aLeZX

Anónimos en la Red

Segunda parte

Bastante tiempo ha transcurrido ya desde la liberación del primer artículo de "Anónimos en la Red". Para ser precisos, fue hace un año cuando ese texto fue publicado. Ya en aquel momento tenía escrito una gran parte del documento que tienes ahora mismo ante tus ojos, pero, finalmente, acabó siendo suprimido. Ninguno de los bocetos que escribí me satisfacían lo más mínimo. Hubo momentos en los que tuve prácticamente terminado todo el capítulo, pero no era suficiente; no superó el examen y, cansado, por falta de tiempo -y, también hay que reconocerlo, por falta de motivación e inspiración- casi abandoné la escritura de la Segunda Parte de Anónimos en la Red.

Sin embargo, recordé que en el primer título prometí que habría una segunda parte. Es por ello que finalmente lo terminé. No ha sido fácil encontrar el tiempo y las ganas necesarias para escribir este documento. Por eso espero que sea de vuestro agrado.

Sin más dilaciones, he aquí la segunda parte de *Anónimos en la Red*.

aLeZX

ÍNDICE

ANÓNIMOS EN LA RED
SEGUNDA PARTE

1.- INTRODUCCIÓN

En el anterior capítulo de Anónimos en la Red tratamos la teoría básica acerca de los proxies, así como su forma de uso. Trasteamos también con el programa Tor en el sistema operativo de Microsoft, Windows XP.

En esta ocasión, volveremos a tratar el tema de los proxies y Tor, aunque desde otra perspectiva.

Mejor me dejo de llenar la página con introducciones y preámbulos, y pasamos directamente a la práctica. Vamos a ello.

2.- ANTES DE EMPEZAR

Existe un magnífico post en los foros de Wadalbertia realizado por Vic_Thor que es de lectura imprescindible para continuar este documento. En él, Vic_Thor pone en entredicho el anonimato por parte de proxies (intenta averiguar si el cliente lo usa o no) y de Tor (analiza si nos conectamos usando Tor), además de enseñar otros muchos conceptos. He aquí el enlace: http://www.wadalbertia.org/phpBB2/viewtopic.php?t=2040

Si por casualidad aún no os habéis leído el documento (mal hecho por vuestra parte), ya sabéis que hacer. ¡Cerrad este PDF y leeos el artículo de Vic_Thor!

También considero altamente necesario haber leído la *Primera Parte de Anónimos en la Red*, ya que todos los términos tratados en el presente documento obviarán la explicación de los conocimientos que ya deberíais tener.

3.- TOR

3.1.- TOR EN GNU/LINUX

En la anterior ocasión trabajamos con Tor en Windows. Usar Tor en GNU/Linux no supone ningún misterio ya que existen paquetes para las distribuciones más comunes. Consistiría en dirigirnos a la página web http://tor.eff.org/download.html.es y desde allí descargarnos el paquete más adecuado o, simplemente, ver cómo proceder en la instalación. Normalmente no nos hará falta *torturarnos* compilando las fuentes nosotros mismos. Yo instalé Tor en mi distribución así:

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

Mediante este método nos quitaremos problemas de librerías, así como la instalación y configuración de otros programas útiles.

De todas formas, explico cómo compilar el programa a través de las fuentes para aquellas personas que usen una distribución para la que no existan paquetes precompilados (existen para las más usuales).

Antes de compilar Tor, debemos asegurarnos de que tenemos instaladas las librerías *libevent* y *zlib*, así como *openssl* (si estas librerías se instalan mediante paquete precompilados hay que incluir también las paquetes –devel de las mismas, si existen). Si no están instaladas, Tor no se compilará. Al final de este documento encontraréis las webs desde las que os podréis descargar estas librerías. Una vez asegurados de esto, procedemos a descargarnos las fuentes de Tor. Tras ello, compilamos el programa de la forma tradicional en Linux, tal que así:

```
$ tar xvfz tor-0.1.2.17.tar.gz
$ cd tor-0.1.2.17
$ ./configure --with-libevent-dir=/usr/local/lib --with-ssl-
dir=/usr/local/openssl
$ make
```

Y como *root*:

```
# make install
```

De la misma forma que hemos instalado Tor, también podría instalarse *Privoxy* (aunque no es estrictamente necesario). Desde http://www.privoxy.org podréis encontrar los paquetes precompilados para una gran cantidad de SOs (Windows, Linux, MacOS, Solaris...) y también las fuentes para compilarlo uno mismo, aunque la instalación mediante esta forma es algo más tediosa. No explicaré la instalación de Privoxy porque no quiero extenderme demasiado en este tema y porque no es obligatorio. Además, la instalación mediante paquetes precompilados es muy sencilla. Sólo debo comentaros que, tras la instalación de *Privoxy* (si es que lo instaláis) debéis configurarlo tal y como lo hacíamos en la *Primera Parte de Anónimos en la Red*. La única diferencia estriba en que el archivo a modificar será */etc/privoxy/config* o */usr/local/etc/config* (no explico los cambios que se deben realizar porque fueron detallados en el artículo anterior).

En este artículo omitiré la configuración de Tor (o de cualquier proxy) en Mozilla Firefox, ya que fue detallado hasta la saciedad en la *Primera Parte de Anónimos en la Red*.

Una vez instalado Tor en nuestro sistema, podremos ejecutarlo abriendo una terminal y ejecutando el comando “tor”. En la línea de comandos nos aparecerá la información del programa de forma semejante a como se nos mostraba en Windows. El modo de empleo básico de Tor es exactamente igual que el que ya fue tratado en la *Primera Parte (Imagen 1)*

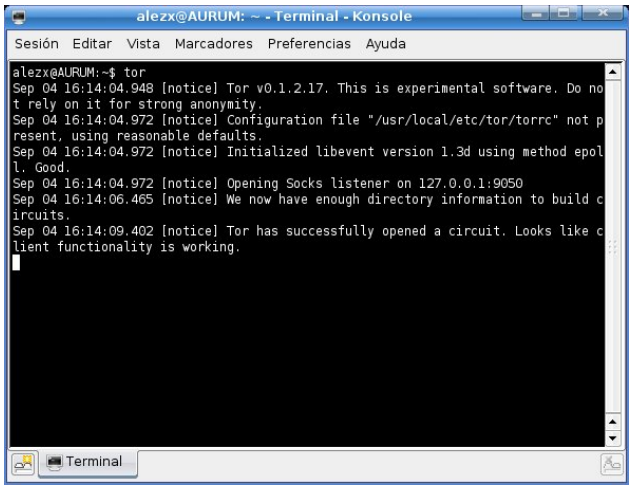

Imagen 1

3.2.- EXTENSIONES DE FIREFOX

Aprovechando que estamos instalando Tor de nuevo comentaré que existen algunas extensiones para el navegador web Mozilla Firefox que nos permitirán usar y dejar de utilizar Tor con un simple clic. Este complemento se denomina *TorButton* y puede ser descargado desde la siguiente dirección web: https://addons.mozilla.org/es-ES/firefox/addon/2275 *(Imagen 2)*. También existe otro *plugin* que podrá ser utilizado para cualquier proxy y no sólo con Tor: *SwitchProxy*. Lo podremos descargar desde aquí: https://addons.mozilla.org/es-ES/firefox/addon/125.

Tanto *TorButton* como *SwitchProxy* nos permitirán utilizar Tor (o cualquier otro proxy) con presionar un tecla del ratón. La ventaja de SwitchProxy es que podremos almacenar la configuración de varios proxies e ir seleccionándolos a nuestro gusto desde una lista desplegable.

