

GEOINT

Devenez un GeoGuessr Master

SecSea 2k22 - 15/10/2022



Who am I ?

Volker Carstein



- Pentester @ Capgemini Méditerranée
- Ingénierie sociale, OSINT et sécurité offensive
- Nerd of all things
- Penguin lover



@volker_carstein

Sommaire

01



Généralités

Définitions et
GEOINT militaire

02



GeoGuessr

Principe, techniques,
exemple

03



Overpass Turbo

Présentation,
langage, exemple

04

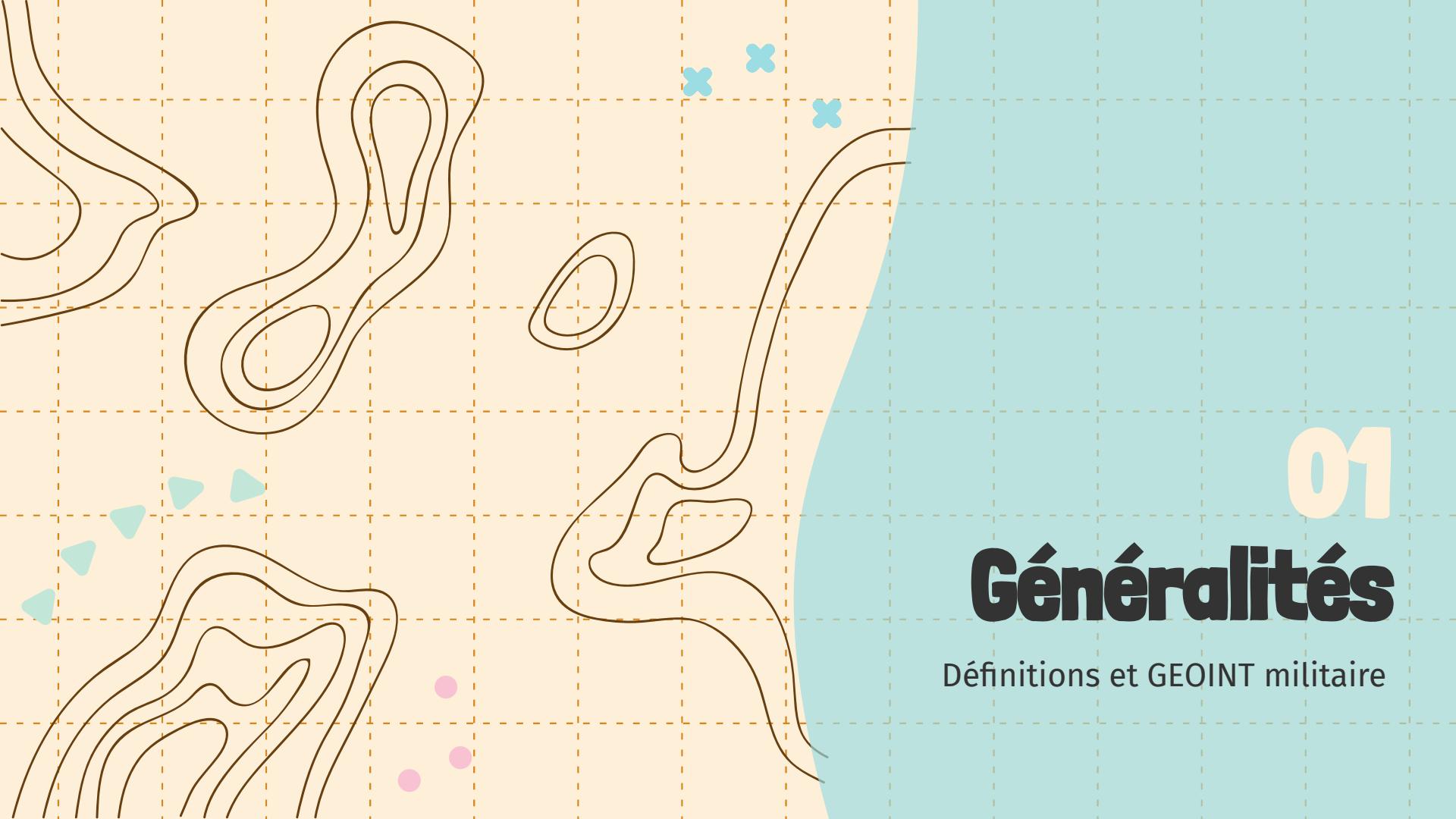


Conclusion

+ quelques
challenges !



@volker_carstein

The background features a light orange gradient with a dashed grid. Overlaid are several brown contour lines forming irregular shapes. There are also blue 'X' marks, teal triangles, and pink dots scattered across the grid.

01

Généralités

Définitions et GEOINT militaire

GEOINT : Définition

Geospatial Intelligence

“Renseignement géospatial” en français.

Fusion de données multicouches et multicapteurs.

- Collecte et recherche des informations ;
- Analyse, traitement et interprétation ;
- Visualisation et réalisation de produits.



Historique

GEOINT américain

- depuis les années 1960
- recherche de la *Global Information Dominance*

National Geospatial-Intelligence Agency (NGA)

- Crée en 2003, environ 14k employés
- Spécialisée dans le processus de fusion d'informations
- **Véritable écosystème** : universités et grands industriels



@volker_carstein



« Le Geoint est **l'exploitation** et **l'analyse** de l'imagerie et de
l'information géospatiale pour décrire et visualiser les
facteurs physiques et les activités géolocalisées sur Terre »

— *Doctrine GEOINT de la NGA, 2006 et 2011*

Historique

GEOINT dans le reste du monde

- Allemagne et Angleterre : 2000
 - Regain d'intérêt en 2011 (Irak, Afghanistan)
- Inde : dès 2002
- Chine et Israël dans la même période

GEOINT en France

- Premier emploi du terme en 2013
- Réforme DRM en 2014
- Centre de renseignement géographique interarmées en 2015



@volker_carstein



MINISTÈRE DE L'INTÉRIEUR

*Liberté
Égalité
Fraternité*

“Par ailleurs, pour la **gestion d'interventions, de grands événements** ou de **crise**, la cartographie doit servir de support à la visualisation des données en temps réel afin de **faciliter la prise de décision.**”

— *Livre blanc de la sécurité intérieure, 2020*



MINISTÈRE DE L'INTÉRIEUR

*Liberté
Égalité
Fraternité*

“[La cartographie] doit également permettre le développement des analyses spatio-temporelles, conformément à la discipline en développement baptisée **GeoINT**.”

— *Livre blanc de la sécurité intérieure, 2020*

Cas d'usage

- Contexte d'opération militaire
 - Préparation
 - Exécution, suivi opérationnel
 - Lutte contre le terrorisme
- Intelligence économique
- Optimisation agricole
- Aide humanitaire
- Luttes contre les incendies
- Géolocaliser des personnes disparues
 - *Tracelabs Search Parties*



@volker_carstein

Différentes informations

- **Information = “nerf de la guerre”**
- Mais toutes les informations ne sont pas pertinentes !

Méthodologie + compréhension du sujet/contexte = WIN

- Recherche de *marqueurs explicites*.



Marqueurs explicites

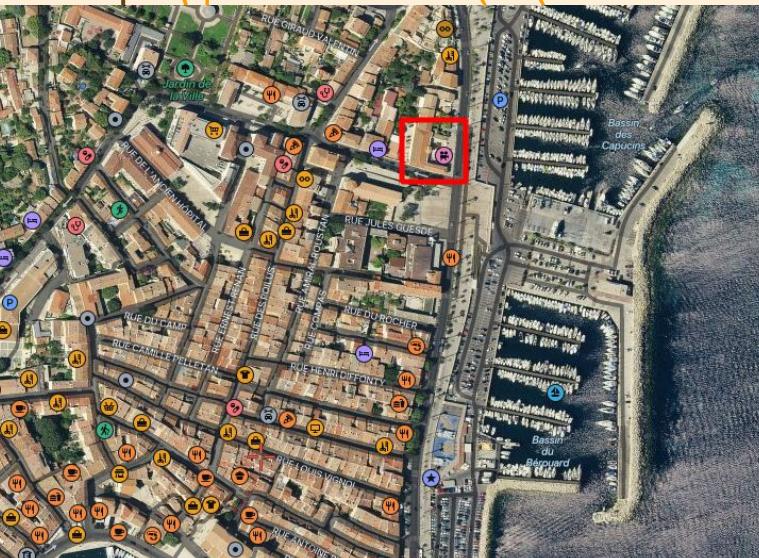
- Proviennent souvent d'un recouplement
- Servent une ou plusieurs tâches
 - Géolocalisation
 - Horodatage
 - Information de valeur
- Noms de rues ou bâtiments particuliers
- Éléments géographiques distinctifs
- Soleil et météo



@volker_carstein

Outils usuels

- Imagerie satellite
 - <https://satellites.pro/>
 - <https://apps.sentinel-hub.com/eo-browser/>
 - <https://maps.google.com/> (ou une alternative)
 - Google Earth (Pro)
- Recherche d'image inversée
 - Google Images, Yandex Images, etc.
- Soleil et météo
 - <https://www.suncalc.org/>
 - <https://www.ventusky.com/>



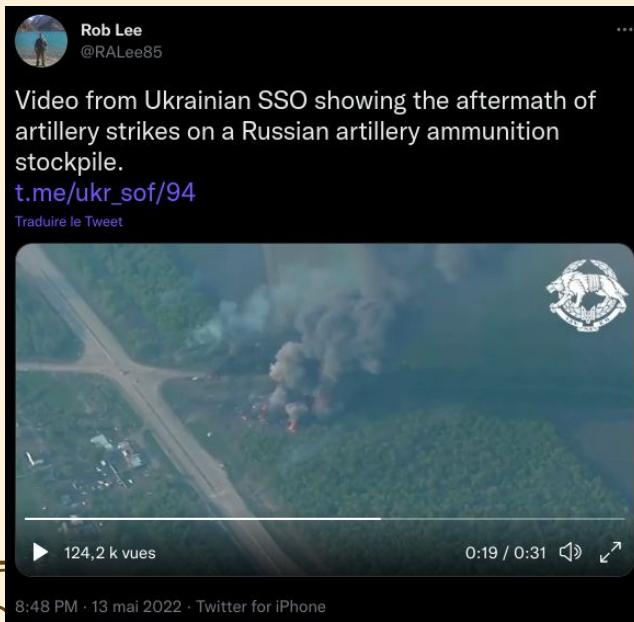
@volker_carstein

Exemple 1 : Frappe d'artillerie ukrainienne

- Basé sur le travail de ROSO (@0I3BK_POCO) et publié sur Osint-FR.
 - <https://osintfr.com/fr/geoint-etude-de-cas-dune-frappe-en-ukraine/>

**But : Vérifier l'information via
géolocalisation et horodatage**

<https://twitter.com/RALee85/status/1525186196963569664>



Exemple 1 : Étape 1 – Soleil

En avril-mai, donne 7h30 ou 17h.

Luminosité + source ukrainienne -> victimes probablement russes.

Donne l'heure approximative (17h) + directions



Dawn:	04:17:25
Sunrise:	04:54:04
Culmination:	12:28:41
Sunset:	20:04:09
Dusk:	20:40:58
Daylight duration:	15h10m5s
Distance [km]:	151.194.654
Altitude:	26.22°
Azimuth:	269.21°
Shadow length [m]:	2.03
at an object level [m]:	1

Exemple 1 : Étape 2 – Environnement

Autoroute orientée Nord-Ouest, plus petite route vers l'Ouest.

Deux zones de forêts, quelques habitations.

Fumée poussée par le vent vers le Nord-Est.

