

Week #4

Week 4 - Setting up local DNS server

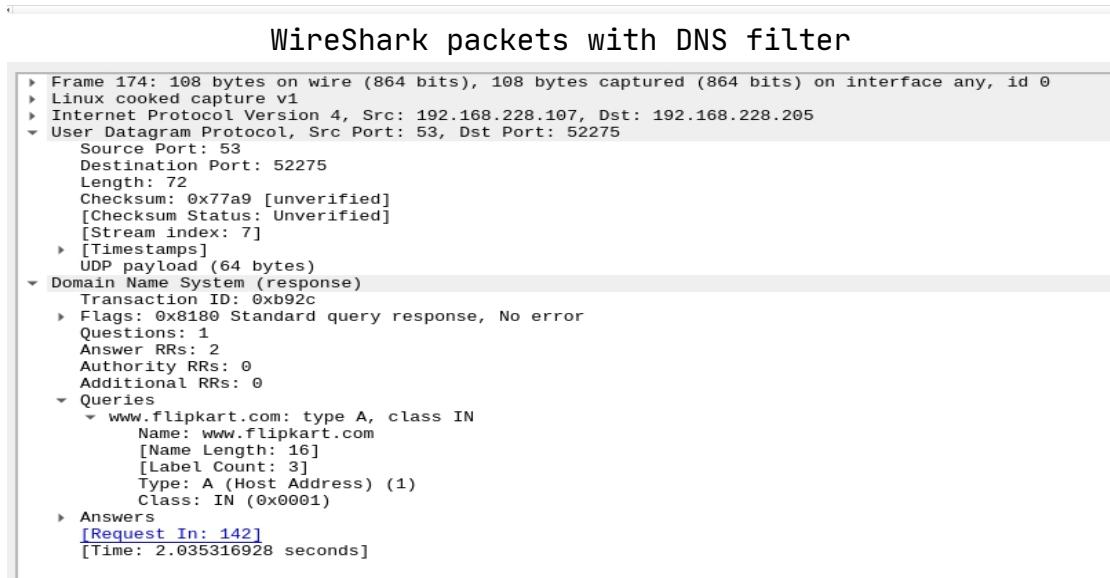
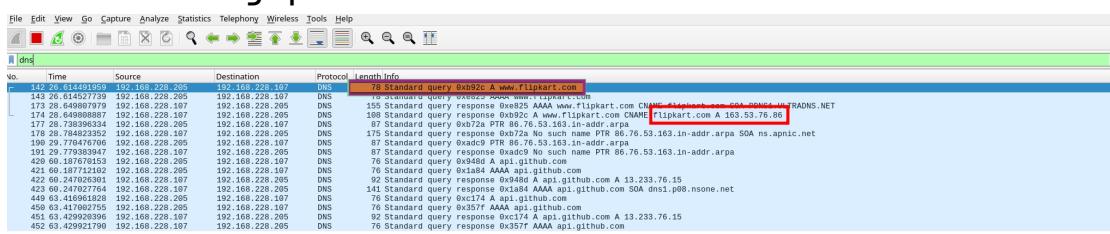
SRN : PES2UG20CS237

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 pinged using ping command, the following packets were observed in wireshark:



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 002s
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

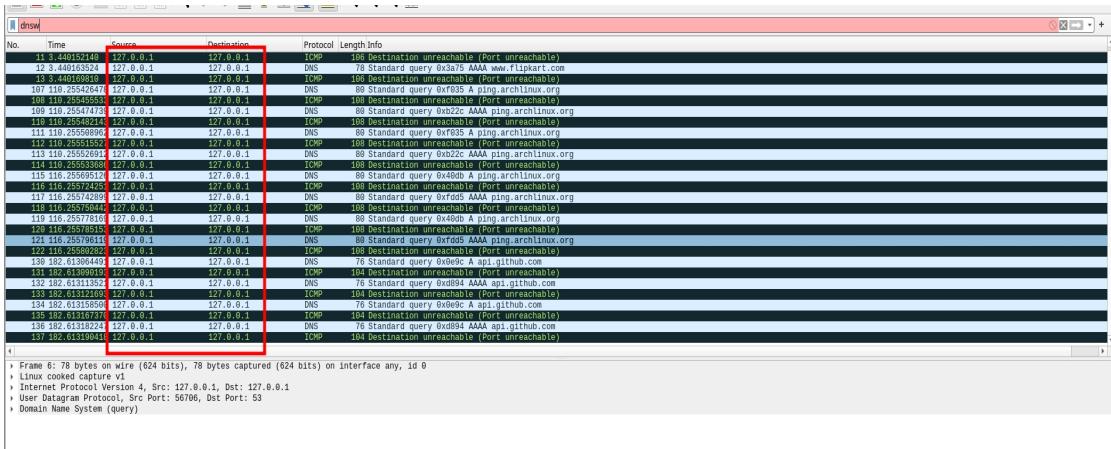
DNS response

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.

```
navin@navin-omenlaptop15en0xxx:~  
└─~ sudo cat /etc/resolv.conf  
# Generated by NetworkManager  
nameserver 127.0.0.1  
# nameserver 2409:4071:e9c:f9a0::5  
└─~ ping www.flipkart.com  
ping: www.flipkart.com: Temporary failure in name resolution  
└─~
```

