

## RECONNAISSANCE

With great knowledge, comes successful attacks!

# COLLECTER DE L'INFORMATION

- O Qu'est-ce?
- Pourquoi le faire ?
- Ce que ce n'est pas ?

L'Open source intelligence (OSINT) est une forme de gestion de la collecte de renseignements qui consiste à trouver, sélectionner et acquérir des informations à partir de sources accessibles au public et à les analyser pour produire des renseignements exploitables.

Il s'agit tout simplement de localiser et d'analyser des sources d'information accessibles au public (ouvertes). Le processus de collecte de renseignements a pour objectif de produire des informations actuelles et pertinentes qui sont utiles à un attaquant ou à un concurrent.

- L'OSINT, ce n'est pas seulement la recherche sur le web!

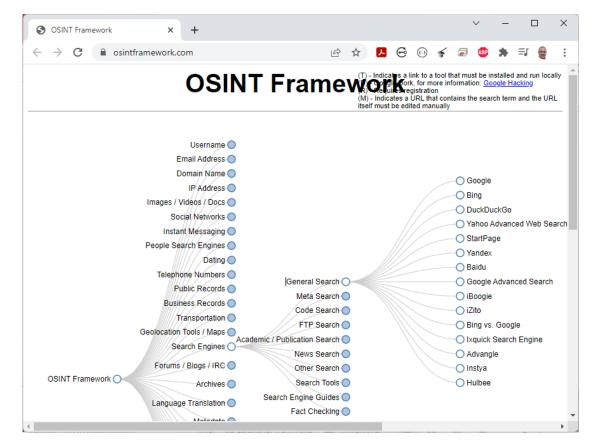
Elle se présente sous trois formes :

- Collecte passive d'informations
- Collecte d'informations semi-passive
- Collecte active d'informations

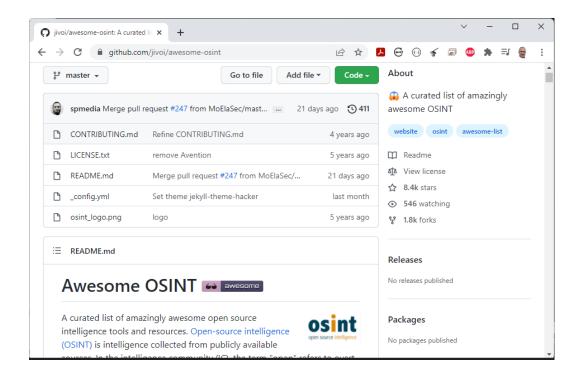
#### Utilisé pour :

- Les entreprises
- Les particuliers

https://osintframework.com



https://github.com/jivoi/awesome-osint



# SELECTION DE LA CIBLE

- Identification et désignation de la cible
- Tenir compte des éventuelles limitations et les Lois

- Tenir compte de la durée de la recherche
- Tenir compte de l'objectif final

# **ENTREPRISE - PHYSIQUE**

### Lieux

Les sites publics peuvent souvent être localisés à l'aide de **moteurs de recherche** tels que : Google, Yahoo, Bing, Ask.com, Baidu, etc.

### Relations

# SITES D'OFFRES D'EMPLOI

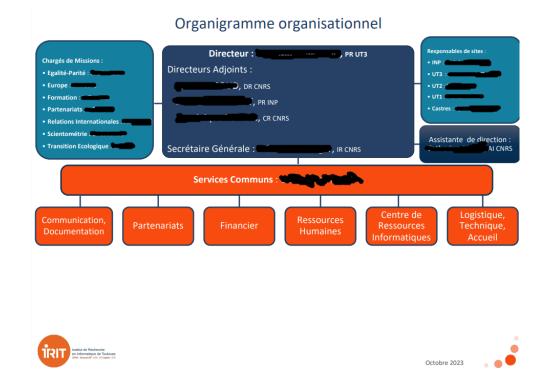
- LinkedIn, https://www.linkedin.com/mynetwork,
- Indeed, https://fr.indeed.com
- Monster, https://www.monster.com
- • •

