

正常情况下，通过cmd命令可以快速找到域名对应IP，最常见的命令如ping、nslookup。但很多站点出于用户体验和安全的角度，使用CDN加速，将域名解析到CDN，这时候就需要绕过CDN来查找真实IP。

## 一、DNS历史解析记录

查询域名的历史解析记录，可能会找到网站使用CDN前的解析记录，从而获取真实ip，相关查询的网站有：

```
iphistory : https://viewdns.info/iphistory/
DNS查询 : ( https://dnsdb.io/zh-cn/ )
微步在线 : ( https://x.threatbook.cn/ )
域名查询 : ( https://site.ip138.com/ )
DNS历史查询 : ( https://securitytrails.com/ )
Netcraft : https://sitereport.netcraft.com/?url=github.com
```

IP History 查询记录：

**Tools** API Research Data

ViewDNS.info > Tools > IP History

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

Domain (e.g. domain.com):

IP history results for alipay.com.  
=====

IP Address	Location	IP Address Owner	Last seen on this IP
110.75.139.5	China	Zhejiang Ant Small And Micro Financial Services	2020-05-22
110.75.129.5	China	Zhejiang Ant Small And Micro Financial Services	2020-05-22
110.76.20.33	China	Zhejiang Ant Small And Micro Financial Services	2017-09-10
110.76.19.33	China	Zhejiang Ant Small And Micro Financial Services	2017-09-10
110.75.139.5	China	Zhejiang Ant Small And Micro Financial Services	2017-09-10
110.75.129.5	China	Zhejiang Ant Small And Micro Financial Services	2017-09-10
110.76.20.33	China	Zhejiang Ant Small And Micro Financial Services	2017-09-08
110.76.19.33	China	Zhejiang Ant Small And Micro Financial Services	2017-09-08
110.76.20.33	China	Zhejiang Ant Small And Micro Financial Services	2017-03-26
110.76.19.33	China	Zhejiang Ant Small And Micro Financial Services	2017-03-26

## 二、查找子域名

很多时候，一些重要的站点会做CDN，而一些子域名站点并没有加入CDN，而且跟主站在同一个C段内，这时候，就可以通过查找子域名来查找网站的真实IP。

常用的子域名查找方法和工具：

- 1、搜索引擎查询：如Google、baidu、Bing等传统搜索引擎，site:baidu.com inurl:baidu.com，搜target.com|公司名字。
- 2、一些在线查询工具，如：

```
http://tool.chinaz.com/subdomain/  
http://i.links.cn/subdomain/  
http://subdomain.chaxun.la/  
http://searchdns.netcraft.com/  
https://www.virustotal.com/
```

### 3、子域名暴力猜解

子域名暴力工具：

Layer子域名挖掘机

wydomain: <https://github.com/ring04h/wydomain>


subDomainsBrute: <https://github.com/lijiejie/>

Sublist3r: <https://github.com/aboul31a/Sublist3r>

## 三、网站邮件头信息

比如说，邮箱注册，邮箱找回密码、RSS邮件订阅等功能场景，通过网站给自己发送邮件，从而让目标主动暴露他们的真实的IP，查看邮件头信息，获取到网站的真实IP。

```
Received: from mail.abc.com (unknown [218.117.211.62])  
        by newmx32.qq.com (NewMx) with SMTP id  
        for <670...528@qq.com>; Tue, 28 Apr 2020 16:54:57 +0800  
X-QQ-SPAM: true  
X-QQ-FEAT: KBpiTUYH2KyEXwQSbQ2gX7M3q6/lN9sJYvipB7xICpOL7MBAegsDH+pOWaQMj  
        eRTWbF5WxQ7su0VCZ+mVJ35+yGD8NeGMw4+hrJB7m2eH9eBMjtdbAFh8yu4SdcKxoPW6w7E  
        9nMs3GA1buAZz4hTCag/7GFGovZcprl07/6LZS9mkNa7nKNvfIQMuBBmb4x7q+jg3D+yHAU  
        oUI9cNXbol7MIId+z3vhfnypnEnFW9gH3QflIDe2HUKgM9vKvSH5I9Y/EPTimVkJy6SttRHP  
        SymbdQRIT4988PsU5MQFHvYhAY=  
X-QQ-MAILINFO: M9mpTqh4QKvq7HMaLmVGaPw/iL6hcy76VxqFmjsoZgowAjpOUlYnKBsaM  
        hSK9asn/cjiRBoj6NIHaw86jDvpyXxLxcjXMP0rFGc6liqJrG1/wU1tctQf13pEFSp9D1W  
        i4RmJPvIzrgFPC+yjPSxXuY=  
X-QQ-mid: mxsza31t1588064096tw2kxgryn  
X-QQ-ORGSender: admin@test.com
```



