Un paseo por la Deep Web

Autor	Carlos Ortega Castillo
Tutor del proyecto	Jorge Chinea
Profesor de la asignatura	Víctor García Font.
Fecha de entrega	1 de enero de 2018
Máster de Seguridad de las Tecnologías de la Información y las Comunicaciones (MISTIC)	
INCIBE: Un paseo por la Deep Web.	

Resumen

El presente proyecto se centra en conocer la internet profunda o Deep Web. Se realizan dos aproximaciones, una teórica donde se analiza la Deep Web enumerando los distintos tipos de redes que podemos encontrar, la infraestructura que utiliza y la evolución de la misma, y por otro lado, se realiza una aproximación práctica, accediendo a ella y descubriendo que servicios e información que es ofrecida.

El proyecto está centrado principalmente en el análisis de la red Tor, se realiza un estudio teórico en profundidad sobre la infraestructura y componentes que la forman. Gracias al análisis y compresión de la tecnología utilizada en la red Tor, se lleva a cabo la implementación de dos servicios ocultos.

Summary

The present project focuses on knowing the Deep Web. Two approaches are carried out, a theoretical one where the Deep Web is analyzed, enumerating the different types of networks that we can find, the infrastructure that it uses and the evolution of it, and on the other hand, a practical approach is made, accessing it and discovering what services and information is offered.

The project is mainly focused on the analysis of the Tor network, an in-depth theoretical study is carried out on the infrastructure and its components. Thanks to the analysis and compression of the technology used in the Tor network, the implementation of two hidden services is carried out.

Índice de imágenes

1 CAPITULO 1: INTRODUCCIÓN

1.1 MOTIVACIÓN

En el mundo en el que nos movemos, cada vez más los usuarios quieren mantener su privacidad y anonimato en la red. A raíz de esto, han surgido una serie de redes que ofrecen estas características los usuarios que la utilizan, así como acceder a contenidos suministrados en internet en aquellos países donde existe una gran censura sobre los mismos. Por otro lado, al preservar el anonimato de los usuarios, los contenidos suministrados son de todo tipo, tanto legales como ilegales.

1.2 OBJETIVOS

Los objetivos a conseguir son los siguientes:

1) Introducción a la Deep Web.

2) Comprender porque surgen este tipo de redes (TOR, I2P, Freenet).

3) Comprender los distintos tipos de redes y que ofrece cada una de ellas (TOR, I2P, Freenet).

4) Comprensión de la infraestructura que da soporte a esta red (TOR).

5) Riesgos y amenazas del uso de esta red (TOR).

6) Compresión del software necesario para acceder a la red (TOR).

7) Caso práctico (TOR):
    a. Acceso a la red.

    b. Tipos de servicios e información que se puede encontrar en dicha red.

8) Evolución de las redes, nuevas redes.

1.3 METODOLOGÍA

El proyecto está dividido en seis etapas, las cuales se describen a continuación:

1) **Planificación:** En esta etapa, se define el alcance y se establecen las acciones que se van a llevar a cabo en el proyecto, se definen los objetivos a alcanzar, un calendario con el listado de tareas a realizar para finalizar cada una de las fases descritas.

2) **Recopilación de información:** En esta etapa, se consulta la información disponible al tema a tratar, recogiendo datos de fuentes fiables.

3) **Análisis de la información:** En esta fase, con los datos recogidos en la etapa anterior, es donde se realiza la aproximación teórica del proyecto.

4) **Diseño e implementación:** A partir del análisis de la información obtenida en las fases anteriores, se define una aproximación práctica a realizar.

5) **Análisis de los resultados y conclusiones:** Una vez se ha realizado la aproximación teórica y práctica, se tiene la información suficiente para analizar si se han alcanzados los objetivos descritos en el presente plan, así como las conclusiones obtenidas del trabajo realizado.

1.4 LISTADO DE TAREAS Y PLANIFICACIÓN TEMPORAL

Para cada una de las fases mencionadas en el apartado anterior, tienen asociadas un conjunto de tareas a realizar, así como una fecha de entrega de las mismas. El seguimiento de cada una de estas fases están asociadas con los entregables de la asignatura, los cuales permiten el seguimiento y control del proyecto.

Hito/Fase	**Tareas**	**Entregable**	**Fecha**
1. Planificación	- Presentación del TFM. - Objetivos. - Metodología. - Listado de Tareas. - Planificación Temporal. - Revisión del arte/Contexto	PEC1	09/10/2017
2. Recopilación de información. 3. Análisis de la información.	- Aproximación teórica: ➢ Enumeración de tipos de redes. ➢ Descripción de la infraestructura.	PEC2	06/11/2017
4. Diseño e implementación.	- Aproximación práctica: ➢ Estudio del software necesario. ➢ Acceso a la red. ➢ Servicios e información ofrecida.	PEC3	04/12/2017
5. Análisis de los resultados y conclusiones. *Memoria Final*	- Análisis de los resultados: ➢ Riesgos y amenazas del uso de esta red. ➢ Evolución de las redes, nuevas redes. - Conclusiones.	PEC4	01/01/2018

1.5 CONTEXTO

Para entender que es la Deep Web, primero definiremos tres conceptos a tener en cuenta:

- La **Deep Web** engloba toda la información que está oculta y es privada. Es decir, son todos aquellos contenidos que no pueden ser indexados por los motores de búsqueda como puede ser Google.

  - Páginas web con contenido dinámico.
  - Páginas web bloqueadas (Capcha, pragma no-cache, Robots.txt).
  - Sitios no linkados o enlazados.
  - Páginas que el buscador decidió no indexar.
  - Documentos con formatos no indexables.
  - Indexados, pero no accesibles con criterios de búsqueda convencionales.
  - Sitios con nombres de dominio no controlados por IANA (Emercoin, Manecoin, name.space…).

- La **Dark Web** es contenido público que existe en las Dark Nets, redes superpuestas al Internet público y que requieren de software específico, configuraciones o autorización para acceder.
  - "La Deep Web es la recopilación de todo lo que hay fuera de los buscadores"
  - "La Dark Web forma parte de la Deep Web, aunque es algo distinto"

- La **Dark Net** son redes independientes que forman la Dark Web. Son las redes específicas que alojan las páginas de la Dark Web, son redes como TOR, I2P o Freenet.
  - "Las Dark Nets es lo más profundo de Internet, ocultando lo que hay dentro de la DarkWeb"

En este proyecto se van a tratar las principales redes como son Tor, Freenet e I2P, las cuales forman parte de la Dark Net, por ello, se realiza una breve introducción a cada una de ellas para conocer que es lo que nos ofrece cada una:

- **TOR** (The Onion Router) surgió para mejorar la privacidad de los usuarios de internet, ya que la identidad de los usuarios no es revelada manteniendo la integridad y el secreto de la información que vieja sobre esta red, además de evitar la censura.
- **Freenet** consiste en una red descentralizada y resistente a la censura. Tiene como objetivo proporcionar la libertad de expresión y el anonimato. Freenet se basa en una red P2P no estructurada de nodos no jerarquizados.
- **I2P** (Invisible Internet Project) es una red que ofrece anonimato y privacidad al usuario, y la gran diferencia con TOR es como están organizados sus nodos.

En la siguiente imagen, se observa contexto temporal de aparición de cada una de las redes mencionadas.

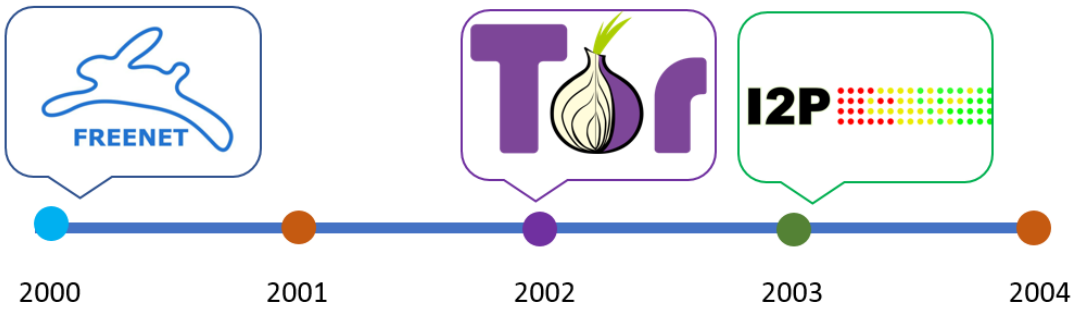


Imagen 1: Cronología

2 CAPITULO 2: RECOPILACIÓN Y ANÁLISIS DE LA INFORMACIÓN

En este capítulo se analiza cómo funciona cada una de las redes a tratar, así como la infraestructura y componen que necesitan cada una de ellas para su funcionamiento.

2.1 RED FREENET

Es una red de distribución de información anónima y descentralizada, no existen servidores para controlar o gestionar la red, ya que trabaja con la puesta en común del ancho de banda y el espacio de almacenamiento de los ordenadores que componen esta red. El objetivo de Freenet es almacenar documentos y permitir su acceso por medio de una clave asociada.

Los contenidos se almacenan en los Datastore en el disco dura de cada usuario, y se mantiene cifrado, y su objetivo es que se mantengan disponibles en la mayor cantidad de datastore en la red.

Como se ha comentado anteriormente, cada uno de los documentos tiene asociado una clave, cuando se quiere encontrar un documento en la red, el usuario envía un mensaje a un nodo solicitando el documento junto con su clave. Si el documento no lo encuentra en su datastore local, entonces realiza una petición a otro nodo vecino, si este tampoco lo tiene, este nodo vecino realizará la misma petición hasta un número máximo de tiempo de vida. Entre estas peticiones, los nodos intermedios no saben si la petición de ha sido originada por el o es transmisor de esta petición, de esta forma se asegura el anonimato del usuario que realizó la petición.

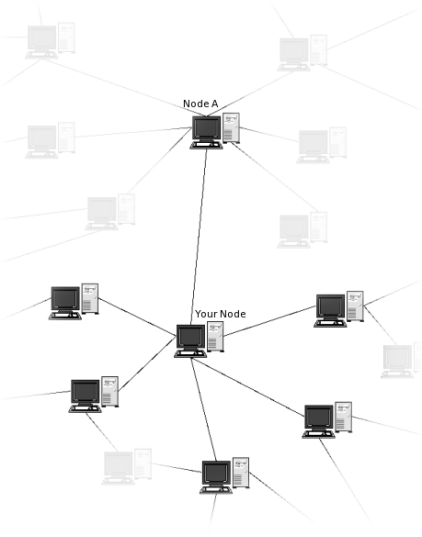


Imagen 2: Ejemplo de nodos

2.2 RED I2P

El proyecto I2P se creó con el objetivo de crear una red virtual privada, resistente a la censura y con un buen rendimiento y escalabilidad, dentro de la cual pueden funcionar gran número de aplicaciones diferentes.

El funcionamiento es similar a otras redes anónimas, en el cual el tráfico es enrutado por varios puntos de la red. Por otro lado, no existen servidores o entidades confiables como en la res Tor, por ello es un red totalmente descentralizada.

La arquitectura de I2P está conformada por varios componentes que interactúan entre si y que se deben entender correctamente para poder tener una visión global sobre su funcionamiento y uso.