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

```
navin@navin-omenlaptop15en0xxx:~                                         |Capturing from any
└─ cat /etc/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 "localhost" IN {
    type master;
    file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "127.0.0.zone";
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" {
    type master;
    file "localhost.ip6.zone";
};
```

Following conf file for Bind9 (should exist)

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

```
navin@navin-omenlaptop15en0xxx:~  
[ ~ sudo rndc dumpdb -cache  
[ ~ cat /var/named/named_dump.db | less  
[ ~ cat /var/named/named_dump.db | head 5  
head: cannot open '5' for reading: No such file or director  
[ ~ cat /var/named/named_dump.db | head  
  
Start view _default  
  
Cache dump of view '_default' (cache _default)  
  
using a 86400 second stale ttl  
$DATE 20220224055659  
secure  
518251 IN NS b.root-servers.net.
```

Dumped cache into db file

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

*any						
File	Edit	View	Go	Capture	Analyze	Statistics
Telephony	Wireless	Tools	Help			
dns						
No.	Time	Source	Destination	Protocol	Length	Info
1	127.0.0.1	127.0.0.1	DNS	78	Standard query 0xb61f A www.flipkart.com	
4	18:49:46.755	127.0.0.1	DNS	78	Standard query 0xb61f A www.flipkart.com	
5	18:49:46.755	2499:1071:ec9::9a0:1:30	DNS	116	Standard query 0xb61f A www.ultradns.net OPT	
6	5.563848478	2891:593:di4:13:39	DNS	527	Standard query response 0xd345 CA flipkart.com NS sdns14.ultradns.com NS sdns14.ultradns.net NS sdns14.ultradns.biz NS	
10	5.893983035	2499:4071:ec9::9a0:1:30	DNS	145	Standard query response 0x7e07 A flipkart.com OPT	
11	6.175085621	2001:593:di4:13:39	DNS	855	Standard query response 0x7e07 A flipkart.com NS sdns14.ultradns.com NS sdns14.ultradns.net NS sdns14.ultradns.biz NS	
14	6.176544727	2499:4071:ec9::9a0:1:30	DNS	120	Standard query response 0x7e07 A www.ultradns.net OPT	
16	6.176454727	2499:4071:ec9::9a0:1:30	DNS	124	Standard query 0x86d3 AAA www.ultradns.org OPT	
17	6.176513886	2499:4071:ec9::9a0:1:30	DNS	124	Standard query 0x2854 A sdns14.ultradns.biz OPT	
18	6.176770831	2499:4071:ec9::9a0:1:30	DNS	124	Standard query 0x8378 AAAA sdns14.ultradns.biz OPT	
19	6.176787731	2499:4071:ec9::9a0:1:30	DNS	124	Standard query 0x8378 AAAA sdns14.ultradns.biz OPT	
20	6.176783658	2001:593:di4:13:39	DNS	124	Standard query 0x7d36 AAAA sdns14.ultradns.net OPT	
22	6.176783658	2499:4071:ec9::9a0:1:30	DNS	160	Standard query response 0x7d36 AAAA sdns14.ultradns.com CNAME flipkart.com SOA PONSI1.ULTRADNS.NET OPT	
23	6.252549661	2499:4071:ec9::9a0:1:30	DNS	117	Standard query 0x4d93 DS flipkart.com OPT	
24	6.2610:1a1:1001:	2499:4071:ec9::9a0:1:30	DNS	268	Standard query response 0x65d1 B www.ultradns.com CNAME flipkart.com A 163.75.110.180.ultradns.org NS sdns14.ultradns.net NS sdns14.ultradns.biz NS	
25	6.483844959	2001:598:48:1:30	DNS	494	Standard query response 0x65d1 A sdns14.ultradns.com CNAME flipkart.com A 163.75.110.180.ultradns.org NS sdns14.ultradns.net NS sdns14.ultradns.biz NS	
32	6.557254665	2001:598:48:1:30	DNS	148	Standard query response 0x8378 Rset exists AAAA sdns14.ultradns.biz OPT	
33	6.557886853	2499:4071:ec9::9a0:1:30	DNS	148	Standard query 0xdb18 AAAA sdns14.ultradns.biz OPT	
34	6.618359262	2499:4071:ec9::9a0:1:30	DNS	148	Standard query 0x86d3 AAAA sdns14.ultradns.biz OPT	
35	6.504487872	2499:4071:ec9::9a0:1:30	DNS	140	Standard query 0x62a2 A sdns14.ultradns.com OPT	
36	6.618359262	2001:592:1:ca1:39	DNS	482	Standard query response 0x4663 A sdns14.ultradns.net NS pdns196.ultradns.com NS pdns196.ultradns.net NS pdns196.ultradns.net NS pdns196.ultradns.net	
37	6.618362639	2001:592:1:ca1:39	DNS	482	Standard query response 0x7d36 AAAA sdns14.ultradns.net NS pdns196.ultradns.com NS pdns196.ultradns.net NS pdns196.ultradns.net	
40	6.717370912	2001:592:1:ca1:39	DNS	532	Standard query response 0x4fd3 DS flipkart.com NSEC3 RRSIG SOA g.tld-servers.net NSEC3 OPT	
46	6.772124024	2499:4071:ec9::9a0:1:30	DNS	158	Standard query response 0x3d42 AAAA sdns14.ultradns.org OPT	