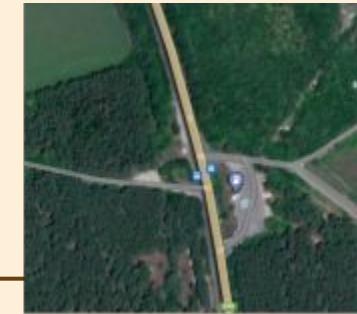
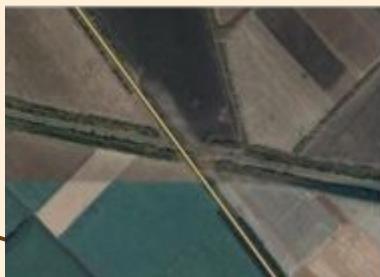
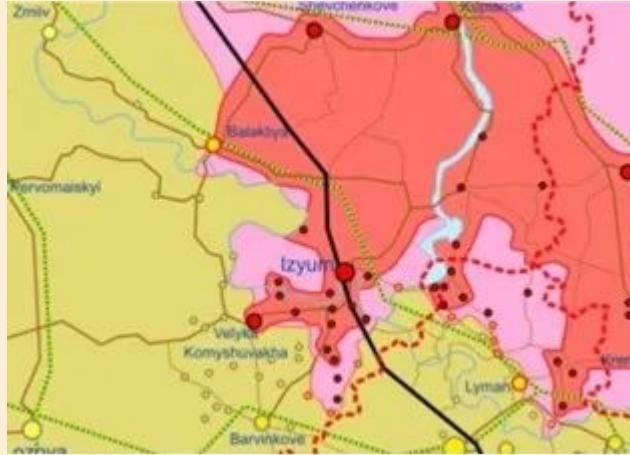


Exemple 1 : Étape 3 – Autoroute

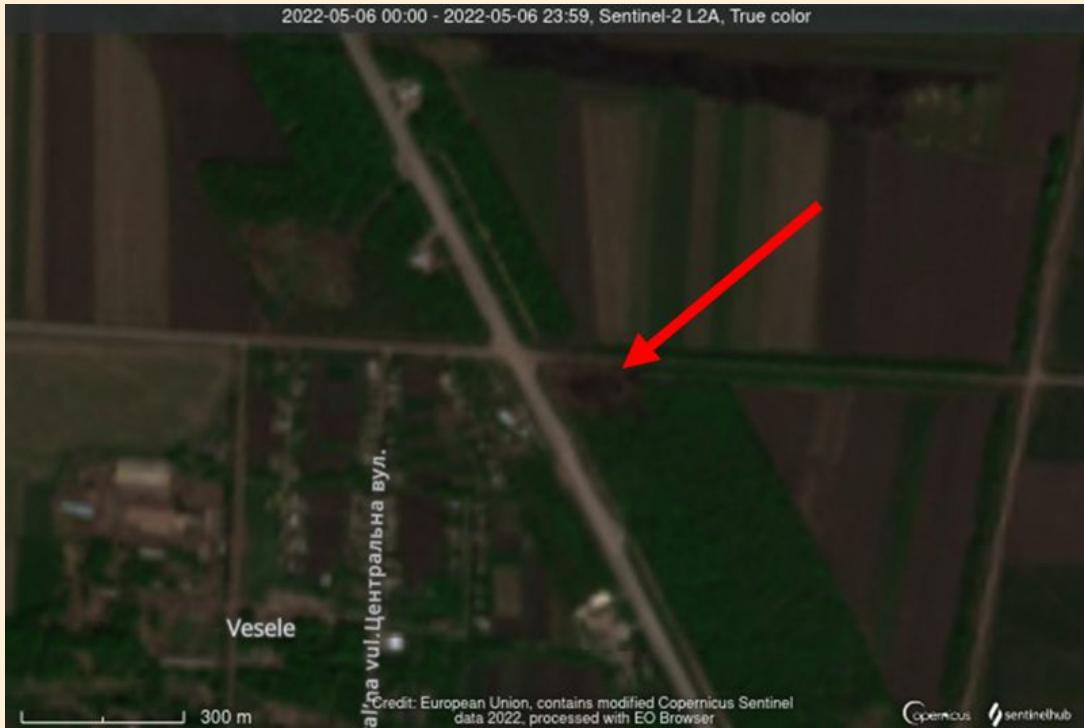
A partir des informations et d'une carte du front en avril-mai : M03 Kharkiv-Sloviansk

Suivre toute la route par satellite pour relever les zones candidates.

Une seule correspond complètement !
Beselé (Vesele), Ukraine

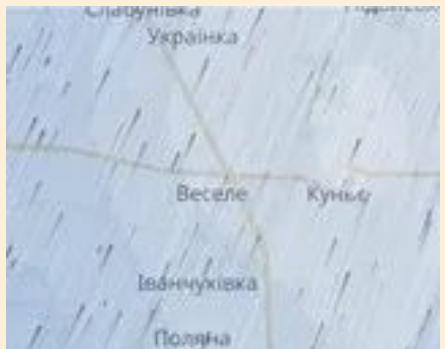


Exemple 1 : Étape 4 – Confirmation géo et date



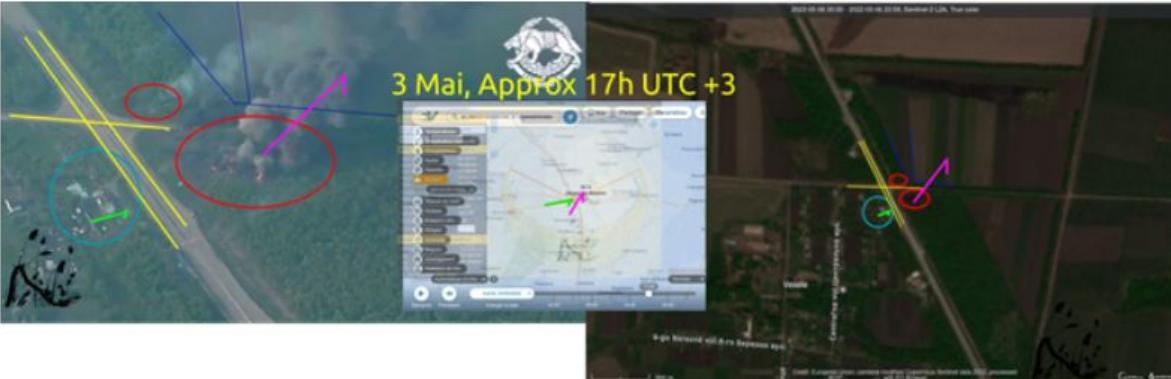
Forêt brûlée au 6 mai
+ mauvais temps en avril
+ champs de couleur
similaire à la vidéo

= Probablement entre le
3 mai et le 6 mai.



@volker_carstein

Exemple 1 : Success !



Ukrainian strike on russian convoy in Веселе (Vesele, Kharkiv Oblast) on the M03.

Location : 49.39732444069642,37.205029686706546

Date : probably 3 mai, approx 17h UTC +3

Source : <https://twitter.com/RALee85/status/1525186196963569664>



@volker_carstein

02

GeoGuessr

Principe, techniques, exemple



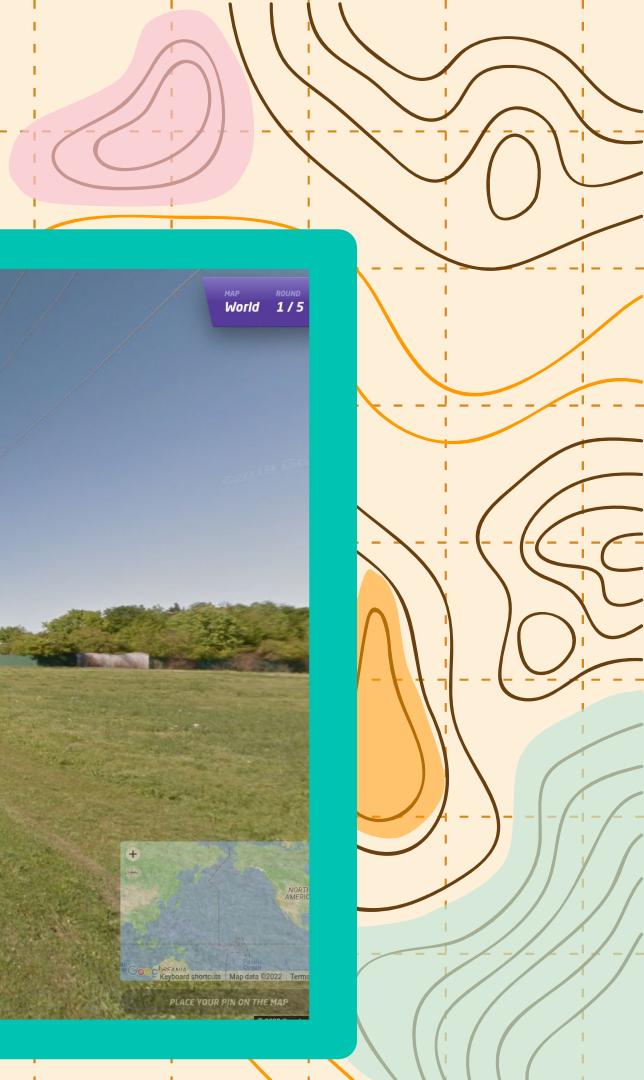
GE[📍]GUESSR

Savoir placer sa géolocalisation sur une carte

- Vue Street View
- Se géolocaliser à partir des indices trouvables
- Proche des coordonnées -> + de points
- Score global sur 5 lieux



GE[📍]GUESSR



Techniques (1/5)

[https://somerandomstuff1.wordpress.com/2019/02/08
/geoguessr-the-top-tips-tricks-and-techniques/](https://somerandomstuff1.wordpress.com/2019/02/08/geoguessr-the-top-tips-tricks-and-techniques/)

Couverture Street View (2018) :



- + Russie, USA, Brésil, Argentine, Australie, Norvège et le reste de l'Europe
= Pays surreprésentés !



Techniques (2/5)

[https://somerandomstuff1.wordpress.com/2019/02/08
/geoguessr-the-top-tips-tricks-and-techniques/](https://somerandomstuff1.wordpress.com/2019/02/08/geoguessr-the-top-tips-tricks-and-techniques/)

- Photos de mauvaise qualité : USA ou Australie
- Soleil et ombre (encore)
 - Ombre pointe vers le nord -> Hémisphère Nord
 - Soleil au Nord -> Hémisphère Sud
- Paraboles satellite : Pointent généralement vers l'équateur



Techniques (3/5)

[https://somerandomstuff1.wordpress.com/2019/02/08
/geoguessr-the-top-tips-tricks-and-techniques/](https://somerandomstuff1.wordpress.com/2019/02/08/geoguessr-the-top-tips-tricks-and-techniques/)

- Plaques d'immatriculation
- Noms de rue / de lieu
- Bâtiments ou structures notables
- Panneaux routiers
 - Type de route
 - Intersections
 - Directions et distances

