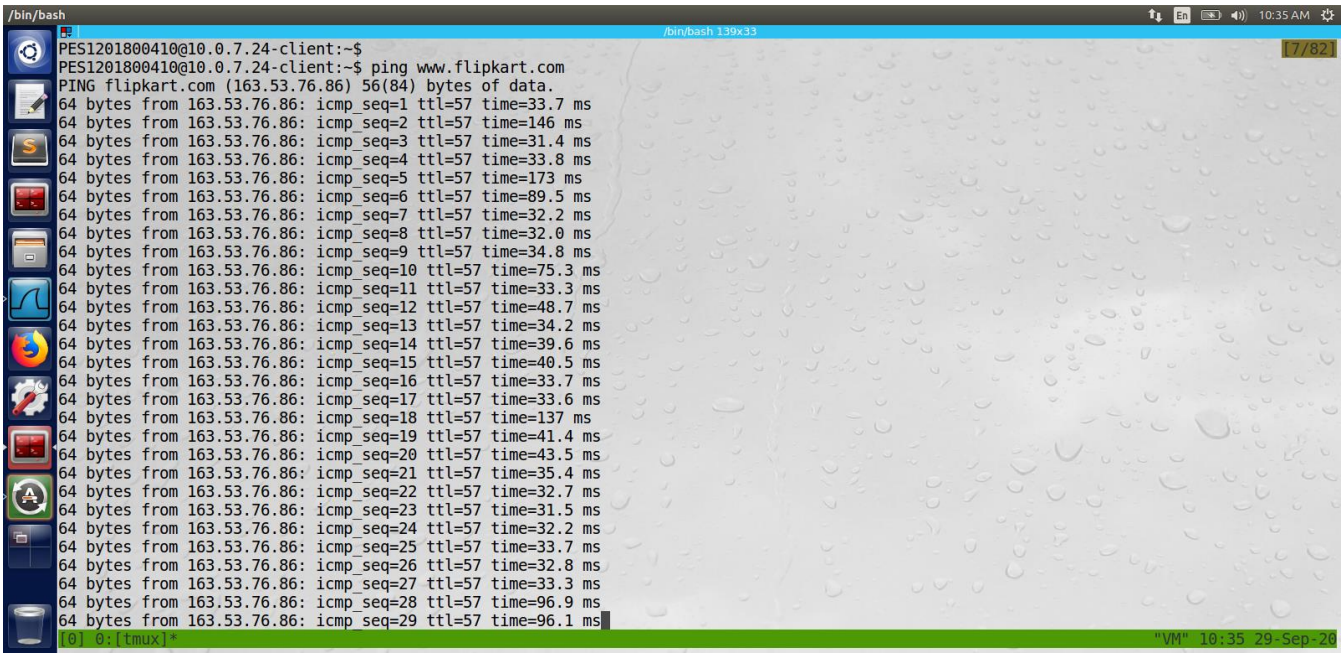
CN Lab Week 4 --- Implementation of a Local DNS Server

