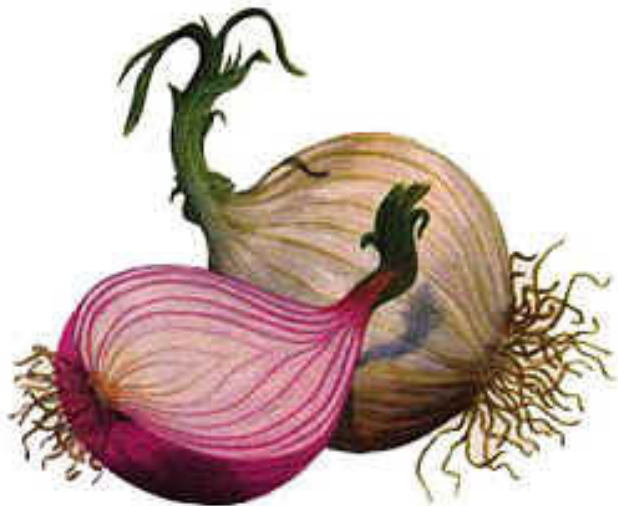


aLeZX

Anónimos en la Red

Primera parte



Este documento ha sido liberado según los términos de la GNU Free Document License (GFDL), que pueden ser consultados en el siguiente sitio web:
<http://www.gnu.org/copyleft/fdl.html>

Copyright © 2006 Alejandro Sánchez Postigo

Se otorga permiso para copiar, distribuir y/o modificar este documento bajo los términos de la Licencia de Documentación Libre de GNU, Versión 1.2 o cualquier otra versión posterior publicada por la Free Software Foundation; sin Secciones Invariantes ni Textos de Cubierta Delantera ni Textos de Cubierta Trasera. Una copia de la licencia está incluida en la sección titulada GNU Free Documentation License.

Cuando uno empieza a escribir un artículo ni se le pasa por la mente la cantidad de información que existe sobre el tema y que desconoce. Cuanto más sabe uno, más cuenta se da de lo poco que conoce. Eso mismo fue lo que me ocurrió a mí cuando, hace algunos meses, me decidí a escribir cierto documento sobre Anonimato en la Red.

Sin embargo, uno se da cuenta de que una de las mejores formas de aprender es mediante la escritura de un artículo que después servirá de ayuda para los demás. Eso fue lo que me llevo a mí a comenzar a escribir el texto que ahora mismo tienes delante de tus ojos.

Espero que sea de tu agrado.

Sin más, comencemos.

aLeZX

ÍNDICE

1.- INTRODUCCIÓN

2.- ENTRANDO EN MATERIA

3.- PROXIES

3.1.- ANONIMATO EN FIREFOX CON PROXIES (NAVEGAR ANÓNIMO)

3.2.- CADENAS DE PROXIES

4.- TOR: THE ONION ROUTER

4.1.- MODUS OPERANDI

4.2.- TOR EN WINDOWS

5.- CONCLUSIONES Y DESPEDIDA

ANÓNIMOS EN LA RED

PRIMERA PARTE

El anonimato, al igual que la privacidad, es, a mi parecer, un bien preciado y, por ello, no podemos permitir que sea vulnerado. También es cierto que, por el mero hecho de existir sobre la faz de la Tierra, en el lugar más recóndito del Universo habrá constancia de nuestra existencia. Si bien, debemos intentar por todos los medios ser nosotros quienes decidamos ser anónimos o no, y que no sean otros quienes se tomen la libertad de hacerlo.

Esto mismo es, igualmente, aplicado a la Red de redes: Internet.

¡Seamos anónimos!

1.- INTRODUCCIÓN

Durante la edición de este documento he cambiado multitud de veces la forma de escribirlo e, incluso, a veces, he variado, dentro de lo que cabe, la temática. Verdaderamente, los numerosos borradores que he escrito nunca me convencían. Finalmente, aparqué este artículo con la idea de no escribirlo.

Sin embargo, mientras un día vagaba por las tierras de Wadalbertia, me topé con cierto post acerca del anonimato e hice saber al resto de mis compañeros la existencia de este documento. Algunos de ellos me motivaron a escribirlo, en especial mi compañero de fatigas, NeTTinG (aprovecho para mandarle un fuerte saludo desde aquí). Gracias a esto, me puse a indagar acerca de este tema y, por fin, he acabado la primera parte del trabajo.

Dicho todo esto, y antes de que comencéis a bostezar y cerrar el PDF, comienza Anónimos en la Red. ¡Qué disfrutéis!

2.- ENTRANDO EN MATERIA

Si escribimos en Google un simple *define:anonimato* nos aparecerá, entre los distintos enlaces, la siguiente definición de la Wikipedia:

El anonimato es el estado de una persona siendo anónima, es decir, que la identidad de dicha persona es desconocida. Esto puede ser simplemente porque no se le haya pedido su identidad, como en un encuentro ocasional entre extraños, o porque la persona no puede o no quiere revelar su identidad.

En el mundo de la informática el anonimato es exactamente lo mismo. Aunque no lo creáis, todo lo que hacéis en Internet va quedando registrado. Por ejemplo, cuando nos conectamos a un servidor web, en éste queda almacenada información referente a nosotros: dirección IP, navegador web usado, sistema operativo, etc. Para que podáis comprobarlo vosotros mismos, entrad en alguna de las siguientes páginas: <http://cualesmiip.net> o <http://webproxies.net> . ¿Os dais cuenta de toda la información que se da a conocer acerca de

vosotros cada vez que accedéis a una página web? Muchos dirán que, si no tienen nada que ocultar, qué más les da que conozcan qué es lo que hacen mientras se conectan a Internet. A mí, personalmente, la idea de que otros puedan vulnerar mi privacidad me aterra.

Para acabar con esta situación existen los proxies. A continuación explicaré su funcionamiento.

3.- PROXIES

Un **proxy** es un programa informático que se encuentra instalado en una máquina (a la que se le suele llamar también *proxy* o *servidor proxy*), la cual actúa de intermediario entre ordenadores, es decir, se interpone entre ellos haciéndose pasar el tráfico por él.

Leyendo esta definición es fácil darse cuenta de que el cometido de la existencia de los proxies en este mundo no es simplemente dar anonimato. Es cierto. Hoy en día se usan proxies para casi todo. Tenemos un proxy para conectar todos nuestros ordenadores a Internet a través de él, tenemos un proxy que nos ha implantado nuestro ISP, tenemos un proxy que actúa de caché, etc. Pero en todos los casos, los proxies no dejan de ser intermediarios entre un origen y un destino.

Ahora centrémonos en el campo del anonimato. ¿Cómo podríamos mediante un proxy hacernos anónimos ante el mundo? Es simple. Si todo nuestro tráfico llegase hasta él, y fuese él quien conectase con nuestro objetivo, nunca quedaría registrada nuestra dirección IP, ni ningún otro dato más en el ordenador destino, sino los datos del proxy. En la siguientes figuras se aprecia bastante bien el funcionamiento de un proxy: conexión directa a Wadalbertia.org (*Imagen 1*); conexión a Wadalbertia.org interponiendo un proxy (*Imagen 2*).

