Shodan資料分析

NASOC 二線工程師 林宜進

E-mail：tjline01@asoc.cc.ntu.edu.tw

日期：2021/12/14

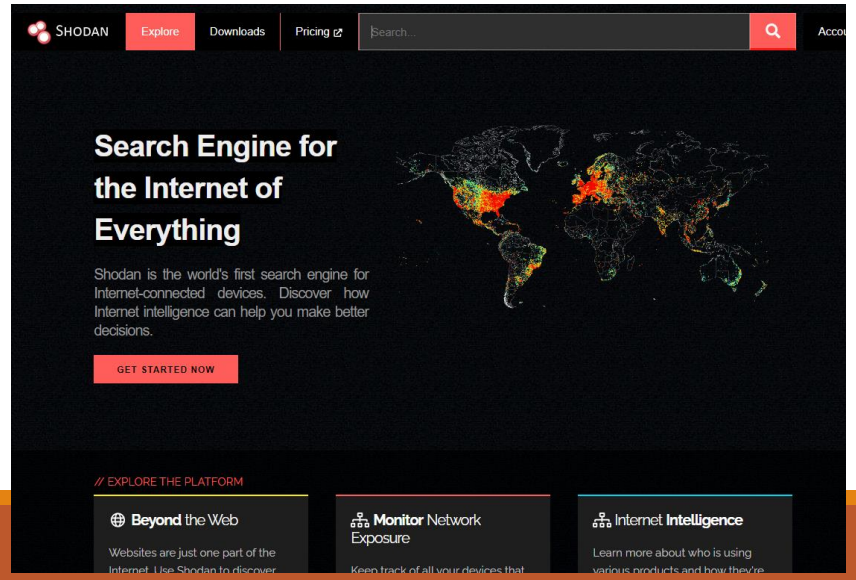
大綱

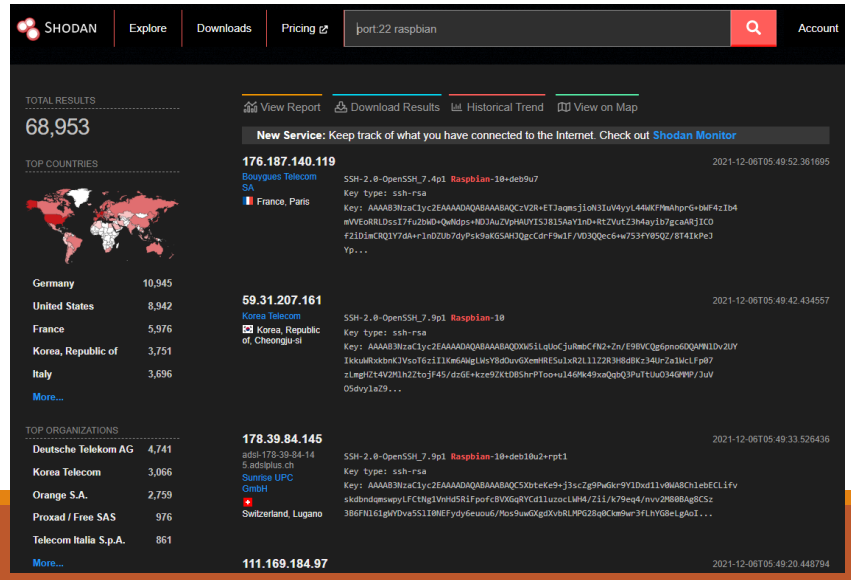
1. Shodan介紹
2. Shodan基本操作
3. 下載Shodan資料
4. 簡易的Shodan資料分析

Shodan介紹

什麼是Shodan?

- Shodan是一個提供網際網路中IoT設備資訊的搜尋引擎
- 透過過濾器(關鍵字)搜尋，可找到特定IoT設備資訊
- 被CNN稱作「網際網路上最危險的搜尋引擎」
- 官方網址： https://www.shodan.io/





CNN
@CNN

"Shodan: The scariest search engine on the Internet" (from @CNNMoney): on.cnn.com/1egSoNY

上午1:37 · 2013年8月3日 · Twitter Web Client

原本縮網址已經無法連結，而原始連結如下：
https://money.cnn.com/2013/04/08/technology/security/shodan/

CNN BUSINESS Markets Tech Media Success Video

The Cybercrime Economy

Shodan: The scariest search engine on the Internet

by David Goldman @DavidGoldmanCNN

April 8, 2013: 1:41 PM ET

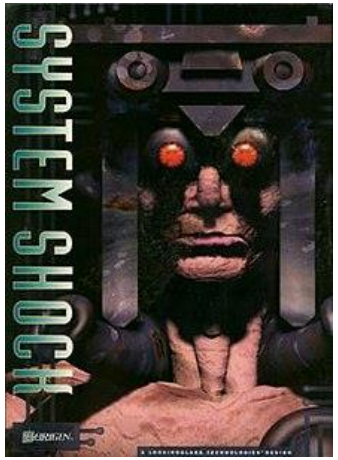
Hacking anything connected to the Internet

"When people don't see stuff on Google, they think no one can find it. That's not true."

That's according to John Matherly, creator of Shodan, the scariest search engine on the Internet.

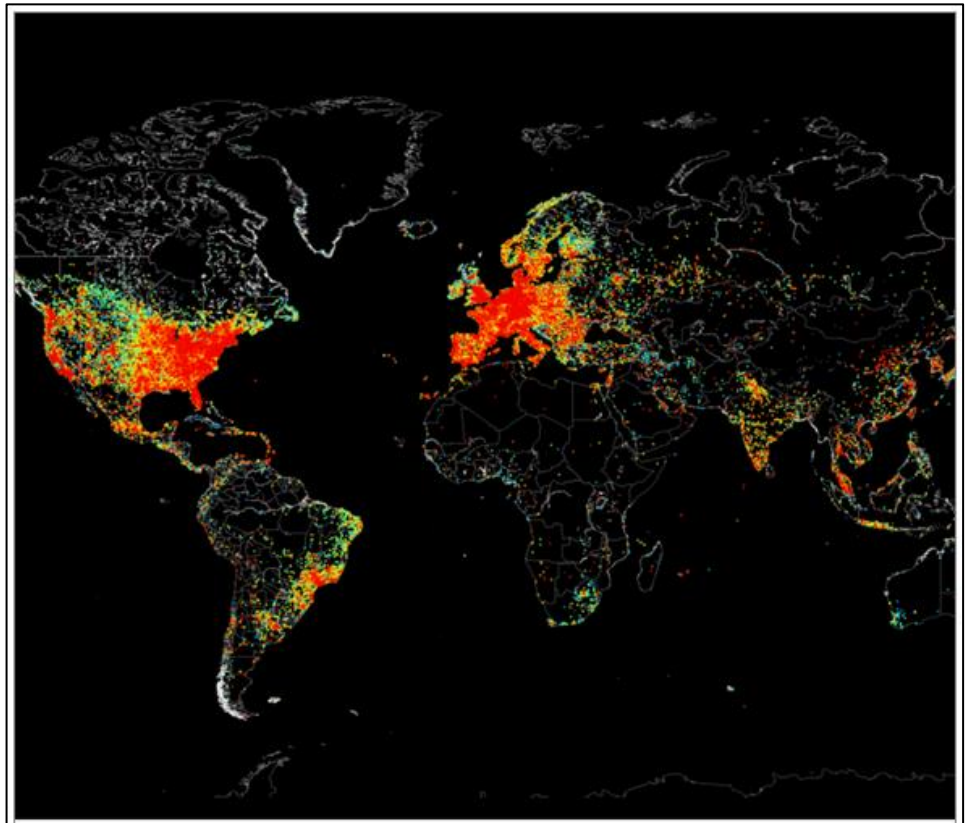
創辦人有關的資訊

- 創辦人為John Matherly，他在2009年建立Shodan搜尋引擎
- 此名稱引用自遊戲「網路奇兵」(System Shock)中，具有邪惡人工智慧的電腦—SHODAN
- 創辦人有發行一本官方電子書「 Complete Guide to Shodan 」



資料來源： https://en.wikipedia.org/wiki/System_Shock

資料來源： https://www.youtube.com/watch?v=n1ChelLmQIc



Complete Guide to Shodan

Collect. Analyze. Visualize. Make Internet Intelligence Work For You.

Complete Guide to Shodan

Collect. Analyze. Visualize. Make Internet Intelligence Work for You.

John Matherly

This book is for sale at http://leanpub.com/shodan

This version was published on 2017-08-23

Leanpub

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once

Contents

Introduction **1**
All About the Data 1
Data Collection 3
SSL In Depth 4
Beyond the Basics 7

Web Interfaces **10**
Search Query Explained 10
Introducing Filters 11
Shodan Search Engine 12
Shodan Maps 18
Shodan Exploits 25
Shodan Images 26
Exercises: Website 28

External Tools **29**
Shodan Command-Line Interface 29
Maltego Add-On 37
Browser Plug-Ins 37
Exercises: Command-Line Interface 38

Developer API **39**
Usage Limits 39
Introducing Facets 40
Getting Started 41
Initialization 41
Search 41
Host Lookup 43
Scanning 43
Real-Time Stream 44
Network Alert 45
Example: Public MongoDB Data 48
Exercises: Shodan API 53

如何使用Shodan(攻擊方)?

- 利用Shodan查詢服務，找出特定IoT設備
- 結合滲透工具、自製攻擊程式做精準打擊

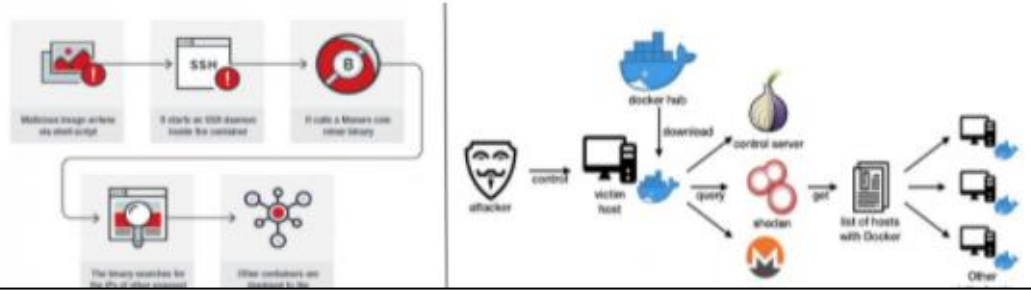
Compromised Docker Hosts Use Shodan to Infect More Victims

By Sergiu Gatlan — May 30, 2019 — 02:46 PM — 0

Hackers are scanning for Docker hosts with exposed APIs to use them for cryptocurrency mining by deploying malicious self-propagating Docker images infected with Monero miners and scripts that make use of Shodan to find other vulnerable targets.

The cryptojacking campaign targeting exposed Docker hosts was unearthed by Trend Micro researchers after a Docker image containing a Monero (XMR) cryptocurrency miner binary was deployed on one of their honeypots.

This type of attack is definitely nothing new seeing that researchers from Imperva discovered a similar campaign abusing the CVE-2019-5736 runc vulnerability to deploy cryptominers during early-March.



資料來源：https://www.bleepingcomputer.com/news/security/compromised-docker-hosts-use-shodan-to-infect-more-victims/

如何使用Shodan(防守方)?

- 當發生CVE漏洞、0-day攻擊時，利用Shodan查詢，找出符合條件的IoT設備
- 研究漏洞發生原因，尋找或自行開發漏洞檢測程式，透過檢測找出存在漏洞的設備，並通知單位盡速修補。

AT&T Reveals Malware Targeting Millions of Routers, IoT Devices

The malware, BotenaGo, has more than 30 different functions.

By Nathaniel Mott Nov. 13, 2021, 12:22 a.m.

AT&T has revealed malware that could affect millions of routers and Internet of Things devices.

The company's Alien Labs threat intelligence unit dubbed the malware BotenaGo because it's written in Go, a programming language that Google designed specifically with networking in mind. It's also capable of creating botnets that function across a variety of device types.

AT&T Alien Labs says BotenaGo can exploit up to 30 different vulnerabilities against its targets. The company used Shodan, a search engine used to look up internet-connected devices, to determine that millions of devices could be affected by at least some of the malware's functions.

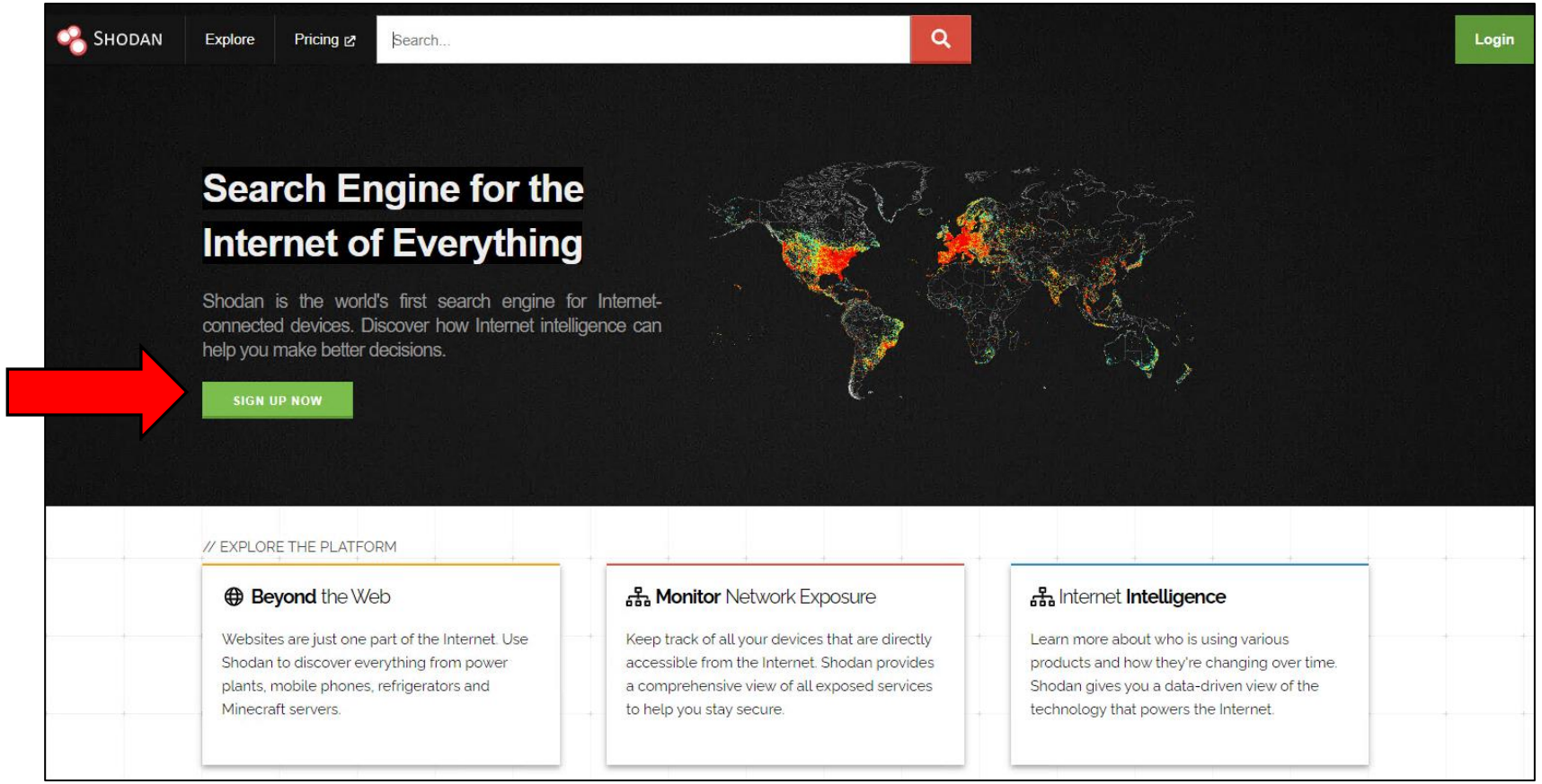
資料來源：https://in.pcmag.com/security/146125/att-reveals-malware-targeting-millions-of-routers-iot-devices

Shodan基本操作

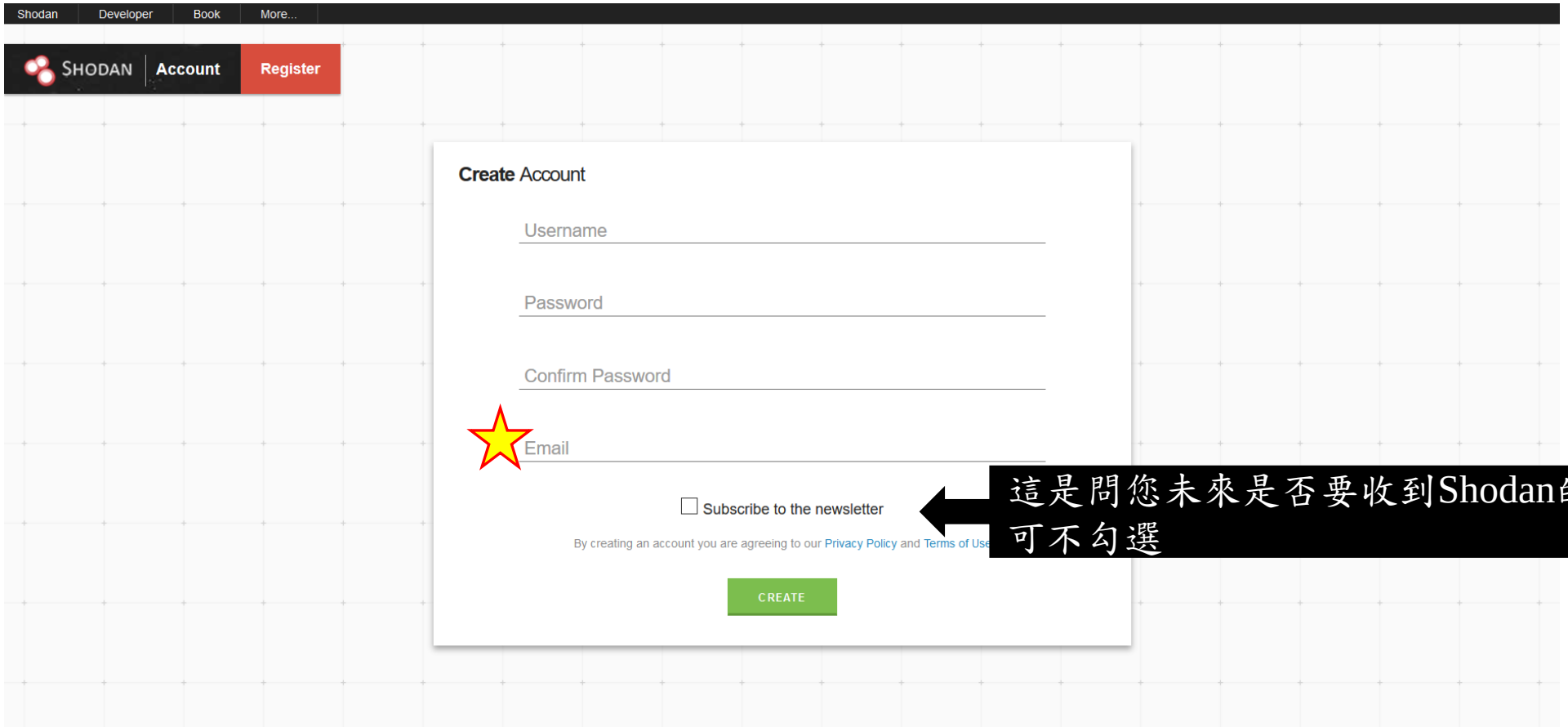
前言

- 使用Shodan服務前，需要建立一個使用帳號，否則有些功能會受到限制
- Shodan帳號有不同等級，但免費帳號就可以使用一些基本功能
- 接下來會從註冊帳號開始，到如何操作Shodan網頁上的搜尋功能

註冊Shodan帳號-1



註冊Shodan帳號-2



註冊Shodan帳號-3

SHODAN | Help Center Search

Academic Upgrade

Shodan provides a free Membership upgrade for users that sign up with an academic email address (ex. ending in `.edu`, `.ac.uk` etc.) The academic membership includes the following:

- Ability to monitor up to 16 IPs
- 100 query credits per month
- 100 scan credits per month
- Access to Shodan Maps and Shodan Images
- `vuln` filter can be used on the website

We also offer a higher academic plan for free that is aimed at university IT departments that want to monitor their Internet-facing infrastructure. The goal is to offer universities a free way to get notified when something unexpected shows up on their network. The academic plus plan provides everything that the Membership does as well as:

- Ability to monitor up to ~120,000 IPs (2 /16s worth of IPs). Note that you're only allowed to monitor your university network.

To receive the academic plus upgrade please email academic@shodan.io from an academic email address with a Shodan account that we can confirm belongs to the university's IT department.

