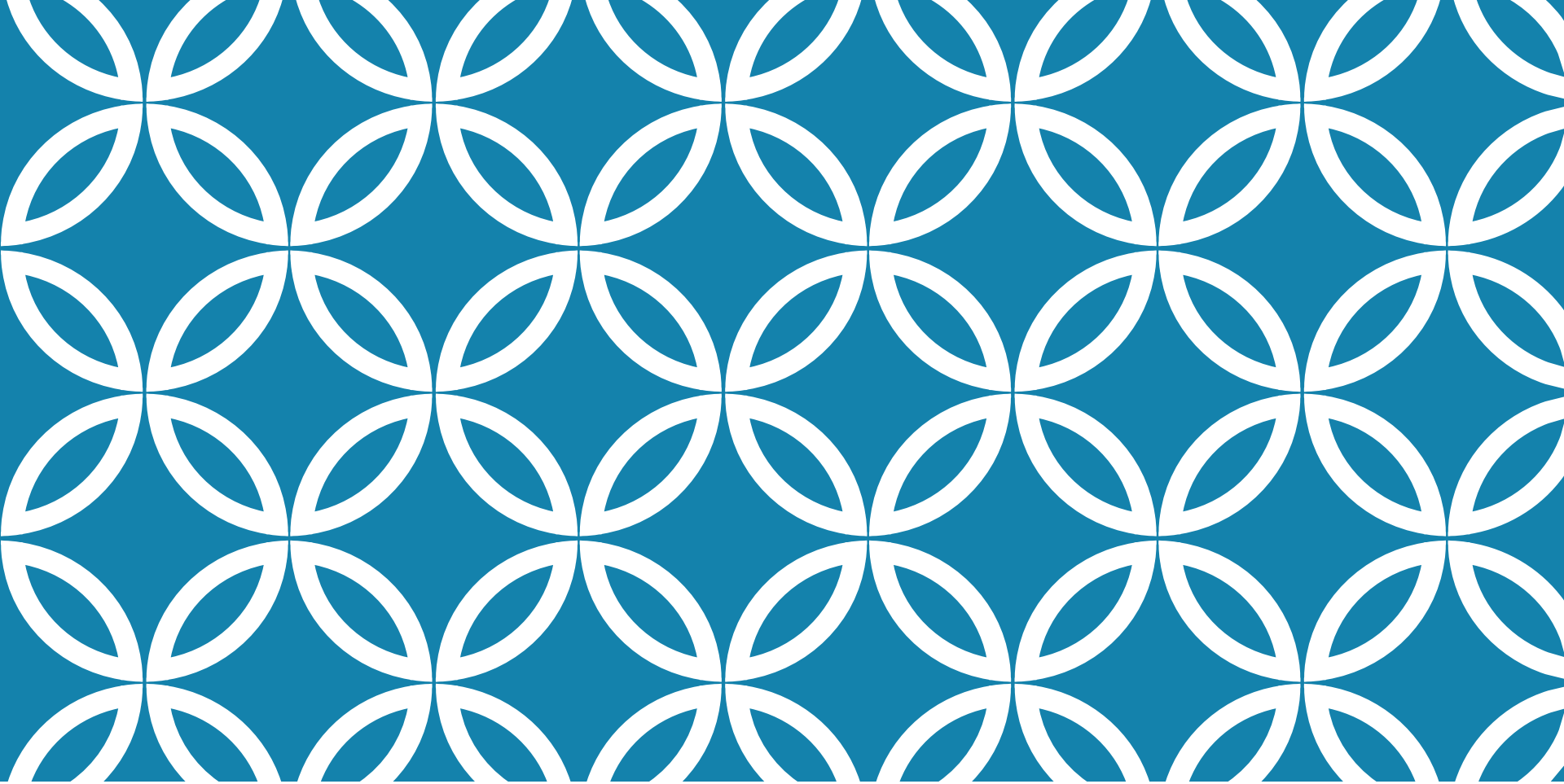


# RECONNAISSANCE

***With great knowledge, comes successful attacks!***

# COLLECTER DE L'INFORMATION

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

L'**O**pen **s**ource **int**elligence (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.

# OPEN SOURCE INTELLIGENCE (OSINT)

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 !*

# OPEN SOURCE INTELLIGENCE (OSINT)

Elle se présente sous trois formes :

