

# L'OSINT/ROSO en pratique

- ▶ Principes et exemples simples
- ▶ Enjeux pour les documentalistes

Serge Courrier ▶ 15 décembre 2021

adbs   
Secteur ATCF

AMENAGEMENT,  
TRANSPORT,  
CONSTRUCTION,  
ENVIRONNEMENT

# Se repérer dans les sigles

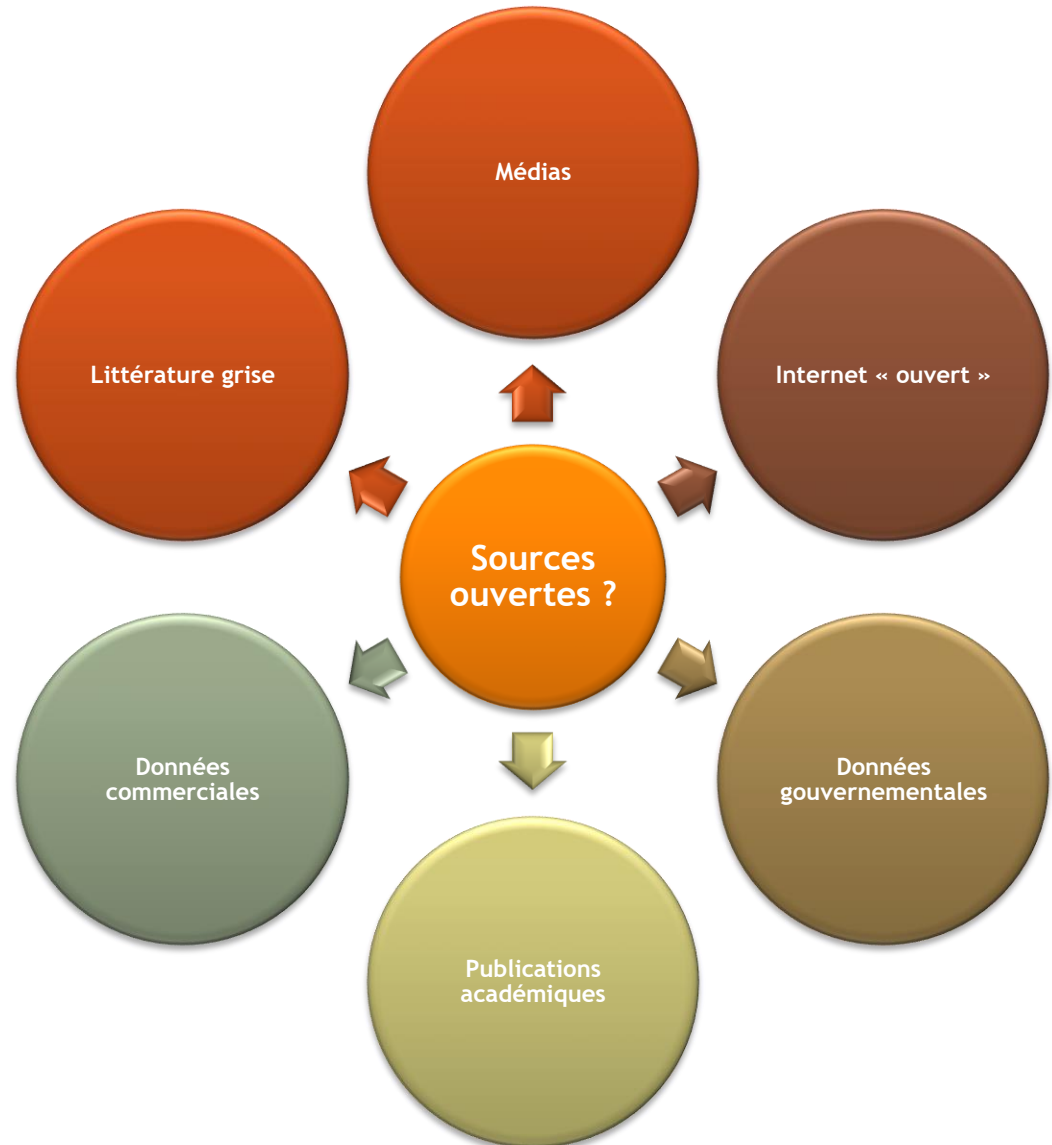
# Se repérer dans les sigles

**OSINT**  
**Open Source Intelligence**

**ROSO**  
**Renseignement d'origine  
sources ouvertes**

*« renseignement produit à partir d'informations publiquement accessibles, qui sont collectées, exploitées et diffusées en temps utile à une audience appropriée afin de répondre à un besoin spécifique en matière de renseignement. »*

Source : [National Defense Authorization Act for Fiscal Year 2006](#). (Sec. 931)



**OSINT = uniquement via Internet ?**

Oui... et non

**OSINT = uniquement la captation ?**

Non

**OSINT ≠ HUMINT ?**

Oui

**OSINT ≠ Piratage ?**

Oui

**IMINT** : Imagery intelligence /  
Renseignement d'origine image (ROIM)

**GEOINT** : Geospatial Intelligence /  
Renseignement géospatial

**SOCMINT** : Social Media Intelligence /  
Renseignement Réseaux Sociaux

**WEBINT/CYBINT/RECON passive** : renseignement  
à partir de sites web, noms de domaines, IP...

# Le foisonnement du ...INT

Acronym	Meaning
OSINT	Open-Source Intelligence
SOCMINT	Social Media Intelligence
GEOINT	Geo-Spatial Intelligence
IMINT	Imagery Intelligence
ORBINT	Orbital Intelligence
VATINT	Vehicle and Transportation Intelligence
SIGINT	Signals Intelligence
TECHINT	Technical Intelligence
FININT	Financial Intelligence
AML	Anti Money Laundering
TRADINT	Trade Intelligence
CORPINT	Corporate Intelligence
HUMINT	Human Intelligence
SE	Social Engineering
MASINT	Measurement and Signature Intelligence
DNINT	Digital Network Intelligence
PERSINT	Personality Intelligence
RUMINT	Rumor Intelligence
OPSEC	Operation Security
TSCM	Technical Surveillance Counter-Measures
CI	Counter-Intelligence/Confidential Informant

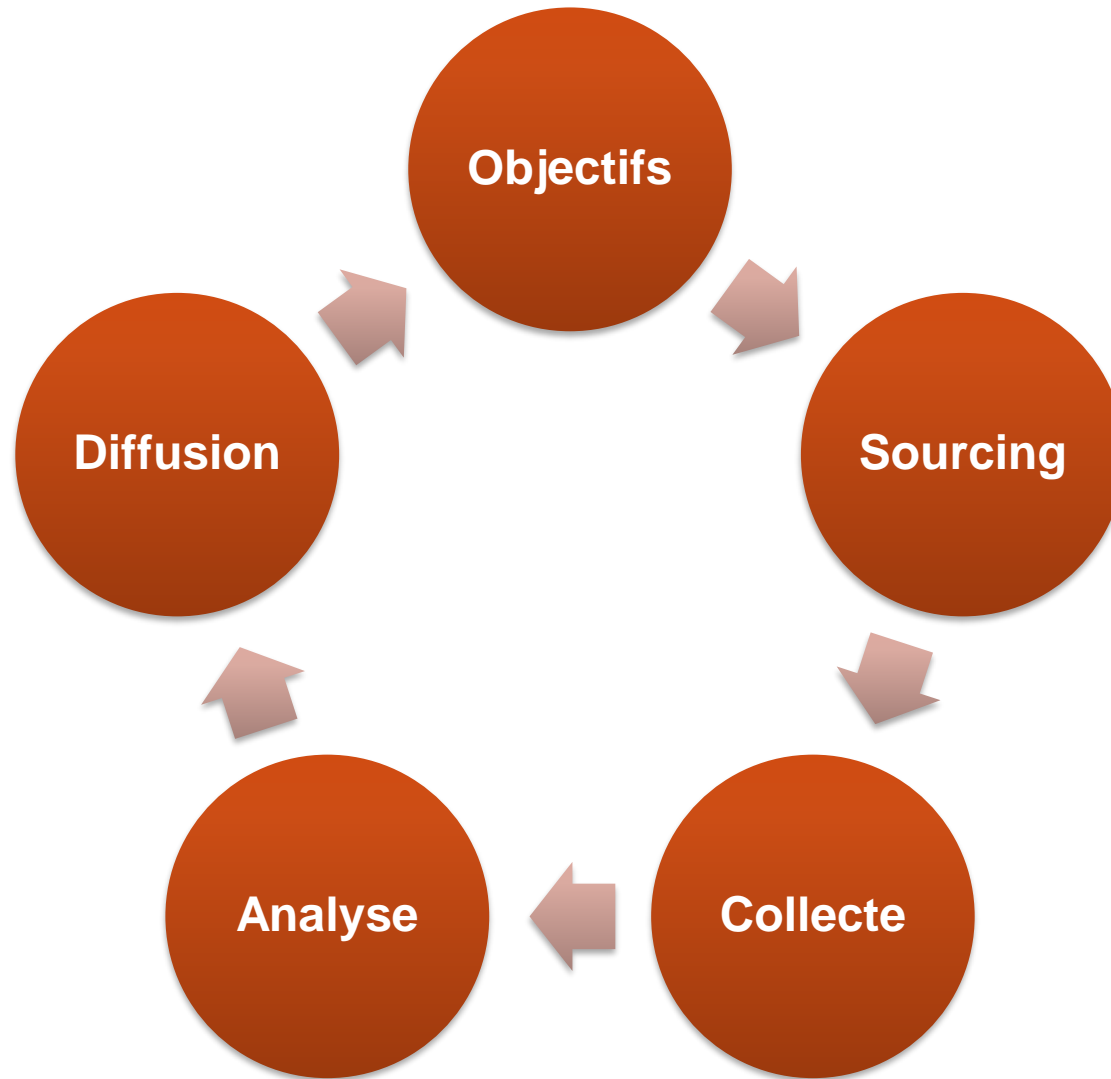
Source :  
OSINT? WTF??  
(OH SHINT!,  
2021)

**Vous faites de l'OSINT  
sans le savoir !**

# Le cercle ~~de la veille~~ du renseignement



# Le cercle de la veille



# Le Web : premier terrain d'investigation

# Recherche simple, recherche avancée, « *dorks* »

L'OSINT commence par la recherche

La question **sys-té-ma-ti-que** à se poser avant de saisir une requête dans un moteur de recherche :

*« Quels mots, expressions ou formulations ont toutes les chances de se trouver dans les pages qui répondent à mon besoin d'information »*

# Travailler les champs lexicaux

Découpez votre besoin en notions. Chaque notion se rapporte à un champ lexical. L'association des champs lexicaux vise à pouvoir extraire un maximum de documents répondant à votre besoin d'informations.

Notion pivot	Notion compl. 1	Notion compl. 2
RGPD	Sanction	Bonnes pratiques
"règlement général sur la protection des données"	sanctions	"bonne pratique"
RGPD	amende	"bonnes pratiques"
	amendes	"mise en conformité"
	pénalité	conforme
	pénalités	conformes
	punition	"aux normes"
	punitions	respect
	violation	"en adéquation"
	manquement	
	manquements	
	avertissement	
	avertissements	
	"à l'encontre"	
	accusation	
	accusations	

Aidez-vous... de votre bon sens, d'un corpus de documents, de Wikipédia, d'un dictionnaire de synonymes, etc.

# Les opérateurs booléens

**Des espaces** pour dire « et » (non... pas de « AND » 😊)

- ▶ "évident" vaccin rfid nanoparticules 5G  
(utiliser le lexique de la cible)

**Des « OR »** pour dire « ou »

- ▶ voiture OR automobile OR véhicule

**Des « - »** pour dire « sans »

- ▶ "nous refusons" dictature sanitaire -manifestants

# Opérateurs avancés : 5 astuces

**"..." (guillemets)** ▶ autour d'un mot, fixe sa graphie (accent/pas d'accent, féminin/masculin, singulier/pluriel)

▶ ["tél" OR "06" OR "07" "membres" association crépus](#)

**\* (troncature)** ▶ remplace une chaîne de caractères

▶ [site:data.\\*.\\* OR site:opendata.\\*.\\* lyon](#)

**before: after:** ▶ avant/après une date

▶ after:2010

▶ after:2010-08

▶ after:2010-08-25

**inurl: intitle:** ▶ dans l'URL, dans le titre

▶ [survivalistes france inurl:liens OR intitle:liens](#)

**"0.. {mot}"** ▶ Mot précédé d'un nombre

▶ [saisie "0.. kg de cocaïne"](#)

# filetype: dans Google Images ?

## organigramme ARS auvergne filetype:pdf (dans Google Images)

The image shows a Google search interface with the query "organigramme ars auvergne filetype:pdf". The search results include various images and documents. A red box highlights a specific search result, which is a PDF document titled "2018-018r\_tome\_II\_.pdf". The document is a detailed organizational chart for ARS Auvergne-Rhône-Alpes, dated 31st November 2018. The chart shows the hierarchy from the Director General down to various departments and their respective staff. The document is displayed in a preview window, showing the title, contact information, and the organizational structure.

Google  
organigramme ars auvergne filetype:pdf

Tous Actualités Images Maps Shopping Plus Outils Collections SafeSearch

cpias assurance maladie haute loire pep agence régionale itep ditep prévention clermont ferrand

2018-018r\_tome\_II\_.pdf 16 / 168 150%

Organisation générale de IARS  
Auvergne-Rhône-Alpes (au 31 novembre 2018)  
04 72 34 74 00  
Adresse du siège  
21 rue Garibaldi  
37 000  
38000 Lyon Cedex 03

Le pilotage de la transformation de l'offre de ...  
igas.gov.fr

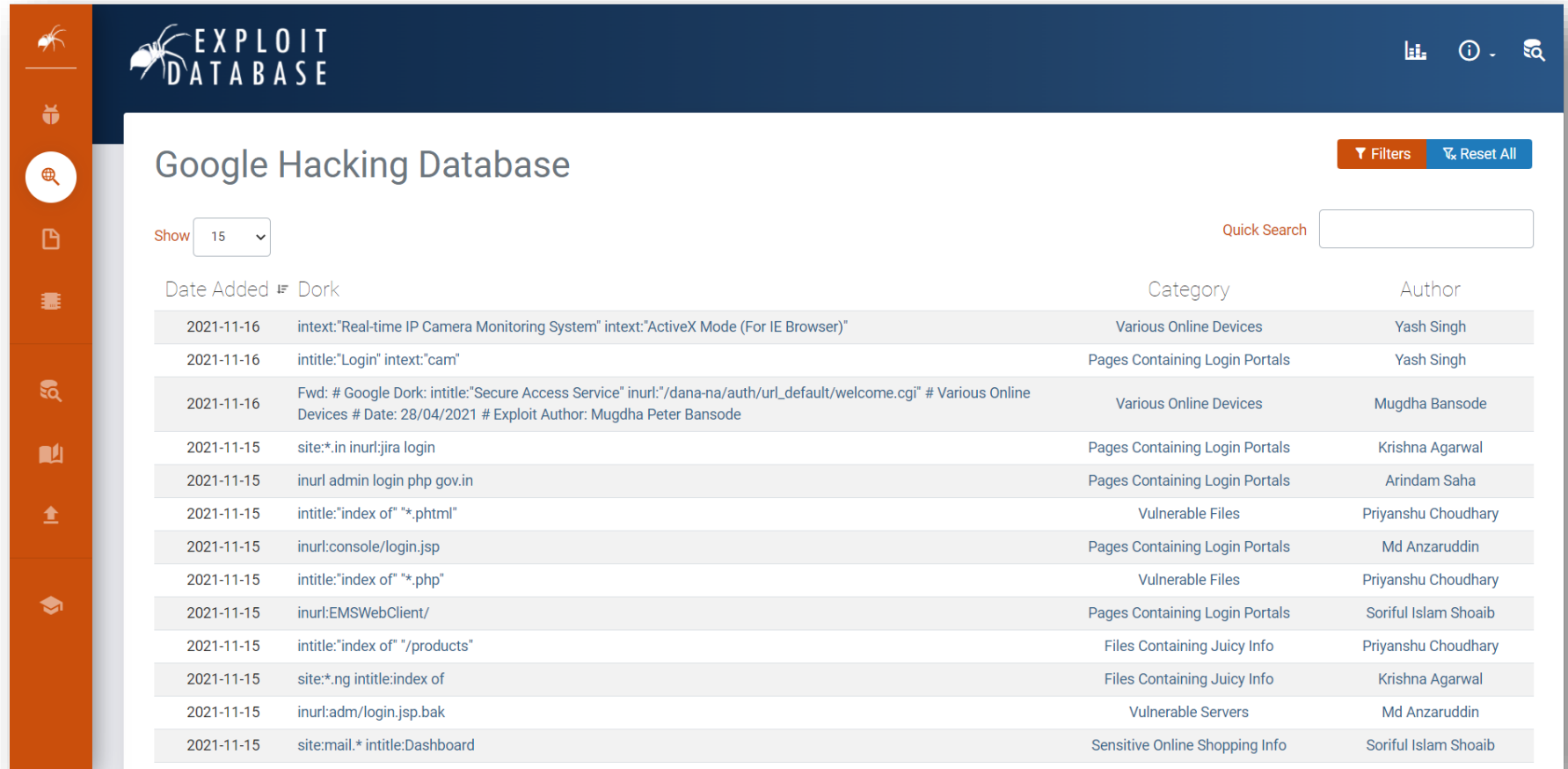
Guide d'aide à la préparation et à la ge...  
solidarites-sante.gov.fr

Dossier de pres...  
expertise.unionsp...



# Google Dorks

## Google Hacking Database



The screenshot displays the Exploit Database website interface. At the top, there is a navigation bar with the 'EXPLOIT DATABASE' logo and several utility icons. Below the navigation bar, the main content area features the title 'Google Hacking Database' and a search bar. A 'Show 15' dropdown menu is visible, along with 'Filters' and 'Reset All' buttons. The main content is a table listing various Google Dorks, their categories, and authors.

Date Added	Dork	Category	Author
2021-11-16	intext:"Real-time IP Camera Monitoring System" intext:"ActiveX Mode (For IE Browser)"	Various Online Devices	Yash Singh
2021-11-16	intitle:"Login" intext:"cam"	Pages Containing Login Portals	Yash Singh
2021-11-16	Fwd: # Google Dork: intitle:"Secure Access Service" inurl:"/dana-na/auth/url_default/welcome.cgi" # Various Online Devices # Date: 28/04/2021 # Exploit Author: Mugdha Peter Bansode	Various Online Devices	Mugdha Bansode
2021-11-15	site:*.in inurl:jira login	Pages Containing Login Portals	Krishna Agarwal
2021-11-15	inurl admin login php gov.in	Pages Containing Login Portals	Arindam Saha
2021-11-15	intitle:"index of" "*.phtml"	Vulnerable Files	Priyanshu Choudhary
2021-11-15	inurl:console/login.jsp	Pages Containing Login Portals	Md Anzaruddin
2021-11-15	intitle:"index of" "*.php"	Vulnerable Files	Priyanshu Choudhary
2021-11-15	inurl:EMSWebClient/	Pages Containing Login Portals	Soriful Islam Shoaib
2021-11-15	intitle:"index of" "/products"	Files Containing Juicy Info	Priyanshu Choudhary
2021-11-15	site:*.ng intitle:index of	Files Containing Juicy Info	Krishna Agarwal
2021-11-15	inurl:adm/login.jsp.bak	Vulnerable Servers	Md Anzaruddin
2021-11-15	site:mail.* intitle:Dashboard	Sensitive Online Shopping Info	Soriful Islam Shoaib

# Accumuler les sources (utiles)

...pour les mobiliser rapidement !

