الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي

Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة

Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا

Faculté de Technologie

قسم الإلكترونيك

Département d'Électronique

Mémoire de Master

Filière Télécommunication

Spécialité Réseaux & Télécommunications

Présenté par

BENGAYOU Djaouida

DJEGHAB Meriem

Mise en place d'une solution de détection des réseaux anonymes

Proposé par notre promoteur : Mr. MEHDI Merouane

Et notre co-promotrice : Mme. AMALOU Warda

Année Universitaire 2021-2022

Remerciements

Nous souhaiterions commencer par exprimer notre gratitude et reconnaissance envers toute personne ayant participé à la progression et l'amélioration de notre mémoire. En commençant par notre très cher encadreur, monsieur MEHDI Merouane ainsi que notre co-promotrice madame AMALOU Warda.

Ces enseignants qui nous ont tant appris et soutenus. Leurs confiances en nous, leurs conseils ainsi que leurs remarques nous ont extrêmement aidés à avancer, tout en s'améliorant et en faisant ressortir le meilleur de nous-même.

Nos deuxièmes remerciements sont dédiés aux membres du jury, qui ont acceptés d'évaluer notre mémoire et d'être présent lors d'une des journées les plus marquantes de notre parcours scolaire.

Sans oublier nos parents, qui sans leurs aides, nous ne serions jamais arrivées là.

ملخص :

استخدام الموظفين لشبكات مجهولة المصدر مثل Tor و I2P للتحايل على القيود التي تفرضها شركتهم يعرض أمن الشركة للخطر. ولمعالجة ذلك ، فإن اكتشافهم ضروري من أجل استخدام التدابير الوقائية الصحيحة. نتيجة لذلك ، تم إجراء تحليل لحركة مرور Tor و I2P في هذه الأطروحة ، وتم الكشف عن بصمات رقمية خاصة بكل شبكة واستخدامها في إنشاء القواعد التي سيتم تنفيذها في اثنين من IDS المختارة ، Suricata و Snort ، والتي كانت قادرة على لتحقيق الحل المقترح مسبقًا بمعدل كشف 73.83٪ لـ Suricata و 86.01٪ لـ Snort.

الكلمات المفتاحية: Anonymat, Tor, I2P, DPI, détection, Suricata, Snort.

Résumé : L'utilisation des réseaux anonymes tels Tor et I2P par les employés afin de contourner des restrictions imposées par leur entreprise compromet la sécurité de cette dernière. Pour remédier à cela, leur détection est nécessaire afin d'employer les bonnes démarches de prévention. De ce fait, une analyse du trafic de Tor et I2P a été faite dans ce projet, des empreintes numériques propre à chaque réseau ont été révélées et utilisées dans l'établissement de règles à implémenter dans deux IDS choisi, Suricata et Snort, qui ont pu réaliser la solution proposée précédemment avec un taux de détection de 73,83% pour Suricata et 86,01% pour Snort.

Mots clés : Anonymat, Tor, I2P, DPI, détection, Suricata, Snort.

Abstract: The use of anonymous networks such as Tor and I2P by employees to circumvent restrictions imposed by their company compromises its security. As a solution, their detection is necessary in order to employ the right prevention measures. For that, an analysis of Tor and I2P's traffic has been made in this thesis, each network's specific digital fingerprints have been revealed and used in the establishment of rules that were implemented in two chosen IDSs, Suricata and Snort, that were able to achieve the previous proposed solution with a detection rate of 73.83% for Suricata and 86,01% for Snort.

Keywords: Anonymity, Tor, I2P, DPI, détection, Suricata, Snort.

Listes des acronymes et abréviations

A
ACK : Acknowledgement.
ACL : Access Control List.
AES : Advanced Encryption Standard.

C
CPU : Central Processing Unit.

D
DSA : Digital Signature Algorithm.
DOS : Denial Of Service.
DDOS : Distributed Denial Of Service.
DSL : Digital Subscriber Line.
DNS : Domain Name System.

F
FAI : Fournisseur Accès Internet.
FTP : File Transfer Protocol.
FIN : Finish.

H
HTML : HyperText Markup Language.
HTTP : HyperText Transfer Protocol.
HTTPS : HyperText Transfer Protocol Secure.
HTTPMU : HTTP over Multicast/UDP.

I
IANA : Internet Assigned Numbers Authority.
IP : Internet Protocol.
IETF : Internet Engineering Task Force.
IANA : Internet Assigned Numbers Authority.
IPv4 : Internet Protocol version 4.
I2P : Invisible Internet Project.
IDS : Intrusion Detection System.
IPS : Intrusion Prevention System.
I2CP : I2P Client Protocol.
ICMP : Internet Control Message Protocol.

L
LAN : Local Area Network.
SSDP : Simple Service Discovery Protocol.
SSU : Secure Semireliable UDP

M
MSS : Maximum Segment Size.
Mbps : Mégabit Par Seconde.
MCAS : Microsoft Cloud App Security.

MAC : Media Access Control.
MiTM : Man-in-the-Middle.

N
NAT : Network Address Translation.
NetDB : Network Tracking Database.
NTP : Network Time Protocol.
NTCP : NIO-based TCP.
NSM : Network Security Monitor.
NIDS : Network-based Intrusion Detection System.
NSM : Network Security Monitoring.

O
OS : Operating System.

P
PC : Personal Computer.
PSH : PUSH.
PCAP : Packet Capture.

R
RAM : Random Access Memory.
RTT : Round Trip Time.

S
SMTP : Simple Mail Transfer Protocol.
SSL : Secure Socket Layer.
SHA : Secure Hash Algorithm.
SYN : Synchronisation.

T
TCP : Transmission Control Protocol.
TTL : Time To live.
TLS : Transport Layer Security.
TOR : The Onion Router.

U
USB : Universal Serial Bus.
UDP : User Datagram Protocol.
URL : Uniform Resource Locator.

V
VPN : Virtual Private Network.

Table des matières

Chapitre 2 : Les vulnérabilités du réseau anonyme

Chapitre 3 : Extraction des signatures numériques

Liste des figures

Chapitre 1 : Les réseaux anonymes « Anonymat et vie privée sur internet »

Chapitre 2 : Les vulnérabilités du réseau anonyme

Chapitre 3 : Extraction des signatures numérique

Chapitre 4 : Implémentation des règles dans deux IDS

Liste des tableaux

Chapitre 1 : Les réseaux anonymes « Anonymat et vie privée sur Internet »

Chapitre 2 : Les vulnérabilités du réseau anonyme

Chapitre 3 : Extraction des signatures numériques

Chapitre 4 : Implémentation des règles dans deux IDS

Introduction générale

Le souhait des internautes d'être anonyme sur Internet grandi amplement. Certains désirent l'être afin d'être libre d'exprimer leurs points de vue réels sans avoir peur d'être jugés ou critiqués par quiconque. D'autres prétendent que c'est par simple mesures de protections de leurs identités virtuelles ainsi que de leurs vies privées sur la toile. Pour ce qui est des utilisateurs malveillants c'est pour attaquer et élaborer des actes illégitimes sans être identifié par les autorités.

Les arguments sont divers, mais la méthode est constamment la même. Ils se dirigent pour la plupart vers l'anonymisation à travers les réseaux anonyme dont Tor et I2P. Tor crée un chemin sécurisé vers Internet et I2P crée son propre Internet avec une connexion Internet sécurisé pour ses usagers. Leur utilisateurs se sentent probablement en sécurité et pensent qu'en aucun cas, leur identité ne sera révélée. Mais est-ce vraiment la réalité ?

Les entreprises bloquent ou limitent l'accès à certains sites ou fonctionnalités d'Internet au sein de leur établissement à leurs employés, cette pratique n'a pas pour but seulement de s'assurer qu'ils ne soient pas distraits pendant les heures de travail, mais aussi pour limiter les risques d'intrusion. Même si une entreprise établit une politique de sécurité informatique, protège ses appareils avec des mots de passe compliqués ou sensibilise ses employés aux cyberattaques, elle ne sera jamais sécurisée complétement.

En mai 2021, l'assurance AXA a été victime d'une cyberattaque dite « rançongiciel », les pirates ont exigé de l'entreprise de payer une rançon car ils ont pris en otage des données personnelles des clients telles que des passeports, des cartes d'identité et des informations de comptes bancaires [1].

L'utilisation de Tor et I2P afin de contourner les restrictions informatiques de leurs entreprises n'est pas sans conséquence non plus, mais augmente la vulnérabilité de cette dernière face aux attaques informatiques. C'est pour cela qu'il est impératif pour la sécurité d'une entreprise de détecter l'utilisation des réseaux anonymes afin de les bloquer.

Ce projet va se focaliser sur l'étude des deux réseaux anonymes les plus populaires Tor et I2P et leur détection dans un réseau d'entreprise. Les étapes à suivre sont comme suit :

La première étape : Consacrée à la présentation des différents termes utiles pour la compréhension de ce sujet, l'explication de l'anonymat sera abordée.

La deuxième étape : Etude théorique approfondie du réseau de Tor et I2P en détail.

La troisième étape : Analyse des paquets par la méthode DPI afin de déduire des signatures numériques propres à Tor et I2P, qui permettront la création des règles de détection de ces derniers.

L'implémentation de ces règles dans un système de détection d'intrusion aura pour but de détecter puis bloquer les données venant de Tor ou I2P en vue de protéger son réseau interne de toute fuite de données ou attaque de pirate à travers ces derniers.

Chapitre 1

Les réseaux anonymes « Anonymat et vie privée sur Internet »

1.1 Introduction

Internet est un ensemble de réseaux mondiaux interconnectés. Afin d'accéder à ses différentes applications, la navigation se fait au niveau du Web, un service d'Internet qui permet de consulter des pages accessibles sur des sites.

Cependant, Internet représente un grand enjeu aussi, et cela concerne l'anonymat et la vie privée des internautes. Les traces laissées par les individus lors de leurs navigations peuvent présenter de graves dangers s'ils tombent entre de mauvaises mains. Raison pour laquelle beaucoup d'internautes se dirigent vers l'utilisation des outils d'anonymat qui, en plus d'une protection, ils leur permettent d'avoir accès à tout ce qui est restreint.

Les applications et outils garantissant l'anonymat sont autant nombreux que variés, et peuvent être utilisés à des fins positives ou négatives. Car oui, même si l'anonymat est un droit qui, de principe, doit être utilisé de façon légale pour se protéger, beaucoup de personnes malveillantes en profitent pour agresser, voler et lancer des attaques sans être détectées. Parmi ces outils, on nomme : le VPN, les réseaux anonymes tels Tor, I2P, Freenet, etc.

1.2 Le Web

Le Web, ou le World Wide Web est un sous-ensemble d'internet constitué de pages accessibles par un navigateur Web, pour visualiser et partager des informations tels que les textes, images, musiques et vidéos.

Les pages Web sont formatées dans un langage appelé HyperText Markup Language ou HTML, qui permet aux utilisateurs d'accéder à des pages via des liens. Le protocole utilisé est le HTTP, pour transmettre les données et partager les informations.

Pour accéder aux pages Web, des navigateurs tels qu'Internet Explorer, Mozilla Firefox et Google Chrome, sont utilisés. Google par exemple gère plus de 40000 recherches par secondes et détient 60% du marché mondial des navigateurs via Chrome [2].

1.3 Le Fonctionnement d'internet

1.3.1 Introduction

Internet fonctionne en utilisant un réseau de routage de paquets. Les données transférées à son niveau sont livrées sous forme de messages et de paquets qui voyagent d'une source à une autre en utilisant le protocole Internet « IP » et le protocole de contrôle de transport « TCP ». Ils permettent de s'assurer qu'aucun paquet n'est perdu, que les paquets soient réassemblés dans le bon ordre et qu'aucun délai n'affecte négativement la qualité des données [3].

1.3.2 Le protocole IP

Internet Protocol « IP » est un protocole dont le rôle est l'adressage et la segmentation des paquets de données dans les réseaux numériques.

Associé du protocole « Transmission Control Protocol » ou TCP, ils composent la base de l'Internet. Afin de faire passer un paquet d'un émetteur à un récepteur, le protocole IP définit une disposition de paquets donnant un aperçu des informations envoyées. Il est responsable de la façon dont les informations sur la source et la destination des données sont représentés et divise ces informations des données informatives dans son en-tête [4].

Le protocole IP détermine le destinataire du message grâce à 3 champs :

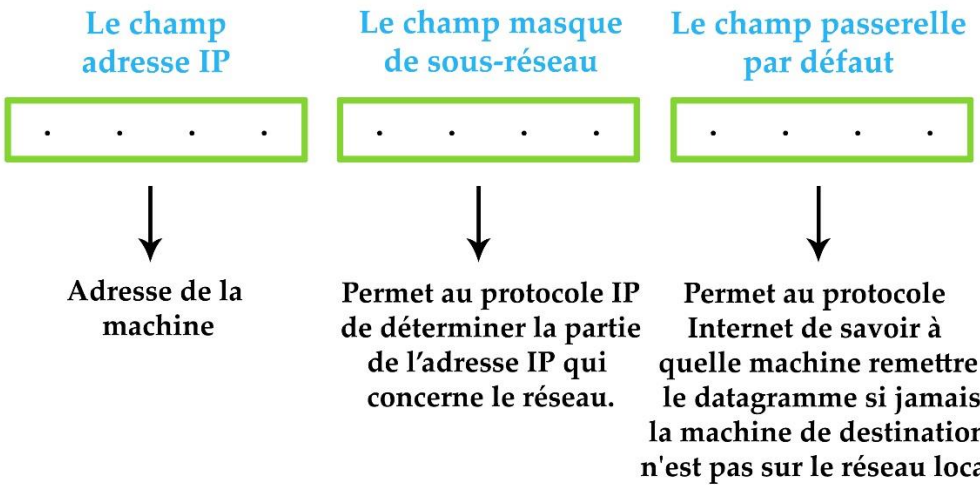


Figure 1.3.1 : *Les champs du protocole IP.*

1.3.2.1 Adresses Publiques :

Les adresses IP publiques sont des adresses globales et uniques utilisées sur des hôtes qui doivent être accessibles au public depuis internet.

L'IANA (Internet Assigned Numbers Authority) est l'organisme qui gère les adresses IP publiques et qui s'assure de l'absence de doublon. Le fournisseur d'accès à internet procure les adresses publiques et les blocs d'adresses [5].

Au total, il existe 5 classes d'adresse IP : A, B, C, D et E adaptées selon la taille du réseau.

Classe	Adresses
A	0.0.0.1 à 126.255.255.254
B	128.0.0.1 à 191.255.255.254
C	192.0.0.1 à 223.255.255.254
D	224.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

Tableau 1.3.1: *Plages d'adresses [6].*

1.3.2.2 Adresses Privées :

Les adresses IP privées sont les adresses de classe A, B et C que l'on peut utiliser dans un réseau local (LAN) tels que dans une entreprise ou dans un réseau domestique. Les hôtes privés qui ne sont pas connectés à internet peuvent utiliser n'importe qu'elle adresse privée valide tant qu'elle est unique dans le réseau interne.

Les routeurs internet sont tous configurés pour éliminer toutes les adresses privées. C'est à dire quelles ne sont pas routables sur internet. Lorsqu'un réseau utilisant des adresses privées veut se connecter à Internet, il a recours à la translation des adresses privées en adresses publiques grâce à la méthode du NAT (Network Address Translation) [5].

Les adresses IP privées se trouvent dans les classes A, B et C comme ceci :

Classe	Adresses
A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255
C	192.168.0.0 à 192.168.255.255

Tableau 1.3.2: *Plages d'adresses privées [6].*

1.3.2.3 Passerelle:

La passerelle est une interface qui permet de relier des réseaux de types différents et ainsi de transférer les informations entre eux. Elle traduit l'information reçue de façon à ce que le réseau destinataire puisse la comprendre.

Le NAT (Network Address Translation), processus de modification d'adresses IP utilise qu'une seule adresse publique celle de la passerelle pour communiquer avec Internet. Cette passerelle peut être un routeur ou un firewall, elle possède deux interfaces, une interface réseau connectée au réseau interne avec une adresse IP privée pour communiquer avec le réseau interne et une interface réseau connectée à internet avec une adresse IP publique utilisable sur internet pour communiquer avec internet [7].

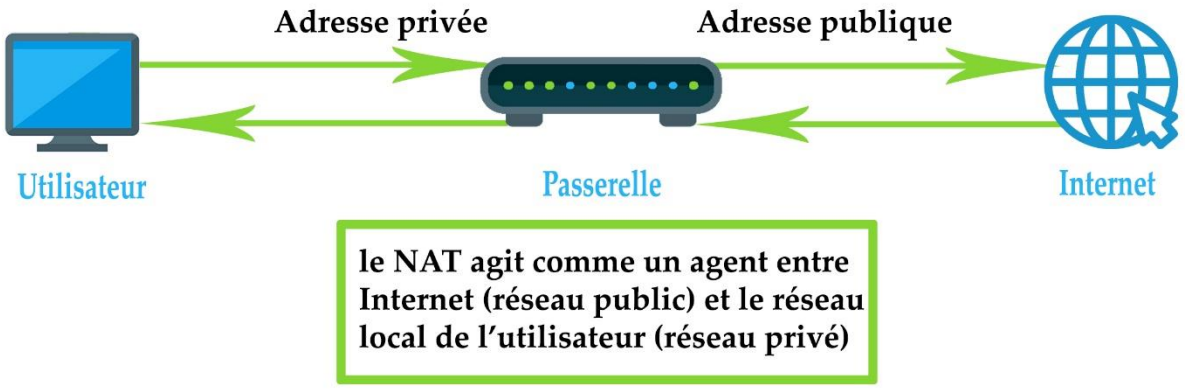


Figure 1.3.2 : *Passerelle et NAT.*

1.3.3 Le protocole TCP

Le TCP où « Transmission Control Protocol » en Anglais, est un protocole de la couche de transport du modèle TCP/IP. Son trafic est reçu à la même disposition que celui envoyé, il est donc orienté connexion.

Les caractéristiques principales du protocole TCP sont les suivantes [4] :

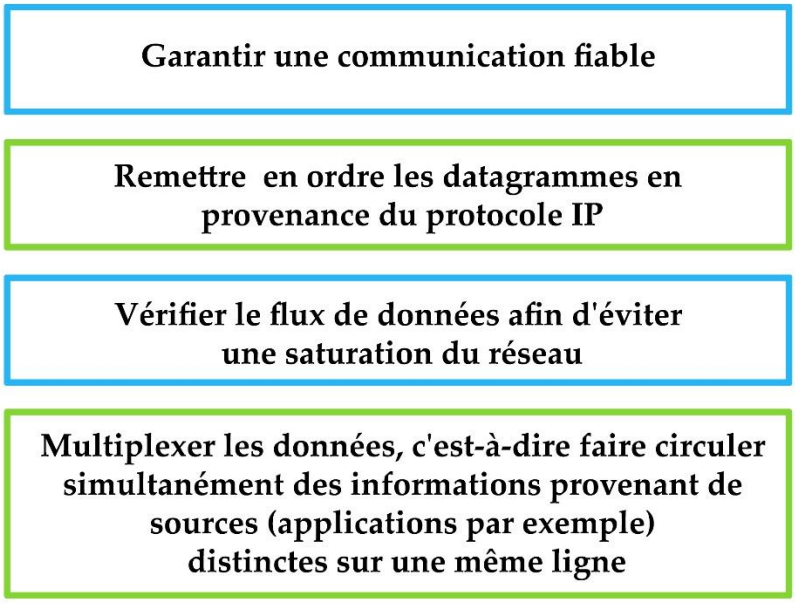


Figure 1.3.3 : *Les caractéristiques principales du protocole TCP.*

1.3.4 Le DNS

Le « Domain Name System » ou DNS est un service qui permet de faire la concordance entre les noms de domaines et les adresses IP qui leurs sont accordées. Cela rend possible la recherche à l'aide des mots et noms familiers au lieu d'une chaîne de chiffres dans un navigateur.

Lorsqu'on effectue une recherche d'un nom de domaine dans un navigateur, une requête est envoyée sur Internet pour associer le domaine avec son adresse IP correspondante. Une fois repéré, l'adresse IP est utilisée pour avoir le contenu du site web. Cette opération ne dure que quelques millisecondes.

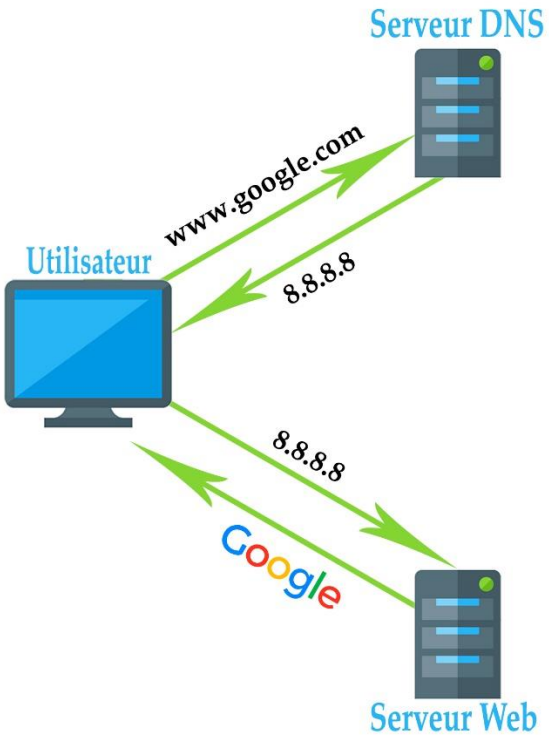


Figure 1.3.4 : *Fonctionnement du DNS.*

Ce protocole est aussi constamment assimilé à la version Internet de l'annuaire téléphonique, où pour effectuer un appel, un numéro de téléphone est nécessaire. Il faut donc chercher le nom du contact [8].

1.3.5 L'adresse URL

Une adresse URL (Uniform Resource Locator) présente l'identité d'une page ou un site sur internet, chaque URL est donc unique dans le monde.

En entrant l'adresse URL d'une page Web dans le navigateur, l'internaute lance une requête HTTP auprès d'un serveur qui se charge de chercher, trouver et envoyer le résultat correspondant à cette page.

L'adresse URL se présente sous la forme : protocole://nom du domaine/répertoire/document

- **Le protocole http://**

Le HyperText Transfer Protocol est un protocole basé sur l'échange de messages entre un client et un serveur web.

Processus de communication http :

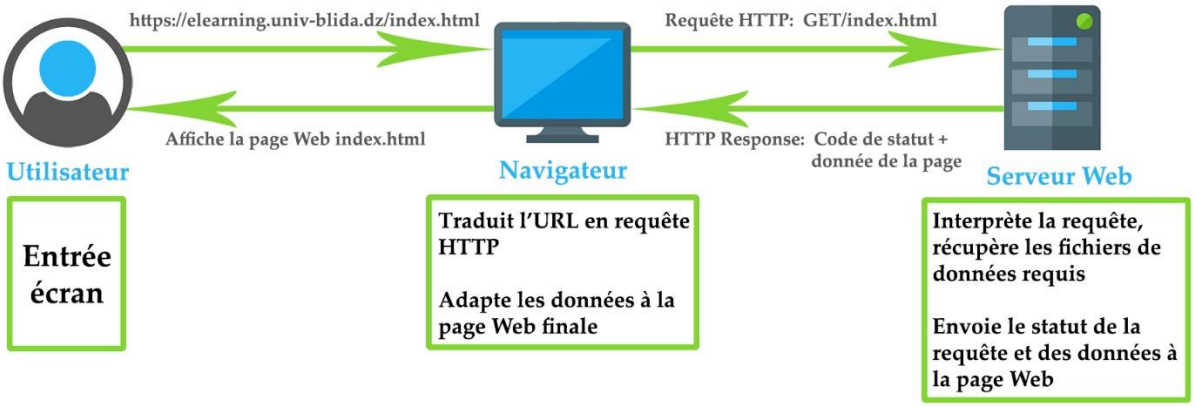


Figure 1.3.5 : *Le processus de communication http.*

- **Le nom de domaine**

Ce nom est constitué de plusieurs domaines séparés par un point. On prend l'exemple de « www.google.fr/ » où :

www : Correspond au domaine du troisième niveau (World Wide Web).

google : Correspond au domaine du deuxième niveau, qui est le nom du site.

fr : Correspond au domaine du premier niveau, appelé aussi « extension du nom du domaine ». Peut être remplacé par :

- com pour commerce.
- Edu pour éducation
- gov pour gouvernement
- int pour institution internationale
- mil pour militaire
- net pour organisme travaillant sur les réseaux
- org pour organismes divers

- **Le chemin complet répertoire/document**

C'est le nom du fichier appelé, précédé de son chemin sur le disque dur du serveur. Il s'agit ici du fichier « document » situé dans le « répertoire » [9].

1.3.6 L’accès à internet

Lors de saisi d’une adresse Web dans un navigateur :

- Le PC ou l’appareil est connecté au Web via un modem ou un routeur. Ensemble, ces appareils permettent de se connecter à d'autres réseaux nationaux et internationaux. Le routeur permet à plusieurs ordinateurs de rejoindre le même réseau tandis qu'un modem se connecte au FAI « fournisseur d'accès Internet » qui fournit un accès Internet par câble ou DSL.
- Une adresse Web est saisie, connue aussi sous le nom d'URL « Uniform Resource Locator ». Chaque site Web a sa propre URL unique qui indique à l’FAI ou aller.
- La requête est transmise à l’FAI qui se connecte à plusieurs serveurs qui stockent et envoient les données, comme le serveur DNS « Domain Name Server ». Ensuite, le navigateur recherche l'adresse IP du nom de domaine tapé dans le moteur de recherche via le DNS, qui traduit ensuite le nom de domaine textuel saisi dans le navigateur en adresse IP numérique (Exemple: Google.com devient 64.213.85.5)
- Le navigateur envoie une requête HTTP « HyperText Transfer Protocol » au serveur cible pour envoyer une copie du site Web au client via TCP/IP.
- Le serveur approuve ensuite la demande et envoie un message d’accord à l’ordinateur. Le serveur envoie par la suite les fichiers du site Web au navigateur sous forme de paquets de données.
- Au fur et à mesure que le navigateur rassemble les paquets de données, le site Web se charge, permettant ainsi aux internautes de profiter des résultats de leurs recherches. [10].

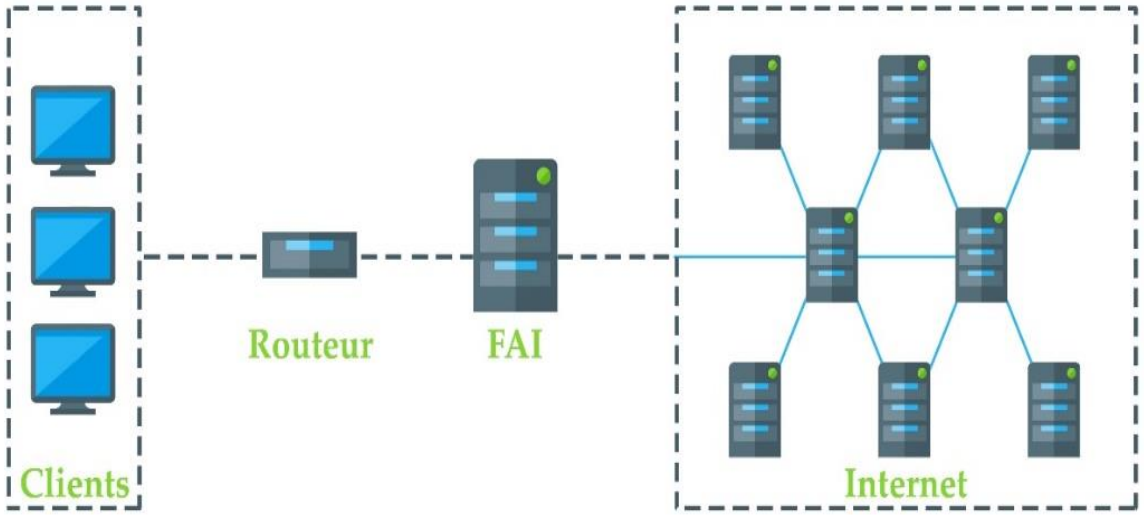


Figure 1.3.6 : *Accès à Internet.*

1.3.7 Réseau privé virtuel VPN

Un VPN ou, de son nom complet « Virtual Private Network » est un logiciel assurant la confidentialité, le cryptage et l'anonymat des donnés en ligne. Il crée un tunnel qui crypte les informations.

De nombreux VPN ne conservent pas les données, mise-à-part l'adresse IP de l'utilisateur [11].

Figure 1.3.7 : *Principe de fonctionnement du VPN.*

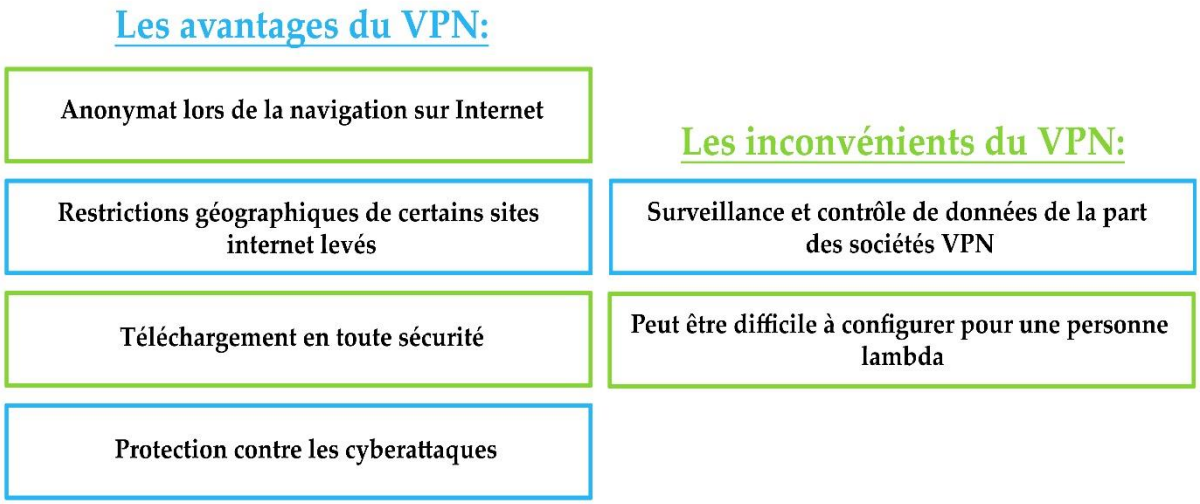


Figure 1.3.8 : *Avantages et inconvénients du VPN.*

1.3.8 Proxy

Le serveur proxy joue le rôle d'intermédiaire entre le client et le serveur lors d'échange du trafic internet, il permet de surfer sur internet de manière anonyme en remplaçant votre adresse IP par celle du proxy.

1.3.8.1 Serveur proxy HTTP

Le proxy web a un travail simple, consistant à réorienter le trafic Web de l'HTTP ou HTTPS du client vers l'hôte, tout en masquant l'adresse IP comme source du trafic Web. Hidester est l'un des proxys web le plus utilisé, connu pour ses qualités en matière de cryptage et sécurité [12].

1.3.8.2 Serveur proxy SOCKS

SOCKS a pour rôle de décider si le client peut accéder au serveur externe et lui envoyer sa requête. Il a un fonctionnement inverse qui permet aux applications de l'extérieur de se connecter aux serveurs derrière le pare-feu.

Il prend en charge le trafic non HTTP tels que SMTP, FTP et Torrent [12].

