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

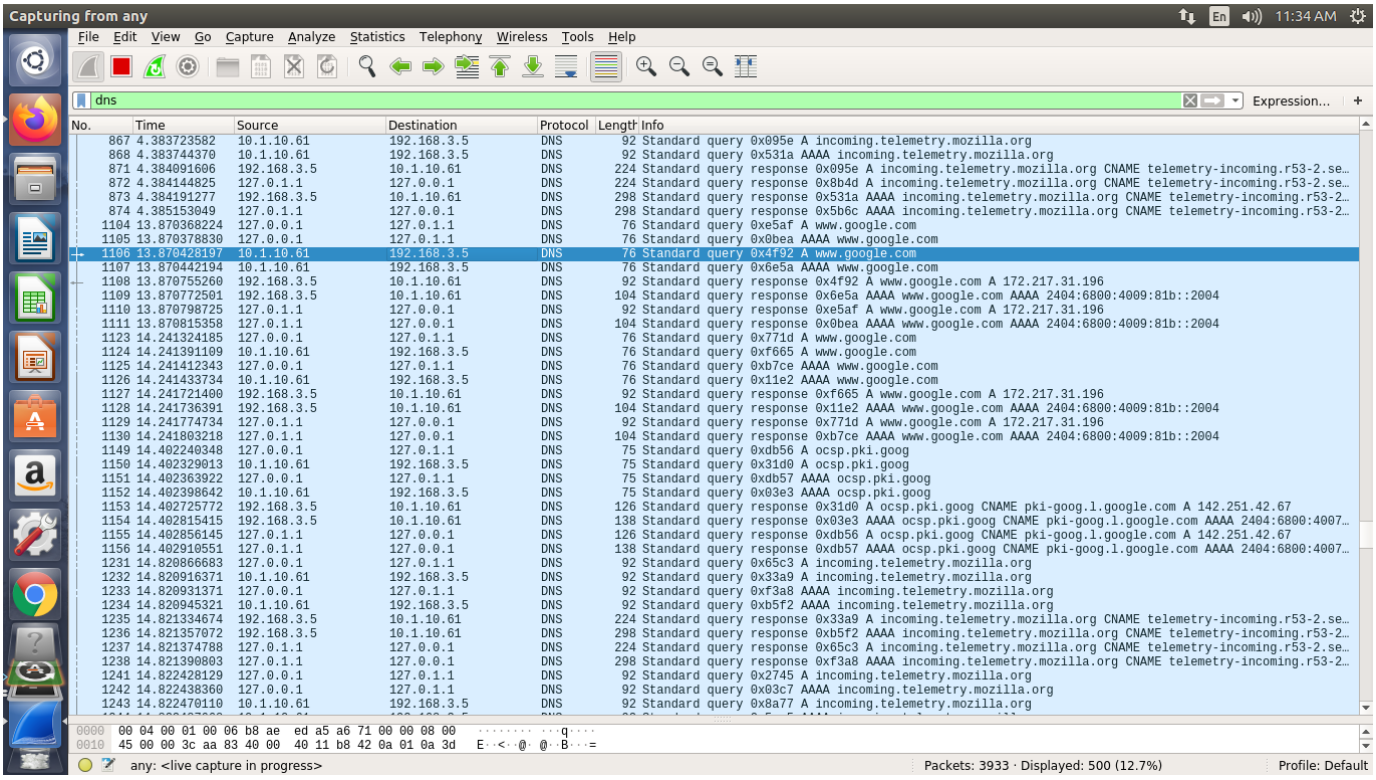
SRN : PES1UG20CS670

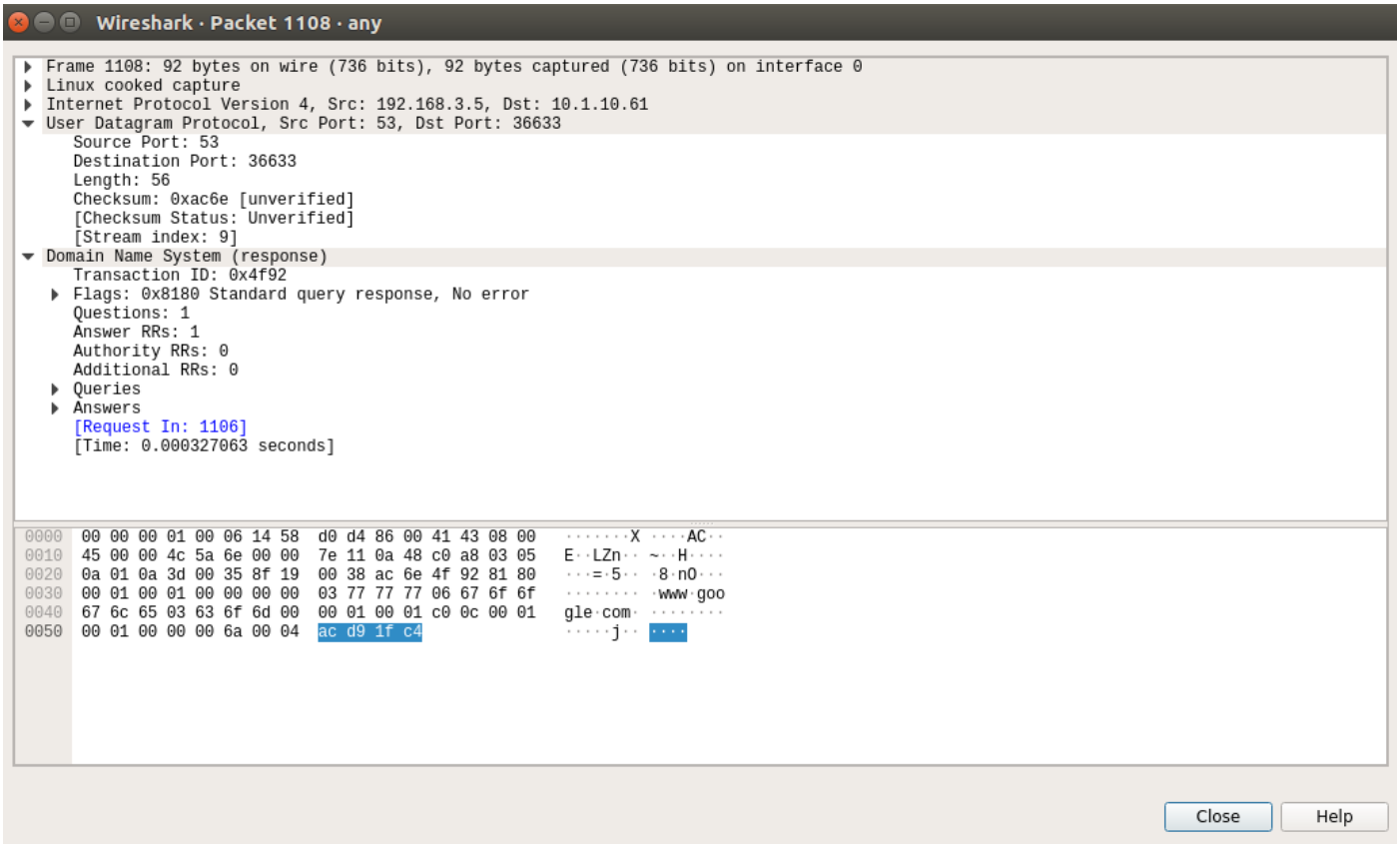
Roll no.: 31

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):

```
Open    head
        /etc/resolvconf/resolv.conf.d                    Save
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.1.10.26
```

```
student@student-H81H3-I:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
student@student-H81H3-I:~$ sudo cat /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.1.10.26
student@student-H81H3-I:~$
```

