Computer Networks Laboratory Week #4

Name – B.Pravena **Sec - B**

SRN – PES2UG19CS076

Implementation of a Local DNS Server and Authoritative NameServer

DNS (Domain Name System) is the Internet's phone book; it translates hostnames to IP addresses (and vice versa). This translation is through DNS resolution, which happens behind the scene.

The objectives of this lab are to understand:

- Install, set up and deploy a local DNS server
- Deploy authoritative nameserver for example.com domain

Lab Setup (with Internet Connection)

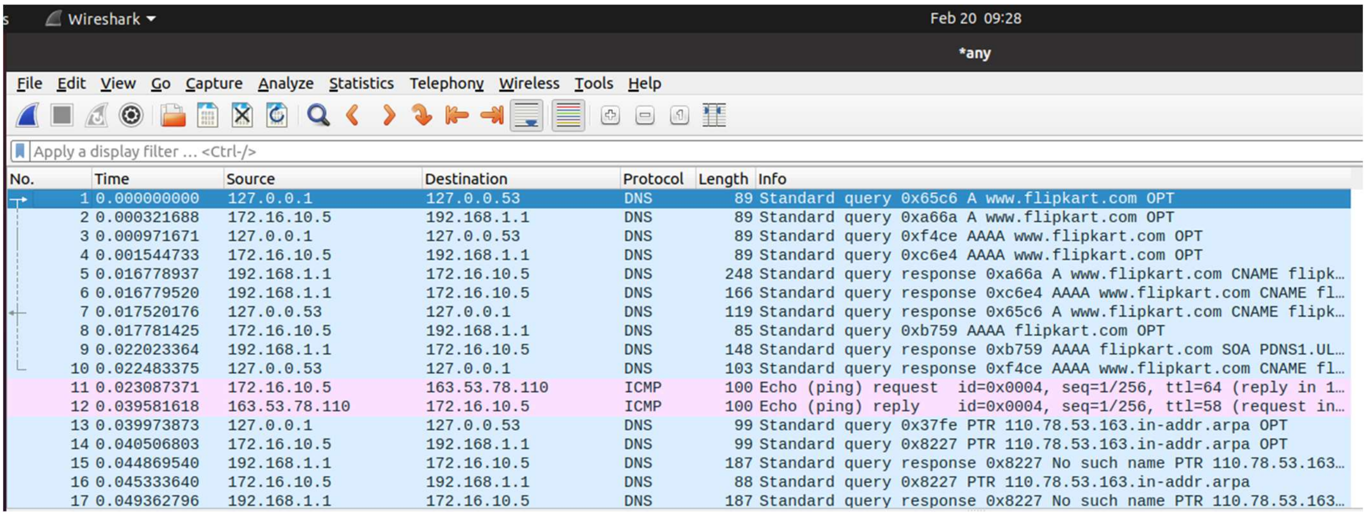
DNS Server: 10.2.22.184 User/Client:

10.2.22.195 ***Note:*** Use the default IP address provided by

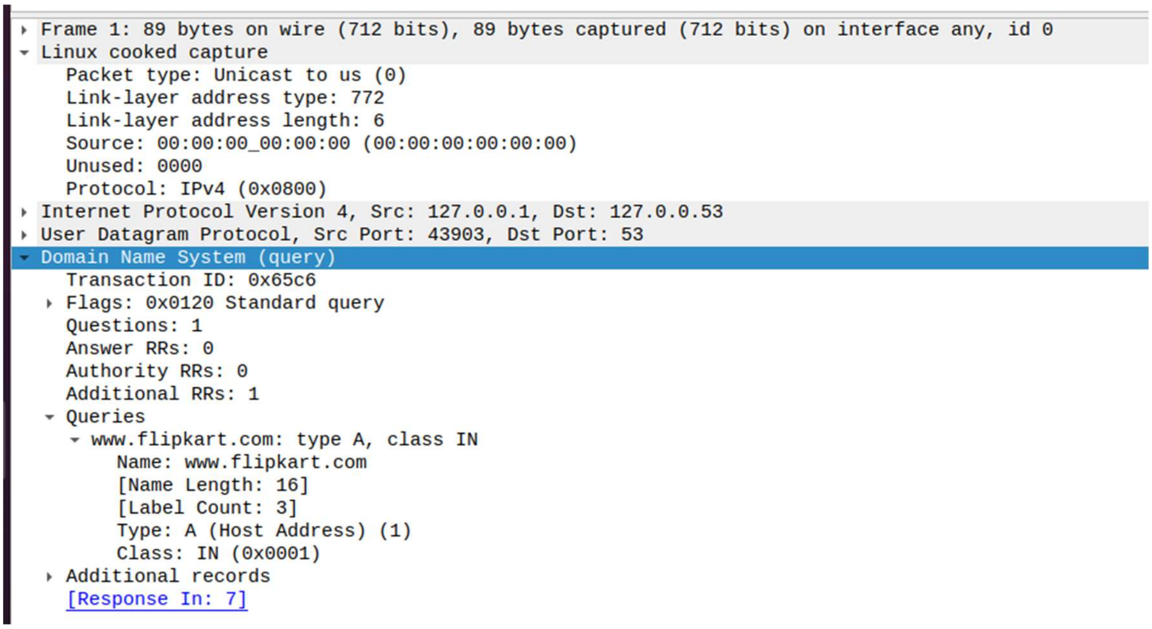
PESU LAN.

Observation 1:

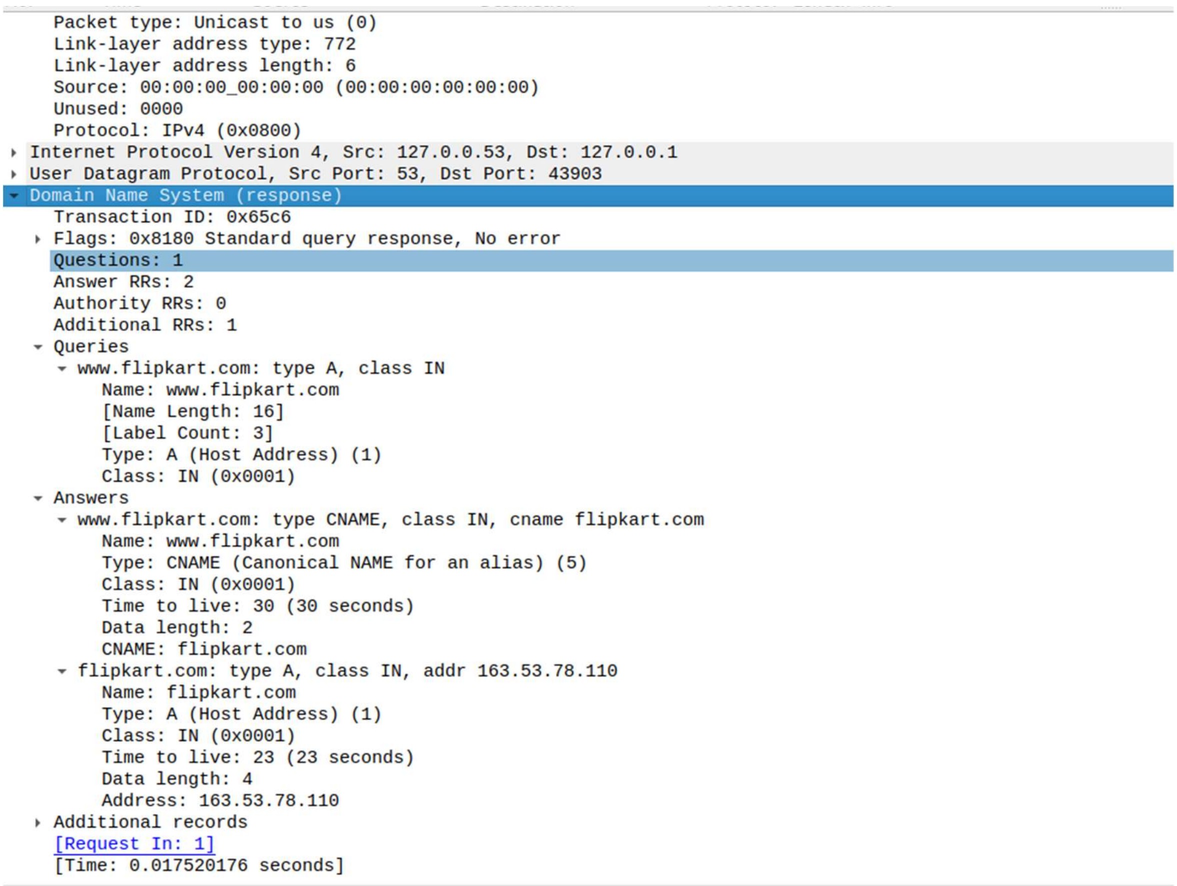
Ping a computer such as [www.google.com (any](www.google.com) domain). Please use Wireshark to show the DNS query triggered by your ping command and DNS response. Describe your observation.


