PRIVACIDAD EN INTERNET Y TOR

1. Historia
2. Introducción
3. Software recomendado y ejemplos de configuración
4. Resumen
5. Enlaces de interés y ampliación de información.

1. HISTORIA:

El acceso y contenidos en internet son vigilados o censurados. Nuestros correos electrónicos, navegación, acceso a redes sociales o llamadas Skype también están comprometidos por el espionaje masivo de las agencias de seguridad en colaboración con operadores de comunicaciones y empresas como Google, Yahoo, Facebook o Microsoft que facilitan acceso directo a sus servidores.

Con la aparición de las redes anónimas como TOR, servicios VPN se pueden reducir los riesgos, pero la realidad es que el paradigma que debe asumir el ciudadano es que la privacidad en internet no existe.

Expertos en seguridad como Bruce Schneier dice, «la privacidad nos protege de los abusos de quienes detentan el poder, incluso si no estamos haciendo nada incorrecto en el momento de la vigilancia»

El propósito de la red TOR es proteger las comunicaciones y ocultar nuestra IP y lo hace mejor que cualquier otro sistema. Lo que no puede hacer TOR es evitar los fallos de seguridad y vulnerabilidades de otros componentes software, de los sistemas operativos o los malos hábitos del propio usuario final.

Además del riesgo que supone exponer constantemente nuestra vida en las redes sociales hay que añadir que aplicaciones como Facebook pueden leer tus SMS, acceder a tu cámara, leer tus contactos y conocer nuestra ubicación sin nuestro conocimiento, que no consentimiento puesto que cuando instalamos estas herramientas les otorgamos ese tipo de privilegios.

Además la simple navegación de las WEBs que visitamos incluye otro tipo de ataques de menor intensidad a nuestra privacidad por el bombardeo de publicidad, herramientas de rastreo, cookies, historial de navegación, etc.

Otra buena razón para el uso de TOR es que permite evadir la Censura de acceso a ciertos sitios de Internet que practican algunos Países.

En cuanto a los terminales móviles, los smartphone no se diseñaron pensando en la seguridad y privacidad del usuario. La mayoría de software existente está mal diseñado o mal desarrollado. Tanto iPhone como Android cuentan con vulnerabilidades relacionadas con las conexiones y sincronizaciones con otros aparatos, aplicaciones y redes. Todas las apps de juegos tienen agujeros de seguridad y son un peligro para la privacidad. , pero lo peor aparte de las vulnerabilidades es que se descubren diariamente modelos de Smartphone que incluyen malware preinstalado en los terminales, ocultos para el usuario codificados dentro de aplicaciones legitimas .

Los teléfonos blackphone basados en un Android securizado y diseñados exclusivamente pensado en la seguridad son caros y no han terminado de cuajar en el mercado. Para el resto de usuarios tenemos SW profesional y libre para securizar las comunicaciones y los datos de nuestros terminales.

En cuanto a TOR, las vulnerabilidades conocidas que han afectado a sus usuarios están relacionadas con componentes software de terceros como los navegadores, también el navegador Firefox modificado en el cual se basa "Tor Browser" inicialmente en su versión para Windows tuvo vulnerabilidades relacionadas con Javascript. Aparte de los fallos de seguridad por el uso de software de terceros y malos hábitos del propio usuario, se han documentado algunos ataques en escenarios controlados de laboratorio basados en algoritmos de correlación de tráfico pasivos que analizan el flujo de paquetes o células TOR, no los paquetes a nivel TCP. El atacante debe controlar muchos o todos los router de la red TOR, lo que es materialmente imposible al tratarse de una red distribuida geográficamente a nivel mundial.

En cuanto a **legalidad,** el acceso a internet a través de redes anónimas como TOR no es delito, y tampoco el acceso a la Deep Web o contenidos no indexados en los motores de búsqueda típicos en internet, como google.

Naciones Unidas hizo una declaración oficial sobre TOR: "El cifrado y la navegación web anónima deben protegerse. TOR, VPNs y servidores proxy, en realidad debería de fomentarse. Son los únicos mecanismos para el ejercicio de la libertad de opinión y expresión de forma segura"

TOR es el espacio más seguro posible para activistas políticos, periodistas, profesionales TI, servicios de seguridad, empresarios y otras personas que potencialmente pueden ser vigiladas o perseguidas. La base del principio de TOR no es ocultar sino proteger. "los datos personales del usuario y lo que hace en la Red no es ningún secreto, simplemente no es asunto de personas ajenas", explicó Runa Sandvik (cofundadora de TOR) al portal ruso Lenta.ru

La primavera árabe o la existencia de Wikileaks deben buena parte de su éxito al sigilo permitido por el empleo de la red TOR y la NSA aseguró en un documento confidencial publicado en 2014 que "en el terreno de la seguridad virtual es el rey y no tiene rivales por el trono

Bruce Schneier experto en seguridad y criptografía opina que TOR es una herramienta de anonimato bien diseñada y robusta, y atacarla con éxito es difícil. Los ataques de la NSA que encontramos se hacen de forma individual y tienen como objetivo explotar las vulnerabilidades de los navegadores, y no la aplicación TOR.

La red TOR ha estado en el punto de mira de diversos gobiernos, instituciones y empresas de forma recurrente ya que una red que permite ocultar las comunicaciones y la navegación en general forma sencilla es una potencial amenaza para los que ambicionan un seguimiento ciudadano.

La red TOR sigue creciendo. Hay bancos que permiten conexiones desde TOR a sus sistemas de e-banking ya que no olvidemos que TOR protege las comunicaciones de los usuarios. Facebook y otras organizaciones que poco tienen que ver con el anonimato han abierto nodos directamente en la red TOR. Medios de comunicación, empresas y ejércitos la utilizan para **proteger sus comunicaciones**. Por ello se cree que TOR finalmente será considerada una red Mainstream y no una red oculta en internet.

Como siempre, están también las teorías de la conspiración que apuntan que TOR en realidad podría tratarse de una trampa de las propias agencias de inteligencia de EEUU. En mi opinión esto carece de sentido tras las revelaciones de Eduard Snowden basadas en informes oficiales sobre espionaje masivo que apuntan a la cooperación necesaria de ISP y empresas como Google o Facebook, o los informes que dan a conocer sistemas de hacking inteligente

desarrollados por agencias como FoxAcid que busca explotar las “vulnerabilidades del sistema final de usuario” infectando mediante malware y no de la propia red TOR .

Lo cierto es que Snowden, aparentemente el hombre más perseguido por gobierno de EEUU, habiendo trabajado para sus servicios de inteligencia como experto en seguridad mantiene su defensa y confianza absoluta en TOR. Debería servir este hecho como garantía pero también hay quien duda que Snowden es quien dice ser y no un impostor o falso soplón, con lo cual su defensa de TOR podría tratarse de una nueva trampa.

La mayoría de la gente piensa que TOR es de algún modo hostil a EE.UU, pero de hecho continúa recibiendo la mayor parte de sus fondos de las mismas agencias militares y de inteligencia que lo crearon. En 2013 TOR recibió el 90% de su financiación del gobierno estadounidense, y la mayor parte la recibió del Pentágono.

El FBI, la CIA, las Fuerzas Armadas y todos los gobiernos del mundo también valoran y persiguen el anonimato, solo que en su mundo ideal TOR existiría pero ellos tendrían la llave secreta para forzar la entrada.

El gobierno Estadounidense ha hecho más que nadie para mantenerlo vivo, donando varios millones de dólares a Dingledine y su equipo desde el principio del proyecto en los 90 y gran parte de los fondos del gobierno estadounidense para la libertad de internet vienen de los republicanos.

2. INTRODUCCIÓN

La necesidad de aumentar la privacidad y conseguir el anonimato en Internet ha favorecido la aparición de proveedores de acceso **VPN** SSL/TLS basados en claves pre-compartidas (cifrado simétrico) o claves RSA (cifrado asimétrico) para autenticación y cifrado de los datos y cabeceras de protocolo. Normalmente el servidor es el único que es autenticado, pero el cliente se mantiene sin autenticar ya que para una autenticación mutua se necesita una infraestructura de claves públicas (PKI) en la cual cada parte involucrada en la comunicación tiene dos claves separadas: una clave pública y una clave privada. Cuando alguien quiere enviarte un mensaje cifrado, utiliza tu clave pública para cifrar el mensaje y cuando lo recibimos utilizamos nuestra clave privada para descifrarlo.

Los túneles TLS (también utilizados por la red TOR) ocultan nuestra IP real y protegen nuestra información hasta sus servidores (terminadores VPN) pero a partir de aquí nuestra privacidad está comprometida porque cualquier organización con una infraestructura de sistemas y comunicaciones requiere algún tipo de administración que es inviable sin logs, más aun si se trata de un servicio de pago que requerirá algún contrato o registro por parte del usuario. Todas las VPN gratuitas o de pago registran como mínimo tu dirección IP, hora de conexión y volumen de tráfico. Varios proveedores de VPN anuncian un "servicio anónimo" en su sitio web, pero luego está la letra pequeña de su política de privacidad indicando que si registran cierta información.

Además toda organización está sujeta a un marco legal por el cual tiene obligación de facilitar los datos (sean muchos o pocos) que tenga disponibles cuando sean requeridos por las autoridades competentes en su jurisdicción. El servicio VPN de tunnelbear está en Canadá y oficialmente sus leyes no obligan todavía a estas empresas a mantener y divulgar información de sus usuarios, pero otras como VPNBook ha recibido acusaciones por parte de Anonymous de filtrar los datos de sus usuarios al gobierno.

Hay soluciones software también gratuitas como FortiClient que además de un módulo antivirus incorpora funcionalidades FW, filtrado web y un cliente VPN. O el cliente forticlient para Android que incorpora un módulo de

seguridad web+ cliente VPN SSL o IPSEC contra sus servidores. Aquí utilizaremos los servicios VPN gratuitos de Proton.

El navegador “Opera” antiguamente tenía la opción de instalar un plugin gratuito que establecía una conexión VPN con el proveedor VPN Surfeasy y nos daba 1GB de navegación segura aunque no anónima ya que previamente había que registrase creando una cuenta. Actualmente Opera ya tiene integrado la opción de navegación por VPN simplemente instalando el navegador y marcando la opción VPN y sin registrase, lo que es bastante más interesante.

Resumiendo. Tanto si usamos **“solamente”** servidores proxy públicos anónimos o un servicio público VPN no tendremos demasiadas garantías de confidencialidad y anonimato porque quedarán registradas trazas de nuestro tráfico como la dirección IP, horas de conexión, contraseñas y en el peor de los casos número de cuentas bancarias.