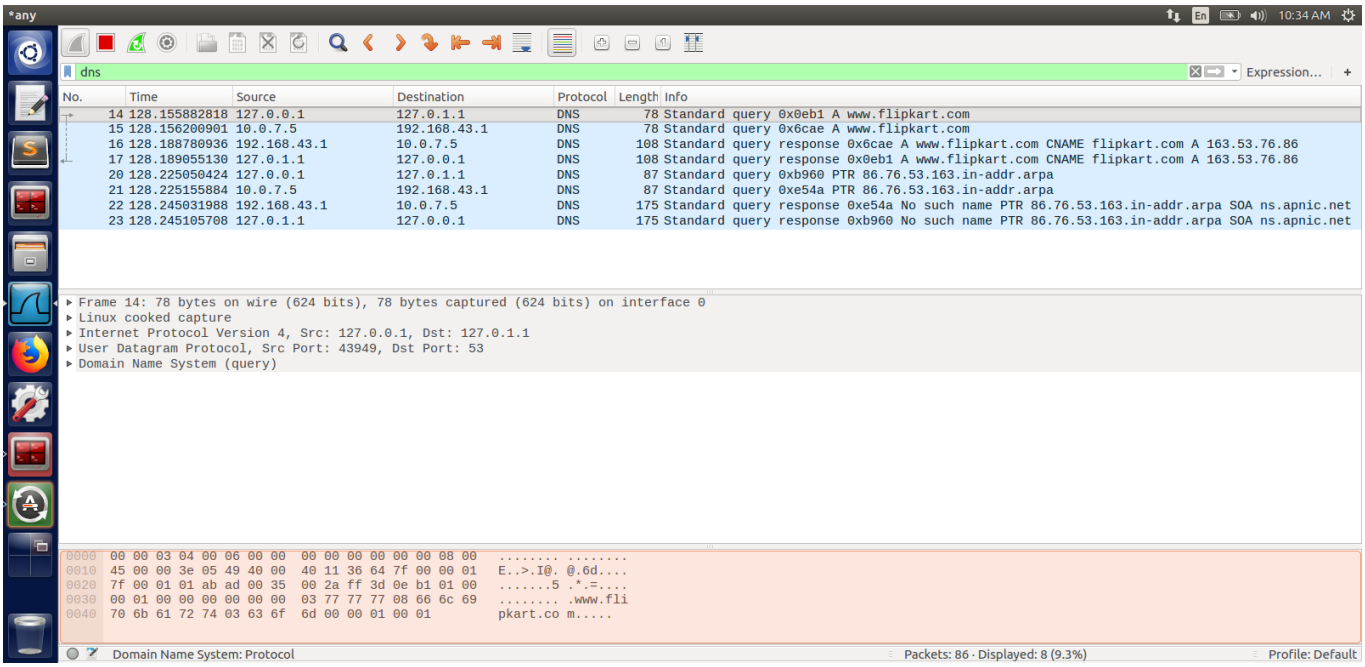
PES1201800410 sem V roll no 24 Prashanth A R

