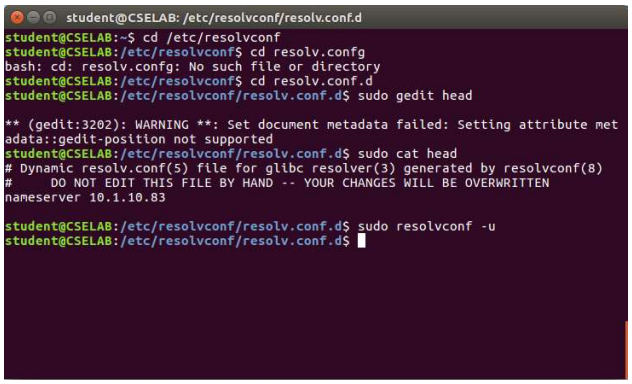
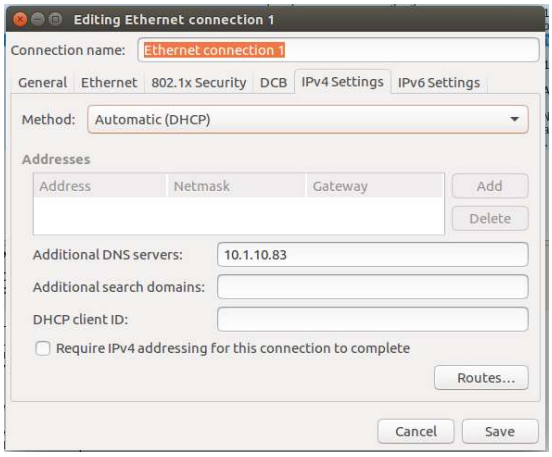
COMPUTER NETWORKS
LABORATORY- Week-4

