Un paseo por la Deep Web

Jordi Cots Sanfeliu
MISTIC
Ad hoc

Victor Garcia Font
Jorge Chinea López

31/12/2018

FICHA DEL TRABAJO FINAL

Título del trabajo:	*TFM – Un paseo por la Deep Web*
Nombre del autor:	*Jordi Cots Sanfeliu*
Nombre del consultor/a:	*Victor Garcia Font*
Nombre del PRA:	*Nombre y dos apellidos*
Fecha de entrega (mm/aaaa):	01/2019
Titulación:	*MISTIC*
Área del Trabajo Final:	*Ad hoc*
Idioma del trabajo:	*Español*
Palabras clave	*Deep web, anonimato, dark net*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo*.

Paralelamente al Internet tal y como se conoce hoy en día, coexiste también la red denominada Internet profunda (Deep Web), Internet invisible o Internet oculta.

En el presente documento, se definirán estos conceptos, además de realizar una aproximación teórica sobre los diferentes medios de acceso a lo que se conoce como la Internet profunda o Deep Web, como son Freenet, Tor y I2P, mediante los cuales se pretende conseguir una navegación anónima a la Deep Web.

Esta aproximación será de tipo técnica-práctica controlada, accediendo a la Internet profunda a través de estos medios de acceso, mediante un laboratorio preparado para maximizar la seguridad, el cual se describirá en el presente documento, así como el tipo de tecnologías que conforman las herramientas y los medios de acceso.

En definitiva, el objetivo de este proyecto es mostrar el acceso a la Deep Web desde un entorno controlado y usando un punto de vista teórico-práctico, para poder analizar las características de este tipo de redes y contenidos.

Abstract (in English, 250 words or less):

Parallel to the Internet as it is known today, the network called Deep Web, Invisible Web or Hidden Web also coexists.

In the present document, these concepts will be defined, in addition to a theoretical approach on the different ways to access to what is known as Deep Internet or Deep Web, such as Freenet, Tor and I2P, through which it is intended to achieve an anonymous navigation to the Deep Web.

This approach will be within a controlled technical-practical nature, accessing the Deep Web through these ways of access, through a laboratory prepared to maximize security, which will be described in this document, as well as the type of technologies that make up the tools and ways of access.

In short, the aim of this project is to show access to the Deep Web from a controlled environment and using a theoretical-practical point of view, to be able to analyze the characteristics of this type of networks and contents.

Índice

1 Introducción

1.1 Contexto y justificación del Trabajo

Desde la creación de Internet, muchas personas han intentado aprovechar la difusión mundial que ésta presenta para la consecución de diferentes objetivos. Algunos de estos objetivos con un claro ánimo de lucro, y otros sin él, persiguiendo sólo la idea de mostrar y compartir información con los demás usuarios/as, en un mundo en el que el conocimiento es de todos/as.

Sea cual sea la finalidad del objetivo por el que se accede a la red, existen diferentes motivos por los que la navegación convencional no ofrece suficiente seguridad a los usuarios/as. Desde las finalidades más ilícitas en contra de la declaración universal de derechos humanos, como puede ser la trata de blancas, hasta finalidades totalmente lícitas en países democráticos, pero castigadas duramente según el código penal de algunos países, como es la libertad de expresión, los usuarios intentan esquivar el castigo y las condenas asociadas a estas acciones. De esta manera, estos usuarios se acogieron a una de las más eficaces medidas de seguridad en la red, el anonimato.

En el año 2000, Ian Clarke creó Freenet, una red de distribución de información descentralizada, con el objetivo de evitar la censura. Posteriormente, en 2002, nació la red Tor (The Onion Router), la cual pretende mantener la integridad y el secreto de la información que viaja a través de ella, además de no revelar la identidad de los usuarios. Por último, es de debido cumplimiento el hecho de nombrar a la red I2P, la cual también permite trabajar con un potente anonimato.

Existen más tecnologías similares a fecha de redacción de este documento, pero se han recogido estas 3 redes por ser las más comúnmente utilizadas por las personas que buscan permanecer anónimas detrás de su ordenador.

Con esta tecnología en forma de redes paralelas o superpuestas a Internet, y los objetivos nombrados, el presente trabajo pretende realizar una comparativa de las distintas tecnologías presentadas, para así poder entender su funcionamiento y filosofía, saber cuál es mas útil según la información que se pretenda consultar o transmitir, así como descubrir posibles vulnerabilidades o ataques que puedan llegar a comprometer el objetivo por el cual se crearon, el anonimato de sus usuarios/as.

1.2 Objetivos del Trabajo

Tal y como se ha informado en el apartado anterior, el objetivo principal de este documento es realizar un análisis y comparativa de las redes anónimas Freenet, Tor y I2P.

Para su consecución, se dividirá el objetivo en los siguientes puntos:

- Breve introducción a Deep Web
    - Conceptos Deep Web, Dark Net y Dark Web
    - Análisis de riesgos
    - Laboratorio para ejemplos prácticos

- Red Freenet
    - Historia y inicio de una red de distribución descentralizada
    - Diseño técnico y componentes
    - Herramientas y ejemplo práctico de uso
    - Debilidades y/o vulnerabilidades
    - Resumen analítico de la red Freenet

- Red Tor
    - Historia y inicio del enrutamiento de cebolla
    - Diseño técnico y componentes
    - Herramientas y ejemplo práctico de uso
    - Debilidades y/o vulnerabilidades
    - Resumen analítico de la red Tor
- Red I2P
    - Historia y inicio de la capa de abstracción anónima
    - Diseño técnico y componentes
    - Herramientas y ejemplo práctico de uso
    - Debilidades y/o vulnerabilidades
    - Resumen analítico de la red I2P
- Comparativa entre las diferentes redes analizadas
- Otras redes anónimas alternativas
- Conclusiones sobre el trabajo realizado

1.3 Enfoque y método seguido

La finalidad de este documento no es enfocar la información referente a la Deep Web en conceptos meramente teóricos, sino que se pretenden introducir estos conceptos de una manera práctica.

Es precisamente por ese motivo, por el que se tratarán cada una de las redes a analizar con la misma metodología de análisis, para así poder compararlas de la manera más directa posible.

Bajo estas premisas, distribuimos el trabajo a realizar en las siguientes etapas:

- Definición del plan de trabajo

  En esta etapa inicial, se establecen los objetivos de cada tarea para cada red a analizar, juntamente con los parámetros que se someterán a análisis. Se realizará una planificación temporal, y se enumerarán los entregables.

- Recopilación de información sobre Deep Web

  Se definen los conceptos de Deep Web, Dark net y Dark Web, así como las partes que comparten cada una de estas definiciones, para así poder entender la finalidad de este documento, ya que resulta muy común saltar de una definición a otra con facilidad.

- Análisis de riesgos

  Se cuantificarán los riesgos referentes al hecho de navegar por este tipo de redes anónimas

- Laboratorio para ejemplos prácticos

  Se describirá el escenario necesario para la realización de los ejemplos prácticos, intentado conseguir el máximo de seguridad posible

- Arquitectura de la red anónima a analizar

  Se describe la especificación técnica de la red estudiada, para entender cómo se consigue el anonimato, y que tipo de tecnología utiliza para conseguirlo, nombrando todos los componentes necesarios para su correcto funcionamiento.

- Demostración práctica de la red anónima

  Definición de las herramientas necesarias para el uso de la red anónima analizada, así como una pequeña demostración práctica de su uso, y contenidos publicados en este tipo de redes.

- Análisis de debilidades y vulnerabilidades de la red anónima

  Se analiza la seguridad que ofrecen las redes anónimas estudiadas ante los posibles ataques de usuarios maliciosos, comprobando hasta qué punto sería posible llegar a perder el propio anonimato.

- Resumen y conclusiones sobre la red anónima analizada

  Definición de ventajas y desventajas referentes a la red anónima presentada.

- Comparativa de las diferentes redes anónimas analizadas

  Se describirá cómo seleccionar una red anónima frente a otras según el objetivo o la finalidad que se pretenda conseguir.

- Alternativa a las redes anónimas analizadas

  Tal y como se ha anunciado en la introducción, éstas son las redes anónimas más conocidas para los usuarios de la Deep Web, pero no son las únicas. En esta etapa se realizará una presentación de otras redes anónimas no tan conocidas, pero igual de útiles.

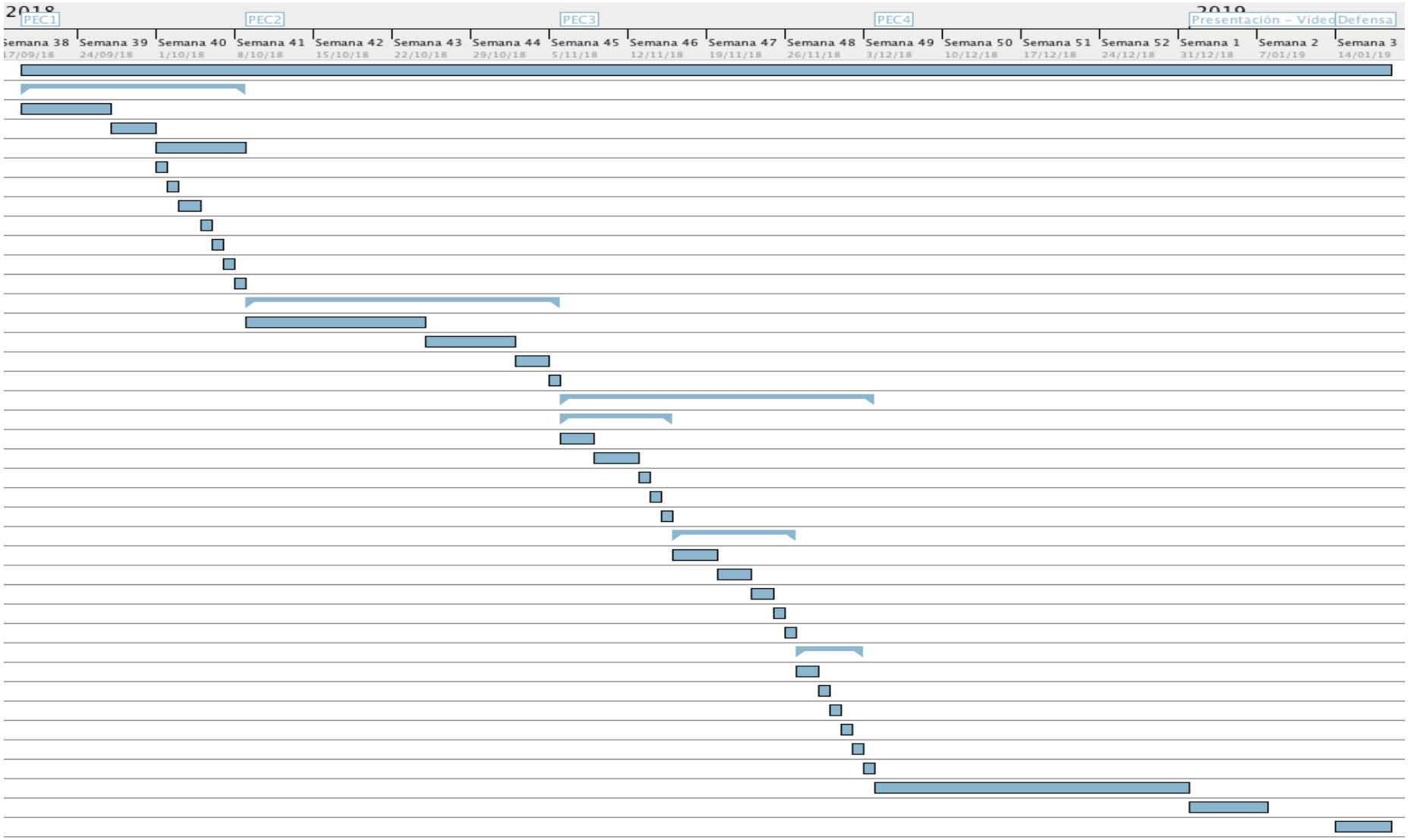
- Resumen y conclusiones sobre todo el trabajo presentado

  En esta última etapa se relacionará todo el contenido del documento, ya que el uso de las redes anónimas lleva provocando desde hace tiempo, una evolución en la manera de gestionar contenido en la red, chocando a menudo con leyes y gobiernos.

1.4 Planificación del Trabajo

A continuación, se presenta el diagrama de Gantt con la planificación temporal referente al trabajo a realizar:

Nombre	Fecha de inicio	Fecha de fin
TFM – Un paseo por la Deep Web	19/09/18	18/01/19
PEC1	19/09/18	8/10/18
Documentación previa	19/09/18	26/09/18
Orientación y ámbito del TFM	27/09/18	30/09/18
Plan de trabajo	1/10/18	8/10/18
Contexto y justificación	1/10/18	1/10/18
Objetivos	2/10/18	2/10/18
Enfoque y método seguido	3/10/18	4/10/18
Planificación del trabajo	5/10/18	5/10/18
Productos obtenidos	6/10/18	6/10/18
Descripción de los capítulos	7/10/18	7/10/18
Entrega PEC1	8/10/18	8/10/18
PEC2	9/10/18	5/11/18
Recopilación de información	9/10/18	24/10/18
Análisis de riesgos	25/10/18	1/11/18
Laboratorio de prácticas	2/11/18	4/11/18
Entrega PEC2	5/11/18	5/11/18
PEC3	6/11/18	3/12/18
Red Freenet	6/11/18	15/11/18
Historia	6/11/18	8/11/18
Diseño técnico	9/11/18	12/11/18
Herramientas y ejemplo de ...	13/11/18	13/11/18
Debilidades/Vulnerabilidades	14/11/18	14/11/18
Resumen analítico	15/11/18	15/11/18
Red Tor	16/11/18	26/11/18
Historia	16/11/18	19/11/18
Diseño técnico	20/11/18	22/11/18
Herramientas y ejemplo de ...	23/11/18	24/11/18
Debilidades/Vulnerabilidades	25/11/18	25/11/18
Resumen analítico	26/11/18	26/11/18
Red I2P	27/11/18	2/12/18
Historia	27/11/18	28/11/18
Diseño técnico	29/11/18	29/11/18
Herramientas y ejemplo de ...	30/11/18	30/11/18
Debilidades/Vulnerabilidades	1/12/18	1/12/18
Resumen analítico	2/12/18	2/12/18
Entrega PEC3	3/12/18	3/12/18
PEC4	4/12/18	31/12/18
Presentación – Vídeo	1/01/19	7/01/19
Defensa	14/01/19	18/01/19


2018
PEC1
PEC2
PEC3
PEC4
2019
Presentación – Vídeo
Defensa
Semana 38 17/09/18
Semana 39 24/09/18
Semana 40 1/10/18
Semana 41 8/10/18
Semana 42 15/10/18
Semana 43 22/10/18
Semana 44 29/10/18
Semana 45 5/11/18
Semana 46 12/11/18
Semana 47 19/11/18
Semana 48 26/11/18
Semana 49 3/12/18
Semana 50 10/12/18
Semana 51 17/12/18
Semana 52 24/12/18
Semana 1 31/12/18
Semana 2 7/01/19
Semana 3 14/01/19

1.5 Breve sumario de productos obtenidos

El presente documento está dividido en distintas entregas, que formaran parte del TFM final:

- PEC1: Se definen los objetivos a alcanzar, identificando la necesidad a cubrir, y indicando la planificación a seguir para la consecución del objetivo

- PEC2: Se definen los conceptos Deep Web, Dark Web y Dark Net, y se realiza en análisis de riesgos, tanto los referentes a la navegación a través de la red Internet convencional como los explícitamente aplicables a las redes anónimas. También se define el laboratorio empleado para la realización de los ejemplos prácticos

- PEC3: Se analizan las redes anónimas Freenet, Tor e I2P, empezando por su historia, origen y creación, pasando por su diseño técnico y funcionamiento, para acabar con una demostración práctica y un resumen tanto de sus debilidades como de sus funcionalidades

- PEC4: Se redacta la comparativa entre las distintas redes, así como el capítulo referente a las alternativas existentes. Finalmente se procede a indicar las conclusiones del documento, así como definir el trabajo futuro

1.6 Breve descripción de los otros capítulos de la memoria

- Breve introducción de Deep Web

- Se definen conceptos que se confunden fácilmente, como pueden ser Deep Web, Dark Net y Dark Web. También se hace referencia a los riesgos que conlleva navegar por redes anónimas, ya que existe el riesgo de incurrir en delitos al existir mucho contenido ilegal. Finalmente se describirá el entorno de prácticas que se ha llevado a cabo para la realización de este documento, intentando maximizar la seguridad tanto física como virtual.

- Red Freenet, Tor y I2P

- Se realiza una introducción sobre la aparición de estas redes, para posteriormente describir sus componentes y diseños técnicos. Posteriormente se realiza un ejemplo práctico de su uso, y se describen sus debilidades y vulnerabilidades, para terminar con un resumen sobre toda la información analizada.

