Top 5 OSINT Tools

We will cover the following top 5 OSINT Tools in this tutorial:

1. Maltego
2. Shodan
3. Google Dorks
4. Recon-ng
5. Harvester

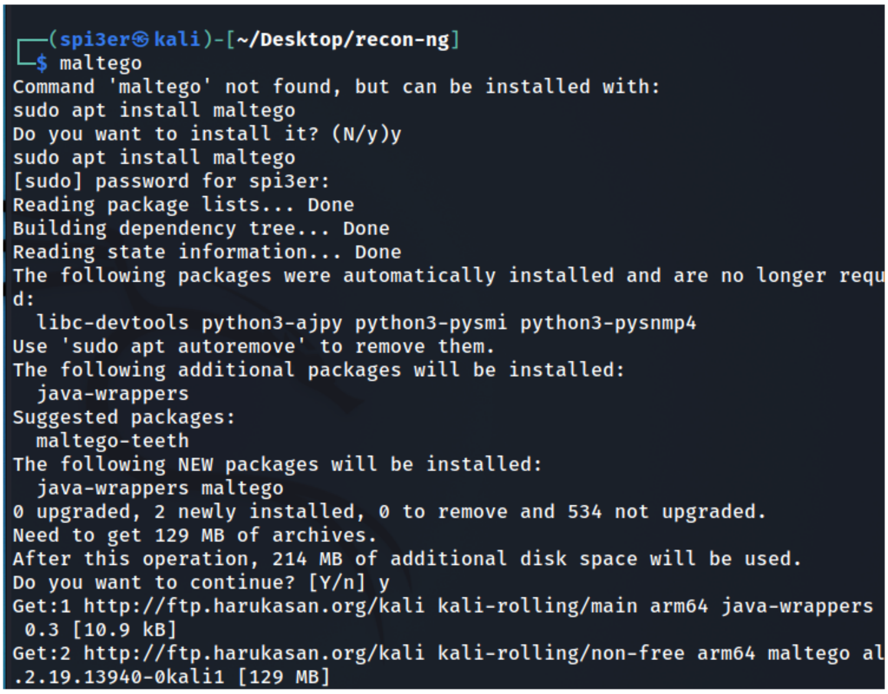
1. Maltego

Maltego can be said the best tool available in the market for OSINT because it grabs the information from various kinds of resources and also presents them in graphs and visuals for an easier review. The graphs contain information such as email , organisation , domains , Nameservers and a lot more. Maltego uses Java, so it is available on Windows , Mac and Linux and is available in many Hacking distro's like Kali Linux and Parrot OS.

Installation

For Ubuntu / Debian

```bash
wget https://maltego-downloads.s3.us-east-2.amazonaws.com/linux/Maltego.v4.2.19.13940.linux.zip

unzip Maltego.v4.2.19.13940.linux.zip

cd bin

./maltego
```



```
┌──(spi3er㉿kali)-[~/Desktop/recon-ng]
└─$ maltego
Command 'maltego' not found, but can be installed with:
sudo apt install maltego
Do you want to install it? (N/y)y
sudo apt install maltego
[sudo] password for spi3er:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer requ
d:
  libc-devtools python3-ajpy python3-pysmi python3-pysnmp4
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  java-wrappers
Suggested packages:
  maltego-teeth
The following NEW packages will be installed:
  java-wrappers maltego
0 upgraded, 2 newly installed, 0 to remove and 534 not upgraded.
Need to get 129 MB of archives.
After this operation, 214 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main arm64 java-wrappers
 0.3 [10.9 kB]
Get:2 http://ftp.harukasan.org/kali kali-rolling/non-free arm64 maltego al
.2.19.13940-0kali1 [129 MB]
```

