

COMPUTER NETWORKS LAB

WEEK 4

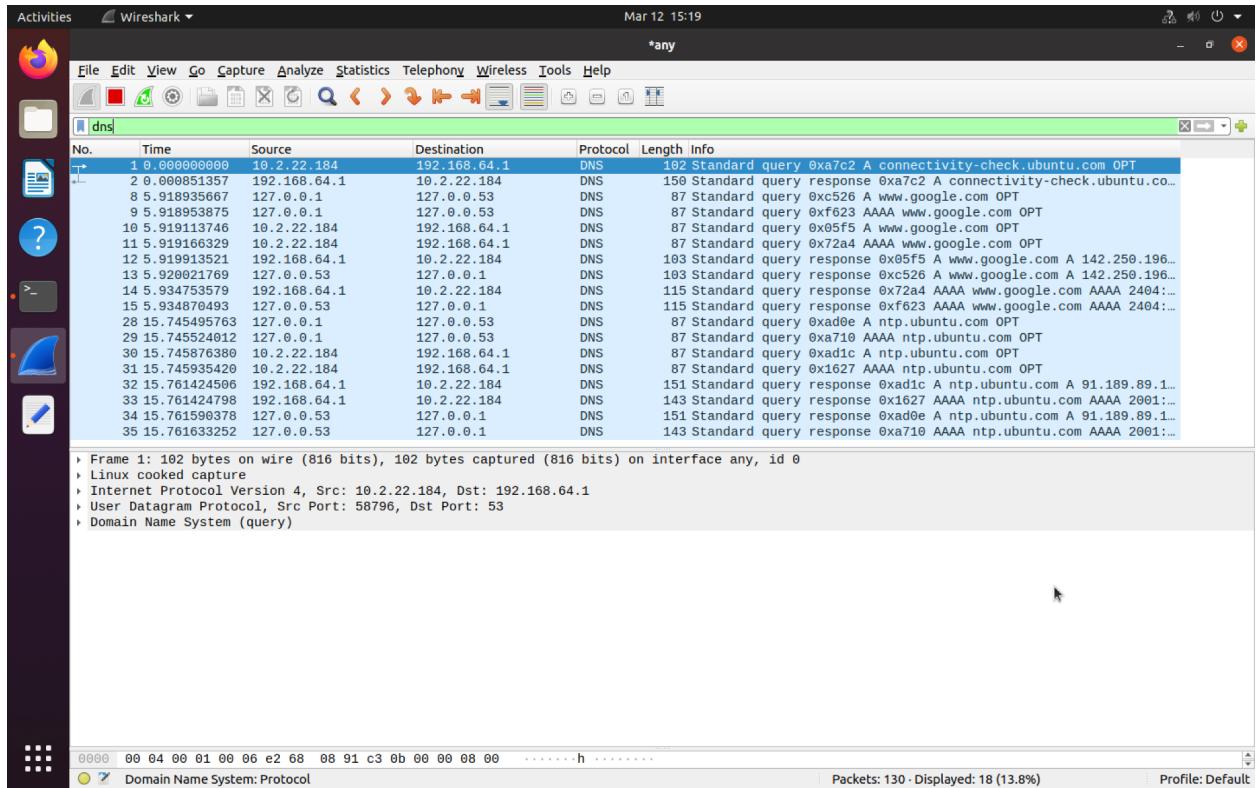
Submitted by: Mahika Gupta

SRN: PES1UG20CS243

Date: 07/03/22

1. Observation 1:

- Sending a ping request to the local DNS server.
- Receiving response from it



2. Configuring client and server machine:

And setting up local dns connection.

