

Identification d'adresses IP

Auteurs : Angel Andrades et Massimo Iritano
Professeur : Stephan Robert, PhD

1. BUT DU PROJET	3
2. INTRODUCTION À L'ADRESSAGE IP	3
3. INTRODUCTION AUX MÉTHODES DE RECHERCHE	4
3.1. METHODES DE RECHERCHE EN UTILISANT LES SITES INTERNET	4
3.1.1. <i>Emploi du DNS pour découvrir le nom du domaine.</i>	5
3.1.2. <i>L'emplacement géographique sur le DNS</i>	6
3.1.3. <i>Recherche par l'adresse URL</i>	7
3.1.4. <i>Aller directement sur l'adresse URL</i>	8
3.1.5. <i>L'annuaire WHOIS</i>	8
3.2. METHODE DE RECHERCHE EN UTILISANT DES LOGICIELS	9
3.2.1. <i>Logiciel traceur de route</i>	9
3.2.1.1. Trout 2.00	9
3.2.1.2. 3d traceroute	10
3.2.1.3. TRACEROUTE en mode DOS	12
3.2.2. <i>Logiciel Neotrace</i>	13
3.2.3. <i>Logiciel VisualRoute</i>	14
3.2.4. <i>Logiciel OstroSoft Internet Tools</i>	15
3.3. CONCLUSION SUR LES METHODES DE RECHERCHE	16
4. COMMENT ÊTRE ANONYME SUR LE WEB	16
4.1. INTRODUCTION.	16
4.2. UTILISATION DE SITE MASQUANT L'ADRESSE IP EN SURFANT.	17
4.2.1. <i>Les proxys</i>	17
4.2.2. <i>Les proxys gratuits</i>	18
4.2.3. <i>Les Tunnels</i>	23
4.3. UTILISATION DE SITE POUR ENVOYER DES E-MAILS.	24
4.3.1. <i>Les Remailers anonymes</i>	24
4.3.2. <i>Les serveurs de pseudonyme</i>	25
5. CONCLUSION	26

IDENTIFICATION D'ADRESSES IP

1. but du projet

Dans le cadre de notre projet de groupe, nous aimerions savoir qui se cache derrière un écran d'ordinateur, où qu'il soit et quoi qu'il fasse, avec comme seul indice pour notre recherche son adresse IP qui lui permet de recevoir et d'envoyer des données.

2. Introduction à l'adressage IP

L'adresse IP est une adresse unique servant à identifier un ordinateur, tout comme un numéro de téléphone identifie une personne de manière unique. Dans le cadre du standard actuel -IPV4-, les adresses sont codées sur 32 bits qui font un maximum de 4'294'967'296 (2^{32}) utilisateurs différents, ce qui est suffisant (à l'heure actuelle !!).

Pour l'ordinateur, cette adresse IP est codée en binaire sur 4 fois 8 bits selon l'exemple suivant :

202.15.170.1
11001010.00001111.10101010.00000001 (en binaire)

les adresses sont répertoriées selon différentes classes qui définissent différents réseaux et dans chaque type de classes il y aura un numéro de réseau et un numéro d'hôte.

Classe	Préfixe	Numéro de réseau	Numéro d'hôte
A	0	bits 1-7	bits 8-31
B	10	bits 2-15	bits 16-31
C	110	bits 3-24	bits 25-31
D	1110	Multicast	Multicast
E	1111	Réservé	Réservé

Dans chaque type de classes il y a un maximum d'hôtes dans le réseau.

Classe	Plage de numéros de réseau	Plage de numéros d'hôte
A	0 à 126	0.0.1 à 255.255.254
B	128.0 à 191.255	0.1 à 255.254
C	192.0.0 à 223.255.255	1 à 254

Classe	Nombre de réseaux	Nombre d'hôtes
A	126	16 777 214
B	16 384	65 534
C	2 097 152	254

Pour mieux illustrer les différentes classes, il serait préférable de voir un exemple :

Hewlett-Packard possède un réseau de classe A alors ils peuvent avoir 16 777 214 ordinateurs sur leur réseau.

De 16.0.0.1 à 16.255.255.254

Numéro du réseau Numéro de l'hôte

3. Introduction aux méthodes de recherche

Les adresses IP sont assignées arbitrairement par le provider (fournisseur d'accès). En effet, il n'y a aucune connexion inhérente entre l'adresse IP et l'emplacement physique de l'utilisateur. Ainsi donc, la recherche ne sera pas facilitée.

Cependant, en effectuant des recherches tel un détective, il est possible de se rapprocher, en quelque sorte, de la personne utilisant cette adresse IP, et même, dans certains cas, de retrouver ses traces.

Il existe diverses méthodes pour retrouver un utilisateur du réseau Internet en connaissant son adresse IP. Ces méthodes, nous les avons retrouvées sur divers sites, en voici une explication.

3.1.Méthodes de recherche en utilisant les sites Internet

Les points suivants peuvent aider à retrouver les traces d'un utilisateur du réseau Internet sans avoir besoin de logiciel. En effet, les méthodes suivantes sont disponibles sur Internet gratuitement.

3.1.1. Emploi du DNS pour découvrir le nom du domaine.

Le serveur permettant de faire la correspondance entre l'URL (compréhensible par un humain) et l'adresse IP (compréhensible par les ordinateurs) s'appelle le DNS (Domain Naming System).

La commande '**nslookup**', en mode DOS, permet de trouver qui est connecté via l'adresse IP que vous inscrivez en consultant le DNS.

Voici comment procéder :

- Vous prenez une adresse IP, par exemple 132.74.18.2. et la saisissez à l'aide du clavier à la suite comme ceci : '**nslookup 132.74.18.2**'. Cela vous donnera comme résultat l'adresse 'haifa.ac.il'. Le nom du domaine correspondant à l'adresse IP inscrite.

De ce résultat, il faut en retirer les informations suivantes :

1. Le TLD (Top Level Domain):**il** indique que le domaine est en Israël.
2. Les deux informations suivantes sont 'haifa.ac'. On sait donc que ce domaine appartient à l'institut académique de Haïfa (dans ce cas, il s'agit d'une université), et que l'université de Haïfa se trouve sûrement à Haïfa.

La commande '**nslookup**', ne donne pas toujours les informations désirées, elle n'est pas toujours apte à nous fournir le nom du domaine, et fonctionne surtout pour les réseaux internes.

La traduction inverse de DNS ne fonctionne pas toujours, cela dépend de la configuration du centre serveur (le domaine avec l'IP donné). La commande '**dig**' sur Linux est paraît-il plus efficace.

Si la commande '**nslookup**' ne peut donner une solution à la requête, il existe des sites ou des logiciels retournant l'adresse du site (DNS) correspondante à une adresse IP, mais aussi l'inverse.

Voici par exemple un site qui possède une base de données permettant de rechercher le propriétaire d'une adresse IP:

<http://www.flumps.org/ip/>

La marche à suivre est la suivante : cliquer sur la classe correspondant à l'intervalle dans lequel est compris le premier chiffre de l'adresse IP. Puis poursuivre la recherche avec la suite des chiffres. Certains logiciels sont plus fonctionnels, mais cela sera développé plus en détails plus bas dans ce document.

Une autre façon de procéder serait l'utilisation d'une requête WHOIS (QUI C'EST). Il existe une multitude de sites qui proposent cette annuaire. Ce sujet sera expliqué, plus en détails dans le paragraphe 3.1.5.

3.1.2. L'emplacement géographique sur le DNS

Quelques serveurs supportent une extension de DNS qui permet d'entrer leur emplacement géographique lors de leur enregistrement. Cette extension du DNS est décrite sur ce lien : <ftp://ftp.rfc-editor.org/in-notes/rfc1876.txt>.

Pour avoir une vue d'ensemble des serveurs utilisant cette extension du DNS, il existe un site qui montre, par des cartes, l'emplacement de ces serveurs. De plus, il propose un formulaire permettant de traduire soit une adresse IP, soit une adresse URL en un lieu géographique sur une carte.

