Un paseo por la Deep Web

Autor: Victor Manuel Comendador Sánchez

Tutor: Jorge Chimea López

Profesor: Victor García Font

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Protocolos y aplicaciones de seguridad

Fecha de entrega: 31 de diciembre 2019

Créditos/Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Un paseo por la Deep Web*
Nombre del autor:	*Victor Manuel Comendador Sánchez*
Nombre del colaborador/a docente:	*Jorge Chimea López*
Nombre del PRA:	*Victor García Font*
Fecha de entrega (mm/aaaa):	*12/2019*
Titulación o programa:	*Máster Inter-Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)*
Área del Trabajo Final:	*Protocolos y aplicaciones de seguridad*
Idioma del trabajo:	*Español*
Palabras clave	*Deep Web, Internet Profunda, Dark Web*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo*

Nuestro Trabajo, en relación con la Seguridad Informática ha sido estudiar e investigar sobre las fundamentales, subredes que operan en el mundo del anonimato en la Red y que pueden posibilitar evitar la censura.

Su contexto de aplicación, ha comprendido un estudio del funcionamiento de las referidas redes (tres básicamente) más utilizadas y conocidas a la fecha en que elaboramos de este trabajo.

Nos hemos centrado en la utilización de estas subredes en su parte de uso negativo, como en aquellos aspectos que pueden ser utilizables desde ópticas positivas, usando un sistema metodológico partiendo de un análisis de la de la Deep Web y subredes como Tor, I2P, FreeNet.

En la parte teórica, exponemos para cada una de las redes, la tecnología utilizada, su funcionamiento y la compatibilidad con diferentes sistemas operativos.

En la parte practica, desarrollamos las redes mencionadas:
Elección de sistema operativo, instalación de software utilizado para operar en cada una de las mismas, realización de configuraciones de cada red y como parte final se ha practicado una navegación breve por ellas haciendo un especial énfasis en la Red Tor por ser la más popularizada.

Se ha implementado un nodo/relay de la Red Tor, utilizando un miniordenador, con sistema operativo Linux, al cual hemos instalado los programas específicos para su funcionamiento y parametrización.

En cuanto a resultados y conclusiones hemos conseguido interactuar dentro las Redes de anonimato, con las debidas cautelas para nuestra seguridad, así como el sistema de funcionamiento en vertiente positiva y negativa, riesgos y ventajas.

Abstract (in English, 250 words or less):

Our work, in relation to Information Security, has been to study and investigate the fundamentals, subnets that operate in the world of anonymity in the Network and that can make it possible to avoid censorship.

Its context of application has included a study of the operation of the aforementioned networks (three basically) most used and known as of the date on which we elaborate this work.

We have focused on the use of these subnets in their part of negative use, as in those aspects that can be usable from positive optics, using a methodological system based on an analysis of the Deep Web and subnets such as Tor, I2P, FreeNet.

In the theoretical part, we expose for each of the networks, the technology used, its operation and compatibility with different operating systems.

In the practical part, we develop the mentioned networks:
Choice of operating system, installation of software used to operate in each of them, making configurations of each network and as a final part, a brief navigation through them has been made with a special emphasis on the Tor Network for being the most popular.

A node / relay of the Tor Network has been implemented, using a minicomputer, with Linux operating system, to which we have installed the specific programs for its operation and parameterization.

Regarding results and conclusions, we have managed to interact within the Anonymity Networks, with the proper precautions for our security, as well as the operating system in positive and negative aspects, risks and advantages.

Dedicatoria/Cita

A mi familia y a mi mujer, con una mención especial a mi padre, ya que sin sus apoyos no hubiera conseguido llegar a donde estoy hoy.

Agradecimientos

Mi agradecimiento a la UOC, cuya altura y calidad docente me han proporcionado unas habilidades y conocimientos técnicos que espero que, en un futuro, me proporcionen éxitos profesionales.

Palabras clave

Deep Web, Dark Net, Internet profunda, Freenet, I2p, Red Tor, Tor Browser, Nodo Tor, Servicios Onion, VPN.

Notaciones y Convenciones

Letra en negrita y cursiva: Expresa los comandos a ejecutar en el sistema operativo de implementación del nodo.

Índice

Figuras y tablas

Índice de figuras

Índice de tablas

1.Introducción.

Internet (La Red de Redes) nos ha proporcionado la opción de estar conectados a nivel global con cualquier parte del mundo. Si buscamos algún estudio sobre el impacto de esta tecnología sobre todas las sociedades podemos leer las palabras de Manuel Castells Profesor de la UOC [1], el cual, en su obra y trabajos, nos muestra de forma clara las transformaciones que la sociedad ha experimentado en todos sus ámbitos como consecuencia del impacto tecnológico – social que la Red le ha aportado.

Hoy el uso de Internet se ha difundido de tal forma que se encuentra en todos los ordenes de la actividad social, gestión de documentación, en general, relación del Ciudadano con las Administraciones Publicas e interactuación con ella, tramites bancarios sin necesidad de acudir a las sucursales u oficinas, estamos informados, prácticamente en tiempo real, de cualquier noticia o suceso ocurrido en cualquier parte del mundo, tenemos a nuestro alcance con un solo clip conocimientos científicos antes reservados a élites muy concretas etc. y como podemos observar, todo esto, a redundado en unos beneficios y avances sociales inimaginables hace, relativamente, poco tiempo.
Con todo lo expuesto, podríamos decir que todo son ventajas, pero esto no seria real, todo tiene su parte negativa y en este caso no podía ser distinto. La parte negativa que los avances indiscutibles de la Red, como antes decimos, nos ha proporcionado, también propician que nuestros datos están expuestos y se encuentren en cantidad de servidores y bases de datos albergados en la conocida como “la Nube”, ¿Quién posee esta información? Los Gobiernos, las grandes empresas de internet ¿Qué saben de nosotros? Todo, incluso desde el lugar en el que nos encontramos navegando.

Vemos que nuestra privacidad y datos personales cada vez están más expuestos y es más vulnerable nuestra intimidad, por lo que se han buscado alternativas tecnológicas para navegar por la Internet de forma anónima, incluso para poder eludir la censura y reglas severas que imponen determinados gobiernos sobre sus ciudadanos. De aquí han salido varias redes con tecnologías especificas para evitar que todos los movimientos que realizamos en Internet, búsquedas, Web visitadas, ficheros descargados, compras etc., sean rastreados con diferentes fines como podrían ser envió de publicidad, estadísticos, el lugar desde donde nos estamos conectando, etc. a fin de conseguir que al usar estas tecnologías nos proporcionen una capa de anonimato o invisibilidad en nuestra incursión en el mundo digital. La otra opción no menos importante que ofrecen, en este caso positiva, es la posibilidad de evitar que se oculte lo que sucede en regímenes dictatoriales del mundo, movimientos terroristas o la posibilidad de publicar documentos y noticias que han sido ocultadas a la opinión publica por estar clasificadas como secretos de estado no muy limpios. Todos tenemos en la memoria casos como WikiLeaks, Julián Assange.

Vamos a estudiar estas redes, e intentar comprender su funcionamiento, intentaremos arrojar un poco más de luz sobre todos los conceptos que se manejan, también realizaremos incursiones practicas de manera que nos conectemos de la forma más segura posible. Cabe destacar que podriremos explorar entornos legales y no tan legales, pero este estudio solo se centrara en la técnica y sitios legales.

1.1.Prefacio.

Cuando se escucha por primera vez las palabras Deep Web y Red Tor, los usuarios de sistemas informáticos con ciertas inquietudes profesionales, reaccionan, queriendo saber el significado de esas palabras, y que se esconde detrás de ella, ¿es una tecnología?, ¿como se implementa? Al realizar una búsqueda es muy fácil encontrar libros que nos aportan información sobre estos términos, como por ejemplo La Red Oscura [2]. Solo con que se lean sus dos primeros capítulos, se observara que, bajo la bandera del anonimato, se esconde un autentico ecosistema de ciberdelitos.
En este momento los interesados, se pueden encontrar en una incertidumbre, mezcla de curiosidad e incluso de pánico, e irán buscando y descubriendo los diferentes contenidos, debiendo eso si, aplicar mucha cautela en esta navegación y adentrándose paso a paso en estas redes. Y como no. ir realizando acercamientos minuciosos a este mundo del anonimato,

Procederemos a pasear por la Deep Web, e intentar comprender y profundizar más todavía en el conocimiento de la materia tanto teórica como práctica. Se puede ver como una gran oportunidad que no tendríamos que desaprovechar. Por eso realizaremos una investigación por las redes anónimas más populares y usos, debiendo destacar muy significativamente. como ya apuntábamos en la introducción, que las redes anónimas, en un plano de utilización positiva, están sirviendo también para escapar de la censura que algunos países ejercen sobre sus ciudadanos y descubrimiento de comunicaciones entre grupos delincuenciales y terroristas, entendiendo que este submundo de la Red, debidamente manejado desde las tecnologías de seguridad informática puede ser, en ocasiones controlado y aportar información que de otra forma no se hubiese podido obtener ya que, obvio es decir, que en Red en abierto, jamás se hubiese incluido información y noticias de esa naturaleza.

Esperemos que la lectura de este trabajo sea tan grata, como su elaboración y ejecución esta siendo para nosotros, que al mismo tiempo que exponemos, adquirimos aprendizaje al experimentar para la realización del mismo.

1.2.Descripción/Definición.

Al realizar una búsqueda por Deep Web aparece en muchísimas paginas la imagen de un Iceberg mostrando de forma esquemática donde esta la Surface Web, la Deep Web y la Dark Web, indicando los porcentajes de sus dimensiones, algunas incluso sus diferentes niveles, etc., hoy podemos decir que estos gráficos son FALSOS.

Queremos empezar aclarando estos conceptos ya que expertos en la materia han descubierto que nadie ha navegado por las Marianas Web [3] y no existen distintos niveles, y tampoco podemos comprobar de forma concreta la cantidad de elemento y servicios que componen estas redes. por ello queremos profundizar e investigar para ver el alcance real a día de hoy de lo que son y significan las subredes que operan bajo la cobertura de la Red de Redes.

Hemos obtenido información de fuentes más actualizadas, las cuales nos indican una nueva estructura de estas tres redes, y exponen la imposibilidad de podre obtener un porcentaje de la red no indexada (Deep Web), al igual que sobre la Dark Web. En el grafico que exponemos a continuación podemos ver la división y posibles contenidos que nos ofrece cada una de las redes.

Web Superficial

Deep Web

Dark Web

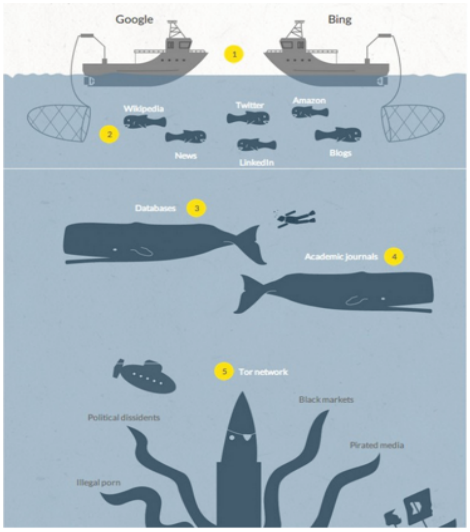


Figura 1: Grafico actual de las estructuras de las Redes [4]

Web Superficial: Es la que todos conocemos y usamos a diario para enviar correo, leer noticias, interactuar con ñas administraciones publicas, etc. Se podría resumir como todo el contenido que pueden indexar los grandes motores de búsqueda cono Google, Bing, etc.

Deep Web: También conocida como la Web profunda, que, a diferencia de la Web Superficial, todos sus contenidos no esta indexado, como por ejemplo bases de datos, correos electrónicos, blogs personales no quieren que se indexen y no sean de domino publico. Se puede decir que lo no indexado no tiene por que ser ilegal, sino simplemente es anónimo.

Dark Net: Para evitar confusiones con el termino anterior, que muchas veces se mezclan como si fueran el mismo concepto, la Dark Net es una subred de la Deep Web, es decir esta dentro de

esta ultima, la cual es denomina como la Red oscura. Esta ultima definición le viene dada porque algunos de sus contenidos se podrían decir que rozan la ilegalidad o son ilegales.
Un tema relevante que nos preguntamos, es si navegar anónimamente es delictivo, en principio y por ese solo hecho, podemos decir que no pues ya estas mismas conductas se encuentran en la red normal y no por ello son delictivas. Otra cosa es que, esa navegación, pueda ser utilizada para la comisión de hechos delictivos.

1.2.1. Aportaciones.

Pretendemos que se clarifiquen los conceptos de las redes anónimas y dar una visión teórico-practica de las posibilidades que existen, a fin de que el propio lector obtenga sus propias conclusiones y sea el que fije los limites de lo legal e ilegal, pudiendo optar por si mismo donde quiere llegar.

1.3. Objetivos generales.

El principal objetivo que nos planteamos con este Trabajo, es dar a conocer el significado completo de la denominación Deep Web, viendo las diferentes subdivisiones que componen La Red de Redes. Hablaremos de las tres redes más populares para navegar de forma anónima o intercambiar información lícitamente, o su utilización en determinadas acciones que rozan la ilegalidad o son ilegales.

Concretando más y por su especial interés, dada su popularidad, nos centraremos en una de las redes más popular dentro de la Deep Wep, la cual es conocida como la red Tor. Se creo con fines de navegación anónima, pero determinadas personas (cibercriminales) vieron la posibilidad de realizar algunas ilegalidades amparados de ese anonimato. Continuaremos con una explicación de como acceder, su funcionamiento y porque de su anonimato.

El objetivo practico de este trabajo, es la implementación uno de los tipos de nodo que ofrece la Red Tor, para ello utilizaremos un dispositivo que nos permitirá ver el trafico que puede pasar por el nodo, así como, ver la opción de usar aplicaciones especificas y de terceros. En este punto expondremos todos los pasos para el despliegue del nodo, así como su funcionamiento y configuración.

Como objetivo final, intentaremos ver las posibilidades de conectarnos a la red TOR de forma segura para preservar nuestro anonimato lo más posible y protegernos ante las posibles amenazas de la red, Para ello intentaremos usar un nodo como proxy parar enrutar todo el trafico de salida siempre por la red TOR. Y no menos importante usando una red virtual privada (VPN) para garantizar aun más nuestro anonimato.

1.3.1. Objetivos principales.

Dar a conocer un análisis teórico de cómo esta estructurada la Deep Web, explicar las tres redes más usadas a la fecha de este estudio, indicaremos sus funcionamientos, mencionaremos los posibles fallos si los tuvieran los cuales puedan rebelar nuera identidad y realizaremos una conexión practica a cada una de las tres redes

En la Red que se focalizara con más detenimiento serán la red Tor, ya que es una de las más populares, extendida y conocida dentro de la Deep Web. Veremos que son los Hidden Services y como accede a estos servicios y las direcciones onion.

Como parte practica que, diferenciada de lo expuesto en los párrafos anteriores, se llevara acabo la implementación y configuración de uno de los tipos de nodo de la red Tor y comprender mejor su funcionamiento para garantizar el anonimato de la navegación por el entramado que compone esta Red.

1.3.2. Objetivos secundarios.

Como objetivos secundarios obtendremos en concreto el conocimiento de cómo instalar cada una de las tres redes, las cuales son I2P, FreeNet y Tor.

Una vez instaladas veremos sus funcionamientos, es decir, direcciones que utilizan (onion, i2p, nombre de ficheros), si podemos acceder a la Web superficial desde ellas, etc.
Concretamente aprenderemos a navegar por cada una de estas redes, ya que una vez este instaladas y funcionando realizaremos una pequeña inmersión en algunos contenidos no lesivos ni ilegales, como puede ser algo de información de cómo crear sitos ocultos dentro de ellas, envió de correos desde estas redes, utilización de buscadores en la que lo permita, como Duckduckgo o paginas de índices de contenidos.

Detallar como en todas las pruebas y conexiones a estas redes se ha utilizado un servicio de VPN para garantizar mejor el anonimato y ubicación física de donde se realiza el estudio.

1.4.Metodología y proceso de trabajo.

Procederemos a detallar las distintas fases que vamos a ir implementando para lograr llevar a cabo los objetivos planteados en los apartados anteriores.

Podemos decir que este apartado se encentra dentro de la primera fase, la cual recogerá la explicación de objetivo o problema a resolver, incluyendo esta metodología que describe los hitos alcanzar, así como, la ejecución de los mismos expuestos en una escala temporal de ejecución.

En esta segunda fase procederemos a realizar búsquedas y recopilación de información de tema a tratar, utilizando Internet, libros, artículos, etc. de fuentes acreditadas en la materia como por ejemplo INCIBE. Seguidamente llevaremos a cabo un análisis exhaustivo de toda la información obtenida para extraer de la misma todo lo necesario para desarrollar y cumplimentar los objetivos de nuestro trabajo.

La tercera fase nos llevara a realizar e implementar todas las partes teóricas y practicas que incluiremos dentro de este documento.

Para finalizar en la cuarta fase expondremos todas las posibles conclusiones derivadas de todas las pruebas practicas realizadas al estudiar los diferentes resultados obtenidos de cada una de ellas.

Estimamos que, con estas cuatro fases en nuestro proceso de trabajo, deberíamos de obtener un producto final acorde a las expectativas planteadas en el documento.

1.5.Planificación.

Consideraremos para realizar la planificación que podríamos dedicar 2 horas diarias a la ejecución del trabajo, por lo que desglosaremos el numero de horas de ejecución por ítem, y lo mostraremos en la tabla.

Mediante las siglas **EP**, hemos marcado las diferentes entregas parciales que se realizaran a lo largo del desarrollo del trabajo.

A continuación, se expondrá la tabla con los diferentes hitos a ejecutar,

0	TFM Un Paseo por la Deep Web (Protocolos y aplicaciones de seguridad)		Días	Horas	18/9/19	30/12/19
1	Plan de Trabajo	PEC 1				
1.1	Introducción, Prefacio, Agradecimientos, Resumen	PEC 1	2	4		
1,2	La explicación detallada del problema a resolver.	PEC 1	1	2		
1,3	La enumeración de los objetivos que se quieren alcanzar con la realización del TFM.	PEC 1	2	4		
1,4	La descripción de la metodología que se seguirá durante el desarrollo del TFM.	PEC 1	2	4		
1,5	El listado de las tareas a realizar para alcanzar los objetivos descritos.	PEC 1	2	4		
1,6	1.6 La planificación temporal detallada de estas tareas y sus dependencias. **EP**	PEC 1	2	4	27/9/19	28/9/19
1,7	1.7 Una pequeña revisión del estado del arte.	PEC 1	3	6		
*	**Entrega PEC1**		**14**	**28**		**1/10/19**
2	PEC2: Entrega 2 Pruebas				2/10/19	29/10/19
2.1	Búsqueda de información	PEC 2	2	4		
2.2	Preparación materiales y equipos de pruebas	PEC 2	1	2		
2.3	¿Que es la Deep Web?	PEC 2	2	4		
2.4	I2P	PEC 2	2	4		
2.5	Freenet	PEC 2	3	6		
2.6	Tor					
2.6.1	¿Que es la Tor Network?	PEC 2	3	6		
2.6.2	Túneles virtuales	PEC 2	3	6		
2.6.3	Tipos de Relays **EP**	PEC 2	3	6	18/10/19	20/9/19
2.6.4	Análisis de Red Tor	PEC 2	3	6		
2.6.5	Servicios onion	PEC 2	3	6		
2.6.6	Servicio oculto **EP**	PEC 2	3	6		
*	**Entrega PEC2**		**28**	**56**		**29/10/19**

3	PEC3: Entrega 3					
3.1	Implantación de pruebas y recogida de información					
3.1.1	Test I2P	PEC 3	4	8		
3.1.2	Test Freenet	PEC 3	4	8		
3.1.3	Test Tor	PEC 3	8	16		
3.1.4	Test Navegación Deep Web **EP**	PEC 3	3	6	15/11/19	17/10/19
3.1.5	Implementación de un nodo Tor	PEC 3	6	12		
3.1.6	Test nodo Tor **EP**	PEC 3	3	6		
*	**Entrega PEC3**		**28**	**56**		**26/11/19**
4	PEC4 Entrega 4 - Memoria final					
4.1	Penúltimo Capitulo que incluye la valoración económica	PEC 4	3	6		
4.2	Añadir ilustraciones	PEC 4	3	6		
4.3	Conclusiones **EP**	PEC 4	4	8	3/12/19	6/12/19
4.4	Glosario	PEC 4	2	4		
4.5	Bibliografía	PEC 4	-			
4.6	Anexos	PEC 4	-			
4.7	Elaboración Presentación TFM	PEC 4	6	12		
4.8	Entrega Final 100% del Proyecto y la Presentación del mismo. **EP**	PEC 4	16	32	17/12/19	22/12/19
*	**Entrega PEC4**		**34**	**68**		**30/12/19**

Tabla 1: Planificación con fechas de Entrega final y parcial

Seguidamente podremos ver el diagrama de Gantt:

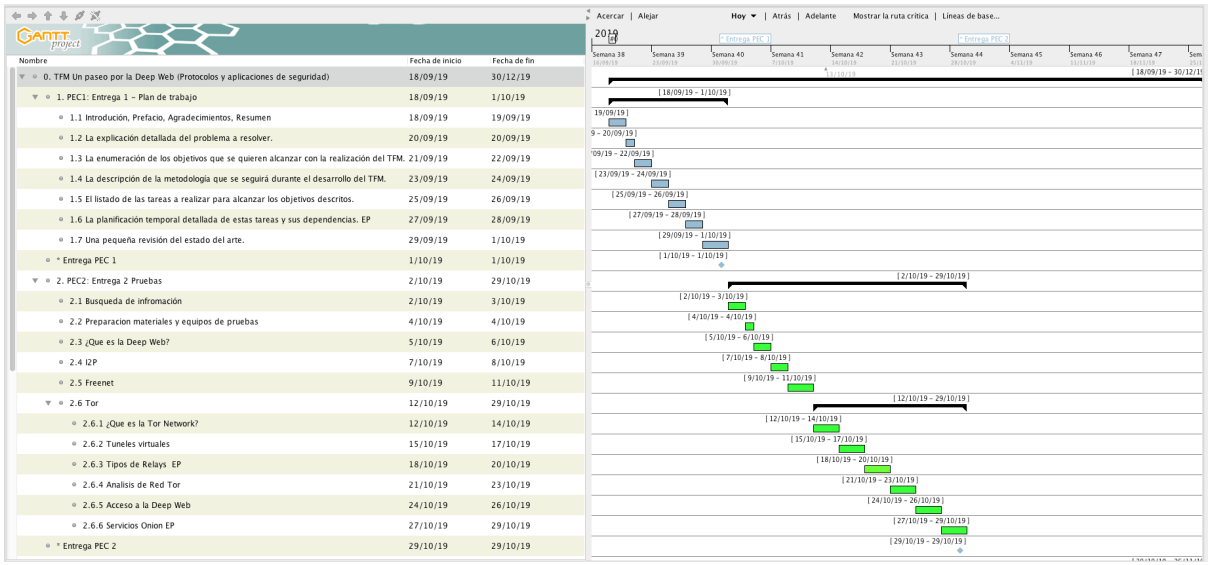


Figura 2: Diagrama de Gantt PEC 1 y 2.