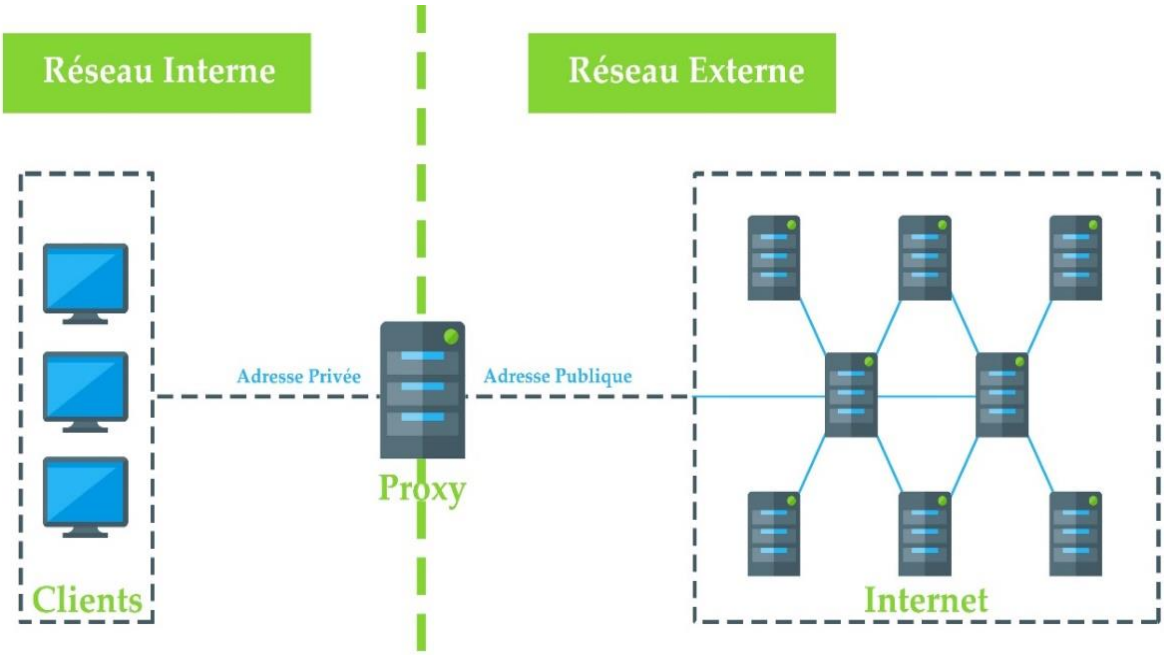


Figure 1.3.9 : *Proxy.*

1.4 Anonymat sur internet

Beaucoup d'internautes estiment que l'atout le plus important d'Internet est l'anonymat, qui fait référence à la protection de l'identité d'un individu utilisant un service ou une ressource, sans que les informations de celui-ci ne soient divulguées.

Cependant, l'Internet de base n'est pas anonyme. Les adresses IP servent d'adresses postales virtuelles, ce qui signifie que chaque fois qu'une ressource sur Internet est consultée, elle est accessible à partir de son adresse IP particulière, et les modèles de trafic de données vers et depuis les adresses IP peuvent être interceptés, surveillés et analysés, même si le contenu de ce trafic est crypté.

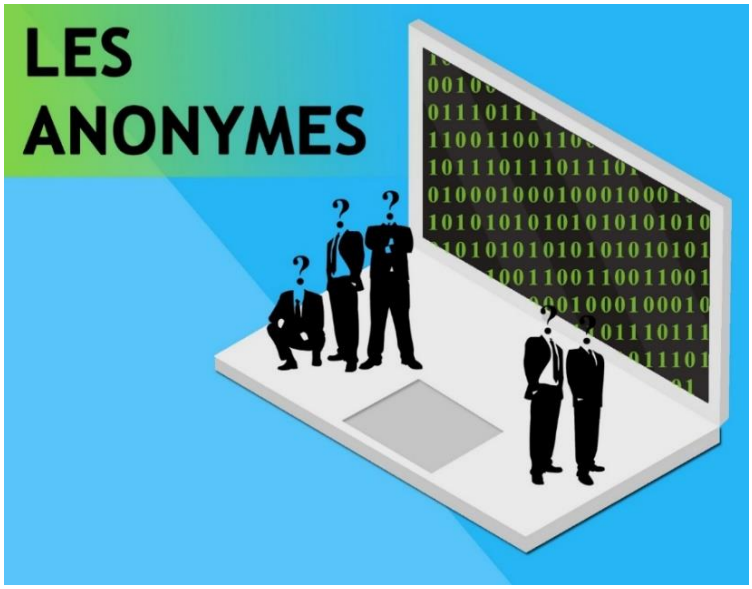


Figure 1.4.1 : *Anonymat sur internet.*

Les services d'anonymat tels que Freenet, Brave et Tor résolvent le problème du suivi IP. Ils fonctionnent en cryptant les paquets dans plusieurs couches de cryptage, où chaque paquet suit un itinéraire prédéterminé à travers le réseau d'anonymisation. Chaque routeur voit le routeur précédent immédiat comme origine et le routeur suivant immédiat comme destination. Ainsi, aucun routeur ne connaît à la fois la véritable origine et la véritable destination du paquet. Cela rend ces services plus sécurisés que les services d'anonymisation centralisés.

L'anonymat est un sujet très discutable. Bien que son utilisation soit bénéfique et est considérée comme un droit de chaque internaute, l'anonymat peut être utilisé par des personnes maléfiques dont le but est le harcèlement criminel, la divulgation d'informations privées ou le lancement d'une attaque destructrice ciblant une entité précise. Les experts disent alors que ses inconvénients ont dépassé ses avantages [13].

1.5 Les profondeurs d'internet

1.5.1 Le Web Surfacique

C'est la première partie visible, correspondante à moins de 5 % du volume total d'Internet. Ce web contient des moteurs de recherches comme Google ou Bing.

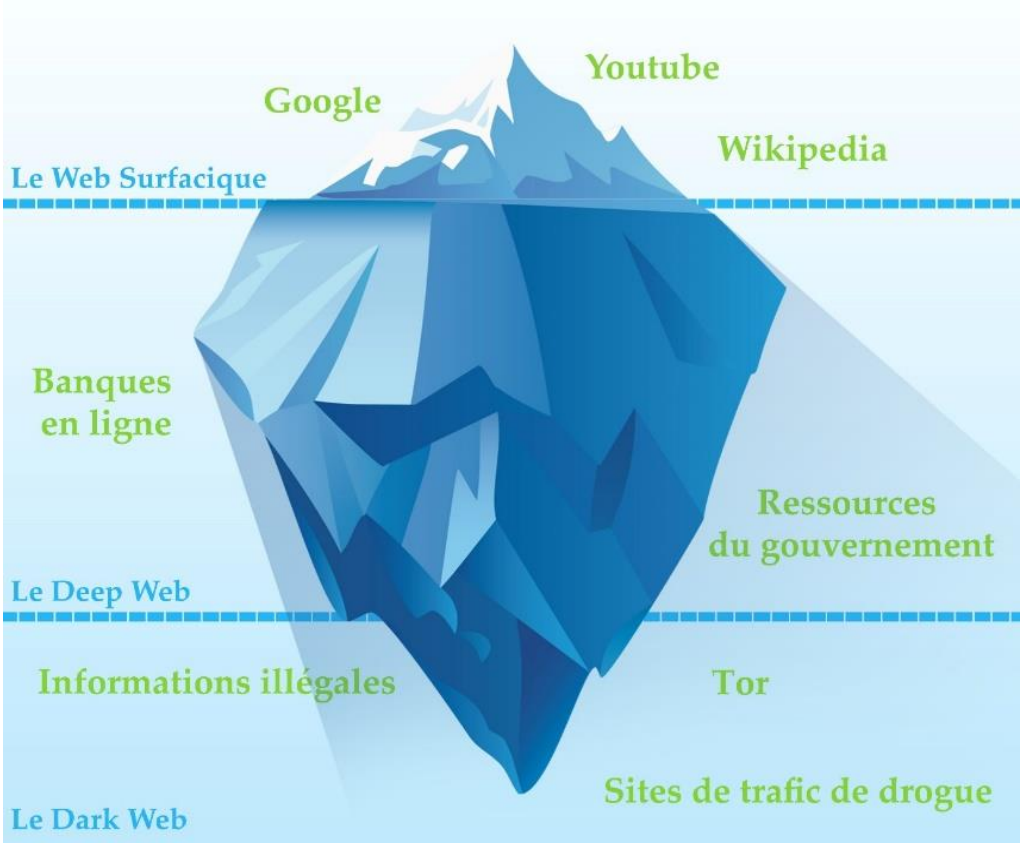


Figure 1.5.1 : *Les profondeurs d'internet.*

1.5.2 Le Deep Web

Cette partie du Web représente 90% du volume d'internet. Elle inclut les bases de données et réseaux internes d'entreprises et gouvernements utilisés à titre privé au niveau de leurs organisations.

1.5.3 Le Dark Web

L'Internet sombre se constitue de réseaux superposés assurant la mise en ligne de sites web non référencés par les moteurs de recherche usuels. Il résulte de l'ensemble du darknet où l'adresse IP, la localisation et les échanges des utilisateurs sont anonymes grâce à un système de chiffrement en couche.

Son infrastructure est généralement liée à des intentions criminelles et contenus illégaux, bien que beaucoup de parties juridiques en aient aussi fait usage. Car contrairement à ce que pensent les gens, l'accès au Dark Web n'est pas illégal, ses utilisations peuvent

parfaitement être légales et avantageuses. Ainsi la légalité du Dark Web dépend de l'utilisation de l'internaute.

Le Dark Web représente un grave danger aux personnes non-expertes dans le domaine. De nombreux logiciels malveillants y sont présents. Un système de distribution et une charge de codes utilisés permettent leur propagation [14].

1.6 Les différents outils d'anonymat

Garantir son anonymat sur la toile et le respect de la vie privée sont devenus des sujets majeurs aujourd'hui.

Il est important de pouvoir protéger ses informations personnelles lors de l'utilisation d'Internet. Cependant, être anonyme ne signifie pas avoir recours à un pseudonyme seulement pour masquer son identité, mais plutôt, une non traçabilité est nécessaire grâce aux différents outils disponibles.

1.6.1 La navigation privée

Naviguer en privée permet de se débarrasser de toute trace du passage sur la toile. Les données de navigation et les cookies par exemple ne seront pas conservés sur le poste client à la fin de la session.

L'activité reste visible des sites Web que vous consultez, de votre employeur ainsi que de votre fournisseur d'accès à Internet.

Certains pensent à tort que la navigation privée les protège contre les pirates informatiques qui sévissent sur Internet. Ce qui n'est pas le cas, car la navigation privée protège uniquement contre le regard indiscret des personnes qui ont un accès physique à un ordinateur [15].

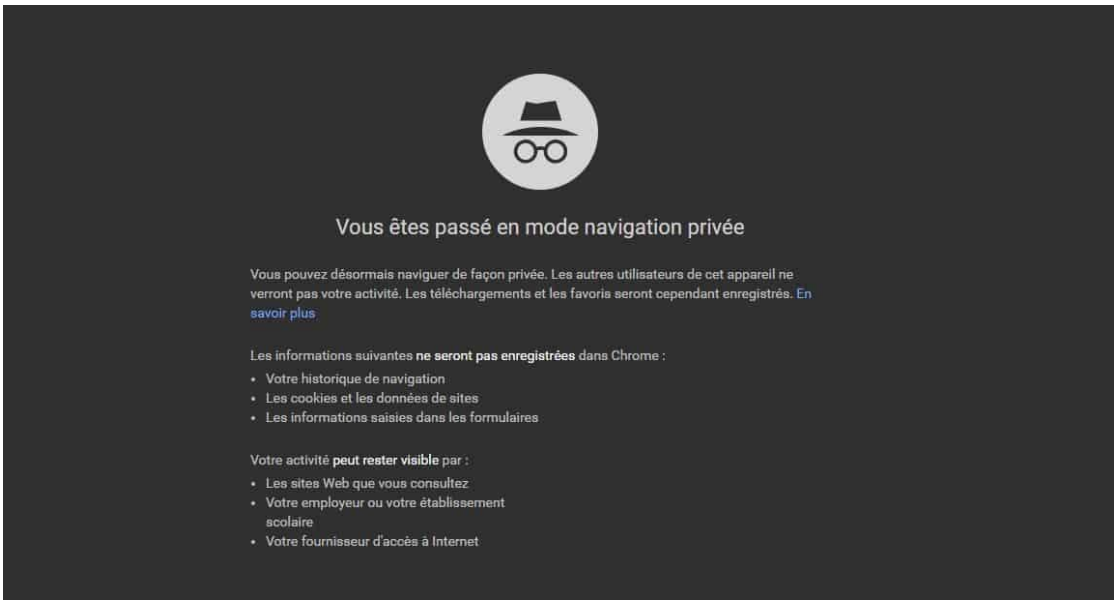


Figure 1.6.1 : *interface Google en navigation privée [16].*

1.6.2 Adresse e-mail jetable

C'est une adresse temporaire communément appelé "trash-mail" ou "tempmail", qui se détruit spontanément après un laps de temps. Elle permet de s'inscrire à un site Web ou blog sans avoir à fournir une adresse mail réel.

Ainsi, avoir recours à une adresse e-mail jetable permet une inscription rapide, une certaine protection contre les virus en évitant les spam et enfin, une meilleure confidentialité [17].

1.6.3 Les réseaux anonymes

1.6.3.1 Tor

"The Onion Router" est un réseau d'anonymisation multi-proxy qui ne repose pas sur des serveurs proxy spécifiques pour traiter les données. Il utilise plutôt des connexions d'une multitude d'autres utilisateurs de Tor afin de masquer l'IP de l'utilisateur original. Sachant que plus de 3 millions d'utilisateurs partagent leurs IP dans le monde entier, le risque de retrouver la provenance d'origine d'une requête internet est pratiquement impossible.

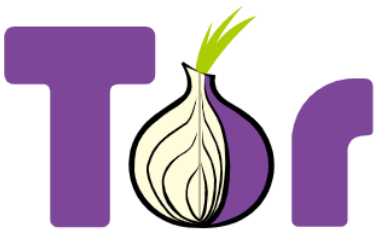


Figure 1.6.2 : *Logo du réseau Tor [18].*

Pour fonctionner, Tor a trois composantes principales. L'utilisateur, le réseau d'utilisateur et le serveur où l'utilisateur reçoit des informations qui lui permettent de dissocier l'utilisateur des données auxquelles il cherche à accéder, en gardant son IP masquée.

Il n'est pas illégal d'utiliser Tor. Cependant, de nombreux gouvernements ont mis en place des mesures pour empêcher les citoyens de le faire. De même, certains fournisseurs d'accès internet empêchent les utilisateurs de Tor d'accéder à leurs données. De nombreuses entreprises bloquent aussi l'accès à leurs services via Tor [19].

Les avantages de Tor:	Les inconvénients de Tor:
Gratuit et ne requiert aucun abonnement	Très lent, car les données passent par trois serveurs avant d'atteindre leur destination finale
Adresse IP masquée aux sites et pages web visités	Uniquement accessible via un navigateur internet défini, dont l'accès TOR est intégré.
Accès à des contenus bloqués	Difficultés pour certains utilisateurs à se connecter, Car Tor est bloqué dans certains FAI
Réseau distribué et exécuté par des volontaires, ce qui empêche un gouvernement ou une quelconque organisation de réussir à le fermer	Pas des communications sécurisées. Le cryptage est utilisé uniquement pour assurer l'anonymat entre les nœuds, les données ne sont pas cryptées autrement

Figure 1.6.3 : *Avantages et inconvénients de Tor.*

1.6.3.2 Comparatif Proxy, Tor et VPN

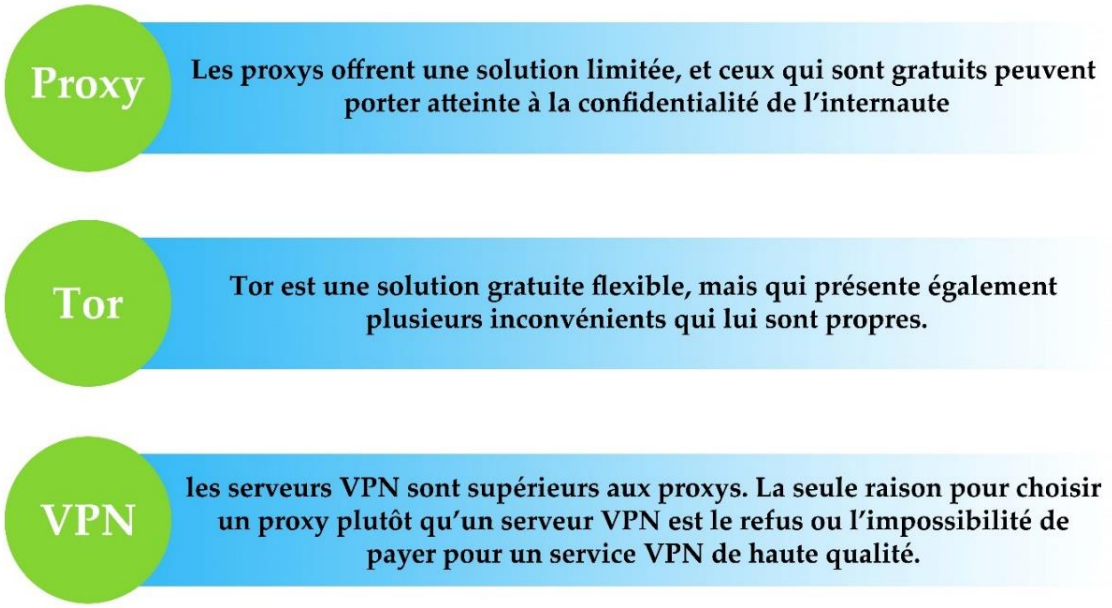


Figure 1.6.4 : *Comparaison entre le Proxy, Tor et VPN.*

1.6.3.3 Freenet

Freenet est un réseau anonyme basé sur un système décentralisé de diffusion et de stockage d'information, son but premier est la liberté d'expression et d'informations instauré par l'anonymat.

Figure 1.6.5 : *Logo de Freenet [20].*

Freenet est composé de nœuds qu'on appelle « freenode » répartis sur internet. Chacun d'eux tient à disposition des autres freenode un cache local crypté, accessible en lecture et écriture. L'espace alloué par le freeenode sert à stocker les données associées à une clé unique. La cache dédié à la conservation des données est crypté, de façon à ce que même le propriétaire du PC ne puisse pas en déterminer le contenu. Le freenode possède également

une table de routage dynamique contenant l'adresse d'un certain nombre de nœud avoisinant. Chaque freenode n'a qu'une connaissance très partielle des nœuds voisins et aucun des freenodes ne peut avoir connaissance de l'emplacement des données sur le réseau [21].

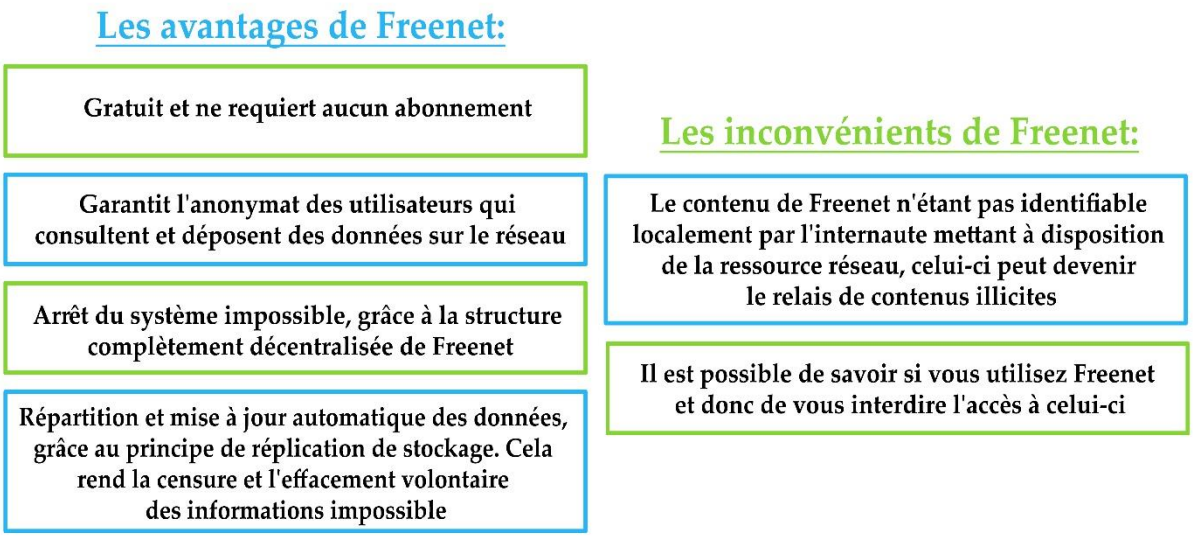


Figure 1.6.6 : *Avantages et inconvénients de Freenet.*

1.6.3.4 I2P

L'Invisible Internet Project "I2P" est un réseau anonyme et décentralisé qui permet aux utilisateurs et aux applications de surfer anonymement.

Contrairement au routage « en oignon » utilisé par Tor, le mode de communication de I2P est comparé à de l'ail, où chaque message est une gousse et l'ensemble d'entre eux est une tête d'ail. Ainsi, dans I2P, plusieurs paquets (ou messages) sont envoyés au lieu d'un seul, passant par différents nœuds. De plus, des tunnels d'entrée et de sortie unidirectionnels sont utilisés, de sorte que la requête et la réponse suivent des chemins différents.

En même temps, à l'intérieur de chaque tunnel, il y a un cheminement d'oignons similaire à celui de Tor. En ce sens, avec I2P, il est beaucoup plus complexe d'effectuer une analyse de trafic que dans Tor ou un VPN traditionnel, car il utilise non seulement plusieurs nœuds et tunnels, mais envoie également plusieurs paquets au lieu d'un seul.

Figure 1.6.7 : *Logo I2P [22].*

Les ordinateurs du réseau ont donc un EEPSITE et une clé de ce dernier, qui remplace l'adresse IP. Pour consulter un site, il suffit de taper sa clé sur le navigateur, mais I2P a amélioré cela en ajoutant un DNS pour transformer la clé asymétrique en un nom de domaine (exemple : forume.i2p)

Lorsqu'un ordinateur souhaite consulter un EEPSITE, il doit passer par différents autres ordinateurs (ou nœuds du réseau) qu'on appelle intermédiaires pour accéder à l'EEPSITE (même concept que l'oignon du réseau Tor) [23].

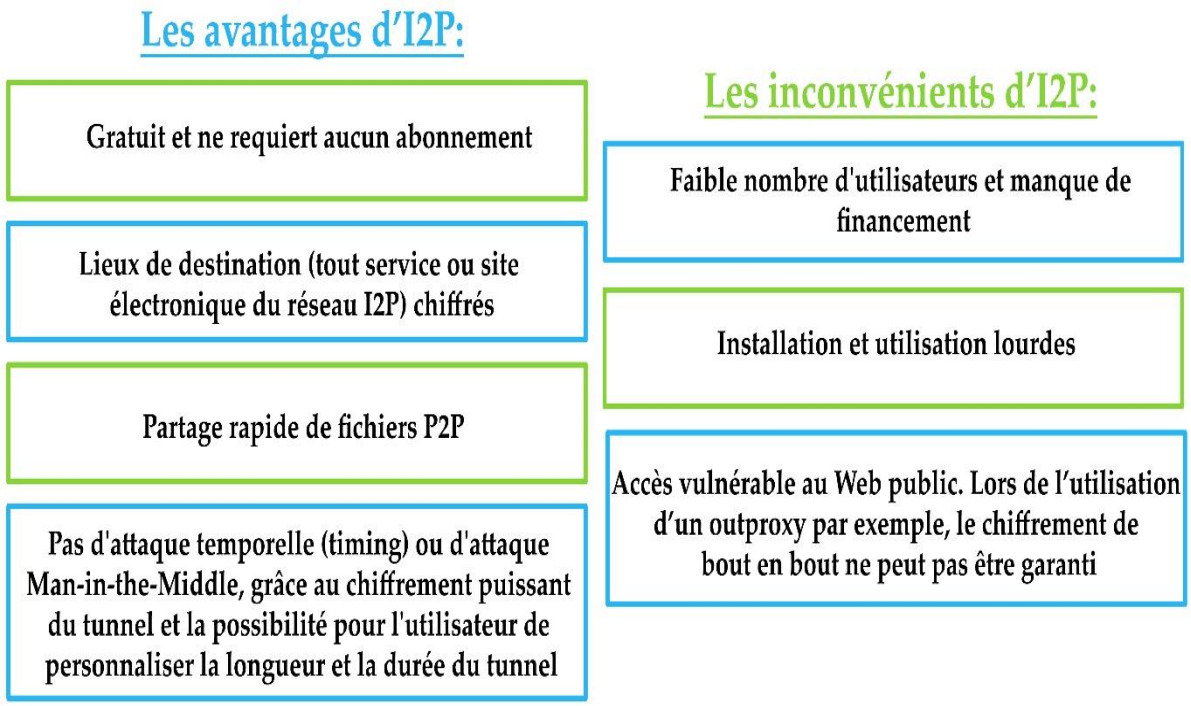


Figure 1.6.8 : *Avantages et inconvénients d'I2P.*

1.6.3.5 Comparaison des réseaux anonymes

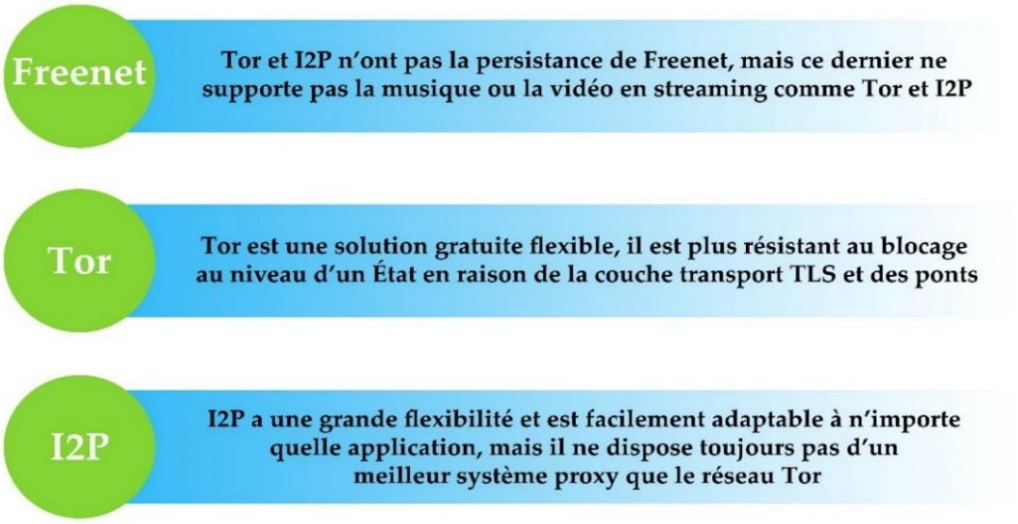


Figure 1.6.9 : *Comparaison entre Freenet, Tor et I2P.*

1.6.5 Les moteurs de recherche privés

Les moteurs de recherches usuels tels que Google et Yahoo collectent et conservent vos données, lorsque vous faites des requêtes en ce qui concerne votre adresse IP, système d'exploitation ,historique de navigation, votre localisation ,etc.

C'est l'un des facteurs qui incite les internautes à utiliser d'autres moteurs de recherche anonyme en alternative.

1.6.5.1 DuckDuckGo

Leader dans le domaine, c'est un outil de méta moteur puissant. Son site web contient une politique de confidentialité complète et transparente, il ne collecte pas d'informations sur l'utilisateur ou les recherches effectuées [24].

Figure 1.6.10 *: Interface DuckDuckGo [25].*

1.6.5.2 Swisscows

La politique de confidentialité de Swisscows assure qu'aucune adresse IP, ni informations de navigation ou informations relatives à un appareil n'est enregistrer.

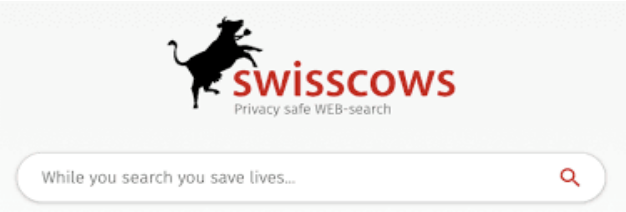


Figure 1.6.11 : *Interface Swisscows[26].*

L'interface Swisscows à recourt à ses propres serveurs privés. Son centre de données est défendu par des lois solides de la Suisse sur la confidentialité et la rétention des données [24].

1.6.6 Module d'extension du navigateur

1.6.6.1 Protection d'extension du navigateur

Lors d'une connexion à un site web, un message apparait pour demander d'accepter ou de refuser des cookies, les cookies sont des fichiers texte de petite taille, qui stockent des informations relatives à un utilisateur sur un serveur. Il existe par contre des cookies tiers non-générées par le site hôte mais par un autre, permettant de tracer les visites des sites internet et le comportement des internautes [27].

Figure 1.6.12 : *Paramètres pour bloquer les cookies tiers.*

"Cookie AutoDelete" est une extension qui supprime les cookies et autres données du site de navigation dès la fermeture de l'onglet, les changements de domaine ou le redémarrage du navigateur.

1.6.6.2 Protection contre les mouchards

Un mouchard est un logiciel espion caché sous un autre pour enregistrer les données confidentielles d'un utilisateur [28].

1.6.6.3 Protection des communications

HTTPS est un protocole associant les deux protocoles HTTP et SSL, le Secure Socket Layer responsable du chiffrement de la communication entre le serveur Web et le client.

"HTTPS Everywhere" est une extension qui déclenche spontanément la navigation chiffrée avec le protocole HTTPS à la place du http [29].

1.6.7 Système d'exploitation

Un système d'exploitation est un assemblage de programmes qui met en relation l'utilisateur avec ses programmes et le matériel de l'ordinateur. Il simplifie la manipulation de la machine physique et offre une interface graphique facilement utilisable.

Les systèmes d'exploitation les plus répandus sont Windows et Mac OS X. Mais en matière de sécurité et anonymat, Linux est le système d'exploitation maitre [30].

1.6.7.1 Tails

« The Amnesic Incognito System » connu sous Tails est un système d'exploitation live du système GNU/Linux Debian, installé sur un port amovible et qui a pour objectif la sécurité et le maintien de l'anonymat.

Figure 1.6.13 : *Logo Tails [31].*

Etant donné que c'est un système live, il n'est pas conçu pour être installé directement sur l'ordinateur, il suffit d'une clé USB pour le lancer. Cette méthode permet de limiter fortement les traces laissées sur l'ordinateur de l'utilisateur et de le rendre utilisable presque partout [32].

1.6.7.2 Qubes OS

Qubes OS fait partie des systèmes d'exploitation les plus sécurisés, il a recourt à différentes machines virtuelles, chacune isolée du système d'administration et est consacré à une fonction précise.

Figure 1.6.14 : *Logo de Qubes OS [33].*

La sécurité vient du processus de virtualisation : chaque machine virtuelle est livrée avec son propre navigateur web, système de fichiers, etc., garantissant que les différentes parties de la vie d'un internaute sont séparées les unes des autres, et donc inaccessibles en cas de violation. Il est également très facile de créer ses propres machines virtuelles, ce qui rend l'expérience parfaitement adaptée aux besoins de chaque individu [34].

1.6.7.3 Whonix

Whonix est une distribution Linux basée sur Debian et qui repose sur l'anonymat, la sécurité et la confidentialité.

Figure 1.6.15 : *Logo de Whonix [35].*

Whonix assure l'anonymat au moyen de VirtualBox et de Tor. Il fait en sorte que ni les logiciels malveillants ni les comptes super-utilisateurs compromis ne peuvent conduire à des fuites IP et DNS. Tous les logiciels fournis avec cet OS sont préconfigurés pour fonctionner avec des paramètres de sécurité maximum [36].

