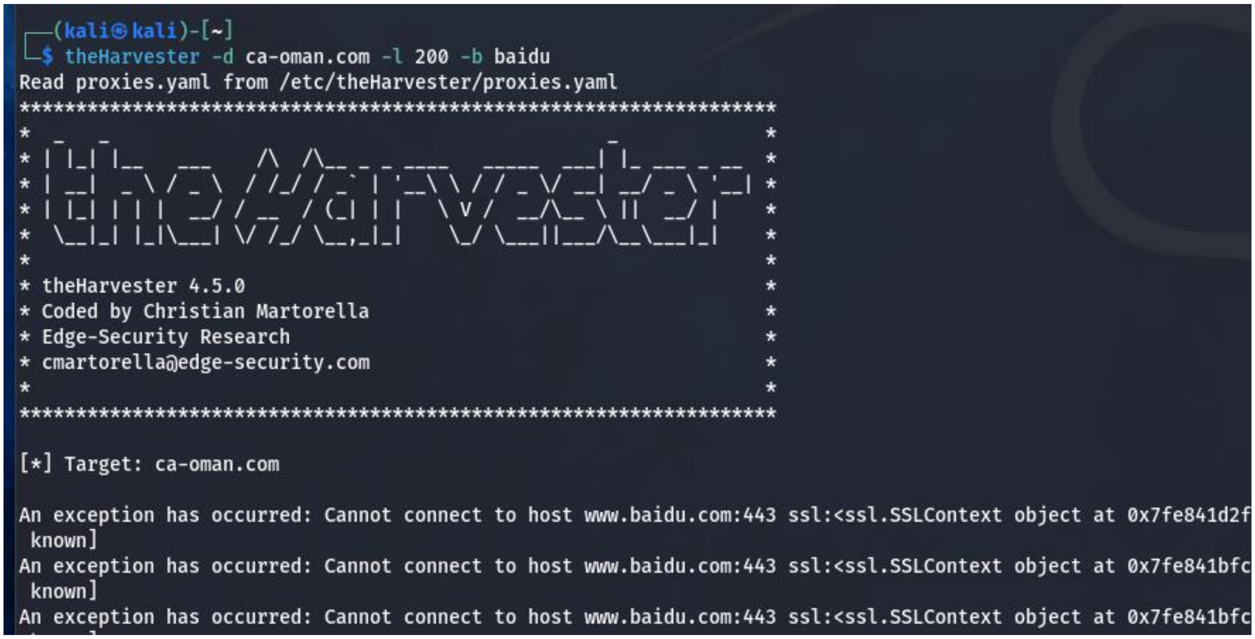
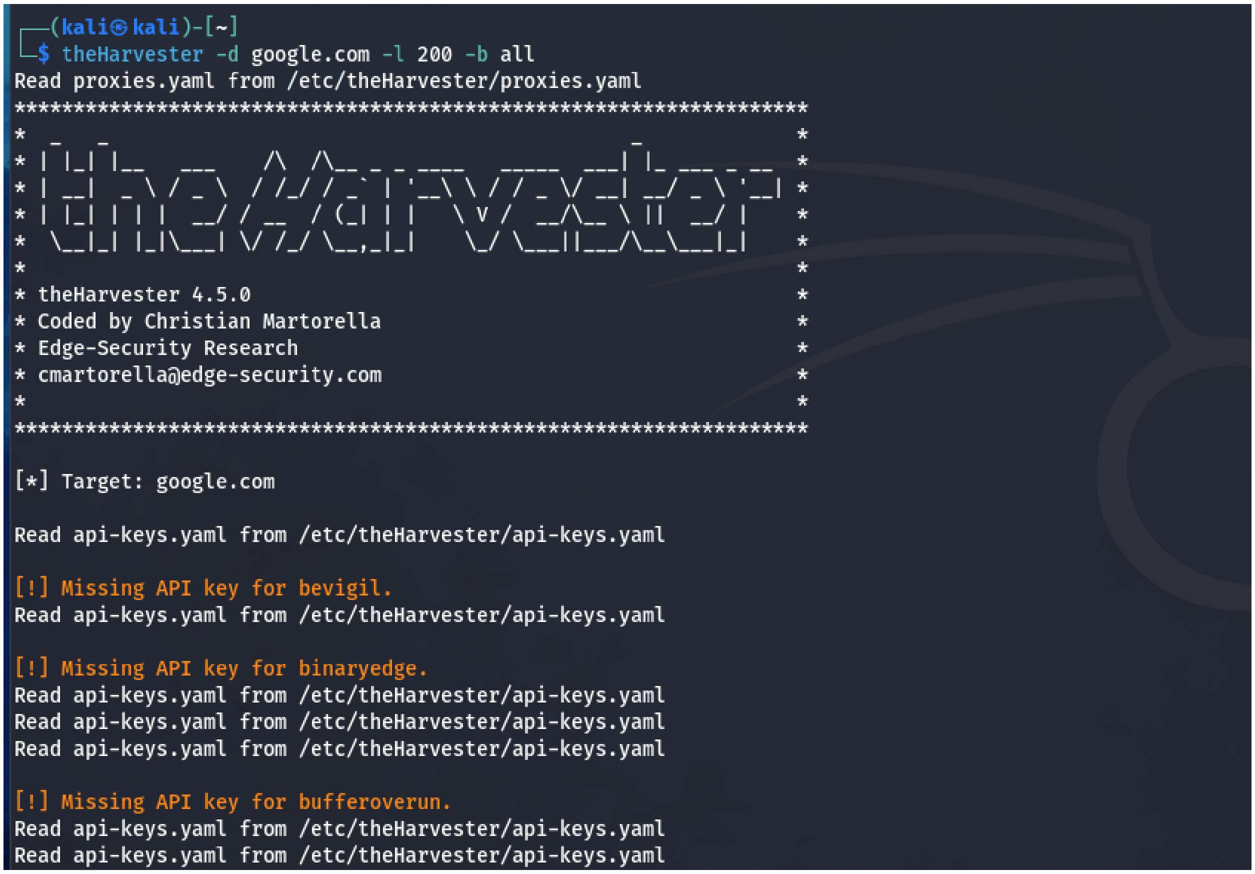
TheHarvester:

