Premiers essais avec le résolveur public DNS4EU

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 5 juin 2025

https://www.bortzmeyer.org/dns4eu.html

On n'y croyait plus mais le résolveur <https://www.bortzmeyer.org/resolveur-dns.html> DNS public DNS4EU <https://www.joindns4.eu/> est désormais disponible <https://www.joindns4.eu/for-public>. Il ne présente pas d'intérêt pratique (il y a déjà beaucoup de résolveurs, y compris publics, y compris européens) mais c'est toujours bien d'élargir le parc. La diversité est une bonne chose.

Leur page d'accueil <https://www.joindns4.eu/for-public> donne les adresses IP à utiliser, après des années d'attente. Comme tous les résolveurs sérieux, il a, en plus des traditionnels UDP et TCP, les transports DoT et DoH (mais pas DoQ mais, bon, ce dernier est nettement moins fréquent aujourd'hui). Comme tous les résolveurs sérieux, il a une adresse IPv4 et une IPv6. En fait, il a même plusieurs adresses dans chaque famille, correspondant à des niveaux de filtrage différents. Aucune de ces adresses n'est spécialement mémorisable, contrairement à dns.sb.

Premier test simple, avec l'adresse mise en avant, "*Protective Resolution*" (tiens, le site Web ne semble exister qu'en anglais, ce qui est curieux pour un projet européen) :

```
% kdig +tls @2a13:1001::86:54:11:1 frnog.org
;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(ECDSA-SECP256R1-SHA256)-(AES-256-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 39597
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 1400 B; ext-rcode: NOERROR
;; PADDING: 410 B

;; QUESTION SECTION:
;; frnog.org.            IN A

;; ANSWER SECTION:
frnog.org.           86400 IN A 213.186.34.12

;; Received 468 B
;; Time 2025-06-04 20:14:45 CEST
;; From 2a13:1001::86:54:11:1@853(TLS) in 190.0 ms
```

OK, tout marche, on s'en doutait, mais c'est bien de vérifier.

Ce premier service ment pour les noms qui sont utilisés à des fins malveillantes. Je n'ai pas de tels noms sous la main tout de suite alors j'ai regardé dans ma boite aux lettres de spams mais les noms testés sont tous acceptés.

D'autres services sont proposés, par exemple "*Protective resolution with child protection & ad-blocking*". Si je l'essaie sur un site porno :

```
% kdig +tls @2a13:1001::86:54:11:11 pornhub.com
;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(ECDSA-SECP256R1-SHA256)-(AES-256-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 679
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0

;; QUESTION SECTION:
;; pornhub.com.          IN A

;; ANSWER SECTION:
pornhub.com.         1 IN A 51.15.69.11

;; Received 45 B
;; Time 2025-06-04 20:22:52 CEST
;; From 2a13:1001::86:54:11:11@853(TLS) in 17.9 ms
```

L'adresse renvoyée n'a rien à voir avec Pornhub et elle héberge un serveur HTTP qui redirige ensuite vers...`localhost`. Bon, ça protège du porno, mais j'avoue ne pas comprendre le comportement du serveur HTTP.

Bien que ce service soit censé protéger de la pub, il dit la vérité (malheureusement) pour des noms comme `google-analytics.com`. Pour `googletagmanager.com`, il renvoie un amusant `0.0.0.0`. Aucune utilisation n'est faite des EDE du RFC 8914 [1], hélas, contrairement à ce que fait Google Public DNS quand il ment. Je n'ai pas encore vu de signe de censure étatique (par exemple au profit des ayant-droits).