I2P se separa entre dos aplicaciones usadas en la red "router" y los puntos finales anónimos "endpoints". Además, introduce otro concepto importante el de "túnel".

2.2.1 TÚNELES

Un túnel es un camino directo a través de una lista de routers seleccionada. Se usa un cifrado por capas, en el que cada router solo puede descifrar una capa, siendo la información descifrada la IP del router siguiente y la información cifrada que se envía. Un túnel tiene un punto de inicio "gateway" y un punto final. Por otro lado, los mensajes solo pueden ser enviados en una dirección, y si se quiere enviar un mensaje de respuesta se tiene que crear otro nuevo túnel. Hay dos tipos de túneles:

- **Túneles de salida (outbound):** Envían los mensajes hacia fuera desde el creador del túnel.
- **Túneles de entrada (inbound):** Envían los mensajes hasta el creador del túnel.

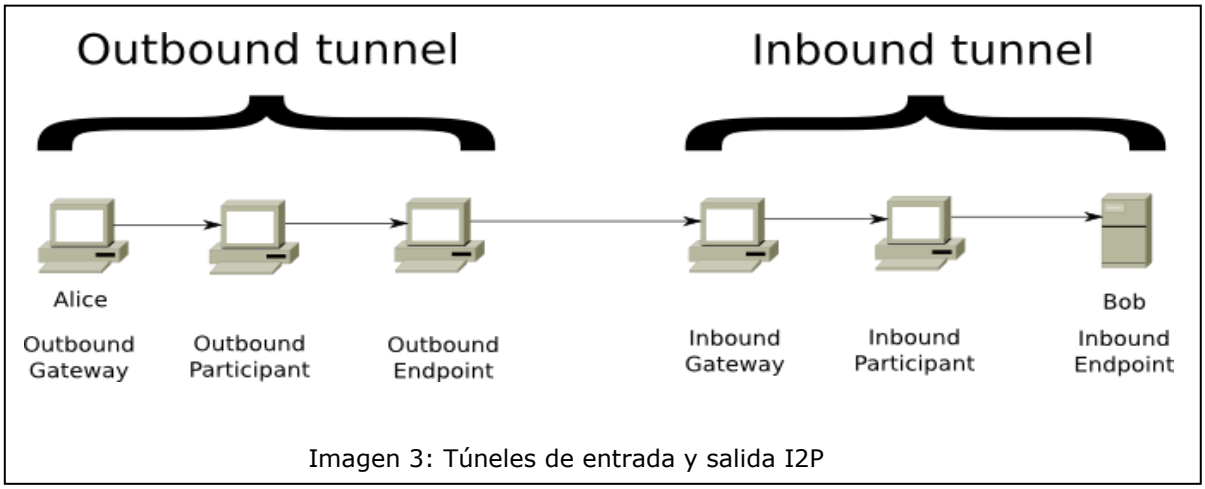


Imagen 3: Túneles de entrada y salida I2P

Como se observa en la imagen anterior, Alice, remitente del mensaje, crea un túnel de salida, mientras que Bob, receptor del mensaje, crea un túnel de entrada. Se utilizan las puertas de salida de los túneles de entrada para recibir los mensajes de cualquier usuario y se envían hasta el destinatario final (Bob), esto se consigue ya que el remitente añade las instrucciones necesarias al mensaje cifrado.

2.2.2 BASE DE DATOS DE LA RED (NETDB)

Este es otro concepto importante, ya que permite compartir dos tipos de datos, "routerInfo" y "leaseSets". A continuación, explicamos estos dos términos:

- **routerInfo:** Proporciona a los routers la información necesaria para poder contactar con un router en particular, como son sus claves públicas, dirección de transporte, etc.

El emisor (Alice) crea sus propios túneles de entrada y salida, y obtiene la lista de pares que puede utilizar para realizar los saltos entre túneles.

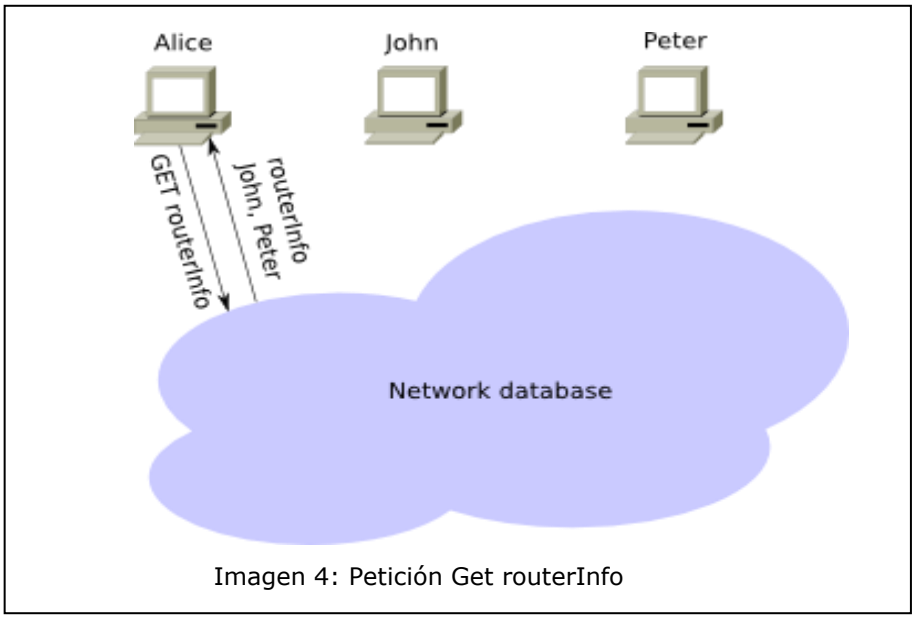


Imagen 4: Petición Get routerInfo

El emisor (Alice) envía un mensaje para construir el primer salto y solicitando a ese router que siga con la construcción del mensaje hasta que se construya el túnel.

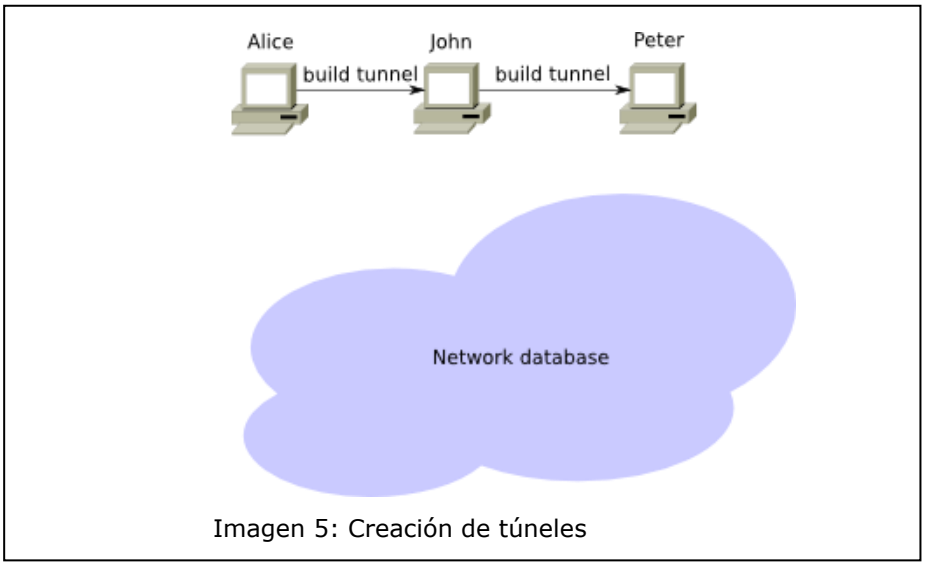


Imagen 5: Creación de túneles

- **leaseSets:** Proporciona a los routers un número de asignaciones, cada una de ellas especifica una puerta de salida de un túnel, la cual le permite alcanzar un destino específico. Esta información es:
    - Gateway de entrada de un túnel para alcanzar un destino específico.
    - Tiempo de espiración del túnel.
    - Par de claves públicas para cifrar el mensaje.

Una vez construido el túnel, descrito anteriormente, Alice solicita la leaseSet del receptor (Bob) en la netDB, selecciona uno de los túneles de salida y envía el mensaje con las instrucciones para que el endpoint del túnel de salida reenvíe el mensaje a uno de los gateways de entrada de Bob.

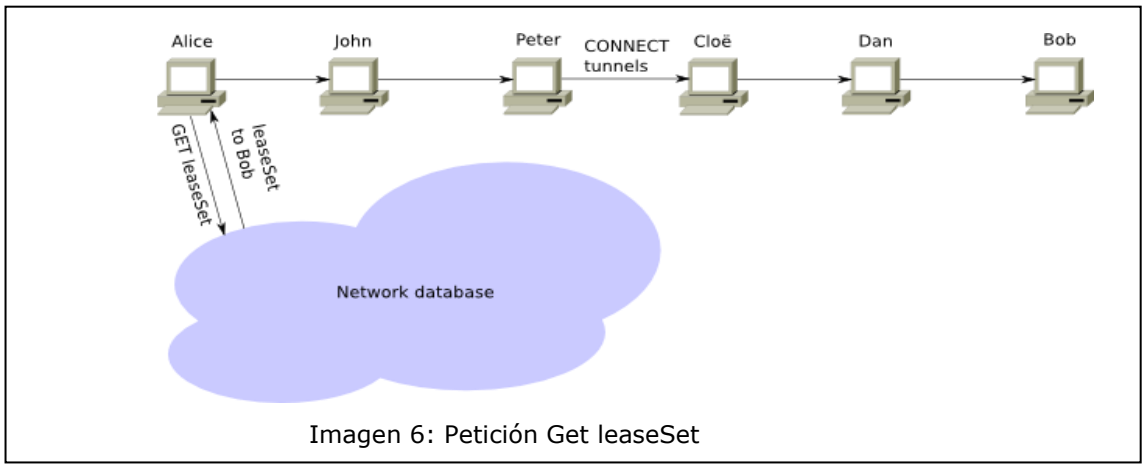


Imagen 6: Petición Get leaseSet

2.3 RED TOR

Es una red anónima soportada y gestionada por el equipo de Tor Project. A diferencia de I2P y Freenet, Tor es una red centralizada, en la que un conjunto de servidores se encargan de gestionar la configuración, así como aportar estadísticas generales sobre el uso de la red. Esta centralización se realiza a través de los servidores son conocidos como "directory authorities" o autoridades de directorio, cuya función más importante es la generación de un consenso que contiene información sobre los relays o repetidores que forman la red Tor. Estos consensos son generados automáticamente cada hora y reflejan el estado de los relays admitidos para ser utilizados por los clientes en sus circuitos.

La red Tor es una red tanto outproxy en donde los usuarios pueden salir hacia Internet utilizando la plataforma de anonimato, los repetidores que se encuentran disponibles en la red, como inproxy solamente permiten la navegación dentro de la red

2.3.1 RELAYS – REPETIDORES

Un Tor relay es un nodo de la red Tor encargado de enrutar las conexiones:

- **Nodos intermedios (internos):** Son los encargados de enrutar las conexiones. Únicamente enrutan en la red Tor.
- **Nodos de salida (externos):** Son los encargados de enrutar el tráfico hacia fuera de la red Tor.

