P5. 使用HTTP/1.1协议进行通信，
服务器端响应码200，成功响应
回应时间2005.12.10，周六.18:27:46
服务器使用 Apache/2.0.52 版本
提供服务.

最后一次修改时间为2005.12.10.周六，
18:27:46

报文是否传输完整的ETag为
52bc3-f22-a88a4c80
文本长度 3874 个字节.
连接方式为长连接(keep-Alive)
文本类型可接受 text/html 语言，
字符集为 ISO-8859-1

P7. 因为一开始没有获得IP地址
所以找到IP地址的总耗时为
$T_1 = \sum_{i=1}^{n}$ ~~RTT~~ RTT_i.

因为要从本地开始不断向上迭代

找到根主机,来找到缓存了目标地址的主机.

找到目标主机后，经过RTT_0时间建立TCP连接，再过RTT_0传文件.

故 $T = T_1 + RTT_0 + RTT_0$

$$T = \sum_{i=1}^{n} RTT_i + 2RTT_0$$

P13 SMTP 中的 From 是

在 SMTP 协议间确定邮件

是哪个 SMTP 服务器的发的

但邮件报文自身的 from 是发件人

的自称

4. P18. a. 是一个用来查询域名是否

已被注册,以及注册域名的详细信息

的数据库.

b. 搜 mihayou.com

网址 www.mihayou.com

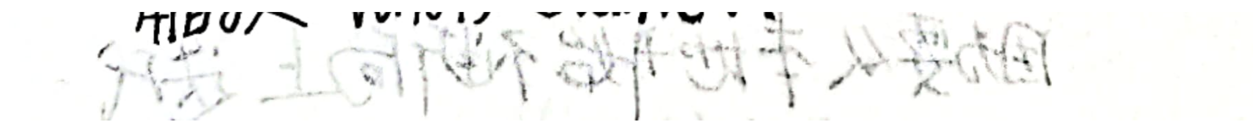
NS 服务器1: f1g1ns1.dnspod.net.

112.80.181.45

NS服务器2: f1g1ns2.dnspod.net.

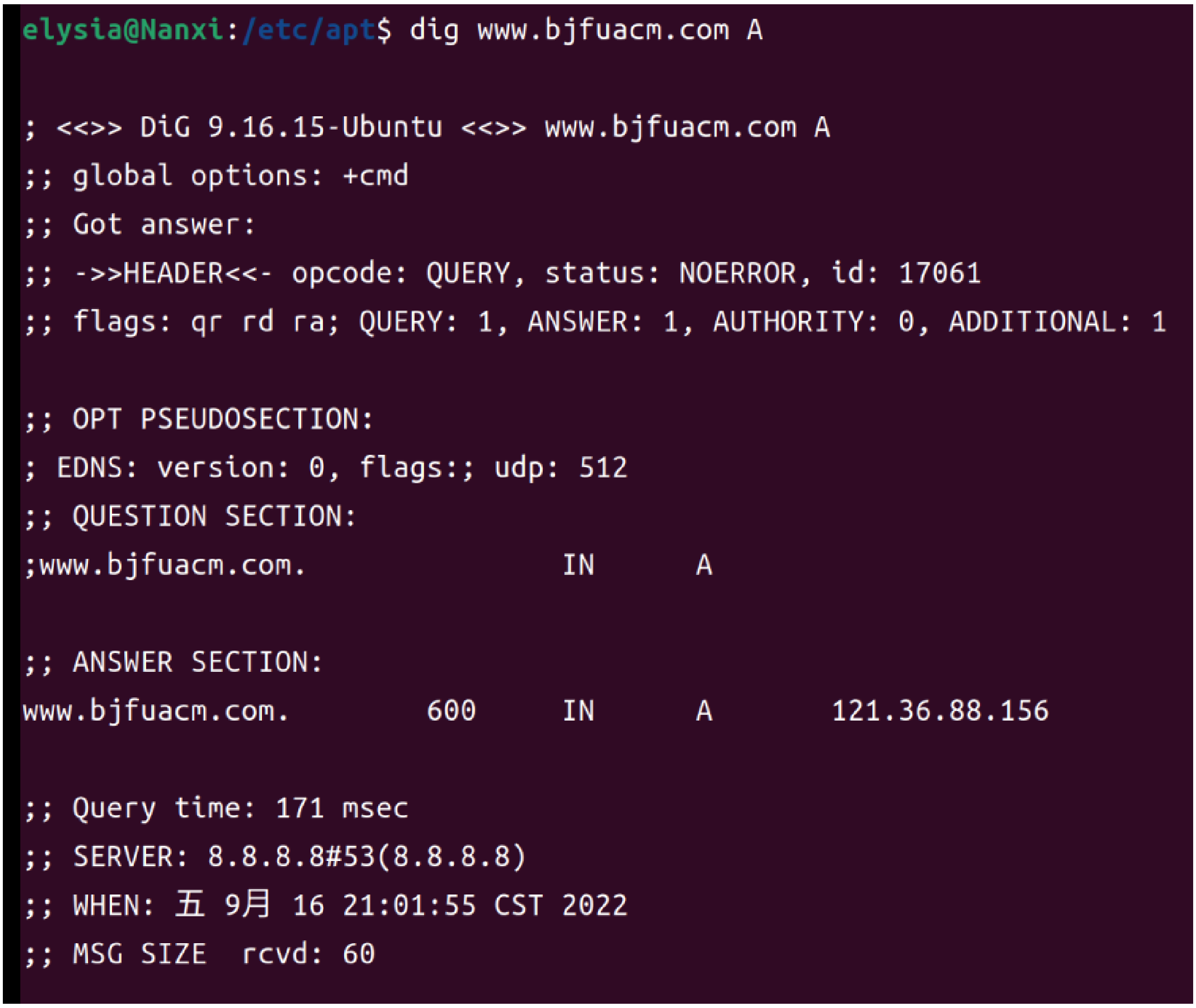
58.251.121.111

用的是 whois.eName.?

