

PEC4

Un paseo por la Deep Web

Fco. Javier García Vázquez

Director en empresa: Jorge Chinaa
Responsable: Victor García Font

Máster Seguridad de las TIC

Curso 2017-2018

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	2/39

Información del documento

	Información
Identificación del documento	<i>PEC4</i>
Autor del documento	<i>Fco. Javier García Vázquez</i>
Fecha de creación	<i>02/04/18</i>
Fecha del documento	<i>04/06/18</i>
Nombre del fichero	<i>PEC4</i>

Historial del documento

Versión	Fecha versión	Cambios
<i>[1.0]</i>	<i>12/03/18</i>	<i>Introducción, objetivos, metodología, diagrama de planificación</i>
<i>[1.1]</i>	<i>08/04/18</i>	<i>Desarrolladas las alternativas para la privacidad en la navegación.</i>
<i>[1.2]</i>	<i>07/05/18</i>	<i>Añadido análisis de TOR y la instalación de su navegador.</i>
<i>[1.3]</i>	<i>04/06/18</i>	<i>Completados resto de <u>apartados</u> (I2P y Freenet)</i>

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	3/39

Tabla de contenidos

1. Abstract.....	4
2. Palabras clave.....	4
3. Introducción.....	4
4. Objetivos del proyecto.....	5
5. Metodología.....	5
6. Desarrollo.....	6
6.1 Alternativas para el anonimato.....	6
6.1.1 Vigilancia y seguimiento de usuarios.....	6
6.1.1.1 Cookies.....	6
6.1.1.2 Browser Fingerprinting.....	7
6.1.1.3 Redes Sociales.....	7
6.1.2 Herramientas para el anonimato.....	7
6.1.2.1 Privacidad del navegador.....	7
6.1.2.2 Conexiones seguras.....	8
6.1.2.3 Redes virtuales.....	8
6.1.2.4 Servidores proxy.....	8
6.1.2.5 Buscadores.....	8
6.1.2.6 Plugins.....	9
6.1.2.7 Redes anonimas.....	9
6.2 TOR.....	9
6.2.1 Estudio y análisis.....	9
6.2.1.1 Objetivos.....	10
6.2.1.2 Relays.....	10
6.2.1.3 Circuito.....	11
6.2.1.4 Hidden Services.....	12
6.2.2 Instalación y Testeo.....	15
6.2.2.1 TOR Browser.....	15
6.2.3 Comunidad.....	18
6.3 I2P.....	21
6.3.1 Estudio y análisis.....	21
6.3.1.1 Túneles.....	21
6.3.1.2 netDB.....	23
6.3.1.3 Capas y protocolos.....	24
6.3.1.4 Hidden Services.....	25
6.3.2 Instalación y Testeo.....	26
6.3.2.1 i2prouter.....	26
6.3.2.1 i2ptunnel.....	27
6.3.2.3 i2psnark.....	27
6.3.2.4 SusiMail.....	28
6.3.3 Comunidad.....	29
6.4 Freenet.....	33
6.4.1 Estudio y análisis.....	33
6.4.1.1 Datastore.....	33
6.4.1.2 Claves.....	33
6.4.1.3 Hidden Services.....	34
6.4.2 Instalación y Testeo.....	34
6.3.2.1 Free Network Project.....	34
6.4.3 Comunidad.....	36
8. Planificación.....	38
8.1 Fases.....	38
8.2 Diagrama.....	38
9. Fuentes de información.....	39

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	4/39

1. Abstract

Este documento supone una versión final del trabajo.

En este documento se han completado los apartados planificados. En este documento se analiza y se comenta la instalación, herramientas y comunidades de usuarios de diferentes soluciones para el anonimato (TOR, I2P y Freenet).

2. Palabras clave

TOR, I2P, Freenet, Tracking, Deep Weeb, Dark Web, Dark Net, User-Agent, hidden service, inproxy, eepsite.

3. Introducción

El uso de las tecnologías web por parte de usuarios permite su monitoreo por parte de entidades privadas y/o gubernamentales.

La empresas privadas utilizan sistemas de monitoreo y análisis de las páginas web visitadas por los usuarios para determinar perfiles con características basadas en las preferencias del usuario, con ello buscan ofrecer una publicidad más personalizada, anuncios propios o de terceros basados en los gustos del usuario.

Las entidades gubernamentales utilizan sus sistemas de monitoreo principalmente en la lucha contra el terrorismo, o al menos ese es su argumento (la información filtrada por Snowden y Assange pueden poner en duda esto).

Esta vigilancia ha despertado los temores de usuarios preocupados por el derecho a su privacidad y anonimato, han surgido herramientas que intentan mitigar esta vigilancia.

Estas herramientas se vuelven especialmente útiles en casos extremos como se dan en países con políticas restrictivas de acceso a Internet o cuando algunos países han restringido el acceso al exterior debido a crisis de gobierno (primaveras árabes). En estos casos estas herramientas son especialmente útiles a la hora de dar a conocer de manera internacional lo que sucede dentro del país que intenta restringir ese acceso a Internet.

Desgraciadamente estas herramientas dan pie a la comisión de delitos, tanto mafias criminales y narcotraficantes como pedófilos, compradores y vendedores de objetos robados, etc. Hay organizaciones centradas en encontrar a estos delincuentes y conocer su ubicación real.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	5/39

4. Objetivos del proyecto

El objetivo de este proyecto es dar a conocer el funcionamiento de las principales plataformas y alternativas que tienen los usuarios a la hora de mantener su anonimato en Internet. Describir desde soluciones sencillas al alcance de cualquier usuario medio a otras alternativas más completas que ofrecen la protección que interesa a los usuarios que buscan utilizar estas plataformas. Estudia y analizar a nivel técnico las principales alternativas de plataformas para el anonimato (TOR, I2P y Freenet) y probarlas. Para no centrar el proyecto en la parte técnica de estas herramientas se han comentado casos reales y hecho mención a algunos de los sites más populares de las comunidades de estas redes anónimas.

	Prioridad
Análisis de las alternativas para el anonimato	crítico
Estudio y análisis técnico (TOR, I2P y Freenet)	prioritario
Instalación y prueba (TOR, I2P y Freenet)	prioritario
Estudio de comunidad y casos reales (TOR, I2P y Freenet)	secundario

5. Metodología

Tras seleccionar las plataformas y alternativas a comentar analicé éstas estudiándolas y probándolas, comentando casos reales y navegando por las comunidades asociadas a éstas.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	6/39

6. Desarrollo

6.1 Alternativas para el anonimato

Al navegar por Internet se hace inevitable dejar ciertos rastros que son utilizados por empresas y organismos gubernamentales para realizar un seguimiento de los usuarios.

La privacidad es un derecho fundamental, sin embargo no es difícil encontrar usuarios que pese a ser conscientes de que se produce esta vigilancia y sus derechos se vulneran no consideran que sea algo de lo que preocuparse, bajo del pretexto del “No tengo nada que ocultar”.

Esta idea instaurada o muy arraigada en la mentalidad de muchos usuarios lleva a éstos a compartir información de la que muchas veces ni son conscientes (localizaciones, hábitos, información laboral, etc.). El seguimiento o “tracking” de los usuarios mediante esta información permite elaborar perfiles muy concretos sobre los usuarios.

6.1.1 Vigilancia y seguimiento de usuarios

6.1.1.1 Cookies

Una cookie es una información enviada por el servicio web y almacenada en el navegador web, su función principal es almacenar información útil entre las diferentes peticiones y respuestas del navegador. De esta manera se solventa el “problema” de que HTTP es un protocolo sin estado, no conserva información entre las peticiones. Adicionalmente las cookies son utilizadas por los servicios web para almacenar información relativa a las preferencias del usuario, mejorando así su experiencia con el servicio web.

Se pueden catalogar las cookies según su función, algunos ejemplos típicos son:

- **Cookies de sesión:** almacenan información (preferencias e identificación) sobre un usuario mientras dura su sesión. Se utilizan para mejorar la experiencia del usuario.
- **Cookies técnicas:** permiten controlar el tráfico y la comunicación de datos, se utilizan para permitir funciones concretas según los requisitos de la aplicación o servicio web.
- **Cookies de personalización:** establecen valores que afectan a la presentación de la web (tipo de navegador, idioma de preferencia, etc.).
- **Cookies de análisis:** buscan conocer los hábitos de los usuarios y su interacción con el servicio o aplicación web, permiten elaborar un perfil de éstos.
- **Cookies de terceros:** son gestionadas por un dominio externo al servicio web que se está visitando. Esta información

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	7/39

es utilizada por entidades para generar perfiles muy concretos sobre los usuarios, los servicios web están obligados a notificar a los usuarios sobre este tipo de cookies (aunque estos no son muy conscientes de esto al aceptarlo).

Al hablar de cookies cabe mencionar que existen las supercookies, este término se refiere a cookies que pese a tener el resto bloqueadas pueden regenerarse automáticamente. Existen supercookies que aprovechan el sistema HSTS (HTTP Strict Transport Security) para saltarse esa protección (envían la información necesaria en los flags durante el protocolo).

Existen cookies persistentes capaces de almacenar información en diferentes espacios del navegador (espacio estándar, cache del navegador, espacio MySQL, etc). Estas cookies son capaces de “regenerarse” si detectan que el usuario ha intentado eliminarla de alguno de los espacios donde se ha almacenado. Se trata de una forma muy agresiva de tracking.

6.1.1.2 Browser Fingerprint

Es posible el seguimiento de usuarios mediante la identificación de características concretas del navegador web como plugins instalados, resolución de la pantalla, idioma preferido, IP, fuentes instaladas... Con todo esto se puede obtener una huella del navegador, esta información puede llegar a identificar a un usuario de manera única, o en el peor de los casos la máquina utilizada si varios usuarios utilizan la misma. Dependiendo del número de datos proporcionados se puede identificar con mayor o menor exactitud al usuario (se habla de entorno a un 85% de efectividad). Desde webs como <https://amiunique.org/> se puede comprobar como de “única” es la huella de tu navegador.

6.1.1.3 Redes sociales

Las redes sociales suponen un riesgo para la privacidad de sus usuarios, pese a que pretenden ser servicios gratuitos éstos se apropian de los datos de los usuarios y hacen negocio con ellos.

6.1.2 Herramientas para el anonimato

6.1.2.1 Privacidad del navegador

La mayoría de navegadores web permiten una configuración de su privacidad, se pueden establecer valores que afecten al comportamiento con cookies de terceros (denegadas por defecto), bloquear cookies según el dominio web, comportamiento del historial de navegación, etc.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	8/39

Es recomendable tener una configuración correcta con un control básico de la privacidad, por ejemplo pidiendo notificación de las cookies.

6.1.2.2 Conexiones seguras

Es recomendable utilizar conexiones seguras, es decir, conexiones HTTP a servicios web que implementen el cifrado SSL/TLS. El protocolo HTTPS utiliza este mecanismo para garantizar la confidencialidad de la comunicación.

6.1.2.3 Redes virtuales

Una red virtual o VPN (Virtual Private Network) es una tecnología que permite una conexión directa y privada entre dos equipos distanciados y conectados a Internet. Simulan una red local entre equipos separados físicamente y en redes distintas. Toda la información transmitida entre estos equipos a través de la red virtual está cifrada. Adicionalmente los servicios VPN se utilizan para ocultar la IP de origen, permitiendo acceder a dominios web bloqueados por firewalls o incluso restringidos en todo un país.

6.1.2.4 Servidores proxy

Un servidor proxy es una pasarela entre el cliente y un servidor en una petición web. Sencillamente se enruta la petición y la respuesta de manera transparente. Un servicio proxy oculta la dirección IP origen. En Internet se pueden encontrar fácilmente servidores proxy gratuitos.

6.1.2.5 Buscadores

Buscadores como Google pueden suponer un problema para la privacidad, pese a que se trata de un buscador potente y preciso Google lo utiliza (al igual que el resto de sus servicios) para hacer un seguimiento de sus usuarios. Google registra entre otras cosas el historial de búsquedas, los dispositivos utilizados desde la cuenta y la ubicación de éstos, etc.

