

INTERNET E04 : LE DNS

Cette activité est très largement inspirée des pages 14 et 15 du manuel Sciences numériques & technologie 2nd, Hachette éducation

EXERCICE N°1 Adresse IP, adresse symbolique et serveur DNS

Pour cet exercice deux aides sont disponibles :

Aide n°1 : <https://www.youtube.com/watch?v=qzWdzAvfBoo>

Aide n°2 : [voir l'annexe](#)

1) Que signifie DNS ?

DNS signifie Domain Name System, on peut traduire par « système de noms de domaine »

2) Quel est l'intérêt des adresses symboliques ?

Elles sont plus faciles à retenir pour un humain. De plus même si l'adresse IP d'un site est modifiée, on peut continuer à y accéder avec la même adresse symbolique (à condition que la mise à jour du serveur DNS soit faite).

3) Quelles sont les différences entre les adresses suivantes : www.wwf.fr , www.wwf.org , www.wwf.be , www.culture.gouv et www.hachette.com ?

www.wwf.fr est un site français

www.wwf.org est le site d'une association

www.wwf.be est un site belge

www.culture.gouv est un site gouvernemental

www.hachette.com est un site commercial

Remarque : pour www.wwf.fr le serveur est aux États-Unis

4) À quoi sert un serveur DNS ?

Il sert à traduire les noms de domaine en adresse IP.

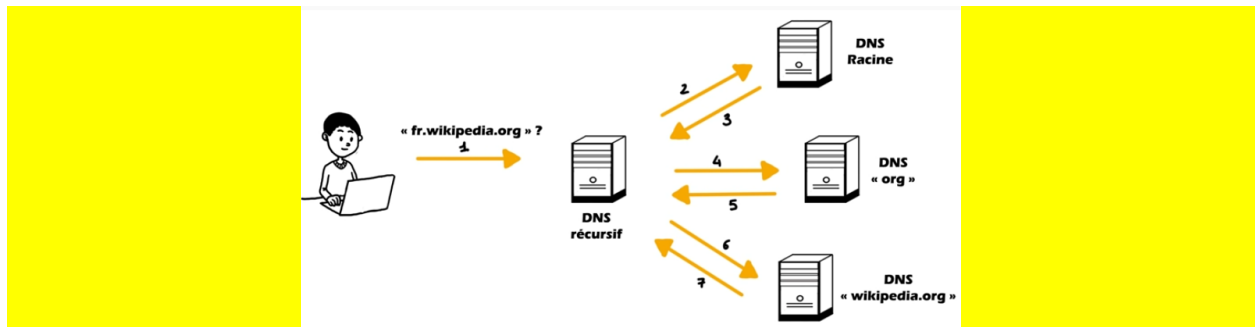
EXERCICE N°2 Fonctionnement d'un serveur DNS

Pour cet exercice deux aides sont disponibles :

Aide n°1 : <https://www.youtube.com/watch?v=qzWdzAvfBoo>

Aide n°3 : [voir l'annexe](#)

1) Détailler les différentes étapes pour que s'affiche sur l'écran de votre ordinateur la page d'un site demandé.



2) Trouver l'adresse IP du site hachette.com.

23.97.191.74

3) Trouver l'adresse IP du site landatome.pagesperso-orange.fr

193.252.121.242

EXERCICE N°3 Contourner les serveurs DNS

Pour cet exercice une aide est disponible ainsi qu'un document :

Aide n°4 : [voir l'annexe](#)

Document : [voir l'annexe](#)

1) À quel serveur correspondent les adresses IP 8.8.8.8 et 8.8.4.4 ?

Elles correspondent au serveur DNS de google.

<https://korben.info/dns-google.html>

2) Après avoir lu le document en annexe, expliquer comment il est possible de censurer un site en contrôlant les serveurs DNS.

Le blocage par nom de domaine (DNS) consiste à rendre inopérant le système de noms utilisé pour localiser des ordinateurs et des services en ligne.

Il suffit donc de changer l'adresse IP associée au nom de domaine afin de rediriger la requête vers un autre site.

3) Selon vous, quelle peut donc être l'utilité du serveur de la question 1 ?

Il a le mérite de fournir une alternative au DNS de notre Fournisseur d'Accès Internet qui est bien souvent installé par défaut.

4) Existe-t-il d'autres procédures pour bloquer un site ?

On peut « neutraliser » l'adresse IP mais c'est peu efficace ou couper le serveur hébergeant le site à bloquer (le site doit alors changer de serveur...)

