Dnstracer

dnstracer确定给定的域名服务器(DNS)从何处获取信息，并跟踪DNS服务器链返回到知道数据的服务器。

一，帮助手册

DNSTRACER版本1.8.1 - (c) Edwin Groothuis - http://www.mavetju.org
使用方法:dnstracer【选项】【主机】
-c 禁用本地缓存，默认启用
-C 启用负缓存，默认禁用
-o:启用收到答案的概述，默认禁用
-q :用于DNS请求的查询类型，默认为A
-r <重试>:DNS请求的重试次数，默认为3
-s :使用此服务器作为初始请求，默认的本地主机
如果。指定,A.ROOT-SERVERS。将使用NET。
-t <最大超时>:限制每次尝试的等待时间

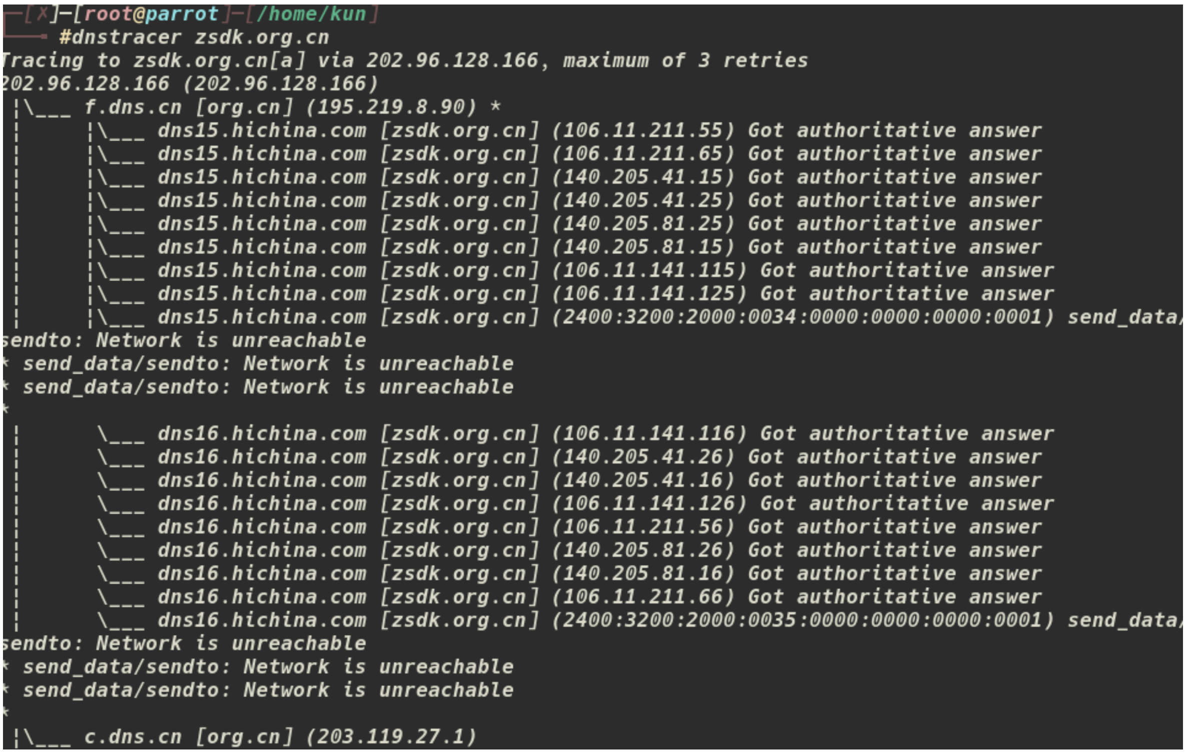
- v:详细
  -S <ip地址>:使用此源地址。</ip地址>
  不要查询IPv6服务器

```
DNSTRACER version 1.8.1 - (c) Edwin Groothuis - http://www.mavetju.org
Usage: dnstracer [options] [host]
    -c: disable local caching, default enabled
    -C: enable negative caching, default disabled
    -o: enable overview of received answers, default disabled
    -q : query-type to use for the DNS requests, default A
    -r : amount of retries for DNS requests, default 3
    -s : use this server for the initial request, default localhost
         If . is specified, A.ROOT-SERVERS.NET will be used.
    -t : Limit time to wait per try
    -v: verbose
    -S : use this source address.
    -4: don't query IPv6 servers
```

