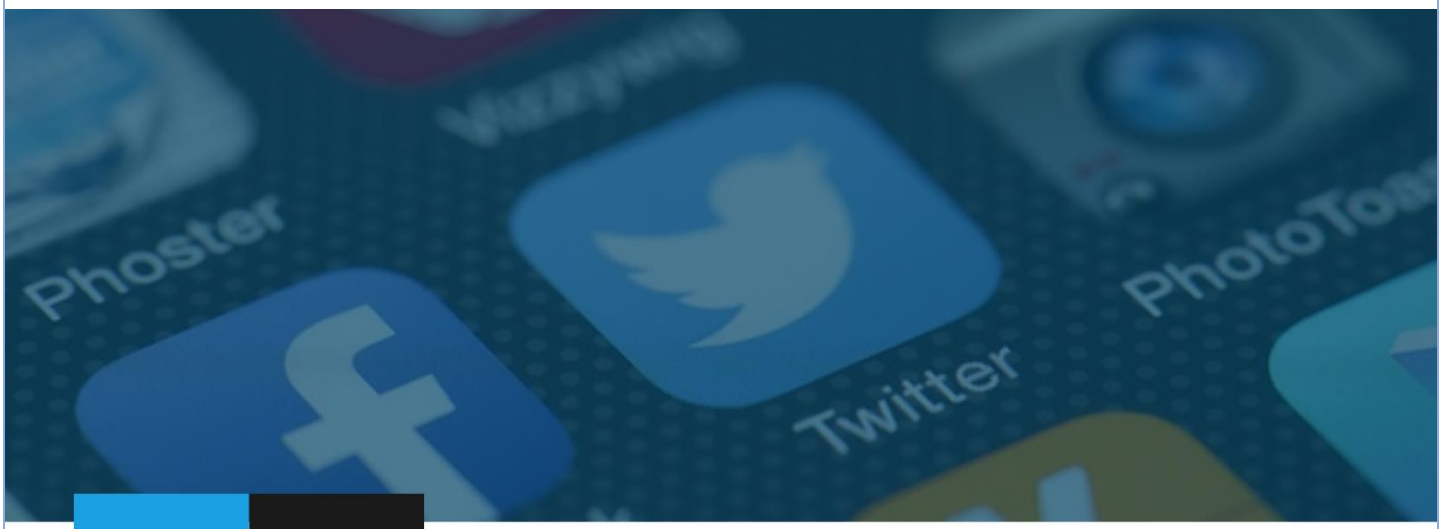


OSINT – GEOINT Formation

Sommaire

Introduction 3
Avis de non-responsabilité 4
L'OSINT, définition et utilisation : 5
Qu'est-ce que l'OSINT ? 5
Comment utiliser l'intelligence open source ? 7
Le côté obscur de l'intelligence open source 7
Techniques d'intelligence open source 8
Outils d'intelligence open source 9
Commencez par la fin 10
Liste d'outils et méthodes 11
Des podcasts à écouter gratuitement 11
Site et blog 11
OSINT : cas concret 11
Twitter : Un vivier d'informations 12
GEOINT : Mise en situation 21
Identification d'un individus par le biais d'une photo anodine 21
Cas d'OSINT / GEOINT dans l'histoire d'internet 68
Mot de la fin 69

Introduction

Avant d'entamer toute introduction, j'aimerais tout d'abord vous remercier pour la confiance dont vous me témoignez à travers l'achat de ce support et j'espère que celui-ci vous permettra de mettre un humble pied à l'étrier de ce domaine.

De fait, à travers ce PDF je souhaite effectivement vous introduire à l'OSINT, pratique extrêmement méconnue, très mal documentée, dont les pratiquants sont très discrets, mais également ses applications dérivées, à la définition, l'étendue, les acteurs, les méthodes, les sites web pertinents, ainsi que quelques exemples.

Ce faisant, j'espère plusieurs choses :

1) Que vous puissiez réellement définir, assimiler et reconnaître la pratique de l'OSINT.

2) Vous donner des pistes intéressantes afin de vous permettre d'entamer votre d'apprentissage de l'OSINT de la meilleure manière qui soit.

3) Vous faire comprendre les risques quant à la propagation de vos données sur les réseaux sociaux et internet en général (notamment à travers le PDF complémentaire au sujet de GDPR -> « Règlement général sur la protection des données »).

4) En parallèle à cela, vous permettre de gérer votre empreinte digitale au mieux, et de ce fait de vous rendre plus difficilement traçable.

5) Accorder aux plus intéressés le maximum d'informations disponibles avant de les introduire aux rouages les plus complexes à travers la formation supplémentaire qui se veut beaucoup plus complète et moins inhibée au sujet du contenu.

Enfin, selon la demande et vos retours, ce document est potentiellement le premier d'une longue série de plus en plus complexe et ésotérique à ce sujet.

Avis de non-responsabilité

Je ne suis en aucun cas responsable des dommages directs et indirects subis, résultant de l'utilisation de cette formation et de l'exécution du présent Contrat, tel que ces dommages sont communément admis par la jurisprudence française.

Raison pour laquelle, l'utilisateur s'engage à être seul responsable de ses actions suite à l'application du contenu et l'utilisation de cette formation.

En outre, je n'exerce pas de contrôle a posteriori et je suis uniquement responsable du contenu posté dans ladite formation, pas des recherches en découlant.

Enfin, l'utilisateur renonce à tout recours contre l'émetteur de ce document.

L’OSINT, définition et utilisation :

- L’Open Source INTelligence (OSINT) est l’exploitation de données, d'informations accessibles au grand public. Cela ne se limite pas à ce que l'on peut trouver via un moteur de recherche, bien que le web soit un élément important.
- Tout aussi utile et important que puisse être l’OSINT, l’abondance d’informations peut devenir un problème selon ce qui est désiré par l’investigateur.
- L’OSINT a son « côté obscur » : tout ce qui peut être trouvé par des professionnels de la sécurité peut également être trouvé (et utilisé) par des personnes malveillantes.

- Il est essentiel de disposer d'une stratégie et d'un cadre clairs pour la collecte de renseignements de sources ouvertes.

Parmi tous les sous-types de renseignements sur les menaces, et la recherche d’information sur des cibles/individus, l’OSINT est peut-être le plus utilisé, ce qui est logique. Après tout, c’est gratuit, et qui peut dire non à cela ?

Malheureusement, contrairement à certains types de mode d’investigation (espionnage, GEOINT, etc.) l’OSINT est le plus mal compris et souvent le plus mal utilisé.

Raison pour laquelle nous allons parler des principes fondamentaux de l’OSINT, y compris son utilisation, ainsi que les outils et techniques pouvant être utilisés pour la collecte et l'analyse.

Qu'est-ce que l’OSINT ?

Avant d'examiner les sources communes et les applications pour faire de l'OSINT, il est important de comprendre ce que c'est réellement.

Est considéré comme intelligence ouverte ce qui est :

- Obtenu à partir d'informations open source
- Collectées, analysées et diffusées en temps voulu et à un public approprié
- Ce qui répond à un besoin de renseignement spécifique

La phrase cruciale sur laquelle il faut se concentrer étant « accessible au public ».

Ainsi, le terme « open source » désigne spécifiquement les informations disponibles au grand public. Si des compétences, des outils ou des techniques sont nécessaires pour accéder à un élément d'information, celui-ci ne peut raisonnablement pas être considéré comme une source ouverte.

Point crucial, les informations open source ne se limitent pas à ce que vous pouvez trouver en utilisant les principaux moteurs de recherche. Les pages web et autres ressources disponibles sur Google constituent certes des sources massives d'informations open source, mais elles sont loin d'être les seules.

Pour commencer, une énorme proportion d'Internet (plus de 99%, selon l'ancien PDG de Google, Eric Schmidt) ne peut être trouvée à l'aide des principaux moteurs de recherche. Ce "Deep web" est une masse de sites, de bases de données, de fichiers, etc., qui (pour diverses raisons, notamment la présence de pages de connexion ou de modules de paiements) ne peuvent pas être indexés par Google, Bing, Yahoo ou tout autre moteur de recherche auquel vous pensez.

Malgré cela, une grande partie du contenu du « deep web » peut être considérée comme une source ouverte, car elle est facilement accessible au public.

En outre, de nombreuses informations en ligne librement accessibles peuvent être trouvées en utilisant des outils en ligne autres que les moteurs de recherche traditionnels. Nous examinerons cela plus tard, mais à titre d'exemple simple, des outils tels que Shodan et Censys peuvent être utilisés pour rechercher des adresses IP, des réseaux, des ports ouverts, des webcams, des imprimantes et à peu près tout ce qui est connecté à Internet.

Les informations peuvent également être considérées comme open source si elles sont :

- Publiées ou diffusées à un auditoire public (par exemple, contenu d'un journal).
- Disponibles au public sur demande (par exemple, données de recensement).
- Accessibles au public par abonnement ou par achat (par exemple, revues professionnelles).
- Pourraient être vues ou entendues par tout observateur occasionnel.
- Mises à disposition lors d'une réunion ouverte au public.

- Obtenues en visitant n'importe quel endroit ou en assistant à tout événement ouvert au public.

Vous pensez qu'il y a beaucoup d'informations à retenir ?

Vous avez raison.

Nous parlons d'un volume de données exponentielles au point où personne ne pourrait suivre leurs croissances.

Même si nous réduisons le champ à une seule source d'information (par exemple Twitter), vous seriez obligés de gérer plusieurs millions de nouvelles sources chaque jour.

Comme vous l'avez probablement compris, il s'agit d'un compromis inhérent à l'OSINT.

En tant qu'analyste, disposer d'une telle quantité d'informations est à la fois une bénédiction et une malédiction. D'une part, vous avez accès à presque tout ce dont vous pourriez avoir besoin, mais, d'autre part, vous devez être capable de trouver vos informations un torrent de données infini.

Comment utiliser l'intelligence open source ?

Maintenant que nous avons couvert les bases de l'intelligence open source, nous pouvons voir comment elle est couramment utilisée pour la cybersécurité. Il existe deux cas d'utilisation courants :

1. Pentests

Les professionnels de la sécurité utilisent l'intelligence open source pour identifier les faiblesses potentielles des réseaux amis afin de pouvoir y remédier avant qu'ils ne soient exploités par des acteurs malveillants. Les faiblesses couramment constatées incluent :

- Fuites accidentelles d'informations sensibles, notamment via les médias sociaux.
- Ports ouverts ou appareils connectés à Internet non sécurisés.
- Logiciels non corrigés, tels que les sites web exécutant d'anciennes versions des produits de CMS.
- Des actifs ayant fui ou exposés, tels que du code propriétaire sur des « pastebins ».

2. Identifier les menaces externes

Tel qu'énoncé précédemment, internet est une excellente source d'informations. De l'identification des nouvelles vulnérabilités exploitées à l'interception de discussions d'acteurs malveillants au sujet d'une attaque imminente, l'intelligence open source permet aux professionnels de la sécurité de hiérarchiser leur temps et leurs ressources pour faire face aux menaces les plus importantes.

Dans la plupart des cas, ce type de travail nécessite qu'un analyste identifie et corrèle plusieurs sources de données afin de valider une menace avant que des mesures ne soient prises. Par exemple, bien qu'un simple tweet menaçant puisse ne pas susciter d'inquiétude, ce même tweet serait interprété différemment s'il était lié à un groupe connu pour être actif dans un secteur spécifique (De LulzSec à l'Etat Islamique).

Une des choses les plus importantes à comprendre à propos de l'intelligence open source est qu'elle est souvent utilisée en combinaison avec d'autres sous-types de renseignements afin de valider la véracité de certaines informations. Les acteurs malveillants du web faisant souvent dans la désinformation afin de dissimuler des opérations à venir.

Le côté obscur de l'intelligence open source

Il est maintenant temps de s'attaquer au deuxième problème majeur en matière de renseignement de source ouverte : si les analystes du renseignement ont facilement accès à un élément, ils le sont également aux acteurs malveillants.

Ces derniers utilisent des techniques et des outils d'intelligence open source pour identifier les cibles potentielles et exploiter les faiblesses des réseaux ciblés. Une fois la vulnérabilité identifiée, il est souvent extrêmement simple et rapide de l'exploiter et d'atteindre divers objectifs malveillants.

Cette méthode est la raison principale pour laquelle tant de PME sont piratées chaque année. Ce n'est pas parce que les groupes s'y intéressent spécifiquement, mais plutôt parce que les vulnérabilités de l'architecture de leur réseau ou de leur site sont découvertes à l'aide de techniques simples d'intelligence open source. En bref, ce sont des cibles faciles.

L'OSINT ne permet pas seulement de commettre des attaques sur l'infrastructure et le système d'une entreprise. Les initiateurs de certaines opérations recherchent également des informations sur des individus et des organisations pouvant être utilisées dans des campagnes d'ingénierie sociale sophistiquées à l'aide de phishing (campagne mail), de vishing (campagne téléphonique) et de SMiShing (SMS). Souvent, des informations apparemment anodines partagées via des réseaux sociaux et des blogs peuvent être utilisées pour développer des campagnes d'ingénierie sociale extrêmement convaincantes, qui sont ensuite utilisées pour amener les utilisateurs bien intentionnés à compromettre le réseau ou les actifs de leur entreprise.

C'est pourquoi il est si important d'utiliser des informations de sécurité open source à des fins de sécurité. C'est une opportunité de rechercher et de corriger les faiblesses du réseau de votre entreprise et de supprimer les informations sensibles *avant* qu'un acteur menaçant n'utilise les mêmes outils et techniques pour les exploiter.

Techniques d'intelligence open source

Maintenant que nous avons abordé les utilisations de l'intelligence open source (bonnes et mauvaises), il est temps d'examiner certaines des techniques pouvant être utilisées pour collecter et traiter des informations open source.

Tout d'abord, vous devez disposer d'une stratégie et d'un cadre clairs pour acquérir et utiliser des informations de source ouverte. Il n'est pas recommandé d'aborder l'intelligence open source dans la perspective de trouver tout ce qui pourrait être intéressant ou utile - comme nous l'avons déjà mentionné, le volume d'informations disponibles via les sources ouvertes vous débordera tout simplement.

Au lieu de cela, vous devez savoir exactement ce que vous essayez d'atteindre - par exemple, identifier et corriger les faiblesses de votre réseau - et concentrer votre énergie sur la réalisation de ces objectifs.

Deuxièmement, vous devez identifier un ensemble d'outils et de techniques permettant de collecter et de traiter des informations open source. Encore une fois, le volume d'informations disponibles est beaucoup trop important pour que les processus manuels soient même légèrement efficaces.

De manière générale, la collecte d'informations open source se divise en deux catégories : collecte passive et collecte active.

La collecte passive implique souvent l'utilisation de plates-formes de renseignement sur les menaces (TIP) pour combiner une variété de sources de menaces en un seul lieu facilement accessible. Bien qu'il s'agisse d'une avancée majeure par rapport à la collecte manuelle de renseignements, le risque de surcharge d'information reste important.

De la même manière, des groupes organisés utilisent souvent des réseaux de zombies pour collecter des informations précieuses à l'aide de techniques telles que la détection de trafic et les Keylogger.

Par ailleurs, **la collecte active** consiste à utiliser diverses techniques pour rechercher des informations spécifiques. Pour les professionnels de la sécurité, ce type de travail de collecte est généralement effectué pour l'une des deux raisons suivantes :

1. La mise en évidence d'une menace imminente.
2. Un Pentest.

Outils d'intelligence open source

Pour clore les choses, nous allons voir quelques outils les utilisés pour collecter et traiter les informations de source ouverte.

Bien que de nombreux outils gratuits et utiles soient à la disposition des professionnels de la sécurité et des personnes malveillantes, certains des outils de renseignement open source les plus couramment utilisés sont les moteurs de recherche tels que Google - mais pas comme la plupart d'entre nous les connaissent.

Tel que précédemment énoncé, l'un des principaux problèmes des professionnels de la sécurité est la régularité avec laquelle des utilisateurs normaux bien intentionnés laissent accidentellement des actifs et des informations sensibles exposés sur Internet. Il existe une série de fonctions de recherche avancée appelée requêtes « Google dork » qui peuvent être utilisées pour identifier les informations et les actifs qu'elles exposent.

Les requêtes Google Dork sont utilisées quotidiennement par les professionnels de l'informatique et les pirates. Les exemples courants incluent « filetype : », qui réduit les résultats de la recherche à un type de fichier spécifique, et « site : », qui renvoie uniquement les résultats d'un site Web ou d'un domaine spécifié.

Le site web de Public Intelligence propose un récapitulatif plus détaillé des requêtes Google Dork, dans lequel il donne l'exemple de recherche suivant :

"sensitive but unclassified" filetype:pdf site:publicintelligence.net

Si vous tapez cette requête dans un moteur de recherche, il ne renvoie que les documents PDF du site web Public Intelligence contenant les mots « sensibles, mais non classifiés » quelque part dans le texte du document. Comme vous pouvez l'imaginer, avec des centaines de commandes à leur disposition, les professionnels de la sécurité et les acteurs malveillants peuvent utiliser des techniques similaires pour rechercher presque n'importe quoi.

Au-delà des moteurs de recherche, il existe littéralement des centaines d'outils permettant d'identifier les faiblesses du réseau ou les actifs exposés. Par exemple, vous pouvez utiliser Wappalyzer pour identifier les technologies utilisées sur un site Web et combiner les résultats avec Sploitus ou la base de données nationale sur les vulnérabilités afin de déterminer l'existence éventuelle de vulnérabilités pertinentes.

Évidemment, les exemples donnés ici ne représentent qu'une infime partie de ce qu'il est possible d'utiliser avec des outils de renseignement à code source ouvert. Il existe un grand nombre d'outils gratuits et premium qui peuvent être utilisés pour rechercher et analyser des informations open source, avec des fonctionnalités communes, notamment :

- Recherche de métadonnées
- Recherche de code
- Enquête sur les personnes et l'identité
- Recherche de numéro de téléphone
- Recherche et vérification par courrier électronique
- Lier des comptes de médias sociaux
- L'analyse d'image
- Recherche géospatiale et cartographie
- Détection de réseau sans fil et analyse de paquets

Ci-dessous, une illustration extraite du kit d'investigation de Bellingcat

Commencez par la fin

Quels que soient vos objectifs, l'intelligence open source peut s'avérer extrêmement utile pour toutes les disciplines de la sécurité. En fin de compte, trouver la bonne combinaison d'outils et de techniques pour vos besoins spécifiques prendra du temps, ainsi que des essais et des erreurs. Les outils et techniques dont vous avez besoin pour identifier les actifs non sécurisés ne sont pas les mêmes que ceux qui vous aideraient à suivre une alerte de menace ou à connecter des points de données à travers diverses sources.