s
Wireshark
Feb 20 09:28
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.53	DNS	89	Standard query 0x65c6 A www.flipkart.com OPT
2	0.000321688	172.16.10.5	192.168.1.1	DNS	89	Standard query 0xa66a A www.flipkart.com OPT
3	0.000971671	127.0.0.1	127.0.0.53	DNS	89	Standard query 0xf4ce AAAA www.flipkart.com OPT
4	0.001544733	172.16.10.5	192.168.1.1	DNS	89	Standard query 0xc6e4 AAAA www.flipkart.com OPT
5	0.016778937	192.168.1.1	172.16.10.5	DNS	248	Standard query response 0xa66a A www.flipkart.com CNAME flipk…
6	0.016779520	192.168.1.1	172.16.10.5	DNS	166	Standard query response 0xc6e4 AAAA www.flipkart.com CNAME fl…
7	0.017520176	127.0.0.53	127.0.0.1	DNS	119	Standard query response 0x65c6 A www.flipkart.com CNAME flipk…
8	0.017781425	172.16.10.5	192.168.1.1	DNS	85	Standard query 0xb759 AAAA flipkart.com OPT
9	0.022023364	192.168.1.1	172.16.10.5	DNS	148	Standard query response 0xb759 AAAA flipkart.com SOA PDNS1.UL…
10	0.022483375	127.0.0.53	127.0.0.1	DNS	103	Standard query response 0xf4ce AAAA www.flipkart.com CNAME fl…
11	0.023087371	172.16.10.5	163.53.78.110	ICMP	100	Echo (ping) request id=0x0004, seq=1/256, ttl=64 (reply in 1…
12	0.039581618	163.53.78.110	172.16.10.5	ICMP	100	Echo (ping) reply id=0x0004, seq=1/256, ttl=58 (request in…
13	0.039973873	127.0.0.1	127.0.0.53	DNS	99	Standard query 0x37fe PTR 110.78.53.163.in-addr.arpa OPT
14	0.040506803	172.16.10.5	192.168.1.1	DNS	99	Standard query 0x8227 PTR 110.78.53.163.in-addr.arpa OPT
15	0.044869540	192.168.1.1	172.16.10.5	DNS	187	Standard query response 0x8227 No such name PTR 110.78.53.163…
16	0.045333640	172.16.10.5	192.168.1.1	DNS	88	Standard query 0x8227 PTR 110.78.53.163.in-addr.arpa
17	0.049362796	192.168.1.1	172.16.10.5	DNS	187	Standard query response 0x8227 No such name PTR 110.78.53.163…



```
▸ Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
▾ Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 772
    Link-layer address length: 6
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
▸ User Datagram Protocol, Src Port: 43903, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x65c6
  ▸ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ 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)
  ▸ Additional records
    [Response In: 7]
```



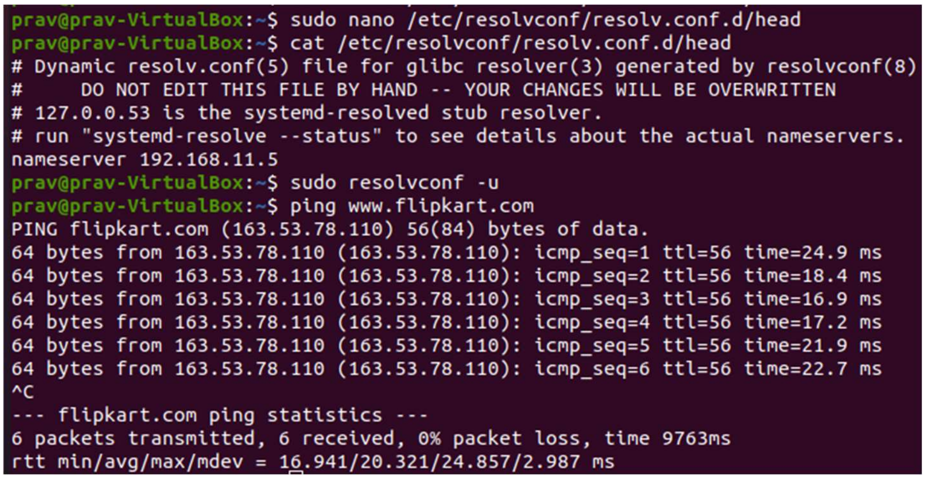
```
    Packet type: Unicast to us (0)
    Link-layer address type: 772
    Link-layer address length: 6
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 127.0.0.53, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 53, Dst Port: 43903
▾ Domain Name System (response)
    Transaction ID: 0x65c6
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 1
  ▾ 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: 30 (30 seconds)
        Data length: 2
        CNAME: flipkart.com
    ▾ flipkart.com: type A, class IN, addr 163.53.78.110
        Name: flipkart.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 23 (23 seconds)
        Data length: 4
        Address: 163.53.78.110
  ▸ Additional records
    [Request In: 1]
    [Time: 0.017520176 seconds]
```

Observations -:

The messages are sent over UDP. The destination port for the DNS query message and the source port for the DNS response message is port 53. DNS query message is sent to 127.0.0.53. The IP address of the local DNS server is also the same. The DNS query message is of ‘A’ type. It does not contain any answers. The DNS response message provides 2 answers. The answer contains A type record along with flipkart ‘s address 163.53.78.110. The destination of the IP address of the SYN packet corresponds to the IP address 163.53.78.110 provided in the response message.

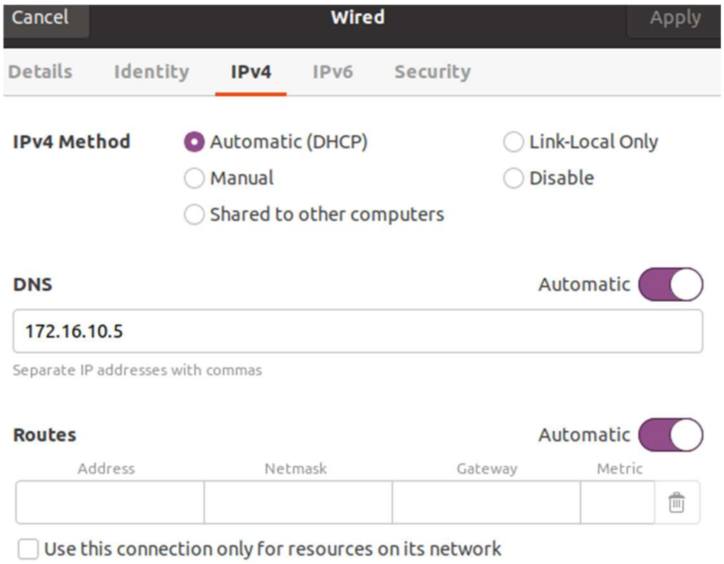
Part 1: Setting Up a Local DNS Server

Task 1: Configure the User/Client Machine



```
prav@prav-VirtualBox:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
prav@prav-VirtualBox:~$ 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
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "systemd-resolve --status" to see details about the actual nameservers.
nameserver 192.168.11.5
prav@prav-VirtualBox:~$ sudo resolvconf -u
prav@prav-VirtualBox:~$ ping www.flipkart.com
PING flipkart.com (163.53.78.110) 56(84) bytes of data.
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=1 ttl=56 time=24.9 ms
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=2 ttl=56 time=18.4 ms
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=3 ttl=56 time=16.9 ms
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=4 ttl=56 time=17.2 ms
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=5 ttl=56 time=21.9 ms
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=6 ttl=56 time=22.7 ms
^C
--- flipkart.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 9763ms
rtt min/avg/max/mdev = 16.941/20.321/24.857/2.987 ms
```

Also, add 172.16.10.5 in ‘Additional DNS servers’ field in IPv4 settings of client machine.



IPv4 Method ● Automatic (DHCP) ○ Link-Local Only
○ Manual ○ Disable
○ Shared to other computers

DNS Automatic ●

172.16.10.5

Separate IP addresses with commas

Routes Automatic ●

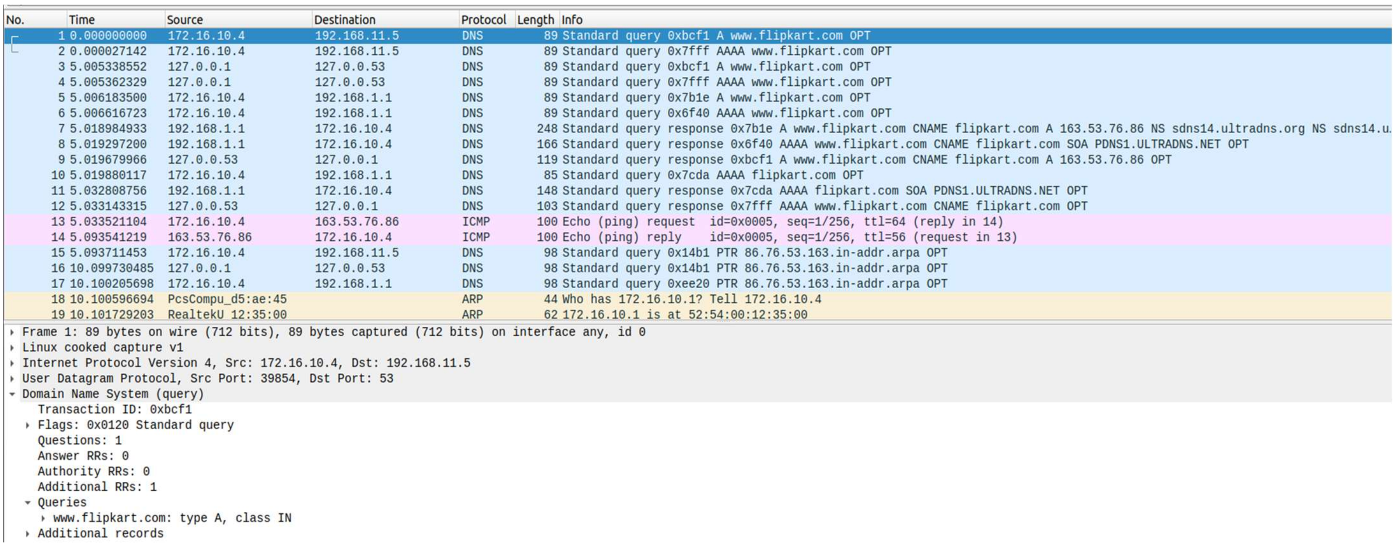
Address Netmask Gateway Metric

□ Use this connection only for resources on its network

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).