二，命令实例

dnstracer zsdk.org.cn

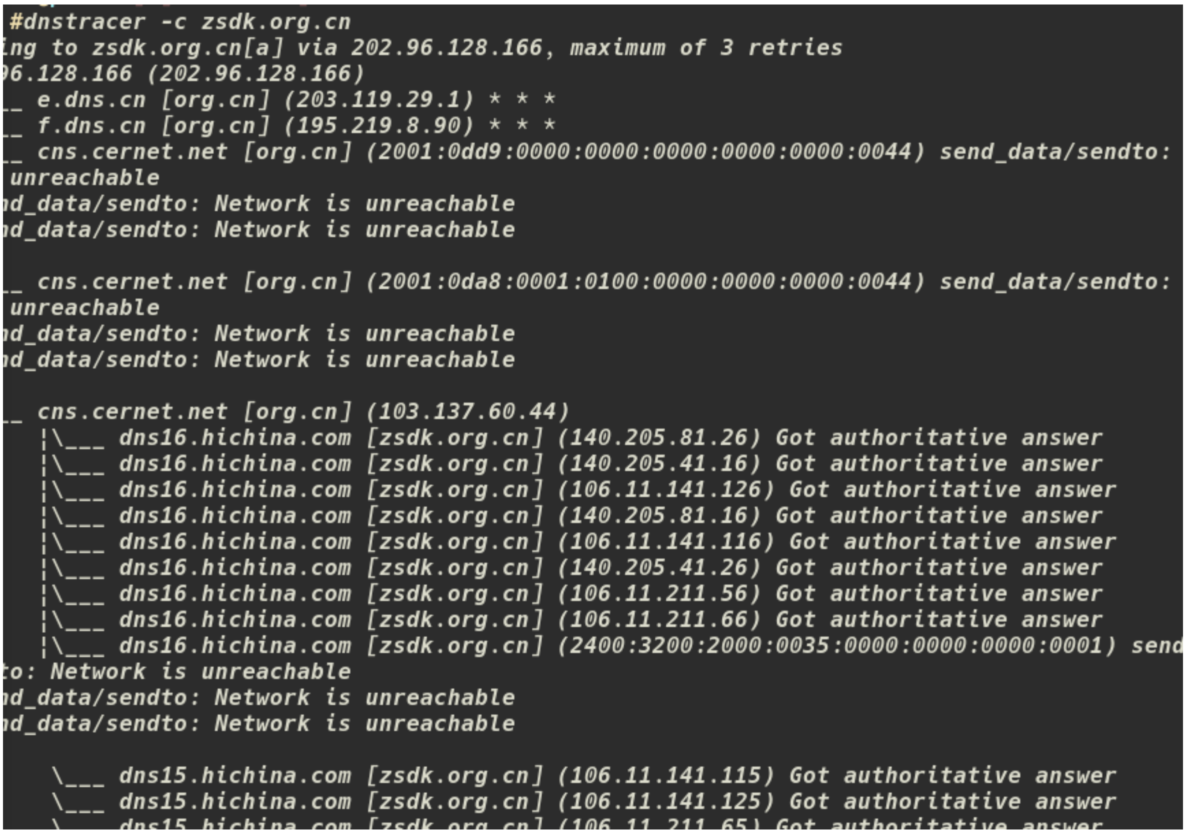
追踪zsdk.org.cn，DNS服务信息



```
┌─[✗]─[root@parrot]─[/home/kun]
└──╼ #dnstracer zsdk.org.cn
Tracing to zsdk.org.cn[a] via 202.96.128.166, maximum of 3 retries
202.96.128.166 (202.96.128.166)
 |\___ f.dns.cn [org.cn] (195.219.8.90) *
 |      |\___ dns15.hichina.com [zsdk.org.cn] (106.11.211.55) Got authoritative answer
 |      |\___ dns15.hichina.com [zsdk.org.cn] (106.11.211.65) Got authoritative answer
 |      |\___ dns15.hichina.com [zsdk.org.cn] (140.205.41.15) Got authoritative answer
 |      |\___ dns15.hichina.com [zsdk.org.cn] (140.205.41.25) Got authoritative answer
 |      |\___ dns15.hichina.com [zsdk.org.cn] (140.205.81.25) Got authoritative answer
 |      |\___ dns15.hichina.com [zsdk.org.cn] (140.205.81.15) Got authoritative answer
 |      |\___ dns15.hichina.com [zsdk.org.cn] (106.11.141.115) Got authoritative answer
 |      |\___ dns15.hichina.com [zsdk.org.cn] (106.11.141.125) Got authoritative answer
 |      |\___ dns15.hichina.com [zsdk.org.cn] (2400:3200:2000:0034:0000:0000:0000:0001) send_data/
sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
*
 |       \___ dns16.hichina.com [zsdk.org.cn] (106.11.141.116) Got authoritative answer
 |       \___ dns16.hichina.com [zsdk.org.cn] (140.205.41.26) Got authoritative answer
 |       \___ dns16.hichina.com [zsdk.org.cn] (140.205.41.16) Got authoritative answer
 |       \___ dns16.hichina.com [zsdk.org.cn] (106.11.141.126) Got authoritative answer
 |       \___ dns16.hichina.com [zsdk.org.cn] (106.11.211.56) Got authoritative answer
 |       \___ dns16.hichina.com [zsdk.org.cn] (140.205.81.26) Got authoritative answer
 |       \___ dns16.hichina.com [zsdk.org.cn] (140.205.81.16) Got authoritative answer
 |       \___ dns16.hichina.com [zsdk.org.cn] (106.11.211.66) Got authoritative answer
 |       \___ dns16.hichina.com [zsdk.org.cn] (2400:3200:2000:0035:0000:0000:0000:0001) send_data/
sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
*
 |\___ c.dns.cn [org.cn] (203.119.27.1)
```