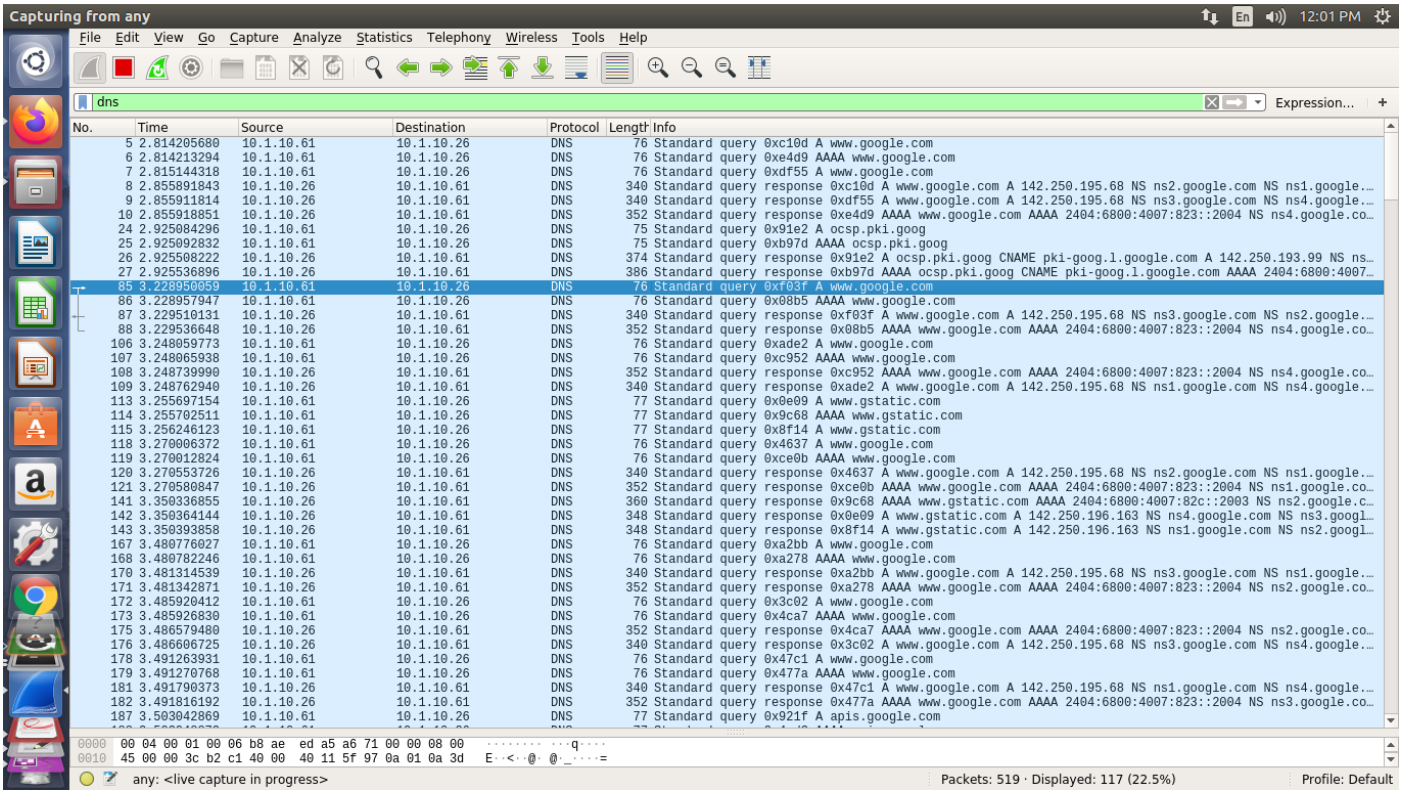
1.2 Run the following command for the change to take effect.

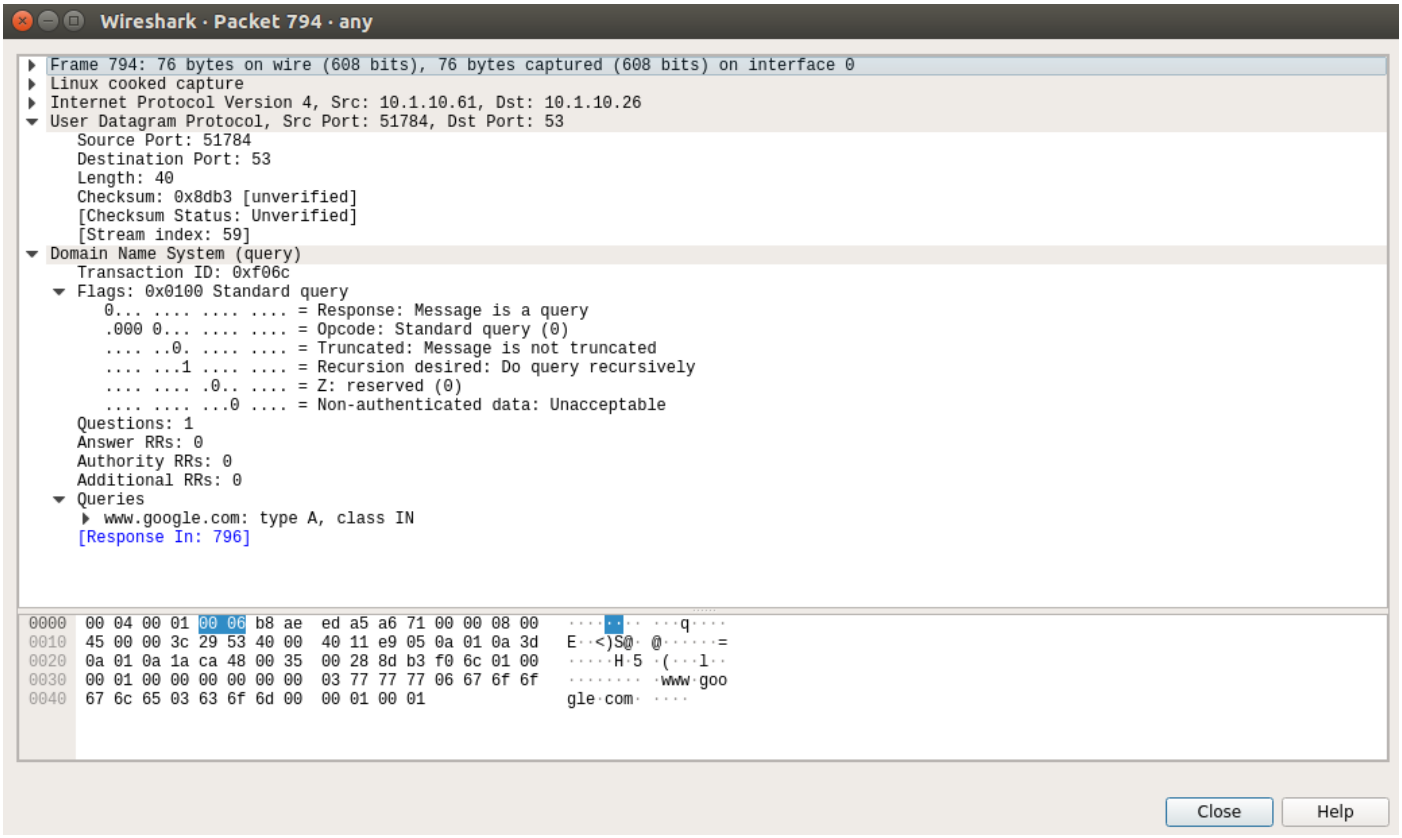
sudo resolvconf -u

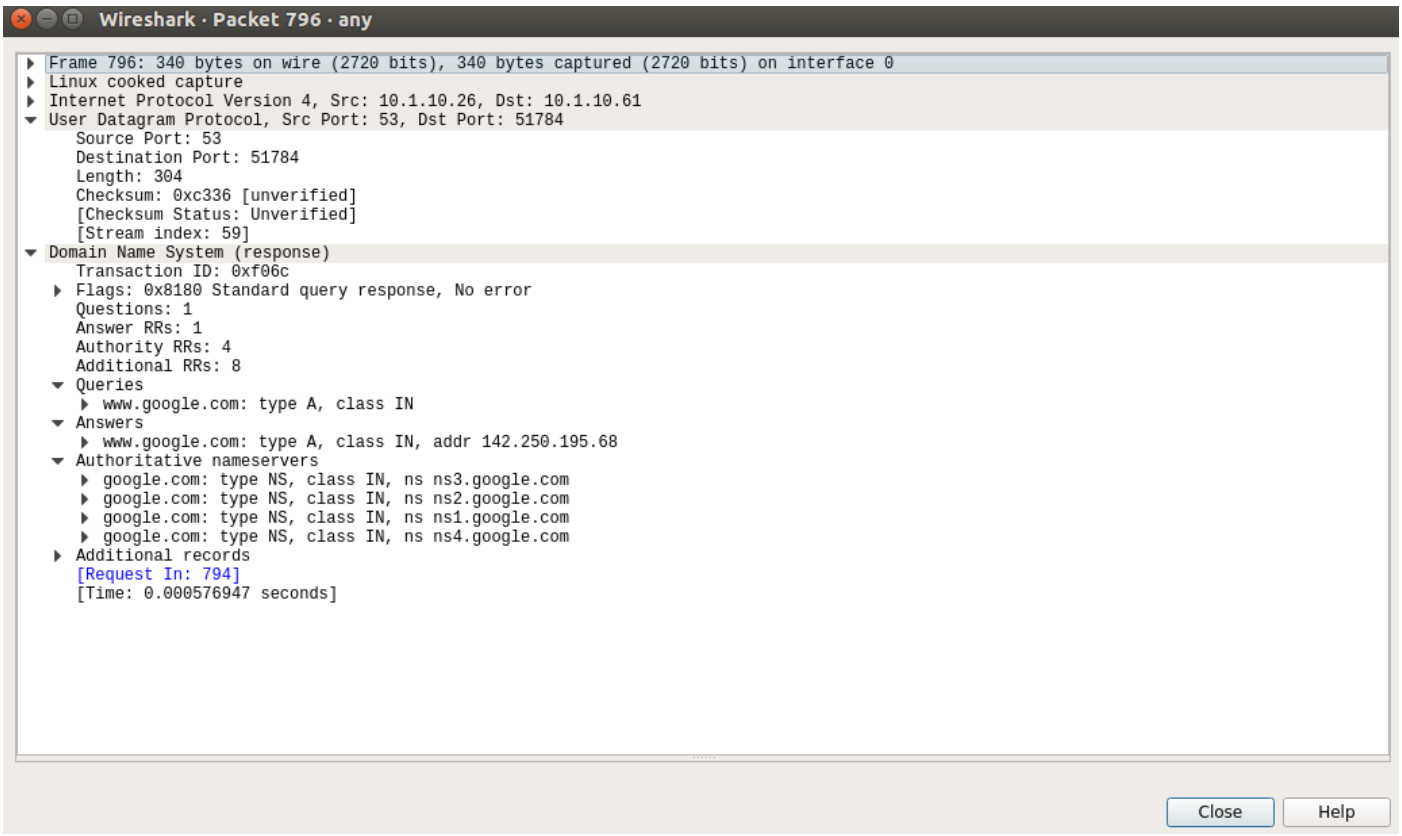
```
student@student-H81H3-I:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
student@student-H81H3-I:~$ sudo cat /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.1.10.26
student@student-H81H3-I:~$ sudo resolvconf -u
student@student-H81H3-I:~$
```

