3. Protección de Datos

5. Anonimato y Deep Web

5.1 Introducción

Internet nos permite compartir información, estar en contacto con familiares y amigos, acceder a recursos muy interesante, pero también estamos dejando a la vista datos personales incluso si no somos conscientes de ello.

En los últimos años ha empezado a ganar importancia la posibilidad de ocultarnos, de navegar en Internet de forma anónima.

¿Cuáles son los objetivos de la ocultación de identidad o el anonimato?

- Derecho a la privacidad y al anonimato
- Evitar que se conozca nuestra IP y/o hábitos de navegación
- Acceder a contenido sin censura
- …
- "Otros" objetivos…

5.2 Uso de Proxies

Una de las formas habituales de ocultar nuestra identidad en Internet es el uso de proxies o intermediarios.

Una IP proporciona mucha información y no queremos revelarla de forma pública. Se puede ocultar la dirección IP usando un proxy:

- El proxy actúa como un intermediario
- El destinatario ve la IP del proxy

Podemos describir dos tipos principales de proxies:

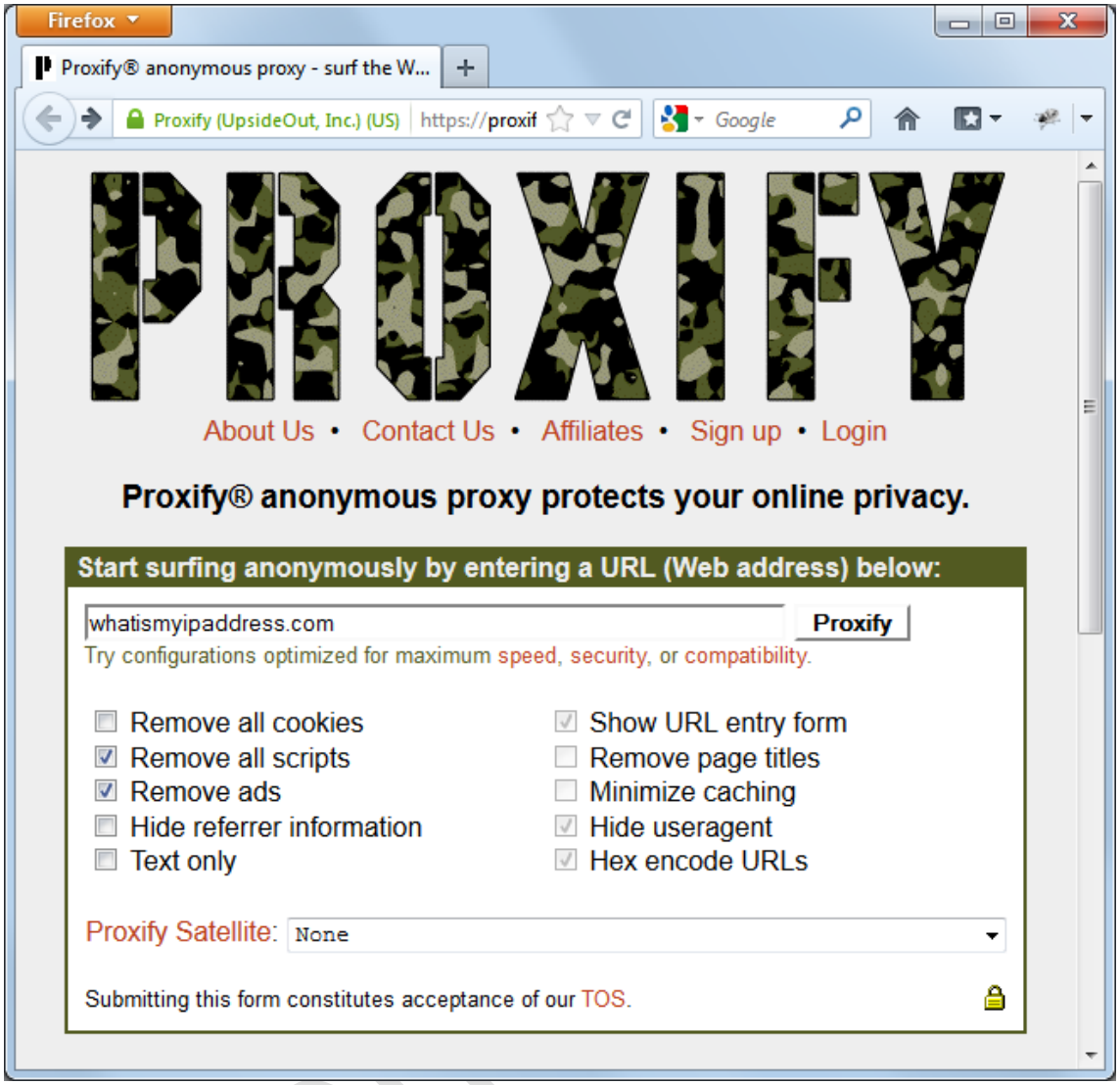
- Web-based Proxies
- Open Proxies

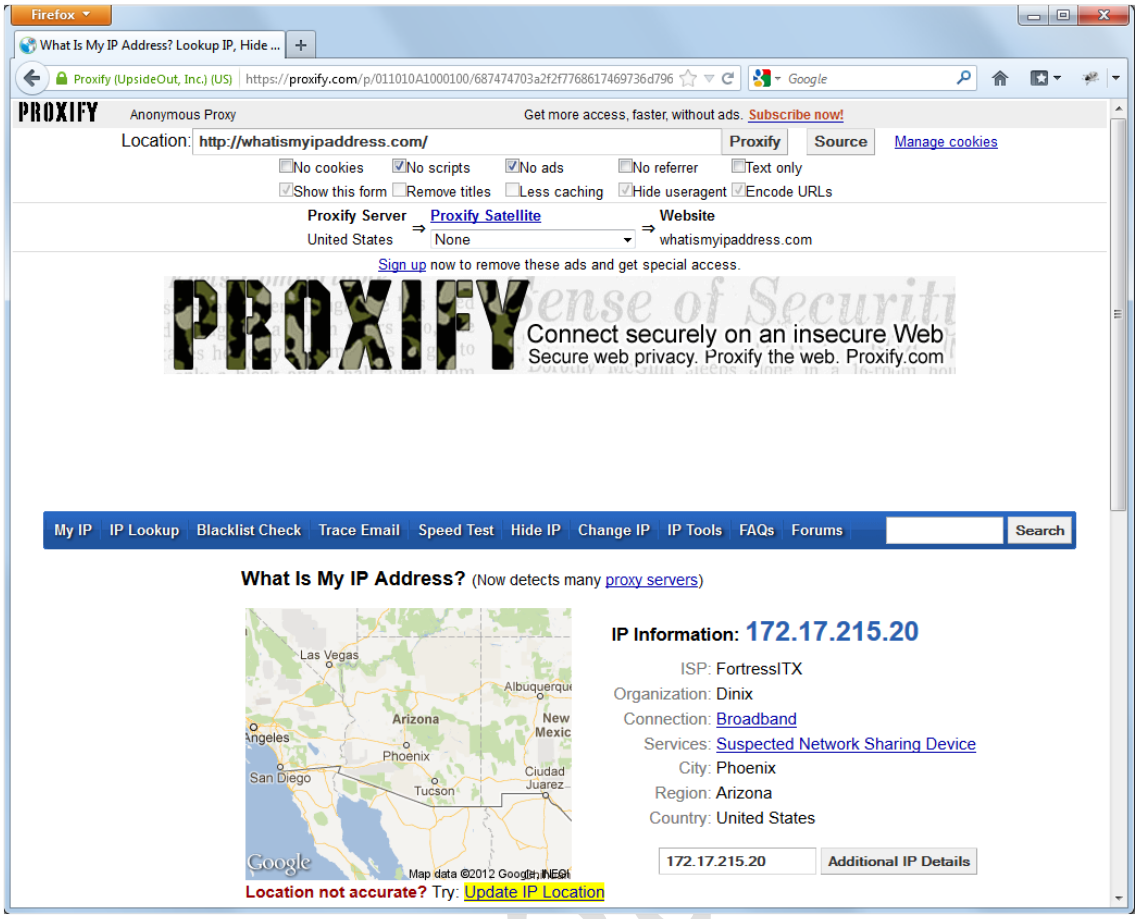
Los Web-based Proxies son sitios Web que permiten acceder al contenido de terceros y que no requieren configuración en cliente (se accede a través del navegador). Son capaces de ocultar la dirección IP del usuario lo que le proporciona cierto nivel de privacidad. Además, la mayoría de los proxies cifra el tráfico entre el usuario y el proxy (ofreciendo también confidencialidad).

El inconveniente es que algunas páginas pueden no mostrarse correctamente, la navegación puede ser más lenta y que la mayoría de proxies se financian cobrando una cuota a los usuarios o mediante publicidad.

Tenemos una lista en:

http://proxy.org/cgi_proxies.shtml





En los Open Proxies el cliente debe configurar los datos del proxy. Después de eso, la navegación es "transparente" para el usuario.

Podemos dividirlos en dos tipos:

- HTTP
- SOCKS

No alteran la página original.

Ejemplos:

http://proxyhttp.net/

http://sockslist.net/

El problema con los proxies es que detrás de ellos hay alguien gestionándolos y si la conexión es en claro (no cifrada, p.ej. http) el proxy puede leer todo el tráfico.

5.3 VPN

Otra forma de conseguir privacidad es el uso de VPNs (Virtual Private Networks).