<http://www.ckdhr.com/dns-loc/>

Exemple de recherche de la localisation graphique du yahoo.com :



Il en résulte que le serveur yahoo.com se trouve à Sunny Vale proche de San Jose. Donc il est localisé au USA.

Pour l'instant, cette extension du DNS est peu utilisée. Ainsi donc, la localisation géographique d'un serveur reste très limitée avec ce moyen.

Une façon différente d'exprimer l'emplacement géographique d'un centre serveur par l'intermédiaire du DNS est faite sur <ftp://ftp.rfc-editor.org/in-notes/rfc1712.txt>.

Les deux RFCs définissent un enregistrement de ressource DNS pour contenir l'emplacement géographique.

3.1.3. Recherche par l'adresse URL

Toutes les adresses URL possèdent un code de pays (TLD : Top Level Domain) qui sont des abréviations de deux ou trois lettres. Ces codes devraient, en principe, nous donner le pays où se trouve le serveur où est enregistré le site.

Il est à noter que l'hôte d'un domaine, pourrait être accueilli dans un autre pays. Cela est dû à l'accueil virtuel, autrement dit, le domaine d'une entreprise pourrait être accueilli meilleur marché dans un pays voisin.

Notez également que les .org, .com, et autres .edu n'indiquent pas où se trouve le centre serveur. Ces domaines appartiennent à des sociétés internationales et on ne peut savoir où elles sont basées en allant que sur leur lien internet. De plus, elles pourraient avoir plusieurs centres serveurs partout dans le monde.

Ces codes et leurs significations sont disponibles sur Internet sous forme de liste. Les sites suivant mettent à la disposition des internautes une liste complète de ces abréviations :

<http://www.iana.org/domain-names.htm>

<http://www.ics.uci.edu/pub/websoft/wwwstat/country-codes.txt>

D'autres abréviations apparaissent dans ces adresses. Généralement, ce sont les sites ayant un grand nombre de pages ou des entreprises ayant différents départements. A titre d'exemple ; voici deux abréviations utilisées aux Etats-Unis.

- Pour se référer aux états : AL pour Alabama.
- Pour l'armée : AP pour Armed Forces Pacific

Le lien suivant fournit une liste complète d'abréviations utiles pour les sites américains :

http://www.usps.gov/ncsc/lookups/abbr_state.txt

Pour se distinguer, les aéroports ont aussi des codes ou abréviations. Une liste complète des codes concernant les aéroports américains sont sur le site suivant :

<http://www.aviationjobsonline.com/airports/citycode.html>

3.1.4. Aller directement sur l'adresse URL

La visite du site Web dont vous avez l'adresse URL peut être un bon moyen d'obtenir quelques informations pertinentes, comme par exemple l'adresse de l'organisation, numéro de téléphone, etc.

Par exemple pour haifa.ac, vous pouvez trouver des informations sur les sites :

<http://www.haifa.ac.il/>

<http://www.ac.il/>

3.1.5. L'annuaire WHOIS

On peut aussi utiliser le WHOIS. Cet annuaire Internet contient les informations concernant l'administrateur de ce site ainsi que les coordonnées permettant de le contacter, mais aussi à qui appartient le domaine.

Ces données administratives sont introduites lors de l'enregistrement du domaine et sont mises à jour périodiquement. Ainsi donc, cet annuaire est une grande source d'information intéressantes sur les propriétaires et concepteurs du domaine.

Mais attention, car l'annuaire Internet WHOIS n'est pas toujours fiable. Si l'adresse appartient à une grande société et, qui plus est, sérieuse, cette entreprise fournira des informations fiables et les mettra à jour régulièrement. Par contre, si la personne qui enregistre l'adresse ne tient pas vraiment à donner des informations correctes et ne donne aucune importance à leur mise à jour, ces données pourraient être incorrectes.

Sur le site <http://www.arin.net/> cliquez sur le lien WHOIS, entrez l'adresse IP dans la case prévue et cliquez sur SUBMIT. Vous obtiendrez des informations sur le détenteur de cette adresse IP. Ce site est principalement destiné aux adresses IP des USA.

Mais, dans le cas où il ne contiendrait pas les informations désirées, par exemple si l'adresse a été attribuée à un domaine en Europe, le site lui-même vous proposera des liens utiles. Par exemple, il vous sera proposé la page <http://www.ripe.net/perl/whois/>, se trouvant sur le site <http://www.ripe.net/>, ou encore <http://www.apnic.net>.

Il existe aussi, un site permettant le passage de l'adresse IP aux coordonnées géographiques, latitude-longitude. Ce site essaiera d'afficher les mêmes informations que WHOIS, mais fournira une représentation graphique du lieu.

<http://cello.cs.uiuc.edu/cgi-bin/slamm/ip2ll/>

Malheureusement, ce site fonctionne principalement pour les serveurs situés au USA.

Le site Allwhois permet de consulter les annuaires Internet WHOIS de plusieurs pays dans le monde : <http://www.allwhois.com/>

De plus, une liste de serveurs WHOIS, collectés par Matt Power, est disponible sur le site suivant : <ftp://sipb.mit.edu/pub/whois/whois-servers.list>.

Il est à noter, que ces informations concernent habituellement le branchement principal des propriétaires ou des points de contact, mais que les adresses IP pourraient être assignées à des centres serveurs qui peuvent être situés à un(des) lieu(x) différent(s).

3.2.Méthode de recherche en utilisant des logiciels

Il existe aussi toute une panoplie de logiciels, plus ou moins efficaces, permettant de faire des recherches d'adresse IP, d'adresse URL, mais aussi de localiser géographiquement un serveur.

3.2.1. Logiciel traceur de route

La fonction TRACEROUTE donne le nom des routeurs au travers desquels les paquets s'écoulent de votre serveur au serveur dont on désire connaître l'emplacement géographique.

Autrement dit, cette fonction envoie des paquets adressés au serveur dont on donne le nom ou l'adresse IP, et elle recueille les adresses IP ainsi que le nom des serveurs par lesquels transitent les paquets pour arriver au serveur de destination.

Ainsi donc, nous obtenons l'emplacement physique de destination des paquets. C'est à dire que nous savons sur quels serveurs se trouve le domaine cherché.

3.2.1.1. Trout 2.00

Ce logiciel est très simple à utiliser. En effet, il suffit d'inscrire une adresse IP ou un nom de domaine dans la case prévue à cet effet, et de cliquer sur Start trace pour lancer la fonction TRACEROUTE.

Il affiche directement les adresses IP et le nom des serveurs que les paquets traversent pour arriver au serveur de destination, ainsi que le domaine de destination lui-même.

De plus, ce logiciel dispose aussi de la fonction WHOIS qui a déjà fait l'objet d'une explication au paragraphe 3.1.5 de ce document. En réalité, il va chercher ces informations sur les serveurs contenant un annuaire WHOIS. Et il est possible de lui spécifier quel serveur WHOIS on désire consulter.

L'avantage de ce logiciel, c'est qu'il ne fait que 40ko et que c'est un simple fichier exécutable.