Le facteur le plus important dans le succès de toute initiative d'OSINT est l'élaboration d'une stratégie claire : une fois que vous savez ce que vous essayez d'accomplir et que vous vous êtes fixé des objectifs, il est beaucoup plus facile d'identifier les outils et techniques les plus pertinents.

Vous trouverez ici, des stratégies complètes d'investigation par l'OSINT (qui seront abordées de manière bien plus technique et approfondies lors de la formation orale) :

https://www.assoeunomia.fr/2019/03/10/guide-dinvestigation-utiliser-les-sources-ouvertes/

https://www.institut-pandore.com/hacking/pister-espionner-retrouver-sur-internet/

https://0xpatrik.com/osint-people/

Liste d'outils et méthodes

https://github.com/jivoi/awesome-osint

https://github.com/Ph055a/OSINT-Collection

https://phonexicum.github.io/infosec/osint.html

Des podcasts à écouter gratuitement

http://osintpodcast.com/

Site et blog

https://osintcurio.us/

https://inteltechniques.com/blog/

Pour illustrer les propos et définitions ci-dessus, je vous propose un exemple d'OSINT basique permettant d'identifier une personne pour une levée de doutes, puis un exemple de GEOINT d'une personne ayant posté une simple photo sur son compte Twitter.

OSINT : cas concret

L'OSINT (Open Source INTelligence) permet parfois d'enquêter sur un individu avec un seul élément et des connaissances basiques d'internet. Je vais ci-dessous, démontrer qu'un simple compte twitter sans information de base peut permettre de remonter jusqu'à un individu, connaître toutes ses habitudes, usurper son identité et éventuellement répandre des fake news.

Twitter : Un vivier d'informations

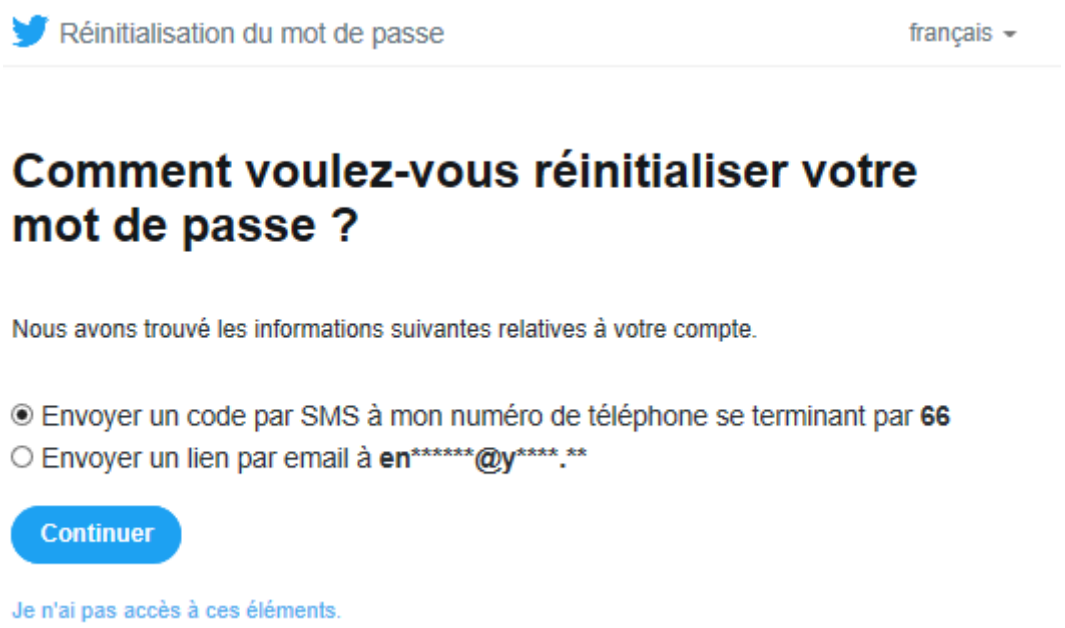
Prenons toujours sur le réseau social Twitter, une utilisatrice lambda : @enimar68. Son contenu est souvent généraliste avec beaucoup de soutien à l'extrême droite et la propagation de fausses nouvelles. Ce compte Twitter est un soutien très actif de Marine Le Pen sur ce réseau. En passant par une simple procédure de déclaration de perte du mot de passe, nous pouvons obtenir ceci :

Nous pouvons deviner l'adresse mail de récupération qui est : enimar68@yahoo.fr

Pour la confirmer, inversons la procédure en déclarant ne plus nous souvenir du nom du compte, mais seulement de l'adresse mail :

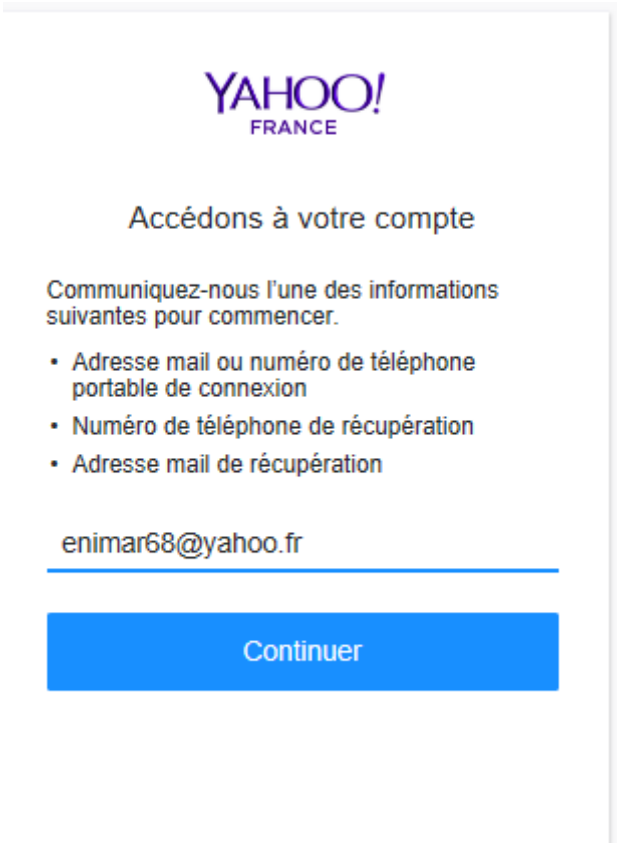
Etape 1 :

Etape 2 :



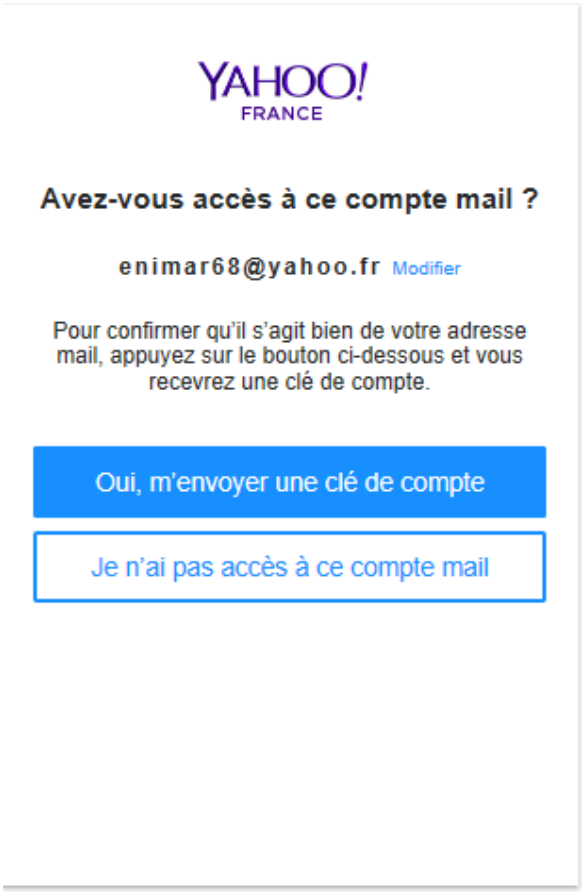
Les informations correspondent, nous pouvons poursuivre la procédure d'OSINT en interrogeant la base de données de Yahoo en suivant la procédure de perte du mot de passe :

Etape 3 :


YAHOO!
FRANCE
Accédons à votre compte
Communiquez-nous l'une des informations suivantes pour commencer.
• Adresse mail ou numéro de téléphone portable de connexion
• Numéro de téléphone de récupération
• Adresse mail de récupération
enimar68@yahoo.fr
Continuer

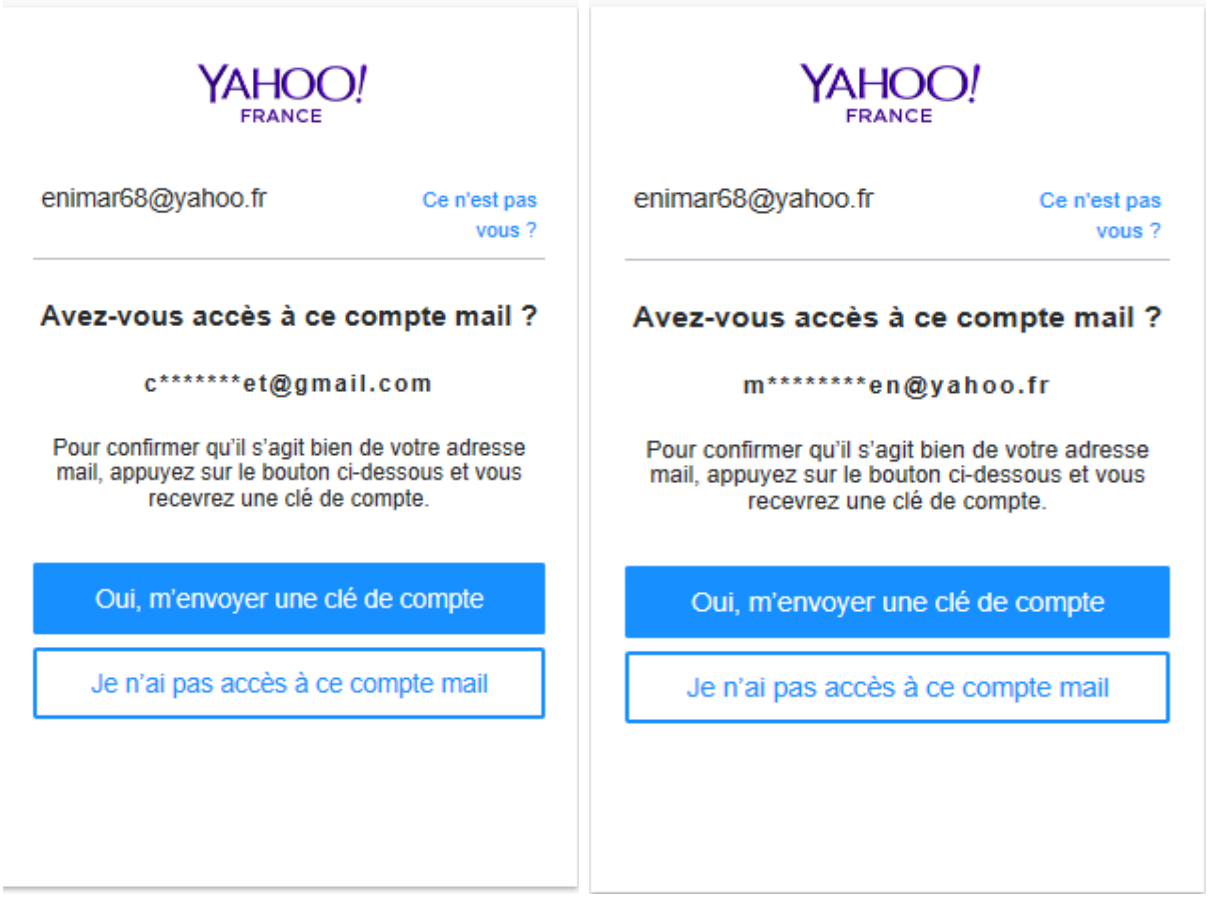
Etape 4 :

Déclarer ne plus avoir accès aux informations de base



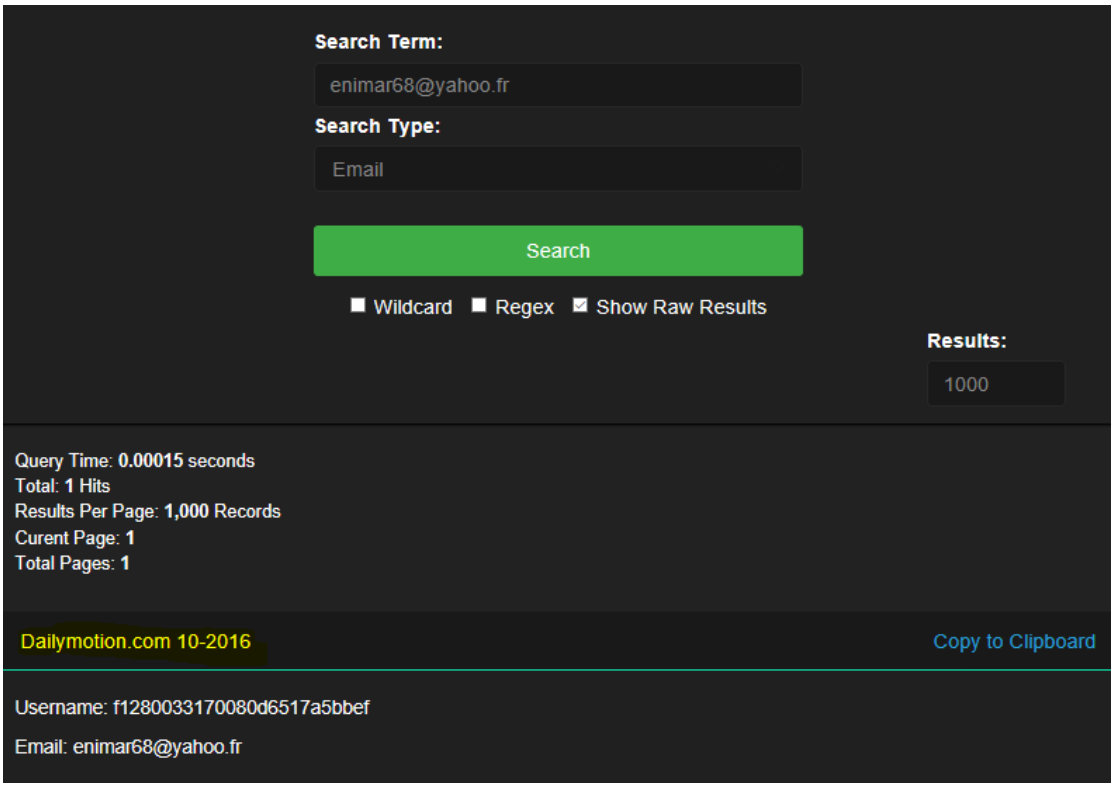
Etape 5 :

Continuer de nier connaître les informations de récupération

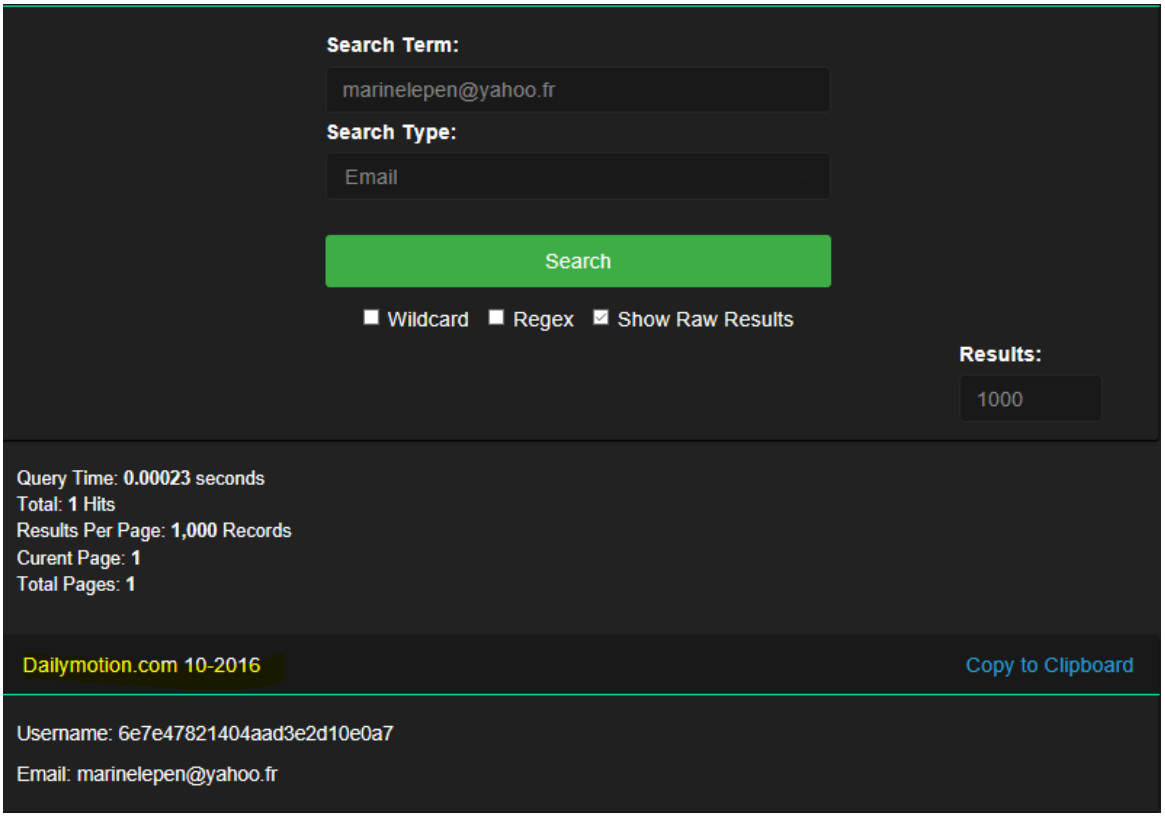


Cette étape permet de « deviner » une adresse bien que nous n'ayons pas d'éléments factuels concernant le possesseur du compte de récupération.

En effet, sur la dernière capture nous pouvons deviner : marinelepen@yahoo.fr, mais aucun élément concret ne peut prouver cela pour l'instant. Nous allons donc nous intéresser aux pistes alternatives en passant par le site de dump de base de données www.weleak.info (un peu plus « intrusif » car il s'agit de DUMP de bases de données). En entrant la première adresse mail, nous obtenons ceci :



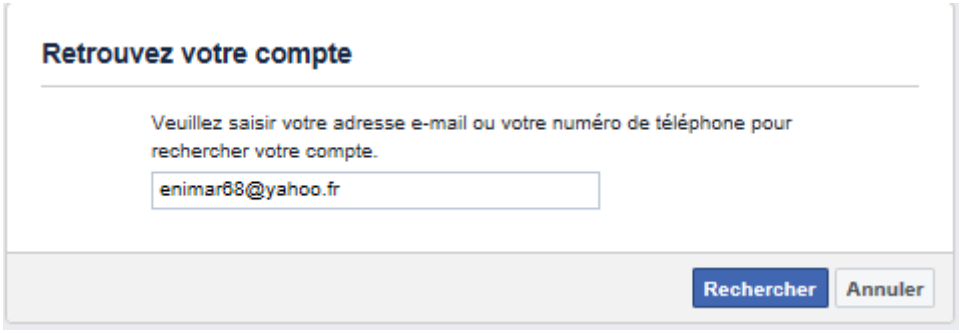
L'utilisateur de cette adresse mail a créé un compte sur le site Dailymotion au mois d'octobre 2016. Répétons l'opération avec la seconde adresse :



L'utilisateur a également utilisé cette adresse pour créer un compte Dailymotion en octobre 2016.

