Universitat Oberta de Catalunya

uoc.edu

UN PASEO POR LA DEEP WEB

TFM en empresa: INCIBE

Máster Interuniversitario de Seguridad de las Tecnologías de la Información y las Comunicaciones

Jorge ÁLVAREZ RODRÍGUEZ

Jorge CHINEA LÓPEZ

Víctor GARCIA FONT

30 de diciembre de 2018


Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

A Patricia,
a Nira.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Un paseo por la *Deep Web*
Nombre del autor:	Jorge ÁLVAREZ RODRÍGUEZ
Nombre del consultor/a:	Jorge CHINEA LÓPEZ
Nombre del PRA:	Víctor GARCIA FONT
Fecha de entrega:	12/2018
Titulación:	Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Área del Trabajo Final:	TFM en empresa: INCIBE
Idioma del trabajo:	Castellano
Palabras clave:	*Deep Web*

Resumen del Trabajo:

"Un paseo por la *Deep Web*" presenta de forma clara y ordenada los principales aspectos que rodean a la conocida como Internet profunda. Partiendo de la definición de la *Deep Web*, se observan las diferencias entre *Surface Web*, *Dark Web* y *Darknet*.

Sentadas las bases de lo que es cada ecosistema se hace un repaso por las *Darknet*s más conocidas, así como otras que empiezan a aflorar. Las más populares, Tor, Freenet e I2P, son analizadas en profundidad, determinando sus principales características y su modo de trabajo y comparando las tres, esgrimiendo sus ventajas y sus inconvenientes.

Una vez que ya se ha accedido a la *Dark Web*, el siguiente paso es descubrir que hay en estas redes, sus contenidos y los servicios que ofrecen y aprovechar para desterrar la idea de que la *Dark Web* solo está llena de ciberdelincuentes, sino que hay muchas más posibilidades y forma de uso totalmente licitas, eso sí, con la característica común de guardar el anonimato y privacidad del usuario.

Pero en ocasiones, este anonimato se ve cuestionado, por ataques y vulnerabilidades que pueden afectar a las *Darknet*s o al software de acceso, este trabajo expone varios de estos impedimentos.

Finalmente se llevan a cabo varios experimentos prácticos: acceso a la cada *Darknet*, evaluación de los distintos mecanismos existentes y su configuración y un intento de desanonimización.

Abstract:

"A walk-through *Deep Web*" presents in a clear and orderly manner the main aspects surrounding the so-called Deep Internet. Starting from the definition of the *Deep Web*, the differences between *Surface Web*, *Dark Web* and *Darknet* are observed.

First, the foundations of each ecosystem are established and then a review is made of the best-known *Darknet*s. The most popular, Tor, Freenet and I2P, are deeply analysed, determining their main characteristics and way of working and comparing their advantages and disadvantages.

Once you have accessed the *Dark Web*, the next step is to discover what is inside these networks, their contents and the services they offer and take the opportunity to banish the idea that the *Dark Web* is only full of cybercriminals, but there are many other possibilities and forms of use that are totally licit, however, with the common characteristic of keeping the anonymity and privacy of the user.

But sometimes, this anonymity is questioned, for attacks and vulnerabilities that can affect the *Darknet*s or access software, this work exposes several of these impediments.

Finally, several practical experiments are carried out: access to each *Darknet*, evaluation of the different existing mechanisms and their configuration and an attempt to deanonymize.

Índice

Lista de figuras

1. INTRODUCCIÓN

1.1. Contexto y justificación del Trabajo

La *Deep Web* es un tema recurrente en estos últimos años. Aunque fue en el año 1994 cuando la doctora Jill Ellsworth utilizó el término Web invisible para denominarla, no es hasta 2001, cuando el informático Mike Bergman establece la actual acepción de *Deep Web* como todo ese **contenido web** que los motores de búsqueda como Google o Bing **no pueden indexar**.

Entre ese contenido web se encuentran aquellas páginas que no desean ser indexadas por los buscadores y permanecen ocultas de forma intencionada; también todas las que se generan de forma dinámica o mediante enlaces formulados bajo algún lenguaje como JavaScript, Flash o Ajax; las que requieren credenciales para su acceso y lectura forman parte de la *Deep Web*; al igual que aquellas que no están enlazadas por otras, las denominadas página sin enlaces de entrada; también los documentos con formatos no indexables y finalmente otro tipo de ficheros web que se encuadran aquí, son las conocidas como páginas contextuales, cuyo contenido viene determinado por varios factores como pueden ser la IP, el número de visitas anteriores, etc.

Habitualmente se afirma que la *Deep Web* lo conforma el 96% del contenido web existente a nivel mundial, dejando tan solo un 4% asociado al **Internet convencional**, denominado en contraposición a la *Deep Web*: ***Surface Web*** o ***Clearnet***. En el año 2010 se estimó que la información que se encuentra en la *Deep Web* es de 7500 terabytes frente a los 19 terabytes que contendría la *Surface Web*. Por el contrario, otros expertos afirman que estas estimaciones carecen de credibilidad ya que si no podemos indexar el contenido de la *Deep Web* no puede tampoco ser contabilizado.

Otra particularidad asociada a la *Deep Web* con cierto cariz ilusorio es su división en varios niveles. Partiendo del primer nivel, que equivaldría a la *Surface Web*, se descendería hasta los niveles más profundos en los que el acceso se dificultaría gradualmente hasta llegar al último que popularmente se conoce como **Las Marianas** en analogía a la fosa de las Marianas. (1) (2) (3)

La popularidad que está alcanzado la *Deep Web* se debe en gran parte a la posibilidad de navegar por sitios web sin necesidad de identificar al consumidor de estos sitios. Es decir, de poder ofrece a ese usuario, una **garantía de anonimato**, que a través de la red convencional sería difícil de llevar a cabo.

Este anonimato permite a los usuarios **burlar la censura** que en muchos lugares del planeta se está ejerciendo con cada vez mayor notoriedad en Internet y acceder a ese contenido web oculto sin restricciones.

Precisamente es esta posibilidad la que está haciendo que se tenga una idea asociada de la *Deep Web* con la **ciberdelincuencia**, debido a que los propios ciberdelincuentes **aprovechan ese anonimato** que les ofrece la *Deep Web* para llevas a cabo sus operaciones ilícitas.

Esa parte de la *Deep Web* donde se puede navegar de forma anónima es lo que se denomina como ***Dark Web*** y vendría a ocupar el 0.1% del tamaño de la *Deep Web*. La *Dark Web* lo forman un **conjunto de redes** con distintos procedimientos para **ocultar la identidad**, así como métodos para acceder. **Cada red** de este tipo es lo que se conoce como ***Darknet***.

Este trabajo pretende profundizar en la *Deep Web*, especialmente en la parte de navegación anónima, en aquellos contenidos que se encuentran ocultos, en los servicios que ofrece, en las acciones que se pueden llevar a cabo, etc. y en tratar de romper esa asociación mencionada en el párrafo anterior, descubriendo que hay mucho más allá que la ciberdelincuencia.

Se estudiarán las redes existentes más conocidas como por ejemplo Tor, I2P o Freenet, pero también otros proyectos que se encuentran en desarrollo. Se detallarán los métodos existentes para acceder, las posibilidades que ofrece cada *Darknet* y se pondrán a prueban, tratando de romper esa característica tan definitoria de las *Dark Web* como es el anonimato.

1.2. Objetivos del Trabajo

Los objetivos de este trabajo son los siguientes:

En primer lugar, **definir** que es la *Deep Web*, indicar que contenido la conforma, aclarar las diferencias existentes entre esta, la *Surface Web*, la *Dark Web* y la *Darknet* y estimar el tamaño que ocupa cada una.

El segundo objetivo que inspira este trabajo es mostrar **qué hay** en la *Deep Web*, y más en concreto en la *Dark Web*, **qué se puede hacer** y qué servicios ofrece. Es en este punto donde se discutirá la relación existente entre la *Deep Web* y la Ciberdelincuencia.

En tercer lugar, se darán a **conocer las distintas redes** existentes, los diversos métodos para acceder a cada *Dark Web*, cuáles son las ventajas e inconvenientes de cada una, que requisitos tienen y en qué punto de desarrollo e implantación se encuentra cada proyecto.

Como cuarto objetivo, se darán a conocer los **motivos** que dieron lugar al **nacimiento** y posterior desarrollo de estas tecnologías, es decir, que necesidad debía de ser cubierta para que en un momento dado se creasen estas redes.

El quinto objetivo, será **comprobar si el anonimato** que se ofrece al navegar por los contenidos que conforman las *Darknet*s es completamente **efectivo** o por el contrario existen métodos que puedan romper ese requisito.

1.3. Enfoque y método seguido

Dentro de la *Deep Web* existen muchos aspectos a tener en cuenta, el enfoque de este trabajo se ciñe en la explotación de esos contenidos web que pueden ser visitados de formar anónima.

Se describirá como llegar a ellos, las distintas redes que posibilitan el anonimato del usuario, los métodos existentes para acceder a cada una de estas y finalmente se verificará la anonimicidad de estas redes, buscando vulnerabilidades que puedan comprometerlas.

La metodología aplicada en este trabajo de investigación es la siguiente:

Definición del Plan de Trabajo

Se definirá el contexto y la justificación de este trabajo de investigación, se plantearán los objetivos, se desarrollará la metodología a seguir y el enfoque del trabajo, se continuará con la lista de tareas y la planificación y finalmente se desarrollará un estado del arte con el objetivo de descubrir la información que existe sobre la *Deep Web*, qué redes existen, cómo se puede acceder a ellas, qué servicios ofrecen, etc.

Introducción

Se tratará de establecer una definición sobre la *Deep Web*, se debatirá sobre las distintas acepciones que se pueden hallar en Internet y se tratará de acotar su significado y extensión.

Formas de acceso

Se analizarán las distintas redes que ofrecen anonimato, como surgieron, en qué estado de desarrollo e implantación se encuentran, cómo se puede acceder a ellas, las diferencias existentes y que ventajas e inconvenientes tienen cada una.

Deep Web

Se detallarán que contenidos ofrece y que servicios posibilita la *Deep Web* y en particular la *Dark Web*, y se analizarán los posibles usuarios de esta, constatando las opciones que ofrece a los ciberdelincuentes, pero también discutiendo si su uso principal está monopolizado por estos, o por el contrario va más allá.

Desanonimización

Se buscarán vulnerabilidades que afecten a las redes que conforman parte de la *Deep Web*. Dado que la característica más relevante que ofrecen estas, es el anonimato, se presentarán acciones que pongan en entredicho la anonimicidad

de estas y de paso se darán a conocer los peligros a los que un usuario se puede exponer.

Experimentos prácticos

Se realizará una batería de experimentos prácticos, con el fin de evaluar las redes existentes, los métodos de acceso a cada una, el contenido que se puede encontrar y las pruebas de anonimicidad.

Conclusiones

Se trasladarán unas conclusiones con los resultados finales de este trabajo de investigación.

1.4. Planificación del Trabajo

A continuación, se detallan las **tareas a realizar** y se plasman en un **diagrama de Gantt** estableciendo los límites temporales de cada una:

Orientación en TFM

Se contacta con el director de este Trabajo Fin de Máster para definir el objetivo y propósito de este trabajo de investigación.

Ámbito del TFM

Se establecen los contenidos que aborda el trabajo, así como las tareas que se van a desarrollar.

Documentación previa

Se realiza una búsqueda amplia y general de los datos existentes sobre la *Deep Web* con el objetivo de asentar las ideas iniciales.

Plan de Trabajo

Contexto del TFM

Se realiza una introducción del origen del término *Deep Web* y qué conceptos abarca y se plantean los desafíos que se tratarán de resolver.

Objetivos del TFM

Se explica cuáles son los propósitos de este trabajo de investigación.

Metodología

Se detallan las fases en las que se divide el desarrollo de este trabajo.

Listado de tareas

Se realiza un listado pormenorizado de las tareas con las que se cumplirán los objetivos y desarrollo de este trabajo.

Planificación

Se escenifica un planteamiento de los límites temporales de cada tarea, incluyendo los entregables asociados a cada PEC que componen este trabajo. Todo ello se presenta en un diagrama de Gantt.

Estado de arte inicial

Se indaga y redacta la información encontrada sobre la *Deep Web* y se establece un punto de partida para el inicio de este trabajo.

PEC 1: Entrega

Primer hito de control: Entrega del Plan de trabajo.

Introducción

Se presenta la *Deep Web*, se establece una definición, indicando los contenidos que abarca y su extensión.

Formas de acceso

Introducción

Se plantean las distintas redes que componen la *Deep Web*.

Tor

Se explica el origen de Tor, su finalidad, sus modos de acceso y sus particularidades en relación al resto.

Freenet

Se detalla el nacimiento de Freenet y sus objetivos, así como el modo de acceso y sus características respecto a otras redes.

I2P

Se indica el motivo del nacimiento de I2P, cuál es su objetivo, como se accede y que particularidades tiene frente a otras redes.

Otras alternativas

Se realiza un estudio de otras alternativas de acceso a la *Dark Web*, su origen, su estado de desarrollo y las ventajas e inconvenientes que presentan.

Deep Web

Introducción

Se presentan los servicios que presta al usuario la *Deep Web* y en particular la *Dark Web*.

Contenidos

Se muestran los contenidos que se puedan encontrar en la *Dark Web*.

Servicios

Se lista una serie de servicios que la *Dark Web* ofrece a los usuarios.

Desmitificando la *Deep Web*

Se debate sobre la idea generalizada de que la *Deep Web* es sinónimo de ciberdelincuencia.

Desanonimización

Introducción

Se presentan los problemas de desanonimización que pueden afectar y comprometer a estas redes.

Vulnerabilidades y explotación

Se explican las distintas vulnerabilidades encontradas y los métodos de explotación.

PEC 2: Entrega

Segundo hito de control: Entrega de los apartados: Introducción, formas de acceso, *Deep Web* y Desanonimización.

Experimentos prácticos

Acceso a la *Deep Web*

Se comprueba el acceso a la *Deep Web* a través de las distintas redes que la componen.

Intento de desanonimización

Se trata de explotar alguna vulnerabilidad que afecte a una red y consiga afectar al anonimato.

PEC 3: Entrega

Tercer hito de control: Entrega de los resultados del apartado: Experimentos prácticos, incluyendo el acceso a la *Deep Web* e intento de desanonimización.

Memoria

Redacción de la memoria: Resumen, conclusiones, bibliografía, etc.

Se compila toda la información recogida y se redactan todos los apartados que falten como el resumen, el abstract, las conclusiones, la bibliografía, etc.

Revisión final de la memoria

Se realiza una revisión final de la memoria, comprobando posibles errores ortográficos, gramaticales, semánticos, etc. Se verifica que todos los contenidos de terceros estén referenciados y se marcan en negrita las ideas principales de cada capítulo.

Maquetación de la memoria

Se comprueban que toda la memoria tenga las mismas pautas de estilo.

PEC 4: Entrega Memoria

Cuarto hito de control: Entrega de la memoria.

Video

Preparación del vídeo

Se realiza un guion del vídeo y se provee de todos los materiales necesarios para su consecución.

Grabación y edición del vídeo

Se graba el vídeo y se edita.

Entrega vídeo

Quinto hito de control: Entrega del vídeo.

Defensa

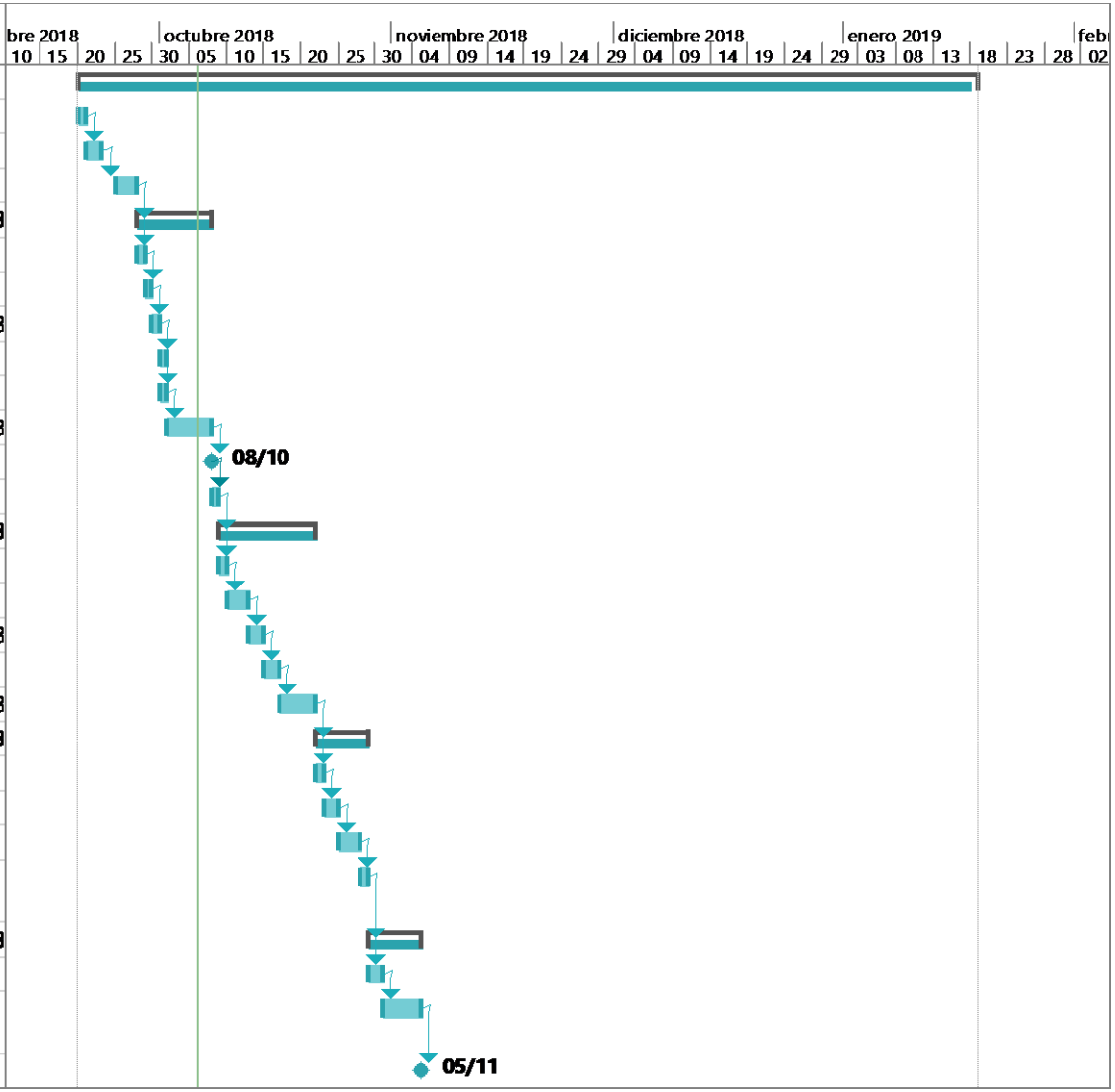
Preparación de la defensa

Se esquematiza una presentación donde se explique el motivo de este trabajo, los análisis realizados, las pruebas llevadas a cabo y los resultados obtenidos.

