**Shodan.io**

[Shodan](https://www.shodan.io/) is a search engine used to source internet-connected devices or servers, webcams, routers, and smart devices, collectively known as IoT (Internet of Things) devices.

Like most search engines, the database can be searched using keywords and filters to source server information, vulnerable services, and even the location of internet-connected devices. Other information such as the current users of a system and system service banners can also be obtained. Such devices can be located in any type of system, including home networks, corporate networks, surveillance networks, and industrial control systems (ICS).

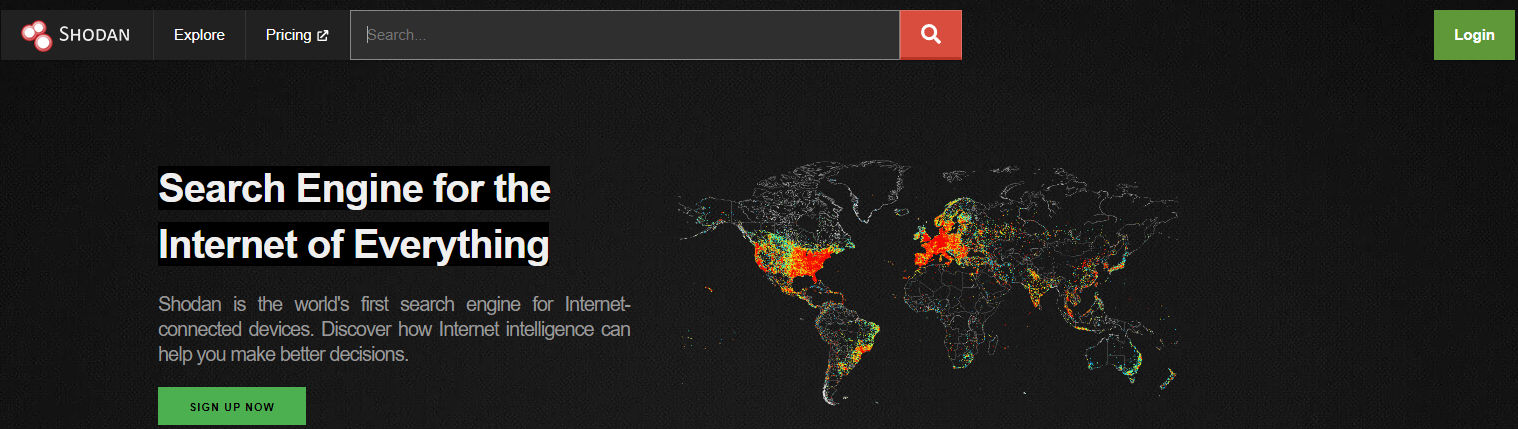
### **How Shodan Finds Information?**

1. **Port Scanning:**
   * Shodan uses port scanning to identify devices connected to the internet. It scans various IP addresses and checks open ports to determine the services running on those devices.
   * Commonly scanned ports include those used by HTTP, HTTPS, FTP, SSH, and other protocols.
2. **Banner Grabbing:**
   * Once Shodan identifies an open port, it performs a process called banner grabbing. This involves sending a request to the service running on the port and capturing the response.
   * The response, or "banner," often contains information about the software version, device type, operating system, and other metadata.
3. **Data Indexing:**
   * The collected data is then indexed and stored in Shodan’s database. Users can search this database using various filters and keywords to find specific types of devices or information.

The **legality** of using Shodan is also influenced by the **intent** and manner in which it is used. Security professionals and researchers use Shodan to identify and fix vulnerabilities, which is a legitimate and beneficial activity.

