Institut Mines-Télécom

QUI SONT LES NOUVEAUX FOURNISSEURS D'INFORMATIONS PERSONNELLES

PHILIPPE JAILLON
MINES DE SAINT-ETIENNE

IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom
IMT Lille Douai École Mines-Télécom IMT-Université de Lille
MINES Albi-Carmaux — Une école de l'IMT
MINES Alès — Une école de l'IMT
MINES Saint-Étienne — Une école de l'IMT
TELECOM Ecole de Management — Une école de l'IMT
TELECOM ParisTech — Une école de l'IMT
TELECOM SudParis — Une école de l'IMT
EURECOM
MINES ParisTech
MINESnancy
ARMINES

Aujourd'hui, tout le monde est conscient que dès que l'on confie une information à un service web :

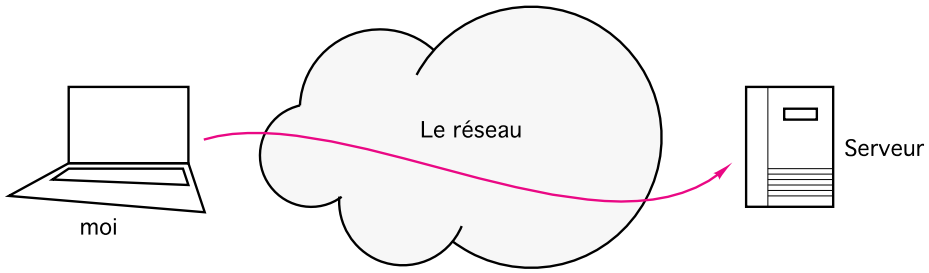
- **Elle nous échappe.**
- **Elle sera « marchandisée » d'une manière ou d'une autre.**

Google, Amazon, Facebook, et tous les services web que nous consultons sont collecteurs et donc potentiellement fournisseurs d'informations personnelles.

- **Mais sont-ils les seuls ?**

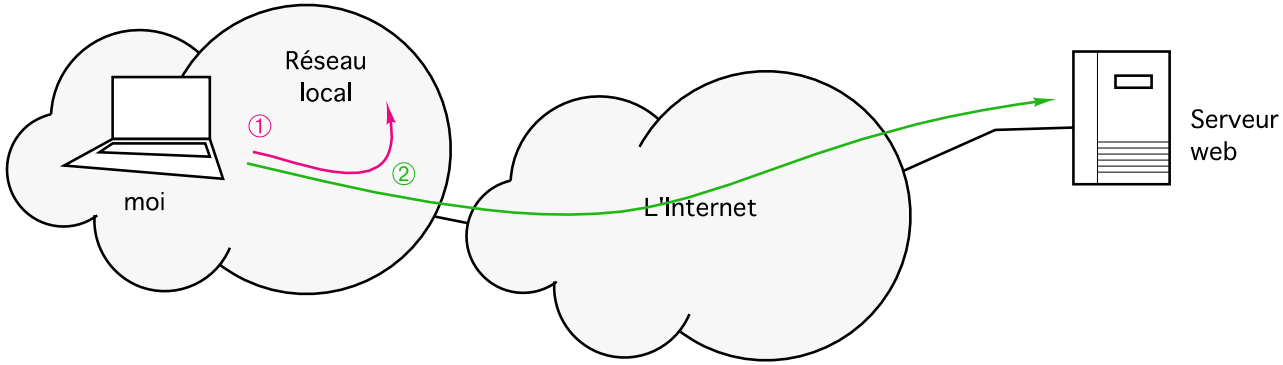
**Aujourd'hui, des protocoles,
de plus en plus enfouis,
manipulent massivement nos données
personnelles.**

Pour utiliser un service sur le réseau, on doit s'adresser à lui.
Dès lors, les informations que nous transmettons nous échappent.



