L'OSINT/ROSO en pratique

- Principes et exemples simples
- Enjeux pour les documentalistes

Serge Courrier ▸ 15 décembre 2021

adbs Secteur ATCE

AMENAGEMENT,
TRANSPORT,
CONSTRUCTION,
ENVIRONNEMENT

Se repérer dans les sigles

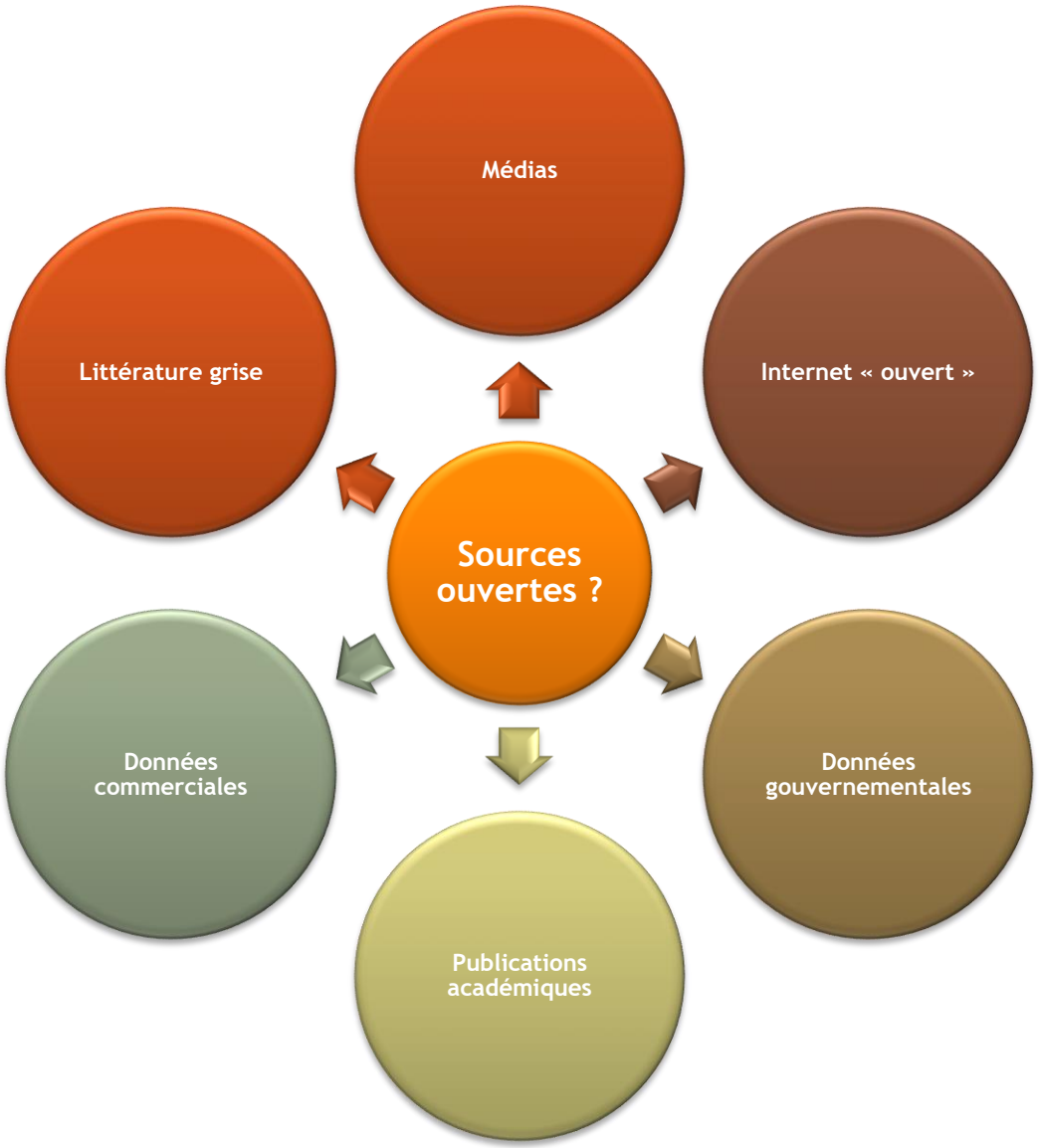
Se repérer dans les sigles

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)



Eviter les malentendus

OSINT = uniquement via Internet ? Oui… et non

OSINT = uniquement la captation ? Non

OSINT ≠ HUMINT ? Oui

OSINT ≠ Piratage ? Oui

Les grandes subdivisions

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

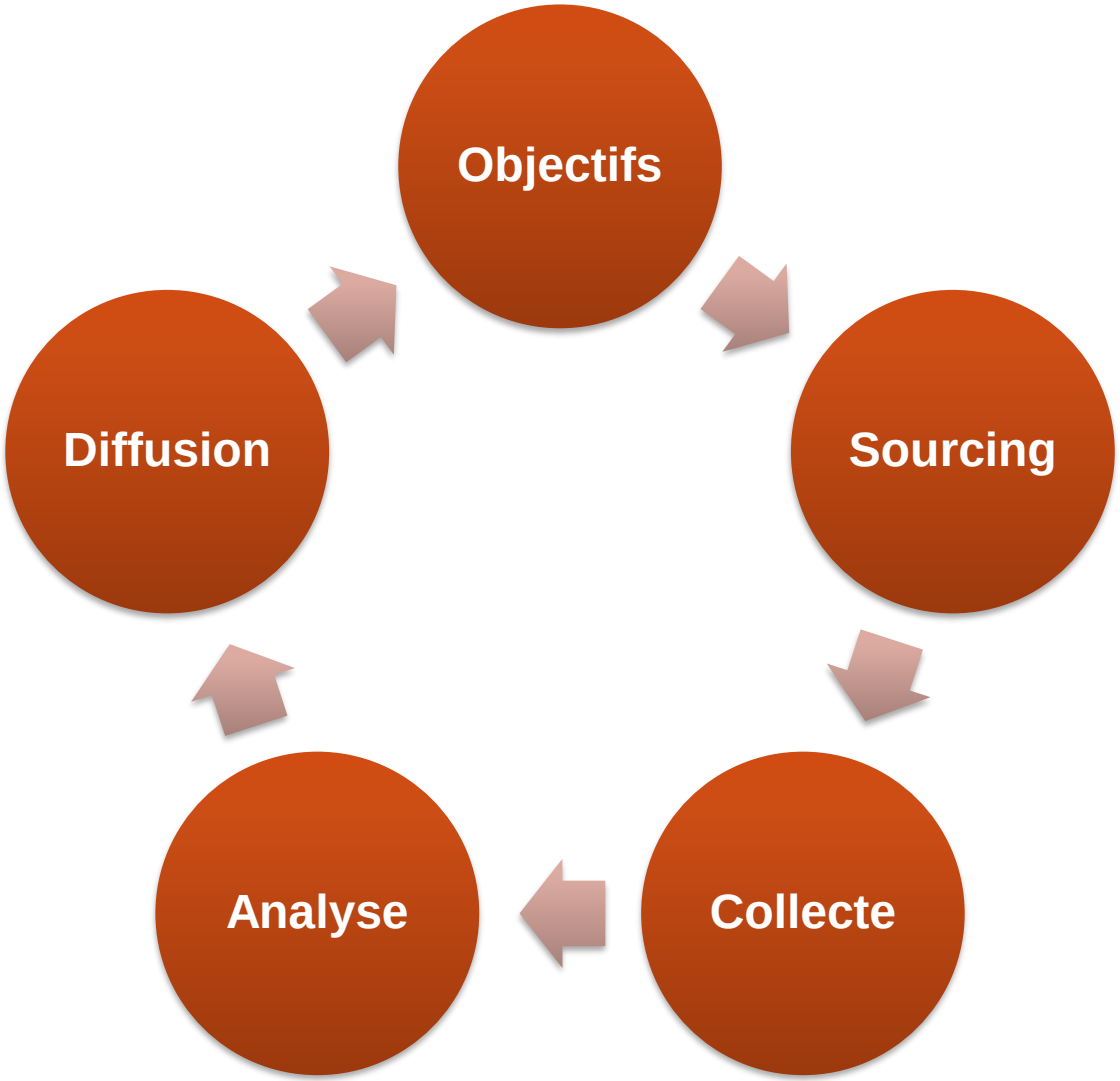
Acronym	Meaning
OSINT	Open-Source Intelligence
SOCMINT	Social Media Intelligence
GEOINT	Geo-Spatial Intelligence
IMINT	Imagery Intelligence
ORBINT	Orbital Intelligence
VATINT	Vehicle and Transportation Intelligence
SIGINT	Signals Intelligence
TECHINT	Technical Intelligence
FININT	Financial Intelligence
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

L’essentiel face à un moteur de 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"
	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 crésus

*** (troncature) ◗ remplace une chaine 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

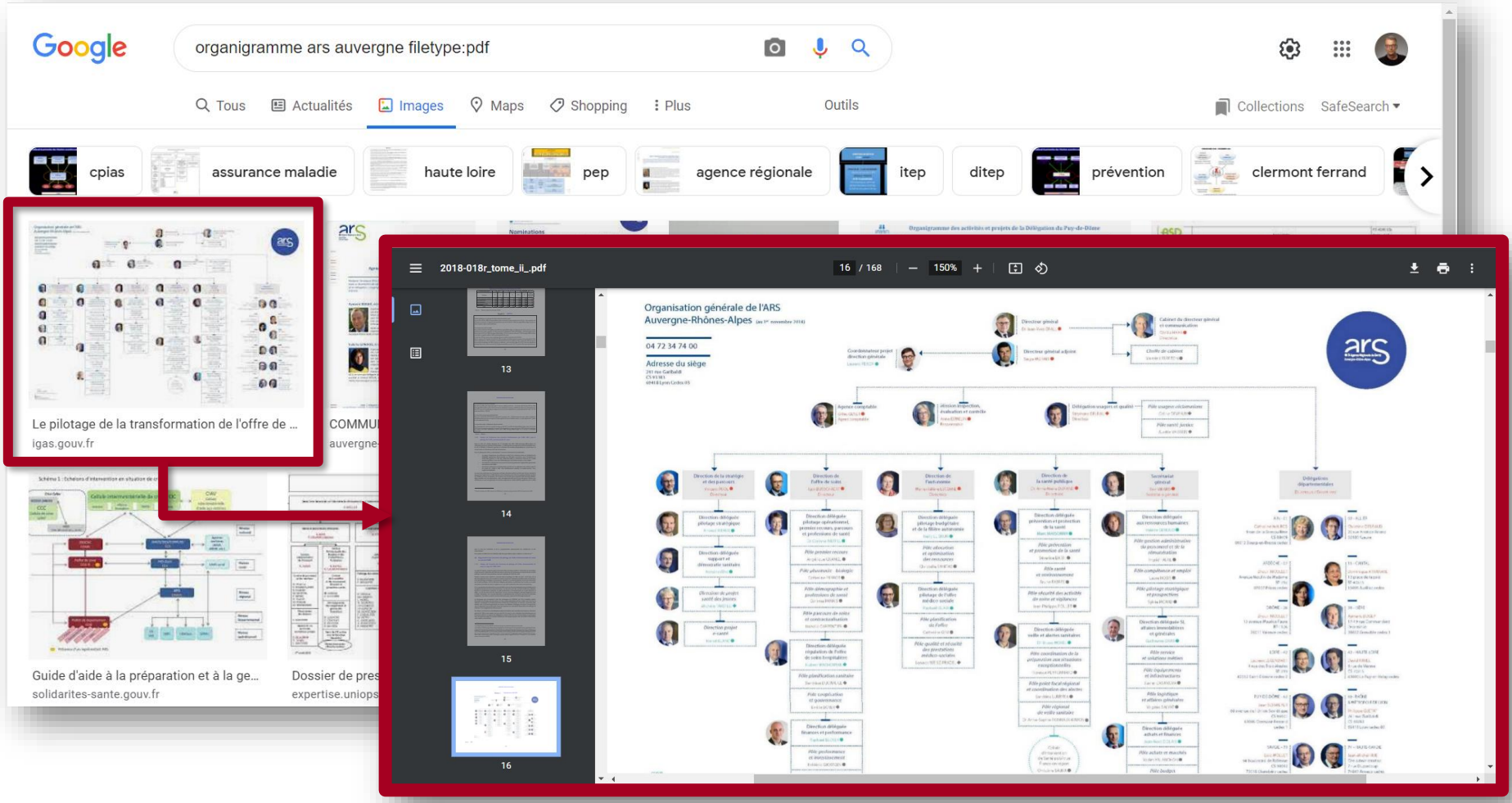
►survivalistes france inurl:liens OR intitle:liens

"0.. {mot}" ◗ Mot précédé d'un nombre

►saisie "0.. kg de cocaïne"

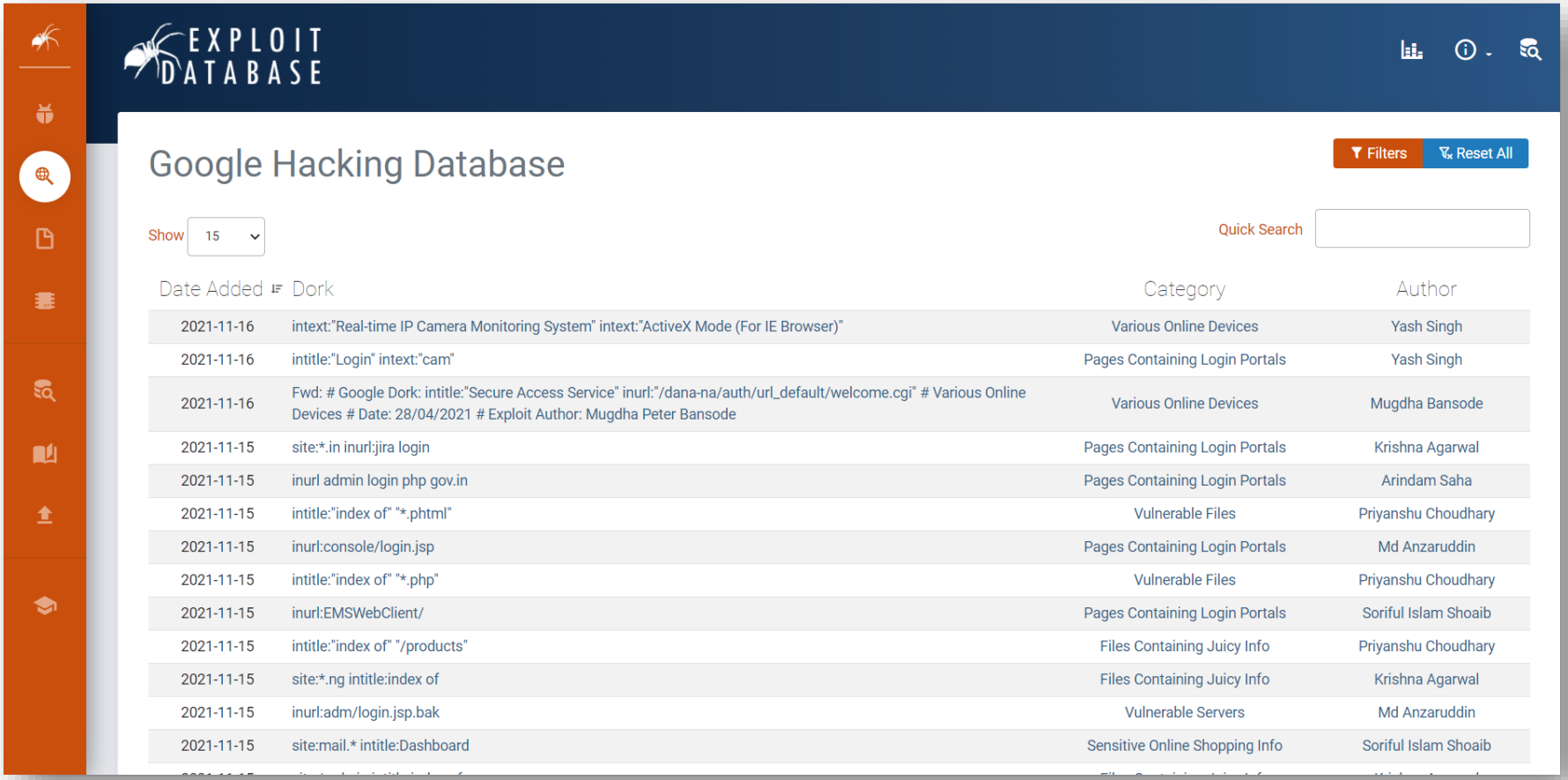
filetype: dans Google Images ?

organigramme ARS auvergne filetype:pdf (dans Google Images)



Google Dorks

Google Hacking Database



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

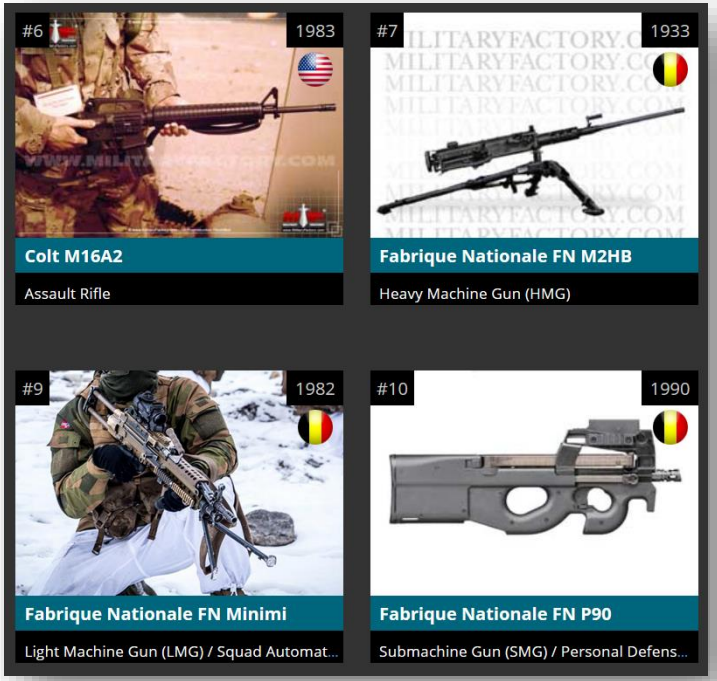
- ► Camopedia (camouflage)
- ► Military Factory
- ► Weapons ID Database
- ► Référentiel général des armes (RGA)

Voitures

- ► Oscaro (identifier le modèle d'une voiture à partir de son immatriculation)

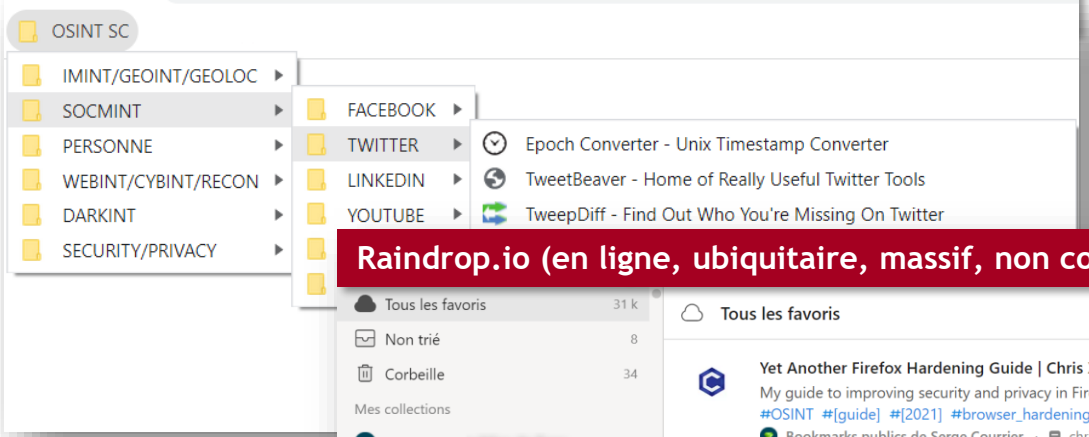
Avions

- ► Aircraft registration (voir External Links)

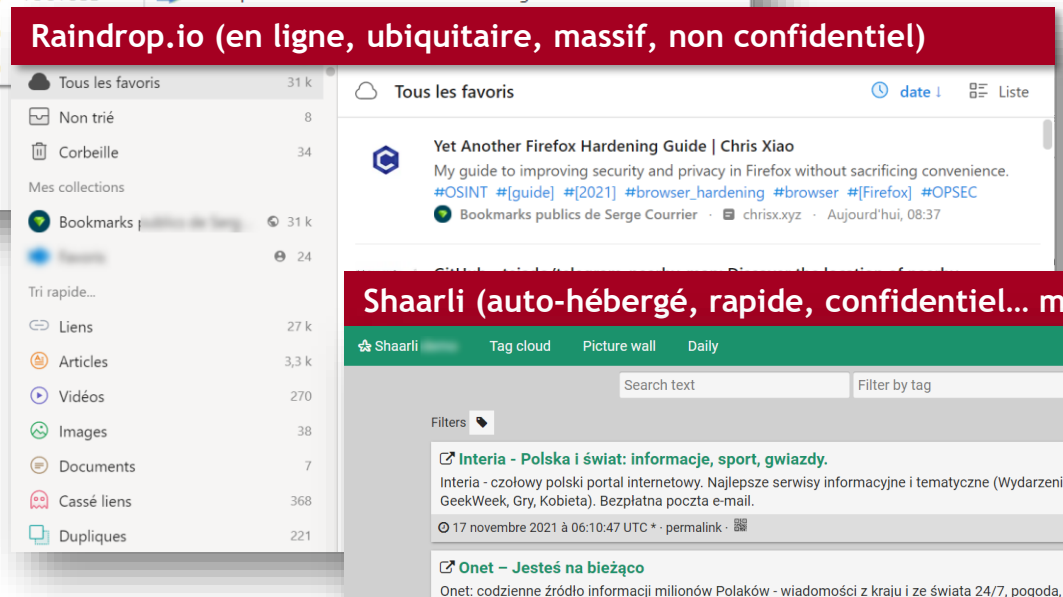


Gérer ses favoris

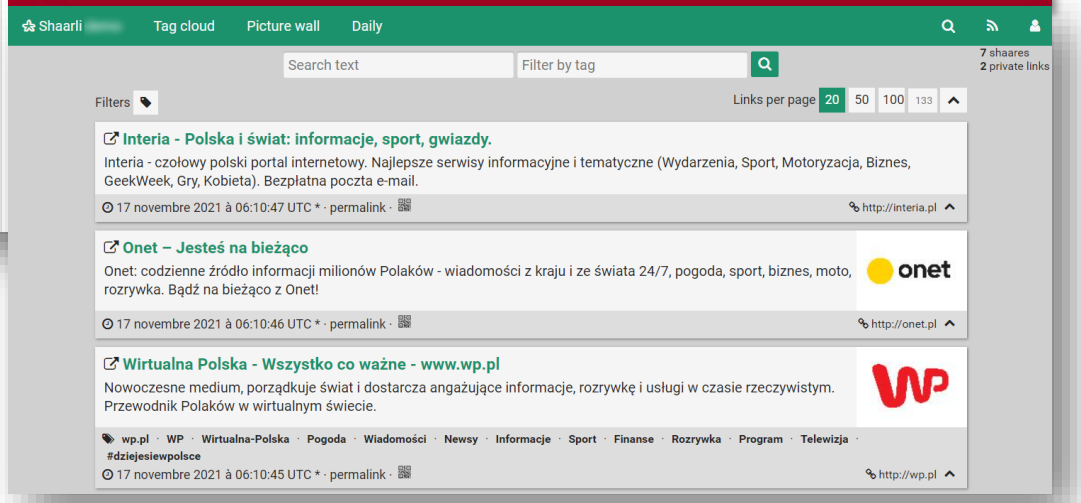
Navigateur (rapide, confidentiel, lourd si les favoris sont nombreux)



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



Shaarli (auto-hébergé, rapide, confidentiel… mais technique)



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
- ▶AmIUnique

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 ?