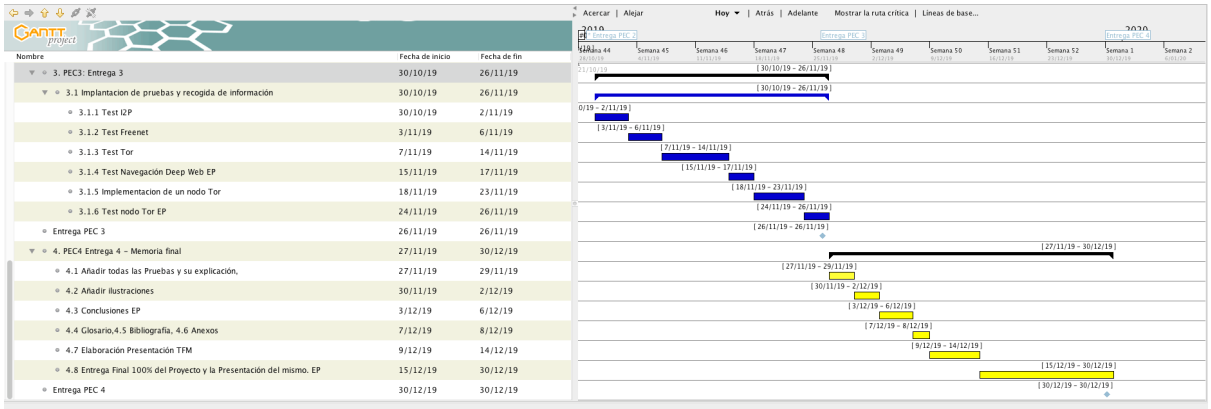


Figura 3: Diagrama de Gantt PEC 3 y 4

1.6. Estructura del resto del documento.

En los próximos apartados del documento estructuraremos nuestro objetivo de la siguiente manera:

En el capitulo 2 expondremos el estado del arte, así como un análisis de posibles riesgos

El capitulo 3 nos introducirá en el conocimiento amplio de las redes de anonimato más conocidas hoy en día, tanto teórica como prácticamente.

Por último, en el capitulo 4 observaremos como hemos realizado el despliegue de uno de los nodos de la red Tor sobre un mini ordenador.

2. Estado del arte.

En apartados anteriores hemos denominado a internet como La Red de Redes, ya que esta interconectando ordenadores a nivel mundial. Solo tenemos que pensar que cualquier casa u oficina se encuentra conectado a esta Red, por lo que podemos deducir que es muy complicado saber el numero de ordenadores unidos en todo el mundo, además según avanzamos tecnológicamente se van incorporando más y más elementos a esta Red, teléfonos inteligentes, consolas de juegos, cámaras de CCTV, elementos de control demótico, etc. De lo anteriormente expuesto se ha creado un concepto denominado, El internet de las cosas [5], por lo que poder dar una cifra de tamaño o dispositivos conectados es muy difícil. Se han creado buscadores como Google para elementos conectados como es Shodan [6] que puede realizar búsquedas de dispositivos por nombre o por IP.

En el párrafo anterior hablábamos de dispositivos Hardware, pero y si pensamos en usuarios o paginas Web, los números son espectaculares, miremos varios ejemplos que podemos obtener en tiempo real [7], usuarios 4.349.000.999, páginas Web 1.717.686.128, estas cifras son de un minuto concreto, porque aumenta a gran velocidad. Todos los datos que visualizamos y todos los estudios que se pueden encontrar, se suelen basar en los datos de los grandes motores de búsqueda como Google, Yahoo, Bing, DuckDuckGo, etc. que indexan los contenidos de las Web que se publican. Todo lo que hemos narrado hasta este punto se conoce como la Surface Web.

Ahora, dentro de todos estos ordenadores y fuera del alcance de estos motores de búsqueda, se encuentra un internet oculto o no accesible de una forma fácil y sencilla. Nos encontraremos con mucho contenido no indexado, sistemas que solo se acceden por consultas especificas, sitios no enlazados, etc., pues toda esta parte de Internet se la denominada The Deep Web, o la parte accesible pero no indexada.

Pero dentro de esta Deep Web nos encontramos una zona más privada que no se accesibles de forma sencilla, ya que se necesitan softwares especiales para acceder a estas Subredes denominadas Dark Web. Fueron creadas inicialmente para proporcionar anonimato y poder saltar algún tipo de censura de algunos países. Pero estas tecnologías se empezaron a utilizar por determinadas personas para realizar actos poco legales, amparándose en el anonimato que ofrecen.

2.1.¿Qué es la Deep Web?.

En apartados anteriores, hemos definido la Deep Web o Web profunda [8] como el contenido que se encuentra en Internet, pero que por diferentes motivos no esta indexado por los grandes buscadores como Google, Bing, DuckDuckGo, etc.

En la Deep Web abarca la información que no encontramos al solicitársela a los buscadores de internet y que sus arañas no han conseguido indexar, como pueden ser bases de datos, sitios Web que no son posible indexar por diferentes motivo o técnicas de ocultación para que los motores no las detecte, sitios FTP, etc. Decir que no se tiene una información exacta de la dimensión del Internet profundo (en búsquedas en la Surface se puede encontrar mucha información que arroja estadísticas de su posible dimensionamiento, pero a día de hoy no se tiene una forma fiable de medirlo), ya que entre muchas Web no mantenidas o enlaces rotos, servidores de acceso privado que pueden proporcionar diferente información pero que su acceso es restringido a usuarios específicos.

Las paginas en la Deep Web para que no sean detectadas por los bots o más comúnmente spiders o crawlers (arañas o rastreadores). Estos últimos son los que acceden a los sitios Web y recopilan todas las referencias de su contenido buscando en el archivo robots.txt, por lo que limitando y controlando este fichero las paginas Web no se indexan y no son localizables.

Lo anteriormente expuesto es la definición de la Deep Web, pero esta muy extendido usar Dark Web como palabras sinónimas, pero esto es un error. La Dark Net es un aparte del la Deep Web y esta ultima una parte de Internet, Si queremos acceder a esta parte de la red se necesita disponer de unos conocimientos algo más precisos que para navegar por la Surface Web que es la que todos los usuarios conocemos y usamos a diario. En la siguiente imagen vemos un ejemplo de la estructura de estas redes:

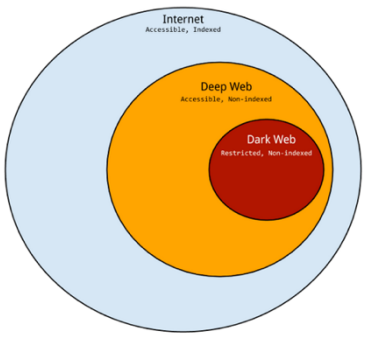


Figura 4: Las subredes de Internet [9]

La Dark Net ofrece una navegación con características especules, las cuales ofrecen a sus usuarios realizar una navegación anónima, poder saltarse la censura que determinados gobiernos ejercen sobre su población (periodismo). Bajo estas circunstancias prolifera las actividades ilegales aprovechando las ventajas del anonimato. Sobre las opciones poco licitas nos podemos encontrar mercados de estupefacientes, servidos de hacker, pornografía, paginas de terrorismo, así como pederastia. En los siguientes apartados expondremos las diferentes redes existentes para la navegación anónima.

2.2.I2P.

I2P es la abreviatura en ingles de Invisible Internet Project [10] (Proyecto de internet invisible) la cual es una red que facilita el anonimato sobre la Red de Redes, es distribuida y de baja latencia. A diferencia de las otras redes usa cuatro capas de cifrado de extremo a extremo para el envió de información entre clientes. Se necesita ser parte de esta red para comunicar dentro de ella, ya que al ser descentralizada se tiene que hablar entre equipos iguales, Peer to Peer, al usar este protocolo podemos decir que esta red no esta pensada para una navegación anónima sino para una comunicación anónima.

I2P se compone de router con n numero de rutas y utiliza dos túneles de entrada y dos de salida entre el cliente y el servidor [12]. Cada túnel está compuesto por una secuencia de nodos padres, los cuales solo transportan la información en un único sentido (unidireccional). I2P cambio sus protocolos de transporte de TCP a UDP Secure Semireliable UDP (UPD seguro semi-fiable) SSU [12]. A nivel de cifrado utiliza AES256/CBC, la clave de sesión se realiza a través de un intercambio Diffie-Hellman de 2048bit. I2P poses su propia base de dato de red por la cual distribuye las rutas y contactos de forma que garantiza la seguridad.

En los grafico siguiente veremos el funcionamiento de los túneles:

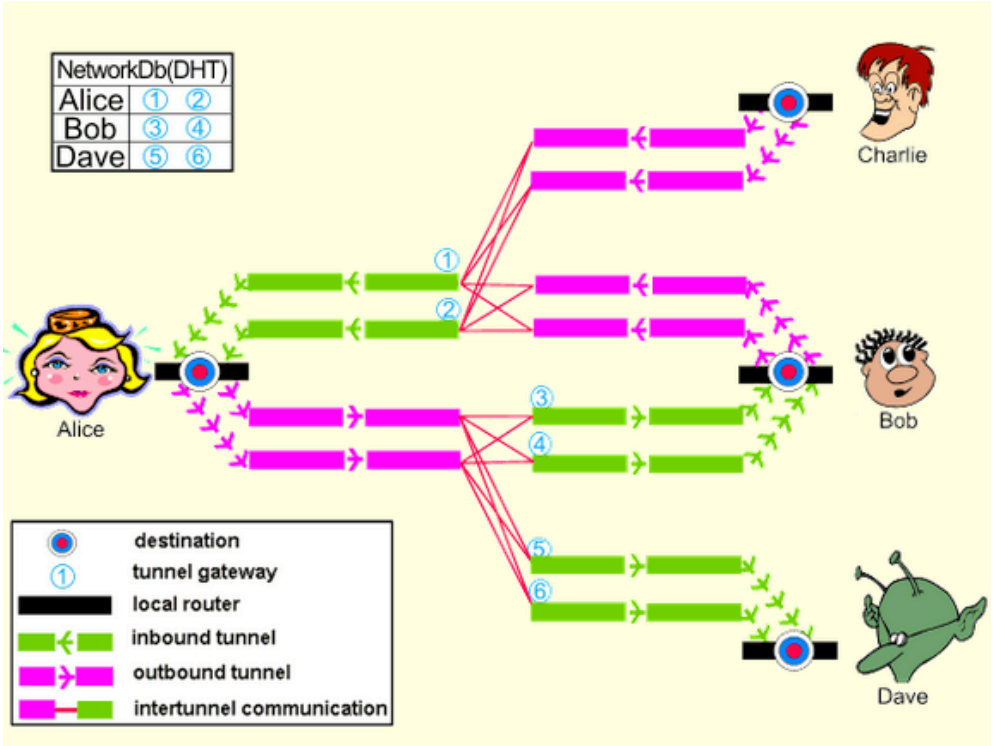


Figura 5: Comunicaciones red I2P (túneles) [10]

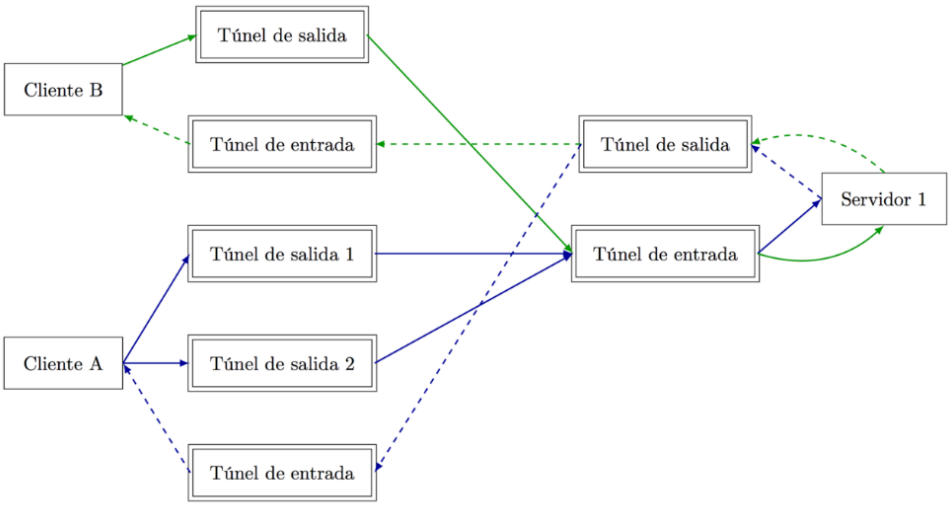


Figura 6: Comunicaciones dos clientes un servidor I2P (túneles)

En la imagen superior podemos observar que en esta red a diferencia de otra no se tiene que establecer un circuito o camino por cada comunicación nueva, sino que el túnel de entrada o salida ya creado es valido para “n” clientes. Una característica importante para garantizar la privacidad por si alguien esta capturando el trafico, es que en el funcionamiento de la red todos los túneles cambian cada 10 minutos y con un máximo de siete saltos o pasos por router/nodo.

I2P posee menos usuarios que Tor, pero su auge subió al producirse algunos fallos en Tor que permitieron identificar algunos usuarios, Habremos de tener en cuenta que esta Red obliga a todos los usuarios a servir de router de la misma, lo cual puede ser una ventaja a la hora de posibles ataques de DoS. La seguridad se podría considerar más alta y con un nivel mayor de privacidad, ya que su expansión y tamaño son más reducidos que, por ejemplo, Tor.

I2P también es una red out-proxy, que quiere decir esto, que mediante una configuración especifica se puede tramitar trafico a la Surface Web o la internet que todos conocemos. Este tipo de nodo tiene que ser realizado por un usuario de forma especifica adaptando un router de esa red para que tramite trafico de una red a otra.

En el capitulo tres apartado numero uno, expondremos la instalación de software necesario para acceder a I2P paso a paso, así como su configuración y mostraremos una breve navegación por sus dominios (.i2p) con contenido licito, hemos evitado, como medida precautoria, entrar en ninguna Dark Net de esta red, dejamos a decisión del lector de este trabajo, si lo considera oportuno, adentrarse más a fondo.

2.3.FreeNet.

FreeNet [13] es una red que nace hace unos 20 años con la intención de ofrecer y garantizar privacidad, así como poder eludir la censura periodística o general de algunos gobiernos.

Se ha desarrollado en java open source [14], basándose en un algoritmo que se ejecuta entre diferentes nodos, los cuales se encuentran conectados y establecen un sistema de almacenamiento sin una administración centralizada y con una indexación propia, además posen una securización por claves, con esto se asegura que los ordenadores que almacenen la información no pueden acceder a ella, eventualmente, en nuestro ordenador pudiéramos tener alojada algún tipo de información o recurso ilegal sin saberlo.

Por lo que venimos exponiendo, estamos ante una Red similar a las BitTorrent de la Surface Web, es decir un peer to peer o P2P y es considerada inproxy [15] (podemos compararlo con una VPN), ya que esta red no tiene desarrollado ningún sistema para comunicar con la Surface.
Se puede realizar entre conocidos en la red de FreeNet unos espacios o parte privada que solo serán visibles entre sus miembros, por lo que podrían crear una Dark Net con contenidos ilegales, o realizar una perfectamente lega, esto quedaría bajo la responsabilidad de los miembros intervinientes. Una parte positiva de esta posibilidad que comentamos es la de que, ante casos de censura de cualquier tipo, contraria al derecho internacional e incluso a los derechos humanos, también se podrían crear redes entre periodistas de distintos países para dar a conocer lo que sucede en determinada parte del mundo.
El funcionamiento de FreeNet es el siguiente:
Cuando se produce la comunicación entre dos nodos para compartir una pagina o archivo, este se copia en el nodo receptor (esta red utiliza un espacio de nuestro disco duro para almacenar todos los elementos que solicitamos y se usa para compartir con otros nodos de la red) ya no es necesario que el primer nodo que envía o tiene ese primer fichero, siga operativo para que el resto de la red lo tenga disponible, por lo que se ira distribuyendo entre los nodos que consulten ese contenido (en caso de crear un DarK Net en nuestro Pc, en el momento que alguien la consulta esta se copia en su equipo y así sucesivamente por lo que siempre el contenido será accesible). Al subir un documento, se le asignara una etiqueta especifica que más otros campos del usuario, los cuales se usarán para crea la clave de cifrado, además de otras dos. Con todo esto se genera una etiqueta especial, la cual será requerida por los usuarios que quieren visualizar el contenido del archivo, junto con las tablas de enrutamiento en los históriales de cada nodo y en el espacio compartido de cada uno de ellos.
Al recibir el contenido en un nodo, se descifrará con la clave correspondiente, seguidamente vamos a exponer un grafico que nos muestra como se realiza el intercambio de mensajes de comunicación entre los nodos de esta red:

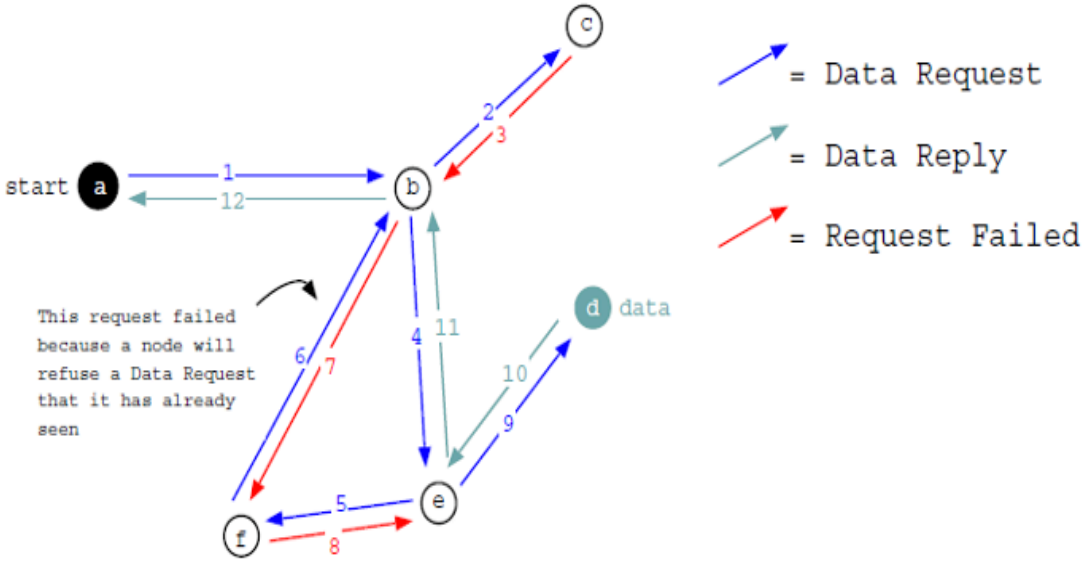


Figura 7: Flujo de los mensajes de comunicación entre nodos. [14]

A tenor de todo lo expuesto, podemos considerar que FreeNet es una red descentralizada, por lo que cuando queremos visualizar un Web, la tenemos que descargar completa a nuestro espacio compartido, lo que provoca que se observe una lentitud al navegar.
Los usuarios de esta red usaran su interface para poder configurar las diferentes opciones que ofrece como espacio en disco, ancho debanda, complementos instalados etc.

También se puede añadir complementos:
Freenet Message System (Foros de mensajes en esta red).
Freemail (Email en esta red).
Sone (Chat social).
jSite (Herramienta para subir sitios web).

Como resumen podemos definir FreeNet como un espacio libre y no censurado, donde podemos encontrar contenidos de varias temáticas, junto con foros donde expresar ideas o opiniones sin ser rastreado como sucede en la Surface.

En el capitulo tres en su apartado numero dos, expondremos la instalación de software necesario para acceder a FreeNet paso a paso, así como su configuración y se muestra una corta navegación por sus dominios con contenido licito, hemos evitado entrar en ninguna Dark Net de esta red, dejando a decisión del lector de este trabajo, si lo considera oportuno y bajo su responsabilidad, adentrarse más a fondo.

2.4.Tor.

El significado de la palabra Tor en ingles es The Onion Router y que, e en castellano, podríamos traducir como El Enrutamiento Cebolla, en concreto es un software basado en un cifrado desarrollado por la marina estadunidense para proteger sus comunicaciones dentro del protocolo IP. Este proyecto se convirtió en el año 2006 en una ONG si animo de lucro para garantizar que los usuarios puedan acceder a Internet de forma anónima a una determinada pagina Web y sin censura por parte de las autoridades competentes [16].

2.4.1. ¿Qué es la Tor Network?.

Tor Network o la red de Tor se compone por servidores dedicados e instalado de forma voluntaria (pueden ser personas anónimas) por diferentes usuarios, los cuales permiten a cualquier usuario de la Tor Network, mejorar su privacidad y seguridad.

Podemos definir que Tor es una red compuesta por servidores de usuarios que de manera altruista permiten usar su ancho de banda y capacidad de procesamiento por el bien del resto de los integrantes de la red y de una forma globalizada.

La conectividad de los usuarios no se realiza conectándose directamente a uno de los servidores, sino que se crean unos túneles virtuales de forma que no se comprometa la privacidad de los miembros de la red. Los túneles virtuales se van creando entre los distintos equipos de la red y de forma predeterminada realiza tres saltos por diferentes sistemas que componen la red antes de llegar la petición al servidor al que se quiere acceder. Mediante esta red se puede navegar por las profundidades de la Deep Web sin exponer nuestra identidad ni la de otros usuarios manteniendo un anonimato de los sitios Web que visitamos, ya que se oculta el origen y el destino dentro del trafico de Internet evitando que alguien descubra fácilmente tu identidad y que paginas o acciones realizas en la Red de Redes.

2.4.2. Análisis de la Red Tor.

Como hemos visto Tor esta compuesta por muchos servidores o nodos voluntarios por todo el mundo, los cuales se conocen como relays (en el capitulo 2.4.4 se detallarán los distintos tipos que existen).

La comunicación origen destino se cifrará por capas y es retransmitida a través de tres nodos de la red que relazan un camino antes de llegar al servidor de destino. Para que la seguridad sea lo más estricta posible cada nodo del camino de comunicación solo sabe de quien recibe los datos y a quien se los tiene que enviar, En cada salto de comunicación se realiza una nueva negociación de claves a usar en

los cifrados, por lo que se asegura una robustez importante entre todas las comunicaciones y dificultad en descifrar su contenido.

Como hemos visto cada nodo encripta de nuevo la información, por esto propiedad se le conoce con el nombre de enrutador cebolla, ya que cuando la información llega a un nodo, este lo encripta con sus datos privados y lo pasa al siguiente, obteniendo las diferentes capas al pasar por cada nodo que pertenece al camino de comunicación. Para obtener la información original se necesitarán la clave o llave del cliente con respecto a los nodos que interviniesen en el camino entre el cliente y el servidor. Seguidamente vamos a ver un grafico esquemático que nos muestra como se realiza la comunicación en la red Tor

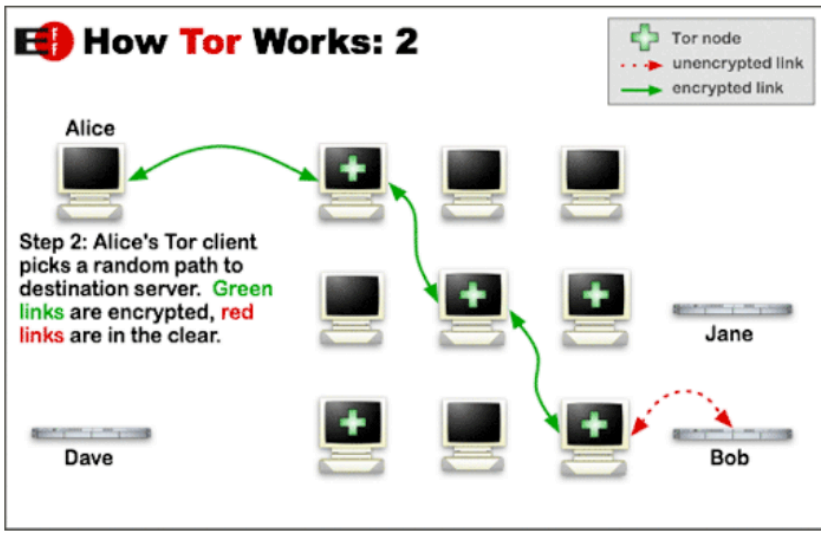


Figura 8: Flujo de comunicación entre nodos Red Tor. [16]

Como podemos observar Alice quiere comunicar con Bob y vemos que se utilizan tres nodos intermedios, En le grafico no esta representado a identidad o servicio de directorio la cual tiene la lista de nodos disponibles, por lo que lo primero que se realizaría es que el Onion Proxy del cliente de Alice solicita la lista de nodos habilitados al servicio de directorios, seguidamente el Onion Proxy de forma aleatoria elige un camino para llegar a Bob, Ahora Alice cifra su comunicación con el primer nodo (1º Capa), el primero lo reenvía al segundo y añade su cifrado (2º Capa) el segundo lo envía al tercer y le añade su cifrado (3º Capa) este ultimo es el que eliminara todas las capas de cifrado en Orden LIFO (del ingles Last In, First Out, ultimo en entrar, primero en salir) y lo enviara en claro sin cifrar al ordenador de Bob, Tanto Bob como alguien que capture este trafico sabría los datos del origen.

