

Open-Source Intelligence (OSINT)

Somesh Sanjay Rasal
Information Security Analyst, Amdocs
https://twitter.com/rasal_somesh

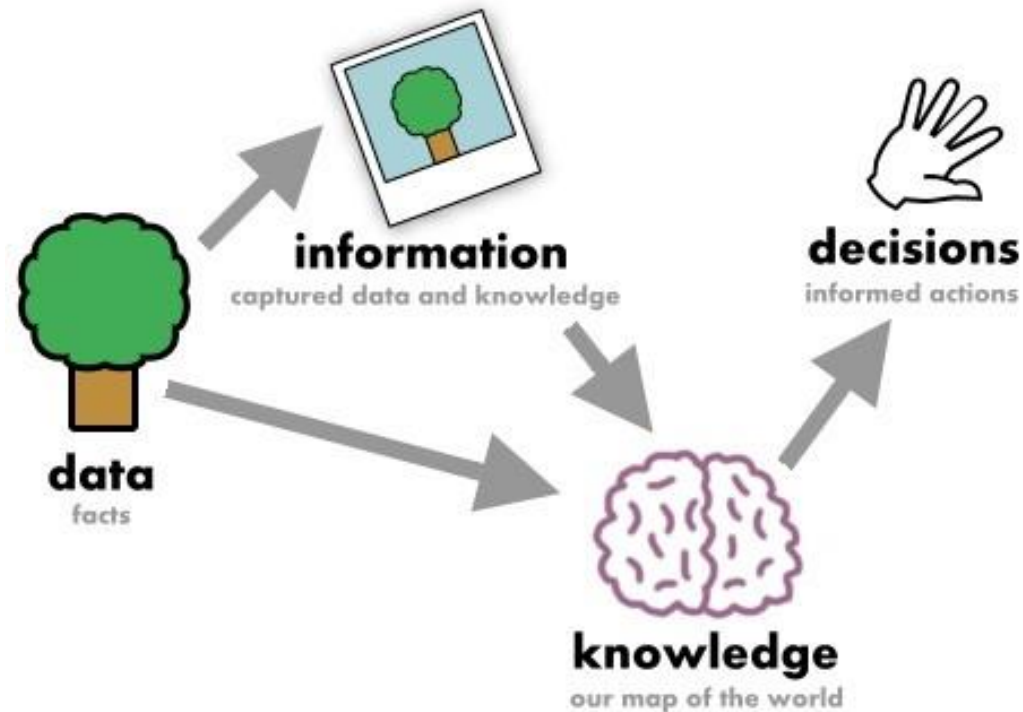
Agenda

To understand the basics of **Open-Source Intelligence**



OSINT

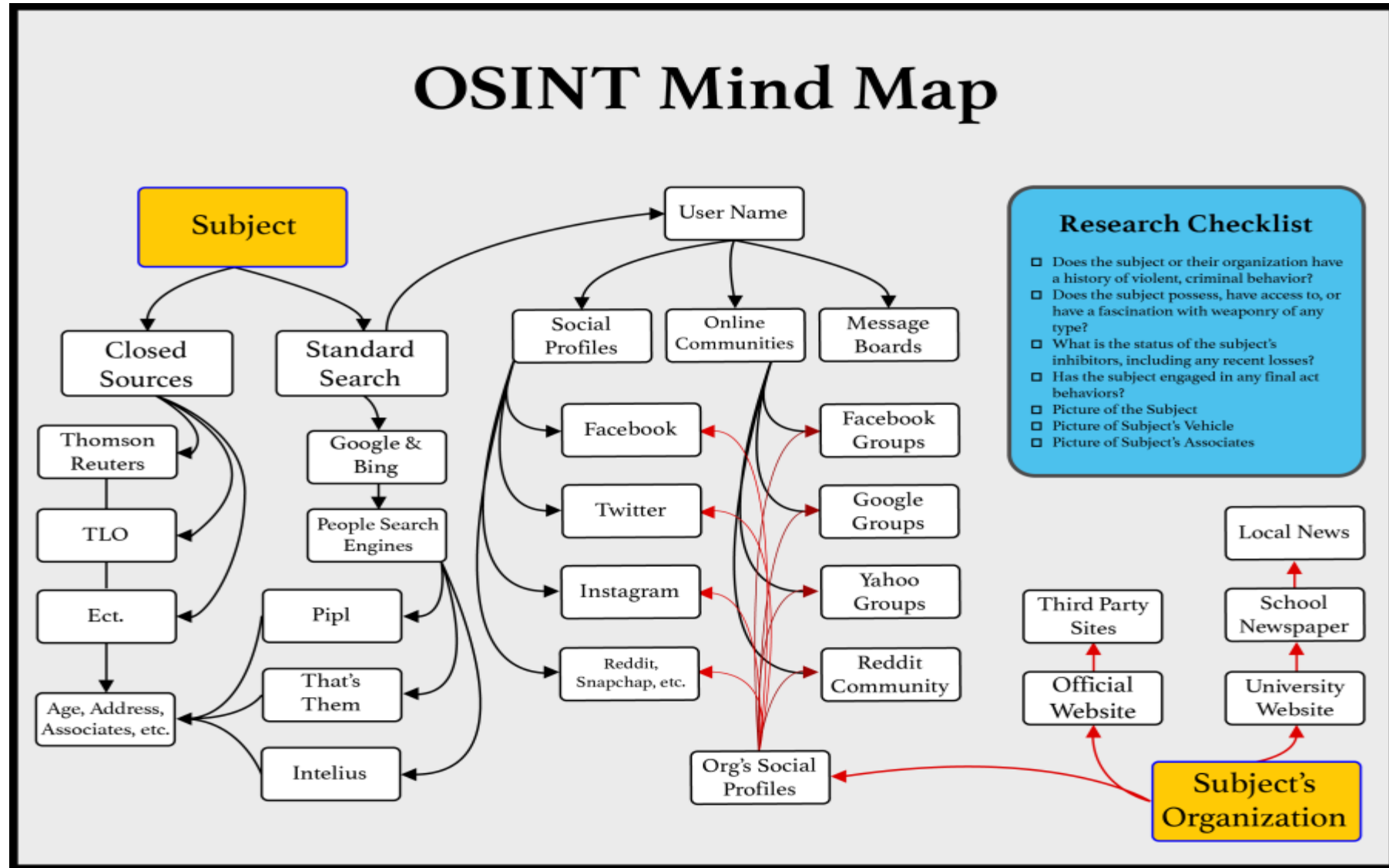
Open-**S**ource **I**NTelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context.



Source = https://en.wikipedia.org/wiki/Open-source_intelligence

OSINT Mind-map

Source = Google Images



Need of OSINT

- To detect and identify the data breaches
- Gather and Understand public sentiments on particular product or service
- Real time incident response for risky situations or places
- To identify external threats
- **Red Teams** = To identify and know more about victims for phishing and vishing