Para prevenir esta intrusión en la privacidad existen plataformas que aprovechan el potencial y los beneficios de buscadores como Google sin perjudicar la privacidad de los usuarios.

Uno de los buscadores más conocidos para esto es Duckduckgo.

Este buscador no registra ningún tipo de información del usuario, no permite el envío de ésta a sitios dominios externos, no registra cookies ni trata las cabeceras con información útil para el tracking como la IP o el User-Agent.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	9/39

6.1.2.6 Plugins

Algunos de los navegadores web comerciales más utilizados (como Chrome o Firefox) permiten incorporar plugins para mejorar la experiencia de navegación del usuario además de añadir funcionalidades a conveniencia del usuario.

Algunos de estos plugins o extensiones del navegador proporcionar una capa extra de protección de la privacidad.

Uno de los más populares es AdBlock Plus, este plugin bloquea rastreadores de cookies. Esta extensión es muy popular ya que permite evitar publicidad en la reproducción de videos en plataformas web como youtube.

Otro plugin popular a la hora de salvaguardar la privacidad es NoScript, este plugin evita la ejecución de scripts protegiendo de posibles ataques maliciosos (tambien es útil a la hora de evitar scripts de minado de monedas, cosa que se ha vuelto habitual). Esta extensión permite marcar sitios webs de confianza para evitar posteriores bloqueos.

6.1.2.7 Redes Anónimas

Existen herramientas potentes a la hora de mantener la privacidad y el anonimato, un ejemplo son TOR, I2P y Freenet.

La DeepWeb o Internet profunda es el contenido no indexado por los motores de búsqueda más populares de Internet. Se considera "Deep Web" a esos contenidos no indexados o imposibles de encontrar. Algunos buscadores ignoran contenido ya que está protegido o incluidos en redes privadas o virtuales. La "Dark Web" es el contenido no indexado ya que los propietarios han protegido el contenido o ubicado en redes privadas anónimas.

Es imposible calcular o conocer el número exacto de contenido no indexado, mucho del contenido es desconocido e incluso temporal.

La compañía de seguridad Hyperion Gray ha recopilado 6.608 dominios web accesibles el pasado Enero de 2018 desde la DarkNet TOR. En el proyecto han catalogado las webs por categorías y ver como están indexadas entre ellas.

Una "Darknet" es un subconjunto de la Deep Web protegido en una red privada o al que solo acceden usuarios autorizados. La red Darknet más popular es TOR, una plataforma gratuita.

6.2 TOR

6.2.1 Estudio y análisis

TOR es la red anónima más popular, considerada la principal y más grande. Esta plataforma está gestionada y mantenida por Tor Project y desde su creación en 2003 (se inició como una red para proteger las

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	10/39

comunicaciones de la marina americana) se han ido sumando voluntarios de todo el mundo.

El propio nombre TOR (The Onion Router) se refiere a la estructura en capas en que está formado, cada una de estas añaden protección de cifrado impidiendo así que los servidores y páginas por las que se navegan no puedan conocer la IP de origen.

Se trata de una plataforma centralizada, TOR cuenta con servidores conocidos como Directory Authorities que sirven la información sobre los repetidores (Relays) que conforman la red TOR.

6.2.1.1 Objetivos

El objetivo principal de TOR es el anonimato y la privacidad.

Con TOR se puede proteger la identidad del usuario durante la navegación en Internet, adicionalmente ayuda a saltar filtros establecidos por entidades gubernamentales.

TOR impide que se pueda realizar un seguimiento entre el origen y el destino del tráfico de datos.

En cada sesión se generan claves simétricas que garantizan la privacidad de la comunicación, los nodos se comunican entre ellos siguiendo el protocolo SSL/TLS.

La integridad de la comunicación se garantiza ya que los mensajes incluyen un MAC (identificador único) que sirve para verificar posibles modificaciones.

6.2.1.2 Relays

El componente principal de la red TOR son sus nodos (también conocidos como repetidores o relays), todos sus nodos son importantes pero hay diferencias técnicas entre ellos:

- **Nodos Cliente:** Un cliente es el primer nodo en un circuito de 3 nodos, para ser cliente el repetidor ha de ser estable y rápido (al menos 2Mb/s) o se comportará como un repetidor intermedio.
- **Nodos Intermedios:** Un repetidor intermedio puede ser otro repetidor cliente pero no uno de salida, actúa como el segundo salto en el circuito de nodos. Tanto los repetidores intermedios como los cliente enrutan el tráfico del interior de la red, y no acceden a los datos de las comunicaciones enrutadas.
- **Nodos Salida:** Este nodo es el último de la cadena de repetidores, enrutan el tráfico al exterior de la red. Estos repetidores pueden acceder de manera indirecta a los datos, se encargan de suprimir la última capa de cifrado de

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	11/39

TOR (pudiendo descubrir el destino y el contenido de la comunicación).

- **Nodos puente:** El diseño de la red TOR trabaja con las IPs públicas de sus nodos, una manera en que los gobiernos consiguen bloquear la redes TOR es haciendo listas negras de las IPs públicas de estos nodos. Los repetidores puente son nodos que no están publicados en el listado publico del directorio TOR, lo que dificulta su bloqueo.

6.2.1.3 Circuito

Estos tres repetidores componen el circuito necesario permitiendo una comunicación bidireccional.

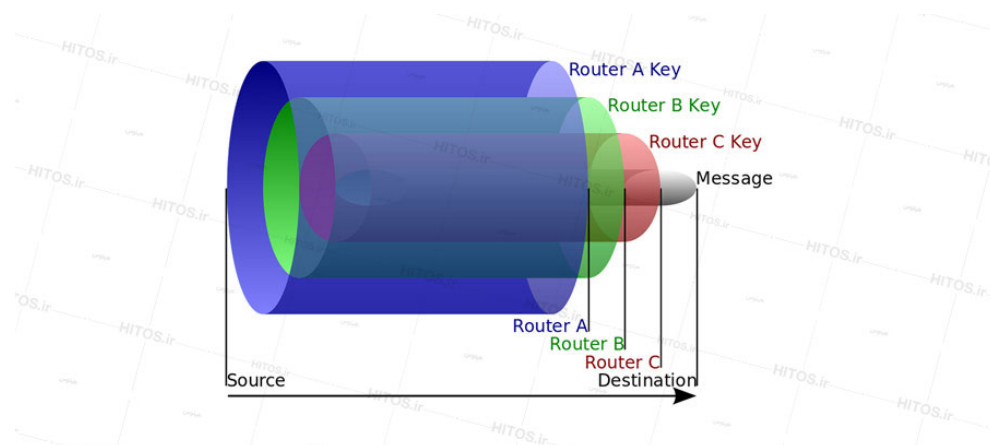


Ilustración 1: Repetidores del circuito

El cliente establece su propio circuito, es decir, selecciona sus propios nodos necesarios. El cliente solicita una clave pública a sus nodos escogidos cifrando con ellas los datos (múltiples capas de cifrado).

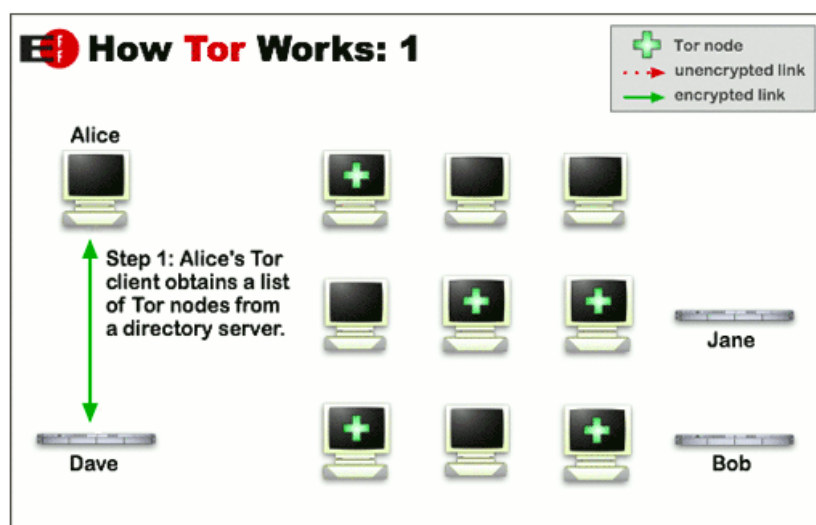


Ilustración 2: Paso 1 circuito

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	12/39

Una vez seleccionado el circuito de manera aleatoria se comienza la comunicación entre el cliente y el servidor a visitar sin que cada nodo pueda conocer y enlazar el origen y el destino de una comunicación.

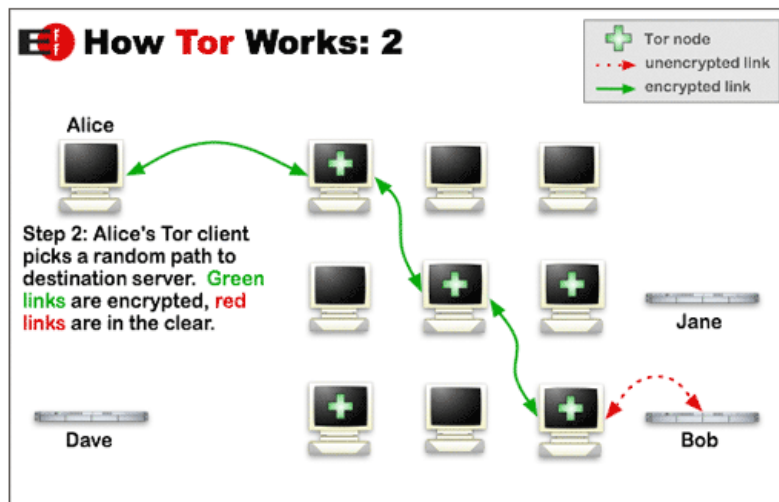


Ilustración 3: Paso 2 circuito

6.2.1.4 Hidden Services

Un servicio oculto puede ser prácticamente cualquier tipo de servicio (HTTP, SSH, FTP...), este servicio ha de estar disponible en la red TOR para que los clientes puedan conectarse a él. Para ello (al igual que en el caso del cliente) selecciona tres nodos de manera aleatoria construyendo así un circuito. Estos nodos son conocidos como Introduction Points, se encargan de enrutar las peticiones de los clientes hacia el servicio oculto. Éste enviará su clave pública a los Introduction Points para poder asociar dicha clave al servicio.

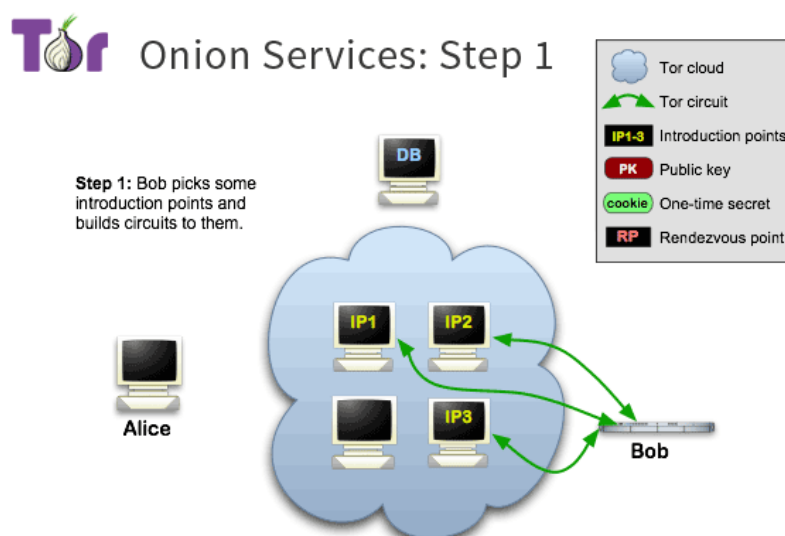


Ilustración 4: Paso 1 hidden service

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	13/39

Para que el servicio esté disponible para los clientes éste ha de publicar una información básica en la red TOR. Para ello se genera un fichero que contiene la dirección del servicio, clave pública y listado de Introduction Points. Este fichero se registra en la base de datos distribuida de TOR (Distributed Hash Table).

