

在一些场景中，我们往往只得到了一个IP地址，那么如何通过IP地址快速找到它绑定的域名呢？

## 1、IP历史解析记录

输入查询的IP地址，获取IP绑定过的域名记录。

ip138查询：<https://site.ip138.com/>

### IP或域名查询

58.23.201.163

X

查询

中国 福建 泉州 联通

58.23.201.163上的网站

绑定过的域名如下：

www.ckjy.com	2019-03-22-----2019-08-31
qjy.com	2019-08-19-----2019-08-19
ww.ckjy.com	2019-08-19-----2019-08-19

在58.23.201.0/24查找网站

## 2、同站/旁站查询

关键词：IP反查域名、同IP网站查询、旁站查询，通过一些在线查询工具获取域名。

IP反查域名：

<https://dns.aizhan.com/>  
反向IP查找：<https://www.yougetsignal.com/tools/web-sites-on-web-server/>  
<https://tools.ipip.net/ipdomain.php?ip=x.x.x.x>

同IP网站查询：

<http://s.tool.chinaz.com/same>  
<https://www.webscan.cc/search/>

查旁站：

https://chapangzhan.com/  
https://phpinfo.me/bing.php

### 3、通过证书反查域名

部分Web服务端口使用了SSL证书，比如访问443端口显示404错误（因非域名访问，所以证书会显示不安全），查看证书可获取域名相关信息。



### 4、网站信息收集

通过服务器开放的IP端口进行信息收集，找到可疑通过ip地址访问的web应用，根据网站的title、keywords等关键词，通过搜索引擎找到站点域名。

### 5、网络空间安全引擎搜索

通过网络空间安全引擎搜索IP地址，快速获取IP地址相关信息，进一步找到网站域名。

zoomeye(钟馗之眼) : <https://www.zoomeye.org>  
shodan : <https://www.shodan.io>  
Fofa : <https://fofa.so>  
Censys : <https://censys.io/ipv4/>  
Dnsdb搜索引擎 : <https://www.dnsdb.io>

## 6、nmap扫描

sn参数是ping scan

```
$ nmap 91.199.104.0/24 -sn | grep "bitdefender.com" | awk '{print $5}'
border.bitdefender.com
applecsrwebservice.bitdefender.com
gw-paxato.bitdefender.com
pan-stage.bitdefender.com
$ █
```

---

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。

