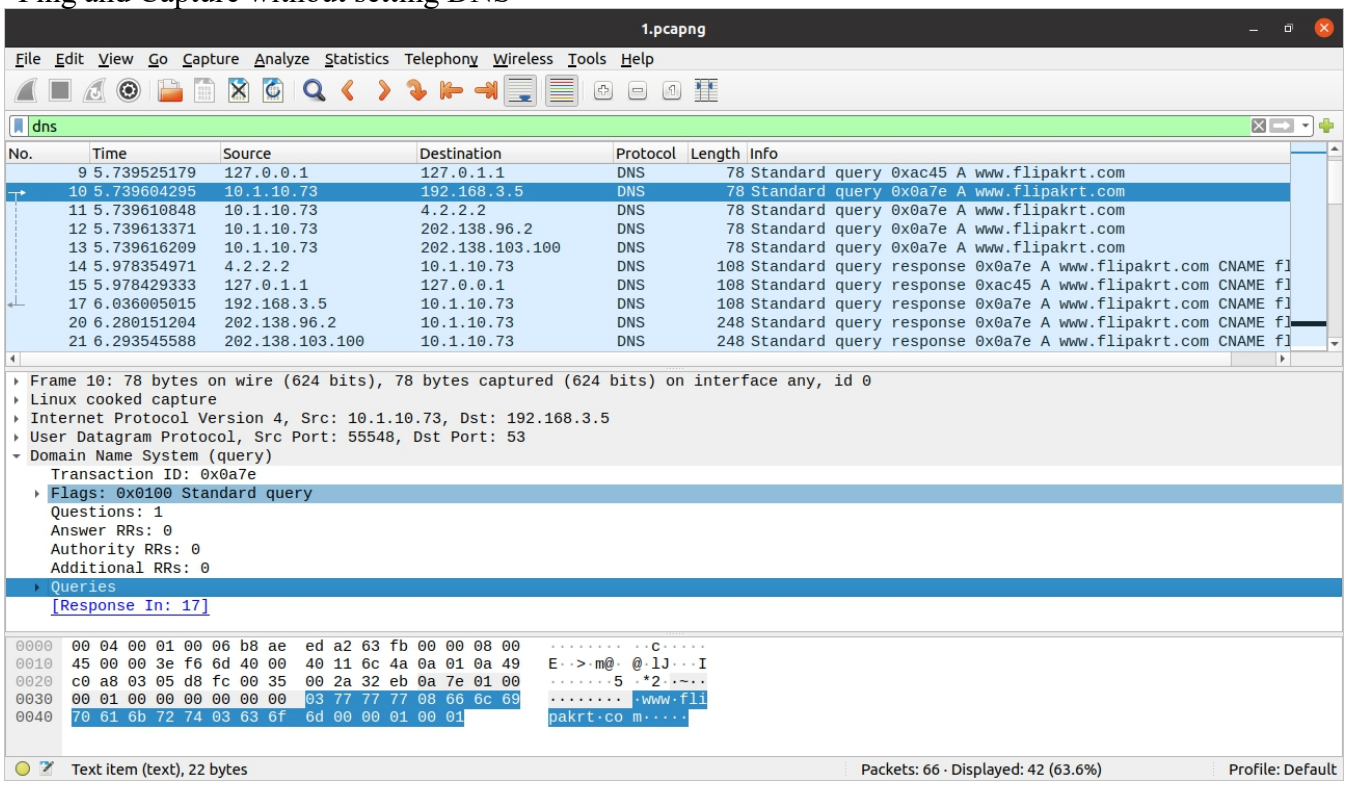
PES1UG20CS821

Nikhil T M

Week-4 Implementation of a Local DNS Server

Ping and Capture without setting DNS



Part 1: Setting Up a Local DNS Server

Task 1: Configure the User Machine

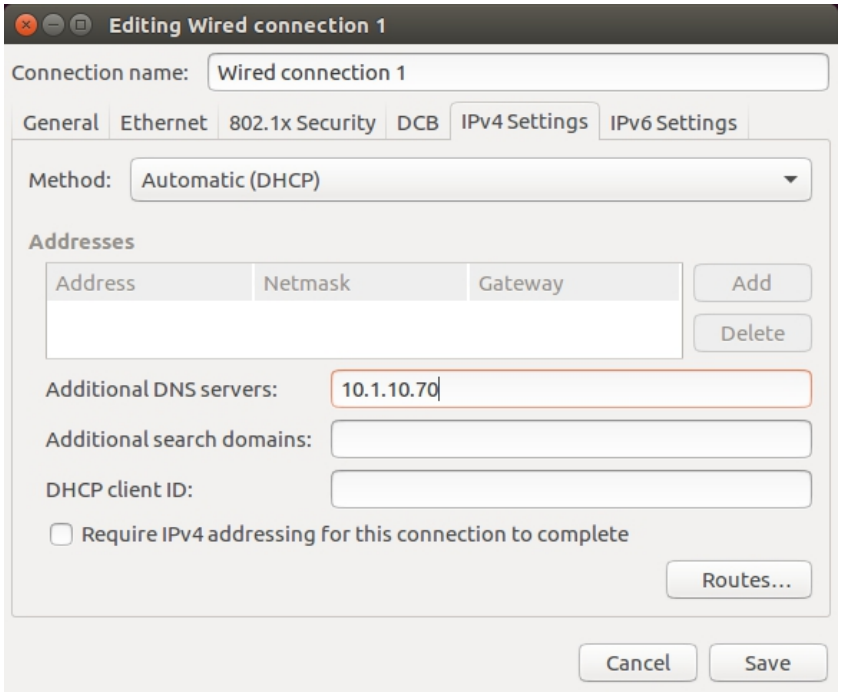
/etc/resolvconf/resolv.conf.d/head file.

nameserver 10.2.22.184

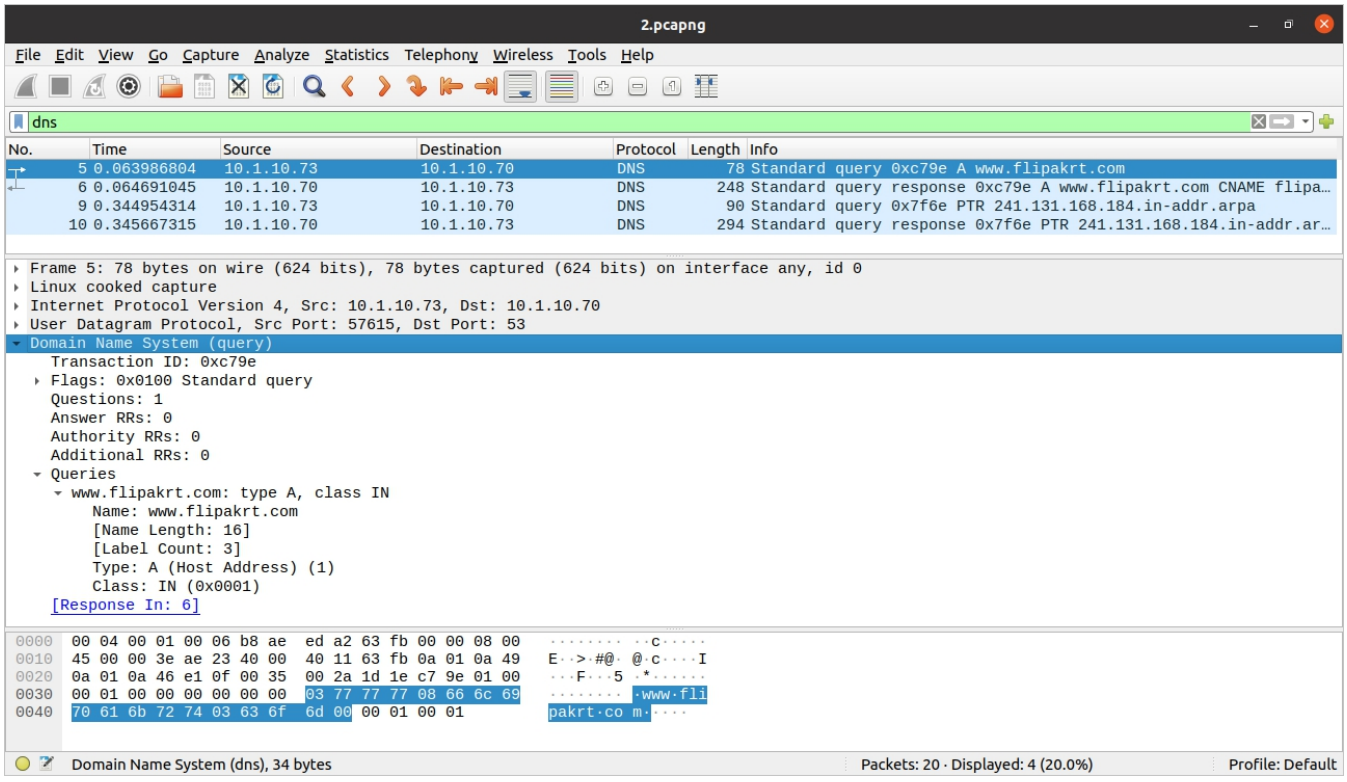
sudo resolvconf -u

```
student@CSELAB:~$ ifconfig
enp2s0    Link encap:Ethernet  HWaddr b8:ae:ed:a2:63:fb
          inet addr:10.1.10.73  Bcast:10.1.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a899:6b98:3e8b:2d11/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:53242 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43059 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32806348 (32.8 MB)  TX bytes:18675722 (18.6 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1224 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1224 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:121487 (121.4 KB)  TX bytes:121487 (121.4 KB)

student@CSELAB:~$ sudo wireshark
student@CSELAB:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
student@CSELAB:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
student@CSELAB:~$ sudo cat /etc/resolvconf/resolv.conf.d/head
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.1.10.70
student@CSELAB:~$ sudo resolvconf -u
student@CSELAB:~$
```