5) Trouver d'autres raisons qui pourraient inciter un État à demander aux FAI de bloquer certains sites à partir de leurs serveurs DNS.

Les raisons autres que le terrorisme pourraient évidemment être : la vente d'arme, la pédopornographie, la vente de drogue ou autres activités illicites

6) À votre avis, quelles sont les dérives possibles?

Un régime totalitaire pourrait limiter l'accès à l'information de ses citoyens...

Une grande entreprise pourraient favoriser ses produits...

ANNEXE

Document

Décret n° 2011-2122 du 30 décembre 2011 relatif aux modalités d'arrêt de L'accès à une activité d'offre de paris ou de jeux d'argent et de hasard en ligne non autorisée NOR: BCRBI1209500

Publics concernés: fournisseurs d'accès à internet; opérateurs de jeux d'argent ou de hasard en ligne non autorisés.

Objet: modalité de blocage des sites de jeux illégaux.

Entrée en vigueur: le texte entre en vigueur le lendemain de sa publication.

Notice: lorsque l'arrêt de l'accès à une offre de paris ou de jeux d'argent et de hasard en ligne a été ordonné par le président du tribunal de grande instance de Paris, les fournisseurs d'accès à internet et les hébergeurs de sites doivent procéder à cet arrêt. Le présent décret explicite les modalités du blocage que doivent mettre en œuvre ces personnes ainsi que la compensation des surcoûts engendrés par cette procédure.

Le blocage par nom de domaine (DNS) consiste à rendre inopérant le système de noms utilisé pour localiser des ordinateurs et des services en ligne.

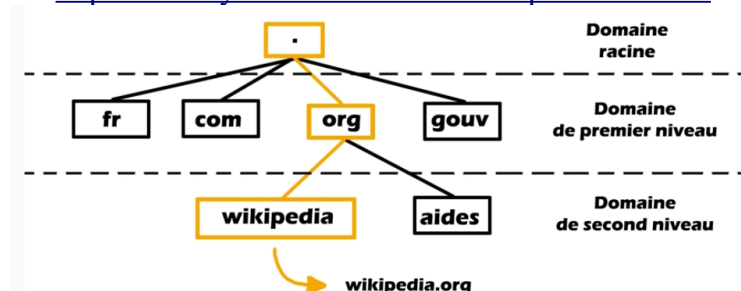
Références: le présent décret est pris pour application de l'article 61 de la loi n°2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne. Il peut être consulté sur le site Légifrance (<http://www.legifrance.gouv.fr>).

Décète:

Art. 1^{er} . - Lorsque l'arrêt de l'accès à une offre de paris ou de jeux d'argent et de hasard en Ligne non autorisée a été ordonné dans Les conditions définies par l'article 61 de la loi du 12 mai 2010 susvisée, les personnes mentionnées au 1 du I de l'article 6 de la loi du 21 juin 2004 susvisée procèdent à cet arrêt en utilisant le protocole de blocage par nom de domaine (DNS).

Aide n°1 : comprendre le DNS en 5 min : vidéo issue de la chaîne youtube cookie connecté

<https://www.youtube.com/watch?v=qzWdzAvfBoo>



Aide n°2 : Anatomie d'une adresse symbolique

wikipedia.org

Nom de domaine

Il est en langage courant, est donc facile à retenir et constitue la conversion de l'adresse IP.

Exemples:

- Wikipédia
- Google
- Paris culture

Extension

C'est une indication de l'organisation qui gère le site. L'extension peut être d'ordre technique ou géographique.

Exemples:

- .org pour les associations
- .gouv pour les organisations gouvernementales
- .com pour les sites commerciaux
- .fr pour les sites français
- .be pour les sites belges

Aide n°3 : Comment trouver l'adresse IP d'un site et inversement ?

Des sites spécialisés permettent de trouver les adresses IP de sites ou les noms de domaine associés à une adresse IP. Une recherche avec les mots-clefs « recherche DNS » donnera plusieurs sites rendant ce service.

Aide n°4 : Comment les autorités peuvent bloquer un site internet ?

Article tiré du site : https://www.sciencesetavenir.fr/high-tech/comment-les-autorites-peuvent-bloquer-un-site-internet_35828

Par [Olivier Hertel](#) le 18.03.2015 à 12h04, mis à jour le 18.03.2015 à 12h04

Comment les autorités peuvent bloquer un site Internet

L'État français dispose de plusieurs techniques pour bloquer des sites interdits. Ces méthodes sont contournables mais contraignantes pour les propriétaires des sites incriminés.