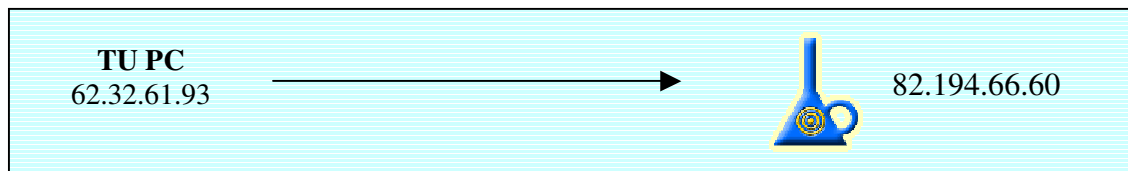


Imagen 1

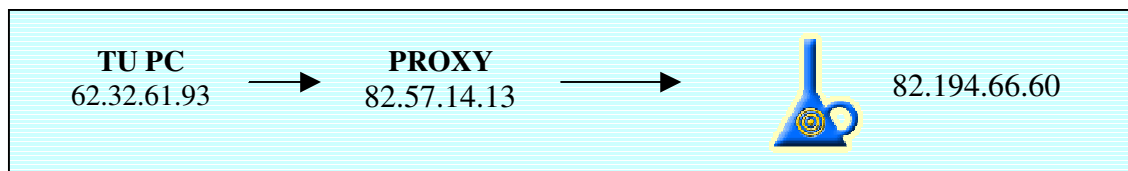


Imagen 2

En la **imagen 1** nos conectamos al servidor web donde se aloja Wadalbertia.org. En ese servidor quedará registrada la dirección IP 62.32.61.93 (nuestra IP) y otra información adicional.

Por el contrario, en la **imagen 2** nos conectamos también al servidor web de Wadalbertia.org, pero esta vez a través de un proxy, por lo que en el servidor quedarán los datos del proxy (82.57.14.13), y no los nuestros.

Más adelante volveremos a tocar el tema de los proxies, pues hablar de anonimato sin nombrar los proxies es como ir a París y no visitar la Torre Eiffel. Sin embargo, antes de entrar en otros temas, vamos a realizar una pequeña práctica en la que *anonimizaremos* nuestro navegador web Mozilla Firefox.

3.1.- ANONIMATO EN FIREFOX CON PROXIES (NAVEGAR ANÓNIMO)

Vamos a hacer una pequeña y fácil práctica con los proxies, que nos dejará bastante claro su funcionamiento y, además, servirá de contacto con el mundo del anonimato. Para empezar, lo ideal sería hacernos con una **lista de proxies**. En Internet existen cientos de webs en las que se muestran las direcciones IP y los puertos de distintos servidores proxies situados en diferentes puntos del planeta. Estos datos serán los que necesitaremos para nuestros fines. Con una simple búsqueda en Google de la palabra *proxy* encontramos miles de webs que nos facilitarán todos estos datos. Algunas de mis webs favoritas son: <http://samair.ru/proxy>, <http://www.multiproxy.org>, <http://www.stayinvisible.com>, etc.

En este ejercicio nos dirigiremos, por ejemplo, a <http://samair.ru/proxy> y elegimos uno de la lista. ¿Cuál? Bien, no todos los proxies son iguales y funcionan de la misma forma. Mi recomendación es usar **elite proxies** (también conocidos como **high anonymity proxies**) ya que usando estos el servidor al que nos conectemos ignorará su existencia (ignorará que estemos usando un proxy). Otra opción es utilizar **proxies anónimos simples**, aunque es posible que el servidor “sea consciente” de su presencia. Desde luego, los que nunca debemos usar para el anonimato son los **proxies transparentes**, ya que estos mostrarán nuestra dirección IP (no se usan para el anonimato).

Una vez que hayamos elegido a nuestro intermediario, nos fijamos en su dirección IP y su puerto (en algunas webs la forma de mostrar estos datos es [IP]:[PUERTO]) y los apuntamos. A continuación nos dirigimos, en nuestro navegador web Mozilla Firefox, a *Herramientas – Opciones (Imagen 3)*. Dentro de la ventana *Opciones (Imagen 4)* nos introducimos en *Configuración de conexión...* (*Imagen 5*). En la ventana que nos aparece escribimos la dirección IP del proxy en *Proxy HTTP* y en *Puerto*, el puerto. Aceptamos todo y ya deberíamos navegar a través del proxy. Para comprobarlo nos dirigimos a alguna de las webs que di anteriormente, por ejemplo, <http://webproxies.net>... *et voilà (Imagen 6)*. Os puedo asegurar que cuando hice esa captura de pantalla no me encontraba en Corea :)

Seguramente, os habréis percatado de que la velocidad de vuestra conexión ha disminuido notablemente. Esto se debe a que vuestro ancho de banda ha quedado reducido al ancho de banda del proxy. A esto hay que añadirle el tiempo que tarden las distintas máquinas en “hablar” entre ellas (ping).

