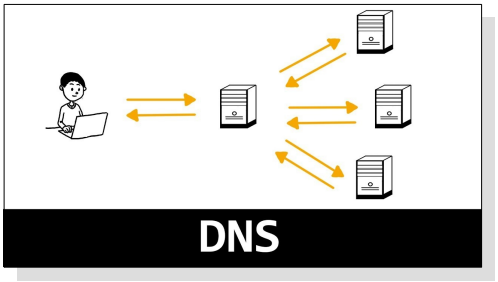
NOM DE DOMAINE (DNS)



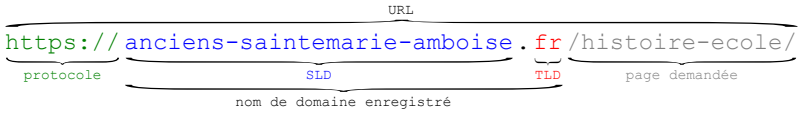
(≈ 5 min)

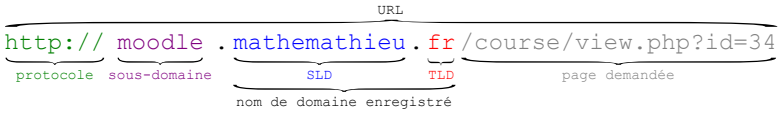
https://youtu.be/qzWdzAvfBoo?t=44

Les équipements reliés à Internet sont identifiés par des adresses IP.
Un nom de domaine, via le **système DNS** (*Domain Name System*), permet d'associer à cette adresse une appellation facilement mémorisable par un humain et, par conséquent, de faciliter l'accès à un site web hébergé sur un serveur à cette adresse. Outre le fait qu'il est plus facile pour un humain de retenir « www.certa.ssi.gouv.fr » que 213.56.176.2, ceci permet au gestionnaire du site de modifier son adresse IP (changement de fournisseur d'accès, par exemple) en ayant juste à mettre à jour le serveur DNS plutôt que d'avoir à informer tous les clients potentiels de la nouvelle adresse IP.

Par exemple, `https://mathemathieu.fr` est ce qu'on appelle une **URL** (*Uniform Resource Locator*, littéralement « localisateur uniforme de ressource ») et l'adresse IPv4 associée (au 11 nov. 2025) est `193.203.239.49`. Le **nom de domaine enregistré** (que l'on a loué auprès d'un registre) est `mathemathieu.fr`.

Le nom de domaine consiste en séquence hiérarchique de noms séparés par des points.
Pour mieux comprendre, voici deux URL :





TLD

Le domaine de premier niveau, appelé **TLD** (*top-level domain*) ou parfois « extension », est le suffixe à la fin du nom de domaine : c'est le `fr` dans `mathemathieu.fr`.

Au 11 novembre 2025, il y avait 1 592 TLD :

- 1 247 *generic top-level Domain* (**gTLD**), utilisables par tous : `org`[1], `net`[2], `com`[3], `info`[4], etc.
- 317 *country code top-level Domain* (**ccTLD**) : `be` pour la Belgique, `ca` pour le Canada, `ch` pour la Suisse, `eu` pour l'Union européenne, `fr` pour la France, `us` pour les États-Unis, etc.
  Les ccTLD sont souvent soumis à certaines conditions : pour le `fr`, il faut résider dans un pays de l'Union européenne ou de l'AELE (Islande, Liechtenstein, Norvège, Suisse) pour pouvoir enregistrer ou renouveler un domaine, la nationalité française seule n'étant plus suffisante depuis 2011 ; il suffit de pouvoir justifier d'une résidence, même secondaire, dans l'un de ces territoires, par exemple via une facture ou un bail.
- 3 *generic-restricted top-level Domain* (**grTLD**), : `biz`[5], `pro`[6] et `name`[7].
  L'idée est d'imposer quelques conditions d'usage ou d'éligibilité plutôt qu'un usage totalement libre. Mais dans la pratique ces conditions ont souvent été assouplies, voire abandonnées.
- 14 *sponsored top-level Domain* (**sTLD**) : `aero`[8], `asia`, `cat`[9], `coop`[10], `edu`[11], `gov`[12], `int`[13], `jobs`, `mil`[14], `museum`, `post`[15], `tel`, `travel`[16] et `xxx`[17].
  Ce sont des domaines spécialisés dotés d'un sponsor représentant une communauté spécifique (ethnique, géographique, professionnelle, technique ou autre). Ils sont proposés par des agences ou organisations privées

1 Abréviation de *organisation*. Destiné aux organisations à but non commercial, mais ouvert à tous sans restrictions depuis août 2019. Traditionnellement utilisé par les écoles, les projets open source (ouverts), et les communautés, et maintenant par des entités à but lucratif.

