Trouver de l'information sur un nom de domaine

Stéphane Bortzmeyer
stephane+jdll@bortzmeyer.org

JDLL - 25 mai 2024

Le problème

Le problème

- Quelque chose ne va pas avec un nom de domaine et on veut des informations pour agir.

Le problème

- Quelque chose ne va pas avec un nom de domaine et on veut des informations pour agir.
- Vous avez déjà eu le cas ?

Le problème

- Quelque chose ne va pas avec un nom de domaine et on veut des informations pour agir.
- Vous avez déjà eu le cas ?
- Quelles informations cherchiez-vous ?

Le problème

- Quelque chose ne va pas avec un nom de domaine et on veut des informations pour agir.
- Vous avez déjà eu le cas ?
- Quelles informations cherchiez-vous ?
- Quelles méthodes et outils avez-vous utilisés ?

Les attributs d'un nom de domaine

Les attributs d'un nom de domaine

- En général, un nom de domaine a :
  - Un titulaire,
  - Un contact administratif
  - Un contact technique
  - Un registre
  - Un BE (Bureau d'Enregistrement)

Les attributs d'un nom de domaine

- En général, un nom de domaine a :
  - Un titulaire,
  - Un contact administratif
  - Un contact technique
  - Un registre
  - Un BE (Bureau d'Enregistrement)
- Mais attention, **ça dépend**. Je vous le dirai souvent mais **je simplifie, en fait, c'est plus compliqué que cela**.

Les attributs d'un nom de domaine

- En général, un nom de domaine a :
  - Un titulaire,
  - Un contact administratif
  - Un contact technique
  - Un registre
  - Un BE (Bureau d'Enregistrement)
- Mais attention, **ça dépend**. Je vous le dirai souvent mais **je simplifie, en fait, c'est plus compliqué que cela**.
- L'industrie des noms de domaine est compliquée.

Les données ne sont pas toujours publiques

Les données ne sont pas toujours publiques

- Loi Informatique & Libertés en France,

Les données ne sont pas toujours publiques

- Loi Informatique & Libertés en France,
- Autres lois,

Les données ne sont pas toujours publiques

- Loi Informatique & Libertés en France,
- Autres lois,
- Politique du registre.

Et quand elles sont publiques

Et quand elles sont publiques

- Elles peuvent être incorrectes, depuis le début, ou bien par dégradation avec le temps.

