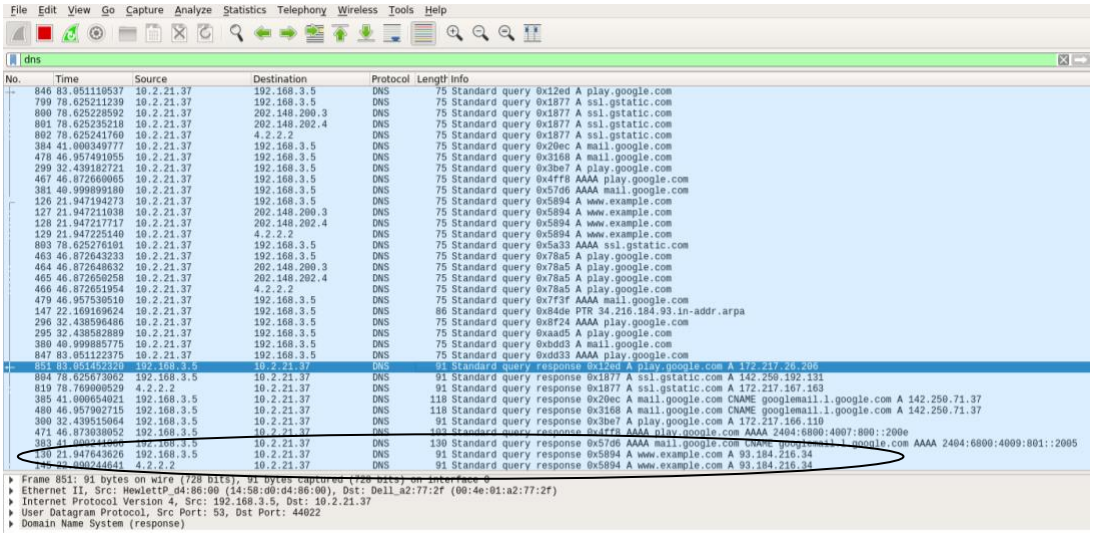
Computer Networks Lab – Week 4
SRN : PES1UG19CS542
Name: Trisha Jain

1. First Test – Pinging before setting up DNS

Wireshark captures packets in while pinging www.example.com
The query is of type A which stands for authoritative.

```
student@pesu-OptiPlex-3070:~$ ping www.example.com
PING www.example.com (93.184.216.34) 56(84) bytes of data.
64 bytes from 93.184.216.34: icmp_seq=1 ttl=52 time=220 ms
64 bytes from 93.184.216.34: icmp_seq=2 ttl=52 time=220 ms
64 bytes from 93.184.216.34: icmp_seq=3 ttl=52 time=220 ms
^C
--- www.example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
```



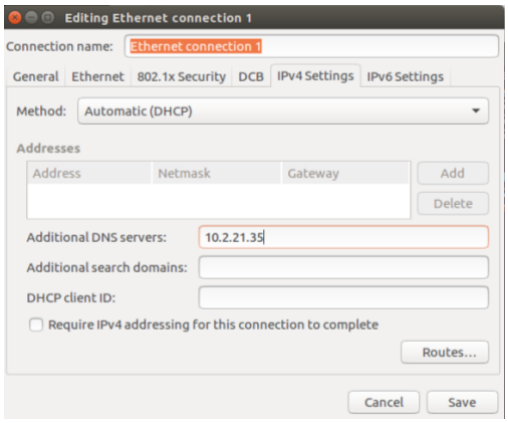
(Wireshark packet capture before DNS was set up)
First Test

2. Setting up a local DNS server

Task 1: Configuring the User Machine

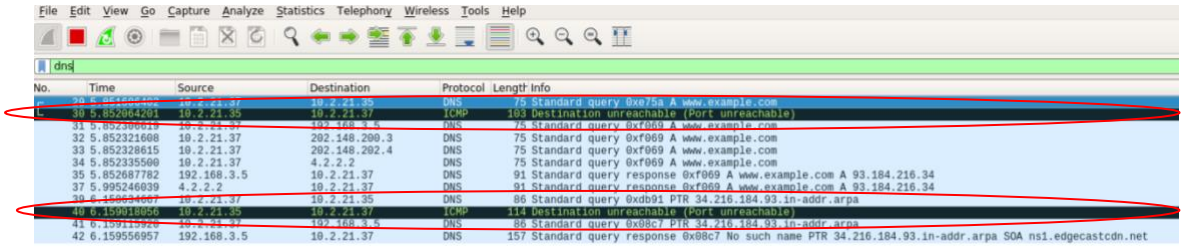
The IP Address of the Custom DNS Server is added to the client machine by adding the IP address of the server to the file : **/etc/resolvconf/resolv.conf.d/head**.
The IP address is also added to the DNS menu under the IPv4 settings.

```
student@pesu-OptiPlex-3070:~$ sudo nano /etc/resolvconf/resolv.conf.d/head
[sudo] password for student:
student@pesu-OptiPlex-3070:~$ sudo resolvconf -u
```