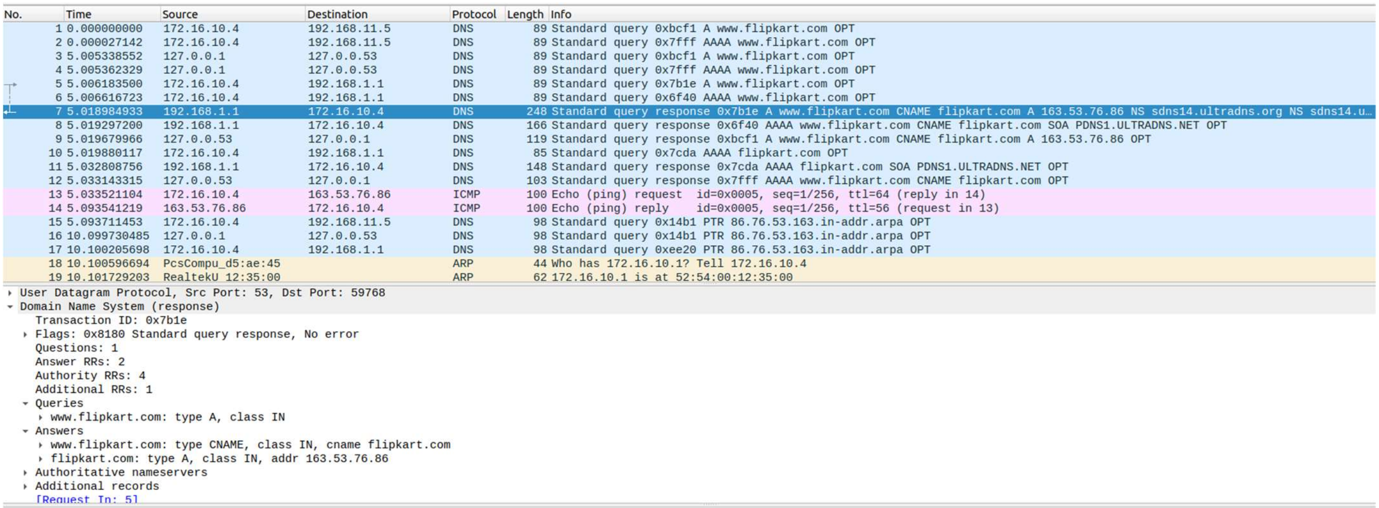
QUERY -:



```
No.   Time          Source             Destination     Protocol  Length Info
    1 0.000000000   172.16.10.4        192.168.11.5    DNS        89 Standard query 0xbcf1 A www.flipkart.com OPT
    2 0.000027142   172.16.10.4        192.168.11.5    DNS        89 Standard query 0x7fff AAAA www.flipkart.com OPT
    3 5.005338552   127.0.0.1          127.0.0.53      DNS        89 Standard query 0xbcf1 A www.flipkart.com OPT
    4 5.005362329   127.0.0.1          127.0.0.53      DNS        89 Standard query 0x7fff AAAA www.flipkart.com OPT
    5 5.006183500   172.16.10.4        192.168.1.1     DNS        89 Standard query 0x7b1e A www.flipkart.com OPT
    6 5.006616723   172.16.10.4        192.168.1.1     DNS        89 Standard query 0x6f40 AAAA www.flipkart.com OPT
    7 5.018984933   192.168.1.1        172.16.10.4     DNS       248 Standard query response 0x7b1e A www.flipkart.com CNAME flipkart.com A 163.53.76.86 NS sdns14.ultradns.org NS sdns14.u
    8 5.019297200   192.168.1.1        172.16.10.4     DNS       166 Standard query response 0x6f40 AAAA www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET OPT
    9 5.019679966   127.0.0.53         127.0.0.1       DNS       119 Standard query response 0xbcf1 A www.flipkart.com CNAME flipkart.com A 163.53.76.86 OPT
   10 5.019880117   172.16.10.4        192.168.1.1     DNS        85 Standard query 0x7cda AAAA flipkart.com OPT
   11 5.032808756   192.168.1.1        172.16.10.4     DNS       148 Standard query response 0x7cda AAAA flipkart.com SOA PDNS1.ULTRADNS.NET OPT
   12 5.033143315   127.0.0.53         127.0.0.1       DNS       103 Standard query response 0x7fff AAAA www.flipkart.com CNAME flipkart.com OPT
   13 5.033521104   172.16.10.4        163.53.76.86    ICMP      100 Echo (ping) request  id=0x0005, seq=1/256, ttl=64 (reply in 14)
   14 5.093541219   163.53.76.86       172.16.10.4     ICMP      100 Echo (ping) reply    id=0x0005, seq=1/256, ttl=56 (request in 13)
   15 5.093711453   172.16.10.4        192.168.11.5    DNS        98 Standard query 0x14b1 PTR 86.76.53.163.in-addr.arpa OPT
   16 10.099730485  127.0.0.1          127.0.0.53      DNS        98 Standard query 0x14b1 PTR 86.76.53.163.in-addr.arpa OPT
   17 10.100205698  172.16.10.4        192.168.1.1     DNS        98 Standard query 0xee20 PTR 86.76.53.163.in-addr.arpa OPT
   18 10.100596694  PcsCompu_d5:ae:45                  ARP        44 Who has 172.16.10.1? Tell 172.16.10.4
   19 10.101729203  RealtekU 12:35:00                  ARP        62 172.16.10.1 is at 52:54:00:12:35:00
```

```
› Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 172.16.10.4, Dst: 192.168.11.5
› User Datagram Protocol, Src Port: 39854, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0xbcf1
  › Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    › www.flipkart.com: type A, class IN
  › Additional records
```

RESPONSE -:



```
No.   Time          Source             Destination     Protocol  Length Info
    1 0.000000000   172.16.10.4        192.168.11.5    DNS        89 Standard query 0xbcf1 A www.flipkart.com OPT
    2 0.000027142   172.16.10.4        192.168.11.5    DNS        89 Standard query 0x7fff AAAA www.flipkart.com OPT
    3 5.005338552   127.0.0.1          127.0.0.53      DNS        89 Standard query 0xbcf1 A www.flipkart.com OPT
    4 5.005362329   127.0.0.1          127.0.0.53      DNS        89 Standard query 0x7fff AAAA www.flipkart.com OPT
    5 5.006183500   172.16.10.4        192.168.1.1     DNS        89 Standard query 0x7b1e A www.flipkart.com OPT
    6 5.006616723   172.16.10.4        192.168.1.1     DNS        89 Standard query 0x6f40 AAAA www.flipkart.com OPT
    7 5.018984933   192.168.1.1        172.16.10.4     DNS       248 Standard query response 0x7b1e A www.flipkart.com CNAME flipkart.com A 163.53.76.86 NS sdns14.ultradns.org NS sdns14.u…
    8 5.019297200   192.168.1.1        172.16.10.4     DNS       166 Standard query response 0x6f40 AAAA www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET OPT
    9 5.019679966   127.0.0.53         127.0.0.1       DNS       119 Standard query response 0xbcf1 A www.flipkart.com CNAME flipkart.com A 163.53.76.86 OPT
   10 5.019880117   172.16.10.4        192.168.1.1     DNS        85 Standard query 0x7cda AAAA flipkart.com OPT
   11 5.032808756   192.168.1.1        172.16.10.4     DNS       148 Standard query response 0x7cda AAAA flipkart.com SOA PDNS1.ULTRADNS.NET OPT
   12 5.033143315   127.0.0.53         127.0.0.1       DNS       103 Standard query response 0x7fff AAAA www.flipkart.com CNAME flipkart.com OPT
   13 5.033521104   172.16.10.4        163.53.76.86    ICMP      100 Echo (ping) request  id=0x0005, seq=1/256, ttl=64 (reply in 14)
   14 5.093541219   163.53.76.86       172.16.10.4     ICMP      100 Echo (ping) reply    id=0x0005, seq=1/256, ttl=56 (request in 13)
   15 5.093711453   172.16.10.4        192.168.11.5    DNS        98 Standard query 0x14b1 PTR 86.76.53.163.in-addr.arpa OPT
   16 10.099730485  127.0.0.1          127.0.0.53      DNS        98 Standard query 0x14b1 PTR 86.76.53.163.in-addr.arpa OPT
   17 10.100205698  172.16.10.4        192.168.1.1     DNS        98 Standard query 0xee20 PTR 86.76.53.163.in-addr.arpa OPT
   18 10.100596694  PcsCompu_d5:ae:45                  ARP        44 Who has 172.16.10.1? Tell 172.16.10.4
   19 10.101729203  RealtekU 12:35:00                  ARP        62 172.16.10.1 is at 52:54:00:12:35:00
```

```
› User Datagram Protocol, Src Port: 53, Dst Port: 59768
▾ Domain Name System (response)
    Transaction ID: 0x7b1e
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 4
    Additional RRs: 1
  ▾ 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
  › Additional records
    [Request In: 5]
```

Messages are sent over UDP. Destination port for DNS query message and source port for query response message is port 53. DNS query is of A type and does not have any answers whereas DNS response has 2 answers.

Task 2: Set Up a Local DNS Server

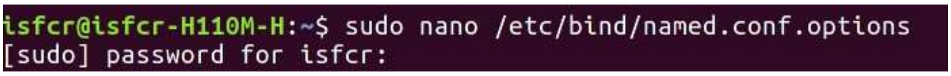
Note: If bind9 server is not already installed, install using the command

$ sudo apt-get update

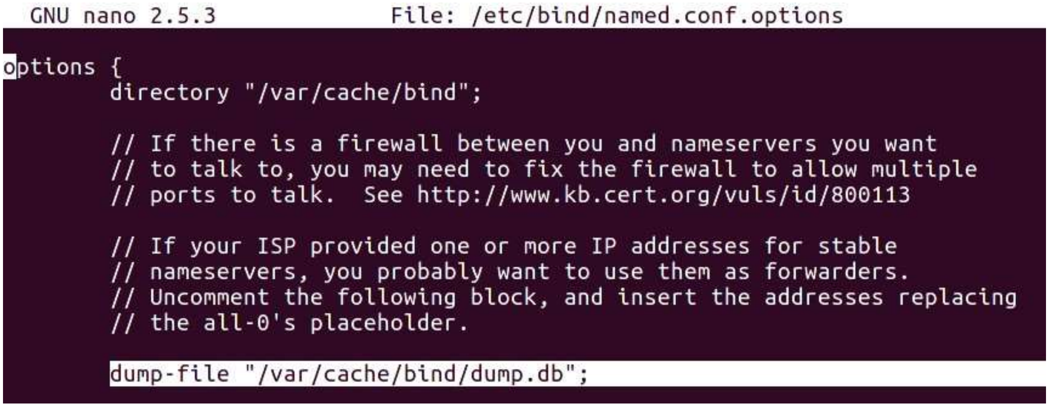
$ sudo apt-get install bind9

Step 1: Configure the BIND9 Server.