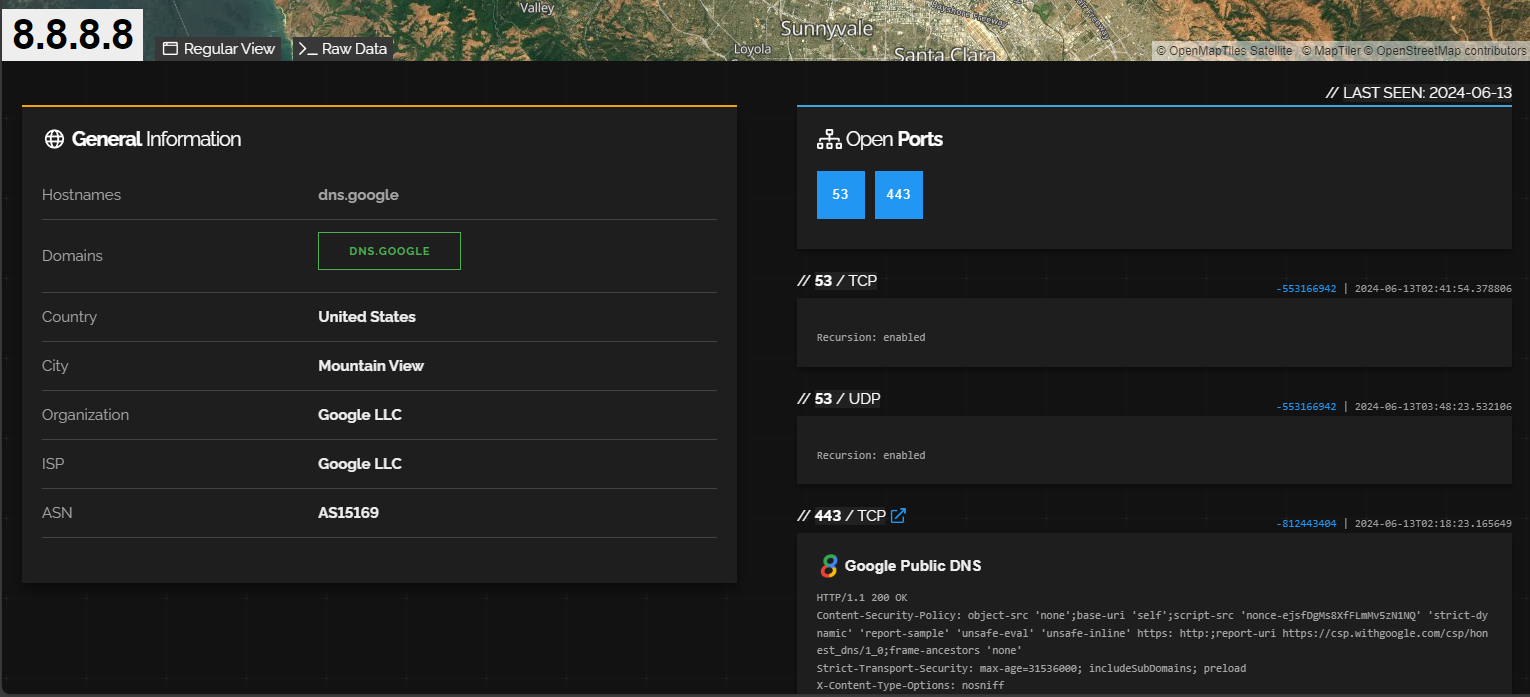
Malicious use of Shodan, such as using the information to launch attacks or unauthorized intrusions, would likely violate the **CFAA(Crime Fraud and Abuse Act).** Violating the CFAA can result in criminal charges, including fines and imprisonment. The severity of the penalties depends on the nature and impact of the offense.