正文

今天介紹一個好用的網站 shodan

Shodan是一個蒐集大量IoT裝置等任何連到網路上且用公共IP的設備資訊，如WiFi AP、網路攝影機、路由器等。這些資訊每天更新，有點類似專掃聯網設備的google。

這個網站蒐集大量的已知弱點的網站，也有提供 api 可以使用。

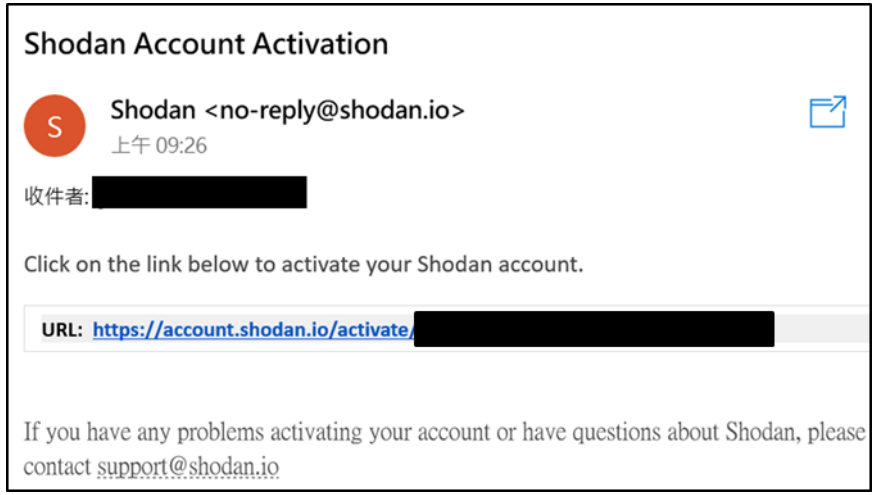
這是不在官方清單的教育版 申請方式

```
1.首先使用教育版的email到Shodan註冊一個帳號
(*@*.edu.*)

2.使用學校的email，發送email到Shodan的信箱academic@shodan.io

3.等待，最快2天最慢1週，你的帳戶就從免費方案變成教育方案了，所用的流量都是每月更新
```

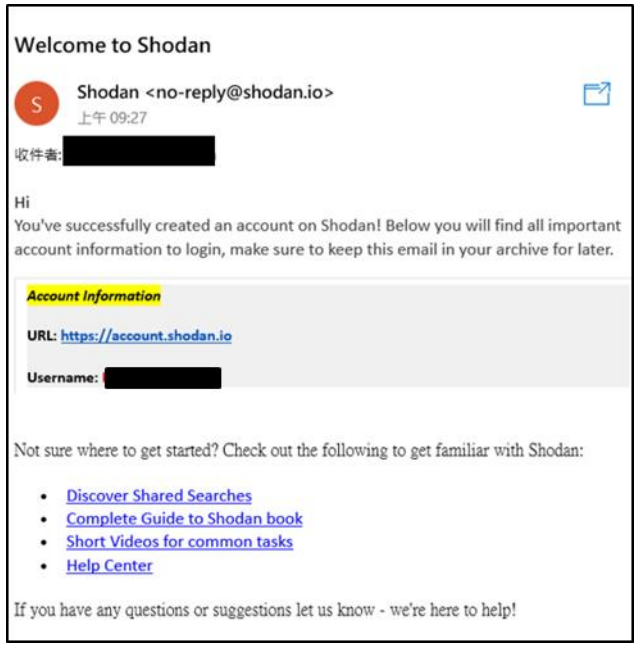
資料來源：https://ithelp.ithome.com.tw/articles/10218769

註冊Shodan帳號-4

- 到註冊的信箱收信，總共會收到兩封信：
  - 第一封信是帳號啟動確認信，請點擊信中的連結啟動帳號
  - 等啟動完成後會收到第二封信，是帳號建立完成信，此時就可以登入Shodan帳號

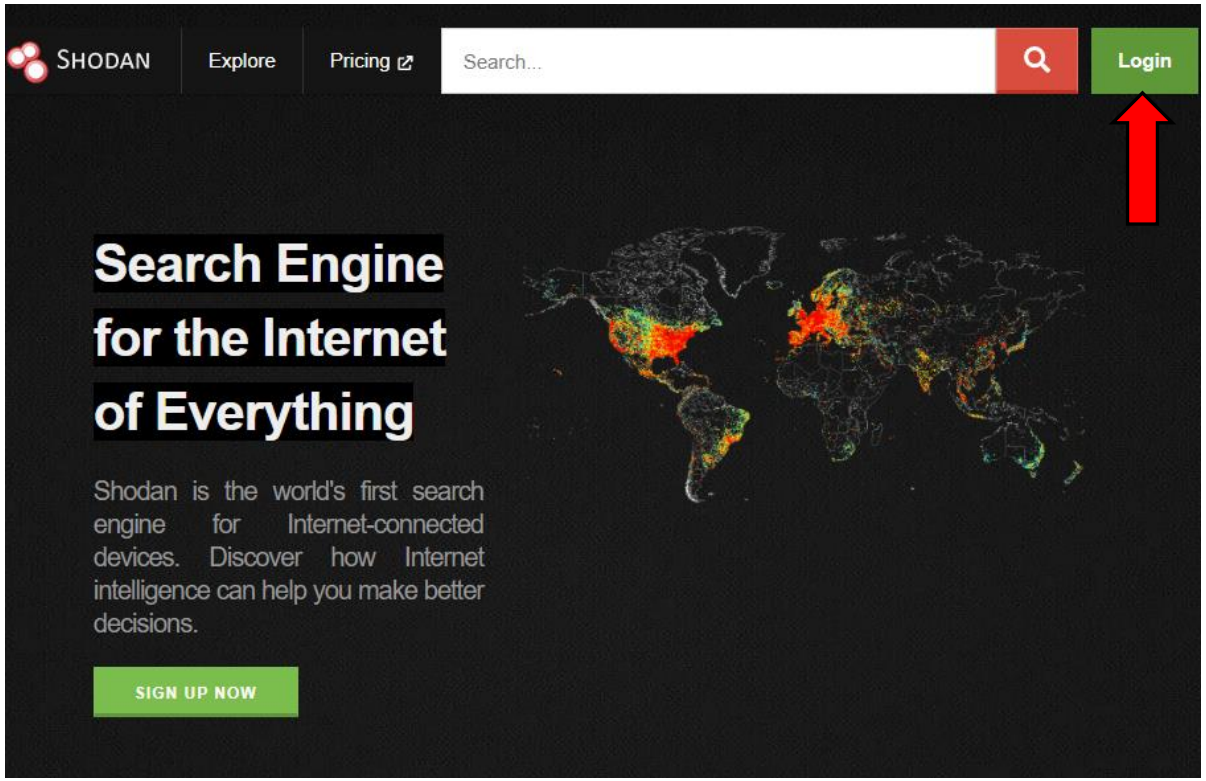


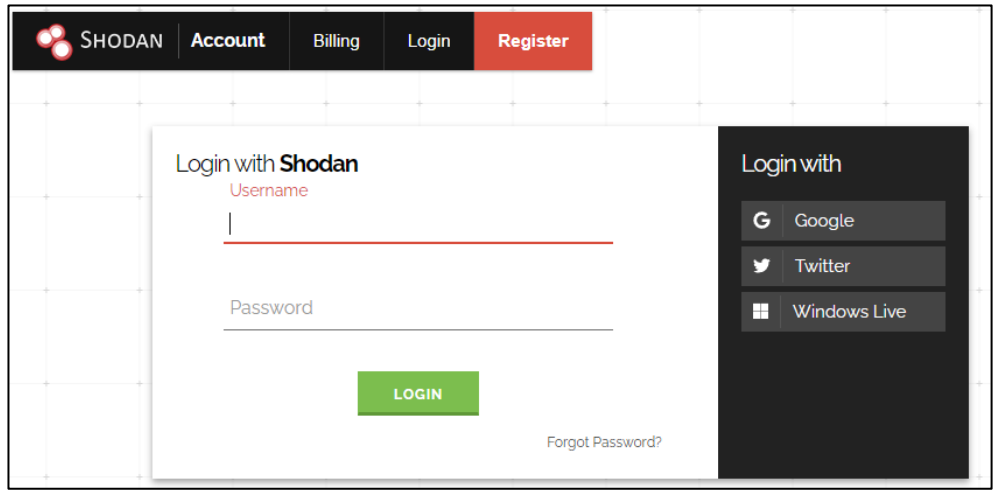
帳號啟動確認信



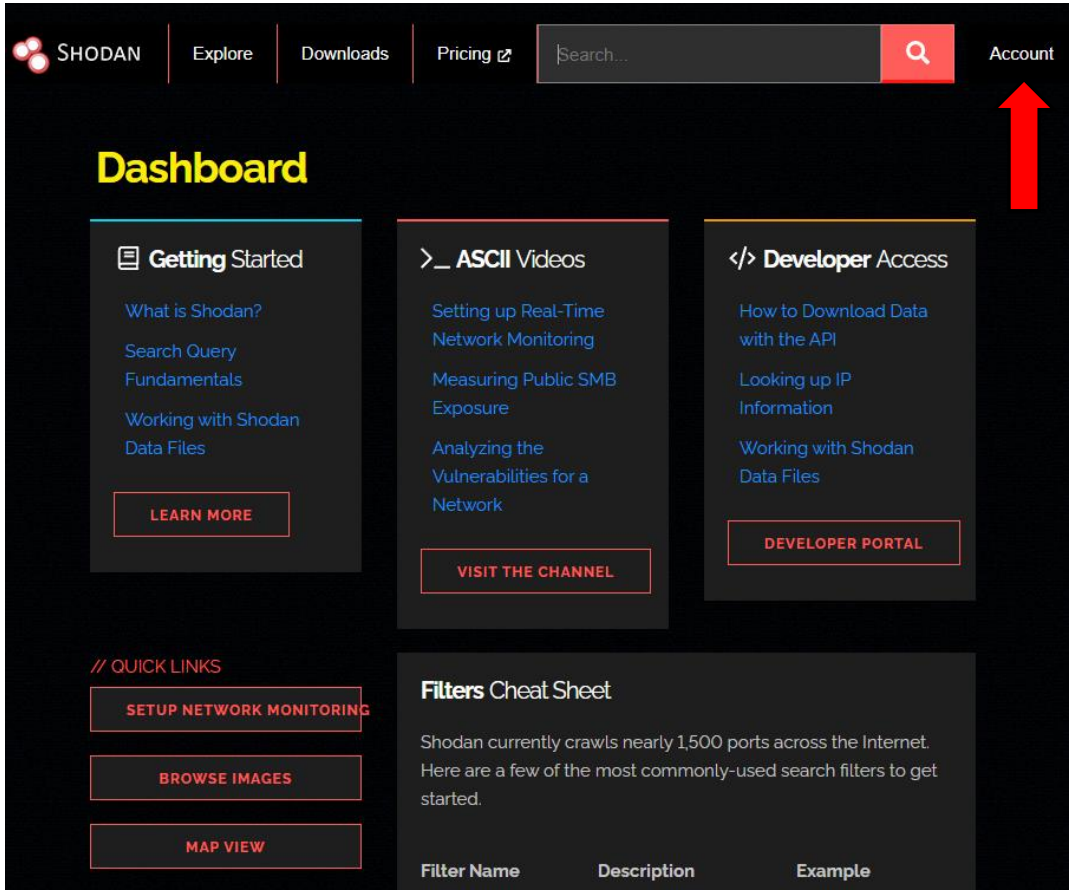
帳號建立完成信

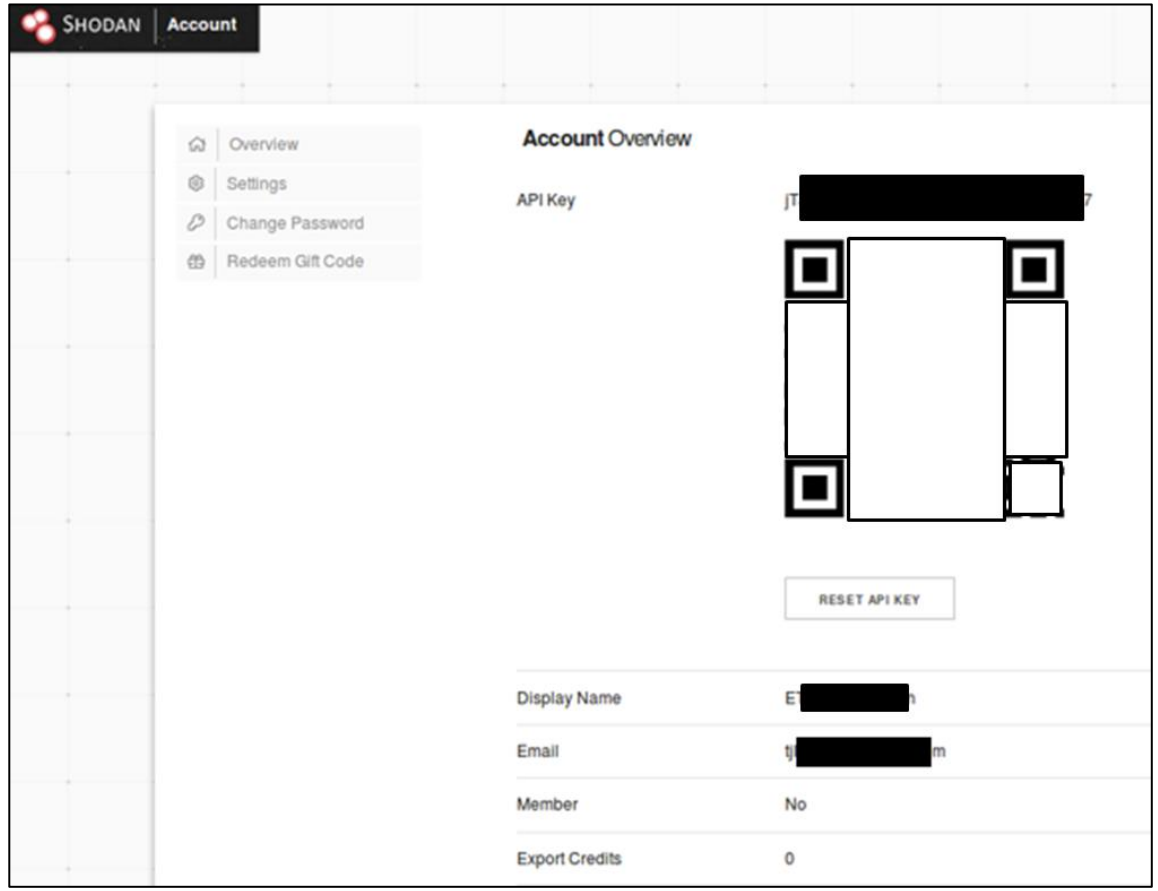
登入Shodan帳號


SHODAN
Explore
Pricing
Search...
Login
Search Engine for the Internet of Everything
Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.
SIGN UP NOW


SHODAN
Account
Billing
Login
Register
Login with Shodan
Username
Password
LOGIN
Forgot Password?
Login with
Google
Twitter
Windows Live

確認Shodan帳號資訊





帳號等級差異

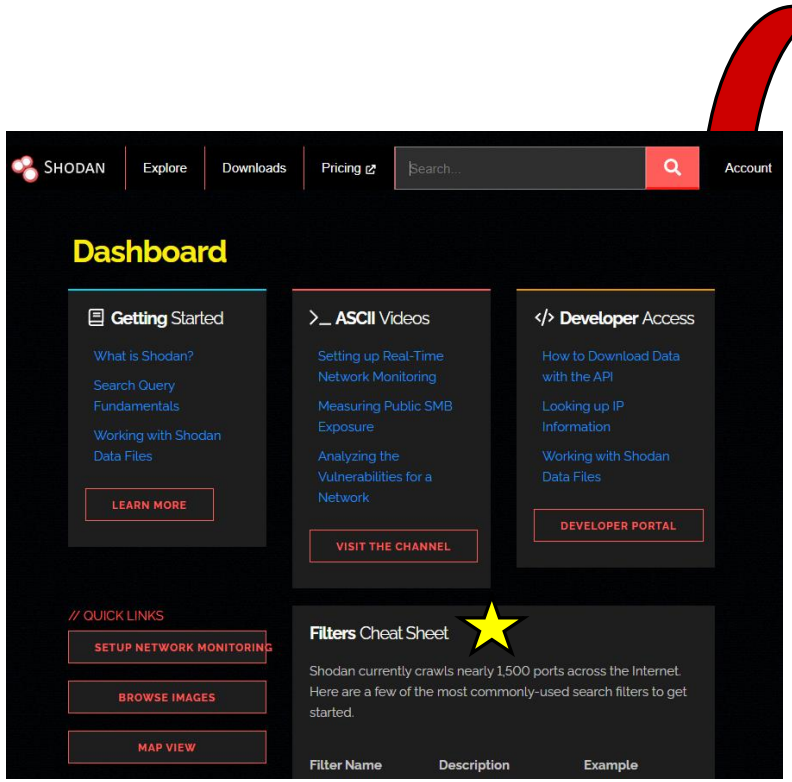
	Free	Membership	Corporate API	Enterprise Data License
Basic Access to Shodan Search Engine The ability to search on Shodan using basic filters. Includes Shodan Maps and Shodan Exploits.	✓	✓	✓	✓
Integrations with Popular Tools Metasploit, Maltego, Nmap and Splunk are just a few of the tools that integrate out of the box with Shodan.	✓	✓	✓	✓
Explore the Internet Visually Use Shodan Images to browse screenshots gathered from devices around the world.		✓	✓	✓
Simple Website Downloads With the click of a button you can download search results to your local computer.		✓	✓	✓
Deep IP Enrichment Learn more about the devices that are interacting with your network by looking them up in Shodan.		✓	✓	✓
On-Demand Scanning Ask Shodan to scan your Internet-facing devices to validate your firewall and make sure existing issues have been fixed.			✓	✓
Real-Time Network Monitoring Keep track of the latest services discovered on your external network in real-time.			✓	✓

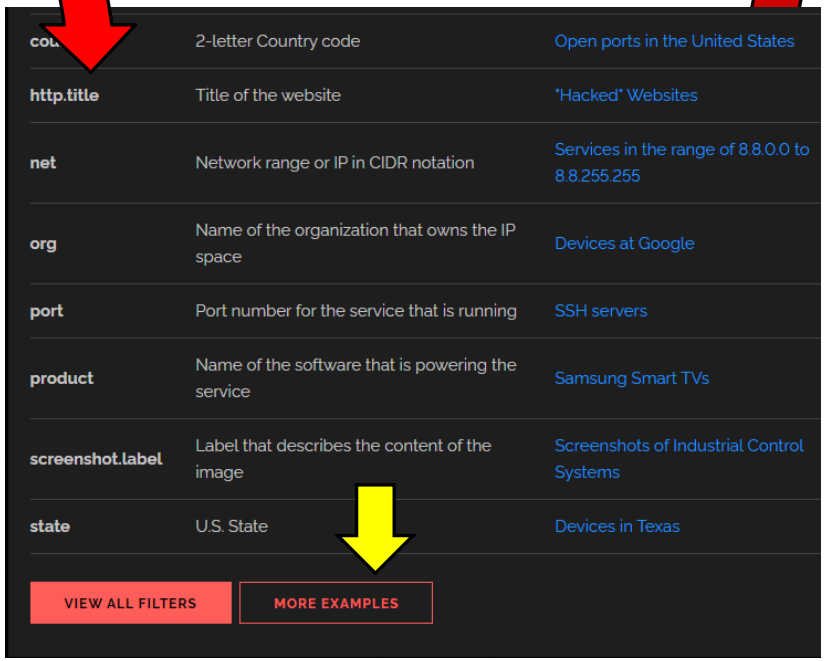
Compare Features

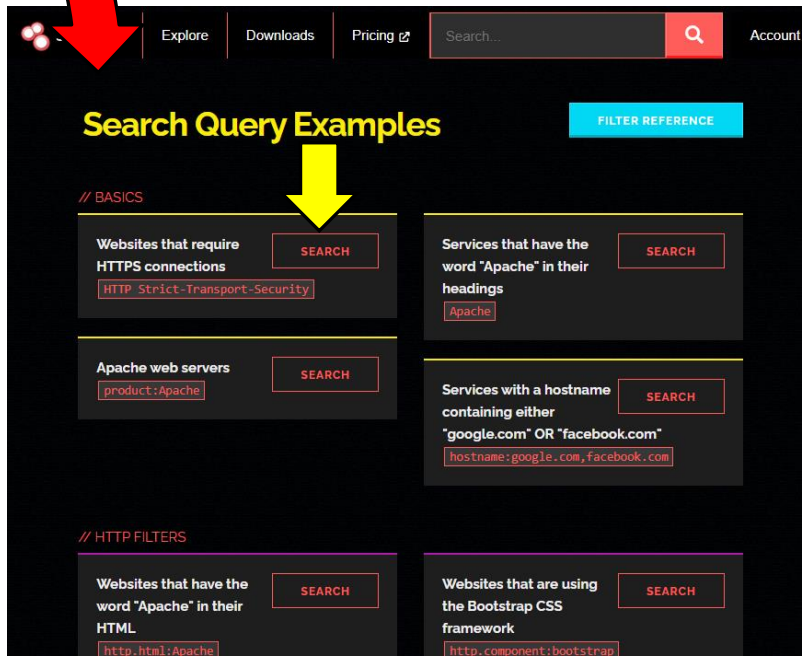
	Membership	Freelancer	Small Business	Corporate	Enterprise
Price	$49 (one-time)	$59/ month	$299/ month	$899/ month	Custom
Query credits (per month)	100	10,000	200,000	Unlimited	Unlimited
Scan credits (per month)	100	5,120	65,536	327,680	Unlimited
Monitored IPs	16	5,120	65,536	327,680	Unlimited
Available search filters	All except `vuln` and `tag`	All except `vuln` and `tag`	All except `tag`	All	All
Number of users	1	1	1	1	Custom
Shodan Search pages	20	20	200	200	200
Shodan Monitor	✓	✓	✓	✓	✓
Shodan Trends	✓	✓	✓	✓	✓
Private firehose	✓	✓	✓	✓	✓
IP lookups	✓	✓	✓	✓	✓
Batch IP lookups				✓	✓
Bulk Data					✓
InternetDB					✓
Full firehose					✓
Internet scanning API					✓

該如何使用Shodan搜尋?

