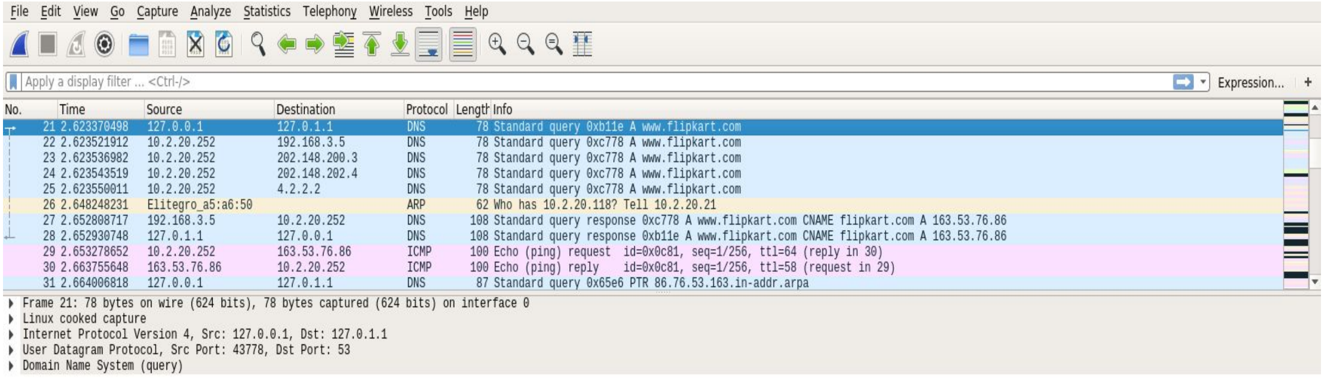
COMPUTER NETWORKS LAB
WEEK 4

ABHISHEK ADITYA BS
PES1UG19CS019
SECTION A

1. First Test – Pinging using default DNS

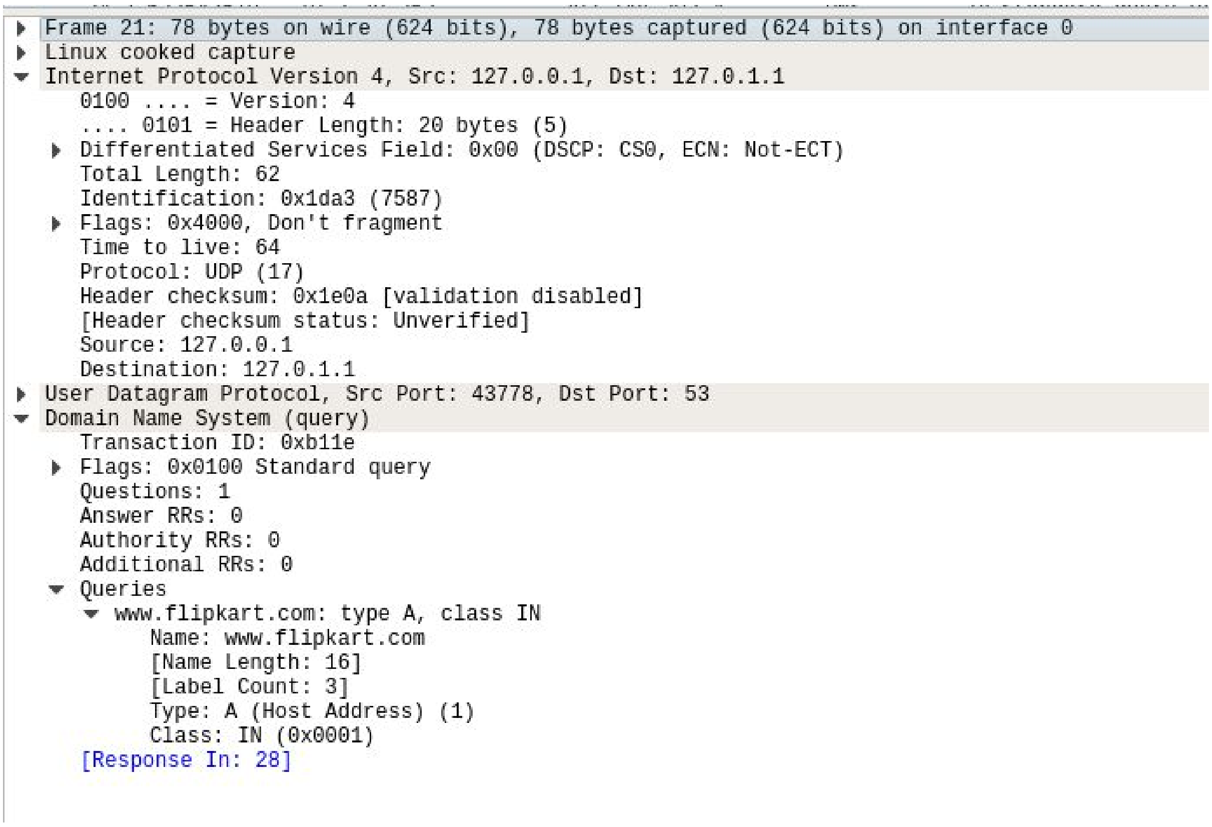
- Wireshark is used to capture the packets in the background while pinging **www.flipkart.com**
- The IP Address of the Local DNS server is observed to be **127.0.1.1**
- The query is of type **A** which stands for authoritative. The answer contains the A type record along with the IP address of the website – **163.53.76.86**
- The first query and authoritative response are shown below.



No.	Time	Source	Destination	Protocol	Length	Info
21	2.623370498	127.0.0.1	127.0.1.1	DNS	78	Standard query 0xb11e A www.flipkart.com
22	2.623521912	10.2.20.252	192.168.3.5	DNS	78	Standard query 0xc778 A www.flipkart.com
23	2.623536982	10.2.20.252	202.148.200.3	DNS	78	Standard query 0xc778 A www.flipkart.com
24	2.623543519	10.2.20.252	202.148.202.4	DNS	78	Standard query 0xc778 A www.flipkart.com
25	2.623550011	10.2.20.252	4.2.2.2	DNS	78	Standard query 0xc778 A www.flipkart.com
26	2.648248231	Elitegro_a5:a6:50		ARP	62	Who has 10.2.20.118? Tell 10.2.20.21
27	2.652808717	192.168.3.5	10.2.20.252	DNS	108	Standard query response 0xc778 A www.flipkart.com CNAME flipkart.com A 163.53.76.86
28	2.652930748	127.0.1.1	127.0.0.1	DNS	108	Standard query response 0xb11e A www.flipkart.com CNAME flipkart.com A 163.53.76.86
29	2.653278652	10.2.20.252	163.53.76.86	ICMP	100	Echo (ping) request id=0x0c81, seq=1/256, ttl=64 (reply in 30)
30	2.663755648	163.53.76.86	10.2.20.252	ICMP	100	Echo (ping) reply id=0x0c81, seq=1/256, ttl=58 (request in 29)
31	2.664006818	127.0.0.1	127.0.1.1	DNS	87	Standard query 0x65e6 PTR 86.76.53.163.in-addr.arpa