**How to use Shodan?**

****

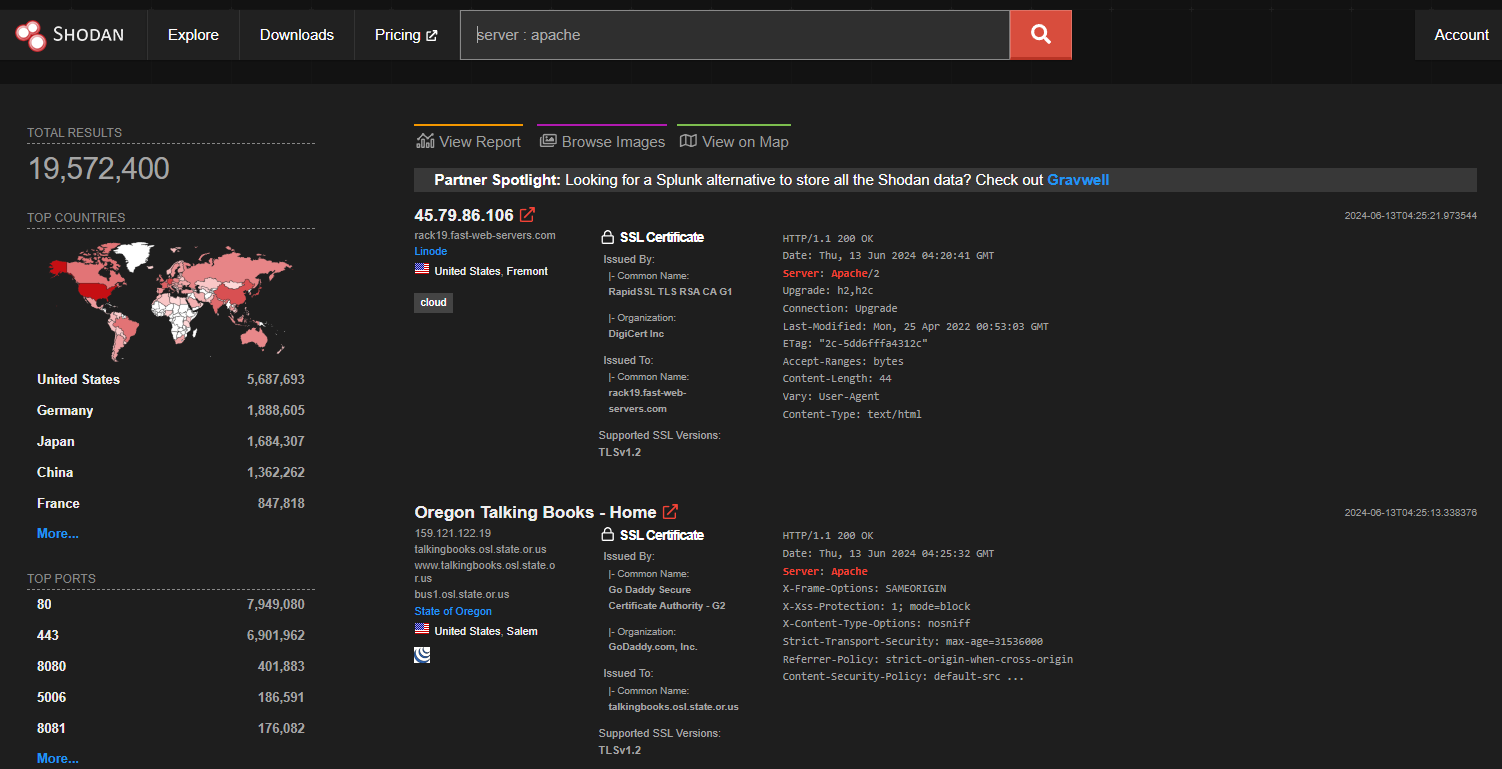
Using the search bar, enter your search query like you would on any search engine to see what Shodan has found. Search for an IP address to see the Shodan results for a specific host.

For example, searching for **8.8.8.8** takes you directly to the host details page for that IP address:



These results contain information on which organization is hosting the IP address, where the server is located, and details on any open ports and running services found on the host. In this example, 8.8.8.8 is an IP address used by **Google LLC**, is based in the United States, and has two open ports: **53 and 443.**