1.7 Avantages et inconvénients de l'anonymat

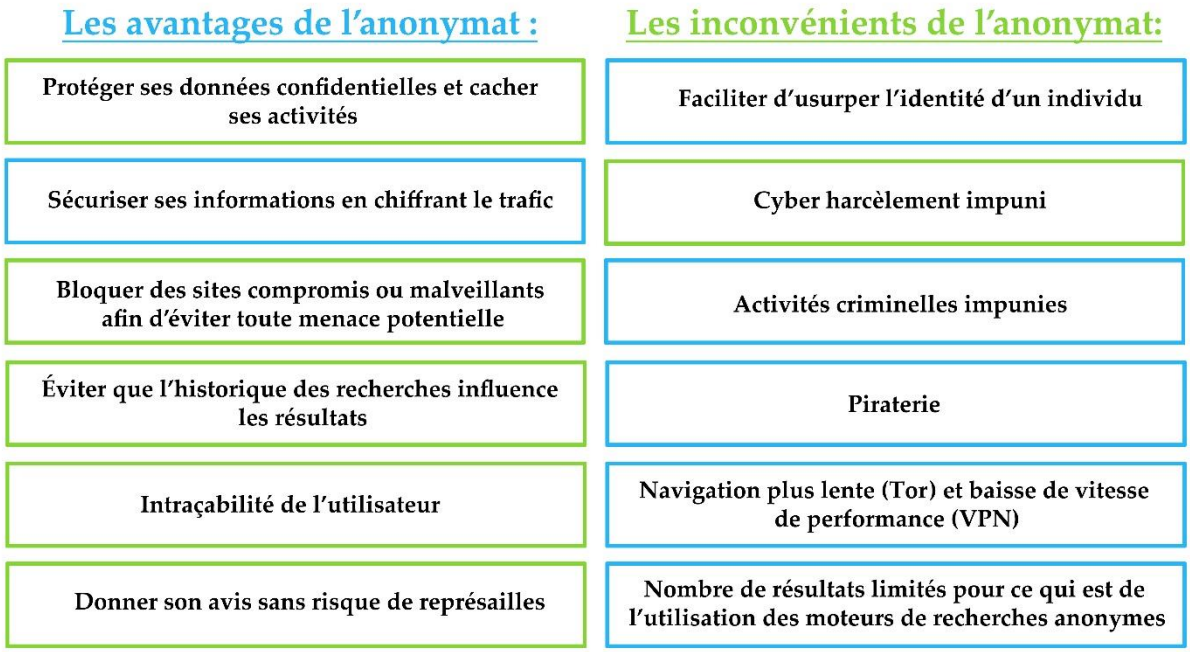


Figure 1.7.1 : *Avantages et inconvénients de l'anonymat.*

1.8 Conclusion

L'état de l'art présenté dans ce chapitre a mis en évidence les divers moyens et techniques de préservation d'anonymat sur Internet, qui permettent simultanément des actions équitables et inéquitables.

Néanmoins, le résultat de ces différents outils ne peut pas être pleinement garanti. Surtout si un internaute n'a pas les connaissances essentielles pour appliquer les mesures de sécurité en vue de protéger son identité.

La compréhensibilité des termes mentionnés sur ce chapitre est indispensable pour la bonne appréhension du prochain.

Chapitre 2

Les vulnérabilités du réseau anonyme

2.1 Introduction

L'anonymisation de l'identité numérique fait directement penser à Tor et I2P, les deux réseaux anonymes les plus populaires et utilisés.

Le routage en oignon de Tor a été déployé dans les années 1990 par les agents du « United States Naval Research Laboratory », laboratoire de recherche de la marine de guerre des États-Unis, pour protéger leurs communications des différentes interceptions possibles [37]. Mais ce n'est qu'en 2002 que le projet Tor a été lancé, et depuis, il ne cesse d'évoluer dans le but d'empêcher l'identification de ses utilisateurs.

I2P de son côté a vu le jour en 2003. Il a été initialement créé à partir du code source du réseau anonyme « Freenet » [38]. L'anonymisation de ses communications se fait en chiffrant le trafic de ses utilisateurs et en l'envoyant pour être transiter à travers de divers chemins afin de compliquer et éviter sa détection.

L'appréciation des internautes envers ces deux méthodes d'anonymat en particulier revient au fait qu'ils offrent une meilleure protection de la vie privée, un meilleur accès à tout ce qui est restreints et une meilleures robustesse et fiabilité selon eux.

C'est pour cette raison-là que ce deuxième chapitre va cibler les deux réseaux Tor et I2P. L'étude approfondie de leur fonctionnement, avantages et inconvénients permettra de vérifier si les idées préconçues sont vraies, ou pas.

2.2 Problématique

Malgré leurs avantages, l'utilisation des réseaux anonymes Tor et I2P se révèlent ne pas être sans conséquence, ce n'est pas parce que la navigation est anonyme que l'utilisateur ne peut être la cible d'attaque.

Opter pour les réseaux anonymes n'est pas une décision à prendre du jour au lendemain. L'utilisateur doit d'abord voir s'il en a réellement besoin, si oui, pour quelle raison ? Que veut-t-il protéger et de quoi ?

2.3 Solution Proposée

Une étude de son équipement est également nécessaire pour le test de la capacité, robustesse et résistance de celui-ci, car le trafic anonyme peut consommer une grande bande passante qui ne pourra peut-être pas être supporté par un simple appareil, non conçu à ces utilisations-là.

Les experts en cyber sécurité travaillent sur la détection de toute trace venant de Tor ou I2P à l'aide de différentes techniques et outils, mais cela n'est jamais une tâche facile.

Microsoft Cloud App Security (MCAS) par exemple est capable de fournir des alertes sur l'activité d'une adresse IP de Tor en détectant son trafic. Par contre, cette solution est propre à l'environnement cloud Azure [39].

Il existe aussi des listes d'adresses IP et de nœuds accessibles au public et utilisées pour la surveillance par diverses applications et protocoles réseau, notamment les pare-feu, IDS/IPS, NetFlow, etc.

Les systèmes de contrôle des applications peuvent être utilisés également pour détecter et alerter le trafic anonyme en fonction des propriétés et du comportement du processus.

2.4 Méthode de travail

Dans le cas de ce mémoire, une analyse a été faite afin d'extraire de différentes caractéristiques propres à chaque réseau, qui seront par la suite utilisées dans la création de diverses règles nécessaire à leur blocage.

Pour cela, la méthode des DPI (Deep Packet Inspection) a été utilisée. Son rôle est de faire une inspection approfondie des paquets dans le but de faciliter leur détection au sein d'une entreprise.

Et afin de tester la fiabilité de ces règles-là, des sites ont été bloqué dans le réseau de l'entreprise, y accéder était donc impossible même en utilisant Tor et I2P. Si c'était le contraire, et qu'un employé a pu y'accéder, les règles créées auraient été non fiables.

2.5 Tor

2.5.1 Fonctionnement de Tor

Tor est le résultat d'un réseau superposé mondial basé sur Internet, ce dernier est décentralisé ayant recours à des serveurs hébergés par de nombreux volontaires.

Les messages sont cryptés en continues et sont envoyés via des nœuds de réseaux appelés des routeurs oignons. Les données sont chiffrées autant de fois qu'il y'a de nœuds traversés lors de la transmission. Le chiffrement est asymétrique, le message est chiffré avec une clé publique et est déchiffrable seulement avec une clé privée. Chaque nœud représente une couche de cryptage de données, chiffrées successivement rappellent l'aspect d'un oignon qui à l'origine du logo de Tor.

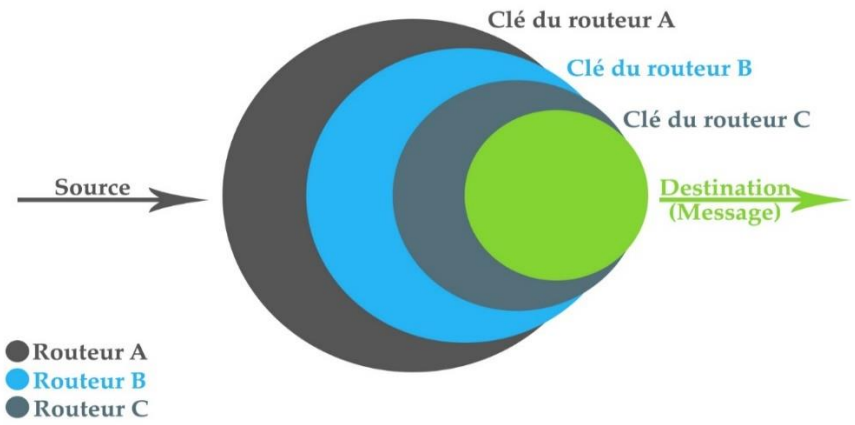


Figure 2.5.1: *Message envoyé encapsuler.*

Chaque transmission de données est choisie de façon automatique et aléatoire, les nœuds n'ont pas connaissance du parcours traversé. Toutes les connexions entre les nœuds et les clients utilisent le protocole TLS [40].

2.5.2 Les types de nœuds Tor

2.5.2.1 Nœuds d'entrée (garde ou de pont)

Ils sont deux sortes :

- Des nœuds gardiens connus de tous dont la liste est publique.

• Des nœuds ponts secrets par le projet Tor qui masquent l'utilisation de Tor au fournisseur d'accès Internet. Ils sont utilisés dans les pays ou Tor est bloqué ou illégal. Il faut faire une demande « auteur project » et remplir certaines conditions telles qu'une bande passante adéquate et une certaine stabilité afin d'être éligible à cette requête.

Le nœud d'entrée reçoit le paquet du destinataire, il déchiffre la première couche avec sa clé privée, il en extrait le paquet à destination du prochain nœud sans connaitre son contenue ni sans destinataire finale car il est chiffré. Il ne connait que I'émetteur et le prochain nœud auquel il envois le paquet.

2.5.2.2 Nœuds intermédiaires

Ce nœud reçoit le paquet et le déchiffre avec sa clé privée, il en sort un paquet à la destination du prochain nœud. Il connait le nœud d'où vient le paquet et le prochain nœud du paquet.

2.5.2.3 Nœuds de sortie

Ce nœud reçoit le paquet et déchiffre la dernière couche. C'est le nœud le plus sensible, il n'a pas d'information sur l'adresse IP de l'émetteur mais il connait l'adresse IP du dernier nœud, le contenu du paquet et l'adresse IP du destinataire.

Le destinataire pense que c'est le nœud de sortie qui communique avec lui et non l'émetteur. Les nœuds de sortie bloquent en générale certains protocoles et ajoutent des systèmes de sécurité afin éviter d'être utilisé comme intermédiaires lors d'une attaque.

Les données qu'on peut extraire du nœud d'entrée et de sortie menaçant peuvent être analysé ou/et corrompu.

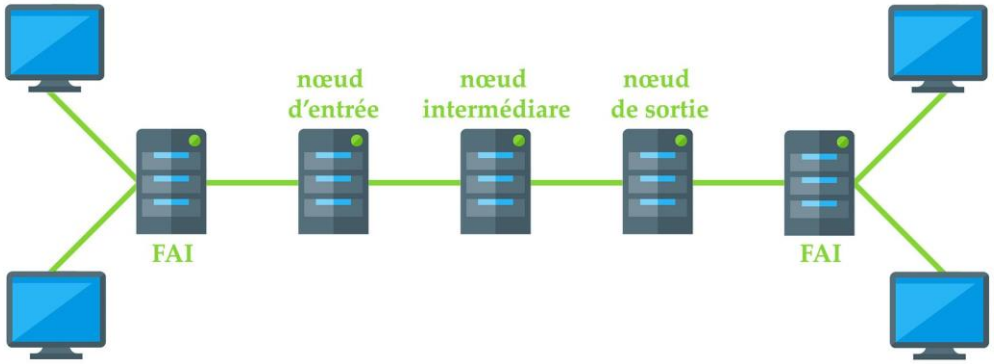


Figure 2.5.2: *Fonctionnement de Tor.*

Si l'expéditeur veut connaitre l'adresse IP de l'émetteur, il peut utiliser un script espion dans le contenu chiffré qui l'envoie. Pour éviter cela, le navigateur Tor Browser utilise par défaut le « no script », un plug in qui bloque tout script [41].

2.5.3 Services de l'onion

Le point onion est un domaine réservé, il n'est pas utilisable sur le web classique et pour accéder à un site, il faut être connecté à Tor. Son avantage est qu'il permet une communication sans connaitre l'adresse IP du destinataire en utilisant le même principe de succession des nœuds du côté de l'émetteur et du récepteur en utilisant un nœud nommé un point de rendez-vous qui remplace le nœud de sortie et joue le rôle d'un intermédiaire.

Http://suw74isz7wqzpmqu.onion est un exemple d'un nom de site en point oignon. Les messages envoyés au destinataire sont chiffrés avec sa clé publique, seul lui peut les déchiffrer avec sa clé privée. L'adresse du destinataire est calculée à partir de sa clé publique à travers un hash que l'émetteur vérifie pour voir s'il correspond à son adresse afin de communiquer avec. Certains sites web bloquent le flux qui provient du réseau de Tor [40].

2.5.4 Création du circuit

Actuellement, l'établissement d'un circuit Tor est réalisé grâce à l'échange de clés Diffie-Hellman entre l'Onion Proxy et chaque nœud du circuit.

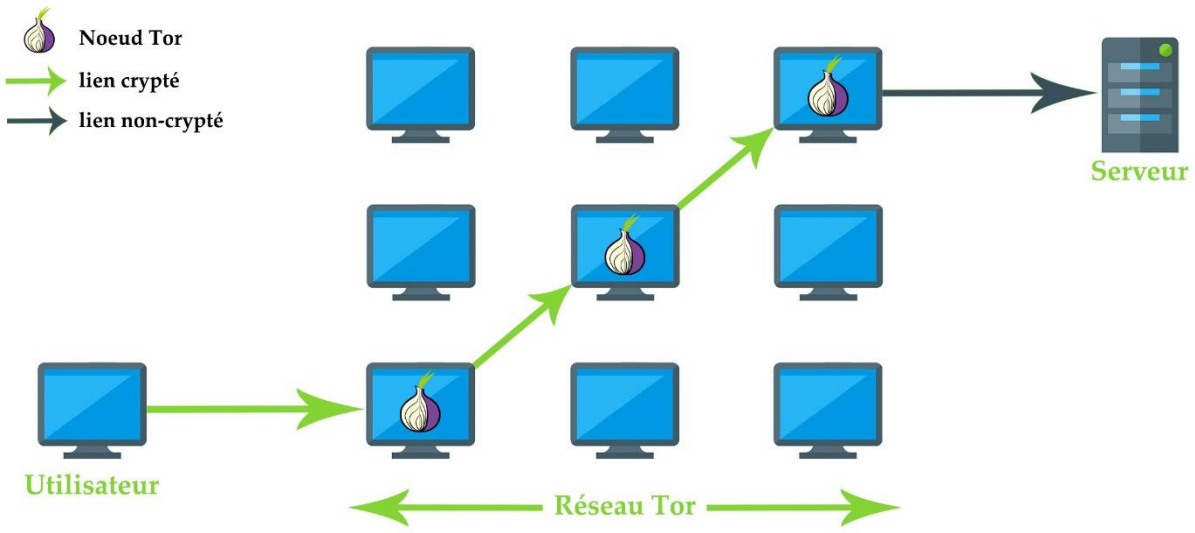


Figure 2.5.3: *Réseau de Tor.*

La conception du circuit est expliquée comme suit :

a. **Choix et sélection du nœud de relais :** L'Onion Proxy commence par choisir un nœud de sortie, un nœud intermédiaire et finalement un nœud d'entrée à partir d'une liste de nœuds de garde enregistrée dans son serveur annuaire. Cette sélection est faite au hasard. L'utilisateur de Tor se trouve donc avec trois nœuds, des nœuds qui ont été choisi selon leur disponibilité et leur bande passante.

b. **Construction du circuit :** Ce circuit est créé entre l'Onion Proxy et ses nœuds qui négocient une clé symétrique à utiliser entre eux.

c. **Echange de clé Diffie-Hellman :** Cet algorithme d'échange de clés permet à deux parties de communiquer, en employant une clé symétrique sur un canal de communication non sécurisé, assurant ainsi une confidentialité pertinente lors de la transmission. Lors de l'échange entre les deux acteurs, ils s'entendent sur une clé privée pour chiffrer le message suivant, de ce fait même si une personne étrangère écoute le trafic, elle ne pourra pas décrypter le message.

   Cette clé privée est valable que lors de cette communication, elle n'est pas réutilisée pour décrypter de nouveau message entre des nœuds.

d. **Transport Layer Security (TLS):** Tor utilise les protocoles de sécurisation des échanges sur internet TLS «Transport Layer Security » afin de chiffrer les contenus transmis entre les nœuds. TLS assure :

- **L'authentification** : inclut un sous protocole TLS- Handshake qui permet aux deux parties de s'authentifier entre elles, et de négocier un algorithme de chiffrement et une clé cryptographique avant l'envoi du message.
- **La confidentialité des données échangées** : Les messages sont chiffrés avec des clés symétriques appelées clé de session.
- **L'intégrité des données** : est garantie par un algorithme de hachage tel que SHA-256 [42].

2.5.5 Service Cachées

Dit aussi « Tor onion services » sont des sites web accessibles sur Tor, offrant une discrétion non négligeable. Leurs avantages sont [40] :

• L'adresse IP des services onions est masquée, ce qui rend l'identification de l'opérateur complexe.

•Le trafic entre les utilisateurs Tor et les services cachés est chiffré de bout en bout.

• L'adresse d'un site web est créé automatiquement, il n'est donc pas nécessaire d'acheter un nom de domaine.

2.5.6 Proxy Tor

La manière la plus simple pour se connecter à Tor est de télécharger et d'installer Tor browser. Cependant, il y'a une autre manière, qui est celle de créer un proxy qui permettra de connecter les appareils à Tor en passant par lui. Il faut donc un serveur sous une distribution Linux et des clients.

Pour commencer il faut installer Tor sur Linux puis proxyfier Tor pour qu'il fonctionne en tant que proxy. Pour s'assurer du fonctionnement du proxy, il faut se rendre sur le site service.korben et voir quelle ville est attribuée à l'adresse IP utilisée [43].

2.6 I2P :

2.6.1 Fonctionnement d'I2P

L'invisible Internet Project est une couche réseau anonyme cryptée qui travaille en Peer-to-Peer. Pour transférer les données, ses usagers interprètent deux rôles, celui du transmetteur et celui du récepteur sans l'intervention d'un serveur entre eux.

Le routage à l'ail signifie qu'I2P ajoute de multiples couches de cryptage aux messages afin de les protéger d'être intercepter par des individus extérieurs, non concernés par ces communications. Chacune de ces couches de cryptage sera par la suite supprimer par un routeur du réseau puis transférer au prochain, jusqu'à la réception finale de l'information par son destinataire. Cette opération assure qu'aucun routeur ne puisse dévoiler le contenu définitif de l'information.

De plus, les trajets adoptés pour transmettre les données sont différents. Un chemin pour arriver à la destination et un autre pour y répondre et renvoyer les données au demandant.

Ce réseau privé est dit isolé du réseau Internet. Ses communications passent par ses tunnels chiffrés pour consulter les sites trouvés sur son réseau seulement. Le passage à Internet à travers I2P n'est en revanche pas impossible à l'aide de son OUTPROXY [44].

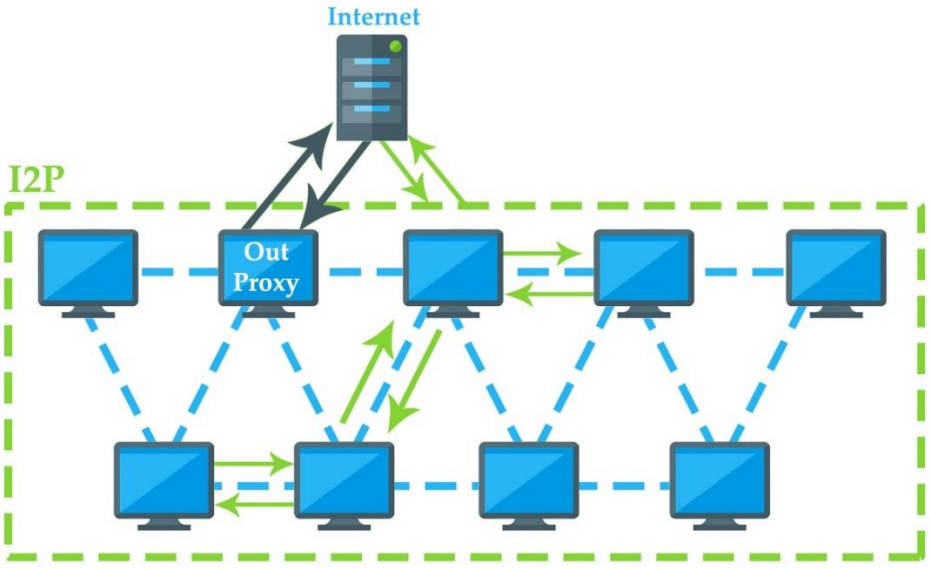


Figure 2.6.1: *Fonctionnement de l'OutProxy.*

2.6.2 Les composantes d'I2P

Pour bien fonctionner, le réseau d'I2P utilise de diverses composantes [44].

1. Les routeurs

Ces nœuds représentent les utilisateurs sur le réseau privé d'I2P.

2. Les tunnels

Un tunnel est une série de routeurs transportant des données dont la durée de vie est dix minutes. Les tunnels sortant expédients l'information et les tunnels entrant l'accueillent.

Le routeur en en-tête du tunnel est désigné entant que « passerelle » tandis que les autres, y compris le dernier sont surnommés les nœuds intermédiaires.

Si un utilisateur « A » transmet un message dans un de ses tunnels de sortie, son nœud de sortie envoie le message à la passerelle d'un des tunnels entrants du destinataire « B »

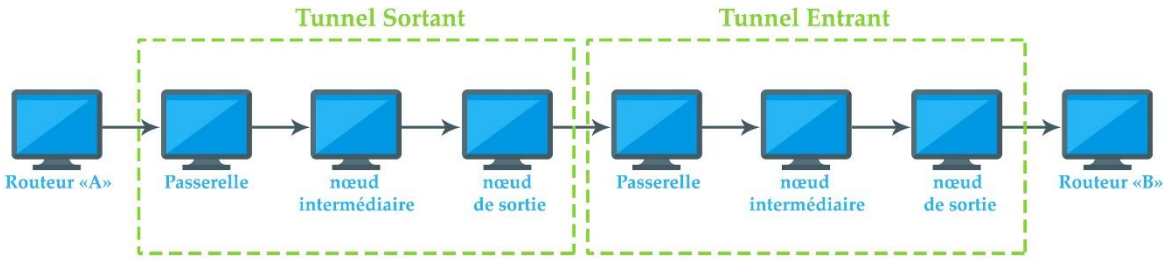


Figure 2.6.2: *Les tunnels d'I2P.*

Un trafic avec une charge bien équilibrer demande l'emploi de multiples tunnels. Ces derniers se catégorise par des tunnels « exploratoires » dont le rôle et de transmettre des requêtes au NetDB qui listera a son rôle sa liste de tunnels « clients ». Cette deuxième catégorie est là pour l'échange de l'information, elle est représentée par les tunnels entrants et sortants.

Pour la conception d'un tunnel d'un nœud, ce dernier a besoin des données « RouterInfo » du NetDB.

3. **La NetDB**

Cette base de données est établie à travers un algorithme pour permettre aux nœuds de communiquer. Ses métadonnées sont deux :

- **Le RouterInfo :** Ensemble d'informations nécessaires aux routeurs pour communiquer avec les autres nœuds du réseau. Ces informations incluent les clés publiques, les adresses de transports, etc. qui seront collecter par la suite par le NetDB.
- **Le LeaseSets :** Assemblage de données nommé « baux » qui permettent aux nœuds de contacter une destination bien précise. Ces baux contiennent des informations concernant la passerelle entrante d'un tunnel, l'heure d'expiration de ce dernier et les clés publiques pour le chiffrement des messages.

4. **Les Eepsites**

Ces derniers représentent un service offert par l'Invisible Internet Project. Ils sont d'ailleurs les équivalents des sites web normales mais pour les utilisateurs du réseau privé d'I2P seulement. Une différence bien remarquée entre les deux est que les Eepsites contiennent moins d'images et vidéos à cause d'un taux plus faible de bande passante [44].

2.6.3 Crypto I2P

I2P utilise différents algorithmes cryptographiques pour ses divers types de communication. La communication entre routeurs, les messages tunnels et les messages à l'ail sont les trois niveaux de communication.

a. **Communications entre routeurs :** C'est le plus bas niveau de communication. A son échelle, les routeurs sélectionnent une clé de session grâce à l'échange Diffie-Hallman. Et avec la clé DSA de chaque routeur, ces derniers s'authentifient entre eux, un auprès de l'autre.
b. **Messages Tunnel :** L'échange des messages ici est au niveau de la couche intermédiaire de la pile de protocole d'I2P. Ils utilisent le cryptage AES256/CBC. Le hachage SHA256 est par la suite utilisé pour la vérification des messages.

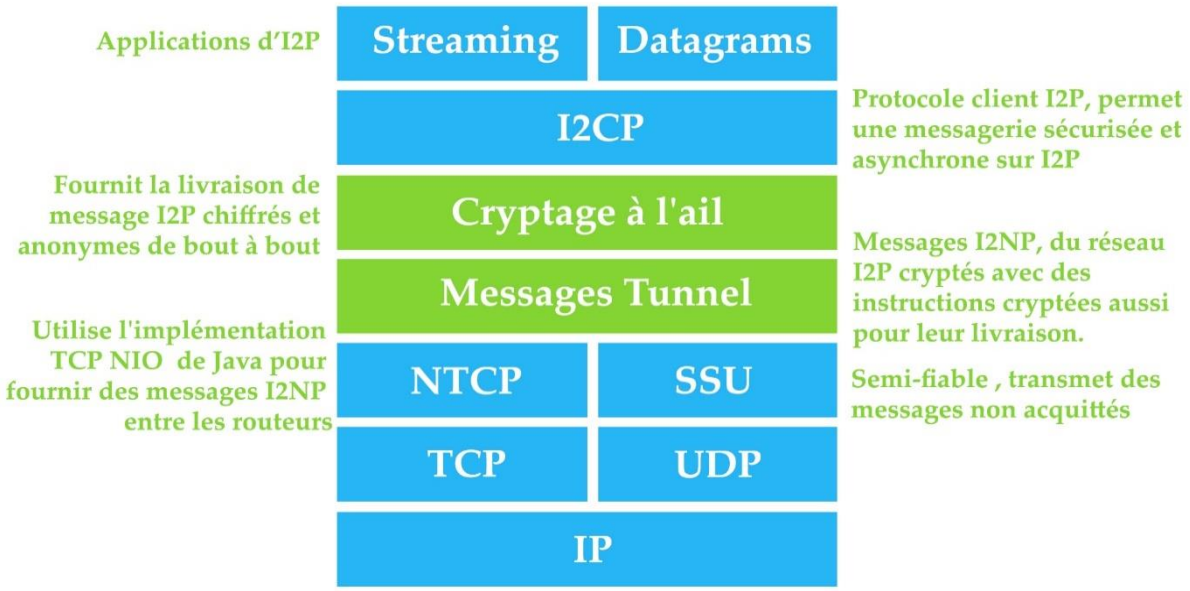


Figure 2.6.3: *La pile de protocole d'I2P.*

c. **Messages Garlic :** Messages transmis sous forme d'ail, cryptés avec ElGamal/AES+SessionTags. Le routeur du client chiffre donc le message avec la clé publique ElGamal et l'envoi dans les tunnels appropriés [44].

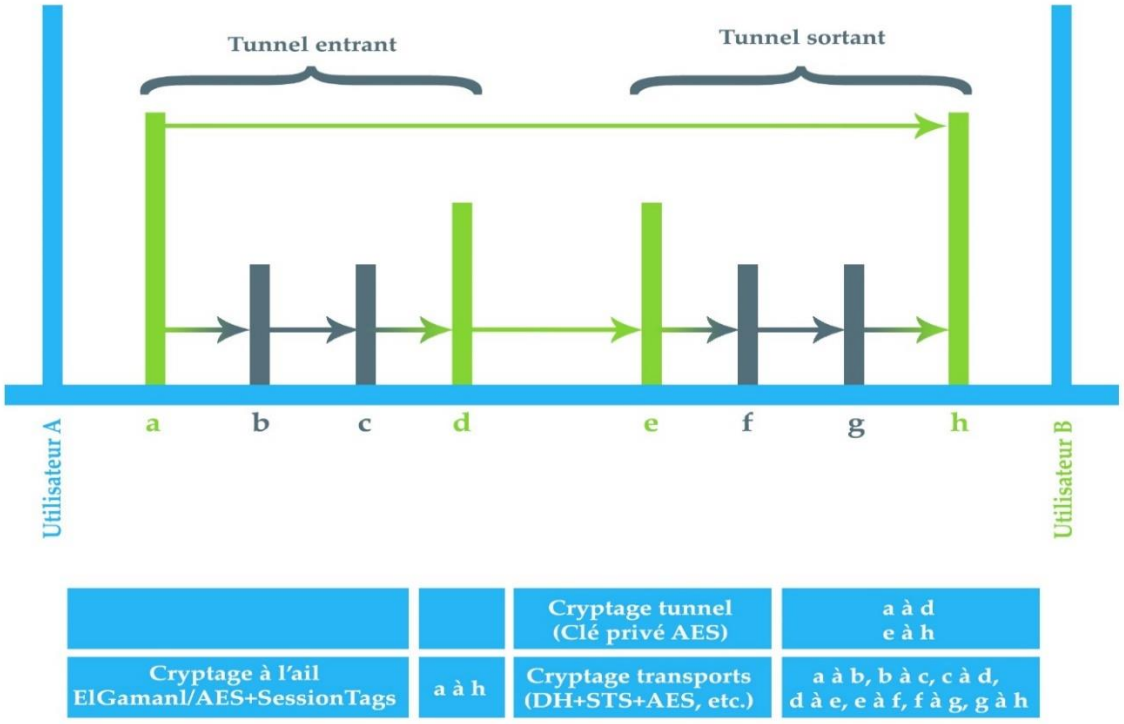


Figure 2.6.4: *Couches de chiffrement dans I2P.*

2.7 Comparatif théorique :

Tor et I2P sont similaires sur plusieurs aspects, cependant une grande partie de la terminologie est différente.

Les différentes techniques entre le réseau Tor et I2P [45] :

- Le flux de message est remplacé par les cellules.
- Les tunnels unidirectionnels représentent les circuits bidirectionnels.
- La commutation de paquets est transformée en commutation de circuit.
- La sélection basée sur les performances remplace la sélection de pair basée sur la bande passante.
- L'architecture distribuée remplace le cadre centralisé.

2.7.1 Dictionnaire Tor vs I2P

Termes	Tor	I2P
Intervenant	Client	Routeur, Client
Infrastructure	Circuit	Tunnel
Base de données	Annuaire	NetDB
Système de stockage de données	Serveur d'annuaire	Routeur floodfill
Composant	Gardien d'entrée	Pair rapide
Composant	Nœud d'entrée	Inproxy
Composant	Nœud de sortie	Outproxy
Service sur Internet	Service caché	Eepsite
Composant	Point d'introduction	Passerelle entrante
Fonctionnement	Routage d'oignon	Routage de l'ail

Tableau 2.7.1: *Dictionnaire Tor vs I2P.*

2.7.2 Caractéristiques Tor vs I2P

Caractéristiques	Tor	I2P
Nombre d'utilisateurs	Elevé	Bas
Utilisation auprès des pirates	Elevé	Bas
Evolutivité	Elevé	Moins
Présence de développeurs	Elevé	Bas
Langage	C	Java
Sensible aux attaques DOS	Plus	Moins
Nombre de nœuds de sortie	Elevé	Moins
Documentation	Bonne	Manquante
Débit	Elevé	Bas
Temporisation	Bas	Elevé
Nom de domaine	.onion	.i2p
Commutation de	circuits	Paquets
Direction	Bidirectionnel	Unidirectionnel
Durée du tunnel	Elevée	Base
Transmission	TCP	TCP/UDP

Tableau 2.7.2: *Caractéristiques Tor vs I2P.*

2.8 Les technologies de Tor et I2P

a. Sélection par pairs

Afin d'accélérer la conception de leurs circuits et tunnels, Tor et I2P emploient la méthode de sélection par pairs. Pour cela, Tor se base sur la bande passante et I2P sur les performances.

