

COMPUTER NETWORKS LABORATORY

By:
Nitish S
PES2201800368
5 'A'

WEEK – 4- Implementation of Local DNS Server

Date: 21/09/2020

The objectives of this lab are to understand:

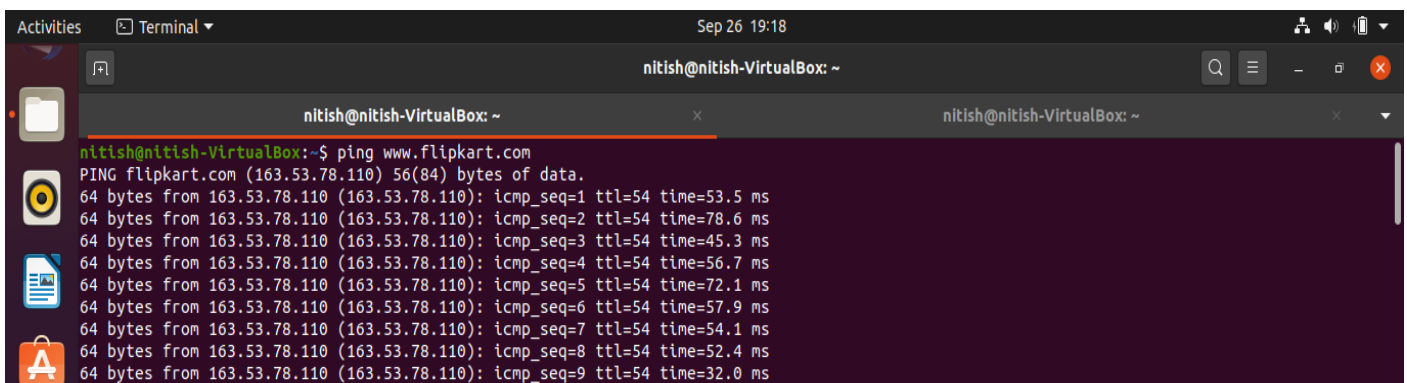
- DNS and how it works
- Install and set up a DNS server
- Functionality and operations

CLIENT MACHINE: 10.0.2.4

SERVER MACHINE:10.0.2.15

First Test:

Ping a computer such as www.flipkart.com. Please use Wireshark to show the DNS query triggered by your ping command and DNS response. Describe your observation. (Take a screenshot).



```
nitish@nitish-VirtualBox: ~  
nitish@nitish-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=54 time=53.5 ms  
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=2 ttl=54 time=78.6 ms  
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=3 ttl=54 time=45.3 ms  
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=4 ttl=54 time=56.7 ms  
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=5 ttl=54 time=72.1 ms  
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=6 ttl=54 time=57.9 ms  
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=7 ttl=54 time=54.1 ms  
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=8 ttl=54 time=52.4 ms  
64 bytes from 163.53.78.110 (163.53.78.110): icmp_seq=9 ttl=54 time=32.0 ms
```

Activities Wireshark Sep 26 19:15

Capturing from 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	78	Standard query 0x7e44 A www.flipkart.com
2	0.000168555	10.0.2.4	192.168.43.1	DNS	78	Standard query 0xca49 A www.flipkart.com
3	0.000695498	127.0.0.1	127.0.0.53	DNS	78	Standard query 0x7c40 AAAA www.flipkart.com
4	0.000863170	10.0.2.4	192.168.43.1	DNS	78	Standard query 0x8329 AAAA www.flipkart.com
5	0.006007912	192.168.43.1	10.0.2.4	DNS	237	Standard query response 0xca49 A www.flipkart.com CNAME flipk...
6	0.006282793	127.0.0.53	127.0.0.1	DNS	108	Standard query response 0x7e44 A www.flipkart.com CNAME flipk...
7	5.005026687	127.0.0.1	127.0.0.53	DNS	78	Standard query 0x7e44 A www.flipkart.com
8	5.005320062	127.0.0.53	127.0.0.1	DNS	108	Standard query response 0x7e44 A www.flipkart.com CNAME flipk...
9	5.005522418	10.0.2.4	192.168.43.1	DNS	74	Standard query 0x6140 AAAA flipkart.com
10	5.005800814	127.0.0.1	127.0.0.53	DNS	78	Standard query 0x7c40 AAAA www.flipkart.com

Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0

Linux cooked capture

Internet Protocol Version 4, Src: 10.0.2.4, Dst: 192.168.43.1

User Datagram Protocol, Src Port: 51487, Dst Port: 53

Domain Name System (query)

Transaction ID: 0xca49

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: 5]

0000 00 04 00 01 00 06 08 00 27 57 91 24 00 00 08 00 'W\$.
0010 45 00 00 3e 70 1b 40 00 40 11 d2 e6 0a 00 02 04 E->p @ @..
0020 c0 a8 2b 01 c9 1f 00 35 00 2a f7 e8 ca 49 01 005...I..
0030 00 01 00 00 00 00 00 03 77 77 77 08 66 6c 69www-fli
0040 70 6b 61 72 74 03 63 6f 6d 00 00 01 00 01pkart.co m...
Domain Name System (dns), 34 bytes

Packets: 50 · Displayed: 50 (100.0%) Profile: Default

Activities Wireshark Sep 26 19:18

Capturing from 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	5.000296947	127.0.0.53	127.0.0.1	DNS	92	Standard query response 0x7c40 AAAA www.flipkart.com CNAME fl...
6	0.006282793	127.0.0.53	127.0.0.1	DNS	108	Standard query response 0x7e44 A www.flipkart.com CNAME flipk...
8	5.005320062	127.0.0.53	127.0.0.1	DNS	108	Standard query response 0x7e44 A www.flipkart.com CNAME flipk...
20	5.138823840	192.168.43.1	10.0.2.4	DNS	88	Standard query response 0x96a4 No such name PTR 110.78.53.163...
59	22.612448851	192.168.43.1	10.0.2.4	DNS	91	Standard query response 0x98e3 AAAA connectivity-check.ubuntu...
5	0.006007912	192.168.43.1	10.0.2.4	DNS	237	Standard query response 0xca49 A www.flipkart.com CNAME flipk...