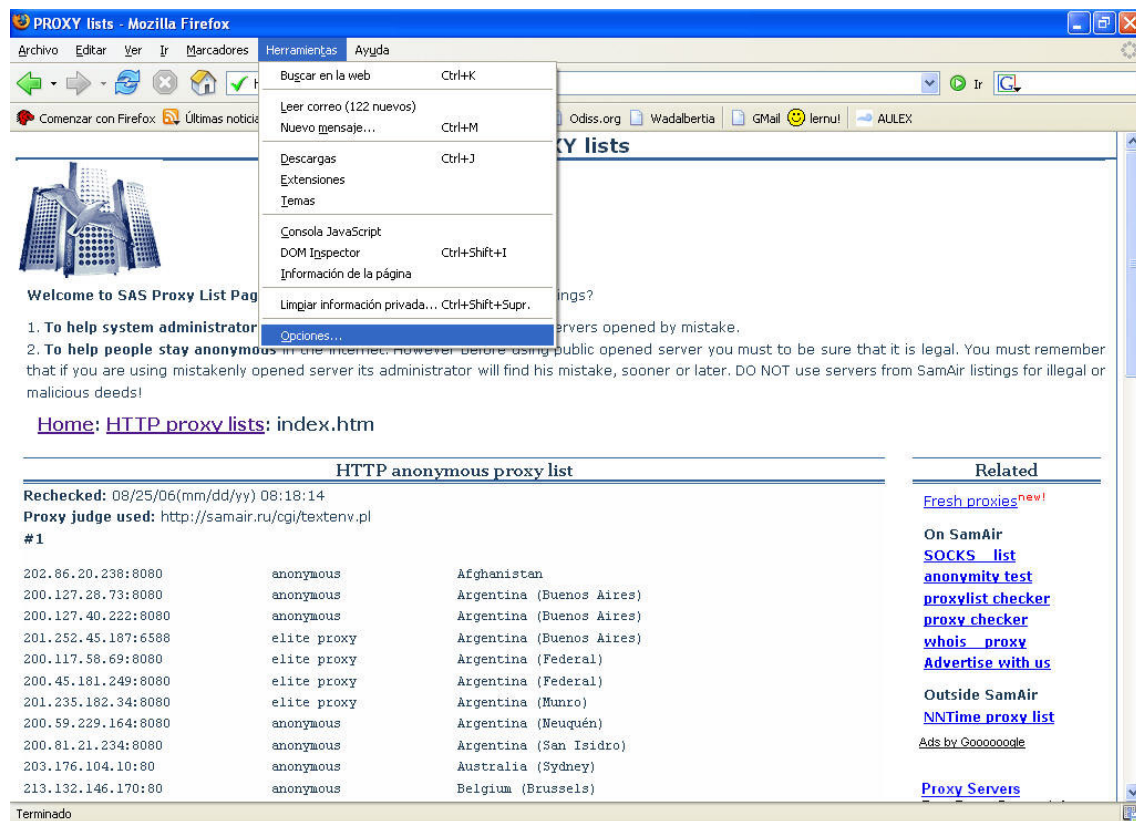


Imagen 3

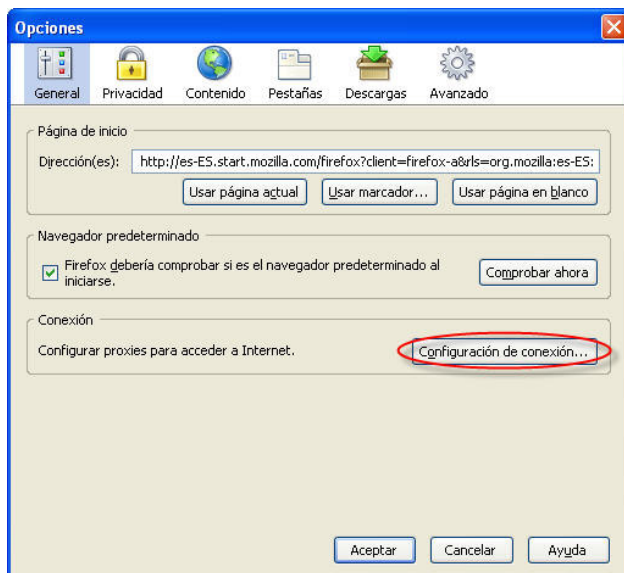


Imagen 4

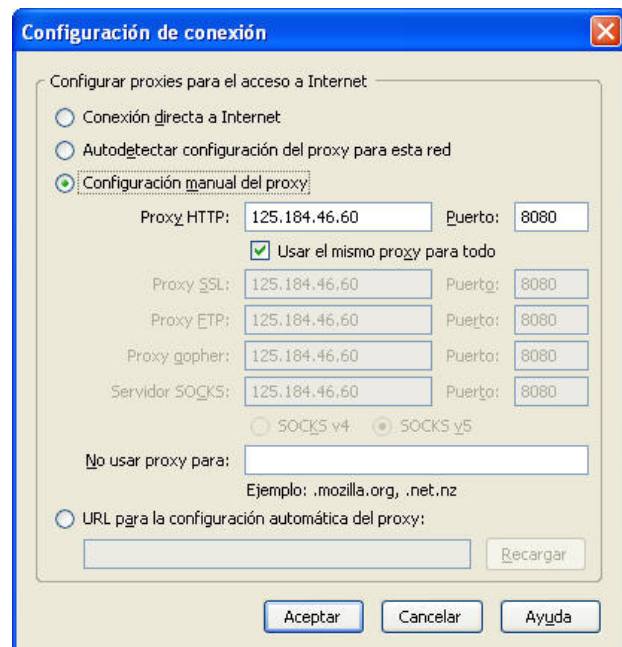



Imagen 5

Over 500 Simple To Use Broadband Web Proxy Servers

UNIQUE INTERNET SERVICES


Unique Internet Services Makes Your Ideas And Needs Come True
Access To Over 500 Web Proxy Servers  [Click Here](#)

Access All Proxy Types

You get access to ALL of these proxy types in our list

- Normal HTTP Web Proxies
These are standard everyday servers
- SSL / Secure Web Proxies
While using these, not even your isp can read the pages that you visit.
- Access To Off-Shore Proxies
These are proxies that are in private data centers off shore and out of the USA.
- Access To Out Source Proxies
These are proxy servers leased from other proxy sources
- Vanity Domains
These are domains made up for fun browsing for example ask.me.for.date.org

Testing Your Firewall...

You are visiting us from Korea, Republic of (KR) 
Your location can be seen, because your Firewall is not hiding your IP address

Until you hide your ip address, anyone on the net can see the personal information shown below

Your IP Address : 125.184.46.60
Your Country : Korea, Republic of (KR)
Your ISP Name : Dacom
Your Latitude : 37.0000
Your Longitude : 127.5000
Your Browser Version : Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.8.0.6) Gecko/20060728 Firefox/1.5.0.6

If you were using our WebProxy, the personal information shown above would be hidden

A WebProxy also keeps others from sniffing your data and reading your e-mail

A Web Proxy is a link to our web page that loads a proxy interface page. It is an easy way to browse the net anonymously. When the proxy page loads, you can type in a URL and visit any web page anonymously. While using the Secure Server option, all web sites that you visit will be encrypted. This means that other computers on the WAN will not be able to read or sniff your Internet packets. Administrators will not be able to view your web pages, images, email text, etc. Also your real ip address

Imagen 6

3.2.- CADENAS DE PROXIES

Fijaos en el título de este apartado: “Cadenas de proxies”. Como su nombre indica, una cadena de proxies no es más que un enlace entre distintos proxies, es decir, en lugar de interponer una máquina entre nosotros y el destino, interponemos varios proxies. Con este dibujo lo entenderéis a la perfección (*Imagen 7*).

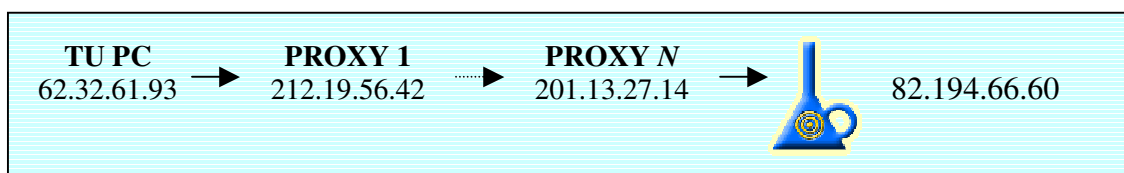


Imagen 7

Desde luego, la seguridad que ofrece una cadena de proxies es considerablemente mayor a la de un proxy solo. También presenta más inconvenientes: mayor pérdida del ancho de banda, si uno de los proxies falla (algo muy común) toda la cadena falla...

Como esto no tiene ninguna complicación, os daré los nombres de algunos programas y OS RECOMIENDO ENCARECIDAMENTE, por no decir que OS OBLIGO, a que trasteéis con ellos. En la Red encontraréis tal cantidad de información que no os resultará nada complejo. Recuerda: Google es tu amigo :). Recuerda 2: En Wadalbertia estamos para ayudarte. A lo que iba. Por un lado tenemos el programa **ChainSocks**, que actuará de servidor proxy y nos permitirá establecer las cadenas, y por otro, **FreeCap** y **SocksCap**, que, además de permitirnos también crear encadenamientos, nos da la opción de interceptar el tráfico y dirigirlo hacia el proxy o cadena (*socksficar*) (usado en los programas que entre sus opciones no incluyen la de introducir proxies).

Espero que os haya gustado el mundo de los proxies, aunque lamento no haberme extendido más por el momento. Algunas recomendaciones antes de hacer una pausa. Cuando creéis una cadena de proxies con los programas que cité anteriormente, probad antes los que la van a constituir. ¿Por qué? Porque es muy común que alguno que otro falle y entonces, adiós cadena. De hecho, cuando hicimos la práctica del Firefox, estoy seguro de que a más de uno le fallaron los proxies (daba error al cargar la página, se agotaba el tiempo de espera, etc.). Así que, es preferible asegurarse de que funcionan los proxies escogidos. Ya, la última recomendación y os dejo: NO os creáis que por usar proxies (o cadenas) habréis dejado de existir en el mundo. Si pensáis esto, estáis muy equivocados. Cualquier individuo con las ganas y, sobre todo, el dinero suficiente, podría encontraros. **EL ANONIMATO TOTAL NO EXISTE.**

Así que ya sabéis, portaos bien, aunque uséis proxies.



4.- TOR: THE ONION ROUTER

Creado por Roger Dingledine y Nick Mathewson (entre otros desarrolladores), el proyecto Tor nació en el US Naval Research Lab (motivo por el cual muchos no se fían de la fiabilidad de este programa). Posteriormente, fue financiado por la EFF (Electronic Frontier Foundation), que actualmente se encarga del hosting de su web.

Según la definición de la EFF (Electronic Frontier Foundation), la cual defiende los derechos en Internet:

Tor es una red de túneles virtuales que permiten a las personas y grupos mejorar su privacidad y seguridad en Internet. También posibilita a los programadores crear nuevas herramientas que incorporen características de privacidad. Tor proporciona la base para un abanico de aplicaciones que permitan a las organizaciones y a los individuos compartir información sobre redes públicas sin comprometer su privacidad.