Also add Additional DNS Server in client machine



Ping the same website and Capture the Packets



Task 2: Set Up a Local DNS Server

Install and Configure the BIND9 Server.

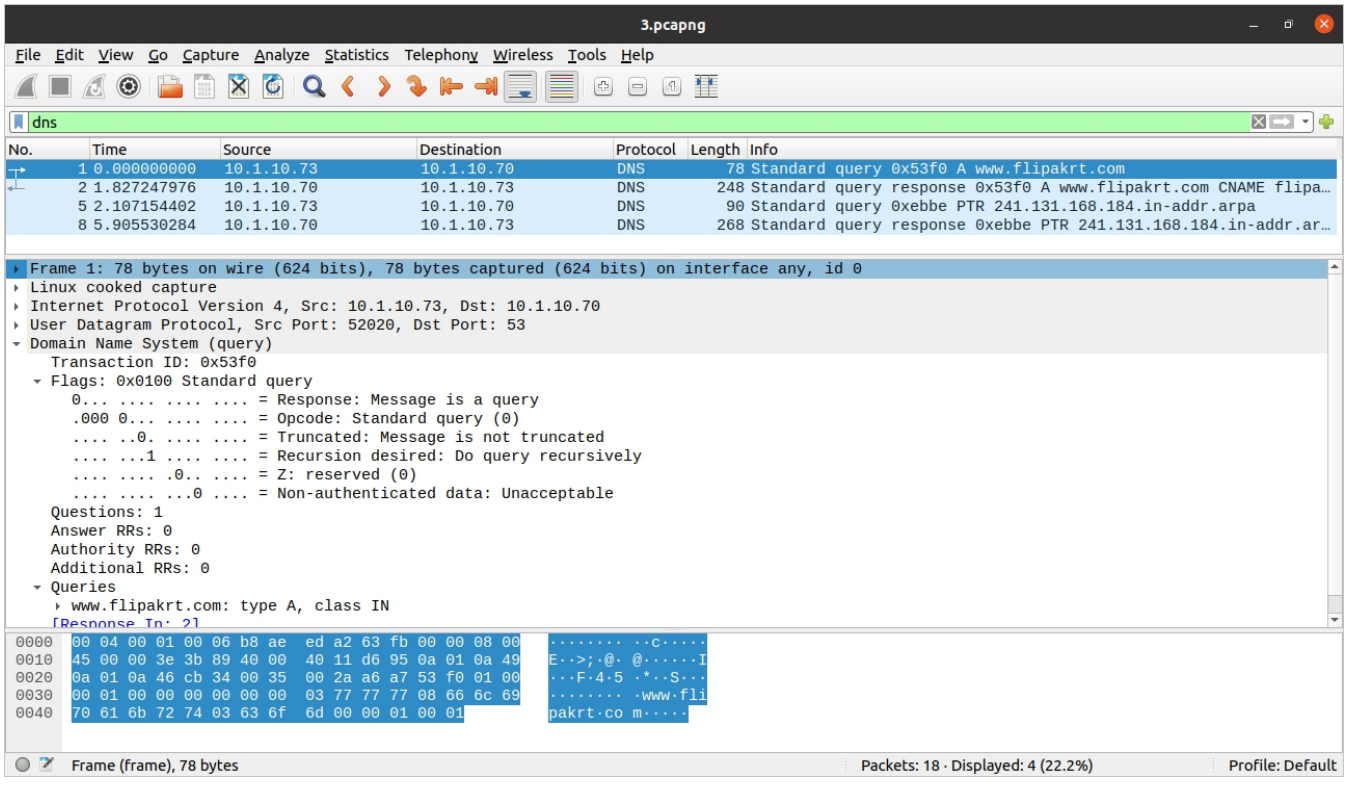
```
student@CSELAB: ~
  GNU nano 2.5.3        File: /etc/bind/named.conf.options          Modified

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 {
        //      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

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^_ Go To Line
```

start DNS Server

$ sudo service bind9 restart

```
student@CSELAB:~$ sudo service bind9 restart
```

Ping and Capture it again



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

```
student@CSELAB:~$ sudo nano /etc/bind/named.conf