For Mac OS

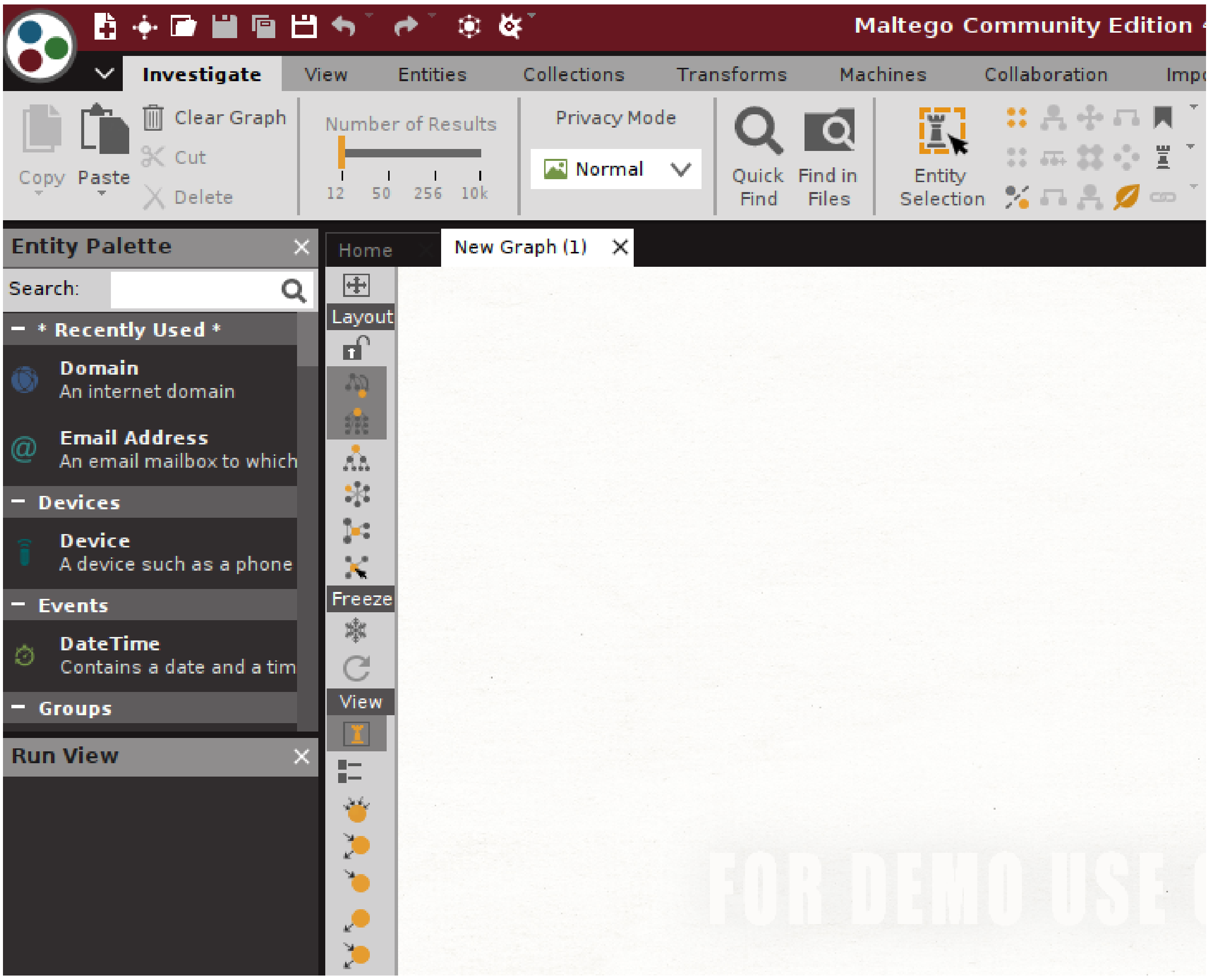
```bash
brew install maltego
```

For Kali Linux

```bash
sudo apt install maltego
```

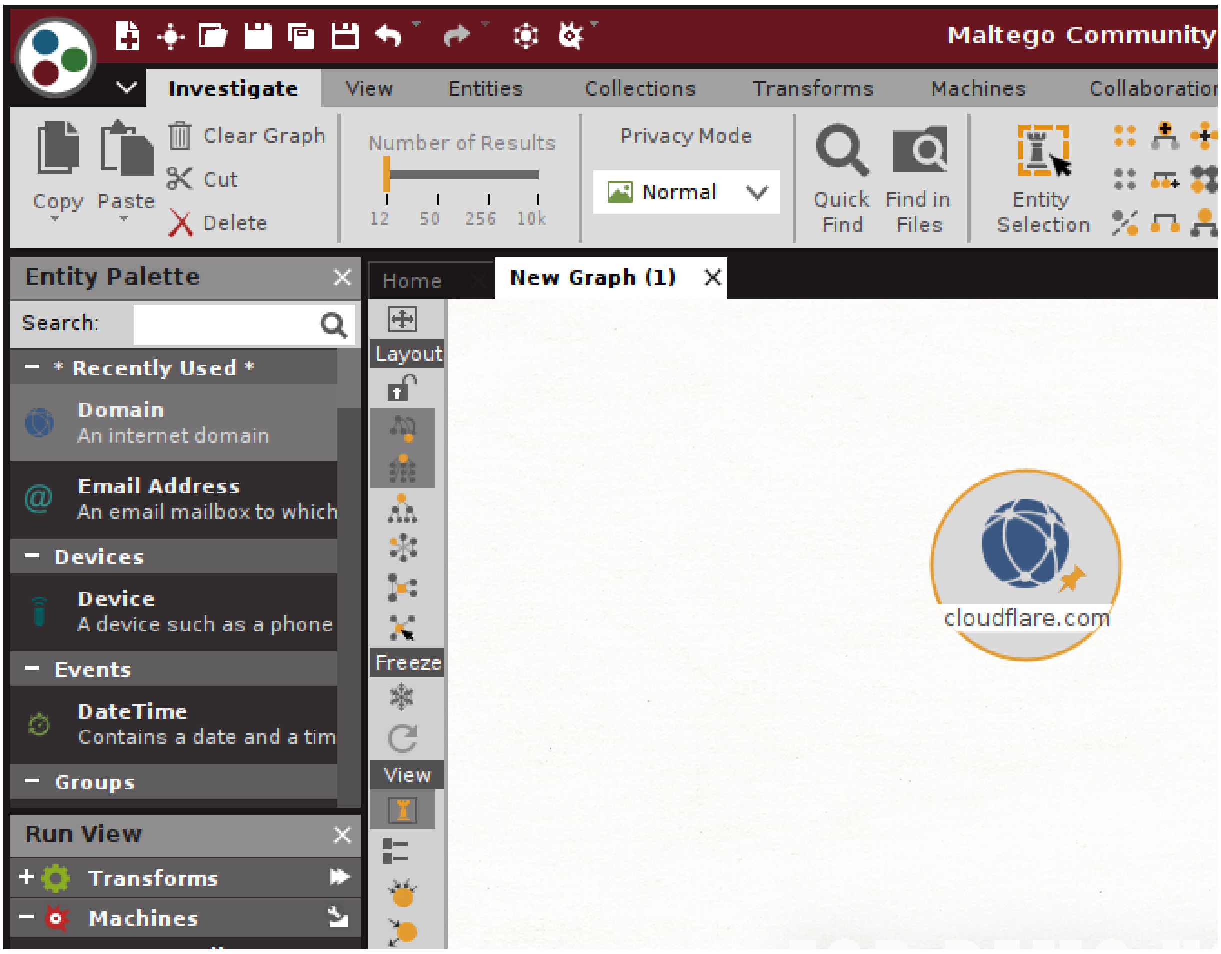
Maltego Usage

1. Open Maltego and click on New --> Create new Graph



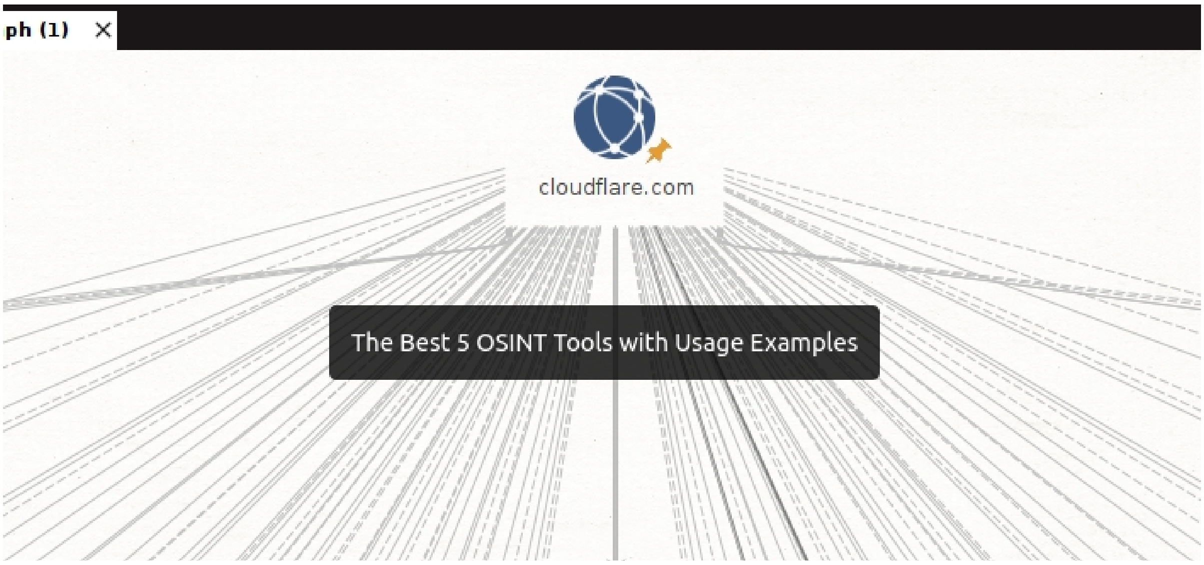
2. After that, all you have to do is select an Entity from the Entity Palette which is on the left side.

3. Let's check what happens if we select **Domain.** Select domain and drag it to the Graph.



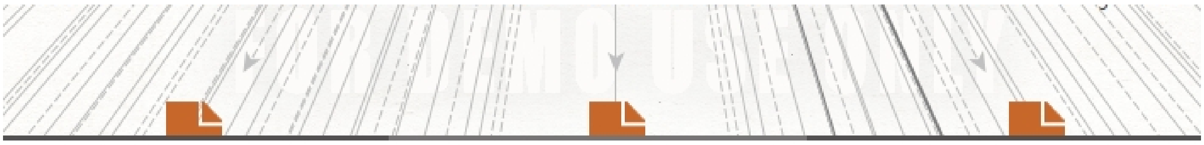
4. Click on the default domain which is white in colour and replace it with your domain.

5. Now click right click on the domain in the graph and select **All Transforms** and click on Run.



2. Shodan

Shodan can be basically called a deep search engine because just like how we use Google dorks, Shodan also has its own dorks which we can use to find CC Cameras , printers , databases , ftp servers, open ports, vulnerable instances and what not. Shodan is a must use tool when you are looking at a large scale for CVE's , vulnerable instances.

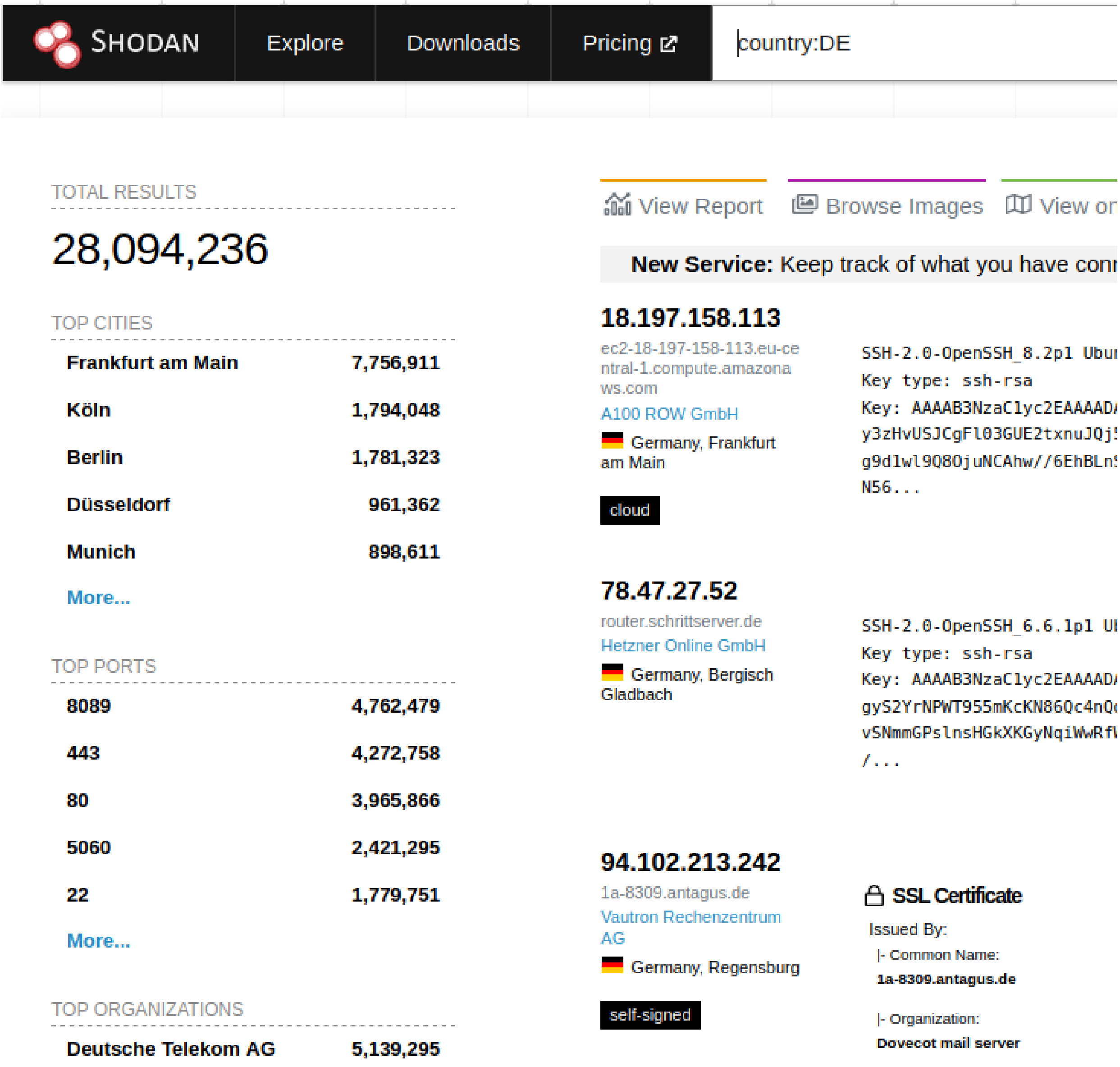


6. You will be able to see all the domains, documents , name servers and a lot of information.

You can perform the same for all the other entities and obtain a lot of information you need from Maltego.

