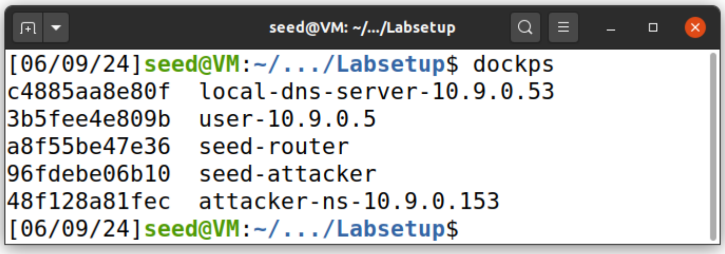
姓名：蔡佩蓉　　　學號：109511286

Local DNS Attack Lab (Lab7)

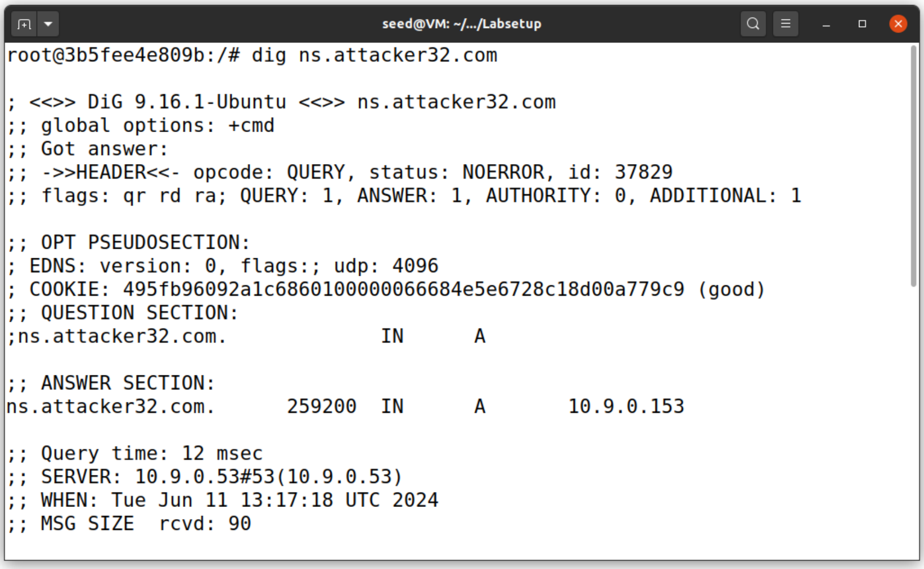
Task 1: Directly Spoofing Response to User



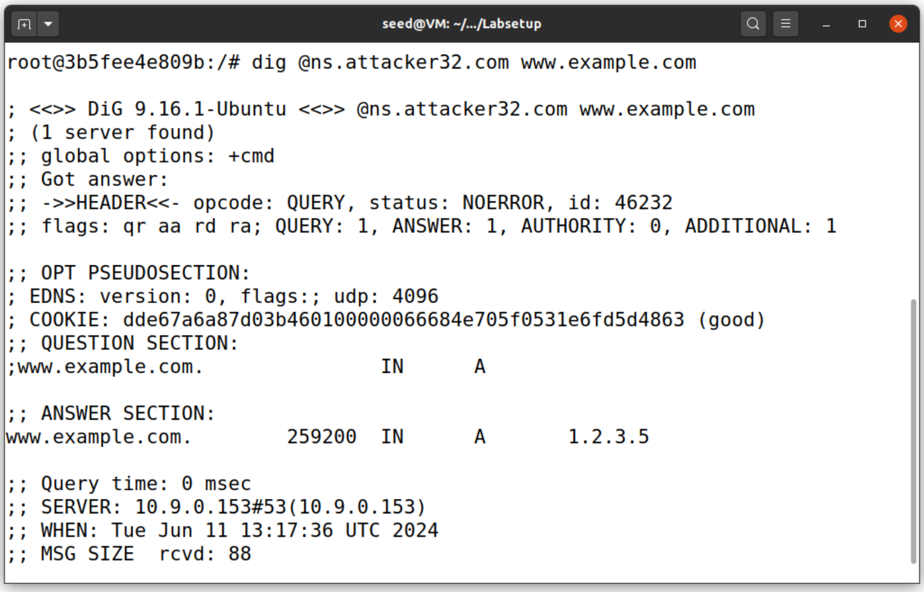
```
[06/09/24]seed@VM:~/.../Labsetup$ dockps
c4885aa8e80f  local-dns-server-10.9.0.53
3b5fee4e809b  user-10.9.0.5
a8f55be47e36  seed-router
96fdebe06b10  seed-attacker
48f128a81fec  attacker-ns-10.9.0.153
[06/09/24]seed@VM:~/.../Labsetup$
```

Before attack:

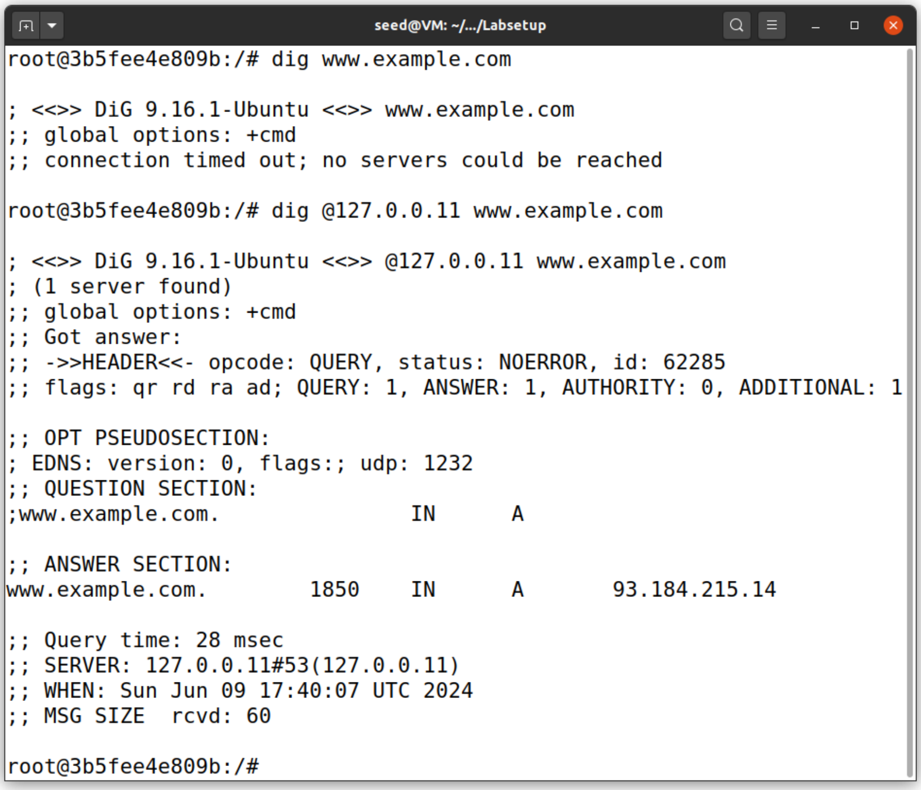
user-10.9.0.5:



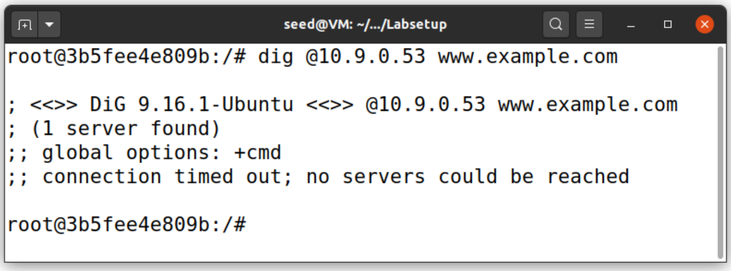
```
root@3b5fee4e809b:/# dig ns.attacker32.com

; <<>> DiG 9.16.1-Ubuntu <<>> ns.attacker32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37829
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 495fb96092a1c6860100000066684e5e6728c18d00a779c9 (good)
;; QUESTION SECTION:
;ns.attacker32.com.             IN      A

;; ANSWER SECTION:
ns.attacker32.com.      259200  IN      A       10.9.0.153

;; Query time: 12 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jun 11 13:17:18 UTC 2024
;; MSG SIZE  rcvd: 90
```



```
root@3b5fee4e809b:/# dig @ns.attacker32.com www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @ns.attacker32.com www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46232
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: dde67a6a87d03b460100000066684e705f0531e6fd5d4863 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.5

;; Query time: 0 msec
;; SERVER: 10.9.0.153#53(10.9.0.153)
;; WHEN: Tue Jun 11 13:17:36 UTC 2024
;; MSG SIZE  rcvd: 88
```

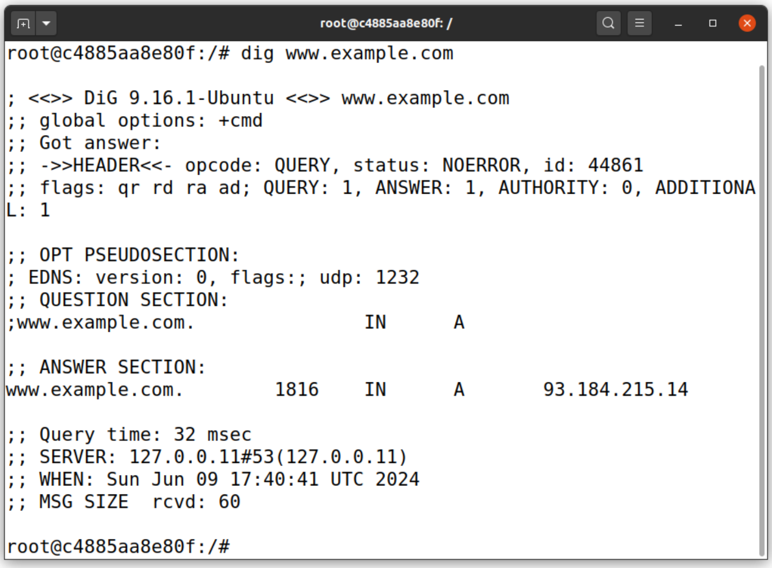


```
root@3b5fee4e809b:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; connection timed out; no servers could be reached

root@3b5fee4e809b:/# dig @127.0.0.11 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @127.0.0.11 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62285
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        1850    IN      A       93.184.215.14

;; Query time: 28 msec
;; SERVER: 127.0.0.11#53(127.0.0.11)
;; WHEN: Sun Jun 09 17:40:07 UTC 2024
;; MSG SIZE  rcvd: 60

root@3b5fee4e809b:/#
```



```
root@3b5fee4e809b:/# dig @10.9.0.53 www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> @10.9.0.53 www.example.com
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached

root@3b5fee4e809b:/#
```

local-dns-server-10.9.0.53:

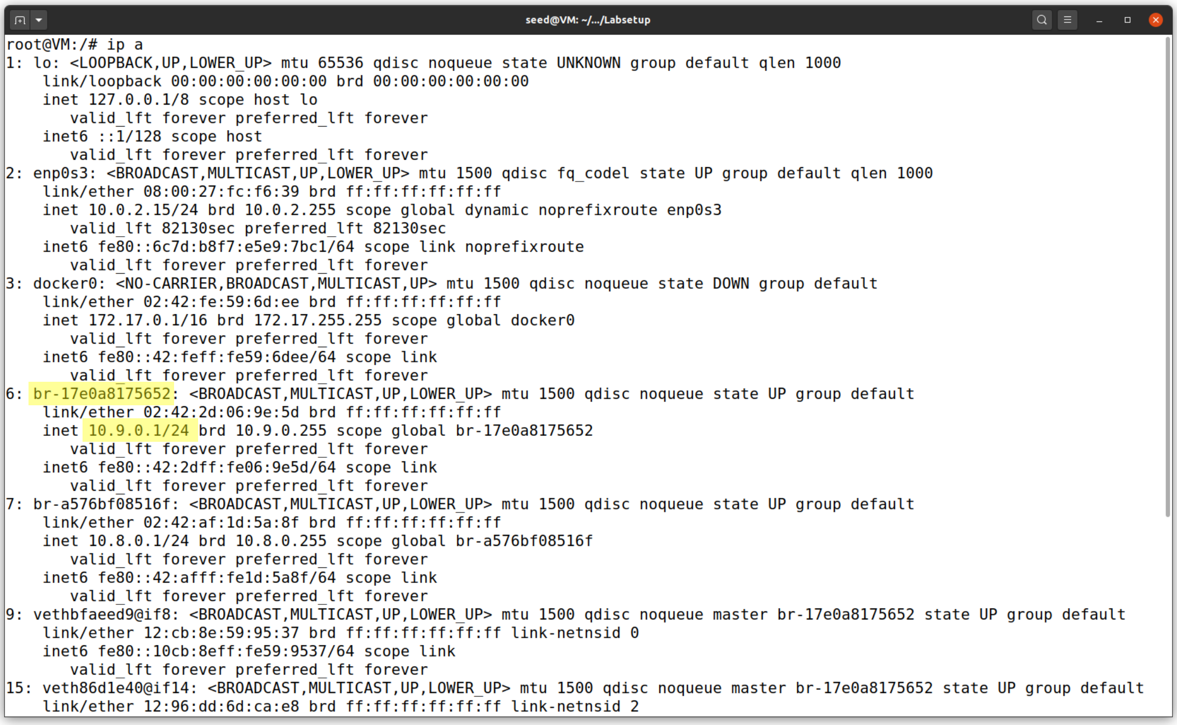


```
root@c4885aa8e80f:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44861
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONA
L: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        1816    IN      A       93.184.215.14

;; Query time: 32 msec
;; SERVER: 127.0.0.11#53(127.0.0.11)
;; WHEN: Sun Jun 09 17:40:41 UTC 2024
;; MSG SIZE  rcvd: 60

root@c4885aa8e80f:/#
```

From the screenshot (local-dns-server-10.9.0.53), there is nothing wrong with the connection between Local DNS Server and the Global DNS servers on the Internet. However, from the screenshots (user-10.9.0.5), we observed that the User Machines have problem connecting to the Local DNS Server as `dig www.example.com` and `dig @10.9.0.53 www.example.com` shown connection timed out error (no server could be reached); while `dig @127.0.0.11 www.example.com` shows no error when the User Machines straightly connect to the Global DNS servers on the Internet.

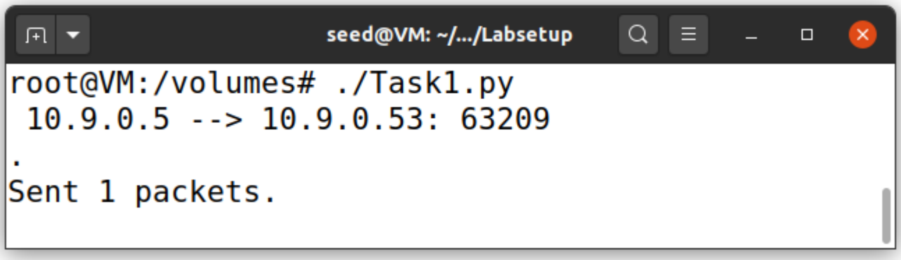
After attack:

seed-attacker:



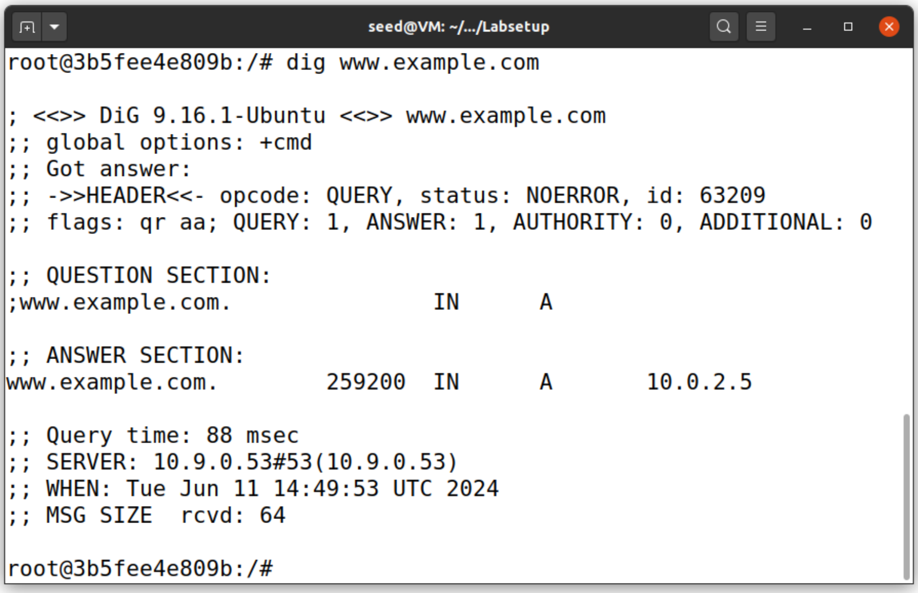
```
root@VM:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:fc:f6:39 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 82130sec preferred_lft 82130sec
    inet6 fe80::6c7d:b8f7:e5e9:7bc1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:fe:59:6d:ee brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:feff:fe59:6dee/64 scope link
       valid_lft forever preferred_lft forever
6: br-17e0a8175652: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:2d:06:9e:5d brd ff:ff:ff:ff:ff:ff
    inet 10.9.0.1/24 brd 10.9.0.255 scope global br-17e0a8175652
       valid_lft forever preferred_lft forever
    inet6 fe80::42:2dff:fe06:9e5d/64 scope link
       valid_lft forever preferred_lft forever
7: br-a576bf08516f: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:af:1d:5a:8f brd ff:ff:ff:ff:ff:ff
    inet 10.8.0.1/24 brd 10.8.0.255 scope global br-a576bf08516f
       valid_lft forever preferred_lft forever
    inet6 fe80::42:afff:fe1d:5a8f/64 scope link
       valid_lft forever preferred_lft forever
9: vethbfaeed9@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-17e0a8175652 state UP group default
    link/ether 12:cb:8e:59:95:37 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::10cb:8eff:fe59:9537/64 scope link
       valid_lft forever preferred_lft forever
15: veth86d1e40@if14: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-17e0a8175652 state UP group default
    link/ether 12:96:dd:6d:ca:e8 brd ff:ff:ff:ff:ff:ff link-netnsid 2
```

From above screenshot, we obtained the actual interface name for the 10.9.0.0/24 network (replace the value for the iface argument)



```
root@VM:/volumes# ./Task1.py
 10.9.0.5 --> 10.9.0.53: 63209

.
Sent 1 packets.
```

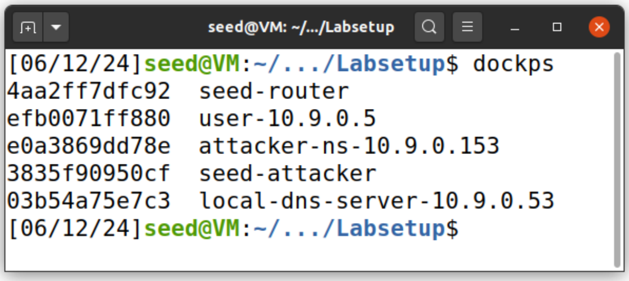
user-10.9.0.5:



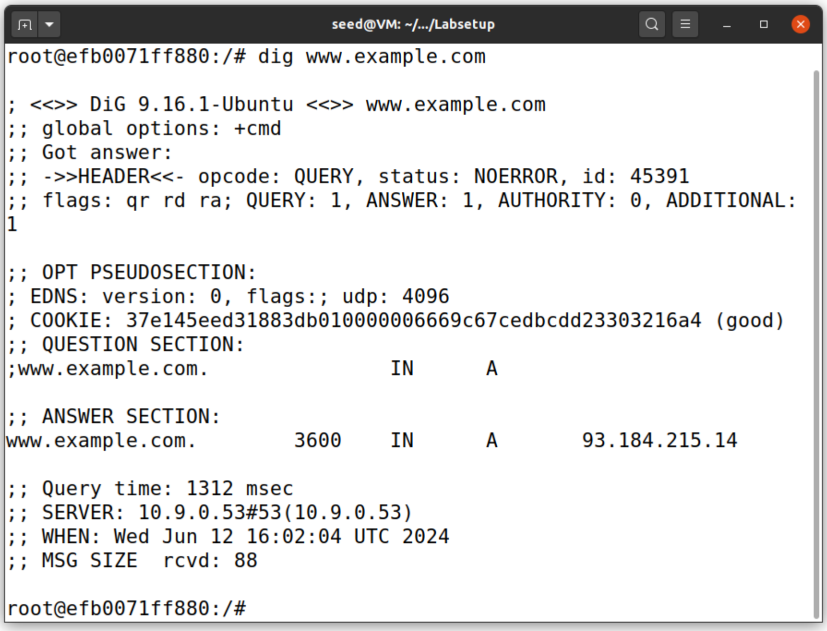
```
root@3b5fee4e809b:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63209
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.0.2.5

;; Query time: 88 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jun 11 14:49:53 UTC 2024
;; MSG SIZE  rcvd: 64

root@3b5fee4e809b:/#
```