dnstracer -c zsdk.org.cn

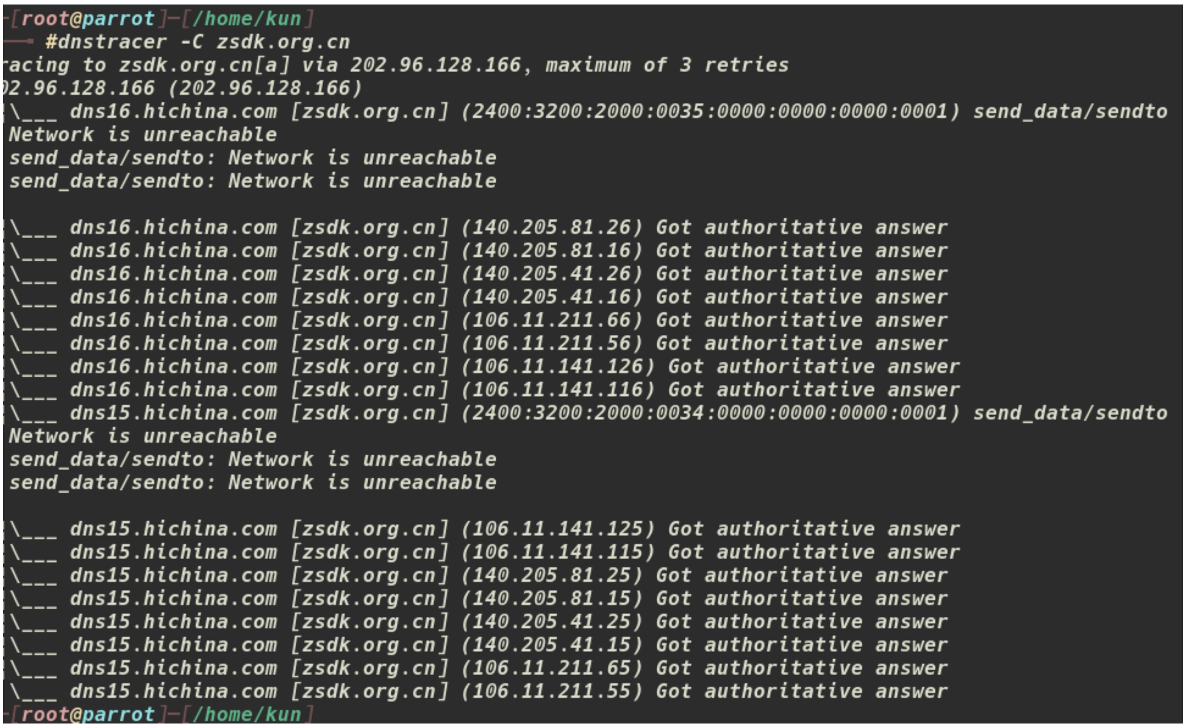
不对此次枚举做DNS缓存[^DNS缓存]



```
 #dnstracer -c zsdk.org.cn
ing to zsdk.org.cn[a] via 202.96.128.166, maximum of 3 retries
96.128.166 (202.96.128.166)
__ e.dns.cn [org.cn] (203.119.29.1) * * *
__ f.dns.cn [org.cn] (195.219.8.90) * * *
__ cns.cernet.net [org.cn] (2001:0dd9:0000:0000:0000:0000:0000:0044) send_data/sendto:
 unreachable
nd_data/sendto: Network is unreachable
nd_data/sendto: Network is unreachable

__ cns.cernet.net [org.cn] (2001:0da8:0001:0100:0000:0000:0000:0044) send_data/sendto:
 unreachable
nd_data/sendto: Network is unreachable
nd_data/sendto: Network is unreachable

__ cns.cernet.net [org.cn] (103.137.60.44)
   |\___ dns16.hichina.com [zsdk.org.cn] (140.205.81.26) Got authoritative answer
   |\___ dns16.hichina.com [zsdk.org.cn] (140.205.41.16) Got authoritative answer
   |\___ dns16.hichina.com [zsdk.org.cn] (106.11.141.126) Got authoritative answer
   |\___ dns16.hichina.com [zsdk.org.cn] (140.205.81.16) Got authoritative answer
   |\___ dns16.hichina.com [zsdk.org.cn] (106.11.141.116) Got authoritative answer
   |\___ dns16.hichina.com [zsdk.org.cn] (140.205.41.26) Got authoritative answer
   |\___ dns16.hichina.com [zsdk.org.cn] (106.11.211.56) Got authoritative answer
   |\___ dns16.hichina.com [zsdk.org.cn] (106.11.211.66) Got authoritative answer
   |\___ dns16.hichina.com [zsdk.org.cn] (2400:3200:2000:0035:0000:0000:0000:0001) send
to: Network is unreachable
nd_data/sendto: Network is unreachable
nd_data/sendto: Network is unreachable

    \___ dns15.hichina.com [zsdk.org.cn] (106.11.141.115) Got authoritative answer
    \___ dns15.hichina.com [zsdk.org.cn] (106.11.141.125) Got authoritative answer
    \___ dns15.hichina.com [zsdk.org.cn] (106.11.211.65) Got authoritative answer
```

