# Week #5

**Week 5 - Setting up local DNS server**

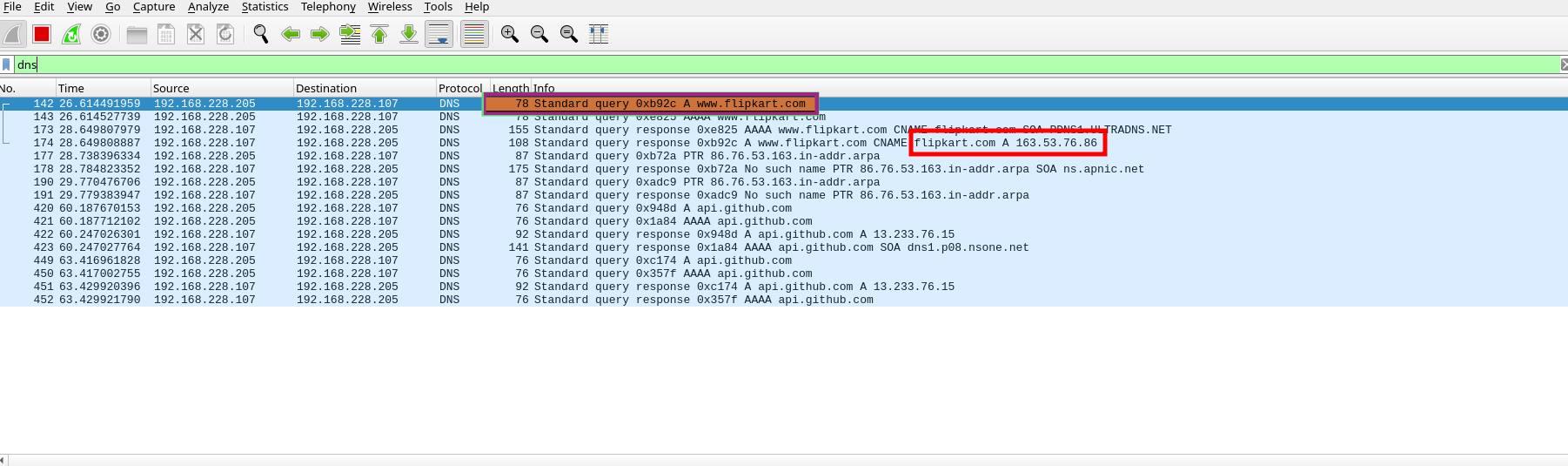
**SRN : PES2UG20CS237**

**Name : P K Navin Shrinivas**

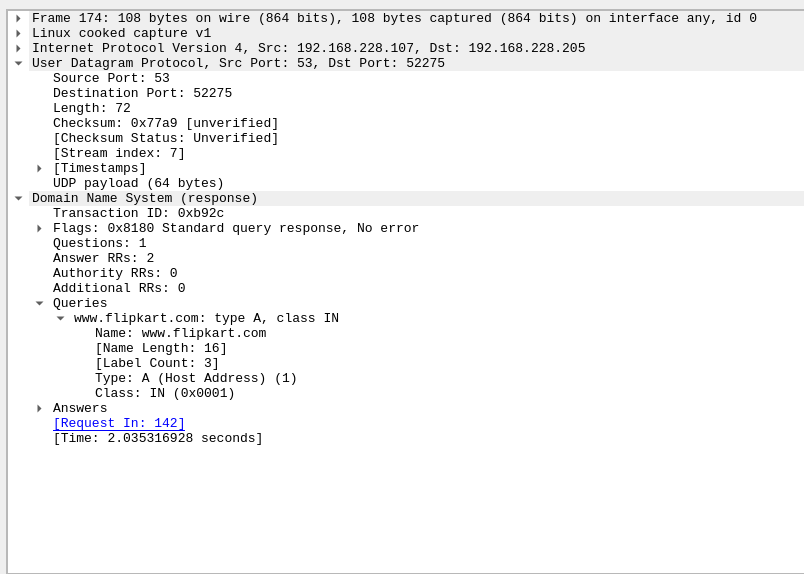
**Section : D**

## Task 1 :Pinging a website using default DNS

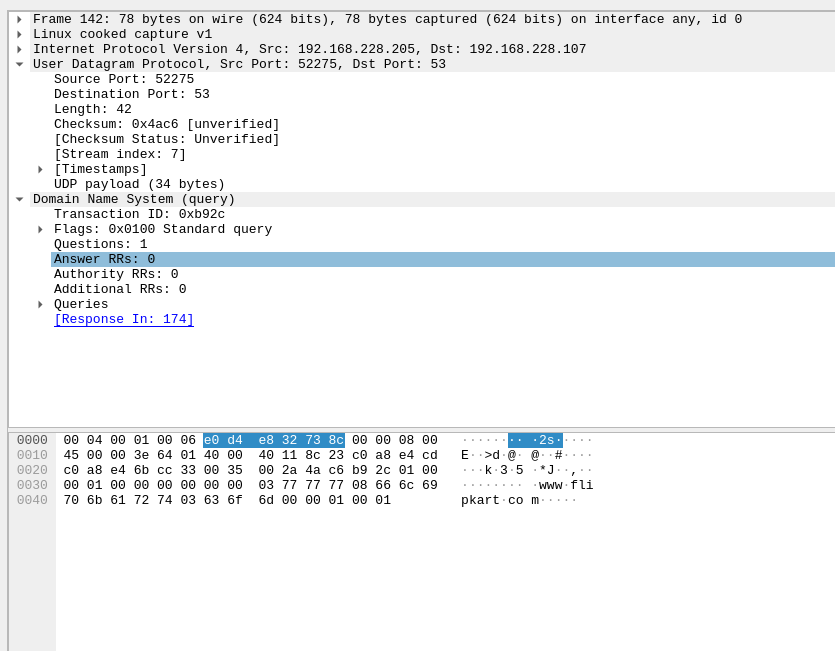
* My default DNS being 1.1.1.1 (cloudflare), flipkart was pinnged using ping command,the following packets were observed in wireshark:



WireShark packets with DNS filter



DNS query



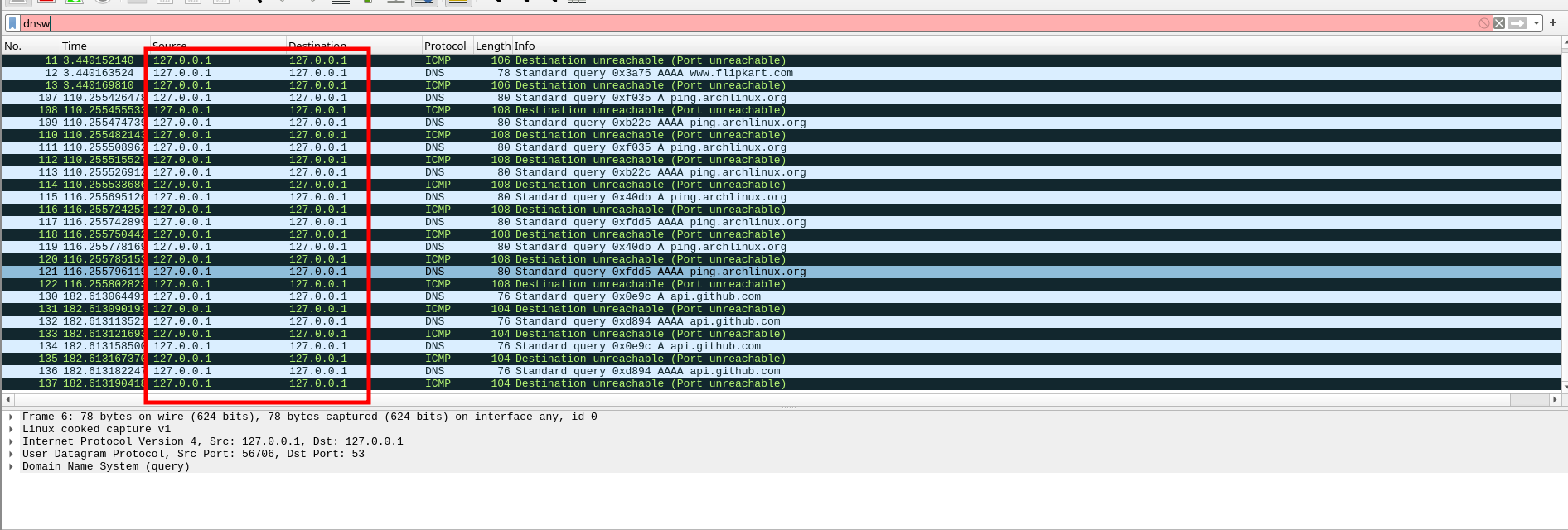
DNS response

## **Task 2 :Configure client to use local DNS**

* Note the ip address of your local DNS server, in my case i am using loopback interface hence my ip is 127.0.0.1
* In my linux distro(Arch linux), to change the DNS used, edit the lines in /etc/resolv.conf. The only line in the file should be the local DNS, rest all can be commented. Pinging a website after this should lead to failure.