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).



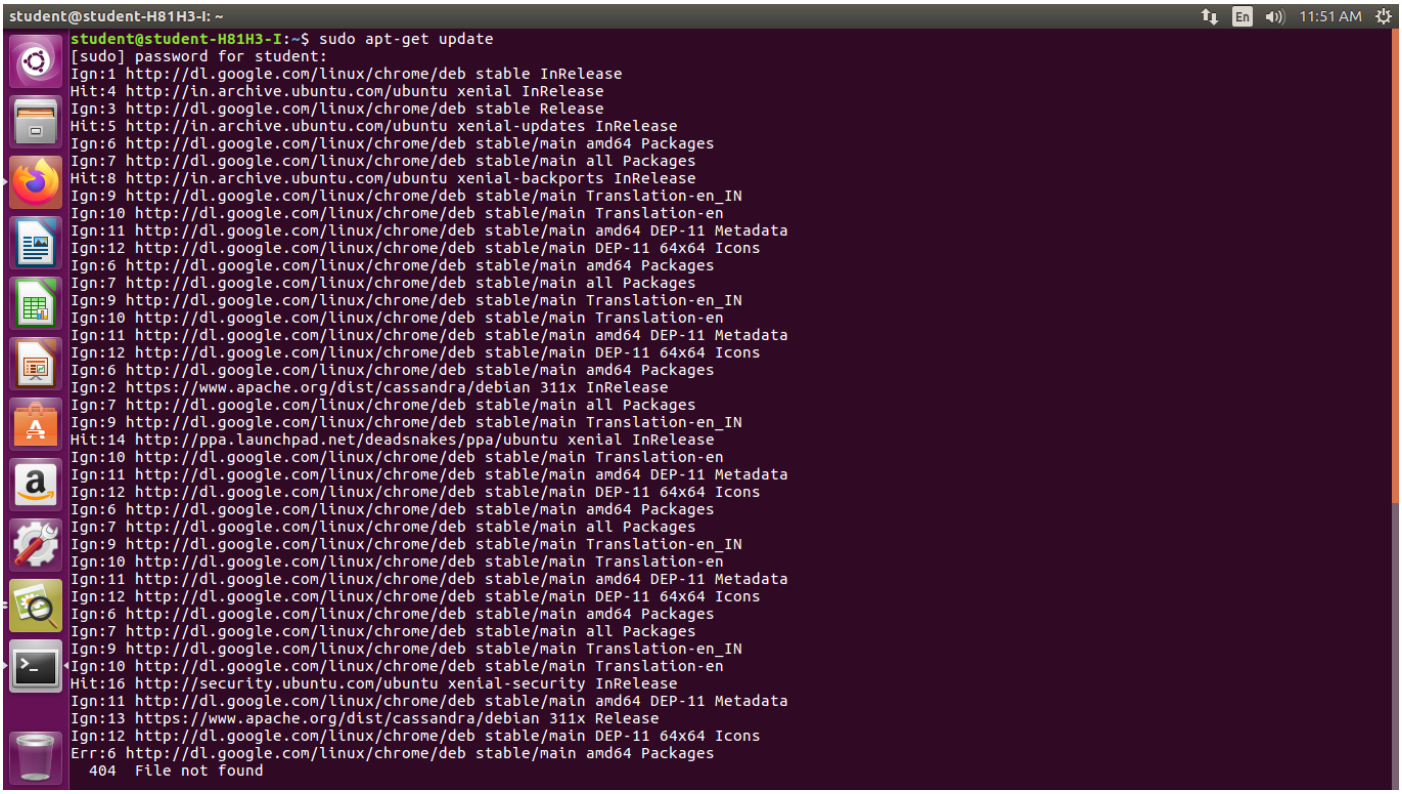

Wireshark · Packet 794 · any
Frame 794: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.1.10.61, Dst: 10.1.10.26
User Datagram Protocol, Src Port: 51784, Dst Port: 53
Source Port: 51784
Destination Port: 53
Length: 40
Checksum: 0x8db3 [unverified]
[Checksum Status: Unverified]
[Stream index: 59]
Domain Name System (query)
Transaction ID: 0xf06c
Flags: 0x0100 Standard query
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... .0.. .... = Z: reserved (0)
....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.google.com: type A, class IN
[Response In: 796]
0000 00 04 00 01 00 06 b8 ae ed a5 a6 71 00 00 08 00
0010 45 00 00 3c 29 53 40 00 40 11 e9 05 0a 01 0a 3d
0020 0a 01 0a 1a ca 48 00 35 00 28 8d b3 f0 6c 01 00
0030 00 01 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f
0040 67 6c 65 03 63 6f 6d 00 00 01 00 01
gle com
Close
Help


Wireshark · Packet 796 · any
Frame 796: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.1.10.26, Dst: 10.1.10.61
User Datagram Protocol, Src Port: 53, Dst Port: 51784
Source Port: 53
Destination Port: 51784
Length: 304
Checksum: 0xc336 [unverified]
[Checksum Status: Unverified]
[Stream index: 59]
Domain Name System (response)
Transaction ID: 0xf06c
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 4
Additional RRs: 8
Queries
www.google.com: type A, class IN
Answers
www.google.com: type A, class IN, addr 142.250.195.68
Authoritative nameservers
google.com: type NS, class IN, ns ns3.google.com
google.com: type NS, class IN, ns ns2.google.com
google.com: type NS, class IN, ns ns1.google.com
google.com: type NS, class IN, ns ns4.google.com
Additional records
[Request In: 794]
[Time: 0.000576947 seconds]
Close
Help

