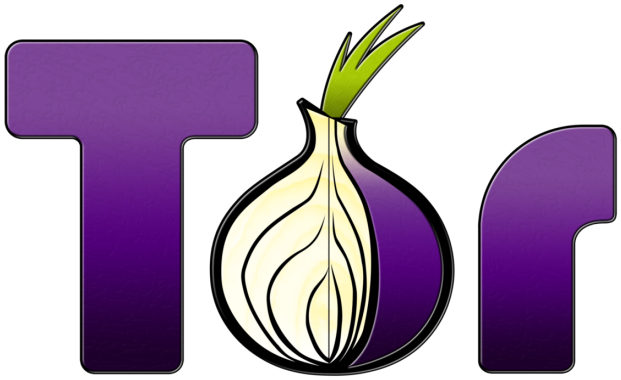
Aspectos Técnicos de la red TOR



Integrantes: Victor Arredondo

Roberto Caro

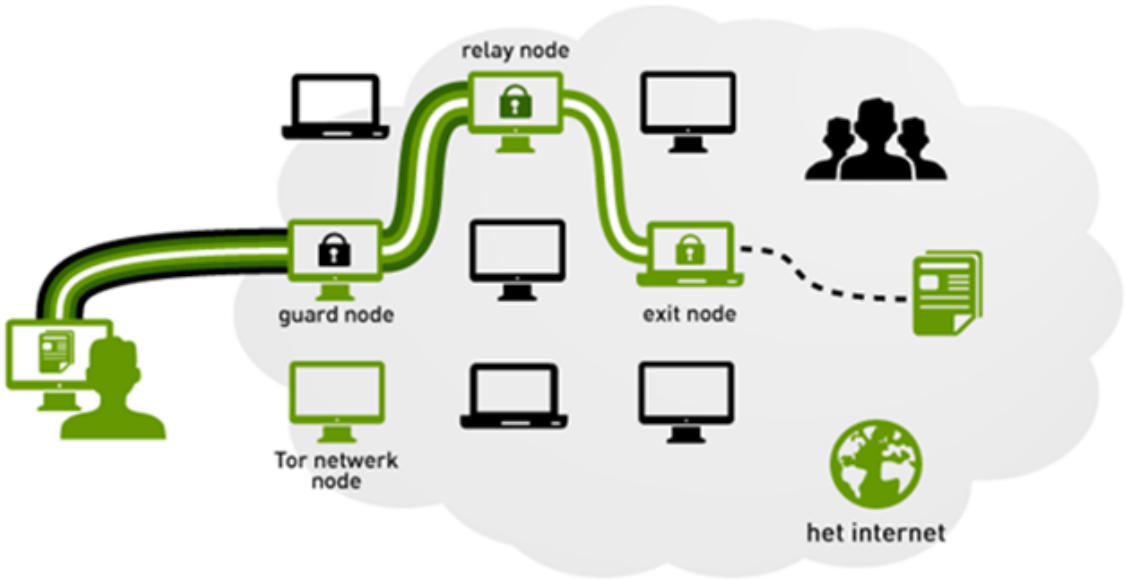
Introducción:

En la navegación por internet, los usuarios pueden sentirse inseguro en cuanto a los contenidos que navega y sobre la confidencialidad de sus comunicaciones con sus pares. Entre diversas formas de ocultar y/o proteger la información que uno ve y utiliza de internet, existe la red TOR.

Las características que ofrece este software libre implican la encriptación de los datos entre dos routers de tors, los cuales se encargan de rutear la información solicitada por el cliente de modo de que el camino entre los routers formados por la red de tor, esté completamente encriptado, garantizando el anonimato en la red.

La red tor:

La red de tor, la cual es una aplicación de código abierto que funciona sobre la internet mediante comunicaciones TCP, nos permite optar por elegir una ruta por la cual nuestro mensajes al salir, no podrán identificar el usuario a menos que este envíe deliberadamente su información privada, por lo que también se aconseja usar https para encriptar el contenido. La red tor está compuesta por servidores como si fueran router de un circuito virtual, para que al salir no se conozca efectivamente la dirección origen real sino una interna de lared, estos servidores generalmente son donaciones de cierto ancho de banda para esta red por su importancia a mantener el anonimato, estos servidores nodos son llamados nodo de guardia con los cuales accedemos a la red tor, los nodos intermedio o relay, y el nodo de salida por donde sale nuestro mensaje sin las encriptaciones que se realizan dentro de la red para hacer más segura la anonimidad.