Podemos observar que siempre se usan tres nodos o relays. Esto es así porqué los desarrolladores estipularon qué un camino más seguro seria de tres miembros, es decir un nodo de entrada, otro intermedio y uno de salida (en el apartado 2.4.4 se tratarán los tipos de Relays). Por lo que en la Red Tor toda las rutas o caminos son de tres nodos y es un parámetro por defecto, que se recomienda no cambiar.

Si solo usásemos dos nodos, la navegación será más rápida y fluida, pero el anonimato se expone ya que solo participarían el nodo de entrada y el de salida, por lo que espiando el nodo de salida podrían saber quien esta originando las peticiones y desde donde. Concluimos que no es seguro usar solo dos nodos.

Si usamos más de tres nodos, podríamos pensar que cuantos más saltos nuestra privacidad se encontraría segura, pero varios estudios indican que la velocidad de navegación se ralentizaría mucho y nuestra privacidad se vería expuesta.

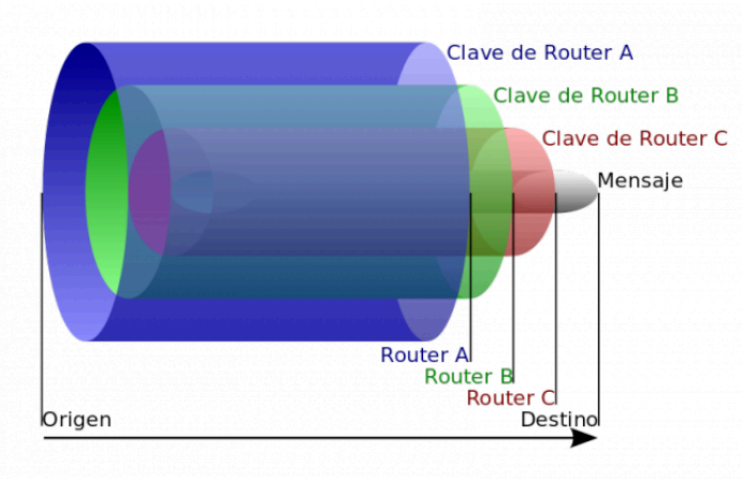


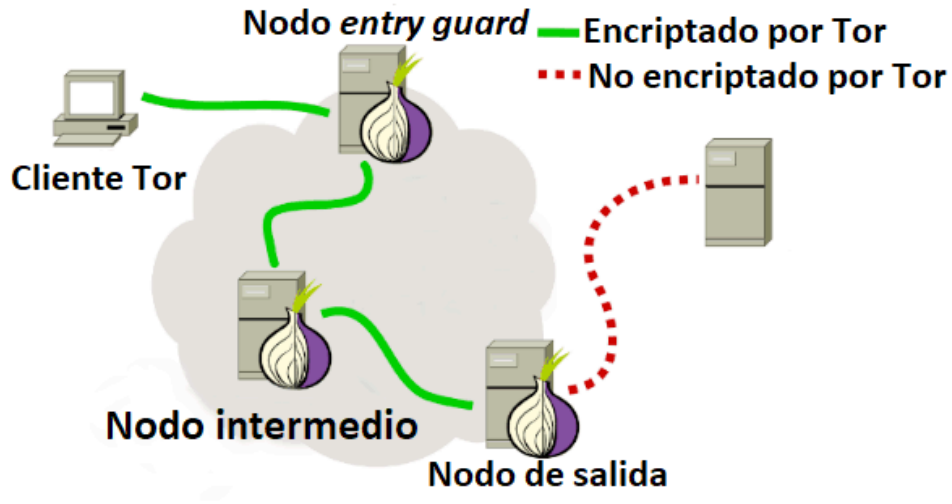
Figura 9: Dibujo explicativo de las capas de encriptación Red Tor [17].

2.4.3. Túneles virtuales.

Tor Network como hemos mencionado se estructura con muchos nodos o relay de usuarios voluntarios por todo el mundo. Ahora vamos a exponer como se forman y funcionan estos túneles virtuales. Cuando desde el navegador Tor browser realizamos una petición a un servidor, de forma transparente y automática se crea un camino virtual entre el usuario y el servidor al cual se quiere acceder es decir se crea un camino virtual entre los nodos solo para esa comunicación. Y estos cambiaran si se realiza una nueva petición a otro servidor distinto, En estos túneles virtuales los nodos del camino virtual entre el servidor y el cliente que solicita su servicio, solo saben quien le ha proporcionado información y a quien se la proporciona. Nadie en el camino virtual tunelizado conoce la ruta completa que toma un determinado paquete. La seguridad se garantiza porque en cada salto que realiza un paquete entre los túneles virtuales, el cliente negocia un nuevo par de claves. Se los conocen como túneles virtuales porque los nodos relays se comunican mediante el protocolo TLS sobre TCP/IP, Por lo que se crea una comunicación íntegra, totalmente privada y secreta, pudiendo de esta forma asegurar que la información que viaja por ese túnel, no podrá ser leída por terceros.

2.4.4. Tipos de Relays.

Vamos a detallar los distintos tipos de nodos o relays que existen en la Red Tor y que misión cumple cada uno dentro de la estructura de red. En la figura siguiente podemos apreciar el circuito de comunicación junto con los nodos que intervienen y sus roles.



Esta imagen muestra un esquema de un circuito de la red Tor contra un servidor convencional. El cliente Tor queda enmascarado al viajar su información por tres nodos antes de llegar al servidor de destino. ¿Por qué se utilizan tres nodos exactamente? Porque una de las mejores maneras de atacar la red Tor pasa por controlar el primer y el último nodo, por lo que el uso de más nodos intermedios no asegura una mayor privacidad y, en cambio, aumenta la carga en la red y genera latencia | The Hacker News

Figura 10: Nodos de comunicación y sus roles de la Red Tor [17].

Nodo de Entrada (Entry Guard)

Es el rol encargado de recibir la información del cliente en su primer salto desde el Onion Proxy del navegador Tor del cliente. Este nodo es similar a uno intermedio, pero mediante diferentes parámetros como el ancho de banda, tiempos de actividad ininterrumpidamente, etc. se obtiene una flag que otorga esta característica al nodo.
Los usuarios que se conectan a la Red Tor se le asigna un nodo de entrada o Entry Guard con el que siempre trabaja este cliente de forma temporal, ya que esta asignación caduca al tiempo y se produce una renovación de la lista de los nodos de entrada, asignándose otro nodo de entrada al usuario, hasta que vuelva a caducar, que volverá a obtener otra nueva lista. Este proceso se repetirá a lo largo del tiempo que el usuario este conectado a la Red Tor.

Nodo Intermedio (Middle Relay)

Es el tipo más fácil de obtener, por no pedir ningún tipo de requerimiento mínimo como sucede en los nodos de Entrada y ser su configuración es más sencilla. Estos nodos o relay son los que reciben la información encriptada de los nodos de entrada, añaden su capa de cifrado y lo reenvían al nodo de salida. Este tipo de nodo no es de mucho interés para obtener información o realizar algún tipo de ataque a la Red, ya que maneja solo información encriptada entre el nodo de entrada y el de salida.

Nodo de Salida (Exit Relay)

Este nodo, es el más deseado por los atacantes, por lo que es complejo y peligroso poseerlo, como para los usuario que salen a través de él, ya que es el ultimo salto que se realiza directamente al servidor que presta el servicio y la información se envía de forma descriptiva, es decir con la IPs de origen de cada comunicación, por lo que los atacantes ponen mucho interés en conseguir información importante de ellos y si la consiguen pueden obtener nuestra identidad o el punto donde se origino la petición de conexión a ese servicio.
Este tipo de nodos, tiene una gran cantidad de exigencias para obtener el rol, tanto de anchos de banda como de respuestas a muchas peticiones. Este tipo de nodo también es igual que un intermedio, pero requiere una configuración especial y más exigente de todas las políticas de salida.

Nodo Puente (Bridge)

Este tipo de nodo no esta catalogado dentro de la estructura de directorios de la Red Tor, En caso de que los proveedores de servicio de internet (ISP) bloque el trafico de la Red Tor por algún tipo de censura, lo que no podrán es bloquear los nodos puente. Estos tienen la misión de evitar la censura de algunos gobiernos.

Si queremos utilizar un nodo de este tipo en nuestro navegador Tor Browser, tenemos que obtener la lista actualizada de puentes que se encuentra en https://bridges.torproject.org/bridges, en ella se indican las instrucciones para incorporar esto puentes en nuestro navegador y de esta forma poder navegar por Tor aunque nuestro ISP corte el trafico mediante alguna técnica de profunda de búsqueda de paquetes. Adjuntamos captura de la Web:

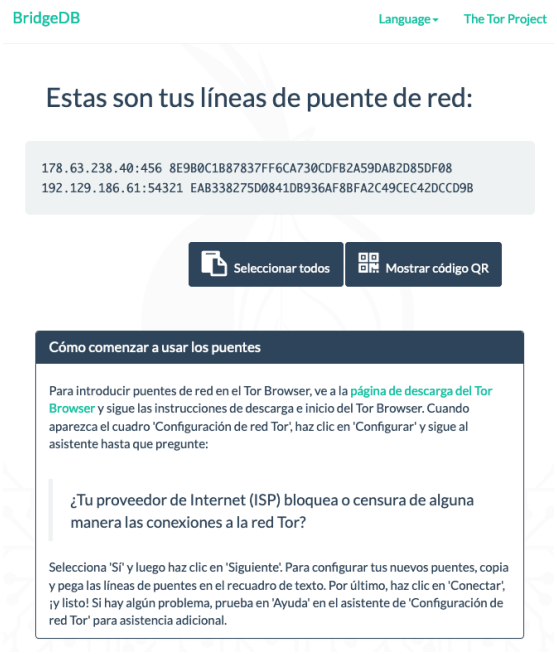


Figura 11: Nodos Puente de la Red Tor.

También podemos usar algún tipo de proxy para ignorar la detección del trafico Tor por el ISP.

En la pagina Web https://tormap.void.gr/ podemos observar los distintos tipos de modos operáticos en todo el mundo, adjuntamos distintas capturas de la información que podemos obtener:

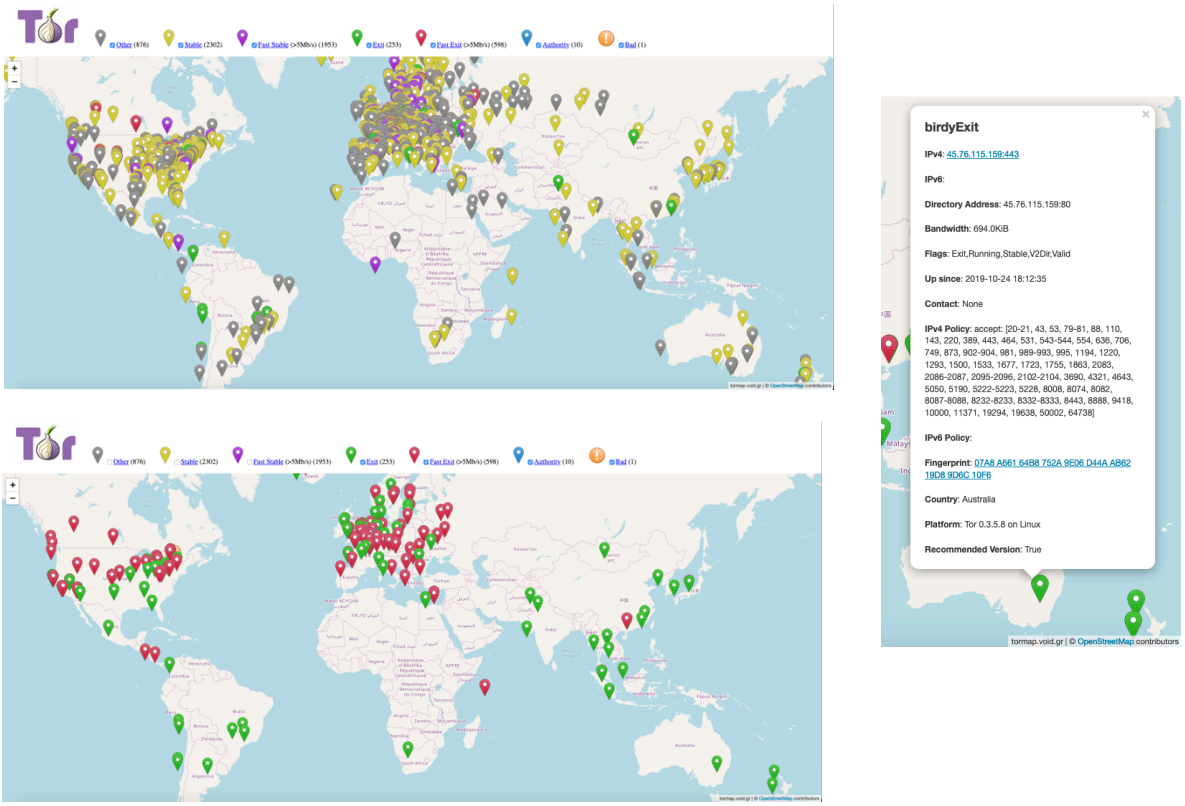


Figura 12: Nodos operativos en todo el mundo de la Red Tor [18].

2.4.5. Servicios Onion.

En la Web Superficial se utilizan conceptos como dominio y DNS, vamos a recordar brevemente que son para luego comparar con los Servicios Onion que usa la Red Tor.

El domino se puede definir como un nombre que nos identifica un servidor especifico que da un servicio, Los más comunes son .com .es .org como por ejemplo http://www.google.es, esto seria la URL de una pagina Web y es lo que mejor recordamos los humanos, ya que es texto legible. Pero en el mundo de las redes todos los servidores conectados se localizan mediante sus direcciones IP, en la siguiente captura vemos como mediante el comando ping sobre la URL anterior nos da como dirección IP 216,58,201.163.

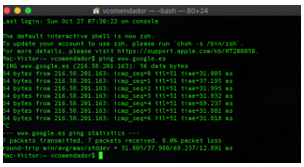


Figura 13: Comando Ping para obtener IP de una URL.

Por lo que aprendernos las direcciones IP de los distintos servidores que visitamos seria muy complejo, por eso se creo el Sistema de Nombre de Dominio DNS para realizar la traducción entre la URL y la Dirección IP del servidor en cuestión. Mediante estos sistemas es sencillo escribir una URL en lenguaje y palabras fáciles de entender y las DNS la traducen a la IP del servidor. Pero esto no sucede en la Red Tor, En esta Red las URL que introducimos en al navegador, no son tan sencilla y fáciles de recordar como en la Surface. Lo primero que observamos es que las tres “w” desaparecen y que ahora ya no tenemos una secuencia de letras fácil de recordar, leer o comprender, las direcciones onion estarán compuestas por 16 caracteres [19] en su mayoría letras y números aleatorios seguidos de .onion,(esto es un pseudo-dominio ya que Tor no posee ningún servidor tipo DNS para resolver la dirección IP). La generación de la dirección onion se realiza usando la clave pública del servicio. Vamos a indicar la dirección del buscador Duckduckgo en la Surface es: https://duckduckgo.com/ y en la Red Tor su URL en el pseudo-dominio onion es: https://3g2upl4pq6kufc4m.onion/ .Podemos apreciar la diferencia de URL para un servicio similar en la Red Superficial y la Red Tor. Cuando se navega por direcciones onion el navegador Tor nos lo indica con un pequeño icono verde representativo de una cebolla [20]

Tor Project ha creado una nueva estructura de estos servicios y que serán direcciones privadas al completo y solo la conocerá su creador. Ahora tendrán 56 caracteres A efectos de nuestro trabajo hemos creado una con la ultima versión.

El resultado ha sido:

oexj6fmfeutb5fvb7ghbvb22oelv32kj7euciwgwj4dova45hf3did.onion

2.4.6. Servicio oculto.

A continuación, vamos a exponer de forma resumida como crear un Servicio oculto dentro de la Red Tor.

Precederemos a desplegar una maquina Linux con un servidor de paginas Web como por ejemplo Apache, podrimos usar la distribución de kali Linux y en la misma maquina crearemos nuestra pagina Web que dará servicio en la Red Tor.

Ahora en la propia maquina crearemos el servicio oculto siguiendo los pasos siguientes:

Instalación de Tor con el siguiente comando:

apt-get install tor

Verificaremos que se ha instalado y su ubicación:

whereis tor

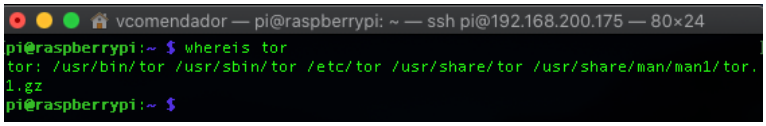


Figura 14: Ubicación de la instalación de Tor en la Raspberrry.

Accedemos al directorio de Tor

cd /etc/tor

Precedemos abrir el fichero de configuración torrc y buscamos el apartado de hidden servces:

sudo nano torrc

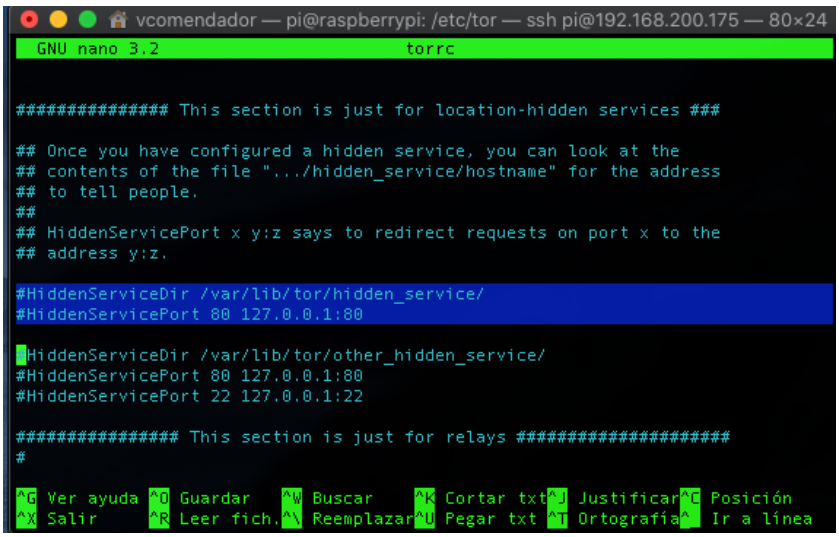


Figura 15: Contenido del fichero torrc.

De las dos líneas marcadas en la captura anterior retiraremos el signo de # para que al arrancar Tor ejecute las líneas.

Arrancamos Tor:

tor

Una vez arrancado nos creara varios archivos, el primero es el hostname, el cual contiene la dirección onion que tendrá nuestra pagina Web dentro de la Red de Tor, la cual se ha generado de forma automática. Como estamos usando la ultima versión de Tor a fecha de la ejecución de este trabajo, obtenemos el nuevo formato de .onion que es de 56 caracteres, así como los dos ficheros con extensión key publico y secreto.

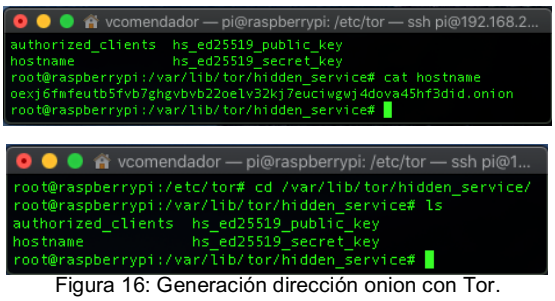


Figura 16: Generación dirección onion con Tor.

2.5.Análisis de Riesgo.

En el capitulo siguiente realizaremos una navegación por varias redes de anonimato y queremos exponer de forma breve algunos riesgos en los que nos podemos ver comprometidos, así como enumerarlos por sus diferentes tipos. Puntualizaremos que en la red superficial nos podemos encontrar también con estos riesgos.

A nivel tecnológico nos podemos encontrar con diferentes problemas como: virus, troyanos, spyware, que son programas maliciosos que intentaran extraer información de nuestro ordenador o encriptarlo nuestros datos solicitándonos dinero para recuperarlos. También podríamos sufrir algún ataque de hacker de sombreo negro.

A nivel de comunicaciones con otras personas o plataformas de comunicación podríamos sufrir los siguientes riesgos: correos ofensivos, correos basura, nos pueden bloqueara el acceso a nuestra cuenta de correo o redes sociales, entrar en nuestra cuenta de correo o redes sociales teniendo acceso a nuestra intimidad, utilizar los datos obtenidos para ejecutar algunas acciones ilegales con nuestros datos obtenidos de forma ilícita.

A nivel de información en estas redes nos podemos encontrar: noticias falsas, acceder a informaciones inmorales o ilícitas, información nociva de imágenes duras de ver, el navegar de forma errática y despistarnos de nuestro objetivo.

A nivel económico: estafas, robos, compras no deseadas, clonación de tarjetas bancarias, uso de la tarjeta por personas no autorizadas, etc.

A niveles legales: La tecnología evoluciona a un ritmo muy superior al que el Derecho, pues este viene a regular situaciones sociales que se producen, inevitablemente, antes y de manera imposible de prever en muchos casos, muy especialmente en el que nos ocupa que avanza en dos vertientes, una la tecnológica científica y otra la de "usuarios cualificados" por utilizar una denominación, que llegan ha hacer un uso de estas tecnologías para amparar hechos o conductas totalmente contrarias a Derecho, aunque, obviamente, no fueran creadas para ello.

Utilizando torticeramente las posibilidades tecnológicas pululan delincuentes de muy diversa índole, acosadores por los distintos medios de Mensajería, ataques a la intimidad el honor y la propia imagen, varias formulaciones del delito de estafa, coacciones delictivas "secuestrando" los datos de Servidores Informáticos de un Corporativo Oficial o Privada, contra la propiedad intelectual, contra la indemnidad sexual engaños en este campo con abuso de menores que se han dado en denominar Grooming. que es la acción que realiza un adulto para ganarse la confianza de un menor con el objetivo de obtención de favores sexuales, el acoso entre iguales, CiberBullying muy extendido entre menores y consistente en ridiculizar o insultar a otro menor por internet, pornografía infantil y un largo etcétera de versiones de estos hechos que pueden variar en su forma o sistemática tecnológica pero no en su fondo.

Es evidente que los Legisladores van incluyendo estos hechos en sus respectivas Legislaciones Penales, pero desgraciadamente avanza más rápido el Delincuente, resultando muchas veces que estamos sometidos al riesgo de ser victimas de alguna de estas conductas que podríamos denominar Delincuenciales Tecnológicas.

Desde el punto de vista, como en nuestro caso ocurre, de Titulados Universitarios Tecnológicos, no cabe duda que estamos en condiciones de detectar muchas de estas conductas y en ocasiones su origen, es por ello que ante la simple sospecha fundada o detección clara de alguna de ellas, debemos proceder a la denuncia inmediata, ante las autoridades competentes y por deontología profesional colaborar siempre en todo lo posible con dichas Autoridades, máxime teniendo en cuenta que los Cuerpos de Seguridad del Estado ya disponen de Unidades de Policía Judicial dedicadas a la persecución de estas conductas delictivas.

Otro caso es el del usuario que, carente de conocimientos tecnológicos, suficientes puede ser victima de una utilización por parte de individuos u organizaciones criminales, de estos delitos incluso con la imputación de aparentes responsabilidades de la propia victima.

En este punto y a efectos, igualmente de deontología profesional debemos prestar nuestras periciales de la forma más honrada y científica posible cunado así de nos solicite por Autoridades o particulares.

No cabe duda de que la denuncia inmediata liberaría de responsabilidad alguna.

Como vemos no estaos exentos de riesgos, aunque estemos detrás de un ordenador.

