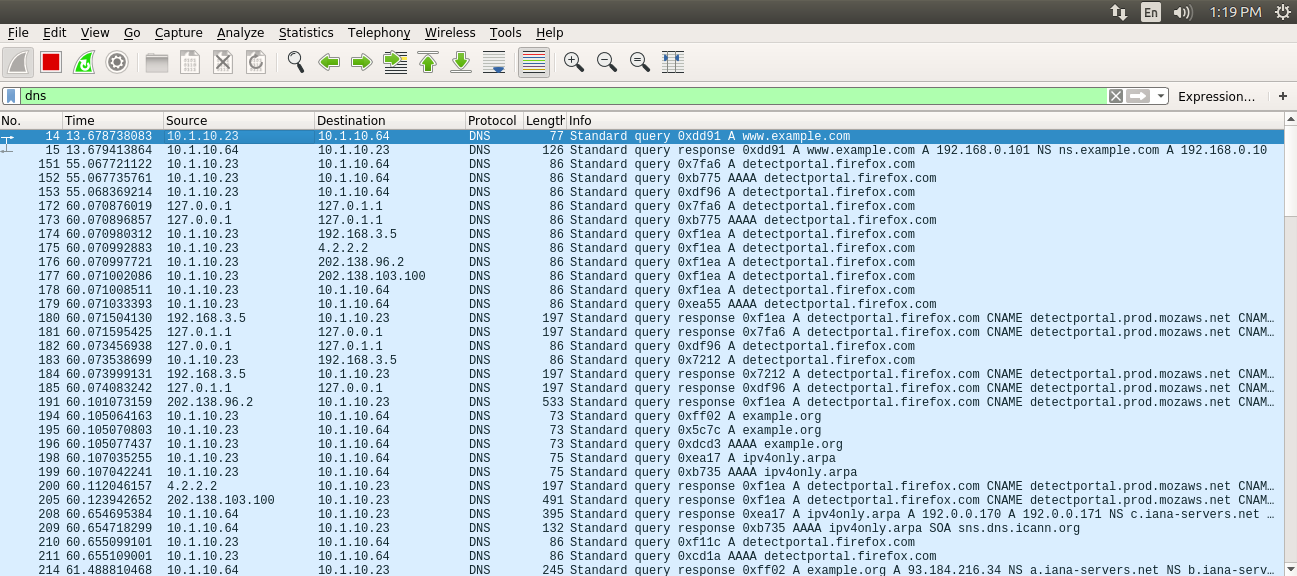
CN LAB REPORT – WEEK 4

NAME: DIVYANSHU SHARMA

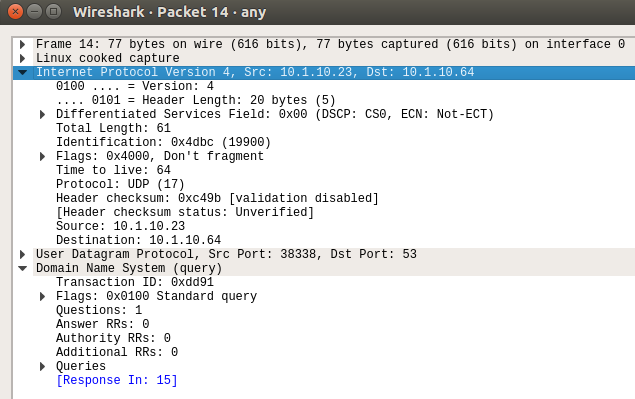
PES1UG20CS806

1. **First Test**

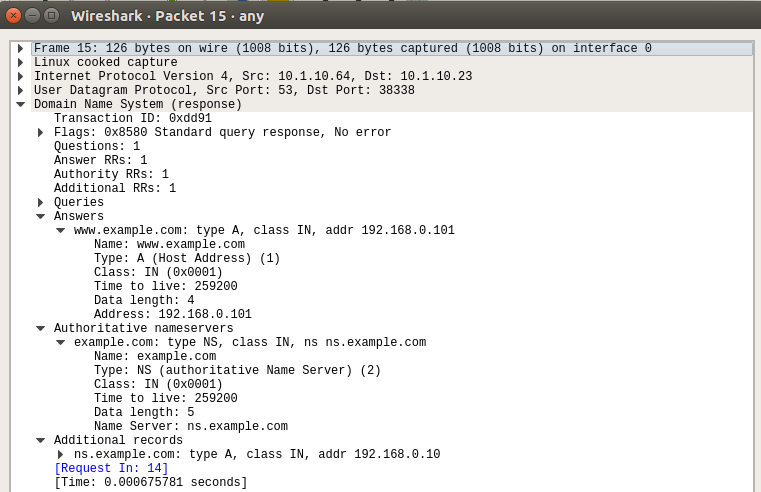
* Ping a computer such as www.example.com. Please use Wireshark to show the DNS query triggered by your ping command and DNS response.



**Wireshark Packet Capture**



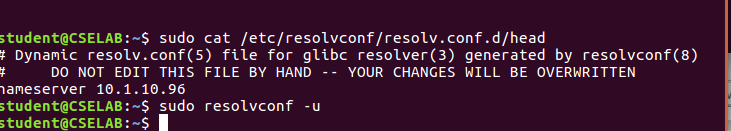
**DNS Query**

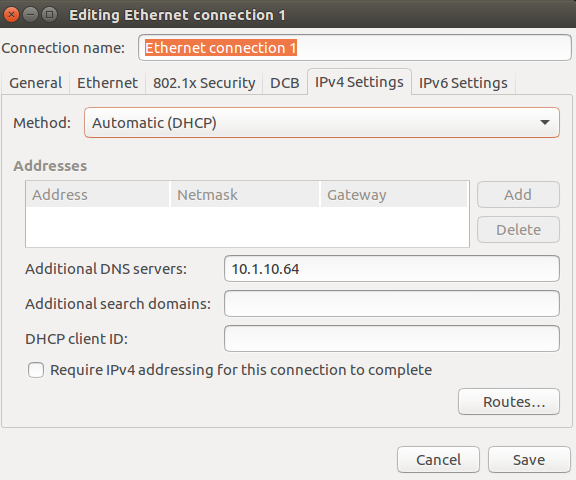