UPDATE

Error solved by using 自己的網路:



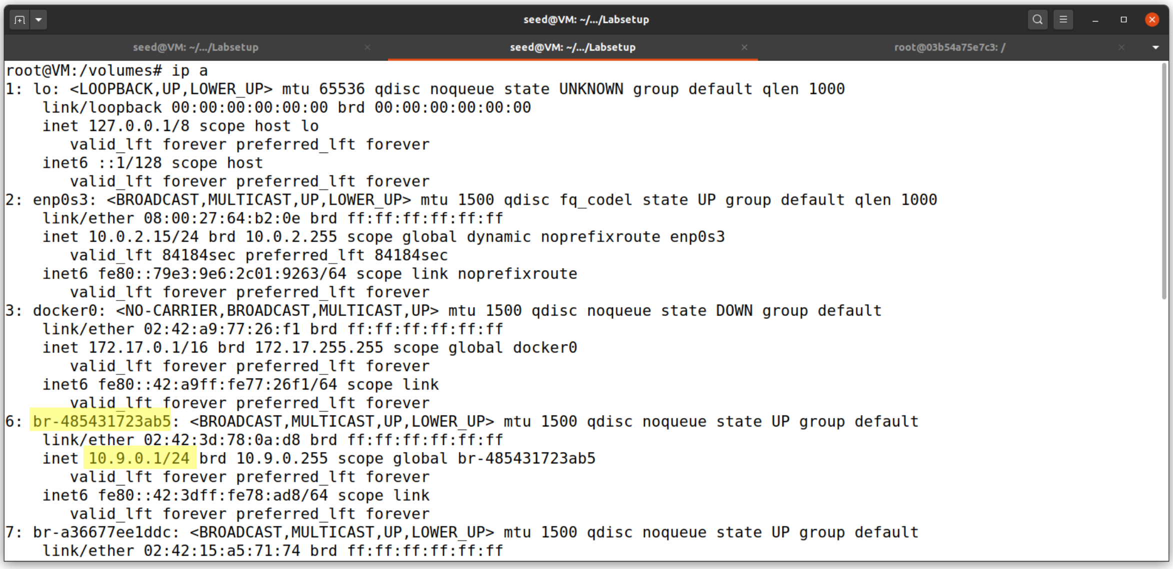
```
[06/12/24]seed@VM:~/.../Labsetup$ dockps
4aa2ff7dfc92  seed-router
efb0071ff880  user-10.9.0.5
e0a3869dd78e  attacker-ns-10.9.0.153
3835f90950cf  seed-attacker
03b54a75e7c3  local-dns-server-10.9.0.53
[06/12/24]seed@VM:~/.../Labsetup$
```



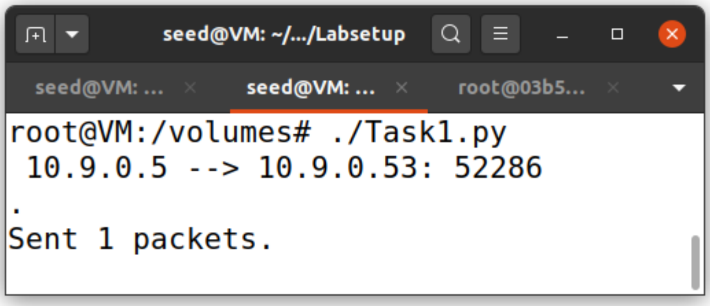
```
root@efb0071ff880:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45391
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 37e145eed31883db010000006669c67cedbcdd23303216a4 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        3600    IN      A       93.184.215.14

;; Query time: 1312 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Jun 12 16:02:04 UTC 2024
;; MSG SIZE  rcvd: 88

root@efb0071ff880:/#
```

After attack:

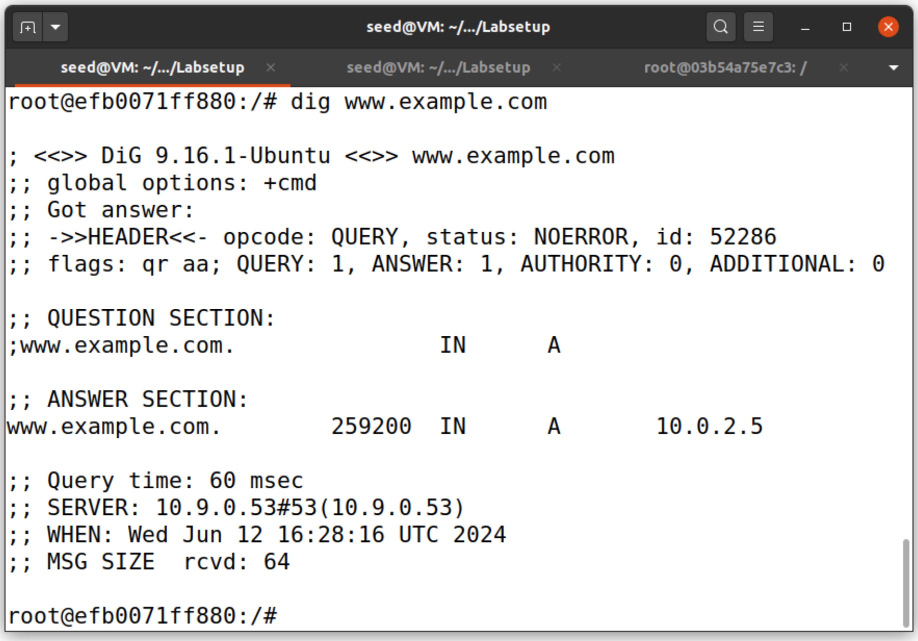
seed-attacker:



```
root@VM:/volumes# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:64:b2:0e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 84184sec preferred_lft 84184sec
    inet6 fe80::79e3:9e6:2c01:9263/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:a9:77:26:f1 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:a9ff:fe77:26f1/64 scope link
       valid_lft forever preferred_lft forever
6: br-485431723ab5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:3d:78:0a:d8 brd ff:ff:ff:ff:ff:ff
    inet 10.9.0.1/24 brd 10.9.0.255 scope global br-485431723ab5
       valid_lft forever preferred_lft forever
    inet6 fe80::42:3dff:fe78:ad8/64 scope link
       valid_lft forever preferred_lft forever
7: br-a36677ee1ddc: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:15:a5:71:74 brd ff:ff:ff:ff:ff:ff
```

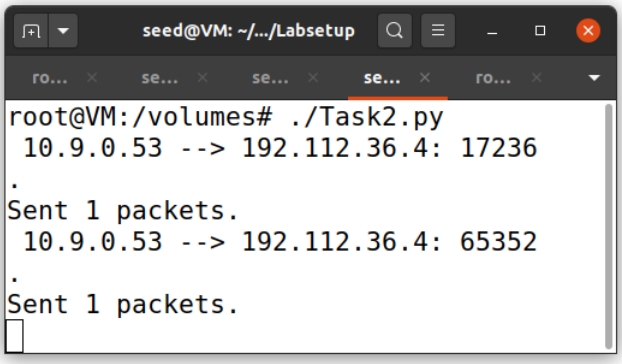


```
root@VM:/volumes# ./Task1.py
 10.9.0.5 --> 10.9.0.53: 52286

.
Sent 1 packets.
```

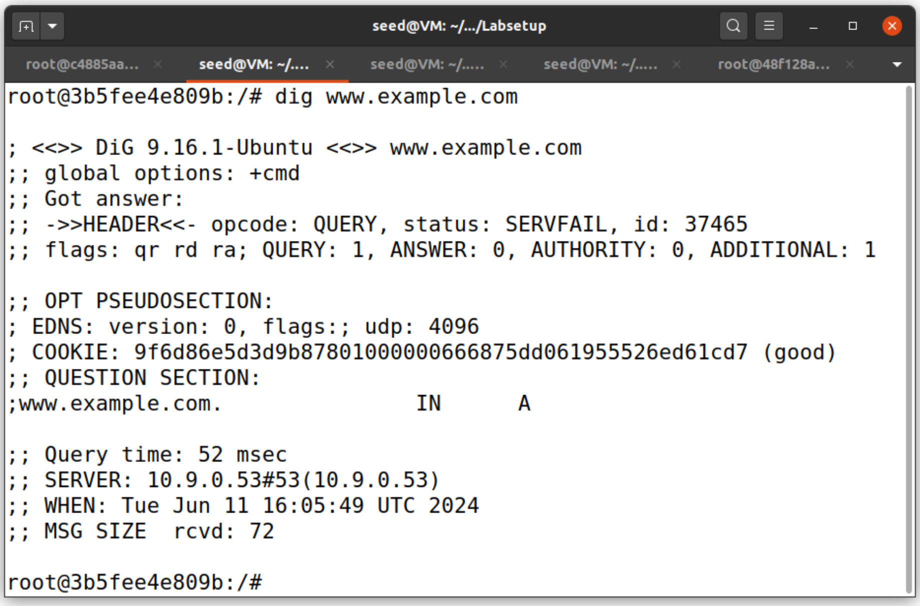


```
root@efb0071ff880:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52286
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.0.2.5

;; Query time: 60 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Jun 12 16:28:16 UTC 2024
;; MSG SIZE  rcvd: 64

root@efb0071ff880:/#
```

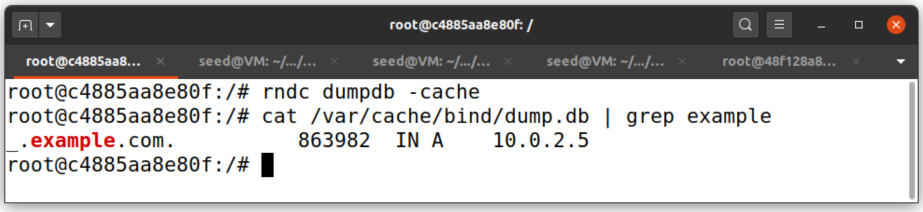
Task 2: DNS Cache Poisoning Attack – Spoofing Answers



```
root@VM:/volumes# ./Task2.py
 10.9.0.53 --> 192.112.36.4: 17236
.
Sent 1 packets.
 10.9.0.53 --> 192.112.36.4: 65352
.
Sent 1 packets.
```