DNS resolved from other servers, first checks in cache

```

navin@navin-omenlaptop15en0xxx:~ | Capturing from any | navin@navin-omenlaptop15en0xxx:~ | 
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Description Protocol Length Info
1 2.318914456 127.0.0.1 DNS 78 Standard query 0x0532 AAAA www.flipkart.com
2 2.318914456 127.0.0.1 DNS 78 Standard query 0x0532 AAAA www.flipkart.com
3 2.318914456 127.0.0.1 DNS 121 Standard query 0x04d0 A www.flipkart.com OPT
4 2.318914456 127.0.0.1 DNS 121 Standard query 0x04d0 A www.flipkart.com OPT
5 2.318914456 127.0.0.1 DNS 260 Standard query response 0x0100 A www.flipkart.com CNNAME flipkart.com A 163.53.76.86 NS sdn$14.ultradns.org NS sdn$14.ultradns.org NS sdn$14.ultradns.org
6 2.318908352 2610.113.102.1 DNS 260 Standard query response 0x0100 A www.flipkart.com CNNAME flipkart.com A 163.53.76.86 NS sdn$14.ultradns.org NS sdn$14.ultradns.org NS sdn$14.ultradns.org
7 2.318908352 2610.113.102.1 DNS 186 Standard query response 0x03d0 AAAA www.flipkart.com CNNAME www.soa.pdns1.ultradns.net OPT
8 2.318908352 2610.113.102.1 DNS 186 Standard query response 0x03d0 AAAA www.flipkart.com CNNAME www.soa.pdns1.ultradns.net OPT
9 2.317791832 127.0.0.1 DNS 117 Standard query 0x05d6 A flipkart.com OPT
10 2.317791832 127.0.0.1 DNS 117 Standard query 0x05d6 A flipkart.com OPT
11 2.317791832 127.0.0.1 DNS 290 Standard query response 0x0100 A www.flipkart.com CNNAME flipkart.com A 163.53.76.86 NS sdn$14.ultradns.org NS sdn$14.ultradns.org NS sdn$14.ultradns.org
12 2.317791832 127.0.0.1 DNS 290 Standard query response 0x0100 A www.flipkart.com CNNAME flipkart.com A 163.53.76.86 NS sdn$14.ultradns.org NS sdn$14.ultradns.org NS sdn$14.ultradns.org
13 2.455581135 2610.113.102.1 DNS 153 Standard query response 0x0532 AAAA www.flipkart.com CNNAME flipkart.com A 163.53.76.86 NS sdn$14.ultradns.org NS sdn$14.ultradns.org
14 2.455581135 2610.113.102.1 DNS 153 Standard query response 0x0532 AAAA www.flipkart.com CNNAME flipkart.com A 163.53.76.86 NS sdn$14.ultradns.org NS sdn$14.ultradns.org
15 2.455626542 127.0.0.1 DNS 153 Standard query response 0x0532 AAAA www.flipkart.com CNNAME flipkart.com A 163.53.76.86 NS sdn$14.ultradns.org NS sdn$14.ultradns.org
16 2.455626542 127.0.0.1 DNS 153 Standard query response 0x0532 AAAA www.flipkart.com CNNAME flipkart.com A 163.53.76.86 NS sdn$14.ultradns.org NS sdn$14.ultradns.org
17 2.455626542 127.0.0.1 DNS 153 Standard query response 0x0532 AAAA www.flipkart.com CNNAME flipkart.com A 163.53.76.86 NS sdn$14.ultradns.org NS sdn$14.ultradns.org
18 2.455626542 127.0.0.1 DNS 153 Standard query response 0x0532 AAAA www.flipkart.com CNNAME flipkart.com A 163.53.76.86 NS sdn$14.ultradns.org NS sdn$14.ultradns.org
19 2.517748363 127.0.0.1 DNS 102 Standard query response 0x0100 No name PTR 110.76.53.163.in-addr.apnic.net
20 24.64839488 127.0.0.1 DNS 80 Standard query 0x055f AAAA ping.archlinux.org
21 34.648704239 127.0.0.1 DNS 80 Standard query 0x055f AAAA ping.archlinux.org
22 34.648704239 127.0.0.1 DNS 80 Standard query 0x055f AAAA ping.archlinux.org CNNAME redirect.archlinux.org A 95.216.195.133
23 34.648704239 127.0.0.1 DNS 80 Standard query 0x055f AAAA ping.archlinux.org CNNAME redirect.archlinux.org AAAA 2a01:4f9:c010:2636::1
24 40.648166698 127.0.0.1 DNS 110 Standard query response 0x0303 A ping.archlinux.org
25 40.648166698 127.0.0.1 DNS 110 Standard query response 0x0303 A ping.archlinux.org CNNAME redirect.archlinux.org A 95.216.195.133
26 40.648166698 127.0.0.1 DNS 110 Standard query response 0x0303 A ping.archlinux.org CNNAME redirect.archlinux.org AAAA 2a01:4f9:c010:2636::1
27 40.648253276 127.0.0.1 DNS 131 Standard query response 0x0284 AAAA ping.archlinux.org CNNAME redirect.archlinux.org AAAA 2a01:4f9:c010:2636::1