# Exemples de bases de données utiles lors d'investigations visuelles

## Plaques minéralogiques

- ▶ [Licence plates of the World](#)

## Armes et matériel militaire

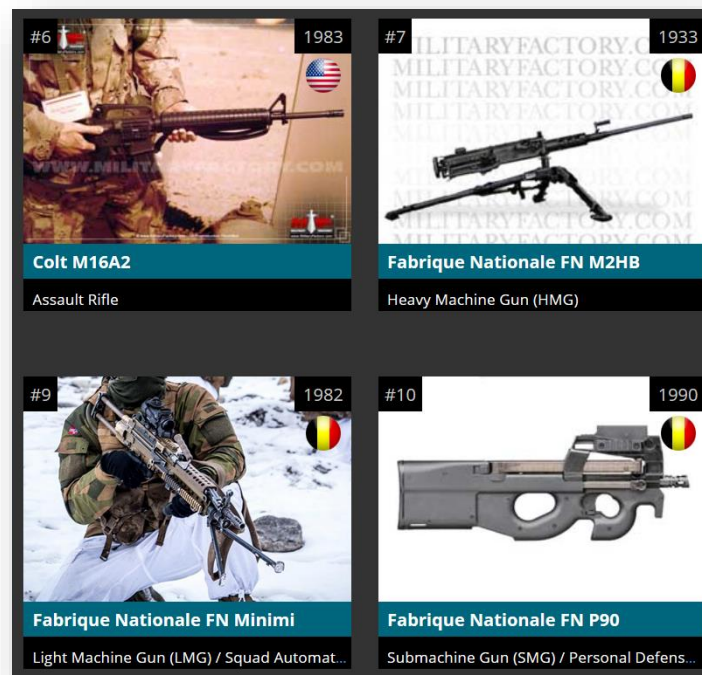
- ▶ [Camopedia](#) (camouflage)
- ▶ [Military Factory](#)
- ▶ [Weapons ID Database](#)
- ▶ [Référentiel général des armes \(RGA\)](#)

## Voitures

- ▶ [Oscaro](#) (identifier le modèle d'une voiture à partir de son immatriculation)

## Avions

- ▶ [Aircraft registration](#) (voir External Links)



# Gérer ses favoris

## Navigateur (rapide, confidentiel, lourd si les favoris sont nombreux)

- OSINT SC
  - IMINT/GEOINT/GEOLOC
  - SOCMINT
  - PERSONNE
  - WEBINT/CYBINT/RECON
  - DARKINT
  - SECURITY/PRIVACY
  - FACEBOOK
    - Epoch Converter - Unix Timestamp Converter
    - TweetBeaver - Home of Really Useful Twitter Tools
    - TweepDiff - Find Out Who You're Missing On Twitter

## Raindrop.io (en ligne, ubiquitaire, massif, non confidentiel)

Tous les favoris 31 k

- Non trié 8
- Corbeille 34
- Mes collections
- Bookmarks 31 k
- Tri rapide...
- Liens 27 k
- Articles 3,3 k
- Vidéos 270
- Images 38
- Documents 7
- Cassé liens 368
- Dupliques 221

Tous les favoris date | Liste

Yet Another Firefox Hardening Guide | Chris Xiao  
My guide to improving security and privacy in Firefox without sacrificing convenience.  
#OSINT #guide #2021 #browser\_hardening #browser #Firefox #OPSEC  
Bookmarks publics de Serge Courrier · chrisxxyz · Aujourd'hui, 08:37

## Shaarli (auto-hébergé, rapide, confidentiel... mais technique)

Shaarli Tag cloud Picture wall Daily

Search text Filter by tag

Filters Links per page 20 50 100 133

Interia - Polska i świat: informacje, sport, gwiazdy.  
Interia - czołowy polski portal internetowy. Najlepsze serwisy informacyjne i tematyczne (Wydarzenia, Sport, Motoryzacja, Biznes, GeekWeek, Gry, Kobieta). Bezpłatna poczta e-mail.  
17 novembre 2021 à 06:10:47 UTC \* · permalink · http://interia.pl

Onet - Jesteś na bieżąco  
Onet: codzienne źródło informacji milionów Polaków - wiadomości z kraju i ze świata 24/7, pogoda, sport, biznes, moto, rozrywka. Bądź na bieżąco z Onet!  
17 novembre 2021 à 06:10:46 UTC \* · permalink · http://onet.pl

Wirtualna Polska - Wszystko co ważne - www.wp.pl  
Nowoczesne medium, porządkuje świat i dostarcza angażujące informacje, rozrywkę i usługi w czasie rzeczywistym. Przewodnik Polaków w wirtualnym świecie.  
wp.pl · WP · Wirtualna-Polska · Pogoda · Wiadomości · Newsy · Informacje · Sport · Finanse · Rozrywka · Program · Telewizja · #dziejesiewpolsce  
17 novembre 2021 à 06:10:45 UTC \* · permalink · http://wp.pl

# Protéger ses investigations : OPSEC

(Operations Security)

# Protéger ses investigations : les questions à se poser

## Modèle de menace ?

- ▶ Pour chaque type d'investigation : définir son [modèle de menace](#) (*threat model*)
- ▶ Identifier et classer par ordre de priorités les menaces potentielles

## Cible ?

- ▶ Qui est ma cible ? Quel est son niveau d'expertise technique ?

## Qu'est-ce qui pourrait mal tourner ?

## Que dois-je protéger ?

- ▶ Mon identité ? (photo, nom, numéro de téléphone, mail, entité de rattachement)
- ▶ Ma localisation ?
- ▶ Mon adresse IP ?
- ▶ Autre ?

## De qui dois-je me protéger ?

- ▶ De ma cible seule ?
- ▶ De sa communauté ?
- ▶ D'acteurs tiers (moteurs de recherche, services en ligne...)

## Quelles informations risque-je de faire fuiter ? Est-ce grave ?

## Quels risques prends-je à être découvert ?

# OPSEC : le minimum

## Navigateur > Choix

- ▶ [Tor](#)
- ▶ [Firefox](#)
- ▶ Basé sur Chromium
  - [Ungoogled Chromium](#)
  - [Iridium](#)
  - [Brave](#)
  - [Chrome](#)

## Navigateur > Profiles

- ▶ [Firefox Profiles](#)

## Navigateur > Configuration

- ▶ [Hardening Firefox](#)

## Navigateur > Extensions

- ▶ Anti traceurs >
  - uBlock [[CHROME](#)] [[FIREFOX](#)]
  - [Decentraleyes](#) : [[CHROME](#)] [[FIREFOX](#)]
  - Chameleon [[FIREFOX](#)]
- ▶ HTTPS
  - [HTTPS Everywhere](#)
- ▶ Isoler les onglets dans des containers étanches
  - [[CHROME](#)] [Session Box](#)
  - [[FIREFOX](#)] [Firefox Multi-Account Containers](#)
- ▶ Pouvoir faire passer son navigateur pour un autre
  - User-Agent Switcher and Manager [[CHROME](#)] [[FIREFOX](#)]

## VPN (cacher son adresse IP)

- ▶ [ExpressVPN](#)
- ▶ [ProtonVPN](#) (gratuit),
- ▶ [Private Internet Access](#)
- ▶ [[comparatif](#)]

## Identités d'emprunt (*sock puppets*)

- ▶ Attention à ne pas trop les recycler

## Tester son empreinte

- ▶ [AmlUnique](#)

# OPSEC : monter en gamme

Téléphone d'occasion + carte SIM prépayée

Adresse mail jetable

Système d'exploitation > Choix

- ▶ [Tails](#)
- ▶ Distribution Linux spécialisée OSINT
  - [Kali Linux](#)
  - [Tsurugi](#)
- ▶ Distribution Linux généraliste
  - [Ubuntu](#)

Système d'exploitation > Installation

- ▶ Machine virtuelle ?
  - [VirtualBox](#)
- ▶ Clé USB ?

Investigations en mode non connecté  
(à quelque service que ce soit)





# Investiguer les images (IMINT/GEOINT/Analyse d'images)

**Qui ? Où ? Quel jour ?  
Quelle heure ?**

# Qui ? Où ? Quel jour ? A quelle heure ?

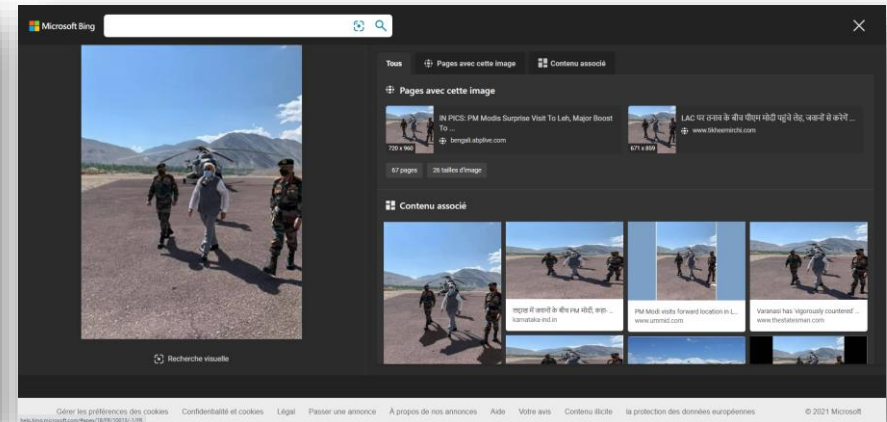
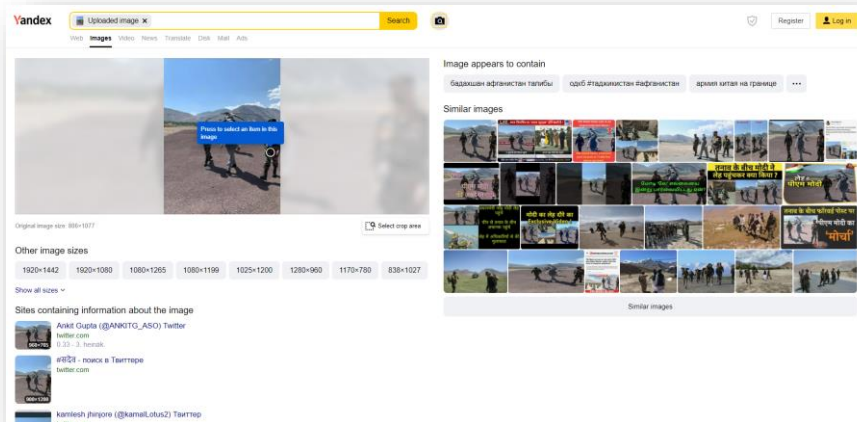
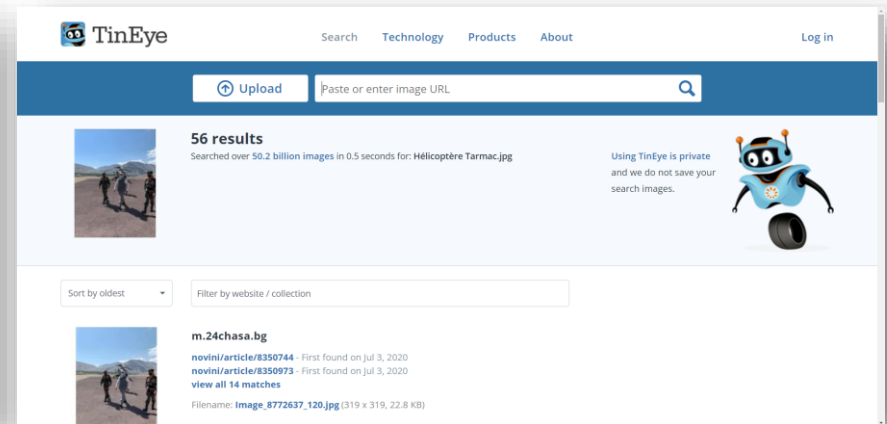
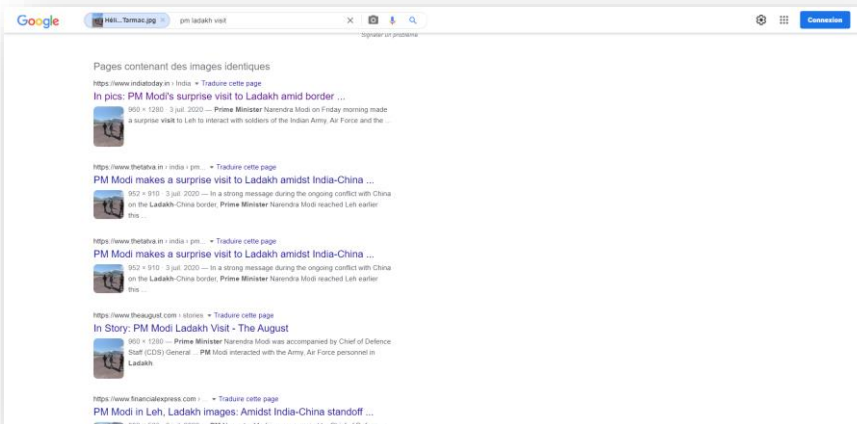


Source : [FINDING: MODI - Find where & when a photo was taken \(geolocation & chronolocation\)](#)  
(Bendobrown, 10/05/2021)

# Recherche inversée

## Extension Search By Image ([Firefox](#), [Chrome](#))

► Clic droit sur l'icône pour afficher les options



# Qui ? Quand ? Où ?

India Today | Malayalam | Business Today | DailyO | Aaj Tak | Lalantop | GNTTV | iChowk | Reader's Digest

NEWS • LIVE TV INDIA TODAY APP MAGAZINE

HOME MY FEED INDIA WORLD BUSINESS TECH MOVIES T20 WC SCIENCE HAPPINESS QUEST

T20 WORLD CUP 2021 ASSOCIATE SPONSOR KOHLER

News / India / In pics: PM Modi's surprise visit to Ladakh amid border tensions with China

## In pics: PM Modi's surprise visit to Ladakh amid border tensions with China

ADVERTISEMENT

India Today Web Desk  
New Delhi  
July 3, 2020 UPDATED: July 3, 2020 15:27 IST

As PM reached Nimoo, PM Modi was also briefed by senior Army officers. Located at 11,000 feet, Nimoo is among the toughest terrains, on the banks of river Indus and surrounded by the Zaskar range.

PM Modi landed in Leh early Friday morning.

PM Modi and Chief of Defence Staff Gen Bipin Rawat reached Leh around 9.30 am.

As PM reached Nimoo, PM Modi was also briefed by senior Army officers. Located at 11,000 feet, Nimoo is among the toughest terrains, on the banks of river Indus and surrounded by the Zaskar range.

CHECK THESE OUT

- Man opens bus window to click pic of lion. Scary...
- Territorial ambitions of China and...
- Jio network down: jio says glitches were reported...

READ THIS

- Meta is shutting down Facebook's face ID system, will delete billions of user photos from its database

TOP TAKES

- Kathmandu: Anupam Kher was amazed by this beggar who speaks fluent English

5G (Sky Blue, 6GB RAM... ₹ 16999 amazon.in

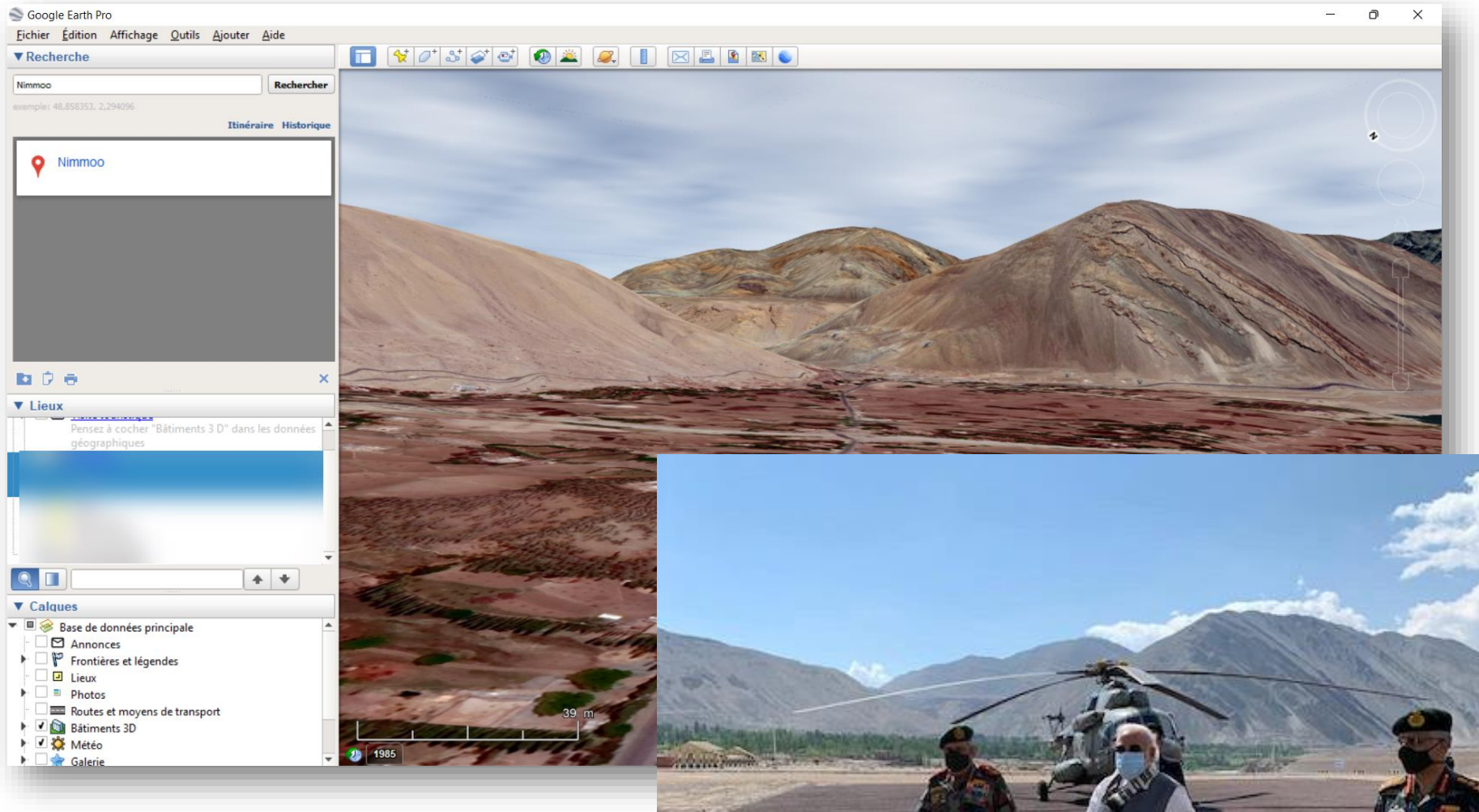
Redmi 9 Activ (Carbon Black, 6GB RAM, 128G... ₹ 10999 amazon.in

Redmi 9 (Sky Blue, 4GB RAM, 64GB Storage) |... ₹ 8499 amazon.in

Best Deals Today >

# Localiser

## Google Earth Pro, Google Maps



# Passer d'une cartographie à l'autre

The image shows a browser window displaying Google Maps. The main map area shows a satellite view of a coastal region in Tanzania, with labels for 'Msitu Kuu Forest', 'Ngezi Forest', 'Konde', 'Tumbe', 'Maziwa Ngombe', 'Gando', 'Junguni', 'Pemba Island', 'Wete', 'Adansoni Bay', and 'Kojana Island'. The left sidebar contains information about 'Msitu Kuu Forest' (Tanzanie, Réserve naturelle) and a 'Photos' section. The right sidebar is open to a 'Map Switcher' utility, showing a list of map providers under three categories: 'Main maps', 'Utilities', and 'Specials'. The 'Main maps' list includes Google Maps, OpenStreetMap, Mapillary, 地理院地図, OpenStreetCam, F4map, Yandex, and Qwant Maps. The 'Utilities' list includes Overpass-turbo, Osmose, KeepRight, OSM Inspector, Who did it?, Map compare, Multimapas, and BigMap 2. The 'Specials' list includes Ingress Intel map, Satellite Tracker 3D, earth, Windy.com, flightradar24, Traze, MarineTraffic, and EO Browser. A red text box is overlaid on the right side of the map, containing the text: 'OpenSwitchMaps (extension Chrome et Firefox) permet de basculer d'une cartographie à l'autre' and 'Map Switcher (extension Chrome)'. The bottom of the browser window shows copyright information: 'Images ©2020 TerraMetrics, Données cartographiques ©2020 France Conditions Envoyer des commentaires 2 km'.

