Una mirada a las profundidades de la deep web usando FreeNet

La Deep Web una mirada a lo profundo

Ana Isabel Valencia Martinez[1]
ana.valencia05@usc.edu.co

Andres Jose Hoyos Perez[1]
Andrés.hoyos01@usc.edu.co

M.Sc Ciro Dussan Clavijo[2]
Ciro.dussan00@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Tecnología en Sistemas de Información (1)
Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Tecnología en Sistemas de Información (2)

Resumen

El presente documento muestra una mirada a una parte de Internet conocida como Deep Web y cómo acceder ella utilizando Freenet, la cual es una alternativa al uso de TOR la red más popular para navegar en la Internet Profunda. Para llevar a cabo la escritura de este documento se utilizó como metodología la experiencia propia al usar Freenet, apoyado en literatura existente acerca de la Deep Web,la World Wide Web y en especial de Freenet. Obteniendo como resultado una visión general acerca de lo que es la Deep Web, como esta dividida la gran red de redes (Internet), el contenido que se puede encontrar en esta parte de World Wide web, cómo funcionan en forma general la mayoría de los buscadores en Internet, las medidas de seguridad que se deben tener para entrar en ella y cómo Freenet garantiza la privacidad de los usuarios que la utilizan para entrar en esta parte de la red invisible.

Palabras Clave: Internet,Freenet,Tor, Deep Web, World Wide Web.

Abstract

This document takes a look at the Deep Web and how to access it via Freenet, an alternative to the more popular Deep Web browser, TOR. For the completion of this document, we made use of personal experience using Freenet, as well as of the available literature about the Deep Web, the World Wide Web, and Freenet itself. As a result, we present a general view of the Deep Web, the organization of the great web (the internet), the content found in the Deep Web, the functioning of internet browsers, the safety measures to observe when browsing the Deep Web, and the ways in which Freenet guarantees the safety of its users when entering the Deep Web.

Key words: Internet, Freenet, Tor,Deep Web, World Wide Web.

1. INTRODUCCIÓN

La Deep Web es conocida como la red invisible, porque se encuentra oculta en Internet, adquirió fama en el año 2013 cuando el FBI descubrió el sitio Silk Road o 'Ruta de la seda', la cual era una tienda que que vendía narcóticos, armas, pornografía infantil, falsificaciones e, incluso, servicios de asesinos profesionales. Fue cerrada y su fundador conocido como "Dread Pirate Roberts" condenado a cadena perpetua en el año 2015. Contenido como el antes mencionado se puede encontrar en la Internet profunda. Pero también se puede encontrar otro tipo de contenido de índole legal, sano e interesante en esta parte de Internet. Navegar en ella es totalmente legal, pero no todo lo que se pueda hacer en ella. Pero qué peligros se pueden correr al navegar en sus profundidades y cómo se puede ingresar en ella, es lo que pretende desvelar este trabajo.(**Medina, 2016)**

Teniendo en cuenta que la Deep Web es un conjunto de redes privadas, este artículo sólo se enfocará en profundidad en una de esas redes conocida como FreeNet, para tal fin se utilizará como metodología de investigación la experiencia propia de navegar en ella y se va a utilizar la literatura disponible sobre el tema. Para desarrollo de esta monografía se cuenta con tres capítulos; en el primero se describe cómo está dividida la World Wide Web (Internet) y cómo trabajan los motores de búsqueda para localizar contenido en la Web; el segundo capítulo explica qué es FreeNet, su estructura, cómo se utiliza para acceder a la Deep Web y además de hablar un poco de TOR la red de la Internet Profunda más popular; en el último capítulo se describe el contenido que se puede encontrar en la Deep Web, pero se hace énfasis sólo en el contenido legal y las cosas buenas que se puede encontrar al navegar en esta parte de Internet.

2. CAPÍTULOS

2.1 Cómo se divide World Wide Web (Internet).

A finales de la década de los ochenta habían miles de redes de área local interconectadas entre sí, pero el acceso a información en ella era caótico: formatos incompatibles, protocolos heterogéneos, etc. Era necesario hacer más sencillo y homogéneo el acceso a este caudal de información, y gracias al surgimiento del proyecto world wide web también conocida como www, w3 o simplemente web, creado por Tim Berners-Lee un científico de la computación británica, logró la integración de recursos de la web y poder acceder a Internet a través de enlaces utilizando web browsers ,también conocidos en español como navegadores siendo los más populares: Google Chrome, Mozilla Firefox, Opera y Safari.(**Adell & Bellver, 1995**).

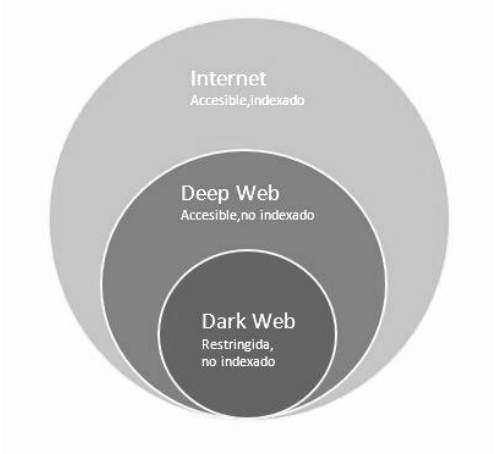
Pero buscar información en Internet no es suficiente solo utilizando navegadores, también es necesario el uso de motores de búsqueda que complementan a los web browsers convirtiéndose así en conjunto, en sistemas de navegación, como lo es Google en general por citar un ejemplo y su fin es el mismo: posibilitar que los usuarios encuentren la información que buscan en la web.(**Pérez & González, 2000**).

