République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université SAAD DAHLEB BLIDA-1
Faculté des sciences
Département d'informatique

Mémoire de fin d'étude pour l'obtention du diplôme MASTER
Option : Systèmes Informatiques et Réseaux

Thème :

Les Réseaux Anonymes TOR vs I2P
« Comparaison et Détection »

Réalisé par :

NACEUR Nabil

TAIBI Mohamed

Soutenu devant un jury constitué de :

- Mme Boutoumi.B — Présidente
- Mme Daoud.H — Examinatrice
- Mr. Mehdi.M — Promoteur
- Mr. Benyahia.M — Encadreur

Année universitaire : 2020/2021

Remerciements

En premier lieu et avant tout nous remercions DIEU « ALLAH » le tout puissant de nous avoir donné le courage, la patience et la force de réaliser ce projet de fin d'étude.

Nous tenons à remercier très chaleureusement notre promoteur Mr. MEHDI Merouane, de nous avoir guidé tout au long de ce travail et de nous avoir aidé et conseillé, nous le remercions pour la confiance qu'il a mis en nous pour que nous puissions donner le meilleur de nous-même, Merci.

Nous vifs remerciements vont également à Mlle AMALOU Warda pour son soutien et son encouragement.

Nous tenons à exprimer notre reconnaissance à notre encadreur Mr. BENYAHIA Mohamed. Nous le remercions pour la confiance qu'il nous a accordée. Qu'il trouve en ce mémoire l'expression de notre respect infini.

Nous présentons nos respects et nos sincères remerciements aux membres du Jury qui nous ont fait l'honneur d'accepter de faire partie du jury et de nous avoir consacré de leur temps précieux.

Nous remercions tous nos collègues et amis, pour les conseils, les services et plus particulièrement pour l'amitié qu'ils nous ont témoignées.

Nous souhaitons aussi exprimer notre grande gratitude à nos familles et à toutes les personnes ayant participé de près ou de loin à la réalisation de ce projet.

Dédicaces

***J**e dédie le fruit de ce modeste travail comme un geste de gratitude*

***À** mes chers parents*

***P**our leur sacrifice, leur amour, leur soutien et encouragement tout au long de mes études*

***À** mes très chères sœurs Mouna et Meriem et frères Abderrahmane et Abdelmoumene*

***À** mon binôme Nabil*

***À** mes amis*

***À** tous les professeurs que ce soit du primaire, du moyen, du secondaire ou de l'enseignement supérieur*

Mohamed

Dédicaces

L*e premier mérite revient à mes très chers parents pour leur amour, leur compréhension et leur soutien moral et matériel*

T*ous les mots ne sauraient témoigner de ma gratitude, de mon amour, mon respect, mon admiration, et de ma reconnaissance. Que dieu leur procure bonne santé et longue vie.*

À *ma très chère sœur Ryme, et* ***À*** *ma chère Gadji*

À *mes chers frères Djihad et Mustapha*

P*our leurs encouragements*

À *toute ma famille*

À *tous mes amis*

A*insi qu'à tous ceux qui me sont chers*

NABIL

Résumé

ملخص:

في هذه الأطروحة، نقترح موضوعًا يتعلق بالشبكات المجهولة الأكثر شيوعًا: طور وإيدوبي ، سيؤدي استخدام طور وإيدوبي في المؤسسة إلى مخاطر أمنية بالإضافة إلى مشاكل قانونية. الغرض من هذا الملخص هو مقارنة وكشف استخدام شبكة طور وإيدوبي.

تقدم هذه الأطروحة أولاً مفاهيم إخفاء الهوية والخصوصية، ثم المقارنة النظرية بين الشبكتين المجهولين طور وإيدوبي. يتم الكشف عن هذه من خلال مقارنة حركة المرور الخاصة بهم بحركة مرور الويب العادية للحصول على بصمات رقمية تميز هاتين الشبكتين. سيتم وضع هاته البصمات في نظام كشف التسلل "سنورت" لإطلاق تنبيه في كل محاولة اتصال مع هاتين الشبكتين المجهولتين.

الكلمات المفتاحية: شبكة طور ; شبكة إيدوبيشخير ;نظام كشف التسلل "سنورت" ; بصمات رقمية ; حركة مرور الويب.

Résumé :

Dans le cadre de ce mémoire, nous proposons un sujet concernant les réseaux anonymes les plus populaires : Tor et I2P, l'utilisation de Tor et I2P au sein d'entreprise entraînera des risques de sécurité ainsi que des problèmes judiciaires. L'objectif de notre projet est la comparaison et la détection de l'utilisation du réseau Tor et I2P.

Ce mémoire présente dans un premier temps les notions d'anonymat et de la vie privée, puis la comparaison théorique entre les deux réseaux anonymes Tor et I2P. La détection de ces derniers se fait en comparant leur trafic avec le trafic Web normal pour obtenir des empreintes numériques qui caractérisent ces deux réseaux Tor et I2P. Ces empreintes seront implémentées dans un IDS "Snort" pour entrainer une alerte à chaque tentative de connexion à Tor ou à I2P.

Mots clés : Réseau Tor ; réseau I2P ; Snort ; IDS ; anonymat ; empreintes numériques ; trafic web.

Abstract:

For this thesis, we propose a topic concerning the most popular anonymous networks: Tor and I2P, the use of Tor and I2P in the enterprise will lead to security risks as well as legal problems. The purpose of this brief is to compare and detect Tor and I2P network usage.

This thesis first presents the concepts of anonymity and privacy, then the theoretical comparison between the two anonymous networks Tor and I2P. The latter are detected by comparing their traffic with normal web traffic to obtain digital fingerprints that characterize these two Tor and I2P networks. These fingerprints will be implemented in an IDS "Snort" to trigger an alert on each connection attempt to Tor or i2P.

Keywords: Tor Network; I2P network; Snort; IDS; anonymity; digital fingerprints; web traffic.

Liste des abréviations

4G: 4 Generation.

ACK: Acknowledge.

ACL: Access Control List

AES: Advanced Encryption Standard.

API: Application Programming Interface.

ARPANET: Advanced Research Projects Agency networks.

CARP: Cache Array Routing Protocol.

CBC: Cipher Block Chaining.

CERN: European Organization for Nuclear Research.

CMD: Command Prompt.

CMS:Continuous Management System.

CPU: Central Processing Unit.

CSS: Cascading Style Sheets.

DAQ: Data Acquisition.

DDOS: Distributed Denial of Service.

DH: Diffie-Hellman.

DHCP: Dynamic Host Configuration Protocol.

DLM: Dynamic Line Management.

DNS: Domain Name System.

DOS: Denial of Service attack.

DPI: Deep packet inspection.

ECDHE: Elliptic Curve Diffie–Hellman Key Exchange.

ECDSA : EllipticCurve Digital Signature Algorithm.

FAI : Fournisseurs d'Accès Internet.

FTP: File Transfer Protocol.

GB: Gigabyte.

GHz: Gigahertz.

HIDS: Host based intrusion detection system.

HIPAA: Health Insurance Portability and Accountability Act.

HSDIR: Hidden Service Directories.

HTCP: Hyper Text Caching Protocol.

HTML: Hypertext Markup Language.

HTTPMU: HTTP Multicast over UDP.

HTTPS: Hypertext Transfer Protocol Secure.

HTTPS: Hypertext Transfer Protocol.

I2P: Invisible Internet Project.

ICMP: Internet Control Message Protocol.

ICP: Internet Cache Protocol.

IDS: Intrusion detection System.

IE: Internet Explorer.

IMAP: Internet Message Access Protocol.

IOT: Internet of Things.

IP: Internet Protocol.

IRC: Internet Relay Chat.

IV: Initialization Vector.

LAN: Local Area Network.

LTE: Long Term Evolution.

MAC: Media Access Control.

MIRC: Internet Relay Chat client.

MiTM: Man-in-the-middle.

MSS: Maximum Segment Size.

NetDB: Network Tracking Database.

Liste des abréviations

NIDS: Network Intrusion Detection System.

NIO: New IO

NSA: National Security Agency.

NTCP: Network Time Control Protocol.

NTP: Network Time Protocol.

OCSP: Online Certificate Status Protocol.

OP: Out Proxy.

OR: Onion Router.

OS: Operating System.

OSI: Open Systems Interconnection.

P2P: Peer-to-Peer.

PCAP: Packet Capture.

PDF : Portable Document Format.

POP: Post Office Protocol.

PSH: Push.

RAM: Random Access Memory.

RFC: Requests For Comments.

RJ45: Registered Jack.

RLOGIN: Remote Login

RSH: remote shell.

RST: Reset.

RTT: Round Trip Time.

RVP: Réseau Virtuel Privé.

SHA: Secure Hash Algorithm.

SMTP: Simple Mail Transfer Protocol.

SNMP: Simple Network Management Protocol.

SSDP: Simple Service Discovery Protocol.

SSH: Secure Shell.

SSL: Secure Socket Layer.

SSU: Synchronization Supply Unit.

SYN: Synchronize.

SYN-ACK:Synchronize Acknowledge.

TAP: Terminal Access Point.

TCP: Transmission Control Protocol.

Telnet: Terminal Network ou Telecommunication Network.

TLS: Transport Layer Security.

TOR: The Onion of Routing.

TOS: Type of Service

TTL: Time to live.

UDP: User Datagram Protocol.

UPnOP: Universal Plugin Play.

URG: Urgent Flag.

URL: Uniform Resource Locator.

UTC : Université de technologie de Compiègne.

VPN: Virtual Private Network.

WCCP: Web Cache Coordination Protocol.

WEB: World Wide Web.

WIFI: Wireless Fidelity.

XOR: Exclusively-OR.

Table des matières

Liste des figures

Liste des figures

Liste des figures

Liste des tableaux

Introduction générale

Au fil des années, Internet est devenu une valeur indispensable à la vie sociale, économique et politique. Malgré cela, Internet sous toutes ses formes et tous ses protocoles s'est avéré extrêmement sensible à la manipulation par les forces contrôlant l'infrastructure d'Internet. Parallèlement à la croissance d'Internet, il y a eu la croissance de la censure et du filtrage par les gouvernements. Les forces gouvernementales du monde entier ont filtré, bloqué et écouté le trafic réseau pour des raisons à la fois économiques et politiques. Dans le monde développé, plus de 77 % de la population a accès à Internet [1]. Les gens utilisent Internet comme moyen de communication, source d'information, source de divertissement et assistant commercial.

Dans la vie sociale et économique quotidienne, Internet joue un rôle de plus en plus important. Les immenses avantages offerts par Internet apportent des inconvénients obscurs dont les utilisateurs ne sont souvent pas conscients. Les récentes fuites de Snowden ont donné matière à réflexion à de nombreux internautes. L'Agence nationale de la sécurité était connue depuis longtemps pour avoir collecté des enregistrements de plus de 1 900 milliards d'appels téléphoniques avec MAINWAY2 [2], et Edward Snowden a révélé que ce n'est rien comparé aux méthodes de surveillance de masse qui sont actuellement déployées. Le centre de données de la NSA dans l'Utah est même supposé avoir des yottaoctets de stockage [3]. Ce terme est peu familier même pour les informaticiens, car il est si rarement utilisé. Un yottaoctet équivaut à 1024 ou 1.000.000.000.000.000.000.000.000 octets. C'est plus que suffisant pour avoir un moniteur vidéo et audio haute définition de chaque personne sur la planète 24h/24 et 7j/7 pendant plus d'un an. Le modèle complet, l'infrastructure et les protocoles utilisés dans l'Internet actuel permettent une surveillance de masse sur chaque couche du système.

1 Source Union internationale des télécommunications:
http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls/

2 En savoir plus sur MAINWAY ici:
http://www.democracynow.org/2006/5/12/three_major_telecom_companies_help_us/

3 Plus d'informations sur le centre de données de l'Utah:
http://siliconangle.com/blog/2013/07/29/the-mind-boggling-capacity-of-the-nsas-utah-facility/

Introduction générale

La communication électronique privée devient de plus en plus une question publique importante. Le cryptage peut effectivement cacher le contenu d'une conversation aux oreilles indiscrètes, et cette protection est intégrée dans de nombreux systèmes.

Qui communique avec qui? Les utilisateurs de messagerie peuvent souhaiter masquer leurs adresses. L'argent anonyme n'est pas anonyme si le canal de communication identifie l'acheteur. La quantité d'informations révélées par la navigation sur le Web doit être délibérée. La Collaboration inter-entreprises peut être confidentielle.

Un objectif de l'analyse du trafic est de révéler qui parle à qui. Les connexions anonymes décrites ici sont conçues pour résister à l'analyse du trafic, c'est-à-dire pour empêcher les observateurs d'apprendre des informations d'identification à partir de la connexion (par exemple, en lisant les en-têtes de paquets, en suivant les charges utiles chiffrées, etc.). Toute information d'identification doit être transmise en tant que données via les connexions anonymes. Notre mise en œuvre de connexions anonymes, le routage en oignon, offre une protection contre l'écoute clandestine en tant qu'effet secondaire. Le routage en oignon fournit une communication bidirectionnelle et en temps quasi réel similaire aux connexions socket TCP/IP.

Les connexions anonymes peuvent remplacer les sockets dans une grande variété d'applications Internet non modifiées au moyen de proxy. Les mandataires peuvent également supprimer des informations d'identification du flux de données, pour communication anonyme aussi.

L'objectif principal de notre travail est d'étudier les deux réseaux anonymes les plus populaires : Tor et I2P. L'utilisation de Tor et I2P au sein de l'entreprise entraîne des risques de sécurité ainsi que des problèmes judiciaires. Donc, Il s'agit de réaliser une comparaison théorique entre ces deux réseaux et leur détection afin que l'entreprise utilisateur puisse prendre des décisions sur l'utilisation de ces deux réseaux. Pour cela, Les étapes suivantes seront suivies :

- **La première étape :** consiste à présenter les deux réseaux anonymes, en se concentrant sur leurs fonctionnements et le cryptage utilisé, puis nous comparerons TOR et i2P en termes de terminologie, d'utilisation et de technologie utilisée.

- **La deuxième étape :** est basée sur une architecture client-serveur, nous utilisons des PC serveurs et des PC clients. Nous installerons le logiciel Squid pour bloquer certains

sites afin de simuler un réseau d'entreprise. Ensuite, nous allons installer le navigateur Tor pour contourner le proxy et naviguer librement sur Internet, puis installer 12P et accéder à ses différents services.

- **La troisième étape :** est basée sur l'utilisation d'un analyseur de paquets « wireshark », qui nous permettra d'extraire la différence entre Tor et IP en termes de vitesse, de latence, de bande passante et de signatures numériques.

- Enfin, ces signatures numériques nous mènent vers une création des règles dans le système de détection d'intrusion "IDS" afin que l'utilisation de Tor et i2P puisse être détectée.

Le mémoire est composé de quatre chapitres organisés comme suit :

Le premier chapitre présente un état de l'art sur les réseaux anonymes.

Le deuxième chapitre introduit la théorie des deux réseaux anonymes Tor et I2P. Le chapitre commence par la présentation des définitions des deux réseaux ainsi leur fonctionnement, leur mécanisme et leur architecture. Une comparaison théorique entre les deux réseaux sera décrite par la suite.

Le troisième chapitre est consacré à la façon d'identifier les deux réseaux à travers de l'extraction des signatures Tor et I2P.

Le quatrième chapitre présente une implémentation des signatures dans le système de Détection d'Intrusion Snort (IDS).

Enfin une conclusion termine ce travail, donnant quelques perspectives pour des travaux futures.

Chapitre 1

Les Réseaux Anonymes

1.1 Introduction

Avec le développement de la technique des réseaux et la prévalence du réseau, la protection de la vie privée des personnes est devenue un hotspot. Cependant, la technologie de la sécurité traditionnelle crypte la charge utile des données des communications sans cacher l'expéditeur, le destinataire et les relations entre eux.

Par conséquent, les attaquants peuvent facilement obtenir des informations sur les cibles telles que l'adresse source, l'adresse de destination et l'identité de l'utilisateur.

Afin de réduire le risque d'exposer les parties de communication, l'outil de communication anonyme adopte une route sinueuse et difficile à suivre plutôt que de prendre une route directe de la source à une destination.

Une technologie de communication anonyme comme une épée à double tranchant. D'une part, elle assure non seulement la protection des utilisateurs du réseau, mais offre également au pirate informatique un outil pour cacher ses traces. D'un autre côté, s'il tombe entre de mauvaises mains, elle peut être utilisée pour connecter la cible sans être pistée.

1.2 Internet

1.2.1 Définition

Internet est un système mondial de réseaux informatiques interconnectés. Lorsque deux ou plusieurs appareils électroniques (par exemple, des ordinateurs) sont connectés afin qu'ils puissent communiquer, ils font partie d'un réseau. Internet consiste en une interconnexion mondiale de tels réseaux, appartenant à des entreprises, des gouvernements et des individus, permettant à tous les appareils connectés à ces réseaux de communiquer entre eux [1].

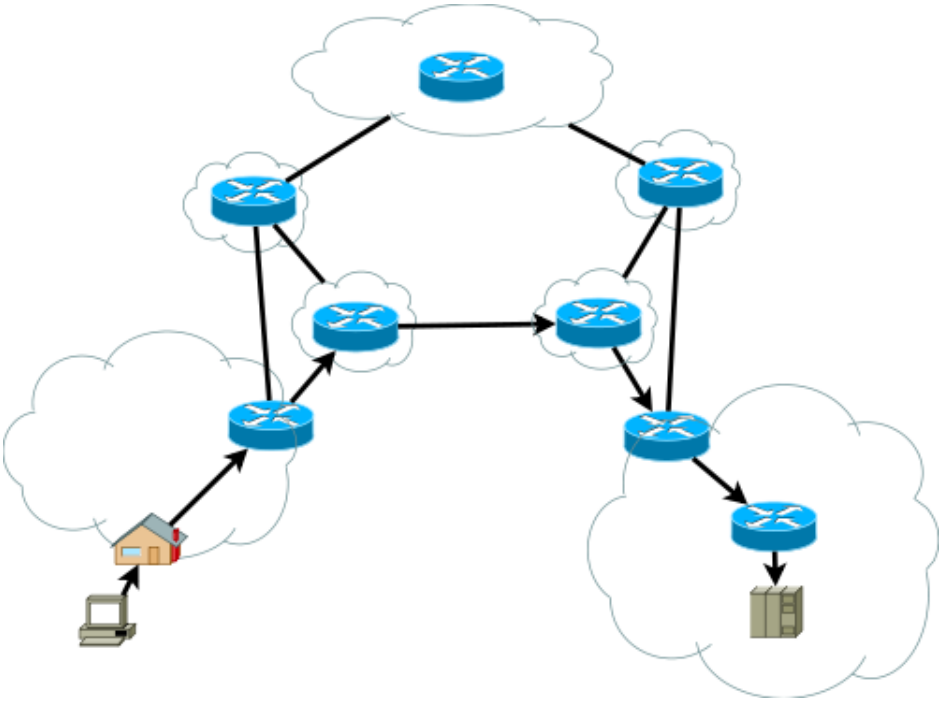

Figure 1.1: *Le réseau internet[31].*

1.2.2 Origine de l'Internet :

Le réseau ARPANET (Advanced Research Projects Agency Network) est le premier réseau mondial de communication par **paquet**, crée au milieu des années 1960 et patronné par le ministère de la défense américaine. C'est sur ce réseau que les protocoles TCP/IP ont été développés au milieu des années 1970, puis unifiés sur tout le réseau. Les scientifiques ont pris ensuite le contrôle de ce réseau, ce qui leur a permis de communiquer plus facilement entre eux sur l'avancée de leurs travaux, et à partir de 1995, Internet s'est ouvert au grand public [2].

Sur Internet, de nombreux protocoles sont utilisés, ils font partie d'une suite de protocoles qui s'appelle TCP/IP. TCP/IP repère chaque ordinateur par une adresse appelée adresse IP qui permet d'acheminer les données à la bonne adresse. Puis on associe à ces adresses des noms de domaine (le nom de la machine dans un domaine) pour une utilisation plus facile de la navigation Internet.

1.2.3 Fonctionnement de l'Internet

Pour communiquer, les ordinateurs doivent pouvoir se comprendre. Sur Internet, la communication est possible car tous les appareils utilisent le même « langage » ou protocole, à savoir le protocole Internet (IP), un « marché unique » sans barrières physiques, techniques ou nationales. Il constitue la base de tous les autres systèmes de communication sur Internet [1].

a. Protocole IP

Le protocole Internet (IP) est un protocole, ou un ensemble de règles, pour le routage et l'adressage des paquets de données afin qu'ils puissent voyager à travers les réseaux et arriver à la bonne destination. Les données qui traversent Internet sont divisées en morceaux plus petites, appelées paquets. Des informations IP sont attachées à chaque paquet, et ces informations aident les routeurs à envoyer les paquets au bon endroit. Chaque appareil ou domaine qui se connecte à Internet se voit attribuer une adresse IP, et comme les paquets sont dirigés vers l'adresse IP qui leur est attachée, les données arrivent là où elles sont nécessaires.

b. L'adressage IP

Une adresse IP (Internet Protocol) est une représentation numérique qui identifie de façon unique une interface donnée sur le réseau.

L'acronyme IP, qui signifie « Internet Protocol », désigne un ensemble de normes et contraintes qui s'appliquent à la création et à la transmission sur les réseaux de paquets de données, aussi appelés datagrammes. Le protocole IP fait partie de la couche Internet de la suite de protocoles Internet. Dans le modèle OSI, IP appartiendrait à la couche réseau. Le protocole est la plupart du temps associé à un protocole de niveau supérieur, généralement TCP. La norme IP est décrite dans la figure 1.2 .

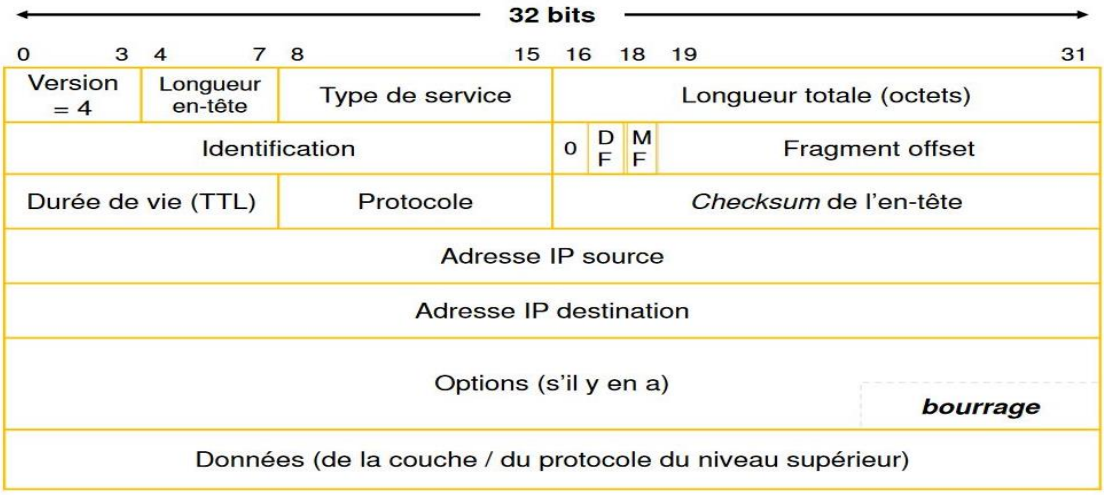

Figure 1.2:*Format d'un paquet IP.*

L'envoi de toute communication sur Internet à l'aide du protocole Internet revient à envoyer les pages d'un livre par la poste dans de nombreuses enveloppes différentes.

Sur Internet, le contenu de l'enveloppe est également basé sur des conventions/protocoles (formats convenus), un pour chaque type de communication :

Services	Protocoles
Navigation	HTTP/HTTPS
Téléchargement	FTP
E-mail	POP, SMTP & IMAP
P2P	BitTorrent
Discuter	IRC
Connexion à distance	Telnet & SSH

Tableau 1-1: *Les services et les protocoles de la communication sur internet.*

On assigne à chacun de ces protocoles un numéro (le port) qui est transmis lors de la communication (la transmission est effectuée par petits paquets d'information). Ainsi, il est possible de savoir à quel programme correspond chaque petit paquet :

- Les paquets HTTP arrivent sur le port 80 et sont transmis au navigateur Internet à partir duquel la page a été appelée.

- Le port 21 est le numéro de port utilisé par défaut par le protocole FTP.
- Les paquets IRC arrivent sur le port 6667 (ou un autre situé généralement autour de 7000) et sont transmis à un programme client de chat tel que mIRC (ou autre).

N'importe qui est libre d'inventer sa propre convention/protocole et de l'utiliser sur Internet, tant qu'il fonctionne sur le protocole Internet. Autrement dit : la seule limite est la limite de l'imagination humaine, la seule règle est que l'adresse sur l'enveloppe soit dans un format standard. L'ouverture du système est ce qui fait d'Internet le phénomène mondial qu'il est. Chaque restriction à l'ouverture d'Internet réduit son potentiel de développement futur. L'utilisation universelle d'un protocole unique pour toutes les communications présente un certain nombre d'avantages importants.

Cela mène à :

- Des possibilités d'innovation illimitées en termes de nouveaux protocoles et applications ;
- « Privacy by design » : il n'est pas nécessaire de savoir quoi que ce soit sur le contenu de toute communication ;
- Flux de données flexible et rapide ;

Fondamentalement, Internet n'offre qu'un seul service flexible : transférer des données d'un appareil à un autre quelle que soit la nature des appareils, quels que soient le mode et l'endroit où les appareils sont connectés à Internet et quelle que soit la nature ou le contenu des données. C'est cette ouverture et cette flexibilité qui sont la principale raison de l'innovation et des succès démocratiques et économiques d'Internet.

1.3 Le Web

1.3.1 Définition de Web

World Wide Web (WWW), sous le nom de Web, le premier service de recherche d'informations sur Internet (le réseau informatique mondial). Le Web donne aux utilisateurs l'accès à une vaste gamme de documents qui sont connectés les uns aux autres au moyen de liens hypertextes ou hypermédias, c'est-à-dire des hyperliens, des connexions électroniques qui relient des éléments d'information connexes afin de permettre à un utilisateur d'y accéder facilement. L'hypertexte permet à l'utilisateur de sélectionner un mot ou une phrase dans le

texte et ainsi d'accéder à d'autres documents contenant des informations supplémentaires relatives à ce mot ou à cette phrase. Les documents hypermédias comportent des liens vers des images, des sons, des animations et des films [3].

1.3.2 Historique de Web

Le développement du World Wide Web a commencé en 1989 par Tim Berners-Lee et ses collègues du CERN, une organisation scientifique internationale basée à Genève, en Suisse. Ils ont créé un protocole, HyperText Transfer Protocol (HTTP), qui standardise la communication entre les serveurs et les clients. Leur navigateur Web basé sur du texte a été mis à disposition pour une diffusion générale en janvier 1992.

Le World Wide Web a été rapidement accepté avec la création d'un navigateur Web appelé Mosaic, qui a été développé aux États-Unis par Marc Andreessen et d'autres au "National Center for Super Computing Applications".

Les travaux Internet de "BookLink Technologies", le premier navigateur à onglets, dans lequel un utilisateur pouvait visiter un autre site Web sans ouvrir une nouvelle fenêtre, a fait ses débuts la même année. Au milieu des années 90, le World Wide Web comptait des millions d'utilisateurs actifs.

Le géant du logiciel Microsoft Corporation s'est intéressé à la prise en charge des applications Internet sur les ordinateurs personnels et a développé son propre navigateur Web (basé initialement sur Mosaic), Internet Explorer (IE), en 1995 en tant que module complémentaire du système d'exploitation Windows 95. IE a été intégré au système d'exploitation Windows en 1996 [3].

1.3.3 Fonctionnement de Web

Le Web fonctionne dans le format client-serveur de base d'Internet ; Les serveurs sont des programmes informatiques qui stockent et transmettent des documents à d'autres ordinateurs sur le réseau lorsqu'on le leur demande, tandis que les clients sont des programmes qui demandent des documents à un serveur lorsque l'utilisateur les demande. Le logiciel de navigation permet aux utilisateurs de visualiser les documents récupérés.

Un document hypertexte avec son texte et ses liens hypertexte correspondants est écrit en langage de balisage hypertexte (HTML) et se voit attribuer une adresse en ligne appelée URL (Uniform Resource Locator).

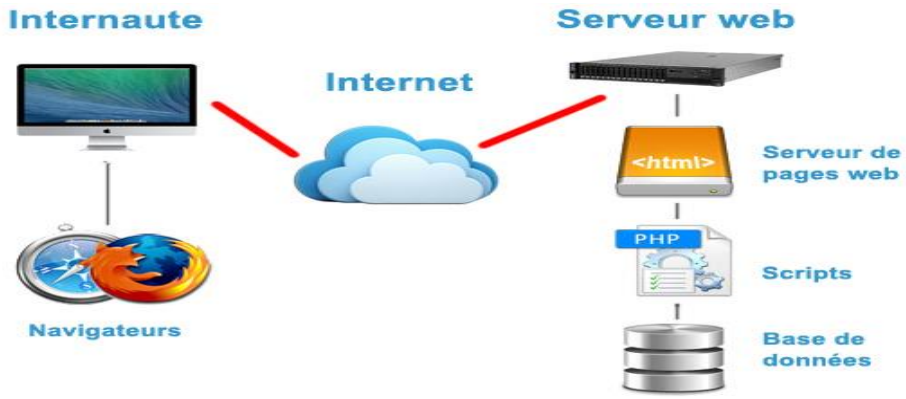

Figure 1.3 : *Mode de fonctionnement des applications Web [32].*

a. L'architecture à 2 niveaux :

L'architecture à deux niveaux (aussi appelée architecture 2-tier, tier signifiant rangée en anglais) caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service [4].

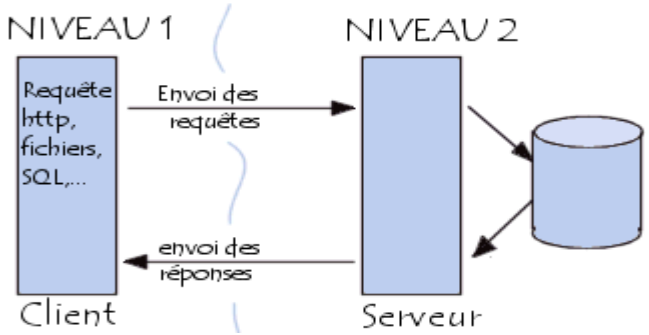

Figure 1.4: *L'architecture à 2 niveaux [33].*

b. L'architecture à 3 niveaux :

Dans l'architecture à 3 niveaux (appelée architecture 3-tier), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre [4]:

1. Un client, c'est-à-dire l'ordinateur demandeur de ressources, équipée d'une interface utilisateur (généralement un navigateur web) chargée de la présentation.
2. Le serveur d'application (appelé également middleware), chargé de fournir la ressource mais faisant appel à un autre serveur.

3. Le serveur de données, fournissant au serveur d'application les données dont il a besoin.

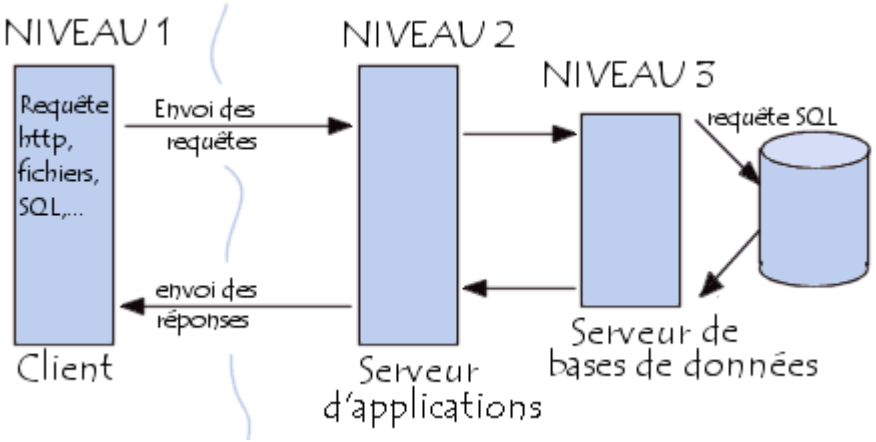

Figure 1.5: *L'architecture à 3 niveaux[33].*

c. Site Web statique

Les sites Web statiques consistent en un nombre fixe de pages Web pré-rendues contenant un contenu et une structure fixes codés en dur. En conséquence, les utilisateurs voient le même contenu, peu importe qui ils sont, d'où ils viennent et quel navigateur ils utilisent.

Les programmeurs Web créent généralement des pages de site Web statiques en utilisant HTML pour configurer la structure et CSS pour ajouter de la couleur et d'autres éléments visuels. Les pages Web statiques sont généralement construites indépendamment, sans connexion à une base de données.

d. Site Web dynamique :

Les sites Web dynamiques génèrent des pages en temps réel. La flexibilité du contenu et de la structure permet de personnaliser l'expérience d'un utilisateur en fonction de sa demande ou du navigateur qu'il utilise. La création d'un site Web dynamique nécessite généralement la connaissance d'un langage de programmation côté serveur comme PHP, C ou Python. Les sites Web dynamiques traitent les demandes et extraient généralement le contenu d'une base de données externe ou d'un système de gestion de contenu (CMS).

Le tableau 1.2 nous montre la comparaison entre le site Web statique et dynamique :

	Les sites web statiques	Les sites web dynamiques
Présentation	Les pages Web statiques resteront les mêmes jusqu'à ce que quelqu'un le modifie manuellement, à moins que quelqu'un le modifie.	Les pages Web dynamiques sont comportementales et ont la capacité de produire un contenu distinct pour différents visiteurs.
Base de données	N'utilise pas de bases de données	Une base de données est utilisée.
Temps de chargement de la page	Demande moins de temps	Demande plus de temps
Changement d'information	Se produit rarement	Fréquemment
Complexité	Simple à concevoir.	Compliqué à construire.

Tableau 1-2: *comparaison entre site web statique et dynamique.*

1.4 Le système de nom de domaine (DNS)

Lorsque vous mettez un site Web sur Internet, il sera accessible via l'adresse IP numérique du serveur Web qui l'héberge. Les adresses IP ne sont cependant pas faciles à retenir pour les humains. Les utiliser pour identifier les ressources en ligne n'est pas non plus pratique car les services sur Internet doivent parfois se déplacer vers une nouvelle adresse IP (s'ils changent de fournisseur de services, par exemple).

Comme l'utilisation d'adresses IP pour les sites Web n'est ni pratique ni conviviale, des « noms de domaine » (comme etu.univ-blida.dz) ont été créés. Le système mondial de noms de domaine fonctionne un peu comme un annuaire téléphonique pour Internet.

Le système de recherche d'un nom de domaine fonctionne sur la base d'une hiérarchie. Lorsque vous tapez http://edri.org, votre ordinateur se connecte d'abord à un serveur pour demander l'adresse. Le serveur DNS par défaut est généralement géré par notre fournisseur d'accès Internet, mais il est possible d'en utiliser un autre.

Figure 1.6: *Fonctionnement de DNS.*

1.5 Les profondeurs d'Internet

Internet est vaste. Il compte des millions de pages Web, de bases de données et de serveurs qui fonctionnent tous 24 heures sur 24. Cependant, l'Internet « visible » (également appelé Web de surface ou Web visible), composé de sites accessibles à l'aide de moteurs de recherche, comme Google et Yahoo, ne constitue que la partie émergée de l'iceberg. Il existe un certain nombre de termes pour qualifier le Web non visible, mais mieux vaut connaître leurs différences si vous prévoyez de naviguer hors des sentiers battus [5].

1.5.1 Le Web de surface (Web visible)

Le Web visible, ou le Web de surface, est la couche de surface « visible ». Si nous continuons à visualiser l'ensemble du Web comme un iceberg, le Web visible serait la partie supérieure qui se trouve au-dessus de l'eau. D'un point de vue statistique, cet ensemble de sites Web et de données représente 4% du volume total d'Internet.

Tous les sites Web accessibles au public via des navigateurs traditionnels, comme Google Chrome, Internet Explorer et Firefox, sont présentés ici. Les sites Web sont généralement étiquetés avec des opérateurs de registre, comme « .com » et « .org », et peuvent être facilement localisés au moyen des moteurs de recherche populaires.

La localisation de sites Web de surface est possible parce que les moteurs de recherche peuvent indexer le Web au moyen de liens visibles (il s'agit d'un processus appelé « exploration du Web » en raison du fait que le moteur de recherche parcourt le Web comme une araignée)[6].

1.5.2 Le Web profond (Deep web)

Le Web profond se trouve sous la surface et représente environ 90 % de tous les sites Web. Il s'agit de la partie d'un iceberg sous l'eau, beaucoup plus grande que le Web de surface. En fait, ce Web invisible est si vaste qu'il est impossible de savoir précisément combien de pages ou de sites Web sont actifs à la fois.

Pour poursuivre l'analogie, les grands moteurs de recherche pourraient être considérés comme des bateaux de pêche qui ne peuvent « attraper » que les sites Web proches de la surface. Tout le reste, des revues universitaires à des bases de données privées en passant par du contenu plus illicite, est hors de portée. Ce Web profond comprend également la partie que nous connaissons sous le nom de Dark Web.

Bien que de nombreux médias utilisent indifféremment les expressions « Deep Web » et « Dark Web », une grande partie du Web profond dans son ensemble est parfaitement légale et sûre. Parmi les parties les plus importantes du Web profond, on trouve ce qui suit :

1. **Bases de données** : collections de fichiers publics et privés protégés qui ne sont pas connectés à d'autres zones du Web, mais qui peuvent être consultés dans la base de données elle-même.
2. **Intranets** : réseaux internes d'entreprises, de gouvernements et d'établissements d'enseignement utilisés pour communiquer et contrôler certains éléments à titre privé au sein de leurs organisations.

Le contenu « caché » du Web profond est généralement plus qualitatif et plus sûr. Qu'il s'agisse d'articles de blog à réviser, de pages Web à repenser, ou encore des pages auxquelles vous accédez lorsque vous effectuez des opérations bancaires en ligne, toutes ces ressources font partie du Web profond. En outre, ces pages ne constituent aucune menace pour votre ordinateur ni pour votre sécurité en général. La plupart de ces pages sont cachées du Web visible pour protéger les informations et la vie privée des utilisateurs, par exemple :

- Les comptes financiers comme les comptes bancaires et les comptes de retraite.
- Les comptes de messagerie électronique et sociale.
- Les bases de données privées des entreprises.
- Les renseignements sensibles de la HIPAA, comme les documents médicaux.
- Les dossiers légaux.

En s'aventurant plus loin dans le Deep Web, on s'expose un peu plus au danger. Pour certains utilisateurs, certaines parties du Web profond permettent de contourner des restrictions locales et d'accéder à des services télévisés ou à des films qui peuvent ne pas être proposés dans leur région. Pour d'autres, ces endroits offrent la possibilité de télécharger de la musique piratée ou de voler des films qui ne sont pas encore sortis au cinéma [6].

1.5.3 Le Dark Web

Le Dark Web fait référence à des sites qui ne sont pas indexés et qui ne sont accessibles que par des navigateurs Web spécialement conçus à cet effet. Beaucoup plus petit que le minuscule Web de surface, le Dark Web est considéré comme faisant partie du Web profond. Si l'on se base sur notre illustration de l'océan et des icebergs, le Dark Web serait la partie inférieure de l'iceberg submergé.

Une analyse de la construction du Dark Web révèle quelques couches clés qui en font un havre d'anonymat :

- Aucune indexation des pages Web par les moteurs de recherche du Web de surface. Google et d'autres outils de recherche populaires ne peuvent pas détecter ni afficher les résultats des pages du Dark Web.
- Présence de « tunnels de circulation virtuels » via une infrastructure de réseau randomisée.
- Inaccessible par les navigateurs traditionnels en raison de son opérateur de registre unique. En outre, il est encore plus caché par diverses mesures de sécurité réseau, comme des pare-feu et du chiffrement.
- En ce qui concerne la sécurité, les dangers du Web profond sont très différents de ceux du Dark Web. IL n'est pas forcément facile de tomber sur une cyber activité illégale, mais celle-ci tend à être beaucoup plus dangereuse et menaçante si vous la découvrez. Avant de dévoiler les menaces liées au Dark Web, voyons comment et pourquoi les utilisateurs accèdent à ces sites [6].

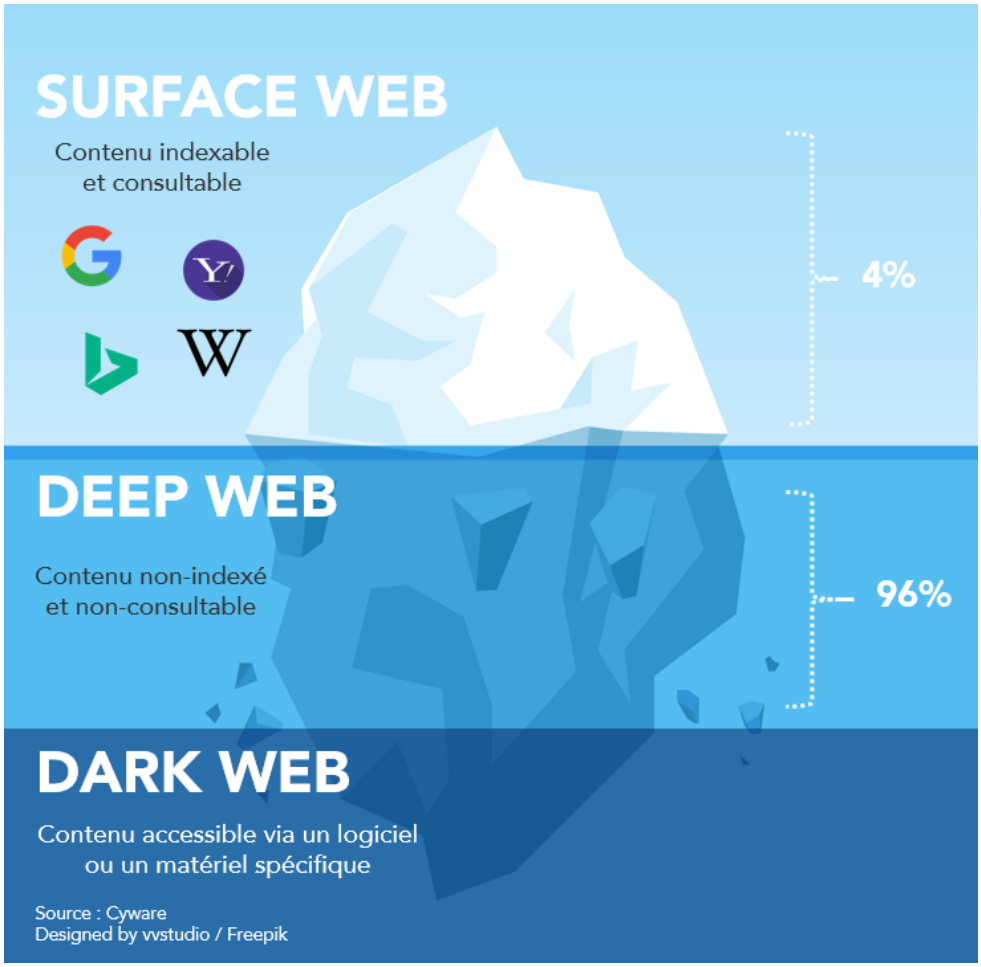

Figure 1.7: *Les différentes interfaces Web[34].*

1.6 Anonymat sur Internet

Anonymat et vie privée sont très souvent associés. Le premier est un moyen de préserver la seconde. La vie privée est la raison pour laquelle on peut recourir à des techniques d'anonymisation. Internet bouleverse la manière dont nous gérons notre vie privée.