student@CSELAB:~$ 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 "22.2.10.in-addr.arpa" {
type master;
file "/etc/bind/10.2.22.db";
};
student@CSELAB:~$
```

Setup the forward lookup zone file
create example.com.db zone file

example.com.db (~/Desktop) - gedit

Open Save

```
$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
```

Setup the reverse lookup zone file
then create a reverse DNS lookup file called 10.0.2.db

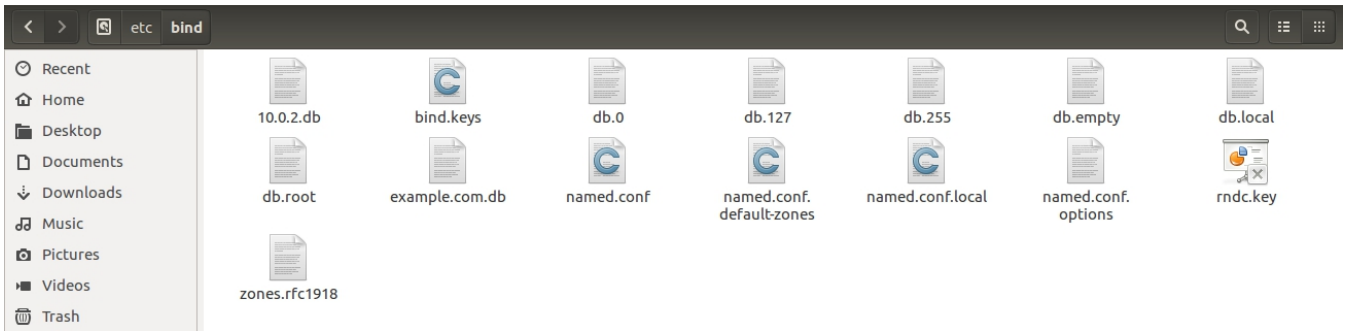
10.0.2.db (~/Desktop) - gedit

Open Save

```
$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.
```

Copy the above files into /etc/bind location.

```
student@CSELAB:~/Desktop$ sudo cp 10.0.2.db /etc/bind
student@CSELAB:~/Desktop$ sudo cp example.com.db /etc/bind
student@CSELAB:~/Desktop$
```