- Comparativa entre las Freenet, Tor y I2P

- Se definen para qué casos es preferible usar una red antes que otra, dado que las tres ofrecen anonimato

- Otras redes anónimas alternativas

- Aunque las redes anónimas analizadas en este documento acumulan la mayoría de los usuarios, en este capítulo se analizan posibles alternativas

2 Breve introducción de Deep Web

2.1 Conceptos Deep Web, Dark Web y Dark Net

Hace ya unos cuantos años que el término Deep Web aparece en casi todos los medios de comunicación, popularizando así su existencia. No es el propósito de este documento publicitar más este concepto, sino que lo que se pretende es definir clara y meridianamente qué contenidos engloba, entendiendo así hasta dónde llega el alcance de su definición.

Genéricamente hablando, se entiende como Deep Web cualquier contenido que no está indexado por los motores de búsqueda de contenidos (entiéndase Google, Bing, Yahoo, Ask, etc.). Esto es así porque el contenido que no se encuentra en estos buscadores no es visible para el público, debido a que se usan los mencionados buscadores precisamente para encontrar contenidos sin tener que memorizar direcciones así que, a priori, no hay manera de acceder a ellos.

Entendido este punto, hay que especificar bien el por qué no pueden ser indexados estos contenidos, para poder aparecer en los motores de búsqueda cuando hagamos consultas, y así poder acceder a los contenidos.

Entre el tipo de contenido no indexado por los buscadores encontramos:

- Páginas web protegidas por usuario y contraseña, como pueden ser las del portal de un servicio bancario, páginas personales, etc.

- Páginas web a las que se accede mediante algún tipo de filtrado, para así evitar público no deseado. Aquí podríamos encontrar acceso a intranets corporativas, ERPs, etc., filtradas por una conexión VPN o IPs de origen mediante un firewall corporativo

- Páginas web con contenido estático des de hace demasiado tiempo y sin ningún interés por parte del público (sin visitas recientes)

- Otras páginas web no indexadas por los buscadores debido a otros criterios o políticas, aunque aquí se podría dar el caso de que un tipo de contenido aparezca en un buscador, pero no en otro

- Páginas web donde se indica claramente a los robots de los buscadores que no se quiere ser indexado

Todo este tipo de contenido forma parte de la Deep Web, ya que es una tarea realmente difícil el hecho de acceder a él, por no decir que se trata de una tarea imposible para una persona con conocimientos de informática a nivel de usuario.

Así las cosas, se puede apreciar que a este contenido se le categoriza razonablemente como Deep Web, sin pretender estar oculto, sino que la casuística concreta de su existencia provoca esta clasificación.

Es precisamente en este concepto de ocultación de la información, donde se definen los términos Dark Web y Dark Net.

Dark Web se utiliza para categorizar específicamente todo el contenido oculto de manera intencionada, evidenciando que Dark Web formaría parte de Deep Web o, mejor dicho, estaría contenido en ella.

Para preservar la ocultación de la información, en muchos casos hay que acceder a ella mediante redes especialmente diseñadas para esta finalidad, las denominadas Dark Net. Estas redes, además, procuran asegurar el anonimato durante su uso, protegiendo así tanto al autor o usuario como al contenido.

Para conseguir su cometido, las Dark Net disponen de su propio funcionamiento, de manera que los contenidos no se sirven a los navegadores de los usuarios mediante los métodos convencionales, sino que disponen de sus propios mecanismos de gestión y sus herramientas de acceso, de manera que un navegador común no serviría.

Aunque la base ideológica sobre la que se crearon las Dark Net fuera la de erradicar la censura, permitiendo ejercer derechos básicos como son la libertad de expresión o el derecho a la información en países donde estos derechos no solo no están recogidos, sino que incluso están perseguidos y castigados, la realidad es otra. La mayoría de ciberdelincuentes han encontrado en este tipo de redes su particular salvoconducto. Hoy en día es difícil usar este tipo de redes sin toparse con pornografía infantil, grabaciones de mutilaciones y asesinatos, venta de sustancias ilegales de cualquier tipo, contratación de sicarios, trata de blancas, etc.

En los siguientes capítulos de este documento se mostrará la forma práctica de acceso a la Deep Web mediante las Dark Net Tor, I2P e Freenet. Tres de las redes más conocidas y usadas dentro del mundo del anonimato, ya sea por cibercriminales, demostrando que este tipo de tecnología realmente funciona, o bien por ciudadanos de bien, sin ningún ánimo de lucro o beneficio más allá de la mera compartición del conocimiento.

2.2 Análisis de riesgos

Como en toda navegación por la red, ya sea la red de Internet estándar, o bien las redes anónimas comentadas en este documento, existen unos riesgos inherentes a la utilización de estos medios.

Debido a que no es el objetivo de este documento, enumeraremos algunos de los riesgos más comunes a los que se exponen las personas a la hora de navegar mediante cualquier navegador, incluso haciendo uso de la red de Internet estándar, pero extenderemos el análisis de riesgos a otros más enfocados a las redes anónimas.

2.3 Riesgos comunes actualmente para todas las redes, anónimas o no

A continuación, se describe una breve lista de los principales riesgos a los que está expuesto cualquier usuario en el momento de navegar por cualquiera de las redes descritas:

- La visualización o descarga de contenido protegido por derechos de autor será considerado delito sobre la propiedad intelectual

- La tenencia de contenido ilegal, como p.ej. el de tipo pedófilo, conllevará la aplicación del código penal

- La introducción de datos personales (direcciones de correo, logins/passwords, etc.) en formularios de contacto, sobretodo en formularios de entidades no oficiales, puede provocar robo o uso fraudulento de la información introducida

- La consulta de información mediante portales o direcciones no oficiales puede conllevar la infección del dispositivo mediante el cual se realiza la navegación, así como la red local y los demás dispositivos conectados

- Debido al apartado anterior, muchas entidades oficiales, públicas y privadas, han realizado un código de buenas prácticas para poder maximizar la seguridad durante la navegación. Estas medidas pasan por disponer de un antivirus eficiente y actualizado, desactivar las funcionalidades del navegador que no vayamos a utilizar, así como dispositivos de tipo webcam o micrófono si no van a ser utilizados, etc.

- Todas las comunicaciones deberían realizarse mediante cifrado, de manera que se evitará el protocolo de navegación http, en favor de https. Del mismo modo se debería migrar el uso de Telnet hacia SSH, etc.

- Utilizar software obsoleto o desactualizado aumentará las posibilidades de que se produzca una situación de riesgo. Disponer de las últimas versiones del sistema operativo, antivirus y navegadores maximizará la seguridad en el acceso a las redes de comunicación

2.4 Riesgos aplicables a las redes anónimas

Una vez descritos los principales riesgos existentes hoy en día a la hora de navegar por las redes de Internet estándar o Deep Web, a continuación, se describen los principales riesgos de las redes anónimas, que son realmente el objeto de estudio de este documento.

2.4.1 Uso de VPNs

Este punto es de vital importancia para el buen funcionamiento de la conexión a las redes anónimas, aunque a continuación se informará sobre la posibilidad de que las soluciones comerciales de este tipo de conexiones puedan no funcionar. En este apartado se detalla la casuística que afecta a la tunelización en las comunicaciones.

En ciertos países la conexión a redes anónimas está censurada, o por lo menos monitorizada y controlada. China es un claro ejemplo de censura aplicada a las conexiones, debido al ya conocido cortafuegos a nivel nacional (denominado Great Firewall, Chinese National Firewall, Golden Shield, etc.).

De todos modos, China no es el único país donde se practica la censura y el control sobre los habitantes. Venezuela nacionalizó CANTV, la principal operadora de comunicaciones del país en el año 2007. Des de entonces, esta operadora bloquea las conexiones a la red Tor, teniendo más del 55% de la cuota de mercado en el momento de su nacionalización.

En posteriores capítulos se describirá el funcionamiento detallado de cada una de las redes anónimas objeto de este documento, pero para hacer un adelanto y así poder entender este capítulo, es de obligado cumplimiento comentar que, para poder acceder a la red Tor, es necesario conectar con una serie de nodos iniciales de acceso, las IPs de los cuales son públicas y conocidas.

Precisamente estas IPs conocidas, son las que bloquean el Golden Shield de China o la operadora CANTV en Venezuela, inhabilitando así el acceso a la red Tor en este caso, y no son los únicos países donde se censura el acceso a Tor, sino que se exponen éstos sólo a modo de ejemplo.

Para evitar este bloqueo, se puede proceder a usar conexiones VPN hacia servidores ubicados geográficamente fuera del país donde se aplica el bloqueo, de manera que sería posible saltar el bloqueo tunelizando la comunicación mediante una comunicación cifrada. Ahora bien, este paso no es del todo eficaz, debido a que muchos ISP o cortafuegos gubernamentales, controlan también este tipo de conexiones, imposibilitando así su uso.

Por si esto fuera poco, muchas de las soluciones comerciales de VPN han sido obligadas a renunciar a ofrecer sus servicios en los países donde se les ha requerido, de manera que muchos de estos servicios no funcionarán dentro de los países donde se les ha exigido no operar, obligando así a los usuarios con suficientes conocimientos sobre el tema, a crear sus propios servidores de VPN privados o particulares.

En cualquier caso, se debería de conocer de antemano la ubicación geográfica desde donde se realizará la conexión a las redes anónimas, para así poder asegurar su uso. Muchas veces las propias herramientas necesarias para establecer las conexiones también estarán prohibidas para su descarga en los países donde se practica este tipo de censura.

En cierta manera, este apartado pretende concienciar a los usuarios de estas redes, de que será necesario un estudio previo del país desde donde se realizará la conexión, ya que puede que sea necesaria una conexión VPN para esquivar la censura, o bien incluso configurar antes un servidor de VPN particular/privado en un tercer país para poder asegurar la tunelización.

Además de todo lo comentado anteriormente referente a las conexiones VPN, otras características de la tunelización a tener en cuenta son:

- La ocultación de la IP pública de origen, publicando la del servidor del servicio VPN

- La ocultación de la información, ya que se cifra la información que viaja por el túnel VPN

Con todos estos riesgos informados, podemos concluir este apartado indicando que las conexiones VPN serán del todo necesarias para conectar con las redes anónimas, encontrando como principal escollo el hecho de que en algunos países se tengan que configurar servidores VPN particulares/privados para poder establecer un túnel fiable.

2.4.2 Inproxy y Outproxy

Las 3 redes anónimas analizadas en este documento se pueden categorizar entre dos tipos: redes inproxy o outproxy.

Outproxy significa que desde la red anónima en cuestión será posible conectarse a la red pública de Internet, como es el caso de Tor y I2P.

Inproxy implica que se trata de una red aislada, donde sólo es posible el acceso a contenidos de la propia red anónima, imposibilitando el poder consultar contenido de la red de Internet convencional.

Una vez definidos estos conceptos, se puede deducir que no tiene ningún sentido utilizar una conexión a una red anónima como Tor o I2P, para modificar un perfil personal en cualquier red social (Facebook, Instagram, Linkedin, etc.), ya que por mucha red de anonimización que se use, incluso accediendo a través de una tunelización mediante VPN, esa anonimización tendrá nombre y apellidos al consultar un perfil privado.

Será básico tener esto en cuenta a la hora de crear o modificar contenidos en la red de Internet convencional cuando se acceda mediante una red anónima de tipo outproxy. Cualquier información que permita una trazabilidad que pueda acabar identificando a personas físicas o jurídicas anulará el anonimato conseguido hasta el momento.

Un recurso utilizado por muchas de las personas dedicadas al periodismo es la creación de perfiles falsos, o bien la introducción de información falsa en cualquier formulario, así como el uso de cuentas de correo específicas para este fin.

En las redes inproxy como Freenet, aunque no exista propiamente Facebook o similares, ya que la información disponible será solo la creada dentro de la misma red anónima, tampoco es recomendable la introducción de datos reales en formularios, ni ningún tipo de información personal.

Hay que recordar que, tanto en redes inproxy como outproxy, se debe omitir la introducción de ningún dato que permita cualquier trazabilidad o identificación posible, ya que será imposible asegurar el anonimato bajo estas circunstancias.

2.4.3 Minimización estándar de riesgos

Aún y con los conceptos comentados anteriormente, existen multitud de factores que podrían llegar a identificar inequívocamente a un usuario mediante el uso de métodos más sofisticados. A continuación, describiremos algunos de los más conocidos, aunque el uso de navegadores personalizados, como Torbrowser, minimiza algunos de los riesgos descritos a continuación:

- Cookies: Este tipo de archivos de texto, imprescindibles en la mayoría de las consultas a contenido mediante navegadores, implican la recopilación de información de nuestro dispositivo, permitiendo analizar muchos parámetros tales como (sistema operativo usado, hardware, idioma, huso horario, resolución de pantalla, etc.). Toda esta información será utilizada para trazar un perfil digital que, aunque no reconozca implícita e inicialmente a una persona física, sí puede llegar a identificarla inequívocamente. A esta técnica se la conoce como Browser fingerprinting, teniendo variantes como Device fingerprinting, etc.

- Javascript: Mantener activa la ejecución de código javascript en el navegador puede llegar a implicar, como en el caso de las cookies, la recopilación no consentida de información. Además, al ser un lenguaje de programación, disfrutaría del agravante de poder realizar llamadas al sistema operativo, mediante la ejecución de código malicioso

- Plugins: Para la correcta visualización de todo el contenido, la mayoría de las veces es necesario recurrir a plugins de otros proveedores (Adobe Flash, Acrobat, etc.). Este tipo de software puede contener vulnerabilidades conocidas, de manera que el mero uso del plugin puede facilitar la apertura de puertas traseras en el dispositivo, el robo de información, etc. En el caso de no estar usando el navegador particular personalizado para cada red anónima, es imprescindible la desactivación de todo tipo de plugins durante la navegación a través de redes anónimas

- Superusuarios: Debido a las posibles brechas de seguridad comentadas anteriormente, es de obligado cumplimiento al navegar por redes anónimas, el hecho de no utilizar un usuario con permisos elevados. Es decir, el usuario utilizado para esta finalidad debe disponer del mínimo de permisos posibles, para así mitigar las consecuencias producidas por la posible ejecución de código malicioso

- Máquinas virtuales: Tal y como se comentará en el siguiente capítulo, para evitar exponer la propia máquina o dispositivo físico a los riesgos de las redes anónimas, existen los denominados entornos virtuales. Estos entornos virtuales expondrán una máquina virtual a la red anónima para que, en caso de sufrir algún ataque, impedir exponer la propia máquina física al ataque. En caso de pérdida de la máquina virtual, ésta puede ser reemplazada rápidamente por otra con las mismas características

2.5 Laboratorio para ejemplos prácticos

Acorde con las características y riesgos citados anteriormente, el laboratorio preparado para el análisis de las redes anónimas Tor, I2P e Freenet es el siguiente:

- Conexión VPN mediante Windscribe

  https://esp.windscribe.com/

  Se trata de un software propietario bajo licencia, pero en el momento de redacción de este documento, existe la posibilidad de ejecutarlo de manera gratuita bajo la limitación de algunas de sus características. Las penalizaciones más importantes al ejecutar la versión gratuita son:

  - Limitación de transferencia de datos a 10Gb mensuales
  - Limitación sobre los países de conexión de los servidores VPN

  Cabe decir que Windscribe está disponible para los principales sistemas operativos (Linux, Windows y MacOS), y también para dispositivos móviles (Android y iOS).

  Como características técnicas configurables, Windscribe permite establecer el modo de conexión manualmente, pudiendo escoger entre:

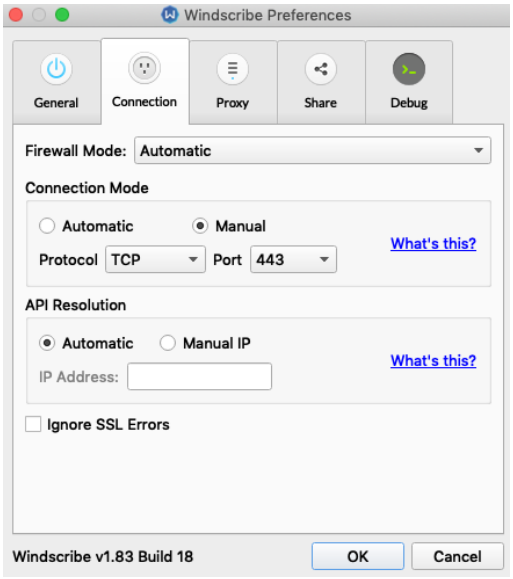
  - IKEv2, el cual es el método por defecto
  - UDP para conexiones OpenVPN
  - TCP también para conexiones OpenVPN
  - Stealth el cual es un OpenVPN encapsulado mediante TLS
  - Wstunnel el cual es OpenVPN encapsulado en WebSocket

También se puede configurar la aplicación para que pase por un proxy, lo que añadirá una capa más de seguridad sacrificando, eso sí, un poco de rendimiento en la velocidad de conexión. Para ello usaremos, a modo de ejemplo, cualquier proxy de la lista que encontramos en el portal https://free-proxy-list.net/

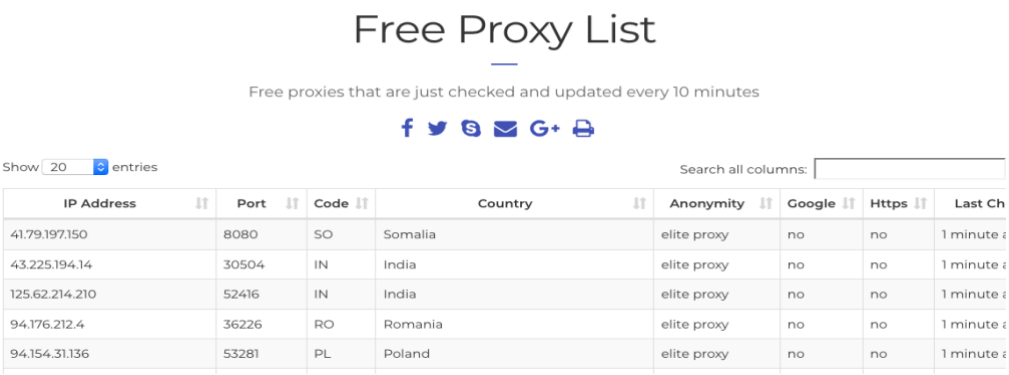
Para la finalidad que se persigue, que no es otra que cifrar el tráfico de red generado, y evitar publicar la IP pública propia desde donde se inicia la conexión, este software es suficiente.

