
Activité 6 - Correction

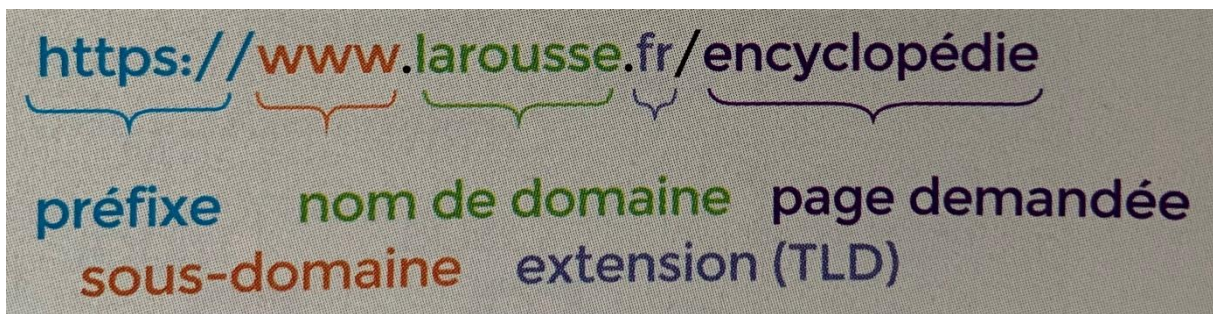
Analyse documentaire

La circulation des données sur Internet

Pour s'adresser à une machine, il faut savoir où elle se trouve sur le réseau Internet et donc son adresse IP. Mais il est impossible de connaître toutes les adresses IP. Un annuaire permet d'accéder à cette information à partir d'une adresse dite « symbolique ».

Document 1 : Nom de domaine

Le **nom de domaine** est une partie de l'adresse URL (**adresse symbolique**) d'un site.



Lorsqu'une entreprise, une association ou même un particulier développe un site Internet, lors de la mise en ligne sur un serveur, il est nécessaire de choisir **un nom** pour ce site : c'est le **nom de domaine**.

Le nom de domaine est la partie d'une **URL** (*Uniform Resource Locator* ou adresse internet), qui renvoie vers le serveur qui héberge ce site.

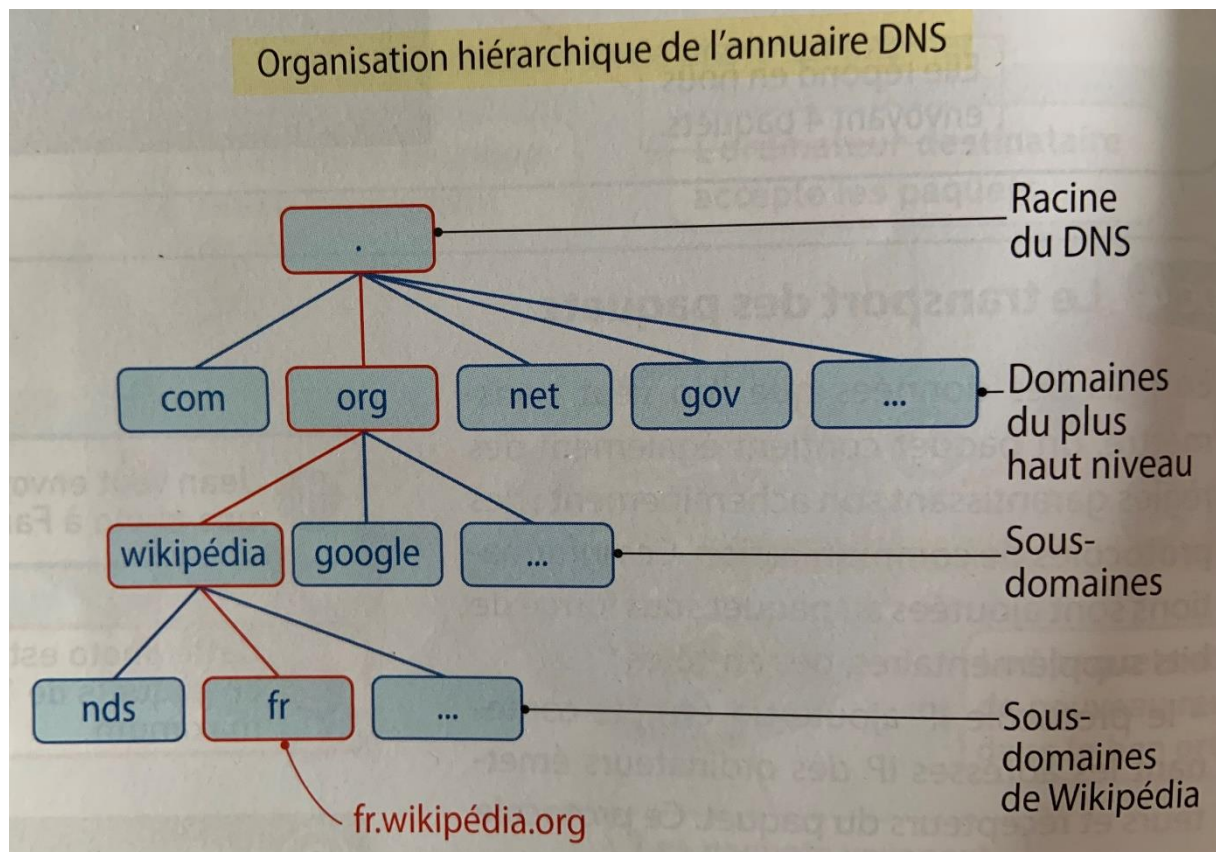
Or les ordinateurs ne connaissent pas le serveur qui héberge le site sous ce nom. En effet, chaque matériel réseau connecté à Internet est accessible via son adresse IP. Il s'agit d'une suite de chiffres, moins simples à mémoriser qu'un nom.