Hay servicios comerciales ofrecen aplicaciones para establecer una conexión a través de VPN

- Mediante un software cliente, se crea un túnel entre el equipo cliente y un servidor de la organización proveedora del servicio
- Depositamos nuestra confianza en la organización
- Un ejemplo es Anonymizer
    - De pago. Versión Trial, pero no para España
    - Desactiva JavaScript
    - Sede en EE.UU.
    - http://www.anonymizer.com/
- Otros: Hotspot Shield, Tunnelbear, …

La calidad, fiabilidad y eficacia de estos servicios varía mucho de unos a otros.

5.4 Anonimity Networks

Son redes que permiten a sus usuarios comunicarse de forma anónima. Entre otras características:

- Usan cifrado por capas (onion routing)
- Los usuarios comparten sus recursos con la red (ancho de banda,…)
- Ralentizan la comunicación
- Ejemplos: Freenet, I2P, JAP, y TOR

5.4.1 La Red Tor

Tor (The Onion Router) Es un servicio online que mediante un software específico permite conectarse a una red de comunicaciones de baja latencia que brinda anonimato a sus usuarios.

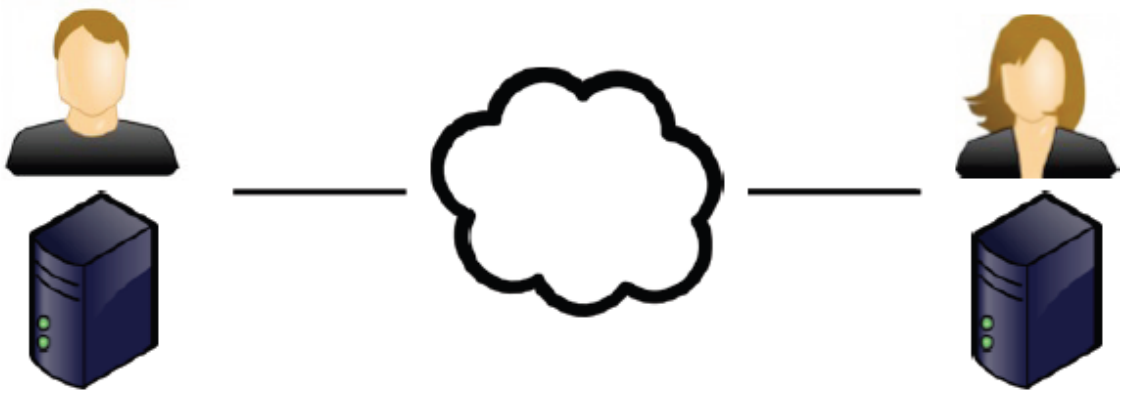
Surge en el 2003 y se basa en el proyecto OR del Laboratorio de Investigación Naval de los Estados Unidos, entidad que financio el proyecto hasta que en 2004 paso a manos de la EFF www.eff.org.

En la actualidad y desde el 2005 el proyecto está en manos de Tor Project, una entidad sin fines de lucro dedicada a la investigación. https://www.torproject.org

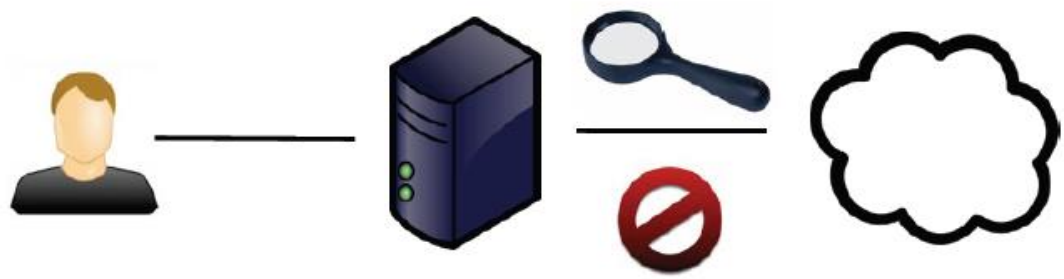
El proyecto TOR es de código abierto y está en permanente evolución.

Según fuentes oficiales se estima que TOR es utilizado diariamente por unos 300.000 usuarios aproximadamente.

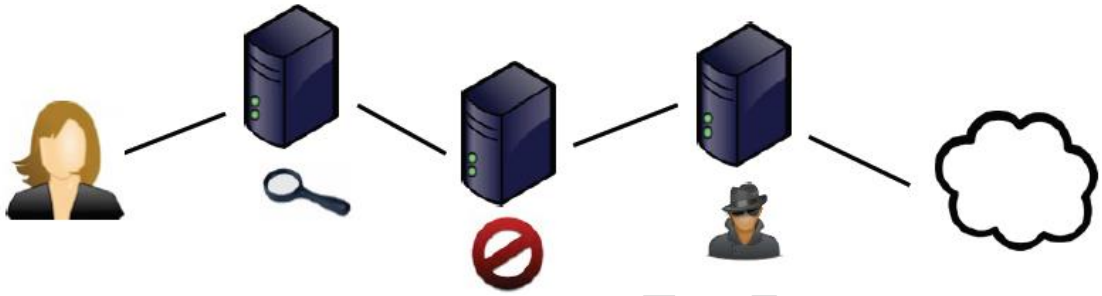
No debe confundirse a TOR con el funcionamiento que tienen las redes P2P.