TOR es una red de acceso anónima y descentralizada, gratuita y con alta disponibilidad. La red no está administrada ni es administrable porque no hay registros ni logs. Por eso se dice que en el terreno de la privacidad es el rey. Eso sí, como todo no puede ser perfecto también introduce mayor latencia en la transmisión de datos que otros sistemas de anonimización como podría ser una VPN, pero sin resultar exagerado.

El funcionamiento básicamente consiste en una red de proxys 'relays' que cifran y reenvían las conexiones, añadiendo múltiples capas hasta ocultar cualquier información sobre el origen de los datos. La idea de navegar a través de una lista de proxies anónimos elite en internet que ocultaban la IP original ya se utilizaba hace años con herramientas específicas como multi-proxy pero sin control ni garantías sobre la reputación de los nodos renviadores y con frecuentes problemas de disponibilidad y sin cifrado seguro.

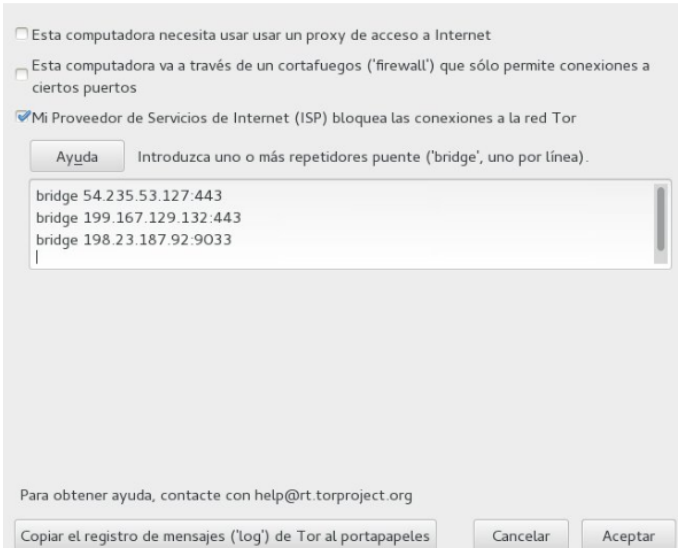
La red TOR está formada por 3 tipos de nodos o routers TOR (entry o guard nodes, relays nodes y exit nodes) en la que participan voluntarios anónimos de todo el mundo que ejecutan software TOR donando parte de su ancho de banda de acceso a internet y también recursos de almacenamiento para anonimizar servidores del dominio ONION. Normalmente estos servicios se prestan a través de algún hosting contratado TOR no es la única red de acceso anónimo, hay otras como I2P o freenet en evolución, cada una con sus propias características.

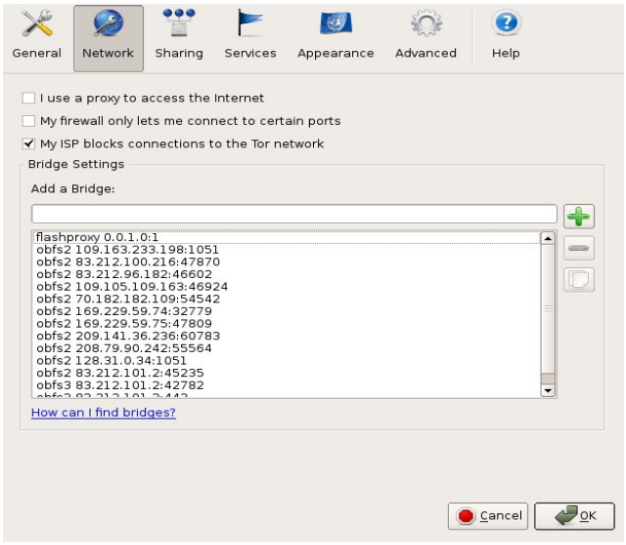
El primer nodo de TOR solo sabe de dónde proviene la información, pero no tiene acceso a la misma ni sabe cuál es el destino final. El segundo nodo tampoco tiene ninguna información de la solicitud y solo el nodo de salida conocerá el destino final al que se intenta acceder y enviará la información desencriptada al servidor destino. En este punto nuestro tráfico se verá igual que si hubiéramos realizado la conexión a través de un túnel VPN, en la que el cifrado desaparece una vez que llega al terminador VPN de la empresa proveedora del servicio. Así que cuando nuestro tráfico llega finalmente al servidor final, este solo ve que proviene de un nodo de TOR, no conoce el verdadero origen de la comunicación.

Algunos gobiernos intentan bloquear el acceso a TOR y para saltarse esa censura hay que utilizar “bridge relays”, que son nodos de acceso a la red no públicos (no están publicados en internet). Para conseguir una lista de relays se pueden solicitar enviando un correo a bridges@TORproject.org incluyendo **get bridges** en el cuerpo del mensaje o ingresando en la URL https://bridges.torproject.org/options para solicitarlos.

Los ISP están usando técnicas DPI (Deep packet inspection) que mediante el sondeo del tráfico inspeccionan los paquetes en busca de patrones reconocibles como tráfico TOR, incluso cuando las conexiones se dirigen a IPs no relacionadas con nodos de entrada TOR (bridges relays). De nuevo se solventó el problema con las herramientas pluggable transport (PT) usadas entre un cliente TOR y un nodo Bridge Relay basándose en nuevos protocolos como obfs4 (el más usado) , FTE o Meek que introducen capas de ofuscación entre el cliente y el nodo de entrada (guard

node) para ocultar la negociación del canal cifrado TLS y otras técnicas para simular un tráfico https “más estándar” y eludir la censura, pero que también nos permiten eludir la vigilancia.



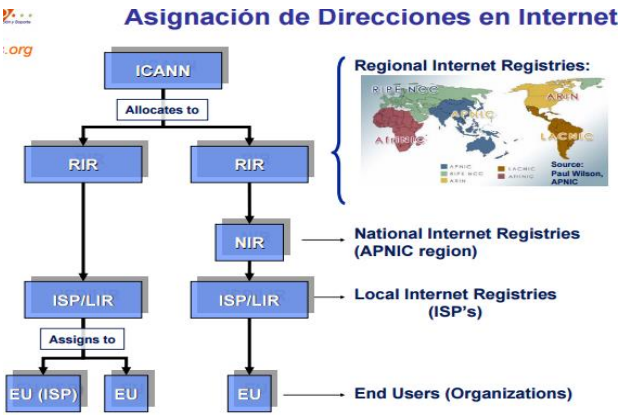


Otros métodos de espionaje de los gobiernos se centran en la interceptación o captura (eavesdropping) de tramas que circulan por las redes privadas (nubes privadas) de proveedores como yahoo o Google en muchos casos sin cifrado en backbone o entre sus CPD. Aunque algunos de estos proveedores ya están trabajando en solucionarlo.

3. Software, recomendaciones y ejemplos

Cuando nos conectamos a un servidor en internet desde nuestro navegador la transmisión de datos (paquetes) a bajo nivel no es directa. Primero enviamos el tráfico a nuestro router de conexión a internet, que lo reenvía al router de nuestro ISP/LIR (Internet Service Provider/Local Internet Registries), el cual la reenvía a uno de los NIRs (National Internet Registries), que por último la renvía a un RIRs (Regional Internet Registries), así hasta que el proceso es revertido para alcanzar el servidor de destino que aloja al página WEB.

En las capa superior de aplicación entre nuestro navegador y el servidor web sí se puede considerar una comunicación directa, a no ser que utilicemos de forma adicional dispositivos intermedios, como un proxy externo, una VPN, o **TOR** que como ya hemos dicho se trata de una red superpuesta en internet formada por nodos proxies que actúan como reenviadores de tráfico .



A nivel de aplicación (nuestro navegador WEB) la diferencia entre usar HTTP o HTTPS es fundamental. En el primer caso queda registrado a que web me he conectado y lo que hemos hecho, pero en el segundo caso no. Ejemplo

Si yo tecleo en mi navegador http://elkino.net en el log típico de un servidor proxy quedará registrado el acceso de esta manera.

Apr 9 18:19:12 10.15.X.X webwasher: 10.38.X.X "mi_usuario" [09/Apr/2019:18:19:08 +0200] 301 "GET http://elkino.net/ HTTP/1.1" "Marketing/Merchandising" "Minimal Risk" "" 785 "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko" "" "0" " NTLM-SANIDAD CATEGORIAS WHITELIST " DISTRIBUCIONES:

Pero si en el navegador pongo https://elkino.net el registro que aparecerá en el log del Proxy será muy distinto y no indicará que hemos solicitado una conexión a la WEB "elkino.net", sino una conexión (connect) en modo túnel (443) hacia un servidor llamado static.wixstatic.com pero no sabe a que WEB alojada en ese servidor hemos accedido ni nuestras acciones posteriores en él.

Apr 9 18:22:44 10.15.X.X webwasher: 10.38.X.X "mi_usuario" [09/Apr/2019:18:22:41 +0200] 200 "CONNECT static.wixstatic.com:443 HTTP/1.1" "Internet Services" "Unverified" "" 5950 "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko" "" "0" " NTLM-SANIDAD "

Esta explicación es fundamental para entender que no servirá de nada usar la red TOR para ocultar el origen de nuestra IP si luego navegamos de forma insegura (HTTP en lugar de HTTPS) y queda registrado en algún nodo intermedio o sonda donde hemos navegado y a que información hemos accedido. Esto vale para otras aplicaciones como el correo, etc.

Al navegar a través de la red TOR la IP pública real con la que nos presentamos en internet es la del último nodo de salida de nuestro circuito virtual. El rol "TOR exit node" es detectable (comprobarlo en https://ipleak.net/) y es el punto más sensible porque el tráfico entre el nodo de salida TOR y el servidor destino al cual accedemos no estará cifrado. Si queremos ser verdaderamente anónimos extremo a extremo, o bien nos cuidamos de introducir ninguna información personal sensible en la capa de datos, o utilizamos siempre conexiones HTTPS cifradas para navegar.

Además aunque no puedan saber quién eres, si saben que ese tráfico proviene de TOR lo que en algunos países da lugar a que las operadoras lo bloqueen o que los sistemas de vigilancia electrónica te coloquen en su punto de mira.

Una solución es usar TOR + VPN para ocultar el uso de TOR y eludir la vigilancia o la censura. Otra solución más sencilla válida si navegamos solo por sitios HTTPS es usar TOR + navegador Opera con VPN activada. Sin instalar

SW de terceros, sin registrarnos, sin contratos, sin pagos. Podemos comprobar que no nos detectan como cliente de TOR en https://check.torproject.org y https://ipleak.net.

Si accedemos a sitios HTTP no funciona porque el proxy de Opera no es anónimo y revela la IP original (forwarded IP) contenida en el campo XFF del encabezado HTTP. Se puede ver la diferencia haciendo búsquedas en Google con HTTP (que nos bloquea las consultas) o con HTTPS (no hay bloqueos).