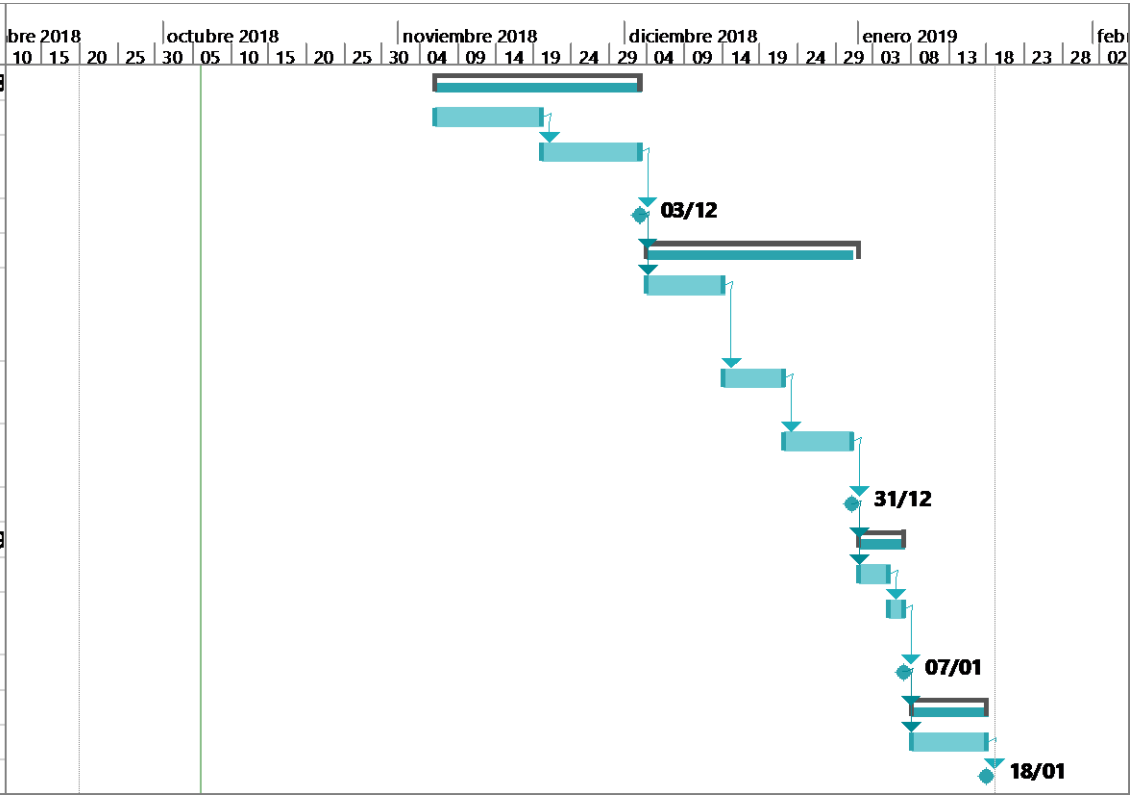
Defensa

Se presenta el Trabajo Fin de Máster.

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**TFM: Un paseo por la Deep We**	**121 días**	**jue 20/09/18**	**vie 18/01/19**
2	Orientación en TFM	1 día	jue 20/09/18	jue 20/09/18
3	Ámbito del TFM	2 días	vie 21/09/18	sáb 22/09/18
4	Documentación previa	3 días	mar 25/09/18	jue 27/09/18
5	**Plan de Trabajo**	**10 días**	**vie 28/09/18**	**dom 07/10/18**
6	Contexto del TFM	1 día	**vie 28/09/18**	vie 28/09/18
7	Objetivos del TFM	1 día	sáb 29/09/18	sáb 29/09/18
8	Metodología	1 día	dom 30/09/1	dom 30/09/18
9	Listado de tareas	1 día	lun 01/10/18	lun 01/10/18
10	Planificación	1 día	lun 01/10/18	lun 01/10/18
11	Estado de arte inicial	6 días	mar 02/10/18	dom 07/10/18
12	PEC 1: Entrega	0 días	lun 08/10/18	lun 08/10/18
13	Introducción	1 día	lun 08/10/18	lun 08/10/18
14	**Formas de acceso**	**13 días**	**mar 09/10/18**	**dom 21/10/18**
15	Introducción	1 día	mar 09/10/18	mar 09/10/18
16	Tor	3 días	mié 10/10/18	vie 12/10/18
17	Freenet	2 días	sáb 13/10/18	dom 14/10/18
18	I2P	2 días	lun 15/10/18	mar 16/10/18
19	Otras alternativas	5 días	mié 17/10/18	dom 21/10/18
20	**Deep Web**	**7 días**	**lun 22/10/18**	**dom 28/10/18**
21	Introducción	1 día	lun 22/10/18	lun 22/10/18
22	Contenidos	2 días	mar 23/10/18	mié 24/10/18
23	Servicios	3 días	jue 25/10/18	sáb 27/10/18
24	Desmitificando la Deep Web	1 día	dom 28/10/18	dom 28/10/18
25	**Desanonimación**	**7 días**	**lun 29/10/18**	**dom 04/11/18**
26	Introducción	2 días	lun 29/10/18	mar 30/10/18
27	Vulnerabilidades y explotación	5 días	mié 31/10/18	dom 04/11/18
28	PEC 2: Entrega	0 días	lun 05/11/18	lun 05/11/18



Id	Nombre de tarea	Duración	Comienzo	Fin
29	**Experimentos prácticos**	**27 días**	**mar 06/11/18**	**dom 02/12/18**
30	Acceso a la deep Web	14 días	mar 06/11/18	lun 19/11/18
31	Intento de desanonimización	13 días	mar 20/11/18	dom 02/12/18
32	PEC 3: Entrega	0 días	lun 03/12/18	lun 03/12/18
33	**Memoria**	**28 días**	**mar 04/12/18**	**lun 31/12/18**
34	Redacción memoria: Resumen, conclusiones, bibliografía, etc.	10 días	mar 04/12/18	jue 13/12/18
35	Revisión final de la memoria	8 días	vie 14/12/18	vie 21/12/18
36	Maquetación de la memoria	9 días	sáb 22/12/18	dom 30/12/18
37	PEC 4: Entrega memoria	0 días	lun 31/12/18	lun 31/12/18
38	**Video**	**6 días**	**mar 01/01/19**	**dom 06/01/19**
39	Preparación del vídeo	4 días	mar 01/01/19	vie 04/01/19
40	Grabación y edición del vídeo	2 días	sáb 05/01/19	dom 06/01/19
41	Entrega vídeo	0 días	lun 07/01/19	lun 07/01/19
42	**Defensa**	**10 días**	**mar 08/01/19**	**jue 17/01/19**
43	Preparación de la defensa	10 días	mar 08/01/19	jue 17/01/19
44	Defensa	0 días	vie 18/01/19	vie 18/01/19



1.5. Estado del arte

En apartados anteriores ya se han mencionado los orígenes del término *Deep Web*, así como se ha plasmado una definición de lo que se entiende por *Deep Web* y que *grosso modo* está formada por esos contenidos web que los motores de búsqueda no indexan, ya sea por decisión del autor de ese contenido, porque no presentan las características para poder ser indexados, o por ser sitios privados entra otras.

También se ha hecho mención a estadísticas y estudios en relación al tamaño de la *Deep Web* frente al Internet convencional o *Surface Web* y la clasificación de la primera en varios niveles según la complejidad de acceso y el tipo de contenidos.

En los últimos años se ha ido incrementado la censura por parte de estados y gobiernos que desvirtúan el contenido de la *World Wide Web*, marcando que pueden o no ver sus súbditos, según sea de interés para los primeros.

Como quiera que el acceso a cualquier página web conlleva la generación de un rastro que identifica inequívocamente al usuario, se hace necesario buscar fórmulas que permitan el consumo de contenidos web de forma totalmente anónima.

Para dar una respuesta a esa necesidad surgen las redes anónimas formadas por contenidos ocultos al Internet convencional y a las que solo se puede acceder después de ejecutar una serie de procedimientos que anonimizan la conexión del cliente de forma que no pueda ser identificado.

El conjunto de estas redes anónimas es lo que se conoce como *Dark Web* y cada una de ellas por separado recibe el nombre de *Darknet*. Estas redes en conjunto con otra serie de contenidos web aglomeran la *Deep Web*.

Las *Darknets* **más conocidas** son **TOR**, **I2P** y **Freenet**, aunque existen muchos más proyectos entre los que se pueden citar: HORNET, Riffle, GNUnet o ZeroNet entre otros. (4) (5) (6)

Aunque cada *Darknet* tiene sus métodos de acceso, el objetivo común de todos ellos es establecer una comunicación anónima, mediante un software específico o mecanismo, de tal forma que no se pueda asociar una dirección IP con un usuario en concreto.

Otras opciones para conectarse y explorar la *Dark Web* son distribuciones basadas en Linux que incorporan estas herramientas y mecanismos para establecer la comunicación. Si bien las más conocidas son Tails, Qubes o Whonix, existen otras como Linux Kodachi, Tens, Jondo o IprediaOS por citar algunas de ellas. (7) (8) (9)

Por ser la *Darknet* más popular, existe mucha más información publicada en fuentes abiertas sobre Tor, que sobre otras redes anónimas.

Por ejemplo, respecto al contenido que se puede encontrar en la red Tor, es muy popular *The Hidden Wiki*. Se trata de un directorio donde encontrar servicios financieros, comerciales, información de seguridad y anonimato, blogs, foros, redes sociales, servicios de email, libros, música, contenido audiovisual o porno.

También existen buscadores como DuckDuckGo o Torch que tienen indexado multitud de ficheros con extensión .onion, que es la nomenclatura de extensión utilizada en Tor.

Además de estos puntos de entrada a la red, existen otros **contenidos** como **comunidades de usuarios**: 8 chan es un ejemplo de ella; servicios de mail como Mail2Tor; foros especializados en diversas temáticas: Moneybook se encargar de la economía sumergida en la *Darknet*, mientras que en ResisTor se centra en Tor, *Deep Web* o seguridad informática entre otros temas.

Otras páginas web que se pueden encontrar en la red Tor son **blogs** como El Binario, directorios de contenido **multimedia** como FileStory o bibliotecas de libros como Imperial Library.

También existen sitios web que tratan sobre las **criptomonedas**, así como otras que brindan la posibilidad de tener monederos virtuales ocultos y anónimos. El interés por estas divisas se debe a que los pagos que se realizan en la red Tor suelen llevarse a cabo en alguna de estas criptomonedas, generalmente en Bitcoin o Monero.

En relación con la **ciberdelincuencia** hay páginas web donde se pueden adquirir **drogas** o contratar hackers para que lleven a cabo acciones ilegales, existen otras donde se pueden comprar **armas** o explosivos, contratar a sicarios o sitios de intercambio de **pornografía infantil**.

Pero esta red anónima no solo ofrece servicios a través de HTTP o HTTPS. También se puede hacer uso de otros servicios como FTP, TELNET, POP3, SMTP, JABBBER, XMMP o IRC. (10)

Por ejemplo, existe un servicio de **mensajería instantánea** denominado CoyIM que hace uso del protocolo XMMP. Sigaint o ProtonMail son servicios de **correo electrónico** que hacen uso de los protocolos propios de estos servicios como SMTP, POP3 o IMAP. Hay servicios de **almacenamiento e intercambio de archivos** como OnionShare. (11) (12) (13)

Otras opciones que nos brinda la red Tor es lo que se conoce como "*torificar*" aplicaciones, es decir, utilizar estas de forma segura y anónima. Por ejemplo, herramientas administrativas como Telnet o SSH, aplicaciones de mensajería instantánea, clientes de correo electrónico como Mozilla Thunderbird o protocolos de transferencia FTP y WGET pueden ser *torificadas*. Este proceso se lleva a cabo mediante la combinación de un servidor de *proxy* como Privoxy o Polipo y la herramienta Torsocks, que

garantiza que las peticiones DNS se realicen de forma segura y rechaza el tráfico UDP de la aplicación en uso. (14)

Como hemos visto anteriormente, la anonimicidad es la propiedad esencial que se busca cuando se navega por estas redes, cualquier vulnerabilidad que permita identificar a los usuarios estaría rompiendo el objetivo perseguido.

Pero como en cualquier software o producto, siempre existen **vulnerabilidades**. En Tor se han descubierto algunas como las que se muestran a continuación.

En el año 2017 se descubrió un problema en el **navegador** Tor Browser, el cual al conectarse a un enlace del tipo “file://”, redirigía directamente al servidor web revelando la IP del usuario sin aplicar los mecanismos de ocultación que en el resto de comunicaciones si lleva a cabo.

Otra vulnerabilidad reportada en septiembre de 2018 residía en el *plugin* “NoScript”, encargado de bloquear JavaScript, Java, Flash y otros elementos potencialmente dañinos para el usuario. El modo de seguridad más alto del navegador, con las versiones 5.0.4 y 5.1.8.6 de este *plugin*, puede ser burlado al permitir ejecutar cualquier fichero JavaScript, mostrando al igual que en la vulnerabilidad anterior la IP del usuario.

Otros métodos que posibilitan la desanonimización de la red Tor, son por ejemplo ataques basados en técnicas de confirmación de tráfico. Un atacante podría introducir nodos ilegítimos en la red Tor que, aprovechándose del mecanismo de funcionamiento de esta, relevaría la IP del servicio oculto atacado.

En los próximos apartados se ahondará más en profundidad sobre varios de los puntos aquí tratados.

2. INTRODUCCIÓN

Los motores de búsqueda, gracias a una aplicación denominada crawler, spider o araña en castellano, recorren las páginas web saltando de unas a otras a través de los enlaces y generando una base de datos con todos esos contenidos indexados. Sin embargo, existen otros elementos, que, por diversos factores, no son indexados. Ese conjunto de contenidos que no están indexados por los motores de búsqueda es lo que se denomina *Deep Web*. De forma antagónica a este término, surge la *Surface Web* o *Clearnet*, como la definición de la parte de Internet que si se encuentra indexada por los buscadores.

Ese **contenido no indexado** está formado por los siguientes elementos:

- Páginas web de **acceso restringido** o privadas: Aquellas que necesitan de unas credenciales para poder ser vistas.

- Páginas web y servicios **ocultos intencionadamente**: Son todos esos elementos web y resto de servicios que necesitan de un software o protocolo específico para poder ser explotados.

- Páginas web de **acceso limitado**: Se refieren a todas las páginas web que están configuradas para que sean excluidas del indexado de los robots de los buscadores.

- Páginas web **dinámicas**: Se trata de aquellas páginas web que se generar de forma dinámica, dependiendo, por ejemplo, de los datos recibidos en un formulario.

- Páginas web **contextuales**: Son elementos web que muestran distintos contenidos según determinados parámetros, como pueden ser el rango de direcciones, la ubicación, el historial de navegación, etc.

- Páginas web **no enlazadas**: Todos aquellos elementos web que no tienen enlaces desde otras páginas, por lo que el buscador no es capaz de rastrear, son las denominadas páginas sin enlaces entrantes.

- Contenido web programado: Elementos web que solo son accesibles a través de enlaces generados por JavaScript, o descargados dinámicamente a partir de servidores web a través de implementaciones en lenguajes Flash o Ajax.

- Sin contenido HTML: Son elementos con formatos específicos que los motores de búsqueda no son capaces de indexar porque no los soportan.

Una imagen muy relevadora y conocida del tamaño de la *Deep Web* es el iceberg. En un principio se decía se la *Deep Web* era el 96% del contenido web, mientras que la *Surface Web* era del 4%.

