UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

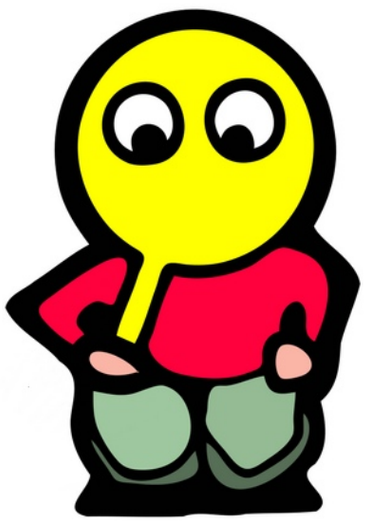
DEPARTAMENTO DE
ELECTRONICA

I2P

Invisible Internet Project

Redes De Computadores

2016-1



Alumnos:	Yerko Tapia	201403016-9
	Matías Zúñiga	201530002-K
Profesor:	Agustín González V.	

Resumen:

Dentro de la gran red de redes conocida como Internet, cada componente de esta red tiene su propia dirección que la diferencia de los demás. Direcciones como IP y Mac son ejemplo de estas, pero esto trae un gran problema. Al ser la dirección IP de uso público, esta puede utilizarse para malos fines, como por ejemplo: conocer la ubicación geográfica del host dueño de la IP, y las distintas acciones que ese hayan hecho utilizando esta IP, etc. Estas cosas pueden llevar a fraudes corporativos, robos de claves secretas e identidad, y muchos otros problemas.

Bajo esta premisa surge la necesidad de crear una forma de navegar por la red de manera anónima, para así evitar robos, fraudes, etc. Obviamente el anonimato en la red no siempre es por "buenas causas" también se puede utilizar para tráfico y venta ilegal, traspaso de archivos ilícitos, etc.

Algunas de las respuestas a esta problemática son: Freenet, Tor e I2P. En esta ocasión nos preocupará mayormente el caso de I2P, que utiliza un método de túneles, separándose en túneles de entrada (llegada de paquetes) y de salida (envío de paquetes).

Utilizando el método Garlic, que consiste en un sistema parecido a Onion Routing. El Onion Routing usa Routers "especializados" llamados Onion Routers, por los cuales se envían los paquetes bajo varias capas de cifrado (de ahí nace la analogía con una cebolla), mientras que el método Garlic puede enviar más que un solo mensaje bajo las varias capas de cifrado, I2P ofrece una cualidad más tentativa que los anteriores métodos nombrados, ya que permite realizar intercambios de archivos más rápidos y de manera más eficiente, presentando así un método nuevo de anonimato en la red.

Introducción

Desde la aparición de ARPANET en el año 1969, las redes de computadores se han ido expandiendo progresivamente, creando lo que hoy se conoce como la Internet, la red de redes.

Los computadores que conforman esta gran red poseen direcciones que los identifican. Está la llamada dirección MAC, la cual no siempre es de conocimiento público, y la dirección IP, la cual si es de uso público y puede ser utilizada para rastrear la ubicación de un usuario y obtener mucha información sobre este que puede ser almacenada por los sitios web.

Estos usos, entre otros varios que podrían ser llamados perjudiciales, son los que dieron inicio a la necesidad de crear una manera para navegar por una red de forma anónima. Dentro de las múltiples respuestas que se le dieron a este problema se encuentra el software llamado Invisible Internet Project o I2P.

Métodos para anonimizar

Bajo la problemática de poder navegar de forma anónima y segura, es que han surgido distintos métodos o posibilidades con las cuales puede efectuarse esta acción, dentro de las cuales destacan los siguientes.

Freenet (2000)

Freenet es una red anónima y distribuida de almacenamiento de datos. En esta, cuando se requiere un archivo, se conecta con un nodo aleatorio. Si este tiene el archivo, lo envía como respuesta, si no lo tiene se conecta con otro nodo, hasta encontrar el archivo, el que es almacenado en todos los nodos de la ruta. Ningún nodo sabe si quien le solicita el archivo es solo un nodo intermedio o el origen. [ref1]

Existen 2 métodos de navegación:

- **Darknet:** Solo es establecen conexiones con nodos conocidos y confiables.
- **Opennet:** Se establecen conexiones con cualquier nodo en la Freenet

Un nodo en la darknet puede ademas estar en la openet, por lo que las darknets se pueden conectar entre si.

