WORKSHOP GEOINT

LeHack 2024

@volker_carstein

Slides !

https://blog.volkercarstein.com/lehack_2024_geoint_workshop_slides.pdf

@volker_carstein

Briefing

1. Les bases du GEOINT
2. Apprendre à utiliser Overpass Turbo
3. Exemples d'utilisation
4. Challenge time

@volker_carstein

Who am I ?

Volker Carstein (@volker_carstein)

- Pentester le jour, jack of all trades la nuit
- Ingénierie sociale, OSINT et sécurité offensive (préférence pour l'Active Directory)
- Speaker @ LeHack, Barbhack, Insomni'hack, SecSea, etc

Les bases du GEOINT : définitions

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.

MINISTÈRE
DE L’INTÉRIEUR
Liberté
Égalité
Fraternité

@volker_carstein

Les bases du GEOINT : 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

Méthodologie +
compréhension du contexte/sujet

Recherche de **marqueurs explicites**

@volker_carstein

Les bases du GEOINT : marqueurs explicites

- Proviennent souvent d'un recoupement
- Servent une ou plusieurs tâches : géolocalisation, horodatage, etc.
- Peuvent constituer une information de valeur
- Noms de rues ou bâtiments particuliers
- Éléments géographiques distinctifs
- Soleil et météo

Apprendre à utiliser Overpass Turbo

- **OpenStreetMap** : Projet de cartographie libre
- Données géographiques basée 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”
- Attention : Données parfois incomplètes ou erronées

Apprendre à utiliser Overpass Turbo

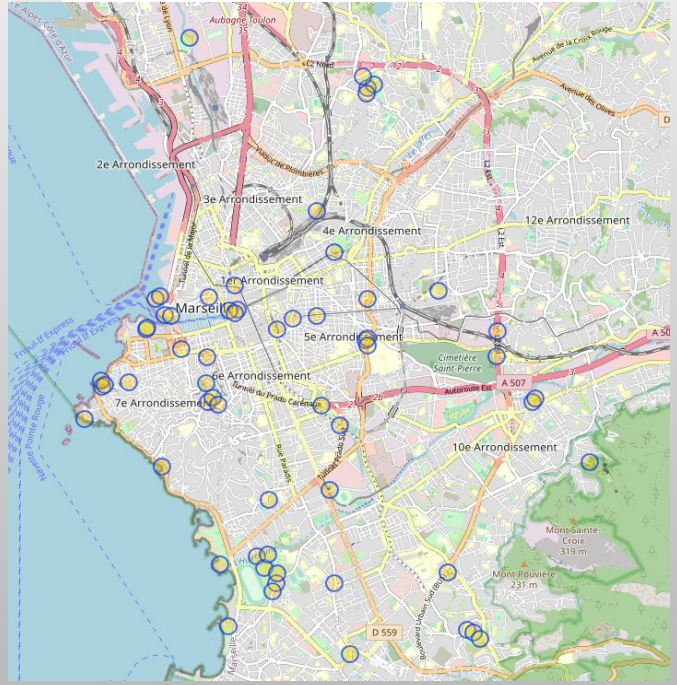
- **Overpass** : API en lecture seule des données OSM
- **Overpass Turbo** : Interface web pour Overpass (https://overpass-turbo.eu/)
- But : Recouper des informations géographiques pour extraire de la valeur
- La ressource indispensable : https://wiki.openstreetmap.org/wiki/Main_Page
- Ready ?

@volker_carstein

Apprendre à utiliser Overpass Turbo

- 3 types d'objets + 1 special (area)
  - 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
- {{bbox}} : Zone de la fenêtre OSM (area spéciale)