2.3.2 DESCRIPTORES

Son documentos que se encuentran de forma pública, los cuales almacenan información sobre los relays que forman la red Tor. Estos se pueden descargar de las autoridades de directorio.

2.3.3 CIRCUITOS

Es un canal de comunicación bidireccional el cual permite a un cliente utilizar la red Tor como una solución "inproxy" o "outproxy". Un circuito se compone, como mínimo, de tres relays (entrada, intermedio, salida). El cliente construye sus propios circuitos, y tiene la opción de seleccionar los distintos realys a utilizar, además, debe solicitar la clave pública de cada uno de estos, para poder cifrar los paquetes de datos con cada una de las claves públicas, de esta forma se crean paquetes de datos con múltiples capas de cifrado.

Como se ha comentado anteriormente, el cliente (Alice) obtiene la lista de nodos del servidor de autoridades.

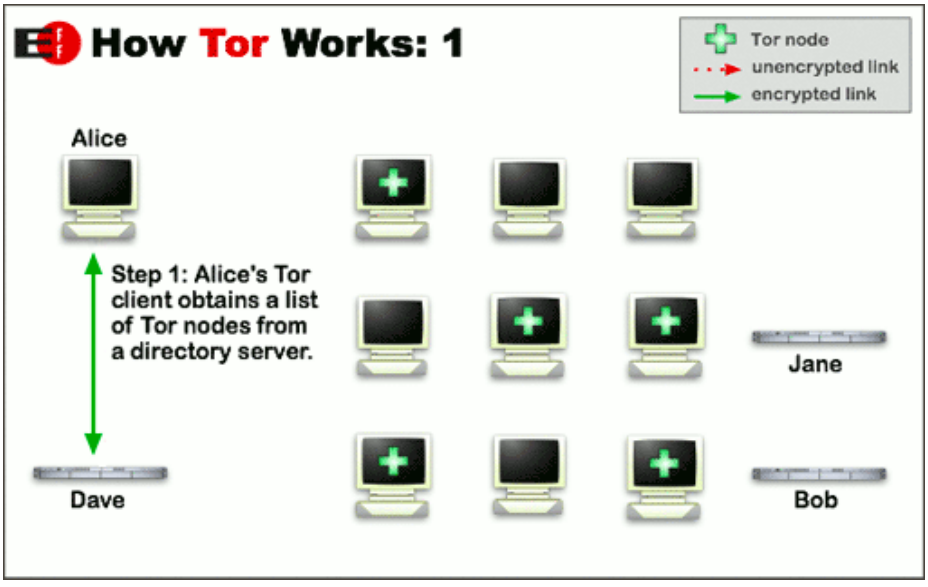


Imagen 7: Cliente solicita lista de nodos desde el servidor de autoridades

El segundo paso, es construir su propio circuito, se puede observar en la siguiente imagen, que una vez el paquete sale por el nodo de salida, este ya no está cifrado, sino que va en texto plano.

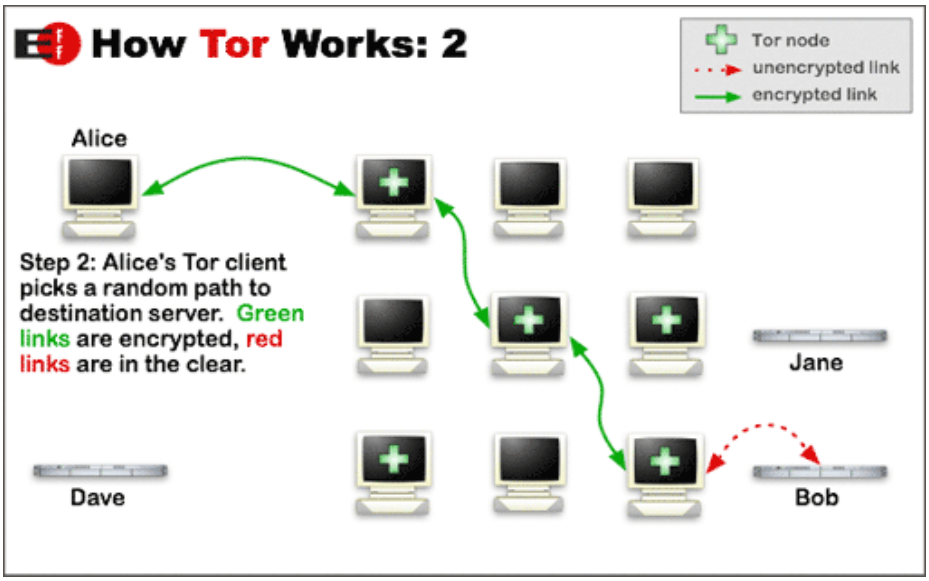


Imagen 8: Cliente crea el circuito

Los circuitos se pueden configurar para que se seleccionen nodos diferentes cada un tiempo determinado, en la siguiente imagen, el circuito es distinto.

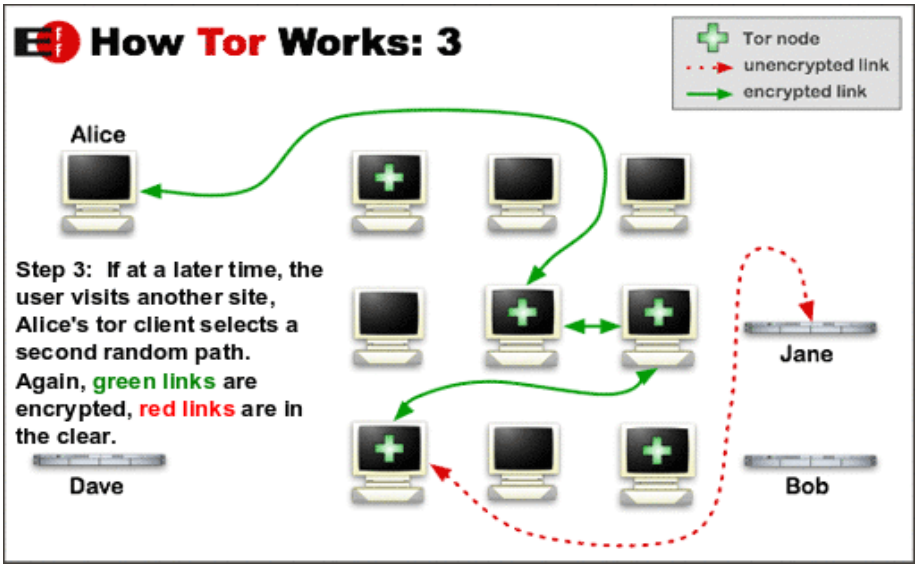


Imagen 9: Generación de un circuito distinto

Un paquete de datos se genera de la siguiente forma:

1) El paquete de datos se cifra con la clave pública del relay de salida (Clave Router C).
2) El cliente utiliza la clave pública del relay intermedio (Clave Router B) añadiendo otra capa de cifrado al paquete de datos.

3) El cliente utiliza la clave pública del relay de entrada (Clave Router A) para añadir la última capa de cifrado sobre el paquete de datos.

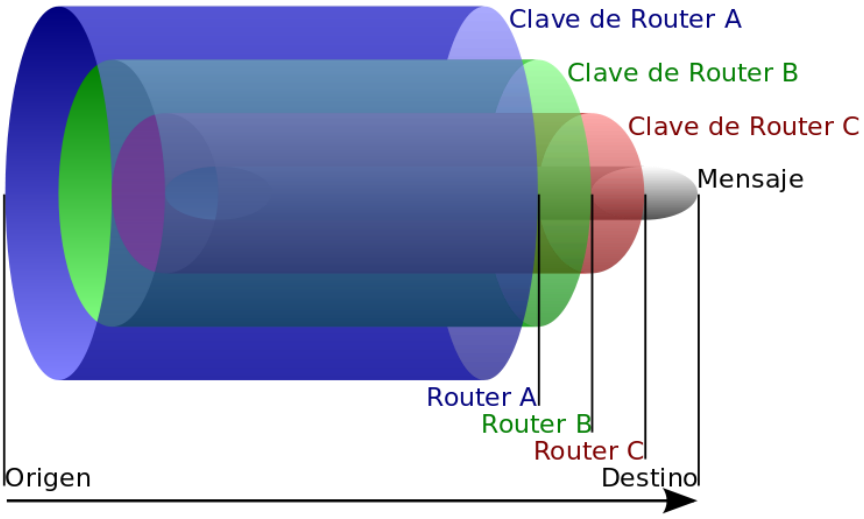


Imagen 10: Estructura de la transmisión de los datos con encaminamiento cebolla

2.3.4 TRANSMISIÓN DEL PAQUETE DE DATOS

Como hemos visto anteriormente, en un circuito por defecto de tres nodos, la transmisión del paquete de datos se realiza de la siguiente forma:

1) El cliente envía el paquete de datos cifrado al primer nodo del circuito (nodo de entrada).
2) El nodo de entrada recibe el paquete de datos del cliente, y utiliza su clave privada para descifrar la capa de cifrado superior del paquete. El resultado de esta operación es el mismo paquete, pero con dos capas de cifrado que solo se pueden descifrar con las claves privadas de los nodos intermedios y salida.
3) El nodo de entrada al eliminar la capa de cifrado accede a la información del siguiente nodo del circuito, es decir, la dirección IP y puerto del nodo intermedio, y envía el paquete al nodo intermedio.
4) El nodo intermedio elimina la capa de cifrado correspondiente, dejando este ya con una sola capa de cifrado, obteniendo la información del nodo de salida, y envía el paquete a este.
5) Finalmente, cuando el nodo de salida recibe el paquete del nodo intermedio, aplica su clave privada para eliminar la última capa de cifrado, obteniendo el paquete original que el cliente desea enviar al destino. En este punto, como comentamos anteriormente, el nodo de salida tiene acceso a toda la información texto plano que el cliente desea enviar al destino.

2.3.5 PUENTES: BRIDGE RELAY

Tor es una red centralizada en la que cada hora, las autoridades de directorio se encargan de generar información sobre los nodos que forman dicha red. Esta información es accesible públicamente, por lo que cualquier persona puede consultarla. Una manera

de censurar la red Tor es, sin duda, controlar y filtrar todo el tráfico que se realice hacia estos nodos, ya que se conocen sus IPs, dejando así inaccesible, y realizando un acto de censura que es utilizar por gobiernos autoritarios. Una manera de proteger y suministrar el acceso a todo aquel que quiera es utilizando los bridge relays. Estos nodos puente, son un mecanismo de defensa, ya que funcionan exactamente igual que un nodo de entrada, pero con la diferencia de que estos no se exponen públicamente.

2.3.6 AUTORIDADES DE DIRECTORIO

Las autoridades de directorio son las encargadas que gestionan la red Tor y que almacenan la información de los relays disponibles para cada momento. Su principal objetivo es garantizar un correcto funcionamiento de la red, y son los únicos servidores dentro de la red Tor que se consideran de confianza, por ello es una red centralizada que depende por completo de estos servidores.

