OSINT Tools

Créé par	Cheikh Fall
Heure de création	@13 novembre 2023 13:55
Étiquettes	infotheque

OSINT Investigation Tools:

Reverse Image Search:

- WeVerify (https://www.invid-project.eu/tools-and-services/invid-verification-plugin/, right click
  on the picture and reverse image search)
- PimEyes (https://pimeyes.com/en, reverse face image search)

Social Media Profiles Identification:

- Online: Whatsmyname.app
- Local environment:
  o Sherlock (
  https://github.com/sherlock-project/sherlock)

o Maigret (
https://github.com/soxoj/maigret)

Email Verification:

- Holehe (https://github.com/megadose/holehe)
- Epieos (https://epieos.com, registration, free)
- Hunter.io (https://hunter.io, registration, free)
- Have I Been Pawned (https://haveibeenpwned.com/, can be used also for a reverse email
  search)

Malicious Files Verification:

- URLVoid (https://www.urlvoid.com/)
- VirusTotal (https://www.virustotal.com/gui/)

Archivization:

- Wayback Machine (https://archive.org/web/, plugin:

  https://chrome.google.com/webstore/detail/wayback-machine/fpnmgdkabkmnadcjpehmlllkndpkmiak)
- Archive Today (https://archive.ph/, plugin:
  https://chrome.google.com/webstore/detail/archive-page/gcaimhkfmliahedmeklebabdgagipbia)
- Ghostarchive (https://ghostarchive.org/)

Coordinated Inauthentic Behavior detection:

- **Facebook**:
  o CooRnet (
  https://coornet.org/) R package, REQUIRES CROWDTANGLE API, results can

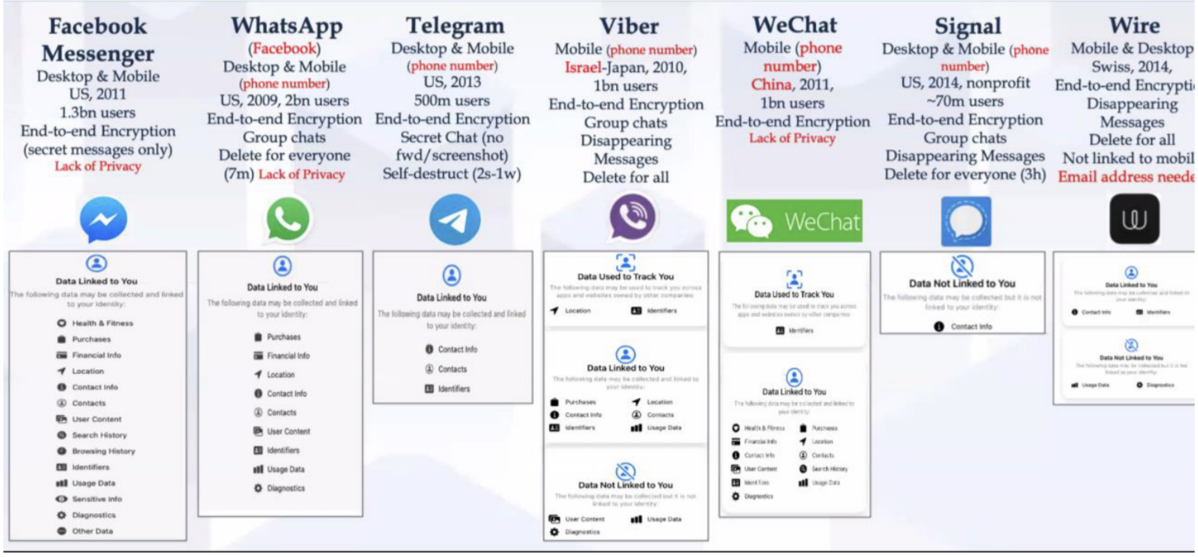
be exported in the .graphml format (f. ex. Gephi)
Scraping:

- **Telegram**:
  o Telegram Tracker (
  https://github.com/estebanpdl/telegram-tracker)
- Instant Data Scraper (https://chrome.google.com/webstore/detail/instant-data-scraper/ofaokhiedipichpaobibbnahnkdoiiah, easy to use, can scrape through next pages or scroll
  down, mind that social media might suspend your account for scraping)
- Data Miner (https://dataminer.io/)

Anonymization:

- VirtualBox (https://www.virtualbox.org/, environment for the virtual machines)
- Trace Labs Virtual Machine (https://www.tracelabs.org/initiatives/osint-vm)
- Kali Linux Virtual Machine (https://www.kali.org/get-kali/#kali-virtual-machines)
- Whonix Virtual Machine (https://www.whonix.org/wiki/VirtualBox#GUI)
- Hunchly Dark Web Investigation Guide (https://www.hunch.ly/resources/Hunchly-Dark-Web-
  Setup.pdf, manual how to combine Linux Virtual Machine with Whonix and drive all internet
  traffic through Tor)
- Tor Project (https://www.torproject.org/)
- How to set specific entry/exit nodes in the Tor Browser (https://www.wikihow.com/Set-a-
  Specific-Country-in-a-Tor-Browser, you can use it as a VPN, fixing nodes always make the
  connection less secure, do not set the same country for the entry and exit node)

Security of social media communicator apps (and why to use Signal or Wire):



Facebook Messenger
Desktop & Mobile
US, 2011
1.3bn users
End-to-end Encryption
(secret messages only)
Lack of Privacy

WhatsApp
(Facebook)
Desktop & Mobile
(phone number)
US, 2009, 2bn users
End-to-end Encryption
Group chats
Delete for everyone
(7m) Lack of Privacy

Telegram
Desktop & Mobile
(phone number)
US, 2013
500m users
End-to-end Encryption
Secret Chat (no
fwd/screenshot)
Self-destruct (2s-1w)

Viber
Mobile (phone number)
Israel-Japan, 2010,
1bn users
End-to-end Encryption
Group chats
Disappearing
Messages
Delete for all

WeChat
Mobile (phone
number)
China, 2011,
1bn users
End-to-end Encryption
Lack of Privacy

Signal
Desktop & Mobile (phone
number)
US, 2014, nonprofit
~70m users
End-to-end Encryption
Group chats
Disappearing Messages
Delete for everyone (3h)

Wire
Mobile & Desktop
Swiss, 2014,
End-to-end Encrypti
Disappearing
Messages
Delete for all
Not linked to mobil
Email address neede

Google Dorking:

- **cache**: this dork will show you the cached version of any website, e.g. cache:securitytrails.com
- **allintext**: searches for specific text contained on any web page, e.g. allintext: hacking tools
- **allintitle**: the same as allintext, but will show pages that contain titles with X characters,
e.g. allintitle:"Security Companies"
- **allinurl**: it can be used to fetch results whose URL contains all the specified characters,
e.g: allinurl:clientarea
- **filetype**: used to search for any kind of file extensions, for example, if you want to search for pdf
files you can use: email security filetype: pdf
- **inurl**: this is the same as allinurl, but it is only useful for one single keyword, e.g. inurl:admin
-

intitle: used to search for various keywords inside the title, for example, intitle:security tools will search for titles beginning with “security” but “tools” can be somewhere else on the page.

- **inanchor**: this is useful when you need to search for an exact anchor text used on any links, e.g. inanchor:"cyber security"
- **intext**: useful to locate pages that contain certain characters or strings inside their text, e.g. intext:"safe internet"
- **site**: will show you the full list of all indexed URLs for the specified domain and subdomain, e.g. site:securitytrails.com
- *: wildcard used to search pages that contain “anything” before your word, e.g. how to * a website, will return “how to…” design/create/hack, etc… “a website”.
- **|** (**OR**): this is a logical operator, e.g. "security" **|** "tips" will show all the sites which contain “security” or “tips,” or both words.
- + (**AND**): used to concatenate words, useful to detect pages that use more than one specific key, e.g. security + trails
- – (**NOT**): minus operator is used to avoiding showing results that contain certain words, e.g. security **-**trails will show pages that use “security” in their text, but not those that have the word “trails.”

Most of Google Dorks works similarly for other browsers, like Bing, Yandex, DuckDuckGo.
Example: Google Dork for finding Google indexed sites with a top domain from Senegal that contain in the page text links to sputniknews.africa or

rt.com.

site:.sn "sputniknews.africa" OR "rt.com" [□ paste this in the Google Search bar]

Example_2: Google Dork for finding Google indexed sites with a top domains from African countries that contain in the page text the title of the Vladimir Putin’s article “Russia and Africa: Joining Efforts for Peace, Progress and a Successful Future“ (there are three chunks due to the query limit in the Google Search):

1.

site:.africa OR site:.africa.com OR site:.bi OR site:.cd OR site:.cg OR site:.cm OR site:.co.bi OR site:.co.cm OR site:.co.ke OR site:.co.mg OR site:.co.mw OR site:.co.na OR site:.co.ug OR site:.co.za OR site:.com.bi OR site:.com.cm OR site:.com.ly OR site:.com.mg OR site:.com.mw OR site:.com.na “Russia and Africa: Joining Efforts for Peace, Progress and a Successful Future“