**DNS Response**

1. **Task 1: Configure the User Machine**

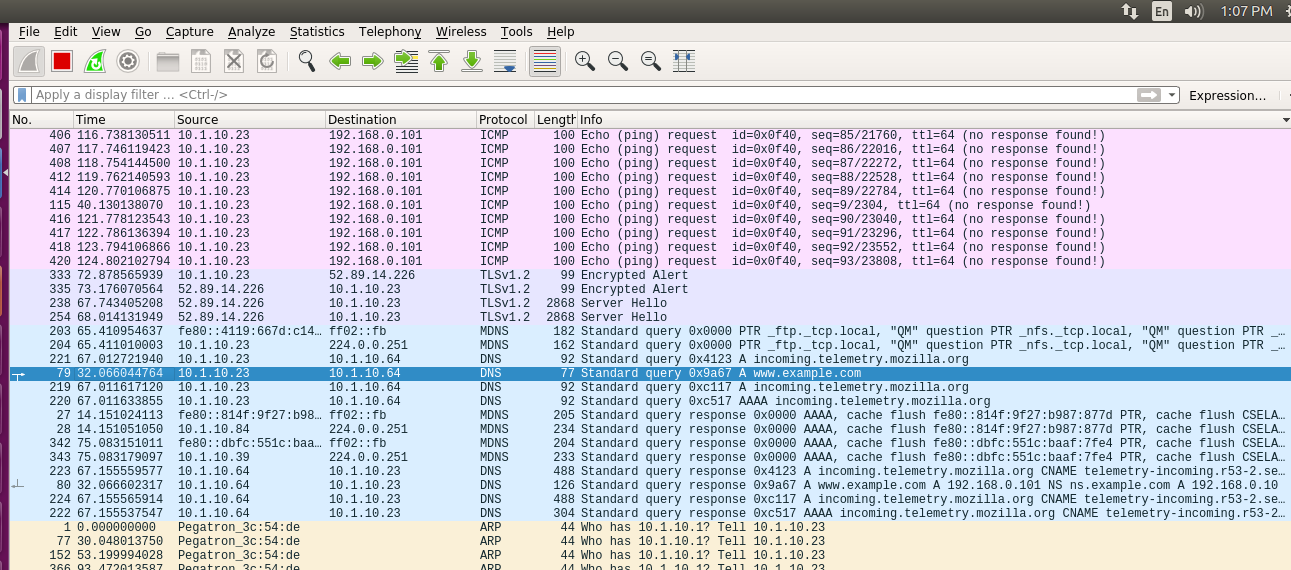
* The IP Address of the client machine is 10.1.10.23 and the IP Address of the server machine is 10.1.10.64
* We need to add the IP Address of the custom DNS server (10.1.10.64) to the client machine.
* This is done by adding the IP address of the server to the file **/etc/resolvconf/resolv.conf.d/head** 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**