2.6. Comparativa I2P, FreeNet, Tor.

Procederemos a continuación a realizar una pequeña comparativa entre las redes comentadas en los apartados anteriores:

Hemos observado que las tres redes tienen sus diferencias tanto en su funcionalidad como en usabilidad, por lo que precedemos a exponerlas a continuación:

I2P sus funcionalidades y comportamiento son similares a la Red Tor, ya que también cada usuario es un nodo/relay de la red, por lo que aumentamos en nivel de anonimato. De igual forma esta red utiliza túneles unidireccionales por lo que se complica la posibilidad de obtener información de un usuario, ya que se tienen que comprometer dos túneles. Esta red posee menos usuario en la actualidad y este hecho, puede permitirnos detectar a un usuario con mayor facilidad que con miles de usuarios siendo nodos/relays. De igual manera el bajo nivel de usuarios, también podría ofrecer un menor rendimiento en cuanto a latencia y velocidad.

FreeNet se puede definir como una red de publicaciones anónimas y distribuidas, que funciona como un almacenamiento de datos. Bajo este concepto se han diseñado paginas Web que se van descargando de ordenador a ordenador sin necesidad de que el usuario que la genero se encuentre en línea. Por lo que la velocidad de esta red dependerá de la cantidad de clientes conectados y que tengan disponible para intercambiar el contenido solicitado.

Tor se compone de servidores proxy para anonimizar la navegación por Internet que permite a las personas hacer un túnel a través de su red mixta de baja latencia, evitando censuras locales, ya que el sitio Web no puede obtener información del origen, por lo consiguiente manteniendo nuestro anonimato. La Red Tor es una de las redes con más usuarios y contenidos disponibles, por lo que suele dar mejor rendimiento ante la latencia y la velocidad.

Compararemos los beneficios de cada red entre ellas:
Tor sobre I2P:

-Base de usuarios muy grande (comunidades académicas y hackers).
-Financiamiento y desarrolladores dedicados.
-Más resistente al bloqueo.
-Diseñado y optimizado para el tráfico de salida.
-Los nodos del cliente poseen una baja sobrecarga de ancho de banda.
-Esta programado en C y no en Java que es interpretado.

I2P sobre Tor:

-Diseñado y optimizado para servicios ocultos.

-Los pares de relleno ("servidores de directorio") varían y no son confiables, en lugar de codificados.

-Paquete conmutado en lugar de circuito conmutado

-Túneles unidireccionales en lugar de circuitos bidireccionales.

-Los túneles en I2P son de corta duración.

-Mecanismo integrado de actualización automática.

-Transportes TCP y UDP.

FreeNet sobre I2P y Tor:

Una funcionalidad que hemos comentado de FreeNet y que en comparación con I2P y Tor, estas dos ultimas no poseen es que al ser Freenet un almacén de datos distribuido (lo que no son ni Tor ni I2P), nos permite recuperar el contenido publicado por otros usuarios incluso cuando el creador del mismo ya no está en línea.

3. Pruebas realizadas.

Para la realización practica de la prueba hemos usado una distribución de Linux denominada Q4OS [22], la cual está basada, a su vez, en una distribución Debian, La aparecía que nos muestra su escritorio es muy similar a Windows, incluso en la instalación de aplicaciones. La referida distribución la hemos instalado en una máquina virtual bajo Vmware,, e iremos realizando el proceso de instalación de las distintas redes de anonimato I2P y Frenet. Al respecto de la navegación sobre la Red Tor la realizaremos de forma distinta. Ajuntamos captura de la pantalla principal de Q4OS:

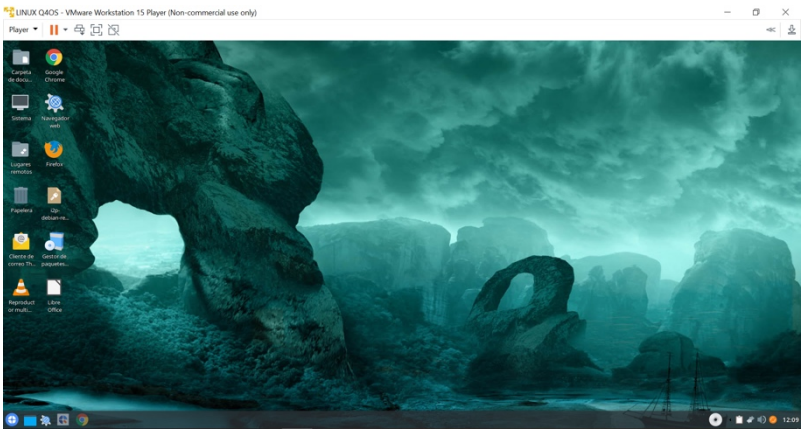


Figura 17: Sistema Operativo Linux Q4os

3.1. Test I2P.

Empezaremos nuestras pruebas con la Red I2P, de cual describimos sus características y funcionamientos en el apartado 2.2. Ahora veremos como se realizará la instalación, configuración y navegación.

3.1.1. Instalación de la red I2P.

En primer lugar, iremos a la Web [23] del proyecto I2P. Seguidamente iremos a la página de descarga de software y procederemos ha buscar el instalador especifico para nuestro sistema operativo, que en nuestro caso son los paquetes para el sistema Debian, los culés los hemos localizado como indican las capturas siguientes:

Figura 18: Web I2P y descarga de software.

Hemos seguido las instrucciones indicadas por la pagina, introduciendo los comandos paso a paso. Al finalizar la instalación procedemos a levantar el router de i2P como muestran las siguientes capturas:

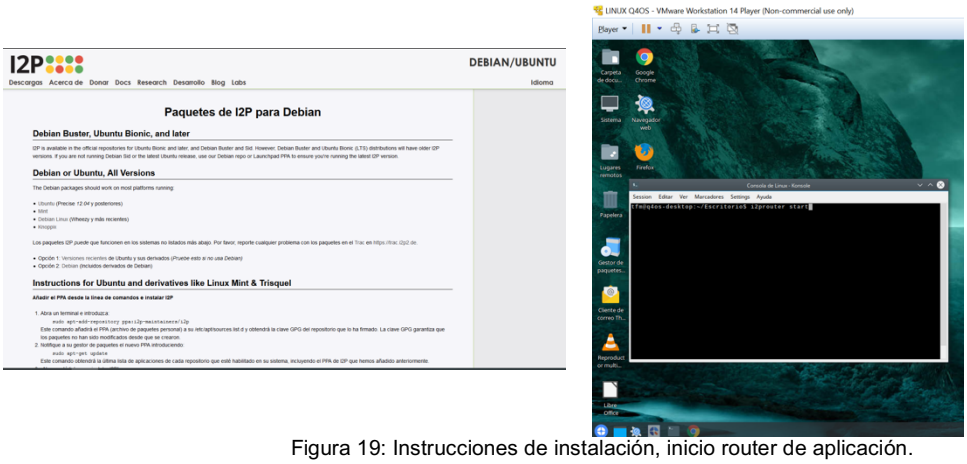


Figura 19: Instrucciones de instalación, inicio router de aplicación.

Una vez iniciado el router de I2P, se nos abrió automáticamente el navegador (por defecto) de sistema operativo con el proceso de configuración que es tipo Wizard. Para acceder al router usaremos la siguiente dirección: http://127.0.0.1:7657/home

He iremos siguiendo los siguientes pasos:

Selección de idioma, nosotros hemos elegido español y seguidamente se realizará un test de ancho de banda como ilustran las siguientes capturas:

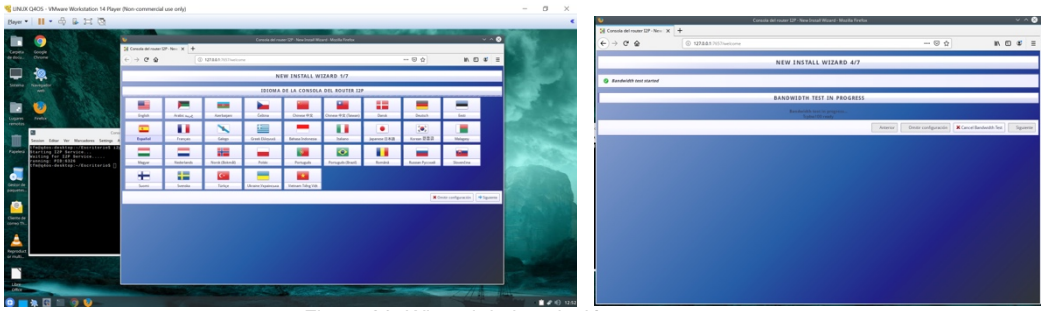


Figura 20: Wizaed de instalación

Ahora podemos configurar de forma personalizada el ancho de banda que vamos a disponer para esta red, así como el navegador:

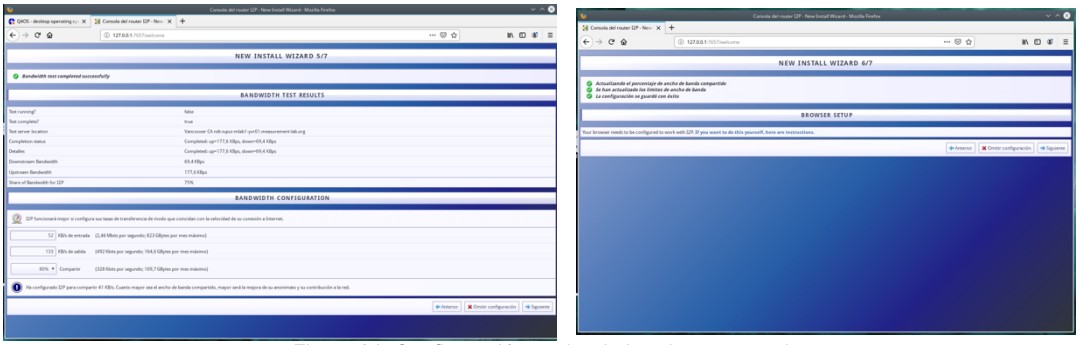


Figura 21: Configuración ancho de banda y navegador.

Ya hemos acabado la instalación de I2P, ahora accederemos a la consola de nuestro router:

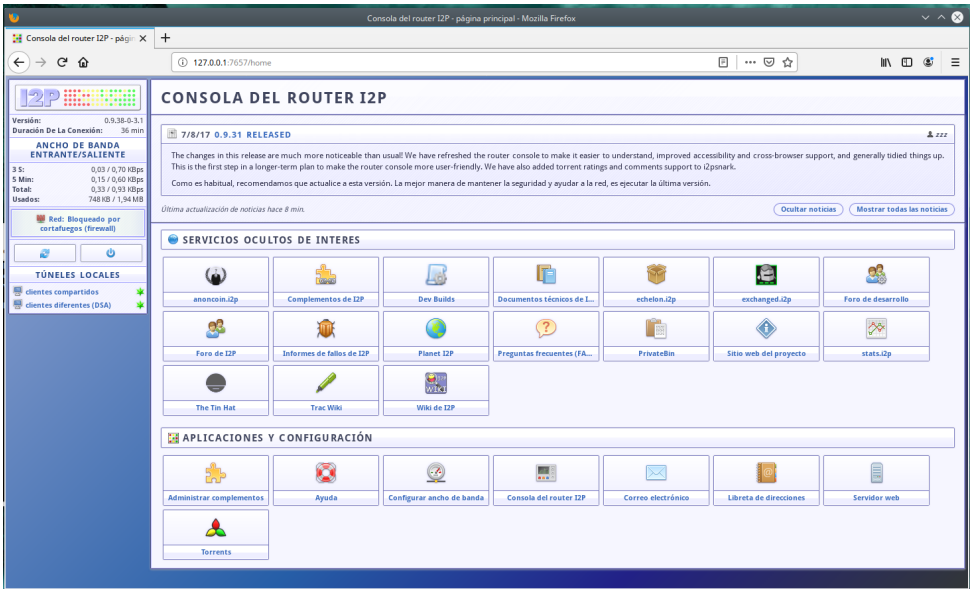


Figura 22: Consola de router I2P

I2P necesita un tiempo para empezar a realizar los túneles para navegar, por lo que tras unos minutos en nuestro router podemos ver todos los caminos locales que se están formando:

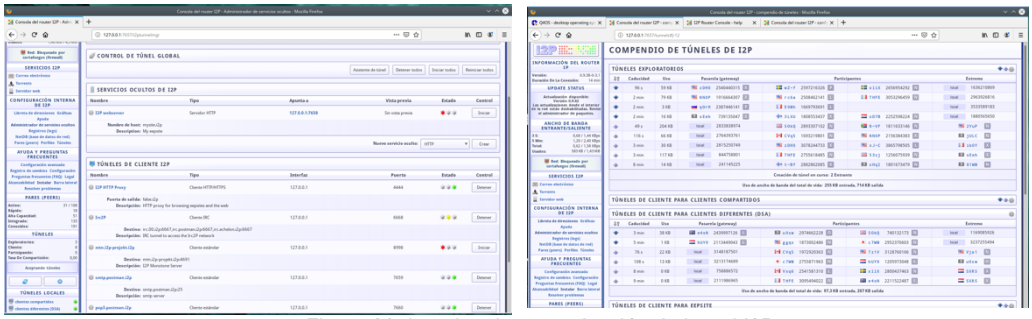


Figura 23: Luneles de comunicación de la red I2P

Ya tenemos operativa y funcionando nuestra conexión a la red I2P.

3.1.2. Test navegación I2P.

Ahora procedemos a navegar por esta red y ver algo de su contenido. Si deseamos navegar con otro navegador, pues antes tendremos que configurarlo, es decir tenemos que indicar los valores en el proxy de navegador, como mostramos en la siguiente imagen:

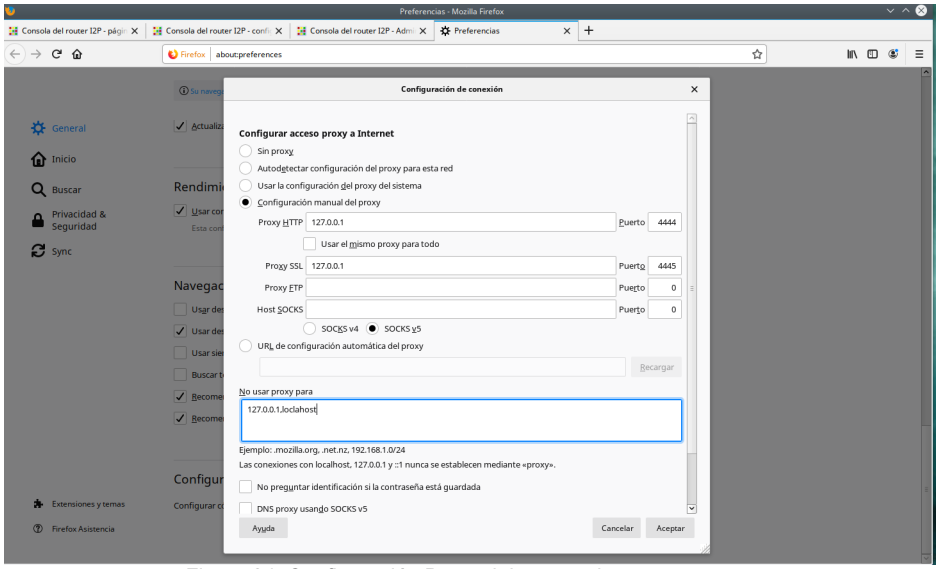


Figura 24: Configuración Proxy del navegador

Los dominios en esta red son punto I2P y pueden ser con letras, así como en base 32 o 64 de igual forma que en la red Tor que la veremos en próximos capítulos. De todas formas, en la propia consola del router se nos ofrecen servicios, así como una libreta de direcciones para ver la de un dominio concreto o añadir direcciones nuevas.

Exponemos una captura de la lista de direcciones del router.

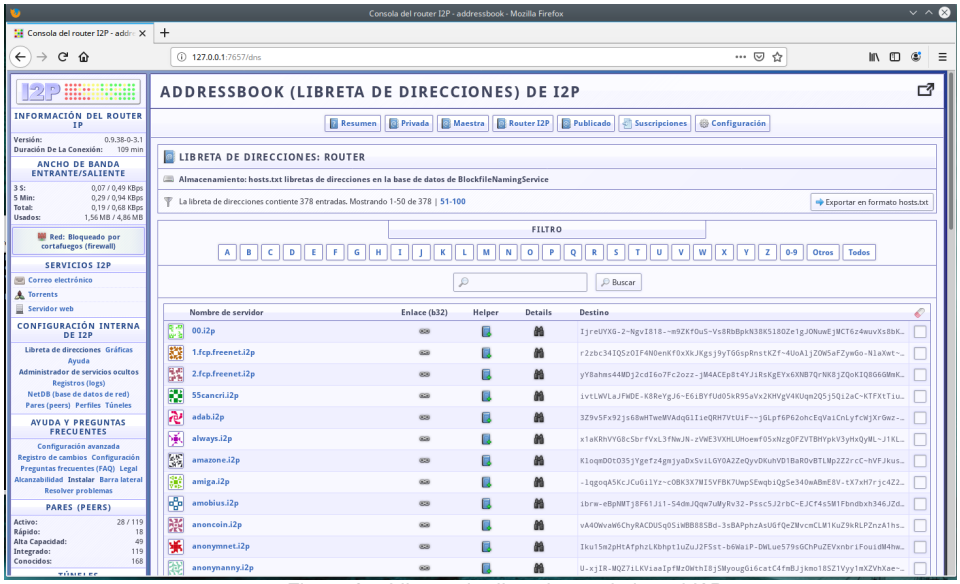


Figura 25: Libreta de direcciones de la red I2P

Hemos accedido a wiki de I2P en la dirección: http://i2pwiki.i2p/.

Dependemos del tiempo que este levantado el router para conseguir poder acceder a páginas más rápidamente, de todas formas, las páginas suelen tardar en cargar e incluso no poder acceder a ellas, mostramos este ultimo caso:

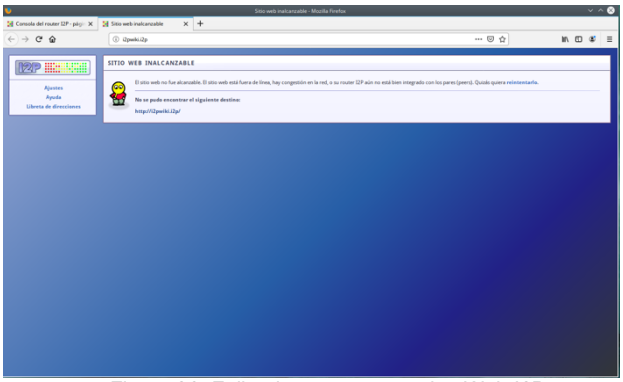


Figura 26: Fallo al cargar una pagina Web I2P

Hemos probado con otras Web y hemos podido acceder a bancos de moneda virtual http://anoncoin.i2p/

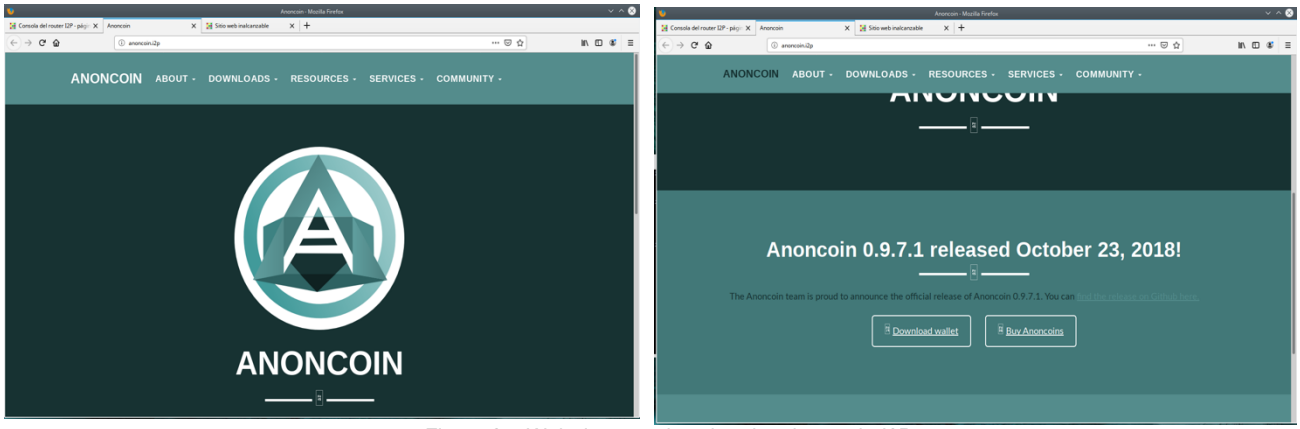


Figura 27: Web de monedas virtuales dentro de I2P

Siguiendo con nuestra navegación, hemos accedido a un Blog http://planet.i2p/.

Y vemos por ejemplo el programa MuWire que es similar a los P2P de la Surface, pero dentro de I2P.

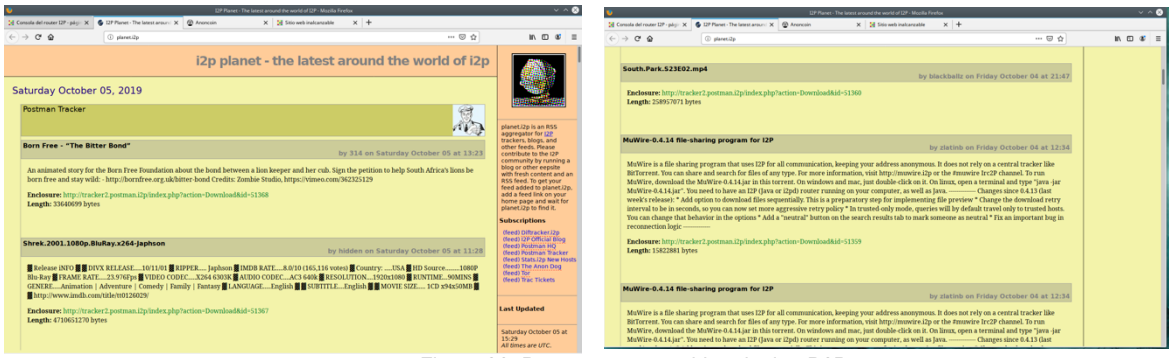


Figura 28: Programas en un blog de tipo P2P

Servicio en I2P para crear cuentas de correo electrónico de forma anónima. http://hq.postman.i2p/.

Se puede crear una cuenta en Postman para usarla anónimamente para recibir y enviar mensajes de correo electrónico con cualquier cliente de la red I2P.

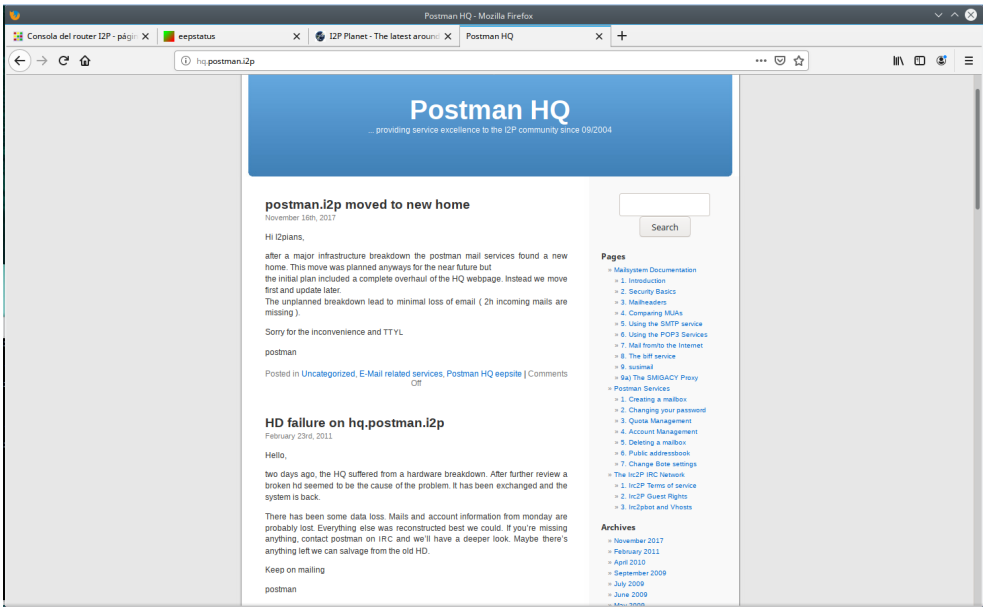


Figura 29: Programas de correo electrónico

3.2.Test Freenet.