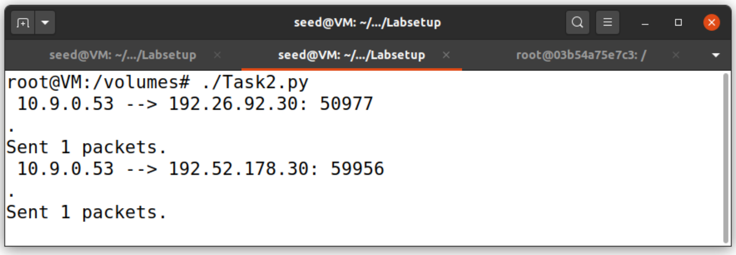
```
root@3b5fee4e809b:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 37465
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9f6d86e5d3d9b87801000000666875dd061955526ed61cd7 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; Query time: 52 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jun 11 16:05:49 UTC 2024
;; MSG SIZE  rcvd: 72

root@3b5fee4e809b:/#
```



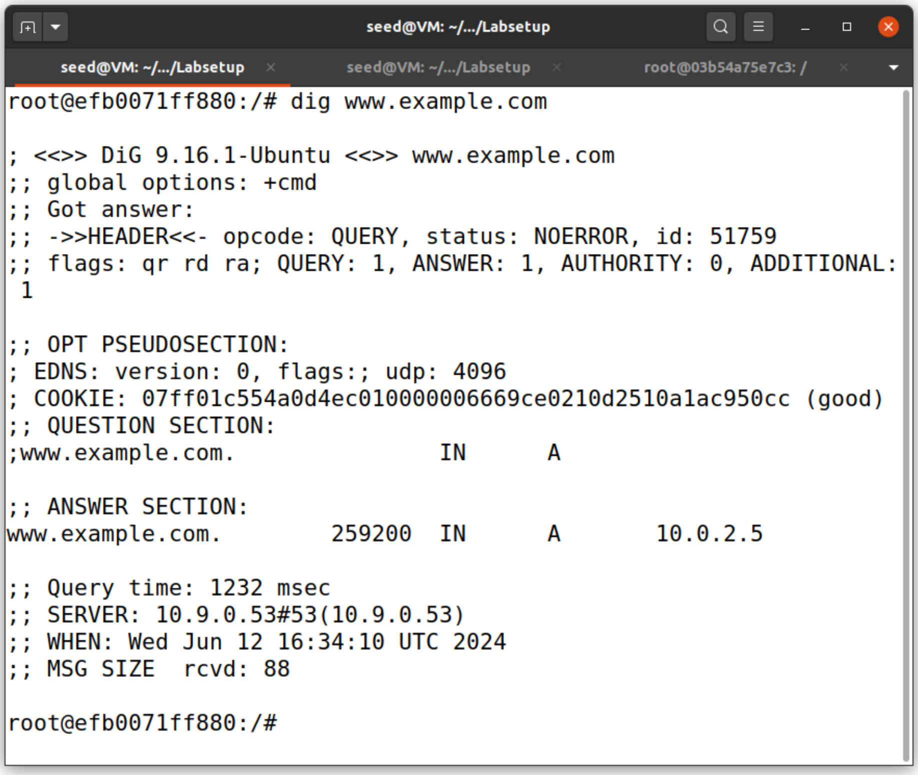
```
root@c4885aa8e80f:/# rndc dumpdb -cache
root@c4885aa8e80f:/# cat /var/cache/bind/dump.db | grep example
_.example.com.          863982  IN A    10.0.2.5
root@c4885aa8e80f:/#
```

Similar error with the one in Task1

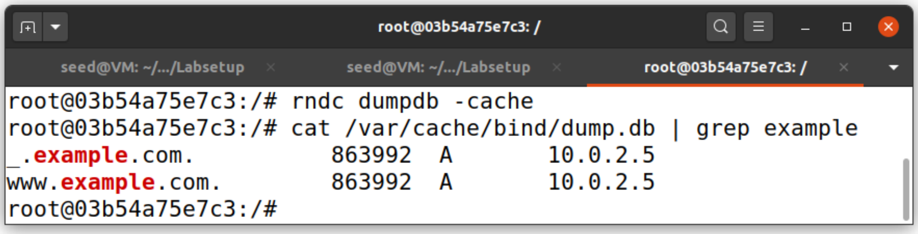
*****UPDATE*****



```
root@VM:/volumes# ./Task2.py
 10.9.0.53 --> 192.26.92.30: 50977
.
Sent 1 packets.
 10.9.0.53 --> 192.52.178.30: 59956
.
Sent 1 packets.
```

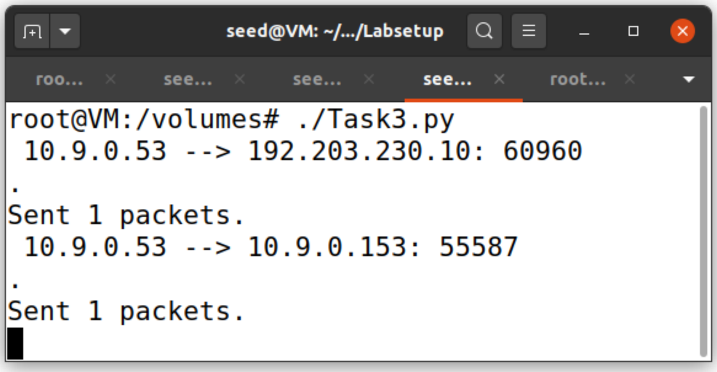


```
root@efb0071ff880:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51759
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 07ff01c554a0d4ec010000006669ce0210d2510a1ac950cc (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.0.2.5

;; Query time: 1232 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Jun 12 16:34:10 UTC 2024
;; MSG SIZE  rcvd: 88

root@efb0071ff880:/#
```

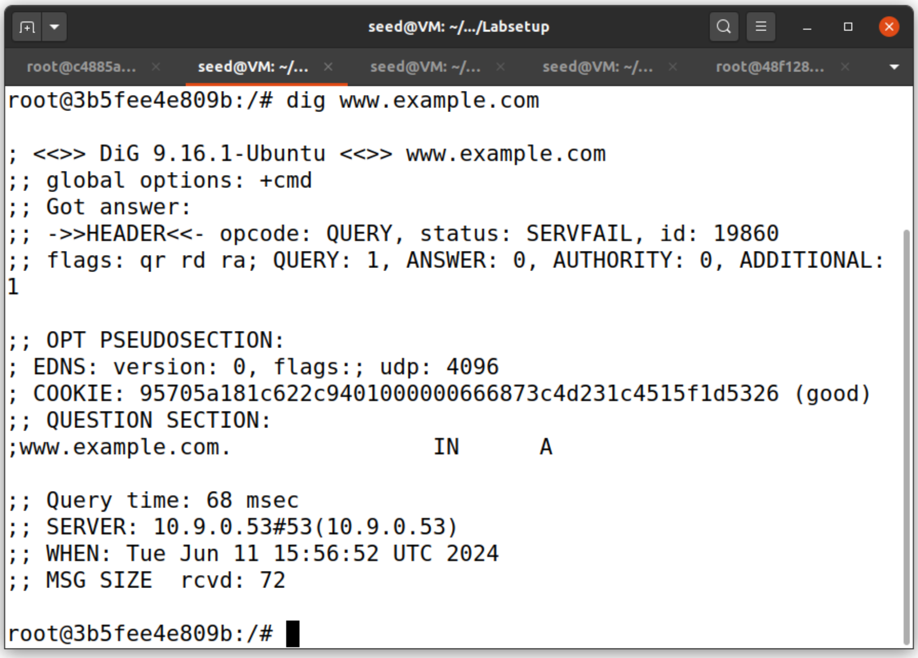


```
root@03b54a75e7c3:/# rndc dumpdb -cache
root@03b54a75e7c3:/# cat /var/cache/bind/dump.db | grep example
_.example.com.          863992  A       10.0.2.5
www.example.com.        863992  A       10.0.2.5
root@03b54a75e7c3:/#
```

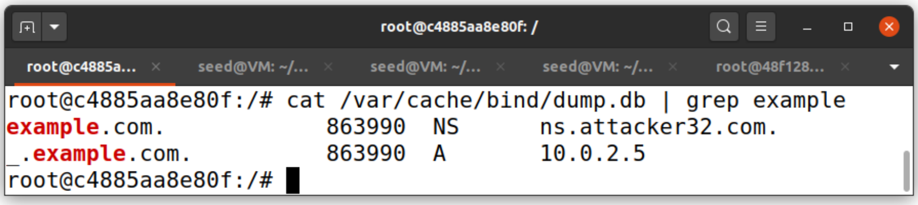
Task 3: Spoofing NS Records



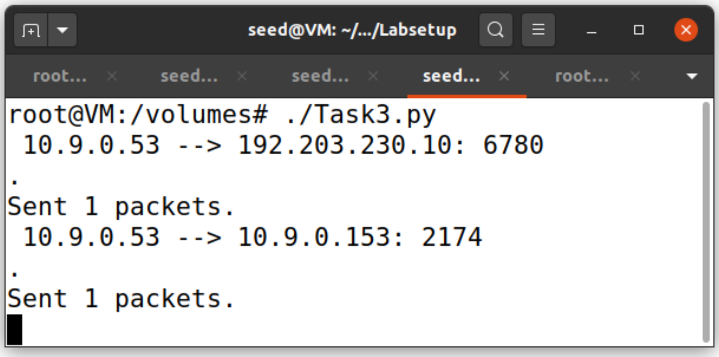
```
root@VM:/volumes# ./Task3.py
 10.9.0.53 --> 192.203.230.10: 60960
.
Sent 1 packets.
 10.9.0.53 --> 10.9.0.153: 55587
.
Sent 1 packets.
```