Un motor de búsqueda regularmente utiliza robots los cuales son procesos que recorren de forma continua la web para desglosar la estructura de un sitio web o incluso del world wide web completa, su trabajo permite crear y actualizar la base de datos usada por un motor de búsqueda, para la recopilación e indexación de los datos de su base, que utiliza una interfaz abierta con el usuario en la cual éste formula una consulta por medio de palabras o frases a la cual se responde con una lista de referencias que cumplan con el criterio de búsqueda (**Barbosa, 2002**).

Vale la pena realizar más claridad sobre el funcionamiento de los motores de búsqueda, se puede decir simplificando un poco que un motor de búsqueda consta de cuatro partes: una interfaz para el usuario para hacer peticiones de búsqueda, un robot o spider que busca la información en Internet, un algoritmo que conecta las peticiones de los usuarios con la base de datos y una base de datos donde se han indexado los contenidos, el corazón de todo motor de búsqueda es sin duda el algoritmo que dirige al robot o spider y después categoriza la información que se mostrará tras las peticiones de los usuarios.(**Archanco, 2014**)

Pero estos sistemas de navegación convencionales solo pueden acceder a datos localizables vía hiperenlaces a lo que se conoce como contenido de la surface web (Internet Superficial), otro nivel de world wide web es la Deep web que es aquella parte de Internet que no es accesible a los motores de búsqueda basados en enlaces como Google, Yahoo o Bing. La única manera de acceder a ella es introducir una consulta directa en un formulario de búsqueda web. Hay que aclarar que Deep web (Internet Profunda) y Dark Web (Internet Oscura) son dos niveles distintos en el world wide web, esta última la Dark Web es lo más profundo que tiene el océano de la Internet pero ambas tienen en común ocultar contenido; Internet se basa en páginas web que hacen referencia a otras páginas web; si tienes una página web de destino que no tiene enlaces entrantes, ha ocultado esa página y los usuarios o motores de búsqueda no pueden encontrarla. Un ejemplo de esto sería una publicación de blog que aún no se ha publicado. La publicación del blog puede existir en Internet público, pero a menos que sepa la URL exacta, nunca se encontrará, entonces se puede entender que la World Wide Web se divide en tres niveles la Surface Web, Deep Web y la Dark Web. **ver Fig 1**.(**Pederson, 2013).**

Figura 1: Estructura en capas de Internet



Fuente: Adaptado de **(Cagiga , 2017)**

Haciendo énfasis un poco más en sus dos últimos niveles, el término Hidden Web empezó a escucharse en el año de 1994, para referirse a los sitios web que no estaban registrados por algún motor de búsqueda, según El Journal of Electronic Publishing mencionó que Jill Ellsworth utilizó el término "la Web invisible" en este año, aunque en el año 2001 fue rebautizada como se conoce hoy la Deep Web, aunque hay quienes postulan que el origen de la Deep Web o Internet Profunda se originó en los años 90 con la creación del proyecto Onion Routing por parte del Laboratorio de Investigación Naval de los Estados (**Martín, 2014, P. 96-97**).

Hay que tener en cuenta que el tamaño de la Deep web como lo revela Michael K. Bergman en unas de sus publicaciones, que la información contenida en la Internet profunda es 400 a 550 veces más grande que la Internet superficial.(**Bergman , 2001**)

2.2 Cómo acceder a una parte de la Deep Web usando FreeNet

Buscar información en Internet realizando una analogía, se puede comprar con arrastrar una red por la superficie del océano. con la gran posibilidad que se atrape mucho en la red, pero teniendo en cuenta que existe una gran cantidad de información que es profunda y, por lo tanto, se omite. Hay una simple razón: la mayor parte de la información de la Web está oculta en sitios generados dinámicamente, y los motores de búsqueda convencionales nunca la encuentran.(**Bergman , 2001**). Es decir La Web profunda consiste en datos que existen en la Web pero son inaccesibles para por los motores de búsqueda a través del rastreo e indexación tradicional.(**Lawrence and Giles, 1998**).

Para poder acceder a este contenido es necesario valerse de un software específico (navegadores especiales de Internet) y poder entrar en estas redes anónimas, que es lo que en realidad se convierte la Internet Profunda. La red Tor llamada así por sus siglas en inglés "The Onion Router" que traduciría en español como "Enrutamiento de cebolla", es un proyecto cuyo objetivo principal es el tener una comunicación privada a través de una red pública, es uno de los más populares y usados para ingresar en la Deep Web y muchos piensan que al utilizarlo ya están dentro de toda la Deep Web y no es cierto, solo están navegando en una parte de la Internet Profunda y es lo que se quiere dejar muy claro en este capítulo, conocer toda la Deep Web es prácticamente imposible, porque a pesar que se utilicen todos los softwares específicos para ingresar en las redes que la conforman como: FreeNet, Tor, I2P,ZeroNet, etc., aún quedaría mucho contenido no indexado que no se encuentra inmerso en las redes antes mencionadas (**Alarcón & Guillén, 2015**).

Pero luego de hablar un poco de la red más popular de la Deep Web, hay que hablar de FreeNet uno de los proyectos más antiguo relacionado con el anonimato, sus inicios se remontan al año 2001 y al día de hoy aún sigue

teniendo vigencia. A diferencia de otras redes anónimas su arquitectura se basa en un modelo totalmente descentralizado, no hay servidores para gestionar la red y en su lugar, cada usuario que se conecta a ella aporta ancho de banda a la red y aporta un espacio para almacenar información de otros usuarios, ese espacio se conoce como "datastore". Ese modelo se convierte en un repositorio de archivo totalmente distribuido y la información que se almacena en dicho espacio se encuentra cifrada y solamente el propietario de esos archivos puede descifrar su contenido utilizando su clave privada.

Es decir cada usuario en FreeNet tiene un directorio en su ordenador que almacena archivos cifrados por otros usuarios miembros de la web profunda de FreeNet y el usuario tiene escaso control sobre el contenido que allí se almacena.

