



WORKSHOP GEOINT

Barbhack 2023

Slides !



https://blog.volker-carstein.com/geoint_workshop_slides.pdf

Briefing

1. Tour d'horizon des tools du jour
2. Apprendre à utiliser Overpass Turbo
3. Apprendre à utiliser les autres tools
4. Challenge time

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, SecSea, AMUSEC

Tour d'horizon des tools du jour

- Overpass Turbo (duh)
- Recherche d'image inversée (Google, Yandex)
- Street View, Yandex View
- Metadonnées des images
- Google Maps/Earth, SentinelHub, satellite.pro
- Ventusky
- Mentions honorables (out-of-scope) : Suncalc, Mappilary, Maphub, Peak Visor

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



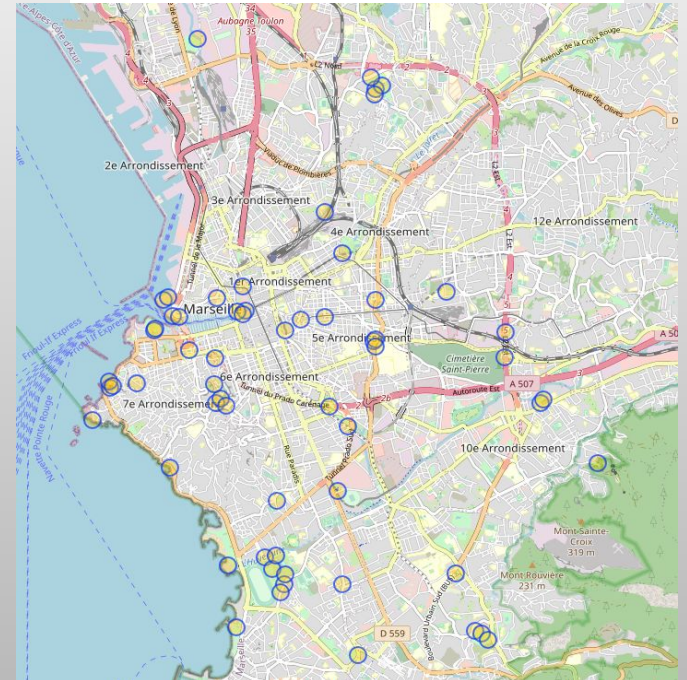
Apprendre à utiliser Overpass Turbo

- **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
- Ready ?

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

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



Apprendre à utiliser Overpass Turbo

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

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

Node 1

Coordinates:
[42.7957187 / 13.5690032](#) (lat/lon)

Monte Piselli - San Giacomo

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

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

Node 1

Tags 8

communication:microwave = yes
communication:radio = fm
description = Radio Subasio
frequency = 105.5 MHz
man_made = mast
name = Monte Piselli - San Giacomo
tower:construction = lattice
tower:type = communication

Coordinates:
[42.7957187 / 13.5690032](#) (lat/lon)

Monte Piselli - San Giacomo

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

Node 1

Tags 8

communication:microwave = yes
communication:radio = fm
description = Radio Subasio
frequency = 105.5 MHz
man_made = mast
name = Monte Piselli - San Giacomo
tower:construction = lattice
tower:type = communication

Meta

timestamp = 2022-07-28T09:47:39Z
version = 33
changeset = [124176968](#)
user = [owene](#)
uid = 29598

Coordinates:
[42.7957187 / 13.5690032](#) (lat/lon)

Monte Piselli - San Giacomo

Apprendre à utiliser Overpass Turbo

- 3 gestion de la zone de recherche
- 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}});
```

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];
```

Apprendre à utiliser les autres outils


- Recherche d'image inversée (Google, Yandex)
- Street View, Yandex View
- Metadonnées des images
- Google Maps/Earth, SentinelHub, satellite.pro
- Ventusky