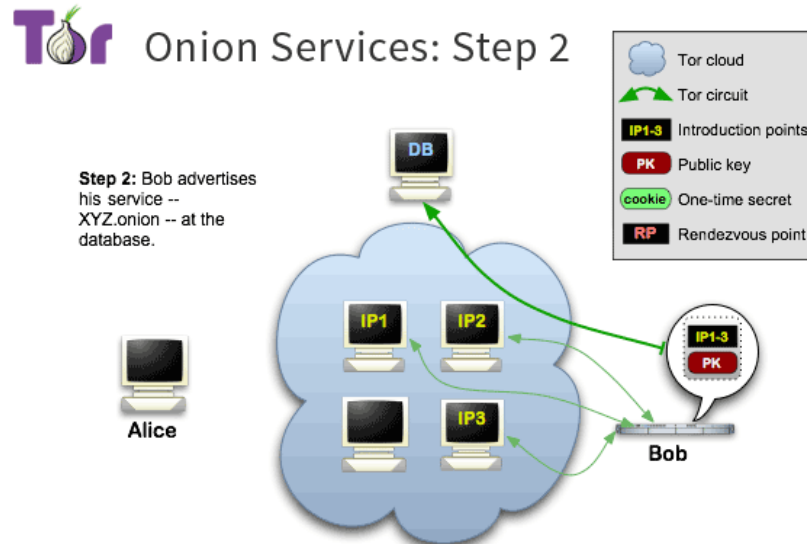


Ilustración 5: Paso 2 hidden service

Una vez el servicio está disponible los clientes han de acceder a él, para ello tras conocer la dirección del servicio a visitar lo consulta en la base de datos distribuida de TOR y crea un circuito con ella. Con ello se obtiene la información asociada a la dirección onion (clave pública y listado de Introduction Points).

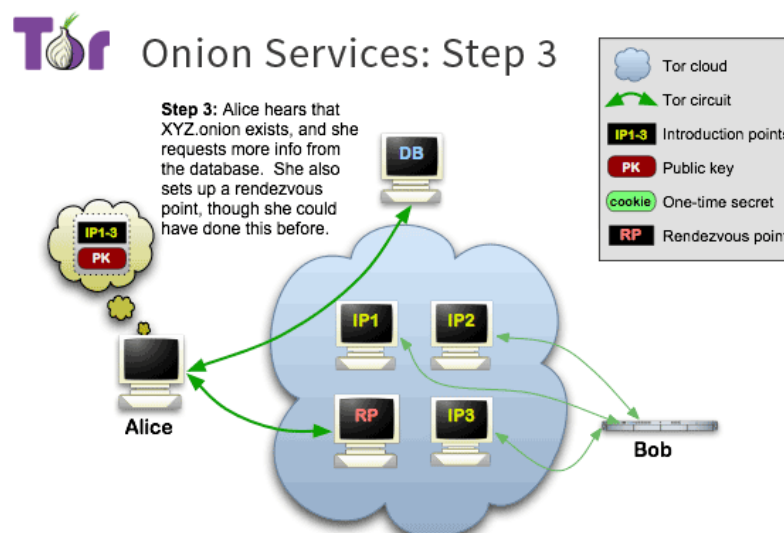


Ilustración 6: Paso 3 hidden service

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	14/39

Una vez el cliente dispone de toda esta información, selecciona aleatoriamente uno de los Introduction Points listados por el servicio oculto y selecciona adicionalmente un nodo que actuará de punto de encuentro (Rendezvous Point) entre el propio cliente y el servicio oculto. El punto de encuentro genera un OTS (One Time Secret) que identifica de forma única su circuito con el cliente.

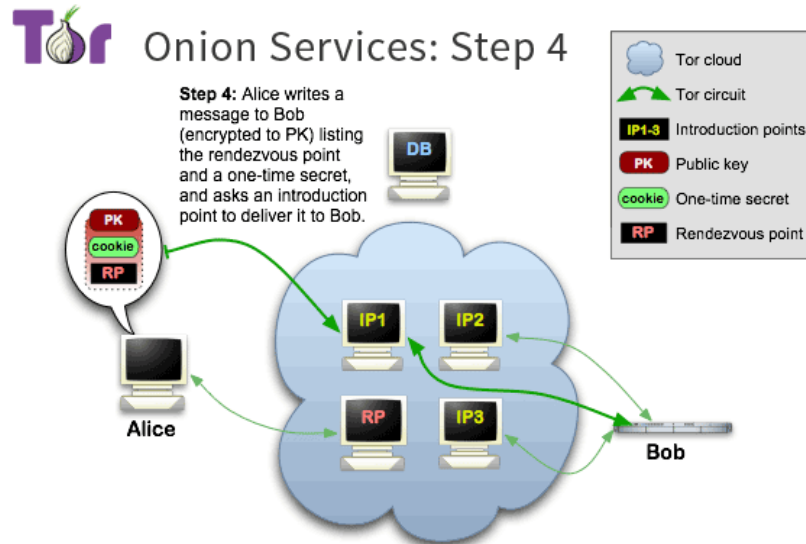


Ilustración 7: Paso 4 hidden service

El cliente genera unos datos conocidos como Introduce Message en los que se especifica la dirección del nodo de punto de encuentro y el OTS generado por éste y lo envía al Introduction Point escogido. Estos datos están cifrados con la clave pública del servicio oculto.

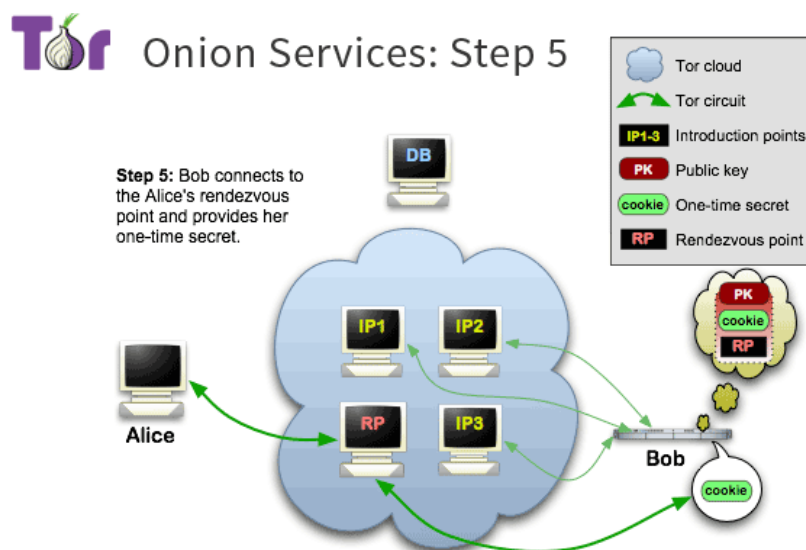


Ilustración 8: Paso 5 hidden service

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	15/39

Una vez el servicio oculto conoce la dirección del nodo de punto de encuentro, el servicio crea un circuito hacia él y le envía el OST. El nodo de punto de encuentro tras verificar el OST responde al Introduce Message del cliente y se enlaza la comunicación de cliente y servicio oculto a través de él.

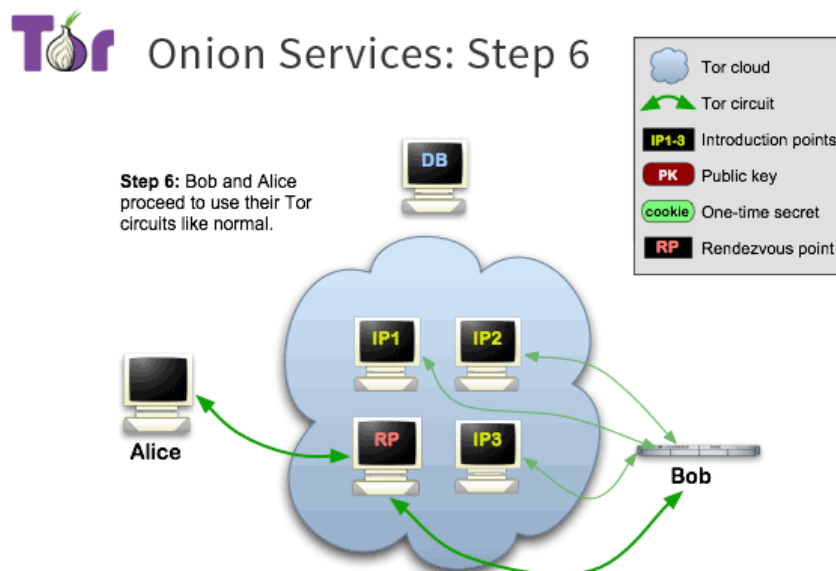


Ilustración 9: Paso 6 hidden service

6.2.2 Instalación y testeo

6.2.2.1 TOR Browser

El equipo que he utilizado para la instalación del navegador de TOR corre un sistema operativo Ubuntu 16.04. He instalado el navegador a través del instalador de paquetes aptitude:

```
$ sudo add-apt-repository ppa:webupd8team/tor-browser
```

```
$ sudo apt-get update
```

```
$ sudo apt-get install tor-browser
```

Al iniciar el navegador podremos configurar la conexión.

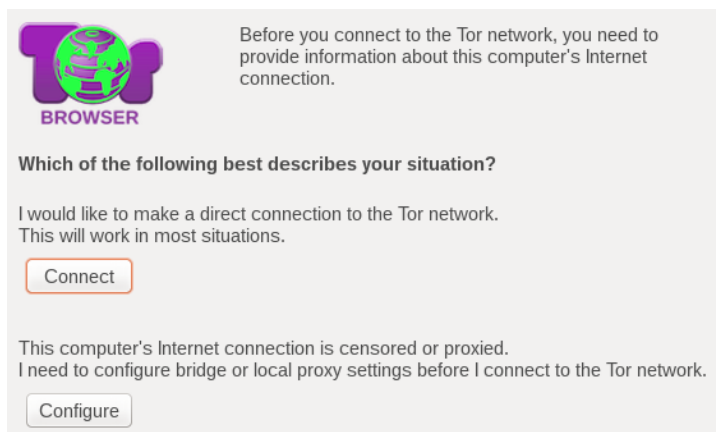


Ilustración 10: Paso 1 tor browser

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	16/39

Se nos ofrece conectarnos directamente a la red TOR o a través de un puente para poder saltar alguna restricción o bloqueo del ISP. En el caso de existir algún tipo de restricción (como nos podríamos encontrar en el caso de algunos países) configuraremos una conexión de tipo puente.

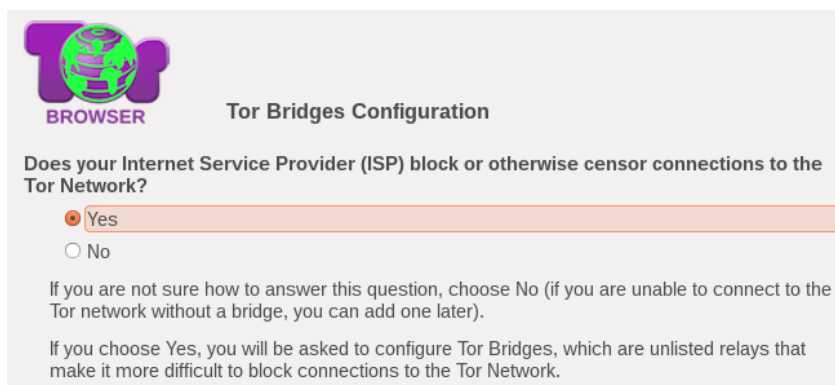


Ilustración 11: Paso 2 tor browser

Se recomienda seleccionar el transporte de tipo obfs4 proxy, se considera el transporte más efectivo para saltarse restricciones.