Client:

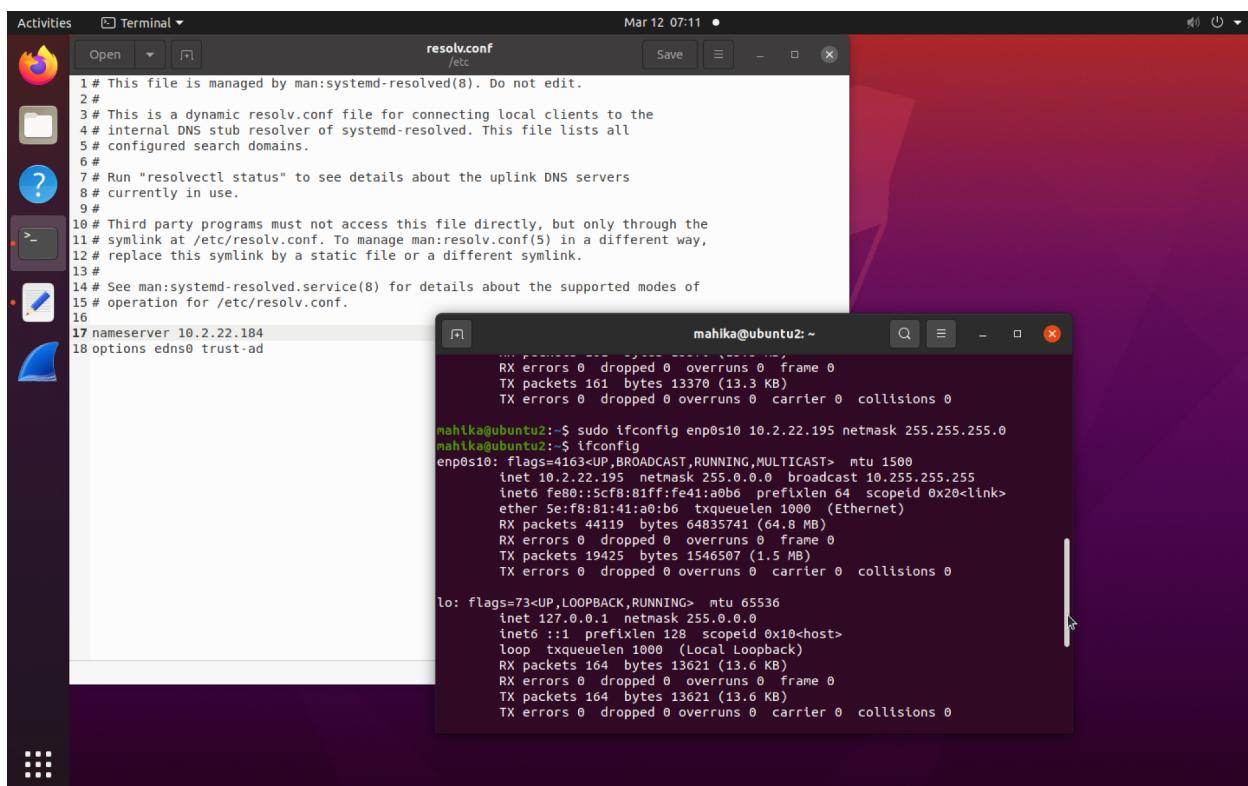
```
mahika@ubuntu2:~ TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
mahika@ubuntu2:~$ sudo ifconfig enp0s10 10.2.22.195 netmask 255.255.255.0  
[sudo] password for mahika:  
mahika@ubuntu2:~$ ifconfig  
enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
      inet 10.2.22.195 netmask 255.255.255.0 broadcast 10.2.22.255  
      inet6 fe80::5cf8:81ff:fe41:a0b6 prefixlen 64 scopeid 0x20<link>  
        ether 5e:f8:81:41:a0:b6 txqueuelen 1000 (Ethernet)  
          RX packets 248 bytes 120243 (120.2 KB)  
          RX errors 0 dropped 1 overruns 0 frame 0  
          TX packets 170 bytes 17792 (17.7 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 135 bytes 11030 (11.0 KB)  
          RX errors 0 dropped 0 overruns 0 frame 0  
          TX packets 135 bytes 11030 (11.0 KB)  
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
mahika@ubuntu2:~$
```