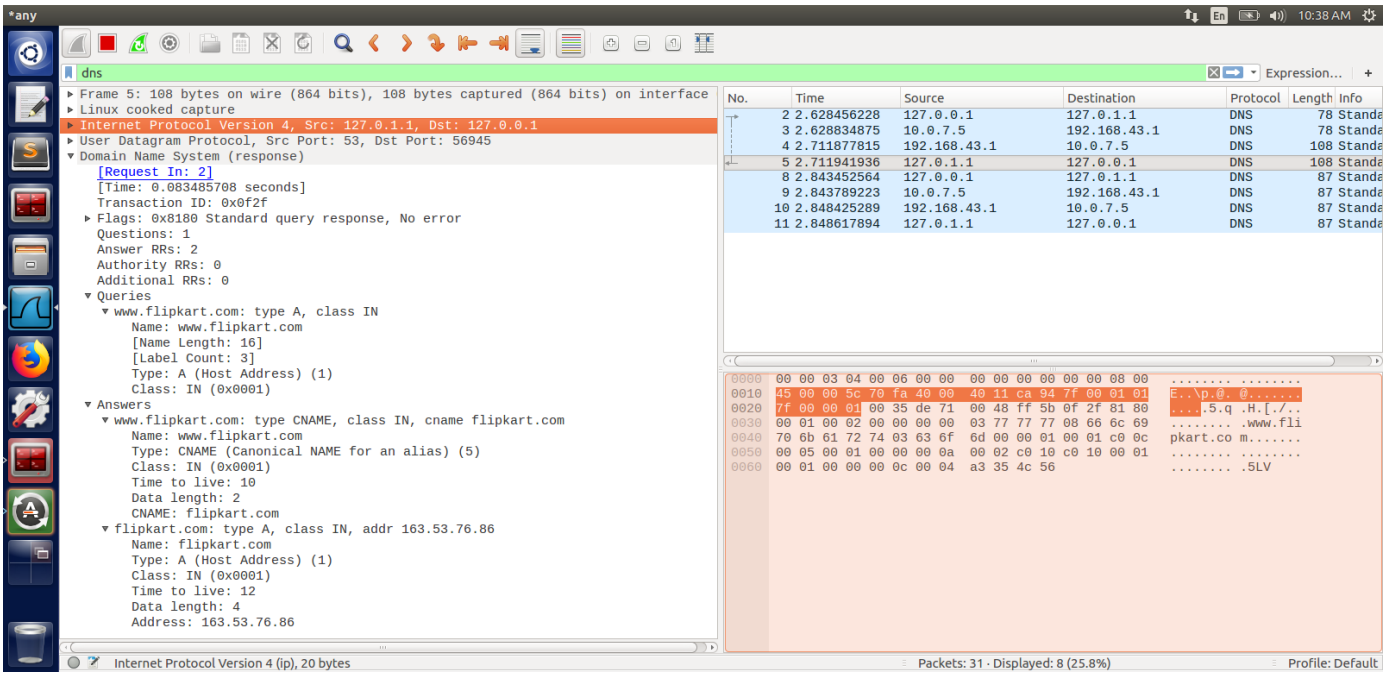
DNS server : 10.0.7.4 Client:10.0.7.5

First Test :



Wireshark output



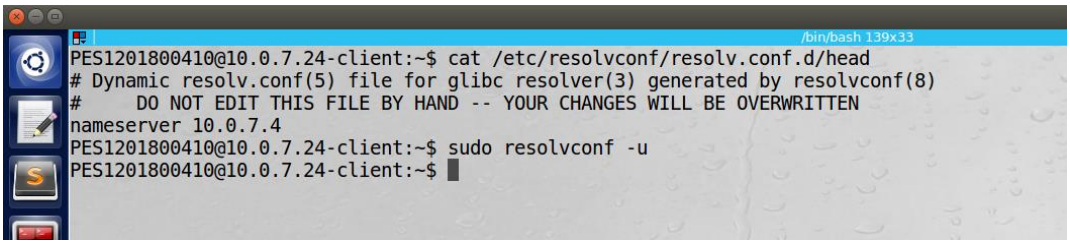


Description:

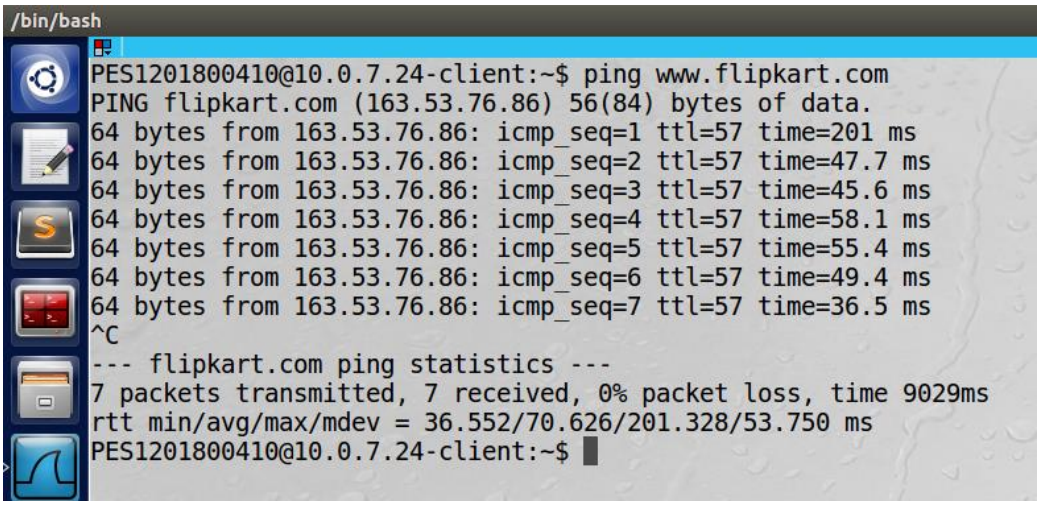
1st it searches the its local dns server which is 127.0.0.1 .

