



HAL
open science

OSINT pour la forensique

Tanguy Gernot

► **To cite this version:**

Tanguy Gernot. OSINT pour la forensique. Master. Forensique, Campus 2 Caen, France. 2024.
hal-04453439

HAL Id: hal-04453439

<https://hal.science/hal-04453439>

Submitted on 12 Feb 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0
International License

OSINT POUR LA FORENSIQUE

Tanguy Gernot
Ingénieur de recherche CNRS

tanguy.gernot@cncrs.fr
<https://gernot.fr>



1. Introduction
2. Recherches Avancées
3. Retour vers le passé
4. Contenus multimédia
5. "Anonymat"
6. Dans la vraie vie
7. Éléments juridiques
8. Conclusion

1. Introduction
2. Recherches Avancées
3. Retour vers le passé
4. Contenus multimédia
5. "Anonymat"
6. Dans la vraie vie
7. Éléments juridiques
8. Conclusion

Kesako ?

- ▶ OSINT : Open Source INTelligence
- ▶ ROSO : Renseignement d'Origine Sources Ouvertes

Concepts

- ▶ Récupérer des informations disponibles publiquement.
- ▶ Agir légalement.
- ▶ Agrégation et analyse des informations pour répondre à une question.
- ▶ Pas de contact !
- ▶ Connexions admises (twitter, linkedin, ...).

Pourquoi ?

Problématiques → Renseignements → Décisions

Pour qui ?

- ▶ Police
- ▶ Armées
- ▶ Presse
- ▶ Entreprises
- ▶ ...

Pour quoi ?

- ▶ Surveillance d'individu
- ▶ Vérification du niveau de vie
- ▶ Veille concurrentielle
- ▶ Vérification de fait
- ▶ Recherche de personnes (!)
- ▶ Curiosité ?

- ▶ Validation par plusieurs méthodes / sources.
- ▶ Pivot : dévier la recherche depuis une nouvelle information validée.
- ▶ Objectifs ou besoins \implies Collectes \iff Analyses \implies Décisions

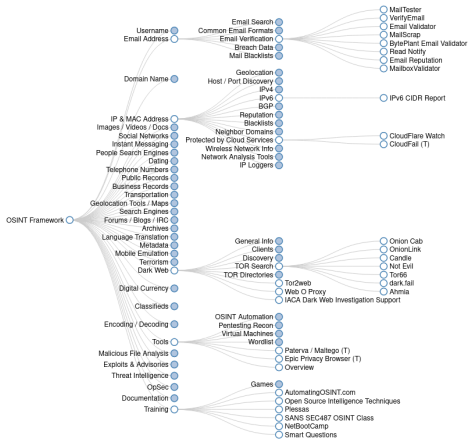
Introduction

Liens avec la cybersécurité et la forensique

- ▶ Ingénierie sociale
- ▶ Attaque au président
- ▶ Phishing personnalisé
- ▶ Dictionnaire personnalisé pour le cassage de mot de passe.

Introduction

Vision générale des outils



<https://osintframework.com/>

1. Introduction
2. Recherches Avancées
3. Retour vers le passé
4. Contenus multimédia
5. "Anonymat"
6. Dans la vraie vie
7. Éléments juridiques
8. Conclusion

Quels moteurs de recherche ?

- ▶ Google
- ▶ Chine : Baidu
- ▶ Russie : Yandex
- ▶ Vie privée : DuckDuckGo

Pour quoi ?