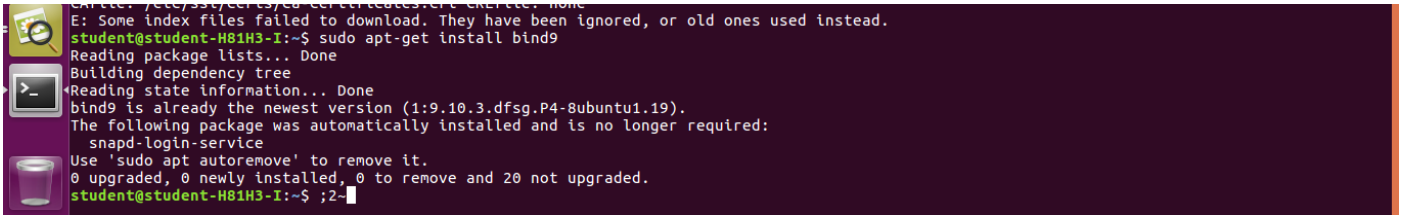
Task 2: Set Up a Local DNS Server

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

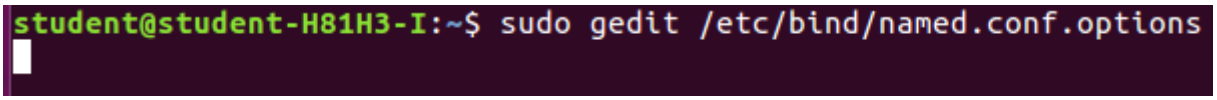
$ sudo apt-get update

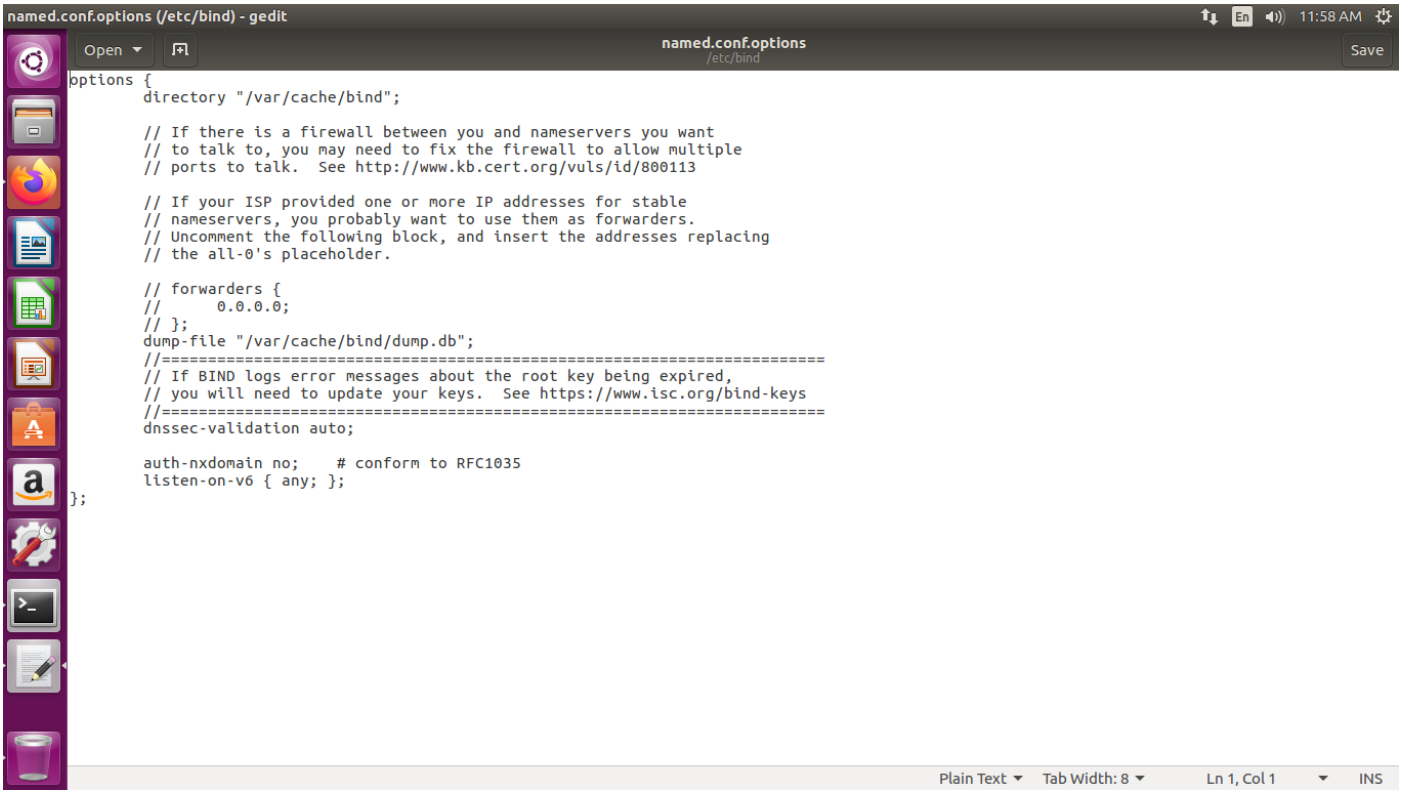


$ sudo apt-get install bind9



2.2 Configure the BIND9 Server :



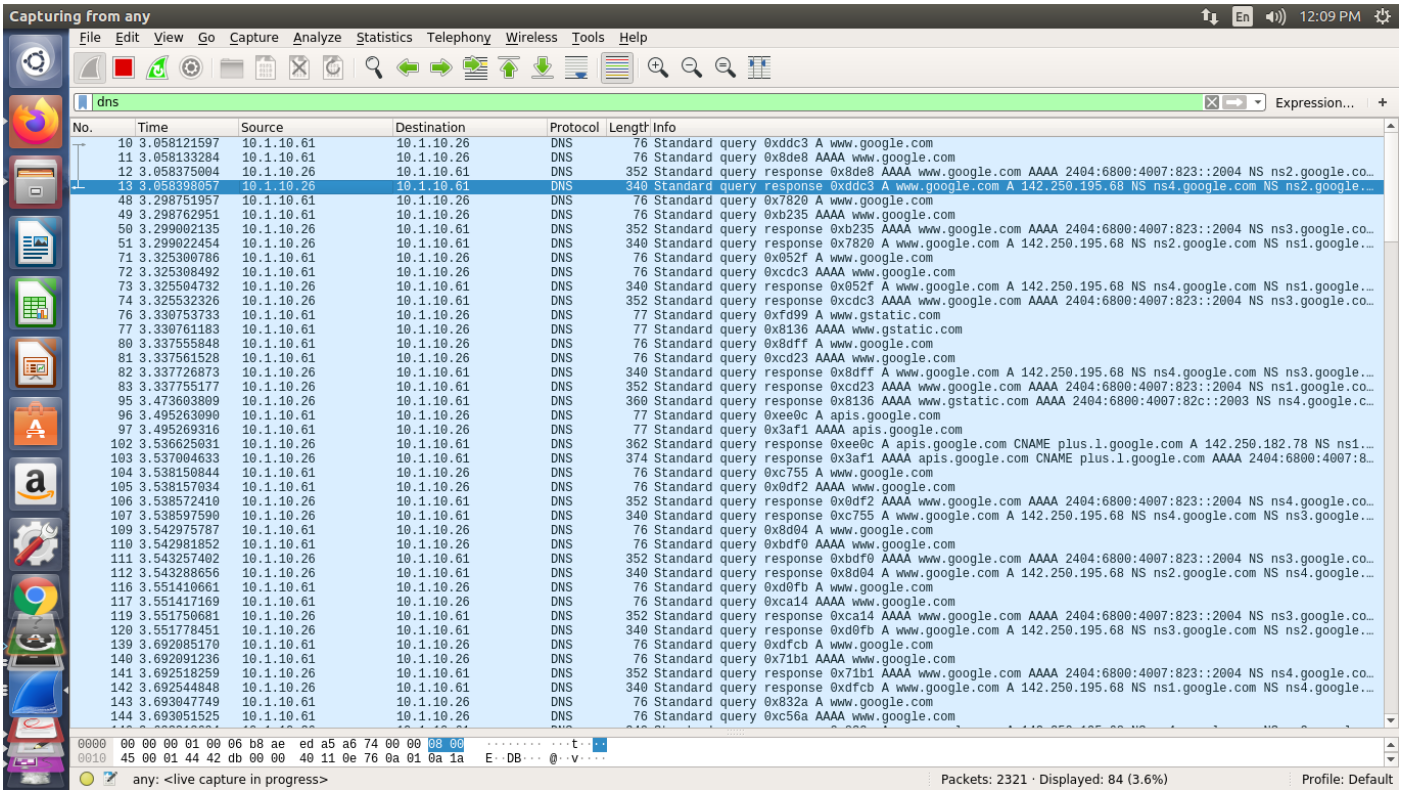