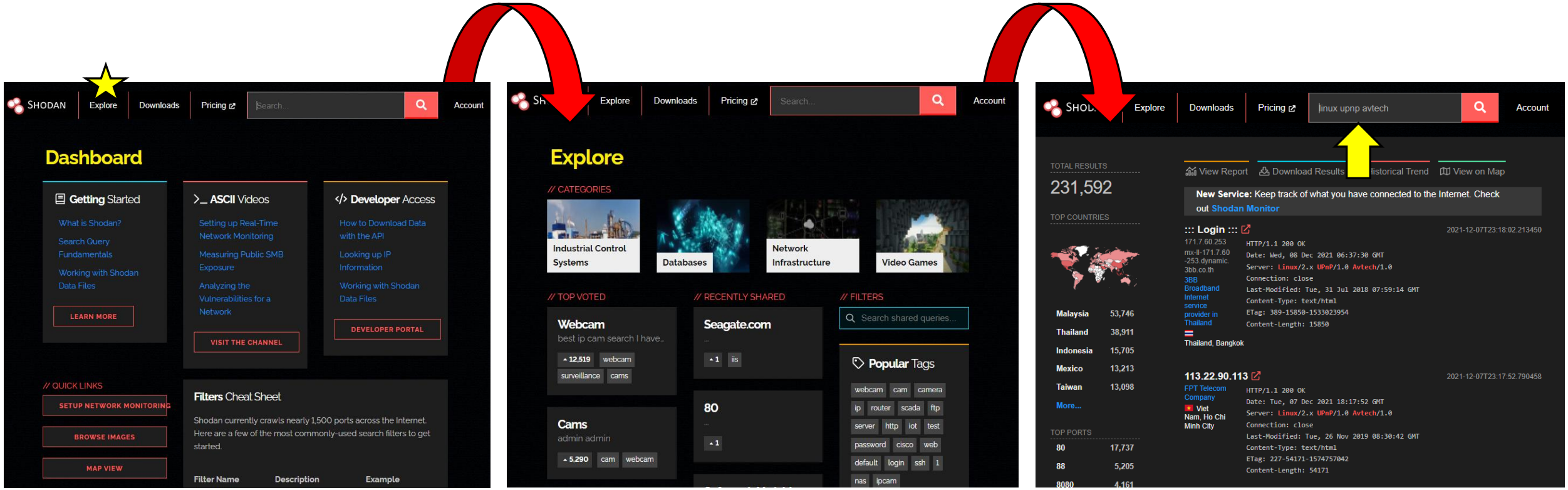
搜尋方法一：參考官方範例



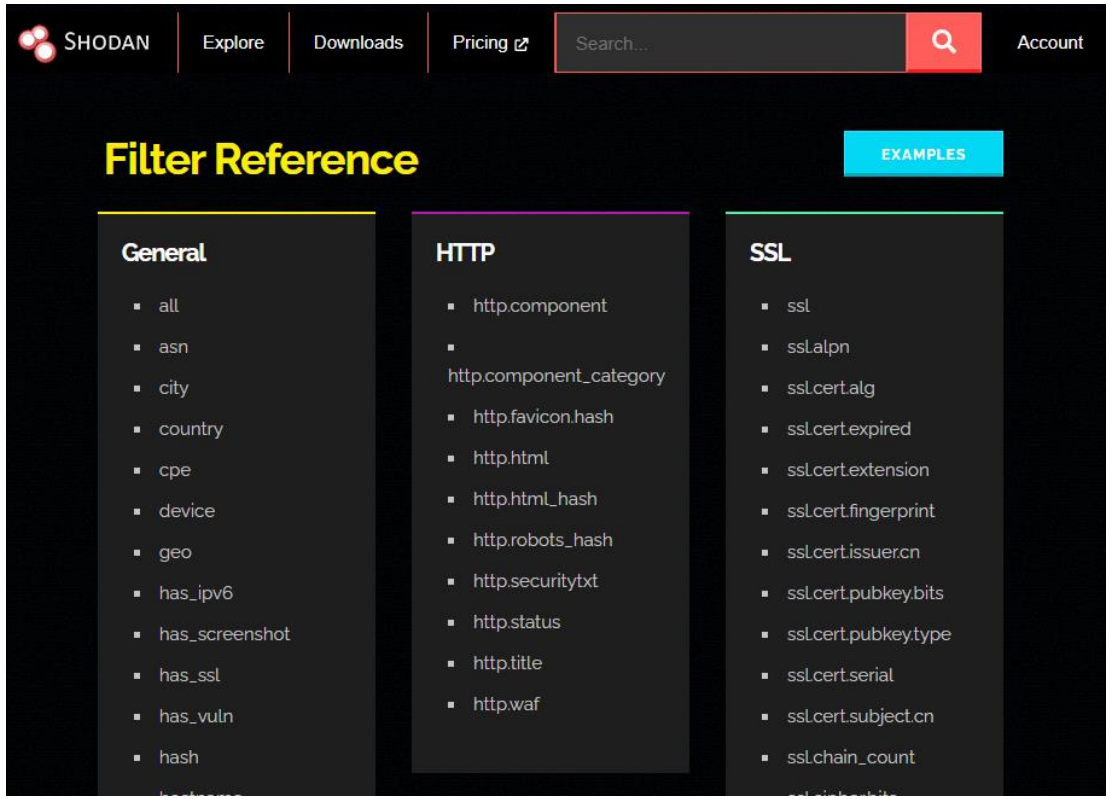


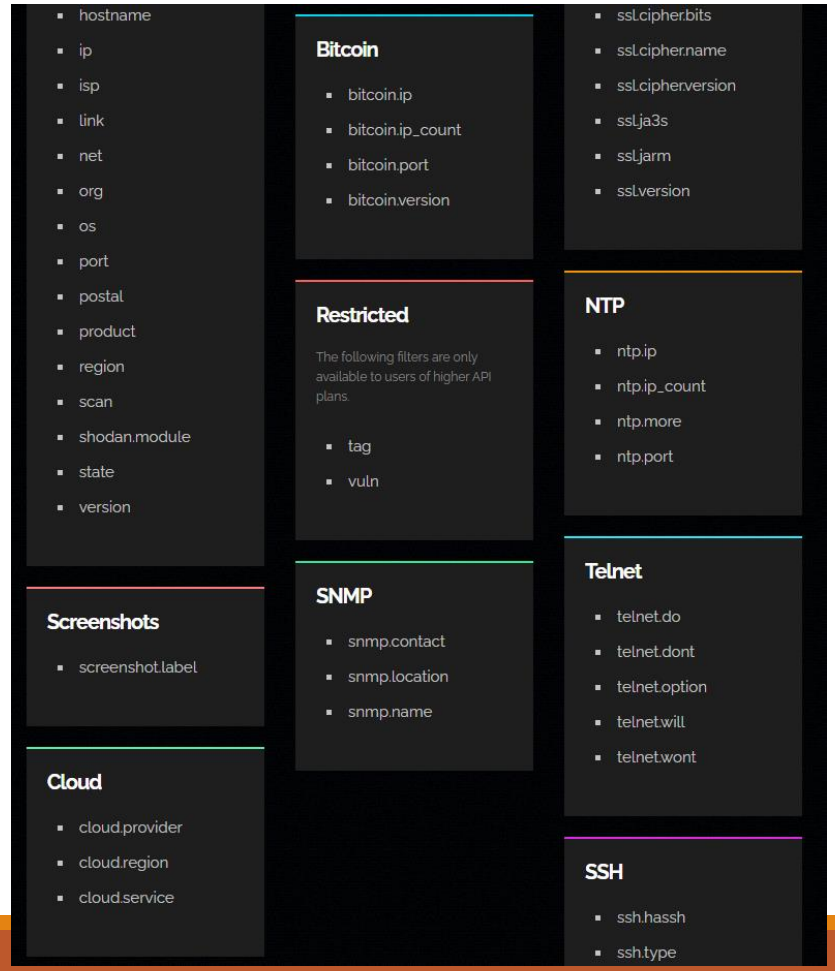


搜尋方法二：參考Explore範例



網頁可使用的過濾器列表





常用的過濾器說明

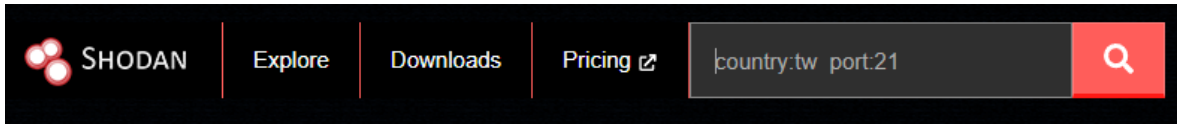
過濾器	說明	範例
net	搜尋指定的ip 位置或是網段	**net**:59.120.179.0/24
port	搜尋指定的連接埠	**port**:80
product	搜尋指定的作業系統/軟體/產品名稱	**product**:windows
country	搜尋指定的國家	**country**:us
org	搜尋指定的組織或公司	**org**:google
hostname	搜尋指定的網域名稱	**hostname**:azure

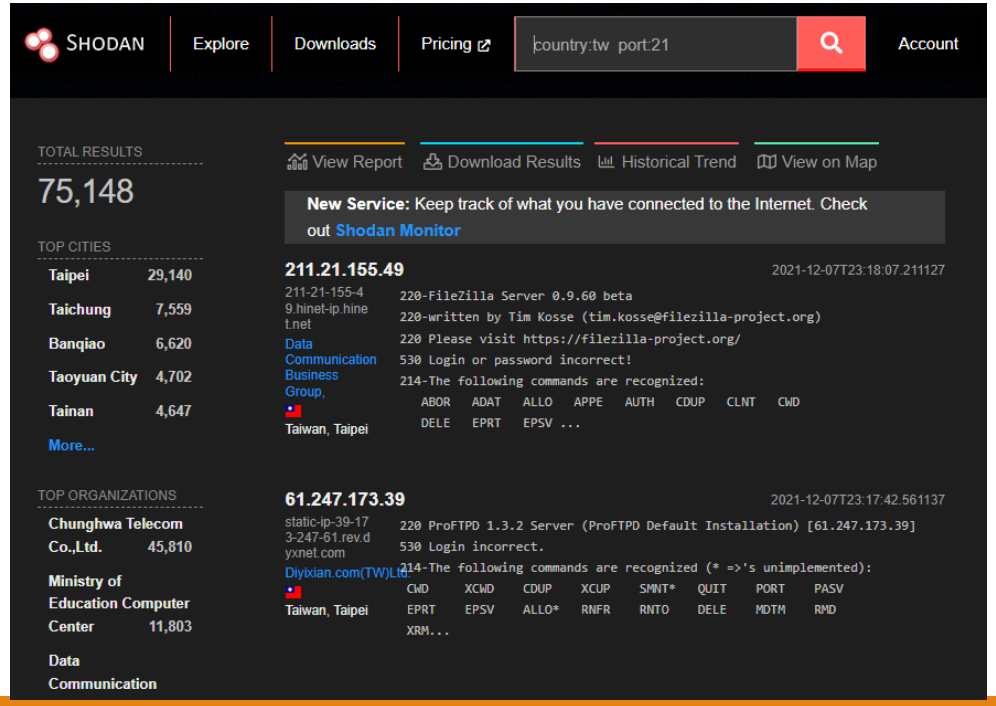
網頁搜尋範例-問題篇

- 假設現在要搜尋具備下列條件的IoT設備：
  1. 設備在台灣
  2. 有開啟FTP服務

網頁搜尋範例-解答篇

- 假設現在要搜尋具備下列條件的IoT設備：
  1. 設備在台灣 ------->country:tw
  2. 有開啟FTP服務 ------->port:21 (FTP服務預設埠號)



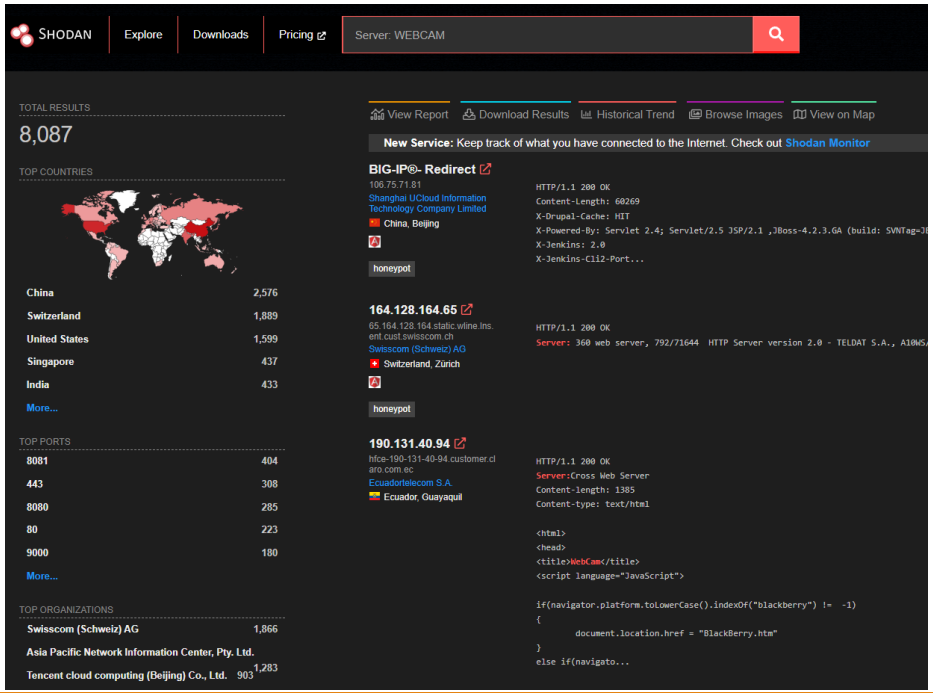


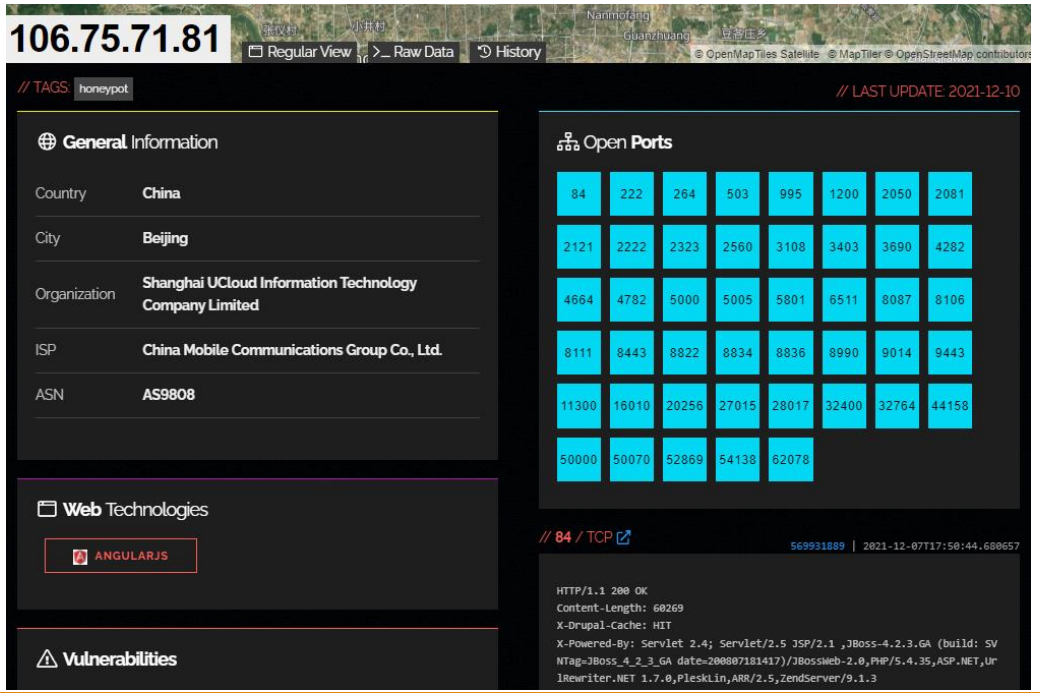
- 備註一：在網頁搜尋時，可以搭配多種過濾器使用，來限縮目標範圍
- 備註二：過濾器使用先後次序無關，不會影響找到設備數量

下載Shodan資料

前言

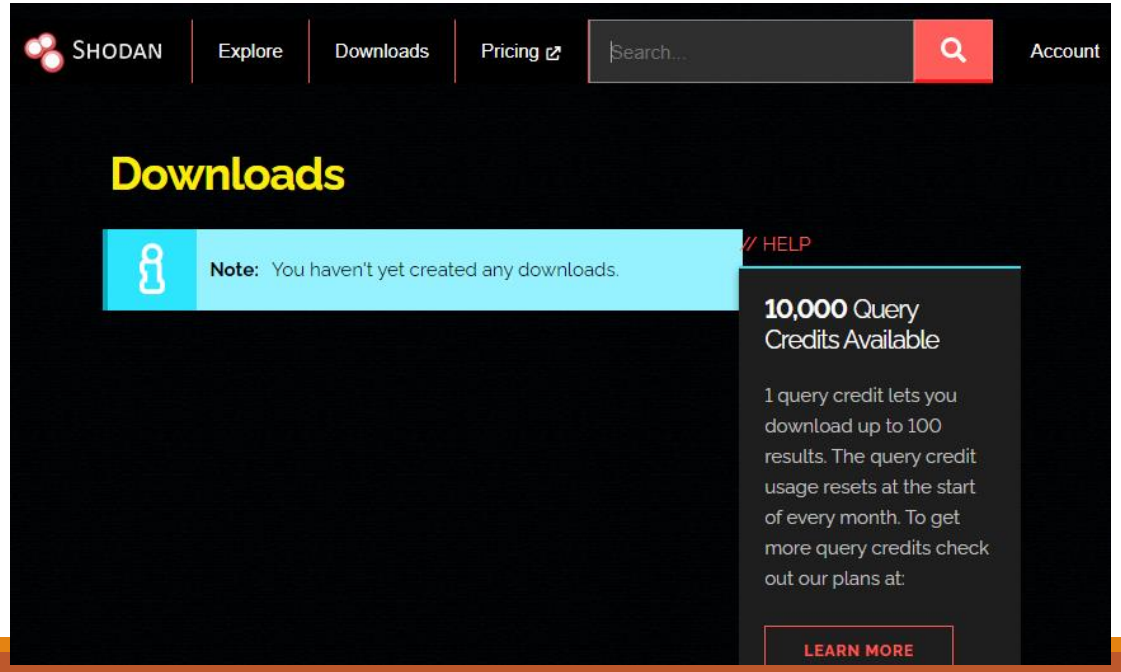
- 如果在短時間內分析大量資料、找到特定目標，不可能單靠網頁就可以辦到
- 資料分析前，最重要的步驟就是收集資料
- 接下來會逐步解說如何從Shodan搜尋引擎下載資料





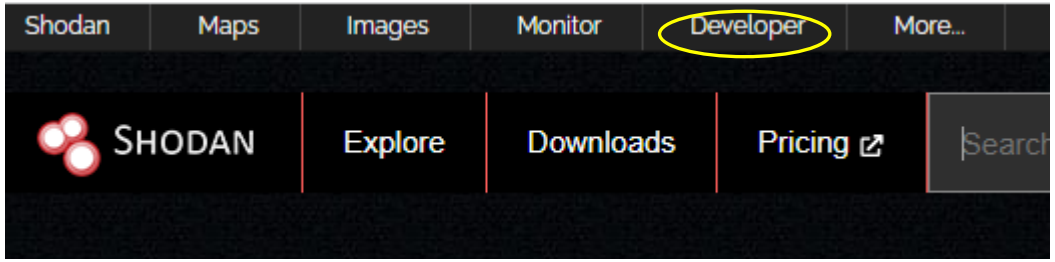
下載資料的方法

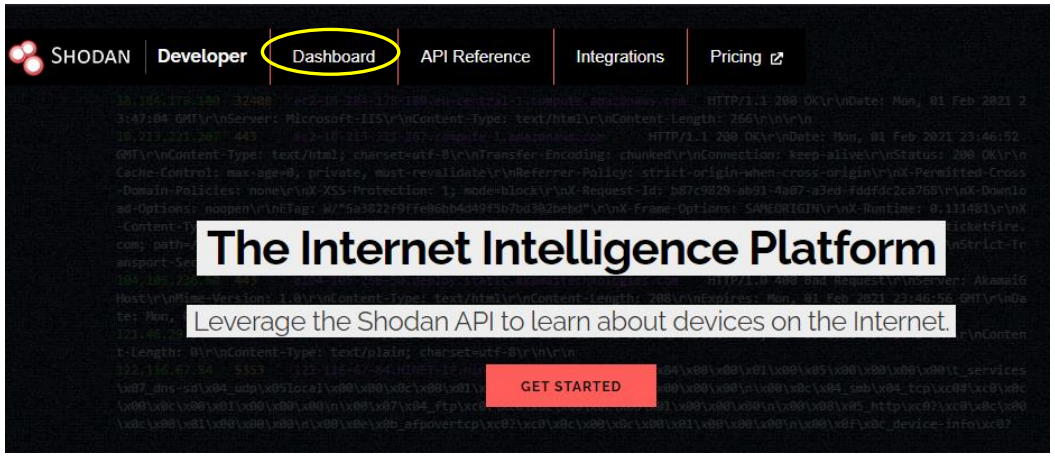
- Shodan有兩種方式可以下載資料
  1. 在網頁上直接下載
  2. 使用命令列(CLI)並透過Shodan API下載
- 但是下載Shodan資料需要點數

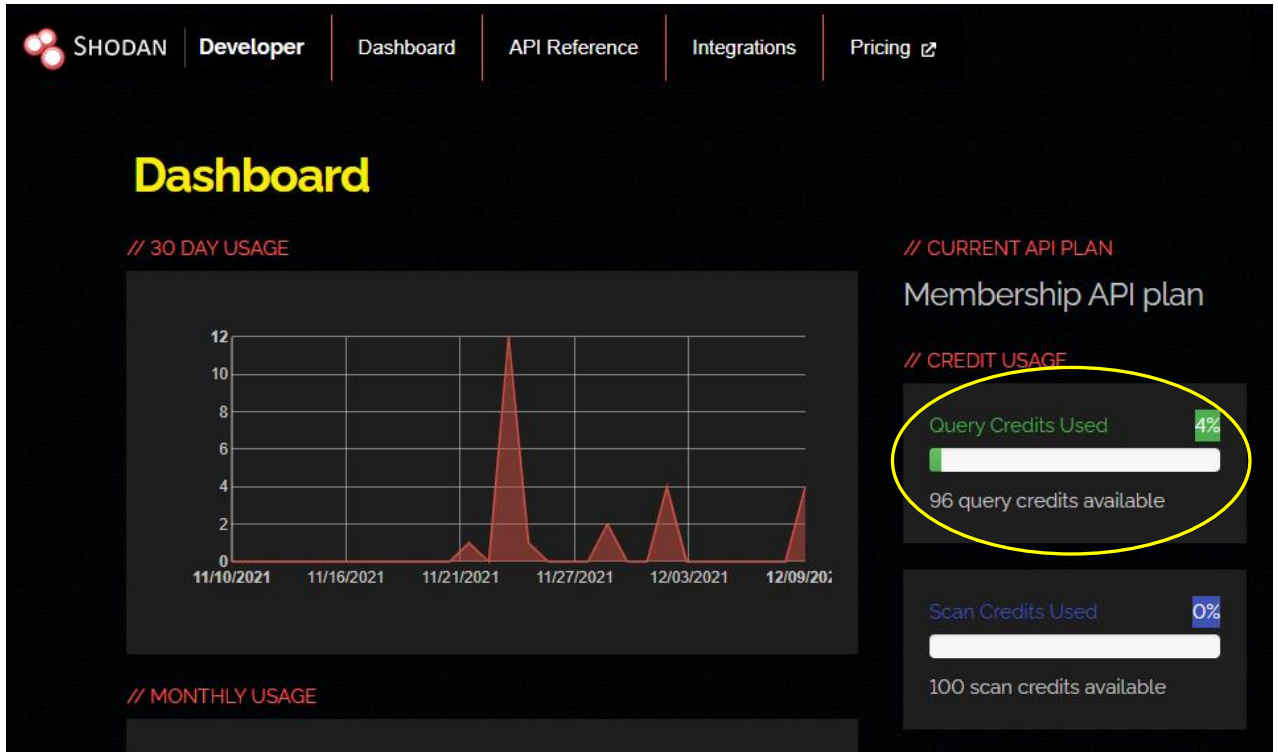



```
achillean@demo:~$ shodan download -h
Usage: shodan download [OPTIONS] <filename> <search query>

  Download search results and save them in a compressed JSON file.

Options:
  --limit INTEGER  The number of results you want to download. -1 to download
                   all the data possible.
  -h, --help       Show this message and exit.
achillean@demo:~$
achillean@demo:~$
achillean@demo:~$ # Download up to 1,000 MongoDB results
achillean@demo:~$
achillean@demo:~$ shodan download --limit 1000 mongodb.json.gz product:mongodb
Search query:                   product:mongodb
Total number of results:        21493
Query credits left:             100000
Output file:                    mongodb.json.gz
  [------------------------------------]    0%
```

如何查詢帳號內持有的點數?