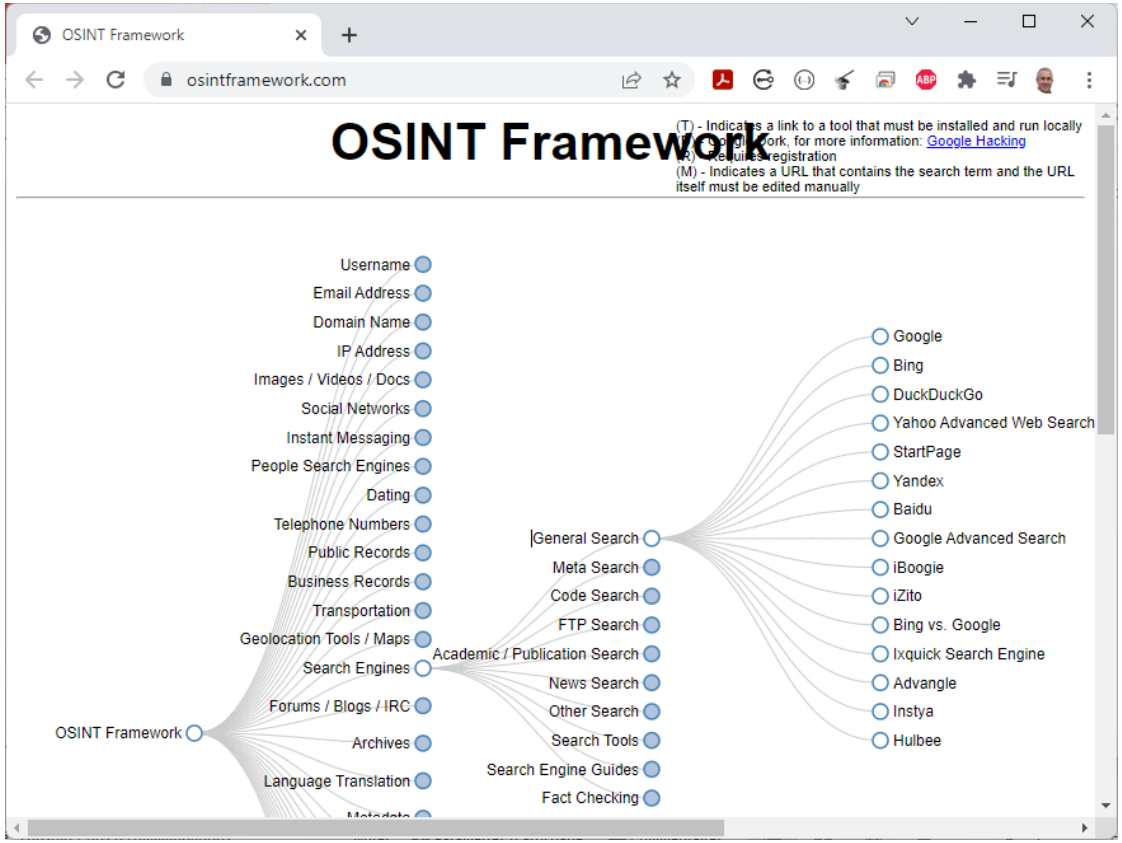
- Collecte passive d'informations
- Collecte d'informations semi-passive
- Collecte active d'informations

Utilisé pour :

- Les entreprises
- Les particuliers

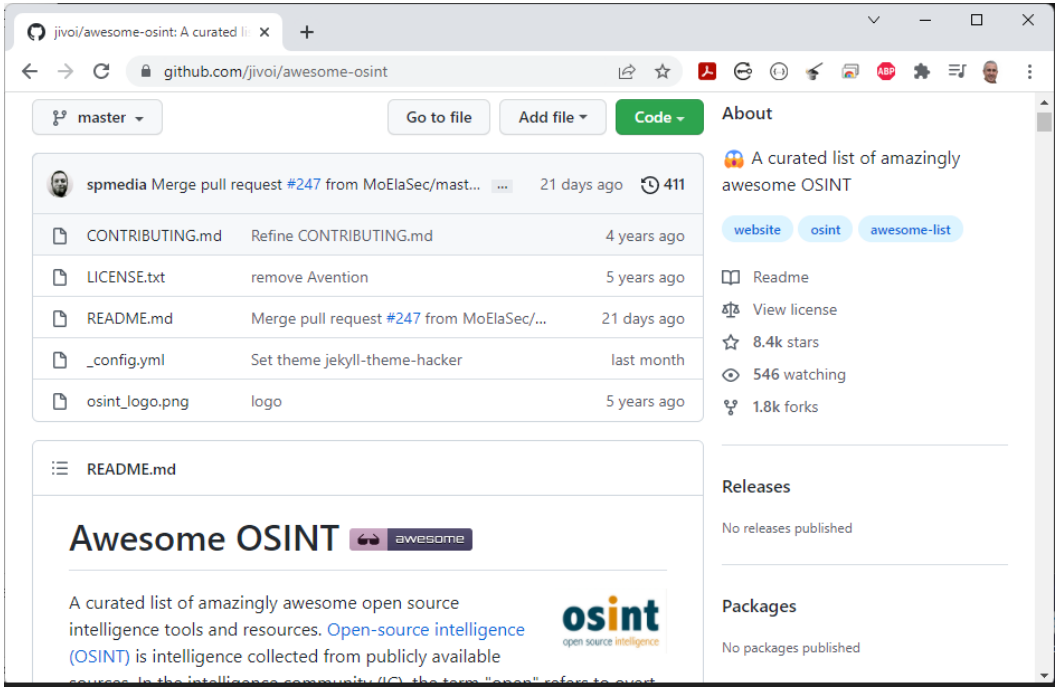
# OPEN SOURCE INTELLIGENCE (OSINT)