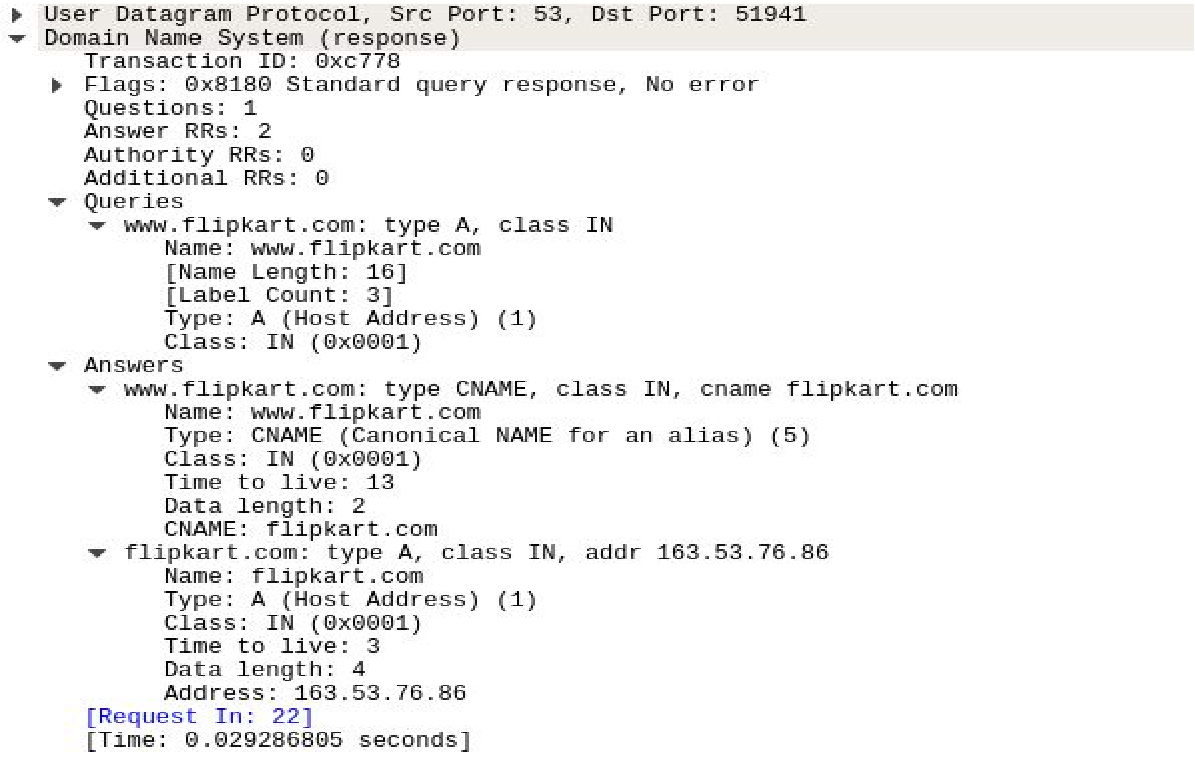
```
▸ Frame 21: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.1.1
▸ User Datagram Protocol, Src Port: 43778, Dst Port: 53
▸ Domain Name System (query)
```

Wireshark Packet Capture



```
▶ Frame 21: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▶ Linux cooked capture
▼ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.1.1
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 62
     Identification: 0x1da3 (7587)
   ▶ Flags: 0x4000, Don't fragment
     Time to live: 64
     Protocol: UDP (17)
     Header checksum: 0x1e0a [validation disabled]
     [Header checksum status: Unverified]
     Source: 127.0.0.1
     Destination: 127.0.1.1
▶ User Datagram Protocol, Src Port: 43778, Dst Port: 53
▼ Domain Name System (query)
     Transaction ID: 0xb11e
   ▶ Flags: 0x0100 Standard query
     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)
     [Response In: 28]
```

DNS Query

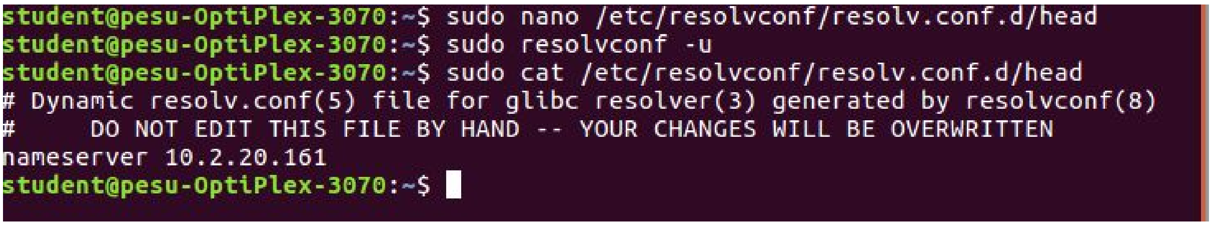


```
▶ User Datagram Protocol, Src Port: 53, Dst Port: 51941
▼ Domain Name System (response)
     Transaction ID: 0xc778
   ▶ Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 2
     Authority RRs: 0
     Additional RRs: 0
   ▼ Queries
      ▼ www.flipkart.com: type A, class IN
           Name: www.flipkart.com
           [Name Length: 16]
           [Label Count: 3]
           Type: A (Host Address) (1)
           Class: IN (0x0001)
   ▼ Answers
      ▼ www.flipkart.com: type CNAME, class IN, cname flipkart.com
           Name: www.flipkart.com
           Type: CNAME (Canonical NAME for an alias) (5)
           Class: IN (0x0001)
           Time to live: 13
           Data length: 2
           CNAME: flipkart.com
      ▼ flipkart.com: type A, class IN, addr 163.53.76.86
           Name: flipkart.com
           Type: A (Host Address) (1)
           Class: IN (0x0001)
           Time to live: 3
           Data length: 4
           Address: 163.53.76.86
     [Request In: 22]
     [Time: 0.029286805 seconds]
```

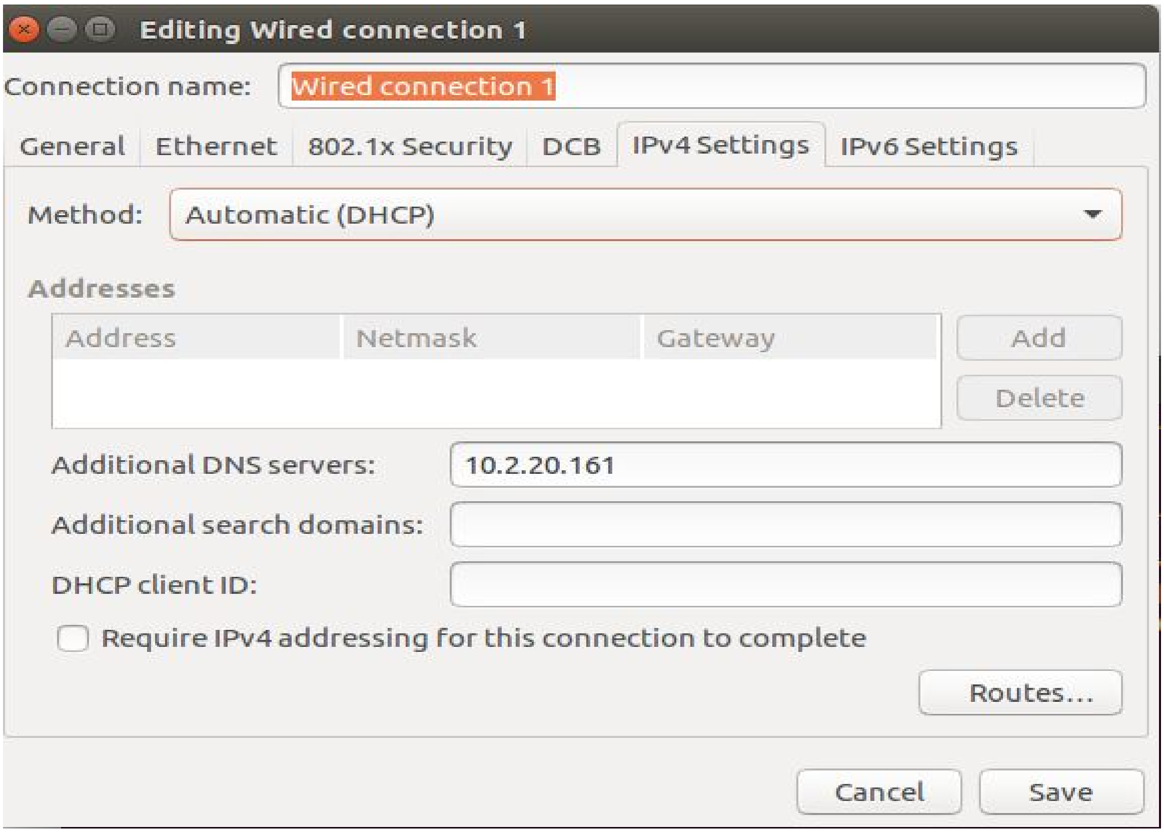
DNS Response

2. Task 1 – Configuring Client Machine

- The IP Address of the client machine is **10.2.20.252** and the IP Address of the server machine is **10.2.20.161**
- We need to add the IP Address of the custom DNS server **(10.2.20.161)** 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**



```
student@pesu-OptiPlex-3070:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
student@pesu-OptiPlex-3070:~$ sudo resolvconf -u
student@pesu-OptiPlex-3070:~$ 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 10.2.20.161
student@pesu-OptiPlex-3070:~$ 
```