Para comprobar el nivel de privacidad que nos proporciona un proxy público una vez estamos conectados, podemos acceder a http://xhaus.com/headers, nos mostrará toda la información que revela nuestra conexión y el navegador a través de las cabeceras HTTP.

URL: http://xhaus.com/headers

Request parameter	Value
Requested URI	**/headers**
Request Method	**GET**
Remote IP Address	**162.247.74.217**
Remote IP Port	**35008**
Protocol version	**HTTP/1.1**
HTTP Header*	**Value**
Accept	**text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8**
Accept-Encoding	**gzip, deflate**
Accept-Language	**en-US,en;q=0.5**
Connection	**keep-alive**
Host	**xhaus.com**
Upgrade-Insecure-Requests	**1**
User-Agent	**Mozilla/5.0 (Windows NT 6.1; rv:60.0) Gecko/20100101 Firefox/60.0**

Hay diversos **paquetes** y aplicaciones diseñados para usar TOR. El recomendado para navegación por el proyecto TOR en Windows es “TOR Browser” que es un Firefox modificado que además funciona como proxy Socks para otras aplicaciones escuchando por el puerto tcp 9150.

Algunas opciones están descontinuadas y obsoletas como OperaTOR que integra Opera+TOR portable. Opera ofrece ahora un complemento para instalar como plugin en sus navegadores. TOR+vidalia también está obsoleto.

Si lo que queremos es TORificar todo el tráfico de red a modo de una VPN, hay herramientas como Tallow o Torifier que serían equivalentes a tsocks o torify en Linux.

LinuxTails es una pequeña distribución portable (live) que combina Debian y TOR diseñada para mantener a un usuario completamente anónimo. Ejecutable desde un CD, tarjeta SD, memoria USB. Lo usaba Edward Snowden para evadir la vigilancia de la NSA. Se ha descubierto alguna vulnerabilidad pero relacionada con el soporte I2P(otra red anónima en auge), no con TOR.

Finalmente como comentaremos más adelante lo recomendable será utilizar algún servicio VPN además de TOR pero hay que tener en cuenta que son varios los casos de proveedores VPN que han roto sus normas de privacidad y han sido demandados por ello.

Hay una serie de **recomendaciones** adicionales al uso de TOR para poder navegar con cierto nivel de anonimato, porque es obvio que no podemos usar la web como haríamos habitualmente.

No visitar la misma web **dentro y fuera** de TOR. Forzar la navegación HTTPS con algún complemento como “https everywhere” y utilizar otros motores búsqueda como **Startpage o DucDucgo** que no registra nuestra dirección IP, no usa cookies de seguimiento y no recoge ni comparte ninguna información personal, ubicación,etc.

No publicar datos personales. **NO** usar el buscador Google o el correo Gmail. Incluso a través de TOR aunque Google no sepa tu ubicación ni quien eres, sistemas espía como PRISM (programa de vigilancia electrónica NSA y FBI) que se centra en el contenido (capa de datos) tiene acceso directo en tiempo real a sus servidores y acceso al historial de búsquedas, contenidos de tus mensajes, Cookies, cabeceras de correo, metadatos de archivos adjuntos, etc.

TOR Mail es un servicio Integrado en el proyecto TOR que permite crear cuentas de correo y recibir/enviar correos de forma anónima y privada. Para utilizarlo es necesario acceder a través de TOR (por ejemplo TOR Browser), visitar su web y crear una cuenta. Luego podemos elegir el tipo de cliente a descargarnos para la gestión de nuestros correos o simplemente hacerlo vía WEB.

Existen otros **servidores de correo** (como protonmail) que no solicitan datos personales y permiten su acceso a través de TOR, las principales características son:

- Permiten cuentas anónimas, sin necesitar más datos que el nombre de usuario y la contraseña.
- Permiten acceder a través de TOR.
- Permiten acceso pop3.
- No guardan rastro en las cabeceras del mensaje.
- Permiten eliminar la cuenta de manera sencilla.

También será importante prestar atención al país en el que se encuentran sus servidores y conocer su legislación .

También se puede descubrir nuestra identidad aprovechando **las cookies** que permanezcan en el navegador por descuido o mal uso durante la navegación con TOR. Si no se borran bien y pasas a navegar normalmente (no anónimo) permitiremos que se pueda asociar ambos tipos de tráfico.

Aunque la primera norma es evitar conexiones a sitios HTTP, el acceso a un sitio por HTTPS no garantiza que la clave pública que nos ofrece un sitio es realmente la suya. Puede ocurrir que un tercero intercepte la comunicación como intermediario (**man in the middle**), y nos dé su clave pública haciéndose pasar por el destinatario real (receptor). Para evitarlo necesitamos que una tercera parte, una entidad de confianza nos diga si una clave pública es precisamente de quién dice ser.

Para evitar estos problemas podemos usar alguna extensión SW en nuestro navegador como **Certificate Patrol** que nos avisa si los certificados que usamos para sitios HTTPS han cambiado, para validarlos de nuevo con las autoridades de certificación de confianza CAs.

Otras precauciones:

Desactivar cookies, javascript, flash, pluggins, WEBrtc, y no abrir archivos adjuntos desconocidos. Los applets de Java y JavaScript, las ventanas CGI o las mencionadas cookies están presentes en casi todas las páginas web actuales e intercambian información con nuestro sistema sin que tengamos el control en muchos casos.

No utilizar TOR para conexiones **P2P**

Cuidado con los **metadatos**. Documentos ofimáticos, archivos PDF, correos electrónicos….todos contienen información adicional llamada metadatos que pueden revelar nombres de usuario, cuentas de correo electrónico, fechas y horas, direcciones IP. Por ejemplo, en el caso de un email, el horario, la fecha en que se envió y la IP del usuario. Son objetivo de los programas de vigilancia masiva para buscar patrones de conducta. Al menos deberíamos tener la precaución de **encriptar todo** lo que necesitemos enviar sobre todo si la conexión con el destino final no es HTTPS.

El análisis de los metadatos de un programa electoral del PP publicado en PDF mostraba un título del que se había copiado el documento y los datos de la persona que lo había publicado, un becario de las FAES.

En un documento que utilizó la defensa de la Infanta aparecían en los metadatos una iniciales del autor del documento que curiosamente se correspondían con las del fiscal del caso.

Software TOR y Protocolos:

El Software TOR previamente se conecta a un servidor de directorio que le ofrece una lista de nodos disponibles y así poder construir de forma aleatoria un **circuito virtual**. Cada establecimiento de conexión entre los nodos subsecuentes del circuito es autenticada y cifrada de nuevo con **diferentes claves**.

Cada nodo sólo conoce el anterior y el siguiente nodo en el circuito virtual. Dado que TOR no puede manejar paquetes ICMP (ping), no hay forma de saber a dónde serán dirigidos los paquetes.

Los nodos proxys/reenviadores que ejecutan software TOR utilizan una técnica llamada “Onion Routing” donde cada nodo intermedio cifra y encapsula independientemente el paquete recibido dentro de un nuevo paquete y se lo pasa al siguiente nodo, que repetirá este proceso hasta llegar al nodo de salida de la red TOR.

Tor se puede instalar y configurar de varias maneras. Instalando su navegador Tor browser que incorpora el cliente TOR integrado. Como cliente para torificar todo el tráfico de red de un sistema utilizando tor como proxy transparente. Instalarlo como un servicio e integrar nuestro propio sistema en la red TOR como un nodo más. En el caso de Android es distinto y lo tratamos mas adelante. La fórmula nativa (torrc) es la recomendada por TOR y se puede instalar como servicio en Linux o en Windows, donde lo llaman expert boundle pero simplemente consiste en un ZIP que hay que descomprimir en el raíz del disco C.

En modo servicio podremos usarlo para lo que queramos, unos ejemplos:

Configuracion de TOR como servicio **nodo repetidor**. Configuración del archivo torrc.conf

Debemos editar el fichero de configuración (etc/tor/torrc) y configurar los parámetros ORPort y ExitPolicy:

ORPort 9001
ExitPolicy reject *:*

ORPort sería el puerto de escucha de nuestro nodo y el parámetro **ExitPolicy** al estar configurado para rechazar todo implica que nuestra instancia de TOR se comportará como un enrutador central y no como un nodo de salida

Otro ejemplo de configuración de TOR, pero esta vez configurado como **nodo de salida** aceptando tráfico 80 y 443

DataDirectory /home/user/tor/Data/Tor
DirPort 9030
ORPort 9001
ExitPolicy accept *:80,accept *:443,reject *:*
Nickname Unnamed
RelayBandwidthBurst 10485760

DirPort

Indica el servicio de directorio corriendo en este puerto para ser consultado por terceros. Si está configurado en auto, Tor automáticamente elegirá un puerto por nosotros. Hay que tener en cuenta que esta opción requiere mayor ancho de banda disponible.

ORPort

Indica el puerto que escucha conexiones para clientes y servidores Tor. Esta opción es requerida si queremos correr nuestro propio Tor relay. Si está configurado en auto, Tor automáticamente elegirá un puerto por nosotros.

ExitPolicy

Si estamos corriendo un nodo exit, entonces esta política especifica que deberíamos aceptar o rechazar. Los valores más básicos de configuración son aceptar o rechazar paquetes basados en su número de puerto destino.

Nickname

Define el alias de nuestro relay.

RelayBandwidthBurst

Limita el número de ráfagas de tráfico transmitido a un número determinado de bytes en cada dirección.

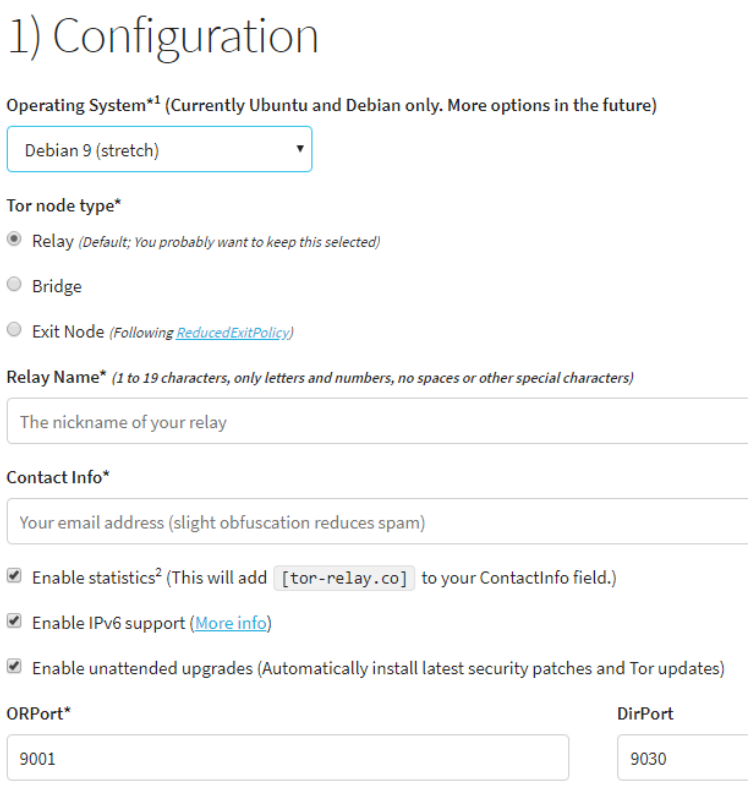
RelayBandwidthRate

Especifica un número de bytes promedio permitido para ser transmitido a través de este nodo.