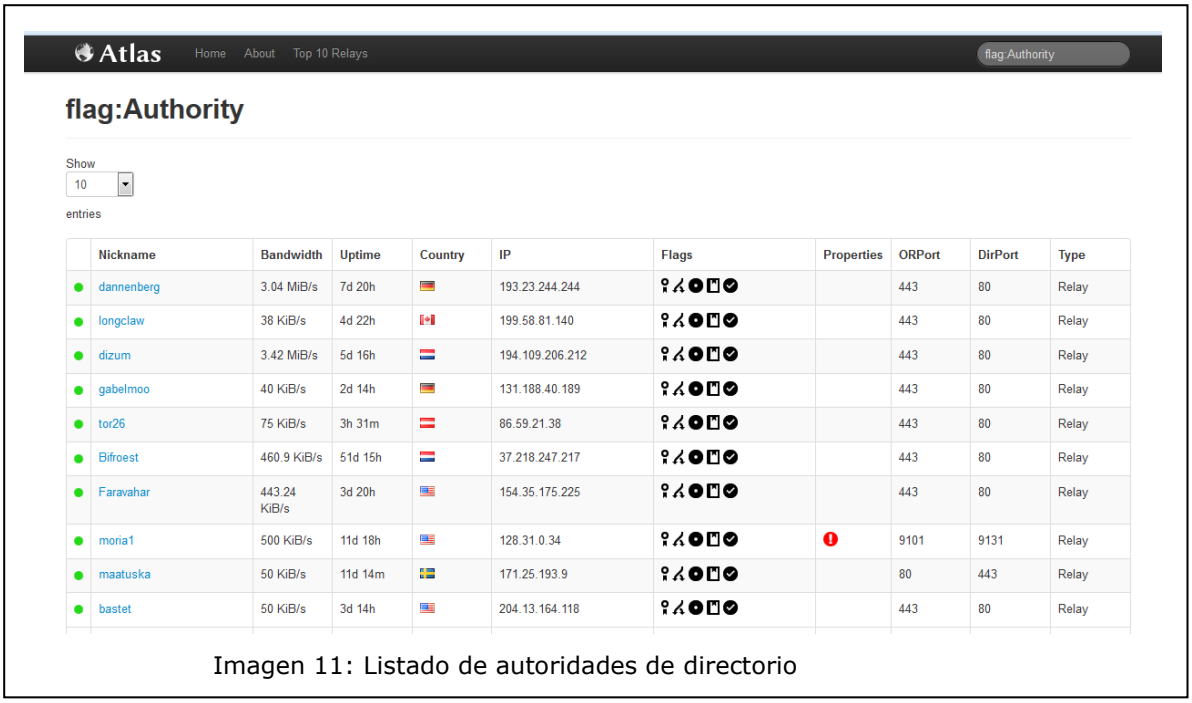
2.3.7 CACHES DE DIRECTORIO

Son las encargadas de consultar y almacenar los documentos de consenso generados por las autoridades de directorio. La principal función de estos servidores es la de servir dichos documentos a los clientes. Estas caches permiten desahogar la carga que reciben las autoridades de directorio, consiguiendo de esta forma, crear menos cuellos de botella y una red más robusta.

2.3.8 PROYECTO ATLAS

Atlas es una aplicación web para descubrir los nodos de Tor, y mostrar información de cada uno de ellos. Anteriormente, se comentaron las autoridades de directorio, las cuales se pueden encontrar en la siguiente url: https://atlas.torproject.org/#search/flag:Authority

Como en apartados anteriores se ha comentado que está disponible la información de los nodos y las autoridades de directorio, vamos a realizar un pequeño paseo por estas.



	Nickname	Bandwidth	Uptime	Country	IP	Flags	Properties	ORPort	DirPort	Type
●	dannenberg	3.04 MiB/s	7d 20h		193.23.244.244			443	80	Relay
●	longclaw	38 KiB/s	4d 22h		199.58.81.140			443	80	Relay
●	dizum	3.42 MiB/s	5d 16h		194.109.206.212			443	80	Relay
●	gabelmoo	40 KiB/s	2d 14h		131.188.40.189			443	80	Relay
●	tor26	75 KiB/s	3h 31m		86.59.21.38			443	80	Relay
●	Bifroest	460.9 KiB/s	51d 15h		37.218.247.217			443	80	Relay
●	Faravahar	443.24 KiB/s	3d 20h		154.35.175.225			443	80	Relay
●	moria1	500 KiB/s	11d 18h		128.31.0.34		!	9101	9131	Relay
●	maatuska	50 KiB/s	11d 14m		171.25.193.9			80	443	Relay
●	bastet	50 KiB/s	3d 14h		204.13.164.118			443	80	Relay

Imagen 11: Listado de autoridades de directorio

Podemos entrar en cada una de las autoridades de directorio y ver la información referente a la misma, en la siguiente imagen se observa bastet que ha sido la última en añadirse (https://blog.torproject.org/introducing-bastet-our-new-directory-authority).

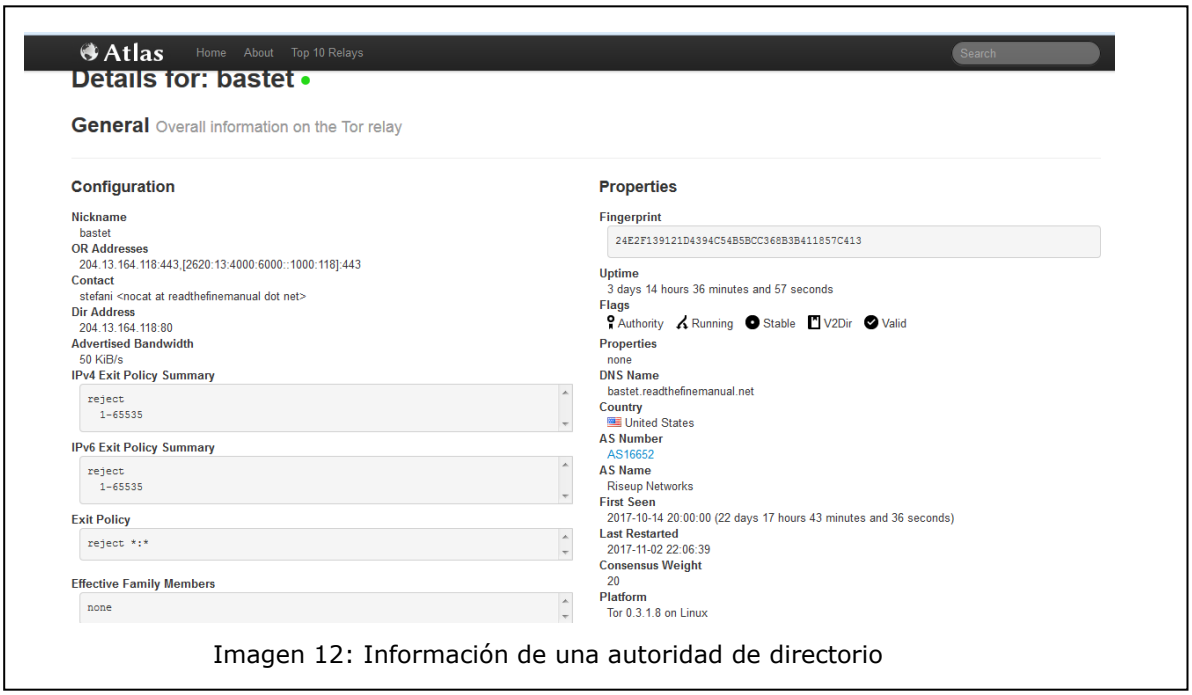
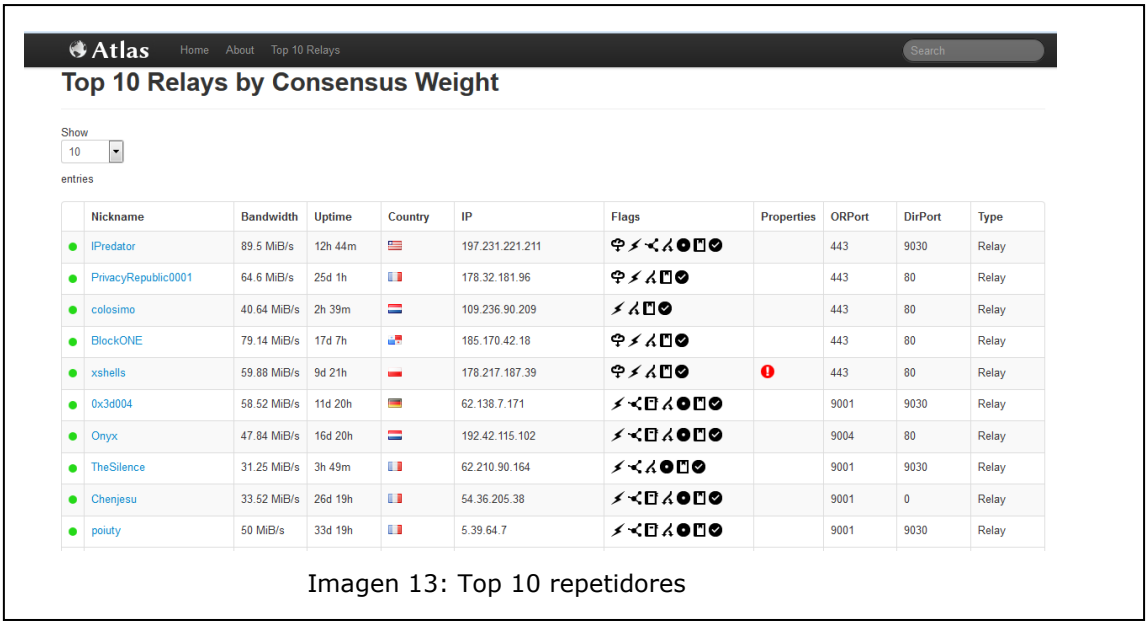


Imagen 12: Información de una autoridad de directorio

También podemos visualizar el top 10 de los nodos, como se muestra en la siguiente imagen.



	Nickname	Bandwidth	Uptime	Country	IP	Flags	Properties	ORPort	DirPort	Type
●	IPredator	89.5 MiB/s	12h 44m		197.231.221.211			443	9030	Relay
●	PrivacyRepublic0001	64.6 MiB/s	25d 1h		178.32.181.96			443	80	Relay
●	colosimo	40.64 MiB/s	2h 39m		109.236.90.209			443	80	Relay
●	BlockONE	79.14 MiB/s	17d 7h		185.170.42.18			443	80	Relay
●	xshells	59.88 MiB/s	9d 21h		178.217.187.39			443	80	Relay
●	0x3d004	58.52 MiB/s	11d 20h		62.138.7.171			9001	9030	Relay
●	Onyx	47.84 MiB/s	16d 20h		192.42.115.102			9004	80	Relay
●	TheSilence	31.25 MiB/s	3h 49m		62.210.90.164			9001	9030	Relay
●	Chenjesu	33.52 MiB/s	26d 19h		54.36.205.38			9001	0	Relay
●	poiuty	50 MiB/s	33d 19h		5.39.64.7			9001	9030	Relay

Imagen 13: Top 10 repetidores

Además de la información de cada uno de ellos, para este caso se ha elegido el primero IPredator.