Editing Wired connection 1

Connection name: Wired connection 1

Method: Automatic (DHCP)

Addresses

Additional DNS servers: 10.2.20.161

Additional search domains:

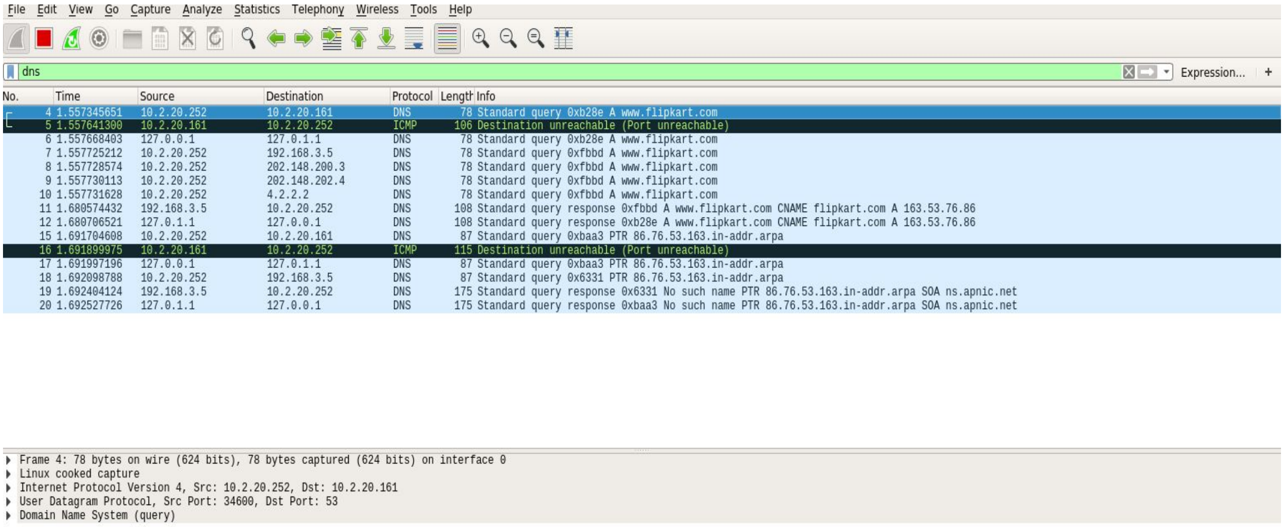
DHCP client ID:

□ Require IPv4 addressing for this connection to complete

Adding 10.2.20.161 in ‘Additional DNS servers’ field in IPv4 settings of client machine

3. Second Test

- The Flipkart website is pinged again, and Wireshark is used to capture packets.
- We obtain a `destination unreachable error` in Wireshark as the server machine does not have a DNS server associated with it
- The client tries to obtain the DNS record from **10.2.20.161** but it does not receive any hence it resorts to using the default DNS server at **127.0.1.1**



dns

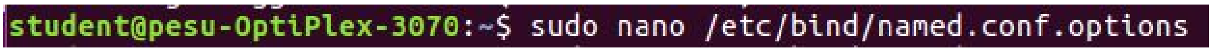
No.	Time	Source	Destination	Protocol	Length	Info
4	1.557345651	10.2.20.252	10.2.20.161	DNS	78	Standard query 0xb28e A www.flipkart.com
5	1.557641300	10.2.20.161	10.2.20.252	ICMP	106	Destination unreachable (Port unreachable)
6	1.557668403	127.0.0.1	127.0.1.1	DNS	78	Standard query 0xb28e A www.flipkart.com
7	1.557725212	10.2.20.252	192.168.3.5	DNS	78	Standard query 0xfbbd A www.flipkart.com
8	1.557728574	10.2.20.252	202.148.200.3	DNS	78	Standard query 0xfbbd A www.flipkart.com
9	1.557730113	10.2.20.252	202.148.202.4	DNS	78	Standard query 0xfbbd A www.flipkart.com
10	1.557731628	10.2.20.252	4.2.2.2	DNS	78	Standard query 0xfbbd A www.flipkart.com
11	1.680574432	192.168.3.5	10.2.20.252	DNS	108	Standard query response 0xfbbd A www.flipkart.com CNAME flipkart.com A 163.53.76.86
12	1.680706521	127.0.1.1	127.0.0.1	DNS	108	Standard query response 0xb28e A www.flipkart.com CNAME flipkart.com A 163.53.76.86
15	1.691704608	10.2.20.252	10.2.20.161	DNS	87	Standard query 0xbaa3 PTR 86.76.53.163.in-addr.arpa
16	1.691899975	10.2.20.161	10.2.20.252	ICMP	115	Destination unreachable (Port unreachable)
17	1.691997196	127.0.0.1	127.0.1.1	DNS	87	Standard query 0xbaa3 PTR 86.76.53.163.in-addr.arpa
18	1.692098788	10.2.20.252	192.168.3.5	DNS	87	Standard query 0x6331 PTR 86.76.53.163.in-addr.arpa
19	1.692404124	192.168.3.5	10.2.20.252	DNS	175	Standard query response 0x6331 No such name PTR 86.76.53.163.in-addr.arpa SOA ns.apnic.net
20	1.692527726	127.0.1.1	127.0.0.1	DNS	175	Standard query response 0xbaa3 No such name PTR 86.76.53.163.in-addr.arpa SOA ns.apnic.net

```
▸ Frame 4: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.2.20.252, Dst: 10.2.20.161
▸ User Datagram Protocol, Src Port: 34600, Dst Port: 53
▸ Domain Name System (query)
```