1. **Second Test**:

* Ping a computer such as [www.example.com](http://www.example.com).
* Please use Wireshark to show the DNS query triggered by your ping command and DNS response. Describe your observation. (Take a screenshot).

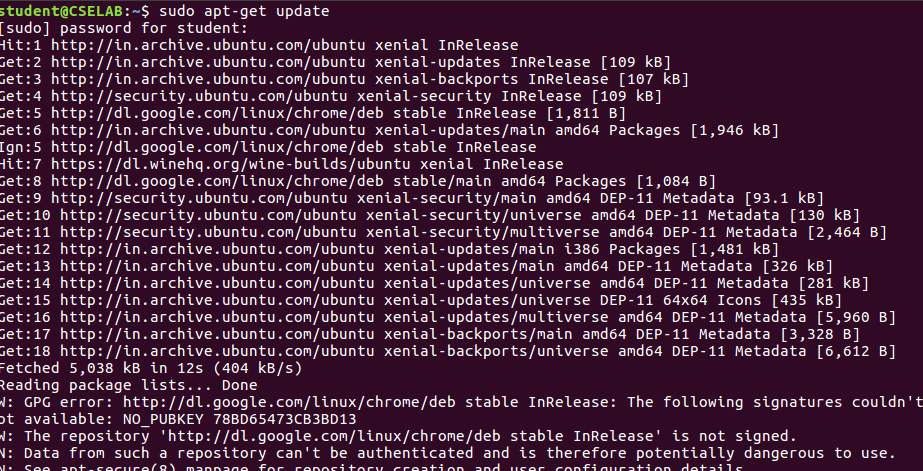


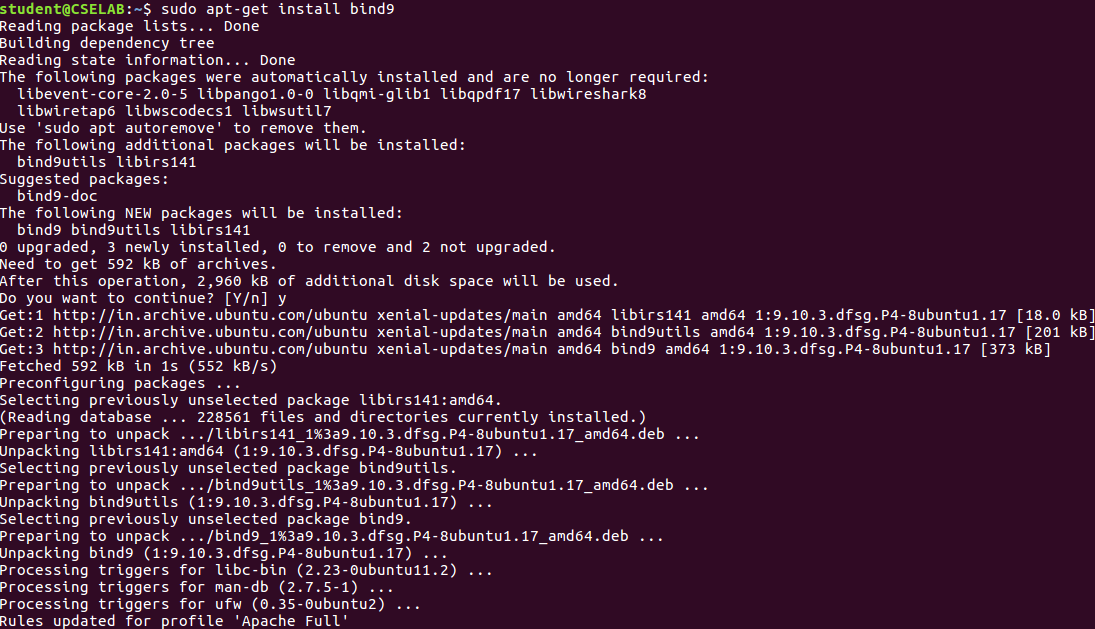
1. **Task 2 – Setting Up Local DNS Server**