Después de haber configurado nuestro nodo relay, deberíamos guardar la configuración y reiniciar Tor. Este proceso debería crear claves privadas para Tor, las cuales son almacenadas en keys/secret_id_key en nuestro

DataDirectory. Si mostramos el contenido de DataDirectory, podemos ver que las claves privadas están presentes.

Existe una WEB que nos ayuda a instalar TOR y configurar los parámetros necesarios para su ejecución en cualquiera de sus modos https//tor-relay.co/: pero en cualquier caso el fichero de configuración de ejemplo torrc.conf posee también información bastante descriptiva de cada parámetro ubicado por distintas secciones.



En modo cliente (sin ejecutar TOR como un nodo integrado en la red) se puede configurar como proxy transparente, que se comportara como una VPN, interceptando todo el tráfico de red y reenviándolo cifrado a través de la red TOR.

Habilitar TOR como **proxy transparente** local y DNS local de modo que sea invisible para aplicaciones y usuarios. (solo para sistemas basados en UNIX). Configuración del archivo torrc.conf

```
VirtualAddrNetworkIPv4 10.192.0.0/10
AutomapHostsOnResolve 1
TransPort 9040 IsolateClientAddr IsolateClientProtocol IsolateDestAddr IsolateDestPort
DNSPort 5353
```

Lo cierto es que esta opción está desaconsejada por el proyecto TOR para la mayoría de usuarios, ya que requiere de altos conocimientos técnicos para configurar el sistema y evitar fugas ya que es necesario configurar bien el FW del sistema para redirigir todo el tráfico soportado hacia TOR y descartar el tráfico no enrutable hacia TOR, además es necesario configurar también /etc/resolv.conf para que apunte a 127.0.0.1 (host local)

Si lo utilizamos en modo proxy local pondrá a la escucha 2 puertos un puerto de control y un puerto de escucha de datos accesible para cualquier otra aplicación que soporte configurar una conexión de red a través de un proxy socks4, socks4a y socks5.

HTTPS:

En el primer salto de nuestra conexión hacia el nodo de entrada TOR, aunque una sonda estuviera monitorizando el tráfico de nuestra IP solamente verá una conexión (connect) tipo túnel TCP/IP cifrada (TLS) establecida contra una IP que corresponde con un servidor de la red TOR. No sabe ni a qué servicio final ni IP destino nos dirigimos realmente, y esto impide que nuestro tráfico sea rastreado y monitorizado en Internet. Recordad que con HTTPS se cifran todos los datos de la capa de transporte incluido direcciones URL, parámetros enviados, etc.

TOR no puede cifrar el tráfico extremo a extremo, hasta el destino final. El camino entre el último nodo de salida TOR y el destino final o servidor al que realmente accedemos no estará cifrado por lo que hay que evitar sitios HTTP y acceder a sitios HTTPS (con SSL/TLS) y otra buena razón para hacerlo es evitar la inyección de supercookies por parte de los operadores de comunicaciones que solo puede realizarse en conexiones HTTP.

Proxy SOCKS:

El proxy SOCKS trabaja en un nivel más bajo que el proxy HTTP, SOCKS es básicamente un proxy TCP por lo tanto tiene la posibilidad de redirigir no sólo peticiones HTTP/HTTPS, sino cualquier conexión TCP/STCP. Al no ser específico de un protocolo cualquier aplicación sólo necesita la capacidad de enviar sus paquetes de datos a través de proxy SOCKS para comunicarse con un servidor en el exterior.

La “TORificación” de otras aplicaciones cliente/servidor es una de las ventajas funcionales de usar TOR frente a las VPN SSL, que de momento no trabajan con aplicaciones cliente/servidor no basadas en protocolos WEB.

Anonimizar DNS:

Las consultas DNS también deben ser anónimas y dirigirse a la red TOR y no a los DNS públicos de nuestro operador donde dejarían rastro de quien somos (nuestra IP) y donde queremos ir (IP destino).
Necesitaremos un navegador que permita especificar un proxy HTTP o SOCKS y Orbot se encargará de todo, aunque la mayoría de navegadores ligeros para android no lo permiten. Si fuera el caso, en Orbot tenemos el modo de proxy transparente para todas las aplicaciones. Intercepta las solicitudes DNS de cualquier navegador (HTTP) y las redirige en formato socks TCP (Proxy Socks4a y Socks5) hacia TOR, y seguiremos siendo anónimos a nivel DNS. Comprobarlo en https://dnsleaktest.com/

Otros navegadores como firefox también permiten utilizar protocolo Socks para convertir tanto el tráfico DNS como HTTP y enviárselo al cliente TOR.

ICMP y UDP

Importante. Es imprescindible verificar previamente cómo funcionan las herramientas de anonimización basadas en TOR antes de utilizarlas y también cómo funciona la aplicación que queremos anonimizar a través de TOR.

Por ejemplo Tallow bloquea el tráfico UDP e ICMP que no puede ser manejado por TOR y solo enruta tráfico TCP y DNS pero otras herramientas como torify advierten que al usar torsocks aunque no hay fugas DNS o UDP sí tendremos fugas si usamos Ping o tracert (ICMP). Si usamos proxyChains y TOR para lanzar escaneos con nmap podríamos tener fugas de DNS UDP si no usamos la opción **–PN** o fugas ICMP si no desactivamos los ping **– P0** y forzar los escaneos TCP **– sT**. Por eso para evitar este tipo de fugas otra recomendación más es utilizar TOR junto a una VPN.

Algunas aplicaciones no fueron construidas pensando en el anonimato. Algunos protocolos, como FTP (modo activo/pasivo), envían la propia dirección IP en la sección de datos del FTP, por lo que no se pueden utilizar en TOR. En su lugar sería necesario utilizar SFTP.

Es importante entender que TOR por sí mismo y únicamente no puede evitar ciertas fugas de información debidas a la utilización de protocolos y servicios que no fueron diseñados para el anonimato ni para ser utilizados con TOR.

IPV6

Es recomendable desactivar este protocolo en la tarjeta de red de nuestro equipo, ya que TOR aún no tiene soporte completo para IPv6 por lo que podríamos exponernos a fugas de información de DNS por ejemplo. IPv6 es el sustituto natural del protocolo IP versión 4 y mucho más seguro al integrar de forma nativa el protocolo de seguridad IPSEC, pero a pesar de los mecanismos de transición desarrollados como túneles, traducciones y doble pila, la migración y despliegue está siendo muy lento y la compatibilidad de los sistemas y servicios no está garantizada.

ANDROID

Funcionamiento Orbot:

Al principio el problema de utilizar TOR era que este solo funcionaba como proxy socks. Muchos navegadores y aplicaciones cliente servidor no permitían el envío de tráfico HTTP y DNS vía proxy SOCKS por lo que se hacía necesario usar un herramienta adicional como “privoxy” que modificaba y redirigía los paquetes HTTP al proxy socks de nuestro cliente TOR.

Ejemplo con Privoxy: Escucha tráfico entrante en el puerto 8118 (http) y lo reenvía al puerto 9150 (socks) como tipo socks.

listen-address 127.0.0.1:8118
forward-socks4 / 127.0.0.1:9150 .
forward-socks4a / 127.0.0.1:9150 .
forward-socks5 / 127.0.0.1:9150

Pero actualmente Orbot funciona tanto como proxy HTTP y SOCKS escuchando en 127.0.0.1:8118 y 127.0.0.1:9050, respectivamente, así que no es necesario utilizar aplicaciones alternativas como privoxy.

<string name="not_anonymous_yet">ADVERTENCIA: ¡Su tráfico no es anónimo aún! Por favor, configure sus aplicaciones para usar el Proxy HTTP 127.0.0.1:8118, el SOCKS4A o el Proxy SOCKS5 127.0.0.1:9050</string>

<string name="wizard_details_msg">Orbot es una aplicación de código abierto que contiene TOR, LibEvent y Privoxy. Provee un Proxy HTTP local (8118) y un Proxy SOCKS (9050) en la red TOR. Orbot también tiene la habilidad, en un dispositivo enrutador, de enviar todo el tráfico de Internet a través de TOR.</string>

Navegadores:

Orweb o lighting browser son navegadores para Smartphone que ya vienen preparados para usar TOR. Para comprobar si estamos conectados a TOR nos conectaremos a https://check.TORproject.org, y podemos verificar el nivel de privacidad que tenemos en internet en https://ipleak.net/ y https://dnsleaktest.com/

Orweb es ligero y rápido pero bastante limitado mientras que “Lightning Browser”, además de rápido es más funcional. Ambos permiten cambiar o eliminar la cabecera http/https “user agent”, que revela información de nuestro terminal. Además es importante comprobar que nuestro navegador no soporte protocolo WebRTC para evitar sus vulnerabilidades, como la obtención de nuestra verdadera dirección IP. Un problema reportado incluso cuando se usan túneles vpn .

Y para el correo electrónico lo mismo, deberíamos usar un cliente específico optimizado para TOR y que utilice servidores de correo anónimos de TOR.

Tampoco conviene usar Google como buscador porque además de intentar bloquear nuestras consultas cuando accedemos desde una IP de TOR (HTTP), Google registra nuestra IP y recopila información de nuestras consultas y nuestro navegador, como mínimo con fines comerciales. Como alternativas tenemos Startpage y DuckDuckGo y otros.

Si nos preocupa un poco la privacidad pero no queremos complicarnos podemos usar el navegador Opera y activar su VPN Nuestro tráfico y estaremos usando los DNS de Opera y no los de nuestro proveedor.

El siguiente nivel puede ser activar Orbot con la opción (2) “apps” para todas las aplicaciones del terminal. Ocultaremos nuestra IP pública real para cualquier conexión IP hacia el exterior que realice cualquier app del terminal y haremos un uso más sigiloso de la red TOR ya que nos presentaremos en Internet navegando a través de un servidor de Opera y no un nodo de TOR. Los DNS que recibirán nuestra consultas serán los de la red opera pero si usamos lighting browser u Orweb, los DNS anónimos asignados aleatoriamente por TOR.

