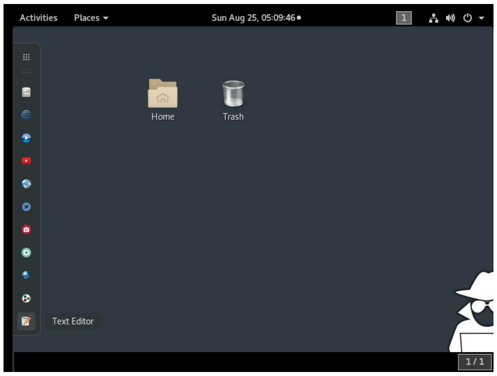
Alec Miller
August Project

Buscador

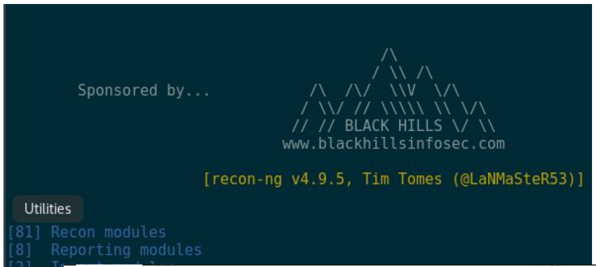
Buscador is a Linux Virtual Machine run with programs like VirtualBox or VMWare. Buscador resembles other OSINT tools such as Kali Linux.



After logging into Buscador, the desktop is filled with useful tools for gathering information on a target. These tools include Recon-NG, Metadata, Maltego and loads more.

Most of the applications are in their respective section on the toolbar on the left side of the screen. These sections include: Social Networks, Domain Interact, Browsers, and Utilities. Two programs, Recon-NG and Maltego, are also displayed without being in a subsection.

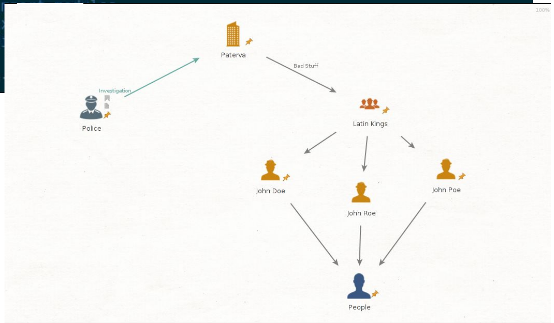
Recon-NG



```
                                  /\
                                 / \\ /\
    Sponsored by...        /\  /\/  \\V  \/\
                          / \\/ // \\\\\ \\ \/\
                         // // BLACK HILLS \/ \\
                        www.blackhillsinfosec.com

                  [recon-ng v4.9.5, Tim Tomes (@LaNMaSteR53)]

[81] Recon modules
[8]  Reporting modules
[2]  I
[2]  E
[2]  D

[recon
```

The first of the two highlighted programs is Recon-NG. This program has extensive tools useful for gathering target data including IP addresses, website vulnerabilities, and geolocation based on the target's activities. For a more indepth look Recon-NG's capabilities, it is available here.

Maltego

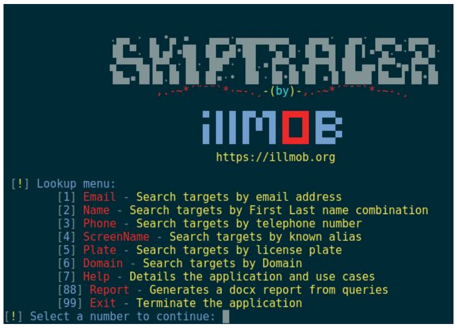


Maltego, a powerful link analysis tool, is showcased by Buscador and frequently demonstrated in Plessas Experts Network's OSINT training classes for its use in website evaluation. Linking sources together, this tool provides a graphic display with loads of options to assist with visually analyzing gathered data. Maltego's graph is easily readable: while zooming in, the properties have unique icons displaying what they are; while zooming out, the icons become dots with a key at the bottom of the screen that defines each dot. Maltego is an amazing tool for finding relationships between pieces of information on an easy to use interface.