Por qué usar TOR:

- Proteger la comunicación de corporaciones extrañas.
- Proteger la privacidad de marketing innecesario y de ladrones de identidad
- Acceso a información prohibida en ciertos países o culturas.
- Creen ser vigilados

Interfaces de acceso a la red de tor:

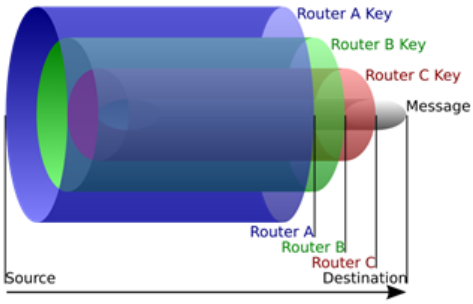
1. **Vidalia**: Es una interfaz gráfica de usuario (GUI) multiplataforma para controlar Tor, construida usando el Qt. Permite al usuario iniciar, detener y ver el estado de Tor, monitorizar el uso de ancho de banda, vista, filtrar y buscar mensajes de registro y configurar algunos aspectos de la Tor. Vidalia también hace más fácil contribuir a la red Tor, ayudando a que el usuario que lo desea configure un servidor Tor.
Otra característica destacada es el mapa de la red Tor, que permite al usuario ver la ubicación geográfica de los servidores de la red Tor, así como por donde está pasando el tráfico de la aplicación del usuario.

2.**Tor Browser**: Es un navegador configurado para funcionar con el programa de tor embebido, de ésta forma la conexión con las redes de tor se realiza en el mismo navegador. Es una versión modificada de firefox, la cual se adapta para usar las funciones de tor, también permite que mediante el puerto asignado, el cliente se comporte como un relay.

3. **Linux Tails**: (The Amnesic Incognito Live System) Sistema operativo basado en debian, linux. Su fin es preservar la privacidad y al anonimato, dado que todas sus conexiones son forzadas a usar tor y conexiones no anónimas son bloqueadas.

4. **Orbot**: Aplicación en android para poder utilizar la red de tor en dispositivos android.

Funcionamiento de la RED de tor : Encriptación



Cada servidor de la red tor es usado como router, para emular un circuito virtual, en donde los servidores solamente conocen las direcciones de los otros dos servidores adyacentes en el circuito, sin tener las direcciones fuente-destino reales como los encabezados típicos, y por lo tanto desconoce la estructura general de la conecciones.
Los servidores encriptan sus mensajes entre ellos,teniendo distintas encriptaciones para cada enlace, y es el usuario origen el que efectivamente conoce las encriptaciones necesarias para enviar los mensaje y tiene el conocimiento además de los nodos utilizados (por defecto son 3 nodos), mensajes los cuales son enviados muchas veces encriptados desde el usuario origen, y por cada enlace se van descriptando o descascarando como si fueran las capas de una cebolla, de donde proviene el nombre de TOR (The Onion Route).

Comunicación entre Onion Routers:

Las conexiones entre los dos repetidores Tor, o entre un cliente y un relay, usan el protocolo TLS/SSLv3 para la autenticación y el cifrado de enlace. Todas las Implementaciones deben apoyar el conjunto de cifrado SSLv3 "SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA", y es debiesen apoyar TLS CipherSuite "TLS_DHE_RSA_WITH_AES_128_CBC_SHA" si está disponible.

Hay tres formas de realizar un handshake TLS con un servidor Tor. en la primera forma, "certificates-up-front", el iniciador y respondedor envía una cadena de dos certificados como parte de su inicial apretón de manos. (Esto se apoya en todas las versiones de Tor.) En el segundo manera, "renegotiation", el que responde proporciona un único certificado, y el iniciador realiza inmediatamente una renegociación TLS. (Esta es soportada en Tor 0.2.0.21 y más tarde.) Y en la tercera forma, "in-protocol", la renegociación TLS inicial se completa, y el partes bootstrap sí mismos para la autenticación mutua a través del uso de la Protocolo Tor sin más protocolo de enlace TLS. (Esto se apoya en 0.2.3.6-alpha y posteriores.)

certificates-up-front

En "certificates-up-front", el iniciador de conexión siempre envía una cadena de dos certificado, que consiste en un certificado X.509 utilizando un clave pública de conexión a corto plazo y un segundo X.509, con firma certificado que contiene su clave de identidad. La otra parte envía un parecido cadena de certificados. El ClientHello del iniciador no debe incluir ningun conjuntos de cifrado que no sea:

TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

renegotiation

En "renegotiation" el iniciador de conexión envía ningún certificado, y el respondedor envía un certificado único de conexión. Una vez que las negociaciones TLS se han completado, el iniciador renegocia el apretón de manos, con cada parte que envía una cadena de dos certificados como en "certificates-up-front".