- Dans le cas de Tor, la bande passante de chaque routeur est mesurée et enregistrer afin d'être utilisé comme critère de sélection des routeurs intermédiaires et routeurs de sorties.
- De son côté, I2P préfère s'appuyer sur les valeurs enregistrer de ses performances. Son algorithme réagit très rapidement aux défaillances et faiblesses de son réseau.

b. Transmission TCP/UDP

TCP et UDP sont des protocoles de communication réseaux. Le réseau I2P utilise le protocole TLS afin de créer ses tunnels, TLS est basé sur les protocoles TCP et UDP ainsi, le routage I2P à recourt à la connexion TCP et UDP pour la transmission des données [45].

2.9 Les inconvénients de Tor et I2P

Tor et I2P sont deux réseaux anonymes qui permettent une certaine confidentialité sur Internet et le maintien de la vie privée de leurs usagers, cependant leurs utilisations présentent quelques inconvénients [23].

Tor
Les données passent par plusieurs relais ce qui ralentie la navigation.
Certains FAI bloquent son utilisation.
Les messages ne sont pas cryptés.
Blocage basé sur l'empreinte digitale de la connexion.

Tableau 2.9.1: *Inconvénients du réseau Tor.*

I2P
Configuration du navigateur lourde.
Blocage basé sur l'empreinte digitale de la connexion.
Manque de surveillance des nœuds
Vulnérable aux attaques de partitionnement.

Tableau 2.9.2: *Inconvénients du réseau I2P.*

2.10 Les menaces à travers les réseaux Tor et I2P

Lors de la prise de décision, les entreprises et différentes organisations veillent à bien choisir les bonnes mesures et technologies à adopter pour leur travail, en effectuant de divers évaluations, tests et gestions de risques afin d'éviter tout impact négatif sur leurs activités par la suite.

Les deux réseaux Tor et I2P présentent l'avantage de l'anonymat qui peut paraître très considérables comme points positif. Cependant, leurs inconvénients ne doivent pas non plus être pris à la légère ou négligés.

2.10.1 Le délit d'initié

L'accès des employés à Tor ou I2P est possible, menacer la sécurité de l'entreprise par la suite est ainsi réalisable. Ils auront une approche directe à tout ce qui est censuré et interdit. A savoir les bases de données, les sites Web illégaux du Dark Web et ses marchés clandestins.

L'exfiltration des données et informations d'une entreprise pendant cela peut engendrer la vente illégale de son bulletin à des tiers malveillants qui l'utiliseront pour des raisons de veille économique ou de délit d'initié.

Le Dark Web contient des forums dédiés au délit d'initié. Pour devenir membre, les utilisateurs étrangers doivent partager des informations secrètes et si c'est derniers sont fiables, les personnes souhaitant rejoindre seront valider.

2.10.2 Nœuds de sortie malveillant

Ce risque concerne le réseau Tor uniquement. A son niveau, tout le trafic passe par trois nœuds : un nœud d'entrée, un nœud intermédiaire et, un nœud de sortie où les utilisateurs peuvent ajouter des logiciels malveillants, injecter du contenu dans le trafic HTTP non crypté ou modifier des téléchargements non cryptés.

Si un employé souhaite télécharger un fichier en passant par Tor, l'exposition du réseau de son entreprise des infections par des logiciels malicieux devient très probable.

A titre d'exemple le OnionDuke, un nouveau logiciel malveillant ayant des liens avec l'APT (Advanced Persistent Threat) Russe, et qui est distribué par des individus malveillants via un nœud de sortie qui enveloppe les exécutables légitimes de logiciels venimeux. Cela augmente les probabilités que l'attaquant exploite les mécanismes de sécurité [46].

2.10.3 Attaque DDOS

Le trafic anonyme de Tor et I2P consomme une quantité extrêmement élevée de la bande passante. Dans une entreprise par exemple, les serveurs pourraient éventuellement submerger.

Ce type d'attaque dans lequel un service en ligne est rendu indisponible en le submergeant de trafic provenant de plusieurs sources est dit attaque par déni de service distribué (DDoS) [47].

2.10.4 Dommage à la réputation

Un autre problème lié à l'utilisation de ces réseaux anonymes est que si l'adresse IP d'un nœud de sortie suspect appartient à une organisation, celle-ci peut être tenue responsable de crimes qu'elle n'a pas commis, comme du piratage ou transactions illégales.

Les autorités enquêtent sur les traces numériques de l'activité d'un cybercriminel en se tournant vers le propriétaire de toute adresse IP trouvée. Plusieurs fois, cette adresse IP n'est nécessairement pas directement liée à l'activité illégale mais elle s'agit quand même de

la première empreinte numérique rencontrée par les autorités. Elle pourrait donc être annexée à une liste noire et bloquée par d'autres organisations cherchant à se protéger.

2.10.5 Exemple d'attaque réelle

Dès l'année 2017, un certain KAX17 a menacé la sécurité du réseau Tor en exécutant plus de 90000 serveurs fonctionnant comme nœuds d'entrée, nœuds intermédiaire ou nœuds de sortie et rajouté sans aucune coordonnée, alors que les serveurs ajoutés au réseau Tor doivent généralement avoir des informations de contact incluses dans leur configuration, comme une adresse e-mail, afin que les administrateurs du réseau Tor et les forces de l'ordre puissent contacter les opérateurs de serveur en cas de mauvaise configuration ou déposer un rapport d'abus.

Selon les statistiques partagées, il y avait 16% de chances qu'un utilisateur de Tor se soit connecté au réseau Tor via l'un des serveurs de KAX17, 35% de chances qu'il est passé par l'un de ses relais intermédiaires, et jusqu'à 5% de chance de sortis par l'un d'entre eux.

Le but ici était de d'effectuer une attaque Sybil, une menace qui a pour objectif de conquérir de l'influence et le contrôle du réseau en créant plusieurs comptes et identités afin de pouvoir enlever le caractère anonyme de Tor et identifier ses utilisateurs [48].

2.7 Analyse des paquets

Afin d'extraire les informations nécessaires pour la création des règles Tor et I2P, l'analyse est divisée en deux parties. L'établissement d'une connexion « TCP Three-Way Handshake » et la création d'une session sécurisée du protocole TLS appelé « TLS Handshake ».

Ces deux méthodes sont expliquées dans ce qui suit, et leurs résultats sont démontrés dans le prochain chapitre.

2.11.1 TCP Three-Way Handshake

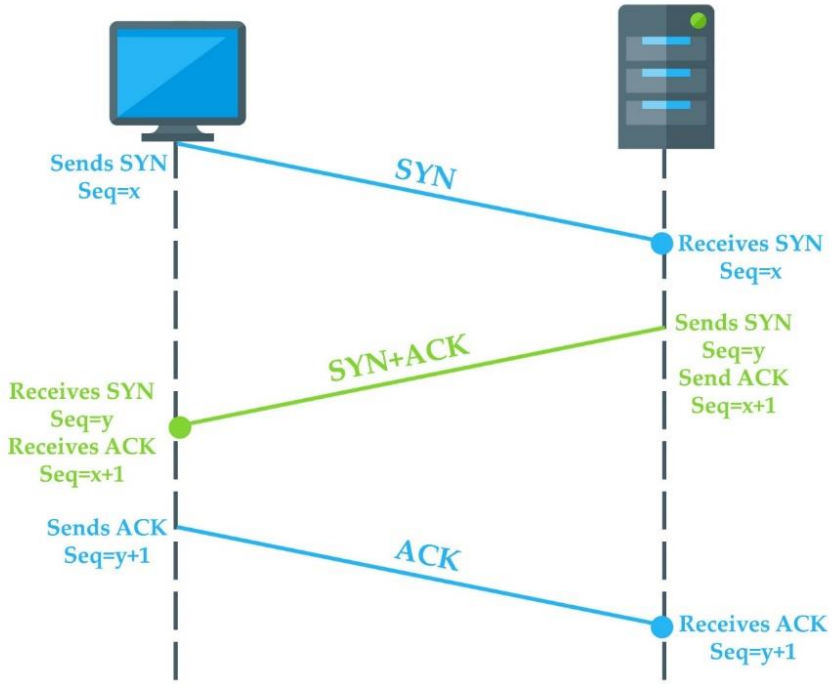


Figure 2.11.1: *TCP Three-Way Handshake.*

La figure ci-dessus montre que dans ce processus, le client envoi en premier lieu un paquet de synchronisation SYN au serveur. Ce dernier va répondre avec un paquet SYN+ACK, pour terminer avec le dernier paquet ACK que le client va envoyer. L'utilité du Three-Way Handshake est d'établir une connexion sécurisée et fiable entre deux appareils [49].

2.11.2 TLS Handshake

Le TLS Handshake démarre une session de communication en utilisant le cryptage TLS. TLS est un protocole de cryptage conçu pour la sécurité de la communication vers internet. Le client et serveur échangent des messages pour se reconnaitre, se vérifier et faire leur chiffrement grâce aux différents algorithmes afin de se partager les clés de session.

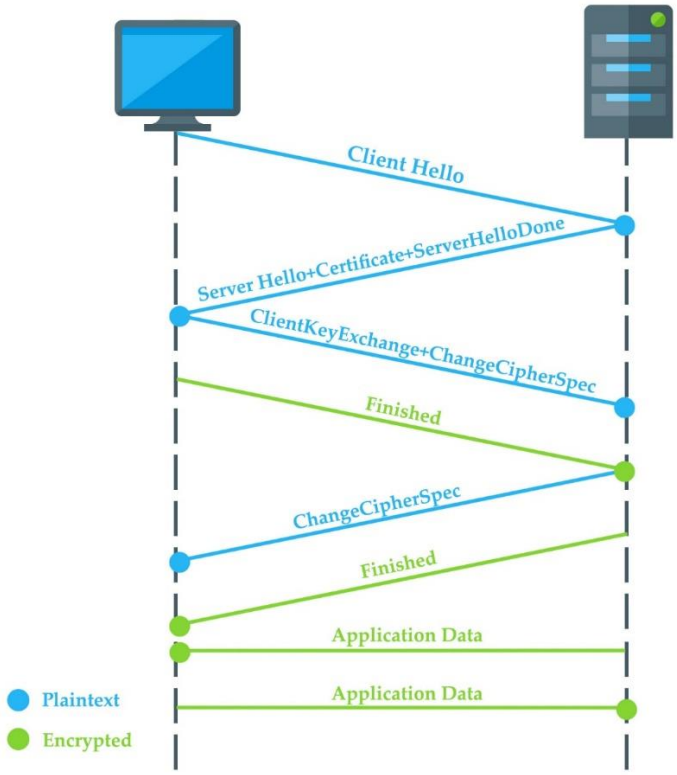


Figure 2.11.2: *TLS Handshake.*

2.11.2.1 Le message « Client Hello »

C'est le premier message que le client envoi. C'est une demande au serveur pour commencer l'établissement du TLS handshake.

Ce paquet contient la version du TLS, une valeur aléatoire qui permet de générer la clé pré-master (valeur qu'on obtient de lors l'échange des clés) et une liste de suite de chiffrement qui permet aux deux parties de se mettre en accord sur la suite de chiffrement à utiliser pour la communication.

Le serveur répond par la suite par 3 messages, le « Server Hello » « Certificate » et « Server Hello Done ».

2.11.2.2 Le message « Server Hello »

Ce message permet de confirmer si le serveur prend en charge la version TLS envoyée par le client ou pas, choisi une suite de chiffrement dans la liste du « Client Hello » et génère sa propre valeur aléatoire. Ce message contient aussi une version, une valeur aléatoire et une suite de chiffrement.

2.11.2.3 Le message « Certificate »

C'est un message qui est envoyé pour l'authentification. Le serveur envoie pour cela sa chaine de certificat SSL au client.

2.11.2.4 Le message « Server Hello Done »

Ce troisième message est pour dire au client que tous les messages ont été envoyés. Une fois que le client a reçu le certificat du serveur, il effectuera une série de vérification pour valider le certificat. Si le résultat est bon, le client envoie deux messages. Le « Client Key Exchange » et le « Change Cipher Spec »

2.11.2.5 Le message « Client Key Exchange »

Ce premier message dépend de l'algorithme de clé publique sélectionné pour l'échange et authentification. Donc à l'intérieur du paquet on trouve l'algorithme utilisé et ses paramètres (comme la taille de la clé et la valeur de celle-ci)

Après la réception de ce message par le serveur, ce dernier utilisera les paramètres de l'algorithme choisi et des valeurs aléatoires pour calculer la clé pré-master. Puis, les deux parties utiliseront cette clé là pour générer la clé de la session.

2.11.2.6 Le message « Change Cipher Spec »

Ce message est envoyé par le client puis le serveur et est utilisé pour informer l'autre partie du passage au cryptage.

2.11.2.7 Le message « Finished »

Ce message est utilisé pour informer la fin de l'échange de clé et authentification.

2.11.3 Exemple de suite de chiffrement

Un exemple de suite de chiffrement est montré dans la figure ci-dessous [50].

Figure 2.11.3: *Suite de chiffrement.*

2.8 Outils utilisés pour la réalisation de ce mémoire

2.12.1 Squid Proxy

Le proxy Squid est un cache proxy qui reçoit des requêtes venant de différents clients, les transmet au serveur Internet concerné et stocke l'information retournée par le serveur.

Figure 2.12.1: *Logo du Squid Proxy [51].*

Si l'information est demandée plusieurs fois, alors le contenu stocké sera retourné aux clients, ce qui réduit la bande passante utilisée et accélère les opérations.

Par défaut, Squid écoute sur toutes les interfaces réseau sur le port 3128, port dédié aux serveurs proxy.

Son utilité dans ce projet est de vérifié la fiabilité du travail fourni. Si les règles créées par la suite arrivent à détecter les réseaux anonymes, le proxy pourra les bloquer. Si cela n'est pas fait, une vérification des règles introduit est indispensable [52].

2.12.2 Wireshark

Wireshark est un logiciel de capture et analyse de trames sur Ethernet qui permet le contrôle du bon fonctionnement du réseau.

Figure 2.12.2: *Logo Wireshark [53].*

Ce logiciel a été choisi pour ses nombreux avantages comme le fait qu'il contient plusieurs opérations tels le calcul du débit moyen sur la durée de la capture en Mbps, le traçage d'un graphe du trafic, le filtrage, l'indication des erreurs et alertes détectées ainsi que pleins d'autres fonctionnalités.

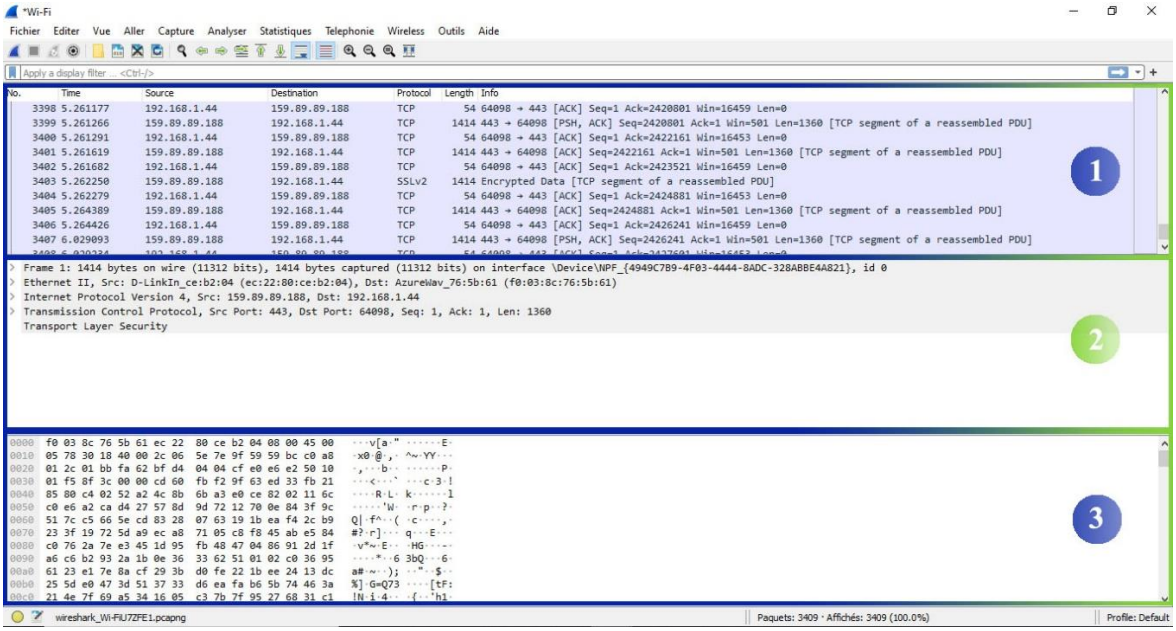


Figure 2.12.3: *Interface Wireshark.*

- La première section affiche la liste des paquets capturés.
- La deuxième section donne des détails sur le paquet sélectionné.
- La troisième section donne le code hexadécimal du paquet [54].

2.12.3 Les IDS

Un système de détection d'intrusion permet la détection précise du trafic malveillant selon 2 méthodes de détection :

- Les signatures d'attaques connues : Signatures comparées et recherchées dans la base de données de l'IDS.

- La détection d'anomalie : Alerte générée lors d'un comportement anormal du système.

Dans un IDS, un faux positif est un paquet qui ne représente aucune menace, mais qui génère une alerte quand même. Tandis qu'un faux négatif représente une intrusion non-détecté par ce dernier.

2.12.3.1 Présentation générale de Suricata

Suricata est un moteur de détection de menaces open source très appréciable par les internautes. Il est un NIDS « Network-based Intrusion Detection System », c'est-à-dire un système de détection basé sur le réseau. Son travail consiste à analyser les paquets entrants afin de les prendre en charge en cas de leur présence. Cette mise-en-charge dépend de la gravité du paquet présentant un danger.

Figure 2.12.4: *Logo Suricata [55].*

Suricata fonctionne pour être un :

- Système de détection d'intrusion « IDS », outil de détection et de surveillance qui n'applique aucune action par lui-même, les résultats nécessitent l'évaluation d'un administrateur.
- Système de prévention d'intrusion « IPS », système de contrôle qui accepte et rejette un paquet en fonction de l'ensemble de règles. Il exige que la base de données soit régulièrement mise à jour avec de nouvelles données sur les menaces.
- Moteur de surveillance de la sécurité du réseau « NSM », pour une détection et blocage d'attaque de hautes performances.

Ce moteur de détection d'intrusion est disponible pour Linux, FreeBSD, OpenBSD, macOS/ Max OS X et Windows [56].

2.12.3.2 Architecture de Suricata

L'architecture de Suricata est présentée dans la figure qui suit [56] :

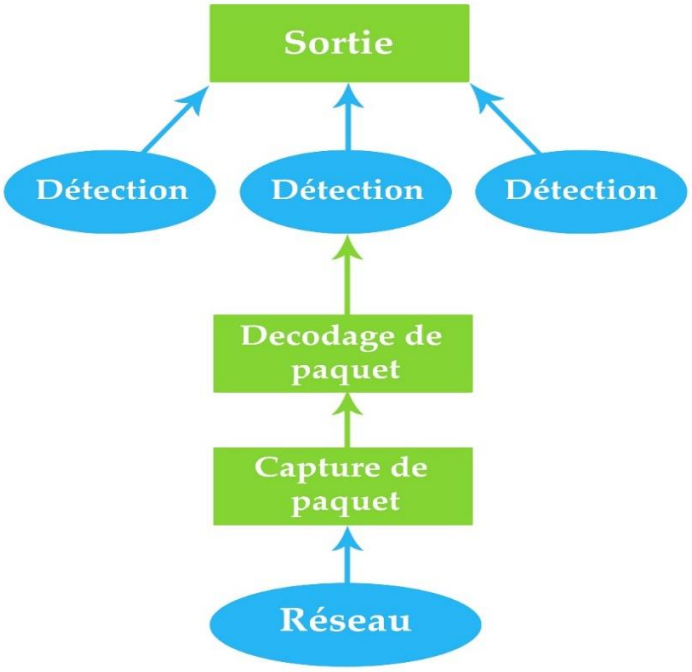


Figure 2.12.5: *Architecture de Suricata.*

L'architecture est donc très simples, les paquets sont capturés puis analysés. Les règles sont par la suite utilisées pour détecter l'intrusion et la traiter à la fin.

2.12.3.3 Présentation générale de Snort

Snort est un système de détection d'intrusion réseau Open Source et gratuit, qui peut être utilisé sur différents système d'exploitation tels que Windows et Linux.Il permet d'analyser le trafic en temps réel et l'enregistrement des paquets sur les réseaux IP. Il a recourt à une série de règles permettant de détecter une activité malveillante.

En analysant le trafic, il compare et cherche les ressemblances entre le trafic et les règles puis génère des alertes lorsqu'il y a correspondance.

Figure 2.12.16: *Logo Snort [57].*

Snort détient une base de signatures mise-à-jour régulièrement. Il est basé sur libpcap qui est une interface qui permet la capture d'un trafic réseau. Il peut fonctionner selon trois modes :

Le mode sniffer (hors ligne) : Lecture des paquets circulants sur le réseau et affichage de façon continue sur l'écran.

Le mode packet logger : Enregistrement du trafic réseau dans des répertoires sur le disque

Le mode détecteur d'intrusion réseau NIDS : Analyse du trafic, comparaison avec les règles et déclenchement d'alerte s'il y'a correspondance [58].

2.12.3.4 Architecture Snort

L'architecture de Snort est présentée dans la figure qui suit [42] :

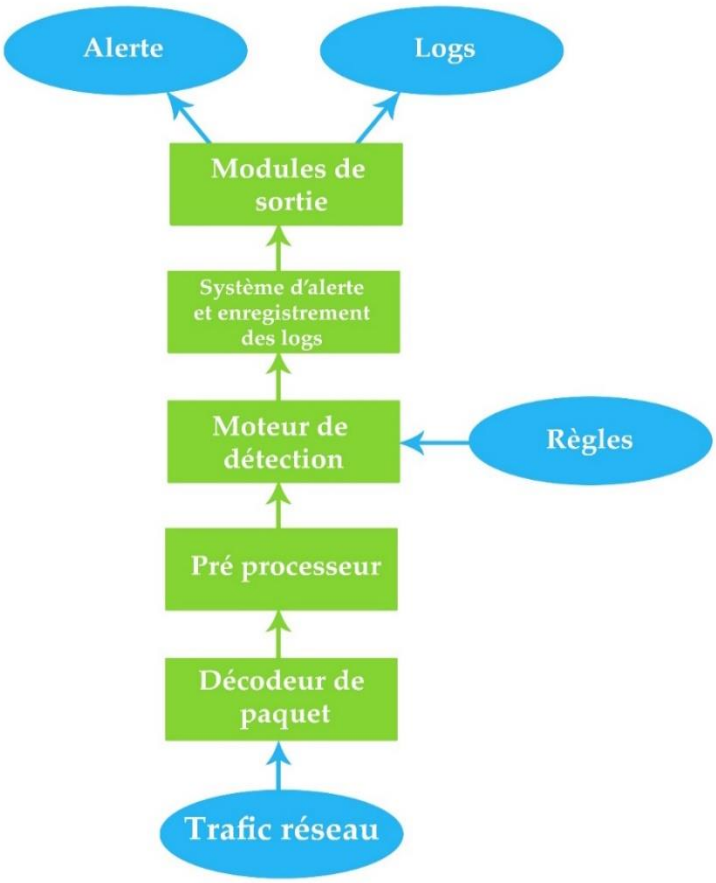


Figure 2.12.17: *Architecture de Snort.*

- Le décodeur de paquet capture et analyse les paquets. Il est composé de plusieurs sous-décodeurs organisés par protocole. Les éléments de ces derniers vont être transformés en une structure de données.
- Le préprocesseur est un programme présent pour détecter les anomalies.
- Le moteur de détection est le composant le plus important ici. Il détecte, grâce aux règles, les intrusions.
- Le système d'alerte quant à lui est là pour la génération des logs et alertes.
- Le module de sortie à la fin traite l'intrusion.

2.9 Conclusion

Les dangers liés à la navigation sur internet rendent nécessaire la protection de l'identité des internautes et le maintien de leur confidentialité. Malgré leurs limites, I2P et Tor sont les deux réseaux anonymes les plus avantageux pour cela. Néanmoins, les menaces que ces deux derniers présentent ne doivent pas être prises à la légère non plus.

Dans le prochain chapitre, des signatures numériques de chaque réseau seront extraites afin de créer des règles qui permettent la détection de l'utilisation des réseaux Tor et I2P.

Chapitre 3

Extraction des signatures numériques

3.1 Introduction

A travers les chapitres précédents, la nécessité de l'anonymat lors d'une navigation sur internet a été prouvée. Les réseaux anonymes ont pour rôle principal de garantir la confidentialité et de protéger contre la surveillance du trafic de données. Cependant, ils ne sont pas toujours utilisés à bon escient, la détection de leur utilisation dans un réseau représente le but de cette étude afin de contrer les personnes malveillantes.

L'étude de ce chapitre se fera comme suit :

Premièrement, la capture et l'analyse des paquets avec Wireshark.

Ensuite, l'analyse détaillées des paquets des différents réseaux anonymes et navigateurs, afin d'extraire les différentes caractéristiques propres à chacun.

3.1.1 L'objectif de cette recherche

L'objectif de la recherche est d'identifier l'utilisation des réseaux anonymes dans un réseau, après avoir extrait des empreintes numériques de l'analyse des paquets et les avoir implémentés dans un IDS.

3.1.2 Plan de travail

Afin de résoudre la problématique et apporter une solution, le déroulement de ces étapes à était suivie :

L'analyse de la documentation : C'est l'approche théorique afin de comprendre les mécanismes de la recherche.

La capture des données : C'est l'analyse détaillée du trafic de données en utilisant l'analyseur de paquet Wireshark.

L'analyse des données : La comparaison des différents paquets capturés permettant d'extraire les empreintes numériques propres à chaque réseau.

La détection mise en pratique : Implémenter les empreintes numériques dans un IDS afin de détecter l'utilisation des réseaux anonymes puis tester la fiabilité de la solution.

3.2 Environnement de travail

Pour réaliser ce projet, une suite d'équipements et logiciels est nécessaire.

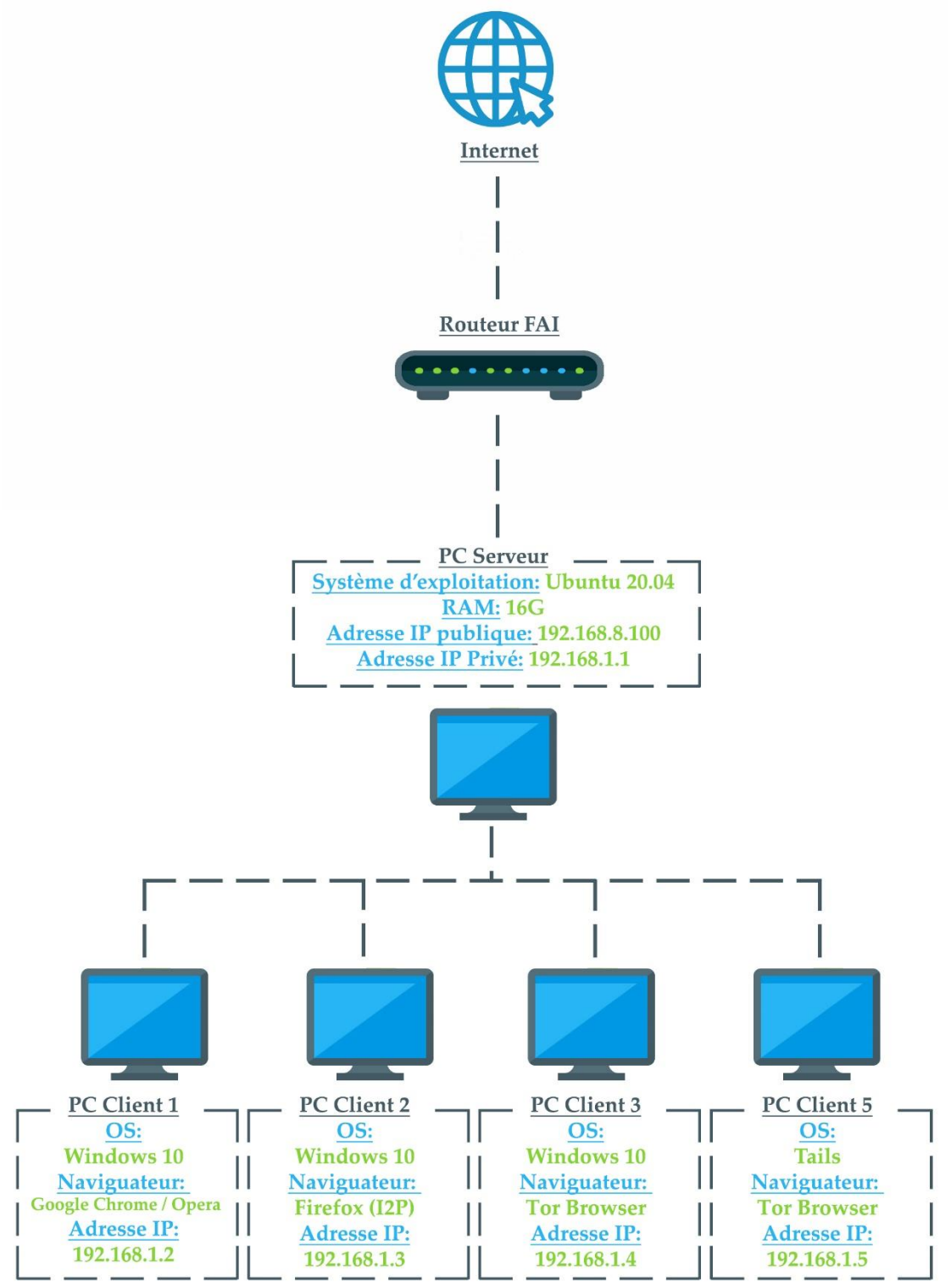


Figure 3.2.1: *Environnement de travail.*

3.3 Architecture

La figure 3.2.1 montre que l'architecture suivie ici est une architecture client-serveur qui désigne l'environnement dans lequel des applications de machines clientes communiquent avec des applications de machines serveurs.

3.3.1 Fonctionnement

Le client émet une requête vers le serveur grâce à son adresse IP et port.

Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et port.

3.4 Partage de connexion

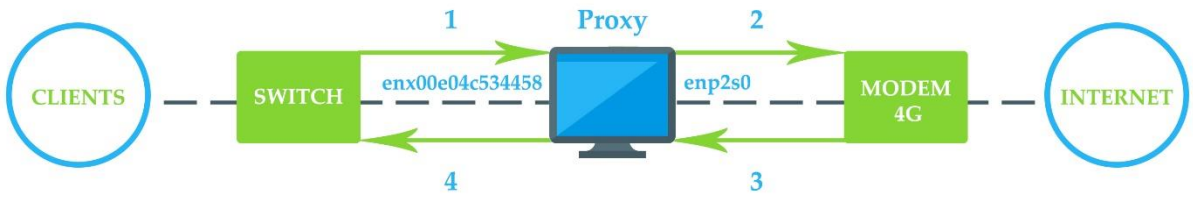


Figure 3.4.1: *Partage de connexion.*

La figure 3.4.1 montre que le PC serveur a deux cartes réseaux. Il est connecté à internet grâce à un routeur à travers l'interface « enp2s0 », et le partage vers les clients se fait à travers un switch. L'interface est « enx00e04c534458 »

Afin que les paquets venant des clients puissent franchir la passerelle et sortir vers Internet, il faut configurer le NAT, Network Address Translation. Dans le cas de ce mémoire, cela se fait grâce à la méthode des Iptables.

3.5 Iptables

C'est un pare-feu de filtrage de paquets gratuit qui inclut une table, une table inclut des chaînes, et les chaînes incluent des règles.

Il faut surtout se rappeler que les paramètres Iptables doivent être configurés à chaque démarrage car ils ne sont pas enregistrés automatiquement.

3.5.1 Configuration

Les commandes utilisées pour cela sont présentées dans la figure ci-dessous.