أداة تعمل على كالي لينكس لاستخراج الاميلات و النطاقات الفرعية للموقع



```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d ca-oman.com -l 200 -b baidu
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.5.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: ca-oman.com

An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0x7fe841d2f
 known]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0x7fe841bfc
 known]
An exception has occurred: Cannot connect to host www.baidu.com:443 ssl:<ssl.SSLContext object at 0x7fe841bfc
```

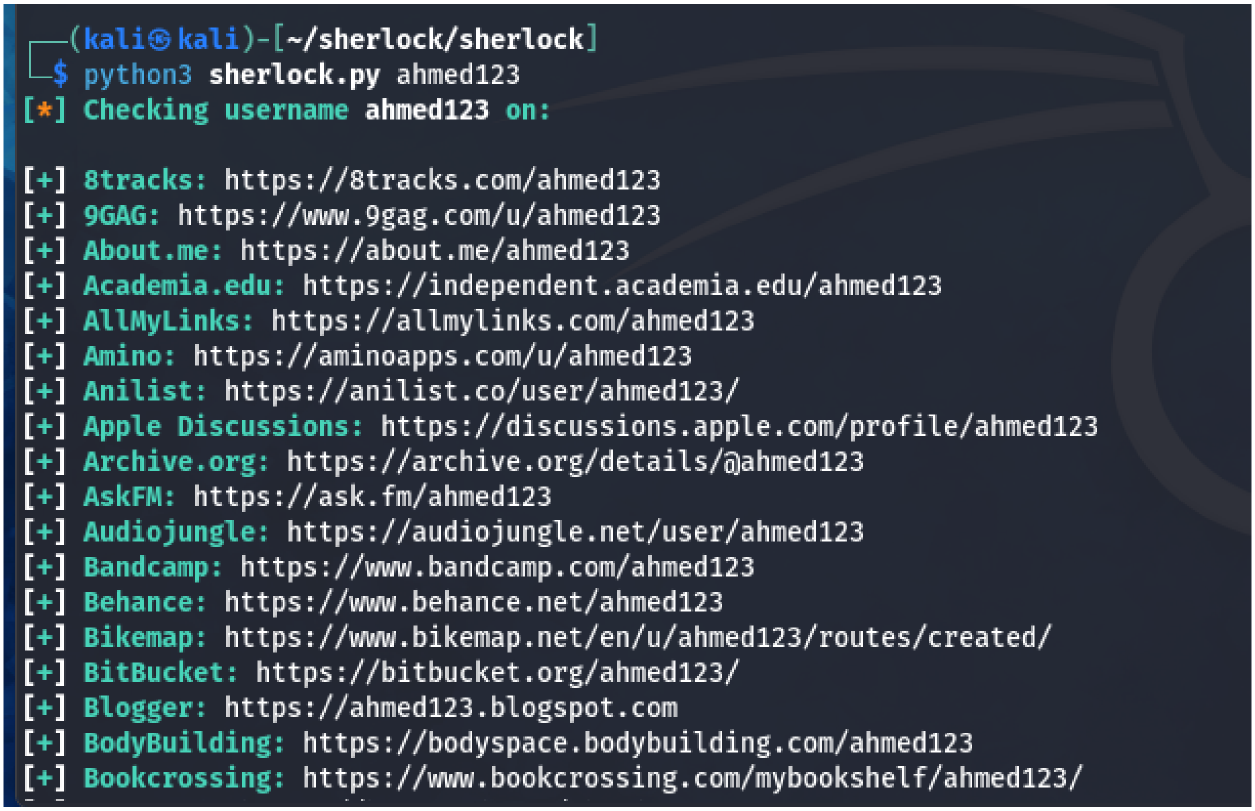


```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d google.com -l 200 -b all
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.5.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: google.com

Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for bevigil.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for binaryedge.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml

[!] Missing API key for bufferoverun.
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
```

Sherlock

أداة sherlock توفر عليك الكثير من الجهد و الوقت الذي تتطلبه عملية البحث حيث يمكنك تزويدها بإسم المستخدم (Username) الخاص بالشخص و هي ستقوم بالبحث عن الحسابات المرتبطة به في شبكات التواصل الإجتماعي أو بمواقع الويب التي يظهر للأداة وجودصلة محتملة بينهما.