La instalación de ambas extensiones no supone la mayor dificultad. Al hacer clic sobre el botón *"Instalar ahora"* se nos abrirá un cuadro de diálogo por medio del que podremos proceder a la instalación *(Imagen 3)*. En la ventana que nos aparece pulsaremos de nuevo en *"Instalar ahora"* y, para finalizar, en el botón *"Reiniciar Firefox" (Imagen 4)*. Las imágenes y explicaciones se aplican a la instalación del complemento *TorButton*, pero son igualmente válidas tanto para *SwitchProxy* como para cualquier otra extensión de Firefox.

Imagen 2

Imagen 3

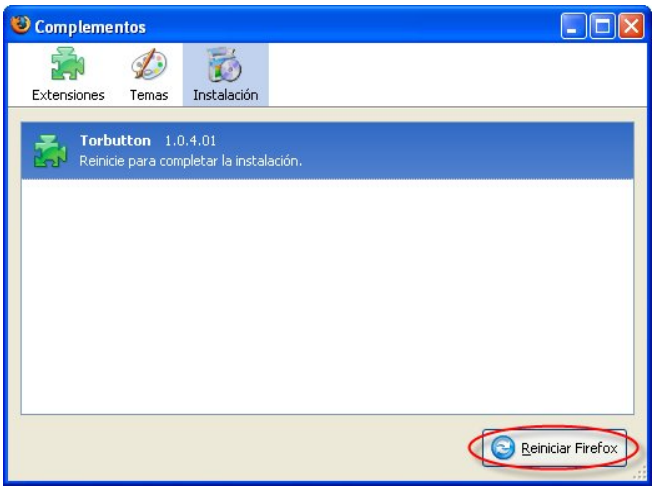

Imagen 4

Una vez instalada la extensión *TorButton* nos aparecerá en la barra de estado de nuestro navegador web Firefox el texto "Tor Disabled" *(Tor desactivado)*. Al pulsar sobre éste será sustituido por "Tor Enabled" *(Tor activado)*. Cuando activemos la extensión *TorButton* (debe estar en "Tor Enabled") podremos navegar anónimamente sin preocuparnos de cambiar la configuración proxy como hacíamos en el primer capítulo de *Anónimos en la Red (Imagen 5)*. Ni que decir tiene que para que esta extensión funcione Tor debe estar activo y funcionando.

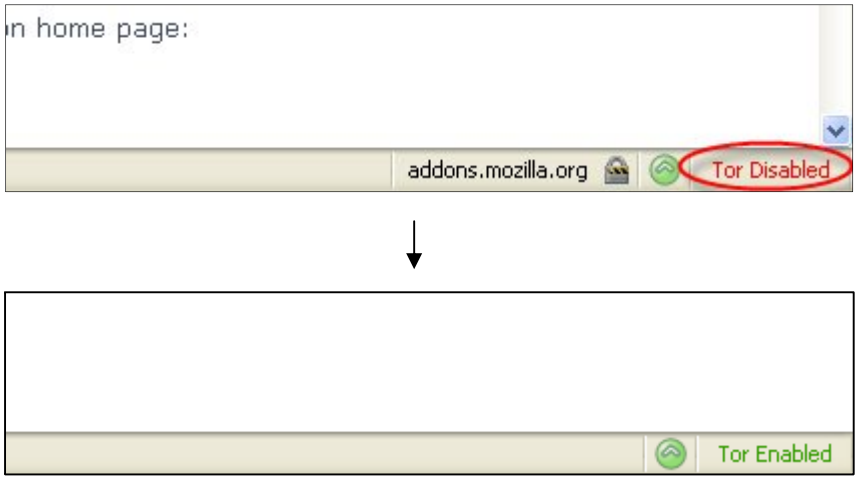

Imagen 5

Si Tor no estuviese ejecutándose, el resultado sería –como es de esperar- el de la *imagen 6*. Fijaos en que la extensión *TorButton* autoconfigura las *Opciones de Red* de nuestro Firefox para facilitarnos la tarea. Lo podéis comprobar (como vimos en la primera parte de esta serie de artículos) en *Herramientas – Opciones... – Red – Configuración...*

Por defecto, *TorButton* está configurado para usar Privoxy (entendiendo que éste se encuentra a la escucha del puerto por defecto 8118). Esto lo podemos modificar haciendo clic derecho en el texto "Tor Disabled/Enabled" de la barra de estado de Firefox y seleccionando *Preferences... (Imagen 7)* Desde esta ventana podemos, además de elegir usar o no Privoxy, establecer la configuración de nuestro Tor de forma manual. Teniendo en cuenta que podemos modificar esta configuración a nuestro antojo, podríamos usar *TorButton* para utilizar cualquier proxy o herramienta de anonimato en lugar de Tor.

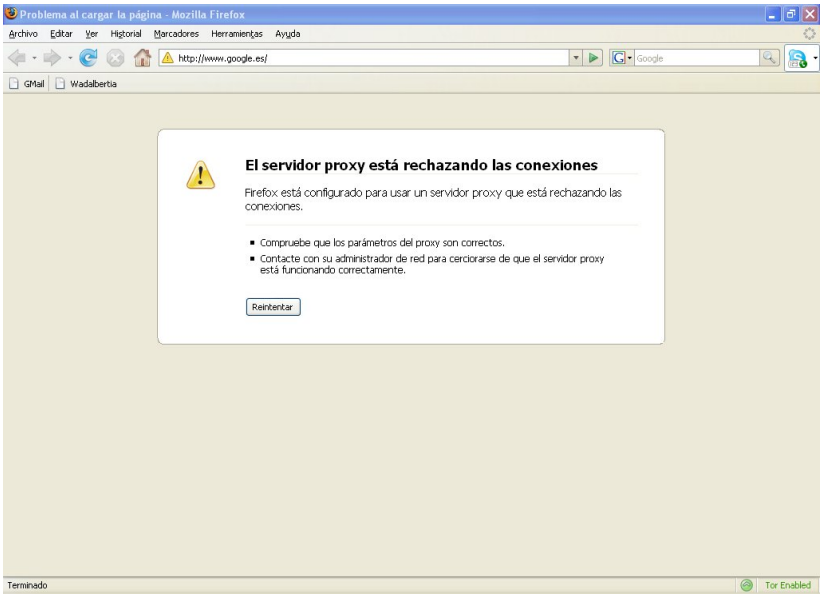

Imagen 6

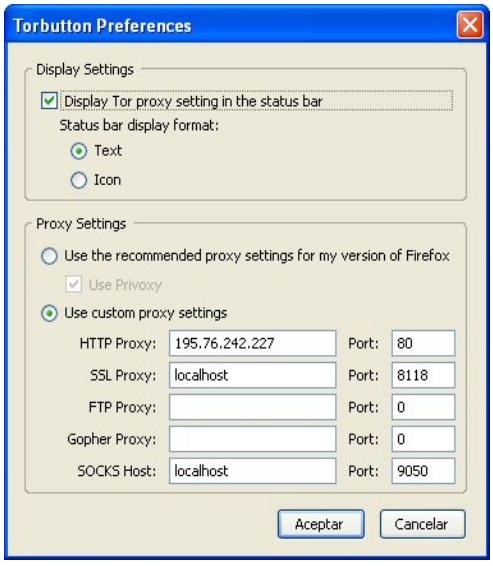

Imagen 7

Como iba diciendo al principio de este apartado, existe también otra extensión de Tor relacionada íntimamente con el anonimato que recibe el nombre de *SwithProxy* (el enlace de descarga ya fue especificado anteriormente). El método de instalación de este *plugin* no varía lo más mínimo con el de *TorButton* ni con el de ningún otro complemento para nuestro navegador Mozilla Firefox. Tras ser instalado, aparecerá una nueva barra de herramientas en Firefox *(Imagen 8)*. El uso es sumamente sencillo. Cada vez que queramos incluir la configuración de una nueva herramienta de anonimato o proxy, debermos pulsar el botón "Add", que nos mostrará un sencillo cuadro de diálogo en el que, tras seleccionar *Standard* nos abrirá una nueva ventana que, a estas alturas, ya tendríais que ser capaces de configurar solitos y sin el mayor inconveniente. La potencia de esta extensión radica en que podremos cambiar fácilmente entre los distintas configuraciones añadidas haciendo clic en su nombre dentro de la lista desplegable que existe junto a la palabra *Proxy:* en la barra de herramientas de *SwitchProxy*.

