

## 1. L'URL.

Une URL (Uniform Resource Locator) est l'adresse d'une ressource d'un site Web. Elle indique où se trouve cette ressource dans l'arborescence du site :

**https://fr.wikipedia.org/wiki/Uniform\_Resource\_Locator**

**Protocole** utilisé. Dans ce cas : le **http**.  
Le « s » indique que la page est sécurisée, le dialogue entre le serveur et le client est crypté

**Nom de domaine**

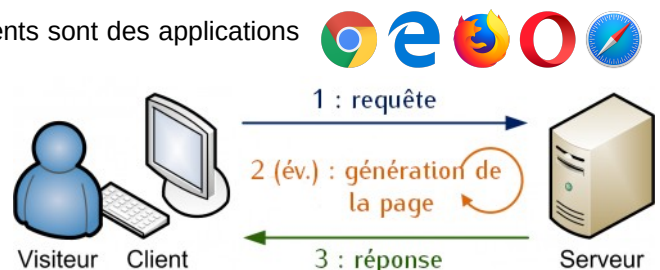
**Chemin vers le fichier.**

Ici le fichier **Uniform\_Resource\_Locator.html** se trouve dans le dossier **/wiki**

## 2. Les échanges clients serveurs - Les requêtes HTTP.

Le Web s'appuie sur un dialogue entre clients et serveurs. Les clients sont des applications qui se connectent au Web, comme les navigateurs.

Ils envoient des requêtes (1) aux serveurs où sont stockées les données. Ces requêtes utilisent le protocole HTTP (HyperText Transfert Protocol), permettant aux clients et au serveur de communiquer entre eux pour afficher une page web.



### Exemple de requête

```
GET /HTTP/1.1
Host: www.lyc-7mares-maurepas.ac-versailles.fr
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.lyc-7mares-maurepas.ac-versailles.fr/
```

Version du protocole

Nom de domaine du serveur

Identifiant du navigateur utilisé

Indique que le client va recevoir du HTML

Langage accepté

Adresse de la page visitée précédente sur laquelle un lien a été suivi

Définit quel sera l'encodage du contenu

**Avez-vous repéré le terme « GET » ?** C'est le nom de la méthode qui permet au client de demander au serveur l'accès à une ressource disponible.

Une fois la requête reçue, le serveur renvoie une réponse (3).

### Exemple de réponse du serveur

```
HTTP/1.1 200 OK
Date: Fri, 25 Oct 2019 16:44:59 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.2.17-0.crdp.0
P3P: CP="NOI ADM DEV PSAI COM NAV OUR OTRP STP IND DEM"
ETag: 38f2df76b2d0d56bfe268b7f84a9f8af
Cache-Control: no-cache
Pragma: no-cache
Set-Cookie: c9a1f7677a29c18bee24af0dd03599a1=fr-FR; expires=Sat, 24-Oct-2020 16:44:59 GMT; path=/
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 6127
Connection: close
Content-Type: text/html
```

En-tête de réponse

```
<!DOCTYPE html>
<html dir="ltr" lang="fr-fr">
<head>
<base href="http://www.lyc-7mares-maurepas.ac-versailles.fr/300MLA/index.php/fr/" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<meta name="keywords" content="lycée, lycée, pédagogie, pédagogie, L7M l7m, lycée les 7 mares, lycée sept mares, 7mares maurepas, 7 mares Elancourt, 7 mares elancourt, BTS , BTSNRC, NRC" />
<meta name="description" content="Site officiel du lycée les 7 mares - Maurepas bassin de Saint Quentin en Yvelines - Yvelines" />
<meta name="generator" content="Joomla! - Open Source Content Management" />
<title>Lycée Les Sept Mares - Accueil</title>
```

Contenu HTML qui permet à votre navigateur d'afficher la page web



**Avez-vous repéré HTTP/1.1 ?** C'est la version du protocole HTTP.

**Avez-vous repéré 200 OK ?** Cela indique la réussite d'une requête.

### 3. La sécurité

**Sur internet, les informations transitent par défaut en clair.** Cela veut dire que lorsque vous accédez à un site Internet, les messages échangés entre votre ordinateur et le serveur sont transmis peuvent être interceptés.

Le protocole **HTTPS (HyperText Transfer Protocol Secure)** est la combinaison du HTTP avec une couche de chiffrement.

Ce protocole permet aussi d'authentifier le site web via un certificat numérique.

#### Https assure la sécurité des échanges

Pour assurer la confidentialité des communications entre un ordinateur et un serveur, il est notamment possible d'utiliser le protocole HTTPS qui est donc sécurisé.

Par "**sécurisé**" on entend que **les données sont chiffrées** avant d'être transmises sur le réseau. Seul le possesseur de la clé de déchiffrement sera en mesure de lire les données transmises sur le réseau.

Celui-ci est identifiable :

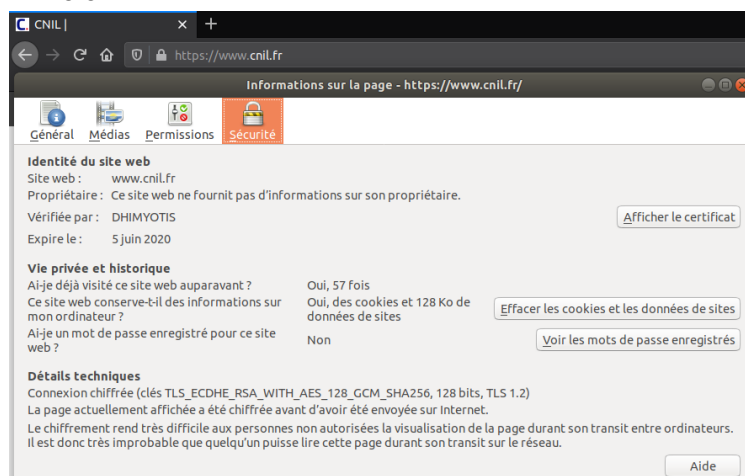
- par la présence d'un "s" après le http ;
- par la présence du symbole du **cadenas fermé**.



Il faut savoir que tous les serveurs ne gèrent pas ce protocole. D'un point de vue strictement pratique **il est nécessaire de bien vérifier que le protocole https est effectivement utilisé** avant de **transmettre des données sensibles (coordonnées bancaires...)**. Si ce n'est pas le cas, passez votre chemin, car toute personne qui interceptera les paquets de données sera en mesure de lire vos données sensibles.

En cliquant sur le **cadenas**, il est possible d'afficher le certificat numérique, d'avoir des informations sur les cookies...

#### Firefox



#### Chrome