User Datagram Protocol, Src Port: 53, Dst Port: 51487

Domain Name System (response)

Transaction ID: 0xca49

Flags: 0x0180 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 4

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: 32 (32 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: 27 (27 seconds)

Data length: 4

Address: 163.53.78.110

Authoritative nameservers

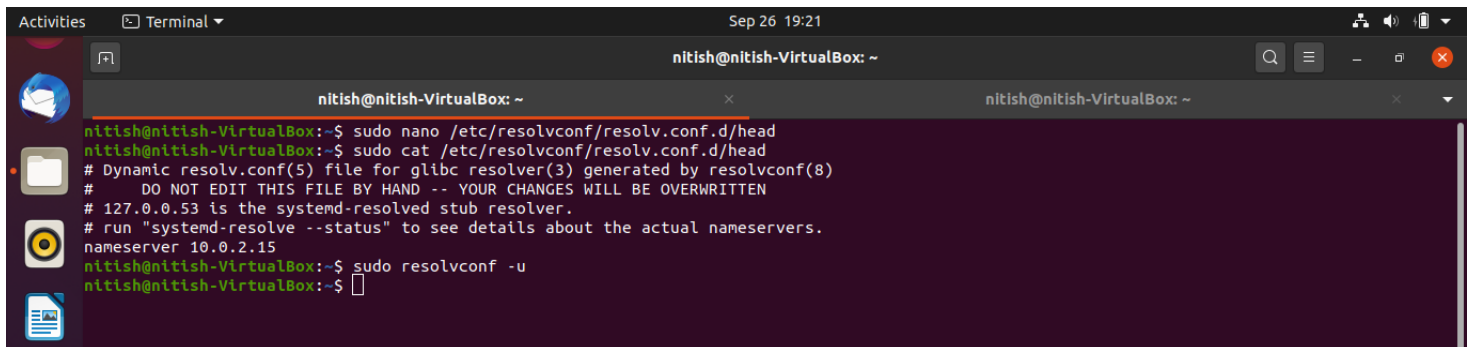
0020 0a 00 02 04 00 35 c9 1f 00 c9 f5 61 ca 49 81 805...aI..
Domain Name System (dns), 193 bytes

Packets: 407 · Displayed: 407 (100.0%) Profile: Default

Observations:-

- 1) First the source system (10.0.2.4) sends a query to the DNS server(192.168.43.55) requesting a type A RR (resource record) consisting of <hostname,IPv4>. It also sends a type AAAA RR requesting for <hostname,IPv6>.
- 2) The DNS server then responds with 3 Answer RR's, specifying the hostname and IPv4.

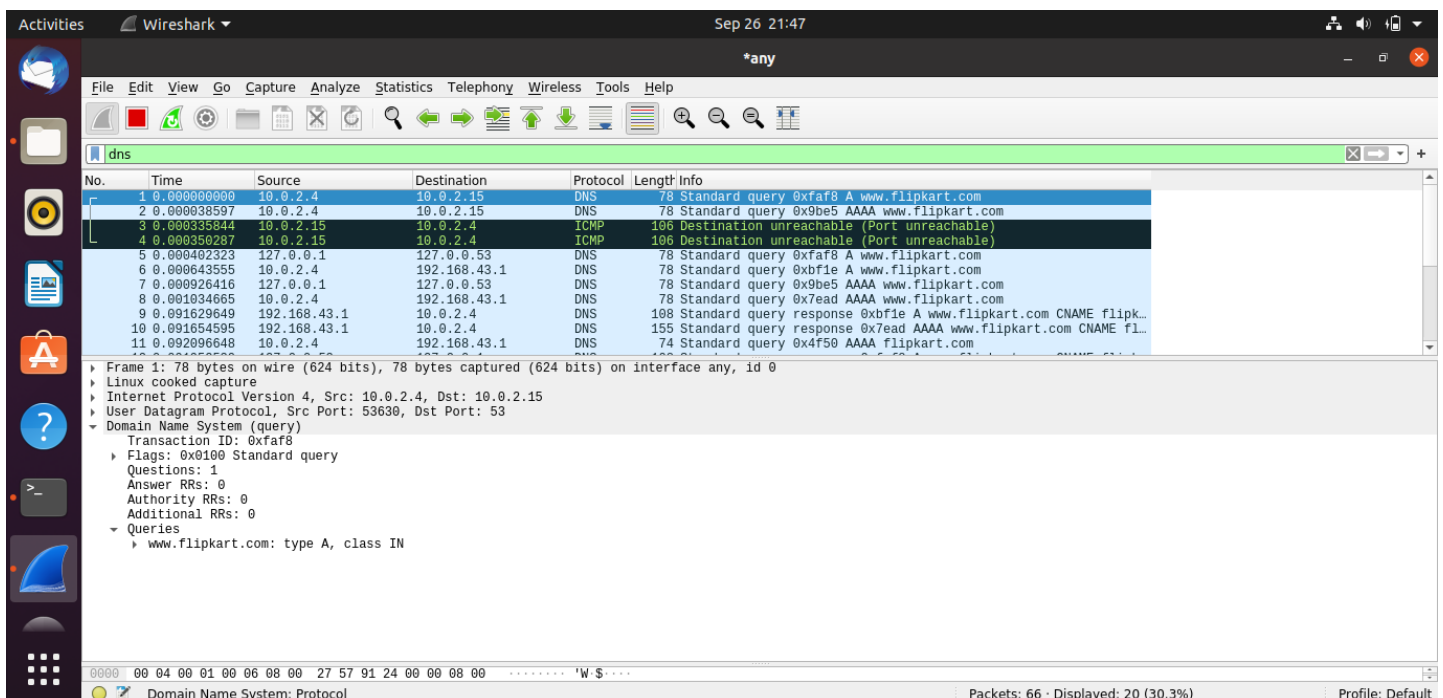
TASK – 1: CONFIGURE THE USER/CLIENT MACHINE:-



```
nitish@nitish-VirtualBox: ~  
nitish@nitish-VirtualBox:~$ sudo nano /etc/resolvconf/resolv.conf.d/head  
nitish@nitish-VirtualBox:~$ 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  
# 127.0.0.53 is the systemd-resolved stub resolver.  
# run "systemd-resolve --status" to see details about the actual nameservers.  
nameserver 10.0.2.15  
nitish@nitish-VirtualBox:~$ sudo resolvconf -u  
nitish@nitish-VirtualBox:~$
```

SECOND TEST:-

Ping a computer such as www.flipkart.com. Please use Wireshark to show the DNS query triggered by your ping command and DNS response. Describe your observation.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.4	10.0.2.15	DNS	78	Standard query 0xfa8 A www.flipkart.com
2	0.000000000	10.0.2.4	10.0.2.15	DNS	78	Standard query 0x9be5 AAAA www.flipkart.com
3	0.000000000	10.0.2.15	10.0.2.4	ICMP	108	Destination unreachable (Port unreachable)
4	0.000000000	10.0.2.15	10.0.2.4	ICMP	108	Destination unreachable (Port unreachable)
5	0.000000000	127.0.0.1	127.0.0.53	DNS	78	Standard query 0xfa8 A www.flipkart.com
6	0.000000000	10.0.2.4	192.168.43.1	DNS	78	Standard query 0xbfe A www.flipkart.com
7	0.000000000	127.0.0.1	127.0.0.53	DNS	78	Standard query 0x9be5 AAAA www.flipkart.com
8	0.000000000	10.0.2.4	192.168.43.1	DNS	78	Standard query 0x7ead AAAA www.flipkart.com
9	0.000000000	192.168.43.1	10.0.2.4	DNS	108	Standard query response 0xbfe A www.flipkart.com CNAME flipk...
10	0.000000000	192.168.43.1	10.0.2.4	DNS	155	Standard query response 0x7ead AAAA www.flipkart.com CNAME fl...
11	0.000000000	10.0.2.4	192.168.43.1	DNS	74	Standard query 0x4f50 AAAA flipkart.com

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53630, Dst Port: 53
Domain Name System (query)
Transaction ID: 0xfa8
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.flipkart.com: type A, class IN