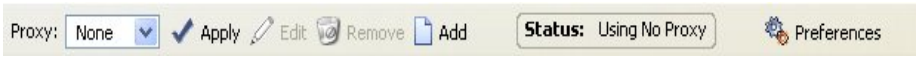

Imagen 8

3.3.- EL FICHERO DE CONFIGURACIÓN DE TOR: *torrc*

Vaya, no quería extenderme tanto como he hecho en un punto tan sencillo como era el anterior. No obstante, nunca viene de más.

A pesar de que en el artículo anterior no hablamos de la posibilidad de configurar Tor, éste cuenta con un archivo de configuración que nos permitirá modificar sus características para adaptarlas a nuestra necesidades y/o gustos. La situación de este fichero dependerá del SO (Sistema Operativo) que utilicemos y del modo que usásemos para instalar Tor. Así, podemos establecer las siguientes diferencias:

- Si instalaste el cliente Tor en un sistema operativo Microsoft Windows por medio del método que explicábamos en el capítulo anterior de *Anónimos en la Red*, el archivo de configuración (que recibe el nombre de *torrc*) se encontrará en *Inicio – Todos los programas – Tor - Torrc (Imagen 9)* o en *\Documents and Settings*\'Usuario'*Datos de programa**Tor*\.

- Si, por el contrario, instalaste Tor en Windows, pero mediante el paquete *Tor & Privoxy & Vidalia* (Vidalia es una interfaz gráfica para Tor) lo más probable es que *torrc* se sitúe en la carpeta correspondiente del Menú Inicio o en *\Documents and Settings*\'Usuario'*Datos de programa**Vidalia*\

- Si instalaste el cliente Tor en un sistema operativo GNU/Linux mediante un paquete precompilado, *torrc* seguramente esté en */etc/torrc* o en */etc/tor/torrc* o en *~/.tor/torrc*

- Si en lugar de usar un paquete precompilado utilizaste las fuentes para compilarlas tú mismo en el sistema UNIX que poseas, deberás copiar el fichero *torrc.example* del fichero */usr/local/etc* a */etc/tor* con el nombre *torrc*. Ése será el fichero que has de usa

Una vez que podamos acceder al archivo de configuración *torrc* lo abrimos con nuestro editor de texto plano preferido. La configuración de Tor que viene por defecto normalmente funciona sin ningún tipo de inconvenientes (como pudimos comprobar en la primera entrega de *Anónimos en la Red*); sin embargo, podemos realizar algunas modificaciones para, por ejemplo, añadirle funcionalidades.

Las líneas que comienzan por # son los comentarios. Para que no se tenga en cuenta algún "comando" del fichero basta con comentar esa línea (añadir un símbolo almohadilla [#] al comienzo de la línea). De las misma forma, para descomentar una línea simplemente habrá que borrar esa almohadilla (#).

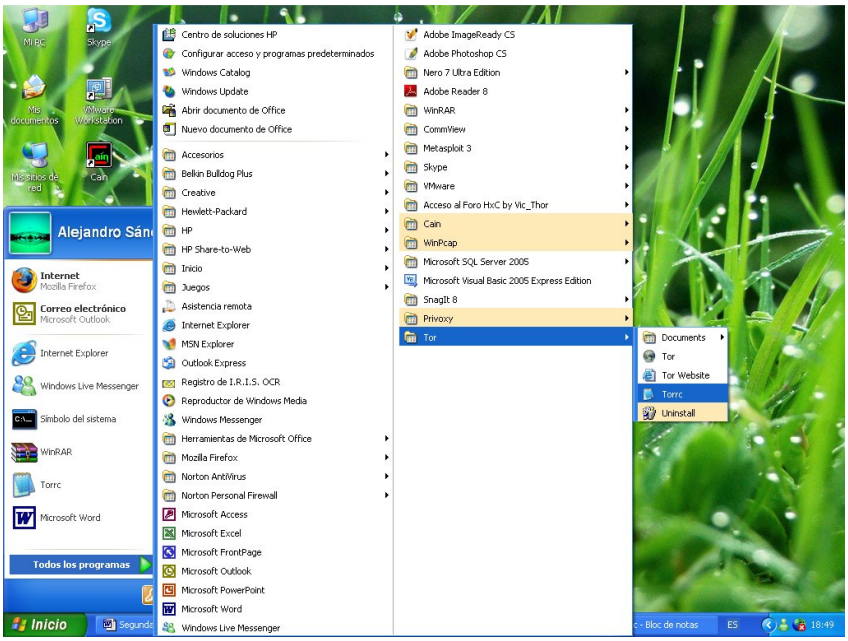

Imagen 9

A continuación detallaré algunas de las opciones de interés general:

- *SocksPort* indica el puerto en el que el cliente Tor estará a la escucha. Como ya deberíais saber, por defecto es el 9050

- *SocksListenAdress 127.0.0.1* nos muestra que el cliente Tor es sólo accesible desde nuestro propio ordenador y no desde Internet. Si cambiamos este valor y el anterior, entre otros, podremos convertir nuestro cliente Tor en un servidor, aunque no trataremos ese tema en este artículo.

- *#ControlPort 9051*, por defecto deshabilitado, indica a programas externos a Tor cómo deben usar éste para manejarlo. Un ejemplo de este tipo de programas es, por ejemplo, Vidalia.

- El resto de opciones no nos deberían importar por ahora ya que, en su gran mayoría, nos sirven para configurar servicios ocultos o para usar Tor como servidor (tema que no trataremos hoy; tal vez en otra ocasión).

3.4.- SELECCIONANDO LA RUTA DE TOR

Más de una vez me han preguntado cómo se puede forzar o cambiar el camino que sigue Tor para llevarnos hasta nuestro destino final. Aplicando la lógica es fácil darse cuenta de que, si reiniciamos Tor, cabe la posibilidad de que se cree un nuevo circuito. No obstante, esto no tiene por qué ocurrir así. Para solucionar este inconveniente podemos indicarle a Tor por qué nodo(s) debe entrar en la red, por qué nodo(s) debe salir y qué nodo(s) nunca debe usar.

En el fichero de configuración de Tor (*torrc*) podemos incluir las siguientes líneas:

```
entrynodes [nickname],[nickname],...
```

Nos permite especificar los nodos por los que entrar a la red Tor.

```
exitnodes [nickname],[nickname],...
```

Nos permite especificar los nodos por los que salir de la red Tor.

```
excludenodes [nickname],[nickname],...
```

Nos permite indicar los nodos que nunca deben formar parte de nuestro circuito.

A pesar de que las indicaciones dadas a Tor mediante *entrynodes* y *exitnodes*, Tor, cada cierto tiempo, cambiará la ruta. También la cambiará si por casualidad algunos de los nodos de entrada o salida que hemos especificado está caído o tarda mucho en responder. Sin embargo, si deseamos que el nodo indicado sea usado pase lo que pase (aunque esté inaccesible, por lo que no podremos conectarnos a él) debemos escribir en *torrc* las siguientes líneas:

```
StrictEntryNodes 1
```

Si queremos obligar el uso de los nodos de entrada

```
StrictExitNodes 1
```

Si queremos obligar el uso de los nodos de salida

Pero, ¿y si sólo queremos conectarnos a un nodo en concreto en un momento determinado y no siempre? ¿Tenemos que modificar el fichero *torrc* cada vez que queramos especificar por qué nodo entrar o salir?

