Introduction to OSINT

BY: JOSE MEJIA

What is OSINT?

- Open-source intelligence
- Collecting artifacts freely available on the internet
  - Clear web
  - Dark web

Where OSINT is used

- CTFs
- Investigating threat actors
- Reporting on someone's internet presence
- Red team engagements
- Creating a pretext
  - Social Engineering (Phishing, Vishing)

OPSEC

- Operation Security
- Ensuring that the target is not aware of the investigation
- Not necessary in a CTF style environment
- VPN
  - Usually blocked by popular websites
- Public Wi-Fi

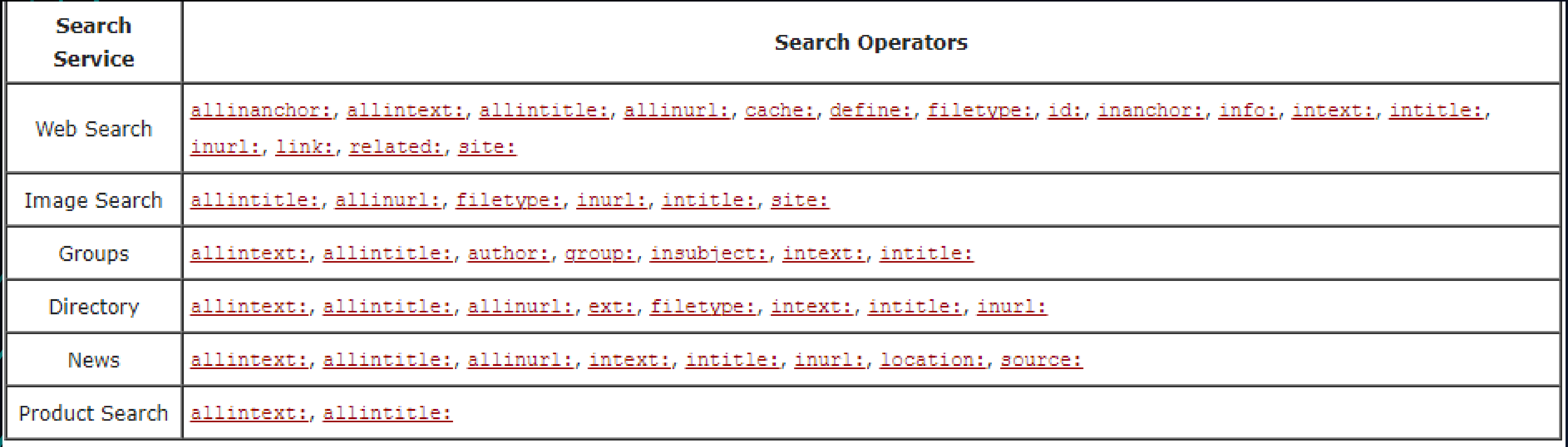
How to ensure OPSEC

- Public Wi-Fi
  - Most public Wi-Fi will work fine
- Sock Puppet accounts
  - Useful to gather personal information
  - Takes time to build a reliable profile
- Burner Phones
  - Used to verify sock puppet accounts

Google Dorking

- AKA Google hacking
- Yes, there’s a way to google “correctly”
- Search Operators
  - Infile:
  - Intext:
- Produces more relevant and accurate results

Example of Google Search Operators



Search Service	Search Operators
Web Search	allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site:
Image Search	allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
Groups	allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
Directory	allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
News	allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:
Product Search	allintext:, allintitle:

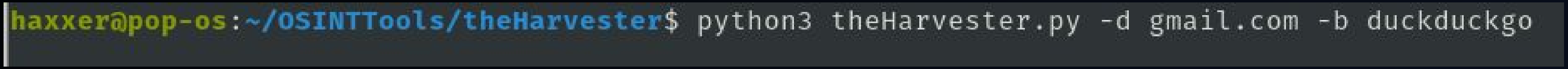
Source:
http://www.googleguide.com/advanced_operators_reference.html

What does an OSINT engagement look like?