Tor es un sistema de anonimato para las comunicaciones en Internet. Con Tor podremos hacer anónima la navegación web, mensajería instantánea, IRC, SSH, y, en definitiva, cualquier aplicación que use el protocolo TCP.

Basándonos en la EFF, el objetivo de Tor es impedir el **análisis de tráfico**. ¿El qué? El análisis de tráfico es una técnica (al igual que el análisis de paquetes, también conocido como sniffing) cuyo objetivo es conocer, no el contenido de tus paquetes, sino los movimientos de éstos por la Red. Si os dais cuenta, esto es lo mismo que llevamos intentado hacer desde que empezamos el artículo: ser anónimos.

4.1.- MODUS OPERANDI

¿Conocéis el refrán: “Todos los caminos conducen a Roma”? Pues en esta frase tan común se basa Tor. Su funcionamiento es bastante sencillo. Imaginad que nos queremos conectar nuevamente a Wadialbertia.org. Si enviásemos nuestros paquetes directamente al servidor en el que se aloja Wadialbertia, tendríamos dos problemas:

- a) Mucha información referente a nosotros podría quedar *logeada* en el servidor de Wadialbertia.
- b) Cualquier individuo interpuesto entre nosotros y nuestro destino que estuviese realizando un análisis de tráfico podría analizar las cabeceras de nuestros paquetes (aunque éstos estuviesen encriptados), con lo que fácilmente sabría a dónde nos dirigimos.

Para impedir que esto ocurra, el cliente Tor que se encuentra instalado en nuestro ordenador establece un circuito constituido por servidores Tor (nodos) elegidos de forma aleatoria. El origen del circuito sería nuestro PC y el final, nuestro destino. Una vez establecido el circuito se emplea éste para enviar los paquetes de datos. Los distintos nodos que constituyen el circuito desconocen el itinerario completo de los paquetes. Simplemente conocen el nodo que se los envían y al que debe enviar. Por si fuera poco, cada tramo del circuito tiene una serie de claves de encriptación. El circuito cambia periódicamente, construyéndose un nuevo camino

cada, aproximadamente, un minuto. De esta forma, es prácticamente imposible que alguien consiga hacernos un análisis de tráfico, pero recordad: EL ANONIMATO TOTAL NO EXISTE.

En las **imágenes 8, 9 y 10** se puede observar como actúa Tor de una forma clara y concisa. Como veis, el funcionamiento de Tor se asemeja en algunos aspectos al de una cadena de proxies, aunque, claro está, no es exactamente igual.



Imagen 8

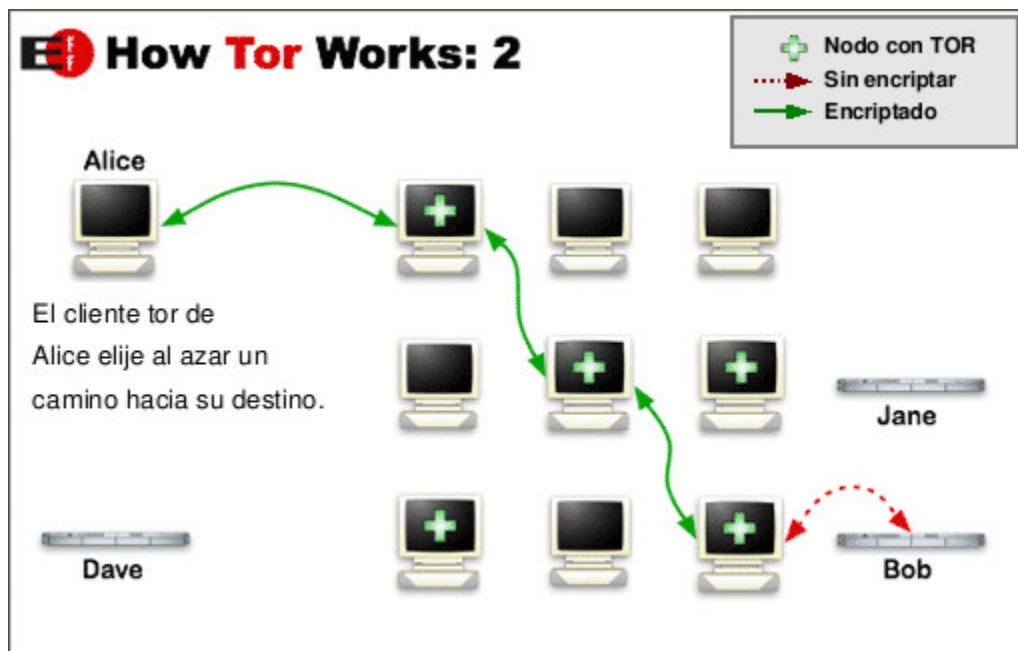


Imagen 9

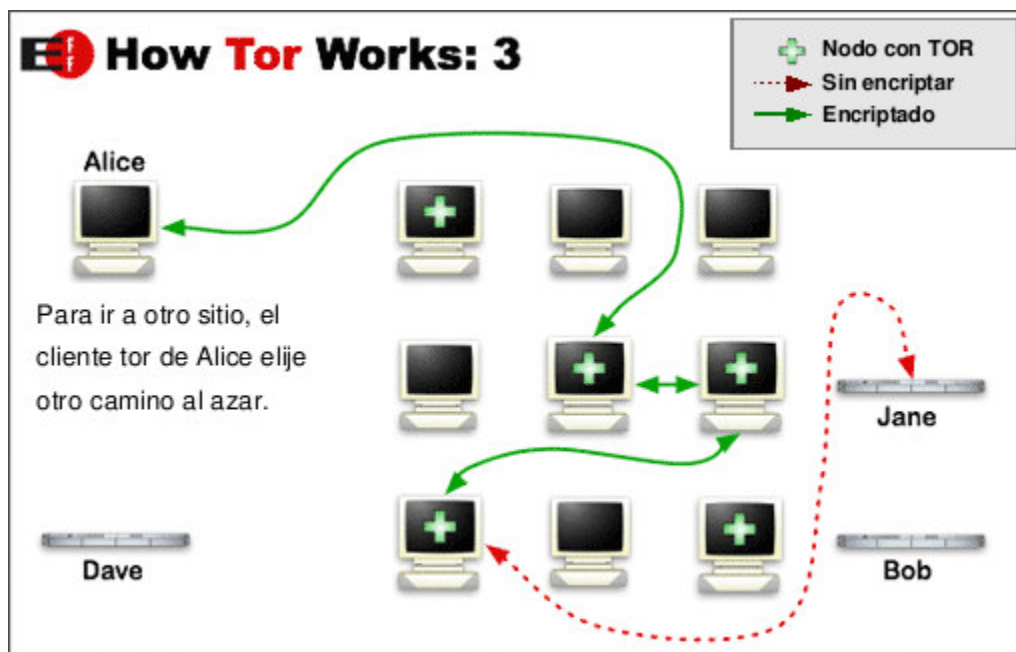


Imagen 10

4.2.- PRACTICANDO CON TOR (WINDOWS)

Vamos a iniciar la parte práctica del artículo. Para poder empezar a trastear con Tor, lo primero es descargárnoslo desde el sitio web oficial: <http://tor.eff.org/>

Para los más vagos, el link directo a la zona de descargas es: <http://tor.eff.org/download.html.es> (Imagen 11)

Tor: Paquetes y fuentes

Tor se distribuye como [Software Libre](#) bajo la [cláusula-3 de la licencia BSD](#).

Si quieres que Tor sea mas rapido y usable, por favor considera [hacer una donacion al proyecto Tor](#).

La ultima version estable es **0.1.1.23**, y la ultima version de desarrollo es **0.1.1.23**.