2 Abréviation de *network* (« réseau » en français). Il s'appliquait à l'origine aux organisations présentant un lien avec les technologies réseau, comme les fournisseurs de services Internet et autres sociétés d'infrastructures réseau. Le domaine n'a jamais fait l'objet d'aucune restriction et représente aujourd'hui un espace de noms généraliste : il reste apprécié des opérateurs réseau.

3 Abréviation de *commercial*. Il s'appliquait à l'origine aux domaines enregistrés par des entités commerciales : cette distinction a disparu.

4 Abréviation de *information*. Créé en 2001, ce domaine est ouvert à tous sans restriction mais est plutôt destiné aux sites web qui veulent informer leurs utilisateurs plutôt que de vendre quelque chose ou être simplement une vitrine.

5 Abréviation de *business*. Créé en 2001, notamment pour offrir une alternative aux entreprises dont le nom de domaine dans `com` avait déjà été enregistré par quelqu'un d'autre. Lors de l'enregistrement, il est imposé que l'usage du domaine soit « solidement lié à une activité commerciale ou d'échange de biens/services ».

6 Abréviation de *professional*. Créé en 2004, à l'origine limité aux professionnels certifiés (avocats, médecins, ingénieurs, etc.) disposant d'une licence ou d'une accréditation. Au fil du temps, les restrictions ont été assouplies : depuis novembre 2015, quasiment tout le monde peut enregistrer un `.pro`, l'idée étant de signaler une présence « professionnelle » crédible en ligne.

7 Créé en 2001 pour offrir aux particuliers un espace de nom personnel, par exemple `johanmathieu.name`. Cela permet aux individus d'enregistrer un nom de domaine reflétant leur identité ou pseudonyme, plus « personnel » que les extensions commerciales classiques.

8 Domaines réservés à la communauté de l'aviation et de l'aéro-spatial (compagnies aériennes, aéroports, fournisseurs, etc.). Une « Aero-ID » d'identification est requise.

9 Pour la communauté linguistique et culturelle catalane (langue catalane). Le site doit avoir un contenu significatif en catalan.

10 Réservée aux coopératives ou organisations de type coopératif. Pour y être éligible, l'enregistrement doit respecter certaines conditions comme « être une coopérative démocratiquement gouvernée et détenue par ses membres, conforme aux sept principes coopératifs reconnus internationalement » ou « être une entité dont l'activité principale est de servir ou promouvoir les coopératives ».

11 Il a été mis en œuvre pour pour les organisations axées sur l'éducation, et il était ouvert à l'enregistrement pour les entités de n'importe quelle région. Depuis 2001, les nouveaux titulaires doivent être des établissements d'enseignement supérieur accrédités par les États-Unis.

12 Réservé aux organismes gouvernementaux américains (fédéraux/étatiques/locaux).

13 Réservé aux organisations intergouvernementales établies par traité international. Plusieurs critères sont requis, comme « fournir un traité international entre gouvernements nationaux (ou plus) qui établit l'organisation », ce traité devant « être publié ou accessible ».

14 Réservé aux forces armées américaines et organismes associés.

15 Pour les services postaux/logistiques : conditions d'usage liées à la livraison de biens/services, marques.

16 Réservé initialement aux acteurs de l'industrie du voyage. Requiert une déclaration de lien à l'activité voyage / tourisme.

17 Créé en 2011 pour la communauté de divertissement pour adultes (contenus sexuels destinés à un public adulte consentant), avec la possibilité de louer un nom de domaine à titre préventif (cela permet à un non membre de la communauté adulte de réserver un nom sous `.xxx` pour bloquer l'usage par des tiers sans pour autant activer un site). Depuis novembre 2024, c'est un TLD ouvert à tous !

qui établissent et appliquent des règles.

- 11 *testing top-level Domain* : إختبار (« test » en arabe), テスト (« test » en japonais), etc.
  Ils sont en phase de test, non disponibles pour l'instant.