Examples of Shodan dorks

1. country:DE



TOTAL RESULTS

28,094,236

TOP CITIES

Frankfurt am Main	7,756,911
Köln	1,794,048
Berlin	1,781,323
Düsseldorf	961,362
Munich	898,611

More...

TOP PORTS

8089	4,762,479
443	4,272,758
80	3,965,866
5060	2,421,295
22	1,779,751

More...

TOP ORGANIZATIONS

Deutsche Telekom AG	5,139,295

New Service: Keep track of what you have conn

18.197.158.113
ec2-18-197-158-113.eu-central-1.compute.amazonaws.com
A100 ROW GmbH
Germany, Frankfurt am Main
cloud

```
SSH-2.0-OpenSSH_8.2p1 Ubu
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAAD
y3zHvUSJCgFl03GUE2txnuJQj
g9d1wl9Q8OjuNCAhw//6EhBLn
N56...
```

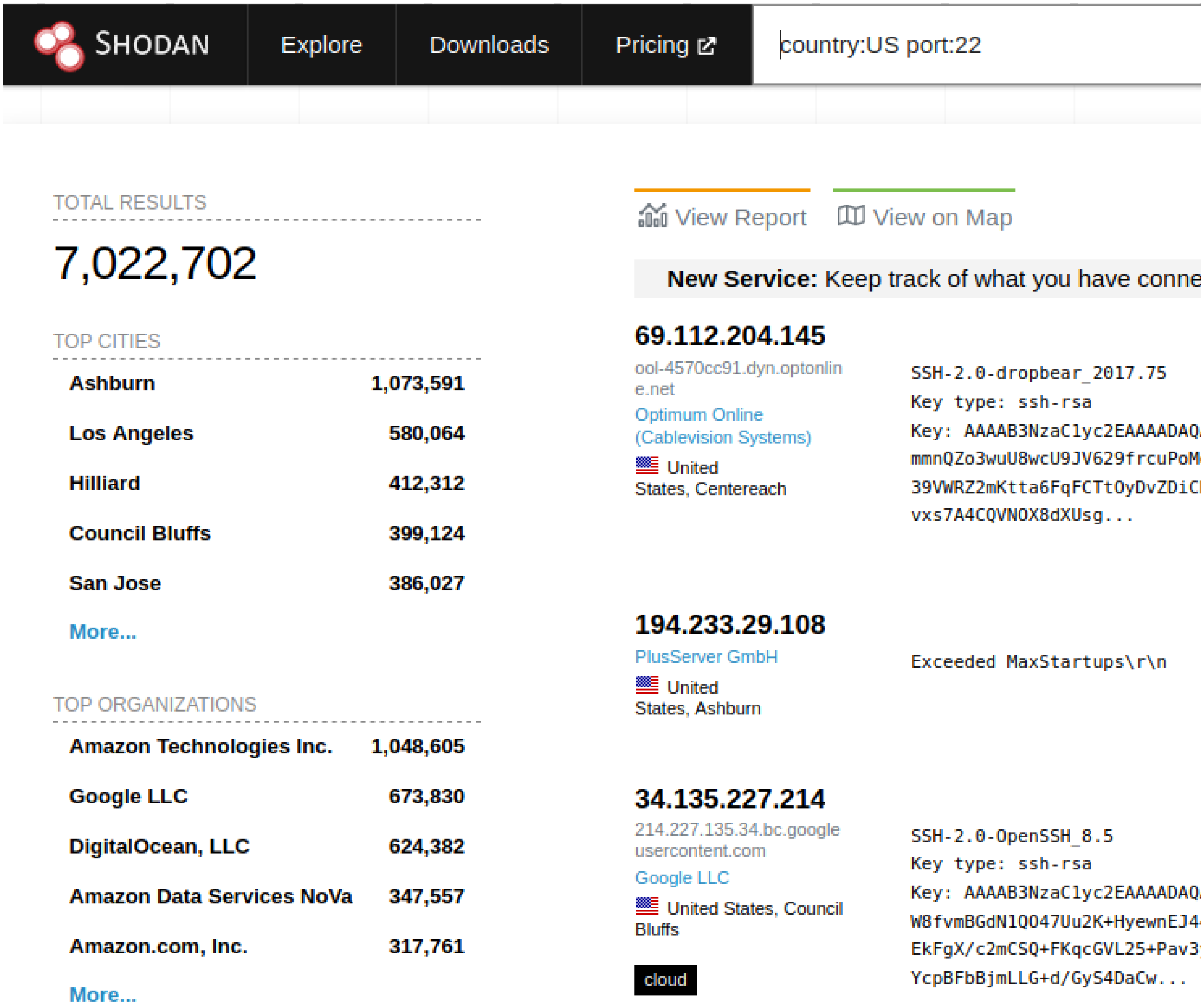
78.47.27.52
router.schrittserver.de
Hetzner Online GmbH
Germany, Bergisch Gladbach

```
SSH-2.0-OpenSSH_6.6.1p1 U
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAAD
gyS2YrNPWT955mKcKN86Qc4nQ
vSNmmGPslnsHGkXKGyNqiWwRf
/...
```

94.102.213.242
1a-8309.antagus.de
Vautron Rechenzentrum AG
Germany, Regensburg
self-signed

SSL Certificate
Issued By:
|- Common Name:
1a-8309.antagus.de
|- Organization:
Dovecot mail server

2. country:US port:22



TOTAL RESULTS

7,022,702

TOP CITIES

Ashburn	1,073,591
Los Angeles	580,064
Hilliard	412,312
Council Bluffs	399,124
San Jose	386,027

More...

TOP ORGANIZATIONS

Amazon Technologies Inc.	1,048,605
Google LLC	673,830
DigitalOcean, LLC	624,382
Amazon Data Services NoVa	347,557
Amazon.com, Inc.	317,761

More...

New Service: Keep track of what you have conne

69.112.204.145

ool-4570cc91.dyn.optonline.net
Optimum Online (Cablevision Systems)
United States, Centereach

```
SSH-2.0-dropbear_2017.75
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQ
mmnQZo3wuU8wcU9JV629frcuPoM
39VWRZ2mKtta6FqFCTtOyDvZDiC
vxs7A4CQVNOX8dXUsg...
```