Student Details-

Name	Siddharth Magadum
SRN	PES1UG19CS482
Section	H

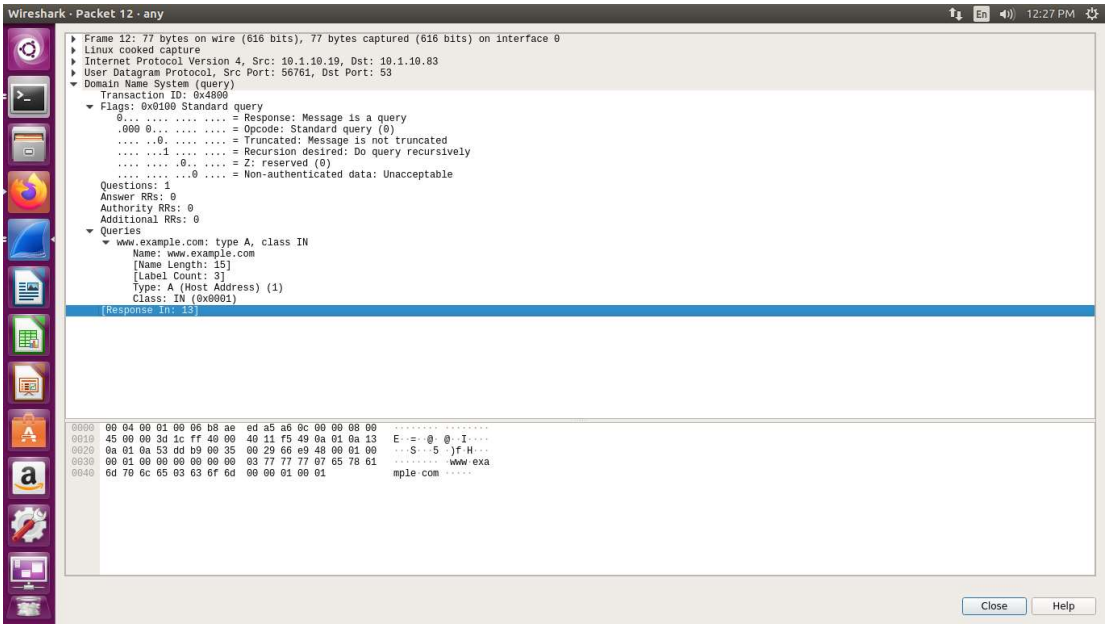
Task 1: Configuring Client Machine





DNS query captured by wireshark for pinging www.example.com

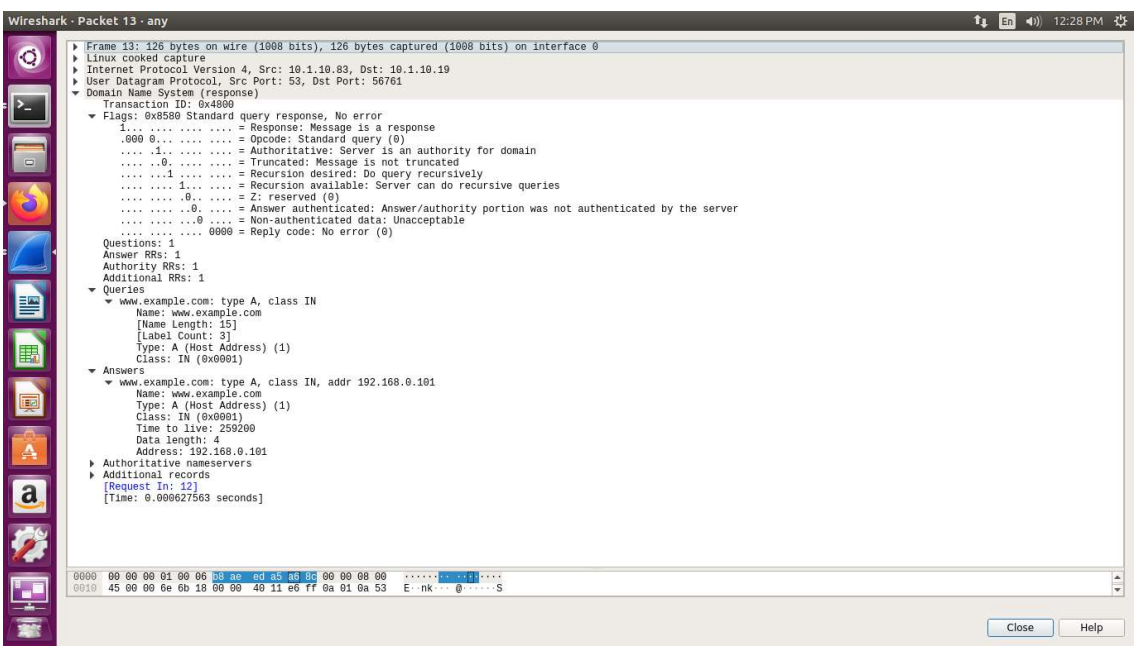
Observation 2:



We can see under the flags section that message is a query. In Queries, the name of query is www.example.com .

The corresponding DNS response

We get a message response, in which we can observe the Name, Class, TTL and Data length.