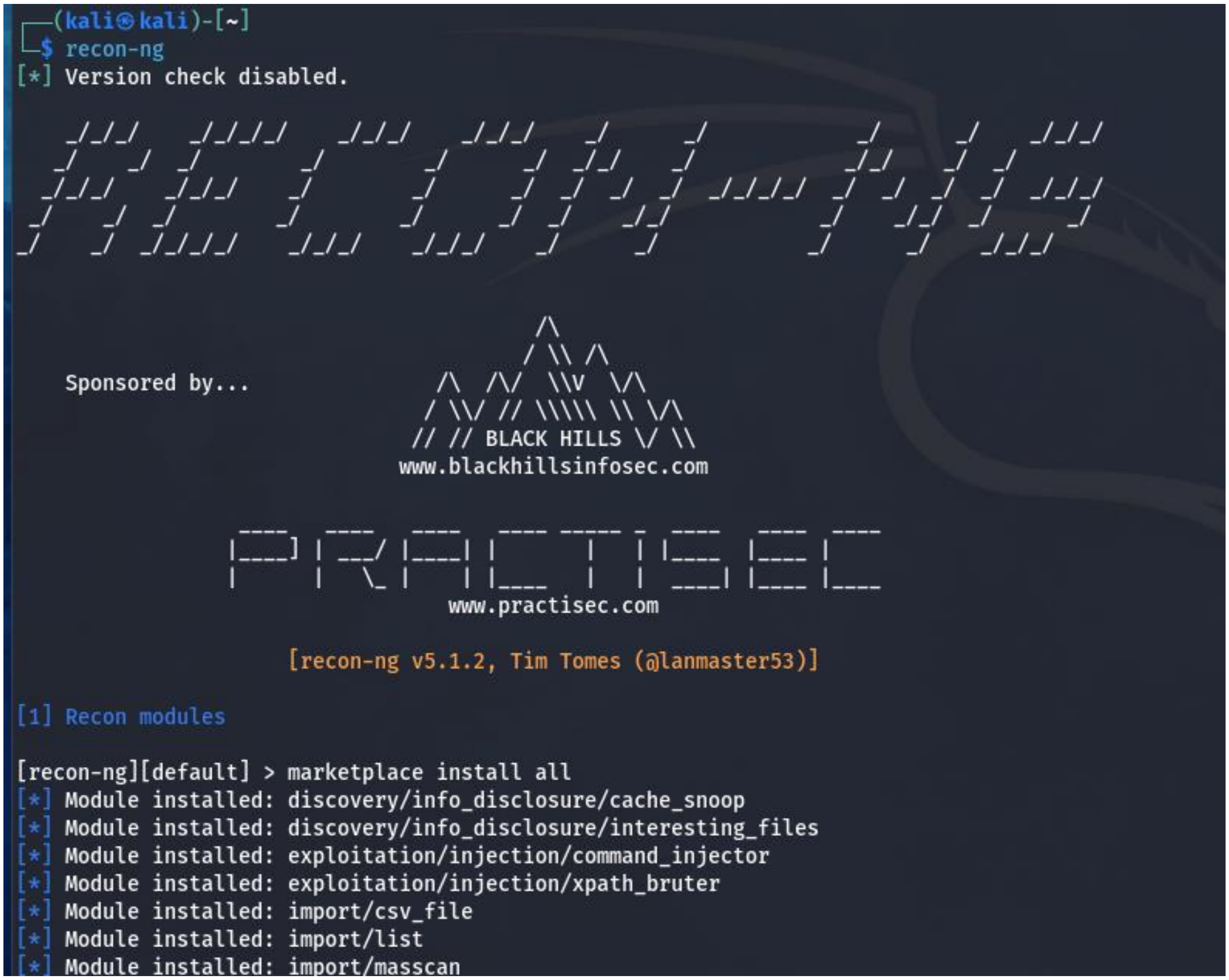
هذه الأداة متاحة على نظام لينكس و على الهاتف المحمول الذي يعمل بنظام آندرويد (Android) على برنامج تيرمكس (Termux).



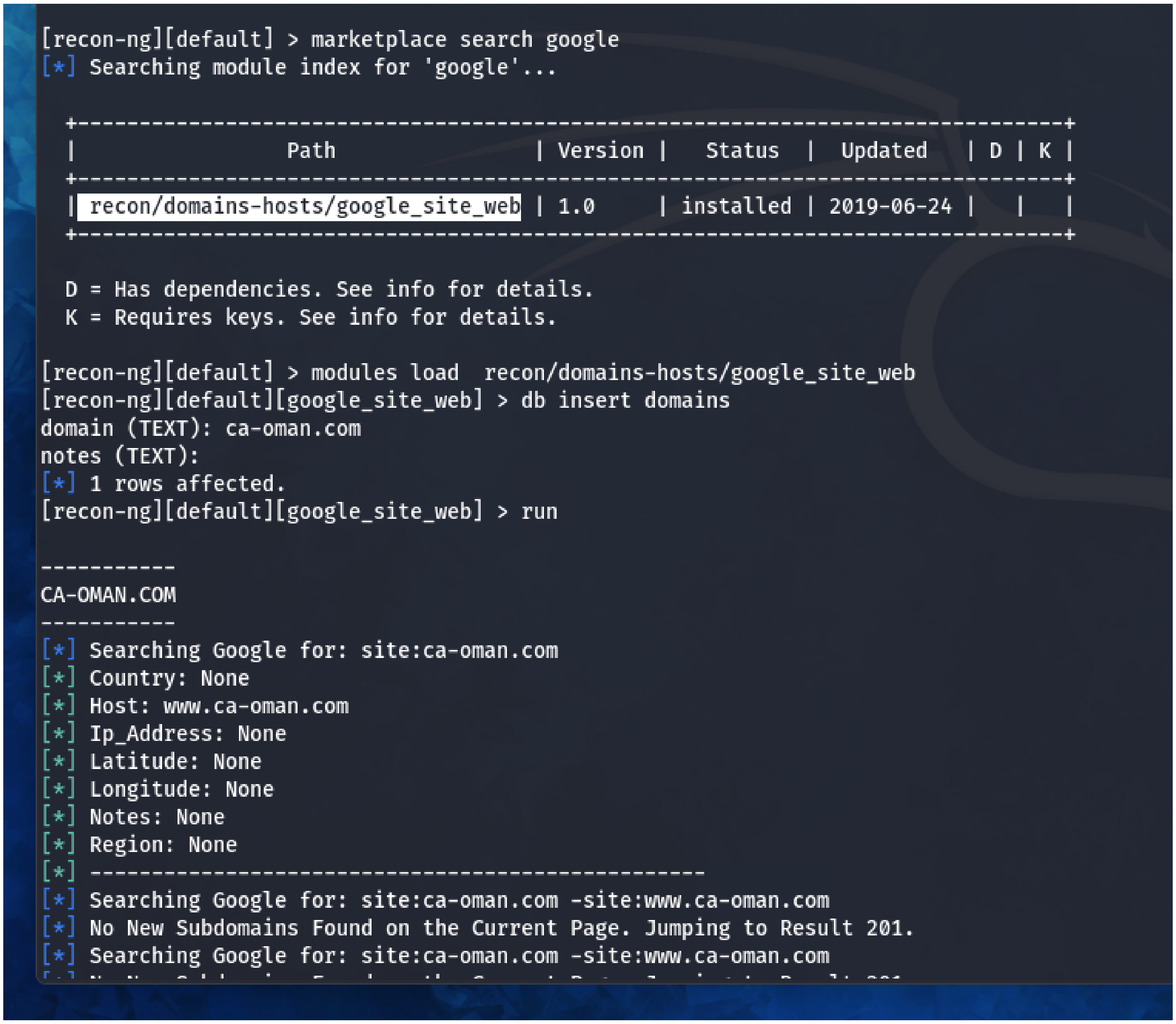
```
┌──(kali㉿kali)-[~/sherlock/sherlock]
└─$ python3 sherlock.py ahmed123
[*] Checking username ahmed123 on:

[+] 8tracks: https://8tracks.com/ahmed123
[+] 9GAG: https://www.9gag.com/u/ahmed123
[+] About.me: https://about.me/ahmed123
[+] Academia.edu: https://independent.academia.edu/ahmed123
[+] AllMyLinks: https://allmylinks.com/ahmed123
[+] Amino: https://aminoapps.com/u/ahmed123
[+] Anilist: https://anilist.co/user/ahmed123/
[+] Apple Discussions: https://discussions.apple.com/profile/ahmed123
[+] Archive.org: https://archive.org/details/@ahmed123
[+] AskFM: https://ask.fm/ahmed123
[+] Audiojungle: https://audiojungle.net/user/ahmed123
[+] Bandcamp: https://www.bandcamp.com/ahmed123
[+] Behance: https://www.behance.net/ahmed123
[+] Bikemap: https://www.bikemap.net/en/u/ahmed123/routes/created/
[+] BitBucket: https://bitbucket.org/ahmed123/
[+] Blogger: https://ahmed123.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/ahmed123
[+] Bookcrossing: https://www.bookcrossing.com/mybookshelf/ahmed123/
```

