

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

PES1201800410 sem V roll no 24 Prashanth A R

DNS server : 10.0.7.4

Client:10.0.7.5

First Test :

```
/bin/bash
PES1201800410@10.0.7.24-client:~$
PES1201800410@10.0.7.24-client:~$ ping www.flipkart.com
PING flipkart.com (163.53.76.86) 56(84) bytes of data:
64 bytes from 163.53.76.86: icmp_seq=1 ttl=57 time=33.7 ms
64 bytes from 163.53.76.86: icmp_seq=2 ttl=57 time=146 ms
64 bytes from 163.53.76.86: icmp_seq=3 ttl=57 time=31.4 ms
64 bytes from 163.53.76.86: icmp_seq=4 ttl=57 time=33.8 ms
64 bytes from 163.53.76.86: icmp_seq=5 ttl=57 time=173 ms
64 bytes from 163.53.76.86: icmp_seq=6 ttl=57 time=89.5 ms
64 bytes from 163.53.76.86: icmp_seq=7 ttl=57 time=32.2 ms
64 bytes from 163.53.76.86: icmp_seq=8 ttl=57 time=32.0 ms
64 bytes from 163.53.76.86: icmp_seq=9 ttl=57 time=34.8 ms
64 bytes from 163.53.76.86: icmp_seq=10 ttl=57 time=75.3 ms
64 bytes from 163.53.76.86: icmp_seq=11 ttl=57 time=33.3 ms
64 bytes from 163.53.76.86: icmp_seq=12 ttl=57 time=48.7 ms
64 bytes from 163.53.76.86: icmp_seq=13 ttl=57 time=34.2 ms
64 bytes from 163.53.76.86: icmp_seq=14 ttl=57 time=39.6 ms
64 bytes from 163.53.76.86: icmp_seq=15 ttl=57 time=40.5 ms
64 bytes from 163.53.76.86: icmp_seq=16 ttl=57 time=33.7 ms
64 bytes from 163.53.76.86: icmp_seq=17 ttl=57 time=33.6 ms
64 bytes from 163.53.76.86: icmp_seq=18 ttl=57 time=137 ms
64 bytes from 163.53.76.86: icmp_seq=19 ttl=57 time=41.4 ms
64 bytes from 163.53.76.86: icmp_seq=20 ttl=57 time=43.5 ms
64 bytes from 163.53.76.86: icmp_seq=21 ttl=57 time=35.4 ms
64 bytes from 163.53.76.86: icmp_seq=22 ttl=57 time=32.7 ms
64 bytes from 163.53.76.86: icmp_seq=23 ttl=57 time=31.5 ms
64 bytes from 163.53.76.86: icmp_seq=24 ttl=57 time=32.2 ms
64 bytes from 163.53.76.86: icmp_seq=25 ttl=57 time=33.7 ms
64 bytes from 163.53.76.86: icmp_seq=26 ttl=57 time=32.8 ms
64 bytes from 163.53.76.86: icmp_seq=27 ttl=57 time=33.3 ms
64 bytes from 163.53.76.86: icmp_seq=28 ttl=57 time=96.9 ms
64 bytes from 163.53.76.86: icmp_seq=29 ttl=57 time=96.1 ms
[0] 0: [tmux] *
```