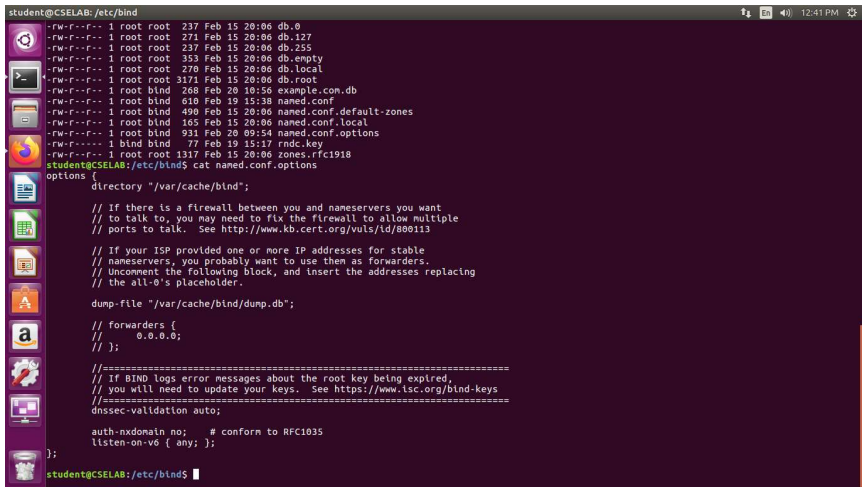


Task 2: Setting up local DNS server

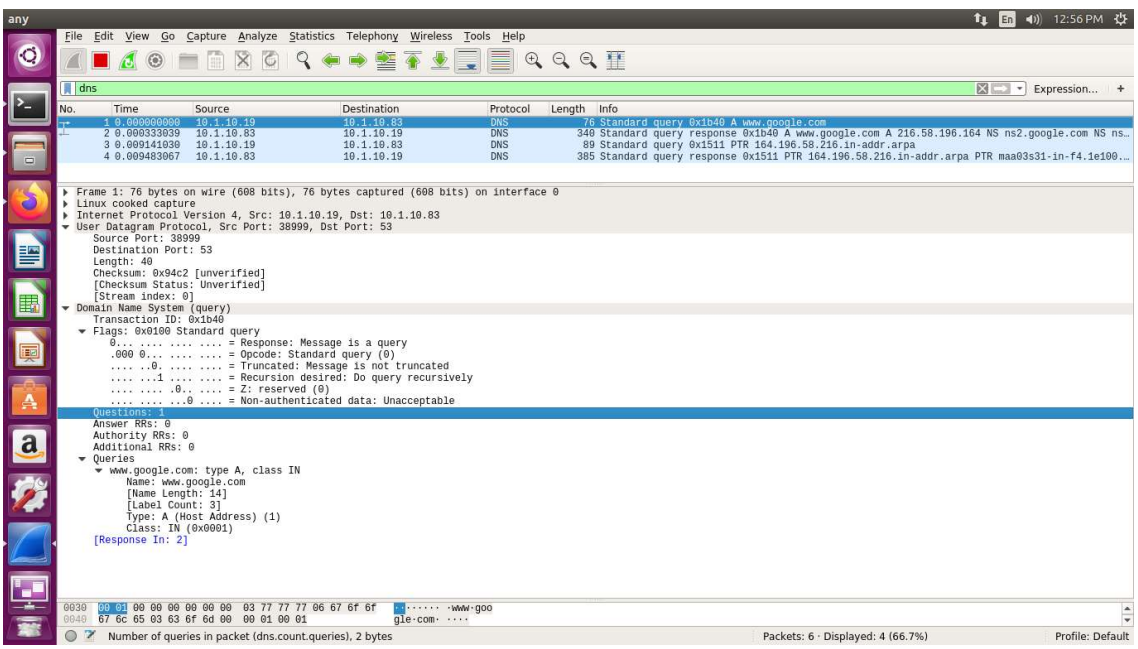
Installing bind9

$ sudo apt-get update

$ sudo apt-get install bind9

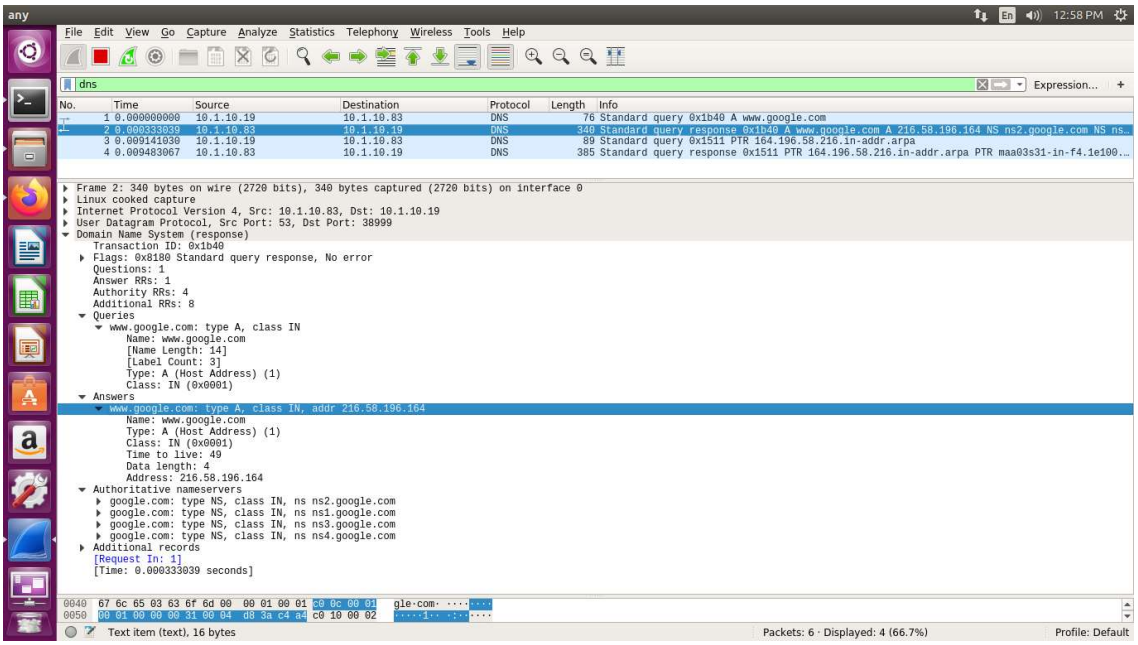


Observation 3: We ping www.google.com and observe the DNS query.