Où trouver ce logiciel : <http://www.hlembke.de/prod/3dtraceroute/>

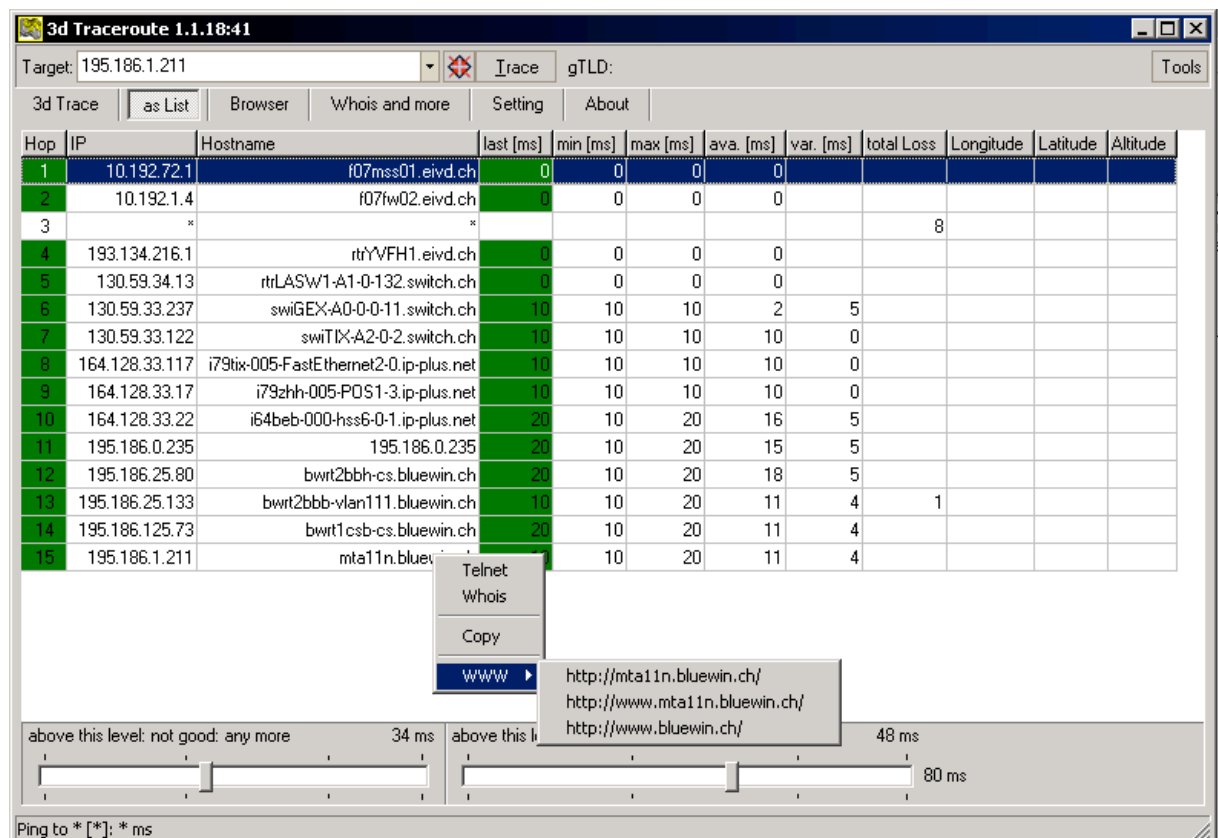
3.2.1.2. 3d traceroute

Ce logiciel est largement plus complet que le précédent. Non seulement il propose les fonctions TRACEROUTE et WHOIS, mais il possède un browser permettant de visualiser le site Internet associé à une adresse IP, si toutefois cette adresse conduit bien à un site, ou plus simplement de surfer sur le Net.

Il propose aussi une représentation graphique très puissante des temps que mettent les paquets pour passer d'un serveur à un autre. Tant qu'on le ne lui demande pas de s'arrêter, il continue à renvoyer des paquets. Cela permet d'avoir une valeur moyenne de temps de transmission ainsi que de voir les différences de temps pour les différents paquets qu'il a envoyés. Mais cela, aussi puissant qu'il soit, ne nous est pas d'une très grande utilité dans le cadre de ce projet.

Encore une chose qui est très bien faite, c'est la partie permettant le paramétrage du logiciel. Cette représentation type organigramme, permet d'avoir d'un seul coup d'œil une vue d'ensemble des différents paramètres modifiable ainsi que les liens qu'ils pourraient avoir avec d'autres paramètres.

Pour tester ce logiciel, nous avons pris, comme exemple, l'adresse IP contenue dans un mail. Cette adresse IP est la suivante : 195.186.1.211



Nous constatons que les paquets, une fois sortis du réseau interne de l'EIVD, passent par les serveurs de switch.ch, mais aussi par ceux de ip-plus.net, et pour finir chez bluewin.ch.

Puis, en cliquant avec le bouton de droite de la souris, il permet de visualiser les données contenues dans un annuaire WHOIS concernant l'adresse sur laquelle on a cliqué, mais aussi de visualiser différentes adresses URL liées à cette adresse IP sur son browser. Bien évidemment, les sites ne sont visitables que si l'adresse URL est bien associée à un site. Sur la figure ci-dessus, seule la dernière adresse mène à un site.

Et pour obtenir les informations concernant l'entreprise, il suffit de cliquer sur l'option WHOIS. Ci-dessous se trouvent les informations fournies par la fonction WHOIS de ce logiciel.

```
Query bluewin.ch at whois.thur.de
Process query: 'bluewin.ch'
Querying whois.nic.ch:43 with whois.

whois: This information is subject to an Acceptable Use Policy.
See http://www.nic.ch/terms/aup.html

Domain name:
bluewin.ch

Holder of domain name:
Bluewin AG
Peter Zollinger / BWN-OP
Finance & Controlling
Hardturmstrasse 3
CH-8005 Zürich
Switzerland

Technical contact:
Bluewin AG
Peter Zollinger / BWN-OP
Finance & Controlling
Hardturmstrasse 3
CH-8005 Zürich
Switzerland

Name servers:
dns1.bluewin.ch [195.186.1.110]
dns2.bluewin.ch [195.186.1.111]

Date of last registration:
31.12.1995

Date of last modification:
27.07.2000
```

Il contient les données de l'entreprise (nom, adresse, etc.) ainsi que de la personne responsable du service technique concernant cette adresse IP, mais aussi, les noms des serveurs avec leurs adresse IP correspondantes. Et pour finir, la date du dernier enregistrement et celle de la dernière mise à jour des données.

Ce logiciel est aussi un simple exécutable qui ne fait pas l'objet d'une installation préalable et n'occupe pas beaucoup de mémoire car il ne fait que 673ko.

Où trouver ce logiciel: <http://www.foundstone.com>

3.2.1.3. TRACEROUTE en mode DOS

Cette fonction est aussi disponible en mode DOS. Elle est exécutable grâce à la commande **tracert** suivie de l'adresse IP. Il faut remarquer qu'elle fonctionne aussi en entrant comme paramètre une adresse URL.

Pour en montrer un exemple d'utilisation de cette commande DOS, nous avons tracé l'adresse suivante : 18.181.0.31

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

U:\>tracert 18.181.0.31

Détermination de l'itinéraire vers DANDELION-PATCH.MIT.EDU [18.181.0.31]
avec un maximum de 30 sauts :