La respuesta es clara: No. Podemos especificar el nodo por el que entrar o salir a la red directamente mediante la línea de comandos o, si lo que queremos es navegar anónimamente, indicándolo en la barra de direcciones de nuestro navegador (obviamente, esto último sólo es válido cuando vayamos a usar nuestro navegador web).

Para especificar esta información desde la línea de comandos, debes iniciar Tor en una shell de esta forma:

```
tor entrynodes [nickname]
```

Para indicar a Tor el nodo de entrada que debe usar durante esta conexión.

```
tor exitnodes [nickname]
```

Para indicar a Tor el nodo de salida que debe usar durante esta conexión.

```
tor entrynodes [nickname] exitnodes [nickname]
```

Para indicar a Tor ambas opciones.

Como decíamos antes, también es posible indicarle a Tor por qué nodo salir escribiendo en la barra de direcciones de nuestro navegador la siguiente línea, como si de la URL de la web que quisiésemos visitar se tratase:

```
http://[URL_de_la_web_a_visitar].[nickname].exit
```

Y a todo esto, ¿de dónde sacamos los *nicknames* de los servidores Tor? Pues de las siguientes páginas:

- http://lefkada.eecs.harvard.edu/cgi-bin/exit.py
- https://torstat.xenobite.eu/
- http://torstatus.kgprog.com/
- http://torstatus.blutmagie.de/
- http://tns.hermetix.org
- http://torstat.kleine-eismaus.de
- http://torstatus.torproxy.net

Veréis qué interesante... Vamos a entrar en una de las páginas que he citado, por ejemplo, la tercera. Una vez dentro vemos que el título de esta web es: *"TorStatus – Tor Network Status"* y lo que tenemos ante nuestros ojos no es más que una lista de nodos Tor, con su correspondiente *nickname*, nombre de host, IP, país, y una ingente cantidad de información. Vamos a analizar brevemente qué se nos nuestra.

En la parte superior de la web nos encontramos un recuadro que nos muestra nuestra IP y nos informa de si usamos o no Tor. Justo debajo otro recuadro nos enseña una leyenda con el significado de los colores.

La primera columna nos muestra la bandera del país en el que está situado el servidor Tor. *Router name* es el nombre (*nickname*) del nodo en cuestión. También se nos muestra el nombre del host, su dirección IP y el ancho de banda disponible, entre otra información. Como

veis, todo está muy bien estructurado. También son intersantes los iconos que observamos a mano derecha de la dirección IP. Al pasar el puntero del ratón por encima de ellos aparece la descripción de los mismos. Así, podremos ver el Sistema Operativo sobre el que corre el servidor Tor, si es un servidor que pueda usarse como nodo de salida o si se trata de un *Fast Server* (Servidor Rápido). Interesante, ¿verdad?

En la parte inferior de la web nos encontramos con algunas estadísticas y otra información de interés general. Si pulsamos sobre el *nickname* de algún nodo entraremos en otra útil información.

Lo mismo ocurre con el resto de páginas anteriormente citadas (son todas muy parecidas).

Y ahora, hagamos algunas pruebas :)

PRÁCTICAS

Vamos a practicar lo último que hemos visto en este apartado. El objetivo será seleccionar un nodo de Tor por el que salgamos y comprobemos que, efectivamente conseguimos salir a Internet a través de él.

En primer lugar, nos dirigimos a una de las páginas en las que podemos encontrar los nodos de Tor. Yo me meteré en http://torstatus.blutmagie.de/. Entre todos los nodos elegimos el que más nos plazca. Como queremos salir a través de él (la IP que quedará registrada será ésa) debemos buscar uno que tenga el icono de la puerta semiabierta (Nodo de salida). Seleccionaremos también uno que esté funcionando ahora mismo (color blanco) y, puestos a pedir, un *Fast Server* con un ancho de banda más que considerable. Con el fin de facilitarnos un poco la tarea de búsqueda, podemos aplicar filtros de ordenación de los nodos. Para ello nos desplazamos hasta la parte inferior de la web y lo configuramos como queramos. Por ejemplo, para que aparezcan los servidores Tor de arriba abajo en función del ancho de banda disponible lo podemos configurar como en la *imagen 10*. Tras seleccionar “Bandwidth” y “Descending” y hacer clic en “Apply Options” el resultado será semejante al de la imagen 11.

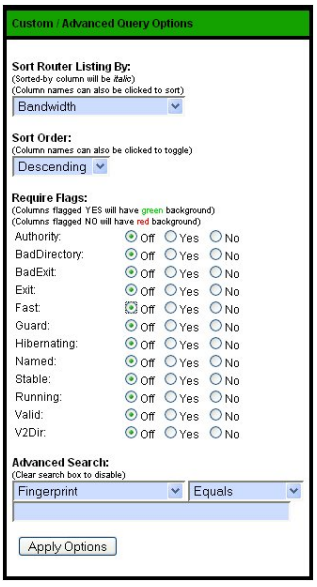

Imagen 10

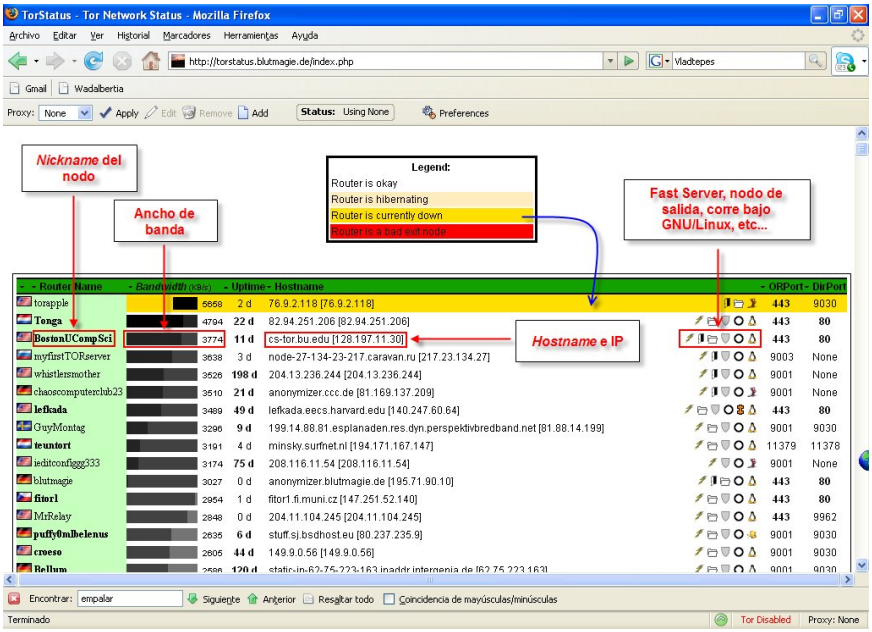

Imagen 11

Una vez elegido, abrimos a la shell del sistema y escribimos el comando necesario para que Tor se ejecute, usando como último nodo el que le especifiquemos. A estas alturas tú mismo debes saber qué comando escribir. Aún así puedes mirar la *imagen 12*.