Suscríbete a la [lista de correo or-announce](#) para mantenerte informado de las recomendaciones de seguridad y las nuevas publicaciones de versiones estables (necesitaras confirmar via email):

Plataforma	Paquete	Info Configuración
Windows: paquete Tor & Privoxy & TorCP	0.1.1.23 (sig) , 0.1.1.23 (sig)	instrucciones Win32
Windows: solo Tor (para expertos)	0.1.1.23 (sig) , 0.1.1.23 (sig)	similar a las instrucciones Unix
Mac OS X Tiger (OSX 10.4)	0.1.1.23 (sig) , 0.1.1.23 (sig)	instrucciones OS X
Mac OS X Panther (OSX 10.3)	0.1.1.23 (sig) , 0.1.1.23 (sig)	instrucciones OS X
Debian	<code>apt-get install tor</code>	<ul style="list-style-type: none"> instrucciones Linux/BSD/Unix Backports para Woody y Sarge, Paquetes para Ubuntu, y paquetes de versiones de Tor

Terminado

Imagen 11

Como a nosotros nos gusta hacer las cosas difíciles y de la forma que más se aprende, NO nos descargaremos el paquete para Windows *Tor & Privoxy & TorCP*, sino que nos bajaremos el paquete *solo Tor (para expertos)* :). Para ello pulsamos en la versión del programa que nos queramos descargar (la última, en mi caso: 0.1.1.23). Una vez hecho esto, nos aparecerá la típica ventanita de si queremos guardarlo en el disco, a lo que pulsaremos que sí... y blablabla blablabla blablabla...

Finalizada la descarga, ejecutamos el instalador (**Imagen 12**). No creo que la instalación requiera la mayor explicación: Next – Next – Install – Finish. Si todo ha salido bien (y si habéis dejado marcada en la última ventana del instalador la opción *Run Tor*) tendréis ante vuestros ojos la grandiosa interfaz del cliente Tor: una línea de comandos :) (**Imagen 13**).



Imagen 12

Como veis, nada más iniciarse Tor, éste comienza a construir el circuito. En el rectángulo rojo de la **imagen 13** se puede apreciar el mensaje que muestra Tor una vez que el circuito se ha establecido.

Ya tenemos ejecutando Tor y el circuito creado. Ahora es el momento de usarlo. Vamos a *anonimizar* nuestra navegación web.

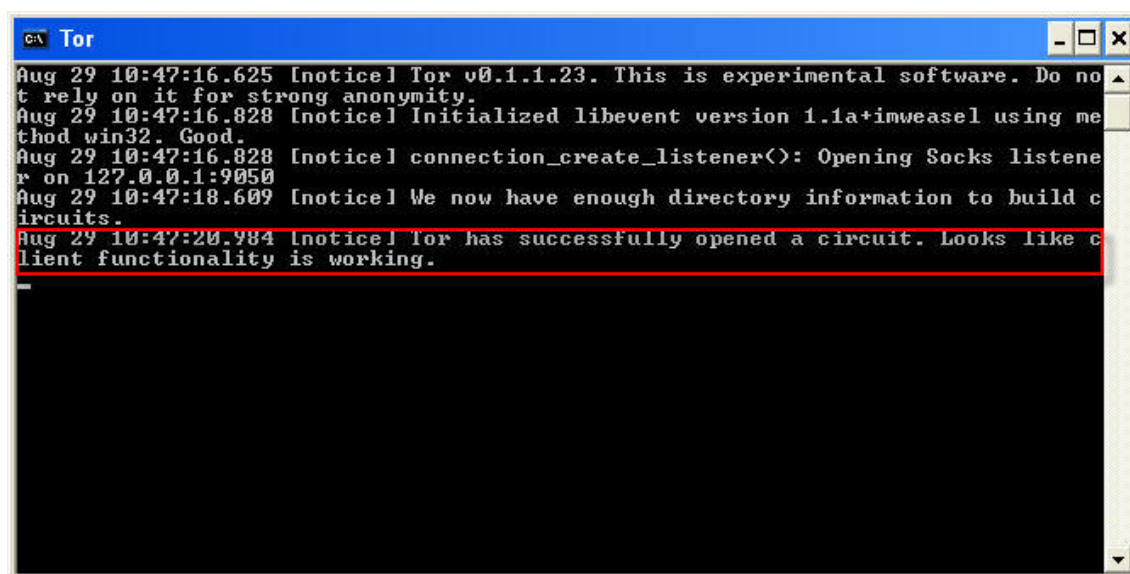


Imagen 13

Digamos que, a la hora de usar el cliente Tor, éste actúa como un servidor proxy. Por lo que, si vamos a *anonimizar* nuestro Mozilla Firefox, nos dirigimos a *Herramientas – Opciones – Configuración de conexión...* y, una vez allí, lo dejamos todo tal como aparece en la **imagen 14**.

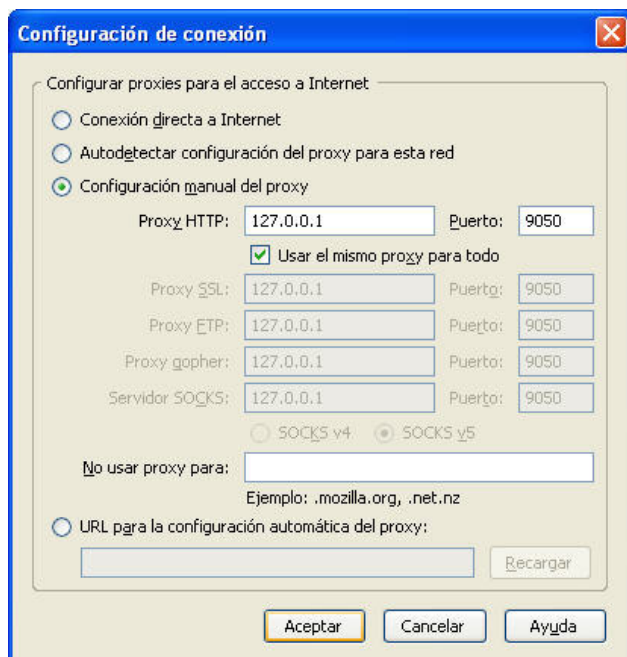
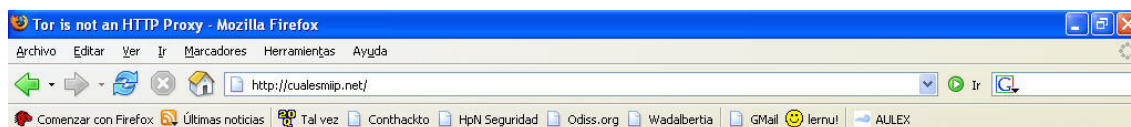


Imagen 14

¿Por qué ponemos en *proxy HTTP* la dirección IP 127.0.0.1? Porque ésta es la dirección IP interna de todo ordenador y que, por lo tanto, apunta a nuestro cliente Tor (actúa de servidor). Ponemos el puerto 9050 porque es el puerto por defecto que escucha Tor.

Aceptamos todo y nos conectamos a, por ejemplo, <http://cualesmiip.net>. Y... ¿qué es esto? (**Imagen 15**). Como vemos, se nos muestra un mensaje de error que nos viene a decir que Tor no es un proxy HTTP, sino un proxy SOCKS. ¿Qué significa esto?



Tor is not an HTTP Proxy

It appears you have configured your web browser to use Tor as an HTTP proxy. This is not correct: Tor is a SOCKS proxy, not an HTTP proxy. Please configure your client accordingly.

See <http://tor.eff.org/documentation.html> for more information.

Terminado

Imagen 15

Por regla general, los proxies HTTP (los que nos solemos encontrar en las listas que circulan por Internet) sólo funcionan con el protocolo HTTP; los proxies FTP, con el protocolo FTP; los proxies IRC, con el protocolo IRC; es decir, necesitaríamos un tipo de proxy para cada servicio. (Digo “por regla general”, porque existen los llamados **proxies HTTP – CONNECT**, que son proxies para TCP que funcionan con prácticamente cualquier servicio).

