[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@3f3109268df64064932814690d6161c2?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

ref <https://geekflare.com/osint-tools/>

**8 Popular Open Source Intelligence Tools for Penetration Testing**

By [ANJANEYULU NAINI](https://geekflare.com/author/anjaneyulu/)on May 26, 2021

Posted in

* [Security](https://geekflare.com/category/security/)

Geekflare is supported by our audience. We may earn affiliate commissions from buying links on this site.

The eye-catching view of different **Open Source Intelligence** (OSINT) tools that are available in the market.

In our daily lives, we search for a lot of information on the internet. If we don’t find the expected results, we usually quit!

But have you ever imagined what lies in that hundreds of page results? “Information”!

This can be possible only by using different tools. Tools play a significant role in searching for information but, without knowing the importance and usage of tools, it will not be helpful for the users. Before getting started with the tools, let’s have a clear idea about [OSINT](https://click.linksynergy.com/deeplink?id=jf7w44yEft4&mid=39197&murl=https%3A%2F%2Fwww.udemy.com%2Fosint-open-source-intelligence%2F).

**What is Open Source Intelligence?**

[Open Source Intelligence](https://en.wikipedia.org/wiki/Open-source_intelligence), in short, called OSINT, refers to the collection of information from public sources to use it in the context of intelligence. As of today, we are living in the “world of the internet” its impact on our lives will have both pros and cons.

The advantages of using the internet are, provides lots of information and easily accessible by everyone. Whereas, the disadvantages are misusing the information and spending a lot of time on it.

Now, here comes the existence of OSINT tools which are mainly used to collect and correlate information on the web. Information can be available in various forms; it can be text format, file, image, and so on. According to the [CSR Report for Congress](https://fas.org/sgp/crs/intel/RL34270.pdf), it has been said that Open Source Intelligence has been produced from the public information that is correctly disseminated, collected, and exploited effectively. And makes this information available for the users to address a specific intelligence requirement.

**Why we require OSINT tools?**

Let us consider one situation or scenario in which we need to find information related to some topics on the web. For this you need first to search and do analysis till you get the exact results, this consumes a lot of time. This is the main reason why we need intelligence tools because the process mentioned above can be done within seconds using these tools.

We even can run multiple tools to collect all the information related to the target, which can be correlated and used later.

So let’s deep dive into some of the best OSINT tools.

**Shodan**

Google is the most used search engine for all, whereas [Shodan](https://www.shodan.io/) is a fantastic and goldmine search engine for hackers to see exposed assets.

When compared to other search engines, Shodan provides you the results that make more sense and related to security professionals. It mainly includes information related to assets that are being connected to the network. The devices may vary from laptops, traffic signals, computers, and various other IoT devices. This open-source tool mainly helps the security analyst in identifying the target and test it for different vulnerabilities, passwords, services, ports, and so on.



Moreover, it provides users with topmost flexible searches by the community.