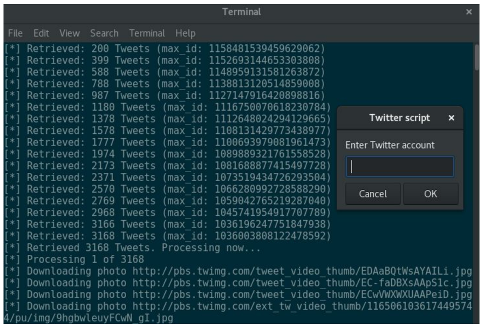
Hyperlinks are given to see the full size photos.

Social Networks

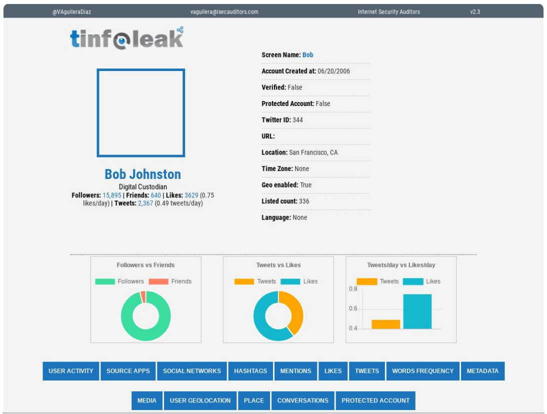
When using Buscador's *Social Networks* tool, there are four options to choose from: skiptracer, Twitter script, Tinfoleak and instalooter (unfortunately, instalooter is currently broken). Skiptracer is a super simple program that is very useful, as its name implies, for people search. Navigation through the program is based on using numbers and the Enter key. Searches that skiptracer provides include: email, name, phone number, screen name, license plate and domain. Within each search type, there are different options to search from: email searches may include LinkedIn, HaveIBeenPwned, Myspace, AdvancedBackgroundChecks, and All. Twitter script is another easy to use program: input a twitter handle and run the search. The output includes all of the tweets by that user and all of the photo links will be given in the Terminal. Finally, Tinfoleak, like Twitter script, simply requires a twitter handle. Enter the user's handle into the blank User space and click Apply. Once the program runs, an HTML report will be given. Copy the entire report and paste it into a browser. This link will give an extensive report on the user's account including location, creation date, and more.



```
SKIPTRACER
-(by)-
iIIMOB
https://illmob.org

[!] Lookup menu:
        [1] Email - Search targets by email address
        [2] Name - Search targets by First Last name combination
        [3] Phone - Search targets by telephone number
        [4] ScreenName - Search targets by known alias
        [5] Plate - Search targets by license plate
        [6] Domain - Search targets by Domain
        [7] Help - Details the application and use cases
        [88] Report - Generates a docx report from queries
        [99] Exit - Terminate the application
[!] Select a number to continue:
```



```
[*] Retrieved: 200 Tweets (max_id: 1158481539459629062)
[*] Retrieved: 399 Tweets (max_id: 1152693144653303808)
[*] Retrieved: 588 Tweets (max_id: 1148959131581263872)
[*] Retrieved: 788 Tweets (max_id: 1138813120514859008)
[*] Retrieved: 987 Tweets (max_id: 1127147916420898816)
[*] Retrieved: 1180 Tweets (max_id: 1116750070618230784)
[*] Retrieved: 1378 Tweets (max_id: 1112648024294129665)
[*] Retrieved: 1578 Tweets (max_id: 1108131429773438977)
[*] Retrieved: 1777 Tweets (max_id: 1100693979081961473)
[*] Retrieved: 1974 Tweets (max_id: 1089889321761558528)
[*] Retrieved: 2173 Tweets (max_id: 1081688877415497728)
[*] Retrieved: 2371 Tweets (max_id: 1073519434726293504)
[*] Retrieved: 2570 Tweets (max_id: 1066280992728588290)
[*] Retrieved: 2769 Tweets (max_id: 1059042765219287040)
[*] Retrieved: 2968 Tweets (max_id: 1045741954917707789)
[*] Retrieved: 3166 Tweets (max_id: 1036196247751847938)
[*] Retrieved: 3168 Tweets (max_id: 1036003808122478592)
[*] Retrieved 3168 Tweets. Processing now...
[*] Processing 1 of 3168
[*] Downloading photo http://pbs.twimg.com/tweet_video_thumb/EDAaBQtWsAYAILi.jpg
[*] Downloading photo http://pbs.twimg.com/tweet_video_thumb/EC-faDBXsAApS1c.jpg
[*] Downloading photo http://pbs.twimg.com/tweet_video_thumb/ECwVWXWXUAAPeiD.jpg
[*] Downloading photo http://pbs.twimg.com/ext_tw_video_thumb/116506103617449574
4/pu/img/9hgbwleuyFCwN_gI.jpg
```