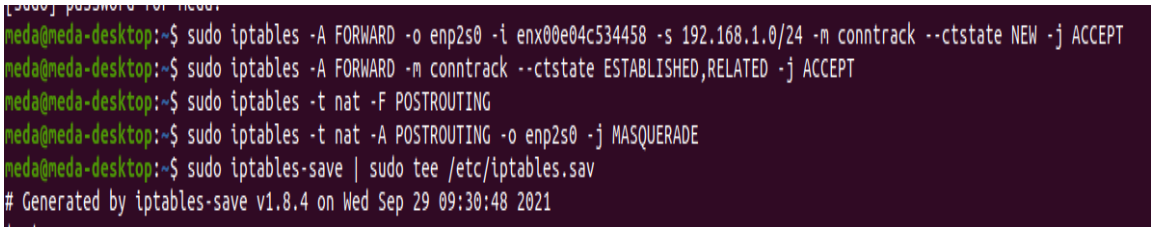


Figure 3.5.1: *Configuration de l'Iptables.*

- La première règle autorise les paquets transférés (les initiaux).
- La deuxième règle permet le transfert des paquets de connexion établis (et ceux liés à ceux qui ont commencé).
- La troisième règle fait le NAT.

3.5.2 Explication des commandes

- -A : Ajoute cette règle à la chaîne « FORWARD » (les autres chaines sont INPUT, OUTPUT)
- -m conntrack : Autorise les règles de filtrage en fonction de l'état de connexion.
- -j : Aller à la cible spécifié (il y'a 4 cibles, « ACCEPT » pour accepter le paquet, « REJECT » pour le rejeter, « DROP » pour ignorer le paquet et « LOG » pour enregistrer le paquet)
- -i : N'est accepté que si le paquet arrive sur l'interface spécifiée.
- -o --out-interface : nom de sortie [+] nom de l'interface réseau [59].

3.6 Les directives à connaître

Les ACL (Access Control List) sont des critères de contrôle d'accès utilisés par la directive « http_access » afin d'autoriser ou interdire les connexions http.

Dans le cas de ce projet, des sites comme Facebook et YouTube ont été bloqués. La figure ci-dessous montre un exemple de cela [60].

```
acl block_websites dstdomain .facebook.com .youtube.com
http_access deny block_websites
#  TAG: proxy_protocol_access
```

Figure 3.6.1: *Configuration des ACLs.*

Les figures qui suivent montrent l'efficacité du proxy Squid. Facebook et YouTube ont bien été bloqués.

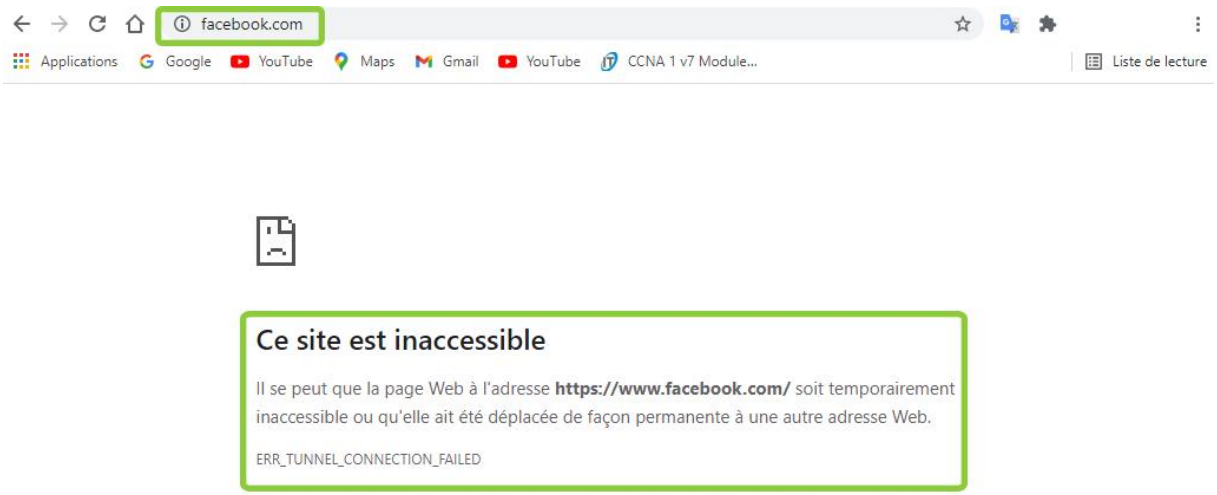


Figure 3.6.2 : *Facebook bloqué.*

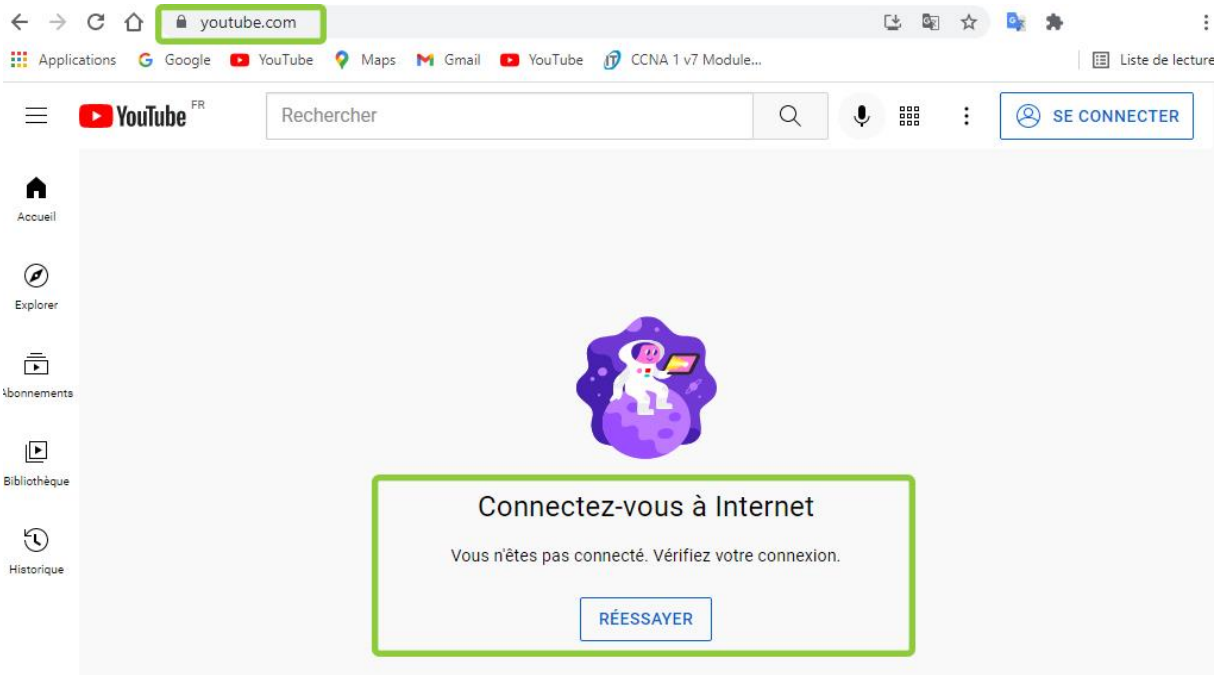


Figure 3.6.3 : *YouTube bloqué.*

3.7 Tor

3.7.1 Etapes d'établissement de connexion entre navigateur Tor et le nœud d'entrée du réseau Tor

Après avoir téléchargé le réseau TOR, vient le lancement du navigateur Tor.

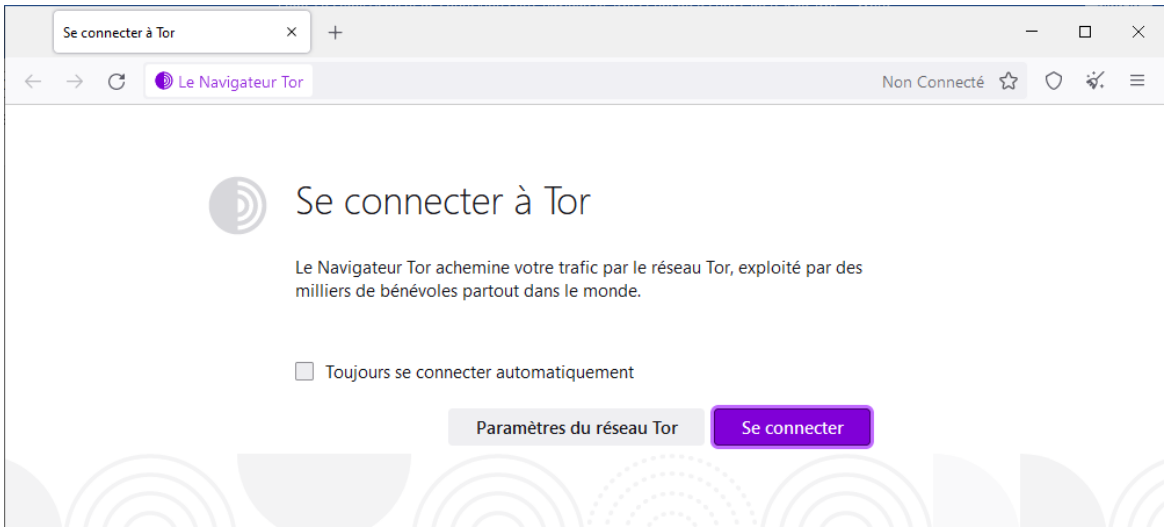


Figure 3.7.1: *Etablissement d'une connexion à Tor.*

Il faut appuyer sur « Se connecter »

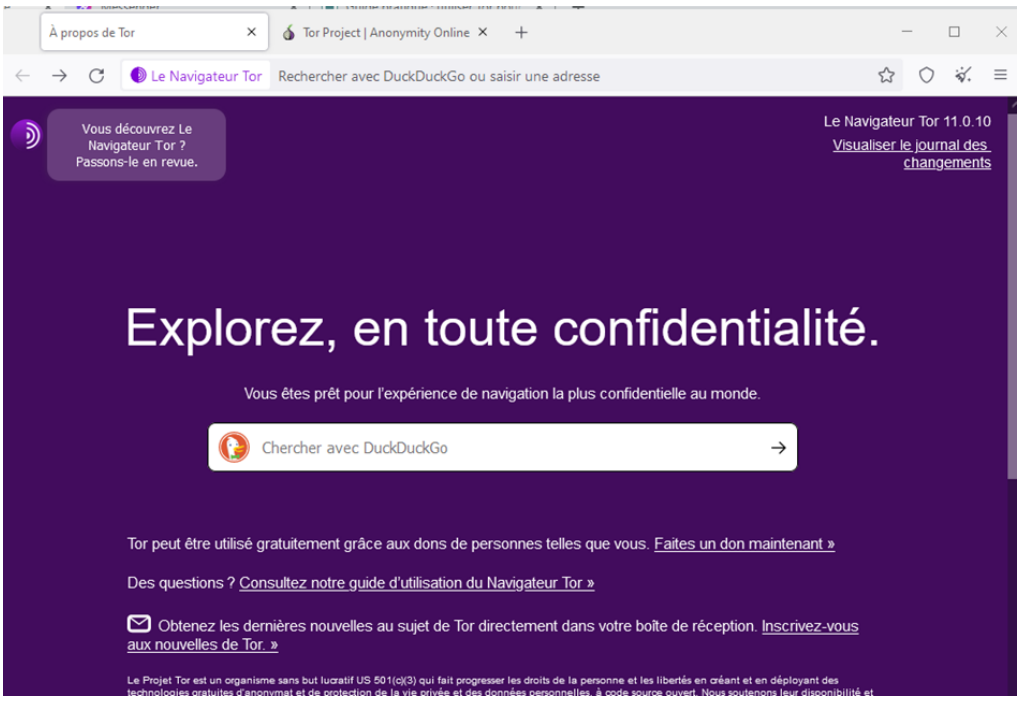


Figure 3.7.2: *Fenêtre de navigation de Tor.*

La barre de recherche du navigateur DuckDuckGo s'affiche.

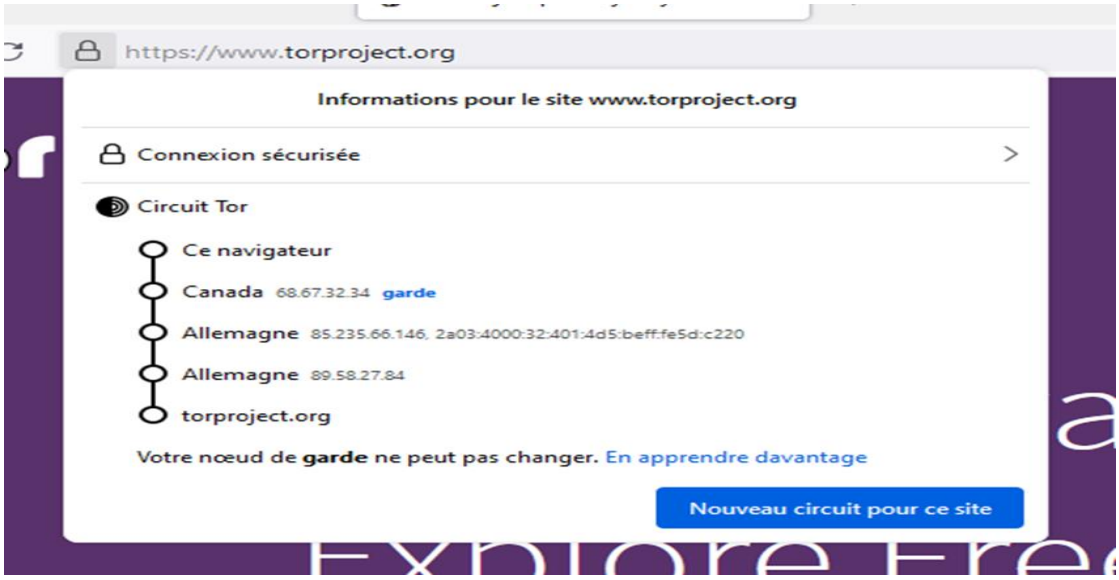


Figure 3.7.3: *Circuit Tor lors de la connexion au site torproject.org*

Le navigateur Tor établit une connexion à travers différentes adresses.

https://metrics.torproject.org/rs.html est un outil de recherche de relais Tor, il suffit d'introduire une adresse IP, un surnom ou une empreinte digitale afin d'avoir plus de détails dessus.

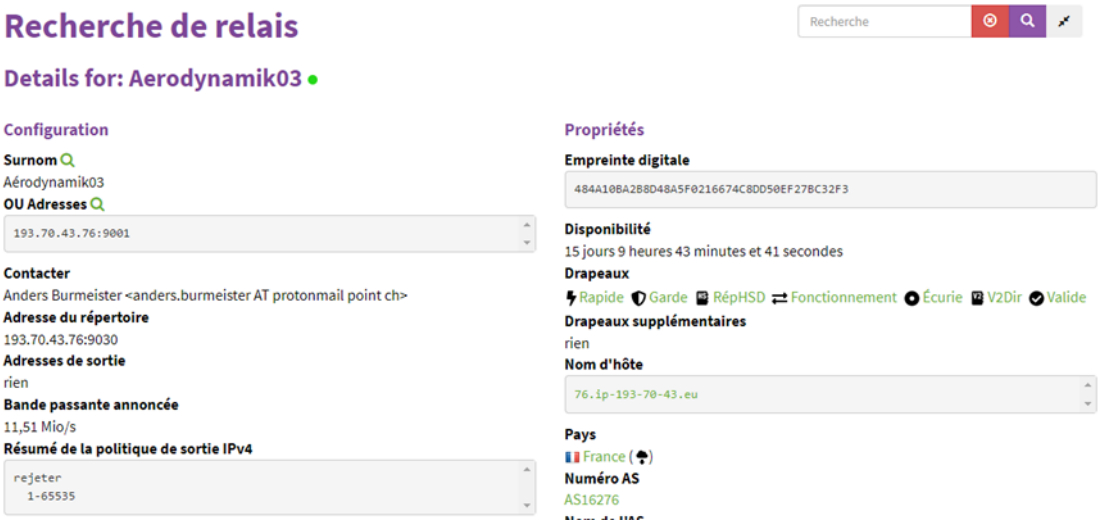


Figure 3.7.4 : *Détail du premier nœud de garde.*

Il a été démontré que l'adresse IP 193.70.43.76 est bien un nœud de garde Tor en utilisant Tor Metrics.

3.8 I2P

Dans I2P, la sécurité de la connexion est de haut niveau grâce aux tunnels proxy entrants et sortants. Ce système de routage garlic crée un réseau qui rend le traçage et le piratage des messages beaucoup plus difficile que les autres réseaux d'anonymat.

3.8.1 Comment utiliser I2P

Installer I2P.

Ouvrir Start I2P (restartable).

Ouvrir un navigateur et configurer le proxy.

3.8.2 Comment configurer le navigateur

Le navigateur utilisé pour cela est Firefox.

Il faut accéder aux paramètres réseaux puis, sélectionner la configuration manuelle du proxy et définir l'adresse proxy http « 127.0.0.1 » et le port « 4444 ». Ainsi que l'adresse proxy https « 127.0.0.1 » et le port « 4445 » [61].

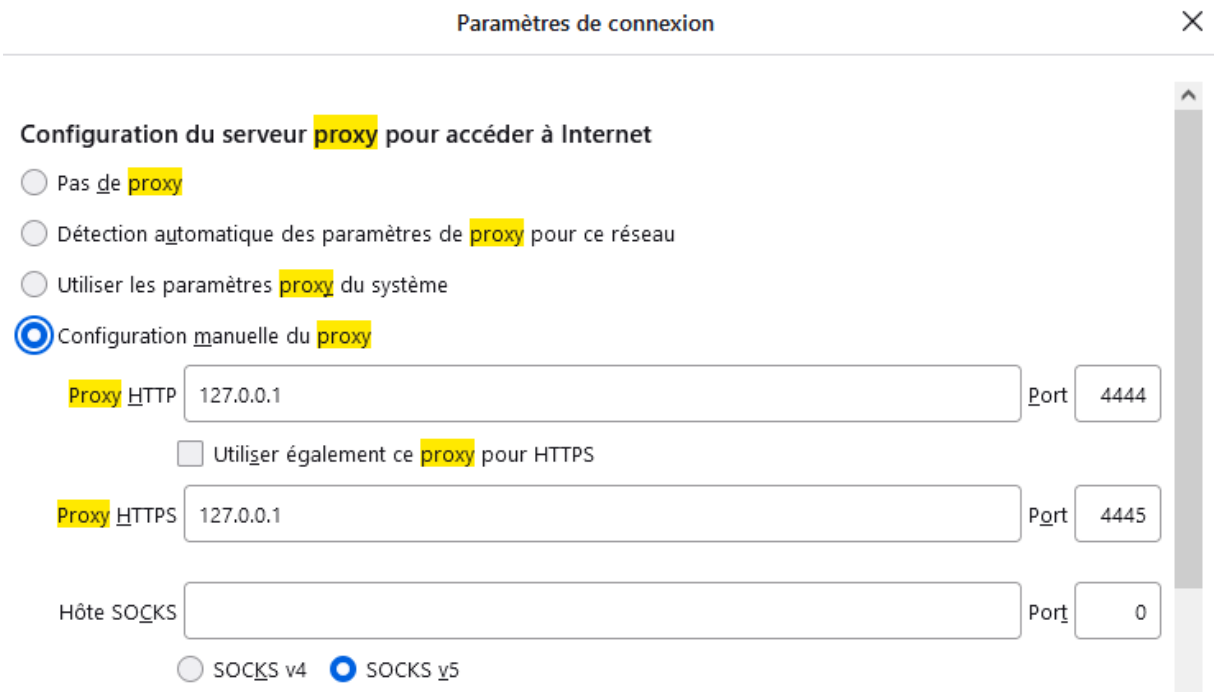


Figure 3.8.1: *Configuration Firefox.*

3.9 Extraction des signatures

3.9.1 Informations extraites du TCP Three-Way Handshake pour Google Chrome, Opera, Firefox et Tor

Les paquets SYN, SYN-ACK et ACK contiennent les informations mentionnées ci-dessous.

- Port Source : numéro de port de l'expéditeur.
- Port Destination : numéro de port du destinataire.
- MSS : Le MSS ou Maximum Segment Size est la taille maximale du segment de données applicatives que l'émetteur est prêt à accepter dans un seul paquet. La valeur maximale dans le cas de l'Ethernet est 1460.
- Longueur totale : la longueur du paquet incluant l'entête IP et les data associées.
- Identification : Valeur qui identifie les fragments d'un même paquet à être reconstituer.
- TTL : la durée de vie maximale qu'un paquet peut atteindre. Le paquet sera détruit si la valeur du TTL arrive à 0.
- Numéro de séquence : correspondant au numéro du paquet et son emplacement par rapport aux autres paquets dans le flux de données.
- Stream Index : Ceci est un mappage Wireshark interne qui identifie un flux TCP unique. Les paquets du même flux TCP ont la même valeur de ce champ-là.
- Flags : permet d'activer des actions TCP qui permettent l'organisation et communication de la transmission de la donnée. Les flags peuvent êtres : un champ URG qui est le pointeur de donnée urgente, un champ ACK indiquant la validité du numéro de séquence, un champ PSH qui demande au récepteur de délivrer les données à l'application sans attendre le remplissage des tampons.
- Window Size Value : Champ indiquant la quantité de donnée à transmettre. C'est la taille du tampon sur l'ordinateur source.
- RTT to ACK : Le Round Time Trip to ACKnowledgement représente le temps entre l'émission d'un paquet et réception de l'ACK correspondant [41].

3.9.1.1 SYN

Les paquets SYN, SYN-ACK et ACK contiennent une multitude d'informations exploitables sur le trafic réseau, leur comparaison est réalisée afin d'étudier la possibilité de déduire des caractéristiques propres à chaque réseau.

	Google Chrome	Opera	Firefox	Tor port 9001	Tor port aléatoire	Tor port 443
Type	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)
Protocole	TCP (6)	TCP (6)	TCP (6)	TCP (6)	TCP (6)	TCP (6)
IP source	192.168.1.3	192.168.1.3	192.168.1.4	192.168.1.3	192.168.1.3	192.168.1.3
IP Destination	192.168.1.1	20.199.120.182	192.168.1.1	193.70.43.76	147.78.125.8	188.114.140.233
Port source	50402	49758	35636	64380	55443	53719
Port Destination	3128	443	3128	9001	8104	443
MSS	1460 bytes	1460 bytes	1460 bytes	1460 bytes	1460 bytes	1460 bytes
Longueur totale	52	52	60	52	52	52
Identification	0x53ed (21485)	0x739b (29595)	0xb950 (47440)	0xb791 (46993)	0x671d (26397)	0xcb49 (52041)
TTL	128	128	64	128	128	128
Numéro de séquence	0	0	0	0	0	0
Stream index	2	9	1	0	0	0
Flags	0x002 (SYN)	0x002 (SYN)	0x002 (SYN)	0x002 (SYN)	0x002 (SYN)	0x002 (SYN)

Windows size value	64240	64240	64240	64240	64240	64240

Tableau 3.9.1: *Informations paquet SYN.*

3.9.1.2 SYN-ACK

	Google Chrome	Opera	Firefox	Tor port 9001	Tor port aléatoire	Tor port 443
Type	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)
Protocole	TCP (6)	TCP (6)	TCP (6)	TCP (6)	TCP (6)	TCP (6)
IP source	192.168.1.1	20.199.120.182	192.168.1.1	193.70.43.76	147.78.125.8	188.114.140.233
IP Destination	192.168.1.3	192.168.1.3	192.168.1.4	192.168.1.3	192.168.1.3	192.168.1.3
Port source	3128	443	3128	9001	8104	443
Port Destination	50402	49758	35636	64380	55443	53719
MSS	1460 bytes	1400 bytes	1400 bytes	1400 bytes	1400 bytes	1400 bytes
Longueur totale	52	52	60	60	52	52
Identification	0x0000 (0)	0x6318 (25368)	0x0000 (0)	0x0000 (0)	0x0000 (0)	0x0000 (0)
TTL	64	107	64	46	50	38
Numéro de séquence	0	0	0	0	0	0
Stream index	2	9	1	0	0	0
Flags	0x012(SYN,ACK)	0x012(SYN,ACK)	0x012(SYN,ACK)	0x012(SYN,ACK)	0x012(SYN,ACK)	0x012(SYN,ACK)
Window size value	64240	8192	65160	64240	64240	64240

RTT TO ACK	0.0.000 63834 seconds	0.082629117 seconds	0.000062710 seconds	0.080697396seconds	0.144453392	0.0943363335

Tableau 3.9.2: *Informations paquet SYN-ACK.*

3.9.1.3 ACK

	Google Chrome	Opera	Firefox	Tor port 9001	Tor port aléatoire	Tor port 443
Type	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)	IPV4(0x0800)
Protocole	TCP (6)	TCP (6)	TCP (6)	TCP (6)	TCP (6)	TCP (6)
IP source	192.168.1.1	192.168.1.3	192.168.1.4	192.168.1.3	192.168.1.3	192.168.1.3
IP Destination	192.168.1.3	20.199.120.182	192.168.1.1	193.70.43.76	147.78.125.8	188.114.140.233
Port source	3128	49758	35636	64380	55443	53719
Port Destination	50402	443	3128	9001	8104	443
Longueur totale	40	40	52	40	40	40
Identification	0x53ee (21486)	0x739c (29596)	0x57b8 (22456)	0xb792 (46994)	0x671e (26398)	0xcb4a (52042)
TTL	128	128	64	128	128	128
Numéro de séquence	1	1	1	1	1	1
Stream index	2	9	1	0	0	0
Flags	0x010 (ACK)	0x010 (ACK)	0x010 (ACK)	0x010 (ACK)	0x010 (ACK)	0x010 (ACK)
Window size value	501	1028	502	1028	1028	263168

RTT TO ACK	0.000684436 seconds	0.000834432 seconds	0.000557265 seconds	0.018188426 seconds	0.007526438 seconds	0.004290640 seconds

Tableau 3.9.3: *Informations paquet ACK.*

3.9.1.4 Constatation

- Le port source est un port alloué dynamiquement.
- Pour le port de destination, Google Chrome et Firefox utilisent le port TCP 3128, dédié au serveur proxy. Opéra utilise le port TCP 443, dédié au protocole HTTPS. Tor de son côté utilise 3 ports, le 9001, 443 et un port aléatoire qui est le 8104.
- Pour l'identification, la valeur dépend de chaque paquet, comme dans le cas du MSS, Longueur Totale, TTL, Numéro de Séquence, Stream Index, Flags, Window Size Value et le RTT to ACK.

L'établissement du TCP Three-Way Handshake est donc le même pour le réseau anonyme Tor que pour le réseau normal. Aucun élément ne permet de différencier leurs paquets TCP.

3.9.2 Comparaison du TLS Handshake entre Google Chrome et Tor

3.9.2.1 Message « Client Hello »

Tor port 443

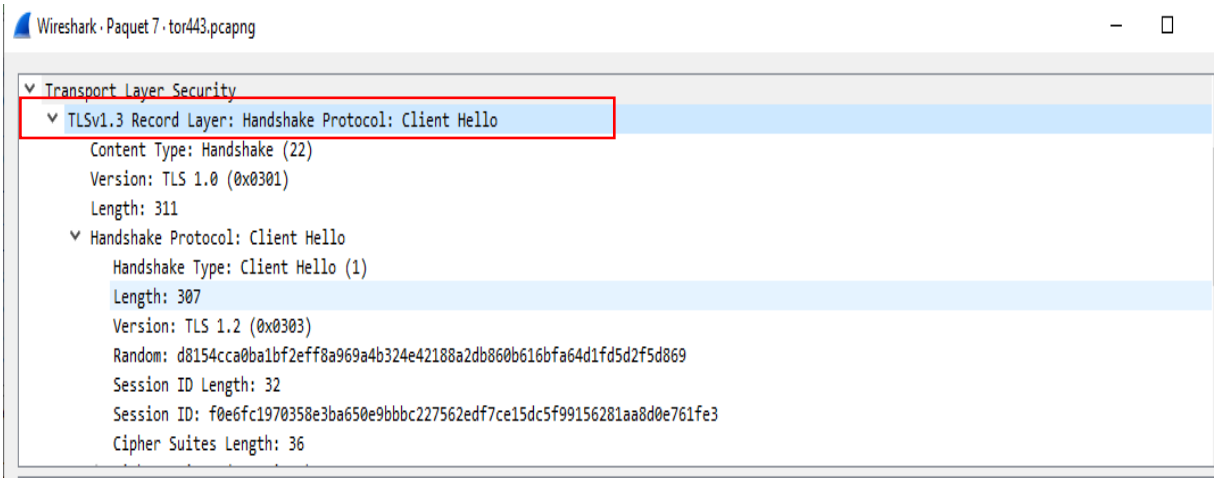


Figure 3.9.1 : *Message « Client Hello » envoyé par Tor port 443.*

Tor port aléatoire

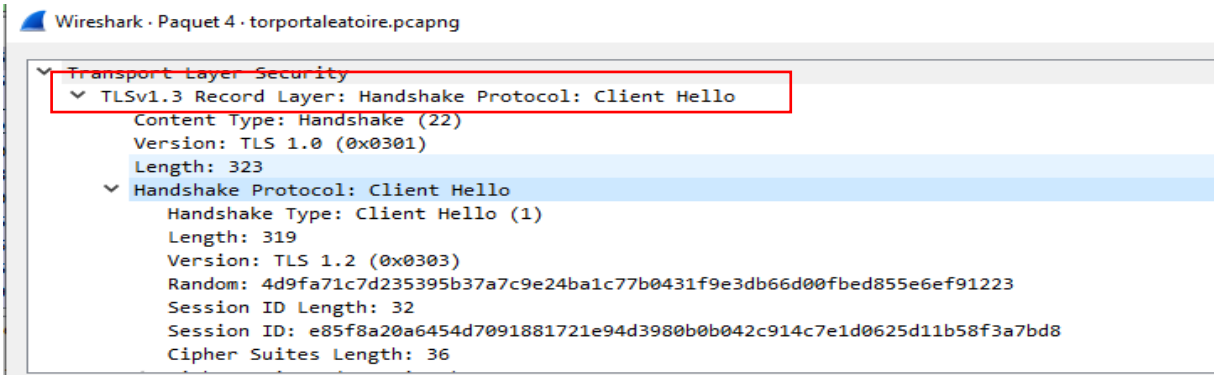


Figure 3.9.2 : *Message « Client Hello » envoyé par Tor port aléatoire.*

Tor port 9001

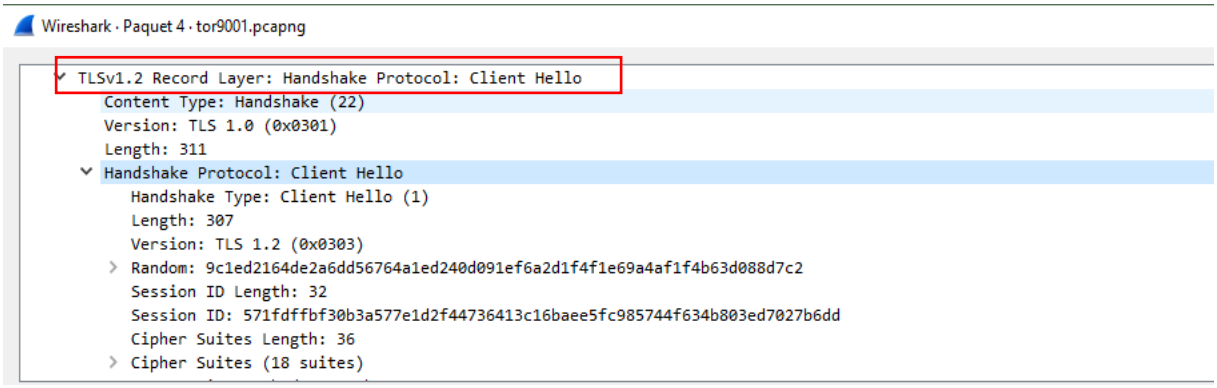


Figure 3.9.3 : *Message « Client Hello » envoyé par Tor 9001.*

Google Chrome

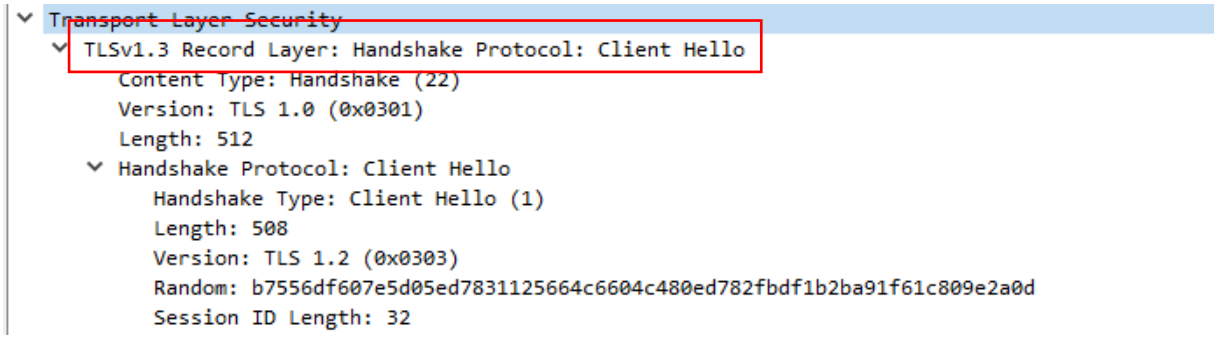


Figure 3.9.4 : *Message « Client Hello » envoyé par Google Chrome*.