A continuación, exponemos la configuración llevada cabo para la redacción de este documento:

Configuramos el modo de conexión en TCP y puerto 443. Esta configuración nos permitiría esquivar algunos firewalls destinados a bloquear este tipo de conexiones, aunque aún sería necesario proteger la conexión mediante TLS.

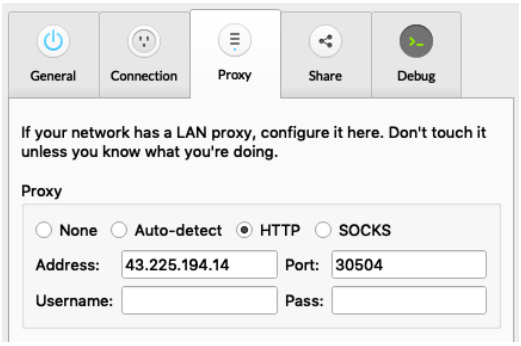


Miramos la lista de proxies disponibles:

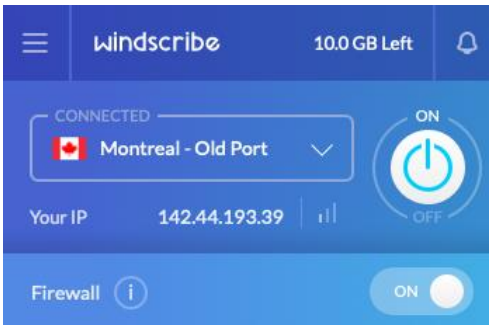


IP Address	Port	Code	Country	Anonymity	Google	Https	Last Ch
41.79.197.150	8080	SO	Somalia	elite proxy	no	no	1 minute
43.225.194.14	30504	IN	India	elite proxy	no	no	1 minute
125.62.214.210	52416	IN	India	elite proxy	no	no	1 minute
94.176.212.4	36226	RO	Romania	elite proxy	no	no	1 minute
94.154.31.136	53281	PL	Poland	elite proxy	no	no	1 minute

Y configuramos el proxy en Windscribe:



Finalmente, establecemos la conexión VPN con el servidor ubicado en el país que mejor convenga:



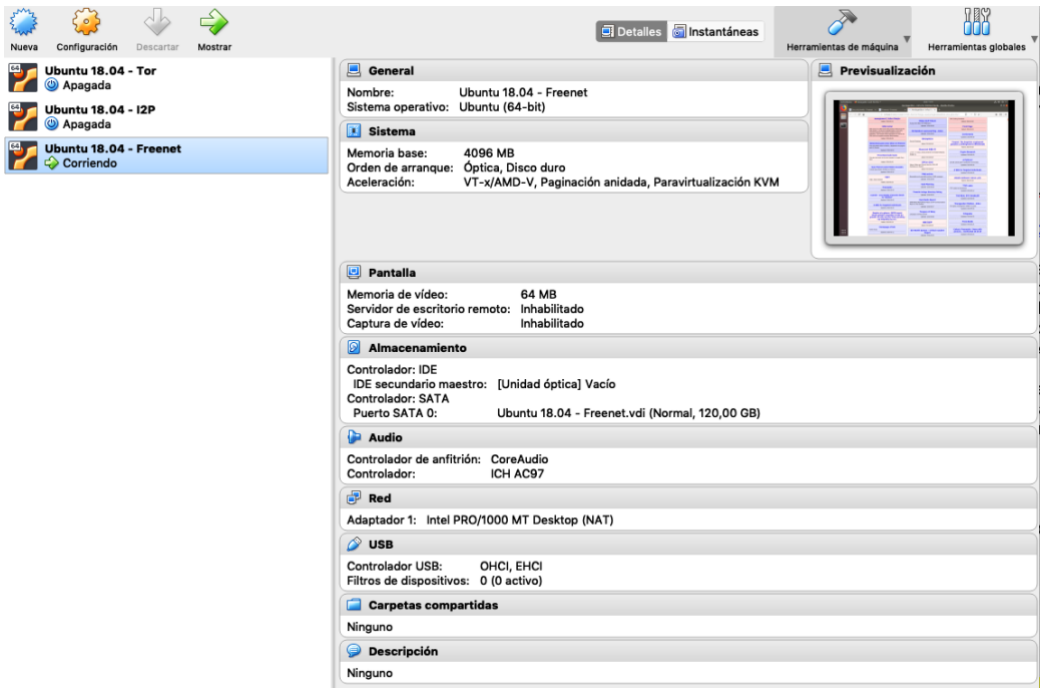
De ahora en adelante, presentaremos la IP pública 142.44.193.39, de manera que simularemos el hecho de estar conectados desde Montreal, enviando toda la información cifrada, y pasando además por un proxy ubicado en India.

- Oracle VM VirtualBox

  https://www.virtualbox.org/

  Con este software se podrá virtualizar, en un entorno doméstico, cualquier máquina de los principales sistemas operativos (Linux, Windows y MacOS). Para la demostración práctica de este documento se ha elegido la distribución de Linux Ubuntu 18.04 Desktop LTS, de manera que no se deberá disponer de licencias de software para utilizar el sistema operativo.

  Se ha creído necesaria la creación de una máquina virtual para cada red anónima, de manera que finalmente se han creado 3 máquinas virtuales con idéntica configuración:



Tal y como se muestra en la captura de pantalla anterior, la configuración utilizada para cada máquina virtual es, a grandes rasgos:

- 1 CPU de 64 bits
- 4Gb de RAM
- 64Mb para tarjeta gráfica
- 120Gb de disco duro
- Tarjeta de red Intel Pro 1000 configurada en modo NAT
- Instalación de drivers de las Guest Additions

El sistema anfitrión está compuesto por:

- CPU Intel i5 3’4GHz
- 24Gb de RAM DDR3
- Gráfica NVIDIA GForce GTX 775M con 2Gb GDDR5
- Disco sólido Crucial MX300 de 525Gb
- Conexión wifi 802.11ac
- Sistema operativo MacOS Mojave versión 10.14.1

Configuraciones adicionales a tener en cuenta:

- Para no tener que configurar Windscribe en todas las máquinas virtuales, hemos instalado este software en la máquina anfitrión, de manera que será la máquina que realizará la conexión VPN, para luego compartirla con las máquinas virtuales

- Para las personas que no estén habituadas a trabajar con entornos virtuales comentar que, al configurar la tarjeta de red de la máquina virtual en modo NAT, automáticamente se excluyen estas máquinas de la red principal, creando una red privada separada de la red anfitrión. La máquina virtual recibe una dirección IP de un servidor DHCP controlado por el propio software de virtualización Oracle VM Virtualbox, compartiendo una única identidad de red que no es visible desde la red exterior

- La instalación de la aplicación Guest Additions en la máquina virtual permitirá la interactuación entre ambas máquinas, anfitrión y virtual, asumiendo por eso una posible brecha de seguridad ante exploits, al comunicar ambas máquinas mediante un driver

3 Red Freenet

3.1 Historia y filosofía de la red de distribución descentralizada

Freenet se basa en el proyecto de final de carrera de 1999 del estudiante Ian Clarke, de la universidad de Edimburgo. Su proyecto, titulado “A distributed decentralized information storage and retrieval system”, sentó las bases para el artículo seminal de 2001 “Freenet: A distributed anonymous information storage and retrieval system”, en colaboración con otros investigadores.

Este informe sugería que Freenet podía proporcionar anonimato en Internet almacenando pequeños fragmentos de contenido cifrado, distribuidos en los ordenadores de los propios usuarios de la red, y conectándose solo a través de ordenadores intermedios que gestionen las solicitudes de contenido, tramitando estas solicitudes sin saber el contenido completo de los fragmentos.

En resumen, se describía la manera en que un grupo interconectado de nodos formaba parte de un robusto sistema de almacenamiento y recuperación, cifrado y indizado mediante claves, y sin ningún elemento central de administración, imitando así el sistema utilizado en las redes P2P.

Las características principales básicas de Freenet, y mediante las cuales se permite a los usuarios publicar información de forma anónima, son:

- Desarrollado en Java

- Multiplataforma y multilenguaje

- Dispone de almacenamiento en cache

- Dispone de una capa sólida de cifrado

- No confía en estructuras centralizadas

La versión actual a fecha de redacción de este documento es la 0.7 build 1483, con fecha 18 de noviembre de 2018, pero a partir de la versión 0.7 se reescribió buena parte del código, aportando las siguientes características:

- Posibilidad de operar en modo darknet o opennet

- Cambio de protocolo TCP a UDP

A partir de la versión 0.7.5, además, se mejoraron los siguientes aspectos:

- Uso reducido de memoria
- Inserción y recuperación rápida de contenido
- Mejoras en la interfaz web de FProxy
- Mejoras de seguridad contra: atacantes, incautación física del ordenador
- Obsolescencia de la base de datos db4o
- Interfaz con complemento Web of Trust para evitar spam
- Cambio de Java a OpenJDK

3.2 Diseño técnico y componentes

Funcionamiento general

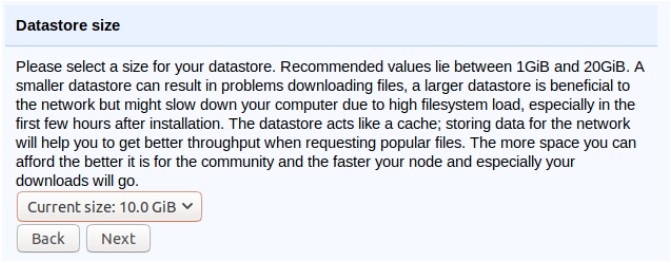
Como bien se ha comentado en el apartado anterior, Freenet imita el funcionamiento de las redes P2P, de manera que se basa en descentralizar la información, para repartirla entre los nodos disponibles que forman la red. Esta información no estará sujeta al control de ningún individuo o organización, incluyendo a los propios diseñadores de Freenet.

Almacenamiento y contenidos

El hecho de que la información esté almacenada en distintos nodos repartidos por la red, así como el cifrado de datos y las solicitudes de retransmisión de información, dificultan enormemente la posibilidad de saber qué nodo insertó el contenido, quién lo está solicitando, o dónde se encuentra almacenada la información, lo que provee anonimidad a los usuarios al mismo tiempo que esquiva de manera muy eficaz las posibles censuras.

A diferencia de otras redes P2P, Freenet no sólo distribuye la información entre los nodos, sino que la gestiona como si de una enorme cache distribuida se tratara. Es precisamente durante la instalación de Freenet donde se define el tamaño de disco destinado a almacenar este tipo de datos.

Para discos duros actuales se pueden llegar a destinar 10Gb sin llegar a tener demasiados problemas de almacenamiento, pero es posible definir espacios desde 512Mb hasta 500Gb.



Un archivo cualquiera, al almacenarse en Freenet, es dividido en múltiples bloques de tamaño reducido. Estos bloques, además, se duplicarán para poder disponer de redundancia, y pasará a almacenarse en diferentes nodos. Con este procedimiento, una persona que introduzca un archivo en Freenet puede apagar tranquilamente su ordenador al finalizar el proceso, sabiendo que su archivo ha quedado distribuido entre distintos nodos de la red, pasando a estar perfectamente disponible. Como se ha mencionado anteriormente, este aspecto maximiza anonimidad y alta disponibilidad de contenidos, pero también tiene aspectos negativos.

Al no haber nodos responsables del contenido, y disponer de una capacidad de almacenamiento limitada (por muy grande que se defina el almacén de datos), los datos que no se soliciten tenderán a ser borrados. Los usuarios generarán nuevos contenidos, que deberán ser dispersados por la red, para ser almacenados, pero en ningún caso es posible borrar datos de un almacén de datos, ni tampoco saber qué contenido está almacenado o quién es el autor, de manera que la única manera de purgar contenidos será a través de las solicitudes que reciba el propio contenido. Así las cosas, si un contenido lleva tiempo almacenado sin que nadie lo solicite, éste será borrado de los almacenes.

De la misma manera que los usuarios de Freenet desconocen qué partes de contenido almacenan en su Datastore y quién dispone de la información solicitada, al realizar una petición de información ésta nunca se retransmite directamente a la fuente de la información, sino que la solicitud será enrutada a varios nodos intermediarios, los cuales no conocen qué nodo ha realizado la petición original, ni qué nodo contiene la información a devolver. Este procedimiento resulta en un mayor ancho de banda necesario para la resolución de peticiones y transferencia de archivos, pero maximiza la anonimidad.

Sistema de red

Como se ha comentado, cuando un usuario de Freenet ejecuta el software correspondiente al acceso a la red, pasa a formar parte de la propia red. Esta relación puede llegar a ser tomando partido como nodo final, el cual almacenará información para ser retransmitida, o bien como nodo de enrutado, gestionando las peticiones de otros nodos de la red. Sea como sea, todos los nodos se intercomunican entre ellos de manera idéntica, sin distinciones de tipo cliente o servidor.

En Freenet, cada nodo solamente conoce la existencia de un número limitado de nodos, llamados vecinos, a los cuales puede acceder directamente, sin haber aquí tampoco una prioridad definida, sino que un nodo puede ser vecino de cualquier otro, sin existir una estructura jerárquica definida. Este es el concepto de red de pequeño mundo, popularizada bajo la conocida frase de que “dos personas pueden llegar a ponerse en contacto entre ellas utilizando un máximo de 6 personas intermedias”, o 6 saltos entre nodos intermedios en redes de computación.

Sin entrar en detalle en las redes de pequeño mundo, las propiedades que interesa nombrar referente a este tipo de modelos son las siguientes:

- Fenómeno de mundo pequeño: Dos nodos cualesquiera dentro de una red de mundo pequeño, se comunicarán entre ellos mediante un camino de nodos intermedio. La distancia máxima de este camino intermedio crecerá logarítmicamente según el número de nodos de la red. En Freenet la información

- Coeficiente de agrupamiento: Si dos nodos no son vecinos, de manera que no existe una conexión directa entre ambos, en las redes de mundo pequeño existe una gran probabilidad de que puedan comunicarse mediante la intervención de otros nodos

Cuando un usuario solicita información, cada mensaje es enrutado a través de Freenet, pasando de un nodo vecino a otro hasta que llegar a su destino. Aunque la localización de la información debería realizarse de forma relativamente rápida, ésta será del orden de O([log (n)]2), pero en ningún caso se garantiza que la información exista y pueda ser consultada.

Durante todo el proceso de solicitud de información, los nodos que enrutan los mensajes desconocen si van a enrutar el mensaje a otro nodo de enrutado, o si el siguiente nodo ya es el nodo final. Ni tan siquiera saben si el nodo mediante el cual han recibido el mensaje inicial es el originario de la comunicación, o bien es otro nodo de enrutado más. De esta manera se puede proteger la anonimidad de los usuarios, ya sean publicadores de información o sólo consumidores.

La única información almacenada en los nodos es la referente a los documentos asociados a sus pertinentes claves, y una tabla de rendimiento de nodos a la hora de recuperar claves distintas.

Este sistema de claves es el sistema de búsquedas utilizado por Freenet para encontrar el nodo más cercano a la información, de acuerdo con una métrica establecida basada en el número de saltos entre nodos. Asemeja al sistema de tabla de hashes distribuida ya que las claves no dejan de ser hashes.

En este tipo de sistemas no existe proximidad semántica, aunque exista proximidad de claves. Es decir, por mucho que se parezcan los contenidos, las claves que los referencian no van a tener ninguna correlación de proximidad, evitando así problemas de congestión de la red para los contenidos más solicitados.

