Domain Information Groper

Dig是域信息搜索器的简称(Domain Information Groper),使用dig命令可以执行查询域名相关的任务。

二，官方帮助手册
1.1原版
C:\root> dig -h
C： \root>挖-h
Usage: dig [@global-server] [domain] [q-type] [q-class] {q-opt}
用法：dig[@global server][domain][q-type][q-class]{q-opt}
{global-d-opt} host [@local-server] {local-d-opt}
{global-d-opt}主机[@local服务器]{local-d-opt}
[host [@local-server] {local-d-opt} [...]]
[主机[@local服务器]{local-d-opt}[...]]
Where: domain   is in the Domain Name System
其中：域在域名系统中
q-class is one of (in,hs,ch,...) [default: in]
q类是（in，hs，ch，...）[默认值：in]
q-type   is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]
q-type是（a，any，mx，ns，soa，hinfo，axfr，txt，...）之一[默认值：a]
(Use ixfr=version for type ixfr)
（使用ixfr=version作为类型ixfr）
q-opt   is one of:
q-opt是一个或：
-4   (use IPv4 query transport only)
-4（仅使用IPv4查询传输）
-6   (use IPv6 query transport only)
-6（仅使用IPv6查询传输）
-b address[#port]   (bind to source address/port)
-b地址[\35；端口]（绑定到源地址/端口）
-c class   (specify query class)
-c类（指定查询类）
-f filename   (batch mode)
-文件名（批处理模式）
-i   (use IP6.INT for IPv6 reverse lookups)
-i（使用IP6.INT进行IPv6反向查找）
-k keyfile   (specify tsig key file)
k密钥文件（指定tsig密钥文件）
-m   (enable memory usage debugging)
-m（启用内存使用调试）
-p port   (specify port number)
-p端口（指定端口号）
-q name   (specify query name)
-q名称（指定查询名称）
-t type   (specify query type)
-t类型（指定查询类型）
-u   (display times in usec instead of msec)
-u（显示时间和usec而不是msec）
-x dot-notation   (shortcut for reverse lookups)

-x点符号（反向查找的快捷方式）
-y [hmac:]name:key (specify named base64 tsig key)
-y[hmac:]name:key（指定命名为base64 tsig key）
d-opt   is of the form +keyword[=value], where keyword is:
d-opt的形式是+keyword[=value]，其中keyword是：
+[no]aaflag   (Set AA flag in query (+[no]aaflag))
+[否]AA flag（在查询中设置AA标志（+[否]aaflag））
+[no]aaonly   (Set AA flag in query (+[no]aaflag))
+[否]aaonly（在查询中设置AA标志（+[否]AA flag））
+[no]additional   (Control display of additional section)
+[否]附加（附加部分的控制显示）
+[no]adflag   (Set AD flag in query (default on))
+[否]adflag（在查询中设置AD标志（默认为打开））
+[no]all   (Set or clear all display flags)
+[否]全部（设置或清除所有显示标志）
+[no]answer   (Control display of answer section)
+[否]应答（应答区控制显示）
+[no]authority   (Control display of authority section)
+[否]权限（权限段控制显示）
+[no]badcookie   (Retry BADCOOKIE responses)
+[否]badcookie（重试badcookie响应）
+[no]besteffort   (Try to parse even illegal messages)
+[否]尽最大努力（甚至尝试解析非法消息）
+bufsize=###   (Set EDNS0 Max UDP packet size)
[设置EDNS0最大UDP数据包大小]
+[no]cdflag   (Set checking disabled flag in query)
+[否]cdflag（在查询中设置检查禁用标志）
+[no]class   (Control display of class in records)
+[否]类（控制记录中类的显示）
+[no]cmd   (Control display of command line)
+[否]命令（命令行的控制显示）
+[no]comments   (Control display of comment lines)
+[否]注释（控制注释行的显示）
+[no]cookie   (Add a COOKIE option to the request)
+[否]cookie（向请求添加cookie选项）
+[no]crypto   (Control display of cryptographic fields in records)
+[否]加密（控制记录中加密字段的显示）
+[no]defname   (Use search list (+[no]search))
+[否]defname（使用搜索列表（+[否]搜索））
+[no]dnssec   (Request DNSSEC records)
+[否]dnssec（请求dnssec记录）
+domain=###   (Set default domainname)
+域=\35；\35；\35；（设置默认域名）
+[no]dscp[=###]   (Set the DSCP value to ### [0..63])
+[否]dscp[=\35；\35；\35；]（将dscp值设置为\35；\35；\353]）
+[no]edns[=###]   (Set EDNS version) [0]
+[否]edns[=\35；\35；\35；]（设置edns版本）[0]
+ednsflags=###   (Set EDNS flag bits)
+ednflags='35；'35；'35；（设置EDNS标志位）
+[no]ednsnegotiation (Set EDNS version negotiation)
+[否]EDNS negotiation（设置EDNS版本协商）
+ednsopt=###[:value] (Send specified EDNS option)