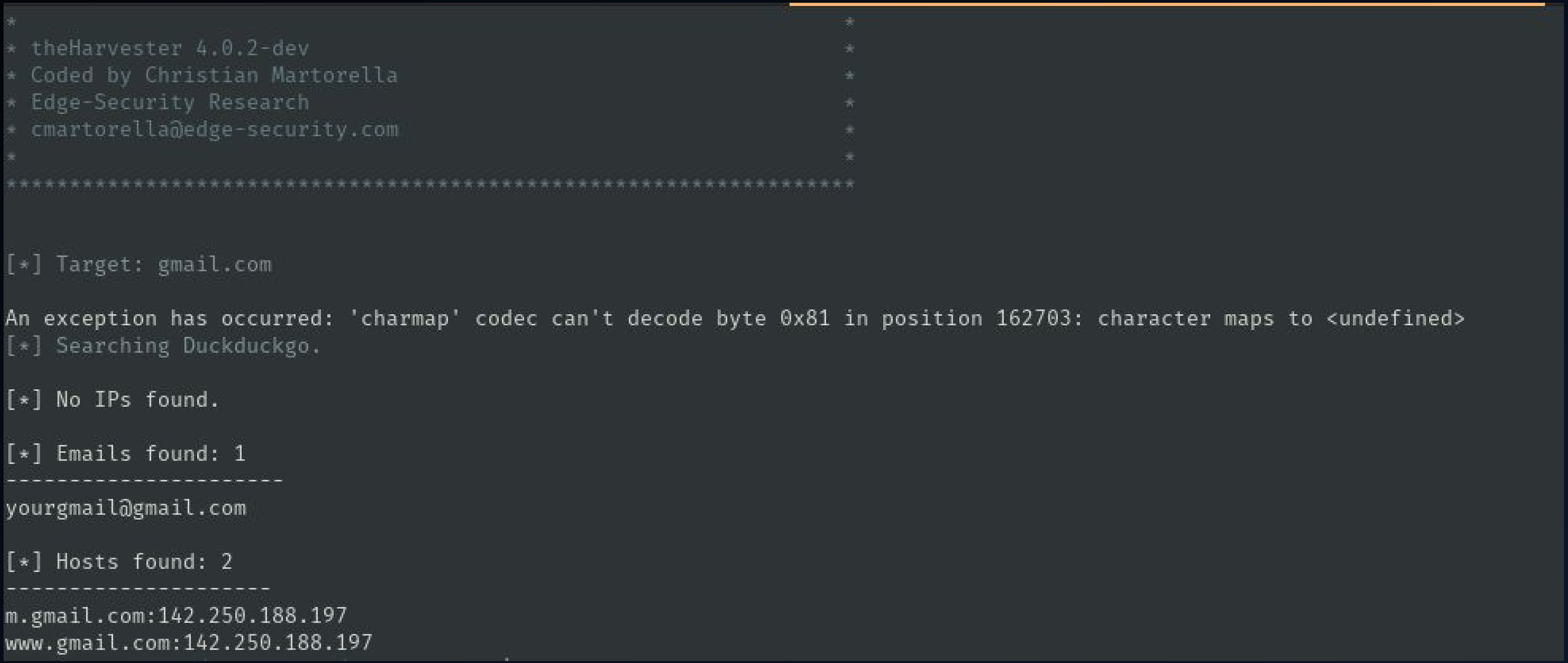
- Depends on the objective
- Finding emails to use in a phishing engagement
- Using information to build a pretext
- Creating a profile on a person of interest
  - Identifying malicious behavior
  - Identifying internet presence

Finding Emails

- Zoominfo: Employee Directory
  - Useful for finding a list of employees
  - Emails listed
- Hunter.io
  - Verifying email naming convention
- TheHarvester
  - Helps in discovering hosts, IPs, and emails
  - Just one of many OSINT Tools available



```
haxxer@pop-os:~/OSINTTools/theHarvester$ python3 theHarvester.py -d gmail.com -b duckduckgo
```

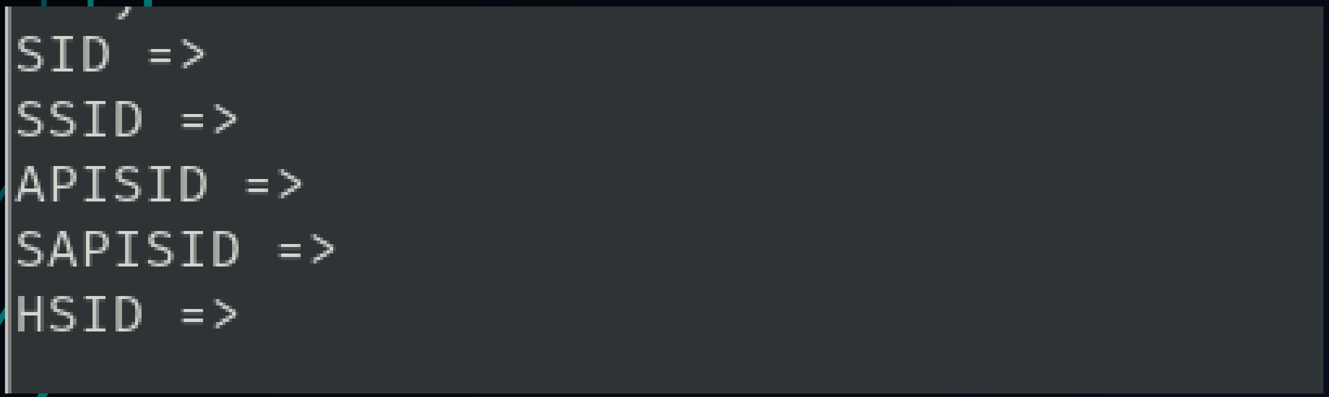


```
*                                                                 *
* theHarvester 4.0.2-dev                                          *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: gmail.com

An exception has occurred: 'charmap' codec can't decode byte 0x81 in position 162703: character maps to <undefined>
[*] Searching Duckduckgo.

[*] No IPs found.

[*] Emails found: 1
----------------------
yourgmail@gmail.com

[*] Hosts found: 2
---------------------
m.gmail.com:142.250.188.197
www.gmail.com:142.250.188.197
```