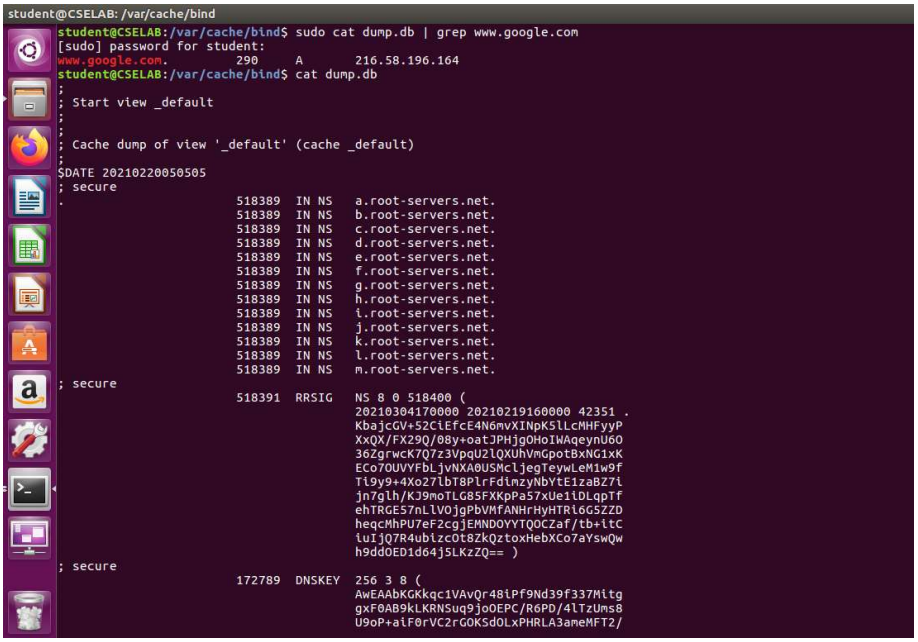


We observe that the client machine send the request for the server machine who's IP address is the one with destination IP address, in this query.

The server now responds to that query, hence, the server computer acts as a local DNS server.



Observation 4: We now observe the cache dumped in the local DNS (server machine). We use grep command for filtering the query name i.e. www.google.com



Task 3: Host a Zone in Local DNS server .

Step 1: Creating Zones.

We had two zone entries in the DNS server by adding the following contents to **/etc/bind/named.conf**

```
student@CSELAB:/etc/bind$ sudo gedit named.conf

** (gedit:4477): WARNING **: Set document metadata failed: Setting attribute metadat
student@CSELAB:/etc/bind$ sudo cat named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "example.com" {
type master;
file "/etc/bind/example.com.db";
};

zone "10.1.10.in-addr.arpa" {
type master;
file "/etc/bind/10.1.10.db";
};
student@CSELAB:/etc/bind$
```

The first zone is forward lookup zone. It resolves the host name to IP address.

The second zone is forward lookup zone. It resolves the IP address to hostname.

Step 2 &3: Setup the forward lookup zone.

We copy the two files given by the faculty members to **/etc/bind** location.

```
student@CSELAB: ~
student@CSELAB:~$ sudo cp 10.1.10.db /etc/bind
student@CSELAB:~$ sudo cp example.com.db /etc/bind
student@CSELAB:~$
```