La longueur totale « length » du message Client Hello envoyé par Google Chrome est fixé à 512 octets, tandis que pour Tor elle est variable, cependant elle avoisine les 300 octets.

Le nombre aléatoire Random, appartenant au TLS handshake est de 32 octets et est utilisé pour la création de la clé de chiffrement, il est propre à chaque paquet

3.9.2.2 Les suites de chiffrement proposées

Tor port 443

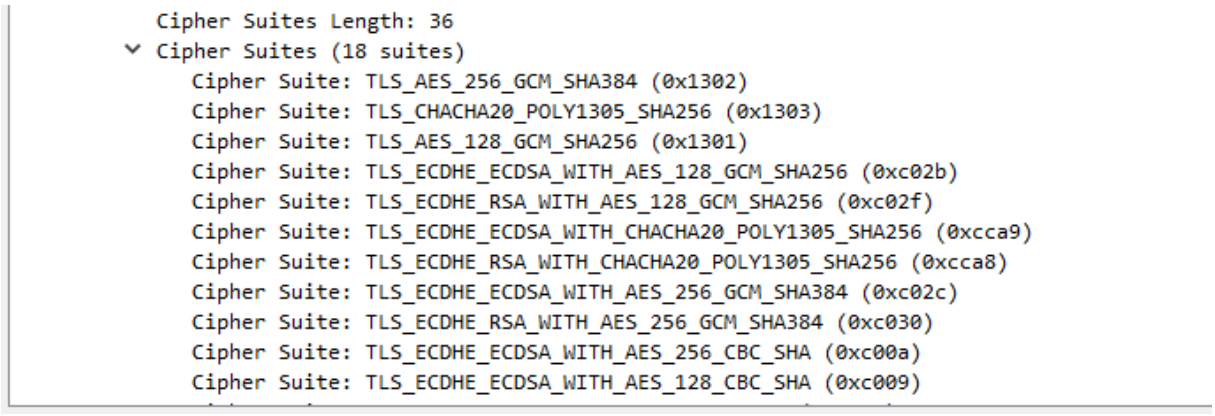


Figure 3.9.5 : *Les suites de chiffrement proposées par Tor port 443.*

Tor port aléatoire

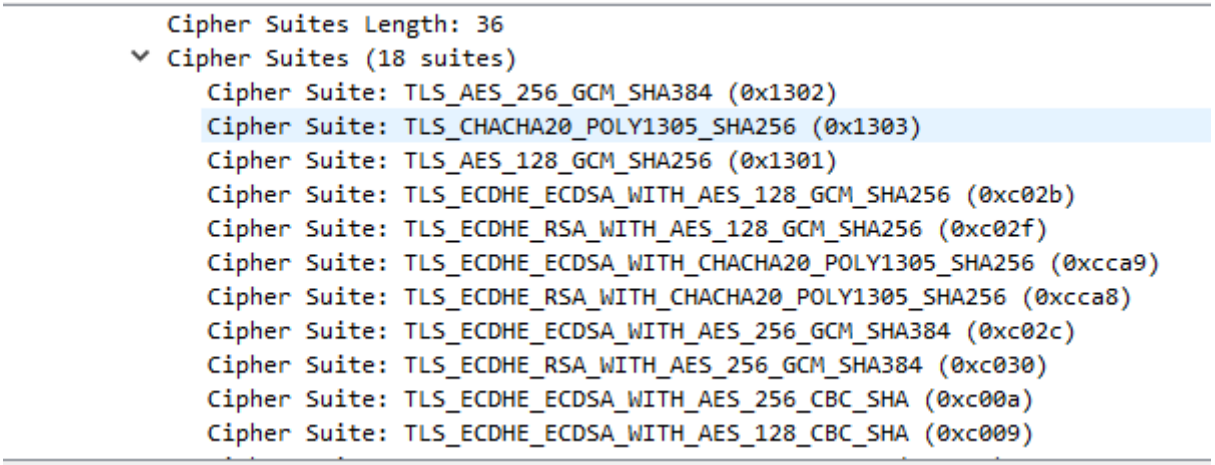


Figure 3.9.6 : *Les suites de chiffrement proposées par Tor port aléatoire.*

Tor port 9001

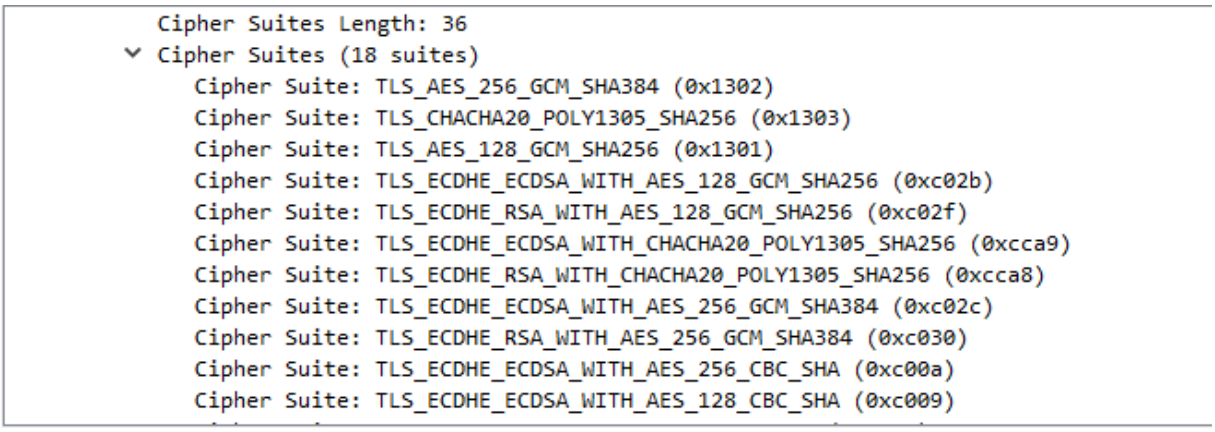


Figure 3.9.7 : *Les suites de chiffrement proposées par Tor port 9001.*

Google Chrome

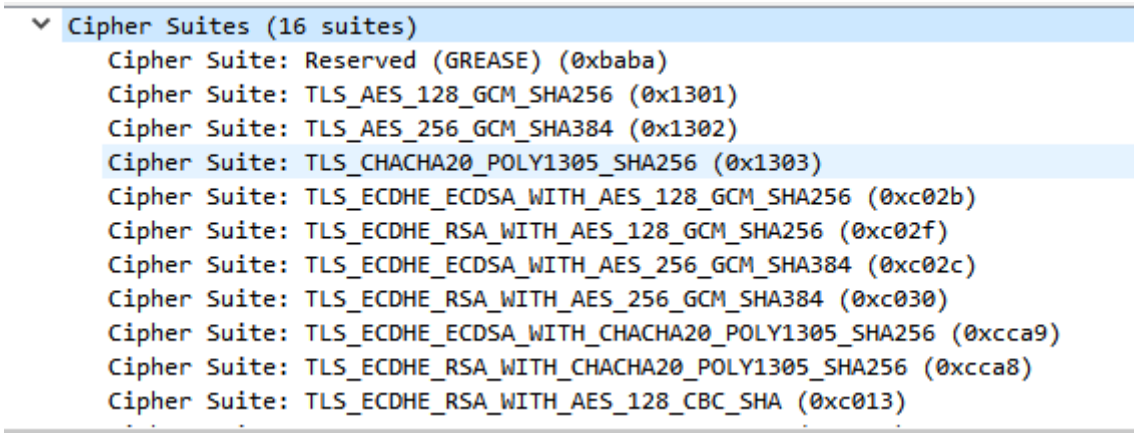


Figure 3.9.8 : *Les suites de chiffrement proposées par Google Chrome.*

Cipher suite est la liste des suites de chiffrement prises en charge par le client classées selon les préférences du client. La suite de chiffrement se compose d'un algorithme d'échange de clés, d'un algorithme de chiffrement en masse, d'un algorithme MAC et d'une fonction pseudo-aléatoire.

Tor contient 18 suites de chiffrement, quant à Google 16, tous dans un ordre bien précis.

Les navigateurs contiennent plusieurs extensions qui permettent d'augmenter la sécurité de l'échange. Le client précise les extensions qu'il prend en charge et le serveur décide quelles extensions appliquées.

3.9.2.3 Les extensions envoyées par le « Client Hello »

Port 443

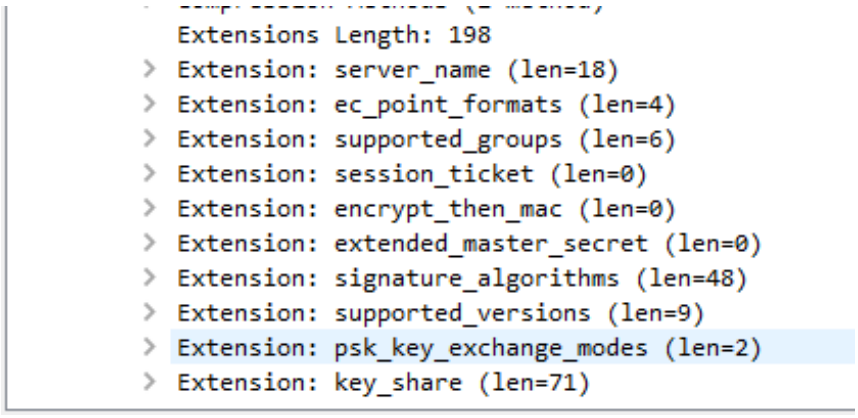


Figure 3.9.9 : *Les extensions envoyées par « le Client Hello » pour Tor port 443.*

Port aléatoire

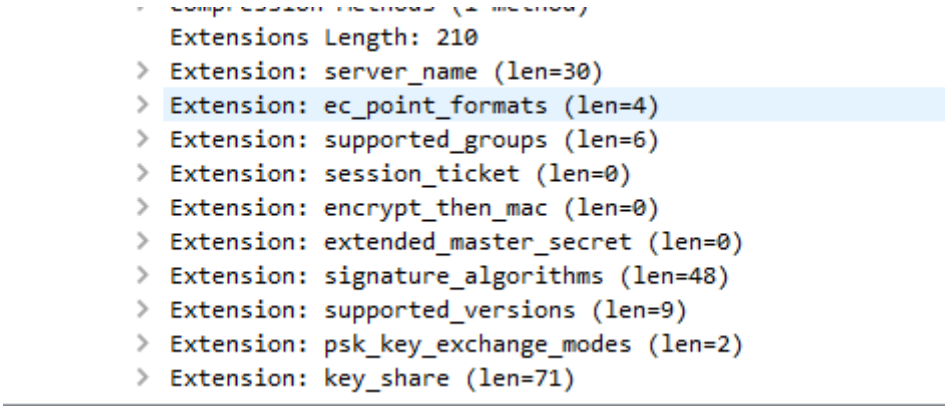


Figure 3.9.10 : *Les extensions envoyées par « le Client Hello » pour Tor port aléatoire.*

Port 9001

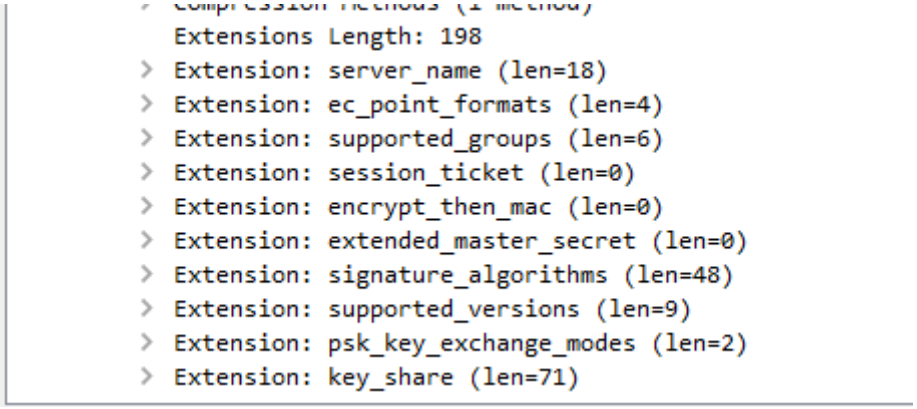


Figure 3.9.11 : *Les extensions envoyées par « le Client Hello » pour Tor port 9001.*

Google Chrome

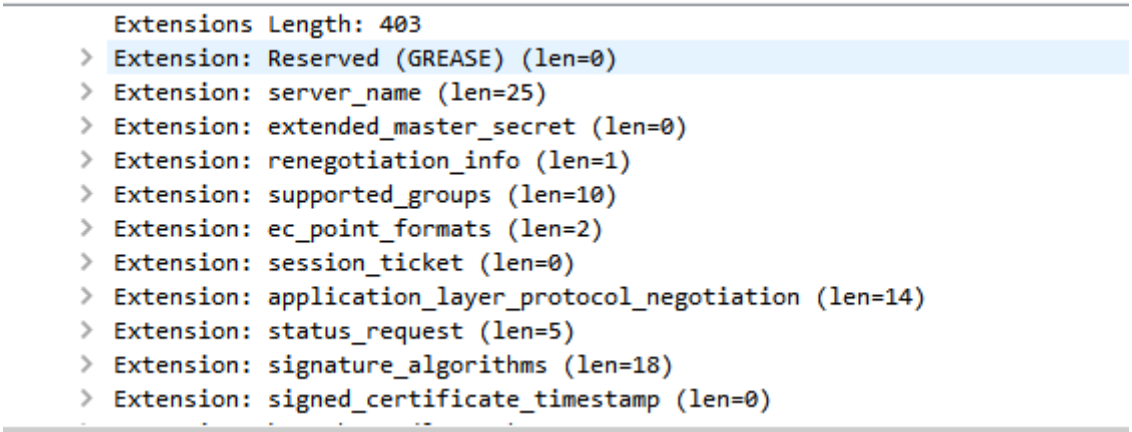


Figure 3.9.12 : *Les extensions envoyées par « le Client Hello » pour Google Chrome.*

Tor contient 10 extensions tandis que Chrome 18, certaines extensions se trouvent dans les 2 cas.

3.9.2.4 L'extension « ec_points_formats »

Tor 443

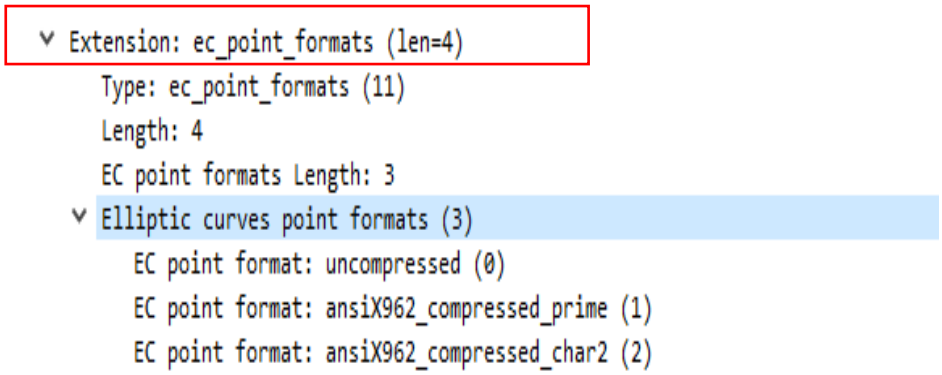


Figure 3.9.13 : *Extension «ec_points_formats» pour port 443.*

Tor 9001

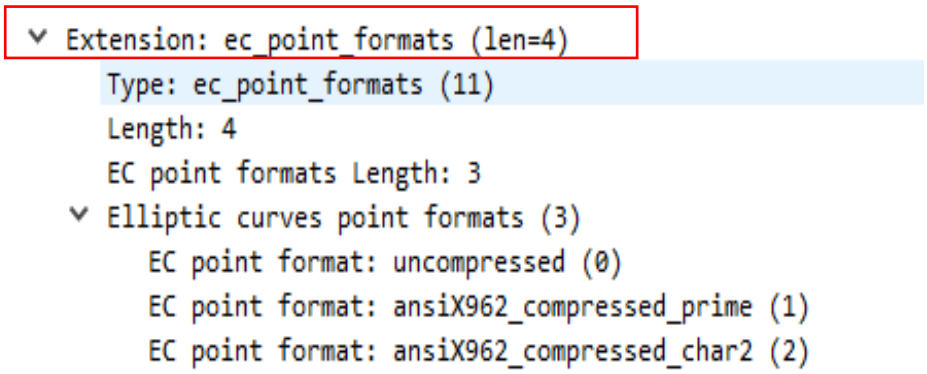


Figure 3.9.14 : *Extension «ec_points_formats» pour Tor port 9001.*

Tor aléatoire

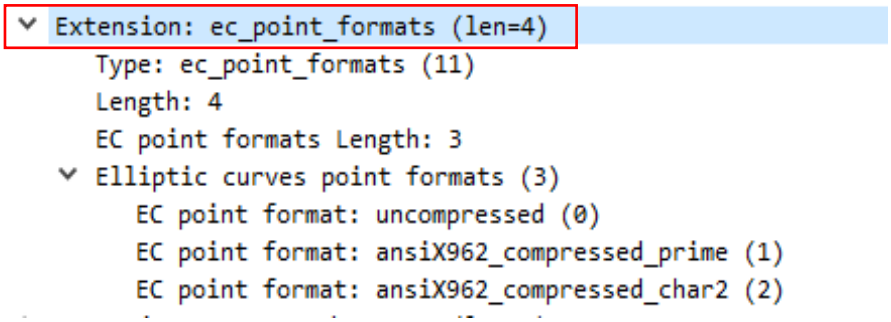


Figure 3.9.15 : *Extension «ec_points_formats» pour Tor port aléatoire.*

Google Chrome

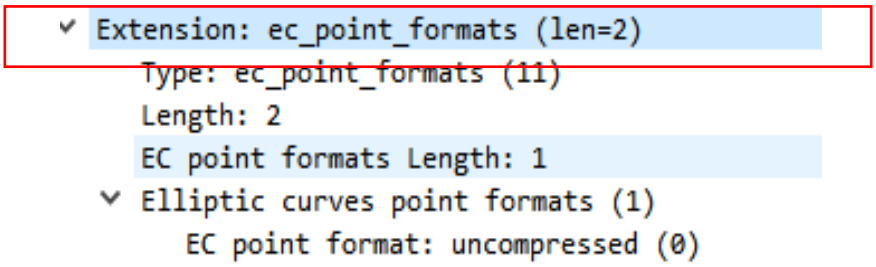


Figure 3.9.16 : *Extension «ec_points_formats» pour Google Chrome.*

Cette extension renseigne sur les formats de point de courbe elliptique pris en charge par le client ou le serveur.

Elle est étudiée pour une question de sécurité, les courbes elliptiques sont bien adaptées à la cryptographie.

Pour ce qui est de Tor elle est identique pour les 3 ports, elle contient 3 formats contrairement à Google qui en contient qu'un.

3.9.2.5 L'extension « supported_groups »

Tor 443

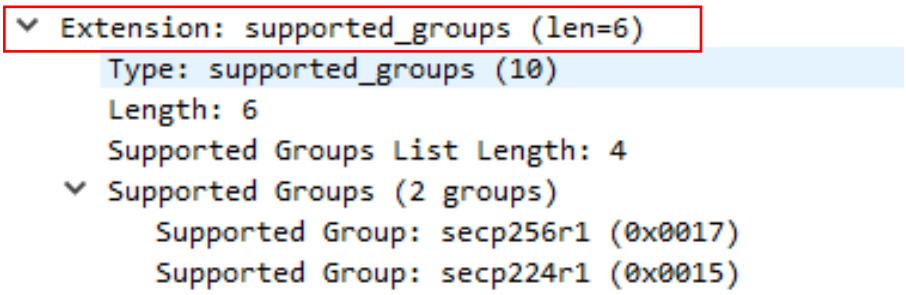


Figure 3.9.17 : *Extension «supported_groups» pour Tor port 443.*

Tor 9001

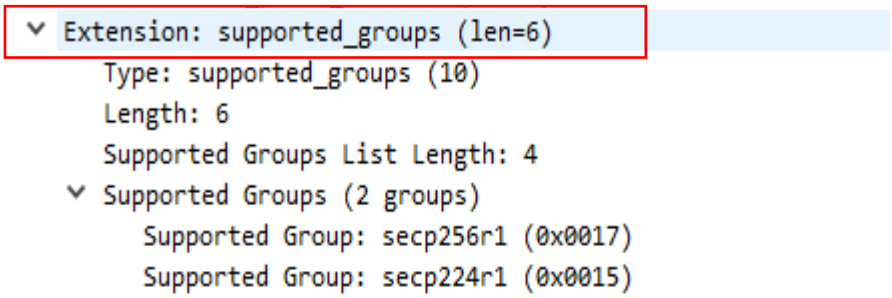


Figure 3.9.18 : *Extension «supported_groups» pour Tor port 9001.*

Tor aléatoire

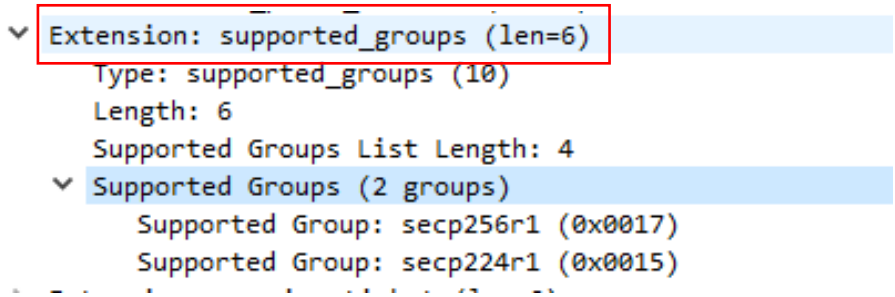


Figure 3.9.19 : *Extension «supported_groups» pour Tor port aléatoire.*

Google Chrome

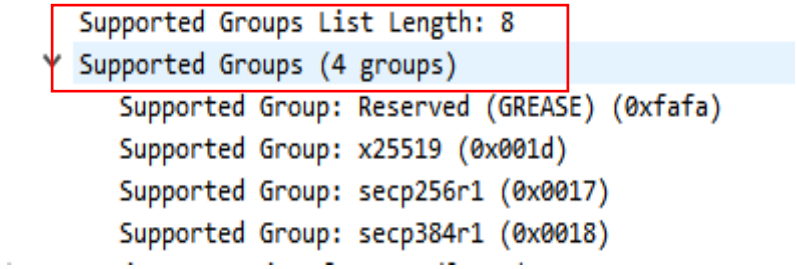


Figure 3.9.20 : *Extension «supported_groups» pour Google Chrome.*

Cette extension propose des algorithmes d'échange de clé.

Tor contient 2 groupes fixes tandis que Google Chrome 4.

3.9.2.6 L'extension « signature_algorithms »

Tor 443

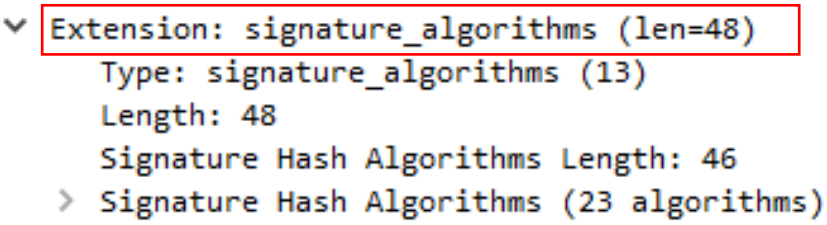


Figure 3.9.21 : *Extension « signature_algorithms » pour Tor port 443.*

Tor port aléatoire

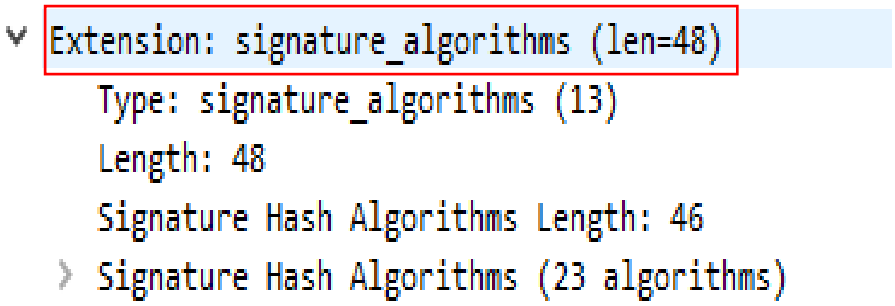


Figure 3.9.22 : *Extension « signature_algorithms » pour Tor port aléatoire.*

Tor 9001

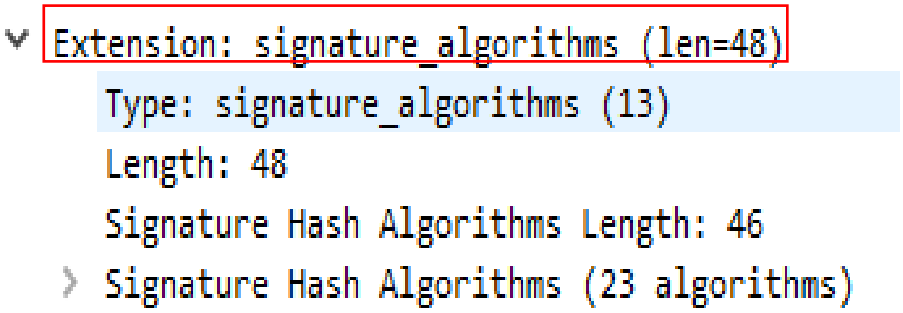


Figure 3.9.23 : *Extension « signature_algorithms » pour Tor port 9001.*

Google Chrome

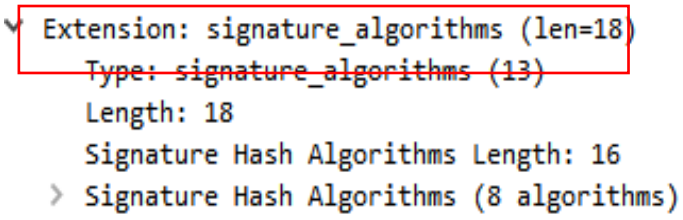


Figure 3.9.24 : *Extension « signature_algorithms » pour Google Chrome.*

Cette extension renseigne sur les algorithmes de signature.

Tor et Google Chrome contiennent les deux 13 algorithmes de signatures, de longueur de 48 octets pour Tor et 18 octets pour Google Chrome.

3.9.2.7 Message « Server Hello »

Tor 443

```
Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 151
    Version: TLS 1.2 (0x0303)
    Random: 55beb26b689efa51474959c707f65e780ad679c5715f56f21ae85a4f2f482d5d
    Session ID Length: 32
    Session ID: f0e6fc1970358e3ba650e9bbbc227562edf7ce15dc5f99156281aa8d0e761fe3
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Compression Method: null (0)
    Extensions Length: 79
  Extension: supported_versions (len=2)
      Type: supported_versions (43)
      Length: 2
```

Figure 3.9.25 : *Message « Server Hello » envoyé par Tor port 443.*

Tor port aléatoire

```
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 155
Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 151
    Version: TLS 1.2 (0x0303)
    Random: 7f89be04545649b89c4c09da27e4c56ee20a6a03b09e51d72bf6ba0e6d208042
    Session ID Length: 32
    Session ID: e85f8a20a6454d7091881721e94d3980b0b042c914c7e1d0625d11b58f3a7bd8
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Compression Method: null (0)
```

Figure 3.9.26 : *Message « Server Hello » envoyé par Tor port aléatoire.*

Tor 9001

```
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 57
Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 53
    Version: TLS 1.2 (0x0303)
  > Random: 83809821abe655bea83a957018cc4d7c65055bac04f9323d1832b25b6072b759
    Session ID Length: 0
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Compression Method: null (0)
    Extensions Length: 13
```

Figure 3.9.27 : *Message « Server Hello » envoyé par Tor port 9001.*

Google Chrome

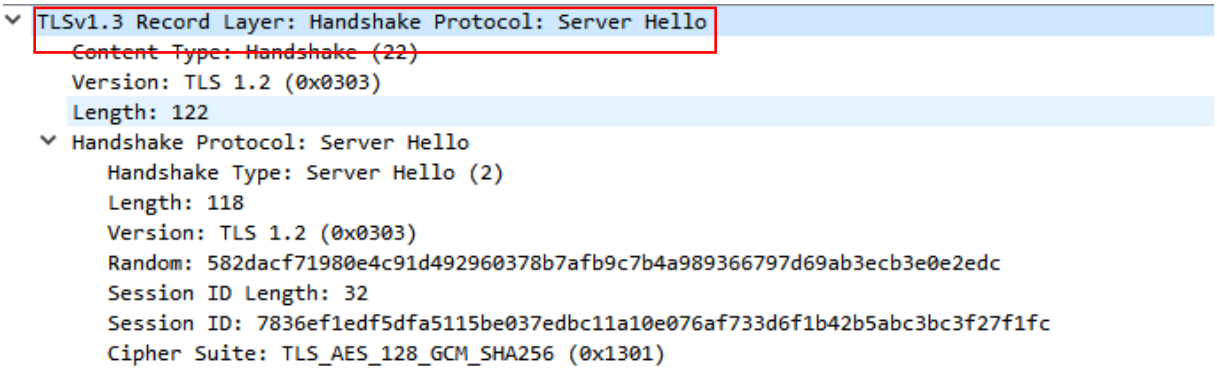


Figure 3.9.28 : *Message « Server Hello » envoyé par Google Chrome.*

Le message « Server Hello » permet de confirmer si le serveur prend en charge la version TLS envoyer par le client ou pas, choisi une suite de chiffrement dans la liste du « Client Hello » et génère sa propre valeur aléatoire. Ce message contient aussi une version, une valeur aléatoire et une suite de chiffrement.

La suite de chiffrement choisi par le serveur pour Tor port 443 et le port aléatoire est : TLS_AES_256_GCM_SHA384.

Pour Tor port 9001: TLS_ECDME_RSA_WITH_AES_256_GCM_SHA384.

Pour Google Chrome: TLS_AES_128_GCM_SHA256.

AES_256_GCM, AES_128_GCM sont des algorithmes de chiffrement.

SHA384 et SHA256 sont des algorithmes de hachage.

3.9.2.8 Constatation

La comparaison des différentes caractéristiques des paquets des connexions « TCP Handshake » et « TLS handshake » selon le navigateur choisi, a permis de constater des différences propres au réseau Tor tels que :

- Le numéro du port.
- Le nombre de suite de chiffrements.
- Le nombre d'extension

3.9.3 Informations extraites d'I2P

Contrairement au réseau Tor, I2P n'établit aucune connexion TCP ou TLS. Les informations extraites concernent le NTP et SSDP.