+ednsopt=\35；\35；\35；[：值]（发送指定的EDNS选项）
+noednsopt (Clear list of +ednsopt options)
+Noednsopt（清除+ednsopt选项列表）
+[no]expire (Request time to expire)
+[否]过期（请求过期时间）
+[no]fail (Don't try next server on SERVFAIL)
+[否]失败（不要在SERVFAIL上尝试下一个服务器）
+[no]header-only (Send query without a question section)
+[否]仅标题（不带问题部分发送查询）
+[no]identify (ID responders in short answers)
+[否]识别（简短回答中的ID响应者）
+[no]idnin (Parse IDN names)
+[否]idnin（解析IDN名称）
+[no]idnout (Convert IDN response)
+[否]idnout（转换IDN响应）
+[no]ignore (Don't revert to TCP for TC responses.)
+[否]忽略（不要还原为TC响应的TCP。）
+[no]keepopen (Keep the TCP socket open between queries)
+[否]Keep open（在查询之间保持TCP套接字打开）
+[no]mapped (Allow mapped IPv4 over IPv6)
+[否]已映射（允许通过IPv6映射IPv4）
+[no]multiline (Print records in an expanded format)
+[否]多行（以扩展格式打印记录）
+ndots=### (Set search NDOTS value)
+ndots=\35；\35；\35；（设置搜索ndots值）
+[no]nsid (Request Name Server ID)
+[否]nsid（请求名称服务器ID）
+[no]nssearch (Search all authoritative nameservers)
+[否]nssearch（搜索所有权威名称服务器）
+[no]onesoa (AXFR prints only one soa record)
+[没有]一个soa（AXFR只打印一个sou记录）
+[no]opcode=### (Set the opcode of the request)
+[否]操作码='35；'35；'35；（设置请求的操作码）
+[no]qr (Print question before sending)
+[否]二维码（发送前打印问题）
+[no]question (Control display of question section)
+[否]问题（控制问题部分的显示）

+[no]rdflag (Recursive mode (+[no]recurse))
+[no]rdflag（递归模式（+[no]recurse））

+[no]recurse (Recursive mode (+[no]rdflag))
+[否]递归（递归模式（+[否]rdflag））

+retry=### (Set number of UDP retries) [2]
[设置UDP重试次数][2]
+[no]rrcomments (Control display of per-record comments)
+[否]rrcomments（控制每条记录注释的显示）
+[no]search (Set whether to use searchlist)
+[否]搜索（设置是否使用搜索列表）
+[no]short (Display nothing except short
+[否]短（除短外不显示任何内容）
form of answer)

回答形式）
+[no]showsearch　(Search with intermediate results)
+[否]showsearch（使用中间结果搜索）
+[no]sigchase　(Chase DNSSEC signatures)
+[否]sigchase（Chase DNSSEC签名）
三，命令演示
1.1指定DNS服务器列举
1.1.1 any
dig sogo.com any @8.8.8.8
使用8.8.8.8DNS主机服务器检索sogo,com所有DNS信息

```
C:\root> dig sogo.com any @8.8.8.8

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> sogo.com any @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48028
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
```

1.1.2 mx
dig sogo.com mx @8.8.8.8
使用8.8.8.8DNS主机服务器检索sogo,com的DNS MX信息

```
C:\root> dig sogo.com mx @8.8.8.8

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> sogo.com mx @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7515
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
```

1.1.3 ns
dig sogo.com ns @8.8.8.8
使用8.8.8.8DNS主机服务器检索sogo,com的DNS NS信息

```
C:\root> dig sogo.com ns @8.8.8.8
```

1.1.4 cname
dig sogo.com cnmae @8.8.8.8
使用8.8.8.8DNS主机服务器检索sogo,com的DNS CBANE信息

```
C:\root> dig sogo.com cname +short
e.proxy.sogou.com.
```

1.1.5 +noall
dig +noall sogo.com any @8.8.8.8
使用8.8.8.8DNS主机服务器不输出任何结果检索sogo.com所有DNS结果

```
\root> dig +noall sogo.com any @8.8.8.8
```

1.1.6 +noall +answer

dig +noall +amswer sogo.com any @8.8.8.8

使用8.8.8.8DNS主机服务器不输出任何结果但只检索sogo.com所有DNS结果

```
C:\root> dig +noall +answer sogo.com any @8.8.8.8
sogo.com.               299     IN      A       118.191.216.57
sogo.com.               299     IN      A       119.28.109.132
sogo.com.               299     IN      A       118.191.216.42
```

1.1.7 awk '{print $1}'

dig +noall +answer sogo.com any @8.8.8.8 | awk '{print $1}'

使用8.8.8.8DNS主机服务器不输出任何结果但只检索sogo.com 所打印结果的第一列。

```
C:\root> dig +noall +answer sogo.com any @8.8.8.8 | awk '{print $1}'
sogo.com.
sogo.com.
sogo.com.
```

1.1.7 -x

dig -x 118.191.216.61

反向解析118.191.216.61DNS主机信息

```
C:\root> dig -x 118.191.216.61

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> -x 118.191.216.61
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 12544
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
; COOKIE: 38bf3a4884db505301b49ea05e3bd54811a3e2b9e861a9b3 (good)
;; QUESTION SECTION:
;61.216.191.118.in-addr.arpa.   IN      PTR
```