Le rôle du système **DNS** (*Domaine Name Service*) est de fournir l'adresse IP correspondant à l'URL du site recherché par un utilisateur.

Document 2 : L'adresse symbolique, plus facile à retenir

Pour un être humain, l'adresse IP d'une machine est difficile à retenir. On l'associe donc à une adresse symbolique : un texte compréhensible et facile à mémoriser. La correspondance entre adresse IP et adresse symbolique est enregistré dans un annuaire, le *Domaine Name System* (DNS). Il est organisé en domaines et sous domaines, chacun correspondant à des ensembles et sous-ensembles d'adresses gérés en commun. Ainsi dans « wikipedia.org », « wikipedia » est un sous domaine de « .org ».

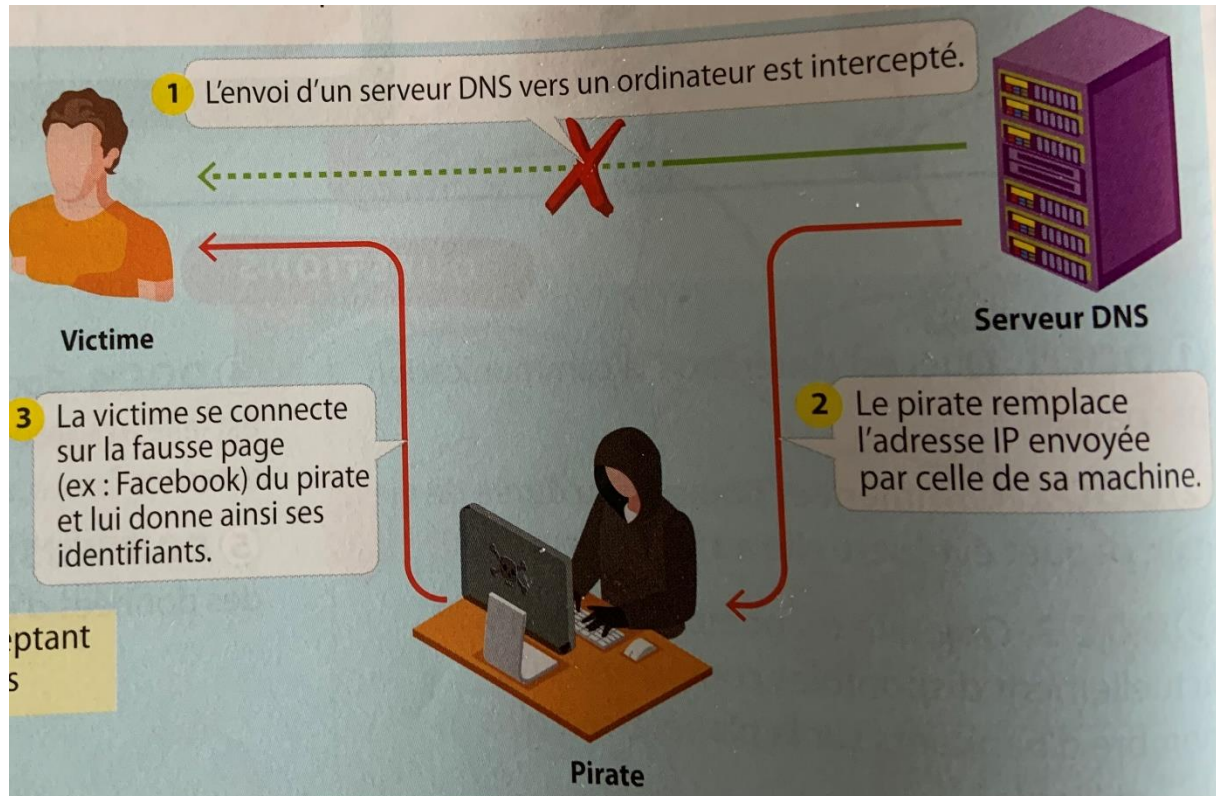
« wikipedia.org » correspond à l'IP d'une machine.