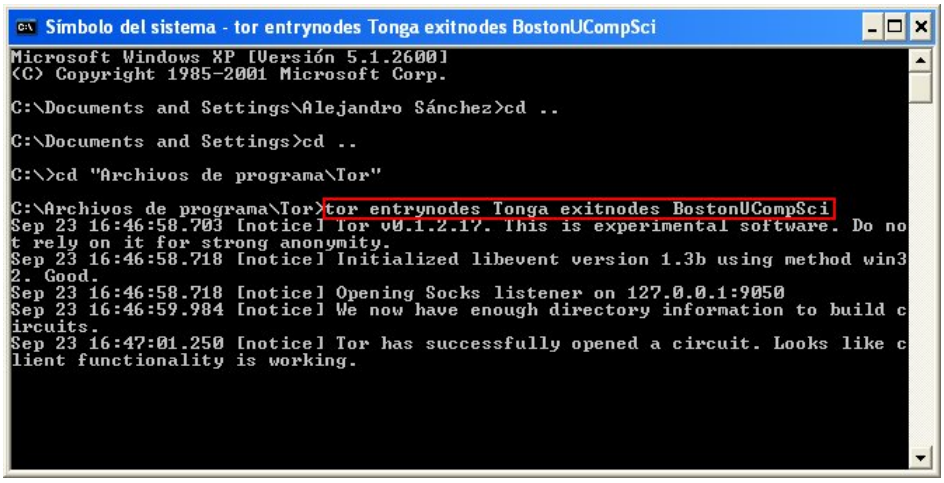

Imagen 12

Como ves, hemos salido a través de la IP seleccionada y, si cogiste un servidor rápido con un buen ancho de banda, seguro que la velocidad ha sido mucho más elevada de lo que estás acostumbrado. Podríamos haber hecho lo mismo modificando el fichero *torrc (Imagen 13)*

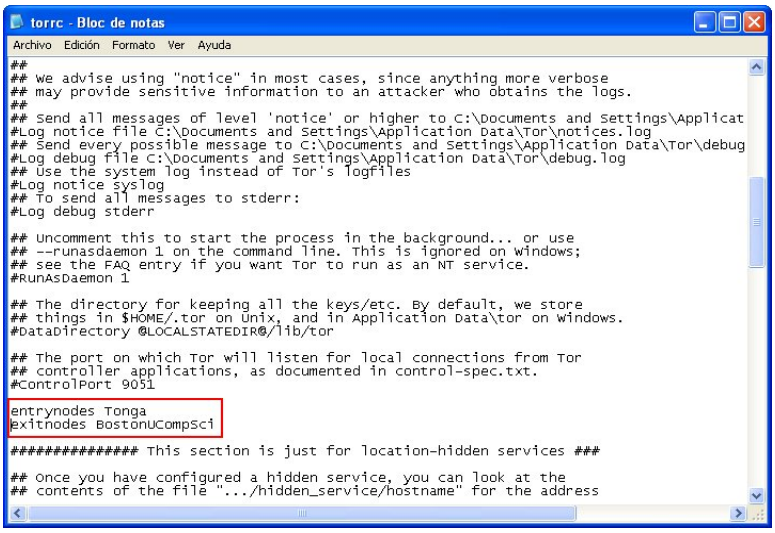

Imagen 13

En la *imagen 13* establecemos "Tonga" como nodo de entrada y "BostonUCompSci" como nodo de salida. Si nos fijamos bien en la *imagen 11*, "Tonga" no es un nodo de salida, por lo que nunca podría ser usado como tal.

Si especificase la opción StrictNodesExit o StrictNodesEntry como 1 y algunos de los servidores Tor indicados fallase, el resultado sería como el expuesto en la *imagen 14*.

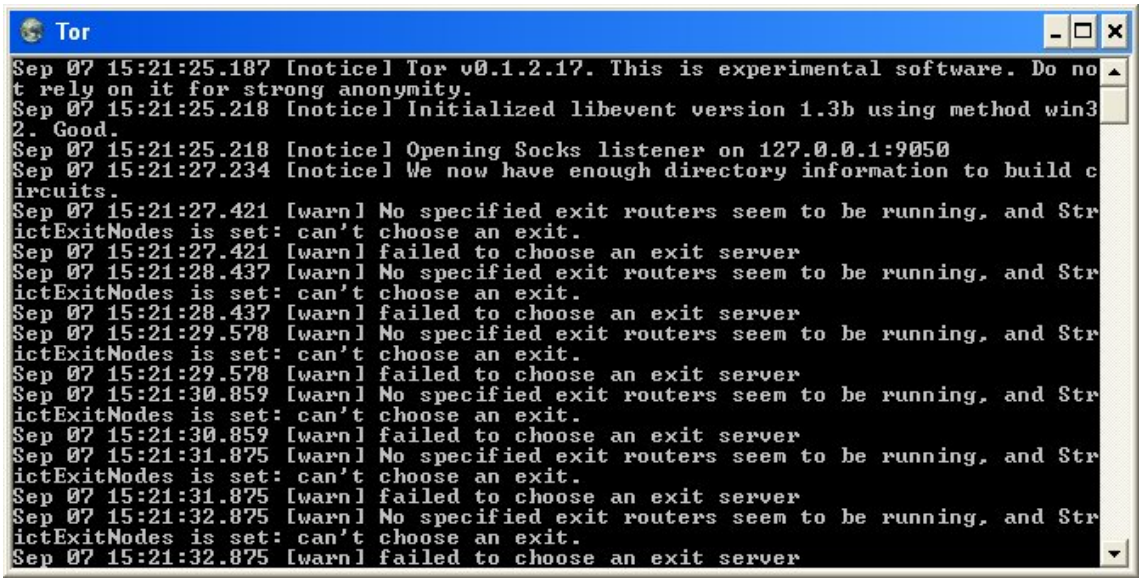

Imagen 14

Y ahora vamos a comprobar que cuando le indicamos el nodo de entrada realmente lo usa y no porque lo digo yo. Para la ocasión vamos a usar un esnifer. Yo usaré CommView para Microsoft Windows, vosotros podéis usar ése u otro cualquiera. Los linuxeros podrán usar Ethereal o WireShark. Al final de este documento incluiré los enlaces de descarga de los mismos. No es la finalidad de este documento explicar cómo instalar y configurar los esnifers, así que daré por sentado que sabéis utilizarlo y que lo tenéis totalmente funcional.

Lo primero que hacemos es iniciar el esnifer y hacer clic en el botón de esnifado (en CommView el símbolo de *play*). Inmediatamente después ejecutamos Tor, pasándole la información referente a los nodos de entrada mediante el fichero *torrc* y especificando *StrictEntryNodes 1* y *StrictExitNodes 1 (Imagen 15)*. Si no especificásemos estas dos opciones, la ruta establecida por Tor sería inicialmente la escogida por nosotros, pero luego podría ser cambiada (por motivos de seguridad). Seguidamente, comenzamos a navegar un poco por Internet y, si todo ha ido bien, nuestro esnifer comenzará a mostrar los paquetes de conexión entre nuestro PC y el servidor Tor. ¿Hacia dónde van dirigidos los paquetes enviados por nuestro cliente Tor? *(Imagen 16)* Correcto, a la dirección IP del nodo seleccionado como "*de entrada*".