# Horodater en étudiant les ombres





# Horodater en étudiant les ombres

## Position de Narendra Modi le 3 juillet 2020

00:00 | 01:00 | 02:00 | 03:00 | 04:00 | 05:00 | 06:00 | 07:00 | 08:00 | 09:00 | 10:00 | 11:00 | 12:00 | 13:00 | 14:00 | 15:00 | 16:00 | 17:00 | 18:00 | 19:00 | 20:00 | 21:00 | 22:00 | 23:00

Computation path of the sun for:  
194101  
03 Jul 2020 18:57 UTC+5.5 >|<

Solar data for the selected location  
Dawn: 04:44:24  
Sunrise: 05:13:12  
Culmination: 12:25:02  
Sunset: 19:36:41  
Dusk: 20:05:27  
Daylight duration: 14h23m29s  
Distance [km]: 152.095.736  
Altitude: 6.61°  
Azimuth: 293.33°  
Shadow length [m]: 8.63  
at an object level [m]: 1

Geodata for the selected location  
Height: 3120m [Set Lat/Lon]  
Lat: N 34°11'59.28" 34.19980°  
Lng: E 77°19'9.83" 77.31940°  
UTM: 43S 713710 3786742  
TZ: Asia/Kolkata IST

More solar data  
Print  
Contact  
Help & API  
More for Moon|Planets|Satellites  
Donate  
Legal Disclosure|Privacy Policy|Cookies

here Partial solar eclipse: 21.06.2020 | 83.6% more

PLUS DE 600 CHARS. LESQUELS MAÎTRISEREZ-VOUS ?  
WORLD OF TANKS  
JOUEZ SUR PC  
SunCalc.org  
SunCalc.org ©Torsten Hoffmann 2015-2021

# Enquêtes satellitaires

[Ocelli Project](#) (base de données sur la destruction de maisons Rohingya en Birmanie, mené notamment par Benjamin Strick).

Voir aussi par exemple les enquêtes géographiques de [Forensic Architecture](#).



# Zoom sur l'OCR

(reconnaissance optique de caractères)

# Google Images : chercher un texte pour trouver une photo (grâce à la fonction d'OCR intégrée)

The image shows two screenshots of Google Images search results. The top screenshot shows a search for 'G-NRFK', displaying four images of a white and red biplane with the registration 'G-NRFK' and a red cross on the tail. The bottom screenshot shows a search for '503-JF-01', displaying four images of a red BMW E46 sedan with the license plate '503 JF 01'. The search interface includes the Google logo, search bar, navigation tabs (Tous, Maps, Shopping, Images, Vidéos, Plus), and utility links (Outils, Collections, SafeSearch).

**Search 1: G-NRFK**

- Aviation photographs of Regi: abpic.co.uk

**Search 2: 503-JF-01**

- La vente diversifiée par Ds - Home | ... facebook.com
- BMW E46 - Okoin okoin.ci
- Voitures BMW E46 2000 neufs et o... ci.coinafrique.com
- BMW E46 | Riviera | Jumia Deals deals.jumia.ci

# Facebook : chercher un texte pour trouver une photo (grâce à la fonction d'OCR intégrée)

**Résultats de la recherche**

Filtres

- Tous
- Publications
- Personnes
- Photos**
- Publié par
- Type de photo
- Lieu identifié
- Vidéos
- Marketplace

**Exemple : EA-356132**

Facebook dispose de fonctions de reconnaissance optique de caractères qui permet par exemple de trouver la photo d'une voiture depuis sa plaque minéralogique.

Source : [Google And Facebook Are Reading Your License Plates](#) (Jalopnik, 2019)

# Zoom sur la reconnaissance faciale

# Recherche inversée avec reconnaissance faciale

## [+++] [PimEyes](#)

- ▶ Excellente reconnaissance faciale
- ▶ Réservé aux abonnés payants depuis octobre 2021

[...]

Pour VKontakte (VK, russe)

- ▶ [Search4Faces](#) (recherche aussi sur Odnoklassniki [copains de classe]).
- ▶ [...]

Pimeyes



# Similarité faciale (Microsoft)

Détection de visages

Vérification des visages

Reconnaissance des émotions

## Vérification des visages

Vérifiez la probabilité pour que deux visages appartiennent à la même personne et recevez



URL de l'image

Envoyer

Parcourir

URL de l'image

Envoyer

Parcourir

Résultat de la vérification : les deux visages appartiennent à la même personne. **Le degré de fiabilité est le suivant : 0.93468.**

Permet d'évaluer le niveau de similarité entre deux visages

[Démonstration](#) du service de vérification des visages (cliquer sur l'onglet "Vérification des visages")  
**Pas plus de 4Mo par image !**

[Logic Apps: Face Verification Using Microsoft Cognitive Services Face Api and Logic Apps](#)

[Documentation](#)



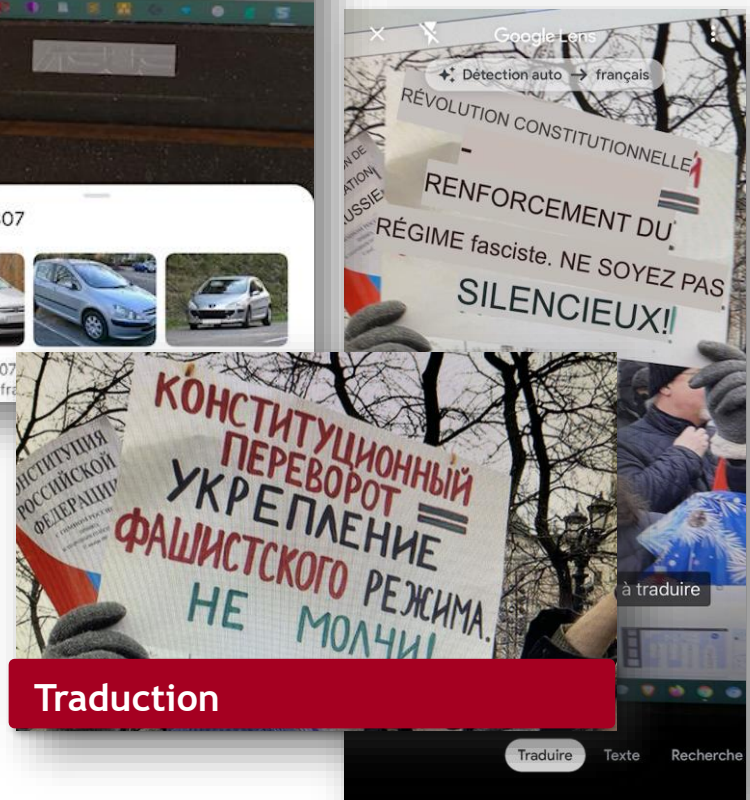
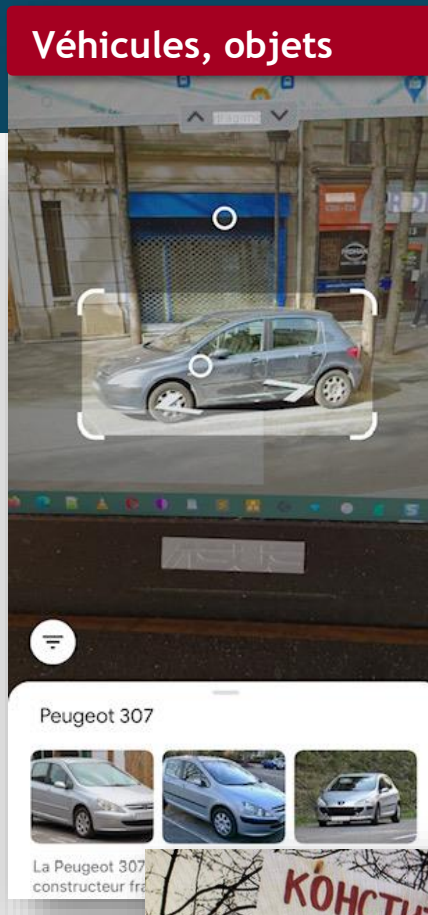
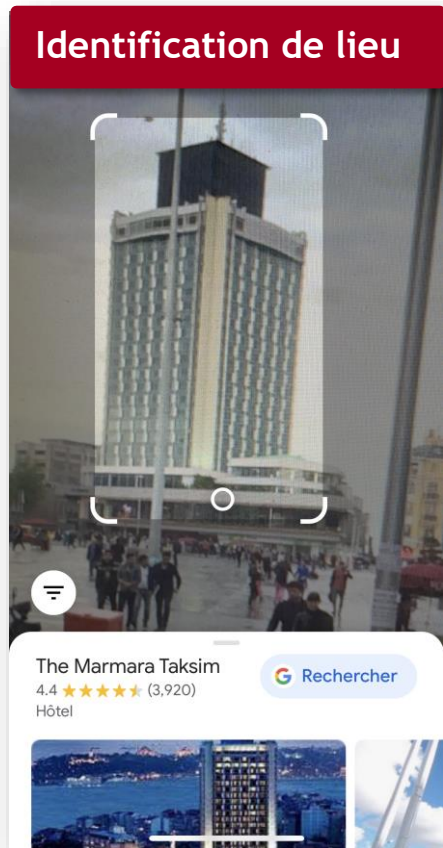
# Zoom sur Google Lens

# Google Lens

## Google Lens

(sur smartphone, mais aussi en ligne)

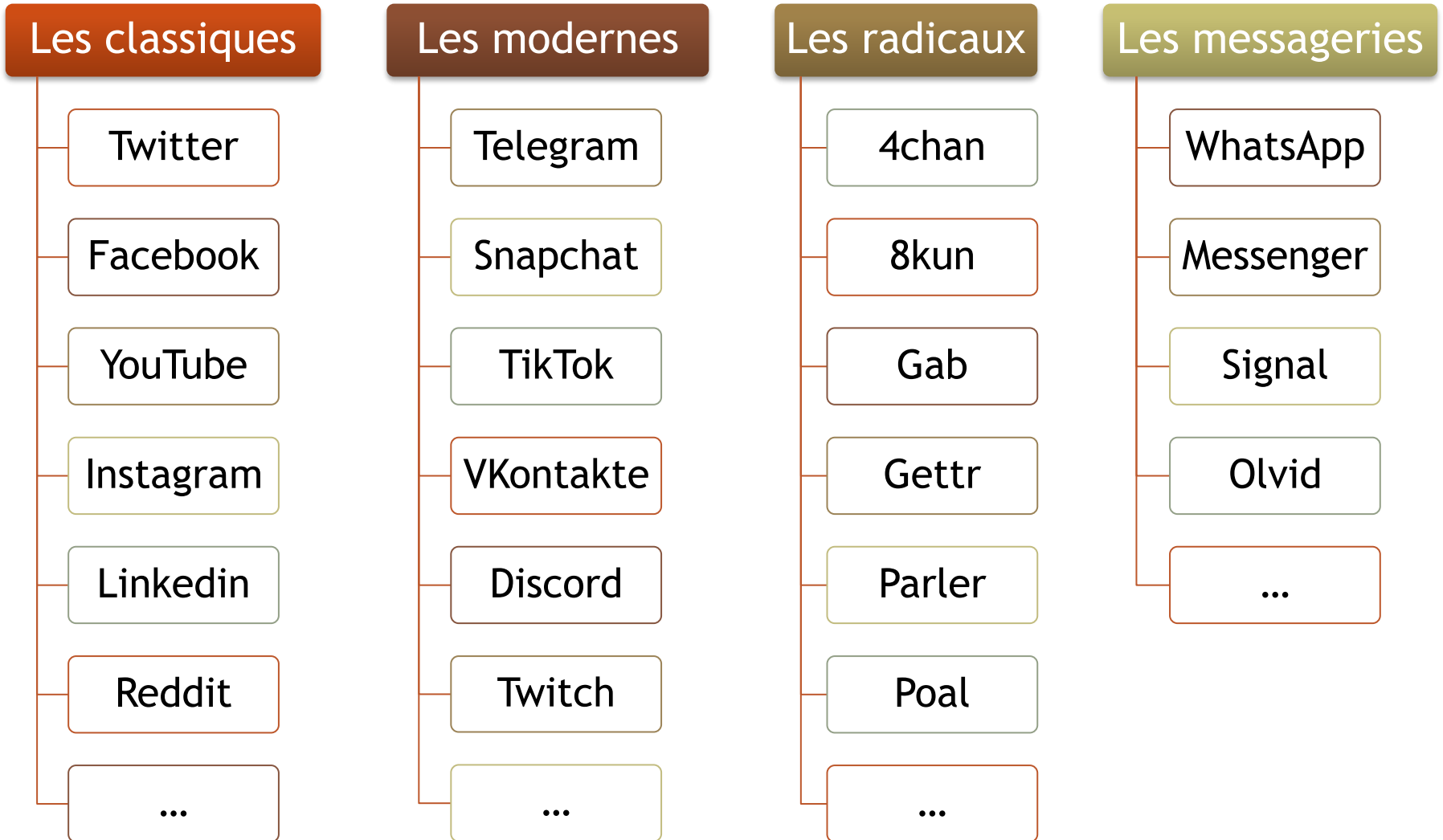
- ▶ Identification d'objets, véhicules, lieux, etc.
- ▶ Traduction
- ▶ OCR



# Investiguer les médias sociaux (SOCMINT/RRS)

# OSINT ? Une nécessaire stratégie du petit pas !

# Médias sociaux : les grandes familles



# Twitter

# **gilets jaunes à Toulouse**

**Le questionnement est simple ?  
Et pourtant...**

# Champs lexicaux dans Twitter

Notion 1 : gilets jaunes	Notion 2 : Toulouse
"gilet jaune"	Toulouse
"gilets jaunes"	Toulousain
#giletjaune	Toulousains
#giletsjaunes	Toulousaine
#gj	Toulousaines
	"ville rose"



"gilet jaune OR "gilets jaunes" OR #giletjaune OR  
#giletsjaunes OR #gj toulouse OR toulousain OR  
toulousains OR toulousaine OR toulousaines OR "ville  
rose" -weed -cocaine -cannabis



# Rechercher un tweet à un jour ou à la seconde près

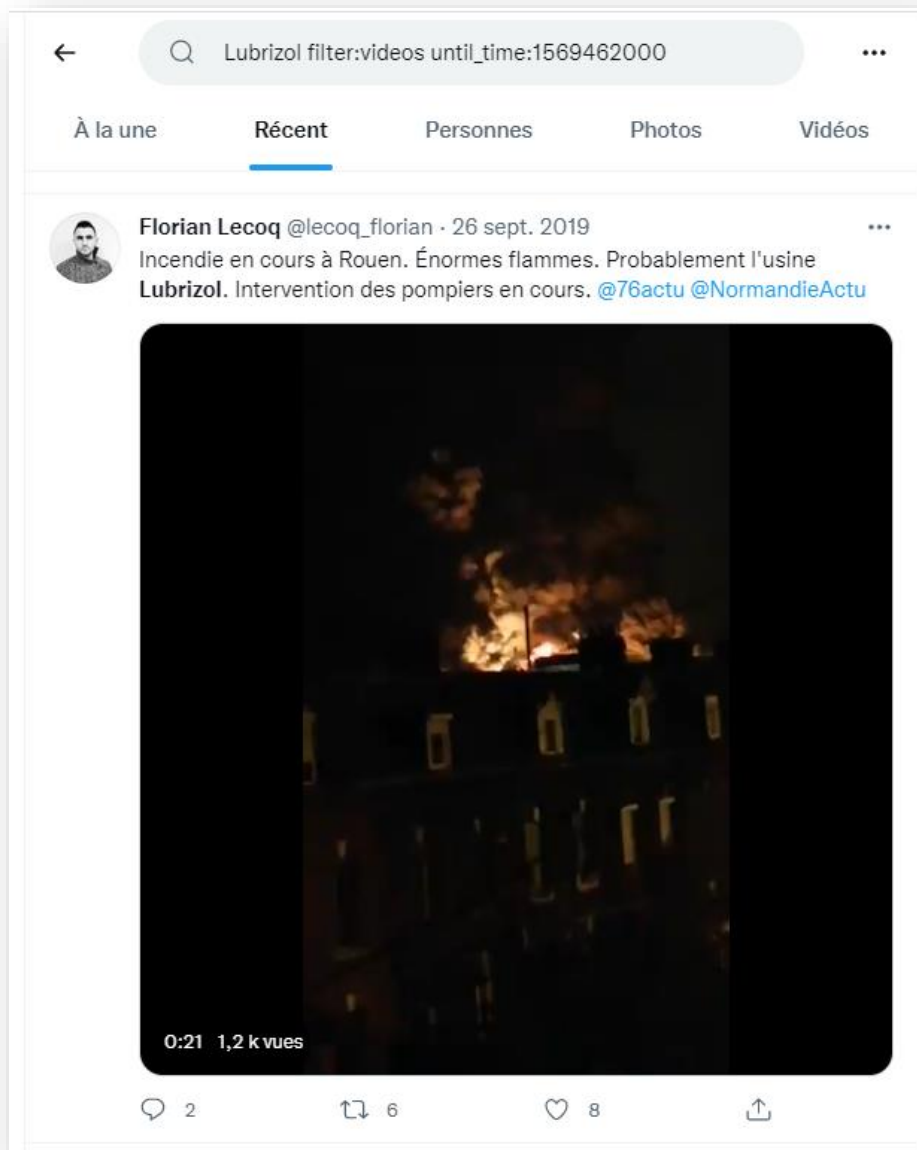
## Première vidéo de l'incendie de Lubrizol (26 septembre 2019)

- ▶ 1<sup>ère</sup> requête envisageable, liée au jour

[Lubrizol filter:videos until:2019-09-27](#)

- ▶ 2<sup>e</sup> requête envisageable, liée à l'heure (déterminée par [epochconverter.com](#))

[Lubrizol filter:videos until\\_time:1569462000](#)



# L'extension utile

[Instant Data Scraper](#) [CHROMIUM] :  
par exemple, récupérer [les abonnés de Wisti-ti](#)

The screenshot shows a Twitter profile page for Wisti-ti (@Wistiti84470505) with the 'Abonnés' (Followers) tab selected. The Instant Data Scraper extension is overlaid on the page, displaying the following information:

- Buttons: Try another table, Start crawling, CSV, XLSX, COPY ALL, Help/Feedback
- Settings: Infinite scroll (checked), Min delay: 1 sec, Max delay: 20 sec
- Status: Pages scraped: 1, Rows collected: 20, Rows from last page: 20, Working time: 0s
- Rating prompt: If you like this extension, please rate it in chrome store: Rate, Later
- Download data or locate "Next" to crawl multiple pages
- Table of scraped data:

css-4rbku5 href	css-9pa8cd src	css-90
https://twitter.com/realmarcel1	https://pbs.twimg.com/profile_images/13479290	Marcel
https://twitter.com/LorentzMathias	https://pbs.twimg.com/profile_images/10953206	Lorentz mathias
https://twitter.com/Babar_Le_Rhino	https://pbs.twimg.com/profile_images/13497405	Babar le Rhinocér
https://twitter.com/CharliB97783485	https://pbs.twimg.com/profile_images/13378367	Charli
https://twitter.com/patnice63	https://pbs.twimg.com/profile_images/13366168	No pasarán!!! (cop
https://twitter.com/LalobaRose	https://pbs.twimg.com/profile_images/79463310	RositaBanana
https://twitter.com/Deeplooo	https://pbs.twimg.com/profile_images/10031789	Deeplo, φ
https://twitter.com/Callystor	https://pbs.twimg.com/profile_images/13381541	Реми φ
https://twitter.com/lapin47	https://pbs.twimg.com/profile_images/51443392	Angry_Bisounours
https://twitter.com/LcrStefany	https://pbs.twimg.com/profile_images/14335002	Stefany

# Spoonbill : changements dans les bios

**Spoonbill** : suivre l'évolution de la bio des comptes que l'on suit et consulter l'historique de modification de la bio de n'importe quel compte.

