IPSeen : Assigning organizational labels to IP addresses to enhance security analysis

To qualify a pool of IP !

July 5, 2022

Camille Moriot, PhD Student
Contact email: camille.moriot@insa-lyon.fr

Code available : https://gitlab.inria.fr/cmoriot/ipseen

François Lesueur
Associate Professor
IRISA - Université Bretagne Sud.

Nicolas Stouls
Associate Professor
CITI - INSA Lyon.

Fabrice Valois
Professor
CITI - INSA Lyon.

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

citi lab

Inria

UNIVERSITÉ DE LYON

UMR IRISA

Université Bretagne Sud

Current IP characterization

- Objective : characterizing attack's infrastructures

ONYPHE

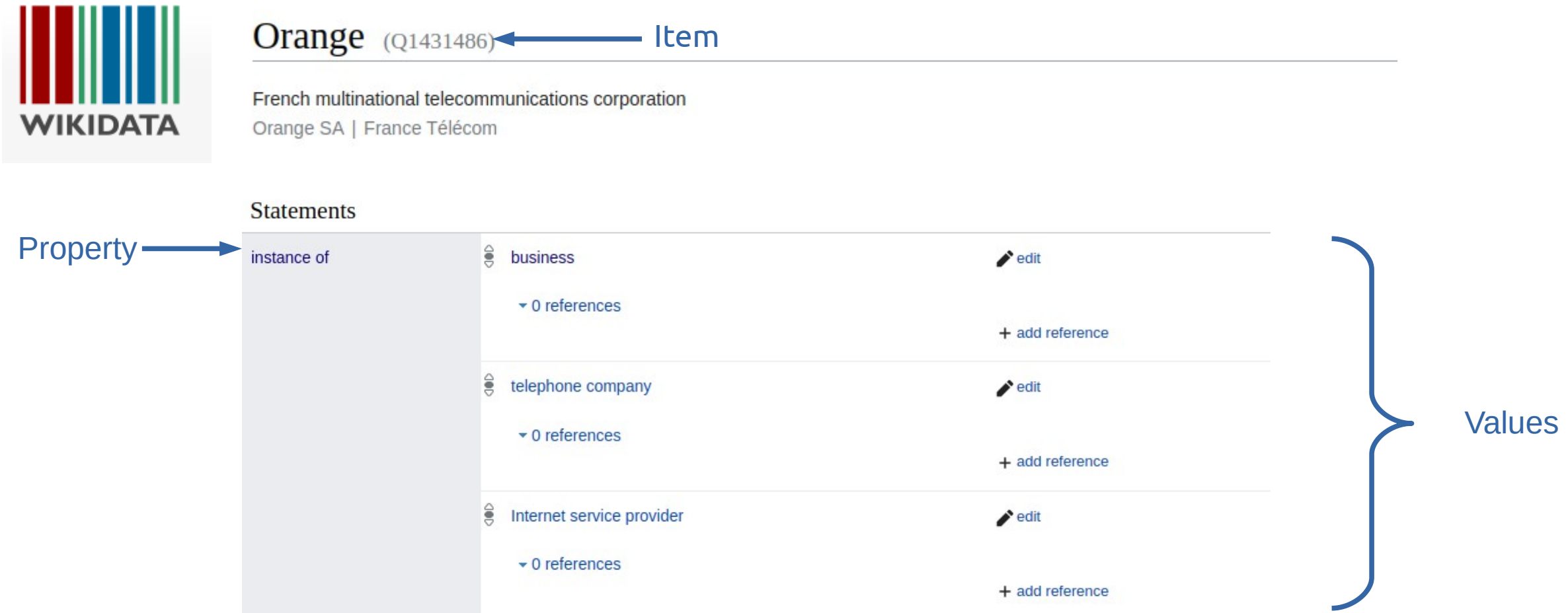
Censys

SHODAN

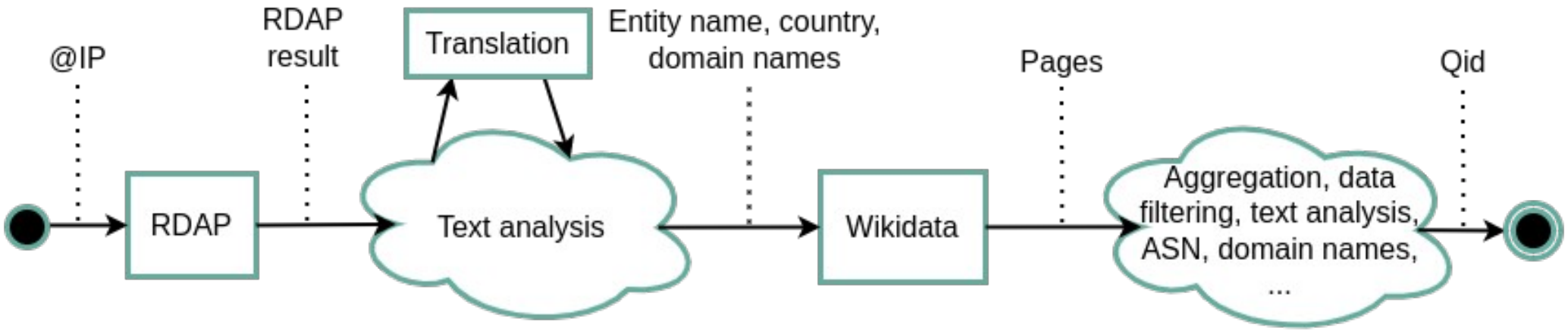
Characterization of the technical infrastructure : type of devices, open ports

Organizational structure

Using Wikidata to obtain organizational labels



How to find information in Wikidata starting from an IP address ?



Example

- ./ipseen 195.101.52.78

```
label : Orange
industryLabel : ['internet industry', 'television', 'telecommunications']
typeLabel : ['mobile network operator', 'telephone company', 'public compa
ny', 'brand', 'Internet service provider', 'enterprise', 'business']
employees : ['132002', '155202', '156000', '165000']
subscribers : ['201700000']
```

- ./ipseen 193.48.64.13

```
193.48.64.13 is in wiki
label : Renater
typeLabel : ['network service provider', 'national
 research and education network']
```