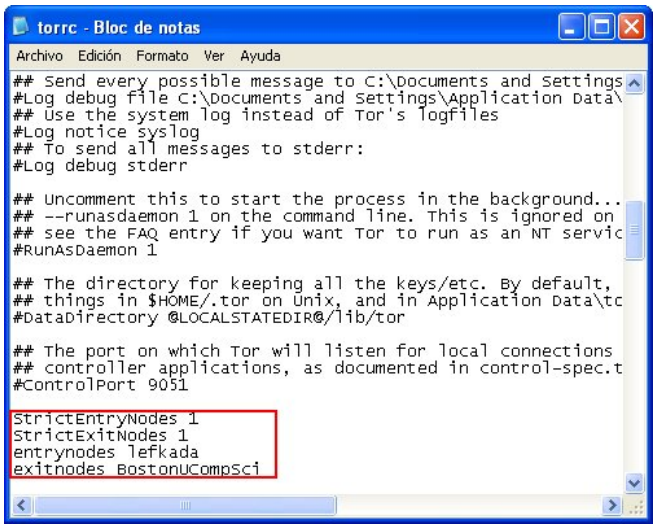

Imagen 15

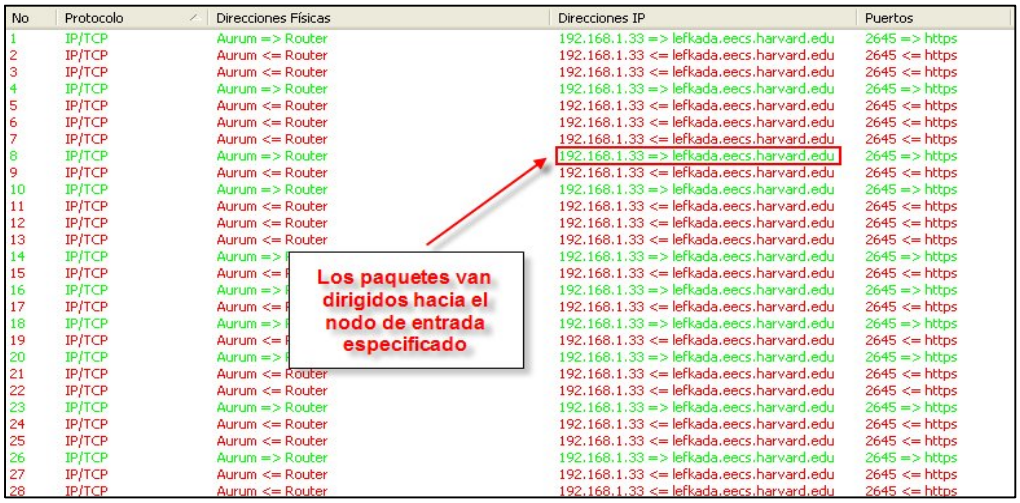

Imagen 16

De esta forma hemos aprendido a "manipular" en cierto modo el circuito que se crea para realizar nuestra conexiones "anónimas" (podemos elegir el país, el ancho de banda de los nodos...) y además hemos comprobado que es cierto.

3.5.- FREECAP (MÁS DE PROXIES)

Hablábamos en la Primera Parte de Anónimos en la Red de la existencia de programas que nos permiten *anonimizar* cualquier aplicación aunque ésta no incluya esa posibilidad entre sus opciones. Existen múltiples programas para ello, tanto para Windows como para GNU/Linux y otros sistemas operativos.

En Microsoft Windows, yo elegiré el programa FreeCap. ¿Por qué? Por varios motivos: nos permite establecer cadenas de proxies (de las que ya hablamos en la primera parte del presente documento), trabaja con varios tipos de proxies (HTTP-CONNECT, SOCKS4, SOCKS5), y es Software Libre (a diferencia del otro programa, también muy conocido: SocksCap)

Esta aplicación redirecciona hacia el servidor proxy indicado las peticiones TCP o UDP (estas últimas sólo por medio de proxies SOCKS) que hagan nuestros programas.

Como podemos deducir, podremos utilizar estas aplicaciones tanto con Tor como con cualquier otro proxy de las características citadas (u otro programa *anonimizador* que actúe como tal)

En primer lugar, nos descargamos el programa de la siguiente web: http://www.freecap.ru/eng/ y hacemos clic en el botón "*Download*" *(Imagen 17)*

Imagen 17

En la página que nos aparece hacemos clic en el primer *"Download program!"*, con lo que nos podremos descargar el programa sin problemas. Una vez que tengamos el fichero en nuestro PC, lo ejecutamos. Seguimos los pasos tradicionales para instalar cualquier programa en

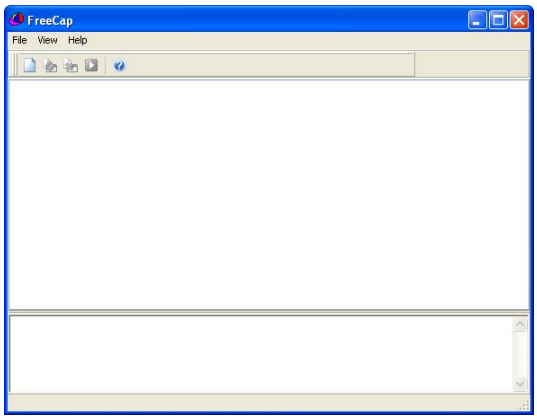

Imagen 18

Windows (*Next – Next – Next – Install – Finish*). Terminada la instalación, ejecutamos *FreeCap (Imagen 18)*

La ventana principal de *FreeCap* es muy simple, como pudimos comprobar en la imagen anterior. Lo primero que deberemos hacer es configurar el programa; para ello nos dirigimos a *File – Settings (Imagen 19)*

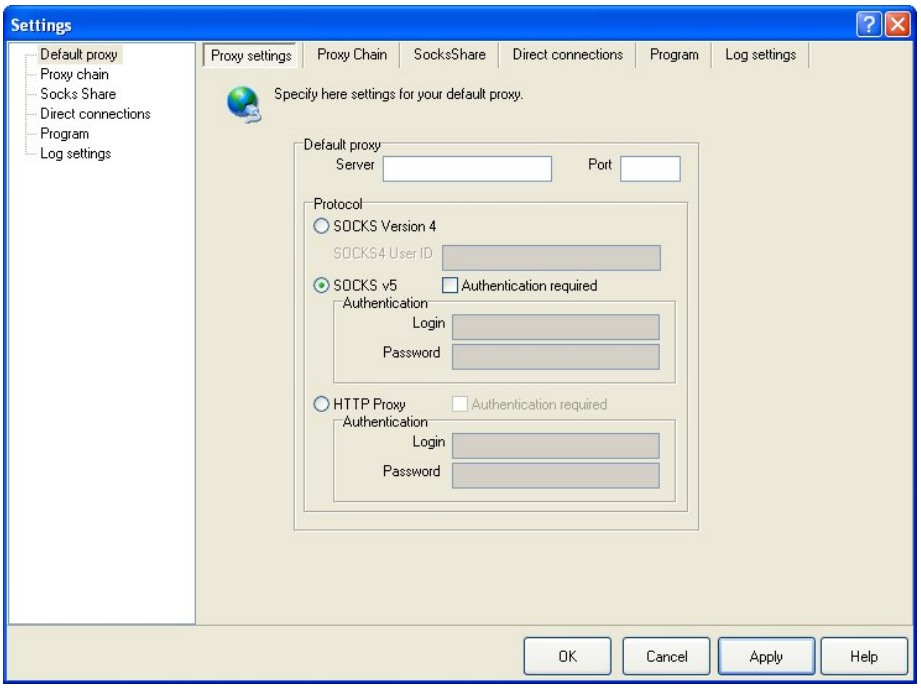

Imagen 19

En la ventana que nos surge a continuación tenemos que especificar el servidor proxy que vayamos a utilizar. A estas alturas deberíais estar completamente capacitados para configurarlo solitos (de hecho, cualquier persona debería estar capacitada sin ningún tipo de ayuda, ya que todo está muy clarito y estructurado). Arriba, donde pone *"Server"* escribimos la dirección del proxy y en *"Port"*, el puerto. Lo mismo en la sección "*Protocol*" (Protocolo). Si buscamos los proxies por Internet tal y como hicimos en la *Primera Parte de Anónimos en la Red*, sabremos perfectamente el protocolo que utilizará el proxy elegido (normalmente nos informará de ello la propia web de la que "extraigamos" los datos del proxy). ¿Y si utilizamos Tor? Pues, como servidor, nuestro propio PC, es decir, 127.0.0.1, y, como puerto, el que venga indicado en el fichero *torrc* de Tor (por defecto, 9050). También deberemos señalar el protocolo SOCKS v5. Con esto tendremos configurado el programa y, si los proxies funcionan bien, será totalmente funcional.

