Week #5

Week 5 - Setting up local DNS server

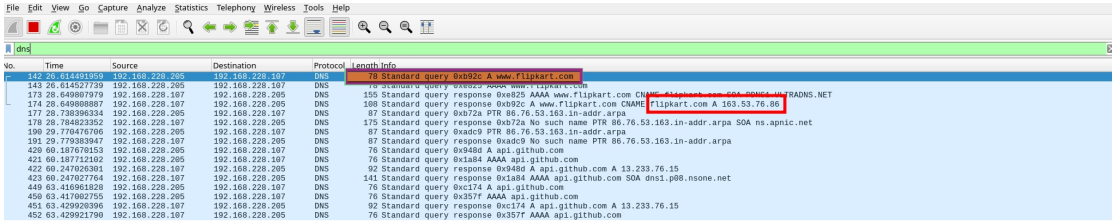
SRN : PES2UG20CS237

Name : P K Navin Shrinivas

Section : D

Task 1 :Pinging a website using default DNS

- My default DNS being 1.1.1.1 (cloudflare), flipkart was pinnged using ping command,the following packets were observed in wireshark:



WireShark packets with DNS filter

```
▸ Frame 174: 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: 192.168.228.107, Dst: 192.168.228.205
▾ User Datagram Protocol, Src Port: 53, Dst Port: 52275
    Source Port: 53
    Destination Port: 52275
    Length: 72
    Checksum: 0x77a9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  ▸ [Timestamps]
    UDP payload (64 bytes)
▾ Domain Name System (response)
    Transaction ID: 0xb92c
  ▸ 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
    [Request In: 142]
    [Time: 2.035316928 seconds]
```

DNS query

```
▸ Frame 142: 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: 192.168.228.205, Dst: 192.168.228.107
▾ User Datagram Protocol, Src Port: 52275, Dst Port: 53
    Source Port: 52275
    Destination Port: 53
    Length: 42
    Checksum: 0x4ac6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  ▸ [Timestamps]
    UDP payload (34 bytes)
▾ Domain Name System (query)
    Transaction ID: 0xb92c
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 174]
```

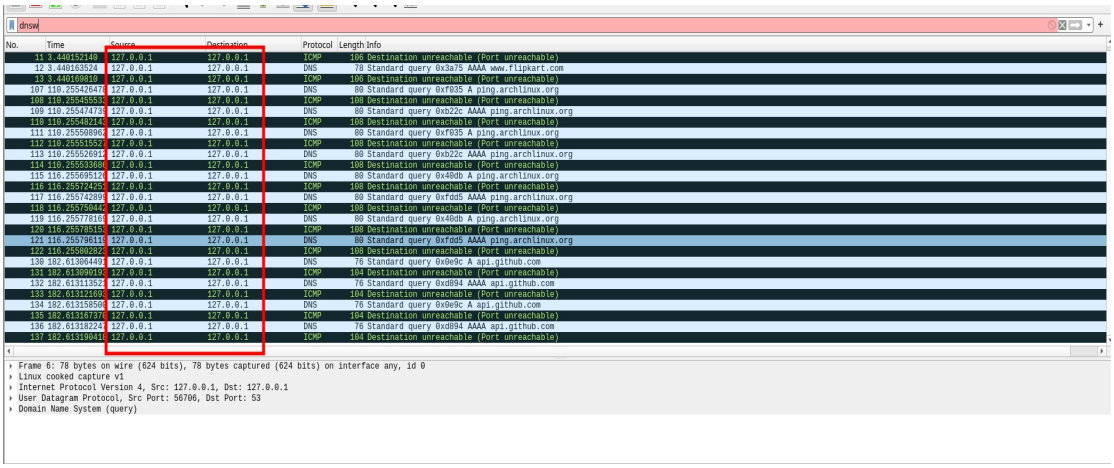
```
0000  00 04 00 01 00 06 e0 d4  e8 32 73 8c 00 00 08 00   ······ ·· ·2s·····
0010  45 00 00 3e 64 01 40 00  40 11 8c 23 c0 a8 e4 cd   E··>d·@· @··#····
0020  c0 a8 e4 6b cc 33 00 35  00 2a 4a c6 b9 2c 01 00   ···k·3·5 ·*J··,··
0030  00 01 00 00 00 00 00 00  03 77 77 77 08 66 6c 69   ········ ·www·fli
0040  70 6b 61 72 74 03 63 6f  6d 00 00 01 00 01         pkart·co m·····
```

DNS response

Task 2 :Configure client to use local DNS

- Note the ip address of your local DNS server, in my case i am using loopback interface hence my ip is 127.0.0.1
- In my linux distro(Arch linux), to change the DNS used, edit the lines in /etc/resolv.conf. The only line in the file should be the local DNS, rest all can be commented. Pinging a website after this should lead to failure.