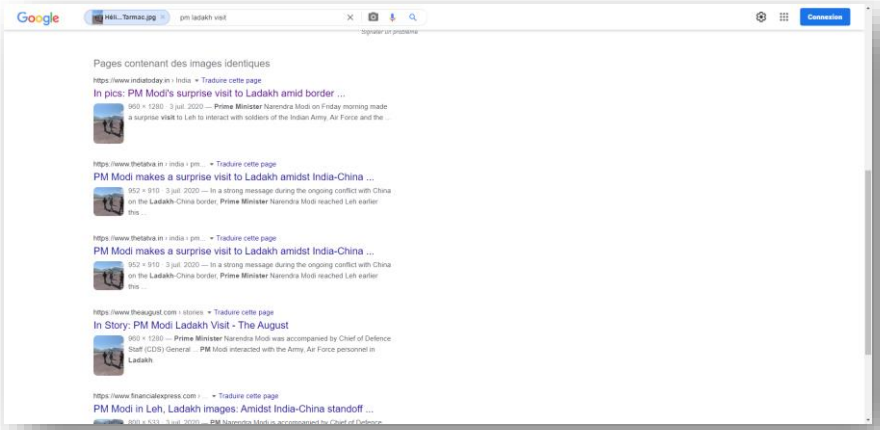
Qui ? Où ? Quel jour ? A quelle heure ?

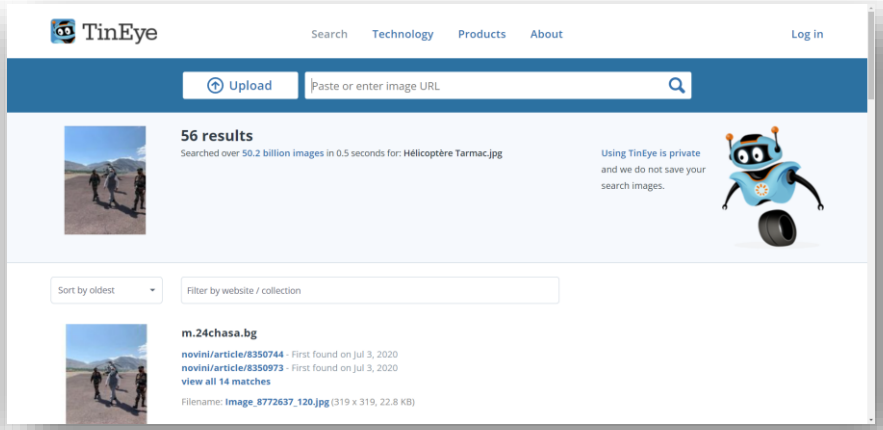
Source : FINDING: MODI – Find where & when a photo was taken (geolocation & chronolocation) (Bendobrown, 10/05/2021)

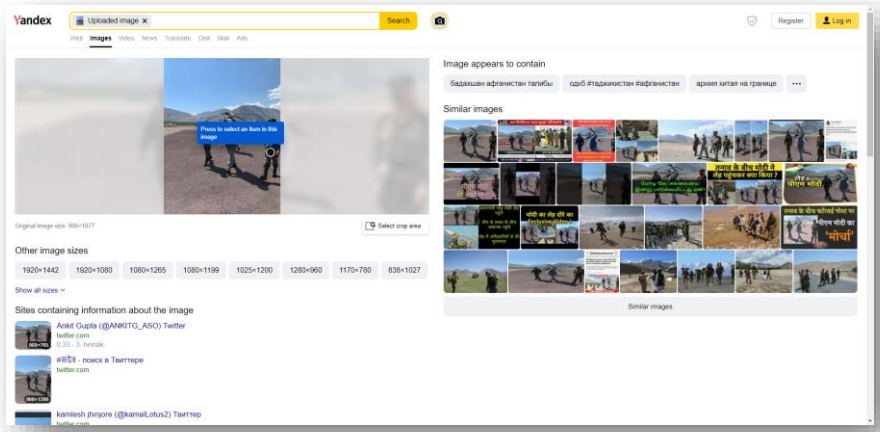
Recherche inversée

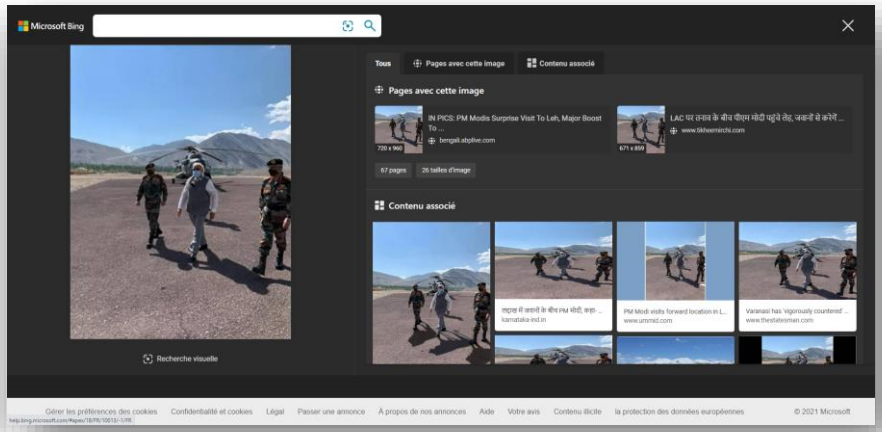
Extension Search By Image (Firefox, Chrome)

►Clic droit sur l'icône pour afficher les options

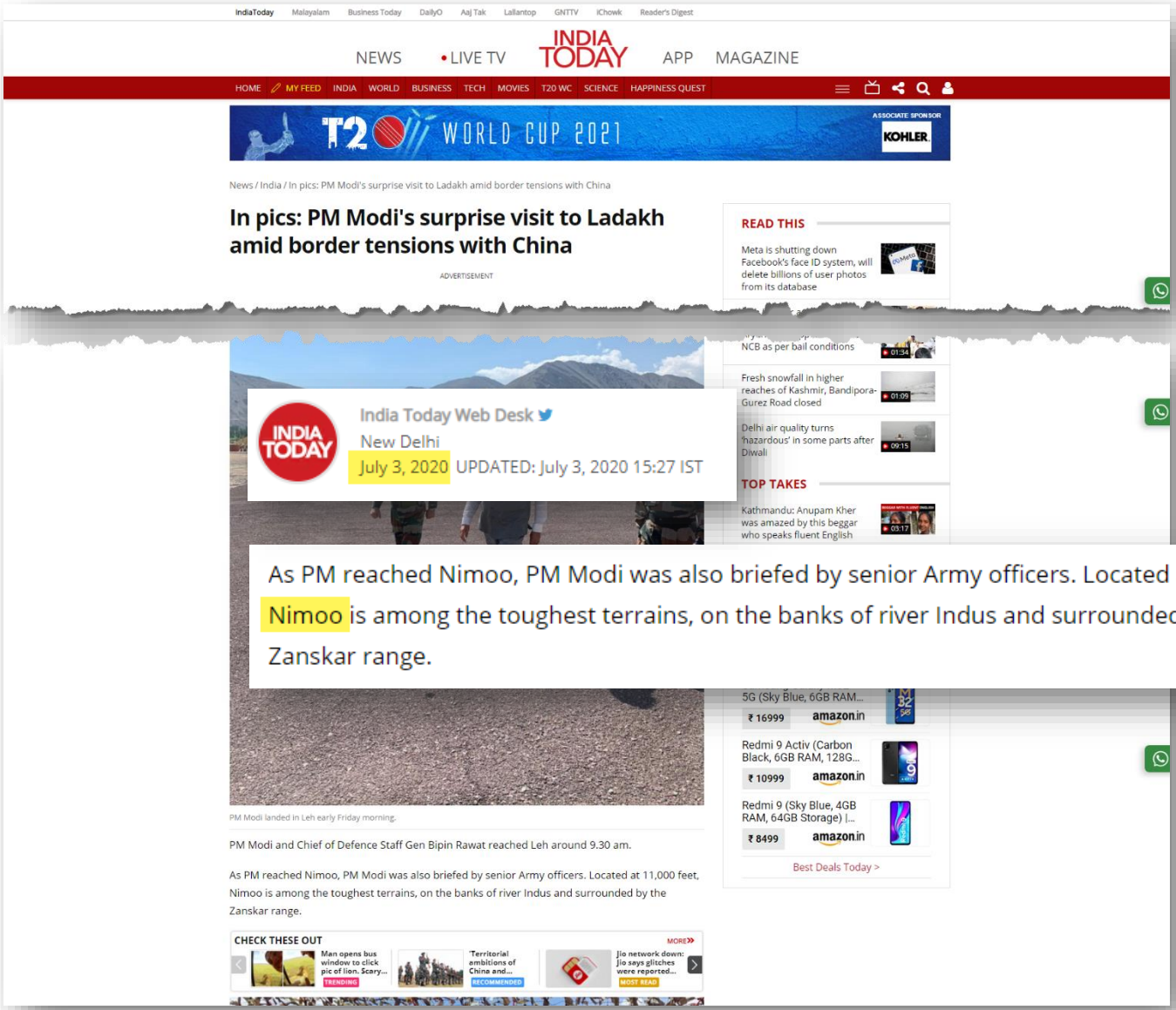






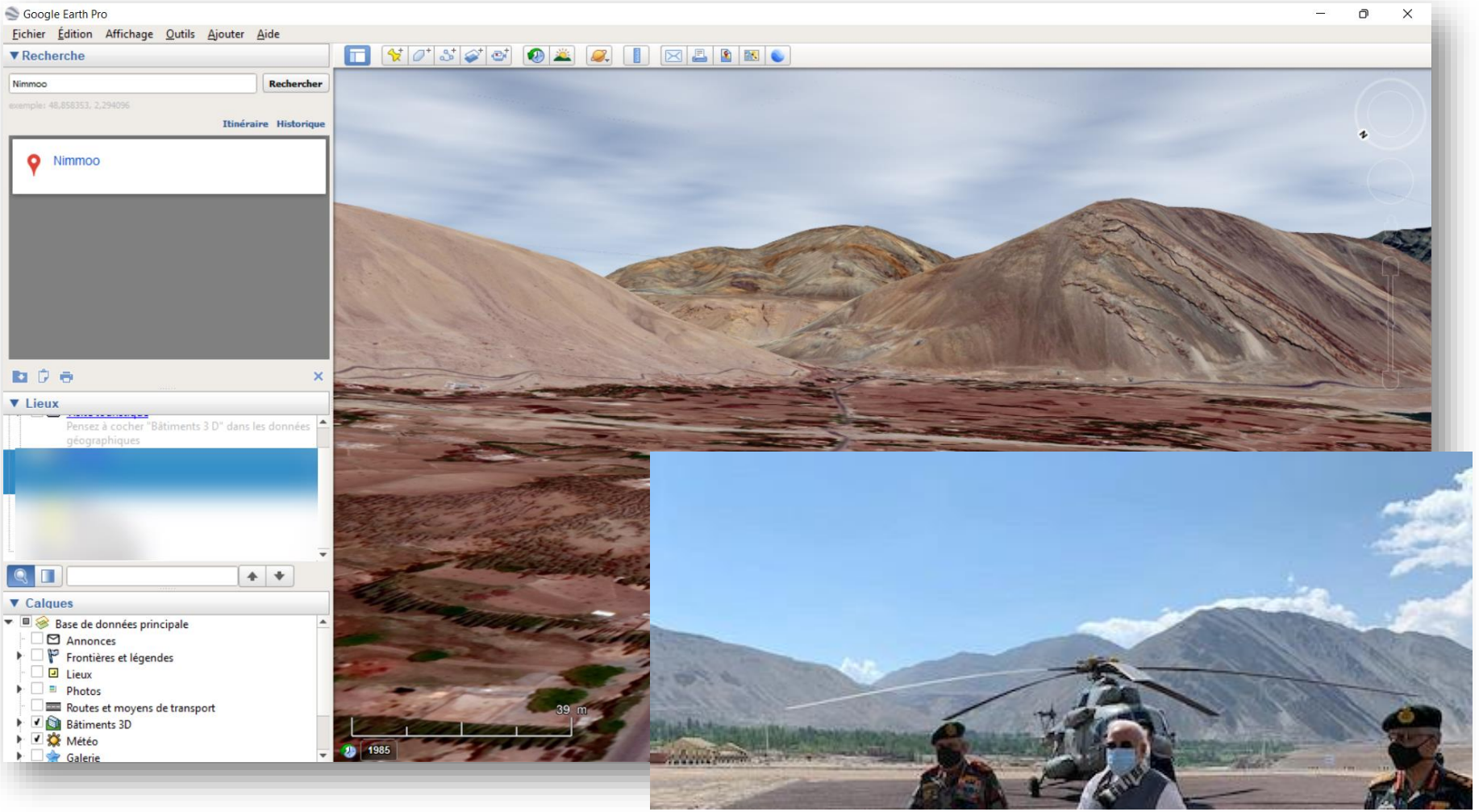


Qui ? Quand ? Où ?

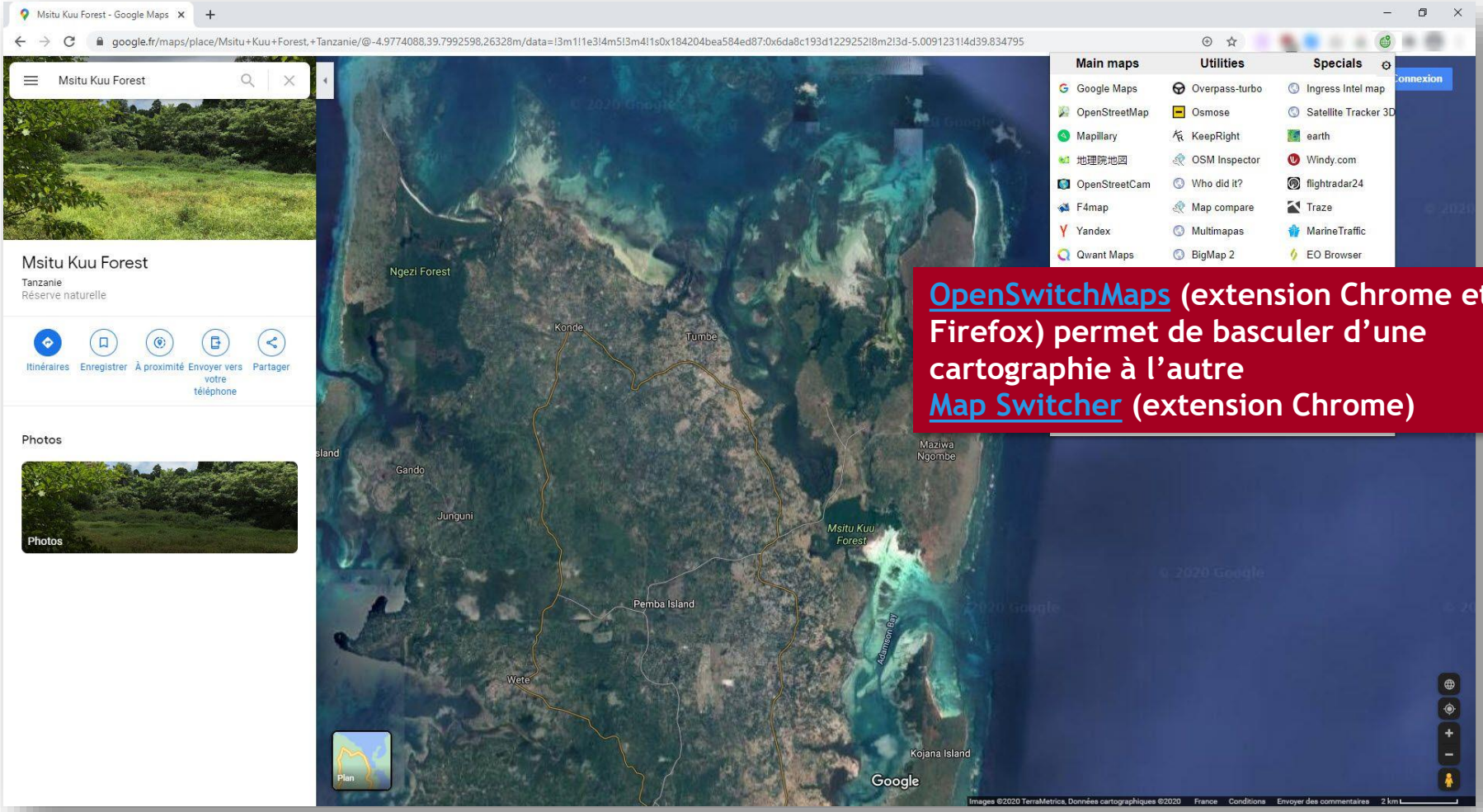

IndiaToday Malayalam Business Today DailyO Aaj Tak Lallantop GNTTV IChowk Reader's Digest
NEWS • LIVE TV INDIA TODAY APP MAGAZINE
HOME MY FEED INDIA WORLD BUSINESS TECH MOVIES T20 WC SCIENCE HAPPINESS QUEST
T20 WORLD CUP 2021
ASSOCIATE SPONSOR KOHLER
News / India / In pics: PM Modi's surprise visit to Ladakh amid border tensions with China
In pics: PM Modi's surprise visit to Ladakh amid border tensions with China
ADVERTISEMENT
READ THIS
Meta is shutting down Facebook's face ID system, will delete billions of user photos from its database
NCB as per bail conditions
Fresh snowfall in higher reaches of Kashmir, Bandipora-Gurez Road closed
Delhi air quality turns 'hazardous' in some parts after Diwali
TOP TAKES
Kathmandu: Anupam Kher was amazed by this beggar who speaks fluent English
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 Zanskar 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 Zanskar range.
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) I... ₹8499 amazon.in
Best Deals Today >
CHECK THESE OUT
MORE
Man opens bus window to click pic of lion. Scary... TRENDING
'Territorial ambitions of China and... RECOMMENDED
Jio network down: Jio says glitches were reported... MOST READ

Localiser

Google Earth Pro, Google Maps



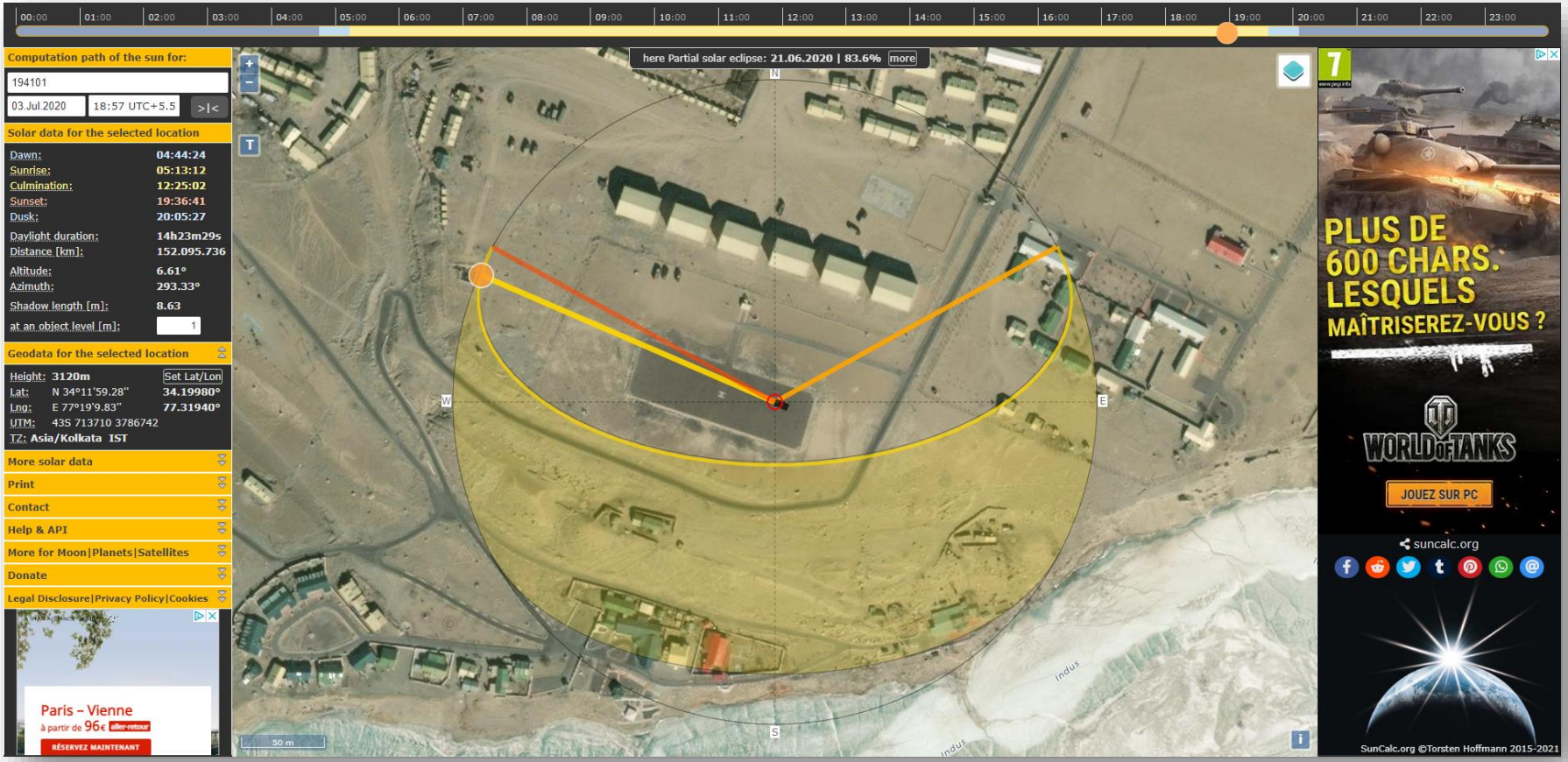
Passer d’une cartographie à l’autre



Horodater en étudiant les ombres

Horodater en étudiant les ombres

Position de Narenda Modi le 3 juillet 2020



Enquêtes satellitaires

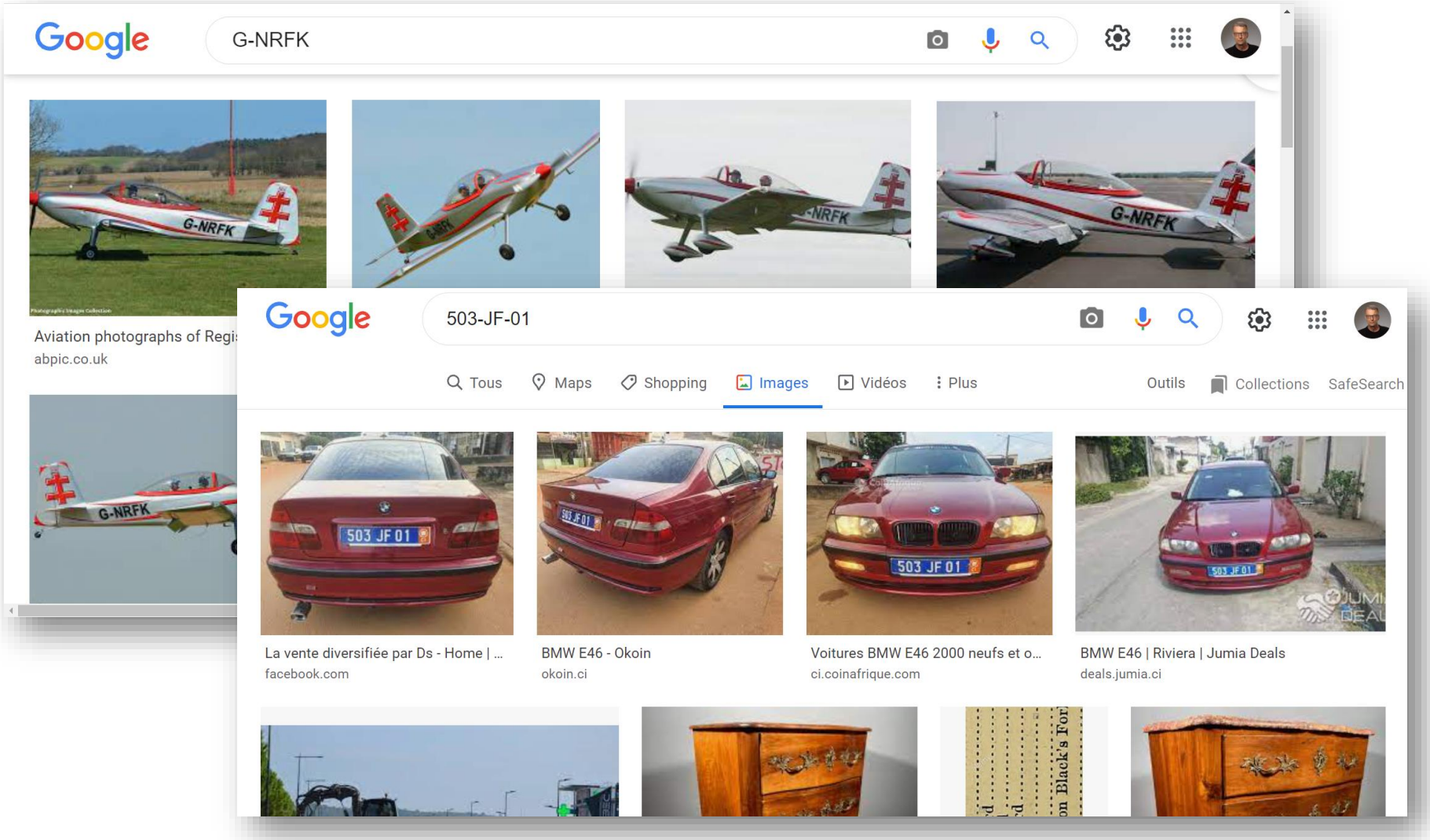
Ocelli Project (base de données sur la destruction de maisons Rohingya en Birmanie, mené notamment par Benjamin Strick).