Le NTP est un protocole de synchronisation, et le SSDP est un protocole de communication informatique.

En réalité, I2P a un problème de décalage horaire qui affecte les applications quotidiennes sur Internet. Et pour remédier à cela, le NTP a été introduit pour synchroniser l'horloge. Le SSDP de son côté permet aux clients de découvrir les services disponibles sur le réseau.

Pour commencer, I2P contacte le DNS de Google pour avoir l'adresse du serveur NTP le plus proche.

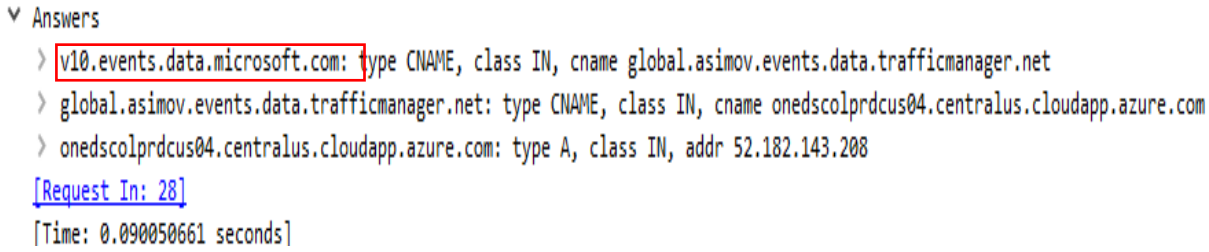
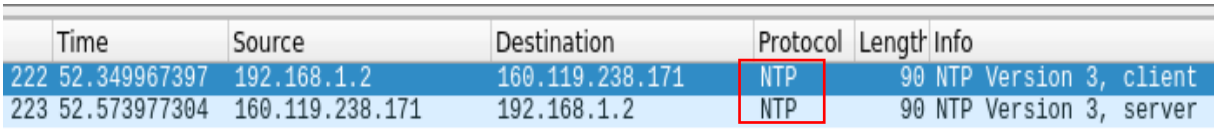


Figure 3.9.29 : *Réponse du serveur DNS.*

La figure ci-dessus montre la réponse du serveur DNS. I2P va choisir une adresse des trois pour contacter son serveur NTP. Le client envoie donc une requête NTP et le serveur lui répond de même comme suit :



	Time	Source	Destination	Protocol	Length	Info
222	52.349967397	192.168.1.2	160.119.238.171	NTP	90	NTP Version 3, client
223	52.573977304	160.119.238.171	192.168.1.2	NTP	90	NTP Version 3, server

Figure 3.9.30 : *Requêtes NTP.*

L'intérieur des paquets nous donne les informations suivantes :

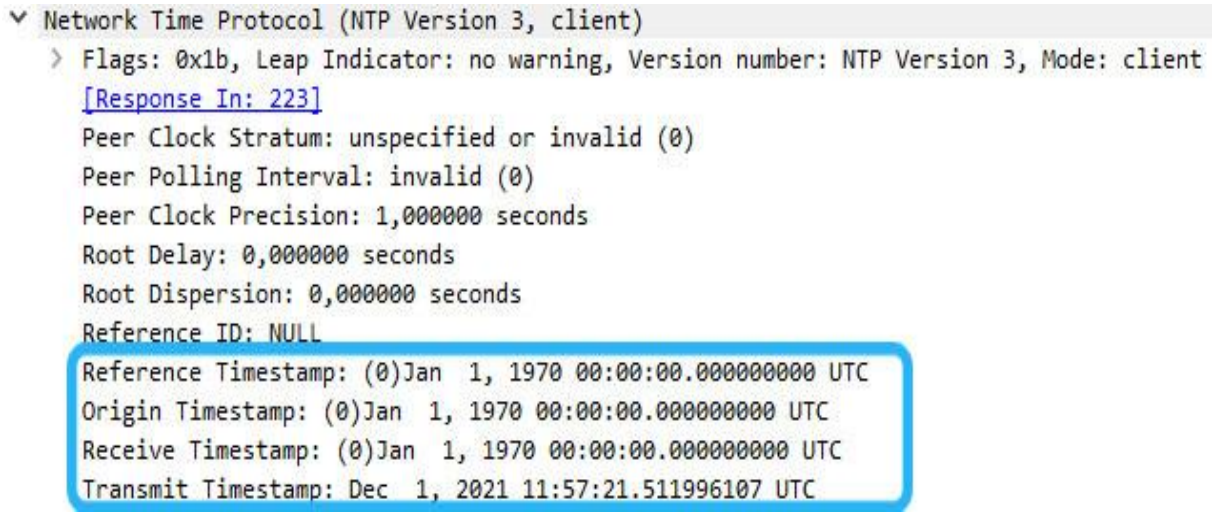


Figure 3.9.31 : *Paquet client.*

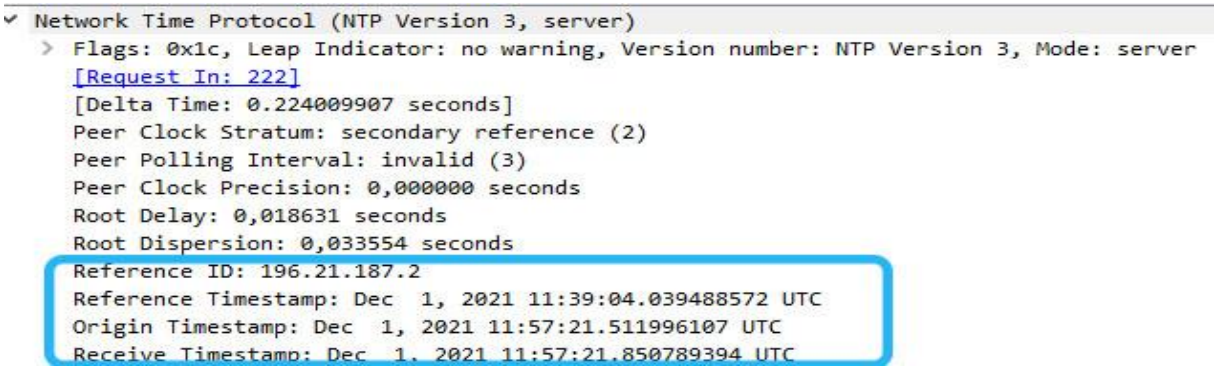


Figure 3.9.32 : *Paquet serveur.*

L'heure du client n'est pas synchronisée. Mais après la réponse du serveur, le problème a été réglé. A noter que le 1er Décembre est le jour où ces paquets-là ont été capturés.

Par la suite, c'est au rôle du SSDP de faire son travail. Il établie des requêtes de découvertes « M-SEARCH » limitées au LAN et basées sur des échanges HTTPMU, de l'http sur UDP en multicast. L'adresse multicast utilisé est « 239.255.255.250 » avec le port UDP « 1900 »

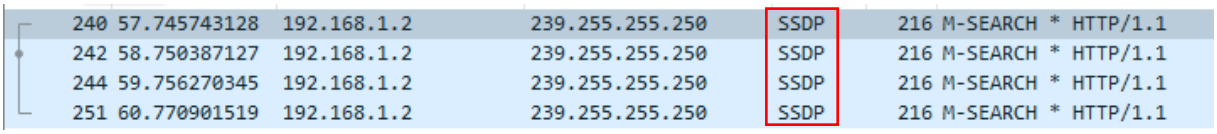


Figure 3.9.33 : *Paquets SSDP.*

Le nombre de paquets capté ici est 4, c'est le nombre capté durant l'utilisation du navigateur Firefox comme dans le cas de ce projet. La longueur du paquet est égale à 216 octets.

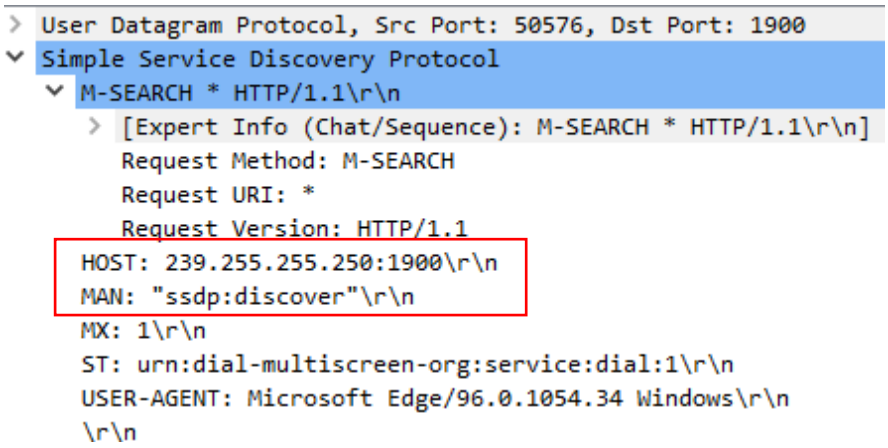


Figure 3.9.34 : *Paquet SSDP.*

Le port utilisé pour envoyer la requête est le 50576.

3.9.3.1 Constatation

- Des requêtes sont envoyées au serveur DNS afin de trouver les serveurs NTP les plus proches pour synchroniser l'horloge.
- La longueur totale du paquet SSDP pour le navigateur Firefox est de 216.
- L'adresse multicast « 239.255.255.250 » est dédiée au SSDP, avec le port 1900.

3.9.4 Informations extraites de Tails

Tails	Application Data	ACK
Type	IPV4 (0x0800)	IPV4 (0x0800)
Protocole	TCP (6)	TCP (6)
IP source	93.180.157.154	192.168.1.5
IP Destination	192.168.1.5	93.180.157.154
Port source	9001	49744

Port Destination	49744	9001
Longueur totale	595	52
Identification	0x64e7 (25831)	0x4fea (20458)
TTL	44	64
Numéro de séquence	1	1
Stream index	0	0
Flags	0x018 (PSH, ACK)	0x010 (ACK)
Window size value	501	3540
RTT TO ACK		0.001862117 seconds

Tableau 3.9.4 : *Informations sur Tails.*

3.9.4.1 Constatation

- L'adresse IP source du paquet « Application Data » et celui du relais Tor et la destination celle du PC avec l'OS Tails.
- Le port 9001 est un port appartenant à Tor. Tandis que le 49744 est un port dynamique.
- La longueur totale du paquet est nettement plus grande dans l'application data que dans le paquet ACK.
- L'ACK a une plus grande valeur de TTL et Window size.
- Le RTT to ACK n'existe pas dans l'application data.

3.9.4.2 TLS du paquet Tails

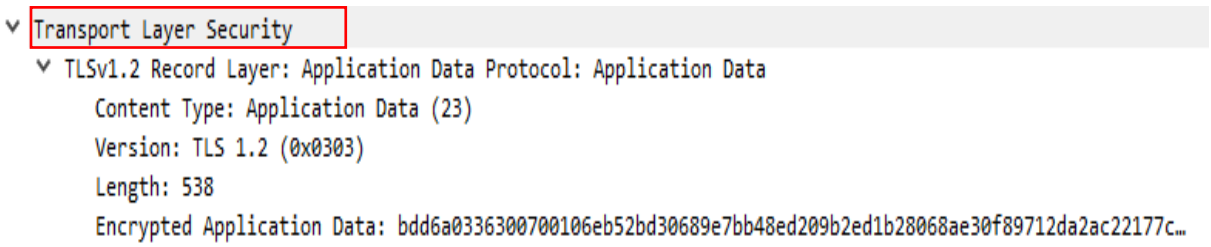


Figure 3.9.35 : *TLS Tails.*

Ce paquet indique la taille qui est de 538 octets, ainsi que le cryptage de l'application data.

3.10 Signatures de chaque réseau

Signature	Nom de la signature	Tor port 9001	Tor port 443	Tor port aléatoire
a	client hello Extension supported_groups	00 0a 00 06 00 04 00 17 00 15	00 0a 00 06 00 04 00 17 00 15	00 0a 00 06 00 04 00 17 00 15
b	client hello Extension signature_algorithms	00 0d 00 30 00 2^{e} 04 03 05 03 06 03 08 07 08 08 08 09 08 0a 08 0b 08 04 08 05 08 06 04 01 05 01 06 01 03 03 02 03 03 01 02 01 03 02 02 02 04 02 05 02 06 02	00 0d 00 30 00 2e 04 03 05 03 06 03 08 07 08 08 08 09 08 0a 08 0b 08 04 08 05 08 06 04 01 05 01 06 01 03 03 02 03 03 01 02 01 03 02 02 02 04 02 05 02 06 02	00 0d 00 30 00 2e 04 03 05 03 06 03 08 07 08 08 08 09 08 0a 08 0b 08 04 08 05 08 06 04 01 05 01 06 01 03 03 02 03 03 01 02 01 03 02 02 02 04 02 05 02 06 02
c	client hello ec_point_format	00 0b 00 04 03 00 01 02	00 0b 00 04 03 00 01 02	00 0b 00 04 03 00 01 02
d	server hello cipher suite	c0 30	c0 30	c0 30

Tableau 3.10.1: *Signatures Tor.*

Signature	Nom de la signature	I2P
a	Contenu NTP	1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
b	Contenu SDDP	53 54 3a 20 75 72 6e 3a 0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e 0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 00a0 6c 3a 31 0d 0a

Tableau 3.10.2: *Signatures I2P.*

3.11 Conclusion

A travers ce chapitre, la comparaison entre les paquets des réseaux anonymes et le navigateur Chrome, a permis d'identifier des attributs propres à chaque réseau anonyme. Ces derniers ont été utilisés comme signatures numériques afin de créer des règles caractéristiques des réseaux anonymes, qui seront implémentées dans un système de détection d'intrusion « Suricata ».

La prochaine étape sera d'implémenter ces signatures dans l'IDS pour qu'il génère une alerte lors de la détection du trafic anonyme.

Chapitre 4

Implémentation des règles dans deux IDS

4.1 Introduction

Les entreprises sont de plus en plus préoccupées par le renforcement de leur sécurité informatique.

Afin de détecter les attaques et les actions suspectes dans le but de les bloquer, une variété d'outils et d'équipements est utilisée. Cependant, de nouveaux exploits et techniques d'attaques sont conçus tous les jours par des cybers attaquants pour contourner la défense des organisations.

C'est pour cette raison-là que l'utilisation d'un outil de sécurité omniprésent est primordiale au sein d'une entreprise. Cet outil est le système de détection d'intrusion IDS, il écoute le trafic et permet de créer des alertes lors de comportements anormales ou d'attaques connues.

A travers ce chapitre, des règles vont être créées à partir des empreintes détectées précédemment, puis implémentées sur les deux systèmes de détection d'intrusion « Suricata » et « Snort » dans le but de détecter les paquets des réseaux Tor et I2P.

Puis pour conclure, la fiabilité des règles de détection du réseau Tor et I2P sera testé.

4.2 Système de détection d'intrusion

4.2.1 Fonctions d'un IDS

Les fonctions principales d'un IDS sont :

- **L'analyse des captures** : Evaluation et traitement des journaux du système afin de garantir la détection d'intrusion.
- **Journalisation** : Enregistrement des événements dans un fichier log dont le but est de garder un historique des actions.
- **Gestion** : Administration de manière continue.
- **Action** : Déclenche une alerte lors de la détection d'une attaque ou d'un comportement suspect. Les alertes sont enregistrées dans des fichiers logs ou dans une base de données [62].

4.2.2 Modes de détection

Elle se fait selon deux méthodes :

- **Les signatures d'attaques connues :** Enregistrées sur une base de données à jour, elles sont comparées et recherchées dans le paquet analysé. Dans ce cas-là, une mise à jour récurrente est nécessaire car l'IDS ne peut pas identifier les attaques dont il n'a pas les signatures.
- **La détection d'anomalie** : L'IDS génère une alerte lors d'un comportement anormal du système. Elle nécessite une phase d'apprentissage durant laquelle l'IDS va définir un fonctionnement normal qui servira de référence [63].

4.3 Règle d'IDS

Les signatures sont un maillon indispensable au fonctionnement d'un IDS. Dans le cas de ce mémoire, les règles utilisées sont les mêmes pour les deux IDS choisi.

Une règle/signature se présente sous forme qui suit:

- **L'action** : Détermine l'action à effectuer lorsque la signature correspond.
- **L'en-tête** : Définit le protocole, les réseaux, les adresses IP, les ports et le sens de la règle.
- **Les options de la règle** : Définit les caractéristiques de la règle.

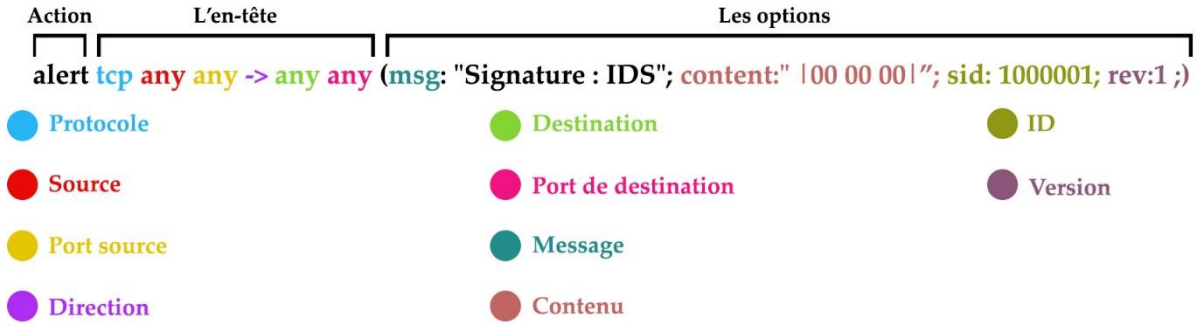


Figure 4.3.1: *Exemple de règle.*

4.3.1 Action

Les actions disponibles sont comme suit :

- **Pass :** Arrête l'inspection ultérieure du paquet, l'IDS stop donc le scan du paquet.

- **Reject** : C'est un rejet actif du paquet où l'IDS génère une alerte, il est reçu par le destinateur et expéditeur. Si le paquet rejeté concerne le protocole TCP, ce sera un paquet « Reset » tandis que pour tous les autres protocoles, c'est un paquet d'erreur « ICMP »
- **Alert :** Génère une alerte lors de la reconnaissance de signatures d'attaques ou d'anomalies.

4.3.2 En-tête

L'en-tête contient quatre champs. Le protocole, l'IP source et l'IP destinations, les ports et la direction.

Une règle peut correspondre à une seule direction « -> » ou bien à deux sens « <> ». Seuls les paquets avec la même direction peuvent correspondre. La direction inverse « <- » n'existe pas.

4.3.3 Options

Les options de règle sont placées entre des parenthèses et séparées par des points-virgules [64].

Option	Signification
Msg	Donne des informations sur la signature
Sid	ID de la signature
Id	Identificateur de chaque paquet envoyé par une hôte
Seq	Utilisé pour la recherche d'un numéro de séquence TCP spécifique
Dsize	Utilisé pour correspondre la taille de la charge utile du paquet

Content	Utilisé pour écrire ce qui correspond à la signature
Rev	Représente la version de la signature
Offset	Modifie l'option « content » et fixe le début de la tentative de correspondance de motif

Tableau 4.3.1: *Options des règles.*

4.4 Implémentation des signatures numériques

4.4.1 Signatures numérique du navigateur Tor

L'analyse du trafic des différents réseaux anonymes a permis d'identifier des caractéristiques propres à chacun. De ces derniers, des empreintes numériques ont été déduites et implémenter dans des systèmes de détection.

A noter que les signatures de Tails abouti au même résultat vu que ce dernier utilise le Tor browser comme navigateur.

a. La première signature détecte les extensions « supported_groups » en vérifiant la présence des deux groupes caractéristiques de Tor.

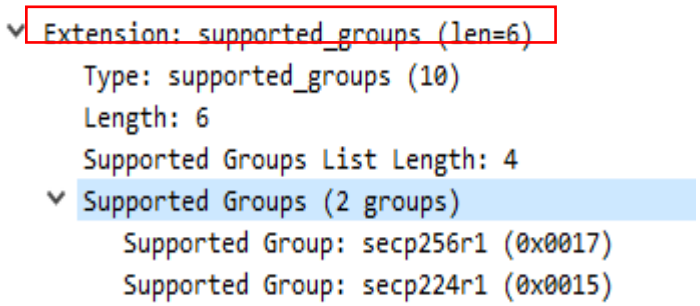


Figure 4.4.1 *: Première signature de Tor « supported_group».*

```
alert tcp any any -> any any (msg: "Possibilite d'utilisation de Tor : client hello Extension supported_groups"; content:"|00 0a 00 06 00 04 00 17 00 15|"; sid:10000001 ;)
```

b. La deuxième signature détecte l'extension « signature_algorithms » qui contient 23 algorithmes de signature utilisés par Tor.

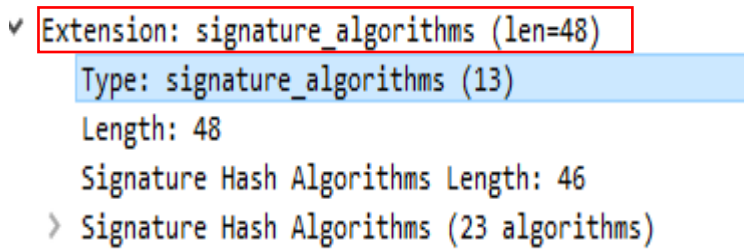


Figure 4.4.2 *: Deuxième signature de Tor «* signature_algorithms*».*

```
alert tcp any any -> any any (msg: "Possibilite d'utilisation de Tor: client hello Extension signature_algorithms"; content:"|00 0d 00 30 00 2e 04 03 05 03 06 03 08 07 08 08 08 09 08 0a 08 0b 08 04 08 05 08 06 04 01 05 01 06 01 03 03 02 03 03 01 02 01 03 02 02 02 04 02 05 02 06 02|";sid:10000002;)
```

c. La troisième signature détecte l'extension « ec_point_format »

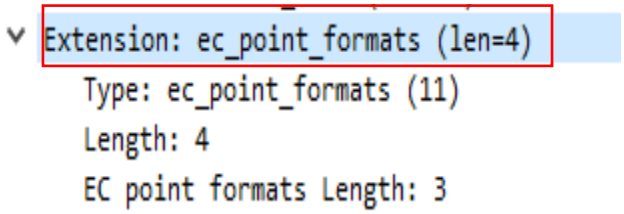


Figure 4.4.3 *: Troisième signature de Tor «* ec_point_format *».*

```
alert tcp any any -> any 9001 (msg: "Possibility d'utilisation de Tor: client hello ec_point_format";content:"| 00 0b 00 04 03 00 01 02|"; sid: 1000003;)
```

d. La quatrième signature détecte « server hello cipher suite »

Figure 4.4.4 *: quatrième signature de Tor « suites de chiffrement » dans le Server Hello.*

alert tcp any any -> any 9001 (msg: "Possibilite d'utilisation de Tor:server hello cipher suite";content:"|c0 30|";sid: 1000004;)

e. La cinquième signature détecte les ports de destination utilisés par les nœuds de Tor.

alert tcp any any -> any 9001 (msg: "Possibilite d'utilisation de Tor : client hello port de destination" ;sid : 10000005;)

4.4.2 Signatures numérique du navigateur I2P

Contrairement au réseau Tor, I2P n'établit aucune connexion TCP ou TLS. Les informations extraites concernent le NTP et SSDP.

- Le NTP est un protocole de synchronisation, et le SSDP est un protocole de communication informatique.
- Les requêtes sont envoyées au serveur DNS afin de trouver les serveurs NTP les plus proches pour synchroniser l'horloge.
- La longueur totale du paquet SSDP pour le navigateur Firefox est de 216.
- L'adresse multicast « 239.255.255.250 » est dédiée au SSDP, avec le port 1900.

a. La Première signature détecte si I2P contacte le serveur NTP.

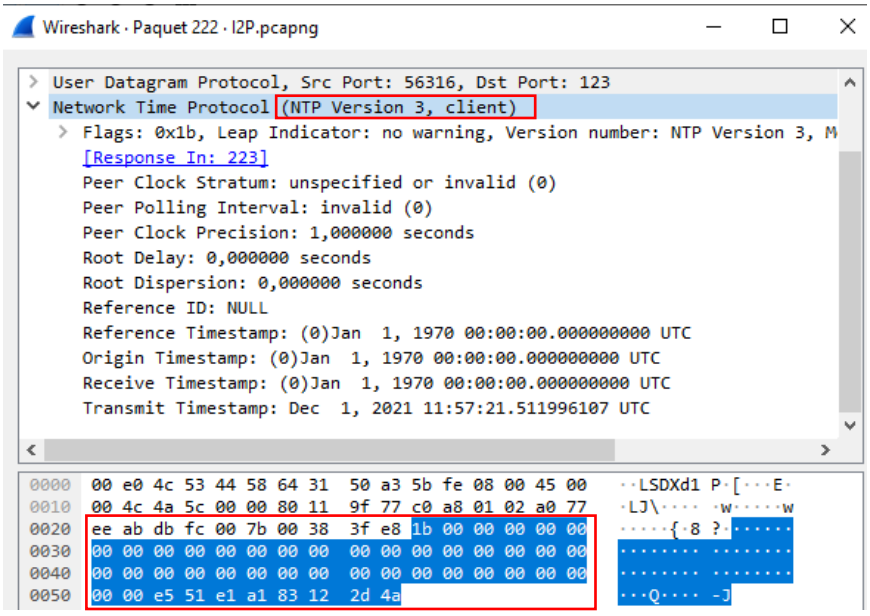


Figure 4.4.5*: Première signature d'I2P.*

alert udp any any -> any 123 (msg: " Possibility de demarrage du routeur I2P: NTP"; content:"|1b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00l"; sid: 1000006;)

b. La deuxième signature détecte si I2P contacte le groupe multicast « 239.255.255.250 »

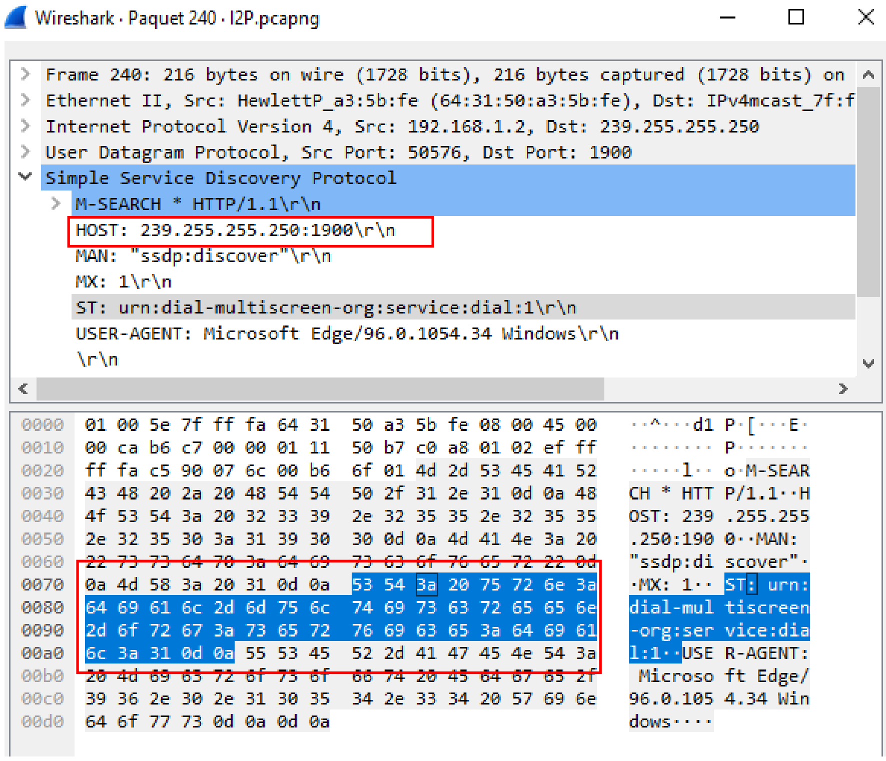


Figure 4.4.6 *: Deuxième signature d'I2P.*

alert udp any 7653 -> 239.255.255.250 1900 (msg:" Possibilite de demarrage du routeur I2P: SSDP "; content:"upnp"; dsize: <150; sid: 10000011;)

4.5 Environnement de test

L'architecture de l'environnement de test est une architecture client-serveur. Les caractéristiques des machines utilisées sont représentés dans le tableau suivant :

Ordinateur	Serveur	Client
Système d'exploitation	Ubuntu 20.04	Windows 10 Professionnel 10.0.19044 Build 19044
RAM	16G	8G

Processeur	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz 4 GHz	Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz 2.59 GHz
Logiciels installés	Squid proxy 3.5.15 | Wireshark 3.6.3 | Suricata 6.0.3 | Snort 3.1.17.0	Tor browser 10.5.2 | I2P 1.7.0
Fabriquant	Condor	ASUS

Tableau 4.5.1: *Caractéristiques des machines.*

4.6 Lancement de Suricata

Afin de bien visualiser les alertes envoyées par Suricata, une interface graphique dont le nom est Wazuh a été utilisée.

4.6.1 Tor

En lançant le navigateur Tor Browser, les 5 signatures implémentées auparavant au niveau de Suricata ont été capturées.

timestamp per 30 minutes

Time	rule.description	rule.level	rule.id
Jun 6, 2022 @ 12:51:17.187	Suricata: Alert - Possibilite d'utilisation de Tor : client hello Extension signature_algorithms	3	86601
Jun 6, 2022 @ 12:51:17.152	Suricata: Alert - Possibilite d'utilisation de Tor : client hello Extension signature_algorithms	3	86601
Jun 6, 2022 @ 12:51:14.579	Suricata: Alert - Possibilite d'utilisation de Tor : client hello Extension signature_algorithms	3	86601
Jun 6, 2022 @ 12:51:14.577	Suricata: Alert - Possibilite d'utilisation de Tor : client hello Extension supported_groups	3	86601
Jun 6, 2022 @ 12:51:14.575	Suricata: Alert - Possibilite d'utilisation de Tor: client hello ec_point_format	3	86601
Jun 6, 2022 @ 12:51:14.573	Suricata: Alert - Possibilite d'utilisation de Tor:server hello cipher suite	3	86601
Jun 6, 2022 @ 12:51:14.571	Suricata: Alert - Possibilite d'utilisation de Tor : client hello port de destination	3	86601

Figure 4.6.1 *: Alertes Tor sur Suricata.*

La navigation sur Tor par la suite n'affiche aucune alerte. Maintenant pour visualiser les signatures de Tor les plus détectées, de nombreux tests ont été effectués et le résultat de cela s'affiche comme suit :

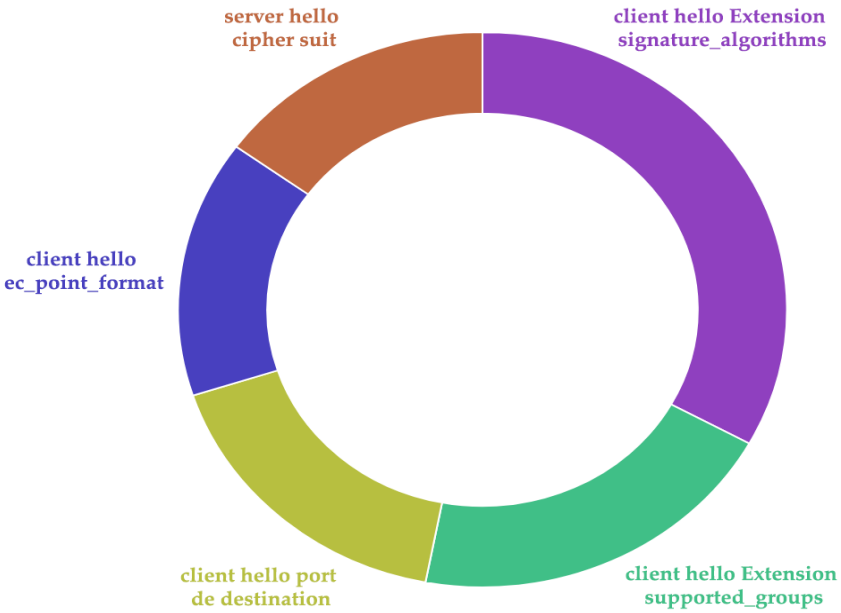


Figure 4.6.2 *: Diagramme circulaire représentant les alertes de Tor sur Suricata.*

Le diagramme démontre que l'extension « signature_algorithms » est la plus présente comparer aux autres. Elle est suivie par l'extension « supported_groups » puis le « port de destination » et finalement, le « client hello ec_point_format » et le « server hello cipher suit » qui ont un taux de présence nettement identique.