Document 3 : Le piratage du DNS

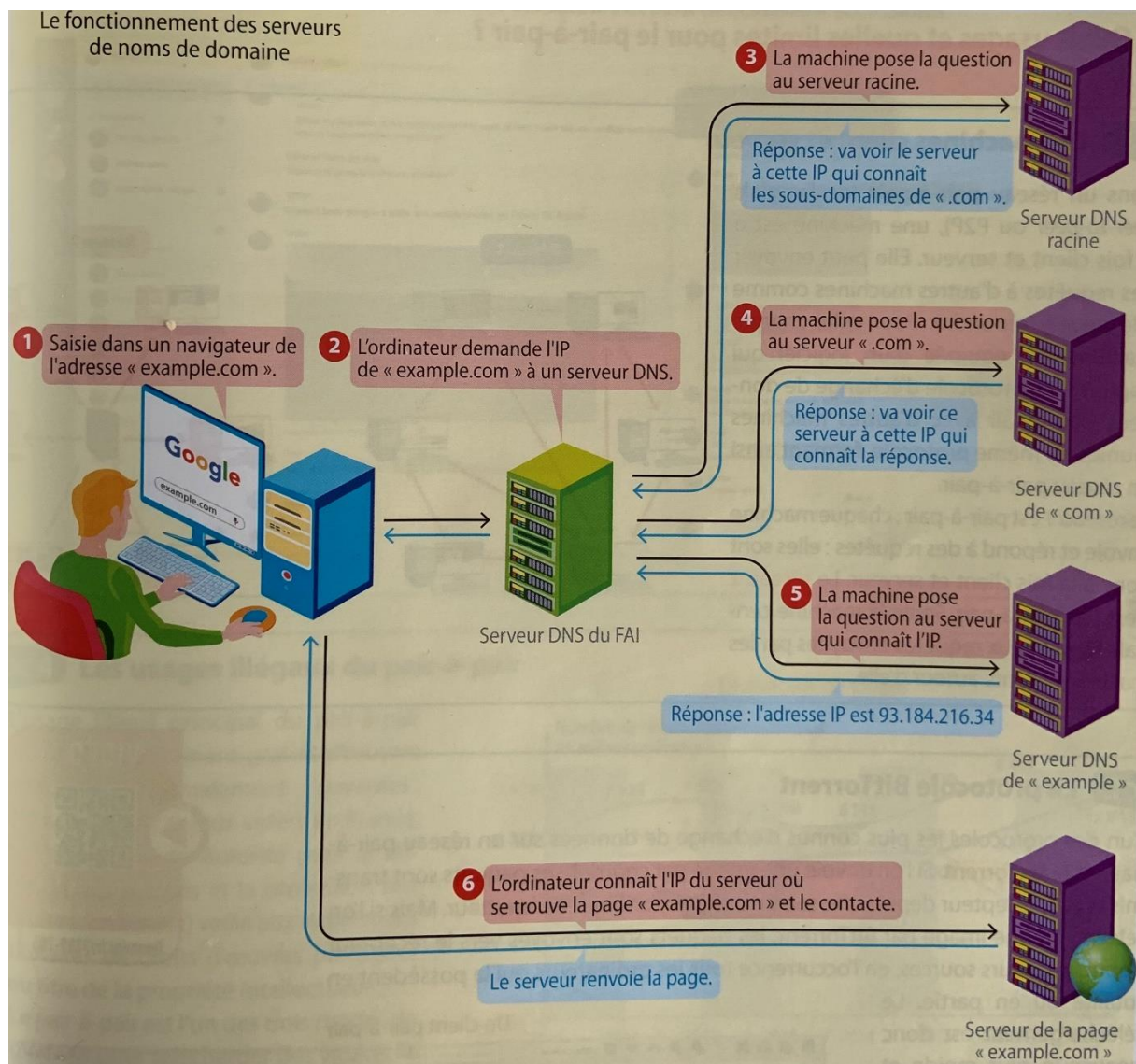
Pour communiquer entre elles, les machines qui permettent d'associer une IP à une adresse symbolique échangent des paquets d'informations. Si un pirate intercepte les paquets où se trouve une adresse IP, il peut remplacer celle-ci par l'IP de son ordinateur, ce qui lui permettra, par exemple, de récolter des données personnelles.