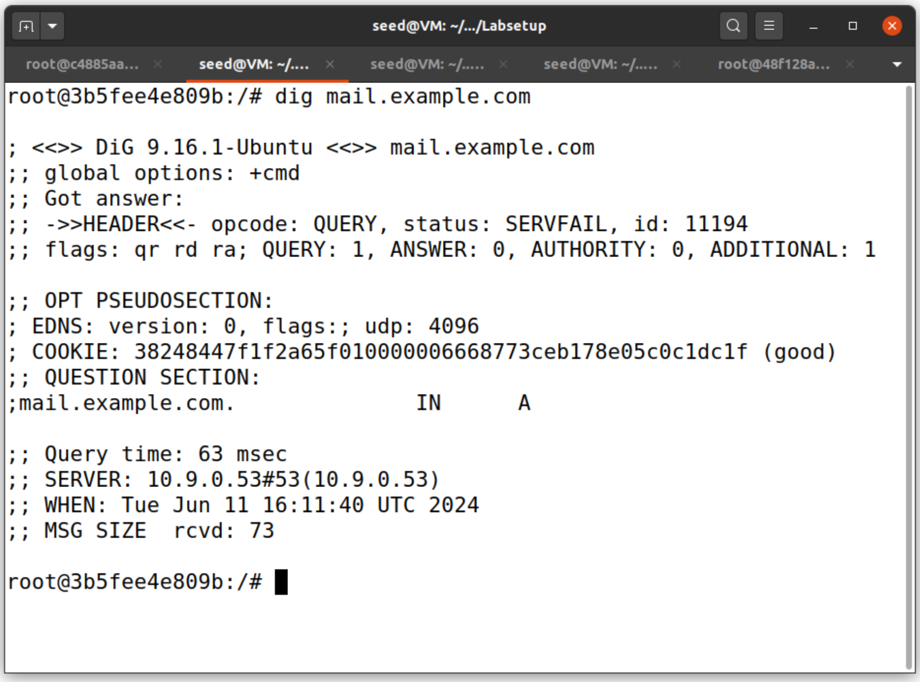
```
root@3b5fee4e809b:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 19860
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL:
1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 95705a181c622c9401000000666873c4d231c4515f1d5326 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; Query time: 68 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jun 11 15:56:52 UTC 2024
;; MSG SIZE  rcvd: 72

root@3b5fee4e809b:/# 
```



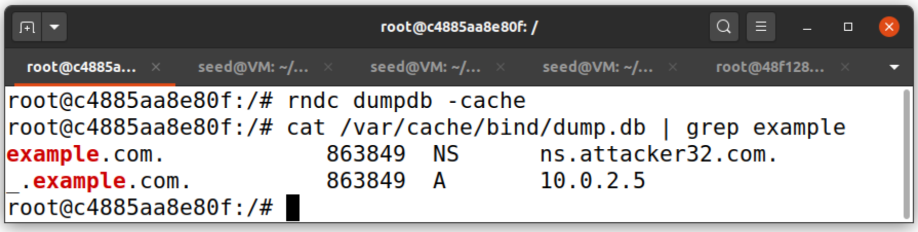
```
root@c4885aa8e80f:/# cat /var/cache/bind/dump.db | grep example
example.com.            863990  NS      ns.attacker32.com.
_.example.com.          863990  A       10.0.2.5
root@c4885aa8e80f:/# 
```



```
root@VM:/volumes# ./Task3.py
 10.9.0.53 --> 192.203.230.10: 6780
.
Sent 1 packets.
 10.9.0.53 --> 10.9.0.153: 2174
.
Sent 1 packets.
```

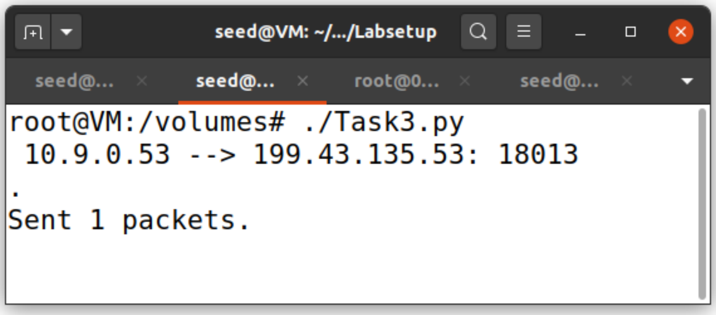


```
root@3b5fee4e809b:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 11194
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 38248447f1f2a65f010000006668773ceb178e05c0c1dc1f (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

;; Query time: 63 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jun 11 16:11:40 UTC 2024
;; MSG SIZE  rcvd: 73

root@3b5fee4e809b:/#
```

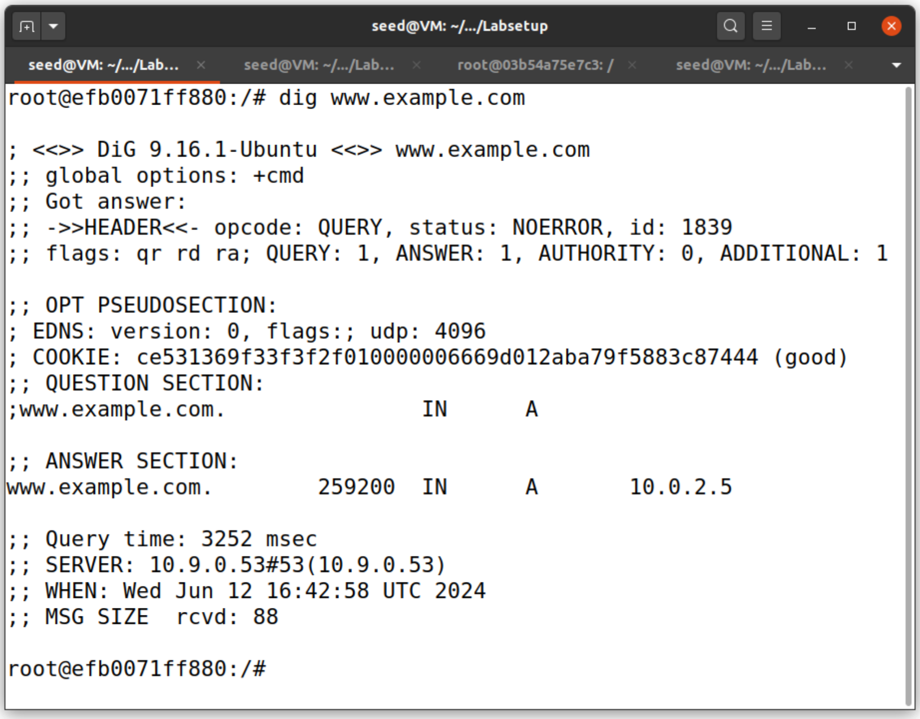


```
root@c4885aa8e80f:/# rndc dumpdb -cache
root@c4885aa8e80f:/# cat /var/cache/bind/dump.db | grep example
example.com.            863849  NS      ns.attacker32.com.
_.example.com.          863849  A       10.0.2.5
root@c4885aa8e80f:/#
```

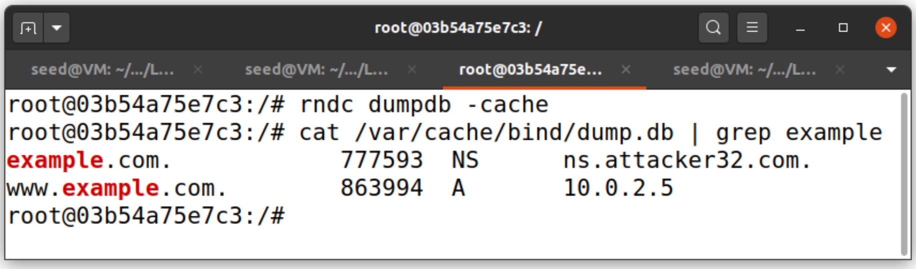
*****UPDATE*****



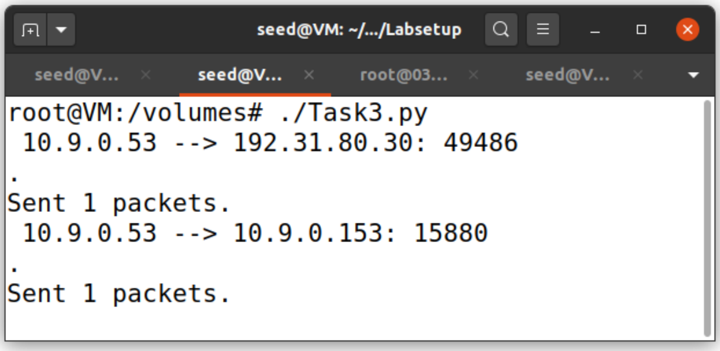
```
root@VM:/volumes# ./Task3.py
 10.9.0.53 --> 199.43.135.53: 18013
.
Sent 1 packets.
```



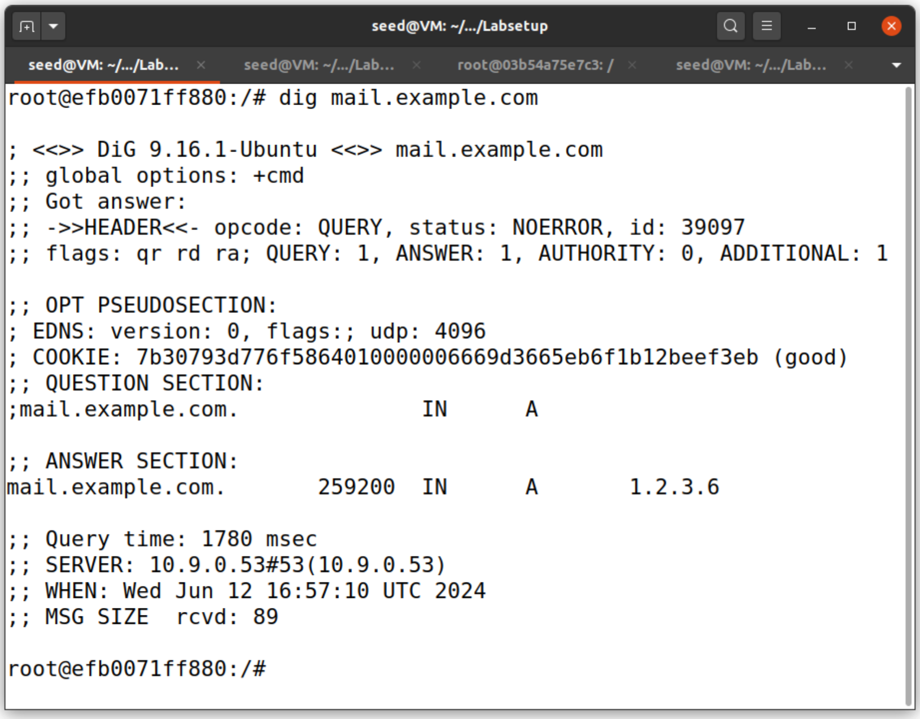
```
root@efb0071ff880:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1839
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ce531369f33f3f2f010000006669d012aba79f5883c87444 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.0.2.5

;; Query time: 3252 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Jun 12 16:42:58 UTC 2024
;; MSG SIZE  rcvd: 88

root@efb0071ff880:/#
```