- ▶ Recherche avancée
- ▶ Recherche booléenne
- ▶ Recherche pointue
- ▶ Filtrage

Exemples éthiques

- ▶ Guillemets : Suite de mots dans ordre déterminé *"unicaen sécurité informatique"*
- ▶ Proximité non immédiate : *"unicaen" NEAR/54 "sécurité informatique"*
- ▶ Limiter la recherche à un nom de domaine :
"unicaen" NEAR/24 "sécurité informatique" AND site:unicaen.fr
- ▶ Format URL : *inurl:login.php AND inurl:id*
- ▶ Type de fichier : *filetype:pdf*

Google Dorking visuellement

https://www.google.com/advanced_search



Recherche avancée

Trouvez des pages avec...

tous les mots suivants :

ce mot ou cette expression exact(e) :

l'un des mots suivants :

aucun des mots suivants :

nombres compris entre :

et

Pour effectuer cette opération dans le champ de recherche

Saisissez les mots importants : terrier tricolore

Ajoutez des guillemets autour des mots exacts : "terrier"

Saisissez OR entre tous les mots à inclure : miniature OR standard

Placez un signe - (moins) devant les mots à exclure :
-rongeur, -"Jack Russell"

Placez deux points entre les nombres, et ajoutez une unité de mesure :
10..35 kilos, 300..500 USD, 2010..2011

Affinez ensuite la recherche par...

langue :

toutes les langues

Rechercher des pages dans la langue sélectionnée

région :

tous les pays/territoires

Rechercher des pages publiées dans une région précise

dernière mise à jour :

à une date indifférente

Rechercher des pages mises à jour durant la période spécifiée

site ou domaine :

Rechercher sur un site (tel que wikipedia.org) ou limitez vos résultats à un domaine tel que .edu, .org ou .gov

termes apparaissant :

n'importe où dans la page

Rechercher des termes dans la page entière, dans le titre d'une page, dans une adresse Web ou dans des liens vers la page recherchée

type de fichier :

tous les formats

Rechercher des pages dans le format que vous préférez

droits d'usage :

non filtré par licence

Rechercher des pages que vous êtes libre d'utiliser

Recherche avancée

Exemples

- ▶ Localisation ville: *"near:caen within:5km"*
- ▶ Localisation exacte : *geocode:LATITUDE, LONGITUDE, RAYON*
- ▶ Exemple Campus 2 (google maps) + twitter
- ▶ Demo <https://birdhunt.co/>

Google Image, Yandex Image (demo)

1. Introduction
2. Recherches Avancées
- 3. Retour vers le passé**
4. Contenus multimédia
5. "Anonymat"
6. Dans la vraie vie
7. Éléments juridiques
8. Conclusion

► `cache:site.fr` permet d'avoir la dernière version récupérée du site web

Ceci est le cache Google de <https://www.unicaen.fr/> [X]. Il s'agit d'un instantané de la page telle qu'elle était affichée le 23 janv. 2024 06:26:47 GMT. La [page actuelle](#) [X] peut avoir changé depuis cette date. [En savoir plus.](#) [X]

[Version intégrale](#) [Version en texte seul](#) [Afficher la source](#)

Astuce : Pour trouver rapidement votre terme de recherche sur cette page, appuyez sur **Ctrl+F** ou sur **⌘+F** (Mac), puis utilisez la barre de recherche.



UNIVERSITÉ
CAEN
NORMANDIE

[actualités](#) [bibliothèques](#) [laboratoires](#) [UFR, écoles, instituts](#) [accès rapide](#) [vous êtes](#) [F](#)

