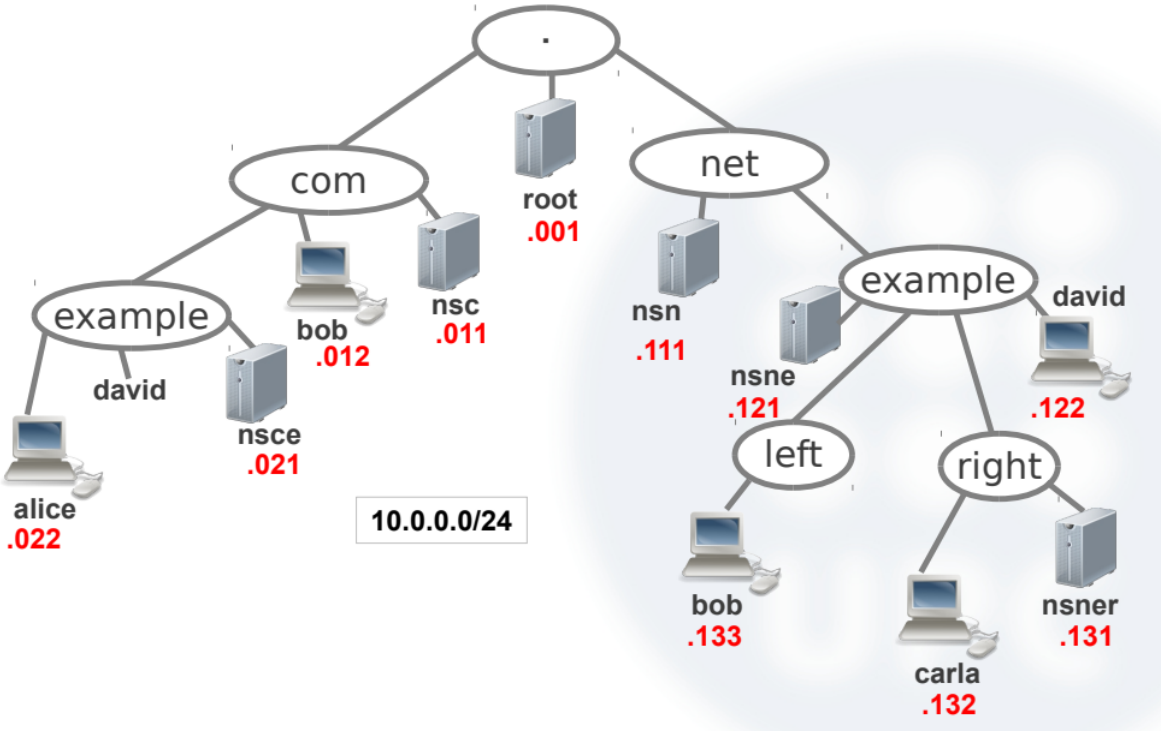
P4: DNS



Exercise 1.1– In this exercise, we are going to study the DNS service using the scenario of Figure 1.15. Before the practice you must answer some questions. To answer consider that ROOT-SERVER is the master of the reverse zone and that it delegates .com to nsc.com and .net to nsn.net. Consider also that nsc.com delegates example.com to nsce.example.com and that nsn.net delegates example.net to nsne.example.net. Finally, consider that nsne.example.net must be configured with a single zone for the zone example.net (single configuration file) and that it must delegate right.example.net to nsner.right.example.net. According to the previous considerations about our DNS tree, explain in which server we should find the following resource records (RR):

• An A record for peter.example.com
nsce
• An A record for peter.left.example.net
nsne
• An A record for peter.right.example.net
nsner
• The SOA record of right.example.net
nsner
• A PTR record for peter.example.com //all the ptr are located in root server
ROOT-SERVER
• A MX record for right.example.net
nsner
• A MX record for left.example.net

nsne,
• A NS record for right.example.net
nsne,nsner

//en terminal
simctl dns-basic sh
start
exec initial

1. Get a console at alice and looking at the configuration explain which is the name server used by this host.
//en alice
host alice

```
alice:~# host alice
alice.example.com has address 10.0.0.22
```

dig alice

```
alice:~# dig alice

; <<>> DiG 9.6-ESV-R4 <<>> alice
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 47453
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;alice.                         IN      A

;; AUTHORITY SECTION:
.                       0       IN      SOA     ROOT-SERVER. admin-mail.ROOT-SERVER.
2006031201 28800 14400 3600000 0

;; Query time: 44 msec
;; SERVER: 10.0.0.21#53(10.0.0.21)
;; WHEN: Sat Oct 22 11:36:22 2022
;; MSG SIZE  rcvd: 80
```

the server used by host is nsce (10.0.0.21)

2. Identify which is the server of the zone example.com and describe the configuration of this zone.

//from nsce
cat /etc/bind/named.conf
cat /etc/bind/db.com.example

```
nsce:~# cat /etc/bind/db.com.example
; /etc/bind/db.com.example
$ORIGIN example.com.
$TTL    60000
@       IN   SOA   nsce  admin-mail.nsce (
2006031201 ; serial
28 ; refresh
14 ; retry
3600000 ; expire
20 ; 20 secs of negative cache ttl
)
@                   IN   NS     nsce       ; unqualified name
nsce                IN   A      10.0.0.21
david               IN   CNAME  david.example.net.
@                   IN   MX   10 mailserver1
@                   IN   MX   20 mailserver2.example.com.
alice               IN   A      10.0.0.22
mailserver1         IN   A      10.0.0.25
mailserver2         IN   A      10.0.0.26
```

the server of the zone example.com with alice is nsce. Alice and nsce are the devices form this zone and david is an alias for the david.example.net.

$ORIGIN example.com, is used to add unqualified names(those which aren't FQDN,(ended without .)). i.e : nsce = nsce.example.com
@ = same as origin
CNAME= alias
MX= mail servers of the domain

3. In nsce using the command netstat, identify the name of the DNS server process.
//en nsce
netstat -ulpn -# u cz now dns is udp

```
nsce:~# netstat -ulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 0.0.0.0:2048            0.0.0.0:*                           946/rpc.statd
udp        0      0 127.0.0.1:53            0.0.0.0:*                           1167/named
udp        0      0 10.0.0.21:53            0.0.0.0:*                           1167/named
udp        0      0 0.0.0.0:698             0.0.0.0:*                           946/rpc.statd
udp        0      0 0.0.0.0:111             0.0.0.0:*                           935/portmap
```

DNS port id UDP 53 so we can see the dns server process are named with PID 1167.