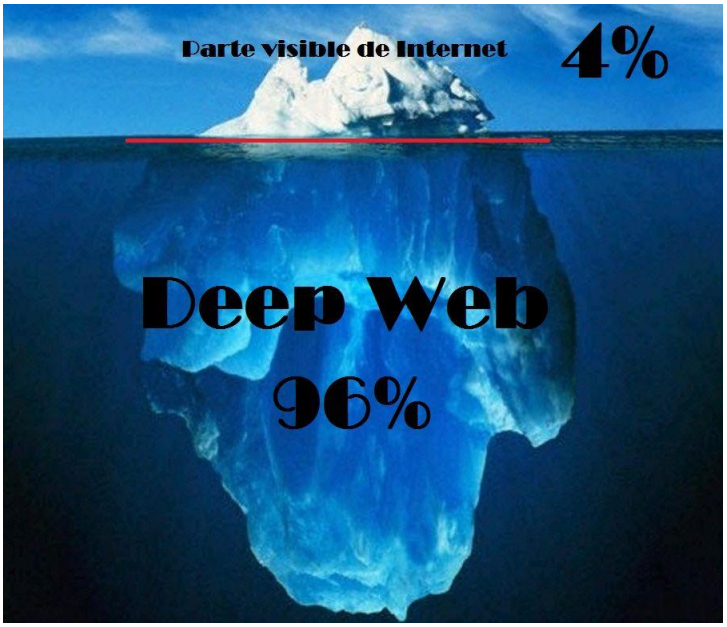


Ilustración 1: Iceberg *Deep Web*
Fuente: statut-auto-entrepreneur.info

Pero **la realidad se asemeja más a esta otra imagen**, en la que dentro de la *Deep Web* se engloban grandes cantidades de información asociada a informes médicos, archivos financieros, repositorios científicos, información académica o bases de datos gubernamentales y administrativas. Todo este contenido formaría parte del primero de los elementos de la *Deep Web* citando anteriormente: las páginas web de acceso restringido o privadas.

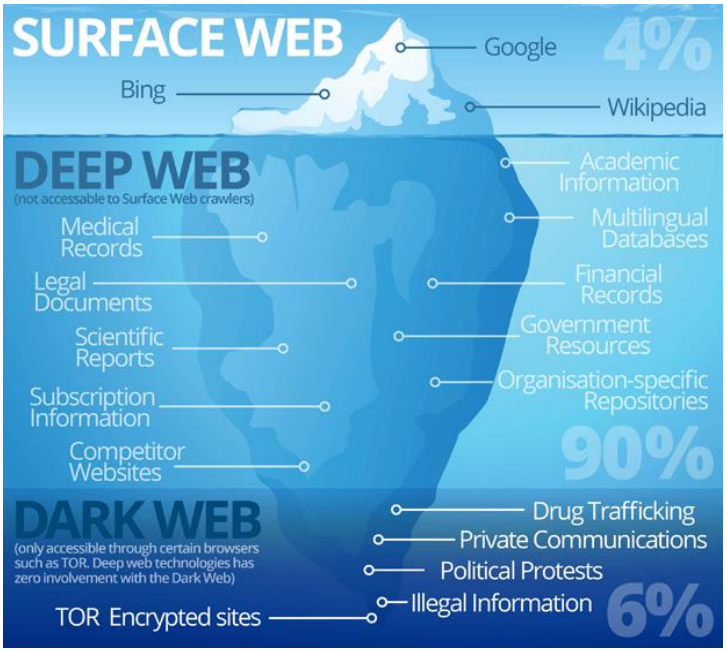


Ilustración 2: Iceberg *Deep Web*
Fuente: dailystar.co.uk

Y otro de los elementos, las páginas web ocultadas intencionadamente, agruparía el conjunto de todas las redes que se denomina *Dark Web*. En la imagen anterior se indica que ocupa un 6%, aunque otras fuentes lo establecen en un 0.1% de la *Deep Web*.

Aún así, esa imagen deja fuera de la *Deep Web* el resto de elementos que se citaban anteriormente como las páginas web dinamicas, contextuales, no enlazadas, etc. Asimismo separa la *Dark Web* de la *Deep Web*, cuando debería ser parte de esta.

Sea como fuere, se debe despejar la confusión existente entre *Deep Web* y *Dark Web* ya que en muchas ocasiones se tratan como lo mismo y no lo son. Como se ha explicado anteriormente: la ***Deep Web*** hace referencia a todo el **contenido** de Internet **no indexado** por los motores de búsqueda. **Dentro de esta,** se encuentra la ***Dark Web*** que aglutina el conjunto de todas **páginas web ocultas** intencionadamente y que está **formada** por varias **redes**. **Cada una** de estas redes es una ***Darknet***, y cada una tiene un protocolo o tecnología de acceso de forma que la navegación dentro de esta sea de forma anónima para los usuarios. (15) (16)

3. FORMAS DE ACCESO

3.1. Tor

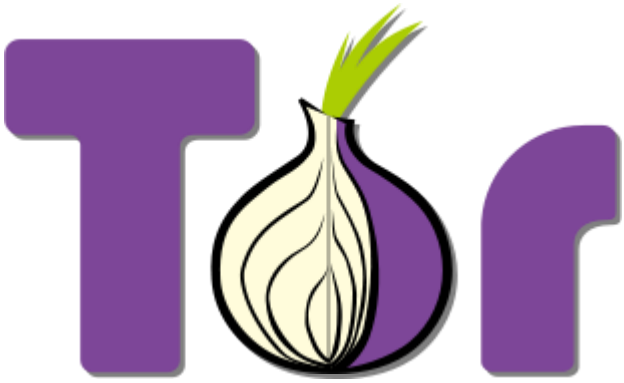


Ilustración 3: Isologo de Tor
Fuente: The Tor Project

La *Darknet* con mayor popularidad es Tor. Tor, son las siglas de The Onion Router. Se trata de un proyecto que nace en el año 2002 con el objetivo de crear una red de comunicaciones distribuida, de baja latencia, superpuesta sobre Internet y donde las rutas de los paquetes entre los usuarios **no revelen** su **dirección IP**, manteniendo en todo momento la integridad y el secreto de la información.

Su origen se encuentra en un proyecto del Laboratorio de Investigación Naval de los Estados Unidos. Actualmente está en manos de **The Tor Project**, una organización sin ánimo de lucro orientada a la investigación y la educación, radicada en Massachusetts y que ha sido financiada por distintas organizaciones. Como líder del proyecto se encuentra Roger Dingledine.

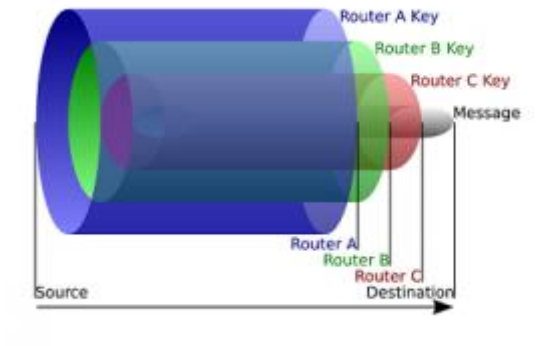


Ilustración 4: Cifrado por capas
Fuente: www.patexia.com

Su funcionamiento se basa en prescindir de realizar una conexión directa entre el cliente y el servidor, y crear un camino o **circuito** a través de varios nodos. El **paquete** se envía **cifrado** de forma incremental con las claves de todos estos nodos, estableciendo **capas**, de ahí el símil con la **cebolla**. A medida que va pasando por cada uno de los nodos se va descifrando y descubriendo la dirección del siguiente nodo por el cual tiene que continuar el paquete. Así, hasta llegar al nodo final.

En el siguiente ejemplo, *Alice* quiere enviar un mensaje a *Bob*.

En primer lugar, el cliente de Tor de *Alice* debe de descargar la información sobre los nodos de la red.

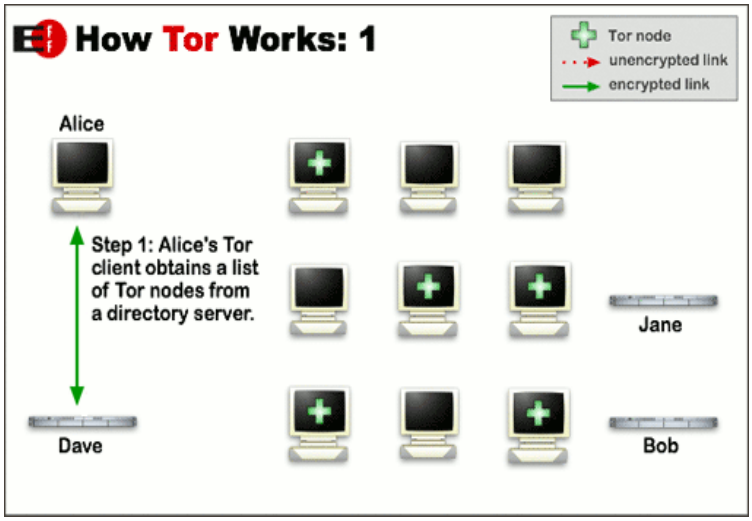


Ilustración 5: El cliente Tor de Alice obtiene la lista de nodos
Fuente: The Tor Project

A continuación, establece el circuito y consigue las claves públicas de todos los nodos que conforman el camino. El cliente de *Alice* cifra el paquete con la clave del último nodo de la ruta acompañado de las instrucciones para llegar al nodo destino. Posteriormente, se vuelve a cifrar con la clave del penúltimo nodo y así hasta que se termina con todos los nodos de la ruta.

Con este proceso ya se obtiene el paquete de datos listo para enviarlo. El cliente de *Alice* conecta con el primer nodo de la ruta, y le envía el paquete. Este nodo lo descifra, y sigue las instrucciones que ha obtenido para enviar el resto del paquete al nodo siguiente. Éste lo descifrará de nuevo y lo envía al siguiente, y así sucesivamente. Los datos llegarán finalmente al nodo de salida, que enviará el mensaje a *Bob*.

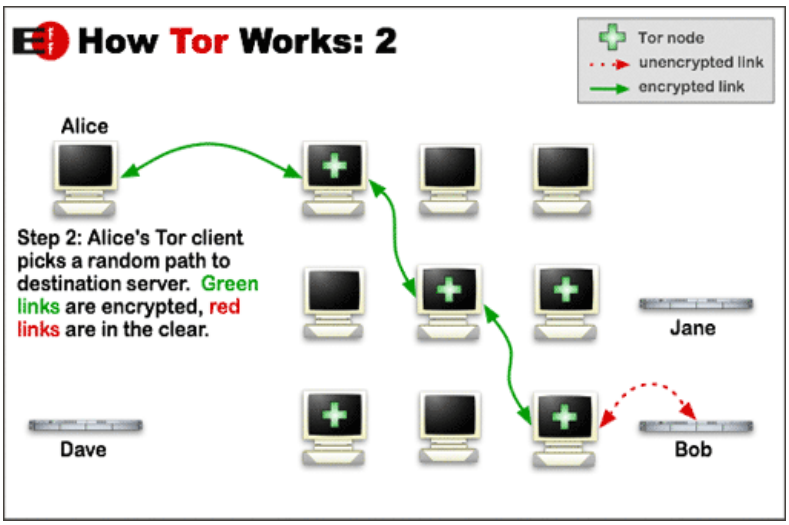


Ilustración 6: El cliente Tor de Alice establece un circuito
Fuente: The Tor Project

Para mayor eficiencia, Tor usa el mismo circuito para las conexiones que ocurren dentro de los mismos diez minutos aproximadamente. Las solicitudes posteriores reciben un nuevo circuito para evitar que las personas vinculen sus acciones anteriores con las nuevas. (17) (18) (19) (20)

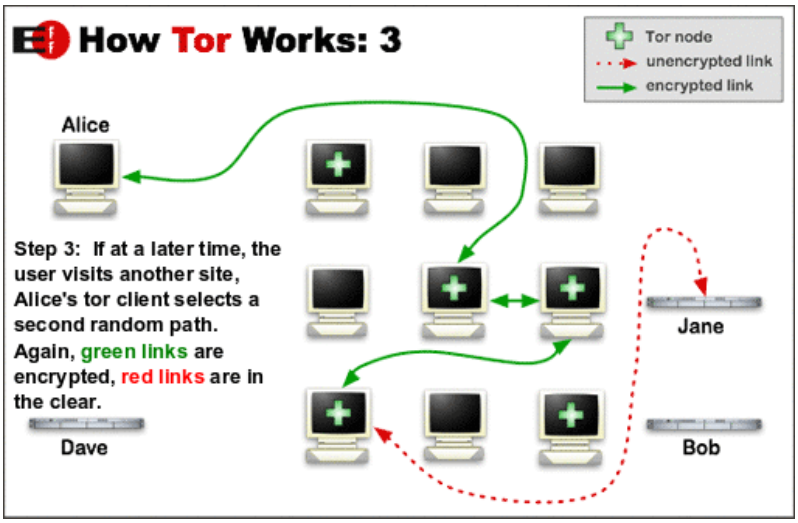


Ilustración 7: El cliente Tor de Alice establece otro circuito para conectarse con Jane
Fuente: The Tor Project

Otra característica es que Tor es una red de tipo *outproxy*. Esto quiere decir que es capaz de comunicarse con otras redes, operando con su misma arquitectura.

3.2. Freenet

Ilustración 8: Isotipo de Freenet
Fuente: The Freenet Project Inc.

Freenet es un proyecto nacido en el año 1999 de la mano de Ian Clarke. Se trata de un sistema de nodos **distribuido y descentralizado** de almacenamiento y recuperación de información que proporciona una navegación anónima.

Estos nodos no están jerarquizados y se transmiten los paquetes de datos entre ellos. Pueden funcionar como nodos finales o intermedios de enrutamiento, alojando cada uno, documentos asociados a claves y una tabla de enrutamiento que asocia los nodos con un historial. Esto quiere decir que no hay conexiones directas ni reconocimiento de

nodos, algo que garantiza un alto nivel de anonimato para todos los usuarios.

Posee un funcionamiento muy **parecido a una red P2P**, con la salvedad de que una vez que se incluye un elemento web nuevo, el fichero queda insertado en la red, por lo que una vez finalizada la inserción ya no hace falta que el nodo siga operativo para poder acceder al contenido.

El principio de P2P implica que un servicio estará disponible siempre y cuando al menos haya un nodo que lo haya utilizado. Esto reduce la posibilidad del éxito de ataques de denegación de servicio, así como evita la dependencia de servidores centrales para que el servicio siga en pie, como si ocurre en Tor.

Dentro de la propia Freenet se pueden crear otras redes propias que no estén conectadas al resto de redes. Esto permite crear un entorno con mayor privacidad que en Tor.

Otra de las diferencias respecto a la red Tor es que Freenet es de tipo *inproxy*, es decir, no es capaz de conectarse con otras redes.

Para acceder a esta red es necesario descargar una aplicación desde su sitio online, la cual configura la conexión del cliente. Presentado el interfaz de Freneet, al acceder a http://localhost:8888/ se debe definir el tipo de conexión: *opennet* para la conexión a cualquier usuario o bien *Darknet* para establecer la conexión al Freenet de un amigo, previo intercambio de referencias, y obteniendo mayores garantías de anonimicidad al conocer con certeza la ruta de la conexión. (21) (22) (23)

3.3. I2P

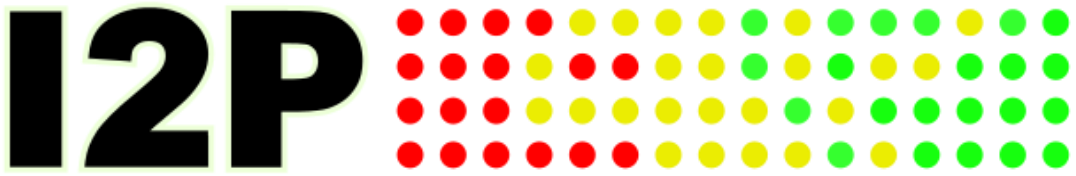


Ilustración 9: Imagotipo de I2P
Fuente: I2P

I2P, Invisible Internet Project es una red diseñada para proteger la información que se transmite por ella. Para ello, **implementa una capa** en la que las aplicaciones pueden **enviar mensajes** entre sí de forma **anónima** y segura. Todas las comunicaciones se realizan **cifradas** de extremo a extremo

Su funcionamiento se basa en el concepto de **túnel**. Cada aplicación que quiere usar la red tiene un router I2P que se encarga de crear túneles de

entrada y salida, es decir, una secuencia de pares que trasladan el mensaje en una sola dirección. Cuando un cliente quiere enviar un mensaje a otro cliente, el primero envía ese mensaje a través de uno de sus túneles de salida hacia uno de los túneles de entrada del segundo. Para enviar un mensaje de respuesta se debe crear un nuevo túnel.

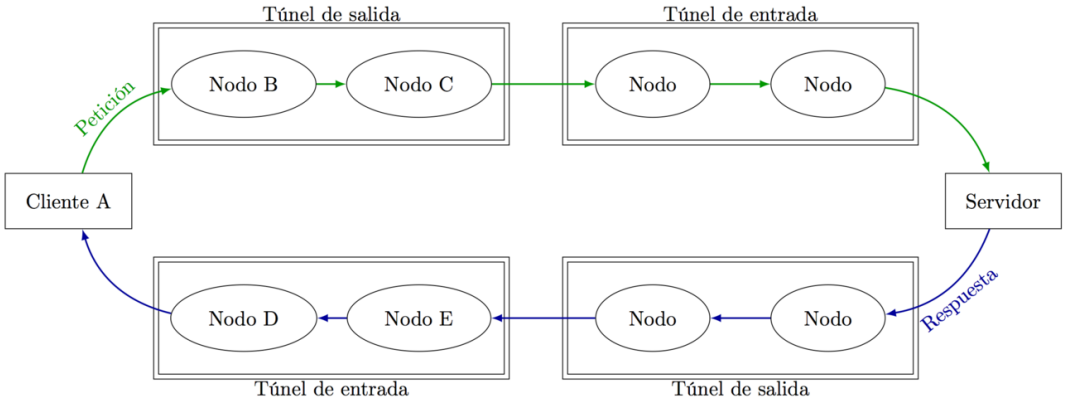


Ilustración 10: Esquema de funcionamiento de los túneles de entrada y salida en I2P
Fuente: Omicrono

La primera vez que un cliente quiere contactar con otro, debe consultar la base de datos de red, esta es una tabla de hash distribuida que permite encontrar eficientemente los túneles entrantes de los otros clientes. Posteriormente, el resto de mensaje, incluyen estos datos, por lo que no requieren ulteriores búsquedas en la base de datos de red.

