

¿Qué es TOR?

Univ. Franklin David Flores Mamani
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de
Información
Frank7david@gmail.com

RESUMEN

En el presente artículo se dará a conocer acerca del programa TOR y su aplicación, en la navegación de sitios web no indexados.

Palabras Clave

Keywords are your own designated keywords.

1. INTRODUCCION

La navegación anónima y para que podemos utilizarlo. Navegar de forma anónima por la red nos permite evitar que sepan quienes somos, la cuestión es que como explicaremos más adelante existen distintos tipos de navegación más o menos anónima por ejemplo navegar a través de un único proxy nos ofrece una navegación poco anónima pues aunque navegamos con una IP que no es la nuestra, en caso de hacer algo “suficientemente malo”, sería “tan fácil” como que la policía fuera a esa IP (En caso de estar en el mismo país ya que si no sería bastante más complicado) y pidiera quien era el que estaba navegando por ella a una hora determinada, en cambio el otro extremo sería que en nuestra navegación capa petición que hagamos sea desde una IP distinta y además utilizando la red TOR, lo cual nos permite

3. ¿QUÉ ES TOR Y SU FUNCIÓN?

¿Has oído hablar de Tor? Pues vamos a hacer un análisis del resultado surgido después de que organismos como la NSA estadounidense haya reconocido que ha tenido acceso a cierta información sobre la navegación de los usuarios.

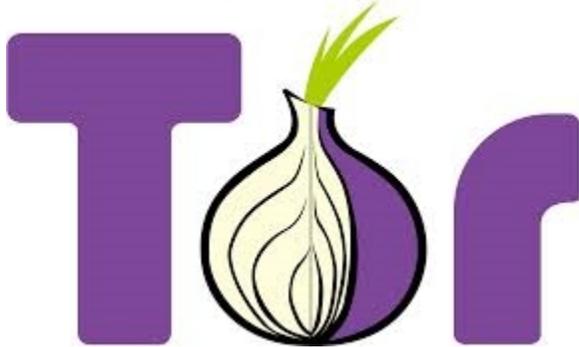


Figura 3.0 The Onion Router

Tor es la abreviatura de The Onion Router (Figura 3 de ahí el logo) y fue inicialmente una red mundial de servidores desarrollados con la Marina de EE.UU. que permitió a la gente a navegar por Internet de forma anónima. Ahora, es una organización sin ánimo de lucro cuyo objetivo principal es la investigación y desarrollo de herramientas de privacidad en línea.

a navegación completamente anónima y contra lo que ni siquiera la policía puede hacer nada.

2. SITIOS WEB

Un **sitio web** es una colección de páginas de internet relacionadas y comunes a un dominio de Internet o subdominio en la World Wide Web en Internet. Una página web es un documento HTML/XHTML que es accesible generalmente mediante el protocolo HTTP de Internet.

Todos los sitios web públicamente accesibles constituyen una gigantesca *World Wide Web* de información (un gigantesco entramado de recursos de alcance mundial).

A las páginas de un sitio web se accede frecuentemente a través de un URL raíz común llamado portada, que normalmente reside en el mismo servidor físico. Los URL organizan las páginas en una jerarquía, aunque los hiperenlaces entre ellas controlan más particularmente cómo el lector percibe la estructura general y cómo el tráfico web fluye entre las diferentes partes de los sitios.

Algunos sitios web requieren una suscripción para acceder a algunos o todos sus contenidos. Ejemplos de sitios con suscripción incluyen algunos sitios de noticias, sitios de juegos, foros, servicios de correo electrónico basados en web, sitios que proporcionan datos de bolsa de valores e información económica

Tor puede ingresar a sitios web el cual no puede ingresar los navegadores comunes, ya que las páginas "onion" no están indexadas. La red Tor disfraza tu identidad moviendo el tráfico a través de diferentes servidores Tor, y cifra además ese tráfico por lo que no se identifica al usuario. Cualquiera que trate de investigar tu navegación vería que el tráfico procede de los nodos al azar en la red Tor, en lugar de su servidor. **Figura 3.1 Nodos de TOR**

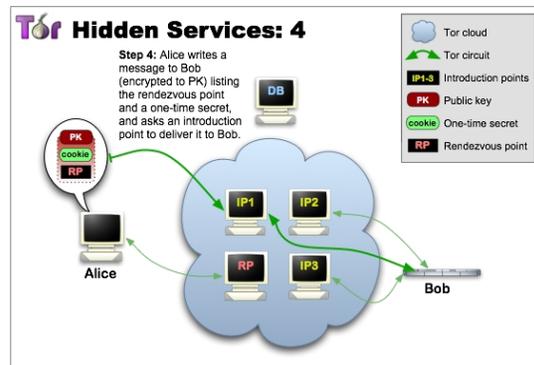


Figura 3.1 Nodos de TOR

3.1 Las Dos Caras de TOR

Para acceder a esta red, sólo tienes que descargar **Tor**. Todo lo que haces en el navegador pasa a través de la red Tor y no necesita ninguna instalación o configuración por tu parte. Hay algo que tienes que tener en cuenta, y es que una navegación tan segura tiene un precio: la pérdida de velocidad de carga. Cuando utilizas el navegador Tor, los datos pasan por un montón de nodos por lo que tendrás una experiencia de navegación mucho más lenta que normalmente. **Figura 3.1.0 Trafico de Datos**