3. Second Test

We ping www.example.com again



The client tries to get the record from the DNS Server 10.2.21.35 but it doesn't get it so it gives an error.

We obtain a destination unreachable error as server machine does not have a DNS server associated with it.

4. Setting up a local DNS Server (In the server Machine)

The bind9 server is installed using the **sudo apt install bind9** command.

```
student@pesu-OptiPlex-3070:~$ sudo apt-get update && sudo apt-get install bind9
[sudo] password for student:
```

The server had the configuration file **/etc/bind/named.conf.options** that needs to be accessed to specify the dumpfile where the cache can be dumped.

```
student@pesu-OptiPlex-3070:~$ sudo 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;

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
        dump-file "/var/cache/bind/named_dump.db";
};
```

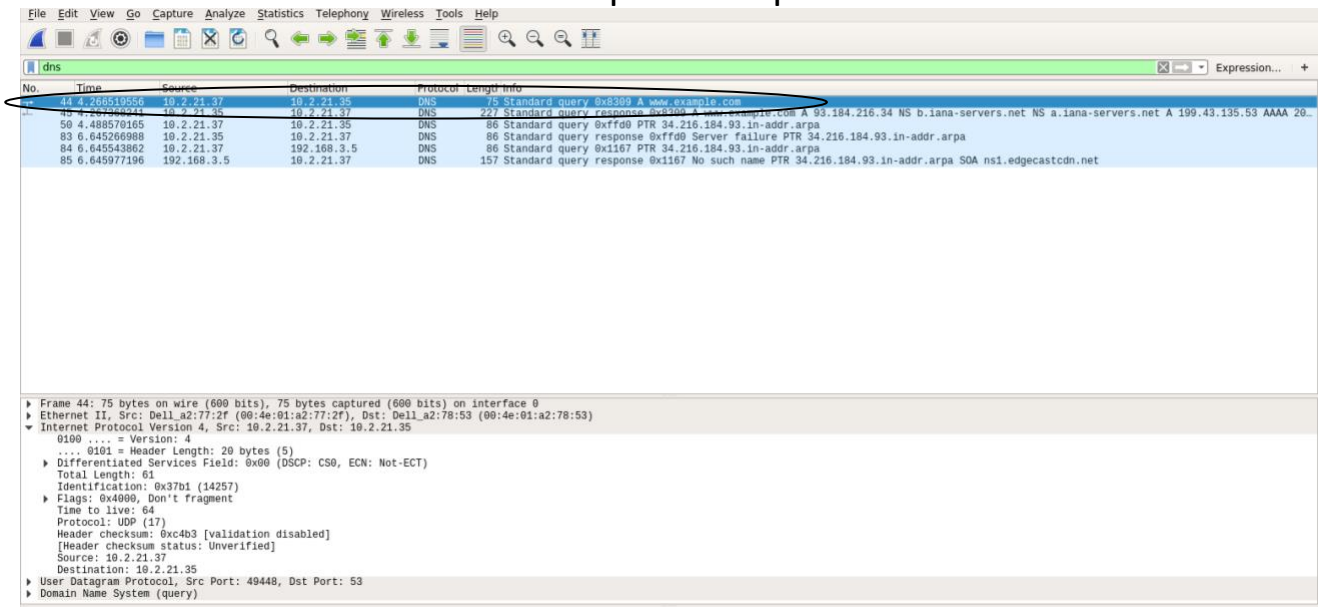
The cache can be dumped using the command **sudo rndc dumpdb -cache** and can be flushed using the command **sudo rndc flush.**

```
student@pesu-OptiPlex-3070:~$ sudo rndc dumpdb -cache
student@pesu-OptiPlex-3070:~$
```

```
student@pesu-OptiPlex-3070:~$ sudo rndc flush
student@pesu-OptiPlex-3070:~$
```

5. Third Test

Example.com is pinged again and now that the DNS server is set up there is no error in the Wireshark packet capture.