Se usa un cifrado por capas, por lo cual cada router sólo puede descifrar una capa. La información descifrada contiene la IP del router siguiente, así como la información cifrada para ser enviada. Cada **mensaje** se considera un garlic clave o **diente de ajo**, y en conjunto con las instrucciones de entrega, generan un garlic message o mensaje ajo, de ahí que se indique que esta red tiene enrutamiento ajo.

Mientras que Tor ofrece *outproxy* por defecto, I2P ha sido desarrollado dejando que sean las aplicaciones las que se encarguen de facilitar esta funcionalidad. (24) (25) (26)

3.4. Ventajas e Inconvenientes

Como se ha visto, cada *Darknet* tiene sus algoritmos de funcionamiento y peculiaridades lo que les otorgan una serie de ventajas e inconvenientes a unas respecto a las otras.

En cuanto a **garantías de anonimato**, Freenet permite la creación de una red de amigos (*Darknet*), es decir, entre nodos confiables, lo que permite

establecer una red muy segura. Por el contrario, en Tor e I2P hay una predisposición de confianza hacia los nodos, aunque existen mecanismo para denunciar un nodo con comportamiento sospechoso, no existen garantías de la identidad del responsable de este, por lo que si una misma organización sostuviese un buen número de ellos, es posible que el circuito llegue a pasar por todos esos nodos y por tanto desanonimizar al usuario.

Respecto al **mecanismo de funcionamiento**, Tor dispone de unos nodos que actúan como servidores de directorios, asociando a cada nodo de la red una serie de información, que se conoce como router descriptor, un ataque a estos nodos produciría la caída de la red al no poder encontrar los nodos para crear el circuito. Por el contrario en Freenet, al basarse en el concepto P2P, siempre estará disponible un servicio cuando al menos haya un nodo, al igual que en I2P donde base de datos de la red está distribuida.

En relación a la **disponibilidad de los datos**, en Freenet al subir un contenido, este se distribuye por la red, siendo innecesario que permanezca online el autor de la publicación. En Tor e I2P esto no sucede, es necesario que esté levantado el servicio oculto para poder acceder a su información.

Como se ha indicado en apartados anteriores, Freenet no permite la comunicación con otras redes, es decir, es una red de tipo ***inproxy***. Por el contrario, tanto Tor de forma nativa, como I2P a través de aplicaciones de terceros, permiten conexiones de tipo ***outproxy***.

Respecto a la **velocidad**, la más rápida es I2P, gracias al diseño optimizado de los servicios ocultos. Por el contrario, Freenet es la más lenta por varios factores: el respaldo solamente por usuarios anónimos y no por grandes corporaciones, el cifrado bit a bit, etc.

Finalmente, en cuanto a respaldo de la **comunidad**. Tor es la que tiene un mayor número de desarrolladores detrás, así como de recursos económicos frente a Freenet e I2P. Esto hace que su desarrollo sea más rápido y exista mayor documentación, lo que implica que lo utilicen más usuarios y en definitiva su popularidad sea mayor. Esto que a priori es una ventaja, puede convertirse también en la mayor desventaja. La popularidad de una herramienta o tecnología implica que un mayor número de individuos traten de romper los mecanismos de seguridad y encuentre vulnerabilidades, que si no son corregidas puede ocasionar la explotación de estos agujeros de seguridad con las consecuencias que estas prácticas pueden llegar a tener.

3.5. Otras alternativas

Sin lugar a duda, Tor, Freenet y I2P son las *Darknets* más conocidas dentro de la *Dark Web*, pero existen otras alternativas que, ya sea mediante otra tecnología o el uso de algoritmo distintos, persiguen el mismo objetivo que las primeras y, que no es otro que el anonimato del usuario. A continuación, se presenta un listado de estos otros proyectos, sus características y sus particularidades:

HORNET, siglas de High-speed Onion Routing at the Network Layer es un proyecto teórico desarrollado por 6 academicos de la Escuela Politécnica de Zurich. Se basa en la misma idea que Tor pero busca la eficiencia en la transmisión de los datos entre los nodos con el fin de **ganar en velocidad**, sin duda, unos de los grandes inconvenientes de la red Tor.

Para conseguir esa celeridad, HORNET elimina el almacenamiento del estado en los nodos intermedios, asi como las claves de cifrado e información de la ruta, dejando esa tarea para los nodos finales. De esta forma, al reducir el trabajo de los nodos intermedios, se espera un aumento de la velocidad, los investigadores aseguran que el tráfico se procesaria a 93 Gb/s. Esta es la teoría, ya que en la práctica se trata de un proyecto inviable, ya que se necesitaría revisar todos y cada uno de los pares que formarían la red, conllevando una gran inversión económica y participación de la comunidad. (27) (28)

Riffle, es un proyecto en desarrollo realizado por investigadores del Instituto Tecnológico de Massachusetts. Al igual que HORNET, se basa en Tor, pero en este caso persigue **aumentar la seguridad** y evitar las vulnerabilidades encontrada en esta última red.

Para conseguir este objetivo, hace uso de un enrutado anónimo, es decir, los datos no solo se envían a un solo nodo en cada salto dentro del circuito, si no que se realiza el envio a varios, de tal forma que se dificulta rastrear los nodos por los que ha pasado el paquete de datos y por tanto localizar su emisor. Esta tecnologia recibe el nombre de *mixnet*.

En cuanto al incremento de velocidad, resulta ser 10 veces mayor que Tor, gracias a que el sistema de comprobación hace uso de un menor ancho de banda. (29) (30) (31)

GNUnet, es una red enfocada en el intercambio de archivos de forma anónima gracias a la utilización de **redes P2P descentralizadas**. Este anonimato se consigue en base a dos premisas: la reescritura del origen y la redirección. La primera busca desconcertar al atacante, al no poder duducir el origen del mensaje. Con la segunda se trata de hacer que el tráfico propio no se diferencie de ajeno.

Además, todas las comunicaciones se realizan entre pares mutuamente autenticados. La autenticación funciona haciendo que cada *peer* firme una clave secreta de sesión con su clave RSA. Además, la clave de sesión está cifrada con la clave pública de otro *peer*. Esa clave se utilizará luego para cifrar la comunicación entre los dos *peers* empleando 256-bit AES.

Finalmente, otra caracteristica de GNUnet es el modelo económico de archivos. Mediante la asignación de una prioridad en las peticiones, los pares atienden a unas antes que a otras, dependiendo de si el par que emite la petición tiene un grado elevado de confianza o no para el receptor. Esta confianza se adjudica dependiendo de como ha respondido el primer par a una peticion de importancia. (32)

ZeroNet, es una **red descentralizada** basada en **P2P** que tiene apenas 4 años de vida. Para acceder a esta red es necesario descargar una aplicación desde su sitio online que configura la conexión del cliente. Una vez dentro, se presenta una página con las distintas opciones que ofrece: ZeroBoard es su chat descentralizado, ZeroMail su servidos de correo electrónico cifrado, ZeroTalk la comunidad descentralizada, el buscado se denomina ZeroSearch (aunque hay otros como Kaffiene Searh o Zearch), también es posible crear encuestas a través de ZeroPolls, o un directorio de citas como ZeroQuotes, un monedero de Bitcoins denominado ZeroWaller y hasta un servicio de mapas, cómo no, denominado ZeroMaps. (33)

4. *DEEP WEB*

4.1. Introducción

Como se veía en el Capítulo 2. Introducción, la *Deep Web* está formada por varios elementos web, entre ellos, esas páginas web que no desean ser indexadas por los buscadores y permanecen ocultas de forma intencionada. Estás páginas son las que forman la *Dark Web*, que será el objeto de estudio de los próximos apartados.

4.2. Contenidos

Los contenidos que podemos encontrar en la *Dark Web* son muy variados y aunque cada *Darknet* posee los suyos propios, existen algunos que pueden estar replicados en más de una de estas redes. Incluso existe la posibilidad de acceder a páginas de la *Surface Web* a través de ellas, como, por ejemplo, a Facebook desde Tor: https://facebookcorewwwi.onion/ (34)

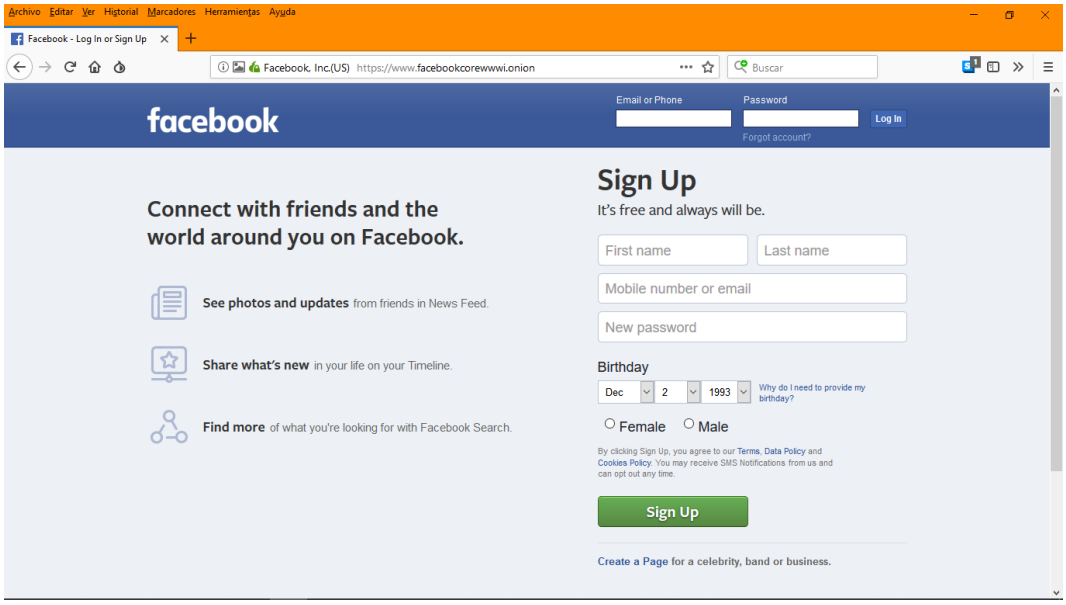


Ilustración 11: Captura de pantalla de la red social Facebook en Tor

A continuación, se muestran ejemplos de que se puede encontrar en las tres *Darknet*s más conocidas.

Contenido en Tor

En Tor, como en la *Surface Web* es una práctica habitual iniciar la navegación a través de un buscador. Uno de los más conocidos en la actualidad es DuckDuckGo, aunque existen otros como Torch, Not Evil, etc. Otra forma de entrada al universo Tor es a través de la popular The Hidden

Wiki, un directorio de enlaces .onion organizados por categorías o La Wiki Oculta, un compendio de links en español.

Sea cual sea el camino de entrada, en Tor se pueden encontrar:

Foros de temática generalista como 8 chan, Cebolla Chan o Café Cebolla, pero también otros enfocados en materias más específicas como Hackplayers en el hacking ético o Privacidad global centrado en la privacidad y anonimato a través de software libre.

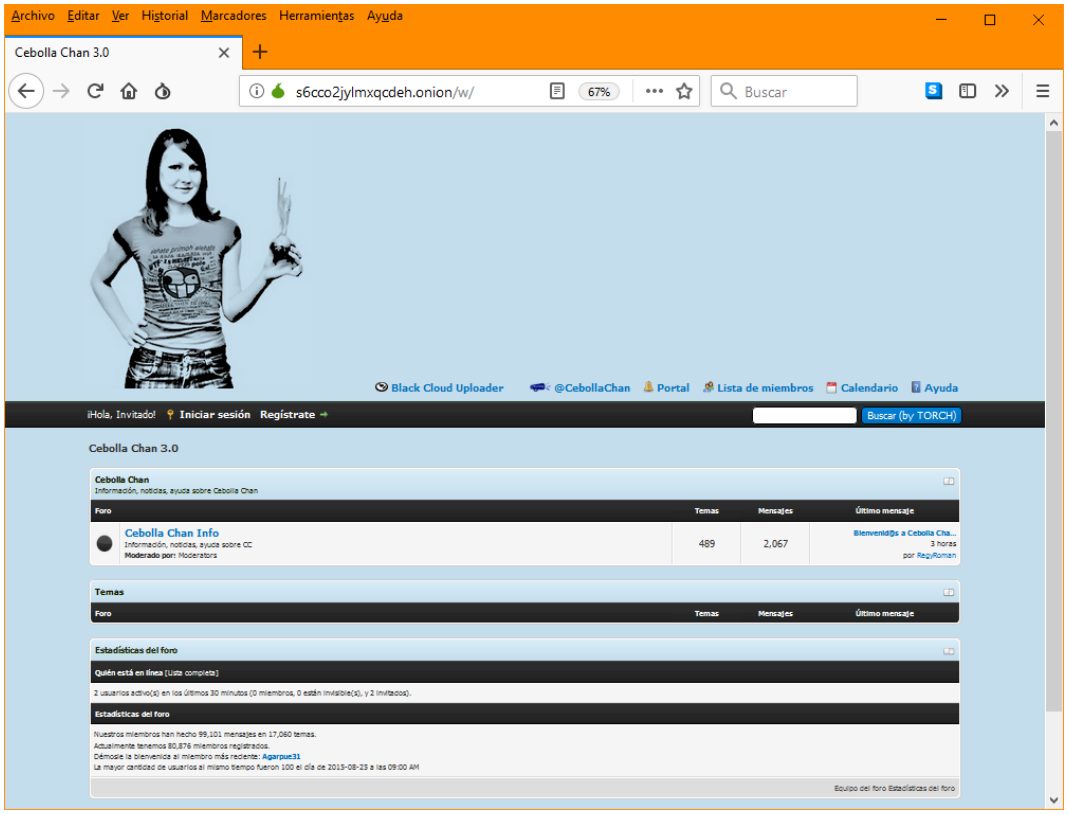


Ilustración 12: Captura de pantalla del foro Cebolla Chan en Tor

Existen **bitácoras** sobre informática, software, redes y seguridad, como por ejemplo El Binario; otros se centran en la *Deep Web* como Hasta Cuando, accesible también desde Freenet e I2P e incluso hay blogs particulares, como el del periodista Mike Tigas.

También es posible encontrar servicios de ***streaming*** de música como Deep Web Radio o descargar ***torrents*** desde la conocida página The Pirate Bay en su versión para Tor.

Hay un gran número de repositorios de **libros**, por citar algunos de ellos: Biblioteca Castor, Imperial Library, The Last of PAPYREFB2, the Incorret Library o Comic Book Library, entre otros.

Enciclopedias online basadas en la tecnología Wiki como Enziclopedhia, disponibles tanto en Tor como en I2P.

Existen otras páginas donde encontrar un *mirror* de WikiLeaks, lugares para intercambiar denuncias como SecureDrop o Cryptome que agrupa documentos etiquetados como confidenciales por diversos gobiernos.

Múltiples **servicios financieros**, monederos virtuales anónimos como Hidden Wallet o Onion Wallet, sitios de adquisición de criptomonedas basadas en el algoritmo Blokchain pero con el registro de transacciones oculto como Litecoin o Dash. Pero también hay otros servicios de dudosa legalidad como por ejemplo la posibilidad de hacerse con cuentas de PayPal en The Paypal Cent, KryptoPayPal o PayPal Bazar; tarjetas de crédito en Premium Cards o dinero falsificado en Guttenbergs Print.

También existen múltiples **servicios comerciales**, quizás sea la categoría que agrupe más opciones ilegales. Artículos tecnológicos de Apple a precio muy inferiores a los de mercado, en Apple Palace World o de Samsung en Samsungstore. Armas y munición en Guns Dark Market. Pero sin duda el producto que más se comercia en Tor son las drogas: Dream Market, Drug Market o Green Road son solo algunos de los mercados online donde poder conseguir estas sustancias.