La vie privée ne peut se comprendre qu'en termes de contrôle de ce qu'on laisse sur internet. Elle consiste à conserver le contrôle d'une information personnelle et ne pas la laisser sortir d'un cadre dans lequel elle a été rendue publique.

Sur internet, l'utilisateur ne laisse pas seulement des traces volontairement et de manière visible. S'il existe bien des traces visibles et intentionnelles (commentaire sur un blog, photo sur les réseaux sociaux), les traces invisibles et non intentionnelles sont d'autant plus nombreuses (l'adresse IP quand on se connecte à un site internet, requête dans les archives d'un moteur de recherche). Il est donc nécessaire, pour garantir l'anonymat au seind'un

réseau de communication, de considérer l'existence d'attaquants. Un attaquant souhaite surveiller ou manipuler les communications du réseau [7].

1.7 Surveillance sur Internet

1.7.1 DeepPacket Inspection

Plusieurs technologies ont été déployées pour observer les communications sur Internet. On nomme l'analyse du contenu de paquet réseau "DeepPacket Inspection" ou "Inspection des paquets en profondeur" en français abrégé DPI.IL se base sur le modèle OSI pour analyser les possibilités d'écoute sur chaque couche du TCP/IP [8]:

1. **La couche physique :** Toute écoute sur cette couche demande un accès direct au matériel. Chaque type de réseau (RJ45, fibre optique, WIFI, etc.) a son propre TAP réseau.
2. **La couche liaison :** La plupart des technologies ciblant cette couche analysent les adresses MAC leur permettant d'identifier les constructeurs et les modèles des interfaces présentes sur le réseau.
3. **La couche réseau :** C'est la couche la plus importante pour l'analyse du trafic Internet. La capture de paquet IP permet d'analyser leurs entêtes et d'obtenir l'adresse IP source et l'adresse IP de destination, ainsi que le protocole de transport employé. L'obtention d'une d'adresse IP permet d'identifier directement l'utilisateur.
4. **La couche transport :** Étant donné que le TCP est le protocole de cette couche le plus utilisé, c'est celui-ci qui est le plus ciblé pour les écoutes. L'entête TCP contient le port source et le port destination permettant de déterminer quel service est utilisé. De plus, toutes les données non cryptées au-dessus de cette couche permettent d'obtenir le contenu en clair de la transmission.
5. **La couche application :** L'analyse du trafic sur cette couche diffère suivant le protocole ciblé. Le trafic Web et le trafic de courriel sont le plus souvent ciblés étant donné que les informations qu'elles contiennent peuvent être critiques.

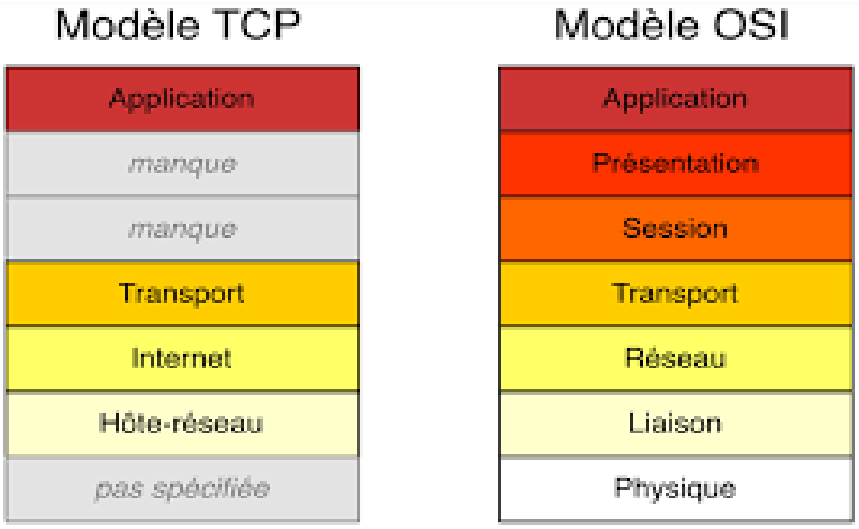

Figure 1.8: *Les différentes couches du model TCP/IP[35].*

1.7.2 Attaques basées sur les applications

Aussi à prendre en compte, le but principal est l'obtention de l'adresse IP de l'utilisateur sans avoir besoin d'analyser le réseau, mais l'adresse IP n'est pas la seule information permettant d'identifier l'utilisateur [9].

Nous verrons donc après avoir faire un tour d'horizon des différentes menaces de votre anonymat et donc plus ou moins directement, de votre vie privée :

- **Plug-ins :** Les plug-ins ajoutent des fonctionnalités sur le navigateur Web, mais peuvent permettre à un attaquant d'établir une connexion directe à l'utilisateur. Les plug-ins les plus connus sont Flash développé par AbobeSystems ainsi que QuickTime développé par Apple. L'API de Flash peut établir une connexion Un attaquant peut récupérer des informations sur l'utilisateur au niveau de l'application. Cela est dû principalement au manque de connaissance ou à la négligence de l'utilisateur, mais le développeur de l'application est TCP sans passer par le réseau anonyme de l'utilisateur tandis qu'avec QuickTime, un paramètre dans la configuration permet d'établir une connexion directe pour voir une vidéo.
- **Document actif :** Un document actif permet une interaction avec l'utilisateur. Les documents actifs les plus populaires sont les fichiers PDF (Portable Document Format) développés par Adobe Systems ainsi que les documents Word et Excel développés par Microsoft. L'interaction avec les fichiers PDF est possible grâce à du code JavaScript intégré dans le fichier et à l'aide de macros pour les documents Word et Excel. Un attaquant peut envoyer des documents actifs contenant du code malicieux à

l'utilisateur. L'utilisateur non vigilant peut exécuter ce code en cliquant sur un bouton ou en visionnant une vidéo incluse dans le document par exemple. L'exécution de ce code peut connecter l'utilisateur à l'attaquant directement ou envoyer des informations personnelles.

- **Cookie :** Un cookie est une suite d'informations générée par un serveur Web pour reconnaître un client. Celui-ci est stocké sur l'ordinateur du client et laisse donc une trace de sa visite ce qui peut compromettre son anonymat.
- **JavaScript :** JavaScript est le langage de script le plus populaire. Il permet de dynamiser les pages web. La grande majorité des navigateurs intègrent un moteur JavaScript permettant l'exécution de code JavaScript. Un attaquant peut faire en sorte qu'un utilisateur exécute du code JavaScript malicieux à l'aide d'ingénierie sociale ou sur un site web vulnérable. L'attaquant pourra récupérer le cookie, l'historique, l'adresse IP réelle de l'utilisateur ainsi que d'autres informations sur la configuration de l'utilisateur (plug-ins utilisés, taille d'écran, etc.).
- **Applications BitTorrent :**Le navigateur Web n'est pas le seul vecteur d'attaque. Les applications P2P BitTorrent sont souvent utilisées dans les réseaux anonymes. BitTorrent est un protocole de transfert de données P2P. Lorsqu'un client demande un fichier, celui-ci est fragmenté sur différents pairs du réseau. Tous ces morceaux sont téléchargés et rassemblés sur la machine du client. Un tracker est un serveur qui permet d'amorcer un téléchargement. C'est lui qui relie les pairs possédant les parties du fichier au client. Lorsque le client souhaite télécharger un fichier, il doit s'annoncer au tracker. Cela s'effectue avec une requête HTTP de type GET. Sur certaines applications BitTorrent, la requête peut contenir l'adresse IP du client.
- **Vulnérabilités logicielles :** En utilisant un navigateur ou toute autre application non mise à jour, un attaquant peut exploiter les vulnérabilités de ces applications pour obtenir des informations personnelles sur l'utilisateur et ce même s'il passe par un réseau anonyme. Même si le navigateur est à jour, il est toujours possible à l'attaquant d'exploiter des failles non corrigées par une mise à jour.

1.7.3 Chiffrement des données

Le chiffrement est un procédé qui permet de transformer un message en clair, lisible par tous, en un message codé uniquement compréhensible par qui dispose du code.
Les techniques de chiffrement (de cryptologie) sont nombreuses, ont des fonctions différentes et sont utilisées par différents types de services[10]. Pour bien comprendre, on note :

a. Chiffrement hors-ligne (données au repos)

Chiffrement de tout ou partie de la mémoire de stockage d'un téléphone, d'une tablette, d'un ordinateur ou simplement d'un disque dur : il est utilisé pour rendre inintelligibles les informations présentes sur un appareil à toute personne qui ne dispose pas de la clé de déchiffrement. La technique utilisée est celle d'un chiffrement symétrique (par phrase de passe) pour des données qui ne sont plus dans un processus de communication, mais auxquelles des individus pourraient accéder en cas de perte ou vol d'ordinateurs, tablettes, etc[10].

b. Chiffrement en ligne (données en mouvement / en transit)

Des données « en transit » sont des informations qui se déplacent d'un endroit à un autre sur un réseau. Par exemple, la navigation sur le Web : quand vous vous rendez sur un site Web, les données de cette page Web voyagent des serveurs du site Web vers votre navigateur. Il est important de vérifier que les conversations entre vous et votre destinataire sont chiffrées. Il existe deux façons de **chiffrer** les données en transit : le **chiffrement de la couche de transport**et le **chiffrement de bout en bout**[11].

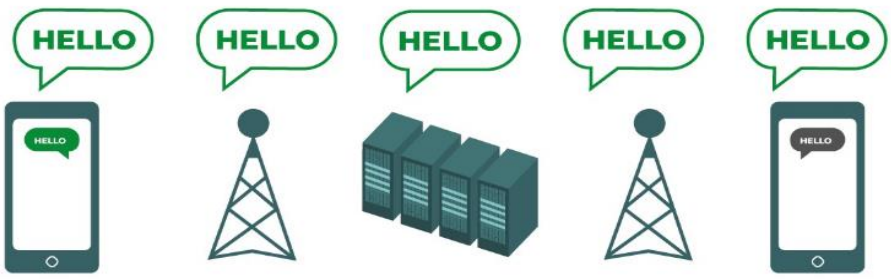

Figure 1.9: *Le chiffrement en ligne[36].*

- **Le chiffrement de la couche de transport**

Le chiffrement de la couche de transport, aussi appelé sécurité de la couche de transport (TLS), protège les messages alors qu'ils voyagent de votre appareil vers les serveurs de l'appli, et des serveurs de l'appli vers l'appareil de votre destinataire. Entre les deux, votre fournisseur de services de messagerie ou le site Web que vous parcourez, ou encore l'appli que vous utilisez peuvent voir des copies non chiffrées de vos messages. On trouve comme exemples de chiffrement de la couche de transport le HTTPS et les RVP (Réseau privé virtuel)[11].

Figure 1.10: *Le chiffrement de la couche de transport[36].*

- **Chiffrement de bout en bout**

Cette technique permet de chiffrer les données avant qu'elles soient envoyées sur le réseau et ne les déchiffre qu'à leur point d'arrivée. À aucun moment, il n'est possible de déchiffrer les données en transit. On ne peut y accéder qu'en ayant accès à l'appareil (ordinateur, téléphone, etc.) des personnes qui communiquent[10].

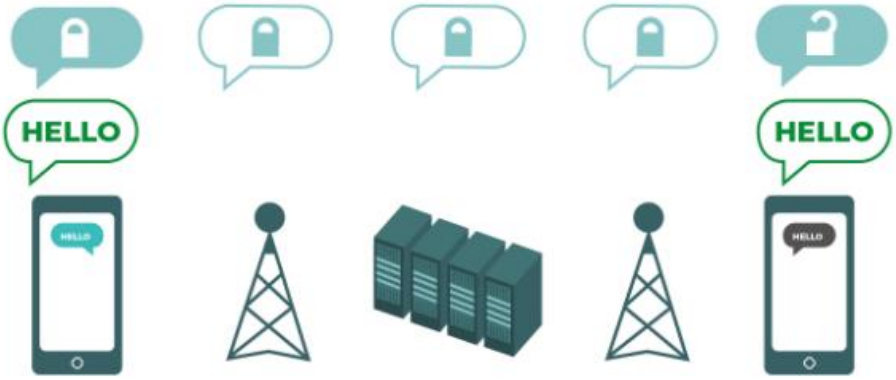

Figure 1.11: *Le chiffrement de bout en bout[36].*

1.8 Les différents outils d'anonymat

Les réseaux anonymes sont des systèmes de communications anonymes caractérisés par des applications distribuées entre clients dans lesquelles toutes les parties sont anonymes, l'anonymat s'obtient à l'aide de technique de surcouche logicielle ou de réseau de superposition. L'intérêt de cet outil est d'empêcher l'analyse et la surveillance du trafic. Ces réseaux tentent de garder une connexion anonyme lors d'une navigation en dirigeant le trafic vers un réseau mondial de relais et de nœuds et agissent donc sur des technologies et infrastructures existantes[12].

1.8.1 Freenet

Freenet est un logiciel libre qui permet d'accéder au réseau du même nom qui est un réseau autonome anonyme distribué le plus ancien avec pour objectif d'assurer la sécurité et l'anonymat à chacun, sa première version a été publiée en mars 2000. Freenet est décentralisé afin de la rendre moins vulnérable aux attaques et permet d'utiliser de façon anonyme les différents services proposés au sein de son propre réseau, il n'est donc pas possible de se connecter à des services comme Facebook ou Google avec Freenet[12].

Figure 1.12: *Logo Freenet.*

1.8.2 I2P (Invisible Internet Project)

I2P signifie "Le projet Internet invisible" dont l'objectif principal est l'anonymat, c'est un réseau isolé des autres réseaux et agit en tant que réseau superposé aux infrastructures internet existantes. Ce réseau anonyme peut donc être utilisé pour créer des services web anonymes : blog, forum, stockage de fichier décentralisé, courriel, SSH, proxys sortants. Dans I2P, les utilisateurs peuvent contrôler le niveau de sécurité, l'anonymat, la bande passante pour répondre à leurs besoins spécifiques. Ce qui garantit l'anonymat avec I2P est le fait que

l'expéditeur et le destinataire ne communiquent jamais directement, mais via plusieurs routeurs nommé tunnels[12].

Figure 1.13: *Interface I2P.*

1.8.3 TOR (The Onion Router)

Le réseau Tor est à l'origine un moyen de rendre anonyme sa connexion pour un accès sur les sites web standard ou ceux de son propre réseau : les services cachés. Fondamentalement, il agit comme un réseau superposé au réseau internet standard en utilisant des serveurs décentralisés appelés nœuds. Ce dernier a pour objectif de rendre confidentiel les applications basées TCP en anonymisant le flux, toutefois l'anonymisation total n'est pas garantie si l'application utilisés collecte des informations, c'est pourquoi il existe un navigateur dédié développé par le projet Tor[12].

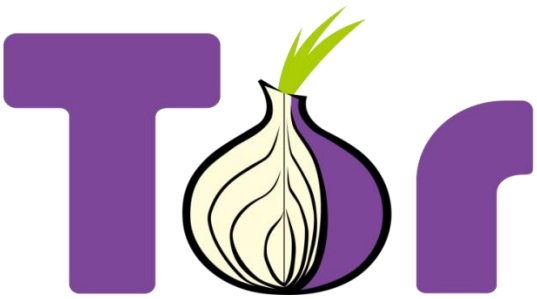

Figure 1.14: *Logo Tor.*

1.8.4 Navigateur privé

Un des premiers outils qui vient à l'esprit de beaucoup lorsqu'on parle d'anonymat sur internet est la navigation privée, une fonctionnalité désormais présente dans la quasi-totalité des navigateurs grand public. Lorsque vous passez en mode navigation privée plusieurs type de de données ne sont plus enregistres : les pages visitées, les données saisies dans les formulaires et la barre de recherche, les mots de passe, la liste des téléchargements, les cookies, les fichiers temporaires. Afin de maximiser la protection de l'anonymat.

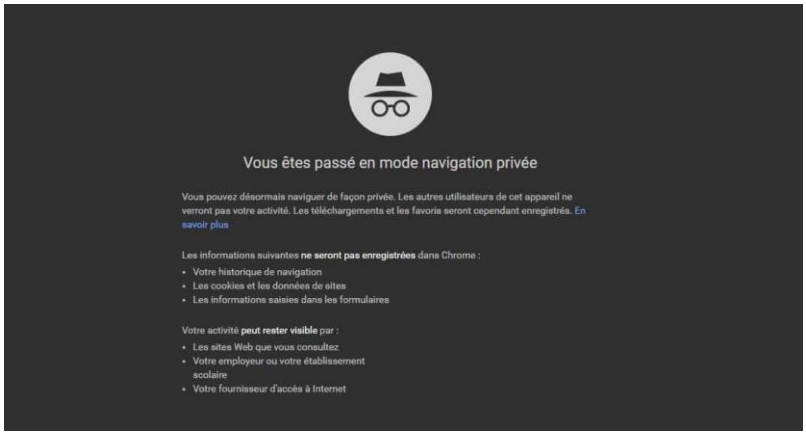

Figure 1.15: *Fenêtre d'une navigation privée.*

1.8.5 VPN

Un VPN est un réseau privé construit au sein d'une infrastructure de réseau public, telle que le réseau mondial Internet qui est un environnement de communication dans lequel l'accès est contrôlé pour permettre les connexions entre pairs uniquement au sein d'une communauté d'intérêts définie, et est construit à travers une certaine forme de partition d'un support de communication sous-jacent commun, où ce support de communication sous-jacent fournit des services au réseau sur une base non exclusive.

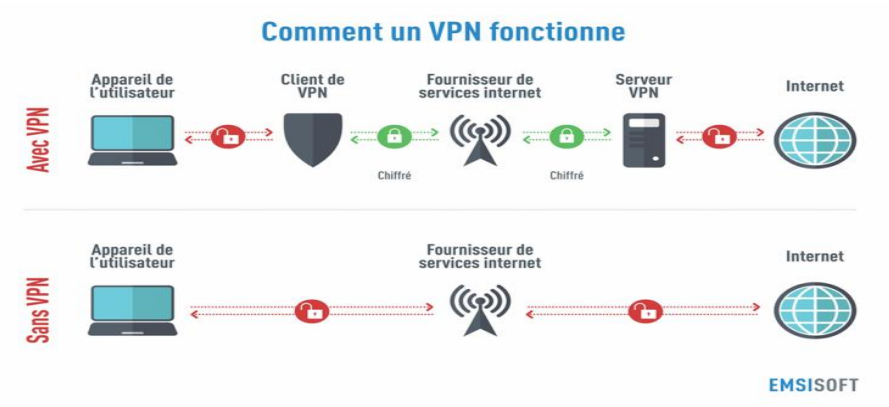

Figure 1.16: *Fonctionnement du VPN [37].*

1.9 Conclusion

Dans ce chapitre, nous avons vu des généralités sur les réseaux anonymes et le fonctionnement de l'internet ainsi que ses profondeurs.

Ce chapitre nous a permis de comprendre le concept de l'internet puis le concept de l'anonymat sur internet et plus précisément la surveillance sur internet, le chiffrement des données, et les différents outils d'anonymat.

La suite de ce mémoire sera consacrée aux réseaux anonymes les plus connus aujourd'hui Tor (The Onion Router) et I2P (Invisible Internet Project).

Chapitre2

TOR vs I2P

2.1 Introduction

Darknet, le mot en lui-même évoque des visions du ventre miteux d'Internet ; un quartier rouge virtuel, une ruelle et un ghetto numérique tout en un. Malgré cette image menaçante que les médias et de nombreux gouvernements aimeraient imprimer dans la conscience publique, les personnes soucieuses de la vie privée savent que dans le monde d'aujourd'hui, la rétention des données des FAI est mesurée en pétaoctets et les ressources de super calcul massives sont jetées sur l'analyse du trafic par les gouvernements et les entreprises privées. Dans l'industrie, les individus doivent prendre sur eux de garantir les libertés qui accompagnent l'accès à l'information et la communication anonymes. Deux des outils les plus populaires pour le faire sur Internet sont Tor et I2P. Les deux seront comparés et contrastés ci-dessous.

2.2 Tor

2.2.1 Définition

a. Le routage d'oignon

Le routage en oignon promettait non seulement de protéger l'intégrité et la confidentialité des données, mais également contre les écoutes et l'analyse du trafic sur le réseau et Internet, car il y a deux entités à protéger, les données et l'identité de ces données. Le routage en oignon protège contre les attaques d'analyse de trafic principalement parce que l'expéditeur ne parle pas directement au destinataire. Au lieu de cela, il initie une connexion avec un routeur spécifique à l'application appelé « proxy de routage en oignon » qui sera capable de gérer la demande TCP et Socks de ce client. Tor est une collection de routeurs d'oignon, qui ont différentes fonctions et rôles dans un réseau et pendant la communication réseau. Chaque routeur envoie des informations de manière sécurisée au prochain saut dans un réseau Tor, de sorte que si un seul routeur de l'ensemble de routeurs en oignon est compromis, cette violation n'affectera pas l'anonymat ni la communication de données envoyée vers et depuis l'expéditeur et le destinataire [13].

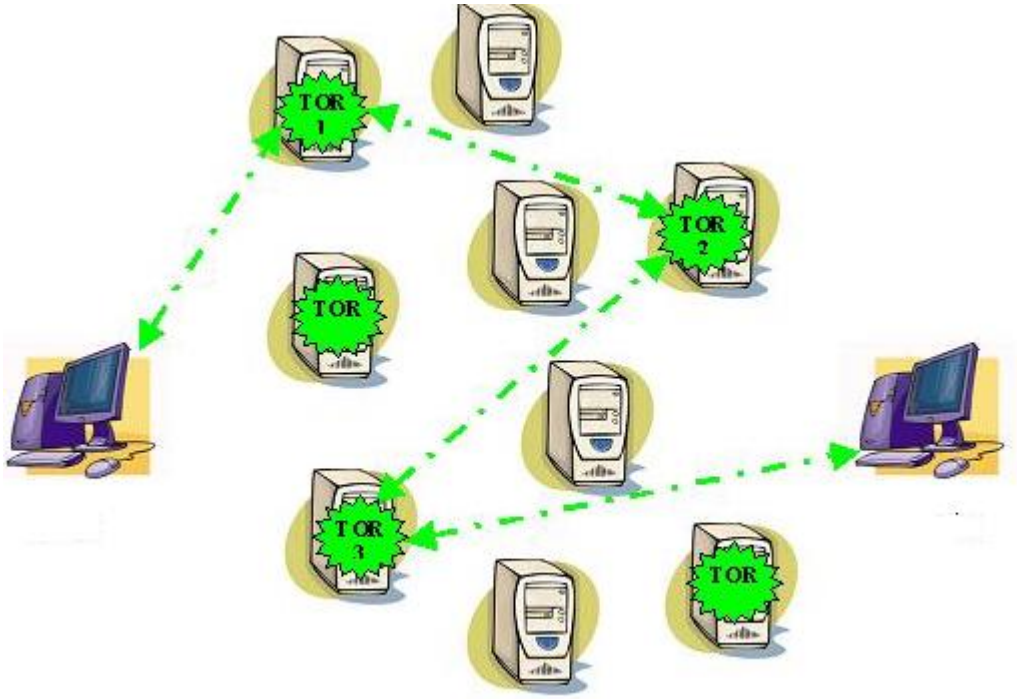

Figure 2.1: *Un instantané de Tor en action où plusieurs routes sont choisies[38].*

b. Lasecond générationdu routage d'oignon :

Tor vise à cacher la communication entre l'initiateur et l'hôte cible pour lequel l'initiateur a besoin de communiquer avec. Et pour cella Tor utilise une série de proxys et fait voyager la communication par un certain nombre de sauts avant de connecter l'initiateur à la cible. De ce qui précède, on peut se rendre compte que plus le nombre de nœuds, plus une connexion devient sécurisée car le suivi de la communication sera difficile de l'expéditeur au destinataire. De plus, plus le nombre de nœuds est important, plus la latence est ajoutée à la connexion, et pour les connexions à faible latence telles que Secure Shell, Telnet et d'autres applications interactives, il devient impossible de travailler avec une connexion à latence élevée. Par conséquent, il existe un compromis entre une connexion sécurisée qui permet l'anonymat et qui est capable d'utiliser un certain nombre de sauts tout en gardant une latence de connexion supportable. Alors Tor a été conçu pour acheminer les connexions via trois nœuds Tor intermédiaires et un dernier nœud de sortie avant de quitter le réseau Tor et de transmettre la communication au récepteur. Au total, quatre nœuds sont impliqués dans toute communication Tor [13].

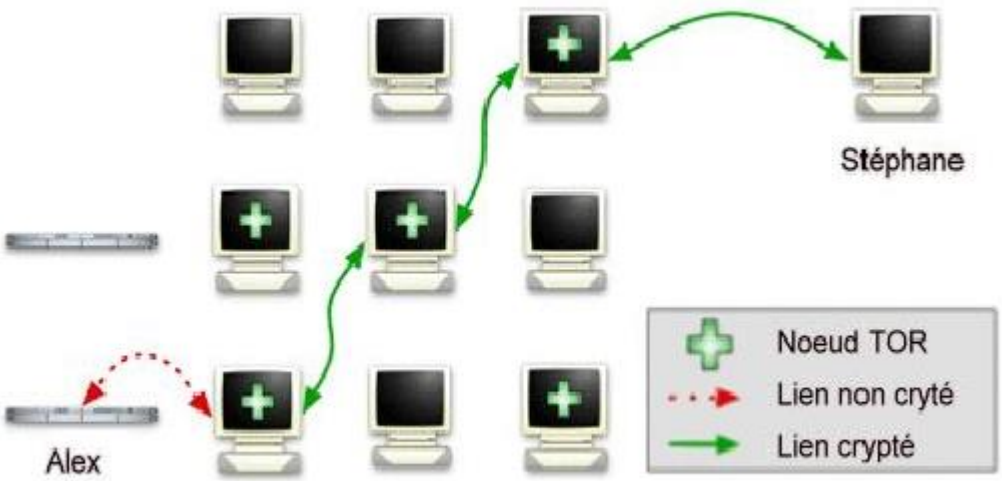

Figure 2.2: *Un utilisateur se connectant via Internet à un réseau Tor[39].*

2.2.2 Architecture

Le réseau Tor se compose d'environ 12 000 routeurs répartis en deux familles, les relais et les ponts. Le réseau Tor est organisé en plusieurs niveaux où les routeurs ont plusieurs rôles. Celles-ci dépendent de la confiance que leur accorde le réseau, qui dépend notamment de la durée d'activité [14]. Les différents rôles par niveau sont :
Quatre niveaux d'autorité sont identifiés :

1. **Neuf autorités d'annuaire et autorités de pont** : Ils répertorient tous les routeurs - relais ou ponts - du réseau, analysent la bande passante, leur attribuent un poids particulier - en fonction de l'âge, de la bande passante et de la stabilité.
2. **Caches d'annuaire** qui téléchargent les données des autorités pour les mettre en cache et les distribuer aux clients qui en font la demande.
3. **Miroirs de répertoire de secours** qui sont des serveurs de cache dont les adresses IP sont également écrites dans le code. Ils permettent aux clients de télécharger le fichier de consensus lors de l'initialisation de la connexion.
4. **HSDir** qui sont des serveurs équivalents aux serveurs DNS. Ils détiennent les informations pour contacter un service caché telles que les adresses des points d'introduction.

Pour les routeurs Tor :

- **Le nœud de sortie** : est le troisième routeur d'un circuit destiné à transmettre le flux réseau vers Internet.
- **Le nœud non sortie :** est un routeur qui ne traite que les flux entrants ou internes dans Tor.
- **Le nœud d'entrée** : est le premier routeur auquel s'adresse un client pour passer par Tor.
- **Le nœud de garde :** est un routeur d'entrée vers le réseau Tor. Il a également le rôle de routeur de non-sortie et peut donc traiter les flux internes du réseau.
- **Le Nœud de pont** : est un routeur dont les informations ne sont que partiellement publiées et dont le but est de permettre aux clients de contourner la censure.

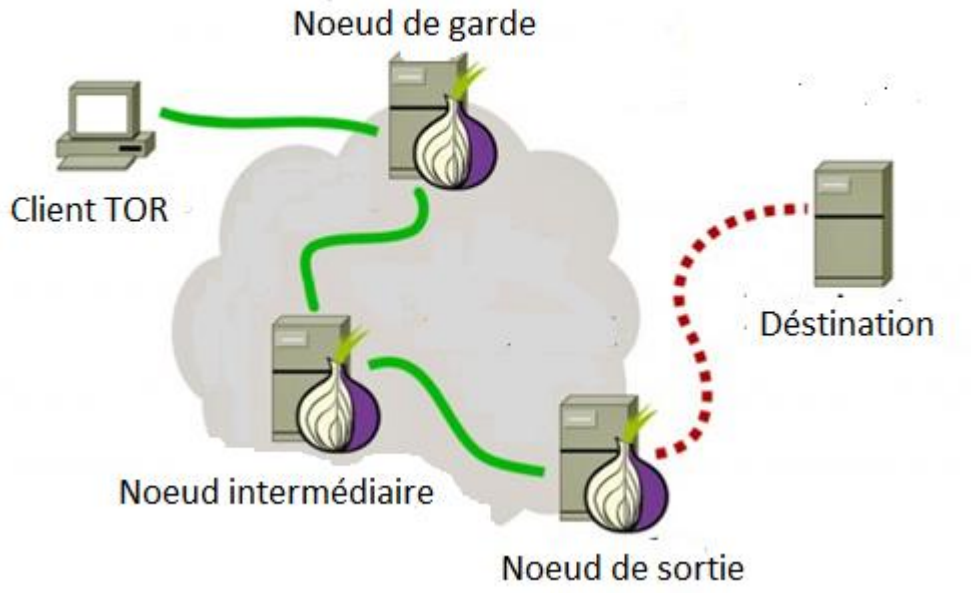

Figure 2.3: *L'acheminement d'une connexion du réseau Tor[40].*

Pour fournir des services au sein du réseau :

- **Le service caché** : est un serveur qui n'acceptera que les connexions entrantes via un protocole particulier. Les initiateurs de la connexion ne pourront pas connaître l'adresse IP du service afin de préserver son anonymat.
- **Le point d'introduction** : est un routeur (type relais) connecté à un service masqué par un circuit particulier et qui permet à un client de soumettre une demande de rendez-vous pour établir une connexion.

- **Le point de rendez-vous :** est un routeur (type relais) qui relie deux circuits construits indépendamment, l'un par un client et l'autre par un service caché pour permettre des échanges de bout en bout.

2.2.3 Fonctionnement générale

Pour bénéficier du réseau Tor et pour devenir anonyme, le client - Onion Proxy (OP) - doit suivre un processus. Prenons une personne qui désire se rendre anonymement sur une page Web, cette dernière peut alors utiliser le navigateur Tor. L'application choisit un chemin composé de nœuds (des routeurs oignons ou "OR" en anglais) par lesquels il voyagera à travers le réseau. Le choix se fait via une liste reçue par les "répertoires de serveurs". Chaque nœud ne connait que son prédécesseur et le nœud suivant. Le contenu à destination des "OR" est crypté, chaque donnée à destination des "hops" (un hop est une portion entre une source et une destination, comme un routeur, une passerelle, un pont) est encapsulée dans une couche propre, comme un oignon, d'où le nom de "routage en oignon". Le client négocie ses clés de chiffrement avec chacun des routeurs séparément. La communication dans le réseau se fait via des cellules de taille fixe de deux types [15].

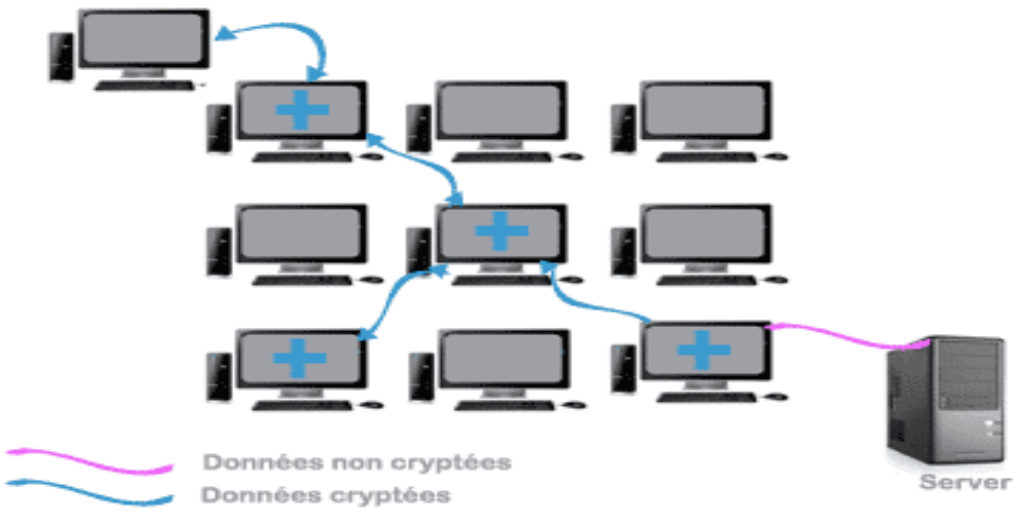

Figure 2.4: *Schéma de fonctionnement de Tor.*

2.2.3.1 Protocole de routage :

Le routage en oignon est une infrastructure à usage général pour les communications privées sur un réseau public. Il fournit des connexions anonymes qui sont fortement résistantes à la fois à l'écoute clandestine et analyse du trafic entre les relais du réseau, bien que les nœuds

de sortie puissent surveiller le trafic puisqu'ils transmettent les paquets du réseau à leurs destinations. La connexion de la source A à la destination B fait un détour le long d'une chaîne cryptée, qui s'appelle un oignon.La communication réseau au sein de l'oignon est également cryptée et chaque nœud, appelé relais, ne dispose que des informations sur les nœuds adjacents de sortie que l'image complète de la chaîne de communication est cachée.Les oignons sont acheminés lorsqu'un paquet de données est protégé par trois couches de cryptage. Ce sont ces couches qui donnent son nom à OnionRouting.Chaque nœud sait seulement comment déchiffrer sa couche particulière, ce qui indique où le paquet est envoyé par la suite. Les canaux cryptés, qui sont créés entre chaque relais de routage, sont donc très efficaces. Lorsque le nombre de nœuds augmente, la complexité et le nombre de canaux cryptés augmentent également[16].

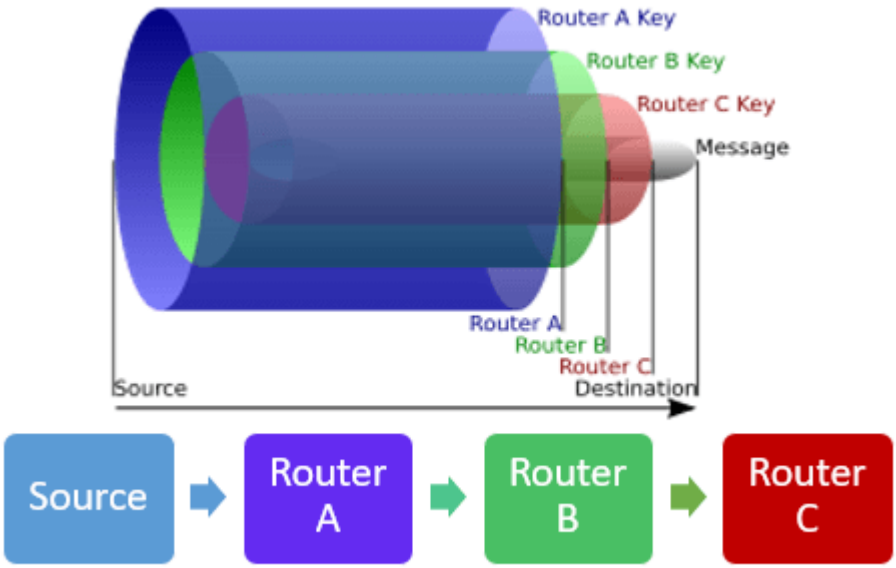

Figure 2.5: *Description générale du protocole Tor.*

2.2.3.2 Serveurs d'annuaires

Pour voyager dans le réseau, l'interlocuteur "A" doit connaître les différents ORs Afin de déterminer à l'avance le chemin vers le nœud de sortie. Pour cela, il a besoin d'un répertoire de référence "Directory Server" afin de recevoir la liste des ORs. Ce répertoire fournit une liste des signatures de tous les relais connus, dans cette liste se trouvent les certificats émis par les routeurs spécifiant leur clé, son emplacement et sa politique de sortie.

Il y a plusieurs de ces annuaires qui ont les mêmes informations et ont donc la même liste d'ORs. Pour que le "Onion router" soit dans le serveur d'annuaire, il doit être approuvé Par l'administrateur. Les Ors envoient périodiquement leur statut au serveur Annuaires et pour s'identifier, ils utilisent la clé fournie par le "serveur d'annuaire" [15].

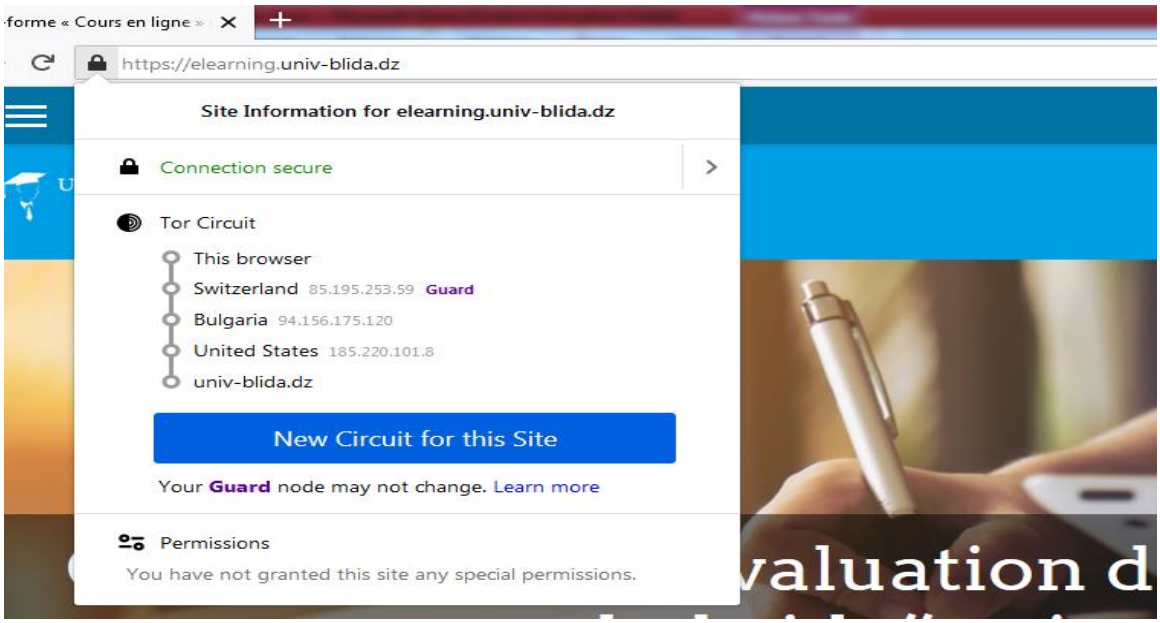

Figure 2.6: *Chemin jusqu'au site de l'Université Blida.*

2.2.3.3 Les cellules de taille fixe

Les routeurs oignon communiquent entre eux, et les utilisateurs Onion Proxy (OP) communiquent via des connexions TLS. Pour cela, ils utilisent des cellules de données de 512 octets[15]. Il en existe deux types :

- **Les cellules de contrôle :**

Les cellules de contrôle comme montré dans la figure 2.7 sont toujours interprétées par le nœud qui les reçoit.

- ✓ **CircID :** défini de quel circuit se rapporte cette cellule.
- ✓ **CMD :** Détermine la commande à utiliser pour cette cellule, nous verrons les différentes commandes un plus bas dans ce point.

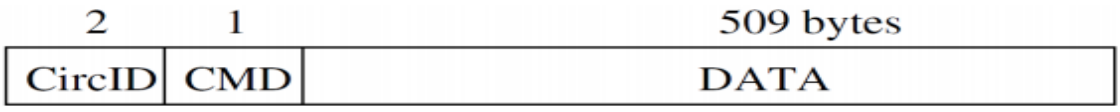

Figure 2.7: *Une cellule de contrôle.*

- **Les cellules de relais :**

Lorsqu'une connexion est établie dans le réseau, L'OP peut envoyer des Cellules relais comme montre la figure 2.8 . Afin de vérifier que la cellule est valide, L'OR va déchiffrer cette dernière et vérifier la correspondance avec la partie "digest" de 6 octets.S'il est valide, il accepte cellule et traite les informations qu'il contient. Sinon, l'OR Transfère la cellule au nœud suivant. Si la fin de la chaine reçoit une cellule de relais non reconnue le circuit est détruit[15].

- ✓ **CircID** : Comme la cellule de contrôle, elle détermine l'Id du circuit.
- ✓ **Relay** : Défini que c'est une cellule de relai.
- ✓ **Stream ID** : Donne la référence du flux à laquelle cette cellule appartient.
- ✓ **Digest** : Sert à contrôler l'intégrité.
- ✓ **Len :** Donne la longueur de la donnée contenue dans le champ DATA.
- ✓ **CMD :** Détermine la commande à utiliser pour cette cellule, nous verrons les différentes commandes un plus bas dans ce point.
- ✓ **DATA :** Ce sont les données envoyées dans la cellule.