**https://osintframework.com**



# OPEN SOURCE INTELLIGENCE (OSINT)

**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

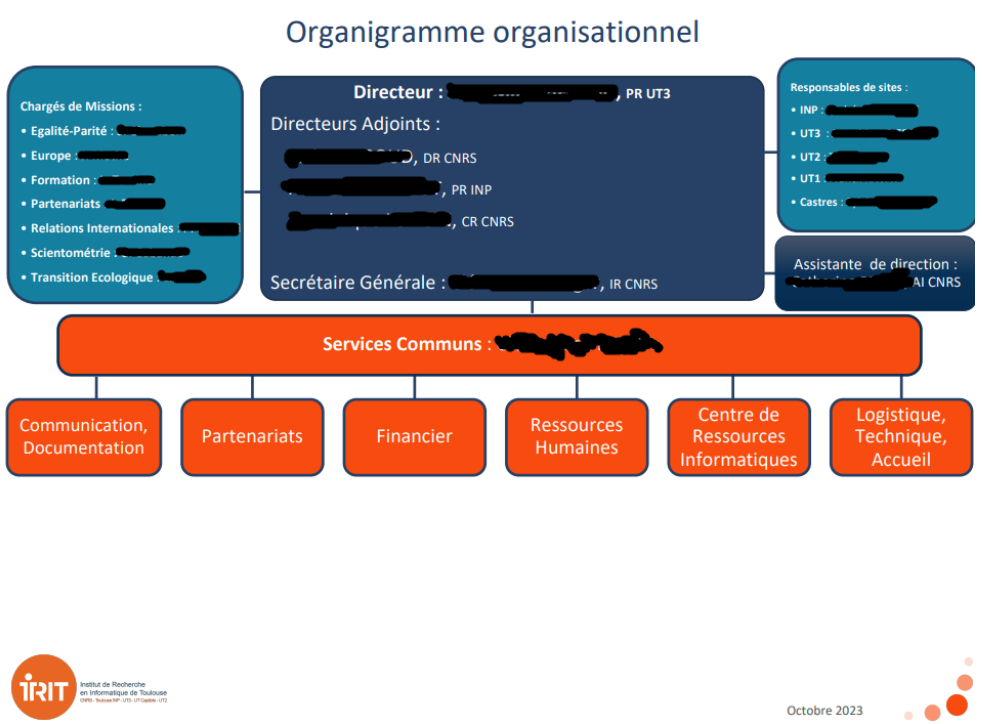
- LinkedIn, https://www.linkedin.com/mynetwork,
- Indeed, https://fr.indeed.com
- Monster, https://www.monster.com
- …

# ENTREPRISE – ORGANISATION

Identification des positions dans l'entreprise

Transactions

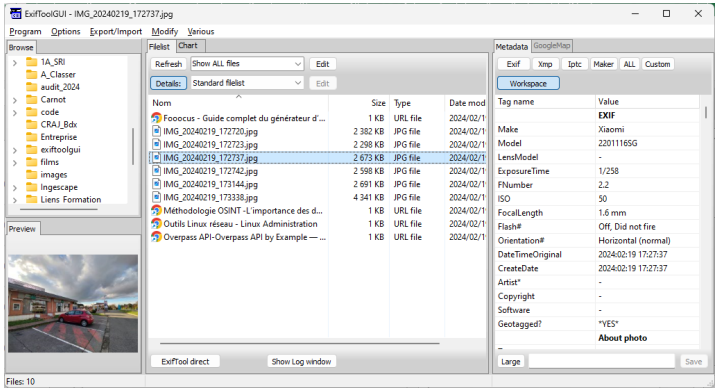
Affiliations

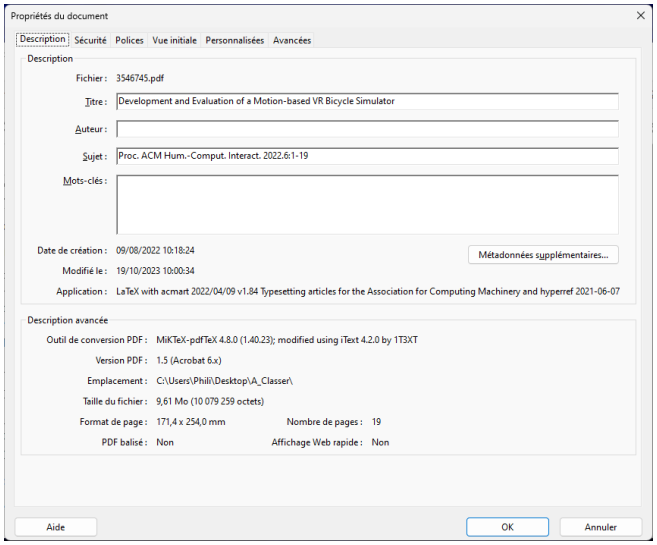


# ENTREPRISE – NUMERIQUE

Métadatas

Communications Marketing



# OUTILS

Outil CLI (commande en ligne) - wget

Example: Retrieve only PDFs from a site

```
$ wget -nd -r -l3 -e robots=off --no-check-certificate
-A .pdf https://contremesures.fr
```