Metadonnées des images

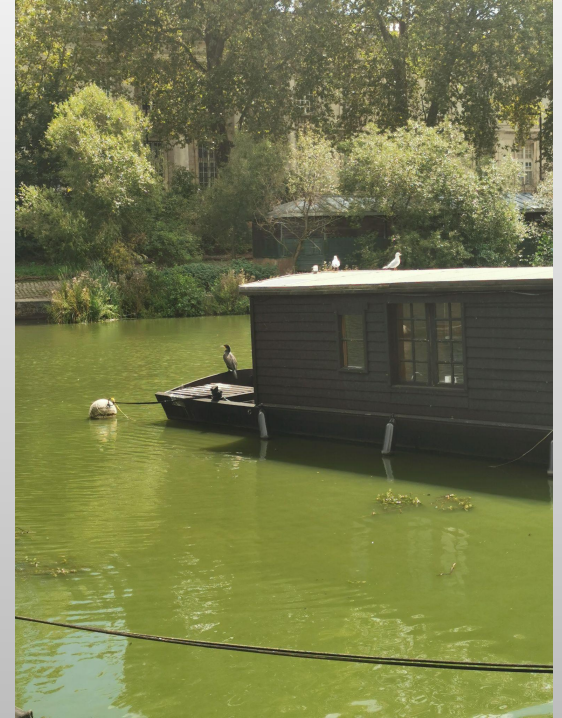
- EXIF tool (en local ou en ligne sur <https://exif.tools/>)