Server:

```
mahika@ubuntu:~$ ifconfig enp0s10 10.2.22.184 netmask 255.255.255.0
mahika@ubuntu:~$ ifconfig
enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.2.22.184 netmask 255.0.0.0 broadcast 10.255.255.255
        inet6 fe80::e068:8ff:fe91:c30b prefixlen 64 scopeid 0x20<link>
          ether e2:68:08:91:c3:0b txqueuelen 1000 (Ethernet)
            RX packets 10166 bytes 13274414 (13.2 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 4566 bytes 365170 (365.1 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 333 bytes 30098 (30.0 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 333 bytes 30098 (30.0 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

mahika@ubuntu:~$
```

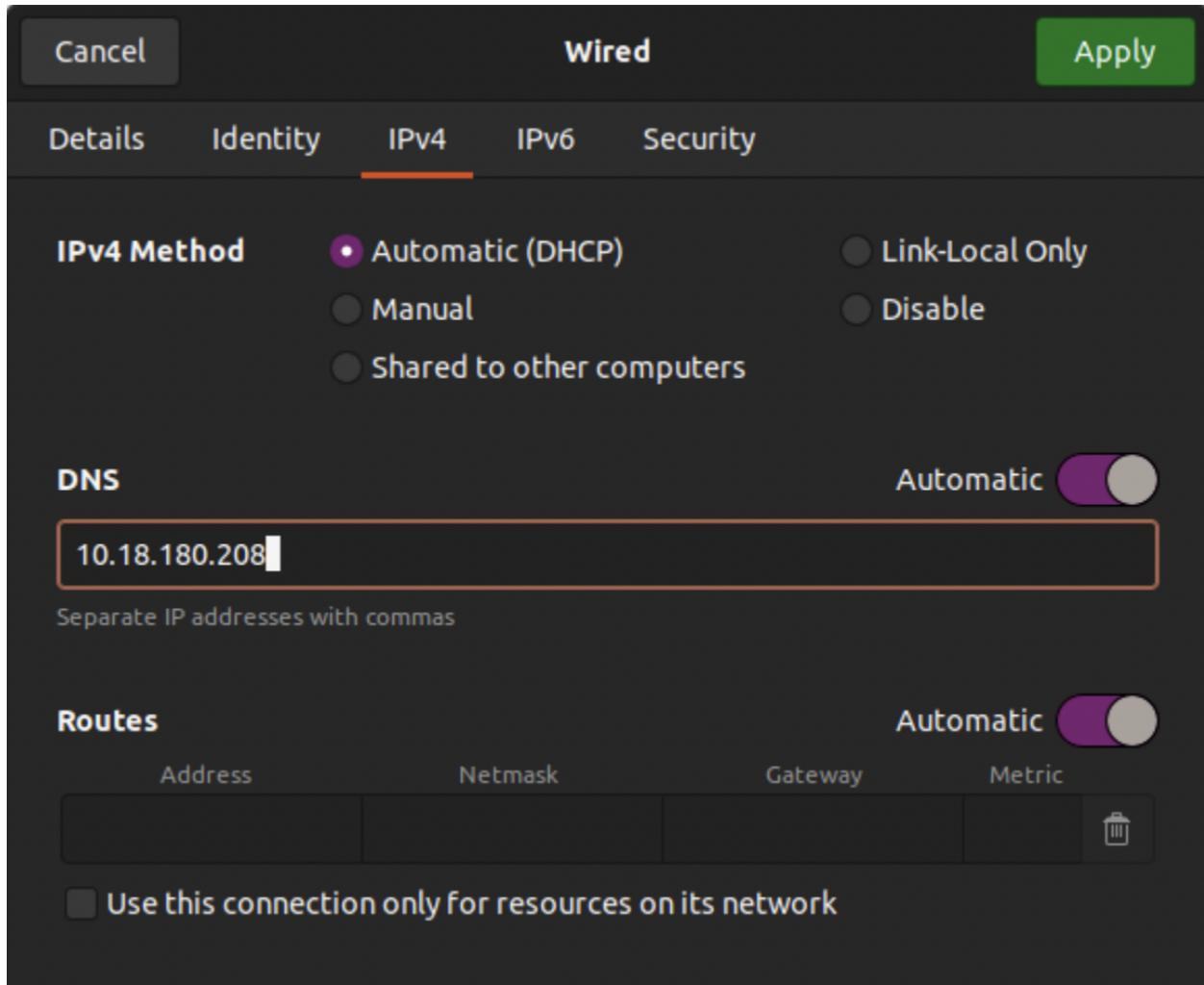


The screenshot shows a standard Ubuntu desktop environment. On the left, there's a dock with icons for Dash, Home, Activities, Terminal, and others. In the center, there's a terminal window titled 'Terminal' with the command 'ifconfig' running, showing network interface details. To the right of the terminal is a file editor window titled 'resolv.conf /etc' with the path 'resolv.conf' in the title bar. The file content includes comments about the file being managed by systemd-resolved and its purpose for connecting local clients to the internal DNS stub resolver. It also contains configuration for nameservers and options like 'trust-ad'. The desktop background is a purple gradient.

```
1 # This file is managed by man:systemd-resolved(8). Do not edit.
2 #
3 # This is a dynamic resolv.conf file for connecting local clients to the