4. In this exercise, we analyze a simple query from alice. In first place, reset the name servers processes and then, capture with wireshark tap0 and explain the output of the following command:
//en terminal
exec resetbind

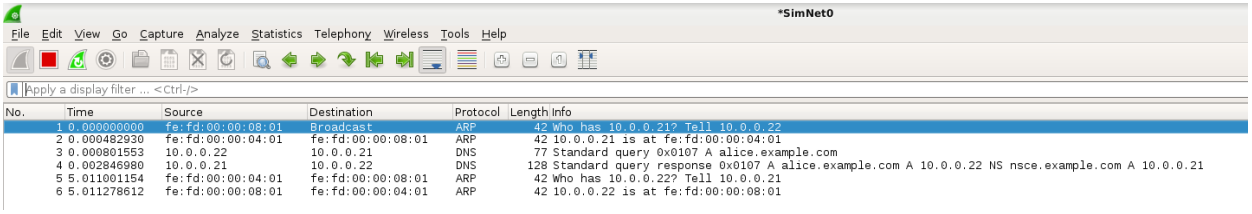
```
dns-basic-> exec resetbind
Virtual machines group: nsner nsne nsn nsce nsc joker root
OK The command has been started successfully.
OK The command has been started successfully.
OK The command has been started successfully.
OK The command has been started successfully.
OK The command has been started successfully.
OK The command has been started successfully.
OK The command has been started successfully.
Total time elapsed: 1 seconds
```

//en alice

dig alice.example.com

```
alice:~# dig alice.example.com

; <<>> DiG 9.6-ESV-R4 <<>> alice.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 263
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;alice.example.com.             IN      A

;; ANSWER SECTION:
alice.example.com.      60000   IN      A       10.0.0.22

;; AUTHORITY SECTION:
example.com.            60000   IN      NS      nsce.example.com.

;; ADDITIONAL SECTION:
nsce.example.com.       60000   IN      A       10.0.0.21

;; Query time: 31 msec
;; SERVER: 10.0.0.21#53(10.0.0.21)
;; WHEN: Fri Oct  7 19:08:53 2022
;; MSG SIZE  rcvd: 86
```

flags qr= query, aa= authoritative, rd= recursion desired, ra=(recursion available)



5. Using dig, try to resolve the IP address of joker.example.com. Did you find any resolution for this name? Discuss the results.

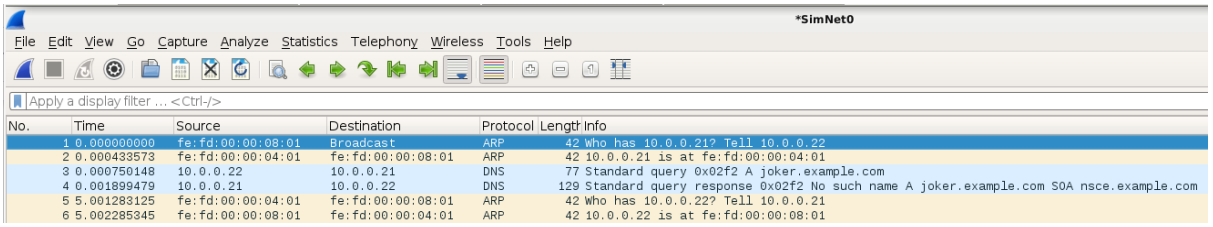
//from alice

dig joker.example.com

```
alice:~# dig joker.example.com

; <<>> DiG 9.6-ESV-R4 <<>> joker.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 754
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;joker.example.com.             IN      A

;; AUTHORITY SECTION:
example.com.            20      IN      SOA     nsce.example.com. admin-mail.nsce.example.com. 2006031201 28 14 3600000 20

;; Query time: 35 msec
;; SERVER: 10.0.0.21#53(10.0.0.21)
;; WHEN: Fri Oct  7 19:41:31 2022
;; MSG SIZE  rcvd: 87
```

The server messages us NXDOMAIN, which means the translation for jokers is not found.

We can also observe the SOA and conclude that the nsce has the maximum information of joker and the TTL is 20.



There is no resolution for this name because in example.com. There is no joker. We can see the dns query and query response frame.

6. Add the adequate RR in the appropriate server to map the name joker.example.com to the IP address 10.0.0.201. Reset the name server to load the configuration and explain how you test your configuration with dig and ping.

//from nsce

cd /etc/bind

cat name.conf

```
zone "example.com" {
        type master;
        file "/etc/bind/db.com.example";
};
```

nano db.com.example

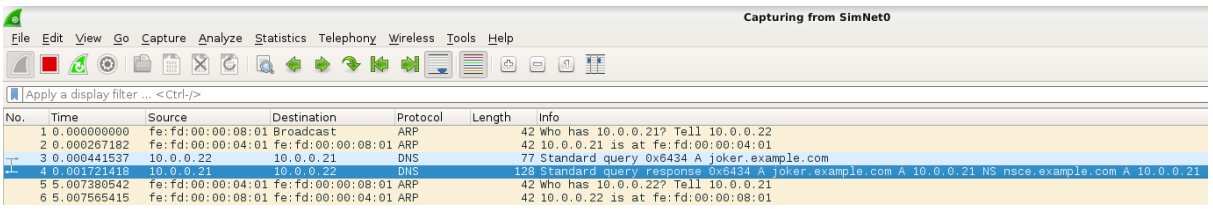
```
nsce.4153.0
File  Edit  View  Search  Terminal  Help
 GNU nano 2.0.7            File: db.com.example

; /etc/bind/db.com.example
$ORIGIN example.com.
$TTL    60000
@       IN   SOA   nsce  admin-mail.nsce (
2006031201 ; serial
28 ; refresh
14 ; retry
3600000 ; expire
20 ; 20 secs of negative cache ttl
)
@                   IN   NS     nsce       ; unqualified name
nsce                IN   A      10.0.0.21
david               IN   CNAME  david.example.net.
@                   IN   MX   10 mailserver1
@                   IN   MX   20 mailserver2.example.com.
alice               IN   A      10.0.0.22
mailserver1         IN   A      10.0.0.25
mailserver2         IN   A      10.0.0.26
joker               IN   A      10.0.0.21
                          [ Wrote 19 lines ]
```