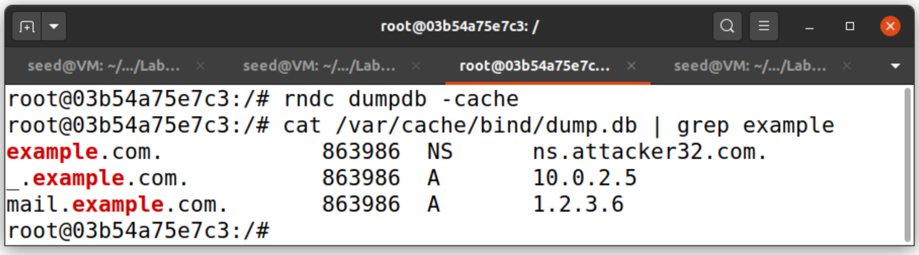
```
root@03b54a75e7c3:/# rndc dumpdb -cache
root@03b54a75e7c3:/# cat /var/cache/bind/dump.db | grep example
example.com.            777593  NS      ns.attacker32.com.
www.example.com.        863994  A       10.0.2.5
root@03b54a75e7c3:/#
```



```
root@VM:/volumes# ./Task3.py
 10.9.0.53 --> 192.31.80.30: 49486
.
Sent 1 packets.
 10.9.0.53 --> 10.9.0.153: 15880
.
Sent 1 packets.
```

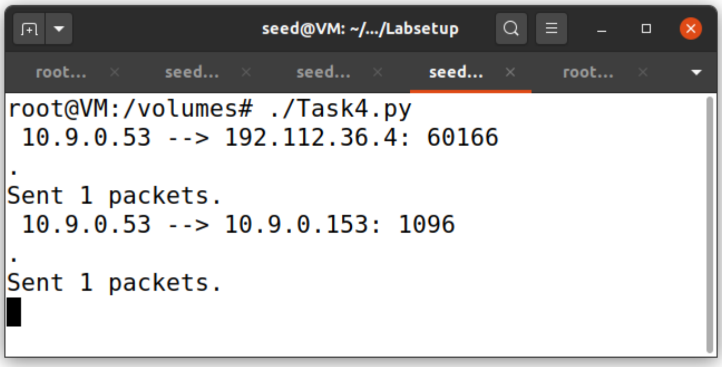


```
root@efb0071ff880:/# dig mail.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39097
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7b30793d776f5864010000006669d3665eb6f1b12beef3eb (good)
;; QUESTION SECTION:
;mail.example.com.              IN      A

;; ANSWER SECTION:
mail.example.com.       259200  IN      A       1.2.3.6

;; Query time: 1780 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Jun 12 16:57:10 UTC 2024
;; MSG SIZE  rcvd: 89

root@efb0071ff880:/#
```

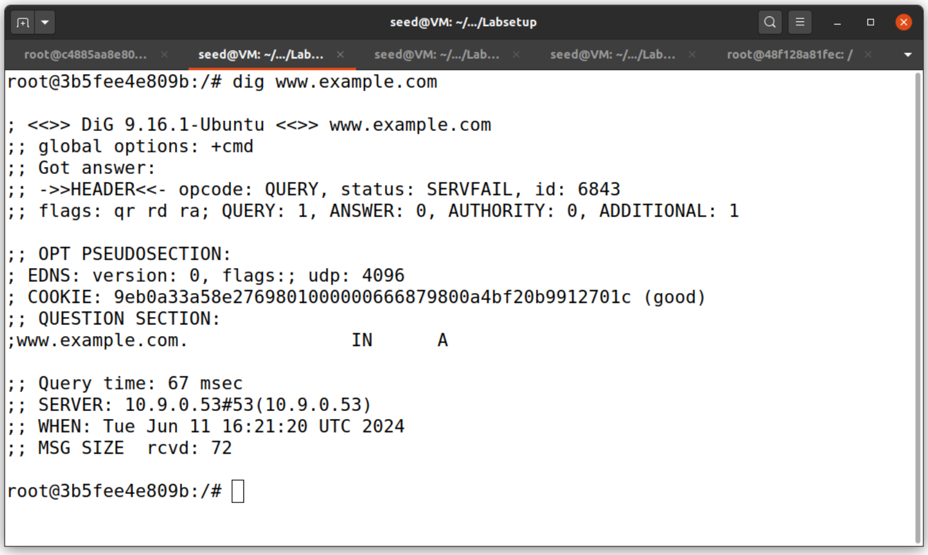


```
root@03b54a75e7c3:/# rndc dumpdb -cache
root@03b54a75e7c3:/# cat /var/cache/bind/dump.db | grep example
example.com.            863986  NS      ns.attacker32.com.
_.example.com.          863986  A       10.0.2.5
mail.example.com.       863986  A       1.2.3.6
root@03b54a75e7c3:/#
```

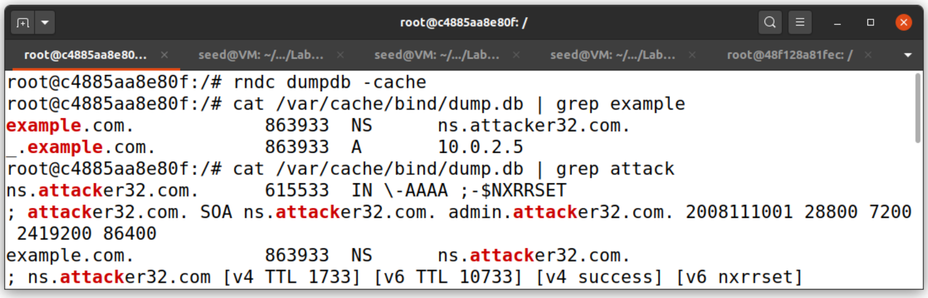
Task 4: Spoofing NS Records for Another Domain



```
root@VM:/volumes# ./Task4.py
 10.9.0.53 --> 192.112.36.4: 60166
.
Sent 1 packets.
 10.9.0.53 --> 10.9.0.153: 1096
.
Sent 1 packets.
```

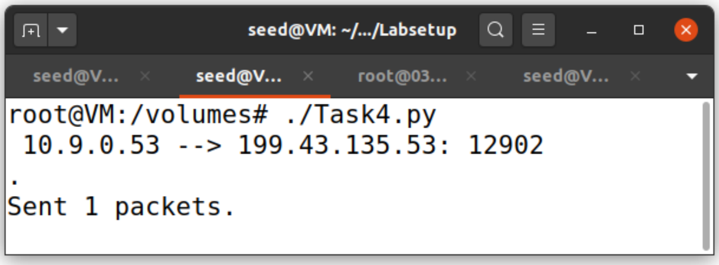


```
root@3b5fee4e809b:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 6843
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9eb0a33a58e2769801000000666879800a4bf20b9912701c (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; Query time: 67 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jun 11 16:21:20 UTC 2024
;; MSG SIZE  rcvd: 72

root@3b5fee4e809b:/# 
```

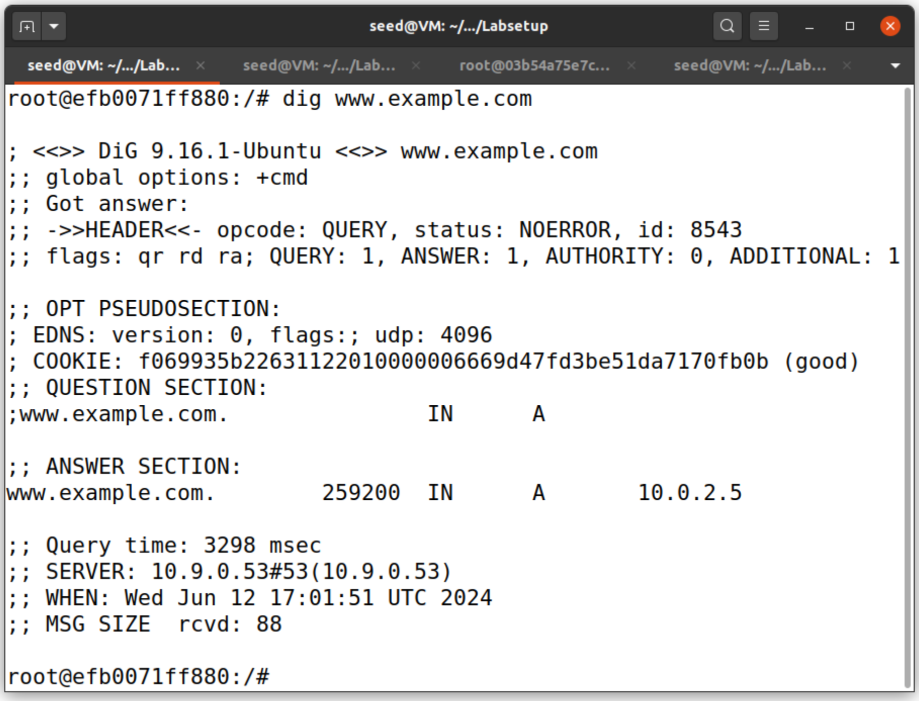


```
root@c4885aa8e80f:/# rndc dumpdb -cache
root@c4885aa8e80f:/# cat /var/cache/bind/dump.db | grep example
example.com.            863933  NS      ns.attacker32.com.
_.example.com.          863933  A       10.0.2.5
root@c4885aa8e80f:/# cat /var/cache/bind/dump.db | grep attack
ns.attacker32.com.      615533  IN \-AAAA ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111001 28800 7200
 2419200 86400
example.com.            863933  NS      ns.attacker32.com.
; ns.attacker32.com [v4 TTL 1733] [v6 TTL 10733] [v4 success] [v6 nxrrset]
```