194.233.29.108

PlusServer GmbH
United States, Ashburn

```
Exceeded MaxStartups\r\n
```

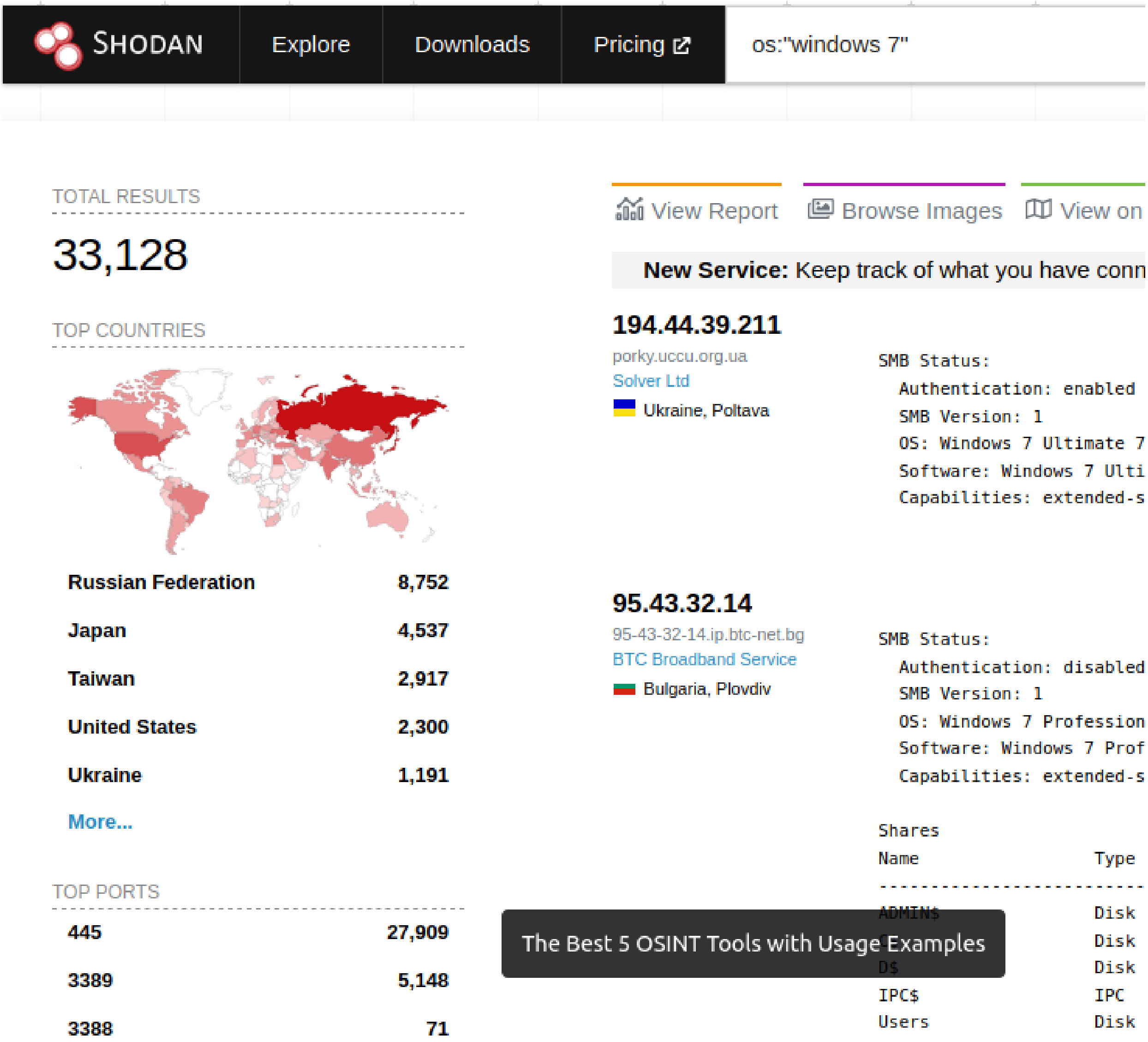
34.135.227.214

214.227.135.34.bc.googleusercontent.com
Google LLC
United States, Council Bluffs

cloud

```
SSH-2.0-OpenSSH_8.5
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQ
W8fvmBGdN1Q047Uu2K+HyewnEJ4
EkFgX/c2mCSQ+FKqcGVL25+Pav3
YcpBFbBjmLLG+d/GyS4DaCw...
```

3. os:"windows 7"



TOTAL RESULTS

33,128

TOP COUNTRIES

Russian Federation	8,752
Japan	4,537
Taiwan	2,917
United States	2,300
Ukraine	1,191

More...

TOP PORTS

445	27,909
3389	5,148
3388	71

New Service: Keep track of what you have conn

194.44.39.211
porky.uccu.org.ua
Solver Ltd
Ukraine, Poltava

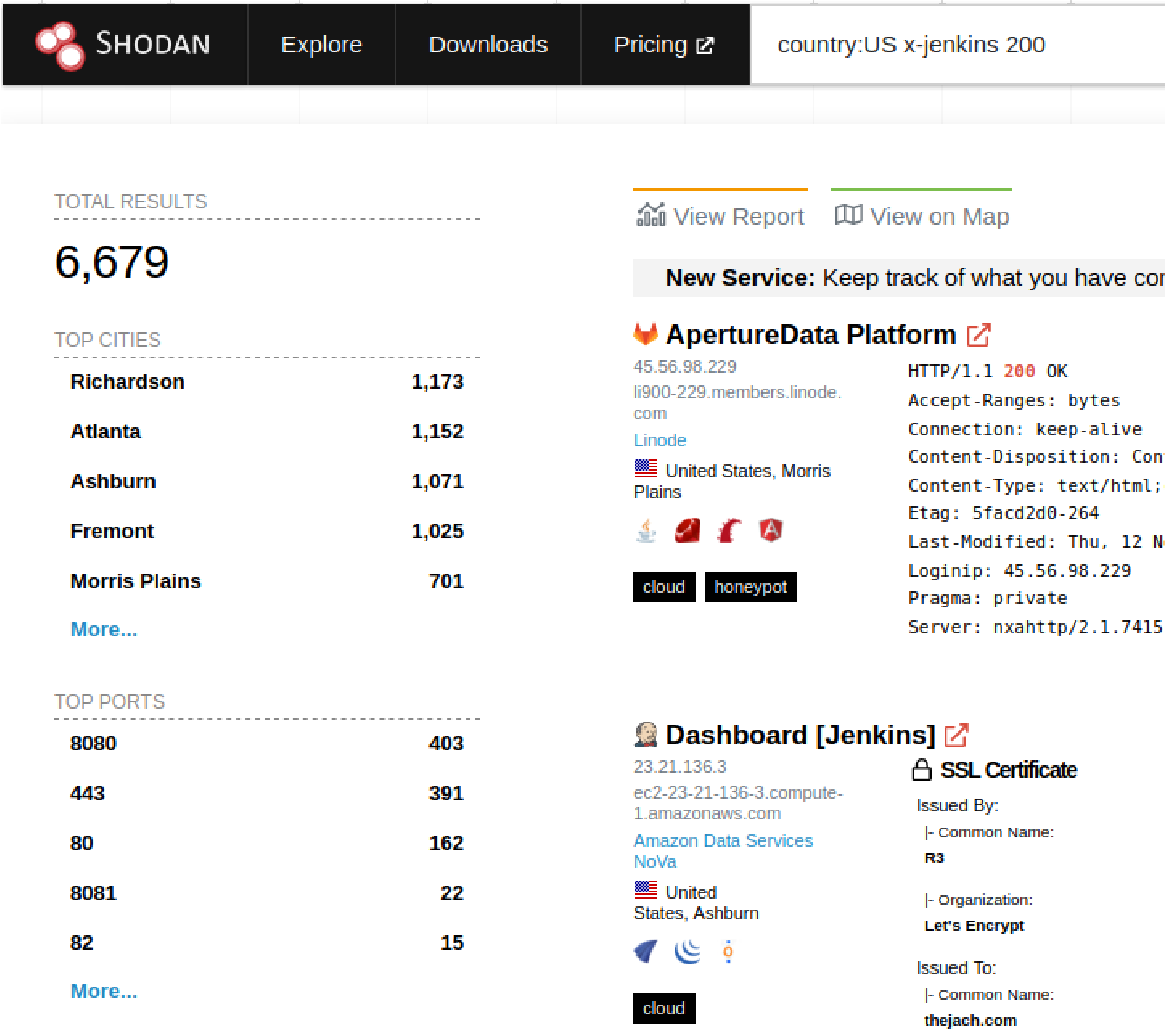
```
SMB Status:
  Authentication: enabled
  SMB Version: 1
  OS: Windows 7 Ultimate 7
  Software: Windows 7 Ulti
  Capabilities: extended-s
```

95.43.32.14
95-43-32-14.ip.btc-net.bg
BTC Broadband Service
Bulgaria, Plovdiv

```
SMB Status:
  Authentication: disabled
  SMB Version: 1
  OS: Windows 7 Profession
  Software: Windows 7 Prof
  Capabilities: extended-s

Shares
Name                 Type
-------------------------
ADMIN$               Disk
C$                   Disk
D$                   Disk
IPC$                 IPC
Users                Disk
```

The Best 5 OSINT Tools with Usage Examples

4. country:US x-jenkins 200



country:US x-jenkins 200

TOTAL RESULTS

6,679

TOP CITIES

Richardson	1,173
Atlanta	1,152
Ashburn	1,071
Fremont	1,025
Morris Plains	701

More...

TOP PORTS

8080	403
443	391
80	162
8081	22
82	15

More...