Les communications sont observables tout au long de leur trajet
un routeur n'est qu'un équipement qui regarde où vont les paquets (et plus si nécessaire) ; ils peuvent être copiés, altérés…

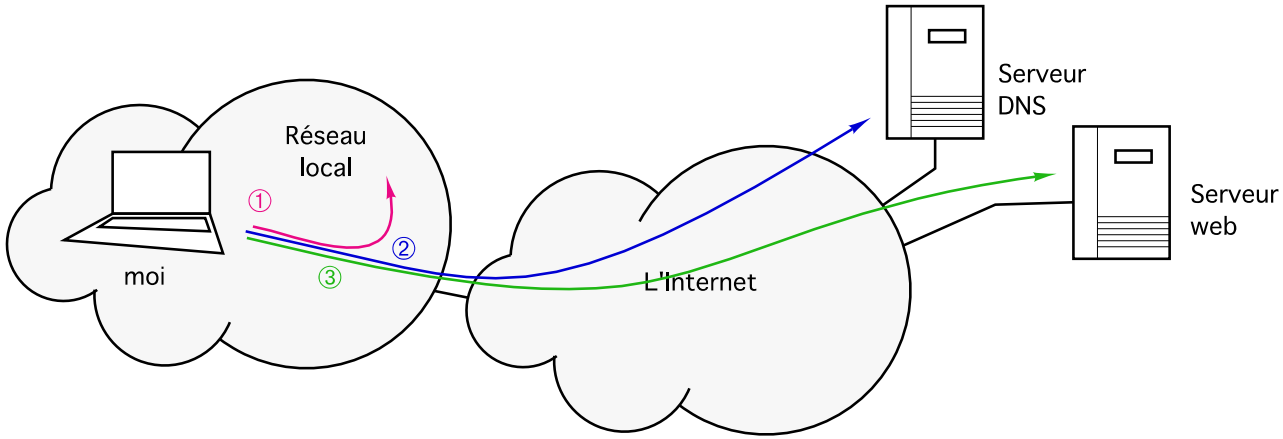
Lorsque je connais l'adresse IP de mon correspondant et de mon routeur par défaut.



Mon réseau local est averti de mes intentions.

Si je ne connais pas l'adresse IP de mon correspondant,

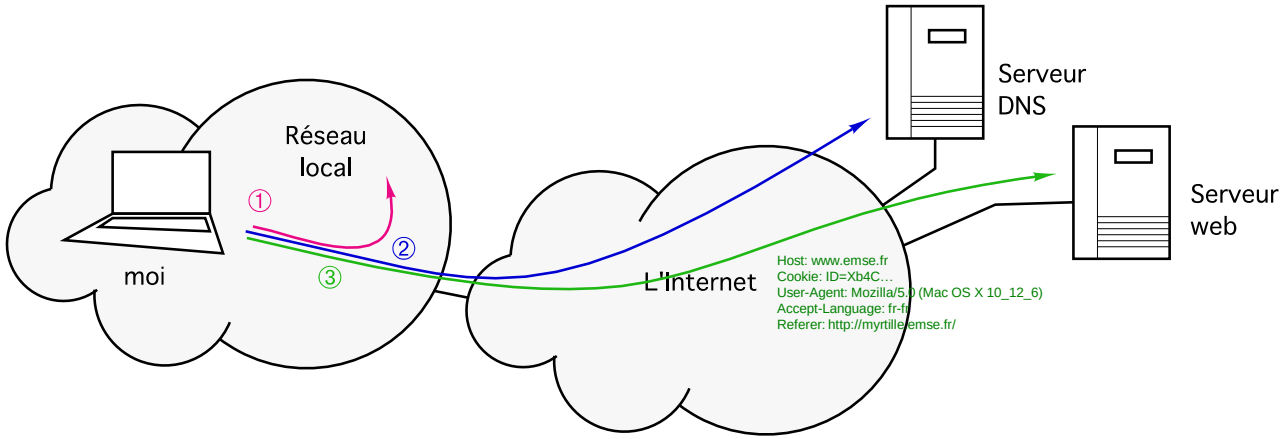
- **J'interroge le service DNS pour l'obtenir.**



Si historiquement les informations relatives à une machine étaient gérées directement par son propriétaire, aujourd'hui c'est rarement le cas : on a externalisé le service.