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



@volker_carstein

Apprendre à utiliser Overpass Turbo

- Grammaire d'une requête

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

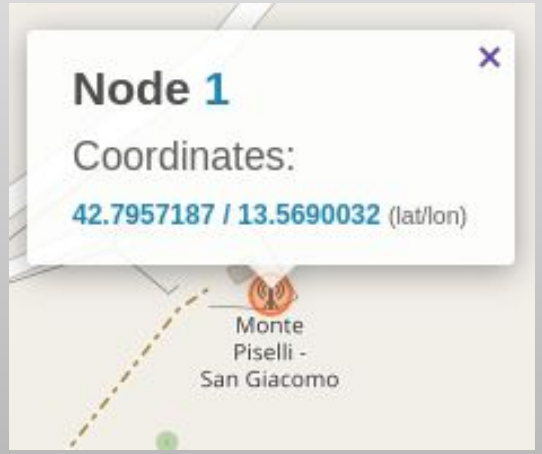
- Type d'objet :
- Tag
- Tag value
- Emprise/portée

@volker_carstein

Apprendre à utiliser Overpass Turbo

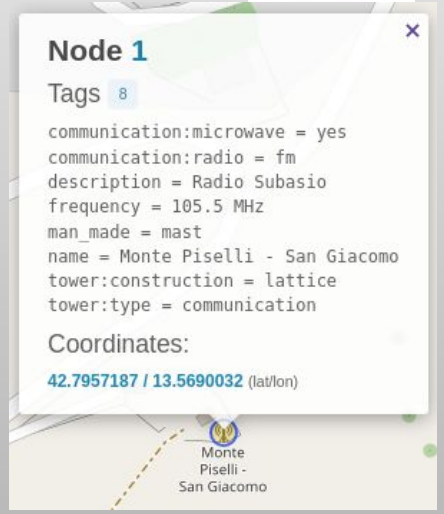
- 3 verbosités d'output : skel, body (default), meta

```
node(1);
out skel;
```




```
node(1);
out;
```

```
node(1);
out body;
```




```
node(1);
out meta;
```

Apprendre à utiliser Overpass Turbo

- 3 gestion de l'emprise
- Requêtes possibles
  - node, way, relation
  - nw (node + way)
  - nwr (node + way + relation)

```
node({{bbox}});

node(42.7957187, 13.5690032, 59.7717926, 30.32611);

{{geocodeArea:"Italia"}} -> .searchArea;
node(area.searchArea);

out;
```

```
node({{bbox}});
way({{bbox}});
relation({{bbox}});

nw({{bbox}});

nwr({{bbox}});
```


@volker_carstein

Apprendre à utiliser Overpass Turbo

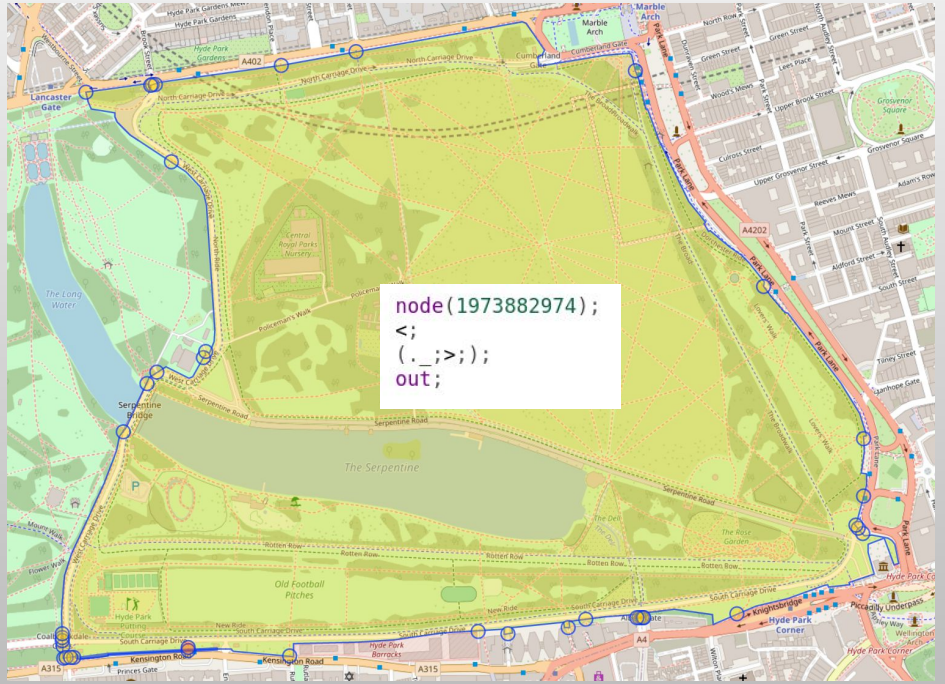
- Récursivité montante / descendante

```
<; // remonte d'un niveau (par ex: node -> way)
<<; //remonte toute l'arborescence (partant d'un node, node -> way -> relation)
```

```
>; // descends d'un niveau (par ex: way -> node)
>>; // descends toute l'arborescence (partant d'une relation, relation -> way -> node)
```