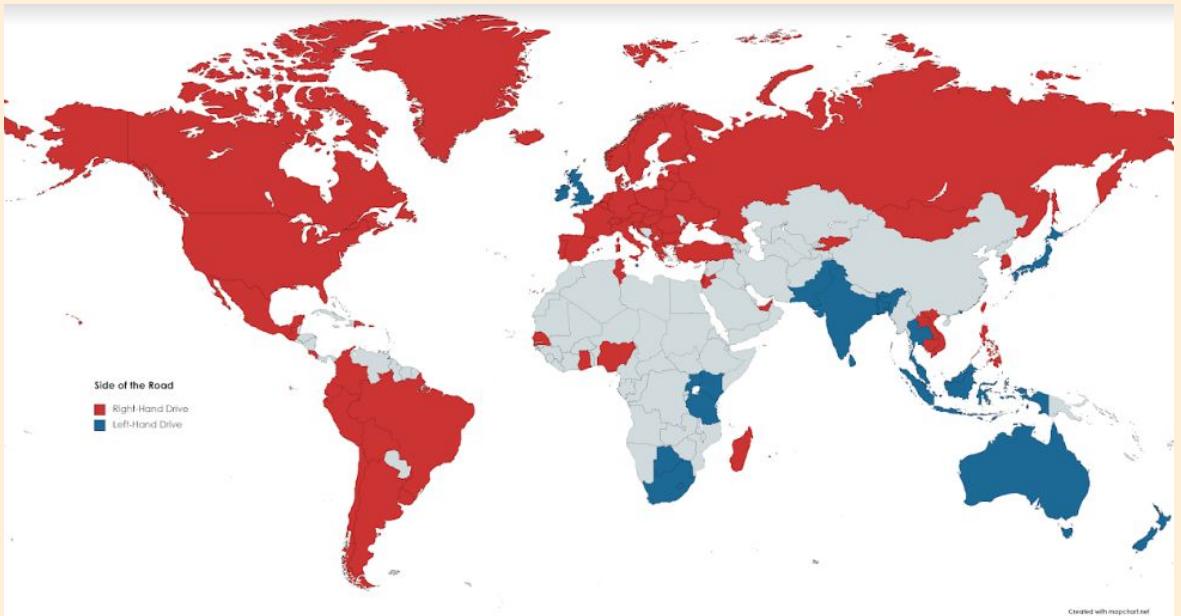


@volker_carstein

Techniques (4/5)

[https://somerandomstuff1.wordpress.com/2019/02/08
/geoguessr-the-top-tips-tricks-and-techniques/](https://somerandomstuff1.wordpress.com/2019/02/08/geoguessr-the-top-tips-tricks-and-techniques/)

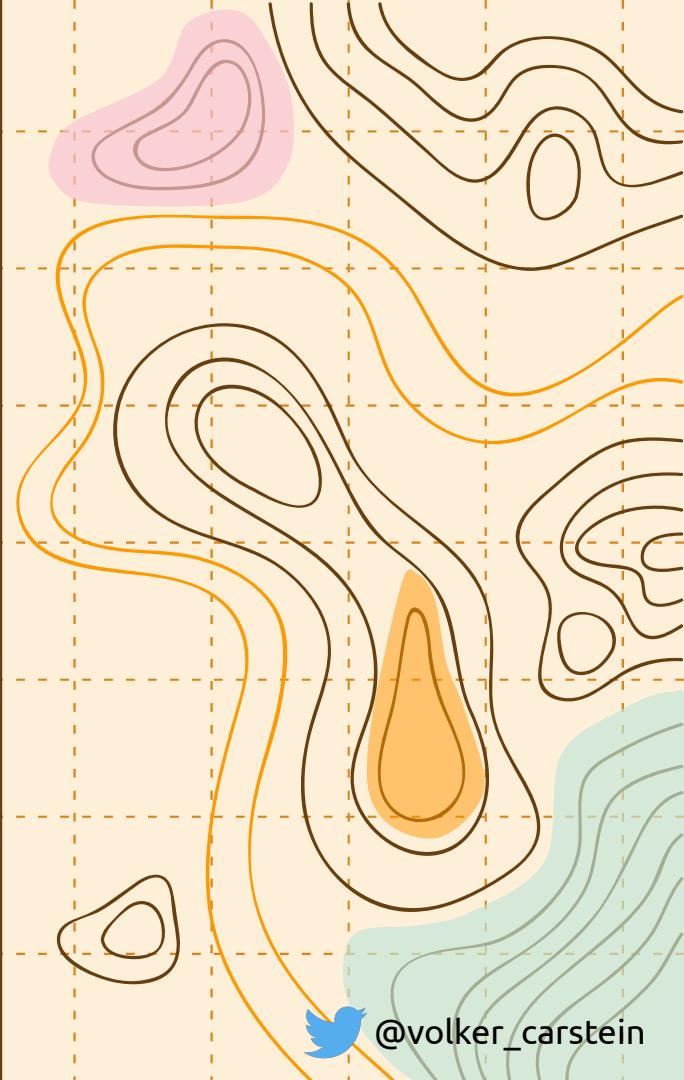
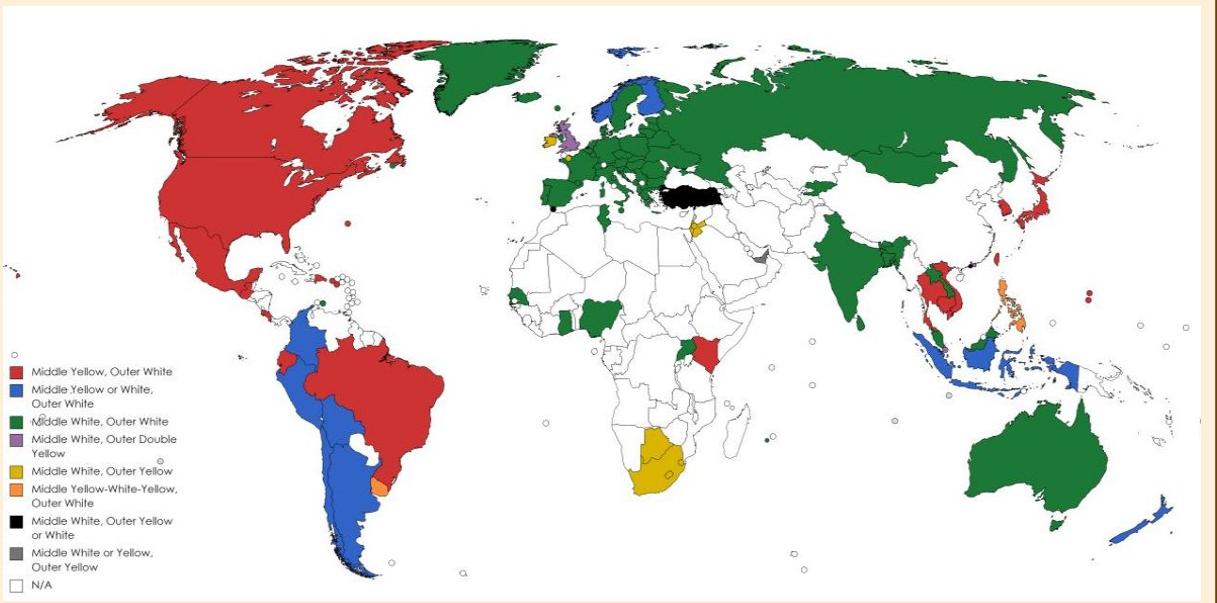
Conduite à droite ou à gauche :



Techniques (5/5)

[https://somerandomstuff1.wordpress.com/2019/02/08
/geoguessr-the-top-tips-tricks-and-techniques/](https://somerandomstuff1.wordpress.com/2019/02/08/geoguessr-the-top-tips-tricks-and-techniques/)

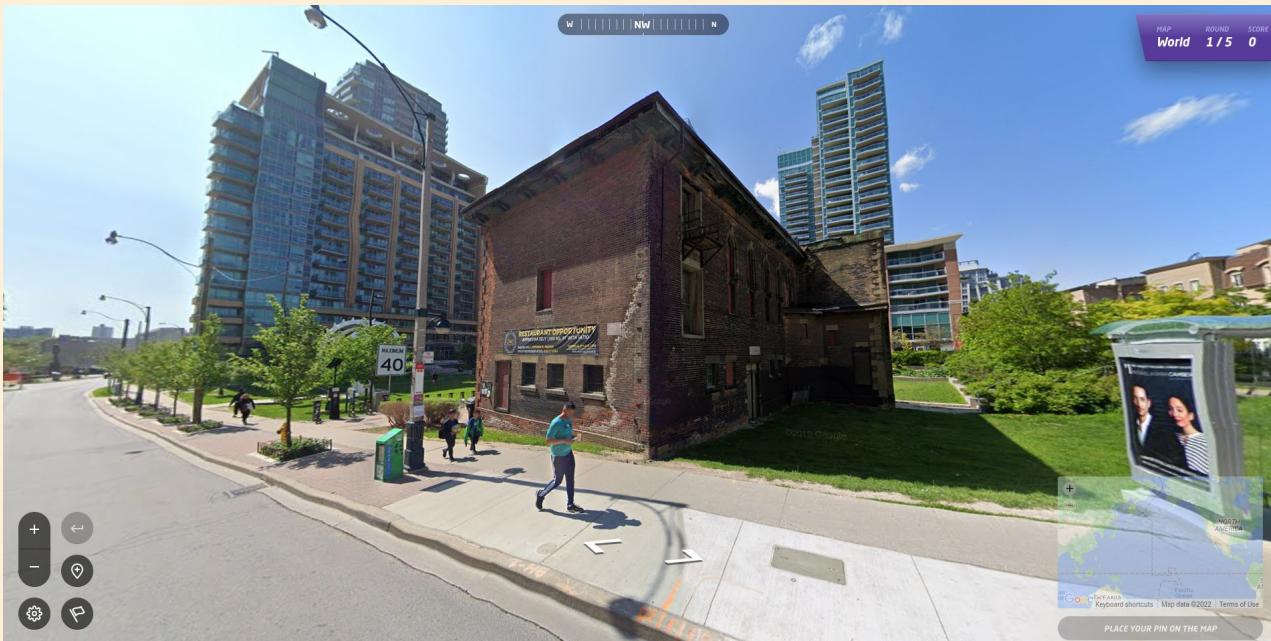
Marquages routiers :



@volker_carstein

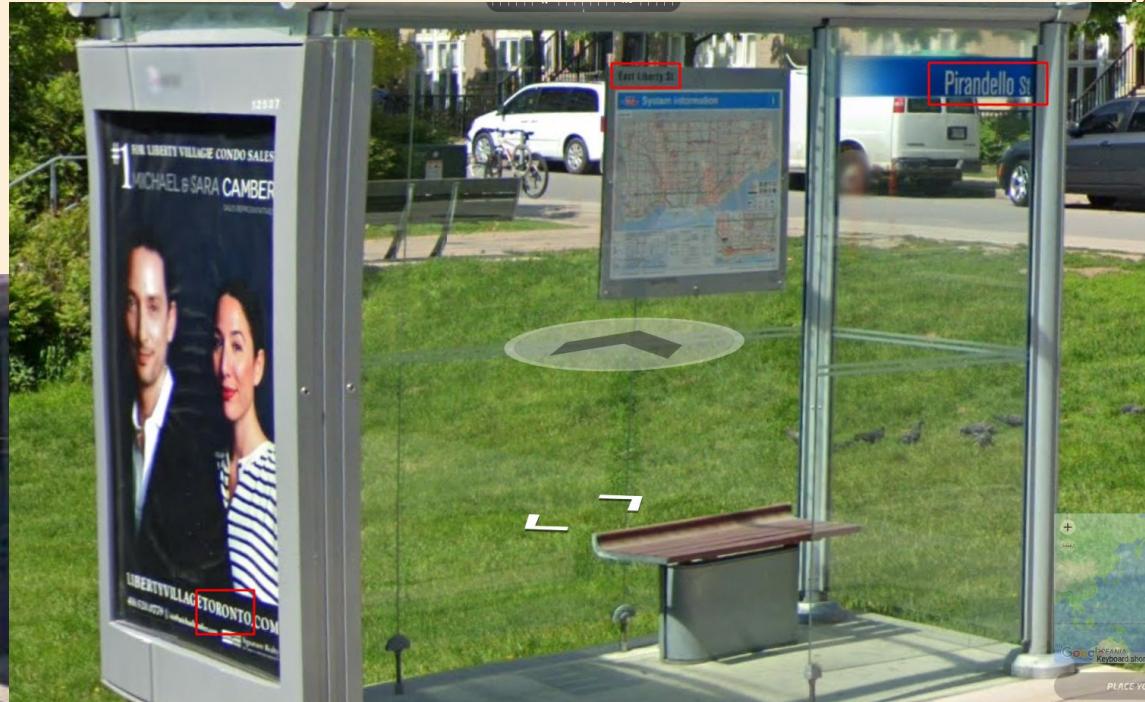
Exemple 2 : GeoGuessr (avec "triche")