Voir aussi par exemple les enquêtes géographiques de Forensic Architecture.

Zoom sur l’OCR

(reconnaissance optique de catacères)

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



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

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

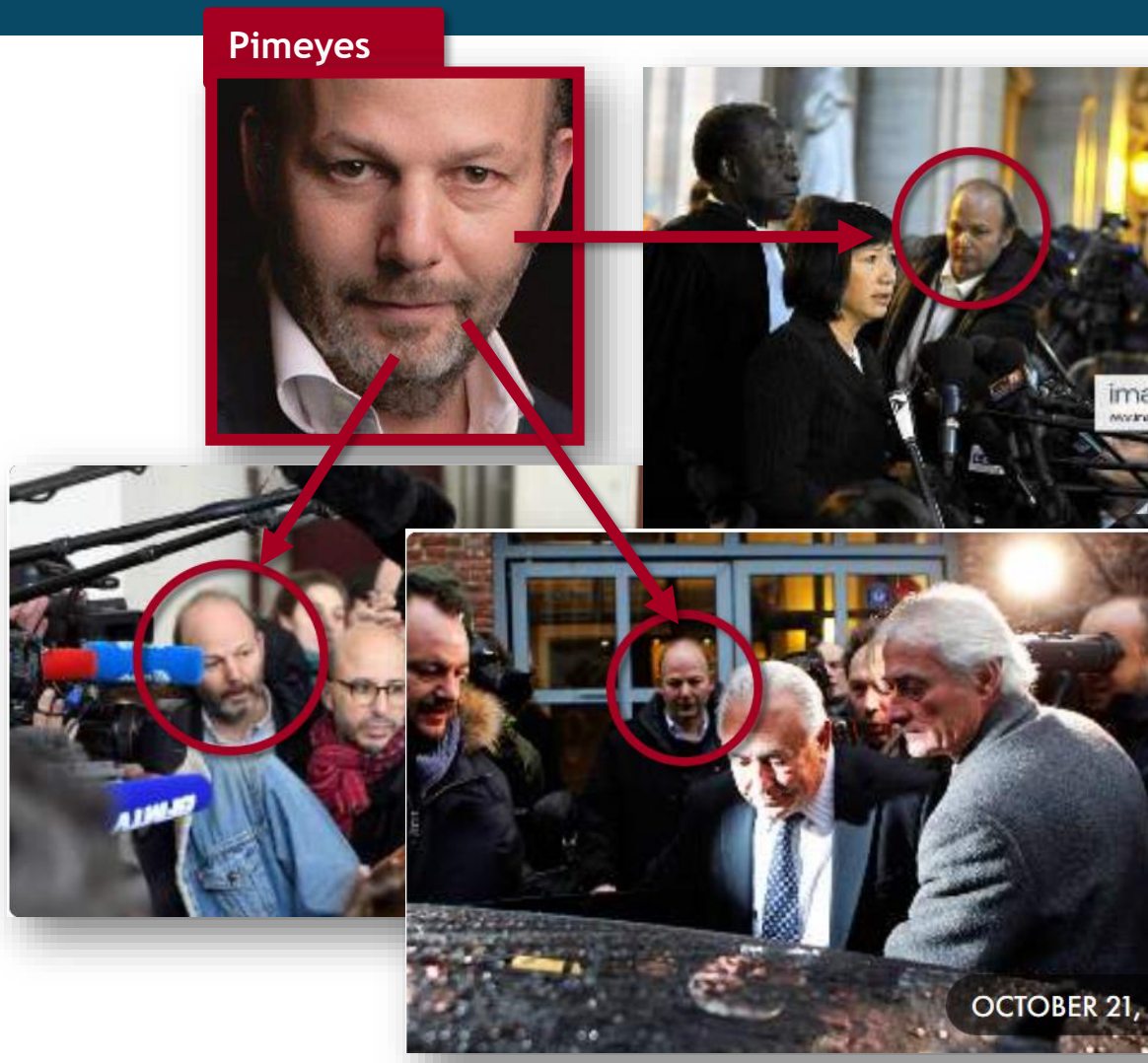
Zoom sur la reconnaissance faciale

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]).
- ► […]



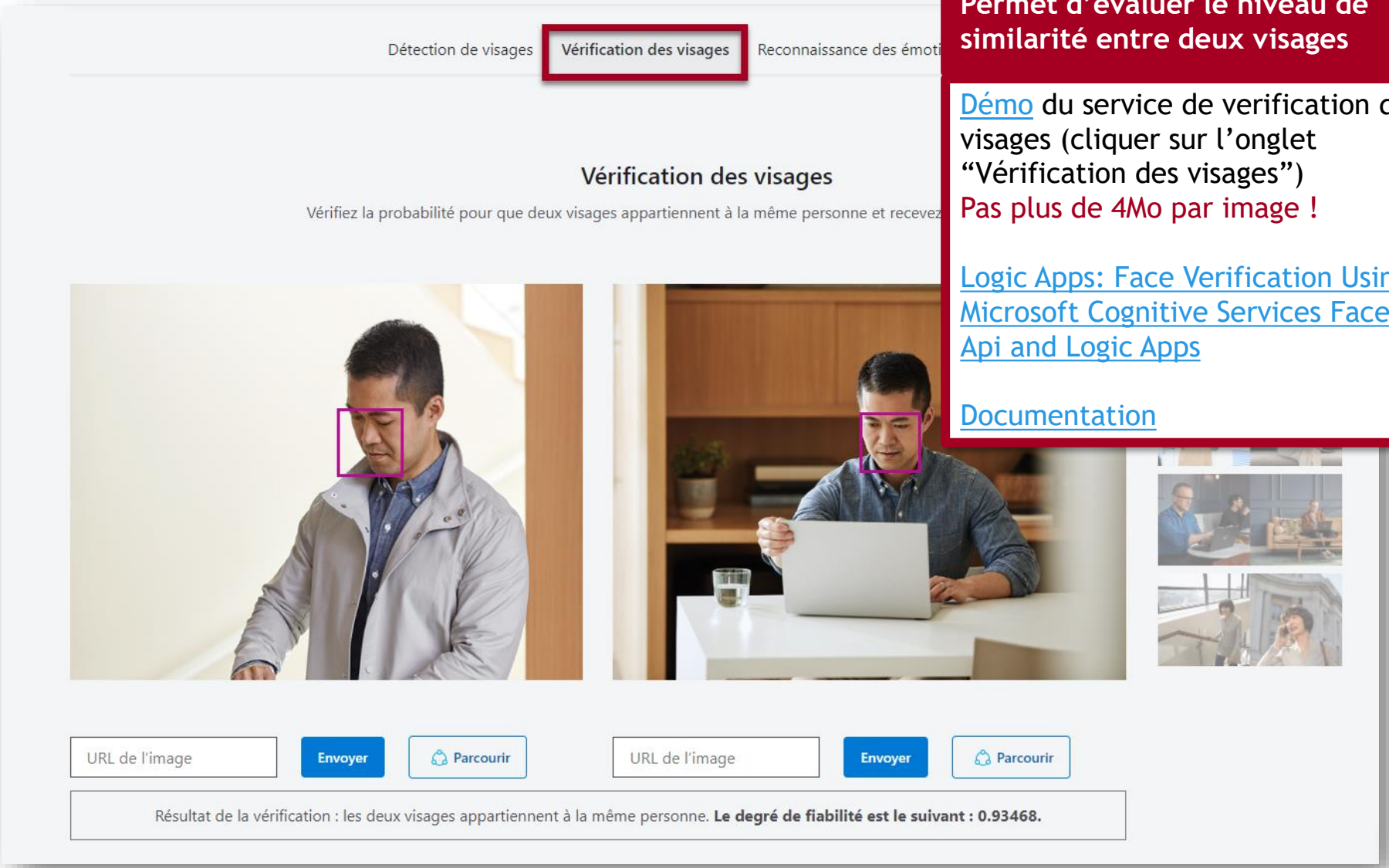
Similarité faciale (Microsoft)

Permet d'évaluer le niveau de similarité entre deux visages

[Démo](#) du service de verification 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](#)

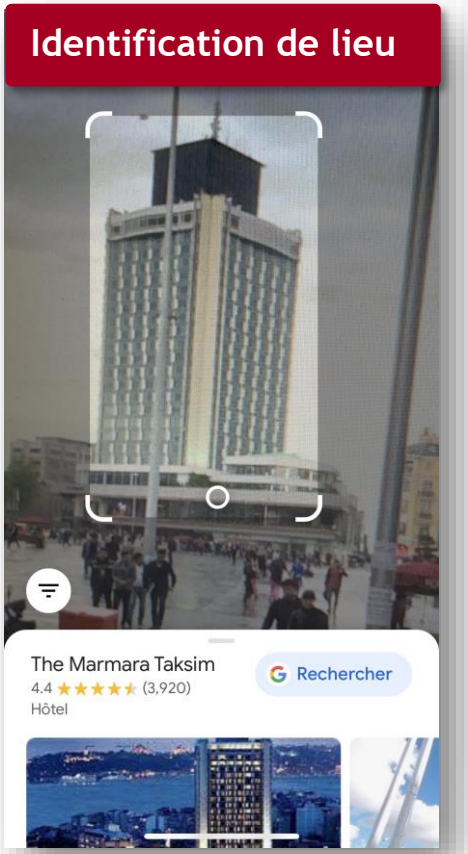


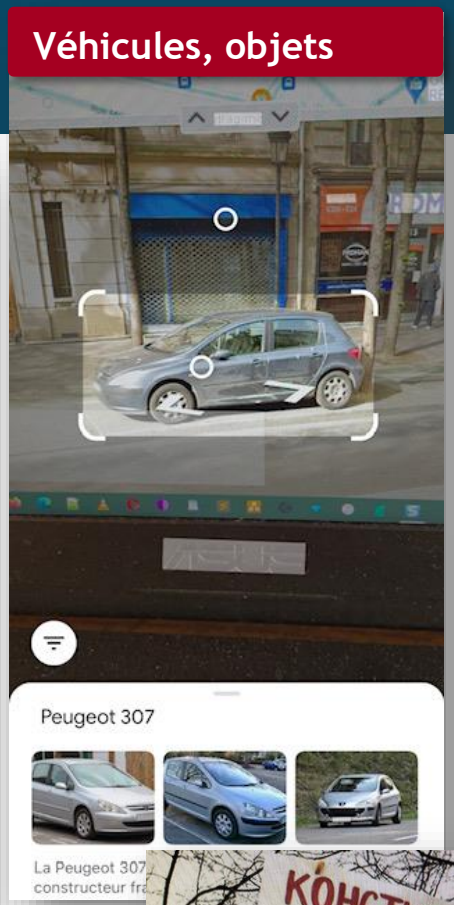
Zoom sur Google Lens

Google Lens

Google Lens
(sur smartphone, mais aussi en ligne)

- ► Indentification d'objets, véhicules, lieux, etc.
- ► Traduction
- ► OCR





Investiguer les médias sociaux (SOCMINT/RRS)

Objectif : maîtrise

OSINT ? Une nécessaire stratégie du petit pas !

Médias sociaux : les grandes familles

Les classiques	Les modernes	Les radicaux	Les messageries
Twitter	Telegram	4chan	WhatsApp
Facebook	Snapchat	8kun	Messenger
YouTube	TikTok	Gab	Signal
Instagram	VKontakte	Gettr	Olvid
Linkedin	Discord	Parler	…
Reddit	Twitch	Poal	
…	…	…	

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"

Requête

"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

Opérateurs orientés médias

filter:images : fichiers images

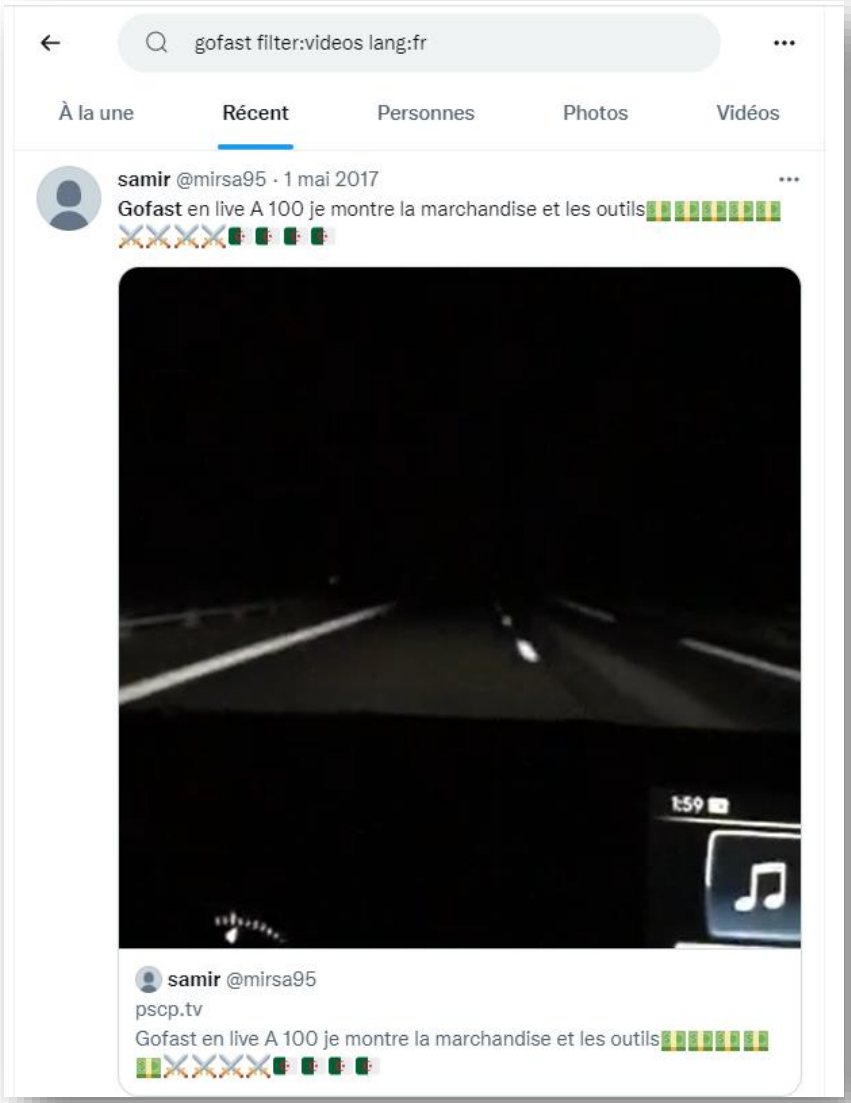
filter:videos : fichiers vidéos (dont partages YouTube…)

filter:media : fichiers images ou vidéos

filter:native_video : fichiers vidéos (sans partages YouTube…)

filter:periscope OR card_domain:pscp.tv OR url:twitter.com/i/broadcasts/ : videos tournées en direct et archivées

- ► manifestation OR manifestant OR manifestants paris OR parisien OR parisiens OR parisienne OR parisiennesfilter:periscope OR card_domain:pscp.tv OR url:twitter.com/i/broadcasts/ lang:fr



Rechercher un tweet à un jour ou à la seconde près

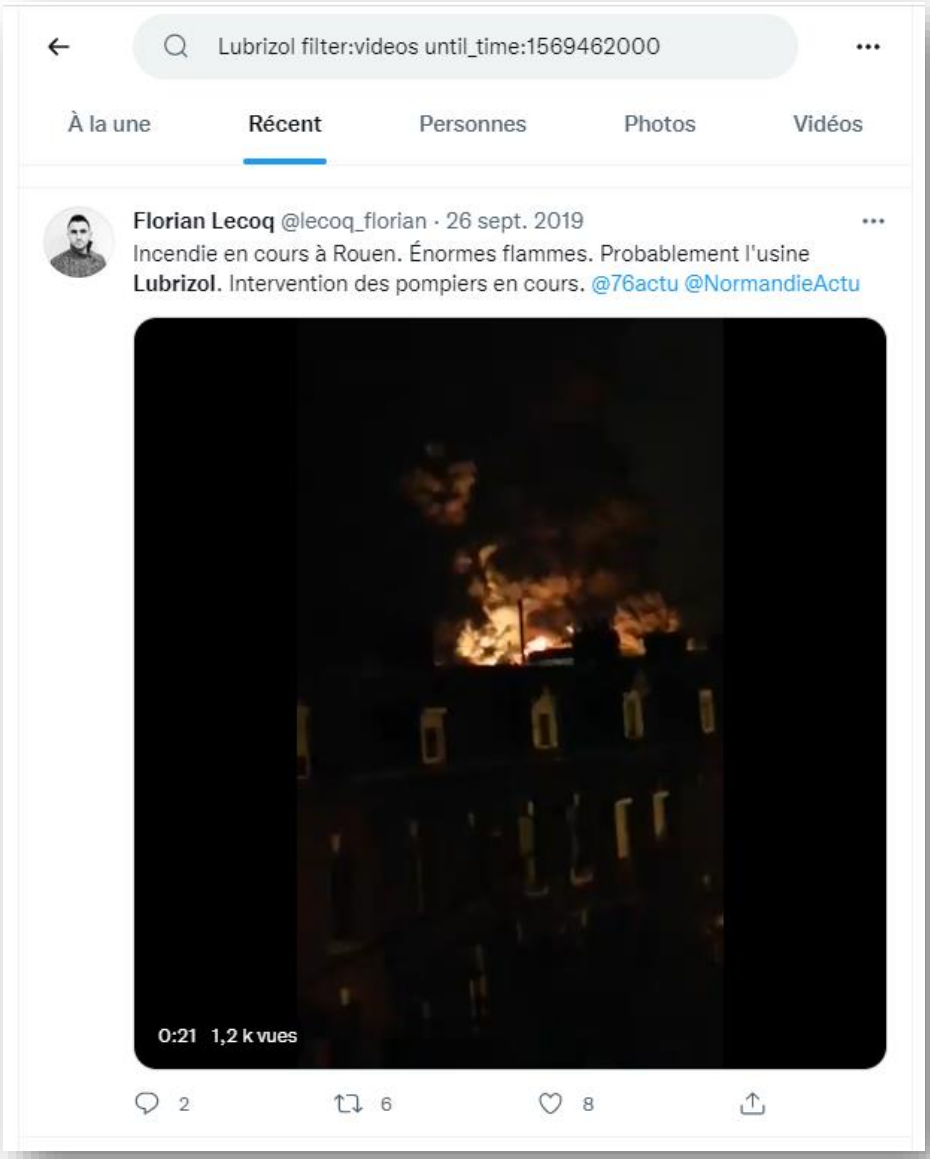
Première vidéo de l'incendie de Lubrizol (26 septembre 2019)

- ►1ère requête envisageable, liée au jour

  Lubrizol filter:videos until:2019-09-27

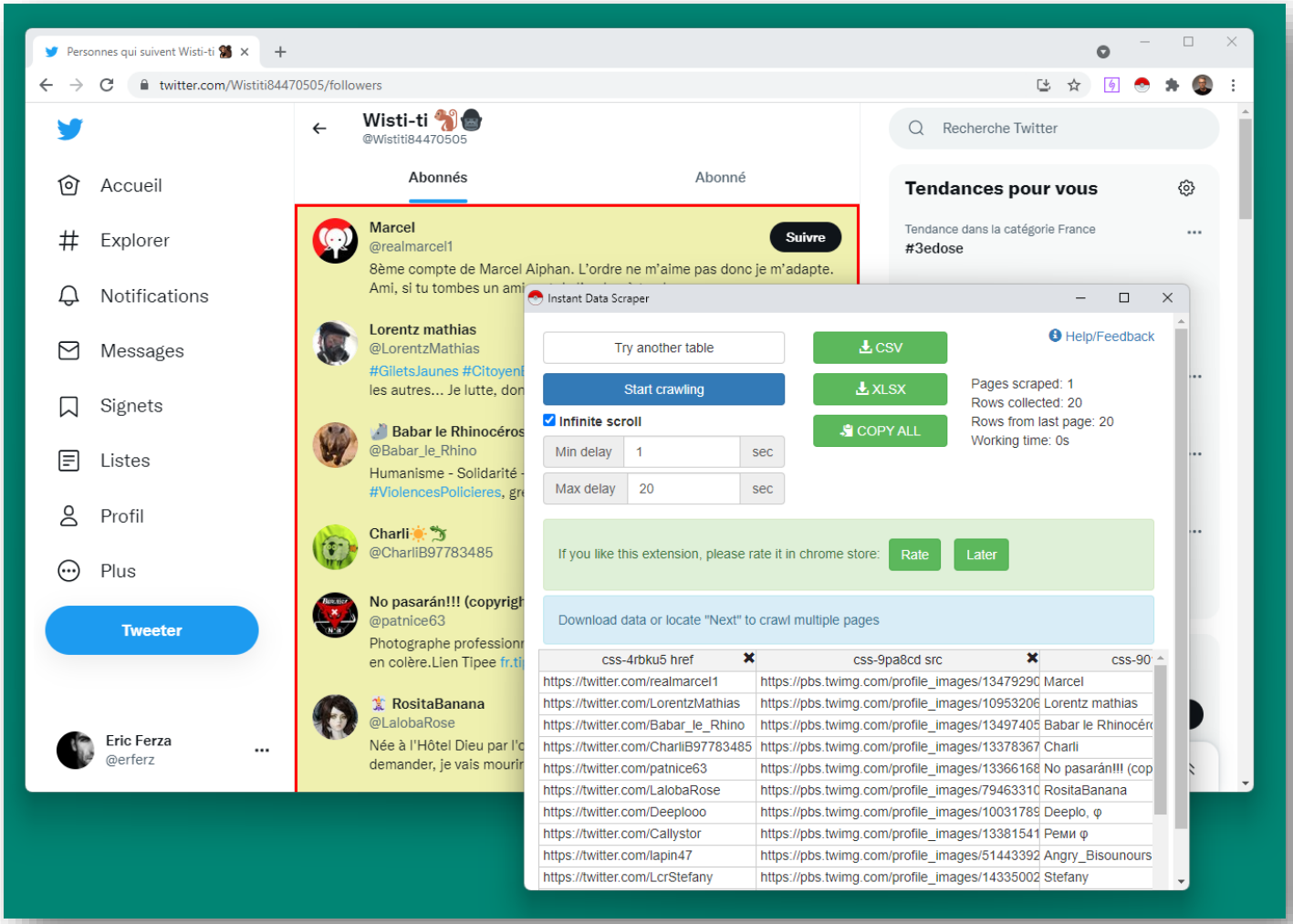
- ►2e requête envisageable, liée à l'heure (déterminée par epochconverter.com)

  Lubrizol filter:videos until_time:1569462000



L’extension utile

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

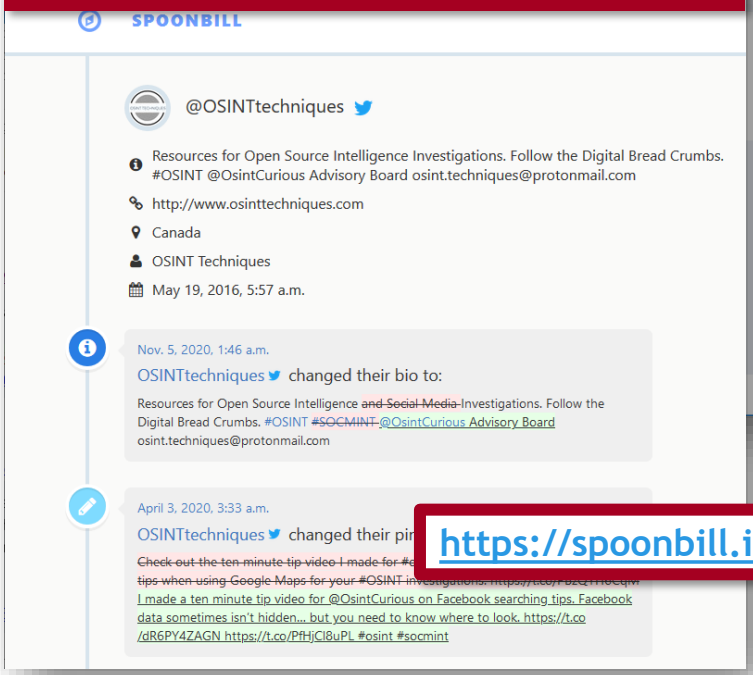


Spoonbill : changements dans les bios

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.

