**Search Query Fundamentals**

To get the most out of Shodan it's important to understand the search query syntax. This article will cover the basics to help get you started; if you're already familiar with search filters then please check out the Mastery series of articles instead.

Before we delve into the actual search query syntax, lets take a look at what you'll be searching in Shodan:

**The Banner**

Devices run services and those services are what Shodan collects information about. For example, websites are hosted on devices that run a web service and Shodan would gather information by speaking with that web service. The information for each service is stored in an object called the **banner**. It is the fundamental unit of data that Shodan gathers and what you'll be searching for. A simplified banner looks like the following:

{

"data": "Moxa Nport Device

Status: Authentication disabled

Name: NP5232I\_4728

MAC: 00:90:e8:47:10:2d",

"ip\_str": "46.252.132.235",

"port": 4800,

"org": "Starhub Mobile",

"location": {

"country\_code": "SG"

}

}

The above banner has 5 **properties**. Note that a real banner will contain many more properties and detailed information about the service. Each **property** stores a different type of information about the service:

* **data**: the main response from the service itself
* **ip\_str**: IP address of the device
* **port**: port number of the service
* **org**: the organization that owns this IP space
* **location.country\_code**: the country where the device is located

By default, only the **data** property is searched by Shodan. The content of the **data** property can vary greatly depending on the type of service. For example, here is a typical HTTP banner:

HTTP/1.1 200 OK

Server: nginx/1.1.19

Date: Sat, 03 Oct 2015 06:09:24 GMT

Content-Type: text/html; charset=utf-8

Content-Length: 6466

Connection: keep-alive

The above banner shows that the device is running the **nginx** web server software with a version of **1.1.19**. To show how different the banners can look like, here is a banner for the Siemens S7 industrial control system protocol:

Copyright: Original Siemens Equipment

PLC name: S7\_Turbine

Module type: CPU 313C

Unknown (129): Boot Loader A

Module: 6ES7 313-5BG04-0AB0 v.0.3

Basic Firmware: v.3.3.8

Module name: CPU 313C

Serial number of module: S Q-D9U083642013

Plant identification:

Basic Hardware: 6ES7 313-5BG04-0AB0 v.0.3

The Siemens S7 protocol returns a completely different banner, this time providing information about the firmware, its serial number and a lot of detailed data to describe the device.

You have to decide what type of service you're interested in when searching in Shodan because the banners vary greatly.

**Search Syntax**

Lets look again at the simplified banner for Moxa devices:

{

"data": "Moxa Nport Device

Status: Authentication disabled

Name: NP5232I\_4728

MAC: 00:90:e8:47:10:2d",

"ip\_str": "46.252.132.235",

"port": 4800,

"org": "Starhub Mobile",

"location": {

"country\_code": "SG"

}

}

If you wanted to find more of these [**Moxa Nport**](https://www.shodan.io/search?q=Moxa%20Nport) devices then a simple search query would be:

Moxa Nport

However, if you wanted to search for devices on the **Starhub Mobile** network then a simple search for [**"Starhub Mobile"**](https://www.shodan.io/search?q=Starhub%20Mobile) won't return the expected results. This is because by default, Shodan only searches the **data** property!

So how do you search those other properties on the banner? How would you ask Shodan to only show Moxa Nport devices located in Singapore?

**Search Filters**

Search **filters** are special keywords to tell Shodan that you wish to search specific properties. They take the format of:

filtername:value

Note that there is no space in between the filtername and its value. Using the above example, if you wanted to find [**devices located in Singapore**](https://www.shodan.io/search?q=country:SG) then you would use the **country** search filter which accepts as an argument a 2-letter country code:

country:SG

If the value you're trying to search contains spaces then you need to wrap the value in quotes. The following search query shows devices that are located on the [**Starhub Mobile**](https://www.shodan.io/search?q=org:%22Starhub%20Mobile%22) network:

org:"Starhub Mobile"

Filters can also be combined to narrow down results even further. For example, here is a search query to find devices located on [**Starhub Mobile and located in the city of Singapore**](https://www.shodan.io/search?query=org%3A%22Starhub+Mobile%22+city%3ASingapore):

org:"Starhub Mobile" city:Singapore

**Conclusion**

The reason we created a search interface that requires you to use filters is that we wanted to prevent returning false positives and thereby misleading numbers. For example, if you're searching for **Apache** you should only get results for the Apache web server software and not accidentally see results for the city of **Apache Junction** in the United States.

At this point you should have a basic understanding of the search query syntax and know how to apply filters. For more examples [**explore the shared search queries**](https://www.shodan.io/explore) that other users have submitted to the website.