4 # internal DNS stub resolver of systemd-resolved. This file lists all
5 # configured search domains.
6 #
7 # Run "resolvectl status" to see details about the uplink DNS servers
8 # currently in use.
9 #
10 # Third party programs must not access this file directly, but only through the
11 # symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
12 # replace this symlink by a static file or a different symlink.
13 #
14 # See man:systemd-resolved.service(8) for details about the supported modes of
15 # operation for /etc/resolv.conf.
16
17 nameserver 10.2.22.184
18 options edns0 trust-ad
```

```
mahika@ubuntu2:~$ sudo ifconfig enp0s10 10.2.22.195 netmask 255.255.255.0
mahika@ubuntu2:~$ ifconfig
enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.2.22.195 netmask 255.0.0.0 broadcast 10.255.255.255
        inet6 fe80::scf8:81ff:fe41:a0b6 prefixlen 64 scopeid 0x20<link>
          ether 5e:f8:81:41:a0:b6 txqueuelen 1000 (Ethernet)
            RX packets 44119 bytes 64835741 (64.8 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 19425 bytes 1546507 (1.5 MB)
            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 164 bytes 13621 (13.6 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 164 bytes 13621 (13.6 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



SET up dns server:

```
pesu@pesu-OptiPlex-3070:~$ sudo nano /etc/bind/named.conf.options
[sudo] password for pesu:
pesu@pesu-OptiPlex-3070:~$ █

GNU nano 5.4                                         pesu@pesu-OptiPlex
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;