ClientHello del iniciador debe incluir al menos un conjunto de cifrado no en la lista de arriba - así es como el iniciador indica que se puede manejar este handshake

in-protocol

En "in-protocolo" (también conocido como "el v3 apretón de manos"), el iniciador envía ninguna certificados y la respondedor envía un certificado único de conexión. La elección de los conjuntos de cifrado deben estar como en un apretón de manos "renegociación". hay además, un conjunto de restricciones sobre el certificado de conexión, que el iniciador puede utilizar para aprender que el apretón de manos en el protocolo está en uso. Específicamente, al menos una de dichas propiedades deberá ser verdadera del certificado:

- El certificado es autofirmado
- Algunos componente que no sea "commonName" se ponga en el asunto o DN emisor del certificado.
- El commonName del sujeto o emisor de los extremos de certificados con un sufijo que no sea ". net".
- Módulo de la clave pública del certificado es de más de 1024 bits

El iniciador envía entonces una célula VERSIONS al respondedor, que luego responde con una célula VERSIONS ; que luego han negociado un Tor versión de protocolo. Suponiendo que la versión que negocian es 3 o superior (los únicos que se especifican para el uso con este apretón de manos en este momento), el respondedor envía una célula CERTS, una célula AUTH_CHALLENGE, y una NETINFO al iniciador, que puede enviar ya sea CERTS, autenticar NETINFO si quiere autenticar, o simplemente NETINFO si no lo hace.

Transporte de Datos

Cell Packet : Unidad básica de comunicación entre OP y OR.Utilizadas para establecer los tipos de comunicación ó terminarla, junto con distintas opciones de acuerdo al tipo de handshake utilizado.

Opciones de las celdas para comunicación más usadas:

- CERTS
- VERSIONS
- AUTHENTICATE
- AUTH_CHALLENGE
- NETINFO

Verificación de los relay de tor con Wireshark

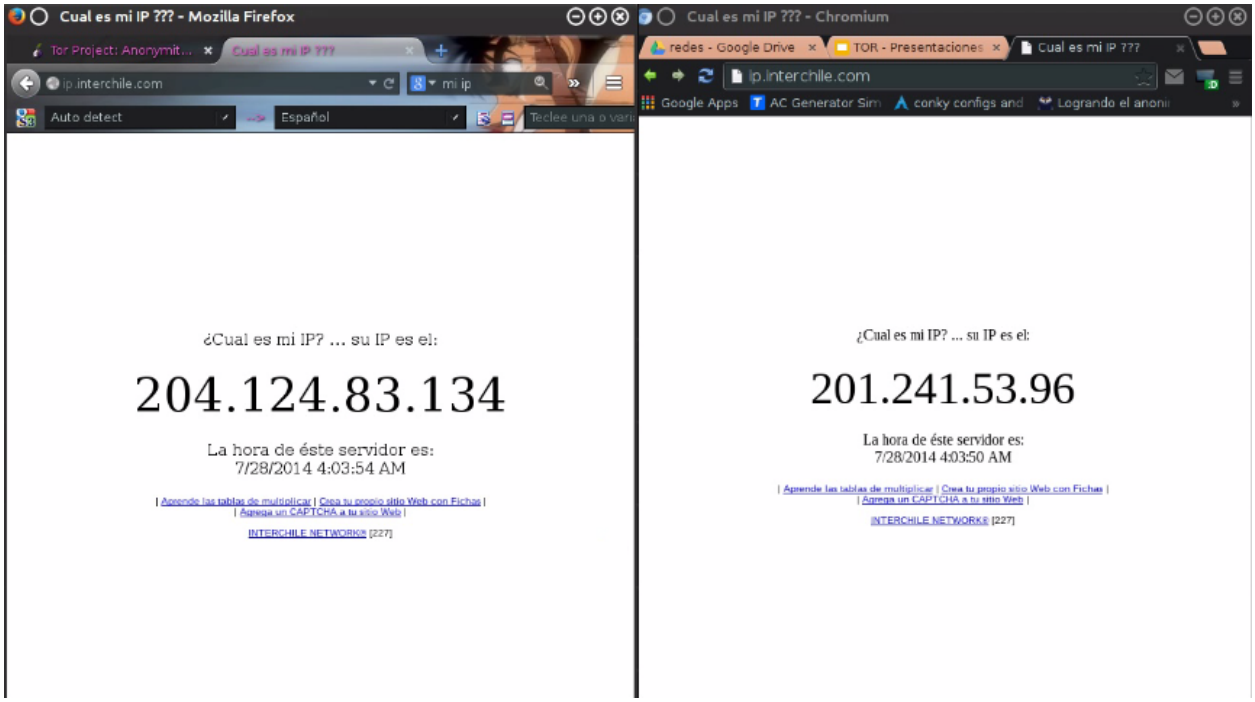
Como se mostró en un comienzo, un circuito de tor normalmente esta formado por 3 nodos,