Tor (2002)

Tor o “The Onion Router” es una red de proxies anónimos. Para que los mensajes viajen desde el origen al destino, se establecen conexiones mediante una red de nodos llamados “onion routers”. El mensaje tiene varias capas de encriptación, y cada nodo desencripta una. [ref2]

I2P (2003)

I2P es la red anónima que se analizará con mas detalle en el siguiente tema.

Al igual que Tor, I2P utiliza el sistema de “Onion Routing”, pero con unas leves diferencias.

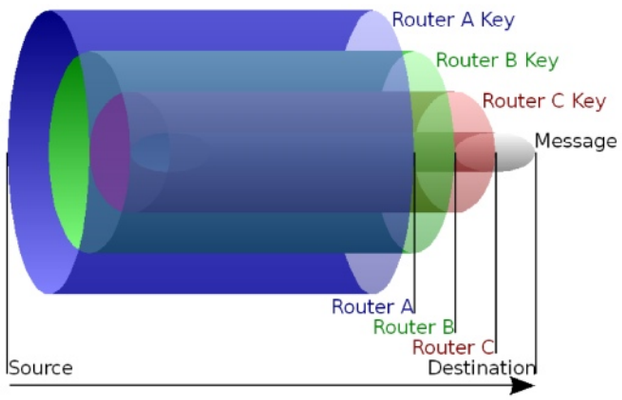


Ilustración 1: Diagrama del Onion Routing

Internet Invisible Project:

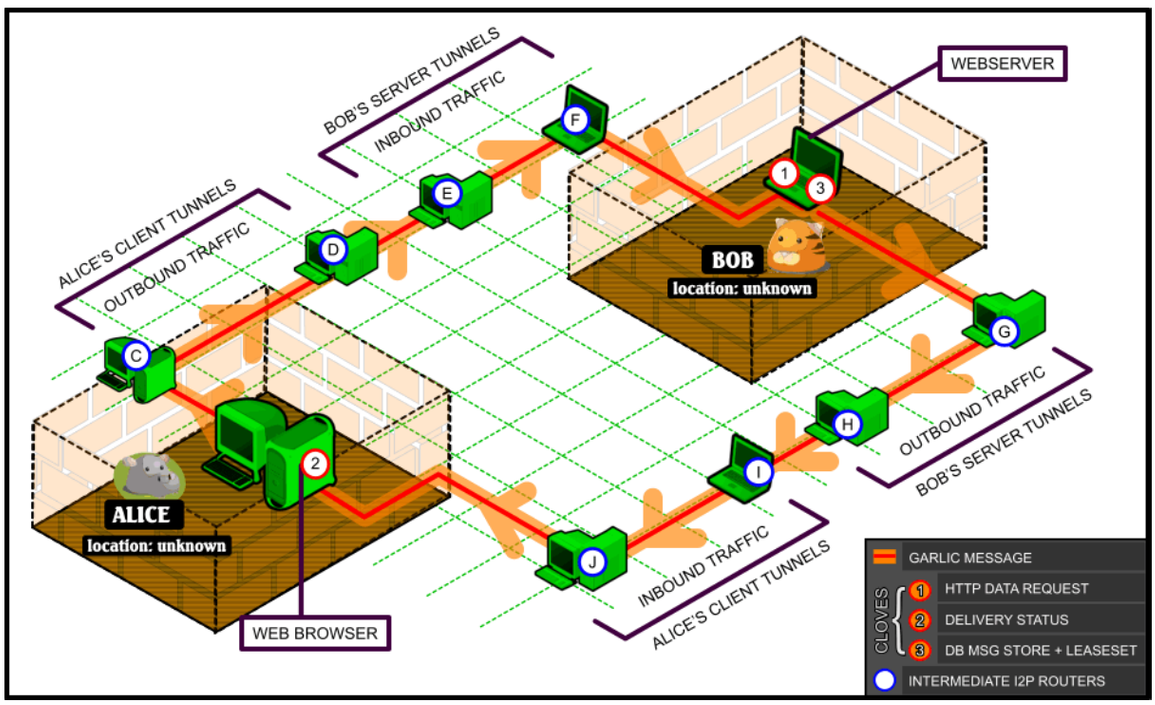
Internet Invisible Project (Proyecto de Internet Invisible) o por sus siglas en ingles, I2P, es una red que presenta una capa simple que las aplicaciones pueden usar para enviarse mensajes entre sí de forma anónima y segura.