dnstracer -C zsdk.org.cn

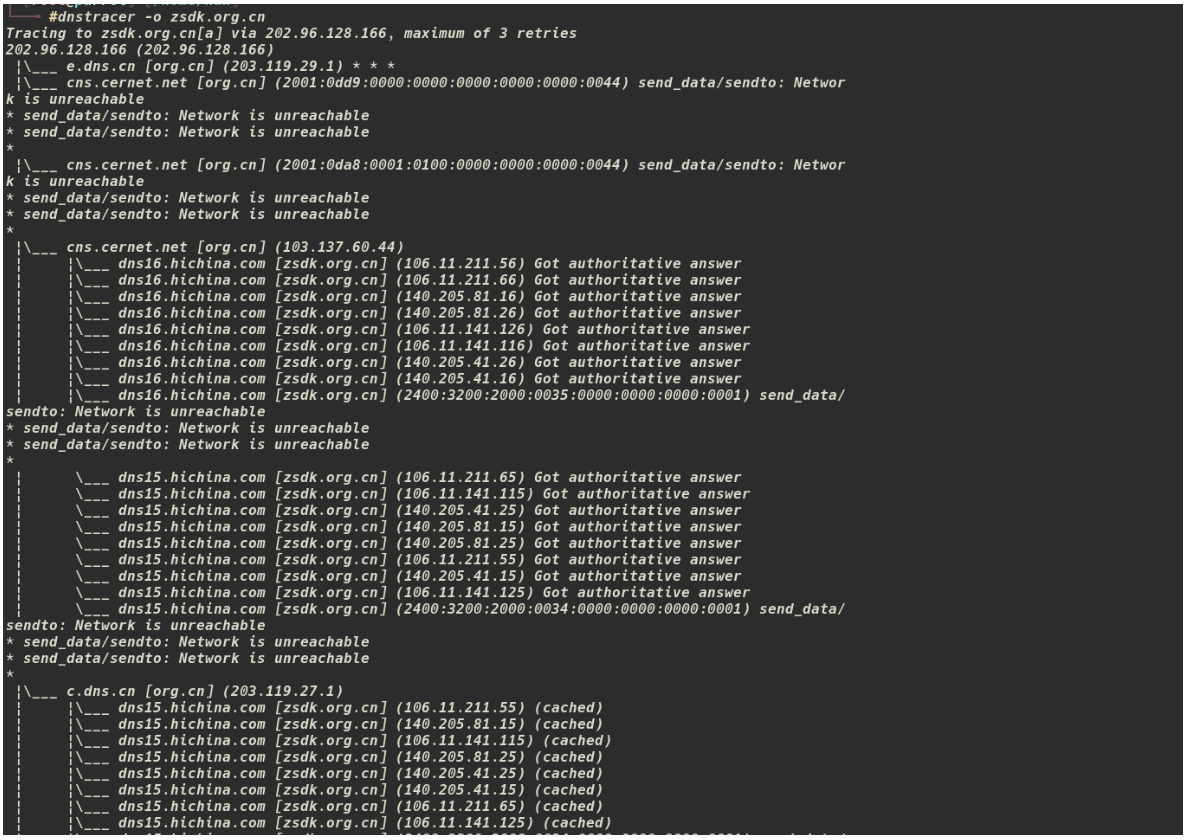
启用负缓存[^默认禁用]



```
-[root@parrot]-[/home/kun]
 ──╼ #dnstracer -C zsdk.org.cn
racing to zsdk.org.cn[a] via 202.96.128.166, maximum of 3 retries
2.96.128.166 (202.96.128.166)
 \___ dns16.hichina.com [zsdk.org.cn] (2400:3200:2000:0035:0000:0000:0000:0001) send_data/sendto
 Network is unreachable
 send_data/sendto: Network is unreachable
 send_data/sendto: Network is unreachable

 \___ dns16.hichina.com [zsdk.org.cn] (140.205.81.26) Got authoritative answer
 \___ dns16.hichina.com [zsdk.org.cn] (140.205.81.16) Got authoritative answer
 \___ dns16.hichina.com [zsdk.org.cn] (140.205.41.26) Got authoritative answer
 \___ dns16.hichina.com [zsdk.org.cn] (140.205.41.16) Got authoritative answer
 \___ dns16.hichina.com [zsdk.org.cn] (106.11.211.66) Got authoritative answer
 \___ dns16.hichina.com [zsdk.org.cn] (106.11.211.56) Got authoritative answer
 \___ dns16.hichina.com [zsdk.org.cn] (106.11.141.126) Got authoritative answer
 \___ dns16.hichina.com [zsdk.org.cn] (106.11.141.116) Got authoritative answer
 \___ dns15.hichina.com [zsdk.org.cn] (2400:3200:2000:0034:0000:0000:0000:0001) send_data/sendto
 Network is unreachable
 send_data/sendto: Network is unreachable
 send_data/sendto: Network is unreachable

 \___ dns15.hichina.com [zsdk.org.cn] (106.11.141.125) Got authoritative answer
 \___ dns15.hichina.com [zsdk.org.cn] (106.11.141.115) Got authoritative answer
 \___ dns15.hichina.com [zsdk.org.cn] (140.205.81.25) Got authoritative answer
 \___ dns15.hichina.com [zsdk.org.cn] (140.205.81.15) Got authoritative answer
 \___ dns15.hichina.com [zsdk.org.cn] (140.205.41.25) Got authoritative answer
 \___ dns15.hichina.com [zsdk.org.cn] (140.205.41.15) Got authoritative answer
 \___ dns15.hichina.com [zsdk.org.cn] (106.11.211.65) Got authoritative answer
 \___ dns15.hichina.com [zsdk.org.cn] (106.11.211.55) Got authoritative answer
-[root@parrot]-[/home/kun]
```

