OSINT pour la forensique

Tanguy Gernot

OSINT POUR LA FORENSIQUE

Tanguy Gernot
Ingénieur de recherche CNRS

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

GREYC
Laboratoire de recherche en sciences du numérique

Normandie Université

UNICAEN

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

cnrs

Plan

Plan

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 $\longrightarrow$ Renseignements $\longrightarrow$ 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 ?

Introduction

Comment ?

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

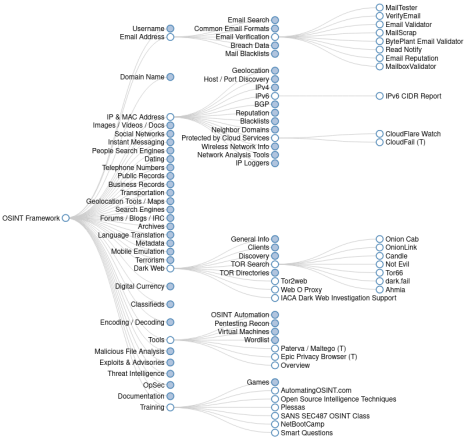
Introduction

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/

Plan

Quels moteurs de recherche ?

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

Google Dorking / Google hacking

Pour quoi ?

- Recherche avancée
- Recherche booléenne
- Recherche pointue
- Filtrage

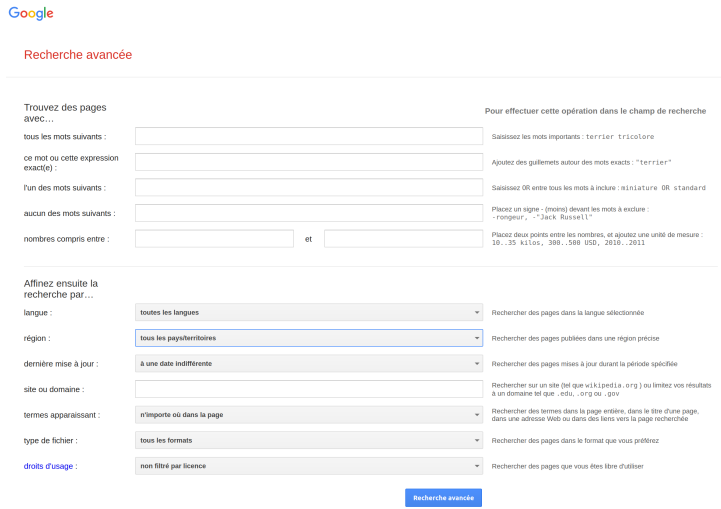
Google Dorking / Google hacking

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



Twitter

Exemples

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

Recherche d'image inversée

Google Image, Yandex Image (demo)

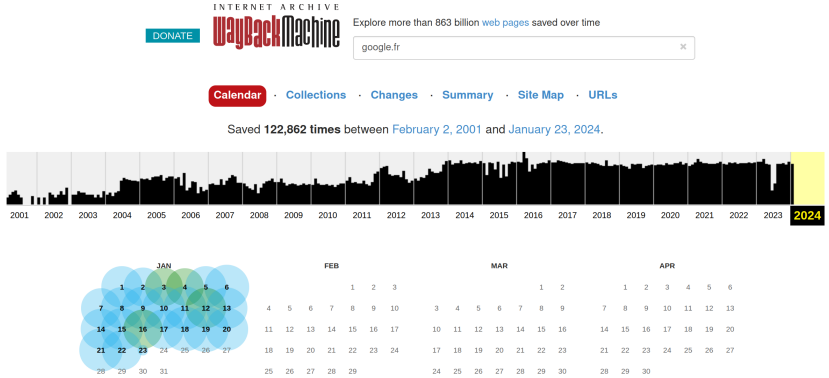
Plan

Google cache

- *cache:site.fr* permet d'avoir la dernière version récupérée du site web

Web Archive

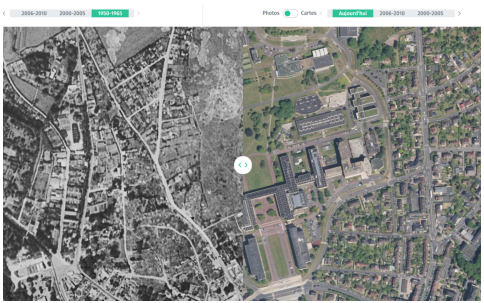
- Organisation à but non lucratif consacrée à l'archivage du Web.

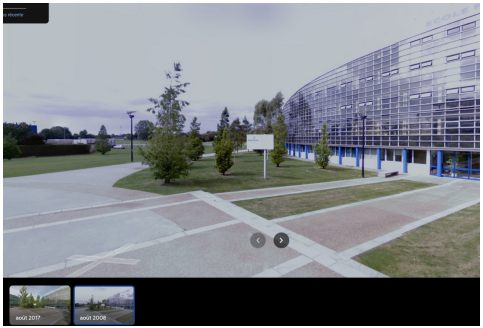


- Possibilité de sauvegarde immédiate : preuve horodatée
  `http://web.archive.org/save`

Cartes

https://remonterletemps.ign.fr/
https://www.google.fr/maps





Cartes isochrones

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

Plan

Image

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

(a) exiftool

(b) exiftool -all=

Plan

Informations techniques

Informations révélant l'identité

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

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

Browser Fingerprint

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

IP

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

Email

- 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/`

Plan

Dans la vraie vie

- `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.

Plan

Rappels juridiques

- 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.

Rappels juridiques

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`

Rappels juridiques - Exception

- 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. »

Rappels juridiques - Exception

› **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/

Sources / Pointeurs

- 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