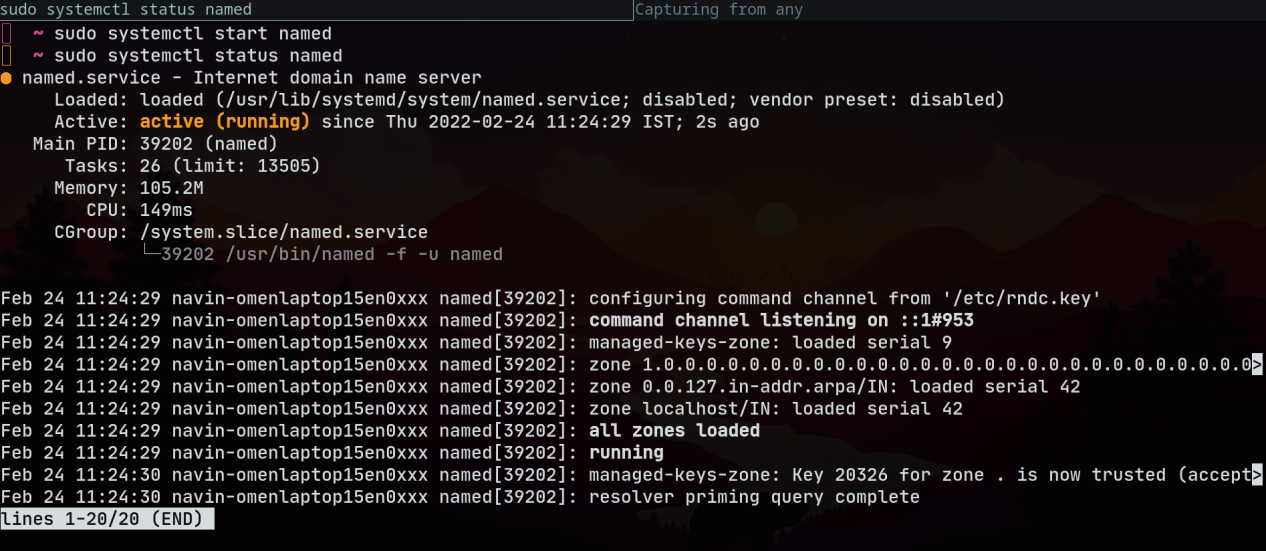
Ping fails, edited /etc/resolv.conf



Failed DNS requests and responses can be seen in wireshark as well

## **Task 3 : Setting up local DNS server**

* Install Bind9 and also start the service, follow so the screenshots :