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

**$ sudo apt-get update**

**$ sudo apt-get install bind9**

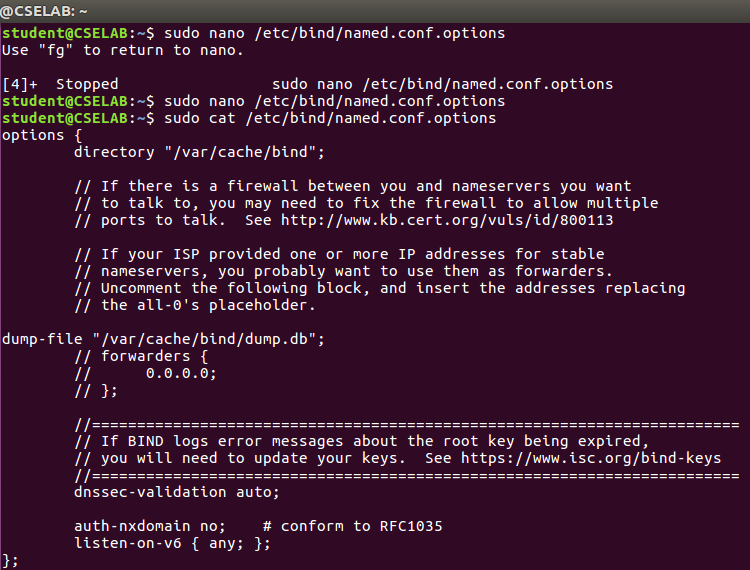




**Step 1: Configure the BIND9 Server**.

* BIND9 gets its configuration from a file called **/etc/bind/named.conf.**
* This file is the primary configuration file, and it usually contains several “include” entries.
* One of the included files is called **/etc/bind/named.conf.options**. This is where we typically set up the configuration options.
* Let us first set up an option related to DNS cache by adding a dump-file entry to the options block. The above option specifies where the cache content should be dumped to if BIND is asked to dump its cache.

G:\IMAGES\BANGALORE\BANGALORE\PESU UNIVERCITY BTECH\PESU\2ND YEAR\4th SEM\Computer Netwok Lab\Week 4\New folder\dayp2.png



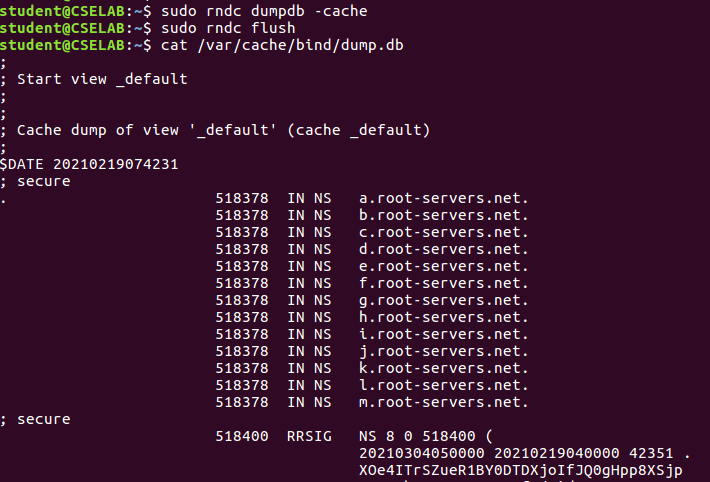
* The above option specifies where the cache content should be dumped to if BIND is asked to dump its cache. If this option is not specified, BIND dumps the cache to a default file called **/var/cache/bind/named\_dump.db**

