

# 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 cherchez-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-connaît 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



[Tous](#) [Images](#) [Actualités](#) [Vidéos](#) [Maps](#) [Google](#) [Essayer avec...](#)

Région de recherche : États-Unis (Anglais) [v](#)    Filtre parental : modéré [v](#)    À tout moment [v](#)

<https://www.whois.com/whois/elysee.fr>

## Whois elysee.fr

See <https://www.afnic.fr/en/domain-names-and-support/everything-there-is-to-know-about-domain-names/find-a-domain-name-or-a-holder-using-whois/> domain: **elysee.fr** status: ACTIVE eppstatus: serverUpdateProhibited eppstatus: serverTransferProhibited eppstatus: serverDeleteProhibited ...

<https://ns.tools/www.elysee.fr>

## WWW.ELYSEE.FR - Check DNS, MX and whois test ... - NS.tools

Retrouvez toute l'actualité du Président Emmanuel Macron sur le site officiel de la Présidence de la République, et (re)plongez au cœur de l'histoire de la République française. ... Content-Security-Policy-Report-Only: default-src 'self' https;; base-uri https://www.elysee.fr; ...

<https://nstools.fr/elysee.fr>

## NsTools.fr : ELYSEE.FR - Analyse DNS, MX et whois du domaine elysee.fr

Audit du domaine **ELYSEE.FR** : Rapport d'analyse technique des **whois**, DNS, MX et serveur web du domaine **elysee.fr**

<https://www.elysee.fr/la-presidence/cabinet-du-president-de-la-republi...>

## Équipe du Président | Élysée

Retrouvez la composition du cabinet du président de la République française, l'État-major particulier et les différents services.

# Pourquoi ce n'est pas bien

## Pourquoi ce n'est pas bien

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

## Pourquoi ce n'est pas bien

- Les algorithmes du moteur de recherche ont pu vous entraîner 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 entraîner 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 connaître le site Web du registre,

# Web

- Simple et connu,
- Principal problème : il faut connaître 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 programmeuses,

# RDAP

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

# RDAP

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

# RDAP

- Surtout pour les programmeuses,
- 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 programmeuses,
- 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.