New Service: Keep track of what you have cor

ApertureData Platform

45.56.98.229
li900-229.members.linode.com
Linode
United States, Morris Plains

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Connection: keep-alive
Content-Disposition: Con
Content-Type: text/html;
Etag: 5facd2d0-264
Last-Modified: Thu, 12 N
Loginip: 45.56.98.229
Pragma: private
Server: nxahttp/2.1.7415
```

Dashboard [Jenkins]

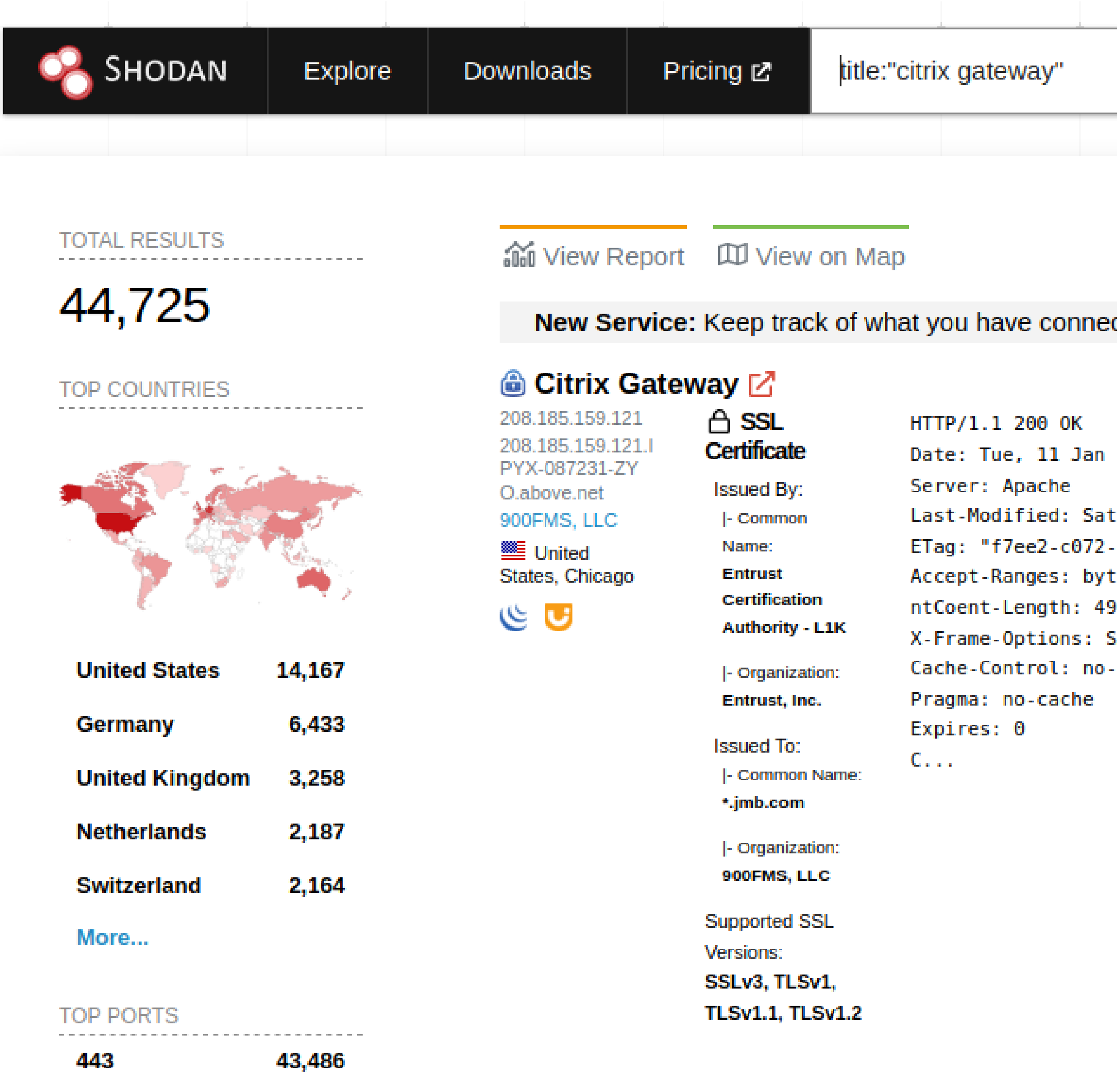
23.21.136.3
ec2-23-21-136-3.compute-1.amazonaws.com
Amazon Data Services NoVa
United States, Ashburn

SSL Certificate

Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
thejach.com

5. title:"citrix gateway"



TOTAL RESULTS

44,725

TOP COUNTRIES

United States	14,167
Germany	6,433
United Kingdom	3,258
Netherlands	2,187
Switzerland	2,164

More...

TOP PORTS

443	43,486

New Service: Keep track of what you have connec

Citrix Gateway

208.185.159.121
208.185.159.121.IPYX-087231-ZYO.above.net
900FMS, LLC
United States, Chicago

SSL Certificate

Issued By:
|- Common Name:
Entrust Certification Authority - L1K
|- Organization:
Entrust, Inc.

Issued To:
|- Common Name:
***.jmb.com**
|- Organization:
900FMS, LLC

Supported SSL Versions:
SSLv3, TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Date: Tue, 11 Jan
Server: Apache
Last-Modified: Sat
ETag: "f7ee2-c072-
Accept-Ranges: byt
ntCoent-Length: 49
X-Frame-Options: S
Cache-Control: no-
Pragma: no-cache
Expires: 0
C...
```

3. Google Dorks

Search engines like Google and bing make finding information easy and simple, particularly if we want to shop , find an address , looking for a job. However, you can use these search engines more advanced by making use of the search operators.

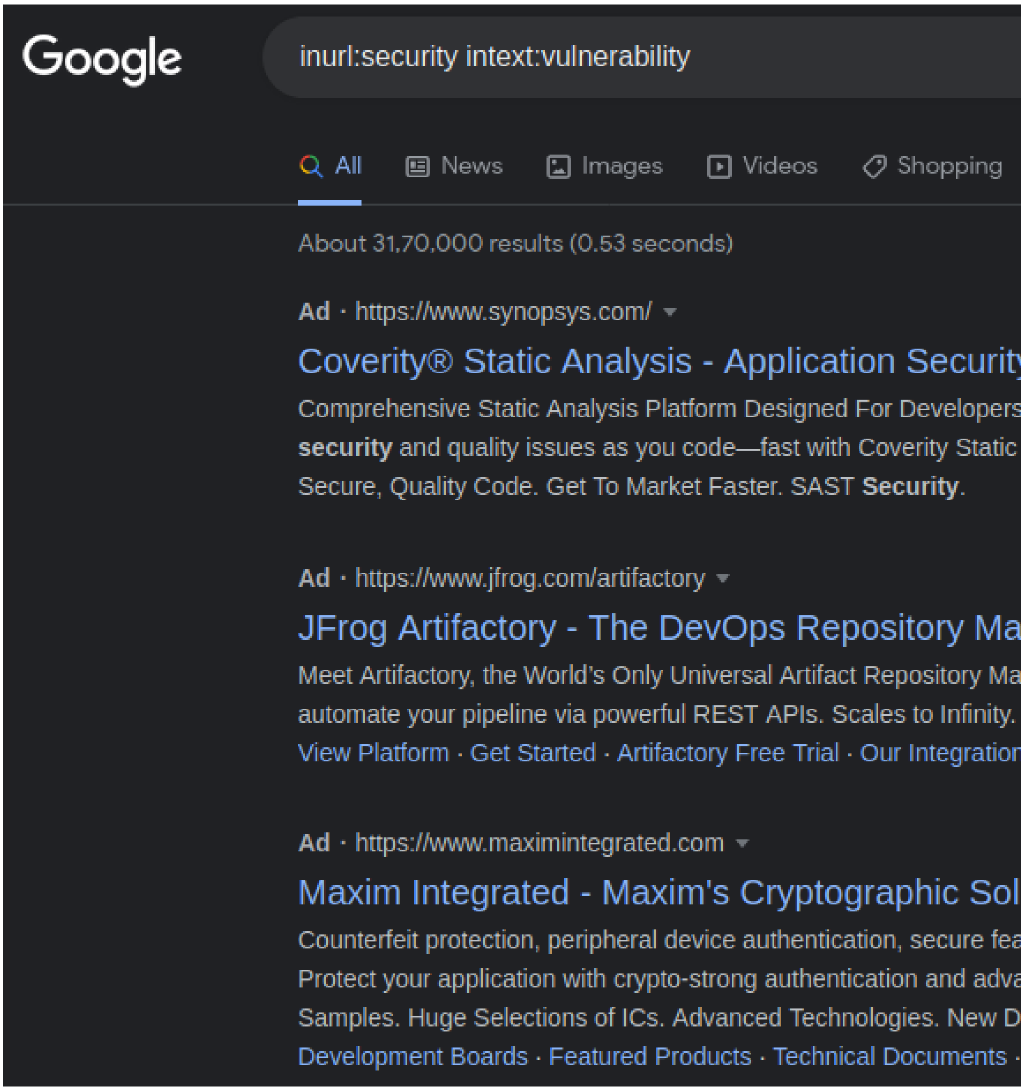
There are various kinds of operators available :

- Inurl:
- intitle:
- intext:
- site:
- cache:
- filetype:
- |
- -
- OR
- AND

We can make use of these operators to filter out any information we need from Google or Bing.

Let's see some examples how we can use Google dorks to find information!