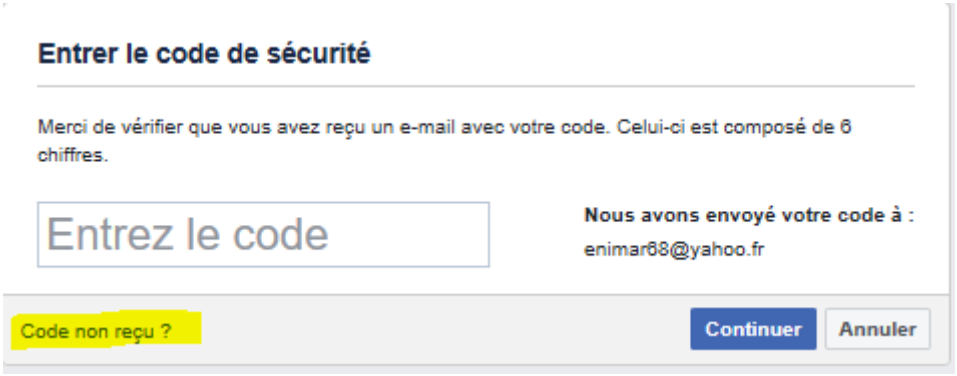
Nous avons donc une piste temporelle, les 2 utilisateurs semblent actifs au même moment sur internet. Dernier point, le réseau social Facebook. Nous allons initier une procédure de perte de mot de passe avec l'adresse enimar68@yahoo.fr

Etape 1



Etape 2 :

Nier avoir reçu le code de sécurité



Etape 3

Dire que l'on ne possède plus accès à la boîte mail

Nous sommes bloqués à la dernière étape, mais cela prouve que l'adresse enimar68@yahoo.fr possède un compte Facebook.

En allant dans la barre de recherche Facebook et en entrant l'adresse mail ci-dessus, nous arrivons sur l'utilisateur suivant, que nous allons comparer à la biographie de la chef du parti « Rassemblement National » :

Biographie	
Nom de naissance	Marion Anne Perrine Le Pen
Date de naissance	5 août 1968 (50 ans)
Lieu de naissance	Neuilly-sur-Seine (Hauts-de-Seine, France)
Nationalité	française
Parti politique	FN (1988-2018) RN (depuis 2018)
Père	Jean-Marie Le Pen
Mère	Pierrette Lalanne
Fratrie	Marie-Caroline Le Pen Yann Le Pen
Conjoint	Louis Aliot (depuis 2009)
Entourage	Marion Maréchal (nièce)
Diplômée de	université Panthéon-Assas
Profession	avocate
Religion	catholique[1]
Site web	marinelepen.fr [archive]

Nous ne pouvons pas aller plus loin pour des problèmes d'éthique et techniques, mais par déduction et croisement des données, il apparaît donc que l'utilisatrice du compte twitter « Anne Lalanne » soit bel et bien Marine Le Pen en personne. Ces informations sont publiques et je n'ai utilisé aucune autre technique que l'OSINT.

GEOINT : Mise en situation

Identification d’un individus par le biais d’une photo anodine

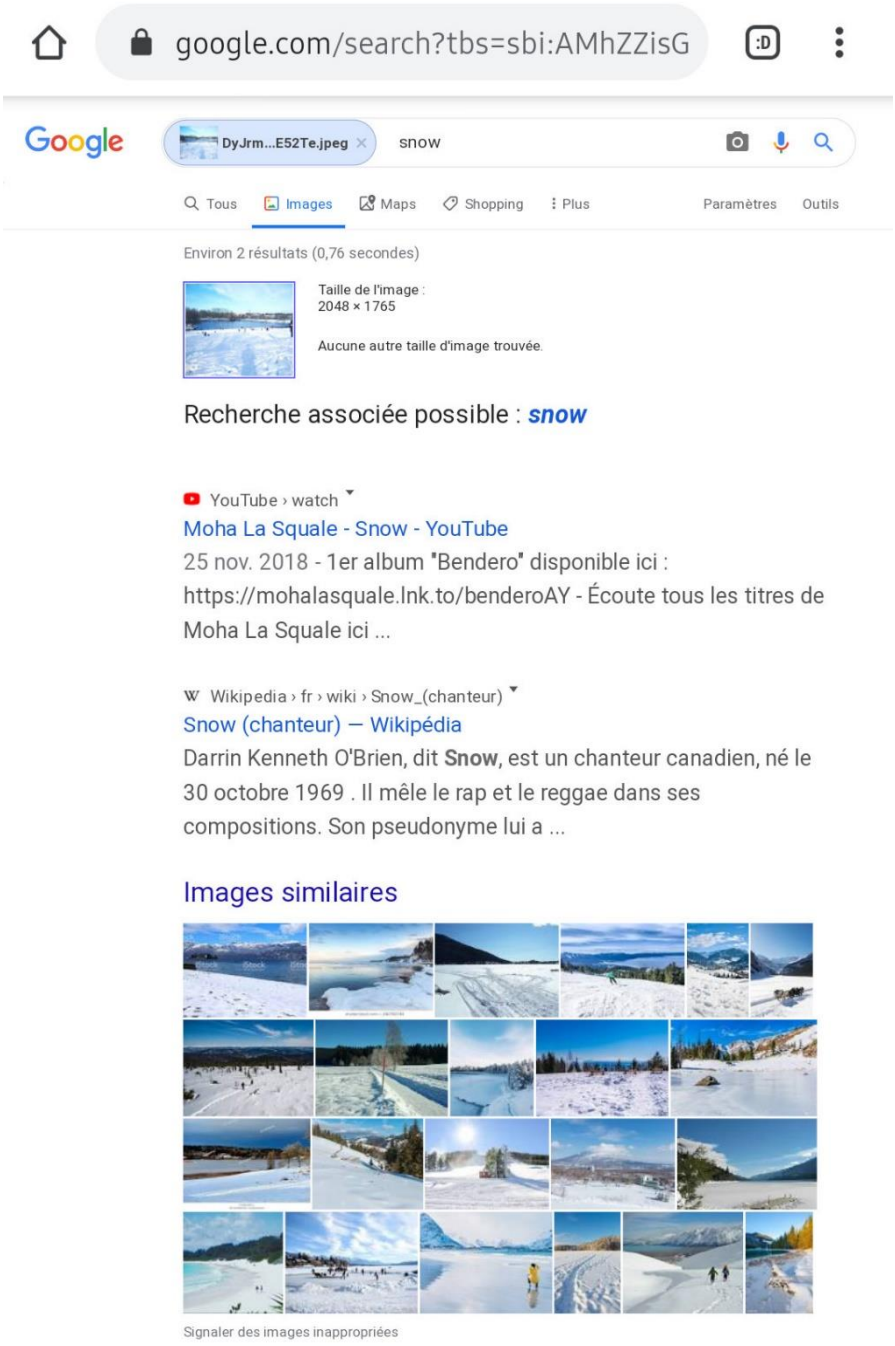
A partir d’une photo trouvée sur Twitter d’un individu ayant désactivé son compte (pour des raisons de confidentialité parmi la dizaine d’exemples de GEOINT dont j’ai été à l’initiative)

Je sais seulement qu’il s’agit d’un individu francophone, photo prise sans savoir si c'est en live

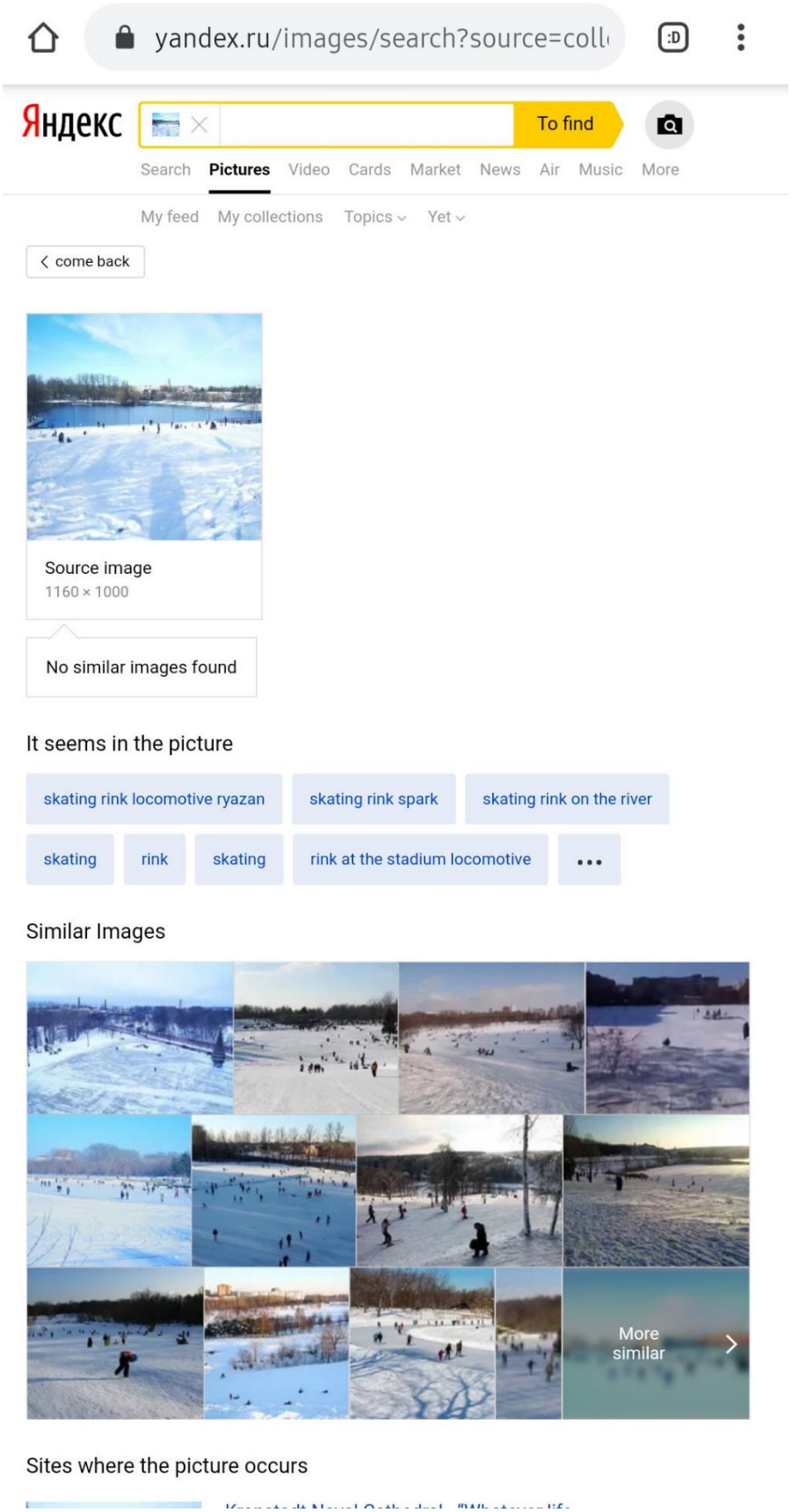
11:08 AM · 30 janv. 2019 · Twitter for Android

La photo téléchargée :

Google Image Reverse = rien

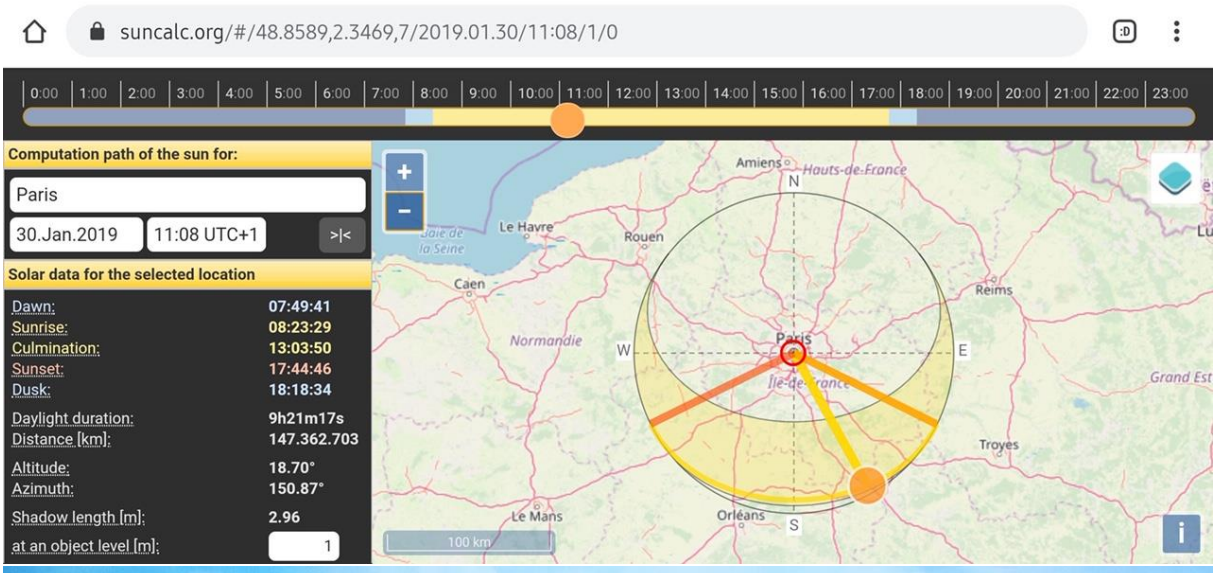


Yandex = résultats approximatifs (couche IA qui tente de reconnaître visage + paysages + monuments historiques) Mais aucun résultat.



Donc tentative de détermination de l'angle de la photo via Suncalc qui donne l'orientation globale.

Cette orientation permet d'estimer si la photo est prise en France ou à l'étranger, le paysage en arrière-plan ne permet pas de déterminer l'emplacement exact et il est similaire à certaines zones au Québec (pas de détails marquants).



Vérification du timing de la timeline de l'utilisateur afin de définir s'il tweet dans des "horaires normaux" GMT +1 et non en décalage horaire (en prenant en compte les heures de sommeil).

Exclusion de la "piste Québec".

Donc hypothèse globale : Photo prise en direct (~10h08), en France, et l'ombre de l'individu donne l'orientation.

Ce que l'on remarque ensuite sur l'image c'est un grand ciel bleu, un lac un peu gelé et la luminosité, un "beau temps". Á partir de ça, il a fallu déterminer dans quelle zone géographique ces conditions étaient réunies.

L'étendue d'eau et la ville font penser à une zone avec parcs + rivières (Lyon, Toulouse, Paris, etc.) donc il a fallu procéder par élimination : historique météo sur Toulouse, Lyon pouvait correspondre mais il n'y a pas eu d'épisode neigeux, Paris pouvait matcher mais également Lille car il y a eu un jour de beaux temps contrairement à Paris (ciel dégagé en premier lieu).

WolframAlpha computational intelligence

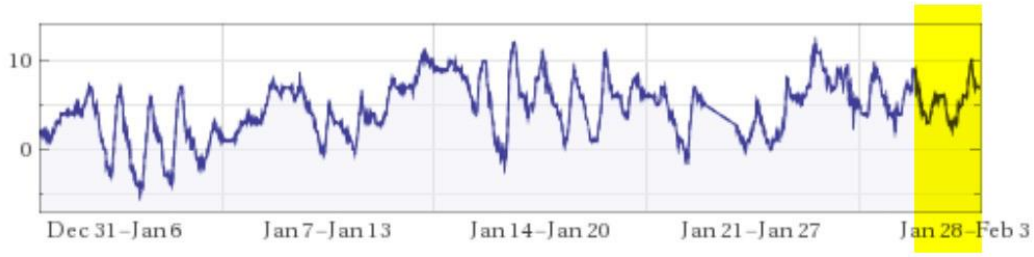
Weather Toulouse January 2019

Upload Examples Random

Weather history:

Month

Temperature

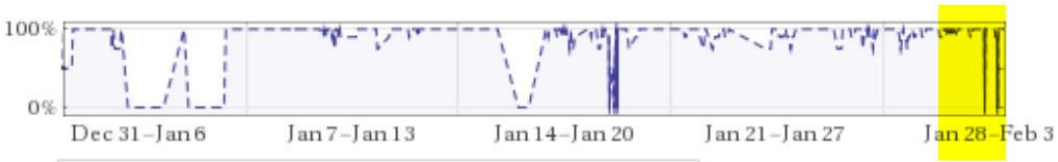


low: −5 °C
Fri, Jan 4, 7:00am

average high: 8 °C
average low: 1 °C

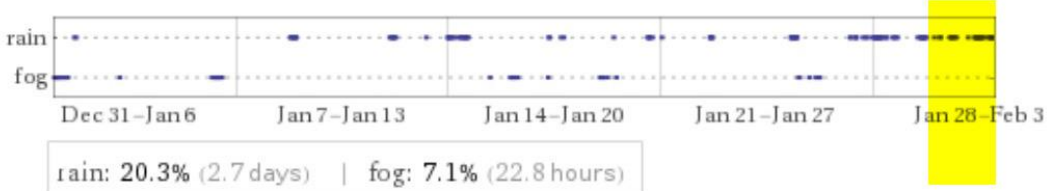
high: 12 °C
Wed, Jan 16, 3:00pm

Cloud cover



overcast: 67.2% (8.9 days) | clear: 4.7% (15 hours)

Conditions



rain: 20.3% (2.7 days) | fog: 7.1% (22.8 hours)

WolframAlpha computational intelligence

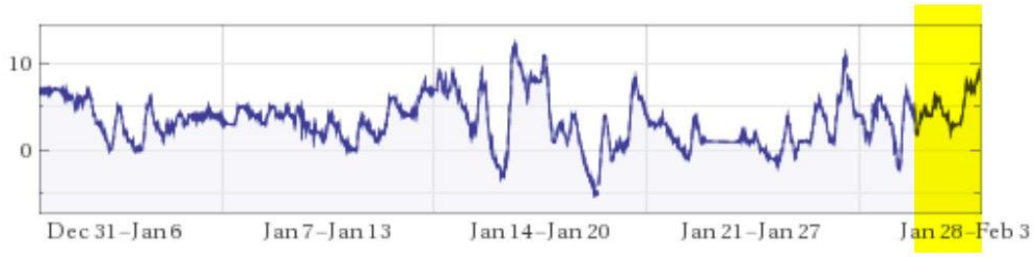
Weather Lyon January 2019

Upload Examples Random

Weather history:

Month

Temperature

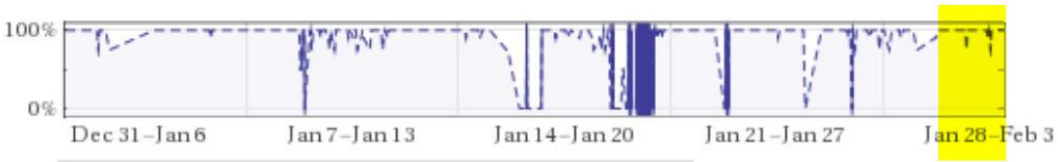


low: −5 °C
Sat, Jan 19, 8:00am

average high: 6 °C
average low: 1 °C

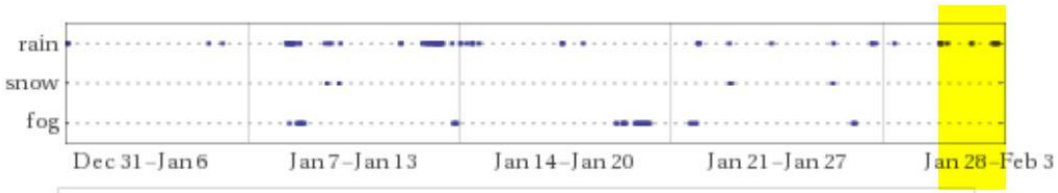
high: 12 °C
Wed, Jan 16, 4:00pm

Cloud cover



overcast: 72.5% (9.9 days) | clear: 8.4% (1.1 days)

Conditions



rain: 13.1% (1.8 days) | fog: 6.3% (20.5 hours) | snow: 2.4% (7.8 hours)

WolframAlpha computational intelligence

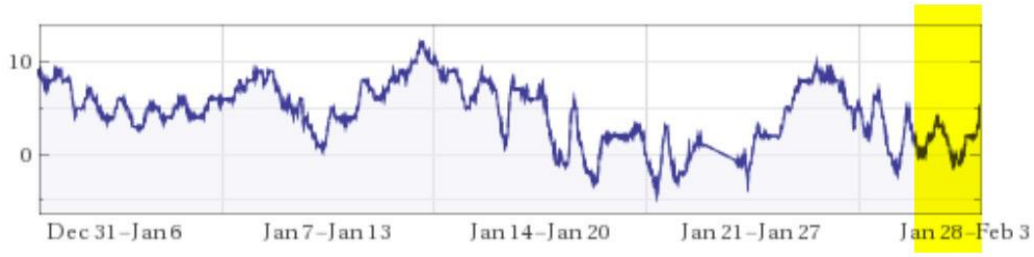
Weather Paris January 2019

Upload Examples Random

Weather history:

Month

Temperature

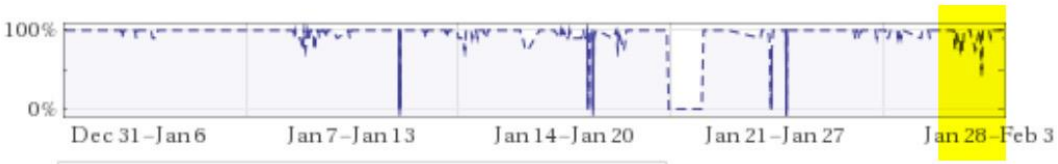


low: −4 °C
Mon, Jan 21, 8:00am

average high: 6 °C
average low: 2 °C

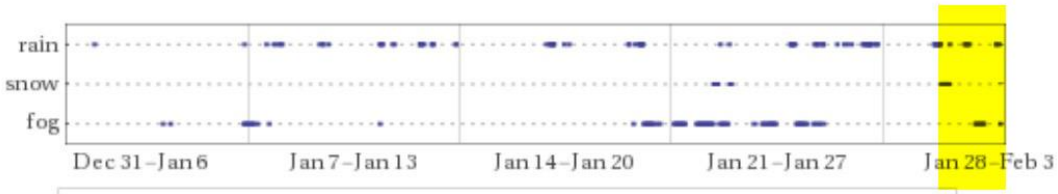
high: 12 °C
Sun, Jan 13, 12:30pm, ...

Cloud cover

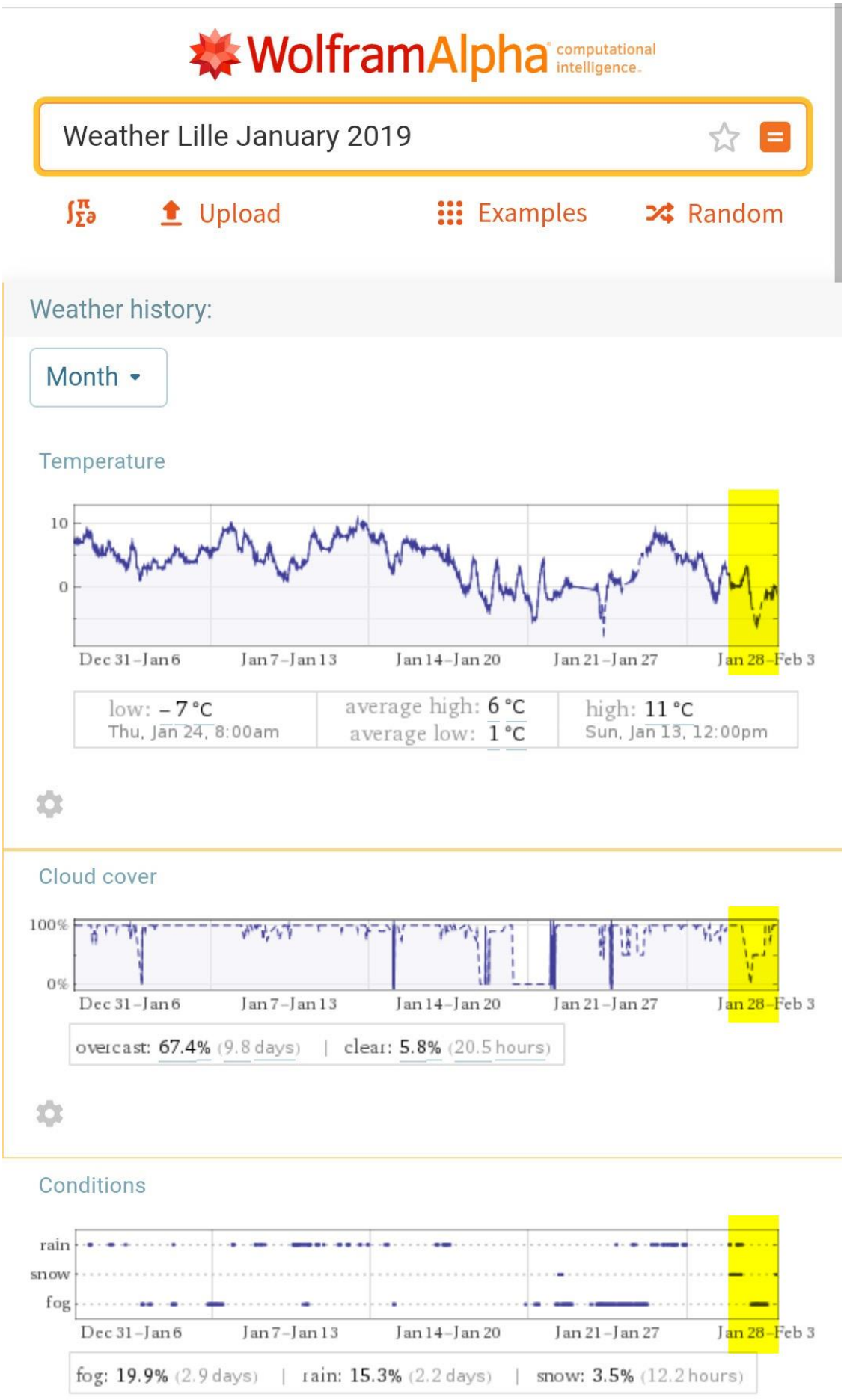


overcast: 73% (11 days) | clear: 3.6% (13 hours)

Conditions



rain: 14% (2.1 days) | fog: 13.9% (2.1 days) | snow: 4.3% (15.8 hours)


WolframAlpha computational intelligence
Weather Lille January 2019
Upload
Examples
Random
Weather history:
Month
Temperature
10
0
Dec 31–Jan 6
Jan 7–Jan 13
Jan 14–Jan 20
Jan 21–Jan 27
Jan 28–Feb 3
low: −7 °C
Thu, Jan 24, 8:00am
average high: 6 °C
average low: 1 °C
high: 11 °C
Sun, Jan 13, 12:00pm
Cloud cover
100%
0%
Dec 31–Jan 6
Jan 7–Jan 13
Jan 14–Jan 20
Jan 21–Jan 27
Jan 28–Feb 3
overcast: 67.4% (9.8 days) | clear: 5.8% (20.5 hours)
Conditions
rain
snow
fog
Dec 31–Jan 6
Jan 7–Jan 13
Jan 14–Jan 20
Jan 21–Jan 27
Jan 28–Feb 3
fog: 19.9% (2.9 days) | rain: 15.3% (2.2 days) | snow: 3.5% (12.2 hours)

Vérification des zones à l'est, Strasbourg est éliminé en plus des conditions météo (pas de neige). Besançon éliminée également, ça laisse donc penser qu'il s'agit d'une zone dans le Nord de la France, potentiellement Lille et Paris grand maximum.

Je pouvais penser également à l'ouest, Reims, etc.

WolframAlpha computational intelligence

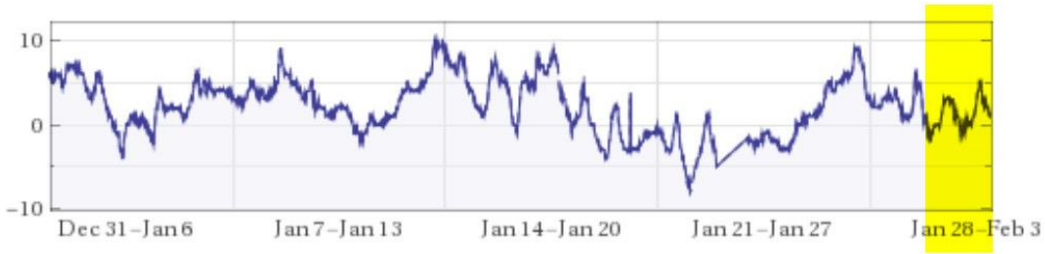
Weather Strasbourg January 2019

Upload Examples Random

Weather history:

Month

Temperature

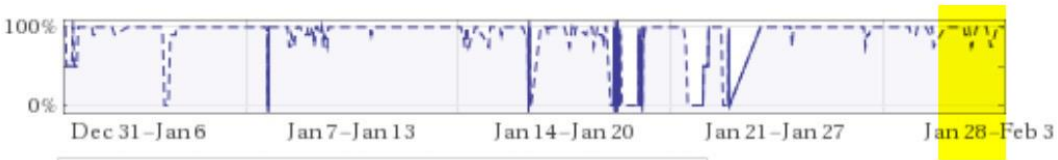


low: −8 °C
Tue, Jan 22, 1:30am

average high: 5 °C
average low: −1 °C

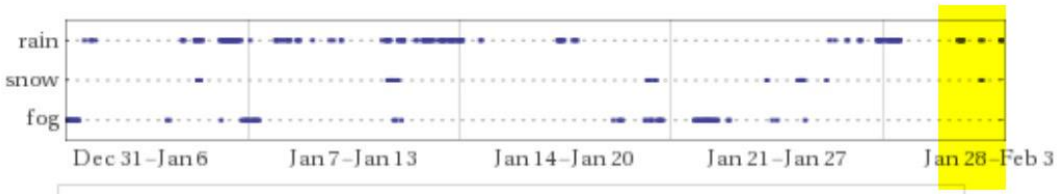
high: 10 °C
Sun, Jan 13, 3:30pm, ...

Cloud cover



overcast: 66.2% (10.8 days) | clear: 6.7% (1.1 days)

Conditions



rain: 23.6% (3.9 days) | fog: 9.6% (1.6 days) | snow: 4.5% (17.5 hours)

WolframAlpha computational intelligence

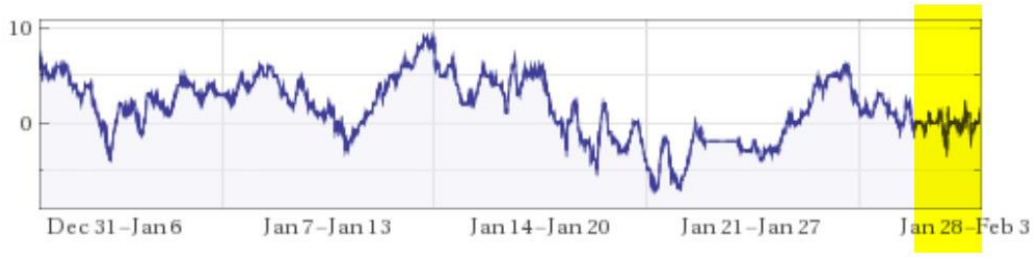
Weather Metz January 2019

Upload Examples Random

Weather history:

Month

Temperature



low: −7 °C
Mon, Jan 21, 8:00am

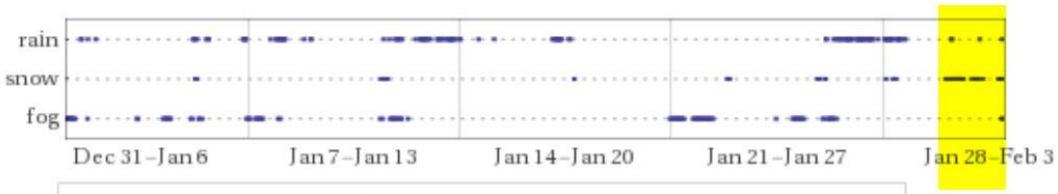
average high: 3 °C
average low: −1 °C

high: 9 °C
Sun, Jan 13, 3:30pm, ...

Cloud cover

overcast: 69.4% (11.6 days) | clear: 6.3% (1.1 days)

Conditions



rain: 17.8% (3 days) | fog: 12.7% (2.1 days) | snow: 7% (1.2 days)

WolframAlpha computational intelligence

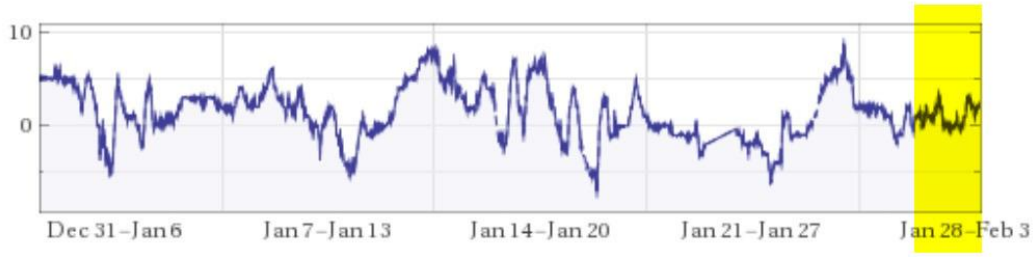
Weather Besançon January 2019

Upload Examples Random

Weather history:

Month

Temperature

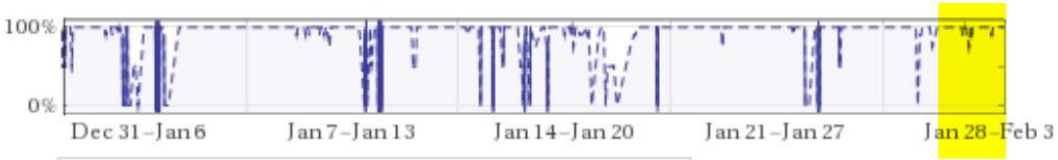


low: −7 °C
Sat, Jan 19, 8:30am

average high: 4 °C
average low: −1 °C

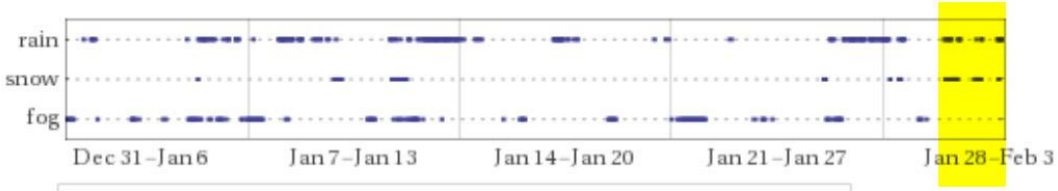
high: 9 °C
Sun, Jan 27, 12:00pm

Cloud cover



overcast: 69% (12.1 days) | clear: 4.5% (19 hours)