## 四、网络空间安全引擎搜索

通过关键字或网站域名，就可以找出被收录的IP，很多时候获取到的就是网站的真实IP。

- 1、钟馗之眼：<https://www.zoomeye.org>
- 2、Shodan：<https://www.shodan.io>
- 3、Fofa：<https://fofa.so>

ZoomEy搜索：

https://asm.ca.com/zh\_cn/ping.php  
http://host-tracker.com/  
http://www.webpagetest.org/  
https://dnscheck.pingdom.com/

国外多ping网站测试：

Ping a server or web site using our network of over 50 monitoring stations worldwide

(e.g. www.yahoo.com)

Start

Ping to: github.com					
Checkpoint	Result	min. rtt	avg. rtt	max. rtt	IP
Bulgaria - Sofia (bgsof02)	OK	30.472	30.575	30.747	140.82.118.3
India - Bangalore (inblr01)	Packets lost (100%)				13.234.210.38
Australia - Brisbane (aubne03)	Packets lost (100%)				52.64.108.95
United States - Council Bluffs (uscb101)	OK	24.999	25.119	25.625	140.82.114.4
India - Chennai (inche01)	Packets lost (100%)				13.234.176.102
United Kingdom - Cardiff (gbcar01)	OK	12.976	13.126	13.488	140.82.118.4
United States - Cheyenne (usche01)	OK	26.264	26.378	26.552	192.30.255.112
United States - Charleston (uschs02)	OK	12.594	12.793	13.331	140.82.114.4
United States - Charleston (uschs01)	OK	12.339	12.442	12.881	140.82.113.3
Canada - Toronto (cator03)	OK	24.766	24.930	25.227	140.82.113.3
Czech Republic - Prague (czprg01)	OK	23.954	24.031	24.067	140.82.118.4
Germany - Berlin (deber01)	OK	23.882	23.987	24.061	140.82.118.4
Germany - Frankfurt (defra05)	OK	6.508	6.607	7.153	140.82.118.3
Ireland - Dublin (iedub03)	OK	22.601	22.667	22.816	140.82.118.4
Netherlands - Eemshaven (nleem01)	OK	3.818	4.121	4.927	140.82.118.4

## 七、扫描全网

通过Zmap、masscan等工具对整个互联网发起扫描，针对扫描结果进行关键字查找，获取网站真实IP。

1、ZMap号称是最快的互联网扫描工具，能够在45分钟扫遍全网。

<https://github.com/zmap/zmap>

2、Masscan号称是最快的互联网端口扫描器，最快可以在六分钟内扫遍互联网。

<https://github.com/robertdavidgraham/masscan>

## 八、配置不当导致绕过

在配置CDN的时候，需要指定域名、端口等信息，有时候小小的配置细节就容易导致CDN防护被绕过。

案例1：为了方便用户访问，我们常常将 `www.test.com` 和 `test.com` 解析到同一个站点，而CDN只配置了 [www.test.com](http://www.test.com)，通过访问 `test.com`，就可以绕过CDN了。

案例2：站点同时支持http和https访问，CDN只配置https协议，那么这时访问http就可以轻易绕过。

---

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。