## **ENTREPRISE - ORGANISATION**

Identification des positions dans l'entreprise

**Transactions** 

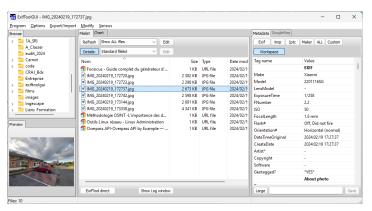
**Affiliations** 



# ENTREPRISE - NUMERIQUE

Métadatas

**Communications Marketing** 



Jecunte.	Polices Vue initiale Personnalisées Avancées	
Description		
Fichier:	3546745.pdf	
_itre:	Development and Evaluation of a Motion-based VR Bicycle Simulator	
<u>A</u> uteur:		
<u>S</u> ujet :	Proc. ACM HumComput. Interact. 2022.6:1-19	
<u>M</u> ots-clés :		
Date de création :	09/08/2022 10:18:24 Métadonnées supplémentaires	
	09/08/2022 10:18:24 Métadonnées supplémentaires 19/10/2023 10:00:34	
Modifié le :	Metadonnees supplementaires	7
Modifié le :	19/10/2023 10:00:34  LaTeX with acmart 2022/04/09 v1.84 Typesetting articles for the Association for Computing Machinery and hyperref 2021-06-0	7
Modifié le : Application : Description avancée	19/10/2023 10:00:34  LaTeX with acmart 2022/04/09 v1.84 Typesetting articles for the Association for Computing Machinery and hyperref 2021-06-0	7
Modifié le : Application : Description avancée Outil de conver	19/10/2023 10:00-34  LaTeX with acmart 2022/04/09 v1.84 Typesetting articles for the Association for Computing Machinery and hyperref 2021-08-0	7
Modifié le : Application : Description avancée Outil de conver	19/10/2023 10:00-34  LaTeX with acmart 2022/04/09 v1.84 Typesetting articles for the Association for Computing Machinery and hyperref 2021-06-0 stone PDF: MikTeX-pdfTeX 4.8.0 (1.40.23); modified using Text 4.2.0 by 1T3XT	7
Modifié le : Application : Description avancée Outil de conven Ven Empl.	19/10/2023 10:00-34  LaTeX with acmart 2022/04/09 v1.84 Typesetting articles for the Association for Computing Machinery and hyperref 2021-06-0 sion PDF: MiKTeX-pdTeX 4.8.0 (1.40.23); modified using TText 4.2.0 by 1T3XT sion PDF: 1.5 (Acrobat 6.x)	7
Modifié le : Application : Description avancée Outil de conven Ven Empl. Taille d	19/10/2023 10:00-34  LaTicX with acmart 2022/04/09 v1.84 Typesetting articles for the Association for Computing Machinery and hyperef 2021-06-0 sion PDF: MiXTeX-pdtTeX 4.8.0 (1.40.23); modified using Text 4.2.0 by 1T3XT sion PDF: 1.5 (Acrobat 6.x) accement: C\U00e4Users\Phi\tilde{\text{Description}} Association for Computing Machinery and hyperef 2021-06-0 sion PDF: 1.5 (Acrobat 6.x)	7

## **OUTILS**

#### Outil CLI (commande en ligne) - wget

Example: Retrieve only PDFs from a site

```
$ wget -nd -r -13 -e robots=off --no-check-certificate
-A .pdf https://contremesures.fr
```

Mythics()ft

https://www.mythicsoft.com/agentransack

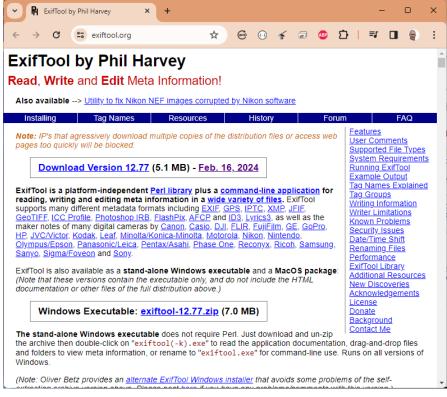


Des outils comme grep

OCR (Tesseract) - https://github.com/tesseractocr/tesseract

### TOOL - EXIF

EXIF Tool - https://exiftool.org



## **ENTREPRISE - INFRASTRUCTURE**

Adresses réseaux utilisées

Adresses émail

Technologies utilisées

Accès à distance

• • •

# **AUTRES OUTILS**

```
nslookup

Lookup - https://lookup.icann.org/en

whois - https://who.is

...

https://visualping.io

https://versionista.com

https://www.copyscape.com/compare.php
```