GPS Latitude 

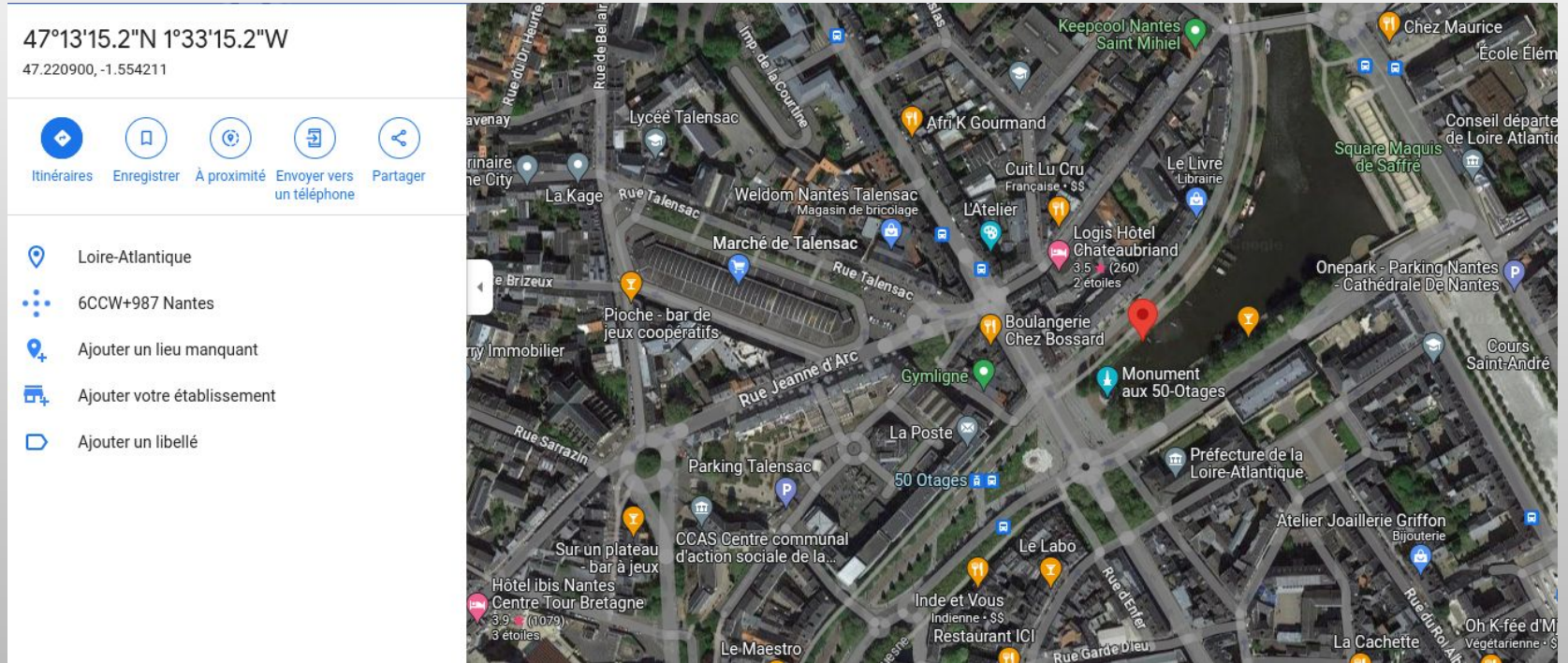
47° 13' 15.24" N

GPS Longitude 

1° 33' 15.16" W



Metadonnées des images



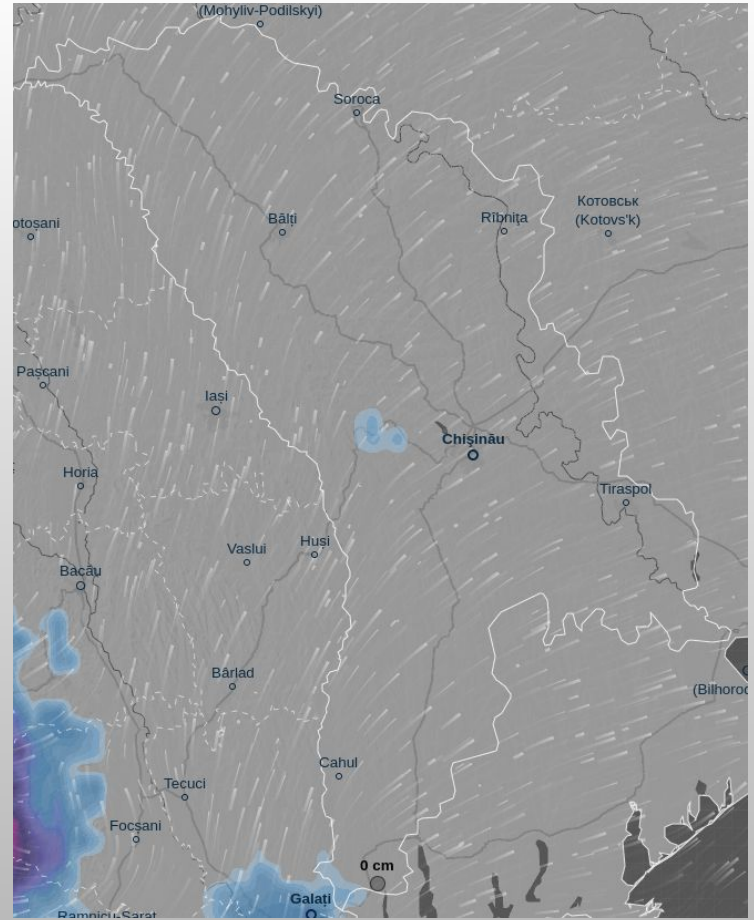
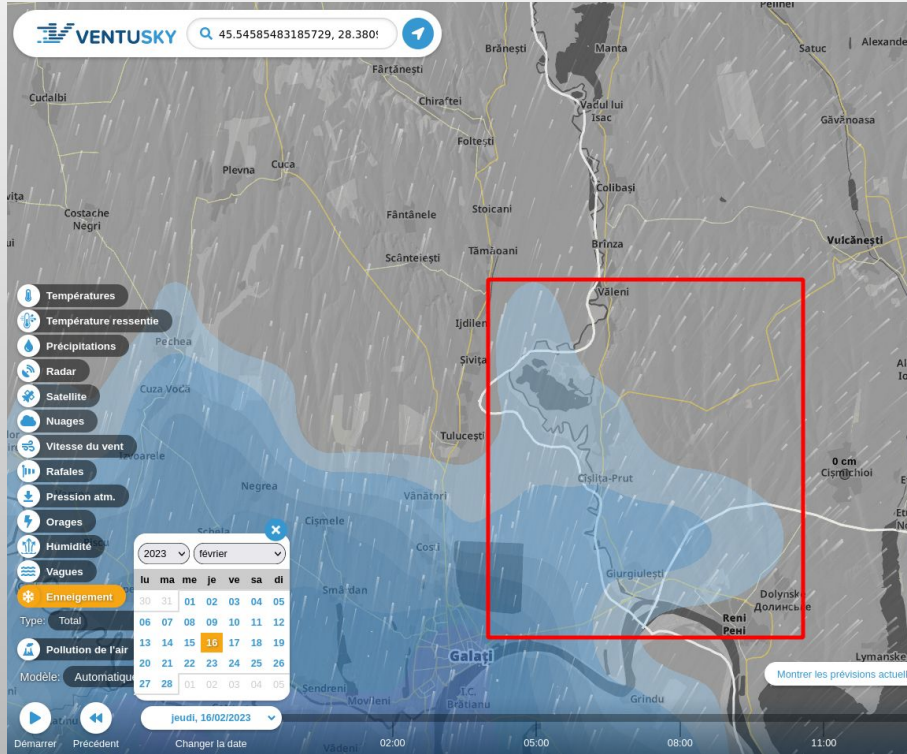
Ventusky