2.
site:.com.ng OR site:.com.sc OR site:.coop.mw OR site:.ke OR site:.ly OR site:.mg OR site:.mu site:.mw
OR site:.na OR site:.net.cm OR site:.net.mg OR site:.net.za OR site:.ng OR site:.or.bi
“Russia and Africa:
Joining Efforts for Peace, Progress and a Successful Future“

3.
site:.org.mg OR site:.org.na OR site:.org.za OR site:.rw OR site:.sc OR site:.sh OR site:.sl OR site:.so OR site:.st OR site:.ug OR site:.web.za OR site:.za.com “Russia and Africa: Joining Efforts for Peace, Progress and a Successful Future“

Database of the Google Dorks:

- https://www.exploit-db.com/google-hacking-database
- https://ahrefs.com/blog/google-advanced-search-operators/
- https://medium.com/codex/master-at-google-hacking-dorking-27d14e7249be

Tools for the automated OSINT research:

- Maltego (https://www.maltego.com/, community version is free and limited, can be connected with many APIs.
- SpiderFoot (https://www.kali.org/tools/spiderfoot/, default in the Kali Linux/TL VM, different APIs can be connected)

Social media sock puppet accounts:

- It is generally advised to never use personal social media accounts for the OSINT investigations.
  Use encrypted email accounts for creating sock puppets, preferably use password manager, like
  KeePassXC (free, local, no threat of a leakage, can be integrated with browser through an
  extension:
  https://chrome.google.com/webstore/detail/keepassxc-browser/oboonakemofpalcgghocfoadofidjkkk)

Introduction for using Python for OSINT:

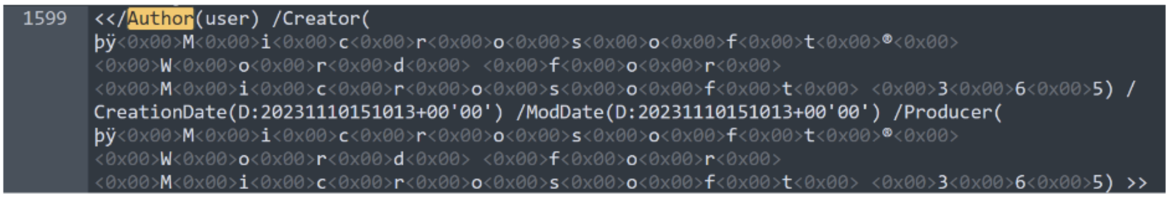
- Python for OSINT 21 days (https://github.com/cipher387/python-for-OSINT-21-days)

Metadata:

- Metagoofil (https://github.com/opsdisk/metagoofil, use grep function for Linux/MacOS or findstr for Windows)
- Microsoft Office documents (right-click → properties → details). [you can change your default name of the user account in the Microsoft Office options]
- To see metadata of the PDF file you have to open it in the text editor, f. ex. SublimeText:
  Details of the PDF file properties:

PDF document opened in the SublimeText editor (username of the author is visible):

You may want to remove metadata
from files that you are sending to
other people.
DO NOT CHANGE METADATA IN TEXT EDITOR AS THE PDF FILE WILL BE UNUSABLE.
OSINT framework (
https://osintframework.com/)



```
<</Author(user) /Creator(
þÿ<0x00>M<0x00>i<0x00>c<0x00>r<0x00>o<0x00>s<0x00>o<0x00>f<0x00>t<0x00>®<0x00>
<0x00>W<0x00>o<0x00>r<0x00>d<0x00> <0x00>f<0x00>o<0x00>r<0x00>
<0x00>M<0x00>i<0x00>c<0x00>r<0x00>o<0x00>s<0x00>o<0x00>f<0x00>t<0x00> <0x00>3<0x00>6<0x00>5) /
CreationDate(D:20231110151013+00'00') /ModDate(D:20231110151013+00'00') /Producer(
þÿ<0x00>M<0x00>i<0x00>c<0x00>r<0x00>o<0x00>s<0x00>o<0x00>f<0x00>t<0x00>®<0x00>
<0x00>W<0x00>o<0x00>r<0x00>d<0x00> <0x00>f<0x00>o<0x00>r<0x00>
<0x00>M<0x00>i<0x00>c<0x00>r<0x00>o<0x00>s<0x00>o<0x00>f<0x00>t<0x00> <0x00>3<0x00>6<0x00>5) >>
```