Wireshark output

any

dns

No.	Time	Source	Destination	Protocol	Length	Info
14	128.155882818	127.0.0.1	127.0.1.1	DNS	78	Standard query 0xeb1 A www.flipkart.com
15	128.156206901	10.0.7.5	192.168.43.1	DNS	78	Standard query 0x6cae A www.flipkart.com
16	128.188788936	192.168.43.1	10.0.7.5	DNS	108	Standard query response 0x6cae A www.flipkart.com CNAME flipkart.com A 163.53.76.86
17	128.189055130	127.0.1.1	127.0.0.1	DNS	108	Standard query response 0xeb1 A www.flipkart.com CNAME flipkart.com A 163.53.76.86
20	128.225050424	127.0.0.1	127.0.1.1	DNS	87	Standard query 0xb960 PTR 86.76.53.163.in-addr.arpa
21	128.225155884	10.0.7.5	192.168.43.1	DNS	87	Standard query 0xe54a PTR 86.76.53.163.in-addr.arpa
22	128.245031988	192.168.43.1	10.0.7.5	DNS	175	Standard query response 0xe54a No such name PTR 86.76.53.163.in-addr.arpa SOA ns.apnic.net
23	128.245105708	127.0.1.1	127.0.0.1	DNS	175	Standard query response 0xb960 No such name PTR 86.76.53.163.in-addr.arpa SOA ns.apnic.net

Frame 14: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0

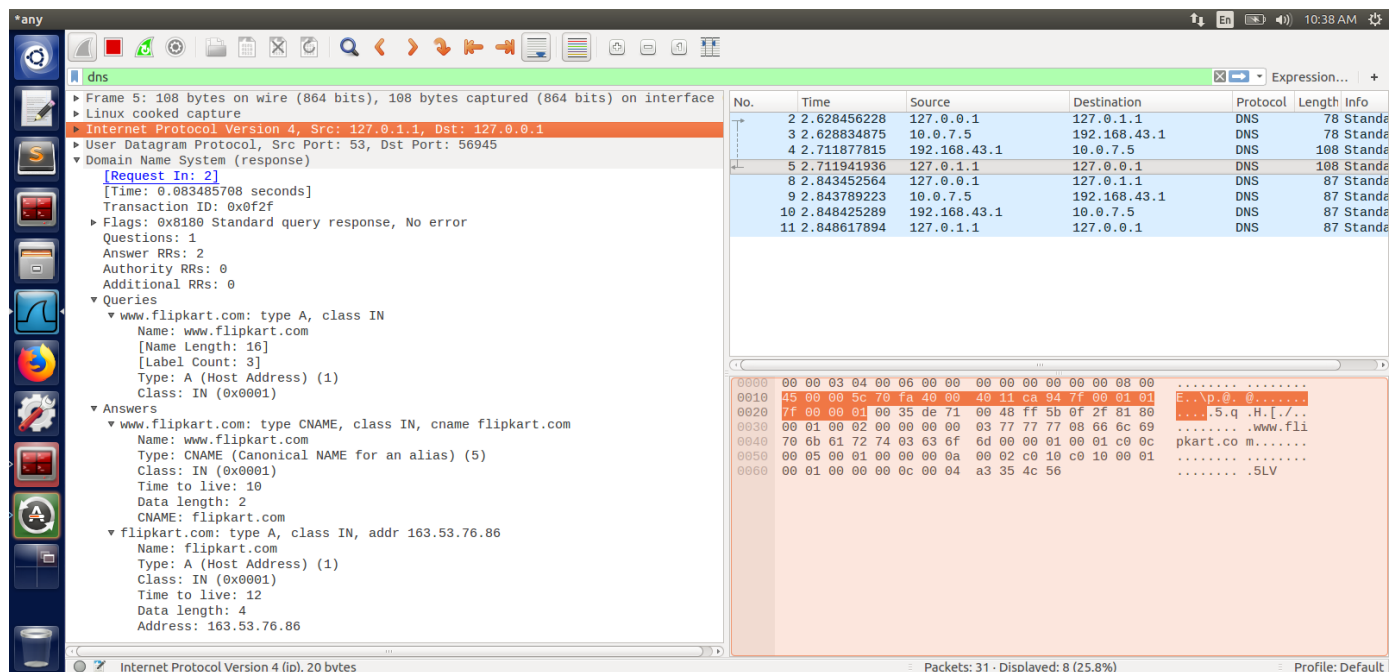
- Linux cooked capture
- Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.1.1
- User Datagram Protocol, Src Port: 43949, Dst Port: 53
- Domain Name System (query)