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

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



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

Abonnés ou abonnements communs ?

TweepDiff : par exemple pour comparer les abonnements communs à…

- @ana_anamddk
- @thalassa2008

TweepDiff
Compare Twitter friends and followers

About
Signals Ready
@bdeter

Do Another Comparison

Common (473) | thalassa2008 following (7005) | ana_anamddk following (1772)
Names | Images | Details | Per Page: 50

1 2 3 4 5 6 7 8 Next

People that are followed by thalassa2008 and ana_anamddk
Click the name to see more details about a tweep...

BEZOMBES Jean-Michel (bezombes_jm)
lynns (lynns68gwada971)
Papanours (papanours60)
alain brugerie (brugerie)
✴ This Is Sparta ✴ (_ThisIsSparta_)
RoOsTer (RoosterV4)
Pinsolle Typhaine (PinsolleT)
LE GÉNÉRAL 0fficiel © (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 Chanelle (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)
Festé (Steco94)

Analyse de graphe

(analyser les relations entre des acteurs)

NodeXL

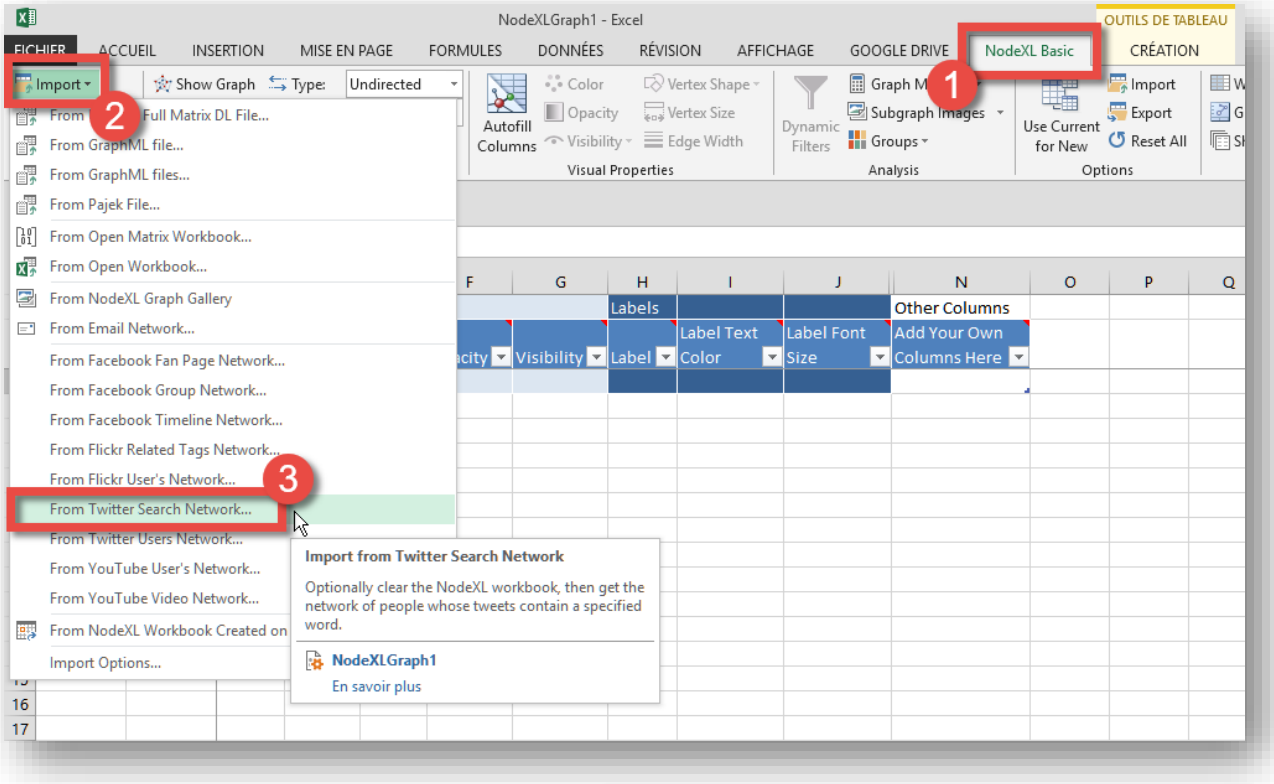
NodeXL est un modèle Excel (compatible Windows à partir d'Excel 2010).

Il ajoute un onglet à Excel.

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

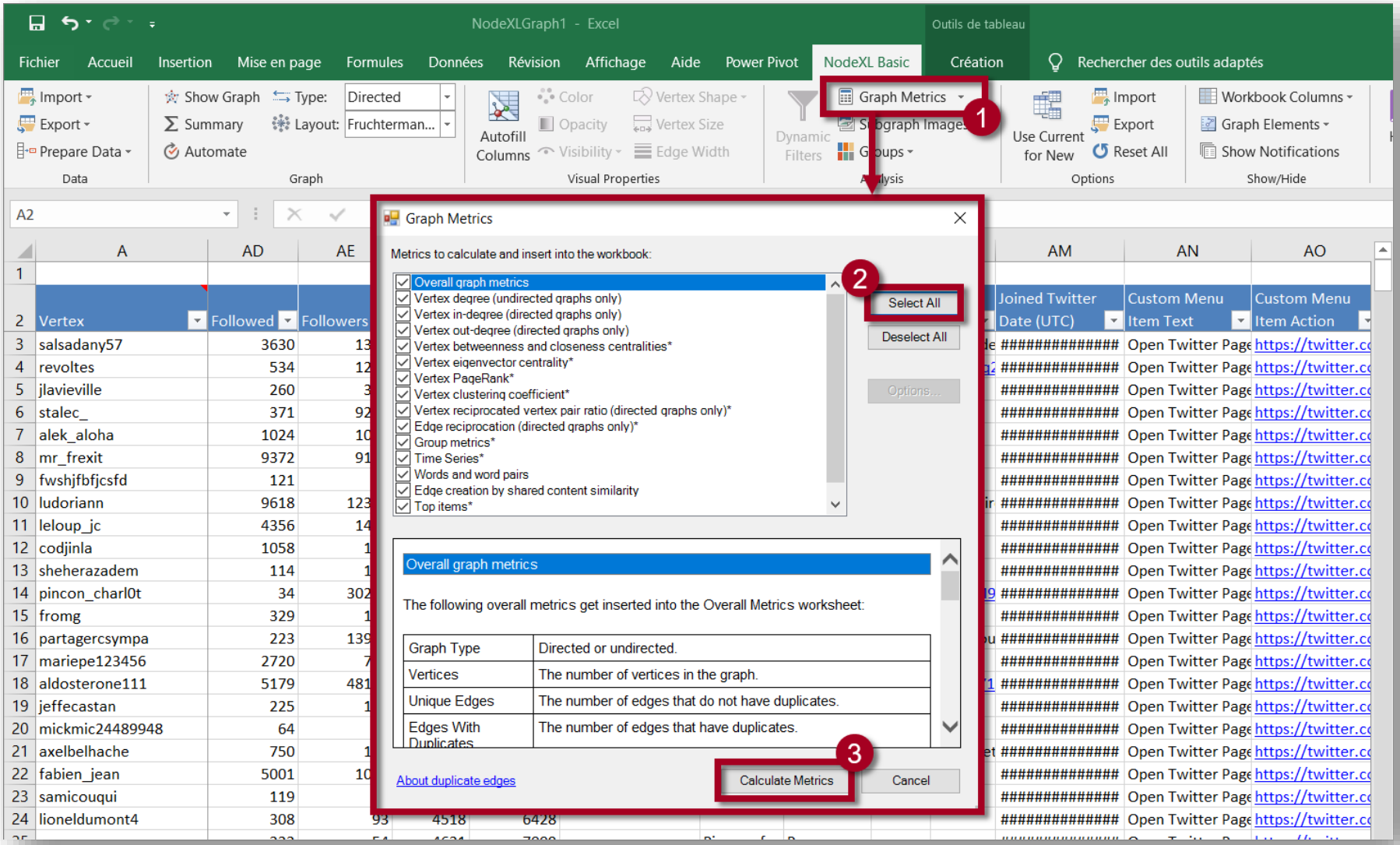
Vous devrez connecter votre compte Twitter à NodeXL pour qu'il puisse interroger Twitter.

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

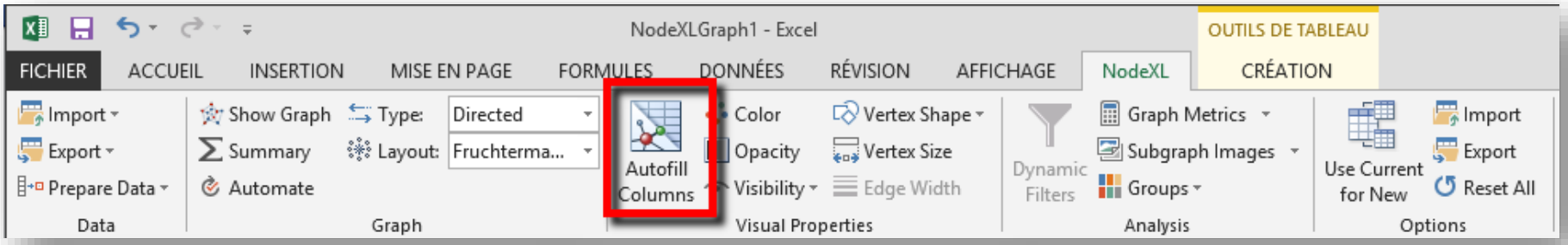


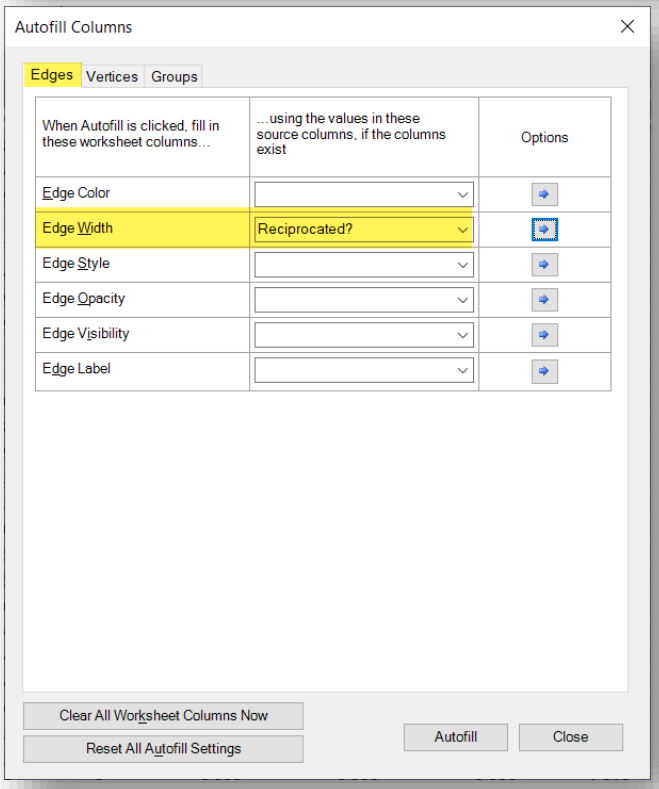
Ici, analyse de #holdup lang:fr

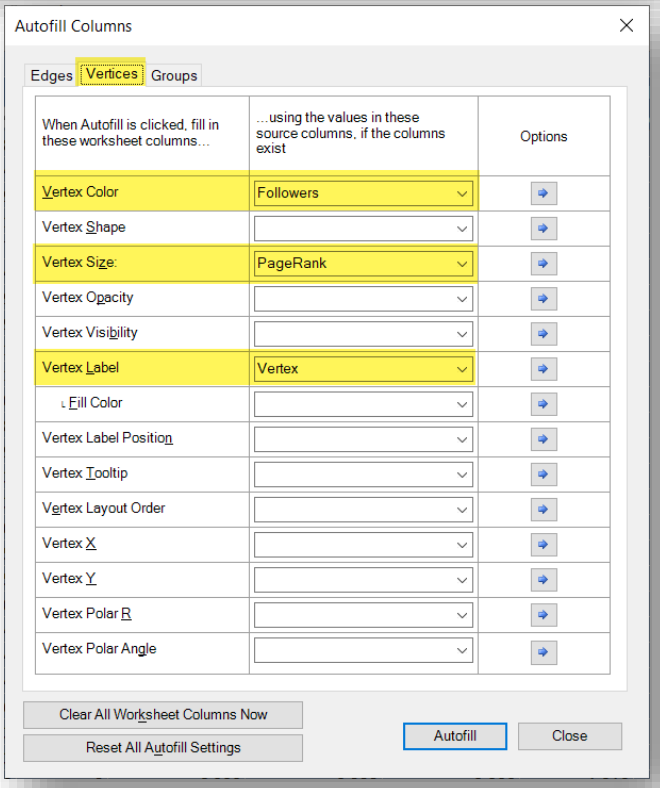
NodeXL


NodeXLGraph1 - Excel
Outils de tableau
Fichier
Accueil
Insertion
Mise en page
Formules
Données
Révision
Affichage
Aide
Power Pivot
NodeXL Basic
Création
Rechercher des outils adaptés
Import
Export
Prepare Data
Data
Show Graph
Summary
Automate
Type:
Directed
Layout:
Fruchterman...
Graph
Autofill Columns
Color
Opacity
Visibility
Vertex Shape
Vertex Size
Edge Width
Visual Properties
Dynamic Filters
Graph Metrics
Groups
1
Use Current for New
Import
Export
Reset All
Options
Workbook Columns
Graph Elements
Show Notifications
Show/Hide
A2
Graph Metrics
Metrics 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*
2
Select All
Deselect All
Options...
Overall graph metrics
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
3
Calculate Metrics
Cancel
Vertex
Followed
Followers
Joined Twitter Date (UTC)
Custom Menu Item Text
Custom Menu Item Action
salsadany57 3630
revoltes 534
jlavieville 260
stalec_ 371
alek_aloha 1024
mr_frexit 9372
fwshjfbfjcsfd 121
ludoriann 9618
leloup_jc 4356
codjinla 1058
sheherazadem 114
pincon_charl0t 34
fromg 329
partagercsympa 223
mariepe123456 2720
aldosterone111 5179
jeffecastan 225
mickmic24489948 64
axelbelhache 750
fabien_jean 5001
samicouqui 119
lioneldumont4 308
Open Twitter Page
https://twitter.co

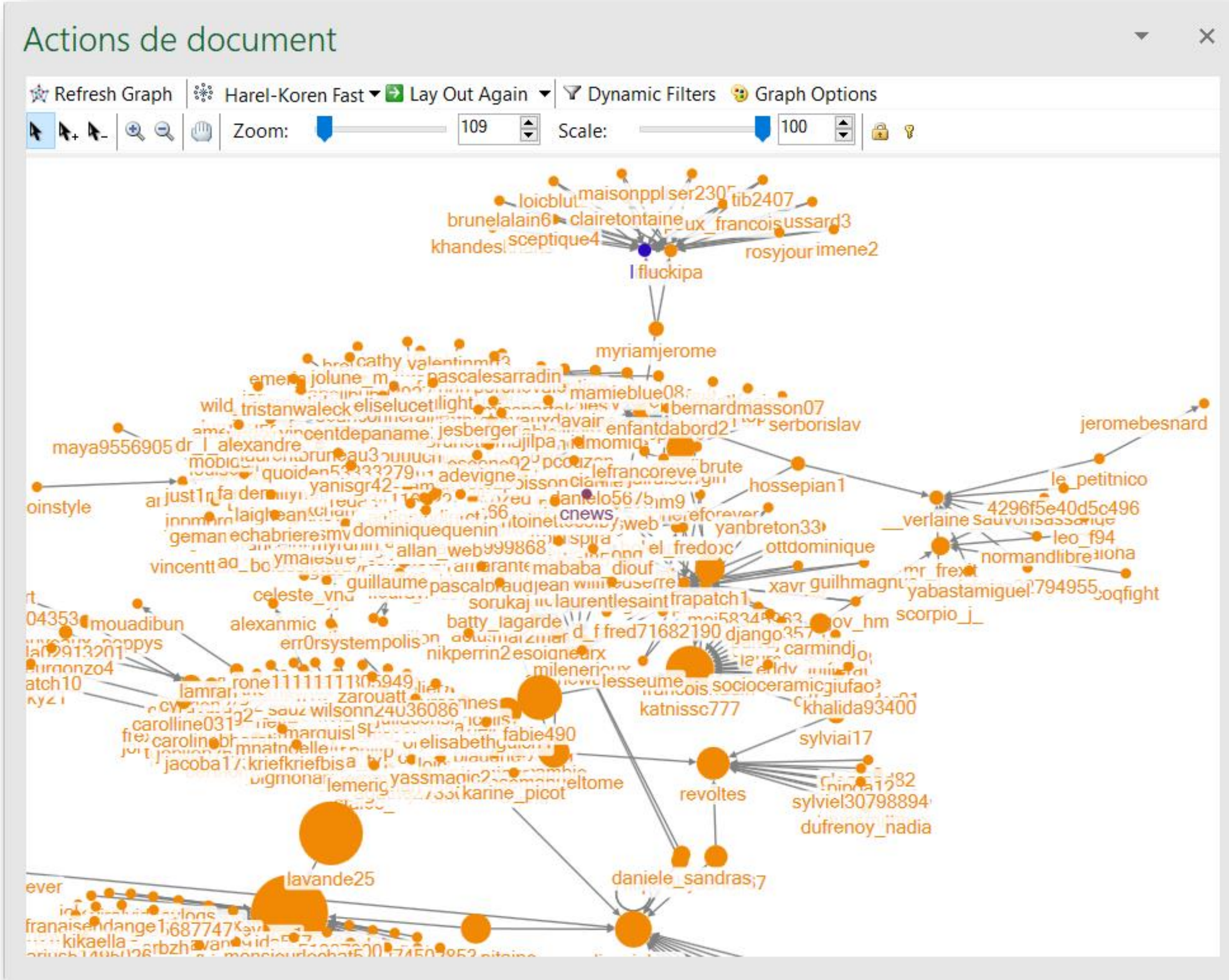
NodeXL


NodeXLGraph1 - Excel
OUTILS DE TABLEAU
FICHIER
ACCUEIL
INSERTION
MISE EN PAGE
FORMULES
DONNÉES
RÉVISION
AFFICHAGE
NodeXL
CRÉATION
Import
Export
Prepare Data
Data
Show Graph
Summary
Automate
Type:
Directed
Layout:
Fruchterma...
Graph
Autofill Columns
Color
Opacity
Visibility
Vertex Shape
Vertex Size
Edge Width
Visual Properties
Dynamic Filters
Graph Metrics
Subgraph Images
Groups
Analysis
Use Current for New
Import
Export
Reset All
Options


Autofill Columns
Edges
Vertices
Groups
When Autofill is clicked, fill in these worksheet columns...
...using the values in these source columns, if the columns exist
Options
Edge Color
Edge Width
Reciprocated?
Edge Style
Edge Opacity
Edge Visibility
Edge Label
Clear All Worksheet Columns Now
Reset All Autofill Settings
Autofill
Close