Un pirate interceptant des paquets



Document 4 : Trouver une IP dans l'annuaire DNS

Lorsque vous tapez une adresse dans votre navigateur web, comme « exemple.com », une requête est envoyée à un serveur de nom de domaine (DNS) qui détermine l'adresse IP de la machine hébergeant cette page sur le réseau. Étant donné le grand nombre d'adresses sur le réseau, un serveur donné ne peut connaître qu'une partie de l'annuaire. Pour retrouver une adresse IP, il va communiquer avec d'autres machines qui connaissent d'autres parties de l'annuaire.



Questions

1. Doc 1 : donner le nom de domaine et le TLD du site dont l'URL est <https://www.chateauversailles.fr>
2. Doc 2 : A quel domaine appartient l'adresse : www.education.gouv.fr ? Comment connaître l'adresse IP correspondante ?
3. Doc 3 et 4 : A quelle étape du document 4 un pirate peut-il intercepter des paquets ?
4. Doc 4 : Pourquoi peut-on dire qu'il faut une collaboration des serveurs de nom de domaine pour retrouver une adresse IP ?
5. Conclusion : Indiquez les principales étapes qui vous permettent de consulter www.education.gouv.fr lorsque vous saisissez son adresse symbolique dans votre navigateur.

Corrections

1. Dans l'URL <https://www.chateauversailles.fr>, voici les éléments demandés :

- **Nom de domaine : chateauversailles**
- **TLD (Top-Level Domain) : .fr**

2. L'adresse www.education.gouv.fr appartient au domaine suivant :

- **Nom de domaine : education.gouv**
- **TLD (Top-Level Domain) : .fr**

Comment connaître l'adresse IP correspondante ?

Utiliser la commande ping :

ping www.education.gouv.fr

Cette méthode vous permettra de connaître l'adresse IP actuelle liée au nom de domaine demandé.

3. Le pirate peut intercepter la requête de demande d'adresse IP qui est faite au serveur DNS du Fournisseur d'accès à Internet. Le pirate renvoie une fausse adresse IP à la victime. L'ordinateur de la victime interroge alors le serveur du pirate pensant accéder à un serveur légitime.

4. Il est nécessaire d'avoir une **collaboration des serveurs de nom de domaine (DNS)** pour retrouver une adresse IP, car le système DNS est **hiérarchique** et décentralisé.

Le **DNS** est un système distribué qui permet de traduire les noms de domaine lisibles par l'homme (comme www.example.com) en adresses IP numériques (comme 192.0.2.1) que les machines utilisent pour se connecter sur Internet.

Hiérarchie des serveurs DNS

Le processus de résolution d'un nom de domaine en adresse IP se fait à travers plusieurs **niveaux de serveurs DNS**, chacun ayant une responsabilité particulière :

- **Serveurs racines (Root DNS servers)** : Ce sont les serveurs situés au sommet de la hiérarchie. Ils ne savent pas directement quelle est l'adresse IP d'un domaine spécifique, mais ils savent à quels serveurs de noms (appelés serveurs de domaine de premier niveau, ou TLD) transférer la requête.
- **Serveurs de TLD (Top-Level Domain)** : Ces serveurs gèrent les domaines de premier niveau, comme .com, .fr, ou .org. Par exemple, si vous cherchez www.example.com, les serveurs de TLD .com seront interrogés.
- **Serveurs DNS de niveau 2, 3 ...** : Ces serveurs contiennent les enregistrements DNS spécifiques pour un domaine particulier.

5.

- Interrogation du serveur DNS du FAI
- Interrogation du serveur DNS racine (.)
- Le serveur racine ne connaît pas directement l'adresse IP de www.education.gouv.fr, mais il sait quel serveur est responsable des domaines de premier niveau (TLD), comme .fr.
- Interrogation du serveur DNS de TLD .fr
- Le serveur DNS envoie alors une requête aux serveurs TLD pour .fr pour obtenir des informations sur le domaine [gouv.fr](http://www.education.gouv.fr).
- Le serveur DNS de domaine [gouv.fr](http://www.education.gouv.fr) renvoie l'adresse IP associée à www.education.gouv.fr (par exemple, **1.2.3.4**).