Dork: inurl:security intext:vulnerability



About 31,70,000 results (0.53 seconds)

Ad · https://www.synopsys.com/

Coverity® Static Analysis - Application Security

Comprehensive Static Analysis Platform Designed For Developers
security and quality issues as you code—fast with Coverity Static
Secure, Quality Code. Get To Market Faster. SAST **Security**.

Ad · https://www.jfrog.com/artifactory

JFrog Artifactory - The DevOps Repository Ma

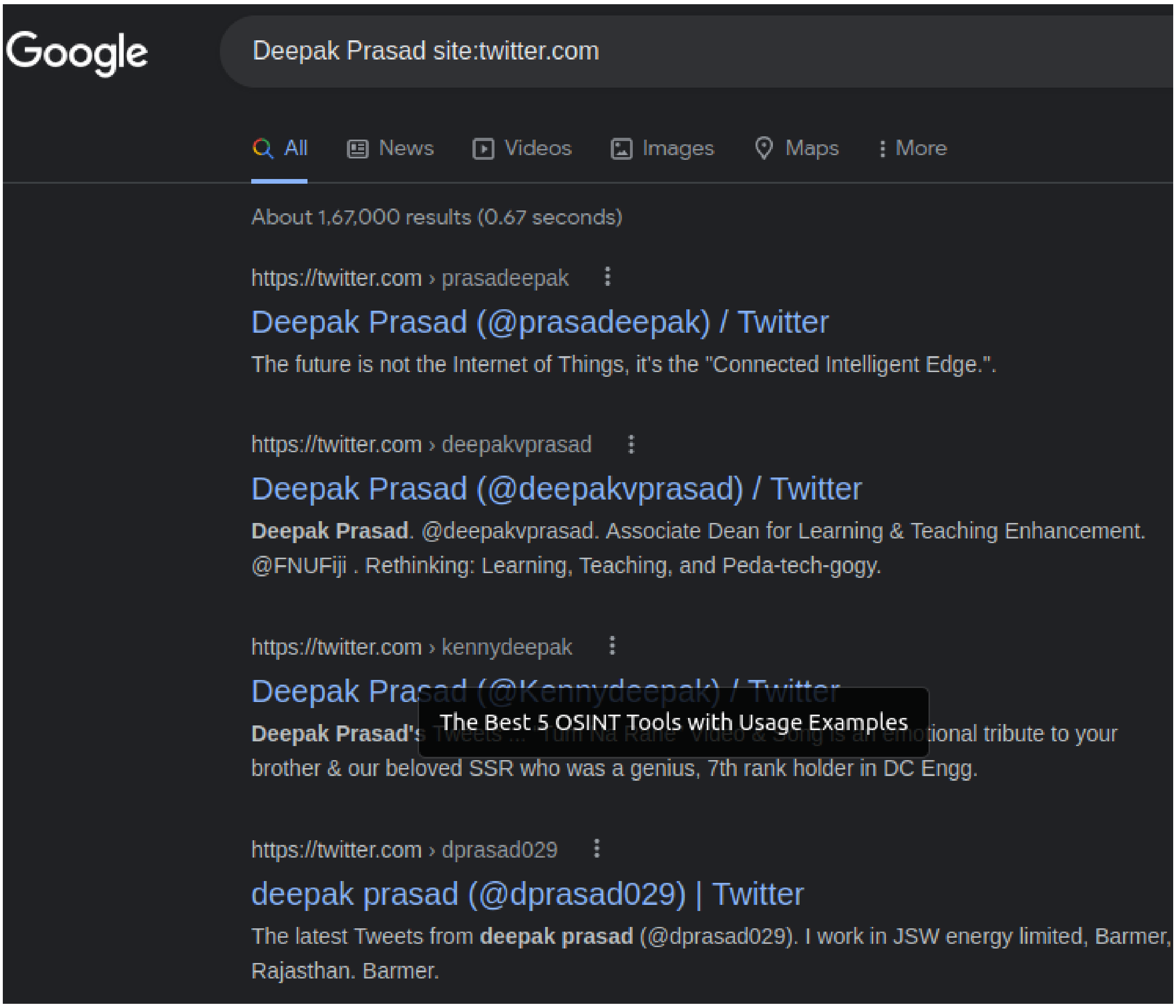
Meet Artifactory, the World's Only Universal Artifact Repository Ma
automate your pipeline via powerful REST APIs. Scales to Infinity.
View Platform · Get Started · Artifactory Free Trial · Our Integration

Ad · https://www.maximintegrated.com

Maxim Integrated - Maxim's Cryptographic Sol

Counterfeit protection, peripheral device authentication, secure fea
Protect your application with crypto-strong authentication and adva
Samples. Huge Selections of ICs. Advanced Technologies. New D
Development Boards · Featured Products · Technical Documents ·

Dork: Deepak Prasad site:twitter.com



Deepak Prasad site:twitter.com

About 1,67,000 results (0.67 seconds)

https://twitter.com › prasadeepak

Deepak Prasad (@prasadeepak) / Twitter

The future is not the Internet of Things, it's the "Connected Intelligent Edge.".

https://twitter.com › deepakvprasad

Deepak Prasad (@deepakvprasad) / Twitter

Deepak Prasad. @deepakvprasad. Associate Dean for Learning & Teaching Enhancement. @FNUFiji . Rethinking: Learning, Teaching, and Peda-tech-gogy.

https://twitter.com › kennydeepak

Deepak Prasad (@Kennydeepak) / Twitter

Deepak Prasad's Tweets ... "Tum Na Rahe" Video & Song is an emotional tribute to your brother & our beloved SSR who was a genius, 7th rank holder in DC Engg.

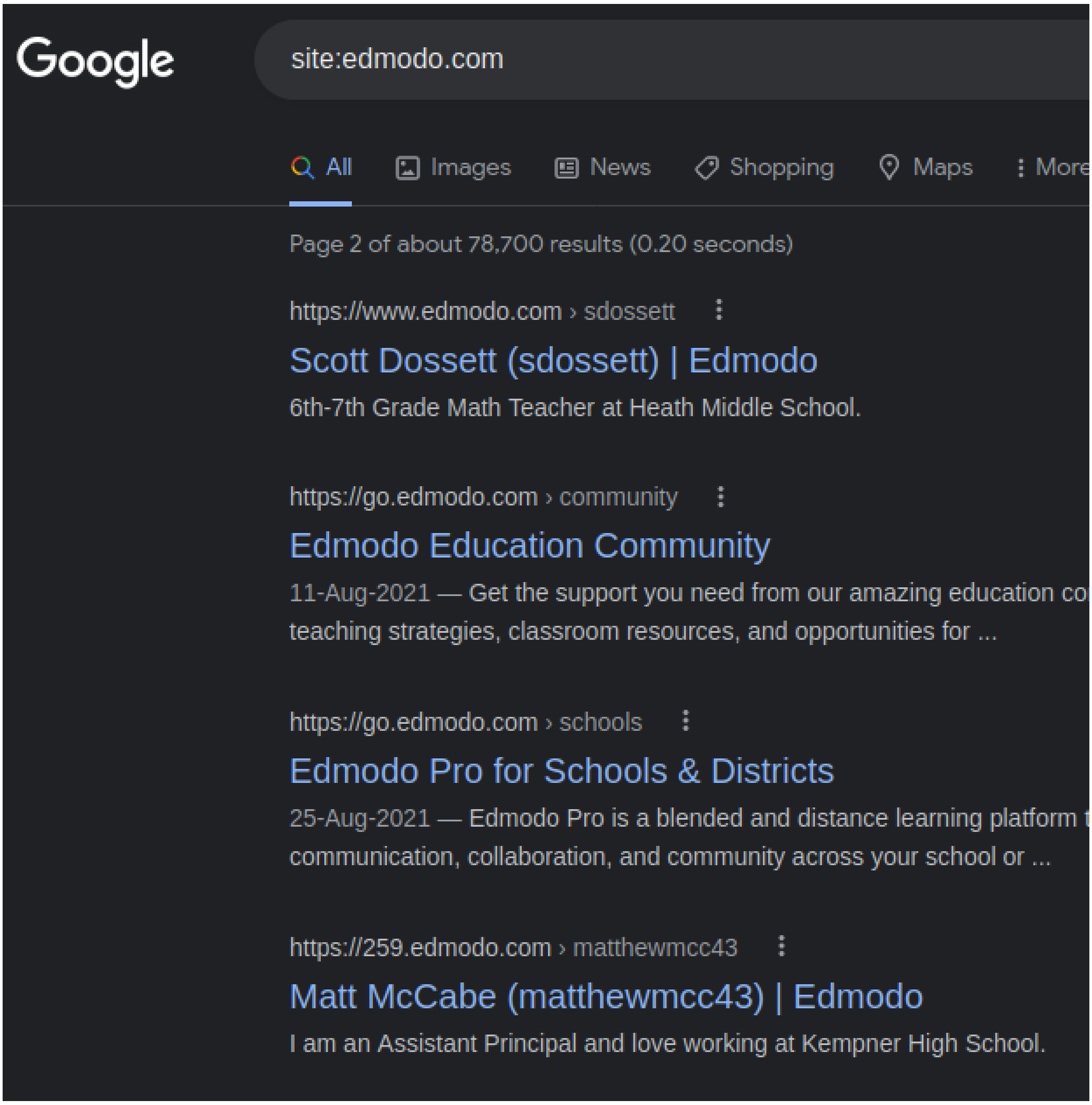
The Best 5 OSINT Tools with Usage Examples

https://twitter.com › dprasad029

deepak prasad (@dprasad029) | Twitter

The latest Tweets from **deepak prasad** (@dprasad029). I work in JSW energy limited, Barmer, Rajasthan. Barmer.