官方點數消耗說明

Shodan Credits Explained

At Shodan, the amount of access you get to data and other features of the infrastructure depend on how many **credits** your account has available. There are 2 types of credits available at Shodan:

- **Query** credits
- **Scan** credits

Note: Export credits are deprecated and can nolonger be purchased.

Query Credits

Query credits are used to download data via the website, command-line interface or the API. If you're using the CLI or API then query credits are deducted if one of the following 2 conditions is met:

- A search filter is used
- Page 2 or beyond is requested

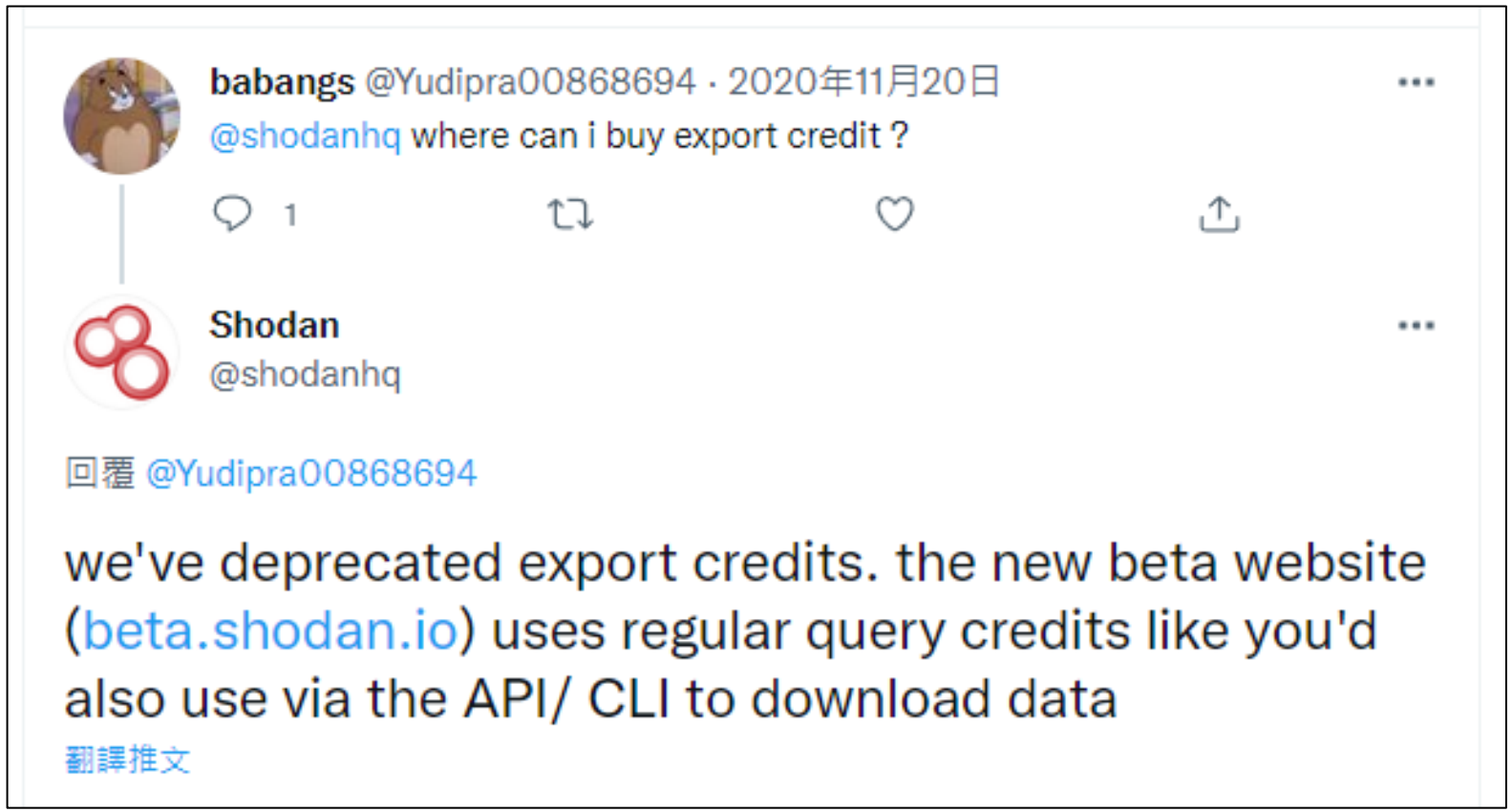
Query credits **renew at the start of the month** and provide the following amount of data:

> **1** query credit lets you download **100 results**

Here are a few search queries and how many **query credits** they consume:

- **apache**: search query without any filters and 1st page of results - **no query credits used**
- **product:mongodb**: searches for MongoDB database servers and uses **1 query credit**
- 3rd page of **apache**: requesting the 3rd page costs **1 query credit**
- 5th page of **product:mongodb**: requesting the 5th page of search results for MongoDB: **1 query credit**

網頁下載的變化：捨棄export credits



babangs @Yudipra00868694 · 2020年11月20日

@shodanhq where can i buy export credit ?

1

Shodan

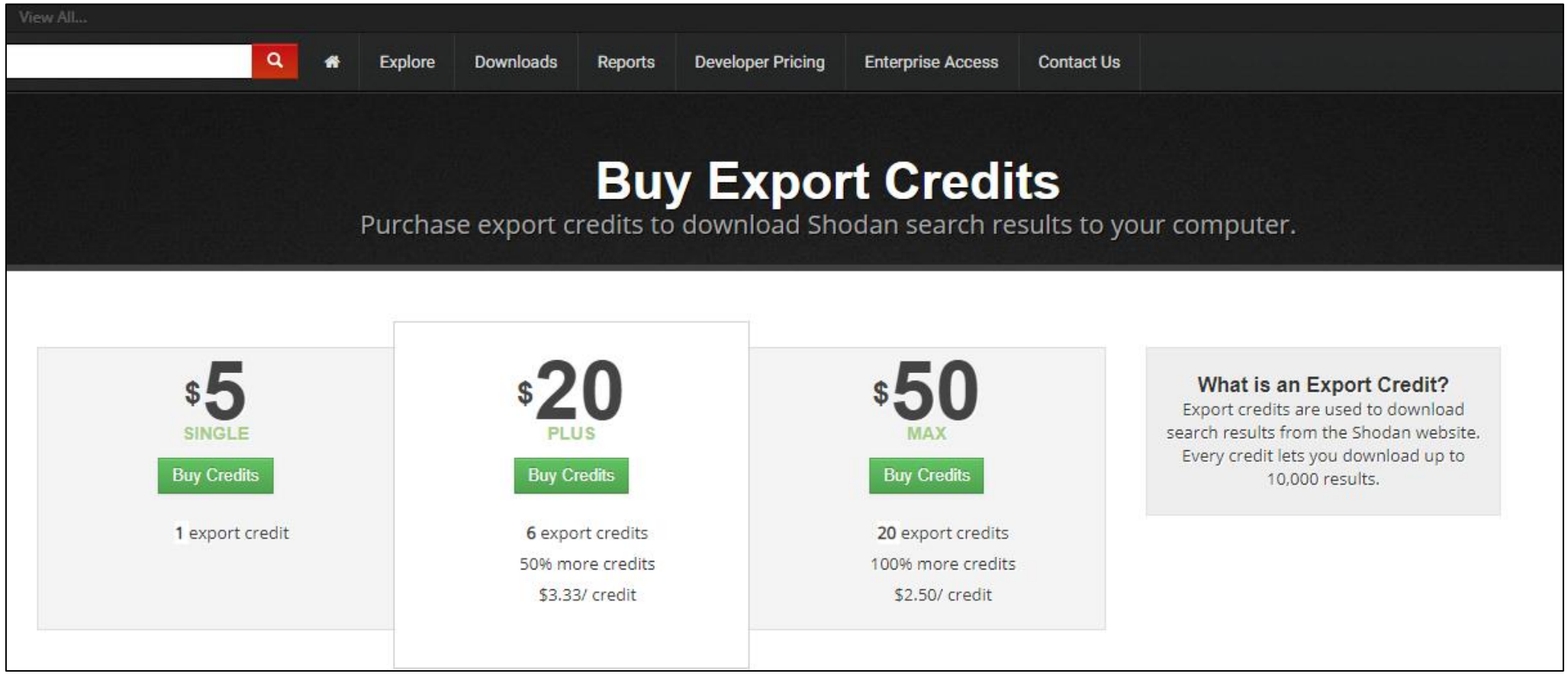
@shodanhq

回覆 @Yudipra00868694

we've deprecated export credits. the new beta website (beta.shodan.io) uses regular query credits like you'd also use via the API/ CLI to download data

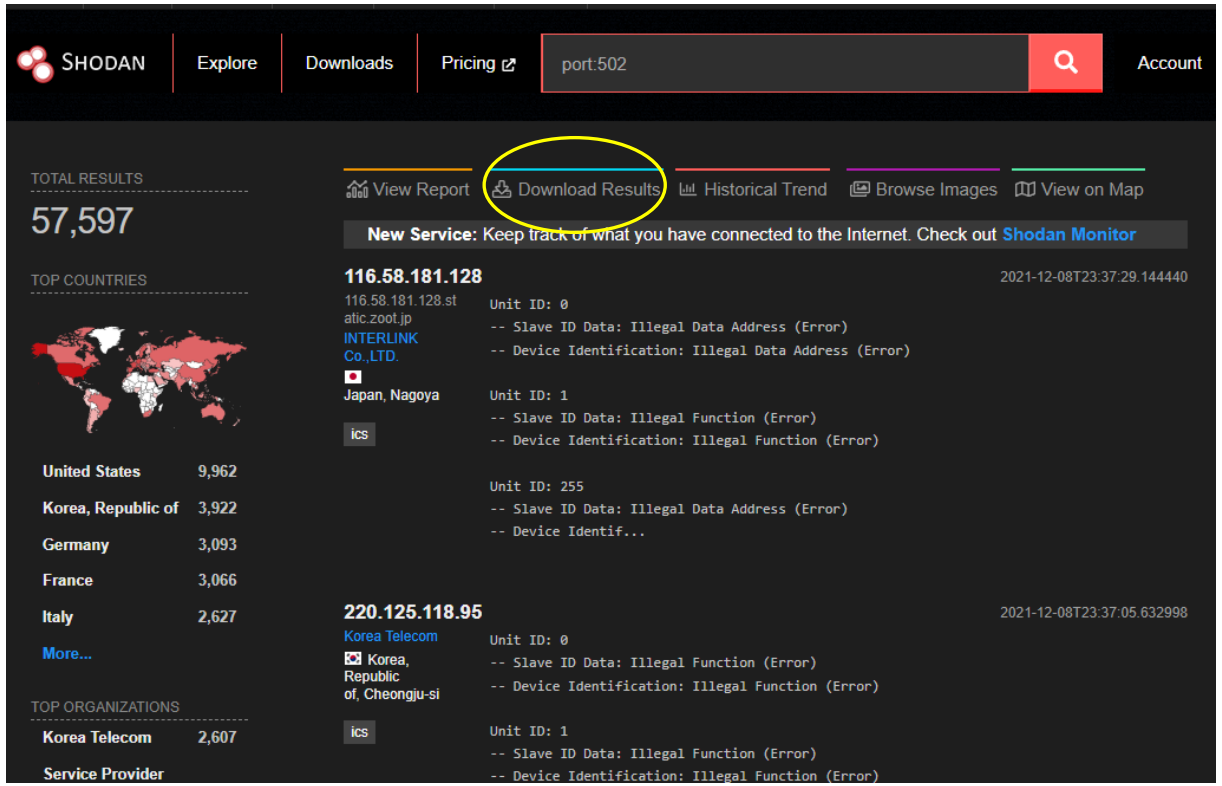
翻譯推文

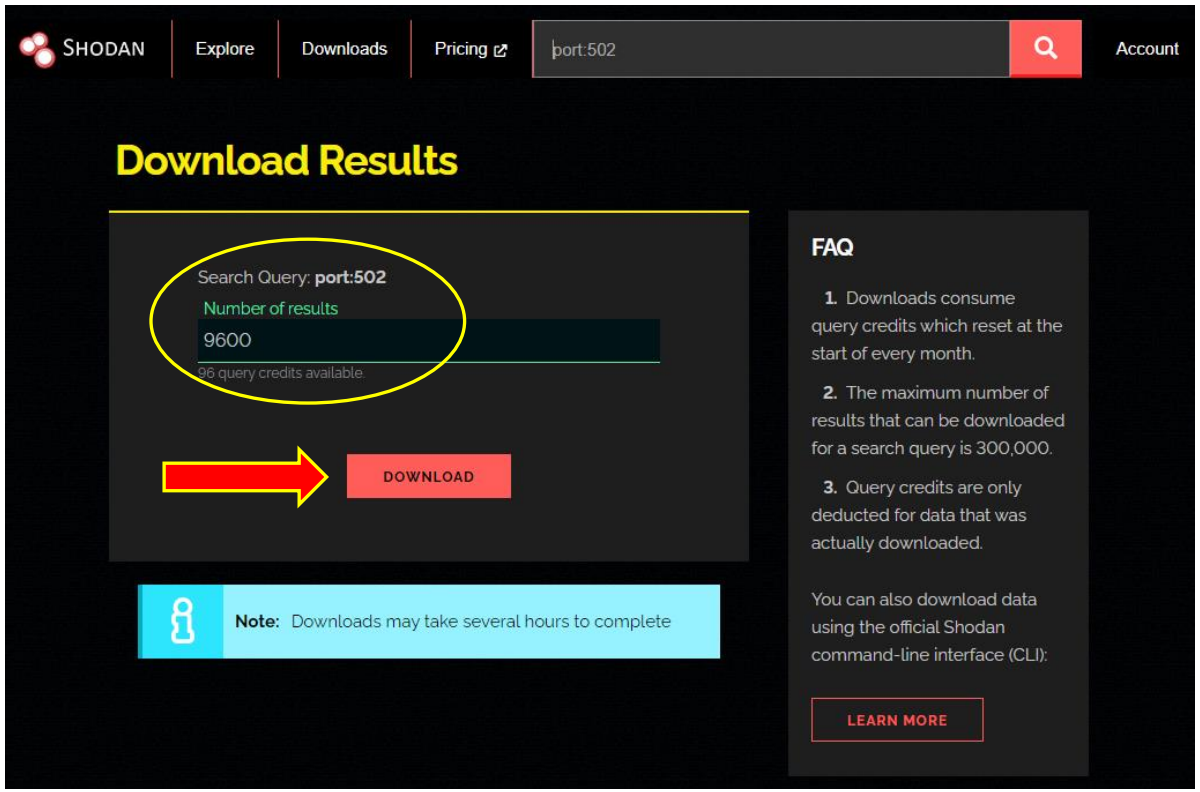
過去的購買Export Credits金額

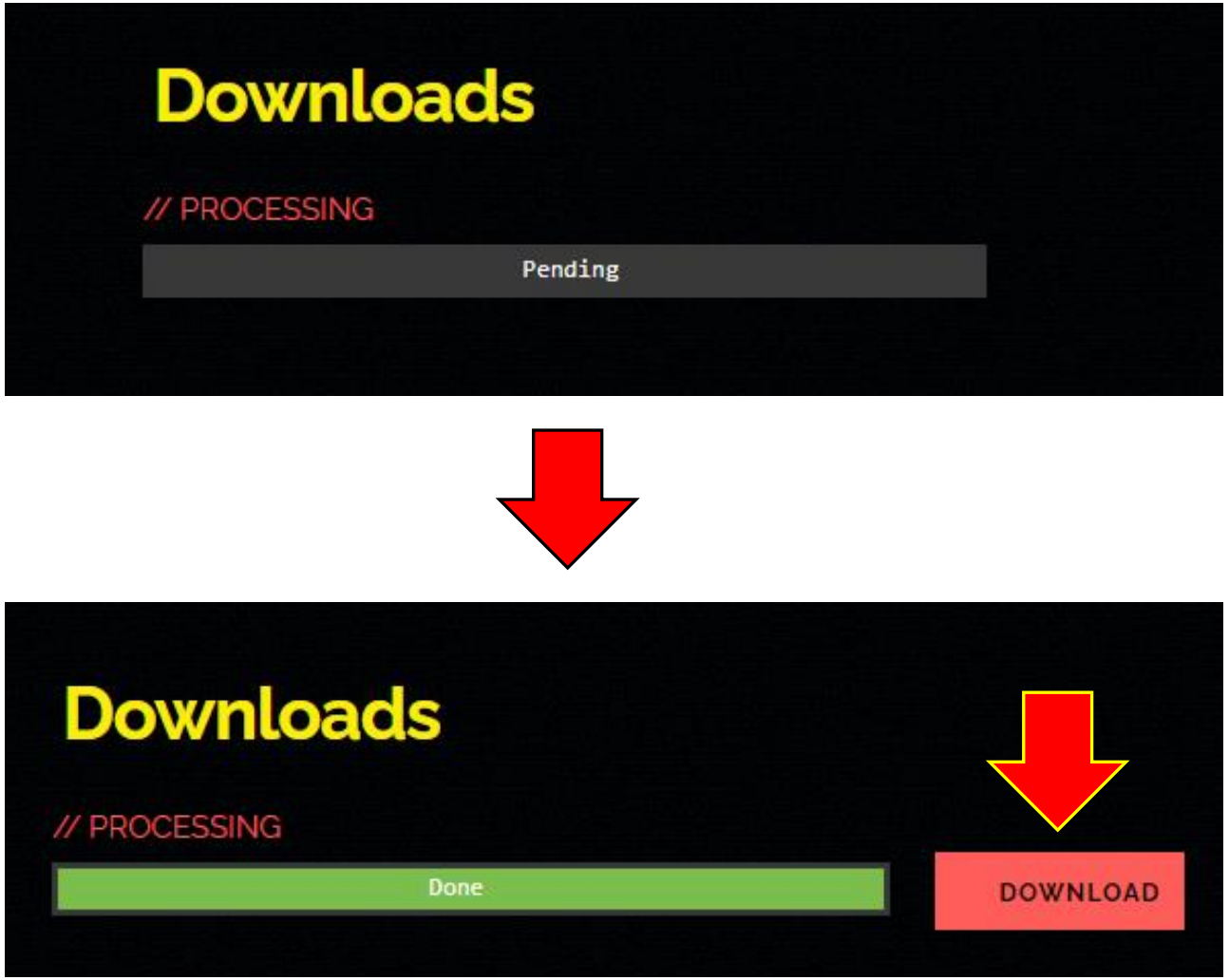


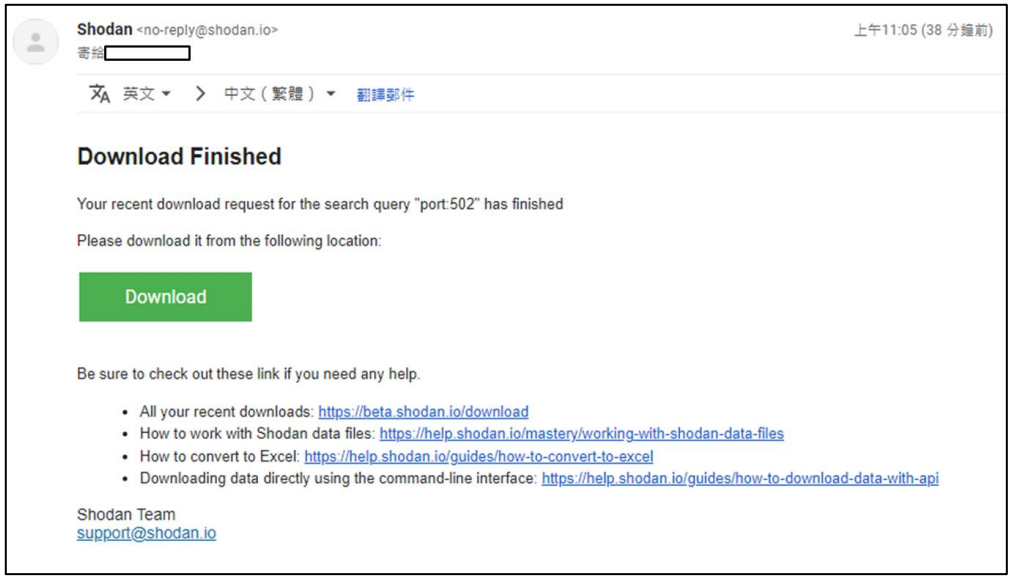
下載方法一：從網頁直接下載

- 假設現在要下載port:502的資料









Shodan <no-reply@shodan.io> 上午11:05 (38 分鐘前)
寄給 [redacted]

英文 > 中文（繁體） 翻譯郵件

Download Finished

Your recent download request for the search query "port:502" has finished

Please download it from the following location:

Download

Be sure to check out these link if you need any help.