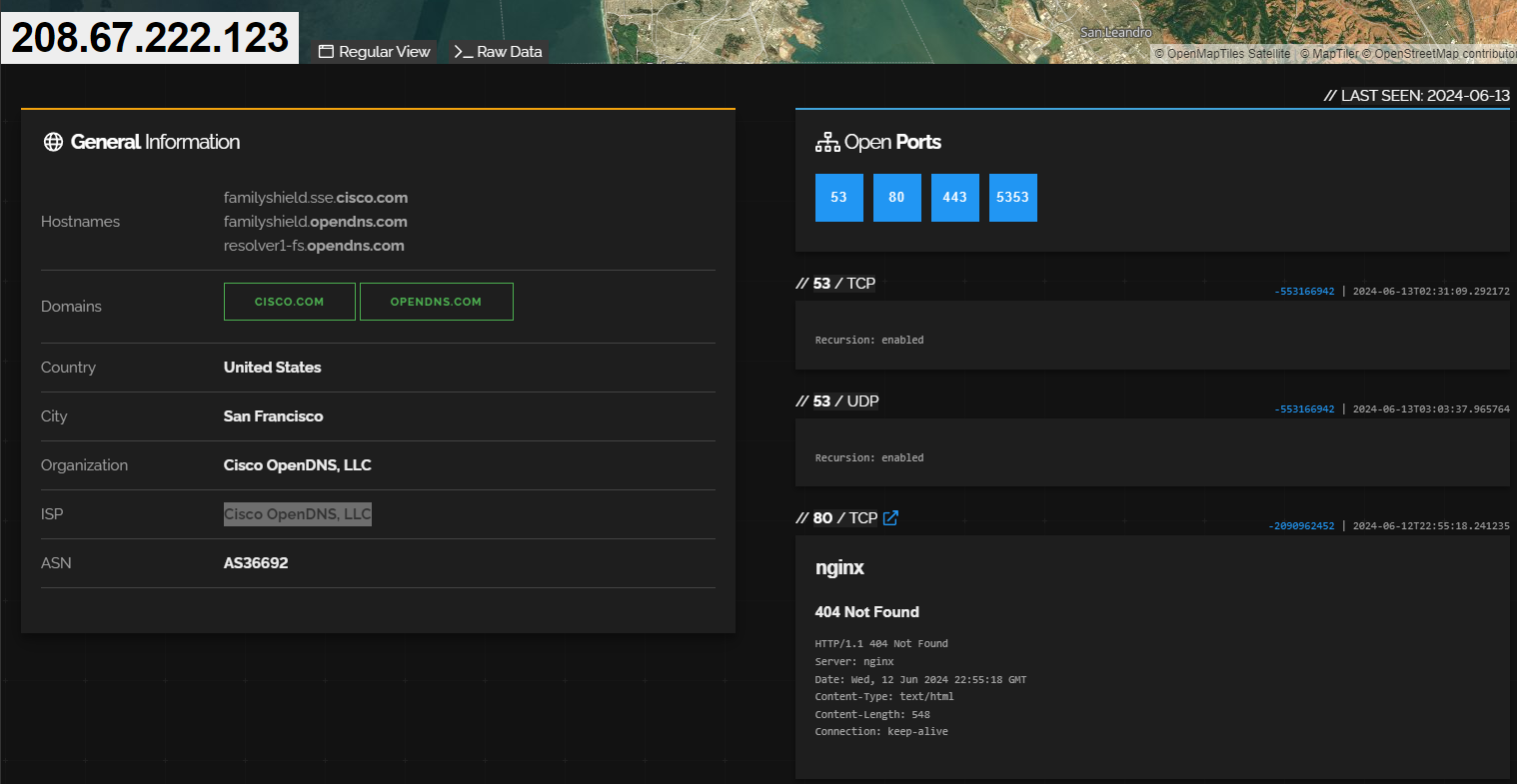
Shodan also supports searching more generically, and you can enter text queries into the search bar. For example, searching for the string **Server: Apache** shows every result that contains this string – just like a typical Google search! Clicking on any IP address in the search results will take you to the host details page for that specific IP address.



In this example, most results were from hosts based in the United States, followed by Germany. The most common open port in these results is port 80, followed by port 443.

**How to find information on target IP (208.67.222.123)?**

Search given ip address on shodan.