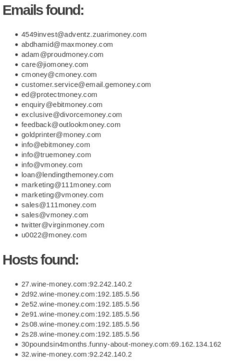


Bob Johnston
Digital Custodian
Followers: 15,895 | Friends: 640 | Likes: 3629 (0.75 likes/day) | Tweets: 2,367 (0.49 tweets/day)

Screen Name: Bob
Account Created at: 06/20/2006
Verified: False
Protected Account: False
Twitter ID: 344
URL:
Location: San Francisco, CA
Time Zone: None
Geo enabled: True
Listed count: 336
Language: None

Domain Interact

The Domain Interact section has many tools including: Amass, theHarvester, EmailHarvester, Metagoofil, Sublist3r, Knock, Photon, Subbrute, Web HTTrack, and EyeWitness. At the time of this writing, Amass seems broken. However, theHarvester is a super useful tool to find user emails, hosts, and their IP addresses based on a domain name. For my example, I used money.com. When theHarvester completes its analysis of a domain, a web browser pops up displaying all the collected information. Next, EmailHarvester searches for email addresses with a specific domain using many websites including Baidu, Exalead, Linkedin, Github, and many more. Using the collected information, EmailHarvester produces a report in two file formats, .txt and .xml. While the two files hold the same information, the .xml file may be viewed in a browser. The next tool is Metagoofil. This program is amazing at gathering information based on the website including the authors, companies, full text, and dates the website has been modified and who modified the website. When first starting Metagoofil and the

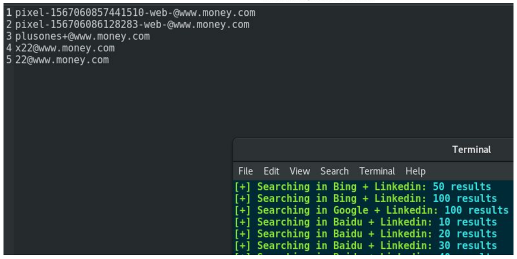


Emails found:

- 4549invest@adventz.zuarimoney.com
- abdhamid@maxmoney.com
- adam@proudmoney.com
- care@jiomoney.com
- cmoney@cmoney.com
- customer.service@email.gemoney.com
- ed@protectmoney.com
- enquiry@ebitmoney.com
- exclusive@divorcemoney.com
- feedback@outlookmoney.com
- goldprinter@money.com
- info@ebitmoney.com
- info@truemoney.com
- info@vmoney.com
- loan@lendingthemoney.com
- marketing@111money.com
- marketing@vmoney.com
- sales@111money.com
- sales@vmoney.com
- twitter@virginmoney.com
- u0022@money.com

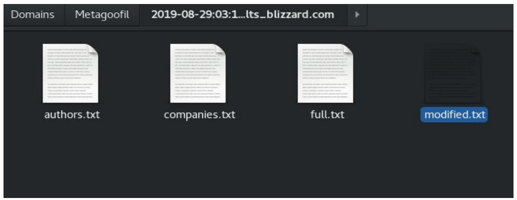
Hosts found:

- 27.wine-money.com:92.242.140.2
- 2d92.wine-money.com:192.185.5.56
- 2e52.wine-money.com:192.185.5.56
- 2e91.wine-money.com:192.185.5.56
- 2s08.wine-money.com:192.185.5.56
- 2s28.wine-money.com:192.185.5.56
- 30poundsin4months.funny-about-money.com:69.162.134.162
- 32.wine-money.com:92.242.140.2



```
pixel-1567060857441510-web-@www.money.com
pixel-156706086128283-web-@www.money.com
plusones+@www.money.com
x22@www.money.com
22@www.money.com
```