@volker_carstein

Apprendre à utiliser Overpass Turbo



Apprendre à utiliser Overpass Turbo

- Lier des requêtes ensembles

```
node[amenity=restaurant]({{bbox}});
node(around:200)[amenity=cinema];
```

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


@volker_carstein

Apprendre à utiliser Overpass Turbo

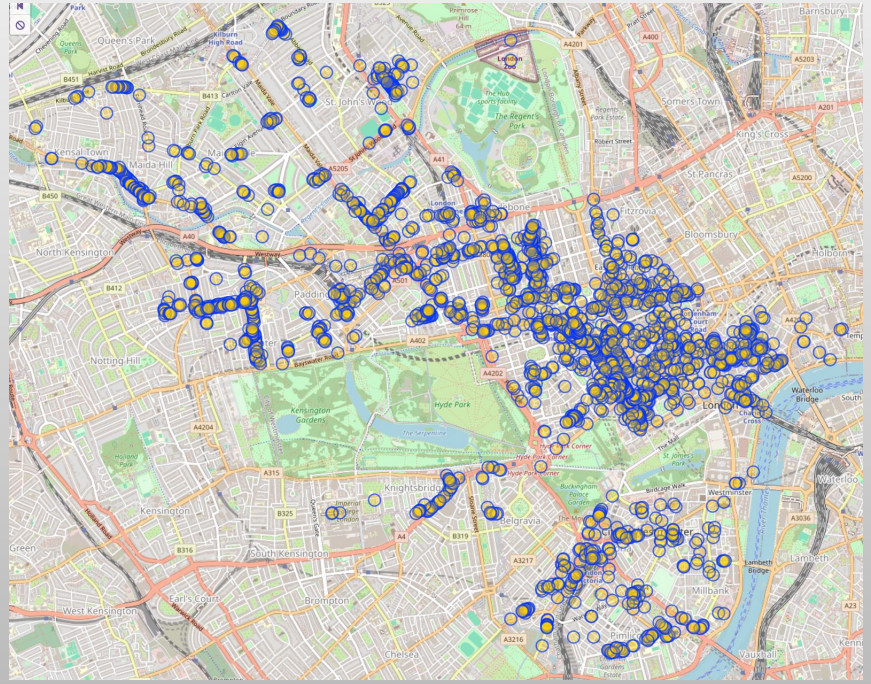
- Logique conditionnelle

```
[out:json];
{{geocodeArea:"Marseille"}} -> .searchArea;

(nwr["addr:housenumber"]
    (if: (is_number(t["addr:housenumber"]) && t["addr:housenumber"] < 3)) (area.searchArea);
);

>;
out;
```

Apprendre à utiliser Overpass Turbo

- Transformer une relation en emprise

```
relation(51781);
map_to_area -> .zone;
node["shop"](area.zone);
/*added by auto repair*/
(._;>;);
/*end of auto repair*/
out;
```