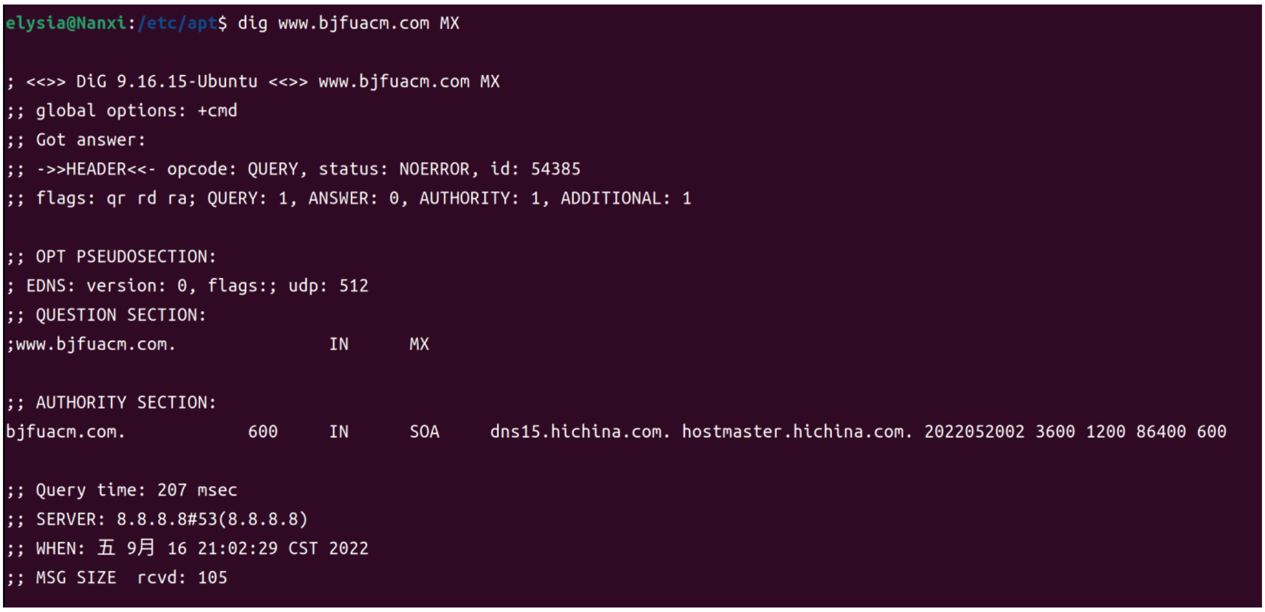


3-p18

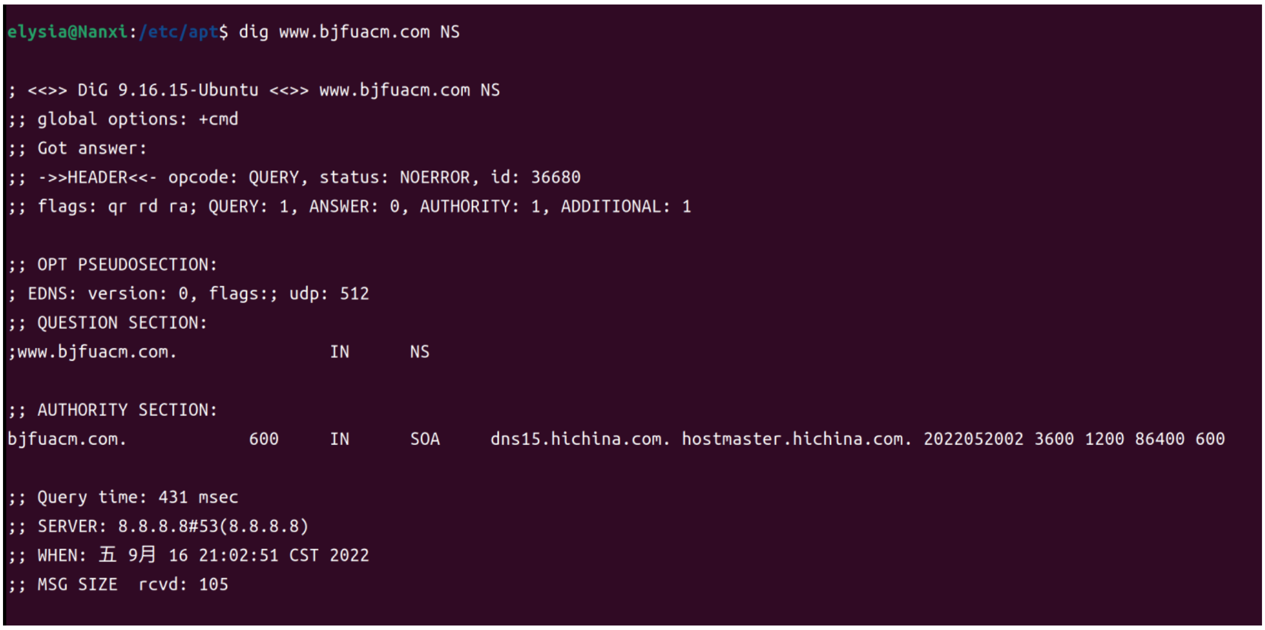
c



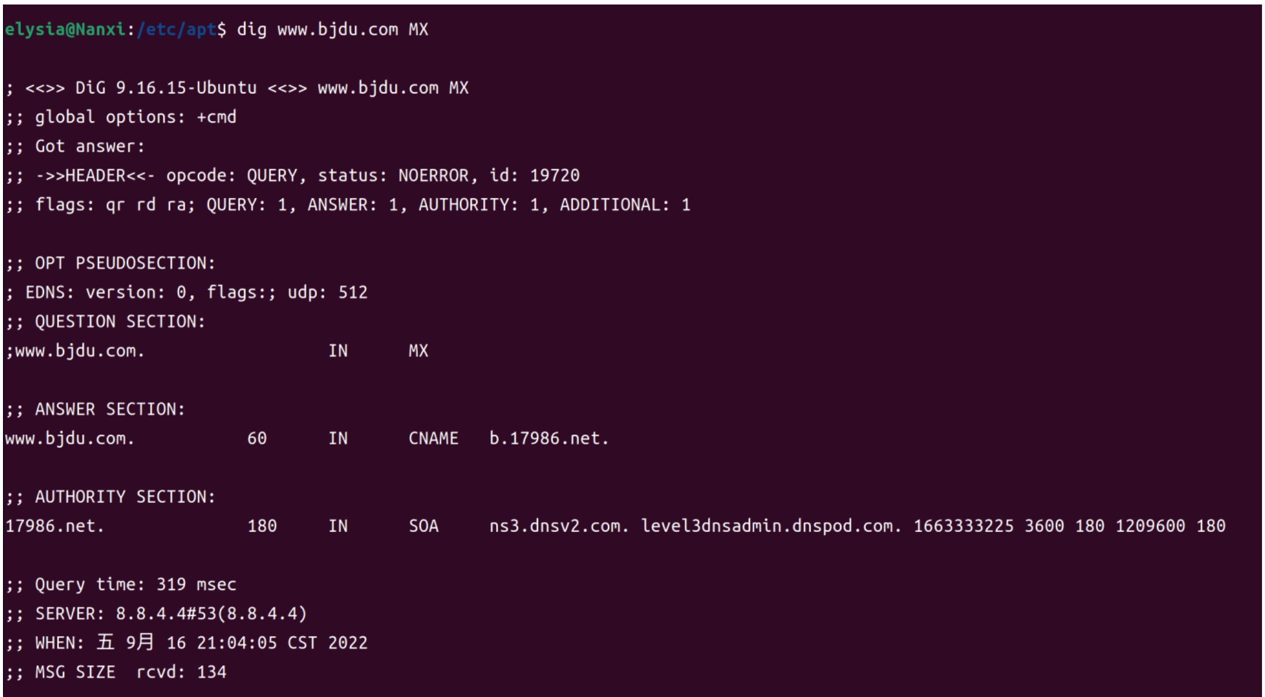
```
elysia@Nanxi:/etc/apt$ dig www.bjfuacm.com A

; <<>> DiG 9.16.15-Ubuntu <<>> www.bjfuacm.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17061
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bjfuacm.com.               IN      A

;; ANSWER SECTION:
www.bjfuacm.com.        600     IN      A       121.36.88.156

;; Query time: 171 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 21:01:55 CST 2022
;; MSG SIZE  rcvd: 60
```