Conditions



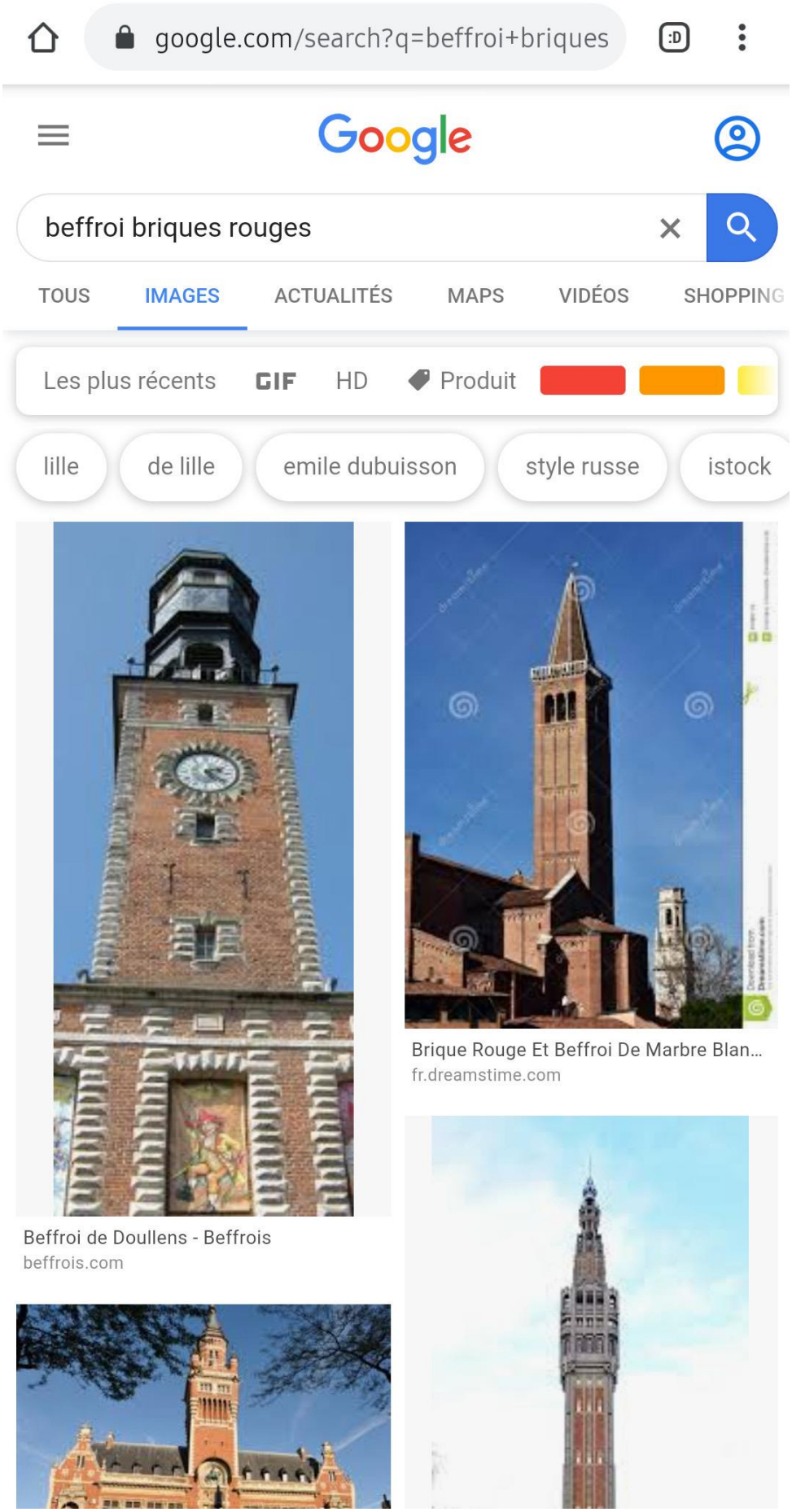
rain: 28% (4.9 days) | fog: 17% (3 days) | snow: 5.7% (1 day)

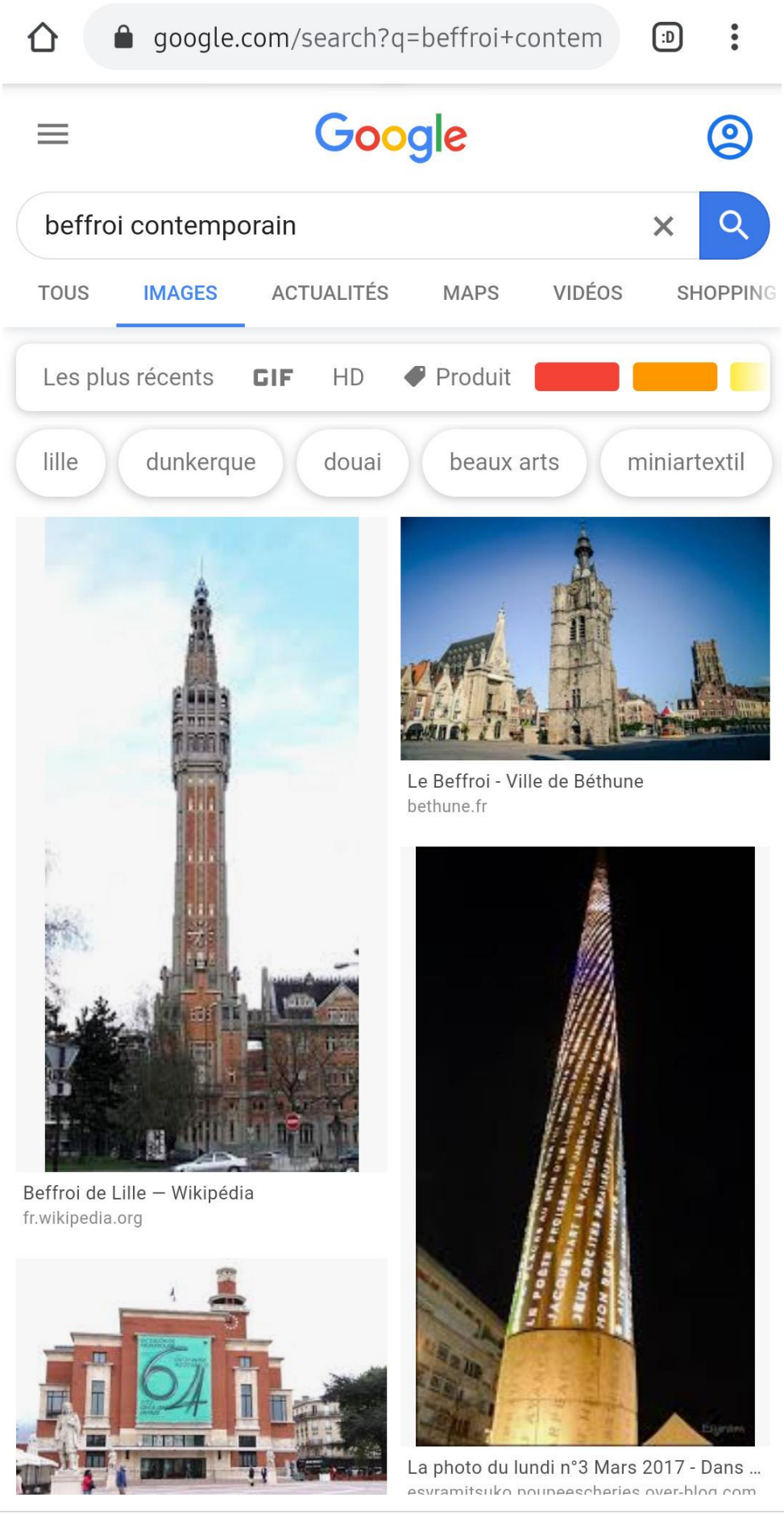
En analysant les éléments de fond de la photo, on peut distinguer un beffroi et des briques rouges. Ces dernières sont très caractéristiques des villes du Nord/Nord-Ouest.

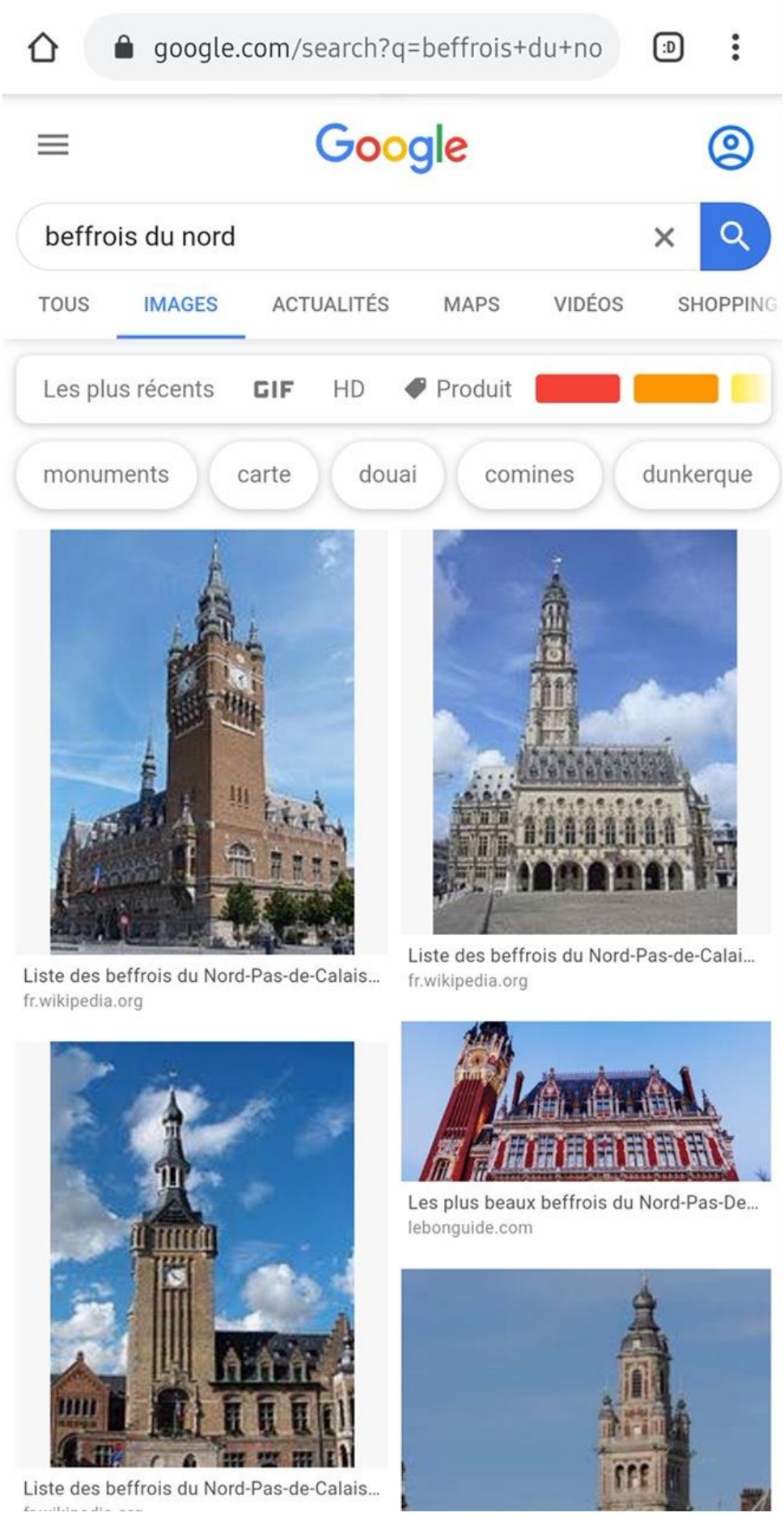
Par contre, le beffroi n'est pas très classique, ce qui donne un indice de plus.

Via Google images, recherche des différents beffrois.

Il s'agit souvent de monuments historiques mais là, nous pouvons clairement voir qu'il s'agit d'un monument moderne/contemporain, aucun résultat via la méthode Google image simple.


google.com/search?q=beffroi+briques
Google
beffroi briques rouges
TOUS
IMAGES
ACTUALITÉS
MAPS
VIDÉOS
SHOPPING
Les plus récents
GIF
HD
Produit
lille
de lille
emile dubuisson
style russe
istock
Brique Rouge Et Beffroi De Marbre Blan...
fr.dreamstime.com
Beffroi de Doullens - Beffrois
beffrois.com


google.com/search?q=beffroi+contem
Google
beffroi contemporain
TOUS
IMAGES
ACTUALITÉS
MAPS
VIDÉOS
SHOPPING
Les plus récents
GIF
HD
Produit
lille
dunkerque
douai
beaux arts
miniartextil
Le Beffroi - Ville de Béthune
bethune.fr
Beffroi de Lille — Wikipédia
fr.wikipedia.org
La photo du lundi n°3 Mars 2017 - Dans ...


google.com/search?q=beffrois+du+no
Google
beffrois du nord
TOUS
IMAGES
ACTUALITÉS
MAPS
VIDÉOS
SHOPPING
Les plus récents
GIF
HD
Produit
monuments
carte
douai
comines
dunkerque
Liste des beffrois du Nord-Pas-de-Calais...
fr.wikipedia.org
Liste des beffrois du Nord-Pas-de-Calai...
fr.wikipedia.org
Liste des beffrois du Nord-Pas-de-Calais...
Les plus beaux beffrois du Nord-Pas-De...
lebonguide.com


google.com/search?q=beffroi+carte&t
Google
beffroi carte
TOUS
IMAGES
ACTUALITÉS
MAPS
VIDÉOS
SHOPPING
Les plus récents
GIF
HD
Produit
belgique
cdv albumen
ebay
bruges
vieux beffro
Beffrois de Belgique et de France — Wiki...
fr.wikipedia.org
BEFFROIS
medieval.mrugala.net
les carillons en Nord-Pas de Calais
LA REGION
asso.nordnet.fr
U.K.
Netherlands
Belgium
Germany
France
Lux.
Beffrois de Belgique et de France
fracademic.com
La Région des beffrois - Réflexions Nord...
pourlenordpasdecalais.over-blog.com
Sites français inscrits au patrimoine mondial de l'UNESCO (2017)
N

Wikipédia

Beffrois de Belgique et de France — Wikipédia

Consulter

Les images peuvent être soumises à des droits d'auteur. **En savoir plus**

Images similaires

fil, info, belgique, carte, info, belgique, c...

fil-info-france.com

Carte de la Belgique - Découvrir plusieur...

actualitix.com

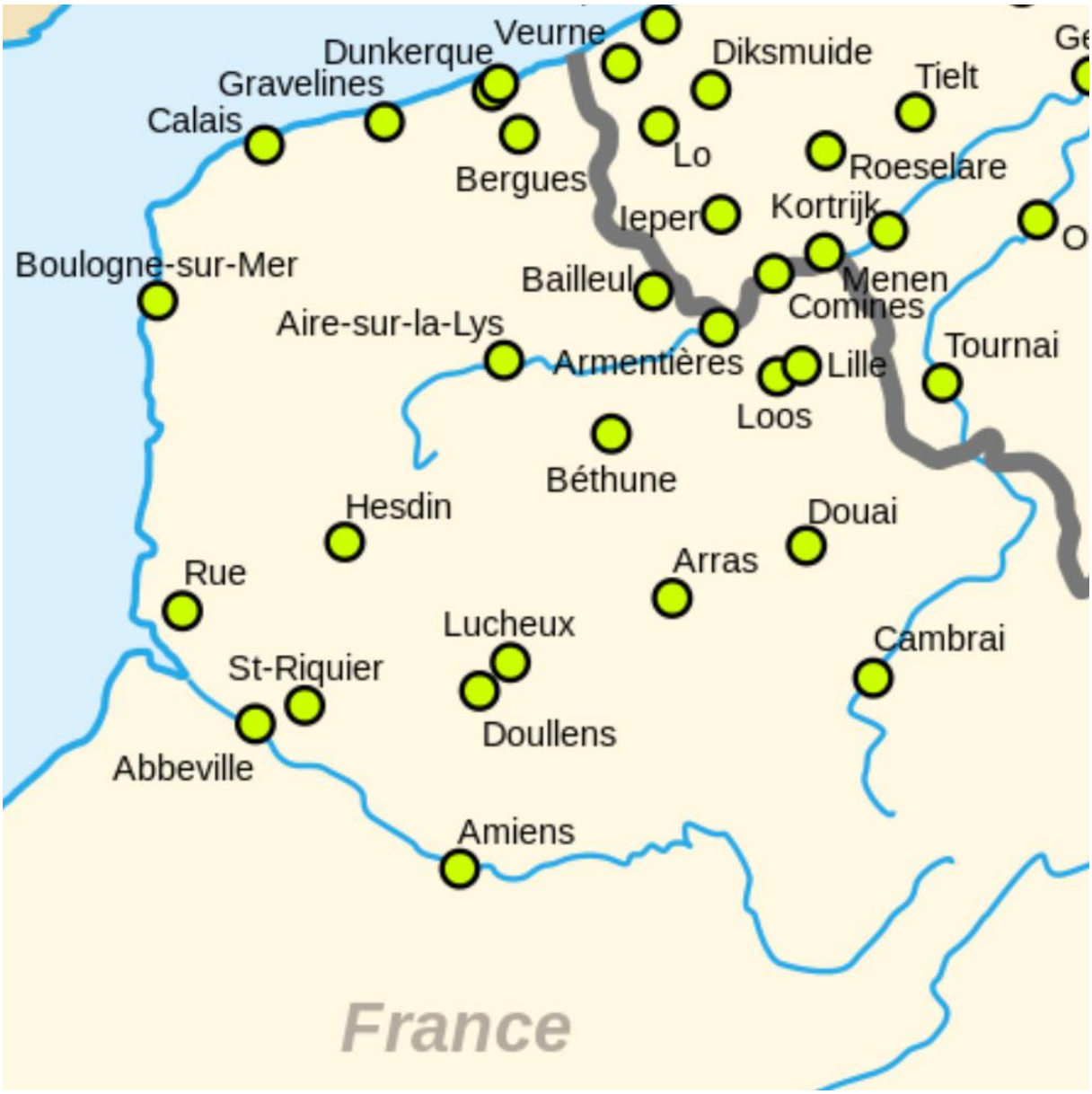
Passage à une recherche web d'une page listant les différents beffrois en France.

Cette dernière donne une carte des beffrois.

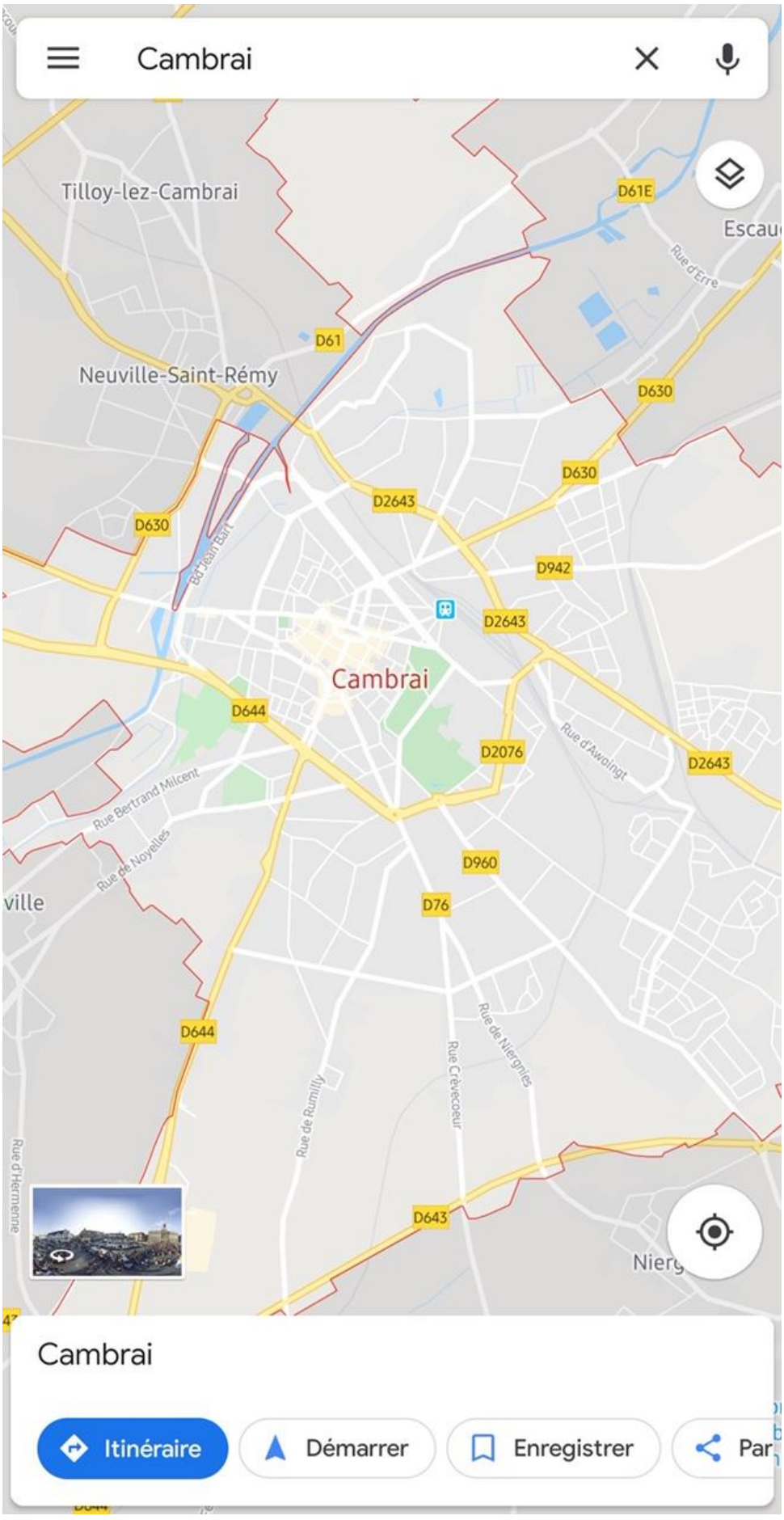
Nous avons donc une image de base avec un beffroi en fond et de l'eau en premier plan, ce qui indique qu'il y a une rivière à proximité.