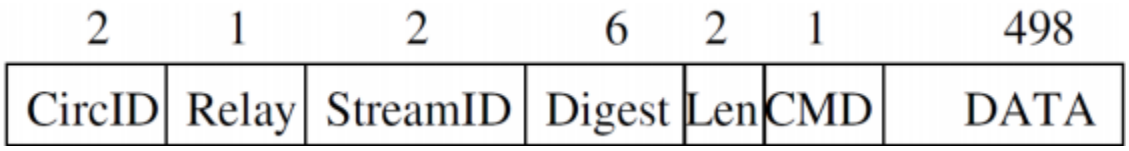

Figure 2.8: *Une cellule de relais.*

2.2.3.4 Initialisation du chemin

Tor a construit à l'origine un circuit pour chaque flux TCP.Pour que l'utilisateur puisse accéder à la page Web, il doit construire son chemin à travers le réseau Tor via des relais qu'il a reçu d'un serveur d'annuaires précédemment. Dès que l'application fait son choix,Celui-ci contactera progressivement chacun des "hops" pour créer un canal sécurisé[15].

Les différentes clés utilisées :

Afin d'assurer l'authentification sur le réseau :

- **La coordination :**En vérifiant si le routeur avec lequel le système communique est le routeur qu'il prétend.

- **L'encryptage des données :** Le réseau utilise un ensemble de clés avec leur caractéristique.
    1) **La clé d'identité de longue durée :** assure la coordination.
    2) **Une clé oignon de courte durée :** Au moment de la création du circuit cette clés nous permet de vérifier si le routeur choisi par le client est bien le routeur prévu. La clé oignon du routeur crypte La cellule de commande "create".
    3) **Des clés de lien de courtes durées :** assurent une couche supplémentaire de cryptage en utilisant L'AES "Advanced Encryption Standard" avec une clé de 128 bits.

2.2.3.5 Création du circuit

Dans la conception Tor actuelle, le circuit est établi par l'échange de clés DiffieHellman (DH) entre l'OP et chaque nœud du circuit.Pour établir le circuit [15]:

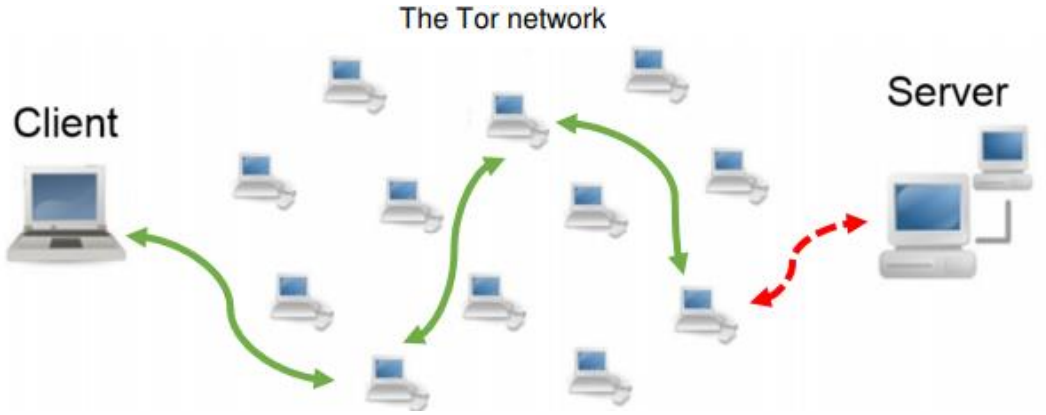

Figure 2.9: *Un circuit Tor construit par un client via le réseau Tor vers un serveur sur l'Internet public.*

a. **La première étape la sélection du nœud de relais** :Le circuit Tor a besoin de troisnœuds relais : un nœud d'entrée, un nœud intermédiaire et un nœud de sortie. Tout d'abord, OP sélectionne tous les routeurs qui ont une politique de transfert acceptable à partir du service d'annuaire, puis choisir un nœud Tor comme nœud de sortie au hasard. Deuxièmement, OP choisit un nœud Tor comme nœud intermédiaire au hasard à partir du service d'annuaire. Enfin, OP choisit un nœud Tor comme nœud d'entrée au hasard dans la liste des nœuds de garde. Chaque utilisateur Tor maintient une liste ordonnée de nœuds de garde comprenant un ensemble de trois nœuds Tor. Les nœuds de garde sont choisis parmi les nœuds stables, c'est-à-dire ceux avec un temps de disponibilité élevé, qui ont une bande passante supérieure à la bande passante médiane.

b. **La deuxième étape est la construction du circuit :** entre OP et ces nœuds relaissélectionnés. L'OP de l'utilisateur Tor construit le circuit un saut à la fois et négocie entre-temps une clé symétrique avec chaque nœud sélectionné.

c. **Echange de clé Diffie-Hellman :** L'échange de clés "Diffie-Hellman" a pour but de créer une clé symétrique afin de communiquer de manière chiffrée entre deux acteurs. L'utilisation de DH fournit une confidentialité de transmission parfaite, les clés sont formées à partir de messages échangés plutôt que d'être envoyées sous forme cryptée. Ainsi, un adversaire ne peut pas obtenir la clé privée de session en surveillant les trafics de transmission. Une fois la session de communication terminée, la clé privée de session sera supprimée. Ainsi, le nœud relais ne peut pas utiliser la clé privée de session pour la communication précédente pour déchiffrer les nouveaux trafics de transmission de circuit.

d. **TLS - Transport Layer Security :** La communication entre deux nœuds du réseau Tor s'effectue via le protocole "Transport Layer Security" (TLS), qui est l'évolution de SSL. En raison du protocole HTTPS, TLS est largement utilisé pour la navigation Web. Car TLS permet :

- **L'authentification :** est la première étape, elle vérifie que le serveur avec qui nous parlons est bien celui qu'il prétend être. Pour ce faire, le client recevra la clé publique du serveur, ses informations et sa signature numérique. Celui-ci doit être déchiffré directement par le navigateur. En cas de succès, il peut envoyer une requête "Online CertificateStatus Protocol" (OCSP) à l'autorité pour vérifier si le certificat du serveur est reconnu et est toujours valide. Pour cette partie, Tor utilise l'algorithme de chiffrement RSA.
- **La confidentialité des données échangées :** est réalisé grâce à un chiffrement de clés symétriques.
- **L'intégrité des données** : Permet d'utiliser une fonction de hachage pour vérifier si ceux-ci n'ont pas été modifiés lors de la transmission.

2.2.4 Nœuds de sortie

Lorsque la connexion sort du réseau Tor, est une vraie problématique. Pour cela une politique de sortie a été élaborée, permettant aux administrateurs de Tor de définir des règles pour ces derniers[15].

- **Ouvrir les nœuds de sortie :** Ce sont les points de sortie du réseau. C'est-à-dire que ceux-ci permettront d'atteindre la destination. Il est important d'en avoir un nombre suffisant, sinon il sera plus facile pour un attaquant de surveiller le réseau de sortie.

- **Nœuds intermédiaires :** Ils ne sont utilisés que pour relayer le trafic dans le réseau. Cependant, il est important d'en avoir un grand nombre pour permettre un réseau robuste.
- **Nœuds de sortie privés :** permet la connexion à un hôte ou à un réseau privé.

2.2.5 Services cachés

Le réseau Tor permet aux utilisateurs de fournir des services TCP cachés [15]. Ces services cachés ont pour but :

- **Le contrôle d'accès** : le service a besoin d'un moyen de filtrer le contenu entrant afin que les attaquants ne puissent pas inonder le service de requêtes
- **La robustesse** Même si le routeur oignon tombe en panne, le service doit rester anonyme et le système doit pouvoir se répercuter sur un autre OR.
- **La résistance au marquage :** un service malveillant, ne doit pas induire en erreur que le routeur "rendez-vous" est à l'origine du service illégal ou d'une mauvaise réputation.
- **Transparence :** Même si l'utilisateur doit utiliser un programme spécial pour bénéficier du service caché, il ne doit pas modifier son application.

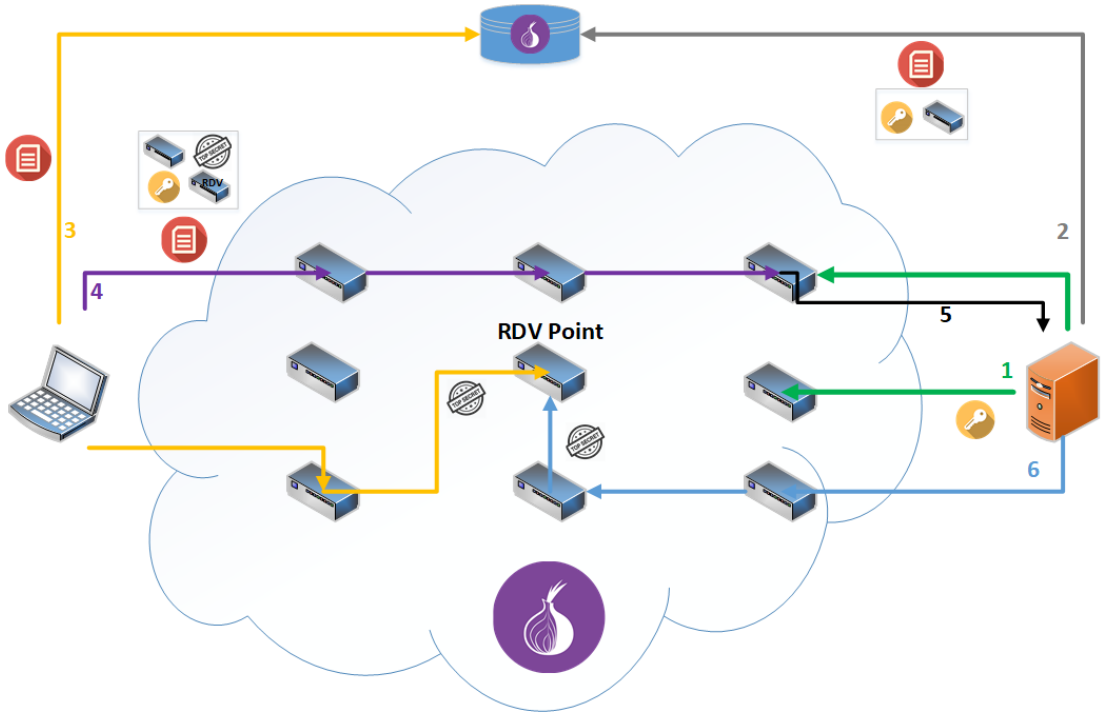

Figure 2.10: *Lancement du service caché [41].*

2.3 I2P

2.3.1 Définition

A première vue, I2P semble offrir bon nombre des mêmes avantages que Tor. Les deux permettent un accès anonyme au contenu en ligne, les deux utilisent une structure de routage de type pair à pair et les deux fonctionnent à l'aide d'un cryptage en couches.

Cependant, I2P a été conçu dès le départ pour offrir un ensemble différent d'avantages. Le principal cas d'utilisation de Tor est de permettre l'accès anonyme à l'Internet public avec des services cachés comme avantage accessoire. I2P, en revanche, a été conçu dès le premier jour pour être un véritable darknet. Sa fonction principale est d'être un réseau au sein d'Internet, le trafic restant contenu dans ses frontières. Très peu de relais sortants existent dans le réseau I2P, et les rares qui existent sont rarement utilisables [17].

2.3.2 Fonctionnement

Comme mentionné ci-dessus, I2P achemine le trafic différemment de Tor. En son cœur, I2P effectue un routage basé sur les paquets par opposition au routage basé sur les circuits de Tor. Cela a l'avantage de permettre à I2P de contourner dynamiquement la congestion et les interruptions de service d'une manière similaire au routage IP d'Internet.

Cela fournit un niveau plus élevé de fiabilité et de redondance au réseau lui-même. De plus, I2P ne s'appuie pas sur un service d'annuaire de confiance pour obtenir des informations sur l'itinéraire. Au lieu de cela, les routes du réseau sont formées et constamment mises à jour de manière dynamique, chaque routeur évaluant constamment les autres routeurs et partageant ce qu'il trouve. Enfin, I2P établit deux tunnels simplex indépendants pour que le trafic traverse le réseau vers et depuis chaque hôte [18].

2.3.3 Mécanisme de routage

Quand Alice veut communiquer avec Bob, elle envoie des messages sur son tunnel sortant. Ces messages se dirigent vers le routeur de passerelle du tunnel entrant de Bob. Alice apprend l'adresse du routeur de passerelle de Bob en interrogeant une base de données de réseau distribué (discutée plus en détail dans la section « Répertoire distribué »). Pour répondre à Alice, Bob suit le même processus en envoyant des messages de réponse sur son tunnel sortant vers la passerelle du tunnel entrant d'Alice.

L'anonymat d'Alice et de Bob est préservé puisqu'ils ne connaissent que les adresses des passerelles, mais pas les adresses réelles de l'autre. Notons que les passerelles des tunnels entrants sont publiées, tandis que les passerelles des tunnels sortants ne sont connues que par la partie qui les utilise. L'exemple de la **figure 2.12** illustre un cas dans lequel I2P est utilisé comme un réseau autonome, avec des pairs participants communiquant uniquement entre eux. Cependant, si Bob fournit également un service proxy de sortie, Alice peut relayer son trafic via Bob pour se connecter à l'Internet public. Le trafic Internet renvoyé est ensuite retransmis en toute sécurité à Alice par Bob via ses tunnels sortants, tandis que l'identité d'Alice reste inconnue à la fois pour Bob et pour la destination visitée sur Internet.

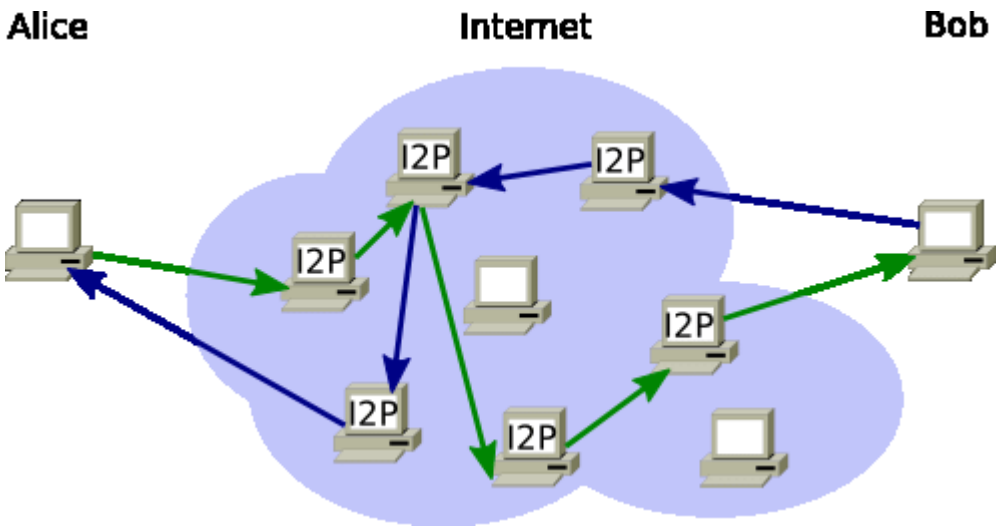

Figure 2.11 : *Communication de base entre deux pairs I2P à l'aide de tunnels unidirectionnels.*

a. Répertoire distribué

La base de données du réseau I2P, appelée netDb, joue un rôle vital dans le réseau I2P en permettant aux pairs de rechercher des informations sur d'autres pairs et des services cachés. La base de données du réseau est implémentée sous la forme d'une table de hachage distribuée en utilisant une variante de l'algorithme de Kademlia. Un pair nouvellement rejoint apprend d'abord une petite partie de la netDb via un processus d'amorçage, en récupérant des informations sur d'autres pairs dans le réseau à partir d'un ensemble de serveurs de réamorçage codés en dur. Contrairement aux autorités d'annuaire Tor, ces serveurs de réamorçage n'ont pas une vue complète de l'ensemble du réseau I2P.

Ils sont équivalents à n'importe quel autre pair du réseau, avec la possibilité supplémentaire d'annoncer une petite partie des routeurs connus aux nouveaux pairs. Les requêtes pour la base de données du réseau sont traitées par un groupe de routeurs spéciaux de remplissage, qui jouent un rôle essentiel dans le maintien de netDb. L'une de leurs principales responsabilités est de stocker des informations sur les pairs et les services cachés dans le réseau de manière décentralisée à l'aide de clés d'indexation (c'est-à-dire des clés de routage). Ces clés sont calculées par une fonction de hachage SHA256 d'une clé de recherche binaire de 32 octets qui est concaténée avec une chaîne de date UTC. En conséquence, ces valeurs de hachage changent chaque jour à UTC 00 :00.

Dans la conception I2P actuelle, il existe deux manières de devenir un routeur floodfill :

- La première option consiste à activer manuellement le mode floodfill à partir de la console du routeur I2P.
- L'autre possibilité est qu'un routeur à large bande passante devienne automatiquement un routeur de remplissage après avoir dépassé le débit de la file d'attente des messages sortants, le délai, etc.

Le netDb contient deux types de métadonnées de réseau : les ensembles de baux (LeaseSets) et les informations de routeur (RouterInfos).

Par exemple, le LeaseSet indique à Alice les coordonnées de la passerelle du tunnel entrant de Bob. Une information de routeur fournit des informations de contact sur un pair I2P particulier, y compris sa clé, sa capacité, son adresse et son port. Pour publier ses leaseSets, Bob envoie un message « Database Store Message » (DSM) à plusieurs routeurs floodfill, qui encapsule ses LeaseSets. Pour interroger les informations de LeaseSets de Bob, Alice envoie un message de recherche de base de données « DatabaseLookup Message (DLM) » à ces routeurs de remplissage.

b. Les tunnels

La mise en œuvre du système de communication anonyme I2P doit s'appuyer sur le tunnel. S'ils sont divisés par la direction de transmission des données, les tunnels I2P peuvent être divisés en entrants et sortants. Le sortant est utilisé pour envoyer des messages et chiffrer les messages de sortie couche par couche. L'entrant est utilisé pour recevoir des messages et décrypter les messages d'entrée couche par couche.

Selon la jonction du tunnel, le tunnel I2P peut être divisé en tunnels d'exploration et tunnels clients. Le tunnel d'exploration est utilisé pour demander des données et gérer les informations du tunnel à partir de la base de données réseau (NetDb). Le tunnel client est utilisé pour la transmission de messages réseau de toutes les couches d'application, telles que la requête d'adresse d'interface de tunnel (LeaseSet), la demande anonyme, le tunnel sortant et le fournisseur de services de tunnel entrant, etc.

En raison des caractéristiques de transmission unidirectionnelle du tunnel, une communication complète entre deux utilisateurs nécessite au moins quatre tunnels, deux sortants et deux entrants, comme la figure ci-dessous.

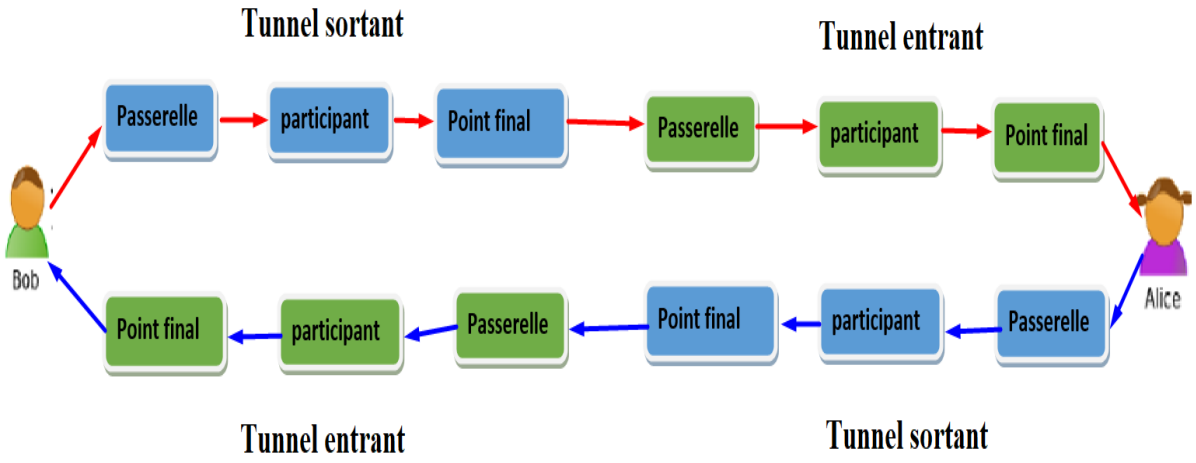

Figure 2.12: *Communication orientée simple tunnel dans I2P.*

Le premier nœud du tunnel, appelé passerelle d'origine du tunnel, est la première des adresses de port de tunnel publiées dans la base de données du réseau. Alice obtient l'adresse de passerelle du tunnel entrant de Bob en interrogeant NetDb, puis envoie un message à Bob via son propre tunnel sortant. Bob reçoit le message via son propre tunnel entrant et envoie le message reçu au tunnel entrant d'Alice via son propre tunnel sortant pour terminer la transmission du message. Les deux parties peuvent lier leur propre adresse de tunnel entrant au message, il n'est donc pas nécessaire d'interroger la base de données du réseau pour l'adresse de tunnel entrant de l'autre partie.

2.3.4 Cryptographie

Afin d'établir une communication anonyme et sécurisée, I2P utilise différentes couches de cryptage. La communication entre les routeurs est protégée par la sécurité de la couche de transport. La couche transport crypte chaque paquet avec AES256/CBC. Les clés sont échangées par un échange Diffie-Hellman 2048 bits [19].

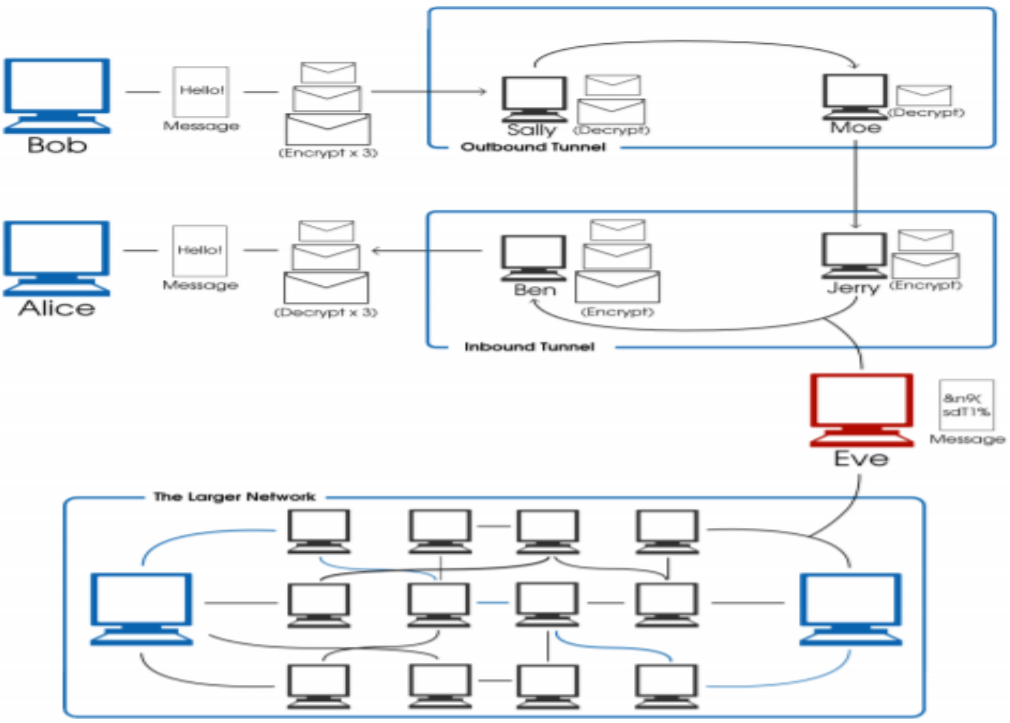

Figure 2.13: *Le transfert des messages via le réseau.*

Les messages du tunnel sont chiffrés avec le chiffrement AES256/CBC avec un IV explicite et vérifiés au point de terminaison du tunnel avec un hachage SHA256 supplémentaire. D'autres messages sont enveloppés dans des « messages à l'ail », qui sont typiques du cryptage I2P. Ce nom est dérivé du « cryptage à l'oignon » utilisé par Tor. Il permet le routage crypté des messages via des tunnels.

Dans le cryptage à l'ail et à l'oignon, un message est enveloppé dans plusieurs couches de cryptage (comme les différentes couches d'un oignon couvrant le centre). Lorsque le message est envoyé via un tunnel, une couche est « décollée » à chaque saut, révélant la prochaine couche de cryptage et des instructions pour l'envoyer au prochain routeur du tunnel.

Le cryptage à l'ail offre en outre la possibilité d'ajouter plusieurs messages (girofle) à l'intérieur des couches de cryptage. I2P l'utilise pour envoyer deux messages supplémentaires à côté du message d'origine : de l'expéditeur du message En envoyant ces messages supplémentaires, moins de requêtes doivent être faites au netDb, ce qui améliore la latence et réduit le risque d'attaques d'analyse de trafic.

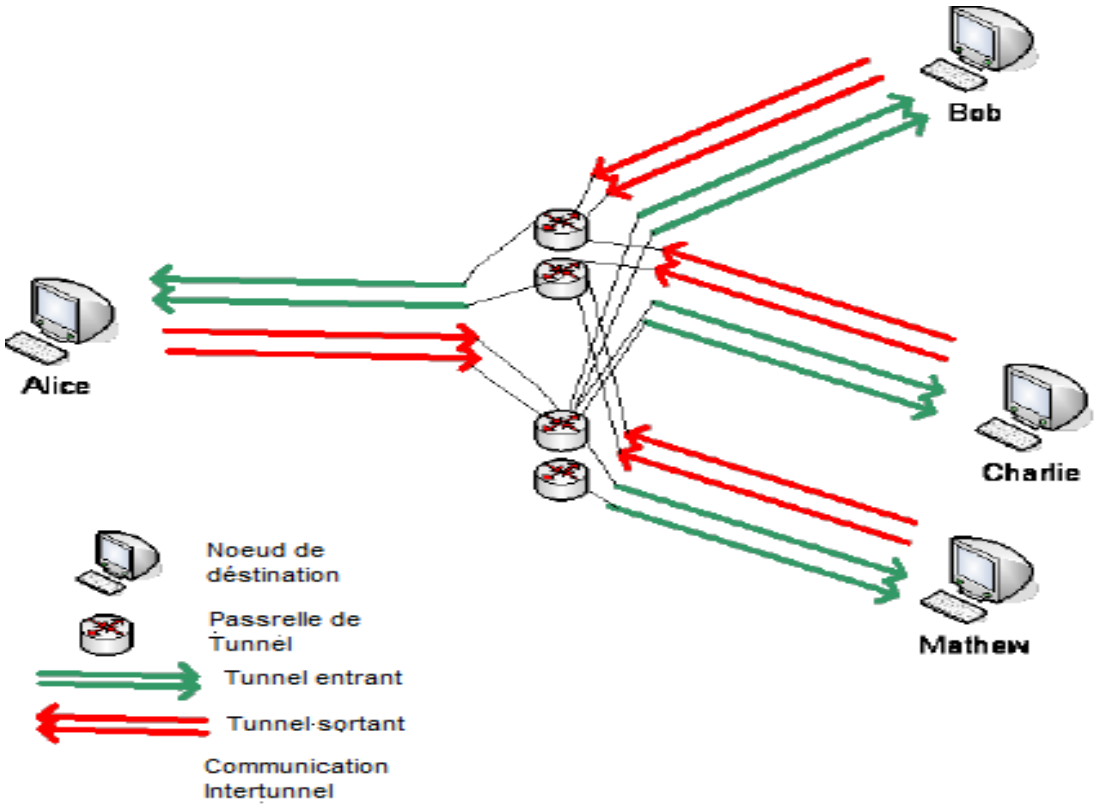

Figure 2.14: *Routage d'un message d'ail [42].*

2.4 Comparatif théorique

I2P est développé sur la base de nombreux concepts de développement et technologies de réseau de Tor. La principale différence entre le réseau Tor et I2P réside dans : I2P tente de transférer des services Internet existants vers des réseaux I2P et de fournir des services dans le cadre de la mise en œuvre, tandis que Tor permet un accès anonyme pour mettre en œuvre et exploiter des services Internet externes séparément.

Les différences techniques principales entre le réseau Tor et I2P sont les suivantes[20] :

- Le flux de messages remplace les cellules.
- Les tunnels unidirectionnels remplacent les circuits bidirectionnels.
- La commutation de paquets est transformée en commutation de circuits.
- La sélection de pairs basée sur les performances remplace la sélection de pairs basée sur la bande passante.
- L'architecture distribuée remplace le cadre centralisé.

2.4.1 Termes utilisés dans Tor et I2P

En termes de technologie, I2P est similaire à Tor à bien des égards, mais ses développeurs utilisent souvent des termes légèrement différents pour presque les mêmes fonctions.

Le tableau 2.1 fournit la correspondance entre les différents termes utilisés entre Tor et I2P.

Tor	I2P
Cellule Client	Message Routeur, Client
Circuit	Tunnel
Annuaire Serveur d'annuaire Guardien d'entrée Nœud d'entrée	NetDB, base de données réseau Routeur floodfill Pair rapide Inproxy, proxy d'entrée
Nœud de sortie Service caché	Outproxy, proxy d'exportation Eepsite ou destination.
Descripteur de service caché Point d'introduction Routage d'oignon Nœud, Serveur	Lease Set Passerelle entrante Routage de l'ail Routeur
Agent d'oignon	Client de tunnel I2P
Service à l'oignon	Service caché, Eepsite ou destination

Tor	I2P
Point de rendez-vous	Passerelle entrante + point de terminaison sortant
Descripteur de routeur	Information routeur

Tableau 2-1: *Comparaison de Tor et I2P : Terminologie utilisée.*

2.4.2 Développement des projets Tor et I2P

Les tableaux 2.2, 2.3 et 2.4 sont construits sur la base des caractéristiques de Tor et I2P. Les réseaux anonymes Tor et I2P sont comparés à partir des trois aspects de la technologie de reconnaissance, de performance et de développement.

Caractéristique	Tor	I2P Small
Groupe d'utilisateurs	Très grande	Petite base
Attention académique	Plus, et visible	Rarement vu
Attention de la communauté des hackers	Plus, et visible	Rarement vu
Évolutivité	Meilleur	Moins
Développeurs	Plus	Moins
Langage	C	Java

Tableau 2-2: *Comparaison de Tor et I2P : sensibilisation.*

Caractéristique	Tor	I2P
Vulnérabilité des attaques DoS	Plus fragile	Pas très fragile
Nombre de nœuds de sortie	Un grand nombre de nœuds d'exportation	Moins de nœuds de sortie
Documentation	Bonne documentation	Mauvaise documentation

Caractéristique	Tor	I2P
Site web	Meilleur	Très bien
Documentation en différentes langues	Disponible	Non disponible
Utilisation de la mémoire	Plus efficace	Invalide
Situation d'écoute clandestine de la bande passante	Très lent	Très haut
Contrôle centralisé/distribué	Centralisé	Distribué
Vulnérable à Sybil	Oui	Non
Débit	Plus haut	Inférieur
Temporisation	Inférieure	Haute

Tableau 2-3: *Comparaison Tor et I2P : performances.*

Caractéristique	Tor	I2p
Nom de domaine	. onion	. i2p
Critères de sélection des nœuds	Confiance, Déclaration, Capacité	Analyser en permanence Classement des performances
Serveur d'annuaire/flood Fill remplissage	Confiance et codage en dur	Modifiable et peu fiable
Commutation de paquet/circuit	Commutation de circuits	Commutation de paquets
Unidirectionnel/bidirectionnel	Circuit bidirectionnel	Tunnel à sens unique

Protection contre la détection de l'activité du client	Moins de protection	Plus de protection
Durée du tunnel/circuit	Longtemps	Court instant
Transmission TCP/UDP	TCP	Les deux sont bons
SOCKS/I2P API	SOCKS	I2P API

Tableau 2-4: *Comparaison de Tor et I2P : technologie de développement.*

- **SOCKS/I2P API** : Tor utilise l'interface Socket Secure (SOCKS), de sorte que SOCKS peut percevoir les applications et peut facilement pointer vers le logiciel Tor, ce qui montre que les applications utilisant SOCKS n'ont besoin d'aucune modification et peuvent être utilisées directement.

  De plus, I2P est un middleware qui fournit des API que les applications peuvent utiliser pour communiquer sur le réseau, ce qui signifie que les applications nécessitent des ajustements complexes. SOCKS et l'API I2P ont considérablement modifié la charge de travail et la capacité de créer des applications qui utilisent les réseaux I2P ou Tor et communiquent de manière anonyme sur Internet.

  L'interface SOCKS ne peut transmettre des messages que via TCP, et I2P peut choisir entre UDP et TCP, ce qui permet à I2P d'offrir de meilleures performances lors de l'utilisation de certaines applications.

- **Applications disponibles** : I2P et Tor ont une large gamme d'applications, et la plupart des applications I2P sont dédiées à l'accès aux services au sein du réseau I2P (à l'exception de Susimail/2IpMail qui peut envoyer et recevoir du courrier depuis l'Internet public).

  De plus, étant donné que Tor utilise l'interface SOCKS, Tor peut être utilisé avec n'importe quelle application qui utilise une configuration de proxy SOCKS (comme un navigateur Web commun).

- **Sécurité des messages et anonymat :** Les deux réseaux ont différentes couches de cryptage, à commencer par le cryptage de la couche de transport fourni par la connexion TLS maintenue par OR (OnionRouters) ou les pairs I2P, I2P dispose également de fonctions de cryptage de tunnel supplémentaires.

Les messages envoyés sur le réseau sont des oignons ou de l'ail cryptés, ce qui signifie que la connexion de l'utilisateur au tunnel ou au circuit est toujours cryptée. Tant qu'il y a une interaction au sein du réseau, les messages dans I2P sont également cryptés de bout en bout. Mais dans le cas de Tor, le chiffrement de bout en bout ne peut pas être garanti, selon le protocole de couche transport utilisé.

- **Performances** : utilisez I2P ou Tor pour accéder à l'Internet public avec la latence et la bande passante comme indicateurs d'évaluation. Les mesures ont révélé que : I2P peut obtenir de meilleurs résultats lors de l'émission d'une simple requête HTTP-GET, mais Tor consiste à accéder à l'intégralité de la page Web et à télécharger des fichiers. Fournit des résultats nettement meilleurs. Dans 50 % des cas, Tor peut récupérer l'intégralité de la page Web en moins de 16,99 s, tandis que 50 % des requêtes I2P coûtent 103,19 s. En termes de vitesse de téléchargement, Tor peut fournir une vitesse moyenne de 51,62 kb/s, tandis que la vitesse moyenne d'I2P est de 12,91 kb/s.

- **Utilisation :** I2P fournit une variété d'applications, spécialement conçues pour la communication au sein du réseau I2P, il a donc très peu d'agents. Tor est conçu pour acheminer le trafic en dehors du réseau et possède plus de nœuds de sortie que I2P.

- **Évolutivité :** l'augmentation du nombre de clients participant au réseau anonyme affecte directement Tor et I2P. Le nombre de paramètres anonymes augmente et le trafic réseau augmente et peut entraîner une congestion et d'autres problèmes. Pour Tor, il peut être nécessaire d'augmenter le nombre de routeurs utilisés pour construire des circuits, augmentant ainsi la latence et réduisant la bande passante disponible. L'augmentation du nombre de routeurs d'oignons crée un autre problème, celui du catalogue en constante augmentation. Dans le cas de l'I2P, en supposant que les nouveaux pairs rejoignant le réseau peuvent fournir une capacité et une bande passante suffisantes, ils peuvent également être des pairs utilisés pour construire des tunnels. Par conséquent, la congestion est peu probable, mais si un nombre suffisant de clients cherchent à accéder à des services en dehors du réseau I2P, plus d'agents externes doivent être fournis.

2.4.3 Les technologies Tor et I2P

a. Sélection par les pairs

Tor est une sélection de pairs basée sur la bande passante et I2P est une sélection de pairs basés sur les performances. Le but de la sélection par les pairs est de construire rapidement des circuits ou des tunnels [20].

- **Tor : sélection des pairs basée sur la bande passante.**

Le serveur d'annuaire de Tor utilise la détection active de bande passante pour mesurer et enregistrer la bande passante que chaque RO (routeur oignon) peut fournir. S'il n'y a pas de données de détection pour ce RO spécifique, Tor doit également s'appuyer sur la valeur de bande passante libérée par chacun. Les informations de bande passante sont utilisées pour sélectionner des routeurs intermédiaires et des routeurs de sortie selon une probabilité pondérée.

Le client Tor utilise un algorithme de sélection de chemin pour sélectionner le RO utilisé pour construire le circuit, et il sera utilisé en premier tant que la valeur mesurée est disponible. La probabilité que tous les autres RO dans Tor soient sélectionnés est proportionnelle à leur bande passante, ce qui signifie que seule la bande passante est prise en compte et que d'autres attributs (tels que l'emplacement réel du RO) sont ignorés.

- **I2P : sélection par les pairs basée sur la performance**

Le client I2P s'appuie sur des valeurs de performances précédemment surveillées et sur l'état actuel du réseau, et n'utilise pas de détection de bande passante efficace. L'algorithme de sélection de nœud I2P peut également réagir très rapidement aux pairs défaillants et à d'autres changements dans la topologie du réseau, et sélectionner les pairs via une analyse continue et des performances de classement au lieu de faire confiance à la capacité revendiquée.

b. Transmission TCP/UDP

Étant donné que les nœuds du réseau Tor (à l'exception du nœud de sortie et du serveur) utilisent TLS pour une connexion cryptée afin de créer des circuits, TLS est utilisé pour empêcher les attaquants potentiels de modifier les données et de se faire passer pour un routeur en oignon, améliorant ainsi l'efficacité et la sécurité du réseau. Tor utilise l'interface SOCKS pour interagir avec Internet afin d'améliorer l'anonymat des utilisateurs.

Mais TLS et SOCKS sont tous basés sur TCP, donc les connexions TCP sont utilisées entre les relais Tor, et plusieurs flux TCP peuvent partager un circuit virtuel, et chaque OU utilise TLS pour se connecter à d'autres ORs [20].

Dans le réseau I2P, tous les nœuds utilisent TLS pour les connexions cryptées afin de créer des tunnels, et les nœuds constatent qu'ils utilisent l'algorithme de distance XOR de Kademlia. TLS et Kademlia sont respectivement basés sur TCP et UDP, donc le routage I2P utilise à la fois la connexion TCP et UDP pour la transmission de données. La connexion de transmission I2P est constituée de deux protocoles de transmission pair à pair NTCP et SSU. NTCP est un TCP basé sur NIO et SSU est un UDP semi-fiable (son objectif principal est de transmettre en toute sécurité des messages I2NP via un tunnel et de crypter uniquement les fonctions UDP). I2P utilise à la fois TCP et UDP pour la transmission. Pour certains périphériques d'inspection approfondie des paquets (DPI), UDP peut être plus difficile à suivre.

2.5 Inconvénients des réseaux Tor et I2P

La gestion des risques joue un rôle essentiel dans la protection des actifs informationnels d'une organisation. Chaque organisation doit évaluer le risque et l'impact que l'utilisation de toute nouvelle technologie dans son réseau d'entreprise peut avoir sur son activité.

Tor et I2P sont l'un de ces outils que les organisations doivent comprendre pour être conscientes des risques associés et de ses avantages. S'il est vrai que Tor et I2P peuvent être utilisé dans un objectif légitime d'anonymat sur Internet, cela peut être un énorme problème pour une organisation : contourner la sécurité du réseau, se connecter à des sites criminels sur le 'darknet' ou 'dark web', impliquant l'organisation dans des activités criminelles, exposant le réseau de l'entreprise à des infections de logiciels malveillants, etc[21]. Le tableau 2.5 nous montre les principaux inconvénients de chaque réseau :

Tor	I2P
Le serveur d'informations d'annuaire peut être bloqué.	Vulnérable aux attaques de partitionnement
Blocage basé sur l'empreinte digitale de la connexion Tor	Attaques d'intersection possibles
Centralisation des serveurs d'annuaire pour la gestion du réseau Tor	Manque de surveillance des nœuds et de la bande passante
Chemin unique pour un flux de données se déplaçant à l'intérieur d'un circuit	Conflits NetDB et résolution
Empreintes digitales de sites Web et attaque en retour en raison de l'absence de camouflage des paquets.	Attaque d'utilisateurs gourmands utilisateurs prêts à télécharger plus qu'à
Les succès ou les échecs des contrôles d'intégrité des données peuvent rendre un circuit inutile.	Attaque de famine : communication mauvaise et intermittente pour les utilisateurs finaux
Empreintes digitales de sites Web et attaque en retour en raison de l'absence de camouflage des paquets.	Uploader ce qui diminue le trafic de relecture

Tableau 2-5: *Les inconvénients du réseau Tor et I2P.*

2.5.1 Les risques d'utiliser Tor ou I2P au sein d'un réseau d'entreprise

1. **Risque 1 : exposer l'entreprise aux attaques de logiciels malveillants et de réseaux de zombies**

Les personnes utilisant l'un des « nœuds de sortie » peuvent utiliser l'appareil pour ajouter des logiciels malveillants. Ainsi, tout utilisateur téléchargeant via Tor expose le réseau de l'organisation à une infection par des logiciels malveillants. En plus de cela, il est important de savoir que les criminels commencent à utiliser Tor comme canal de communication pour les logiciels malveillants.

2. **Risque 2 : exposer l'organisation à des attaques DDoS**

Avoir un ou plusieurs ordinateurs fonctionnant en nœuds Tor ou I2P expose l'entreprise au risque de DDoS. Le fait qu'un ou plusieurs serveurs d'entreprise relayent le trafic réseau Tor peut entraîner une consommation élevée de la bande passante du réseau d'entreprise, ce qui expose l'organisation en permanence à une attaque DDoS.

3. **Risque 3 : Permettre aux employés de contourner les contrôles de sécurité**

Le fait que Tor ou I2P crypte tout le trafic sur le réseau rend très difficile la surveillance des activités du réseau entre le nœud Tor (ou I2P) et Internet. De cette façon, les gens peuvent contourner très facilement les politiques de sécurité et les contrôles de l'organisation. Ils peuvent se connecter à des sites Web illégaux, atteindre le Darknet et acheter des services illégaux, et voler des données sensibles à l'insu de quiconque.

4. **Risque 4: Être victime d'un vol d'informations**

Le trafic peut être reniflé au nœud de sortie. Les personnes exploitant le nœud de sortie peuvent surveiller le trafic transitant par son appareil puis capturer toute information sensible non cryptée (HTTP, FTP, SMTP sans TLS…). Cela étant dit, les employés utilisant Tor (ou I2P) sont exposés au risque de voir leurs données et les informations appartenant à leurs organisations volées, ce qui peut avoir un impact majeur sur leur entreprise. Cette attaque est également connue sous le nom d'attaque MiTM (Man in The Middle).

5. **Risque 5 : Liste noire**

La mise en place d'un nœud Tor à l'intérieur d'un réseau court le risque que l'IP d'une organisation soit ajoutée à une liste noire Internet, notamment si le nœud est impliqué dans des activités illégales.