**Step 2: Start DNS server**

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

G:\IMAGES\BANGALORE\BANGALORE\PESU UNIVERCITY BTECH\PESU\2ND YEAR\4th SEM\Computer Netwok Lab\Week 4\restart.png

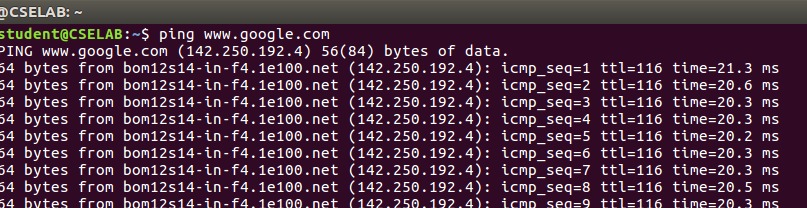
* The two commands shown below are related to DNS cache.
* The first command is **sudo rndc dumpdb -cache**, dumps the content of the cache to the file specified above.
* And the second command is **sudo rndc flush** which clears the cache.

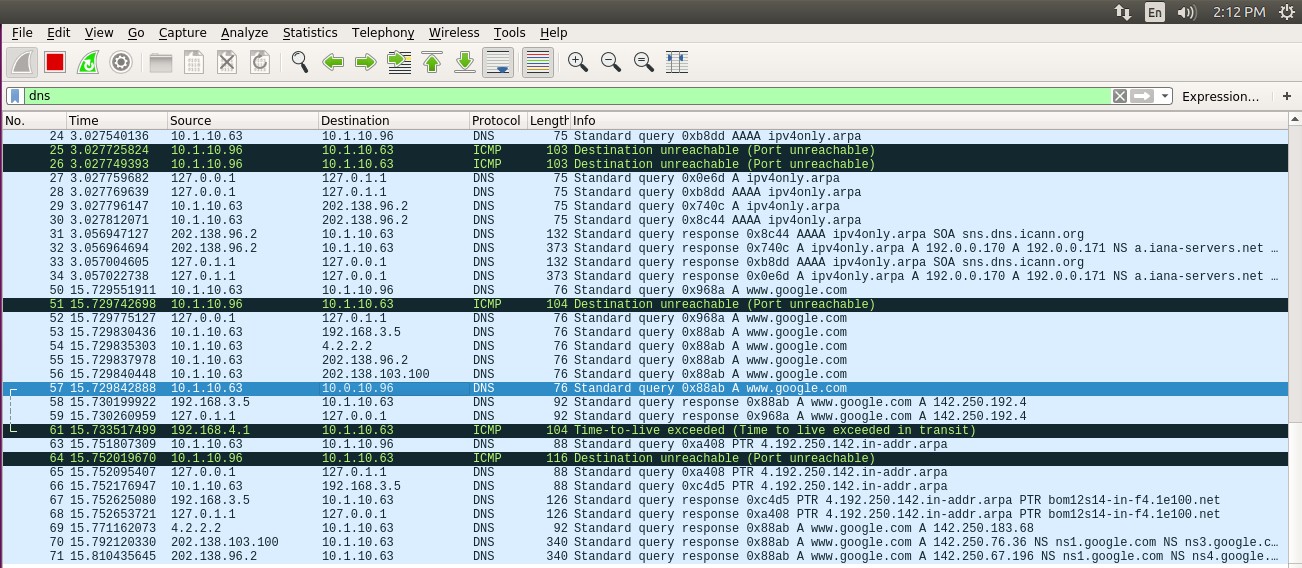


**Step 3: Use the DNS server**

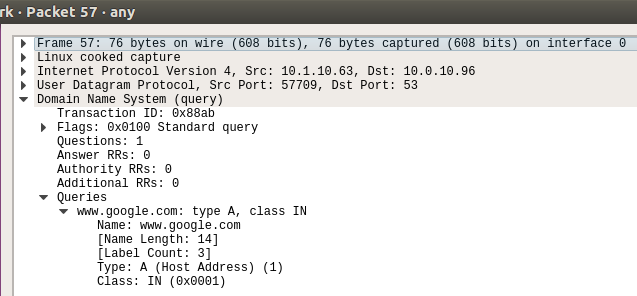
1. **Third Test:**

* Now, go back to your user machine, and ping a computer such as [www.google.com](http://www.google.com)
* 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 Flipkart website