Observations:-

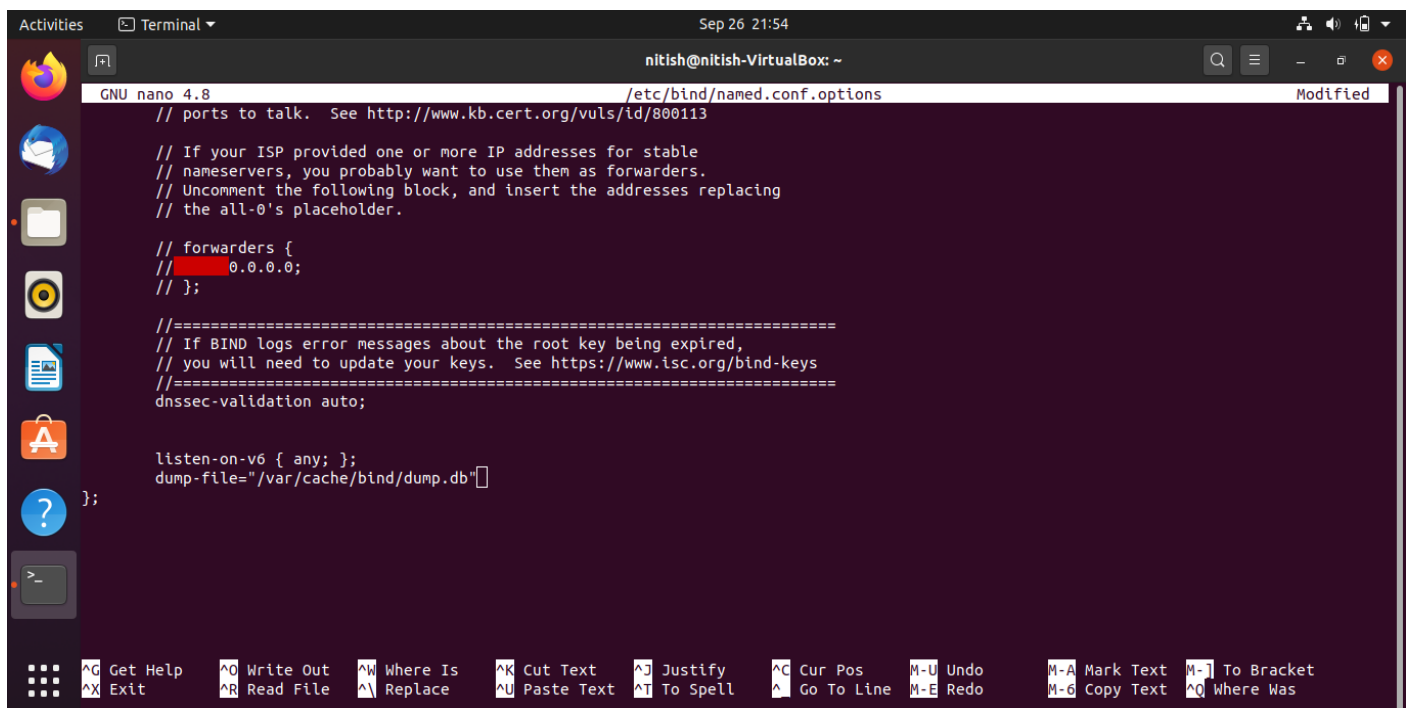
- 1) The DNS query is sent from the user(10.0.2.4) to the local DNS nameserver(10.0.2.15).
- 2) The response is not received from the local DNS server as it is still not configured to act as a DNS server. (Hence the 'destination unreachable' message is displayed in the WireShark capture.

TASK – 2: Set Up a Local DNS Server

\$ sudo apt-get update

\$ sudo apt-get install bind9

Step 1: Configure the BIND9 Server.



```
GNU nano 4.8 /etc/bind/named.conf.options Modified
// 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.

// forwarders {
//     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;

listen-on-v6 { any; };
dump-file="/var/cache/bind/dump.db";
};
```

Step 2: Start DNS server

We start the DNS server using the command:

\$ sudo service bind9 restart

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.