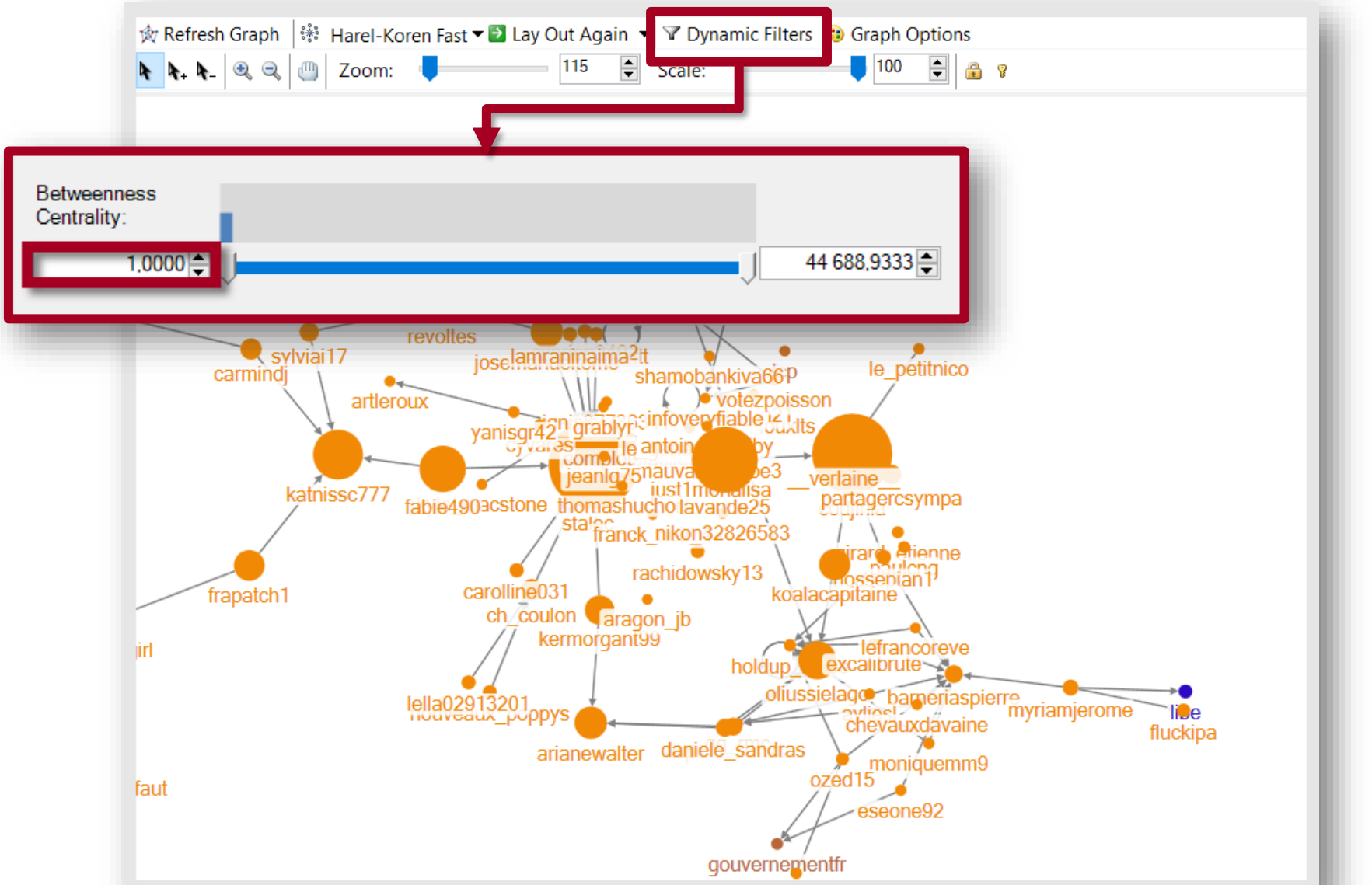

Autofill Columns
Edges
Vertices
Groups
When Autofill is clicked, fill in these worksheet columns...
...using the values in these source columns, if the columns exist
Options
Vertex Color
Followers
Vertex Shape
Vertex Size
PageRank
Vertex Opacity
Vertex Visibility
Vertex Label
Vertex
Fill Color
Vertex Label Position
Vertex Tooltip
Vertex Layout Order
Vertex X
Vertex Y
Vertex Polar R
Vertex Polar Angle
Clear All Worksheet Columns Now
Reset All Autofill Settings
Autofill
Close

NodeXL

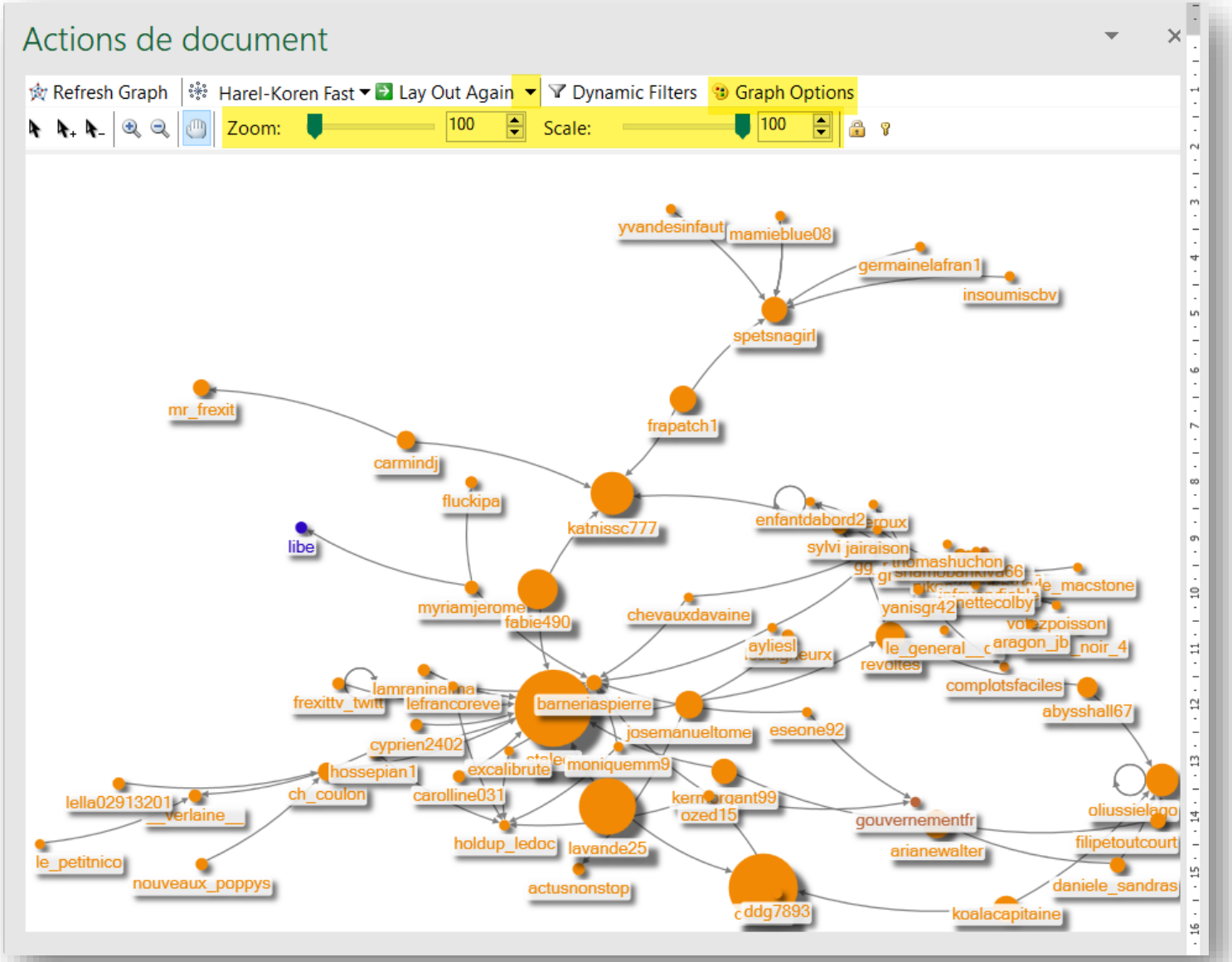


Actions de document
Refresh Graph
Harel-Koren Fast
Lay Out Again
Dynamic Filters
Graph Options
Zoom:
109
Scale:
100
fluckipa
myriamjerome
jeromebesnard
cnews
revoltes
lavande25
hossepian1
sylviai17
dufrenoy_nadia
katnissc777
khalida93400

NodeXL


Refresh Graph
Harel-Koren Fast
Lay Out Again
Dynamic Filters
Graph Options
Zoom:
115
Scale:
100
Betweenness Centrality:
1,0000
44 688,9333
revoltes
sylviai17
carmindj
artleroux
shamobankiva66
votezpoisson
le_petitnico
yanisgr42
grablyr
infoveryfiable
verlaine
partagercsympa
katnissc777
fabie490
thomashucho
lavande25
franck_nikon32826583
rachidowsky13
frapatch1
carolline031
ch_coulon
aragon_jb
kermorgant99
koalacapitaine
lefrancoreve
holdup
excalibrute
lella02913201
arianewalter
daniele_sandras
chevauxdavaine
myriamjerome
fluckipa
moniquemm9
ozed15
eseone92
gouvernementfr
faut

NodeXL

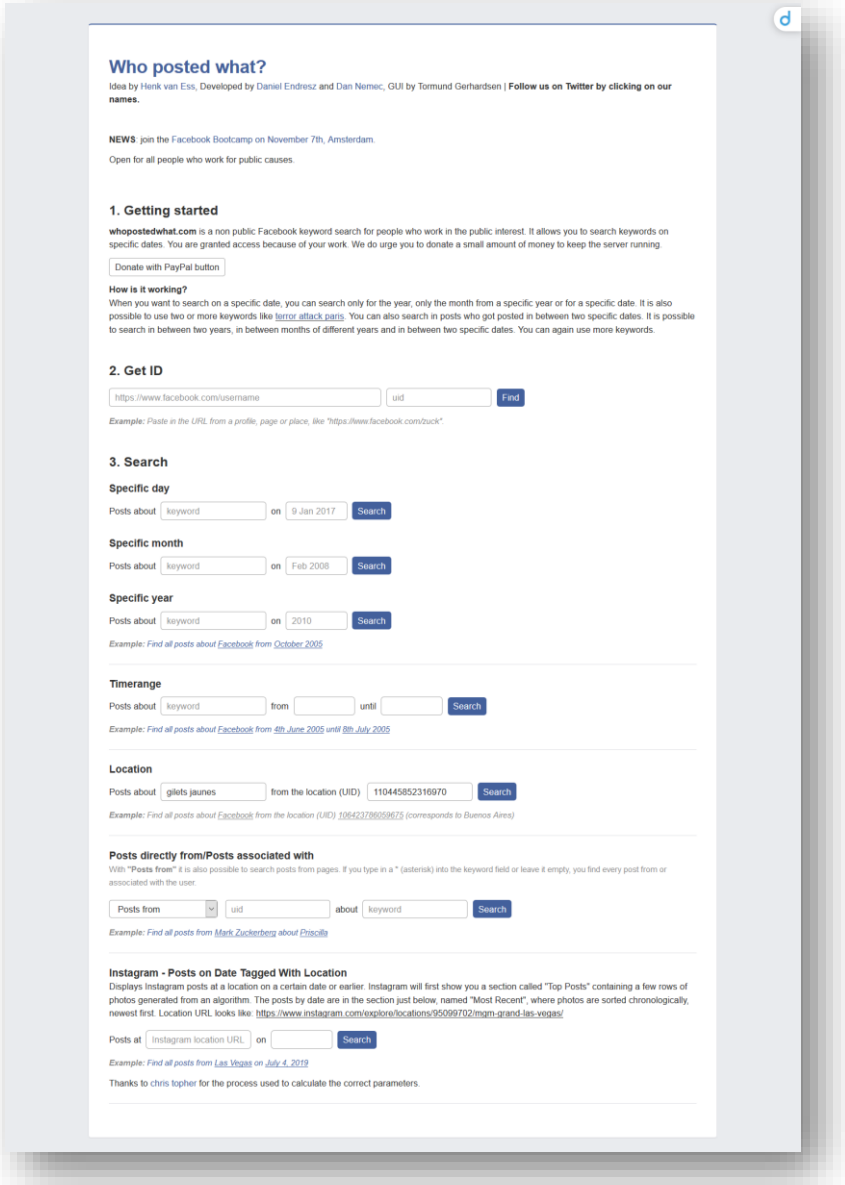

Actions de document
Refresh Graph
Harel-Koren Fast
Lay Out Again
Dynamic Filters
Graph Options
Zoom:
100
Scale:
100
yvandesinfaut
mamieblue08
germainelafran1
insoumiscbv
spetsnagirl
mr_frexit
frapatch1
carmindj
fluckipa
katnissc777
libe
enfantdabord2
sylvi
jairaison
thomashuchon
yanisgr42
nettecolby
myriamjerome
fabie490
chevauxdavaine
aylies
le_general
aragon_jb
noir_4
revoltes
complotsfaciles
abysshall67
frexittv_twitt
lefrancoreve
barneriaspierre
josemanueltome
eseone92
cyprien2402
hossepian1
excalibrute
moniquemm9
lella02913201
verlaine__
ch_coulon
carolline031
ozed15
gouvernementfr
oliussielago
arianewalter
filipetoutcourt
holdup_ledoc
lavande25
le_petitnico
nouveaux_poppys
actusnonstop
ddg7893
daniele_sandras
koalacapitaine

Facebook

Recherches précises sur une date ou une période ?

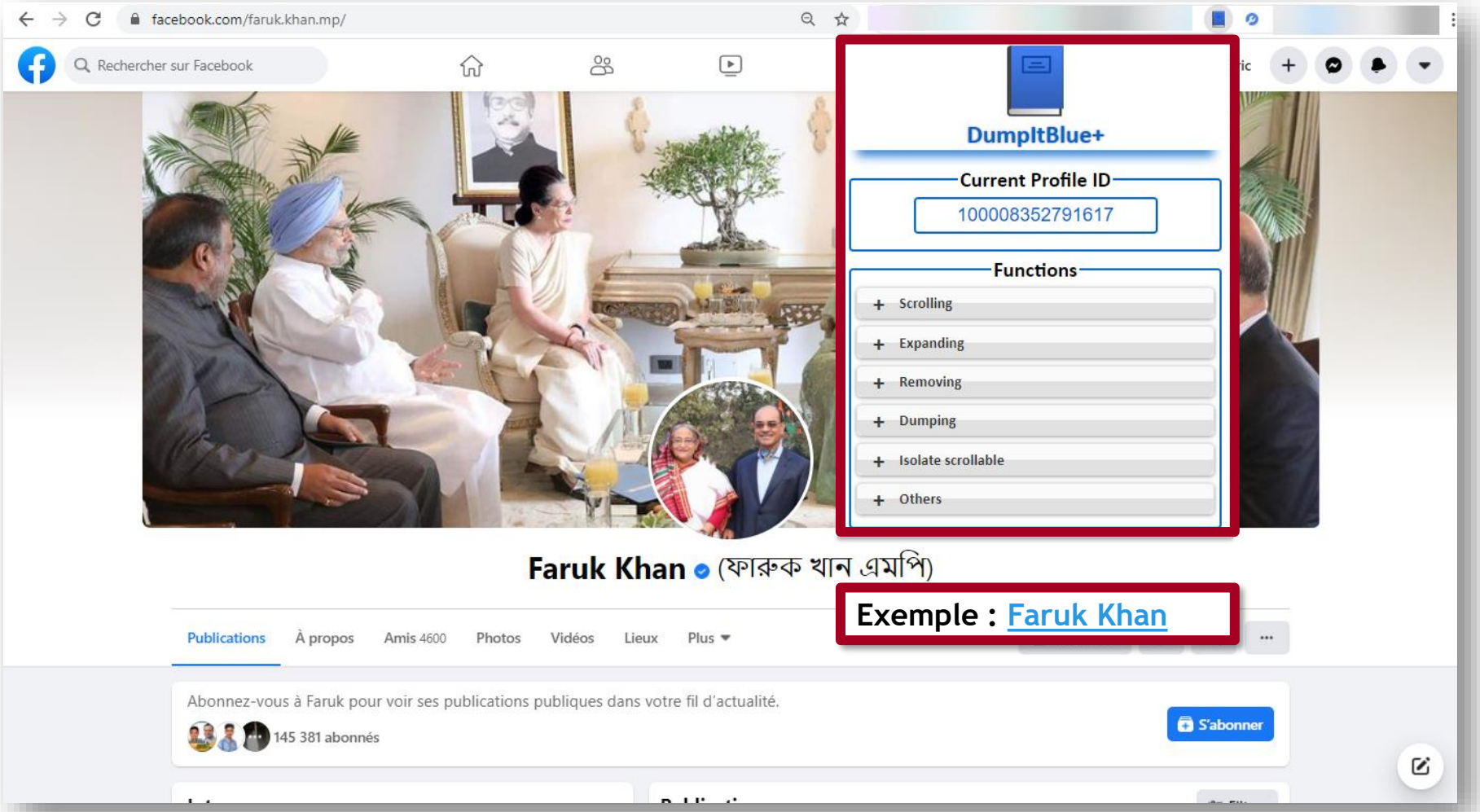
Who posted what ?

- ►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 connaitre 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