# INDIVUDU – PROFIL DES RÉSEAUX SOCIAUX

Fuite de métadonnées

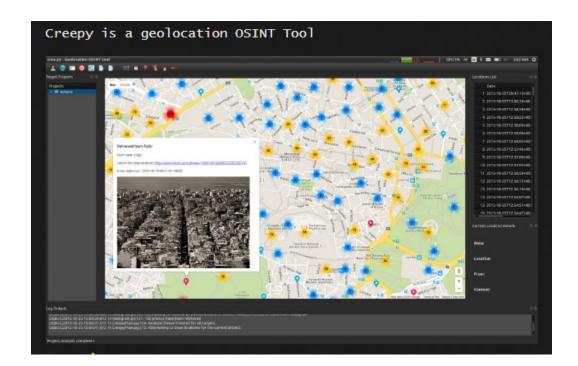
Sensibilisation à la localisation

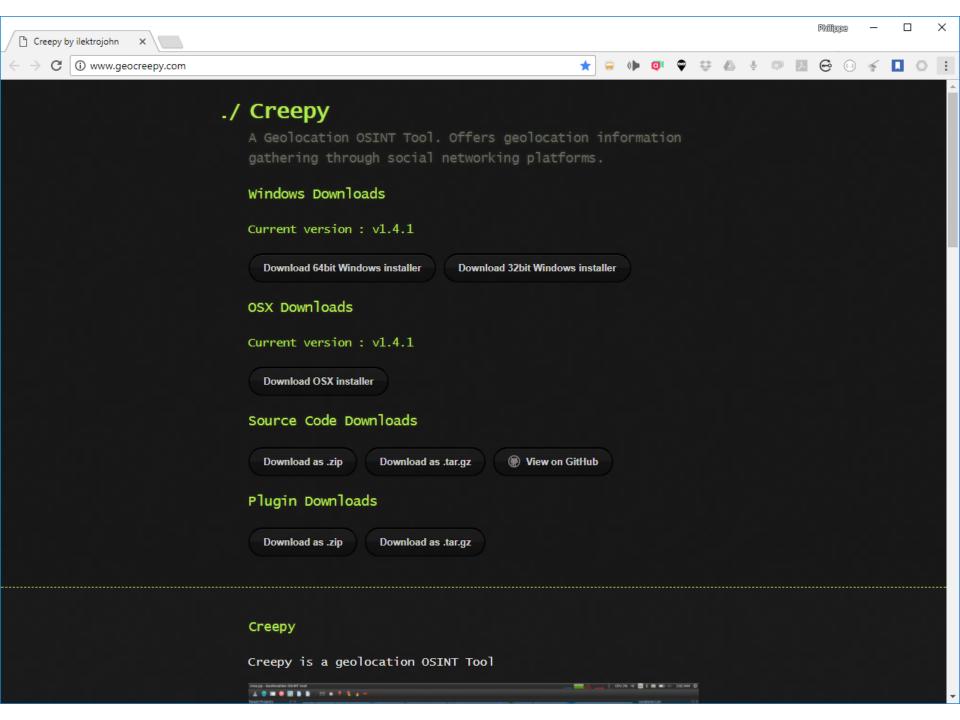
Présence dans les médias sociaux

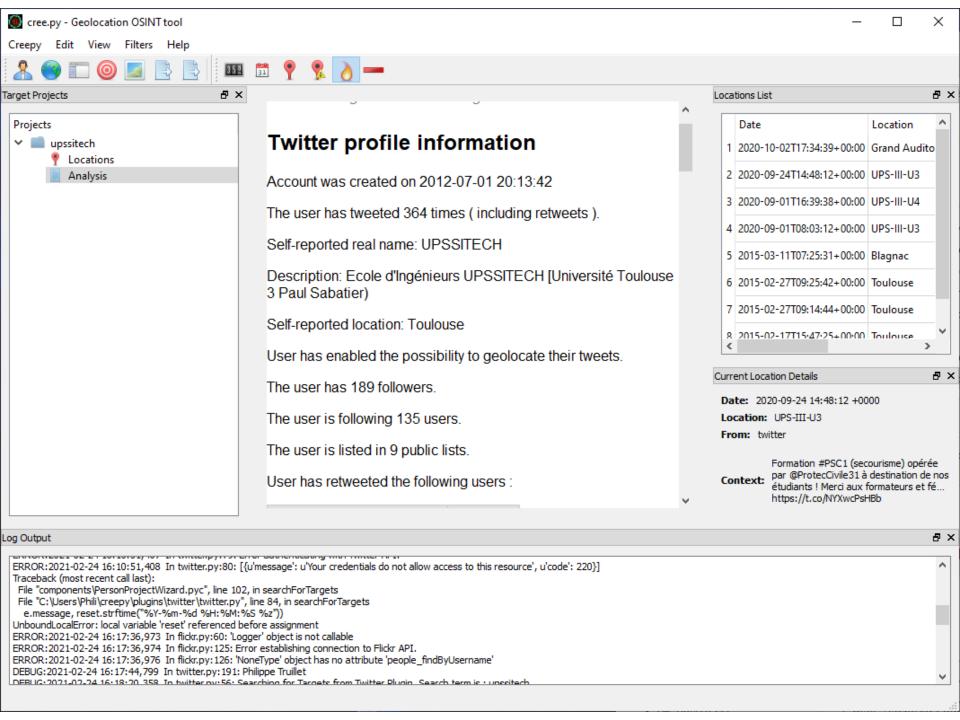
# LOCATION AWARENESS - CREE.PY

Cree.py (https://www.geocreepy.com) est une application open source de collecte de renseignements. Elle peut collecter des données de Twitter et des données

de géolocalisation à partir de plusieurs sites web.