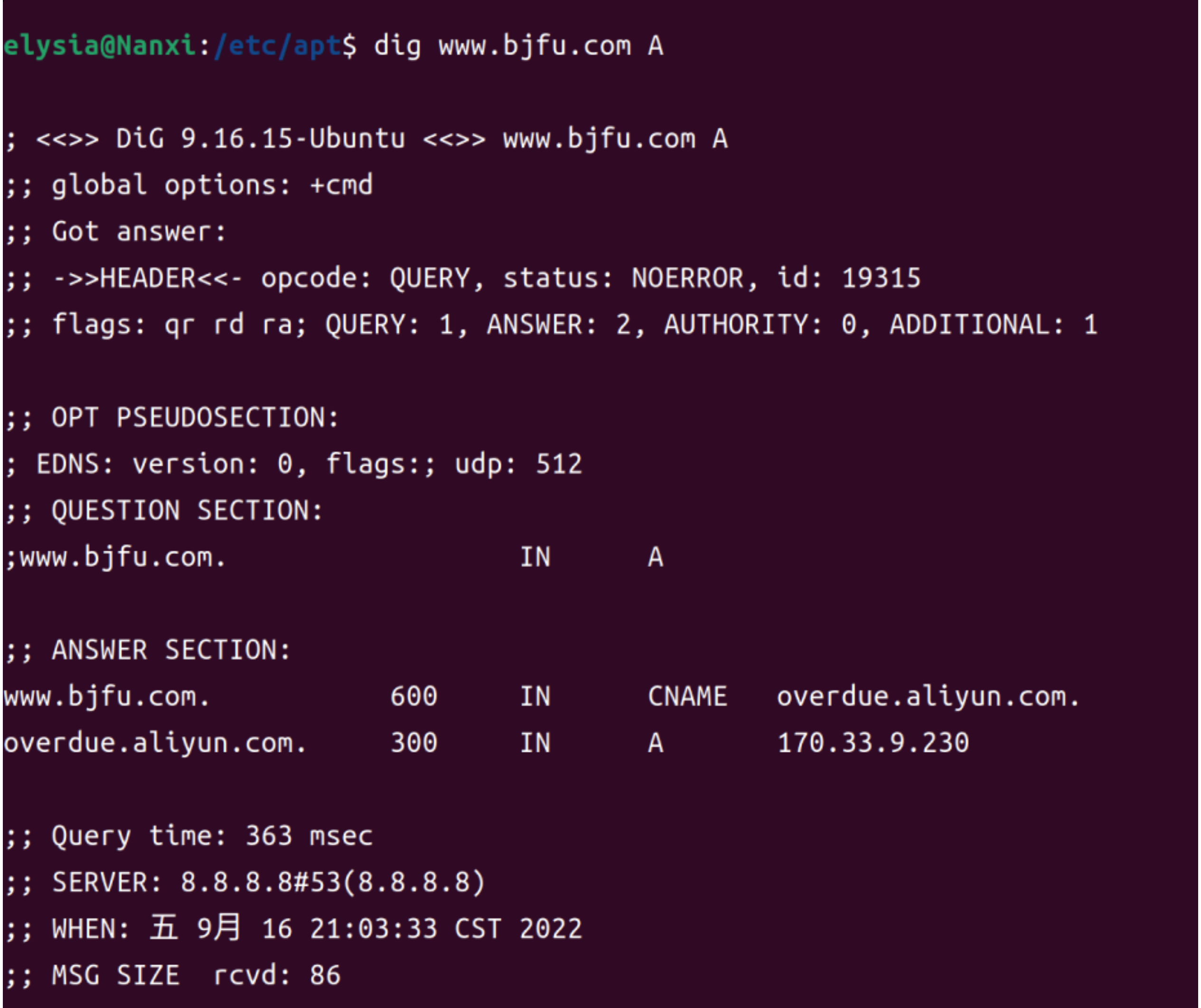
```
elysia@Nanxi:/etc/apt$ dig www.bjfuacm.com MX

; <<>> DiG 9.16.15-Ubuntu <<>> www.bjfuacm.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54385
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bjfuacm.com.               IN      MX

;; AUTHORITY SECTION:
bjfuacm.com.            600     IN      SOA     dns15.hichina.com. hostmaster.hichina.com. 2022052002 3600 1200 86400 600

;; Query time: 207 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 21:02:29 CST 2022
;; MSG SIZE  rcvd: 105
```



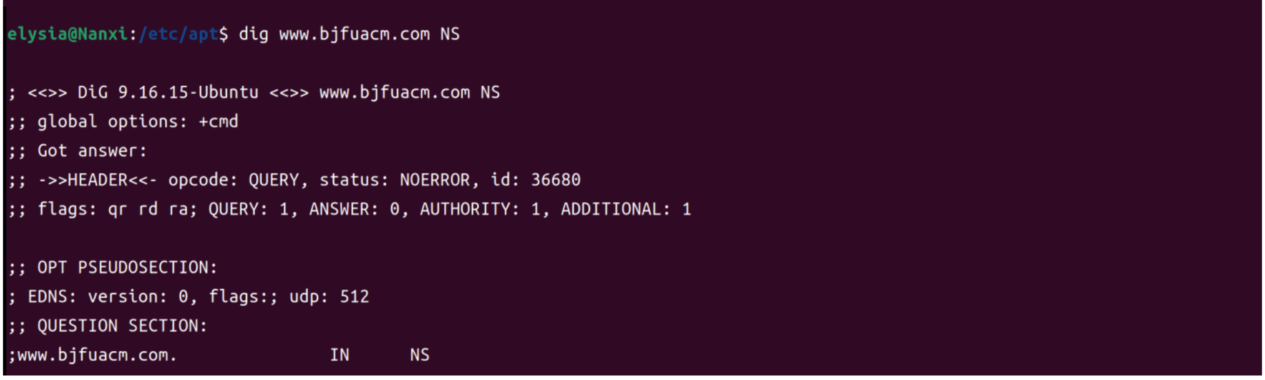
```
elysia@Nanxi:/etc/apt$ dig www.bjfuacm.com NS

; <<>> DiG 9.16.15-Ubuntu <<>> www.bjfuacm.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36680
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bjfuacm.com.               IN      NS

;; AUTHORITY SECTION:
bjfuacm.com.            600     IN      SOA     dns15.hichina.com. hostmaster.hichina.com. 2022052002 3600 1200 86400 600

;; Query time: 431 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 21:02:51 CST 2022
;; MSG SIZE  rcvd: 105
```



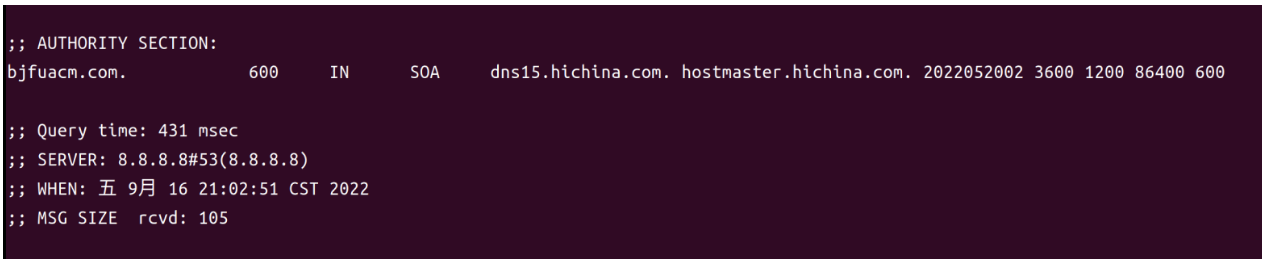
```
elysia@Nanxi:/etc/apt$ dig www.bjdu.com MX

; <<>> DiG 9.16.15-Ubuntu <<>> www.bjdu.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19720
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bjdu.com.                  IN      MX

;; ANSWER SECTION:
www.bjdu.com.           60      IN      CNAME   b.17986.net.

;; AUTHORITY SECTION:
17986.net.              180     IN      SOA     ns3.dnsv2.com. level3dnsadmin.dnspod.com. 1663333225 3600 180 1209600 180

;; Query time: 319 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: 五 9月 16 21:04:05 CST 2022
;; MSG SIZE  rcvd: 134
```