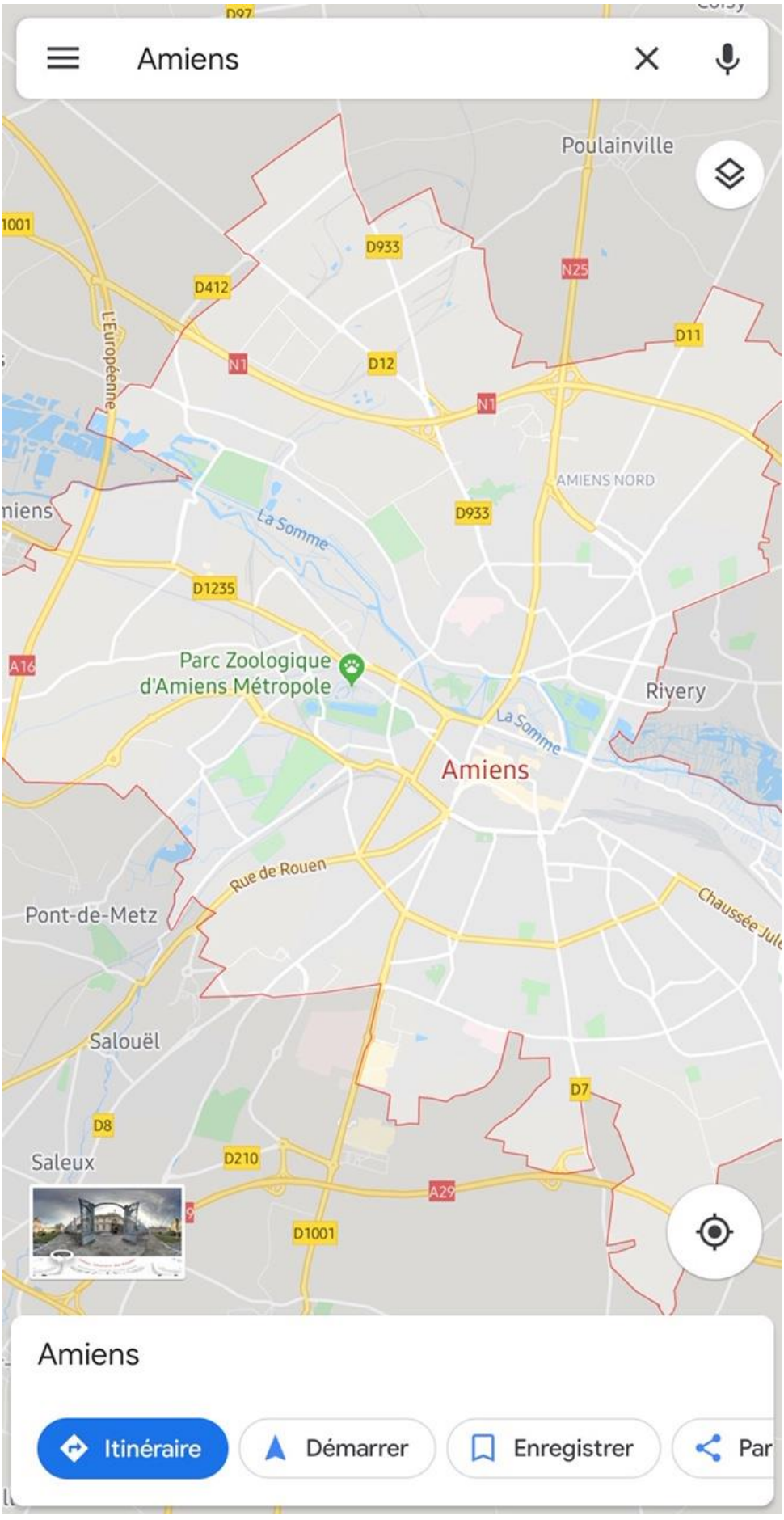
Une étendue d'eau où la glace n'est pas uniforme donc un lac (sinon la glace serait plateformée)

Partons sur cette hypothèse avec risque de fausse piste et retour aux étapes précédentes.



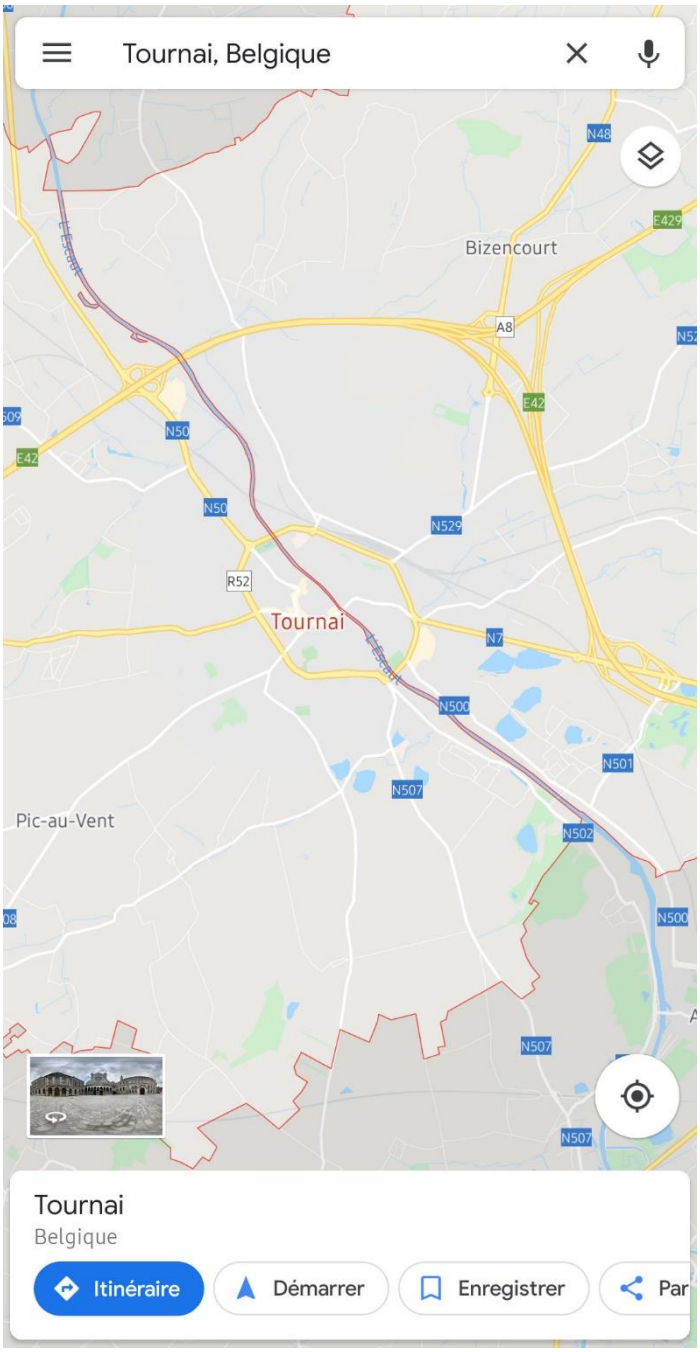
En regardant le plan des villes où les beffrois sont listés par le site précédent, nous allons tenter de trouver un lac et beaucoup ne collent pas. Typiquement Cambrai, Amiens peut-être, mais trop vaste donc pas de conclusion.


Cambrai
Tilloy-lez-Cambrai
D61E
Escau
Rue d'Erre
D61
Neuville-Saint-Rémy
D630
D630
D2643
D630
Bd Jean Bart
D942
D2643
Cambrai
D644
D2076
Rue d'Awoingt
D2643
Rue Bertrand Milcent
Rue de Noyelles
D960
ville
D76
D644
Rue de Nierguies
Rue Crèvecoeur
Rue de Rumilly
Rue d'Hermenne
D643
Nier
Cambrai
Itinéraire
Démarrer
Enregistrer
Par

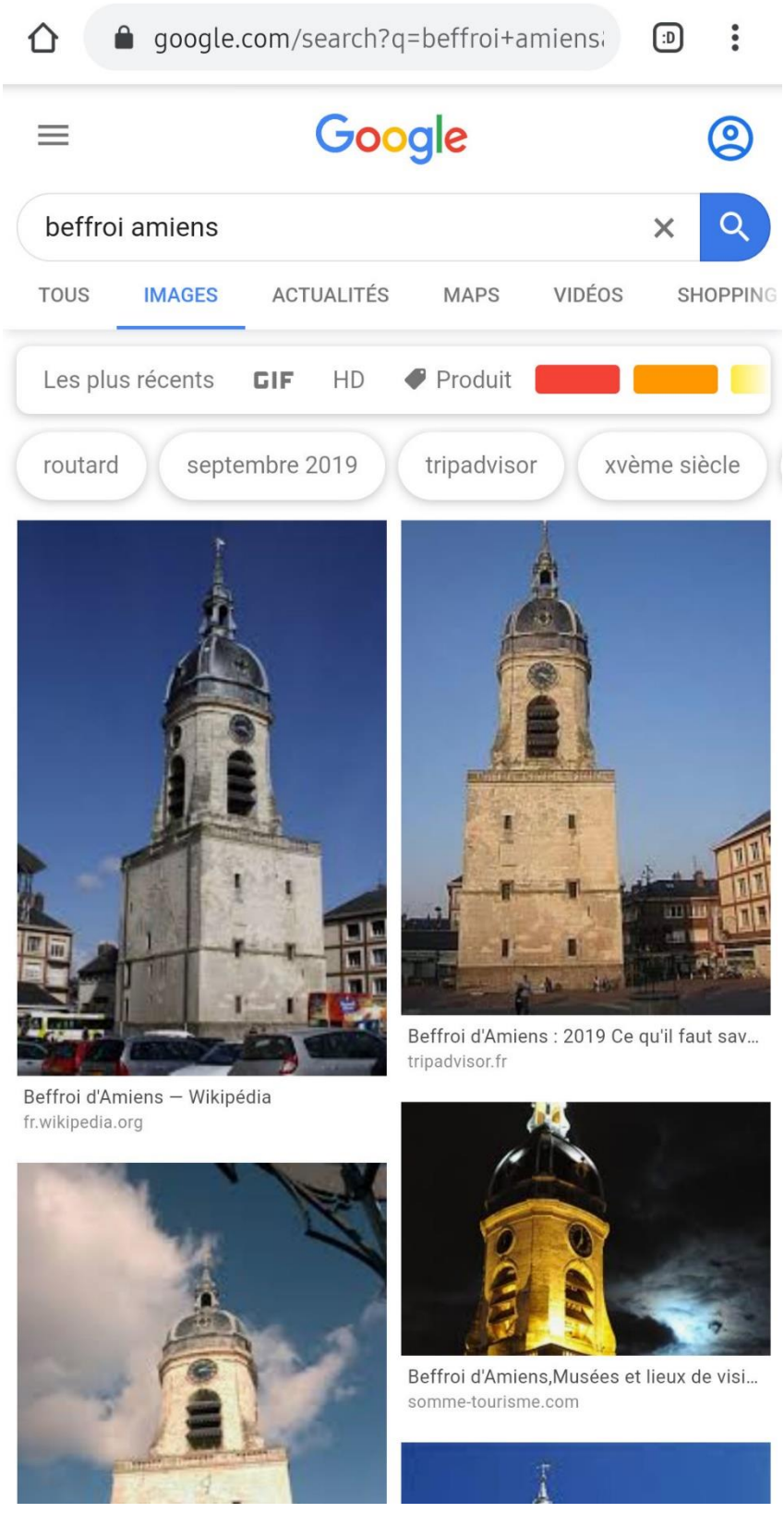

Amiens
Poulainville
D933
N25
D412
D11
N1
D12
N1
AMIENS NORD
D933
La Somme
D1235
Parc Zoologique
d'Amiens Métropole
Rivery
La Somme
Amiens
Rue de Rouen
Pont-de-Metz
Salouël
D7
D8
Saleux
D210
A29
D1001
Amiens
Itinéraire
Démarrer
Enregistrer

Tournai également, l'individu aurait pu être en Belgique zone francophone.

Retour sur Amiens, recherche des monuments historiques sans résultat mais je remarque une tour, comme sur la photo d'origine, aucun résultat.



Toujours avec le risque de fausse piste, je retourne sur la « piste Amiens »



Le beffroi d'Amiens : Beffroi d'Amiens : ...
routard.com

Amiens : présentation des anciennes pri...
criminocorpus.hypotheses.org

Beffroi d'Amiens,Musées et lieux de visit...
somme-tourisme.com

Beffroi d'Amiens - Des Voyages et des ...
desvoyagesetdesmots.fr

Recherches associées

tour amiens

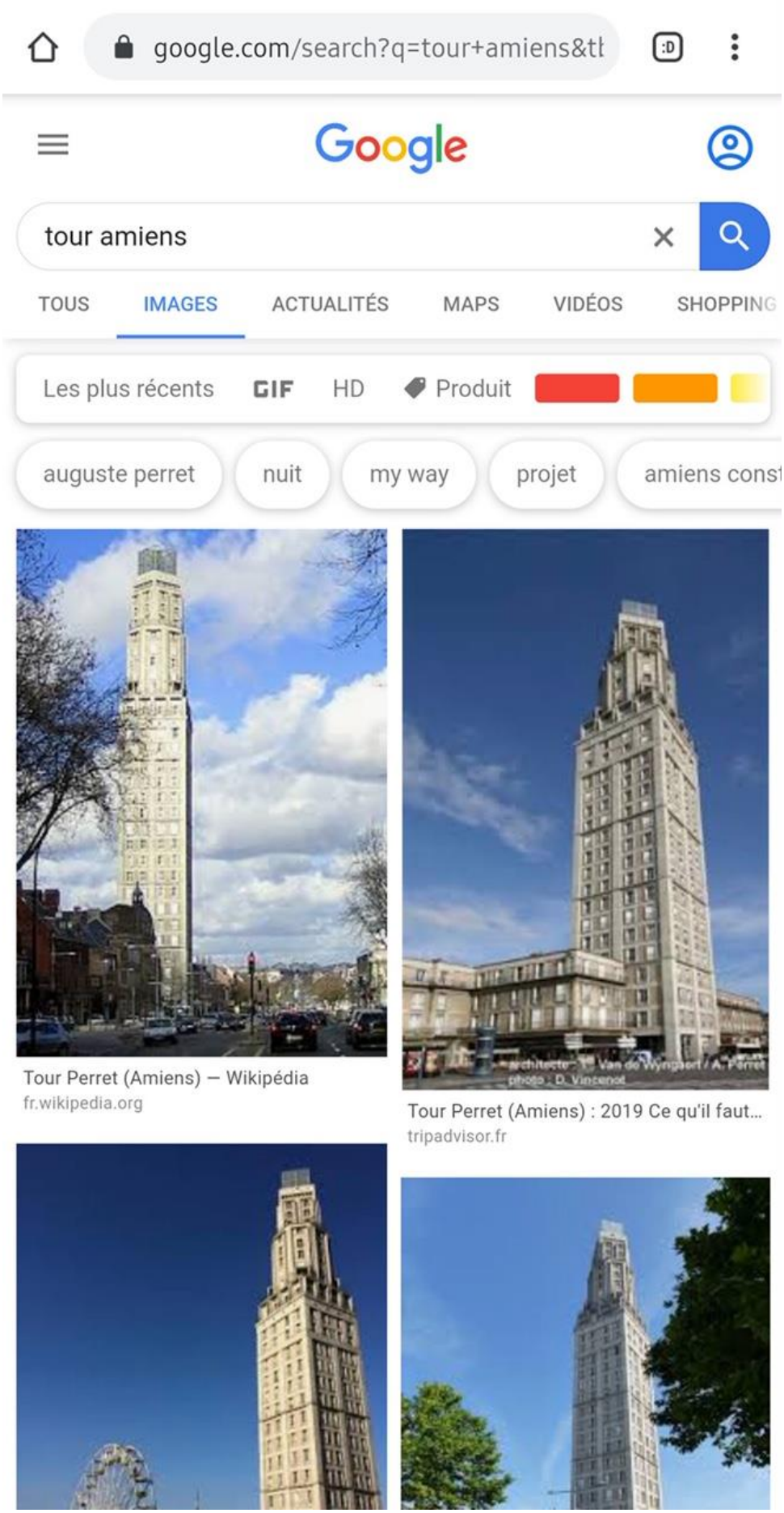
hotel de ville amiens

monument amiens

beffroi douai

Le beffroi d'Amiens – Nord Escapade
nord-escapade.com

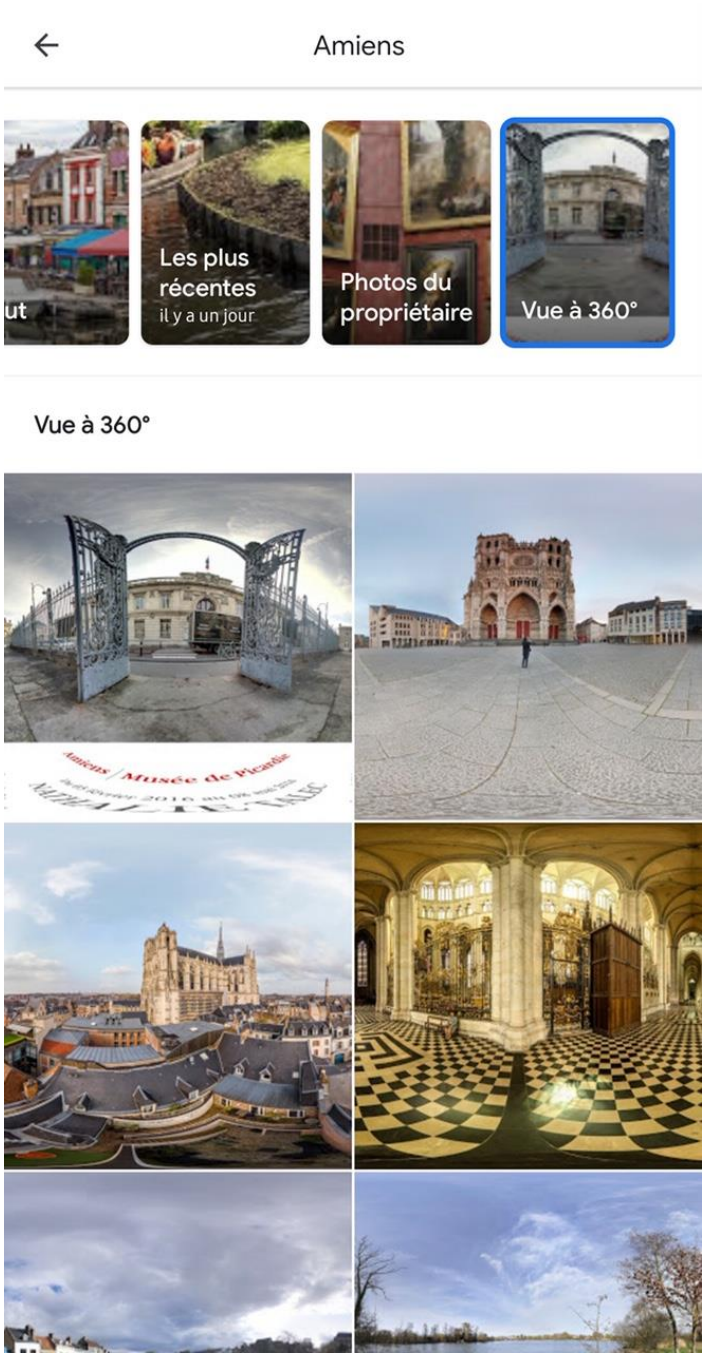
Beffroi d'Amiens à Amiens: 2 expérienc...
monnuage.fr