Regardons maintenant son hébergement. Il utilise des adresses IP allouées à Whalebone <`https://www.whalebone.io/`>, leader du consortium, ou bien à l'opérateur KCOM (mais elles restent à l'ancien nom, Mistral, les bases des RIR ne sont pas toujours bien fraiches). Voyons combien il y a d'instances différentes, avec Blaeu <`https://framagit.org/bortzmeyer/blaeu`> :

```
%  blaeu-resolve --requested 200 --nsid --nameserver 2a13:1001::86:54:11:1  www.bortzmeyer.org
Nameserver 2a13:1001::86:54:11:1
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eiu-mil-01;] : 40 occurrences
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-fra-01;] : 35 occurrences
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-ams-01;] : 55 occurrences
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-prg-01;] : 5 occurrences
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-par-01;] : 33 occurrences
[TIMEOUT] : 9 occurrences
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-mad-01;] : 7 occurrences
```

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc8914.txt`

```
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-sto-01;] : 7 occurrences
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: ;] : 2 occurrences
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-waw-01;] : 2 occurrences
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-sof-01;] : 1 occurrences
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: None;] : 1 occurrences
Test #107704910 done at 2025-06-04T18:31:21Z
```

À part les quelques cas où un relais transparent interceptait les requêtes DNS et renvoyaient un NSID (RFC 5001) trompeur, on voit qu'il y a actuellement neuf instances. (On voit un peu plus d'instances en utilisant l'adresse IPv4 du résolveur.) L'affichage du temps de réponse est compatible avec des serveurs entièrement en Europe (ce qui est logique pour un service européen, le résolveur indien <https://www.bortzmeyer.org/resolveur-inde.html> a fait un choix analogue) :

```
%  blaeu-resolve --old-measurement 107705432 --nsid --displayrtt --nameserver 86.54.11.1  www.bortzmeyer.org
Nameserver 86.54.11.1
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-par-01;] : 113 occurrences Average RTT 13
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-fra-01;] : 22 occurrences Average RTT 152
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eiu-mil-01;] : 10 occurrences Average RTT 13
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-prg-01;] : 5 occurrences Average RTT 138 m
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-ams-01;] : 31 occurrences Average RTT 117
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: None;] : 4 occurrences Average RTT 14 ms
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-mad-01;] : 2 occurrences Average RTT 123 m
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: 90m8;] : 1 occurrences Average RTT 156 ms
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: ;] : 3 occurrences Average RTT 1 ms
[TIMEOUT] : 5 occurrences
[2001:4b98:dc0:41:216:3eff:fe27:3d3f 2602:fbb1:1:245b::42 NSID: dns4eu-bud-01;] : 3 occurrences Average RTT 251 m
Test #107705867 done at 2025-06-04T18:41:34Z
```

(Une première mesure, la 107705432, avait servi à remplir la mémoire des résolveurs, afin que le temps de réponse dépende surtout du résolveur, pas des serveurs faisant autorité interrogés. Elle avait indiqué `--area West`, donc l'Amérique.) Le temps de réponse permet de voir que le résolveur n'est pas sur le continent américain. Pour un résolveur censé servir essentiellement au public européen, c'est logique.

Curieusement, alors que le cahier des charges de DNS4EU prévoyait explicitement la mise en œuvre de la censure des 27 États membres de l'UE, je n'ai pas trouvé de domaine censuré. Même Sci-Hub marche :

```
% kdig +nsid +tls @2a13:1001::86:54:11:11 sci-hub.se
;; TLS session (TLS1.3)-(ECDHE-SECP256R1)-(ECDSA-SECP256R1-SHA256)-(AES-256-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 14949
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 1400 B; ext-rcode: NOERROR
;; NSID: 646E733465752D7061722D3031 "dns4eu-par-01"
;; PADDING: 392 B

;; QUESTION SECTION:
;; sci-hub.se.           IN A

;; ANSWER SECTION:
sci-hub.se.          60 IN A 186.2.163.219

;; Received 468 B
;; Time 2025-06-04 20:44:22 CEST
;; From 2a13:1001::86:54:11:11@853(TLS) in 58.3 ms
```

Sinon, je l'ai dit, avoir juste un autre résolveur DNS public n'est pas super intéressant. Parmi ceux qui existent en Europe :

— DNS4ALL <https://www.bortzmeyer.org/resolveur-dns-sidn.html>.
— dns.sb <https://www.bortzmeyer.org/dns-sb.html>.
— FDN <https://www.bortzmeyer.org/fdn-dot-doh.html>.

Et il existe d'autres résolveurs européens, sans compter ceux de Wikipédia <https://www.bortzmeyer.org/wikidough.html>.