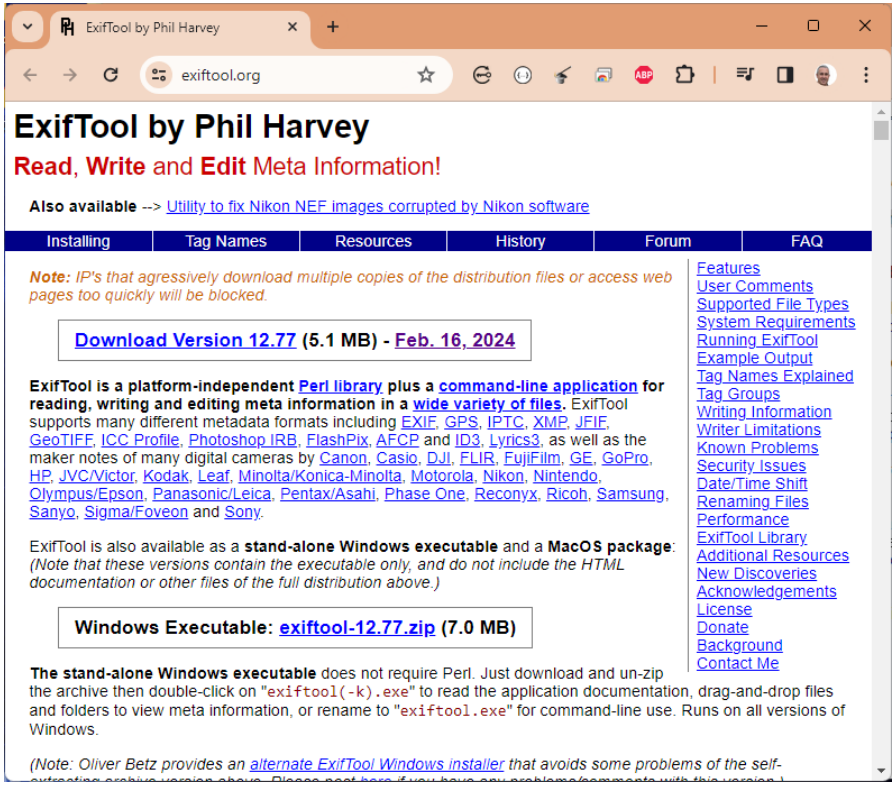
https://www.mythicsoft.com/agentransack


Des outils comme grep

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

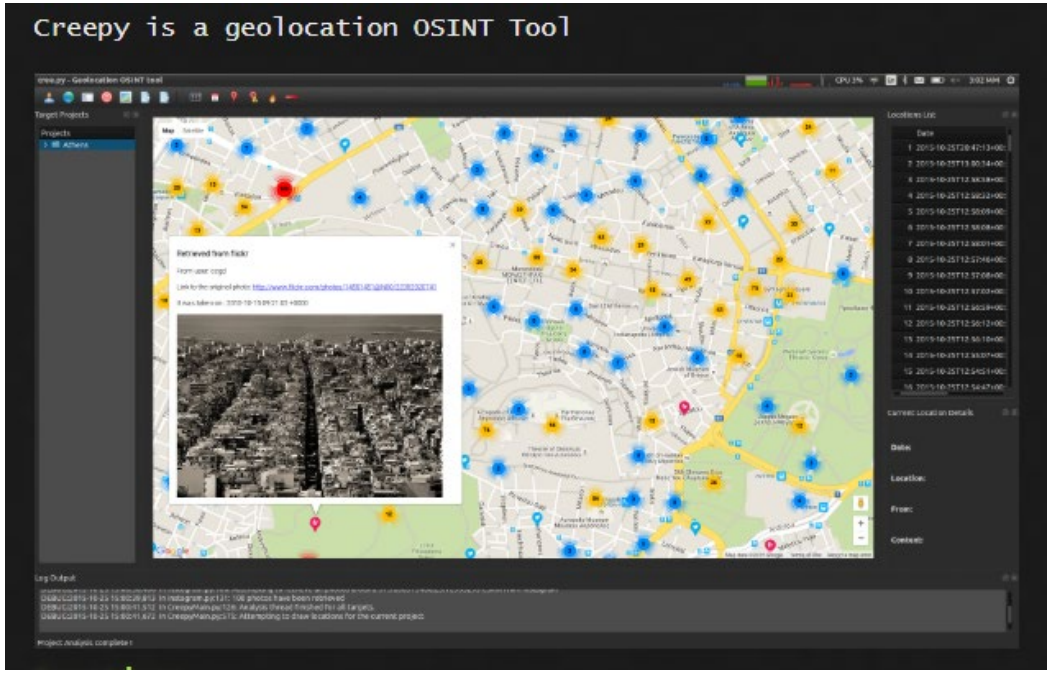
Fuite de métadonnées

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.