**En ligne : l'historique des changements de bio de n'importe quel compte**

**SPoonBILL**

**@OSINTtechniques**

Resources for Open Source Intelligence Investigations. Follow the Digital Bread Crumbs. #OSINT @OsintCurious Advisory Board osint.techniques@protonmail.com

<http://www.osinttechniques.com>

Canada

OSINT Techniques

May 19, 2016, 5:57 a.m.

Nov. 5, 2020, 1:46 a.m.

**OSINTtechniques** changed their bio to:

Resources for Open Source Intelligence and Social Media Investigations. Follow the Digital Bread Crumbs. #OSINT #SOCMINT-@OsintCurious Advisory Board osint.techniques@protonmail.com

April 3, 2020, 3:33 a.m.

**OSINTtechniques** changed their profile picture to:

Check out the ten minute tip video I made for #tips when using Google Maps for your #OSINT investigations: <https://t.co/r0z21t0cqv> I made a ten minute tip video for @OsintCurious on Facebook searching tips. Facebook data sometimes isn't hidden... but you need to know where to look. <https://t.co/dR6PY4ZAGN> <https://t.co/PPHjCl8uPL> #osint #socmint

<https://spoonbill.io/twitter/data/OSINTtechniques/>

**Par mail quotidien : tous les changements dans les bios des personnes que vous suivez**

Updates from Spoonbill

En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur web.

**TWITTER**

**OSINTTechniques** changed their bio →

Resources for Open Source Intelligence and Social Media Investigations. Follow the Digital Bread Crumbs. #OSINT #SOCMINT-@OsintCurious Advisory Board osint.techniques@protonmail.com

**UnderTheBreach** changed their bio →

Co-Founder & CTO & Hudson Rock @hrock  
Always behind 7 proxies  
ישראל ו underthebreach.com  
Cyber Cyber Cyber

#Bitcoin #Ethereum

# Abonnés ou abonnements communs ?

[TweepDiff](#) : par exemple pour comparer les abonnements communs à...

- ▶ [@ana\\_anamddk](#)
- ▶ [@thalassa2008](#)

The screenshot shows the TweepDiff interface. At the top, it says 'TweepDiff' and 'Compare Twitter friends and followers'. There are links for 'About', 'Signals Ready', and '@bdeter'. Below this is a section 'Do Another Comparison' with a search bar containing '@ana\_anamddk' and '@thalassa2008'. The results show 'Common (473)' and 'thalassa2008 following (7005) | ana\_anamddk following (1772)'. A list of common followers follows, including: BEZOMBES Jean-Michel (bezombes\_jm), lynns (lynns68gwada971), Papanours (papanours60), alain brugerie (brugerie), \* This Is Sparta \* (\_ThisIsSparta\_), RoOsTer (RoosterV4), Pinsolle Typhaine (PinsolleT), LE GÉNÉRAL Officiel (LE\_GENERAL\_OFFL), Maurice BÉTRA (BetraMaurice), Antoine Gavory (Antoine\_Gavory), MAMMIE Bocock (Medic4allHuman), VERITY France (verity\_france), -Gino\_2019\_nCoV-IT (GiNo\_2019\_nCoV), Docteur P.E.B (DocteurPEB1), Francois-Xavier (F\_Xavier\_dA), @ElDictaTorOfficiel (El\_Dic\_TatoR), Kler Éclaire (Kler\_Eclaire), Christophe DEBIEN (ChrisDebien), Uriel (777appocalypse), Eliza Channele (ChanelleEliza), Perlé Caroline (perle\_caroline), Post Scriptum (Quotes\_PS), Cohérence (coherence\_e), Jirokana (Jirokkana), Claire Brunel Di Vizio (DiBrunel), La minute libre (MinuteLibre), JuanHERNANDEZ (Pajuanico), David La Haye (DavidLaHaye), and Festé (Steco94).

# Analyse de graphe

(analyser les relations entre des acteurs)

# NodeXL

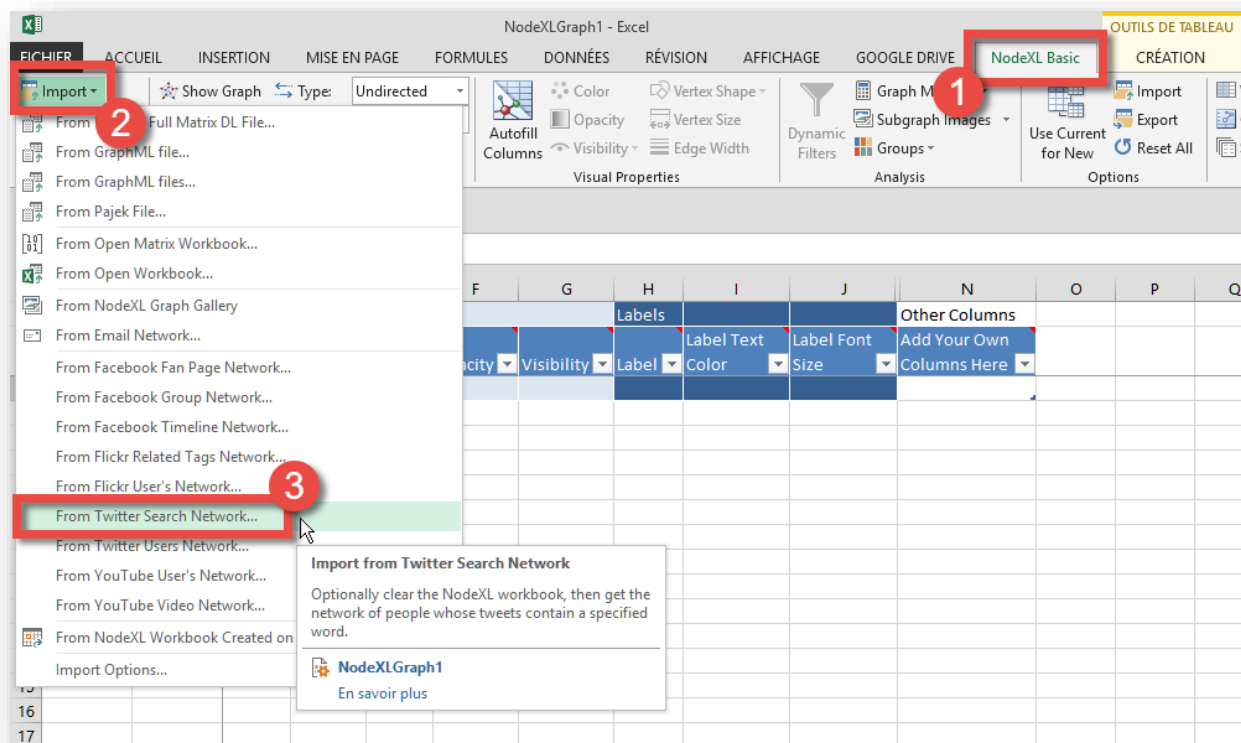
NodeXL est un modèle Excel (compatible Windows à partir d'Excel 2010).

Il ajoute un onglet à Excel.

Il est capable d'interroger le moteur de recherche de Twitter ou le réseau d'utilisateurs.

**Vous devrez connecter votre compte Twitter à NodeXL pour qu'il puisse interroger Twitter.**

**La version Basic est limitée au niveau du nombre maximal de tweets récupérés : 3200.**



Ici, analyse de #holdup lang:fr



NodeXLGraph1 - Excel

Fichier Accueil Insertion Mise en page Formules Données Révision Affichage Aide Power Pivot NodeXL Basic Création Rechercher des outils adaptés

Graph Metrics

Metric to calculate and insert into the workbook:

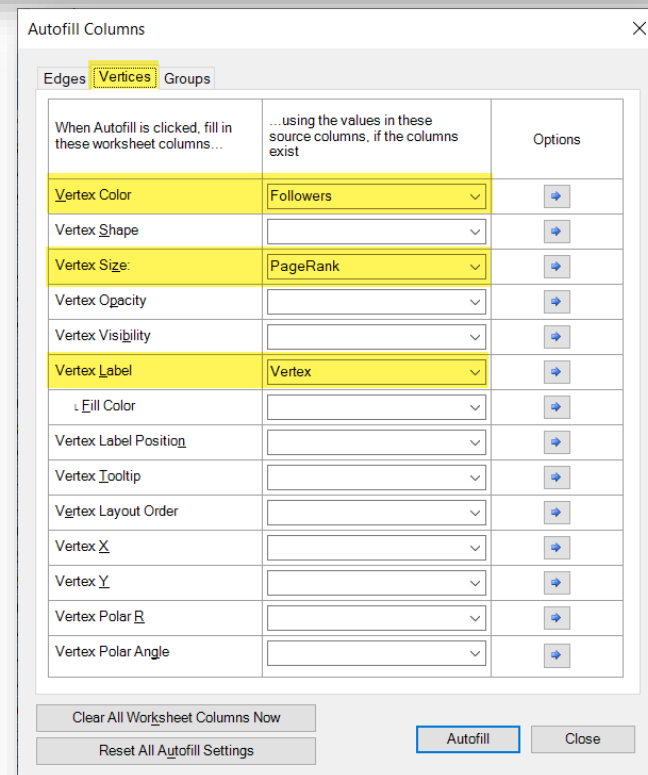
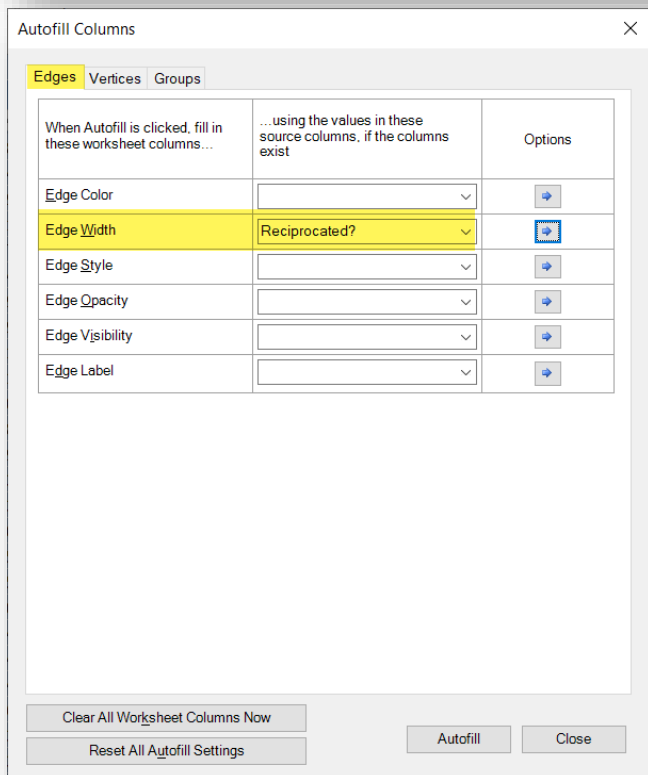
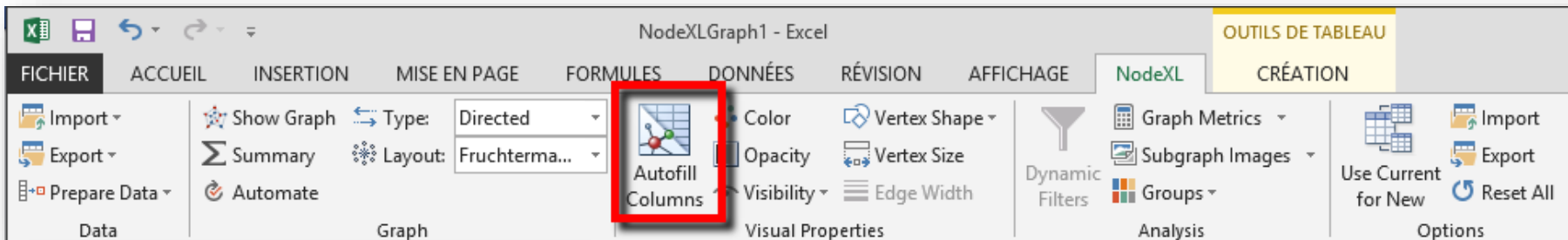
- Overall graph metrics
- Vertex degree (undirected graphs only)
- Vertex in-degree (directed graphs only)
- Vertex out-degree (directed graphs only)
- Vertex betweenness and closeness centralities\*
- Vertex eigenvector centrality\*
- Vertex PageRank\*
- Vertex clustering coefficient\*
- Vertex reciprocated vertex pair ratio (directed graphs only)\*
- Edge reciprocation (directed graphs only)\*
- Group metrics\*
- Time Series\*
- Words and word pairs
- Edge creation by shared content similarity
- Top items\*

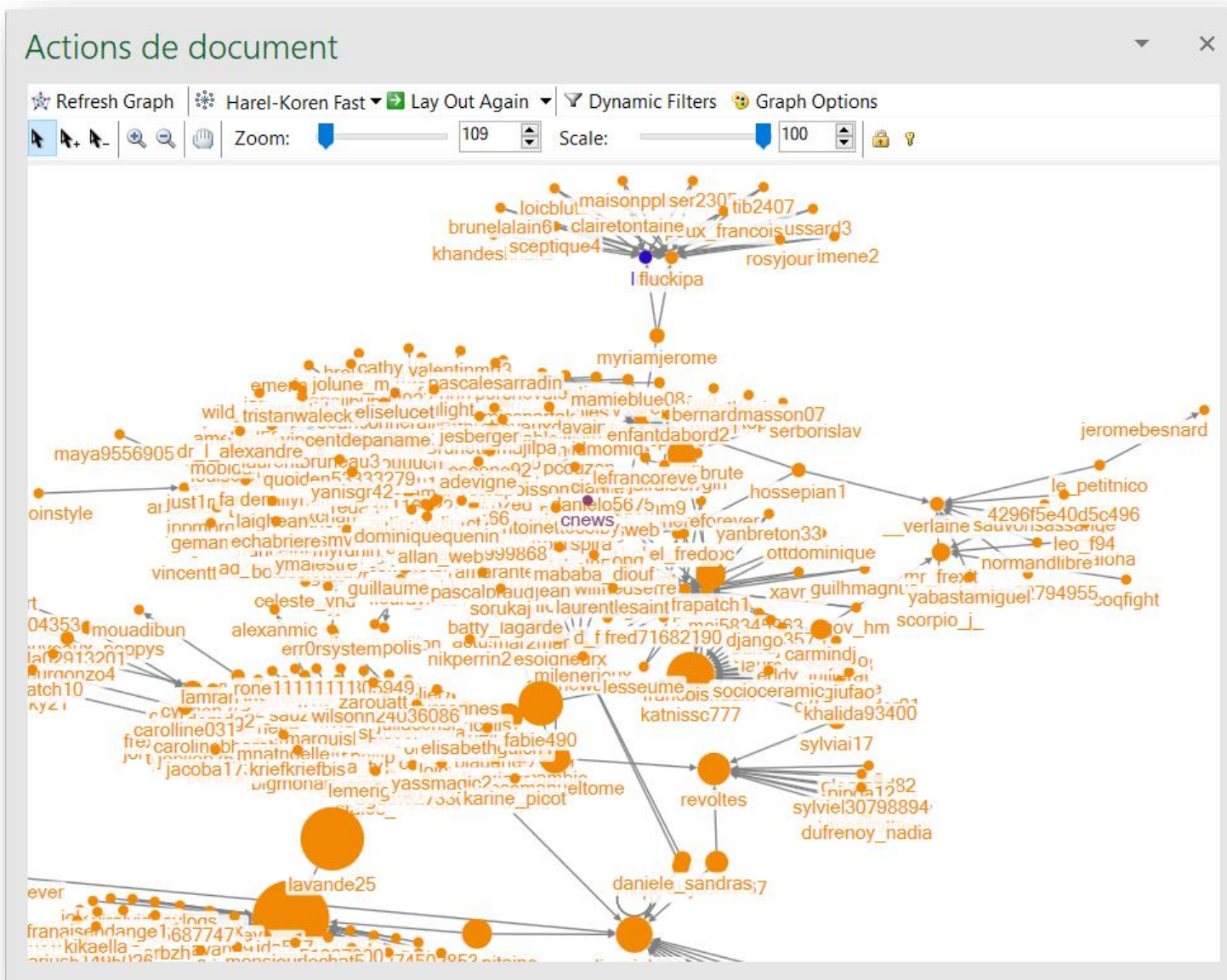
The following overall metrics get inserted into the Overall Metrics worksheet:

Graph Type	Directed or undirected.
Vertices	The number of vertices in the graph.
Unique Edges	The number of edges that do not have duplicates.
Edges With Duplicates	The number of edges that have duplicates.