**les grands opérateurs et *registrars*
offrent ce service.**

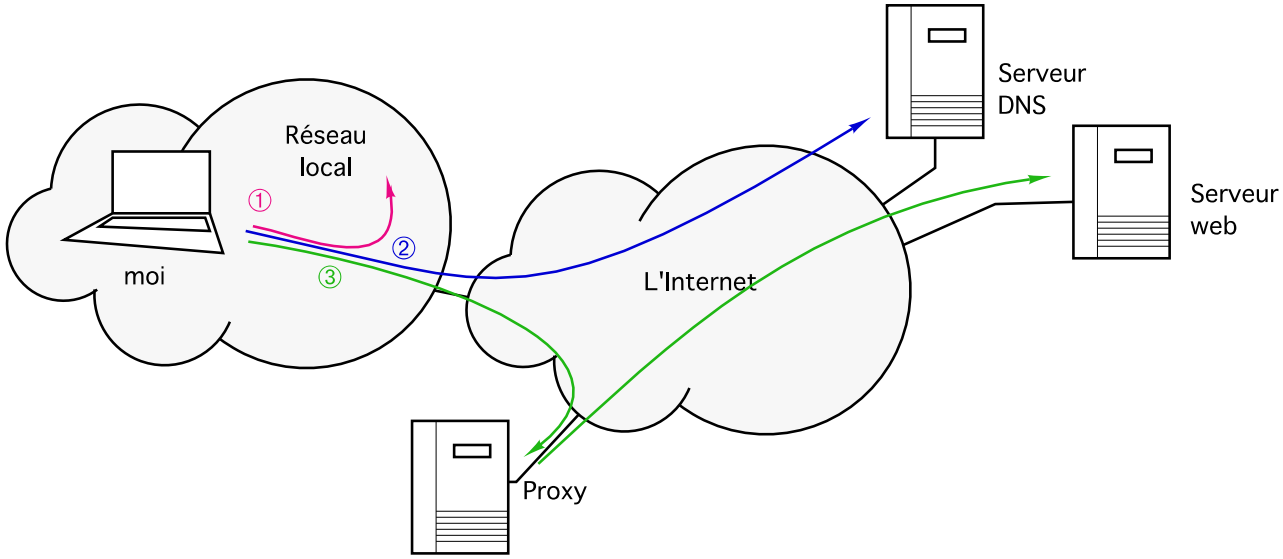
Après s'être connecté au serveur Web, notre navigateur web lui réclame les documents convoités.



La requête contient un ensemble d'informations « personnelles » :

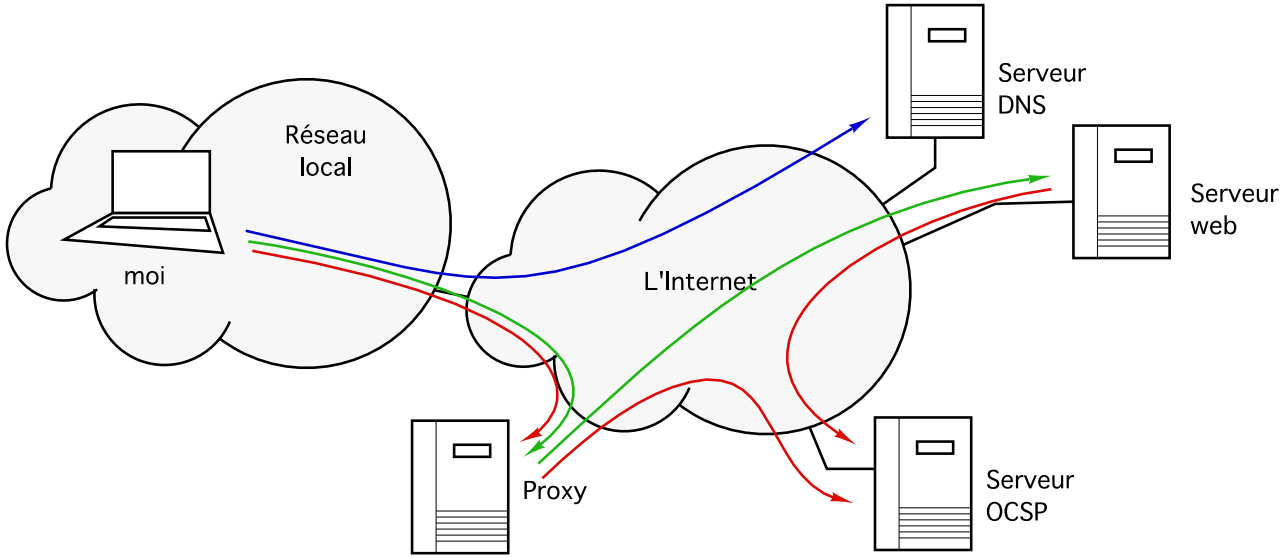
- le type du navigateur,
- des cookies,
- l'origine du lien (*referer*),
- …