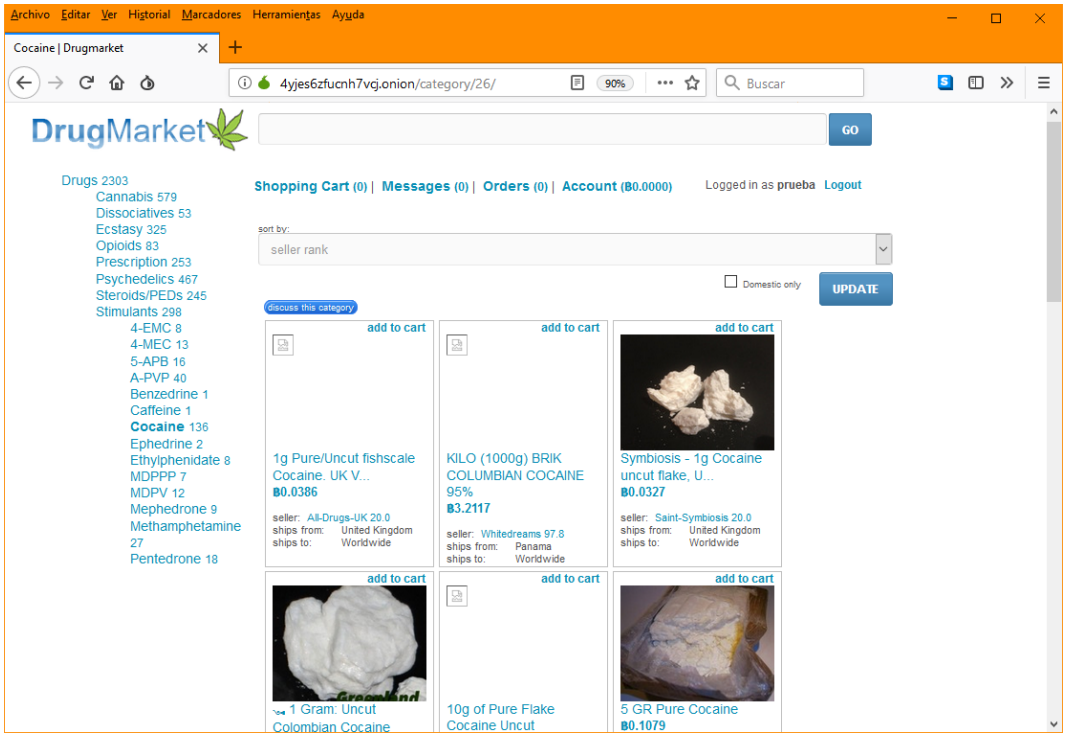


Ilustración 13: Captura de pantalla del mercado de drogas DrugMarket en Tor

Y finalmente, el **porno**, ya sea gratuito o de pago, es otro de los caballos de batalla de las Fuerzas y Cuerpos de seguridad en esta red, debido al intercambio de pornografía infantil. (35) (36) (37)

Contenido en Freenet

El punto de acceso en Freenet es Enzo's Index, que engloba la mayoría de sitios web de esta red ordenados por categorías. Aunque existen otros como The Filtered Index, sin enlaces a sitios porno o Nerdageddon, donde se ha eliminado el contenido más ofensivo.

Muchos de los contenidos versan sobre la propia red Freenet: cómo funciona; cómo se pueden implementar servicios de mensajería, de chat, foros; cómo publicar en Freenet, o códigos de buenas prácticas en la red.

Pero también se pueden encontrar **foros** donde se discute sobre temas tan variopintos como software, seguridad, ciencia, política o religión. Hay **blogs**, algunos de los más conocidos son: Hasta Cuando, Memorias del Fuego o Mr Bamboo's personal flog.

Se pueden localizar repositorios de **libros** electrónicos como Biblioteca Calibre o música en The Best-Selling Music Albums of All Time y Music for Masses así como películas y series en TV Episodes.

Y también existen **enciclopedias** como WikI2P, disponible también en la red I2P.

Contenido en I2P

En I2P, es posible tomar como referencia de punto de acceso INR. Se trata de un directorio que recoge la mayoría de los servicios ocultos en I2P. También, se puede acceder a I2P Wiki, una wiki que recoge *eepsites*, término con el que se denomina a los sitios en la red I2P y otros recursos variados.

Existen **foros** como el de ZZZ, uno de los desarrolladores de I2P, **blogs** como Killyourtv que aporta información técnica de utilidad, así como manuales y guías variadas, o Shadowlife donde se discute sobre el anonimato y la privacidad.

También es posible acceder a un buscador de ***torrent*** con *Torrent* Finder, o subir archivos a través de Postman Tracker.

El PasteBin de I2P se denomina PasteThis y GIT Histing brinda la opción de publicar proyectos de desarrollo de software. (38)

Estos son algunos de los principales contenidos que conforman las tres principales *Darknet*s. El número de contenidos, como es lógico, es mayor en Tor que en Freenet y I2P, debido a que el número de usuarios de la primera también es mayor que en las otras dos. No obstante, es interesante destacar la existencia de algunas páginas en las tres redes como el blog Hasta Cuando.

También es relevante, la migración de algunos sitios famosos, como el portal de venta de drogas Silk Road en Tor, que en su nuevo periplo después de haber sido cerrado por el FBI se ha trasladado a I2P.

4.3. Servicios

Las *Darknets* no solo proporcionan contenidos de tipo web, sino que también ofrecen servicios típicos de Internet como el correo electrónico, o el almacenamiento de ficheros. La diferencia con estos últimos es que todas las comunicaciones que establezcan se llevan a cabo con la misma premisa de anonimato que existe en la navegación web.

Por ejemplo, el servicio de **correo electrónico** en Tor es ofrecido por Protonmail o SIGAINT. En la red Freenet se implementa por Freemail. Y en I2P se encargan de este servicio dos aplicaciones I2Pmail/susimail o I2P-Bote.

En el caso de **mensajería instantánea** o chat, Tor dispone de CoyIM. Sone es uno de los muchos servicios de chat existentes en Freenet y en I2P este servicio es ofrecido por I2P-Messenger.

Para el **almacenamiento e intercambio de archivos**, Tor dispone de OnionShare. En el caso de la red I2P este servicio es proporcionado por Tahoe-LAFS.

4.5. Desmitificando la *Deep Web*

Una vez que se han plasmado los contenidos y todos los servicios que ofrece la *Deep Web* y más en concreto cada una de las *Darknets* analizadas, se puede aseverar que detrás de ellas no solo se encuentran organizaciones criminales y delincuentes intentando hacer negocio a través de estas. Sino que también **existen** multitud de **contenidos lícitos** que nada tienen que ver con estos.

Es cierta su existencia, se ha visto cómo operan mercados de drogas, se pueden contratar hackers con fines delictivos, métodos para blanquear dinero a través de criptomonedas, incluso acciones más deleznables como utilizar los servicios de sicarios o el intercambio de pornografía infantil. Pero no es menos cierto, que la **red convencional** también es un medio ampliamente **utilizado para cometer actos delictivos**. Estafas bancarias, chantajes gracias a malwares de tipo *ramsomware*, distribución de pornografía infantil, son solo algunos de los actos que también se presentan en la *Surface Web*.

El incremento del uso de las *Darknets* por estos individuos viene determinado por el mayor anonimato que les provee en relación a la red convencional, pero no por ello se debe definir a la *Deep Web* como un reducto de criminales y delincuentes.

Se ha plasmado que estas redes disponen de una oferta amplia y variada de contenidos que van desde foros de discusión, blog de diversa índole, libros, archivos multimedia, etc. hasta servicios de correo electrónico, mensajería instantánea, compartición de archivos, etc.

La diferencia principal de estos contenidos y servicios con los que pueblan la *Surface Web* es la búsqueda del **anonimato y la privacidad de los usuarios** en el uso de estos. Este es el **verdadero espíritu** de estas redes, que todos los usuarios pueda expresar sus ideas, sin que ningún gobierno o administración pueda coartar esa libertad ni decidir que contenidos pueden o no consumir sus súbditos.

5. DESANONIMIZACIÓN

5.1. Introducción

El objetivo principal de las redes que conforman la *Dark Web* es el anonimato del usuario mientras navega por ella. La neutralización de esta característica significaría la **perdida de la confianza** y credibilidad en la red, de ahí la importancia de que su tecnología sea robusta.

Como sucede habitualmente, el aumento de popularidad en una tecnología supone el incremento del número de ataques con el fin de conseguir encontrar vulnerabilidades y explotarlas. En el siguiente apartado se presentan algunas de las vulnerabilidades y el modo de explotación, que se han descubierto en las principales *Darknet*s.

5.2. Vulnerabilidades y explotación

Existen varios ataques que se podrian explotar en Tor, así como vulnerabilidades que se han ido descubriendo en el navegador Tor Browser.

El ataque **sybil** se basa en el despliegue de nodos por parte del atacante. Teniendo en cuenta que hay una cantidad finita de nodos, aquel que obtenga un control sobre un mayor número de ellos tendrá más opciones de participar en los circuitos que establece esta red. Si la intención es tratar de desanonimizar a los usuarios podría conseguir su objetivo. Para evitar este tipo de ataques, la red dispone de varias contramedidas. Una es la ejecución de un script “sybil_cheker.py” que detecta si existe un incremento repentino y anormal de nuevos nodos, y otra es la existencia de una dirección de correo electrónico bad-relays@list.torproject.org para comunicar la existencia de nodos sospechosos.

Otro ataque es el denominado **predecesor**, cuyo objetivo es identificar a los usuarios, reconstruyendo los circuitos. Para ello, uno o varios nodos desplegados por el atacante realizan seguimientos de las conexiones. Cada vez que el cliente reconstruye un circuito (por norma general, cada diez minutos), se vuelve a conectar a otros nodos. De esta manera, el atacante identificará al cliente porque tenderá a conectarse más veces que cualquier otro nodo. Incluso, un atacante que tenga un control sobre un número importante de nodos podría deliberadamente hacerlos fallar, obligando al usuario a reconectarse una y otra vez con el fin de aumentar el éxito del ataque.

En un ataque de **correlación de tráfico**, se conecta un usuario de la red y el servidor final (los dos extremos de una conexión) mediante el control del nodo de entrada y el nodo de salida del circuito. Una vez ejecutada esta acción, analizando el tamaño, la frecuencia y otros parámetros entre los datos de entrada y salida, podría establecer una relación objetiva.

El ataque de **reconstrucción de circuitos** tiene una complejidad elevada. Su objetivo es controlar los tres nodos de una conexión, mediante una reconstrucción, y posteriormente identificar al usuario y el servidor de destino.

Finalmente, el ataque ***sniffer*** se basa espiar la información enviada por el cliente en los nodos salida, obteniendo mejores resultados si la comunicación entre el nodo final y el cliente se realiza mediante el protocolo HTTP, aunque existen métodos para vulnerar HTTPS como SSLStrip, SSLStrip 2, o el uso de certificados autofirmados. Al igual que en el ataque Sybil, se podría notificar la existencia de estos nodos y suprimirlos de la red. (39)

Respecto al navegador Tor Browser, a finales del año 2017, se descubrió una vulnerabilidad denominada **TorMoil**, donde al establecerse una conexión a un enlace de tipo “file://”, esta redirigía directamente al servidor web, sin aplicar los mecanismos de ocultación que en el resto de comunicaciones si lleva a cabo, revelando con ello la IP del usuario. (40)

Otra vulnerabilidad reportada en septiembre de 2018 residía en las versiones 5.0.4 y 5.1.8.6 del *plugin* “NoScript”, encargado de bloquear JavaScript, Java, Flash y otros elementos potencialmente dañinos para el usuario. El modo de seguridad más alto del Tor Browser puede ser burlado al permitir ejecutar cualquier fichero JavaScript, mostrando la IP del usuario. (41)

También se ha encontrado otra vulnerabilidad en la librería “WebRTC” del navegador que está diseñada para organizar un canal de transmisión de flujo de vídeo de apoyo a HTML5, que se utiliza para establecer la dirección IP real de la víctima. Las peticiones del llamado STUN de “WebRTC” se envían en texto plano, evitando Tor y las consecuencias resultantes. (42)

En junio de 2014, otra vulnerabilidad, esta vez involucrando a la red I2P. destapaba un fallo en el módulo I2P que venía por defecto en la distribución Tails, permitía la identificación de los usuarios. (43)

6. EXPERIMENTOS PRÁCTICOS

6.1. Acceso a la *Deep Web*

El acceso a la *Deep Web*, o en particular a la *Dark Web* se realiza de distintas formas, ya que cada *Darknet* proporciona un método y tecnología distinta. En este capítulo se realizarán varios experimentos prácticos con el objetivo de conocer y describir las distintas opciones existentes para accederá a las tres principales *Darknet*s.

La red Tor, ya sea por ser la más conocida es la que dispone de más formas de acceso. Se accederá a través del navegador desarrollado para ese cometido: Tor Browser; también a través de *proxys* web y finalmente se describirá el acceso, a través del propio navegador Tor Browser pero ejecutándose sobre entornos que prometen mayor seguridad, esto es a través de las distribuciones Linux Tails y Whonix.

En el caso de I2P y Freenet se accederá a través de las aplicaciones propias desarrolladas para ese cometido y se describirán sus principales características.

Acceso a Tor a través de Tor Browser.

La forma **más común** de acceder a la red Tor es a través de **Tor Browser**. Tor Browser es un navegador basado en Mozilla Firefox. La primera versión salió a la luz en el año 2008 y dotaba al navegador Firefox de funcionalidades para ofrecer anonimato en la navegación.

En la actualidad se basa en versiones Extended Support Release de Mozilla Firefox, una línea de versiones que no incluyen las últimas funcionalidades, pero sí las actualizaciones de seguridad y estabilidad más recientes. La última versión es Tor Browser 8.0, basada en Mozilla Firefox 60.2 ESR. Su descarga se puede realizar desde la página web de Tor Project: https://www.torproject.org/index.html.es

Una vez abierto el navegador, se indica el dominio del *Hidden service* al que se desea acceder, por ejemplo para visitar The Hidden Wiki, se debe ir a zqktlwi4fecvo6ri.onion.

El navegador establece el circuito seleccionando los nodos por los que circularán los paquetes de datos. El circuito generado se puede consultar a través de la información del sitio.

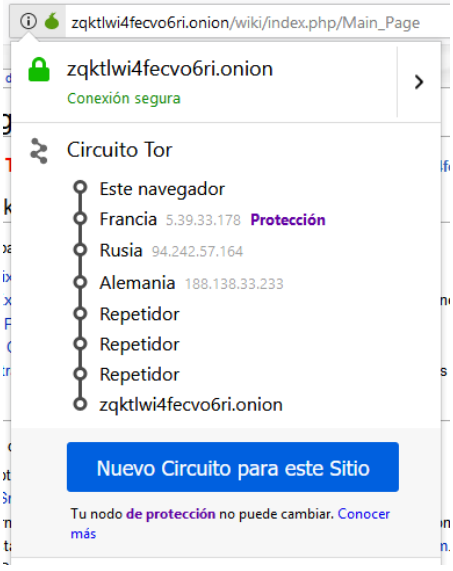


Ilustración 14: Captura de pantalla del Circuito Tor en Tor Browser

En el ejemplo de la imagen se observa cómo se crea un camino con seis. nodos, de los que se conoce la ubicación de los tres primeros.

Para garantizar mayor protección, pero también eficiencia, Tor genera un nuevo circuito cada diez minutos, pero es posible crear uno nuevo a petición del usuario.

El resultado final será el sitio web que se ha solicitado.

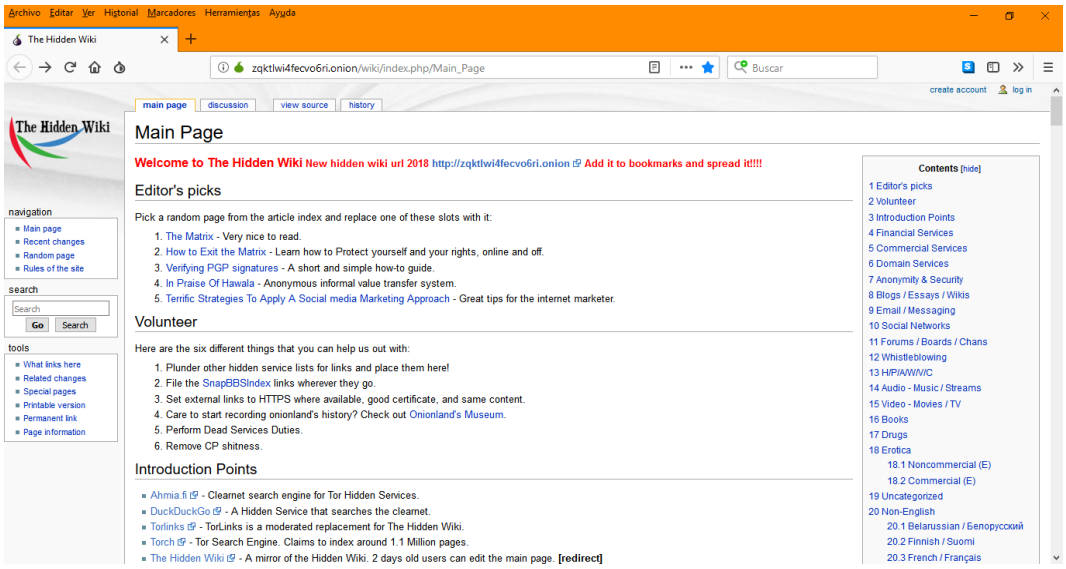


Ilustración 15: Captura de pantalla de The Hidden Wiki en Tor

Acceso a Tor a través de un *proxy* web.

La forma **más sencilla** pero también **menos segura** de acceder es a través de los *proxys* disponibles en Internet. Uno de los más conocidos es Tor2Web. En la propia página web indican que no existe anonimato, y que tanto este *proxy* como el *Hidden service* pueden ver la dirección del visitante.