El modelo de anonimato que utiliza FreeNet es "inproy", es decir, es limitado únicamente al contexto de una Red Privada Virtual (VPN) sin acceso directamente a Internet. Su principal objetivo es facilitar las comunicaciones entre dos o más integrantes de forma anónima, privada y segura.

FreeNet es una red que depende en gran medida de la cantidad de usuarios que la utilizan debido que entre más usuarios se encuentren conectados la red será más grande y esto hará que sea más difícil para un atacante localizar el origen de una petición determinada y como resultado será más fuerte su anonimato.

Uno de los enfoques que hace muy interesante FreeNet, es el concepto de "Darknet", el cual consiste en permitir solamente las conexiones a aquellos nodos en la red que se consideren "amigos",es decir, que dentro de la red de FreeNet, pueden existir segmentos de redes de personas que se comunican entre sí y ningún otro nodo puede unirse a dichos segmentos sin permiso, reduciendo así las posibles vulnerabilidades o fugas de información realizados en ataques comunes que se realizan a este tipo de redes anónimas.**(Ortega, 2018).**

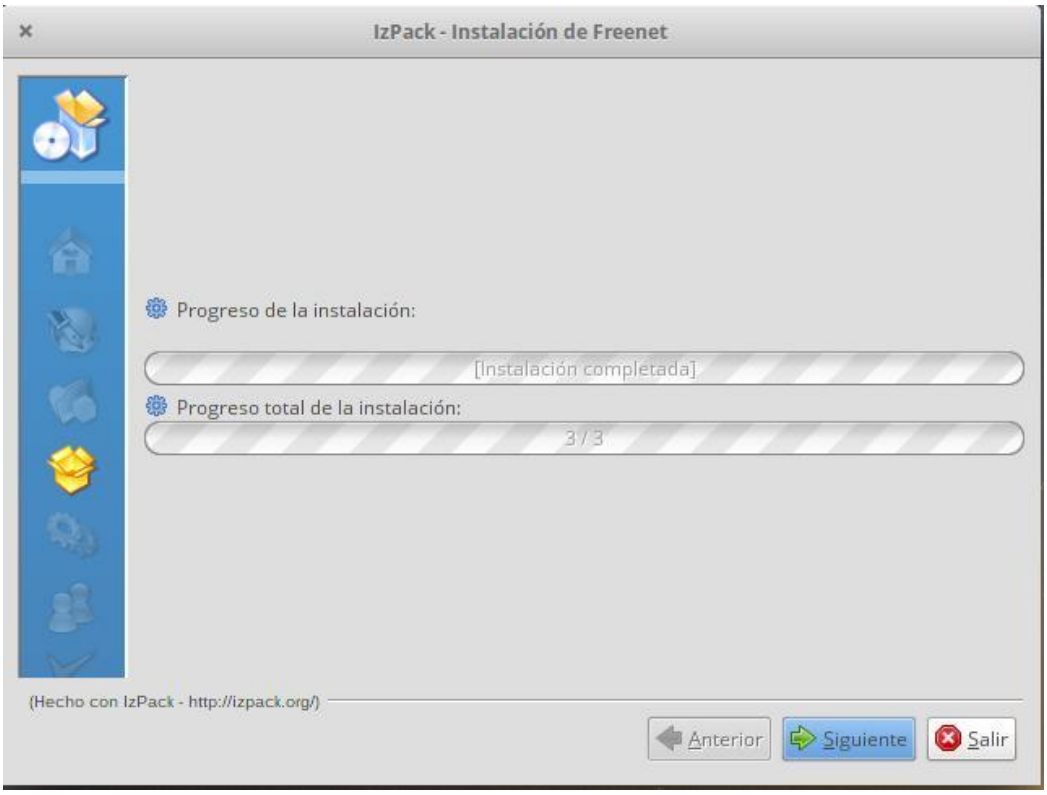
2.2.1 Instalación y configuración de FreNet

FreeNet se encuentra desarrollado en Java, por eso uno de sus requisitos de instalación es contar con una máquina virtual de java. Es compatible con múltiples sistemas operativos y aunque es un proyecto que lleva varios años activo, aún se liberan nuevas versiones y mejoras que hacen de FreeNet un software cada vez más estable y robusto.

A continuación se detallan los pasos para llevar a cabo la instalación de FreeNet:

1. Descargar y ejecutar el instalador de FreeNet el cual es un archivo "JAR" que se puede lanzar directamente con Java, el cual despliega un asistente muy simple e intuitivo que permite con muy pocos pasos completar el proceso de instalación.

   wget 'https://github.com/freenet/fred/releases/download/build01483/new_installer_offline_1483.jar' -O new_installer_offline.jar;



Proceso de Instalación de Freenet. Imagen1.0

2. Luego de completar el proceso de instalación, se abrirá un nuevo asistente de configuración en el navegador web por defecto del usuario, en el sitio "https://127.0.0.1:8888/wizard/" y en dicho sitio se solicitará el nivel de seguridad que se quiere utilizar en la instalación como se muestra en la imagen.