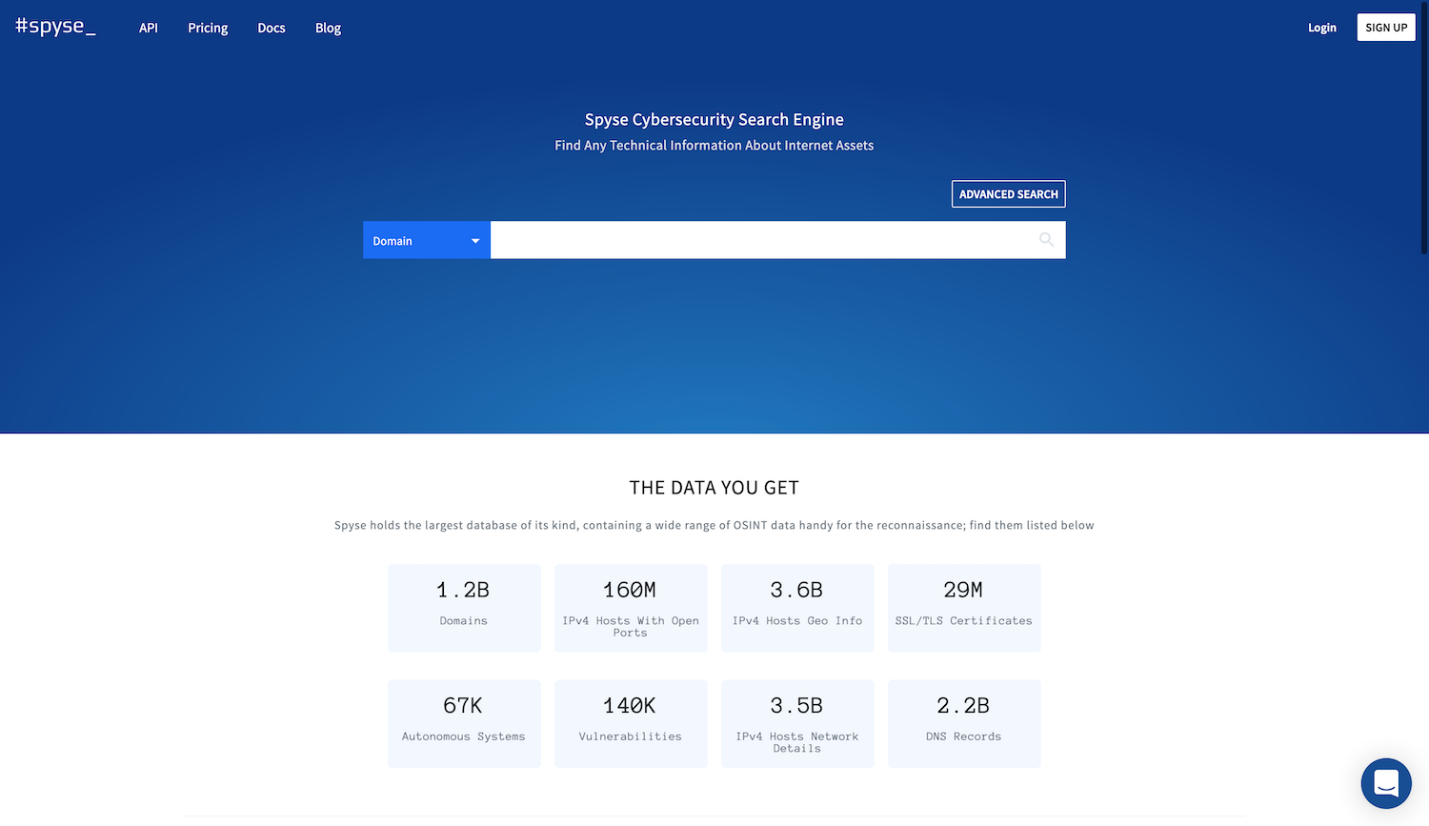
For example, let us consider the situation in which the single user can see the connected netcams, webcams, traffic lights, and so on. We will have a look at some of the use cases from Shodan:

* Testing “default Passwords”
* Assets with VNC viewer
* Using the RDP port open to testing the available assets

**Spyse**

[Spyse](https://spyse.com/) is a cybersecurity search engine for obtaining technical information that is commonly used by hackers in cyber reconnaissance.

Spyse provides vast data for exploring the target through different entry points. The user can start with one domain and expand the investigation radius by checking different types of target-related data such as Vulnerabilities, IPs, ASNs, DNS records, Domains on the same IP, Domains with the same MX/NS, and much more.