dnstracer -o zsdk.org.cn

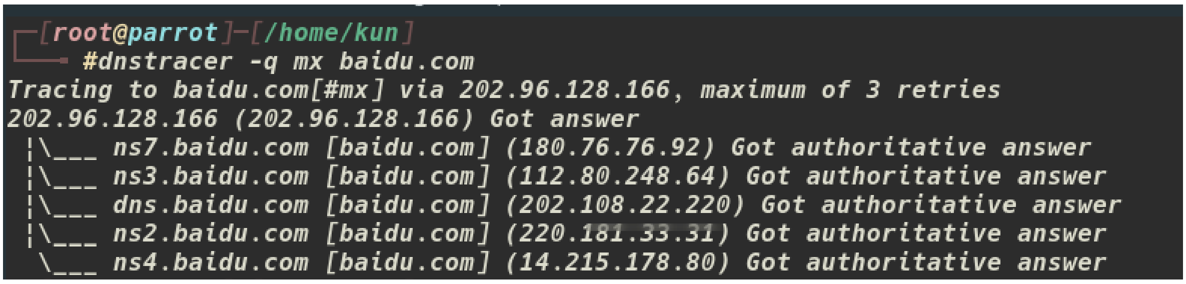
启用收到的答案概述，默认是启用的



```
 └──╼ #dnstracer -o zsdk.org.cn
Tracing to zsdk.org.cn[a] via 202.96.128.166, maximum of 3 retries
202.96.128.166 (202.96.128.166)
 ¦\___ e.dns.cn [org.cn] (203.119.29.1) * * *
 ¦\___ cns.cernet.net [org.cn] (2001:0dd9:0000:0000:0000:0000:0000:0044) send_data/sendto: Networ
k is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
*
 ¦\___ cns.cernet.net [org.cn] (2001:0da8:0001:0100:0000:0000:0000:0044) send_data/sendto: Networ
k is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
*
 ¦\___ cns.cernet.net [org.cn] (103.137.60.44)
 ¦     ¦\___ dns16.hichina.com [zsdk.org.cn] (106.11.211.56) Got authoritative answer
 ¦     ¦\___ dns16.hichina.com [zsdk.org.cn] (106.11.211.66) Got authoritative answer
 ¦     ¦\___ dns16.hichina.com [zsdk.org.cn] (140.205.81.16) Got authoritative answer
 ¦     ¦\___ dns16.hichina.com [zsdk.org.cn] (140.205.81.26) Got authoritative answer
 ¦     ¦\___ dns16.hichina.com [zsdk.org.cn] (106.11.141.126) Got authoritative answer
 ¦     ¦\___ dns16.hichina.com [zsdk.org.cn] (106.11.141.116) Got authoritative answer
 ¦     ¦\___ dns16.hichina.com [zsdk.org.cn] (140.205.41.26) Got authoritative answer
 ¦     ¦\___ dns16.hichina.com [zsdk.org.cn] (140.205.41.16) Got authoritative answer
 ¦     ¦\___ dns16.hichina.com [zsdk.org.cn] (2400:3200:2000:0035:0000:0000:0000:0001) send_data/
sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
*
 ¦      \___ dns15.hichina.com [zsdk.org.cn] (106.11.211.65) Got authoritative answer
 ¦      \___ dns15.hichina.com [zsdk.org.cn] (106.11.141.115) Got authoritative answer
 ¦      \___ dns15.hichina.com [zsdk.org.cn] (140.205.41.25) Got authoritative answer
 ¦      \___ dns15.hichina.com [zsdk.org.cn] (140.205.81.15) Got authoritative answer
 ¦      \___ dns15.hichina.com [zsdk.org.cn] (140.205.81.25) Got authoritative answer
 ¦      \___ dns15.hichina.com [zsdk.org.cn] (106.11.211.55) Got authoritative answer
 ¦      \___ dns15.hichina.com [zsdk.org.cn] (140.205.41.15) Got authoritative answer
 ¦      \___ dns15.hichina.com [zsdk.org.cn] (106.11.141.125) Got authoritative answer
 ¦      \___ dns15.hichina.com [zsdk.org.cn] (2400:3200:2000:0034:0000:0000:0000:0001) send_data/
sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
*
 ¦\___ c.dns.cn [org.cn] (203.119.27.1)
 ¦     ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.211.55) (cached)
 ¦     ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.81.15) (cached)
 ¦     ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.141.115) (cached)
 ¦     ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.81.25) (cached)
 ¦     ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.41.25) (cached)
 ¦     ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.41.15) (cached)
 ¦     ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.211.65) (cached)
 ¦     ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.141.125) (cached)
```

dnstracer -q mx baidu.com

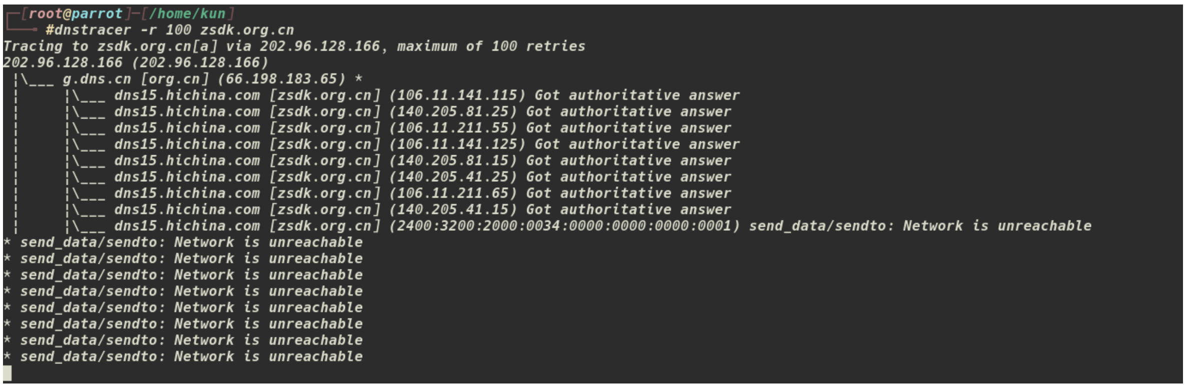
检索baidu的mx记录[^默认为A记录]



```
┌─[root@parrot]─[/home/kun]
└──╼ #dnstracer -q mx baidu.com
Tracing to baidu.com[#mx] via 202.96.128.166, maximum of 3 retries
202.96.128.166 (202.96.128.166) Got answer
 ¦\___ ns7.baidu.com [baidu.com] (180.76.76.92) Got authoritative answer
 ¦\___ ns3.baidu.com [baidu.com] (112.80.248.64) Got authoritative answer
 ¦\___ dns.baidu.com [baidu.com] (202.108.22.220) Got authoritative answer
 ¦\___ ns2.baidu.com [baidu.com] (220.181.33.31) Got authoritative answer
  \___ ns4.baidu.com [baidu.com] (14.215.178.80) Got authoritative answer
```