Otra opción mejor podría ser arrancar Orbot y un navegador que permita configuración manual de proxy o utilizar directamente el “lighting browser” que ya viene preparado trabajar con Orbot . Esto nos permite usar en nuestro Android otras opciones adicionales como pueden ser la funcionalidad de un FW o una conexión VPN para aumentar nuestra seguridad, aunque también aumentará la latencia de las conexiones.

Ejemplos Android y Windows

Tengo 2 opciones desde Android:

(1) iniciar orbot con modo normal (sin VPN activado). Orbort creará un circuito en la red TOR y a partir de aquí podríamos usar navegadores orbweb o Lightning Browser que ya vienen diseñados para detectar orbot y utilizarlo para conectarse a internet, pero también podríamos usar cualquier navegador o app con capacidad de dirigir su tráfico a través de un proxy, ya que orbot funciona como proxy local http/https:

Proxy http y https: localhost o 127.0.0.1 puerto 8118
y…
Proxy socks: localhost o 127.0.0.1 y puerto 9050

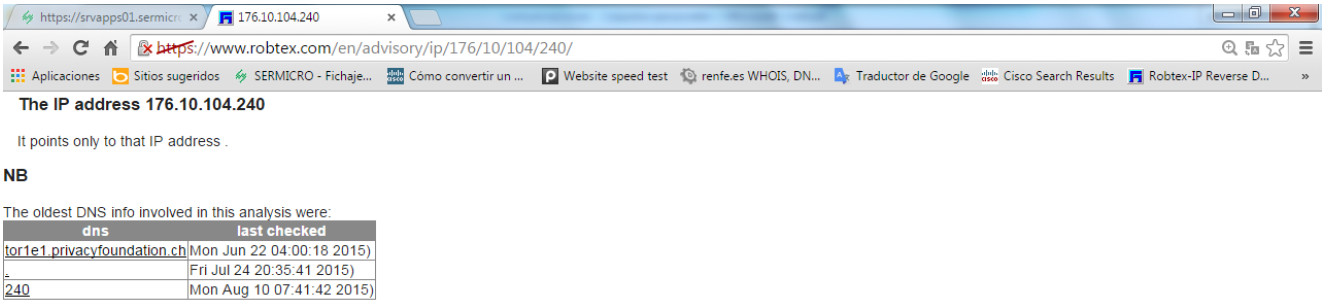
Como siempre podemos comprobar que la IP con la que nos presentamos en Internet es distinta si nos conectamos a Ipleak.org, ipecho.net/plain o canihazip.com/s. El resto de aplicaciones seguirán usando la ip pública asignada por nuestro proveedor ISP (nuestra verdadera IP pública).

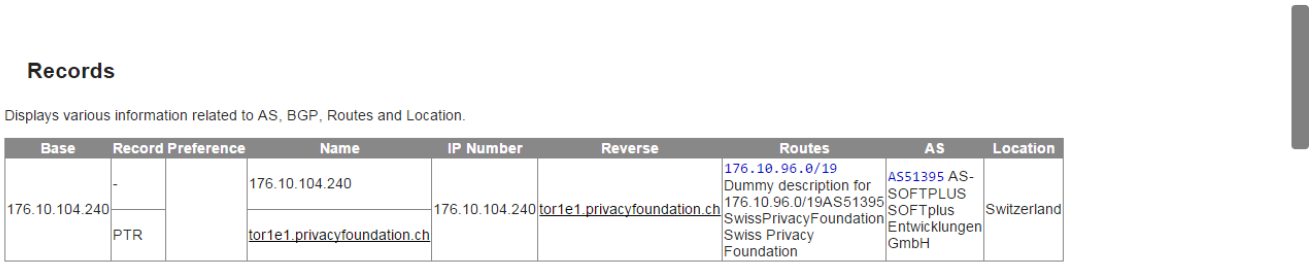
(2) Iniciar Orbot con el botón VPN activado. Esta opción arranca Orbot en modo VPN para todas las aplicaciones que hayamos seleccionado en la configuración de Orbot --- apps capturando el tráfico IP de todas las aplicaciones o las que hayamos indicado en su configuración redirigiéndolo el tráfico hacia la red TOR.

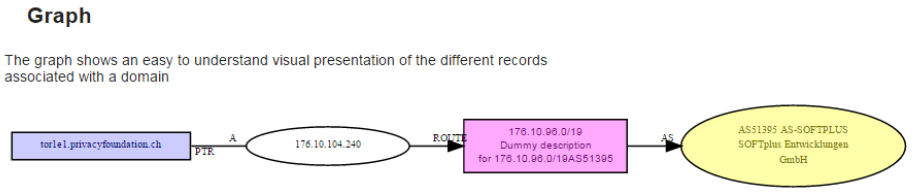
**Para garantizar la privacidad también en el envío de correo deberíamos de tomar la misma precaución y usar otro cliente de correo optimizado para TOR o usar alguna App como Protonmail con una cuenta anónima creada previamente, etc.

Siguiendo el ejemplo opción (1), si nos vamos a una web para chequear nuestra conexión IP como ”cualesmiip.com” o directamente abrimos el navegador Orweb que chequea nuestra conexión contra los servidores TOR, vemos que la IP real con la cual me presento en internet es 176.10.104.240

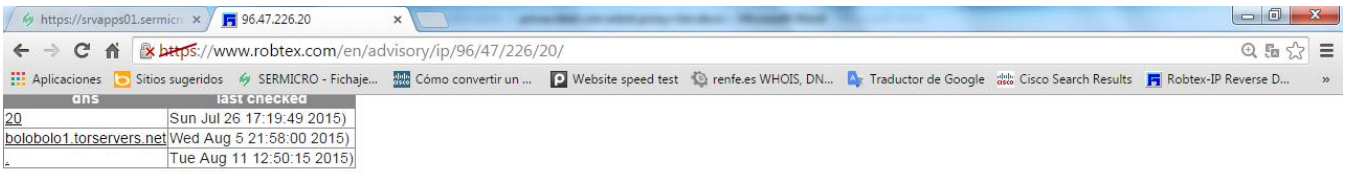
Si nos vamos al portal web robtex para el rastreo de IPs y dominios e introducimos esa dirección nos dirá que esta IP pública pertenece a un nodo de TOR de una fundación privada en Suiza







Además esa IP cambia dinámicamente, cada 10 minutos se reinicia el circuito virtual en la red TOR (también lo podemos forzar nosotros en cualquier momento) y nuestra IP pública y origen geográfico cambiará. Si abro otra ventana de navegación o refresco al cabo de un rato la sesión actual del navegador seguiremos conectador a través de la red TOR, pero se habrá creado un nuevo circuito virtual y nuestra dirección IP cambiará, ahora es 96.47.226.20



ans	last checked
20	Sun Jul 26 17:19:49 2015)
bolobolo1.torservers.net	Wed Aug 5 21:58:00 2015)
.	Tue Aug 11 12:50:15 2015)

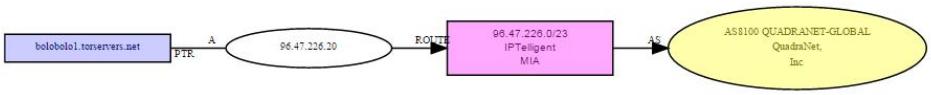
Records

Displays various information related to AS, BGP, Routes and Location.

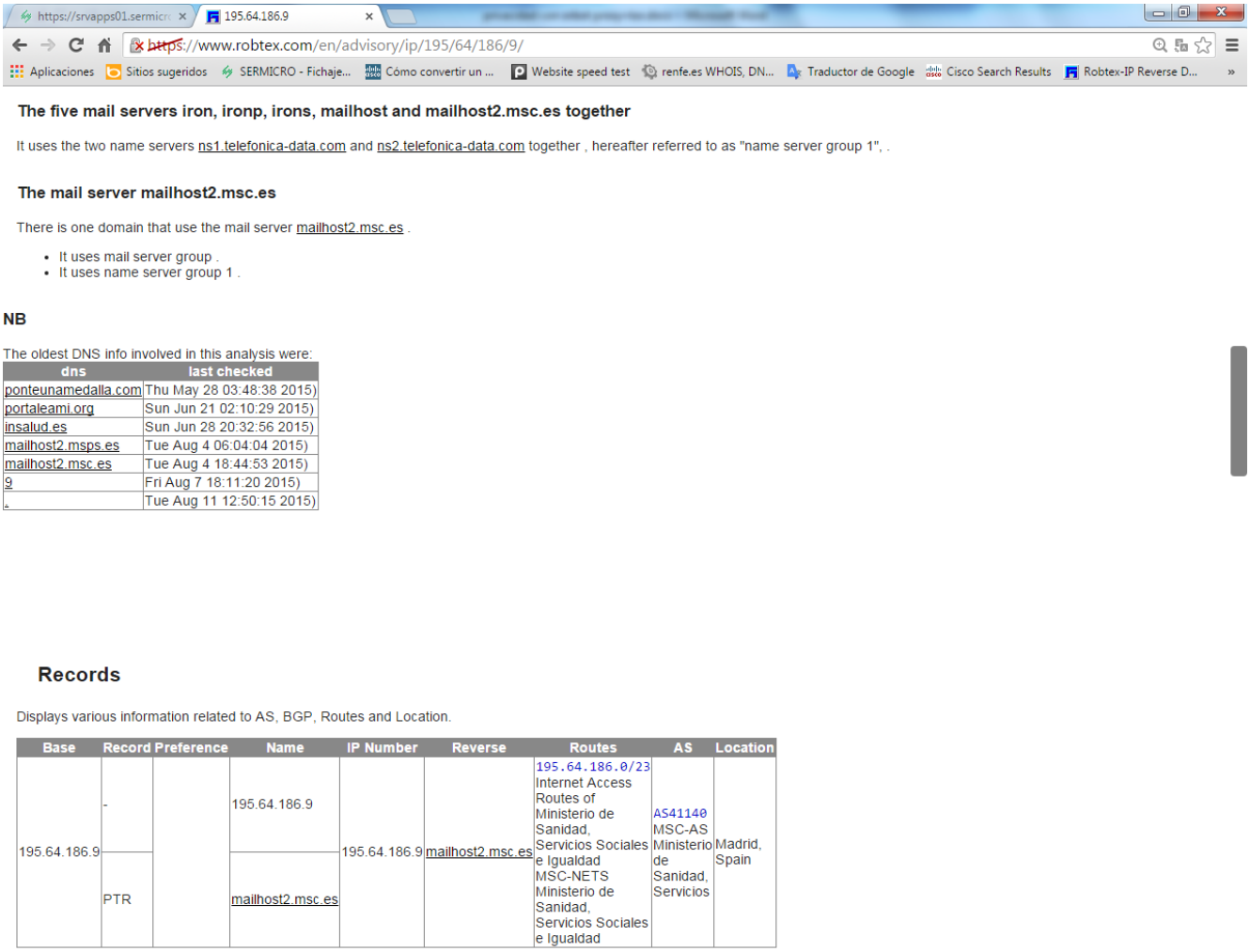
Base	Record	Preference	Name	IP Number	Reverse	Routes	AS	Location
96.47.226.20	-		96.47.226.20	96.47.226.20	bolobolo1.torservers.net	96.47.226.0/23 96.47.224.0/22 IPTelligent MIA TOR-MIA01	AS8100 QUADRANET-GLOBAL QuadraNet, Inc	Anonymous Proxy
	PTR		bolobolo1.torservers.net					

Graph

The graph shows an easy to understand visual presentation of the different records associated with a domain



Si cierro Orbot y abro una nueva sesión con el navegador orweb que chequea si estas o no conectado a TOR…me dira, sorry you are not using TOR (your ip add…. Is…. 195.64.X.X (Tfnca. DATA).



https://srvapps01.sermicr | 195.64.186.9

https://www.robtex.com/en/advisory/ip/195/64/186/9/

Aplicaciones | Sitios sugeridos | SERMICRO - Fichaje... | Cómo convertir un ... | Website speed test | renfe.es WHOIS, DN... | Traductor de Google | Cisco Search Results | Robtex-IP Reverse D...