No me gustaría acabar esto sin comentar antes la pestaña *"Proxy Chain" (Imagen 20)*. Recordáis que en la primera parte de este documento tratamos teóricamente las cadenas de proxies, pero no tuvimos el placer de trabajar con ellas en la práctica. Mediante este programa podremos encadenar muchos de los proxies que encontremos por la Red. Siguiendo con la facilidad y lo intuitivo del programa, sólo tendremos que darle al botón "*Add*". La ventana que nos saldrá a continuación es tan obvia que me niego a explicarla *(Imagen 21)*. Cuantos más proxies añadáis mediante el botón "*Add*", más proxies constituirán la cadena, pero, eso sí, a mayor seguridad, menor velocidad de conexión. Todo esto ya fue explicado teóricamente en el primer capítulo.

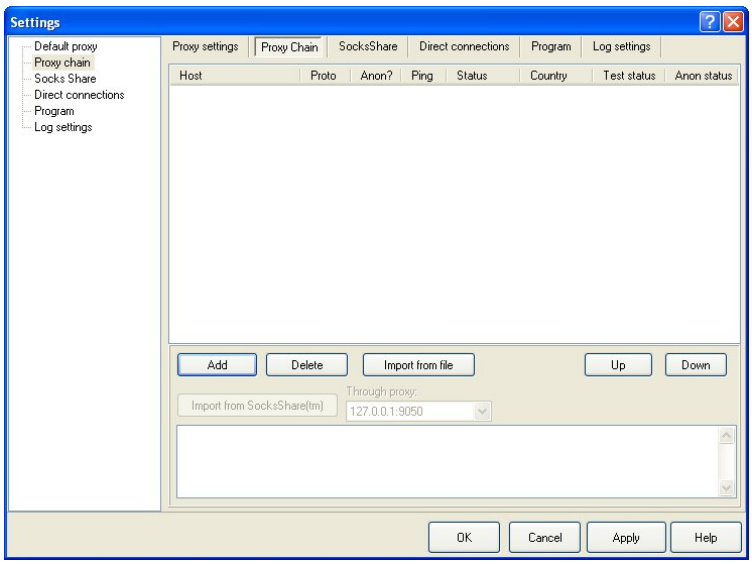

Imagen 20

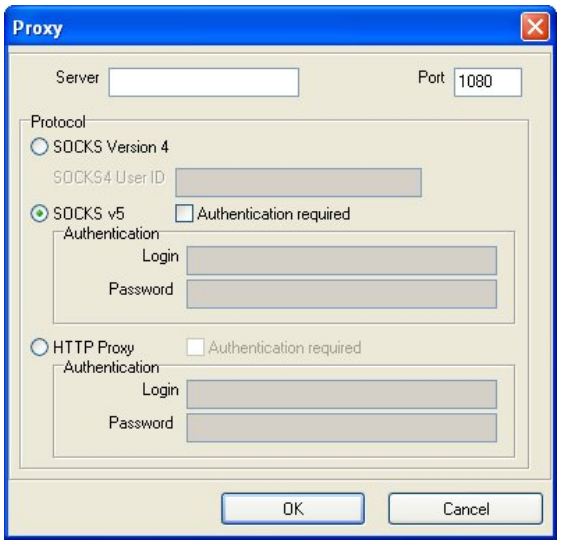

Imagen 21

El resto de opciones no las explicaré porque no son indispensables para este documento y sólo servirían para engordarlo. Además, son muy fáciles de entender. Sirven para que se muestren *logs*, para que se ejecute como servicio,... Ya vosotros vais mirando, si queréis.

Volvamos a lo nuestro. Como ya estamos hartos de *anonimizar* el navegador web, vamos a dar anonimato a otro programa, por ejemplo, un cliente IRC. En mi caso *anonimizaré mIRC* (enlace de descarga al final del documento), si bien, en principio no debería de haber ningún problema si deseáis dar anonimato a cualquier programa que trabaje con TCP (o UDP dependiendo del proxy que uséis). Digo en principio porque hay aplicaciones TCP que no han pasado a través del proxy aun usando *FreeCap* cuando realizaba mis pruebas.

Yo utilizaré Tor como proxy. En primer lugar, ejectuamos Tor como ya sabemos. Seguidamente, abrimos el programa *FreeCap*. En la ventana principal del programa, hacemos clic en el icono "*New application*" *(Imagen 22)*. En la ventana "Profile" que nos aparece indicamos los siguientes datos:

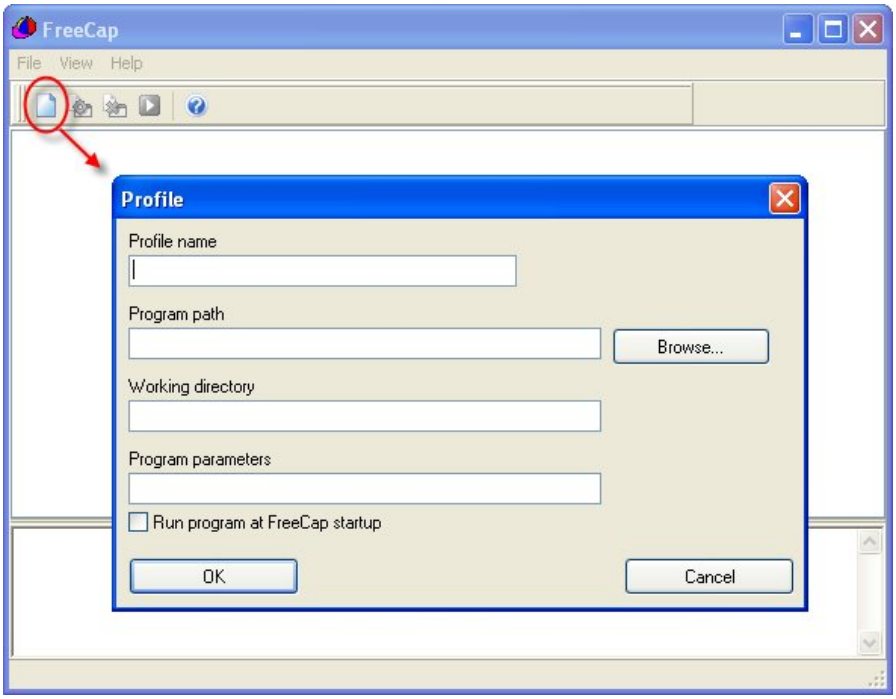

Imagen 22

- *Profile Name*: El nombre que nos dé la gana (simplemente servirá para identificar el programa).
- *Program Path:* Ruta del programa. Podemos buscarlo a través del botón "Browse..."
- *Working directory:* Directorio donde se encuentra instalado el programa (se rellenará sólo)
- *Program parameters:* Nos permite indicar parámetros con los que se debe ejecutar el programa (normalmente para aplicaciones en modo texto).
- *Run program at FreeCap startup:* Lo señalamos si queremos que el programa añadido se cargue siempre cada vez que ejecutemos *FreeCap*.

Así es como yo dejé *FreeCap* para su uso con *mIRC*: *(Imagen 23)*

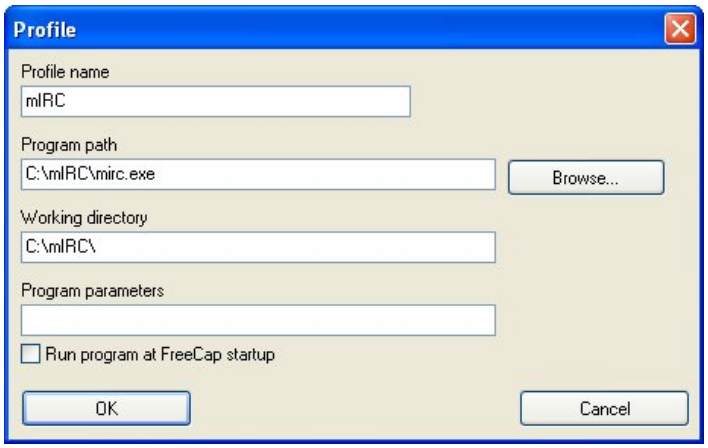

Imagen 23

Una vez hecho todo esto, en la ventana principal de *FreeCap* aparecerá algo tal que así: *(Imagen 24)*.