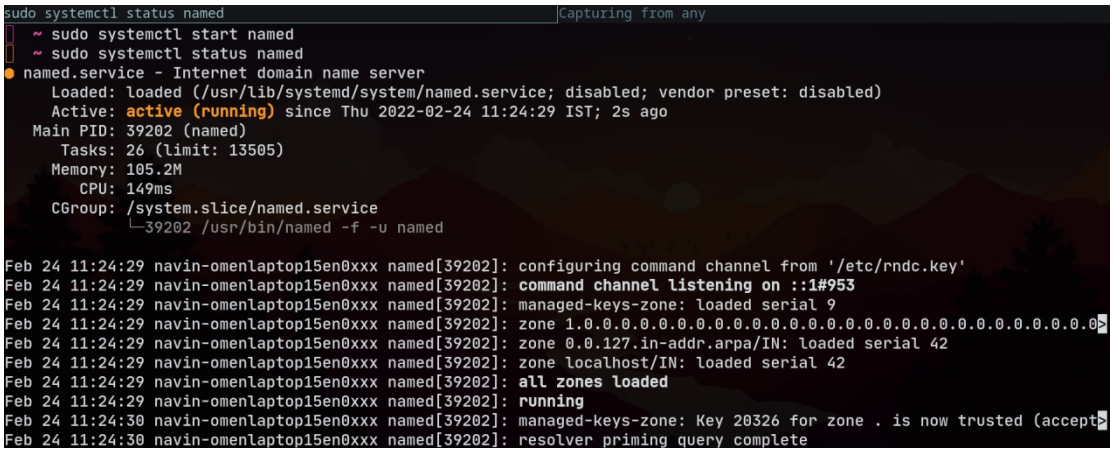
Ping fails, edited /etc/resolv.conf



Failed DNS requests and responses can be seen in wireshark as well

Task 3 : Setting up local DNS server

- Install Bind9 and also start the service, follow so the screenshots :



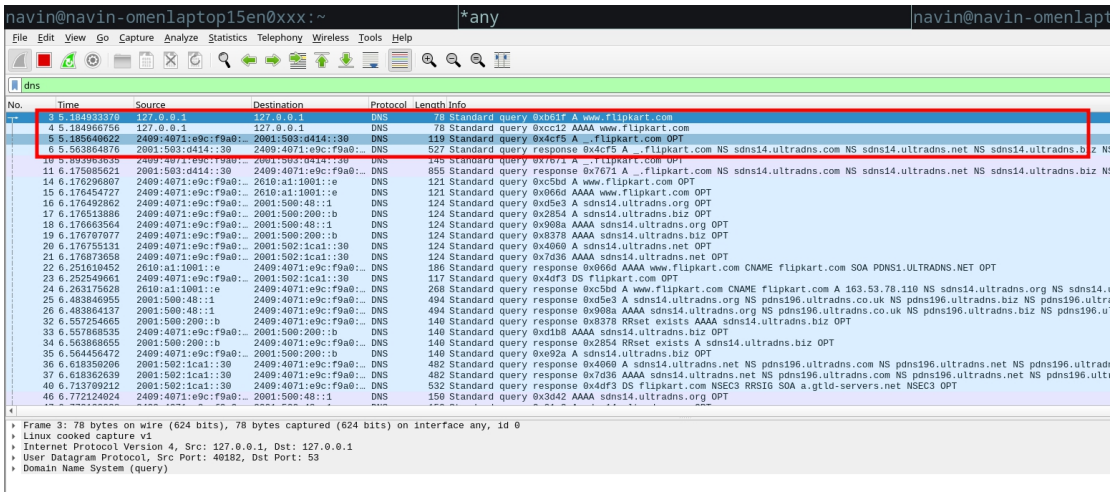
After starting Bind9 daemon

Following conf file for Bind9 (should exist)

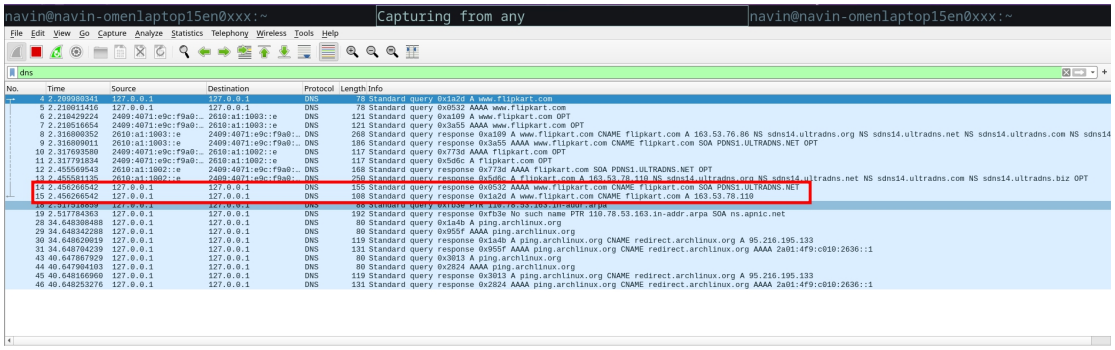
- Dump the cache to a db file so it is visible to us using the following commands:

Dumped cache into db file

- Now pinging a website for the first time should cause a rescurive reolving using other DNS serverl, the second ping should be resolved from the local DNS server itself.



DNS resolved from other servers, first checks in cache



DNS resolved from local cache server

Task 5 : Setting up a zone in local DNS

- First edit the named.conf to check particual files for the query zone like so:

```
➜  /etc cat ./named.conf
options {
    directory "/var/named";
    pid-file "/tmp/named.pid";

    allow-recursion { 127.0.0.1; };
    allow-transfer { none; };
    allow-update { none; };

    version none;
    hostname none;
    server-id none;
};

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

zone "10.0.2.in-addr.arpa"{
 type master;
 file "/var/named/10.0.2.db";
};
```

Entering new zones to bind9 service

- Being very careful of the file names, create the zone records (both forward and reverse lookup), doing so:

```
➜  /etc cat /var/named/10.0.2.db
$TTL 3D
@       IN      SOA ns.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
➜  /etc
```

Reverse Lookup Zone records

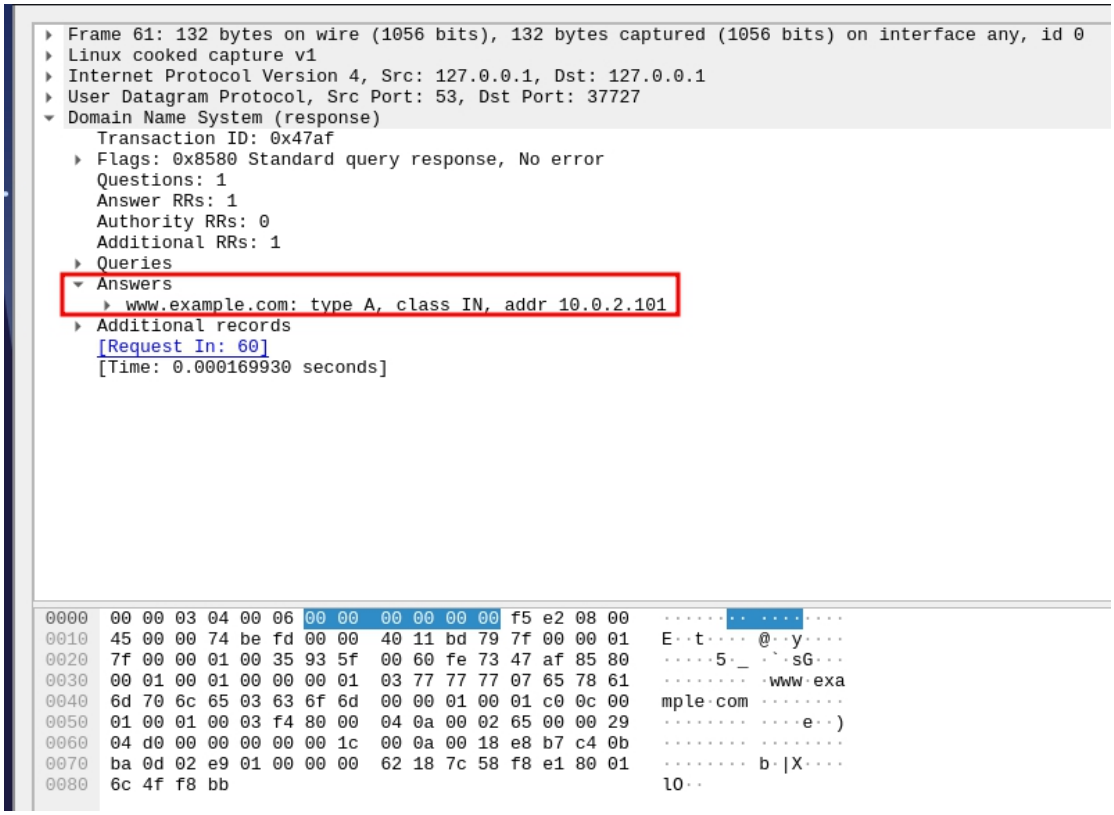
```
➜  /etc cat /var/named/example.com.db
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com(
                        2008111001
                        8H
                        2H
                        4W
                        1D)
@       IN      NS      ns.example.com.
@       IN      MX      10 mail.example.com.

www     IN      A       10.0.2.101
mail    IN      A       10.0.2.102
ns      IN      A       10.0.2.10
*.example.com.          IN A 10.0.2.100
➜  /etc
```