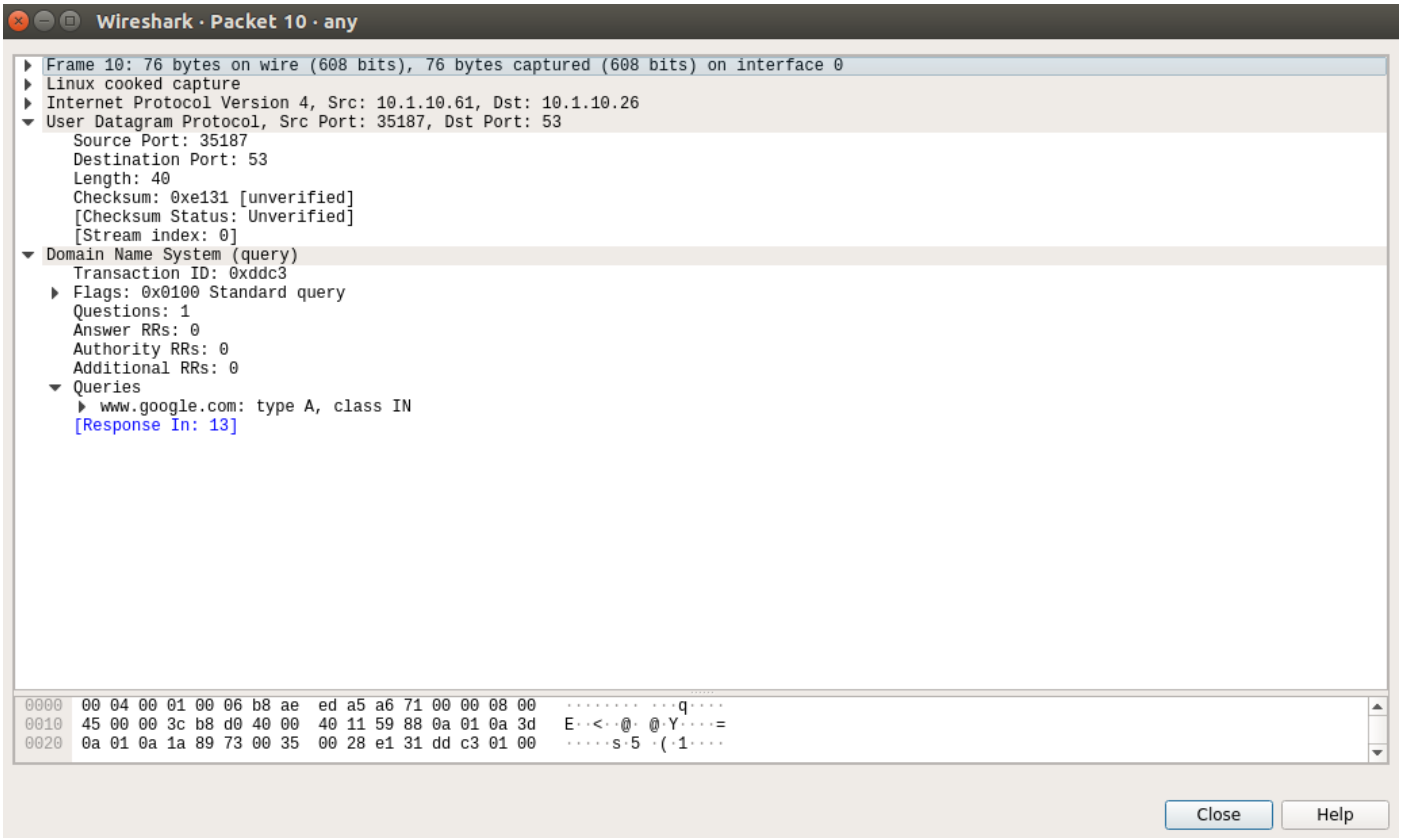
2.3 Start DNS server :

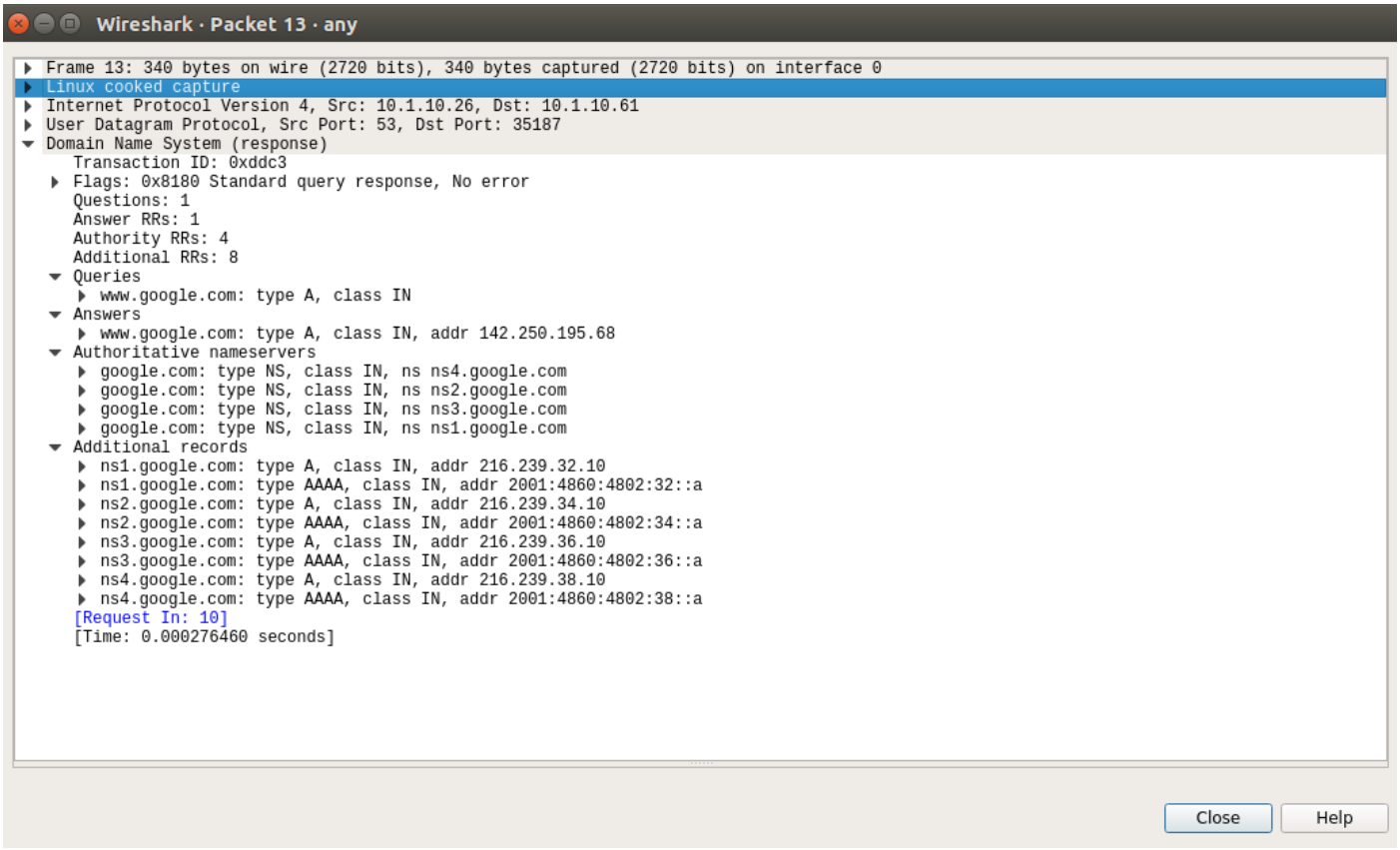
```
student@student-H81H3-I:~$ sudo service bind9 restart
student@student-H81H3-I:~$
```

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).





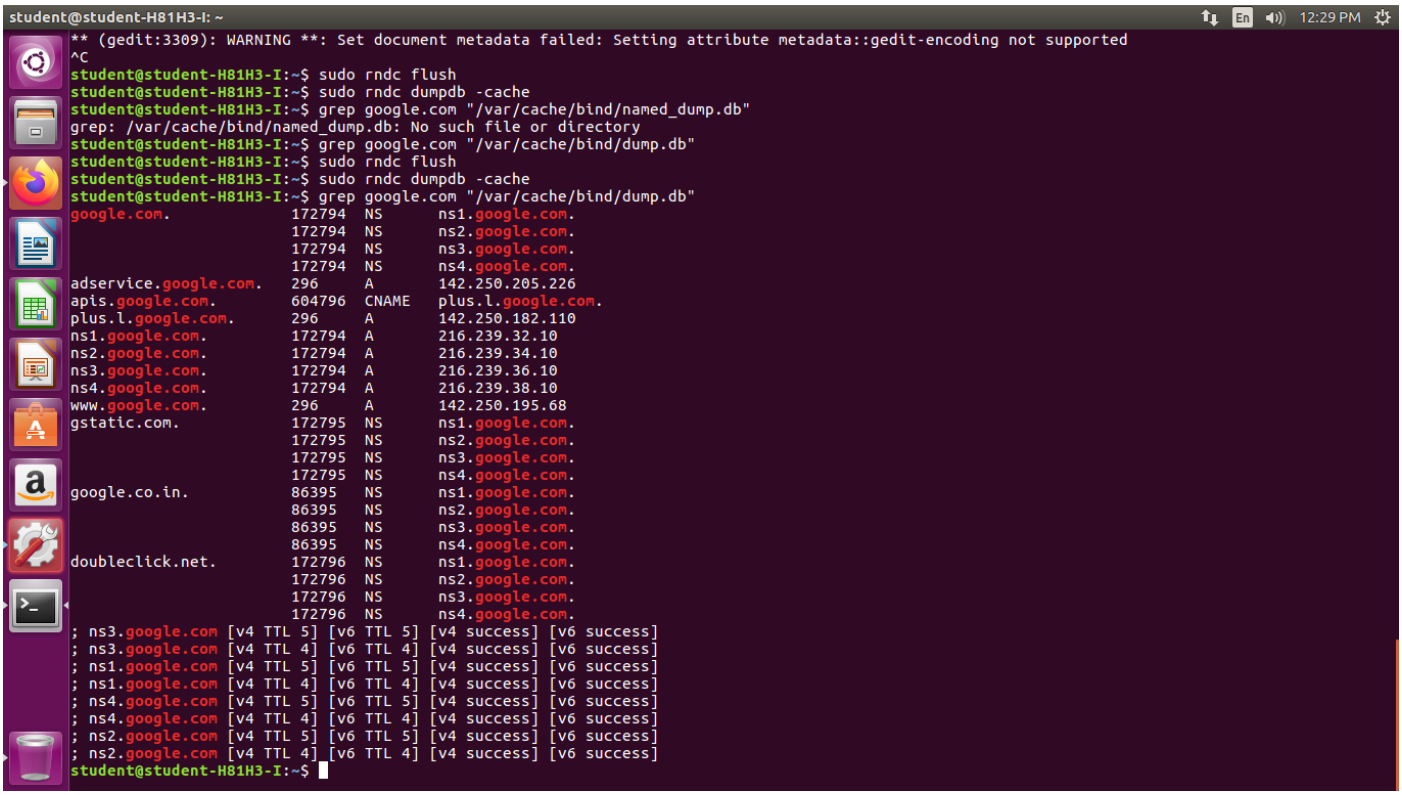


Observation 4:

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 DNS cache.

```
student@student-H81H3-I:~$ sudo rndc dumpdb -cache
student@student-H81H3-I:~$ sudo rndc flush
student@student-H81H3-I:~$
```

DNS Cache using ‘grep’ command:

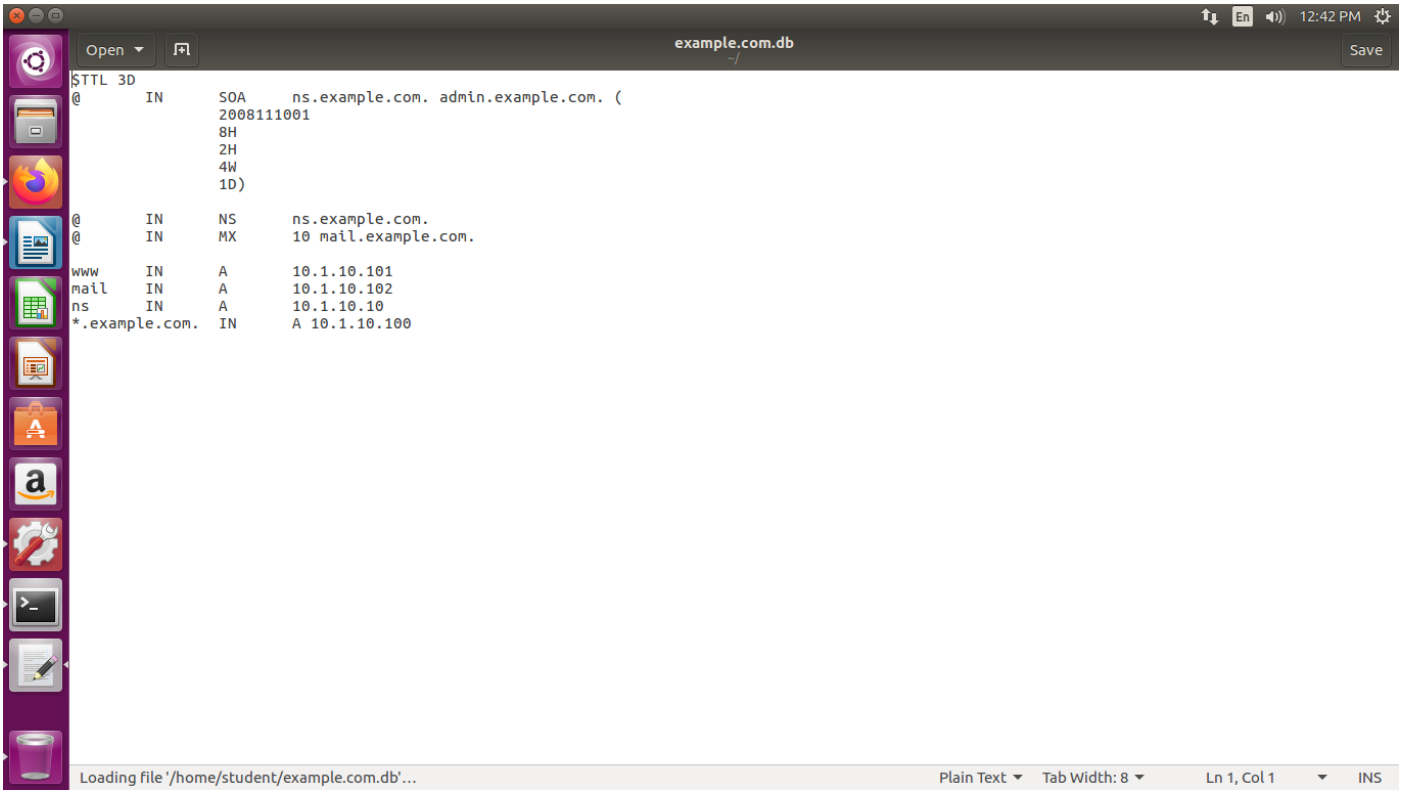


Part 2: Setting Up an Authoritative Nameserver for example.com domain

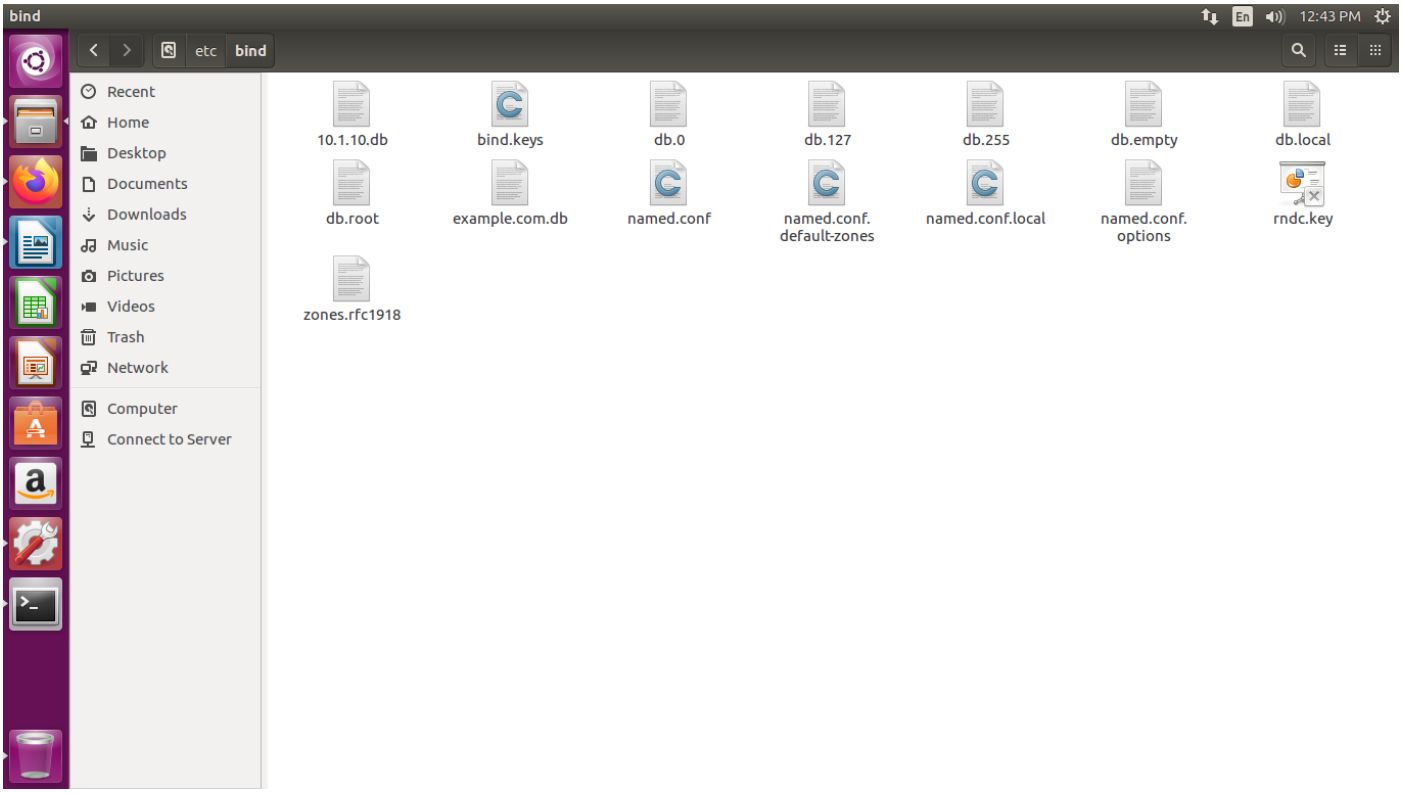
Task 3: Host a Zone in the Local DNS server.