Toda comunicación se encuentra bajo varias capas de cifrado, e inclusive los receptores son identificadores criptográficos.

Funcionamiento:

Cada aplicación cliente posee su “router” I2P, el cual crea una “túneles”. Estos túneles son caminos temporales y unidireccionales a través de una serie de routers. Los túneles se clasifican entre aquellos que son de entrada (que reciben paquetes) o de salida (que envían los paquetes).

La primera vez que se establece la conexión entre 2 clientes, ambos hacen una consulta en la “base de datos de red” (netDb). La netDb de I2P es una base de datos distribuida especializada que contiene 2 tipos de datos: la información de contacto de un router específico, y la información de contacto de un destino (LeaseSet). De esta forma es posible encontrar de manera efectiva los túneles de entrada y de salida de cada cliente. Luego de establecer la primera conexión no es necesario volver a consultar la base de datos, ya que los mensajes entre ambos cliente poseen esta información.



Usos:

Mediante la aplicación I2Ptunnel, que es parte de I2P, es posible para un usuario crear sus propios sitios web en la red I2P, así como navegar por sitios de la red I2P con un navegador normal, ejecutando un proxy HTTP.

I2P provee un servidor de mail y un servicio IRC, al que se puede acceder desde un cliente IRC común mediante un proxy I2PTunnel, y la aplicación I2P-Messenger ofrece un servicio de mensajería instantánea sin servidores.

Hay aplicaciones como I2PSnark que utilizan el protocolo BitTorrent para compartir archivos en la red I2P, y también existen aplicaciones para postear contenido online, en blogs o foros.

A pesar de que por defecto solo se pueden usar servicios pertenecientes a la red I2P, existen outproxys de terceros para navegar por la Internet normal a través de I2P (actualmente solo false.i2p está en funcionamiento).

Especificaciones de I2P

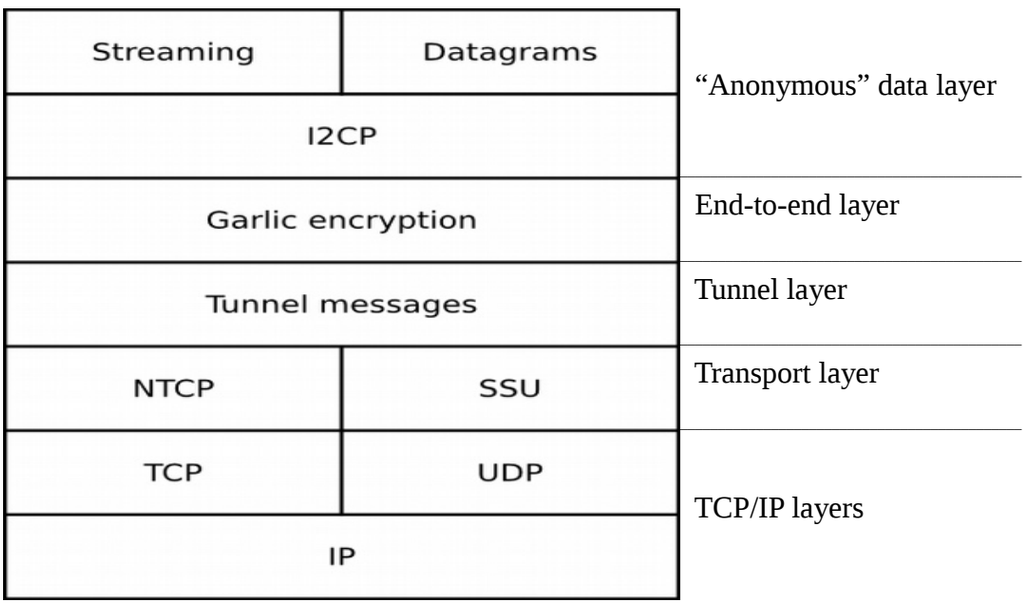
Ya se ha estudiado el funcionamiento básico de I2P, a continuación se pasara a ver como funciona pero de manera más detallada.