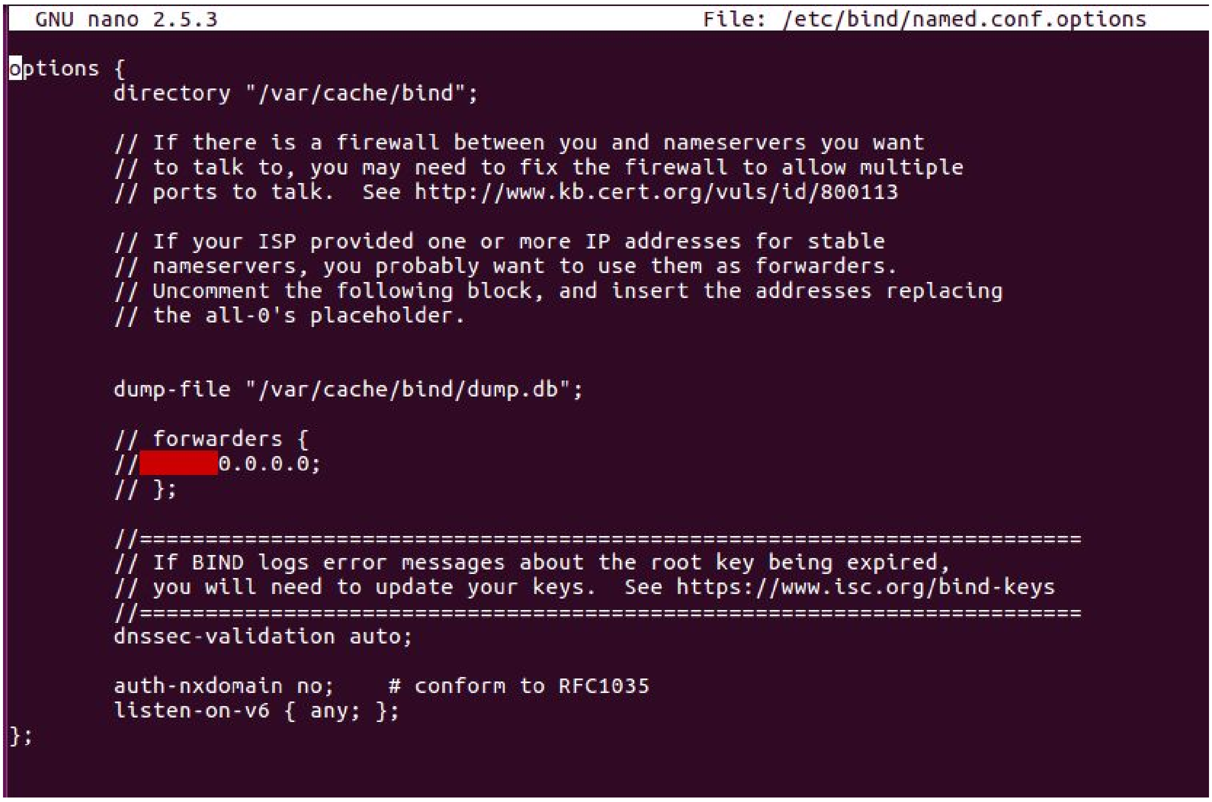
Wireshark Packet Capture

4. Task 2 – Setting Up Local DNS Server

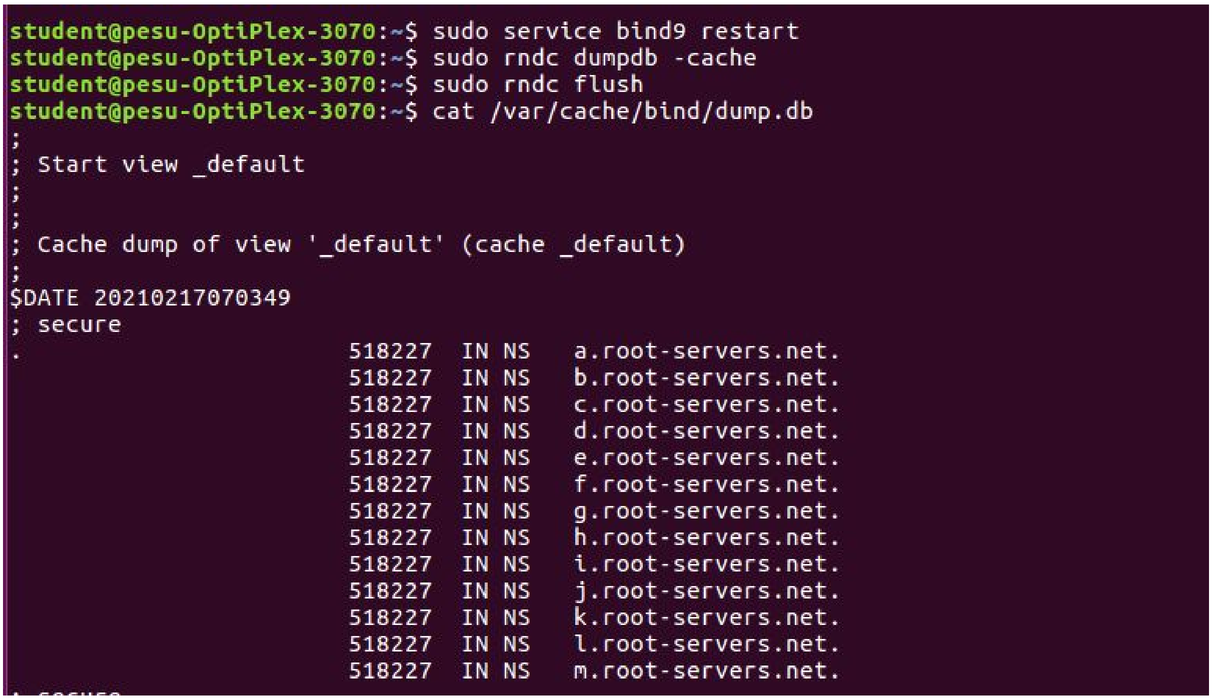
- The **bind9** server is used as the DNS server on the server machine. It is installed using **sudo apt install bind9**.
- The configuration file for the server is **/etc/bind/named.conf.options**
- An entry specifying the dump file for the DNS cache is added to the configuration file.
- The cache can be dumped into the file using **sudo rndc dumpdb -cache** and can be cleared or flushed out using **sudo rndc flush**.



```
student@pesu-OptiPlex-3070:~$ sudo nano /etc/bind/named.conf.options
```



```
  GNU nano 2.5.3                                 File: /etc/bind/named.conf.options

options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.


        dump-file "/var/cache/bind/dump.db";

        // forwarders {
        //[redacted]0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

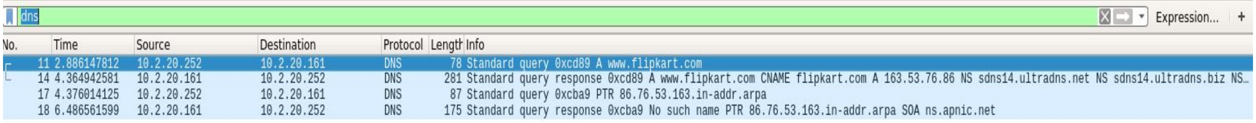