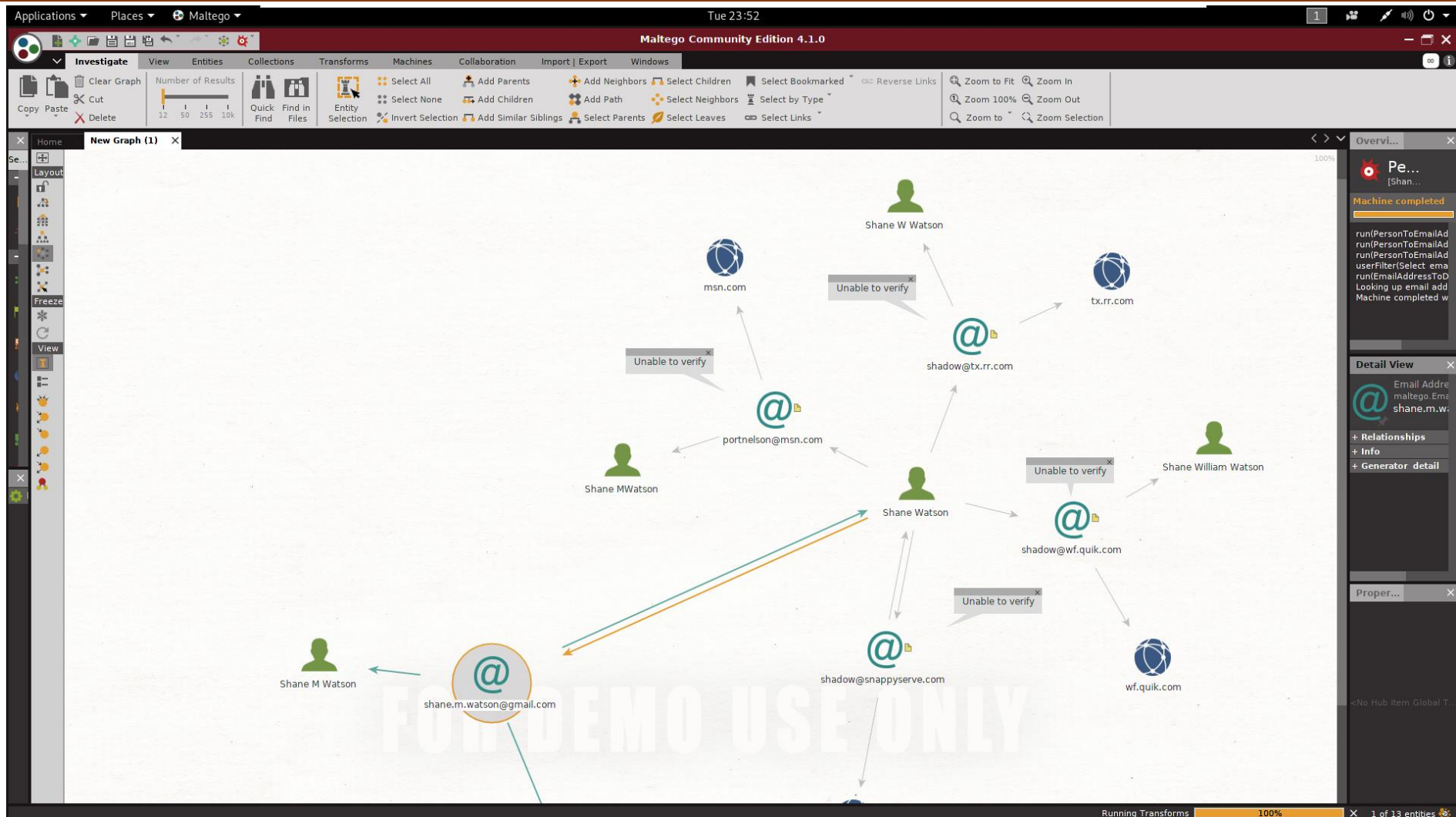
Difference between OSINT and Recon



Key Points for effective OSINT

- Process
- Requirements
- System
- Network
- Personal Accounts
- Documentations

Tools of Trade: Maltego



Source = <https://www.paterva.com/buy/maltego-clients.php>

Tools of Trade: Shodan

The screenshot shows the Shodan search engine interface. The search bar at the top contains the query "linux upnp avtech country:MY port:80". The results show 603 total results. The top countries are listed as Malaysia (603), and the top cities are Kuala Lumpur (119), Johor Bahru (33), Petaling Jaya (31), Shah Alam (27), and Klang (20). The top organizations are TM Net (440), Maxis Communications (127), Tt Dotcom Sdn Bhd (14), Streamyx-biz-central (6), and Maxis Broadband Sdn.Bhd (4). The search results are displayed in a table format with columns for the organization name, location, and a link to the search results.

TOTAL RESULTS
603

TOP COUNTRIES

Country	Count
Malaysia	603

TOP CITIES

City	Count
Kuala Lumpur	119
Johor Bahru	33
Petaling Jaya	31
Shah Alam	27
Klang	20

TOP ORGANIZATIONS

Organization	Count
TM Net	440
Maxis Communications	127
Tt Dotcom Sdn Bhd	14
Streamyx-biz-central	6
Maxis Broadband Sdn.Bhd	4

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

TM Net
Added on 2019-12-09 23:17:08 GMT
Malaysia, Kuala Lumpur

HTTP/1.1 200 OK
Date: Tue, 10 Dec 2019 07:15:00 GMT
Server: Linux/2.x UPnP/1.0 Avtech/1.0
Connection: close
Last-Modified: Wed, 26 Apr 2017 07:45:42 GMT
Content-Type: text/html
ETag: 378-15850-1493192742
Content-Length: 15850

Remote Surveillance, Any time & Any where

Streamyx-biz-central
Added on 2019-12-10 02:05:07 GMT
Malaysia, Klang

HTTP/1.1 200 OK
Date: Tue, 10 Dec 2019 10:05:06 GMT
Server: Linux/2.x UPnP/1.0 Avtech/1.0
Connection: close
Last-Modified: Wed, 14 Nov 2018 05:53:38 GMT
Content-Type: text/html
ETag: 222-54171-1542174818
Content-Length: 54171

Source = <https://www.shodan.io/>

Tools of Trade: Shodan

The screenshot displays the Shodan web interface. At the top, the browser address bar shows the IP address 175.140.219.150 and the AVTECH NVR. The Shodan logo and search bar are prominent. Below the search bar, a map shows the location of the host in George Town, Malaysia. The main content area is divided into two sections: Host Information and Ports/Services.