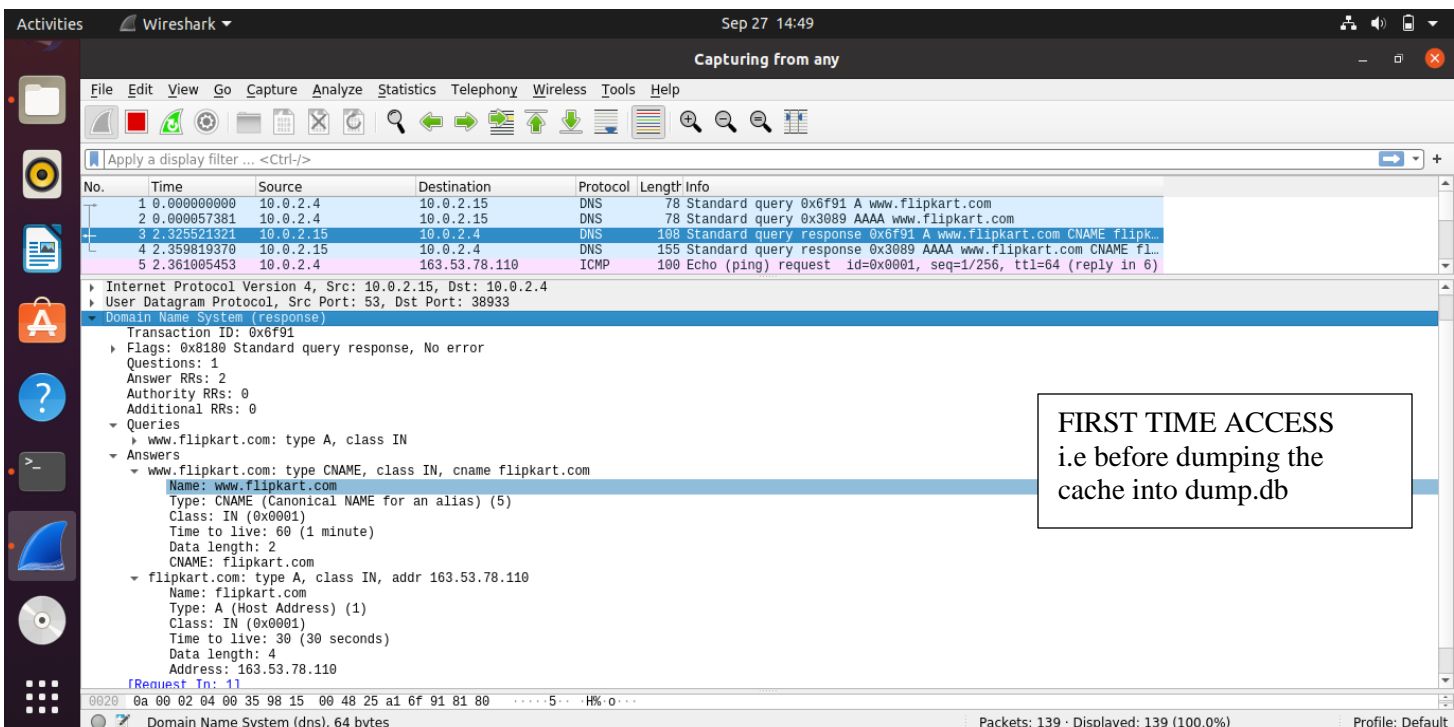
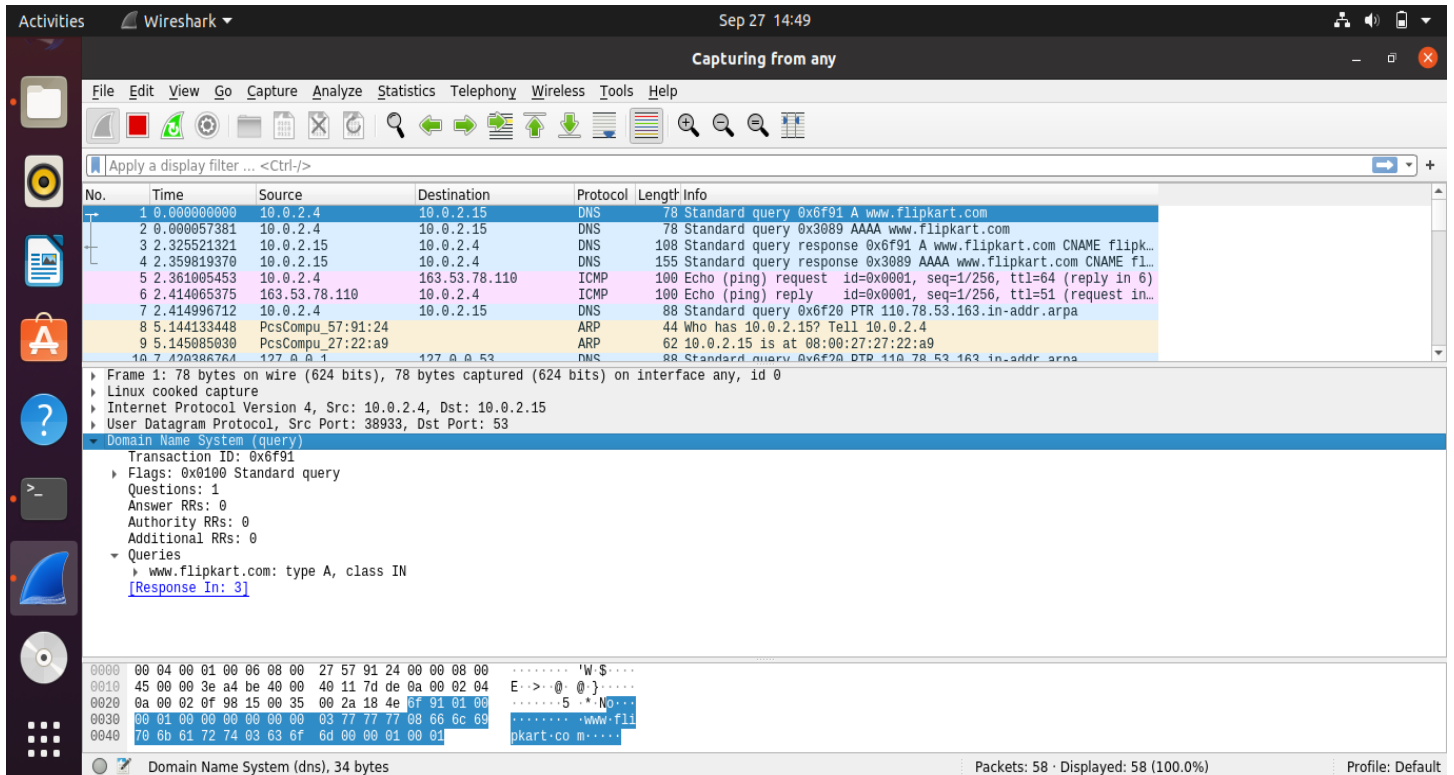
\$ sudo rndc dumpdb -cache

\$ sudo rndc flush

Step 3: Use the DNS server

Third Test:

In the user machine (10.0.2.4), and ping a computer such as www.flipkart.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)



Activities Wireshark Sep 27 20:39

Capturing from 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	10.0.2.4	10.0.2.15	DNS	78	Standard query 0xc6cc A www.flipkart.com
2	0.000042141	10.0.2.4	10.0.2.15	DNS	78	Standard query 0x4dc0 AAAA www.flipkart.com
3	0.257070976	10.0.2.15	10.0.2.4	DNS	108	Standard query response 0xc6cc A www.flipkart.com CNAME flipkart.c...
4	0.257129327	10.0.2.15	10.0.2.4	DNS	155	Standard query response 0x4dc0 AAAA www.flipkart.com CNAME flipkar...
5	0.257742545	10.0.2.4	163.53.78.110	ICMP	100	Echo (ping) request id=0x0002, seq=1/256, ttl=64 (reply in 6)
6	0.308919382	163.53.78.110	10.0.2.4	ICMP	100	Echo (ping) reply id=0x0002, seq=1/256, ttl=51 (request in 5)
7	0.309156085	10.0.2.4	10.0.2.15	DNS	88	Standard query 0x22dc PTR 110.78.53.163.in-addr.arpa
8	2.554429093	10.0.2.15	10.0.2.4	DNS	192	Standard query response 0x22dc No such name PTR 110.78.53.163.in-a...
9	2.554662135	10.0.2.4	163.53.78.110	ICMP	100	Echo (ping) request id=0x0002, seq=2/512, ttl=64 (reply in 10)
10	2.5885983761	163.53.78.110	10.0.2.4	ICMP	100	Echo (ping) reply id=0x0002, seq=2/512, ttl=51 (request in 9)
11	3.555416971	10.0.2.4	163.53.78.110	ICMP	100	Echo (ping) request id=0x0002, seq=3/768, ttl=64 (reply in 12)
12	3.610606003	163.53.78.110	10.0.2.4	ICMP	100	Echo (ping) reply id=0x0002, seq=3/768, ttl=51 (request in 11)

Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface any, id 0

Linux cooked capture

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.4

User Datagram Protocol, Src Port: 53, Dst Port: 42628

Domain Name System (response)

Transaction ID: 0xc6cc

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: 60 (1 minute)

Data length: 2

0000 00 00 00 01 00 06 00 00 27 27 22 a0 00 00 08 00 11.....

any: <live capture in progress>

Packets: 62 · Displayed: 62 (100.0%) Profile: Default

SECOND TIME ACCESS
i.e after dumping the cache
into dump.db

Activities Text Editor Sep 27 21:06

dump.db [Read-Only]