Pour des raisons d'efficacité, de contrôle ou de sécurité, de nombreuses organisations ou opérateurs relaient les requêtes web (proxy).



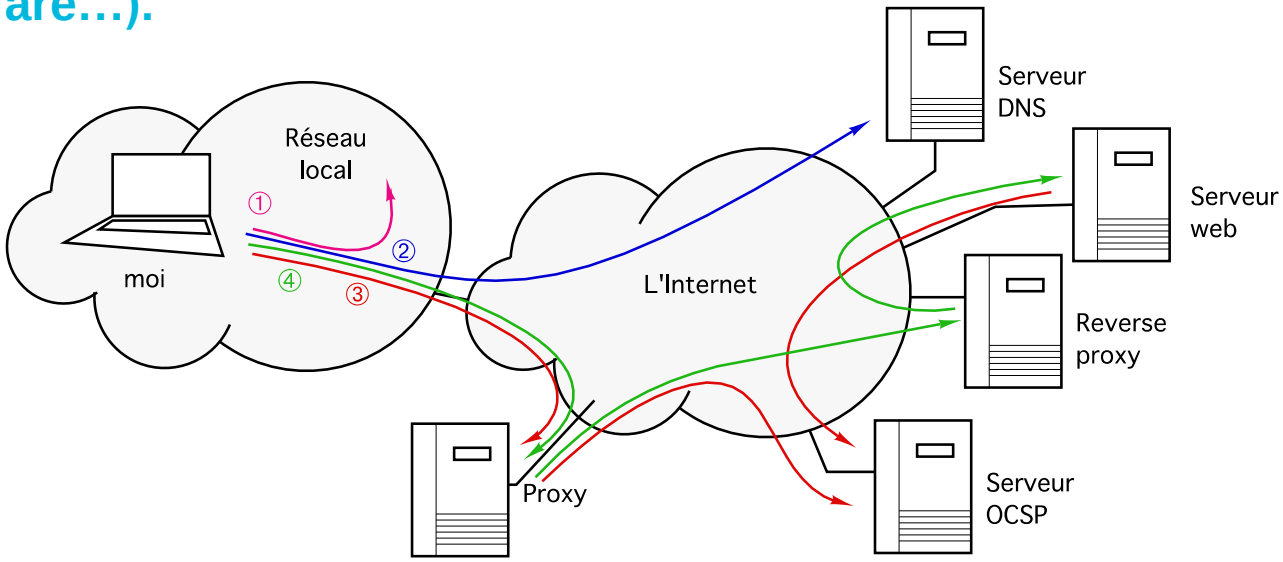
De nombreux Firewalls offrent ce service de manière transparente.

La confidentialité et l'intégrité des communications est assurée par TLS. La validité des certificats est vérifier auprès des AC avec OCSP.