```
student@pesu-OptiPlex-3070:~$ sudo service bind9 restart
student@pesu-OptiPlex-3070:~$ sudo rndc dumpdb -cache
student@pesu-OptiPlex-3070:~$ sudo rndc flush
student@pesu-OptiPlex-3070:~$ cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20210217070349
; secure
.                       518227  IN NS   a.root-servers.net.
                        518227  IN NS   b.root-servers.net.
                        518227  IN NS   c.root-servers.net.
                        518227  IN NS   d.root-servers.net.
                        518227  IN NS   e.root-servers.net.
                        518227  IN NS   f.root-servers.net.
                        518227  IN NS   g.root-servers.net.
                        518227  IN NS   h.root-servers.net.
                        518227  IN NS   i.root-servers.net.
                        518227  IN NS   j.root-servers.net.
                        518227  IN NS   k.root-servers.net.
                        518227  IN NS   l.root-servers.net.
                        518227  IN NS   m.root-servers.net.
; secure
```

Viewing the cache dumpfile

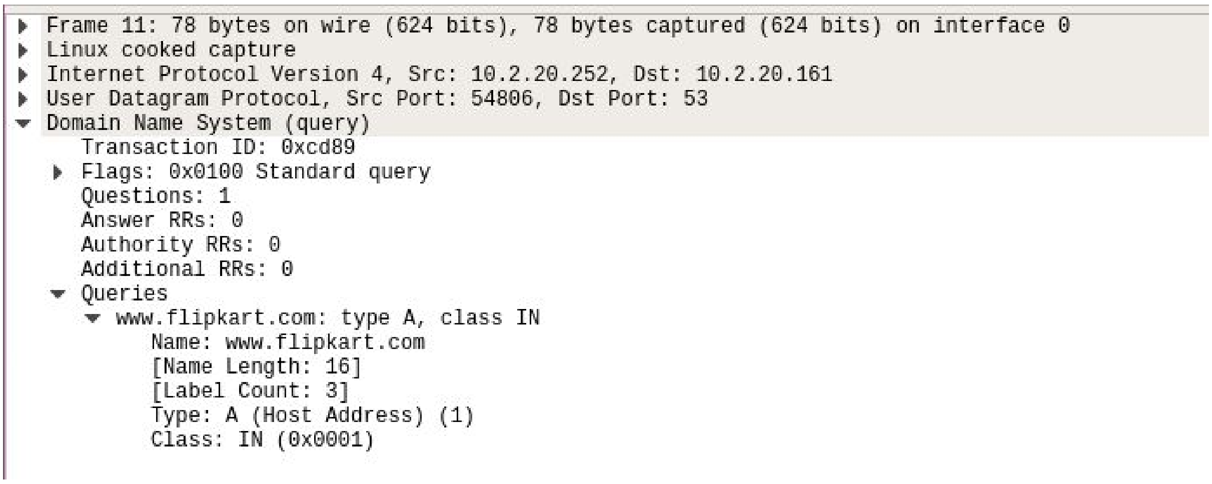
5. Third Test

- The Flipkart website is pinged again with Wireshark running in the background
- The IP Address of the local DNS server is clearly seen in the screenshots below
- The cache is dumped into the dump file 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.



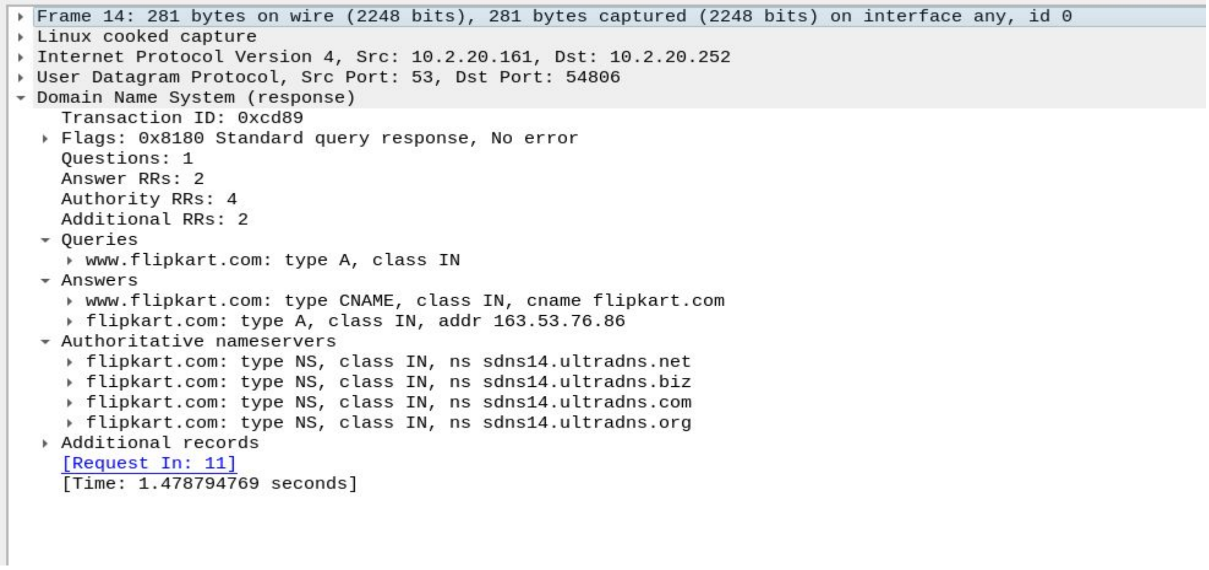
No.	Time	Source	Destination	Protocol	Length	Info
11	2.886147812	10.2.20.252	10.2.20.161	DNS	78	Standard query 0xcd89 A www.flipkart.com
14	4.364942581	10.2.20.161	10.2.20.252	DNS	281	Standard query response 0xcd89 A www.flipkart.com CNAME flipkart.com A 163.53.76.86 NS sdns14.ultradns.net NS sdns14.ultradns.biz NS…
17	4.376014125	10.2.20.252	10.2.20.161	DNS	87	Standard query 0xcba9 PTR 86.76.53.163.in-addr.arpa
18	6.486561599	10.2.20.161	10.2.20.252	DNS	175	Standard query response 0xcba9 No such name PTR 86.76.53.163.in-addr.arpa SOA ns.apnic.net

Wireshark Packet Capture



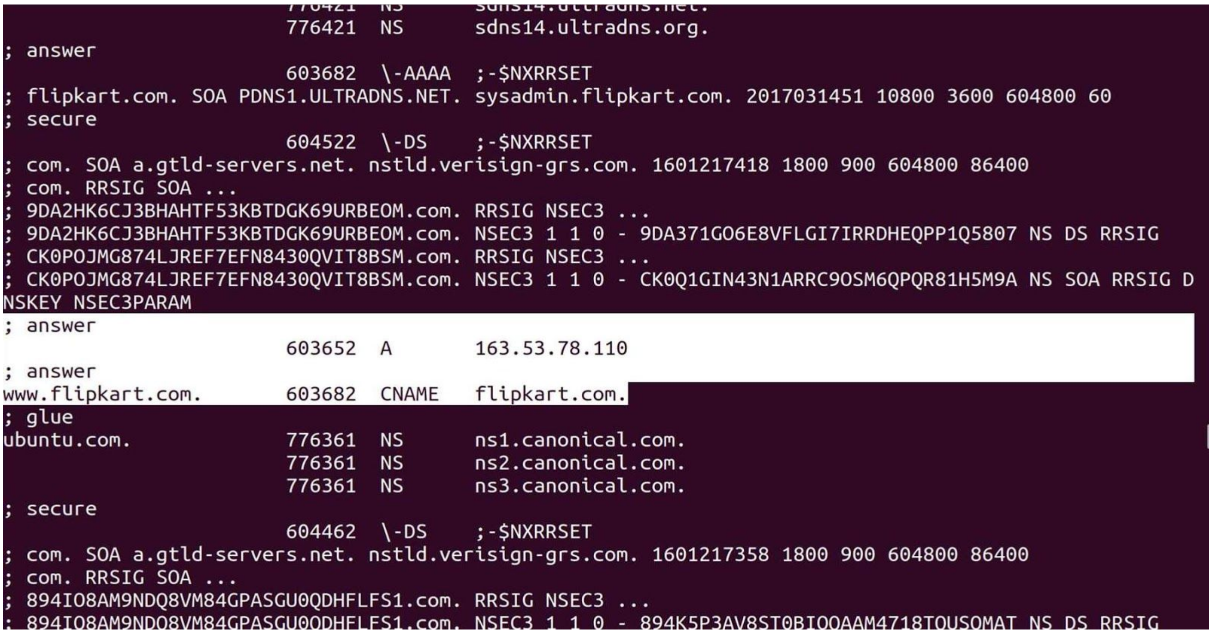
```
▶ Frame 11: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 10.2.20.252, Dst: 10.2.20.161
▶ User Datagram Protocol, Src Port: 54806, Dst Port: 53
▼ Domain Name System (query)
     Transaction ID: 0xcd89
   ▶ Flags: 0x0100 Standard query
     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)
```

DNS Query Packet