Creepy by ilektrojohn

www.geocreepy.com

# ./ Creepy

A Geolocation OSINT Tool. Offers geolocation information gathering through social networking platforms.

## Windows Downloads

Current version : v1.4.1

Download 64bit Windows installer | Download 32bit Windows installer

## OSX Downloads

Current version : v1.4.1

Download OSX installer

## Source Code Downloads

Download as .zip | Download as .tar.gz | View on GitHub

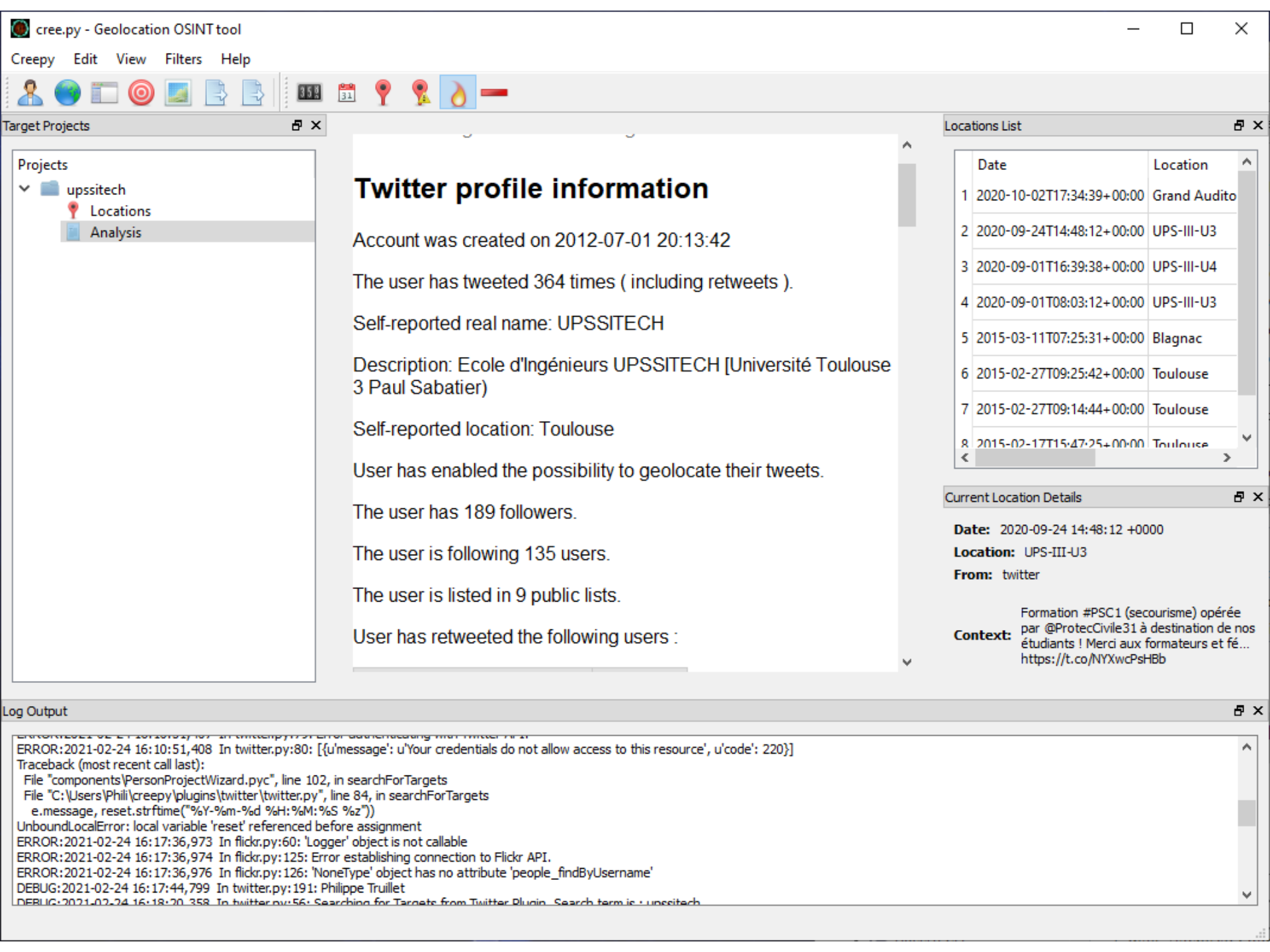
## Plugin Downloads

Download as .zip | Download as .tar.gz

---

## Creepy

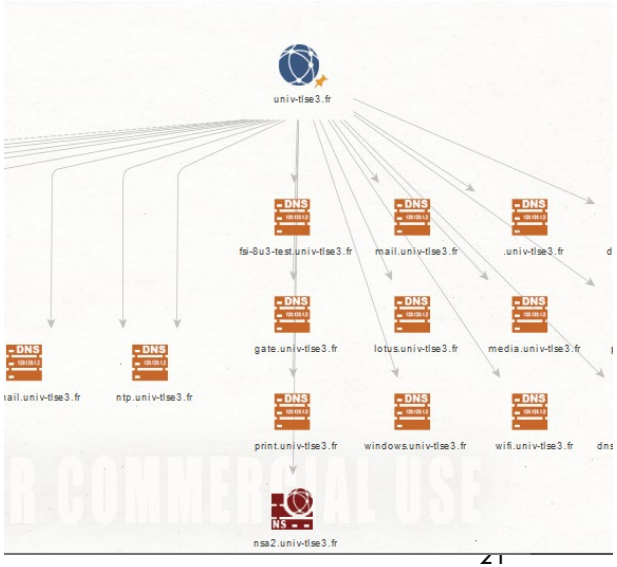
Creepy is a geolocation OSINT Tool

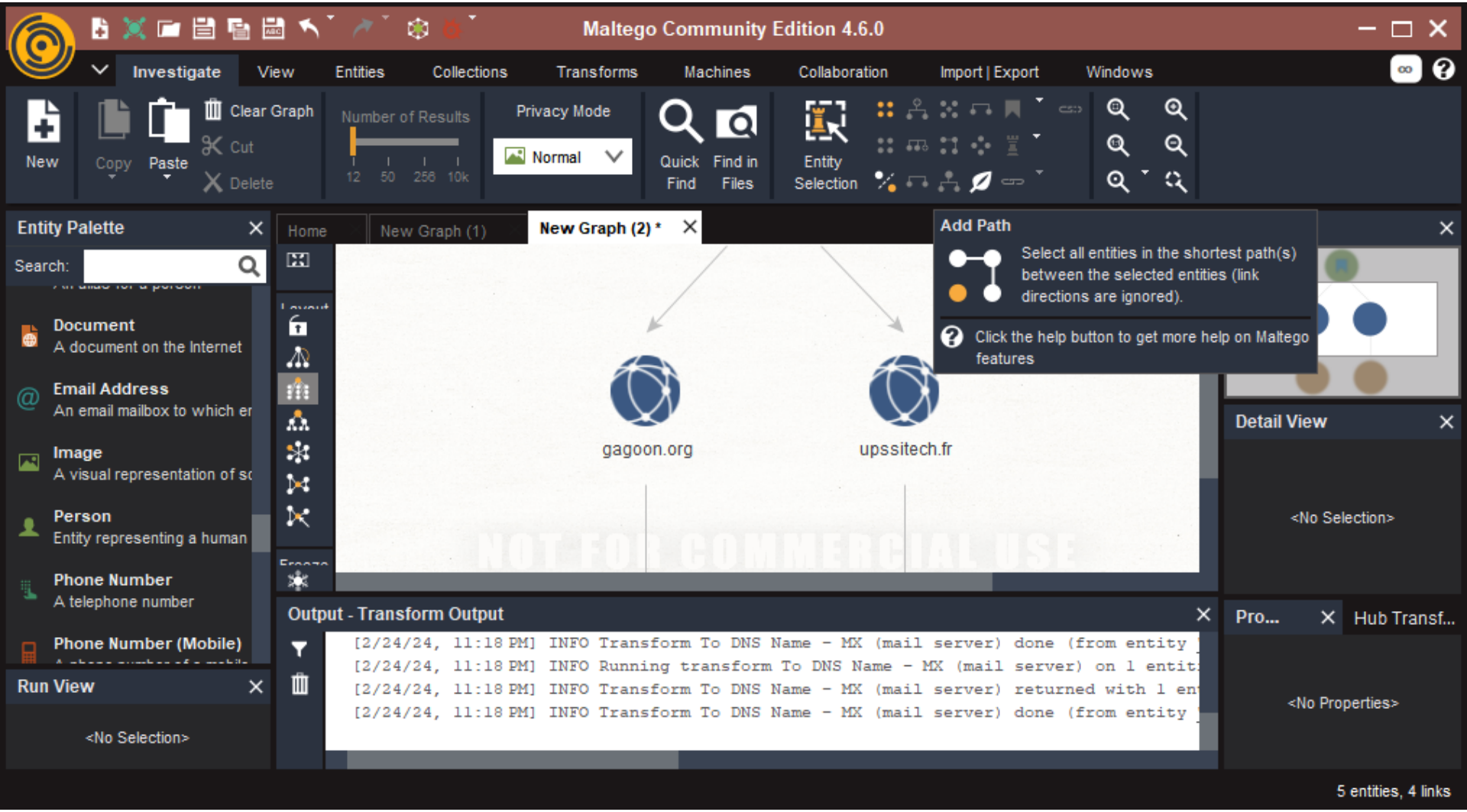

cree.py - Geolocation OSINT tool
Creepy Edit View Filters Help
Target Projects
Projects
upssitech
Locations
Analysis
Twitter profile information
Account was created on 2012-07-01 20:13:42
The user has tweeted 364 times ( including retweets ).
Self-reported real name: UPSSITECH
Description: Ecole d'Ingénieurs UPSSITECH [Université Toulouse 3 Paul Sabatier)
Self-reported location: Toulouse
User has enabled the possibility to geolocate their tweets.
The user has 189 followers.
The user is following 135 users.
The user is listed in 9 public lists.
User has retweeted the following users :
Locations List
Date
Location