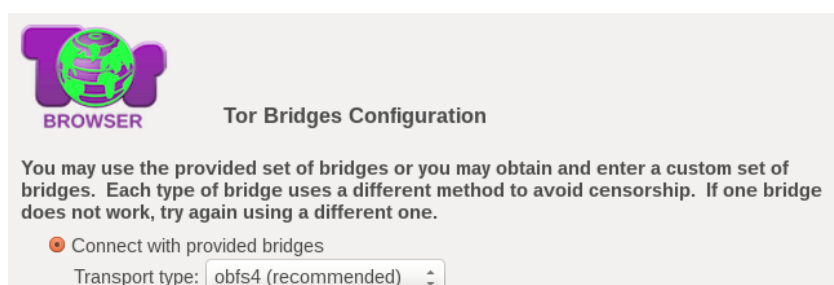


Ilustración 12: Paso 3 tor browser

La última ventana pregunta acerca del uso de algún proxy, ya que seguramente el nodo puente ya será capaz de conectarse al destino este paso no será necesario en la mayoría de escenarios.

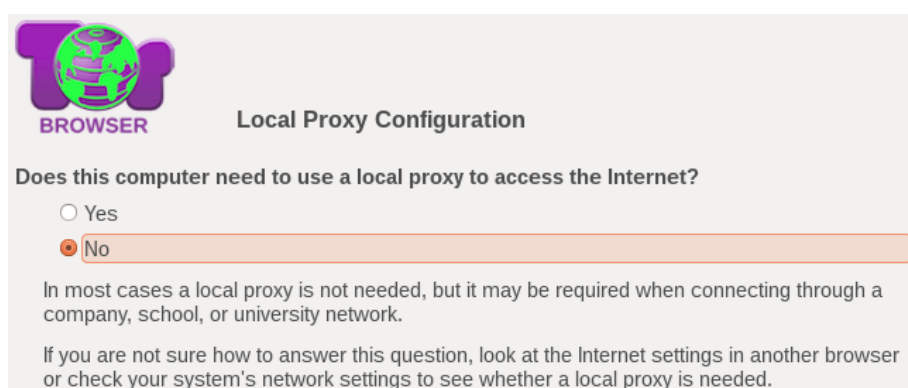


Ilustración 13: Paso 4 tor browser

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	17/39

El navegador TOR está basado en un Mozilla Firefox.

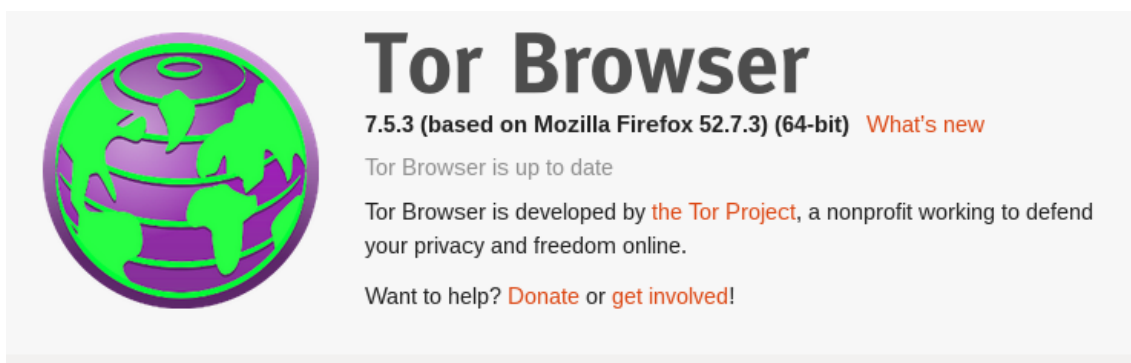


Ilustración 14: Tor Browser instalado

Su última versión incluye un par de plugins del navegador bastante útiles para ayudar a la navegación privada.

Uno de los plugins deshabilita la ejecución de scripts en las páginas webs visitadas.

El otro plugin se trata del conocido HTTPS Everywhere, un proyecto de código abierto entre TOR Project y Electronic Frontier Foundation cuyo propósito es hacer que los sitios web utilicen HTTPS en lugar de HTTP.

Adicionalmente desde el propio navegador podemos configurar niveles de seguridad, al incrementarlo se restringen funcionalidades de la navegación.

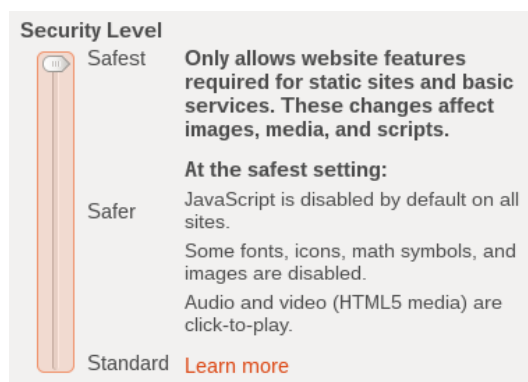


Ilustración 15: Niveles de seguridad

Con el nivel standard se mantienen todas las funcionalidad del navegador.

Con el nivel medio (Safer) todo los recursos de audio y video html5 se deshabilitan via NoScript, se deshabilita las funcionalidades JavaScript

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	18/39

en webs no-https, algunas imagenes se deshabilitan igual que ciertas funciones de renderizado.

Con el nivel alto (Safest) adicionalmente se deshabilita JavaScript en todos los sites web, la mayoría de audio y video queda deshabilitado y algunas fuentes e iconos podrían no mostrarse bien.

Desde el propio navegador se pueden comprobar los 3 nodos escogidos por el cliente (el cliente no puede conocer los escogidos a su vez por el hidden service).



Ilustración 16: Nodos conocidos

Por último, el navegador ofrece la posibilidad de comprobar la conexión a través de la red TOR.



Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **51.15.63.43**

Ilustración 17: Conexión TOR correcta

6.2.3 Comunidad

TOR es una de las plataformas más populares por lo tanto es rica en contenidos. Es prácticamente impensable pretender conocer la magnitud o hacer un recuento del número de servicios web disponibles en esta red. La mayoría de sitios web desaparecen tan rápido como se crean y muchos no son conocidos o no están indexados por otras web de la red TOR.

Es conocido que plataformas como TOR se utilizan para llevar a cabo prácticas ilegales en sitios web que se transmiten por el boca a boca entre los participantes de la actividad ilícita (un ejemplo ilustrativo son las subastas y ventas de arte y bienes robados).

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	19/39

Existen casos de actividades ilícitas llevadas a cabo a TOR que han llegado a tener un reflejo en los medios.

Uno de los casos más conocidos es el de la web SilkRoad, se trató de un mercado negro de objetos sin ningún tipo de restricción y que garantizaba la privacidad y el anonimato de compradores y vendedores. Esa plataforma fue utilizada por criminales para la compraventa de armas y drogas hasta que finalmente el FBI logró cerrar la web el 3 de octubre de 2013 capturando a su fundador gracias a unas técnicas de muy dudosa legalidad (no explicaron a nivel técnico cómo dieron con el servidor del hidden service violando la seguridad de TOR y más de una ley internacional).

La compañía de seguridad HyperionGrey consiguió recopilar una red de casi 7000 páginas web accesibles durante el pasado Enero.

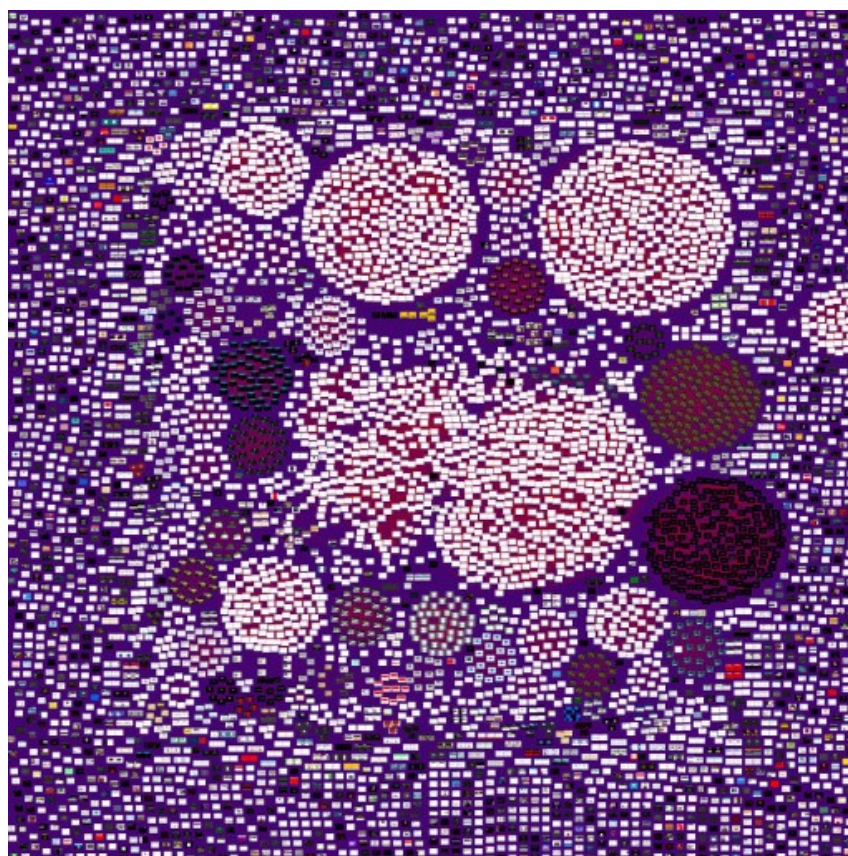


Ilustración 18: Mapa de la red TOR por HyperVision

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	20/39

The Hidden Wiki; <http://zqktlwi4fecvo6ri.onion/>

The Hidden Wiki Main Page

Welcome to The Hidden Wiki New hidden wiki url 2018 <http://zqktlwi4fecvo6ri.onion/> Add it to bookmarks and spread it!!!!

Editor's picks

Pick a random page from the article index and replace one of these slots with it:

1. The Matrix - Very nice to read.
2. How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off.
3. Verifying PGP signatures - A short and simple how-to guide.
4. In Praise Of Hawala - Anonymous informal value transfer system.
5. Terrific Strategies To Apply A Social media Marketing Approach - Great tips for the internet marketer.

Volunteer

Here are the six different things that you can help us out with:

1. Plunder other hidden service lists for links and place them here!
2. File the SnapBBSIndex links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
4. Care to start recording onionland's history? Check out Onionland's Museum.
5. Perform Dead Services Duties.
6. Remove CP shitness.

Contents [hide]

- 1 Editor's picks
- 2 Volunteer
- 3 Introduction Points
- 4 Financial Services
- 5 Commercial Services
- 6 Domain Services
- 7 Anonymity & Security
- 8 Hosting / Web / File / Image
- 9 Blogs / Essays / Wikis
- 10 Email / Messaging
- 11 Social Networks
- 12 Forums / Boards / Chans
- 13 Whistleblowing
- 14 HIPAA/WVC
- 15 Audio - Music / Streams
- 16 Video - Movies / TV
- 17 Books
- 18 Drugs

Ilustración 19: Hidden Wiki

Sin duda uno de los sitios web más populares de TOR, en la hidden wiki se recoge un amplio listado de enlaces a otros servicios web de la red TOR. Permite ver estos enlaces de manera ordenada y filtrada, los enlaces en esta web suelen estar actualizados.

Silk Road 3.1: <http://silkroad7rn2puhj.onion/>

Silk Road
the darknet's most resilient marketplace

Home Stealth Order Login ZFA Register Recover F.A.Q. Forums

Hello, comrade! You are not logged in. You can still browse the Silk Road and place anonymous orders (click to read more and access your stealth orders).
For a full experience, please log into your account , or register a new account ! Dismiss

Bitcoin \$ 7,506 Litecoin \$ 120 Monero \$ 162 Dash \$ 594

May 27th update:
-Support center reworked and improved.
-Addressing the recent PGP security flaw here.
-New phishing prevention page here.
-New helpdesk with Frequently Asked Questions for both buyers and vendors here.