La liste complète des TLD est consultable sur : https://www.iana.org/domains/root/db.

Les TLD sont administrés par l'**ICANN** (*Internet Corporation for Assigned Names and Numbers*), une organisation à but non lucratif chargée de coordonner le système mondial des noms de domaine et des adresses IP. Chaque TLD est délégué à un registre qui en assure la gestion opérationnelle.
En France, c'est l'association **Afnic** (*Association Française pour le Nommage Internet en Coopération*) qui a pour mission de gérer les TLD de la France (`.fr`), La Réunion (`.re`), des Terres australes et antarctiques françaises (TAAF) (`.tf`), Mayotte (`.yt`), Saint-Pierre-et-Miquelon (`.pm`) et Wallis-et-Futuna (`.wf`).
Elle est aussi le partenaire technique de nouveaux gTLD comme `.paris`, `.bzh` ou `.alsace`.

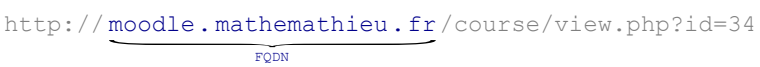
SLD et sous-domaines

Le domaine de deuxième niveau, appelé **SLD** (*second level domain*), est le libellé qui apparaît juste avant le TLD.

Viennent ensuite les autres niveaux (troisième, quatrième, etc.) que l'on qualifie souvent de **sous-domaines**.

FQDN

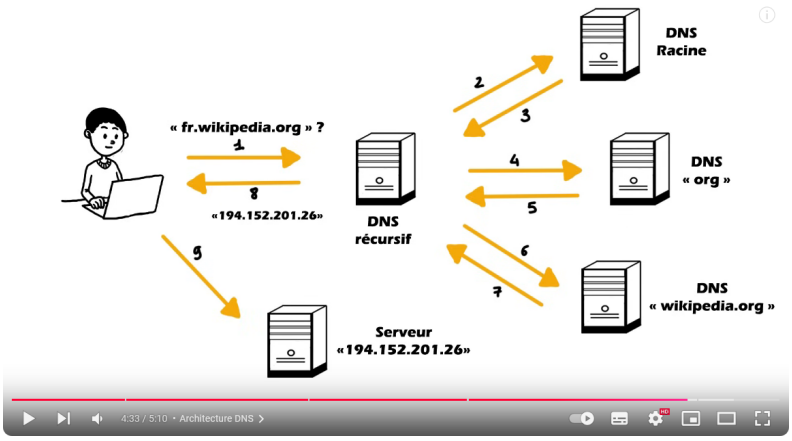
Dans une URL, le regroupement du sous-domaine, du SLD et du TLD forment[18] ce qu'on appelle un **FQDN** (*Fully Qualified Domain Name*). On parle aussi parfois de « domaine absolu ». Par exemple :



Chaque étiquette d'un FQDN, c'est-à-dire la partie entre deux points, doit contenir **au maximum 63 caractères**, et le FQDN ne doit pas dépasser 253 caractères en représentation textuelle.

18 En réalité, le FQDN contient un point final à la fin, par exemple « `moodle.mathemathieu.fr.` ». Mais cela n'est pas important pour l'instant.

La résolution DNS



La résolution DNS est le processus permettant de trouver l'adresse IP d'un FQDN.
Voici comment cela se déroule étape par étape, avec l'exemple de `fr.wikipedia.org` :

→ Étape 0 : **fichier hosts**

Votre navigateur analyse d'abord si l'adresse se trouve dans un fichier nommé « hosts » : c'est un fichier texte (pour Windows, situé dans le répertoire *C:\Windows\System32\Drivers\etc*) qui contient d'un côté les noms de domaine et de l'autre les adresses IP correspondantes.
Si aucune entrée n'est trouvée, on passe à l'étape suivante.

→ Étape 1 : la demande au **serveur DNS récursif**

Le navigateur interroge un serveur DNS récursif : il joue le rôle d'intermédiaire et lance une série de requêtes pour trouver l'adresse IP demandée.

