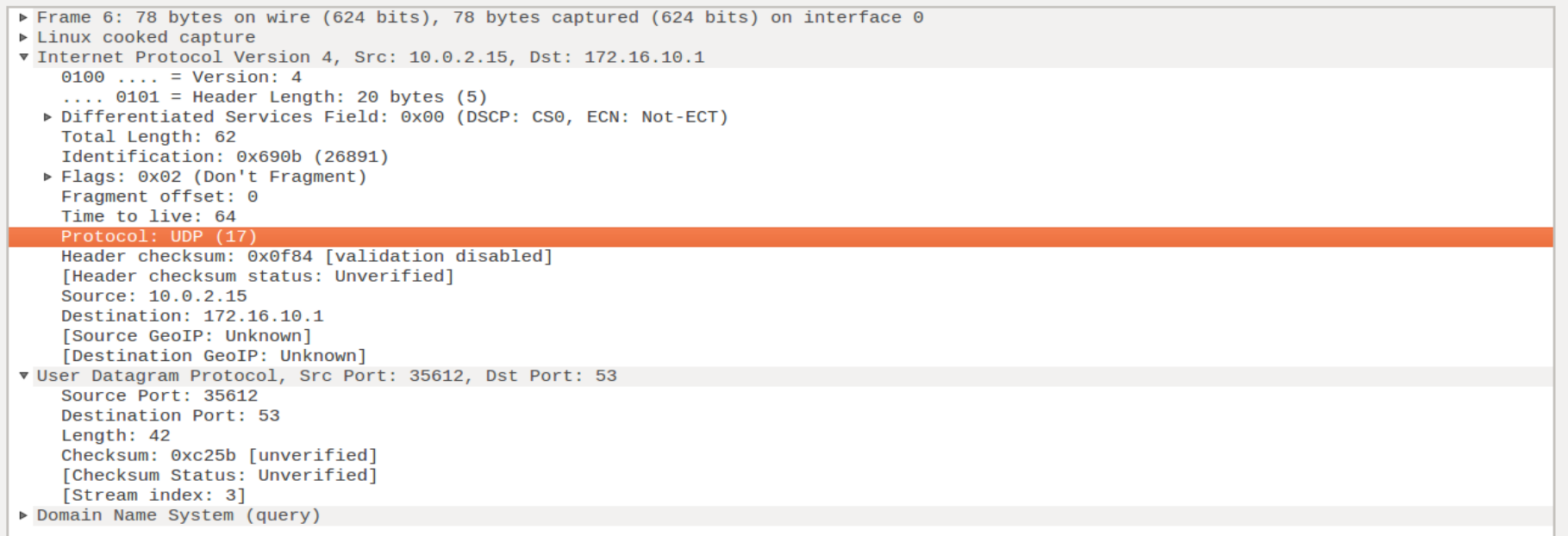
**Observation Notebook Requirements:**

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

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

* DNS Query 0x7939. It uses UDP Protocol.





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

**DNS response message?**

**🡪** Destination port for the DNS query message : 172.16.10.1

Source port of DNS response message : 127.0.1.1

**3) To what IP address is the DNS query message sent? Use ipconfig to determine the IP**

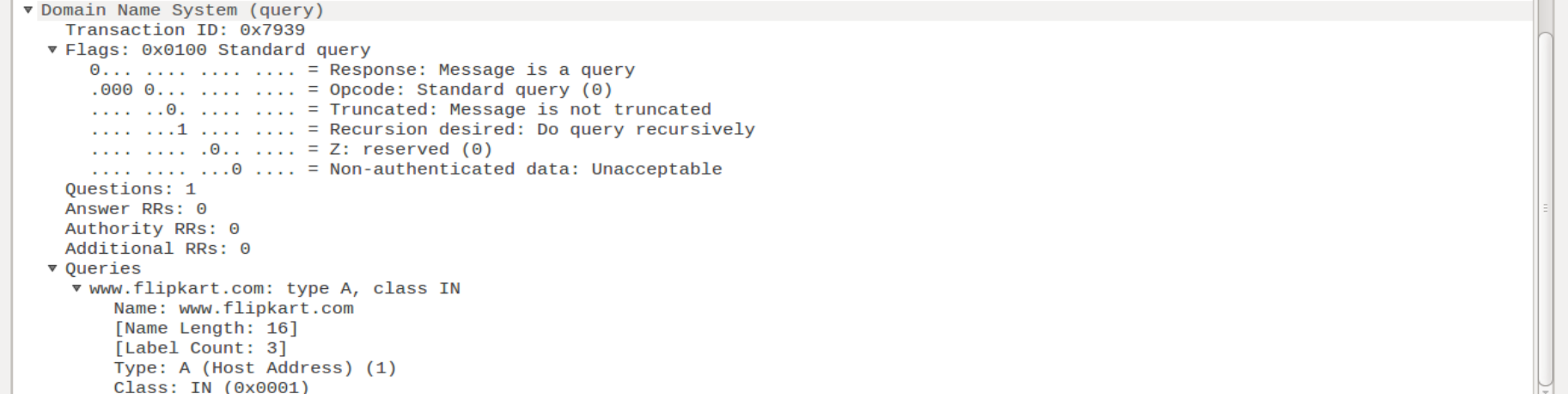
**address of your local DNS server. Are these two IP addresses the same?**