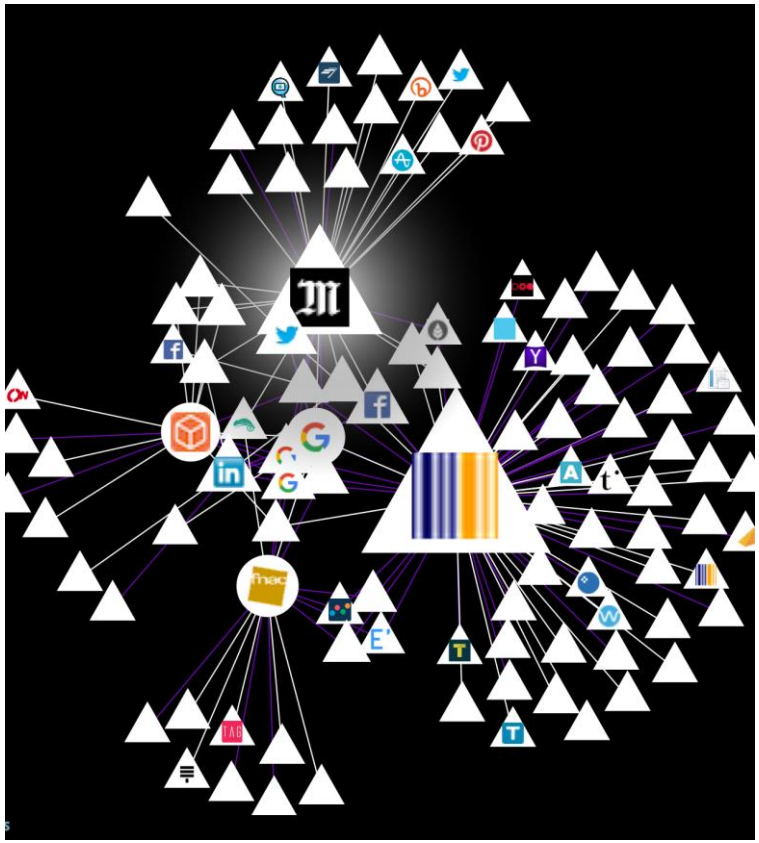


Comodo est le plus grand fournisseur de certificat de la planète (40% des certificats utilisés), Symantec ceux de Google, Facebook, Wikipedia…

Pour protéger leurs serveurs des dénis de services et autres attaques, de nombreux acteurs du web utilisent les services de *reverse proxy* (Cloudfare…).