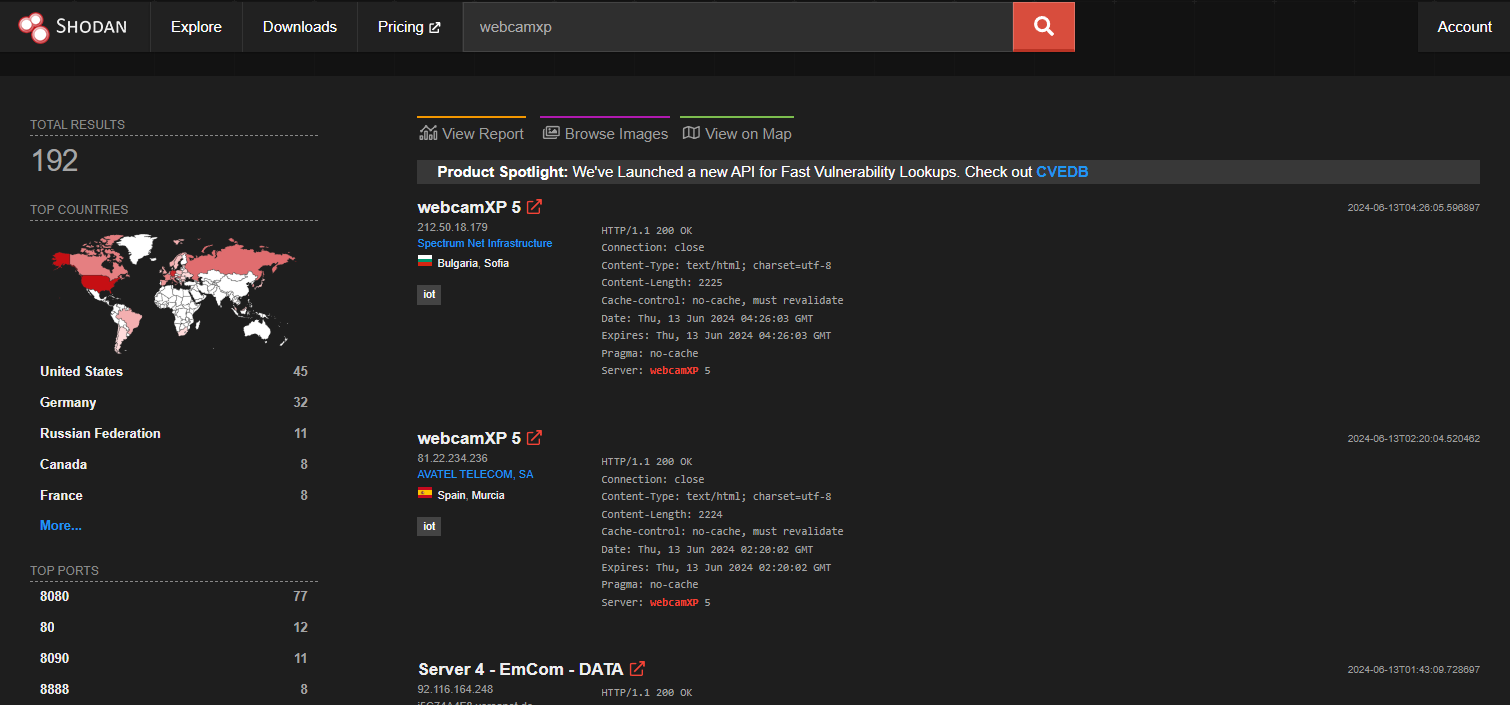
Now we can get the following info from this :