6. **Risque 6: Impact négatif sur la réputation de l'organisation**

Les organisations exploitant des nœuds Tor peuvent être tenues responsables des activités (illégales) d'autrui. Ainsi, ils peuvent s'exposer à de graves sanctions pénales si l'un des nœuds qu'ils exploitent est découvert en train de transporter du matériel illégal ou en train de mener des activités illégales (piratage, attaques DDoS, espionnage, etc.). Cela se produit généralement lorsque vous exploitez un nœud de sortie, car c'est l'adresse IP du

nœud de sortie qui apparaît lorsque les autorités commencent à enquêter sur les empreintes digitales du crime.

2.6 Conclusion

Après l'énumération des techniques et technologies des réseaux anonymes Tor et I2P. Nous avons vu que ce sont conçus pour protéger l'anonymat de leurs utilisateurs. Les réseaux anonymes sont souvent construits sur le même modèle, celui du relais de proxy et du chiffrement en couche. Malgré ça, il y a toujours un moyen de détecter l'utilisation de l'un de ces deux réseaux.

Cette étude détaillée de ces réseaux anonymes va nous permettre de proposer une méthode de détection de l'utilisation des deux réseaux anonymes dans le chapitre suivant pour lutter contre toute forme de mauvaise utilisation de l'anonymat sur internet dans une entreprise.

Chapitre 3 :

Extraction des signatures Tor & I2P

3.1 Introduction

L'utilisation des réseaux anonymes Tor et I2P sont considérés comme les piliers de l'anonymat sur internet. Malheureusement un utilisateur se cache derrière ces réseaux pour contourner la réglementation interne du réseau de l'entreprise, Car cela peut causer divers risques de sécurité et de problèmes judiciaires. C'est pour cette raison qu'une entreprise souhaite bannir tout le trafic anonyme.

La première chose à noter est que dans un réseau d'entreprise, il est difficile à détecter et à intercepter les deux réseaux Tor et I2P. Car pour détecter ces derniers, l'administrateur doit analyser le trafic Web normal et le trafic du réseau Tor et I2P pour comprendre la différence entre eux. Cela nous mènera à extraire les signatures numériques du réseau Tor et I2P qui les définit.

Dans ce chapitre, nous allons aborder notre architecture de travail dont le but est de simuler le réseau d'entreprise. Ensuite, nous effectuerons une détection Tor et I2P dans notre réseau. En se basant sur l'utilisation de Wireshark afin d'analyser les paquets qui contiennent des signatures ayant lien avec les réseaux Tor et I2p.

3.2 L'explication du projet

Rappelons, que l'objectif de ce projet est la détection de l'utilisation des réseaux Tor et Wireshark. Pour atteindre cet objectif, il faut passer par plusieurs étapes successives pour trouver une solution à ces abus qui surviennent lorsqu'un individu utilise des réseaux anonymes au sein d'une entreprise :

1. **Phase de compréhension :** Etude théorique afin de comprendre le fonctionnement en détails des deux réseaux.
2. **Phase de capture :** cette phase permet de récolter des d'informations sur plusieurs protocoles ayant lieu avec les deux réseaux grâce au logiciel « Wireshark ».
3. **Phase de l'analyse :** cette partie d'analyse permet le maximum d'informations pour l'extraction d'empreintes avec un taux de faux positif plus faible.

4. **Phase de détection :** implémentation des signatures extraites dans la phase analyse. Au niveau du système de détection d'intrusions « Snort » qui va nous permettre d'observer de près l'efficacité de la solution proposée.

3.3 Architecture de réseau

3.3.1 Matériels

Nous avons réalisé un réseau local connecté à internet, les expériences ont été faites sur :

a. Partie Serveur :

- Un ordinateur portable DELL avec un processeur Intel(R) Core (TM) i5-7200U CPU @ 2.50GHz 2.70 GHz avec 8.00 GB de RAM.

b. Partie cliente :

- Un ordinateur portable HP avec un processeur Intel(R) Core (TM) i5 -2nd Gen CPU @ 2.50GHz avec 4.00 GB de RAM.

c. Backbone :

- Modem 4G LTE (Algérie télécom)

d. Liaison :

- Des câbles RJ45

3.3.2 Environnement

a. Architecture client/serveur

La figure 3.1 va nous montrer notre architecture de travail :

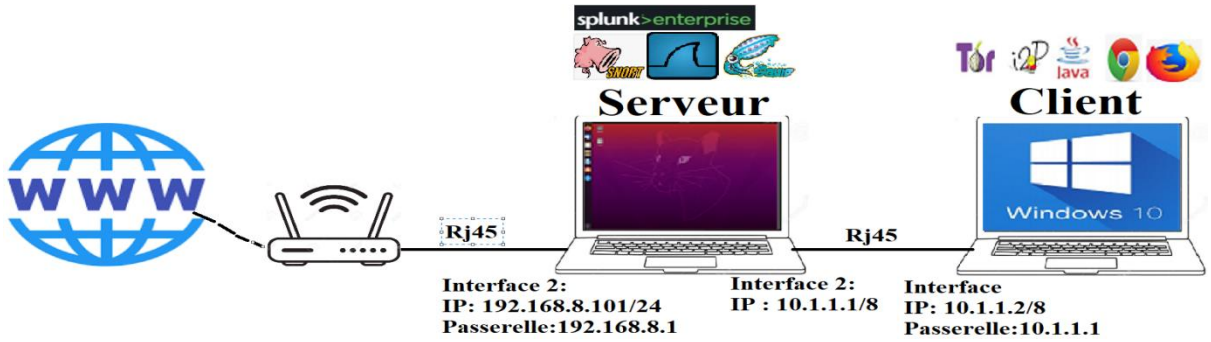

Figure 3.1: *Architecture de réseau*

- **Le pc serveur a deux interfaces réseau :**
  - La première interface Ethernet est liée au backbone d'internet à travers le modem 4G LTE d'Algérie télécom avec un câble Rj45.
  - La deuxième interface est un adaptateur USB Ethernet branché sur le port USB qui est connecté au réseau local avec une plage d'adresses privée (10.1.1.0/8) par l'adresse : 10.1.1.1 (passerelle).
- **Le pc client** : est connecte au réseau local par l'adresse : 10.1.1.2 et la passerelle : 10.1.1.1

b. Serveur « Ubuntu »

Dans notre travail on a opté pour la distribution Linux Open Source pour le serveur d'entreprise, le bureau, le Cloud et l'IOT. Et tout comme d'autres projets basés sur Linux, Ubuntu bénéficie d'un solide soutien de la communauté et c'est l'un des plus grands avantages d'Ubuntu par rapport aux autres distributions.

c. Logiciels

Ordinateur	Serveur	Client
Systèmed'expoilatation	Système d'exploitation Ubuntu 20.04 64 bits.	Système d'exploitation Windows 10 professionnel 64 bits.

Logicielsinstallés	• Wireshark • Squid • Snort • Splunk	• Google chrome • Mozilla Firefox • Tor • I2P • Java

Tableau 3-1:*Logiciels installés dans le serveur et le client.*

d. Logiciels PC Serveur

1. Squid

Squid est une application de serveur de cache proxy Web qui fournit des services de proxy et de cache pour le protocole de transport hypertexte (HTTP), le protocole de transfert de fichiers (FTP) et d'autres protocoles réseau populaires. Squid peut implémenter la mise en cache et le proxy des requêtes SSL (Secure Sockets Layer) et la mise en cache des recherches DNS (Domain Name Server) et effectuer une mise en cache transparente [22].

Squid prend également en charge une grande variété de protocoles de mise en cache, tels qu'Internet Cache Protocol (ICP), « Hyper TextCaching Protocol (HTCP) », « Cache ArrayRouting Protocol (CARP) » et « Web Cache Coordination Protocol (WCCP) ».

Le serveur de cache proxy Squid est une excellente solution pour une variété de besoins de serveur proxy et de mise en cache, et s'adapte des succursales aux réseaux d'entreprise tout en fournissant des mécanismes de contrôle d'accès étendus et une surveillance des paramètres critiques via le protocole de gestion de réseau simple (SNMP).

Apres l'installation de Squid nous avons créé une ACL dans le fichier **« /etc/squid/squid.conf »**Pour empêcher le client d'accéder à certains sites Web l'exemple de : **(.amazon.com , .centos.org).**

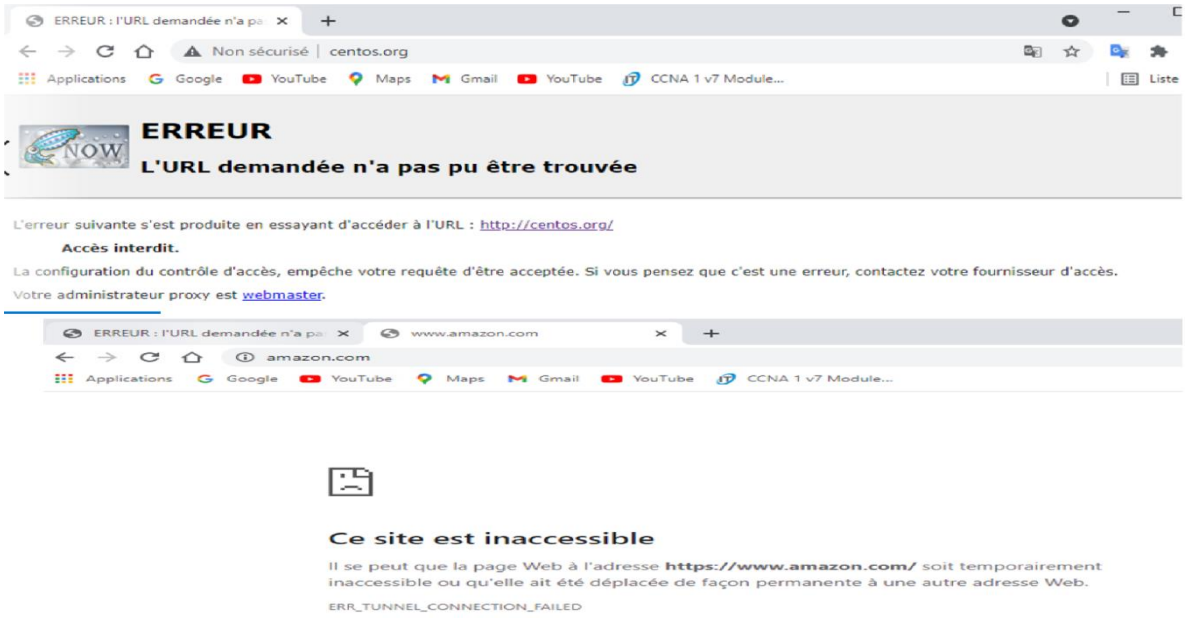

Figure 3.2: *Sites centos.org et amazon.com bloqués par Squid.*

2. Outil d'analyse et de capture « Wireshark »

Wireshark est un analyseur de paquets réseau. Un analyseur de paquets réseau présente les données de paquets capturées de manière aussi détaillée que possible [23].

Nous pourrions considérer un analyseur de paquets réseau comme un appareil de mesure permettant d'examiner ce qui se passe à l'intérieur d'un câble réseau.

Dans le passé, ces outils étaient soit très coûteux, propriétaires ou les deux. Cependant, avec l'avènement de Wireshark, cela a changé. Wireshark est disponible gratuitement, est open source, il est l'un des meilleurs analyseurs de paquets actuellement[23].

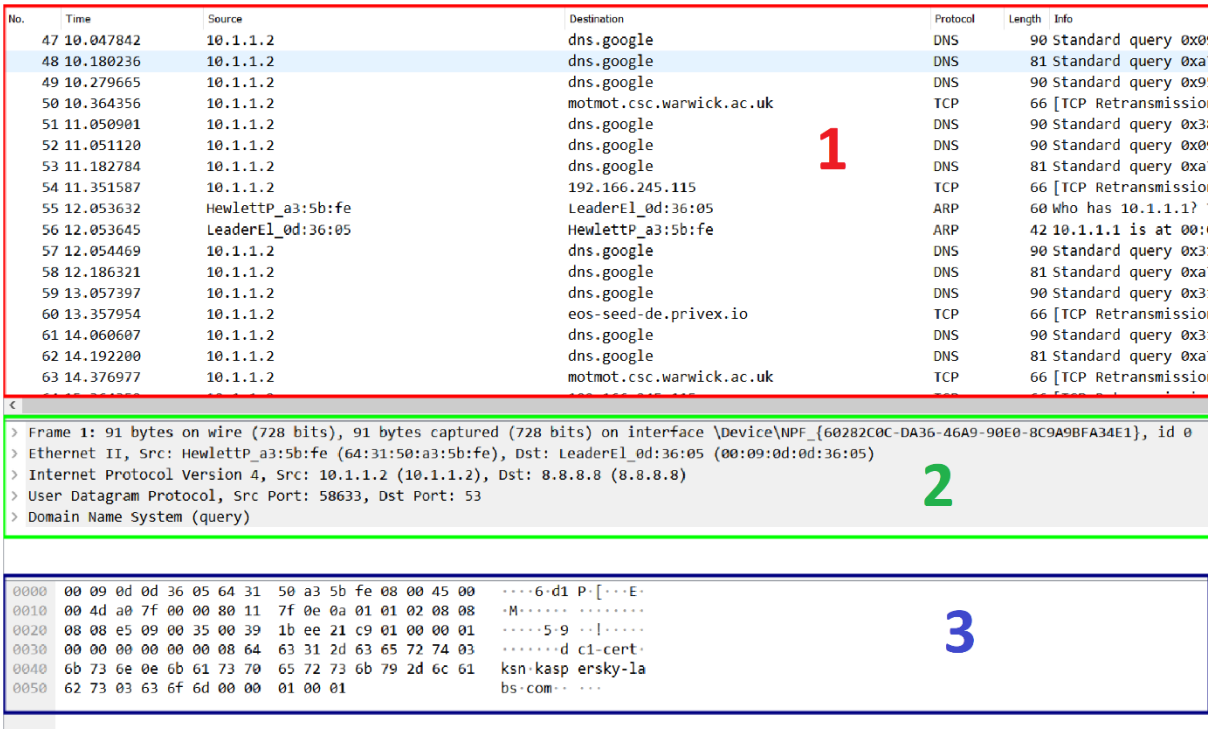

Figure 3.3: *Interface Wireshark.*

- **Le rectangle rouge (numéro 1**) dans la figure 3.3 affiche les paquets captures.
- **Le rectangle vert (numéro 2)** affiche les détails de chaque paquet sélectionné dans le rectangle rouge.
- **Le rectangle bleu (numéro 3)** affiche le code hexadécimal pour chaque ligne sélectionnée dans le rectangle vert.

Remarque : les deux autres logiciels (Snort et Splunk) seront discutés dans le chapitre suivant.

3.4 Réseau Tor

3.4.1 Circuit Tor

Le lancement du navigateur Tor est simple, il suffit juste de cliquer sur l'icône Start Tor Browser et la connexion du navigateur au réseau Tor s'établie.

Le circuit Tor nous permet de surfer sur internet ou sur des sites en .onion . Le circuit est composé de relais qui lui sont attribué aléatoirement, ces relais sont des ordinateurs éparpillés partout dans le monde, afin de garantir l'acheminement du trafic Tor.

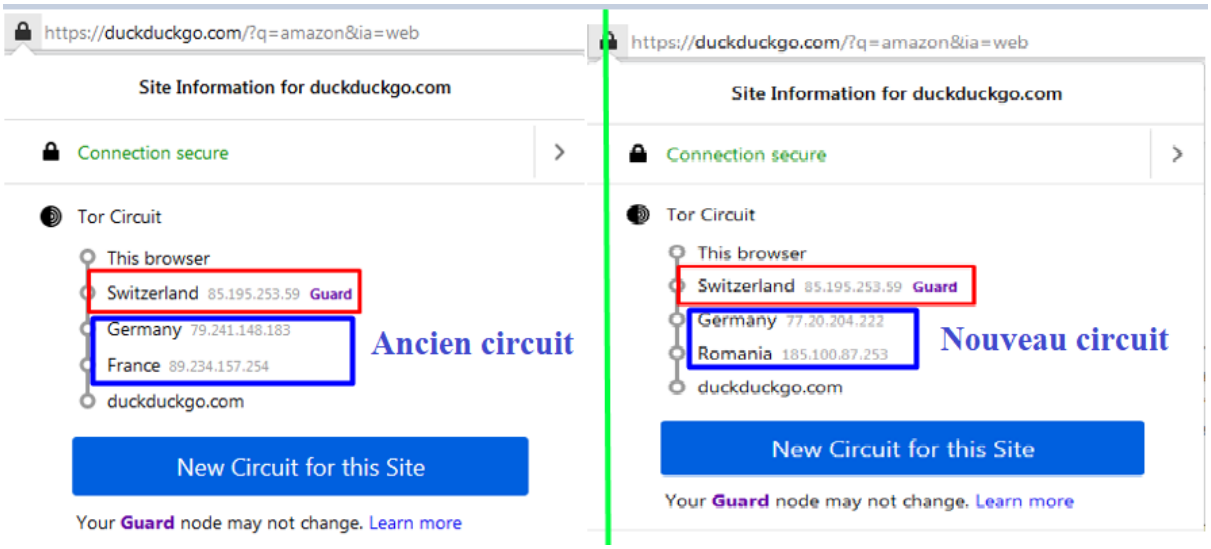

Figure 3.4: *Circuit Tor.*

Les adresses mentionnées dans la figure 3.4 sont les adresses des relais qui composent le circuit. Il existe une possibilité de donner un nouveau circuit Tor manuellement mais tout en gardant le premier nœud (Relais garde/Garde d'entrée), il s'agit d'un nœud rapide et stable. Le reste du circuit change pour chaque nouveau site visité.

3.4.2 Accès aux sites bloqués via Tor

Tor peut détourner le blocage des sites censurés par le proxy squid comme nous montre la figure ci-dessus.

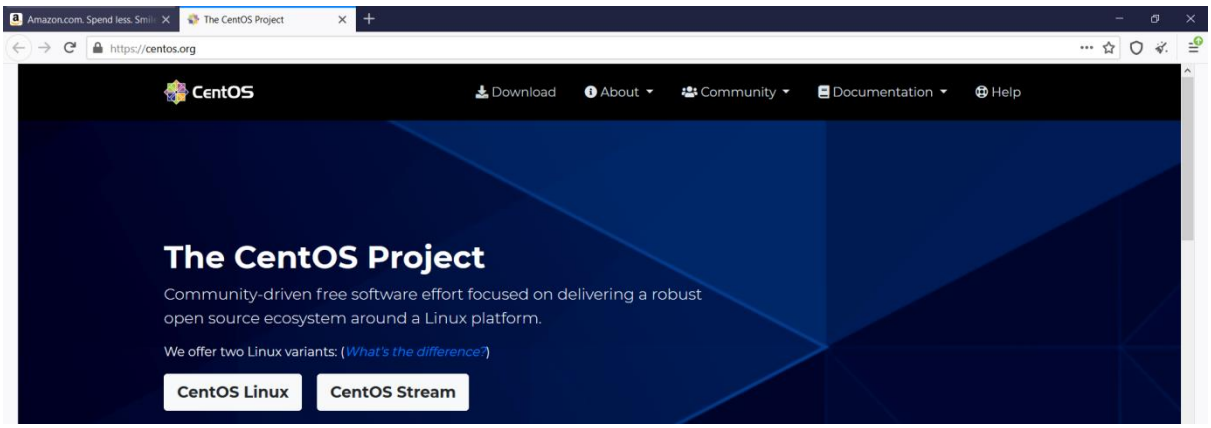

Figure 3.5: *Accès à "centos.org" avec Tor.*

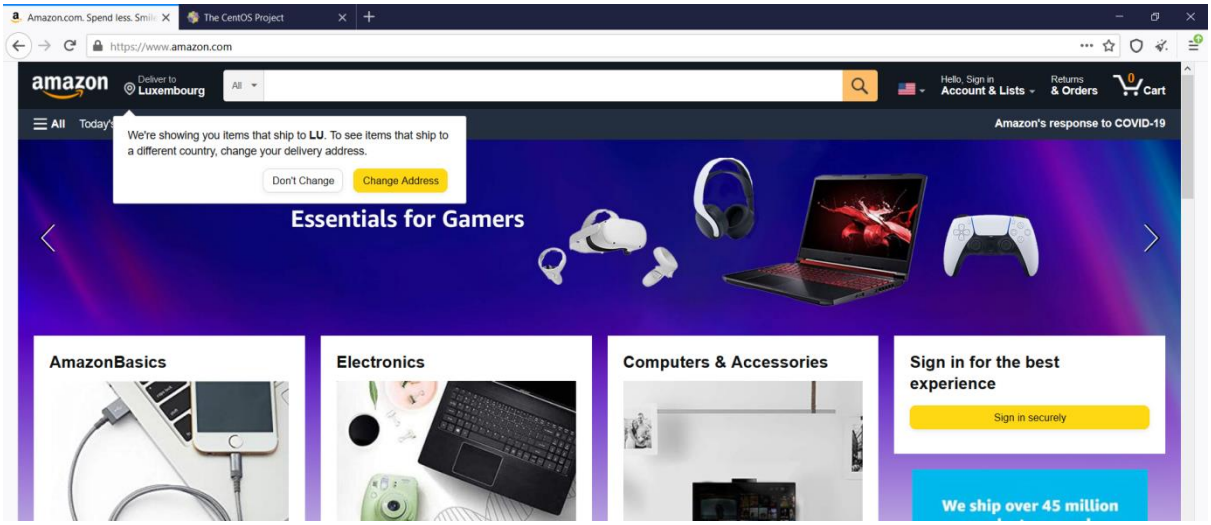

Figure 3.6: *Accès à "amazon.com" avec Tor.*

Comme nous montre la figure ci-dessus, nous avons pu y accéder aux sites Web bloqués par le serveur via le navigateur Tor à l'aide des circuits variables pour chaque site.

3.4.3 Phase d'analyse pour le réseau Tor

3.4.3.1 Extraction des signatures du réseau Tor

Comme les autres réseaux anonymes, Tor utilise le protocole TLS pour chiffrer le trafic. Et comme il est considéré comme étant un réseau fiable alors il nécessite un transport fiable basé sur TCP. Le client Tor établit une connexion TCP avec le nœud de garde, puis établit une session chiffrée TLS, c'est pour cela qu'on va renifler les paquets juste au moment de la création (lancement), car on ne pourra pas analyser les paquets lorsque le cryptage TLS serra effectuer. Notre travail se résume sur l'analyse et la comparaison des différents paquets ordinaires (paquet de Chrome et Mozilla) et les paquets TOR, lors de la réalisation d'une connexion TCP et TLS.

Pour faire l'analyse on a choisi les sites :

- **Site 1 :** centos.org avec les deux adresses : 81.171.33.202 et 81.171.33.201 (Firefox, chrome)
- **Site 2 :** amazon.com avec l'adresse : 162.219.225.118.

Et pour extraire des signatures fiables, on va utiliser 3 nœuds de garde différents pour récolter le maximum d'empreintes qui vont identifier par la suite l'utilisation du réseau Tor.

Nom de l'hôte	Adresses IP	port
Rick.83e.de	178.63.69.2	9001
none	82.223.222.61	9054(aléatoire)
none	116.203.78.147	443(HTTPS)

Tableau 3-2: *Les nœuds de Tor.*

Pour extraire les informations sur les nœuds, les développeurs de TOR offrent un accès à une plateforme accessible via : https://metrics.torproject.org/rs.html.

Informations sur les nœuds de garde :

- Le premier nœud garde : 178.63.69.2.

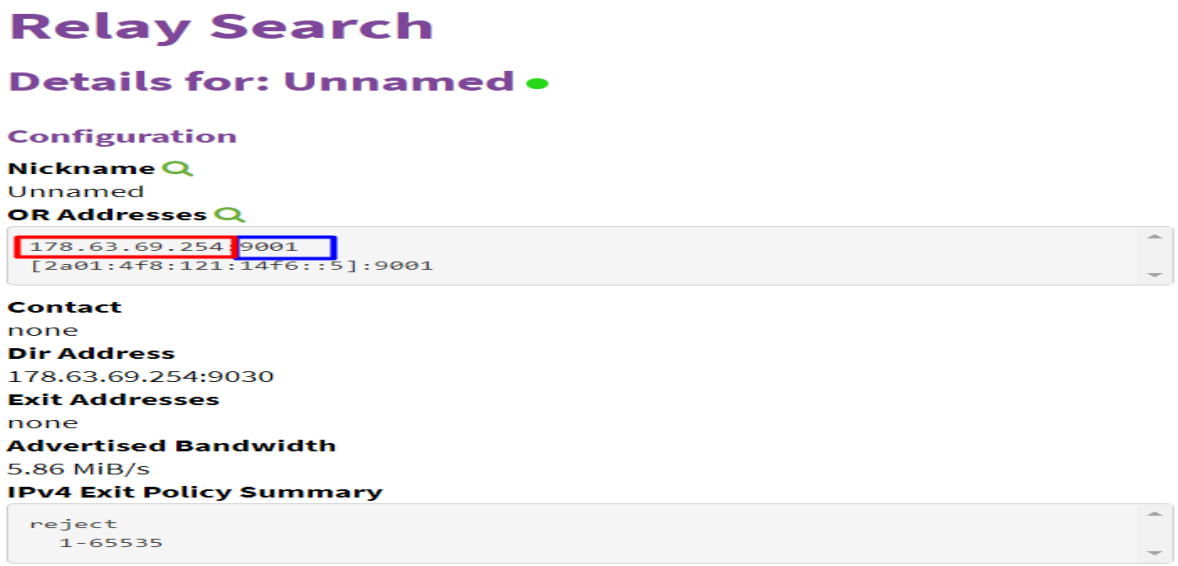

Figure 3.7: *Premier nœud de garde.*

- Le deuxième nœud de garde : 82.223.222.61

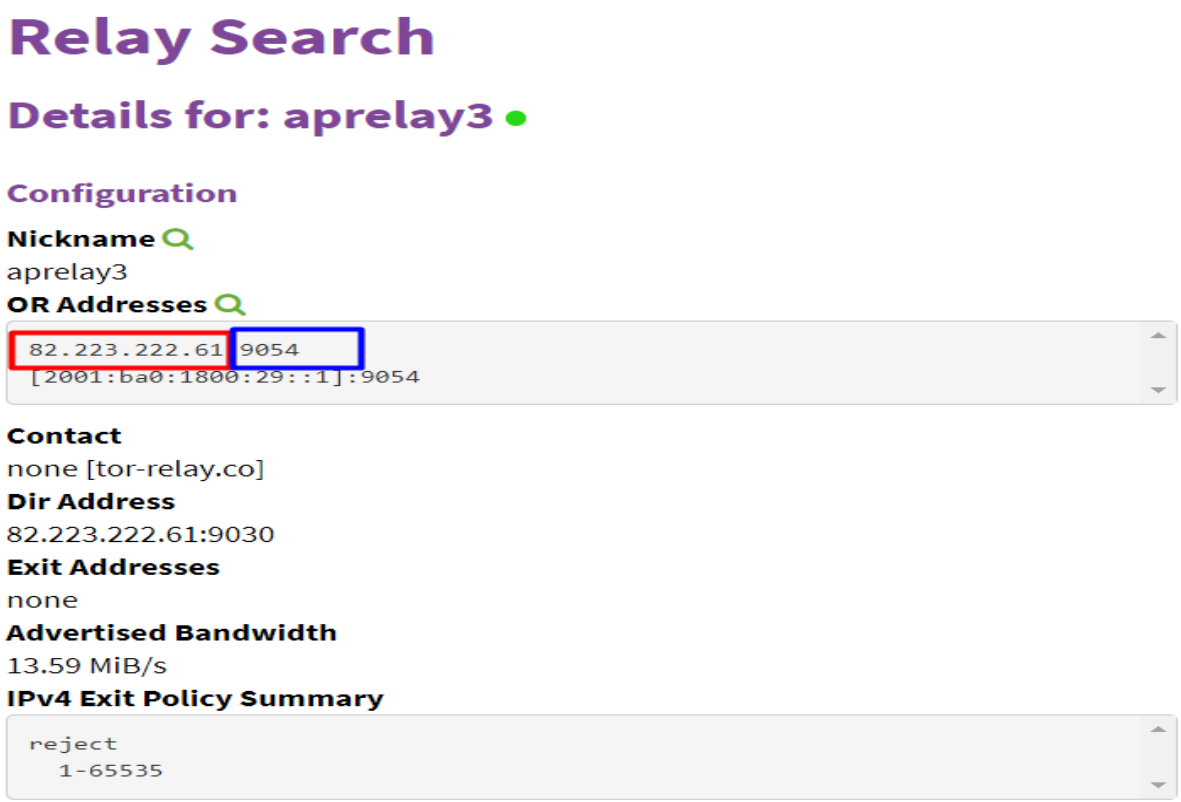

Figure 3.8: *Deuxième nœud de garde.*

- Le troisième nœud de garde : 116.203.78.147

Figure 3.9: *Le troisième nœud de garde.*

3.4.3.2 Analyse du trafic Web des différents navigateurs

a. Etude des étapes de la connexion TCP « ThreeWay Handshake » :

La connexion TCP s'effectue en trois phases [SYN, SYN-ACK, ACK].Pour une recherche fluide de cette connexion nous allons spécifier un filtre sur Wireshark ip.addr == 81.171.33.201 && TCP.

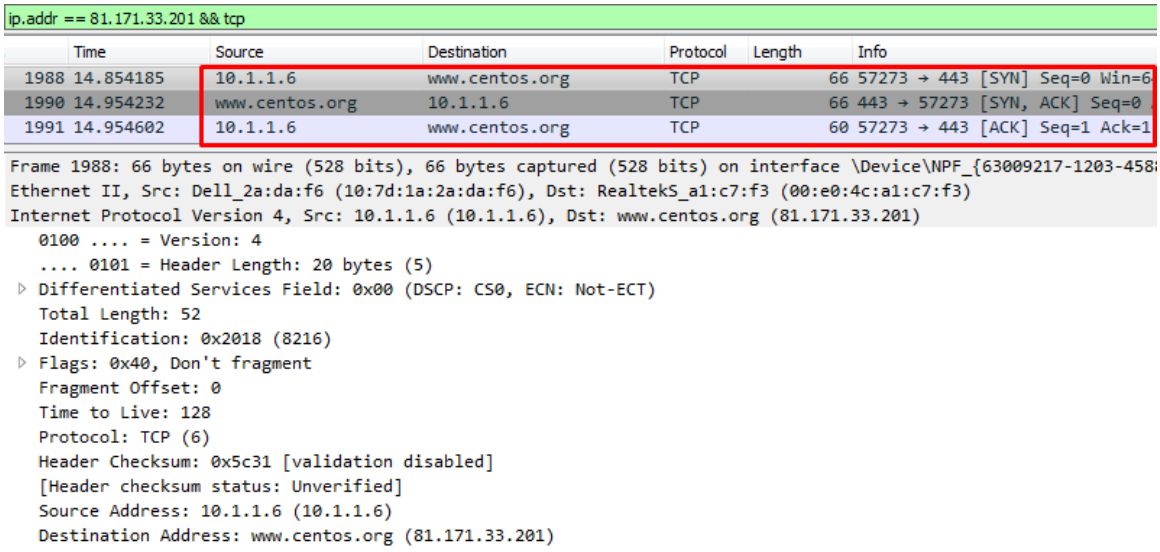

Figure 3.10: *Connexion TCP entre le navigateur chrome et centos.org.*

Pour l'étude des paquets TCP nous allons analyser les connexions établies entre :

- Le navigateur TOR et le premier nœud de garde 178.63.69.2 (port= 9001).
- Le navigateur TOR deuxième nœud de garde 82.223.222.61 (port= 9054 aléatoire).
- Le navigateur TOR et le troisième nœud de garde 116.203.78.147 (port= 443).
- Le navigateur Chrome et le site www.centos.org avec une adresse 81.171.33.201.
- Le navigateur Firefox et le site www.centos.org avec une adresse 81.171.33.202

Dès que les paquets sont capturées par l'outil Wireshark, on va comparer les résultatsextraits des captures Wireshark du navigateur TOR, le navigateur Chrome et Firefox. La comparaison se fera entre les trois phases de la connexion TCP.

Exemple d'un affichage de la deuxième partie Wireshark qui couvre les différentes couches d'encapsulation d'un paquet « SYN ».

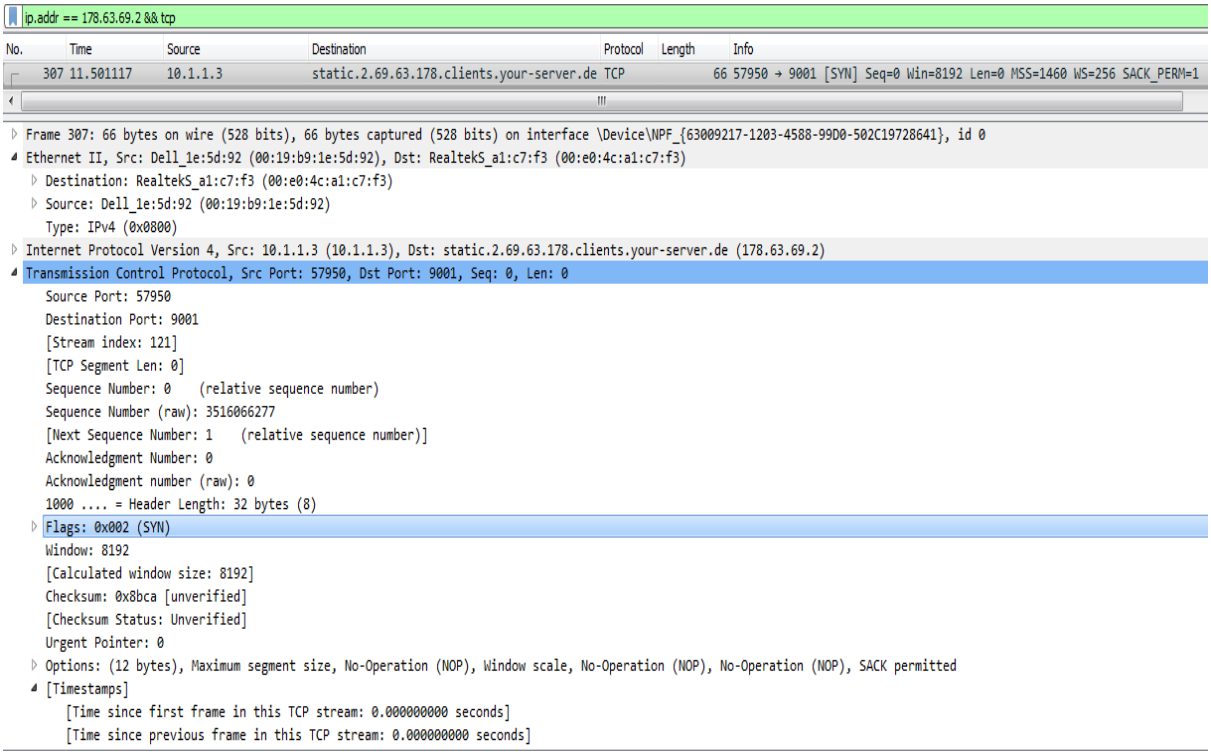

***Figure 3.11**: Paquet Tor / TCP (SYN).*

Cette partie nous permet d'extraire les informations ayant lien avec :

- **Total Length :** le champ Longueur totale est codé sur 16 bits et représente la longueur du paquet incluant l'entête IP et les Data associées.
- **Identification :** numéro permettant d'identifier les fragments d'un même paquet.
- **Le champ TTL (Time To Live) :** il est codé sur 8 bits et indique la durée de vie maximale du paquet. Il représente la durée de vie en seconde du paquet. Si le TTL arrive à 0, alors l'équipement qui possède le paquet, le détruira.
- **Port Source :** le champ Port source est codé sur 16 bits et indique le numéro de port de l'expéditeur
- **Port Destination :** le champ Port destination est codé sur 16 bits et indique le numéro de port du destinataire.
- **Numéro de séquence** :le champ numéro de séquence est codé sur 32 bits et correspond au numéro du paquet. Cette valeur permet de situer à quel endroit du flux de données le paquet, qui est arrivé, doit se situer par rapport aux autres paquets.
- **Stream Index:** Stream Index ou l'index de flux est un mappage Wireshark interne.

- **Flags (6 bits) :** les 6 bits individuels disponibles au champ Flags permettent d'activer différentes actions TCP visant l'organisation de la communication et de la transmission de données. Les Flags suivants peuvent être activés ou désactivés :
  - **Le champ URG** est codé sur 1 bit et indique que le champ Pointeur de donnée urgente est utilisé.
  - **Le champ ACK** est codé sur 1 bit et indique que le numéro de séquence pour les acquittements est valide.
  - **Le champ PSH** est codé sur 1 bit et indique au récepteur de délivrer les données à l'application et de ne pas attendre le remplissage des tampons.
  - **Le champ RST** est codé sur 1 bit et demande la réinitialisation de la connexion.
  - **Le champ SYN** est codé sur 1 bit et initie donc l'activation de la connexion.
  - **Le champ FIN est** codé sur 1 bit et indique fin de transmission.
  - **Window Size Value :** elle est utilisée pour indiquer à l'expéditeur la quantité de données à transmettre avant de recevoir un accusé de réception.
  - **Maximum Segment Size :** MSS est la taille maximale du datagramme TCP. II représente la taille de charge utile maximale qu'un point d'extrémité est prêt à accepter dans un seul paquet.
  - **RTT to ACK (Round Time Trip to ACKnowledgement) :** RTT to ACK est un mécanisme de temporisation et de retransmission. RTT est le temps que met un signal pour parcourir l'ensemble d'un circuit fermé.

Avant de passer à l'étude des étapes de TLS, on constate que cette analyse de l'étude des étapes de la connexion TCP nous n'a pas permet d'extraire des signatures qui vont empreinter par la suite l'utilisation du réseau Tor.

Paquet TCP (SYN) :

	Chrome 10.1.1.3 to 81.171.33.201	Firefox 10.1.1.3 To 81.171.33.202	Tor 9001 to 178.63.69.2	Tor HTTPS to 116.203.78.147	Tor aléatoire to 82.223.222.61
type	Ipv4(0x800)	Ipv4(0x800)	Ipv4(0x800)	Ipv4(0x800)	Ipv4(0x800)
Total length	52	52	52	52	52
Identification	0x04be(1214)	0x319b (12699)	0x724d(29261)	0xa660 (42592)	0x01b98(7064)
TTL	128	128	128	128	128
Protocol	Tcp(6)	Tcp 6	Tcp(6)	Tcp(6)	Tcp(6)
Port source	61101	54179	57950	59311	50548
Port dest	443	443	9001	443	9054
Stream index	56	24	121	2	2
Numéro de séquence	0	0	0	0	0
Flags	0x002 (SYN)	0x002(SYN)	0x002(SYN)	0x002(SYN)	0x002(SYN)
Window size value	8192	8192	8192	64240	64240
Checksum(tcp)	0x8e50	0x7609	0x08bca	0xf539	0x0cfd
Maximum segment size	1460	1460	1460	1460	1460

Paquet TCP (SYN-ACK)

Tableau 3-3 : Paquet SYN d'une connexion TCP.

	Chrome 10.1.1.3 to 81.171.33.201	Firefox 10.1.1.3 To 81.171.33.202	Tor 9001 to 178.63.69.2	Tor HTTPS to 116.203.78.147	Tor aléatoire to 82.223.222.61
Type	Ipv4(0x800)	Ipv4(0x800)	Ipv4(0x800)	Ipv4(0x800)	Ipv4(0x800)
Total length	52	52	52	52	52
Identification	0x0000(0)	0x0000(0)	0x0000(0)	0x0000(0)	0x0000(0)
TTL	32	51	52	37	51
Protocol	Tcp(6)	Tcp 6	Tcp(6)	Tcp(6)	Tcp(6)
Port source	443	443	9001	443	9054
Port dest	49267	54179	57950	59311	50548
Stream index	55	24	121	2	2
Numéro de séquence	0	0	0	0	0
Flags	0x012 (SYN, ACK)	0x012 (SYN, ACK)	0x012 (SYN, ACK)	0x012 (SYN, ACK)	0x012 (SYN, ACK)
Window size value	26883	29200	64240	64240	64240
Checksum(tcp)	0x405a	0xeac7	0x6115	0xf2ac	0x7a7a
Maximum segment size	1460	1460	1460	1400	1460
RTT to ACK(sec)	0.068067000	0.073819000	0.065275000	0.091746995	0.084015000

Tableau 3-4: Paquet SYN-ACK d'une connexion TCP.

Paquet TCP (ACK):

	Chrome 10.1.1.3 to 81.171.33.201	firefox 10.1.1.3 To 81.171.33.202	Tor 9001 to 178.63.69.2	Tor HTTPS to 116.203.78 .147	Tor aléatoire to 82.223.2 22.61
type	Ipv4(0x800)	Ipv4(0x800)	Ipv4(0x800)	Ipv4(0x80 0)	Ipv4(0x8 00)
Total length	40	40	40	40	40
Identification	0x04c9(1225)	0x319d(12701)	0x724f(2926 3)	0x0xa661(42593)	0x1b99(7 065)
TTL	128	128	128	128	128
Protocol	Tcp(6)	Tcp 6	Tcp(6)	Tcp(6)	Tcp(6)
Port source	49267	54179	57950	59311	50548
Port dest	443	443	9001	443	9054
Stream index	55	24	121	2	2
Numero de sequence	1	1	1	1	1
Flags	0x010 (ACK)	0x010 (ACK)	0x010 (ACK)	0x010 (ACK)	0x010 (ACK)
Window size value	65536	65536	65536	65792	131328
Checksum(tcp)	0xe92f	0x9caa	0x9bd8	0x2d33	0xb43b
RTT to ACK(sec)	0.000255000	0.000270000	0.000218000	0.0038943 52	0.000270 000

Tableau 3-5: Paquet ACK d'une connexion TCP.

- Constatations et remarques :

Après avoir identifié correctement les différents caractères des champs de chaque paquet TCP, on constate que :

- **Identification :** les valeurs changeaient pour chaque paquet, car chaque connexion est identifier d'une manière unique.
- **Port source :** les ports changes dynamiquement, ils sont reliés par l'application en cours sur la machine source.
- **Port destination :** les portschangent d'une application à une autre .Le navigateur Chrome et Firefox utilisent le port 443 (dédié au protocole HTTPS), tandis que le navigateur TOR utilise les ports 9001 et 443 et le port aléatoire 9054.
- **Stream index :** est un mappage interne de Wireshark, qui change d'un paquet à un autre.
- **Checksum TCP :** il protège TCP contre les erreurs de routage, il varie d'un paquet a un autre donc ce n'est pas une référence de comparaison.
- **RTT to ACK :** c'est le temps entre l'émission d'un paquet et la réception de l'ACK correspondant. Il varie d'un paquet à un autre.

b. Etude des étapes de la connexion TLS « protocole d'établissement de connexion SSL handshake »

❖ **Transport Layer Security Protocol :**

Le protocole TLS a été développé principalement pour assurer la confidentialité mais aussi l'intégrité et l'authenticitédes données entre deux applications informatiques communicantes. Il s'agit du protocole de sécurité le plus largement déployé à l'heure actuelle. Il est utilisé pour les navigateurs Web et d'autres applications qui nécessitent l'échange sécurisé de données sur un réseau. Le TLS a évolué à partir du protocole SSL (Secure Sockets Layer) et l'a largement remplacé. Les principales différences entre SSL et TLS qui font de TLS un protocole plus sûr et plus efficace sont l'authentification des messages, la génération de clé et les suites de chiffrement prises en charge, TLS prenant en charge des algorithmes plus récents et plus sûrs [24].