Tampoco es un servicio de Proxy, porque los servicios tradicionales del tipo Simple Proxy descansan sobre un único punto que intermedia el tráfico entre el destino y el origen.



Del mismo modo, Tor no es un servicio de Proxy Chain. Los servicios de encadenamiento de Proxies son igualmente arriesgados e ineficientes ya que la ruta es siempre estática y podría ser controlada por un usuario malintencionado.

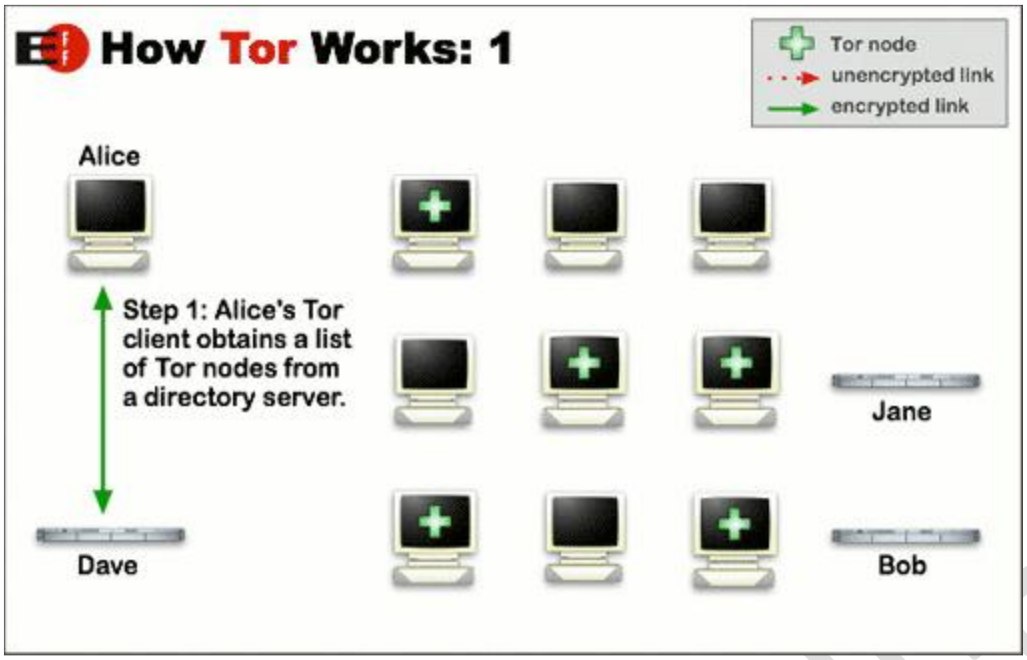


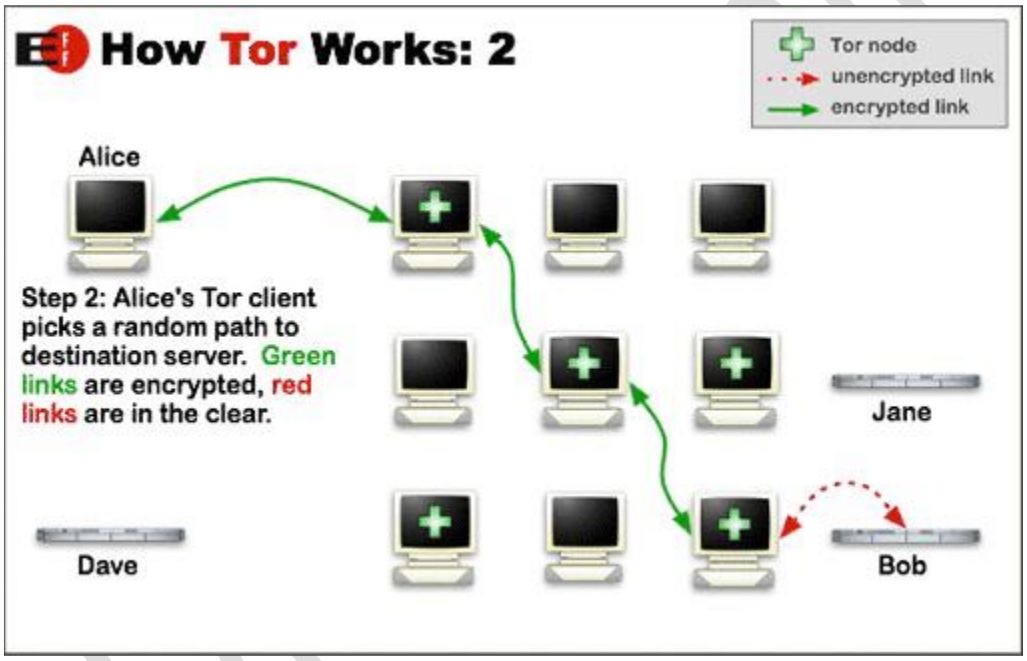
Los componentes de Tor son los siguientes:

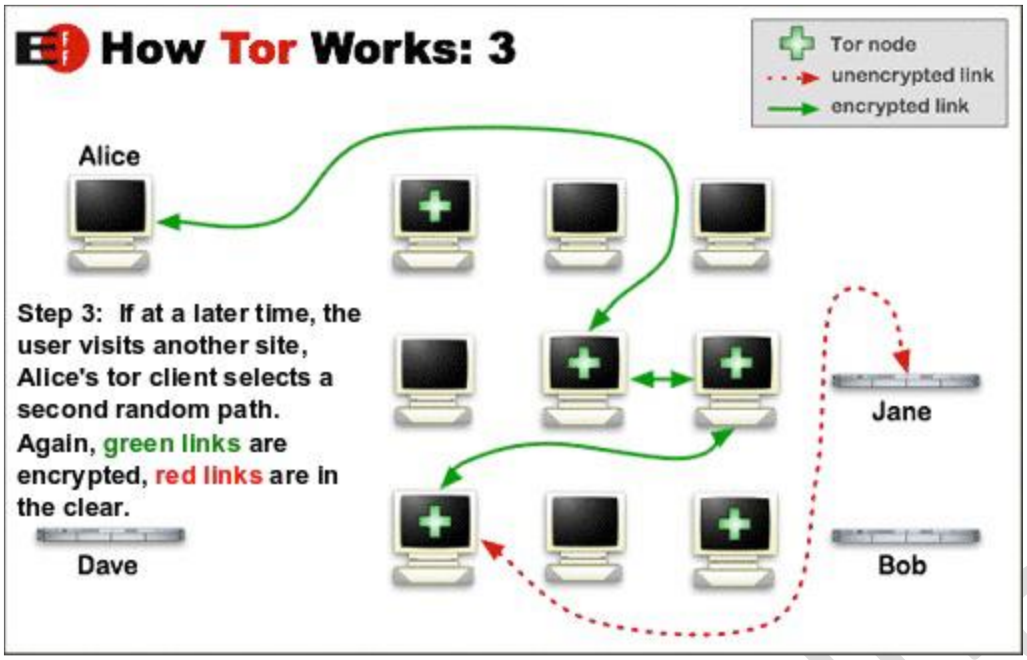
- OP (Onion Proxy) Cliente: Representa al cliente, quien mediante un software específico, se conecta a la red TOR https://www.torproject.org/download/download-easy.html.en
- OR (Onion Router) de Entrada, Intermedio, de Salida, Servicio de Directorio

Los Onion Routers son los responsables del direccionar el tráfico que les envían los OP, lo hacen multiplexando el trafico TCP. Se conectan entre ellos utilizando un canal seguro de comunicación que brinda integridad y confidencialidad. Dependiendo su ubicación en una conexión pueden cumplir diferentes roles y funciones.

- OR-Servicio de Directorio: El OR que cumple esta función almacena información sobre los demás OR, esta información se conoce como router descriptor. Esta información es compartida entre los OP y los OR permitiendo “dibujar” la red a cada momento y de esta forma permitir la conexión
- OR de Entrada: Es el OR dentro de la red TOR que recibe contacto directo del OP. Es el único OR que recibe el contacto del origen de la comunicación, es decir la IP origen real.
- OR Intermedio: Es el OR intermedio solo recibe comunicaciones de otro OR y procede a direccionar el tráfico al destino especificado. Los OR Intermedios no pueden repetirse nunca dos veces en el mismo circuito.
- OR de Salida: Es el OR encargado de llevar el tráfico a su destino final. Es el único OR del circuito que tiene conocimiento del destino final del tráfico.


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Jane
Dave
Bob


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob



TOR es considerado como la tercera generación de Onion Routing .El OP realiza un intercambio de claves telescópico (OP>ORn>ORn1>ORn2) este posee una clave de sesión diferente con cada OR.

El OP utiliza las claves en este orden:

1. Primero cifra el paquete con la clave del ultimo OR
2. Segundo cifra el paquete con la clave del penúltimo OR
3. Tercero cifra el paquete con la clave del primer OR
4. Cada OR quita la capa que le corresponde y no puede ver el resto, por ende no conoce nunca la totalidad del circuito. Solo sabe el salto anterior y el posterior

¿Qué ofrecer Tor?