1. ISP hosting this IP address is **Cisco OpenDNS, LLC**
2. Ports that are open **53, 80, 443, 5353**

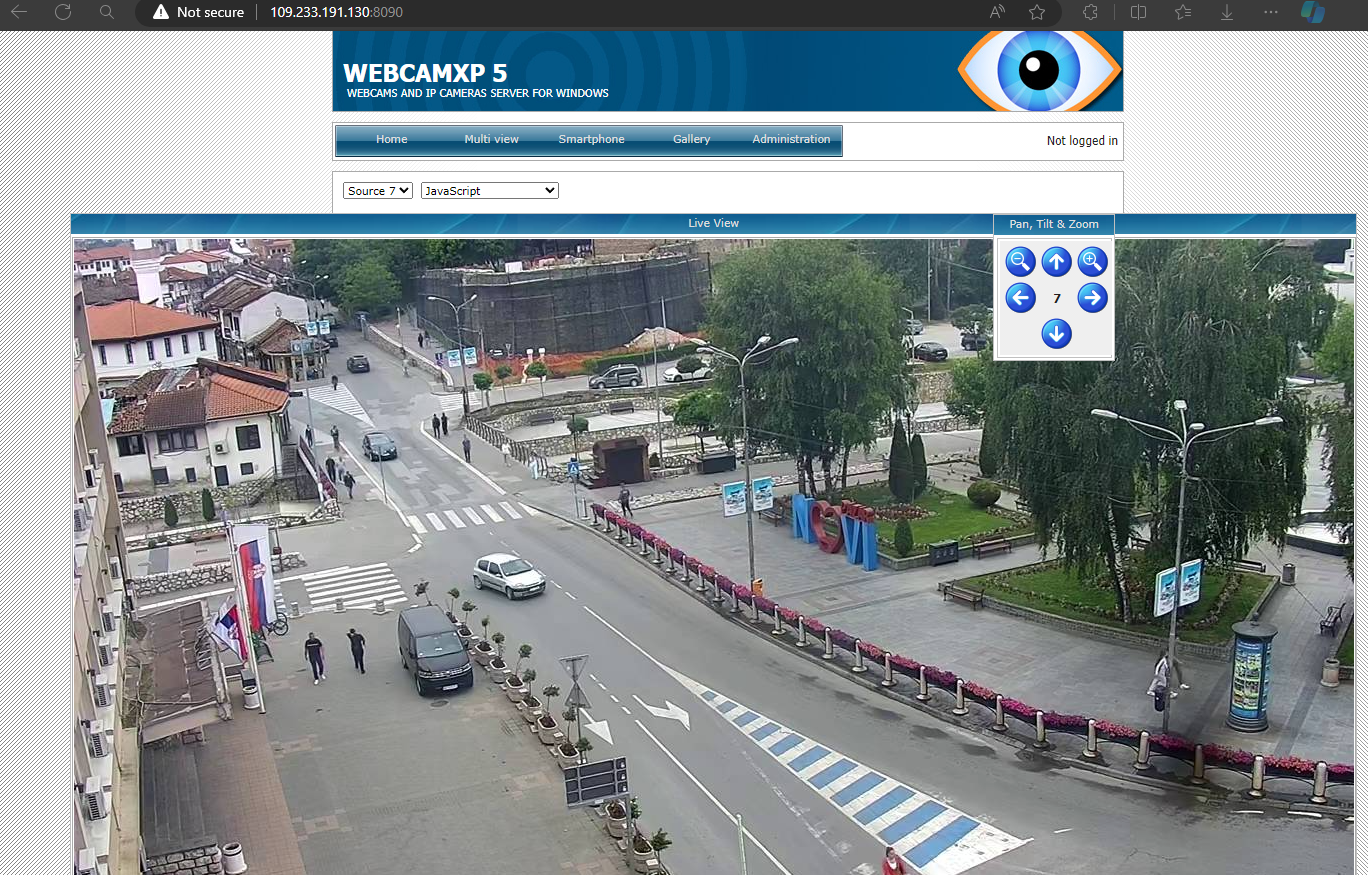
**How to search for accessible webcams ?**

There are various methods to locate webcams on Shodan. A common approach is to search using the name of the webcam's manufacturer or the webcam server software. Shodan indexes information based on the banner, not the content, so if the manufacturer's name appears in the banner, it can be easily found. If not, the search might not yield results.

One particularly effective search term is "**webcamxp**," a software for webcams and network cameras designed for older Windows systems. A search query for "webcamxp" on the Shodan platform may yield numerous results pointing to web-connected surveillance devices worldwide.

****

Using a hit and trial method you will be able to find an unprotected camera.



When exploring the search results on Shodan for such devices, it's important to understand that while some may lack proper security measures, a significant portion will have authentication systems in place to restrict unauthorized access. To attempt to gain access without too much effort, try the **default username and password** for the security camera hardware or software.

Some of the cameras like **ACTi** have admin/123456 or **Axis** have root/pass as default username and passwords.

Note that there is no guarantee that any of these will work, but sometimes admin simply leave the default settings in place.

**Some Additional dorks of Shodan which you can try in the search bar are:**

1. **To find surveillance cams**: Server: uc-httpd 1.0.0
2. **To find some vulnerable Devices**:
   1. XZERES Wind Turbines: title:"xzeres wind"
   2. MikroTik Routers: port:8291 os:"MikroTik RouterOS 6.45.9"
   3. Minecraft Servers: "Minecraft Server" "protocol 340" port:25565
   4. Smart TVs: "Chromecast:" port:8008
3. **To find some vulnerable Services**:
4. EternalBlue SMB RCE: os: Windows 10 Home 19041
5. Anonymous FTP Login : "230 User anonymous"
6. No password for Telnet Access: port:23 console gateway

To conclude, Shodan is a powerful search engine tool that indexes internet-connected devices, revealing information about their configurations and vulnerabilities.