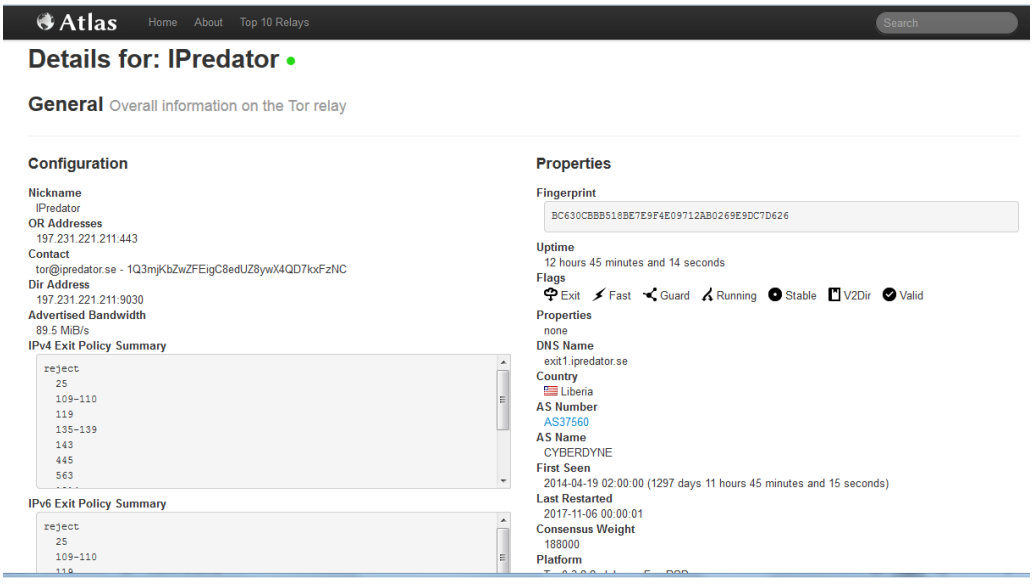


Imagen 14: Información de un repetidor

2.3.9 SERVICIOS OCULTOS

Los servicios ocultos o hidden services, es una de las caracteristicas más importantes que ofrece la res Tor. Estos servicios basados por ejemplo en (TCP, SSH, HTTP, FTP, etc) son configurados en una máquina la cual la red Tor ofrece anonimato sobre está, ya que lo único que está disponible es el servicio configurado, y únicamente accesible desde la red Tor.

2.3.10 COMO SE FORMAN LAS DIRECCIONES .ONION

Cuando se configura un servicio oculto y es desplegado en Tor, se crea un par de claves RSA de 1024 bits. Para construir la dirección se calcula el SHA1 de la clave pública generada, de estos 160 bits que forman el hash, se obtiene la primera mitad y se codifica en Base32, de esta forma se consigue que todos los nombres de dominio (direcciones .onion) tengan una longitud de 16 caracteres, los cuales están formados por números entre 2-7 y letras entra a-z.

3 CAPITULO 3: DISEÑO E IMPLEMENTACIÓN

Una vez realizado el estudio y análisis de las redes en cuestión, y más profundamente la red Tor, el siguiente paso es realizar el acceso a la red Tor.

3.1 ACCESO A LA RED TOR

Para el acceso a la red tor, se utiliza el navegador Tor Browser, lo descargamos desde la url https://www.torproject.org/download/download.

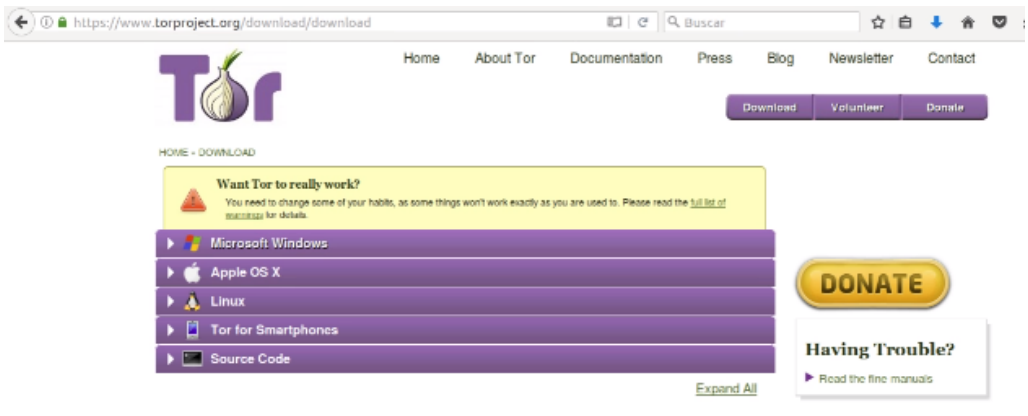


Imagen 15: Descarga de Software Tor Browser

En nuestro caso, realizamos la descarga para un equipo Linux. La descarga contiene una carpeta, ya que Tor Browser no es un instalador, sino que es un ejecutable, como podemos observar en la imagen siguiente:

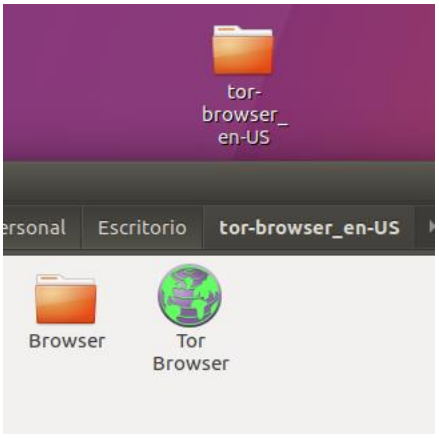


Imagen 16: Contenido de la descarga de Tor Browser

Al ejecutar el software pregunta cómo se va a realizar la conexión:

1) Me gustaría conectar directamente a la red Tor.
2) La conexión a Internet de este equipo está censurada o proxificada. Esta segunda opción está orientada para el acceso desde sitios donde la red Tor está censurada.

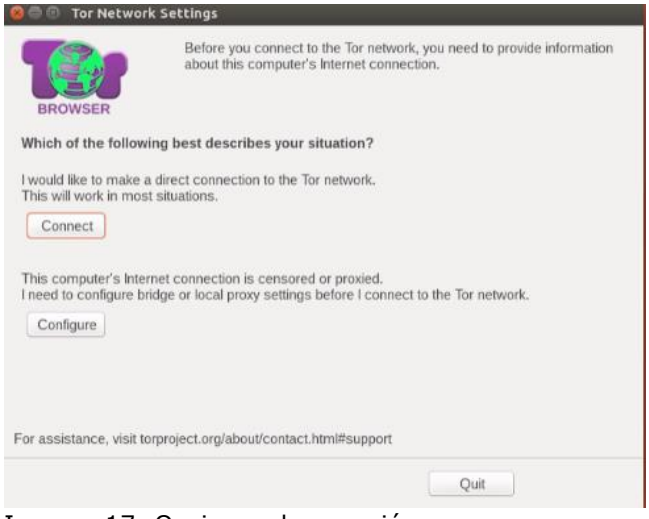


Imagen 17: Opciones de conexión

En nuestro caso, seleccionamos la primera opción, y empieza a realizar la conexión a la red Tor, el establecimiento de la conexión puede durar varios minutos.

Imagen 18: Conectado con la red Tor

Una vez conectado, se inicia el Tor Browser (el cual está basado el Firefox).

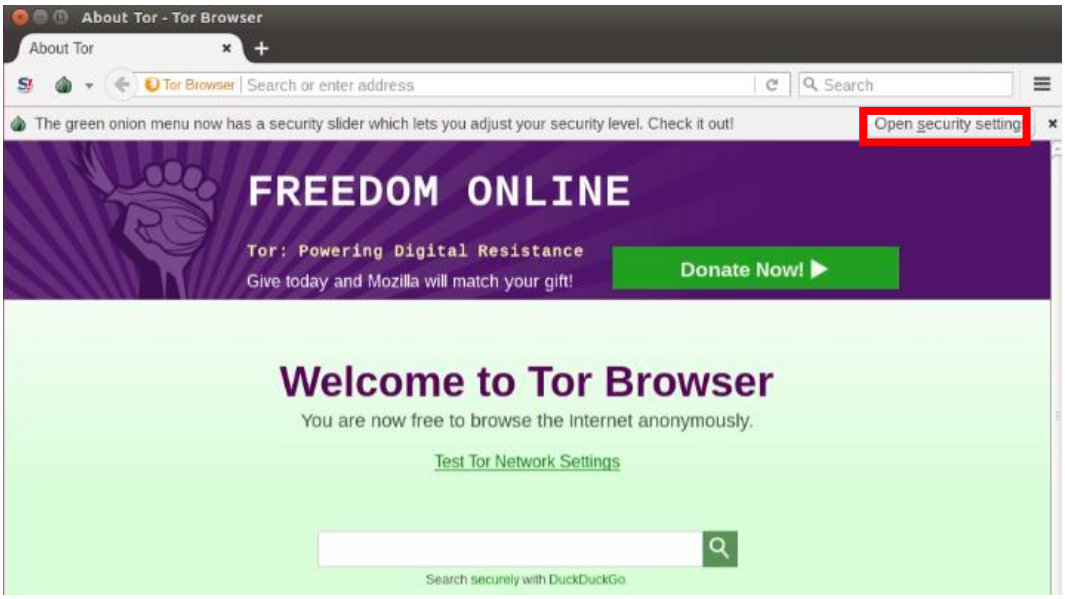


Imagen 19: Inicio del navegador Tor

Se puede consultar las opciones de seguridad, tiene tres niveles, seguridad alto, medio y bajo) contra más seguridad menos funcionalidad. A continuación, se muestran junto con las restricciones de cada uno de ellos.

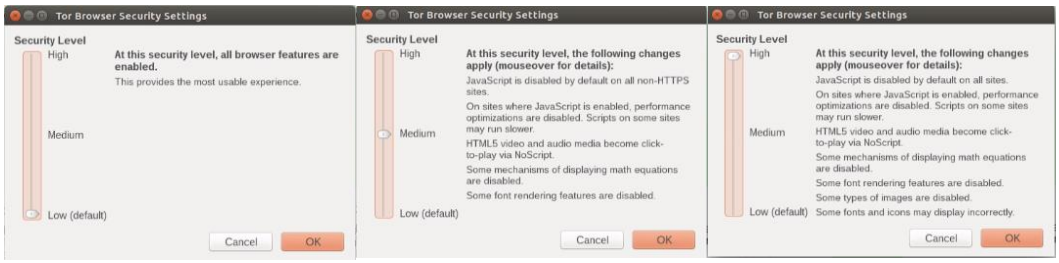


Imagen 20: Niveles de seguridad del navegador Tor

Otra medida de seguridad que tiene preinstalada Tor Browser es NoScript, es una protección extra para la ejecución de JavaScript, Java y otros plugins con dominios de confianza, creando listas negras o listas blancas donde permitir la ejecución.

Imagen 21: Información NoScript

NoScript tiene multitud de opciones de configuración, la cual aumenta en seguridad en la navegación por Tor.