- Navegación
- Correo Electrónico
- Mensajería Instantánea
- Almacenamiento
- Redes Sociales
- P2P
- Cualquier otra actividad o aplicación que pueda ser TORIFICADA (Protocolo TCP, Soporte SOCKS)

Y también:

- Hidden Service: TOR le permite a un usuario publicar diferentes servicios sin que nadie que los acceda pueda identificar su ubicación real. Por supuesto que tampoco el Hidden Service puede identificar la ubicación real de quienes lo están utilizando.
- El HS genera a su vez un dominio.onion que será publicado en una base de datos para que pueda ser ubicado por los clientes. Este estará compuesto por 16 caracteres únicos que se derivan de una función de hash sobre la clave pública del HS.
- Cuando un cliente desea acceder a un HS, busca la información de su descriptor en la base de datos y genera un circuito hacia él.

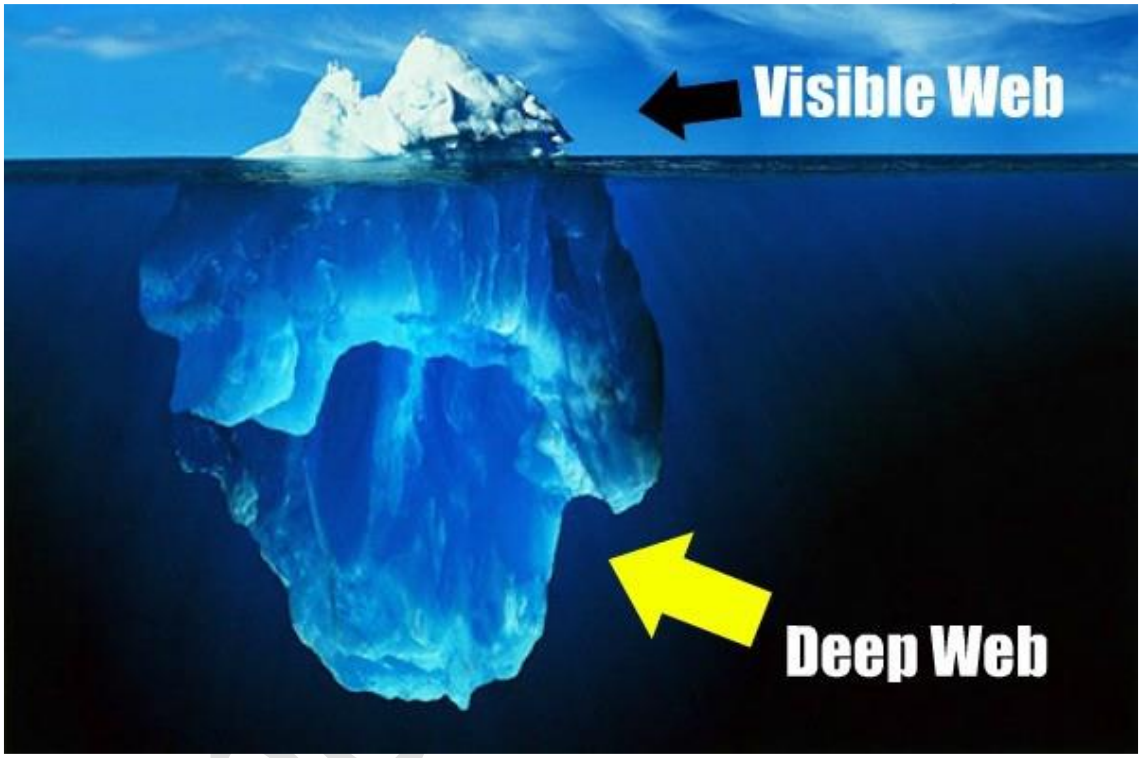
- El circuito se genera eligiendo un OR al azar y asignándole la función de RP (Rendezvous Point) y otros 2 OR en su función clásica.
- El RP (Rendezvous Point) nunca obtiene información de la ubicación del HS preservando de esta forma su anonimato.

5.5 Deep Web

La deep web o Internet profunda son redes que escapan a los buscadores más conocidos de la superficie, de ahí su nombre. Sus páginas, manuales, documentos..., no están indexados y necesitamos usar programas específicos para poder acceder a ellas. Son las bases de datos no indexadas, son redes que no quieren mantener comunicación con la Internet común, son las entrañas de la red, los suburbios. No se trata de un dogma de fe, algo supuesto e intangible; en el 2000 se hablaba de 7.500 TeraBytes de información.

http://es.wikipedia.org/wiki/Internet_profunda

Tal vez la forma más sencilla, aunque poco original de explicar este fenómeno, sea el iceberg. Es un excelente símil; claro y conciso.