Task 4: Restart the BIND server and test

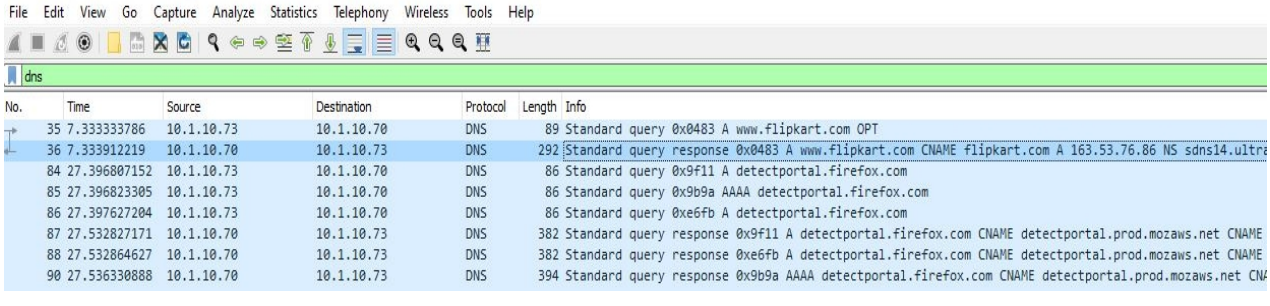
$ sudo service bind9 restart

```
student@CSELAB:~$ sudo service bind9 restart
```

Dig the website

```
student@CSELAB:~$ dig www.flipkart.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.flipkart.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1155
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 3

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

;; ANSWER SECTION:
www.flipkart.com.       53      IN      CNAME   flipkart.com.
flipkart.com.           23      IN      A       163.53.76.86

;; AUTHORITY SECTION:
flipkart.com.           172793  IN      NS      sdns14.ultradns.biz.
flipkart.com.           172793  IN      NS      sdns14.ultradns.com.
flipkart.com.           172793  IN      NS      sdns14.ultradns.org.
flipkart.com.           172793  IN      NS      sdns14.ultradns.net.

;; ADDITIONAL SECTION:
sdns14.ultradns.com.    172793  IN      A       156.154.140.14
sdns14.ultradns.com.    172793  IN      AAAA    2610:a1:1001::e

;; Query time: 0 msec
;; SERVER: 10.1.10.70#53(10.1.10.70)
;; WHEN: Sat Feb 20 12:05:39 IST 2021
;; MSG SIZE  rcvd: 248

student@CSELAB:~$
```

Capture using Wireshark



```
> Frame 36: 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.1.10.70, Dst: 10.1.10.73
> User Datagram Protocol, Src Port: 53, Dst Port: 49873
v Domain Name System (response)
    Transaction ID: 0x0483
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 4
    Additional RRs: 3
  > Queries
  v Answers
    v 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: 53 (53 seconds)
        Data length: 2
        CNAME: flipkart.com
    v 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: 23 (23 seconds)
        Data length: 4
        Address: 163.53.76.86
  v Authoritative nameservers
    v flipkart.com: type NS, class IN, ns sdns14.ultradns.biz
        Name: flipkart.com
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
        Time to live: 172793 (1 day, 23 hours, 59 minutes, 53 seconds)
        Data length: 21
        Name Server: sdns14.ultradns.biz
    v 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: 172793 (1 day, 23 hours, 59 minutes, 53 seconds)
        Data length: 18
        Name Server: sdns14.ultradns.com
    v 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: 172793 (1 day, 23 hours, 59 minutes, 53 seconds)
        Data length: 21
        Name Server: sdns14.ultradns.org
    v 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: 172793 (1 day, 23 hours, 59 minutes, 53 seconds)
        Data length: 21
        Name Server: sdns14.ultradns.net
  v Additional records
    v sdns14.ultradns.com: type A, class IN, addr 156.154.140.14
        Name: sdns14.ultradns.com
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 172793 (1 day, 23 hours, 59 minutes, 53 seconds)
        Data length: 4
        Address: 156.154.140.14
    v sdns14.ultradns.com: type AAAA, class IN, addr 2610:a1:1001::e
        Name: sdns14.ultradns.com
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
        Time to live: 172793 (1 day, 23 hours, 59 minutes, 53 seconds)
        Data length: 16
        AAAA Address: 2610:a1:1001::e
    v <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      > Z: 0x0000
        Data length: 0
    [Request In: 35]
    [Time: 0.000578433 seconds]
```