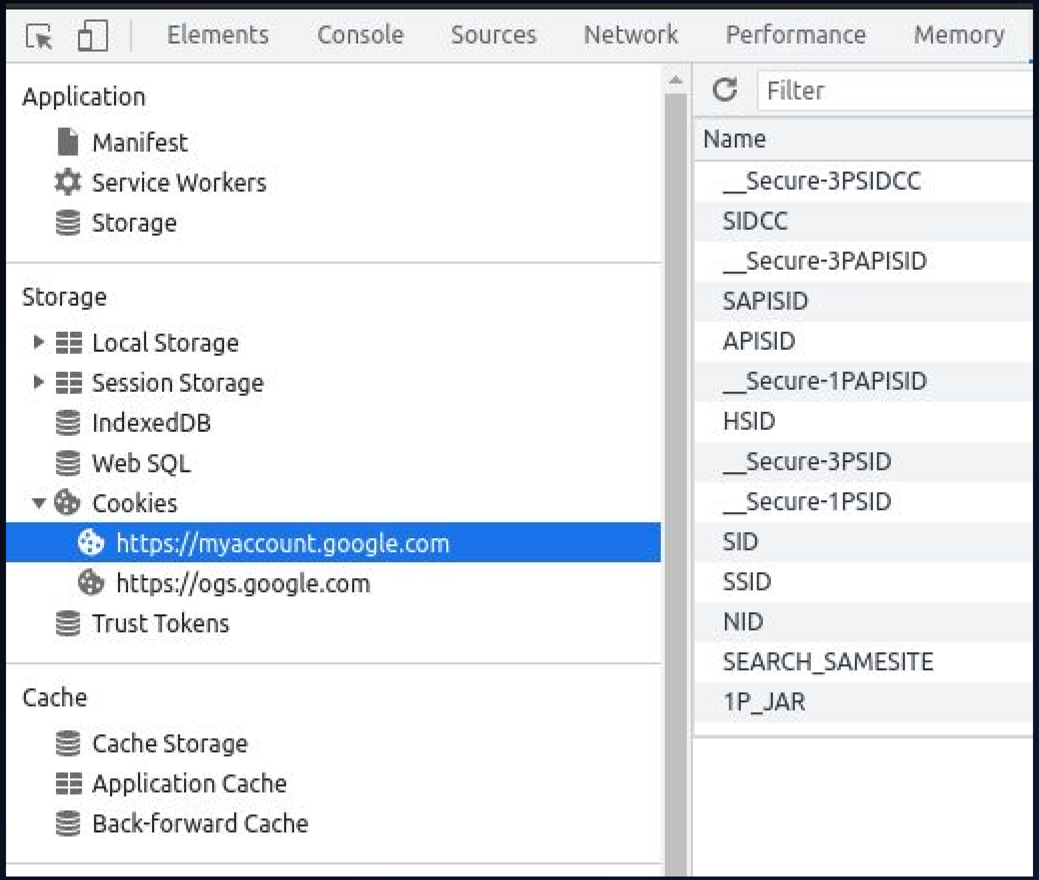
Investigating Google Emails

- Most individuals use Gmail
- Able to retrieve an emails registered name
- Google Map reviews
- Straight forward installation
- https://github.com/mxrch/GHunt

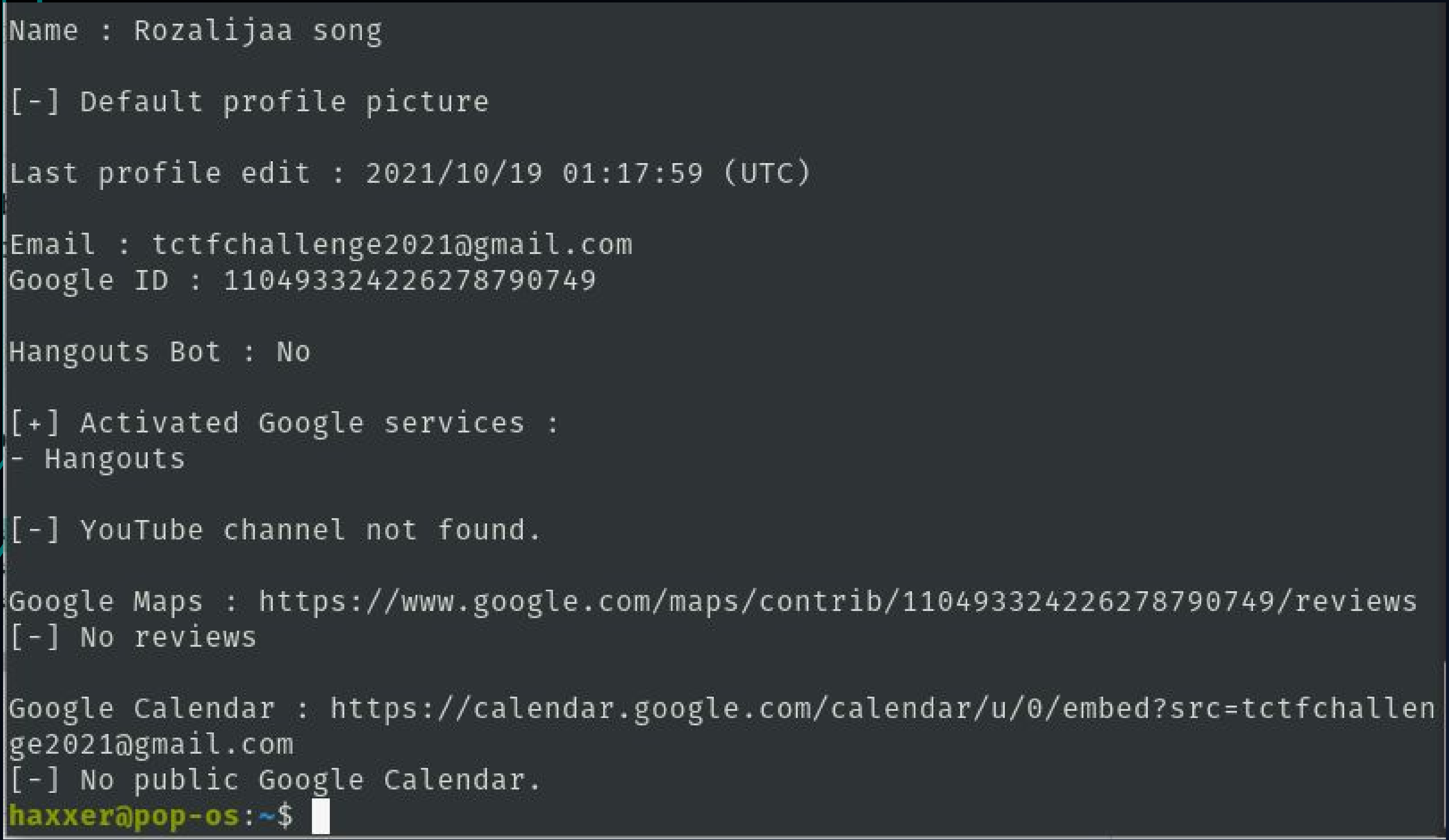
Ghunt Setup



```
SID =>
SSID =>
APISID =>
SAPISID =>
HSID =>
```