  1  <10 ms    <10 ms    <10 ms    f07mss01.eivd.ch [10.192.72.1]
  2  <10 ms    <10 ms    <10 ms    f07fw02.eivd.ch [10.192.1.4]
  3  *          *          *          Délai d'attente de la demande dépassé.
  4  <10 ms    <10 ms    <10 ms    rtrYVFH1.eivd.ch [193.134.216.1]
  5  <10 ms    <10 ms    <10 ms    rtrLASW1-A1-0-132.switch.ch [130.59.34.13]
  6  <10 ms    10 ms     10 ms     swiGEX-A0-0-0-11.switch.ch [130.59.33.237]
  7  <10 ms    <10 ms    10 ms     swiCE1-A4-0-0-5.switch.ch [130.59.33.66]
  8  10 ms     10 ms     10 ms     swiCE2-G2-1.switch.ch [130.59.36.25]
  9  10 ms     10 ms     10 ms     switch.ch1.ch.geant.net [62.40.103.17]
 10  10 ms     20 ms     20 ms     ch.fr1.fr.geant.net [62.40.96.30]
 11  20 ms     30 ms     20 ms     fr.uk1.uk.geant.net [62.40.96.90]
 12  90 ms     90 ms     91 ms     62.40.126.13
 13  110 ms    130 ms    130 ms    62.40.126.6
 14  130 ms    130 ms    120 ms    mit-nyc.es.net [134.55.208.142]
 15  110 ms    120 ms    111 ms    B24-RTR-1-ESNET.MIT.EDU [18.201.0.117]
 16  110 ms    110 ms    110 ms    NW12-RTR-2-BACKBONE.MIT.EDU [18.168.0.21]
 17  110 ms    110 ms    120 ms    DANDELION-PATCH.MIT.EDU [18.181.0.31]
```

Les deux premières lignes donnent des adresses IP internes à l'EIVD. La quatrième donne l'adresse IP utilisée pour passer du réseau interne de l'école au réseau Internet.

Les lignes 5 à 8 montrent que les serveurs de Switch.ch ont été utilisés (localisés en Suisse). Sur la ligne 7 apparaît une adresse IP qui appartient à Geant.net (situé en Grande-Bretagne) et c'est celle utilisée entre les serveurs de Switch.ch et ceux de Geant.net. Les lignes suivantes, jusqu'à la douzième, indiquent que les serveurs de Geant.net sont empruntés.

Puis, les paquets passent par l'université de Harvard dans le Massachusetts aux USA, pour ensuite arriver à l'Institut Technologique du Massachusetts où se trouve MIT (www.mit.edu).

Comme on peut le voir, les informations concernant l'emplacement des serveurs ci-dessus ne sont pas fournies par la commande **tracert** en mode DOS. Elles sont données par les annuaires WHOIS que nous avons consultés après avoir obtenu les informations de la fonction TRACEROUTE.

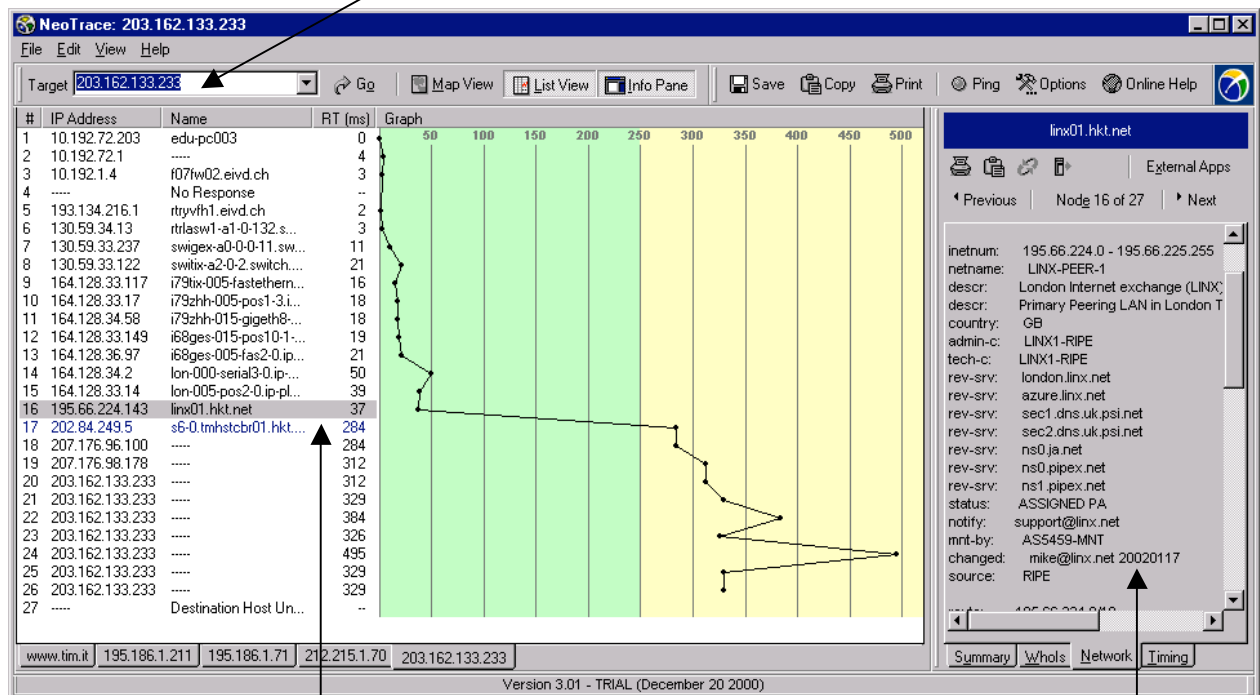
Comme nous l'avons fait remarquer dans le paragraphe 3.1.5 concernant la fonction WHOIS, les informations fournies par ces annuaires peuvent être erronées.

3.2.2. Logiciel Neotrace

Ce logiciel nous permet de voir le trajet des paquets comme les logiciels de type traceur vus ci-dessus, et en plus de pouvoir visualiser sur une carte du monde, ce qui permet de mieux comprendre par où passent les paquets. De plus, il y a la possibilité de voir les informations relatives à chaque saut de nos paquets (sur le logiciel, correspondant à chaque ligne), tout simplement en allant dans l'onglet 'Network' ou 'Whois'.

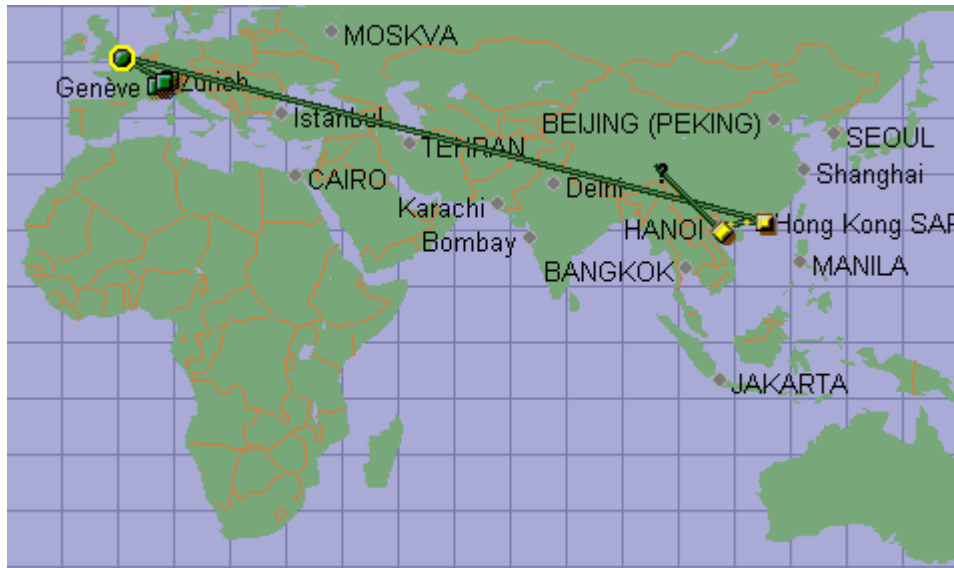
Exemple d'un e-mail reçu par un internaute se trouvant au Vietnam

Adresse IP de l'internaute (203.162.133.233)



Ligne sélectionnée
correspondant au
16^{ème} saut.

Information correspondant à
la ligne 16 dans l'onglet
Network, et on constate que
notre paquet a passé par
Londres.



Vue géographique de notre recherche.

Où trouver le logiciel : <http://www.neotrace.com>

3.2.3. Logiciel VisualRoute

VisualRoute fournit à quelque chose près les mêmes possibilités que le logiciel Neotrace, mais on peut faire en plus la recherche par l'e-mail d'une personne.

Exemple d'une recherche d'un e-mail (patric@usa.net)

164.128.236.93	i00nyh-015-fastethernet9-1-0.i	(Switzerland)	+01:00	101	Loopbacks+LANs USA								
164.128.236.98	i00nyh-005-fastethernet9-1-0.i	(Switzerland)	+01:00	110	Loopbacks+LANs USA								
<div style="border: 1px solid black; padding: 5px;"> <p>eMailTracker by Visualware</p> <p>patric@usa.net</p> <table border="1"> <thead> <tr> <th>Server</th> <th>Prio</th> <th>IP Address</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>mxpool01.netaddress.usa.net</td> <td>10</td> <td>165.212.8.32</td> <td>ESMTP USA.NET-MTA vM3.4.JUL00</td> </tr> </tbody> </table> <p>Click on a server name to start a VisualRoute trace</p> </div>						Server	Prio	IP Address	Status	mxpool01.netaddress.usa.net	10	165.212.8.32	ESMTP USA.NET-MTA vM3.4.JUL00
Server	Prio	IP Address	Status										
mxpool01.netaddress.usa.net	10	165.212.8.32	ESMTP USA.NET-MTA vM3.4.JUL00										
12.122.11.146	gbr1-p80.la2ca.ip.att.net	Los Angeles, CA, USA	-08:00	176	AT&T ITS								
12.123.199.33	ar1-p310.so2ca.ip.att.net	San Luis Obispo, CA, USA	-08:00	185	AT&T ITS								
12.124.252.26	-	Middletown, NJ 07748		203	AT&T ITS								
165.212.8.32	mxpool01.netaddress.usa.net	Colorado Springs, CO 80917		189	USA.NET, Inc.								

er-retour pour mxpool01.netaddress.usa.net, moyenne = 189ms, min = 180ms, max = 270ms -- Feb 28, 2002 4:49:27 PM

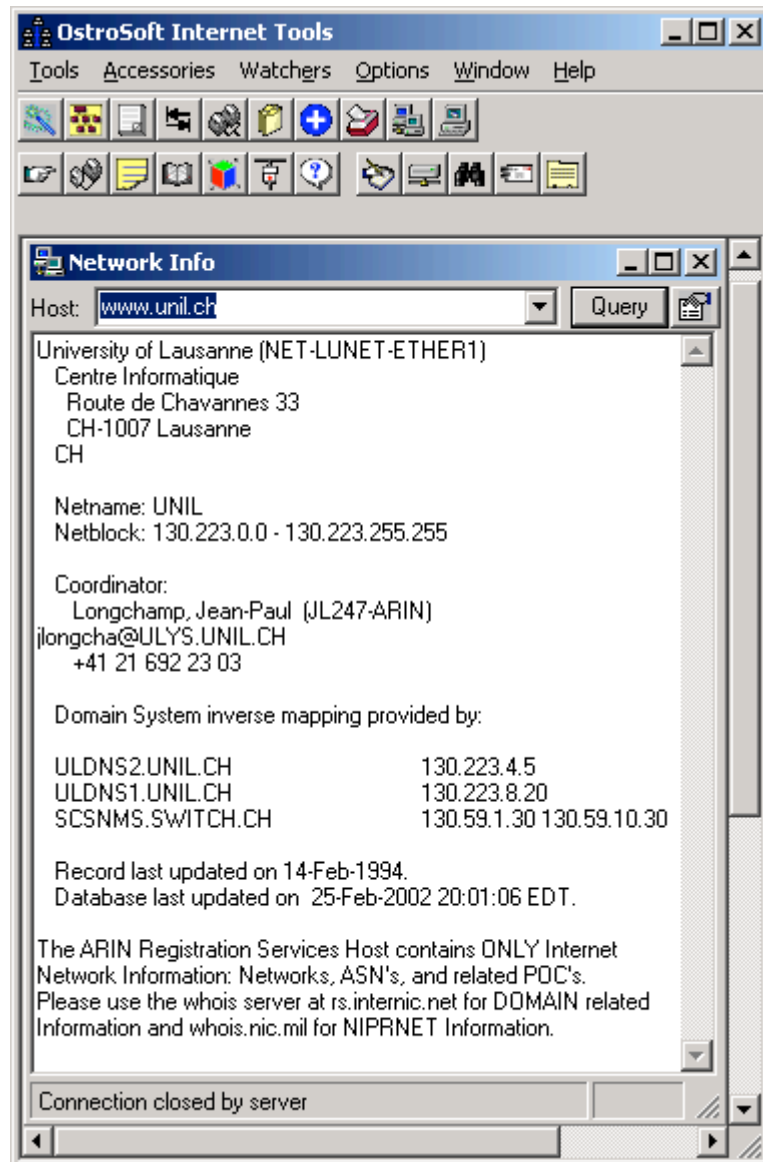
Mais avec l'adresse e-mail nous n'obtenons pas où est localisé l'internaute mais plutôt la où est localisé le Webmail, donc en mettant l'adresse URL du Webmail (www.usa.net) nous serions arrivés au même résultat.