Recon-ng

هي بيئة عمل مفتوحة المصدر مطورة بلغة **python** هدفها جمع البيانات من الإنترنت عن الهدف المراد اختبار اختراقه وتحتوي هذه الأداة على العديد من **(modules)** وتستطيع تحميل واستخدام كل **(module)** واستخدامه بطريقة بسيطه.



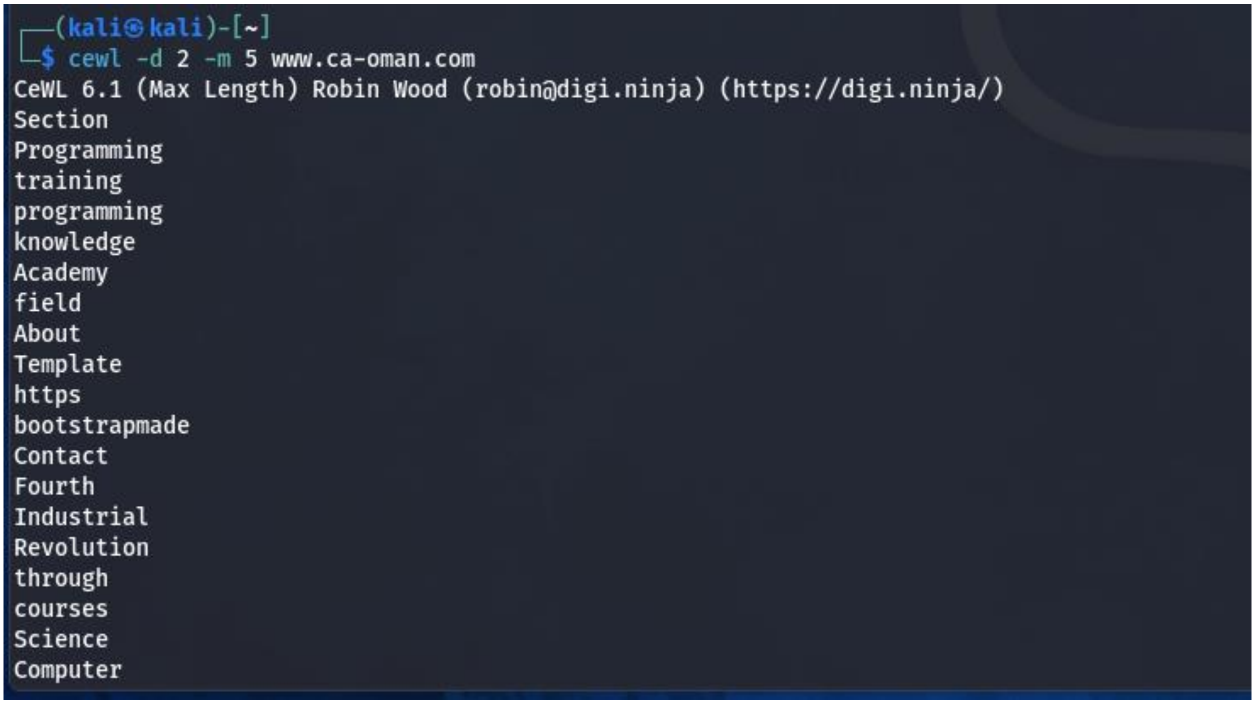
```
┌──(kali㉿kali)-[~]
└─$ recon-ng
[*] Version check disabled.

    _/_/_/    _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/
   _/    _/  _/        _/        _/      _/  _/_/    _/            _/_/    _/  _/
  _/_/_/    _/_/_/    _/        _/      _/  _/  _/  _/  _/_/_/_/  _/  _/  _/  _/  _/_/_/
 _/    _/  _/        _/        _/      _/  _/    _/_/            _/    _/_/  _/      _/
_/    _/  _/_/_/_/    _/_/_/    _/_/_/    _/      _/            _/      _/    _/_/_/


                                          /\
                                         / \\ /\
    Sponsored by...               /\  /\/  \\v  \/\
                                 / \\/ // \\\\\ \\ \/\
                                // // BLACK HILLS \/ \\
                               www.blackhillsinfosec.com

                  ____   ____   ____   ____ _____ _ ____   ____  ____
                 |____] |___/ |____| |       |   | |____  |____ |
                 |      |   \_ |    | |____   |   | ____| |____ |____
                                   www.practisec.com

                      [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[1] Recon modules

[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
```



```
[recon-ng][default] > marketplace search google
[*] Searching module index for 'google'...

  +--------------------------------------------------------------------------------+
  |                 Path                 | Version |   Status  |  Updated   | D | K |
  +--------------------------------------------------------------------------------+
  | recon/domains-hosts/google_site_web | 1.0     | installed | 2019-06-24 |   |   |
  +--------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][default] > modules load  recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > db insert domains
domain (TEXT): ca-oman.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][default][google_site_web] > run

-----------
CA-OMAN.COM
-----------
[*] Searching Google for: site:ca-oman.com
[*] Country: None
[*] Host: www.ca-oman.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Searching Google for: site:ca-oman.com -site:www.ca-oman.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 201.
[*] Searching Google for: site:ca-oman.com -site:www.ca-oman.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 201.
```