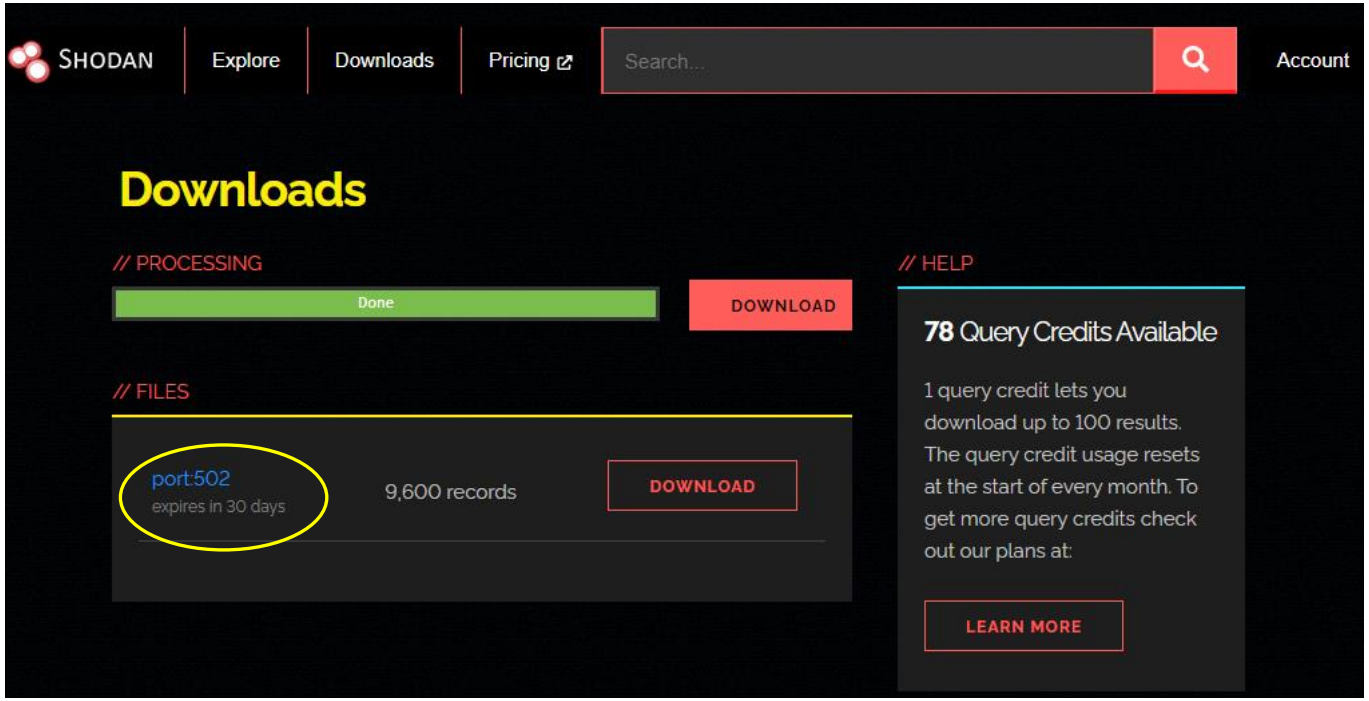
- All your recent downloads: https://beta.shodan.io/download
- How to work with Shodan data files: https://help.shodan.io/mastery/working-with-shodan-data-files
- How to convert to Excel: https://help.shodan.io/guides/how-to-convert-to-excel
- Downloading data directly using the command-line interface: https://help.shodan.io/guides/how-to-download-data-with-api

Shodan Team
support@shodan.io

下載作業進度完成後，官方會寄信通知

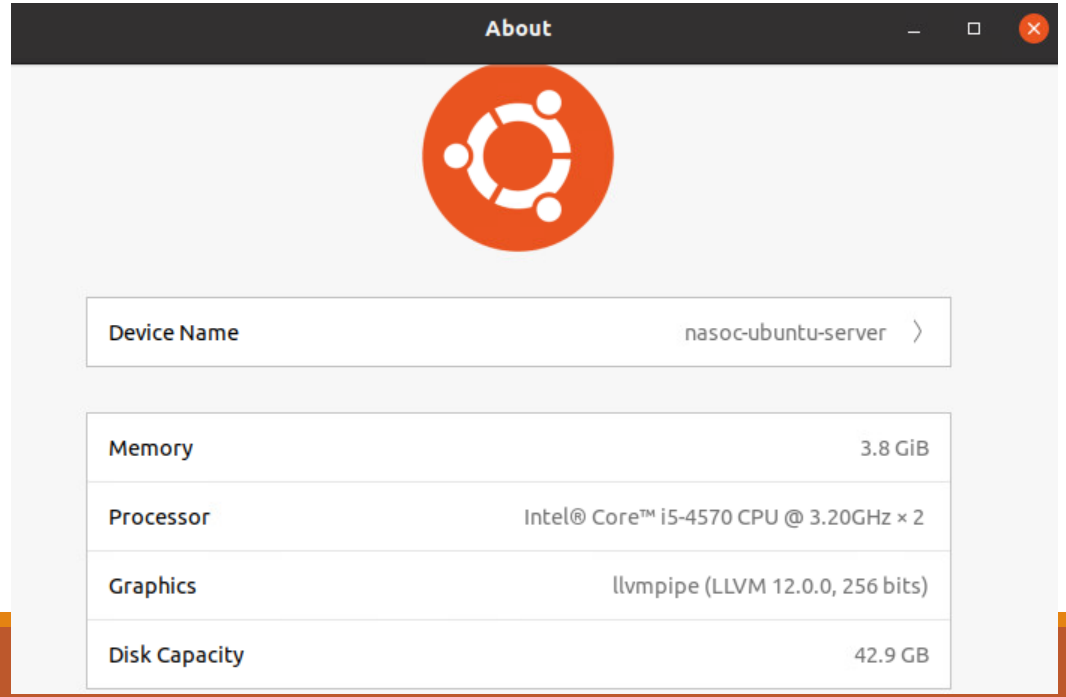
如何重新下載資料?


SHODAN
Explore
Downloads
Pricing
Search...


SHODAN
Explore
Downloads
Pricing
Search...
Account
Downloads
// PROCESSING
Done
DOWNLOAD
// FILES
port:502
expires in 30 days
9,600 records
DOWNLOAD
// HELP
78 Query Credits Available
1 query credit lets you download up to 100 results. The query credit usage resets at the start of every month. To get more query credits check out our plans at:
LEARN MORE

下載方法二：使用命令列下載

- Shodan官方(創辦人)有提供python套件，讓使用者在命令列上操作Shodan服務，或自行寫python程式碼import Shodan套件
- 下載網址: https://github.com/achillean/shodan-python
- 後續安裝教學會以Ubuntu做示範



安裝Shodan套件

- 可以依照Github上的說明指示安裝
- Ubuntu有整合Shodan安裝套件，可以直接安裝套件

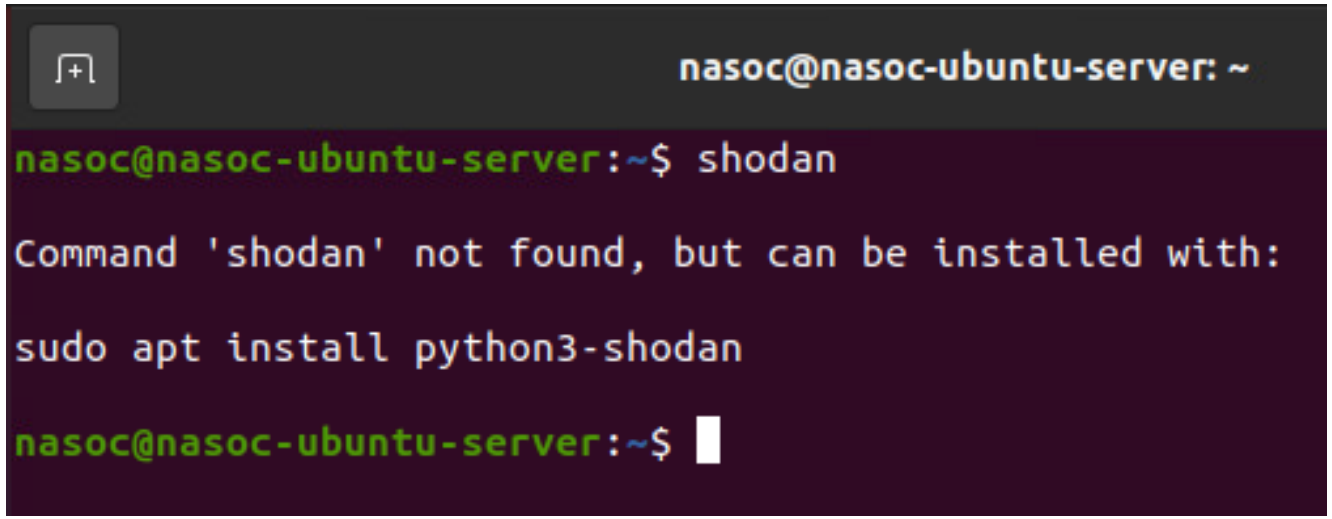
Installation

To install the Shodan library, simply:

```
$ pip install shodan
```

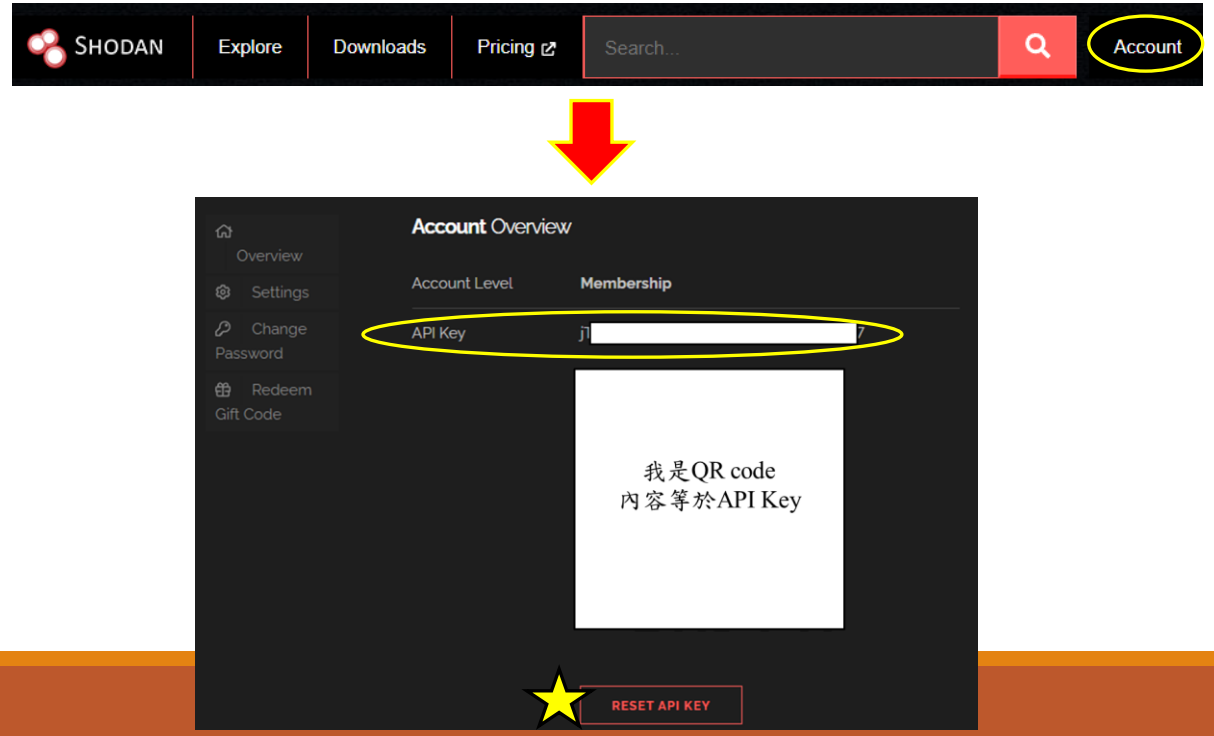
Or if you don't have pip installed (which you should seriously install):

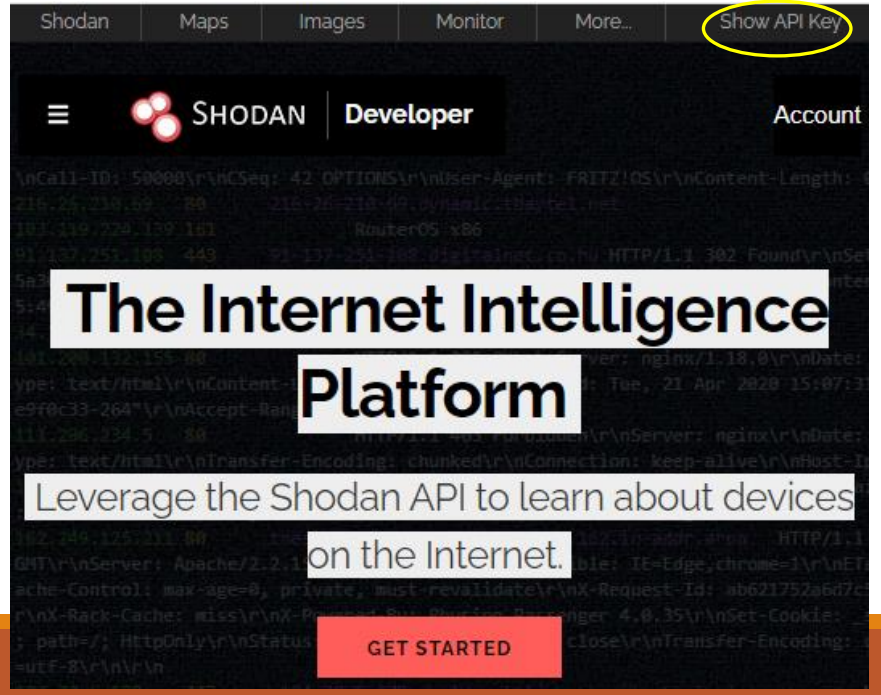
```
$ easy_install shodan
```



查詢個人帳號的API Key

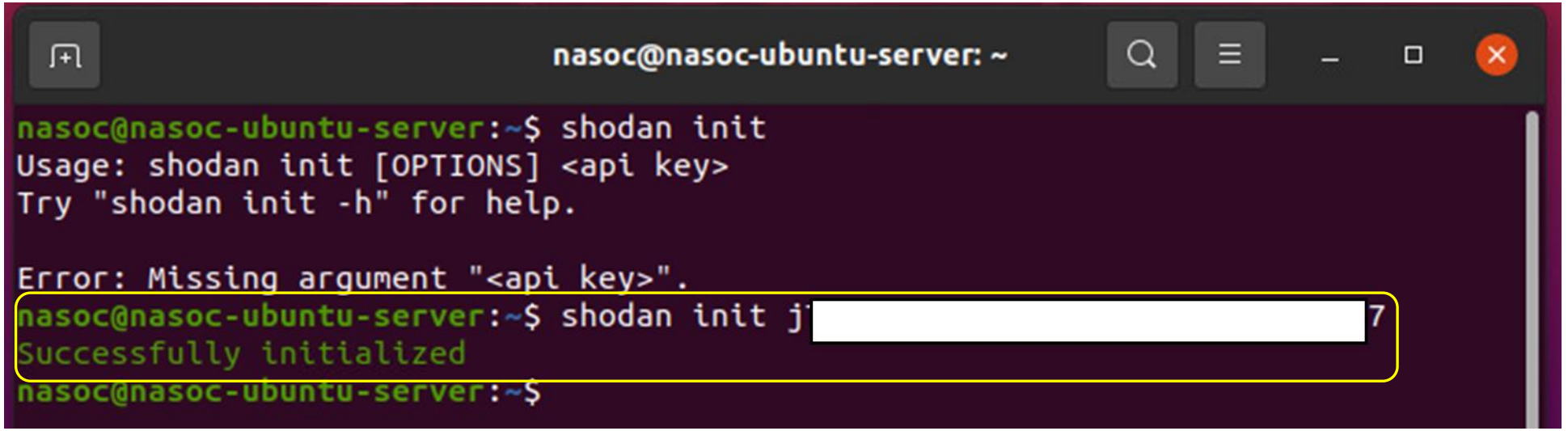
- 兩種方式取得API Key
  1. 點選Account，進入後會寫在API Key
  2. 在Developer頁面的右上角，點擊Show API Key





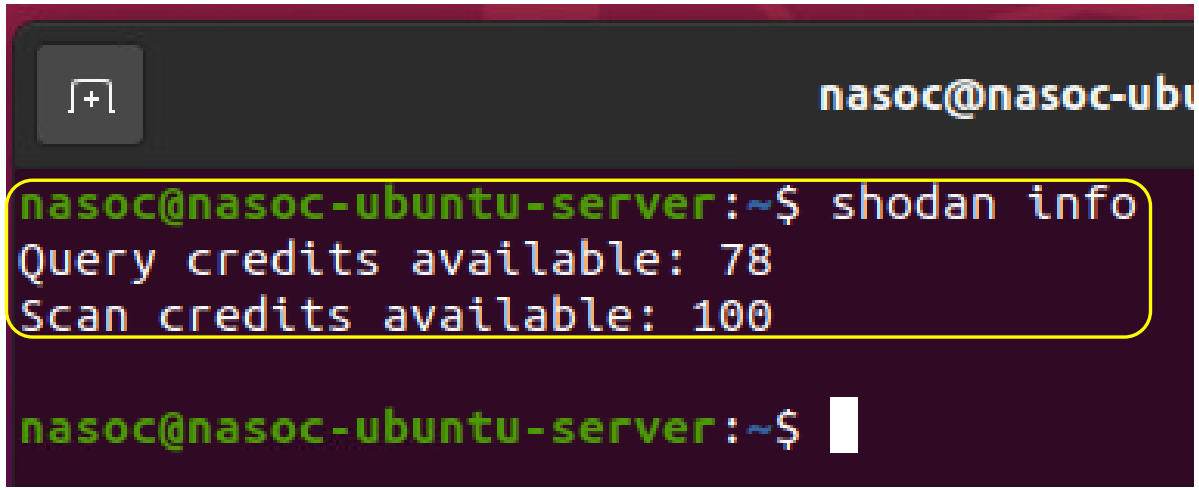
初始化Shodan服務

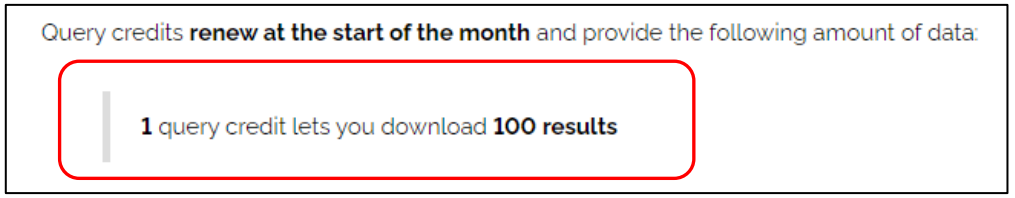
- 請保管好個人帳號的API Key，否則可能會被外人偷用帳號內的點數
- 使用Shodan服務前，要先經過初始化設定
  - shodan init <api-key>



查詢點數數量

- 下載資料前，要先知道個人帳號剩下多少下載點數
  - shodan info



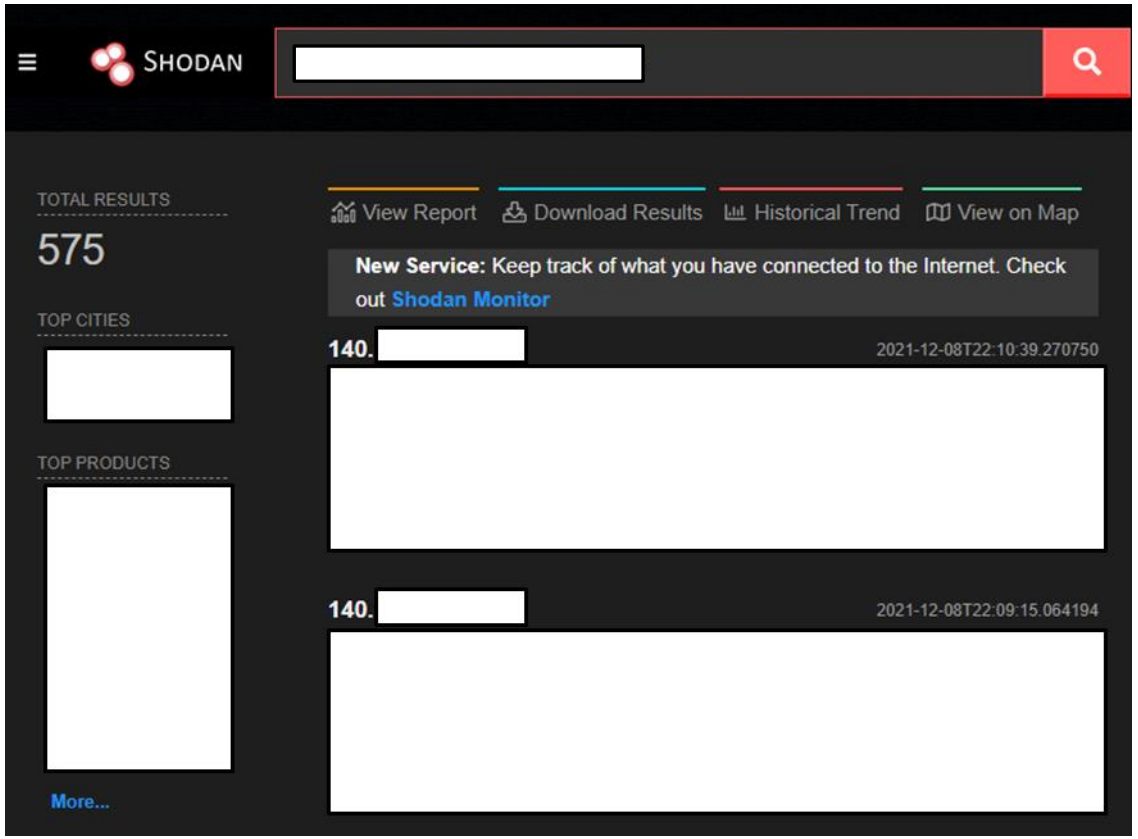


查詢目標數量

- 下載資料前，要先知道目標有多少筆資料
  - shodan count <搜尋條件> *

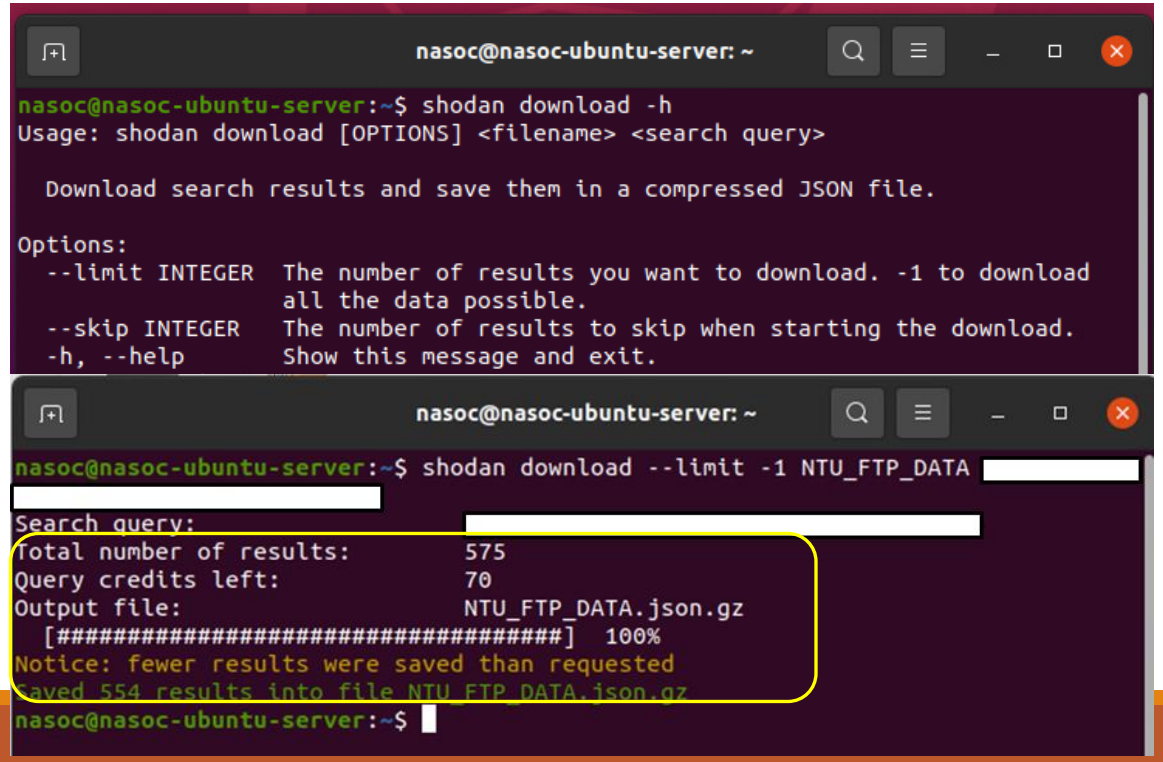
```
nasoc@nasoc-ubuntu
nasoc@nasoc-ubuntu-server:~$ shodan count -h
Usage: shodan count [OPTIONS] <search query>

  Returns the number of results for a search

Options:
  -h, --help  Show this message and exit.
nasoc@nasoc-ubuntu-server:~$
```