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

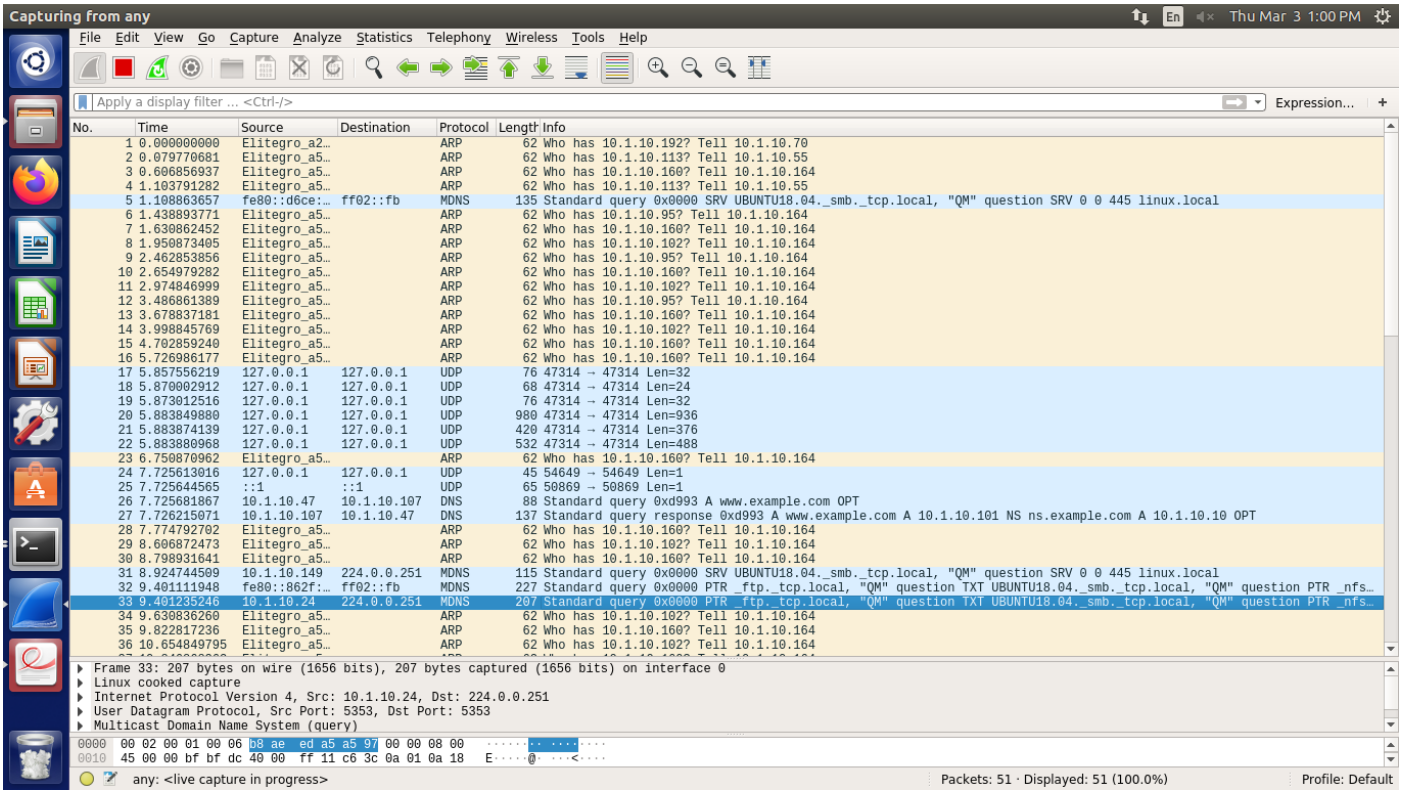
4.1 When all the changes are made, remember to restart the BIND server. Now we will restart the DNS server using the following command:

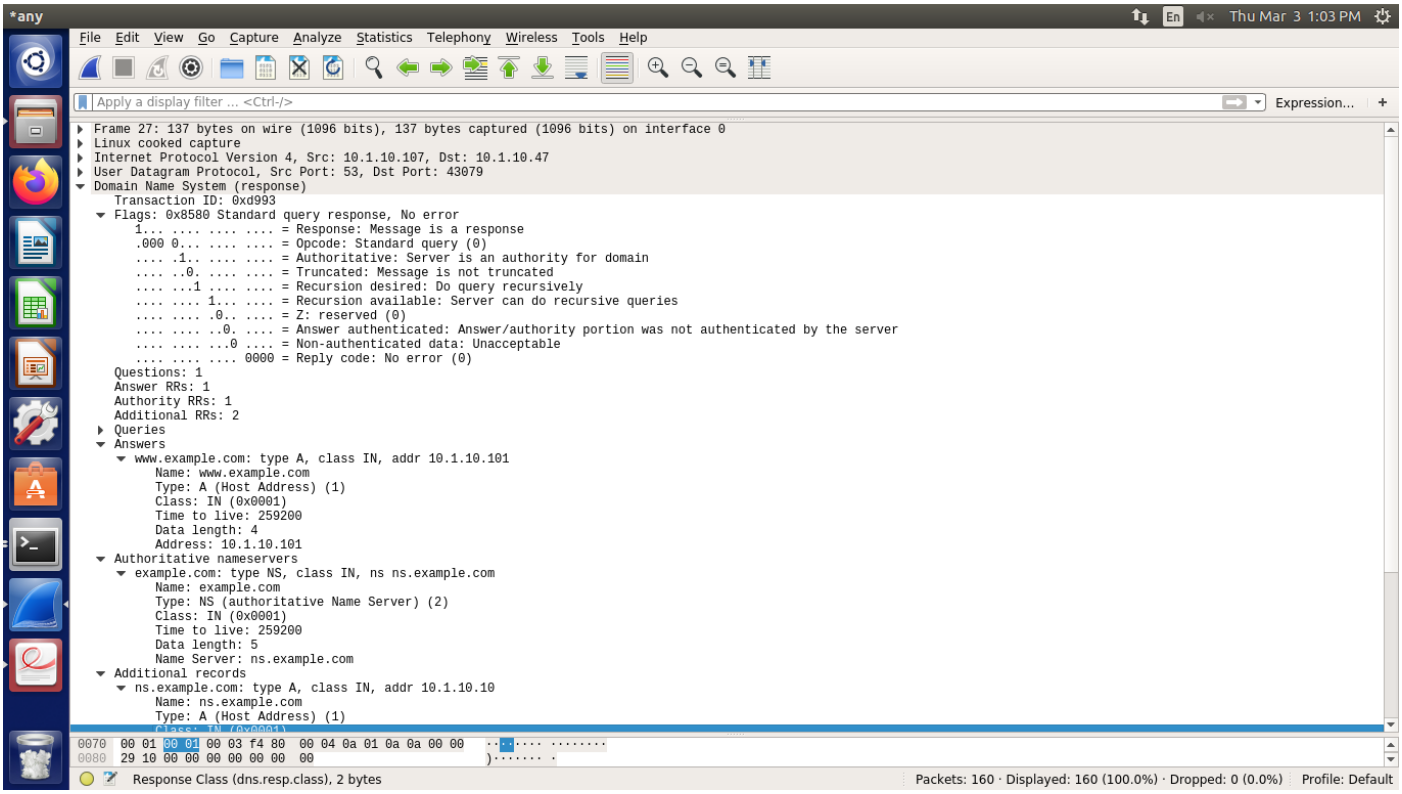
```
student@student-H81H3-I:~$ sudo service bind9 restart
student@student-H81H3-I:~$
```

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.

```
student@localhost: ~
student@localhost:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
student@localhost:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48415
;; 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: 10.1.10.107#53(10.1.10.107)
;; WHEN: Thu Mar 03 12:51:10 IST 2022
;; MSG SIZE  rcvd: 93

student@localhost:~$
```