Nodo de guardia: Al cual el cliente realiza las peticiones de paginas web y contenido de internet.
Nodo de relay: Sirve de nodo intermedio entre el nodo de guardia y el nodo de salida
Nodo de salida: Nodo que realiza la petición al servidor web con la peticion echa por el cliente.

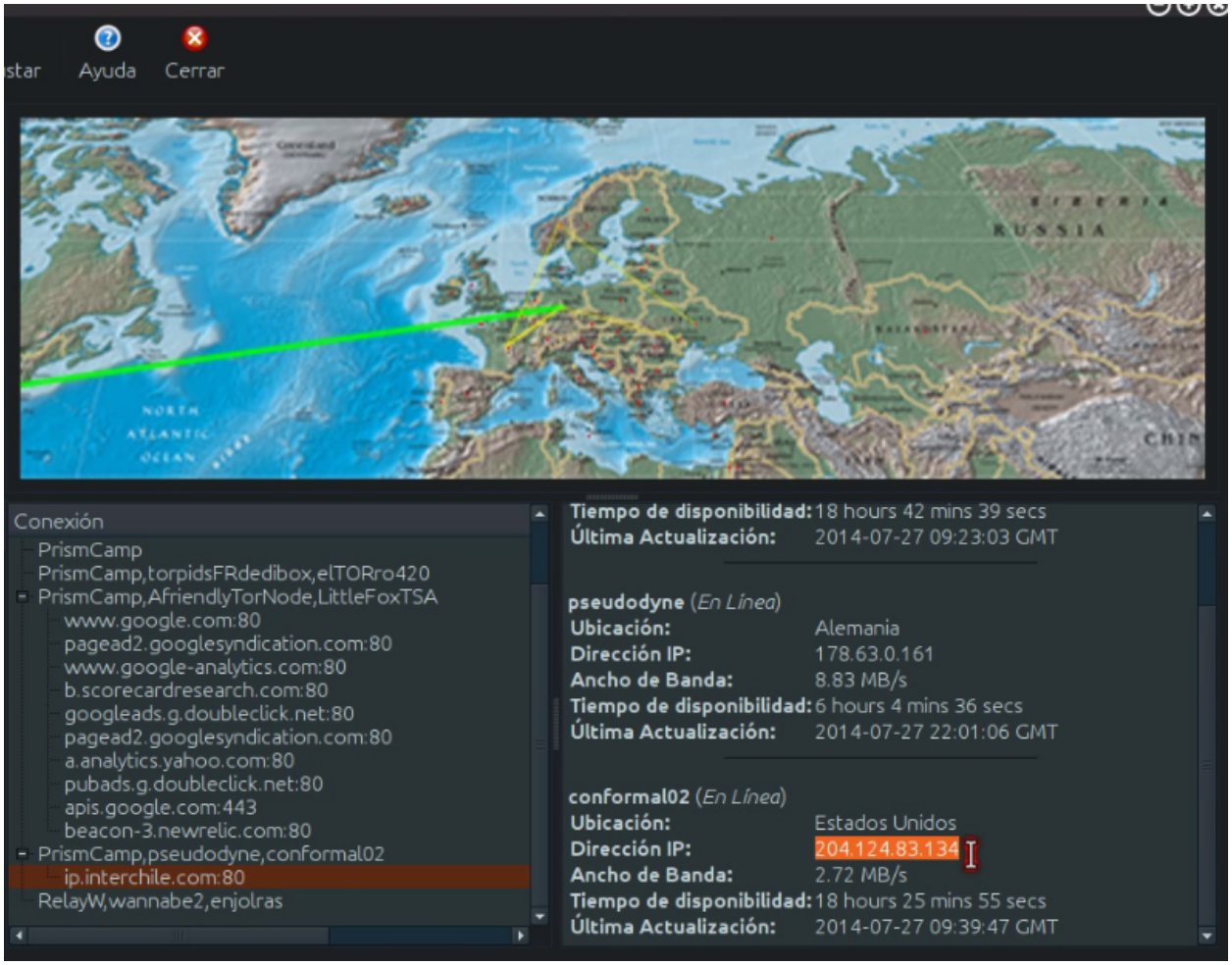
El camino que toma el mensaje por los nodos es entonces encriptado y privado, de modo que el servidor web observa que la notificación pidiendo su contenido es a travéz del nodo de salida, mientras que el nodo de guardia es el que entrega este contenido al cliente.
Un simple experimento utilizando wireshar, y verificando la dirección IP permite comprobar las declaraciones anteriores. Como se observa en las imágenes, los datos TCP y TLS que captura wireshark en el momento de cargar una página web poseen la como fuente de la información la IP del nodo de guardia.