But : Retrouver la géolocalisation de la vue Street View donnée par le jeu



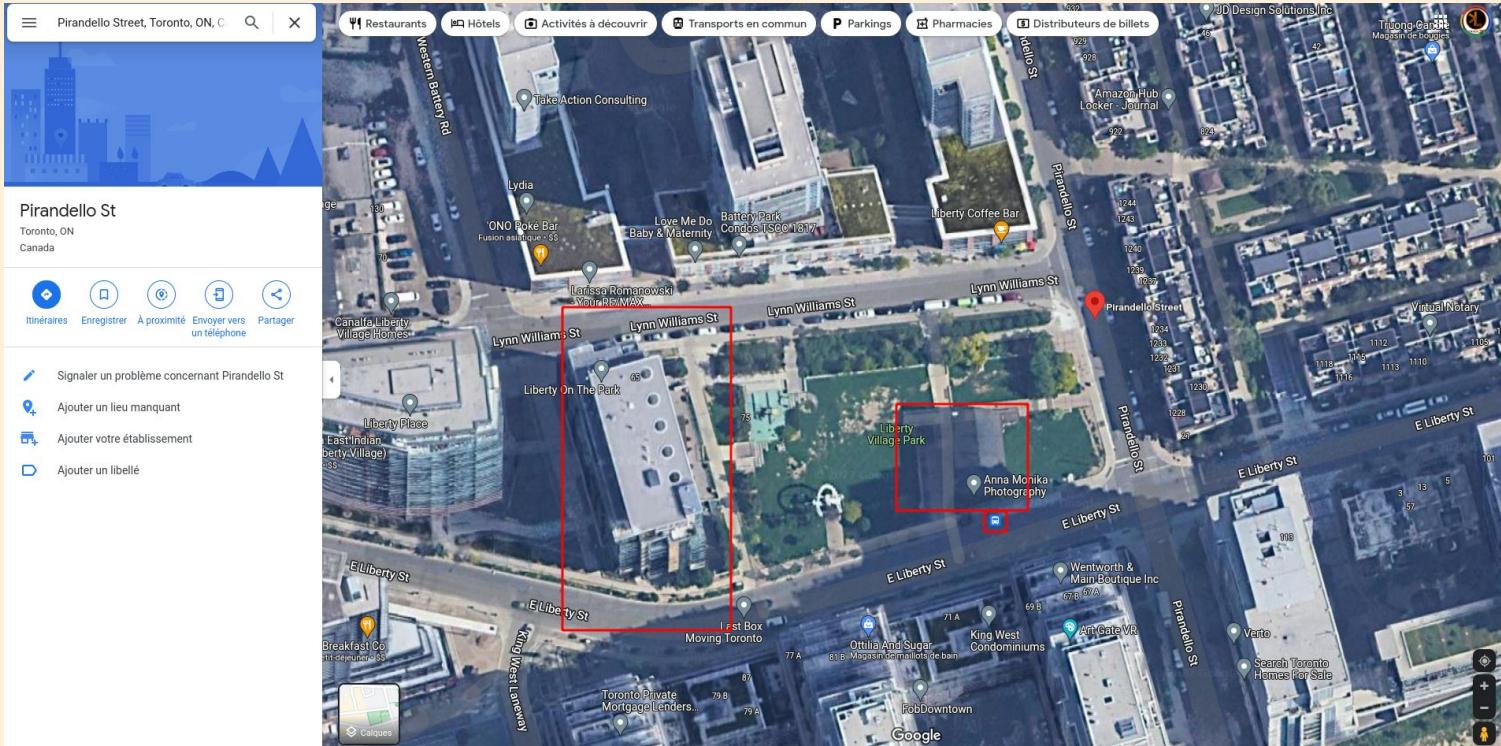
@volker_carstein

Exemple 2 : Étape 1 – Éléments discriminants



@volker_carstein

Exemple 2 : Étape 2 – Recherche Google Maps



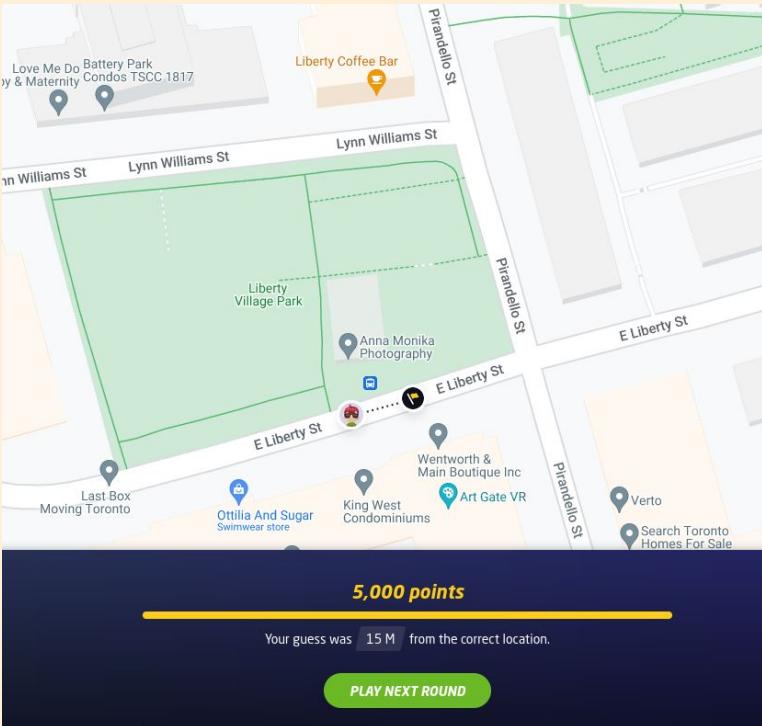
@volker_carstein

Exemple 2 : Étape 3 – Confirmation



@volker_carstein

Exemple 2 : Success !



@volker_carstein



03

Overpass Turbo

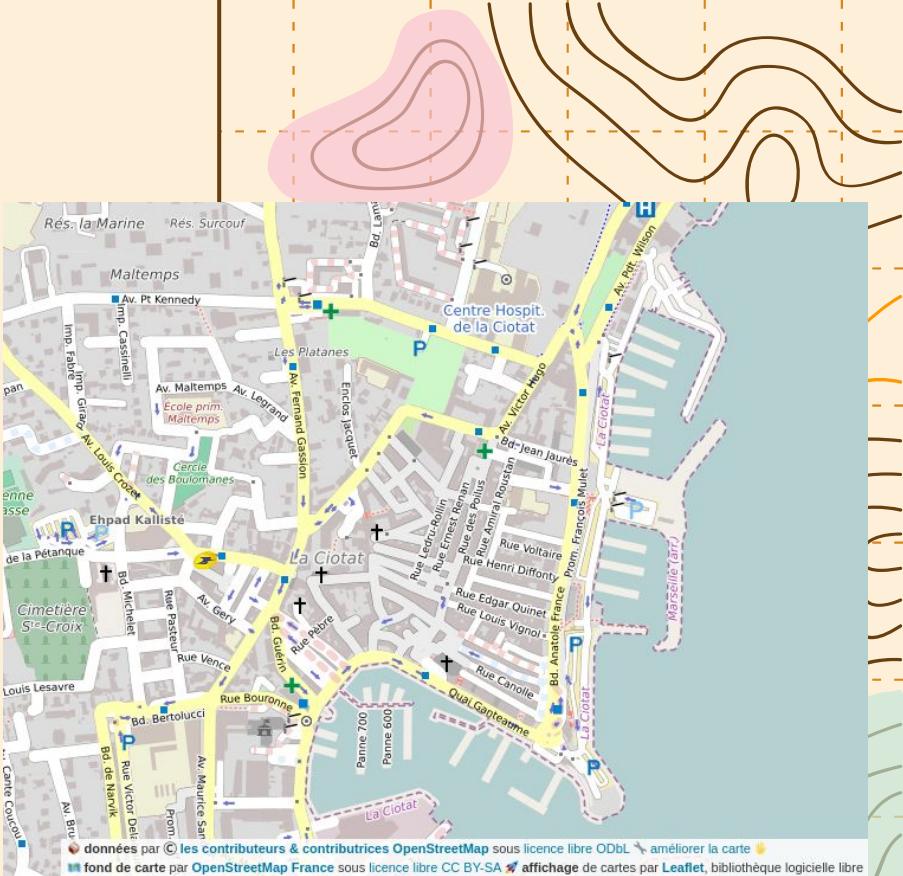
Présentation, langage, exemple



OpenStreetMap

Projet de cartographie libre

- Données géographiques libre
- Basé sur le travail des contributeurs
- Piloté par la Fondation OSM
- Rassemble un volume colossal de données géographiques sur le monde entier
- Le “Wikipedia des données géo”



données par © les contributeurs & contributrices OpenStreetMap sous licence libre ODbL améliorer la carte
fond de carte par OpenStreetMap France sous licence libre CC BY-SA affichage de cartes par Leaflet, bibliothèque logicielle libre



@volker_carstein

Overpass Turbo

Outil web pour faire des requêtes à
Overpass

- Overpass : API en lecture seule des données OSM
- Requêtes dans une syntaxe précise pour extraire des données spécifiques d'OSM
- Utile pour le GEOINT pour recouper des informations géospatiales



@volker_carstein

Overpass Turbo

Exécuter Partager Exporter Assistant Enregistrer Charger Paramètres Aide overpass turbo

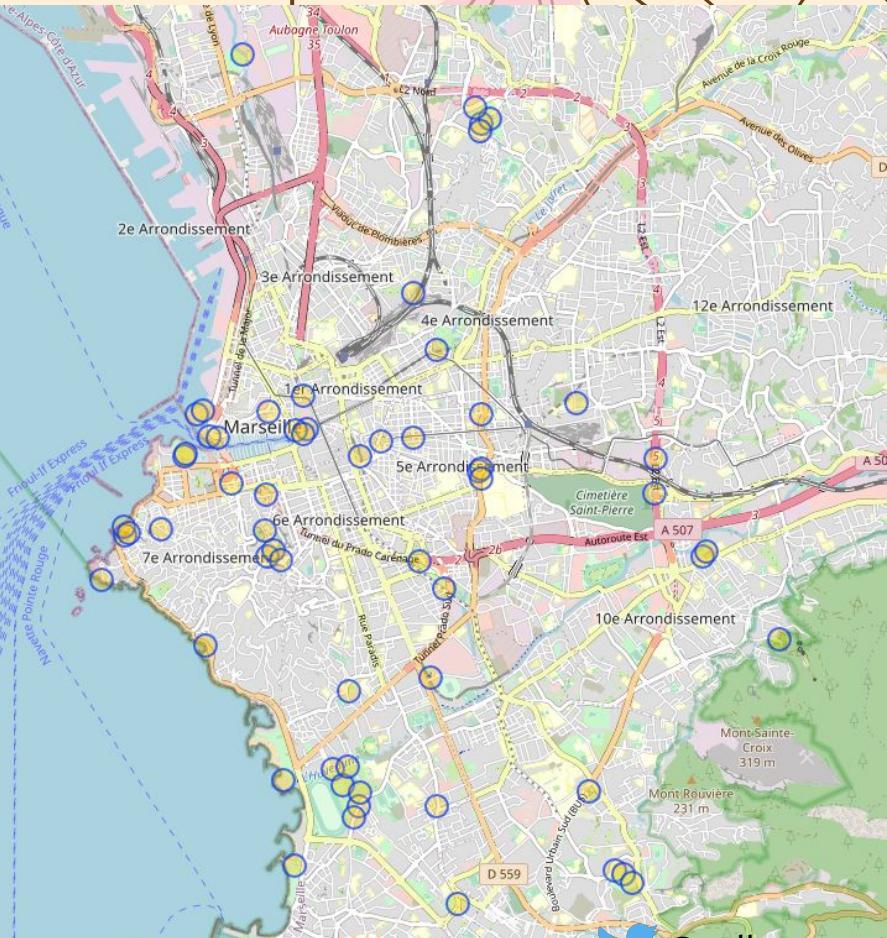
```
/*
1 This is an example Overpass query.
2 Try it out by pressing the Run button above!
3 You can find more examples with the Load tool.
4 */
5 node
6 [amenity=drinking_water]
7 {{bbox}};
8 out;
```