dnstracer -r 100 zsdk.org.cn

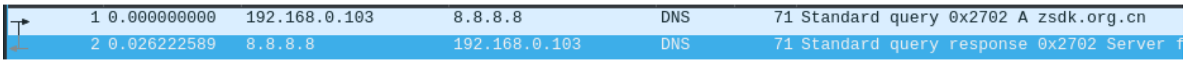
重试的请求次数为100,默认为3,此处重次请求次数为100。



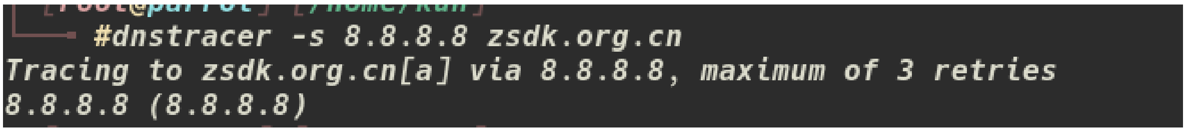
```
┌─[root@parrot]─[/home/kun]
└──╼ #dnstracer -r 100 zsdk.org.cn
Tracing to zsdk.org.cn[a] via 202.96.128.166, maximum of 100 retries
202.96.128.166 (202.96.128.166)
 ¦\___ g.dns.cn [org.cn] (66.198.183.65) *
 ¦      ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.141.115) Got authoritative answer
 ¦      ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.81.25) Got authoritative answer
 ¦      ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.211.55) Got authoritative answer
 ¦      ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.141.125) Got authoritative answer
 ¦      ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.81.15) Got authoritative answer
 ¦      ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.41.25) Got authoritative answer
 ¦      ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.211.65) Got authoritative answer
 ¦      ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.41.15) Got authoritative answer
 ¦      ¦\___ dns15.hichina.com [zsdk.org.cn] (2400:3200:2000:0034:0000:0000:0000:0001) send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
```

dnstracer -s 8.8.8.8 zsdk.org.cn

使用8.8.8.8DNS服务器对zsdk.org.cn进行握手[^指定DNS服务器，默认与服务器握手3次]



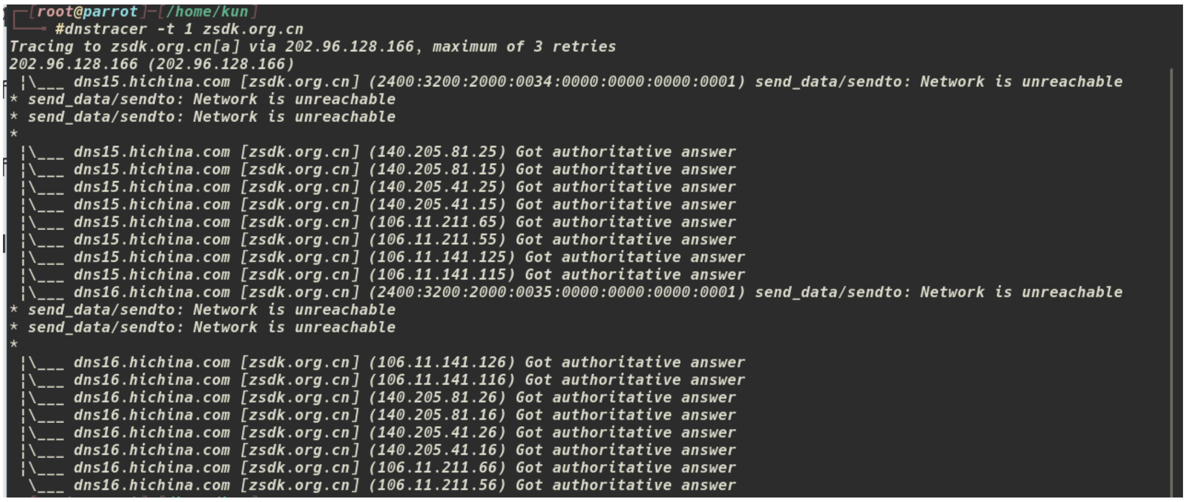
```
    1 0.000000000   192.168.0.103      8.8.8.8          DNS       71 Standard query 0x2702 A zsdk.org.cn
    2 0.026222589   8.8.8.8            192.168.0.103    DNS       71 Standard query response 0x2702 Server f
```



```
┌─[root@parrot]─[/home/kun]
└──╼ #dnstracer -s 8.8.8.8 zsdk.org.cn
Tracing to zsdk.org.cn[a] via 8.8.8.8, maximum of 3 retries
8.8.8.8 (8.8.8.8)
```