Field	Value
City	George Town
Country	Malaysia
Organization	TM Net
ISP	TM Net
Last Update	2019-12-10T06:43:48.198890
ASN	AS13191

Ports

- 80
- 123

Services

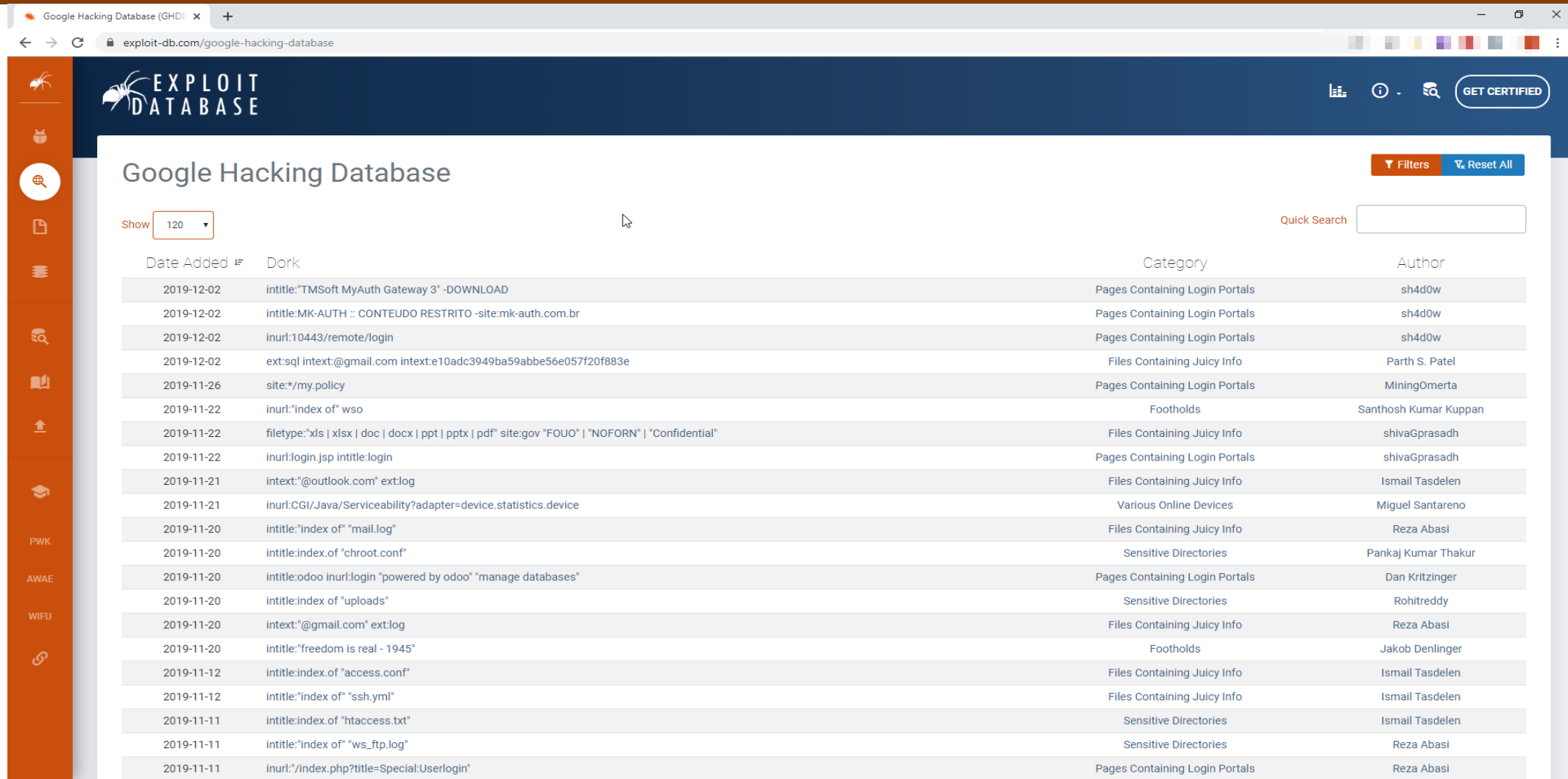
- 80 tcp http

Avtech AVN801 network camera Version: 1.0

HTTP/1.1 200 OK
Date: Tue, 10 Dec 2019 06:05:18 GMT
Server: Linux/2.x UPnP/1.0 Avtech/1.0
Connection: close

Source = <https://www.shodan.io/>

Tools of Trade: GHDB



The screenshot shows the Google Hacking Database (GHDB) interface. The header includes the 'EXPLOIT DATABASE' logo and a 'GET CERTIFIED' button. A sidebar on the left contains various icons for navigation. The main content area displays a table of search results with columns for 'Date Added', 'Dork', 'Category', and 'Author'. A 'Show 120' dropdown is visible, and a 'Quick Search' bar is on the right. The table lists 20 entries, each with a date, a specific search query (dork), a category, and the author's name.