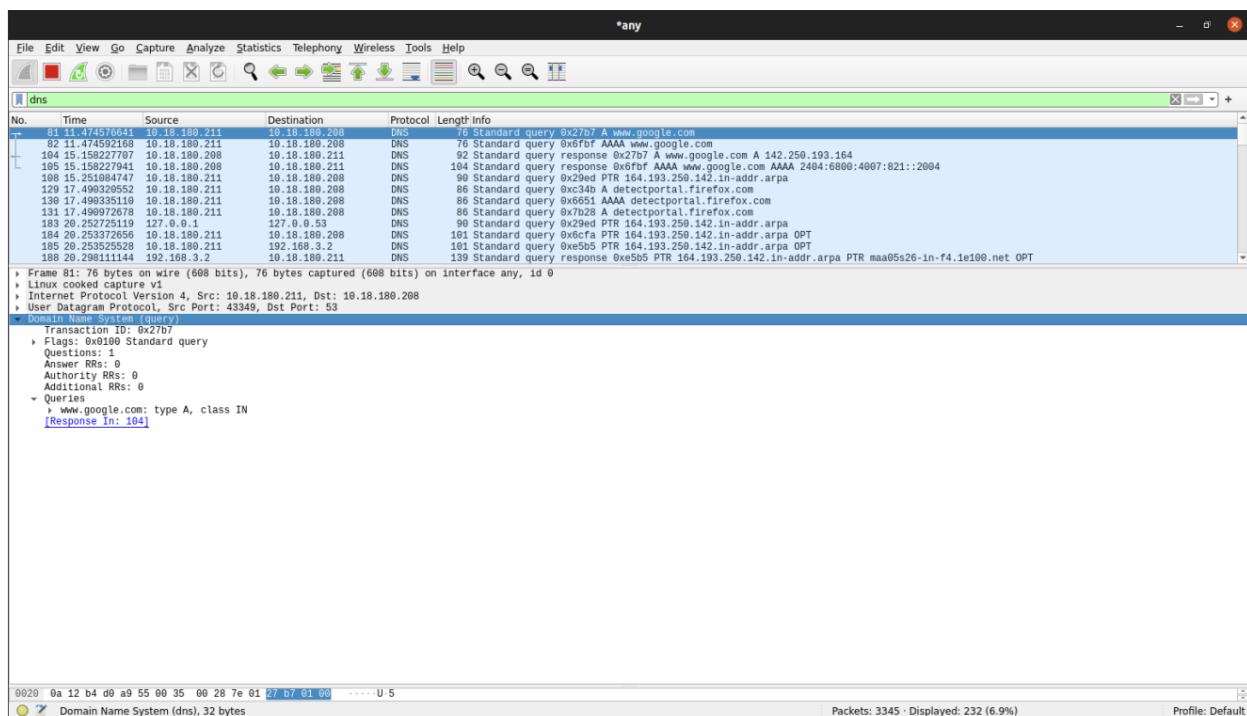
    listen-on-v6 { any; };
    dump-file "/var/cache/bind/dump.db";
};


```

OBservation 3:

pesu@pesu-OptiPlex-3070:~

```
pesu@pesu-OptiPlex-3070:~$ ping www.google.com
PING www.google.com (142.250.182.4) 56(84) bytes of data.
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=1 ttl=108 time=74.9 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=2 ttl=108 time=80.9 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=3 ttl=108 time=83.6 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=4 ttl=108 time=87.3 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=5 ttl=108 time=89.8 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=6 ttl=108 time=68.9 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=7 ttl=108 time=60.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=8 ttl=108 time=66.2 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=9 ttl=108 time=68.8 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=10 ttl=108 time=76.9 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=11 ttl=108 time=77.2 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=12 ttl=108 time=47.2 ms
```



OBservation 4:

```
[+] pesu@pesu-OptiPlex-3070:~$ sudo rndc dumpdb -cache  
pesu@pesu-OptiPlex-3070:~$ sudo rndc flush  
pesu@pesu-OptiPlex-3070:~$
```

```
[+] pesu@pesu-OptiPlex-3070:~$ pesu@pesu-OptiPlex-3070:~  
pesu@pesu-OptiPlex-3070:~$ sudo nano /etc/bind/named.conf  
pesu@pesu-OptiPlex-3070:~$ 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.apra" {  
type master;  
file "/etc/bind/10.2.22.db";  
};  
pesu@pesu-OptiPlex-3070:~$
```

```
$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 10.2.22.101
mail IN A 10.2.22.102
ns IN A 10.2.22.10
*.example.com. IN A 10.2.22.100
```

```
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
    2008111001
    8H
    2H
    4W
    1D)
@ IN NS ns.example.com.