joker has ip 10.0.0.201

//from terminal
exec resetbind
exec start

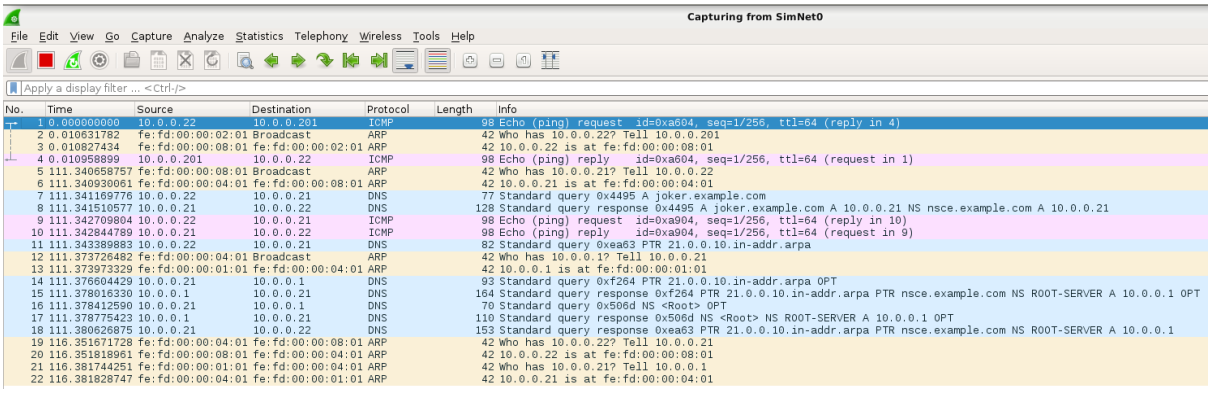
//from alice
dig joker.example.com.

```
alice:~# dig joker.example.com.

; <<>> DiG 9.6-ESV-R4 <<>> joker.example.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62057
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;joker.example.com.             IN      A

;; ANSWER SECTION:
joker.example.com.      60000   IN      A       10.0.0.21

;; AUTHORITY SECTION:
example.com.            60000   IN      NS      nsce.example.com.

;; ADDITIONAL SECTION:
nsce.example.com.       60000   IN      A       10.0.0.21

;; Query time: 27 msec
;; SERVER: 10.0.0.21#53(10.0.0.21)
;; WHEN: Fri Oct 14 19:04:51 2022
;; MSG SIZE  rcvd: 86
```



Now there is a resolution for the joker.example.com

//from alice
ping -c 1 joker.example.com.



WIth dig we obtain the info of joker and we can do some requests. (con commando de dig -...)
with ping we reach joker.

7. Which IP address will be contacted by a mail server if it has to send an e-mail to john@example.com.
//from nsce
cat /etc/bind/db.com.example
here we obtain the SOA file where we can see the 1st mailserver1 has ip 10.0.0.25

8. Try the following command: alice:~# dig -t MX example.com

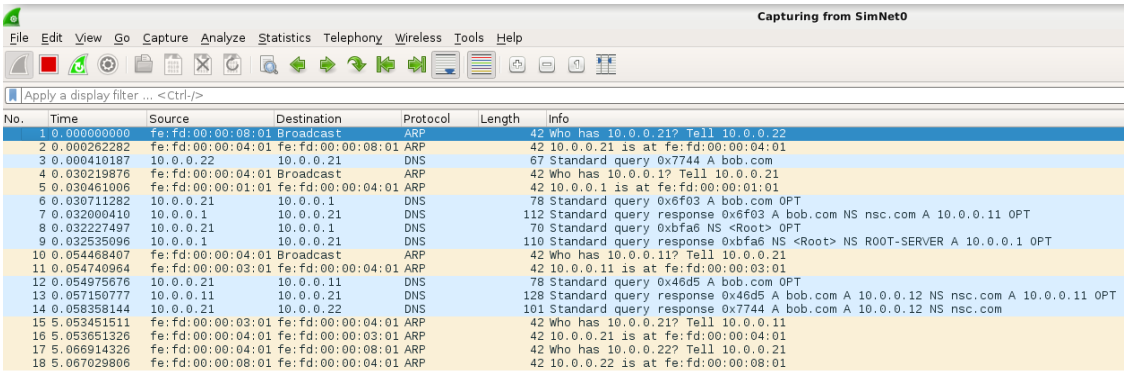
```
alice:~# dig -t MX example.com

; <<>> DiG 9.6-ESV-R4 <<>> -t MX example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4310
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 3

;; QUESTION SECTION:
;example.com.                   IN      MX

;; ANSWER SECTION:
example.com.            60000   IN      MX      10 mailserver1.example.com.
example.com.            60000   IN      MX      20 mailserver2.example.com.

;; AUTHORITY SECTION:
example.com.            60000   IN      NS      nsce.example.com.

;; ADDITIONAL SECTION:
mailserver1.example.com. 60000  IN      A       10.0.0.25
mailserver2.example.com. 60000  IN      A       10.0.0.26
nsce.example.com.       60000   IN      A       10.0.0.21

;; Query time: 6 msec
;; SERVER: 10.0.0.21#53(10.0.0.21)
;; WHEN: Sat Oct 15 13:38:16 2022
;; MSG SIZE  rcvd: 152
```

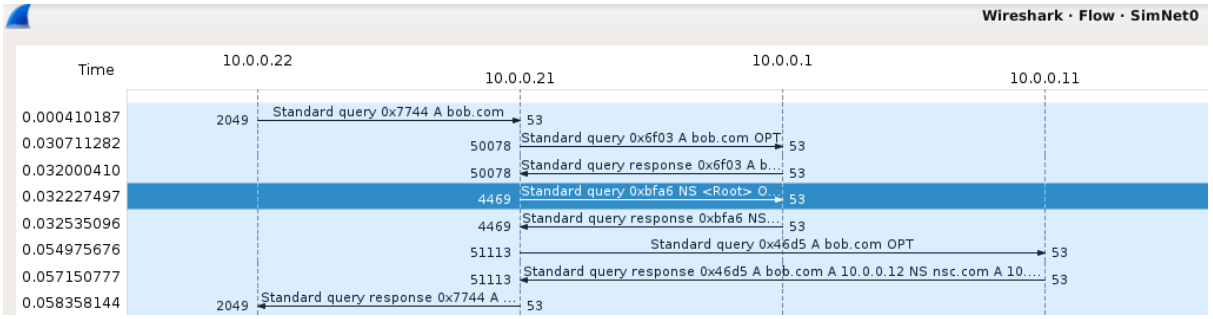
-t =type
Its give us information about which servers controls the MX(mail eXchanger)

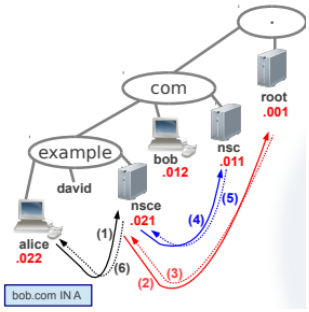
Exercise 1.2– Using the scenario dns-basic, in this exercise we analyze the recursive queries and the caching strategy of DNS.