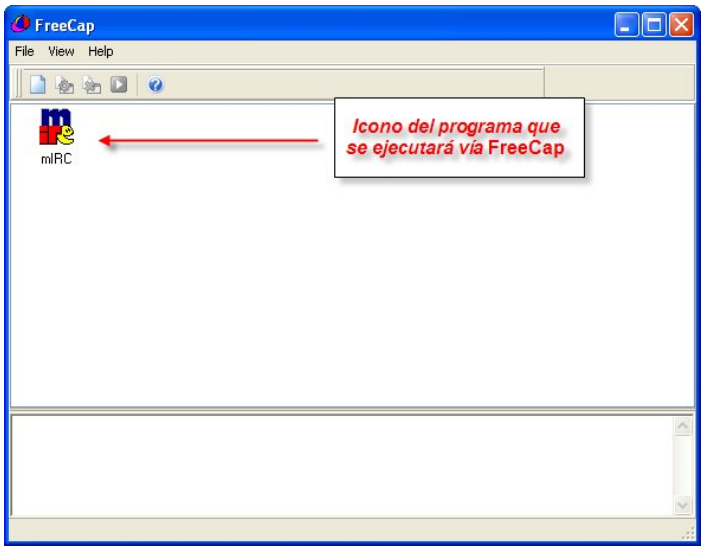

Imagen 24

Ahora podemos optar por ejecutar mIRC anónimamente (vía *FreeCap*) o de forma normal. Para ejecutarlo con algo de anonimato hacemos clic en el icono situado dentro de la ventana de *FreeCap*.

Inmediatamente nos surgirá la ventana de mIRC (o el programa que estemos usando). Si os fijáis en la parte superior de mIRC podemos leer el texto: “mIRC via FreeCap”. Bueno, nos conectamos a cualquier servidor (en mi caso entro en el canal #wadalbertitas de irc.irc-domain.org). Ahora hacemos un */whois [nuestro_nick].* Y... ¿ésa es nuestra IP? ¡Nooo! Es la IP del proxy elegido. De esta forma ya hemos conseguido un mínimo de anonimato *(Imagen 25)*.

Aunque mIRC permite entre sus opciones el uso de proxies, nos puede resultar mucho más sencillo el uso de *FreeCap*.

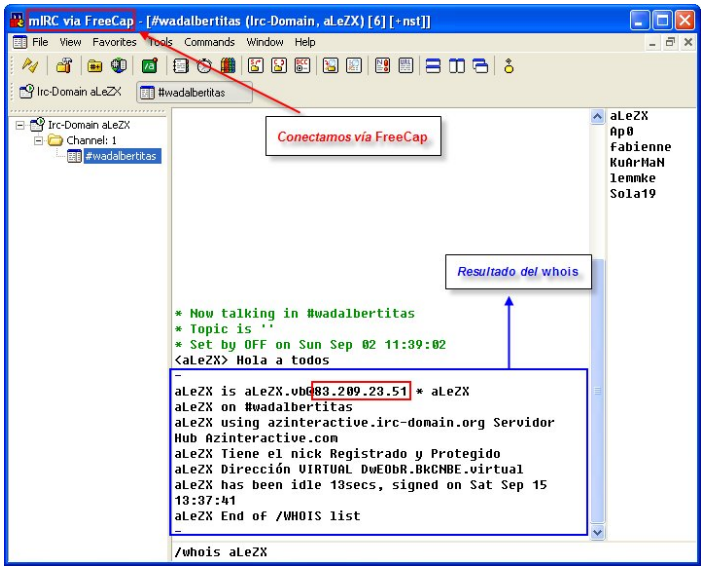

Imagen 25

En GNU/Linux, si instalamos Tor a través de los paquetes precompilados, se instalaría también el programa *tsocks*. Con él, podremos conseguir resultados similares a *FreeCap*, y además, podremos utilizar la herramienta *torify* que nos permitirá hacer pasar por Tor cualquier programa basado en TCP (*Tor-ificar*)

5.- CONCLUSIÓN FINAL, OPINIÓN PERSONAL Y DESPEDIDA

El anonimato en Internet no existe. Nunca ha existido. Podemos usar métodos que nos permitan "parecer" anónimos, pero ¿valen para algo estas técnicas?

A estas alturas habréis leído el artículo publicado por el compañero Vic_Thor en las extensas tierras wadalbertitas. Mediante sencillos *scripts* podemos conseguir que una página web detecte si llegamos a ella "limpios" o a través de un proxy o Tor. Si bien es cierto, esos *scripts* se puede "saltar", pero nunca, nunca se podrá conseguir un anonimato definitivo.

Hablar de anonimato es entrar en un debate sin fin. Yo, como escritor de artículos de este tipo, podría decir que todo lo explicado nos da anonimato, pero mentiría. Nos da algo de seguridad, suficiente para las tareas más comunes, así como para saltarnos algunos tipos de protecciones (podremos cambiar de IP, pensad lo que nos ofrece esto), pero, si verdaderamente quisiésemos hacernos los *superhackers-malos-malísimos*, la seguridad es siempre completamente escasa.

Por ejemplo, navegando por la web uno se encuentra con un post de Kriptópolis como este: http://www.kriptopolis.org/tor-parcheado-adios-al-anonimato . Siempre hay que tener en mente que programas como Tor, JAP,... se basan en un anonimato proporcionado por terceros. ¿Hasta qué punto podemos fiarnos de éstos? Depende de para qué queramos el anonimato, pero es indudable que, por mucho que nos aseguren que somos realmente anónimos, nunca podremos estar 100% seguros.

Sin embargo, el mundo del anonimato en la Red es mucho más amplio que lo expuesto en éste y el anterior documento. En ellos se incluye una ínfima parte dentro de la increíble extensión de este campo (al igual que en todos los ámbitos de la informática). El programa Tor da mucho más juego, existen otras herramientas de anonimato, técnicas totalmente distintas, *remailers* anónimos, ... Vamos, para aburrirse.

Por lo pronto, y para continuar con el programa Tor sería interesante que instalaseis la herramienta Vidalia. Esta herramienta crea un archivo de configuración de Tor (torrc) en este directorio (si nos referimos a Windows): *C:\Documents and Settings\'Usuario'\Datos de programa*\. Este archivo de configuración es un tanto especial, ya que tiene la línea *ControlPort 9051*, lo que nos permitirá usar programas de Control de Tor (en este caso, Vidalia) por medio del protocolo de control de Tor. También es adecuado probar Tor en GNU/Linux, junto con la herramienta *Torify* (recomiendo instalar Tor mediante los paquetes precompilados, ya que de este forma nos resultará mucho más fácil). Y, en definitiva, trastead todo lo que podáis. Indagad. Mirad otros programas, otras técnicas, otros métodos de anonimato. En definitiva, aprended.

Y de esta forma me despido. Espero volver a veros pronto en artículos como éste o de otra temática. Y recordad: EL ANONIMATO TOTAL NO EXISTE.

Enlaces de descarga

Tor: http://tor.eff.org/download.html.es
Librería OpenSSL: http://www.openssl.org/
Librería Libevent: http://monkey.org/~provos/libevent/
Librería Zlib: http://www.zlib.net/
Extensión TorButton: https://addons.mozilla.org/es-ES/firefox/addon/2275
Extensión SwitchProxy: https://addons.mozilla.org/es-ES/firefox/addon/125
Vidalia: http:/vidalia-project.net
Ethereal: http://www.ethereal.com/download.html
CommView: http://www.tamos.com/download/main/
FreeCap: http://www.freecap.ru/eng/?p=download
mIRC: http://www.mirces.com/

aLeZX (Alejandro Sánchez Postigo)
aLeZX.vb@gmail.com
www.alezx.odiss.org
www.alezx.wordpress.com