```
▸ Frame 14: 281 bytes on wire (2248 bits), 281 bytes captured (2248 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.2.20.161, Dst: 10.2.20.252
▸ User Datagram Protocol, Src Port: 53, Dst Port: 54806
▾ Domain Name System (response)
    Transaction ID: 0xcd89
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 4
    Additional RRs: 2
  ▾ Queries
    ▸ www.flipkart.com: type A, class IN
  ▾ Answers
    ▸ www.flipkart.com: type CNAME, class IN, cname flipkart.com
    ▸ flipkart.com: type A, class IN, addr 163.53.76.86
  ▾ Authoritative nameservers
    ▸ flipkart.com: type NS, class IN, ns sdns14.ultradns.net
    ▸ flipkart.com: type NS, class IN, ns sdns14.ultradns.biz
    ▸ flipkart.com: type NS, class IN, ns sdns14.ultradns.com
    ▸ flipkart.com: type NS, class IN, ns sdns14.ultradns.org
  ▸ Additional records
    [Request In: 11]
    [Time: 1.478794769 seconds]
```

DNS Response Packet



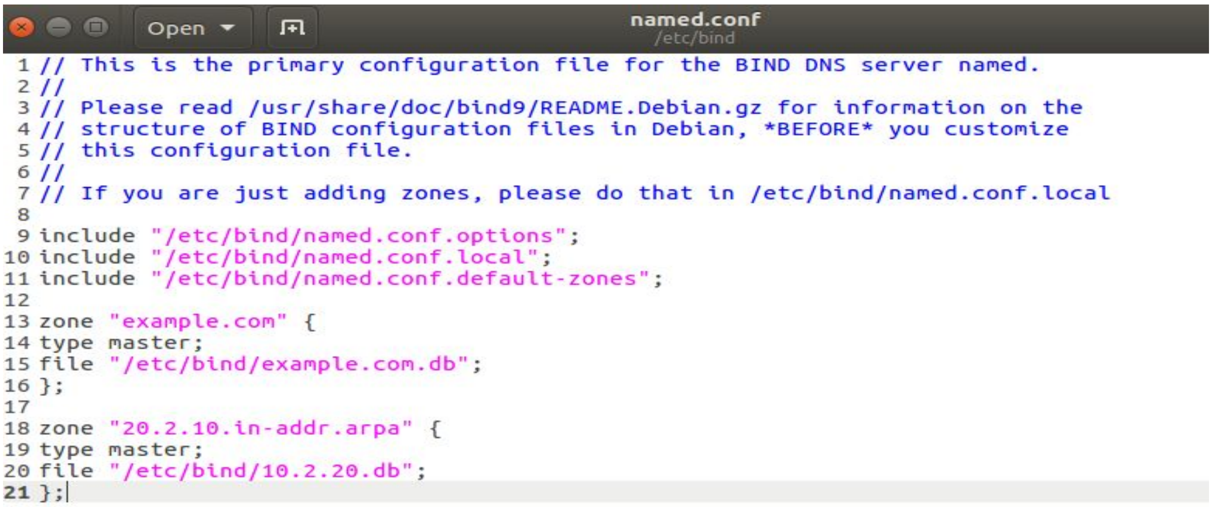
```
                        776421   NS      sdns14.ultradns.net.
                        776421   NS      sdns14.ultradns.org.
; answer
                        603682   \-AAAA  ;-$NXRRSET
; flipkart.com. SOA PDNS1.ULTRADNS.NET. sysadmin.flipkart.com. 2017031451 10800 3600 604800 60
; secure
                        604522   \-DS    ;-$NXRRSET
; com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1601217418 1800 900 604800 86400
; com. RRSIG SOA ...
; 9DA2HK6CJ3BHAHTF53KBTDGK69URBEOM.com. RRSIG NSEC3 ...
; 9DA2HK6CJ3BHAHTF53KBTDGK69URBEOM.com. NSEC3 1 1 0 - 9DA371GO6E8VFLGI7IRRDHEQPP1Q5807 NS DS RRSIG
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. RRSIG NSEC3 ...
; CK0POJMG874LJREF7EFN8430QVIT8BSM.com. NSEC3 1 1 0 - CK0Q1GIN43N1ARRC9OSM6QPQR81H5M9A NS SOA RRSIG D
NSKEY NSEC3PARAM
; answer
                        603652   A       163.53.78.110
; answer
www.flipkart.com.       603682   CNAME   flipkart.com.
; glue
ubuntu.com.             776361   NS      ns1.canonical.com.
                        776361   NS      ns2.canonical.com.
                        776361   NS      ns3.canonical.com.
; secure
                        604462   \-DS    ;-$NXRRSET
; com. SOA a.gtld-servers.net. nstld.verisign-grs.com. 1601217358 1800 900 604800 86400
; com. RRSIG SOA ...
; 894IO8AM9NDQ8VM84GPASGU0QDHFLFS1.com. RRSIG NSEC3 ...
; 894IO8AM9NDQ8VM84GPASGU0QDHFLFS1.com. NSEC3 1 1 0 - 894K5P3AV8ST0BIOOAAM4718TOUSOMAT NS DS RRSIG
```

Cache Dumpfile

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

6.1 Zone Creation

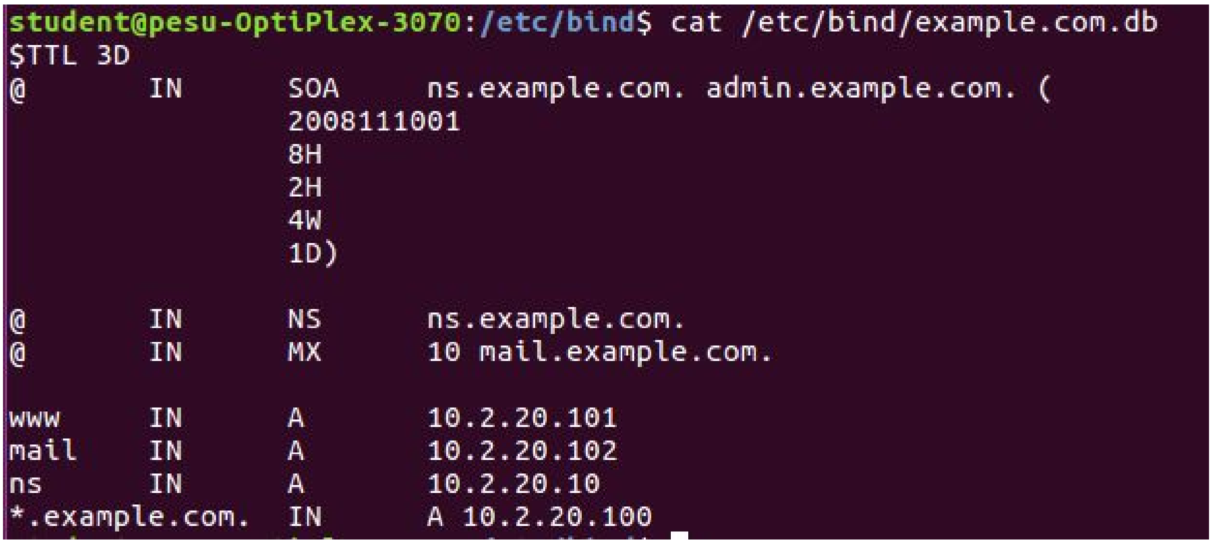
- The two zones corresponding to the domain **www.example.com** must be added to the **/etc/bind/named.conf** file in the server.
- The first zone corresponds to the forward lookup (translation from hostname to IP Address) and the second zone is for the reverse lookup (translation from IP Address to hostname).