1. In this exercise, we analyze a recursive query from alice. To do so, reset the name servers processes of the scenario, capture with wireshark tap0 and explain the flow of DNS messages captured when executing the following command line: alice:~# dig bob.com
//from terminal
exec resetbind

//from alice
dig bob.com





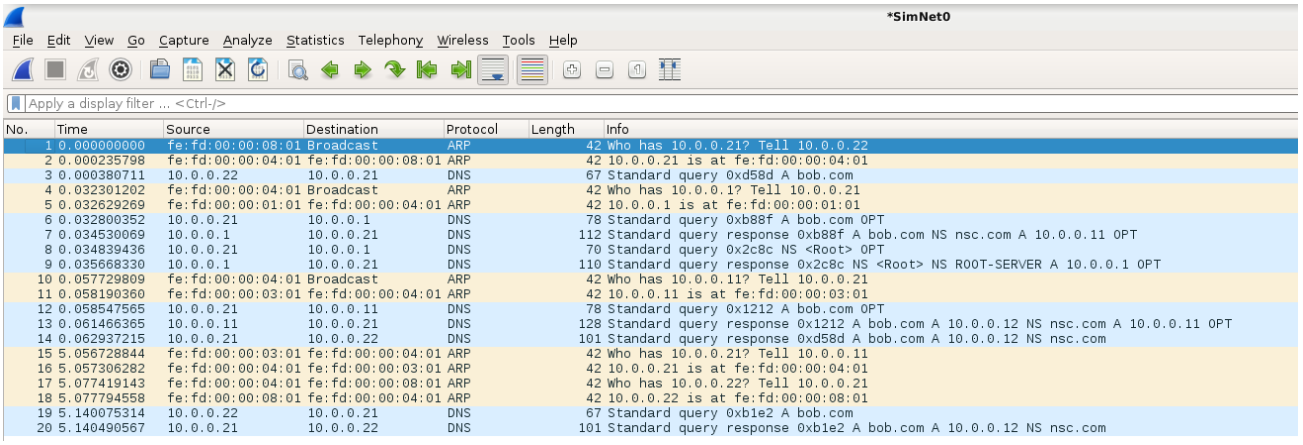


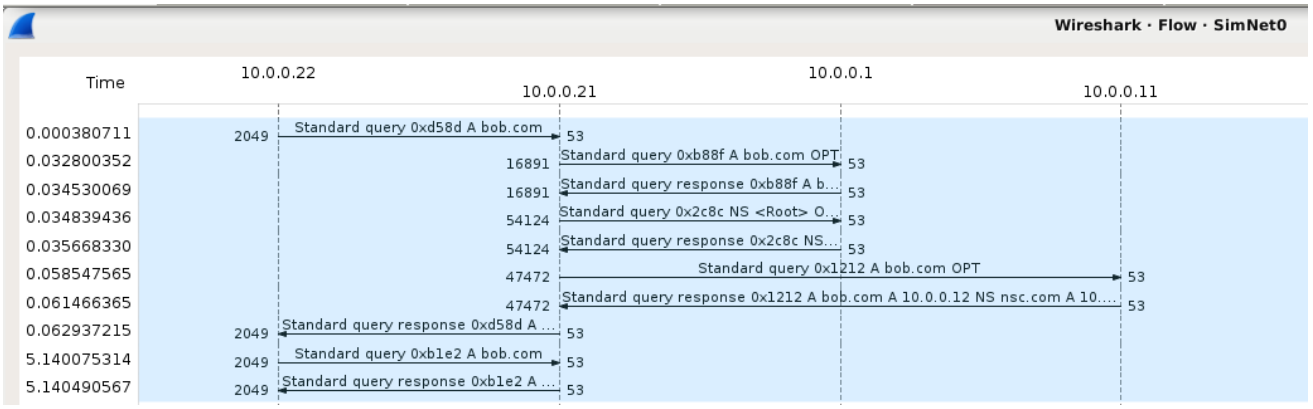
The flow of dns is following

1) **alice** sends a recursive query for the A register of bob.com to **nsce**.
2) **nsce** sends an iterative query for the A record of bob.com to **root**.
3) **root** sends query response for the A record of bob.com which is in nsc.com.
4) **nsce** also asks for the NS record of the **root.**
5) **root** provides its NS/A and the NS/A records of **nsc**, which is who serves .com
6) Then,**nsce** sends an iterative query to **nsc** for A record for bob.com
7) Then, **nsc** sends the A register of bob.com to **nsce**
8) Finally, **nsce** sends the A register of bob.com to **alice**

2. We analyze DNS caching in this exercise. To do so, reset the name servers processes of the scenario, capture with wireshark tap0 and explain the flow of DNS messages captured when executing the following command line:

//terminal
exec resetbind
dig bob.com ; sleep 5 ; dig bob.com





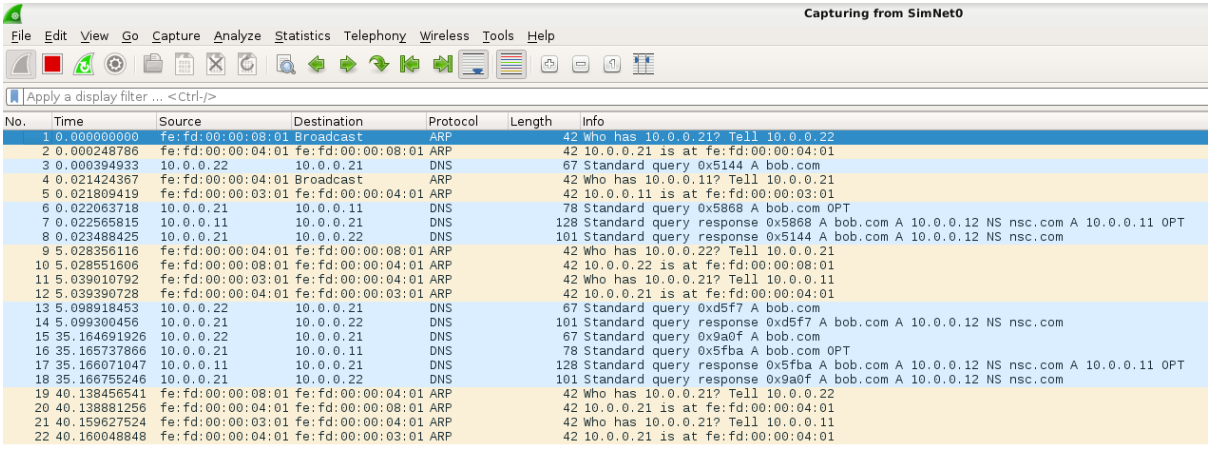
We got here same flow as in previous exercise for the first dig, but for the second dig the query is directly answered by bob its because the ttl is not expired.