Configuración de Freenet, Imagen 2.0

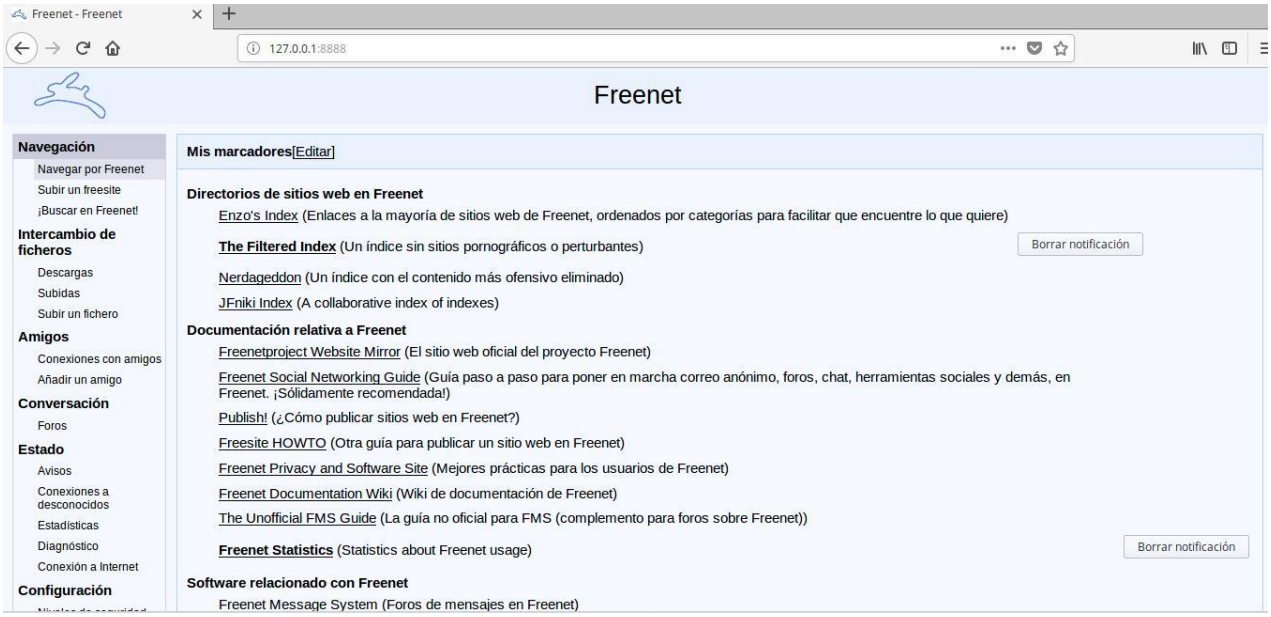
Existen tres niveles posibles "BAJO , ALTO Y PERSONALIZADO". En el caso de seleccionar el primero "BAJO" deja el nodo abierto a que cualquier miembro de la red pueda contactar y establecer conexiones. "ALTO" indica que nadie puede realizar conexiones a este nodo excepción de los

"amigos", lo que permite crear "Darknets", tal cual como se ha explicado en párrafos anteriores. Por último tenemos el nivel "PERSONALIZADO" permite al usuario realizar sus propias políticas de privacidad **(Rathod, 2017).**

3. Después de haber seleccionado el nivel de instalación y asignado el tamaño del "Datastore" que debe ser proporcional al tamaño del disco que tenga el usuario. El espacio reservado para el almacén de datos de FreeNet es el 5% de espacio disponible en disco si su capacidad es superior a 20 GB, 10% si su capacidad es mayor a 100 GB o 512 MB si su capacidad disponible en disco es menor a 10 GB.

4. Finalmente, el último paso consiste en asignar el ancho de banda que se le desea brindar a FreeNet de nuestra conexión a Internet, se recomienda asignar aproximadamente la mitad sobre el límite que establece el ISP a conexión del usuario.

Después de realizar estos sencillos pasos, aparecerá en el navegador la interfaz principal FProxy como se muestra en la siguiente imagen.



FProxy de Freenet. Imagen 3.0

Es la interfaz web de Freenet que puede ser accedida mediante el uso de cualquier navegador web. Desde aquí podremos acceder a Freesites, manejar nuestras conexiones con otros nodos, algunas estadísticas sobre el funcionamiento del nodo, revisar la lista de descargas y envíos, como así también, ver y modificar la configuración de nuestro nodo.

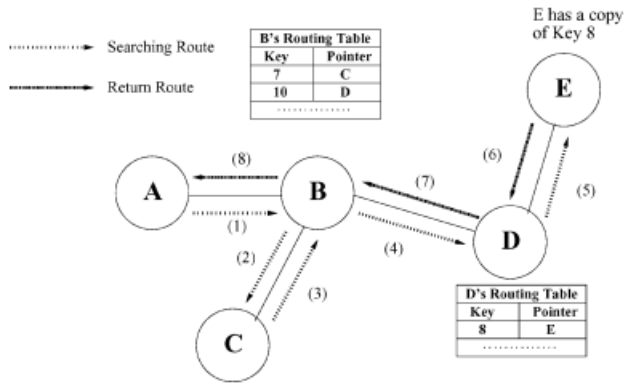
2.2.2 Generalidades de FreeNet

Luego de describir la instalación y configuración de Freenet, se puede definir un concepto más teórico acerca de esta red. Freenet se implementa como una red de nodos adaptables de igual a igual (**peer-to-peer**) que consulta unos a otros para almacenar y recuperar archivos de datos, cada nodo mantiene su propio almacén de datos local que hace disponible para la red tanto para lectura y escritura, así como una tabla de enrutamiento dinámico que contiene direcciones de otros nodos y las claves que se cree que contiene. El algoritmo de enrutamiento de Freenet se basa en una ligera agrupación de las entradas de la tabla de enrutamiento. Luego se puede observar que las tablas de enrutamiento se pueden configurar cambiando la política de reemplazo de caché en cada nodo; esto no incluye ningún cambio en el protocolo de enrutamiento de Freenet (**Zhang,Goel,Govindan, 2004**).