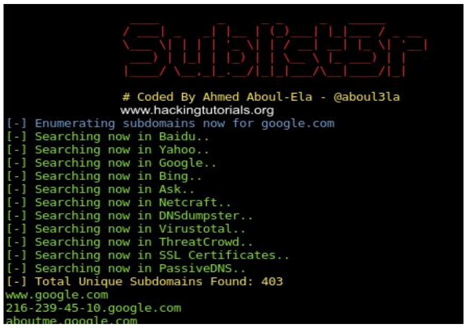
```
[+] Searching in Bing + Linkedin: 50 results
[+] Searching in Bing + Linkedin: 100 results
[+] Searching in Google + Linkedin: 100 results
[+] Searching in Baidu + Linkedin: 10 results
[+] Searching in Baidu + Linkedin: 20 results
[+] Searching in Baidu + Linkedin: 30 results
```



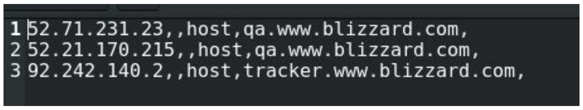
authors.txt
companies.txt
full.txt
modified.txt

Hyperlinks are given to see the full size photos.

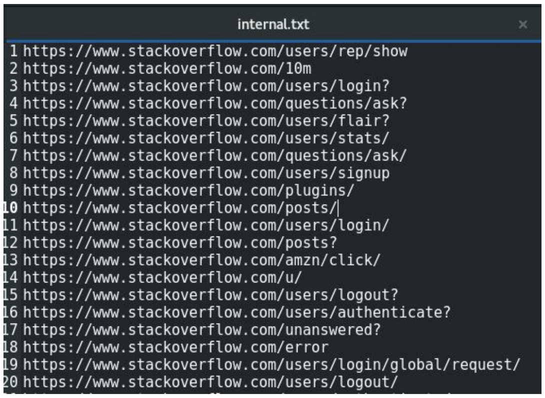
website has been entered the user can input the amount of files they would like Metagoofil to retrieve from the website. When the program finishes running, the files should pop up on the screen like the others described above. If this does not happen, the information may be located by searching the home folder for Metagoofil. Sublist3r evaluates a website by searching for all subdomains associated with the website. Google, for example, has many subdomains that millions of people access every day including: docs.google.com, maps.google.com, mail.google.com that Sublist3r had no trouble indexing for my search. Similar to Sublist3r, Knock finds the subdomains linked to a designated domain. Unlike Sublist3r, this program also includes the subdomain's ip address. Once searched, the information can be found in the Knock folder as described above. Besides the subdomain's IP, Knock also searches for subdomain's status, type, domain name (of course) and the server. If some of these are not found, the file will have two commas next to each other, as depicted in the image to the right. Photon is next up on the Domain Interact list. When starting Photon in Buscador, a blank box appears with a confusing example: "Enter target base URL (ex: https://inteltechniques.com). However, if the user includes the "https://", Photon gives an error and quits. Instead, do NOT include the "https://" prefix when entering a target. Once Photon runs, two files will be created: internal.txt and robots.txt. Both of these files have relatively the same information. Photon returns different parts of the website; for example I used stackoverflow.com and one of the many results is "stackoverflow.com/users/logout?". The next program, Subbrute, uses brute force to find the subdomains of websites and does not send traffic to the target. Subbrute is anonymous, using DNS rate-limiting to ensure the safety of the user to not send multiple requests to a server leading to an unintentional DDoS. When the program is done running, Subbrute creates a file with all the gathered information including the subdomain URL, sometimes an IP address, and more. Web HTTrack downloads a target website, saving it into your computer's "websites" folder. For archiving and monitoring a website, this is a very useful tool.



```
                # Coded By Ahmed Aboul-Ela - @aboul3la
                www.hackingtutorials.org
[-] Enumerating subdomains now for google.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 403
www.google.com
216-239-45-10.google.com
aboutme.google.com
```