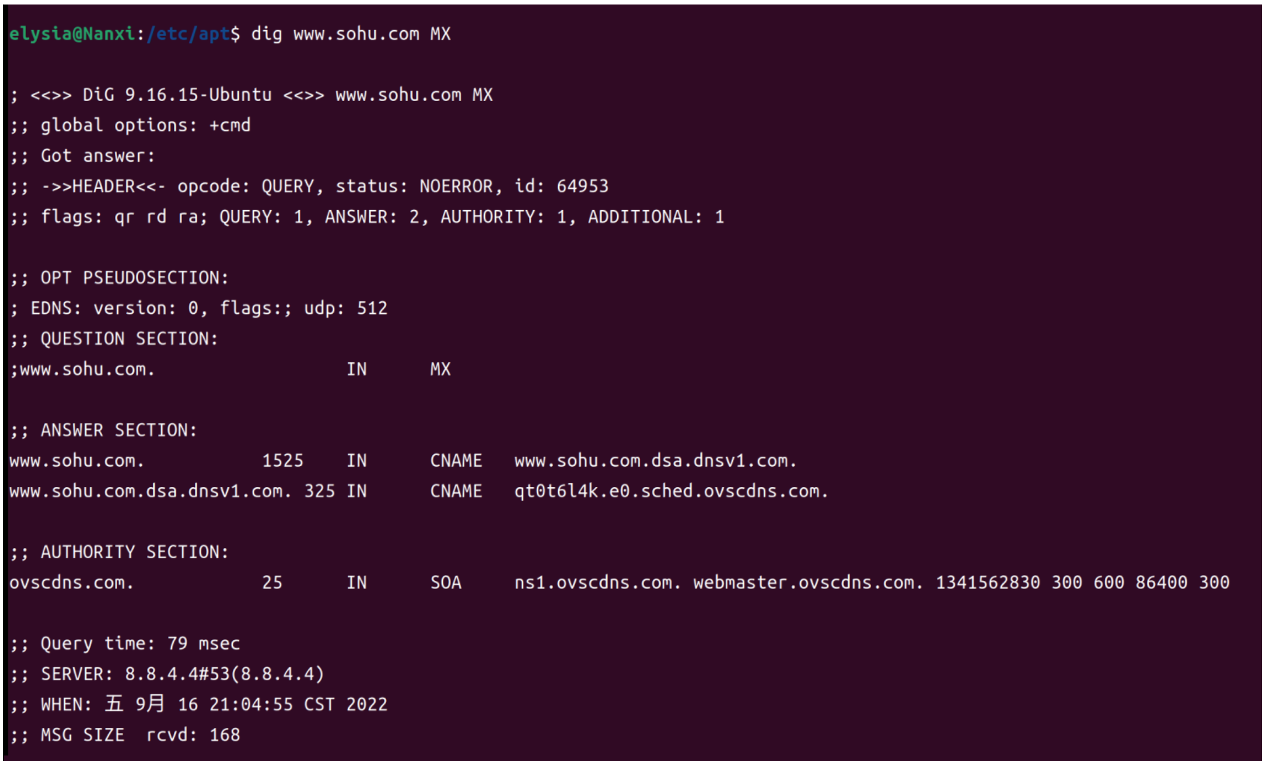
```
elysia@Nanxi:/etc/apt$ dig www.bjfu.com A

; <<>> DiG 9.16.15-Ubuntu <<>> www.bjfu.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19315
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bjfu.com.                  IN      A

;; ANSWER SECTION:
www.bjfu.com.           600     IN      CNAME   overdue.aliyun.com.
overdue.aliyun.com.     300     IN      A       170.33.9.230

;; Query time: 363 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 21:03:33 CST 2022
;; MSG SIZE  rcvd: 86
```



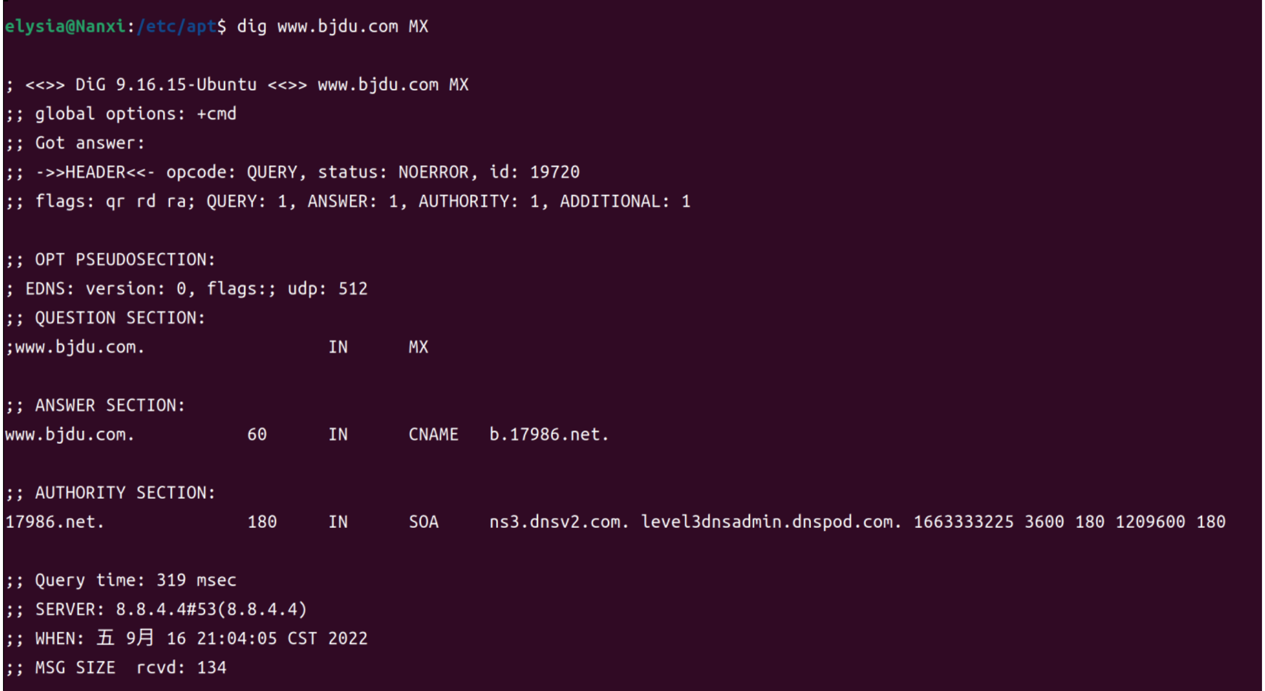
```
elysia@Nanxi:/etc/apt$ dig www.bjfuacm.com NS

; <<>> DiG 9.16.15-Ubuntu <<>> www.bjfuacm.com NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36680
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bjfuacm.com.               IN      NS
```



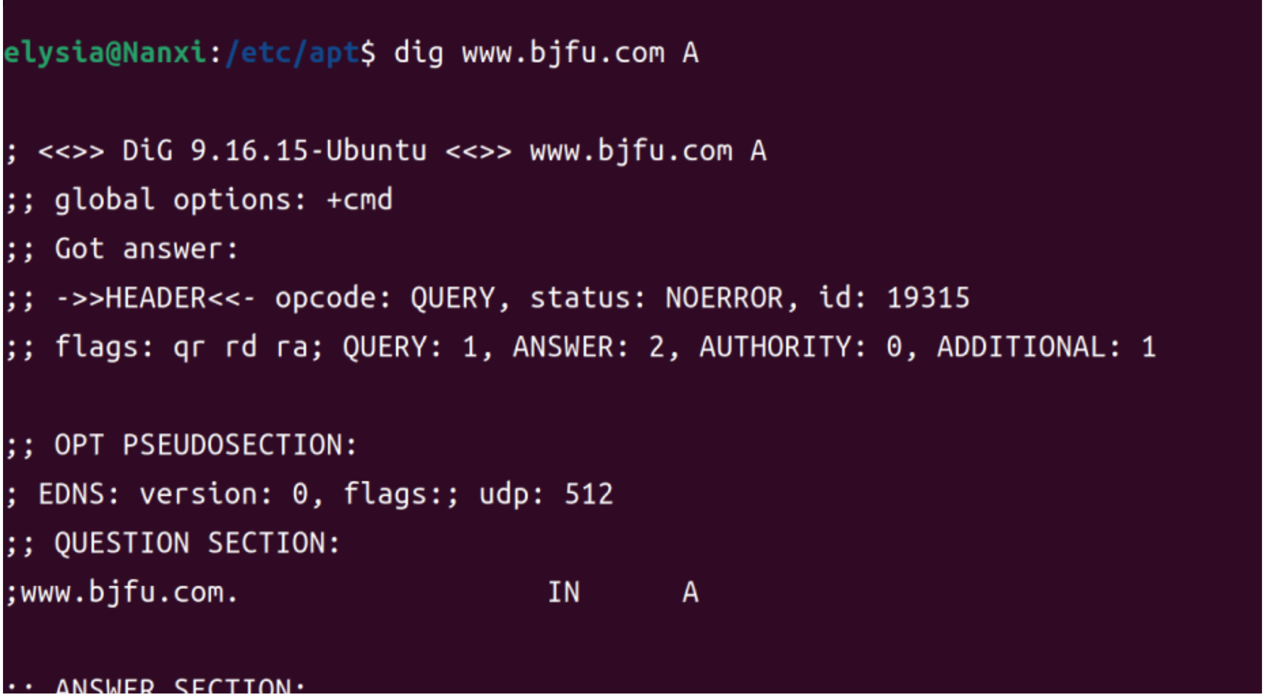
```
;; AUTHORITY SECTION:
bjfuacm.com.            600     IN      SOA     dns15.hichina.com. hostmaster.hichina.com. 2022052002 3600 1200 86400 600

;; Query time: 431 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 21:02:51 CST 2022
;; MSG SIZE  rcvd: 105
```