Carte Données

Overpass Turbo

```
node[amenity=drinking_water]({{bbox}});
out;
```

- {{bbox}} : Zone de la fenêtre OSM
- 3 types d'objets
 - Node : point
 - Way : lien entre des points
 - Relation : collection de nodes et de ways liés
- Tous les objets ont des propriétés
 - Type de la propriété + valeur associée



@volker_carstein

Overpass Turbo

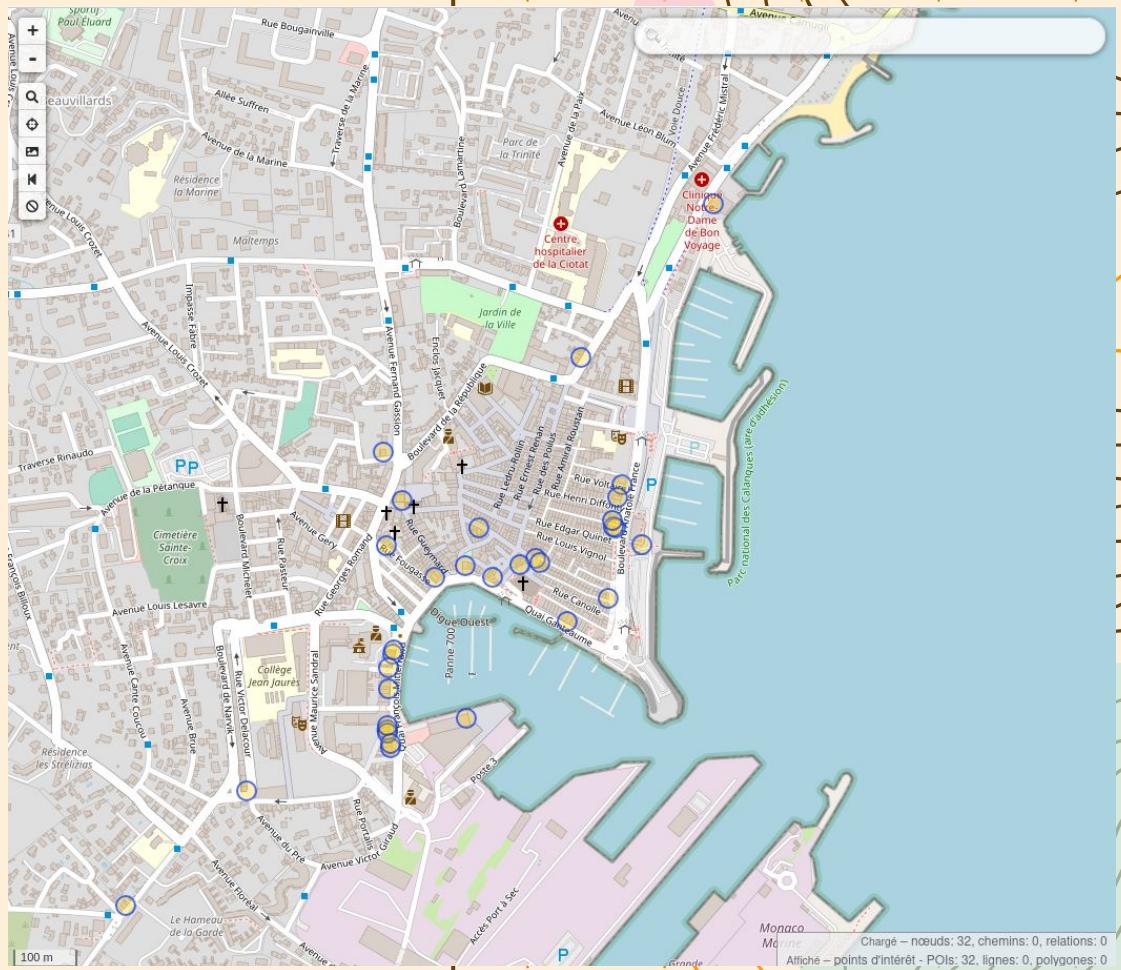
Exemple : Tous les restaurants de La Ciotat

```
node["amenity"="restaurant"]({{bbox}});  
out;
```

```
(  
  node["amenity"="restaurant"]({{bbox}});  
) -> .restaurant;  
.restaurant;;  
out;
```

.<name> : “variable”

Possibilité de mettre les variables en relation !

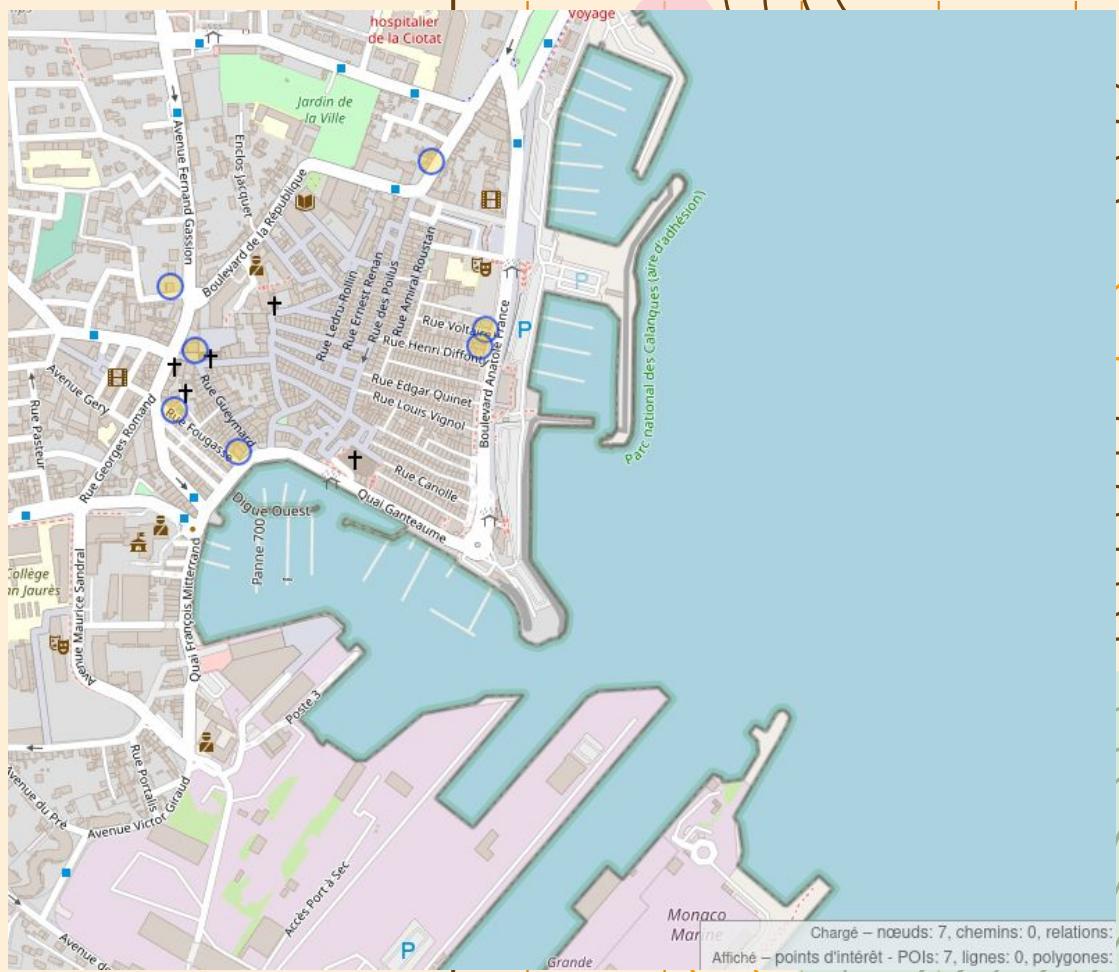


@volker_carstein

Overpass Turbo

Exemple : Tous les restaurants de La Ciotat à moins de 200m d'un cinéma

```
(  
  node["amenity"]=="cinema"]({{bbox}});  
  -> .cinema;  
  
(  
  node(around.cinema:200)["amenity"]=="restaurant");  
  -> .restaurant;  
  
.restaurant;  
out;
```

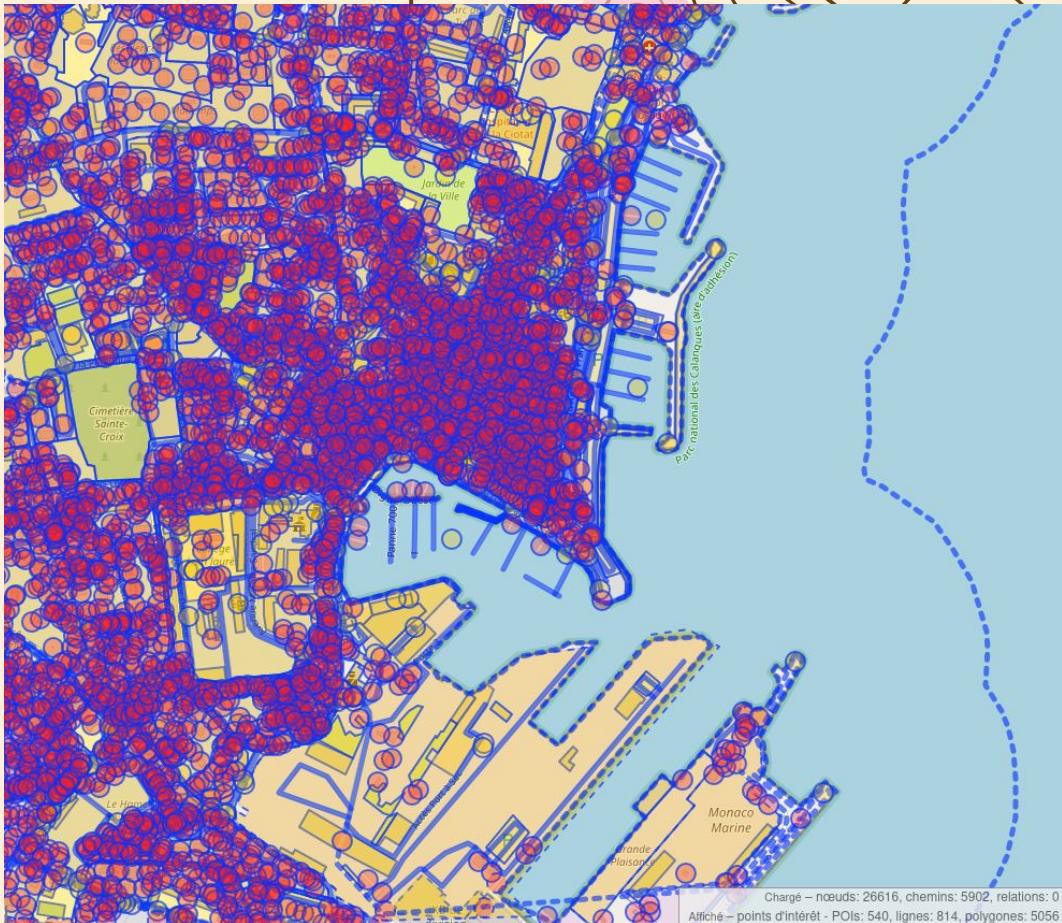


@volker_carstein

Overpass Turbo

Exemple : Tous les nodes et les ways dans la vue OSM

```
(  
  nw({{bbox}});  
) -> .nodes_and_ways;  
  
.nodes_and_ways;  
  
out;
```