❖ **TLS Handshake Protocol :**

Le protocole TLS Handshake est responsable d'établir la connexion. Nous nous concentrons uniquement sur le TLS authentifié par le serveur et non sur l'authentification mutuelle. Dans une session authentifiée mutuelle, le client présentera également un certificat client pour s'authentifier auprès du serveur [25].

Nous allons maintenant présenter les étapes pour créer une nouvelle session sécurisée avec TLS. Dans le protocole TLS Handshake, nous avons ces étapes :

1. Le client envoie un message « Client hello » au serveur, avec la valeur aléatoire du client et les suites de chiffrement prises en charge.
2. Le serveur répond en envoyant un message "Server hello" au client, accompagné de la valeur aléatoire du serveur.
3. Le serveur envoie son certificat au client pour authentification et peut demander un certificat au client. Le serveur envoie le message "Server hello done".
4. Si le serveur a demandé un certificat au client, le client l'envoie.
5. Le client crée un secret pré-maître aléatoire et le crypte avec la clé publique du certificat du serveur, en envoyant le secret pré-maître crypté au serveur.
6. Le serveur reçoit le secret pré-maître. Le serveur et le client génèrent chacun le secret principal et les clés de session en fonction du secret pré-maître.
7. Le client envoie une notification "Change cipherspec" au serveur pour indiquer que le client commencera à utiliser les nouvelles clés de session pour le hachage et le cryptage des messages. Le client envoie également le message « Client finished ».
8. Le serveur reçoit "Change cipherspec" et bascule son état de sécurité de la couche d'enregistrement sur le chiffrement symétrique à l'aide des clés de session. Le serveur envoie le message « Server finished » au client.
9. Le client et le serveur peuvent désormais échanger des données d'application sur le canal sécurisé qu'ils ont établi. Tous les messages envoyés du client au serveur et du serveur au client sont cryptés à l'aide de la clé de session.

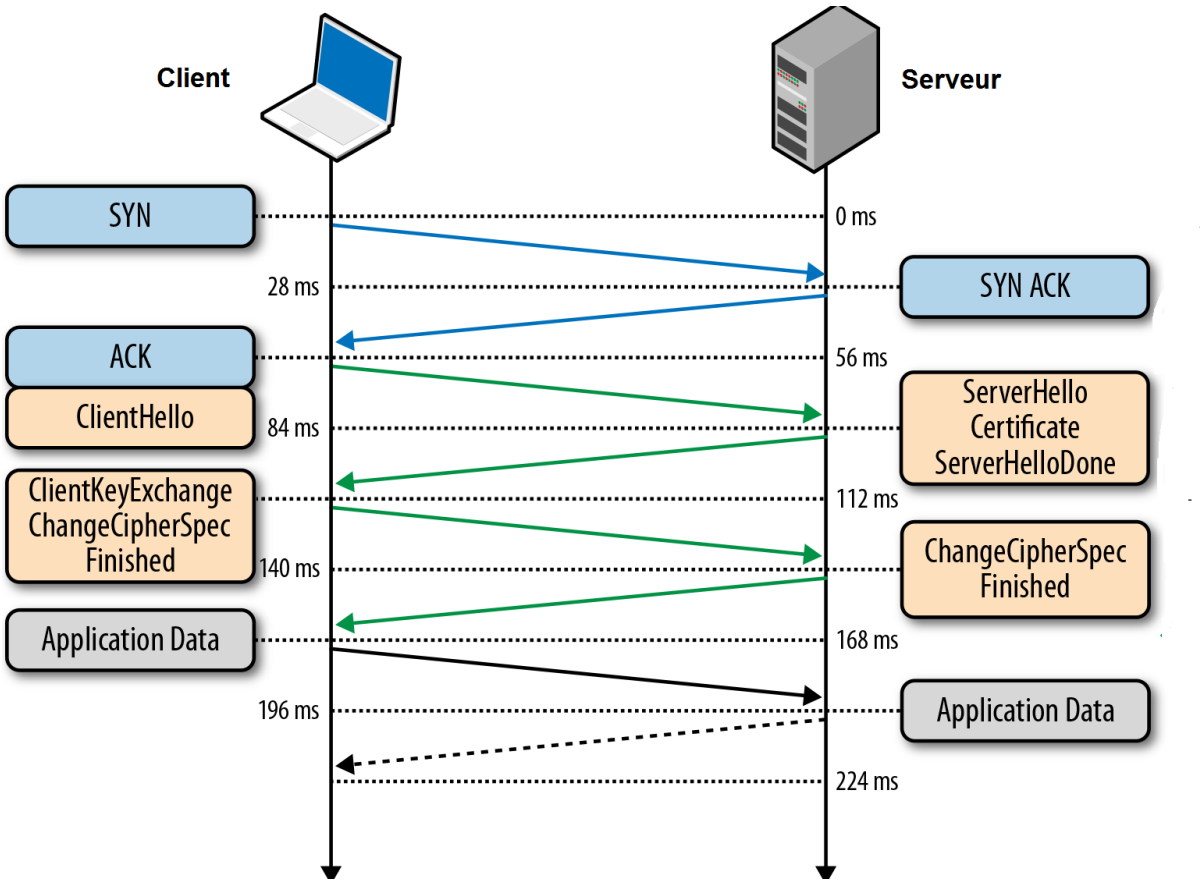

Figure 3.12: *Etapes de la connexion TLS.*

Apres avoir vu le fonctionnement du TLS handshake, on entame l'analyse des captures Wireshark des paquets TLS. On va montrer un exemple d'une connexion SSL du navigateur TOR (port : 9001) avec le nœud de garde (178.63.69.2) et le navigateur Chrome avec le site centos.org (35.178.203.231). Pour une recherche fluide nous allons utiliser les deux filtres :

- ip.addr== 178.63.69.2 &&tls.handshake.
- ip.addr== 81.171.33.201 &&tls.handshake.

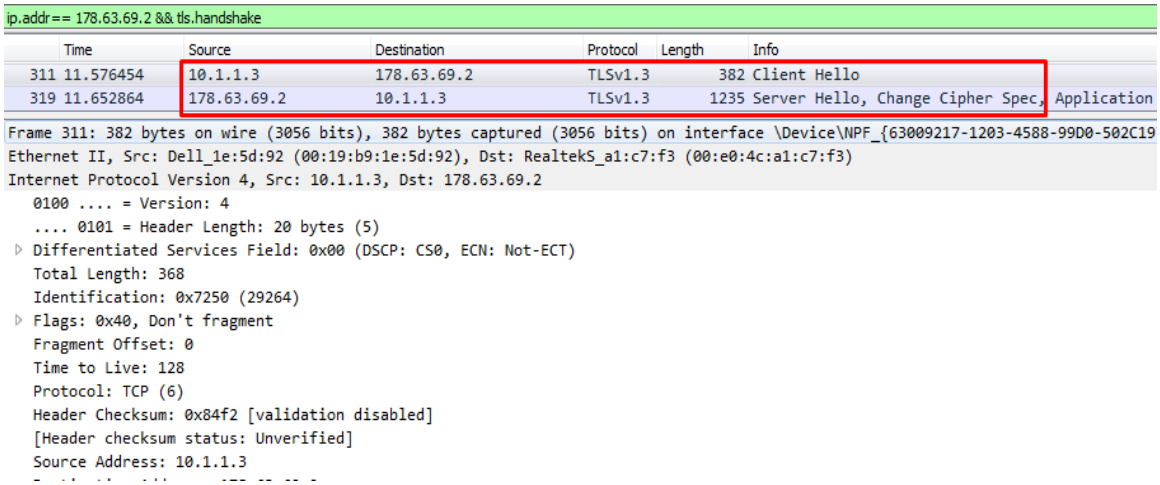

Figure 3.13: *Connexion SSL Handshake entre navigateur TOR et le nœud de garde 178.63.69.2.*

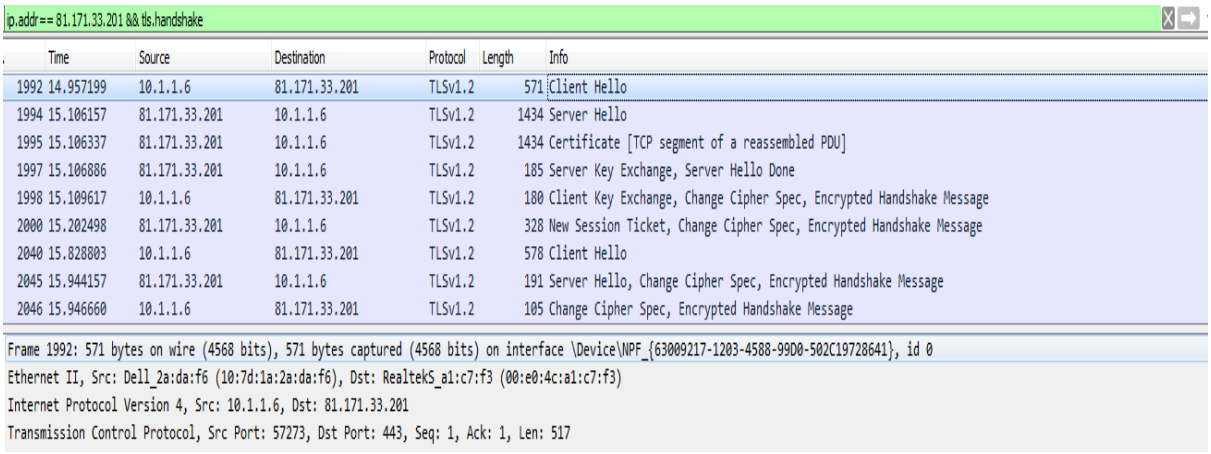

Figure 3.14: *Connexion SSL Handshake entre navigateur Chrome et le site 81.171.33.201.*

Sur cette partie nous allons analyser les paquets échanges lors de l'établissement d'une connexion SSL handshake. On utilise les mêmes captures Wireshark analysé dans la connexion TCP.

- Le navigateur TOR et le premier nœud de garde 178.63.69.2 (port= 9001).
- Le navigateur TOR deuxième nœud de garde 82.223.222.61 (port= 9054 aléatoire).
- Le navigateur TOR et le troisième nœud de garde 116.203.78.147 (port= 443).
- Le navigateur Chrome et le site www.centos.org avec une adresse 81.171.33.201.
- Le navigateur Firefox et le site www.centos.org avec une adresse 81.171.33.202.

❖ **Comparaison entre l'analyse du navigateur TOR et les navigateurs Chrome et Firefox :**

➢ **Client hello :**

Les différences dans le premier paquet client hello de la connexion SSL sont :

1. **La longueur totale (length)** : la longueur totale du paquet client hello émise par le navigateur Tor dans les trois différents types de nœud de garde est largement inferieure par rapport à celle du paquet client hello émise par les deux navigateurs Chrome et Firefox qui est fixe à 512, tandis que la longueur du paquet Tor varie entre 314 et 331.

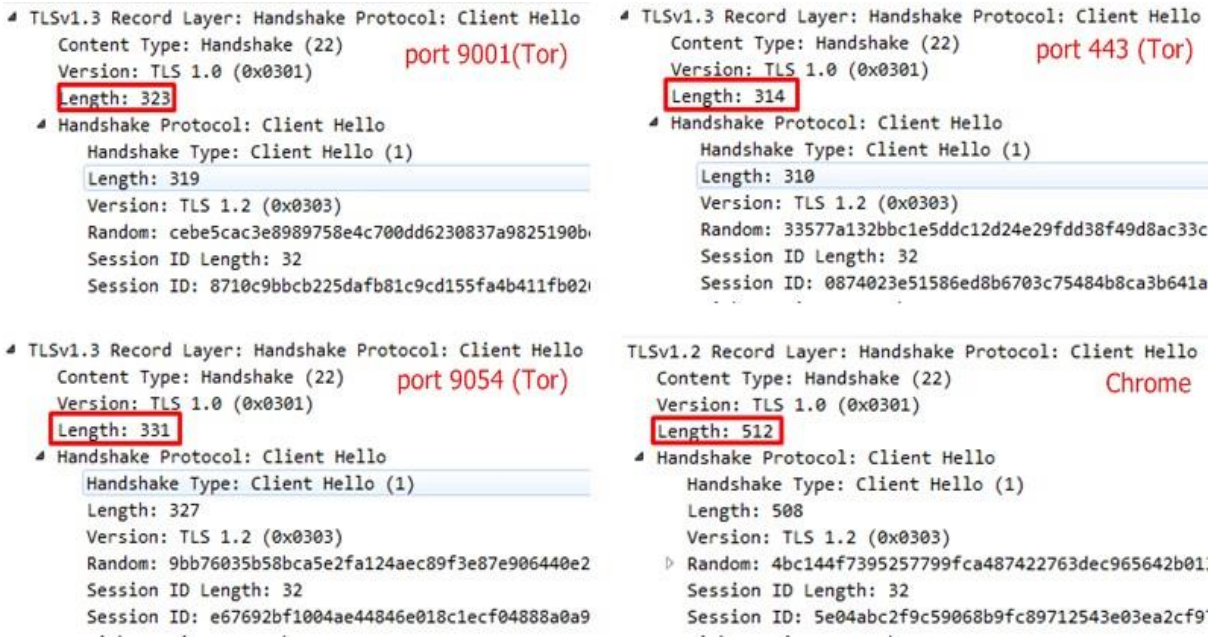

Figure 3.15: La longueur totale du paquet client hello émise par les navigateurs.

2. **Cipher suites :** le navigateur Chrome contient 16 suites de chiffrement, le navigateur Firefox et le navigateur Tor contiennent 18 suites de chiffrements. D'où on va comparer et extraire les différentes suites de chiffrement de ses trois derniers. On déduit que : le navigateur Tor contient 18 suites de chiffrements dans un ordre bien précis pour chaque communication avec les trois nœuds de gardes.

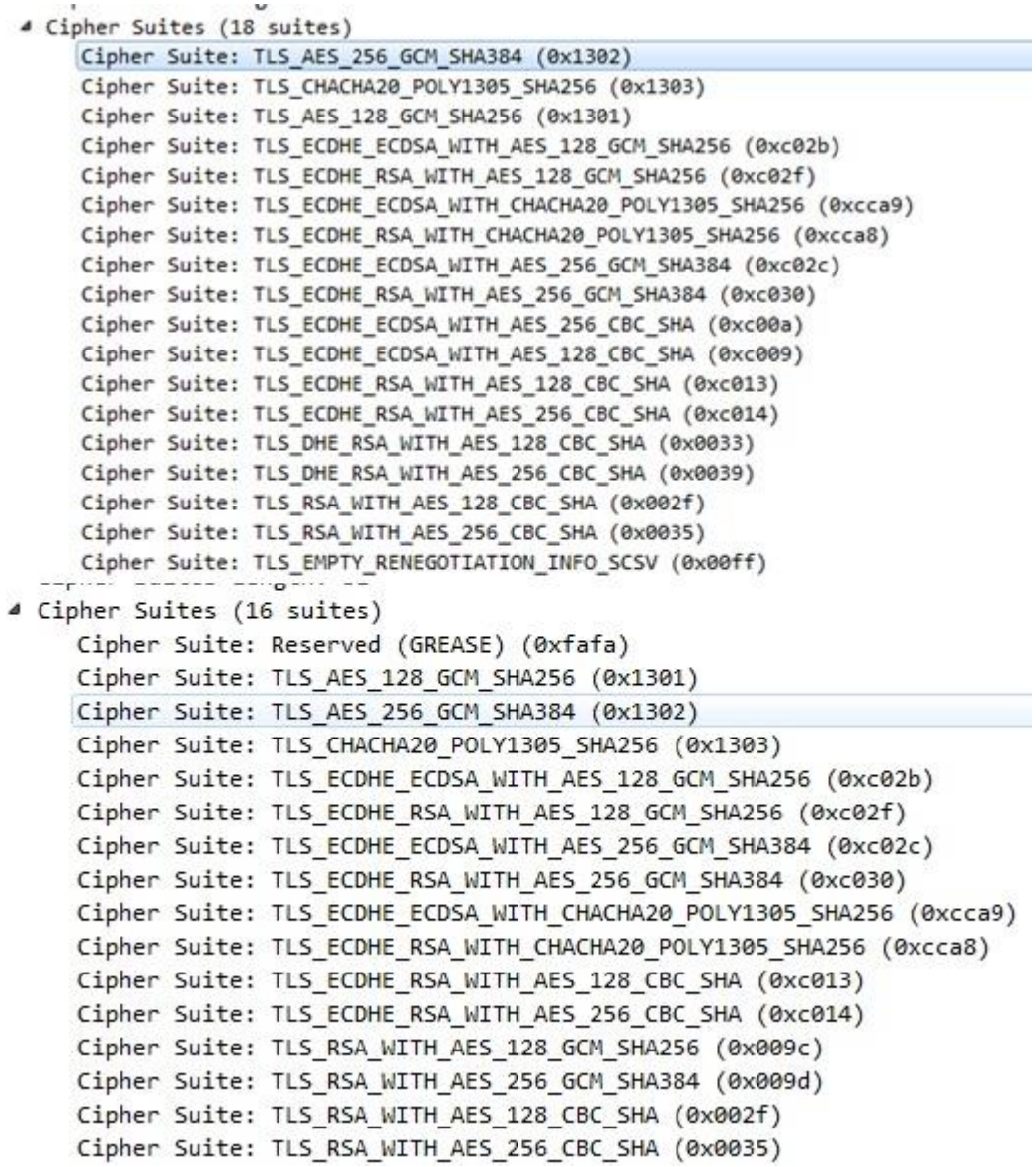

Figure 3.16: Les suites de chiffrements appartenant au navigateur TOR et le navigateur Chrome.

En revanche le navigateur TOR contient 5 suites de chiffrements différentes par rapport aux navigateurs Chrome et Firefox.

Suites de chiffrements du navigateur TOR
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(0xc00a)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(0xc009)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0x0033)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA(0x0039)
TLS_EMPTY_RENEGOTIATION_INFO_SCSV(0x00ff)

Tableau 3-6: *Les suites de chiffrement unique pour le navigateur Tor.*

3. **Les extensions :** Le navigateur contient plusieurs extensions. Pendant la poignée de main, le client indique quelles extensions il prend en charge (dans le message client hello), et le serveur choisit les extensions à utiliser. En basant sur les captures de Wireshark, on remarque que le navigateur Tor utilise 10 extensions, Chrome utilise 18 extensions, et Firefox utilise 15 extensions comme montre les figures ci-dessous.

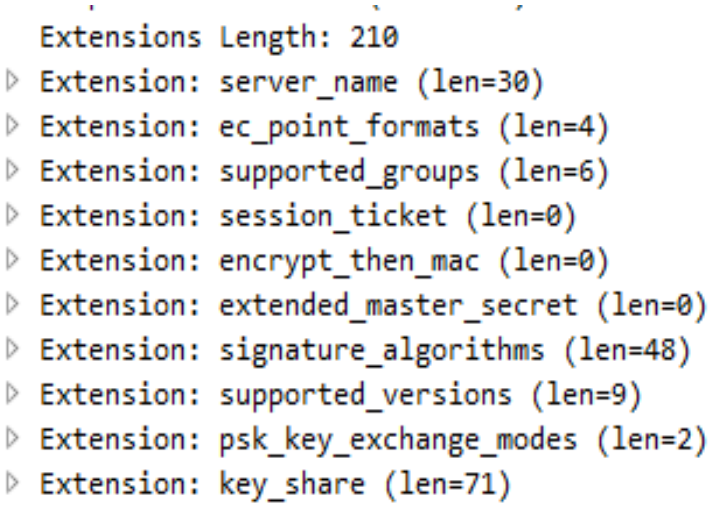

Figure 3.17:*Les extensions du navigateur Tor.*

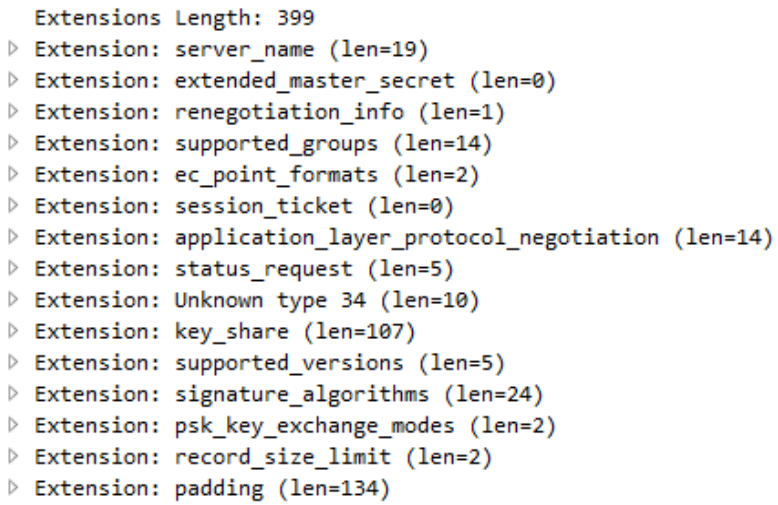

Figure 3.18: *Les extensions du navigateur Firefox.*

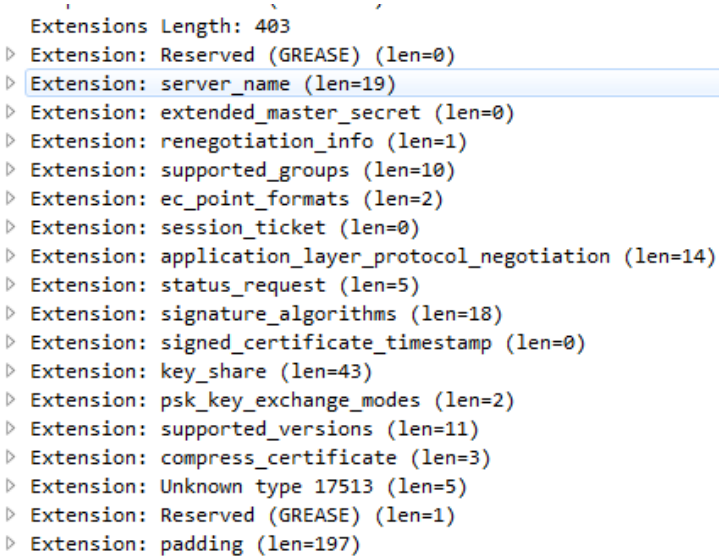

Figure 3.19: *Les extensions du navigateur Chrome.*

On déduit que :

- **Extension lenght** : la valeur de l'extension du navigateur Tor est entre 201 et 218 qui est inferieur par rapport à l'autre navigateur. On remarque aussi qu'ils partagent entre eux les mêmes extensions.

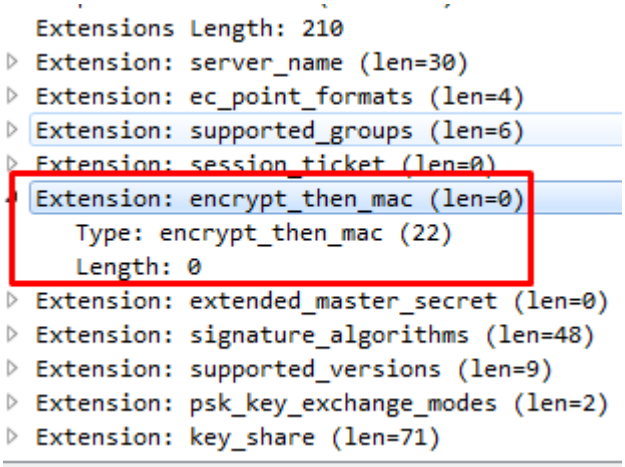

Figure 3.20: L'extension unique pour TOR.

- TLS utilise une construction **encrypt_then_mac** qui était considérée comme sécurisée au moment où le protocole Secure Socket Layer (SSL) d'origine a été spécifié, mais qui n'est plus considérée comme sécurisée.

- Cette construction, telle qu'elle est utilisée dans TLS a fait l'objet de nombreuses vulnérabilités et attaques de sécurité s'étendant sur une période de plusieurs

années.La valeur **"extension_type"** pour cette extension est de 22 (0x16), et le champ **"extension_data"** de cette extension est vide.

4. **Extension«server_name» :** Il s'agit d'une extension du protocole TLS utilisé en HTTPS. Cette extension vous permet de spécifier le nom d'hôte ou le nom de domaine du site Web lors de l'ouverture d'une connexion HTTP pendant la poignée de main TLS plutôt qu'après la poignée de main.

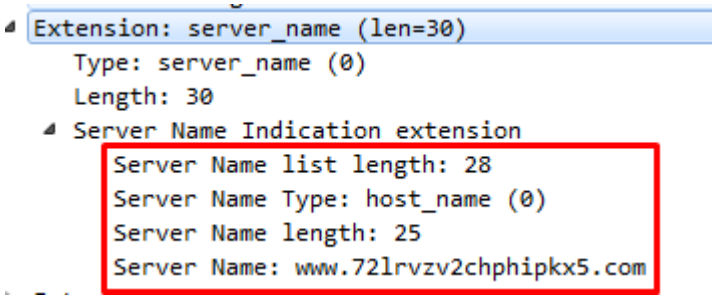

Figure 3.21: *Extension server_name du navigateur Tor.*

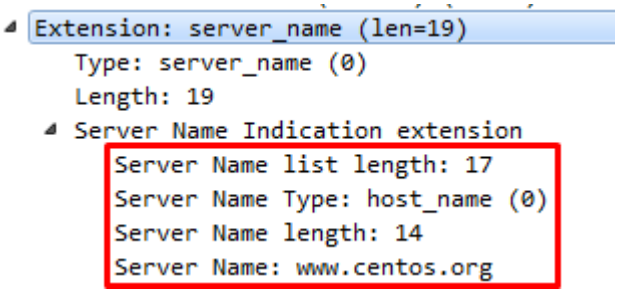

Figure 3.22:*Extension server_name du navigateur Chrome.*

Nous allons vérifier si le nom de domaine affiché par le navigateur Tor existe avec la commande**: nslookup www.72lrvzv2chphipkx5.com**

```
C:\Windows\system32>nslookup  www.72lrvzv2chphipkx5.com
Serveur :   UnKnown
Address:  192.168.1.1

*** UnKnown ne parvient pas à trouver www.72lrvzv2chphipkx5.com : Non-existent d
omain

C:\Windows\system32>nslookup www.centos.org
Serveur :   UnKnown
Address:  192.168.1.1

Réponse ne faisant pas autorité :
Nom :    www.centos.org
Addresses:  2a05:d01c:c6a:cc02:e4d3:88b0:60da:6fb4
          2001:4de0:aaae::202
          2001:4de0:aaae::201
          35.178.203.231
          81.171.33.202
          81.171.33.201
```

Figure 3.23: *Nom de domaine délivré par le navigateur Tor.*

5. **Extension « signature_algorithms » :** cette extension contient les algorithmes de hachagesupportésparlenavigateur.
   LenavigateurTorcontient23algorithmes,lenavigateurChromecontient8algorithmes etlenavigateur Firefox contient 11algorithmes.

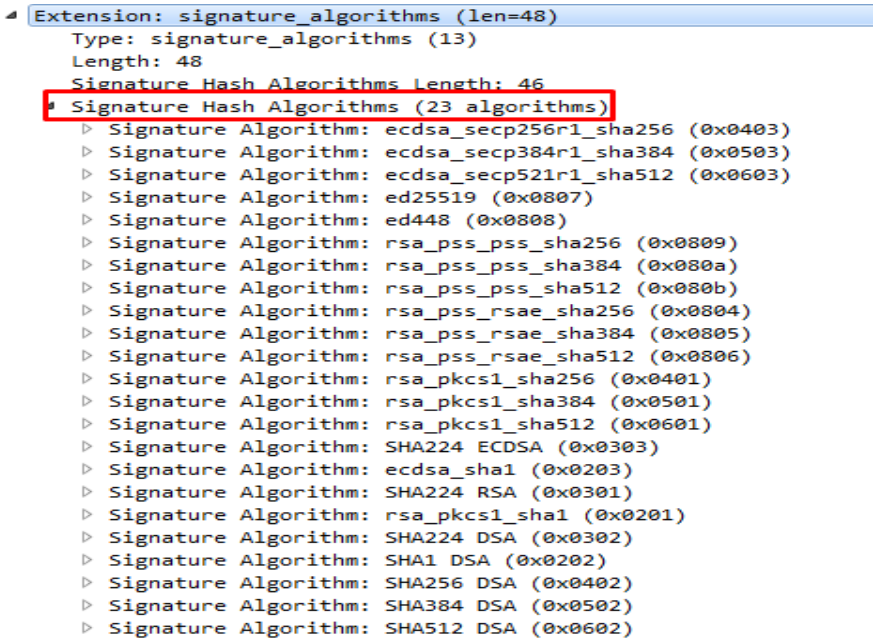

Figure 3.24: *Extension signature_algorithms envoyée par le navigateur Tor.*

Figure 3.25: *Extension signature_algorithms envoyée par les navigateurs.*

6. **Extension « supported_groups » :** Pour les clients, les groupes sont envoyés à l'aide de l'extension supported_groups. Pour les serveurs, il est utilisé pour déterminer le groupe à utiliser. Ce paramètre affecte les groupes utilisés pour les signatures et l'échange de clés .Le premier groupe répertorié sera également

utilisé pour le partage de la clé envoyé par un client dans un client hello. Le navigateur Tor contient 2 groupes, le navigateur Firefox contient 6 groupes et le navigateur Google Chrome a 4 groupes. Et on remarque aussi que la taille du navigateur Tor est inférieure aux autres.

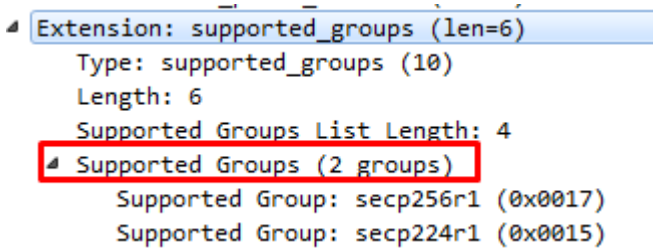

Figure 3.26: Extension supported_groups envoyée par le navigateur Tor.

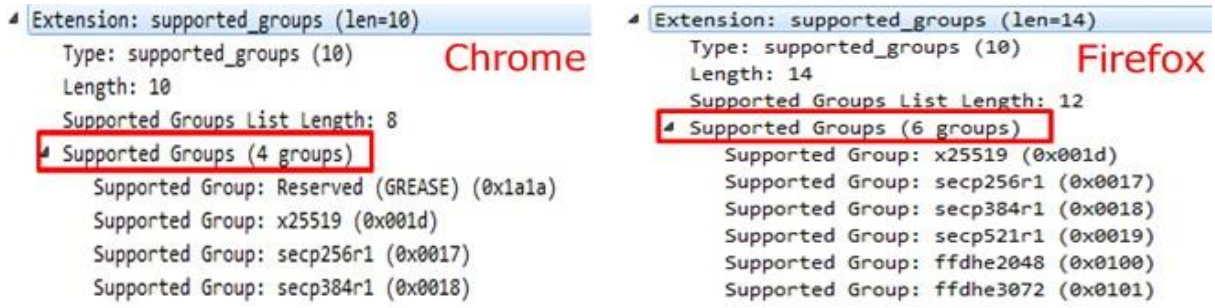

Figure 3.27: *Extension supported_groups envoyé par les navigateurs.*

- **Server hello :**

Les différences les plus apparentes dans le premier paquet server hello de la connexion SSL sont :

1. En analysant les paquets du navigateur Tor venant des trois nœuds de garde et les paquets des navigateurs Chrome et Firefox venant du site centos.org, on remarque que les informations du server hello des trois nœuds de garde sont identique d'où on va prendre port 9001 comme référence, de même pour Chrome et Firefox.

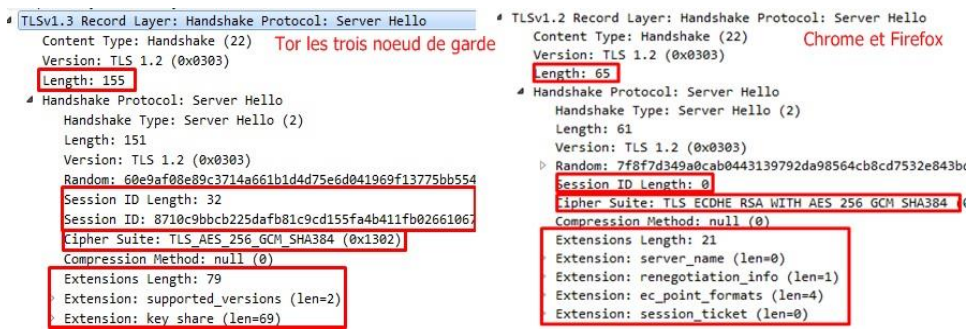

Figure 3.28: *Le paquet server hello de Tor et les navigateurs.*

2. **La longueur totale** dans les paquets du navigateur Tor , cette longueur est supérieure à celle des deux navigateurs Chrome et Firefox.
3. Lepaquetserverhellodu navigateurTor contientl'information**«Sessionid»**.
4. Session id length contient la valeur 0 pour les navigateurs Chrome et Firefox, et une valeur de 32 pour le navigateur Tor.
5. Les extensions utilisées par le navigateur Tor sont :**« supported_version »** et **« key_share ».** Les autres navigateurs contiennent 4 extensions différentes.
6. Les suites de chiffrements choisies par les serveurs sur les navigateurs sont :
   - TLS_AES_256_GCM_SHA384 pour le navigateur Tor.
   - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 pour Chrome et Firefox.

TLS_AES_256_GCM_SHA384 : cette suite contient pas mal d'informations sur les techniques de cryptage et de chiffrement. Elle est traduite par l'utilisation de TLS, de AES_256 cryptage symétrique, ce qui signifie qu'il crypte et décrypte les données, il utilise une clé cryptographique spécifique, qui est effectivement un ensemble de protocoles pour masquer les informations. Cette clé a une taille de 256 bits, SHA384 pour la vérification de l'intégrité des données

❖ **Constations :**

A partir de nos comparaisons et analyses effectuées du protocole TLS nous avons distingué plusieurs différences qui peuvent identifier l'utilisation du navigateur Tor. Pour cela nous allons utiliser ses différences pour extraire le maximum d'empreintes numérique.

3.5 Réseau I2P

Après le téléchargement et l'installation de I2P (voici un guide pour le télécharger : https://geti2p.net/en/download) et quand on clique sur 'Terminer' dans la dernière fenêtre de l'installation, trois icones seront créés dans le bureau du Pc.

3.5.1 Lancement du réseau

Il suffit de cliquer sur l'icône « Start I2P (Restartable) », cela démarre le réseau i2p avec la console CMD (command terminal). Après l'initialisation d'I2P, il ouvre automatiquement une fenêtre du navigateur 'internet explorer' qui affiche la page 'Home'.

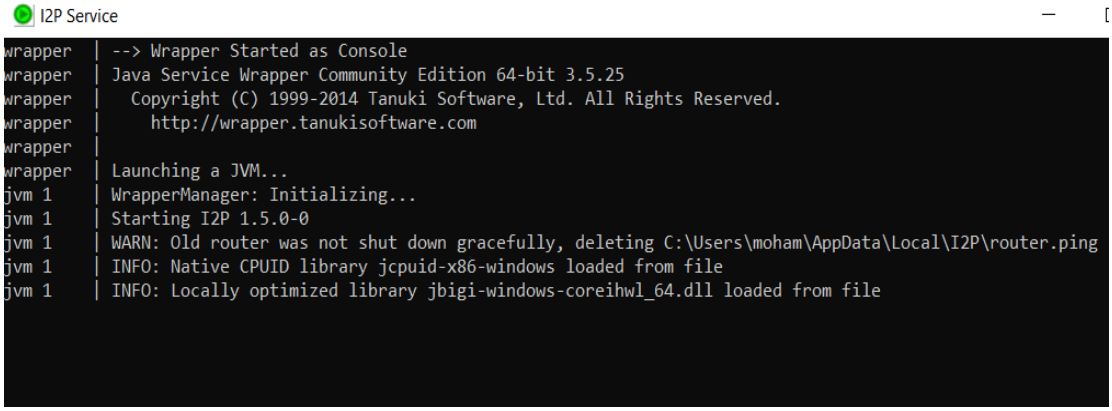

Figure 3.29: *Lancement d'I2P à partir de la console CMD.*

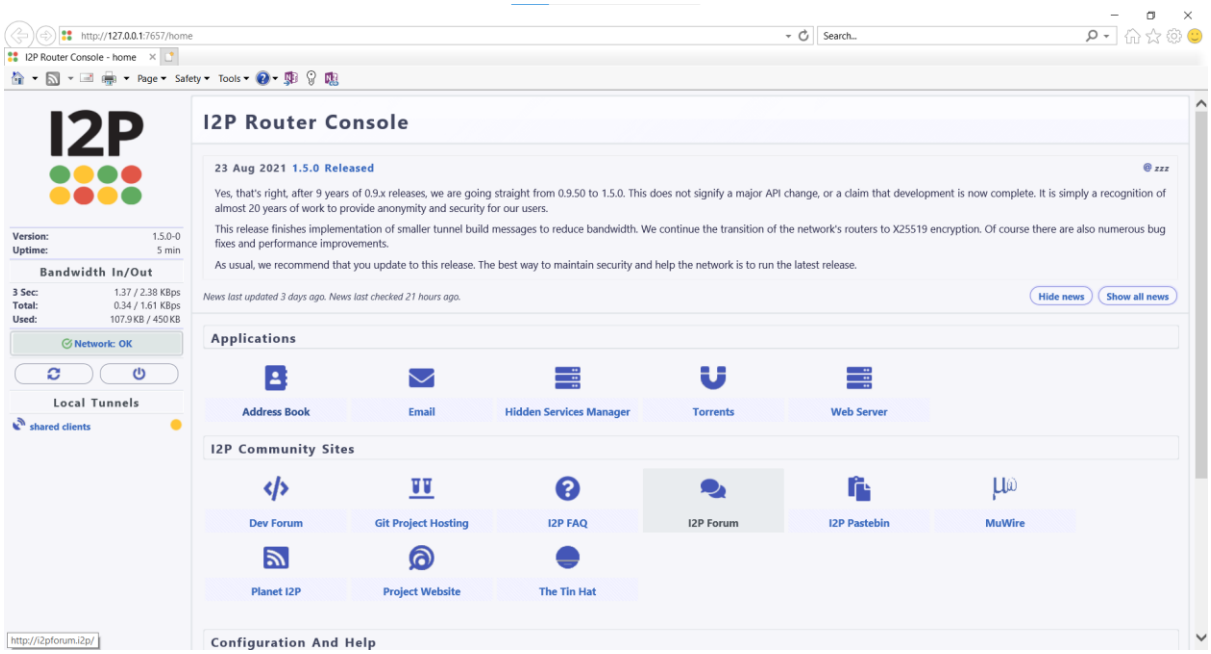

Figure 3.30: *Page d'accueil d'I2P.*

3.5.2 Configuration de navigateur « Mozilla Firefox » pour naviguer sur les eepsites

La navigation sur les eepsites se fait par l'utilisation d'un proxy et nous devons activer ce proxy à chaque fois nous voulons naviguer sur ces eepsites, et désactiver le proxy lors de la navigation des sites web normal.

Dans notre projet nous allons utiliser le navigateur Firefox car il est recommandé de l'utiliser par les fondateurs d'I2P.