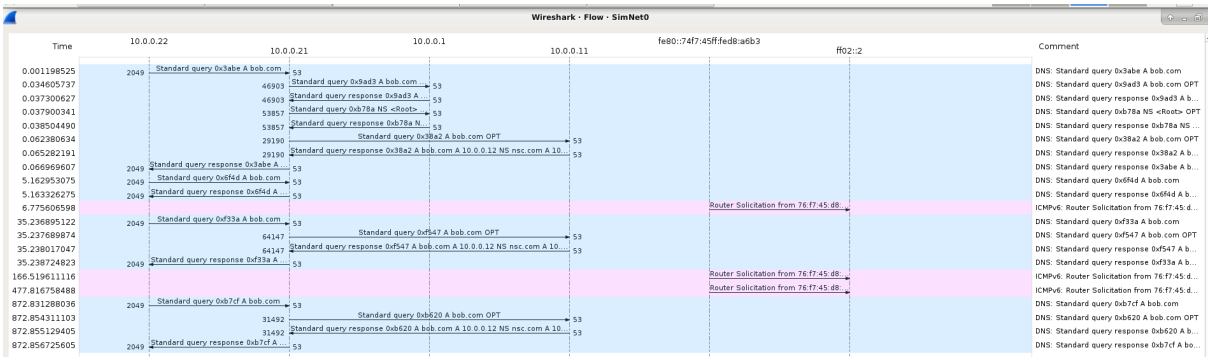
```
alice:~# dig bob.com

; <<>> DiG 9.6-ESV-R4 <<>> bob.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47055
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;bob.com.                       IN      A

;; ANSWER SECTION:
bob.com.                30      IN      A       10.0.0.12
```

bob has ttl 30 seg.

3. Continuing with the analysis of DNS caching, reset the name servers processes of the scenario, capture with wireshark tap0 and explain the flow of DNS messages captured when executing the following command line:

//terminal
exec resetbind
//from alice
dig bob.com ; sleep 5 ; dig bob.com ; sleep 30 ; dig bob.com

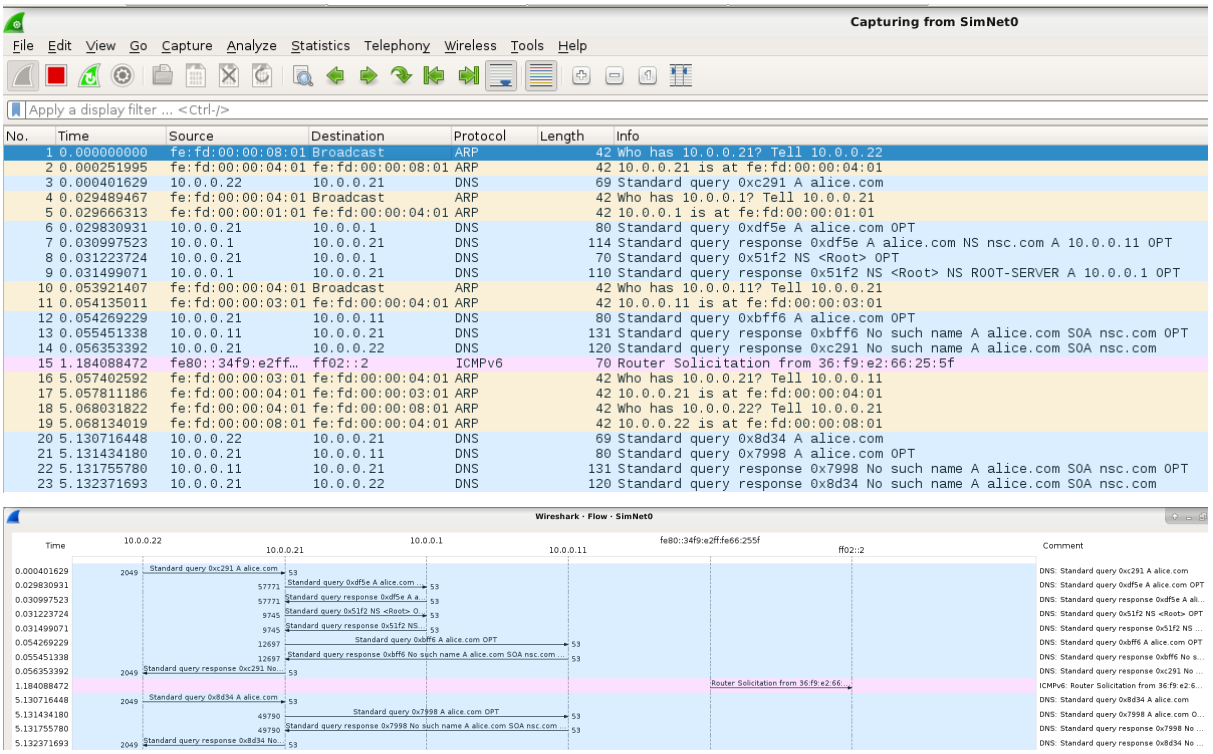




As we saw before, bob has ttl 30s so after that time the route that before was established is deleted and then, nsce has to send dns query to root again and do the same process of establishing a connection as in previous exercises.

4. Continuing with the analysis of DNS caching, reset the name servers processes of the scenario, capture with wireshark tap0 and explain the flow of DNS messages captured when executing the following command line:

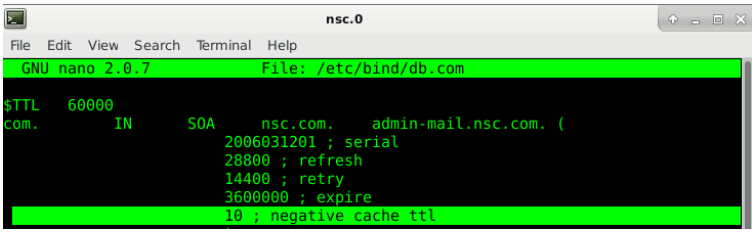
//terminal
exec resetbind
//from alice
dig alice.com ; sleep 5 ; dig alice.com



The flow is similar as before, but now in query response we obtain SOA form nsc because alice.com is not FQDN and it doesn't exist. We also can see, the second dig hasn't reached to the root although error and its because the negative TTL is not defined.