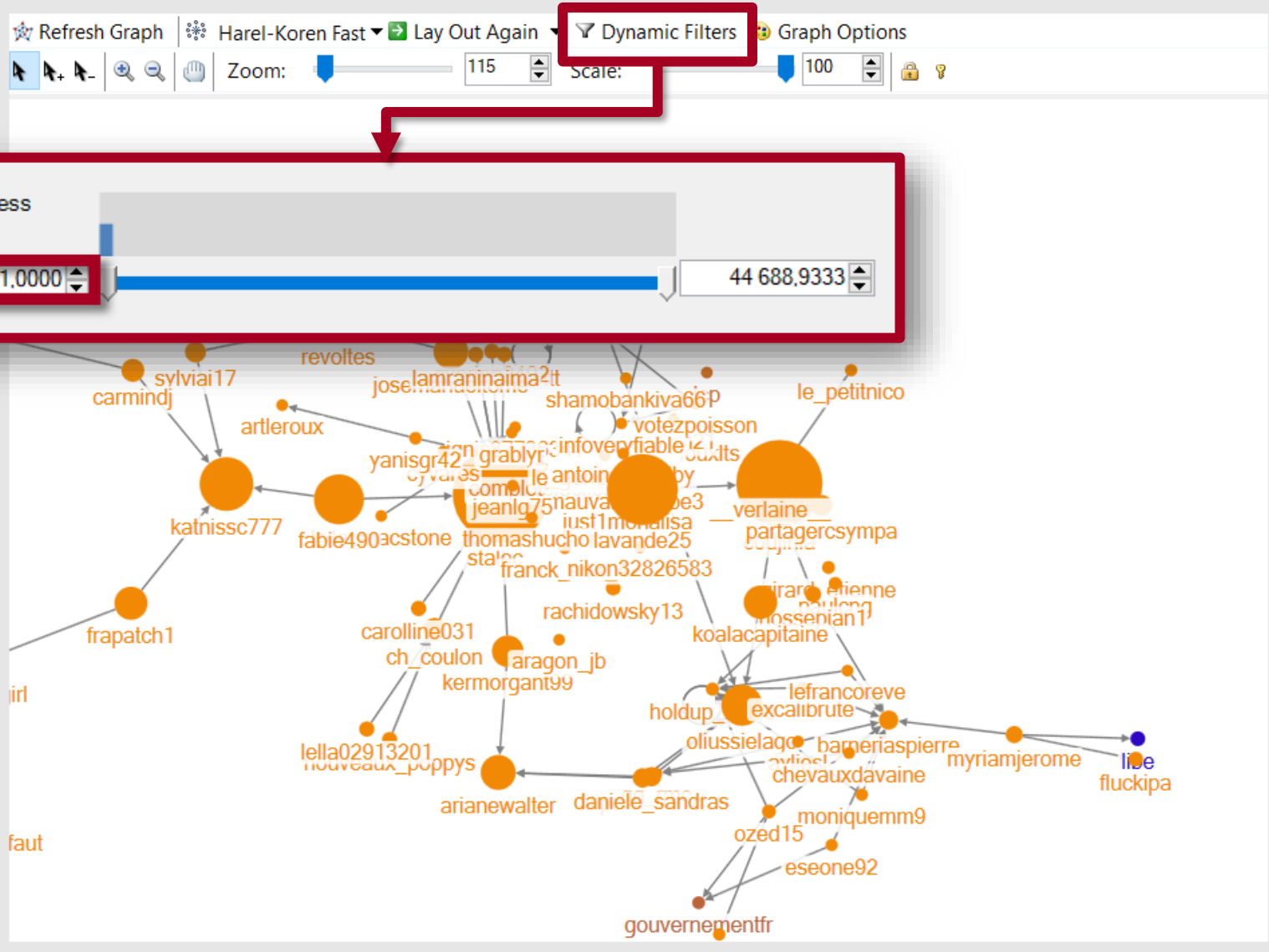
[About duplicate edges](#)

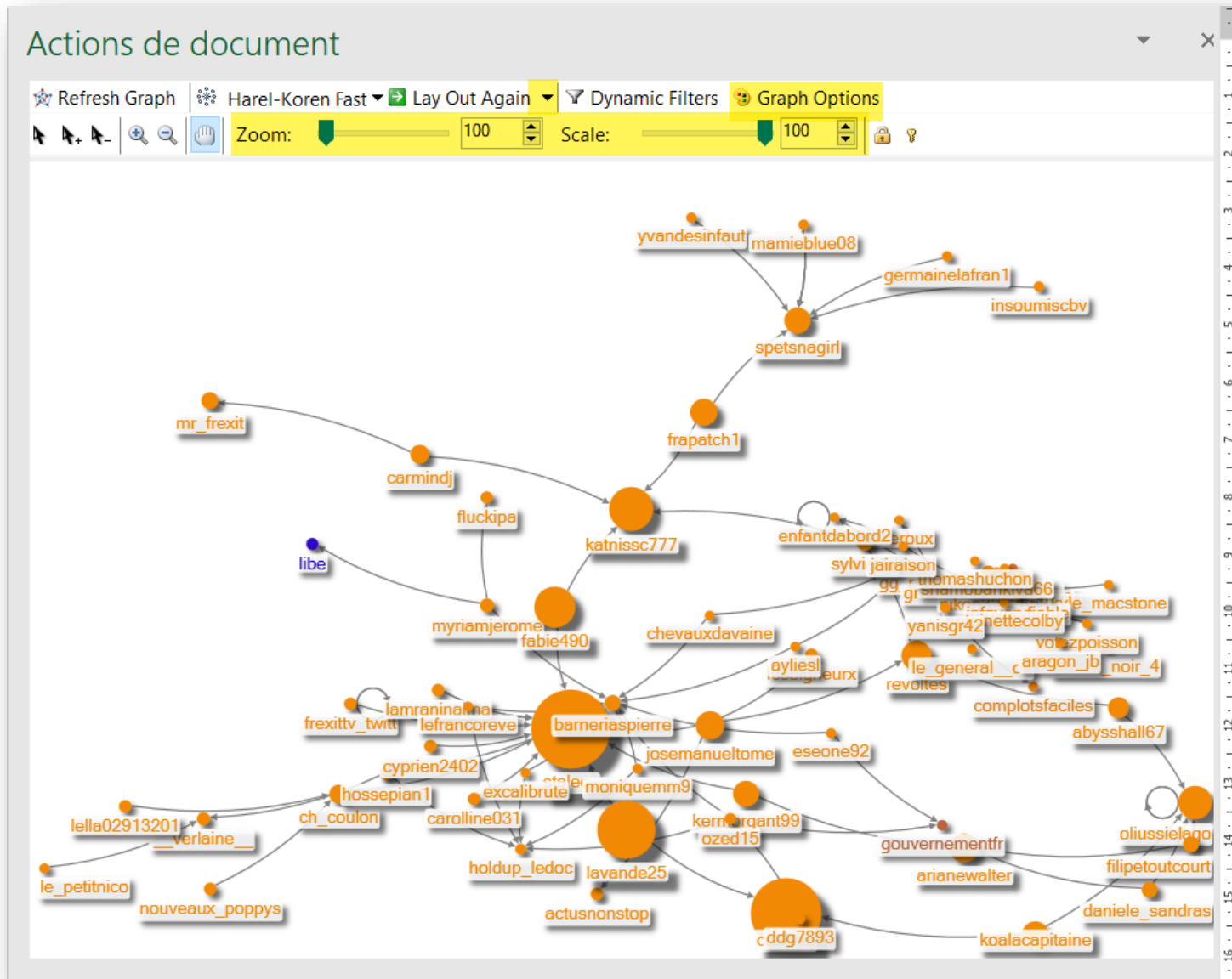
Calculate Metrics Cancel





# NodeXL





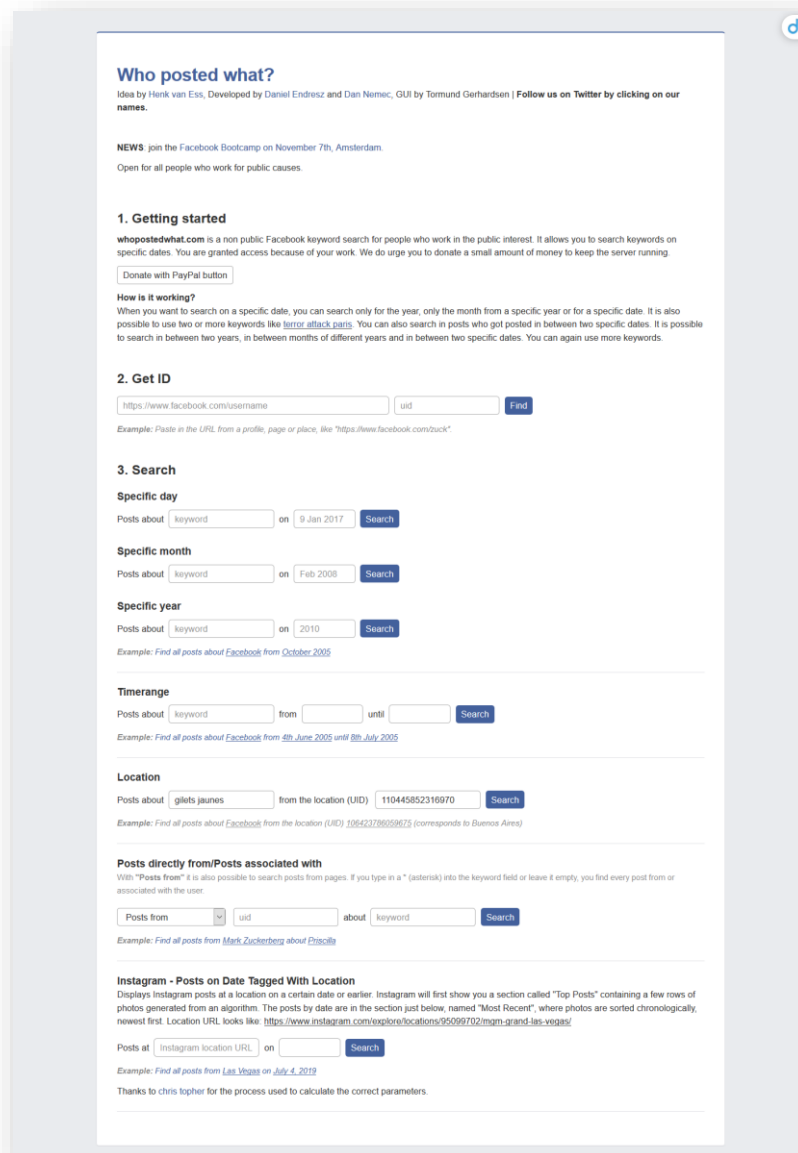
# Facebook

# Recherches précises sur une date ou une période ?

## Who posted what ?

### ► Recherche de posts (publics) contenant des mots particuliers

- à une date ou sur une période précise
- à partir d'une localisation précise (encore faut-il connaître l'identifiant du lieu ou sinon préciser la ville dans la page de réponse)
- utilisés par un compte ou une Page particulière



# Un couteau suisse pour investiguer

[DumpItBlue+](#) (Le Tools), [documentation](#), [extension Chrome](#)

The image shows a browser window displaying a Facebook profile for Faruk Khan. The browser's address bar shows the URL `facebook.com/faruk.khan.mp/`. The Facebook navigation bar is visible at the top. The profile picture shows three people sitting in a room. Below the profile picture, the name **Faruk Khan** is displayed with a verified badge and the Bengali text **(ফারুক খান এমপি)**. Below the name, there are tabs for **Publications**, **À propos**, **Amis 4600**, **Photos**, **Vidéos**, **Lieux**, and **Plus**. A notification bar at the bottom of the profile section says "Abonnez-vous à Faruk pour voir ses publications publiques dans votre fil d'actualité." and shows **145 381 abonnés** with a **S'abonner** button.

Overlaid on the right side of the browser window is the **DumpItBlue+** extension interface, which is highlighted with a red border. The interface includes the following elements:

- DumpItBlue+** logo and title.
- Current Profile ID**: A text box containing the ID `100008352791617`.
- Fonctions** (Functions) section with a list of options, each with a plus sign and a button:
  - + Scrolling
  - + Expanding
  - + Removing
  - + Dumping
  - + Isolate scrollable
  - + Others

Below the profile name, a red-bordered box contains the text **Exemple : [Faruk Khan](#)**.



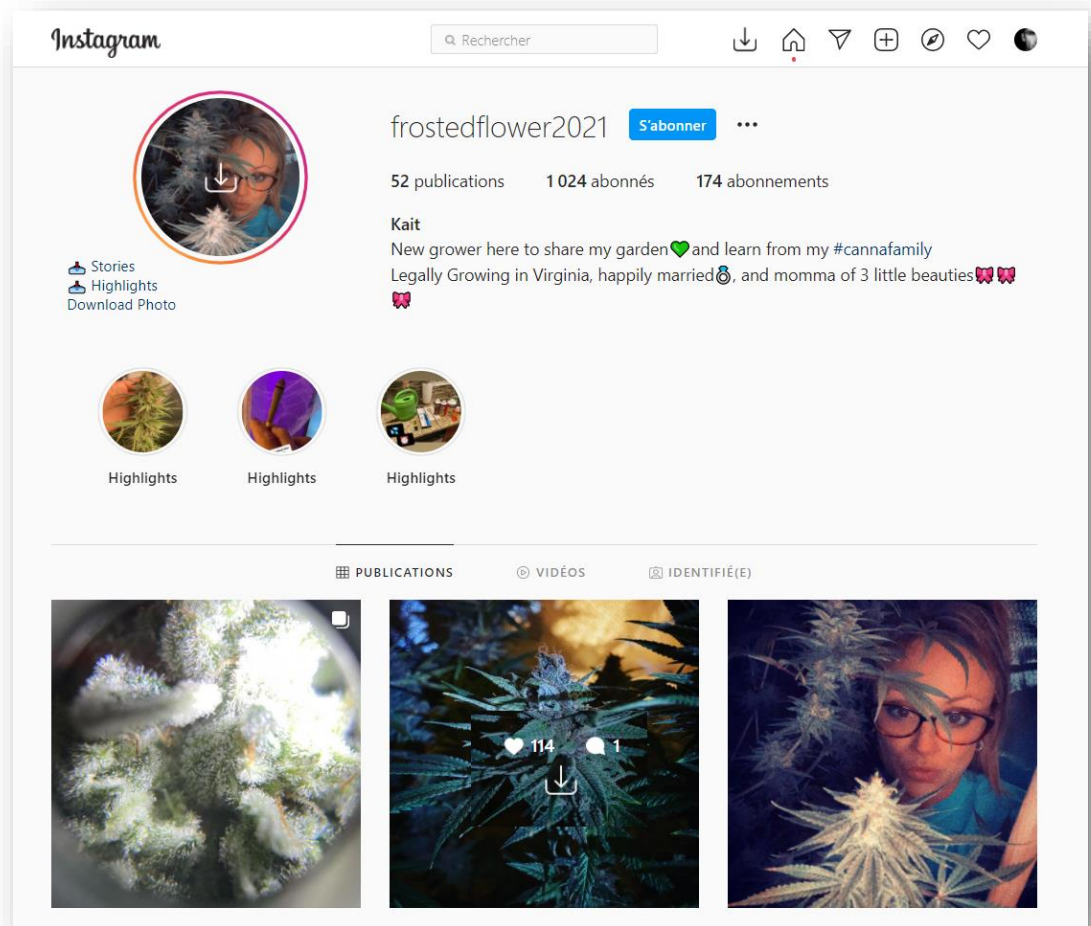
# Instagram

# Télécharger facilement photos, vidéos, stories

## IG Downloader

► Téléchargement de stories, images, vidéos, stories et même ensemble des images (mais à éviter sur de gros comptes au risque de se faire bloquer par Instagram)

► Exemple avec [@frostedflower2021](https://www.instagram.com/frostedflower2021)

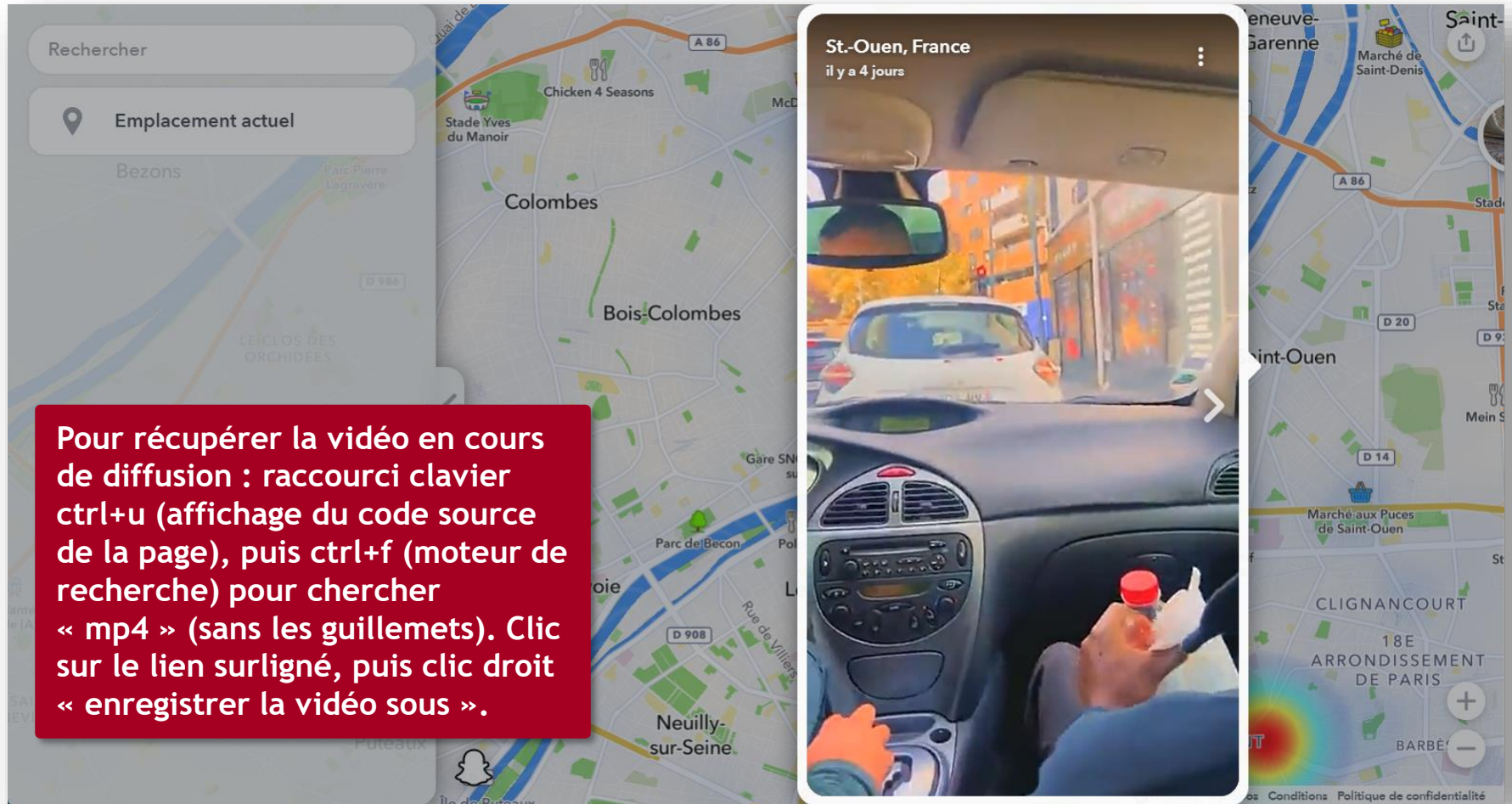


# Snapchat

Application très utilisée par des préados, ados et jeunes adultes

# Visualiser et télécharger des stories géolocalisées

## Snapmap : stories géolocalisées



The image shows a composite of three elements. On the left is a search interface with a 'Rechercher' field and an 'Emplacement actuel' button. Below this is a map of Paris with various districts labeled, including Bezons, Colombes, Bois-Colombes, Neuilly-sur-Seine, and Clignancourt. A red text box is overlaid on the map. In the center is a video story from a car, showing a white car in traffic, with the text 'St.-Ouen, France' and 'il y a 4 jours'. On the right is another map view showing the location of the video story in Saint-Ouen, France, with a heatmap overlay indicating the video's path.

