Les adresses symboliques et le serveur DNS

Conversion d'une adresse symbolique en adresse IP

1) Retrouver l'adresse IP des adresses symboliques suivantes (ping ou tracert avec l'invite de commande CMD).

Adresses symboliques	google.com	wikipédia.org	amazone.fr	amazone.com	amazon.com
Adresse IP					

2) Vérifier chaque adresse IP avec votre Navigateur

3) Retrouver l'adresse IP des adresses symbolique de vos sites préférés.

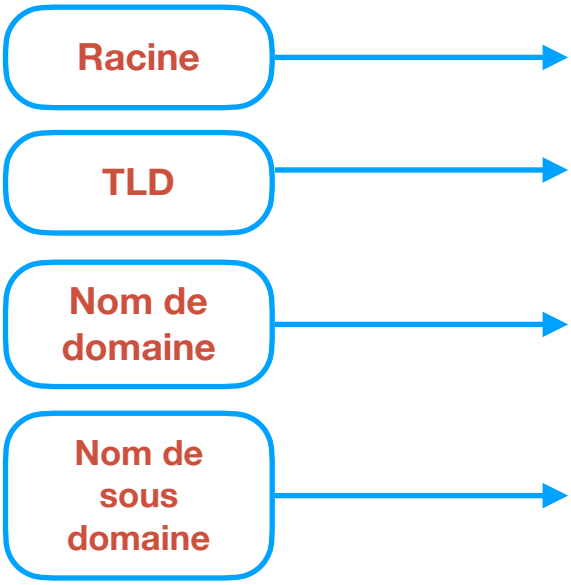
Adresses symboliques				
Adresse IP				

4) Échanger vos adresses IP et retrouver les adresses symboliques de votre camarade.

Adresse IP				
Adresse symbolique				

Structure d'une adresse symbolique d'une adresse symbolique

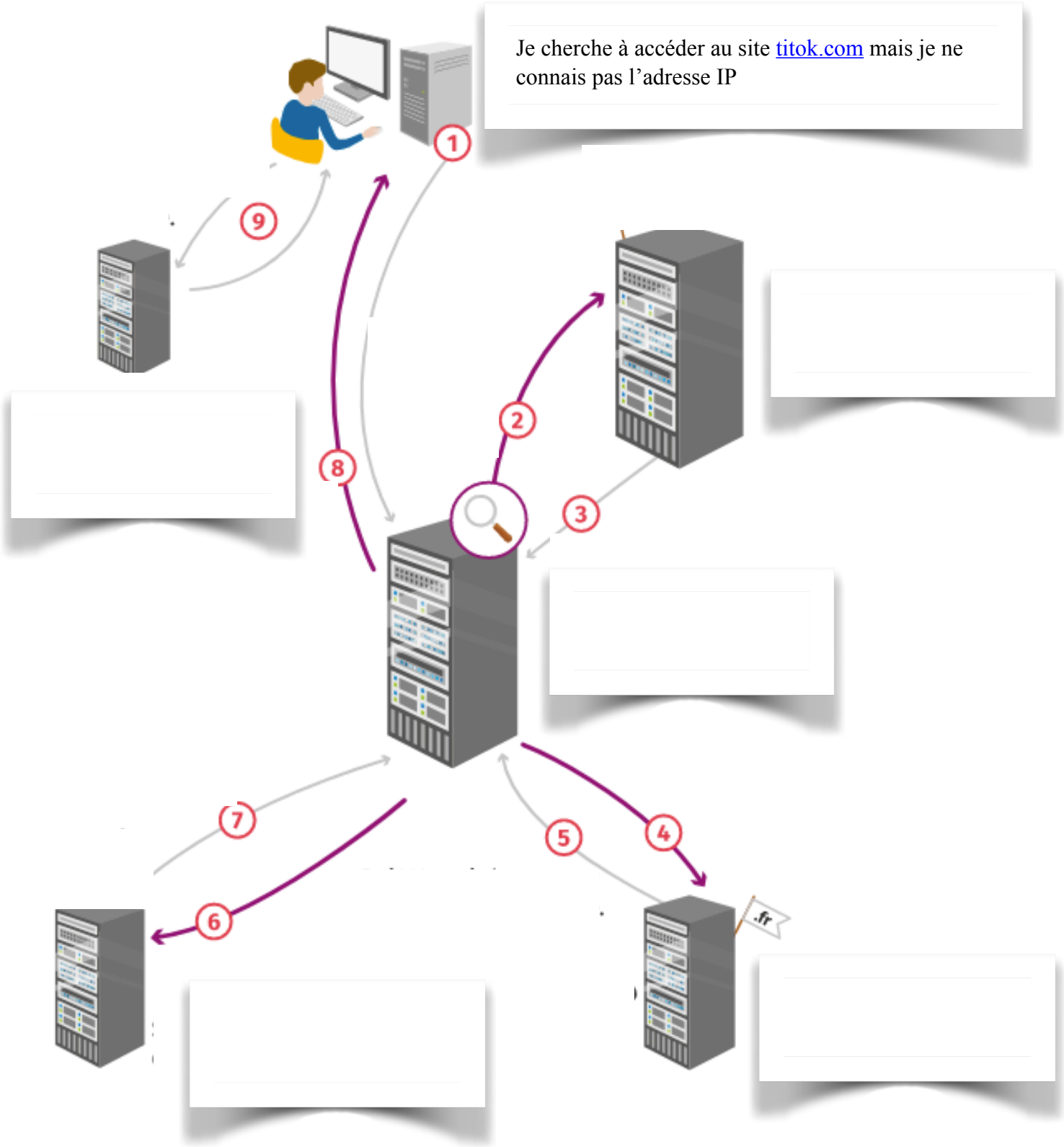
Décrire la lecture par le DNS de l'adresse symbolique www.leboncoin.fr.