/var/cache/bind

```

318;
319; 199.9.14.201 [srvt 229332] [flags 00004000] [edns 1/0/0/0] [plain 0/0] [udpsize 512]
[cookie=d7218bd3b99051ca902f04265f707a99198c405fe037f4b5] [ttl 1039]
320; 192.55.83.30 [srvt 17] [flags 00000000] [edns 0/0/0/0] [plain 0/0] [ttl 1062]
321; 192.112.36.4 [srvt 19] [flags 00000000] [edns 0/0/0/0] [plain 0/0] [ttl 1039]
322; 192.5.6.30 [srvt 15] [flags 00000000] [edns 0/0/0/0] [plain 0/0] [ttl 1062]
323; 91.189.95.3 [srvt 373500] [flags 00000000] [edns 0/4/4/4/4] [plain 0/0] [ttl 1062]
324; 2001:500:1::53 [srvt 177663] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1039]
325; 91.189.94.173 [srvt 538785] [flags 00004000] [edns 3/4/4/4/4] [plain 0/0] [udpsize 512] [ttl 1062]
326; 199.7.83.42 [srvt 14] [flags 00000000] [edns 0/0/0/0] [plain 0/0] [ttl 1039]
327; 192.58.128.30 [srvt 26] [flags 00000000] [edns 0/0/0/0] [plain 0/0] [ttl 1039]
328; 192.26.92.30 [srvt 143529] [flags 00004000] [edns 1/0/0/0] [plain 0/0] [udpsize 512] [ttl 1062]
329; 202.12.27.33 [srvt 8] [flags 00000000] [edns 0/0/0/0] [plain 0/0] [ttl 1039]
330; 2001:503:39c1::30 [srvt 143126] [flags 00000000] [edns 0/1/1/1/1] [plain 0/0] [ttl 1062]
331; 2001:503:231d::2:30 [srvt 128483] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1062]
332; 198.41.0.4 [srvt 10] [flags 00000000] [edns 0/0/0/0] [plain 0/0] [ttl 1039]
333; 2001:503:eea3::30 [srvt 83975] [flags 00000000] [edns 0/1/1/1/1] [plain 0/0] [ttl 1062]
334; 2001:dc3::35 [srvt 79428] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1039]
335; 192.42.93.30 [srvt 6] [flags 00000000] [edns 0/0/0/0] [plain 0/0] [ttl 1062]
336; 2001:501:b1f9::30 [srvt 160624] [flags 00000000] [edns 0/1/1/1/1] [plain 0/0] [ttl 1062]
337; 192.203.230.10 [srvt 117030] [flags 00004000] [edns 2/0/0/0/0] [plain 0/0] [udpsize 512] [ttl 1039]
338; 2001:503:d2d::30 [srvt 161976] [flags 00000000] [edns 0/1/1/1/1] [plain 0/0] [ttl 1062]
339; 192.5.5.241 [srvt 16] [flags 00000000] [edns 0/0/0/0] [plain 0/0] [ttl 1039]
340; 2001:503:c27::2:30 [srvt 118824] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1039]
341; 2001:7fd::1 [srvt 68062] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1039]
342; 2001:500:2::c [srvt 79970] [flags 00000000] [edns 0/3/3/3/3] [plain 0/0] [ttl 1039]
343; 2001:7fe::53 [srvt 189696] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1039]
344; 192.36.148.17 [srvt 17] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1039]
345; 192.52.178.30 [srvt 289258] [flags 00004000] [edns 1/0/0/0/0] [plain 0/0] [udpsize 512] [ttl 1062]
346; 2001:503:83eb::30 [srvt 25864] [flags 00000000] [edns 0/1/1/1/1] [plain 0/0] [ttl 1062]
347; 192.12.94.30 [srvt 7] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1062]

```

OBSERVATIONS:-

1) The DNS query is sent from the client machine 10.0.2.4 to the local DNS server machine 10.0.2.15.

2) We can observe that when the ping command is done for the first time, the time taken to obtain the query response from 10.0.2.15 is **2.3255sec**.

But when the ping command is run from the second time, the time taken to obtain query response from 10.0.2.15 is **0.2570sec**.

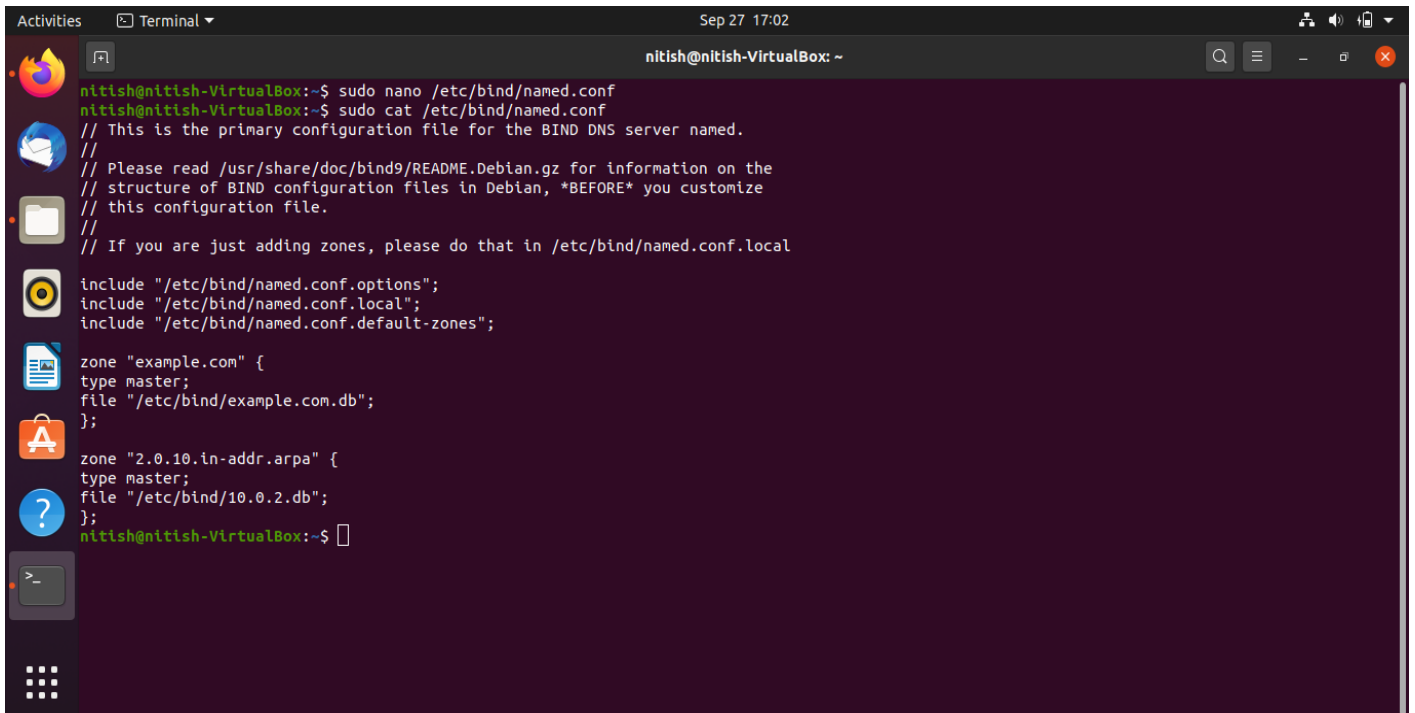
The time taken during the second time is less indicating that it is stored in the local cache of the local DNS server machine and hence faster response is obtained.

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

Assume that we own a domain, we will be responsible for providing the definitive answer regarding this domain. We will use our local DNS server as the authoritative nameserver for the domain. In this lab, we will set up an authoritative server for the **example.com** domain.

This domain name is reserved for use in documentation, and is not owned by anybody, so it is safe to use it.