The five mail servers iron, ironp, irons, mailhost and mailhost2.msc.es together

It uses the two name servers ns1.telefonica-data.com and ns2.telefonica-data.com together , hereafter referred to as "name server group 1", .

The mail server mailhost2.msc.es

There is one domain that use the mail server mailhost2.msc.es .

- It uses mail server group .
- It uses name server group 1 .

NB

The oldest DNS info involved in this analysis were:

dns	last checked
ponteunamedalla.com	Thu May 28 03:48:38 2015)
portaleami.org	Sun Jun 21 02:10:29 2015)
insalud.es	Sun Jun 28 20:32:56 2015)
mailhost2.msps.es	Tue Aug 4 06:04:04 2015)
mailhost2.msc.es	Tue Aug 4 18:44:53 2015)
9	Fri Aug 7 18:11:20 2015)
.	Tue Aug 11 12:50:15 2015)

Records

Displays various information related to AS, BGP, Routes and Location.

Base	Record	Preference	Name	IP Number	Reverse	Routes	AS	Location
195.64.186.9	-		195.64.186.9	195.64.186.9	mailhost2.msc.es	195.64.186.0/23 Internet Access Routes of Ministerio de Sanidad, Servicios Sociales e Igualdad MSC-NETS Ministerio de Sanidad, Servicios Sociales e Igualdad	AS41140 MSC-AS Ministerio de Sanidad, Servicios	Madrid, Spain
	PTR		mailhost2.msc.es					

Ahora vemos que pasa con otros navegadores no diseñados para TOR específicamente, pero que ofrecen características interesantes.

Instalación del navegador “**Opera Beta**” con capacidad VPN.

Opera Beta ofrece la posibilidad de navegar directamente, o navegar a través de sus propios servidores proxy (ahorro de datos), o navegar a través de sus servidores OpenVpn(TLS) simplemente activando la casilla correspondiente a VPN.

La primera opción (proxy) no es recomendable si nos preocupa nuestro anonimato y no hemos arrancado previamente alguna VPN u Orbot , ya que de lo contrario además de mostrar que nos presentamos en Internet con una IP de la red Opera también revelará nuestra “IP pública real” (forwarded IP) asignada por mi operador. Dicho de otra forma esta fórmula de navegación aplica el concepto proxy **NO** anónimo. Podemos comprobarlo en ipleak.net.

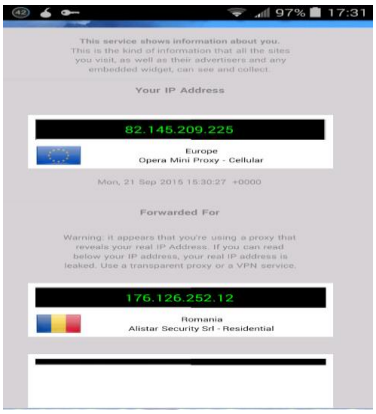
La segunda opción (modo VPN) enmascara nuestra IP real, presentándonos en Internet con una IP de Opera u otro proveedor VPN y sin que revele nuestra IP publica real. Además nuestro tráfico irá cifrado desde nuestro navegador hasta la red del proveedor VPN, lo que no está mal.

Pero utilizar solamente una VPN implica que el proveedor tendrá registros de quien somos o como mínimo nuestra IP real y a donde nos hemos conectado. Este argumento debe tenerse en cuenta para cualquier servicio VPN , ya que ninguno puede garantizar al 100% nuestro anonimato desde el momento que se registran trazas de conexión y como mínimo nuestra IP publica de origen.

Para ello podríamos Iniciar primero Orbot para que funcione en modo VPN y tunelice o encapsule el tráfico de navegación que generamos con Opera Beta (Debemos indicar a Orbot en ---- > configuración ----- >apps que queremos utilizarlo para Opera). Ahora activamos la casilla de VPN del navegador Opera y nos conectarnos a ipleak.net. Comprobamos que seguimos presentándonos en Internet igualmente con una IP de la red de Opera, pero en este caso si alguien tuviera acceso a los logs en los servidores de Opera le resultaría imposible asociar un determinado tráfico con nosotros ya que solo verían que proviene de la red TOR. De esta manera estamos añadiendo más capas de cifrado y autenticación a nuestro tráfico y ocultamos nuestra IP pública de origen real.

MiPC ------->TOR ------->VPN------- >Internet

Además es una opción interesante para evitar que los buscadores o sistemas finales detecten que estamos usando la red TOR cuando accedemos a alguna aplicación o sitio WEB. Si nos dirigimos a https://check.torproject.org nos dirá “sorry you are not using TOR “.



Solo es posible reproducir esta topología en un equipo Windows para navegación WEB. Ejecutando Tor browser y luego el navegador Opera Beta con la pestaña VPN habilitada. Previamente habremos configurado OPERA para usar proxy Socks 4a/5 en la dirección localhost:9150

También podríamos usar inicialmente Torify o Tallow y luego navegar con Opera, que en este caso no requeriría cambiar la configuración de proxy. Lo que no va a funcionar en ningún caso será iniciar una VPN con un cliente tipo OpenVPN (en modo SSL o IPsec) después de haber ejecutado Torify o Tallow.

Este modelo también es interesante en caso de requerir solo navegación anónima, porque nuestro proveedor de servicios Internet (ISP) aunque puede saber cuándo nos hemos conectado a la red TOR y quiénes somos, no sabrá que sitios hemos visitado ni que información hemos transmitido. Los servidores de opera no sabrán quienes somos y los aplicativos finales tampoco, además estos últimos tampoco detectarán que el trafico proviene de TOR.

En cualquier caso, bien por evitar la censura para acceder a la red TOR en algunos países o bien para evitar que el proveedor de acceso registre cuando estamos accediendo a Internet a través de TOR, nos puede interesar utilizar una conexión VPN previa que encapsule nuestra conexiones hacia TOR. La topología será distinta.

MiPC ------->VPN -------> TOR ------- >Internet

Por ejemplo, podemos instalar el cliente VPN de Proton (ProtonVPN) aprovechando que ya deberíamos tener una cuenta de correo anónima en ProtonMail. Si estamos en android su cliente gratuito solo tiene posibilidad de elegir 3 ubicaciones geográficas pero será suficiente y si elegimos el nodo que existe en España la velocidad de conexión será buena y con mínima latencia.

Si ahora nos conectamos con el navegador Opera (sin marcar la opción VPN de opera) a ipleak.net , nos mostrará que navegamos con una IP pública tipo unn-195-181-167-147.datapacket.com así que ya estaríamos conectados vía VPN a un servidor de protonVPN.

El problema que se nos presenta ahora en Android es que no podemos usar Orbot en modo VPN porque ya tenemos levantado un túnel VPN contra un servidor de protonVPN. Lo que sí podemos hacer es arrancar Orbot sin VPN (en modo proxy) para que establezca una conexión (circuito) TOR a través de nuestra VPN. Y …¿Cómo podemos usar ese circuito TOR?. Utilizaremos cualquier otro navegador o app que permita configurar manualmente un proxy. Por ejemplo lighting browser, indicándole que tenemos un proxy http en el puerto 8118. Bueno en el caso de lighting browser podemos especificarle directamente que tenemos Orbot instalado ya que viene preparado para trabajar directamente con el cliente Orbot para TOR como proxy.

Si volvemos a comprobar nuestra conexión a internet a través de ipleak.net veremos que ya nos presentamos con otra IP pública que será la de un nodo de salida de TOR y nuestro proveedor de acceso a Internet no puede saber que estamos conectados en TOR ya que solo verá una conexión desde nuestra IP hacia un servicio VPN.

Por ultimo insistir por seguridad que para este modelo de configuración de acceso a TOR a través de VPN la opción recomendada será siempre evitar el uso de Orbot + un navegador de terceros y utilizar Tor Browser para Android, que es el navegador nativo desarrollado específicamente por TOR.

Evidentemente no hay un modelo de configuración de acceso a TOR definitivamente mejor que otro, cada uno tiene sus ventajas e inconvenientes. Hay quien prefiere este último modelo alegando que el ISP no puede sondear nuestro tráfico y detectar que nos estamos conectando a TOR, pero en realidad con la utilización de nodos bridge relay junto la implementación de los protocolos de ofuscación (pluggable transport) se cumple precisamente ese cometido, evitar ser detectados y por consiguiente bloqueados o sondeados.

Aun así, para los más paranoicos todavía podríamos complicar más la topología con una configuración tipo:

MiPC----- >VPN----- >TOR----->VPN-------->Internet

Tanto en Windows como en Linux es sencillo, solo necesitamos una conexión VPN inicial, por ejemplo openVPN contra un servidor de protonVPN. Una vez establecida la VPN arrancar un navegador Tor Browser. En Linux instalar tor con sudo apt-get install tor y levantar el Servicio con **service tor start**, podemos ver que levanta un proxy local escuchando por el puerto 9050 o 9150 dependiendo del sistema anfitrión. Hay otras formas de usar TOR en Linux, como hacer que una aplicación se conecte a internet a través de TOR la app **torsocks** o también utilizar **proxychains**.