**🡪** The DNS Query is sent to IP address172.16.10.1. YES , both IP addresses are the same.

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

**message contain any “answers”?**

**🡪** Type of the Query is Standard. NO, it does not contain any answers.

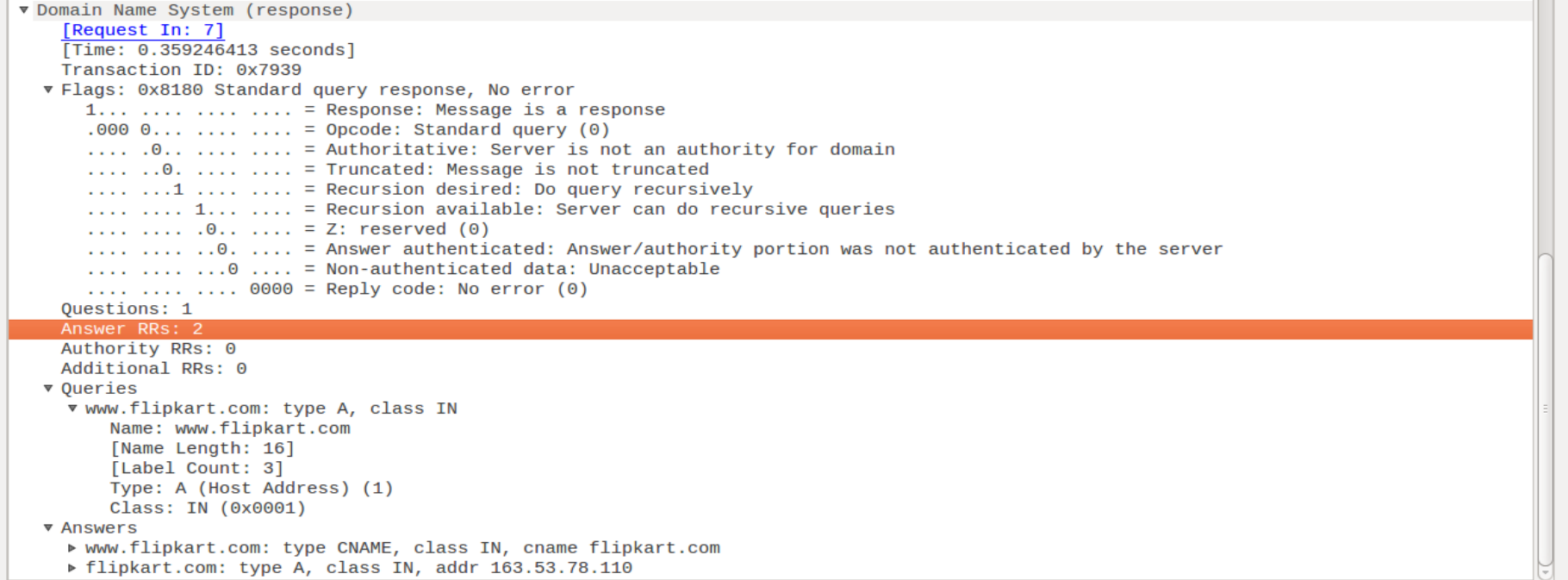


**5) Examine the DNS response message. How many “answers” are provided? What do**

**each of these answers contain?**

**🡪** There are 2 answers provided.

1. Canonical name for the given query
2. IP address for the given query



**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?**

**🡪** NO