Dork: site: edmodo.com



Page 2 of about 78,700 results (0.20 seconds)

https://www.edmodo.com › sdossett

Scott Dossett (sdossett) | Edmodo

6th-7th Grade Math Teacher at Heath Middle School.

https://go.edmodo.com › community

Edmodo Education Community

11-Aug-2021 — Get the support you need from our amazing education co teaching strategies, classroom resources, and opportunities for ...

https://go.edmodo.com › schools

Edmodo Pro for Schools & Districts

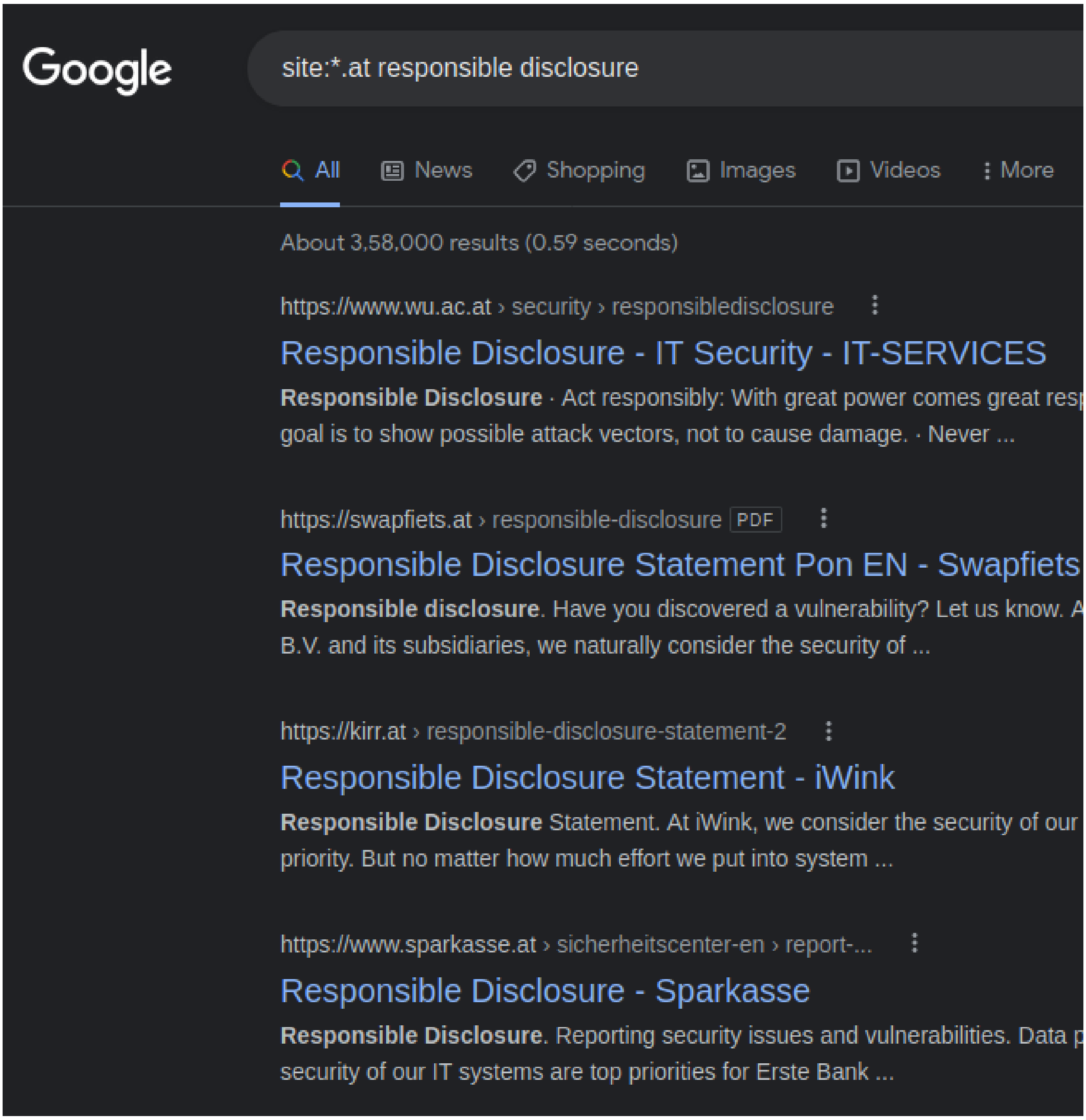
25-Aug-2021 — Edmodo Pro is a blended and distance learning platform t communication, collaboration, and community across your school or ...

https://259.edmodo.com › matthewmcc43

Matt McCabe (matthewmcc43) | Edmodo

I am an Assistant Principal and love working at Kempner High School.

Dork: site:*.at responsible disclosure



About 3,58,000 results (0.59 seconds)

https://www.wu.ac.at › security › responsibledisclosure

Responsible Disclosure - IT Security - IT-SERVICES

Responsible Disclosure · Act responsibly: With great power comes great resp goal is to show possible attack vectors, not to cause damage. · Never ...

https://swapfiets.at › responsible-disclosure PDF

Responsible Disclosure Statement Pon EN - Swapfiets

Responsible disclosure. Have you discovered a vulnerability? Let us know. A B.V. and its subsidiaries, we naturally consider the security of ...

https://kirr.at › responsible-disclosure-statement-2

Responsible Disclosure Statement - iWink

Responsible Disclosure Statement. At iWink, we consider the security of our priority. But no matter how much effort we put into system ...

https://www.sparkasse.at › sicherheitscenter-en › report-...

Responsible Disclosure - Sparkasse

Responsible Disclosure. Reporting security issues and vulnerabilities. Data p security of our IT systems are top priorities for Erste Bank ...

4. Recon-ng

Recon-ng is one of the easiest tools available to use for your OSINT purposes. If you have ever used Metasploit , then you will find the syntax and interface very similar. Recon-ng has its own modules inbuilt through which we can find information like social media handles , email addresses , domains , files and etc. You can also write your own modules and use them if you want to.

Recon-ng can also be used as a recon tool while you are doing Web Penetration testing , so it can be said to an ultimate tool for Web pentesters Recon and OSINT. You can create your own workspace in Recon-ng too. All the recon or OSINT will be done by inserting values into Db schema.

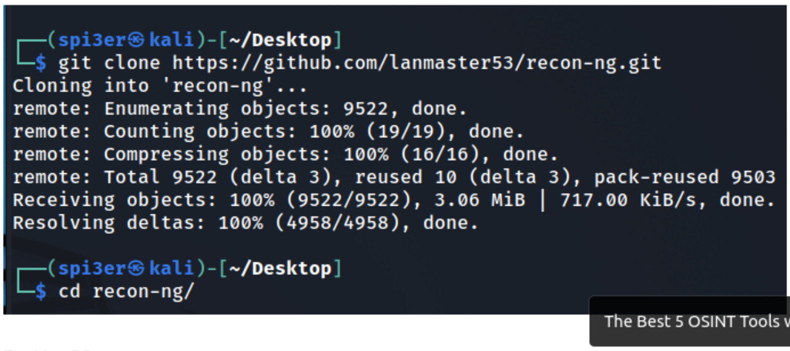
There are multiple tables in the db module:

```bash
companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities
```

Installation

Ubuntu/Debian

```bash
git clone https://github.com/lanmaster53/recon-ng.git
cd recon-ng
recon-ng
```



```
┌──(spi3er㉿kali)-[~/Desktop]
└─$ git clone https://github.com/lanmaster53/recon-ng.git
Cloning into 'recon-ng'...
remote: Enumerating objects: 9522, done.
remote: Counting objects: 100% (19/19), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 9522 (delta 3), reused 10 (delta 3), pack-reused 9503
Receiving objects: 100% (9522/9522), 3.06 MiB | 717.00 KiB/s, done.
Resolving deltas: 100% (4958/4958), done.

┌──(spi3er㉿kali)-[~/Desktop]
└─$ cd recon-ng/
```