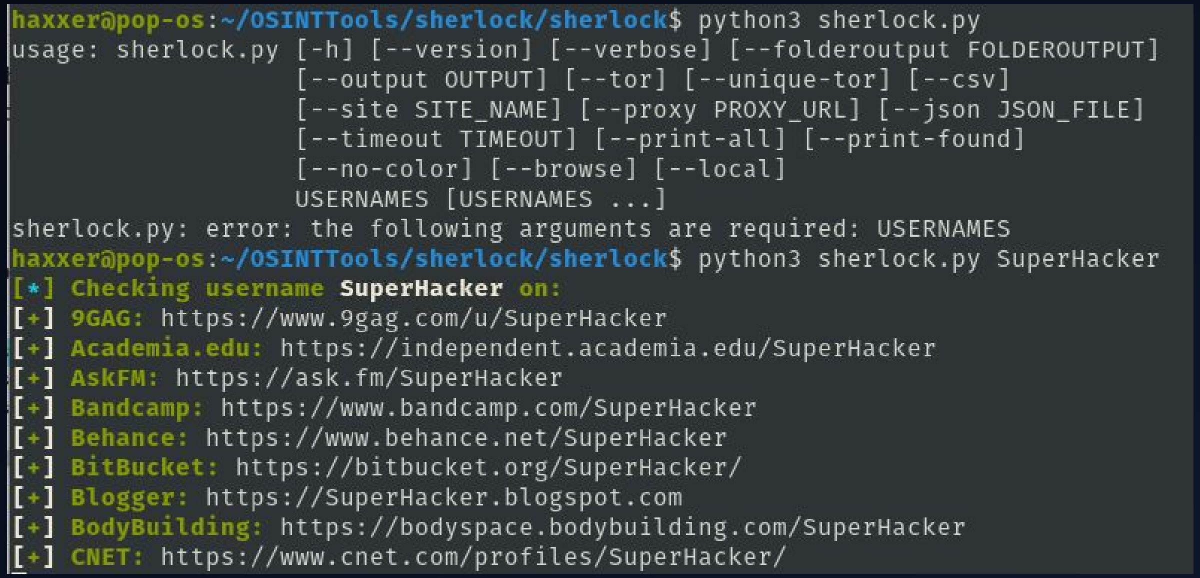
Name
__Secure-3PSIDCC
SIDCC
__Secure-3PAPISID
SAPISID
APISID
__Secure-1PAPISID
HSID
__Secure-3PSID
__Secure-1PSID
SID
SSID
NID
SEARCH_SAMESITE
1P_JAR



```
Name : Rozalijaa song

[-] Default profile picture

Last profile edit : 2021/10/19 01:17:59 (UTC)

Email : tctfchallenge2021@gmail.com
Google ID : 110493324226278790749

Hangouts Bot : No

[+] Activated Google services :
- Hangouts

[-] YouTube channel not found.

Google Maps : https://www.google.com/maps/contrib/110493324226278790749/reviews
[-] No reviews

Google Calendar : https://calendar.google.com/calendar/u/0/embed?src=tctfchallen
ge2021@gmail.com
[-] No public Google Calendar.
haxxer@pop-os:~$ 
```