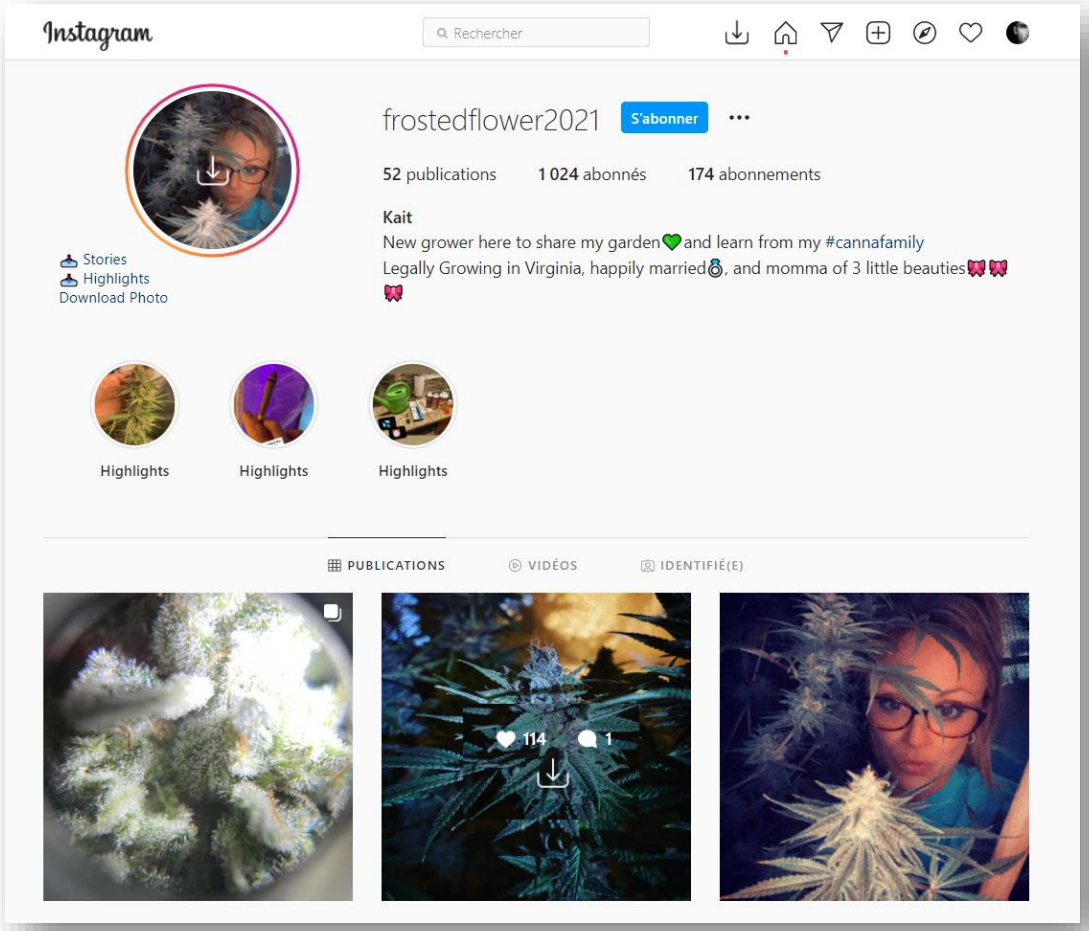
Instagram

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

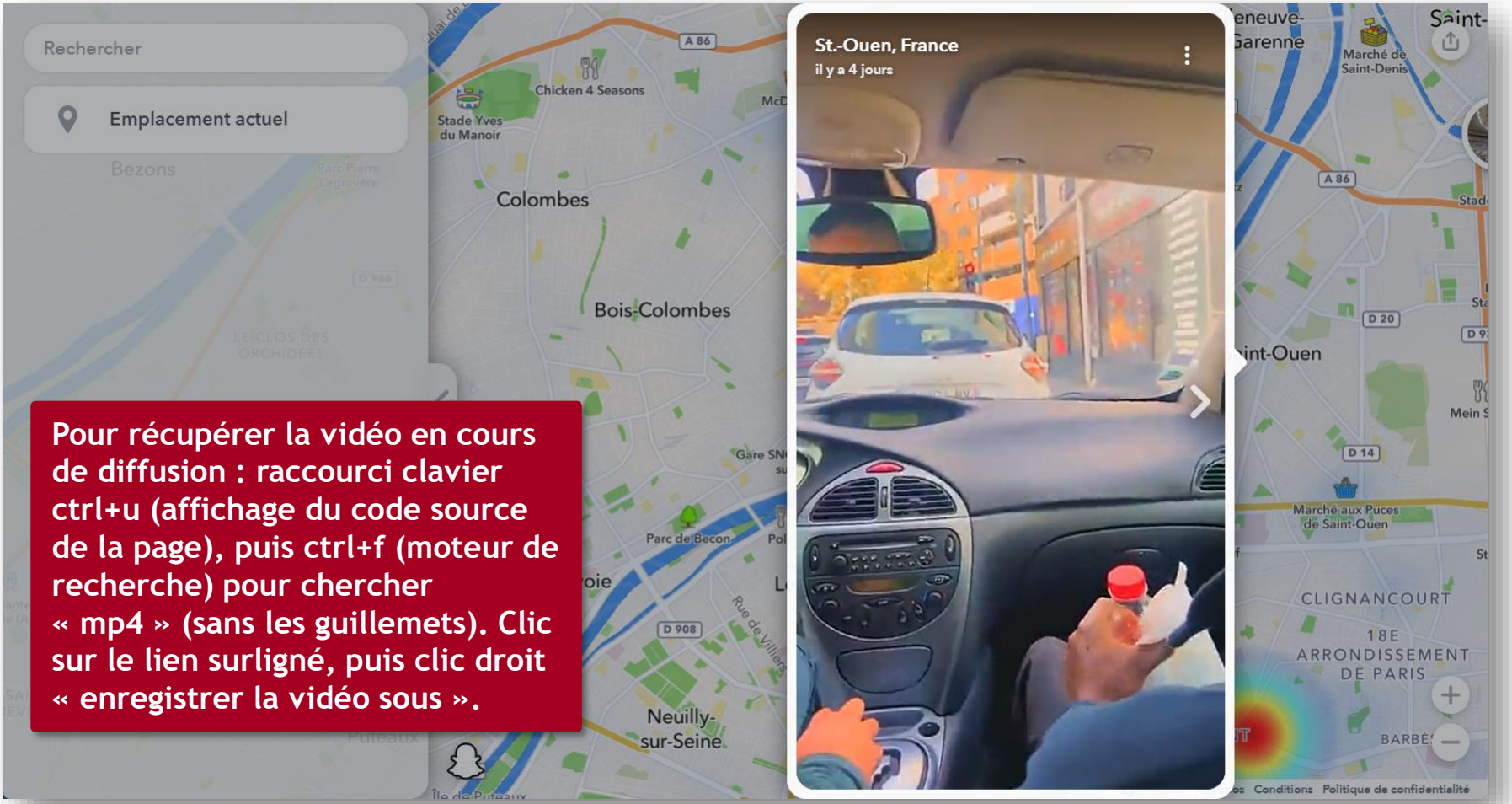


Snapchat

Application très utilisée par des préados, ados et jeunes adultes

Visualiser et télécharger des stories géolocalisées

Snapmap : stories géolocalisées

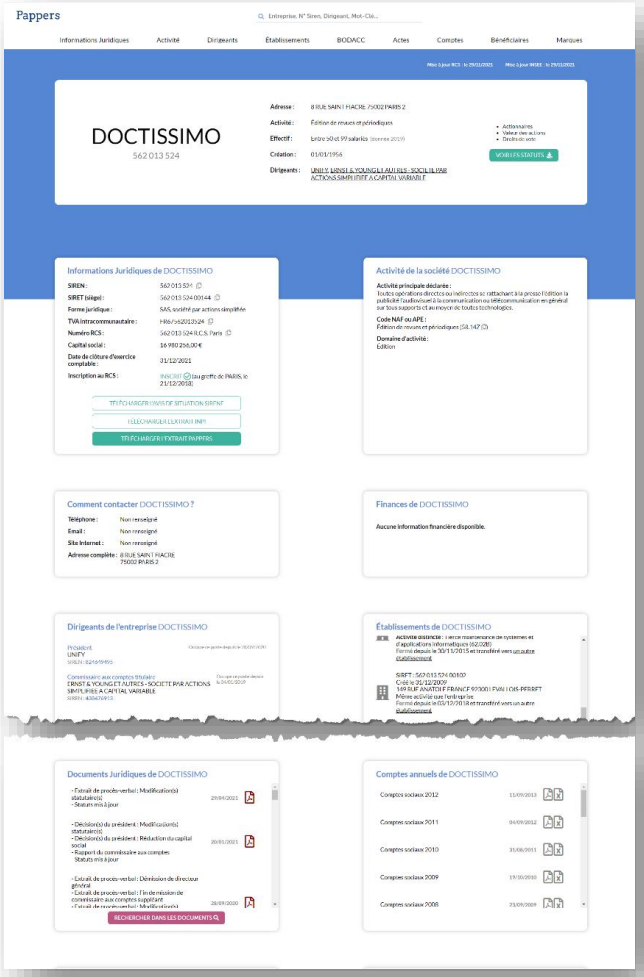


FININT

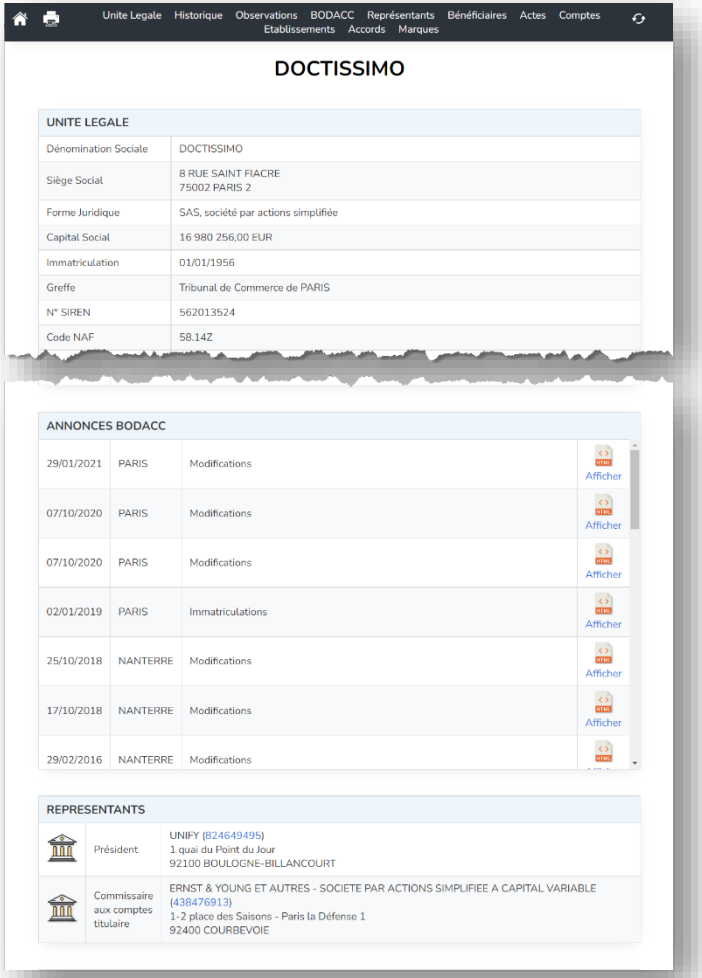
L’investigation financière

Ouverture de la base Sirene

Pappers

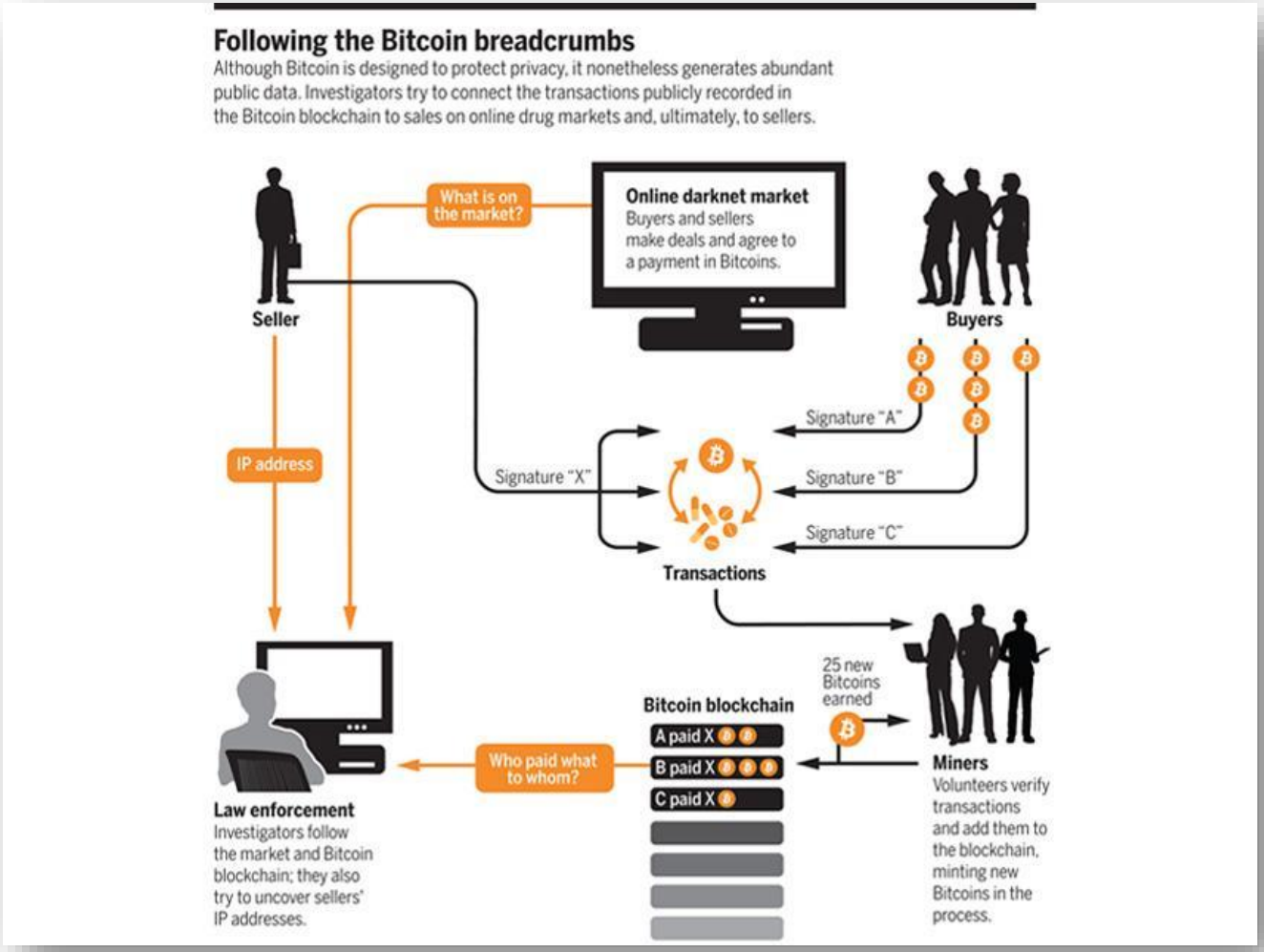


Societe.ninja



Follow the Money

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



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)

Etude de cas

Accumuler les indices sur marquechere.fr

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)

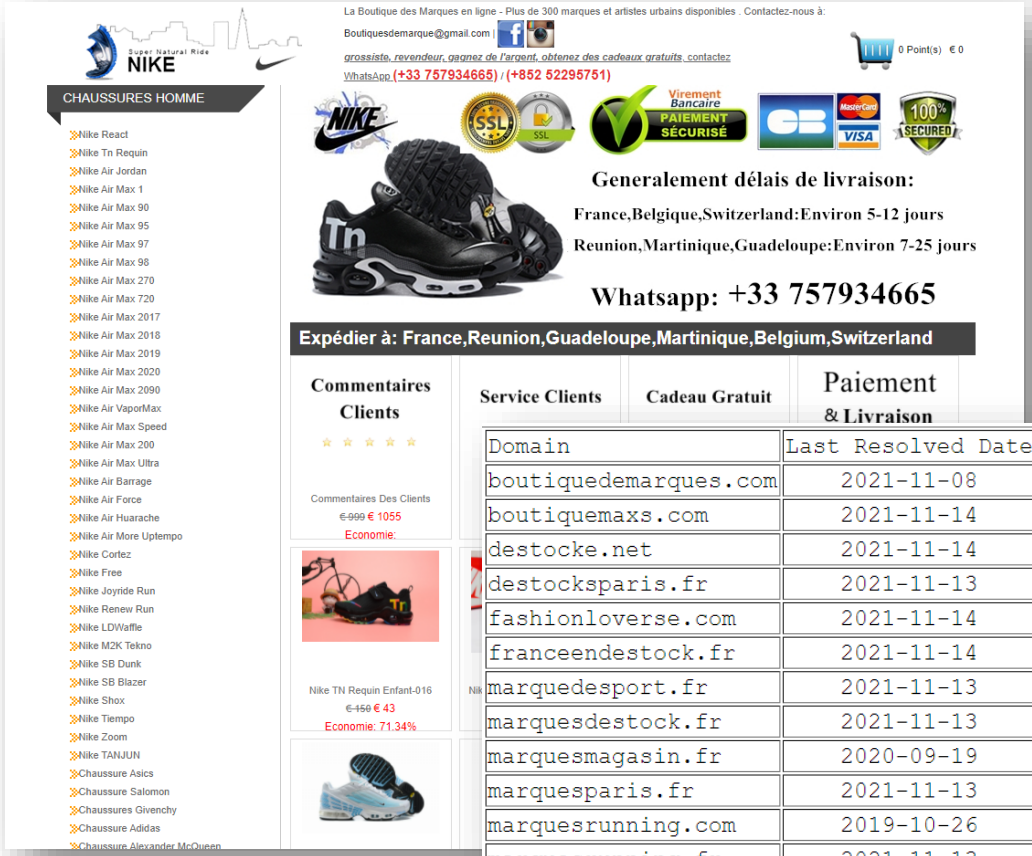
► IPinfo

Astuce : investiguer les IP proches

► InfoByIp : exemple des IP proches

- Reverse IP de 94.130.80.125 (par ViewDNS)

URLscan



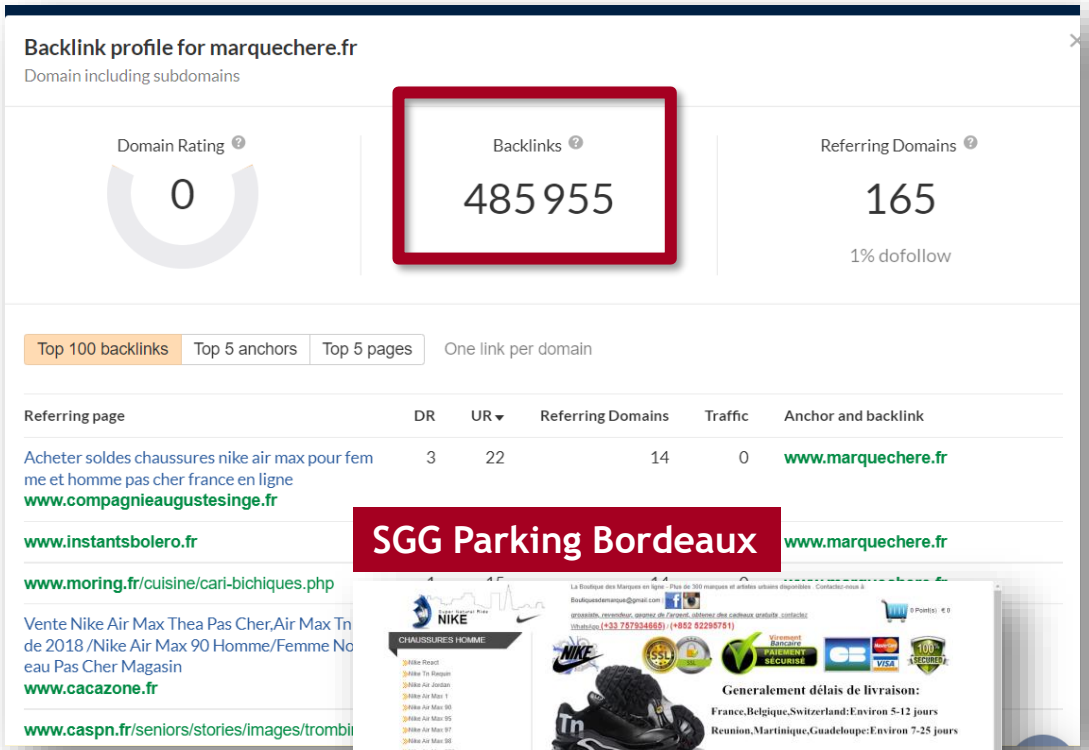
Domain	Last Resolved Date
boutiquedemarques.com	2021-11-08
boutiquemaxs.com	2021-11-14
destocke.net	2021-11-14
destocksparis.fr	2021-11-13
fashionloverse.com	2021-11-14
franceendestock.fr	2021-11-14
marquedesport.fr	2021-11-13
marquesdestock.fr	2021-11-13
marquesmagasin.fr	2020-09-19
marquesparis.fr	2021-11-13
marquesrunning.com	2019-10-26
marquesrunning.fr	2021-11-13
soldedemarque.fr	2021-11-13
tnpaschers.fr	2018-09-22
tnusine.fr	2019-09-07
usinemagasin.fr	2021-11-13
usinemax.fr	2021-11-13
vraisdestock.fr	2021-11-13

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/



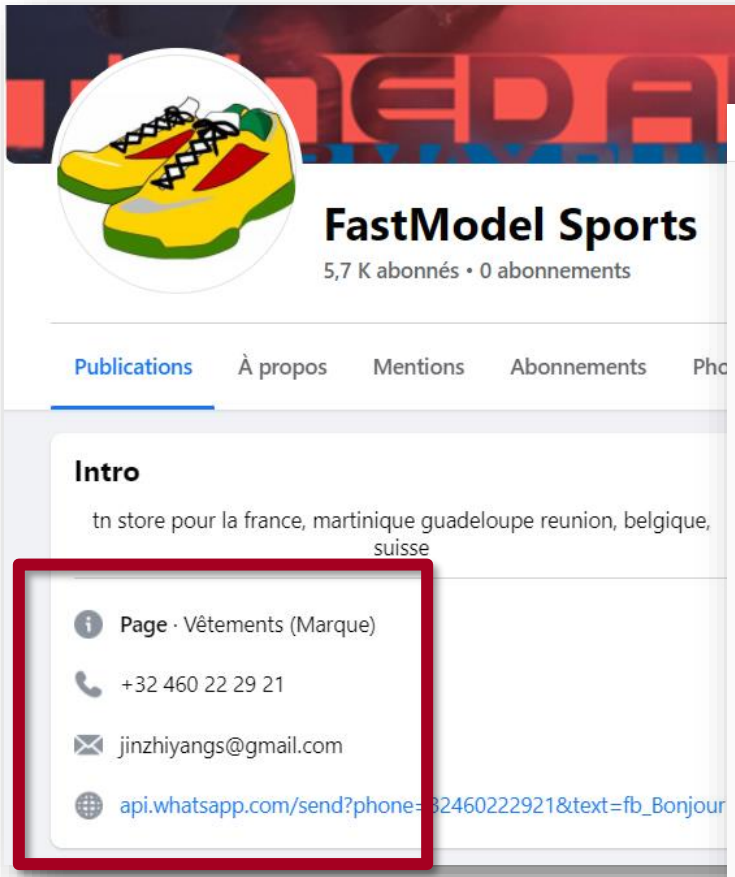
Recueil d'indices dans un fichier Excezl

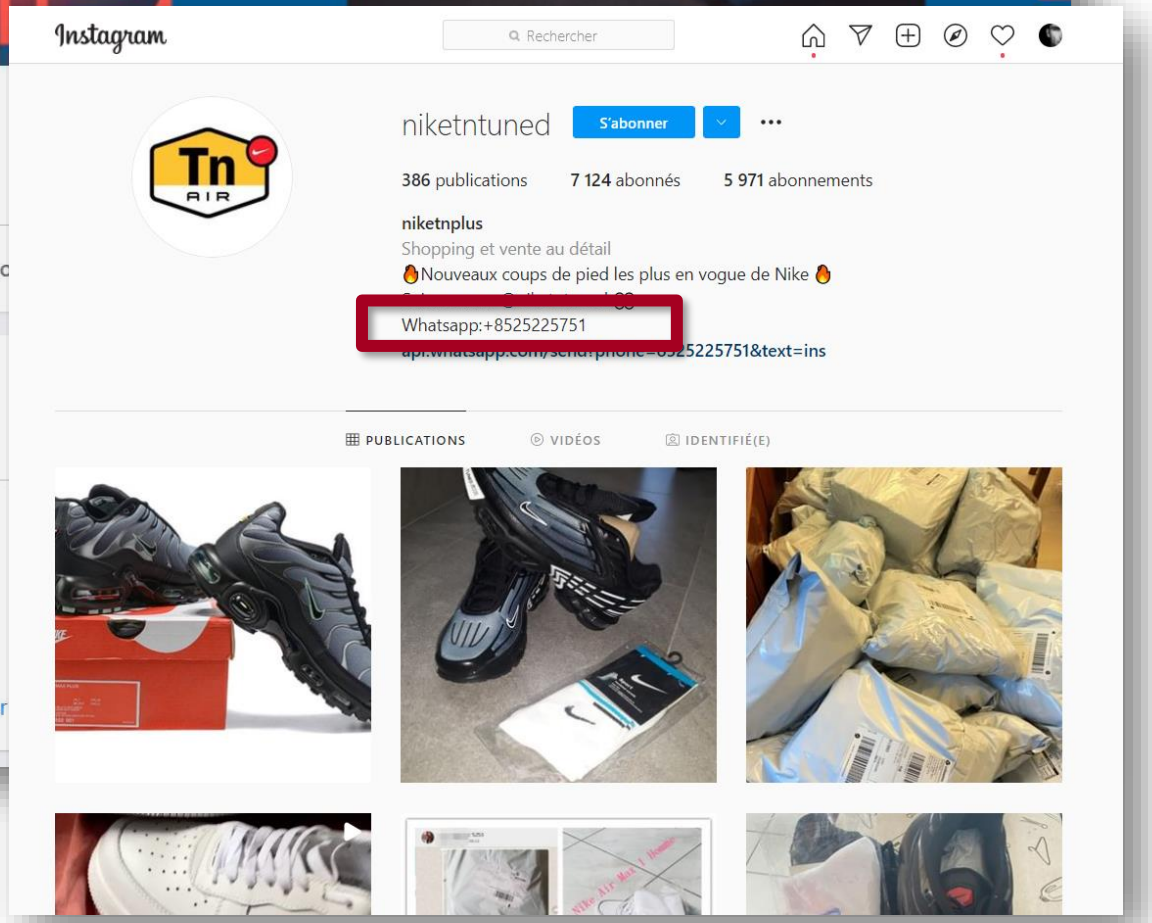
IP	NOM DE DOMAINE	DATE ENREGISTREMENT SITE WEB	adresse mail enregistrement nom de domaine	COMPTE FACEBOOK	INSTAGRAM	ADRESSE MAIL sur le site web	NR DE TELEPHONE 1	NR DE TELEPHONE	NR DE TELEPHONE	SKYPE	SNAPCHATT	LOGO	MEME STRUCTURE PAGE WEB
141.105.67.37	airmax.fr	29/04/2019	null			yy68a60@gmail.com	85252296088	32480361807	null	YY660_1	YOY9367	NIKE	1
94.130.80.123	airmaxfermeapascher.com	26/12/2019	null	https://www.facebook.com/FastModel-Sports-1115263868850154/	null	Boutiquesdemarque@gmail.com	32480222921	85152295751	null	null	null	NIKE	1
94.130.80.122	airmaxgros.com	04/12/2019	null	https://www.facebook.com/FastModel-Sports-1115263868850154/	https://www.instagram.com/niketntuned	Boutiquesdemarque@gmail.com	32480222921	85152295751	null	null	null	NIKE	1
141.105.67.38	airs.fr	29/04/2017	jamesyingst@outlook.com	https://www.facebook.com/FastModel-Sports-1115263868850154/	null	yy68a60@gmail.com	85252296088	32480361807	null	YY660_1	YOY9367	NIKE	1
94.130.80.125	boutiquesdemarques.com	26/07/2017	null	https://www.facebook.com/FastModel-Sports-1115263868850154/	null	Boutiquesdemarque@gmail.com	32480222921	85152295751	null	null	null	NIKE	1
94.130.80.123	boutiquefr.com	12/02/2019	null	https://www.facebook.com/FastModel-Sports-1115263868850154/	null	Boutiquesdemarque@gmail.com	32480222921	85152295751	null	null	null	NIKE	1
94.130.80.125	boutiquemass.com	23/02/2018	null	https://www.facebook.com/FastModel-Sports-1115263868850154/	null	Boutiquesdemarque@gmail.com	32480222921	85152295751	null	null	null	NIKE	1
94.130.80.122	boutiquemoncler.fr	09/12/2019	null	https://www.facebook.com/FastModel-Sports-1115263868850154/	https://www.instagram.com/niketntuned	Boutiquesdemarque@gmail.com	32480222921	85152295751	null	null	null	NIKE	1
94.130.80.123	boutiquesdemarque.com	06/09/2017	null	https://www.facebook.com/FastModel-Sports-	https://www.instagram.com/niketntuned	Boutiquesdemarque@gmail.com	32480222921	85152295751	null	null	null	NIKE	1