6. Task 3 - Hosting a zone in the local DNS Server

The two zones corresponding to www.example.com are added to the **/etc/bind/named.conf** file in the server. The first zone corresponds to forward lookup and the second zone corresponds to backward lookup.

```
student@pesu-OptiPlex-3070:~$ 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 "21.2.10.in-addr.arpa" {
type master;
file "/etc/bind/10.2.21.db";
};
```

The forward lookup file is put at the location **/etc/bind/example.com.db**

```
student@pesu-OptiPlex-3070:/etc/bind$ cat 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       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
```

The backward lookup file is put at the location **/etc/bind/10.2.21.db**

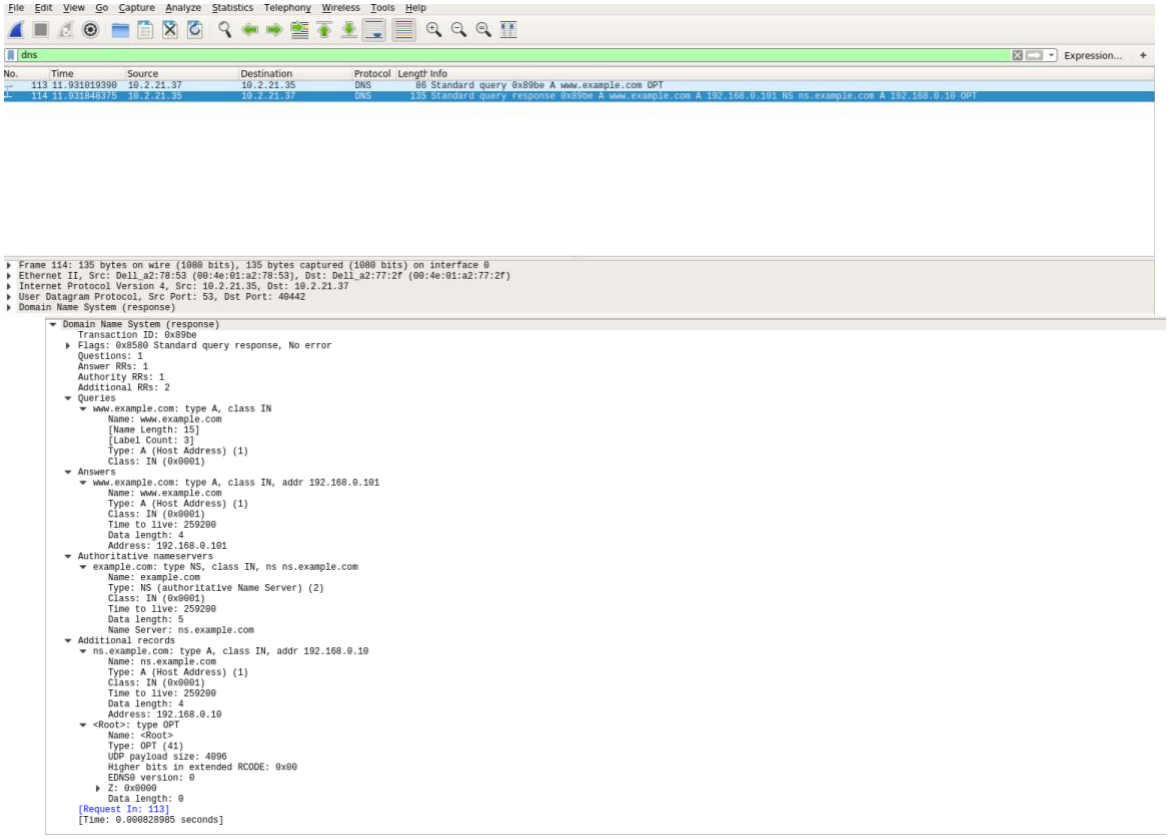
```
student@pesu-OptiPlex-3070:/etc/bind$ cat 10.2.21.db
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                2008111001
                8H
                2H
                4W
                1D)
@       IN      NS      ns.example.com.

101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
10      IN      PTR     ns.example.com.
student@pesu-OptiPlex-3070:/etc/bind$
```

7. Fourth test

The dig command is used to lookup named servers.
Wireshark is used to capture commands while running the command **dig www.example.com.**

```
student@pesu-OptiPlex-3070:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54388
;; 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       192.168.0.101

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168.0.10

;; Query time: 0 msec
;; SERVER: 10.2.21.35#53(10.2.21.35)
;; WHEN: Tue Feb 16 14:48:33 IST 2021
;; MSG SIZE  rcvd: 93
```