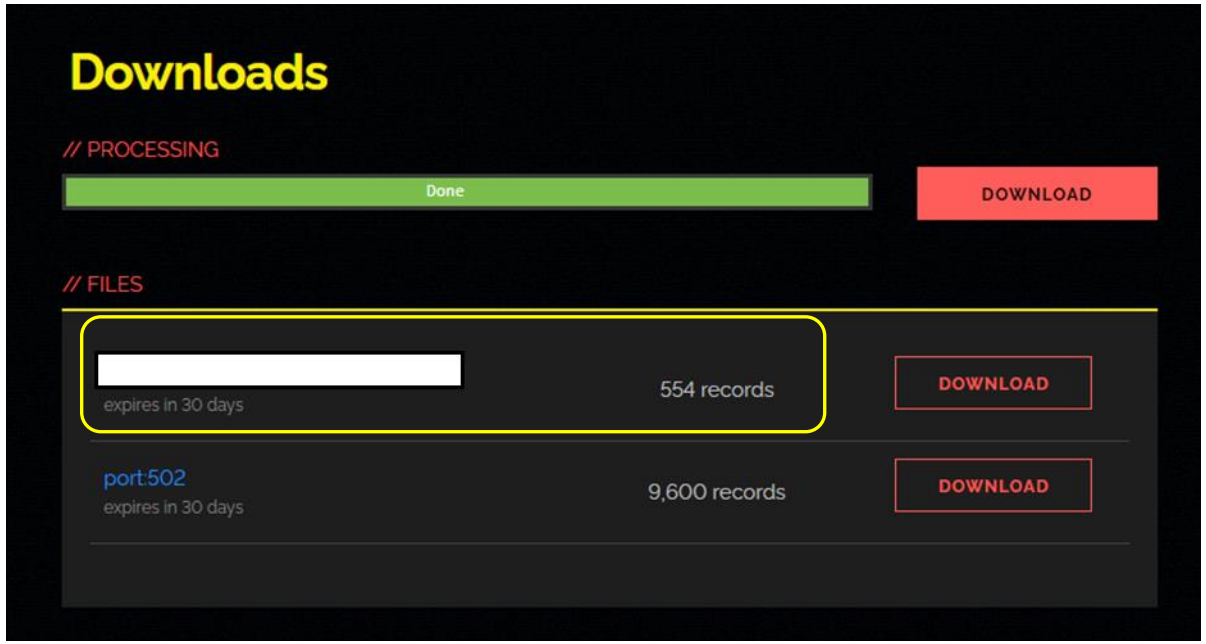
```
nasoc@nasoc-ubuntu-server: ~
nasoc@nasoc-ubuntu-server:~$ shodan count [redacted]
[redacted]
nasoc@nasoc-ubuntu-server:~$ shodan count [redacted]
[redacted]
nasoc@nasoc-ubuntu-server:~$ shodan count [redacted]
[redacted]
nasoc@nasoc-ubuntu-server:~$
```



下載Shodan資料

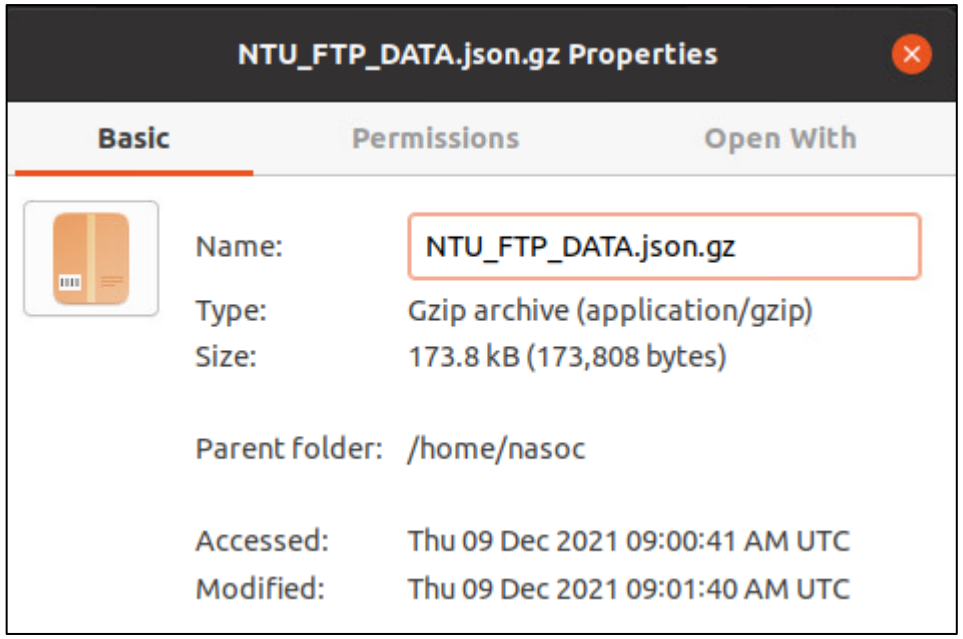
- 確認目標數量和下載點數後，就可以進行資料下載
  - shodan download [OPTIONS] <儲存檔案名稱> <搜尋條件>
- 使用命令列下載或網頁下載的檔案內容都相同

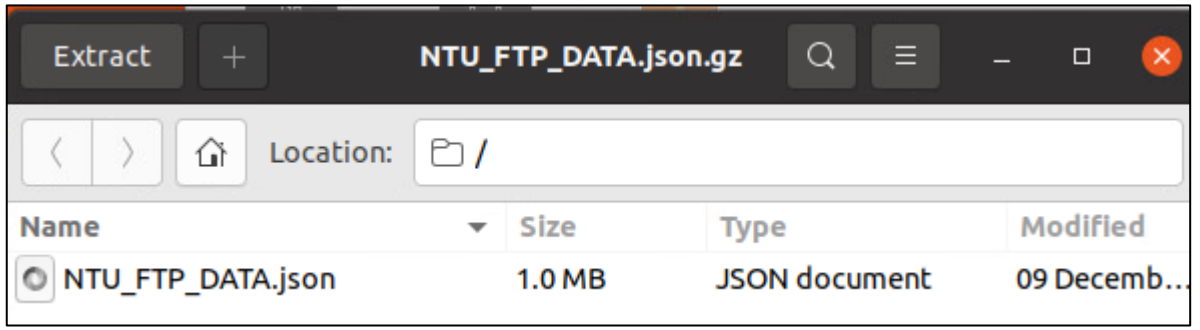




下載資料的說明

- 下載資料時，Shodan會先把資料壓縮成「.gz」的壓縮檔格式
- 原始資料要經過解壓縮後才能取出
- Shodan資料儲存的資料型態為「.json」



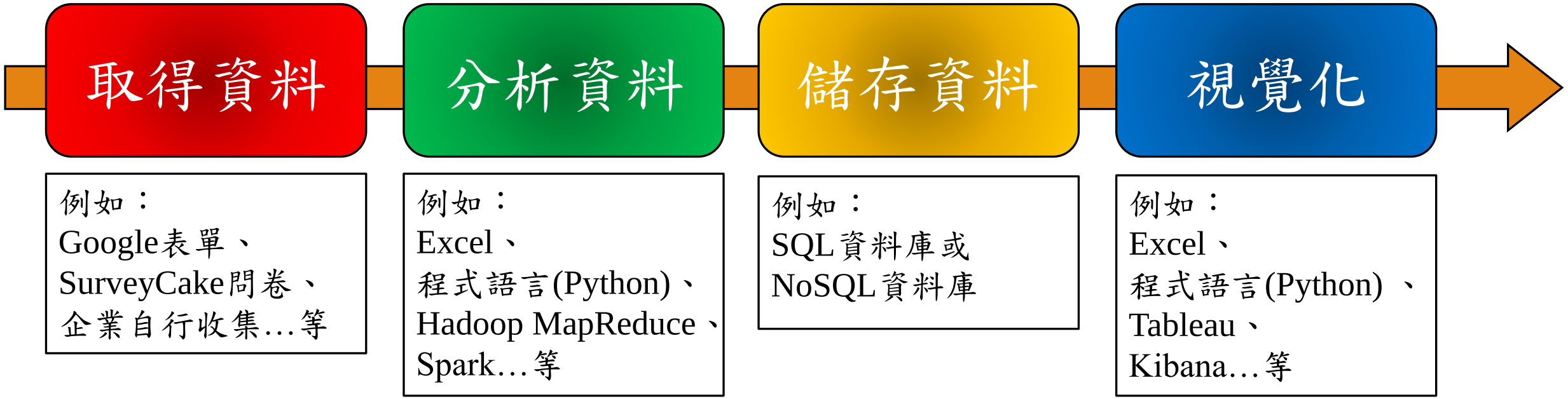


簡易的Shodan資料分析

前言

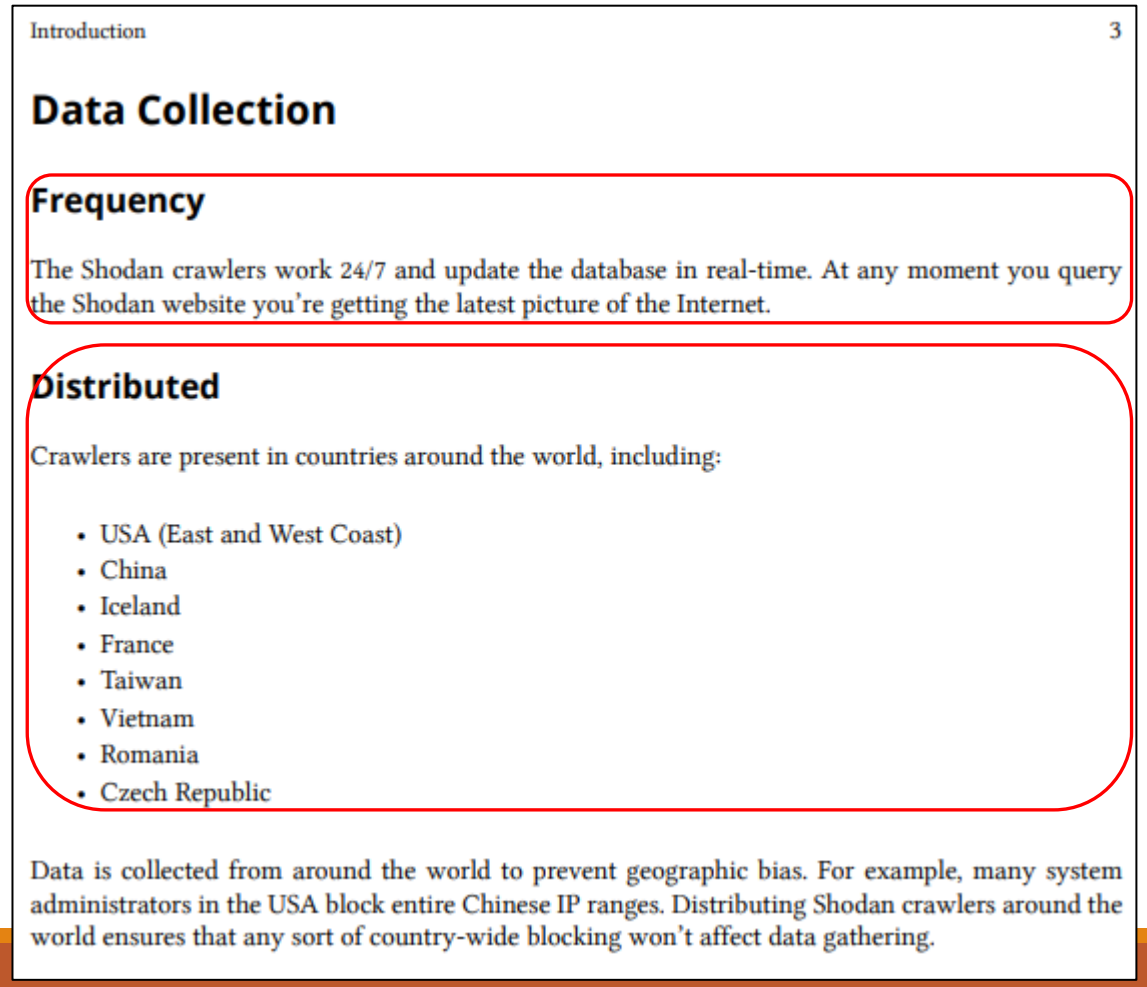
- 前一章節講解資料的下載，緊接著要進入到資料分析部分
- 資料分析的工具可以自行開發或使用商業軟體
- 本章節將使用Shodan套件、Excel做說明

資料分析步驟



引用的資料來源：
https://www.largitdata.com/blog_detail/20190725
https://blog.tibame.com/?p=17894

Shodan資料收集說明



Introduction 3

Data Collection

Frequency

The Shodan crawlers work 24/7 and update the database in real-time. At any moment you query the Shodan website you're getting the latest picture of the Internet.

Distributed

Crawlers are present in countries around the world, including:

- USA (East and West Coast)
- China
- Iceland
- France
- Taiwan
- Vietnam
- Romania
- Czech Republic

Data is collected from around the world to prevent geographic bias. For example, many system administrators in the USA block entire Chinese IP ranges. Distributing Shodan crawlers around the world ensures that any sort of country-wide blocking won't affect data gathering.

- 限制
  1. 不保證可以在短時間內獲得最新資訊，最晚一個月內會更新資料
  2. 每次更新時，上次的資料不一定馬上刪除

爬蟲(crawlers)基本演算法

Randomized

The basic algorithm for the crawlers is:

1. Generate a random IPv4 address
2. Generate a random port to test from the list of ports that Shodan understands
3. Check the random IPv4 address on the random port and grab a banner
4. Goto 1

This means that the crawlers don't scan incremental network ranges. The crawling is performed completely random to ensure a uniform coverage of the Internet and prevent bias in the data at any given time.

Shodan資訊元素—Banner & Metedata

Banner

The basic unit of data that Shodan gathers is the **banner**. The banner is textual information that describes a service on a device. For web servers this would be the headers that are returned or for Telnet it would be the login screen.

The content of the banner varies 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
```

Device Metadata

In addition to the banner, Shodan also grabs meta-data about the device such as its geographic location, hostname, operating system and more (see Appendix A). Most of the meta-data is searchable via the main Shodan website, however a few fields are only available to users of the developer API.

Appendix A: Banner Specification

For the latest list of fields that the banner contains please visit the online documentation[32].

A banner may contain the following properties/ fields:

General Properties

Name	Description	Example
asn	Autonomous system number	AS4837
data	Main banner for the service	HTTP/1.1 200...
ip	IP address as an integer	493427495
ip_str	IP address as a string	199.30.15.20
ipv6	IPv6 address as a string	2001:4860:4860::8888
port	Port number for the service	80
timestamp	Date and time the information was collected	2014-01-15T05:49:56.283713
hash	Numeric hash of the *data* property	
hostnames	List of hostnames for the IP	["shodan.io", "www.shodan.io"]
domains	List of domains for the IP	["shodan.io"]
link	Network link type	Ethernet or modem
location	Geographic location of the device	*see below*
opts	Supplemental/ experimental data not contained in main banner	
org	Organization that is assigned the IP	Google Inc.
isp	ISP that is responsible for the IP space	Verizon Wireless
os	Operating system	Linux
uptime	Uptime of the IP in minutes	50
tags	List of tags that describe the purpose of the device (Enterprise-only)	["ics", "vpn"]
transport	Type of transport protocol used to collect banner; either "udp" or "tcp"	tcp

[32] https://developer.shodan.io/api/banner-specification

JSON格式簡介