Finding Usernames Using Sherlock

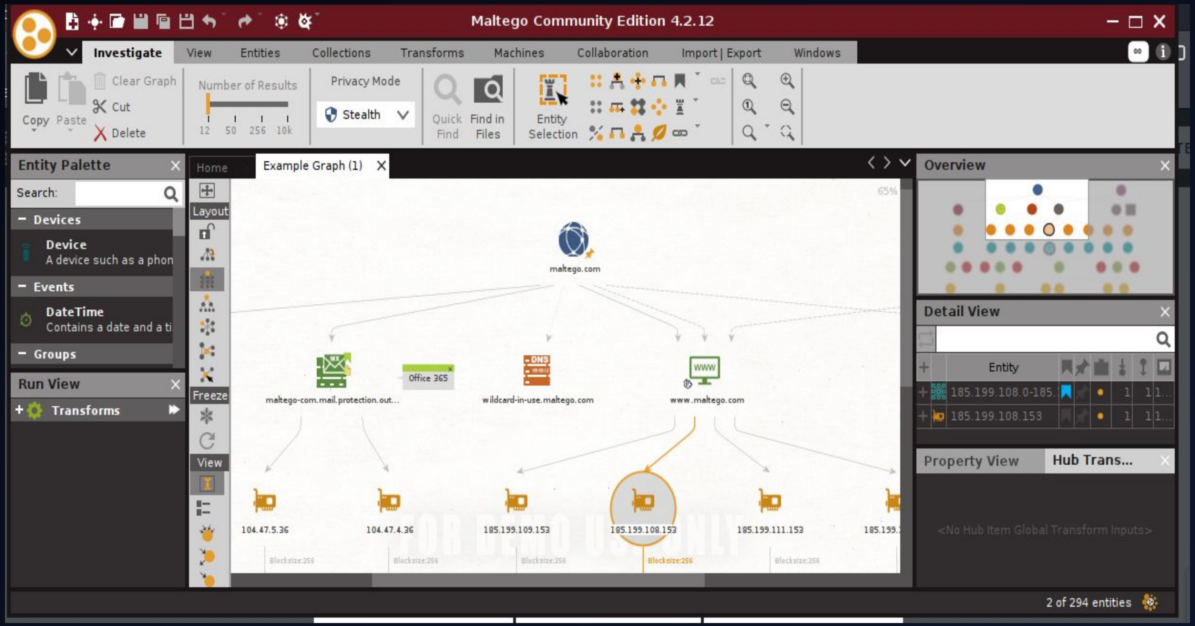
- Individuals tend to use the same username across platforms
- Useful in speeding up the process of discovering social media accounts



```
haxxer@pop-os:~/OSINTTools/sherlock/sherlock$ python3 sherlock.py
usage: sherlock.py [-h] [--version] [--verbose] [--folderoutput FOLDEROUTPUT]
                   [--output OUTPUT] [--tor] [--unique-tor] [--csv]
                   [--site SITE_NAME] [--proxy PROXY_URL] [--json JSON_FILE]
                   [--timeout TIMEOUT] [--print-all] [--print-found]
                   [--no-color] [--browse] [--local]
                   USERNAMES [USERNAMES ...]
sherlock.py: error: the following arguments are required: USERNAMES
haxxer@pop-os:~/OSINTTools/sherlock/sherlock$ python3 sherlock.py SuperHacker
[*] Checking username SuperHacker on:
[+] 9GAG: https://www.9gag.com/u/SuperHacker
[+] Academia.edu: https://independent.academia.edu/SuperHacker
[+] AskFM: https://ask.fm/SuperHacker
[+] Bandcamp: https://www.bandcamp.com/SuperHacker
[+] Behance: https://www.behance.net/SuperHacker
[+] BitBucket: https://bitbucket.org/SuperHacker/
[+] Blogger: https://SuperHacker.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/SuperHacker
[+] CNET: https://www.cnet.com/profiles/SuperHacker/
```

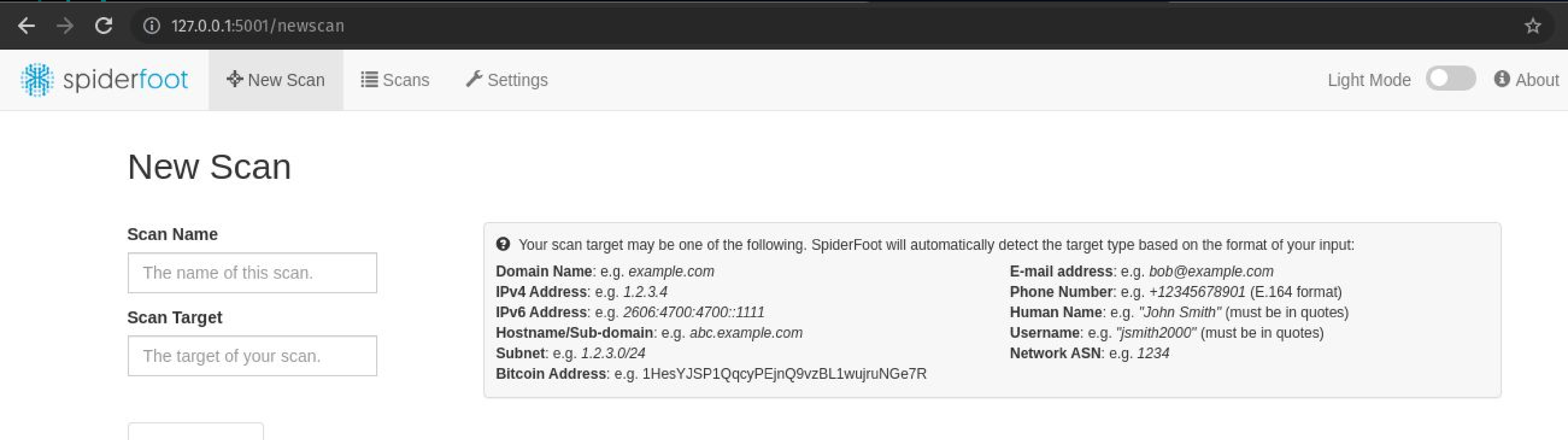
Let’s Speed It Up

- Recon-ng
- Maltego
  - Uses Transforms and Machines
- Spiderfoot
- Ensure Stealth/Passive mode is enabled to keep OPSEC
- May require sign up



Expanding on Spiderfoot

- Free and easy installation
- Great resource for finding breadcrumbs
- Handles a variety of inputs
  - Phone numbers
  - Emails
- Receive a wide variety of artifacts in a small amount of time



New Scan

Scan Name

The name of this scan.