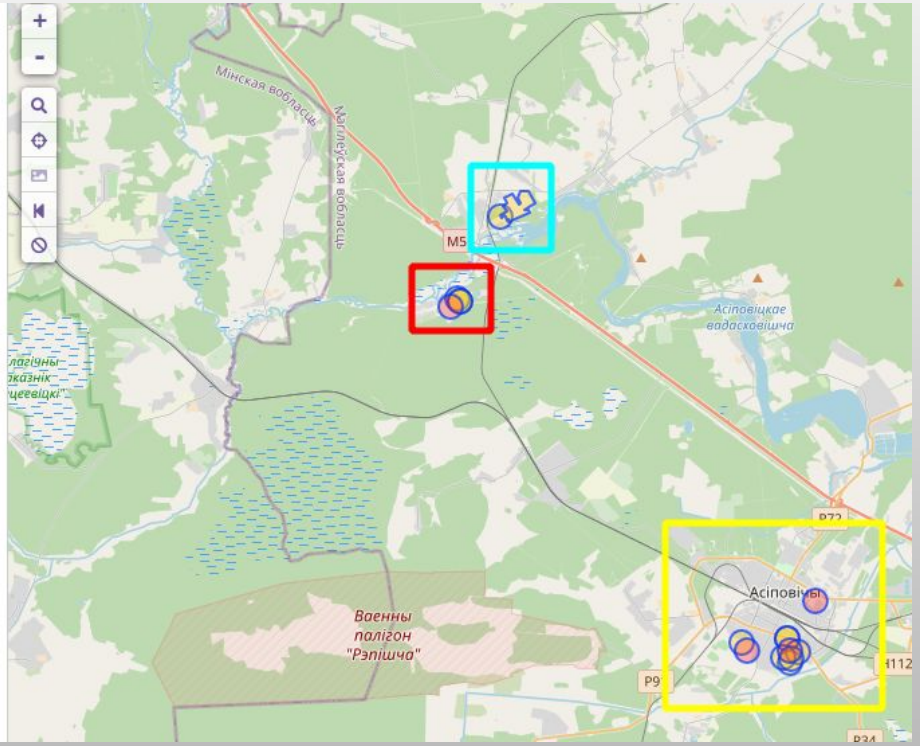


Cas réel : Overpass Turbo + SentinelHub

- Base militaire “near Osipovichi”, Belarus (source Armytimes)

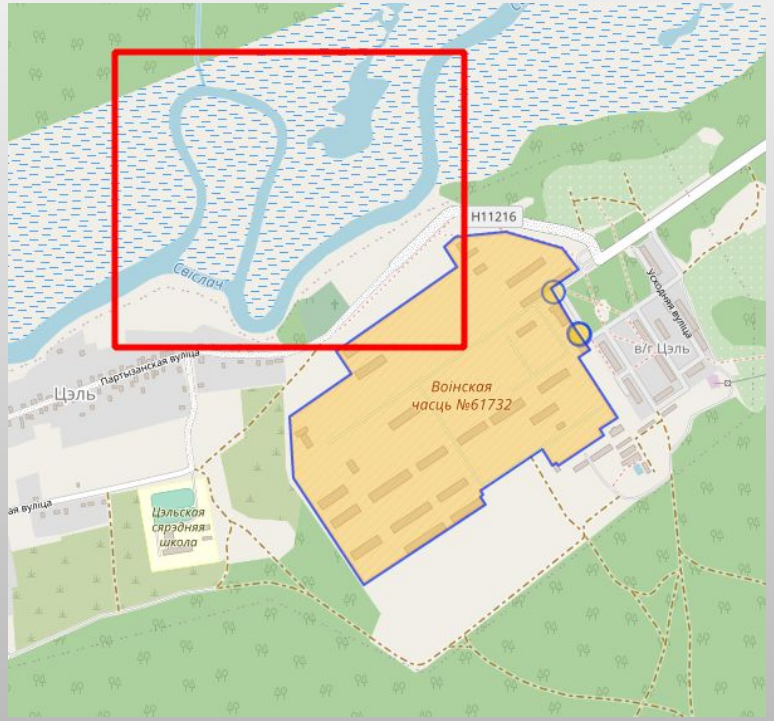
Cas réel : Overpass Turbo + SentinelHub

```
{{geocodeArea:"Belarus"}} -> .searchArea;

node["name"="Асіповічы"]["place"="town"](area.searchArea);
nwr(around:15000)[landuse=military] -> .camps;
nwr(around.camps:1000)[waterway=river] -> .rivers;
nwr(around.rivers:1000)[sport] -> .sportfield;
nwr(around.sportfield:2000)[landuse=military];

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



@volker_carstein

Cas réel : Overpass Turbo + SentinelHub



53.397289, 28.4714977

Cas réel : Overpass Turbo + SentinelHub

8 mai 2023

13 août 2023

@volker_carstein

Challenge time !

http://workshop.volkercarstein.com/