Por otro lado, existen los **proxies SOCKS**, que también son proxies para TCP que usan el protocolo SOCKS (RFC1928) y que pueden ser usados para prácticamente cualquier servicio. Pues bien, Tor actúa como un servidor SOCKS, motivo por el cual puede ser utilizado con cualquier aplicación que emplee el protocolo TCP (RFC0793).

El error de la **imagen 15** se debe a que hemos indicado a Firefox que utilice un servidor SOCKS (Tor) como un proxy HTTP. El navegador web Mozilla Firefox tiene soporte para los protocolos SOCKSv4 y SOCKSv5 (distintas versiones del protocolo SOCKS). Por lo tanto, para poder usar Tor, simplemente debemos indicar que usaremos un proxy SOCKS y no un proxy HTTP. Para ello, nos dirigimos a *Herramientas - Opciones – Configuración de conexión...* y lo dejamos como se observa en la **imagen 16**.

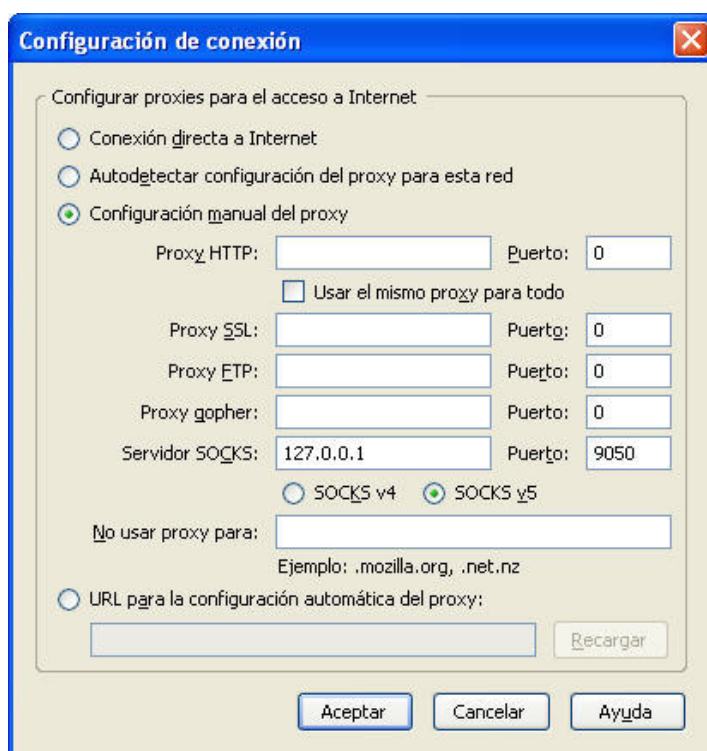


Imagen 16

¿Veis? En este caso hemos introducido los datos de Tor en las casillas de *Servidor SOCKS*. Cuando lo poníamos en Proxy HTTP, Firefox intentaba “hablar” con Tor en HTTP y como Tor no es un proxy HTTP (no entiende el protocolo HTTP) daba el error anterior.

Una vez hecho todo esto, aceptamos todo y nos dirigimos, ésta vez sí, a <http://cualesmiip.net> (**Imagen 17**). Nuestra IP real no aparece (supuestamente conecto desde Estados Unidos). Al poco tiempo de hacer este pantallazo volví a conectarme a <http://cualesmiip.net> (**Imagen 18**). El circuito ya había cambiado: IP nueva.



Imagen 17



Imagen 18

Ahora nos vamos a centrar en la ventanita de línea de comandos de Tor. Mmm... hay algunos cambios (*Imagen 19*).

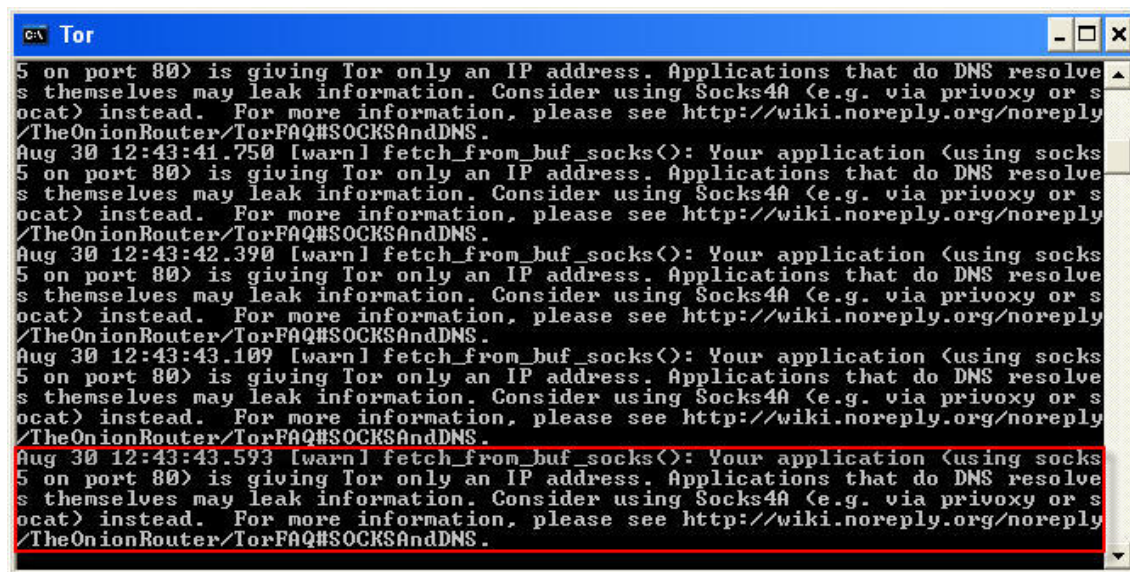


Imagen 19

Al hacer peticiones DNS usando directamente un proxy SOCKS5, Tor nos advierte de que nuestro explorador (aplicación usando SOCKS5 en el puerto 80) falla. Esto nos quiere decir que la petición DNS (para resolver los nombres de dominio) no pasa por el servidor SOCKS, es decir, no pasa por Tor, lo cual no es muy recomendable (en ese aspecto no seríamos anónimos).

Tenemos varias opciones, pero aquí sólo trataré las más extendidas. Para más información: <http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#SOCKSAndDNS>.

Primera opción: Por defecto, Mozilla Firefox no hace pasar las peticiones DNS a través de los servidores SOCKS, pero a partir de la versión 1.5.0.1 puede ser configurado para que lo haga. Vayamos a ello. En primer lugar configuramos Firefox para usar Tor. Una vez hecho esto, escribimos en la barra de direcciones del navegador: *about:config*. Nos aparecerá la página de información sobre la configuración del explorador web (*Imagen 20*). En la parte superior de la página, en el cuadro de texto donde pone *Filtro*, tecleamos: *socks_remote_dns* (*Imagen 21*). Por último, hacemos doble clic en *network.proxy.socks_remote_dns*, con lo que esta entrada tomará el valor *True* y, por consiguiente, la resolución de nombres de dominio se realizará también a través de Tor (*Imagen 22*). Reiniciamos Firefox y listo.

Comprobamos que somos anónimos y nos aseguramos de que, esta vez, Tor no nos advierte de ningún problema con las DNS.