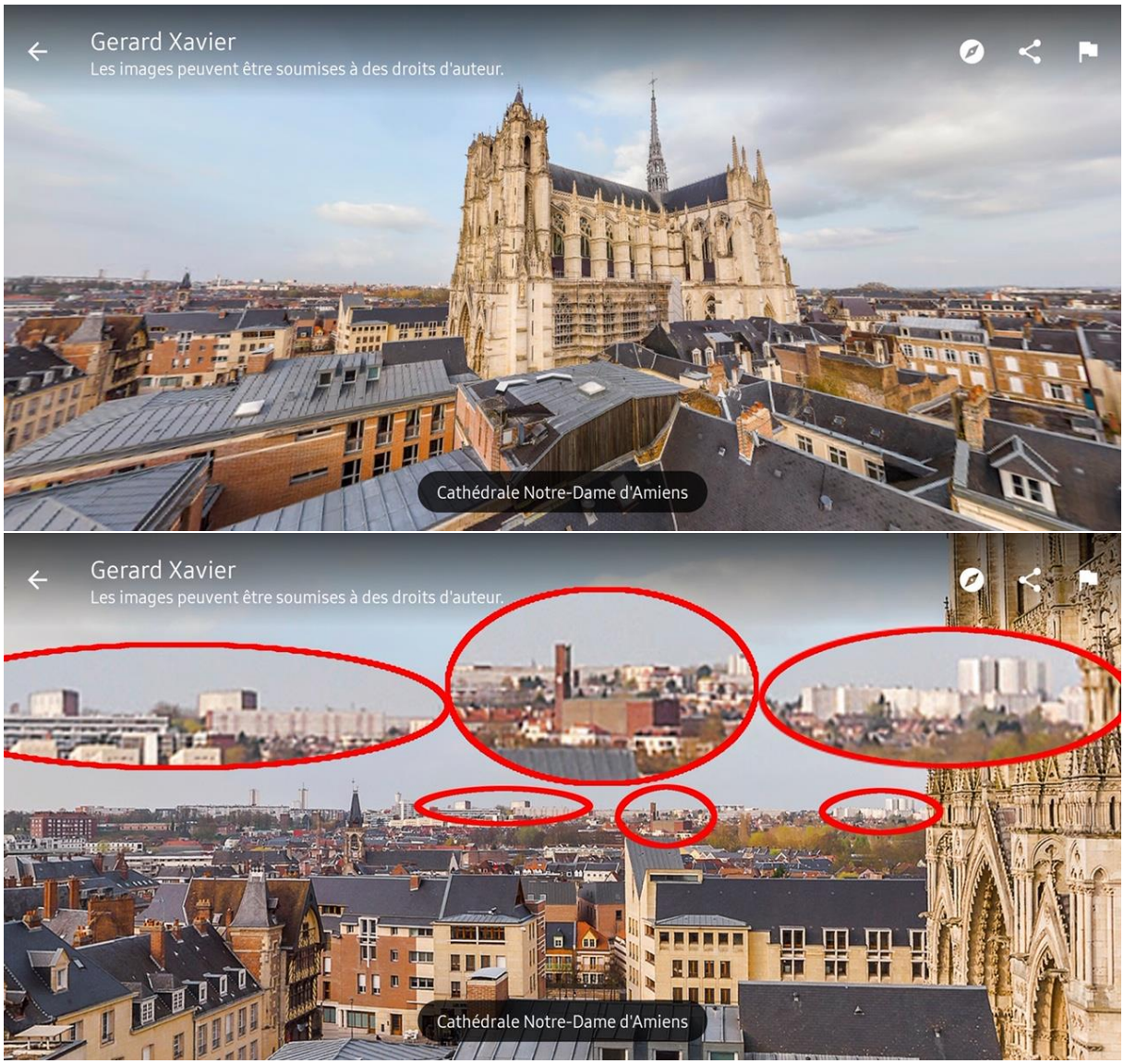

google.com/search?q=tour+amiens&tl
Google
tour amiens
TOUS
IMAGES
ACTUALITÉS
MAPS
VIDÉOS
SHOPPING
Les plus récents
GIF
HD
Produit
auguste perret
nuit
my way
projet
Tour Perret (Amiens) — Wikipédia
fr.wikipedia.org
Tour Perret (Amiens) : 2019 Ce qu'il faut...
tripadvisor.fr

Retour sur Google maps avec recherche sur des photos à 360°, idéalement en hauteur.

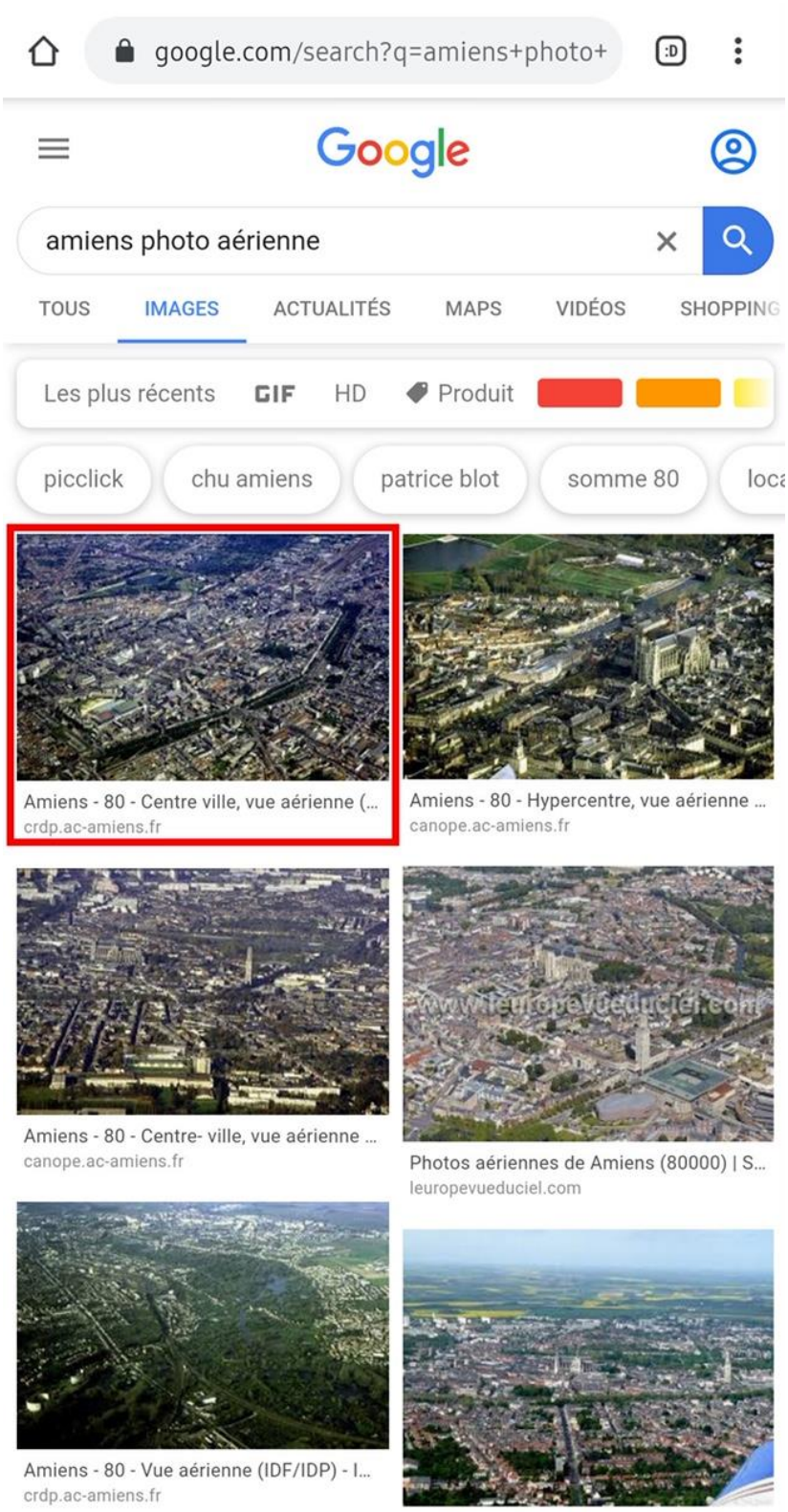
Sélection d'une photo avec ces critères proches de la cathédrale et zoom sur les hauteurs de la ville en panoramique, certains éléments collent avec la photo d'origine.

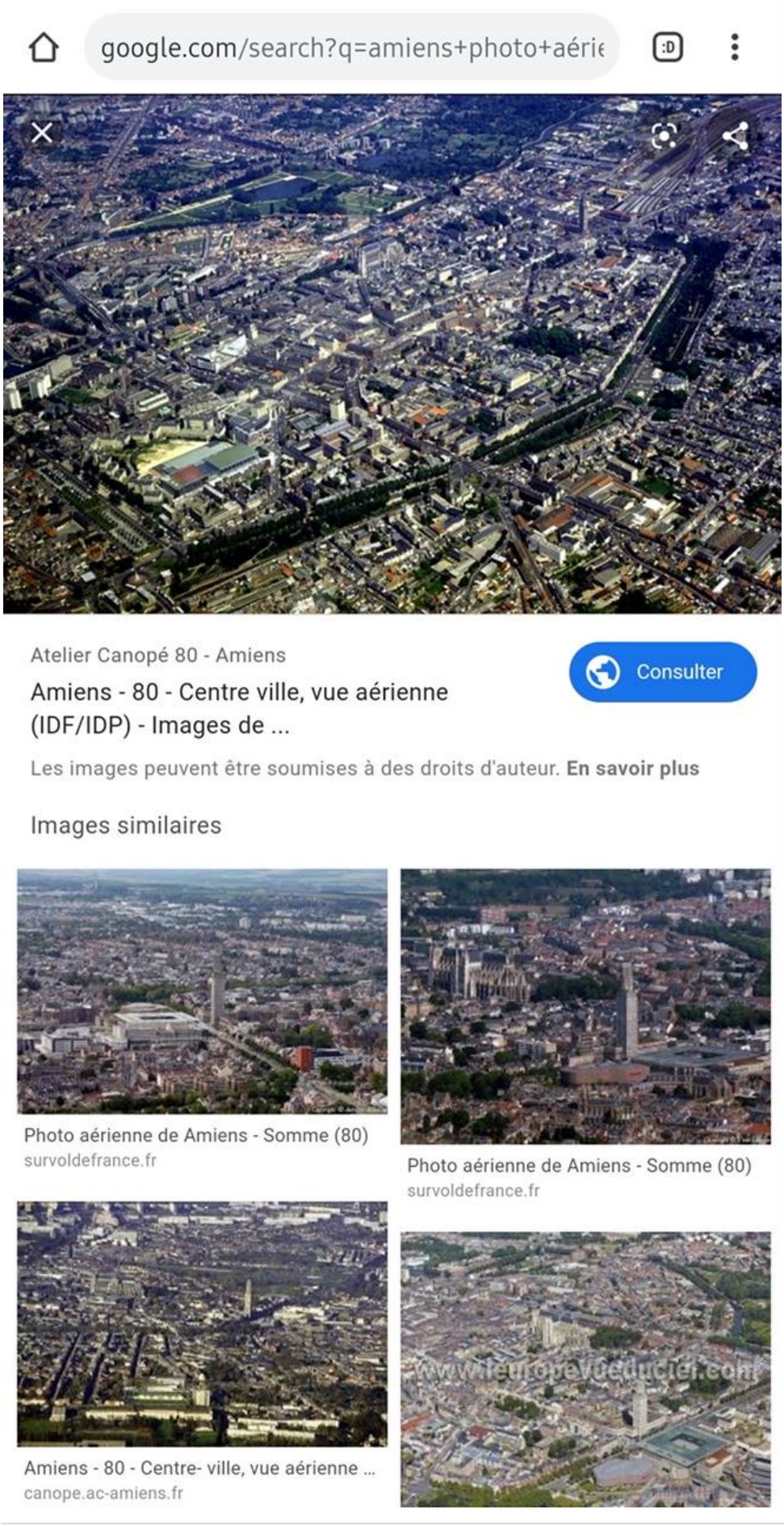
Au fond, à côté de la cathédrale plusieurs éléments semblent matcher mais c'est encore trop imprécis.





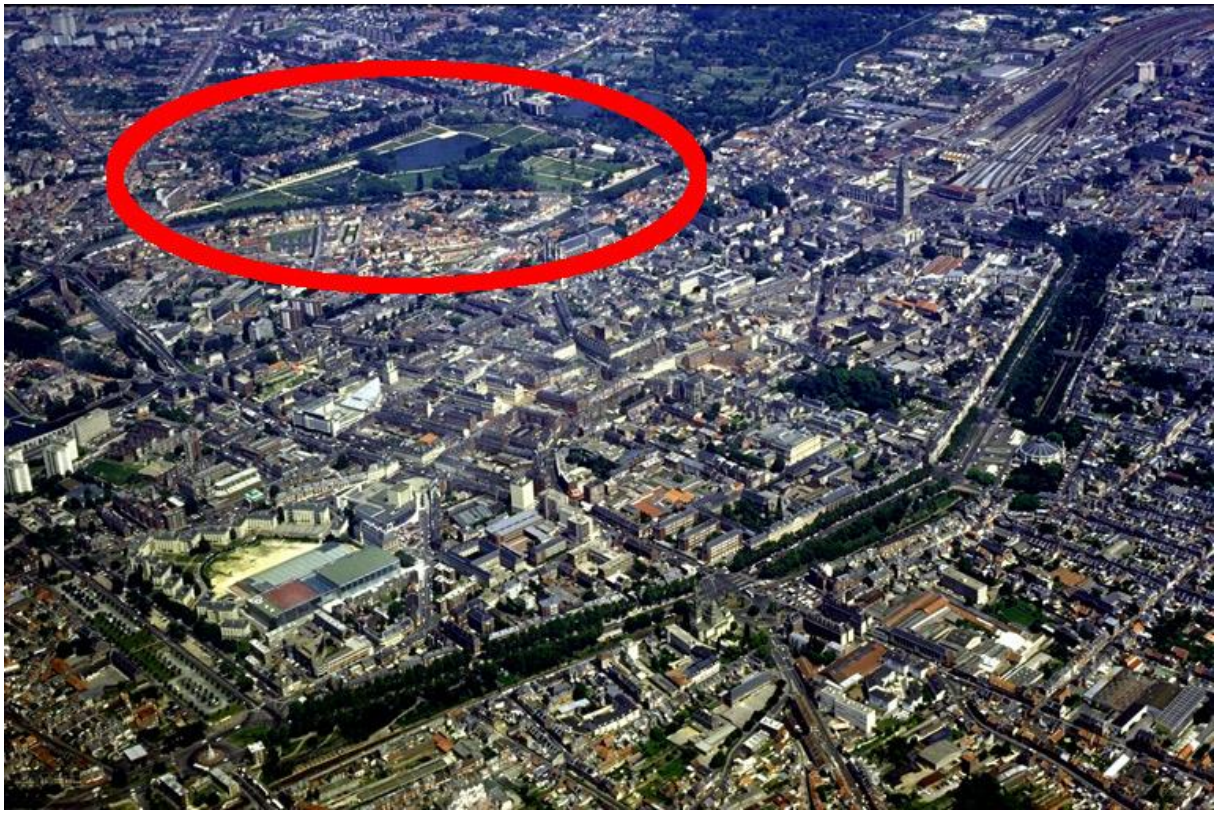
Poursuite de la recherche dans cette zone via des photos aériennes sur Google avec la simple requête :« Amiens photo aérienne », Les photos satellites ne sont pas assez précises et nous arrivons facilement au flou, trop plat pour repérer les bâtiments.


google.com/search?q=amiens+photo+
Google
amiens photo aérienne
TOUS
IMAGES
ACTUALITÉS
MAPS
VIDÉOS
SHOPPING
Les plus récents
GIF
HD
Produit
picclick
chu amiens
patrice blot
somme 80
Amiens - 80 - Centre ville, vue aérienne (...
crdp.ac-amiens.fr
Amiens - 80 - Hypercentre, vue aérienne ...
canope.ac-amiens.fr
Amiens - 80 - Centre- ville, vue aérienne ...
canope.ac-amiens.fr
Photos aériennes de Amiens (80000) | S...
leuropevueduciel.com
Amiens - 80 - Vue aérienne (IDF/IDP) - I...
crdp.ac-amiens.fr


google.com/search?q=amiens+photo+aérie
Atelier Canopé 80 - Amiens
Amiens - 80 - Centre ville, vue aérienne (IDF/IDP) - Images de ...
Consulter
Les images peuvent être soumises à des droits d'auteur. En savoir plus
Images similaires
Photo aérienne de Amiens - Somme (80)
survoldefrance.fr
Photo aérienne de Amiens - Somme (80)
survoldefrance.fr
Amiens - 80 - Centre- ville, vue aérienne ...
canope.ac-amiens.fr

J'arrive donc à identifier une zone avec un lac et de l'herbe donc un parc autour.