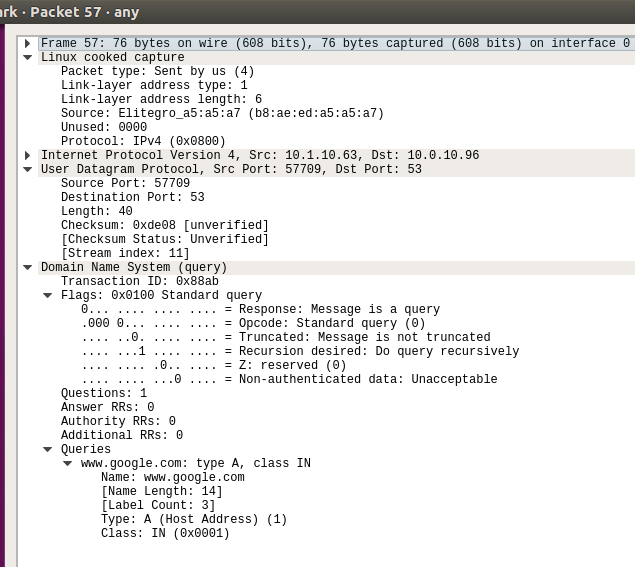




**Wireshark Packet Capture**



**DNS Query Packet**



**DNS Response Packet**

1. **Task 3 – Hosting a Zone in the Local DNS Server**

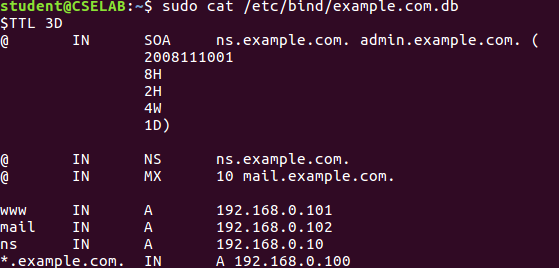
**Step 1:** **Create Zones**

* 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).



**Step 2: 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 used to indicate the origin specified, in this case [**www.example.com**](http://www.example.com)
* There are **7 records** in the lookup file, an SOA record, a nameserver, a mailserver and 4 authoritative records



**Forward Lookup file**

**Step 3: Setup the reverse lookup zone file**

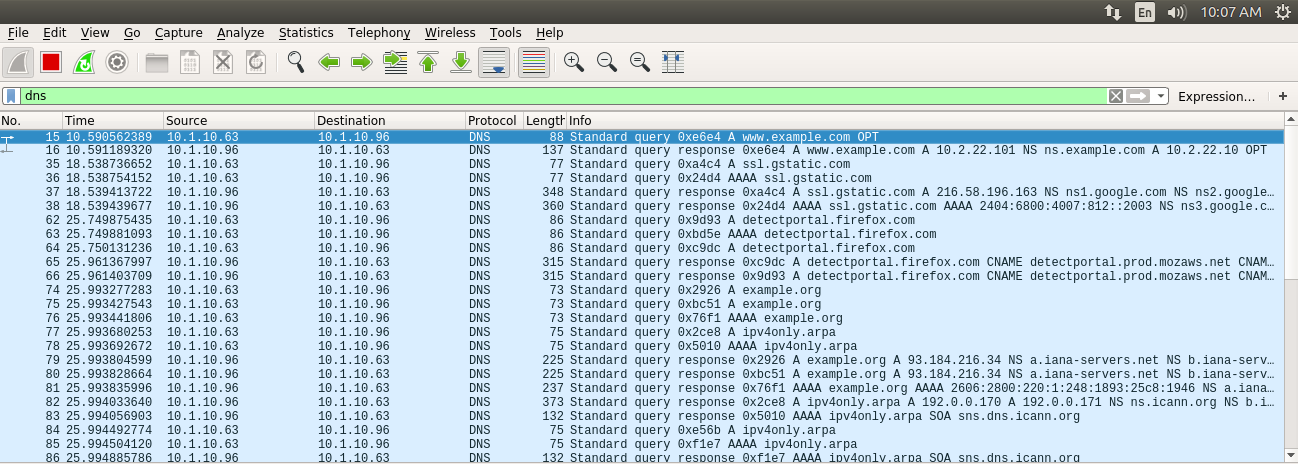
* We create a reverse DNS lookup file called **10.0.63.db for** the example.net domain to support DNS reverse lookup, i.e., from IP address to hostname in the /etc/bind/ directory with the following contents