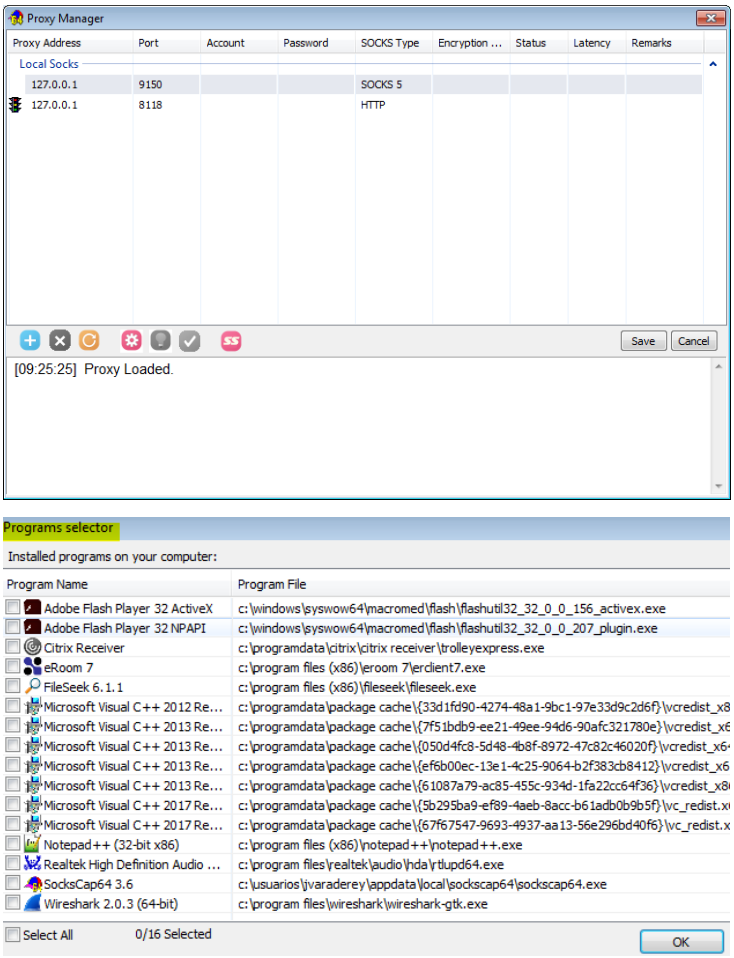
Si hemos escogido la primera opción ejecutaremos el navegador Opera Beta, al que habremos modificado la configuración de Proxy indicando que tenemos un proxy Socks local disponible en el puerto 9150(tor browser). Ahora solo resta activar el modo VPN del navegador Opera y el circuito estará establecido.

En Android no podremos configurar esta topología porque el navegador Opera Beta aunque dispone también de su propia conexión VPN hacia los servidores de Opera no permite configurar manualmente un proxy.

Para trabajar en Windows con otro tipo de aplicaciones en red a través de TOR existen varias opciones. La primera sería usar TOR browser porque ofrece la funcionalidad añadida de Proxy local TOR para tráfico HTTP y socks4/5 así que puede ser utilizado por otras aplicaciones. Esto nos valdría para configurar manualmente cualquier otro navegador apuntando como proxy socks nuestra dirección local 127.0.0.1:9150, pero no para otras aplicaciones que solamente permiten configurar un proxy HTTP o no disponen de la capacidad de “proxyficacion”.

La alternativa en este caso sería utilizar además de TOR browser la herramienta privoxy, que es un proxy renviador multiprotocolo. Escucha peticiones HTTP por el puerto que definamos (por defecto 8118) y lo traduce a tráfico TCP socks, renviándolo donde queramos, por ejemplo al puerto local 9150 donde escucha TOR Browser. Pero una vez más la aplicación que queramos “torificar” debe permitir la opción de configuración proxy manualmente.

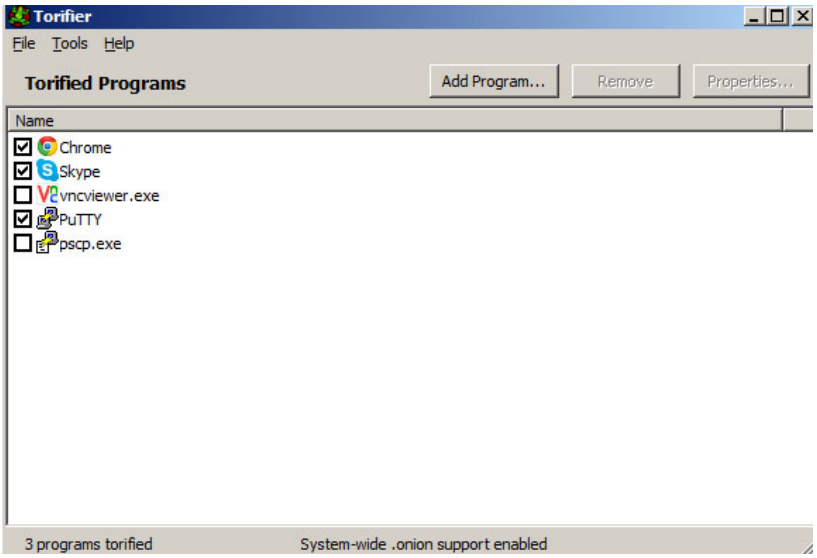
La tercera alernativa para aplicativos que no disponen de configuración manual de proxy, podría ser utilizar una herramienta que capture todas las solicitudes de red de otras aplicaciones y las renvíe donde queramos. Existen varias herramientas de este tipo pero algunas son de pago, así que pondré como ejemplo una libre **sockscap** donde definimos el tipo de proxy y su dirección/puerto, y por otro lado definimos que aplicaciones vamos a interceptar y para reenviar el trafico de red a través de alguno de los proxies definidos.



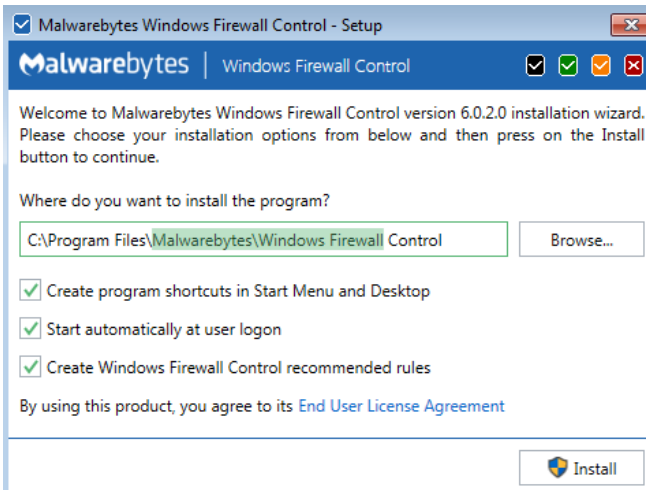
La última opción es utilizar herramientas específicamente diseñadas para Torificar otras aplicaciones y tras crear un circuito virtual (túnel TOR) pueden capturar y redirigir el flujo de tráfico de red de cualquier aplicación o de todo el sistema directamente hacia TOR. Es el caso de **tallow y torifier,** que es más completa y configurable porque

además de un modo VPN tiene la posibilidad de escoger qué aplicaciones se conectarán a internet a través de TOR y cuáles no.

Tendríamos la misma funcionalidad que hablamos con **Tor Browser+sockscap** en una sola herramienta.



En cualquier caso no es **aconsejable** usar estas herramientas para “torificar” todas las conexiones de un sistema Windows como si estuviésemos usando una conexión VPN, ya que no tendremos un control absoluto de las conexiones de red TCP que periódicamente se establecen desde diversos procesos de Windows a través de servicios como svchosts y que son difíciles de identificar y filtrar, salvo con alguna aplicación Firewall integrada con el Firewall de Windows que presta información detallada de estos procesos como Malware Bytes Windows firewall o Windows firewall control de sphinx-sof.



Aun así resulta complejo analizar y discriminar en un sistema Windows cuales de estos procesos ocultos debemos permitir conectarse públicamente y cuáles no, y existe el riesgo de fugas de información que puedan revelar nuestra identidad. Esto con Entonos Linux no debería ocurrir y es la principal razón por la que los expertos no recomiendan el uso de TOR en sistemas Windows.

LINUX

En el caso de Linux ya hemos comentado antes que hay distribuciones ISO para arranque en CD o USB que no dejan registros con TOR preinstalado que son la opción más segura. Si queremos usarlo en otra máquina Linux virtual o física tendremos las mismas opciones y herramientas que ya hemos comentado en el apartado Windows. En este caso se utilizan herramientas como **Polipo, Proxychains y torify**

VPN+TOR

La opción más interesante es la que incorporan los nuevos navegadores Opera (también en Android) es la de activar el envío de tráfico a través de una conexión VPN contra los servidores de Opera.

Si usamos esta opción y previamente hemos lanzado la conexión a TOR inicializado orbot en modo VPN, una vez establecido el circuito TOR, al navegar desde opera el tráfico que generamos se cursará tunelizado por la VPN SSL de Opera, pero primero se encaminará por la red TOR. Con esto tendremos un encapsulado adicional de 3 capas de cifrado asimétrico.

Cuando nuestro tráfico salga de la red TOR por el nodo de salida que le corresponda, como es trafico VPN, este se encaminará hacia los routers/terminadores VPN de la red Opera encapsulados/cifrados, lo que nos aporta seguridad en el punto más vulnerable de TOR (El nodo de salida de la red) que podría estar comprometido.

Cuando los paquetes llegan al terminador VPN se descifran y en ese punto si hay trazabilidad de la dirección de nuestro destino final (servidor/servicio) pero no del origen de la petición ya que para los servidores de Opera todo el tráfico proviene de una IP de la red TOR.

Por tanto, utilizar VPN+TOR en este orden nos aporta un altísimo nivel de seguridad y privacidad.

El proveedor de servicios Internet solo verá una conexión desde nuestra IP a un servidor de la red TOR (sabe que nos hemos conectado a TOR) y el proveedor de VPN (Opera) no verá el origen real de la conexión VPN.