FEATURED

<p>Pauli +1795, -34, 98%</p> <p>5g Moroccan Hash Hasj Normal Quality Very cheap</p>	<p>Pauli +1795, -34, 98%</p> <p>Amnesia HAZE WEED 5G</p>	<p>Pauli +1795, -34, 98%</p> <p>1gr PURE UNCUT COCAINE We accept all coins SHIPPINGFREE</p>	<p>ViceKings +6571, -327, 95%</p> <p>LSD BLOTTERS 220 UG 10X</p>	<p>greenmonkey +1435, -0, 100%</p> <p>QP BLUE DREAM SHATTER 1250! FULL ESCROW!</p>	<p>probitexchange +4159, -17, 100%</p> <p>50 X 2mg Xanax bars Worldwide (PROMO CODE: 50WXXB - \$50 off)</p>
---	--	---	--	--	---

Ilustración 20: Silk Road 3.1

Tras el arresto del fundador del SilkRoad original (Ross William Ulbricht) apareció una replica de la popular plataforma de compravenda, esta segunda versión duró poco más de un año ya que su administrador fue detenido.

En la tercera versión de SilkRoad participó el equipo de Crypto Market e hicieron una copia con mejoras en la seguridad. Esta tercera versión

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	21/39

se cerró por los propios administradores tras unos periodos de inactividad debidos a actualizaciones en la seguridad.

La versión 3.1 de SilkRoad apareció con el mismo diseño y los mismos administradores que la tercera versión pero las cuentas de los usuarios de la anterior versión no funcionaban en la actual, esto hizo pensar a algunos usuarios que se tratase de scam, pero tras el registro y aportando cierta información se les permitió recuperar dinero del market anterior.

Empire Market: <http://empiremktxgiovhm.onion>



Ilustración 21: Empire Market

Otro mercado negro sucesor de AlphaBay Market.

6.3 I2P

6.3.1 Estudio y análisis

El proyecto I2P (Invisible Internet Project) es hoy en día una de las plataformas de red anónimas más robustas y sus comienzos remontan a 2003. Se encuentra desarrollado en Java (con lo que necesita una JVM) aunque incluye componentes programados en C.

I2P se basa en un modelo descentralizado, los usuarios son capaces de conocer la existencia de otros usuarios pero no pueden ver el contenido y los destinatarios de los datos que intercambian con otros usuarios (el tráfico es mezclado y difuminado a través de proxys).

I2P ofrece herramientas para acceder a servicios web (eepsites), cliente de bitorrent (i2PSnark), servicios con conexiones TCP/IP (I2PTunnel) además de permitir poner en marcha todos esos tipos de servicios de manera transparente.

6.3.1.1 Túneles

Los túneles representan uno de los componentes más importantes de la arquitectura de la red I2P, permiten el tráfico de datos entre los diferentes usuarios de la red I2P.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	22/39

Un túnel es la ruta entre dos usuarios a través de varios enrutadores. Cuando un usuario nuevo entra en la red éste pasa a ser a su vez un enrutador de otros usuarios, compartiendo su ancho de banda con el resto de la red I2P.

Los enrutadores solo pueden conocer la información relativa al siguiente ya que la información que enrutan va cifrada.

Los túneles son unidireccionales por lo que los usuarios deberán crear túneles de entrada y de salida si desean una comunicación bidireccional.

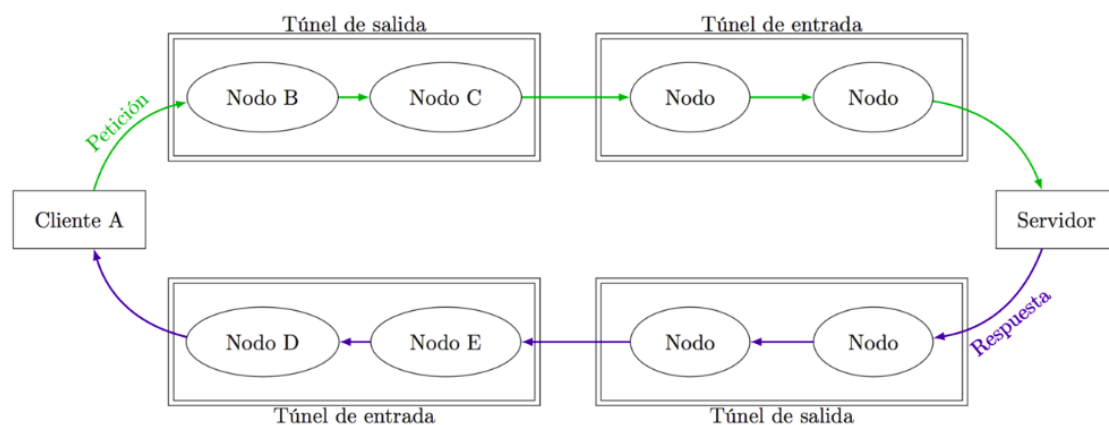


Ilustración 22: Túneles I2P

El usuario A que desea comunicarse con un servidor escoge los nodos que formarán su túnel de salida y los que formarán el túnel de entrada. El túnel de salida del usuario A se conectará con el túnel de entrada del servidor y viceversa.

Puede parecer que este sistema es similar al de TOR, la ventaja de los túneles es que el usuario se conecta a varios nodos, no solo con uno.

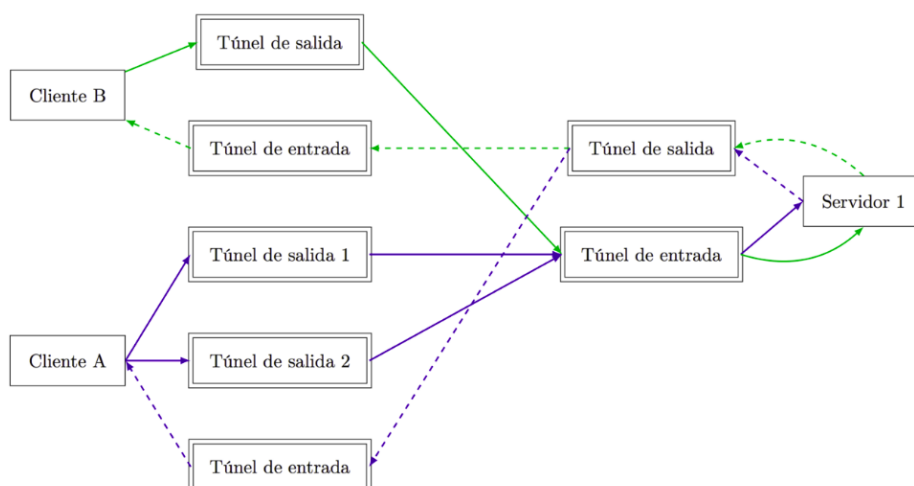


Ilustración 23: Túneles complejos I2P

El mismo túnel I2P de salida puede servir para comunicarse con varios nodos e incluso se pueden configurar túneles de salida en paralelo.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	23/39

6.3.1.2 netDB

Se trata de una base de datos distribuida que contiene dos tipos de datos: información de contacto del router (routerInfo) y la información de contacto del destino (leaveSets).

- **routerInfo:** cuando un usuario de I2P quiere contactar con otro necesitan conocer algunos datos clave que están agrupados y firmados en esta netDB. La estructura routerInfo contiene información relativa a la identidad del router (clave de cifrado ElGamal de 2048 bits, clave de firmado y certificado), dirección de contacto, cuándo fue publicada, firmada de todo lo anterior generada por la clave de firmado de la identidad.
- **leaveSets:** Documenta un conjunto de puntos de entrada del túnel para una destinación de un cliente en particular. Cada uno de los leases define la puerta de salida del túnel del ruter, el ID del túnel (numero de 4 bytes) y cuando expira el túnel.

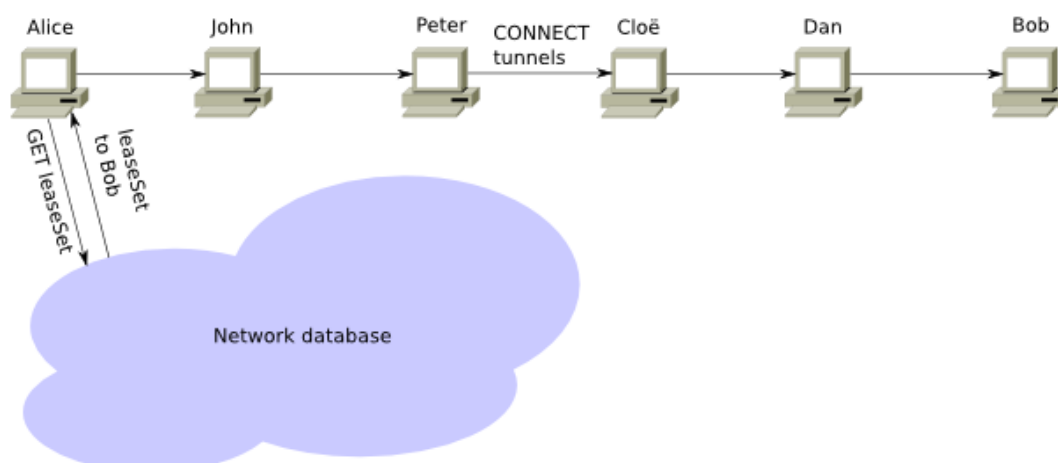


Ilustración 24: Túnel I2P de origen a destino

Cuando un usuario quiere comunicarse con otro nodo consulta en la netDB para encontrar los metadatos relativos al leaveSets del nodo destino, obteniendo el nodo gateway de su túnel de entrada. El usuario genera un túnel de salida enviando un mensaje con instrucciones hacia el gateway del túnel de entrada del destino y éste enruta el mensaje hacia el nodo destino.

Si el usuario desea que el destino sea capaz de comunicarse con él explicitará información relativa al gateway de su túnel de entrada, para que el destino sea capaz de crear otro túnel y tener una comunicación bidireccional.

La netDb se distribuye con una técnica simple llamada "FloodFill", donde un subconjunto de nodos, llamados nodos "floodfill", mantienen la base de datos distribuida y sincronizada.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	24/39

6.3.1.3 Capas y protocolos

La pila de protocolos soportados en I2P siguen el modelo clásico OSI para comunicaciones en Internet pero implementa algunas capas y protocolos específicos de I2P.

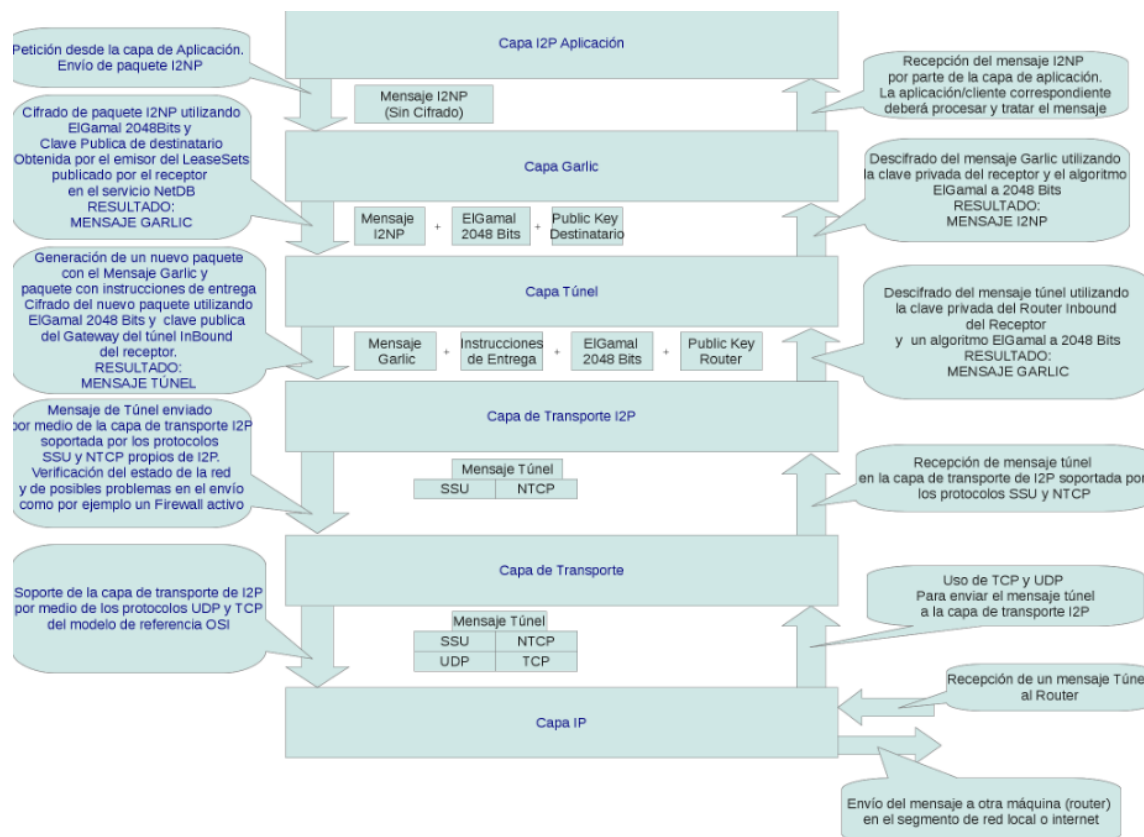


Ilustración 25: Capas y Protocolos I2P

Capa de Aplicación

En esta capa se encuentran las aplicaciones y herramientas que ofrece I2P, permiten el acceso a los usuarios a los servicios que corren en ésta red. I2P soporta comunicaciones basadas en protocolos TCP, UDP o ICMP.