```

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: a8b2e29e92c67a09010000062187ba7c01e6a4b0135f875 (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

```

▶ Frame 61: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface any, id 0
▶ Linux cooked capture v1
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▶ User Datagram Protocol, Src Port: 53, Dst Port: 37727
▼ Domain Name System (response)
    Transaction ID: 0x47af
    ▶ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
    ▶ Queries
    ▼ Answers
        ▶ www.example.com: type A, class IN, addr 10.0.2.101
    ▶ Additional records
    [Request In: 60]
    [Time: 0.000169930 seconds]

0000  00 00 03 04 00 06 00 00 00 00 00 f5 e2 08 00  .....
0010  45 00 00 74 be fd 00 00 40 11 bd 79 7f 00 00 01  E..t....@.y...
0020  7f 00 00 01 00 35 93 5f 00 60 fe 73 47 af 85 80  ....5_...SG...
0030  00 01 00 01 00 00 01 03 77 77 77 07 65 78 61  .....www.exa...
0040  6d 70 6c 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00  mple.com.....
0050  01 00 01 00 03 f4 80 00 04 0a 00 02 65 00 00 29  .....
0060  04 d0 00 00 00 00 01 c0 00 0a 00 18 e8 b7 c4 0b  .....
0070  ba 0d 02 e9 01 00 00 00 62 18 7c 58 f8 e1 80 01  ....b|X....
0080  6c 4f f8 bb 10...

```

DNS response from local DNS server

```

▶ Frame 60: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
▶ Linux cooked capture v1
▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▶ User Datagram Protocol, Src Port: 37727, Dst Port: 53
▼ Domain Name System (query)
    Transaction ID: 0x47af
    ▶ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
    ▶ Queries
    ▶ Additional records
    [Response In: 61]

```

```

0000  00 00 03 04 00 06 00 00 00 00 00 de 71 08 00  .....
0010  45 00 00 54 be fc 00 00 40 11 bd 9a 7f 00 00 01  E..T....@.....
0020  7f 00 00 01 93 5f 00 35 00 40 fe 53 47 af 01 20  ....5_...@.SG...
0030  00 01 00 00 00 00 00 01 03 77 77 77 07 65 78 61  .....www.exa...
0040  6d 70 6c 65 03 63 6f 6d 00 00 01 00 01 00 00 29  mple.com....)
0050  10 00 00 00 00 00 00 0c 00 0a 00 08 e8 b7 c4 0b  .....
0060  ba 0d 02 e9

```

DNS query to local DNS server

No.	Time	Source	Destination	Protocol	Length Info
60	6.316258511	127.0.0.1	127.0.0.1	DNS	100 Standard query 0x47af A www.example.com OPT
61	6.316428441	127.0.0.1	127.0.0.1	DNS	132 Standard query response 0x47af A www.example.com A 10.0.2.101 OPT

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.apnic.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