Existen 2 tipos de claves, las CHK, o claves hash de contenido, y las SSK, o claves de subespacio firmadas, derivando estas últimas en USK o claves de subespacio actualizables, que añaden control de versiones sobre los contenidos para garantizar que las actualizaciones se realizan de manera segura, y también derivando en KSK, o claves firmadas mediante palabra clave.

Una clave CHK es un hash mediante SHA-256 del documento solicitado, de manera que esta clave CHK será única y, en caso de producirse colisiones, significará que se trata del mismo documento. Esta comprobación es muy válida para verificar que el documento recibido es el correcto, o bien no se han realizado modificaciones sobre él, al mismo tiempo que evita redundancia en los datos.

Una clave SSK es un hash basado en criptografía de clave pública mediante algoritmo DSA. Un documento insertado mediante clave SSK estará firmado por el publicador del documento, el cual obtendrá una identidad seudónima verificable por el resto de nodos. Esta identidad seudónima permitirá al publicador insertar de manera segura en Freenet múltiples documentos. Para evitar colisiones a la hora de nombrar documentos de un mismo publicador con el mismo nombre de documento, se usará la clave USK, la cual añadirá número de versión al documento, y proporcionará notificaciones de actualización. Si además queremos que el contenido sea descifrado únicamente si el solicitante conoce la palabra secreta, entonces se usará una clave de tipo KSK.

Freenet permite el funcionamiento bajo los modos Opennet o Darknet, o ambos simultáneamente. En modo Darknet, el nodo del usuario solo conectará con nodos catalogados como amigos, mientras que en modo Opennet, todos los nodos de Freenet serán válidos para conectar, aunque es posible utilizar los dos modos a la vez. El modo Darknet inicialmente carecerá de utilidad, ya que lo normal es empezar sin nodos amigos, pero a la larga será el más seguro, sobretodo ante posibles atacantes remotos.

Ya sea en modo Darknet o bien en modo Opennet, las claves referentes a solicitudes de contenido se tratan de la siguiente manera:

- Cada nodo dispone de una ubicación, la cual es definida con un número real entre 0 y 1

- Si la clave solicitada no se encuentra en el Datastore local, se genera un nuevo número entre 0 y 1 con el hash de la clave solicitada

- Se enruta hacia el nodo vecino que disponga de la ubicación que más se asemeje a la nueva clave generada

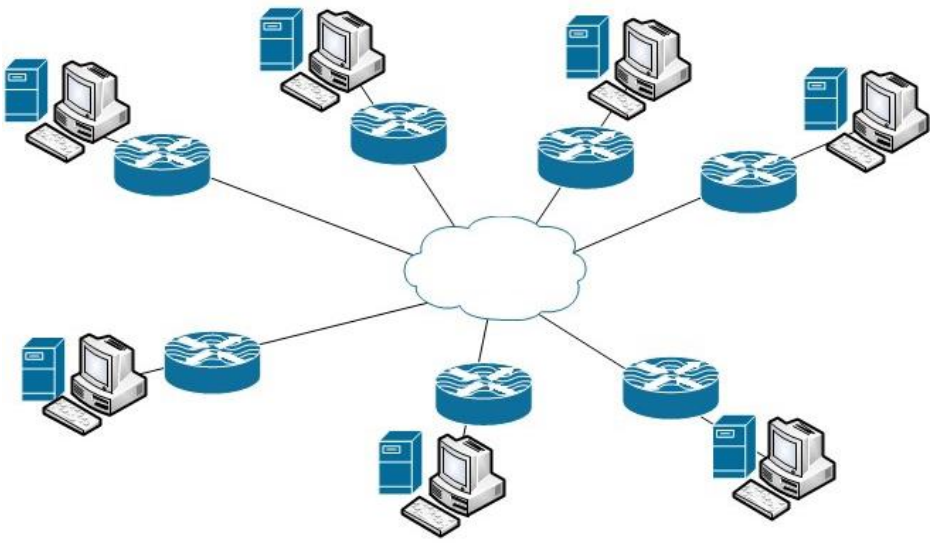
- Se repiten los pasos mientras no se superen el número máximo de saltos, o bien se encuentre la información, o bien no existan más nodos por los que pasar

En caso de que los datos hayan sido encontrados, estos se almacenan en la cache de todos los nodos de la ruta recorrida.

Para la inserción de datos se procede de la misma manera, enrutando la clave hasta agotar los saltos posibles, o bien se encuentre un documento con la misma clave, momento en que se habrá producido una colisión. En caso de que no se encuentre ningún documento con la misma clave, se almacenarán los datos en cada nodo de la ruta recorrida.

Con la forma de operar comentada, la tendencia de la red será que los nodos cercanos verán incrementada su cercanía, y los nodos lejanos cada vez estarán más distantes, además de que informaciones diferentes pero con claves similares serán almacenadas en un mismo nodo, dando lugar a una estructura distribuida y agrupada en clústeres donde los nodos tiendan a contener elementos de datos cercanos dentro de un espacio de claves.

Estos clústeres se repetirán a lo largo de la red, dependiendo del tipo de datos almacenados. Los datos menos solicitados serán almacenados en nodos específicos o especializados en este tipo de contenido, generando agrupaciones de clústeres, mientras que los datos más solicitados serán ampliamente difundidos por la red, siendo almacenados constantemente en las cachés locales de los nodos, rompiendo así el agrupamiento de los clústeres.



Interfaz de usuario

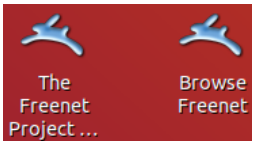
La herramienta básica de gestión del software Freenet se llama FProxy. Esta herramienta se instala con el software proporcionado por la página oficial de Freenet, y ejecutará un servicio que permitirá acceder a Freenet desde cualquier navegador.

A fecha de redacción de este documento, Freenet recomienda casi cualquier navegador excepto Internet Explorer, aunque recomienda configurar y personalizar el navegador para maximizar la anonimidad.
Para evitar configurar el navegador mediante el que habitualmente se usa para navegar por la web convencional, Freenet proporciona un navegador ya personalizado listo para su uso, y con las principales funciones de configuración y navegación incluidas.

3.3 Herramientas y ejemplo práctico de uso

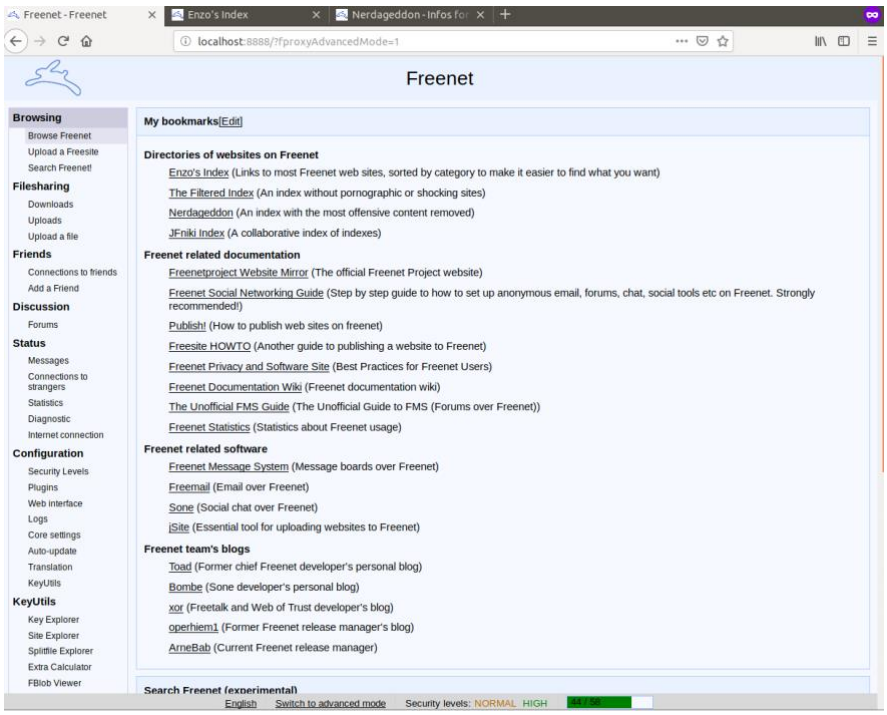
En la página oficial de Freenet existe diversa documentación referente a la instalación y primeros pasos, pero aún y así, Freenet tampoco provee demasiadas funcionalidades.

Una vez instalado el software, dispondremos de los siguientes iconos en el escritorio de nuestro ordenador:



El icono “The Freenet Project” llevará únicamente a la web oficial del proyecto, para poder consultar documentación o cualquier otra gestión.

El icono “Browse Freenet”, después de preguntar algunos datos en caso de que sea la primera vez que se abra la aplicación, mostrará la siguiente página inicial:

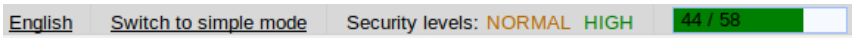


Cabe decir que inicialmente, incluso el navegador proporcionado por Freenet, que no es otro que una personalización de Firefox, arranca sin el modo de navegación privada activado, para no almacenar las URL que se vayan visitando. Esta característica la recomienda Freenet, pero no la incluye en el modo de navegación por defecto del navegador que trae incorporado.

Antes de dar los primeros pasos en Freenet, es recomendable ajustar algunos parámetros de seguridad, aún estando en modo Opennet, como pueden ser establecer los niveles de seguridad contra posibles atacantes en “Normal”, y proteger descargas, subidas y cache de navegación mediante una contraseña, de manera que se alcance el nivel de seguridad “High” en este aspecto.

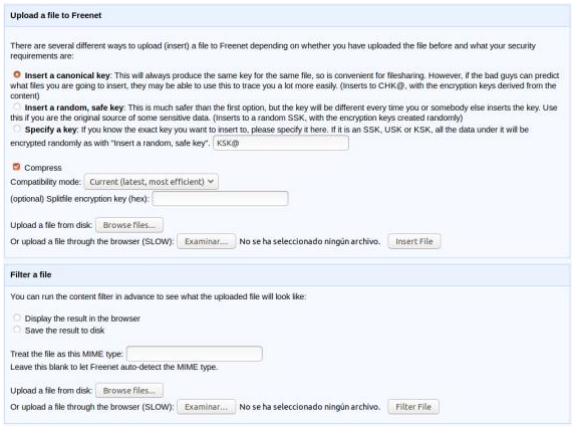
Para las personas más entendidas es posible activar el modo avanzado, donde no solo se habilitarán nuevos menús para personalizar del todo la configuración, sino que se añadirán opciones a los menús ya existentes en el modo simple.

Estas últimas características las podemos encontrar en la parte inferior de la ventana del navegador:



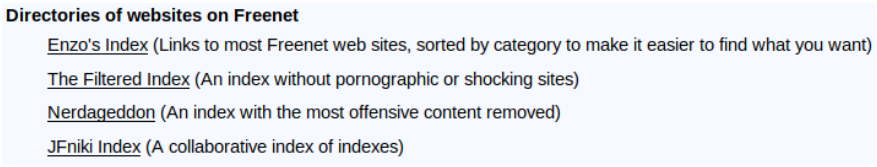
Como primeros pasos, si lo que se busca es compartir información, se puede acceder al apartado “Filesharing”, disponible en el menú de la izquierda del navegador.

La captura anterior muestra las opciones disponibles para la opción de menú “Upload a file” mediante la configuración simple. Si activamos el modo avanzado obtendremos las siguientes opciones:

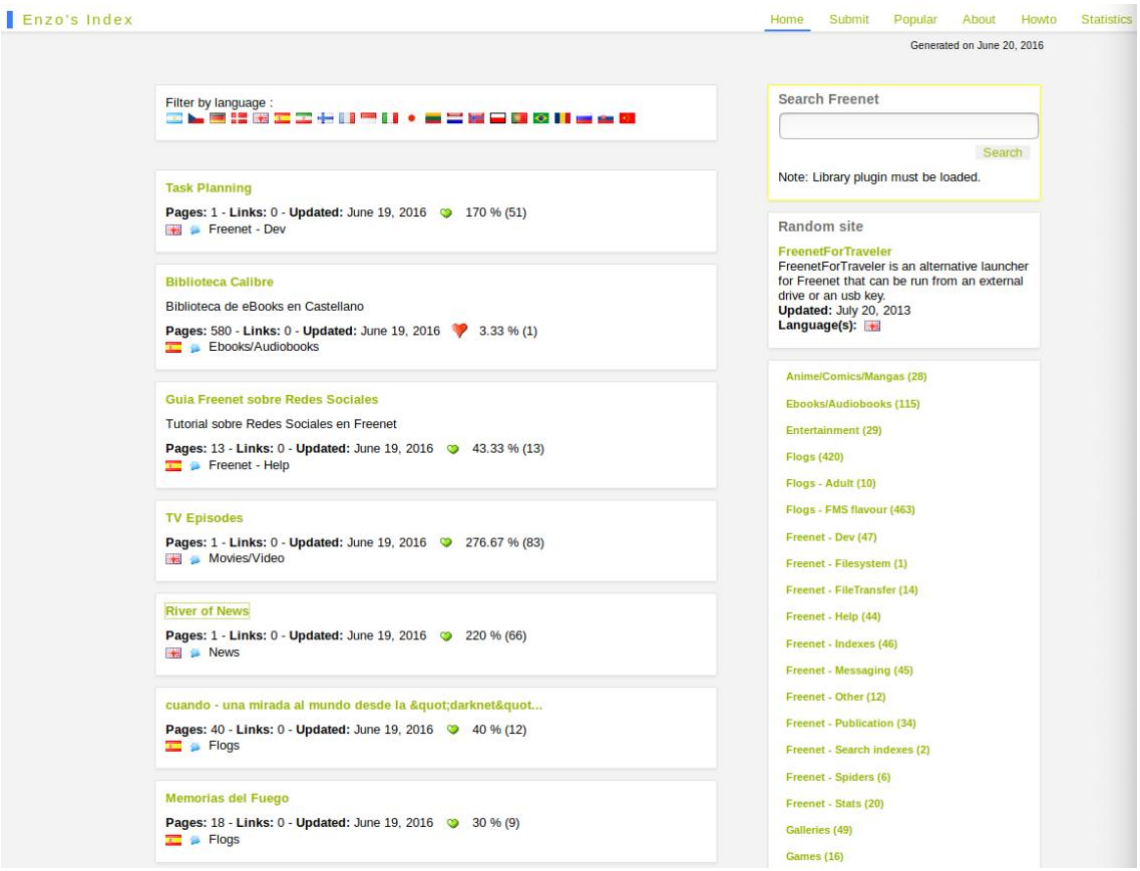


Tal y como se puede apreciar, el menú avanzado realmente permite una mayor parametrización de la aplicación.

Suponiendo un acceso a Freenet para descargar información, en vez de acceder para subir contenidos, si no se sabe muy bien por donde empezar, siempre es posible acceder al apartado “Browse Freenet”, donde se mostrará una lista de páginas para visitar, las cuales contendrán información a modo de directorio.



Una visita a la web de Enzo dará una idea del tipo de páginas que tiene enlazadas, pudiendo ver las entradas de distintas categorías en el menú de la derecha:



Al escoger la categoría Movies/Video se puede acceder a contenido ilícito, como en la mayoría de portales de este tipo:

TV episodes in the past week

Date	Magnet link	Freenet key	Torrent Name
2018-11-27 01:00	D13575AA5EBDDF9AE6C48D9933B2283E023DC968		Frankie.Drake.Mysteries.S02E10.WEBRip.x264-TBS[rartv]
2018-11-27 01:00	18DC64BEC9BDF849CF2BA9DCF63AFAFF18E87C9C		Murdoch.Mysteries.S12E09.WEBRip.x264-TBS[rartv]
2018-11-27 01:00	D40352301F103A7AC87D475FED2D636ACBF39EC7		The.Resident.S02E09.WEB.x264-TBS[rartv]
2018-11-27 00:00	213A6B4FE424F74AC35951F900F3597E81DB389C		Dream.Corp.LLC.S02E11.HDTV.x264-MiNDTHEGAP[rartv]
2018-11-27 00:00	9AB1413216CDB52C85CB4C290CE5A5118CFCE8F9		Dream.Corp.LLC.S02E12.HDTV.x264-MiNDTHEGAP[rartv]
2018-11-27 00:00	D44E7D1822E37C6FC669A696E9AEC4EBCA82C453		People.Just.Do.Nothing.S05E03.HDTV.x264-RiVER[rartv]
2018-11-26 23:00	59AAFA68DFBFE35166EEF43EF779D3D751DD1909		Im.A.Celebrity.Get.Me.Out.Of.Here.S18E09.HDTV.x264-PLUTONiUM[rartv]
2018-11-26 22:00	77BCDF1459A3521B39EF61A513A7F8DC0CBD46DE		90.Day.Fiance.S06E07.WEBRip.x264-TBS[rartv]
2018-11-26 22:00	710842B44A5DFB9B79E1E6731683C4C23CF7FA38		My.Lottery.Dream.Home.S05E09.Athol.Family.Dream.Home.HDTV.x264-CRiMSON[rartv]
2018-11-26 19:00	8DEF2210B101EC1AC0207BD2A02C9449EE4BF65A		House.Hunters.S173E01.Moving.Back.Home.for.the.Holidays.WEB.x264-CAFFEiNE[rartv]
2018-11-26 19:00	834964A8B20ED299D43A0471BF87A48B4BADB019		Mythical.Beasts.S01E07.Dark.Secrets.of.the.Sphinx.WEBRip.x264-CAFFEiNE[rartv]
2018-11-26 17:00	A2116D00A507CCC2793FF8F8730EA6B7DEE2D681	CHK	Talking.Dead.S09E08.WEB.h264-TBS[rartv]
2018-11-26 16:00	3CA7D417B84256A26B05AD098F961203F7ABD871	CHK	Criminal.Confessions.S02E08.WEB.x264-WEBSTER[rartv]
2018-11-26 16:00	682A2B3291282EF9017AFD1588B8CA080E0B3B1D		Snapped.S24E14.Marie.Strickland.WEB.x264-WEBSTER[rartv]

También es posible encontrar mirrors de webs pertenecientes a otras redes anónimas, como puede ser la Hidden Wiki de Tor, aunque el Mirror data de 12 de enero de 2014.