If the website is not found the local dns server it sends dns query to default router dns server. In my case 192.168.43.1

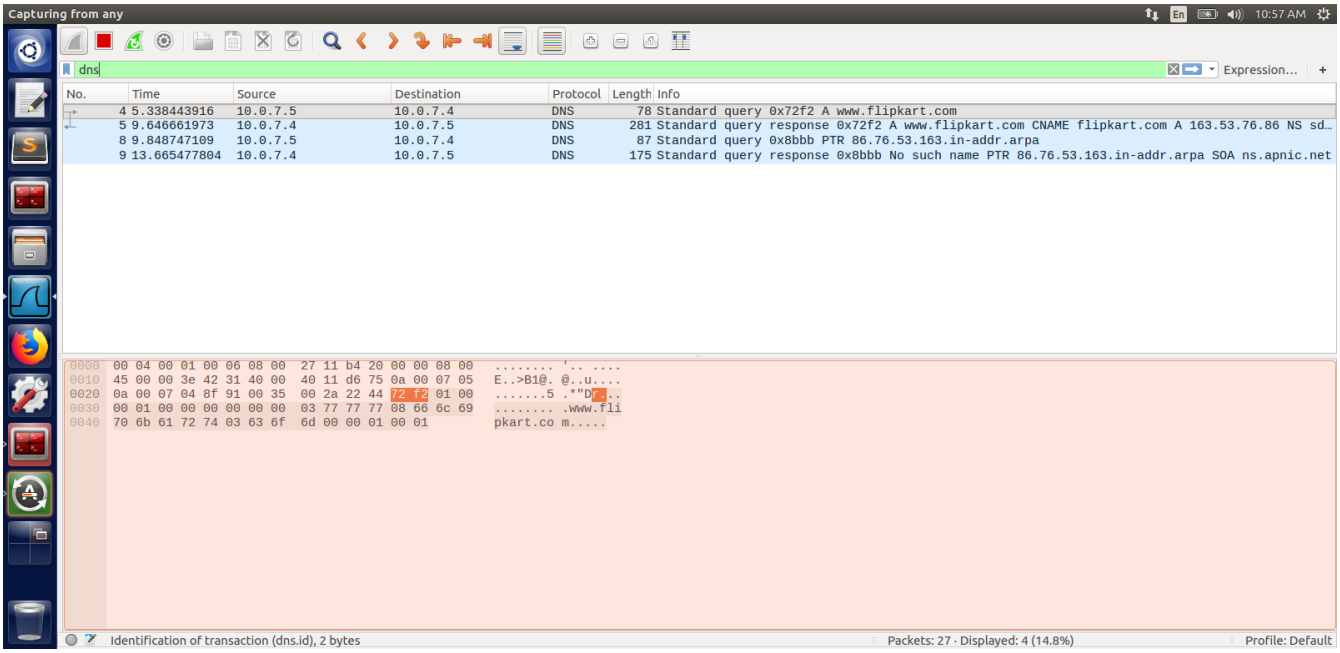
Setup for second test:

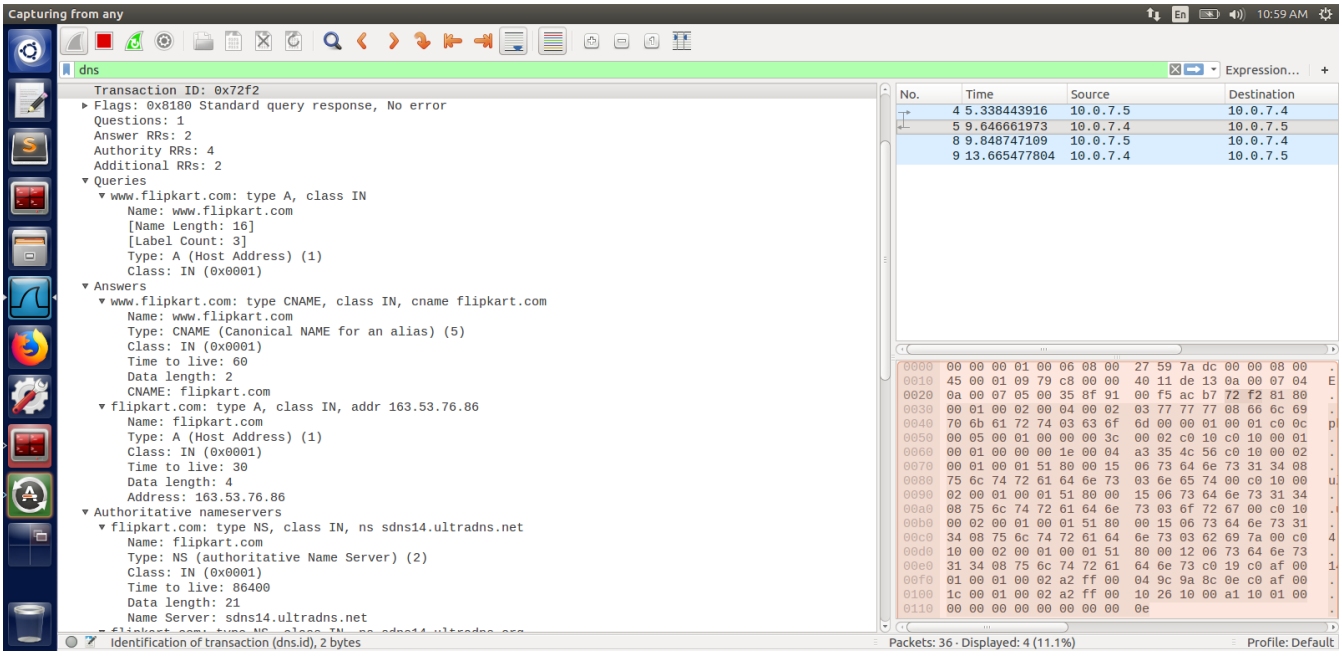


Second Test:



Wireshark output



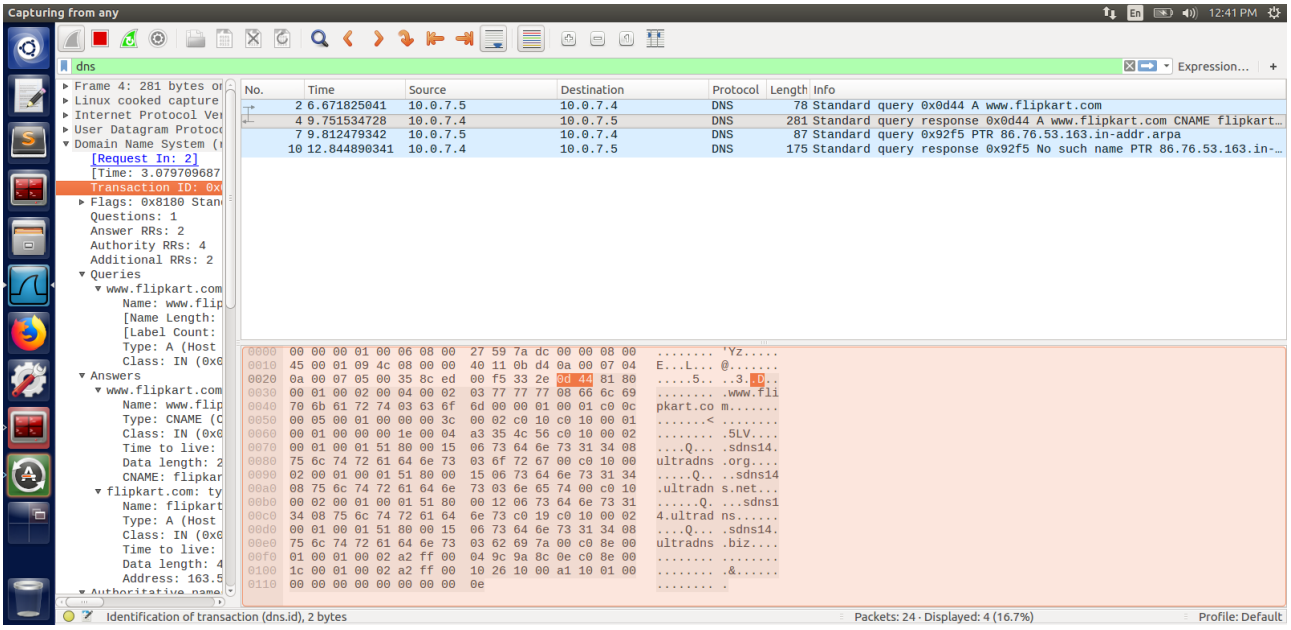


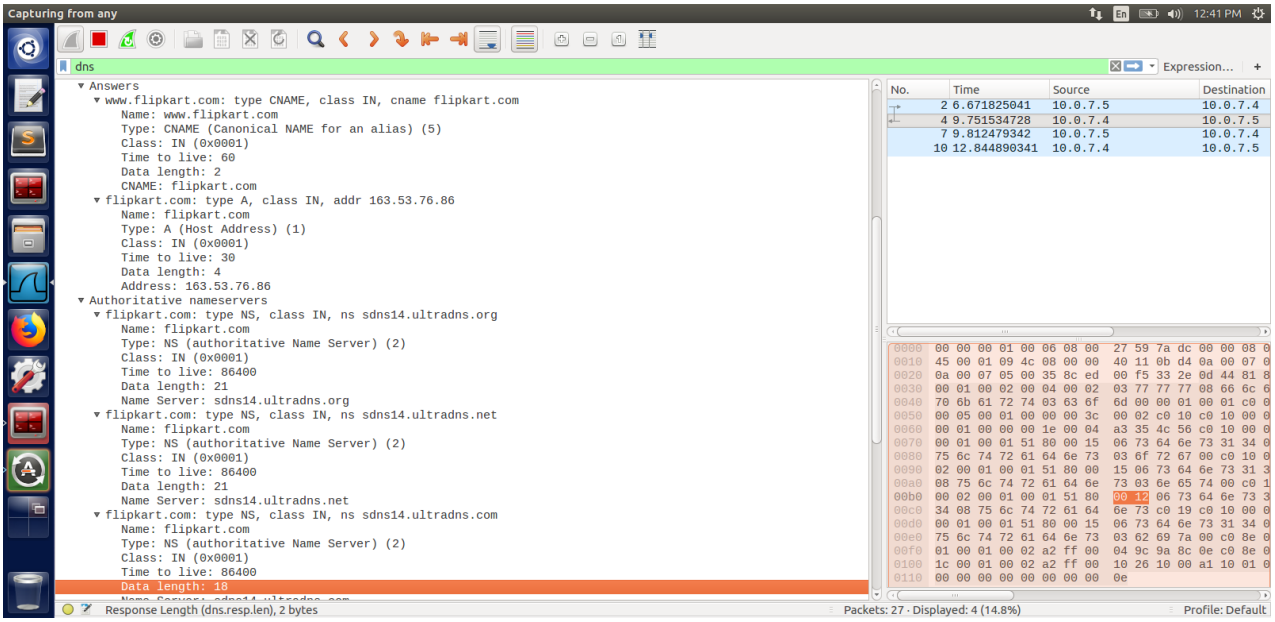
Observation:

This time the dns request is