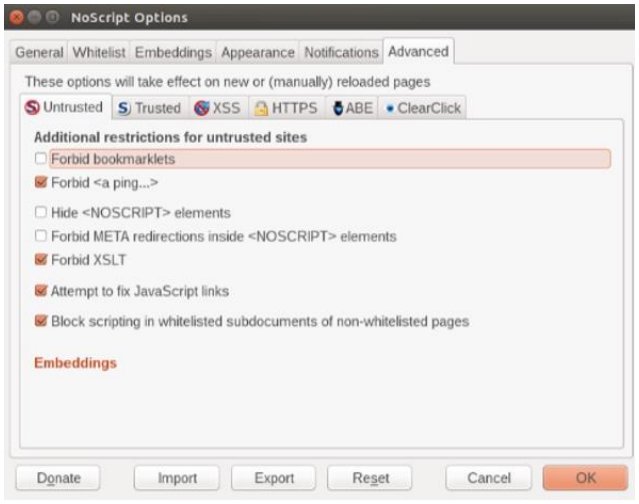


Imagen 22: Opciones de configuración NoScript

Otra medida de seguridad que vemos es que cuando se maximiza el navegador, este avisa que esto puede permitir a las webs determinar el tamaño de tu monitor, lo cual se puede usar para rastrearte.

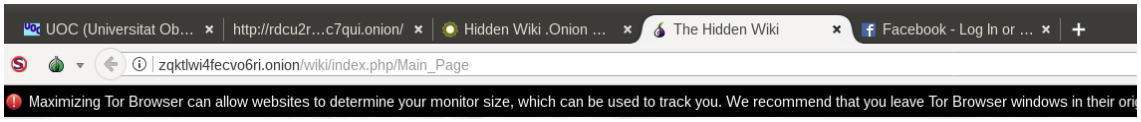


Imagen 23: Aviso al maximizar el navegador

Una vez que hemos visto la medidas de seguridad que tiene implementadas el navegador Tor, vamos a acceder a la web https://ipchicken.com para comprobar la IP con la que estamos saliendo a internet.

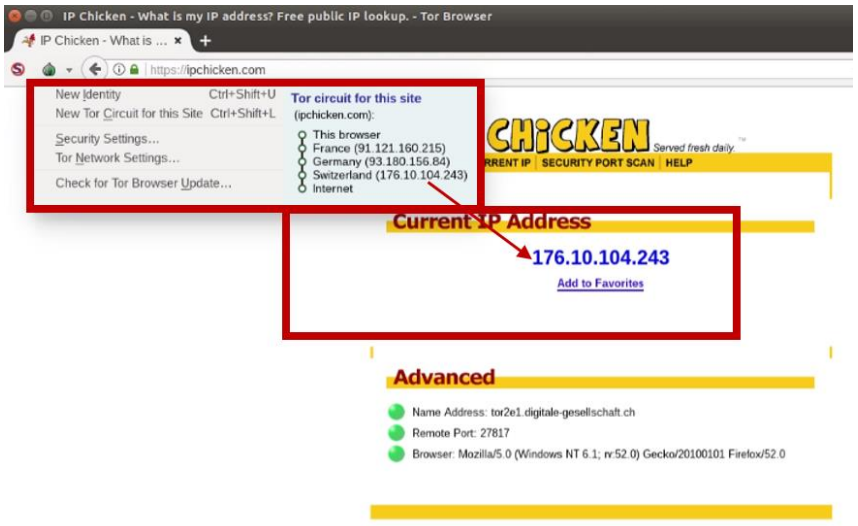


Imagen 24: IP de salida

Como se puede observar en la imagen anterior, comprobamos que la IP de salida es 176.10.104.243. Además, podemos ver el circuito de Tor que estamos siguiendo (France, Germany y Switzerland), podemos renovar el circuito manualmente cada vez que se quiera, renovando así cada uno de los nodos que lo forman, para ello realizamos click en "New Tor Circuit for this Site".

Imagen 25: Nodos que forman el circuito

Si volvemos a acceder a la web https://ipchicken.com, verificamos que nuestra IP ha vuelto a cambiar.

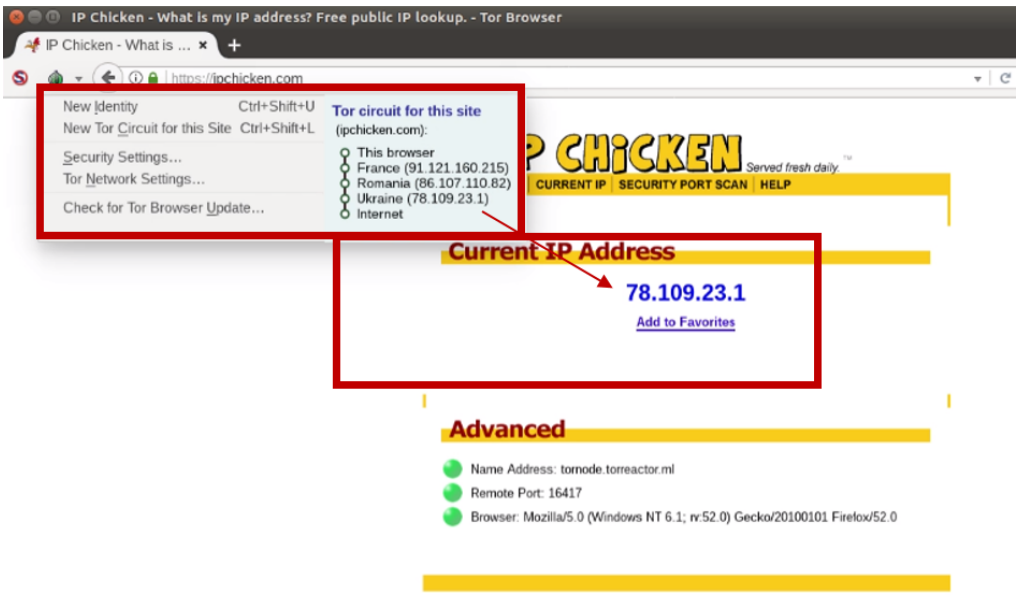


Imagen 26: IP de salida

Las urls .onion no están indexadas y no pueden ser consultadas como podría ser desde un motor de búsqueda como Google, por ello, para poder acceder a una dirección .onion, el autor o alguna persona tiene que publicarla.

Ahora vamos a navegar por la red de tor, es decir, urls .onion, accedemos a la hidden wiki, es una web que contiene direcciones .onion, estructurado por categorías. La url de acceso es: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page

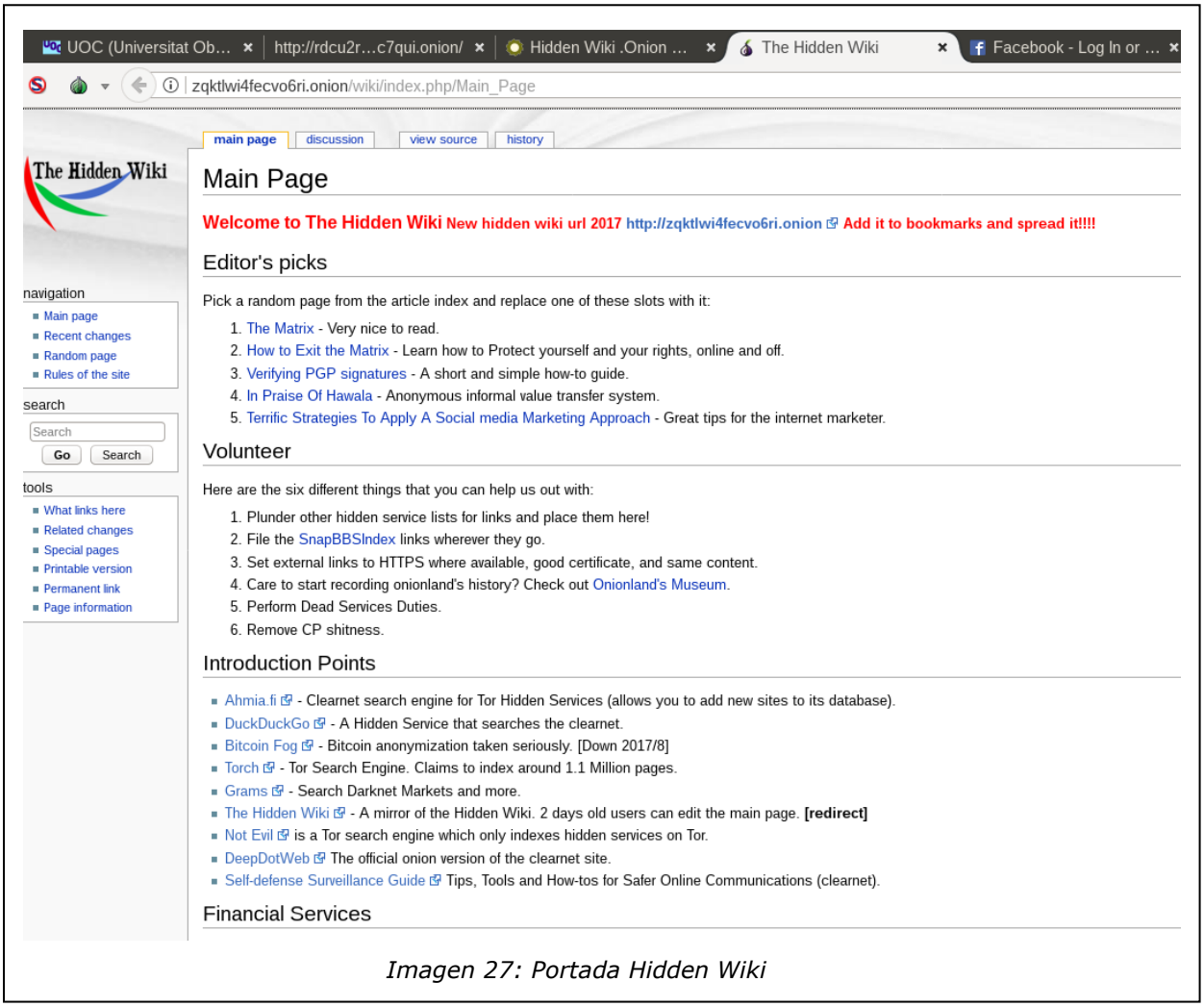


Imagen 27: Portada Hidden Wiki

Las categorías que podemos encontrar son, junto con un listado de enlaces son:

- Introduction Points
- Financial Services
- Commercial Services
- Domain Services
- Anonymity & Security
- Hosting / Web / File / Image
- Blogs / Essays / Wikis
- Email / Messaging
- Social Networks
- Forums / Boards / Chans
- Whistleblowing
- H/P/A/W/V/C Hack, Phreak, Anarchy (internet), Warez, Virus, Crack
- Audio - Music / Streams
- Video - Movies / TV
- Books

- Drugs
- Erotica
- Non-English
- Hidden Services - Other Protocols

Podemos ver, por ejemplo, que Facebook también tiene url .onion: https://www.facebookcorewwwi.onion