Encriptación:

Se usa una combinación de dos algoritmos de encriptación en distintas capas de la red. El primero es el cifrado ElGamal, algoritmo de clave asimétrica, y el segundo es el algoritmo de clave simétrica AES. La llave AES suele cifrarse con ElGamal.

Protocol Stack

I2P añade capas adicionales sobre el tradicional stack TCP-IP



- **Transport layer:** I2P presenta 2 protocolos distintos para su capa de transporte: NTCP (NIO-based TCP) que como su nombre dice es de confianza, y SSU (Secure Semi-reliable UDP) que, a pesar de operar sobre UDP, usa ACKs hasta cierto límite de intentos. Este protocolo opera en la comunicación entre un nodo y el siguiente.
- **Tunnel layer:** Comunica el principio de un túnel con el final de este. Acá la encriptación es por capas, que se desencriptan sucesivamente en cada nodo (Onion Routing).
- **End-to-end layer:** Como el nombre indica, comunica el origen con el destino. En un solo paquete garlic se incluyen, además de los datos, un mensaje que debe ser devuelto al origen para asegurar que la conexión es efectiva, y las actualizaciones al LeaseSet.
- **“Anonymous” data layer:** Técnicamente ya parte de la capa de aplicación, pero se ofrecen APIs para el desarrollo de los programas que quieran usar I2P. La API I2CP ofrece directamente las funcionalidades I2P, mientras que por medio de las APIs de Streaming y Datagrams se ofrecen conexiones tipo socket (el primero parecido a lo que es TCP, el segundo a lo que es UDP).