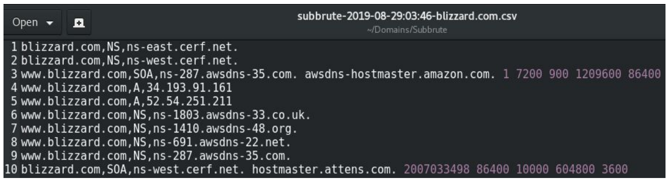


```
52.71.231.23,,host,qa.www.blizzard.com,
52.21.170.215,,host,qa.www.blizzard.com,
92.242.140.2,,host,tracker.www.blizzard.com,
```



internal.txt

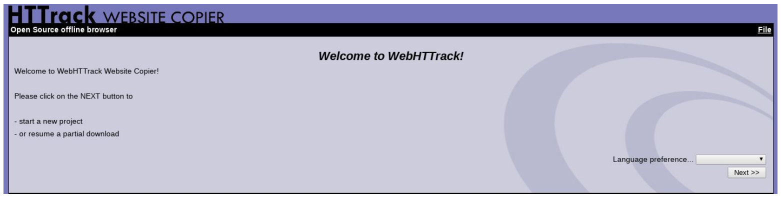
```
https://www.stackoverflow.com/users/rep/show
https://www.stackoverflow.com/10m
https://www.stackoverflow.com/users/login?
https://www.stackoverflow.com/questions/ask?
https://www.stackoverflow.com/users/flair?
https://www.stackoverflow.com/users/stats/
https://www.stackoverflow.com/questions/ask/
https://www.stackoverflow.com/users/signup
https://www.stackoverflow.com/plugins/
https://www.stackoverflow.com/posts/
https://www.stackoverflow.com/users/login/
https://www.stackoverflow.com/posts?
https://www.stackoverflow.com/amzn/click/
https://www.stackoverflow.com/u/
https://www.stackoverflow.com/users/logout?
https://www.stackoverflow.com/users/authenticate?
https://www.stackoverflow.com/unanswered?
https://www.stackoverflow.com/error
https://www.stackoverflow.com/users/login/global/request/
https://www.stackoverflow.com/users/logout/
```



subbrute-2019-08-29:03:46-blizzard.com.csv
~/Domains/Subbrute

```
blizzard.com,NS,ns-east.cerf.net.
blizzard.com,NS,ns-west.cerf.net.
www.blizzard.com,SOA,ns-287.awsdns-35.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
www.blizzard.com,A,34.193.91.161
www.blizzard.com,A,52.54.251.211
www.blizzard.com,NS,ns-1803.awsdns-33.co.uk.
www.blizzard.com,NS,ns-1410.awsdns-48.org.
www.blizzard.com,NS,ns-691.awsdns-22.net.
www.blizzard.com,NS,ns-287.awsdns-35.com.
blizzard.com,SOA,ns-west.cerf.net. hostmaster.attens.com. 2007033498 86400 10000 604800 3600
```

EyeWitness is a time-saving screenshotting tool used to take multiple screenshots of multiple websites at the same time and create a single image of all the screenshots. Instead of looking at every website one by one, they are all placed into a single file for quick review and comparison. Here is a screenshot captured by Eyewitness (on right).



Welcome to WebHTTrack!

Welcome to WebHTTrack Website Copier!

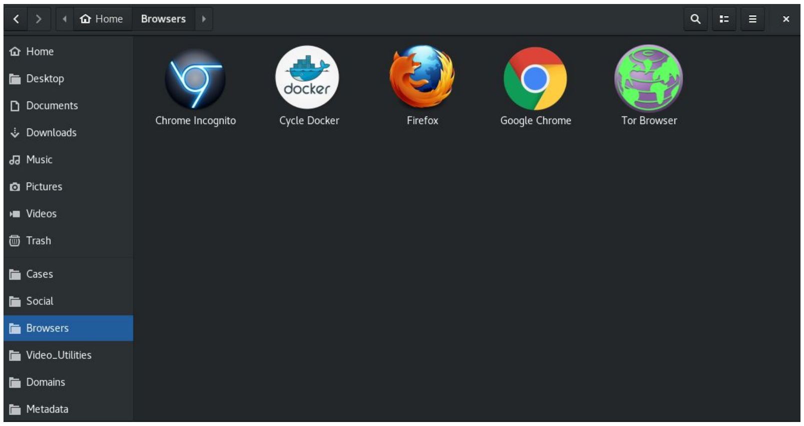
Please click on the NEXT button to

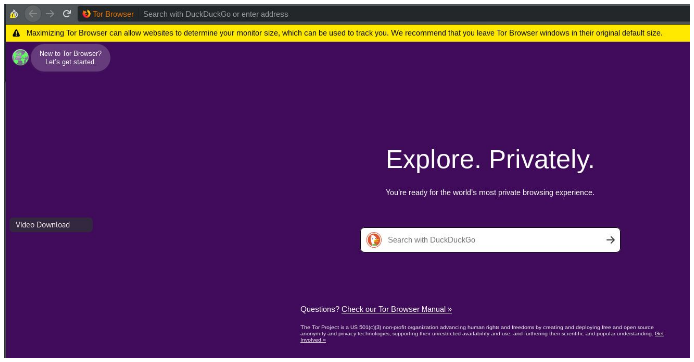
- start a new project
- or resume a partial download