Où trouver le logiciel : <http://www.visualware.com/visualroute/index.html>

3.2.4. Logiciel OstroSoft Internet Tools

Comme les logiciels précédents, celui-ci permet de nous fournir les informations trace route (dans le menu tools) et il permet aussi d'aller interroger des sites de type 'whois' pour en tirer les informations associées au nom du domaine ou à l'adresse IP, ceci avec la commande 'Network Info'. Il y a aussi la possibilité de faire la recherche par l'e-mail par la commande 'finger', mais celle-ci ne se révèle pas concluante.

Exemple de recherche :



Où trouver le logiciel : <http://www.ostrosoft.com/ostronet.html>

3.3. Conclusion sur les méthodes de recherche

Nous avons énuméré plusieurs méthodes de recherche avec différentes manières de s'informer sur la localité par où passent les paquets et autres informations. Mais malheureusement toutes nos méthodes ne nous permettent pas d'arriver à identifier la personne recherchée, nous arrivons seulement à savoir par quel provider il accède à internet.

Il n'y a que la police qui peut identifier une personne, car en cas d'activité illégale sur Internet, la police doit en premier lieu déterminer l'adresse IP du criminel. Ensuite, elle doit consulter la table du fournisseur d'accès pour déterminer quel abonné était associé à cette adresse IP à l'heure du délit.

4. Comment être anonyme sur le Web

Après avoir vu comment on recherche une personne sur Internet, nous allons montrer comment un utilisateur peut surfer sans qu'un site ou un autre utilisateur puisse connaître la véritable adresse IP.

4.1. Introduction.

L'anonymat d'un internaute n'est absolument pas garanti lorsqu'il utilise le réseau Internet. En effet, il existe plusieurs techniques, utilisées par les régies de publicité en ligne ou même par les services de renseignement des grands pays, pour identifier les internautes.

Voici un petit aperçu des méthodes utilisées :

- La technique la plus utilisée sont les **cookies**. Petits fichiers texte contenant un numéro d'identification ainsi que des informations concernant les pages consultées, le nombre de visites, les actions effectuées et plus encore.
- L'adresse IP via laquelle l'internaute est connecté.
- Une sorte de **cookies** intelligents appelés "Web bugs" qui sont sous forme d'une image d'un seul pixel invisible et indétectable. Ces "Web bugs" se trouvent soit dans des e-mails, soit sur certains sites Web ou encore dans certains groupes de discussions.
- Mais aussi, l'espionnage de données informatiques tels que les e-mails.

En plus chaque information personnelle présente sur votre ordinateur permet de vous identifier, notamment :

- La base de registration de Windows fournit de nombreuses informations pouvant vous identifier (nom, adresse e-mail, numéro de série de Windows) et pouvant être lues par un VbScript ou un ActiveX inclus dans une page Web.
- L'adresse MAC unique de votre carte réseau.
- Le Processor Serial Number, ce numéro de série étant intégré au Pentium III, peut vous identifier, si vous ne l'avez pas désactivé dans le BIOS de votre ordinateur.

Il s'en suit un besoin grandissant, ressenti par beaucoup d'utilisateurs d'Internet, de conserver leur anonymat sans que cela ait un quelconque rapport avec des procédures illégales.

Dans la suite de ce document, nous allons présenter quelques moyens, plus ou moins efficaces, pour surfer et même envoyer des e-mails, anonymement.

4.2.Utilisation de site masquant l'adresse IP en surfant.

4.2.1. Les proxys

Les proxys peuvent vous aider à préserver votre anonymat sur le Web en masquant votre adresse IP de telle sorte que les sites que vous visitez ne verront que l'adresse IP du proxy dont vous vous servez. En fait, le proxy se connecte sur le serveur à votre place puis vous retransmet les données.

De plus les sites que vous allez visiter ne pourront installer des cookies sur votre ordinateur. En effet, ceux-ci seront installés sur le proxy.

Tout comme pour les **cookies**, le proxy faisant les requêtes en votre nom, intercepte les **applets** Java et JavaScripts/VBScripts ainsi que les ActiveX, mais aussi les bannières publicitaires. Ceci vous évite d'être identifié.

Il faut savoir que, comme votre fournisseur d'accès, le proxy enregistre votre passage, mais votre anonymat est garanti auprès des services que vous visitez, exceptés pour les accès FTP, les messageries en direct (ICQ, AOL...), ou encore les sites de "Webmail". (Ms-Hotmail)

Il peut être utile de se servir d'un proxy situé hors des frontières de votre pays. Vous pouvez aussi enchaîner plusieurs proxys pour brouiller encore plus les pistes, même si cela peut aussi ralentir votre connexion.

Certains sites ont une liste "noire", qu'ils mettent régulièrement à jour, d'adresses IP de proxys. Si l'adresse IP du proxy que vous utilisez est contenue dans la liste du site que vous voulez visiter, le site refusera la connexion. Mais vous pouvez toujours essayer avec un autre proxy.