Capa de cifrado Garlic

En esta capa se provee el cifrado de los mensajes y la correcta entrega de los mismos. Comunica la capa de aplicación con las inferiores haciendo que éstas últimas no puedan descifrar las comunicaciones a enviar o recibir.

Todos los mensajes en I2P tienen un formato y una estructura definida, estos mensajes son conocidos como I2NP (I2P Network Protocol) y estos pueden ser usados para mezclarse o difundirse otros mensajes que sean transportados hacia el nodo destino. En esta capa se transportan mensajes Garlic, que son mensajes cifrados y

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	25/39

recubiertos por un mensaje standard que contiene información relativa a la entrega al usuario final. Además se aplica un cifrado al mensaje con la clave pública del destinatario. En esta capa también se incluyen las capas de cifrado de los participantes del túnel de salida del emisor.

Capa de túneles

En esta capa se manipulan “mensajes de túnel” (mensajes Garlic con instrucciones de entrega cifradas). Se establecen las comunicaciones seguras en cada túnel. Los mensajes Garlic no pueden ser descifrados pero las instrucciones de entrega pueden ser descifradas por cada nodo del túnel ya que para establecer la conexión entre los nodos se utiliza la misma clave pública, pueden acceder a la información necesaria para enviar el mensaje al siguiente nodo.

Capa de transporte I2P

En esta capa se implementa un cifrado entre dos nodos I2P, el protocolo utilizado depende directamente de aquel que utilice la capa de aplicación. En I2P se utilizan dos tipos especiales de extensiones:

- **SSU**: Protocolo soportado por UDP, proporciona una capa de transporte segura, cifrada y orientada a la conexión. Adicionalmente provee otros servicios como detección de firewalls, servicios NAT o detección de IP. Estos servicios son utilizados por NTCP por lo tanto existe una dependencia entre ambos protocolos.
- **NTCP**: Protocolo de transporte basado en Java y que mejora la eficiencia del protocolo TCP sobre el que está construido. NTCP utiliza una dirección IP y un puerto que por defecto son auto-detectados.

Capa de Transporte

Capa definida en el modelo OSI, basada en los protocolos TCP y UDP que son el apoyo de los protocolos implementados en la capa de transporte I2P (SSU y NTCP).

Capa IP

La capa de nivel más bajo que proporciona conectividad entre dos máquinas, se trata de la implementación standard del modelo OSI

6.3.1.4 Hidden Services

En I2P no existe un sistema de resolución de nombres al estilo DNS, se utiliza un sistema de nombrado básico que vincula un dominio .i2p con una dirección en base32 o base64. Esta dirección constituye una firma del hidden service e incluye la información necesaria para poder acceder a él.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	26/39

La red I2P permite acceder a todo tipo de hidden services, soporta protocolos conocidos como SSH, FTP, SMB, SMTP, etc. Tanto la conexión a dichos servicios como la creación de éstos se realiza de una manera transparente al usuario.

Los servicios web disponibles en I2P son conocidos como eepsites y no son accesibles directamente desde Internet.

Cuando un usuario establece una conexión en la red I2P es posible que note lentitud en la red al principio incluso no pudiendo acceder a ciertos contenidos, a medida que transcurre el tiempo y su conexión sea conocida en la red contará con suficientes nodos para establecer túneles más eficientes y su conexión mejorará.

6.3.2 Instalación y testeo

6.3.2.1 i2prouter

El equipo que he utilizado para la instalación del I2P es el mismo que en el caso de TOR, corre un sistema operativo Ubuntu 16.04.

He instalado el paquete I2P a través del instalador de paquetes aptitude:

```
$ sudo apt-add-repository ppa:i2p-maintainers/i2p
```

```
$ sudo apt-get update
```

```
$ sudo apt-get install i2p
```

Una vez instalado el paquete ya podemos ejecutar una instancia de I2P.

```
$ i2prouter start
```

Con el servicio I2P corriendo ya podemos acceder al servidor web desde un navegador web a través del puerto 7657.

The screenshot displays the 'CONSOLA DEL ROUTER I2P' interface. On the left, a sidebar shows connection statistics: 'ANCHO DE BANDA ENTRANTE/SALIENTE' with 3S at 1.47 / 1.62 KBps, 5 Min at 0.25 / 1.96 KBps, Total at 1.56 / 1.52 KBps, and Usados at 641 KB / 876 KB. Below this, it indicates 'Red: Bien' and 'Resembrado exitoso, se descargaron 154 router info'. The main content area features a welcome message dated 4/06/18, stating '¡FELICIDADES!, HAS INSTALADO I2P CON ÉXITO.' and providing instructions on how to configure the bandwidth and proxy. A grid of application buttons is visible, including 'Administrar comple...', 'Ayuda', 'Configurar ancho de ...', 'Configurar interfaz d...', 'Consola del router I2P', 'Correo electrónico', 'Libreta de direcciones', 'Personalizar Barra la...', 'Personalizar página ...', 'Servidor web', and 'Torrents'. At the bottom, there is a section for 'SERVICIOS OCULTOS DE INTERES' with links to 'anoncoin.i2p', 'Complementos de I2P', 'Documentos técnico...', 'echelon.i2p', 'exchanged.i2p', 'Foro de desarrollo', 'Foro de I2P', 'Informes de fallos d...', 'Pastebin', 'Planet I2P', 'Preguntas frecuente...', 'Sitio web del proyecto', 'stats.i2p', 'The Tin Hat', 'Trac Wiki', and 'Wiki de I2P'.

Ilustración 26: Interfaz principal I2P

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	27/39

6.3.2.2 i2ptunnel

Es posible configurar y gestionar los diferentes túneles a partir de la interfaz de administración que ofrece el servicio web de I2P. Para ello accedemos a <http://127.0.0.1:7657/i2ptunnelmgr>.



Ilustración 27: Gestión de túneles

Por defecto i2ptunnel cuenta con dos túneles configurados que permiten acceder a la red I2P a partir de proxys utilizando HTTP y HTTPS además de servidores de correo.

6.3.2.3 i2ptsnark

Como se ha mencionado anteriormente el proyecto I2P cuenta con un cliente de torrent. Para acceder a su interfaz entramos en <http://127.0.0.1:7657/i2psnark>



Ilustración 28: Cliente Torrent por I2P

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	28/39

6.3.2.4 SusiMail

Se trata de un cliente de correo para el envío y recepción de mensajes de manera anónima.

Para generar una cuenta compatible con SusiMail accedemos a la dirección http://hq.postman.i2p/?page_id=16

desired accountname: @mail.i2p

desired password:

repeat password:

Your nick/handle:

Do you want to appear in the public addressbook? (Yes/No)

Proceed

Ilustración 29: Registro en postman

Una vez generada (puede llegar a tardar algunos minutos en estar disponible y funcional) ya podemos iniciar sesión con ella en la herramienta SusiMail incluida en la plataforma I2P a partir de la dirección <http://127.0.0.1:7657/susimail/>

INICIO DE SESIÓN DE I2PMAIL

Usuario @mail.i2p

Contraseña

Host

Puerto POP3

Puerto SMTP

[Aprende sobre I2P mail](#)
[Crear una cuenta](#)

Ilustración 30: Inicio de sesión en SusiMail

Nuevo Comprobar correo Desconectarse

De Asunto Fecha Tamaño

No hay mensajes

susimail © 2004-2005 susi

Ilustración 31: Interfaz principal SusiMail

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	29/39

Es posible gestionar algunos aspectos de la cuenta de correo a través del enlace http://hq.postman.i2p/?page_id=19.

4. Account Management

Manage Account Information for iraxavi

List you in the addressbook? **Yes/No?**

scan incoming mails for viruses? **Yes/No?**

spamtag incoming mails? **Yes/No?**

receive a notification when i'm virus sender? **Yes/No?**

receive a notification when i'm virus recipient? **Yes/No?**

your nick/handle? (optional)

PGP Key upload: *disabled*

automatic key uploads are disabled!

delay of outgoing mail send it out immediately
 delay sending (10-50min)
 batch send it (12:00/0:00 UTC)

Confirm changes with your user password!

Ilustración 32: Gestión de la cuenta postman

6.3.3 Comunidad

Para la búsqueda de eepsites me han sido muy útiles webs que recogen de manera actualizada los últimos sites disponibles, un ejemplo es <http://identiguy.i2p/>

Sites		
Hostname		Last Reachable
102chan.i2p	a b	2018-06-04 17:41:49
1st.i2p	a b	2018-06-04 18:45:34
2cnnkdi24ep1wz5irb5w55ugk3cbsotnfiw13vf2oct2ix26nvsa.b32.i2p		2018-06-04 17:42:08
6d2tru665udixwb7miyml7joxusehrwmbikvijpwwwwdpand2lza.b32.i2p		2018-06-04 19:21:26

Ilustración 33: eepsites en línea

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	30/39

Los sites disponibles en esta red son los esperables de una red anónima, unos ejemplos son:

La wiki de I2p: <http://i2pwiki.i2p/>



Ilustración 34: I2P Wiki

Es útil para encontrar artículos relacionados con contenido de la red I2P, por ejemplo en http://i2pwiki.i2p/index.php?title=Directorio_I2P/es se puede encontrar un listado (no actualizado) de sites por categorías.