1 2020-10-02T17:34:39+00:00 Grand Audito
2 2020-09-24T14:48:12+00:00 UPS-III-U3
3 2020-09-01T16:39:38+00:00 UPS-III-U4
4 2020-09-01T08:03:12+00:00 UPS-III-U3
5 2015-03-11T07:25:31+00:00 Blagnac
6 2015-02-27T09:25:42+00:00 Toulouse
7 2015-02-27T09:14:44+00:00 Toulouse
Current Location Details
Date: 2020-09-24 14:48:12 +0000
Location: UPS-III-U3
From: twitter
Context: Formation #PSC1 (secourisme) opérée par @ProtecCivile31 à destination de nos étudiants ! Merci aux formateurs et fé... https://t.co/NYXwcPsHBb
Log Output
ERROR:2021-02-24 16:10:51,408 In twitter.py:80: [{u'message': u'Your credentials do not allow access to this resource', u'code': 220}]
Traceback (most recent call last):
File "components\PersonProjectWizard.pyc", line 102, in searchForTargets
File "C:\Users\Phili\creepy\plugins\twitter\twitter.py", line 84, in searchForTargets
e.message, reset.strftime("%Y-%m-%d %H:%M:%S %z"))
UnboundLocalError: local variable 'reset' referenced before assignment
ERROR:2021-02-24 16:17:36,973 In flickr.py:60: 'Logger' object is not callable
ERROR:2021-02-24 16:17:36,974 In flickr.py:125: Error establishing connection to Flickr API.
ERROR:2021-02-24 16:17:36,976 In flickr.py:126: 'NoneType' object has no attribute 'people_findByUsername'
DEBUG:2021-02-24 16:17:44,799 In twitter.py:191: Philippe Truillet