Les sites comme Anonymizer.com ou SpaceProxy.com masquent votre navigation en utilisant des proxys. Ils permettent de saisir directement l'adresse du site qu'on désire visiter anonymement.

Voici un site pour trouver une liste de proxy :

http://www.multiproxy.org/all_list.htm

Ou encore, il est possible de s'inscrire à la liste proxy de e-groupes, pour recevoir une liste de proxys qui ont été testés, ainsi que des liens vous permettant de les tester. Pour l'abonnement à cette liste, envoyez un e-mail à l'adresse suivante :

proxies-subscribe@egroups.com

4.2.2. Les proxys gratuits

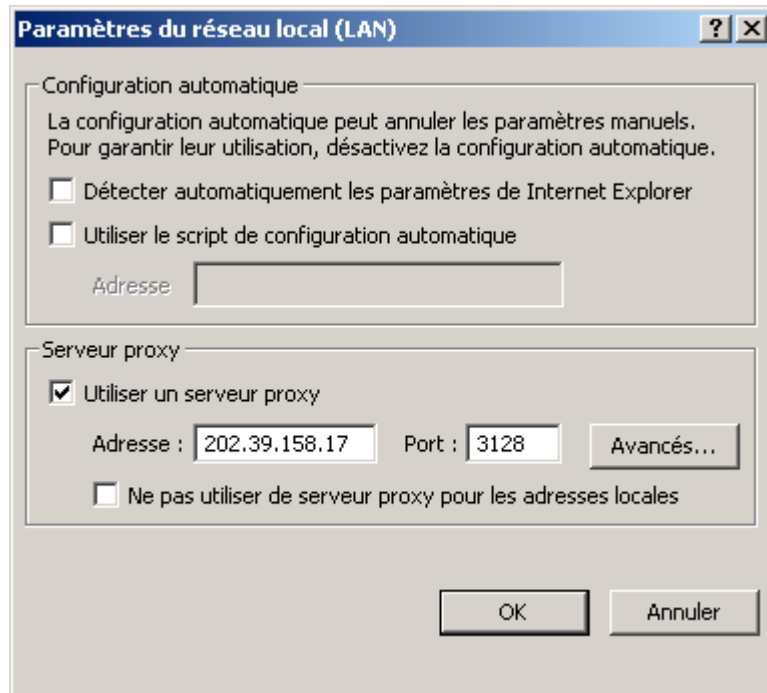
Pour utiliser la majorité de ces proxys anonymes et gratuits, il faut écrire une ligne de commande dans le navigateur.

Nous avons effectué un test, en entrant l'adresse IP d'un proxy anonyme directement sur "Internet Explorer 5".

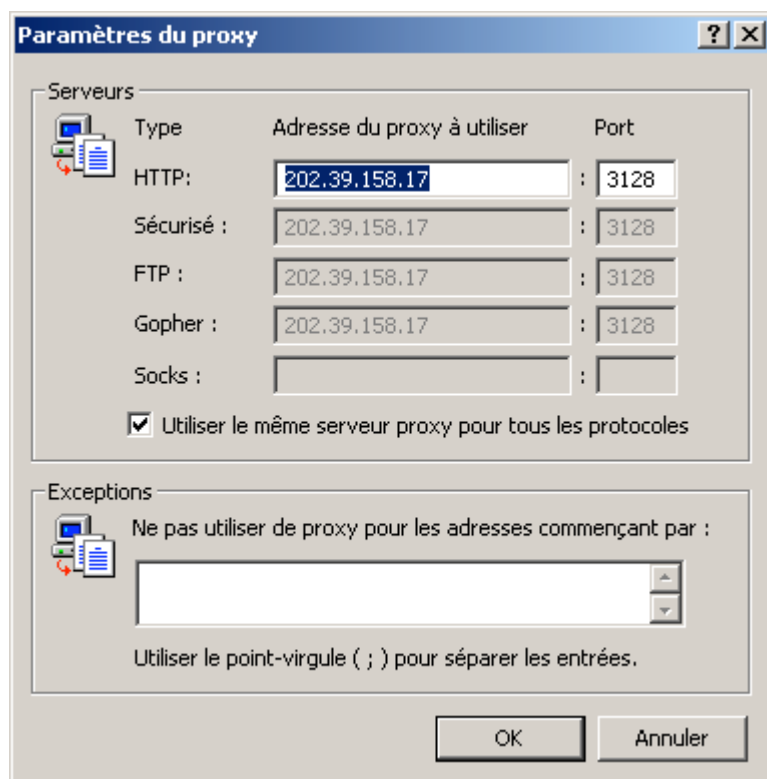
Lorsqu'on va chercher l'adresse du proxy sur un des sites (comme celui cité plus haut), voici comment l'information nous est fournie : 202.39.158.17:3128 de là on va pouvoir prendre l'adresse IP (les quatre premiers chiffres) puis les derniers représentent le numéro de port sur lequel on va se connecter.

Pour faire ce test, nous sommes tout d'abord allés dans le menu "Outils", puis dans le sous-menu "Options Internet" et avons cliqué dans l'onglet "Connexion", et ensuite cliqué sur le bouton "Paramètres LAN".

Ensuite, nous avons sélectionné l'option "Utiliser un serveur proxy" et introduit l'adresse IP du proxy ainsi que son numéro de port.



Pour que tous les protocoles passent par ce proxy, il faut cliquer sur le bouton "Avancés...", puis, dans la fenêtre qui apparaît, sélectionner l'option "Utiliser le même serveur proxy pour tous les protocoles".



Pour tester si notre IP anonymat était bien réel, nous sommes allés sur le site www.cnil.fr qui nous donne les paramètres qu'il obtient de notre connexion sur leur site.

Sur l'image ci-dessous, nous voyons que l'adresse IP n'est pas une adresse IP de EIVD (193.134.216.2). Mais plutôt, l'adresse IP du proxy que nous avons utilisé. De plus, l'adresse DNS n'y est pas. Le site ne sait pas qui nous sommes.

Votre configuration

Saviez vous que **l'adresse IP** de votre machine est : 202.39.158.17
et que votre **adresse DNS** est :

Nous pouvons voir que votre ordinateur utilise : Microsoft Windows NT
comme **système d'exploitation**.

Votre navigateur a comme nom de code : Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0) via NetCache version 3.1.2c-Solaris
mais c'est en fait : Microsoft Internet Explorer 5.01 .

Pour accéder à cette page, vous avez cliqué sur un lien situé à l'adresse suivante :
<http://www.cnil.fr/traces/demonst/demo.htm>

Cette page montre comment le serveur peut exploiter les variables d'environnement de votre navigateur.

Voici ce que nous affiche le site si on se connecte sans utiliser un proxy anonyme :

Votre configuration

Saviez vous que **l'adresse IP** de votre machine est : 193.134.216.2
et que votre **adresse DNS** est : pub1.eivd.ch

Nous pouvons voir que votre ordinateur utilise : Microsoft Windows NT
comme **système d'exploitation**.

Votre navigateur a comme nom de code : Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
mais c'est en fait : Microsoft Internet Explorer 5.01 .

Pour accéder à cette page, vous avez cliqué sur un lien situé à l'adresse suivante :
<http://www.cnil.fr/traces/demonst/demo.htm>

Cette page montre comment le serveur peut exploiter les variables d'environnement de votre navigateur.

Pour finaliser notre test, nous avons envoyé un mail depuis une adresse bidon créée par nos soins sur un fournisseur d'e-mails gratuits, en l'occurrence www.caramail.com, et nous avons visualisé l'entête de l'e-mail reçu. Voir l'image ci-dessous :



Entête d' e-mail anonyme reçu

Nous constatons que l'adresse IP est bien celle du proxy et non pas celle de l'EIVD. Le test est donc concluant. Nous avons pu envoyer un mail anonymement.

Mais l'idéal serait de chaîner plusieurs proxys, si possible localisés dans des pays différents. Il serait ainsi quasiment impossible de remonter jusqu'à l'utilisateur. L'utilité d'enchaîner les proxys se ressent lorsqu'on sait que le proxy stocke des informations liées à votre passage.

Un exemple d'enchaînement de proxy :

- Inscrire directement dans les paramètres de votre navigateur Internet quel proxy anonyme vous voulez utiliser en premier lieu (voir explication plus bas).
- Se connecter sur un site utilisant, lui-même, un proxy anonyme (exemple : Anonymizer.com ou SpaceProxy.com).
- Depuis ce site aller sur un autre site du même type. Et ainsi de suite.
- Une fois que vous pensez avoir assez de proxys, allez sur le site sur lequel vous voulez naviguer anonymement.

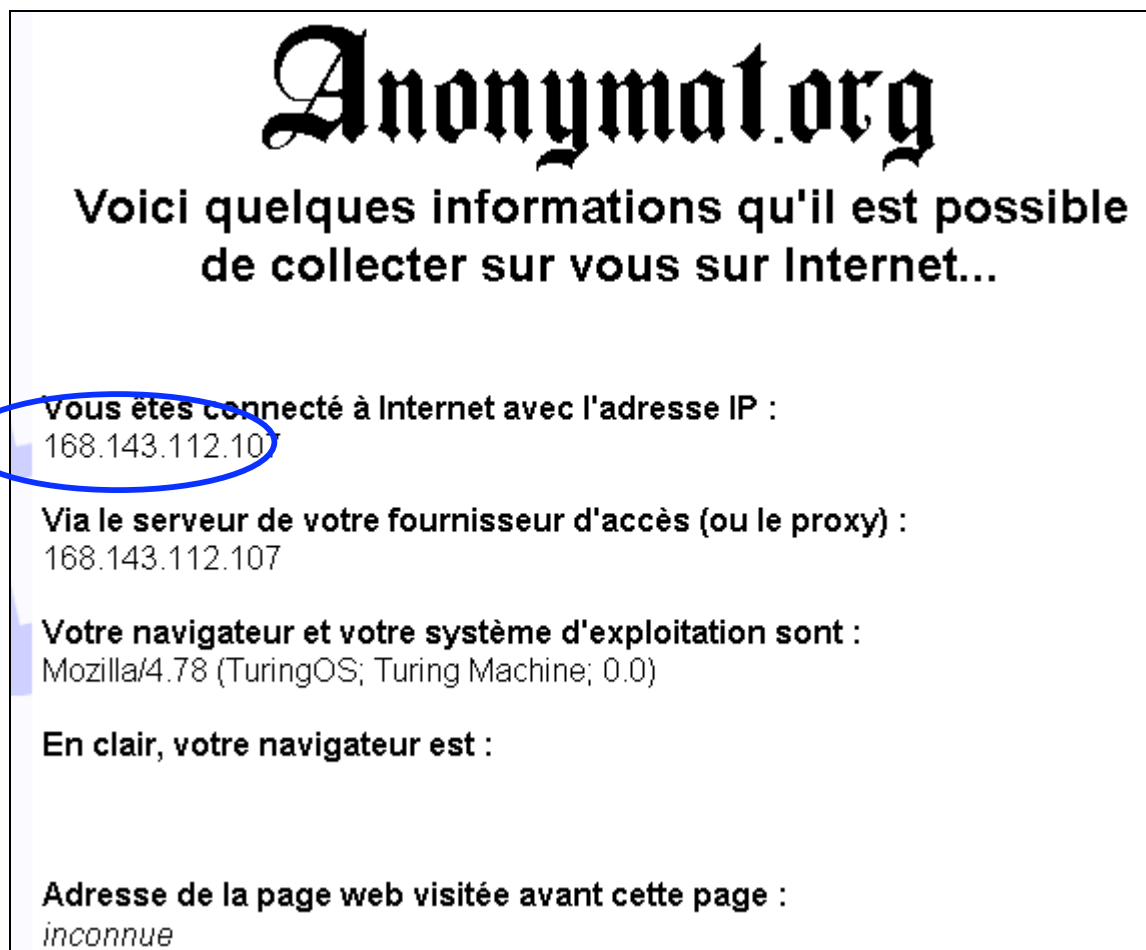
Il faut tenir compte du fait que plus il y a de proxys entre vous et le destinataire final, plus le transfert de données sera long.

Dans cet exemple, nous avons voulu faire une démonstration du chaînage de proxys.