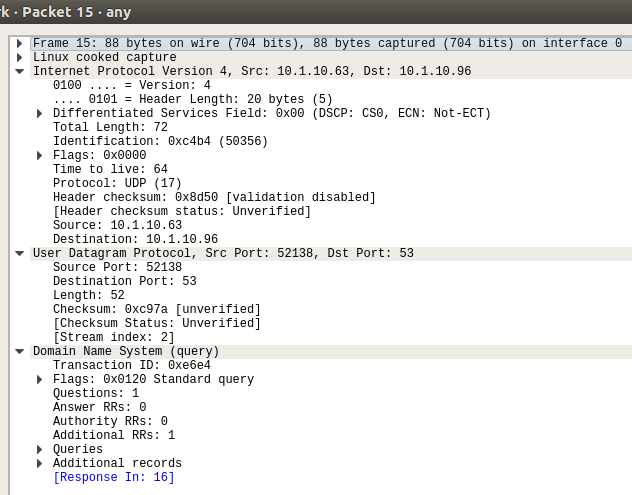
**Reverse Lookup file**

1. **Fourth Test – Testing** [**www.example.com**](http://www.example.com)

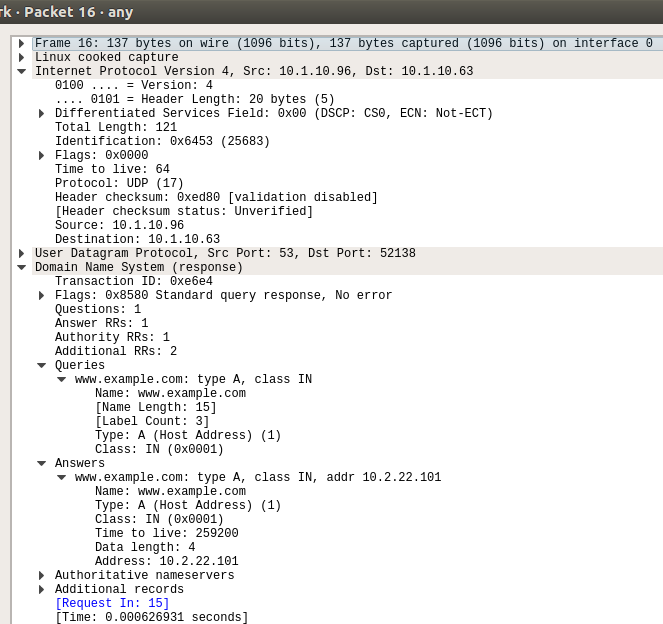
* The dig command is used to lookup name servers specified in the file **/etc/resolv.conf**



**Wireshark Packet Capture**



**DNS Response Packet**



**DNS Response Packet**

1. **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 10.0.2.63. 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 example.com refers to the canonical hostname www.example.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.example.com) retrieved from the response message.

**Q7**. *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

**Q8**. *To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?*

**Answer –** The DNS query message sent to the IP 10.1.10.96. No, this is not the IP address of your default local DNS server.

**Q9**. *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.

**Q10*.*** *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 example.com refers to the canonical hostname www.example.com.
* **A type RR:** This provides the IP Address of the canonical hostname.