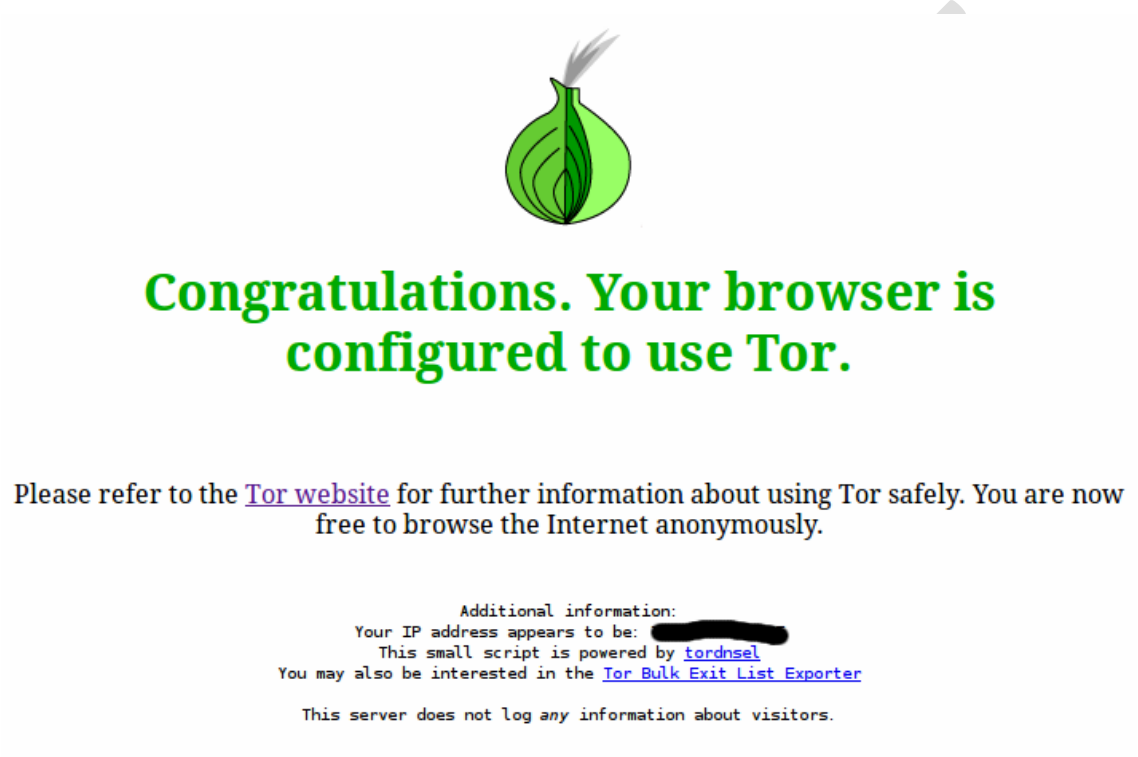


Se dice que la Deep web no se navega, se bucea, y es común sentirse perdido las primeras veces; se trata de un ejercicio nuevo en un elemento conocido, y eso genera cierta confusión y tendencia a abandonar el intento. Los principales problemas con los que tropezamos son los siguientes: No sabemos cuáles son los enlaces de interés ni sabemos cómo llegar a ellos. También es común que al intentar acceder a un servicio de la Deep web, este se encuentre caído, perdido o muerto. Hay que tener en cuenta que el mantenimiento de estas páginas, foros, chat, servicios..., no es tan habitual como el de una página web comercial, la de un periódico de éxito o la de un blog conocido en la Internet común, pero como todo en esta vida, no tenemos más que seguir buscando, curioseando e incluso fisgando para poder encontrar cuales son esos buenos enlaces.

Son muchos los servicios y programas que nos permiten bucear por ella y aunque TOR es una de los más conocidos y es sobre el que haremos hincapié, también es cierto que existen algunos otros y que funcionan igual de bien, o incluso mejor que TOR. Cabe mencionar también dos grandes redes que aunque menos conocidas son igual de importantes: FreeNet o i2p. Tenemos que hacer la elección correcta en base a nuestras necesidades ya que todas han sido desarrolladas con diferentes propósitos.

TOR ofrece un software para conectarnos a los diferentes proxyes de su red. Para ello es necesario acceder a su web en la Internet comercial y descargarnos el software en forma de bundle o instalarlo en GNU/Linux usando el gestor de paquetes de nuestra distribución favorita. En los dos casos se recomienda la instalación del Vidalia, su panel de administración, así como Polipo, nuestro propio PROXY. Y en caso de que elijamos la segunda forma de instalación tendremos que instalar el plugin ProxyFoxy para Firefox, en el primer caso el navegador en formato de Bundle ya dispone de la gestión de proxy necesaria para red TOR usando la extensión de Firefox TOR Buttom.