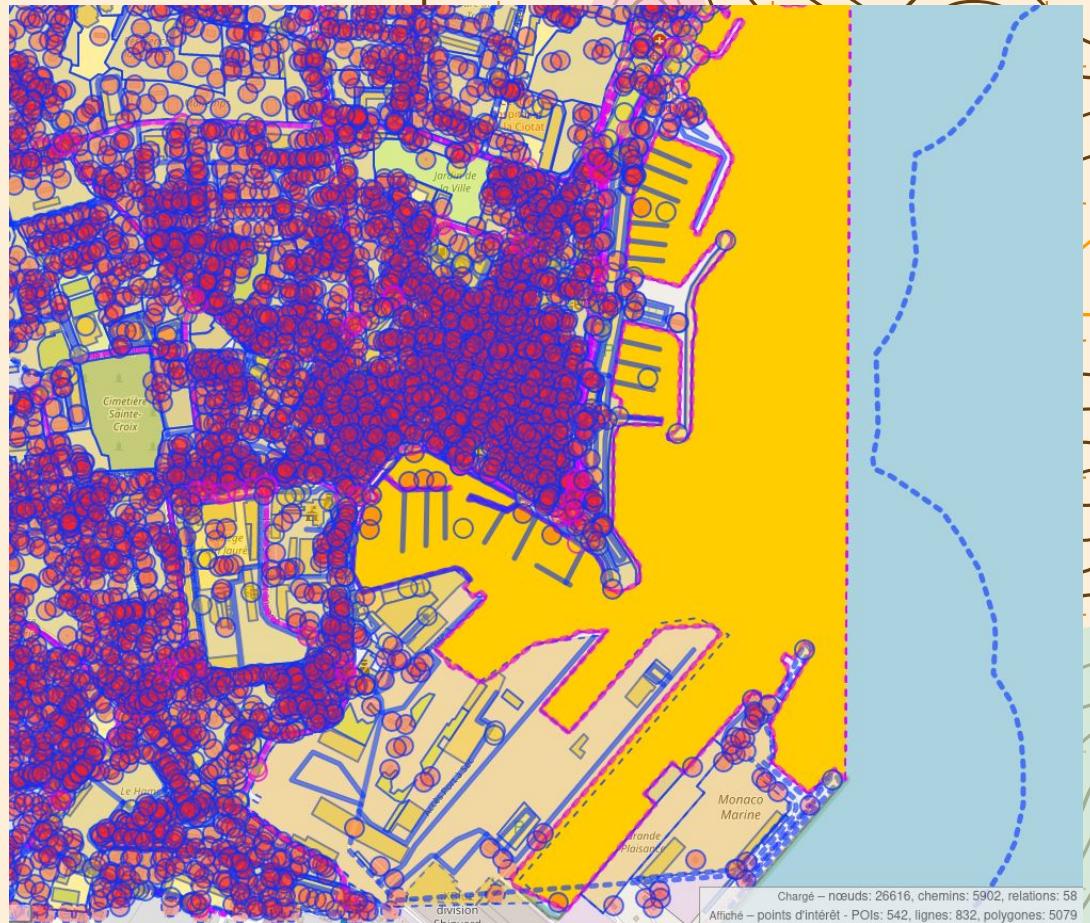


@volker_carstein

Overpass Turbo

Exemple : Tous les nodes, les ways et les relations dans la vue OSM

```
(  
    nwr({{bbox}});  
) -> .nodes_ways_relations;  
  
.nodes_ways_relations;;  
  
out;|
```



@volker_carstein

Exemple 3 : Partons en vacances

But : Retrouver la géolocalisation de la vue Street View suivante



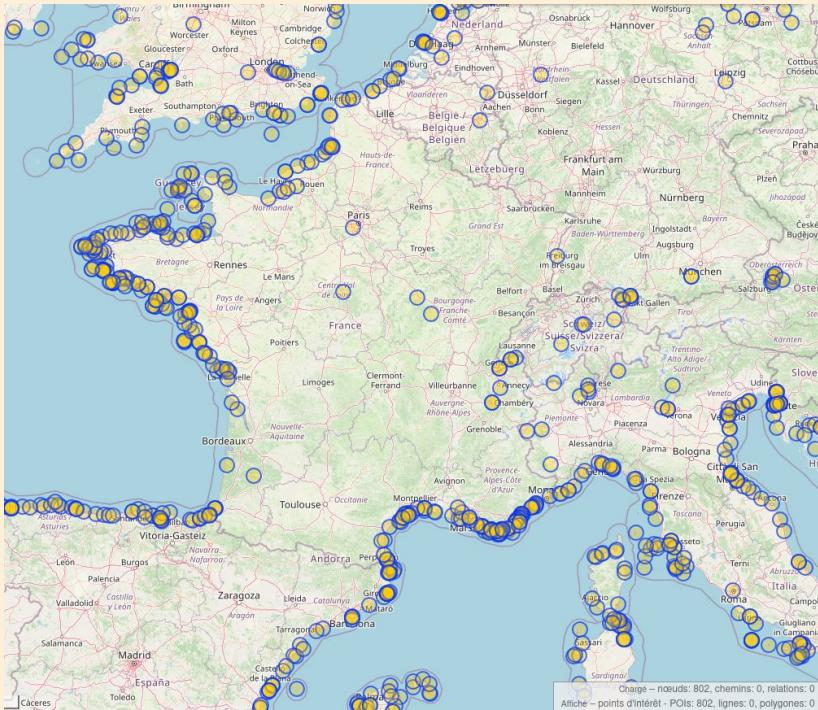
@volker_carstein

Exemple 3 : Étape 1 – Requête avec le phare

```
[out:json][timeout:120];
(
    node["man_made"="lighthouse"]({{bbox}});
)->.lighthouse;

(.lighthouse;);

out body;
```



@volker_carstein

Exemple 3 : Étape 2 – Château et pont

```
[out:json][timeout:120];
{
    node["man_made"]=="lighthouse"]({{bbox}});
->.lighthouse;

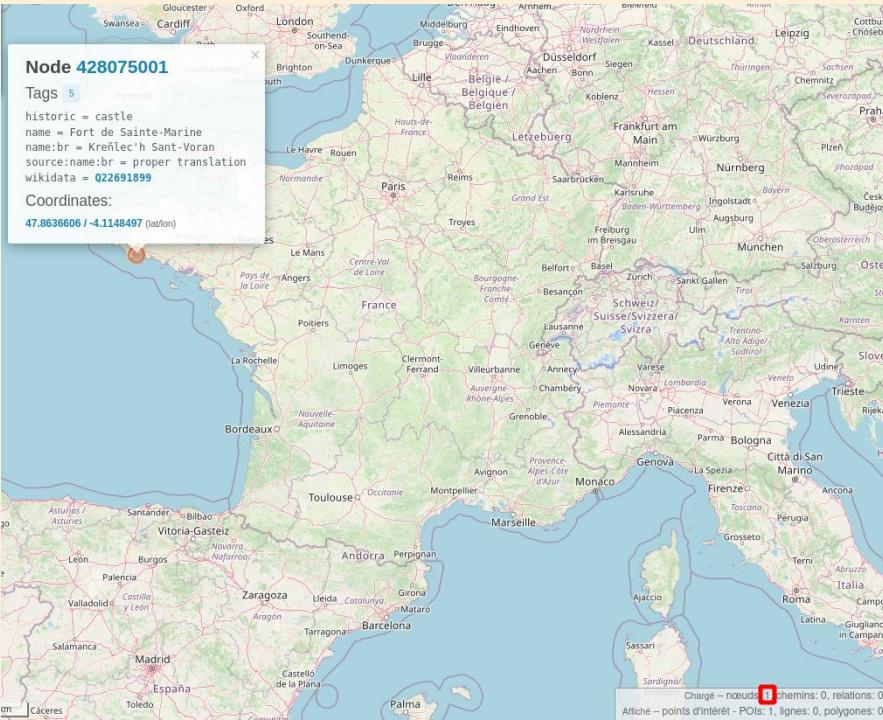
(
    node(around.lighthouse:200)["historic"]=="castle"];
->.castle;

(
    nwr(around.lighthouse:1000) ["man_made"]=="bridge";
->.bridge;

(.castle;);

out body;
```

Faux : n'a pas de pont proche +
infirimation avec Street View.
Il faut étendre la zone et prendre
en compte le pont.



@volker_carstein

Exemple 3 : Étape 3 – Tout relier ensemble

```
[out:json][timeout:120];
(
  node["man_made"]=="lighthouse"({{bbox}});
->.lighthouse;

(
  node(around:lighthouse:200)["historic"]=="castle";
)->.castle;

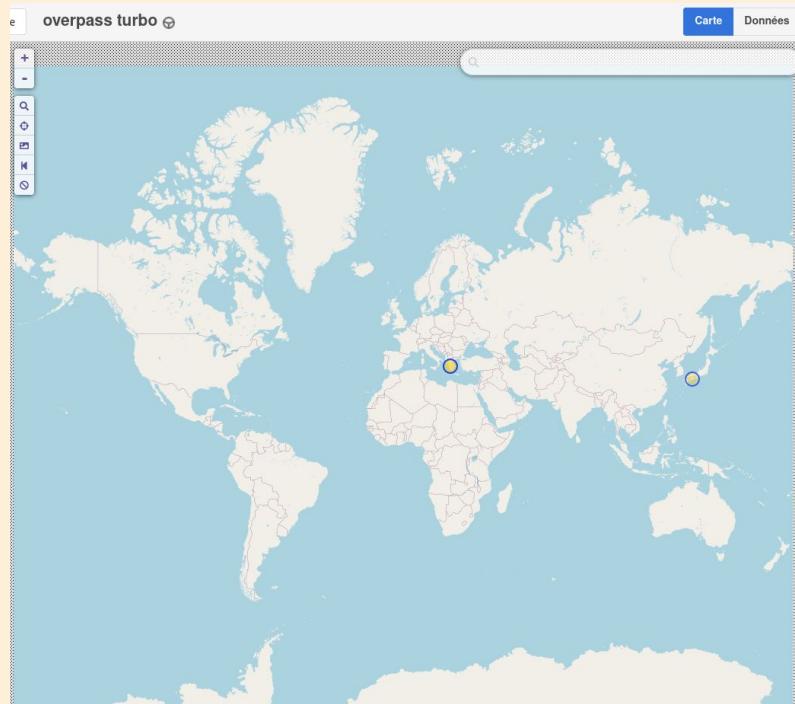
(
  nwr(around:lighthouse:1000)["man_made"]=="bridge";
)->.bridge;

(
  node.castle(around:bridge:1000);
)->.matching_castle;

(
  node.lighthouse(around:matching_castle:200);
)->.matching_lighthouse;

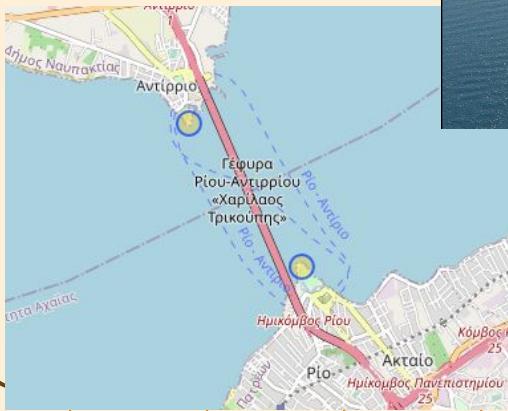
(.matching_lighthouse;);

out body;
```



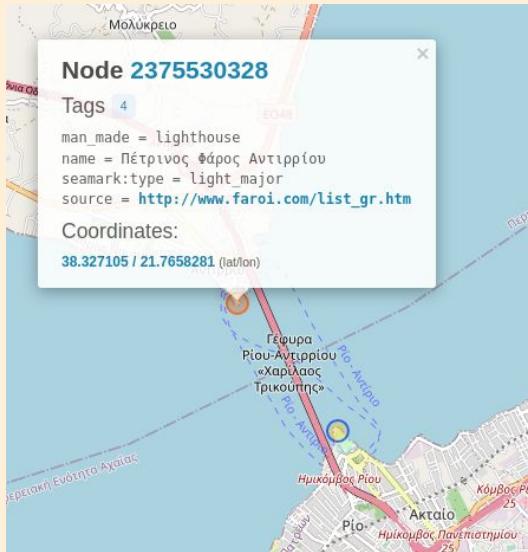
@volker_carstein

Exemple 3 : Étape 4 – Confirmation



@volker_carstein

Exemple 3 : Success !