Por ejemplo, si se desea acceder al motor de búsqueda Torch, se debe indicar en el campo habilitado para ello la dirección .onion de esta página: https://xmh57jrzrnw6insl.onion y hacer clic en el botón open vía onion.to *proxy*

Otra opción es indicar directamente en la barra de direcciones del navegador web el dominio .onion seguido de .to, es decir, la dirección quedaría así: https://xmh57jrzrnw6insl.onion.to

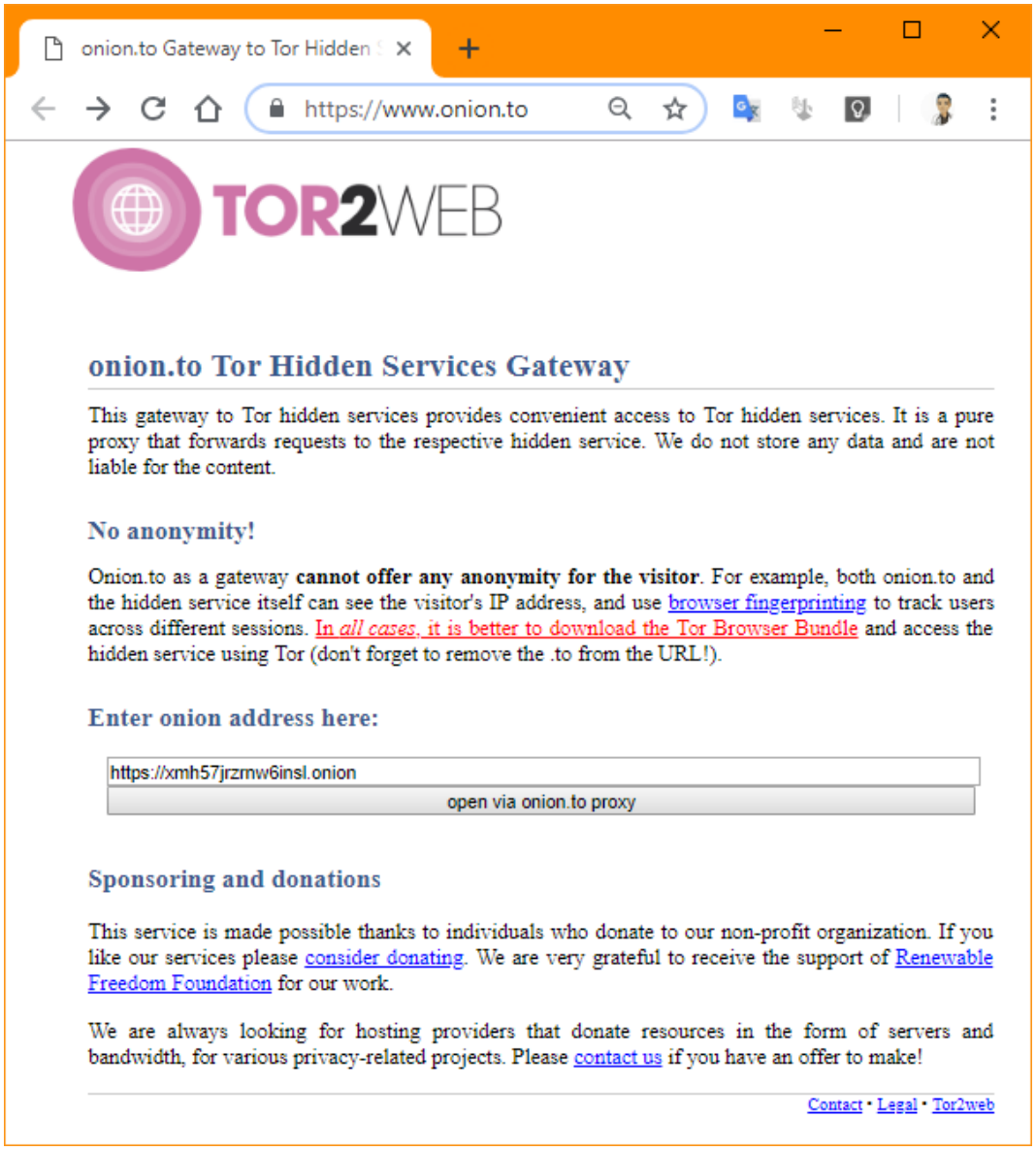


Ilustración 16: Captura de pantalla del *proxy* web Tor2Web

Existen otros *proxys* web como Onion.Link donde a la dirección .onion, se debe añadir .link. (44) (45)

Acceso a Tor a través de Tor Browser en Tails.

Si por el contrario lo que se busca es **la máxima privacidad y anonimato**, una de las formas más seguras de acceder a Tor es a través de Tails.

Tails son las siglas de The Amnesic Incognito Live System, se trata de una distribución Linux basada en Debian que ha sido diseñada para preservar el anonimato del usuario en la red. Se ejecuta como un **sistema operativo live** desde una memoria USB o un DVD independientemente del sistema operativo del equipo original.

Para poder ofrecer el máximo grado de seguridad, incluso el proceso de instalación de la distribución live en la memoria USB se realiza a través de un Tails intermedio, presente en una segunda memoria USB, y no directamente desde el sistema operativo anfitrión.

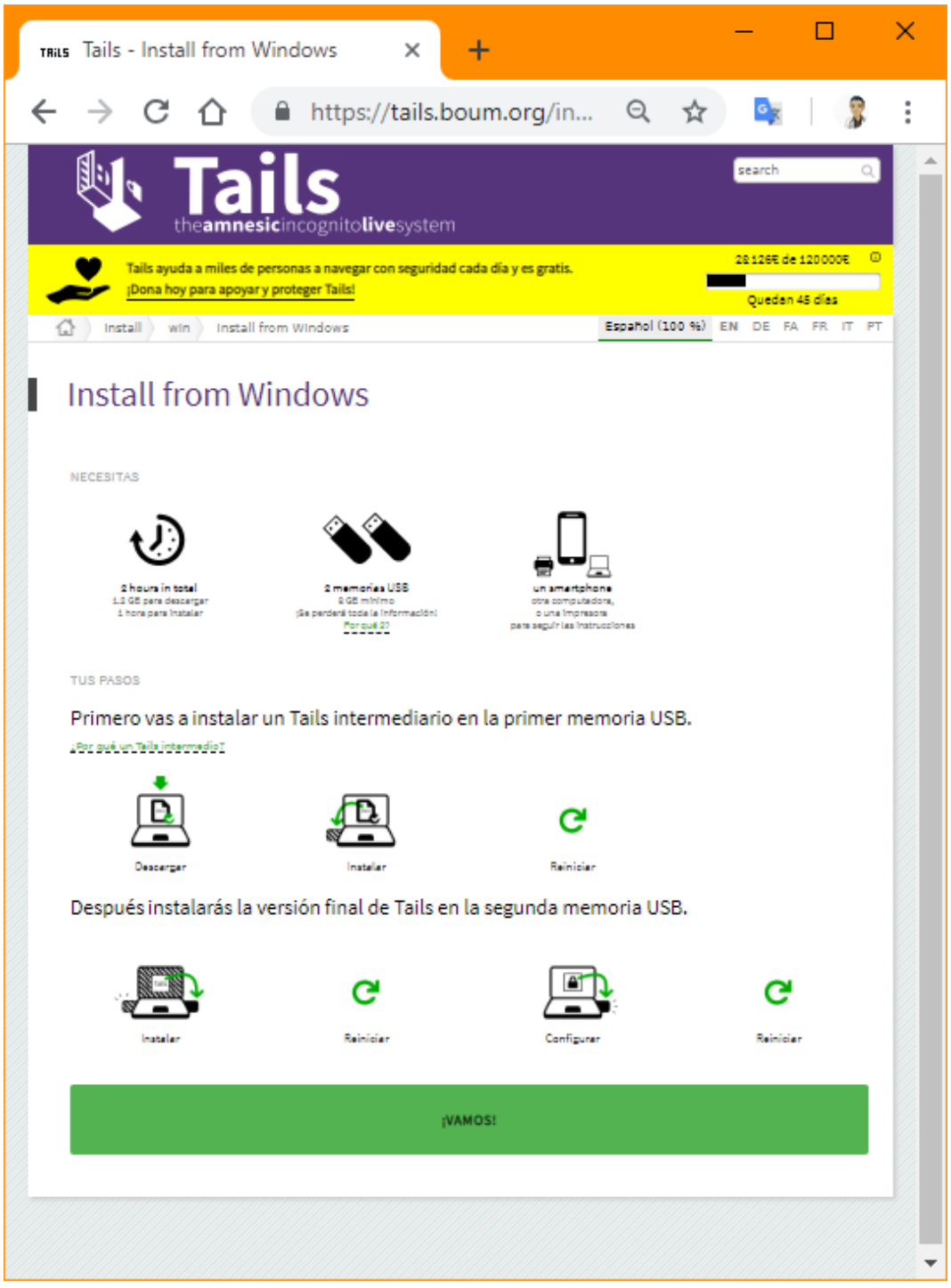


Ilustración 17: Captura de pantalla de la guía de instalación de Tails desde Windows

Una vez arrancado Tails, previa configuración de la conexión de red, se puede acceder a través de Tor Browser al servicio de correo electrónico Mail2Tor cuya dirección es mail2tor2zyjdctd.onion.

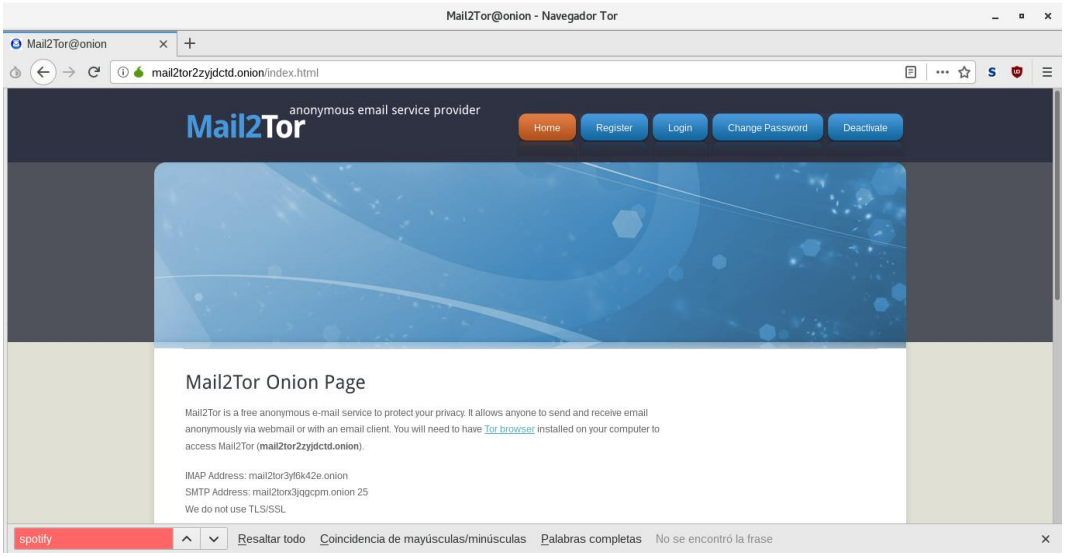


Ilustración 18: Captura de pantalla de Mail2Tor en Tor desde Tails

En Tails se puede observar los circuitos existentes en Tor, a través de la opción “Circuitos Cebolla”.

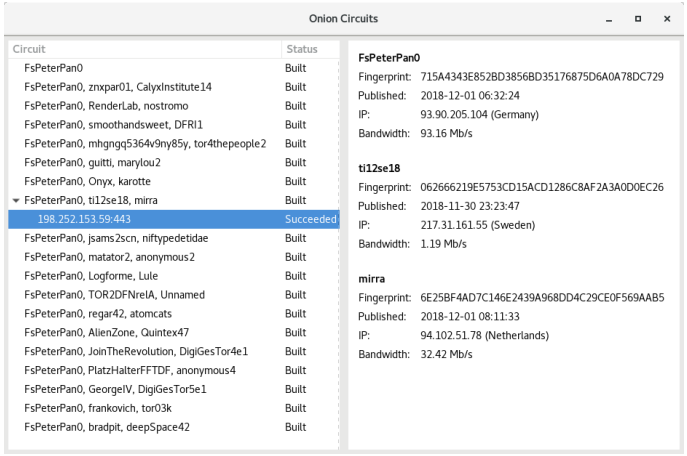


Ilustración 19: Captura de pantalla de los Circuitos Cebolla en Tails

Al apagar Tails, gracias a su condición de sistema operativo live, todo el rastro de actividad se eliminará, incrementando con ello la privacidad y anonimato.

Acceso a Tor a través de Tor Browser en Whonix

El acceso a través de Whonix, al igual que con Tails, implica **incrementar el anonimato y la privacidad**, en gran medida a su particular esquema de uso.

Whonix es un sistema operativo virtualizado, es decir, se ejecuta en una máquina de forma virtual, en este caso en VirtualBox. Se trata de una

distribución Linux, basada en Debian, que utiliza la red Tor para todas las comunicaciones.

Su peculiar esquema de seguridad es el siguiente: Se deben ejecutar **dos instancias virtuales** de Whonix. La primera, denominada *gateway* o puerta de enlace hace las funciones de un *proxy* Tor. La segunda, denominada Workstation o estación de trabajo trabaja con una red completamente aislada en la que solo son posibles las conexiones a través de Tor.

De esta forma, cualquiera aplicación que se quiera conectar en la estación de trabajo, lo hará obligatoriamente a través de la puerta de enlace, y por lo tanto, las comunicaciones serán forzosamente a través de la red Tor.

En la imagen inferior se observan las dos instancias de Whonix ejecutándose simultáneamente sobre VirtualBox. A la izquierda se encuentra la puerta de enlace, donde a modo de ejemplo se han capturado los circuitos onion. A la derecha se encuentra la estación de trabajo, ejecutando Tor Browser, con el servicio de oculto Hidden Wallet cargado en este. Este *Hidden service* permite mantener una cartera oculta de criptomonedas y su dirección es nql7pv7k32nnqor2.onion. (46)

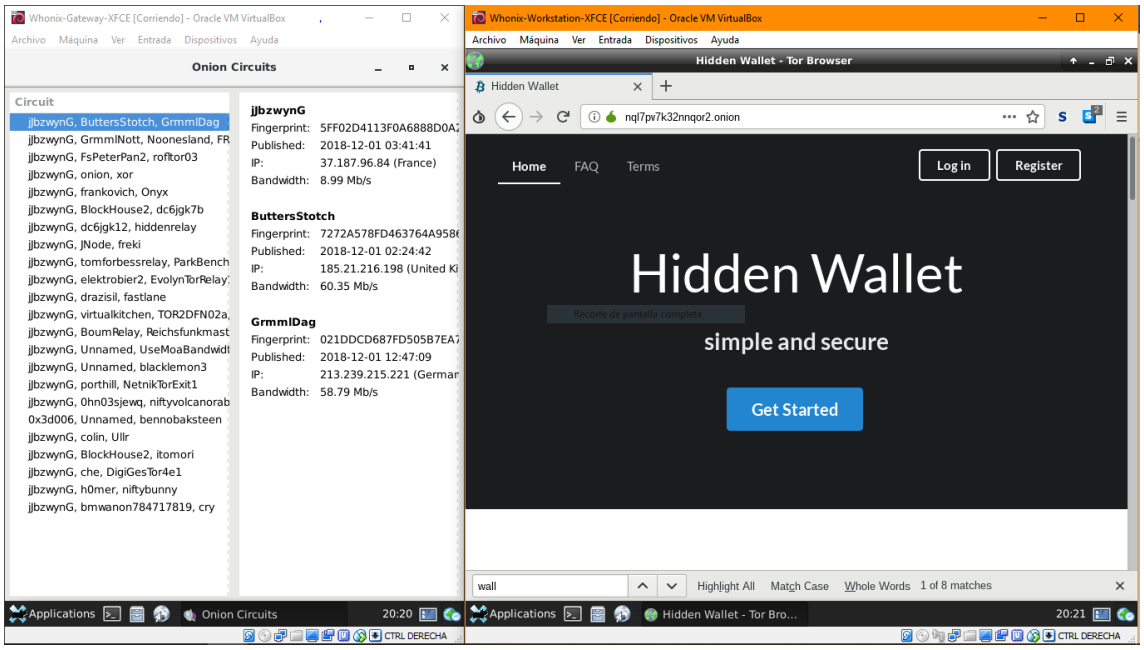


Ilustración 20: Captura de pantalla de los Circuitos Onion y del servicio oculto Hidden Wallet desde Whonix

Acceso a I2P

Como primer requisito para acceder a la red I2P es descargar el software desde la página web del proyecto I2P: https://geti2p.net/es/ e instalarlo.

Una vez que se ejecuta, se cargará en el navegador web una consola asociada a la IP y puerto: http://127.0.0.1:7657

Ilustración 21: Captura de pantalla de la consola de I2P

Esta **consola**, que es completamente configurable se divide en tres partes principalmente.

A la izquierda se encuentra la barra lateral o de resumen en donde se puede acceder a los servicios existentes en la red (correo electrónico, servidor web, *torrents*), la configuración interna de I2P, información del router IP, los pares o *peers*, los túneles y finalmente un apartado de ayuda.

Ocupando el resto de la consola se encuentran dos zonas: La superior presenta los servicios ocultos de interés, es ahí donde se pueden almacenar a modo de favoritos los sitios I2P que se deseen. La inferior contiene diversos accesos a los servicios y configuraciones, que pueden ser los mismos presentes en la barra lateral.

Para poder acceder a los servicios ocultos o *eepsites* es necesario configurar el navegador web para que use el *proxy* HTTP: 127.0.0.1 y puerto 4444.

Por ejemplo, para acceder al directorio de enlaces INR, se indica en la barra de direcciones del navegador http://inr.i2p/ y aparecerá la página de ese *eepsite*.