```
[
        {
                "timestamp":"2021-12-09T14:44:55.289866",
                "isp":"DaDa Broadband LTD.",
                "asn":"AS18419",
                "port":80,
                "transport":"tcp",
                "domains":["da.net.tw"],
                "ip_str":"61.60.203.179"
        }
]
```


JSON（**J**ava**S**cript **O**bject **N**otation, /ˈdʒeɪsən/）是由道格拉斯·克羅克福特構想和設計的一種輕量級資料交換格式。其內容由屬性和值所組成，因此也有易於閱讀和處理的優勢。JSON是獨立於程式語言的資料格式，其不僅是JavaScript的子集，也採用了C語言家族的習慣用法，目前也有許多程式語言都能夠將其解析和字串化，其廣泛使用的程度也使其成為通用的資料格式。

簡介 [編輯]

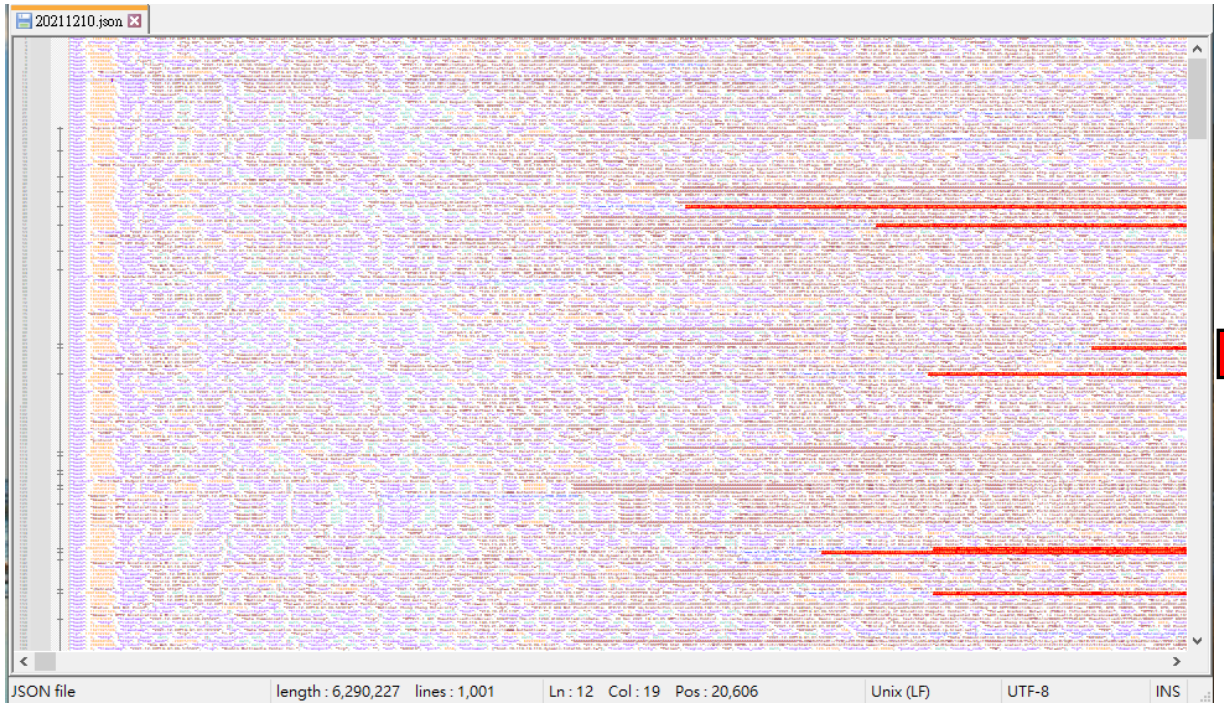
JSON格式是1999年《*JavaScript Programming Language, Standard ECMA-262 3rd Edition*》的子集合，所以可以在JavaScript以`eval()`函式（javascript通過eval()呼叫解析器）讀入。不過這並不代表JSON無法使用於其他語言，事實上幾乎所有與網路開發相關的語言都有JSON函式庫。

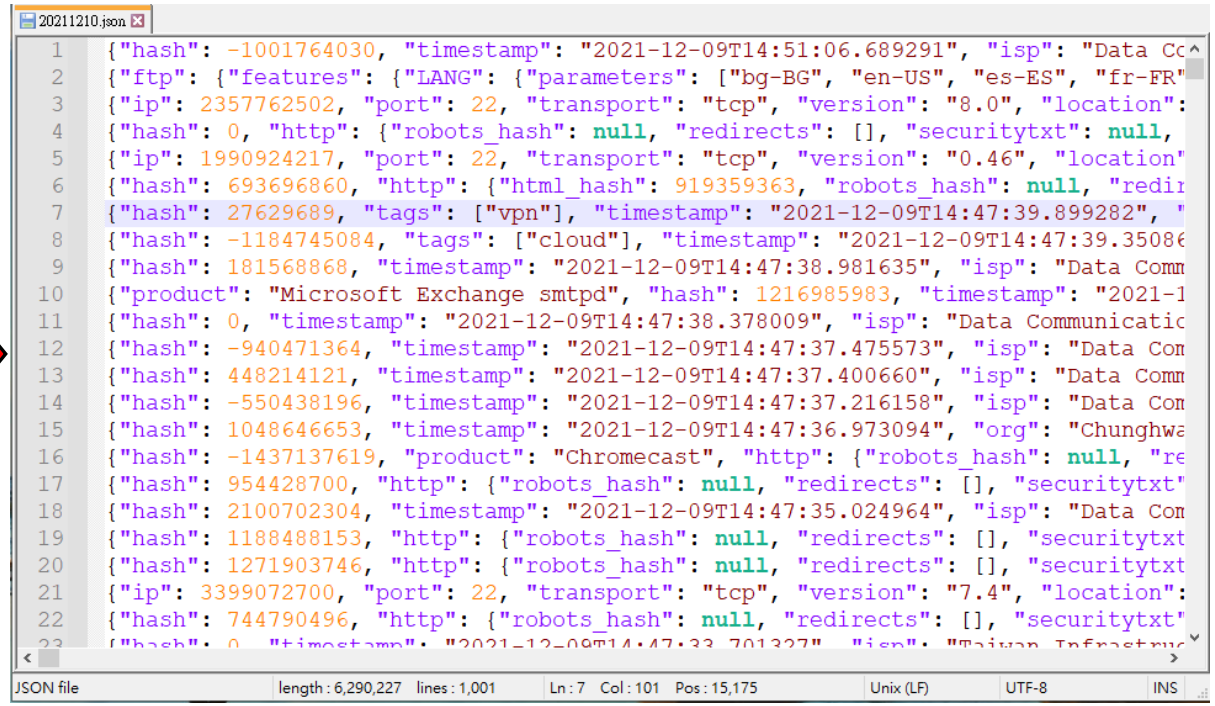
JSON的基本資料類型：

- 數值：十進位數，不能有前導0，可以為負數，可以有小數部分。還可以用`e`或者`E`表示指數部分。不能包含非數，如NaN。不區分整數與浮點數。JavaScript用雙精度浮點數表示所有數值。
- 字串：以雙引號`""`括起來的零個或多個Unicode碼位。支援反斜槓開始的跳脫字元序列。
- 布林值：表示為`true`或者`false`。
- 陣列：有序的零個或者多個值。每個值可以為任意類型。序列表使用方括號`[`，`]`括起來。元素之間用逗號`,`分割。形如：`[value, value]`
- 物件：若干無序的「鍵-值對」(key-value pairs)，其中鍵只能是字串[1]。建議但不強制要求物件中的鍵是獨一無二的。物件以花括號`{`開始，並以`}`結束。鍵-值對之間使用逗號分隔。鍵與值之間用冒號`:`分割。
- 空值：值寫為`null`

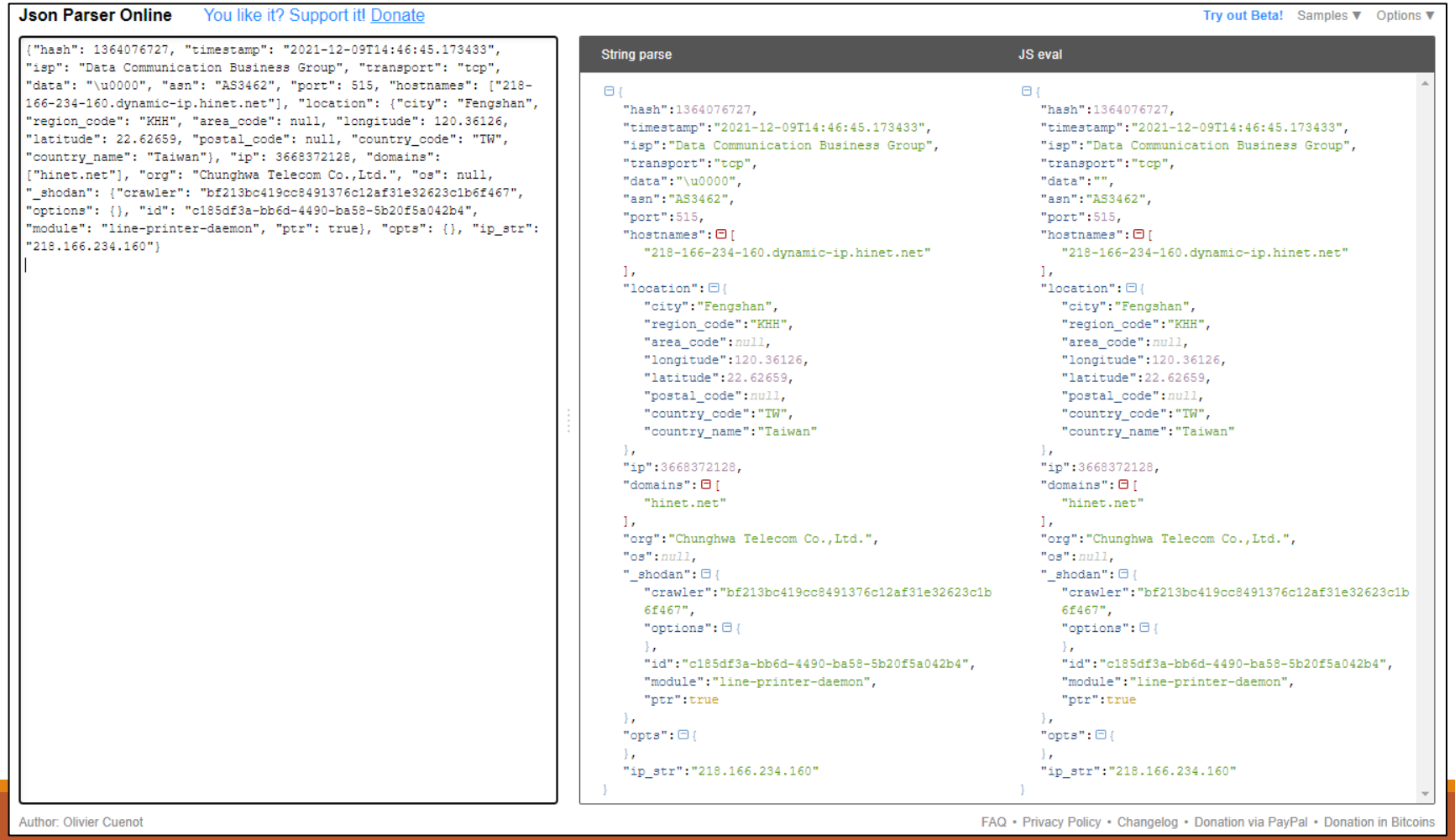
引用資料來源：https://zh.wikipedia.org/zh-tw/JSON

原始Shodan資料範例

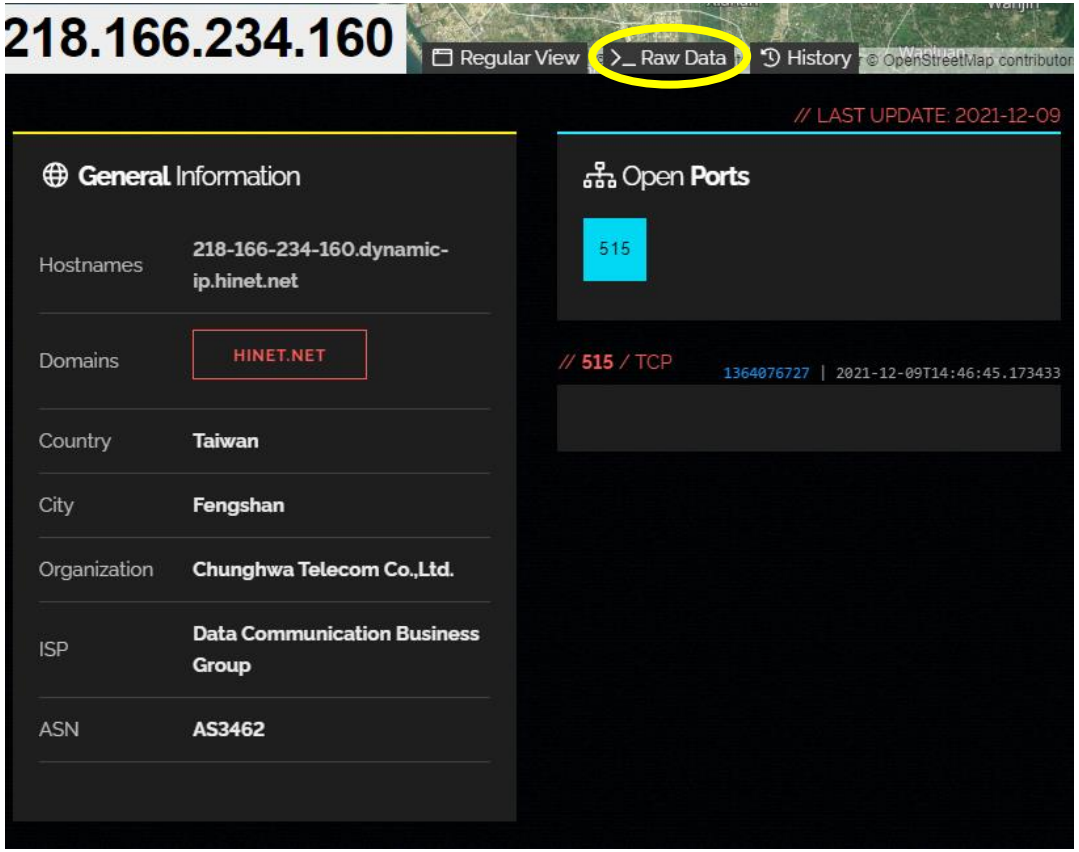


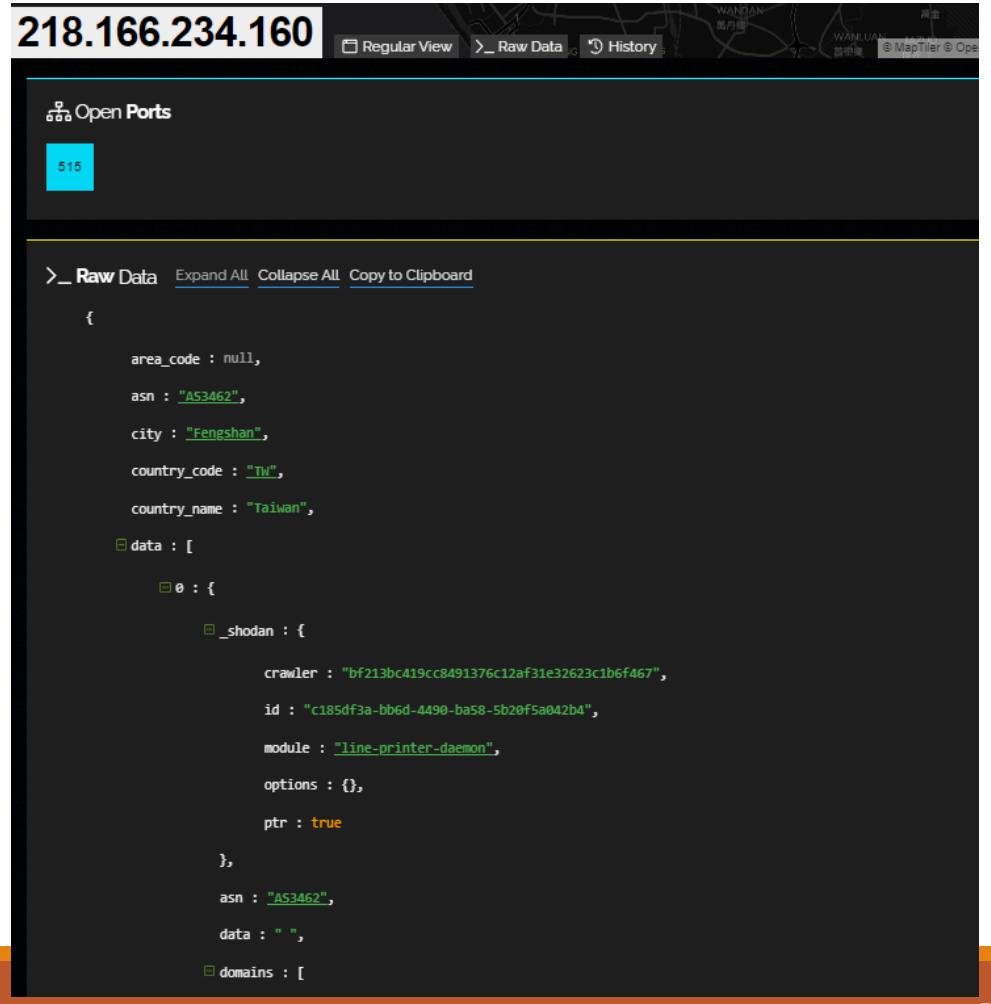


單一Shodan資料範例



單一Shodan資料範例(續)



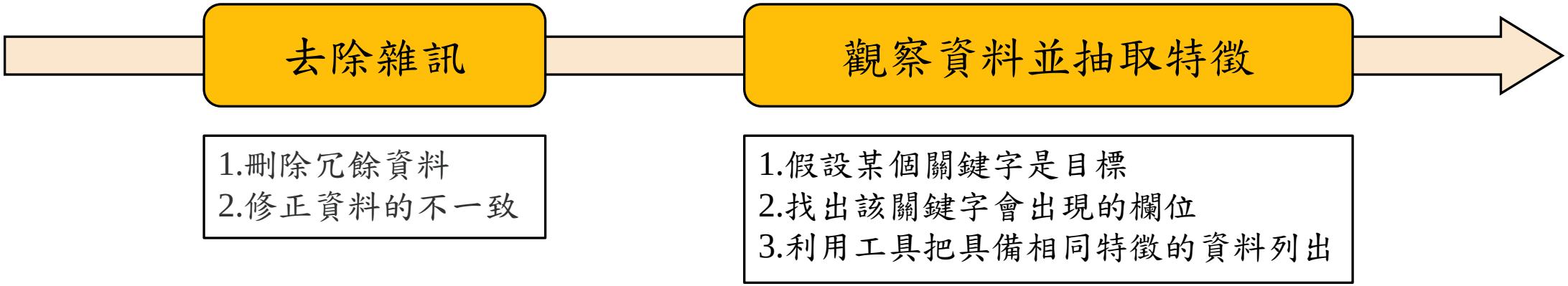


資料分析說明

- 進行分析前，需要做資料前處理
- 資料前處理完成後，才開始從細節上對資料進行分析

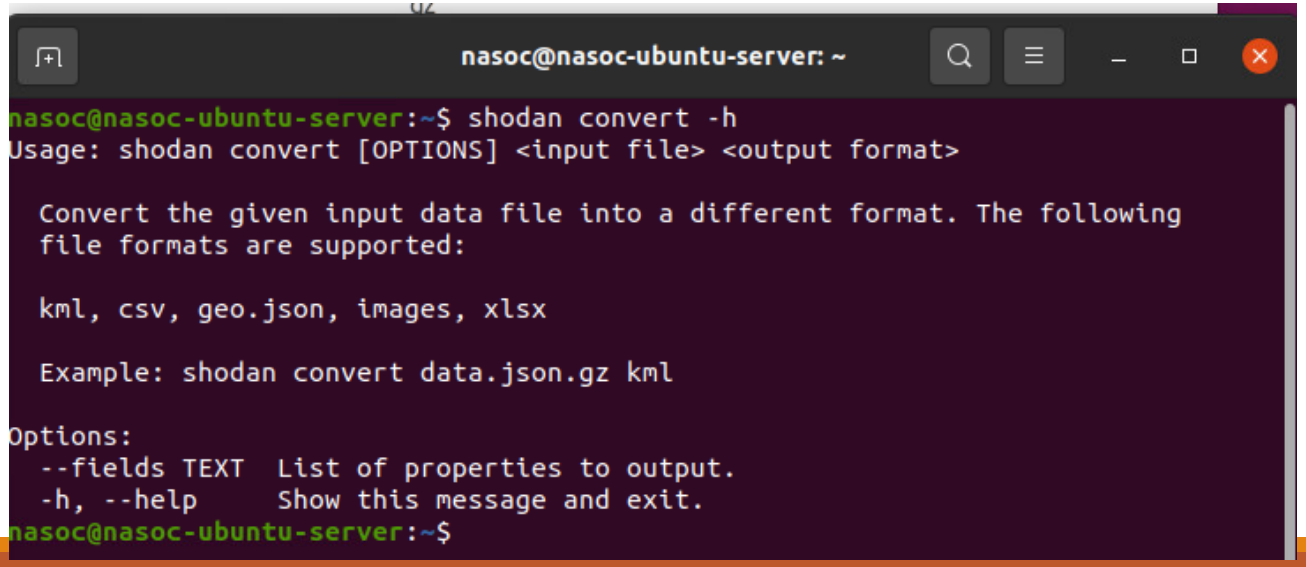
資料來源：https://ithelp.ithome.com.tw/articles/10231293

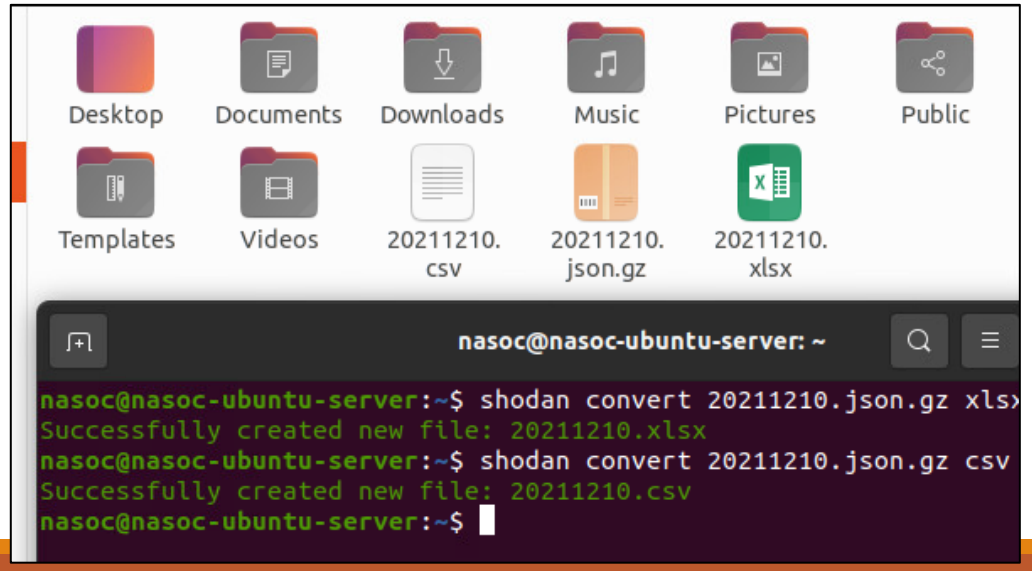
簡化後的資料分析步驟


去除雜訊
觀察資料並抽取特徵
1.刪除冗餘資料
2.修正資料的不一致
1.假設某個關鍵字是目標
2.找出該關鍵字會出現的欄位
3.利用工具把具備相同特徵的資料列出

內建套件的資料格式轉換

- 原始資料有太多資訊，比較難以直接檢視資料
- 套件中有包含資料格式的轉換功能，讓使用者方便轉換格式資料
  - shodan convert <要轉檔的檔案> <轉換後的格式>
- 轉換後的資料比較容易查閱內容





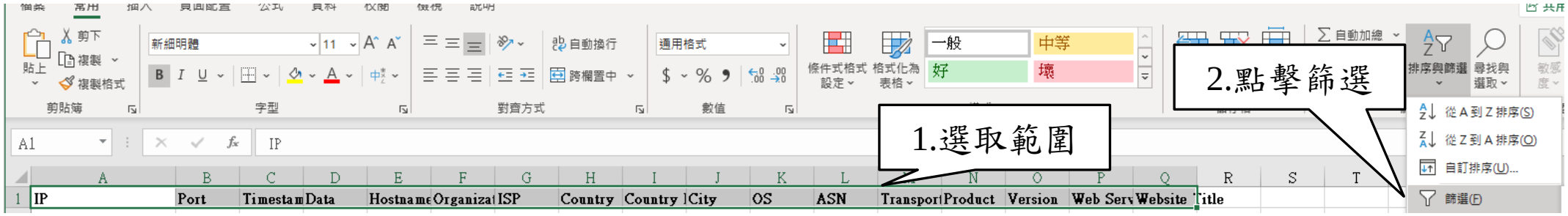
轉換後的資料範例(csv)

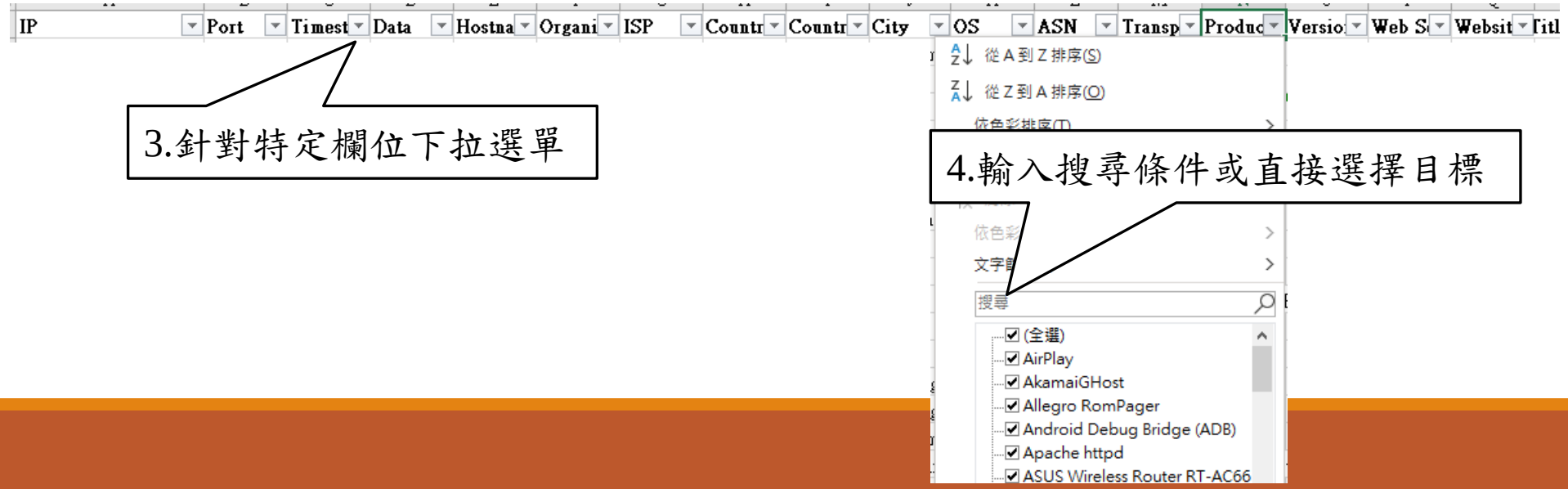
data	hostnames	ip	ip_str	ipv6	org	isp	location	location.cit	locatio	location	location	os	asn	port	tags	timestamp
+OK Dovecot ready. +OK	mail.fast.org.tw	998085218	59.125.146.98		Chunghwa Telecom Co	Data Communication Busin	TW	Fengshan	Taiwan	22.62659	120.36126		AS3462	110		2021/12/9 14:51
220 FTP Server ready. 53(	59-124-162-194	998023874	59.124.162.194		Chunghwa Telecom Co	Data Communication Busin	TW	Taipei	Taiwan	25.04776	121.53185		AS3462	21		2021/12/9 14:49
SSH-2.0-OpenSSH_8.0 Ke		2357762502	140.136.153.198		Ministry of Education (	Fu Jen Catholic University	TW	Banqiao	Taiwan	25.01427	121.46719		AS38845	22		2021/12/9 14:47
	120-114-141-20	2020773320	120.114.141.200		Ministry of Education (	National Cheng Kung Unive	TW	Tainan	Taiwan	22.99083	120.21333		AS18177	8010		2021/12/9 14:47
SSH-2.0-dropbear_0.46 Ke	118-171-23-185	1990924217	118.171.23.185		Chunghwa Telecom Co	Data Communication Busin	TW	Tainan	Taiwan	22.99083	120.21333		AS3462	22		2021/12/9 14:47
HTTP/1.1 200 OK Date: T	114-39-177-218	1915204058	114.39.177.218		Chunghwa Telecom Co	Data Communication Busin	TW	Tainan	Taiwan	22.99083	120.21333		AS3462	80		2021/12/9 14:47
Firmware: 1 Hostname: Vig	61-222-88-148.I	1037981844	61.222.88.148		Chunghwa Telecom Co	Data Communication Busin	TW	Taoyuan City	Taiwan	24.99368	121.29696		AS3462	1723	vpn	2021/12/9 14:47
HTTP/1.1 302 FOUND Cc	93.151.236.35.b	602707805	35.236.151.93		Google LLC	Google LLC	TW	Taipei	Taiwan	25.04776	121.53185		AS15169	8443	cloud	2021/12/9 14:47
\xff\xfd\x01\xff\xfd\x1f\xff	59-127-33-64.hi	998187328	59.127.33.64		Chunghwa Telecom Co	Data Communication Busin	TW	Taitung	Taiwan	22.75991	121.14457		AS3462	2323		2021/12/9 14:47
220 TWTPS201.tpvaoc.con	tpex.tpvaoc.com	3544769455	211.72.227.175		Chunghwa Telecom Co	Data Communication Busin	TW	Banqiao	Taiwan	25.01427	121.46719		AS3462	465		2021/12/9 14:47
	114-34-63-212.I	1914847188	114.34.63.212		Chunghwa Telecom Co	Data Communication Busin	TW	Yilan	Taiwan	24.757	121.753		AS3462	9530		2021/12/9 14:47
RTSP/1.0 200 OK CSeq: 1	218-161-112-11	3668013166	218.161.112.110		Chunghwa Telecom Co	Data Communication Busin	TW	Tainan	Taiwan	22.99083	120.21333		AS3462	554		2021/12/9 14:47
RTSP/1.0 200 OK Server:	125-227-71-77.I	2112046925	125.227.71.77		Data Communication B	Data Communication Busin	TW	Taichung	Taiwan	24.1469	120.6839		AS3462	554		2021/12/9 14:47
head\x03\x00\x00\x00\x00 '	220-132-167-71	3699681095	220.132.167.71		Chunghwa Telecom Co	Data Communication Busin	TW	Taichung	Taiwan	24.1469	120.6839		AS3462	6036		2021/12/9 14:47
NetBIOS Response: Serve	114-40-120-226	1915255010	114.40.120.226		Chunghwa Telecom Co	Data Communication Busin	TW	Kaohsiung	Taiwan	22.61626	120.31333		AS3462	137		2021/12/9 14:47
HTTP/1.1 403 Forbidden (	112-105-56-45.a	1885943853	112.105.56.45		New Century InfoCom	Taiwan Infrastructure Netw	TW	Fengyuan	Taiwan	24.25	120.71694		AS18049	8008	iot	2021/12/9 14:47
HTTP/1.1 200 OK Content	1-161-69-208.dy	27346384	1.161.69.208		Chunghwa Telecom Co	Data Communication Busin	TW	Taipei	Taiwan	25.04776	121.53185		AS3462	80		2021/12/9 14:47
HTTP/1.1 400 Bad Request	210-65-240-7.hi	3527536647	210.65.240.7		Chunghwa Telecom Co	Data Communication Busin	TW	Taipei	Taiwan	25.04776	121.53185		AS3462	1723		2021/12/9 14:47
HTTP/1.1 200 OK Date: T	211-22-230-144	3541493392	211.22.230.144		Chunghwa Telecom Co	Data Communication Busin	TW	Tainan	Taiwan	22.99083	120.21333		AS3462	82		2021/12/9 14:47
HTTP/1.1 302 Found Loca	124-108-171-12	2087496572	124.108.171.124		Taiwan Fixed Network	Taiwan Fixed Network, Tel	TW	Taipei	Taiwan	25.04776	121.53185		AS9924	8008		2021/12/9 14:47
SSH-2.0-OpenSSH_7.4 Ke	188-187-153-20	3399072700	202.153.187.188		UnigateNet, Internet Se	AboveNet Communications	TW	Taipei	Taiwan	25.04776	121.53185		AS17408	22		2021/12/9 14:47
HTTP/1.1 302 Found Loca		2020423316	120.109.54.148		Ministry of Education (	Taiwan Academic Network	TW	Taichung	Taiwan	24.1469	120.6839		AS1659	8008		2021/12/9 14:47
	123-205-57-165	2077047205	123.205.57.165		New Century InfoCom	Taiwan Infrastructure Netw	TW	Zhongxing New	Taiwan	23.95908	120.68516		AS18049	8009		2021/12/9 14:47
HTTP/1.1 400 Bad Request	visit.keznews.co	2823859236	168.80.172.36		Cooperative Investment	QT Inc.	TW	Taipei	Taiwan	25.04776	121.53185		AS24567	8200		2021/12/9 14:47
HTTP/1.1 200 OK X-Pow		2356615211	140.119.24.43		Ministry of Education (	Taiwan Academic Network	TW	Xindian	Taiwan	24.96005	121.53892		AS1659	3000		2021/12/9 14:47
HTTP/1.1 200 OK Content	220-132-123-14	3699669902	220.132.123.142		Chunghwa Telecom Co	Data Communication Busin	TW	Tainan	Taiwan	22.99083	120.21333		AS3462	80		2021/12/9 14:47
VPN (IKE) Initiator SPI: 7	114-32-219-221	1914756061	114.32.219.221		Chunghwa Telecom Co	Data Communication Busin	TW	Taipei	Taiwan	25.04776	121.53185		AS3462	500	vpn	2021/12/9 14:47
SSH-2.0-OpenSSH_7.7 \n'	118-168-135-7.(	1000756103	118.168.135.7		Chunghwa Telecom Co	Data Communication Busin	TW	Taipei	Taiwan	25.04776	121.53185		AS3462	22		2021/12/9 14:47

轉換後的資料範例(xlsx)

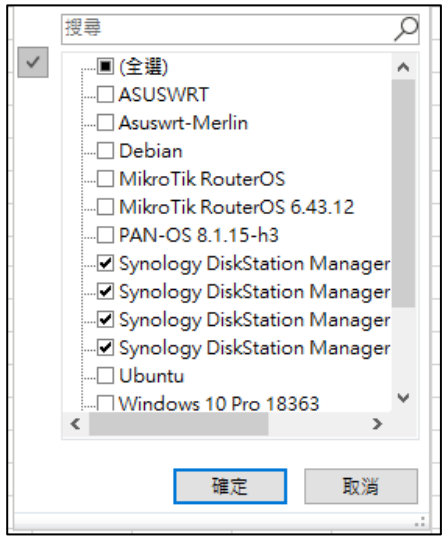
IP	Port	Timestamp	Data	Hostnames	Organization	ISP	Country	Country ISO Code	City	OS	ASN	Transport	Product	Version	Web Server	Website Title