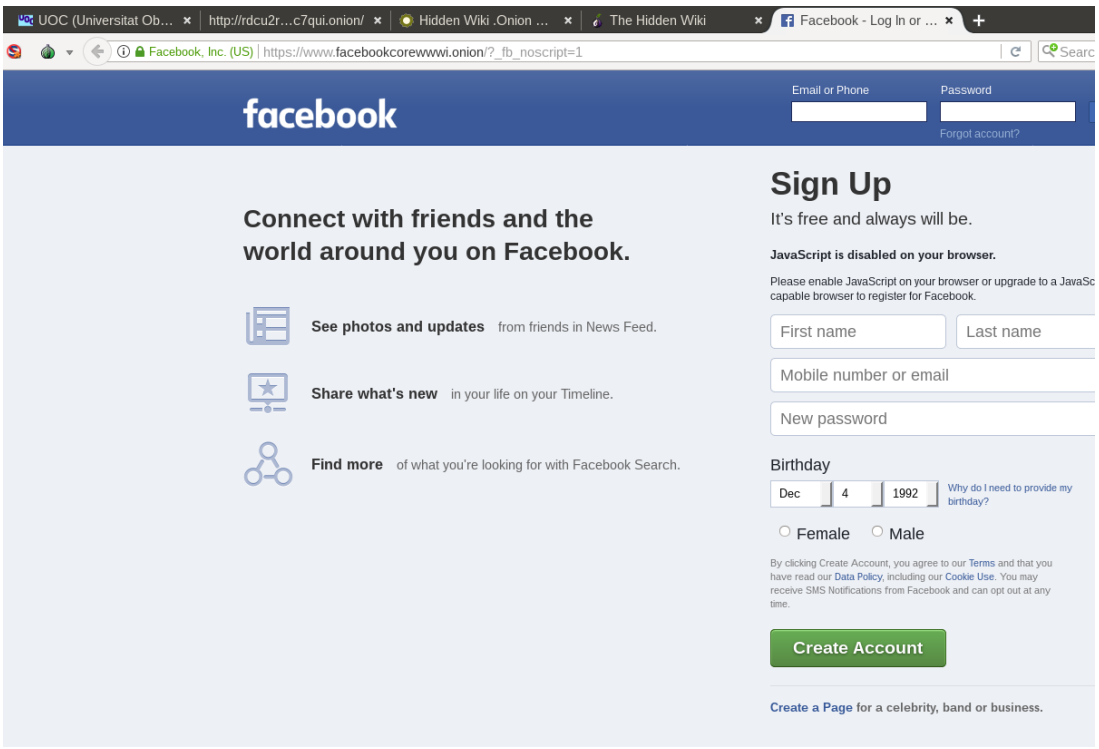


Imagen 28: Sitio web Facebook en red Tor

Como se comentó anteriormente, las webs disponibles no se conocen en su totalidad, ya que estas no están indexadas, la hidden wiki es un lugar donde se puede encontrar un listado de servicios que van actualizando, como en la Internet conocida por todos, se encuentran servicios de todo tipo, Tor es una red que permite el anonimato, y si que es verdad que es posible que ciertos servicios y contenidos ilegales puedan surgir más fácilmente.

Además, comentar que la red Tor es una red que permite tanto la navegación por la red de Tor (internamente), como la navegación por la Internet convencional.

3.2 CASOS PRÁCTICOS DEL USO DE LA RED TOR

Hasta este momento, hemos visto el funcionamiento de red Tor, y de los servicios ocultos, más concretamente, unos ejemplos de las webs que forman la red Tor. En este apartado, se va a realizar la instalación y configuración de dos servicios ocultos:

- Servicio oculto HTTP (Servidor Web).
- Servicio oculto SSH.

Los recursos necesarios para la implementación de los servicios ocultos utilizando la red Tor, son los siguientes:

- Dos máquinas virtuales con el Sistema Operativo Ubuntu Server:
  - Servidor: Contiene los servicios ocultos (Servidor Web y servidor SSH).
  - Cliente: Se utilizará para realizar la conexión por SSH al servidor.

3.2.1 INSTALAR Y CONFIGURAR TOR

1) Instalar Tor:

   sudo apt-get install tor

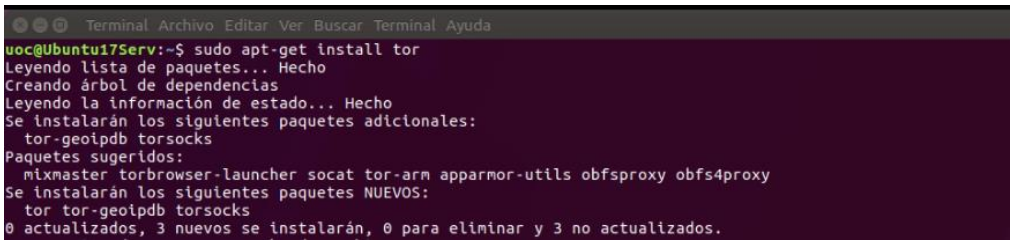


Imagen 29: Instalación de Tor

2) Con la instalación de tor, se crea el usuario *debian-tor*, crearemos su carpeta y nos aseguramos de que el usuario es el propietario de ellas y de también del directorio */var/lib/tor .Ejecutamos los siguientes comandos* como usuario root*:*

   mkdir -p /usr/tor/data
   chown -R debian-tor /usr/tor
   usermod -d /usr/tor -s /bin/bash debian-tor
   chown -R debian-tor: debian-tor /var/lib/tor

En este punto, ya tenemos Tor instalado y configurado, pero no tenemos ningún servicio oculto instalado.

3.2.2 SERVICIO OCULTO HTTP (SERVIDOR WEB)

Ahora vamos a instalar un servidor apache y luego realizaremos la configuración del servicio oculto para que sea accesible desde la red Tor con una url .onion.

1) Instalar el servidor apache
   sudo apt-get install apache2

2) Modificamos el contenido del fichero index.html, para añadir el contenido que queremos tener en nuestra web, del directorio /var/www/html

Imagen 30: Contenido del fichero index.html

3) Realizamos la configuración del servicio web oculto modificando el fichero */etc/tor/torrc*, definiendo cual va a ser el directorio del servicio y el puerto añadiendo las siguientes líneas:
   HiddenServiceDir /var/lib/tor/hiddenweb/
   HiddenServicePort 80 127.0.0.1:80

4) Creamos el directorio que hemos incluido anteriormente.
   sudo mkdir /var/lib/tor/hiddenweb/

5) Le asignamos los permisos necesarios.
   sudo chmod 700 /var/lib/tor/ hiddenweb

6) Reiniciamos el servicio de tor con el usuario debian-tor.
   su debian-tor
   /etc/init.d/tor restart

7) Una vez reiniciado el servicio, crea dos ficheros en el directorio */var/lib/tor/hiddenweb/:*
   a. **Hostname:** Corresponde con el nombre del servicio
   b. **private_key:** Corresponde con la clave privada

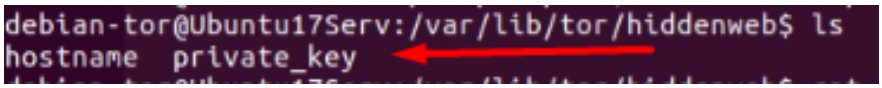


Imagen 31: Muestra de los ficheros creados

8) El contenido del fichero hostname es la url del servicio, para nuestro caso *rdcu2r5pyvhc7qui.onion*

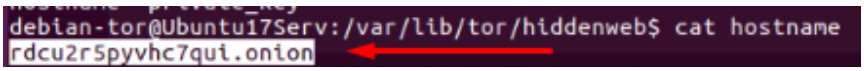


Imagen 32: Dirección .onion servicio HTTP

9) Para acceder al servicio web que se ha creado, utilizamos el navegador tor

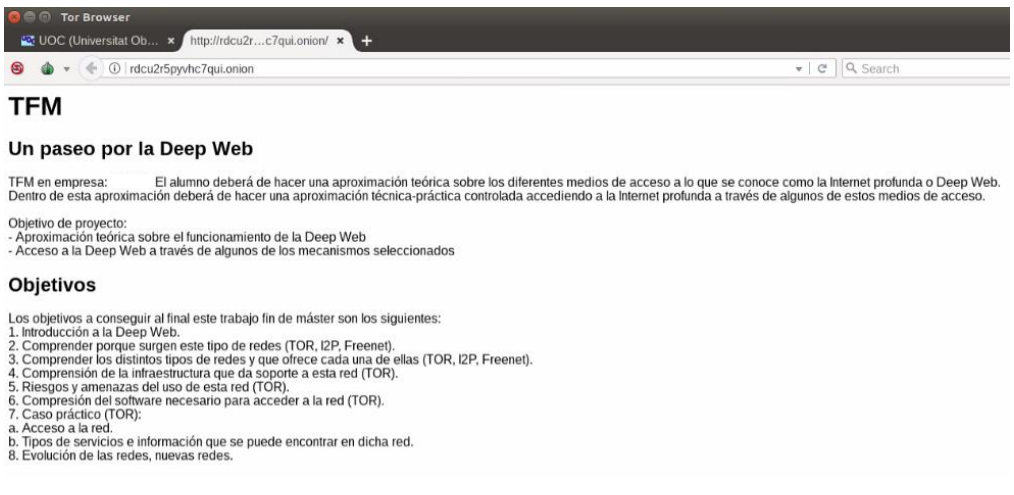


Imagen 33: Visualización del servicio oculto HTTP desde el navegador Tor

3.2.3 SERVICIO OCULTO SSH

Para este segundo caso, vamos a configurar el servicio de SSH, el funcionamiento de estos servicios ocultos que funcionan bajo la red Tor, y en concreto este que vamos a configurar, es como se ilustra en la imagen siguiente.

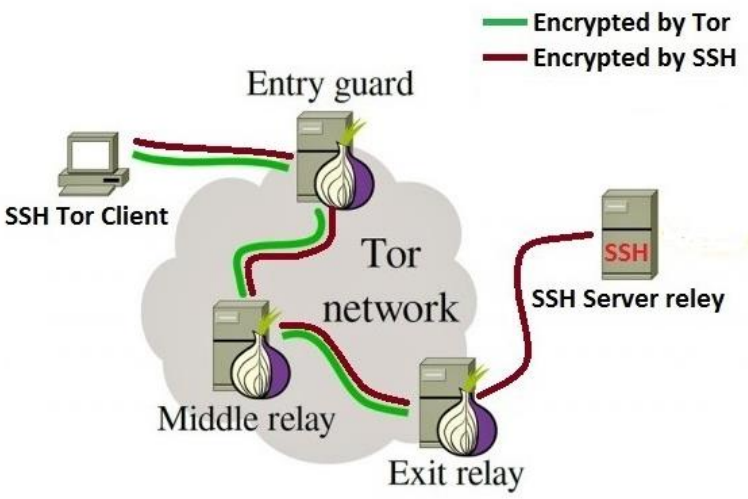


Imagen 34: Funcionamiento de conexión SSH bajo red Tor

En la misma máquina virtual, que ya instalamos con servidor SSH, vamos a configurarla, del modo que utilice la red Tor para poder conectar por SSH. Realizaremos los mismos pasos que para la configuración del servicio web anterior.