Para finalizar, hay que comentar que existen varios programas para sacar el máximo provecho de Freenet, y que pasamos a comentar a continuación:

- Sone → Intenta ser una red social, pero se asemeja más a un Foro. Sea como sea, este plugin permite compartir contenido multimedia, así como postear comentarios esperando ser respondidos. Requiere de la instalación del plugin Web of Trust para funcionar

- jSite → Sirve para crear webs propias dentro de Freenet. Existe mucha información sobre cómo crearlas

- Freemail → Servicio de correo a través de Freenet, aunque parece que está sin mantener desde 2016

- Freenet Message System → Foro en Freenet

- Toad, Bombe, xor, operhiem1 → Blogs de diversas temáticas

3.4 Debilidades y/o vulnerabilidades de Freenet

Al tratarse de una red InProxy, no padece la mayoría de las vulnerabilidades de las otras redes anónimas. Aún y así, las vulnerabilidades más conocidas son las siguientes:

- Archivos con código malicioso incorporado → Al tratarse de una red de compartición de archivos, resulta muy fácil descargar contenido con código malicioso. Más aún cuando el contenido a buscar resulta del tipo ejecutable. Para esta vulnerabilidad no hay más solución que el sentido común, ya que es una vulnerabilidad existente en la red de Internet convencional. No es recomendable ejecutar aplicaciones o archivos de orígenes desconocidos

- Plugins programados por terceros con código malicioso → Freenet permite programar plugins personalizados en Java. Un usuario mal intencionado podría llegar a programar un plugin, o modificar uno existente, para distribuirlo entre los usuarios de Freenet y así infectar al máximo de personas posible. La solución es la misma que en el apartado anterior, no debiendo instalar plugins de fuentes no conocidas o no oficiales

- JavaScript, Cookies, XSS, XSRF, etc. → Como en la mayoría de los ataques contra navegadores, una mala configuración de este puede provocar que los ataques de estas características surjan efecto. Para evitar este escenario, la mejor manera de esquivar los ataques, o de que resulten inofensivos, será utilizar navegadores independientes para navegar por redes anónimas, o bien usar la configuración de máquina virtual para esta finalidad, de manera que nunca se vea comprometida la máquina física

- Un usuario de Freenet puede estar almacenando contenido ilícito sin saberlo, ya que no es capaz de descifrar el contenido de su Datastore, aunque ese mismo argumento puede usarse para no tener que responsabilizarse del contenido almacenado

3.5 Resumen analítico de la red Freenet

Freenet es una plataforma de software que permite a los usuarios compartir y publicar anónimamente contenido, así como navegar por los Freesites que proporciona la plataforma.

Se trata de una red de tipo InProxy, de manera que sólo se va a poder acceder a contenido dentro de la misma red, sin la posibilidad de mostrar contenido de Internet ni de otras redes.

La idea principal de Freenet es la de construir una red de comunicación resistente a la censura. Como se verá en siguientes capítulos, Freenet sigue muchos de los mecanismos de otras redes anónimas como I2P y Tor, tales como el cifrado de las comunicaciones para ocultar contenidos y el enrutado a través de varios nodos para dificultar el rastreo.

Cada usuario de Freenet contribuye a la propia red proporcionando ancho de banda y espacio de almacenamiento de disco duro para el conocido Dataset.

Los datos del Dataset se almacenarán o se descartarán dependiendo de su popularidad. A más accesos solicitados, durante más tiempo quedará almacenado un archivo, de manera que los contenidos menos populares se descartarán en favor de los nuevos que se vayan generando.

A grandes rasgos, Freenet es un repositorio de almacenamiento descentralizado, ya que se trata de una base de datos replicada entre los Datastores de los nodos que la conforman.

4 Red Tor

4.1 Historia y filosofía del enrutamiento de cebolla

Tor quizá sea la red anónima más conocida, ya sea debido tanto por su uso como por su abuso. Su nombre es un acrónimo de The Onion Router y redirige el tráfico de Internet a través de una red de relays para ocultar la ubicación y el uso de Internet de los usuarios a las personas o entidades que analizan el tráfico, dificultando así el rastreo de actividades.

Tal y como sucedía en Freenet, Tor fue creado para proteger la privacidad personal de los usuarios, así como la libertad y confidencialidad en las comunicaciones.

Creado en 2003 por el actual líder del proyecto, Roger Dingledine. Esta red resultó ser una evolución del Onion Routing del Laboratorio de Investigación Naval de los Estados Unidos. De finales de 2004 a finales de 2005 fue patrocinado por Electronic Frontier Foundation. Actualmente The Tor Project, una ONG orientada a la investigación y educación ubicada en Massachusetts mantiene vivo el proyecto Tor.

A diferencia de Freenet, no se trata de una red P2P, donde todos los nodos son tratados de la misma forma, sino que en Tor existen usuarios, encaminadores y servicios de directorio. Aún y así la red Tor, como Freenet, también funciona a través de un conjunto de organizaciones y usuarios que ceden o donan su ancho de banda y poder de procesamiento.

A fecha de redacción de este documento, Tor está compuesto por más de 7000 encaminadores, de los cuales se rumorea que la mayoría pertenecen a FBI, CIA, NSA, y otras agencias de seguridad norteamericanas, llegando incluso a acuerdos con países como China, Irán o Rusia. Hay quien asegura que The Tor Project se está financiando mediante el gobierno de los estados unidos, de manera que no se puede asegurar el anonimato.

4.2 Diseño técnico y componentes

Funcionamiento general

A diferencia de Freenet, Tor permite tráfico InProxy y OutProxy. Esto significa que desde Tor es posible visitar páginas web de la red de Internet convencional, además de acceder a los servicios ocultos dentro de la propia red Tor.

Para el tráfico OutProxy, el objetivo de Tor es el de reducir las posibilidades de que una persona pueda ser rastreada. Aunque no se ha conseguido este objetivo completamente, para lograrlo Tor cifra las comunicaciones para posteriormente enrutarlas a través de una red de reenviadores ejecutados por voluntarios de todo el mundo. Los reenviadores utilizan el cifrado a modo de multicapa, de ahí la metáfora con la cebolla, para poder asegurar el secreto en las comunicaciones entre enrutadores. El único momento en el que se envía la información sin cifrar, es cuando la solicitud sale de la red Tor por el último reenviador, para llegar a su destino. Aún y así, en ninguna parte del recorrido se ha mostrado la IP del remitente, así que cualquiera que escuche el canal de comunicación en cualquier punto a lo largo del camino será incapaz de identificar directamente al remitente. Para el destinatario de la información, el originador de la comunicación será el último nodo Tor, el de salida.

Para el tráfico InProxy, Tor puede proporcionar anonimidad para ambas partes, remitente y destinataria. Los servicios ocultos de Tor son accesibles a través de direcciones ".onion", de manera que no se utiliza el sistema convencional de resolución de nombres DNS para así poder resguardar la anonimidad. Tampoco existe una lista donde se puedan consultar todos los servicios ocultos de Tor, demostrando su descentralización.

Por último, el hecho de que para acceder a un servicio oculto se deba pasar exclusivamente por la red Tor, implica que la conexión quede cifrada de extremo a extremo, sin estar expuesta teóricamente a escuchas ilegales.

Almacenamiento y contenidos

A diferencia de Freenet, donde los contenidos se repartían entre los nodos que formaban la misma red, en Tor la información se encuentra:

- Para los casos InProxy, en los servidores que ofrecen los servicios ocultos. En breve se realizará una demostración de cómo acceder a servidores que ofrecen servicios ocultos dentro de la red Tor

- Para los casos OutProxy, en los servidores convencionales. Aquí encontraríamos cualquier servicio accesible mediante un navegador

Además de estos dos casos, también es posible acceder a cualquier información mediante esquema cliente-servidor siempre y cuando la conexión hacia el servidor pueda llegar a pasar por un Proxy que acepte conexiones SOCKS.

A modo de ejemplo típico de este tipo de conexiones, existen los conocidísimos servidores IRC, o bien de mensajería instantánea. Enviando la información mediante un Proxy SOCKS a través de Tor, se consigue anonimizar la conexión y cifrar el contenido durante el envío, hasta llegar al nodo de salida de la red Tor.

En caso de que la aplicación que queramos anonimizar no soporte SOCKS, siempre se puede hacer uso de herramientas como “Torify” para Linux, o bien “SocksCap” para Windows.

Sistema de red

Antes que nada, es importante indicar que Tor sólo intentará anonimizar tránsito de tipo TCP. Cualquier otro tipo de tránsito deberá seguir su curso normal, sin pasar por esta red anónima, ya que ésta será incapaz de gestionarlo.

Toda la red Tor puede resumirse de manera muy genérica en dos tipos de componentes o nodos:

- Onion Proxies: Se trata de los dispositivos de los usuarios finales que estén ejecutando el software de Tor en ese momento. Este software, de manera transparente a los usuarios, accederá a los servicios de directorio, atenderá las aplicaciones de usuario y gestionará los circuitos aleatorios dentro de la red Tor, multiplexando los flujos de datos hacia la red de enrutado de Tor, y cerrando las conexiones donde finalicen los temporizadores definidos sobre ellas o bien finalice el flujo de datos

- Onion Routers: Disponen de varias funcionalidades, ya que pueden ser simples encaminadores o, adicionalmente, ofrecer servicios de directorio. Entre ellos se establecerán conexiones TLS, cerrándose solamente en caso de inactividad.

  El servicio de directorio ofrece una base de datos con conocimiento de la red tanto a nodos de tipo proxy como a nodos de tipo encaminador. Para evitar caídas del sistema debidas a fallos en los nodos que ofrecen servicios de directorio, esta base de datos se replica constantemente entre los nodos de encaminamiento que ofrecen este servicio.

Un nodo encaminador tiene que considerarse confiable para que pueda ofrecer servicios de directorio. Esta confianza se gana a través de la aprobación de un proceso manual que realizan los administradores del servidor de servicios de directorio. De esta manera se evita la aparición de nodos no confiables y así posibles ataques desde este tipo de servidores. Todo nuevo nodo de encaminamiento deberá ser aprobado manualmente para así garantizar la fiabilidad de la información del servicio de directorio.

Tal y como se ha descrito anteriormente, las dos principales modalidades de uso son el modo InProxy y el modo OutProxy.

- OutProxy → Es el modelo de conexión más sencillo y, por consiguiente, menos seguro. Aún y así maximiza la anonimidad sacrificando rendimiento, ya que se pierde cierto ancho de banda por el paso a través de los reenviadores. En esta modalidad, usada a modo genérico, se gana una capa de seguridad a la navegación tradicional, si bien es cierto que toda anonimidad se pierde al acceder mediante un usuario privado a portales de tipo redes sociales, servicios en la nube (Amazon, Google, Microsoft, etc.).

- InProxy → Es el modelo más complejo y seguro, al establecer cifrado extremo a extremo durante la comunicación. Para este tipo de comunicación, se necesitan varios elementos exclusivos a la red Tor, como son la tabla de hashes distribuida o el nodo con función de punto de encuentro.

Para el modo OutProxy, o cuando no se solicita el acceso a un servicio oculto de Tor, sino que lo que se pretende es anonimizar una conexión a un servidor de la red internet convencional, el procedimiento de conexión es el siguiente:

- Se establece un circuito de 3 nodos de encaminamiento según la configuración de TorBrowser y del resultado devuelto por el servicio de directorio al consultar la lista de nodos disponibles

- El propio software TorBrowser, realizando la función de onion proxy comentada anteriormente, negocia las claves de cifrado con todos los nodos encaminadores del circuito a establecer. Para cada nodo del circuito se establecerán 2 claves simétricas, una de envío y otra de recepción de datos

- TorBrowser cifrará los paquetes con la información empezando por la clave del último nodo del circuito, ya que se descifrará la información de manera secuencial, y terminando por cifrar con las claves del primer nodo del circuito, simulando así una cebolla debido a las diferentes capas de cifrado

- Enviará la información al primer nodo del circuito, también llamado “Entry Node”, el cual sacará la primera capa de cifrado ya que dispone de las claves para poder realizar este paso y enviará la información al siguiente nodo del circuito, que también será capaz de sacar la siguiente capa de cifrado debido a que conocerá las claves de descifrado. Este proceso se repetirá para los 3 nodos del circuito, de manera que el último nodo, o también llamado “Exit Node”, sacará la última capa de cifrado y entregará el paquete al servidor de destino

Para el modo InProxy, es decir, para acceder a un servicio oculto, el procedimiento de conexión es diferente al comentado anteriormente, pasando a ser el siguiente:

- Antes que nada, hay que indicar que el servicio oculto tiene que estar publicado en una tabla de hashes distribuida. Este paso lo llevará a cabo el servidor que ofrece el servicio, mediante una metodología de clave asimétrica pública/privada con los nodos de entrada para conseguir finalmente un descriptor, que será cargado a la tabla hash distribuida. El descriptor será encontrado por los clientes que soliciten la dirección ".onion" derivada de la clave pública del servicio comentado

- Una vez publicado, el servidor que aloja el servicio oculto preguntará a algún nodo de encaminamiento si éste puede ser su "Introduction Point", o nodo de entrada a su servicio oculto. Si el nodo acepta, se creará un circuito permanente entre el nodo encaminador y el servidor que ofrece el servicio oculto. Este circuito sólo podrá ser destruido si una de las dos partes reinicia sus conexiones, o bien decide unilateralmente romper el circuito. Debido a estas posibles causas de rotura de circuitos hacia servicios ocultos, para garantizar la actividad de estos, pueden existir múltiples nodos de entrada para un mismo servicio oculto

- Una vez establecidos los nodos de introducción hacia los servicios ocultos, el propio servidor que aloja estos servicios solicita publicar en el servicio de directorio la información de contacto de su servicio oculto. Una vez publicado en el servicio de directorio, el servicio estará listo para recibir peticiones de clientes

- Cuando un cliente solicita acceso al servicio oculto mediante el servicio de directorio, se le entrega la información del servicio, incluida la dirección del nodo de introducción

- Una vez el cliente dispone de la información del servicio oculto, éste solicitará a un nodo de encaminamiento que realice la tarea de punto de encuentro o "Rendezvous Point". Se repetirá solicitud las veces que sean necesarias a diferentes nodos hasta que un nodo acepte, momento en el cual se establecerá un circuito entre el cliente y el punto de encuentro. Este circuito entre cliente y punto de encuentro estará formado por 2 o 3 nodos de encaminamiento para garantizar el cifrado y la anonimidad en todo momento, como sucede en los circuitos OutProxy. El nodo de punto de encuentro realizará las conexiones directamente contra el servidor que aloja el servicio oculto

- El cliente informará al nodo de entrada o "Introduction Point" de qué nodo hará de punto de encuentro entre el servicio oculto y el cliente

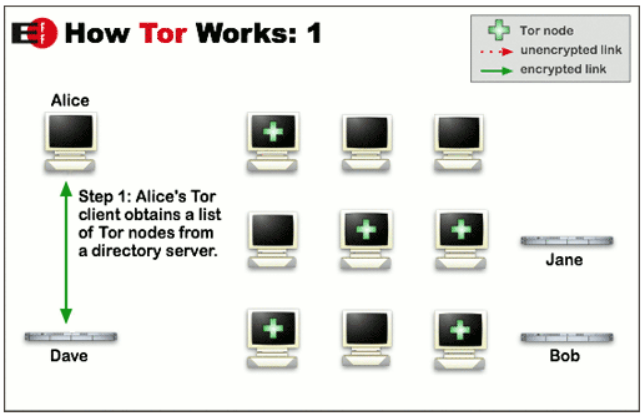
- El nodo de entrada, a su vez, informará al servidor que aloja el servicio oculto sobre el nodo de punto de encuentro

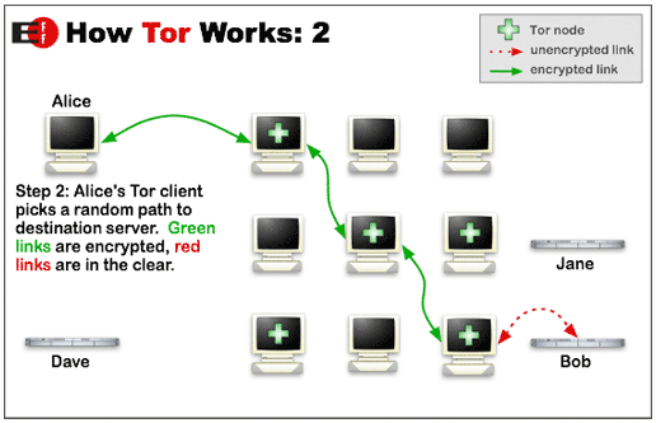
- Llegados a este punto, el servidor puede decidir si establece un circuito o no con el punto de encuentro. En caso afirmativo, el servidor establece el circuito, pasando otra vez por 3 nodos de encaminamiento desde el servidor hasta el punto de encuentro, y solicita mantener el circuito activo a la espera de solicitudes

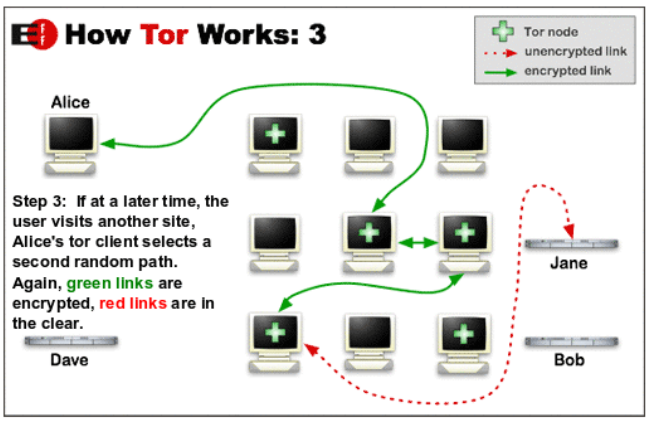
- El nodo de punto de encuentro informa del establecimiento del circuito al cliente, y éste puede proceder al envío de solicitudes y información

Para entender mejor los conceptos InProxy y OutProxy, se adjuntan unas imágenes sacadas de la web oficial, que muestran de manera muy gráfica el funcionamiento de ambos sistemas.