En cambio, al preguntar por la IP del computador en alguna página que diga la IP, ésta página arrojará como respuesta el nodo de salida, que es quien realiza la petición al servidor web.

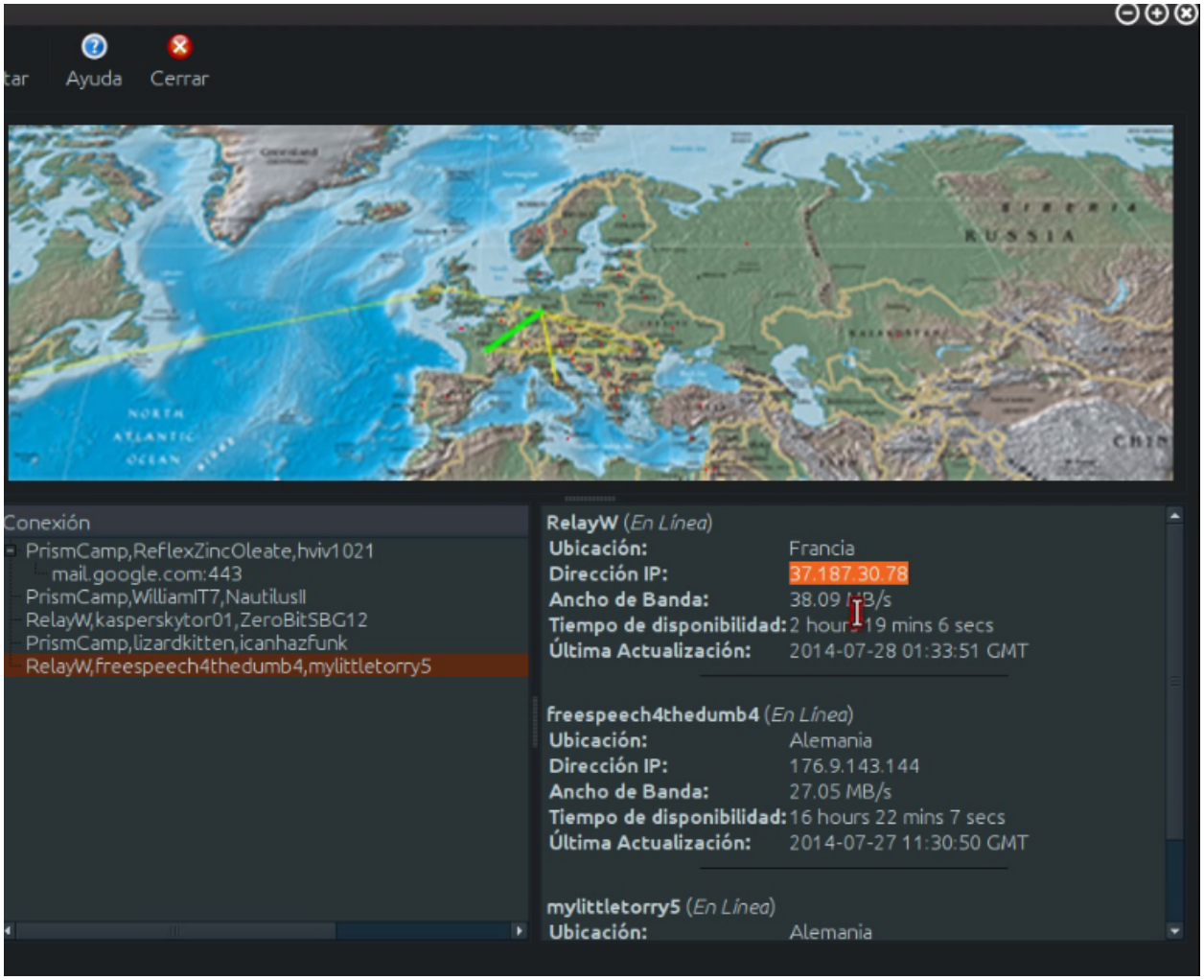
La imagen de la izquierda es el navegador configurado para usar la red tor por su puerto de comunicación, el navegador de la derecha no lo está.