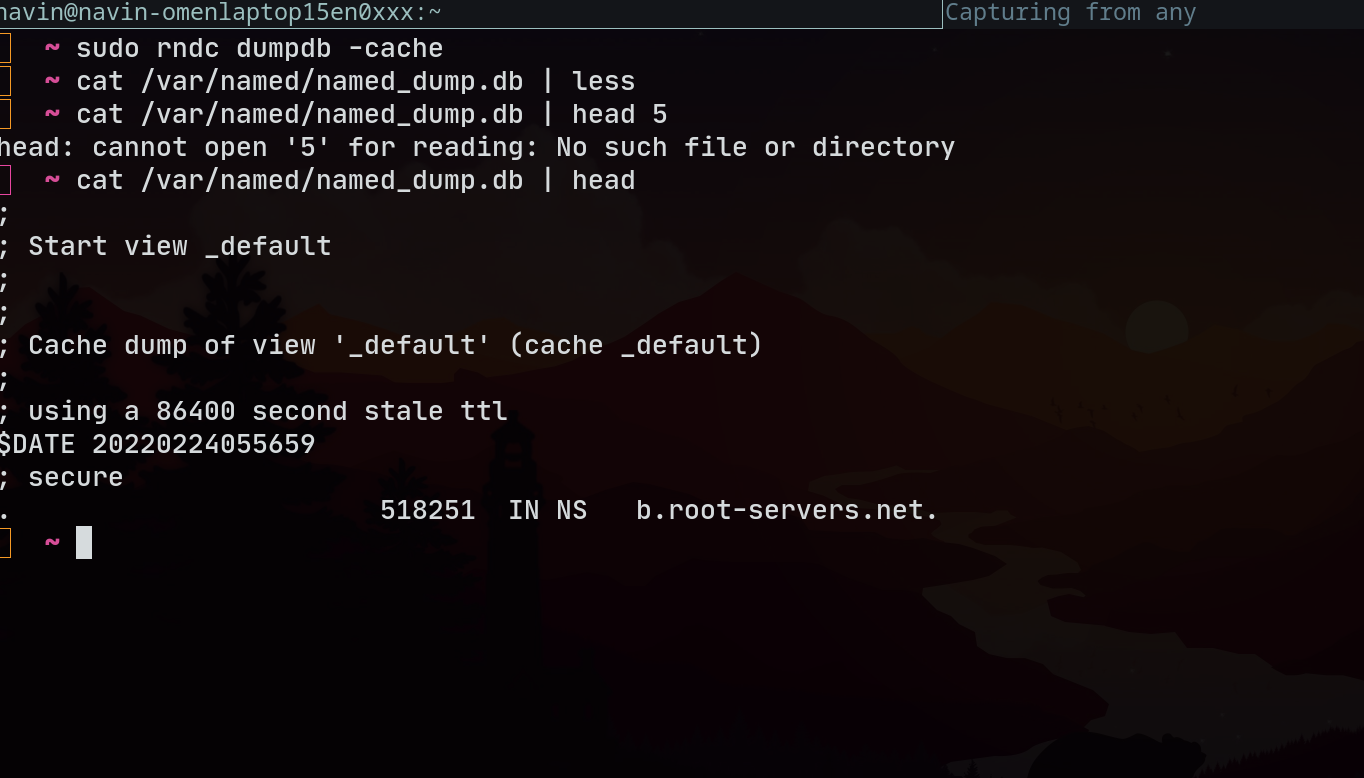


After starting Bind9 daemon



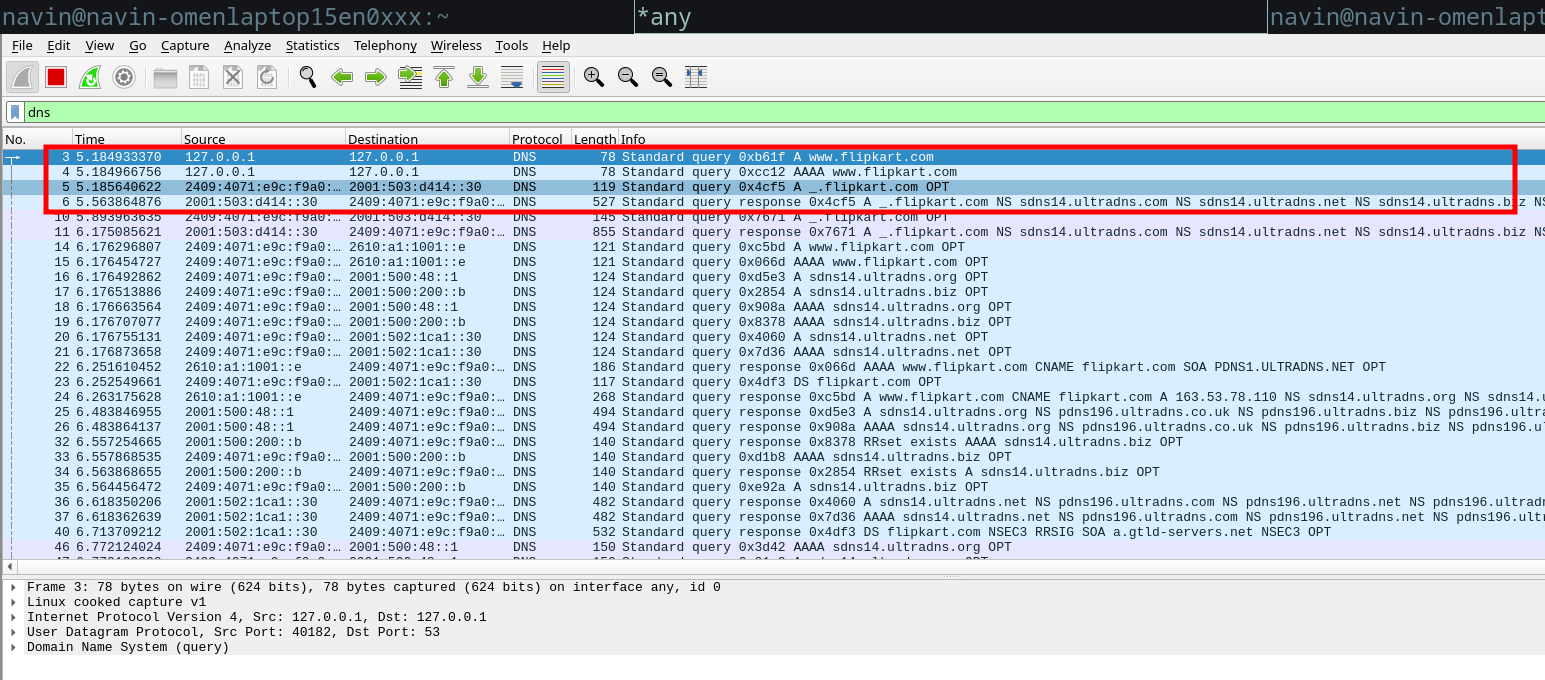
Following conf file for Bind9 (should exist)

* Dump the cache to a db file so it is visible to us using the following commands:

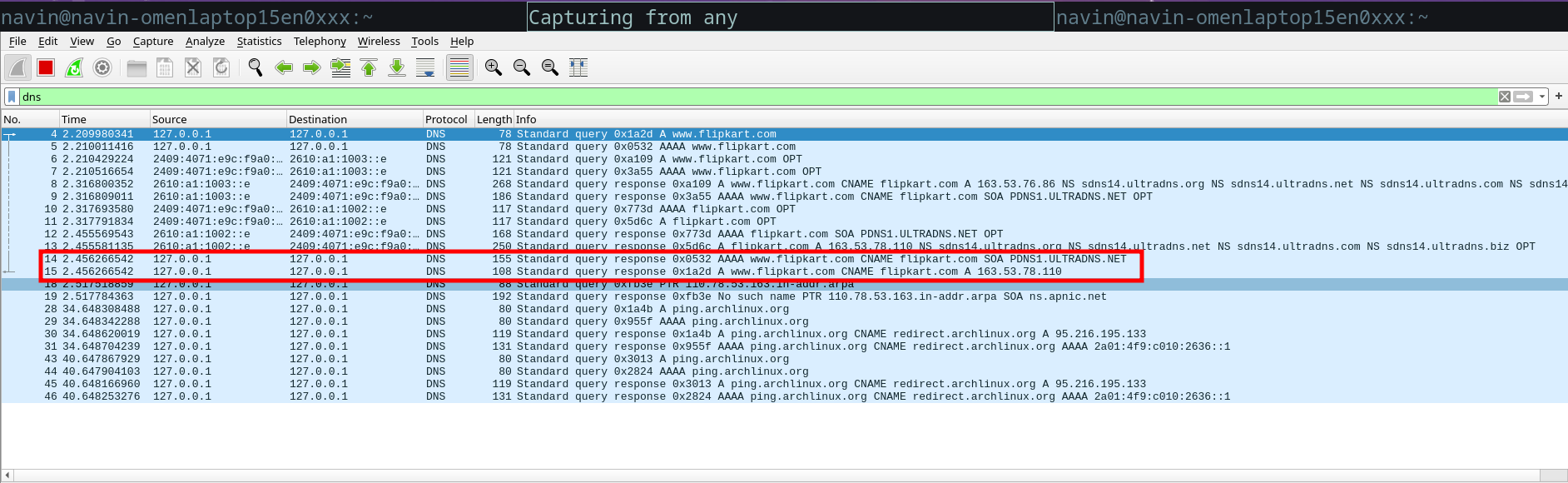


Dumped cache into db file

* Now pinging a website for the first time should cause a rescurive reolving using other DNS serverl, the second ping should be resolved from the local DNS server itself.

