

What is Shodan?

Shodan is “the world’s first search engine for internet-connected devices.”¹ But what exactly does this mean?

Most search engines are text indexes, meaning they allow search for content based on keywords. However, the task of scanning, indexing the ports and services running, and then searching for internet-connected devices at the scope and scale of the internet has been largely impossible to do.

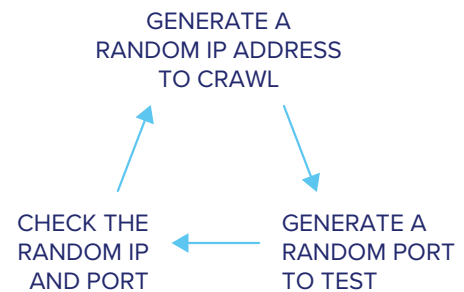
With Shodan, it is now possible to identify nearly any internet-connected device, such as industrial control systems running specific software, Internet-of-Things devices like smart TVs, FTP servers with sensitive information, and even Very Small Aperture Terminals (VSATs) on naval vessels.

How Shodan Works

Shodan maintains servers across the globe that scan the internet-connected devices and harvest the banner of whatever is running on the server.

The diagram shows how these servers crawl.

These internet-connected devices return different banners depending on the different service running on it.




Example Search Returns

Please see two examples below — one for an IP camera, and the other for an FTP server (FTP runs on port 21).

Basic Shodan Searches/Filters

Document Error: Unauthorized

62.112.117.205
0AO MGTS
 Added on 2019-05-07 10:56:51 GMT
 Russian Federation, Odintsovo
 Technologies: IIS;confidence:50 

```

HTTP/1.1 401 Unauthorized
Server: Cam-Webs
Date: Tue May 7 13:20:55 2019
WWW-Authenticate: Basic realm="Megapixel_IP_Camera"
Pragma: no-cache
Cache-Control: no-cache
Content-Type: text/html
  
```

188.225.26.71

vds-olgafirsova.timeweb.ru
hosting & vds
 Added on 2019-05-28 17:02:17 GMT
 Russian Federation

```

220 (vsFTPD 3.0.2)
230 Login successful.
214-The following commands are recognized.
ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MKD
MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR
RNT0 SITE SIZE SMNT STAT STOR STOJ STRU SYST TYPE USER XCUP XCWD XMKD...
  
```

¹ <https://github.com/polarityio/shodan>

Shodan allows for advanced search using filters. Filters are entered in a simple format: a filter, a colon, and the search value, with no spaces between these three components.

Filter format	<code>filtername:value</code>
Filter example	<code>City:Moscow</code>

In searching for a value that includes a space, double quotes must be used.

Filter example	<code>City:"Saint Petersburg"</code>
----------------	--------------------------------------

Examples of Shodan's most useful geographic filters:

Country using 2 letter geocode	<code>country:XX</code>
City using city name	<code>city:cityname</code>
Geographic coordinates in a bounding box	<code>geo:top-left-lat,top-left-long, top-right-lat,top-right-long</code>
Region	<code>region:region-name-or-state</code>

These filters are useful when attempting to identify something of interest in a specific AOR.

For example, a search for `webcam City:Incirlik` would find webcams, with some hopefully located near Incirlik Air Base.

Examples of software-focused filters:

Firewall port	<code>port:XX</code>
Product name	<code>product:XX</code>
Product version	<code>version:XX</code>
Product vulnerability CVE	<code>vuln:XX</code>

These filters are useful when searching for a particular technology, like a database, a file server, or vulnerable software.

For example, a search for `port:21 country:"RU" "login successful"` would find file transfer protocol (FTP) servers in Russia that do not require logins. This could yield valuable unsecured information if found in a location of interest, or can be used as a non-attributable temporary data transfer point.



CONNECT WITH US

+1 877-659-6535

www.Authentic8.com



PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.