Merci à Projet FOX d'avoir fourni l'exemple : <https://discord.gg/nxdfsWBNRK>

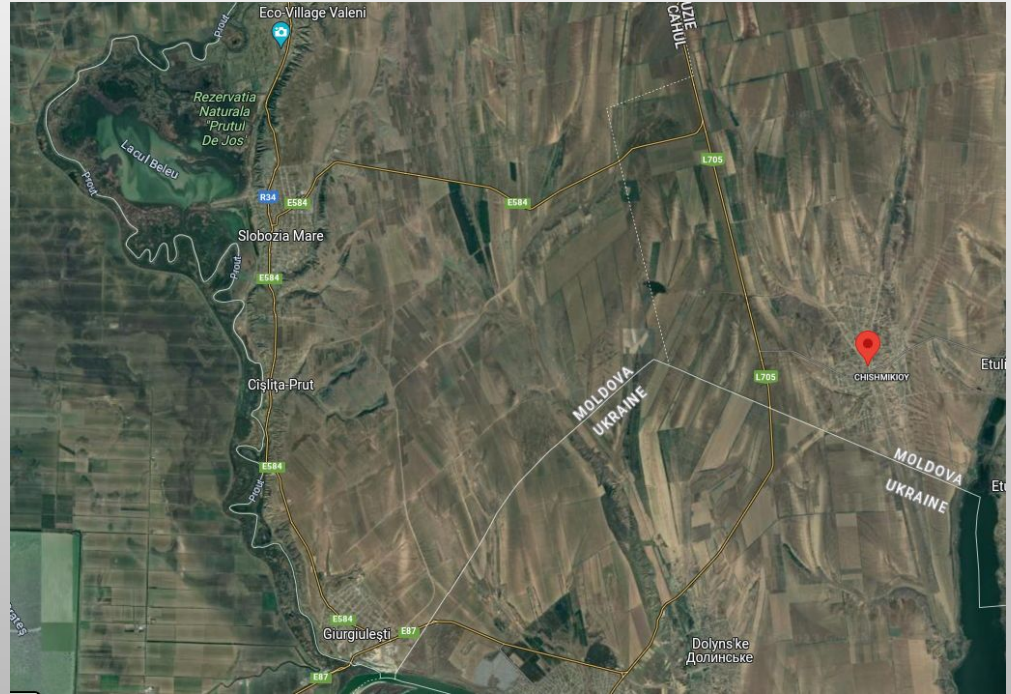
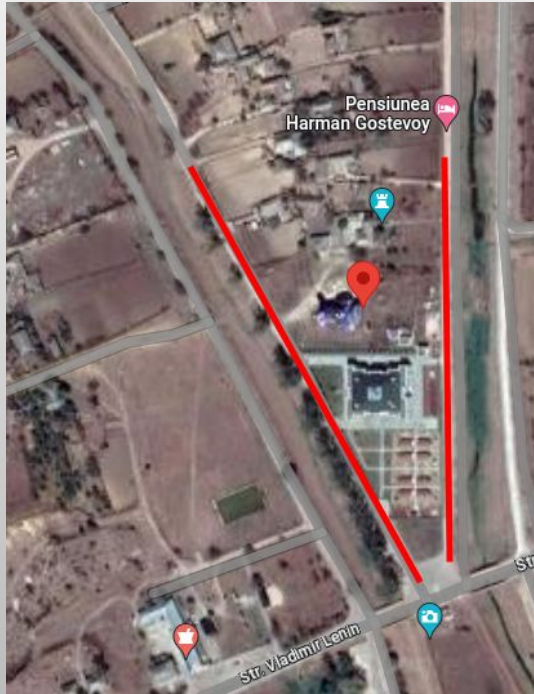
- Timelapse satellite via SentinelHub, moitié sud de la Moldavie