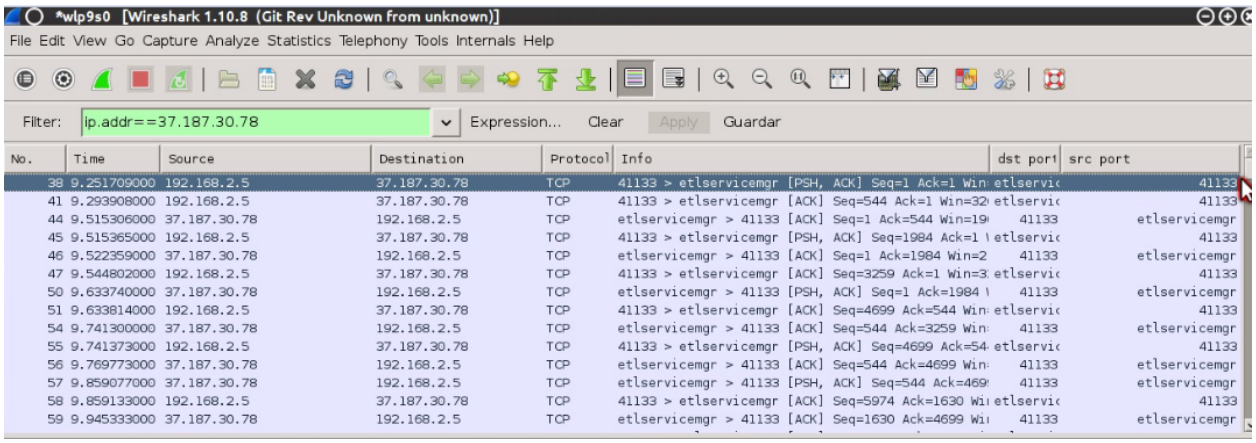


En la imagen siguiente se muestra el nodo de salida de la red tor, cuya IP es el mensaje de respuesta que da el servidor al que se le pregunta la IP, y se observa en el navegador configurado por TOR.


star
Ayuda
Cerrar
RUSSIA
NORTH ATLANTIC OCEAN
Conexión
PrismCamp
PrismCamp,torpidsFRdedibox,elTORro420
PrismCamp,AfriendlyTorNode,LittleFoxTSA
www.google.com:80
pagead2.googlesyndication.com:80
www.google-analytics.com:80
b.scorecardresearch.com:80
googleads.g.doubleclick.net:80
pagead2.googlesyndication.com:80
a.analytics.yahoo.com:80
pubads.g.doubleclick.net:80
apis.google.com:443
beacon-3.newrelic.com:80
PrismCamp,pseudodyne,conformal02
ip.interchile.com:80
RelayW,wannabe2,enjolras
Tiempo de disponibilidad: 18 hours 42 mins 39 secs
Última Actualización: 2014-07-27 09:23:03 GMT
pseudodyne (En Línea)
Ubicación: Alemania
Dirección IP: 178.63.0.161
Ancho de Banda: 8.83 MB/s
Tiempo de disponibilidad: 6 hours 4 mins 36 secs
Última Actualización: 2014-07-27 22:01:06 GMT
conformal02 (En Línea)
Ubicación: Estados Unidos
Dirección IP: 204.124.83.134
Ancho de Banda: 2.72 MB/s
Tiempo de disponibilidad: 18 hours 25 mins 55 secs
Última Actualización: 2014-07-27 09:39:47 GMT

En las imágenes siguientes se muestra la interacción con el cliente y el nodo guardia. La ip del nodo guardia es por la cual se reciben los contenidos del servidor web.





Referencias:

http://www.doctortecno.com/noticia/tor-para-garantizar-anonimato-virtual
https://gitweb.torproject.org/torspec.git?a=blob_plain;hb=HEAD;f=tor-spec.txt
https://www.torproject.org/
http://screwsandmarbles.wordpress.com/2013/06/14/tor-is-not-magic/
http://smallbusinesswoman.co.uk/the-inside-story-of-tor-the-best-internet-anonymity-tool-the-government-ever-built/