BIND9 gets its configuration from a file called **/etc/bind/named.conf**. This file is the primary configuration file, and it usually contains several "include" entries. One of the included files is called **/etc/bind/named.conf.options**. This is where we typically set up the configuration options. Let us first set up an option related to DNS cache by adding a dump-file entry to the options block. The above option specifies where the cache content should be dumped to if BIND is asked to dump its cache.



```
isfcr@isfcr-H110M-H:~$ sudo nano /etc/bind/named.conf.options
[sudo] password for isfcr:
```



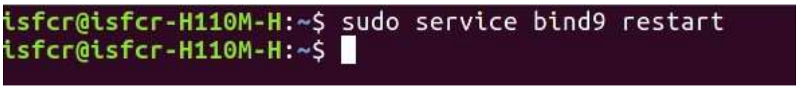
```
  GNU nano 2.5.3             File: /etc/bind/named.conf.options

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";
```

The above option specifies where the cache content should be dumped to if BIND is asked to dump its cache. If this option is not specified, BIND dumps the cache to a default file called **/var/cache/bind/named_dump.db**.

Step 2: Start DNS server

We start the DNS server using the command:

$ sudo service bind9 restart

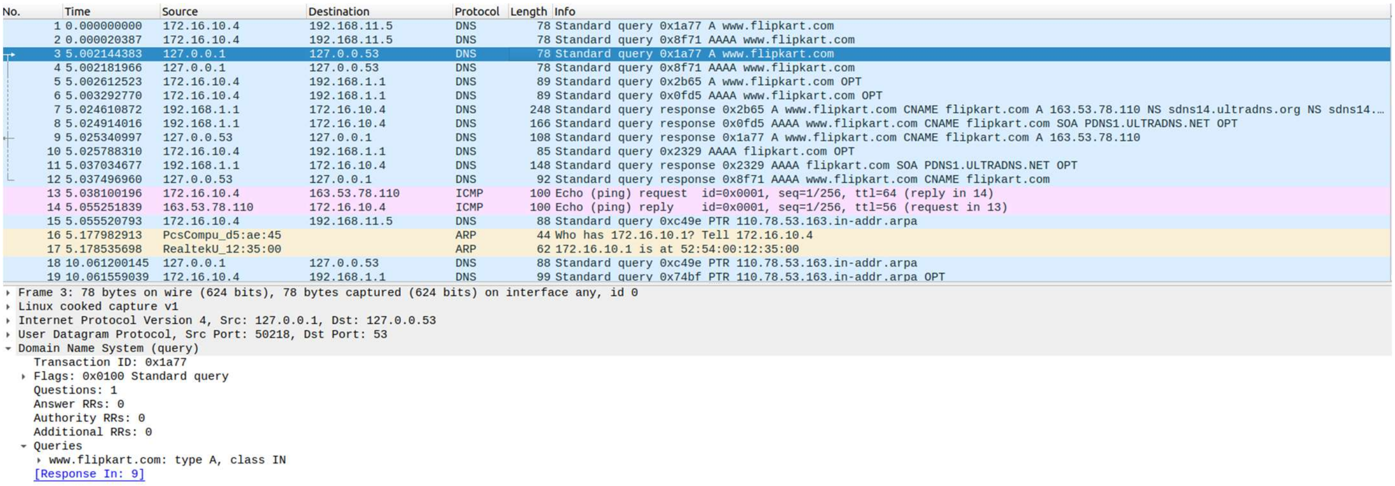


```
isfcr@isfcr-H110M-H:~$ sudo service bind9 restart
isfcr@isfcr-H110M-H:~$ 
```

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).

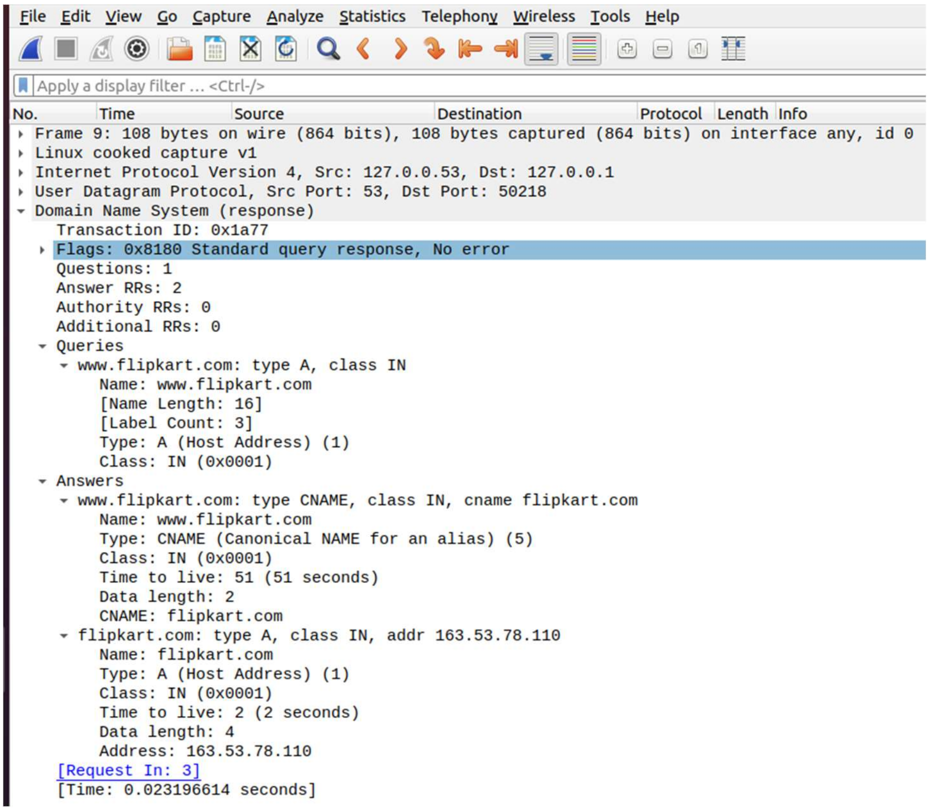
Query -:



```
No.      Time          Source              Destination       Protocol Length Info
      1 0.000000000   172.16.10.4         192.168.11.5      DNS         78 Standard query 0x1a77 A www.flipkart.com
      2 0.000020387   172.16.10.4         192.168.11.5      DNS         78 Standard query 0x8f71 AAAA www.flipkart.com
      3 5.002144383   127.0.0.1           127.0.0.53        DNS         78 Standard query 0x1a77 A www.flipkart.com
      4 5.002181966   127.0.0.1           127.0.0.53        DNS         78 Standard query 0x8f71 AAAA www.flipkart.com
      5 5.002612523   172.16.10.4         192.168.1.1       DNS         89 Standard query 0x2b65 A www.flipkart.com OPT
      6 5.003292770   172.16.10.4         192.168.1.1       DNS         89 Standard query 0x0fd5 AAAA www.flipkart.com OPT
      7 5.024610872   192.168.1.1         172.16.10.4       DNS        248 Standard query response 0x2b65 A www.flipkart.com CNAME flipkart.com A 163.53.78.110 NS sdns14.ultradns.org NS sdns14.…
      8 5.024914016   192.168.1.1         172.16.10.4       DNS        166 Standard query response 0x0fd5 AAAA www.flipkart.com CNAME flipkart.com SOA PDNS1.ULTRADNS.NET OPT
      9 5.025340997   127.0.0.53          127.0.0.1         DNS        108 Standard query response 0x1a77 A www.flipkart.com CNAME flipkart.com A 163.53.78.110
     10 5.025788310   172.16.10.4         192.168.1.1       DNS         85 Standard query 0x2329 AAAA flipkart.com OPT
     11 5.037034677   192.168.1.1         172.16.10.4       DNS        148 Standard query response 0x2329 AAAA flipkart.com SOA PDNS1.ULTRADNS.NET OPT
     12 5.037496960   127.0.0.53          127.0.0.1         DNS         92 Standard query response 0x8f71 AAAA www.flipkart.com CNAME flipkart.com
     13 5.038100196   172.16.10.4         163.53.78.110     ICMP       100 Echo (ping) request  id=0x0001, seq=1/256, ttl=64 (reply in 14)
     14 5.055251839   163.53.78.110       172.16.10.4       ICMP       100 Echo (ping) reply    id=0x0001, seq=1/256, ttl=56 (request in 13)
     15 5.055520793   172.16.10.4         192.168.11.5      DNS         88 Standard query 0xc49e PTR 110.78.53.163.in-addr.arpa
     16 5.177982913   PcsCompu_d5:ae:45                     ARP         44 Who has 172.16.10.1? Tell 172.16.10.4
     17 5.178535698   RealtekU_12:35:00                     ARP         62 172.16.10.1 is at 52:54:00:12:35:00
     18 10.061200145  127.0.0.1           127.0.0.53        DNS         88 Standard query 0xc49e PTR 110.78.53.163.in-addr.arpa
     19 10.061559039  172.16.10.4         192.168.1.1       DNS         99 Standard query 0x74bf PTR 110.78.53.163.in-addr.arpa OPT
```

```
▸ Frame 3: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
▸ User Datagram Protocol, Src Port: 50218, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x1a77
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.flipkart.com: type A, class IN
    [Response In: 9]
```