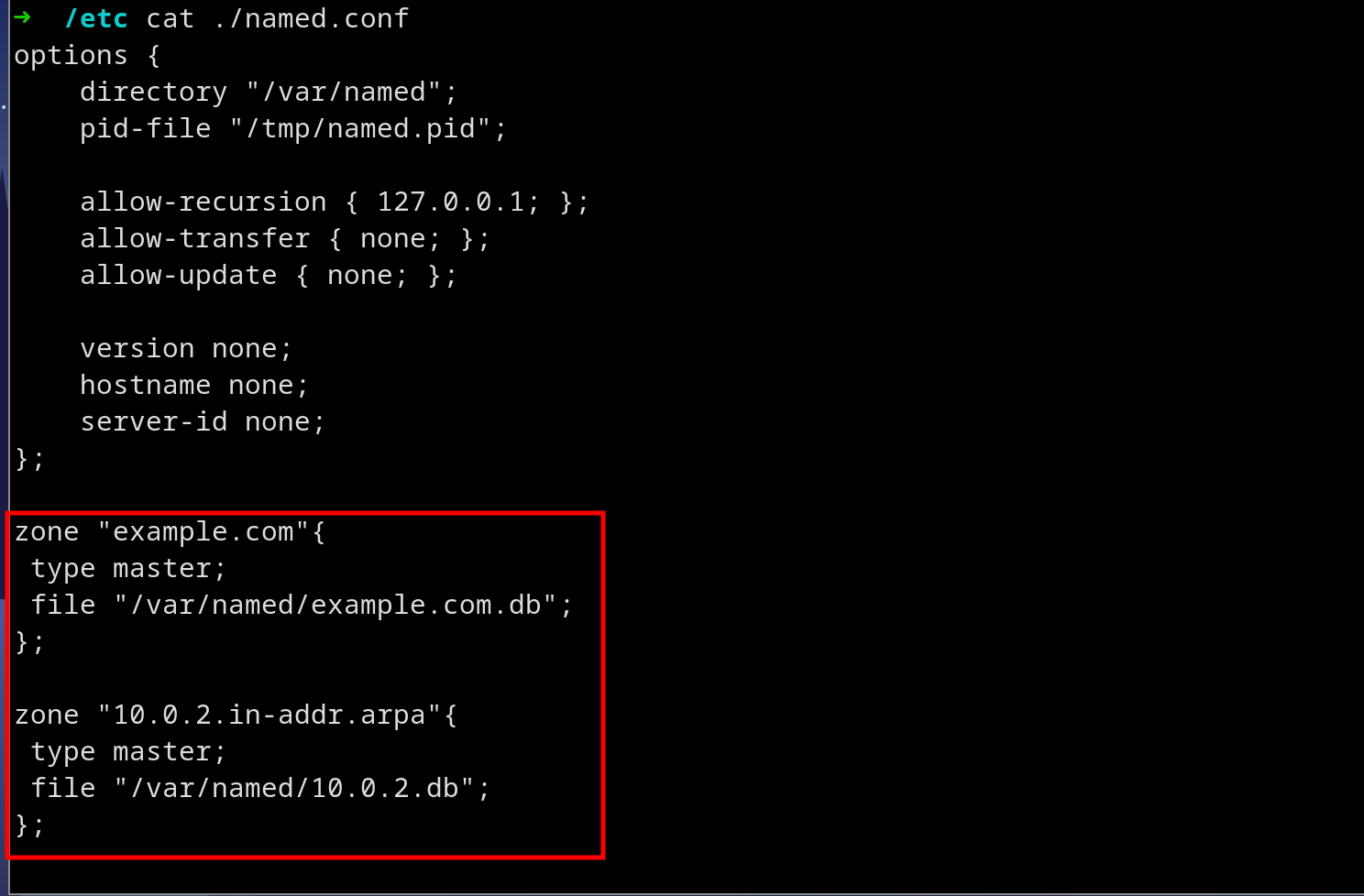


DNS resolved from other servers, first checks in cache

DNS resolved from local cache server

## **Task 5 : Setting up a zone in local DNS**

* First edit the named.conf to check particual files for the query zone like so:

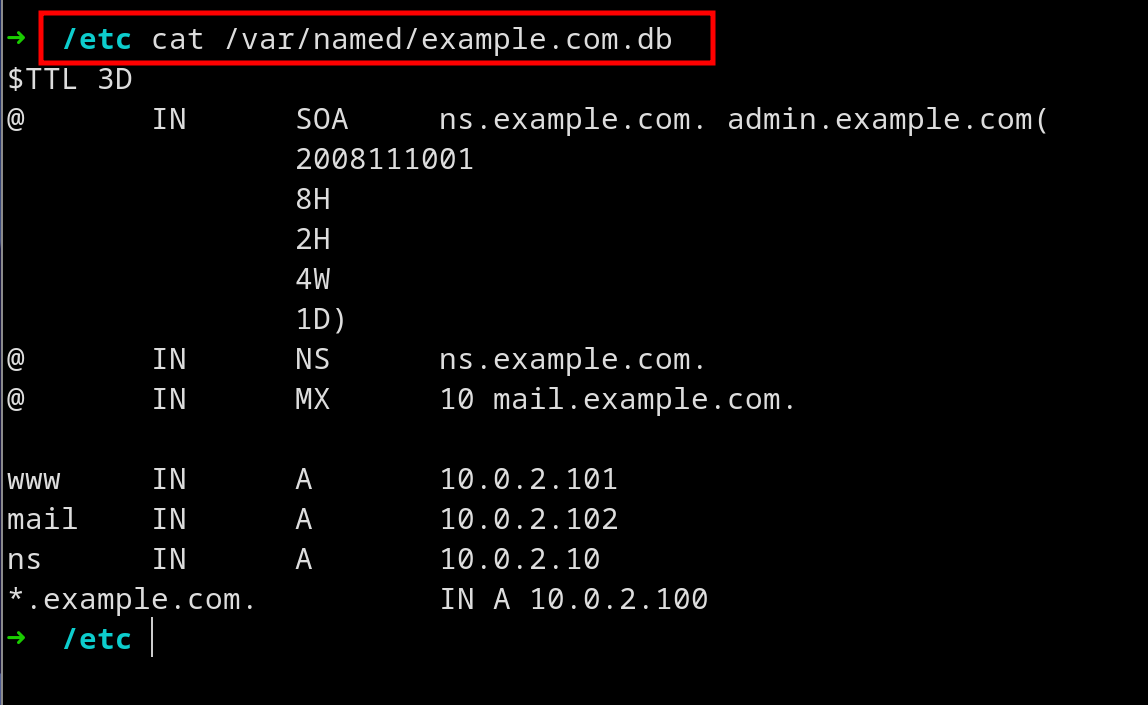


Entering new zones to bind9 service

* Being very careful of the file names, create the zone records (both forward and reverse lookup), doing so:

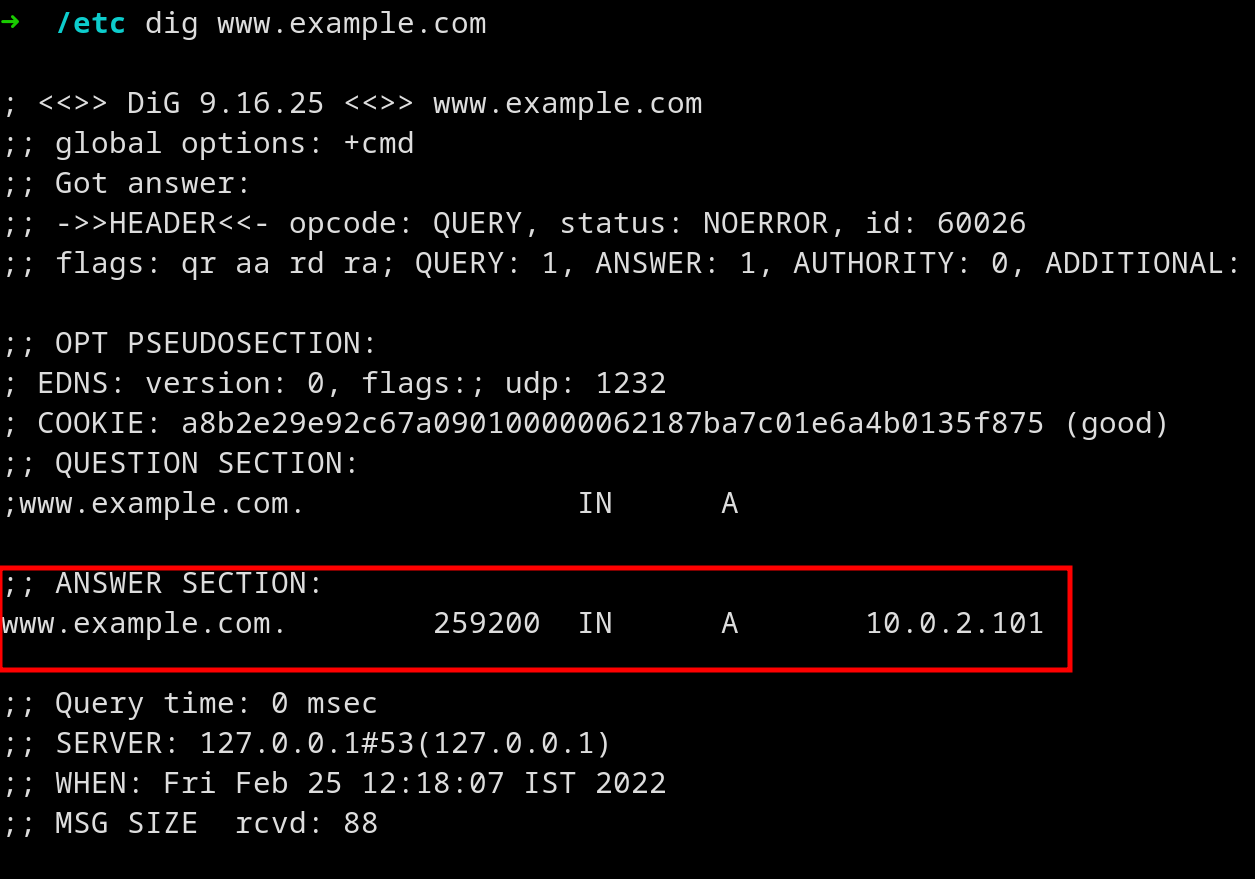


Reverse Lookup Zone records

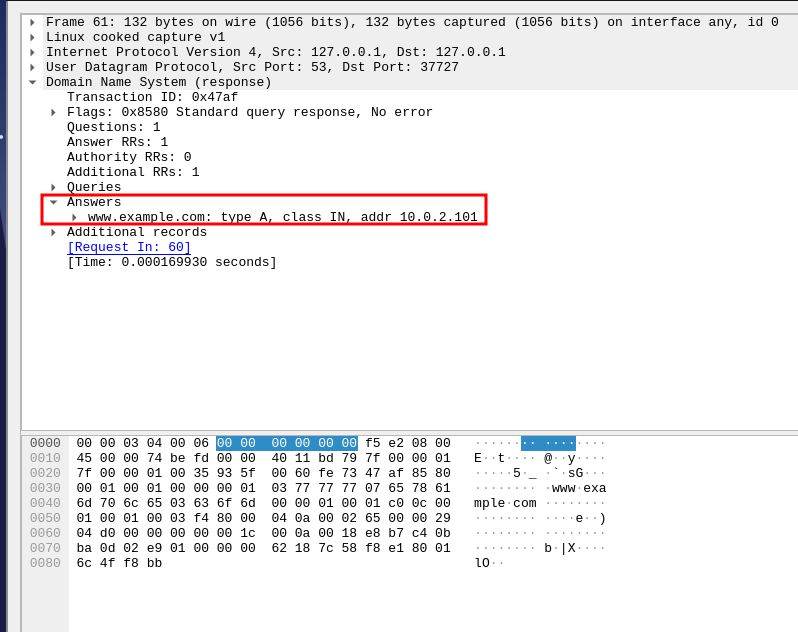


Forward lookup zone records

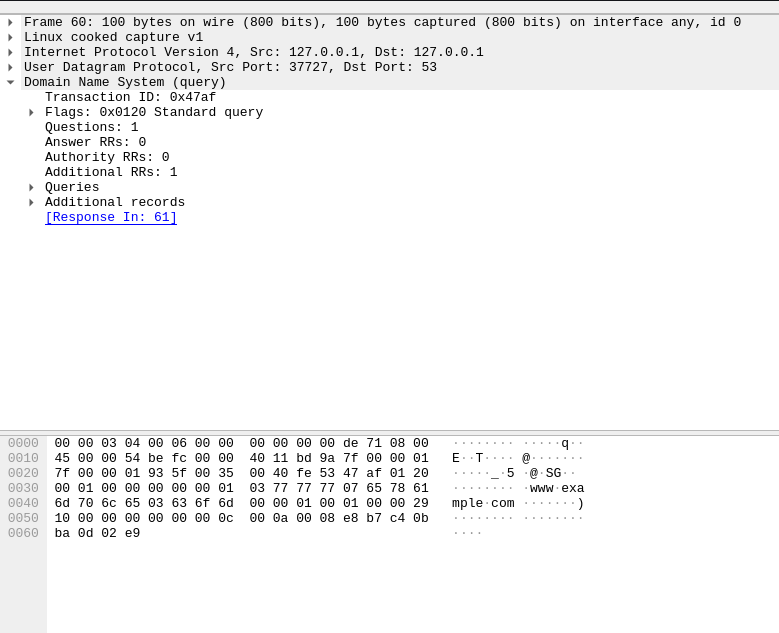
* Now restart the bind9 service using systemctl and now pingin [www.example.com](http://www.example.com) should be resolve from our local DNS and should return contents from it, like so:



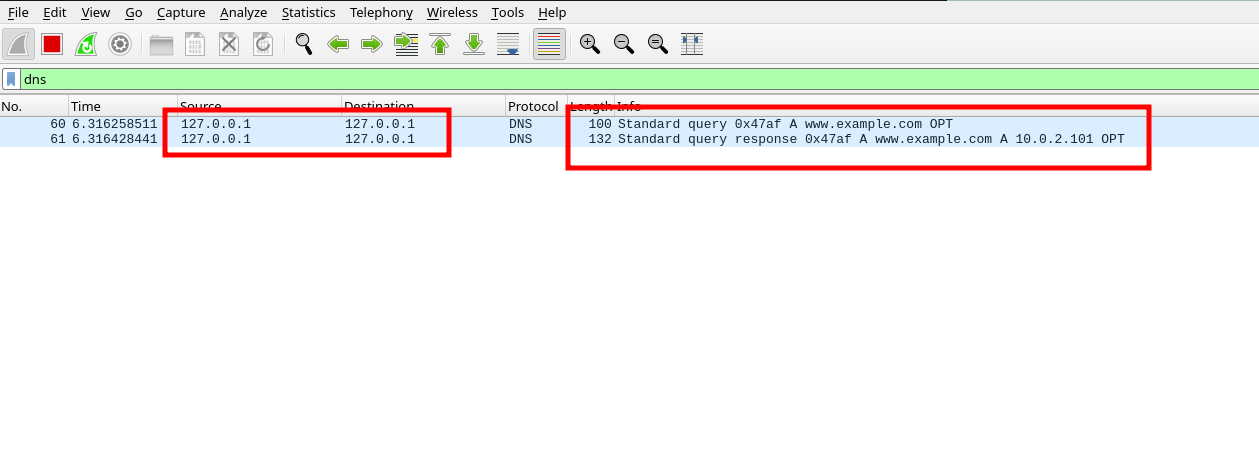
Ping to [www.example.com](http://www.example.com) giving IP from our DNS server



DNS response from local DNS server

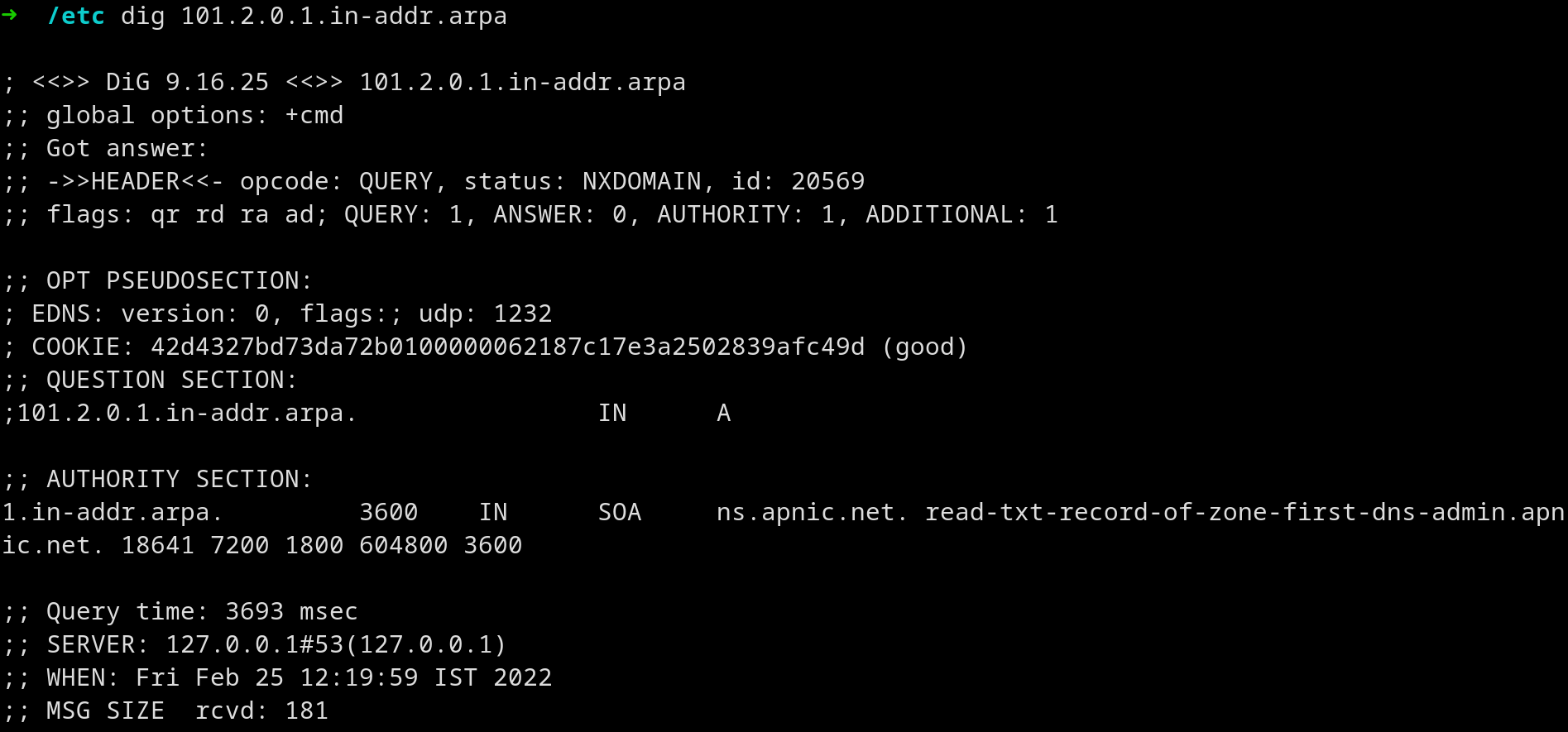


DNS query to local DNS server



WireShark packets with DNS filter

* The same dig command for reverse lookup :



Reverse lookup using dig tool