Cewl

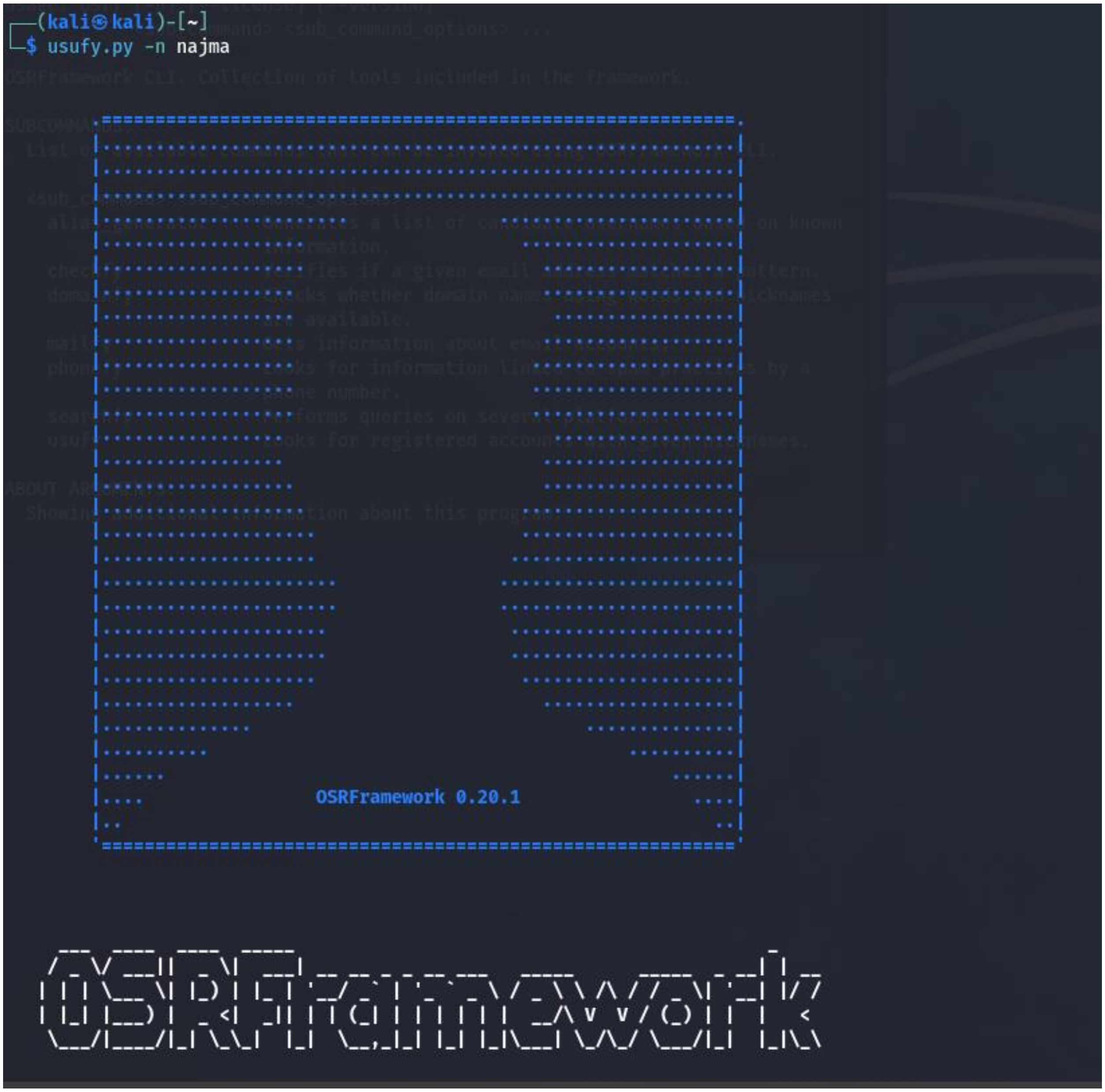
the Custom Word List generator.



```
┌──(kali㉿kali)-[~]
└─$ cewl -d 2 -m 5 www.ca-oman.com
CeWL 6.1 (Max Length) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Section
Programming
training
programming
knowledge
Academy
field
About
Template
https
bootstrapmade
Contact
Fourth
Industrial
Revolution
through
courses
Science
Computer
```