Step 1: Create Zones



```
nitish@nitish-VirtualBox:~$ sudo nano /etc/bind/named.conf
nitish@nitish-VirtualBox:~$ sudo cat /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 "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/10.0.2.db";
};
nitish@nitish-VirtualBox:~$
```

Step 2: Setup the forward lookup zone file

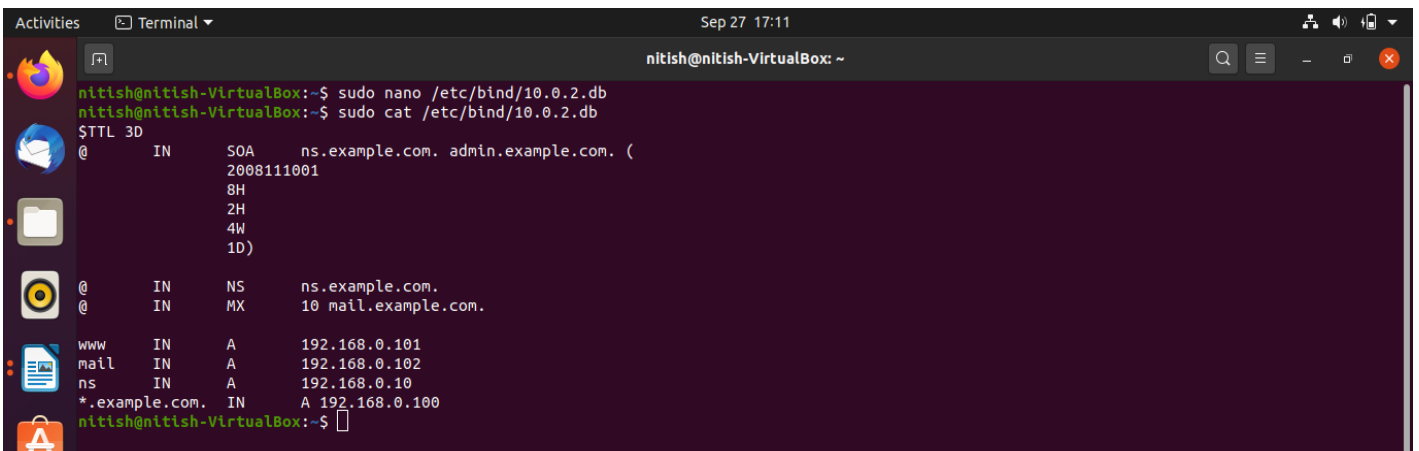


A terminal window titled 'nitish@nitish-VirtualBox: ~' showing the process of editing the forward lookup zone file. The user runs 'sudo nano /etc/bind/10.0.2.db' and then 'sudo cat /etc/bind/10.0.2.db' to display the contents of the file. The file contains DNS records for the example.com domain.

```
nitish@nitish-VirtualBox:~$ sudo nano /etc/bind/10.0.2.db
nitish@nitish-VirtualBox:~$ sudo cat /etc/bind/10.0.2.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       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
nitish@nitish-VirtualBox:~$
```

Step 3: Setup the reverse lookup zone file



A terminal window titled 'nitish@nitish-VirtualBox: ~' showing the process of editing the reverse lookup zone file. The user runs 'sudo nano /etc/bind/10.0.2.db' and then 'sudo cat /etc/bind/10.0.2.db' to display the contents of the file. The file contains DNS records for the example.com domain.

```
nitish@nitish-VirtualBox:~$ sudo nano /etc/bind/10.0.2.db
nitish@nitish-VirtualBox:~$ sudo cat /etc/bind/10.0.2.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       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
nitish@nitish-VirtualBox:~$
```

Task 4: Restart the BIND server and test

Step – 1:

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.


```
Activities Terminal Sep 27 17:12 nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox:~$ dig www.example.com
; <<> DiG 9.16.1-Ubuntu <<> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 61796
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 4096
;; COOKIE: 1669ee7686428f2c010000005f707aab264820bb7cb41e75 (good)
;; QUESTION SECTION:
;www.example.com.                IN      A
;; ANSWER SECTION:
www.example.com.                259200 IN      A      192.168.0.101
;; Query time: 0 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Sun Sep 27 17:12:35 IST 2020
;; MSG SIZE rcvd: 88
nitish@nitish-VirtualBox:~$
```

Step 2: Observe the results in Wireshark capture.

Activities Wireshark Sep 27 17:22

Capturing from any

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000136962	10.0.2.4	10.0.2.15	DNS	100	Standard query 0x1a3c A www.example.com OPT
4	0.048724125	10.0.2.15	10.0.2.4	DNS	132	Standard query response 0x1a3c A www.example.com A 192.168.0.101 0...

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: 10.0.2.15, Dst: 10.0.2.4

User Datagram Protocol, Src Port: 53, Dst Port: 57194

Domain Name System (response)

Transaction ID: 0x1a3c

Flags: 0x8580 Standard query response, No error

- 1... .. = Response: Message is a response
- .000 0... .. = Opcode: Standard query (0)
- 1... .. = Authoritative: Server is an authority for domain
- 0... .. = Truncated: Message is not truncated
- 1... .. = Recursion desired: Do query recursively
- 1... .. = Recursion available: Server can do recursive queries
- 0... .. = Z: reserved (0)
- 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
- 0... .. = Non-authenticated data: Unacceptable
- 0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 1

Queries

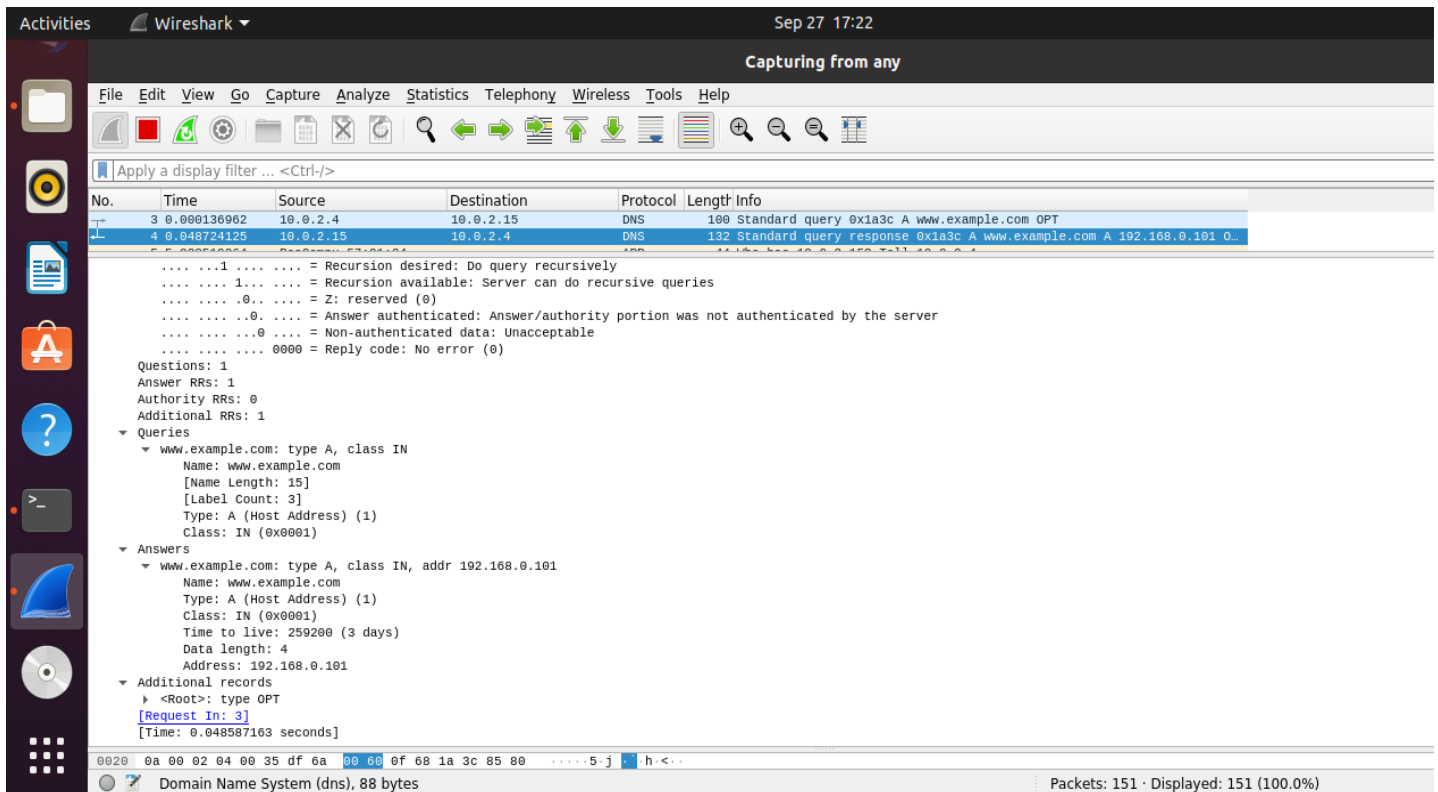
- www.example.com: type A, class IN
 - Name: www.example.com
 - [Name Length: 15]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