→ Étape 2 : la navigation dans la hiérarchie DNS

Si le serveur DNS récursif ne connaît pas directement l'adresse IP, il va remonter dans la hiérarchie pour obtenir les informations nécessaires :

1. Le **serveur DNS racine** est interrogé pour connaître les serveurs responsables du TLD concerné (dans ce cas, `.org`).
2. Le **serveur DNS TLD** `.org` indique les serveurs DNS responsables du domaine `wikipedia.org`.
3. Le serveur `wikipedia.org` fournit enfin l'adresse IP exacte du sous-domaine demandé.

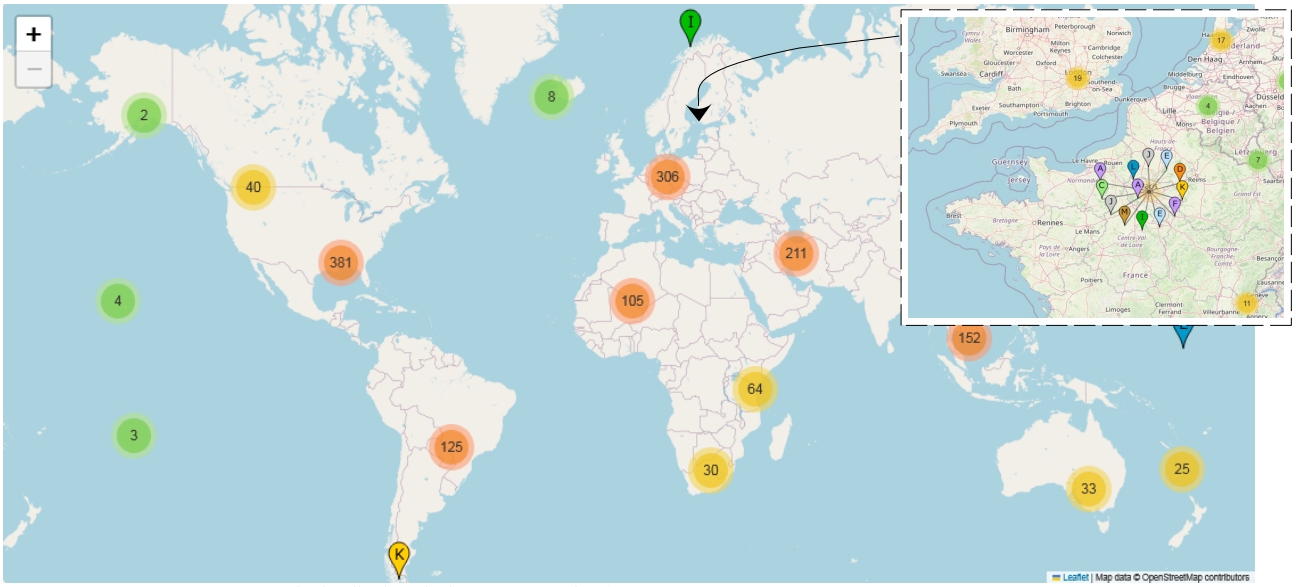
→ Étape 3 : la **réponse au navigateur**

Une fois que le serveur DNS récursif obtient l'adresse IP finale, il la transmet au navigateur. Celui-ci utilise alors cette adresse IP pour se connecter au serveur correspondant et afficher la page web demandée.

Serveur(s) DNS racine

Fin 2016, sous pression internationale (de l'UE, de nombreux pays d'Asie et d'Amérique du Sud), les États-Unis ont renoncé à des décennies de gérance du DNS racine via l'organisme ICANN[19] qui était rattaché au *Département du Commerce* de l'administration américaine. La gérance, toujours via l'ICANN, est désormais placée sous un modèle de gouvernance multi-parties, sans supervision exclusive américaine.

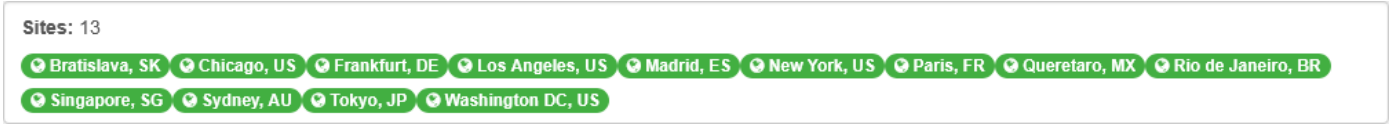
On entend souvent parler de « la » racine (ou *server root*), mais il y en a plusieurs.
On lit aussi souvent qu'il en existe 13… Il y a bien 13 « root name servers » mais il s'agit en réalité de 13 « identités de serveur » (serveurs A, B, C, … , M) ayant chacun une adresse IP[20] ; les serveurs racines sont donc un réseau de milliers de serveurs dans de nombreux pays à travers le monde – 1 952 serveurs[21] au 11 novembre 2025, répartis sur 1 558 sites – et chacun est une copie du véritable serveur maître à partir duquel les copies sont effectuées, ce dernier n'étant pas l'un des serveurs racines publics.