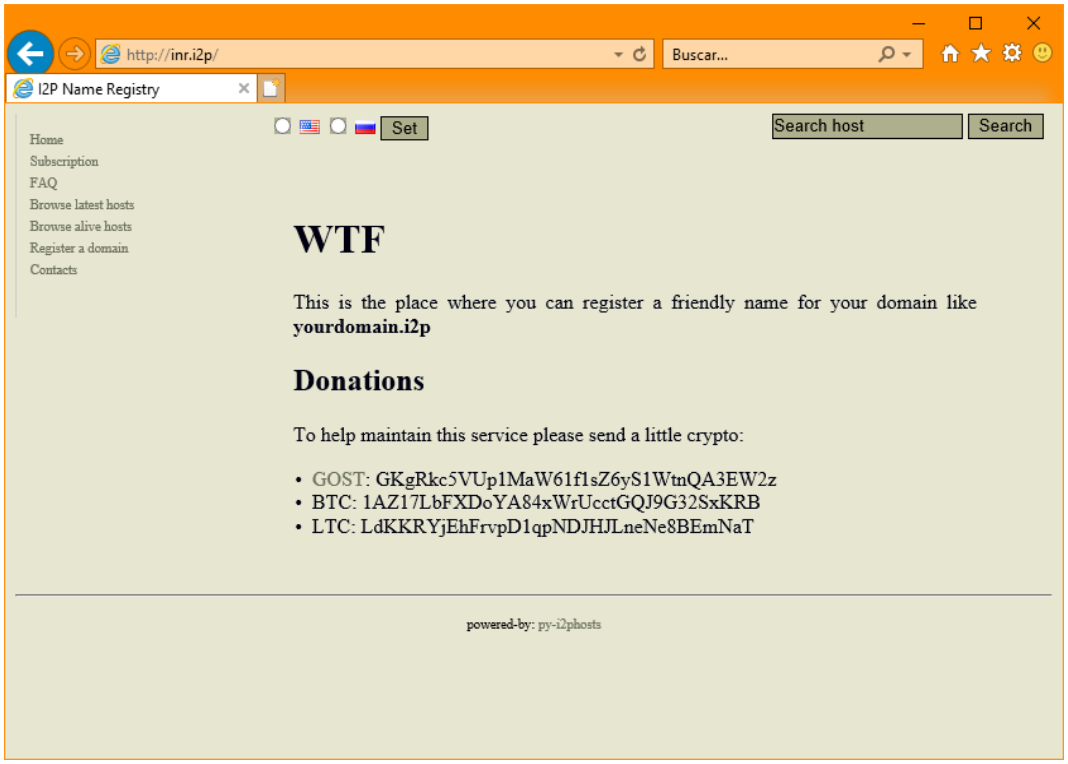


Ilustración 22: Captura del directorio de enlaces INR en I2P

Como se mencionaba en el apartado 3.2. Freenet, aunque I2P no está pensando para funcionar como *outproxy*, es decir, para navegar fuera de esta red, se permite esta funcionalidad gracias a desarrollos de terceros. El tráfico por tanto, será enrutado a través de la red I2P.

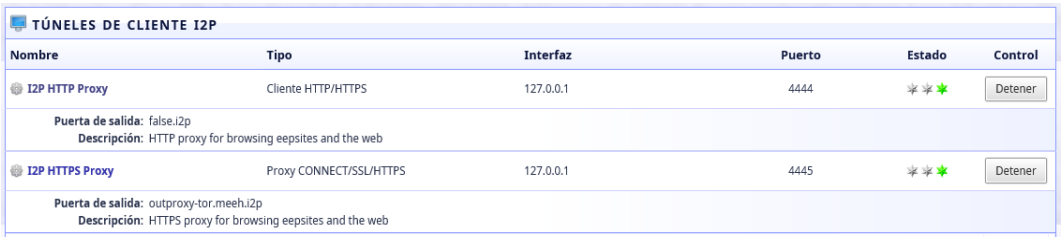


Ilustración 23: Captura de pantalla de los módulos de I2P para comunicaciones *outproxy*

No obstante, desde la página web del proyecto apuntan que si bien este servicio existe actualmente, no hay garantías de que siempre esté disponible ya que no es un servicio oficial.

Acceso a Freenet

Para poder acceder a Freenet es necesario descargar la aplicación desde la página web del proyecto: https://freenetproject.org/author/freenet-project-inc.html e instalarla.

Por defecto, al ejecutarla se abrirá una ventana en modo incógnito del navegador web Chrome en la dirección y puerto localhost:8888. Es posible utilizar cualquier otro navegador, en cualquier caso, se recomienda activar su modo de navegación privada.

La primera vez que se accede aparecerá un asistente donde se deberán configurar ciertos parámetros de conexión, el tamaño asignado a la aplicación, etc. En el primero de ellos hay que elegir el nivel de seguridad: baja o alta.

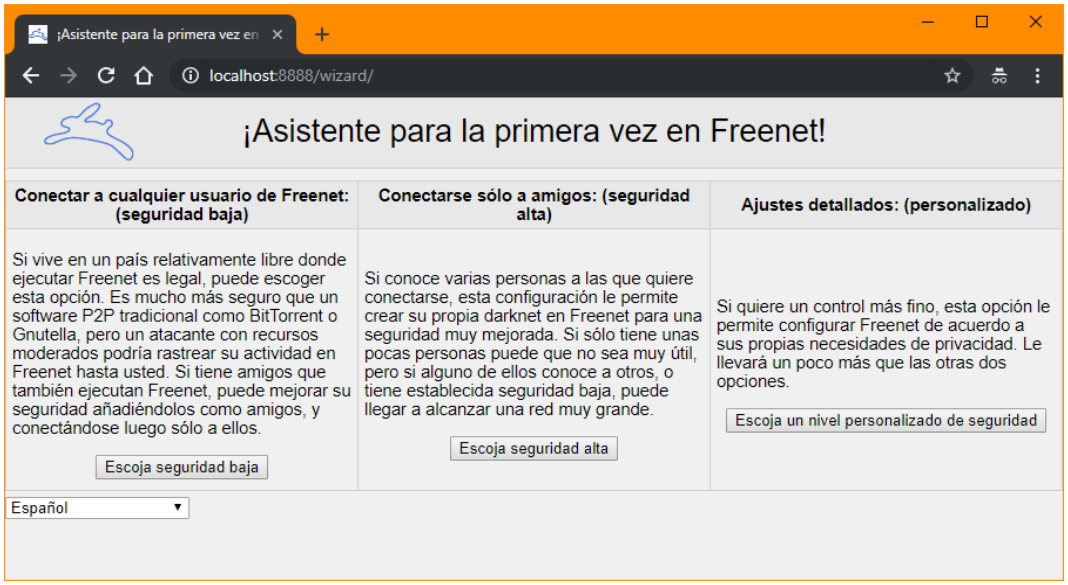


Ilustración 24: Captura de pantalla del asistente de primera vez de Freenet

Cuando se selecciona seguridad baja (*opennet*), la conexión se realiza a cualquier usuario de Freenet, desconociendo si este es fiable o no, por lo que en cierto modo existe un grado de exposición en la red.

La otra opción es el nivel de seguridad alto (*darknet*). En este caso la conexión se realiza a un amigo, por lo que existe una relación de confianza que incrementa el grado de seguridad al haber previamente intercambiado sus referencias, un proceso similar al intercambio de claves. En la imagen de la derecha se puede observar en la parte superior un recuadro donde se introducirá la referencia de nodo de un amigo. En la parte inferior, se encuentra la del usuario, la cual, se puede modificar. Este último modo de conexión se utiliza para crear

Ilustración 25: Captura de pantalla de la configuración para conectarse con un amigo en Freenet

redes de amigos, donde la seguridad prima por encima de cualquier otra característica o funcionalidad.

A continuación, aparece la pantalla de inicio con un cierto parecido en cuanto estructura a I2P

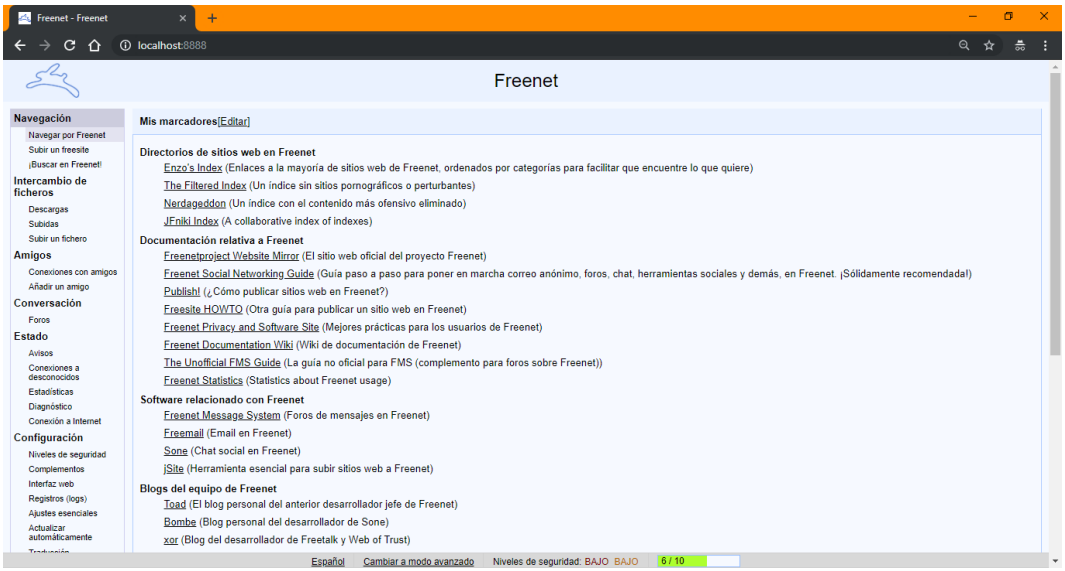


Ilustración 26: Captura de pantalla de la pantalla de inicio de Freenet

En la parte izquierda presenta una columna con acceso para navegar, intercambiar ficheros, agregar y conectar con amigos y otras opciones de estado de la conexión, configuración, etc. El resto de la página muestra varios enlaces a modo de marcadores por defecto, relativos a directorios de sitios web, documentación, software o blogs, todos ellos relacionados con la red Freenet. Por supuesto, este listado es modificable para incluir aquellos que el usuario considere.

Si se desea acceder a Nerdageddon cuyo enlace es: http://localhost:8888/USK@tiYrPDh~fDeH5V7NZjpp~QuubaHwgks88iwlRXXLLWA,yboLMwX1dChz8fWKjmbdtl38HR5uiCOdIUT86ohUyRg,AQACAAE/nerdageddon/247/ se mostraría la página de este índice de enlaces donde se ha eliminado el contenido más ofensivo.

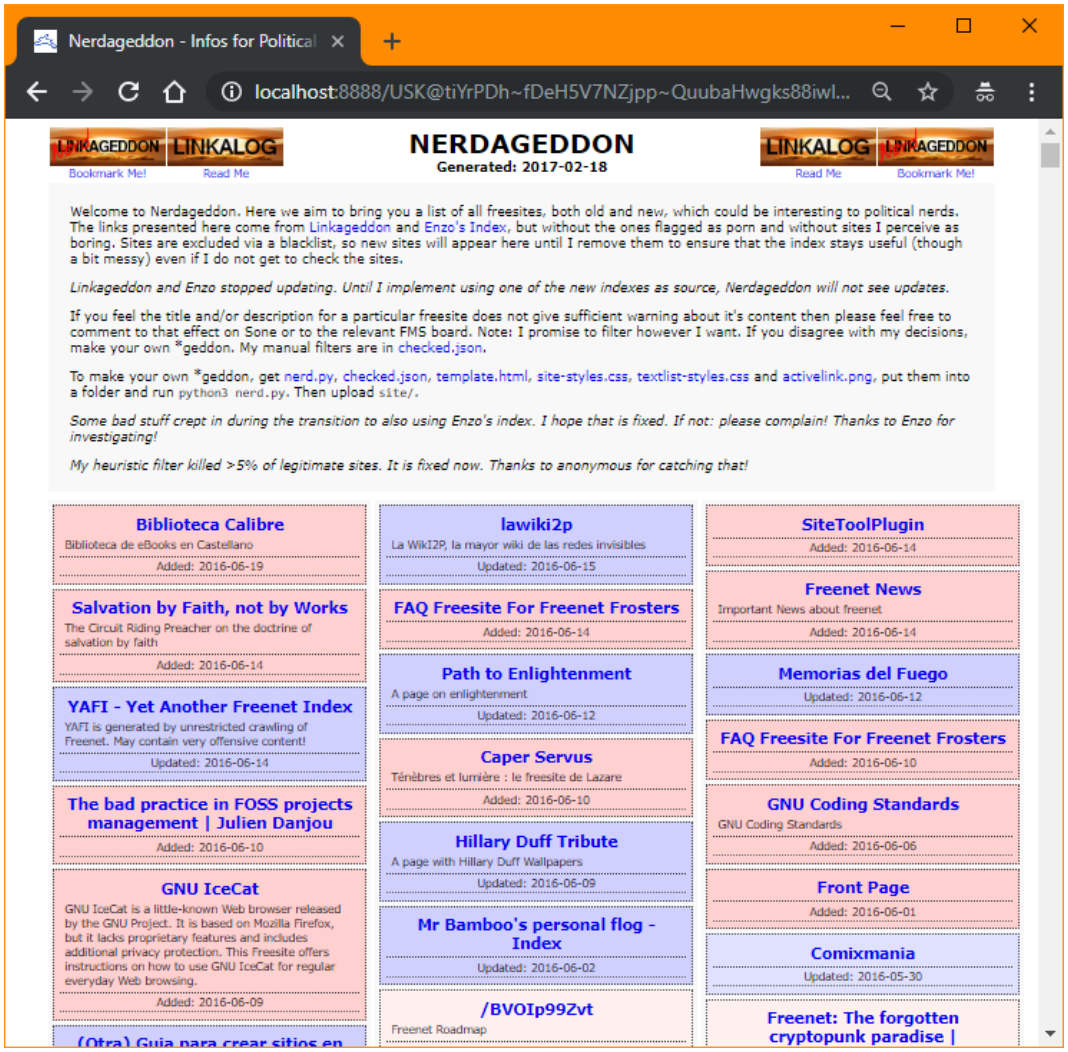


Ilustración 27: Captura de pantalla del índice de enlaces Nerdageddon en Freenet

6.2. Intento de desanonimización

En este capítulo se realizará un experimento práctico cuyo objetivo principal es comprobar la dificultad de desanonimizar un usuario de una *Darknet*, Tor en este caso. No cabe duda de que estas prácticas deben tener un bajo nivel de éxito, ya que de otra manera, el uso de estas tecnologías perdería la confianza del usuario. Como curiosidad, la compañía de especializada en seguridad de las TIC Zerodium, lanzaba el 13 de septiembre de 2017 una recompensa de un millón de dólares a quien descubriese una vulnerabilidad de tipo *zero-day* en Tor Browser operado en Windows o Tails. El 30 de noviembre de ese mismo año dio por terminada la mencionada campaña, desconociendo si alguien llego a encontrarla. (47)

En el capítulo 5.2. Vulnerabilidades y explotación se citaban algunas de las vulnerabilidades más importantes descubiertas hasta ahora en Tor Browser. Para el desarrollo de este experimento práctico se tratará de explotar la vulnerabilidad conocida como TorMoil.

TorMoil fue descubierta y publicada el 26 de octubre de 2017 por el investigador de seguridad italiano Filippo Cavallarin de la compañía We Are Segment. Se trata de una vulnerabilidad que afecta a las versiones de Tor Browser anteriores a 7.0.9 en sistemas operativos Linux y MacOS. El problema residía en que cuando un usuario accedía a un enlace de tipo "file://", la comunicación no se realizaba a través de la red Tor, sino, directamente al servidor web, y por tanto, revelándose la dirección IP del usuario.

Con estas premisas se prepara el experimento práctico que se describe a continuación.

Por un lado, se virtualiza un sistema operativo Ubuntu en VirtualBox, con el interfaz de red configurado como adaptador puente, de tal forma que tenga una IP propia. Este sistema es el que actuará como servidor web.

Por otro lado, se virtualiza otro sistema operativo Ubuntu, con la misma configuración de red que la anterior, en el cual está instalado la versión de Tor Browser que es vulnerable, es decir, la 7.07 y desde donde se accederá al sitio .onion.

En el primer sistema, el que hace de servidor, se crea una página web simple, que contiene un enlace tipo "file://" a un fichero de prueba con extensión .txt. Como servidor web se levanta una instancia de Apache.

Para crear el servicio oculto, hay que incluir dos directivas en el fichero "torrc":

HiddenServiceDir /home/mistic/Escritorio/hidden_service_prueba/

HiddenServicePort 80 127.0.0.1

Al levantar la instancia de Tor, se crean dos ficheros, "hostname" con el dominio .onion y "private_key" con la clave privada.

En el segundo sistema, se ejecuta Tor Browser, accediendo a twbwuyrje6ueqsxh.onion que es la dirección .onion que se indica en el menciona fichero "hostname", aparece la página web almacenada en el primer sistema que se muestra en la imagen inferior izquierda.

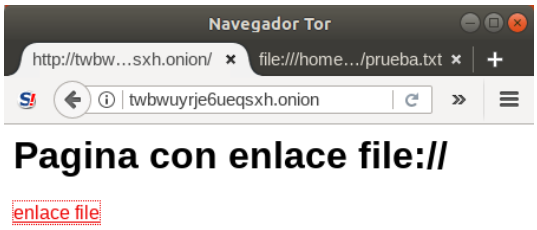


Ilustración 28: Captura de pantalla de un servicio oculto en Tor con un enlace de tipo “file://”

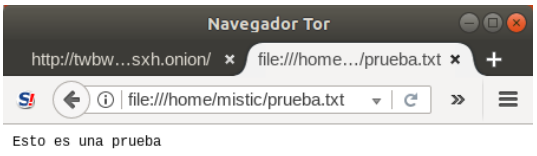


Ilustración 29: Captura de pantalla del resultado de acceder a un enlace de tipo “file://” arrastrando este hasta la zona de pestañas.