Empezaremos nuestras pruebas con la Red Freenet, de la cual describimos sus características y funcionamientos en el apartado 2.3. Ahora veremos como realizara la instalación, configuración y navegación.

3.2.1. Instalación de la red Freenet.

En primer lugar, iremos a la Web [24] del proyecto de FreeNet. Seguidamente iremos a la página de descarga de software y procedemos ha buscar el instalador especifico para nuestro sistema operativo, que en nuestro caso son los paquetes para el sistema Debian, los culés los hemos localizado como indican las capturas siguientes:

Figura 30: Web FreeNett y descarga de software.

Procederemos a iniciar nuestra máquina virtual con el sistema operativo Q4OS, para proceder a la instalación del FreeNet.

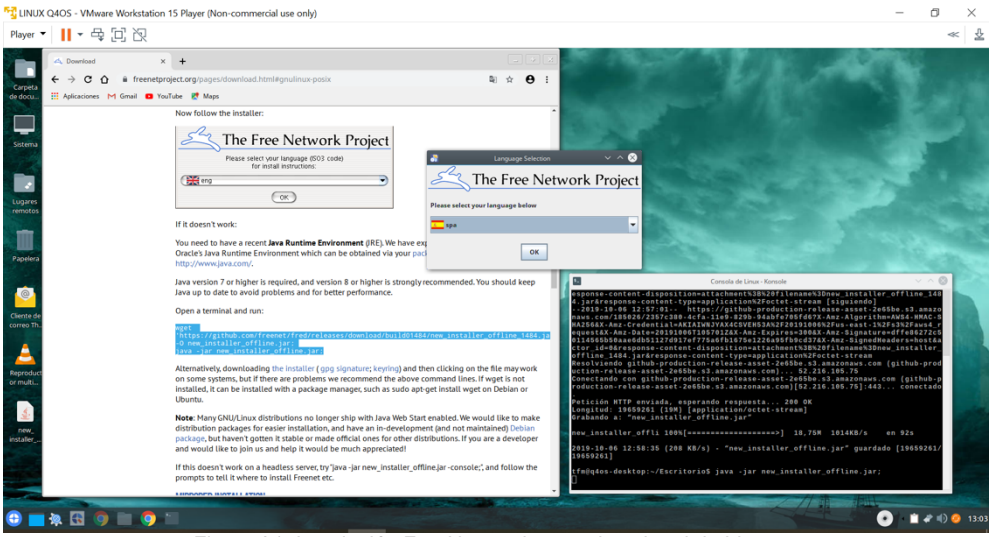


Figura 31: Instalación FreeNett en la maquina virtual de Linux.

Seguidamente mostraremos las capturas del proceso de instalación:

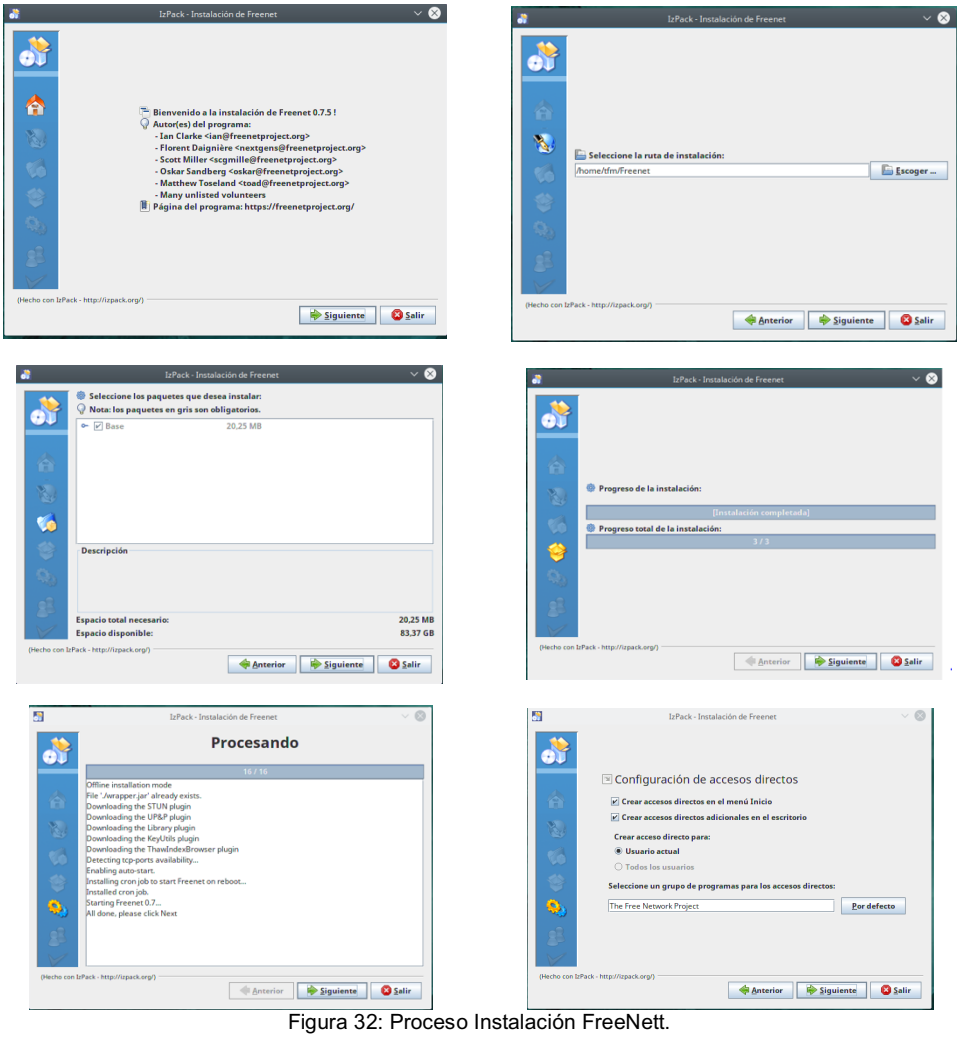


Figura 32: Proceso Instalación FreeNett.

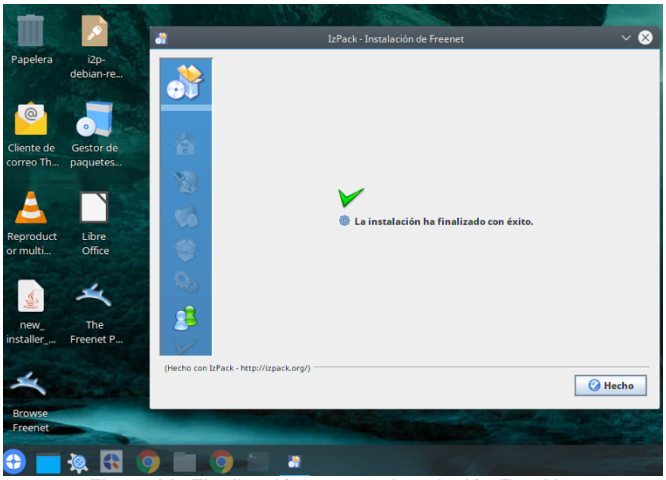


Figura 33: Finalización proceso Instalación FreeNett.

Una vez finalizada la instalación se nos abre al navegador (por defecto) con los pasos de configuración de FreeNet ya con el idioma en español.

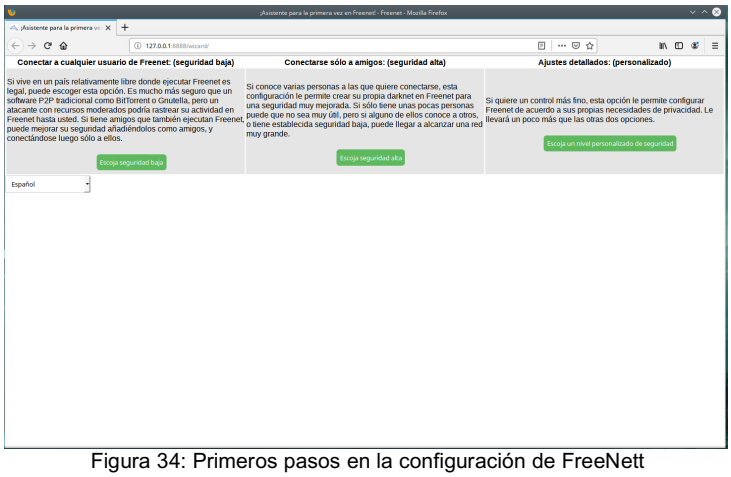


Figura 34: Primeros pasos en la configuración de FreeNett

En la imagen superior observamos tres opciones de seguridad para conectarnos a FreeNet. La primera sería una opción de seguridad baja, ya que conectamos a cualquiera ordenador de la red y desde alguno de estos podría ser fácil tracear nuestro tráfico, nos indica también que si en nuestro país no está censurado o es ilegal la utilización de este programa podemos optar por elle. La siguiente opción y recomendada es realizar una red entre amigos que usen esta red y así poder realizar Dark Net privadas con mejor seguridad, Por último, esta la opción de ajustes personalizados donde podemos realizar configuraciones para obtener una posible mezcla de los dos puntos anteriores.

Como estamos dentro de una máquina virtual de Linux, vamos a proceder a escoger la seguridad más baja y si nos encontrásemos con algún problema en la navegación, procederíamos a eliminarla.

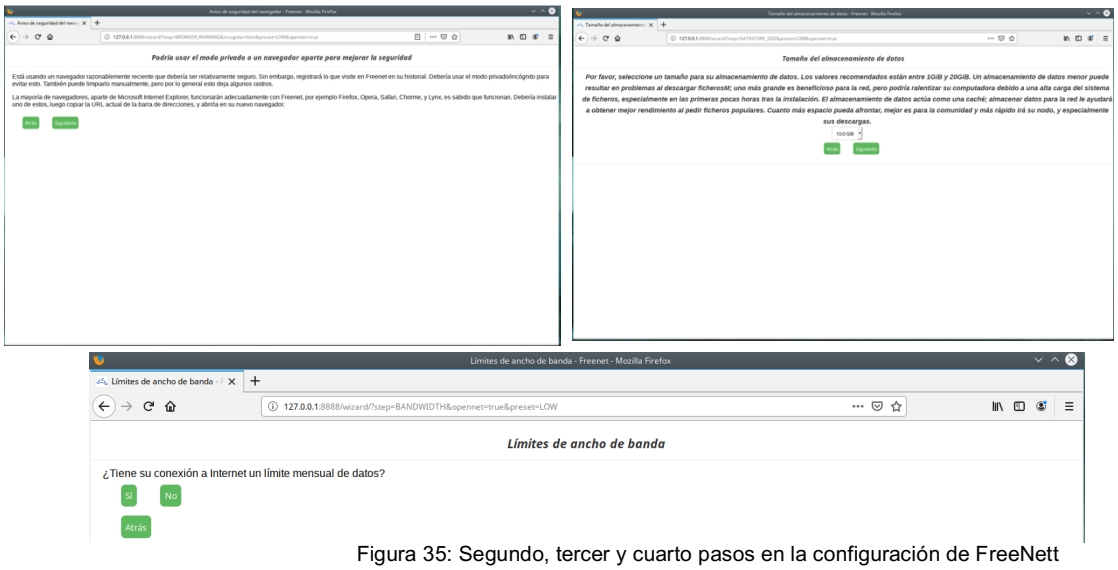


Figura 35: Segundo, tercer y cuarto pasos en la configuración de FreeNett

Nos recomienda navegar en modo privado u oculto para garantizar que no quede rastros de nuestra navegación por esta red. En el paso siguiente se solicita que indiquemos el espacio de disco duro que vamos a asignar para utilizarlo como almacenamiento de datos y cache, lo dejaremos por defecto en el valor que nos ofrece. En el cuarto paso se nos pregunta si tenemos una línea de internet con tope de descarga mensual, en nuestro caso diremos que no.

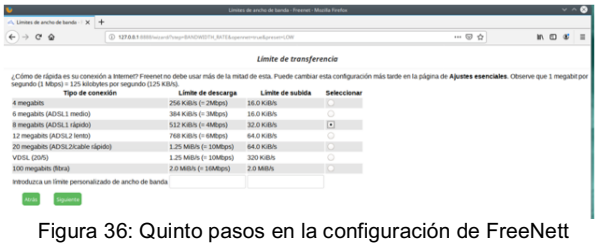


Figura 36: Quinto pasos en la configuración de FreeNett

Como se observa, nos solicita que tipo de anchos debanda disponemos en nuestra conexión, le daremos 8 megabit para que no se nos sature nuestra conexión.

Tras la última pregunta nos cometamos a FreeNet mediante el navegador y se nos mostraran los directorios de las páginas Web, en la siguiente captura lo podemos observar:

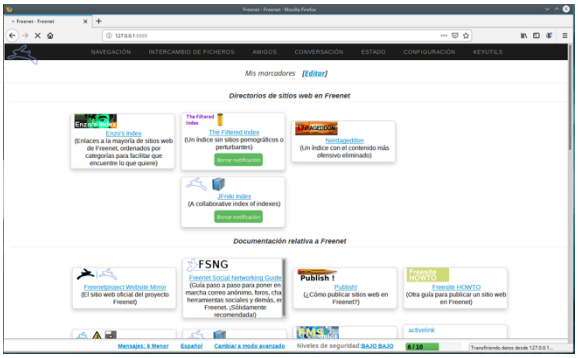


Figura 37: Enlace Web de FreeNett

3.2.2. Test navegación Freenet.

Ahora procederemos abrir nuestro navegador en modo privado para navegar de forma más segura.

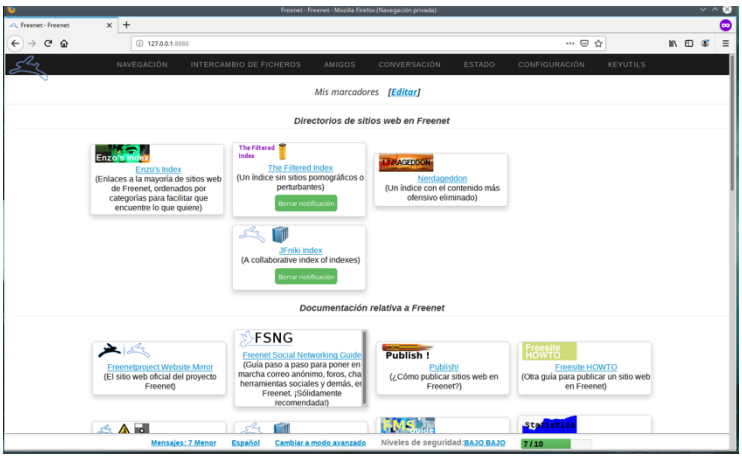


Figura 38: Enlace Web de FreeNett en navegador modo seguro

Hemos solicitado una página y vemos como FreeNet procede a descargarla:

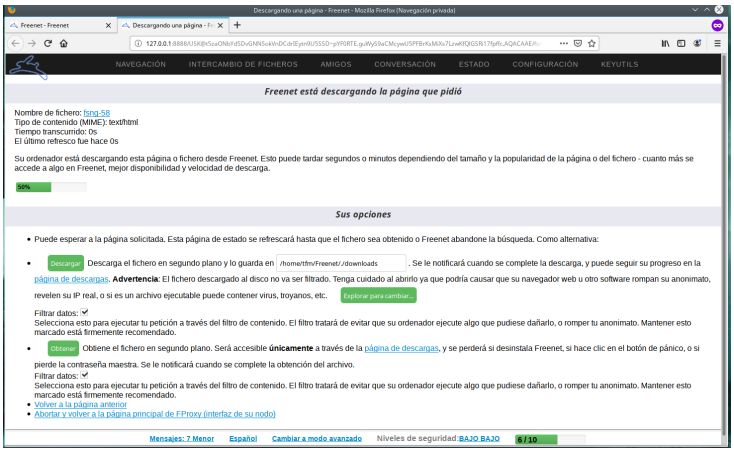


Figura 39: Descarga de una página Web de FreeNett

Una vez descargar se abre una pagina web con información de cómo crear servicios dentro de esta red:

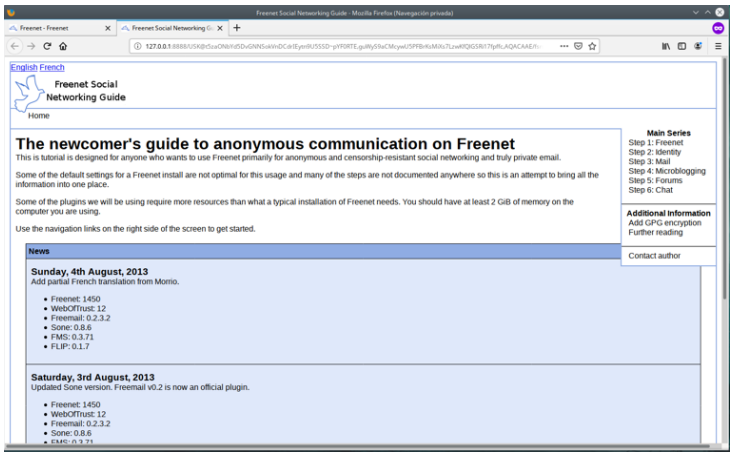


Figura 40: Web de información de comunicaciones FreeNett

Hemos accedido a otra web que nos permite enviar correo entre usuarios.

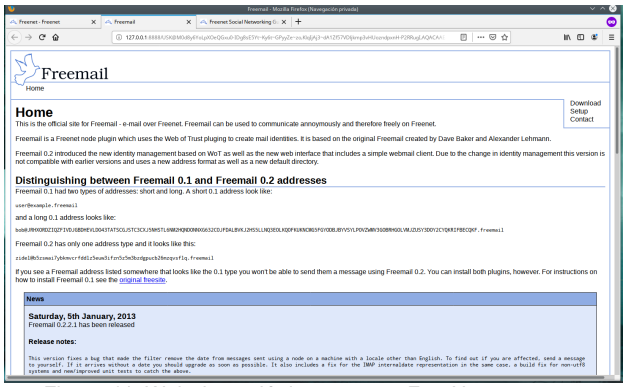


Figura 41: Web de envió de correo en FreeNett

Vemos ahora alguna de las opciones de esta red. En apartados anteriores se comento la posibilidad de crear redes privadas entre amigos, tanto por seguridad como si se quiere tener una Dark Net propia para el grupo, en la siguiente captura podemos ver este apartado:

Figura 42: Red privada entre amigos en FreeNett

A nivel de configuración podemos descargar de forma consecutiva diferente paginas o archivos si conocemos las claves.

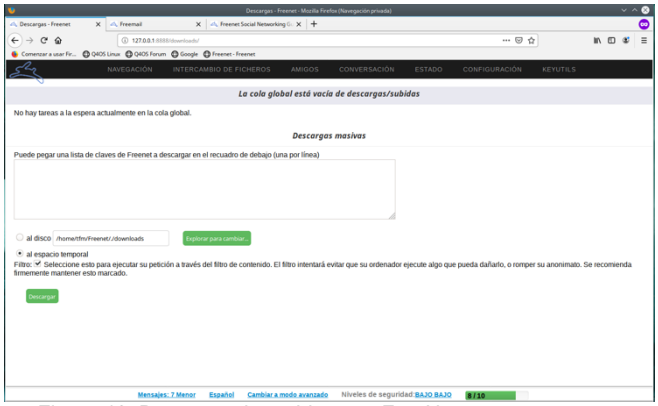


Figura 43: Descarga de archivos en FreeNett

Podemos hablar con otros usuarios de la red mediante los foros que nos ofrece la misma y la mensajería instantánea.

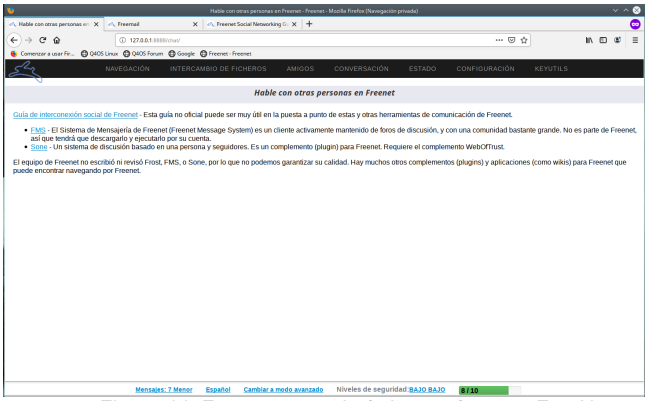


Figura 44: Foros y mensajería instantánea en FreeNett

Como herramienta nos ofrece la posibilidad de obtener estadísticas de nuestro nodo, como nos muestra la siguiente captura:

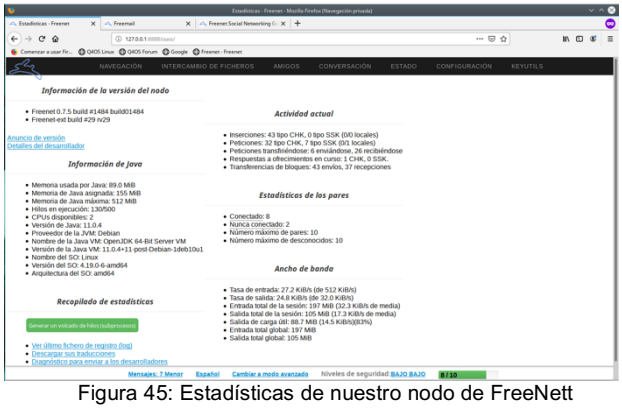
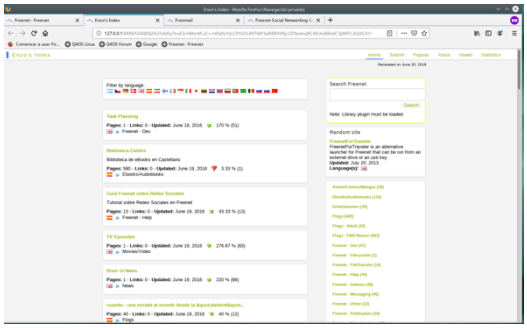


Figura 45: Estadísticas de nuestro nodo de FreeNett

Como continuación a nuestra navegación adjuntamos unas capturas obtenida de los directorios principales, como enciclopedias en castellano, foro de seguridad, etc:



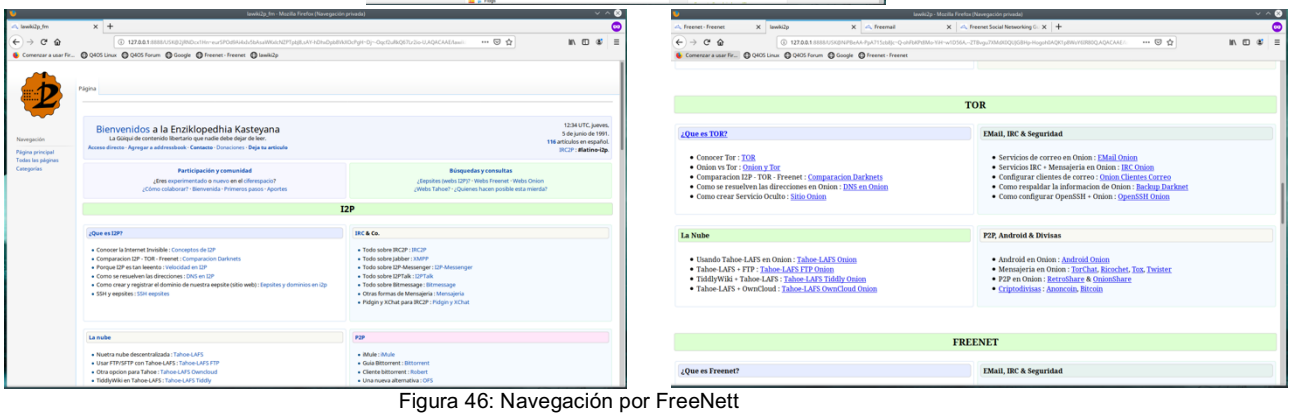


Figura 46: Navegación por FreeNett

3.3.Test Tor.