Answers

0020 0a 00 02 04 00 35 df 6a 00 60 0f 68 1a 3c 85 805.j...h<..

Domain Name System (dns), 88 bytes

Packets: 151 · Displayed: 151 (100.0%)



To load and clear DNS cache, use the below commands.

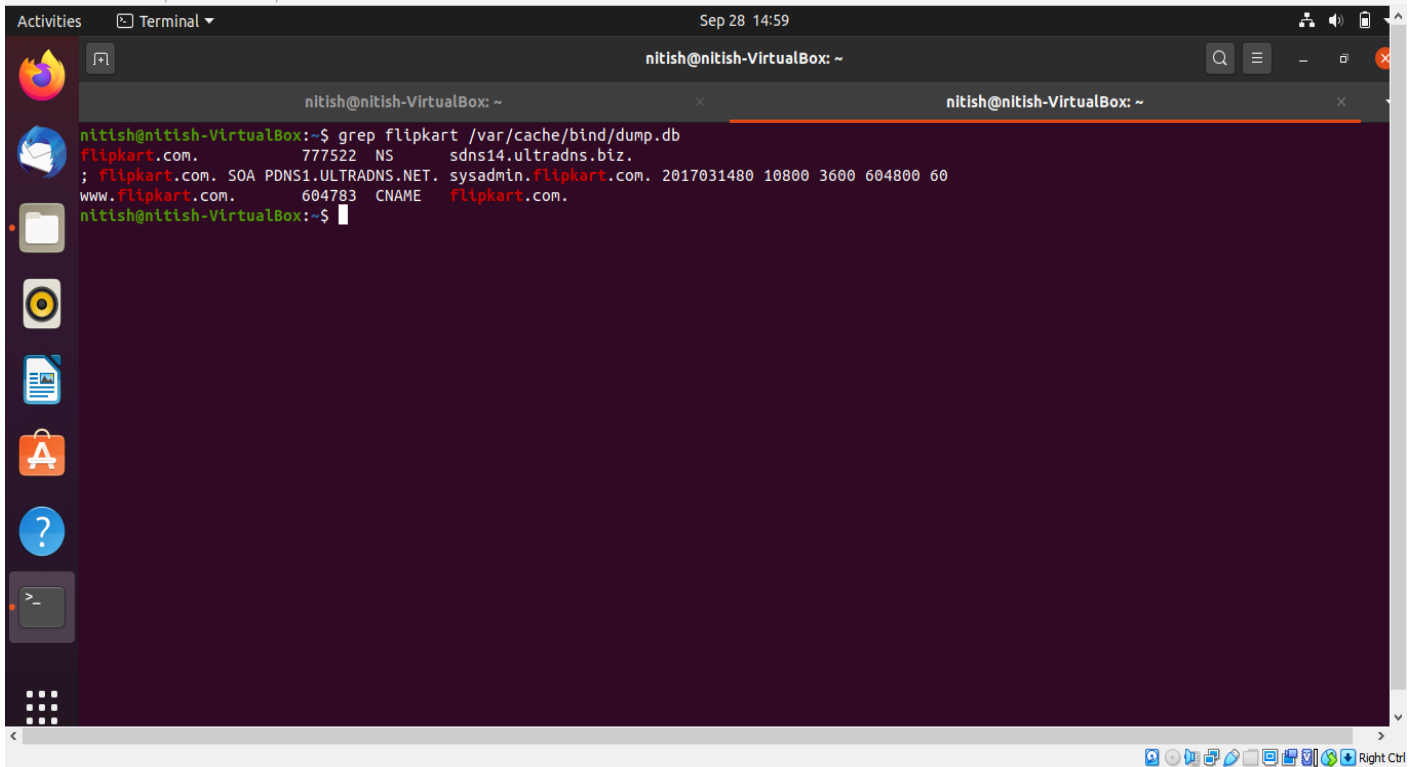
\$ sudo rndc dumpdb -cache

\$ sudo rndc flush

Local DNS Cache:-

```
Ubuntu 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Text Editor Sep 27 21:51
dump.db [Read-Only] /var/cache/bind
1;
2; Start view _default
3;
4;
5; Cache dump of view '_default' (cache _default)
6;
7; using a 604800 second stale ttl
8 $DATE 20200920115436
9; secure
10 . 1122439 IN NS a.root-servers.net.
11 1122439 IN NS b.root-servers.net.
12 1122439 IN NS c.root-servers.net.
13 1122439 IN NS d.root-servers.net.
14 1122439 IN NS e.root-servers.net.
15 1122439 IN NS f.root-servers.net.
16 1122439 IN NS g.root-servers.net.
17 1122439 IN NS h.root-servers.net.
18 1122439 IN NS i.root-servers.net.
19 1122439 IN NS j.root-servers.net.
20 1122439 IN NS k.root-servers.net.
21 1122439 IN NS l.root-servers.net.
22 1122439 IN NS m.root-servers.net.
23; secure
24 1122439 RRSIG NS 8 0 518400 (
25 20201010050000 20200927040000 46594 .
26 jVDplmTKbR3iNeIGBBFCwamSzY3F61exMJ
27 PoFpXiFOVhNcY8V5DBBQydvuPJ03WUK9mBI
28 iL09I1CVhyTUD1pkxEfmEtvTHYUSeUKNJgaf
29 7w6S/rtrUsRVhsnJHpb8Mu3d/GW4g3HCW7fm
30 +o/8B2P1klpL+urHKJVjOpZG7e1YEQ6PCGB
31 DLS3lsgvBAYZbLHctVQHbQ2Y10GKd6sJR0aY
32 kZ7T3g0c0d0Cn3u01a0E5F570u0V00167
```

```
Ubuntu 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Text Editor Sep 27 21:06
dump.db [Read-Only] /var/cache/bind
318;
319 199.9.14.201 [srtt 229332] [flags 00004000] [edns 1/0/0/0/0] [plain 0/0] [udp size 512]
[cookie=d7218bd3b99051ca902f04265f707a99198c405fe037f4b5] [ttl 1039]
320 192.55.83.30 [srtt 17] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1062]
321 192.112.36.4 [srtt 19] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1039]
322 192.5.6.30 [srtt 15] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1062]
323 91.189.95.3 [srtt 373500] [flags 00000000] [edns 0/4/4/4/4] [plain 0/0] [ttl 1062]
324 2001:500:1::53 [srtt 177663] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1039]
325 91.189.94.173 [srtt 538785] [flags 00004000] [edns 3/4/4/4/4] [plain 0/0] [udp size 512] [ttl 1062]
326 199.7.83.42 [srtt 14] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1039]
327 192.58.128.30 [srtt 26] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1039]
328 192.26.92.30 [srtt 143529] [flags 00004000] [edns 1/0/0/0/0] [plain 0/0] [udp size 512] [ttl 1062]
329 202.12.27.33 [srtt 8] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1039]
330 2001:503:39c1::30 [srtt 143126] [flags 00000000] [edns 0/1/1/1/1] [plain 0/0] [ttl 1062]
331 2001:503:231d::2:30 [srtt 128483] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1062]
332 198.41.0.4 [srtt 10] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1039]
333 2001:503:eea3::30 [srtt 83975] [flags 00000000] [edns 0/1/1/1/1] [plain 0/0] [ttl 1062]
334 2001:dc3::35 [srtt 79428] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1039]
335 192.42.93.30 [srtt 6] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1062]
336 2001:501:b1f9::30 [srtt 160624] [flags 00000000] [edns 0/1/1/1/1] [plain 0/0] [ttl 1062]