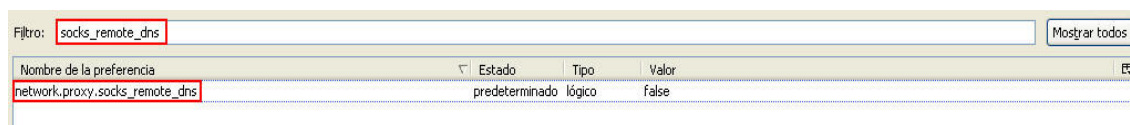


Imagen 21

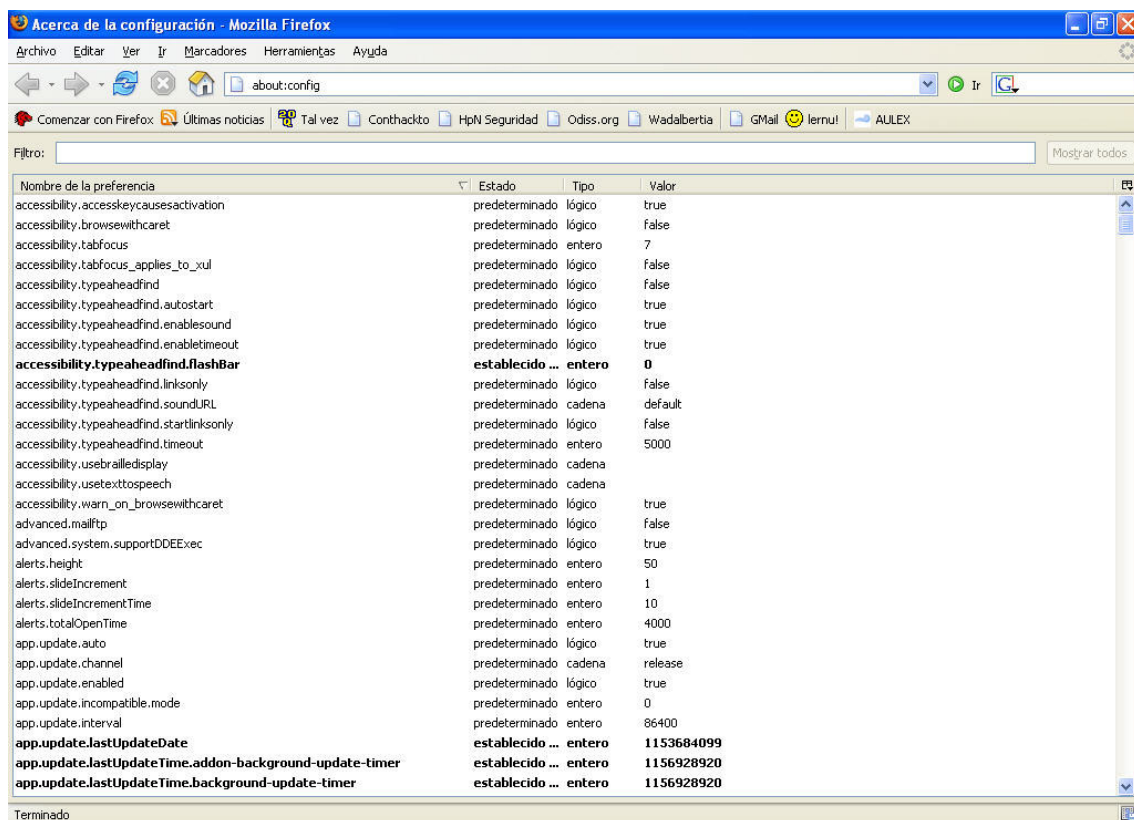


Imagen 20

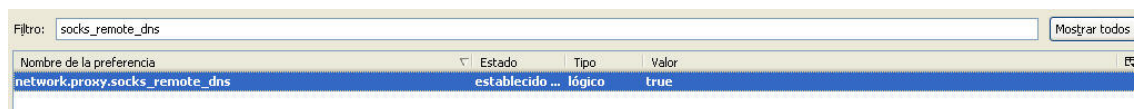


Imagen 22

Ahora es el turno de la segunda opción, la cual no puedo pasar por alto ya que es, posiblemente, la más usada de todas. De hecho, está tan difundida que en la web de descarga de Tor existe el paquete para Windows: *Tor + Privoxy*, y, es que, cualquier persona que use Tor, sin duda, habrá oído hablar del proxy HTTP Privoxy, uno de sus mejores amigos. Además, Privoxy nos filtrará información sobre nuestro navegador, cookies y nos protegerá de banners, pop-ups, que a veces atentan contra nuestra privacidad.

En primer lugar vamos a descargarnos Privoxy desde su sitio web oficial: <http://www.privoxy.org>. Pulsamos en *Download recents releases* y pasamos a la típica página de *SourceForge*. Nos descargamos el paquete para Win32 *clicando* en *Download (Imagen 23)*. En la siguiente web seleccionamos el archivo; posteriormente, un mirror y nos lo descargamos.

A continuación iniciamos el programa de instalación (*Imagen 24*). La instalación no supone ninguna dificultad: *I Agree – Next – Install – Aceptar*

Latest File Releases				
Package	Release	Date	Notes / Monitor	Downloads
Actions File	1.8	January 30, 2004	-	Download
AmigaOS	3.0.3 (stable)	January 30, 2004	-	Download
Conectiva Linux (RPM)	3.0.0 (stable)	August 29, 2002	-	Download
Debian	3.0.3 (stable) woody	January 30, 2004	-	Download
Fedora Core 1	3.0.3 (stable) FC1	February 19, 2004	-	Download
HP-UX 11	3.0.0 (stable)	August 29, 2002	-	Download
Mac OSX	3.0.3 (stable)	January 30, 2004	-	Download
OS/2	3.0.3 (stable)	January 30, 2004	-	Download
Redhat RPM	3.0.3 (stable) RH6.x	February 17, 2004	-	Download
Sources	3.0.3 (stable)	January 30, 2004	-	Download
SuSE RPM	3.0.3 (stable)	January 30, 2004	-	Download
Win32	3.0.3 (stable)	January 30, 2004	-	Download

Imagen 23**Imagen 24**

Una vez instalado, veremos que nos aparece un icono con forma de “P” en la barra de tareas, al lado del reloj de Windows (**Imagen 25**).

**Imagen 25**

Si hacemos doble clic sobre el icono de Privoxy nos aparecerá la ventana principal del programa. En el log que vemos en la pantalla se nos especifica, entre otros datos, el puerto en el que el servidor proxy se encuentra a la escucha. Por defecto: 8118. Pero para que Tor y Privoxy se lleven bien, hace falta configurar Privoxy para que interactúe con Tor. Para ello, nos dirigimos, en Privoxy, a *Options – Edit Main Configuration* y nos aparecerá un fichero del bloc de notas que deberemos modificar. Las modificaciones a realizar son:

1. Añadir la siguiente línea al fichero para, de esta forma, redirigir el tráfico desde Privoxy hasta Tor. Hay que tener en cuenta el punto al final de la cadena.

forward-socks4a / localhost:9050 .

2. Comentar las siguientes líneas del fichero (añadiéndoles una almohadilla #), para que no se guarden logs:

```
logfile privoxy.log  
jarfile jar.log
```



```
# logfile privoxy.log  
# jarfile jar.log
```

Una vez hecho esto guardamos la nueva configuración y reiniciamos Privoxy. Para ello cerramos la ventana principal y el tray icon (botón derecho sobre el icono de la barra de tareas – *Exit Privoxy*) y los volvemos a abrir desde *Inicio – Todos los programas – Privoxy – Privoxy*.

De nuevo toca anonimizar Firefox. Esta vez, mediante Privoxy-Tor. Como Privoxy es un proxy HTTP, debemos indicar a Firefox que usamos un proxy HTTP y no uno SOCKS, como antes. En Firefox nos dirigimos a *Herramientas – Opciones – Configuración de conexión...* y lo dejamos como aparece en la **imagen 26**.

