

# Turbolist3r: 列舉子域名

列出一些幫助列舉子域名的工具。

## Turbolist3r

Turbolist3r on GitHub

基於 Sublist3r 由 Ahmed Aboul-Ela - @aboul3la 分叉由 Carl Pearson - GitHub

```
python turbolist3r.py -d google.com
```

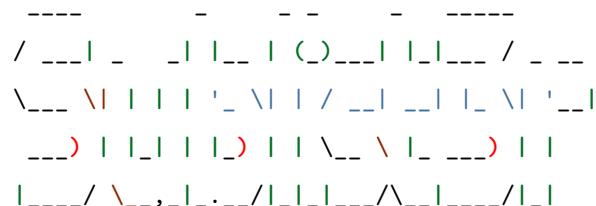
## Sublist3r

已嘗試。Sublist3r

```
% python sublist3r.py -d google.com
```

\*\*Proxy 設定已檢測到:\*\*

```
- HTTP_PROXY: http://127.0.0.1:7890  
- HTTPS_PROXY: http://127.0.0.1:7890
```



# 編寫者 Ahmed Aboul-Ela - @aboul3la

[+] 正在列舉 google.com 的子域名

[+] 正在 Baidu 中搜索..

[+] 正在 Yahoo 中搜索..

[+] 正在 Google 中搜索..

[+] 正在 Bing 中搜索..

[+] 正在 Ask 中搜索..

[+] 正在 Netcraft 中搜索..

[+] 正在 DNSdumpster 中搜索..

[+] 正在 Virustotal 中搜索..

[+] 正在 ThreatCrowd 中搜索..

[+] 正在 SSL 認證中搜索..

[+] 正在 PassiveDNS 中搜索..

```
Process DNSdumpster-8:  
Traceback (most recent call last):  
  File "/Users/lzwjava/anaconda3/lib/python3.10/multiprocessing/process.py", line 314, in _bootstrap  
    self.run()  
  File "/Users/lzwjava/projects/Sublist3r/sublist3r.py", line 268, in run  
    domain_list = self.enumerate()  
  File "/Users/lzwjava/projects/Sublist3r/sublist3r.py", line 647, in enumerate  
    token = self.get_csrf_token(resp)  
  File "/Users/lzwjava/projects/Sublist3r/sublist3r.py", line 641, in get_csrf_token  
    token = csrf_regex.findall(resp)[0]  
IndexError: list index out of range  
[!] 錯誤: Virustotal 可能現在正在封鎖我們的請求  
[-] 總計找到 97 個獨特子域名  
  
www.google.com  
accounts.google.com  
freezone.accounts.google.com  
adwords.google.com  
qa.adz.google.com  
answers.google.com  
apps-secure-data-connector.google.com  
audioads.google.com  
checkout.google.com  
mtv-da-1.ad.corp.google.com  
ads-compare.eem.corp.google.com  
da.ext.corp.google.com  
m.guts.corp.google.com  
m.gutsdev.corp.google.com  
login.corp.google.com  
mtv-da.corp.google.com  
mygeist.corp.google.com  
mygeist2010.corp.google.com  
proxyconfig.corp.google.com  
reseed.corp.google.com  
twdsalesgsa.twd.corp.google.com  
uberproxy.corp.google.com  
uberproxy-nocert.corp.google.com  
uberproxy-san.corp.google.com  
ext.google.com  
cag.ext.google.com  
cod.ext.google.com
```

da.ext.google.com  
eggroll.ext.google.com  
fra-da.ext.google.com  
glass.ext.google.com  
glass-eur.ext.google.com  
glass-mtv.ext.google.com  
glass-twd.ext.google.com  
hot-da.ext.google.com  
hyd-da.ext.google.com  
ice.ext.google.com  
meeting.ext.google.com  
mtv-da.ext.google.com  
soaproxyprod01.ext.google.com  
soaproxytest01.ext.google.com  
spdy-proxy.ext.google.com  
spdy-proxy-debug.ext.google.com  
twd-da.ext.google.com  
flexpack.google.com  
www.flexpack.google.com  
accounts.flexpack.google.com  
gaiastaging.flexpack.google.com  
mail.flexpack.google.com  
plus.flexpack.google.com  
search.flexpack.google.com  
freezone.google.com  
www.freezone.google.com  
accounts.freezone.google.com  
gaiastaging.freezone.google.com  
mail.freezone.google.com  
news.freezone.google.com  
plus.freezone.google.com  
search.freezone.google.com  
gmail.google.com  
hosted-id.google.com  
jmt0.google.com  
aspmx.l.google.com  
alt1.aspmx.l.google.com  
alt2.aspmx.l.google.com  
alt3.aspmx.l.google.com  
alt4.aspmx.l.google.com

gmail-smtp-in.l.google.com  
alt1.gmail-smtp-in.l.google.com  
alt2.gmail-smtp-in.l.google.com  
alt3.gmail-smtp-in.l.google.com  
alt4.gmail-smtp-in.l.google.com  
gmr-smtp-in.l.google.com  
alt1.gmr-smtp-in.l.google.com  
alt2.gmr-smtp-in.l.google.com  
alt3.gmr-smtp-in.l.google.com  
alt4.gmr-smtp-in.l.google.com  
vp.video.l.google.com  
m.google.com  
freezone.m.google.com  
mail.google.com  
freezone.mail.google.com  
misc.google.com  
misc-sni.google.com  
mtalk.google.com  
mx.google.com  
ics.prod.google.com  
sandbox.google.com  
cert-test.sandbox.google.com  
ecc-test.sandbox.google.com  
services.google.com  
talk.google.com  
upload.google.com  
dg.video.google.com  
upload.video.google.com  
wifi.google.com  
onex.wifi.google.com