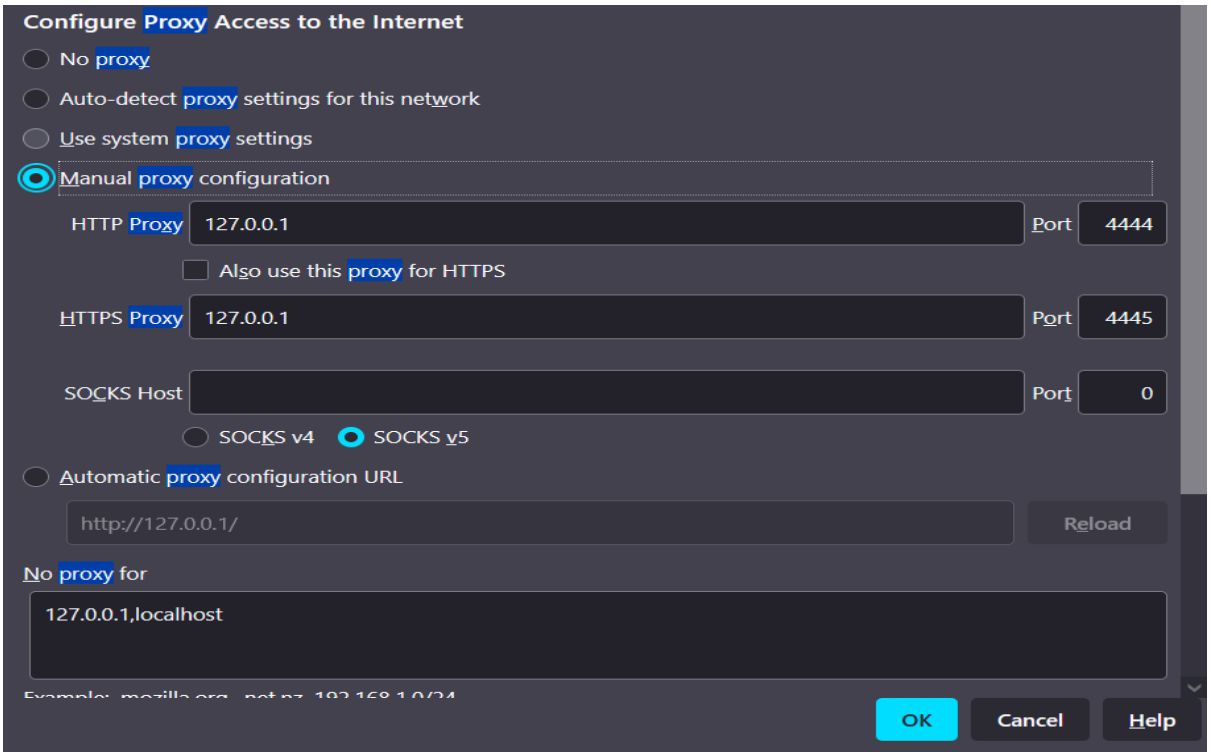

Figure 3.31: *Configuration proxy Firefox pour I2P.*

Nous allons visiter quelques sites d'I2P :

a. I2pforum.i2p :

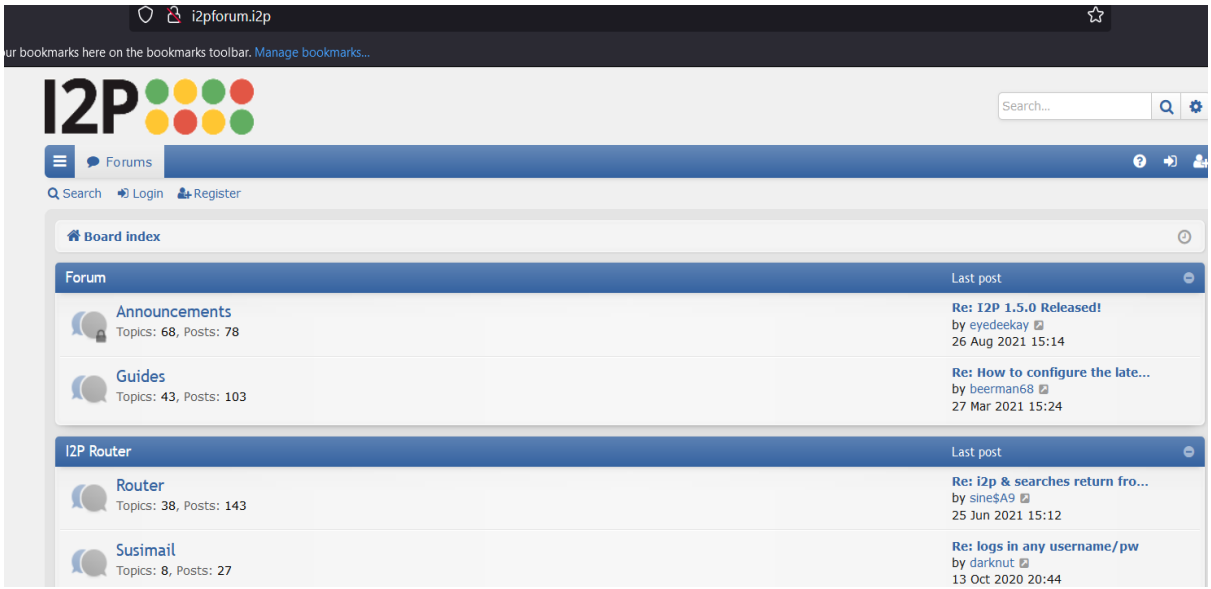

Figure 3.32: *I2pforum.i2p.*

b. Identiguy.i2p :

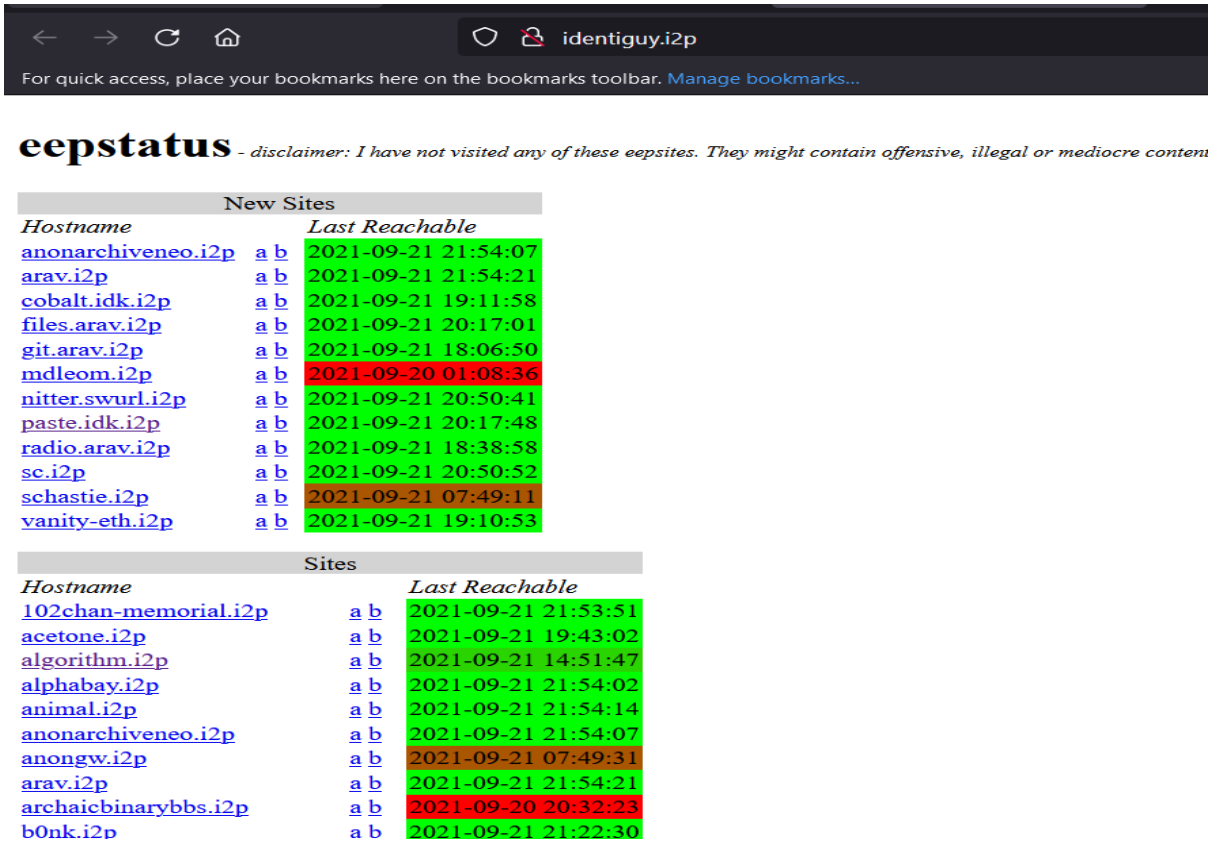

Figure 3.33: *Identiguy.i2p.*

c. I2PTunnel :

I2PTunnel est un outil d'interfaçage et de fourniture de services sur I2P. La destination d'un I2PTunnel peut être définie à l'aide d'un nom d'hôte, Base32 ou d'une clé de destination complète de 516 octets. Un I2PTunnel sera disponible sur votre machine cliente en tant que localhost:port : (localhost:7657/i2ptunnel/).

Il existe plusieurs tunnels sur i2p, voici deux qui nous intéressent le plus :

- **I2P HTTP Proxy :** (127.0.0.1 :4444) un mandataire HTTP utilisé pour naviguer le Web ordinaire à travers i2p et pour cela i2p utilise des mandataires sortants comme l'outproxy qui se trouve dans le carnet d'adresses d'i2p « false.i2p ».(un lien vers le site d'I2P pour comprendre comment fonctionne le carnet d'adresses : https://geti2p.net/en/docs/naming)

Figure 3.34: *I2P HTTP Proxy.*

- **I2P HTTPS Proxy :** (127.0.0.1 :4445) un mandataire HTTP utilisé pour naviguer le web ordinaire à travers i2p et pour cela i2p utilise des mandataires sortants comme l'outproxy par défauts de https dans i2p « outproxy-tor.meeh.i2p » est relié avec Tor.

Figure 3.35: *I2P HTTPS Proxy.*

d. Mandataire sortant false.i2p :

La configuration par défauts d'I2P HTTP Proxy utilise un mandataire sortant « false.i2p » pour sortir vers le web normal malgré qu'i2p n'est pas conçu pour être utilisé comme proxy pour l'Internet ordinaire. Quoi que rien est garanti sur false.i2p pour qu'il soit toujours en marche car il ne s'agit pas d'un service officiel d'I2P.

Aprèsavoirdémarré lesservicesI2PTunnel, Nous allonsutiliser l'outproxy « false.i2p »pourcontournerleproxyetyaccéderauxsitesinterdis.

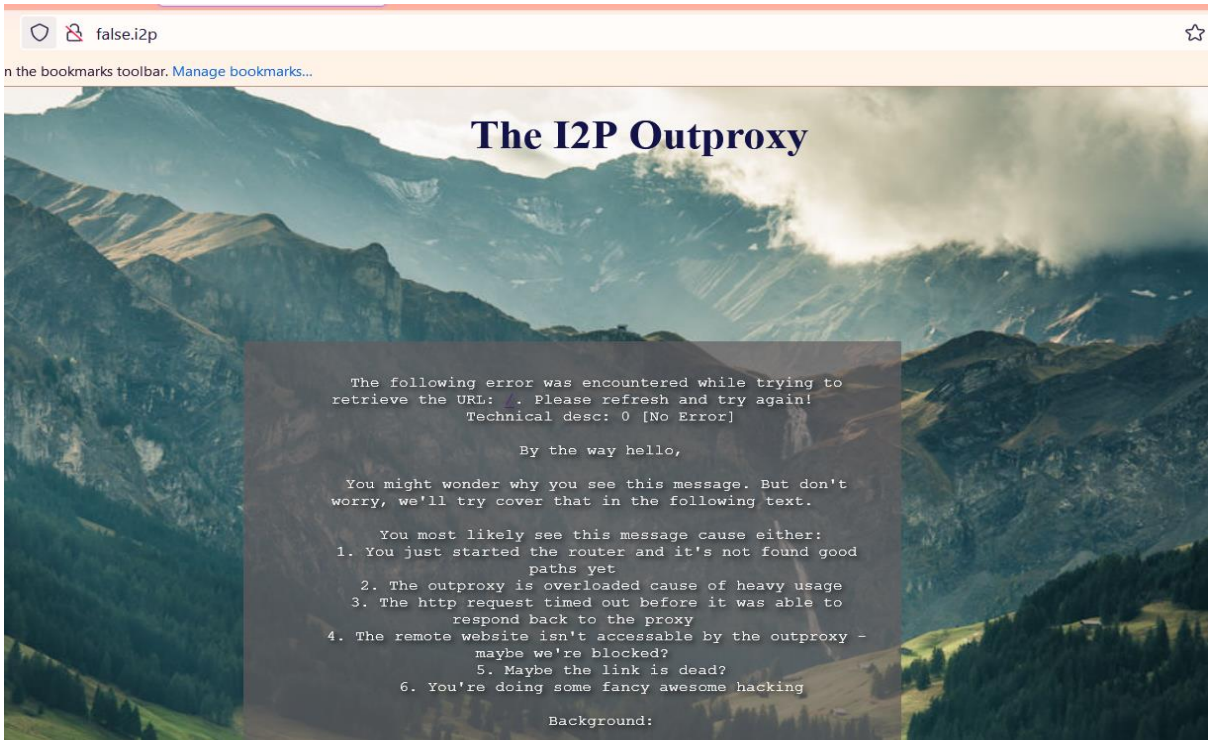

***Figure 3.36**: Mandataire sortant false.i2p*

Remarque :Au cours des mois précédents, lorsque nous étions dans les expériences, false.i2p ne fonctionnait pas, nous avons donc dû chercher un autre mandataire sortant, En cherchant un autre, nous avons trouvé un article sur le site bien connu « Reddit.com ». Cet article parle d'un nouveau mandataire sortant « purokishi.i2p » et explique comment nous pouvons ajouter cette destination à notre carnet d'adresses.

Nouveau service d'outproxy I2P : purokishi.i2p

Il s'agit d'un nouveau service géré par des bénévoles pour fournir un proxy externe fonctionnel et rapide aux utilisateurs I2P. Afin de fournir les meilleures performances possibles, le proxy externe est configuré pour s'exécuter à l'aide du nouveau cryptage ECIES-X25519 introduit avec la version I2P 0.9.45, et s'efforce de bloquer les publicités et autres contenus indésirables.

Sur le site « Reddit.com » : voici un lien vers la publication :

«https://www.reddit.com/r/i2p/comments/hcezcq/new_i2p_outproxy_service_purokishii2p/»

Après l'ajout de ce mandataire sortant à notre carnet d'adresse nous avons pu accéder à « http://outproxy.purokishi.i2p/ »

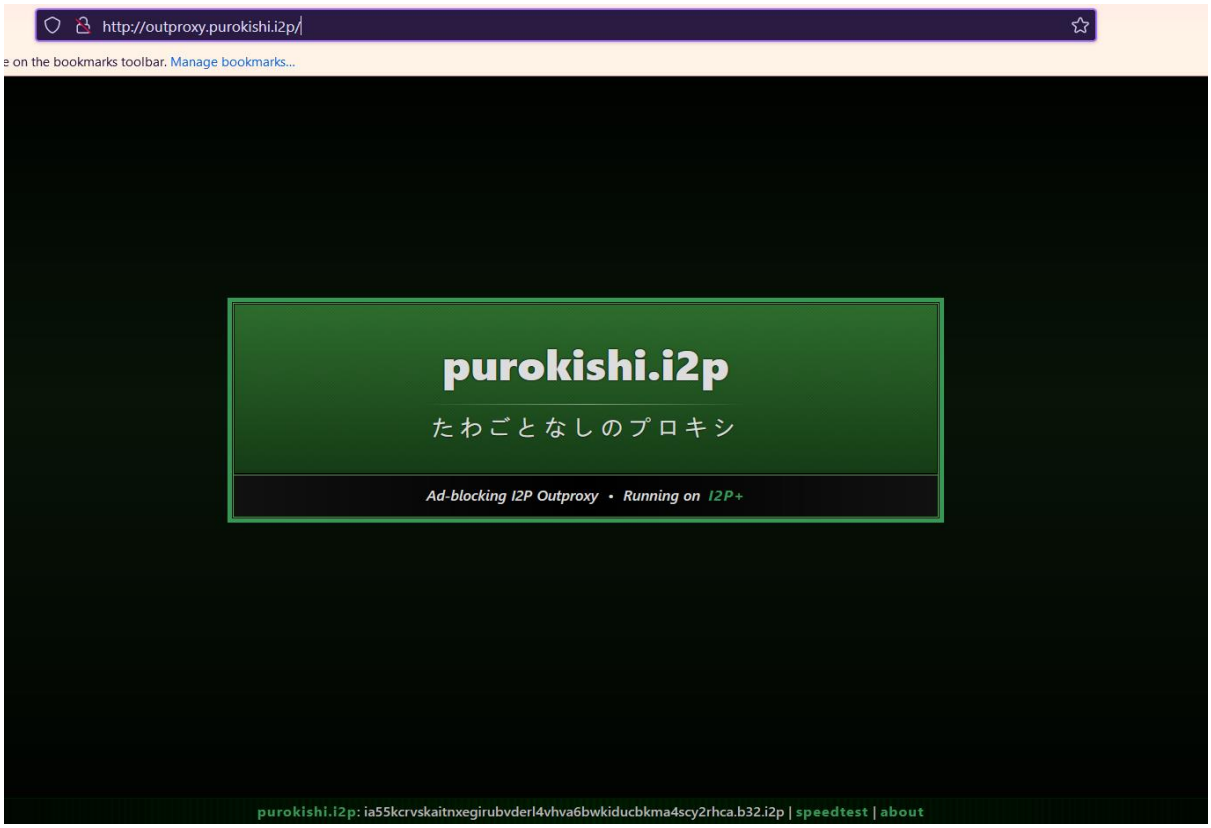

Figure 3.37: *Interface de mandataire sortant « http://outproxy.purokishi.i2p/ »*

Puisquel'outproxyfonctionnebiennousallonsl'utiliserpourcontournerle proxydu serveur et visiter les sitesWebinterdis.

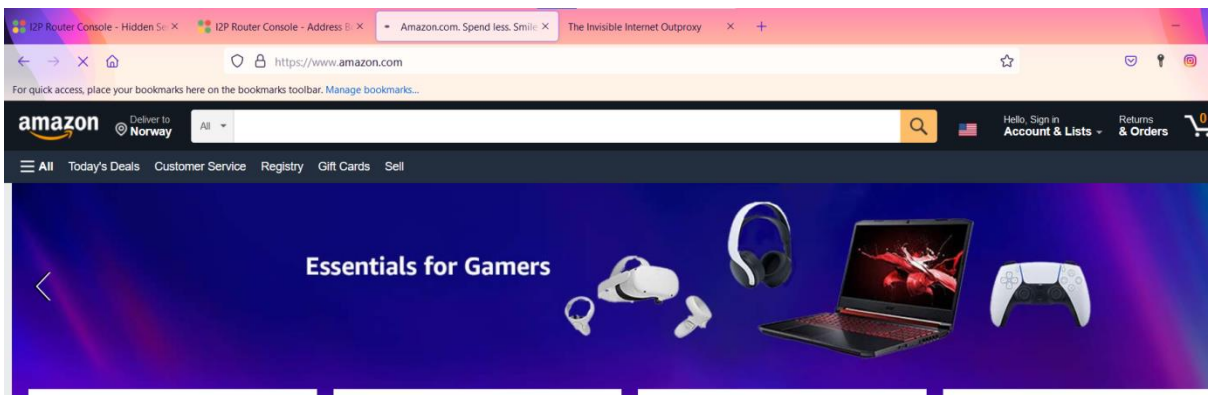

Figure 3.38: *Accès à "amazon.com" avec le mandataire sortant d'I2P.*

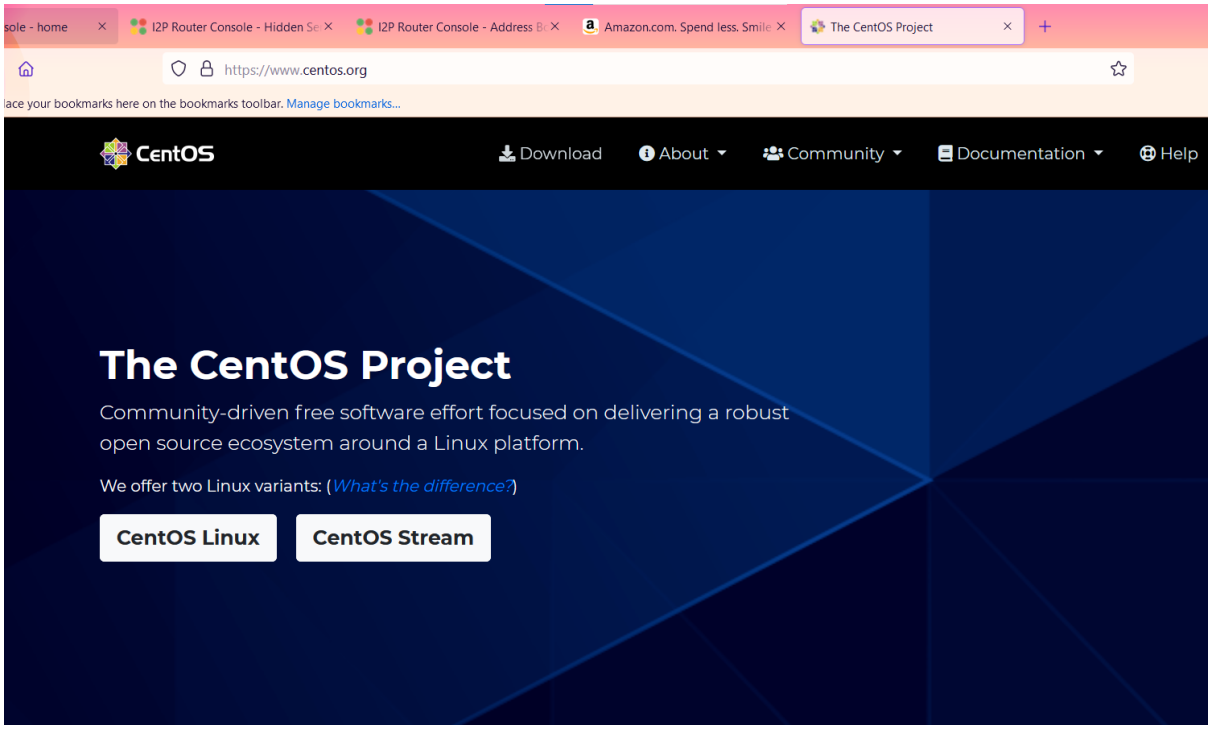

Figure 3.39: *Accès à "centos.org" avec le mandataire sortant d'I2P.*

3.5.3 Phase d'analyse du réseau « I2P »

3.5.3.1 Extraction des signatures du réseau I2P

a. Pool.ntp.org

Le projet pool.ntp.org est une grappe virtuelle de serveurs de temps qui permet de fournir à un grand nombre de clients, une source de temps NTP facile à utiliser.

Cette grappe de serveurs est utilisée par des centaines de millions de systèmes à travers le monde. Ces serveurs de temps sont utilisés dans la plupart des grandes distributions Linux et dans de nombreux équipements réseau.

Le Network Time Protocol (NTP) est utilisé depuis plusieurs décennies pour synchroniser les horloges des ordinateurs dans les réseaux à commutation de paquets et à latence variable. Le logiciel client pour NTP est intégré à de nombreux systèmes d'exploitation et appareils Internet, et les serveurs NTP du monde entier reçoivent désormais plusieurs milliards de demandes de synchronisation par jour.

Le NTP est généralement considéré comme une source de temps « marchande », et non comme un véhicule de haute précision pour le transfert de temps. Cela est principalement dû au fait que la plupart des utilisateurs de NTP utilisent l'Internet public, généralement dans le

but de synchroniser l'horloge de leur ordinateur à la seconde entière la plus proche, un objectif qui est facilement atteint.

Quand I2P démarre il contacte le DNS Google pour chercher un pool.ntp.org :

- D'abord, il essaie de contacter un serveur en Algérie avec trois serveurs différents qui sont : « 0.dz.pool.ntp.org », « 1.dz.pool.ntp.org » et « 2.dz.pool.ntp.org »

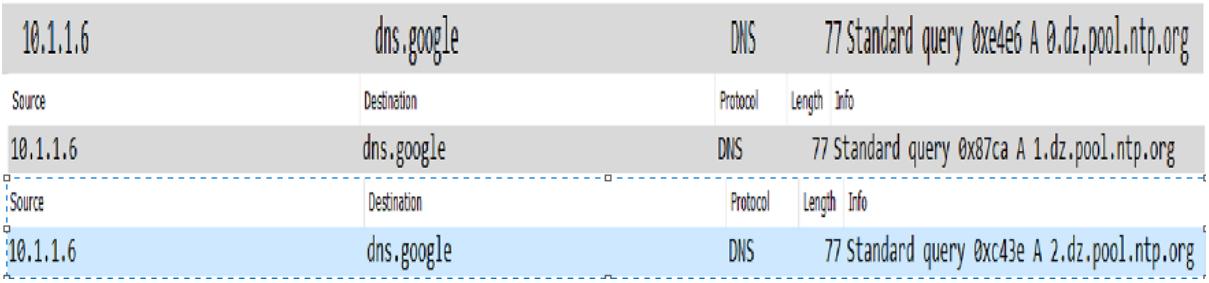

Figure 3.40: *I2P contacte le DNS Google pour un serveur NTP dans l'Algérie.*

Figure 3.41: *0 serveurs NTP Algérie.*

- Le client I2P contacte le DNS encore une fois pour avoir le plus proche serveur NTP, dans ce cas il va faire une requête a « 1.africa.pool.ntp.org » et « 2.africa.pool.ntp.org »

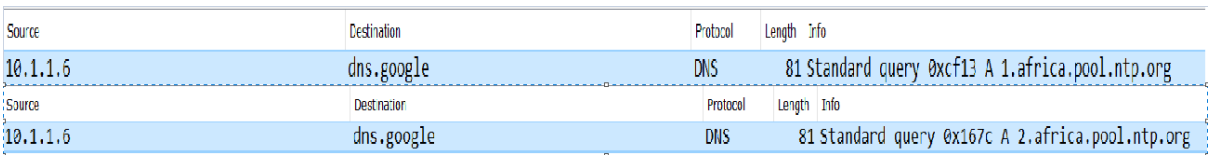

Figure 3.42: *Requête vers le serveur NTP « Afrique ».*

Remarque : Dans le site officiel « https://www.ntppool.org/zone/africa » il existe 4 serveurs NTP. (Donc I2P peut contacter les deux autres si les deux premiers seront en pannes.

Figure 3.43: *4 serveurs NTP pour le continent Afrique.*

Dans notre projet, après la réponse du serveur DNS le routeur I2P a choisi l'adresse « 2.africa.pool.ntp.org » pour contacter le serveur NTP, le serveur NTP lui répond. Ceci va synchroniser l'heure interne d'I2P.

Nous remarquons dans la figure 3.45 que le routeur I2P envoie unerequête de type client au serveur NTP du « africa.pool.ntp.org », ce dernier lui répond avecune requête de type serveur, celui-ci lui retourne l'heure courante. On peut voir aussi que leprotocoleNTP utilisele port 123.

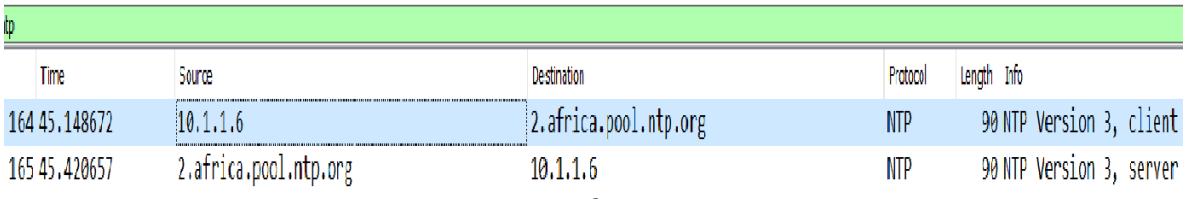

Figure 3.44: *Requête/Réponse client, serveur NTP.*

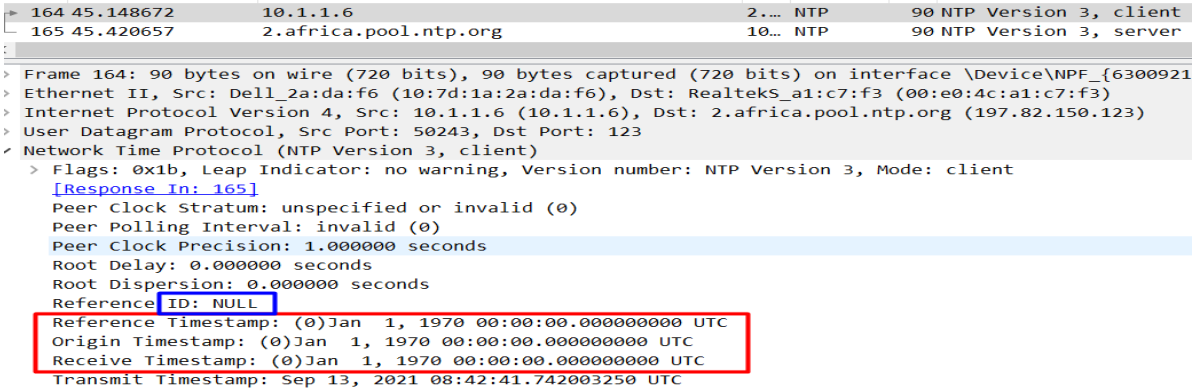

Figure 3.45: *L'heure de client n'est pas synchronisée.*

On remarque que l'heure de client qui a un Id nul n'est pas synchronisée.

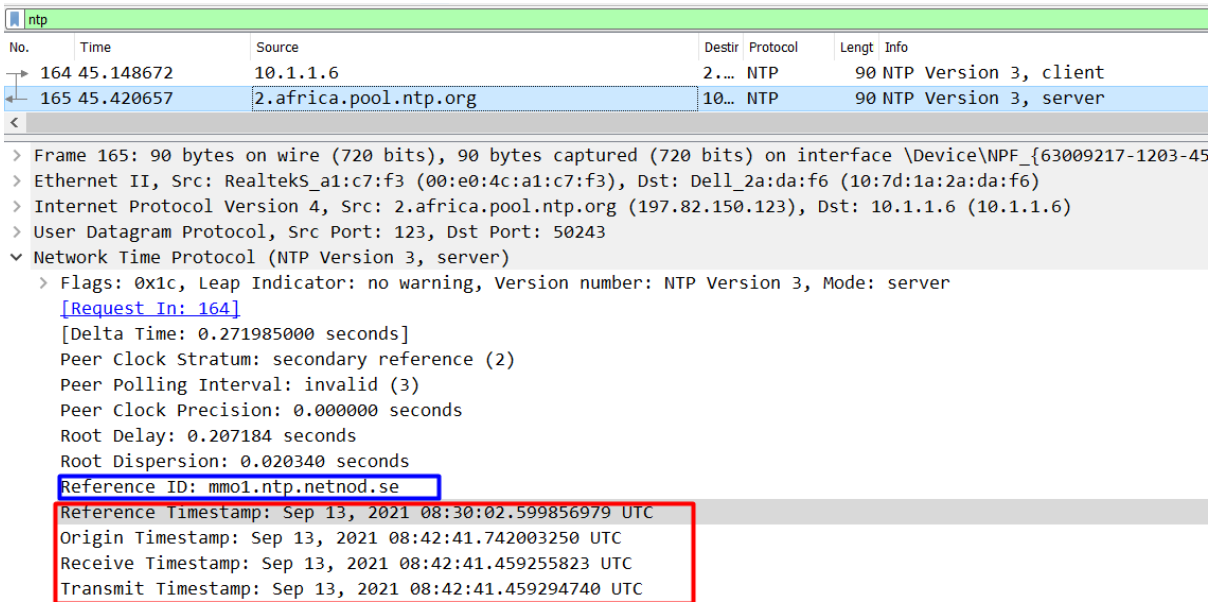

Figure 3.46: *Le serveur synchronise l'heure.*

On remarque que le serveur qui a un Id « mm01.ntp.netnod.se » synchronise l'heure.

b. SSDP

SSDP (Simple Service Discovery Protocol) Une norme pour la publicité des services sur un réseau TCP/IP et leur découverte. Le protocole Universal Plug and Play (UPnP) utilise SSDP pour annoncer et rechercher des périphériques afin, par exemple, de diffuser de la vidéo d'une source vers un système de lecture.

La description des services renvoyés à partir d'une requête SSDP peut inclure une URL qui fournit des informations supplémentaires. Les requêtes et les réponses SSDP sont transférées dans des paquets UDP plutôt que dans le TCP plus fiable.

SSDPeffectuedesannoncespériodiquesNOTIFY oudesrequêtesdedécouvertesM-SEARCH.CesannoncesetrequêtessontlimitéesauLANetsontbaséessurdeséchangesHTTPMU (HTTPsurUDPenmulticast).Legroupe«multicast»utiliséest «239.255.255.250»etleportUDPest«1900».

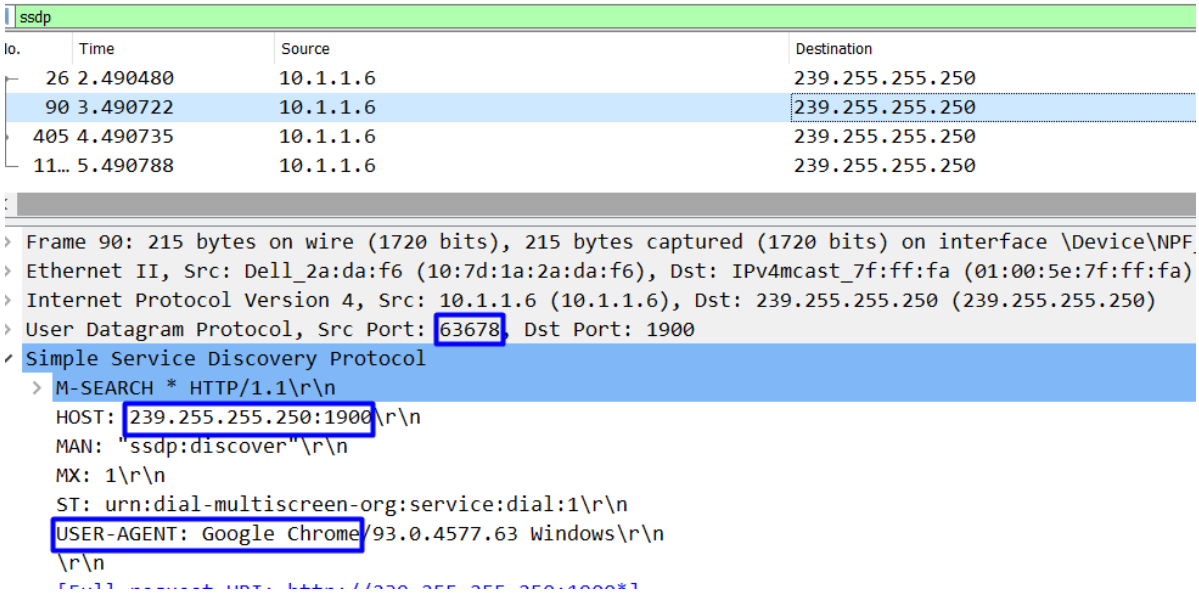

Figure 3.47: *SSDP Chrome.*

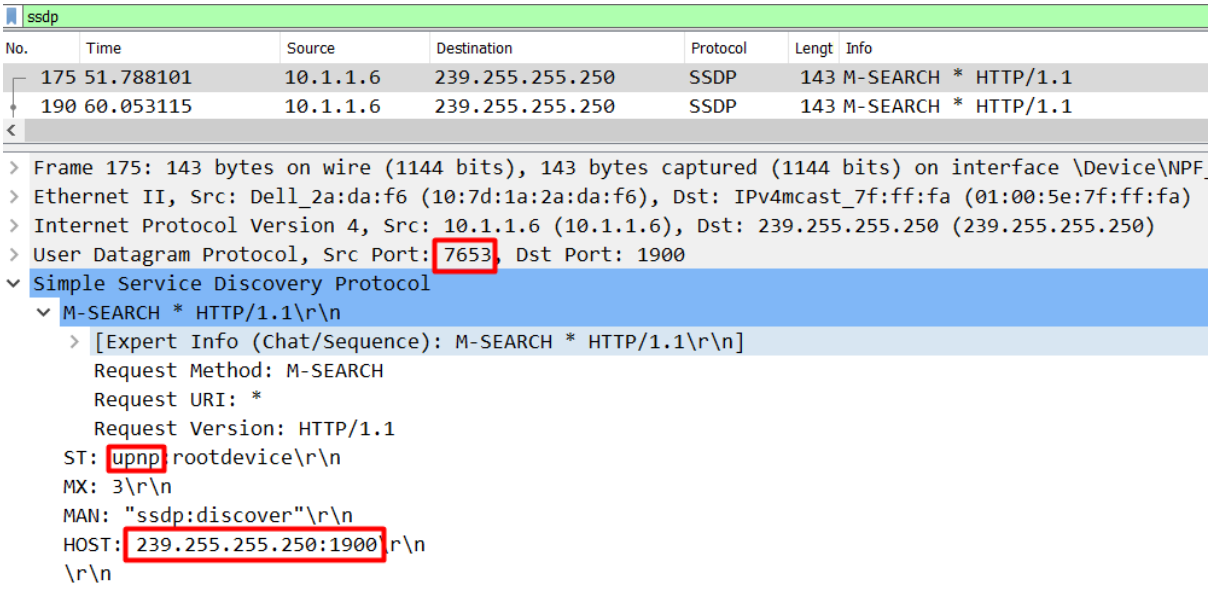

Figure 3.48: *SSDP I2P.*

Après l'analyse des captures selon les figures 3.48 et 3.49, on a remarqué que les paquets SSDP interceptés par Wireshark d'I2P sont égaux à 2 alors que dans les navigateurs Chrome et Firefox sont égaux à 4 paquets.

- Le port utilisé par le routeur I2P pour envoyer la requête M-SEARCH est « 7653 » mais Chrome et Firefox utilisent des ports aléatoires (63678, 64902 dans notre projet) pour envoyer la même requête.

- LalongueurdespaquetsSSDPestégaleà143 bytes pour réseauI2Pcontrairementaux navigateursChromeetFirefox qui est égale à 215 bytes.
- Les deux navigateurs Chromeet Firefox contient un champ « user-agent » dans le paquet SSDP alors qu'il est inexistant dans le paquet SSDP dans le réseau I2P.
- Le champ ST ("Search Target" : Cible de recherche) : est le même pour les deux navigateurs « ST : urn : dial-multiscreen-org : service : dial : 1\r\n » contrairement à le paquet SSDP envoyé par le retour I2P qui contient : « ST : upnp :rootdevice\r\n »
- UPnP : Universal Plug and Play (UPnP) est un protocole qui permet aux appareils compatibles UPnP de votre réseau de se découvrir et de communiquer automatiquement les uns avec les autres, ainsi que de créer des canaux de communication plus directs avec Internet.

❖ **Constatations :**

Après la terminaison de l'analyse de la capture Wireshark du réseau I2P nous avons pu sélectionner les différences entre le réseau I2P et les deux autres navigateurs Chrome et Firefox, pour cela nous pouvons identifier alors le réseau I2P avecses caractéristiques ci-dessous :

- L'envoie des requêtes « dz.pool.ntp.org » au serveur DNS pour trouver les serveursNTP.
- L'envoiedesrequêtes«africa.pool.ntp.org»auserveurDNSpourtrouverlesserveursNTP.
- DemandedesynchronisationauserveurNTP«africa.pool.ntp.org».
- LongueurtotaledupaquetSSDPetleportsource SSDP/UPnPutilisé.

Ces identifiants seront utilisés par la suite comme signatures numériques pour détecter letraficI2P.

3.6 Extraction des empreintes numériques

3.6.1 Extraction des empreintes numériques du réseau Tor

Depuis les analyses des captures Wireshark traitées précédemment, on n'a pas trouvé beaucoup de différences dans les paquets de la connexion TCP. Contrairement à la connexion TLS. A partirde ces différences on va extraire les empreintes qui vont nous aider à détecter l'utilisation du navigateur, qui sont représentées en une suite d'octets en hexadécimale.Notre signature sera le code encadré (code en hexadécimal).

- La première empreinte représente les suites de chiffrement **« Cipher suites »** dupaquet «clienthello**».** LenavigateurTor utilise18suitesdechiffrement.

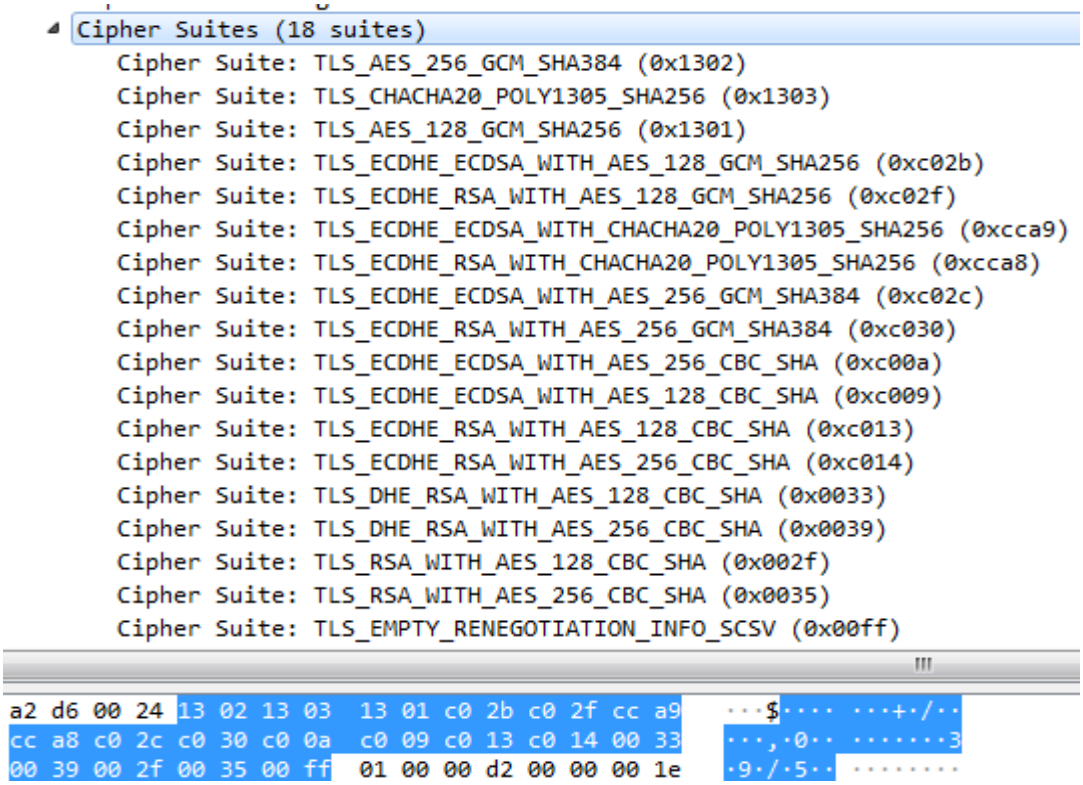

Figure 3.49: *L'empreinte de suite de chiffrement du paquet client hello.*

```
13 02 13 03 13 01 c0 2b c0 2f cc a9 cc a8 c0 2c c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00 39
00 2f 00 35 00 ff
```

- La deuxième empreinte identifie les algorithmes de signatures « **signaturealgorithms»**dupaquet**«clienthello».**,lenavigateurTor utilise23signatures.

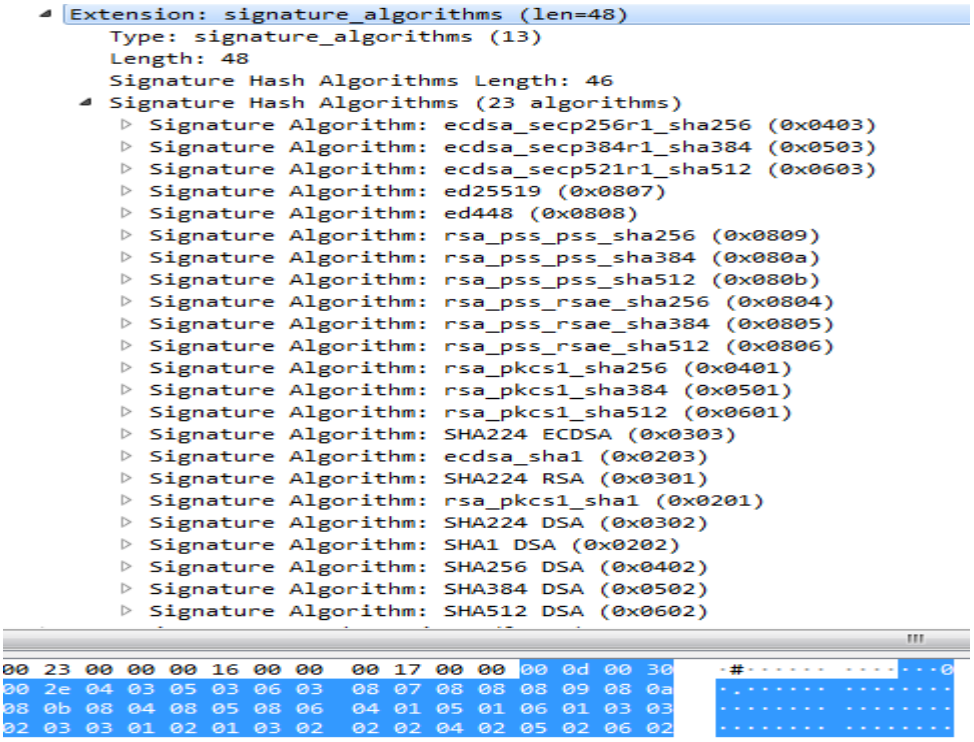

Figure 3.50: *L'empreinte des algorithmes de signature du paquet client hello.*

- La troisième empreinte identifie les groupes supportés **« supported_groups »** du paquet**«clienthello».** lenavigateurTorutilise 2groupes.