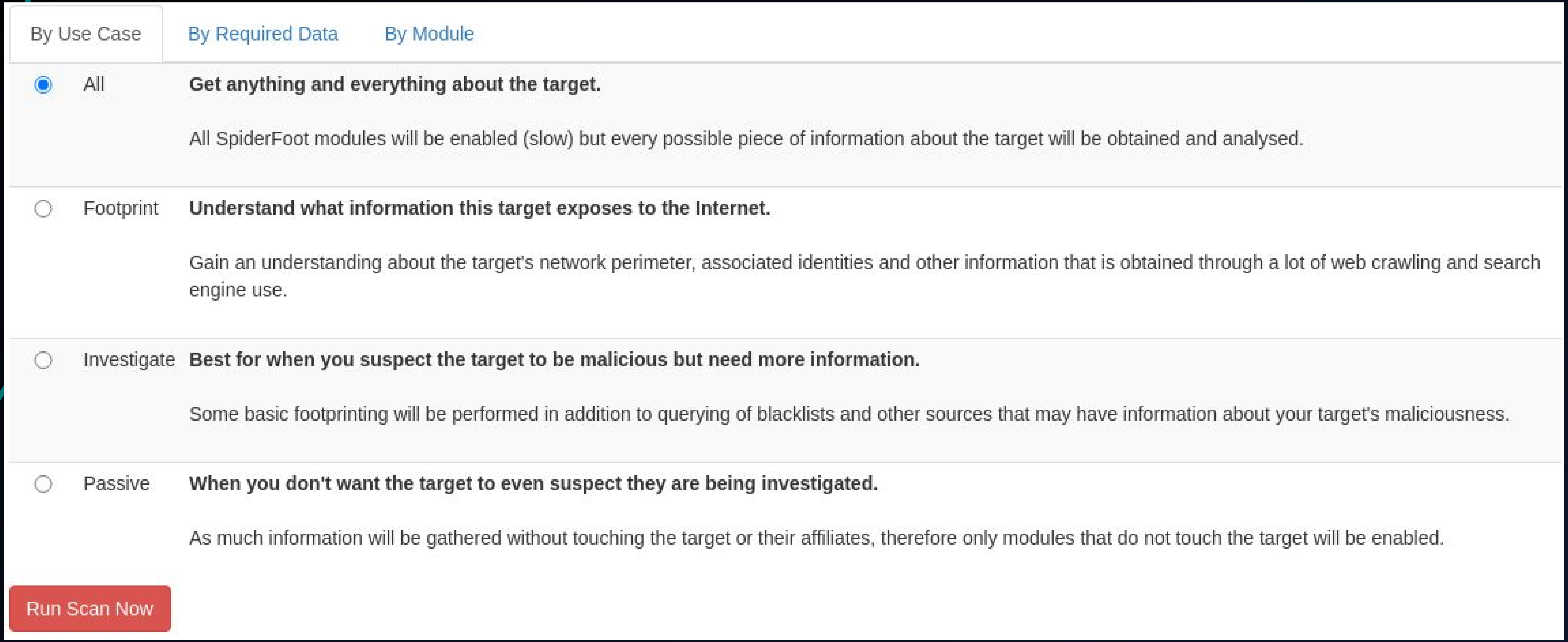
Scan Target

The target of your scan.

Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

Domain Name: e.g. *example.com*
IPv4 Address: e.g. *1.2.3.4*
IPv6 Address: e.g. *2606:4700:4700::1111*
Hostname/Sub-domain: e.g. *abc.example.com*
Subnet: e.g. *1.2.3.0/24*
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R

E-mail address: e.g. *bob@example.com*
Phone Number: e.g. *+12345678901* (E.164 format)
Human Name: e.g. *"John Smith"* (must be in quotes)
Username: e.g. *"jsmith2000"* (must be in quotes)
Network ASN: e.g. *1234*



● All **Get anything and everything about the target.**

All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

○ Footprint **Understand what information this target exposes to the Internet.**

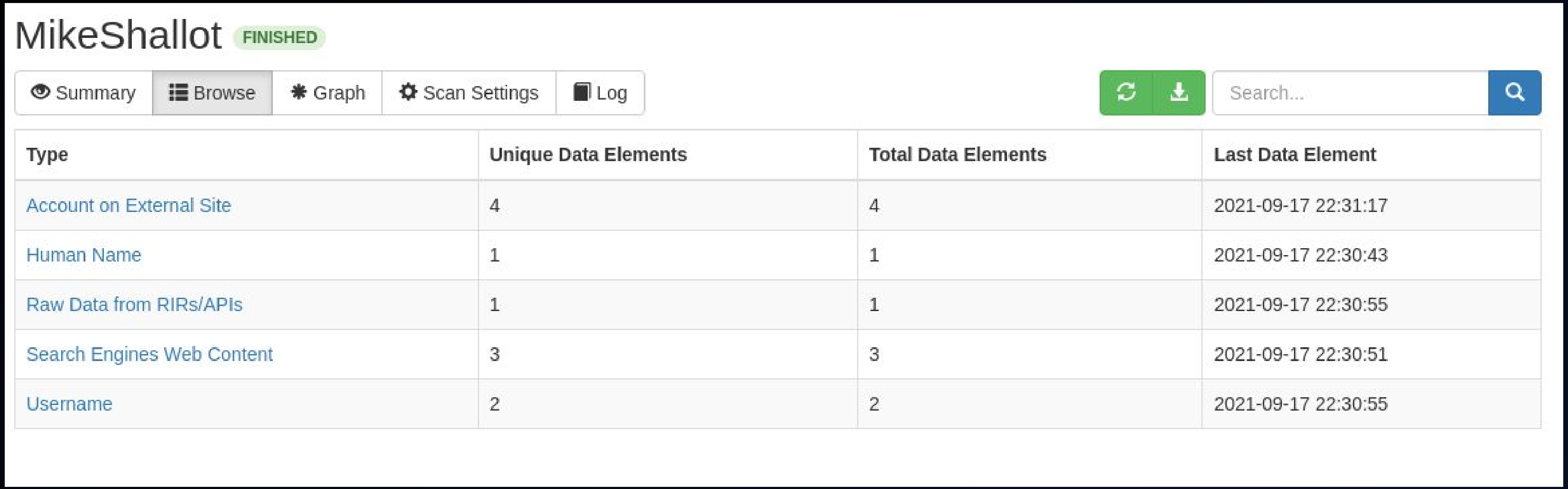
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