# 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.

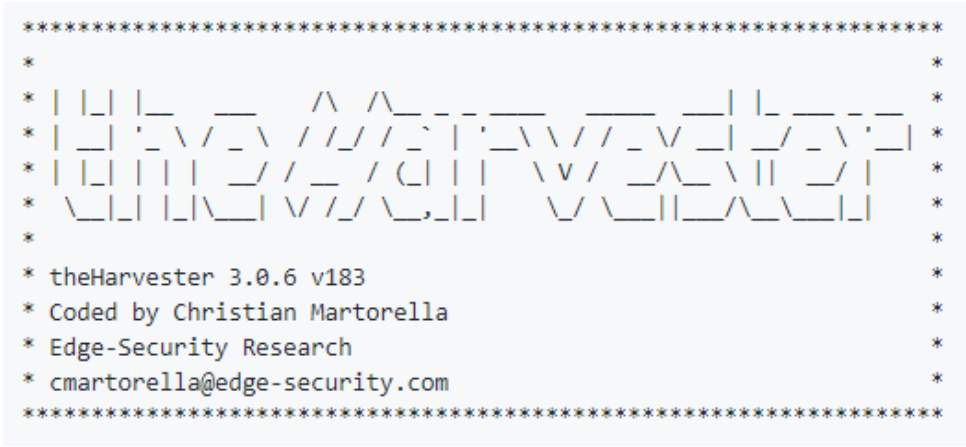



Maltego Community Edition 4.6.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
New
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
12
50
256
10k
Privacy Mode
Normal
Quick Find
Find in Files
Entity Selection
Entity Palette
Search:
Document
A document on the Internet
Email Address
An email mailbox to which er
Image
A visual representation of sc
Person
Entity representing a human
Phone Number
A telephone number
Phone Number (Mobile)
Run View
<No Selection>
Home
New Graph (1)
New Graph (2) *
gagoon.org
upssitech.fr
NOT FOR COMMERCIAL USE
Add Path
Select all entities in the shortest path(s) between the selected entities (link directions are ignored).
Click the help button to get more help on Maltego features
Detail View
<No Selection>
Output - Transform Output
[2/24/24, 11:18 PM] INFO Transform To DNS Name - MX (mail server) done (from entity
[2/24/24, 11:18 PM] INFO Running transform To DNS Name - MX (mail server) on 1 entit
[2/24/24, 11:18 PM] INFO Transform To DNS Name - MX (mail server) returned with 1 en
[2/24/24, 11:18 PM] INFO Transform To DNS Name - MX (mail server) done (from entity
Pro...
Hub Transf...
<No Properties>
5 entities, 4 links