Este almacenamiento distribuido sirve para aumentar la capacidad de almacenamiento disponible para la red y permite a los usuarios comunes compartir ciclos de CPU no utilizados en sus máquinas. Por es que FreeNet no

necesita de servidores centralizados, sino que depende de las máquinas distribuidas tanto de su hardware, como su banda de ancha. Siendo el objetivo principal de la seguridad de Freenet proteger el anonimato de los solicitantes e insertadores de archivos. Aunque trivialmente cualquiera puede convertir un nodo en un almacén solicitando un archivo a través de él, por lo tanto "identificarlo" como un almacenador, lo importante es que hay permanezcan otros titulares no identificados del archivo para que un adversario no pueda eliminar un archivo atacando todos los nodos que lo tienen. Los archivos deben estar protegidos contra modificación maliciosa, y finalmente, el sistema debe ser resistente a la negación de ataques de servicio.(**Clarke, Sandberg, Wiley & Hong, 2001**),

Figura 2 : Ejemplo de búsqueda en FreeNet



Fuente: Tomada de (**Zhang, Goel, & Govindan, 2002**)

Para terminar este capítulo es importante aclarar un poco el concepto de (**Peer-to-Peer**). Una arquitectura de red distribuida puede denominarse red Peer-to-Peer, si los participantes comparten una parte de sus propios recursos de hardware (poder de procesamiento, capacidad de almacenamiento, capacidad de enlace de red, impresoras, ...). Estos recursos compartidos son necesarios para proporcionar el Servicio y el contenido ofrecido por la red (por ejemplo, uso compartido de archivos o espacios de trabajo compartidos para la colaboración): Son accesibles por otros pares directamente, sin pasar entidades intermediarias. Los participantes de dicha red son, por lo tanto, proveedores de recursos (Servicio y contenido).(**Schollmeier, 2001**).

2.3 Contenido que se puede encontrar en la Deep Web Usando FreeNet

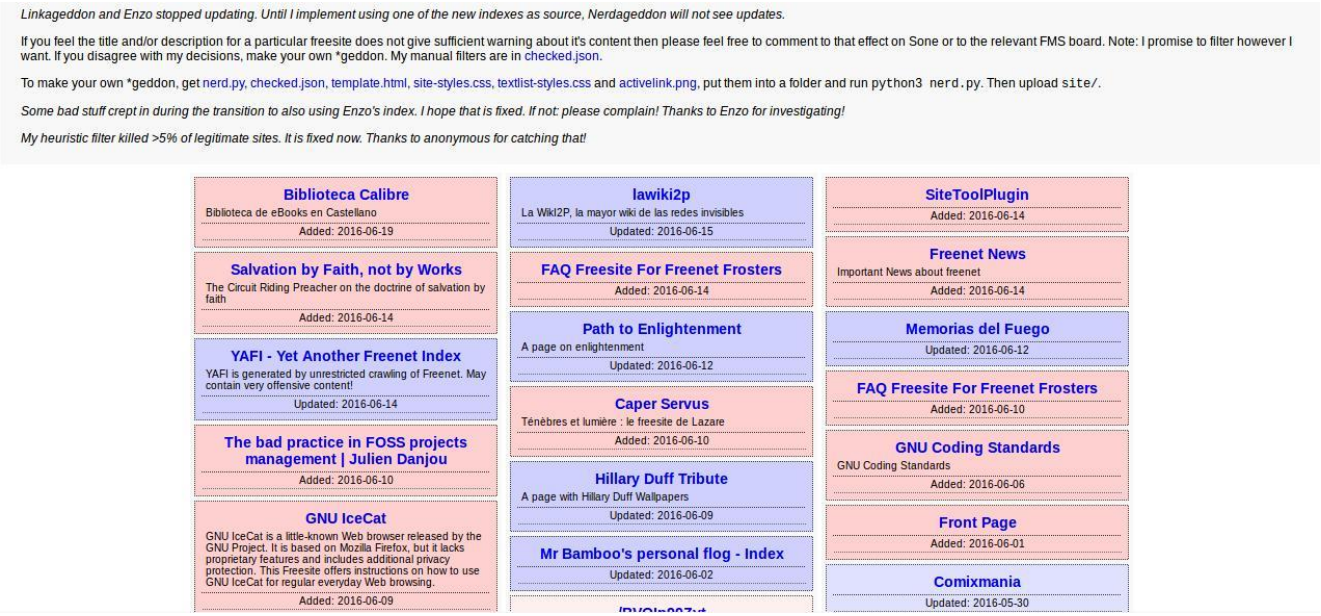
En promedio, los sitios en la Deep Web reciben arriba del 50% del tráfico mensual que los sitios contenidos en la web de la superficie. **(Bergman,Cafarella, Madhavan, and Halevy, 2011).**La Deep Web contiene mucha información y se puede encontrar todo tipo de contenido tanto legal como ilegal usando Freenet, pero como se ha mencionado en varias partes de este documento, este trabajo solo busca mostrar la información legal y sana que se puede encontrar en ella y cómo utilizar esta herramienta con responsabilidad, permitiendo al usuario una navegación en incógnito o anonimato que no deja rastro solo como protección y privacidad al internauta y no aprovechar este anonimato para cometer actos delictivos**.(Calderón & Tapia, 2018).** Aunque es difícil de creer hay mucho contenido y actividades legales que se desarrollan en la Deep Web, a continuación se describen diversos tipos de contenido que se encuentran en FreeNet y la cual es una recopilación de otros internautas, experiencia propia al navegar en ella y documentación disponible.**(Ibáñez, 2017,P. 78).**

A diferencia de TOR o I2P, los contenidos en FreeNet suelen encontrarse disponibles la mayor parte del tiempo gracias al modelo de almacenamiento distribuido que utiliza esta red anónima, no obstante, la disponibilidad de estos contenidos depende directamente de la cantidad de visitas que reciban y el número de "datastores" en los que se encuentren integrados.

Por otro lado, los servicios ocultos que existen en FreeNet pueden ser accedidos solamente con la clave correspondiente de cada uno de ellos y es necesario utilizar la herramienta "FProxy" y suponiendo que se encuentra

en ejecución en el puerto “8888”, que es el puerto por defecto , un usuario accede a cualquier servicio o contenido ingresando “https://127.0.0.1:8888/<CLAVE_FREENET>”. Un ejemplo de clave FreeNet es la siguiente:

clave:“USK@Isel-izgllc8sr~lreXQJzlLNGLIY-voOnLWWOyagYQ,xWfr4py0YZqAQSI-BX7bolDe-kI3DW~i9xHCHd-Bu9k,AQACAAE/linkageddon/1121/”, **nombre del servicio**: Linkageddon, **descripción**: Directorio que contiene varios enlaces a servicios en la web profunda de FreeNet. se actualiza frecuentemente, pero contiene bastantes contenidos que puede ser maliciosos u ofensivos, los cuales se encuentran marcados en rojo para advertir al usuario, como se muestra en la siguiente imagen.