○ Investigate **Best for when you suspect the target to be malicious but need more information.**

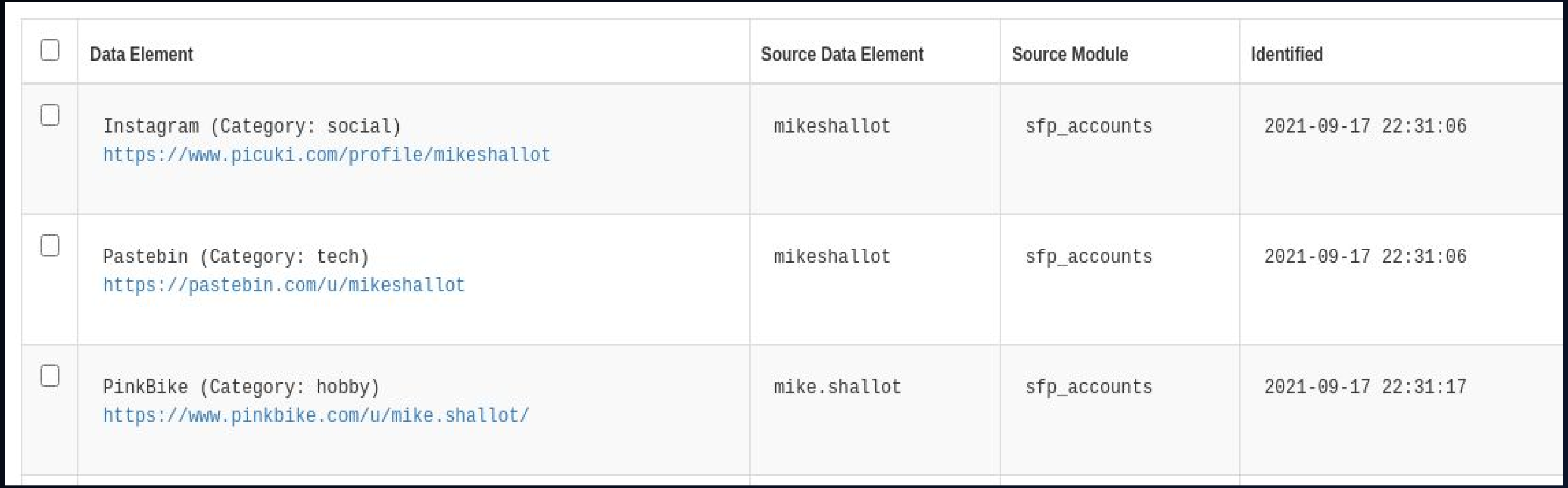
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

○ Passive **When you don't want the target to even suspect they are being investigated.**

As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.