Toujours en étant connecté sur le proxy de l'exemple précédant, nous sommes allés sur le site <http://www.anonymizer.com> qui nous permet de naviguer anonymement et de plus gratuitement. Pour cela, il suffit de saisir l'URL du site sur lequel nous voulons naviguer dans la case prévue à cet effet.

Pour contrôler si l'adresse IP est bien cachée, nous avons saisi l'adresse de la page www.anonymat.org/vostraces/index.htm. Cette dernière nous indique quelles sont les informations que le serveur a pu tirer de notre visite.

Sur l'image qui suit, nous voyons ces informations, et nous constatons que l'adresse IP indiquée par la page Web n'est ni celle de l'EIVD, ni celle du proxy que nous avons introduit dans notre navigateur. En effet, cette adresse IP est celle du proxy qu'utilise le site Anonymizer.com.



Anonymat.org

Voici quelques informations qu'il est possible de collecter sur vous sur Internet...

Vous êtes connecté à Internet avec l'adresse IP :
168.143.112.10

Via le serveur de votre fournisseur d'accès (ou le proxy) :
168.143.112.107

Votre navigateur et votre système d'exploitation sont :
Mozilla/4.78 (TuringOS; Turing Machine; 0.0)

En clair, votre navigateur est :

Adresse de la page web visitée avant cette page :
inconnue

La recherche sur l'annuaire WHOIS nous informe que l'adresse IP de notre premier proxy (premier exemple sur les proxys), à savoir 202.39.158.17, appartient à l'entreprise suivante :

CHTD, Chunghwa Telecom Co.,Ltd.
Data-Bldg.6F, No.21, Sec.21, Hsin-Yi Rd.
Taipei Taiwan 100
country: TW

Et celle de notre deuxième exemple, à savoir 168.143.112.107, à l'entreprise :

Verio, Inc. (NET-VRIO-168-143)
8005 South Chester Street
Englewood, CO 80112
US

Donc, nous nous connectons via un proxy situé à Taiwan, puis depuis ce dernier à un proxy situé aux US. Pour finir sur le site anonymat.org qui, selon l'annuaire WHOIS, l'entreprise se trouve en France. Mais si on fait un trace route, on obtient l'IP 128.242.232.233 qui appartient à l'entreprise Verio, dont nous avons les coordonnées plus haut.

Nous avons contrôlé tout cela avec le logiciel NeoTrace et nous obtenons les mêmes résultats. Cela nous confirme que le domaine de Anonimat.org se trouve sur un serveur appartenant à Verio, localisé aux Etats-Unis, mais que le propriétaire du domaine en question est une entreprise basée en France. Un exemple flagrant du fait qu'une entreprise basée dans le pays X peut très bien avoir un domaine sur un serveur situé dans un pays Y.

De plus, nous avons constaté un ralentissement assez important du transfert des données.

4.2.3. Les Tunnels

Malgré l'utilisation des proxys, l'anonymat n'est que relatif. En effet, les fournisseurs d'accès Internet peuvent très bien intercepter et analyser les données transitant entre l'ordinateur de l'internaute et le proxy utilisé.

Un moyen d'éviter cela, est la création d'un tunnel. Un tunnel est une liaison cryptée entre le proxy et l'ordinateur. En fait, vos données seront cryptées par vos soins, puis décryptées par le proxy via lequel vous êtes connectés.

Pour ce faire, il faut vous connecter sur un proxy acceptant le cryptage et le décryptage des vos données. Ces proxys sont en règle générale payants.

De plus, pour le cryptage, tout comme pour le décryptage, il faut se procurer un logiciel qui doit être le même que celui utilisé par le proxy.

De plus, le camouflage de l'adresse IP est aussi garantie.

4.3. Utilisation de site pour envoyer des e-mails.

4.3.1. Les Remailers anonymes

Si vous souhaitez envoyer des e-mails de façon anonyme (sans divulguer votre identité au destinataire), on utilise des Remailers, car si vous pensiez modifier votre adresse e-mail dans le navigateur, l'entête du message comporte de nombreuses informations dont votre adresse IP.

De plus votre fournisseur d'accès Internet (FAI) peut lire votre courrier. Il convient donc, pour une plus grande confidentialité, en plus de cacher votre IP, de crypter vos messages entrant et sortant.

La procédure à suivre est d'indiquer au Remailer l'adresse de votre correspondant qui peut être un autre Remailer, vous pouvez les chaîner, de plus nous vous le conseillons car :

- Le dernier Remailer de la chaîne ne saura pas d'où vient le message.
- En cas de contrôle par les services de police, il suffit que l'un d'entre eux ne soit pas contrôlé pour que votre message soit confidentiel.

La réception anonyme de courriers électroniques est finalement plus problématique car les Remailers ne le permettent pas pour les messageries gratuites, malgré le fait de pouvoir entrer de fausses informations nominatives, Ils offrent très peu de possibilités d'anonymat du fait qu'ils mémorisent souvent votre adresse IP ou qu'ils vous obligent à accepter un cookies.

Il existe aussi d'autres types de Remailers, les cypherpunks et les mixmasters qui proposent d'autres propriétés de masquage de votre identité et aussi différents niveaux de sécurité lors de l'envoi des paquets.

Mise en garde :