Fonctionnement du serveur DNS

Comment le serveur résolveur étudie-t-il l'adresse symbolique ?

Déterminer l'adresse IP du site tiktok.com à partir des protocoles à disposition.



Informations officielles sur un nom de domaine

Que nous donne comme informations Ipconfig / all sur l'invite de commande (CMD sur windows) ?

Afficher les informations associées au nom de domaine google.fr. En quelle année a-t-il été créé ? Dans quel pays le titulaire du domaine est-il installé ?

Le site afnic permet d'obtenir toutes les informations légales d'un nom de domaine. Indiquer le pays du titulaire du nom de domaine snapchat.com, ainsi que sa date de création.

Utiliser la commande host sur MacOs/Linux ou nslookup pour google.fr : Quelle information est donnée ?

Utiliser le site "https://dnslookup.online/" et rechercher l'adresse Ip de google.

Modifier le DNS et regarder si l'adresse Ip de Google change ?

Quelle remarque pouvons nous faire si nous pouvons avoir le même site avec des DNS différents et des IP différentes ?

Le site afnic permet d'obtenir toutes les informations légales d'un nom de domaine. Indiquer le pays du titulaire du nom de domaine snapchat.com, ainsi que sa date de création.

Afficher les informations associées au nom de domaine google.fr. En quelle année a-t-il été créé ? Dans quel pays le titulaire du domaine est-il installé ?

Piratage du DNS

Qu'est ce que le DNS spoofing ?

A quelle étape une attaque sur les paquets peut-être faites dans l'exercice du fonctionnement du serveur DNS

Proposer plusieurs solution pour s'en protéger ?

Afficher le cache de résolution DNS ipconfig/displaydns

Comparer le avec l'historique de navigation. Le résultat est-il similaire ?

Tester ipconfig /all et donner la commande qui permet de vider le cache ?

Serveur racine *Serveurs TLD connus :* Serveur TLD 1 pour les **.fr** Serveur TLD 2 pour les **.com** Serveur TLD 3 pour **.io**	Serveur TLD 1 *Serveurs de domaines connus :* Serveur de domaine 2 pour **lemonde** Serveur de domaine 3 pour **lequipe** Serveur de domaine 1 pour **education.gouv** Serveur de domaine 4 pour **leboncoin**	Serveur TLD 2 *Serveurs de domaines connus :* Serveur de domaine 5 pour **google** Serveur de domaine 7 pour **facebook** Serveur de domaine 6 pour **snapchat** Serveur de domaine 6 pour **tiktok**
Serveur TLD 3 *Serveurs de domaines connus :* Serveur de domaine 1 pour **agar** Serveur de domaine 2 pour **brutal** Serveur de domaine 3 pour **superhex** Serveur de domaine 4 pour **slither**	Serveur de domaine 1 *Adresses IP connues :* 46.105.57.169 : gcbk.fr 104.17.151.222 : agar.io 91.198.174.192 : wikipedia.org 185.75.143.24 : education.gouv.fr 213.186.33.5 : lelivrescolaire.fr	Serveur de domaine 2 *Adresses IP connues :* 172.65.248.213 : doctolib.fr 104.21.90.97 : brutal.io 104.244.42.193 : twitter.com 151.101.194.217 : lemonde.fr 185.161.46.228 : agriculture.gouv.fr
Serveur de domaine 3 *Adresses IP connues* : 18.200.8.190 : netflix.com 172.67.142.206 : superhex.io 35.186.248.227 : lequipe.fr 176.32.103.205 : amazon.com 81.92.80.55 : figaro.fr	Serveur de domaine 4 *Adresses IP connues :* 172.67.38.239 : slither.io 208.84.41.110 : classmates.com 217.70.184.38 : w3c.org 13.225.38.60 : leboncoin.fr 185.129.44.23 : allocine.fr	Serveur de domaine 5 *Adresses IP connues :* 3.222.163.94 : instagram.com 216.58.209.238 : google.com 188.165.198.223 : stargate-fusion.com 142.250.179.110 : youtube.com 151.101.65.140 : reddit.com
Serveur de domaine 6 *Adresses IP connues :* 47.254.33.193 : yahoo.com 216.239.32.21 : snapchat.com 161.117.111.4 : tiktok.com 204.79.197.212 : live.com 13.107.42.14 : linkedin.com	Serveur de domaine 7 *Adresses IP connues :* 13.107.21.200 : bing.com 66.211.175.229 : ebay.com 157.240.21.35 : facebook.com 39.156.69.79 : baidu.com 151.101.2.167 : twitch.tv	