All of this is possible thanks to a huge database with stored and interlinked data which users can access instantly:

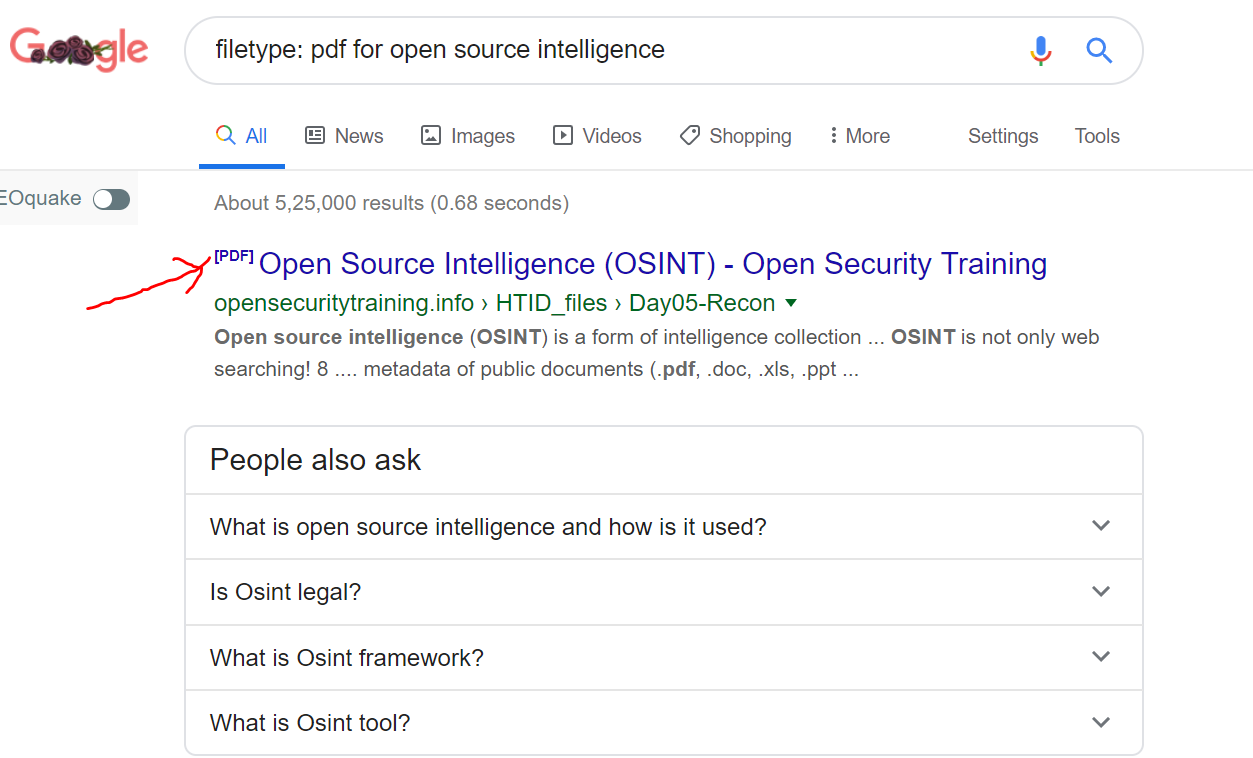
* Domains – 1.2 B
* IP Hosts with Ports –  160M
* SSL/TLS –  29M
* IPv4 Hosts- 3.6B
* Autonomous Systems – 67k
* Vulnerabilities – 140k
* DNS records – 2.2B

Moreover, the search engine provides users with unique search opportunities that simplify the process of obtaining the necessary data. Its distinctive characteristic is the possibility to apply 5 different search parameters for a precise and detailed search.

**Google Dorks**

[Google Dorks](https://en.wikipedia.org/wiki/Google_hacking) have come into existence since 2002, and it gives effective results with excellent performance. This query-based open-source intelligence tool is mainly developed and created to help users in targeting the index or search results appropriately and effectively.