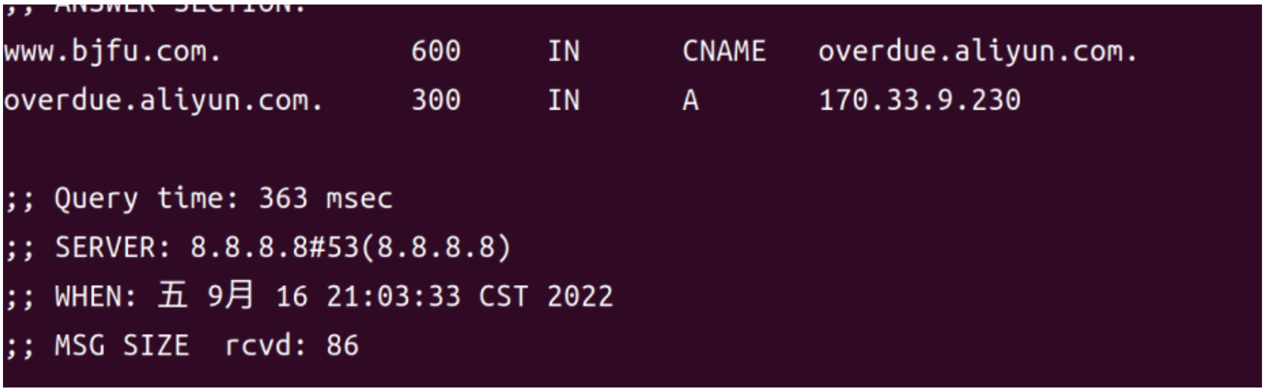
```
elysia@Nanxi:/etc/apt$ dig www.sohu.com MX

; <<>> DiG 9.16.15-Ubuntu <<>> www.sohu.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64953
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.sohu.com.                  IN      MX

;; ANSWER SECTION:
www.sohu.com.           1525    IN      CNAME   www.sohu.com.dsa.dnsv1.com.
www.sohu.com.dsa.dnsv1.com. 325 IN      CNAME   qt0t6l4k.e0.sched.ovscdns.com.

;; AUTHORITY SECTION:
ovscdns.com.            25      IN      SOA     ns1.ovscdns.com. webmaster.ovscdns.com. 1341562830 300 600 86400 300

;; Query time: 79 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: 五 9月 16 21:04:55 CST 2022
;; MSG SIZE  rcvd: 168
```



```
elysia@Nanxi:/etc/apt$ dig www.bjdu.com MX

; <<>> DiG 9.16.15-Ubuntu <<>> www.bjdu.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19720
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bjdu.com.                  IN      MX

;; ANSWER SECTION:
www.bjdu.com.           60      IN      CNAME   b.17986.net.

;; AUTHORITY SECTION:
17986.net.              180     IN      SOA     ns3.dnsv2.com. level3dnsadmin.dnspod.com. 1663333225 3600 180 1209600 180

;; Query time: 319 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: 五 9月 16 21:04:05 CST 2022
;; MSG SIZE  rcvd: 134
```



```
elysia@Nanxi:/etc/apt$ dig www.bjfu.com A

; <<>> DiG 9.16.15-Ubuntu <<>> www.bjfu.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19315
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bjfu.com.                  IN      A

;; ANSWER SECTION:
```



```
;; ANSWER SECTION:
www.bjfu.com.           600     IN      CNAME   overdue.aliyun.com.
overdue.aliyun.com.     300     IN      A       170.33.9.230

;; Query time: 363 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 21:03:33 CST 2022
;; MSG SIZE  rcvd: 86
```

f

用whois数据库查询域名是否已被注册，以及注册域名的详细信息，用nslookup确定域名的IP地址、DNS服务器地址等信息。

g

大家都会了的话，就能通过nslookup查看自己服务器的部署情况，IP地址情况，从而围绕他们做出恰当的安全防备；而且既然攻击者可以用nslookup查到本地服务器的信息，我们可以反过来利用它

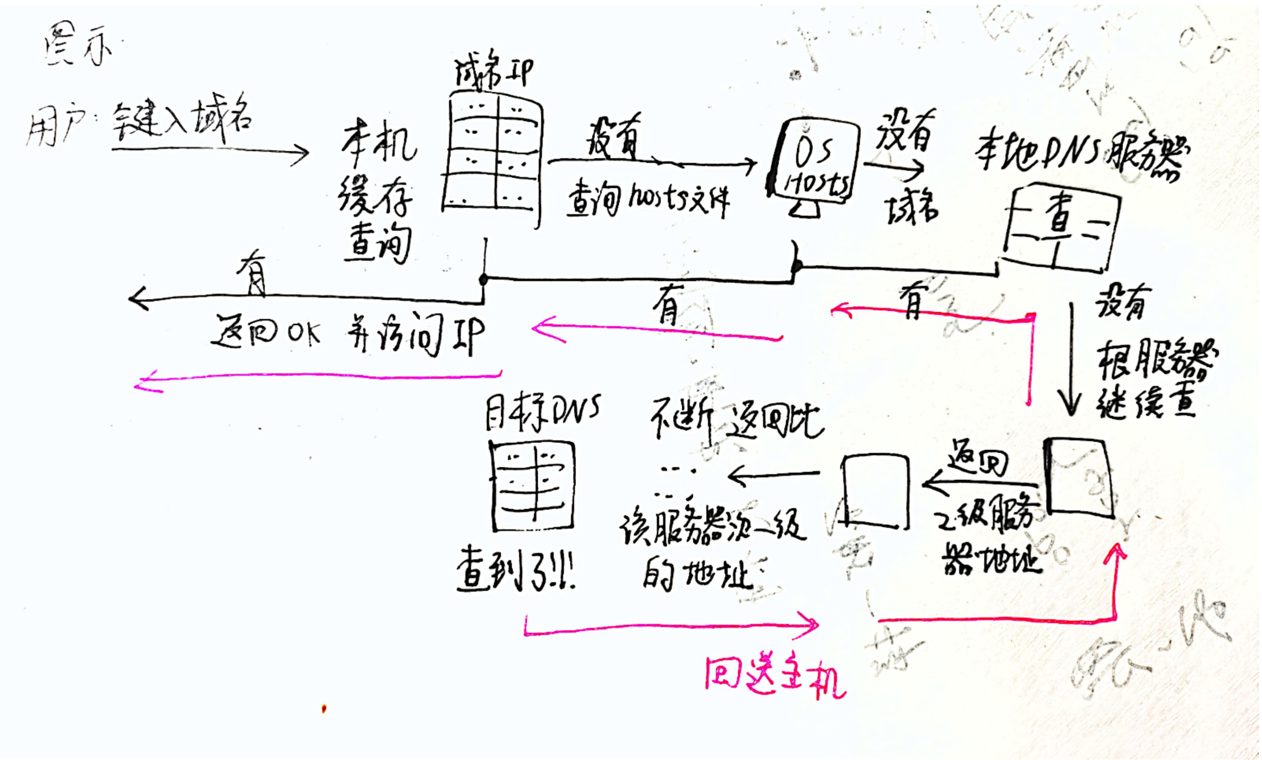
分析攻击者的源地址，然后进行报警或增加防火墙。

5-p21

能，在本地DNS服务器中用dig命令查询欲查询的外部站点，如果它刚被访问过，则其站点信息将被DNS缓存，这样的话查询耗时会很短；否则查询时间很长。

6

query报文会在首部写明自己是query报文，会有一句Response:Message is a query，而reply报文也会有一句注明自己是reply报文的语句：Response:Message is a response。