FORMATION

RECHERCHE

INTERNATI

Autres options

Partager

Enregistrer

Commentaires

En cache

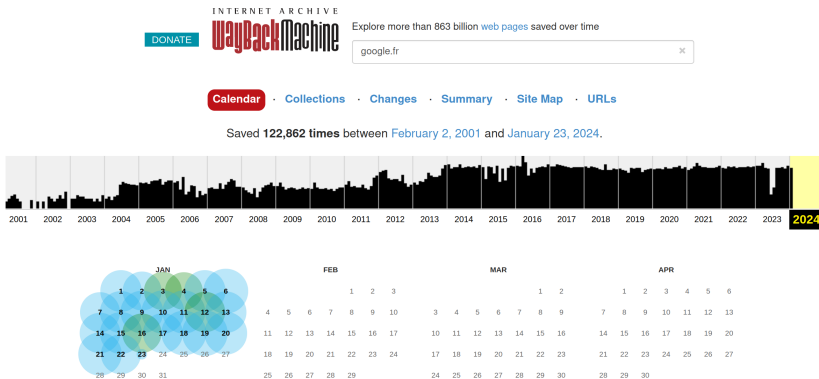
À propos de ce résultat

Bêta



<https://www.unicaen.fr/>

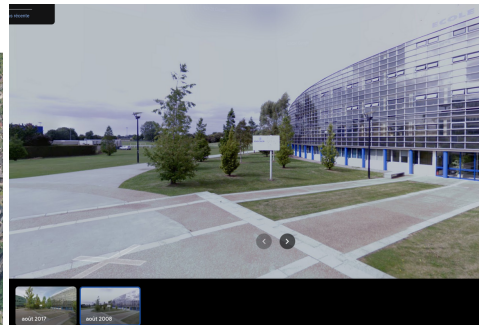
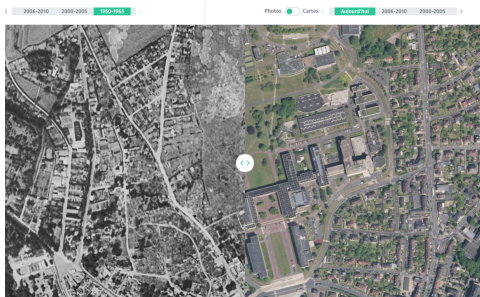
- Organisation à but non lucratif consacrée à l'archivage du Web.



- Possibilité de sauvegarde immédiate : preuve horodatée
<http://web.archive.org/save>

<https://remonterletemps.ign.fr/>

<https://www.google.fr/maps>



Cartes isochrones

<https://www.geoportail.gouv.fr/carte>



1. Introduction
2. Recherches Avancées
3. Retour vers le passé
- 4. Contenus multimédia**
5. "Anonymat"
6. Dans la vraie vie
7. Éléments juridiques
8. Conclusion

Image

- ▶ EXIF : Exchangeable image file format
- ▶ <https://jimpl.com/>
- ▶ Attention à l'envoi d'une photo !



(a) exiftool



(b) exiftool -all=

1. Introduction
2. Recherches Avancées
3. Retour vers le passé
4. Contenus multimédia
- 5. "Anonymat"**
6. Dans la vraie vie
7. Éléments juridiques
8. Conclusion

Informations révélant l'identité

- ▶ IP
- ▶ Numéro de téléphone
- ▶ Mail
- ▶ Mot de passe
- ▶ Fingerprint du navigateur
- ▶ Identité
- ▶ ...

`https://www.fakenamegenerator.com/`
`https://thispersondoesnotexist.com/`
`https://pimeyes.com`

Michel Talon

33, Place Napoléon
56600 LANESTER

Curious what **Michel** means? [Click here to find out!](#)

Mother's maiden name Sarrazin
NIRPP 1930885243828 46
Geo coordinates [47.846442, -3.420418](#)

PHONE

Phone 02.78.56.40.75
Country code 33

BIRTHDAY

Birthday August 7, 1993
Age 30 years old
Tropical zodiac Leo

ONLINE

Email Address MichelTalon@dayrep.com
This is a real email address. [Click here to activate it!](#)
Username Hortudy1993
Password hiPuphiewah0
Website ZeroDividend.fr
Browser user agent Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.131 Safari/537.36

FINANCE

MasterCard 5462 8187 3063 0824



- ▶ Qu'est-ce qui caractérise mon navigateur ?
- ▶ `https://amiunique.org/fingerprint`

- ▶ `https://whatismyipaddress.com/`
- ▶ TOR (demo)
- ▶ Noeud d'entrée, noeud de sortie, noeud intermédiaire
- ▶ Tails