dnstracer -t 1 zsdk.org.cn

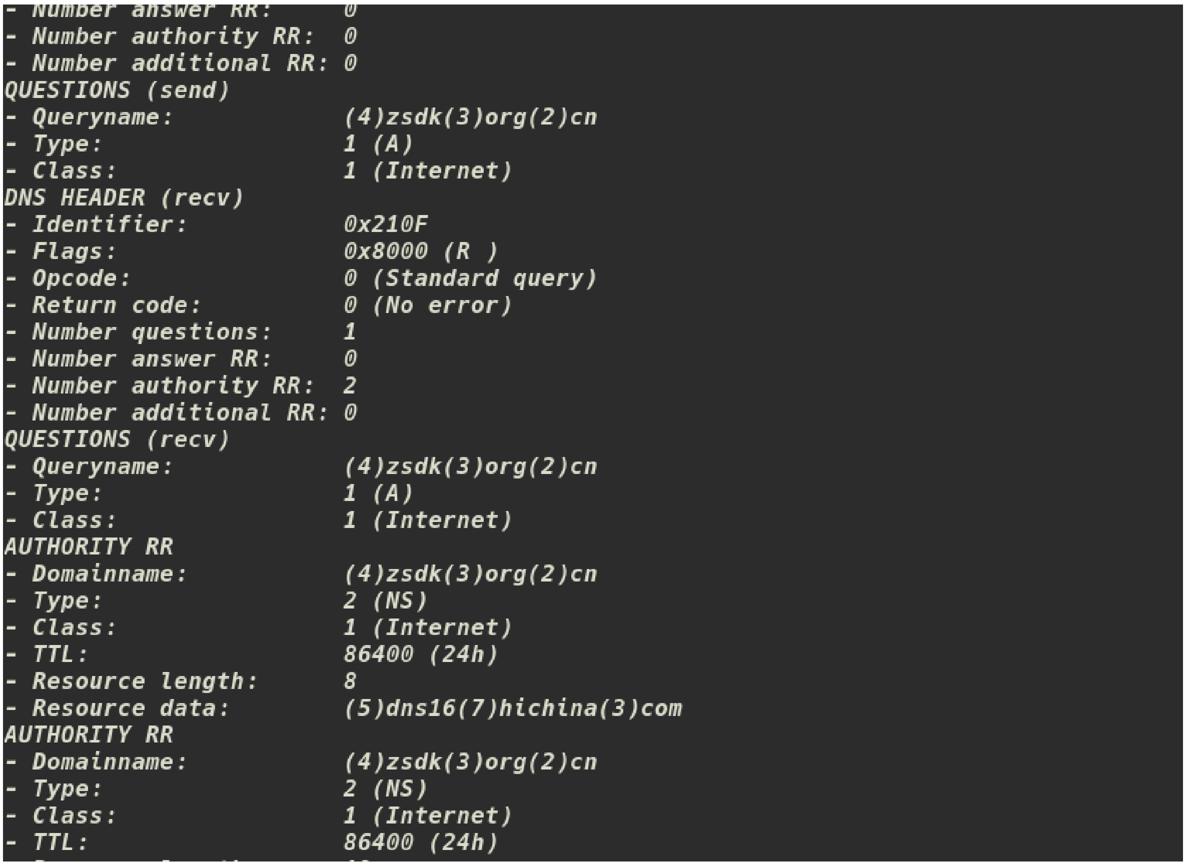
超过1秒则放弃与服务器进行握手[^等待值限制]



```
┌─[root@parrot]─[/home/kun]
└──╼ #dnstracer -t 1 zsdk.org.cn
Tracing to zsdk.org.cn[a] via 202.96.128.166, maximum of 3 retries
202.96.128.166 (202.96.128.166)
 ¦\___ dns15.hichina.com [zsdk.org.cn] (2400:3200:2000:0034:0000:0000:0000:0001) send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
*
 ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.81.25) Got authoritative answer
 ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.81.15) Got authoritative answer
 ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.41.25) Got authoritative answer
 ¦\___ dns15.hichina.com [zsdk.org.cn] (140.205.41.15) Got authoritative answer
 ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.211.65) Got authoritative answer
 ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.211.55) Got authoritative answer
 ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.141.125) Got authoritative answer
 ¦\___ dns15.hichina.com [zsdk.org.cn] (106.11.141.115) Got authoritative answer
 ¦\___ dns16.hichina.com [zsdk.org.cn] (2400:3200:2000:0035:0000:0000:0000:0001) send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
* send_data/sendto: Network is unreachable
*
 ¦\___ dns16.hichina.com [zsdk.org.cn] (106.11.141.126) Got authoritative answer
 ¦\___ dns16.hichina.com [zsdk.org.cn] (106.11.141.116) Got authoritative answer
 ¦\___ dns16.hichina.com [zsdk.org.cn] (140.205.81.26) Got authoritative answer
 ¦\___ dns16.hichina.com [zsdk.org.cn] (140.205.81.16) Got authoritative answer
 ¦\___ dns16.hichina.com [zsdk.org.cn] (140.205.41.26) Got authoritative answer
 ¦\___ dns16.hichina.com [zsdk.org.cn] (140.205.41.16) Got authoritative answer
 ¦\___ dns16.hichina.com [zsdk.org.cn] (106.11.211.66) Got authoritative answer
  \___ dns16.hichina.com [zsdk.org.cn] (106.11.211.56) Got authoritative answer
```

dnstracer -v zsdk.org.cn

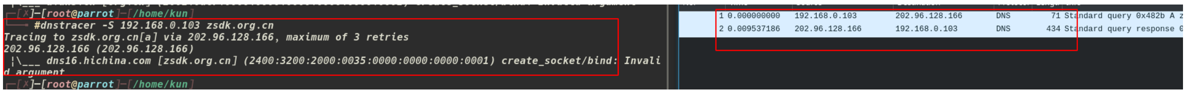
枚举zsdk.org.cn详细DNS信息



```
- Number answer RR:     0
- Number authority RR:  0
- Number additional RR: 0
QUESTIONS (send)
- Queryname:            (4)zsdk(3)org(2)cn
- Type:                 1 (A)
- Class:                1 (Internet)
DNS HEADER (recv)
- Identifier:           0x210F
- Flags:                0x8000 (R )
- Opcode:               0 (Standard query)
- Return code:          0 (No error)
- Number questions:     1
- Number answer RR:     0
- Number authority RR:  2
- Number additional RR: 0
QUESTIONS (recv)
- Queryname:            (4)zsdk(3)org(2)cn
- Type:                 1 (A)
- Class:                1 (Internet)
AUTHORITY RR
- Domainname:           (4)zsdk(3)org(2)cn
- Type:                 2 (NS)
- Class:                1 (Internet)
- TTL:                  86400 (24h)
- Resource length:      8
- Resource data:        (5)dns16(7)hichina(3)com
AUTHORITY RR
- Domainname:           (4)zsdk(3)org(2)cn
- Type:                 2 (NS)
- Class:                1 (Internet)
- TTL:                  86400 (24h)
```