Les Remailers anonymes sont des services totalement gratuits mis à la disposition des internautes par quelques pionniers qui se battent pour le respect de l'anonymat et de la vie privée. Une démarche à soutenir, donc. Cela dit, on commence à voir apparaître des serveurs commerciaux qui proposent un anonymat tarifé (et assez cher): à éviter.

Vérifiez bien que votre connexion est sécurisée (dans la mesure du possible) avant de composer et d'envoyer votre message. Si vous ne prenez pas de précautions, votre message et l'adresse de son destinataire seront envoyés "en clair" vers le Remailer, permettant à quelqu'un qui aurait intercepté votre communication d'en connaître le contenu. En vue d'éviter cela, vérifiez bien que votre browser supporte le cryptage SSL à 128 bit SSL et que vous êtes connecté à un Remailer qui utilise une connexion HTTPS.

Voici quelques liens :

<http://www.business2.com/webguide/0,,23901,00.html>

<https://freedom.gmsociety.org/remailer/mixmaster.html>

4.3.2. Les serveurs de pseudonyme

Sans avoir trop approfondi les Remailers, les serveurs de pseudonymes (Nymserver) sont plus efficaces car ceux-ci utilisent une chaîne de Remailers cryptés permettant virtuellement de rendre impossible la traçabilité des e-mails. Même l'opérateur du remailer ne peut découvrir votre véritable identité. De plus, et contrairement aux Remailers classiques, vous pouvez également recevoir des e-mails.

Les Nymserver vous permettent de créer une adresse e-mail permanente qui vous permet d'envoyer à votre véritable adresse les mails que l'on vous envoie via une chaîne de Remailers qui re cryptent à chaque fois le message. Utilisé proprement, il est quasiment impossible de pouvoir le suivre à la trace.

Pour pouvoir utiliser ces services, vous devez envoyer un e-mail vide au Nymserver de votre choix (`liste@nymserverDeVotreChoix`), vous recevrez en retour une liste des noms déjà utilisés sur ce Nymserver.

Il existe actuellement 3 Nymserver :

- `nym.alias.net`
- `redneck.gacracker.org`
- `anon.xg.nu`

Recevoir un message sur un compte nym peut prendre plusieurs heures contrairement à un envoi classique, mais c'est le prix à payer pour être anonyme sur le net avec un compte nym.

5. Conclusion

Le but de départ de ce mini-projet était de trouver des méthodes pour identifier un utilisateur du réseaux Internet via son adresse IP. La tâche était, dès lors, ardue quand on sait que les adresses IP sont attribuées arbitrairement et, qui plus est, changent à chaque connexion à son provider pour la majeure partie des internautes. De plus, si on accède à Internet depuis un cybercafé et qu'il est possible de spécifier l'utilisation d'un proxy sur le navigateur fourni, la trace de notre passage sur le Web est d'autant plus invisible.

Nos multiples recherches nous ont montré que les traces de l'utilisateur s'arrêtent sur le provider (fournisseur d'accès Internet) ou sur le serveur d'une grande organisation (siemens, EIVD...). Pour en savoir plus, autrement dit pour connaître l'identité de l'utilisateur, il faut avoir accès aux données du serveur qui garde les informations concernant votre passage. Malheureusement, ces informations sont confidentielles et les seuls qui peuvent y avoir accès sont les autorités compétentes.

Ceci étant, notre projet a pris une autre voie, à savoir : Comment surfer caché ?

Plusieurs méthodes et logiciels sont disponible, mais seul un petit nombre de ceux-ci ont apporté des résultats concluants.

Nos exemples d'utilisation de proxys, montre que les sites que nous visitons n'ont plus la possibilité de connaître notre adresse IP. Mais le ralentissement du transfert des données devient très important à cause du parcours des paquets qui est ainsi considérablement prolongé.

Les Remailers permettent l'envoi d' e-mails depuis une simple page Web. Ainsi le récepteur, de l'e-mail, ne peut voir l'adresse IP de l'expéditeur. De plus, certains de ces sites supportent le cryptage. Ce qui permet de créer un tunnel, qui évite que le contenu des paquets échangés ne puisse être connu par votre provider. Idem pour les autres serveurs à travers lesquels vos paquets transitent.

Les Nymserver offrent les mêmes services, à la différence que ceux-ci permettent la réception des messages en retour. En fait, un compte d'e-mail, proche de ceux proposés sur Caramail.com ou Hotmail.com, est créé. Mais, contrairement à ces derniers, votre adresse IP n'est pas jointe à l'e-mail, c'est l'adresse IP du serveur qui est utilisée. Ces serveurs supportent aussi le cryptage des données.

Malheureusement, les tests que nous avons effectués n'ont pas été concluants.

Finalement, l'anonymat sur Internet est plus que facilité. Même s'il n'est pas possible d'être cent pour cent anonyme. Et donc, la recherche d'un internaute qui ne veut en aucun cas qu'on le retrouve s'avère très difficile.

Par contre, si le but est l'envoi d'e-mails anonymes et que l'on veut simplement que le récepteur ne connaisse pas notre identité, la plus simple des méthodes est de spécifier à votre navigateur Internet préféré par quel proxy anonyme vous voulez transiter.