The Best 5 OSINT Tools with Usage Examples

For Mac OS

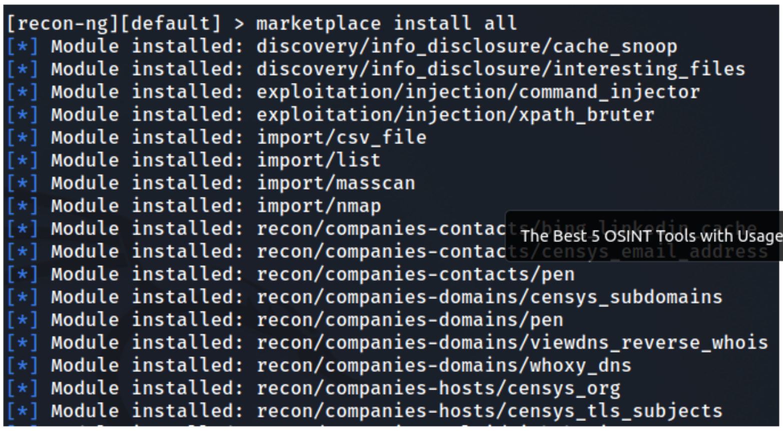
```bash
brew install recon-ng
```

Recon-ng Usage

Before we start the using Recon-ng, we have to perform some commands in recon-ng using

```bash
marketplace install all ---> Install all the modules [image in media]
workspaces create Osint ---> Create a workspace for us.
db schema ---> Check the Database schema
db insert domains ---> Use this command and enter your domain
```

Only after you execute these 4 commands , you can start using Recon-ng.

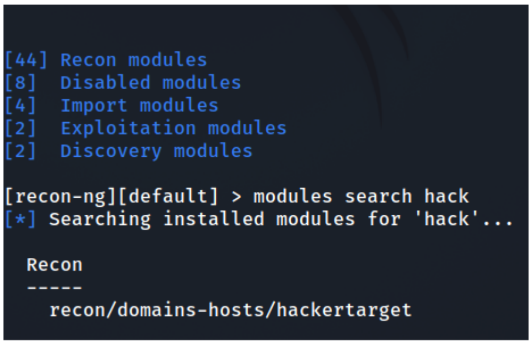


```
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
```

The Best 5 OSINT Tools with Usage Examples

Search for modules installed

```bash
modules search hack
```

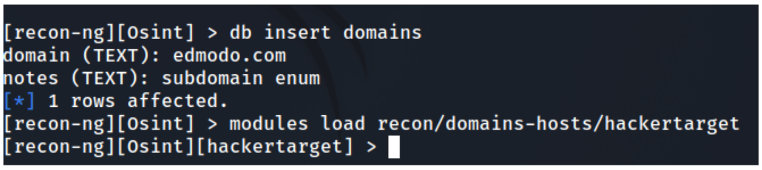


```
[44] Recon modules
[8]  Disabled modules
[4]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

[recon-ng][default] > modules search hack
[*] Searching installed modules for 'hack'...

  Recon
  -----
    recon/domains-hosts/hackertarget
```

Load the module you searched

The Best 5 OSINT Tools with Usage Examples

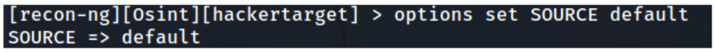
```bash
modules load recon/domain-hosts/hackertarget
```



```
[recon-ng][Osint] > db insert domains
domain (TEXT): edmodo.com
notes (TEXT): subdomain enum
[*] 1 rows affected.
[recon-ng][Osint] > modules load recon/domains-hosts/hackertarget
[recon-ng][Osint][hackertarget] >
```

Set Options Source to Default to use the domains inserted into Db Schema

```bash
 options set SOURCE default
```



```
[recon-ng][Osint][hackertarget] > options set SOURCE default
SOURCE => default
```

Last and final, use command **run** and you will be able to find lot's of subdomains. There are various modules installed in recon-ng and you can always load them and set options for each module and run them according to your need.

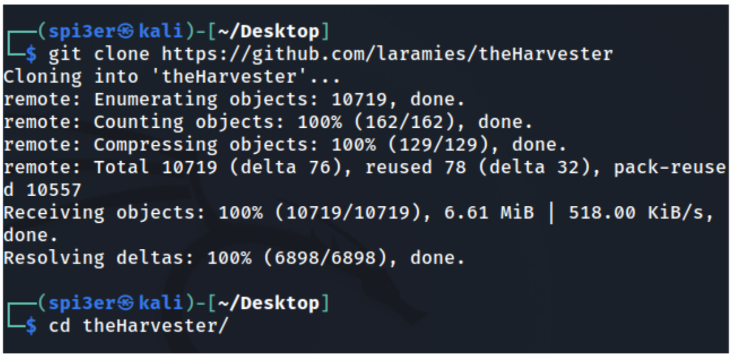
5. Harvester

Harvester is an open source tool made with python which is very easy to use and configure. It can be used to find domains , email addresses , IP's , employee names , open ports and etc. It grabs the information from many sources like google , bing , Anubis, censys, shodan and 15 more.

Installation

You can install `theHarvester` on Linux OS using the following commands :

```bash
git clone https://github.com/laramies/theHarvester
cd theHarvester
pip3 install -r requirements.txt
```



```
┌──(spi3er㉿kali)-[~/Desktop]
└─$ git clone https://github.com/laramies/theHarvester
Cloning into 'theHarvester'...
remote: Enumerating objects: 10719, done.
remote: Counting objects: 100% (162/162), done.
remote: Compressing objects: 100% (129/129), done.
remote: Total 10719 (delta 76), reused 78 (delta 32), pack-reuse
d 10557
Receiving objects: 100% (10719/10719), 6.61 MiB | 518.00 KiB/s,
done.
Resolving deltas: 100% (6898/6898), done.

┌──(spi3er㉿kali)-[~/Desktop]
└─$ cd theHarvester/
```

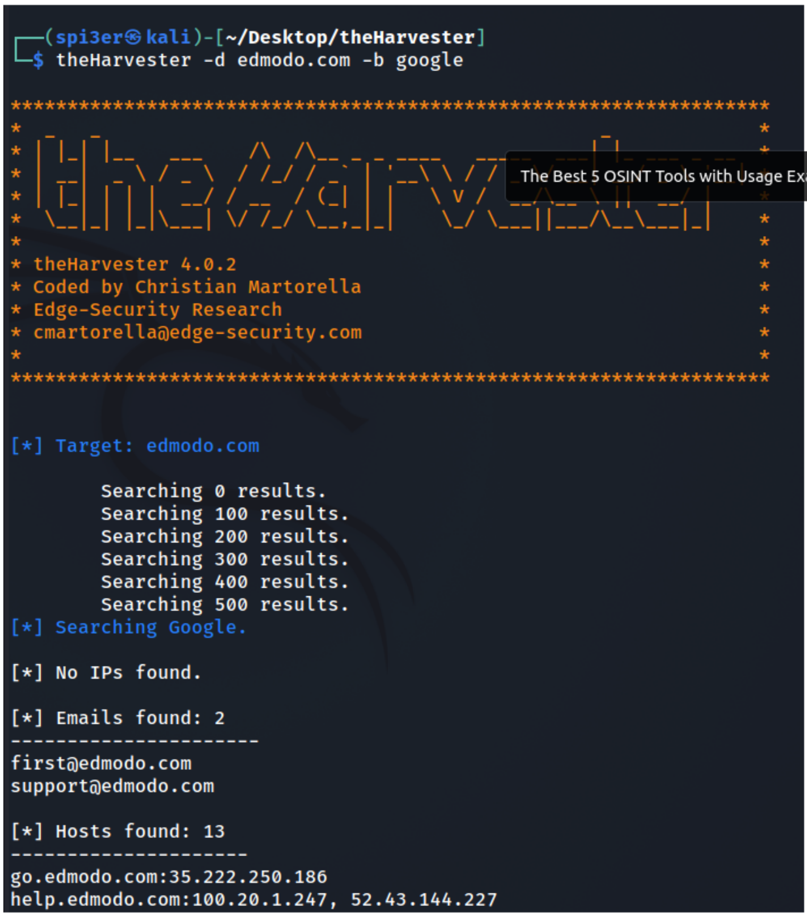
For Mac OS

```bash
brew install theharvester
```

Harvester Usage

Search email addresses and domains from example.com and using **Google** as data source.

```bash
theHarvester -d example.com -b google
```



```
┌──(spi3er㉿kali)-[~/Desktop/theHarvester]
└─$ theHarvester -d edmodo.com -b google

*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.0.2                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: edmodo.com

        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
        Searching 300 results.
        Searching 400 results.
        Searching 500 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 2
----------------------
first@edmodo.com
support@edmodo.com

[*] Hosts found: 13
---------------------
go.edmodo.com:35.222.250.186
help.edmodo.com:100.20.1.247, 52.43.144.227
```

The Best 5 OSINT Tools with Usage Examples

Set limits to your results.

```bash
theHarvester -d example.com -l 400 -b google
```

Save the result in HTML file by using **-f** option.

```bash
theHarvester -d example.com -b google -f results.html
```