Google Dorks provides a flexible way of searching for information by using of some operators, and perhaps it is also called Google Hacking. These operators make the search easier to extract information. Below are some of the operators or indexing options provided by Google Docker, and they are:

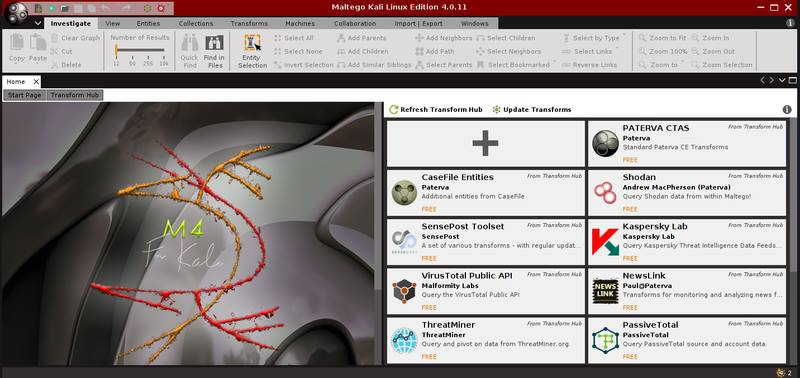


* **Filetype:** This operator is mainly used to find the file types or to search for a particular string
* **Intext:** This indexing option is used to search for a specific text on a specific page.
* **Ext:** This is used to search for a specific extension in a file.
* **Inurl:** Used to search for the specific string or word in the URL
* **Intitle:** To search for the title or words mentioned above in the URL

**Maltego**

[Maltego](https://www.paterva.com/index.php) is designed and developed by Paterva, and it is one of the inbuilt tools in Kali Linux. This open-source intelligence tool is mainly used to perform a significant exploration against various targets with the help of several in-built transforms (and also provides the capability to write custom ones).

A programming language that you use in Maltego is written in Java and displays as a built-in pre-packaged in the Kali Linux. To use this tool, registration is necessary, the registration is free of cost, and the user should register on paterva site. Once the registration process is done, then the users can use this tool to create and develop effective digital footprints of the particular target on the internet.



The expected results may happen to IP conversion, AS number is identified, Netblock is also identified, even the phrases and locations are also identified. These are all the icons in Maltego that provides a detailed view and information about all the icons.

You can even know more information about the target by digging more into the process. Finally, I can say that it is an excellent tool to track the footprints of each and every single entity over the internet. Maltego is available across all popular operating systems.

**TheHarvester**

[TheHarvester](https://github.com/laramies/theHarvester) is an amazing tool for finding emails, subdomains, IPs, etc. from various public data.

Below example to find the subdomains using DNSdumpster.

[root@geekflare theHarvester]# python theHarvester.py -d geekflare.com -v -b dnsdumpster   
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* \* \_ \_ \_ \* \* | |\_| |\_\_ \_\_\_ /\ /\\_\_ \_ \_ \_\_\_\_ \_\_\_\_\_ \_\_\_| |\_ \_\_\_ \_ \_\_ \* \* | \_\_| \_ \ / \_ \ / /\_/ / \_` | '\_\_\ \ / / \_ \/ \_\_| \_\_/ \_ \ '\_\_| \* \* | |\_| | | | \_\_/ / \_\_ / (\_| | | \ V / \_\_/\\_\_ \ || \_\_/ | \* \* \\_\_|\_| |\_|\\_\_\_| \/ /\_/ \\_\_,\_|\_| \\_/ \\_\_\_||\_\_\_/\\_\_\\_\_\_|\_| \* \* \* \* theHarvester 3.1.0.dev1 \* \* Coded by Christian Martorella \* \* Edge-Security Research \* \* cmartorella@edge-security.com \* \* \* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* [\*] Target: geekflare.com [\*] Searching DNSdumpster. [\*] No IPs found.   
[\*] No emails found.   
[\*] Hosts found: 3 --------------------- lab.geekflare.com:104.25.134.107 tools.geekflare.com:104.25.134.107 www.geekflare.com:104.25.134.107   
[\*] Virtual hosts: ------------------ [root@geekflare theHarvester]#

Copy

TheHarvester is also available on Kali Linux. You can check the [Kali Linux installation guide](https://geekflare.com/kali-linux-installation-guide-vmware/) if you need it.