Rechercher

Emplacement actuel

Bezons

Colombes

Bois-Colombes

Neuilly-sur-Seine

CLIGNANCOURT

18E ARRONDISSEMENT DE PARIS

St.-Ouen, France  
il y a 4 jours

Stade Yves du Manoir

Chicken 4 Seasons

Marché aux Puces de Saint-Ouen

Marché de Saint-Denis

Stade de Saint-Denis

Stade de Saint-Ouen

Mein S

Conditions Politique de confidentialité

**Pour récupérer la vidéo en cours de diffusion : raccourci clavier ctrl+u (affichage du code source de la page), puis ctrl+f (moteur de recherche) pour chercher « mp4 » (sans les guillemets). Clic sur le lien surligné, puis clic droit « enregistrer la vidéo sous ».**

# FININT

L'investigation financière

# Ouverture de la base Sirene

## Pappers

The screenshot shows the Pappers website interface for the company DOCTISSIMO. The main header includes navigation tabs like 'Informations Juridiques', 'Activité', 'Dirigeants', 'Établissements', 'BODACC', 'Actes', 'Comptes', 'Bénéficiaires', and 'Marques'. The company name 'DOCTISSIMO' and SIREN number '562 013 524' are prominently displayed. Below this, there are several sections: 'Informations Juridiques de DOCTISSIMO' with details on SIREN, SIRET, legal form (SAS), and capital; 'Activité de la société DOCTISSIMO' describing its core business in software development; 'Finances de DOCTISSIMO' with a note that no financial information is currently available; 'Dirigeants de l'entreprise DOCTISSIMO' listing the president; 'Établissements de DOCTISSIMO' listing the company's address; and 'Documents Juridiques de DOCTISSIMO' listing various legal documents like articles of association and annual reports.

## Societe.ninja

The screenshot shows the Societe.ninja website interface for the company DOCTISSIMO. The main header includes navigation tabs like 'Unité Légale', 'Historique', 'Observations', 'BODACC', 'Représentants', 'Bénéficiaires', 'Actes', and 'Comptes'. The company name 'DOCTISSIMO' is at the top. Below this, there are several sections: 'UNITE LEGALE' with a table of key information; 'ANNONCES BODACC' with a table of recent announcements; and 'REPRESENTANTS' with a table of company officers.

UNITE LEGALE	
Dénomination Sociale	DOCTISSIMO
Siège Social	8 RUE SAINT FIACRE 75002 PARIS 2
Forme Juridique	SAS, société par actions simplifiée
Capital Social	16 980 256,00 EUR
Immatriculation	01/01/1956
Greffe	Tribunal de Commerce de PARIS
N° SIREN	562013524
Code NAF	58.14Z

ANNONCES BODACC			
29/01/2021	PARIS	Modifications	Afficher
07/10/2020	PARIS	Modifications	Afficher
07/10/2020	PARIS	Modifications	Afficher
02/01/2019	PARIS	Immatriculations	Afficher
25/10/2018	NANTERRE	Modifications	Afficher
17/10/2018	NANTERRE	Modifications	Afficher
29/02/2016	NANTERRE	Modifications	Afficher

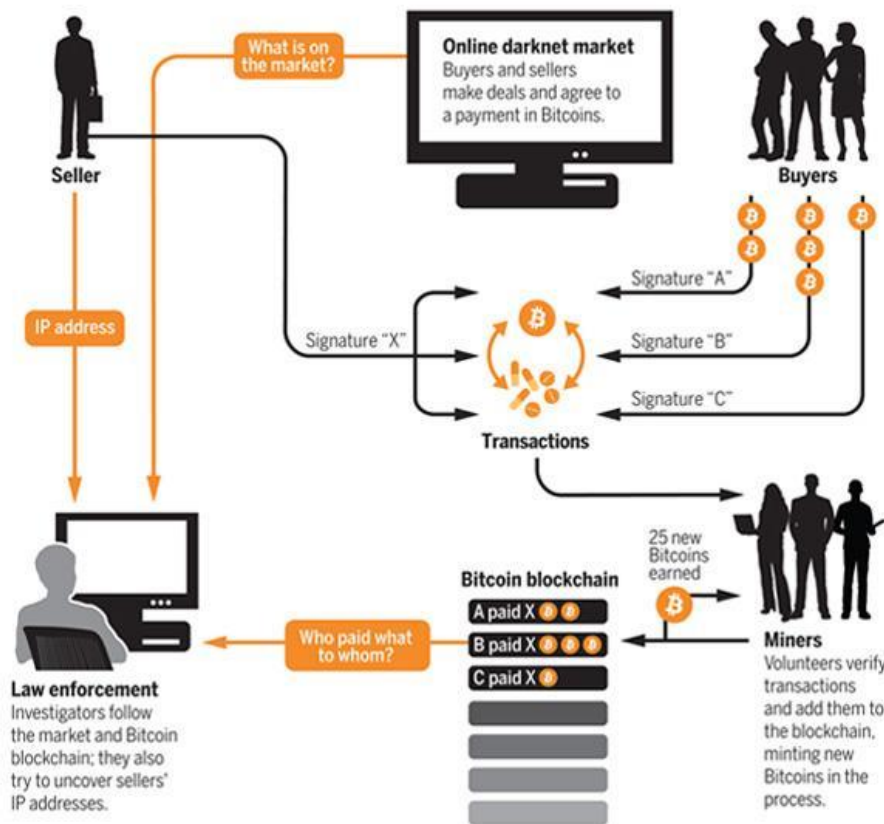
REPRESENTANTS	
Président	UNIFY (824649495) 1 quai du Point du Jour 92100 BOULOGNE-BILLANCOURT
Commissaire aux comptes titulaire	ERNST & YOUNG ET AUTRES - SOCIETE PAR ACTIONS SIMPLIFIEE A CAPITAL VARIABLE (438476913) 1-2 place des Saisons - Paris la Défense 1 92400 COURBEVOIE

# Follow the Money

## Why criminals can't hide behind Bitcoin (ScienceMag, 2016)

### Following the Bitcoin breadcrumbs

Although Bitcoin is designed to protect privacy, it nonetheless generates abundant public data. Investigators try to connect the transactions publicly recorded in the Bitcoin blockchain to sales on online drug markets and, ultimately, to sellers.



# Investiguer les sites Web (CYBINT/WEBINT)



# L'extension utile pour télécharger une page

Singlefile [[FIREFOX](#)] [[CHROMIUM](#)]

► Enregistrer la copie (horodatée) d'une page Web ([exemple avec qactus.fr](https://qactus.fr))



The image shows a browser window with the URL `qactus.fr/2021/11/15/maitre-carlos-alberto-brusa-avocat-et-president-d...`. The page features the **Qactus** logo and a video player. The video player has a title: **RÉACTION 19 Maître Carlos Alberto Brusa avocat et président de l'association Réaction19 a fait confirmer la présence de code alphanumérique chez les vaccinés.** A context menu for the SingleFile extension is open, listing options such as "Sauver la page avec SingleFile", "Annoter et sauver la page...", "Sauver les liens sélectionnés", "Sauver la sélection", "Sauver les onglets", "Auto-sauvegarde", "Possibilité de lire et de modifier les données du site", "Options", "Supprimer de Chrome", "Retirer", "Gérer les extensions", and "Inspecter le pop-up".

Etude de cas

# Accumuler les indices sur [marquechere.fr](https://marquechere.fr)

## Le couteau suisse : [ViewDNS](#)

WHOIS > Qui a déposé le nom de domaine ? Quand ? Quelle est l'adresse IP du serveur ?

- ▶ [Whois Lookup](#) (de DomainTools)

WHOIS History > Comment à évolué le WHOIS dans le temps ?

- ▶ [WHOIS History \(OSINT.SH\)](#)

Reverse IP > Quels sites sont hébergés sur la même adresse IP ?

- ▶ [Reverse IP \(de View DNS\)](#)
- ▶ [IPinfo](#)

Astuce : investiguer les IP proches

- ▶ [InfoByIp : exemple des IP proches](#)
  - [Reverse IP de 94.130.80.125](#) (par ViewDNS)

## [URLscan](#)



CHAUSSURES HOMME

- ▶ Nike React
- ▶ Nike Tn Requin
- ▶ Nike Air Jordan
- ▶ Nike Air Max 1
- ▶ Nike Air Max 90
- ▶ Nike Air Max 95
- ▶ Nike Air Max 97
- ▶ Nike Air Max 98
- ▶ Nike Air Max 270
- ▶ Nike Air Max 720
- ▶ Nike Air Max 2017
- ▶ Nike Air Max 2018
- ▶ Nike Air Max 2019
- ▶ Nike Air Max 2020
- ▶ Nike Air Max 2090
- ▶ Nike Air VaporMax
- ▶ Nike Air Max Speed
- ▶ Nike Air Max 200
- ▶ Nike Air Max Ultra
- ▶ Nike Air Barrage
- ▶ Nike Air Force
- ▶ Nike Air Huarache
- ▶ Nike Air More Uptempo
- ▶ Nike Cortez
- ▶ Nike Free
- ▶ Nike Joyride Run
- ▶ Nike Renew Run
- ▶ Nike LD+affle
- ▶ Nike M2K Tekno
- ▶ Nike SB Dunk
- ▶ Nike Shox
- ▶ Nike Tiempo
- ▶ Nike Zoom
- ▶ Nike TANJUN
- ▶ Chaussure Asics
- ▶ Chaussure Salomon
- ▶ Chaussures Givenchy
- ▶ Chaussure Adidas
- ▶ Chaussure Alexander McQueen

La Boutique des Marques en ligne - Plus de 300 marques et artistes urbains disponibles. Contactez-nous à :  
 Boutiquedesmarques@gmail.com    
 grossiste, revendeur, gagnez de l'argent, obtenez des cadeaux gratuits, contactez  
 WhatsApp: (+33 757934665) / (+852 62295751)

**Chaussure Nike Tn**

SSL    Paiement SÉCURISÉ    100% SECURISÉ

Generalement délais de livraison:  
 France, Belgique, Switzerland: Environ 5-12 jours  
 Reunion, Martinique, Guadeloupe: Environ 7-25 jours

Whatsapp: +33 757934665

Expédier à: France, Reunion, Guadeloupe, Martinique, Belgium, Switzerland

Commentaires Clients	Service Clients	Cadeau Gratuit	Paiement & Livraison
★★★★★			Domain
Commentaires Des Clients €-999 € 1055 Economie:			Last Resolved Date
			boutiquedesmarques.com
Nike Tn Requin Enfant-016 €-450 € 43 Economie: 71.34%			boutiquemaxs.com
			destocke.net
			destocksparis.fr
			fashionloverse.com
			franceendestock.fr
			marquedesport.fr
			marquedestock.fr
			marquesmagasin.fr
			marquesparis.fr
			marquesrunning.com
			marquesrunning.fr
			soldedemarque.fr
			tnpaschers.fr
			tnusine.fr
			usinemagasin.fr
			usinemax.fr
			vraisdestock.fr

Source : Clone Wars > [1ère partie](#), [2e partie](#), [3e partie](#), [4e partie](#) (Sherlock 2.0, oct. 2020)

# Les sites qui pointent dans sa direction

## Ahrefs Backlink Checker

(freemium, nombre de résultats limité à 100 dans la version gratuite)

- ▶ <http://shoeoutlet.site/>
- ▶ <http://sggparkingbordeaux.fr/SGGPB/SGGPB.asp>
- ▶ <http://www.brasserie-vaudemont.fr/brasserie/brasserie.asp>
- ▶ <https://emarque.fr>
- ▶ <https://boutiquemaxs.com/>

Backlink profile for **marquechere.fr**  
Domain including subdomains

Domain Rating: 0

Backlinks: 485 955

Referring Domains: 165  
1% dofollow

Top 100 backlinks | Top 5 anchors | Top 5 pages | One link per domain

Referring page	DR	UR	Referring Domains	Traffic	Anchor and backlink
Acheter soldes chaussures nike air max pour femme et homme pas cher france en ligne <a href="http://www.compagnieaugustesinge.fr">www.compagnieaugustesinge.fr</a>	3	22	14	0	<a href="http://www.marquechere.fr">www.marquechere.fr</a>
<a href="http://www.instantsbolero.fr">www.instantsbolero.fr</a>					<a href="http://www.marquechere.fr">www.marquechere.fr</a>
<a href="http://www.moring.fr/cuisine/cari-bichiques.php">www.moring.fr/cuisine/cari-bichiques.php</a>					
Vente Nike Air Max Thea Pas Cher, Air Max Thea de 2018 / Nike Air Max 90 Homme / Femme No... eau Pas Cher Magasin <a href="http://www.cacazone.fr">www.cacazone.fr</a>					
<a href="http://www.caspn.fr/seniors/stories/images/trombi">www.caspn.fr/seniors/stories/images/trombi</a>					

**SGG Parking Bordeaux** [www.marquechere.fr](http://www.marquechere.fr)

La Boutique des Marques en ligne - Plus de 100 marques et articles toujours disponibles - Contactez-nous à [backlinkchecker@gmail.com](mailto:backlinkchecker@gmail.com)

Expédier à: France, Reunion, Guadeloupe, Martinique, Belgium, Switzerland

Commentaires Clients: 5/5

Service Clients: 0-999 € 1055 Economie

Cadeau Gratuit: Cadeau Gratuit 0-999 € 1055 Economie

Paiement & Livraison: Paiement & Livraison 0-999 € 1055 Economie

Nike TR Reunion Entree 016 0-999 € 43 Economie: 71,34%

Nike Jordan Plus Entree 005 0-999 € 43 Economie: 64%

Nike Air Max Plus 3 0-999 € 54 Economie: 64%

Nike Air Max Plus 3 0-999 € 54 Economie: 64%

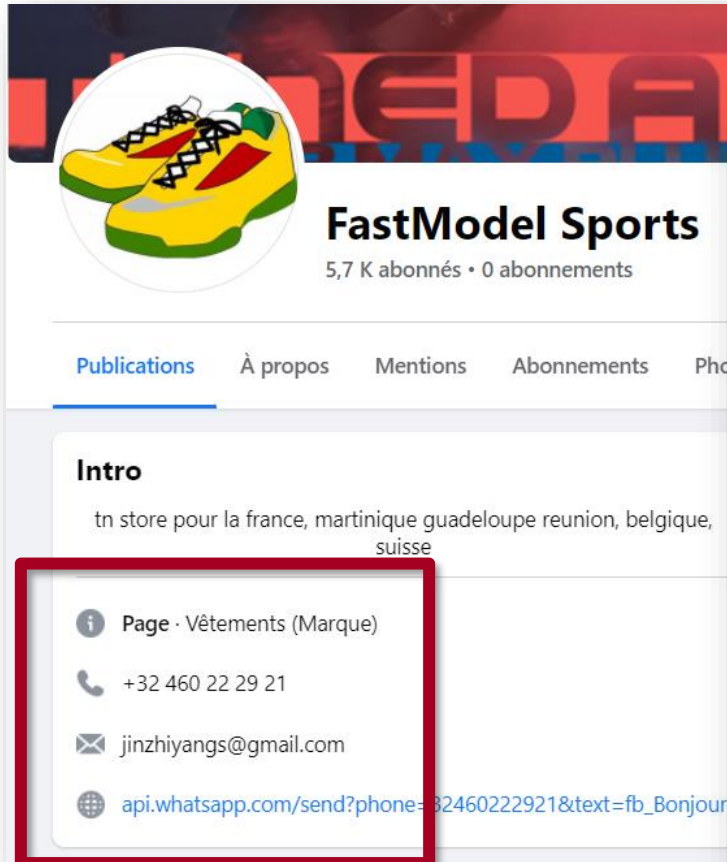
# Recueil d'indices dans un fichier Excezl

IP	NOM DE DOMAINE	DATE ENREGISTREMENT SITE WEB	adresse mail enregistrement nom domaine	COMPTE FACEBOOK	INSTAGRAM	ADRESSE MAIL sur le site web	NR DE TELEPHONE 1	NR DE TELEPHONE	NR DE TELEPHONE	SKYPE	SWAPCHAT	LOGO	MEME STRUCTURE PASE WEB	
143.205.67.37	alnetus.fr	29/04/2019	null			yy66a80@gmail.com	0525229908	32480322921	32480341807	null	Y966_1	YOY967	NIKE	1
94.130.80.121	arnaudlemepaschet.com	26/12/2019	null	<a href="https://www.facebook.com/FactMedelSports-111526386850254/">https://www.facebook.com/FactMedelSports-111526386850254/</a>	null	Boutiquedemarque@gmail.com	32480322921	85252295751	null	null	null	NIKE	1	
94.130.80.122	airmaxgros.com	04/12/2019	null	<a href="https://www.facebook.com/FactMedelSports-111526386850254/">https://www.facebook.com/FactMedelSports-111526386850254/</a>	<a href="https://www.instagram.com/nikeintuned">https://www.instagram.com/nikeintuned</a>	Boutiquedemarque@gmail.com	32480322921	85252295751	null	null	null	NIKE	1	
143.205.67.38	arts.fr	29/04/2017	jameyngit@ourlook.com	<a href="https://www.facebook.com/FactMedelSports-111526386850254/">https://www.facebook.com/FactMedelSports-111526386850254/</a>	null	yy66a80@gmail.com	0525229908	32480341807	null	Y966_1	YOY967	NIKE	1	
94.130.80.125	boutiquedemarque.com	26/03/2017	null	<a href="https://www.facebook.com/FactMedelSports-111526386850254/">https://www.facebook.com/FactMedelSports-111526386850254/</a>	null	Boutiquedemarque@gmail.com	32480322921	85252295751	null	null	null	NIKE	1	
94.130.80.123	boutiquefr.com	12/02/2019	null	<a href="https://www.facebook.com/FactMedelSports-111526386850254/">https://www.facebook.com/FactMedelSports-111526386850254/</a>	null	Boutiquedemarque@gmail.com	32480322921	85252295751	null	null	null	NIKE	1	
94.130.80.125	boutiquemais.com	29/02/2018	null	<a href="https://www.facebook.com/FactMedelSports-111526386850254/">https://www.facebook.com/FactMedelSports-111526386850254/</a>	null	Boutiquedemarque@gmail.com	32480322921	85252295751	null	null	null	NIKE	1	
94.130.80.122	boutiquemocler.fr	09/12/2019	null	<a href="https://www.facebook.com/FactMedelSports-111526386850254/">https://www.facebook.com/FactMedelSports-111526386850254/</a>	<a href="https://www.instagram.com/nikeintuned">https://www.instagram.com/nikeintuned</a>	Boutiquedemarque@gmail.com	32480322921	85252295751	null	null	null	NIKE	1	
94.130.80.123	boutiquedemarque.com	06/09/2017	null	<a href="https://www.facebook.com/FactMedelSports-111526386850254/">https://www.facebook.com/FactMedelSports-111526386850254/</a>	<a href="https://www.instagram.com/nikeintuned">https://www.instagram.com/nikeintuned</a>	Boutiquedemarque@gmail.com	32480322921	85252295751	null	null	null	NIKE	1	