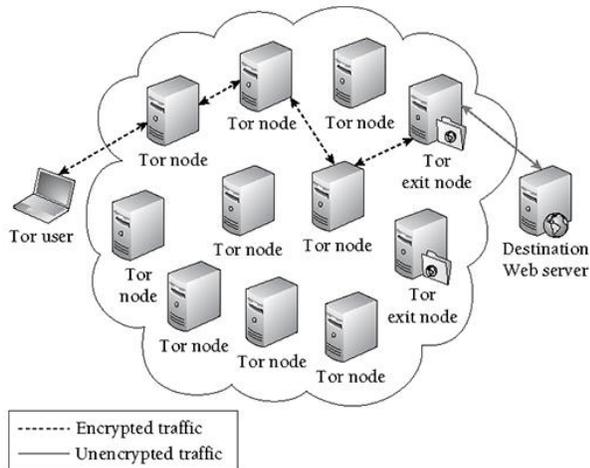


Figura 3.1.0 Trafico de Datos

La tecnología de Tor no es sólo la navegación anónima. También se pueden alojar sitios web a través de sus **servicios ocultos** que sólo son accesibles por otros usuarios del navegador Tor. Es en uno de estos sitios de servicio ocultos en el que se aloja algo que se conoce como **la Ruta de la Seda**, una red para traficar con drogas. Según algunos informes policiales, por lo visto también se utilizan para alojar pornografía infantil o información relativa al tráfico de armas.

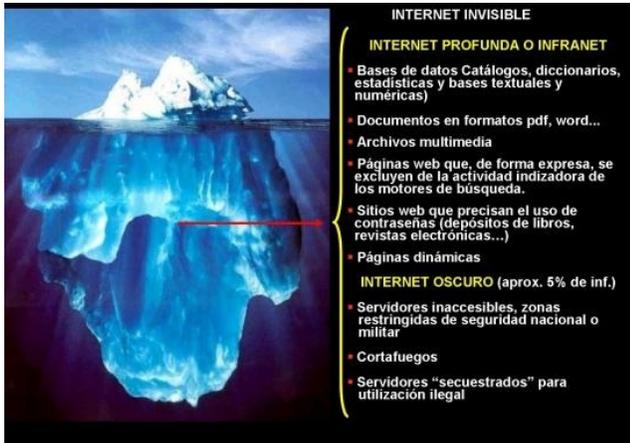


Figura 3.1.1 Internet Inesible

No pienses que sólo porque estás usando Tor eres perfectamente anónimo. Alguien como la NSA puede averiguar si eres un usuario de Tor y eso haría que estuvieras en el punto de mira porque quizá piensen que tienes algo que ocultar. Con un poco de esfuerzo, se podría averiguar quién eres y lo que estás haciendo.

Además, el anonimato no es lo mismo que la seguridad. Es difícil hackear la red Tor, pero el navegador es una historia diferente. Como ya hemos visto últimamente, la NSA puede entrar en tu navegador mucho más fácil de lo que puede la red y una vez que lo hace, se obtiene acceso a todo lo demás.

3.2 Como Usar TOR

La forma más sencilla de usar Tor es descargar el paquete de navegación Tor Browser Bundle. Se trata de una versión de Firefox que viene pre configurada para usar la red Tor, lo que permite empezar a usarla sin cometer errores habituales en la configuración. Si queremos usar Tor de una manera más amplia, o para algo más que navegar.

3.3 ¿Si uso TOR Tendré Seguridad Perfecta?

Nada es perfecto, ni siquiera Tor. Si se utiliza incorrectamente, Tor puede destruir completamente la privacidad que deseábamos construir. Si se utiliza Tor, por ejemplo, para acceder a Facebook o Gmail, los servidores pueden no saber de donde viene la petición, pero indudablemente saben quién eres y pueden rastrearlo.

Si se utiliza correctamente, Tor es una de las herramientas de privacidad más útiles que podemos encontrar. Podemos utilizarla para saltar cortafuegos (firewalls) en un país con bloqueos por censura, proteger nuestra privacidad, o navegar de forma segura desde un ordenador público. Instalar y ejecutar Tor es sencillo, y utilizarlo es una de las maneras más fáciles de asegurar una Internet libre y abierta.