going through 10.0.7.4(dns server which I set) .

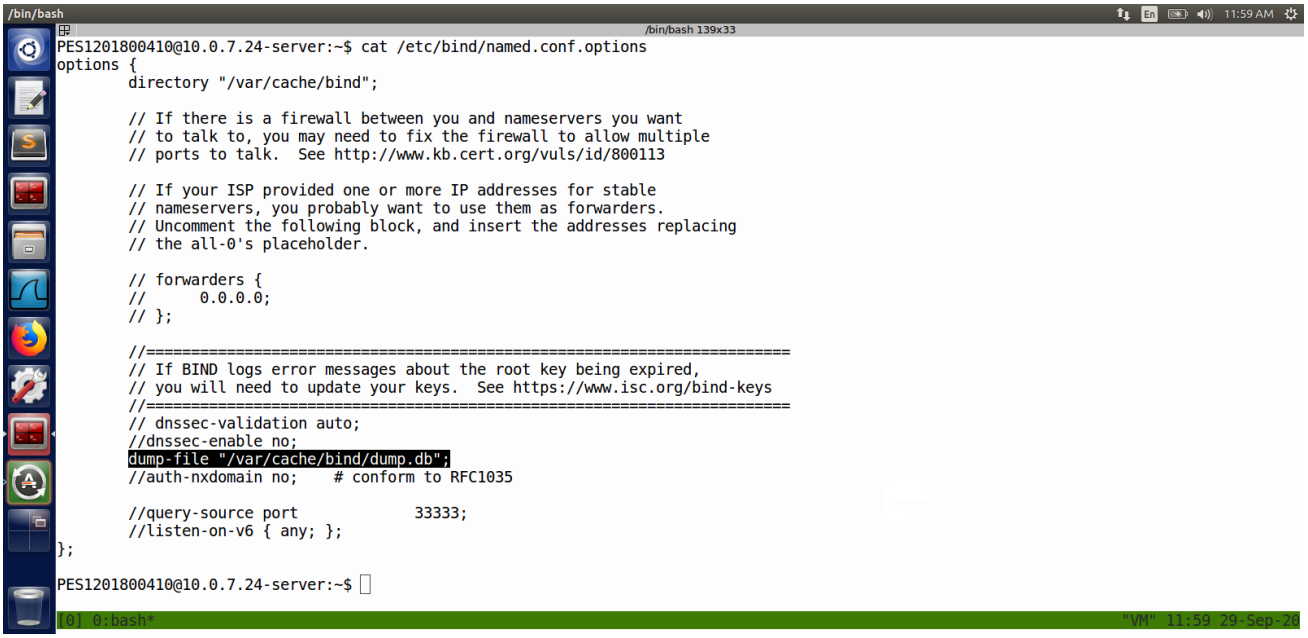
Now VM 10.0.7.4 is acting as dns server for 10.0.7.5