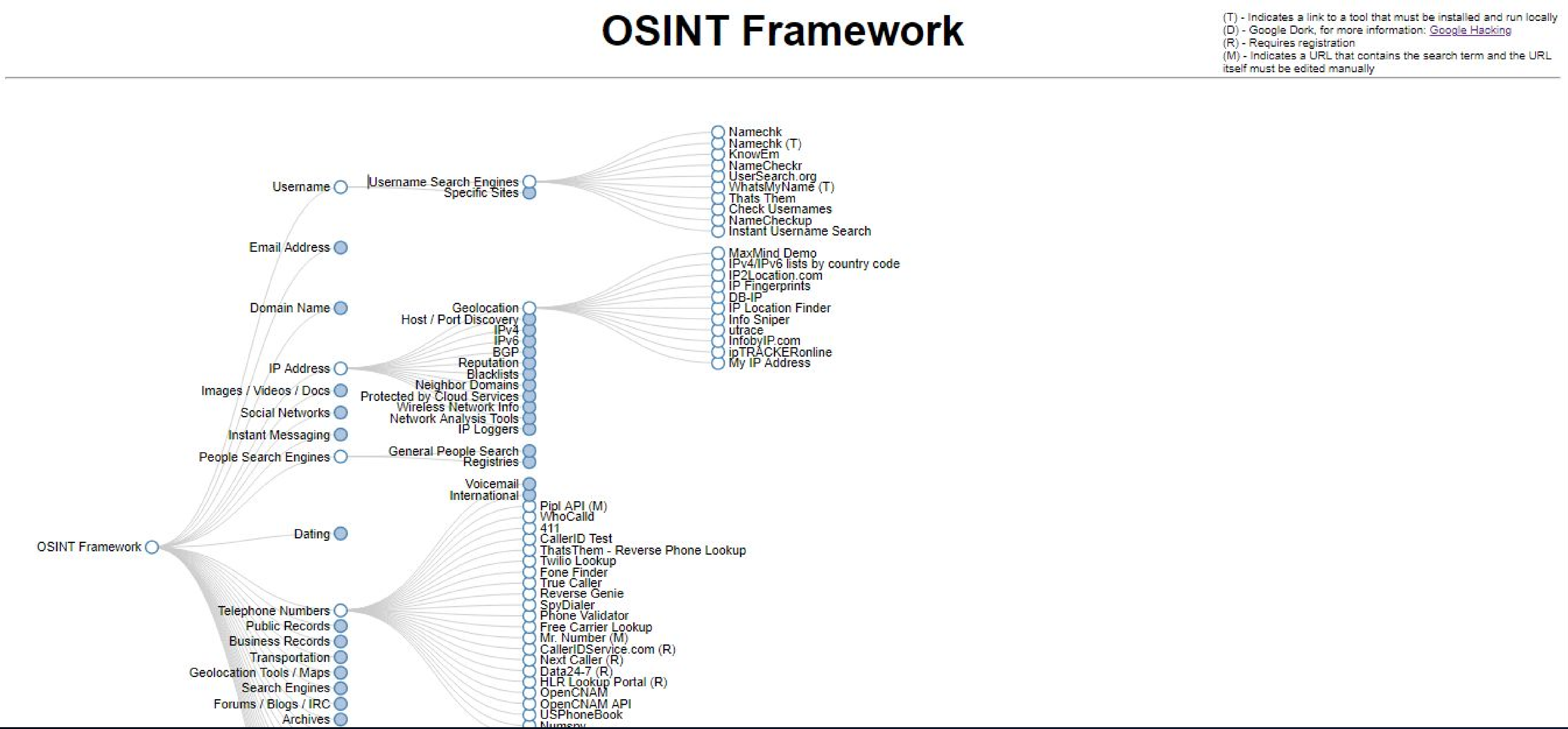
Type	Unique Data Elements	Total Data Elements	Last Data Element
Account on External Site	4	4	2021-09-17 22:31:17
Human Name	1	1	2021-09-17 22:30:43
Raw Data from RIRs/APIs	1	1	2021-09-17 22:30:55
Search Engines Web Content	3	3	2021-09-17 22:30:51
Username	2	2	2021-09-17 22:30:55



□	Data Element	Source Data Element	Source Module	Identified
□	Instagram (Category: social) https://www.picuki.com/profile/mikeshallot	mikeshallot	sfp_accounts	2021-09-17 22:31:06
□	Pastebin (Category: tech) https://pastebin.com/u/mikeshallot	mikeshallot	sfp_accounts	2021-09-17 22:31:06
□	PinkBike (Category: hobby) https://www.pinkbike.com/u/mike.shallot/	mike.shallot	sfp_accounts	2021-09-17 22:31:17

Websites Used to Build Profiles

- ThatsThem
- Spokeo
- FamilyTreeNow
- NameChk
  - Username search
- Keep in mind of daily search limits
  - Just switch IPs if you’re using a VPN



OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: Google Hacking
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually

OSINT Framework

- Username
  - Username Search Engines
    - Namechk
    - Namechk (T)
    - KnowEm
    - NameCheckr
    - UserSearch.org
    - WhatsMyName (T)
    - Thats Them
    - Check Usernames
    - NameCheckup
    - Instant Username Search
  - Specific Sites
- Email Address
- Domain Name
- IP Address
  - Geolocation
    - MaxMind Demo
    - IPv4/IPv6 lists by country code
    - IP2Location.com
    - IP Fingerprints
    - DB-IP
    - IP Location Finder
    - Info Sniper
    - utrace
    - InfobyIP.com
    - ipTRACKERonline
    - My IP Address
  - Host / Port Discovery
  - IPv4
  - IPv6
  - BGP
  - Reputation
  - Blacklists
  - Neighbor Domains
  - Protected by Cloud Services
  - Wireless Network Info
  - Network Analysis Tools
  - IP Loggers
- Images / Videos / Docs
- Social Networks
- Instant Messaging
- People Search Engines
  - General People Search
  - Registries
- Dating
- Telephone Numbers
  - Voicemail
  - International
  - Pipl API (M)
  - WhoCalld
  - 411
  - CallerID Test
  - ThatsThem - Reverse Phone Lookup
  - Twilio Lookup
  - Fone Finder
  - True Caller
  - Reverse Genie
  - SpyDialer
  - Phone Validator
  - Free Carrier Lookup
  - Mr. Number (M)
  - CallerIDService.com (R)
  - Next Caller (R)
  - Data24-7 (R)
  - HLR Lookup Portal (R)
  - OpenCNAM
  - OpenCNAM API
  - USPhoneBook
  - Numspy
- Public Records
- Business Records
- Transportation
- Geolocation Tools / Maps
- Search Engines
- Forums / Blogs / IRC
- Archives

Proud Sponsors

Live Demo

Questions

Resources

- Ghunt: https://github.com/mxrch/GHunt
- Spiderfoot: https://github.com/smicallef/spiderfoot?ref=d
- Sherlock: https://github.com/sherlock-project/sherlock
- OSINT Framework: https://osintframework.com/
- TheHarvester: https://github.com/laramies/theHarvester