1) Realizamos la configuración del servicio web oculto modificando el fichero */etc/tor/torrc*, definiendo cual va a ser el directorio del servicio y el puerto añadiendo las siguientes líneas:

   HiddenServiceDir /var/lib/tor/hiddenssh/
   HiddenServicePort 22 127.0.0.1:22

2) Creamos el directorio que hemos incluido anteriormente

   sudo mkdir /var/lib/tor/hiddenssh/

3) Le damos los permisos necesarios

   sudo chmod 700 /var/lib/tor/ hiddenssh

4) Reiniciamos el servicio de tor con el usuario debian-tor

   su debian-tor
   /etc/init.d/tor restart

5) Una vez reiniciado el servicio, nos crea dos ficheros en el directorio */var/lib/tor/hiddenssh/:*
   a. **Hostname:** Corresponde con el nombre del servicio
   b. **private_key:** Corresponde con la clave privada

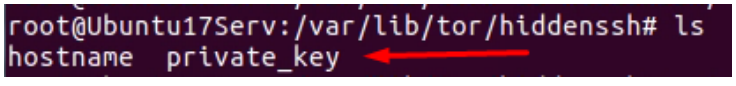


Imagen 35: Muestra de los ficheros creados

6) El contenido del fichero hostname es la url del servicio, para nuestro caso *m3knpm6njw7ly3sc*.onion

Imagen 36: Dirección .onion servicio SSH

7) Instalamos Tor en la máquina cliente desde la que conectaremos por SSH.

sudo apt-get install tor

8) Realizamos la conexión utilizando el siguiente comando

torify ssh uoc@m3knpm6njw7ly3sc.onion

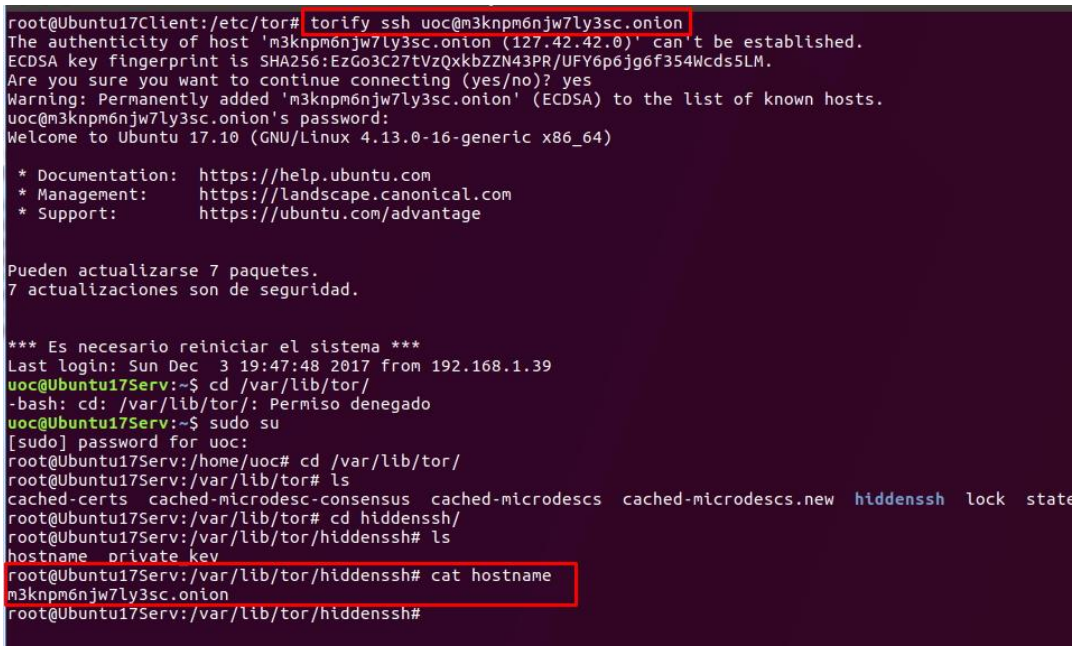


Imagen 37: Conexión SSH desde cliente a servidor utilizando red Tor

Como hemos visto, se pueden crear tantos servicios como se requieran, todos ellos utilizando la red Tor, la configuración de estos servicios es bastante sencilla. Además, en este último caso, parece una idea bastante interesante configurar el servicio de SSH, ya que no se ha tenido que realizar ninguna configuración en el router para abrir un puerto específico y redirigirlo al puerto 22 (puerto por defecto utilizado por SSH) de la máquina virtual para que pueda se pueda acceder desde el exterior de la red interna. Ante un posible ataque, lo primero que realizamos sería un escaneo de puertos para ver cuales están abiertos y ver qué servicios se están ofreciendo, en este caso estamos protegidos ante este tipo de recopilación de información, y posibles ataques contra el servicio SSH configurado.

4 CAPITULO 4: ANÁLISIS DE LOS RESULTADOS

4.1 RIESGOS Y AMENAZAS DEL USO DE ESTA RED

La red Tor surge, como objetivo principal, dar anonimato y privacidad a los usuarios que navegan por esta, por lo tanto, el mayor riesgo del uso de Tor es comprometer esta privacidad y anonimato.

Uno de los puntos críticos de la infraestructura de la red Tor son los nodos de salida, ya que estos conocen hacía donde se dirigen las peticiones realizadas por los usuarios, además que todo el tráfico va cifrado salvo en el nodo de salida.

Por otro lado, como en todo software o infraestructura, a lo largo de los años de vida de la red Tor, se han detectado vulnerabilidades en el Tor Browser (basado en el navegador Firefox). En el mes de diciembre de este año, el investigador Filippo Cavallarin, detectó una vulnerabilidad la cual permitía revelar la dirección IP de los usuarios que navegaban por la red anónima de Tor.

4.2 MITOS Y LEYENDAS

Después de realizar un recorrido por la Deep Web, más en concreto sobre la red Tor, hay una serie de mitos a desmentir:

- Todo el contenido y servicios que se ofrecen son ilegales.
- Todos los usuarios de estas redes son ciberdelincuentes.

Estas redes surgen para ofrecer al usuario anonimato, privacidad y evadir la censura que ciertos países realizan sobre sus ciudadanos. En el estudio de la red Tor, se ha demostrado que hay direcciones .onion las cuales ofrecen contenidos y servicios totalmente legales como es el caso de Facebook.

No hay que criminalizar la tecnología, ya que esta dependerá del uso que el individuo realice con ella.

4.3 ALTERNATIVAS PARA OFRECER ANONIMATO Y PRIVACIDAD

Además de las soluciones tratadas (FreeNet, I2P y Tor) en los capítulos anteriores, existen más tipos de herramientas y redes las cuales ofrecen anonimato y privacidad al usuario en el uso de Internet. A continuación, se realiza una pequeña descripción de algunas de ellas:

- **GNUnet:** Es un framework con el que se pueden crear redes del tipo "peer-to-peer" seguras, y totalmente descentralizadas.
- **Latern:** Es una solución peer-to-peer, la cual permite evadir las medidas de censura que intentan bloquear ciertos sitios de Internet. Este detecta si un sitio se encuentra censurado, por lo tanto, no es accesible, y permite el acceso mediante una red distribuida de usuarios que utilizan esta solución y que si tienen acceso al sitio.

- **Hyperboria**: Es una red de prueba construida con nodos que utilizan el protocolo de enrutamiento cjdns.
- **Hornet**: High-speed Onion Routing at the Network Layer, es una red con enrutamiento de tipo cebolla, al igual que Tor. La diferencia es que consiguen obtener mayor velocidad que en la red Tor.

4.4 EVOLUCIÓN DE LAS REDES

Como hemos visto anteriormente, hay multitud de opciones para ofrecer privacidad y anonimato a los usuarios. Por otro lado, las grandes empresas que tratan y comercializan datos de los usuarios para obtener beneficios (mayoritariamente ofreciendo publicidad), es por ello por lo que un grupo de usuarios utilice este tipo de redes por está cuestión. Además, en ciertos países existe la censura de ciertos contenidos de Internet, que, utilizando por ejemplo la red Tor, podemos acceder a estos contenidos.

5 CAPITULO 5: CONCLUSIONES

5.1 RELACIÓN DE OBJETIVOS

A continuación, se enumeran los objetivos del proyecto para relacionar como estos han sido realizados:

Objetivo 1	Introducción a la Deep Web.	✓
	Se ha realizado una introducción teórica de la Deep Web, poniéndola en el contexto actual.	
Objetivo 2	Comprender porque surgen este tipo de redes (TOR, I2P, Freenet).	✓
	Se ha realizado un recorrido por las redes más importantes, así como el porque de la aparición de estás redes, ya que estás ofrecen un "servicio" a los usuarios que no pueden disponer con la Internet convencional.	
Objetivo 3	Comprender los distintos tipos de redes y que ofrece cada una de ellas (TOR, I2P, Freenet).	✓
	Se ha realizado un estudio de las redes más importantes comparándolas entre ellas, de esta forma se puede conocer la información que puede ofrecer cada una de ellas.	
Objetivo 4	Comprensión de la infraestructura que da soporte a esta red (TOR).	✓
	Se ha realiza un estudio en profundidad de la infraestructura de la red Tor, para comprender como funciona y que componentes dan soporte a la misma.	

Objetivo 5	Riesgos y amenazas del uso de esta red (TOR).	✓
	Se ha realizado un estudio de los riesgos del uso de esta red, así como las vulnerabilidades que se han detectado recientemente.	
Objetivo 6	Compresión del software necesario para acceder a la red (TOR).	✓
	Se ha realizado un caso práctico de acceso a la red Tor, utilizando el software necesario para el acceso (Tor Browser).	
Objetivo 7	Caso práctico (TOR): • Acceso a la red. • Tipos de servicios e información que se puede encontrar en dicha red.	✓
	Se han implementado los casos prácticos propuestos, además se ha ampliado este caso práctico instalando y configurando dos servicios ocultos (HHTP y SSH).	
Objetivo 8	Evolución de las redes, nuevas redes	✓
	Se realiza una aproximación de opciones alternativas a las redes tratadas (Tor, I2P y FreeNet), y se considera la evolución de estas redes.	

5.2 AMPLIACIONES DEL TRABAJO

El presente proyecto ha tratado teóricamente las redes más importantes (FreeNet, I2P y Tor), implementando casos prácticos en esta última red. Como ampliación del proyecto se puede realizar un estudio más profundo sobre el resto de redes, así como implementaciones prácticas.

6 BIBLIOGRAFÍA

6.1 LIBROS

- **Daniel Echeverri Montoya** (2016), Deep Web: TOR, FreeNet & I2P Privacidad y Anonimato, Edición Zeroxword Computing S.L 2016.

6.2 CONTENIDO WEB

- **FreeNet:** https://freenetproject.org/

- **I2P:** https://geti2p.net/
- **Tor:** https://www.torproject.org/
- **Instituto Nacional de Ciberseguridad (INCIBE):** https://www.incibe.es/
- **Cert de Seguridad e Industria (certsi):** https://www.certsi.es/
- **Wikipedia:** https://wikipedia.org
- **GNUNET:** https://gnunet.org/
- **Latern:** https://getlantern.org/
- **Hyperboria:** https://hyperboria.net/
- **Un informático en el lado del mal:** http://www.elladodelmal.com/

6.3 CONTENIDO AUDIOVISUAL

- **Taller: Cambiando el CuenTOR (Francisco Rodríguez - INCIBE & Manu Guerra - FCSE) CyberCamp 2016:** https://www.youtube.com/watch?v=PYu9Zkwmhw0
- **¿Qué es la Deep Web? Ciberdebate Palabra de hacker:** https://www.youtube.com/watch?v=6lr5khBoSik