0000 00 00 03 04 00 06 00 00 00 00 00 00 00 08 00 .....  
0010 45 00 00 3e 05 49 40 00 40 11 36 64 7f 00 00 01 E..>.I@. @.6d...  
0020 7f 00 01 01 ab ad 00 35 00 2a ff 3d 0e b1 01 00 .....5 .\*.=-....  
0030 00 01 00 00 00 00 00 00 03 77 77 77 08 66 6c 69 .....www.fli  
0040 70 6b 61 72 74 03 63 6f 6d 00 00 01 00 01 .....pkart.co m.....

Domain Name System: Protocol

Packets: 86 - Displayed: 8 (9.3%)

Profile: Default

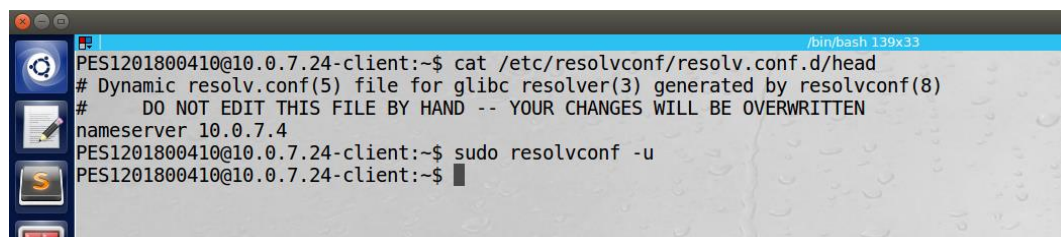


## Description:

1<sup>st</sup> it searches the its local dns server which is 127.0.0.1 .

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

## Setup for second test:



## Second Test:

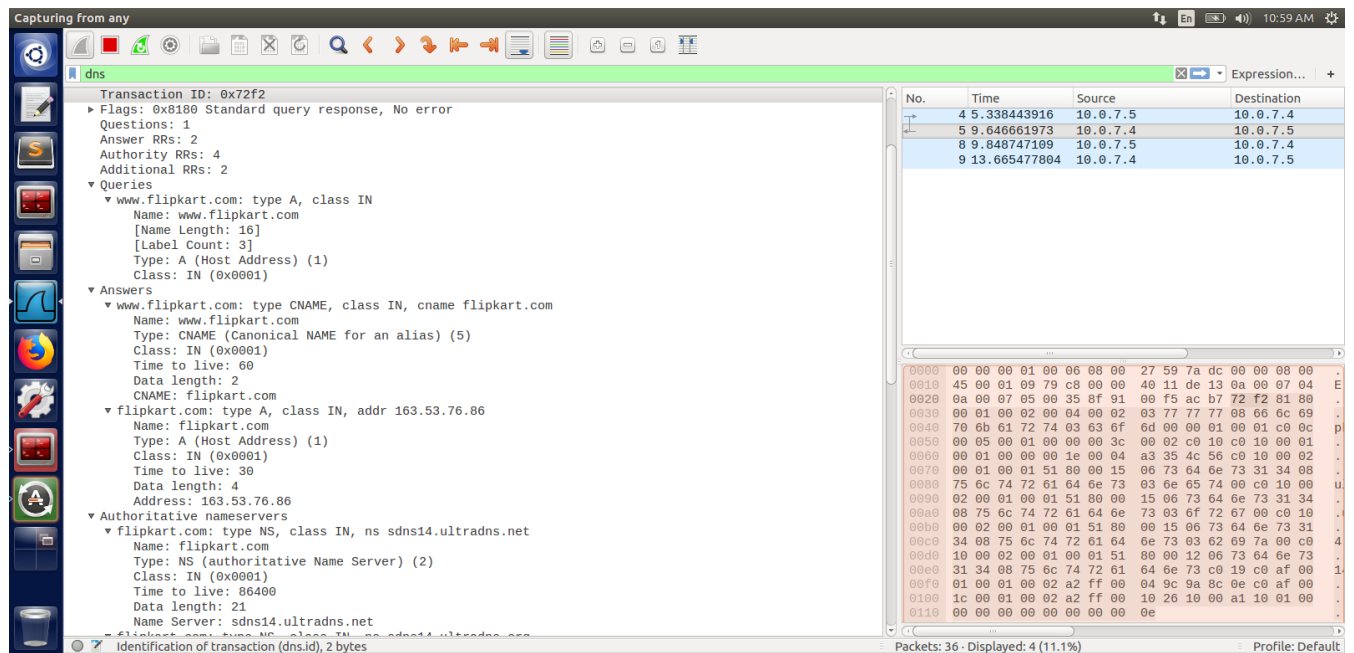
```
/bin/bash
PES1201800410@10.0.7.24-client:~$ ping www.flipkart.com
PING flipkart.com (163.53.76.86) 56(84) bytes of data.
64 bytes from 163.53.76.86: icmp_seq=1 ttl=57 time=201 ms
64 bytes from 163.53.76.86: icmp_seq=2 ttl=57 time=47.7 ms
64 bytes from 163.53.76.86: icmp_seq=3 ttl=57 time=45.6 ms
64 bytes from 163.53.76.86: icmp_seq=4 ttl=57 time=58.1 ms
64 bytes from 163.53.76.86: icmp_seq=5 ttl=57 time=55.4 ms
64 bytes from 163.53.76.86: icmp_seq=6 ttl=57 time=49.4 ms
64 bytes from 163.53.76.86: icmp_seq=7 ttl=57 time=36.5 ms
^C
--- flipkart.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 9029ms
rtt min/avg/max/mdev = 36.552/70.626/201.328/53.750 ms
PES1201800410@10.0.7.24-client:~$
```