@volker_carstein

Exemple 4 : Frappe russe en Ukraine

But : Retrouver la géolocalisation de la photo suivante

https://www.reddit.com/r/pics/comments/y0d2zr/russia_bombed_a_playground_as_revenge_against/



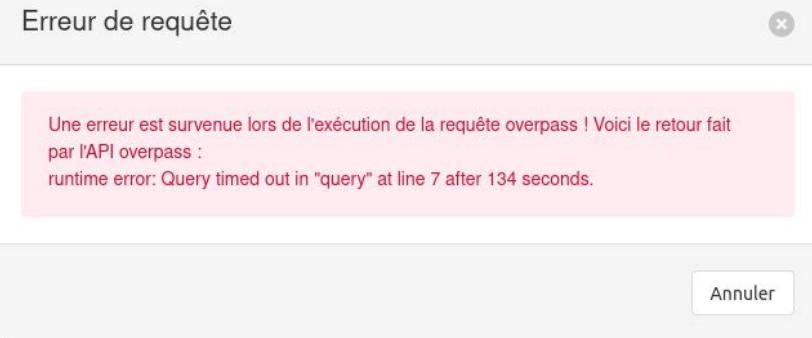
@volker_carstein



@volker_carstein

Exemple 4 : Étape 1 – Première requête

- Zone géographique : Ukraine
- Parc pour enfant
- Arbres -> Probablement situé dans un parc



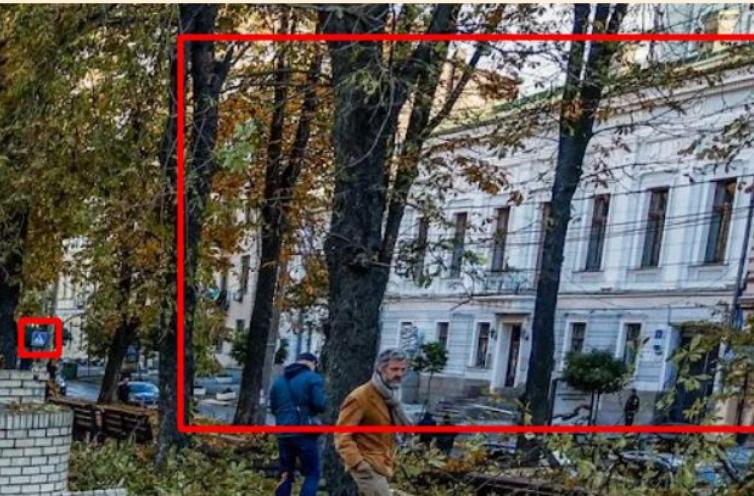
```
[out:json][timeout:120];
(
  nwr["leisure"="playground"]({{bbox}});
)->.playground;
(
  nwr(around.playground:50)["leisure"="park"];
)->.park;
(
  nwr.playground(around.park:50);
)->.playground_park;
(.playground_park;);

/*added by auto repair*/
(_.;>););
/*end of auto repair*/
out body;
```



Exemple 4 : Étape 2 – Nouveaux éléments

- Passage piéton
- Bâtiment à 2 étages



```
[out:json][timeout:120];
(
  nwr["leisure"]="playground"]({{bbox}});
)->.playground;

(
  nwr(around.playground:50)["leisure"]="park";
)->.park;

(
  nwr.playground(around.park:50);
)->.playground_park;

(
  nwr(around.playground:50)["highway"]="crossing";
)->.crossing;

(
  nwr.playground_park(around.crossing:50);
)->.playground_park_crossing;

(
  nwr(around.playground_park_crossing:50)["building:levels"]==2;
)->.level;

(
  nwr.playground_park_crossing(around.level:50);
)->.playground_park_crossing_level;

(.playground_park_crossing_level;);

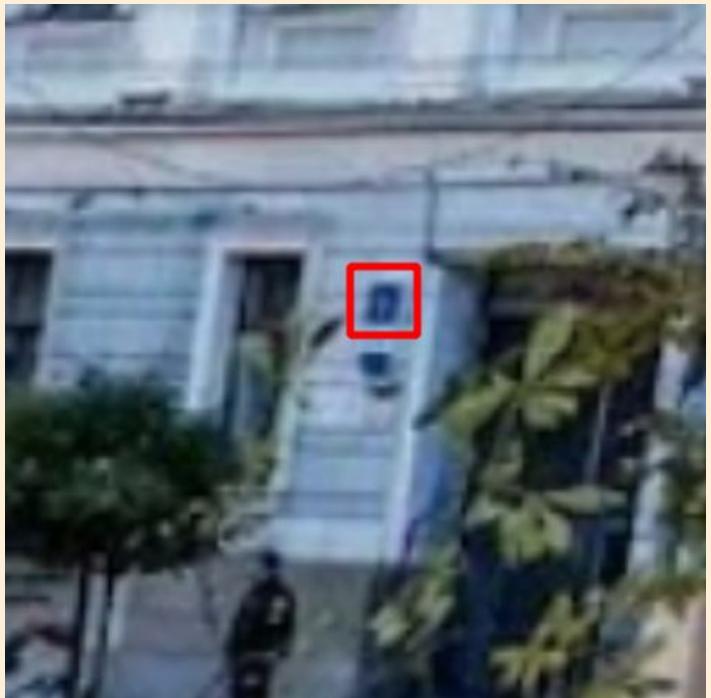
/*added by auto repair*/
(_;>););
/*end of auto repair*/
out body;
```



@volker_carstein

Exemple 4 : Étape 3 – Élément décisif

- Chiffre, donc 0-9
- Trop fin sur le bas pour un 2, 3, 5, 6, 8
- Trop épais en haut pour un 1
- Reste 4, 7 et 9
- **Bâtiment n°9**



Exemple 4 : Étape 3 – Élément décisif

```
[out:json][timeout:120];
(
  nwr["leisure"="playground"]({{bbox}});
->.playground;

(
  nwr(around.playground:50)["leisure"="park"];
->.park;

(
  nwr.playground(around.park:50);
->.playground_park;

(
  nwr(around.playground:50)["highway"="crossing"];
->.crossing;

(
  nwr.playground_park(around.crossing:50);
->.playground_park_crossing;

(
  nwr(around.playground_park_crossing:50)["building:levels"=2];
->.level;

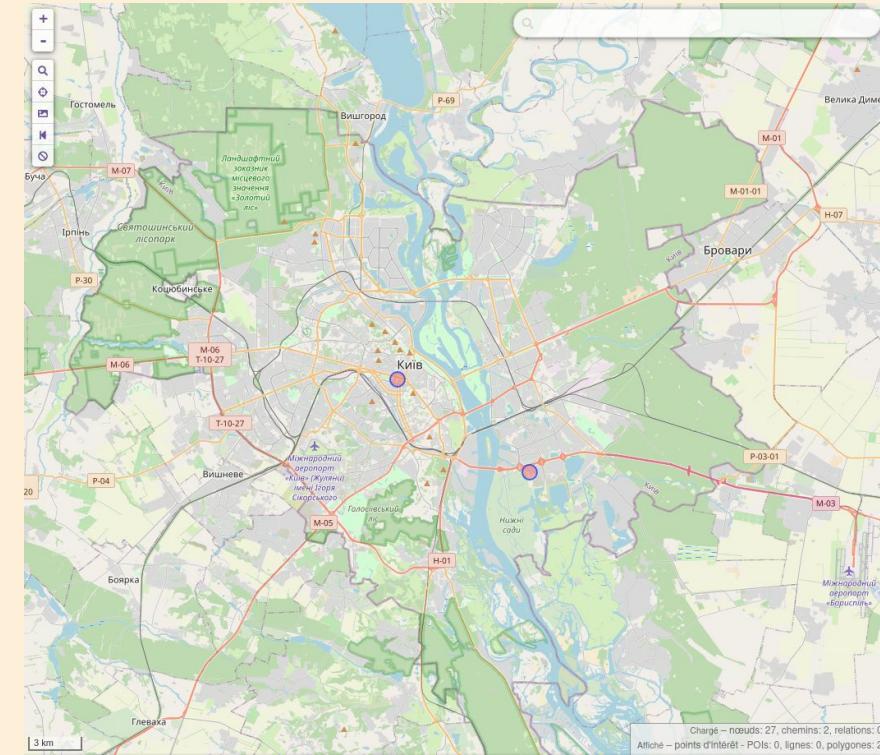
(
  nwr.playground_park_crossing(around.level:50);
->.playground_park_crossing_level;

(
  nwr(around.playground_park_crossing_level:50)["addr:housenumber"=9];
->.number;

(
  nwr.playground_park_crossing_level(around.number:50);
->.playground_park_crossing_level_number;

(.playground_park_crossing_level_number;);

/*added by auto repair*/
(_;_);
/*end of auto repair*/
out body;
```



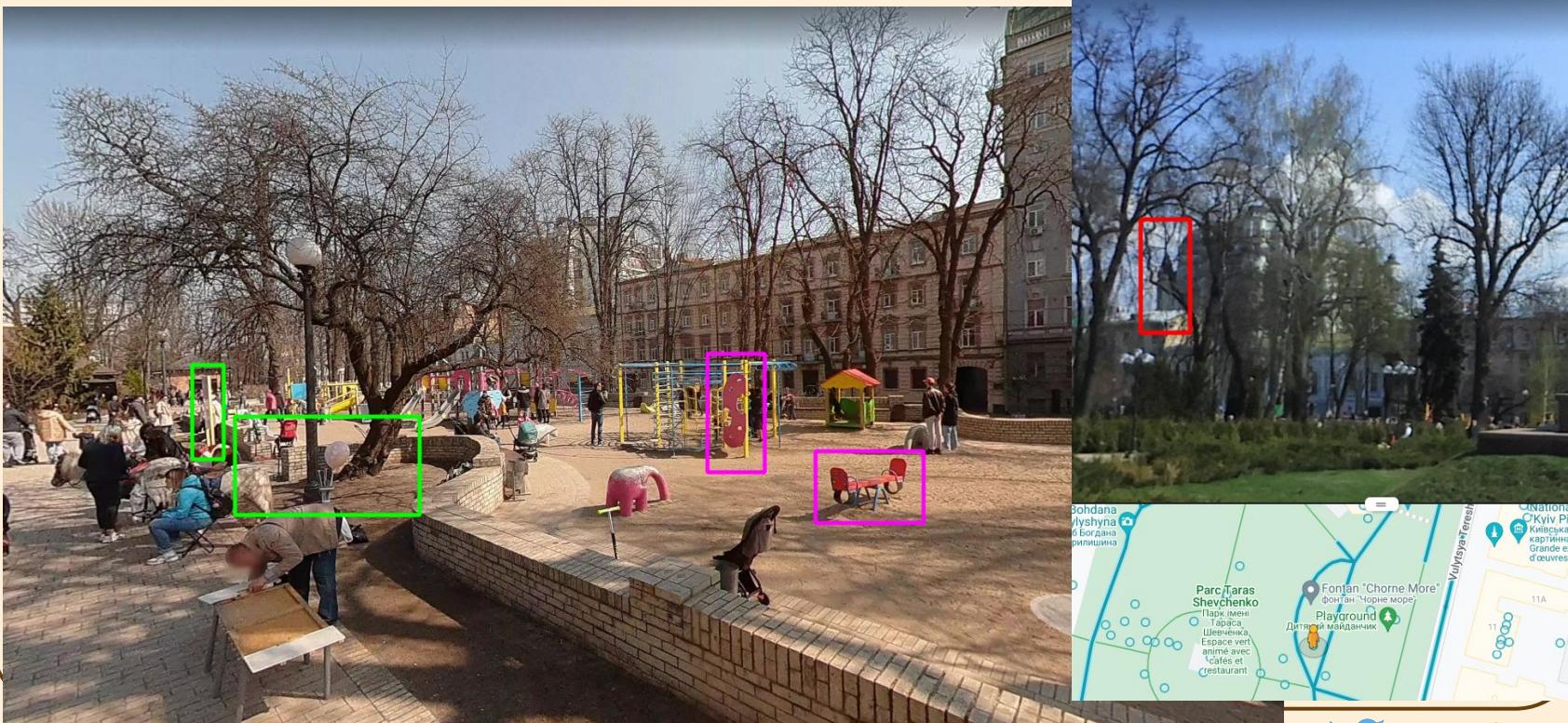
@volker_carstein

Exemple 4 : Étape 4 – Confirmation via Street View



@volker_carstein

Exemple 4 : Étape 4 – Confirmation via Street View



@volker_carstein

Exemple 4 : Success !