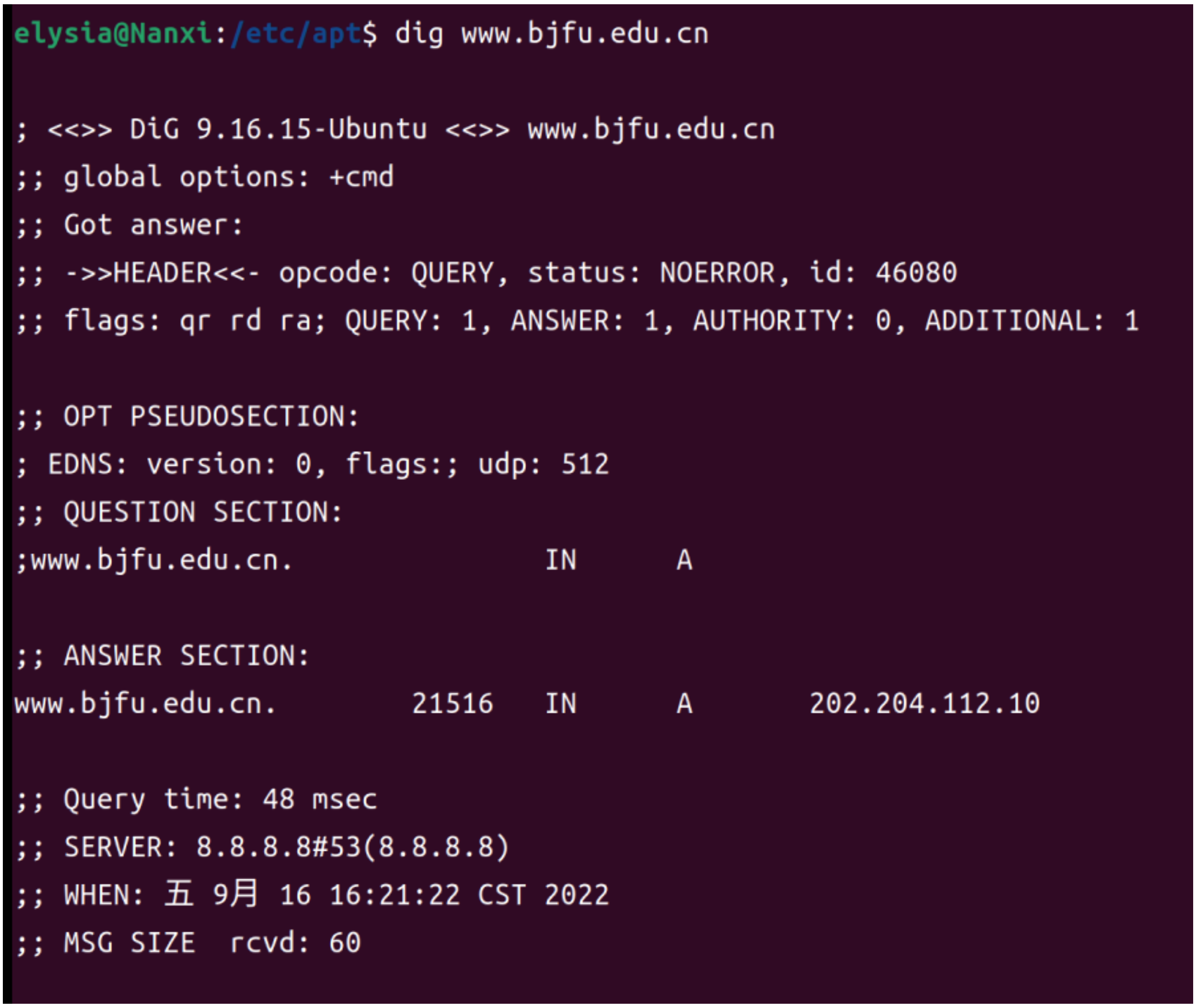


7

a

i

答案：202.204.112.10

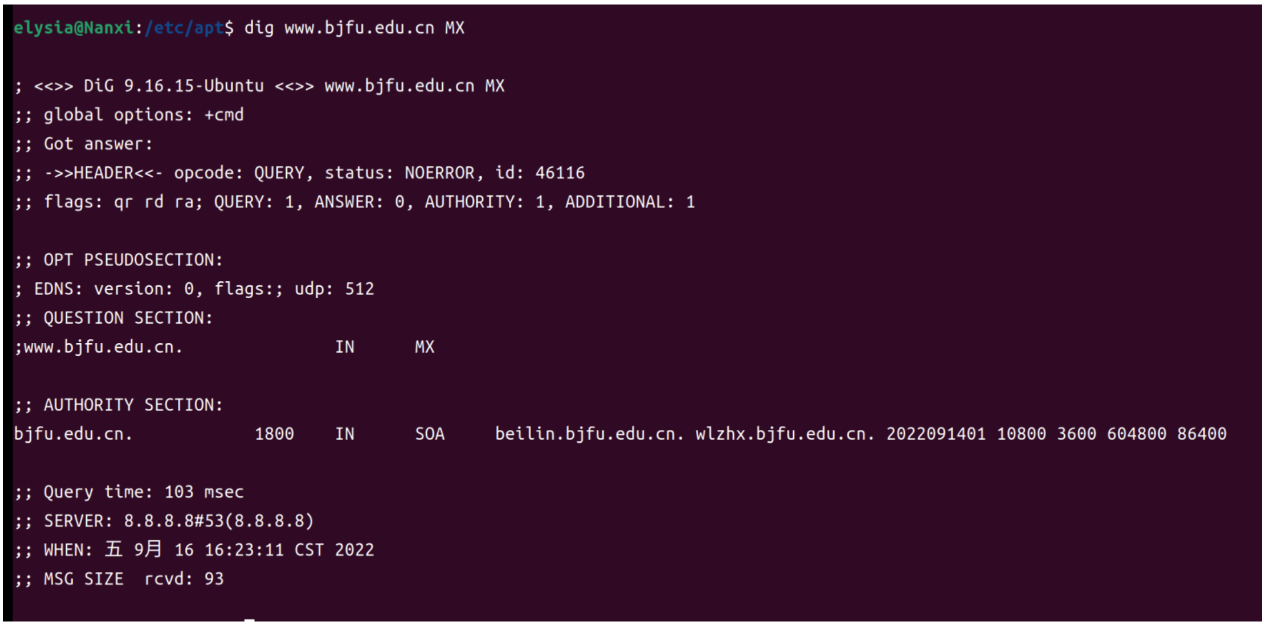


```
elysia@Nanxi:/etc/apt$ dig www.bjfu.edu.cn

; <<>> DiG 9.16.15-Ubuntu <<>> www.bjfu.edu.cn
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46080
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bjfu.edu.cn.               IN      A

;; ANSWER SECTION:
www.bjfu.edu.cn.        21516   IN      A       202.204.112.10

;; Query time: 48 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 16:21:22 CST 2022
;; MSG SIZE  rcvd: 60
```

ii

北林域名服务器名：beilin.bjfu.edu.cn.