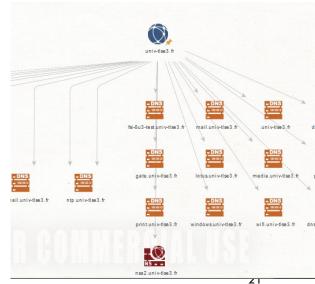


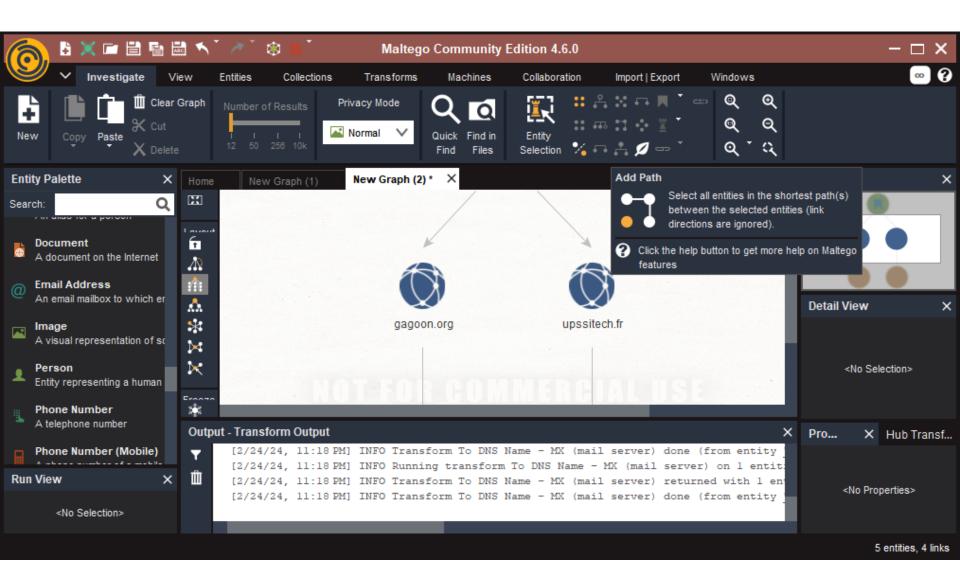


## **MALTEGO**

Maltego (https://www.maltego.com/downloads) est un outil d'exploration de données et de collecte d'informations qui met en correspondance les informations recueillies dans un format facile à comprendre et à manipuler.

automatise des tâches telles que la collecte d'e-mails et la cartographie des sous-domaines.





## THE HARVESTER



#### **TheHarvester**

(https://github.com/laramies/theHarvester) est un outil qui peut être utilisé pour collecter des comptes e-mail et des noms de sous-domaines à partir de différentes sources publiques (moteurs de recherche, serveurs de clés pgp).

→ http://www.edge-security.com





# RÉSEAUX SOCIAUX

Check Usernames - Utile pour vérifier l'existence d'un nom d'utilisateur donné sur 160 réseaux sociaux.