Source : root-servers.org (en zoomant, les localisations des instances se précisent)

Douze organisations contrôlent ces serveurs, deux sont européennes, une japonaise, les autres étant américaines. Ces serveurs ne sont pas de simples machines mais correspondent à plusieurs installations réparties dans des lieux géographiques divers.

Par exemple, la racine « C » est contrôlée par *Cogent Communications* (opérateur de télécommunications multinational américain) et elle est constituée de 13 serveurs situés sur 13 sites :



Source : root-servers.org

19 *Internet Corporation for Assigned Names and Numbers*.
20 La liste de ces 13 adresses IP et leurs opérateurs est disponible ici : https://www.iana.org/domains/root/servers.
21 Il y avait 130 sites en 2007. Pour voir la liste actualisée de ces sites : https://root-servers.org/.

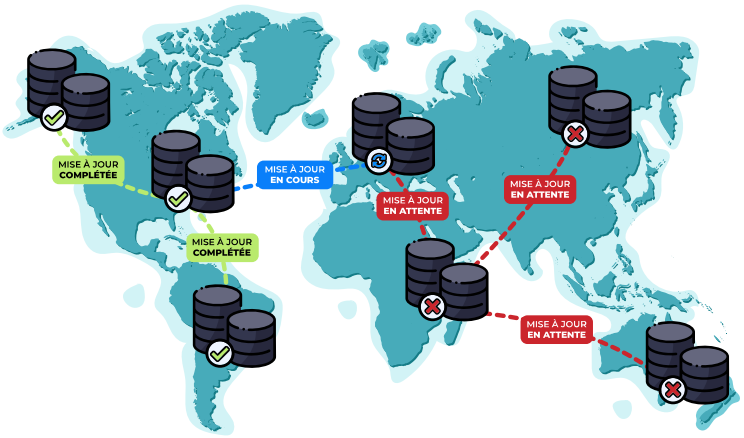
Si l'un des *root servers* ne répond plus, la charge est répartie entre les serveurs qui subsistent. Si aucun d'entre eux ne pouvait répondre aux requêtes, les noms de domaines deviendraient progressivement inaccessibles, au fur et à mesure que les informations dans les caches parviendraient à expiration. L'adresse exacte de la plupart des serveurs n'est pas publiée pour éviter les attaques ciblées.

Compléments

Pour plus de détails sur les serveurs racines (ainsi que le protocole DNSSEC), voir « Internet est-il réellement contrôlé par 14 personnes qui détiennent 7 clés secrètes ? » : mathemathieu.fr/1565.

La propagation DNS

La propagation DNS désigne le processus par lequel les modifications des enregistrements DNS se répercutent sur l'ensemble des réseaux mondiaux. Ce processus n'est pas instantané : le délai de mise à jour peut varier **de quelques secondes à plusieurs heures**, selon votre localisation et la configuration des appareils connectés à Internet, mais aussi de la manière dont certains services DNS mettent en cache ces informations.



De plus, un résolveur DNS garde en mémoire (« **mise en cache** ») les résultats ; si on cherche deux fois le même nom de domaine, le résolveur de mon FAI[22] répondra très vite la seconde fois, car il garde en mémoire le résultat. La durée de cette mémoire dépend du **TTL** (*Time To Live*), qui peut être différent pour chaque nom de domaine. Cela se configure.