Empezaremos nuestras pruebas con la Red Tor, sobre la que describimos sus características y funcionamientos en el apartado 2.4. Ahora veremos como se realizará su instalación, configuración y como se navega por ella.

3.3.1. Instalación de la red Tor.

En esta ocasión para proteger más nuestro anonimato dentro de la red Tor, hemos usado una distribución enfocada a seguridad llamada Whonix [25] la cual esta basada en Debian. El sistema consta de dos maquinas, una es la estación de trabajo y la otra la pasarela o puerta de enlace a Tor. Whonix enruta todas sus comunicaciones por la red de Tor, evitando así que la estación de trabajo pueda comunicar por algún motivo por la Surface exponiendo así nuestra identidad. Es importante subrayar que, a causa errores del navegador, o enlaces a la internet superficial se han detectado a personas que realizaban acciones ilegales en esta Red.

Procederemos a ir a la pagina de descarga del proyecto Whonix [26] y en la sección de descarga Linux, en las siguientes capturas observamos el proceso:

Figura 47: Descarga de Whonix

Como podemos observar en la tercera imagen para Linux, Mac y Windows se aconseja la descarga de las dos maquinas para ser desplegadas como virtuales y procedemos a descargar la ova.

Figura 48: Fichero ova con las dos maquinas de Whonix

Procedemos a instalar VirtualBox en el sistema operativo que deseemos, ya que Whonix se ejecutara de igual forma en el sistema host que usemos. Procedemos a ejecutarlo y lo primero sería el cambio de las claves por defecto de las dos maquinas y seguidamente proceder a actualizar el sistema operativo y los navegadores a las ultimas versiones disponibles para garantizar más seguridad en nuestra navegación.

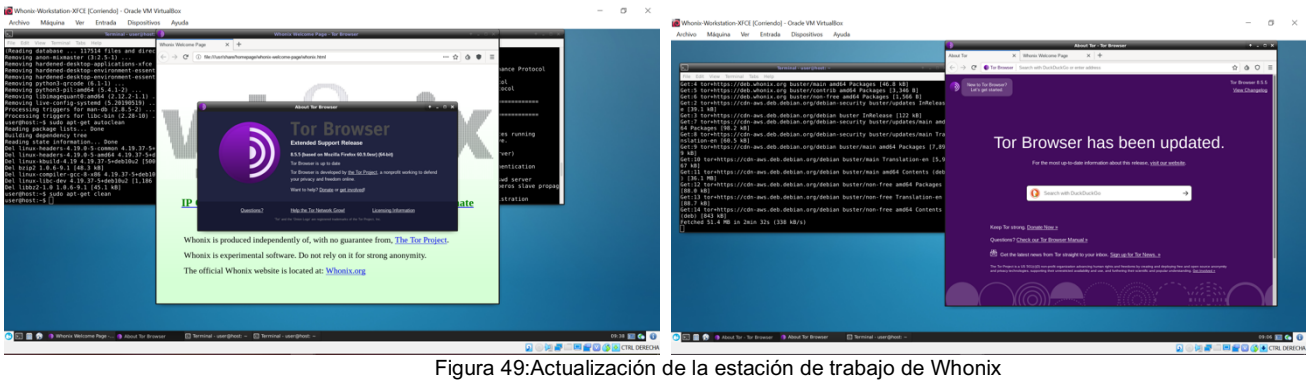


Figura 49:Actualización de la estación de trabajo de Whonix

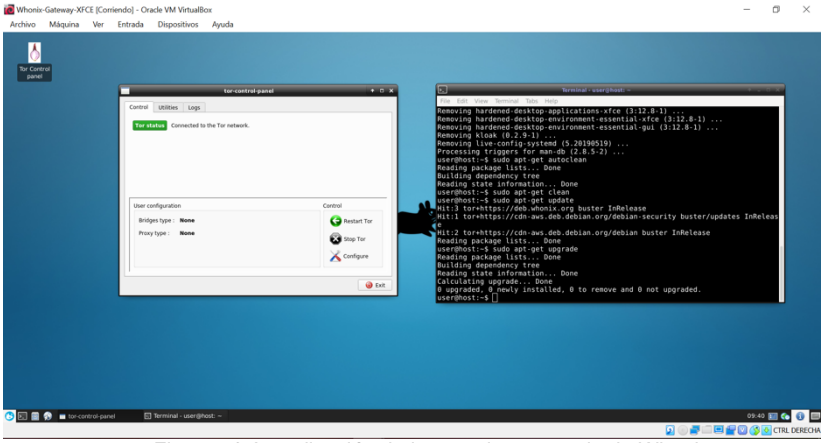


Figura 50:Actualización de la maquina pasarela de Whonix

Una vez realizado todas las actualizaciones ya nos encontramos navegando por la red de Tor. En la maquina pasarela mediante Tor Control Panel podemos conectar y desconectar de la red Tora si como obtener información de la conexión a la red Tor

En la estación de trabajo abriremos nuestro navegador Tor Browser y accederemos al buscador Duckduckgo por su URL onion https://3g2upl4pq6kufc4m.onion/ obteniendo el resultado siguiente:

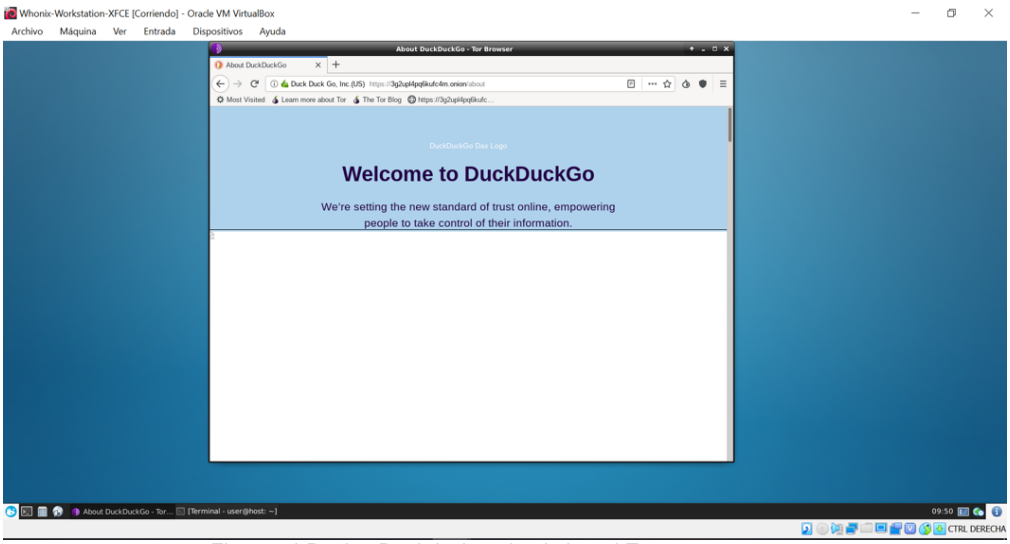


Figura 51:Pagina Duckduckgo desde la red Tor

3.3.2. Test navegación Tor.

Procederemos a navegar desde la estación de trabajo de Whonix, y como hemos comentado en apartados anteriores Tor es una red outproxy, por lo que al hacer búsquedas en el navegador Duckduckgo obtenemos enlaces de la Surface.

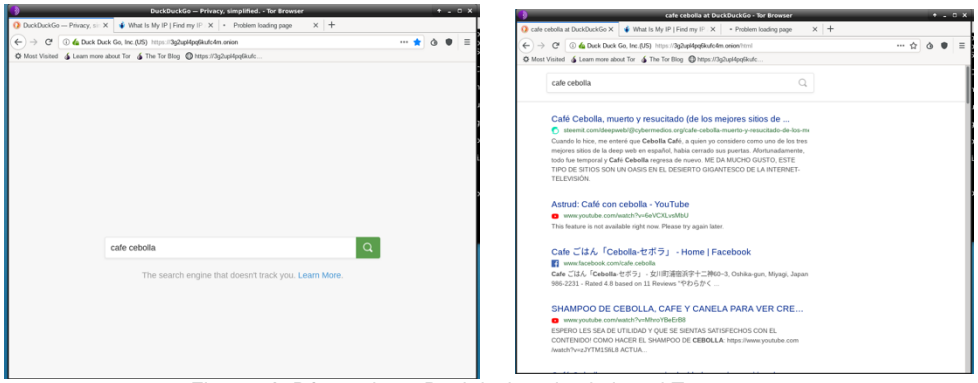


Figura 52: Búsqueda en Duckduckgo desde la red Tor

Desde la Surface podemos obtener paginas con direcciones onion que nos llevan a paginas dentro de la red de Tor, como por ejemplo http://hiddenwikitor.com/.

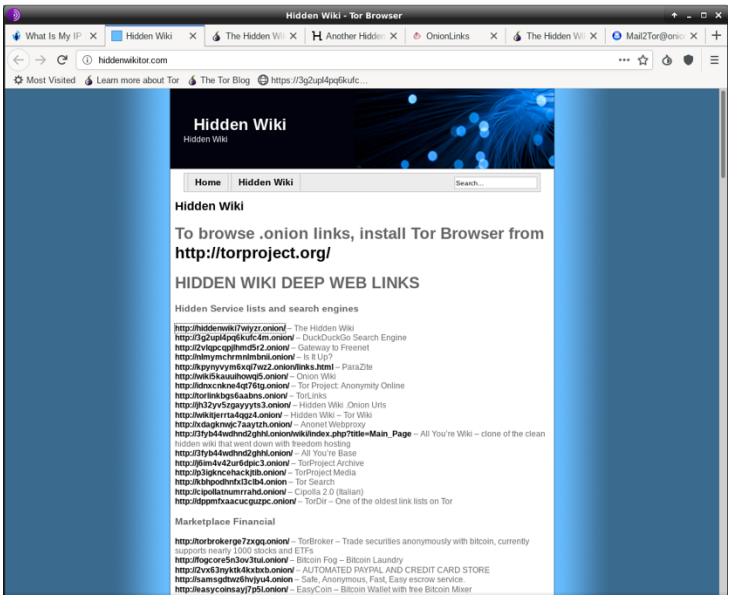


Figura 53: Enlaces onion para la red Tor desde la Surface

Accedemos a una de las paginas más conocidas de la red Tor y la cual nos proporcionara más enlaces de diferentes temáticas dentro de Tor: Hidden Wiki.

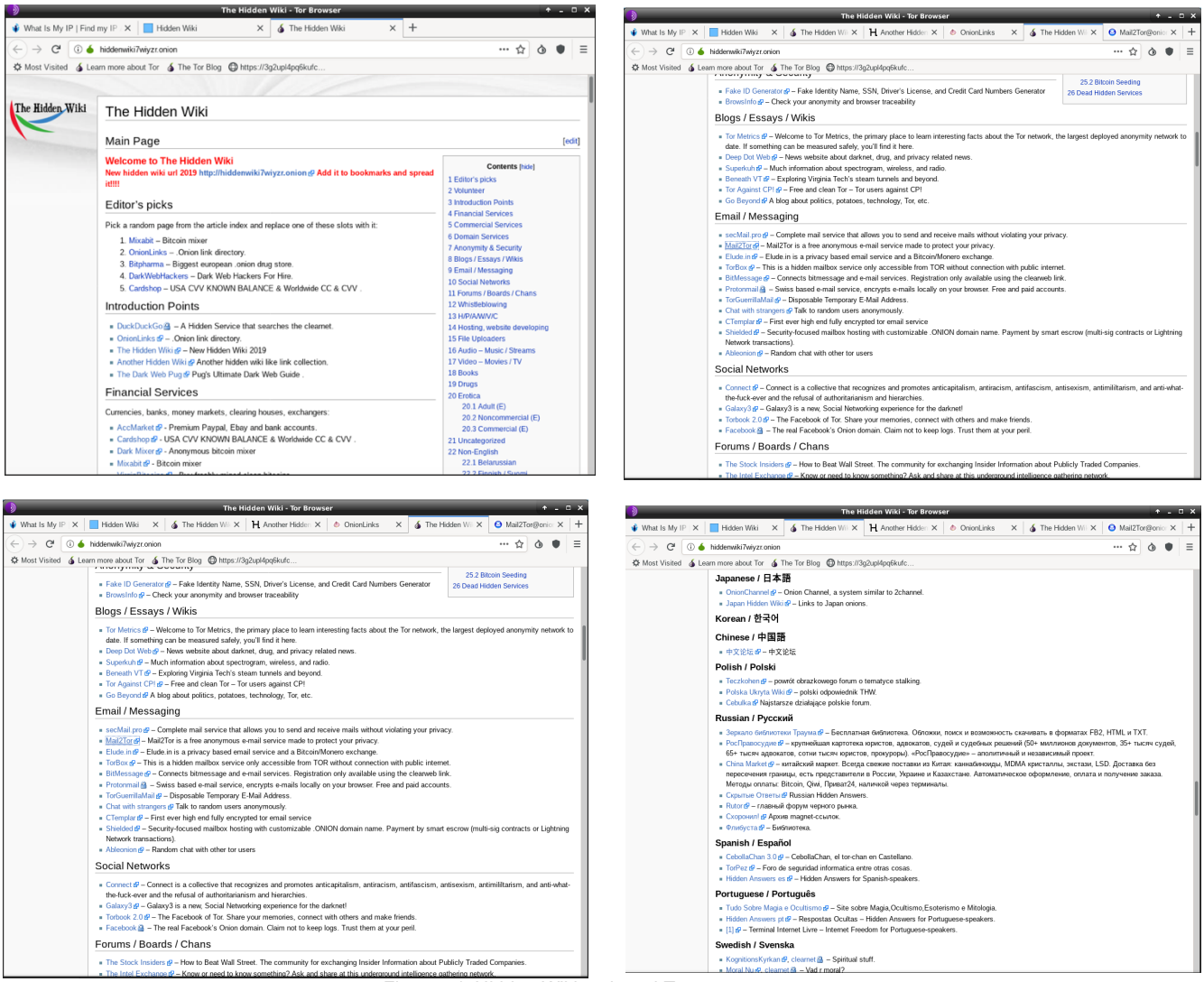


Figura 54: Hidden Wiki en la red Tor

Ahora accederemos a uno de los foros más populares en español de la res Tor. http://s6cco2jylmxqcdeh.onion/w/.

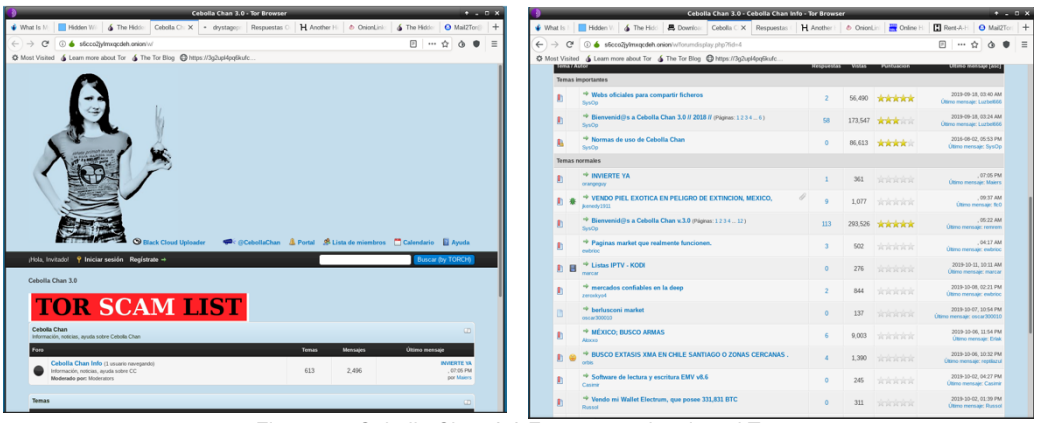
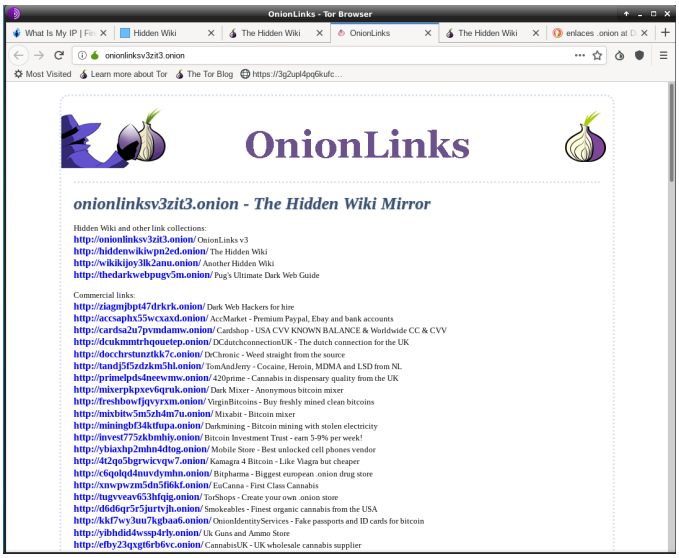


Figura 55: Cebolla Chan 3.0 Foro español en la red Tor.

Navegando por diferentes paginas, accedemos a índices propios de la red Tor con más enlaces de servicios ocultos que se ofrecen: http://wikikijoy3lk2anu.onion/



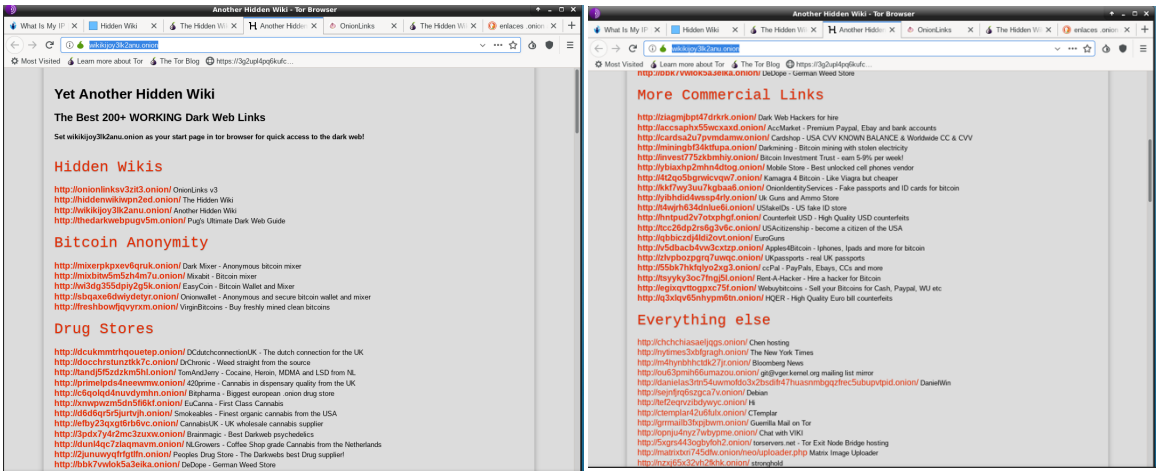


Figura 56: Enlaces a servicios dentro de la red Tor.

Hemos navegado por las paginas que son más conocidas en la Surface sobre Tor, en este caso es: Rent-A-Hacker (http://tsyyky3oc7fngj5l.onion/)

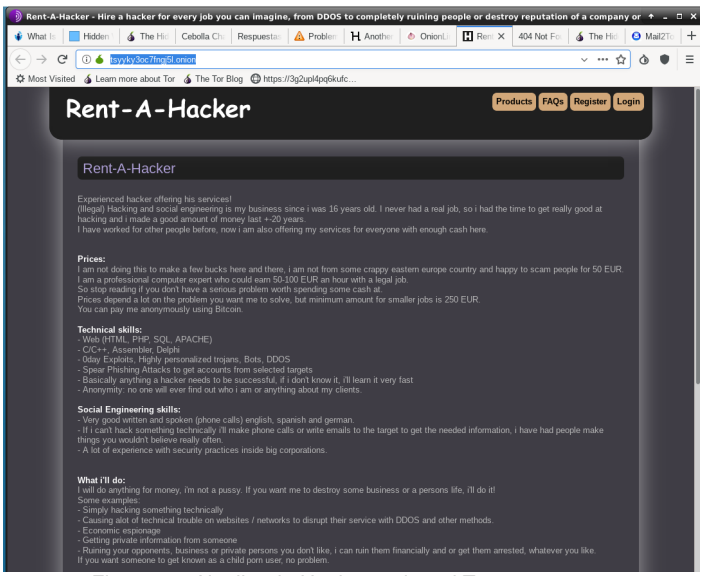


Figura 57: Alquiler de Hacker en la red Tor

Hemos encontrado alguna más sobre la temática anterior Dark Web Hacker (http://ziagmjbpt47drkrk.onion/)

Figura 58: Alquiler de Hacker en la red Tor

Siguiendo nuestro paseo hemos encontrado Mail2Tor para cuentas de correo anónimas (http://mail2tor2zyjdctd.onion/),

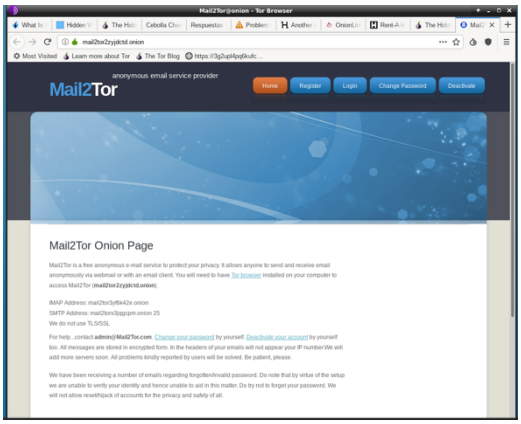


Figura 59: Cuentas de correo anónimo en la red Tor

Sobre correo hemos encontrado TorGuerrillaMail - Dirección de correo electrónico temporal desechable (http://grrmailb3fxpjbwm.onion/).

Figura 60: Cuentas de correo anónimo temporales la red Tor

Sobre Web de compra tipo EBay de la Surface hemos encontrado Tarjeta regalo de Amazon muy baratas, comercios con pago en Bitcoin. (http://escobaypw64njaqr.onion/ http://2mbag6csiomy2e7l.onion/ http://4mjc7ee6n6hcyspv.onion/).