Cinq sites faisant l'apologie du [terrorisme](#) ont été bloqués ces derniers jours. Une opération exceptionnelle prévue par la nouvelle loi antiterroriste votée par le parlement en novembre 2014 et qui désormais ne nécessite plus l'autorisation d'un juge. Les internautes qui tentent de se rendre sur ces sites sont désormais redirigés vers une page contrôlée par le ministère de l'Intérieur. Celle-ci 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."



Une portion de la page qui s'affiche lorsque qu'un internaute tente de se connecter à une page dont l'accès au contenu a été bloqué
©Ministère de l'intérieur

Plusieurs méthodes pour bloquer un site

BLOQUER L'URL. S'il existe plusieurs manières d'entraver l'accès d'un site, le ministère de l'Intérieur a choisi celles consistant à bloquer l'adresse, la fameuse URL ou nom de domaine. *"Sur [Internet](#), il existe une sorte d'annuaire des sites, le DNS (Domain Name System) qui fait la conversion de l'URL en adresse IP. L'adresse IP est une suite de chiffres qui indique l'emplacement physique du site, c'est-à-dire le serveur sur lequel il est stocké au sein d'un data center",* explique Gêrôme Billois, expert en cybersécurité chez Solucom.

Concrètement, quand l'internaute tape l'adresse d'un site dans son navigateur – par exemple www.sciencesetavenir.fr – le DNS le redirige vers le serveur qui l'héberge physiquement, à une adresse du type 62.210.93.41. Le blocage mis en place par les autorités intercepte la conversion opérée par le DNS afin de remplacer l'adresse IP du site par une autre, celle de la page d'avertissement contrôlée par le ministère de l'Intérieur. Chaque fournisseur d'accès à Internet (les FAI comme Orange, Free, Bouygues, SFR...) a son propre annuaire de sites, son propre DNS. Ce sont donc les FAI qui effectuent le changement d'adresse IP. Ainsi, tous les internautes français ne pourront plus accéder aux sites censurés.

COUPER LES SERVEURS. Une autre technique de blocage consiste tout simplement à couper les serveurs qui accueillent le site chez son hébergeur. C'est normalement ce qui est prévu dans ce genre de situations. Mais cela n'a visiblement pas été le cas lors de cette opération. Octave Klabar, patron d'OVH l'hébergeur de l'un des sites incriminés (islamic-news.info), a en effet indiqué le 16 mars sur Twitter qu'il n'avait pas reçu de demande du ministère de l'Intérieur. Probablement les autorités ont-elles voulu faire très vite.

Dans certains cas, quand les sites sont hébergés à l'étranger, ces demandes prennent plusieurs mois avant d'être effectives. C'est notamment le cas avec des pays amis comme les Etats-Unis. Mais il existe aussi des hébergeurs, souvent situés dans les pays de l'Est ou en Asie, qui eux ne répondent jamais aux demandes des forces de l'ordre. Dans ce cas, le blocage ne peut se faire qu'auprès des DNS des fournisseurs d'accès.

NEUTRALISER L'ADRESSE IP. Enfin une autre approche vise à bloquer directement l'adresse IP du site "blacklisté". *"Mais cette méthode n'est pas très efficace puisqu'il suffit au propriétaire du site de changer son adresse IP. Il conserve en plus la même URL ce qui permet aux internautes de se connecter sur son site comme avant"*, précise G r me Billois. D'ailleurs, cette m thode comme toutes celles que nous venons de voir peuvent  tre contourn es. *"La meilleure fa on d' chapper   ces blocages est d'utiliser les r seaux d'anonymisation comme TOR, qui h bergent des serveurs sans que l'on sache o  ils se trouvent et comment on y acc de, et ce par le jeu de rebonds entre plusieurs serveurs plac s entre l'internaute et le serveur qui h berge le site"*, explique l'expert en cybercriminalit .

La m thode choisie par le minist re de l'Int rieur n'est donc pas infaillible. Sans passer par TOR, les administrateurs des sites bloqu s pourraient simplement faire ressurgir leurs contenus sur un d'autres sites avec de nouvelles adresses. L'op ration de l'Etat vise donc certainement plus   multiplier les obstacles,   d courager les propagandistes du [dijihad](#) plut t qu'  les museler d finitivement. En effet,   chaque blocage, ils devront repartir de z ro, faire conna tre leurs nouvelles adresses pour que leurs sites puissent de nouveau  tre consult s.