**Pivoter :**  
**changer de plateforme et d'outils**  
**à partir d'un point particulier**

# La Page Facebook

<https://www.facebook.com/profile.php?id=100057197119938>

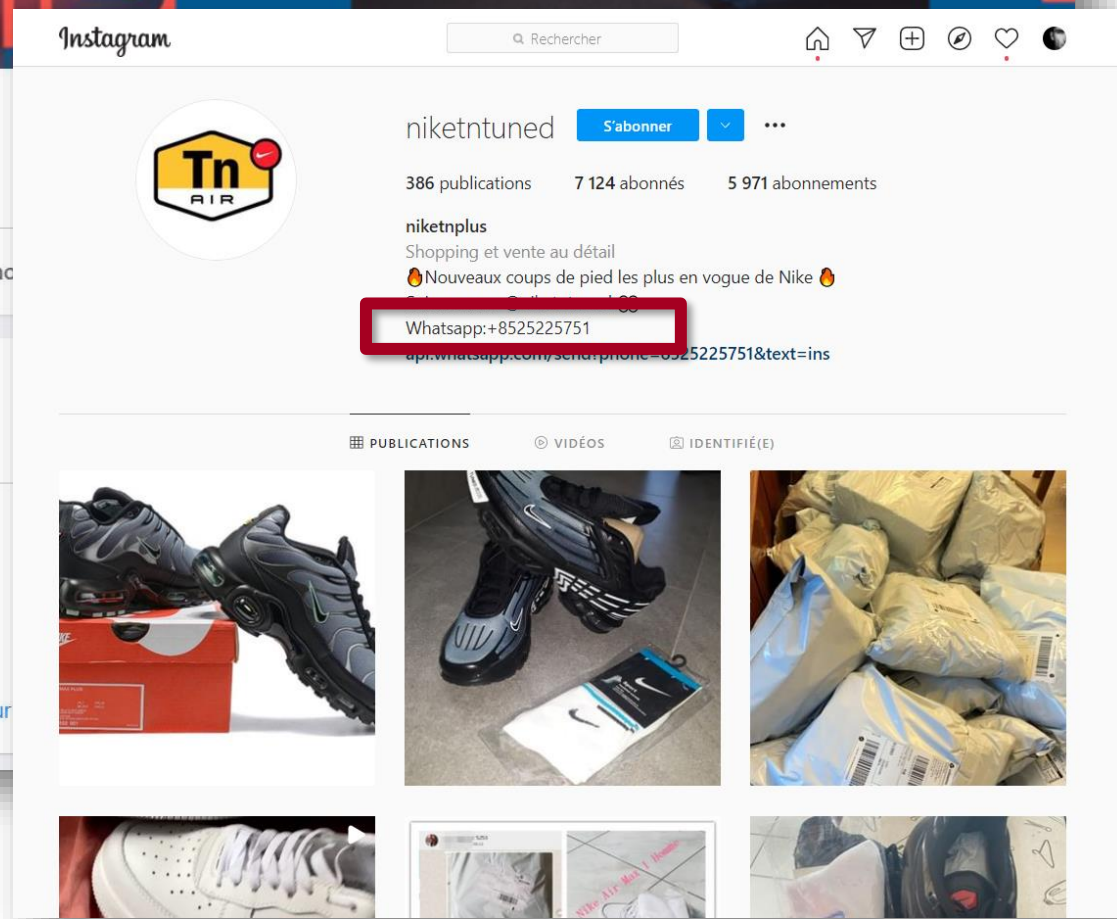


**FastModel Sports**  
5,7 K abonnés • 0 abonnements

Publications À propos Mentions Abonnements Photos

**Intro**  
tn store pour la france, martinique guadeloupe reunion, belgique, suisse

Page · Vêtements (Marque)  
+32 460 22 29 21  
jinzhiyangs@gmail.com  
[api.whatsapp.com/send?phone=32460222921&text=fb\\_Bonjour](https://api.whatsapp.com/send?phone=32460222921&text=fb_Bonjour)



Instagram

Rechercher

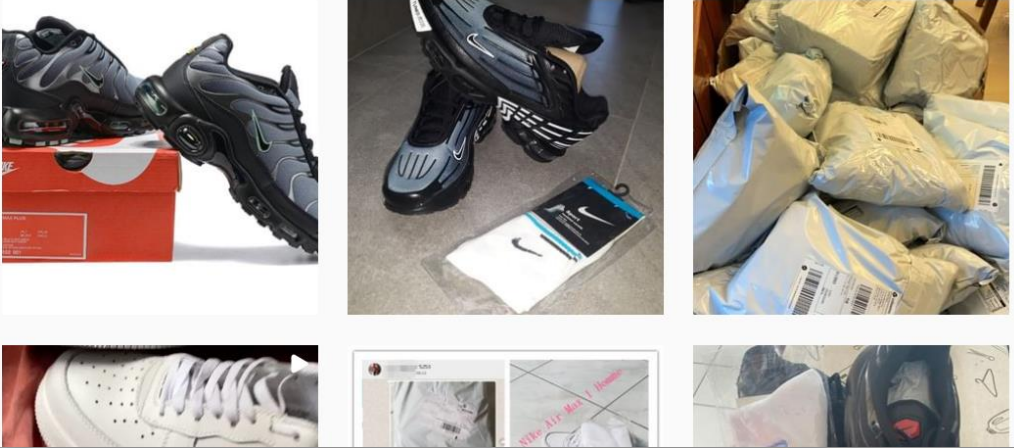
niketntuned S'abonner

386 publications 7 124 abonnés 5 971 abonnements

niketnplus  
Shopping et vente au détail  
🔥 Nouveaux coups de pied les plus en vogue de Nike 🔥

Whatsapp: +8525225751  
[api.whatsapp.com/send?phone=8525225751&text=ins](https://api.whatsapp.com/send?phone=8525225751&text=ins)


PUBLICATIONS VIDÉOS IDENTIFIÉ(E)



# Le compte Instagram

Instagram

<https://www.instagram.com/niketntuned/>

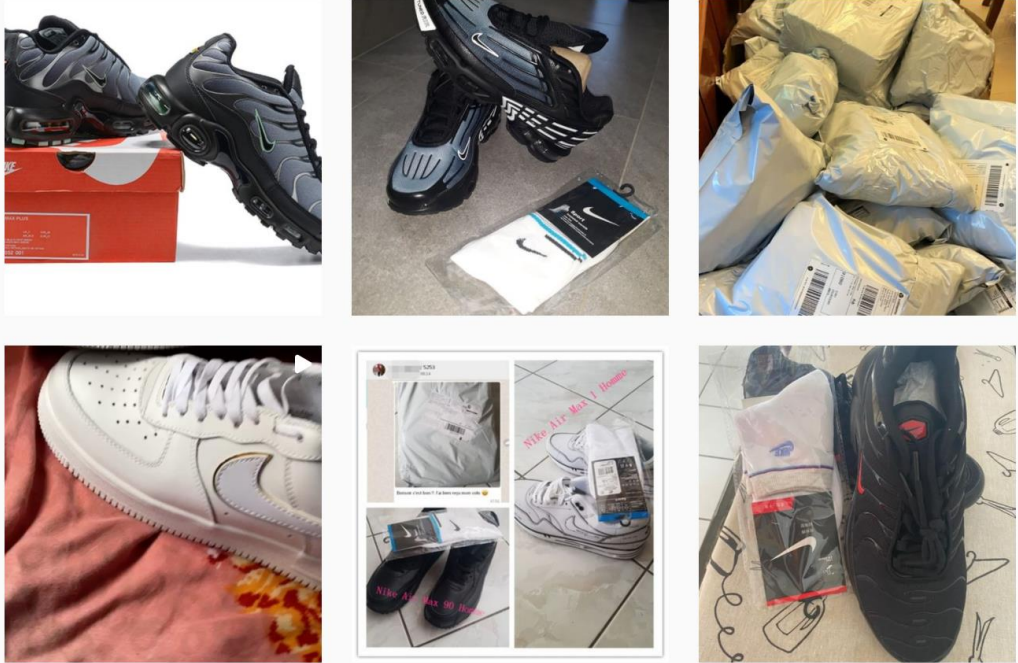


**niketntuned** S'abonner

386 publications 7 460 abonnés 5 970 abonnements

**niketnplus**  
Shopping et vente au détail  
🔥 Nouveaux coups de pied les plus en vogue de Nike 🔥  
Suivez nous: @niketntuned 📞  
Whatsapp: +8525225751  
[api.whatsapp.com/send?phone=8525225751&text=ins](https://api.whatsapp.com/send?phone=8525225751&text=ins)

PUBLICATIONS VIDEOS IDENTIFIÉ(E)





<https://twitter.com/YorkyyFN/status/1253013452332941312>

The image shows a screenshot of a Twitter post from the user Bébew Yorky (@YorkyyFN). The text of the tweet asks if anyone has ordered on a website and mentions a 'fake' or 'scam' site. A red box highlights the URL 'airtn.fr'. Below the text is a screenshot of a website for Nike shoes, which includes a list of sizes, a product image, and shipping information. A red box highlights the WhatsApp contact number '+32460244413' at the bottom of the website screenshot.

Bébew Yorky 🦉  
@YorkyyFN

il ya déjà des gens qui sont commander sur ce site ?  
parce que jsp si ses du fake ou ses de l'arnaque ditent  
moi svp le site ses : [airtn.fr](https://airtn.fr)

NIKE  
CHAUSSURE S HOMME

1 Nike Air Max  
2 Nike Air Max  
3 Nike Air Max  
4 Nike Air Max  
5 Nike Air Max  
6 Nike Air Max  
7 Nike Air Max  
8 Nike Air Max  
9 Nike Air Max  
10 Nike Air Max  
11 Nike Air Max  
12 Nike Air Max  
13 Nike Air Max  
14 Nike Air Max  
15 Nike Air Max  
16 Nike Air Max  
17 Nike Air Max  
18 Nike Air Max  
19 Nike Air Max  
20 Nike Air Max  
21 Nike Air Max  
22 Nike Air Max  
23 Nike Air Max  
24 Nike Air Max  
25 Nike Air Max  
26 Nike Air Max  
27 Nike Air Max  
28 Nike Air Max  
29 Nike Air Max  
30 Nike Air Max  
31 Nike Air Max  
32 Nike Air Max  
33 Nike Air Max  
34 Nike Air Max  
35 Nike Air Max  
36 Nike Air Max  
37 Nike Air Max  
38 Nike Air Max  
39 Nike Air Max  
40 Nike Air Max  
41 Nike Air Max  
42 Nike Air Max  
43 Nike Air Max  
44 Nike Air Max  
45 Nike Air Max  
46 Nike Air Max  
47 Nike Air Max  
48 Nike Air Max  
49 Nike Air Max  
50 Nike Air Max

Generalement deail de livraison:  
France,Belgique,Switzerland:Environ 5-12 jours  
Reunion,Martinique,Guadeloupe:Environ 7-25 jours

Whatsapp: +32460244413

Expédier à: France,Reunion,Guadeloupe,Martinique,Belgium,Switzerland

Whatsapp: +32460244413

# Le compte Gmail

## EPIOS Email Lookup

[jinzhiyangs@gmail.com](mailto:jinzhiyangs@gmail.com)

[boutiquesdemarque@gmail.com](mailto:boutiquesdemarque@gmail.com)

Google account finder will show you if the requested email address is linked to a google account, if the person has left reviews on google maps...

Email : Boutiquesdemarque@gmail.com

Name : lavie davina

GoogleID : 110343424259121042216

Last Update : 2021-05-02 16:51:50

Maps

<https://www.google.com/maps/contrib/110343424259121042216>

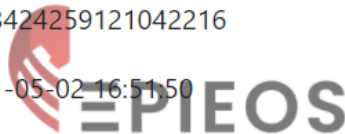
Photos

<https://get.google.com/albumarchive/110343424259121042216/albums/profile-photos>

Calendar : <https://calendar.google.com/calendar/htmlembed?src=Boutiquesdemarque@gmail.com>

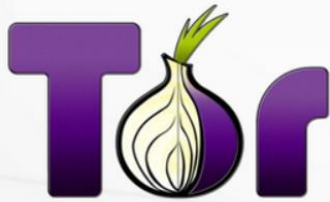
Reverse Image :

[Bing](#) [Google](#) [Yandex](#)



# Investiguer le dark web (DARKINT)

## Different “Dark Nets”



- Anonymous internet proxy network
- Data is routed through relays
- Internal & external network



- Anonymous peer-to-peer network
- Garlic routing with unidirectional “tunnels”
- Slow

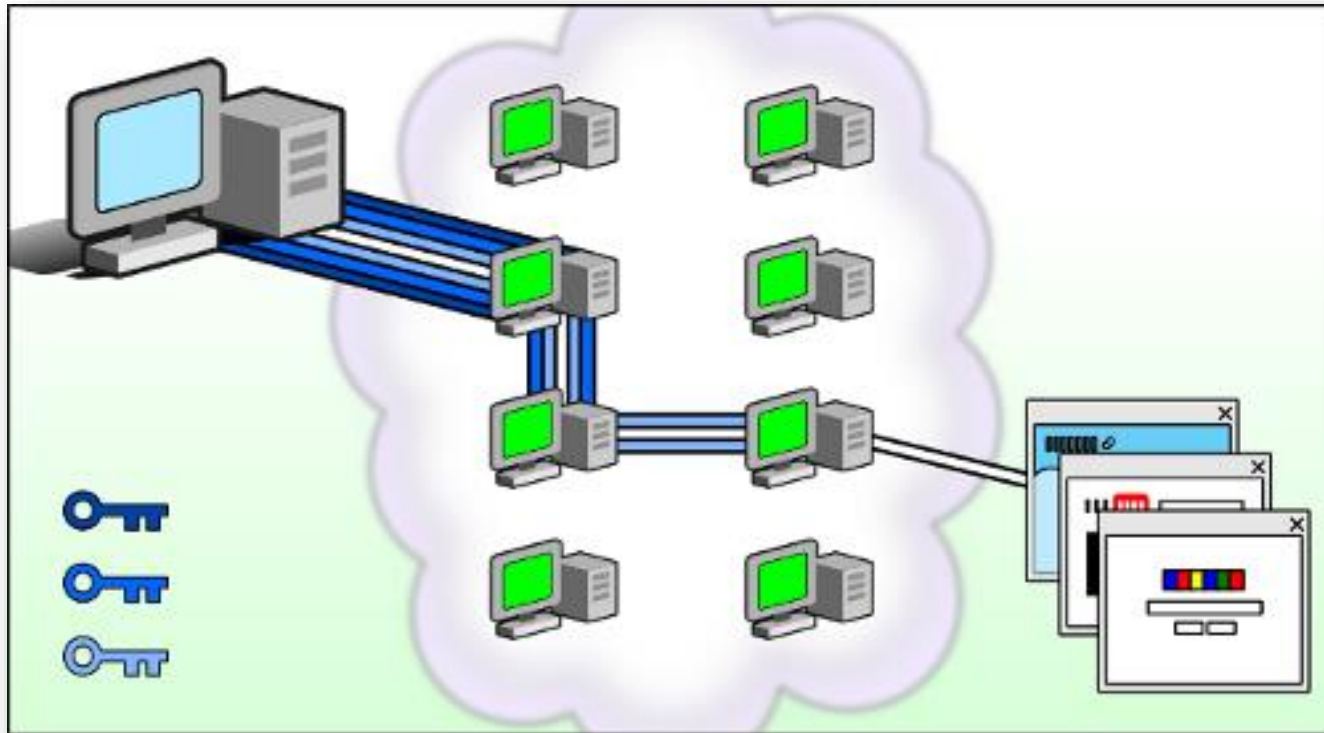


- Anonymous data publishing network
- Users “share” portions of their bandwidth & drive
- **Darknets** possible by strict peer-to-peer friends networks



Source : [Dark Web Searching](#) (OSINT Combine, 2020)

# Tor pour accéder anonymement à des sites Web



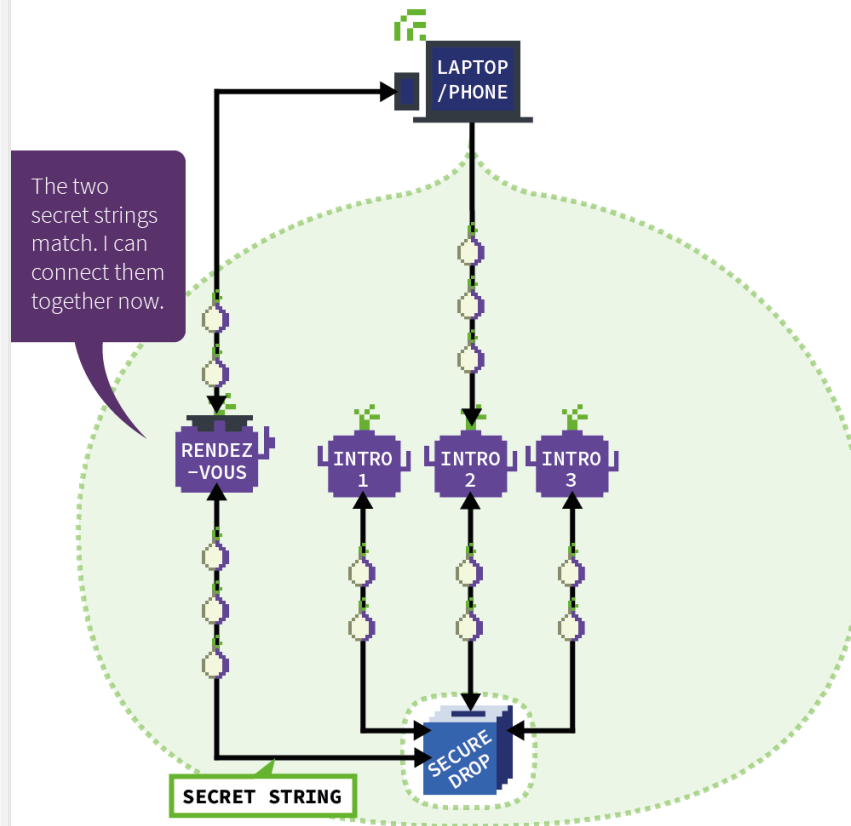
Source : [A propos du navigateur Tor](#) (Torproject, 2021)

# Tor pour héberger un « service Tor »

## ONION SERVICE

8/9

The rendezvous point makes one final verification to match the secret strings from you and service (the latter also comes from you but has been relayed through the service).