Date Added	Dork	Category	Author
2019-12-02	intitle:"TMSoft MyAuth Gateway 3" -DOWNLOAD	Pages Containing Login Portals	sh4d0w
2019-12-02	intitle:MK-AUTH :: CONTEUDO RESTRITO -site:mk-auth.com.br	Pages Containing Login Portals	sh4d0w
2019-12-02	inurl:10443/remote/login	Pages Containing Login Portals	sh4d0w
2019-12-02	ext:sql intext:@gmail.com intext:e10adc3949ba59abbe56e057f20f883e	Files Containing Juicy Info	Parth S. Patel
2019-11-26	site:*/my.policy	Pages Containing Login Portals	MiningOmerta
2019-11-22	inurl:"index of" wso	Footholds	Santhosh Kumar Kuppan
2019-11-22	filetype:"xls xlsx doc docx ppt pptx pdf" site:gov "FOUO" "NOFORN" "Confidential"	Files Containing Juicy Info	shivaGprasadh
2019-11-22	inurl:login.jsp intitle:login	Pages Containing Login Portals	shivaGprasadh
2019-11-21	intext:"@outlook.com" ext:log	Files Containing Juicy Info	Ismail Tasdelen
2019-11-21	inurl:CGI/Java/Serviceability?adapter=device.statistics.device	Various Online Devices	Miguel Santareno
2019-11-20	intitle:"index of" "mail.log"	Files Containing Juicy Info	Reza Abasi
2019-11-20	intitle:index of "chroot.conf"	Sensitive Directories	Pankaj Kumar Thakur
2019-11-20	intitle:odoo inurl:login "powered by odoo" "manage databases"	Pages Containing Login Portals	Dan Kritzing
2019-11-20	intitle:index of "uploads"	Sensitive Directories	Rohitreddy
2019-11-20	intext:"@gmail.com" ext:log	Files Containing Juicy Info	Reza Abasi
2019-11-20	intitle:"freedom is real - 1945"	Footholds	Jakob Denlinger
2019-11-12	intitle:index of "access.conf"	Files Containing Juicy Info	Ismail Tasdelen
2019-11-12	intitle:"index of" "ssh.yml"	Files Containing Juicy Info	Ismail Tasdelen
2019-11-11	intitle:index of "htaccess.txt"	Sensitive Directories	Ismail Tasdelen
2019-11-11	intitle:"index of" "ws_ftp.log"	Sensitive Directories	Reza Abasi
2019-11-11	inurl:./index.php?title=Special:Userlogin"	Pages Containing Login Portals	Reza Abasi

Source = <https://www.exploit-db.com/google-hacking-database>

Tools of Trade: CTFR

```

Applications ▾ Places ▾ Terminal ▾
Tue 12:57
root@kali: ~/ctfr
File Edit View Search Terminal Help
root@kali:~/ctfr# python3 ctfr.py -d twitter.com

  ____  _  _  _  _  _
 / ___|| | | | | | |
| |___| |_| | |_| |
 \___ \|  _  |  _  |
    ___| | | | | | |
   |___|_|_|_|_|_|_|

Version 1.2 - Hey don't miss AXFR!
Made by Sheila A. Berta (UnaPibaGeek)

[!] ---- TARGET: twitter.com ---- [!]

[-] *.atl1.twitter.com
[-] *.atla.twitter.com
[-] *.smf1.twitter.com
[-] *.twitter.com
[-] 0.twitter.com
[-] alerts.atlb.twitter.com
[-] alerts.atlc.twitter.com
[-] alerts.smfc.twitter.com
[-] api.netsec.smfc.twitter.com
[-] api.twitter.com
[-] atl1.twitter.com
[-] atla.twitter.com
[-] audubon.ams1.twitter.com
[-] audubon.atl2.twitter.com
[-] audubon.atl4.twitter.com
[-] audubon.atla.twitter.com
[-] audubon.atlb.twitter.com
[-] audubon.atlc.twitter.com
[-] audubon.chi1.twitter.com
[-] audubon.dfw1.twitter.com
[-] audubon.dxb1.twitter.com
[-] audubon.dxb2.twitter.com
[-] audubon.fra1.twitter.com
[-] audubon.fra2.twitter.com

```

Source = <https://github.com/UnaPibaGeek/ctfr>



Thank You 😊

Somesh Sanjay Rasal
Information Security Analyst, Amdocs
https://twitter.com/rasal_somesh