Le parc semble donc être l'endroit où a été prise la photo mais la recherche continue afin d'être sûr.



canope.ac-amiens.fr

Amiens - 80 - Hypercentre, vue aérienne (IDF/IDP) - Images de Picardie

Consulter

Les images peuvent être soumises à des droits d'auteur. **En savoir plus**

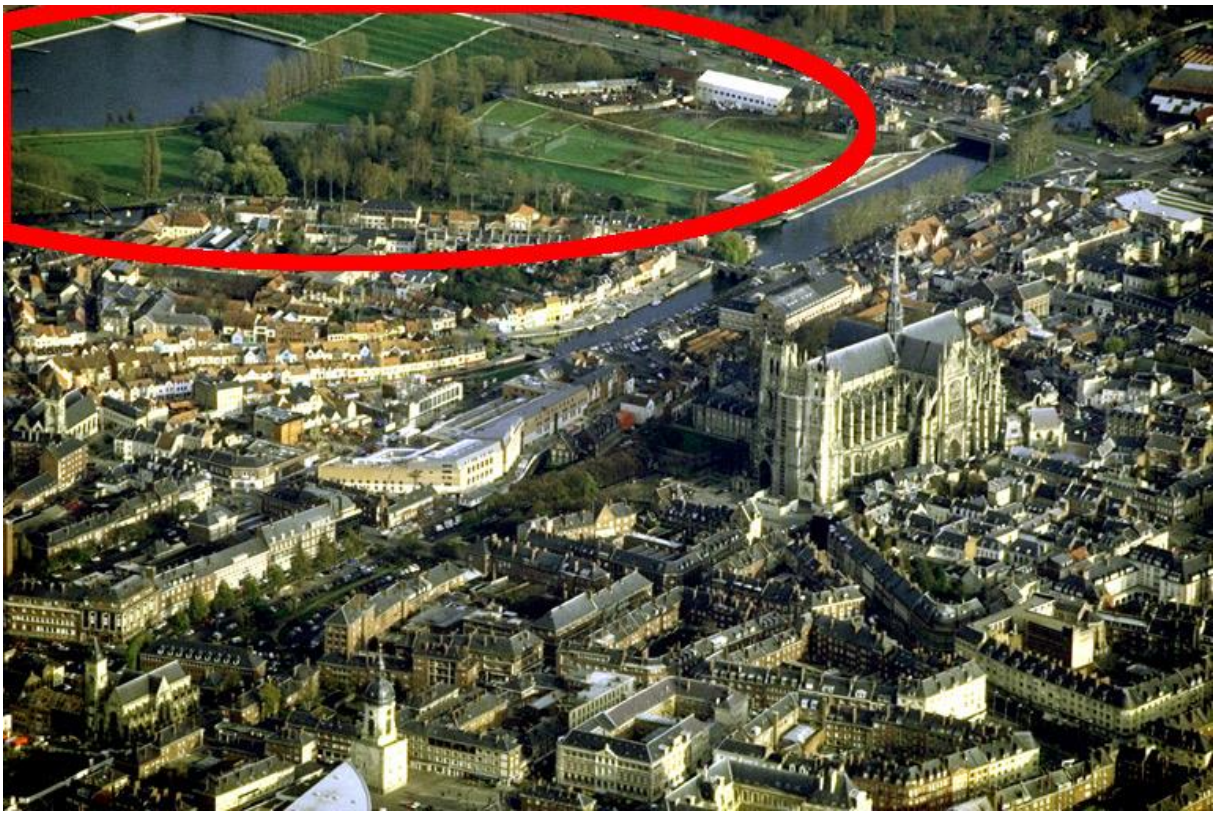
Images similaires

Amiens - 80 - Cathédrale, vue aérienne (I...
canope.ac-amiens.fr

Photo aérienne de Amiens - Somme (80)
survoldefrance.fr

Photos aériennes de Amiens (80000) | S...
leuropevueduciel.com

Amiens - 80 - Centre- ville, vue aérienne ...
canope.ac-amiens.fr



Vue aérienne d'Amiens avec la cathédral...
alamyimages.fr

Amiens - 80 - Quartier de la Vallée des V...
canope.ac-amiens.fr

Photo aérienne de Amiens - Somme (80)
survoldefrance.fr

Amiens - 80 - Parc Saint Pierre, vue aéri...
canope.ac-amiens.fr

L'isolation vue d'en haut - Amiens Métro...
amiens.fr

Autour d'Amiens / La culturelle - Amiens...
amiens-tourisme.com

Amiens - Vue aérienne du quartier Etouv...
anru.fr

13480932 AMIENS VUE aérienne Amien...
picclick.fr

Atelier Canopé 80 - Amiens

Amiens - 80 - Parc Saint Pierre, vue aérienne - Images de Picardie

Consulter

Les images peuvent être soumises à des droits d'auteur. **En savoir plus**

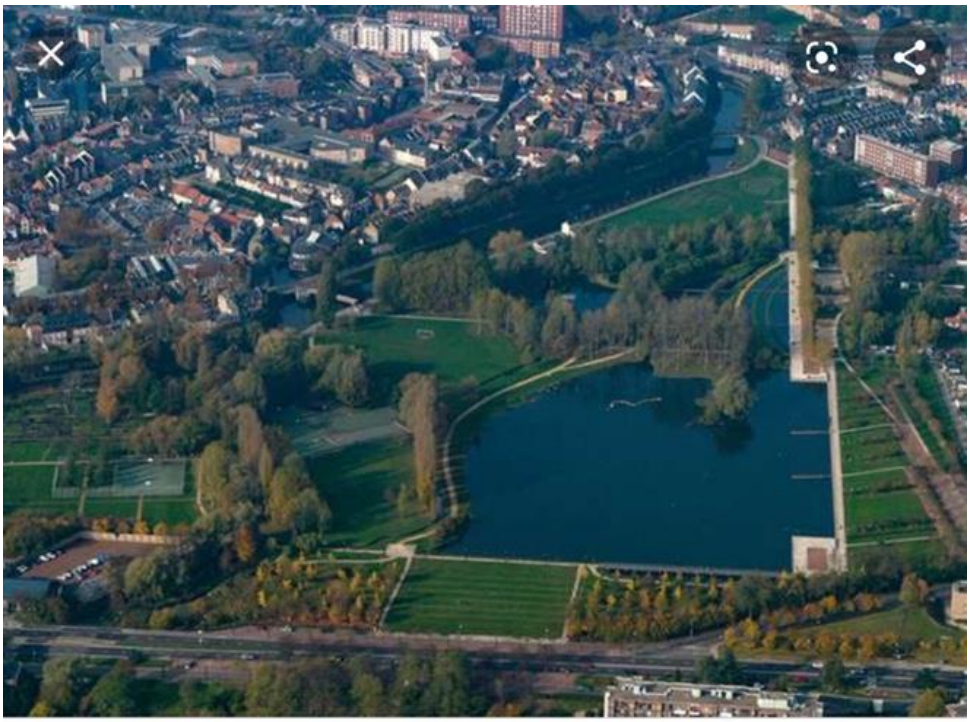
Images similaires

Travaux d'aménagement du parc Saint-P...
amiens.fr

PARC SAINT PIERRE AMIENS
aesgsf.free.fr

Amiens - 80 - Parc Saint Pierre et quarti...
canope.ac-amiens.fr

Amiens - 80 - Hypercentre, vue aérienne ...
canope.ac-amiens.fr



www.amiens.fr

Travaux d'aménagement du parc Saint-Pierre - Amiens Métropole

Consulter

Les images peuvent être soumises à des droits d'auteur. **En savoir plus**

Images similaires

Amiens - 80 - Parc Saint Pierre, vue aéri...
canope.ac-amiens.fr

Amiens : les activités du Parc Saint-Pier...
evasionfm.com

Amiens - 80 - Les Hortillons - Images de...
canope.ac-amiens.fr

PARC SAINT PIERRE AMIENS
aesgsf.free.fr

gazettesports.fr

[HORS-CHAMPS] FERMETURE TEMPORAIRE DE LA BAIGNADE AU PARC ST PIERRE ! -...

Consulter

Les images peuvent être soumises à des droits d'auteur. **En savoir plus**

Images similaires

Amiens - 80 - Parc Saint-Pierre - Images ...
canope.ac-amiens.fr

Parc Saint Pierre d'Amiens - Photo de P...
tripadvisor.fr

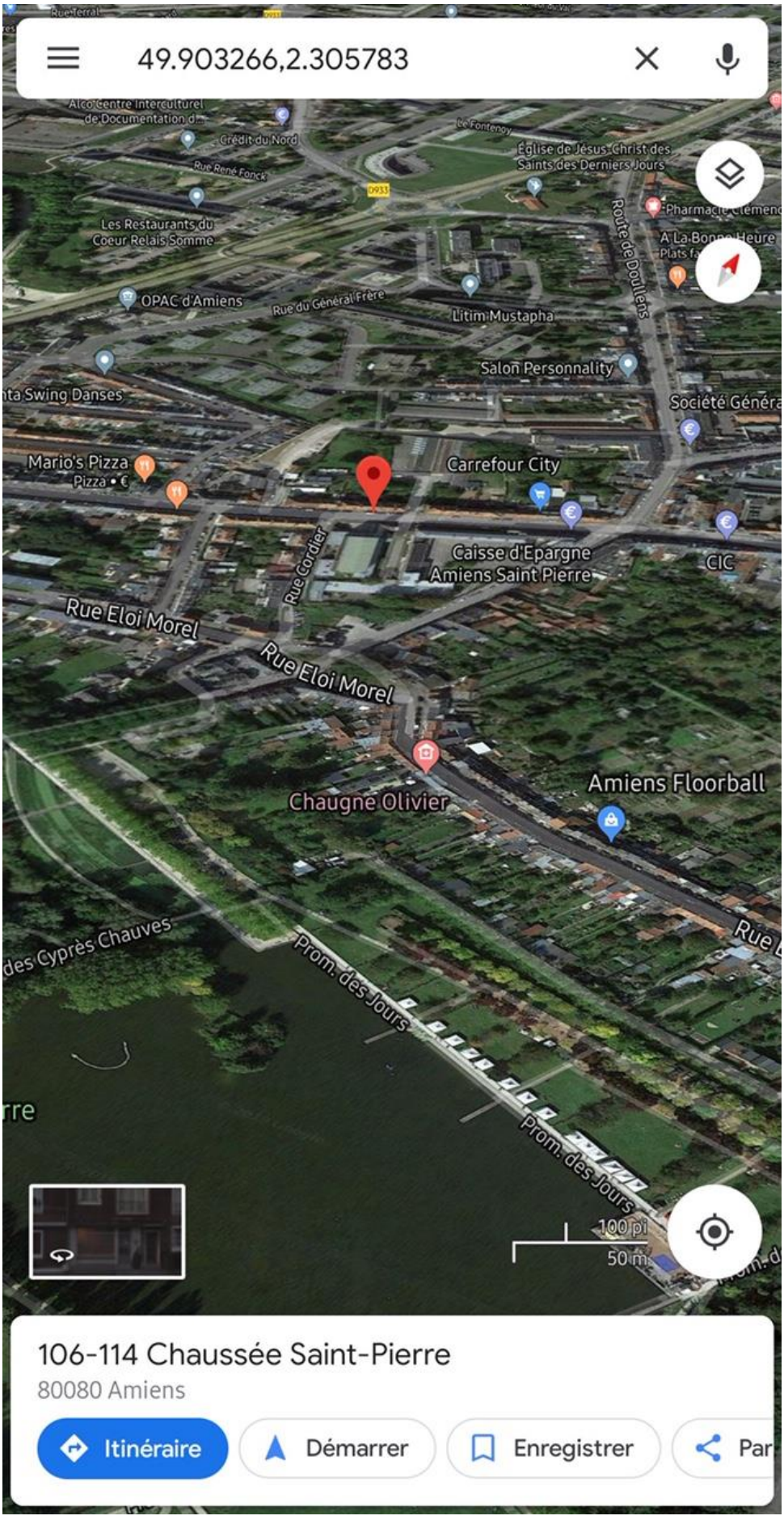
Amiens : du nouveau dans l'accès au Pa...
evasionfm.com

Parc Saint-Pierre,Parcs et Jardins,

Pour me "balader" dans le parc, passage de Google photo aérienne à Google Street View (parc saint pierre, Amiens).

L'endroit est le bon, maintenant, je tente d'identifier l'emplacement exact où a été prise la photo.

Retour sur Google Maps, "parc saint pierre" pour voir si je peux retrouver le point de vue de la personne à l'origine de la photo et retour sur Street View : Emplacement exact identifié


49.903266,2.305783
Alco Centre Interculturel de Documentation d...
Crédit du Nord
Rue René Fonck
Le Fontenoy
Église de Jésus-Christ des Saints des Derniers Jours
Les Restaurants du Coeur Relais Somme
Route de Doullens
OPAC d'Amiens
Rue du Général Frère
Litim Mustapha
Salon Personnality
Mario's Pizza
Pizza • €
Carrefour City
Caisse d'Epargne Amiens Saint Pierre
CIC
Rue Cordier
Rue Eloi Morel
Rue Eloi Morel
Chaugne Olivier
Amiens Floorball
des Cyprès Chauves
Prom. des Jours
Prom. des Jours
100 pi
50 m
106-114 Chaussée Saint-Pierre
80080 Amiens
Itinéraire
Démarrer
Enregistrer


49.903311,2.305875
Tchip
La Myrtille
Carrefour City
Eglise Saint-Pierre d'Amiens
Ecole élémentaire Saint-Pierre
Caisse d'Epargne Amiens Saint Pier
Paroisse Saint Pierre
Rue des Bonnards
Rue Cordier
Rue Decourt
Rue Eloi Morel
100 pi
20 m
127-115 Chaussée Saint-Pierre
80080 Amiens
Itinéraire
Démarrer
Enregistrer
Par

Je finis par la recherche des détails de la photo et tout colle parfaitement.

Cette recherche a été faite simplement via un smartphone. Tout le monde peut accéder aux outils et pour réaliser ce genre de chose, il faut également s'armer de patience.

Sur PC, vous avez de meilleures chances de localisations car les photos en 360 sont plus exploitables pour de la géolocalisation à 99% (exemple ici)

Cette démo de GEOINT a été réalisée en 40 minutes.

Cas d'OSINT / GEOINT dans l'histoire d'internet

Le plus connu étant le conflit opposant Shia LABOEUF au forum 4Chan. Les utilisateurs ayant eu recours à des techniques comme la localisation via la position des étoiles et l'analyse du trafic aérien via flightradar24.

Le dox du compte twitter @Avec_Marlene a également été fait via une procédure de reset et de l'OSINT. Comme l'a décrit le journal Libération :

« La démarche est assez simple : l'internaute essaye de se connecter au compte Twitter @Avec_Marlene. Le réseau social lui indique qu'il est associé à l'adresse *«av**********@g****.***»* (ce n'est dorénavant plus le cas, a constaté CheckNews). L'internaute essaye ensuite de se connecter à la boîte Gmail (la messagerie de Google) *« avecmarleneschiappa@gmail.com »*. Cette adresse existe bien : nous lui avons envoyé un mail, resté sans réponse.

L'internaute constate ensuite que l'adresse de récupération de ce compte Gmail, c'est-à-dire l'adresse de secours pour récupérer le mot de passe du compte, est une autre adresse Gmail. Elle commence par *« mpo… »* (la suite est masquée par Google). Ces trois lettres amènent l'internaute à faire le lien avec Mathieu Pontécaille, *« conseiller spécial, chargé de la stratégie communication et de la* presse» au sein du cabinet de Marlène Schiappa. Mathieu Pontécaille possède bien une adresse Gmail commençant par « mpo », a constaté CheckNews. »

Par contre, il manque une étape : Pour arriver au nom de Mathieu Pontécaille, je suis allé sur le site du ministère attribué à Mme Schiappa et j'ai simplement vérifié les noms de ses assistants. Le mail de récupération commençant par mpo…. Correspondait à Mathieu Pontécaille qui possédait également un compte Twitter avec cette adresse.

Juste pour le fun, saviez-vous qu'il était possible de localiser Donald TRUMP en temps-réel au début de son mandat ?

En effet, il utilisait au départ son mobile Android (Samsung Galaxy S3) non sécurisé et avait laissé la géolocalisation activée…

Via une API, nous avions eu avec @Donot3sk, la possibilité de le suivre selon ses tweets et de faire un « rapport » de ses habitudes hebdomadaires.

A vous de trouver la méthode et de revenir vers moi ! ☺

Mot de la fin

Ce document étant très probablement l'un des premiers supports francophones ayant été publié à ce sujet, il me sert essentiellement à vous introduire candidement à ce domaine et également à capturer la demande et l'engouement réels derrière cette pratique.

Vous l'aurez compris, le monde de l'OSINT est encore très méconnu et sa communauté reste extrêmement imperméable aux néophytes, raison pour laquelle je me propose de jouer le rôle du guide, et de vous introduire graduellement à cette pratique.

Toutefois, afin de m'éviter de lourdes représailles ainsi que des impacts négatifs trop importants suite à l'utilisation de cette formation, j'espère que vous aurez compris qu'il m'est également impossible de tout dévoiler sans le moindre contrôle, raison pour laquelle la formation vocale est un format plus adapté pour une mise en pratique plus réelle et plus précise.

Néanmoins, l'OSINT est une pratique typique de l'ère digitale, pour laquelle l'écrasante majorité des pratiquants sont des autodidactes ayant investi énormément d'heures dans la recherche et le développement de ses compétences.

Raison pour laquelle je peux vous garantir que les outils que j'ai mentionnés, les sous-entendus ainsi que les sites web/forums cités vous permettront, si vous vous y mettez réellement, de vous construire l'entièreté de votre portefeuille de compétences.

J'ai confiance en vous pour vous frayer votre chemin dans la sinueuse recherche d'informations complémentaire, je vous souhaite également beaucoup de courage dans cette quête et j'espère que vous mettrez ces informations à usage pour une bonne cause.

Selon les retombées de cette formation tant auprès de la communauté OSINT, qu'auprès de vous, je pourrais potentiellement envisager des formations de plus en plus complexes et approfondies.

J'espère que vous avez apprécié la lecture de ce document et je reste disponible pour tous vos retours potentiels.

LC