Source : [How do onion services work?](#)  
(Torproject, 2021)

# Moteurs de recherche

[Ahmia](#)

[TOR66 \(Fresh Onions\)](#)

[TORCH](#)

[OnionLand Search](#)






**TOR66** 01F 500 Search 01F 660 Random Onions

Promoted site ⓘ

**DIGITAL (COVID-19) CERTIFICATE**

Tor66 is moving to Onion-Version 3 Address: Please be sure to bookmark the right address!  
<http://tor66sewebgixwhcfnp5inzp5x5uohhdy3kvtnyfxc2e5mxiuh34iid.onion/>

Last 100 ( ⓘ fresh) .ONION websites found

Site	First seen * crawled	Lang
 ⓘ <a href="http://cashctdcopv3tbndc4hbj4tgky352znh2soqiww67qzr67237vomid.onion">http://cashctdcopv3tbndc4hbj4tgky352znh2soqiww67qzr67237vomid.onion</a> Cash Cow. PrePaid cards, Paypal Transfers and Accounts, Bank Transfers, Western Union Transfers, MoneyGram Transfers, Real Money, Gift Cards	4 Days ago * 4 Days ago	
 ⓘ <a href="http://preplyqxgvapegf44xvv3c2kgccyi7enmcbqpck63j54c6av4fj2e2qd.onion">http://preplyqxgvapegf44xvv3c2kgccyi7enmcbqpck63j54c6av4fj2e2qd.onion</a> A Prepaid Credit - Card Supplier	5 Days ago * 5 Days ago	EN
 ⓘ <a href="http://csalryx3xenotylyjtttsju6jfhtrjyt6ijwd3zzykhkpyfoeao2nxaqd.onion">http://csalryx3xenotylyjtttsju6jfhtrjyt6ijwd3zzykhkpyfoeao2nxaqd.onion</a> Trusted Credit Cards Vendor	5 Days ago * 5 Days ago	EN
 ⓘ <a href="http://cardpl74ltmwe4o7pgpefjcnng6qr36cnn7gzer2wermedxz3volxkqd.onion">http://cardpl74ltmwe4o7pgpefjcnng6qr36cnn7gzer2wermedxz3volxkqd.onion</a> 1A Credit Cards	5 Days ago * 5 Days ago	
 ⓘ <a href="http://undeb6m465pjocdl6kvyiwefj5xxzcu3hgznpgpe5eolw764suu5v3id.onion">http://undeb6m465pjocdl6kvyiwefj5xxzcu3hgznpgpe5eolw764suu5v3id.onion</a> Underground Market - Prepaid & Cloned Cards, Amazon Gift, PayPal	5 Days ago * 5 Days ago	

# Localiser un serveur

Une simple recherche dans [Shodan](#) pour trouver la localisation de [BlockStream Explorer](#) (insuffisamment protégé)

The image shows two overlapping screenshots. The background screenshot is from Shodan, displaying search results for the query `http://explorerzydxu5ecjrkwceayqybizmpjjznk5izmitf2modhcusuqlid.onion`. The results list one item: "Bitcoin Explorer - Blockstream". The location is listed as "United States, Kansas City" and is highlighted with a red box. The IP address is 35.201.74.156. The foreground screenshot is from the BlockStream Explorer website, showing a transaction page for the address `f82206145413db5c1272d5609c88581c414815e36e400aee6410e0de9a2d46b5`. The transaction status is "122025 Confirmations" and it was included in a block at height 588121 on 2019-08-01 18:22:20 UTC.


Source : [Shodan Dark Web Queries for OSINT Investigations](#) (OSINT Dojo, 2021)



# Marchés/vendeurs


## [List of darknet markets & vendor shops for investigators #3 \(OSINT.ME, 2021\)](#)


[[[[ PHISHING ALERT ]]] DNSTATS.NET DAKR.FAIL ASAPMARKETURL.COM [[[ PHISHING ALERT ]]] Avoid using any cleartnet proxy. ONLY GET VERIFIED LINKS FROM [ASAPMARKET dot CO] [DARK dot FAIL] [DARKNETLIVE dot COM] DISMISS


 Search for listings Login Register


- Categories
  - > Stimulants 2010
  - RCs 30
  - > Cannabis & hashish 2460
  - Drug paraphernalia 8
  - Steroids 554
  - Barbiturates 2
  - > Fraud 3595
  - Weight loss 26
  - > Ecstasy 803
  - Prescription 628
  - > Opioids 673
  - > Counterfeits 109
  - > Dissociatives 572
  - > Digital goods 4712
  - > Benzos 583
  - > Psychedelics 989
- Admin
- EXPAND

### Featured listings

- 

105ug LSD tabs - GammaGoblin
- 

Acetone Washed Columbian
- 

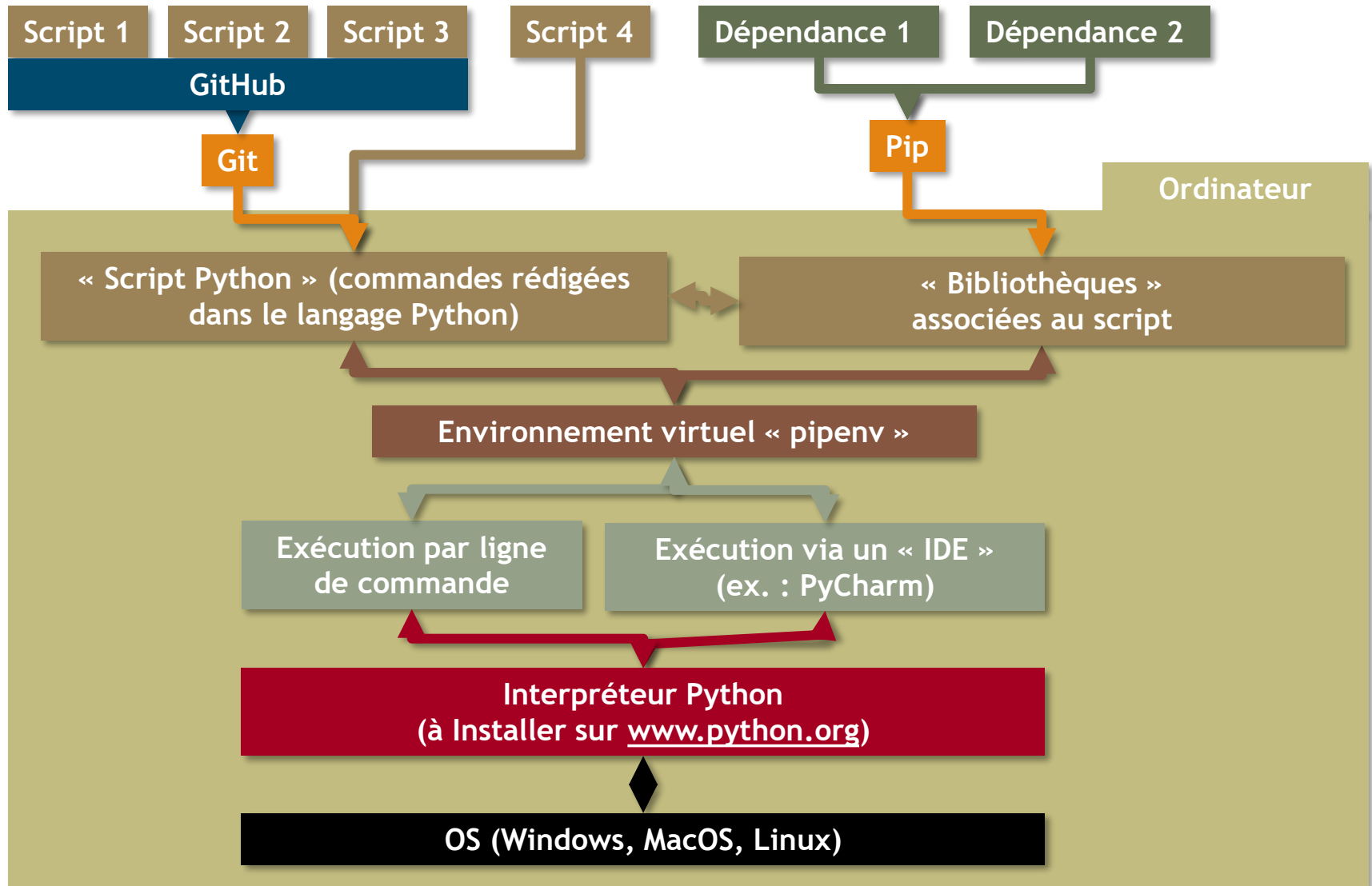
(Premium) Ohio Fake ID/Drivers
- 

Requires FE Amphetamin Oil Base

# Python

Accéder au niveau supérieur de l'OSINT

# Script Python : un exemple de fonctionnement

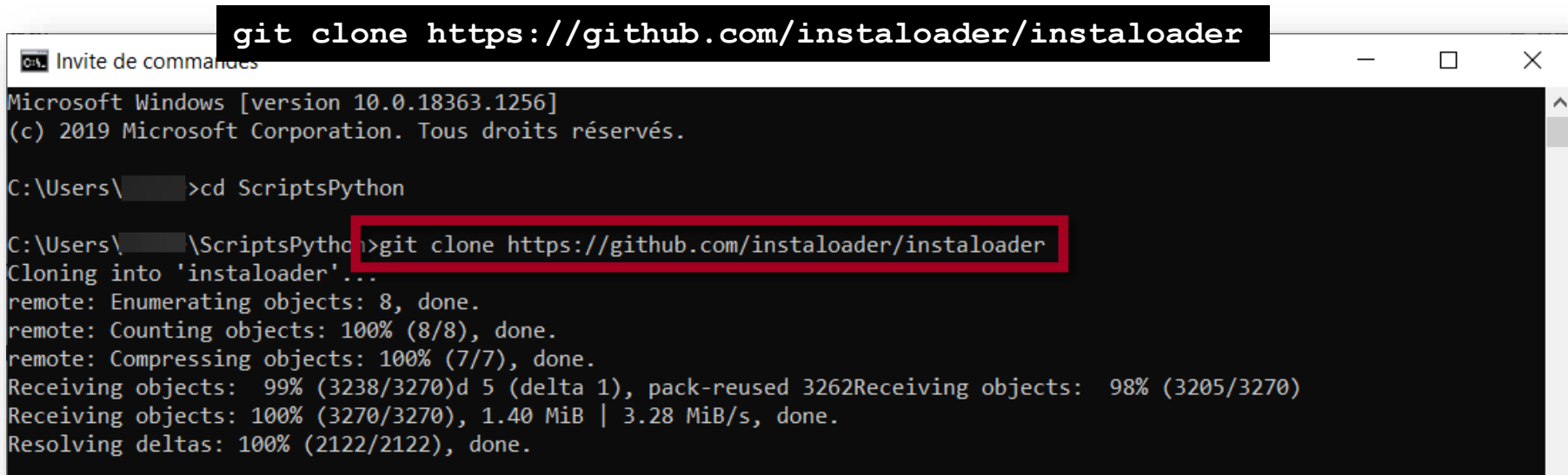


# Récupérer (« cloner ») un script en ligne de commande avec Git

L'exemple de Instaloader

# Récupérer (« cloner ») un script en ligne de commande avec Git

1. Accéder à l'invite de commande (cmd)
2. Accéder au dossier dans lequel vous souhaitez déposer le projet (cd) en utilisant la touche « tab » de votre clavier pour faciliter l'autocomplétion des noms de dossiers
3. saisissez « git clone » suivi de l'adresse du dépôt GitHub (ici : <https://github.com/instaloader/instaloader>)



```
git clone https://github.com/instaloader/instaloader
C:\Users\>cd ScriptsPython
C:\Users\>git clone https://github.com/instaloader/instaloader
Cloning into 'instaloader'...
remote: Enumerating objects: 8, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (7/7), done.
Receiving objects: 99% (3238/3270)d 5 (delta 1), pack-reused 3262Receiving objects: 98% (3205/3270)
Receiving objects: 100% (3270/3270), 1.40 MiB | 3.28 MiB/s, done.
Resolving deltas: 100% (2122/2122), done.
```

# Placer son script dans un environnement virtuel pipenv

# Placer son script dans un environnement virtuel pipenv

Pour installer le script dans un environnement ET télécharger les dépendances... se placer dans le dossier du projet, puis... 5 cas de figure se présentent

1. Si vous voyez à la racine du projet des fichiers Pipefile et Pifile.lock

```
pipenv install
```

# Se préparer à l'exécution

Votre script est placé dans un conteneur pipenv ? Il faut y entrer !

**pipenv shell**

```
To activate this project's virtualenv, run pipenv shell.  
Alternatively, run a command inside the virtualenv with pipenv run.  
  
C:\Users\██████\ScriptsPython\instaloder>pipenv shell  
Launching subshell in virtual environment...  
Microsoft Windows [version 10.0.18363.1256]  
(c) 2019 Microsoft Corporation. Tous droits réservés.  
  
(instaloder-qJRqQcp3) C:\Users\██████\ScriptsPython\instaloder>
```

**Vous voici dans le conteneur, d'où vous pourrez lancer le script**



# Exécuter le script

<https://www.instagram.com/fsin.russia/>

```
pipenv run instaloader profile fsin.russia
```

The image shows a terminal window on the left and a file explorer on the right. The terminal window displays the output of the command `pipenv run instaloader profile fsin.russia`. It shows the creation of a virtual environment, the installation of dependencies, and the execution of the `instaloader` script. The script successfully downloads a profile for `fsin.russia` and lists the most similar profiles. The file explorer on the right shows the directory `fsin.russia` containing a folder `ScriptsPython` and a subfolder `instaloader`. The `instaloader` folder contains a subfolder `fsin.russia` which contains a grid of downloaded images and videos. The files are named with their original filename and a timestamp, such as `2020-10-26_07-54-06_UTC_profile_pic.jpg`.

# Autres scripts à tester

# Quelques scripts à tester

## Facebook

- ▶ [FFFF : Find Facebook Friends](#)

## Twitter

- ▶ [Twint](#)
- ▶ [TwitWork](#)

## YouTube

- ▶ [YouTube Comment Downloader](#)

## Instagram

- ▶ [Instaloder](#)

## Discord

- ▶ [DiscordChatExporter](#)

## Snapchat

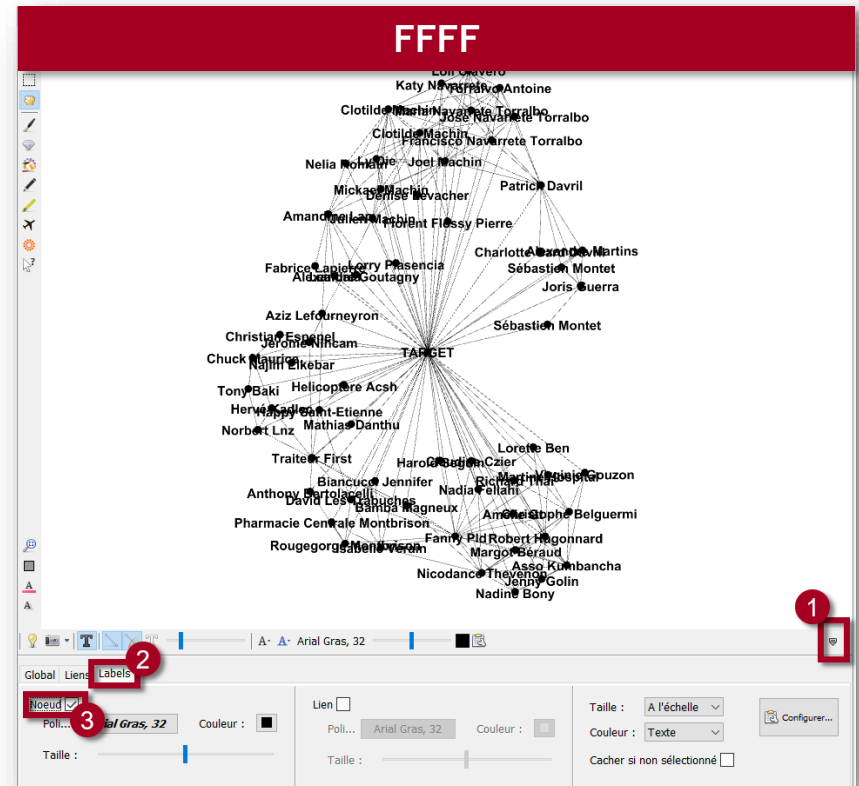
- ▶ [Snapchat Map Scraper](#)

## Nom d'utilisateur (associé à des comptes sociaux ?)

- ▶ [Sherlock](#)

## Email (associé à des comptes sociaux ?)

- ▶ [Holehe](#)



# A lire, à suivre

# A lire à suivre

Serge Courrier sur Twitter ([@secou](#))

► [Liste spécialisée OSINT](#)

Communauté OSINTFR sur Discord

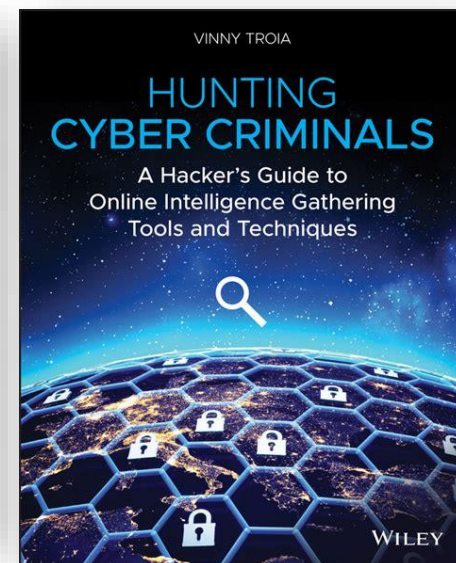
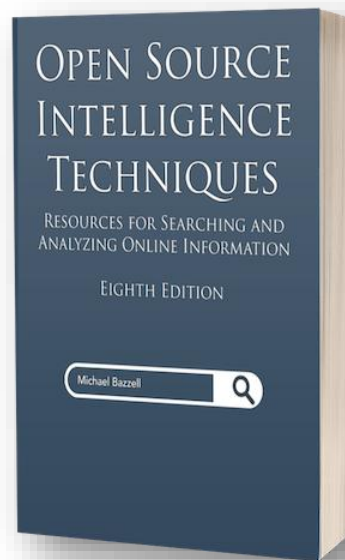
► Lien d'accès dans la bi du compte  
Twitter [@OSINTFR](#)

[Open Source Intelligence Techniques](#)

(Michael Bazzell, 2021)

[Hunting Cyber Criminals](#) (Vinny

Troia, 2020)



# Serge Courrier



- **Consultant** : intervient depuis 2005 auprès d'entreprises et d'organismes publics, pour développer leurs outils, méthodologies et stratégies de recherche, de veille et d'investigation, ainsi que leurs usages avancés d'Internet et notamment des réseaux et médias sociaux.
- **Formateur** : enseigne depuis 1996 les stratégies de recherche, de veille et d'investigation via Internet. Intervenant notamment à l'École Européenne d'intelligence économique (EEIE) où il pilote la spécialité OSINT, à l'Institut national de l'audiovisuel (INA), à l'association des professionnels de l'information (ADBS). Il assure également depuis 1998 la formation des rédactions de France Télévisions.
- **Auteur** : a publié un guide de 500 pages sur les outils, les usages et les méthodes de recherche via Internet (*Internet pour les journalistes*, Victoire Éditions, 2004), deux guides pratiques sur la syndication de contenu (*Utiliser les fils RSS et Atom*, février 2008, ADBS ; *Produire des fils RSS et Atom*, mars 2009, ADBS). A collaboré à *Le Web 2.0 en bibliothèque. Quels services ? Quels usages ?* (Le Cercle de la librairie, 2009)
- **Ex-Journaliste spécialisé** : a traité entre 1990 et 2014 de sujets liés à Internet et à l'Intelligence économique pour des magazines spécialisés et grand public. A précédemment occupé les postes de rédacteur en chef adjoint de *Génie Industriel*, *Science et Vie Micro (SVM)* et *Micro Hebdo*.