Servicio de Freenet. Imagen 4.0

Como se ha mencionado en el capítulo y secciones anteriores en esta monografía, los contenidos y servicios en FreeNet se encuentran almacenados de forma descentralizada en los “datastores” y los mismos se encuentran cifrados. sin embargo, para que la información que se almacena en cada nodo pueda ser identificable y sobre todo descifrada por otros nodos, los contenidos se encuentran vinculados a diferentes tipos de claves como la que se mostró en el ejemplo anterior. Dichas claves son simplemente hashes que no guardan ningún tipo de relación con el contenido de su fichero, lo que quiere decir que las claves no revelan ningún tipo de detalle de su contenido. para acceder a cualquier contenido en FreeNet, es necesario conocer la clave que tiene asociada y además, existen diferentes clasificaciones las cuales se detallan a continuación.

Los tipos de claves en FreeNet son: CHK (Content Hash Key), SSK (Signed Subspace Key), USK (Updatable Subspace Key) y KSK (Keyword Signed Key).

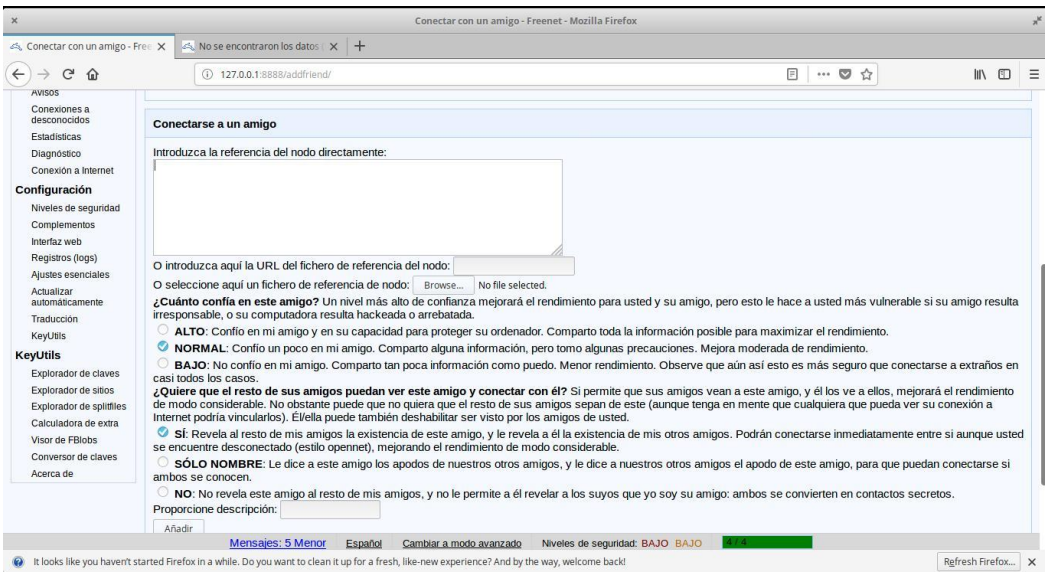
Por otro lado, también se pudo observar que personas sea han tomado el tiempo de crear índices como el de Noerdageddon, en esta página se ha eliminado todo contenido pornografico y que su creador ha considerado aburrido, se han indexado únicamente enlaces a freesites de interés. Un tipo de información que se puede encontrar aquí son páginas como la LaWiki2p en donde hay información de sistemas operativos y el mundo digital, guías para crear sitios en Freenet o blogs donde se habla del mundo de la Deep Web. También se puede encontrar otras páginas en inglés con temáticas diversas, como noticias sobre Freenet, herramientas sobre seguridad y privacidad o una página dedicada exclusivamente a Vladimir Putin. Hay que destacar que cada página a la que se accede en Freenet se descarga en el ordenador antes de poder ser vista en el navegador. **(Yubal , 2016).**

También se presta como medio de expresión y comunicación para ciudadanos de países profundamente censores, o colectivos que son perseguidos por razones culturales, sexuales, de género, políticas, religiosa y/o económicas dentro de la sociedad.También se pudo encontrar fresites de activistas anti-capitalistas, portales de descarga de contenido, comunidades en torno a una serie de TV, un estilo de música, una cultura…, blogs de la más diversa índole, tutoriales para proteger nuestra privacidad o sobre software libre…. Eso sí, las páginas son sencillas y van al grano, sin grandes diseños o formatos de vanguardia. La mayoría es simplemente texto enriquecido con hipervínculos y listas interminables de elementos, centrándose en lo verdaderamente valioso, que es el contenido, y obviando el contenedor, todo esto se logró evidenciar al navegar en la configuración Opennet o seguridad baja. (**Pablo F. Iglesias, 2017**).