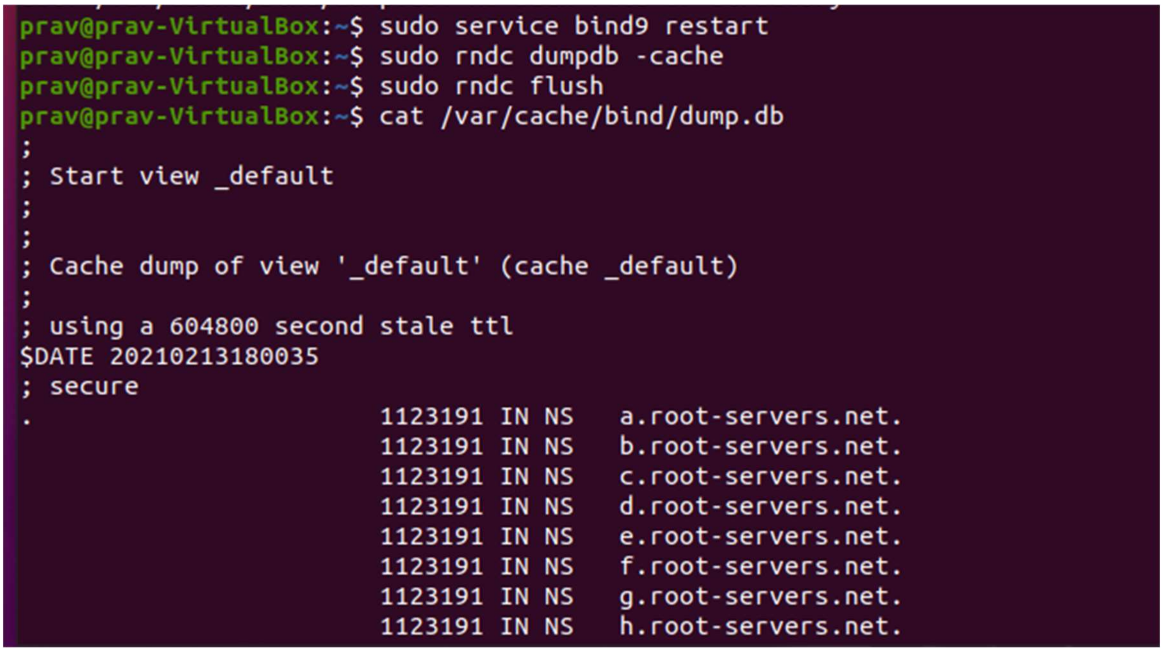
Response -:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.      Time          Source              Destination       Protocol Length Info
▸ Frame 9: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 127.0.0.53, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 53, Dst Port: 50218
▾ Domain Name System (response)
    Transaction ID: 0x1a77
  ▸ 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: 51 (51 seconds)
        Data length: 2
        CNAME: flipkart.com
    ▾ flipkart.com: type A, class IN, addr 163.53.78.110
        Name: flipkart.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 2 (2 seconds)
        Data length: 4
        Address: 163.53.78.110
    [Request In: 3]
    [Time: 0.023196614 seconds]
```

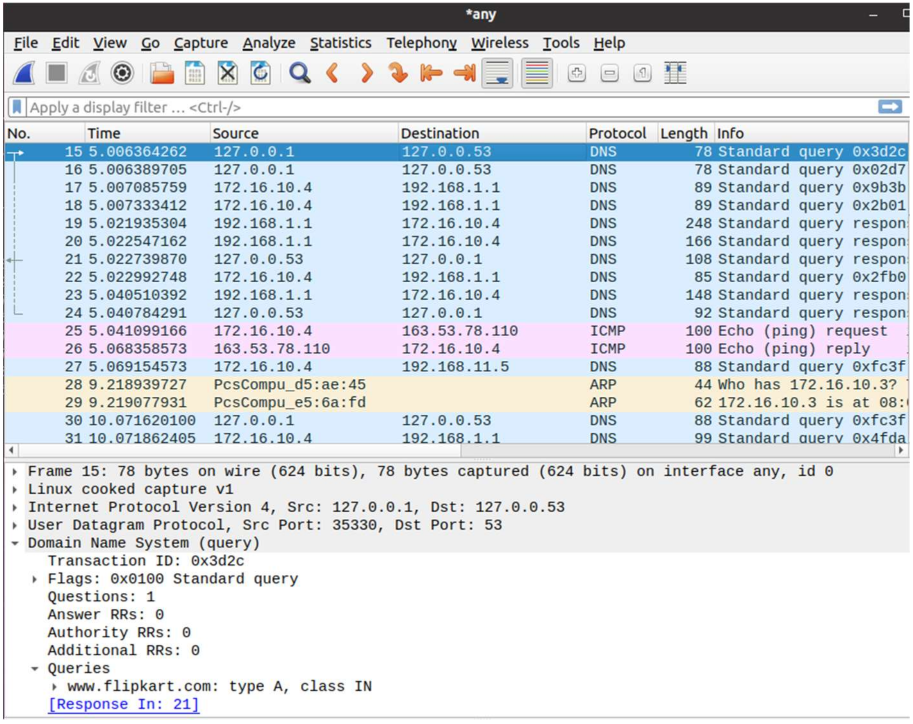
Observation 4:

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.



```
prav@prav-VirtualBox:~$ sudo service bind9 restart
prav@prav-VirtualBox:~$ sudo rndc dumpdb -cache
prav@prav-VirtualBox:~$ sudo rndc flush
prav@prav-VirtualBox:~$ cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
; using a 604800 second stale ttl
$DATE 20210213180035
; secure
.                       1123191 IN NS   a.root-servers.net.
                        1123191 IN NS   b.root-servers.net.
                        1123191 IN NS   c.root-servers.net.
                        1123191 IN NS   d.root-servers.net.
                        1123191 IN NS   e.root-servers.net.
                        1123191 IN NS   f.root-servers.net.
                        1123191 IN NS   g.root-servers.net.
                        1123191 IN NS   h.root-servers.net.
```

Query -:

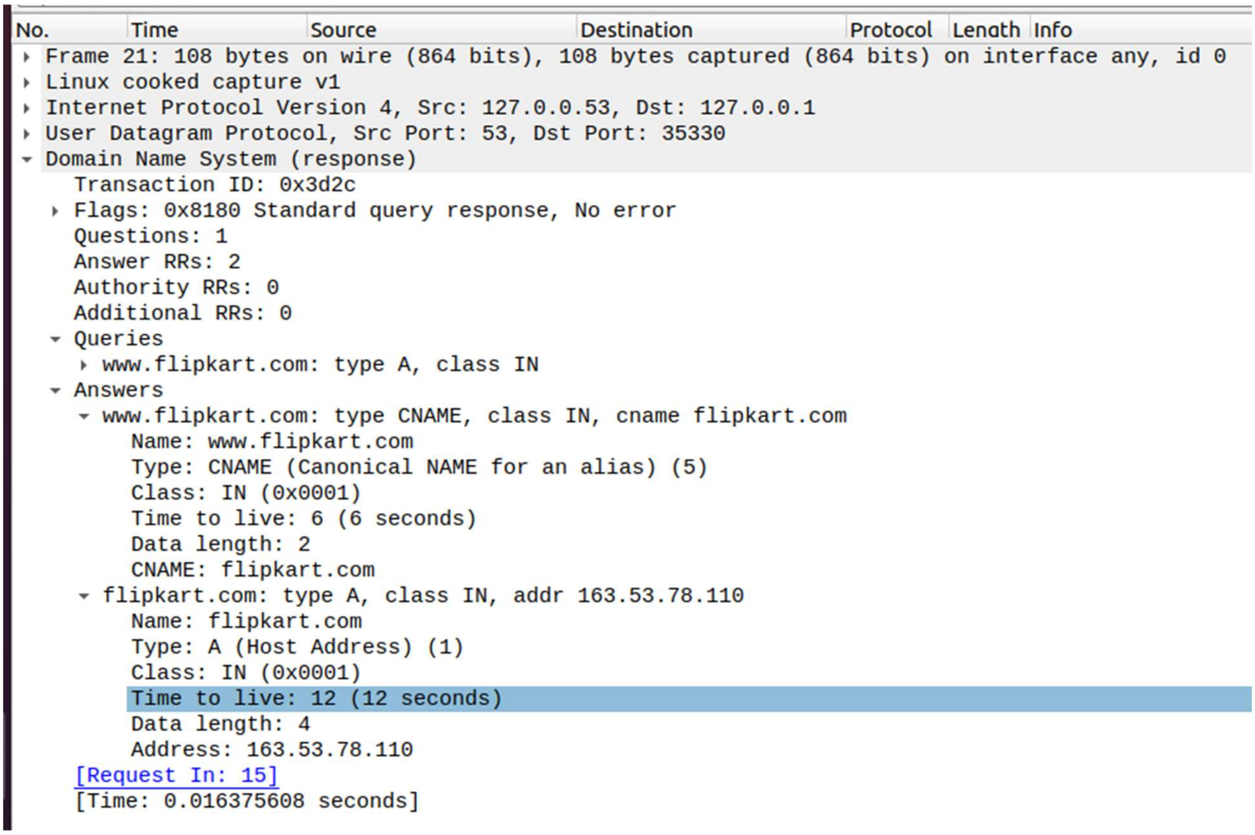


*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

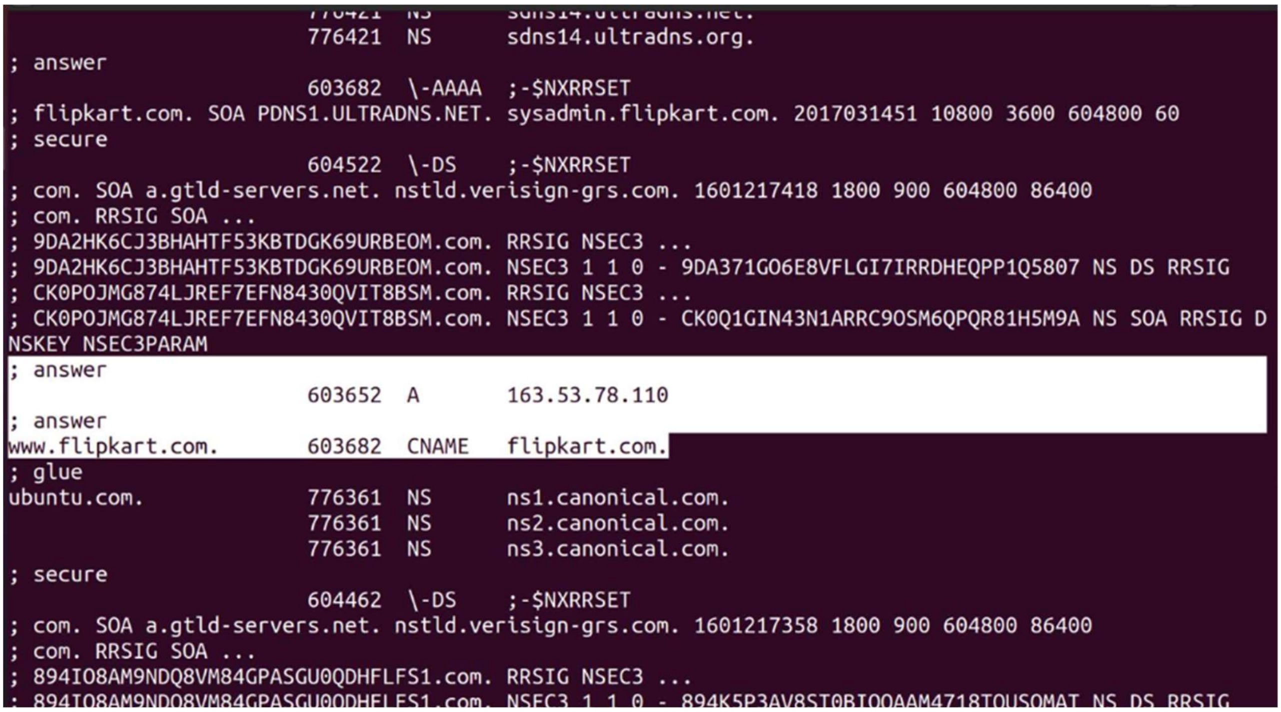
No.	Time	Source	Destination	Protocol	Length	Info
15	5.006364262	127.0.0.1	127.0.0.53	DNS	78	Standard query 0x3d2c
16	5.006389705	127.0.0.1	127.0.0.53	DNS	78	Standard query 0x02d7
17	5.007085759	172.16.10.4	192.168.1.1	DNS	89	Standard query 0x9b3b
18	5.007333412	172.16.10.4	192.168.1.1	DNS	89	Standard query 0x2b01
19	5.021935304	192.168.1.1	172.16.10.4	DNS	248	Standard query respon
20	5.022547162	192.168.1.1	172.16.10.4	DNS	166	Standard query respon
21	5.022739870	127.0.0.53	127.0.0.1	DNS	108	Standard query respon
22	5.022992748	172.16.10.4	192.168.1.1	DNS	85	Standard query 0x2fb0
23	5.040510392	192.168.1.1	172.16.10.4	DNS	148	Standard query respon
24	5.040784291	127.0.0.53	127.0.0.1	DNS	92	Standard query respon
25	5.041099166	172.16.10.4	163.53.78.110	ICMP	100	Echo (ping) request
26	5.068358573	163.53.78.110	172.16.10.4	ICMP	100	Echo (ping) reply
27	5.069154573	172.16.10.4	192.168.11.5	DNS	88	Standard query 0xfc3f
28	9.218939727	PcsCompu_d5:ae:45		ARP	44	Who has 172.16.10.3?
29	9.219077931	PcsCompu_e5:6a:fd		ARP	62	172.16.10.3 is at 08:
30	10.071620100	127.0.0.1	127.0.0.53	DNS	88	Standard query 0xfc3f
31	10.071862405	172.16.10.4	192.168.1.1	DNS	99	Standard query 0x4fda