4. ONION

.ONION es un pseudo dominio de nivel superior genérico que indica una dirección IP anónima accesible por medio de la red Tor y forman parte de la Deep Web. Aunque tales direcciones no son en realidad DNS, los buscadores web pueden acceder a sitios **.onion** usando proxy y enviando la solicitud a través de servidores de la red Tor. El objetivo de usar este sistema es hacer que tanto el distribuidor de información como el receptor sean difícilmente trazables, ya sea entre ellos, o por un tercero.

En la web de la "superficie" podemos hacer un seguimiento, o encontrar webs por medio de buscadores. En la Deep Web no hay buscadores, (sólo algunos facilitadores), el usuario debe conocer la web que va a visitar, muchas veces bajo contraseña. En la Deep Web se puede encontrar el contenido de la web tradicional pero también todo aquello que no aparece en la ella: pornografía, manuales de guerrilla, hacer explosivos, procedimientos para envenenar, asesinar, ocultar rastros, hackear, narcotráfico, trata de blancas, sicarios, nazismo, venta de órganos, lavado de dinero, compra de artículos robados, pedofilia, etc.

Las direcciones con el pseudo-dominio **.onion** son opacas, no mnemotécnicas y fruto de una combinación de 16 caracteres alfanuméricos generados automáticamente basándose en una clave pública cuando Tor es configurado. Esa combinación de 16 caracteres puede ser creada con cualquier letra del alfabeto y con dígitos decimales entre y 2 y 7 representando un número de 80-bit en base32.

En el siguiente sitio **.onion** se puede encontrar información sobre esta red: <http://am4wuhz3zifexz5u.onion/> pero para ingresar se debe tener TOR instalado o bien utilizar un proxy web como Tor2Web e ingresar al siguiente enlace: <https://am4wuhz3zifexz5u.tor2web.org/> (**Figura 4.0**)



Figura 4.0 Paginas .onion

El Onion Routing, fue introducido por David M. Goldshlag, Michael Reed y Paul Syverson aplicando las ideas de David Chaum para conseguir redes que preserven la privacidad y anonimato (tanto del mensaje como los interlocutores) de forma transparente a las entidades que se comunican. Los mensajes son repetidamente cifrados e enviados a través de varios nodos y redes (*onion routers*) y cada nodo elimina la información del nodo anterior, previniendo que se conozca la información de origen/destino y el contenido del mensaje. En esta red alternativa, las direcciones de las páginas no tienen el formato habitual y son casi ilegibles e imposibles de recordar, empiezan por HTTP (no dejan de ser páginas Web) y tienen la terminación **.ONION**. Para poder acceder a la Deep Web es indispensable estar conectado a la red Tor y utilizar un navegador Web como Tor Project que dispone de versiones para Windows, Linux y Mac.

5. CONCLUSIONES

Para finalizar este artículo, es importante que los usuarios de estas herramientas entiendan que la Deep Web en una red para tener cuidado y TOR no es un navegador 100% seguro Este comentario viene porque es muy frecuente ver que muchas personas ven esta red como un juego o como algo inofensivo. Luego también es necesario comprender que estas soluciones son “óptimas” o no dependiendo de lo que se quiera hacer, por ejemplo si lo que se desea es tener un sitio web anónimo donde publicar cualquier tipo de contenido, probablemente podrían utilizar TOR Por otro lado la intención de esta serie de “tutoriales” (si os apetece llamarlos así) es simplemente informar y dar a conocer estas herramientas,

que existen y están ahí para que cualquiera las utilice, no se trata de “el lado oscuro” como muchos pretenden denominar a este tipo de tecnologías, son HERRAMIENTAS que tienen un alto nivel de seguridad y un alto nivel técnico que han sido desarrolladas por hackers con conocimientos avanzados y que cualquier persona con la intención de ser uno, debería estar interesado en aprender. Ahora bien, muchas personas asocian a TOR como una zona “malvada” llena de terroristas y delincuentes, pero no es así, existen sitios anónimos destinados a investigación en muchas áreas del conocimiento humano y que con el fin de preservar y hacer públicos estos avances, deciden “liberar” sus documentos en este tipo de redes, simplemente con el fin de que se mantengan como un recurso de todos y para todos, minimizando el riesgo de censura o limitación (lo cual es muy común en regímenes totalitarios o estados represores). Por este motivo, insisto en que es importante y merece la pena aportar a estas soluciones, que no necesariamente tienen que ser aportes económicos, simplemente usarlas, probarlas, documentarlas, estudiarlas (caso de TOR) o dejar levantado el servicio en una máquina ya es un aporte significativo.

6. BIBLIOGRAFIA

- [1] <http://www.ingeniosistemas.com/caracteristicas-de-un-sitio-web/2012/04/01/>
- [2] <http://thehackerway.com/2012/02/08/preservando-el-anonimato-y-extendiendo-su-uso-comparacion-de-redes-anonimas-y-conclusiones-finales-parte-xxxxii/>
- [3] <http://highsec.es/2013/03/introduccion-a-la-navegacion-anonima-tor/>
- [4] <http://es.wikipedia.org/wiki/Tor>
- [5] <https://www.torproject.org/>