## Wireshark output

The image shows a Wireshark capture of network traffic. The top pane displays a list of captured packets, with the first four packets selected. These packets are DNS-related: a standard query (No. 4), a standard query response (No. 5), another standard query (No. 8), and another standard query response (No. 9). The bottom pane shows the packet details for the selected packet (No. 4), which is a DNS standard query. The packet structure is shown in hexadecimal and ASCII, with the query name 'www.flipkart.com' visible in the ASCII column.

No.	Time	Source	Destination	Protocol	Length	Info
4	5.338443916	10.0.7.5	10.0.7.4	DNS	78	Standard query 0x72f2 A www.flipkart.com
5	9.646661973	10.0.7.4	10.0.7.5	DNS	281	Standard query response 0x72f2 A www.flipkart.com CNAME flipkart.com A 163.53.76.86 NS sd...
8	9.848747189	10.0.7.5	10.0.7.4	DNS	87	Standard query 0x8bbb PTR 86.76.53.163.in-addr.arpa
9	13.665477884	10.0.7.4	10.0.7.5	DNS	175	Standard query response 0x8bbb No such name PTR 86.76.53.163.in-addr.arpa SOA ns.apnic.net

Packet 4 details (hex):  
0000 00 64 00 01 00 06 08 00 27 11 b4 20 00 00 08 00 .....  
0010 45 00 00 3e 42 31 40 00 40 11 d6 75 0a 00 07 05 E..>B1@. @..u....  
0020 0a 00 07 04 8f 91 00 35 00 2a 22 44 72 f2 01 00 .....5 \*"D...  
0030 00 01 00 00 00 00 00 00 03 77 77 08 66 6c 69 .....www.fli  
0040 70 6b 61 72 74 03 63 6f 6d 00 00 01 00 01 pkart.co m.....