Recherche Où est-ce ? Aller

Nœud :
9291373683

Version #1

Уточнення геометрії парку Шевченка

Modifié il y a 11 mois par darkonus
Groupe de modifications #114337760

Emplacement : 50,4421839, 30,5139902

Partie de

▼ 1 chemin
1007138161

Télécharger en XML · Voir l'historique

Київська міська клінічна лікарня №18
Наукова бібліотека ім. М. Макаровського
Червоний корпус
Філія №1 НБУВ
ПриwatBank
Університет
Київські шахи
Шевченківський район
Любов-Всесвіт
Парк Шевченка
Тарасу Шевченку
КНУ ім. Тараса Шевченка
Грушевський
Терещенківська вулиця
Вулиця Володимирська
Тараса
Київська національна картинна галерея
Музей мистецтв ім. Ханенків

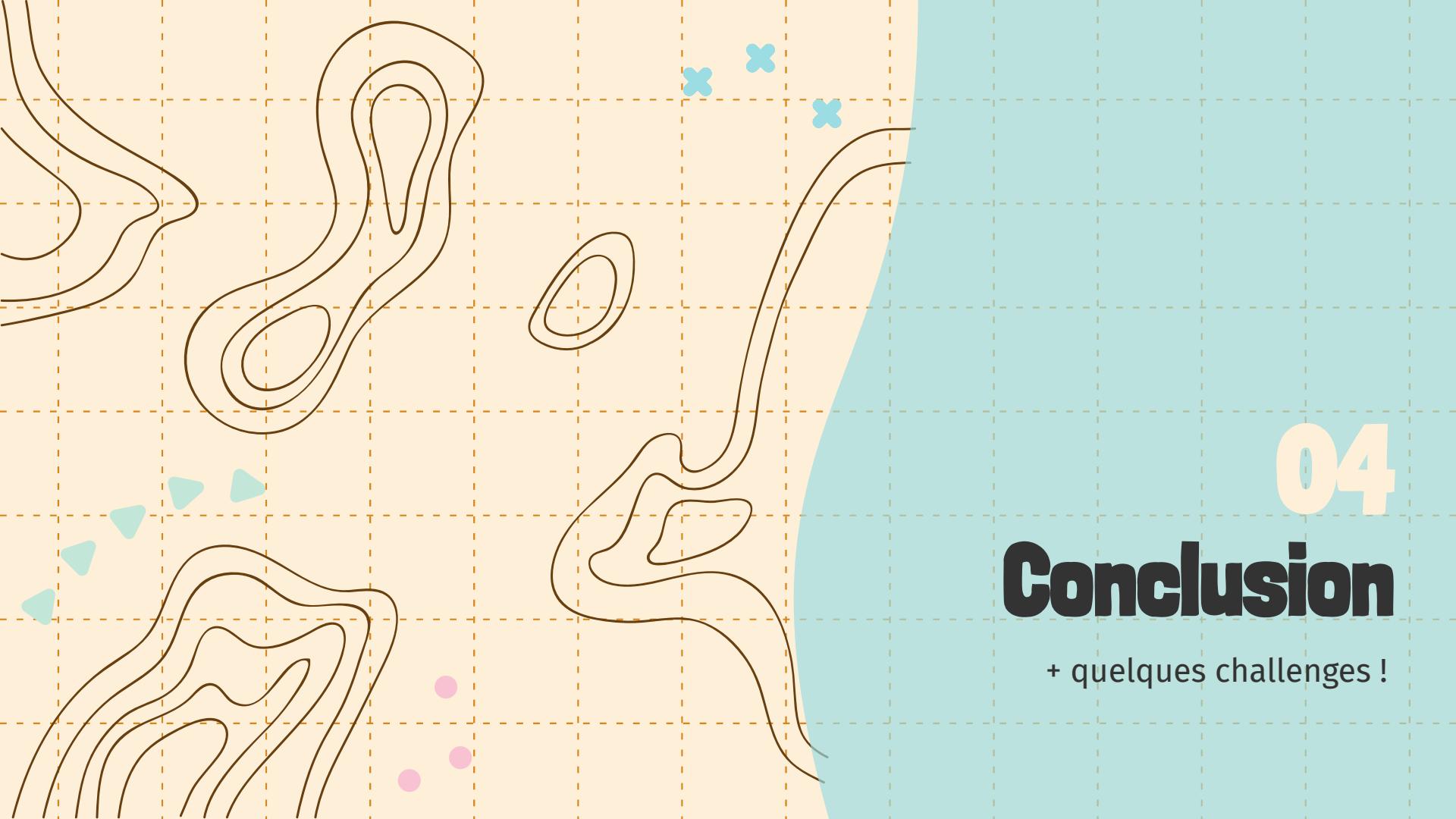


@volker_carstein

04

Conclusion

+ quelques challenges !



Conclusion

- **GEOINT : Geospatial Intelligence.** Discipline en plein essor.
- Dégager les **informations pertinentes** du volume global
 - Passe par le recoupement des informations
- GeoGuessr pour s'entraîner à la géolocalisation (et s'amuser)
- Overpass Turbo pour manipuler des gros volumes de données géospatiales (pour la géoloc et/ou la vérification)
- **Méthodologie + compréhension du contexte**



@volker_carstein

Sources

- <https://www.cairn.info/revue-defense-nationale-2016-10-page-103.htm>
- <https://www.sorbonne-universite.fr/actualites/dcouvrez-le-geoint-ce-nouveau-systeme-militaire-de-renseignement-sur-les-lieux-et-les>
- <https://www.youtube.com/watch?v=xawo4fBU13Q>
- <https://www.vie-publique.fr/sites/default/files/rapport/pdf/277185.pdf>
- <https://www.youtube.com/watch?v=L-azI0OOOWXY>
- <https://www.heavy.ai/technical-glossary/geoint>
- <https://www.tracelabs.org/initiatives/search-party>
- <https://github.com/cartographia/geospatial-intelligence-library>
- <https://satellites.pro/>
- <https://apps.sentinel-hub.com/eo-browser/>
- <https://osintfr.com/fr/geoint-etude-de-cas-dune-frappe-en-ukraine/>
- <https://geoguessr.zendesk.com/hc/en-us/articles/9486501024401-What-is-GeoGuessr->
- <https://geointblog.wordpress.com/2020/12/21/le-ministere-de-linterieur-inscrit-le-geoint-dans-son-livre-blanc/>
- <https://somerandomstuff1.wordpress.com/2019/02/08/geoguessr-the-top-tips-tricks-and-techniques/>
- <https://www.openstreetmap.org/about>
- https://wiki.osmfoundation.org/wiki/Main_Page
- https://www.reddit.com/r/pics/comments/y0d2zr/russia_bombed_a_playground_as_revenge_against/



@volker_carstein

Challenge time !

- 3 challenges en tout
- Le but de chaque challenge est précisé sur la slide associé
- Pas de métadonnées dans les images
- Deux catégories de gagnant : avec/sans recherche inversée d'image
- Explications à envoyer... (parce que juste donner la réponse ne compte pas !)
 - en MP Discord (Volker#2998)
 - ou via Twitter (@volker_carstein)
- Une bière/soft pour le premier solve de chaque catégorie pour chaque image !



@volker_carstein

Challenge 1

But : Trouver le nom de l'entreprise dont le siège social est le bâtiment à droite sur la photo
<https://bit.ly/3rVlZM7>

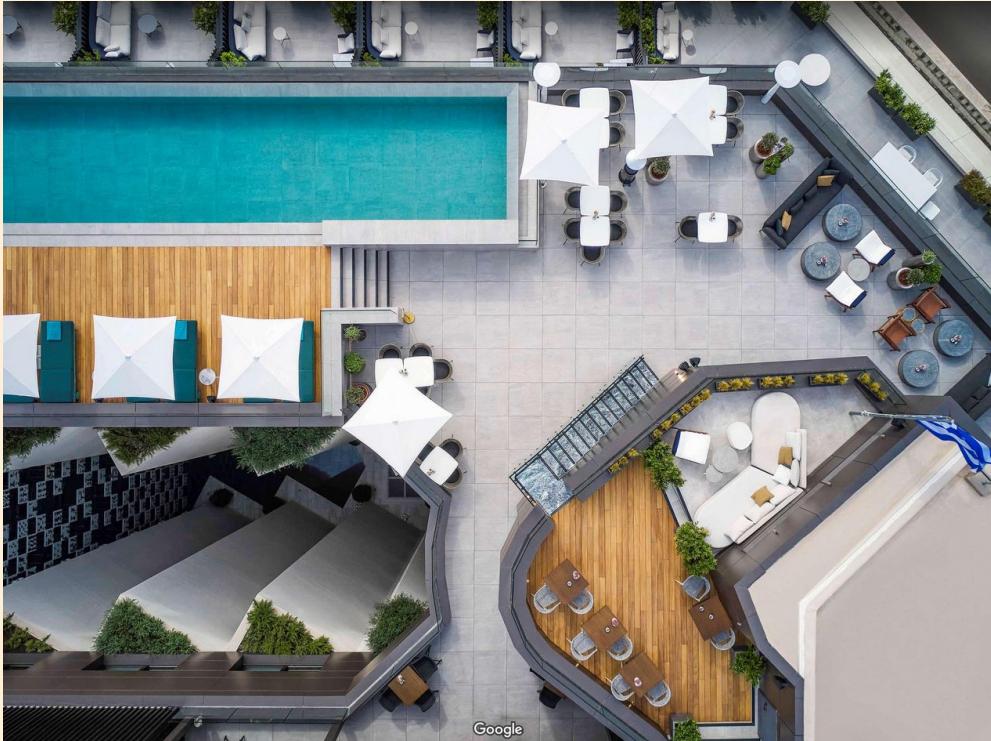


@volker_carstein

Challenge 2

But : Trouver les coordonnées GPS du bâtiment + le nom du directeur

<https://bit.ly/3TnmKcj>



@volker_carstein

Challenge 3

But : Trouver la superficie globale du parc depuis lequel la photo a été prise

<https://bit.ly/3Tpxs28>



@volker_carstein

Thanks !

GEOINT - Devenez un
GeoGuessr Master

SecSea 2k22 - 15/10/2022