OSR-FRAMEWORK

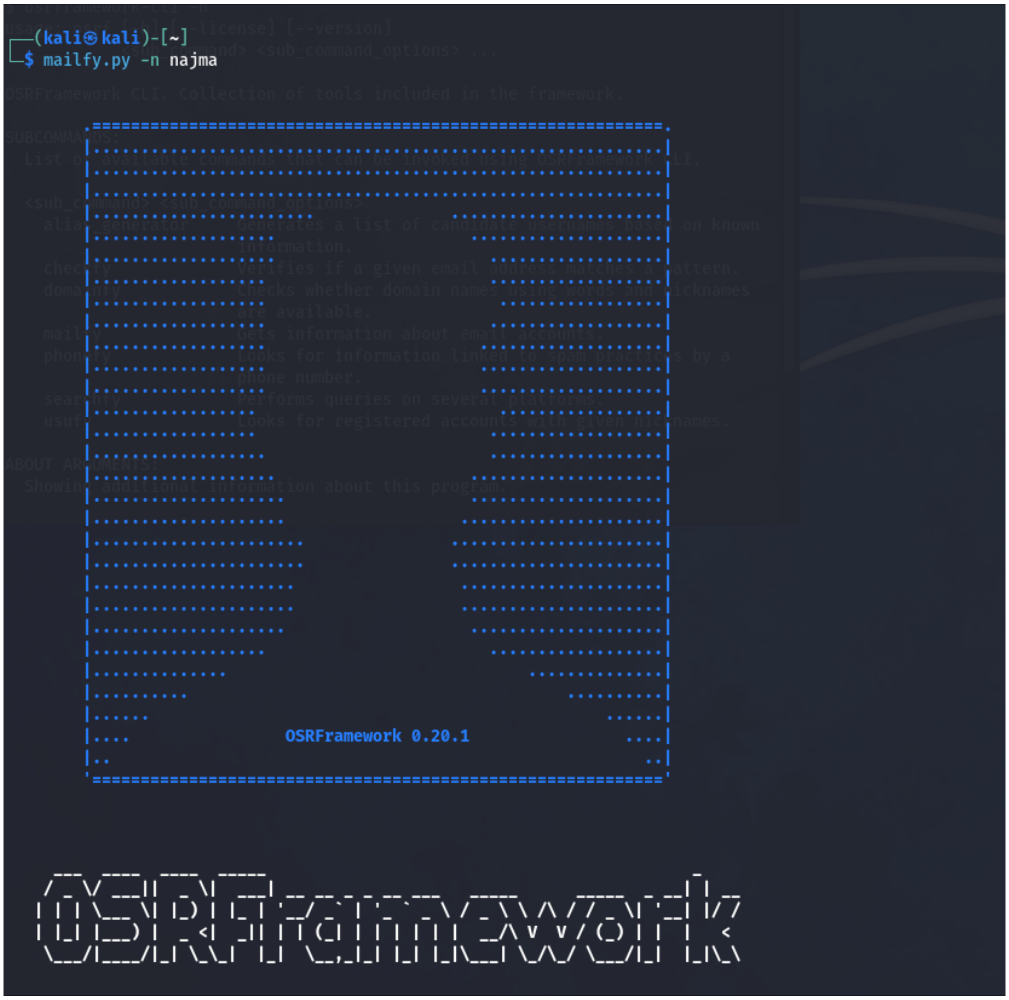
Search for user:



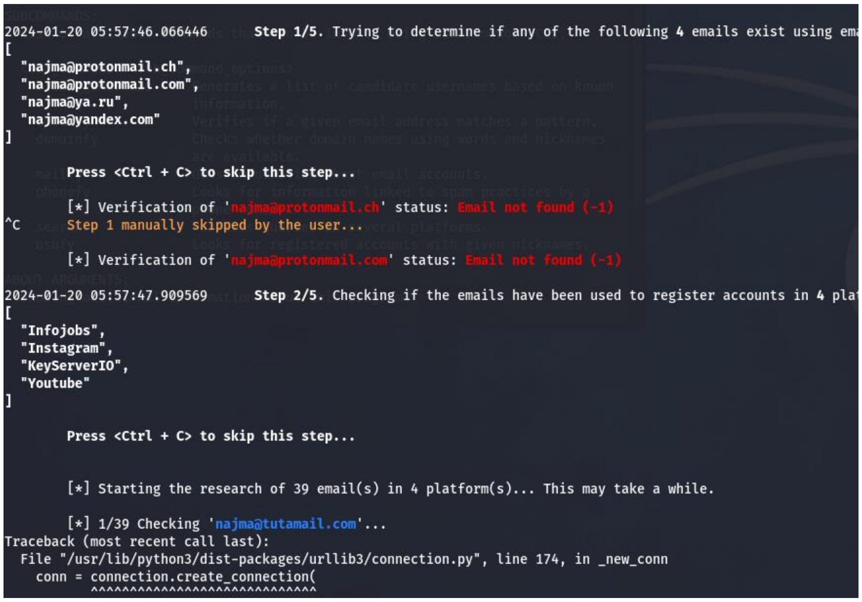
```
┌──(kali㉿kali)-[~]
└─$ usufy.py -n najma
```

```
OSRFramework 0.20.1
```

Search for email:



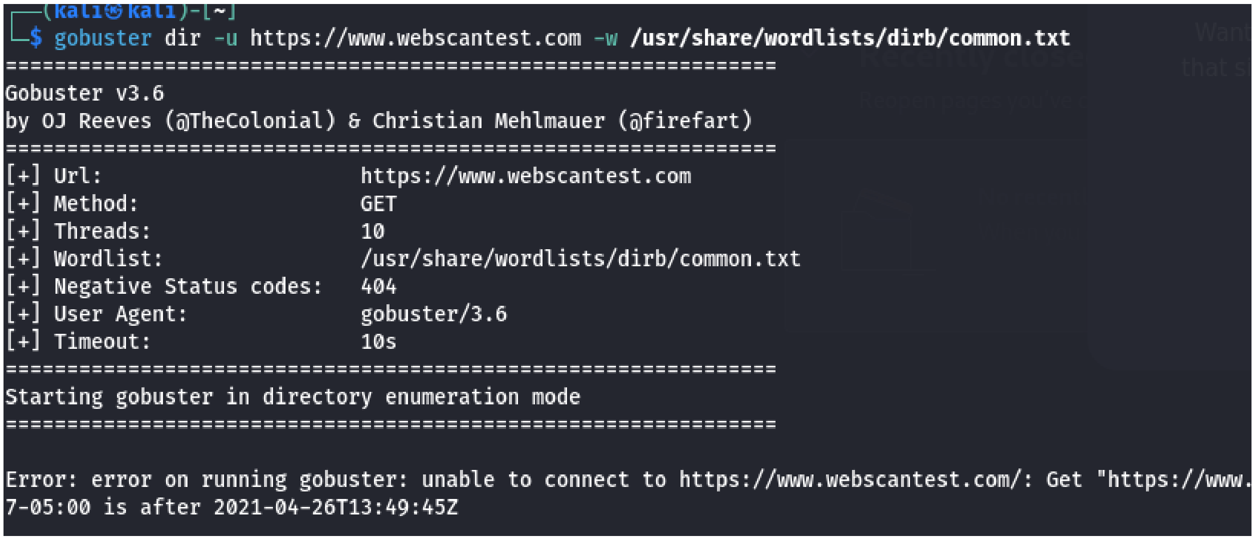
```
┌──(kali㉿kali)-[~]
└─$ mailfy.py -n najma

                              OSRFramework 0.20.1
```



```
2024-01-20 05:57:46.066446      Step 1/5. Trying to determine if any of the following 4 emails exist using ema
[
  "najma@protonmail.ch",
  "najma@protonmail.com",
  "najma@ya.ru",
  "najma@yandex.com"
]

        Press <Ctrl + C> to skip this step...

        [*] Verification of 'najma@protonmail.ch' status: Email not found (-1)
^C      Step 1 manually skipped by the user...

        [*] Verification of 'najma@protonmail.com' status: Email not found (-1)

2024-01-20 05:57:47.909569      Step 2/5. Checking if the emails have been used to register accounts in 4 pla
[
  "Infojobs",
  "Instagram",
  "KeyServerIO",
  "Youtube"
]

        Press <Ctrl + C> to skip this step...


        [*] Starting the research of 39 email(s) in 4 platform(s)... This may take a while.

        [*] 1/39 Checking 'najma@tutamail.com'...
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/urllib3/connection.py", line 174, in _new_conn
    conn = connection.create_connection(
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

Gobuster

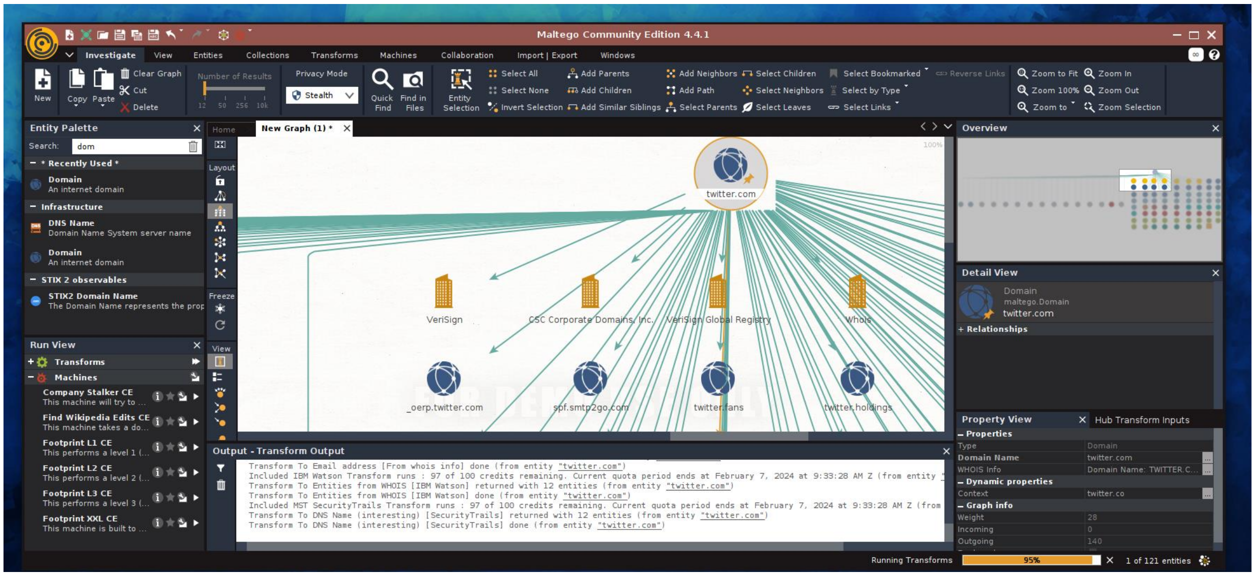
Gobuster is a tool used to brute-force URIs including directories and files as well as DNS subdomains.



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u https://www.webscantest.com -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://www.webscantest.com
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================

Error: error on running gobuster: unable to connect to https://www.webscantest.com/: Get "https://www.
7-05:00 is after 2021-04-26T13:49:45Z
```

Maltego

و هي أداة مفيدة جداً فيما يتعلق ببناء العلاقات بين الكيانات الموجودة على الإنترنت كالناس و أسمائهم و عناوين بريدهم الإلكتروني إلخ.. و كمجموعات الناس من الشركات و المنظمات المربوطة بمواقع إلكترونية.