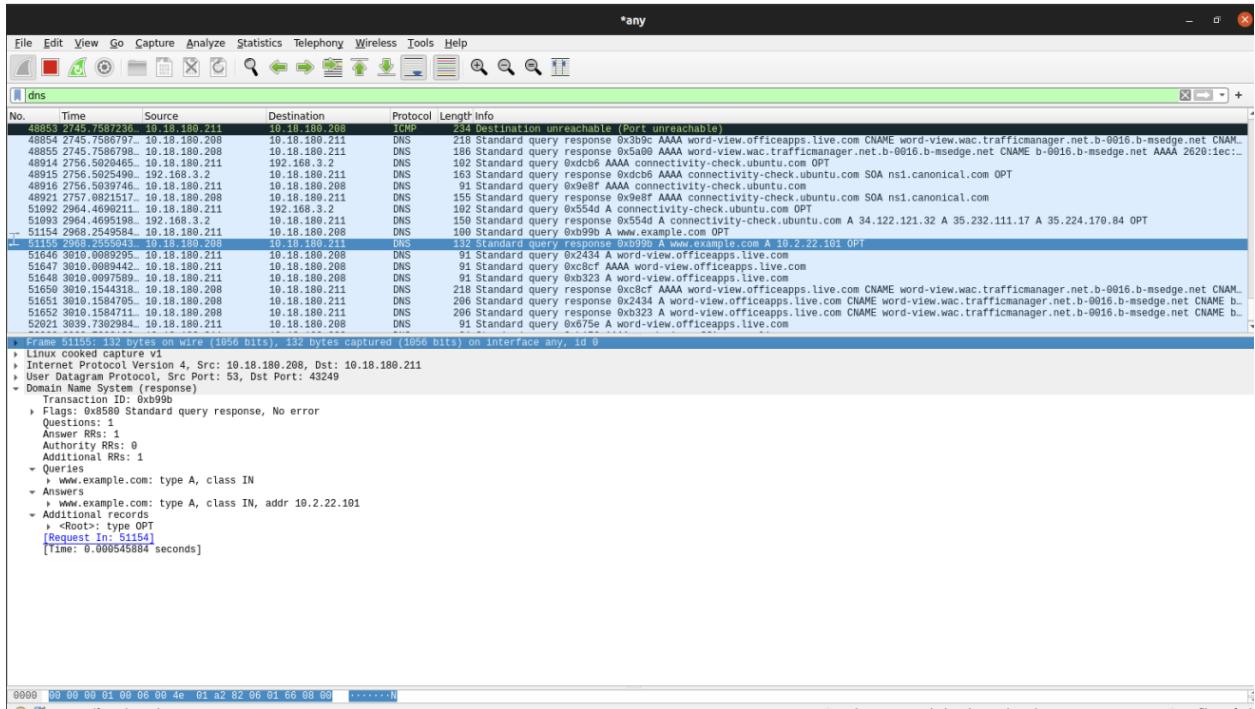
101 IN PTR www.example.com.
102 IN PTR mail.example.com.
10 IN PTR ns.example.com.
```

```
[+] pesu@pesu-OptiPlex-3070:~$ sudo cp 10.2.22.db /etc/bind  
[sudo] password for pesu:  
Sorry, try again.  
[sudo] password for pesu:  
pesu@pesu-OptiPlex-3070:~$ sudo cp example.com.db /etc/bind  
pesu@pesu-OptiPlex-3070:~$
```



```
[+] pesu@pesu-OptiPlex-3070:~$ sudo service bind9 restart  
pesu@pesu-OptiPlex-3070:~$ sudo cp 10.2.22.db /etc/bind  
pesu@pesu-OptiPlex-3070:~$ sudo service bind9 restart  
pesu@pesu-OptiPlex-3070:~$ dig www.example.com  
  
; <>> DiG 9.16.8-Ubuntu <>> www.example.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40628  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 65494  
;; QUESTION SECTION:  
;www.example.com. IN A  
  
;; ANSWER SECTION:  
www.example.com. 4940 IN A 93.184.216.34  
  
;; Query time: 0 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53)  
;; WHEN: Thu Mar 03 12:35:24 IST 2022  
;; MSG SIZE rcvd: 60  
  
pesu@pesu-OptiPlex-3070:~$
```

The answer section contains dns mapping. IP address of www.example.com is now 10.2.22.184



OBSERVATION NOTEBOOK REQUIREMENTS:

1. The DNS query and response messages are sent over UDP.
2. Destination port for DNS query message: 10.2.22.184 , source port of dns response: 10.2.22.184
3. IP address is same for DNS server and destination of dns query.
4. It is TYPE A query message. Answers in query messages displays the record resources.
5. 4 answers. The answers contain the record resources: the name,value,type and rtt
6. Yes.