Se comprueba este tipo de enlaces no funcionan, es decir, al hacer clic en ellos no cargan el contenido vinculado. El único método de acceder a este contenido es arrastrar el enlace hasta la zona de pestañas para que se abra como una pestaña independiente como se observa en la imagen derecha superior.

Comprobado el fichero “accese.log” del servidor web Apache, se comprueba que no existe ninguna llamada desde la IP del equipo cliente. Esto tiene su explicación en que el enlace es hacia el propio equipo del usuario y por tanto, no se establece comunicación alguna del servidor web.

Dado que por este camino no es posible desanonimizar al usuario, se ahonda en la información que hay sobre TorMoil, descubriendo que Filippo Cavallarin, describe a través de la página web de su empresa https://www.wearesegment.com/research/tormoil-deanonymize-tor-browser-users-with-automount/ una prueba de concepto para demostrar esta vulnerabilidad.

En ella indica cuatro pasos a seguir:

Ilustración 30: Captura de pantalla de los pasos a ejecutar para demostrar la vulnerabilidad TorMoil

De esta forma, se modifica la página web, incluyendo en la cabecera la llamada a la hoja de estilos, al servidor con IP 12.12.12.12.

En el primer equipo, el que actúa como servidor, se ejecuta la herramienta "tcpdump" en el puerto 111. Esta herramienta es un esnifador de paquetes que circulan por la red. En este caso se captan los paquetes que atraviesan el puerto 111.

Desde el segundo equipo se accede de nuevo al servicio oculto.

Tal y como se indica en el último paso, tcpdump debería de captar los paquetes UDP hacía la dirección 12.12.12.12 desde la dirección IP del cliente. Sin embargo en este experimento práctico no se ha podido lograr desenmascarar esta IP, ya que la herramienta tcpdump no capta ningún paquete en el puerto 111. (48)

Con este experimento práctico, se demuestra **que desanonimizar la red Tor** es relativamente **complejo** y que aun intentando explotar una vulnerabilidad conocida como TorMoil es difícil llegar al resultado deseado.

No solo se puede tratar de desanonimizar al usuario de la red Tor aprovechando vulnerabilidades en Tor Browser, si no que teniendo en cuenta otros métodos como la búsqueda de configuraciones erróneas, fallos humanos, etc. también es posible.

Por citar algún ejemplo, en el descubrimiento de Ross William Ulbricht como creador del conocido mercado negro Silk Road, el error de configuración del captcha alojado en el servicio oculto el cual realizaba las peticiones por fuera de la red Tor fue lo que le delató. (49)

7. CONCLUSIONES

Las lecciones más destacables aprendidas a lo largo de este trabajo han sido:

- La **adecuada interpretación de los términos** *Deep Web*, *Dark Web* y *Darknet*.
- La existencia de **otras redes** más allá de Tor, así como sus diferentes métodos de acceso.
- La navegación en la *Dark Web*, descubriendo **contenidos**, pero también, otros **servicios** como el correo electrónico o la mensajería instantánea.
- Y las posibilidades de **ataques de desanonimización** y el grado de materialización de estos.

Con respecto a los objetivos conseguidos, se han explorado los aspectos más representativos de la *Deep Web*, recorriendo un **amplio abanico de conceptos, tecnologías, prestaciones y riesgos**, contribuyendo con ello a generar una idea global de lo que es la *Deep Web*, las posibilidades que ofrece, como explotarla de forma inteligente y que directrices hay que tener presentes a la hora de sumergirse en ella. Se puede afirmar que los objetivos que se planteaban inicialmente en este trabajo han sido alcanzados.

En cuanto a la planificación que se había establecido para el desarrollo de este trabajo, obra decir que se ha cumplido en su totalidad. Si bien es cierto, que se ha detectado que el capítulo 4.2. Contenidos hubiera sido más adecuado desarrollarlo una vez se hubiera ejecutado el experimento práctico del apartado 6.1. Acceso a la *Deep Web* ya que para realizar un análisis exhaustivo del contenido es más oportuno haber accedido previamente.

Finalmente de cara al futuro se podrían seguir explorando las *Darknet*s en desarrollo y las que están por venir. Otras líneas a seguir son: la investigación de fallos de seguridad de la red, así como su prevención y en última instancia seguir apostando por herramientas y tecnologías que impliquen mayor anonimato y privacidad.

8. GLOSARIO

Blockchain

Estructura de datos en la que la información se agrupa en bloques con información de otros bloques generando una línea temporal, de manera que gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores.

Clearnet

(Ver *Surface Web*).

Criptomoneda

Moneda digital de intercambio que utiliza técnicas criptográficas para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos.

Darknet

Red anónima.

Dark Web

Conjunto de redes anónimas.

Deep Web

Conjunto de contenidos web no indexado por los motores de búsqueda.

Distribución live

Sistema operativo basado en Linux que se ejecuta en la memoria volátil de un equipo.

Eepsite

Sitio web en la red I2P.

Esnifador

(ver *Sniffer*).

Hidden service

Sitio web en la red Tor.

Internet oscura

(ver *Dark Web*).

Internet profunda

(ver *Deep Web*).

Malware

Software malicioso cuyo propósito es infiltrarse o dañar un equipo.

P2P

Red *peer*-to-*peer*, o red entre pares en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino con una serie de nodos que se comportan como iguales entre sí.

Proxy

Programa o dispositivo que hace de intermediario en las peticiones de recursos que realiza un cliente a un servidor con el objetivo de ofrecer diversas funcionalidades: control de acceso, registro del tráfico, restricción a determinados tipos de tráfico, mejora de rendimiento, anonimato de la comunicación, caché web, etc.

Servicio oculto

(Ver *Hidden service*).

Ramsonware

Malware que cifra la información alojada en un equipo y solicita un rescate económico para revertir el cifrado.

RSA

Algoritmo de cifrado de clave pública desarrollado en 1979.

Sniffer

Software que captura los paquetes del trafico de red de un equipo para su posterior análisis.

Surface Web

Conjunto de sitios web indexados por los motores de búsquedas.

9. BIBLIOGRAFÍA

1. trabajo-deep-web. *NIVELES DEEP WEB.* [En línea] [Citado el: 6 de 10 de 2018.] https://sites.google.com/site/trabajodeepweeb/home/5-niveles.

2. *Deep Web* - Casos reales. *Mariana Web.* [En línea] [Citado el: 5 de 10 de 2018.] http://deeplstweb.blogspot.com/2014/11/mariana-web.html.

3. Mundo *Deep Web*. *Deep Web.* [En línea] [Citado el: 5 de 10 de 2018.] http://comunidaddeepweb.blogspot.com/p/deep-web.html.

4. INCIBE. *Redes anónimas: más allá de Tor.* [En línea] [Citado el: 26 de 10 de 2016.] https://www.incibe-cert.es/blog/redes-anonimas-mas-alla-de-tor.

5. SOFTzone. *Las mejores alternativas a Tor para navegar de forma privada.* [En línea] [Citado el: 6 de 10 de 2018.] https://www.softzone.es/2018/02/19/mejores-alternativas-tor/.

6. Comparitech. *La guía definitiva para la navegación anónima con Tor.* [En línea] [Citado el: 1 de 12 de 2018.] https://www.comparitech.com/es/blog/vpn-privacidad/qu-es-tor-segu-alternativas/.

7. Comparitech. *Qubes, Whonix, or Tails: which Linux distro should you use to stay anonymous?* [En línea] [Citado el: 6 de 10 de 2018.] https://www.comparitech.com/blog/vpn-privacy/anonymity-focused-linux-distributions/.

8. Profesional review. *Las mejores Linux en seguridad y privacidad.* [En línea] [Citado el: 6 de 10 de 2018.] https://www.profesionalreview.com/2018/04/29/mejores-linux-seguridad-privacidad/.

9. La mirada del replicante. *JonDo: distribución GNU/Linux especializada en el anonimato en la red.* [En línea] [Citado el: 6 de 10 de 2018.] http://lamiradadelreplicante.com/2013/09/30/jondo-distribucion-gnulinux-especializada-en-el-anonimato-en-la-red/.

10. Youtube. *Taller: Cambiando el CuenTOR.* [En línea] [Citado el: 29 de 09 de 2018.] https://youtu.be/PYu9Zkwmhw0.

11. Wikipedia. *SIGAINT.* [En línea] [Citado el: 8 de 10 de 2018.] https://en.wikipedia.org/wiki/SIGAINT.

12. Wikipedia. *Proton Mail.* [En línea] [Citado el: 8 de 10 de 2018.] https://es.wikipedia.org/wiki/ProtonMail.

13. Redeszone. *Envía archivos de forma privada a través de la red Tor con OnionShare.* [En línea] [Citado el: 8 de 10 de 2018.] https://www.redeszone.net/2017/01/31/envia-archivos-forma-privada-traves-la-red-tor-onionshare/.

14. La mirada del replicante. *Mantén todas tus comunicaciones anónimas con Torsocks.* [En línea] [Citado el: 6 de 10 de 2018.] https://lamiradadelreplicante.com/2012/03/08/manten-todas-tus-comunicaciones-anonimas-con-torsocks/.

15. N+1. *La guía última hacia la red oscura.* [En línea] [Citado el: 28 de 10 de 2018.] https://nmas1.org/material/2017/11/09/*Darknet*.

16. Wikipedia. *Internet Profunda.* [En línea] [Citado el: 1 de 10 de 2018.] https://es.wikipedia.org/wiki/Internet_profunda.

17. Tor. *Tor: Overview.* [En línea] [Citado el: 31 de 10 de 2018.] https://www.torproject.org/about/overview.html.en.

18. Genbeta. *¿Cómo funciona la red Tor?* [En línea] [Citado el: 31 de 10 de 2018.] https://www.genbeta.com/seguridad/como-funciona-la-red-tor.

19. INCIBE. *Tor, servicios ocultos y desanonimización.* [En línea] [Citado el: 26 de 09 de 2018.] https://www.incibe-cert.es/blog/tor-servicios-ocultos-desanonimizacion.

20. Yolanda Corral. *Tor vs. Freenet. Diferencias redes inproxy y outproxy.* [En línea] [Citado el: 8 de 10 de 2018.] https://www.yolandacorral.com/tor-vs-freenet/.

21. Consumer. *Freenet, la libertad primero.* [En línea] [Citado el: 29 de 10 de 2018.] http://www.consumer.es/web/es/tecnologia/internet/2006/05/15/151941.php.

22. Genbeta. *Así es Freenet, Deep Web alternativa a Tor e I2P.* [En línea] [Citado el: 6 de 10 de 2018.] https://www.genbeta.com/a-fondo/asi-es-freenet-deep-web-alternativa-a-tor-e-i2p.

23. PabloYglesias. *#MundoHacker: Freenet, una alternativa inproxy a TOR o I2P.* [En línea] [Citado el: 29 de 10 de 2018.] https://www.pabloyglesias.com/freenet-red-*inproxy*/.

24. I2P. [En línea] [Citado el: 3 de 11 de 2018.] https://geti2p.net/es/.

25. Genbeta. *I2P, la nueva generación de la Deep Web.* [En línea] [Citado el: 3 de 11 de 2018.] https://www.genbeta.com/actualidad/i2p-la-nueva-generacion-de-la-deep-web.

26. Omicrono. *Qué son las redes I2P: el Internet invisible.* [En línea] [Citado el: 3 de 11 de 2018.] https://omicrono.elespanol.com/2017/07/red-i2p-anonimato-en-internet/.

27. Redeszone. *HORNET, una red anónima de alta velocidad.* [En línea] [Citado el: 6 de 10 de 2018.] https://www.redeszone.net/2015/07/28/hornet-una-red-anonima-de-alta-velocidad/.

28. Omicrono. *Investigadores crean una red anónima de alta velocidad, la sucesora de TOR.* [En línea] [Citado el: 29 de 10 de 2018.] https://omicrono.elespanol.com/2015/07/hornet-sucesor-de-tor/.

29. Gizmodo. *Riffle, la red anónima del MIT que soluciona los problemas de seguridad de Tor.* [En línea] [Citado el: 6 de 10 de 2018.] https://es.gizmodo.com/riffle-la-red-anonima-del-mit-que-soluciona-los-proble-1783517629.

30. Xataxa. *El MIT ha creado una red anónima que dice ser hasta 10 veces más rápida que Tor.* [En línea] [Citado el: 29 de 10 de 2018.] https://www.xataka.com/privacidad/el-mit-ha-creado-una-red-anonima-que-dice-ser-hasta-10-veces-mas-rapida-que-tor.

31. Globb Security. *Riffle, la red de anonimato que promete mejorar la privacidad de Tor.* [En línea] [Citado el: 29 de 10 de 2018.] https://globbsecurity.com/riffle-red-anonimato-mejorar-tor-39150/.

32. GNU's Framework for Secure *Peer*-to-*Peer* Networking. [En línea] [Citado el: 3 de 11 de 2018.] https://gnunet.org/.

33. Genbeta. *Esto es lo que te encuentras al navegar por ZeroNet, el Internet alternativo mediante P2P.* [En línea] [Citado el: 29 de 10 de 2018.] https://www.genbeta.com/intercambio-de-ficheros/esto-es-lo-que-te-encuentras-al-navegar-por-zeronet-el-internet-alternativo-mediante-p2p.

34. FayerWayer. *Facebook ahora tiene su versión Onion.* [En línea] [Citado el: 29 de 10 de 2018.] https://www.fayerwayer.com/2014/10/facebook-ahora-tiene-su-version-onion/.

35. Genbeta. *47 páginas .onion para visitar el lado amable de la Deep Web.* [En línea] [Citado el: 6 de 10 de 2018.] https://www.genbeta.com/web-20/47-paginas-onion-para-visitar-el-lado-amable-de-la-deep-web.

36. Xataka. *Una semana en la Deep Web. Esto es lo que me he encontrado.* [En línea] [Citado el: 24 de 09 de 2018.] https://www.xataka.com/analisis/una-semana-en-la-deep-web-esto-es-lo-que-me-he-encontrado.

37. Xataka. *Una semana en la Deep Web, tres años después.* [En línea] [Citado el: 3 de 11 de 2018.] https://www.xataka.com/analisis/una-semana-en-la-deep-web-tres-anos-despues.

38. TheHackerWay. *20 eepsites en la web profunda de I2P que te podrían interesar.* [En línea] [Citado el: 3 de 11 de 2018.] https://thehackerway.com/2015/02/05/20-eepsites-en-la-web-profunda-de-i2p-que-te-podrian-interesar/.

39. Periodismo actual. *Las principales vulnerabilidades de Tor.* [En línea] [Citado el: 30 de 10 de 2018.] https://periodismoactual.com/las-principales-vulnerabilidades-de-tor.

40. Redeszone. *TorMoil, una grave vulnerabilidad que expone la IP de los usuarios de Tor.* [En línea] [Citado el: 6 de 10 de 2018.] https://www.redeszone.net/2017/11/06/tormoil-vulnerabilidad-tor/.

41. Muy seguridad. *Publican una vulnerabilidad zero-day hallada en Tor Browser.* [En línea] [Citado el: 6 de 10 de 2018.] https://www.muyseguridad.net/2018/09/11/vulnerabilidad-zero-day-tor-browser/.

42. Globb Security. *Análisis de la red Tor: defectos y vulnerabilidades.* [En línea] [Citado el: 30 de 10 de 2018.] https://globbsecurity.com/vulnerabilidades-tor-35381/.

43. Redeszone. *Solucionada la vulnerabilidad I2P que identificaba a los usuarios.* [En línea] [Citado el: 30 de 10 de 2018.] https://www.redeszone.net/2014/07/29/solucionada-la-vulnerabilidad-i2p-que-identificaba-los-usuarios/.

44. TheHackerWay. *Instalación de un proxy TOR2WEB para acceder a servicios ocultos desde Internet.* [En línea] [Citado el: 6 de 12 de 2018.] https://thehackerway.com/2015/01/22/instalacion-de-un-*proxy*-tor2web-para-acceder-a-servicios-ocultos-desde-internet/.

45. TechPlusMe. *How to access Deep Web onion sites without using Tor.* [En línea] [Citado el: 6 de 12 de 2018.] http://www.techplusme.com/web/access-deep-web-onion-sites-without-using-tor.

46. Whonix. *Anonymity Operating System Comparison.* [En línea] [Citado el: 6 de 10 de 2018.] https://www.whonix.org/wiki/Comparison_with_Others.

47. Zeerodium. *Tor Browser Zero-Day Exploits Bounty (Expired).* [En línea] [Citado el: 2018 de 12 de 8.] https://zerodium.com/tor.html.

48. We Are Segment. *TorMoil – Deanonymize Tor Browser Users with Automount.* [En línea] [Citado el: 6 de 12 de 2018.] https://www.wearesegment.com/research/tormoil-deanonymize-tor-browser-users-with-automount/.

49. The Register . *Doubts cast over FBI 'leaky CAPTCHA' Silk Road rapture.* [En línea] [Citado el: 8 de 12 de 2018.] https://www.theregister.co.uk/2014/09/08/leaky_captcha_behind_fbis_silk_road_rapture/.