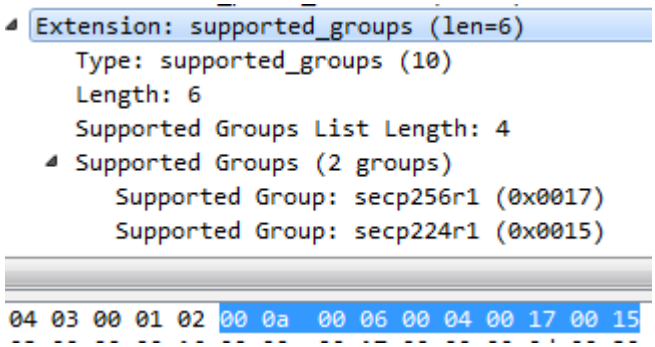

Figure 3.51: *L'empreinte des groupes supportés du paquet client hello.*

00 0a 00 06 00 04 00 17 00 15

- Laquatrième empreinteidentifieleport9001utiliséparlencœuddduréseau Tor.

Le port 9001

- La cinquième empreinte identifie la suite de chiffrement **« Cipher suite »** utilisée dans le paquet « server hello ».

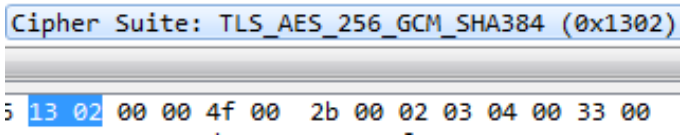

Figure 3.52: *L'empreinte des suites de chiffrements du paquet server hello.*

13 02 && le port 9001.

- La sixième empreinte identifie le nom du serveur **« Servername »** utilisée dans le paquet « client hello ».

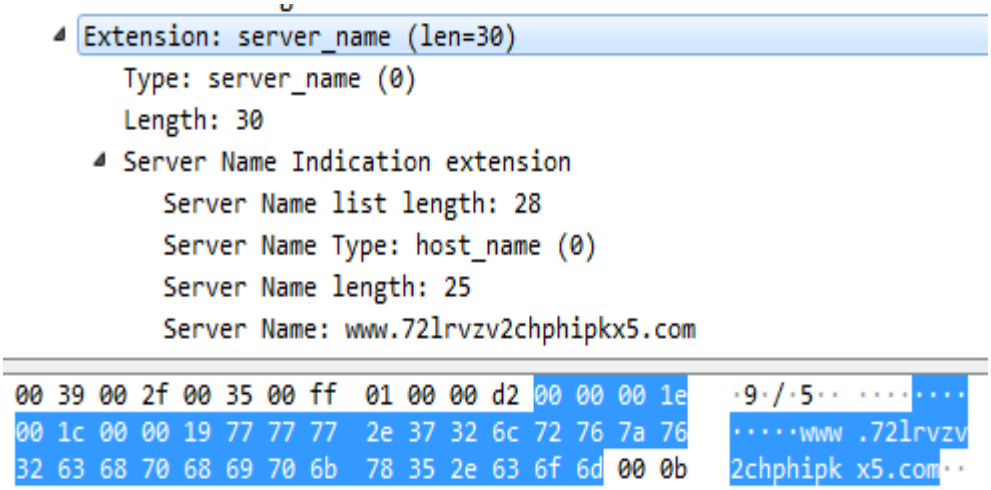

Figure 3.53: *L'empreinte de nom de serveur du paquet client hello.*

0000 00 00 00 1e 00 1c 00 00 19 77 77 77 2e 37 32 6c 72 76 7a 76 32 63 68 70 68 69 70 6b 78 35 2e 636f 6d

- La septième empreinte identifie **« ec_point_format »** utilisée dans le paquet « client hello ».

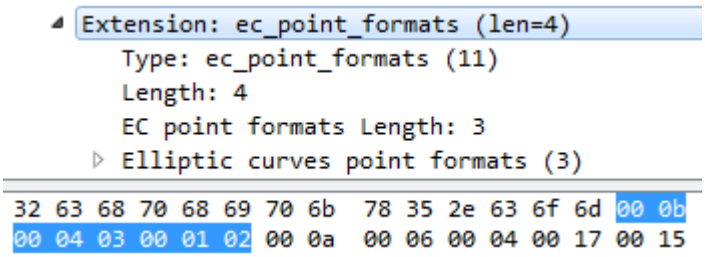

Figure 3.54: *L'empreinte ec_point_format du paquet client hello.*

00 0b 00 04 03 00 01 02

3.6.2 Extraction des empreintes numériques du réseau I2P

- La première empreinte est l'envoie des requêtes **« dz.pool.ntp.org »** au serveur DNS pour trouver les serveursNTP.

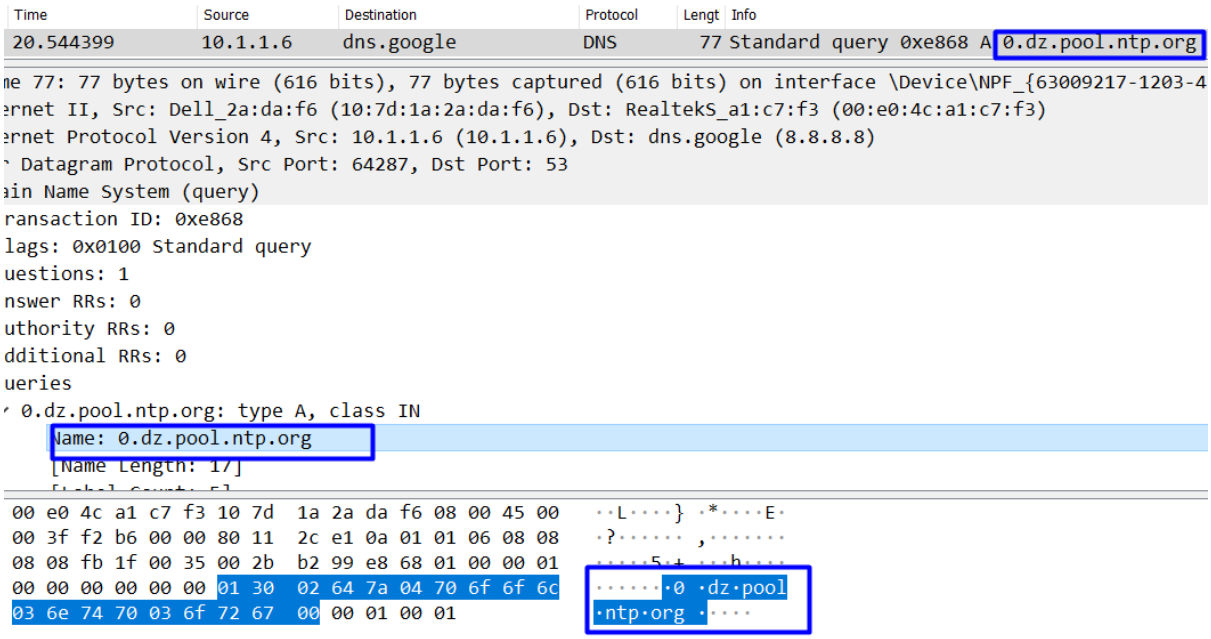

Figure 3.55: *Empreinte numérique 0.dz.pool.ntp.org*

01 30 02 64 7a 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00

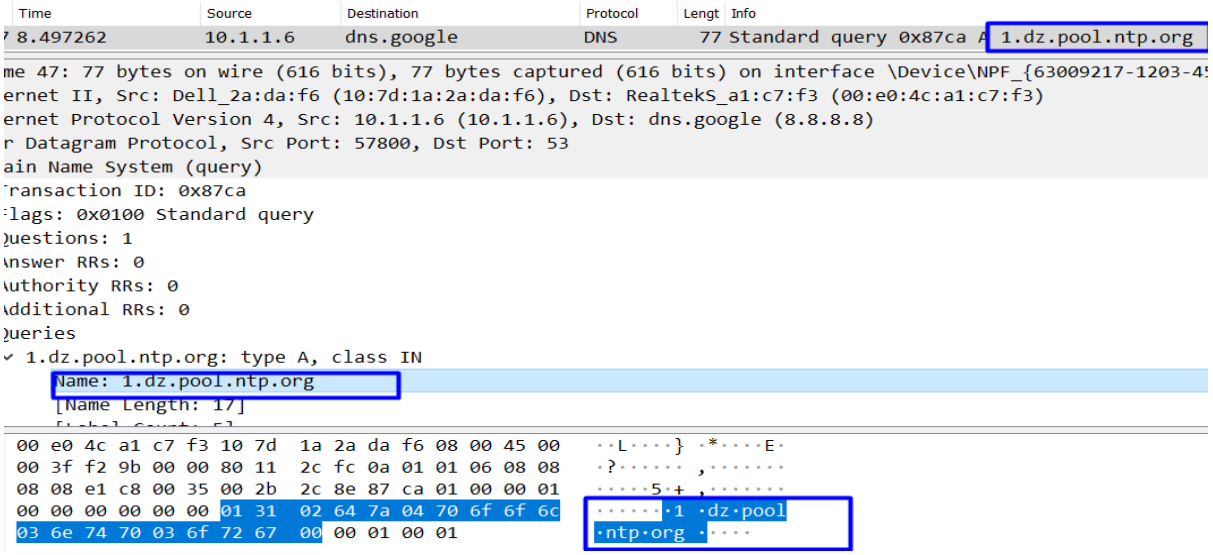

Figure 3.56: *Empreinte numérique 1.dz.pool.ntp.org.*

01 31 02 64 7a 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00

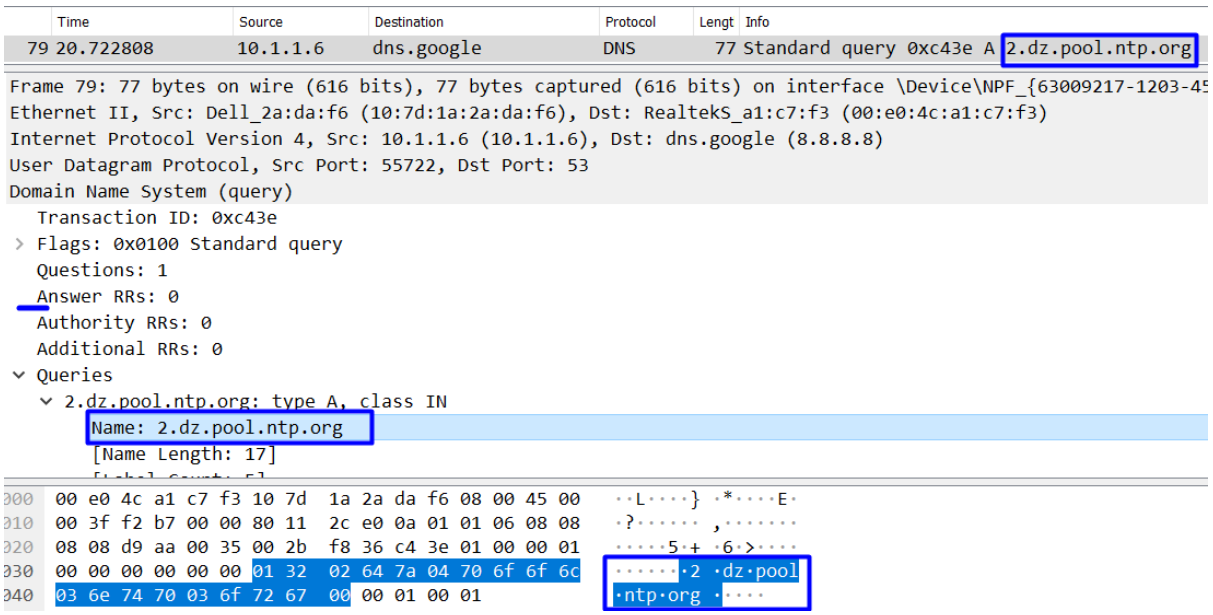

Figure 3.57: *Empreinte numérique 2.dz.pool.ntp.org.*

01 32 02 64 7a 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00

- La deuxième empreinte est l'envoiedesrequêtes**«africa.pool.ntp.org»**auserveurDNSpourtrouverlesserveursNTP.

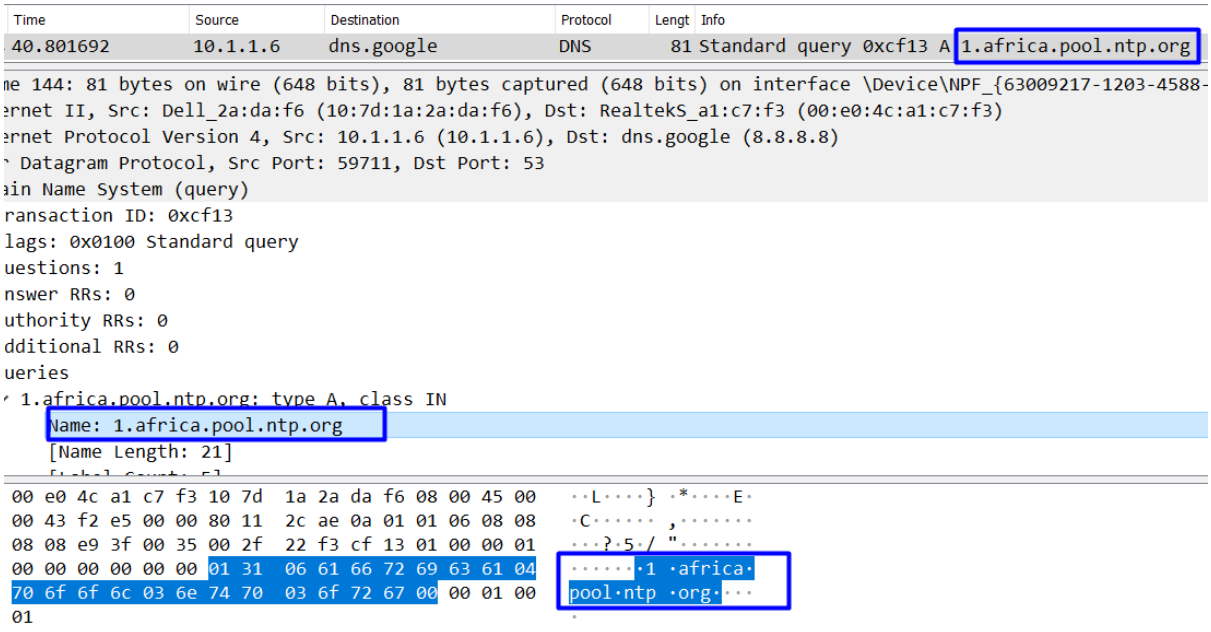

Figure 3.58: *Empreinte numérique 1.africa.pool.ntp.org.*

01 31 06 61 66 72 69 63 61 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00

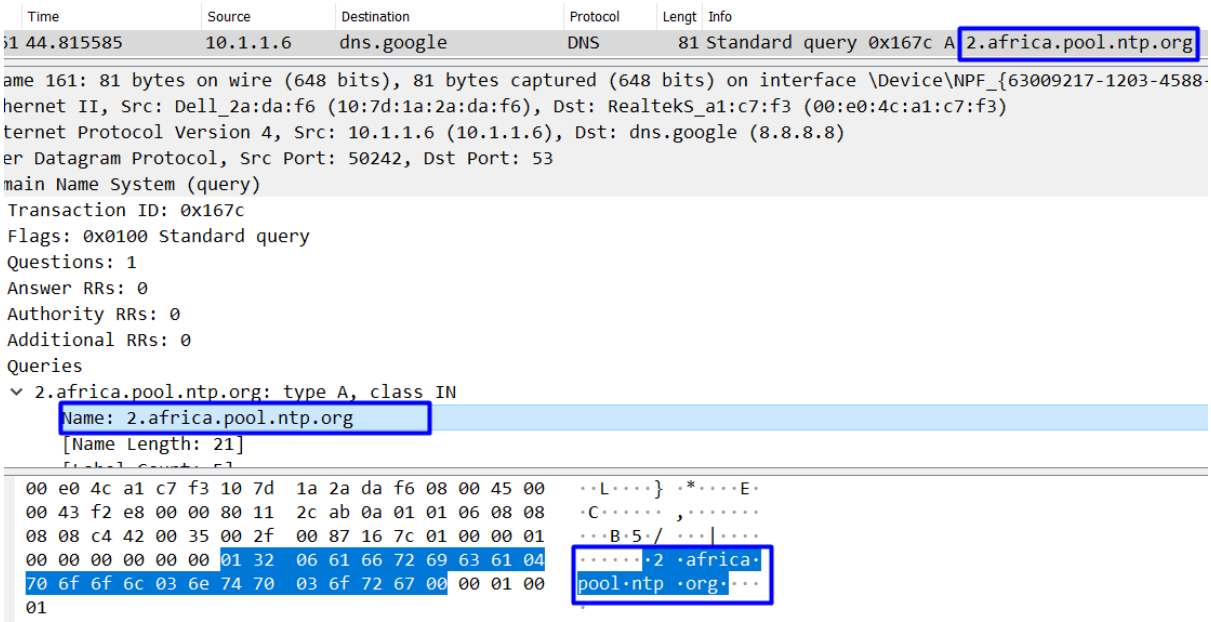

Figure 3.59: *Empreinte numérique 2.africa.pool.ntp.org.*

01 32 06 61 66 72 69 63 61 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00

«**africa.pool.ntp.org**»: Nous ne devons pas prendre l'empreinte du temps de transmission car ce dernier change à chaque fois (temps réel).

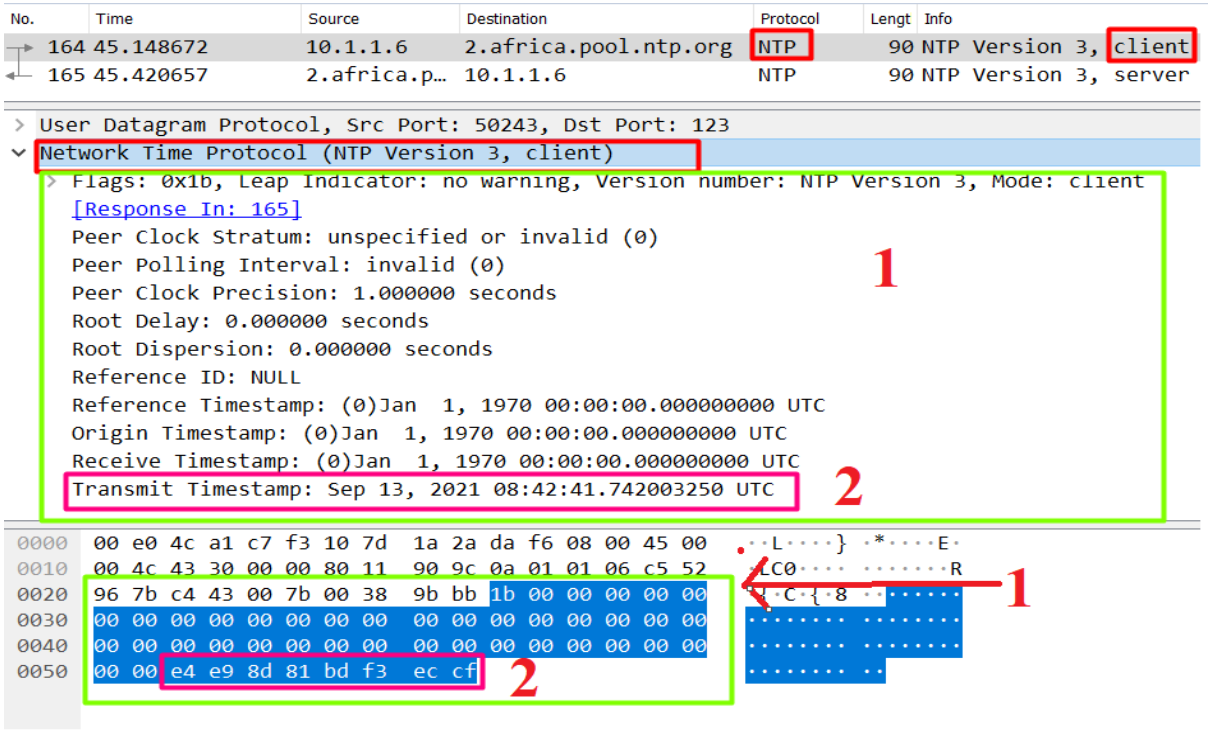

Figure 3.60: *Empreinte numérique synchronisation au serveur NTP.*

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 00 00 00 00 00 00

- La dernière empreinte numérique est le mot clé **« upnp »** et le port de source est égale à 7653 et l'adresse de destination 239.255.255.250 avec son port qui est égale à 1900.

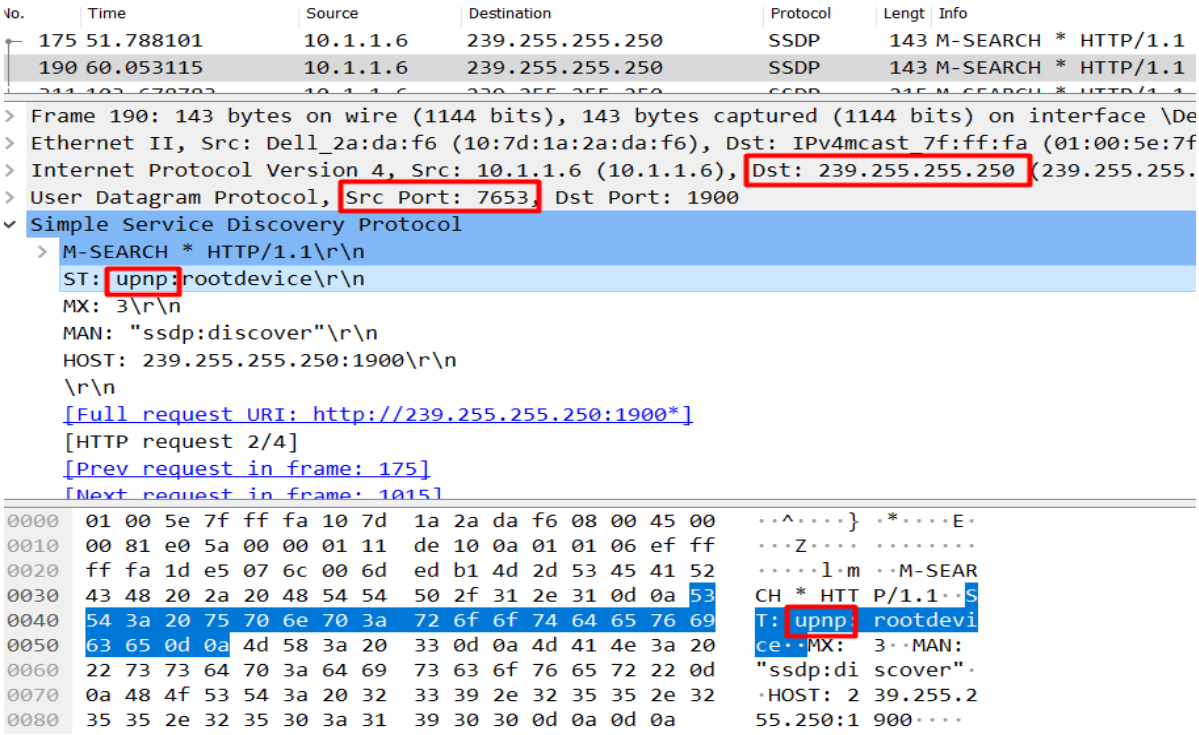

Figure 3.61: *Empreinte numérique « upnp ».*

3.7 Tableau comparatif des deux réseaux anonymes

Tor	Leport 9001. Lessuitesdechiffrements«CipherSuites»utilisées danslemessage«Client hello» Lesgroupessupportés«Supportedgroups»utilisées danslemessage«Client hello» Lessuitesdechiffrements«CipherSuites»utilisées danslemessage«server hello» Le Nom du serveur«server name»utilisées danslemessage «Client hello» Extension «ec_point_format»utilisées danslemessage «Client hello»
I2P	L'envoie des requêtes « dz.pool.ntp.org » au serveur DNS pour trouverles serveurs NTP L'envoiedesrequêtes«africa.pool.ntp.org»auserveurDNSpour trouverlesserveursNTP DemandedesynchronisationauserveurNTP«africa.pool.ntp.org». LongueurtotaledupaquetSSDPetleportsource SSDP/UPnPutilisé.

Tableau 3-7:Tableau comparatif des deux réseaux anonymes.

3.8 Conclusion

Dans ce chapitre nous avons effectué une analyse de deux réseaux anonymes Tor et I2P, c'est ce qui nous a permis de connaître l'identité des deux réseaux.

Apres avoir analysé le trafic venant de deux réseaux Tor et I2P on a pu extraire les signatures de ces derniers après les avoir comparés avec les deux navigateurs Chrome et Firefox.

Cette étude nous a permis d'extraire les empreintes numériques qui seront transformées à des règles implémentées dans un IDS (Snort) pour faire la détection des deux réseaux.

Chapitre 4 : Implémentation des signatures dans L'IDS

4.1 Introduction

Les réseaux anonymes permettent à leurs utilisateurs une protection de leur vie privée. Mais l'utilisation de cet outil sur un système informatique d'une entreprise peut exposer l'entreprise à divers risques de sécurité et l'entrainer à des problèmes judiciaires. Pour se protéger à ces attaques, il nous est nécessaire de mettre en place diverses mesures visant à augmenter le niveau de sécurité. En quelque sorte des moyens, face à la menace d'intrusion. Pour cela les entreprises se tournent de plus en plus vers les solutions de détection d'intrusion IDS.

Nous appelons IDS un mécanisme qui écoute secrètement le trafic réseau pour identifier les activités suspectes, permettant ainsi des alertes d'intrusion.

Dans ce chapitre nous allons procéder à une implémentation des règles basées sur les signatures extraites sous forme de règles. Puis on va les implémenter dans un système de détection d'intrusion « Snort ».A la fin tester la fiabilité de nos règles pour le but de détecter l'utilisation de Tor et I2p.

4.2 Système de détection d'intrusion

4.2.1 Définition

Un système de détection d'intrusions comme un système automatisé dont le rôle est la détection des intrusions dans un système informatique tout en examinant les audits de sécurité fournis par le système d'exploitation ou bien les outils de contrôle du réseau. Son but principal est la détection des utilisations non autorisées, les mauvaises utilisations et les abus dans un système informatique par les utilisateurs internes et externes [26].

4.2.2 Principe de fonctionnement des IDS

Un IDS est un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné. Composé généralement de logiciel et éventuellement de matériel, ce système informatique a le rôle de détecter toute tentative d'intrusion. Par définition, un IDS n'a pas de signal antiseptique ou réactif dans la mesure où il n'empêche pas une intrusion de se produire. Il se contente juste de faire une analyse de certaines informations en vue de détecter des activités malveillantes qui seront notifiées aux responsables de la sécurité du

système dans le plus bref délai possible. Cette raison fait de la majorité des IDS des systèmes qui opèrent en temps réel pourtant, il y'a des IDS qui réagissent en mettant fin à une connexion suspecte par exemple suite à la détection d'une intrusion[27].

4.2.3 Principes de détection d'intrusion

Généralement, dans les systèmes informatiques, il existe deux types d'approches pour la détection d'intrusion : l'approche par scénario ou bien dite par signature basée sur un modèle constitué des actions interdites contrairement à l'approche comportementale qui est basée sur un modèle constitué des actions autorisées [27].

a. Approche par scénario ou signature

Dans cette approche, les détecteurs d'intrusion reposent sur la création d'une base de motifs qui représente des scénarios d'attaques connus au préalable et qui sera utilisé par la suite, le plus souvent en temps réel, sur les informations fournies par les sondes de détection. C'est donc un système de reconnaissance de motifs qui permet de mettre en évidence dans ces informations la présence d'une intrusion connue par la base de signature.

b. Approche comportementale (Anomalydetection)

Les détecteurs d'intrusion comportementaux reposent sur la création d'un modèle de référence qui représente le comportement de l'entité surveillé en situation de fonctionnement normale. Ce modèle est ensuite utilisé durant la phase de détection afin de pouvoir mettre en évidence d'éventuelles déviations comportementales. Pour cela, le comportement de l'entité surveillée est comparé à son modèle de référence. Le principe de cette approche est de considérer tout comportement n'appartenant pas au modèle de comportement normale comme une anomalie symptomatique d'une intrusion ou d'une tentative d'intrusion.

4.2.4 Différents types d'IDS

Les attaques utilisées par les pirates sont très variées, puisque certaines utilisent des failles réseaux et d'autres des failles de programmation. C'est la raison pour laquelle la détection d'intrusion doit se faire à plusieurs niveaux. Donc, on distingue un d'IDS que nous détaillerons ci-dessous.

a. Systèmes de détection d'intrusion réseau (NIDS)

Les IDS réseaux analysent en temps réel le trafic qu'ils aspirent à l'aide d'une sonde (carte réseau en mode promiscuous). Ensuite, les paquets sont décortiqués puis analysés. Il est fréquent de trouver plusieurs IDS sur les différentes parties du réseau. On trouve souvent une architecture composée d'une sonde placée à l'extérieure du réseau afin d'étudier les tentatives d'attaques et d'une sonde en interne pour analyser les requêtes ayant traversé le pare-feu.

b. Systèmes de détection d'intrusion de type hôte (HIDS)

Les IDS systèmes analysent le fonctionnement de l'état des machines sur lesquelles ils sont installés afin de détecter les attaques en se basant sur des démons. L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levées.

c. Systèmes de détection d'intrusion Hybrides

Les IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, en un seul outil, de surveiller le réseau et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser le tout, et lier les informations d'origine multiple. Ainsi, on comprend que les IDS hybrides sont basés sur une architecture distribuée, ou chaque composant unifie son format d'envoi. Cela permet de communiquer et d'extraire des alertes plus pertinentes.

4.1.1 Concepts de base

Nous désirons dans cette section d'éclairer quelques notions qui seront utilisées dans le reste de ce travail.

- **Système :** dénote un système d'information contrôlé par un système de détection d'intrusions. Cela peut être un poste de travail, un élément du réseau, une unité centrale, un pare-feu, un serveur Web, un réseau d'entreprise, etc.
- **Alarme :** c'est la réponse générée par le système de détection d'intrusions lors de la détection d'une intrusion. Cependant les erreurs de détection peuvent être classées selon deux types :
  - ✓ **Les faux positifs :** signifie qu'un système de détection d'intrusions détecte une intrusion là où aucune intrusion réelle n'a été commise.

- ✓ **Les faux négatifs :** A l'inverse de « faux positif », « faux négatif » signifie que le système de détection d'intrusions n'a pas détecté une intrusion ayant réussi.

4.3 IDS Snort

4.3.1 Définition

Snort est un système de détection d'intrusion réseau open source capable d'effectuer une analyse du trafic en temps réel et une journalisation des paquets sur les réseaux IP [28].

Snort est composé de deux composants principaux :

- Un moteur de détection qui utilise une architecture de plug-in modulaire (le « moteur Snort »).
- Un langage de règles flexible pour décrire le trafic à collecter (les « règles Snort »).

4.3.2 Installation

Dans notre projet nous avonsopté pour la **version 3.1.12.0 de Snort**. Pour utiliser cette version, nous avons dû télécharger différentes bibliothèques qui sont ajoutées pour aider ce logiciel à fonctionner avec toutes ses capacités [29].

Nous avons installé les bibliothèques et les package suivant :

- La bibliothèque **« Safec »**
- La bibliothèque **« Hyperscan »**
- La bibliothèque **« Gperftools 2.8 »**
- La bibliothèque **« Ragel »**
- La bibliothèque **« Boost C++ »**
- La bibliothèque **« Flatbuffers »**
- La bibliothèque **« DAQ (Data Acquisition)»**
- La bibliothèque **« LuaJIT »**

```
mohamed@mohamed-Inspiron-15-3567:~$ /usr/local/bin/snort -V

   ,,_     -*> Snort++ <*-
  o"  )~   Version 3.1.12.0
   ''''    By Martin Roesch & The Snort Team
           http://snort.org/contact#team
           Copyright (C) 2014-2021 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using DAQ version 3.0.5
           Using LuaJIT version 2.1.0-beta3
           Using OpenSSL 1.1.1f  31 Mar 2020
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version 8.44 2020-02-12
           Using ZLIB version 1.2.11
           Using FlatBuffers 1.12.0
           Using Hyperscan version 5.3.0 2021-09-20
           Using LZMA version 5.2.4

mohamed@mohamed-Inspiron-15-3567:~$
```

Figure 4.1: *Bibliothèquesinstallées.*

4.3.3 Fonctionnement de Snort

Snort capture des paquets sur un point d'un réseau IP, analyse le flux obtenu en temps réel, et compare le trafic réseau à une base de données d'attaques connues. Les attaques connues sont répertoriées dans des librairies de règles mises à jour par plusieurs communautés très actives.

Figure 4.2: *Fonctionnement de Snort.*

Snort peut également être utilisé avec d'autres modules compatibles (tels que des interfaces graphiques, des actualisateurs de librairies d'attaques indépendants, etc.) Snort est compatible avec la plupart des OS comme Windows, Mac, Linux Ubuntu, CentOS…etc.

4.3.4 Les règles de Snort

a. Création des règles

Les règles de SNORT sont composées de deux parties distinctes : **le header et les options**.

- **Le header :** permet de spécifier le type d'alerte à générer **(alert, log et pass)** et d'indiquer les champs de base nécessaires au filtrage : le protocole ainsi que les adresses IP et ports sources et destination.
- **Les options** : spécifiées entre parenthèses, permettent d'affiner l'analyse, en décomposant la signature en différentes valeurs à observer parmi certains champs du header ou parmi les données.

Figure 4.3: *Les différents champs d'une règle Snort.*

1. **Header**

✓ **Le champ « action »** : il peut prendre plusieurs valeurs selon l'action à mener par Snort en détectant des paquets réseaux répondant au critère défini dans la règle. Ces valeurs sont les suivantes :

- **alert :** génère une alerte et log le paquet.
- **log :** log le paquet
- **pass :** ignore le paquet
- **activate :** active une règle dynamique
- **dynamic :** définie une règle dynamique.

✓ **Le champ « Protocole »** : décrit le protocole utilisé pour la communication. Snort supporte les protocoles TCP, UDP, ICMP et IP.

✓ **Les champs « Direction »** : renseignent Snort sur la direction des échanges réseau (->, <-, <->).

✓ **Les champs « Adress/Port »** : décrivent les adresses IP et les ports des machines qui échangent des données sur le réseau.

2. Options

Pour chaque option le format est nom (option), ci-dessous les options utilisées dans la création des règles :

- **msg :** affiche un message dans les alertes et journalise les paquets.
- **Logto :** journalise le paquet dans un fichier nommé par l'utilisateur au lieu de la sortie standard.
- **TTL:** teste la valeur du champ TTL de l'entête IP.
- **TOS :** teste la valeur du champ TOS de l'entête.
- **Id :** teste le champ ID de fragment de l'entête IP pour une valeur spécifiée.
- **Ipoption :** regarde les champs des options IP pour des codes spécifiques
- **Fragbits**: teste les bits de fragmentation de l'entête IP.
- **Dsize :** teste la taille de la charge du paquet contre une valeur.
- **Flags :** teste les drapeaux TCP pour certaines valeurs.
- **Seq :** teste le champ TCP de numéro de séquence pour une valeur spécifique.
- **Ack :** teste le champ TCP d'acquittement pour une valeur spécifiée.
- **Itype :** teste le champ type ICMP contre une valeur spécifiée.
- **Icode :** teste le champ code ICMP contre
- **Icmp_id :** teste le champ ICMP ECHO ID contre une valeur spécifiée.
- **Icmp_seq :** teste le numéro de séquence ECHO ICMP contre une valeur spécifiée.
- **Content :** recherche un motif dans la charge d'un paquet.
- **Content-list :** recherche un ensemble de motifs dans la charge d'un paquet.
- **Offset :** modifie l'option contente, fixe le décalage du début de la tentative de correspondance de motif.
- **Depth :** modifie l'option content, fixe la profondeur maximale de recherche pour la tentative de correspondance de motif.
- **Nocase :** correspond à la procédure de chaine de contenu sans sensibilité aux différences majuscules/minuscule

4.4 Architecture de la détection

L'architecture de Snort est organisée en modules, elle est composée de quatre grands modules : Le décodeur de paquets, les préprocesseurs, le moteur de détection et le système d'alerte et d'enregistrement de log comme montré dans la figure ci-dessous [27] :

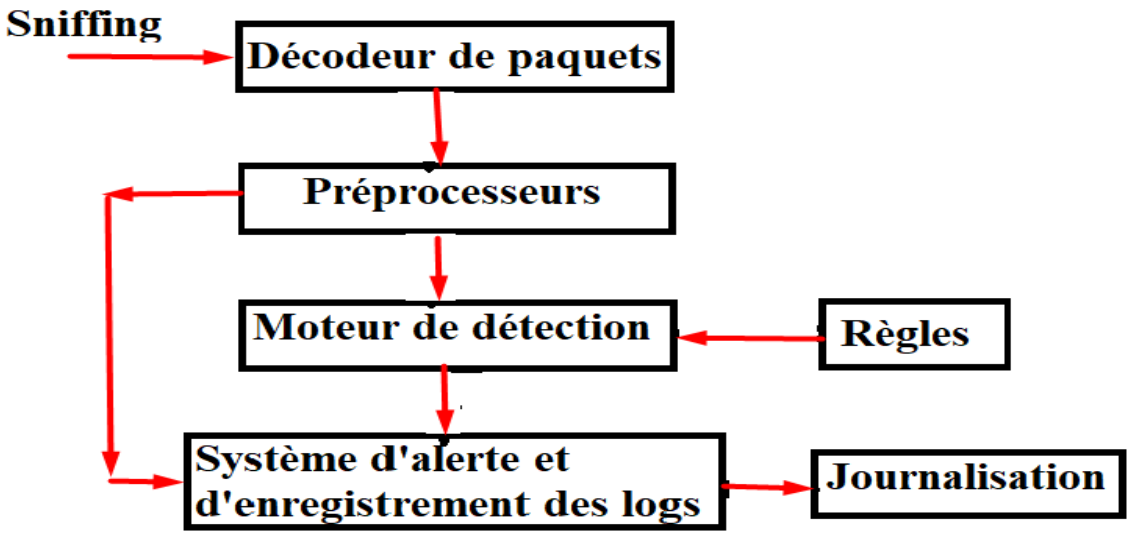

Figure 4.4: *Architecture de Snort.*

a. Le décodeur de paquets

Un système de détection d'intrusion active un ou plusieurs interfaces réseau de la machine en mode espion (promiscuous mode), ceci va lui permettre de lire et d'analyser tous les paquets qui passent par le lien de communication. SNORT utilise la bibliothèque « libpcap » pour faire la capture des trames.

b. Les préprocesseurs

Les préprocesseurs s'occupent de la détection d'intrusion en cherchant les anomalies. Un préprocesseur envoie une alerte si les paquets ne respectent pas les normes des protocoles utilisées. Un préprocesseur est différent d'une règle de détection, il est un programme qui vise à aller plus en détail dans l'analyse de trafic.

Les préprocesseurs permettent aussi d'étendre les fonctionnalités de SNORT. Ils sont exécutés avant le lancement du moteur de détection et après le décodage du paquet IP.

c. Moteur de détection

C'est la partie la plus importante dans un IDS. Le moteur de détection utilise les règles pour faire la détection des activités d'intrusion. Si un paquet correspond à une règle, alors une alerte est générée. Les règles sont groupées en plusieurs catégories sous forme de fichiers. SNORT vient avec un ensemble de règles prédéfinies.

Ces règles ne sont pas activées automatiquement, il faut les activer dans le fichier de configuration **snort.conf**.

d. Système d'alerte et d'enregistrement des logs

Le système d'alerte et d'enregistrement des logs s'occupe de la génération des logs et des alertes. Les alertes sont stockées par défaut dans le répertoire **« /usr/local/etc/rules »**

Dès que le système devient opérationnel, on pourra consulter les alertes générées directement dans les fichiers textes ou bien utiliser une interface graphique dans un navigateur avec **« localhost ».**

4.5 Création des règles Snort à partir des empreintes extraites

Au cours de ces chapitres nous avons pu extraire plusieurs identifiants de Tor et I2P, certains sont faciles à implémenter et tester au niveau de notre IDS, mais certains d'autre sont difficiles ou même dire irréalisables. Nous allons implémenter certaines informations d'identification pouvant impliquer l'utilisation de Tor et I2P. Pour cela, nous utilisons un système de détection d'intrusion open source (Snort). Snort utilise des signatures pour analyser le trafic réseau. Premièrement, nous devons créer une signature qui déclenche l'utilisation de Tor et I2P. Pour ajouter une nouvelle signature on utilise un langage simple qui spécifie la direction du trafic et les octets qui identifient le trafic. Nous avons écrit des signatures basées sur certains identifiants que nous avons trouvées précédent.