Pour bien s'informer sur le paquet reçu, un simple clic sur celui-ci affiche les détails suivants:

t data.dest_port	9001	→ Port de destination
t data.event_type	alert	→ Type d'action de l'IDS
t rule.description	Suricata: Alert - Possibilite d'utilisation de Tor : client hello Extension supported _groups	→ Signature détectée
t data.src_ip	192.168.1.3	→ Adresse IP source (d'où vient l'alerte?)
t data.src_port	50470	→ Port source
data.timestamp	Jun 6, 2022 @ 12:55:22.720	→ Date et heure où l'alerte a été détectée

Figure 4.6.3 *: Exemple de détails d'une alertes Tor sur Suricata.*

Les détails précédent ne représente qu'une petite partie de ce que l'interface de Wazuh fournis comme détails. Cela permet aux chercheurs de bien s'approfondir dans leurs recherches si souhaiter.

4.6.2 I2P

Le lancement d'I2P affiche des alertes qui contiennent les signatures utilisées autrefois pour la création des règles d'I2P. Cependant, ces dernières ne se sont pas présentées seuls. L'extension « signature_algorithms » qui devait représenter que Tor a fait surface aussi.

Time	rule.description	rule.level	rule.id
Jun 6, 2022 @ 13:09:03.917	Suricata: Alert - Possibilite d'utilisation de Tor : client hello Extension signature_algorithms	3	86601
Jun 6, 2022 @ 13:08:53.363	Suricata: Alert - Possibilite de demarrage du routeur I2P: SSDP	3	86601
Jun 6, 2022 @ 13:08:51.368	Suricata: Alert - Possibilite de demarrage du routeur I2P: SSDP	3	86601
Jun 6, 2022 @ 13:08:45.367	Suricata: Alert - Possibilite de demarrage du routeur I2P: NTP	3	86601
Jun 6, 2022 @ 13:08:45.359	Suricata: Alert - Possibilite de demarrage du routeur I2P: NTP	3	86601

Figure 4.6.4 *: Alertes I2P sur Suricata.*

Le diagramme d'I2P s'affiche comme suit :

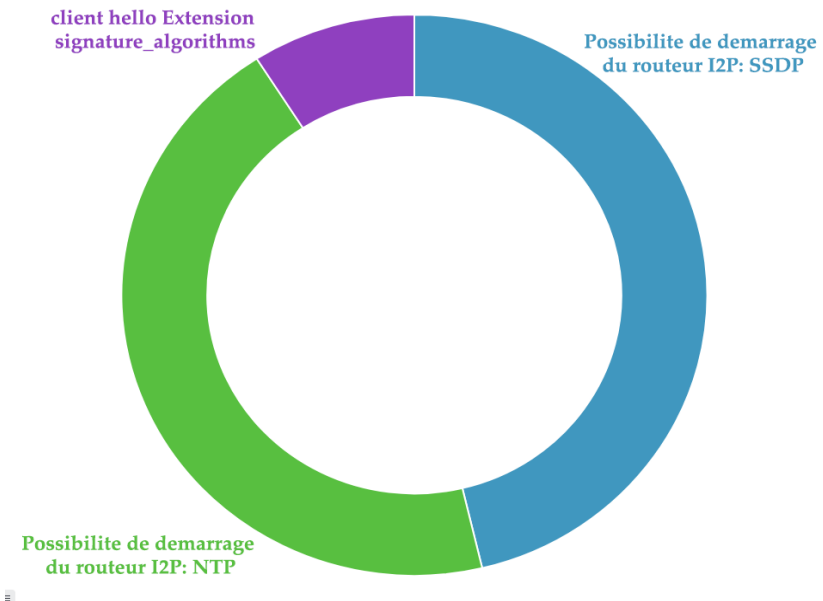


Figure 4.6.5 *: Diagramme circulaire représentant les alertes d'I2P sur Suricata.*

La présence du SSDP et NTP ici est d'un taux clairement égal. Les extensions « signature_algorthms » se sont manifesté ici autant que faux positives.

4.6.3 Google

Avec pour objectif d'affirmer la fiabilité des règles implémentées précédemment, ces dernières seront testées sur Google, sans la présence des deux réseaux anonymes Tor et I2P.

timestamp per 30 minutes

Time	rule.description	rule.level	rule.id
Jun 6, 2022 @ 13:06:19.284	Suricata: Alert - Possibilite d'utilisation de Tor : client hello Extension signature_algorithms	3	86601
Jun 6, 2022 @ 13:06:19.245	Suricata: Alert - Possibilite d'utilisation de Tor : client hello Extension signature_algorithms	3	86601
Jun 6, 2022 @ 13:03:19.155	Suricata: Alert - Possibilite d'utilisation de Tor : client hello Extension signature_algorithms	3	86601

Figure 4.6.6 *: Alertes Google sur Suricata.*

En navigant sur Google, l'extension qui s'affiche régulièrement est celle de « signature_algorithms ». La figure ci-dessus représente un extrait de cela.

4.6.4 Résultat

En utilisant Suricata comme IDS, les points qui suivent ont été conclue :

- L'extension « signature_algorithms » est un faux positif. Elle ne peut pas être utilisée pour distinguer la présence du réseau Tor.
- La détection des deux réseaux Tor et I2P peut se faire au lancement uniquement. Si la période de celle-ci est ratée, la navigation n'affichera pas d'alertes et les utilisateurs des deux réseaux anonymes ne seront pas détectés.
- Le SSDP et NTP sont véritablement propres à I2P, ils n'ont générés aucun faux positif.
- Sur 417 alertes, 122 d'entre elles représentent le NTP et 97 le SSDP, les deux protocoles propres au réseau I2P.
- L'extension « signature_algorithms » qui représente un faux positif est massivement présente dans Tor, I2P et Google avec 109 alertes et un taux de 26,13%
- Les quatre extensions propres à Tor sont présentes comme ceci: l'extension « supported-groups » avec 29 alertes, l'extension « port de destination » avec 24 alertes,

l'extension « hello ec_point_format » avec 18 alertes et finalement, l'extension « server hello cipher suite » avec 18 alertes également.

- Suricata a un taux de détection de 73,83%, selon une étude faite dans un environnement de laboratoire pendant 4 jours.

4.7 Lancement de Snort

Dans le cas de Snort, une interface plus adaptée à celui-ci a été utilisée est c'est celle de Splunk.

4.7.1 Tor

Le résultat du lancement de Tor affiche la présence de toutes les signatures implémentées. Dans ce deuxième cas, c'était les signatures du « client hello port de destination » et l'extension « supported_groups » qui étaient les plus présentes.

Et tout comme l'interface de Wazuh, Splunk offre la possibilité de consulter chaque alerte afin d'en tirer plus de détails si nécessaire.

_time	src_ap	dst_ap	msg
2022-06-06 09:49:24	192.168.1.3:49827	148.251.11.21:443	Possibilite d'utilisation de Tor : client hello Extension supported_groups
2022-06-06 09:49:23	192.168.1.3:49827	148.251.11.21:443	Possibilite d'utilisation de Tor : client hello Extension signature_algorithms
2022-06-06 09:49:20	192.168.1.3:49826	54.36.166.86:9001	Possibilite d'utilisation de Tor : client hello port de destination
2022-06-06 09:49:20	192.168.1.3:49826	54.36.166.86:9001	Possibilite d'utilisation de Tor : client hello port de destination
2022-06-06 09:49:20	192.168.1.3:49826	54.36.166.86:9001	Possibilite d'utilisation de Tor : client hello port de destination
2022-06-06 09:49:20	192.168.1.3:49826	54.36.166.86:9001	Possibilite d'utilisation de Tor : client hello port de destination
2022-06-06 09:48:54	192.168.1.3:49826	54.36.166.86:9001	Possibilite d'utilisation de Tor : client hello port de destination
2022-06-06 09:48:28	192.168.1.3:49826	54.36.166.86:9001	Possibilite d'utilisation de Tor : client hello port de destination
2022-06-06 09:48:28	192.168.1.3:49826	54.36.166.86:9001	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:48:25	192.168.1.3:49826	54.36.166.86:9001	Possibilite d'utilisation de Tor: client hello ec_point_format

Figure 4.7.1 *: Alertes lancement de Tor sur Snort.*

Contrairement à ce que Suricata a affirmé, Snort affiche quelques alertes après la navigation avec le Tor browser.

_time	src_ap	dst_ap	msg
2022-06-06 09:51:30	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:31	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:33	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:33	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:33	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:33	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:33	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:34	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:34	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:34	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:35	45.58.156.77:80	192.168.1.3:57004	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 09:51:36	192.168.1.3:57213	130.117.190.148:443	Possibilite d'utilisation de Tor : client hello Extension signature_algorithms
2022-06-06 09:51:36	192.168.1.3:57213	130.117.190.148:443	Possibilite d'utilisation de Tor: client hello ec_point_format
2022-06-06 09:51:36	192.168.1.3:57213	130.117.190.148:443	Possibilite d'utilisation de Tor:server hello cipher suite

Figure 4.7.2 *: Alertes après la navigation sous Tor sur Snort.*

Les 3 signatures détectées ici sont celles du « server hello cipher suite », « signature_algorithms » et le « client hello ec_point_format »

4.7.2 I2P

Le démarrage d'I2P projette les alertes propres à lui, celles du NTP et SSDP. L'extension « signature_algorithms » est également présente.

_time	src_ap	dst_ap	msg
2022-06-06 11:15:26	192.168.137.1:7653	239.255.255.250:1900	Possibilite de demarrage du routeur I2P: SSDP
2022-06-06 11:15:26	192.168.1.4:7653	239.255.255.250:1900	Possibilite de demarrage du routeur I2P: SSDP
2022-06-06 11:15:23	192.168.137.1:7653	239.255.255.250:1900	Possibilite de demarrage du routeur I2P: SSDP
2022-06-06 11:15:23	192.168.1.4:7653	239.255.255.250:1900	Possibilite de demarrage du routeur I2P: SSDP
2022-06-06 11:15:01	192.168.1.4:50114	196.10.52.58:123	Possibilite de demarrage du routeur I2P: NTP
2022-06-06 11:14:37	192.168.1.3:57527	80.231.123.131:443	Possibilite d'utilisation de Tor : client hello Extension signature_algorithms

Figure 4.7.3 *: Alertes I2P sur Snort.*

4.7.3 Google

Naviguer sur Google a montré la présence de 3 faux positifs dont le « server hello cipher suite », le « client hello ec_point_format » et l'extension « signature_algorithms »

_time	src_ap	dst_ap	msg
2022-06-06 10:05:00	192.168.1.4:65437	20.82.209.183:443	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 10:05:01	192.168.1.4:65441	13.33.232.64:443	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 10:05:01	192.168.1.4:65442	142.251.37.35:443	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 10:05:01	34.102.176.152:443	192.168.1.4:65439	Possibilite d'utilisation de Tor:server hello cipher suite
2022-06-06 10:05:42	35.173.119.210:443	192.168.1.4:49181	Possibilite d'utilisation de Tor: client hello ec_point_format
2022-06-06 10:07:12	2.18.0.196:443	192.168.1.4:49381	Possibilite d'utilisation de Tor: client hello ec_point_format
2022-06-06 10:09:27	192.168.1.4:49624	82.202.184.193:443	Possibilite d'utilisation de Tor : client hello Extension signature_algorithms
2022-06-06 10:09:27	192.168.1.4:49623	62.67.238.152:443	Possibilite d'utilisation de Tor : client hello Extension signature_algorithms

Figure 4.7.4 *: Alertes Google sur Snort.*

4.7.4 Résultat

L'emploi de Snort atteste que :

- Trois faux positifs ont été détectés, le « server hello cipher suite », le « client hello ec_point_format » et l'extension « signature_algorithms »
- Les signatures qui représentent Tor réellement sont donc le « client hello port destination » et l'extension « supported_groups »
- Le SSDP et NTP sont véritablement propres à I2P.
- Sur 11440 alertes, 5 d'entre elles représentent le NTP et 40 le SSDP, les deux protocoles propres au réseau I2P.
- Les extensions « server hello cipher suite », le « client hello ec_point_format » et « signature_algorithms » qui représentent des faux positifs se présentent dans Tor, I2P et Google avec 1090 alertes, 396 et 106 respectivement et un taux total de 13,99%

- Les deux extensions propres à Tor sont présentes comme ceci: l'extension « supported-groups » avec 36 alertes et l'extension « port de destination » avec 9702 alertes.
- Snort a un taux de détection de 86,01%, selon une étude faite dans un environnement de laboratoire pendant 4 jours.

4.8 Comparaison et résultat

Après avoir testé les deux IDS, il a été conclue que :

- L'implémentation de Snort et son interface Splunk demande beaucoup plus de ressource (RAM et CPU) et de temps que Suricata et son interface Wazuh. C'est à peu près le double.
- La rapidité des deux IDS était distinctement la même.
- Snort a généré plus d'alerte que Suricata sur le même trafic réseau (Les alertes montrées ici ne représentent qu'une petite partie de ce qui a été réellement capturé)
- Avec l'emploi des mêmes règles, Snort a engendré plus de faux positifs que Suricata.

Caractéristiques	Suricata	Snort
Ressource (RAM et CPU)	Plus accessible	Moins
Rapidité	Élevée	Élevée
Nombre d'alertes	Élevée	Plus élevée
Nombre de faux positifs	Bas	Élevée

Tableau 4.8.1: *Caractéristiques de Suricata vs Snort.*

4.9 Solution proposée

Maintenant que les signatures des deux réseaux anonymes sont détectées, il ne reste plus qu'à les bloquer pour empêcher toute tentative qui puisse nuire à la sécurité d'un réseau.

Pour cela, un IPS (Intrusion Prevention System) est employé. Il s'agit d'un outil de prévention semblable à l'IDS mais qui, contrairement à ce dernier qui ne fait qu'alerter, il peut réagir en temps réel en bloquant le trafic malveillant.

L'action adoptée par ce dispositif est celle du « drop » qui supprime un paquet et génère une alerte avec.

Et pour une meilleure évaluation du réseau dans un environnement réel tel celui d'une entreprise, l'utilisation d'un serveur annuaire contenant des comptes d'utilisateurs est largement conseillé dans le but de reconnaitre facilement et de manière ordonnée les employés qui tentent d'accéder aux réseaux anonymes.

4.10 Conclusion

Le travail effectué dans cette partie certifie la constance de tout ce qui a été énoncer et inclus dans les chapitres précédents.

Les faux positifs ne présentent pas d'échec dans ce travail mais bien au contraire, leur présence a contribué à la spécification des empreintes dites ADN de chaque réseau anonyme. C'est-à-dire des empreintes trouvées que chez Tor ou I2P et non pas autrement, jusqu'à preuve du contraire évidement.

L'utilisation de deux IDS a sur le même trafic réseau a abouti à des résultats non-semblables. Cela atteste qu'avoir la même tâche ne signifie pas avoir les mêmes résultats. Ces derniers sont jugés meilleure ou pas selon l'environnement et le besoin de chacun.

Conclusion générale

A travers ce projet de fin d'étude, l'importance de l'anonymat et du respect de la vie privée sur Internet a été mis en relief, ainsi que les outils qui y contribue.

Les réseaux anonymes sont le sujet de l'analyse de cette étude, Tor et I2P sont les deux réseaux anonymes les plus utilisés, tout au long de ce mémoire, leur fonctionnement a été étudié ainsi que leurs différences.

La comparaison des paquets TLS Handshake de Tor, I2P et du web ordinaire a permis de déduire des caractéristiques propres à chaque réseau anonyme, en analysant leurs paquets à l'aide de l'analyseur du paquet Wireshark.

D'après ces propriétés, des signatures numériques sont déduites et implémentées dans les deux systèmes de détection d'intrusion Snort et Suricata et testées dans un environnement de laboratoire avec une architecture client-serveur.

Cinq règles ont été implémentées pour détecter le trafic de Tor et deux pour I2P.

- Pour ce qui est de l'IDS Suricata :

L'extension « signature_algorithms » est un faux positif, elle revient avec 109 alertes sur 417, environ 26,17%. Le taux de détection de Suricata est donc 73,83%

La détection des deux réseaux Tor et I2P se fait au lancement uniquement.

Les régles de déction du SSDP et NTP sont totalement fiables, elles n'ont générées aucun faux positif.

- Pour ce qui est de l'IDS Snort :

Trois faux positifs ont été détectés, le « server hello cipher suite » avec 1090 alertes sur 113750, le « client hello ec_point_format » avec 396 alertes et « signature_algorithms » avec 106 alertes donc environ 13,99%. Le taux de détection de Snort est donc 86,01%

Snort a engendré plus de faux positifs que Suricata, raison pour laquelle le nombre d'alertes est plus grand pour Snort.

La comparaison des deux IDS montre que Snort a généré plus d'alerte que Suricata pour le même trafic réseau. Les deux IDS ont le même temps de réponse.

Les alertes générées sur les deux systèmes de détection ont confirmé l'utilité de la méthode utilisée à travers ce mémoire.

Afin de renforcer la sécurité au sein d'une entreprise, il est préférable d'ajouter un IPS (Intrusion Prevention System) qui en plus de générer une alerte, il supprime les paquets suspects, et l'utilisation d'un serveur annuaire pour pouvoir associer chaque employé à son propre profil avec un compte dédié.

[1] ‘Top 10 des cyberattaques qui ont marqué 2021’ par Hiscox Assurance, Février 2022, consulté en Juin 2022 sur:

https://www.hiscox.fr/blog/je-protege-mon-activite/cyberattaques-top-10-2021#user-popup--4901

[2] ’Qu'est-ce que l’Internet ? Réponses à 13 questions clés ’par Ian Sample, 22 Octobre 2018 ,consulté en Septembre 2021 sur :
https://www-theguardian-com.translate.goog/technology/2018/oct/22/what-is-the-internet-13-key-questions-answered?_x_tr_sl=en&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc

[3] ‘Qu'est-ce que l’internet ? ’ par Techopedia ,17 Aout 2018, consulté en Septembre 2021 sur :

https://fr.theastrologypage.com/internet#:~:text=Internet%20est%20un%20syst%C3%A8me%20de,via%20diff%C3%A9rents%20types%20de%20m%C3%A9dias.

[4] ‘Le protocole IP et TCP ‘ par Olha Nahorna, Septembre 2010, consulté en Septembre 2021 sur : http://www.gipsa-lab.grenoble-inp.fr/~olha.nahorna/Stendhal_2010-2011/L1S1-BasesNumeriques/TD4/TCP-IP.pdf

[5] ‘Adresses IP publiques et privées : quelle est la différence ? par Ellie Farrier, 9 Décembre 2021, consulté en Septembre 2021 sur :
https://www.avast.com/fr-fr/c-ip-address-public-vs-private?redirect=1#:~:text=Une%20adresse%20IP%20publique%20vous,d'autres%20appareils%20du%20r%C3%A9seau.

[6] ‘Explication : adresse IP privée et publique’ consulté en Juin 2022, sur :

https://globanet.fr/blog/2018/01/23/explication-adresse-ip-privee-et-publique/

[7] ‘C’est quoi le NAT et le PAT ?’ par culture-informatique, Janvier 2015, consulté en Septembre 2021 sur : https://culture-informatique.net/cest-quoi-le-nat-cest-quoi-le-pat/

[8] ‘Définition du DNS (Domain Namer Server)’ par actualité informatique, consulté en Septembre 2021 sur :
https://actualiteinformatique.fr/cloud/definition-du-dns-domain-namer-server

[9] ‘Comprendre les URL et leur structure’ par MDN, Mai 2022, consulté en Septembre 2021 sur : https://developer.mozilla.org/fr/docs/Learn/Common_questions/What_is_a_URL

[10] ‘Comment fonctionne l'Internet : un didacticiel étape par étape’ par Hp, 24 Mai 2019, consulté en Septembre 2021 sur : https://www.hp.com/us-en/shop/tech-takes/how-does-the-internet-work

[11] ‘VPN : avantages et inconvénients à en utiliser’ par JdG, consulté en Septembre 2021 sur :https://www.journaldugeek.com/vpn/faq/avantages-inconvenients/#:~:text=L'inconv%C3%A9nient%20des%20VPN%20c,plus%20lent%20et%20moins%20stable.

[12] ‘Quelle est la différence entre les proxys SOCKS et les proxys HTTP ?’ par Moyens staff, Janvier 2022, consulté en Septembre 2021 sur : https://www.moyens.net/tech/quelle-est-la-difference-entre-les-proxys-socks-et-les-proxys-http/#rb-qu039est-ce-qu039un-proxy-socks-5

[13] ‘Anonymat’ par Wikipedia, Mai 2022, consulté en Septembre 2021 sur : https://en.wikipedia.org/wiki/Anonymity

[14] ‘Que sont le Deep Web et le Dark Web ?’ par Kaspersky, consulté en Septembre 2021 sur : https://www.kaspersky.fr/resource-center/threats/deep-web

[15] ‘Navigation privée : comment l'activer dans un navigateur’ par Laurent Cohen, Novembre 2021, consulté en Septembre 2021 sur : https://www.commentcamarche.net/securite/confidentialite/1255-ouvrir-une-fenetre-de-navigation-privee/

[16] ‘Interface Google en navigation privée’, consulté en Septembre 2021 sur : https://www.astuces-aide-informatique.info/5818/navigation-privee

[17] ‘Qu’est-ce qu’un email jetable ?’ par Astuces & Aide Informatique, Mai 2021, consulté en Septembre 2021 sur : https://www.astuces-aide-informatique.info/6675/email-jetable

[18] 'Logo du réseau Tor', consulté en Septembre 2021 sur :
https://www.pngegg.com/fr/png-isqvf

[19] 'Tor : tout savoir sur le navigateur web qui protège vos données' par Bastien L, Décembre 2021, consulté en Septembre 2021 sur :
https://www.lebigdata.fr/tor-tout-savoir

[20] 'Logo de freenet', consulté en Septembre 2021 sur :
https://fr.wikipedia.org/wiki/Freenet

[21] 'Anonymat et Internet' par TELECOMLille1, 2007, consulté en Septembre 2021 sur :
http://wapiti.enic.fr/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2007/BouillinMorvan/les_outils.htm#:~:text=Avantages%20et%20inconv%C3%A9nients%20de%20Freenet%20%3A&text=il%20rend%20impossible%20la%20censure,le%20relais%20de%20contenus%20illicites.

[22] 'Logo I2P', consulté en Septembre 2021 sur :
https://www.redbubble.com/fr/shop/i2p

[23] 'Fonctionnement I2P' par Souleimane Aslam, 2019, consulté en Septembre 2021 sur :
https://www.ivacy.com/blog/fr/details-et-fonctionnement-i2p/ souleimane-aslam

[24] 'Top 7 des moteurs de recherche privés – services sans log' par Guy Fawkes ,2022 , consulté en Septembre 2021 sur :
https://fr.vpnmentor.com/blog/meilleurs-moteurs-de-recherche-prives-des-services-sans-aucun-log/#section-5 Matthew Amos 2022

[25] 'Interface DuckDuckGo', consulté en Septembre 2021 sur :https://fr.sawakinome.com/articles/internet/difference-between-duckduckgo-and-google.html

[26] 'Interface Swisscows', consulté en Septembre 2021 sur :https://geekflare.com/fr/search-engine-better-privacy/

[27] ’Supprimer, autoriser et gérer les cookies dans Chrome’ par Google, consulté en Septembre 2021 sur :

https://support.google.com/chrome/answer/95647?hl=fr&co=GENIE.Platform%3DAndroid

[28] ‘Mouchard : Définition’ par 1min30, consulté en Septembre 2021 sur :

https://www.1min30.com/dictionnaire-du-web/mouchard-definition

[29] ‘HTTPS : ce que cela signifie et pourquoi c’est important’ par ionos, Juin 2020, consulté en Septembre 2021 sur :

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/le-https-cest-quoi/

[30] ‘Système d'exploitation : définition, traduction et acteurs’ par journaldunet, Janvier 2019, consulté en Septembre 2021 sur :

https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203371-systeme-d-exploitation-definition-traduction-et-acteurs/#:~:text=Un%20syst%C3%A8me%20d'exploitation%2C%20ou,d'exploitation%20a%20plusieurs%20missions.

[31] ‘Logo Tails’ consulté, en Septembre 2021 sur :

https://tails.boum.org/contribute/how/promote/material/logo/[

[32] ’Présentation & Installation de Tails’ par Net Security, Février 2020, consulté en Septembre 2021 sur :

https://net-security.fr/security/privacy/tails-os/

[33] ‘Logo Qubes Os’, consulté en Septembre 2021 sur :

https://www.qubes-os.org/

[34] ‘Système d'exploitation Qubes’ par Wikipedia, Mai 2022, consulté en Septembre 2021 sur : https://en.wikipedia.org/wiki/Qubes_OS

[35] 'Logo Whonix', consulté en Septembre 2021 sur :

https://www.pngwing.com/en/search?q=whonix

[36] 'Whonix : définition et utilité' par Mallory Lebel, Avril 2019, consulté en Septembre 2021 sur : https://desgeeksetdeslettres.com/software-freeware/whonix-definition-et-utilite

[37] 'Aux origines du dark web : la naissance de Tor dans un laboratoire militaire' par Sébastien Wesolowski, Septembre 2019, consulté en Septembre 2021 sur :

https://www.vice.com/fr/article/mbmbbn/aux-origines-du-dark-web-la-naissance-de-tor-dans-un-laboratoire-militaire

[38] 'I2P' par stringfixer, consulté en Septembre 2021 sur :

https://stringfixer.com/fr/I2P

[39] 'Cloud App Security : bloquer le navigateur TOR (adresse IP anonyme)' par drware, Juin 2021, consulté en Octobre 2021 sur :

https://www.drware.com/cloud-app-security-block-tor-browser-anonymous-ip/

[40] 'Tor' par Wikipedia, Juin 2022, consulté en Octobre 2021 sur :

https://en.wikipedia.org/wiki/Tor_(network)

[41] 'Tor est-il sûr à utiliser ?' par David Janssen, Mai 2021, consulté en Octobre 2021 sur :

https://vpnoverview.com/privacy/anonymous-browsing/is-tor-safe/

[42] Mémoire de Master en Informatique Université Saad Dahelb 'Les Réseaux Anonymes TOR vs I2P « Comparaison et Détection »' par Naceur Nabil et TAIBI Mohamed 2020-2021, consulté en Octobre 2021 sur :

https://di.univ-blida.dz/jspui/handle/123456789/13375

[43] 'Comment mettre en place un proxy TOR ?' par Korben, Juillet 2020, consulté en Octobre 2021 sur :

https://korben.info/installer-proxy-tor.html

[44] ‘A Survey on I2P Crypto Mechanism’ par Miss. Dipal Vashi, et Mr. Girish Khilari 2014 IJEDR | Volume 3, Issue 1 | ISSN : 2321-9939, consulté en Octobre 2021 :

https://www.ijedr.org/papers/IJEDR1501021.pdf

[45] Yun YANG, Lingyan LI, Qingzheng WEI. Etude comparative du réseau anonyme Tor et I2P[J]. Journal chinois de la sécurité des réseaux et de l'information, 2019, 5(1) : 66-77.

[46] ’OnionDuke Malware utilisés dans les attaques APT par le réseau Tor’ par Berta Bilbao, Novembre 2014, consulté en Octobre 2021 sur :

https://sensorstechforum.com/fr/onionduke-malware-used-in-apt-attacks-through-the-tor-network/

[47] ’Qu'est-ce qu'une attaque DDoS ?’ par Kaspersky, consulté en Octobre 2021 sur :

https://www.kaspersky.fr/resource-center/threats/ddos-attacks

[48] ‘Tor : qui est le mystérieux acteur malveillant qui a mis en place des centaines de serveurs vérolés ?’ par Alexandre Horn, Décembre 2021, consulté en Novembre 2021 sur :

https://www.numerama.com/cyberguerre/762553-tor-qui-est-le-mysterieux-acteur-malveillant-qui-a-mis-en-place-des-centaines-de-serveurs-veroles.html

[49] ‘Processus de prise de contact TCP à 3 voies’ par geekforgeeks, Octobre 2021, consulté en Novembre 2021 sur :

https://www.geeksforgeeks.org/tcp-3-way-handshake-process/

[50] ‘Que se passe-t-il lors d'une négociation TLS ? | Négociation SSL’ par cloudfare, consulté en Novembre 2021 sur :

https://www.cloudflare.com/fr-fr/learning/ssl/what-happens-in-a-tls-handshake/

[51] ‘Logo du Squid proxy’, consulté en Novembre 2021 sur :

https://planete-warez.net/topic/78/s%C3%A9curit%C3%A9-installation-d-un-proxy-cache-squid-et-filtrage-via-squidguard

[52] ‘squid-cache.org’ par Squid, Mai 2009, consulté en Novembre 2021 sur :

http://www.squid-cache.org/Intro/

[53] ‘Logo Wireshark’, consulté en Novembre 2021 sur :

https://www.brandsoftheworld.com/logo/wireshark

[54] ‘Comment utiliser Wireshark : tutoriel complet + astuces’ par Jeff Petters, Mai 2021, consulté en Novembre 2021 sur :

https://www.varonis.com/fr/blog/comment-utiliser-wireshark#:~:text=Wireshark%20est%20un%20outil%20de,Frame%20Relay%20et%20plus%20encore.

[55] ‘Logo Suricata’, consulté en Novembre 2021 sur :

https://suricata.io/

[56] ‘Liste complète des fonctionnalités de Suricata’ par Suricata, consulté en Mai 2022 sur :

https://suricata.io/features/all-features/

[57] ‘Logo Snort’, consulté en Mai 2022 sur :

http://assets.stickpng.com/thumbs/586e6b2cc2d41da57a33ca0d.png

[58] ’Pourquoi Snort3’ par Snort, consulté en Mai 2022 sur :

https://www.snort.org/snort3

[59] ’IptablesHowTo’ par UbuntuDocumentation, Avril 2011, consulté en Mai 2022 sur :

https://help.ubuntu.com/community/IptablesHowTo

[60] ’Configuration des acls sur un routeur Cisco’par clemanet, consulté en Mai 2022 sur :

https://routeur.clemanet.com/acl-cisco.php

[61] ‘Post-install work’ par I2P, consulté en Mai 2022 sur :
https://geti2p.net/en/download/1.07.2/clearnet/https/files.i2p-projekt.de/I2P-Profile-Installer-1.07.2-signed.exe/download7

[62] ‘Optimisation de la sécurité dans un environnement de travail bancaire : cas de la BSIC-Togo’ par Fissale TCHAKALA, 2011, consulté en Mai 2022 sur :

https://www.memoireonline.com/10/12/6259/m_Optimisation-de-la-securite-dans-un-environnement-de-travail-bancaire-cas-de-la-BSIC-Togo16.html

[63] ‘Système de détection d’intrusion (IDS)’ par Glossaire IIoT, consulté en Mai 2022 sur :

https://iotindustriel.com/glossaire-iiot/systeme-de-detection-dintrusion-ids/#:~:text=Un%20syst%C3%A8me%20de%20d%C3%A9tection%20d'intrusion%20(IDS)%20est%20le,r%C3%A9seau%20sont%20les%20plus%20courants.

[64] ’L'écriture de règles Snort’ par Martin Roesch, Avril 2021, consulté en Mai 2022 sur :

http://www.madchat.fr/reseau/ids%7Cnids/L'%E9criture%20de%20r%E8gles%20Snort.htm