3rd Test:





Setting up DNS server:



named.conf (/etc/bind) - gedit

Open

```
// 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 "/var/cache/bind/example.com.db";
};

zone "7.0.10.in-addr.arpa" {
type master;
file "/var/cache/bind/10.0.7.db";
};
```

Dig www.example.com

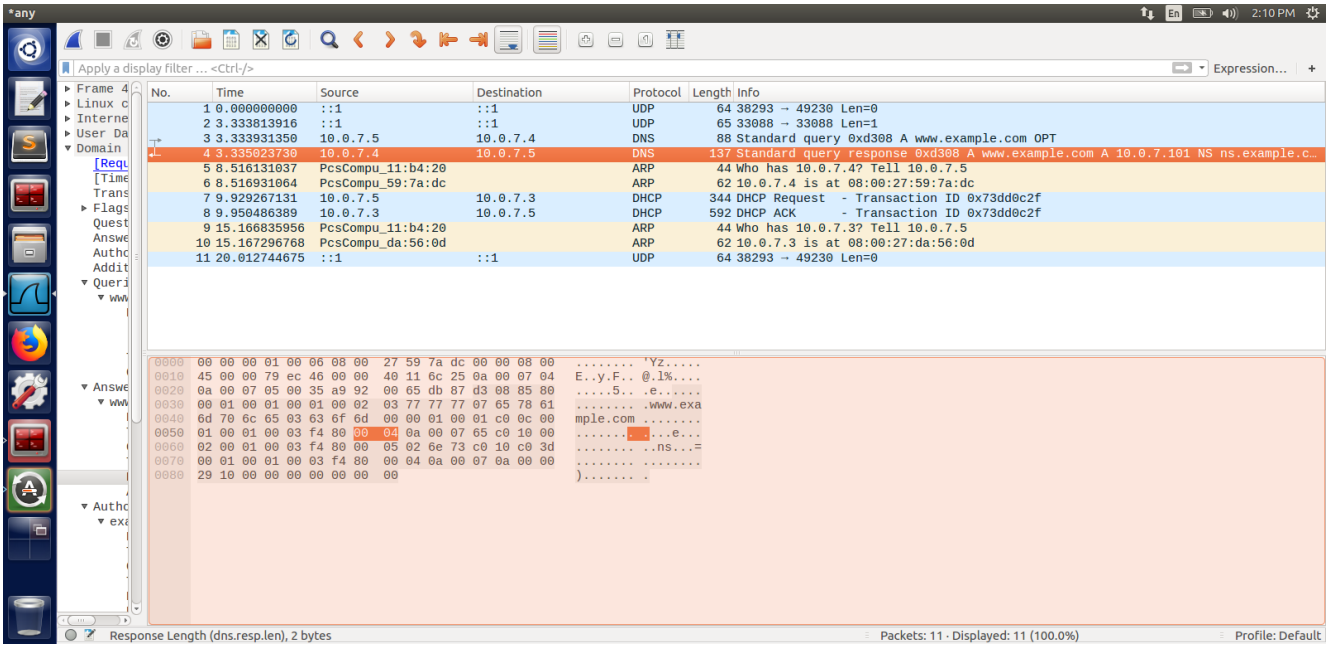
/bin/bash

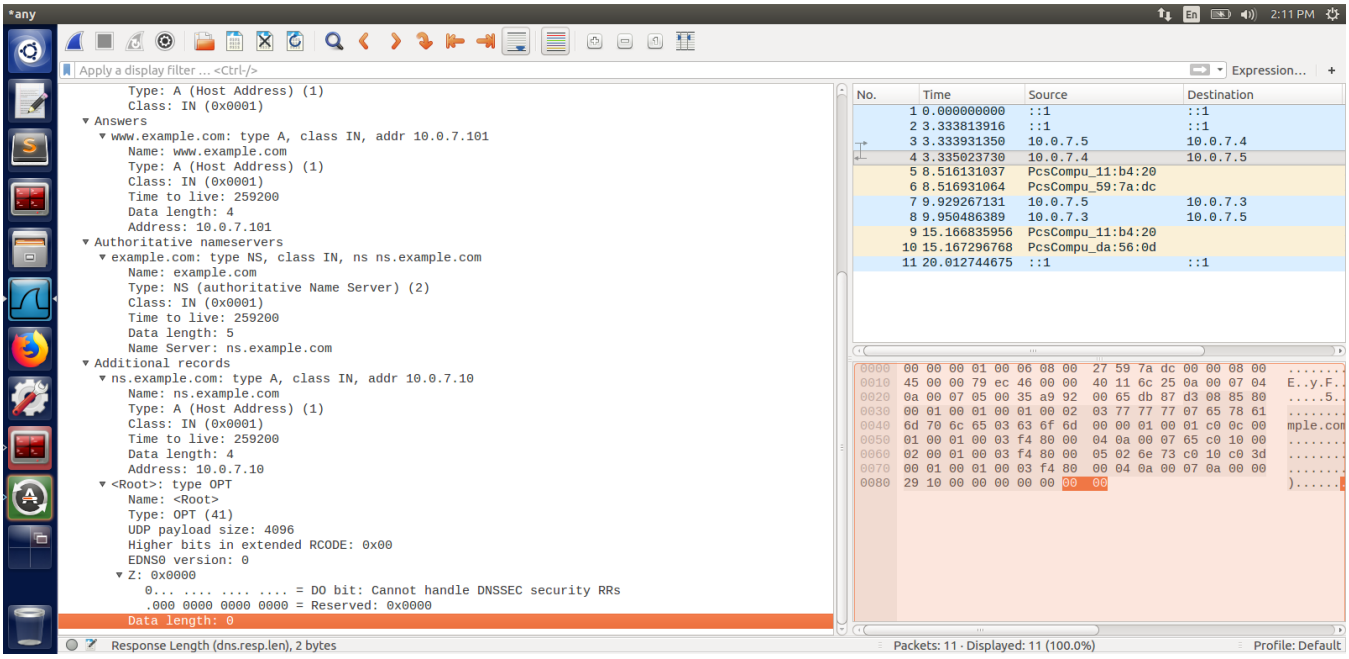
/bin/bash 139x33

```
PES1201800410@10.0.7.24-client:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18758
;; 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       10.0.7.101

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       10.0.7.10

;; Query time: 0 msec
;; SERVER: 10.0.7.4#53(10.0.7.4)
;; WHEN: Tue Sep 29 14:00:57 EDT 2020
;; MSG SIZE  rcvd: 93

PES1201800410@10.0.7.24-client:~$
```

[1] 0:bash- 1:bash*

wireshark output





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?

Ans : UDP

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

Ans : port 53 for both question

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?

Ans: ip address of dns - 10.0.7.4. it is what I have set it to be the local dns server so yes it is one of the local dns server

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

And: type: A , it didn’t contain any answer.

5)Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans: I got 2 answers

Each answer contained hostname , Type , Class , Time to live , Data length , CNAME or Address

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?

Ans: The 1st SYN packet was sent to 163.53.76.86 which is the ip address given by dns.