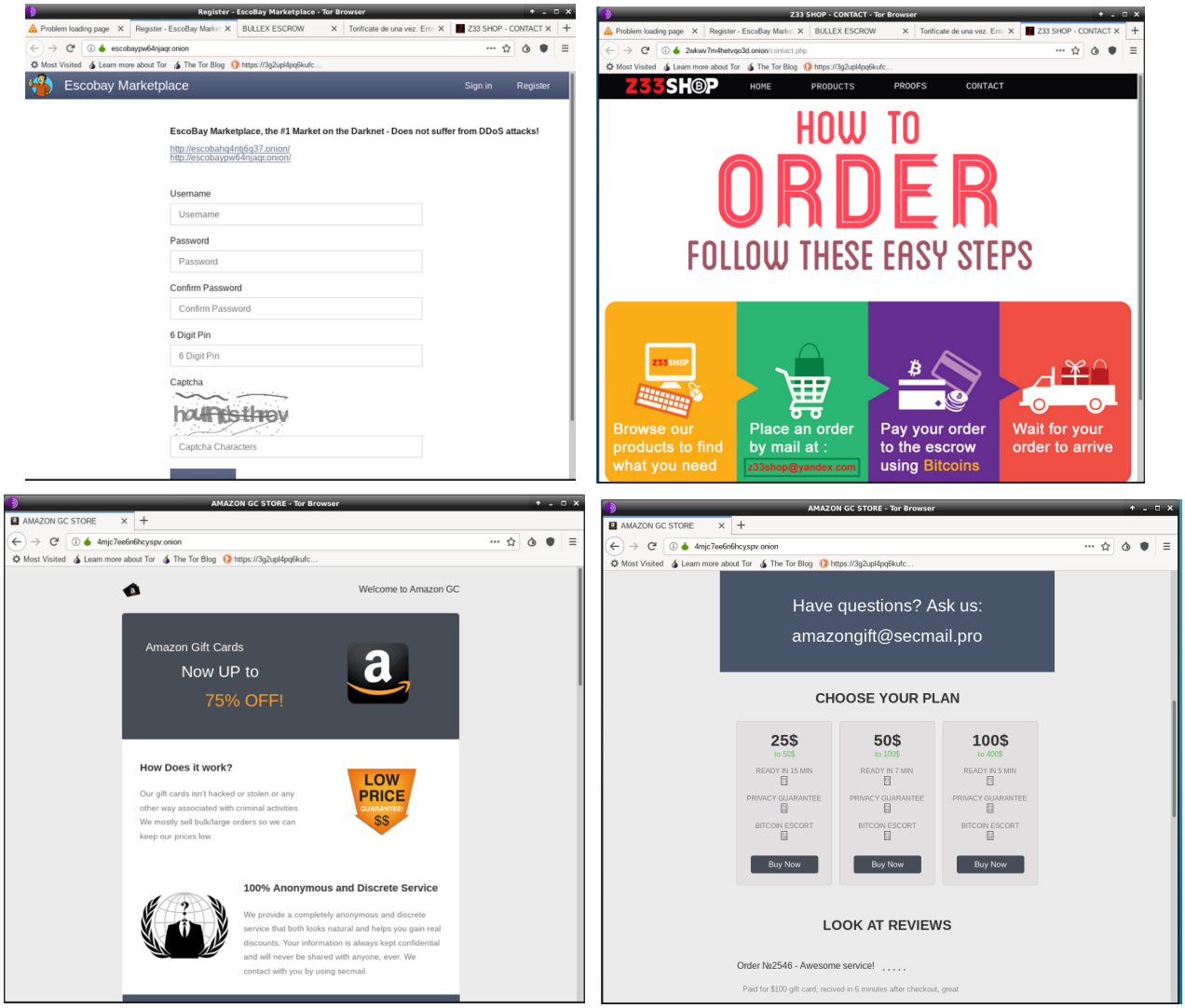


Figura 61: De compras por la red Tor

4. Implementación de un Nodo Tor.

Los nodos Tor pueden trabajar en diferentes plataformas de software y hardware. Por lo que el primer paso es la elección de donde se ejecutara el nodo. Nos hemos decidido por mini ordenador formado por una simple placa llamada Raspberry PI, el cual nos otorgara una gran versatilidad ya que nos ofrece un amplio abanico de posibilidades en proyectos tecnológico de diferente índole, así como la alta disponibilidad de funcionamiento que nos ofrece de 24 horas los siete días de la semana. Adjuntamos capturas del mini ordenador donde instalaremos y ejecutaremos nuestro nodo:

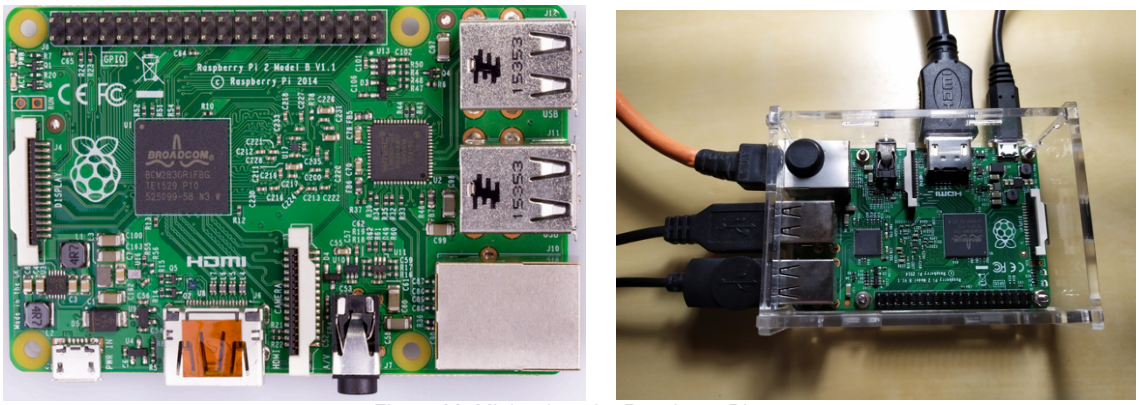


Figura 62: Mini ordenador Raspberry Pi

En el mercado existen dos modelos superiores Raspberry Pi 3 [27] y acaba de salir este año Raspberry PI 4.

4.1. Requisitos de instalación.

A continuación, exponemos las necesidades de software y hardware para desplegar nuestro nodo:

- Software

  El sistema operativo para Raspberry se llama Raspbian [28] y lo hemos descargado de su pagina Web oficial [29] y siendo este muy liviano, no requiriendo un rendimiento de procesamiento elevado. Existen varias distribuciones distintas para este hardware como Ubuntu MATE, Ubuntu Core, etc. pero hemos elegido Raspbian el cual es un sistema operativo GNU/LINUX libre basada en Debian y de código abierto que Raspberry Fundation la estableció como distribución oficial para sus mini ordenadores.

  Nos hemos descargado la versión: Raspbian Buster with desktop and recommended software.Hemos descargado un fichero zip con el cual al descomprimir se obtiene un fichero imagen (.img), el cual mediante el programa ApplePiiBaker (estamos usando un ordenador Mac de Apple para despegar la imagen en caso de hacerlo con Windows se puede usar el programa Win32DiskImager) grabamos la imagen en una tarjeta MicroSD de 16 Gb de capacidad y ya tendremos el sistema Raspbian listo para insertar en nuestra Raspberry. Adjuntamos imagen del proceso descrito:

Figura 63: Grabación Micro SD Raspbian.

- Hardware

  Exponemos las características del modelo que usaremos.

	Raspberry Pi 2 Model B
SoC	Broadcom BCM2836
CPU	ARM11 ARMv7 ARM Cortex-A7 4 núcleos @ 900 MHz
Overclocking	Sí, hasta arm_freq=1000 sdram_freq=500 core_freq=500 over_voltage=2 de forma segura
GPU	Broadcom VideoCore IV 250 MHz. OpenGL ES 2.0
RAM	1 GB LPDDR2 SDRAM 450 MHz
USB 2.0	4
Salidas de vídeo	HDMI 1.4 @ 1920x1200 píxeles
Almacenamiento	microSD
Ethernet	Sí, 10/100 Mbps
Tamaño	85,60x56,5 mm
Peso	45 g
Consumo	5v, 900mA, aunque depende de la carga de trabajo de los 4 cores
Precio	35 euros

Tabla 2: Características Hardware Raspberry Pi 2.

- Otros requisitos

  Tendremos que disponer de un monitor con entrada HDMI, teclado y ratón, para proceder a realizar la configuración del sistema operativo de nuestro nodo.

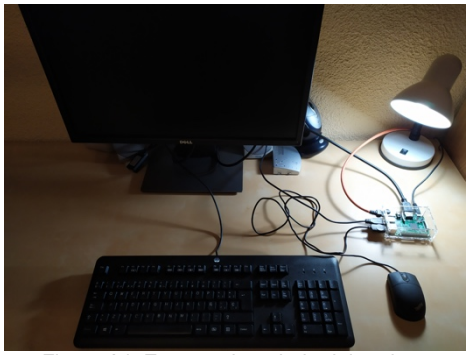


Figura 64: Entorno de trabajo del nodo.

4.2.Instrucciones de instalación.

Procederemos a encender nuestro nodo y el asistente de instalación nos ira solicitando información como el lenguaje del sistema operativo, ubicación, etc., al finalizar obtendremos la pantalla principal del sistema Raspbian, adjuntamos captura:

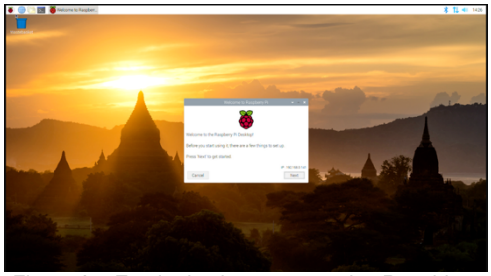


Figura 65: Escritorio sistema operativo Raspbian,

Seguidamente configuraremos todos los parámetros en el siguiente orden:

- Configuraremos una IP fija dentro de nuestra red interna de nuestro router.
  En nuestro caso 192.168.200.200/24 con puerta de enlace 192.168.200.254
  En las ultimas versiones de Raspbian la modificación de la dirección IP o se realiza mediante el entrono grafico, o mediante el nuevo fichero de configuración /etc/dhcpcd.conf [30]:

Figura 66: Fichero configuración IP Raspbian Buster,

- Procederemos a configurar el acceso SSH [31] en el sistema operativo para tener acceso remoto a nuestro nodo sin necesidad de usar el teclado, ratón y pantalla conectado al mini ordenador Raspberry. Como medida de seguridad hemos modificado el puerto de conexión del servicio SSH que es el 22 por el 1971. Ahora podremos conectarnos a nuestro nodo desde un ordenado externo dentro de nuestra red interna no dando acceso a configurarlo desde internet, en nuestro caso usaremos un Mac de Apple y mediante este comando: ***ssh -p 1971 pi@192.168.200.200*** En la imagen adjunta vemos el cambio.

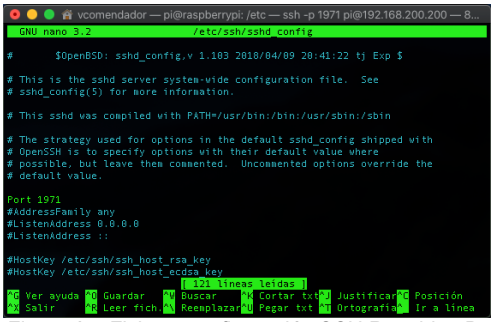


Figura 67: Fichero configuración SSH Raspbian Buster,

- Ahora actualizaremos nuestro sistema operativo mediante los comandos:

  sudo apt-get update: Actualizara las versiones y la lista de paquetes.

  sudo apt-get upgrade: una vez descargada la lista anterior se actualizarán todos los paquetes cuando ejecutamos este comando

- En este paso instalaremos del servicio Tor en la Raspberry con el siguiente comando:

  sudo apt-get install tor: instalamos Tor ya que buscamos los paquetes en los repositorios.

  Una vez finalizada la instalación de los paquetes de Tor, ya disponemos de todos los archivos necesarios para poder comenzar a configurar nuestro nodo Tor. Ahora procedernos a localizar los archivos para configurar nuestro nodo, estos se encuentran en /etc/tor/, adjuntamos captura:

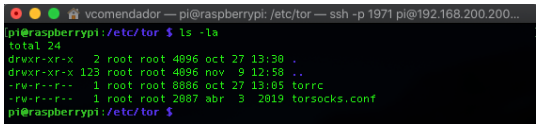


Figura 68: Ubicación ficheros configuración del nodo Tor,

El nodo/relay que vamos a configurar será de tipo nodo **intermedio o Middle Relay.**

Editaremos el fichero de configuración torrc con el comando:

sudo nano /etc/tor/torrc: Con el editor nano (o cualquier editor de Linux como vi) procreemos a ir modificando las distintas variables que necesitamos para poder poner en funcionamiento nuestro relay/nodo de la Red Tor.

Vamos a enumerar y modificar las variables necesarias del fichero torrc [32]:

SocksPort

Tor abre un proxy en el puerto '9050' por defecto, como nosotros vamos a usarlo como un relay y no para establecer conexiones locales, pondremos este valor a cero, El valor será: ***SocksPort*** 0:

Log notice file

Con este parámetro incidamos la ruta donde se encuentra el documento que realiza las labores de registro (LOG), que por defecto es /var/log/tor/notices.log y que en el se almacenaran todos los cambios que sucedan en nuestro relay/nodo. El valor será:

Log notice file /var/log/tor/notices.log

RunAsDaemon

Con este comando el proceso de Tor se auto-arranca en segundo plano. El valor será:

RunAsDaemon 1

ControlPort

Es el puerto en el que Tor escuchará conexiones locales y lo utilizaremos para la monitorización del nodo. Tor aceptará conexiones en este puerto y permitirá que esas conexiones controlen el proceso Tor usando el Protocolo de Control Tor. El valor será:
ControlPort 9051

ORPort

Es el puerto que se anunciará a las conexiones de Tor entrantes. El valor será:

ORPort 9001

ExitPolicy

Esta modificación es importante, ya que con ella indicamos que no queremos ser un Exit Relay, este tipo de nodo puede comprometer nuestras seguridad y vulnerabilidad. El valor será:

ExitPolicy reject *:*

DirPort

Indicamos el puerto destinado al servicio de directorio. El valor será:

DirPort 9030

Nickname

En esta variable pondremos el nombre de nuestro nodo nombre, el cual se verá en la red Tor. El valor será:

Nickname TFMUOC2019

Importante tener en cuenta el formato del nombre ya que no acepta caracteres especiales como guiones, inicialmente pusimos como nombre TFM-UOC y Tor no arrancaba, para detectar el fallo usamos el comando ***cat /var/log/syslog | grep tor -i***, el cual nos indicó que el nombre no era correcto, se adjunta captura:

Figura 69: Log de error de configuración de Tor,

RelayBandwidthRate

Ahora indicaremos el ancho de banda que daremos a nuestro nodo. El valor será:

RelayBandwidthRate 10MB

RelayBandwidthBurst

Aquí daremos el valor máximo por ráfaga que permitimos a nuestro nodo. El valor será:

RelayBandwidthBurst 20MB:

Adjuntamos captura de parte del fichero torrc ya configurado:

Figura 70: Edición del fichero torrc,

- Ahora procederemos a reiniciar el proceso de Tor. Se puede parar y arrancar de nuevo o reiniciarlo con los siguientes comandos:

  sudo service tor restart

  O también:

  sudo service tor stop

  sudo service tor start

  Para verificar si el nodo esta funcionado miraremos en los ficheros LOG que se irán generando. El valor será:

  cat /var/log/tor/log

  Y estudiando este fichero sabremos si nuestro nodo esta funcionando de forma correcta.

- Hemos instalado en nuestra Raspberry Pi el paquete tcpdump [33] que nos dará la posibilidad de caturra el trafico que se origina en nuestro nodo/relay, para luego poderlo analizar de forma precisa. El valor será:

  sudo tcpdump -i eth0 -w /InicioRelay.pcap &

  Con & podremos salir con control “C” y la captura seguirá en segundo plano, para volver a ella usaremos el comando ***fg.***

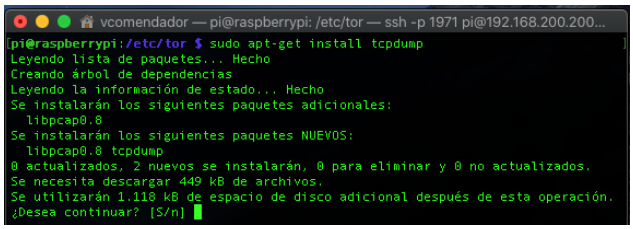


Figura 71: Instalación tcpdump,

5. Demostración de operatividad

5.1. Inicio de nuestro Nodo Tor.

En el capitulo anterior hemos realizado toda la instancian y configuración necesaria para poder poner operativo nuestro nodo. Procedernos en este capitulo a describir su puesta en marcha y verificación del correcto funcionamiento del mismo.

Comprobaremos y detendremos el servicio de Tor con los siguientes comandos:

sudo service tor status

sudo service tor stop

Ejecutaremos el comando para capturar el trafico que generara nuestro nodo al iniciarse:

sudo tcpdump -i eth0 -w /InicioRelay.pcap &

Crt + C para liberar la consola (en caso de querer volver usaremos fg).

Indicamos el servicio de Tor:

sudo service tor start

Con los siguientes comandos verificamos los ficheros Log que genera nuestro nodo, y podemos verificar su correcto funcionamiento.

cat /var/log/tor/notices.log

tail -f /var/log/tor/notices.log

Con las siguientes capturas vemos que tenemos nuestro nodo operativo en la red de Tor:

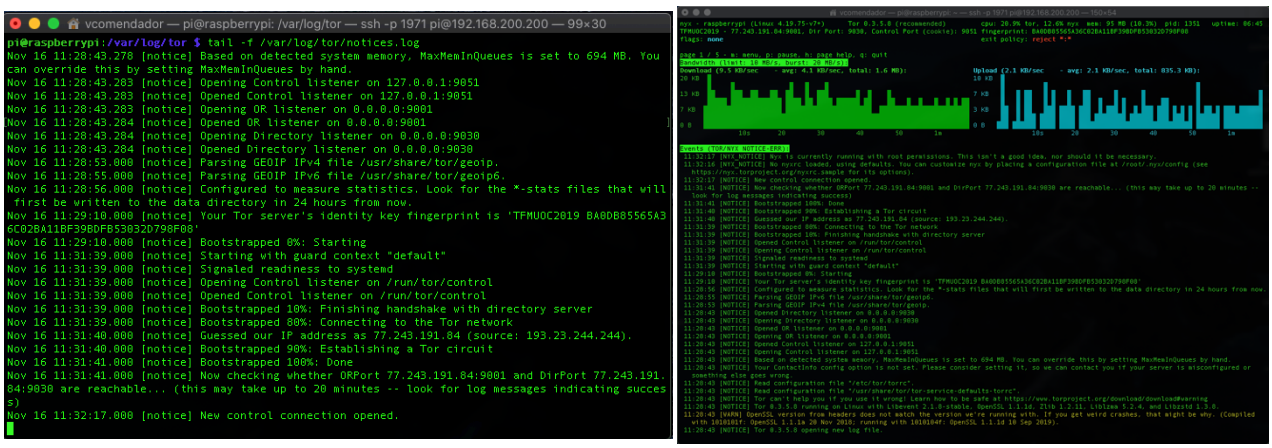


Figura 72: Log de Tor y captura de Nyx,

Ahora tendremos que dejar nuestro nodo operativo para que se integre en la red de nodos de Tor.

5.2.Herramienta de Monitorización.

Para la monitorización de nuestro nodo en tiempo real, vamos a usar la aplicación Nyx, que es la evolución de la aplicación que se usaba antes llamada Arm.

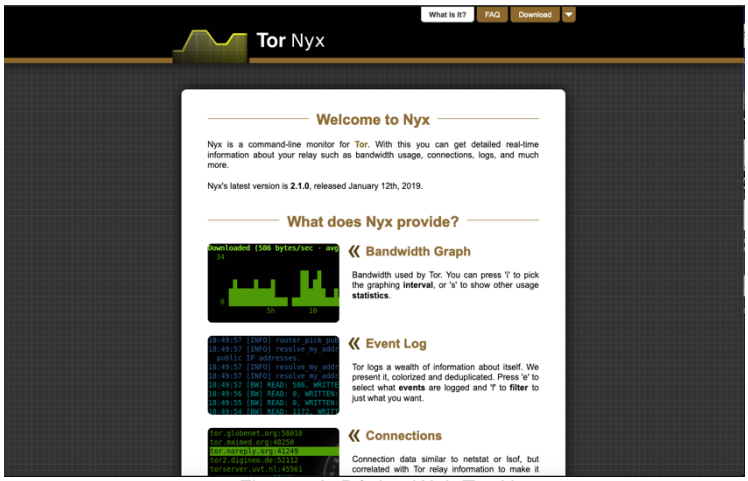


Figura 73: Página Web Tor Nyx,

Precedemos a instalarlo con el siguiente comando:
sudo apt-get install nyx
y lo ejecutaremos con:
sudo nyx
Si Tor no se encuentra en ejecución en el nodo/relay y Nyx no puede conectar con los procesos de Tor, nos mostrara el siguiente mensaje:
Unable to connect to tor. Are you sure it's running?
En caso de conexión con Tor se nos mostrara el aplicativo. Seguidamente describiremos las diferentes pantallas que nos ofrece este software:

5.2.1. Funcionamiento de la herramienta Nyx.

Mediante Nyx podremos monitorizar el estado de nuestro nodo/relay, ya que nos dará estadísticas del comportamiento del nodo en tiempo real como:

- Consumo de CPU, consumo de memoria Ram. Pid de l proceso de Tor, tiempo de operatividad del nodo, etc.
- Conexiones establecidas.
- Información relativa a la configuración de nuestro nodo.
- Configuración del fichero torrc

Seguidamente describiremos las diferentes pantallas de información que nos ofrece Nyx para la monitorización del estado de nuestro nodo.

- Pantalla 1

  Como podemos observar en la parte superior se nos muestra toda la información genérica y esta se replicara en todas las demás pantallas del aplicativo la cual muestra: sistema operativo, versión de Tor, los diferentes puertos que el servicio de Tor, carga de CPU, RAM y PID, tiempo de funcionamiento de nuestro nodo, así como los distintos flags que puede tener activado nuestro nodo, en la captura no tenemos ninguno activado ya que esta en le proceso de conexión y validación, mostraremos ahora el significado de los posibles flags [35] que puede tener un nodo:

  BadExit: Este nodo rompe cosas, ya sea de forma maliciosa o por una configuración incorrecta.

  Fast: Este nodo tiene mucho ancho de banda disponible.

  Guard: Este nodo es adecuado para ser el primer salto (nodo de entrada) en un circuito Tor.

  HSDir: Este nodo es un directorio de servicio oculto v2.

  Named: Este nodo tiene un apodo.

  Running: Este nodo ha estado en línea en los últimos 45 minutos.

  Stable: Este nodo se considera estable.

  V2Dir: Este nodo admite el protocolo de directorio v2.

  Valid: Está ejecutando una versión de Tor correcta y la autoridad del directorio no lo ha incluido en la lista negra como sospechoso.

  Unnamed: El apodo configurado de este nodo es utilizado por otro.

  Exit: Este nodo está configurado para ser el último salto (nodo de salida) en un circuito Tor.

  Authority: En nodo es un directory authority.

  Seguidamente veremos unas graficas de trafico de bajada y subida y por tanto, del trafico que esta gestionando nuestro nodo, también nos indicará la forma de transmisión de datos, si es continua o a intervalos de tiempo, si estamos conectados a la red y transmitimos trafico o estamos fuera de la misma. En la siguiente zona nos muestra el log en tiempo real de todo lo que esta sucediendo en nuestro nodo.

Figura 74: Nyx Pantalla 1,

- Pantalla 2

  En esta pantalla observaremos todas las conexiones que maneja nuestro nodo como: conexiones entrantes y salientes con sus respectivas direcciones IP y puertos y los circuitos Tor con sus tres saltos desde el origen al destino en donde actúa nuestro nodo. Podemos ver que en cada fila tenemos la dirección IP pública del nodo al que nos conectamos en el circuito, las direcciones IP de nuestro propio nodo, la huella única, como se llama ese nodo, que va a continuación en la conexión, el tiempo que encontramos activa la conexión y para finalizar que tipo de comunicación se realiza.

  - Inbound: Conexiones entrantes en nuestro nodo.
  - Outbound: Conexiones salientes de nuestro nodo.
  - Circuit: Recabar información sobre el estado de la red, sobrecarga, etc.

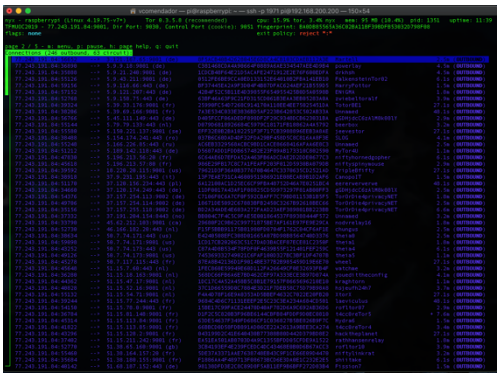


Figura 75: Nyx Pantalla 2.

- Pantalla 3

  Aquí podemos observar como la parametrización de nuestro nodo y analizar si podemos realizar algún cambio para aumentar o mejorar su rendimiento dentro de la red.