BTW, there are more tools to [find subdomains](https://geekflare.com/find-subdomains/).

**Recon-Ng**

[Recon-ng](https://github.com/lanmaster53/recon-ng) is an effective tool to perform reconnaissance on the target.

The entire power of this tool lies completely in the modular approach. The power of modular tools can be understood for those used Metasploit. Recon-ng has various built-in modules that are used to target mainly while extracting information as per user needs. We can use the Recon-ng modules just by adding the domains in the workspace.

Workspaces are mainly created to carry out the operations inside it. The users will be redirected to the workspace as soon as it is created. Inside the workspace, the domain can be particularly specified using add domain <domainname>. Modules of Recon-ng are used to fetch information about the specific domain after they (domains) are added into the recon-ng.

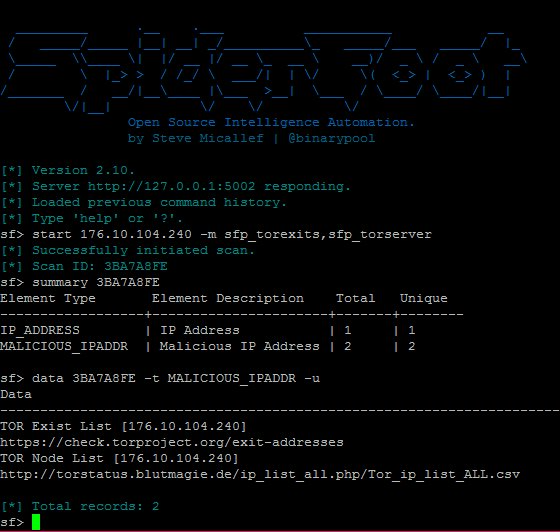
Some of the excellent modules, such as google-site-web and bing-domain-web, are used to find further domains related to the first initial target domain. The result of these domains will be all the indexed domains to the search engines. Another catchy module is bing\_linkedin\_cache which is mainly used to fetch the details of the email addresses related to the domain. This module can also be used to leverage in performing social engineering.

Moreover, using other modules, we can get fetch the extra or additional information about targets. So finally, this open-source intelligence tool is a fantastic tool and also must be included in the toolkit of researchers.

**SpiderFoot**

[SpiderFoot](https://www.spiderfoot.net/) is an open-source reconnaissance tool available for Linux and Windows. It has developed using Python language with high configuration and runs virtually on any platform. It integrates with easy and interactive GUI with a powerful command-line interface.

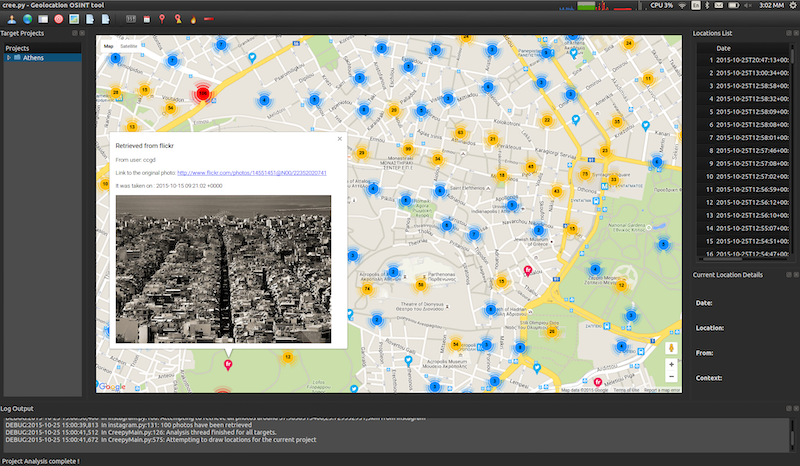
It has automatically enabled us to use queries over 100+ OSINT sources to grab the intelligence on emails, names, IP addresses, domain names, etc. It collects an extensive range of information about a target, such as netblocks, e-mails, web servers, and many more. Using Spiderfoot, you may able to target as per your requirement because it will collect the data by understanding how they are related to each other.