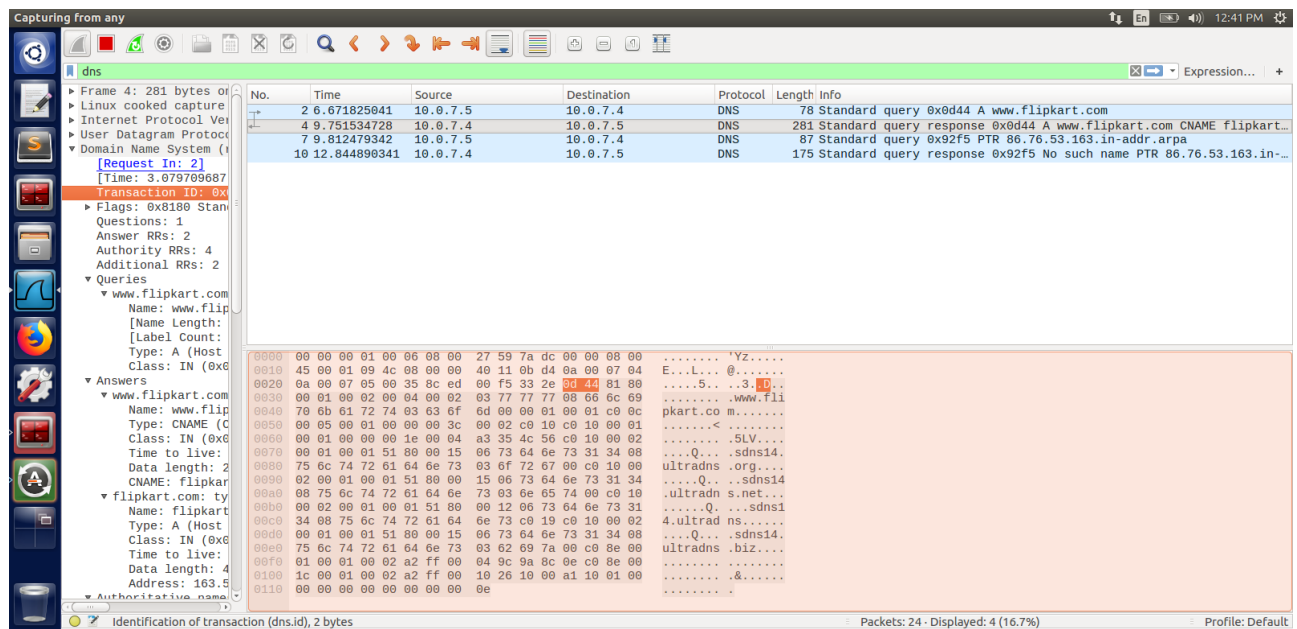


Observation:

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

Now VM 10.0.7.4 is acting as dns server for 10.0.7.5

3<sup>rd</sup> Test:





Capturing from any

dns

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
  - 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: 30
  - Data length: 4
  - Address: 163.53.76.86
- Authoritative nameservers
  - flipkart.com: type NS, class IN, ns sdns14.ultradns.org
    - Name: flipkart.com
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 86400
    - Data length: 21
    - Name Server: sdns14.ultradns.org
  - flipkart.com: type NS, class IN, ns sdns14.ultradns.net
    - Name: flipkart.com
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 86400
    - Data length: 21
    - Name Server: sdns14.ultradns.net
  - flipkart.com: type NS, class IN, ns sdns14.ultradns.com
    - Name: flipkart.com
    - Type: NS (authoritative Name Server) (2)
    - Class: IN (0x0001)
    - Time to live: 86400
    - Data length: 18

Response Length (dns.resp.len), 2 bytes

Packets: 27 - Displayed: 4 (14.8%)

Profile: Default

No.	Time	Source	Destination
2	6.671825041	10.0.7.5	10.0.7.4
4	9.751534728	10.0.7.4	10.0.7.5
7	9.812479342	10.0.7.5	10.0.7.4
10	12.844898341	10.0.7.4	10.0.7.5