# 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).

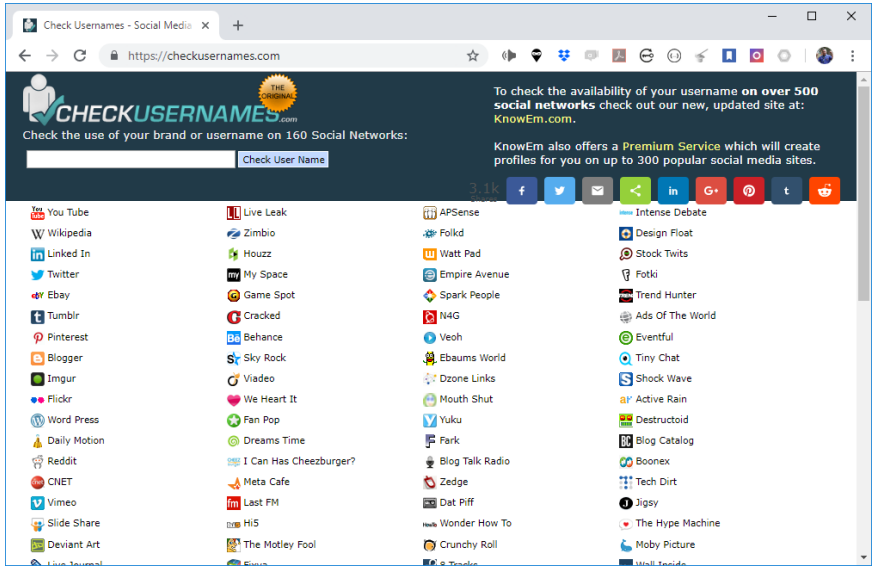
→ **http://www.edge-security.com**



# 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.

1. 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**).

Internet Archive: Wayback Machi

archive.org/web/

INTERNET ARCHIVE

SIGN UP | LOG IN UPLOAD

ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE

INTERNET ARCHIVE
WayBackMachine

Explore more than 538 billion web pages saved over time

http://

BROWSE HISTORY

Find the Wayback Machine useful? DONATE

## Tools

Wayback Machine Availability API
Build your own tools.

WordPress Broken Link Checker
Banish broken links from your blog.

404 Handler for Webmasters
Help users get where they were

## Subscription Service

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. Visit Archive-It to build and browse the collections.

## Save Page Now

http://

SAVE PAGE

Capture a web page as it appears now for use as a trusted citation in the future.

Only available for sites that allow crawlers.

En attente de archive.org...

# 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**

**“Empreinte” mobile**

téléphone #

type de téléphone

applications installées

# ENTREPRISE

## Récolte sur site

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

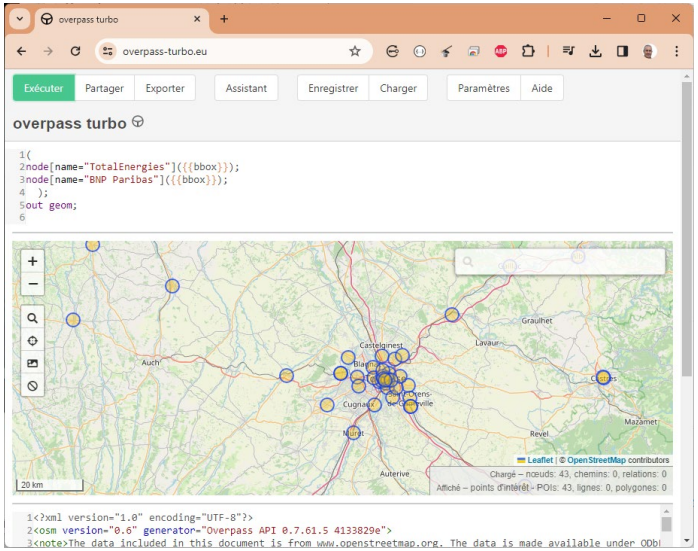
# AUTRES FORMES DE RÉCOLTE

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 un maximum d'informations sur le domaine **univ-toulouse.fr**

- **qui est gestionnaire**
- **la plage d'adresses 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)


BNP PARIBAS
BNP PARIBAS