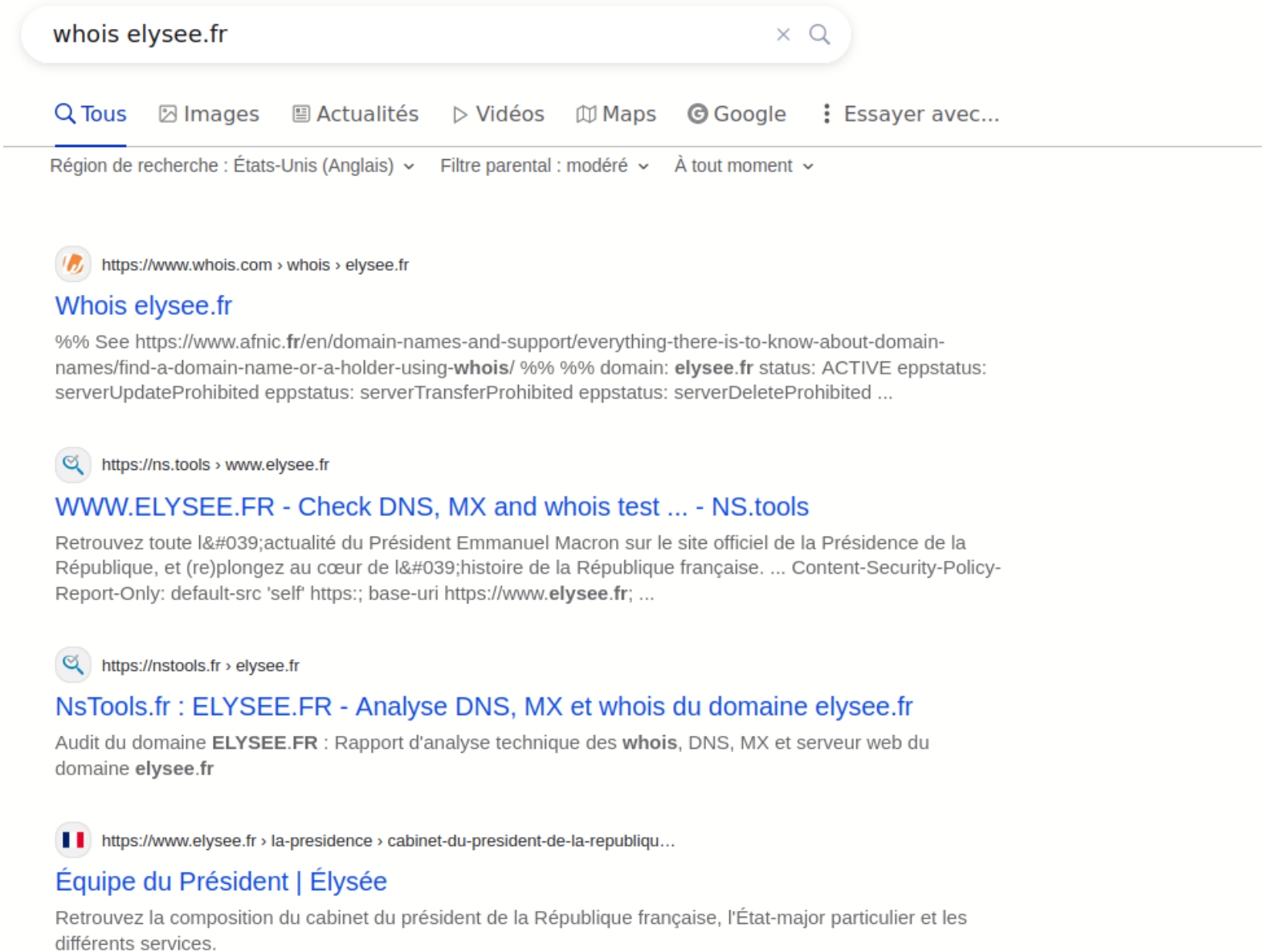
Et quand elles sont publiques

- Elles peuvent être incorrectes, depuis le début, ou bien par dégradation avec le temps.
- Elles peuvent être mal interprétées (99 % des messages sur Twitter quand le type-qui-s-y-connait joue à l'investigation numérique).

Et quand elles sont publiques

- Elles peuvent être incorrectes, depuis le début, ou bien par dégradation avec le temps.
- Elles peuvent être mal interprétées.
- Les outils sont faciles à utiliser, leur résultat difficile à interpréter.

La mauvaise méthode



Pourquoi ce n'est pas bien

Pourquoi ce n'est pas bien

- Les algorithmes du moteur de recherche ont pu vous entrainer n'importe où,

Pourquoi ce n'est pas bien

- Les algorithmes du moteur de recherche ont pu vous entrainer n'importe où,
- Les plate-formes qui relaient vos requêtes vers le registre peuvent mentir ou, plus souvent, servir des résultats dépassés.

Pourquoi ce n'est pas bien

- Les algorithmes du moteur de recherche ont pu vous entrainer n'importe où,
- Les plate-formes qui relaient vos requêtes vers le registre peuvent mentir ou, plus souvent, servir des résultats dépassés.
- Il faut une source **qui fasse autorité**, en général le registre.

Les méthodes

On parle parfois de RDDS (*Registration Data Directory Services*).

Les méthodes

On parle parfois de RDDS.

- Web

Les méthodes

On parle parfois de RDDS.

- Web
- RDAP (*Registration Data Access Protocol*)

Les méthodes

On parle parfois de RDDS.

- Web
- RDAP
- whois (RFC 3912)

Web

Web

- Simple et connu,

Web

- Simple et connu,
- Principal problème : il faut connaitre le site Web du registre,

Web

- Simple et connu,
- Principal problème : il faut connaitre le site Web du registre,
- Solution : `https://www.iana.org/domains/root/db`.
  Notez que cela ne marche pas pour `.com`.

RDAP

Registration Data Directory Services

RDAP

- Surtout pour les programmeureuses,

RDAP

- Surtout pour les programmeureuses,
- Permet des traitements automatisés (surveillance de l'expiration, contrôle des serveurs de noms, des changements de titulaire...),

RDAP

- Surtout pour les programmeureuses,
- Permet des traitements automatisés,
- HTTPS + JSON,

RDAP

- Surtout pour les programmeureuses,
- Permet des traitements automatisés,
- HTTPS + JSON,
- `https://lookup.icann.org/` est un client RDAP en Javascript : Web et RDAP en même temps,

RDAP

- Surtout pour les programmeureuses,
- Permet des traitements automatisés,
- HTTPS + JSON,
- `https://lookup.icann.org/` est un client RDAP en Javascript : Web et RDAP en même temps,
- Pas beaucoup de clients perfectionnés.

Principal problème : pas déployé partout.

whois

whois

- Le traditionnel, toujours très utilisé,

whois

- Le traditionnel, toujours très utilisé,
- Format non structuré et non standard mais beaucoup d'outils pour l'analyser,

whois

- Le traditionnel, toujours très utilisé,
- Format non structuré et non standard mais beaucoup d'outils pour l'analyser,
- Il faut indiquer le serveur mais la plupart des clients whois utilisent des heuristiques qui vous en dispensent.

Et encore d'autres pièges

Et encore d'autres pièges

- Il y a les registres épais (l'information sociale est au registre), ce sont la grande majorité,

Et encore d'autres pièges

- Il y a les registres épais (l'information sociale est au registre),
- et les registres minces (l'information sociale est au BE),

Et encore d'autres pièges

- Il y a les registres épais (l'information sociale est au registre),
- et les registres minces (l'information sociale est au BE),
- RDAP sait gérer. Les clients whois se débrouillent en général.