## Setting up DNS server:

```

/bin/bash
PES1201800410@10.0.7.24-server:~$ cat /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.

    // 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;  

    // dnssec-enable no;  

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

    // auth-nxdomain no;    # conform to RFC1035

    // query-source port    33333;  

    // listen-on-v6 { any; };
};
PES1201800410@10.0.7.24-server:~$
  
```

VM 11:59:29 Sep-28

```
named.conf (/etc/bind) - gedit
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "example.com" {
    type master;
    file "/var/cache/bind/example.com.db";
};

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

Dig [www.example.com](http://www.example.com)

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

;<>> DiG 9.10.3-P4-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 18758
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.                IN      A

;; ANSWER SECTION:
www.example.com.                259200  IN      A      10.0.7.101

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

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

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

PES1201800410@10.0.7.24-client:~$
```

## wireshark output

The screenshot shows the Wireshark interface with a packet capture of a DNS query and response. The packet list on the left shows 11 packets. The selected packet (No. 4) is a DNS Standard query response from 10.0.7.4 to 10.0.7.5. The packet details pane on the right shows the response structure, including the question section (www.example.com) and the answer section (www.example.com type A, class IN, address 10.0.7.101). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	:::1	:::1	UDP	64	38293 → 49230 Len=0
2	3.333813916	:::1	:::1	UDP	65	33088 → 33088 Len=1
3	3.333931350	10.0.7.5	10.0.7.4	DNS	88	Standard query 0xd308 A www.example.com OPT
4	3.335023730	10.0.7.4	10.0.7.5	DNS	137	Standard query response 0xd308 A www.example.com A 10.0.7.101 NS ns.example.com
5	8.516131037	PcsCompu_11:b4:20		ARP	44	Who has 10.0.7.4? Tell 10.0.7.5
6	8.516931064	PcsCompu_59:7a:dc		ARP	62	10.0.7.4 is at 08:00:27:59:7a:dc
7	9.929267131	10.0.7.5	10.0.7.3	DHCP	344	DHCP Request - Transaction ID 0x73dd0c2f
8	9.950486389	10.0.7.3	10.0.7.5	DHCP	592	DHCP ACK - Transaction ID 0x73dd0c2f
9	15.166835956	PcsCompu_11:b4:20		ARP	44	Who has 10.0.7.3? Tell 10.0.7.5
10	15.167296768	PcsCompu_da:56:0d		ARP	62	10.0.7.3 is at 08:00:27:da:56:0d
11	20.012744675	:::1	:::1	UDP	64	38293 → 49230 Len=0

The screenshot shows the Wireshark interface with a packet capture of a DNS query and response. The packet list on the left shows 11 packets. The selected packet (No. 4) is a DNS Standard query response from 10.0.7.4 to 10.0.7.5. The packet details pane on the right shows the response structure, including the question section (www.example.com) and the answer section (www.example.com type A, class IN, address 10.0.7.101). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination
1	0.000000000	:::1	:::1
2	3.333813916	:::1	:::1
3	3.333931350	10.0.7.5	10.0.7.4
4	3.335023730	10.0.7.4	10.0.7.5
5	8.516131037	PcsCompu_11:b4:20	
6	8.516931064	PcsCompu_59:7a:dc	
7	9.929267131	10.0.7.5	10.0.7.3
8	9.950486389	10.0.7.3	10.0.7.5
9	15.166835956	PcsCompu_11:b4:20	
10	15.167296768	PcsCompu_da:56:0d	
11	20.012744675	:::1	:::1

## Observation Notebook Requirements:

For 'ping www.flipkart.com', answer the following questions

1) Locate the DNS query and response messages. Are they sent over UDP or TCP?

Ans : UDP

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

Ans : port 53 for both questions

3) To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

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

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

Ans: type: A, it didn't contain any answer.

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

Ans: I got 2 answers

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



6) Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

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