2.3.1 Darknets en FreeNet

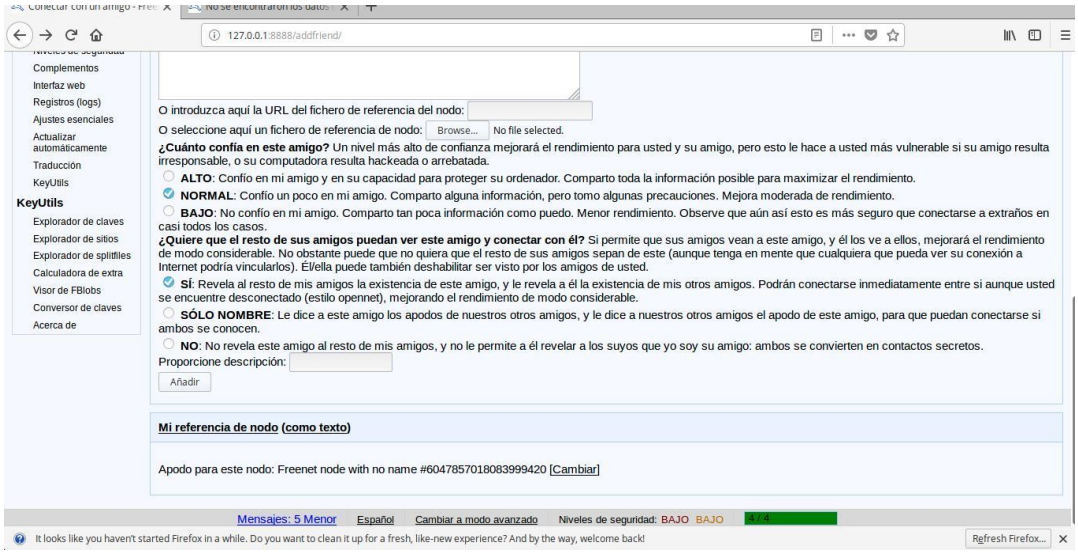
pero el arma más fuerte que se pudo encontrar al utilizar Freenet fue en su configuración de seguridad alta (Darknet). Una "Darknet" al interior de FreeNet le permite a un usuario definir grupos privados de "amigos" con los cuales se podrá comunicar de forma anónima, este modo de navegación es sin duda mucho más seguro que permitir que cualquier enrutador pueda contactar con la instancia local del usuario , sin embargo es mucho más lento y pobre su rendimiento, especialmente cuando se tiene pocos amigos adicionados en la instancia, de hecho, para poder crear una "Darknet" es necesario contar mínimo con cinco miembros, para que el mecanismo de "amigos" funcione adecuadamente, la comunicación y la confianza debe establecerse en doble sentido, esto quiere decir que no basta con que un usuario agregue a otro como "amigo", el nodo adicionado debe aceptar dicha solicitud de unión y para hacerlo debe adicionar como "amigo" al solicitante. Todo el tráfico entre los nodos "amigos" viajará cifrado, lo que quiere decir que es difícil para cualquiera de ellos conocer exactamente qué tipo de información está transportando alguno de los otros nodos (**Bruno, 2018**),(**Echeverri, 2016)**.

Para adicionar "amigos" en la instancia local de FreeNet, es necesario dirigirse a "http://127.0.0.1:8888/addfriend/", como se puede observar en la imagen inferior, es posible agregar un nuevo contacto adicionando su correspondiente referencia en el campo destinado para ello.



Agregar amigos en Darknet. Imagen 5.0

Para que otros nodos puedan adicionar también la instancia local como "amigo", también es necesario que conozcan la referencia del nodo, por ese motivo al final de la página web (imagen anterior), se encuentra la referencia del nodo local, la cual debe ser entregada a los contactos que se han agregado como se muestra en la siguiente imagen.



Referencia al nodo local. Imagen. 6.0

También se puede contar con servicios y complementos como Frost la cual es una de las aplicaciones más populares en Freenet que permite subir, descargar y compartir información de una forma fácil y sobre todo, anonima.Otra de las aplicaciones populares en Freenet es JSite, la cual se utiliza para agregar,modificar, eliminar o publicar freesites y después que todos los contenidos son insertados en la red se podrá utilizar la clave generada para poder acceder al servicio oculto en Freenet.(**Echeverri, 2016**).

2.3.2 Freemail (complemento oficial)

Para finalizar y complementar el recorrido por el contenido que podemos encontrar en FreeNet, Tenemos a Freemail, este complemento permite que cualquier cliente de correo electrónico pueda enviar mensajes de forma anónima utilizando FreeNet.Puede ser instalado desde la opción de "Complementos" ubicada en el menú "Configuración". No obstante, se trata de un complemento que a la fecha se encuentra en constante desarrollo.

Una vez que el complemento se encuentra cargado en la instancia de FreeNet, es obligatorio configurar una nueva cuenta de correo que será utilizada para el envío de mensajes de forma anónima, para ello se debe seleccionar la opciçon "Visite", con esto se abrirá una nueva ventana donde se ingresará la información relacionada con dicha cuenta y sus credenciales de acceso.

Después de crear la cuenta es necesario configurar una cuenta de correo electrónico utilizando el puerto 3143 para el protocolo IMAP y el puerto 3025 para SMTP. Dicha configuración es bastante sencilla y se encuentra soportada por prácticamente todos los clientes de correo electrónico.

El formato de una cuenta de correo Freemail quedará de la siguiente manera:

<usuario>@clave.freemail

3. CONCLUSIONES

Después de hacer un recorrido por la web profunda de Freenet, se puede concluir que su principal diferencia con otros redes anónimas es su descentralización, es decir, no necesita de servidores para controlar o gestionar su red. La información se encuentra distribuida en múltiples nodos y se necesitan de claves privadas para poder acceder a dichos ficheros, otro punto a tener en cuenta es que evidemente los usuarios que comparten su "datastore" desconocen el contenido que se encuentra en este espacio de almacenamiento utilizado por Freenet en sus computadoras. Además esta red necesita para poder sobrevivir al ser descentralizada y garantizar un buen

anonimato de un número considerable de host conectados a ella y por último podemos afirmar que su navegación es "inproxy" es decir no permite conectarse directamente a Internet.