Modo OutProxy:







Modo InProxy:

La secuencia de números marca el orden a seguir para establecer la comunicación con el servicio oculto.

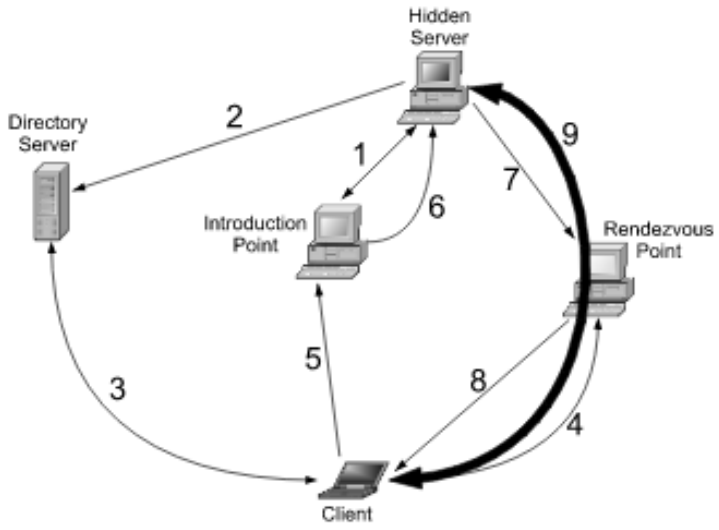


Figure 1. Normal use of hidden services and rendezvous servers

Interfaz de usuario

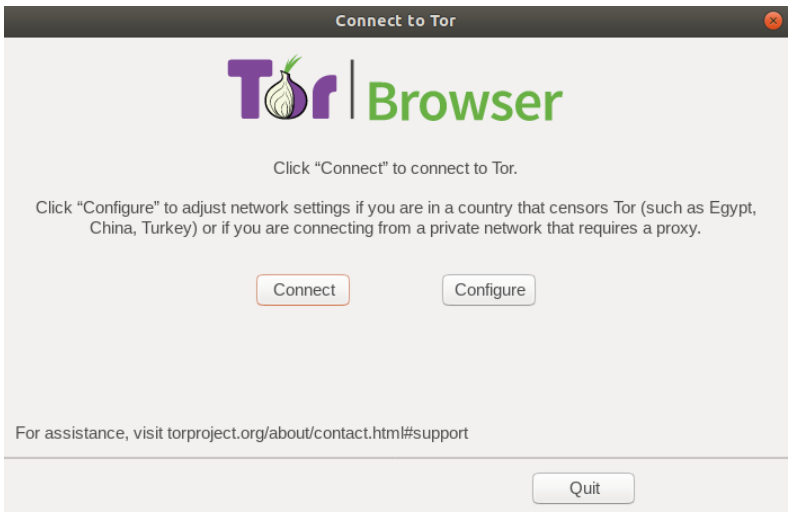
Como en Freenet, la interfaz de usuario de Tor es un navegador. La web oficial de Tor ofrece Tor Browser, un navegador ya configurado con los parámetros necesarios para acceder a esta red. El navegador utilizado está basado en Firefox, como en Freenet.

La versión oficial de Tor Browser a fecha de redacción de este documento es la 8.0.3, y está basada en Firefox 60.3.0.

También como en el caso de Freenet, existe la posibilidad de escoger otros navegadores, y configurarlos manualmente para conectar con Tor mediante la instalación de plugins, pero para el objetivo de este documento se ha creído conveniente mostrar la herramienta oficial.

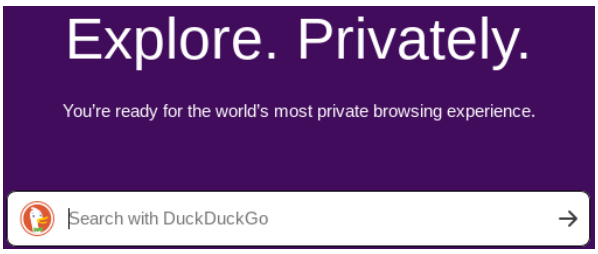
4.3 Herramientas y ejemplo práctico de uso

Una vez descargada la aplicación Tor Browser de la página oficial de Tor, nos encontramos con un par de configuraciones iniciales:



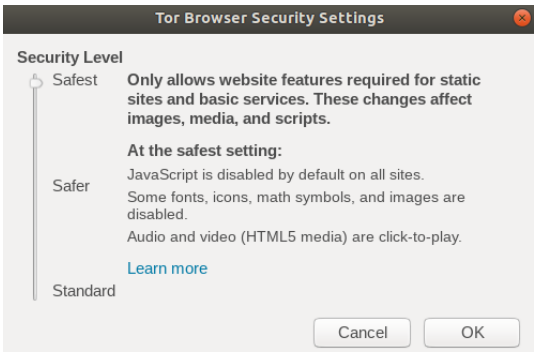
Nos ofrece la posibilidad de esquivar la censura si nos encontramos en países donde existe la prohibición explícita conocida sobre la conexión a este tipo de redes anónimas, o bien conecta directamente a Tor.

Si conectamos, el navegador realizará unas comprobaciones previas, para terminar mostrándonos una página inicial donde podremos realizar búsquedas mediante el motor de búsqueda DuckDuckGo:



En este buscador se mostrarán resultados de ambas redes, Internet y Tor. La mayoría de resultados, a fecha de redactado de este documento, pertenecen a la red de Internet convencional.

Antes de explorar la red Tor, es recomendable configurar los parámetros de seguridad a niveles máximos para que no haya scripts alojados en las páginas por las que se navegue, que permitan recabar información sobre la máquina, navegador, etc.



Para evitar la ejecución de scripts es recomendable situar el nivel de seguridad al máximo, de manera que se bloquearán absolutamente todos los scripts, lo que provocará errores o incluso la imposibilidad de funcionamiento de muchas páginas, sobretodo las de la red de Internet convencional.

Debemos recordar en todo momento que, aunque se trate de un navegador Firefox personalizado, nos encontramos navegando a través de una red anónima OutProxy. Podemos realizar la comprobación mediante cualquier página que nos indique qué IP pública presentamos para, sabiendo que estábamos en un servidor de Canadá, poder comprobar que estamos presentando otra IP pública.

Hay que recordar que partíamos de esta IP:

Y que ahora mismo tenemos esta:

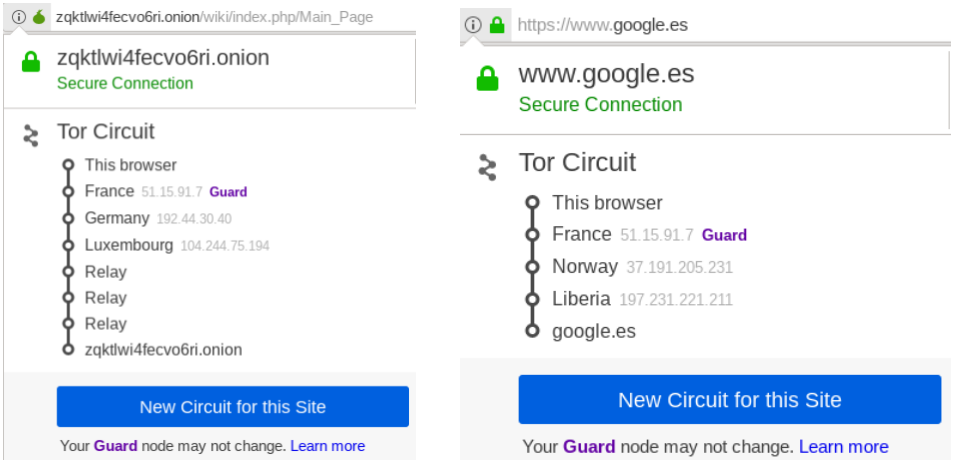
Your Public IP Address Is:

195.176.3.19

Country:	Switzerland
Region:	Basel-Stadt
City:	Basel
Latitude:	47.5584
Longitude:	7.57327

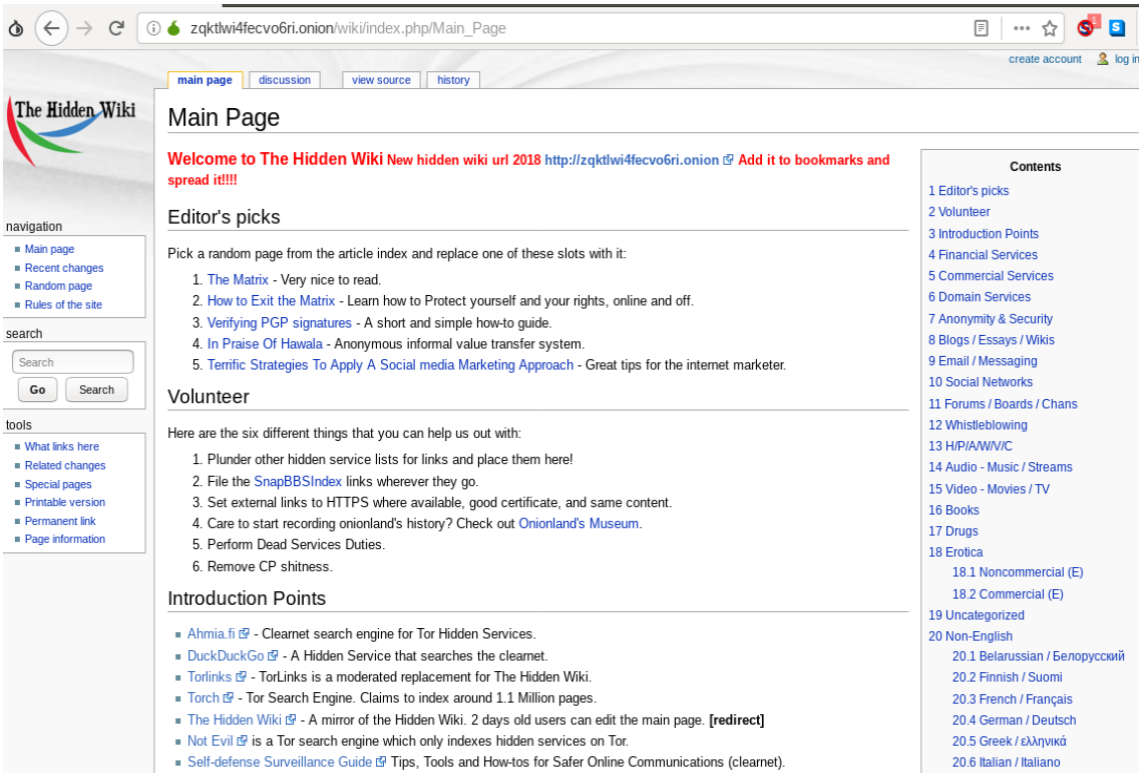
De esta manera queda comprobado que estamos navegando a través de la red Tor, y que el último nodo reenviador, el que será el nodo de salida de la red, se posicionará como el originario de la comunicación, de ahí la dirección IP mostrada.

Además, es posible consultar los nodos o camino utilizado para llegar a un servicio oculto, o a una web OutProxy en particular:



Si no parece correcto el circuito utilizado, siempre existe la posibilidad de cambiarlo, sólo para ese destino, haciendo clic en el botón azul. Al hacer clic nos establecerá otro circuito de nodos para llegar a la misma destinación.

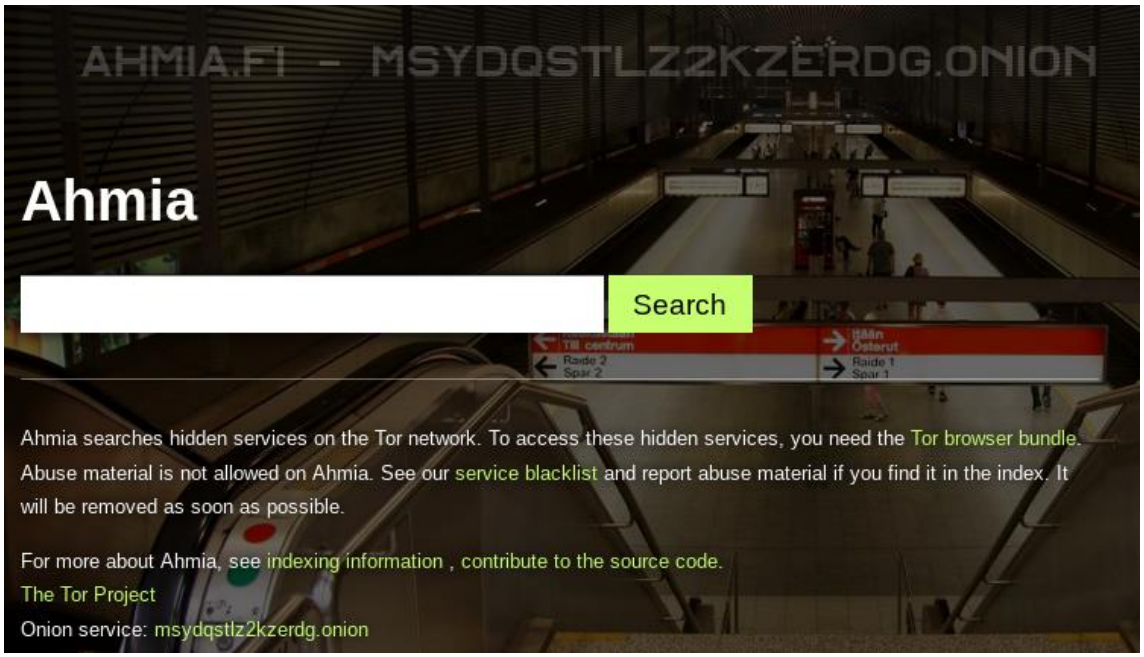
Una vez demostrado el enrutado para navegación OutProxy, pasamos a mostrar la navegación InProxy. Al no existir un listado completo con todos los servicios disponibles dentro de Tor, un lugar de partida común suele ser la Hidden Wiki:



Con una presentación visual imitando la Wikipedia, de ahí su nombre, la Hidden Wiki es un primer listado de los servicios ocultos más conocidos, categorizado por idioma, productos y/o servicios, etc. Aún y no contener la totalidad de servicios ocultos existentes en Tor, el listado es realmente abultado, pudíendose ampliar si se visitan otras páginas de directorio anunciadas en la propia Hidden Wiki, como pueden ser: Ahmia, Torlinks, Torch, etc.

Como en todas las redes anónimas, el apartado visual de los servicios ocultos recuerda a las primeras páginas web allá por la década de los 90. Este hecho radica en la caída de rendimiento que provoca el hecho de estar constantemente enrutado a través de los nodos, y de ahí que se pongan en marcha webs con poco contenido, como en la época donde no se disponía de demasiado ancho de banda para las comunicaciones.