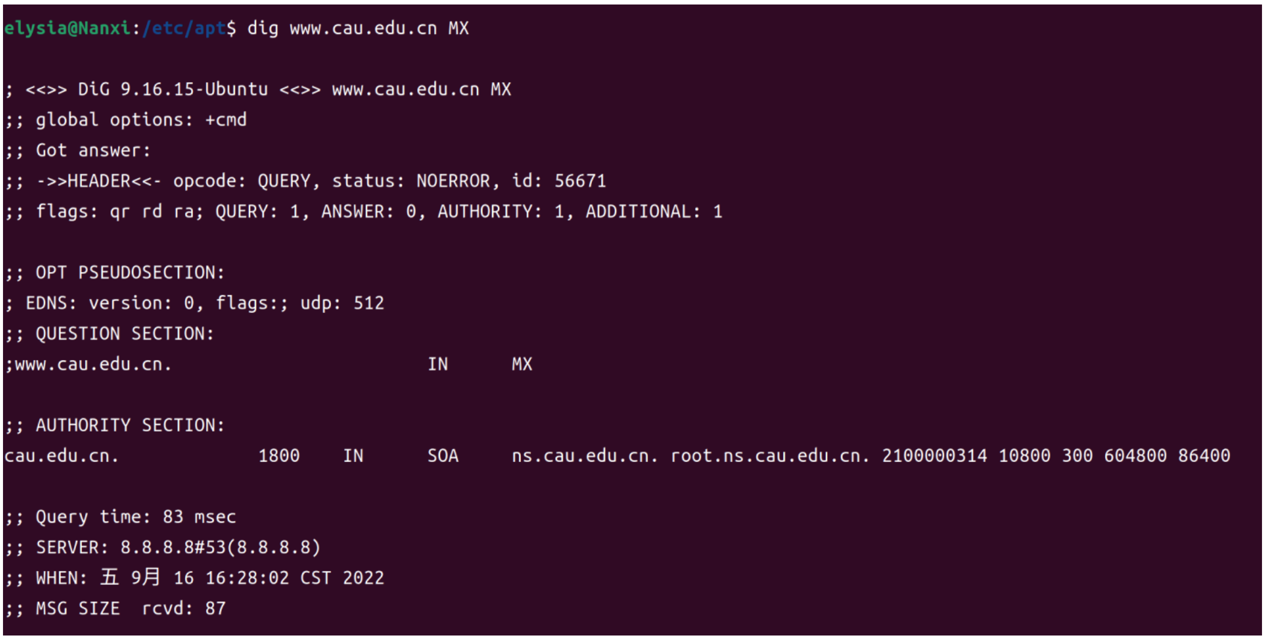
邮件服务器名：wlzhx.bjfu.edu.cn.



```
elysia@Nanxi:/etc/apt$ dig www.bjfu.edu.cn MX

; <<>> DiG 9.16.15-Ubuntu <<>> www.bjfu.edu.cn MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46116
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.bjfu.edu.cn.               IN      MX

;; AUTHORITY SECTION:
bjfu.edu.cn.            1800    IN      SOA     beilin.bjfu.edu.cn. wlzhx.bjfu.edu.cn. 2022091401 10800 3600 604800 86400

;; Query time: 103 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 16:23:11 CST 2022
;; MSG SIZE  rcvd: 93
```

中农域名服务器名：ns.cau.edu.cn.

邮件服务器名：root.ns.cau.edu.cn.



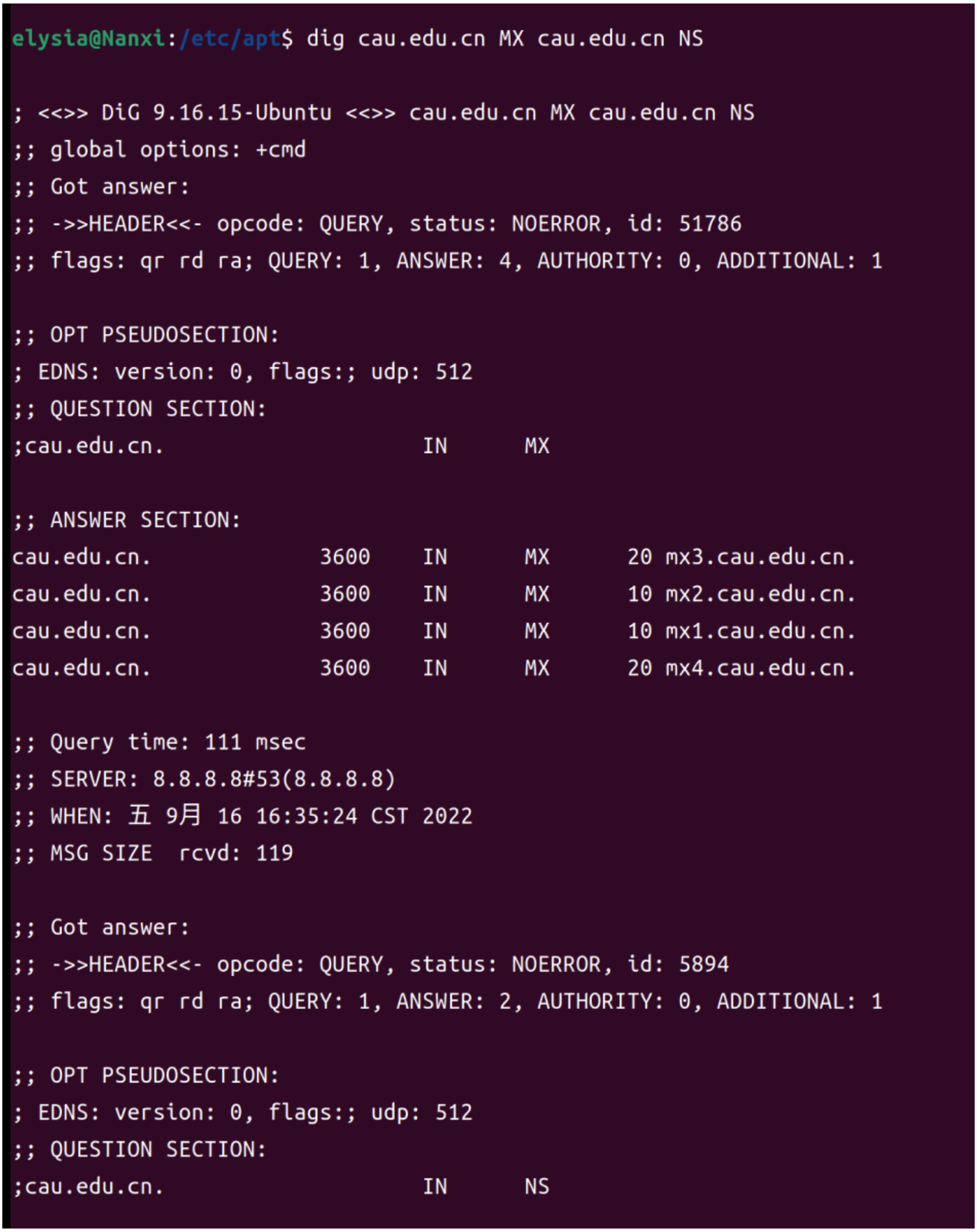
```
elysia@Nanxi:/etc/apt$ dig www.cau.edu.cn MX

; <<>> DiG 9.16.15-Ubuntu <<>> www.cau.edu.cn MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56671
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.cau.edu.cn.                IN      MX

;; AUTHORITY SECTION:
cau.edu.cn.             1800    IN      SOA     ns.cau.edu.cn. root.ns.cau.edu.cn. 2100000314 10800 300 604800 86400

;; Query time: 83 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 16:28:02 CST 2022
;; MSG SIZE  rcvd: 87
```

iii

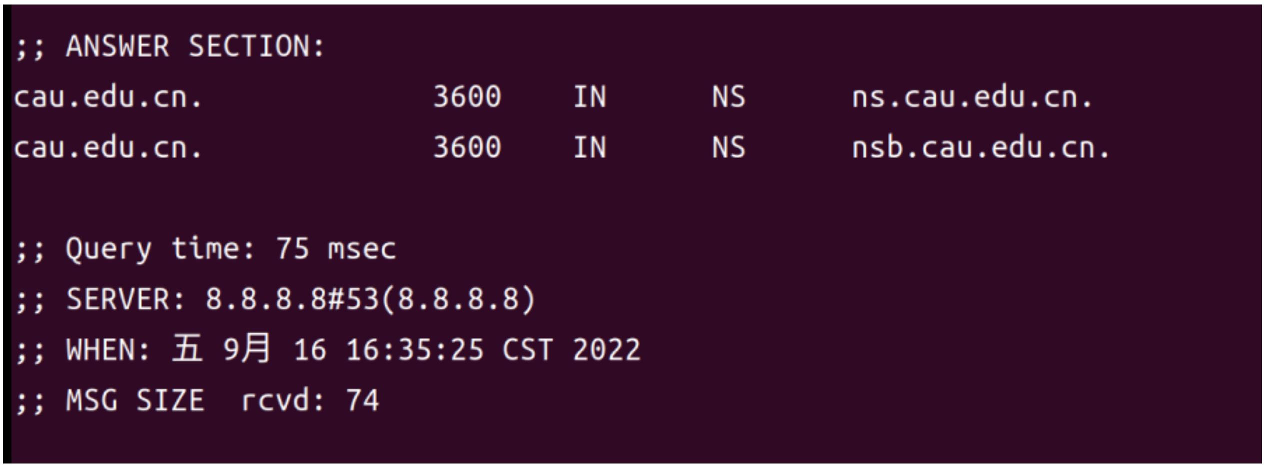
NS：ns.cau.edu.cn，nsb.cau.edu.cn

邮件服务器记录：

- 20 mx3.cau.edu.cn.
- 10 mx2.cau.edu.cn.
- 10 mx1.cau.edu.cn.
- 20 mx4.cau.edu.cn.