1.2不指定DNS服务器列举（使用本机DNS）

1.2.1 any

dig sogo.com any

检索sogo,com所有DNS主机信息

1.2.2 mx

dig sogo.com mx

检索sogo,com的DNS主机 MX信息

1.2.3 awk '{print $1}'

dig +noall +answer sogo.com any | awk '{print $1}'

DNS主机服务器不输出任何结果但只检索sogo.com 所打印结果的第一列。

1.2.4 +noall

dig +noall sogo.com any

DNS服务器不输出任何结果检索sogo.com所有DNS主机结果

1.2.5 +noall +answer

dig +noall +amswer sogo.com any

DNS服务器不输出任何结果但只检索sogo.com所有DNS主机结果

1.2.6 ns

dig sogo.com ns

DNS服务器检索sogo,com的DNS主机 NS信息

1.2.7 cname

dig sogo.com cnmae

DNS服务器检索sogo,com的DNS主机 cnmae信息

1.3 BIND

dig txt cgaos VERSION.BIND @ns2.sogo.com

检索ns2.sogo.com DNS主机服务器的BIND信息

```
C:\root> dig txt cgaos VERSION.BIND @ns2.sogou.com

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> txt cgaos VERSION.BIND @ns2.sogou.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 284
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
; COOKIE: 47bbe2768444455e016ffe6f5e3bd7e310c7b430f9efeb58 (good)
;; QUESTION SECTION:
;cgaos.                         IN      TXT
```

30% 音量

dig +noall +answer txt cgais VERSION.BIND @ns2.sogo.com

不输出任何结果但只检索ns2.sogo.com主机DNS服务器的BIND信息

```
dig +noall +answer txt cgais VERSION.BIND @ns1.sogou.com
```

1.4 +TRACE

dig +trace sogo.com

追踪sogo.com 主机DNS信息

```
C:\root> dig +trace sogo.com

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> +trace sogo.com
;; global options: +cmd
.                       5       IN      NS      c.root-servers.net.
.                       5       IN      NS      l.root-servers.net.
.                       5       IN      NS      g.root-servers.net.
.                       5       IN      NS      j.root-servers.net.
```

No.	Time	Source	Destination	Protocol	Length	Info
120	5.768532469	192.168.79.132	192.168.79.2	DNS	73	Standard query 0x50da A
121	5.768657768	192.168.79.132	192.168.79.2	DNS	73	Standard query 0x9ce3 A
122	5.779692451	192.168.79.2	192.168.79.132	DNS	153	Standard query response
123	5.780307449	192.168.79.2	192.168.79.132	DNS	143	Standard query response
124	5.781004759	192.168.79.132	123.126.51.12	DNS	107	Standard query 0x2b4e A
125	5.849597673	123.126.51.12	192.168.79.132	DNS	250	Standard query response
126	11.093825517	192.168.79.1	192.168.79.254	DHCP	358	DHCP Request - Transac
127	11.093941242	192.168.79.254	192.168.79.1	DHCP	342	DHCP ACK - Transac

1.5 +SHOURT

dig sogo.com +shourt cname

DNS服务器不输出任何结果检索sogo.com的 DNS主机 cname结果

```
C:\root> dig sogo.com +short cname
e.proxy.sogou.com.
```

dig sogo.com +shourt mx

DNS服务器不输出任何结果检索sogo.com的 DNS主机 mx结果

```
C:\root> dig sogo.com +short mx
5 mx.sogou.com.
```

dig sogo.com +shourt any
DNS服务器不输出任何结果检索sogo.com的 DNS主机 any结果

```
^CC:\root> dig sogo.com +short any @8.8.8.8
119.28.109.132
118.191.216.42
118.191.216.57
```

dig sogo.com +shourt ns
DNS服务器不输出任何结果检索sogo.com的 DNS主机 ns结果

```
C:\root> dig sogo.com +short ns
ns1.sogou.com.
ns2.sogou.com.
```

dig sogo.com +shourt a
DNS服务器不输出任何结果检索sogo.com的DNS主机 a结果

```
C:\root> dig sogo.com +short a
36.110.164.37
36.110.165.43
106.39.246.42
49.7.20.53
36.110.170.48
```

四，DNS区域传输
dig @ns2.sogo.com sogo.com axfr
在域名服务器里面传输搜狗所有记录

```
C:\root> dig @ns1.sogo.com sogo.com axfr

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @ns1.sogo.com sogo.com axfr
; (1 server found)
;; global options: +cmd
sogo.com.               600     IN      SOA     ns1.sogou.com. dnsadmin.sogou
-inc.com. 1581126241 300 180 1209600 180
; Transfer failed.
C:\root> dig @ns1.sogo.com sogo.com axfr

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> @ns1.sogo.com sogo.com axfr
; (1 server found)
;; global options: +cmd
sogo.com.               600     IN      SOA     ns1.sogou.com. dnsadmin.sogou
```


附加内容：host
host -T -l sogo.com 8.8.8.8
在域名服务器里面传输搜狗所有记录