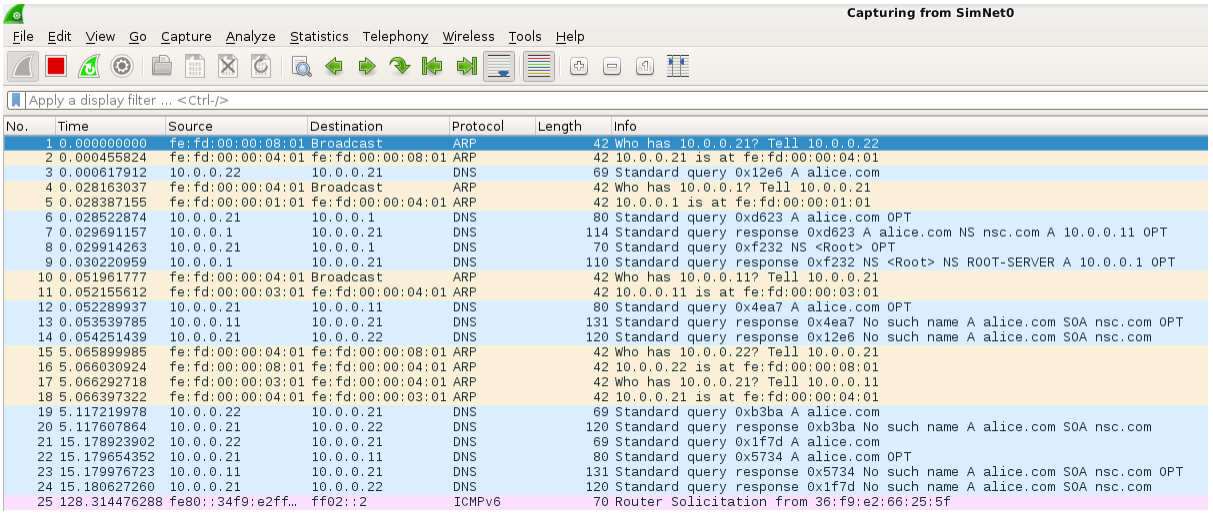
5. Set the negative cache TTL to 10 in the SOA of nsc. Reset the name servers processes of the scenario, capture with wireshark tap0 and explain the flow of DNS messages captured when executing the following command line:

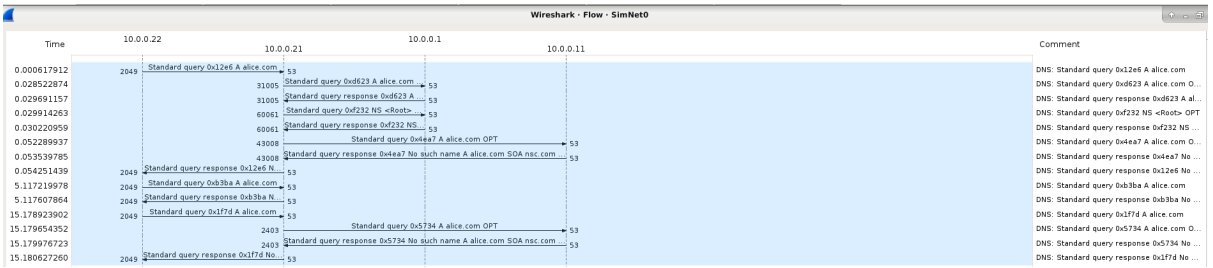
//from nsc
nano /etc/bind/db.com



//terminal
exec resetbind

//from alice
dig alice.com ; sleep 5 ; dig alice.com ; sleep 10 ; dig alice.com





First dig follows the same path as always, alice->nsce->root->nsce->nsc->nsce->alice
The second one doesn't go through root because it's under 10s.
The third dig goes from beginning because the ttl is 0 and the flow established before is deleted.

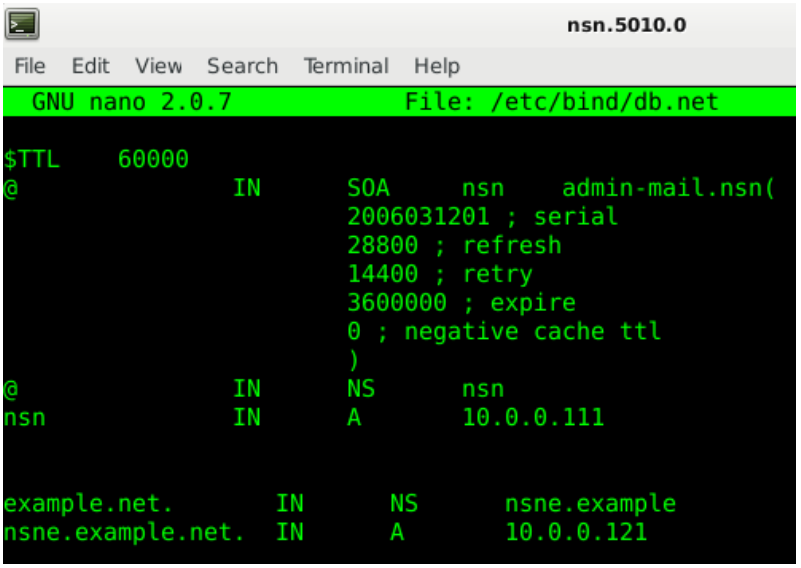
Exercise 1.3– (*) Using the scenario dns-basic, you have to configure the name servers and zones of .net.

1. In your configuration consider that nsne must be configured with a single zone for example.net (single configuration file) and that it must delegate right.example.net to nsner.