210.242.9	143	2021-12-09T1	* OK [CAPABILITY	210-242-91-7.h	Chunghwa Telecc	Data Comr	Taiwan	TW	Miaoli		AS3462	tcp				
220.141.1	135	2021-12-09T1	Microsoft RPC Endpo	220-141-196-17	Chunghwa Telecc	Data Comr	Taiwan	TW	Taoyuan City		AS3462	tcp	Microsoft RPC Endpoint Mapper			
125.227.2	465	2021-12-09T1	220 ESMTP MAIL S	mail.jetvox.com	Chunghwa Telecc	Data Comr	Taiwan	TW	Taipei		AS3462	tcp				
125.227.6	80	2021-12-09T1	HTTP/1.1 401 Unauth	125-227-67-19.	Data Communicat	Data Comr	Taiwan	TW	Taichung		AS3462	tcp	mini_httpd	1.19 19dec	mini_httpd/1.19	401 Unauthorized
1.171.116	8800	2021-12-09T	14:47:25.341681	1-171-116-85.d	Chunghwa Telecc	Data Comr	Taiwan	TW	Taipei		AS3462	tcp				
125.228.9	554	2021-12-09T1	RTSP/1.0 401 Unauth	125-228-91-80.	Chunghwa Telecc	Data Comr	Taiwan	TW	Taipei		AS3462	tcp				
1.170.54.	443	2021-12-09T	14:47:25.075744	1-170-54-144.d	Chunghwa Telecc	Data Comr	Taiwan	TW	Fengyuan		AS3462	tcp				
114.33.10	80	2021-12-09T1	HTTP/1.1 200 OK D	114-33-100-169	Chunghwa Telecc	Data Comr	Taiwan	TW	Douliu		AS3462	tcp	Boa Web Serv	$1	Boa/0.94.14rc2	
116.241.2	80	2021-12-09T1	HTTP/1.1 200 OK D	116-241-217-49	TBC	TBC	Taiwan	TW	Taoyuan City		AS131596	tcp	Boa Web Serv	$1	Boa/0.94.14rc21	
114.32.39	554	2021-12-09T1	RTSP/1.0 200 OK CS	114-32-39-240.	Chunghwa Telecc	Data Comr	Taiwan	TW	Taipei		AS3462	tcp				
1.162.57.	2000	2021-12-09T1	\x01\x00\x00\x00	1-162-57-146.d	Chunghwa Telecc	Data Comr	Taiwan	TW	Taipei		AS3462	tcp	MikroTik bandwidth-test server			
34.81.71.2	22	2021-12-09T1	SSH-2.0-OpenSSH_7.	220.71.81.34.b	Google LLC	Google LL	Taiwan	TW	Taipei		AS396982	tcp	OpenSSH	7.4		
59.127.10	80	2021-12-09T1	HTTP/1.1 200 OK Se	59-127-102-8.h	Chunghwa Telecc	Data Comr	Taiwan	TW	Hualien City		AS3462	tcp	Cross Web Server		Cross Web Serv	DVR Components
111.241.2	81	2021-12-09T	14:47:23.666712	111-241-218-12	Chunghwa Telecc	Data Comr	Taiwan	TW	Taipei		AS3462	tcp				
120.107.1	8008	2021-12-09T1	HTTP/1.1 302 Found	Location: https:	Ministry of Educa	Taiwan Ac	Taiwan	TW	Chang-hua		AS1659	tcp				
168.80.17	3001	2021-12-09T1	HTTP/1.1 400 Bad Re	visit.keznews.cc	Cooperative Inves	QT Inc.	Taiwan	TW	Taipei		AS24567	tcp				
220.135.1	123	2021-12-09T1	NTP protocolversion:	220-135-19-140	Chunghwa Telecc	Data Comr	Taiwan	TW	Taitung		AS3462	udp				
210.71.19	2323	2021-12-09T1	HTTP/1.0 404 FAIL	210-71-196-198	Data Communicat	Data Comr	Taiwan	TW	Taipei		AS3462	tcp				
103.10.20	80	2021-12-09T1	HTTP/1.1 200 OK Server: 01_16320	141 Yang Guan Ji	141 Yang (	Taiwan	TW	Tainan			AS45599	tcp			01_1632062562	
183.182.7	9998	2021-12-09T	14:47:22.215539		Asia Pacific Netw	60 Market	Taiwan	TW	Taichung		AS55303	tcp				
61.223.18	445	2021-12-09T1	SMB Status: Authen	61-223-187-245	Chunghwa Telecc	Data Comr	Taiwan	TW	Chang-hua	Windows 1	AS3462	tcp				
49.158.21	123	2021-12-09T1	NTP protocolversion:	49-158-216-72.	TFN MEDIA CO	UNION BI	Taiwan	TW	Hualien City		AS24164	udp				
140.126.1	8008	2021-12-09T1	HTTP/1.1 302 Found	Class5-27.cc-pc	Ministry of Educa	National C	Taiwan	TW	Miaoli		AS9916	tcp				
36.230.26	81	2021-12-09T	14:47:21.829061	36-230-26-82.d	Chunghwa Telecc	Data Comr	Taiwan	TW	Taoyuan City		AS3462	tcp				
114.33.18	80	2021-12-09T1	HTTP/1.1 200 OK C	114-33-189-240	Chunghwa Telecc	Data Comr	Taiwan	TW	Tainan		AS3462	tcp				
114.42.20	80	2021-12-09T1	HTTP/1.1 301 Moved	114-42-209-126	Chunghwa Telecc	Data Comr	Taiwan	TW	Chang-hua		AS3462	tcp	lighttpd	1.4.45	lighttpd/1.4.45	
114.33.2.8	80	2021-12-09T	14:47:21.378702	114-33-2-88.hir	Chunghwa Telecc	Data Comr	Taiwan	TW	Taichung		AS3462	tcp				

利用Excel的功能分析資料





驗證示範



測試驗證，例如
在瀏覽器上輸入IP
+ port

IP	Port	Timest	Data	Hostna	Organi	ISP	Countr	Countr	City	OS	ASN	Transp	Produc	Versio	Web S	Websit	Title
2	5000	2021-12-0	HTTP/1.1	220-135-2	Chunghwa	Data Com	Taiwan	TW	Fengshan	Synology I	AS3462	tcp	nginx	6.2.3-2542	nginx	DS918 - Synology DiskStation	
1	5000	2021-12-0	HTTP/1.1	114-35-24	Chunghwa	Data Com	Taiwan	TW	Banqiao	Synology I	AS3462	tcp	nginx	6.2.2-2492	nginx	Family-NAS - Synology DiskStation	
1	5000	2021-12-0	HTTP/1.1	180-177-1	kbro CO. I	kbro CO. I	Taiwan	TW	Hsinchu	Synology I	AS38841	tcp	nginx	7.0.1-4221	nginx	SkyDisk - Synology DiskStation	
2	5000	2021-12-0	HTTP/1.1	pc169-165	Taiwan Ac	Taiwan Ac	Taiwan	TW	Taitung	Synology I	AS1659	tcp	nginx	6.2.4-2555	nginx	NTTU - Synology DiskStation	
6	5001	2021-12-0	HTTP/1.1	33-238.63.	Savecom I	SaveCom I	Taiwan	TW	Taichung	Synology I	AS9676	tcp		6.2.2-2492	nginx	OFFICE - Synology DiskStation	
1	5001	2021-12-0	HTTP/1.1	122-116-5	Chunghwa	Data Com	Taiwan	TW	Taipei	Synology I	AS3462	tcp		6.2.3-2542	nginx	EDG2550 - Synology DiskStation	
2	5000	2021-12-0	HTTP/1.1	210-244-1	New Centu	Digital Un	Taiwan	TW	Tainan	Synology I	AS4780	tcp	nginx	6.2.4-2555	nginx	MKX5 - Synology NAS	
1	5000	2021-12-0	HTTP/1.1	111-246-3	Chunghwa	Data Com	Taiwan	TW	Yuanlin	Synology I	AS3462	tcp	nginx	6.2.4-2555	nginx	stfrancis - Synology NAS	

NoSQL資料庫簡介

什麼是 NoSQL 資料庫？

NoSQL 資料庫也稱為「非關聯式」、「NoSQL DB」或「非 SQL」，以強調它們能夠以不同於關聯式 (SQL) 資料庫 (利用資料列和資料表) 的方式，來處理大量快速變化的非結構化資料。

NoSQL 技術大約從 1960 年代開始就已存在，但由於資料環境變化，開發人員必須做出調整才能處理雲端、行動裝置、社交媒體和巨量資料所產生數量龐大且種類繁多的資料，因此突然大受歡迎。

從熱門名人推文到電子病歷中的救生資訊，迅速就能產生新的資料和資料類型。NoSQL 資料庫已發展成可協助開發人員快速建立資料庫系統，以儲存新的資訊，並讓該項資訊立即可供搜尋、彙總和分析。

彈性處理資料

NoSQL 可讓開發人員更自由、快速且彈性地變更結構描述和查詢，以配合資料需求。儲存為彙總的資訊可更輕鬆快速地反覆改善，而不需要事先設計結構描述。

NoSQL 資料庫的資料模型類型

大多數非關聯式高效能資料庫 (有時稱為「不只是 SQL」) 也可以處理高結構化資料，而不像關聯式 (SQL) 資料庫僅限於固定資料模型。

NoSQL 資料庫最常見的四種類型如下：

索引鍵/值

索引鍵/值使用雜湊表來儲存索引鍵/值組。當索引鍵為已知但與索引鍵建立關聯的值為未知時，最適合使用索引鍵/值類型。

文件

文件資料庫透過將整份文件分成稱為集合的群組，來延伸索引鍵/值資料庫的概念。它們支援巢狀索引鍵/值組，並允許查詢文件內的任何屬性。

單欄式

單欄式、寬資料行或資料行系列資料庫可以有效率地儲存資料，並在多列疏鬆資料間查詢，而且有利於在資料庫的特定資料行間查詢。

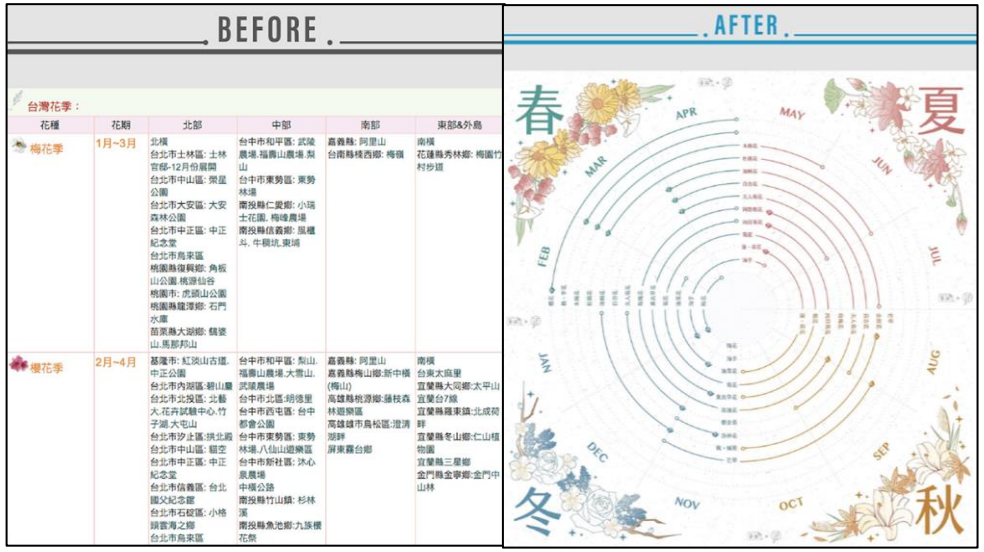
圖表

圖形資料庫使用以節點和邊緣來表示互連資料的模型 (例如社交網路中人與人之間的關係)，並提供簡化的儲存體及瀏覽複雜關聯性的功能。

資料來源：https://azure.microsoft.com/zh-tw/overview/nosql-database/

資料視覺化說明

- 資料視覺化是將複雜的資訊以視覺圖像呈現、簡化的過程
- 把生硬的資料變成簡單易懂的圖片、動畫、以及其他有效的溝通媒介，將艱澀理性的資訊變有趣、感性的內容



引用資料來源：https://relab.cc/blog/%E8%B3%87%E6%96%99%E8%A6%96%E8%A6%BA%E5%8C%96

結論

- Shodan是一個專門蒐集IoT設備資訊的搜尋引擎
- 如何在資安事件發生前或大規模漏洞攻擊前，利用Shodan找出學術網路中有漏洞的設備並進行通報，是目前北區ASOC團隊正在努力的方向

資料來源-1

1. CNN報導：https://money.cnn.com/2013/04/08/technology/security/shodan/
2. System Shock圖片來源： https://en.wikipedia.org/wiki/System_Shock
3. 巴哈電玩瘋報導： https://www.youtube.com/watch?v=n1ChelLmQIc
4. iT邦幫忙：https://ithelp.ithome.com.tw/articles/10218769
5. Bleepingcomputer報導： https://www.bleepingcomputer.com/news/security/compromised-docker-hosts-use-shodan-to-infect-more-victims/
6. PCMagazine報導： https://in.pcmag.com/security/146125/att-reveals-malware-targeting-millions-of-routers-iot-devices
7. 維基百科—JSON：https://zh.wikipedia.org/zh-tw/JSON
8. JSON線上解析器：http://json.parser.online.fr/

資料來源-2

1. Shodan官方網站：https://cli.shodan.io/
2. Github-Shodan套件：https://github.com/achillean/shodan-python
3. 大數據分析步驟-1：https://www.largitdata.com/blog_detail/20190725
4. 大數據分析步驟-2： https://blog.tibame.com/?p=17894
5. 微軟—NoSQL 資料庫：https://azure.microsoft.com/zh-tw/overview/nosql-database/
6. 資料分析說明：https://ithelp.ithome.com.tw/articles/10231293
7. 資料視覺化是什麼？：https://relab.cc/blog/%E8%B3%87%E6%96%99%E8%A6%96%E8%A6%BA%E5%8C%96
8. John Matherly (2017), Complete Guide to Shodan: Collect. Analyze. Visualize. Make Internet Intelligence Work for You, Leanpub.

報告完畢　　謝謝大家