4.3 Observe the results in Wireshark capture :





4.4 DNS cache on server machine after dig command :

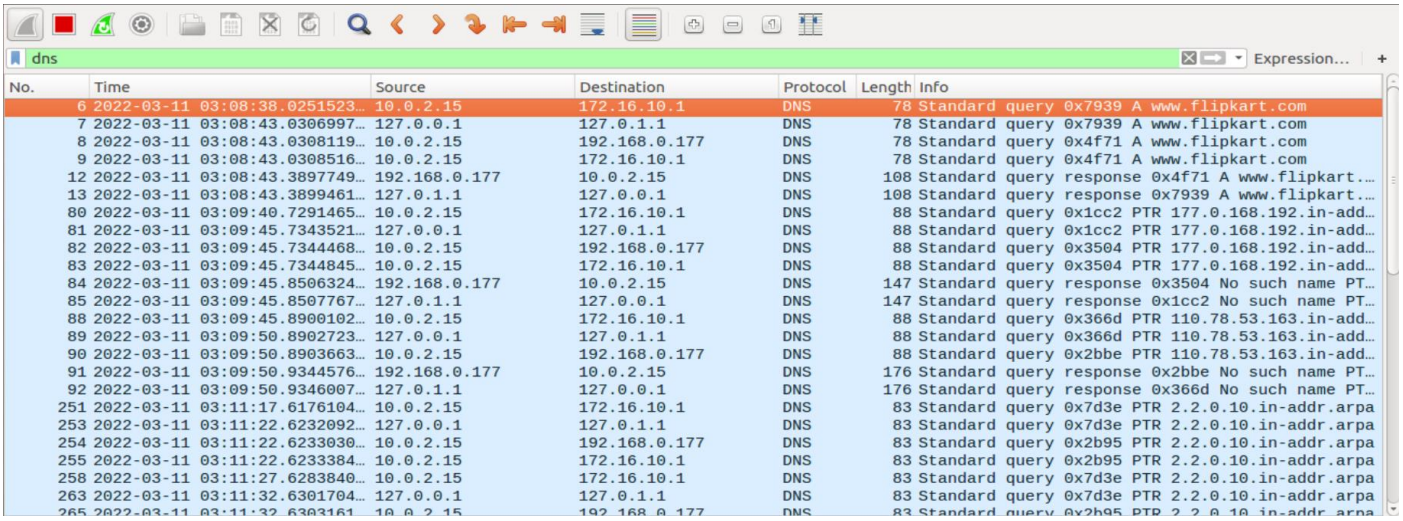
```
student@localhost: ~                                                    En  10:42 AM
** (gedit:29089): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
student@localhost:~$ sudo CAT /var/cache/bind/named_dump.db
sudo: CAT: command not found
student@localhost:~$ sudo cat /var/cache/bind/named_dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20220303065554
; secure
.                       518357  IN NS   a.root-servers.net.
                        518357  IN NS   b.root-servers.net.
                        518357  IN NS   c.root-servers.net.
                        518357  IN NS   d.root-servers.net.
                        518357  IN NS   e.root-servers.net.
                        518357  IN NS   f.root-servers.net.
                        518357  IN NS   g.root-servers.net.
                        518357  IN NS   h.root-servers.net.
                        518357  IN NS   i.root-servers.net.
                        518357  IN NS   j.root-servers.net.
                        518357  IN NS   k.root-servers.net.
                        518357  IN NS   l.root-servers.net.
                        518357  IN NS   m.root-servers.net.
; secure
                        518394  RRSIG   NS 8 0 518400 (
                                        20220316050000 20220303040000 9799 .
                                        WHZ//zKcRc0aFze+haFiC5a0GwaCwCsopDkM
                                        LzMZrOTTvejeb96R01h+2mlnsd4qivrbop0a
                                        7fBz+Vs/m+YVOPku+vCO/fnZ+NW/KgrtXpHo
                                        PopEWayXrfwtEC+Iu/G7gD1bePIhXqeEMSYl
                                        fLD84g7ezASeXc4q3Yrfw3+sSnKkG/vwlZ3I
                                        FcSw90bqyYoV597fRLZYdEoUzDjp9onU/Ncw
                                        qmWJ6muVMs2IO7kHTaUfMO7z6mgf5PGC2ylT
                                        ywz+4WZLFd6t8QvZypEMGFwPSxJ2W86Sdh2Q
                                        JSDznW3V5CFW3tW+59ZzKsJHuGlHTwqem+eg
                                        ipZMXoMW9y+F08ZVlg== )
; secure
                        172757  DNSKEY  256 3 8 (
                                        AwEAAZym4HCWiTAAl2Mv1izgTyn9sKwgi5eB
                                        xpG29bVlefq/r+TGCtmUElvFyBWHRjvf9mBg
```

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.



dns — Expression…

No.	Time	Source	Destination	Protocol	Length	Info
6	2022-03-11 03:08:38.0251523…	10.0.2.15	172.16.10.1	DNS	78	Standard query 0x7939 A www.flipkart.com
7	2022-03-11 03:08:43.0306997…	127.0.0.1	127.0.1.1	DNS	78	Standard query 0x7939 A www.flipkart.com
8	2022-03-11 03:08:43.0308119…	10.0.2.15	192.168.0.177	DNS	78	Standard query 0x4f71 A www.flipkart.com
9	2022-03-11 03:08:43.0308516…	10.0.2.15	172.16.10.1	DNS	78	Standard query 0x4f71 A www.flipkart.com
12	2022-03-11 03:08:43.3897749…	192.168.0.177	10.0.2.15	DNS	108	Standard query response 0x4f71 A www.flipkart.…
13	2022-03-11 03:08:43.3899461…	127.0.1.1	127.0.0.1	DNS	108	Standard query response 0x7939 A www.flipkart.…
80	2022-03-11 03:09:40.7291465…	10.0.2.15	172.16.10.1	DNS	88	Standard query 0x1cc2 PTR 177.0.168.192.in-add…
81	2022-03-11 03:09:45.7343521…	127.0.0.1	127.0.1.1	DNS	88	Standard query 0x1cc2 PTR 177.0.168.192.in-add…
82	2022-03-11 03:09:45.7344468…	10.0.2.15	192.168.0.177	DNS	88	Standard query 0x3504 PTR 177.0.168.192.in-add…
83	2022-03-11 03:09:45.7344845…	10.0.2.15	172.16.10.1	DNS	88	Standard query 0x3504 PTR 177.0.168.192.in-add…
84	2022-03-11 03:09:45.8506324…	192.168.0.177	10.0.2.15	DNS	147	Standard query response 0x3504 No such name PT…
85	2022-03-11 03:09:45.8507767…	127.0.1.1	127.0.0.1	DNS	147	Standard query response 0x1cc2 No such name PT…
88	2022-03-11 03:09:45.8900102…	10.0.2.15	172.16.10.1	DNS	88	Standard query 0x366d PTR 110.78.53.163.in-add…
89	2022-03-11 03:09:50.8902723…	127.0.0.1	127.0.1.1	DNS	88	Standard query 0x366d PTR 110.78.53.163.in-add…
90	2022-03-11 03:09:50.8903663…	10.0.2.15	192.168.0.177	DNS	88	Standard query 0x2bbe PTR 110.78.53.163.in-add…
91	2022-03-11 03:09:50.9344576…	192.168.0.177	10.0.2.15	DNS	176	Standard query response 0x2bbe No such name PT…
92	2022-03-11 03:09:50.9346007…	127.0.1.1	127.0.0.1	DNS	176	Standard query response 0x366d No such name PT…
251	2022-03-11 03:11:17.6176104…	10.0.2.15	172.16.10.1	DNS	83	Standard query 0x7d3e PTR 2.2.0.10.in-addr.arpa
253	2022-03-11 03:11:22.6232092…	127.0.0.1	127.0.1.1	DNS	83	Standard query 0x7d3e PTR 2.2.0.10.in-addr.arpa
254	2022-03-11 03:11:22.6233030…	10.0.2.15	192.168.0.177	DNS	83	Standard query 0x2b95 PTR 2.2.0.10.in-addr.arpa
255	2022-03-11 03:11:22.6233384…	10.0.2.15	172.16.10.1	DNS	83	Standard query 0x2b95 PTR 2.2.0.10.in-addr.arpa
258	2022-03-11 03:11:27.6283840…	10.0.2.15	172.16.10.1	DNS	83	Standard query 0x7d3e PTR 2.2.0.10.in-addr.arpa
263	2022-03-11 03:11:32.6301704…	127.0.0.1	127.0.1.1	DNS	83	Standard query 0x7d3e PTR 2.2.0.10.in-addr.arpa
265	2022-03-11 03:11:32.6303161…	10.0.2.15	192.168.0.177	DNS	83	Standard query 0x2b95 PTR 2.2.0.10.in-addr.arpa

```
▸ Frame 6: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▸ Linux cooked capture
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 172.16.10.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 62
    Identification: 0x690b (26891)
  ▸ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x0f84 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.2.15
    Destination: 172.16.10.1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▾ User Datagram Protocol, Src Port: 35612, Dst Port: 53
    Source Port: 35612
    Destination Port: 53
    Length: 42
    Checksum: 0xc25b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
▸ Domain Name System (query)
```

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 address 172.16.10.1. 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.

```
▾ Domain Name System (query)
    Transaction ID: 0x7939
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▾ www.flipkart.com: type A, class IN
        Name: www.flipkart.com
        [Name Length: 16]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

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

→ There are 2 answers provided.

a. Canonical name for the given query
b. 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