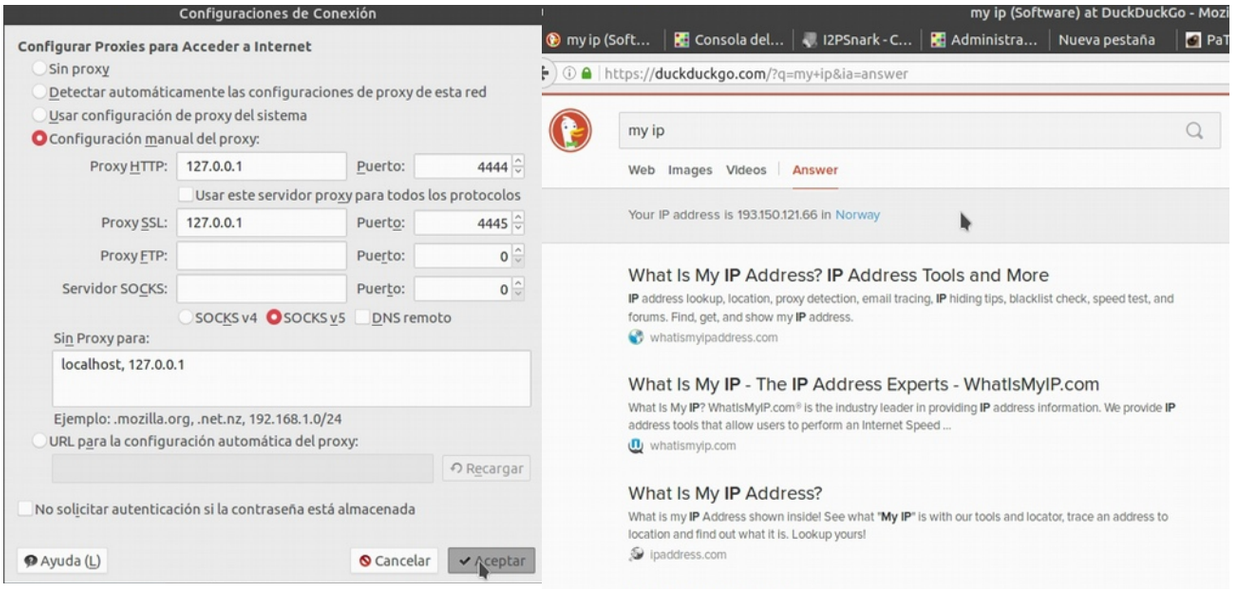
I2P en acción

Para esto se usó un sistema GNU/Linux. Luego de instalar el paquete correspondiente a la distribución se inicia el router con el comando:

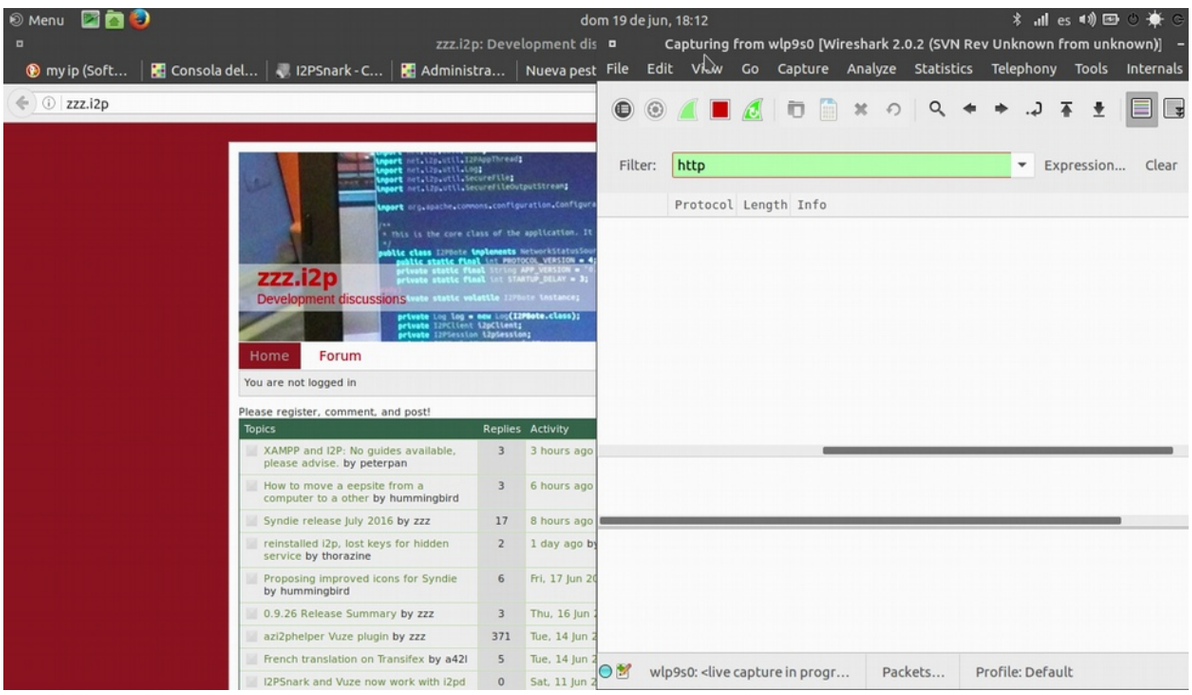
```
i2prouter start
```

Inmediatamente después de eso se abre automáticamente la “consola” de I2P en el navegador predeterminado.

Para usar I2P para las conexiones del navegador, debe configurarse el proxy de I2Ptunnel, luego de esto puede verificarse como la IP detectada por los sitios es distinta.



Se pueden cargar páginas de la red I2P, y además en Wireshark no se encuentran paquetes HTTP (ya que toda la conexión está cifrada, y Wireshark no sabe que es cada paquete).



Bibliografía

Technical Documentation – I2P - https://geti2p.net/en/docs

Referencias

[ref1] Inserting and Requesting data - The Dark Freenet (PDF) Pag. 4

[ref2] How is Tor different from other proxies? torproject.org/docs/faq