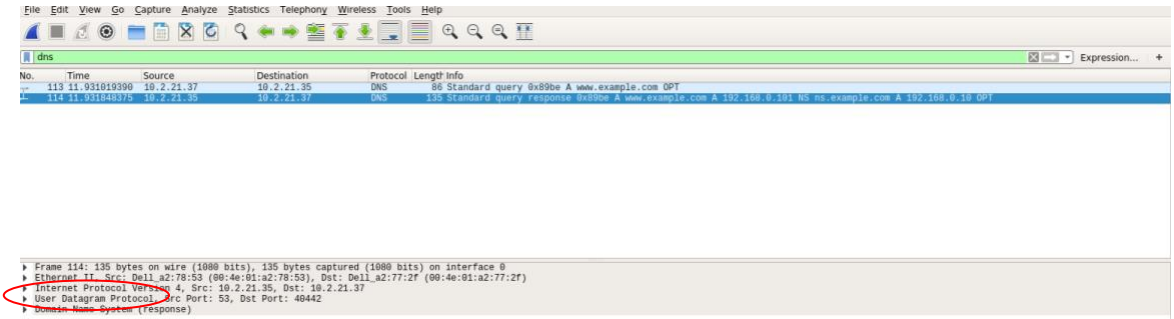
Wireshark capture :-



Observations : -

Q1. **Locate the DNS query and response messages. Are they sent over UDP or TCP ?**

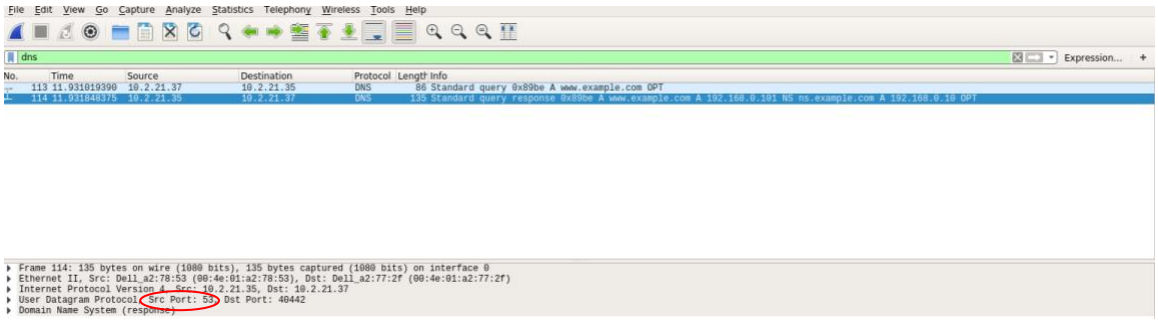
A1.



As it is clear from the screenshot : DCP messages are sent over UDP.

Q2. **What is the destination port for the DNS query message? What is the source port of the DNS response message?**

A2. The port number for both the destination for query message and source for response message is the same. It is 53. As it is seen in the screenshot pasted.



Q3**. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of the local DNS server. Are these two IP addresses the same?**

A3. The DNS query message is sent to the IP address of the local DNS server which is 10.2.21.35.

```
student@pesu-OptiPlex-3070:~$ ifconfig
enp1s0    Link encap:Ethernet  HWaddr 00:4e:01:a2:78:53
          inet addr:10.2.21.35  Bcast:10.2.21.255  Mask:255.255.255.0
          inet6 addr: fe80::a415:4b3e:93cf:8b35/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:30035 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22661488 (22.6 MB)  TX bytes:2974915 (2.9 MB)
```

Q4. **Examine the DNS query message. What TYPE of DNS query is it? Does the query message contain any ANSWERS?**

A4. The type is A which stands for Authoritative. Since the request is made for an authoritative record. And the query method's answer section is empty since it does not contain any answers.

Q5. **Examine the DNS response message. How many ANSWERS are provided? What do these answers contain?**

A5. The answer section of the DNS response message contains one resource record. The resource record shows the name of the host, type of request, address of the host.

Q6. **Consider the subsequent TCP SYN packet sent by the host. Does the destination IP address of the SYN packet correspond to any of the IP address provided in the DNS response message?**

A6. The destination IP address of the SYN packet corresponds to the IP address of the hostname(www.example.com) retrieved from the response message.