Exemple : →

A	Nom	Cliquez pour configurer	6 heure(s)
Type	**Nom**	**Valeur**	**TTL**
MX	@	10 mail.mathemathieu.fr.	24 heure(s)
A	@	185.98.131.144	6 heure(s)
A	mail	91.216.107.217	6 heure(s)
CNAME	ftp	@	24 heure(s)
CNAME	imap	mail.mathemathieu.fr.	24 heure(s)
CNAME	pop	mail.mathemathieu.fr.	24 heure(s)
CNAME	smtp	mail.mathemathieu.fr.	24 heure(s)
CNAME	www	@	24 heure(s)
TXT	@	v=spf1 mx:mathemathieu.fr a:mail.mathemathieu.fr a:mailphp.lws-hosting.co…	24 heure(s)

Mais il vaut mieux éviter de mettre un TTL trop bas pour ne pas finir sur une liste de *spam*[23].
Sans compter que s'il y a une panne (liée à une attaque ou pas), toute l'infrastructure est HS après TTL minutes, tandis que s'il y a une mémoire cache plus conséquente, une partie des utilisateurs ne sera pas impactée.

Voilà pourquoi, lorsqu'on change d'hébergeur (du nom de domaine), cela peut mettre jusqu'à 2 jours, le temps que les caches soient actualisés.

22 Fournisseur d'Accès à Internet.

23 Courriel indésirable (*pourriel* en français).

Bloquer un site

L'État français dispose de plusieurs moyens techniques pour bloquer l'accès à des sites interdits. Ces dispositifs restent contournables, mais **ils compliquent la tâche** des administrateurs des sites visés.

Au début de l'année 2015, cinq sites faisant l'apologie du terrorisme ont ainsi été « bloqués », en application de la nouvelle loi antiterroriste adoptée par le Parlement en novembre 2014. Celle-ci permet au ministère de l'Intérieur d'**ordonner un blocage sans autorisation préalable d'un juge**. Les internautes tentant d'accéder à ces sites sont redirigés vers une page officielle du ministère, qui affiche en rouge le message suivant : « *Vous avez été redirigé vers ce site officiel car votre ordinateur allait se connecter à une page dont le contenu provoque à des actes de terrorisme ou fait publiquement l'apologie d'actes de terrorisme.* »

Ce type de dispositif repose sur ce qu'on appelle un **DNS menteur** : il s'agit de manipuler les réponses DNS pour rediriger les requêtes de l'internaute vers une adresse IP différente de celle du site d'origine, en l'occurrence vers une page d'avertissement contrôlée par les autorités.
L'usage de DNS menteurs est généralement mis en œuvre par les FAI en réponse à des obligations légales ou administratives. En revanche, ces obligations s'appliquent beaucoup plus rarement aux **DNS alternatifs**, qui échappent PARFOIS au contrôle direct de l'État.
Ainsi, dans un tel contexte, l'utilisation de serveurs DNS alternatifs est souvent recommandée pour préserver un certain degré de liberté sur Internet.

DNS récursif : un choix flexible

Les serveurs DNS récursifs sont souvent fournis par votre FAI et offrent généralement une bonne rapidité et des protections de base contre certaines attaques. Cependant, ils peuvent varier en qualité selon l'opérateur, notamment en termes de performance ou de respect de la vie privée.
Ils peuvent aussi être en panne, comme cela est arrivé le mardi 22 octobre 2019 pour les abonnés Free[24].

Pour ces raisons, certains utilisateurs préfèrent des alternatives comme Quad9, Google Public DNS, OpenDNS, FDN ou Cloudflare. Ces DNS publics sont souvent plus transparents concernant la collecte et l'utilisation des données.
Cependant, il faut bien rappeler que **le serveur DNS récursif que vous utilisez verra toutes vos requêtes DNS** (tous les domaines que vous visitez). Lui faites-vous confiance ? Mieux vaut donc réfléchir un peu à qui nous donnons nos informations.
De plus, depuis 2024 certaines alternatives comme Google DNS, Cloudflare ou OpenDNS ont été attaquées en justice[25] par Canal+ : ils ont combattu mais ont été condamnées par un juge français à devenir des DNS menteurs afin de bloquer plus d'une centaine de sites de streaming diffusant sans autorisation le Top 14 de rugby, la Champions League et la Premier League de football.

Si vous souhaitez changer vos DNS, ce n'est pas compliqué, tout est expliqué ici : changetondns.fr
Et pour une liste de DNS alternatives, mise à jour avec quelques commentaires :
sebsauvage.net/wiki/doku.php?id=dns-alternatifs

24 Source : https://actu.fr/economie/free-mobile-victime-dune-panne-geante-dans-toute-france_16543280.html
25 Source : https://next.ink/159484/streaming-sportif-la-justice-ordonne-le-blocage-par-les-dns-de-google-cloudflare-et-cisco