```
// 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 "20.2.10.in-addr.arpa" {
type master;
file "/etc/bind/10.2.20.db";
};
```

6.2 Forward and Reverse Lookup

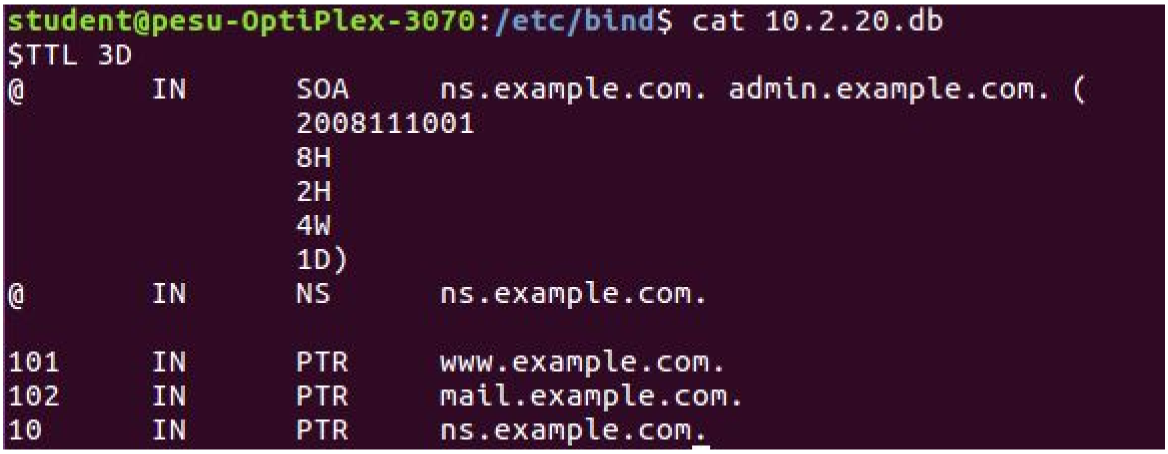
- The forward lookup file is located at **/etc/bind/example.com.db**
- The symbol @ is used to indicate the origin specified, in this case **www.example.com**
- There are 7 records in the lookup file, an SOA record, a nameserver, a mail server and 4 authoritative records.
- The TTL field tells the server how long this record should stay in the cache before being removed. In this case the local DNS server requests for a fresh entry from the name server.



```
student@pesu-OptiPlex-3070:/etc/bind$ cat /etc/bind/example.com.db
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                2008111001
                8H
                2H
                4W
                1D)

@       IN      NS      ns.example.com.
@       IN      MX      10 mail.example.com.

www     IN      A       10.2.20.101
mail    IN      A       10.2.20.102
ns      IN      A       10.2.20.10
*.example.com.  IN      A 10.2.20.100
```

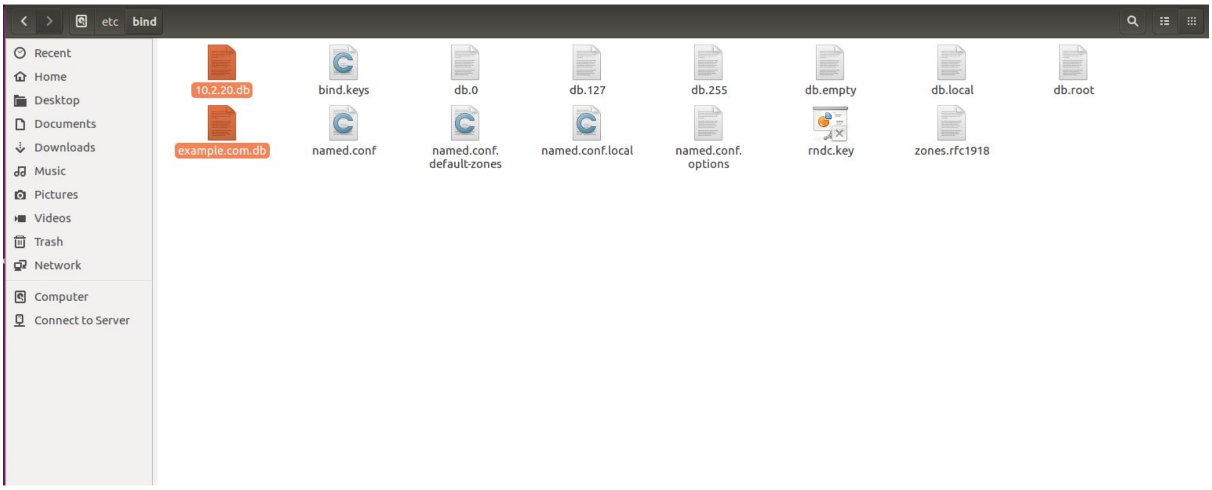
Forward Lookup File

- The reverse lookup file is stored at **/etc/bind/10.2.20.db** and is used to translate IP Addresses to hostnames for the given domain, in this case example.com.
- For each IP Address defined in the forward lookup file, a corresponding hostname is referenced here.
- The record type here is PTR or DNS Pointer Record.



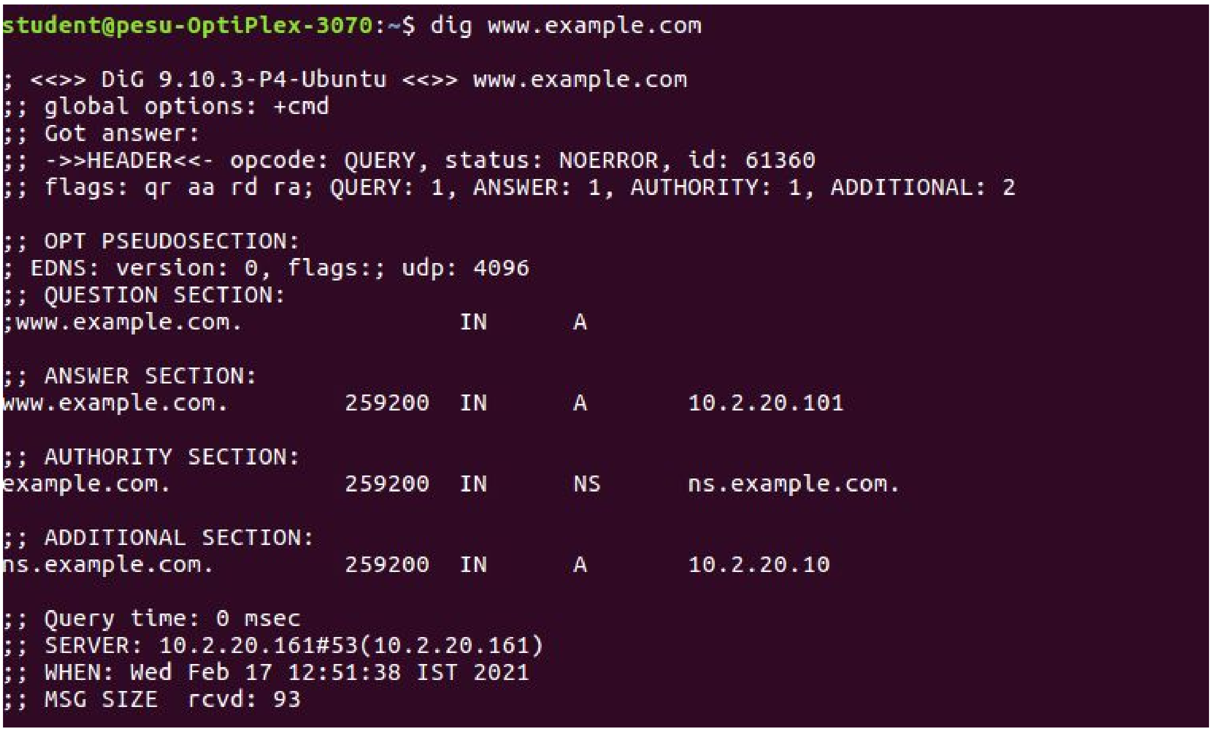
```
student@pesu-OptiPlex-3070:/etc/bind$ cat 10.2.20.db
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                        2008111001
                        8H
                        2H
                        4W
                        1D)
@       IN      NS      ns.example.com.