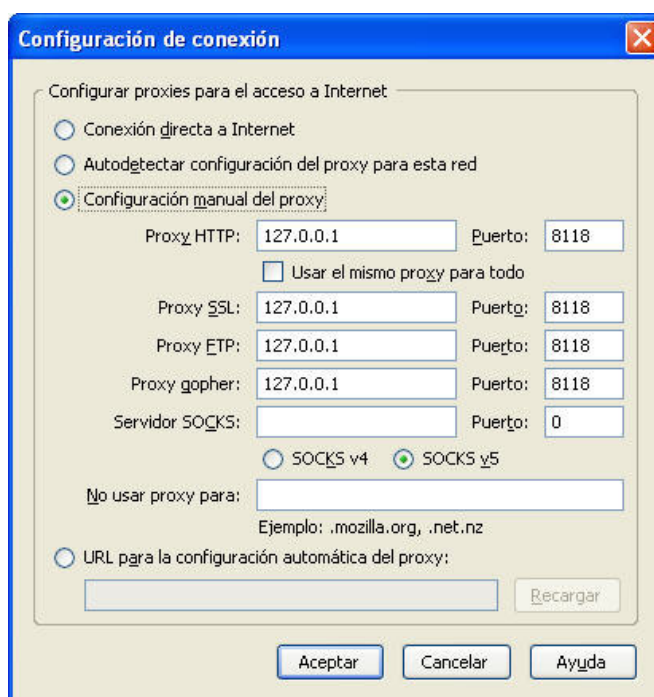


Imagen 26

Configurándolo así, podremos navegar anónimos por Internet siempre que usemos el protocolo HTTP. Firefox se conecta con Privoxy (Proxy HTTP) y Privoxy con Tor (servidor SOCKS). De esta forma, no tenemos el problema con las DNS y además, quedan filtrados los banners y pop-ups que atentan contra nuestra privacidad (**Imagen 27**).

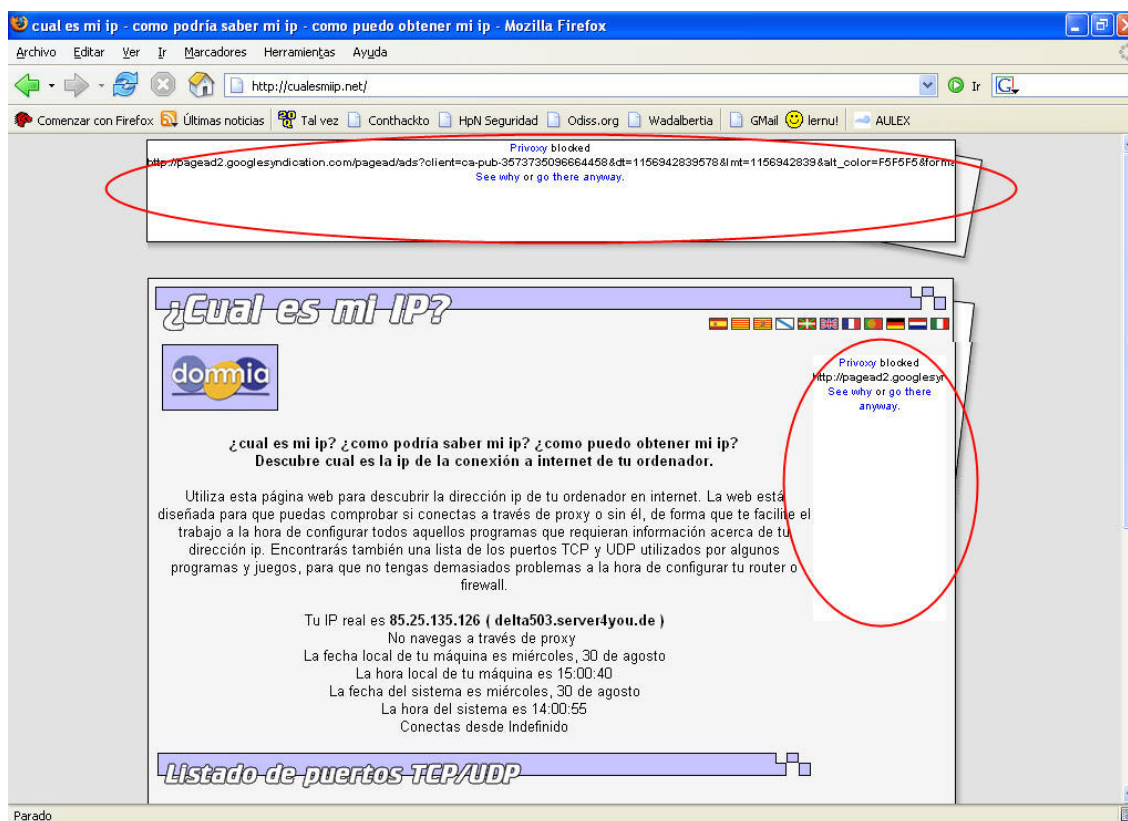


Imagen 27

Algunos quizá se pregunten la razón por la que indicamos también que Privoxy es un proxy SSL, FTP... en la configuración de Firefox. Pues bien, el motivo es porque si nos dejamos en blanco este espacio, y por alguna razón entramos en un servidor FTP, SSL..., nos conectaremos directamente, sin proxies, sin anonimato. Indicando que Privoxy no sólo es un proxy HTTP nos dará error (**Imagen 28**) y, aunque no podamos conectar a estos servicios, seguiremos siendo anónimos, que, en algunos casos, es preferible.

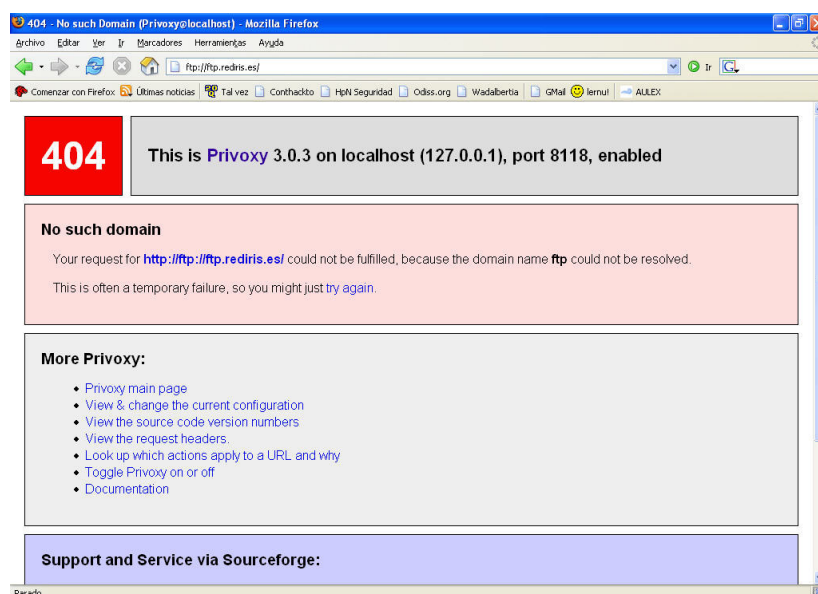


Imagen 28

5.- CONCLUSIONES Y DESPEDIDA

Y con esto terminamos por ahora con el maravilloso mundo del anonimato en Windows. En esta entrega de este pequeño “Taller de anonimato” solamente hemos *anonimizado* nuestro navegador web, pues es la forma más simple de demostrar que somos anónimos (mediante webs como Cualesmiip.net). Sin embargo, hemos trabajado también con el protocolo SOCKS y hemos visto cómo, al conectarnos a un FTP mediante un proxy http, daba error. Os animo a que intentéis *torificar* otras aplicaciones para Windows que tengáis, para que veáis cómo Tor sirve para mucho más que para la navegación web anónima.

Me dejo muchas explicaciones en el tintero; pero no os preocupéis, en la próxima entrega profundizaremos aún más en el tema del anonimato en Internet, pues ése es nuestro objetivo: ser **ANÓNIMOS EN LA RED**.

Continuará...

Por **Alejandro Sánchez Postigo** (también conocido como **aLeZX**)
Dedicado a mi caballito de mar

<http://www.alezx.odiss.org>
aLeZX.vb@gmail.com