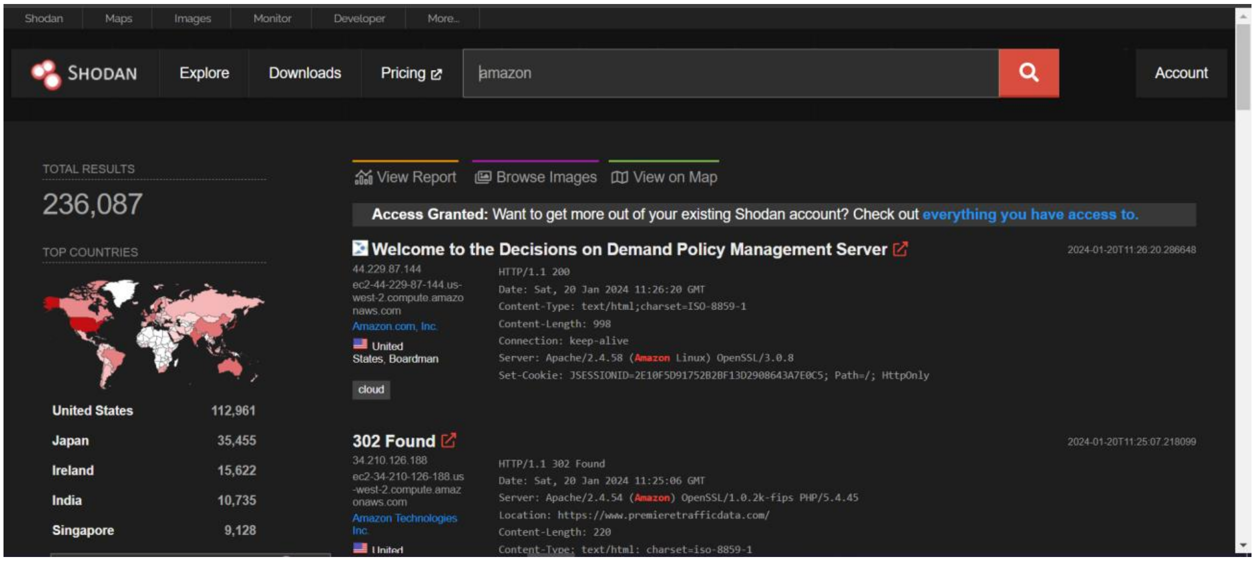


Output - Transform Output

```
Transform To Email address [From whois info] done (from entity "twitter.com")
Included IBM Watson Transform runs : 97 of 100 credits remaining. Current quota period ends at February 7, 2024 at 9:33:28 AM Z (from entity "
Transform To Entities from WHOIS [IBM Watson] returned with 12 entities (from entity "twitter.com")
Transform To Entities from WHOIS [IBM Watson] done (from entity "twitter.com")
Included MST SecurityTrails Transform runs : 97 of 100 credits remaining. Current quota period ends at February 7, 2024 at 9:33:28 AM Z (from
Transform To DNS Name (interesting) [SecurityTrails] returned with 12 entities (from entity "twitter.com")
Transform To DNS Name (interesting) [SecurityTrails] done (from entity "twitter.com")
```

Properties
Type: Domain
Domain Name: twitter.com
WHOIS Info: Domain Name: TWITTER.C...
Dynamic properties
Context: twitter.co
Graph info
Weight: 28
Incoming: 0
Outgoing: 140

Shodan



TOTAL RESULTS

236,087

TOP COUNTRIES

United States	112,961
Japan	35,455
Ireland	15,622
India	10,735
Singapore	9,128

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

Welcome to the Decisions on Demand Policy Management Server 2024-01-20T11:26:20.286648

44.229.87.144
ec2-44-229-87-144.us-west-2.compute.amazonaws.com
Amazon.com, Inc.
United States, Boardman
cloud

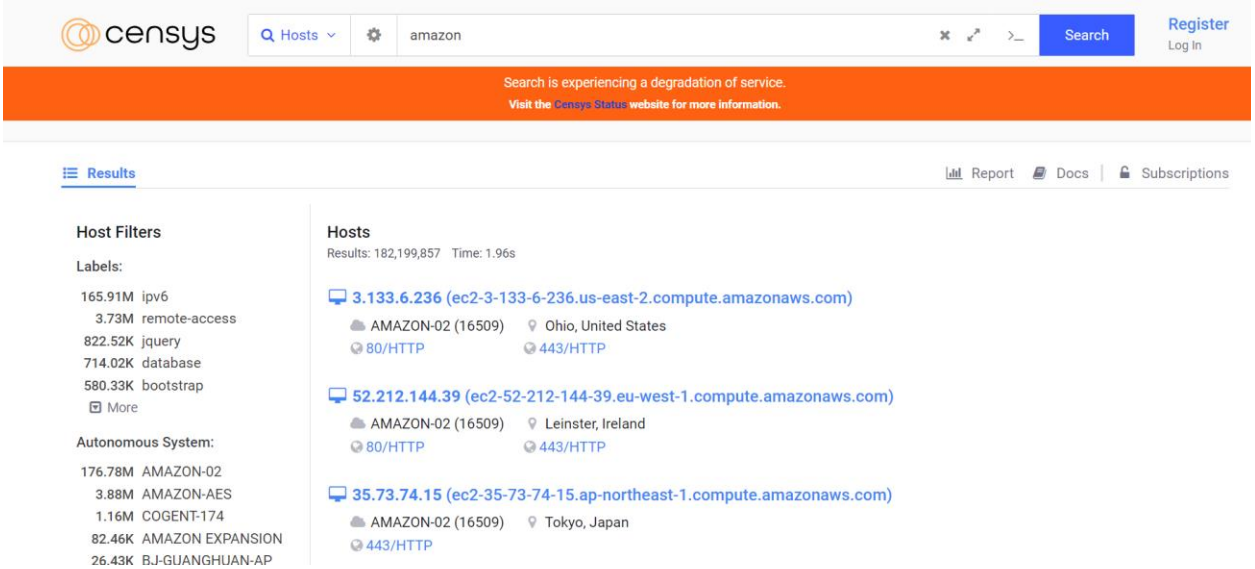
```
HTTP/1.1 200
Date: Sat, 20 Jan 2024 11:26:20 GMT
Content-Type: text/html;charset=ISO-8859-1
Content-Length: 998
Connection: keep-alive
Server: Apache/2.4.58 (Amazon Linux) OpenSSL/3.0.8
Set-Cookie: JSESSIONID=2E10F5D91752B2BF13D2908643A7E0C5; Path=/; HttpOnly
```

302 Found 2024-01-20T11:25:07.218099

34.210.126.188
ec2-34-210-126-188.us-west-2.compute.amazonaws.com
Amazon Technologies Inc.
United

```
HTTP/1.1 302 Found
Date: Sat, 20 Jan 2024 11:25:06 GMT
Server: Apache/2.4.54 (Amazon) OpenSSL/1.0.2k-fips PHP/5.4.45
Location: https://www.premieretrafficdata.com/
Content-Length: 220
Content-Type: text/html; charset=iso-8859-1
```

Censys



Search is experiencing a degradation of service.
Visit the Censys Status website for more information.

Host Filters

Labels:

165.91M	ipv6
3.73M	remote-access
822.52K	jquery
714.02K	database
580.33K	bootstrap

Autonomous System:

176.78M	AMAZON-02
3.88M	AMAZON-AES
1.16M	COGENT-174
82.46K	AMAZON EXPANSION
26.43K	BJ-GUANGHUAN-AP

Hosts

Results: 182,199,857 Time: 1.96s

3.133.6.236 (ec2-3-133-6-236.us-east-2.compute.amazonaws.com)
AMAZON-02 (16509) Ohio, United States
80/HTTP 443/HTTP

52.212.144.39 (ec2-52-212-144-39.eu-west-1.compute.amazonaws.com)
AMAZON-02 (16509) Leinster, Ireland
80/HTTP 443/HTTP

35.73.74.15 (ec2-35-73-74-15.ap-northeast-1.compute.amazonaws.com)
AMAZON-02 (16509) Tokyo, Japan
443/HTTP