https://checkusernames.com



#### **Mail Lists**

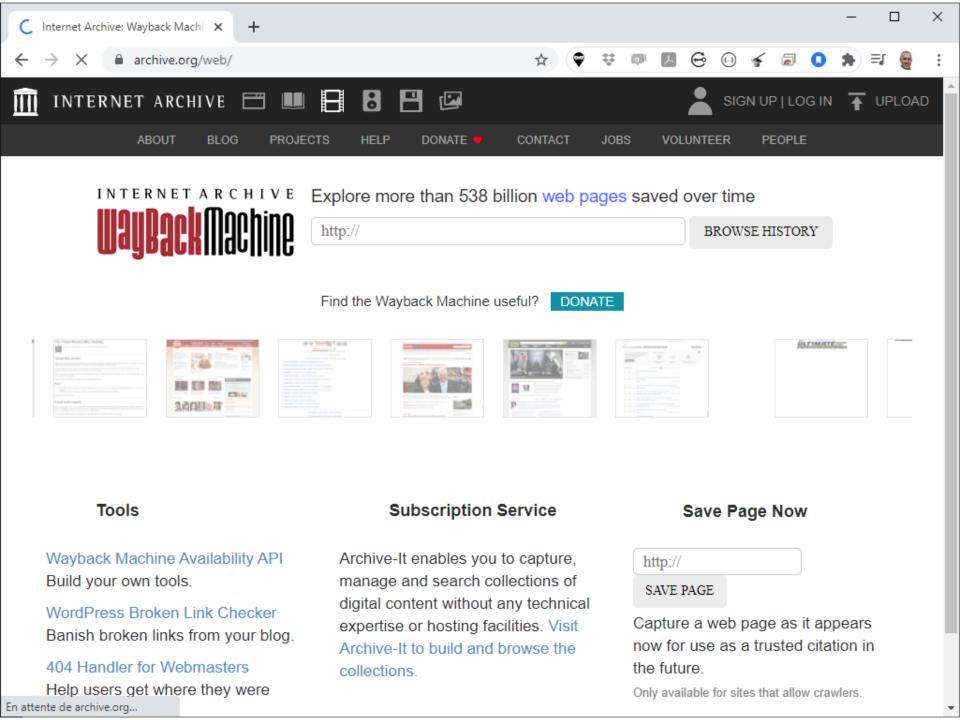
The Mail Archive - https://www.mail-archive.com

# INFORMATIONS ARCHIVÉES

Il arrive que nous ne puissions pas accéder aux informations d'un site web parce que le contenu n'est plus disponible auprès de la source d'origine.

La possibilité d'accéder à des copies archivées de ces informations permet d'accéder à des informations antérieures.

- Effectuer des recherches sur Google en utilisant des chaînes de recherche spécialement ciblées : cache:<site.com>
- 2. Utiliser les informations archivées dans la Wayback Machine (https://www.archive.org/web).



## EXTRACTION DE METADATA

L'objectif est d'identifier les données pertinentes pour l'entreprise cible.

Il peut être possible d'identifier des lieux, du matériel, des logiciels et d'autres données pertinentes à partir de messages publiés sur les réseaux sociaux.

#### **Exemples:**

- ixquick https://ixquick.com
- MetaCrawler https://metacrawler.com
- Dogpile https://www.dogpile.com
- Search.com https://www.search.com
- Jeffery's Exif Viewer https://exif.regex.info/exif.cgi

## **PARTICULIER**

#### Localisation

"Empriente" mobilet

téléphone #

type de téléphone

applications installées

## **ENTREPRISE**

#### Récolte sur sute

Inspections de sécurité physique

Balayage des fréquences (wifi, autre, ...)

Inspection de la formation au comportement des employés

Installations accessibles/ espaces partagés)Types d'équipements utilisés

#### Récolte hors-site

Emplacement des centres de données

Fourniture de réseau/fournisseur

# AUTRES FORMES DE RECOLTE

Human Intelligence (**HUMINT**)

La méthodologie implique toujours une interaction directe, qu'elle soit physique ou verbale.

- Employés clés
- Partenaires/fournisseurs

# AUTRES FORMES DE RECOLTE

Signals Intelligence (**SIGINT**):

Renseignement recueilli par l'utilisation de technologies d'interception ou d'écoute.

#### Exemple:

- Wired/Wireless Sniffer
- TAP devices

# AUTRES FORMES DE RÉCOLTE

Imagery Intelligence (IMINT):

Renseignement recueilli grâce à l'imagerie enregistrée, c'est-à-dire la photographie.

IMINT peut également faire référence au renseignement satellitaire (croisement entre IMINT et OSINT s'il s'étend à

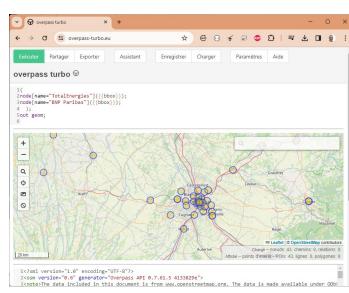
Google Earth et ses équivalents).

• https://www.geoportail.gouv.fr

https://remonterletemps.ign.fr

https://earth.google.com/web

https://overpass-turbo.eu (OSM)



# **UN EXERCICE**

Trouver une maximum d'information sur le domaine univ-toulouse.fr

- qui est gestionnaire
- la plage d'addresses d'IP
- les machines allumées
- les services
- etc.

## **UN EXERCICE**

Trouver la localisation exacte de la photo suivante ...

- données EXIF
- éléments de la photo
- (autre)