La finalidad de Ahmia, junto con muchas otras páginas de servicio de directorio para servicios ocultos, es indizar contenido que no contenga pornografía infantil, animando además a los usuarios que encuentren contenido de este tipo, a denunciar los hechos.



4.4 Debilidades y/o vulnerabilidades

Como se ha comentado anteriormente, Tor es la red anónima más usada. Eso resulta en que dispone de un mayor número de desarrolladores ampliando la red y parcheándola, pero también en un mayor número de personas y entidades intentando vulnerar su seguridad.

Aunque la mayoría de las vulnerabilidades más importantes se encuentran en agujeros observados en software de terceros, o bien en el mismo Firefox usado para distribuir Tor Browser, la propia red Tor presenta algunas vulnerabilidades conocidas y documentadas:

- Espionaje de sistemas autónomos → Si se controlan los nodos de entrada y salida, es posible correlacionar estadísticamente el tráfico entre los segmentos de entrada y salida, para finalmente interferir en el destino que el cliente ha solicitado. Actualmente existen algoritmos de selección de rutas con la finalidad de predecir y evitar estos sistemas autónomos

- Espionaje en nodos de salida → Cuando la información sale de la red Tor, se puede dar el caso que no se haya establecido una conexión cifrada HTTPS y, por lo tanto, la información viaje sin cifrar. Si un usuario malintencionado, o bien el propietario del nodo de salida, espiara la información que viaja por la red, sería posible recabar información

- Ataque de análisis de tráfico → Este ataque se puede dar de manera tanto de manera activa como de forma pasiva. En el modo pasivo, un atacante extrae características del tráfico de un determinado flujo de datos en un lado de la red, mientras que observa esas características en otro lado de la propia red. En el modo activo, el atacante altera los tiempos de los paquetes en un flujo de información, y observa ese patrón de tiempos en otro lado de la red, estableciendo un vínculo entre un lado y otro de la red, rompiendo así la anonimidad

- Bloqueo de nodos de salida → Como los nodos que conforman la red Tor son conocidos, existen múltiples proveedores que bloquean sus servicios a estas direcciones IP de origen. Esto sucede con la Wikipedia oficial, el servicio de iPlayer de la cadena BBC, etc.

Como se ha comentado anteriormente, Tor es la red anónima más usada de todas las conocidas a fecha de redacción de este documento, de manera que existen infinidad de vulnerabilidades encontradas y escapa del objetivo de este documento mencionarlas.

Al mismo tiempo, existen multitud de desarrolladores preparados para parchear las aplicaciones y mejorar el funcionamiento de la red.

4.5 Resumen analítico de la red Tor

A diferencia de Freenet, Tor no almacena información en el ordenador o dispositivo del usuario de manera que, a priori, gestiona mejor la privacidad.

Es una red híbrida InProxy y OutProxy, pudiendo navegar por la red de Internet convencional, o bien acceder a servicios ocultos de la propia red Tor.

Aunque Freenet y Tor basan parte de su velocidad de acceso a los recursos y servicios en el número de nodos/enrutadores existentes en la red, Tor es mucho más eficiente que Freenet.

Una de las características importantes que tiene Tor es la posibilidad de proxificar aplicaciones a través de SOCKS, deslimitando así el uso de la red a su uso mediante navegadores web.

Es importante tener en mente que Tor mantiene un cifrado extremo a extremo cuando se accede a servicios ocultos, pero este cifrado extremo a extremo desaparece cuando accedemos a contenido en la red de Internet. En ese momento, a no ser que se esté trabajando bajo HTTPS o similares, cuando la información salga por el último nodo del circuito de la red Tor, ésta viajará sin cifrar, y puede verse comprometida.

Lo que en parte puede llegar a ser una amenaza, como puede ser el hecho de que se trate de la red anónima más conocida de las existentes, debido a que puede llegar a ser el foco de ataques, por otra parte es un gran beneficio, ya que existe infinidad de información en los ámbitos: académico, comunidades, hackers, etc., existiendo multitud de “papers”, herramientas, librerías, trabajos de investigación, etc.

5 Red I2P

5.1 Historia y filosofía de la capa de abstracción anónima

El proyecto I2P, Invisible Internet Project, se basa en una capa de red anónima, o capa de abstracción, la cual permite una comunicación P2P resistente a la censura. Las conexiones anónimas se consiguen cifrando el tráfico del usuario, para posteriormente enviarlo a través de una red formada por unos 55000 nodos, y administrada por voluntarios de todo el mundo.

Debido a la cantidad de rutas posibles por las que puede transitar la información, es bastante improbable que una tercera persona sea capaz de ver una comunicación completa.

El software que implementa esta capa se llama enrutador I2P, y el dispositivo que ejecuta I2P se denomina nodo I2P. A este tipo de enrutado se le denomina de tipo ajo, debido a la similitud entre el envío de paquetes que formarían los dientes de una cabeza de ajos.

Esta red anónima nació del 2003 con la intención de llegar a ser una red virtual privada incapaz de ser censurada, y con buenos niveles de protección y seguridad.

Su uso se basa en el establecimiento de túneles de entrada y salida de la información, los cuales están formados por nodos. Dentro de estos túneles, la información viaja en una única dirección.

5.2 Diseño técnico y componentes

Funcionamiento general

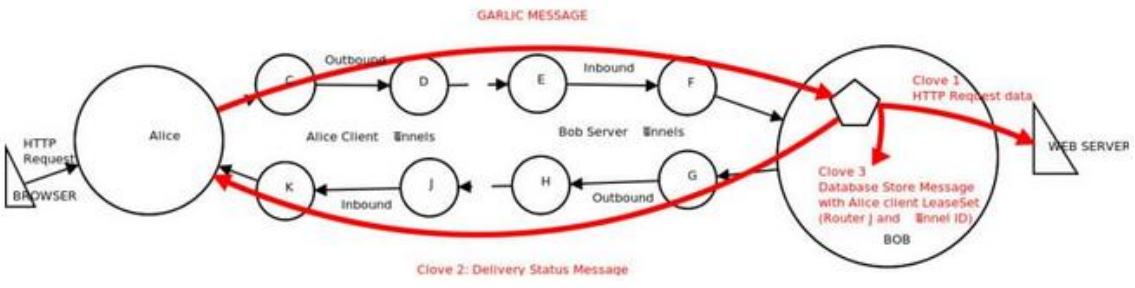
Como sucedía en Freenet, y como también se ha comentado anteriormente, I2P imita el funcionamiento de las redes P2P, ya que la información se transmite a través de los nodos de los voluntarios que mantienen y gestionan I2P.

A diferencia de Freenet por eso, en esta ocasión tan sólo serán necesarios 2 nodos aleatorios para establecer el túnel de salida, y otros 2 nodos aleatorios para el túnel de entrada. Con ambos túneles establecidos, el nodo emisor ya es capaz de transmitir información al nodo receptor, que también dispondrá de sus respectivos túneles de entrada y salida.

Almacenamiento y contenidos

Otra diferencia respecto a Freenet, donde la información se almacenaba distribuida entre los nodos que conformaban la red, es que en este caso los contenidos formaran parte de cada servicio oculto.

En el caso de I2P, estos servicios ocultos se llaman eepsites. En caso de que un eepsite esté apagado, el servicio oculto no estará disponible.



Sistema de red

Aunque sería posible añadir un nodo de salida para poder acceder a la red de Internet convencional, el sistema por el que fue creado I2P es para un uso de tipo InProxy, donde las conexiones se establecerán entre nodos dentro de la misma red, y en ningún caso se saldrá a buscar la información fuera de esta red.

Como se ha comentado anteriormente, I2P utiliza en encaminamiento llamado encaminamiento de tipo ajo. Esta denominación, además de establecer distinciones con la red Tor comentada en el anterior capítulo, viene a ilustrar que cada mensaje mandado significará un gajo o un diente dentro de una cabeza de ajos, que vendría a ser el mensaje completo.

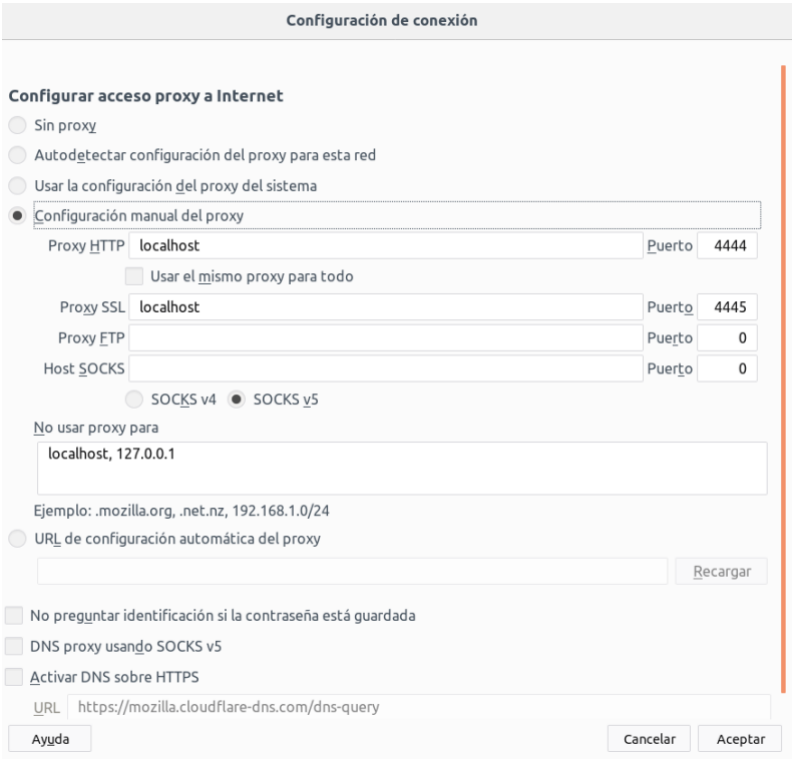
Cada cliente de I2P establecerá túneles diferenciados para la salida y entrada de información. Estos túneles estarán formados por una pareja de nodos dentro del universo de la red I2P, de manera que tendremos una pareja de nodos para el envío de información, y otra pareja de nodos para la recepción de información.

Por su parte, el propio servicio oculto dispondrá también de sus parejas de nodos para el envío y recepción de información, de manera que resultará prácticamente imposible correlacionar la información de un nodo de salida con la de los nodos de entrada, al haber demasiadas combinaciones posibles de nodos.

Interfaz de usuario

Como en las anteriores redes anónimas, la interfaz de usuario será un simple navegador web. Descargando y ejecutando Java, además del instalador de la web oficial, sea para la plataforma que sea, nos permitirá levantar el servicio de enrutado i2proute.

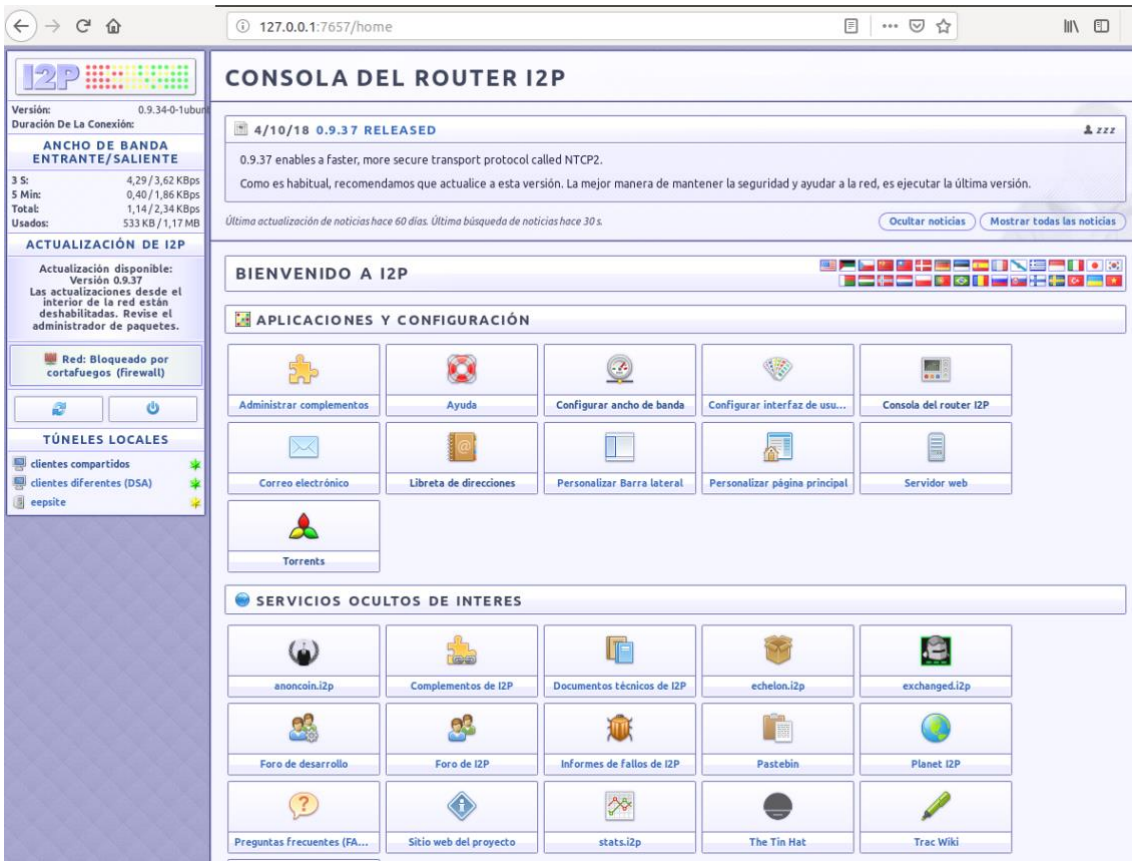
Una vez levantado el servicio, tendremos que modificar la configuración de red del navegador, para que la navegación pase a través del servicio i2proute. Esto lo conseguimos con la siguiente configuración:



Accederemos al servicio i2proute configurándolo como proxy para nuestro navegador, similar a la configuración de Freenet.

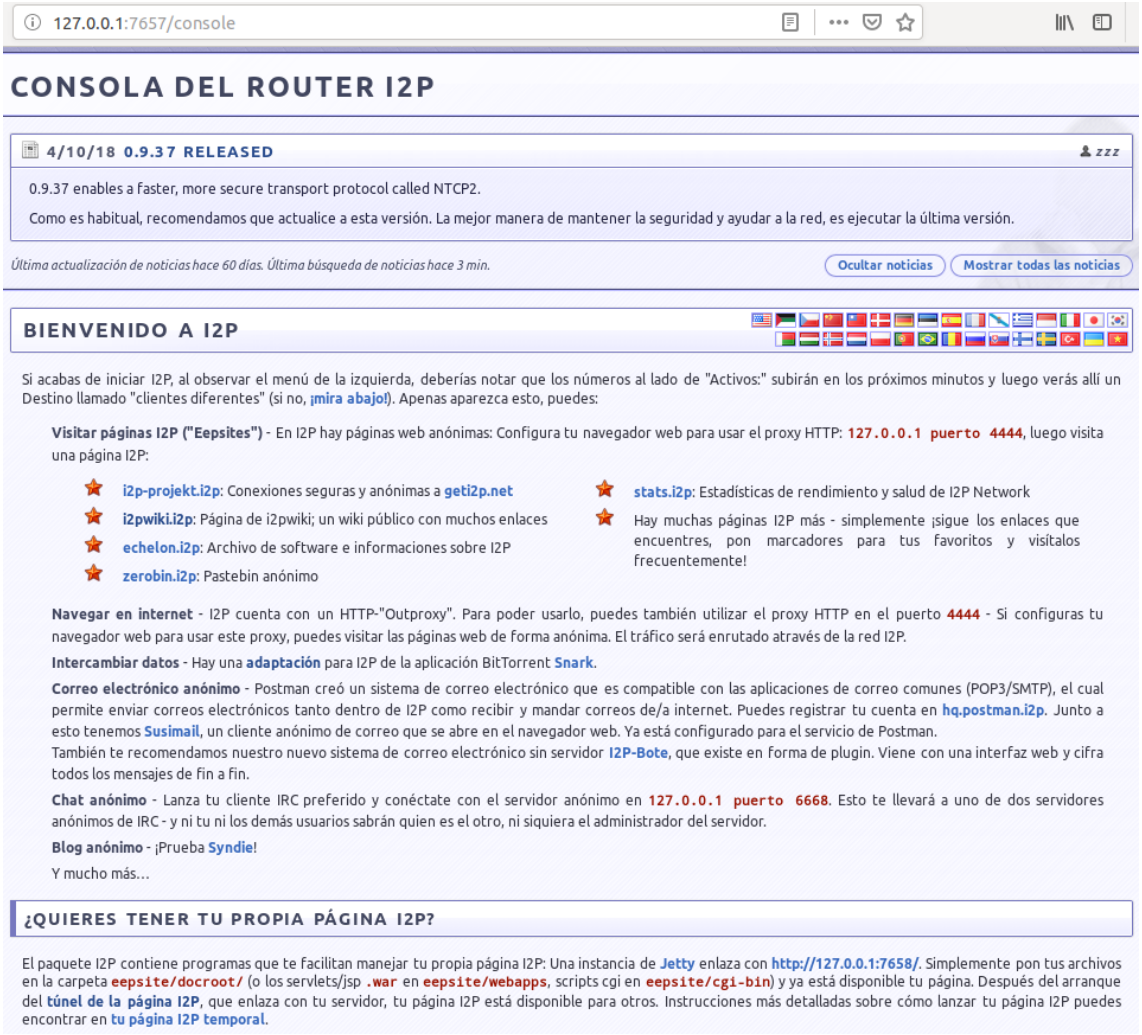
5.3 Herramientas y ejemplo práctico de uso