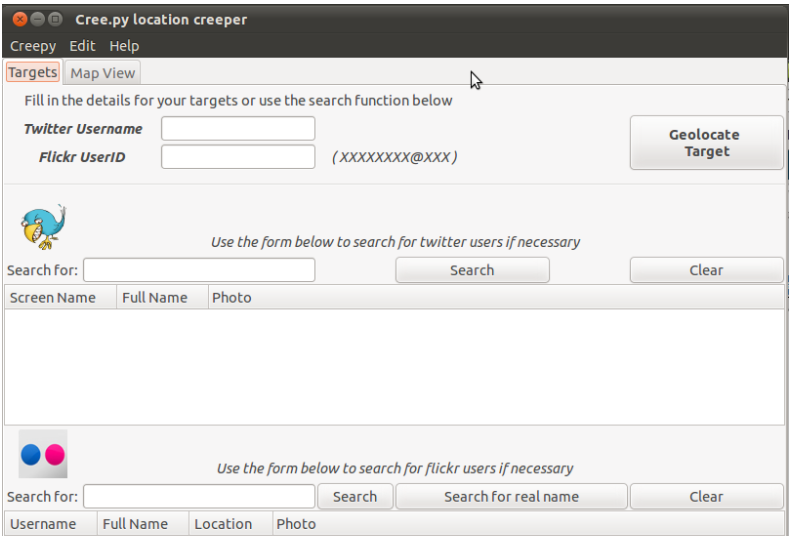
The data collected from a SpiderFoot will provide a wide range of information about your specific target. It provides clear insights about possible hacking threats which are leads to vulnerabilities, data leaks, and other vital information. So these insights will help to leverage the [penetration test](https://geekflare.com/web-penetration-testing-tools/) and enhance the threat intelligence to alert before it gets attacked or stolen.

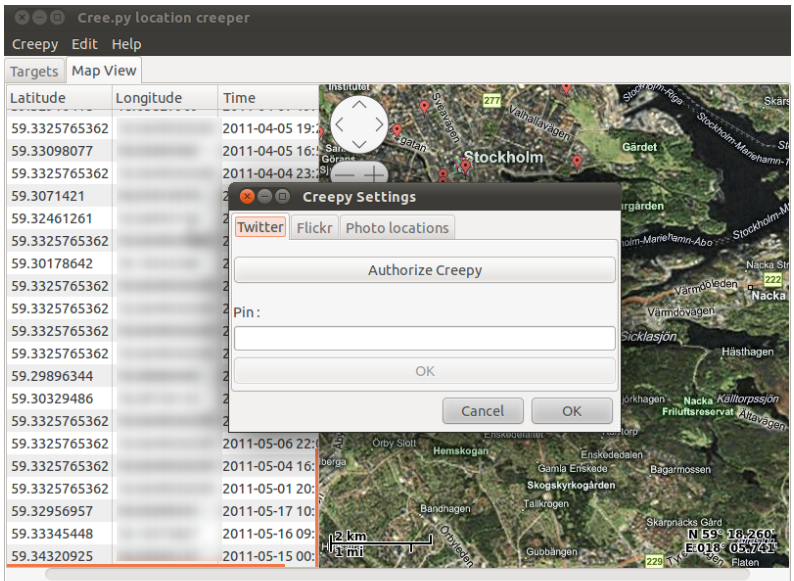
**Creepy**

[Creepy](https://www.geocreepy.com/) is an open-source Geolocation intelligence tool. It collects information about Geolocation by using various social networking platforms and image hosting services that are already published somewhere else. Creepy presents the reports on the map, using a search filter based on the exact location and date. These reports are available in CSV or KML format to export for additional analysis.



The main functionality in Creepy is divided into two main tabs viz. ‘Targets’ and ‘map view’ tabs.





Creepy is written in python and also comes with a packaged binary for Linux distributions such as Debian, Backtrack, Ubuntu, and Microsoft windows.