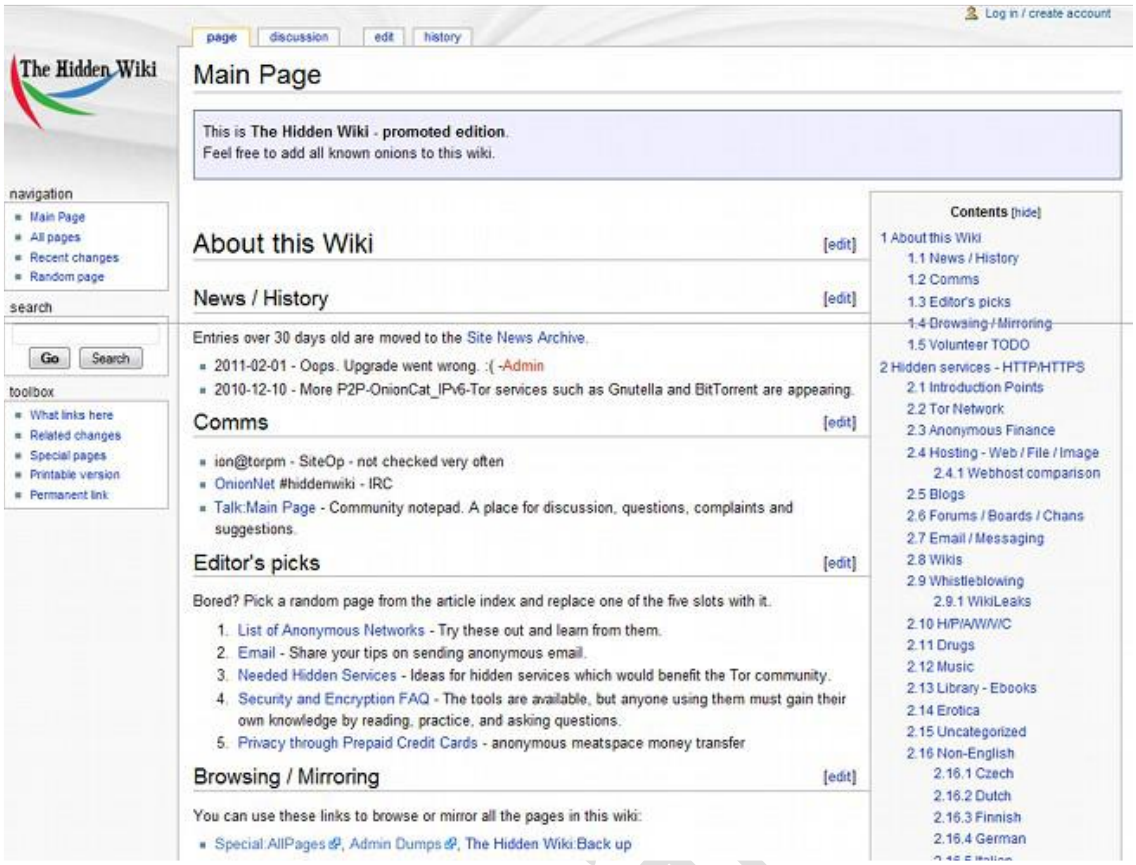
Si todo ha ido bien podremos ir a la web que nos permite mirar si nuestro TOR está bien configurado. En caso de que todo este correcto ya podremos hacer nuestra primera inmersión a UNO de los suburbios de Internet, The Onion Web.



Los servicios que podremos encontrar en la deep web son comúnmente conocidos con Hidden Services o servicios ocultos y no van mucho más allá de los servicios que podemos encontrar en la Internet común, pero tienen el añadido de la privacidad:

- Foros
- comercio electrónico (donde aseguran el anonimato)
- bibliotecas de documentos en PDF o TXT
- servidores de correo...
- y sobre todo muchas cosas que tacharíamos de menos interesantes en la internet común, pero que aquí adquieren el valor añadido de gestionar correctamente nuestra privacidad.

Una de las webs de referencia en TOR es The hiden Wiki, La wiki oculta, allí con mucha frecuencia se cambian los enlaces a las webs más comunes dentro de TOR, buscadores internos, repositorios de documentación importante, enlaces a foros de interés..., incluso enlaces a cosas que no nos gustaría tener que ver, lo dicho, los suburbios.



Es muy conocido el mundo de los BitCoin en estos lares del ciberespacio, todo se paga con una moneda digital, global, anónima y P2P. Esta moneda tiene buena fama dentro de todos los usuarios de este tipo de servicios y cada vez estamos viendo que llega más arriba ya que hoy por hoy es bastante común encontrarnos con BitCoin en la Internet comercial. BitCoin es un sistema de pago en la que todos los pares validan todas las transacciones que se efectúan en esa red (TODOS los pares TODAS las tansacciones), incluso las que se hayan efectuado antes de que nuestro usuario entrara en la red de BitCoin, por lo tanto tiene carácter retroactivo. Por ello es habitual que al arrancar por primera vez el Wallet de BitCoin tarde en dejarte hacer operaciones, ya que actualmente se descarga y valida unos 3 GB de datos.

5.6 Un Ejemplo de Negocio en la Deep Web

Un ejemplo de qué se mueve en la Deep Web es la conocida Silk Road, que ya ha sido desmantelada por el FBI:

http://www.internautas.org/html/7824.html