Démasquer une tentative d'arnaque grâce à l'IP

2.9

Parfois il est prudent de ne pas se fier à l'adresse symbolique et de s'intéresser à l'adresse IP. Imaginez, vous venez de recevoir un mail douteux qui dit ceci :

Cher(e) Client(e);
Nous enregistrons ce Jeudi 04 février 2016 un chèque d'un montant de **€340*.00 EUR*

*à l'ordre de MR LUSTIG VICTOR - 1 RUE ARSENE LUPIN - 39250 SHERWOOD - FRANCE
émis par *M.VERGER BENOÎT - 18 ALLEE DES TILLEULS - 64122 URRUGNE- FRANCE *

REMARQUE: Il est impératif de nous faire parvenir en répondant à ce mail (1) code de recharge PCS * de €100.00 EUR* pour vous acquitter des frais d'assurance. Dès réception et approbation du code après vérification, votre chèque vous sera expédié immédiatement. Vous le recevrez par courrier dans un (1) jour au maximum, à compter du jour de
réception du code de la recharge PCS MASTERCARD.

Christian SAINZ,
Directeur Relation Client, DHL Finance

Vous n'êtes pas bien sûr de comprendre pourquoi on vous envoie ça (pourtant c'est bien vous, Victor Lustig) mais il semble facile de gagner les 240€ promis. Que faire ?
Il faut être prudent et vérifier la provenance exacte de ce message, vérifier si tout colle bien. Voici l'entête complète de ce mail (qu'on peut faire apparaître, par ex. dans Gmail, en cliquant sur les trois points verticaux à droite de la flèche pour répondre, en haut à droite du message, puis « Afficher l'original » :

Delivered-To: isn.pourriel@gmail.com
Received: by 10.27.14.197 with SMTP id 66csp330398wlo;
Thu, 4 Feb 2016 00:23:13 -0800 (PST)
X-Received: by 10.55.15.199 with SMTP id 68mr2039057qkp.42.1454574192794;
Thu, 04 Feb 2016 00:23:12 -0800 (PST)
Return-Path: service.dhl.international@post.com
Received: from mout.gmx.com (mout.gmx.com. [74.208.4.200])
by mx.google.com with ESMTPS id a141si9579378qkb.16.2016.02.04.00.23.12
for isn.pourriel@gmail.com
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Thu, 04 Feb 2016 00:23:12 -0800 (PST)
Received-SPF: pass (google.com: domain of service.dhl.international@post.com designates 74.208.4.200 as permitted sender) client-ip=74.208.4.200;
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of service.dhl.international@post.com designates 74.208.4.200 as permitted sender) smtp.mailfrom=service.dhl.international@post.com
Received: from [192.168.1.100] ([41.191.68.245]) by mail.gmx.com (mrgmxus001) with ESMTPSA (Nemesis) id 0LrNUo-1a4NkD30Ga-01354I for isn.pourriel@gmail.com; Thu, 04 Feb 2016 09:23:11 +0100
From: "Service Expédition et Validation" service.dhl.international@post.com
To: isn.pourriel@gmail.com
Subject: CONFIRMATION DU DÉPÔT DE CHÈQUE DE BANQUE CERTIFIE

Quels sont le nom et l'adresse symbolique *apparents* de l'expéditeur ? Mais quelle est l'adresse symbolique *réelle* de son serveur mail ?
Cherchez son adresse IP dans l'entête (ou plus précisément celle de son serveur mail), puis dans un navigateur, allez sur le site https://ipgetinfo.com et cherchez des renseignements sur cette adresse. Est-elle compatible avec l'expéditeur supposé ?