Local DNS cache on server machine:

```
student@CSELAB:~$ cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20210220061646
; secure
.                       518398  IN NS   a.root-servers.net.
                        518398  IN NS   b.root-servers.net.
                        518398  IN NS   c.root-servers.net.
                        518398  IN NS   d.root-servers.net.
                        518398  IN NS   e.root-servers.net.
                        518398  IN NS   f.root-servers.net.
                        518398  IN NS   g.root-servers.net.
                        518398  IN NS   h.root-servers.net.
                        518398  IN NS   i.root-servers.net.
                        518398  IN NS   j.root-servers.net.
                        518398  IN NS   k.root-servers.net.
                        518398  IN NS   l.root-servers.net.
                        518398  IN NS   m.root-servers.net.
; secure
                        518398  RRSIG   NS 8 0 518400 (
                                        20210305050000 20210220040000 42351 .
                                        dznKZcOFoelpHH7xOwm8BTDOSIPU3DP4busK
                                        uSvx0Lt5GknARf/gGweufb7jevSHpzlHcD93
                                        SVFE6LmPFsqRLwmYHCa0YLUSdnzr/pmPTEVq
                                        leCnhkI/XBQTqnFI9LsMU1cqNNRcvwVNZ6YY
                                        QHiFCLnqvNW/CQOdN3YXq3FeD0IbjJWcPUTa
                                        lExhKe2pEnnEBrQaCxZ0ooSW5ykApZuqXjRx
                                        4vjhIxpZIq/R1urlVeYX6VOg2pEtFKmme0k0
                                        jYq1z8ZrkDODweumV6m5JPnnaY2Z97SQ2A0z
                                        foMf3zI6kdZOaXkFkfwtPoo3Ht3OJD4WCaTa
                                        pKw5rOd1CTF6SrLYsA== )
; secure
                        172798  DNSKEY  256 3 8 (
                                        AwEAAbKGKkqc1VAvQr48iPf9Nd39f337Mitg
                                        gxF0AB9kLKRNSuq9joOEPC/R6PD/4lTzUms8
                                        U9oP+aiF0rVC2rGOKSdOLxPHRLA3ameMFT2/
                                        3bmVCFsRsn03IVTdN5VUAfczjqjmA0t9NM7b
                                        bN5oVzuQL3P1FyQb1q6HX4M1qg+htMNEd9Pd
                                        lPLMFcrUg5fcYtTr2llVkO1Xo3lAdrjmmxfG
; secure
                        172798  DNSKEY  256 3 8 (
                                        AwEAAbKGKkqc1VAvQr48iPf9Nd39f337Mitg
                                        gxF0AB9kLKRNSuq9joOEPC/R6PD/4lTzUms8
                                        U9oP+aiF0rVC2rGOKSdOLxPHRLA3ameMFT2/
                                        3bmVCFsRsn03IVTdN5VUAfczjqjmA0t9NM7b
                                        bN5oVzuQL3P1FyQb1q6HX4M1qg+htMNEd9Pd
                                        lPLMFcrUg5fcYtTr2llVkO1Xo3lAdrjmmxfG
                                        eIyQnskpwPyW88J527DEytmgPo5KzLBYLMoL
                                        2Q41PK0ul0rs7yN+g5IG4LnJOcjew1yrmHXr
                                        p/OzrpsO4FkicufYt/ygfQKkT5HYbr/yFgeZ
                                        AfaF80nYyc7wgDYxOeHdiRk=
                                        ) ; ZSK; alg = RSASHA256; key id = 42351
                        172798  DNSKEY  257 3 8 (
                                        AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvk
                                        MgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRixH
                                        lFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8O
                                        g8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n9WG
                                        e2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8efS3
                                        rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eN
                                        buv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1
                                        uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6
                                        +cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa
                                        8subX2Nn6UwNR1AkUTV74bU=
                                        ) ; KSK; alg = RSASHA256; key id = 20326
; secure
                        172798  RRSIG   DNSKEY 8 0 172800 (
                                        20210313000000 20210220000000 20326 .
                                        pQBGiP7oxZqBaSdQ/CrejUs2H0lqdHhzeowe
                                        DucnavdzVK3CYHhGExnjuE+t8NI2Habz5nvY
                                        gyxdj/MCZEmEIomL/YuCPMd+BfOtykAUTaqH
                                        SWIVdvANBRepO7q3XcIAs6++na+SGzYpriMC
                                        SaSnjb0fa3O54yEZrJt2hD1pxdB0W4TlAa5W