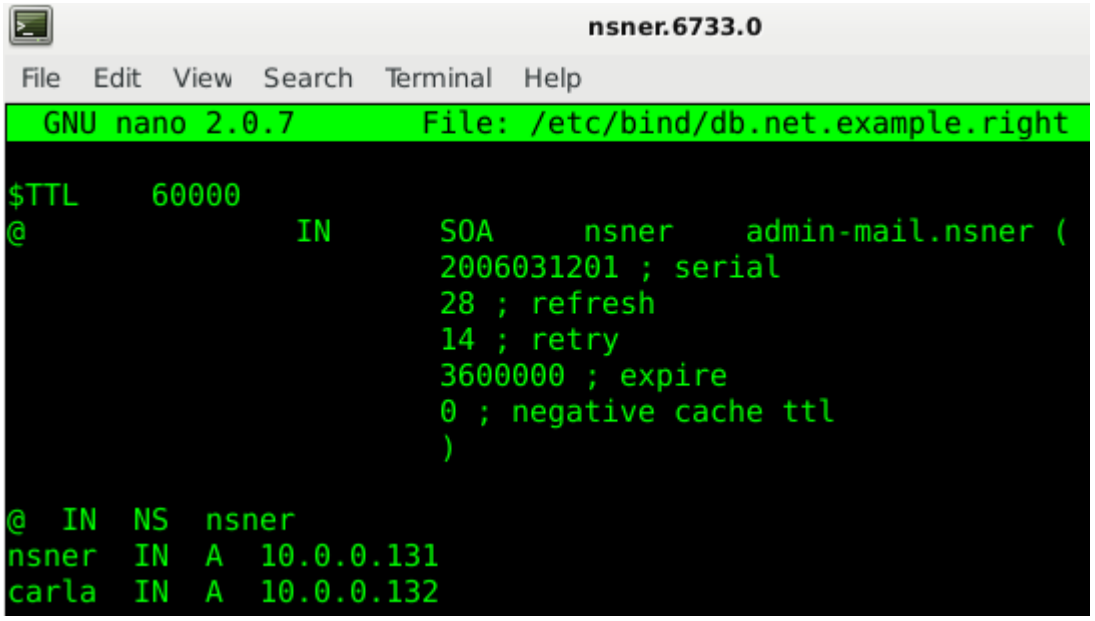
Modify the configuration files of nsn, nsne, and nsner appropriately and describe and test your configuration.

//terminal
exec resetbind

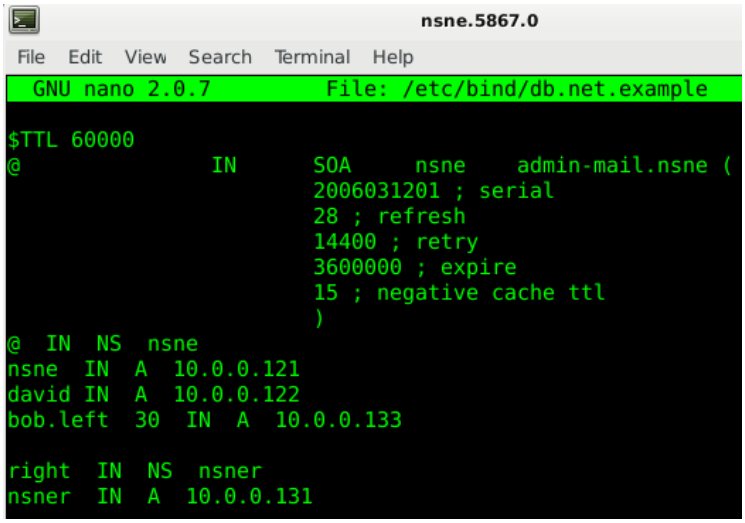
//from nsn
nano /etc/bind/db.net



//from nsner
nano /etc/bind/db.net.example.right



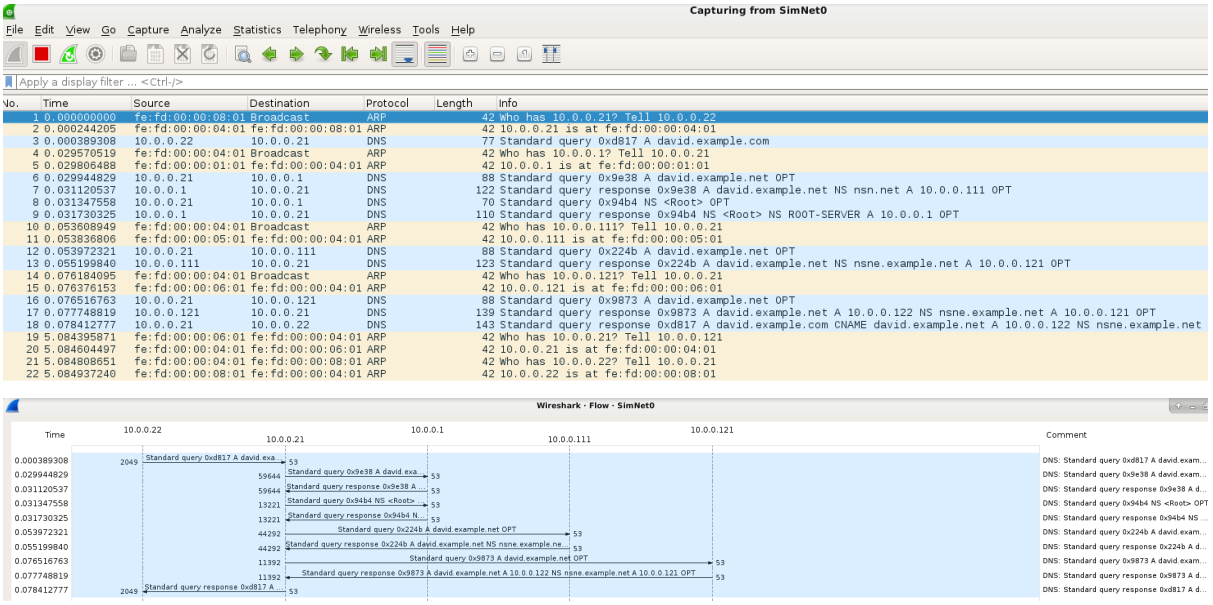
//from nsne
nano /etc/bind/db.net.example



2. Notice that the server nsn has a mistake in its initial configuration file, describe this mistake.
initially there was a "." missing at the end and the domains were interpreted as no qualified names.

3. After you have implemented the configuration, reset bind in all the name servers of the scenario, capture with wireshark tap0 and comment the traffic and the results observed when executing:
//terminal
exec resetbind

//alice
dig david.example.com



The flow is the same, but the particularity here is at the end we received a query response, one of the domain example.net. and other of the domain example.com.
Exercise 1.4– (*) In this exercise we study some more features of the DNS service using the same scenario.