En términos generales la web profunda de Freenet contiene un gran volumen de información, distribuida en su gran mayoría en varias redes privadas dentro de Internet y Freenet es una de ellas, la cual es una red descentralizada que permite aislar redes dentro de ella como es el caso de las Darknets y cuya navegación se hace "inproxy", es decir, solo se puede acceder al contenido que se comparte y distribuye dentro de ella. Pero lo más interesante de ella es precisamente las Darknets, debido a que permite crear redes independiente dentro de ella misma, garantiza un gran anonimato y nivel de seguridad que puede ser un arma de doble filo en el ámbito de la legalidad e ilegalidad.

En base a la experiencia personal de utilizar FreeNet se puede concluir que es una red amigable con el usuario porque es muy intuitiva,fácil de acceder y configurar para empezar a navegar con ella , aunque su interfaz gráfica es un poco antigua. Es recomendable usarla utilizando una máquina virtual debido a que las páginas o freesites se descargan en el ordenador y esto puede generar inconvenientes de seguridad al no saber qué tipo de archivos estamos alojando en nuestro disco duro y de esta manera mitigar el único peligro que se pudo evidenciar al usar esta subred. La utilidad más importante que encontramos al utilizar FreeNet es el uso de la configuración en modo DarkNet debido a que usted se vuelve invisibles en la subred debido a que solo usted y sus amigos que están conectados con usted en esa darknet sabrán que está utilizando FreeNet y por este hecho su seguridad aumenta drásticamente, recordando que deben haber mínimo entre 5 a 10 amigos para que la subred (DarkNet) que crea en FreeNet no se vuelva muy lenta , hay que tener en cuenta que en este nivel usted estará protegido contra gobiernos y personas que puedan afectar su libertad de alguna forma y la comunicación en ella está blindada contra interceptaciones porque es prácticamente irrastreable.

Entonces se puede decir analogicamente que la Deep Web es como un arma que dependiendo cómo se use puede ser buena o mala.

4. REFERENCIAS

- **Martín, A. L. B. (2014). 'Deep Web O Internet profundo. *Seguritecnia*, (407), 96-97.**
- **Calderón, F. M. M., & Tapia, D. R. D.(2018). Internet profundo Deep Web.**
- **Ibáñez, E. M. (2017). Dark Web y Deep Web como fuentes de ciberinteligencia utilizando minería de datos. *3ª ÉPOCA*, 74.**
- **Adell, J., & Bellver, C. (1995). La internet como telaraña: el World-Wide Web. *Métodos de información*, *2*(3), 25-32.**
- **Pérez, T. H., & González, J. T. (2000). Arquitectura de la información: el diseño de los espacios y flujos de información en la World Wide Web. *Bibliodoc: anuari de biblioteconomia, documentació i informació*, 103-122.**
- **Barbosa, R. R. L., & Rosales, M. R. G. (2002). Desarrollo de un motor de búsqueda. *Coquimatlán, Colima*.**
- **Pederson, S. (2013, marzo). Understanding the Deep Web in 10 Minutes. BrightPlanet. Disponible en http://bigdata2.brightplanet.com/whitepaper-understanding-the-deep-web-in-10-minutes**

- **Bergman, M. K. (2001). White paper: the deep web: surfacing hidden value. *Journal of electronic publishing*, *7*(1).**

- **Alarcón, V., Andrés, J., & Guillén Guillén, V. C. (2015). *Guía metodológica de uso seguro de internet para personas y empresas utilizando la Red Tor* (Bachelor's thesis, PUCE)**

- **Ortega Castillo, C. Un paseo por la Deep Web.(2018)**

- ***Rathod, D. (2017). Darknet Forensics. future, 11, 12.***

- **Clarke, I., Sandberg, O., Wiley, B., & Hong, T. W. (2001). Freenet: A distributed anonymous information storage and retrieval system. In Designing privacy enhancing technologies (pp. 46-66). Springer, Berlin, Heidelberg.**

- **Yúbal F.M. (2016) Así es Freenet, deep web alternativa a Tor e I2P :https://www.genbeta.com/a-fondo/asi-es-freenet-deep-web-alternativa-a-tor-e-i2p**

- **Pablo F. Iglesias (2017) MundoHacker: Freenet, una alternativa inproxy a TOR o I2P : https://www.pabloyglesias.com/freenet-red-inproxy/**

- **Cagiga Vila, I. (2017). Deep Web: acceso, seguridad y análisis de tráfico.**

- **Archanco, R. (4 de Febrero de 2014). papelesdeinteligencia.com. Obtenido de papelesdeinteligencia.com: http://papelesdeinteligencia.com/como-funciona-unmotor-de-busqueda/**

- **Schollmeier, R. (2001, August). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In *Peer-to-Peer Computing, 2001. Proceedings. First International Conference on* (pp. 101-102). IEEE.**

- **Lawrence, S., and Giles, C. L. 1998. Searching the World Wide Web. Science, 280, 5360(Apr. 1998), 98-100.**

- **Hui Zhang, Ashish Goel, Ramesh Govindan,Using the small-world model to improve Freenet performance,Computer Networks,Volume 46, Issue 4,2004,Pages 555-574**

- **M. K. Bergman, M. J. Cafarella, J. Madhavan, and A. Halevy, "Papers ' Contributions," pp. 1–23, 2011.**

- **Greenstadt, R., & Defcon, X. I. I. (2004). Tools for Censorship Resistance.https://freenetproject.org/author/freenet-project-inc.html**

- **Bruno (2018) darkwebnews: Freenet – Another Secure Anonymity Browser:https://darkwebnews.com/anonymity/freenet-secure-anonymity-browser/**

- **MEDINA, ÉDGAR (2016) Un viaje a la web oscura, el rincón del crimen en la red: https://www.eltiempo.com/archivo/documento/CMS-16504411**

- **Echeverri, Daniel (2016). Deep Web: TOR, FREENET & I2P privacidad y anonimato, Madrid, España: Editorial ZeroX word Computing**

- **Zhang, H., Goel, A., & Govindan, R. (2002). Using the small-world model to improve freenet performance. In *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*(Vol. 3, pp. 1228-1237). IEEE.**