                                        dcbl1hkczzPLPLL5/7v1FXg2/soCgakJ/Em6
                                        0pmy8T3zYzCy5A3fpiZc4fZsp9GQKX6HRuoQ
                                        QtgpB4cHBcFiKdW7IMHZPgM9xT0MiDlfLwv7
                                        dhvF6RPRhBDDDWHYf45IMt3dNiyfqKvEnOZI
                                        yRRFBjFoxEyHenxBGg== )
; pending-answer
e.root-servers.net.     604798  AAAA    2001:500:a8::e
; pending-answer
g.root-servers.net.     604798  AAAA    2001:500:12::d0d
;
```

```
                                    rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eN
                                    buv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1
                                    uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUfhHdY6
                                    +cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa
                                    8subX2Nn6UwNR1AkUTV74bU=
                                    ) ; KSK; alg = RSASHA256; key id = 20326
; secure
                        172798  RRSIG   DNSKEY 8 0 172800 (
                                    20210313000000 20210220000000 20326 .
                                    pQBGiP7oxZqBaSdQ/CrejUs2H0lqdHhzeowe
                                    DucnavdzVK3CYHhGExnjuE+t8NI2Habz5nvY
                                    gyxdj/MCZEmEIomL/YuCPMd+BfOtykAUTaqH
                                    SWIVdvANBRepO7q3XcIAs6++na+SGzYpriMC
                                    SaSnjb0fa3O54yEZrJt2hD1pxdB0W4TlAa5W
                                    dcbl1hkczzPLPLL5/7v1FXg2/soCgakJ/Em6
                                    0pmy8T3zYzCy5A3fpiZc4fZsp9GQKX6HRuoQ
                                    QtgpB4cHBcFiKdW7IMHZPgM9xT0MiDlfLwv7
                                    dhvF6RPRhBDDDWHYf45IMt3dNiyfqKvEnOZI
                                    yRRFBjFoxEyHenxBGg== )
; pending-answer
e.root-servers.net.     604798  AAAA    2001:500:a8::e
; pending-answer
g.root-servers.net.     604798  AAAA    2001:500:12::d0d
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
; G.ROOT-SERVERS.NET [v6 TTL 1798] [v4 unexpected] [v6 success]
;       2001:500:12::d0d [srtt 16] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0]
; E.ROOT-SERVERS.NET [v6 TTL 1798] [v4 unexpected] [v6 success]
;       2001:500:a8::e [srtt 11] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0]
;
; Unassociated entries
;
;       199.7.91.13 [srtt 19] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       192.58.128.30 [srtt 24] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       2001:503:ba3e::2:30 [srtt 30] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       192.5.5.241 [srtt 31] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       2001:500:2d::d [srtt 148060] [flags 00000000] [edns 0/2/2/2/2] [plain 0/0] [ttl 1798]
;       192.203.230.10 [srtt 18] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       2001:dc3::35 [srtt 18] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       192.203.230.10 [srtt 18] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       2001:dc3::35 [srtt 18] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       192.112.36.4 [srtt 159319] [flags 00004000] [edns 4/0/0/0/0] [plain 0/0] [udpsize 512] [ttl 1798]
;       2001:500:84::b [srtt 16] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       2001:500:1::53 [srtt 29] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       193.0.14.129 [srtt 19] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       2001:500:2f::f [srtt 22] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       192.228.79.201 [srtt 17] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       2001:503:c27::2:30 [srtt 93516] [flags 00000000] [edns 0/3/3/3/3] [plain 0/0] [ttl 1798]
;       2001:500:3::42 [srtt 11] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       198.97.190.53 [srtt 21] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       192.36.148.17 [srtt 25] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       198.41.0.4 [srtt 25] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       2001:500:2::c [srtt 8] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       199.7.83.42 [srtt 31] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       202.12.27.33 [srtt 28] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       2001:7fe::53 [srtt 28] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       192.33.4.12 [srtt 17] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;       2001:7fd::1 [srtt 14] [flags 00000000] [edns 0/0/0/0/0] [plain 0/0] [ttl 1798]
;
; Bad cache
;
;
; Start view _bind
;
;
; Cache dump of view '_bind' (cache _bind)
;
$DATE 20210220061646
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
; Dump complete
student@CSELAB:~$
```