Ventusky



Ventusky



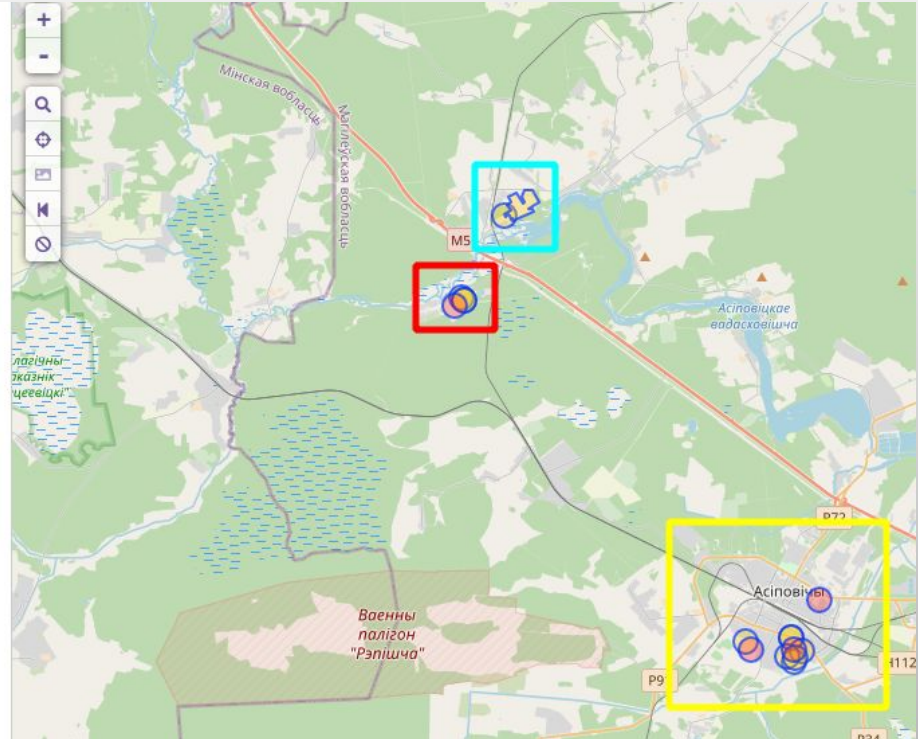
Cas réel : Overpass Turbo + SentinelHub

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



Cas réel : Overpass Turbo + SentinelHub

```
1  {{geocodeArea:"Belarus"}} -> .searchArea;
2
3  node["name"="Асіновічы"]["place"="town"](area.searchArea);
4  nwr(around:15000)[landuse=military] -> .camps;
5  nwr(around.camps:1000)[waterway=river] -> .rivers;
6  nwr(around.rivers:1000)[sport] -> .sportfield;
7  nwr(around.sportfield:2000)[landuse=military];
8
9  /*added by auto repair*/
10 (.;>);
11 /*end of auto repair*/
12 out;
```



Cas réel : Overpass Turbo + SentinelHub



53.397289, 28.4714977



Cas réel : Overpass Turbo + SentinelHub

8 mai 2023



13 août 2023



Challenge time !



"GEOINT Trooper" sticker : 1050 points.

"GEOINT Master" sticker : 2050 points.

Good luck, and Hack the planet !

<http://workshop.volkercarstein.com/>