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

La Page Facebook

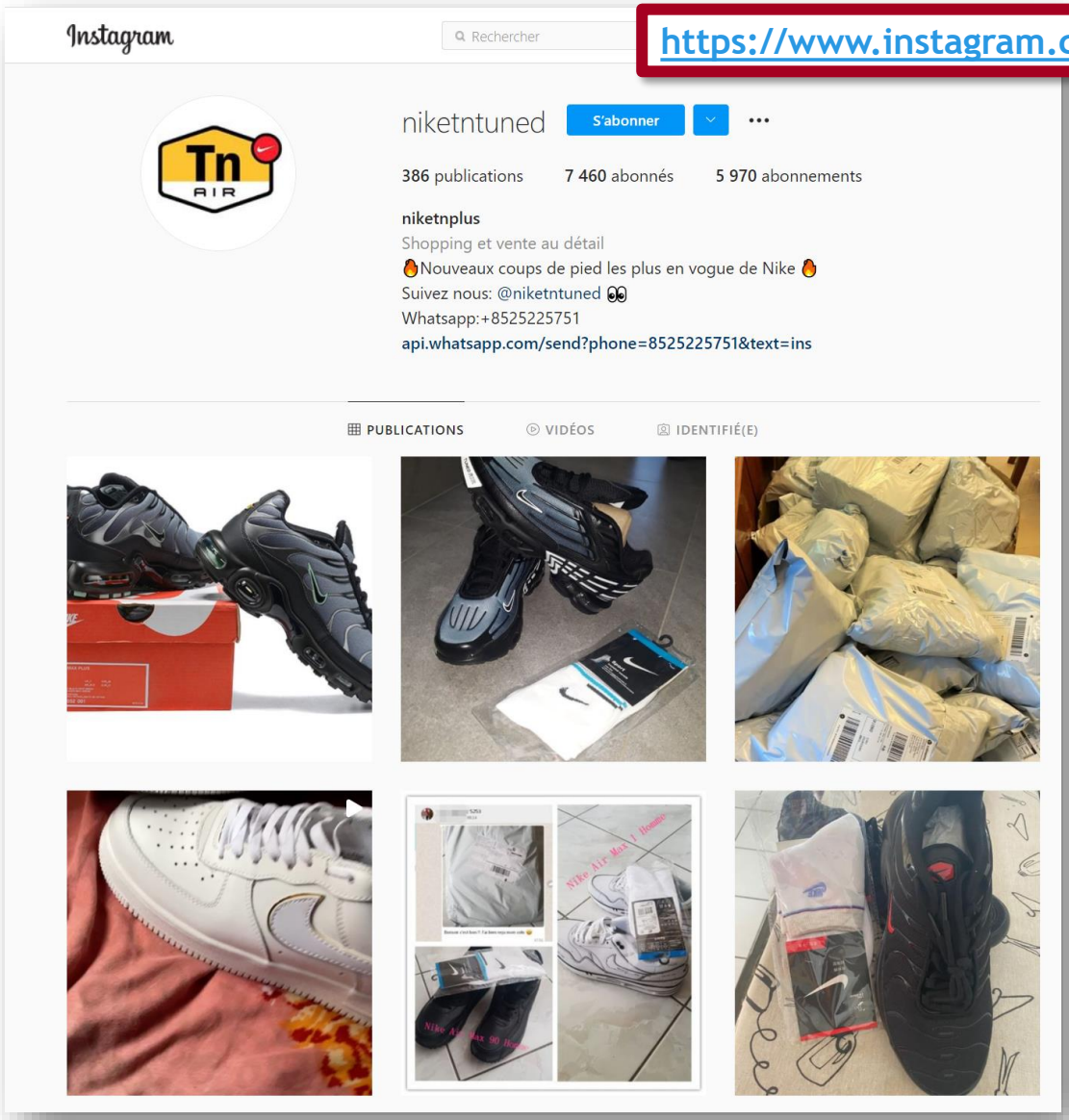
https://www.facebook.com/profile.php?id=100057197119938





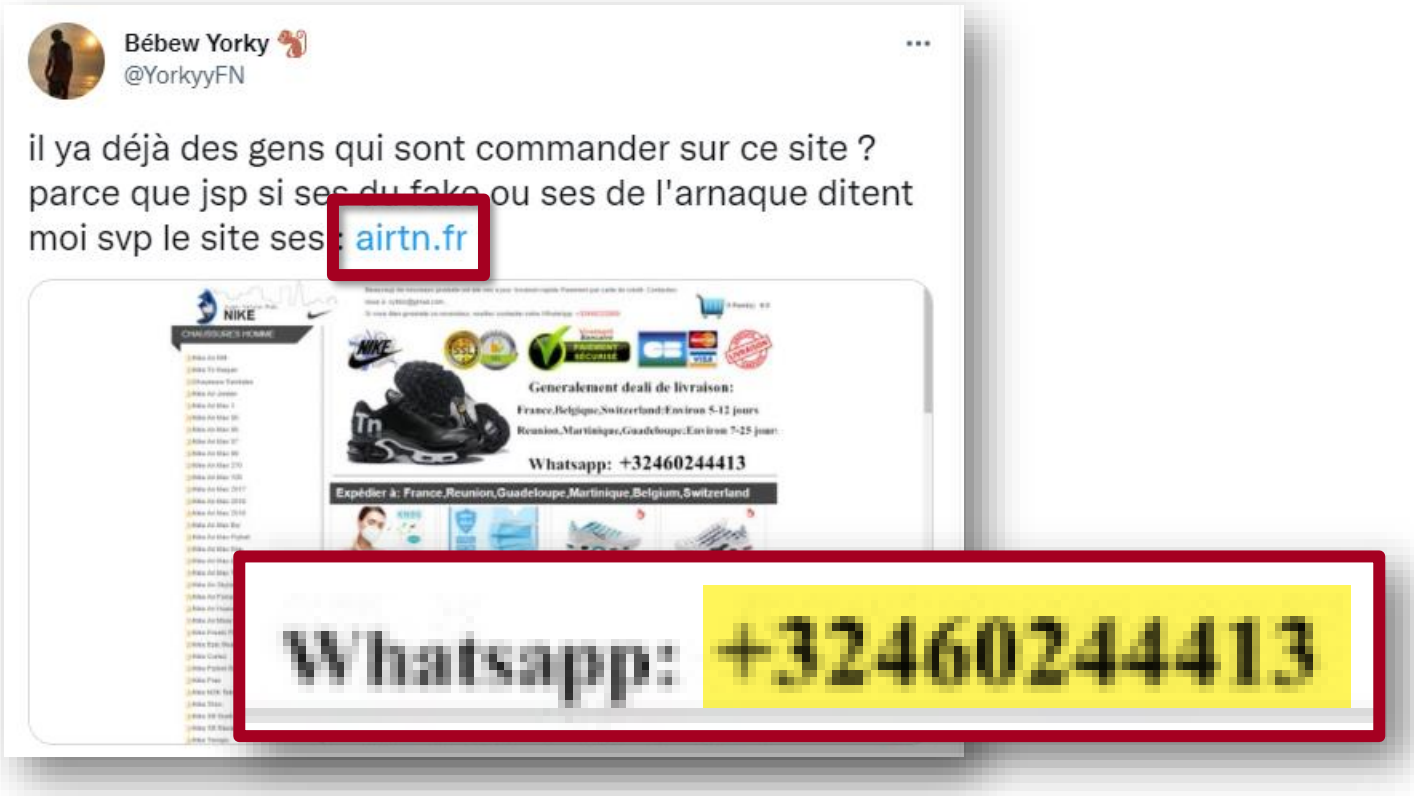
Le compte Instagram

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



Twitter

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



Le compte Gmail

EPIOS Email Lookup

jinzhiyangs@gmail.com
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

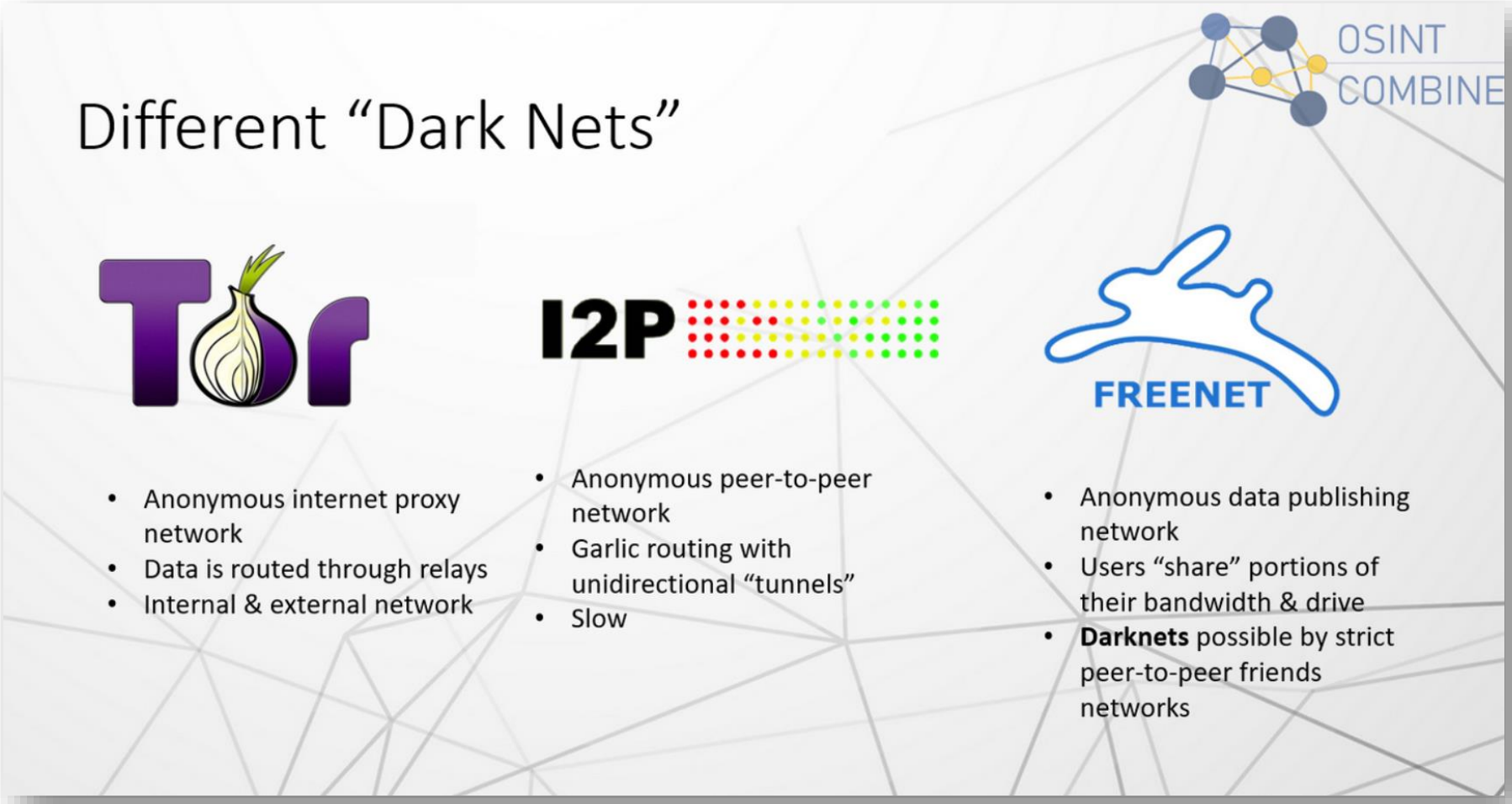
Calendar : https://calendar.google.com/calendar/htmlembed?src=Boutiquesdemarque@gmail.com

Reverse Image :

Bing Google Yandex

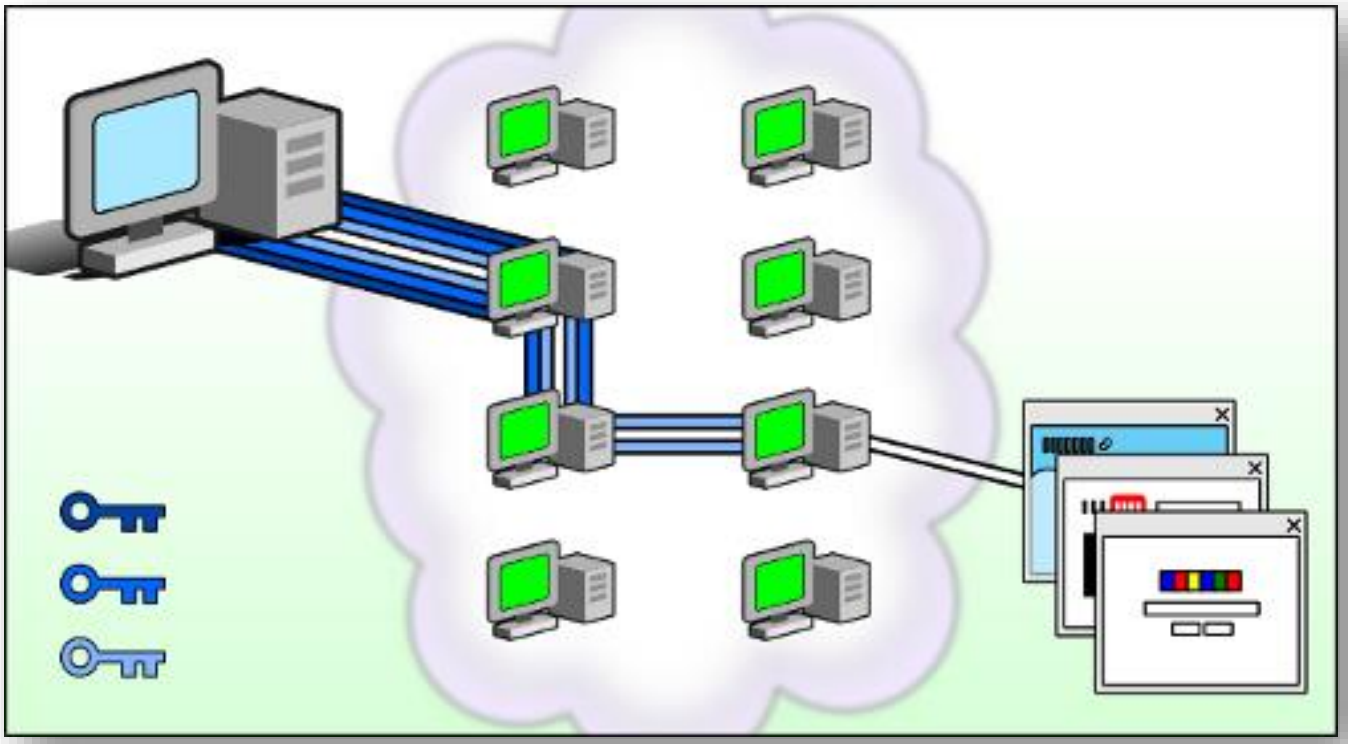
Investiguer le dark web (DARKINT)

Dark Web = Tor ?



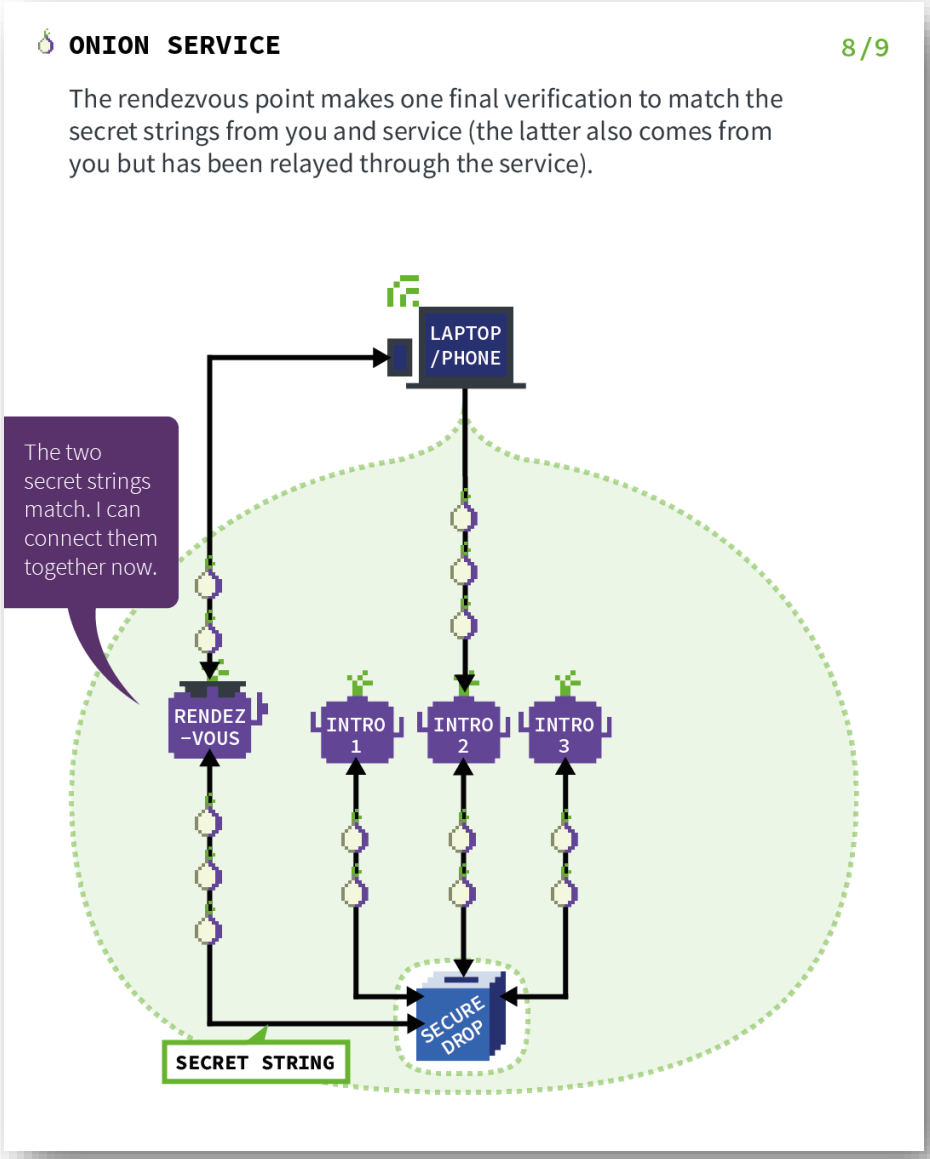
Source : Dark Web Searching (OSINT Combine, 2020)

Tor pour accéder anonymement à des sites Web



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

Tor pour héberger un « service Tor »



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

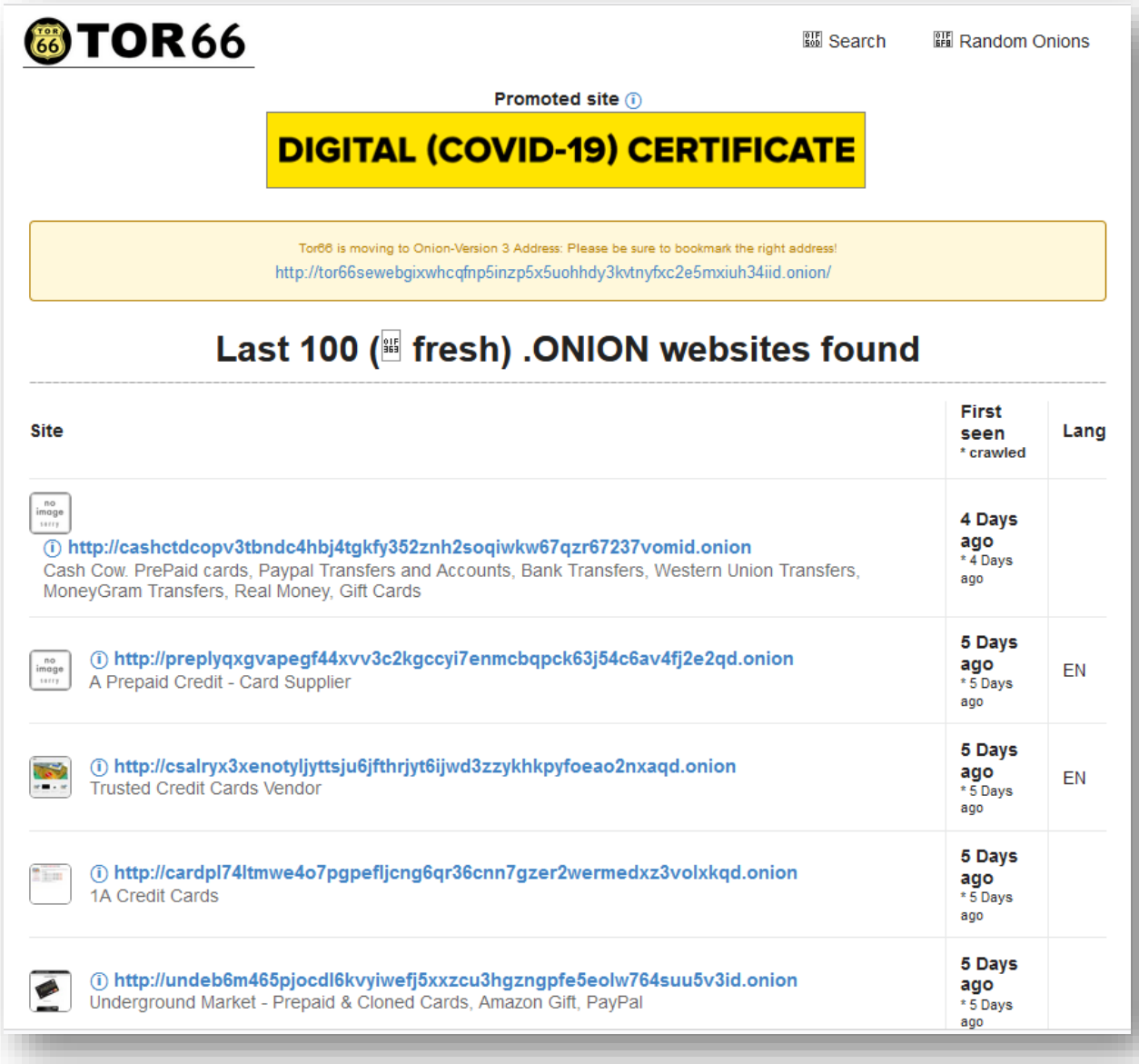
Moteurs de recherche

[Ahmia]

[TOR66] ([Fresh Onions])

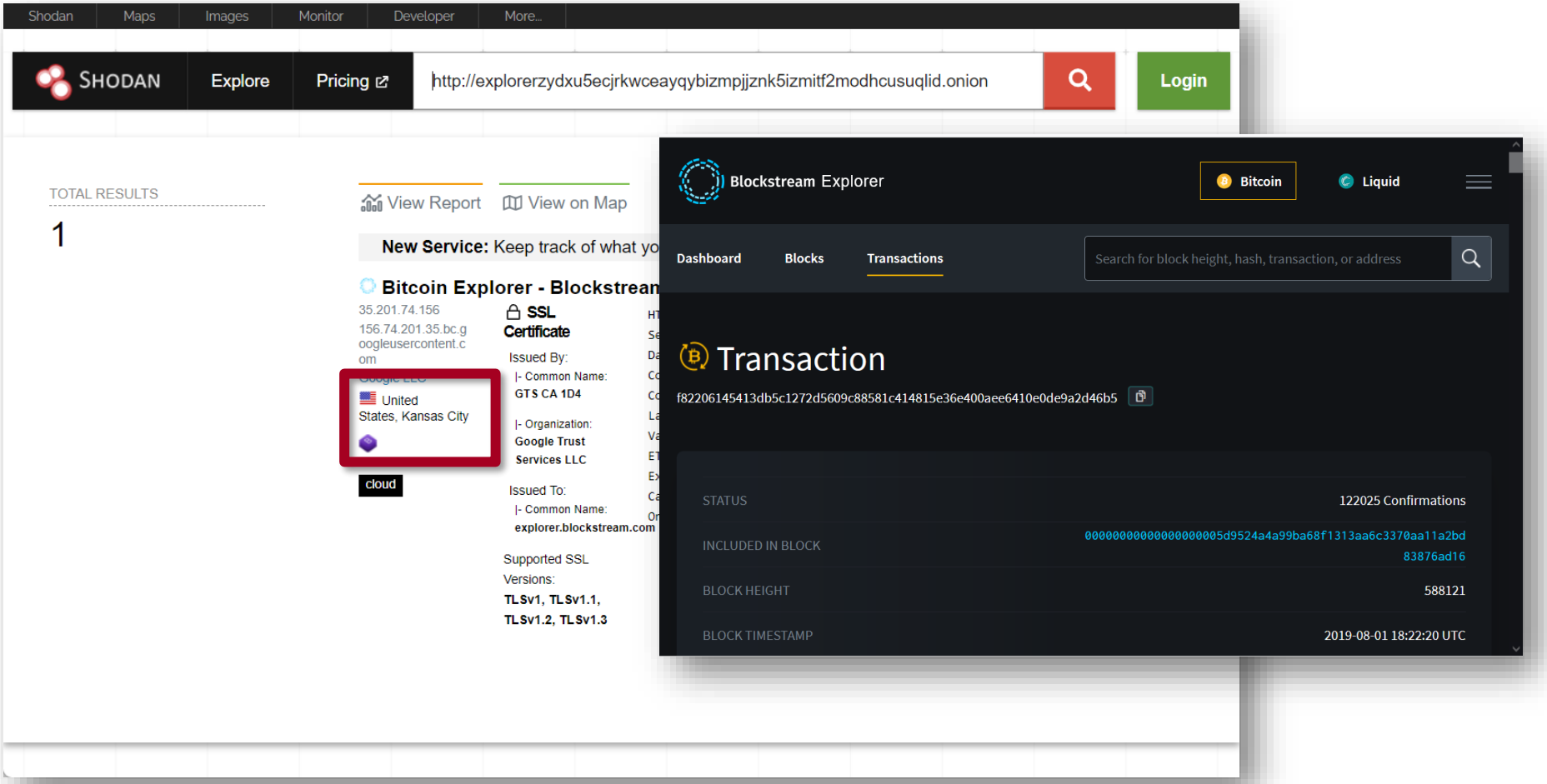
[TORCH]