Blogs y foros sobre privacidad:
<http://libertor.i2p/blog/>

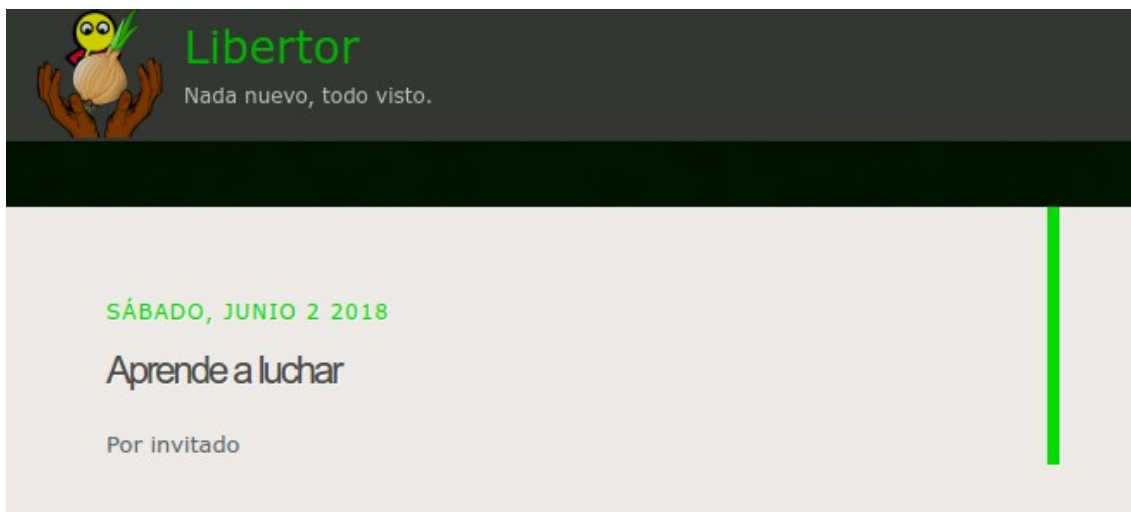


Ilustración 35: Libertor Blog

Cuenta con entradas a artículos sobre darknets y anonimato.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	31/39

<http://def2.i2p/>



Show: [Today's Messages](#) :: [Unanswered Messages](#) :: [Show Polls](#) :: [Message Navigator](#)

Forum

Rocksolid forums - Forums networked with retobbs.i2p, retobbs2.i2p and def3.i2p. Login with guest/guest to post

	Dancing elephants Topics specific for the nodes def2.i2p and def3.i2p, Check this forum also for TOS and announcements.
	Encryption Forum to post public keys and encrypted messages. Also contact data and instructions.
	Entertainment Links to downloads, torrents, articles and so on. Also silly pictures of a negative intellectual level.
	Freenet Discussions and questions about the oldest darknet around.
	General Topics of general interest, technical or social. Also general questions or requests.
	Hacking The art of using technology for your own purposes, and by your own means.

Ilustración 36: Dancing elephants, foro de privacidad

Foro popular y actualizado sobre privacidad y soluciones para el anonimato.

Repositorios de archivos:

<http://ebooks.i2p/>

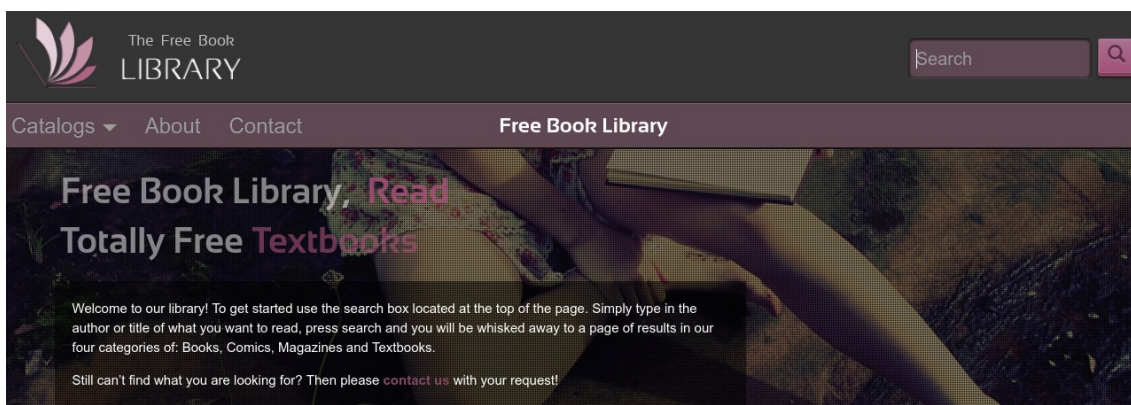


Ilustración 37: Biblioteca de ebooks gratuitos

Biblioteca gratuita que almacena más de 36.000 libros (aparte de comics y revistas) en formato epub.

Repositorios de torrents: <http://torrentfinder.i2p/>, <http://torrfreedom.i2p/>, <http://anodex.i2p/>

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	32/39

O simplemente webs y foros dedicados a temáticas concretas:

<http://exchanged.i2p/en/home>



Ilustración 38: Exchanged, criptomonedas

Información y foro de discusión sobre criptodivisas

<http://garden.i2p/>

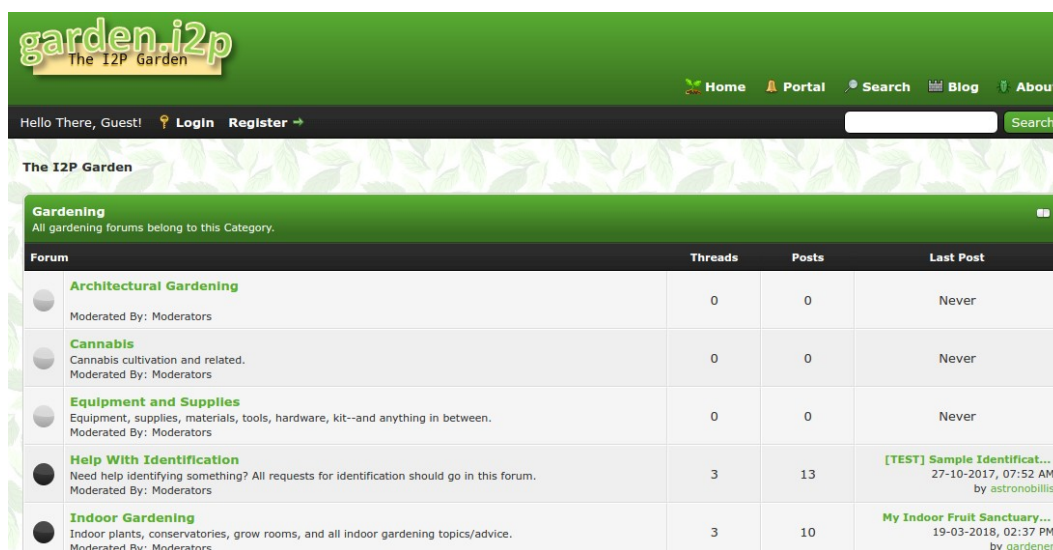


Ilustración 39: Garden, foro sobre plantación de cannabis

Información y foro de debate sobre plantación de cannabis.

<http://anonyradio.i2p/>



Ilustración 40: Streaming de radio por I2P

Eepsite con canales de radio por streaming.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	33/39

6.4 Freenet

6.4.1 Estudio y análisis

Freenet es una red de las redes anónimas más conocidas y sus inicios se remontan a 2001 siendo uno de los proyectos para el anonimato más antiguos.

Este tipo de red se basa en un modelo descentralizado en el que cada uno de los usuarios aportan ancho de banda y espacio de almacenamiento (en este espacio se almacenan datos cifrados de otros usuarios de la Freenet).

Al igual que I2P la red Freenet sigue un modelo de anonimato inproxy, las comunicaciones en esta red quedan restringidas a su propia red privada, sin acceso directo desde Internet.

Del mismo modo que ocurre en TOR y I2P cada usuario aportará ancho de banda para ser utilizado en las comunicaciones de otros nodos siguiendo un mecanismo de onion-routing.

Una característica interesante de Freenet es que permite generar pequeñas darknets, redes en las que solo los nodos considerados como friends pueden conectarse y obtener información de sus comunicaciones.

6.4.1.1 Datastore

Freenet obliga a sus usuarios a reservar un espacio de almacenamiento en sus propios equipos, ese espacio es conocido como Datastore y en él se almacenan datos que otros usuarios aportan a la red. Un usuario tiene escaso control sobre este contenido ya que se encuentra cifrado.

La disponibilidad de los contenidos depende en gran medida de su popularidad, cuantos más clientes accedan a un contenido específico, éste estará replicado en más datastores. Un contenido replicado será eliminado automáticamente cuando ningún usuario de la red Freenet acceda a él en un determinado tiempo.

6.4.1.2 Claves

Como ya se ha comentado anteriormente Freenet funciona siguiendo un modelo descentralizado, para acceder a los contenidos replicados en los datastore se utilizan claves vinculadas a éstos.

Estas claves sirven para poder identificar y descifrar los contenidos almacenados en los datastore de los diferentes clientes de la red.

Las claves de Freenet son hashes sin relación con el contenido que indexan y existen diferentes tipos de éstas:

- **CHK**: Claves Content Hash Key, se tratan de simples hashes de documentos estáticos, identifican de manera única un

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	34/39

documento pudiendo alertar de su modificación. Gracias a esta clave es posible acceder a la clave de descifrado almacenada dentro del fichero y utilizarla para hacer el fichero legible.

- **SSK**: Claves Signed Subspace Key, se tratan de claves que identifican contenidos dinámicos (como los servicios ocultos), utilizan criptografía de clave pública y permiten al autor de los contenidos firmar éstos y únicamente se podrán modificar teniendo la clave privada.

- **USK**: Claves Updateable Subspace Key, se tratan de claves SSK pero sirven para enlazar a éstas con la última versión del contenido. Dependiendo del número de versión de éstas (positivo o negativo) se realizarán búsquedas de versiones superiores o búsquedas profundas de hasta 4 versiones superiores del documento.

- **KSK**: Claves Keyword Subspace Key, se tratan del tipo de claves más sencillas, enlazan directamente páginas etiquetadas en la red Freenet.

6.2.1.3 Hidden Services

Pese a tratarse de un sistema inproxy sin acceso directo a Internet, Freenet proporciona herramientas como listados de servicios ocultos o buscadores de éstos.

Como se ha mencionado anteriormente, la disponibilidad de estos servicios y contenidos queda garantizada por la popularidad de éstos, cuando los clientes navegan por los distintos servicios de la Freenet se almacenan las claves de éstos servicios facilitando así luego su enrutamiento para otros clientes.

Cuando un cliente recibe una solicitud de un servicio oculto o un contenido determinado asociado a una clave primero comprueba si él mismo puede satisfacer la solicitud al contar con esos contenidos en su propio datastore. En el caso de no contar con ellos y asegurarse que la petición ha de ser enrutada se selecciona un listado de clientes que en algún momento han solicitado el contenido asociado a la clave y se selecciona la ruta más óptima.

6.4.2 Instalación y testeo

6.4.2.1 Free Network Project

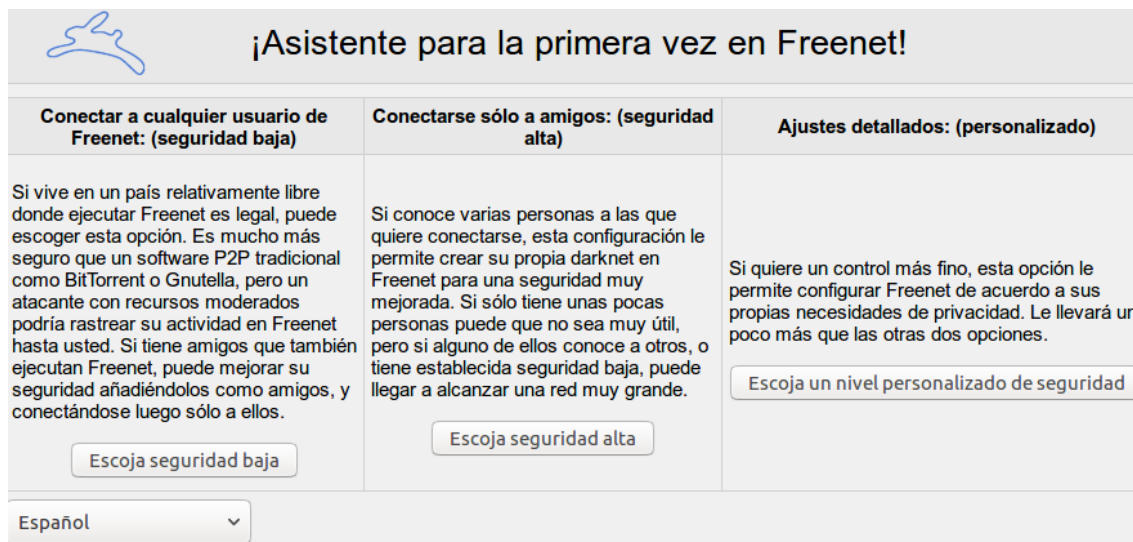
Para la instalación de esta plataforma se requiere descargar un instalador desde la web del proyecto:

<https://freenetproject.org/pages/download.html>

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	35/39

El instalador es bastante intuitivo y al finalizar la descarga y la instalación de los elementos necesarios se despliega el navegador con la dirección del Asistente de Freenet:

<http://127.0.0.1:8888/wizard/>



¡Asistente para la primera vez en Freenet!