Forward lookup zone records

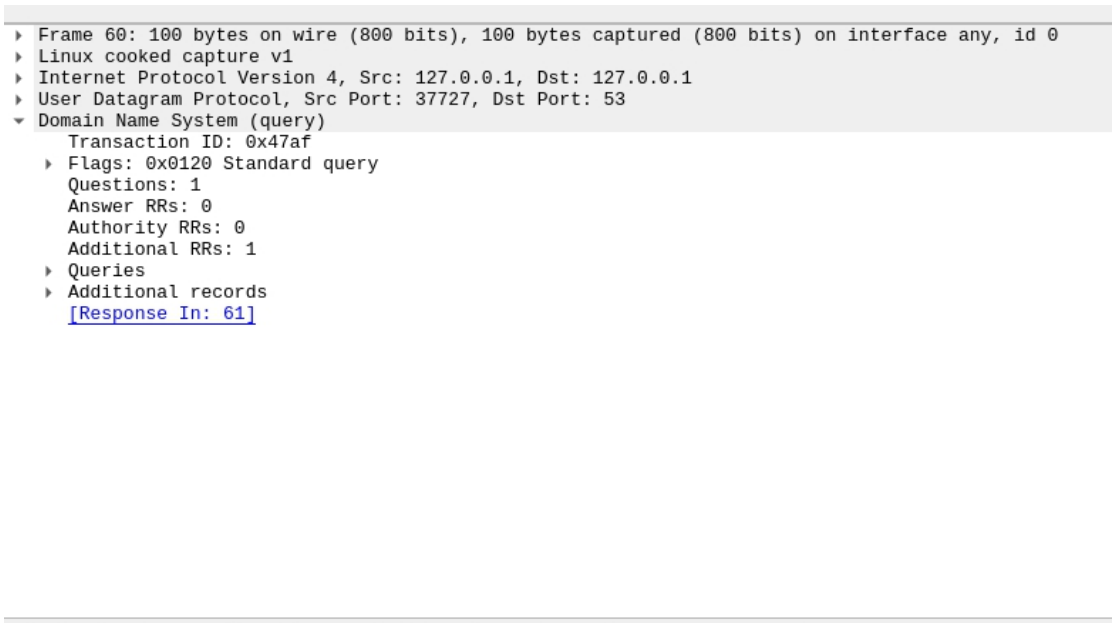
- Now restart the bind9 service using systemctl and now pingin www.example.com should be resolve from our local DNS and should return contents from it, like so:

```
➜  /etc dig www.example.com

; <<>> DiG 9.16.25 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60026
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a8b2e29e92c67a090100000062187ba7c01e6a4b0135f875 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.0.2.101

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Feb 25 12:18:07 IST 2022
;; MSG SIZE  rcvd: 88
```

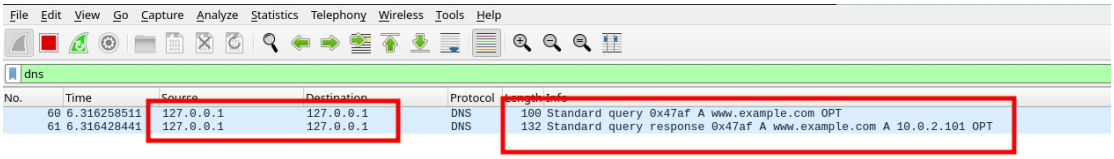
Ping to www.example.com giving IP from our DNS server



DNS response from local DNS server



DNS query to local DNS server



WireShark packets with DNS filter

- The same dig command for reverse lookup :

```
➜  /etc dig 101.2.0.1.in-addr.arpa

; <<>> DiG 9.16.25 <<>> 101.2.0.1.in-addr.arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 20569
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 42d4327bd73da72b0100000062187c17e3a2502839afc49d (good)
;; QUESTION SECTION:
;101.2.0.1.in-addr.arpa.                IN      A

;; AUTHORITY SECTION:
1.in-addr.arpa.         3600    IN      SOA     ns.apnic.net. read-txt-record-of-zone-first-dns-admin.apn
ic.net. 18641 7200 1800 604800 3600

;; Query time: 3693 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Feb 25 12:19:59 IST 2022
;; MSG SIZE  rcvd: 181
```

Reverse lookup using dig tool