Task 4 : Restart the BIND server and test

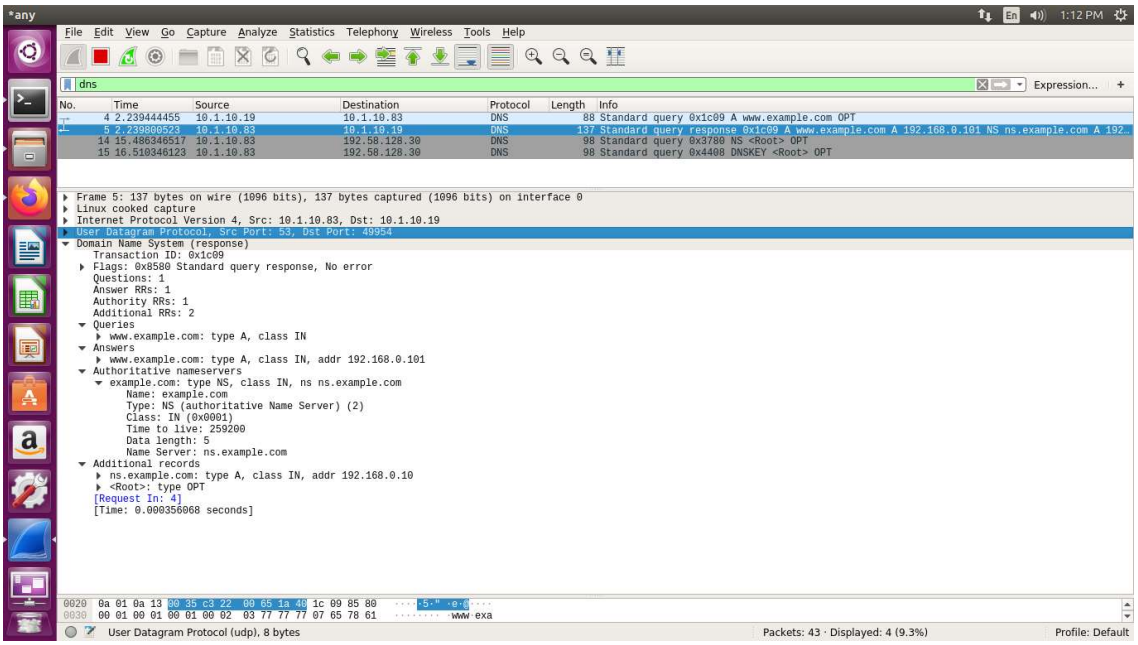
Step1: We restart the bind9 server using command **sudo service bind9 restart**

Step 2: We find the IP address of Local DNS server from the client computer using dig command

```
student@CSELAB: /etc/resolvconf/resolv.conf.d
;; MSG SIZE  rcvd: 93

student@CSELAB:/etc/resolvconf/resolv.conf.d$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7177
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       192.168.0.101

;; AUTHORITY SECTION:
example.com.            259200  IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168.0.10

;; Query time: 0 msec
;; SERVER: 10.1.10.83#53(10.1.10.83)
;; WHEN: Sat Feb 20 13:11:12 IST 2021
;; MSG SIZE  rcvd: 93

student@CSELAB:/etc/resolvconf/resolv.conf.d$
```

We can see that the ANSWER SECTION contains the DNS mapping. We can see that the IP address of www.example.com is now 192.168.0.101, which is what we have setup in the DNS server.

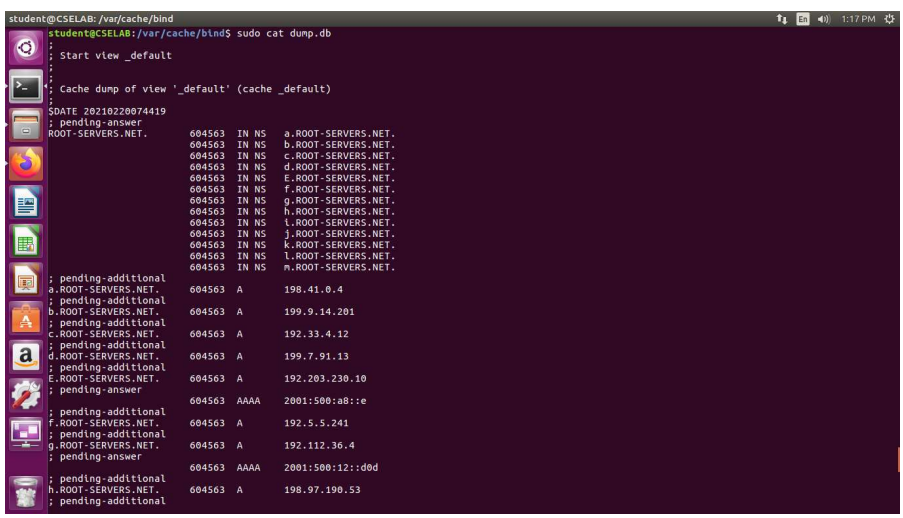
Step 3: Observe the wireshark capture



We load DNS cache, use the below command.

sudo rndc dump.db -cache

The Local DNS cache on server machine after dig command



We clear DNS cache by using command **sudo rndc flush**

----------x----------