```
▸ Frame 15: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.53
▸ User Datagram Protocol, Src Port: 35330, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x3d2c
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.flipkart.com: type A, class IN
    [Response In: 21]
```

Response -:



```
No.        Time          Source              Destination         Protocol  Length  Info
▸ Frame 21: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 127.0.0.53, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 53, Dst Port: 35330
▾ Domain Name System (response)
    Transaction ID: 0x3d2c
  ▸ 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
  ▾ 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: 6 (6 seconds)
        Data length: 2
        CNAME: flipkart.com
    ▾ flipkart.com: type A, class IN, addr 163.53.78.110
        Name: flipkart.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 12 (12 seconds)
        Data length: 4
        Address: 163.53.78.110
    [Request In: 15]
    [Time: 0.016375608 seconds]
```

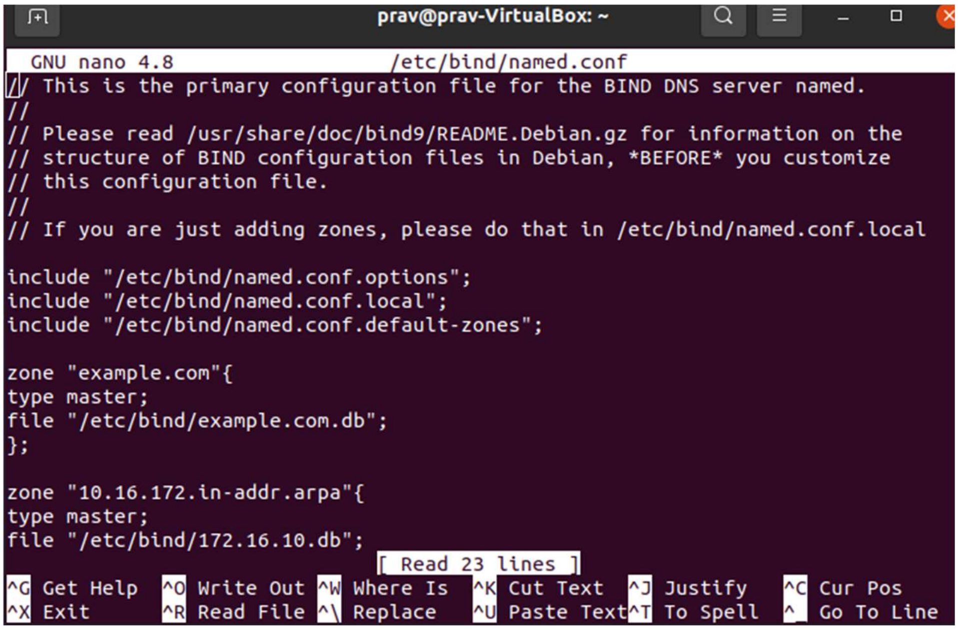


```
                        776421  NS      sdns14.ultradns.net.
                        776421  NS      sdns14.ultradns.org.
; answer
                        603682  \-AAAA  ;-$NXRRSET
; flipkart.com. SOA PDNS1.ULTRADNS.NET. sysadmin.flipkart.com. 2017031451 10800 3600 604800 60
; secure
                        604522  \-DS    ;-$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 - 894K5P3AV8ST0BIOOAM4718TOUSOMAT NS DS RRSIG
```

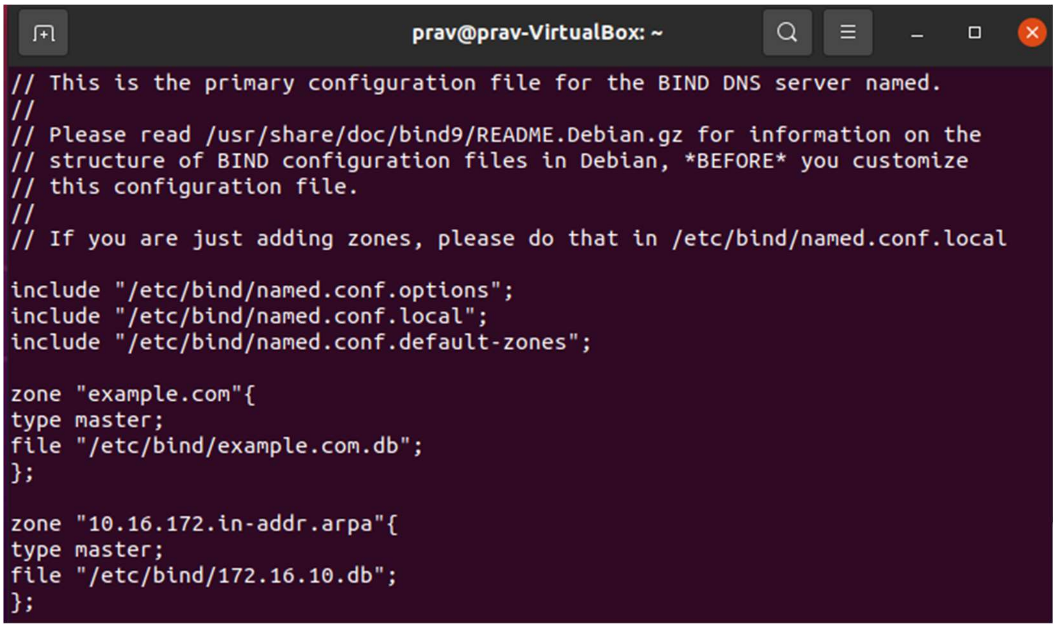
Part 2: Setting Up Authoritative Nameserver for example.com domain

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

Step 1: Create Zones



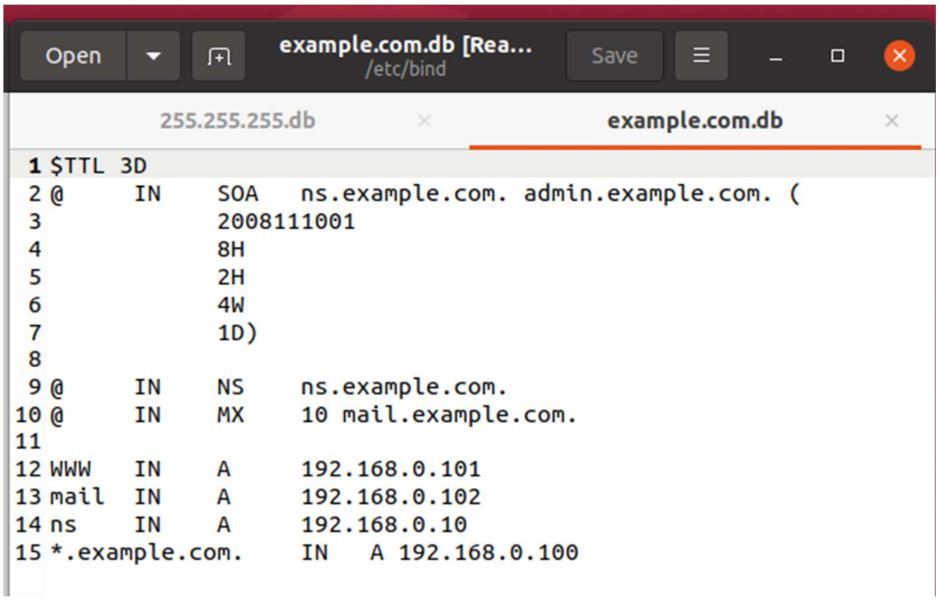
```
  GNU nano 4.8                    /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration 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 "10.16.172.in-addr.arpa"{
type master;
file "/etc/bind/172.16.10.db";
                               [ Read 23 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text^T To Spell    ^_ Go To Line
```