5. Enlaces de interés y ampliación de información.

https://elbauldelprogramador.com/logrando-el-anonimato-con-tor-parte-1 y 2

http://actualidad.rt.com/actualidad/view/132610-representante-TOR-internet-seguridad

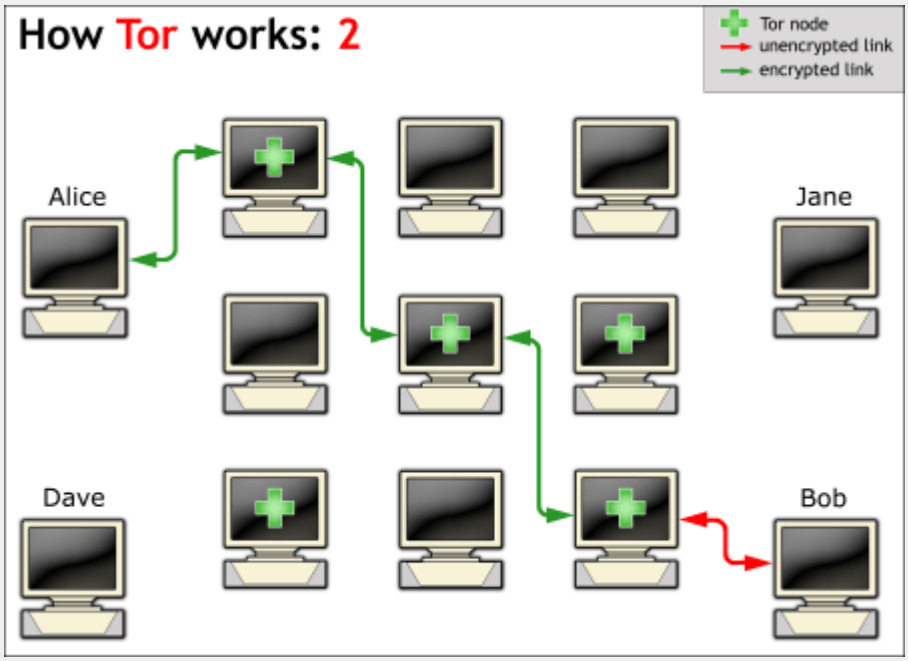
https://geekytheory.com/que-es-y-como-funciona-la-red-TOR/

http://www.expresionbinaria.com/navegar-de-forma-anonima-en-internet/

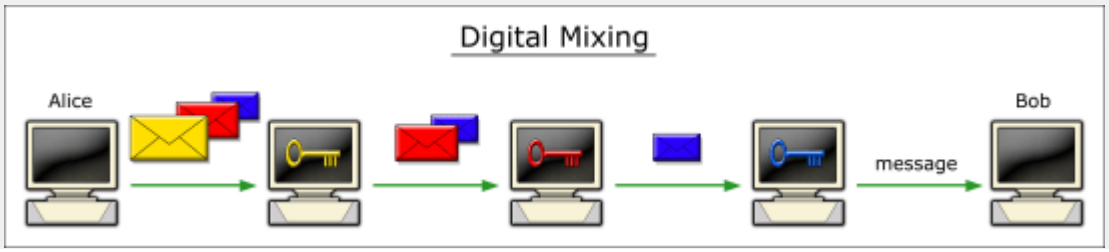
https://doble69.wordpress.com/2014/01/17/TOR-vidalia-anonimato-en-internet/

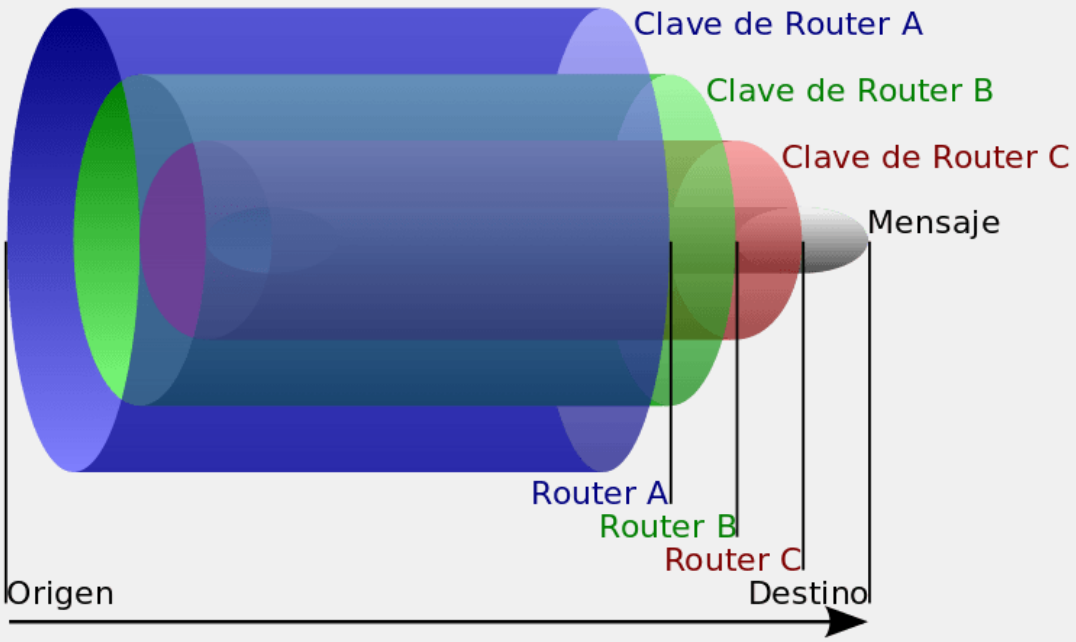
Más información:

Después de recibir la lista de direcciones de nodos desde un servidor TOR, **nuestro cliente TOR** (estará en nuestro equipo) **se conectará a un nodo aleatorio a través de una conexión encriptada**. Este nodo escogerá otro nodo aleatorio con otra conexión cifrada y, así hasta llegar al nodo de antes de Bob. El nodo de salida (penúltimo de la comunicación) hará una conexión no encriptada con Bob. **Todos los nodos TOR son elegidos al azar y ningún nodo puede ser utilizado dos veces**. En caso de que la red esté congestionada, habrá nodos que no se utilicen. Esto lo vemos en la siguiente imagen:

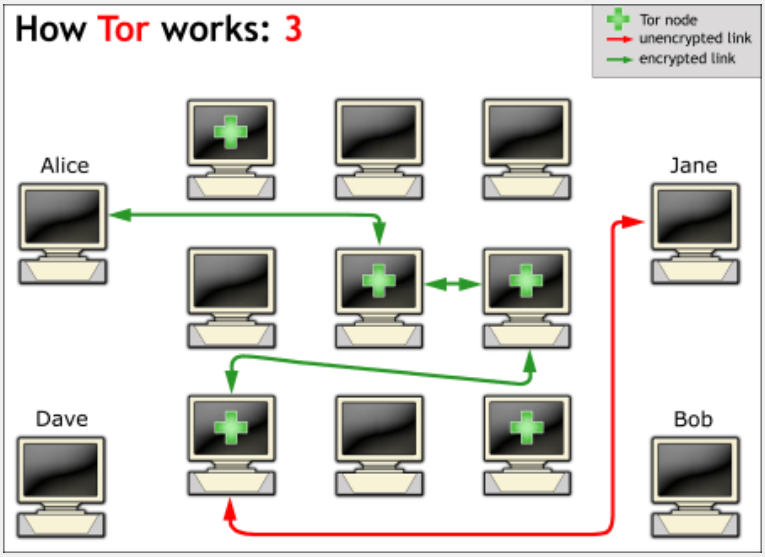


Ahora, ya podemos ver la estructura de los datos en el enrutamiento cebolla. Utilizando un **cifrado asimétrico**, Alice cifra el **mensaje por capas** (como una cebolla). Lo primero que hará es cifrar el mensaje con la clave pública del último nodo de la lista, para que sólo él lo pueda descifrar. Además, cifra e incluye las instrucciones para llegar al destino, que es Bob. Todo este paquete se cifra de nuevo añadiéndole las instrucciones para llegar al último nodo de la lista con el fin de que sólo este pueda descifrar el paquete y que acabe llegando al nodo Bob.



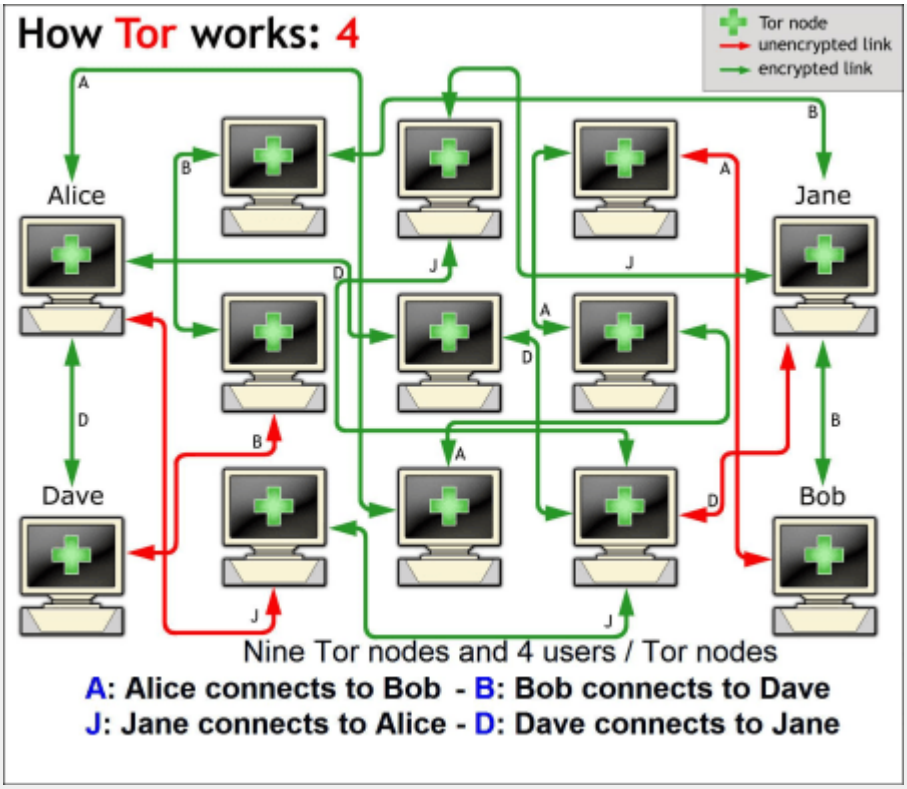


Para evitar el análisis de nuestras comunicaciones por parte de terceros, **cada 10 minutos se cambian los nodos de la conexión TOR**, escogiendo nuevos nodos. Esto podemos verlo en la siguiente figura:



Los nodos de la red TOR son públicos. Si nosotros mismos somos un nodo, incrementaremos nuestra **privacidad**. Aunque esto suene contradicTORio, explicaré por qué ocurre esto: si Alice usa la red TOR para conectarse a Bob, necesitará conectarse a otro nodo TOR. Sin embargo, si funciona como un nodo para Jane o Dave, también estará conectada a otro nodo. Por lo tanto, un tercero no podrá saber si la comunicación por parte de Alice ha sido iniciada como usuario o como nodo.

Esto hace que **la extracción de información sea más compleja por parte de un tercero**. Si Alice funcionase como nodo para decenas, centenas de usuarios, sería **realmente complicado espiar sus datos**.



Como conclusión, podemos decir que el **onion routing nos proporciona más privacidad** que el enrutado normal y corriente. Exceptuando el primer y último nodo, **nadie sabe de dónde viene o a dónde va la información que enviamos**. El mensaje va encapsulado en muchas capas encriptadas