[OnionLand Search]



Localiser un serveur

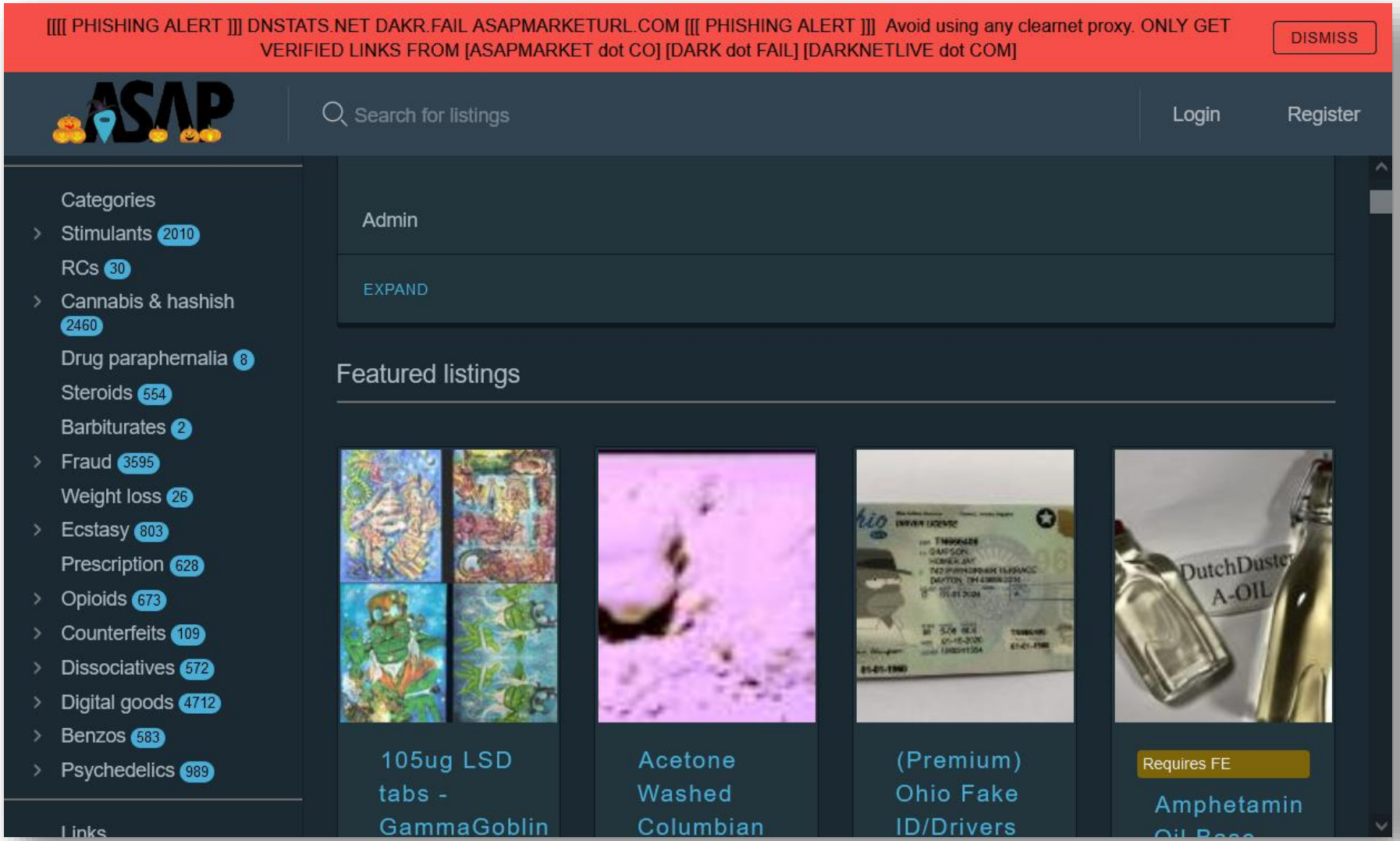
Une simple recherche dans Shodan pour trouver la localisation de BlockStream Explorer (insuffisamment protégé)



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

Marchés/vendeurs

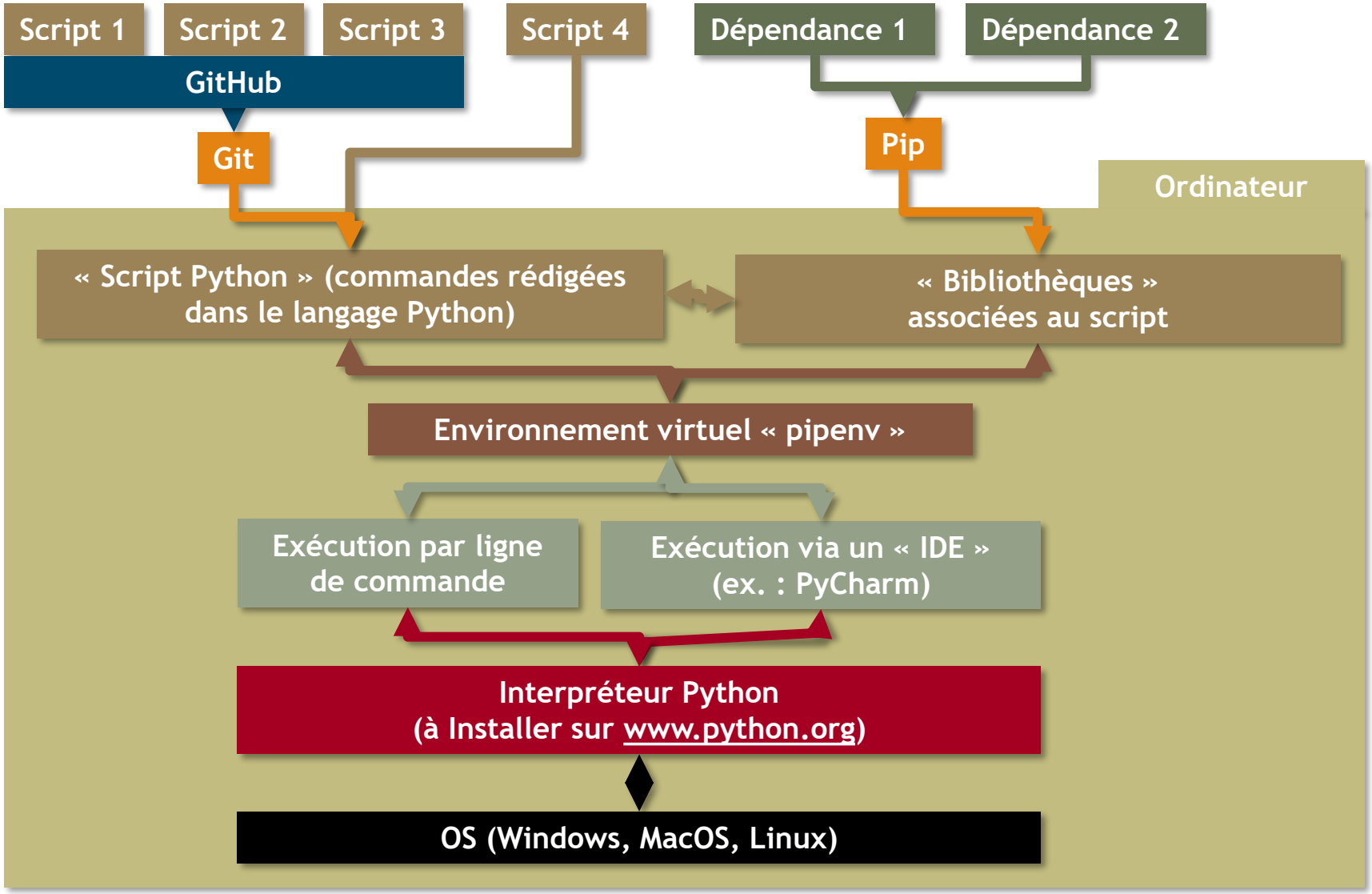
[List of darknet markets & vendor shops for investigators #3](#) **(OSINT.ME, 2021)**



Python

Accéder au niveau supérieur de l'OSINT

Script Python : un exemple de fonctionnement

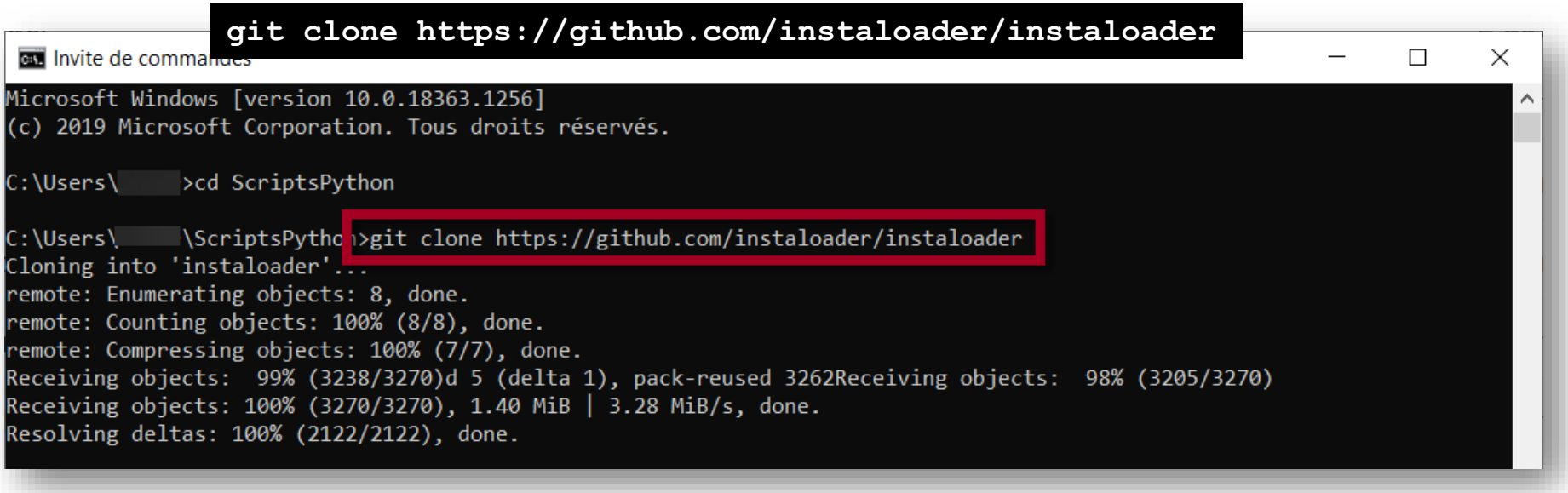


Récupérer (« cloner ») un script en ligne de commande avec Git

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)



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

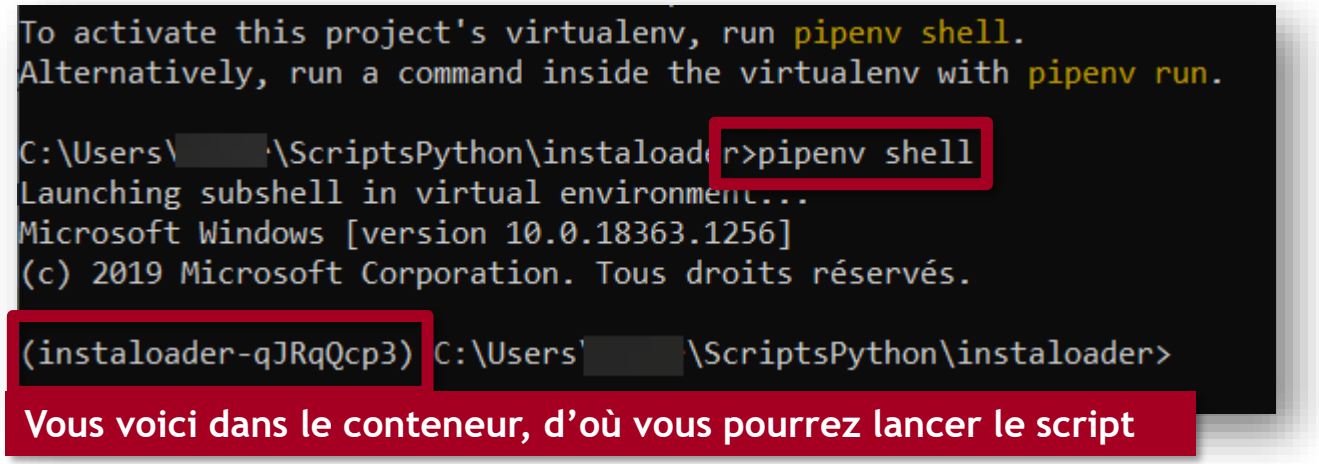
1. Si vous voyez à la racine du projet des fichiers Pipefile et Pifile.lock

```
pipenv install
```

Se préparer à l'exécution

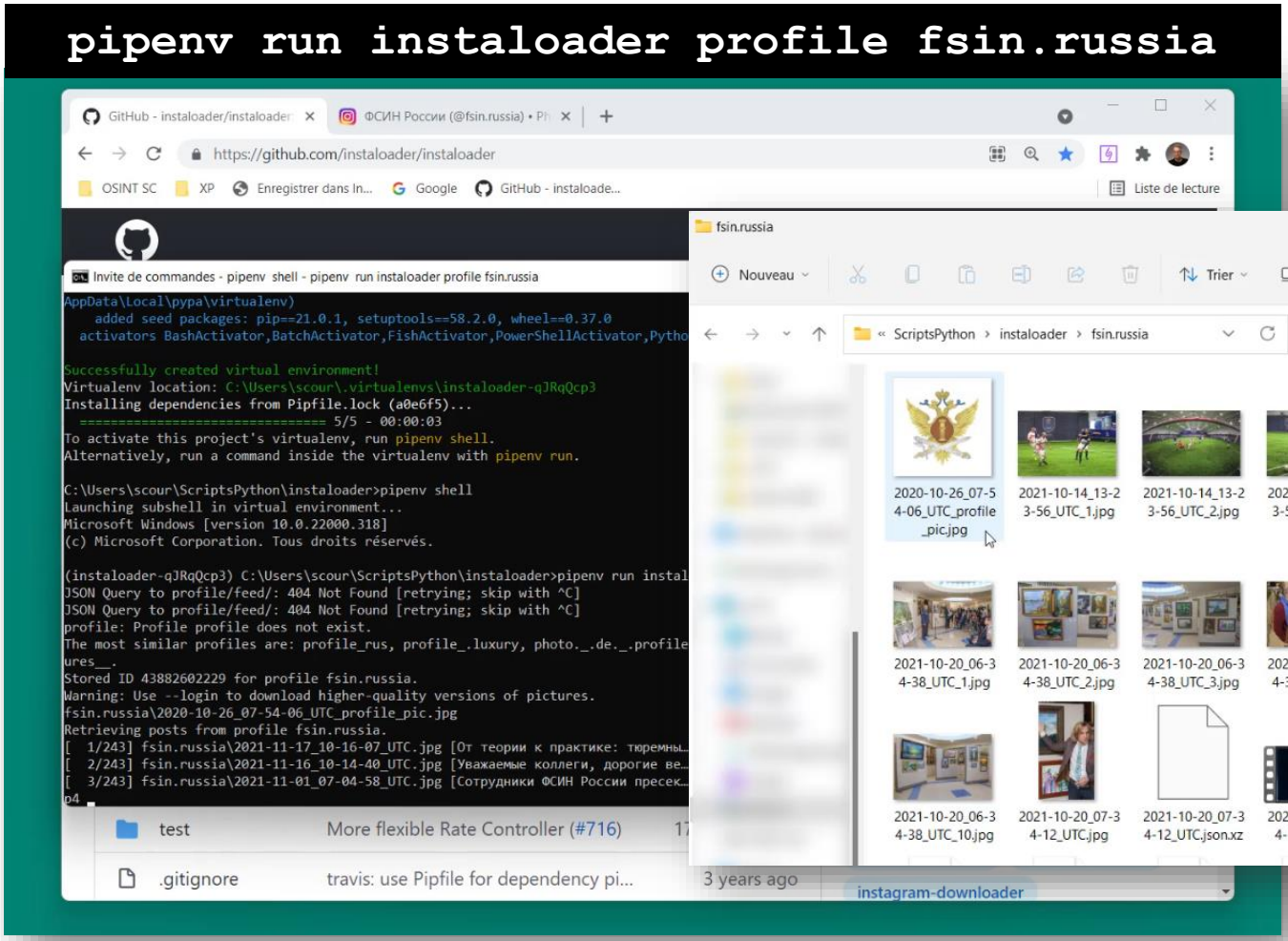
Votre script est placé dans un conteneur pipenv ? Il faut y entrer !

```
pipenv shell
```



Exécuter le script

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



Autres scripts à tester

Quelques scripts à tester

Facebook
- ▶ FFFF : Find Facebook Friends

Twitter
- ▶ Twint
- ▶ TwitWork

YouTube
- ▶ YouTube Comment Downloader

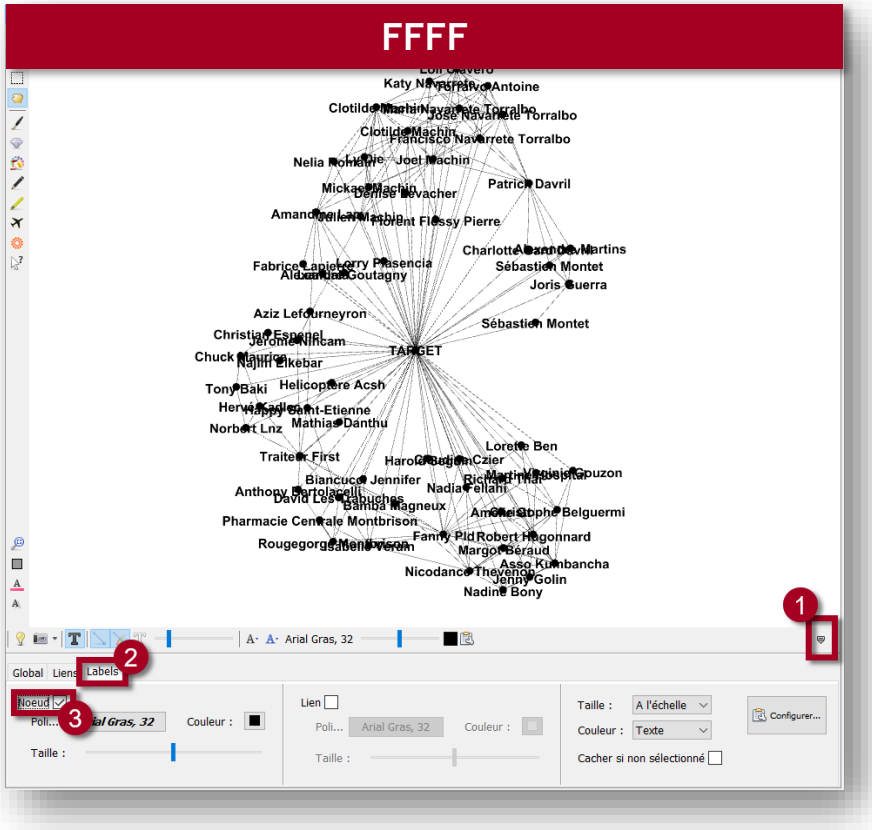
Instagram
- ▶ Instaloader

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)

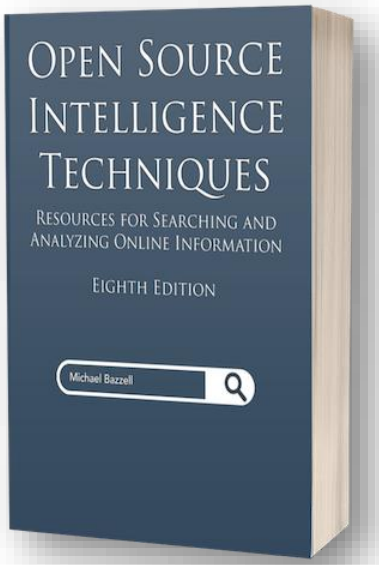
► Liste spécialisée OSINT

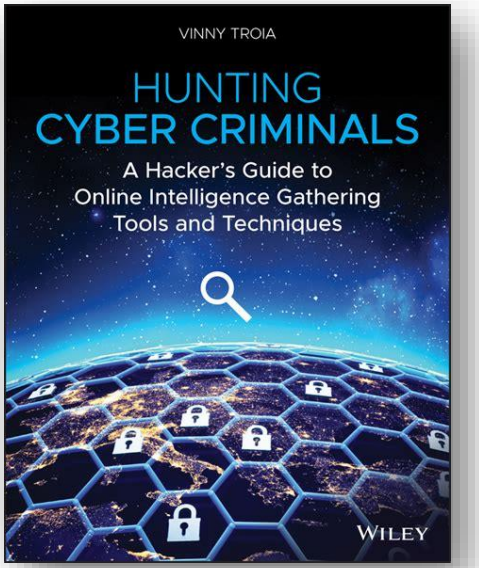
Communauté OSINTFR sur Discord

► Lien d'accès dans la bi du compte Twitter @OSINTFR

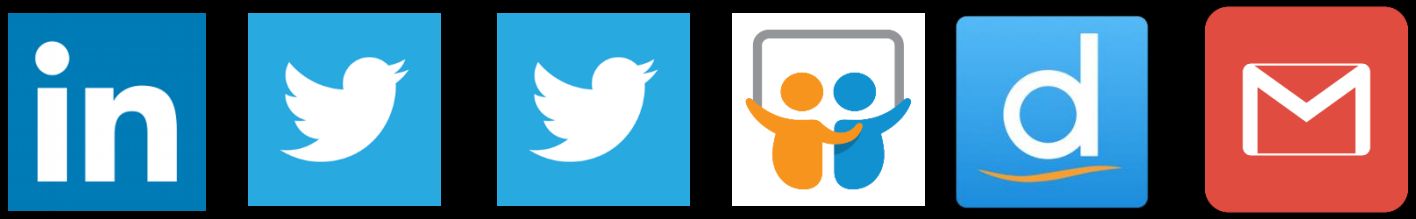
Open Source Intelligence Techniques **(Michael Bazzell, 2021)**

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*.