Observations:

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

Ans: Its sent over UDP

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

Ans:Source Port is 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:Yes both the IP addresses are same.

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

Ans:It's a type A Standard Query and it doesn't contain any answers.

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

Ans:2 answers are provided.

It contains:

1.Name

2.Type

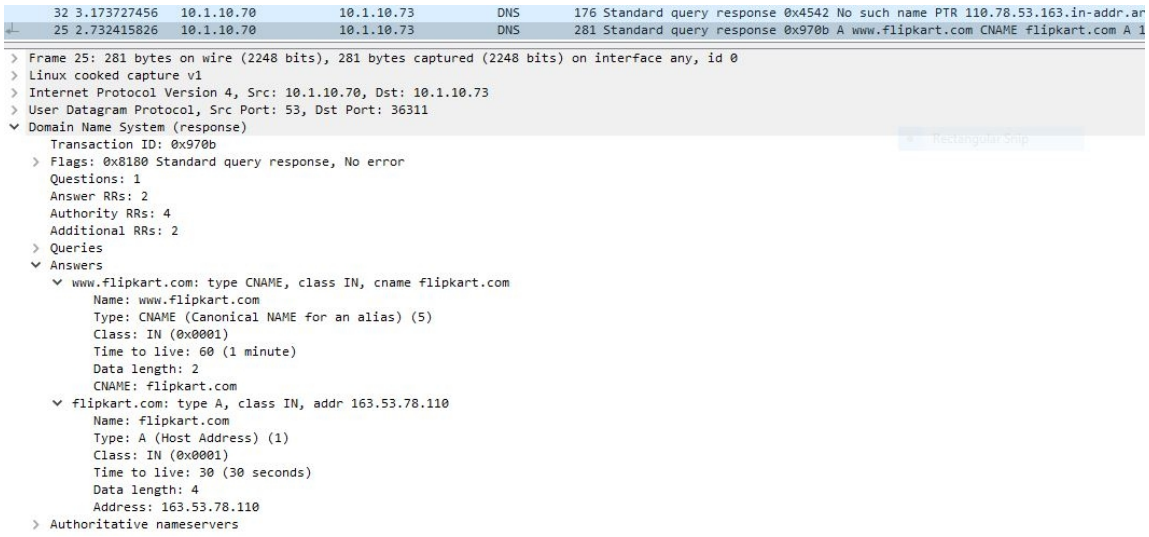
3.Class

4.Time to live(ttl)

5.Data Length

6.Cname

7.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:Yes