- ▶ Crossmatch email
- ▶ <https://epieos.com>
- ▶ Comment lutter ?
- ▶ Catch all email.
- ▶ Jetable (site spécialisé, icloud, ...).
- ▶ Même problématique pour les numéros de téléphone ([onoff.app](#))
- ▶ Pseudo : <https://blackbird-osint.herokuapp.com/>

1. Introduction
2. Recherches Avancées
3. Retour vers le passé
4. Contenus multimédia
5. "Anonymat"
- 6. Dans la vraie vie**
7. Éléments juridiques
8. Conclusion

- ▶ <https://www.interpol.int/How-we-work/Notices/Red-Notices/View-Red-Notices>
- ▶ <https://www.europol.europa.eu/stopchildabuse>
- ▶ <https://www.fbi.gov/wanted/ecap/seeking-information>
- ▶ <https://www.accce.gov.au/what-we-do/trace-an-object>
- ▶ **Attention : certaines personnes disparaissent volontairement. Une fois retrouvée, il faut son accord pour transmettre les résultats de l'enquête.**
- ▶ **Cas récurrent : conjoint(e) violent.**

1. Introduction
2. Recherches Avancées
3. Retour vers le passé
4. Contenus multimédia
5. "Anonymat"
6. Dans la vraie vie
7. Éléments juridiques
8. Conclusion

- ▶ Le cadre légal de l'OSINT
- ▶ <https://ozint.eu/contributions/Livre%20blanc-Le%20cadre%20legal%20OSINT-2023.pdf>
- ▶ Droit d'accès, droit de collecter, droit de réutiliser.
- ▶ Scraping : soustraire des données sans le consentement de leur propriétaire constitue le délit pénal de vol. (linkedin)
- ▶ Téléchargement d'une fuite de données : recel de vol.
- ▶ Stalking / Doxing : délit pénal de traitement frauduleux, déloyal ou illicite de données personnelles.

Checklist & questions à se poser AVANT une enquête OSINT

Voici les principales questions à se poser AVANT de pratiquer une enquête OSINT :

- Ai-je un **accès légitime** aux données ? (*accès dans un STAD, lettre de mission...*)
- Les données sont-elles de **provenance légitime** ? (*leak, fuites de données...*)
- Ai-je le droit de **copier et d'utiliser** cette information ? (*CGU, propriété intellectuelle...*)
- L'information ne comporte-t-elle pas d'indication manifeste qu'elle est **confidentielle** ?
- Si je révèle cette information publiquement, je m'assure de ne pas risquer de **nuire** à quelqu'un ? (*doxing*)
- Suis-je en mesure de **sourcer** chaque élément ?
- Est-ce possible que quelqu'un d'autre puisse **refaire** le processus/cheminement jusqu'à l'information trouvée ? (*réversibilité de la méthode, des pivots*)
- Est-ce que l'ensemble des cases de cette checklist sont bien cochées ? Si oui, je peux démarrer mon investigation en toute **sérénité** !

<https://ozint.eu/contributions/Livre%20blanc-Le%20cadre%20legal%20OSINT-2023.pdf>

- ▶ Signaler une faille à l'ANSSI

- ▶ `https:`

- `//www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000033203174`

« Art. L. 2321-4.-Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'[article 40 du code de procédure pénale](#) n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.

« L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.

« L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

› [Article 323-3-1](#)

[Modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 25](#)

Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les [articles 323-1 à 323-3](#) est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Rappels juridiques

<https://technique-et-droit-du-numerique.fr/le-blog-en-bd/>



- ▶ <https://ozint.eu/>
- ▶ <https://osintframework.com/>
- ▶ Institut des Hautes Etudes de Défense Nationale
- ▶ <https://osintfr.com/fr>

[Merci]

Questions ?

`tanguy.gernot@cnrs.fr`
`https://gernot.fr`