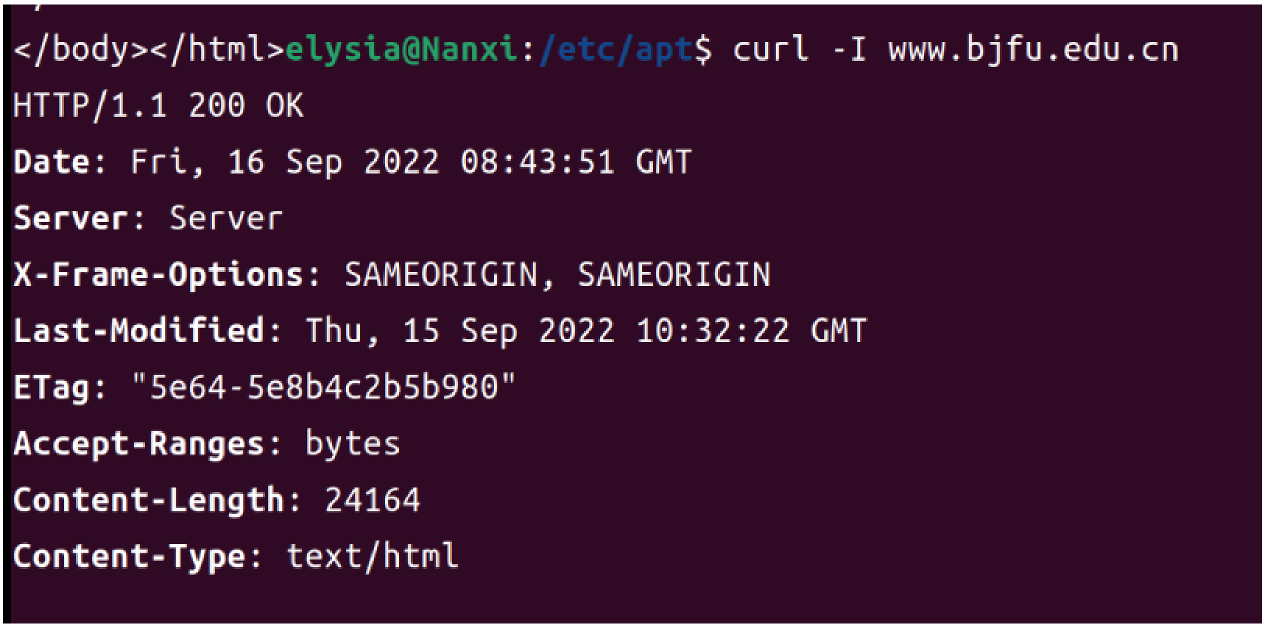


```
elysia@Nanxi:/etc/apt$ dig cau.edu.cn MX cau.edu.cn NS

; <<>> DiG 9.16.15-Ubuntu <<>> cau.edu.cn MX cau.edu.cn NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51786
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cau.edu.cn.                    IN      MX

;; ANSWER SECTION:
cau.edu.cn.             3600    IN      MX      20 mx3.cau.edu.cn.
cau.edu.cn.             3600    IN      MX      10 mx2.cau.edu.cn.
cau.edu.cn.             3600    IN      MX      10 mx1.cau.edu.cn.
cau.edu.cn.             3600    IN      MX      20 mx4.cau.edu.cn.

;; Query time: 111 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 16:35:24 CST 2022
;; MSG SIZE  rcvd: 119

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5894
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cau.edu.cn.                    IN      NS
```



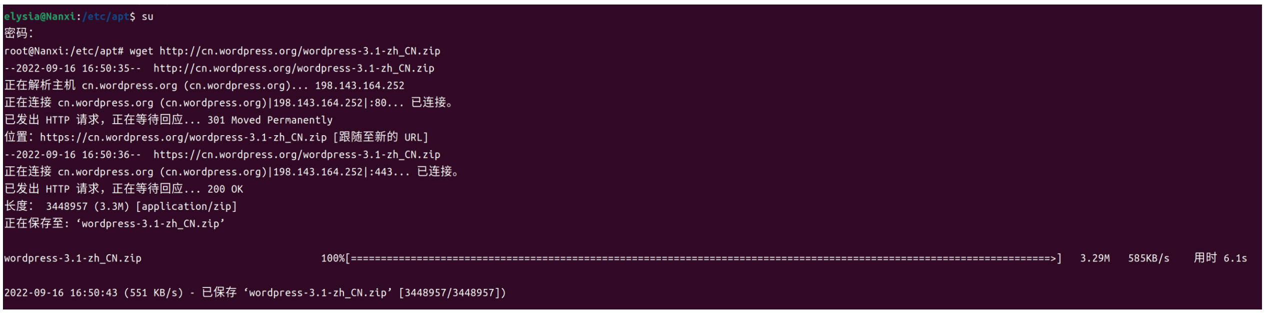
```
;; ANSWER SECTION:
cau.edu.cn.             3600    IN      NS      ns.cau.edu.cn.
cau.edu.cn.             3600    IN      NS      nsb.cau.edu.cn.

;; Query time: 75 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: 五 9月 16 16:35:25 CST 2022
;; MSG SIZE  rcvd: 74
```

b



```
</body></html>elysia@Nanxi:/etc/apt$ curl -I www.bjfu.edu.cn
HTTP/1.1 200 OK
Date: Fri, 16 Sep 2022 08:43:51 GMT
Server: Server
X-Frame-Options: SAMEORIGIN, SAMEORIGIN
Last-Modified: Thu, 15 Sep 2022 10:32:22 GMT
ETag: "5e64-5e8b4c2b5b980"
Accept-Ranges: bytes
Content-Length: 24164
Content-Type: text/html
```

c



```
elysia@Nanxi:/etc/apt$ su
密码：
root@Nanxi:/etc/apt# wget http://cn.wordpress.org/wordpress-3.1-zh_CN.zip
--2022-09-16 16:50:35--  http://cn.wordpress.org/wordpress-3.1-zh_CN.zip
正在解析主机 cn.wordpress.org (cn.wordpress.org)... 198.143.164.252
正在连接 cn.wordpress.org (cn.wordpress.org)|198.143.164.252|:80... 已连接。
已发出 HTTP 请求，正在等待回应... 301 Moved Permanently
位置：https://cn.wordpress.org/wordpress-3.1-zh_CN.zip [跟随至新的 URL]
--2022-09-16 16:50:36--  https://cn.wordpress.org/wordpress-3.1-zh_CN.zip
正在连接 cn.wordpress.org (cn.wordpress.org)|198.143.164.252|:443... 已连接。
已发出 HTTP 请求，正在等待回应... 200 OK
长度： 3448957 (3.3M) [application/zip]
正在保存至：‘wordpress-3.1-zh_CN.zip’

wordpress-3.1-zh_CN.zip                              100%[=====================================================================================================================>]   3.29M   585KB/s    用时 6.1s

2022-09-16 16:50:43 (551 KB/s) - 已保存 ‘wordpress-3.1-zh_CN.zip’ [3448957/3448957])
```