101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
10      IN      PTR     ns.example.com.
```

Reverse Lookup File



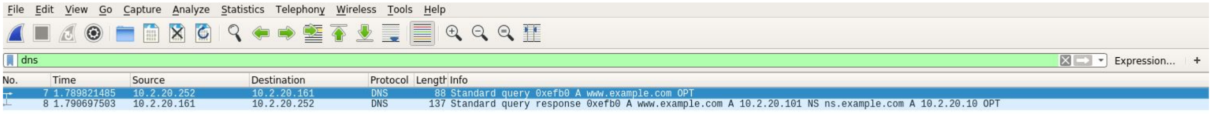
7. Fourth Test – Testing www.example.com

- The dig command is used to lookup name servers specified in the file **/etc/resolv.conf**
- Wireshark is used to capture the packets while running the command dig **www.example.com**
- The IP Address of the DNS Server and the returned IP Address of the domain set by us can be seen in the query and response packets.



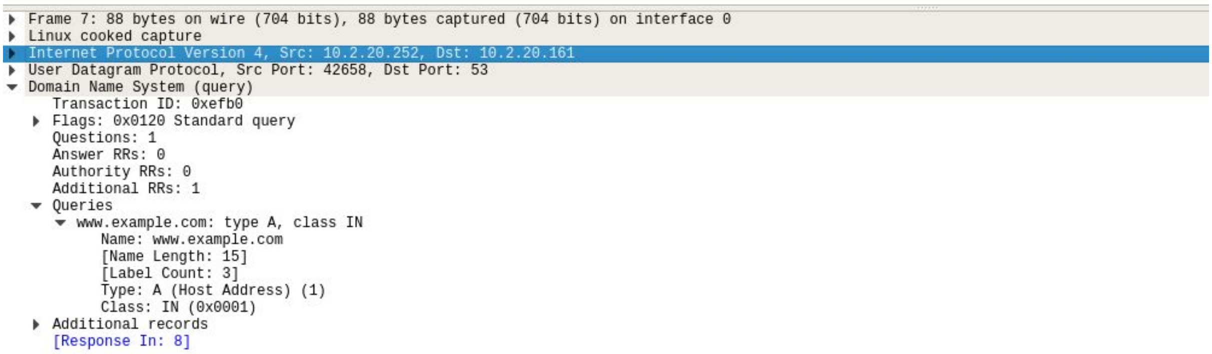
```
student@pesu-OptiPlex-3070:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61360
;; 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       10.2.20.101

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       10.2.20.10

;; Query time: 0 msec
;; SERVER: 10.2.20.161#53(10.2.20.161)
;; WHEN: Wed Feb 17 12:51:38 IST 2021
;; MSG SIZE  rcvd: 93
```

dig **www.example.com**



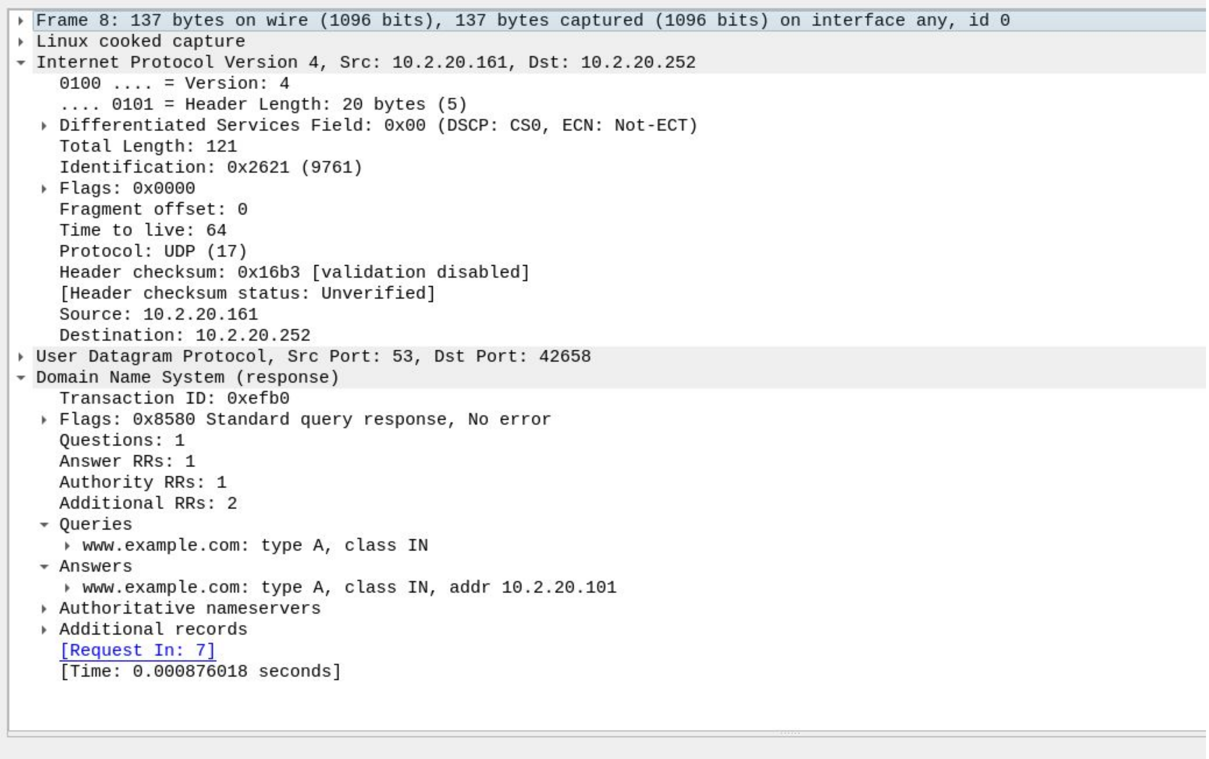
```
dns
No.   Time          Source        Destination   Protocol Length Info
    7 1.789821485   10.2.20.252   10.2.20.161   DNS       88 Standard query 0xefb0 A www.example.com OPT
    8 1.790697503   10.2.20.161   10.2.20.252   DNS      137 Standard query response 0xefb0 A www.example.com A 10.2.20.101 NS ns.example.com A 10.2.20.10 OPT
```

Wireshark Packet Capture



```
▸ Frame 7: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 10.2.20.252, Dst: 10.2.20.161
▸ User Datagram Protocol, Src Port: 42658, Dst Port: 53
▾ Domain Name System (query)
     Transaction ID: 0xefb0
   ▸ Flags: 0x0120 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 1
   ▾ Queries
      ▾ www.example.com: type A, class IN
           Name: www.example.com
           [Name Length: 15]
           [Label Count: 3]
           Type: A (Host Address) (1)
           Class: IN (0x0001)
   ▸ Additional records
     [Response In: 8]
```

DNS Query Packet



```
▸ Frame 8: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface any, id 0
▸ Linux cooked capture
▾ Internet Protocol Version 4, Src: 10.2.20.161, Dst: 10.2.20.252
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 121
    Identification: 0x2621 (9761)
  ▸ Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x16b3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.2.20.161
    Destination: 10.2.20.252
▸ User Datagram Protocol, Src Port: 53, Dst Port: 42658
▾ Domain Name System (response)
    Transaction ID: 0xefb0
  ▸ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 2
  ▾ Queries
    ▸ www.example.com: type A, class IN
  ▾ Answers
    ▸ www.example.com: type A, class IN, addr 10.2.20.101
  ▸ Authoritative nameservers
  ▸ Additional records
    [Request In: 7]
    [Time: 0.000876018 seconds]
```

DNS Response Packet

8. Questions

Q1. Locate the DNS query and response messages. Are they 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 the 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 the server at the IP Address 10.2.20.161 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 flipkart.com refers to the canonical hostname www.flipkart.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.flipkart.com)* retrieved from the response message.