Conectar a cualquier usuario de Freenet: (seguridad baja)	Conectarse sólo a amigos: (seguridad alta)	Ajustes detallados: (personalizado)
<p>Si vive en un país relativamente libre donde ejecutar Freenet es legal, puede escoger esta opción. Es mucho más seguro que un software P2P tradicional como BitTorrent o Gnutella, pero un atacante con recursos moderados podría rastrear su actividad en Freenet hasta usted. Si tiene amigos que también ejecutan Freenet, puede mejorar su seguridad añadiéndolos como amigos, y conectándose luego sólo a ellos.</p> <p><input type="button" value="Escoja seguridad baja"/></p>	<p>Si conoce varias personas a las que quiere conectarse, esta configuración le permite crear su propia darknet en Freenet para una seguridad muy mejorada. Si sólo tiene unas pocas personas puede que no sea muy útil, pero si alguno de ellos conoce a otros, o tiene establecida seguridad baja, puede llegar a alcanzar una red muy grande.</p> <p><input type="button" value="Escoja seguridad alta"/></p>	<p>Si quiere un control más fino, esta opción le permite configurar Freenet de acuerdo a sus propias necesidades de privacidad. Le llevará un poco más que las otras dos opciones.</p> <p><input type="button" value="Escoja un nivel personalizado de seguridad"/></p>

Español

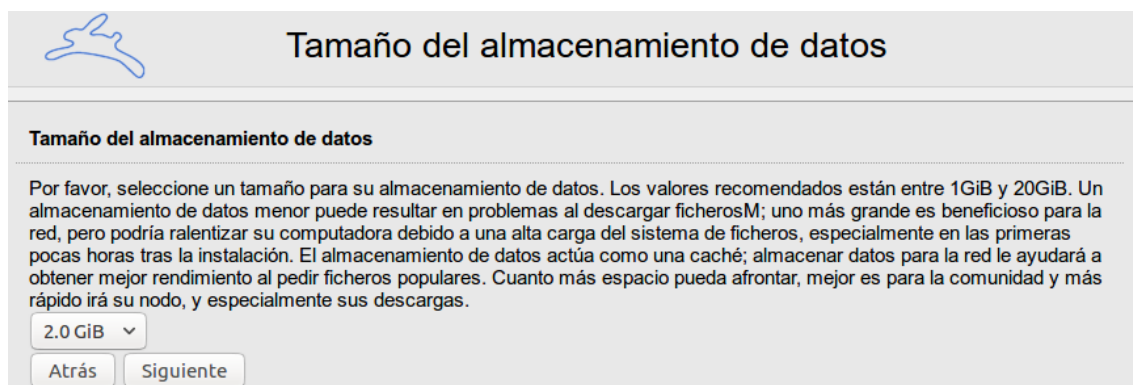
Ilustración 41: Paso 1 Freenet

Con el nivel bajo se asume que el uso de Freenet está permitido en el país desde el que se usa y cualquier usuario de la red podrá utilizar nuestro nodo.

El nivel alto implica que solo podrán conectarse a nuestro nodo nuestros friends, con esto se pueden generar darknets dentro de la red Freenet.

El nivel personalizado permite realizar ajustes de privacidad a medida.

Uno de los parámetros a establecer en esta instalación es el tamaño del datastore.



Tamaño del almacenamiento de datos

Tamaño del almacenamiento de datos

Por favor, seleccione un tamaño para su almacenamiento de datos. Los valores recomendados están entre 1GiB y 20GiB. Un almacenamiento de datos menor puede resultar en problemas al descargar ficherosM; uno más grande es beneficioso para la red, pero podría ralentizar su computadora debido a una alta carga del sistema de ficheros, especialmente en las primeras horas tras la instalación. El almacenamiento de datos actúa como una caché; almacenar datos para la red le ayudará a obtener mejor rendimiento al pedir ficheros populares. Cuanto más espacio pueda afrontar, mejor es para la comunidad y más rápido irá su nodo, y especialmente sus descargas.

2.0 GiB

Ilustración 42: Paso 2 Freenet

Como ya hemos mencionado Freenet recomienda disponer del máximo espacio posible pero como sugerencia se establece un tamaño del 5% del espacio si la capacidad disponible es mayor de

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	36/39

20Gb, 10% si es mayor de 10Gb, 512Mb si es menor a 10Gb y 256 si es menor de 5Gb.

Otro parámetro a configurar es el ancho de banda a ceder.

Ilustración 43: Paso 3 Freenet

Con todo esto ya tenemos en marcha una instancia en la red Freenet.

6.4.3 Comunidad

La interfaz principal de Freenet ya recomienda unos sites que listan una amplia variedad de webs disponibles en la red Freenet:

Nerdageddon:

<http://127.0.0.1:8888/USK@tiYrPDh~fDeH5V7NZjpp~QuubaHwgks88i wIRXXLLWA.yboLMwX1dChz8fWKjmbdtl38HR5uiCOdiUT86ohUyRg.AQA CAAE/nerdageddon/247/>

Ilustración 44: Nerdageddon

Contiene un listado actualizado y controlado de sites disponibles.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	37/39

Enzo's Index

<http://127.0.0.1:8888/USK@XJZAi25dd5y7lrxE3cHMmM-xZ-c-hlPpKLYeLC0YG5l,8XTbR1bd9RBXIX6j-OZNednsj8Cl6EAeBBebC3jtMFU,AQACAAE/index/711/>

Ilustración 45: Enzo's Index

Listado muy completo y organizado (permite aplicar filtros) de distintos sitios web disponibles en la red Freenet.

Los sites disponibles en esta plataforma de anonimato siguen la misma línea que los encontrados en TOR y I2P, multitud de blogs sobre privacidad, foros de discusión privados, repositorios de ficheros... A simple vista parece una red más amplia que I2P y es sencillo encontrar sitios web, algunos ejemplos son:

Biblioteca Calibre

<http://127.0.0.1:8888/USK@ueGkuYERvLyWLwbDf-fYNn~qIZR7KG~FNALH3DWpUyo,MEsM7dD-r5ij6ePo9cXPS9CE4lhuEMRkZcykH-akvos,AQACAAE/calibre/10/>

Biblioteca Calibre

Ilustración 46: Biblioteca Calibre

Biblioteca de libros en formato epub disponibles en castellano.

Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	38/39

Freesite HOWTO

<http://127.0.0.1:8888/USK@8r-uSRcJPkAr-3v3YJR16OCx~lyV2XOKsiG4MOOQBMM,P42IqNemestUdal7T6z3Og6P-Hi7g9U~e37R3kWGvJ8,AQACAAE/freesite-HOWTO/4/>

Freesite HOWTO

FProxy

Freesite Addresses

- Content Hash Keys (CHKs)
- Signed Subspace Keys (SSKs)
- Updateable Subspace Keys (USKs)

Designing Your Freesite

- Keep It Simple
- Images
- Activelink Images
- Favicons
- Links
- CSS
- Title Tag
- Description Meta Tags

Freesite HOWTO

This is a guide to making websites for use on Freenet, known as **freesites**. The process is similar to making standard websites, but there are few things that work differently due to things like the latency and storage model of Freenet. I also give some tips on how to ensure that your freesite is accessible as fast as possible to the highest number of readers, and how to publicise it effectively. I will assume you have a basic knowledge of HTML.

The basic idea is that you design your webpage as usual using HTML and CSS and then you upload the files to Freenet using an **SSK** key.

FProxy

FProxy is the magic that allows you to use a standard web browser to view freesites.

Ilustración 47: Freesite HOWTO, tutorial para montar una web en Freenet

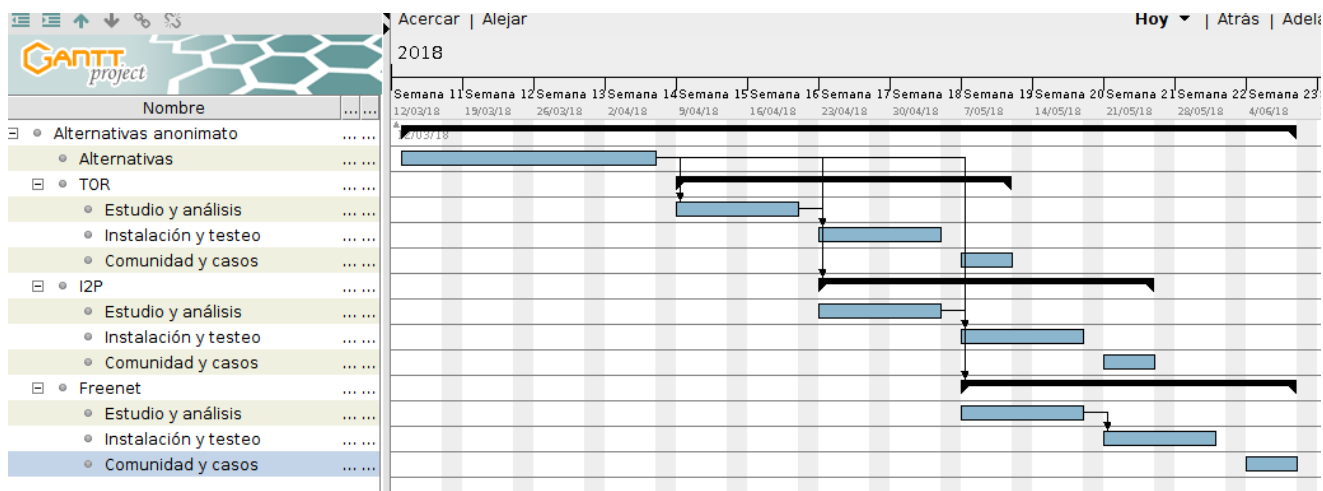
Existen variedad de webs pensadas para enseñar a poner en marcha un servicio web en la propia red Freenet. No es difícil encontrar tutoriales básicos y avanzados en distintos idiomas.

7. Planificación

7.1 Fases

Tras estudiar y analizar las diferentes alternativas y plataformas para el anonimato web, empecé con el estudio a nivel técnico de TOR y tras eso lo instalé y probé, empezando a la vez el estudio de I2P. Tras finalizar a su vez el estudio de Freenet y probado el resto de herramientas navegué por los contenidos web de las plataformas analizadas y documenté algunos de los sites más llamativos.

7.2 Diagrama



Un paseo por la Deep Web	1
Fco. Javier García Vázquez	04/06/18
PEC4	39/39

8. Fuentes de información

[1] TOR Project - [en línea]

<https://www.torproject.org/docs/documentation.html.en>

[2] Dark Web News, Silk Road - [en línea]

<https://darkwebnews.com/darkwebmarkets/silk-road-3/>

[3] Dark Web Map - [en línea]

<https://blog.hyperiongray.com/dark-web-map-introduction/>

[4] Hidden Wiki | TOR .onion urls directories - [en línea]

<https://thehiddenwiki.org/>

[5] The Invisible Internet Project- [en línea]

<https://geti2p.net/en/about/intro>

[6] Security Inside, I2P - [en línea]

<https://securityinside.info/i2p-una-red-anonima-que-deberias-conocer/>

[7] The Hacker Way, Arquitectura y protocolos en I2P - [en línea]

<https://thehackerway.com/2011/12/12/preservando-el-anonimato-y-extendiendo-su-uso-arquitectura-y-protocolos-utilizados-en-i2p-parte-xxviii/>

[8] The Freenet Project, Documentation - [en línea]

<https://freenetproject.org/pages/documentation.html>

[9] Pablo Yglesias, Freenet una alternativa inproxy a TOR o I2P - [en línea]

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

[10] Deep Web: TOR, Freenet, I2P -Privacidad y anonimato- Daniel Echeverri -- [ISBN 978-84-608-4628-4]

<https://0xword.com/es/libros/75-deep-web-tor-freenet-i2p-privacidad-y-anonimato.html>