Hyperlinks are given to see the full size photos.

Browsers

In the Buscador's *Browsers* section, there are five different browsers to choose from: Chrome Incognito, Cycle Docker, Firefox, Google Chrome and Tor Browser. Most of these browsers are self explanatory such as Google Chrome, Firefox, and Chrome Incognito (which is Google Chrome locked into its Incognito mode). Tor Browser is the most popular browser to reach the dark web. Tor searches with DuckDuckGo, which is a search engine that doesn't track the user. Tor is used to travel to many thousands of websites that are not accessible to browsers used for the clear web. Prior to its takedown by law enforcement, the most notorious website on the dark web was the market for illicit goods known as, "The Silk Road." While the anonymity provided by the peer-to-peer connections of the dark web benefit some legitimate, benevolent users or others who employ the dark web due to privacy concerns, there are many places in the dark web that are definitely scary. My experience is that Tor is a dangerous web browser if used without care. When first opening it, a message to users reads, "Maximizing Tor Browser can allow websites to determine your monitor size, which can be used to track you." (Well, isn't that pleasant!) Cycle Docker is an anonymization tool used to change the user's IP address while using the Tor Browser. The clear web, more commonly used browsers in Buscador are equipped with multiple add-ons that benefit personal privacy and have OSINT value. Some of these add-ons include: SpiderFoot, the Wayback Machine, DuckDuckGo browser, YTReverse, and more.




Tor Browser   Search with DuckDuckGo or enter address

⚠ Maximizing Tor Browser can allow websites to determine your monitor size, which can be used to track you. We recommend that you leave Tor Browser windows in their original default size.

New to Tor Browser?
Let's get started.

Video Download

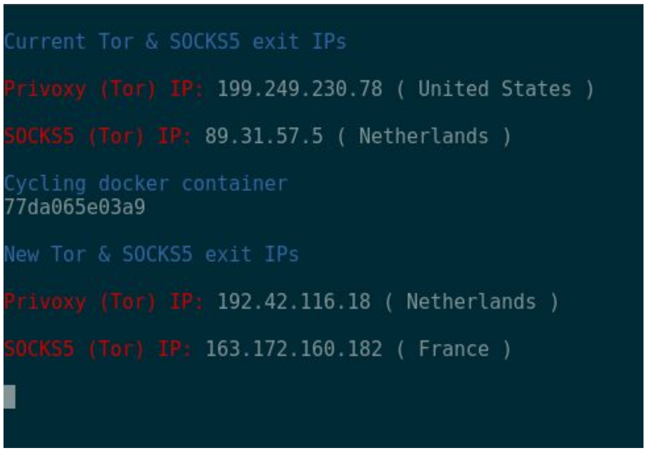
Explore. Privately.

You're ready for the world's most private browsing experience.

Search with DuckDuckGo →

Questions? Check our Tor Browser Manual »

The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »


```
Current Tor & SOCKS5 exit IPs

Privoxy (Tor) IP: 199.249.230.78 ( United States )

SOCKS5 (Tor) IP: 89.31.57.5 ( Netherlands )

Cycling docker container
77da065e03a9

New Tor & SOCKS5 exit IPs

Privoxy (Tor) IP: 192.42.116.18 ( Netherlands )

SOCKS5 (Tor) IP: 163.172.160.182 ( France )
```

Hyperlinks are given to see the full size photos.

In my opinion, Buscador is a super useful tool for OSINT. The virtual machine comes fully loaded with many valuable, diverse investigative tools ranging from analysis of a target's Twitter feed to searches based on a license plate. Overall, Buscador is an amazing tool, easy to understand, and capable of conducting deep, targeted searches.

Hyperlinks are given to see the full size photos.