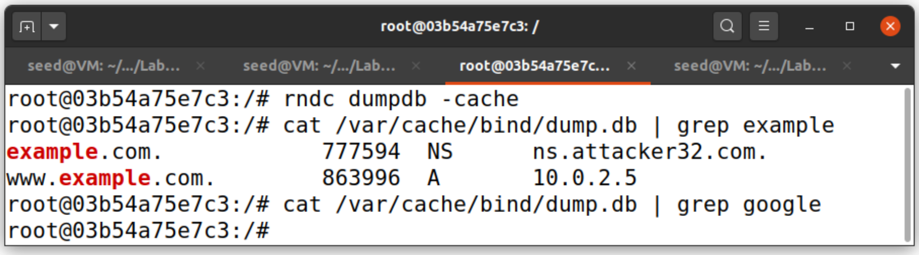
*****UPDATE*****



```
root@VM:/volumes# ./Task4.py
 10.9.0.53 --> 199.43.135.53: 12902
.
Sent 1 packets.
```



```
root@efb0071ff880:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8543
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: f069935b2263112201000000 6669d47fd3be51da7170fb0b (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       10.0.2.5

;; Query time: 3298 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Jun 12 17:01:51 UTC 2024
;; MSG SIZE  rcvd: 88

root@efb0071ff880:/#
```

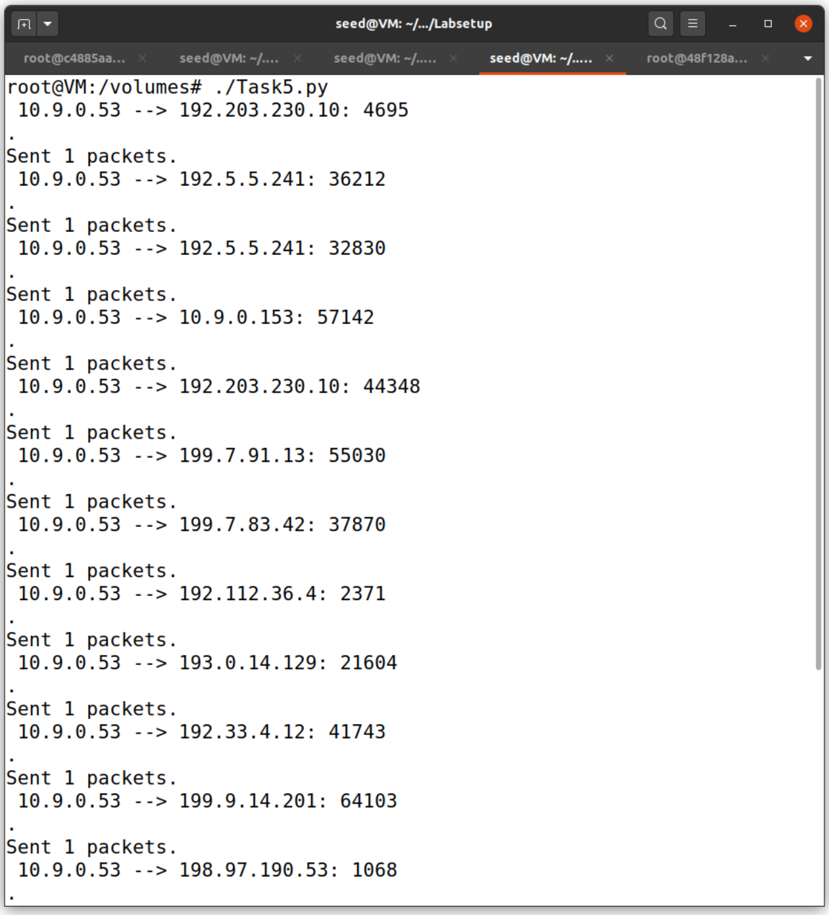


```
root@03b54a75e7c3:/# rndc dumpdb -cache
root@03b54a75e7c3:/# cat /var/cache/bind/dump.db | grep example
example.com.            777594  NS      ns.attacker32.com.
www.example.com.        863996  A       10.0.2.5
root@03b54a75e7c3:/# cat /var/cache/bind/dump.db | grep google
root@03b54a75e7c3:/#
```

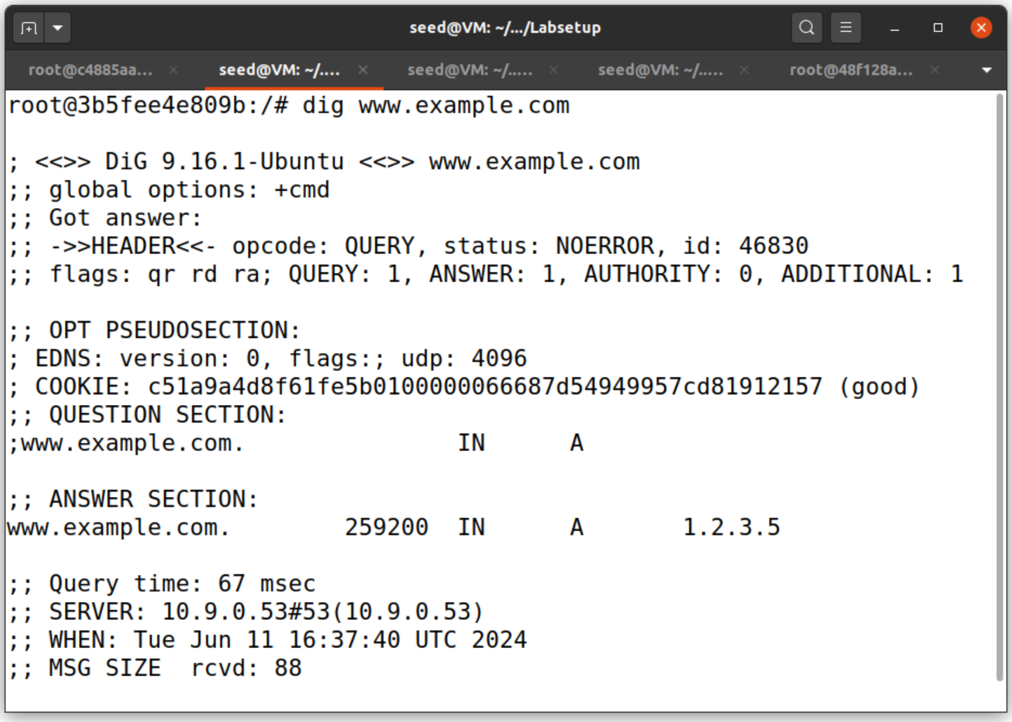
`google.com. 259200 IN NS ns.attacker32.com.` is not cached.

When a user query www.example.com, the local DNS server will respond with the cached information, directing the user's browser to the attacker's-controlled IP address. Furthermore, due to the additional NS record in the Authority section, the local DNS server will now consider the attacker's nameserver as authoritative for google.com as well. Therefore, any subsequent queries for google.com might also be directed to the attacker's nameserver. However, there is no query to google.com in this task, hence not directed to the attacker's nameserver and cached.

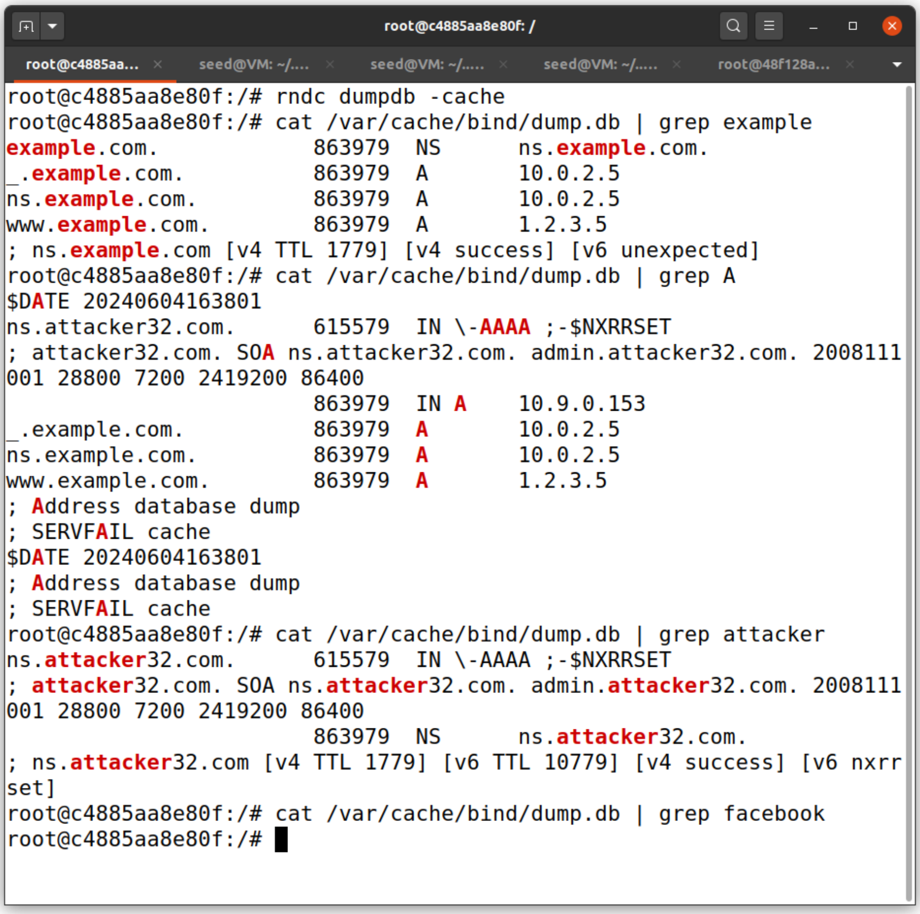
Task 5: Spoofing Records in the Additional Section



```
root@VM:/volumes# ./Task5.py
 10.9.0.53 --> 192.203.230.10: 4695
.
Sent 1 packets.
 10.9.0.53 --> 192.5.5.241: 36212
.
Sent 1 packets.
 10.9.0.53 --> 192.5.5.241: 32830
.
Sent 1 packets.
 10.9.0.53 --> 10.9.0.153: 57142
.
Sent 1 packets.
 10.9.0.53 --> 192.203.230.10: 44348
.
Sent 1 packets.
 10.9.0.53 --> 199.7.91.13: 55030
.
Sent 1 packets.
 10.9.0.53 --> 199.7.83.42: 37870
.
Sent 1 packets.
 10.9.0.53 --> 192.112.36.4: 2371
.
Sent 1 packets.
 10.9.0.53 --> 193.0.14.129: 21604
.
Sent 1 packets.
 10.9.0.53 --> 192.33.4.12: 41743
.
Sent 1 packets.
 10.9.0.53 --> 199.9.14.201: 64103
.
Sent 1 packets.
 10.9.0.53 --> 198.97.190.53: 1068
.
```