dnstracer -S 192.168.0.103 zsdk.org.cn

使用源地址对zsdk.org.cn进行枚举

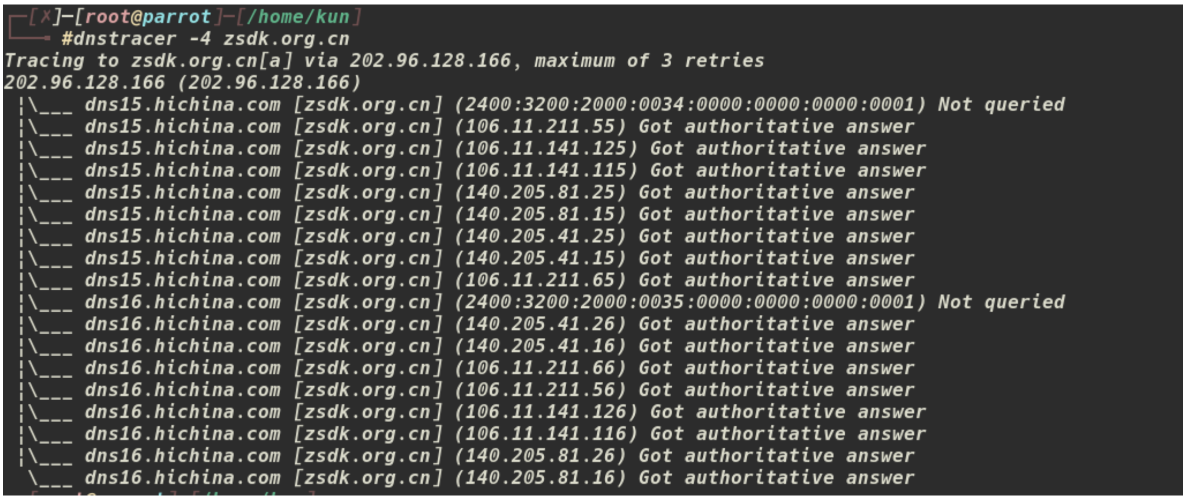


```
┌─[✗]─[root@parrot]─[/home/kun]
└──╼ #dnstracer -S 192.168.0.103 zsdk.org.cn
Tracing to zsdk.org.cn[a] via 202.96.128.166, maximum of 3 retries
202.96.128.166 (202.96.128.166)
 |\___ dns16.hichina.com [zsdk.org.cn] (2400:3200:2000:0035:0000:0000:0000:0001) create_socket/bind: Invali
d argument
┌─[✗]─[root@parrot]─[/home/kun]
```

```
1 0.000000000   192.168.0.103    202.96.128.166   DNS    71 Standard query 0x482b A z
2 0.009537186   202.96.128.166   192.168.0.103    DNS   434 Standard query response 0
```

dnstracer -4 zsdk.org.cn

不枚举IPv6服务器



```
┌─[✗]─[root@parrot]─[/home/kun]
└──╼ #dnstracer -4 zsdk.org.cn
Tracing to zsdk.org.cn[a] via 202.96.128.166, maximum of 3 retries
202.96.128.166 (202.96.128.166)
 |\___ dns15.hichina.com [zsdk.org.cn] (2400:3200:2000:0034:0000:0000:0000:0001) Not queried
 |\___ dns15.hichina.com [zsdk.org.cn] (106.11.211.55) Got authoritative answer
 |\___ dns15.hichina.com [zsdk.org.cn] (106.11.141.125) Got authoritative answer
 |\___ dns15.hichina.com [zsdk.org.cn] (106.11.141.115) Got authoritative answer
 |\___ dns15.hichina.com [zsdk.org.cn] (140.205.81.25) Got authoritative answer
 |\___ dns15.hichina.com [zsdk.org.cn] (140.205.81.15) Got authoritative answer
 |\___ dns15.hichina.com [zsdk.org.cn] (140.205.41.25) Got authoritative answer
 |\___ dns15.hichina.com [zsdk.org.cn] (140.205.41.15) Got authoritative answer
 |\___ dns15.hichina.com [zsdk.org.cn] (106.11.211.65) Got authoritative answer
 |\___ dns16.hichina.com [zsdk.org.cn] (2400:3200:2000:0035:0000:0000:0000:0001) Not queried
 |\___ dns16.hichina.com [zsdk.org.cn] (140.205.41.26) Got authoritative answer
 |\___ dns16.hichina.com [zsdk.org.cn] (140.205.41.16) Got authoritative answer
 |\___ dns16.hichina.com [zsdk.org.cn] (106.11.211.66) Got authoritative answer
 |\___ dns16.hichina.com [zsdk.org.cn] (106.11.211.56) Got authoritative answer
 |\___ dns16.hichina.com [zsdk.org.cn] (106.11.141.126) Got authoritative answer
 |\___ dns16.hichina.com [zsdk.org.cn] (106.11.141.116) Got authoritative answer
 |\___ dns16.hichina.com [zsdk.org.cn] (140.205.81.26) Got authoritative answer
  \___ dns16.hichina.com [zsdk.org.cn] (140.205.81.16) Got authoritative answer
```