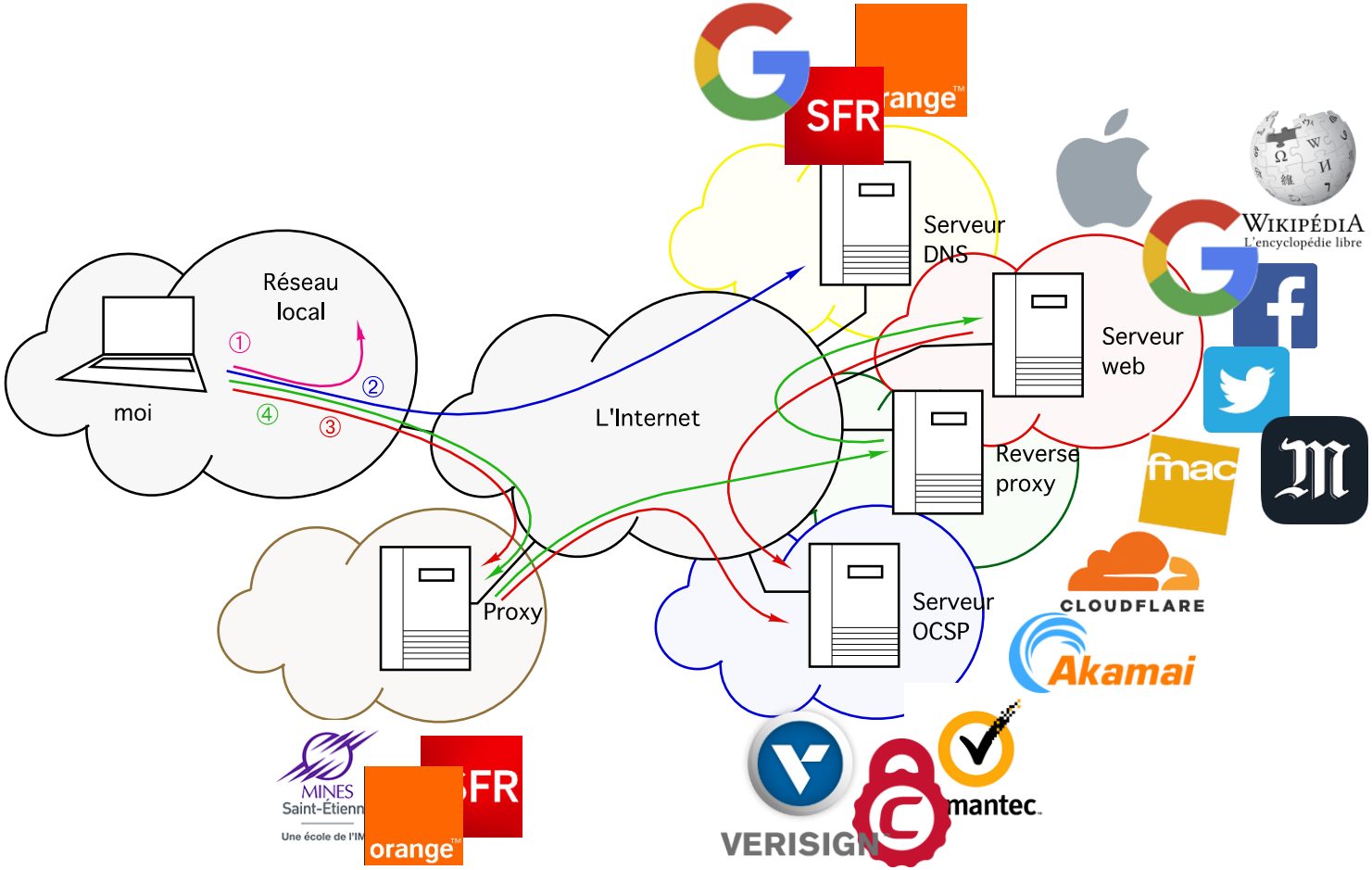
Pour accélérer les communications, de nombreux grands acteurs du web utilisent les services de caches distribués (Akamai…).



Lightbean – addon Firefox

Tout ça sans parler des informations qui nous échappent dès lors que l'on affiche une page web ou un email :

- **Des images importées de « l'exterieur ».**
- **Des librairies javascript indispensables.**
- **Les « web bugs ».**
- **Le pre-fetch des navigateurs.**
- **…**


Réseau
local
moi
①
②
③
④
L'Internet
Proxy
Serveur
DNS
Serveur
web
Reverse
proxy
Serveur
OCSP
SFR
orange
WIKIPÉDIA
L'encyclopédie libre
fnac
CLOUDFLARE
Akamai
VERISIGN
mantec
MINES
Saint-Étienn
Une école de l'IM

En plus des informations observables en différents points du réseau :

- **Les relais DNS savent avec qui vous allez vous connecter.**
- **Les serveurs OCSP des grand fournisseurs de certificats savent avec quel serveur vous êtes connectés, éventuellement avec quelle identité vous vous êtes présenté.**
- **Les proxys, les *reverse proxys*, les caches sont à même de prendre connaissance de vos requêtes, même si celles-ci sont chiffrées.**
- **De nombreux services (publicité, analyse d'audience…) sont informés de vos activités.**
- **…**

Aujourd'hui, ce n'est plus un problème de conserver et d'analyser toutes ces informations: le BigData est là pour ça.

**C’est sans aucun doute lui,
le réseau,
qui est le nouveau fournisseur d’informations personnelles.**

Nous devons prendre conscience que, au delà de transporter des informations, le réseau, les protocoles que nous utilisons ou que nous proposons laissent s'échapper des informations personnelles.

Chaque couche laisse échapper des informations.
Plus les couches sont basses, plus les informations sont enfouies et moins les utilisateurs sont conscients de ces fuites.

Nous devons aller vers des protocoles dont le design même doit prendre en compte le respect de la vie privée.

PEP : Privacy Enhanced Protocols

Merci de votre attention.