Una vez instalado y configurado el servicio, se puede proceder a abrir el navegador, y acceder a la consola de I2P, accesible mediante el puerto 7657:



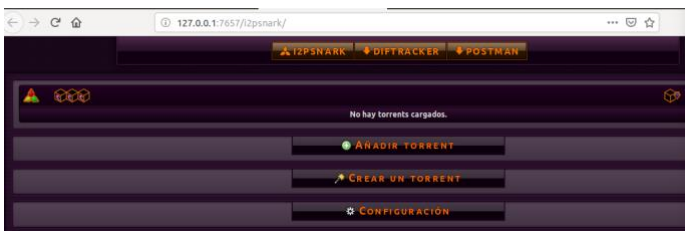
Los primeros pasos a realizar serán configurar el ancho de banda de la conexión a Internet, para que la velocidad de I2P no sea realmente lenta:

A partir de aquí, en la propia página principal se nos ofrecerán varias opciones iniciales, en caso de no saber muy bien por dónde empezar:

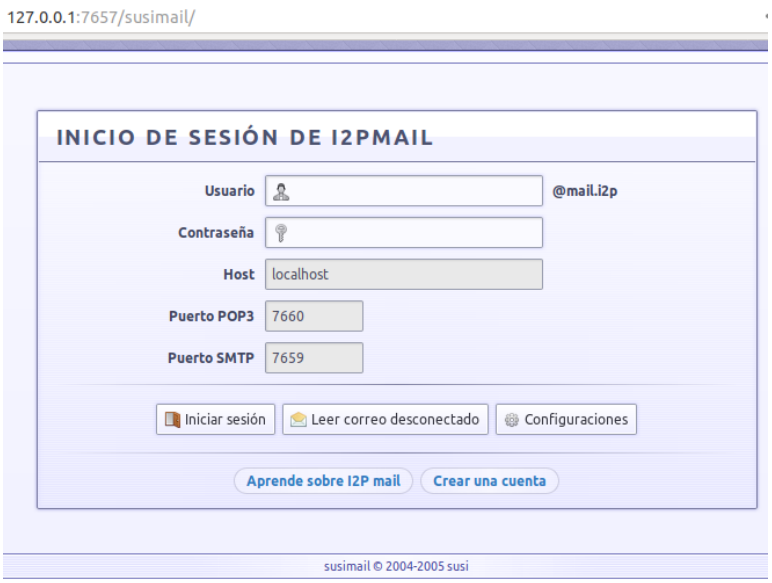


Entre la captura de pantalla anterior, y esta, se nos ofrecen varias opciones para tener en cuenta a la hora de empezar a navegar por I2P:

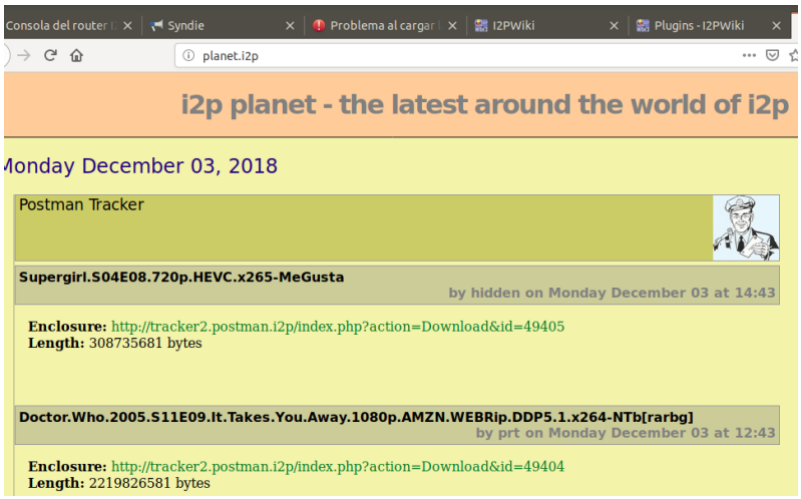
- Snark → Aplicación para descarga de archivs torrent



- Susimail → Servicio de correo anónimo, previo registro en hq.postman.i2p



- planet.i2p → Una web de directorio de archivos multimedia



Como se puede apreciar, existen varios servicios instalados por defecto, que pueden ser de mucha utilidad, así como otros de tipo foros, estadísticas, wiki, informativos, etc.

5.4 Debilidades y/o vulnerabilidades

Aparte de posibles vulnerabilidades explícitas en el uso de navegadores y acceso a contenido web, como pueden ser ataques XSS, CSRF, etc., se tiene constancia de otro tipo de ataques, ya inherentes a la red I2P, como pueden ser los siguientes:

- Floodfill takeover → Se trata de un ataque con la finalidad de controlar la mayoría de nodos de base de datos de la red I2P

- Sybil Attack → Similar a Floodfill takeover pero para una parte limitada del espacio de claves

- Eclipse Attack → Permite a un atacante inutilizar un registro de base de datos a ojos de los participantes

- Deanonimización de usuarios → Enlaza a un usuario con su dirección IP a los servicios que está usando. Requiere de una combinación de Sybil Attack para ubicar nodos maliciosos en la base de datos para así observar acontecimientos

5.5 Resumen analítico de la red I2P

I2P utiliza canales de comunicación unidireccionales llamados túneles, creando un túnel para el envío de información, y otro para la recepción de datos. Estos túneles, además, tienen un tiempo de vida relativamente corto, para reconstruirlos con nuevos pares y así evitar posibles ataques.

Se trata de un modelo de red anónima InProxy, aunque hay opciones de convertir los túneles de salida en OutProxy, para poder así salir a la red de Internet convencional, aunque por defecto no trae esta opción ya que no es la funcionalidad por la que fue creada.

En una instalación por defecto, sin demasiada complicación, un usuario estándar puede disponer de variedad de servicios funcionando bajo la protección del anonimato, como pueden ser la compartición de ficheros, el envío y recepción de correo electrónico, el uso de canales de chat, etc.

Cada usuario de la red I2P es, al mismo tiempo, un nodo que participa activamente en la red para componer túneles con otros usuarios.

Por último, resaltar que, al igual que en Freenet, I2P está programado en Java, y cuenta con varias API para desarrollo de aplicaciones. Esta característica no aplica a Tor, que está programado en C.

6 Comparativa entre las diferentes redes analizadas

Cada red anónima dispone de sus características, de manera que no existe una red mejor o peor, sino que la finalidad por la que se requiera el acceso a una red anónima llevará al uso de una de ellas en concreto.

Así pues, Freenet será de gran utilidad en caso de querer compartir documentos si no se dispone de la posibilidad de tener un servidor arrancado permanentemente con el servicio oculto en funcionamiento ya que, como recordaremos, los documentos introducidos en Freenet se repartirán entre los nodos que conforman la propia red, dentro de sus almacenes de datos, y no requieren servidores dedicados para esta finalidad.

Por su parte Tor nos será de gran utilidad si lo que se busca es usar servicios de la red de Internet convencional, pero manteniendo la anonimidad. Hay que tener en cuenta que el uso de determinados portales o servicios en la nube pueden anular la anonimidad que proporcionará Tor, ya que pueden identificarnos mediante otros métodos.

De todas formas, la manera de sacar el máximo provecho de Tor será creando un servicio oculto dentro de la red, ya que de esta manera los accesos al servicio serán de tipo InProxy, y se maximizará la seguridad y la anonimidad durante todo el proceso.

Por último, I2P se presenta como una alternativa a ambas redes Freenet y Tor. Como Tor porque permitirá conexiones OutProxy, aunque sea mediante la instalación de un pequeño plugin que permitirá añadir un nodo de salida hacia la red Internet convencional, y aunque no sea esta finalidad el principal motivo de su creación. Como Freenet por la similitud a las redes P2P, y debido a que su principal naturaleza será la de funcionamiento tipo InProxy.

Así las cosas, la finalidad por la que se requiera I2P será para el intercambio de información de manera anónima y segura entre dos nodos, ya sea en forma de servicio oculto “eepsite”, o bien utilizando alguno de los plugins existentes para esta red.

Además de todo lo expuesto, y como en cualquier campo relacionado con las tecnologías de la información y las comunicaciones, indicar que estas redes pueden verse modificadas por completo por parte de sus programadores o comunidades, o bien surgir otras redes nuevas que lleguen a ser más populares y desbancarlas del ranking que actualmente ocupan.

7 Otras redes anónimas alternativas

Las redes que pueden considerarse como alternativa a las estudiadas en este documento, se basan en el funcionamiento de redes P2P de distribución de contenidos de manera descentralizada.

Este es el caso de redes como pueden ser:

- GNUtella
- ZeroNet
- GNUnet
- RetroShare

Aunque algunas de ellas, como es el caso de RetroShare, podría no ser considerada como Dark Net, al disponer de la posibilidad de establecer comunicaciones mediante certificados, y publicar direcciones IP de nodos amigos, la finalidad de la mayoría de ellas es permitir que los usuarios publiquen o obtengan de manera anónima contenidos, evitando así posibles censuras gubernamentales.

Para no realizar una larga lista de redes anónimas, de tecnologías similares, en este capítulo se ha querido avanzar un poco en el tema de la seguridad, sobretodo a nivel de sistema operativo, ya que hasta ahora sólo se han nombrado aplicaciones instalables sobre un sistema operativo ya existente por parte del usuario.

Es por este motivo que, además de nombrar posibles alternativas a redes anónimas, parece razonable hablar de sistemas operativos que proporcionan comunicaciones seguras, ya que la mayoría de ellos basan su tecnología en las redes anónimas nombradas en este documento:

- Whonix: Se trata de una distribución basada en GNU/Linux totalmente enfocada a la seguridad, buscando proporcionar intimidad, anonimato y seguridad en Internet, forzando todas las comunicaciones a pasar a través de la red Tor

  https://www.whonix.org

- Qubes OS: Es un sistema operativo centrado en la seguridad a través del aislamiento de sus módulos. Los desarrolladores asumen que no existe un sistema operativo perfecto, de manera que reconocen posibles errores y fallos tanto de componentes de hardware como de software. Tanto es así que si uno de los componentes del sistema operativo se ve comprometido, éste quedará aislado del resto , y el atacante sólo podrá disponer de la información de ese módulo o componente.

  Para lograr su cometido, Qubes implementa un sistema de máquinas virtuales, utilizando así un hipervisor que se instala sobre el propio hardware "bare metal", como si fuera el sistema ESXi de VMWare. De esta manera, si un atacante llega a ser capaz de comprometer la máquina virtual, debería escalar la vulnerabilidad hasta el nivel de hipervisor, lo que no parece una tarea realmente sencilla de llevar a cabo.

  El mejor aprovechamiento de este sistema operativo viene cuando se combina con Whonix, comentado anteriormente, ya que se dispondrá de dos tecnologías desarrolladas inequívocamente para garantizar la seguridad en las comunicaciones de Internet

  https://www.qubes-os.org

8 Conclusiones

En el mundo de principios del siglo XXI donde nos encontramos, donde las redes de comunicaciones están altamente monitorizadas por entidades tanto públicas como privadas y donde términos como Big Data, Data Mining y Data Science obtienen todo el sentido posible, se cree estrictamente necesario el hecho de poder disponer de herramientas para contrarrestar a las grandes corporaciones y potencias que trazan perfiles y identifican comportamientos en base a los movimientos realizados por los usuarios.

Estas herramientas permitirán realizar comunicaciones sin tener que contribuir obligatoriamente a engrosar las ya de por sí extensas bases de datos de dichas compañías, siendo cada vez más fácil su uso y configuración, y gozando de una interfaz de usuario realmente conocida, como es el navegador web.

Países donde desgraciadamente existe la censura a cierto tipo de contenidos, o bien donde los derechos de expresión y de información están fuertemente sesgados, catalogarán este tipo de redes como un problema difícil de mitigar.

Por otro lado, vuelve a quedar demostrado que la codicia humana no tiene límites. Las redes anónimas has servido para que un grupo de personas se enriquezca a base de contenido generado sin escrúpulos. Pornografía infantil, venta de datos robados, drogas, trata de personas, mercenarios y asesinos a sueldo, y una gran variedad de actos delictivos, campan impunemente por este tipo de redes. No merece la pena ni tan siquiera pensar que son contenidos falsos o de impostores, ya que de todos modos han sido creados con finalidad de engaño y manipulación, para conseguir dinero o otros beneficios.

Así, se entiende como logrado el objetivo del documento, que no era otro que el de realizar una demostración práctica de las 3 redes anónimas más populares hasta la fecha, introduciendo las características técnicas de cada una de ellas, y indicando sus ventajas y inconvenientes.

Trabajo futuro

Tal y como se ha comentado en el capítulo anterior, un paso adelante en el tema de la anonimidad sería poder añadir esta característica a todo un sistema operativo, sin necesidad de tener que instalar software en el sistema del usuario. Es realmente vergonzoso que sistemas operativos de primera línea nos sigan obligando a ver publicidad, o sigan registrando los movimientos realizados por sus usuarios, esperemos que futuras leyes puedan llegar a regular o incluso prohibir este tipo de comportamientos.

9 Bibliografía

[1] “Deep Web: TOR, Freenet & I2P Privacidad y Anonimato”, Daniel Echeverri Montoya, 0xWORD

[2] “Comparison of Anonymous Communication Networks – Tor, I2P, Freenet”, Neelam Negi, International Research Journal of Engineering and Technology (IRJET)

https://www.irjet.net

[3] “Locating Hidden Servers”, Lasse Overlier, Norwegian Defence Research Establishment and Gjovik University College

https://www.onion-router.net/Publications/locating-hidden-servers.pdf

[4] “Preservando el anonimato y extendiendo su uso – Conceptos básicos – Freenet”

https://thehackerway.com/2012/01/23/1556/

[5] “#Mundohacker: Freenet, una alternativa inproxy a TOR”, Pablo F. Iglesias

https://www.pabloyglesias.com/freenet-red-inproxy/

[6] “Hackeando TOR y Freenet por diversión, lucro y detener a los malos”, Daniel Echeverri

https://www.youtube.com/watch?v=V1msORieS4I

[7] “The ultimate guide to I2P and how to install and use it”, Jon Watson

https://www.comparitech.com/blog/vpn-privacy/i2p-install-use-guide/

[8] “NSA-proof TOR actually funded by US govt agency, Works with BBG, FBI & DOJ – FOIA docs”

https://www.rt.com/usa/420219-tor-us-government-funded-bbg/

[9] “Instalación y configuración de I2P en sistemas GNU/Linux”, D1nam0

https://securityhacklabs.net/articulo/instalacion-y-configuracion-de-i2p-invisible-internet-project-en-sistemas-gnulinux

[10] “Qué son las redes I2P: el Internet invisible”, Elías Rodríguez García

https://omicrono.elespanol.com/2017/07/red-i2p-anonimato-en-internet/

[11] “Qué es I2P”, KALRONG

https://blog.kalrong.net/es/2017/02/07/que-es-i2p/

[12] “The Definitive Guide to I2P”, Cléber Zavadniak

https://medium.com/clebertech-en/the-definitive-guide-to-i2p-5ddcf04b5b7b

[13] The Tor Project

https://www.torproject.org

[14] Wikipedia

https://www.wikipedia.org

[15] I2P

https://geti2p.net

[16] Tails

https://tails.boum.org

[17] Freenet

https://freenetproject.org

[18] “Así es Freenet, depp web alternativa a Tor e I2P”, Yúbal FM

https://www.genbeta.com/a-fondo/asi-es-freenet-deep-web-alternativa-a-tor-e-i2p

[19] Instituto nacional de ciberseguridad

https://www.incibe.es

[20] Deep.Dot.Web

https://www.depdotweb.com

[21] “The dark side of I2P, a forensic analysis case study”, Behnam Bazli, Maxim Wilson & William Hurst

https://www.tandfonline.com/doi/full/10.1080/21642583.2017.1331770

[22] “Practical Attacks Against The I2P Network”, Christoph Egger, Johannes Schumberger, Christopher Kruegel and Giovanni Vigna

https://www.cs.ucsb.edu/~chris/research/doc/raid13_i2p.pdf