```
// 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 "10.16.172.in-addr.arpa"{
type master;
file "/etc/bind/172.16.10.db";
};
```

Step 2: Setup the forward lookup zone file

We create **example.com.db** zone file with the following contents in the **/etc/bind/** directory where the actual DNS resolution is stored.

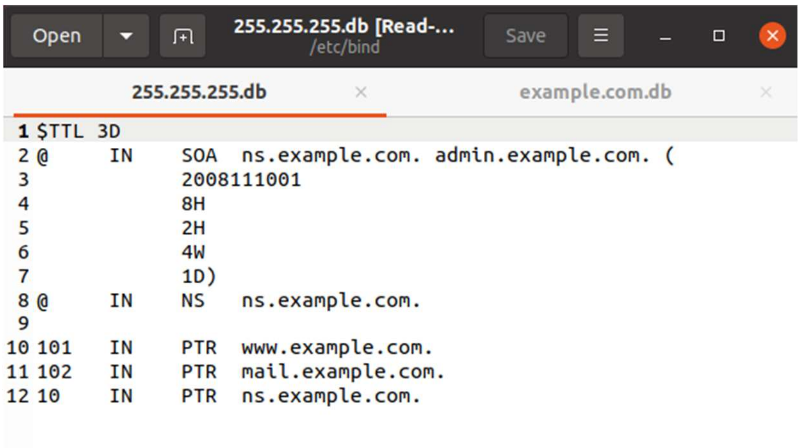


```
$TTL  3D
@      IN     SOA    ns.example.com. admin.example.com. (
              2008111001
              8H
              2H
              4W
              1D)

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

www    IN     A      192.168.0.101
mail   IN     A      192.168.0.102
ns     IN     A      192.168.0.10
*.example.com.       IN    A 192.168.0.100
```

The symbol '@' is a special notation representing the origin specified in **named.conf** (the string after "**zone**"). Therefore, '@' here stands for **example.com**. This zone file contains 7 resource records (RRs), including a SOA (Start Of Authority) RR, a NS (Name Server) RR, a MX (Mail eXchanger) RR, and 4 A (host Address) RRs.

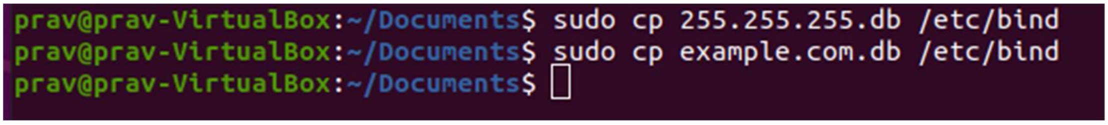
Step 3: Setup the reverse lookup zone file

We create a reverse DNS lookup file called **255.255.255.db** for the example.net domain to support DNS reverse lookup, i.e., from IP address to hostname in the **/etc/bind/** directory with the following contents.

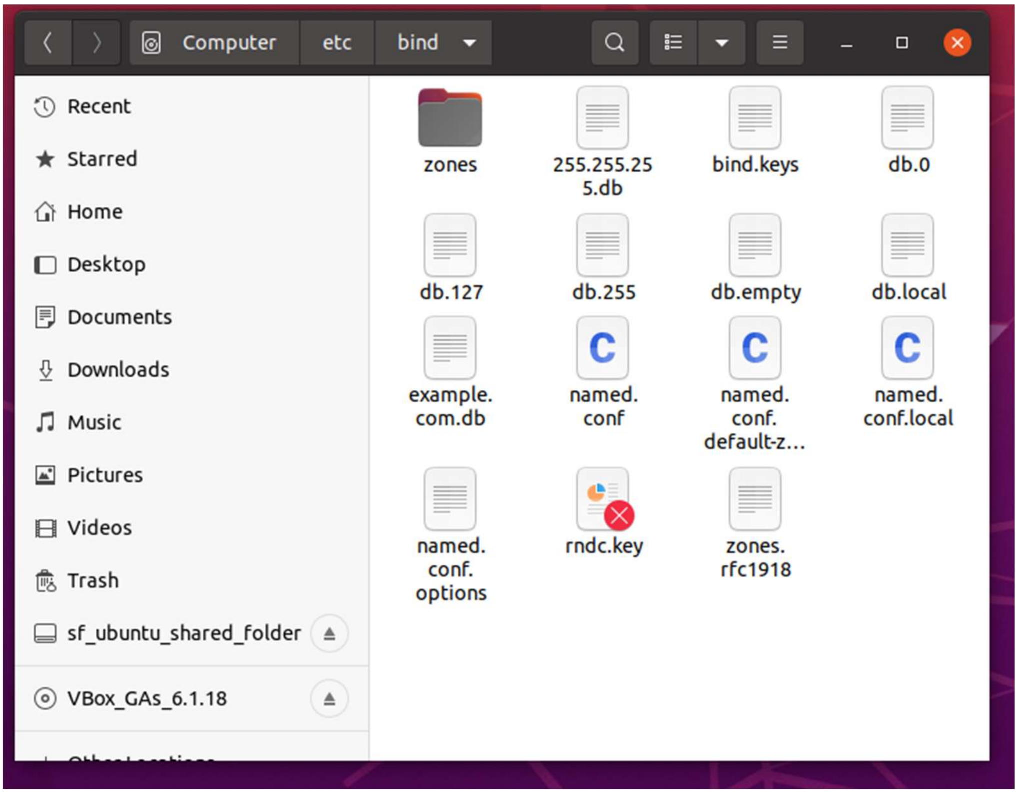


```
$TTL  3D
@      IN     SOA    ns.example.com. admin.example.com. (
              2008111001
              8H
              2H
              4W
              1D)
@      IN     NS     ns.example.com.

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

Step 4: Copy the above files into **/etc/bind** location.



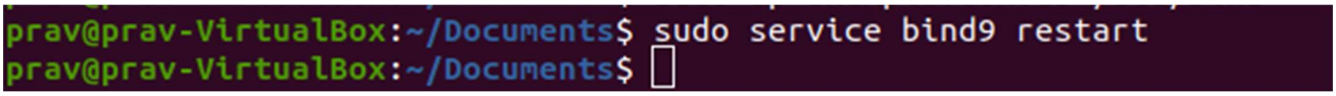
```
prav@prav-VirtualBox:~/Documents$ sudo cp 255.255.255.db /etc/bind
prav@prav-VirtualBox:~/Documents$ sudo cp example.com.db /etc/bind
prav@prav-VirtualBox:~/Documents$ 
```



Task 4: Restart the BIND server and test

Step 1: When all the changes are made, remember to restart the BIND server. Now we will restart the DNS server using the following command:

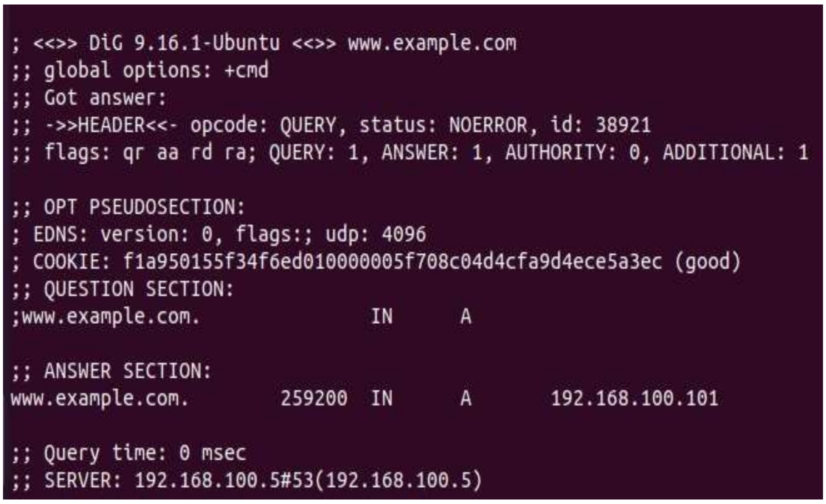
$ sudo service bind9 restart



```
prav@prav-VirtualBox:~/Documents$ sudo service bind9 restart
prav@prav-VirtualBox:~/Documents$ 
```

Step 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.

Dig stands for (Domain Information Groper) is a network administration command-line tool for querying DNS name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups and displays the answers that are returned from the name server that were queried. dig is part of the BIND domain name server software suite.