4.5.1 Règles Snort

4.5.1.1 Navigateur Tor

✓ **Règle 1 :** la première règle identifie les suites de chiffrement, cette règle va lancer une alerte avec le message **« possibilité d'utilisation de Tor : client hello cipher suites ».**

```
alert tcp any any -> any any (msg:" possibilitéd'utilisation de Tor: client hello cipher suites"; content:"|13 02 13 03 13 01 c0 2b c0 2f cc a9 cc a8 c0 2c c0 30 c0 0a c0 09 c0 13 c0 14 00 33 00 39 00 2f 00 35 00 ff|"; sid:10000001 ;)
```

✓ **Règle 2 :** la deuxième règle identifie server_name, cette règle va lancer une alerte avec le message **«possibilité d'utilisation de Tor : client hello servername extension».**

```
alert tcp any any -> any any (msg:" possibilitéd'utilisation de Tor:client hello servername extension "; content:"| 00 00 00 1e 00 1c 00 00 19 77 77 77 2e 37 32 6c 72 76 7a 76 32 63 68 70 68 69 70 6b 78 35 2e 63 6f 6d|"; sid:10000005; )
```

✓ **Règle 3 :** latroisièmerègleidentifielesgroupessupportés,cetterèglevalancerunealerteavec le message **« possibilité d'utilisation de Tor : client hello extension supported groups»**

```
alert tcp any 9001-> any any (msg:"possibilitéd'utilisation de Tor: client hello extension supported groups"; content:"|00 0a 00 06 00 04 00 17 00 15|"; sid: 10000002; )
```

✓ **Règle 4 :** la quatrième règle identifie les ports utilisés, cette règle va lancer une alerte avec le message **« possibilité d'utilisation de Tor : client hello port de destination»**

```
alerttcpanyany ->any 9001 (msg :"possibilité d'utilisation de Tor: client hello port de destination " ; sid : 10000003; )
```

✓ **Règle 5 :** lacinquièmerègleidentifielessuitesdechiffrementdupaquetserverhello,cette règle va lancer une alerte avec le message**«msg:"possibilitéd'utilisationdeTor:serverhellociphersuite»**.

```
alerttcpanyany ->any 9001 (msg:"possibilité d'utilisation de Tor:server hello cipher suite "; content:"|13 02|";  sid : 10000004;)
```

✓ **Règle 6 :** la sixième règle identifie ec_point_format, cette règle va lancer une alerte avec le message **« possibilité d'utilisation de Tor : client hello ec_point_format».**

```
alerttcpanyany ->any 9001 (msg :"possibilité d'utilisation de Tor : client hello ec_point_format " ; content:"| 00 0b 00 04 03 00 01 02|"; sid : 10000006; )
```

4.5.1.2 Réseau I2P

✓ **Règle 1** : la première signature détecte si le routeur I2P contacte le serveur DNS pour avoirl'adresse IP du serveur NTP de la « dz.pool.ntp.org » (de l'Algérie). S'il y'aura unerequête DNS demandant les adresses IP des « 0.dz.pool.ntp.org, 1.dz.pool.ntp.org et2.dz.pool.ntp.org » l'alerte se déclenche.

```
alertudpanyany ->any 53 (msg: "Possibilité de démarrage du routeur 12P: 0.dz.pool.ntp.org"; content:"|01 30 02 64 7a 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00|"; sid: 10000007;)
```

```
alertudpanyany ->any 53 (msg: "Possibilité de démarrage du routeur 12P: 1.dz.pool.ntp.org"; content:"|01 31 02 64 7a 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00|"; sid: 10000008;)
```

```
alertudpanyany ->any 53 (msg: "Possibilité de démarrage du routeur 12P: 2.dz.pool.ntp.org"; content:"|01 32 02 64 72 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00|"; sid: 10000009;)
```

✓ **Règle 2 :** la deuxième signature détecte si le routeur I2P contacte le serveur DNS pour avoirl'adresse IP du serveur NTP de la « africa.pool.ntp.org » (de l'Afrique). S'il y'auraune requête DNS demandant les adresses IP de l'une des Pool d'Afrique soit«0.africa.pool.ntp.org » ou « 1.africa.pool.ntp.org » ou bien « 2.africa.pool.ntp.org »,l'alertesedéclenche.

```
alertudpanyany ->any 53 (msg: "Possibilité de démarrage du routeur 12P: 0.africa.pool.ntp.org"; content:"|01 30 06 61 66 72 69 63 61 04 70 6f 6f 6c 03 6e 74 7 03 6f 72 67 00|"; sid: 10000010;)
```

alertudpanyany ->any 53 (msg: "Possibilité de démarrage du routeur i2p:1.africa.pool.ntp.org"; content:"|01 31 06 61 66 72 69 63 61 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00|"; sid: 10000011;)

alertudpanyany ->any 53 (msg: "Possibilité de démarrage du routeur 12P: 2.africa.pool.ntp.org"; content:"|01 32 06 61 66 72 69 63 61 04 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00|"; sid: 10000012;)

Remarque :Il existe un troisième IP pool en Afrique (3.africa.pool.ntp.org) mais on ne l'a pas détecté sur notre capture.

- ✓ **Règle 3 :** la troisième signature détecte si le routeur I2P contacte le serveur NTP par l'une desadressesIP proposées par leserveur DNS.

  Pour écrire cette alerte nous avons utilisé les 40 premiers octets (en hexadécimal)fixes représentant la requête client NTP. Ces 40 octets regroupent tous les champs sauf lechamp « Transmit Timetamp » qui change, il représente le temps de l'envoie de la requêteNTPpuis nousavonsspécifiéleport associéauNTP«123».

alertudpanyany ->any 123 (msg: " Possibilité de démarrage du routeur 12P: 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 |"; sid: 10000013;)

- ✓ **Règle 4 :** laquatrièmesignaturedétectesilerouteurI2Pcontactelegroupemulticast«239.255.255.250»eneffectuant unerequête SSDPM-SEARCH.

  Pour écrire cette alerte nous avons utilisé le port UDP destination « 1900 » duSSDPetleportsource«7653»spécifique utilisé par le routeur I2P pour lancer les requête SSDP M-SEARCH en multicast.Puis nous avons le contenu « UPnP » trouvé seulement dans le paquet SSDP envoyé par lerouteur I2P ainsi que la langueur de ce dernier qui est « 143 » inferieur a la langueur dupaquetSSDP ordinaire«216».

alertudpany 7653 -> 239.255.255.250 1900 (msg: " Possibilité de démarrage du routeur 12P: SSDP "; content:"upnp"; sid: 10000014;)

4.6 Implémentation des empreintes

Pour implémenter nos règles dans Snort, nous avons créé le fichier « local.rules », ensuite exécuter Snort et faire une demande pour charger ce fichier (avec l'indicateur -R), après nous avons réexécuté Snort en mode détection sur une interface (l'interface de passerelle de notre réseau LAN).

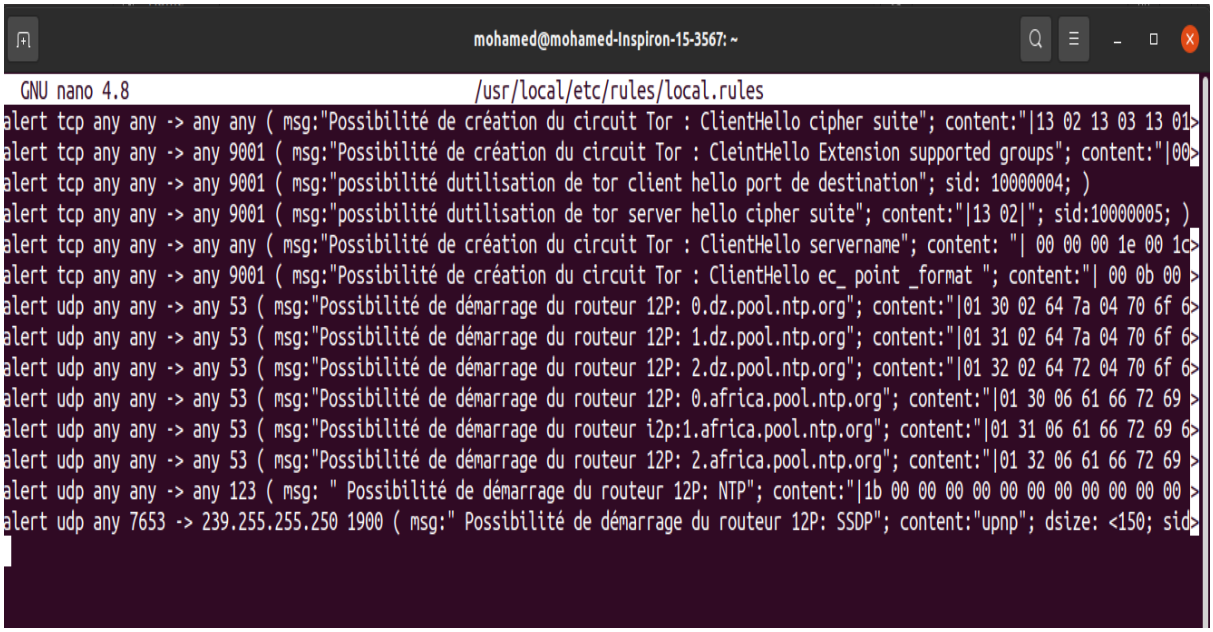

Figure 4.5: *Règles implémentées dans le fichier local.rules.*

4.6.1 Splunk

a. Définition

Splunk est le logiciel que nous utiliserons comme solution de gestion des informations et des événements de sécurité, qui affichera graphiquement (via une interface Web) toutes les alertes générées par Snort et nous fournira des outils puissants pour rechercher et comprendre ces alertes, ainsi qu'en tirer des informations plus approfondies [30].

b. Installation Splunk

Nous avons dû créer un compte gratuit sur le site Web de Splunk pour télécharger le logiciel et les modules complémentaires, après l'installation ce termine nous devons le configurer.

e. Configuration Splunk

Le serveur Splunk est à l'écoute sur le port 8000 (http://localhost:8000).Nous devons installer un plugin Splunk (appelé un module complémentaire) qui nous permettra de collecter facilement les journaux créés par Snort 3 et de les normaliser. Dans cette interface graphique, nous avons dû rechercher et installer **"Snort 3 JSON Alerts".**

f. Utilisation Splunk

Nous utilisons le filtre (**sourcetype="snort3:alert:json" | table _time src_apdst_ap msg**) pour afficher tous les événements dans un tableau avec l'heure, la source, la destination et un message.

Figure 4.6: *Identification dans l'interface Splunk.*

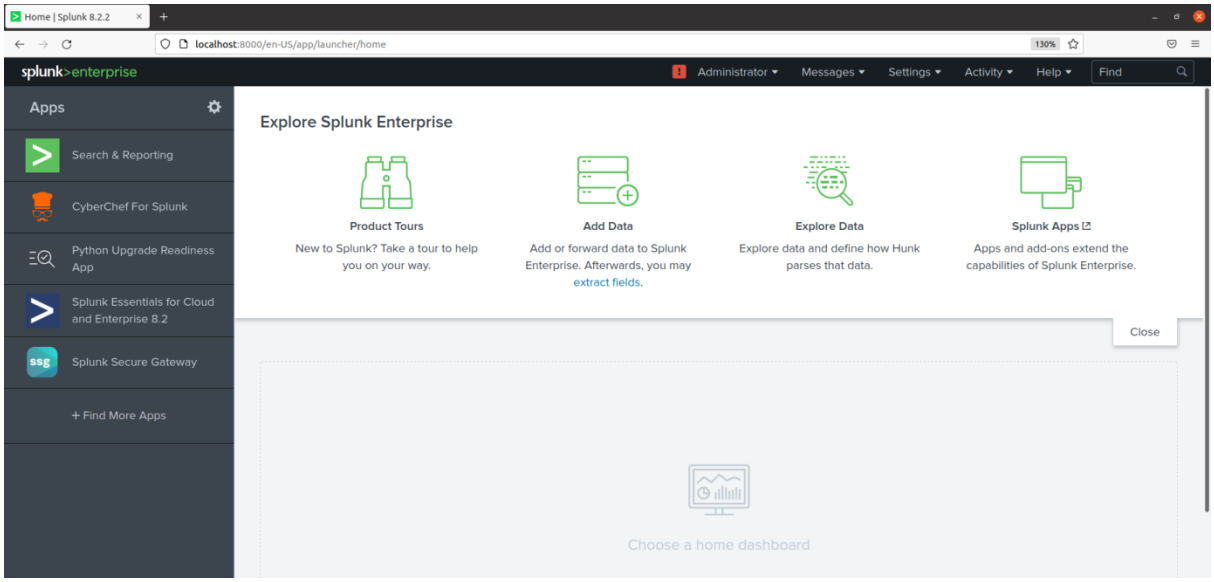

Figure 4.7: *Page d'accueil de l'interface Splunk.*

4.6.2 Résultats obtenus

Après le lancement de Snort et Splunk avec les commandes dans la figure 4.8 :

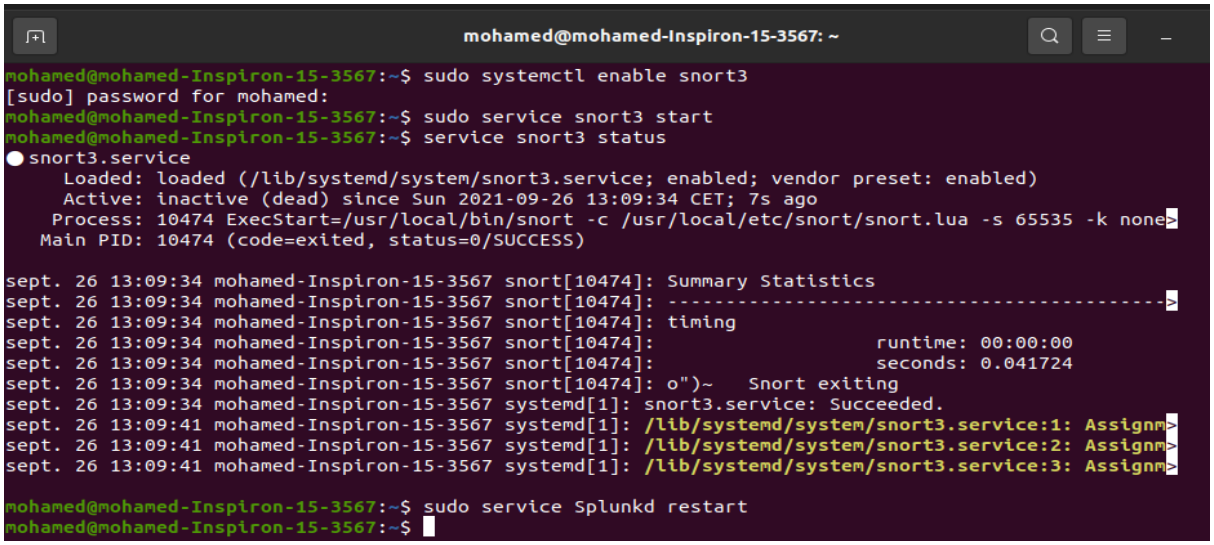

Figure 4.8: *Lancement de Snort et l'interface Splunk à partir du Terminal.*

D'abord on doit tester la fiabilité de nos règles en faisant la détection et en utilisant Snort avec un trafic venant de divers sites **(Google.com, Youtube.com, Facebook.com).**

Le résultat de cette détection est affiché dans la figure suivante :

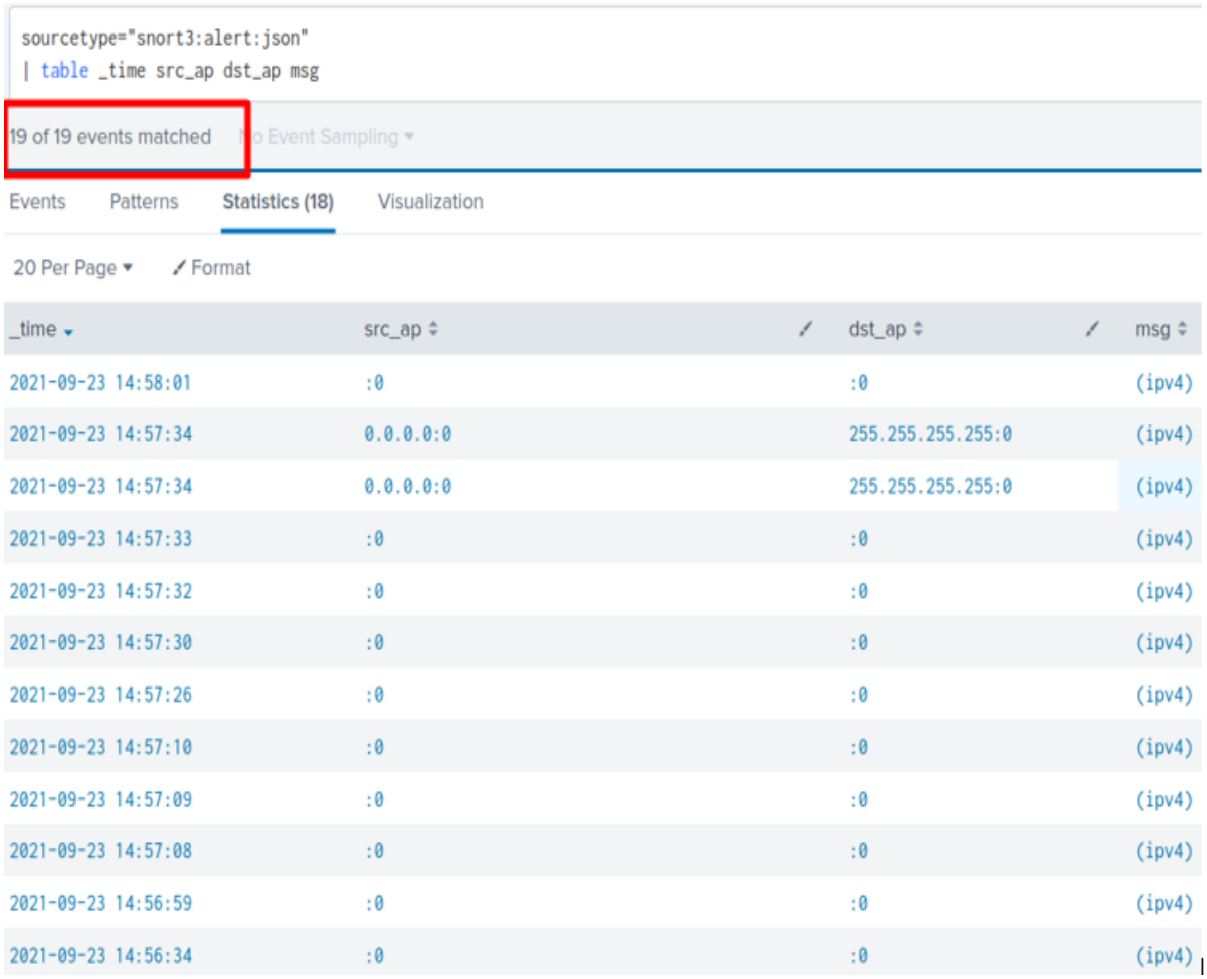

Figure 4.9: *Affichage Splunk lors d'une navigation normale du Web.*

Lors de la navigation de Web normal, Splunk affichera le nombre des évènements mais aucune alerte n'est lancée, nous pouvons voir que l'adresse de destination est 255.255.255.255 et l'adresse source est 0.0.0.0. La section DHCP identifie le paquet en tant que paquet Discover et identifie le client à deux endroits en utilisant l'adresse physique de la carte réseau (paquet ipv4 vers l'adresse de diffusion).

Nous remarquons aussi que lors de la recherche en temps réel, le temps est synchronisé.

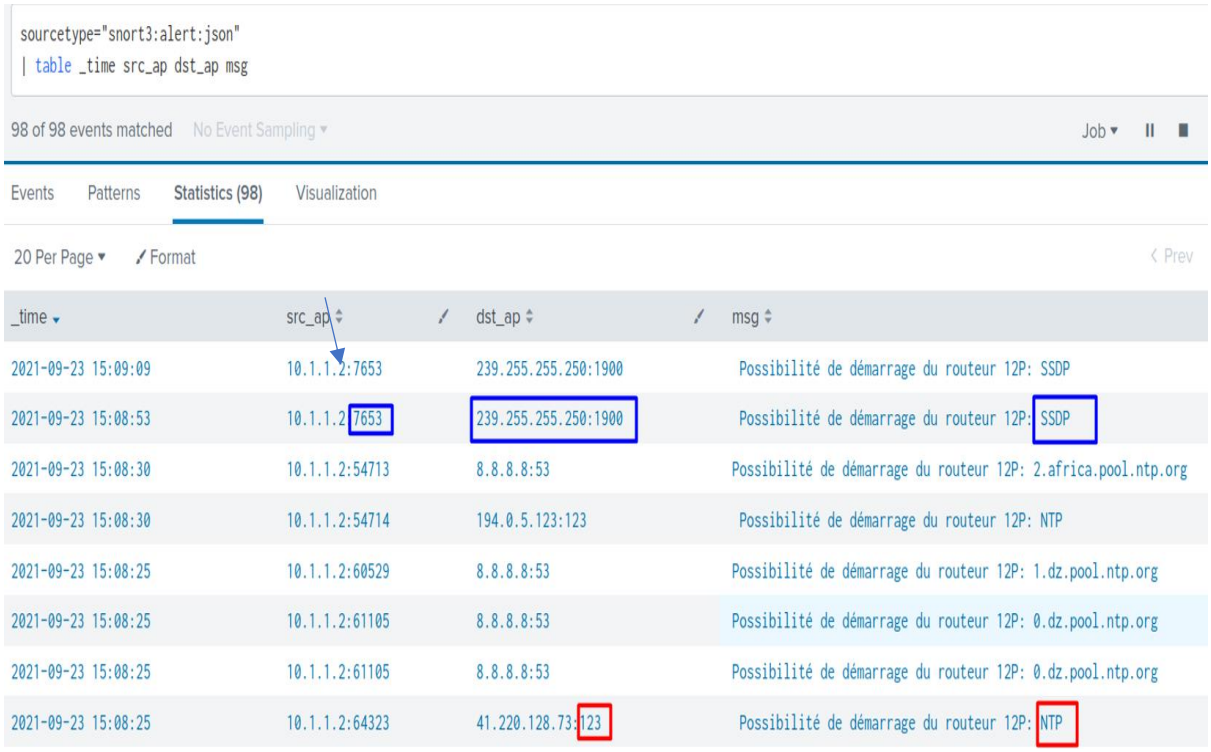

Figure 4.10: *Affichage Splunk lors de démarrage de réseau I2P.*

Lors de démarrage de réseau I2P dans le pc client, on remarque que Splunk affiche des alertes suivant nos règles intégrées dans le fichier **local.rules**.

Figure 4.11: *Affichage Splunk lors de démarrage de réseau Tor.*

Au moment du lancement de navigateur Tor dans le Pc client, nous remarquons que Splunk affiche l'un des nœuds de Tor comme adresse de destination avec le port de destination 9001, on a vérifié (dans le site mentionné précédemment

« metrics.torproject.org ») si l'adresse de destination affiché par Splunk appartient au réseau Tor. Le résultat est dans la figure suivante :

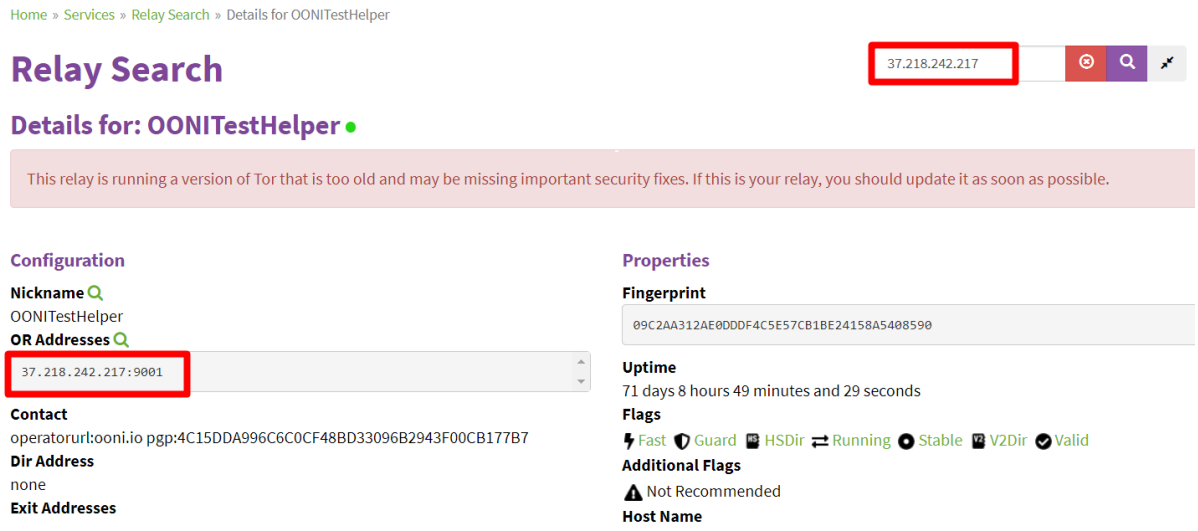

Figure 4.12: *Vérification de l'adresse de destination dans « metrics.torproject.org ».*

4.7 Discussion

La validation des résultats doit s'effectuer de deux manières : test dans un laboratoire et l'autre sur un environnement réel pour la validation de notre solution.

Durant le test des règles implémentées sur Snort on a constaté que certaines signatures qui identifient le réseau Tor nous ont causé des alertes lors d'une navigation normale sur le web. C'est ce qu'on appelle des faux positifs. Pour connaitre la cause des alertes on a procédé comme suit :

- Lancer l'analyseur Wireshark au moment de la navigation.
- Nous avons récupéré les adresses de destination qui appartiennent à l'alerte affichée sur l'interface Splunk.
- On a pris comme exemple l'adresse 77.74.181.62
- Vérifier si l'adresse n'appartient pas aux nœuds Tor.
- Consulter le site https://mxtoolbox.com/ Pour connaitre le DNS de cette adresse .on a trouvé que L'adresse 77.74.181.62 appartient à l'antivirus Kaspersky. Car notre Pc client a Kaspersky comme un antivirus.

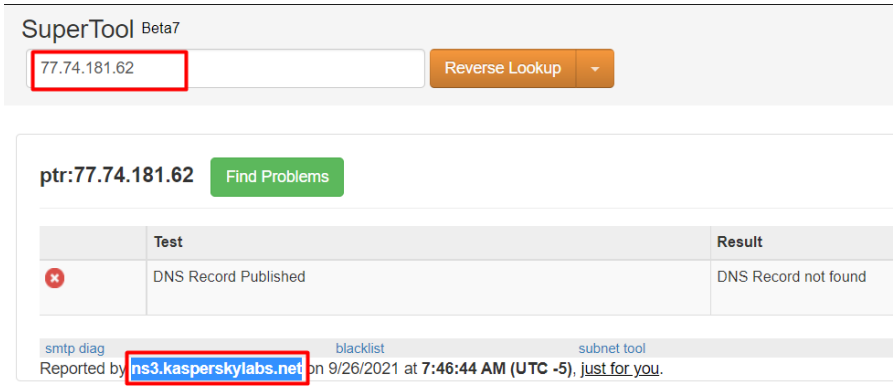

Figure 4.13: *DNS de l'adresse 77.74.181.62.*

Analyser la capture Wireshark :

- Mettre le filtre « ip.addr==77.74.181.62 &&tls » en place
- Identifier les signatures en commun avec Tor, durant l'analyse on a remarqué que les deux extensions **Encrypt_then_mac et signature algorithme** sont identiques à ceux de Tor, comme illustré sur les figures 4.14 et 4.15 :

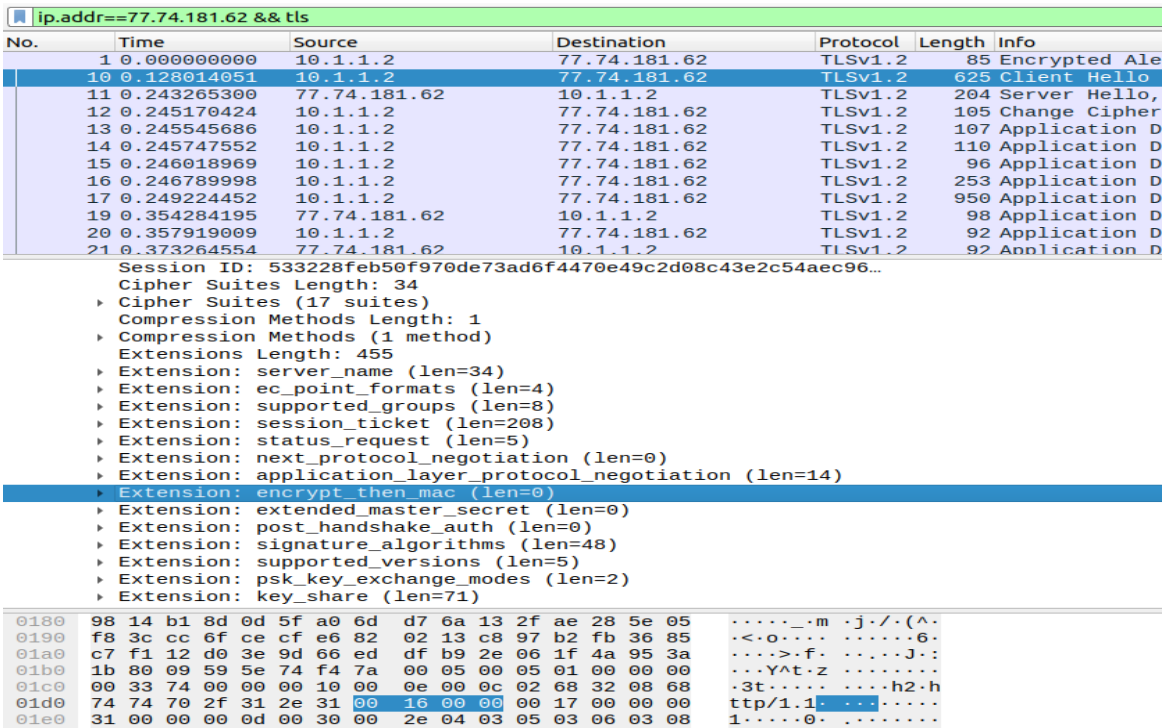

Figure 4.14: *Signature client hello « encrypt_then_mac » kaspersky.*

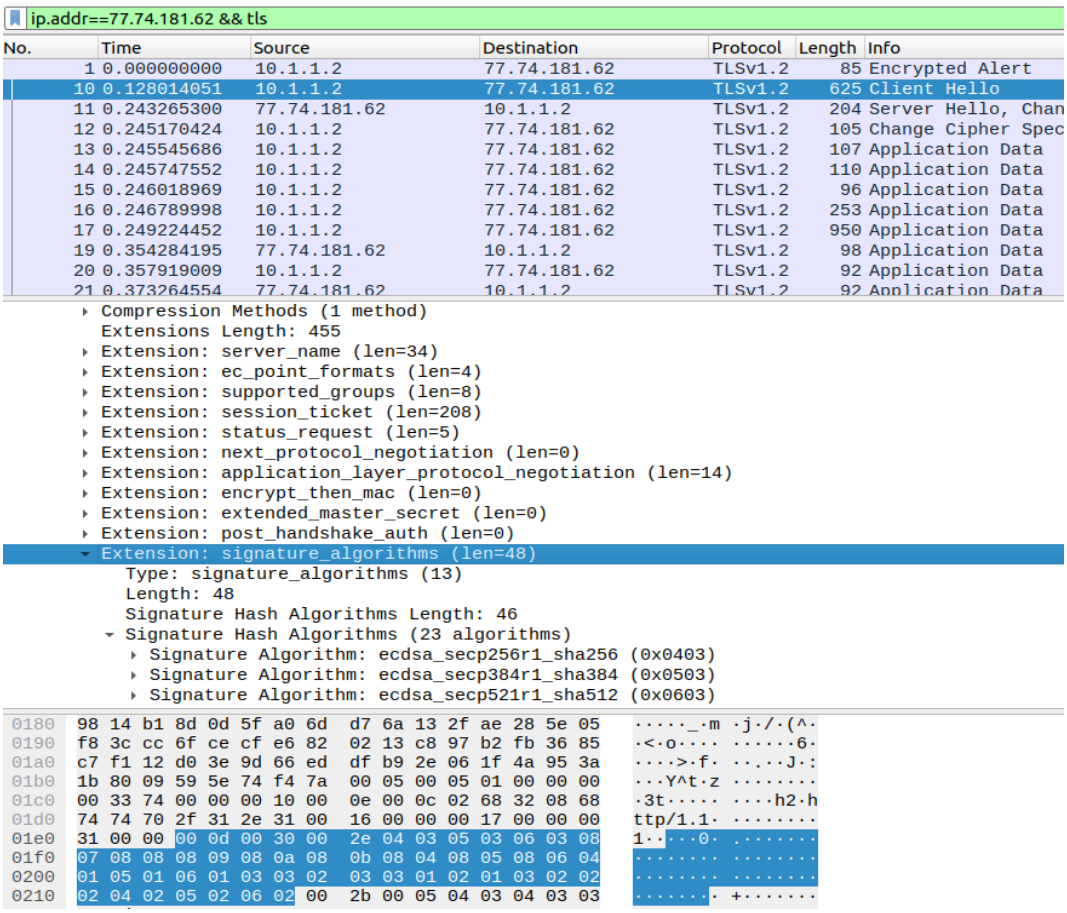

Figure 4.15: *Signature client hello « signature_algorithme » kaspersky.*

Après les résultats obtenus de cette analyse, on a enlevé ces signatures du dossier **« rules »** d'où on a obtenu des résultats satisfaisants. Doncpour remédier à ces alertes on a fait le choix d'ignorer ces signatures.

Comme mentionné précédemment les deux types de test sont différents, car dans un test de laboratoire le réseau est restreint, il contient peu de machine client donc peu de test. Dans notre étude, le client est identifié par son adresses IP, pour cela l'affichage des alertes dans l'interface graphique Splunk est par adresse IP.

Pour une meilleure implémentation sur un environnement réel (entreprise ou campus universitaire) les employeurs doivent s'enregistrer dans un serveur d'annuaire. Donc pour l'accès au réseau de l'entreprise ils doivent s'authentifier à un compte dédié par l'administrateur, dans le but est d'afficher et identifier les utilisateurs des réseaux anonymes « Tor et I2p » par leurs propres comptes « nom, prénom… » Même si les utilisateurs changent de poste « ordinateur » ou de travail à distance.

4.8 Conclusion

Dans ce chapitre, nous avons vu comment configurer et exécuter Snort en tant que Système de détection d'intrusion réseau (NIDS) sous Linux Ubuntu.

Tout d'abord, on a montré qu'avec Snort nous avons pu détecter l'utilisation du réseau Tor et I2Pen temps réel en utilisant les différentes règles que nous avons extrait au chapitre3.

Ensuite à l'aide de L'interface Splunknous avons surveillé les alertes générées par Snort.Ce type d'alerte à un taux de fausses alarmes, il est donc nécessaire de vérifier le contexte de l'alerte pour déterminer s'il s'agit d'une réelle tentative d'utilisation du réseau Tor et I2P.

Enfin nous somme parvenu à confirmer la fiabilité de nos règles.

Conclusion générale

L'utilisation des réseaux anonymes Tor et I2P n'est pas conseillée dans n'importe quelles organisations ou entreprises. En effet La détection des réseaux anonymes dans un réseau d'entreprise est très compliquée et nécessite une mise à jour permanente des règles permettant d'identifier le trafic Tor/I2P, mais nous aidera à identifier les infections possibles sur le réseau d'organisation (entreprise). C'est pour cette raison qu'ils devraient envisager de déployer plusieurs solutions pour augmenter les chances d'empêcher l'utilisation de Tor/I2P dans le réseau. Ce mémoire présente une étude expérimentale utilisant SNORT « système de détection d'intrusion réseau (NIDS) » qui peut détecter l'utilisation des réseaux Tor /I2P sur la base d'une base de données d'empreintes digitales. La recherche se concentre principalement sur la comparaison entre le trafic Web normal et le trafic venant des réseaux Tor/I2P. Pour la réalisation de cette recherche on a répondu aux questions suivantes :

- Qu'est-ce que l'anonymat et la vie privée sur internet ?
- Quels sont les outils permettant l'anonymat et quels sont les plus populaires ?
- Qu'est-ce qu'un réseau Tor et un réseau I2P et quel est leurs fonctionnements ?
- En quoi le réseau Tor diffère du réseau I2P ?
- Y-a-t-il une différence entre le trafic Tor/I2P et le trafic du web ordinaire ?
- L'implémentation des règles identifiant Tor et I2P dans un système de détection d'intrusion « Snort » sont-elles fiables ?

Lors de nos tests est après certaines améliorations des identifiants on est parvenue à identifier le trafic venant des réseaux Tor et I2p avec un taux élevé (sans faille). Détection a 100% (pas de faux positifs).

À partir de notre travail, on propose une liste de recommandation pour empêcher l'utilisation de réseau Tor dans une entreprise/organisation :

- Implémentations d'un système de détection d'intrusion réseau (NIDS), avec des mises à jour permanentes des règles permettent d'identifier le trafic Tor/I2P.
- Mise en place d'un serveur d'annuaire en attribuant un compte pour chaque employé afin de faciliter l'identification de l'utilisateur de Tor/I2P.
- Imposer des règlements stricte et sévères pour l'utilisateur de Tor/I2P.
- La vigilance à travers la sensibilisation et les formations.

Bibliographie et Webographie

[1] Preston Gralla: 'How the internet works', 8 ème edition (November 21, 2006)

[2] 'INTERNET Histoire ' : récupérer en Juillet sur : https://www.universalis.fr/encyclopedie/internet-histoire/

[3] 'World Wide Web information network ': récupéré en Juillet sur: https://www.britannica.com/topic/World-Wide-Web.

[4] 'Réseaux - Architecture client/serveur à 3 niveaux': récupéré en Juillet sur: https://web.maths.unsw.edu.au/~lafaye/CCM/initiation/3tier.html

[5] Won Kim n, Ok-Ran Jeong, Chulyun Kim ,"The dark side of the Internet: Attacks, costs and responses", Jungmin So Kyungwon University, Seongnam City, Republic of Korea

[6] 'What is the Deep and Dark Web?' : récupéré en Juillet sur: https://www.kaspersky.com/resource-center/threats/deep-web

[7] 'ANONYMAT SUR INTERNET' : récupéré en Juillet sur : https://www.murielle-cahen.com/publications/anonymat.asp

[8] A. Yanes. Privacy and anonymity. CoRR, abs/1407.0423, Juillet 2014

[9] C. Zachor E. Erdin and M. H. Gunes. How to nd hidden users: A survey of attacks on anonymity networks. IEEE Communication surveys & tutorials, vol. 17, no. 4, 2015

[10] Ligue des droits d'homme : 'Chiffrement, sécurité et libertés 'Positionnement de l'Observatoire des libertés et du Numérique, janvier 2017.

[11] Que devrais-je savoir au sujet du chiffrement - Surveillance : récupéré en Juillet sur : https://ssd.eff.org/fr/module/que-devrais-je-savoir-au-sujet-du-chiffrement%E2%80%89

[12] Artrit AJDINI ,Bryce CIARAN , « Étude et conception d'un service assurant l'anonymat », le 30 septembre 2019 Haute École de Gestion de Genève (HEG-GE).

[13] Ramzi A. Haraty and Bassam Zantout , "the TOR Data Communication System", "JOURNAL OF COMMUNICATIONS AND NETWORKS", VOL. 16, NO. 4, AUGUST 2014,

[14] Eric Filiol, Nicolas J. and Maxence Delong , "Statistical and Combinatorial Analysis of the TOR Routing Protocol , Structural Weaknesses Identified in the TOR Network", "Laboratoire

de Virologie et de Cryptologie Op´erationnelles, ESIEA, Laval, France Department of Defense, Paris, France".

[15] Brieuc Barthelemy, « L'anonymat dans le réseau Tor (The Second-Generation Onion) », université de Mons .

[16] Michael G. Reed, Member, IEEE, Paul F. Syverson, and David M. Goldschlag , "Anonymous Connections and Onion Routing" , "IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 16, NO. 4, MAY 1998".

[17] 'The Invisible Internet Project (I2P)' : récupéré en Juillet 2021 sur : https://geti2p.net/en/about/intro.

[18] Hongshan Yin Lab , Beijing Jiaotong & Yongzhong He Lab, "I2P Anonymous Traffic Detection and Identification 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)", University Beijing, China.

[19] 'Low-level Cryptography Specification ': récupéré en Juillet 2021 sur : https://geti2p.net/spec/cryptography

[20] 'Comparative study of anonymous network Tor and I2P': récupéré en Juillet 2021 sur: http://www.infocomm-journal.com/cjnis/article/2019/2096-109x/2096-109x-5-1-00066.shtml.

[21] 'Risks Associated to Using Tor inside a Business Network': récupéré en Juillet 2021 sur: https://hitachi-systems-security.com/risks-associated-to-using-tor-inside-a-business-network/

[22] 'What is Squid?' : récupéré en 2021 sur : http://www.squid-cache.org/Intro/

[23] 'Learn Wireshark' : récupéré en Juillet 2021 sur : https://www.wireshark.org/#learnWS

[24] 'Définition de TLS (Transport Layer Security)' : récupéré en Juillet 2021 sur : https://actualiteinformatique.fr/cybersecurite/definition-de-tls-transport-layer-security

[25] Anders Olaus Granerud , Identifying TLS abnormalities in Tor , Master's Thesis Master of Science in Information Security 30 ECTS , Department of Computer Science and Media Technology Gjøvik University College, 2010

[26] Kim, Jung Won, Integrating artificial immune algorithms for intrusion detection, University of London, University College London (United Kingdom). ProQuest Dissertations Publishing, 2002.

[27] Mémoire de Master en Informatique Option Administration et Sécurité des Réseaux Thème Etude et mise en place d'un système de Détection d'intrusion sous Linux, Université Abderrahmane Mira de Bejaïa Faculté des Sciences Exactes Département d'Informatique

[28] 'Snort 3 Is available!' : récupéré en Juillet 2021 sur : https://snort.org/

[29] Snort 3.1.0.0 on Ubuntu 18 & 20, Configuring a Full NIDS & SIEM Noah Dietrich, Snort Manuel.

[30] 'Why Customers Choose Splunk': récupéré en Septembre 2021 sur: https://www.splunk.com/en_us/about-us/why-splunk.html

[31] : https://rm.wikipedia.org/wiki/Datoteca:Internet-transit.svg

[32] : https://www.skymac.org/Admin-Dev/article-e4091b59-Guide-du-debutant-Les-bases-du-fonctionnement-d-internet-Partie-2-1.htm

[33] http://www-igm.univ-mlv.fr/~dr/XPOSE2001/perrot/Intro-Comparatif.htm

[34]https://www.tumgir.com/tag/Intechinfo

[35] https://www.marcos-rubinstein.ch/app/download/9629726384/1 Modele+OSI+AP-OSER+2019.pdf?t=1542385195

[36] https://ssd.eff.org/en/module/what-should-i-know-about-encryption

[37] https://blog.emsisoft.com/en/27485/vpn-privacy-2/

[38] https://linuxtrack.net/viewtopic.php?id=658

[39] https://www.scmp.com/news/world/article/1325310/national-security-agency-seeks-break-tor-anonymous-network

[40] https://medium.com/@monismagic/tor-vs-nsa-1d1cace21a38

[41]https://esdacademy.blogspot.com/2019/10/darknet-lautre-reseau-v2.html

[42]https://www.researchgate.net/figure/I2P-network-A-sample-of-inbound-and-outbound-tunnels-used-for-communication_fig2_268253957