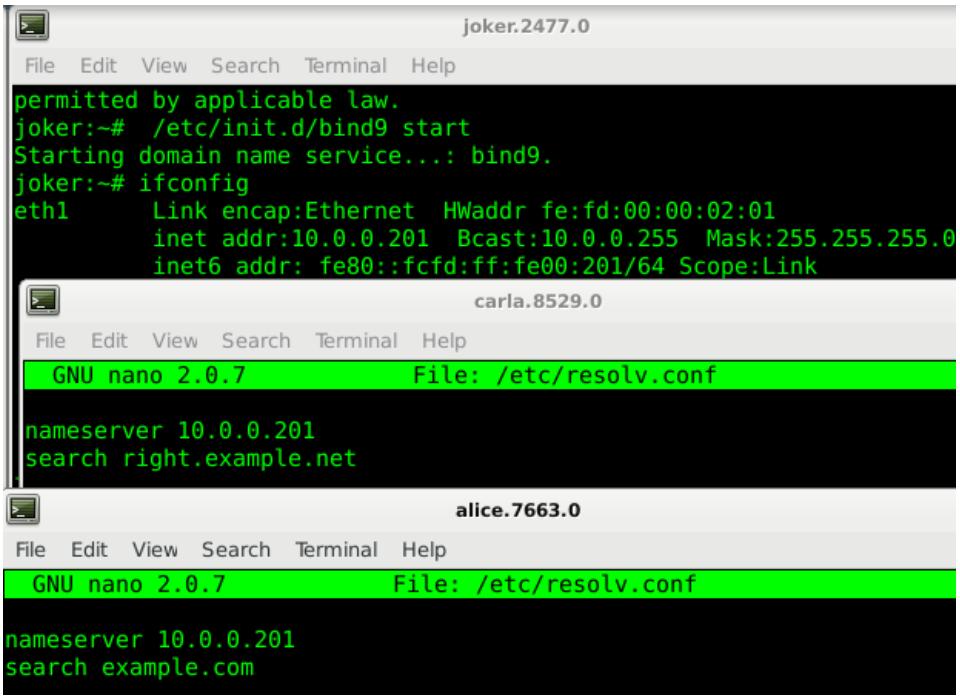
1. Use the machine joker as a DNS server just for caching and for making queries to the DNS tree on behalf of its clients. Make the clients alice and carla point to this server and test your configuration, for example asking for one register from alice and then, for the same register from carla.

//from joker

/etc/init.d/bind9 start

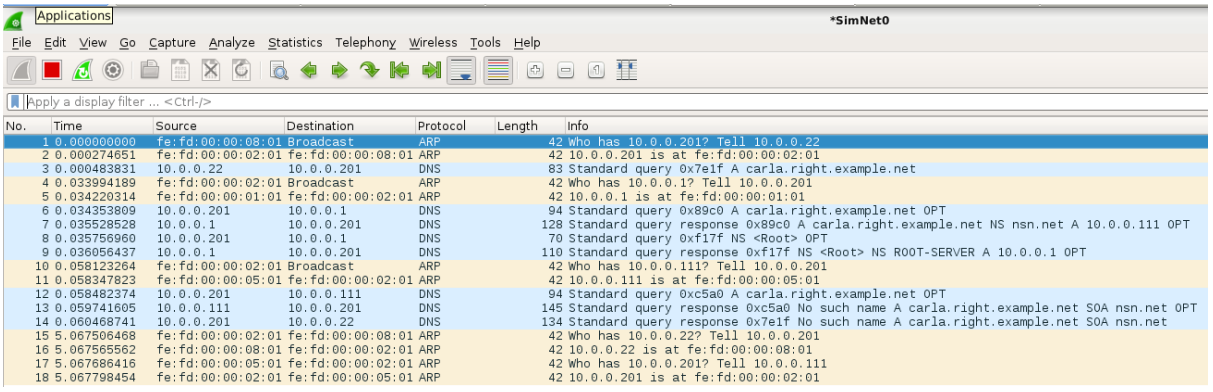
//from alice //from carla

ano /etc/resolv.conf

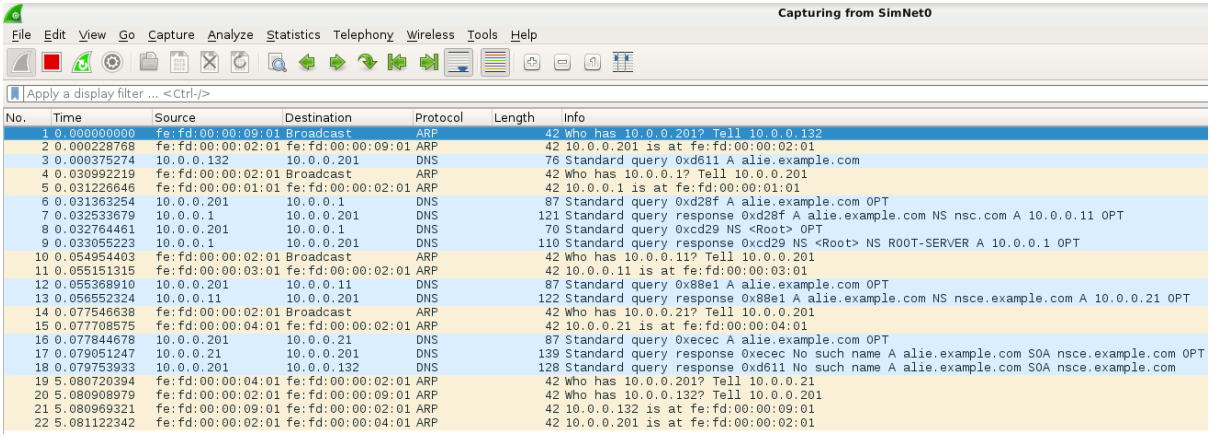


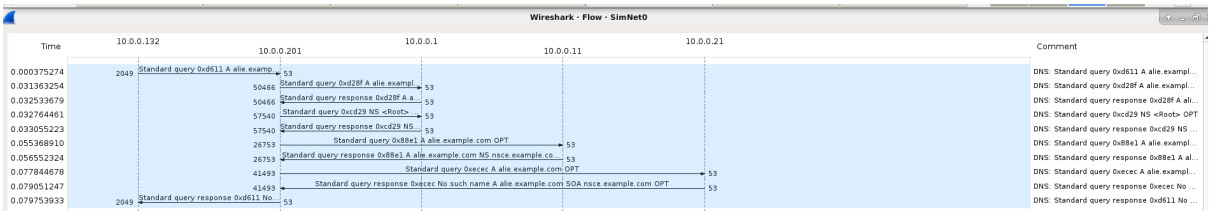
//from alice

dig carla.right.example.net



//from carla
dig alie.example.com





As we can see in both case, the joker does the function of the server who communicates with root to establish the path of alice and carla or vice versa.

2. Change the configuration to delegate the reverse lookup of all the IP addresses of the scenario to the machine joker. Describe how you test that your configuration is correct.