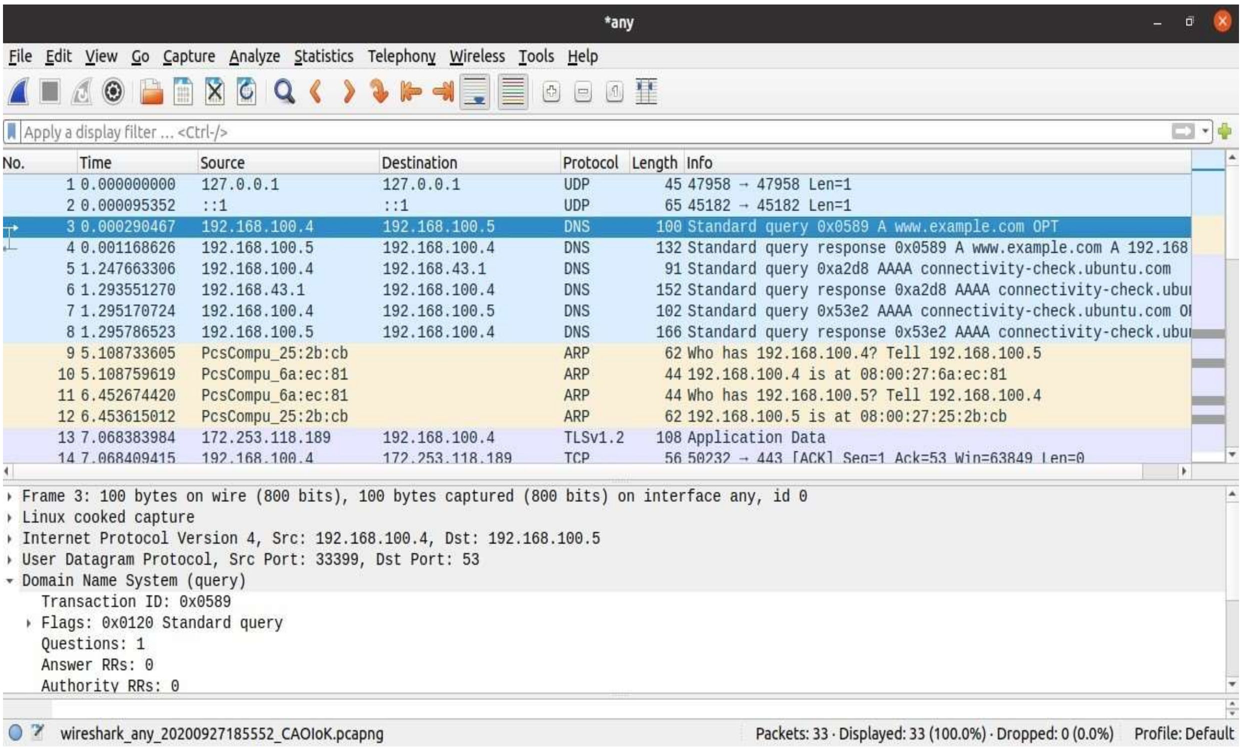


```
; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38921
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: f1a950155f34f6ed010000005f708c04d4cfa9d4ece5a3ec (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       192.168.100.101

;; Query time: 0 msec
;; SERVER: 192.168.100.5#53(192.168.100.5)
```

We can see that the ANSWER SECTION contains the DNS mapping. We can see that the IP address of www.example.com is now 10.2.22.101, which is what we have setup in the DNS server.

Step 3: Observe the results in Wireshark capture.

Query -:

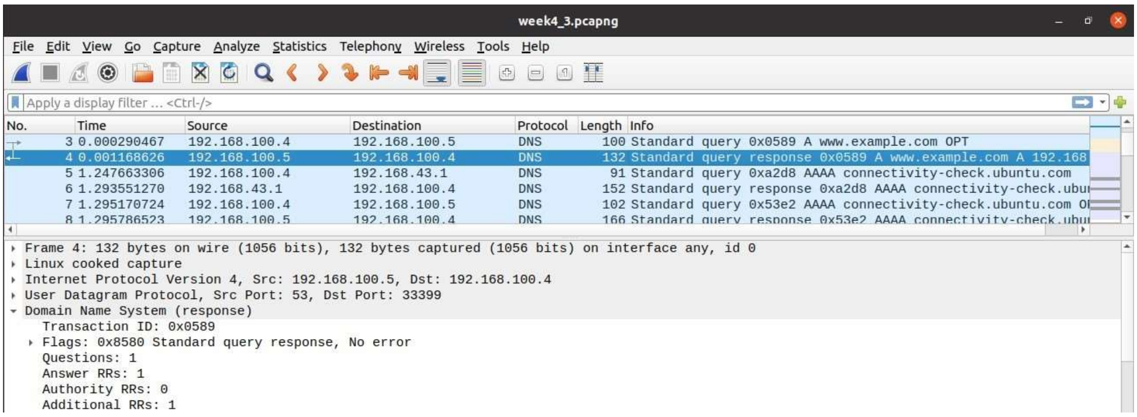

*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time         Source             Destination        Protocol Length Info
      1 0.000000000  127.0.0.1          127.0.0.1          UDP        45 47958 → 47958 Len=1
      2 0.000095352  ::1                ::1                UDP        65 45182 → 45182 Len=1
      3 0.000290467  192.168.100.4      192.168.100.5      DNS       100 Standard query 0x0589 A www.example.com OPT
      4 0.001168626  192.168.100.5      192.168.100.4      DNS       132 Standard query response 0x0589 A www.example.com A 192.168
      5 1.247663306  192.168.100.4      192.168.43.1       DNS        91 Standard query 0xa2d8 AAAA connectivity-check.ubuntu.com
      6 1.293551270  192.168.43.1       192.168.100.4      DNS       152 Standard query response 0xa2d8 AAAA connectivity-check.ubu
      7 1.295170724  192.168.100.4      192.168.100.5      DNS       102 Standard query 0x53e2 AAAA connectivity-check.ubuntu.com O
      8 1.295786523  192.168.100.5      192.168.100.4      DNS       166 Standard query response 0x53e2 AAAA connectivity-check.ubu
      9 5.108733605  PcsCompu_25:2b:cb                     ARP        62 Who has 192.168.100.4? Tell 192.168.100.5
     10 5.108759619  PcsCompu_6a:ec:81                     ARP        44 192.168.100.4 is at 08:00:27:6a:ec:81
     11 6.452674420  PcsCompu_6a:ec:81                     ARP        44 Who has 192.168.100.5? Tell 192.168.100.4
     12 6.453615012  PcsCompu_25:2b:cb                     ARP        62 192.168.100.5 is at 08:00:27:25:2b:cb
     13 7.068383984  172.253.118.189    192.168.100.4      TLSv1.2   108 Application Data
     14 7.068409415  192.168.100.4      172.253.118.189    TCP        56 50232 → 443 [ACK] Seq=1 Ack=53 Win=63849 Len=0
```

```
▸ Frame 3: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 192.168.100.4, Dst: 192.168.100.5
▸ User Datagram Protocol, Src Port: 33399, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x0589
  ▸ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

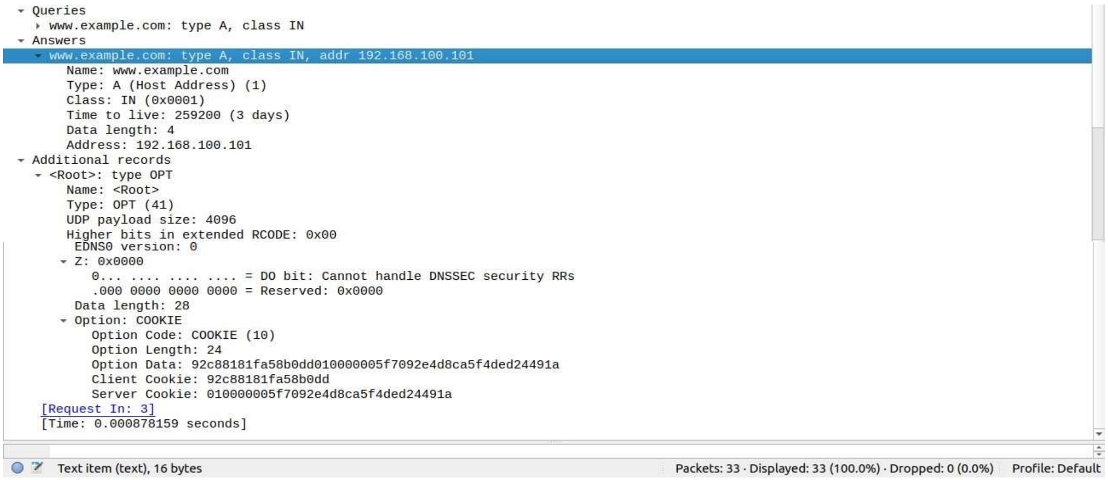
```
wireshark_any_20200927185552_CAOIoK.pcapng          Packets: 33 · Displayed: 33 (100.0%) · Dropped: 0 (0.0%)    Profile: Default
```

Response -:


week4_3.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source           Destination      Protocol Length Info
    3 0.000290467   192.168.100.4    192.168.100.5    DNS        100 Standard query 0x0589 A www.example.com OPT
    4 0.001168626   192.168.100.5    192.168.100.4    DNS        132 Standard query response 0x0589 A www.example.com A 192.168
    5 1.247663306   192.168.100.4    192.168.43.1     DNS         91 Standard query 0xa2d8 AAAA connectivity-check.ubuntu.com
    6 1.293551270   192.168.43.1     192.168.100.4    DNS        152 Standard query response 0xa2d8 AAAA connectivity-check.ubu
    7 1.295170724   192.168.100.4    192.168.100.5    DNS        102 Standard query 0x53e2 AAAA connectivity-check.ubuntu.com OI
    8 1.295786523   192.168.100.5    192.168.100.4    DNS        166 Standard query response 0x53e2 AAAA connectivity-check.ubu
```

```
▸ Frame 4: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 192.168.100.5, Dst: 192.168.100.4
▸ User Datagram Protocol, Src Port: 53, Dst Port: 33399
▾ Domain Name System (response)
    Transaction ID: 0x0589
  ▸ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
```



```
  ▾ Queries
    ▸ www.example.com: type A, class IN
  ▾ Answers
    ▾ www.example.com: type A, class IN, addr 192.168.100.101
        Name: www.example.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 259200 (3 days)
        Data length: 4
        Address: 192.168.100.101
  ▾ Additional records
    ▾ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
         EDNS0 version: 0
       ▾ Z: 0x0000
           0... .... .... .... = DO bit: Cannot handle DNSSEC security RRs
           .000 0000 0000 0000 = Reserved: 0x0000
         Data length: 28
       ▾ Option: COOKIE
           Option Code: COOKIE (10)
           Option Length: 24
           Option Data: 92c88181fa58b0dd010000005f7092e4d8ca5f4ded24491a
           Client Cookie: 92c88181fa58b0dd
           Server Cookie: 010000005f7092e4d8ca5f4ded24491a
    [Request In: 3]
    [Time: 0.000878159 seconds]

Text item (text), 16 bytes          Packets: 33 · Displayed: 33 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

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?

   The DNS query and response messages are sent over UDP.

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

   The destination port for the query message and the source port for the DNS response message is port 53.

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 message is made to server at the IP Address 192.168.100. Yes, the 2 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"?

It is of type A, which means authoritative. The query message does not contain any answers.

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

The answer section of DNS response message contains 1 resource record, which is from example.com and its of type A, class IN.

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?

The destination IP address of the SYN packet corresponds to the IP address of hostname (www.example.com) retrieved from the response message.