337 192.203.230.10 [srtt 117030] [flags 00004000] [edns 2/0/0/0/0] [plain 0/0] [udp size 512] [ttl 1039]
338 2001:503:d2d::30 [srtt 161976] [flags 00000000] [edns 0/1/1/1/1] [plain 0/0] [ttl 1062]
339 192.5.5.241 [srtt 16] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1039]
340 2001:503:c27::2:30 [srtt 118824] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1039]
341 2001:7fd::1 [srtt 68062] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1039]
342 2001:500:2::c [srtt 79970] [flags 00000000] [edns 0/3/3/3/3] [plain 0/0] [ttl 1039]
343 2001:7fe::53 [srtt 189696] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1039]
344 192.36.148.17 [srtt 17] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1039]
345 192.52.178.30 [srtt 289258] [flags 00004000] [edns 1/0/0/0/0] [plain 0/0] [udp size 512] [ttl 1062]
346 2001:503:83eb::30 [srtt 255864] [flags 00000000] [edns 0/1/1/1/1] [plain 0/0] [ttl 1062]
347 192.12.94.30 [srtt 7] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1062]
```



The screenshot shows a terminal window titled 'nitish@nitish-VirtualBox: ~' with a dark purple background. The command `grep flipkart /var/cache/bind/dump.db` has been executed, resulting in the following output:

```
nitish@nitish-VirtualBox:~$ grep flipkart /var/cache/bind/dump.db
flipkart.com. 777522 NS sdns14.ultradns.biz.
; flipkart.com. SOA PDNS1.ULTRADNS.NET. sysadmin.flipkart.com. 2017031480 10800 3600 604800 60
www.flipkart.com. 604783 CNAME flipkart.com.
nitish@nitish-VirtualBox:~$
```

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?

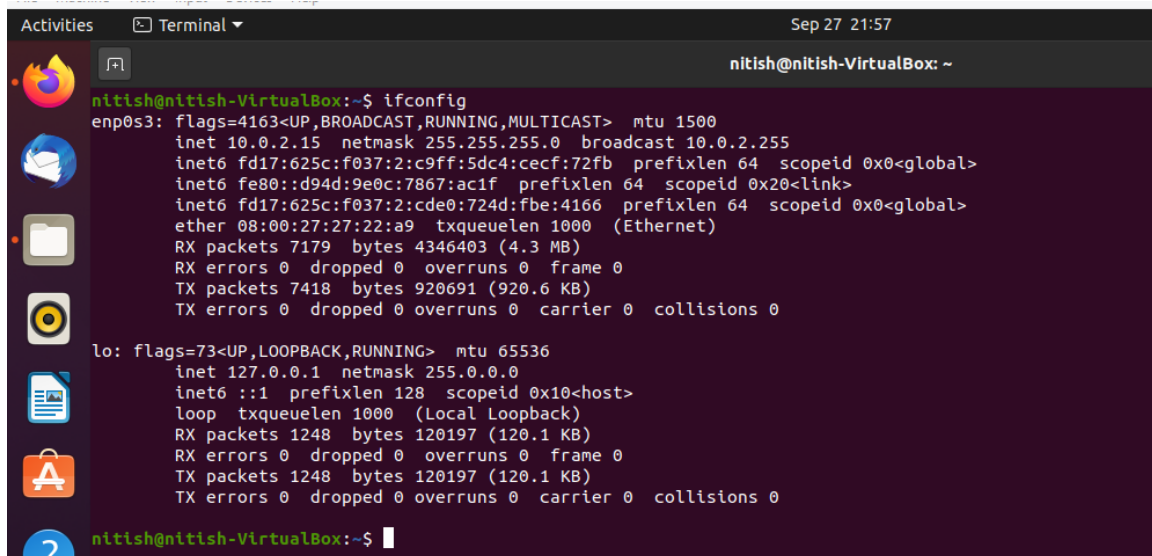
Ans:- The DNS query and response messages are shown above. They are sent over UDP.

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

Ans:- The destination port of the DNS query message is 53. The source port of DNS response message is also 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?

Ans:- The DNS query message is sent to 10.0.2.15. The IPv4 of the DNS server is also 10.0.2.15. Both are the same.



```
nitish@nitish-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fd17:625c:f037:2:c9ff:5dc4:cecf:72fb prefixlen 64 scopeid 0x0<global>
    inet6 fe80::d94d:9e0c:7867:ac1f prefixlen 64 scopeid 0x20<link>
    inet6 fd17:625c:f037:2:cde0:724d:fbe:4166 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:27:22:a9 txqueuelen 1000 (Ethernet)
    RX packets 7179 bytes 4346403 (4.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7418 bytes 920691 (920.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1248 bytes 120197 (120.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1248 bytes 120197 (120.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

nitish@nitish-VirtualBox:~$
```

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

Ans:- The type of DNS query message is **A (for IPv4)** and in some cases **AAAA (for IPv6)** too. The query message does not contain any **Answer RR** 's.

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

Ans:- The number of Answer RR's depends on the particular website.

Each one contains Name, Type, Class, TTL, Data length, 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:- No, the destination IP addresses does not match with any of our IP addresses from DNS response message.