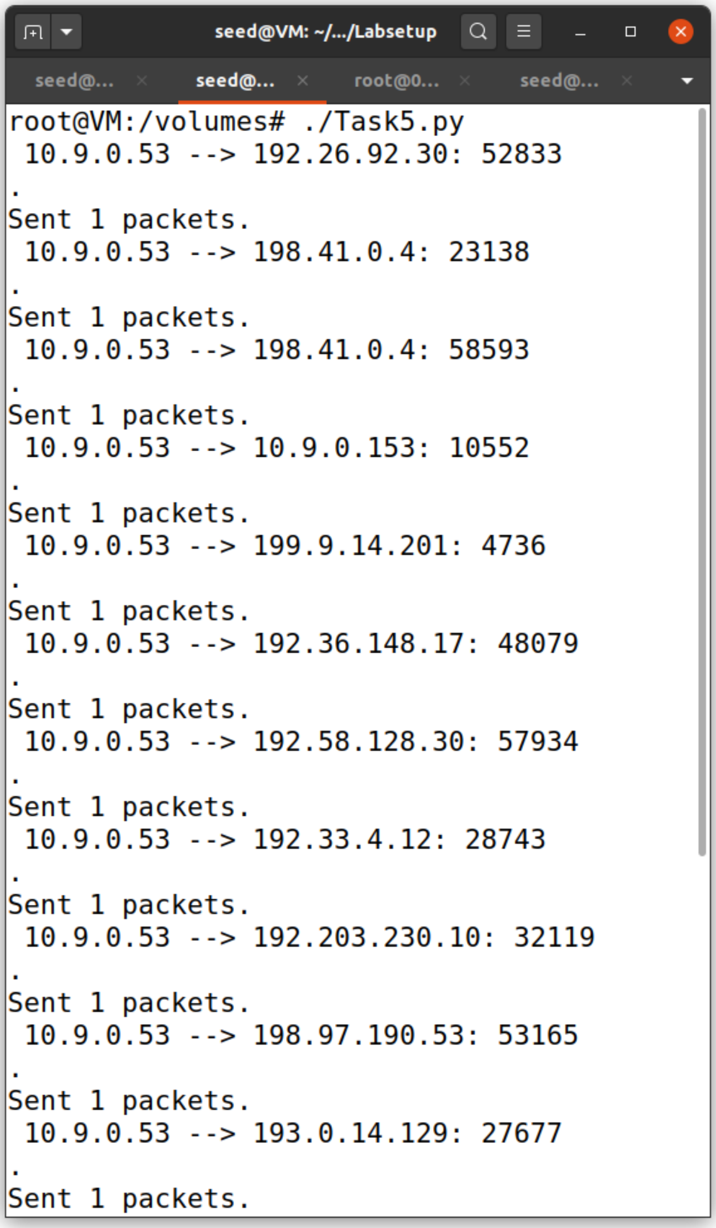
```
root@3b5fee4e809b:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46830
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: c51a9a4d8f61fe5b0100000066687d54949957cd81912157 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.5

;; Query time: 67 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Tue Jun 11 16:37:40 UTC 2024
;; MSG SIZE  rcvd: 88
```



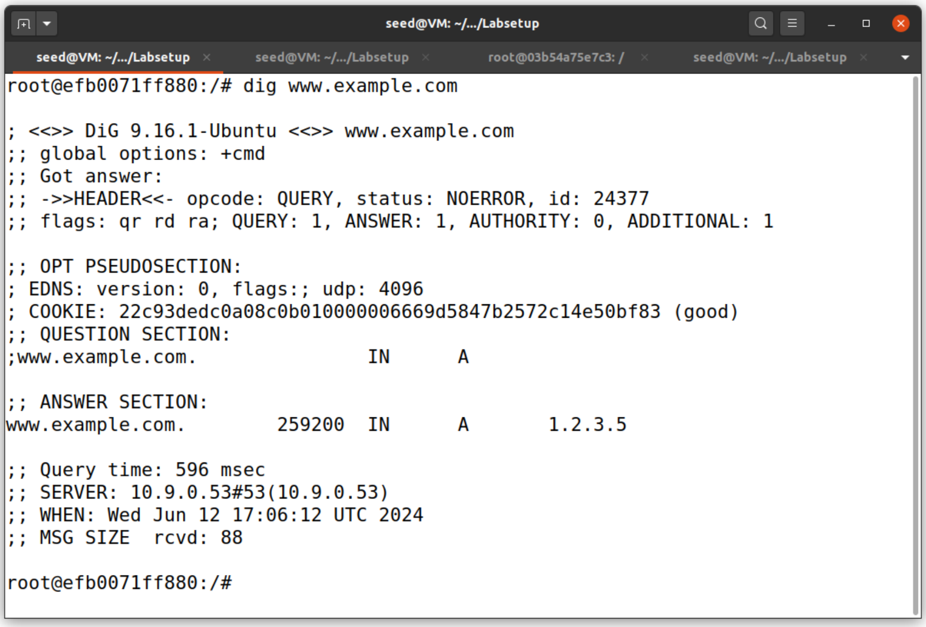
```
root@c4885aa8e80f:/# rndc dumpdb -cache
root@c4885aa8e80f:/# cat /var/cache/bind/dump.db | grep example
example.com.            863979  NS      ns.example.com.
_.example.com.          863979  A       10.0.2.5
ns.example.com.         863979  A       10.0.2.5
www.example.com.        863979  A       1.2.3.5
; ns.example.com [v4 TTL 1779] [v4 success] [v6 unexpected]
root@c4885aa8e80f:/# cat /var/cache/bind/dump.db | grep A
$DATE 20240604163801
ns.attacker32.com.      615579  IN \-AAAA ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111
001 28800 7200 2419200 86400
                        863979  IN A    10.9.0.153
_.example.com.          863979  A       10.0.2.5
ns.example.com.         863979  A       10.0.2.5
www.example.com.        863979  A       1.2.3.5
; Address database dump
; SERVFAIL cache
$DATE 20240604163801
; Address database dump
; SERVFAIL cache
root@c4885aa8e80f:/# cat /var/cache/bind/dump.db | grep attacker
ns.attacker32.com.      615579  IN \-AAAA ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111
001 28800 7200 2419200 86400
                        863979  NS      ns.attacker32.com.
; ns.attacker32.com [v4 TTL 1779] [v6 TTL 10779] [v4 success] [v6 nxrr
set]
root@c4885aa8e80f:/# cat /var/cache/bind/dump.db | grep facebook
root@c4885aa8e80f:/# 
```

The entry for www.facebook.com in the Additional section will not be cached by the DNS server because it is not related to the queried domain (www.example.com). The DNS server typically caches only relevant information provided in the DNS response.

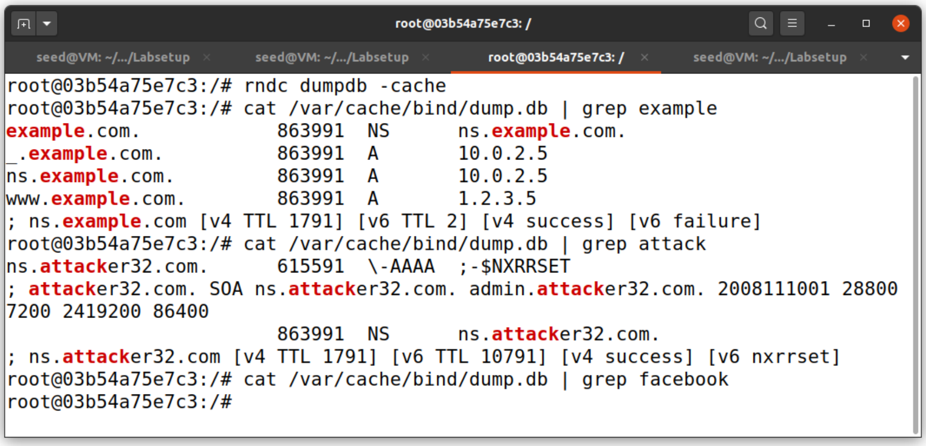
*****UPDATE*****



```
root@VM:/volumes# ./Task5.py
 10.9.0.53 --> 192.26.92.30: 52833
.
Sent 1 packets.
 10.9.0.53 --> 198.41.0.4: 23138
.
Sent 1 packets.
 10.9.0.53 --> 198.41.0.4: 58593
.
Sent 1 packets.
 10.9.0.53 --> 10.9.0.153: 10552
.
Sent 1 packets.
 10.9.0.53 --> 199.9.14.201: 4736
.
Sent 1 packets.
 10.9.0.53 --> 192.36.148.17: 48079
.
Sent 1 packets.
 10.9.0.53 --> 192.58.128.30: 57934
.
Sent 1 packets.
 10.9.0.53 --> 192.33.4.12: 28743
.
Sent 1 packets.
 10.9.0.53 --> 192.203.230.10: 32119
.
Sent 1 packets.
 10.9.0.53 --> 198.97.190.53: 53165
.
Sent 1 packets.
 10.9.0.53 --> 193.0.14.129: 27677
.
Sent 1 packets.
```



```
root@efb0071ff880:/# dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24377
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 22c93dedc0a08c0b010000006669d5847b2572c14e50bf83 (good)
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        259200  IN      A       1.2.3.5

;; Query time: 596 msec
;; SERVER: 10.9.0.53#53(10.9.0.53)
;; WHEN: Wed Jun 12 17:06:12 UTC 2024
;; MSG SIZE  rcvd: 88

root@efb0071ff880:/#
```



```
root@03b54a75e7c3:/# rndc dumpdb -cache
root@03b54a75e7c3:/# cat /var/cache/bind/dump.db | grep example
example.com.            863991  NS      ns.example.com.
_.example.com.          863991  A       10.0.2.5
ns.example.com.         863991  A       10.0.2.5
www.example.com.        863991  A       1.2.3.5
; ns.example.com [v4 TTL 1791] [v6 TTL 2] [v4 success] [v6 failure]
root@03b54a75e7c3:/# cat /var/cache/bind/dump.db | grep attack
ns.attacker32.com.      615591  \-AAAA  ;-$NXRRSET
; attacker32.com. SOA ns.attacker32.com. admin.attacker32.com. 2008111001 28800
7200 2419200 86400
                        863991  NS      ns.attacker32.com.
; ns.attacker32.com [v4 TTL 1791] [v6 TTL 10791] [v4 success] [v6 nxrrset]
root@03b54a75e7c3:/# cat /var/cache/bind/dump.db | grep facebook
root@03b54a75e7c3:/#
```