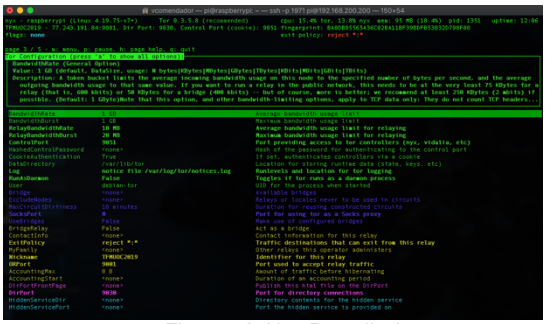


Figura 76: Nyx Pantalla 3.

- Pantalla 4

  Podemos ver en esta pantalla el fichero torrc de igual forma que si usamos nano en la consola de comandos y podemos usarlos para verificar que parámetros teníamos configurados sin salir de Nyx.

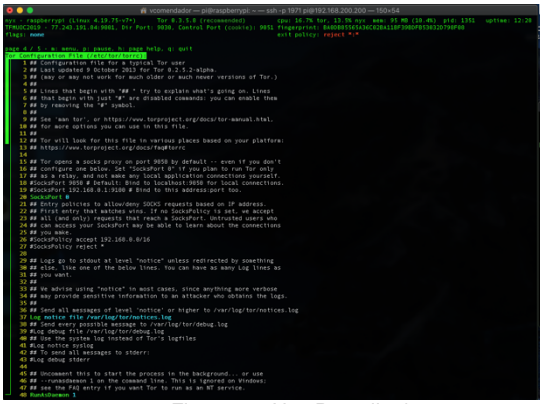


Figura 77: Nyx Pantalla 4.

- Pantalla 5

  En esta ultima pantalla obtenemos una Shell o intérprete de comandos para enviar ordenes a nuestro servicio de Tor usando Nyx. Si introducimos el comando ***/help*** nos mostrara las diferentes instrucciones que podemos utilizar. En la captura siguiente observaremos lo comentado en las líneas anteriores.

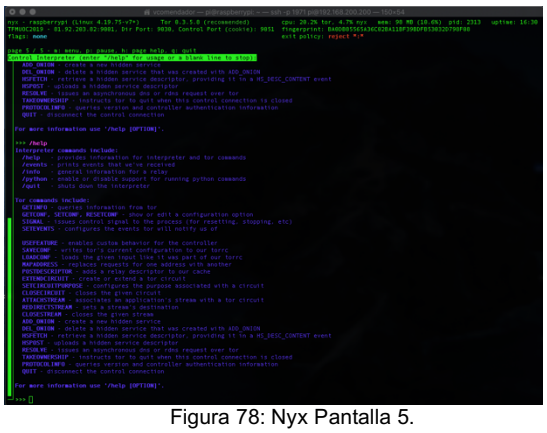


Figura 78: Nyx Pantalla 5.

5.3.Test de funcionamiento.

Para la verificación del funcionamiento de nuestro nodo hemos seguido las indicaciones que nos da Tor Project como buenas practicas [36].

- Primer paso:
  Verificamos que los puertos que hemos seleccionado en torrc como ORPort, y DirPort son accesibles y están habilitados. Para conseguir este punto hemos tenido que modificar la configuración de nuestro router, Port Forwarding (asignación de puertos para transmitir información a través de una red. El protocolo TCP/IP se encarga de transmitir paquetes entre servidores externos e internos de una red particular) para permitir la comunicación entre la red Tor y nuestro nodo por los puertos específicos. La Captura siguiente muestra es configuración:

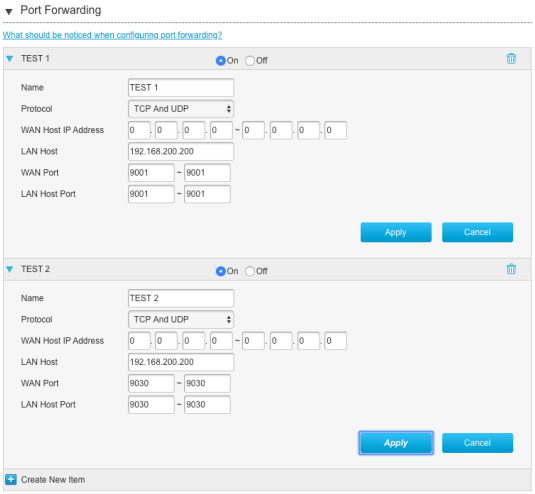


Figura 79: Configuración puertos en nuestro router.

- Segundo paso:
  Verificamos que nuestro nodo este operativo y trabajando correctamente. Para ello usaremos los diferentes archivos de log que nos proporciona el servicio Tor, los cuales suelen ser dos posibles ficheros, los cuales indicamos a continuación:
  /var/log/tor/notices.log
  /var/log/syslog
  Y mediante las instrucciones siguientes podemos estudiar su contenido:
  cat /var/log/tor/notices.log
  tail -f /var/log/tor/notices.log
  cat /var/log/syslog | grep tor -i
  En pasos sucesivos utilizaremos estos comandos para verificar que el nodo esta funcionando correctamente.

- Tercer Paso:

  En este punto ya tendríamos nuestro nodo operativo y con un funcionamiento correcto, Ahora tenemos que esperar a las diferentes fases [37] que la red Tor somonte a los nodos/relays. Las fases son cuatro. Las describiremos:

  - **Fase primera dura del día 0 al 3:**

    Al iniciar por primera vez un nodo, este realiza un test de ancho de banda creando cuatro circuitos que retornan y envía 125Kb por cada uno, empezando así la medicación del ancho de banda. Usando la formula 4x(tráfico envido por el relé) / 10 = X Kbyte por segundo.

    Una vez que se ha superado este proceso las autoridades de directorio y dependiendo de nuestro ancho se usara más o meno nuestro nodo.

  - **Fase segunda dura del día 3 al 8:**

    Ahora entramos en un periodo de confianza dentro de la red por tiempo de funcionamiento y estabilidad del nodo y se nos darán diferentes circuitos para que vallamos cogiendo peso dentro de los nodos de confianza. De todas formas, en los primeros momentos siempre seremos un nodo intermedio para evitar ataques a la red Tor.

  - **Fase tercera dura del día 8 al 68:**

    En esta fase serán las autoridades de directorio son las que otorgan los flags a los nodos/relays. En el apartado 5.2.1 describimos los diferentes flag que puede obtener un nodo y para ir obteniéndolos se considera:

    1. Ancho de banda.
    2. Tiempo de actividad ponderado.
    3. Tiempo conocido.

    Ya formamos parte de la red de Tor.

  - **Fase cuarta más de 68 días:**

    Esta fase es en la que el nodo pertenece a la red al terminar su periodo de cíclico completo en la red Tor.

- Cuarto paso:

  Ahora mostraremos los diferentes estadios que ha sufrido nuestro nodo:

  Arrancamos el proceso y obtenemos las siguientes capturas del Log de servicio de Tor y del software de monitorización:

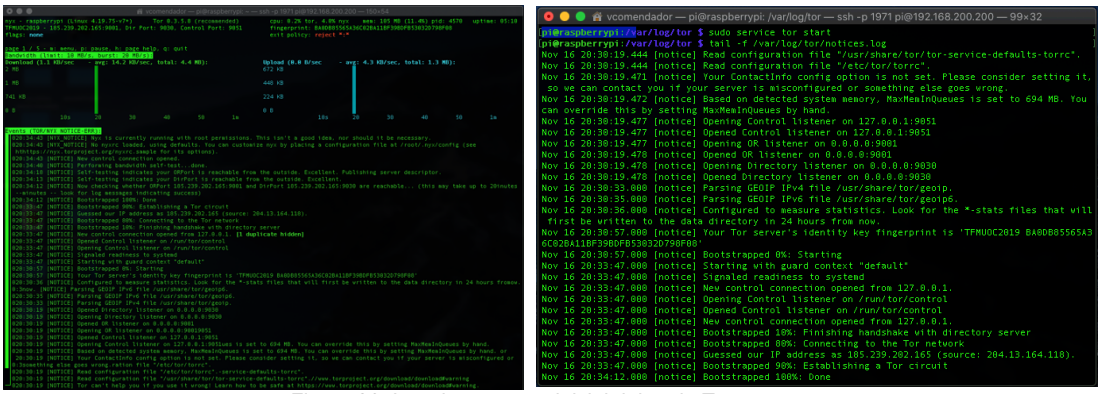


Figura 80: Log de arranque inicial del nodo Tor.

En el Log de Tor se nos indica los siguiente:

Nov 16 20:34:13.000 [notice] Self-testing indicates your DirPort is reachable from the outside. Excellent.

Nov 16 20:34:18.000 [notice] Self-testing indicates your ORPort is reachable from the outside. Excellent. Publishing server descriptor.

Esto significa que el primer paso que indicamos en este apartado lo hemos realizado correctamente.

Ahora se ha producido el estudio del ancho de banda de nuestro nodo y se ha concluido:

Nov 16 20:34:40.000 [notice] Performing bandwidth self-test...done.

Primeros intercambios de tramas de nuestro nodo en la red Tor:

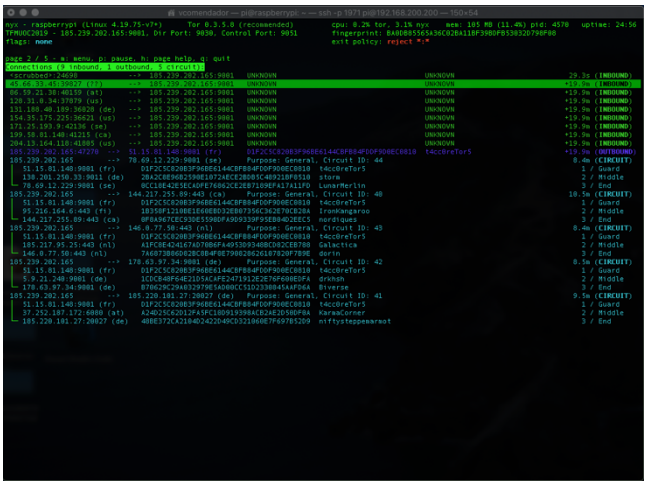


Figura 81: Primeras Tramas intercambiadas por el nodo Tor

Legado este punto tenemos que dejar que la red Tor pase nuestro nodo por las distintas fases antes expuestas.

A la hora y media de estar operativo el nodo y utilizando el software de monitorización Nyx, vemos que la red Tor ya ha otorgado a nuestro nodo varios Flags, los cuales son:

Running: Este nodo ha estado en línea en los últimos 45 minutos.

V2Dir: Este nodo admite el protocolo de directorio v2.

Valid: Está ejecutando una versión de Tor correcta y la autoridad del directorio no lo ha incluido en la lista negra como sospechoso.

Ahora adjuntamos capturas del software de monitorización, donde podemos observar los Flags antes mencionados y las conexiones en ese momento.

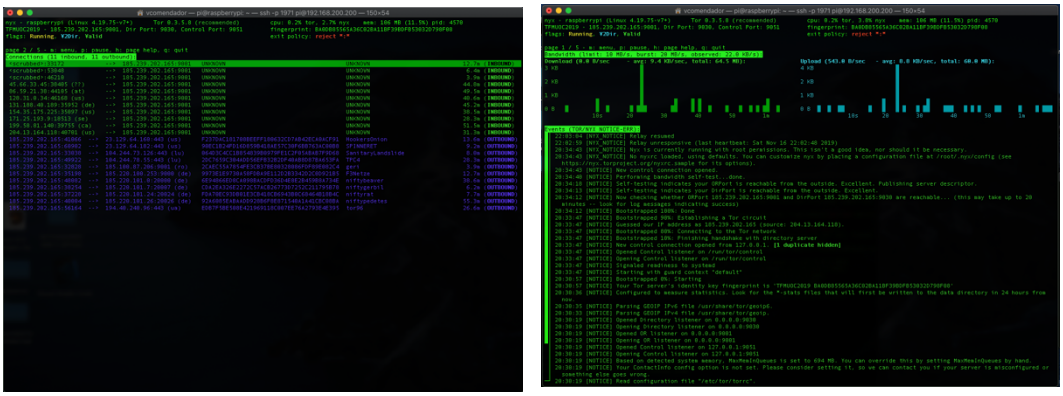


Figura 82: Flags obtenidos por el nodo Tor de la Red.

Utilizando Tor Metrics [38] hemos obtenido la información de nuestro nodo una vez indexado en la Red Tor, adjuntamos captura, donde se puede ver el nombre, dirección IP, no es nodo de salid, operador del internet (ISP), el país, la huella de nuestro nodo, la plataforma en la que corre Tor:

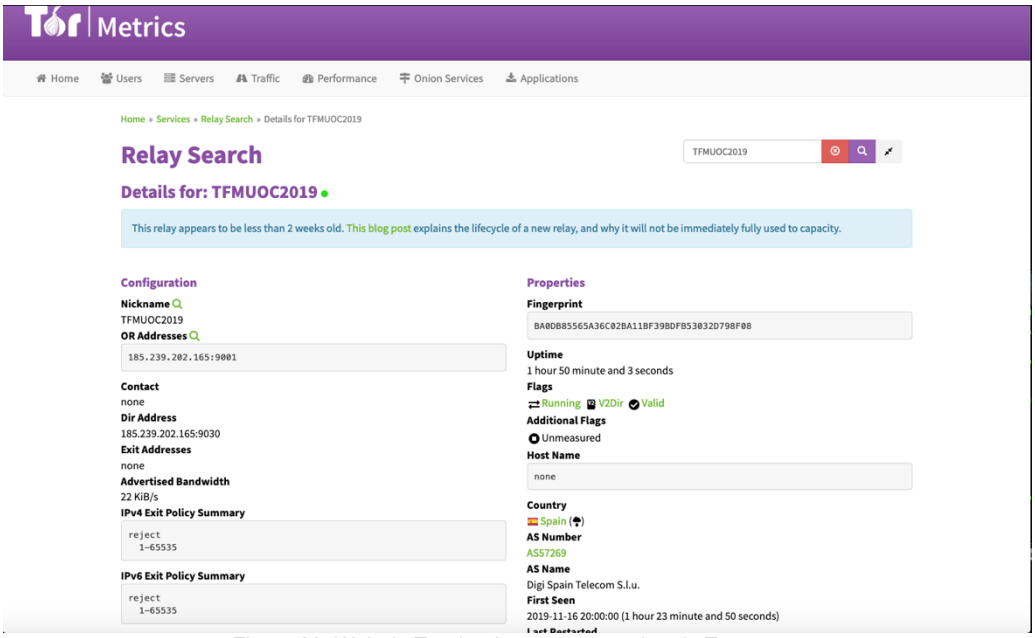


Figura 83: Web de Tor donde se muestra el nodo Tor.

Nuestro nodo ya se encuentra operativo en la Red de Tor y ahora vamos a darle más horas de funcionamiento para poder obtener mejor monitorización y estadísticas.

En el arranque de nuestro nodo hemos realizado una captura de trafico con ***tcpdump*** y hemos procedido analizarla con WireShark y hemos observado que nuestro nodo en su inicio contacta con varios nodos con el Flag de autoridad del directorio, adjuntamos captura de pantalla:

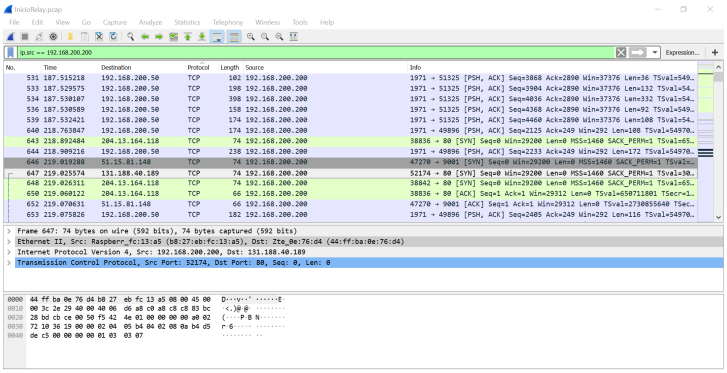


Figura 84: Captura de trafico al inicio del nodo Tor.

Analizando la captura y usando la pagina Web de Tor Metrics [38], vemos que nuestro nodo contacta con gabelmoo y bastet los cuales son autoridades de directorios ya que en estos últimos se encuentra información del estrado de la red y el estado de todos los nodos/relays, posteriormente se contacta también con tor26 y dizum que también son autoridades de directorios, adjuntamos captura de la ficha de estos nodos:

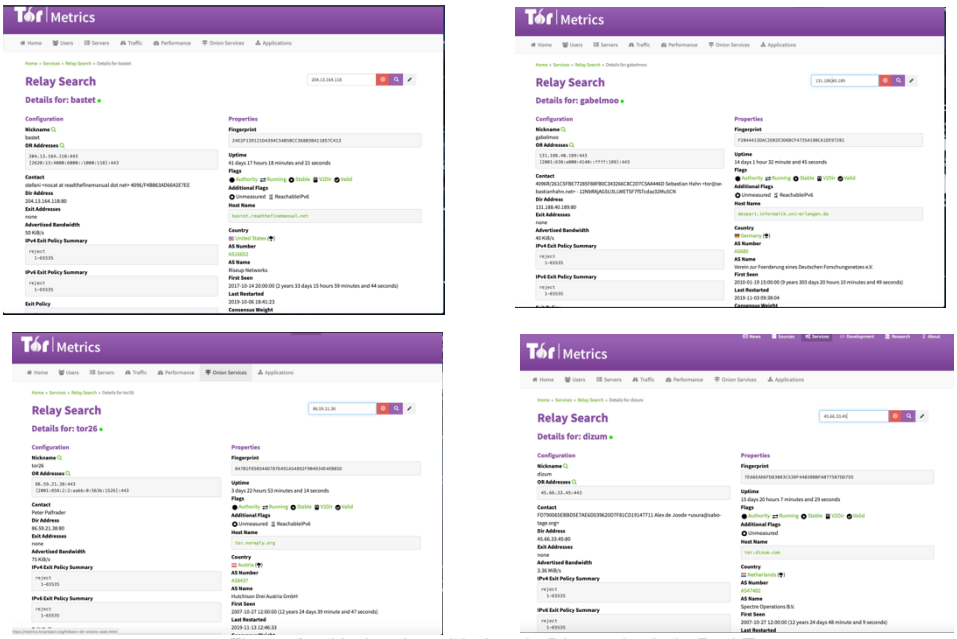


Figura 85: Nodos Autoridades de Directorio de la Red Tor.

Seguidamente se procede a contactar con otros nodos de la Red, en nuestro caso han sido t4cc0reTor5 51.15.81.148, tiflin 163.172.21.117.

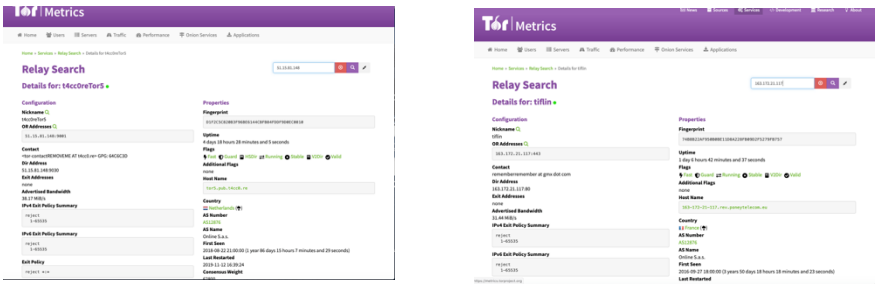


Figura 86: Nodos de Entrada de la Red Tor.

También hemos obtenido el nodo de salida que se nos asigno en los primeros momentos, el cual es freki 185.100.87.207, adjuntamos sus propiedades:

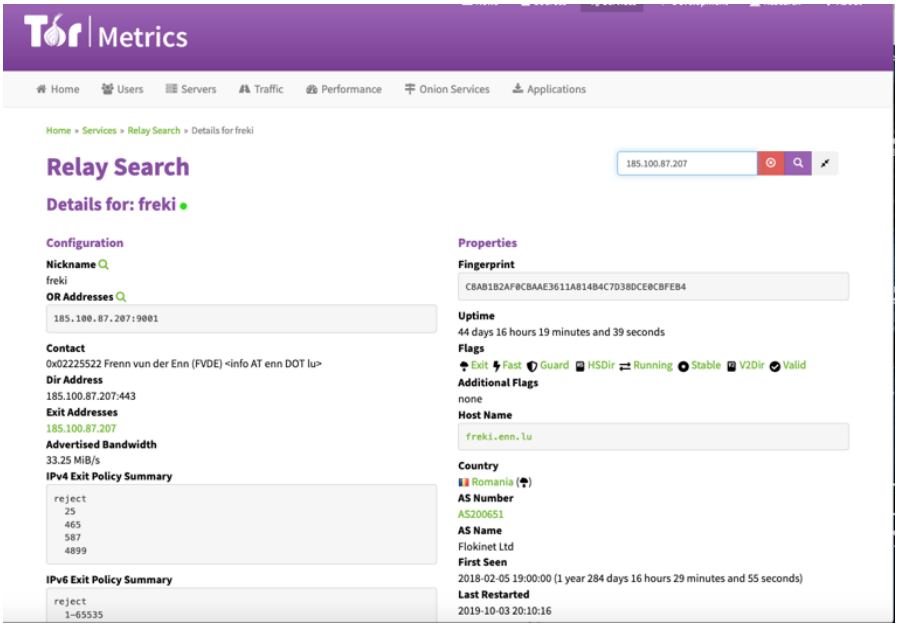


Figura 87: Nodos de Salida de la Red Tor.

También hemos establecido comunicación con nodos de servicio oculto como Donatello 190.10.8.166, sus propiedades son:

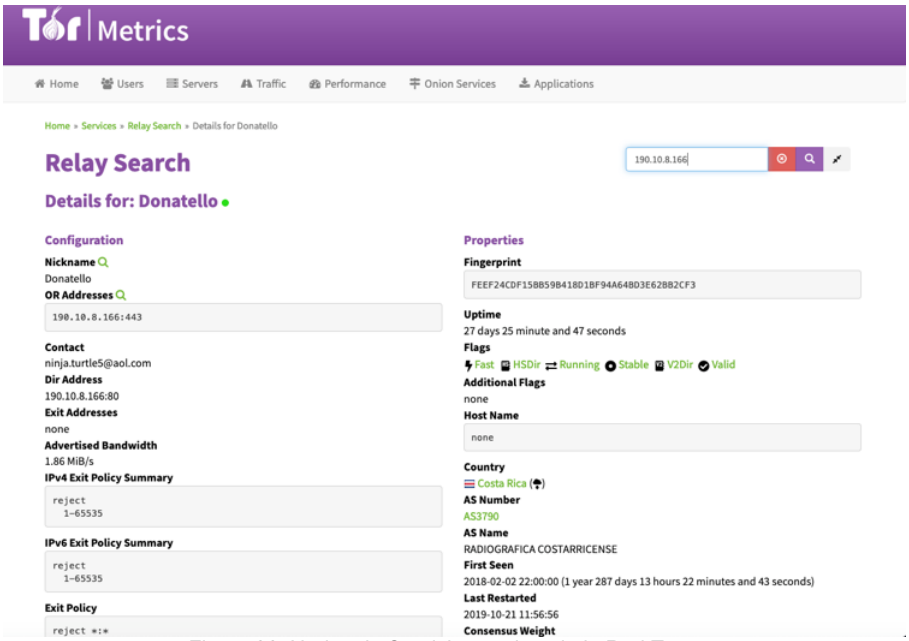


Figura 88: Nodos de Servicios ocultos de la Red Tor.

5.4.Monitorización y estadísticas.

Para la monitorización de nuestro nodo/relay vamos a usar la herramienta mencionada en el apartado 5.2 de este capitulo Nyx y la realizaremos en tiempo real y además usaremos las estadísticas que nos ofrece la aplicación de Tor en sus Log.

Fase primera de 0-3 días:

Tras 24 horas de funcionamiento de nuestro nodo hemos obtenido las primeras estadísticas:

Nov 17 20:33:47.000 [notice] Heartbeat: Tor's uptime is 1 day 0:00 hours, with 1 circuits open. I've sent 434.26 MB and received 432.37 MB.

Adjuntamos captura de los Logs y del Nyx mostarndo las conexiones con otros nodos:

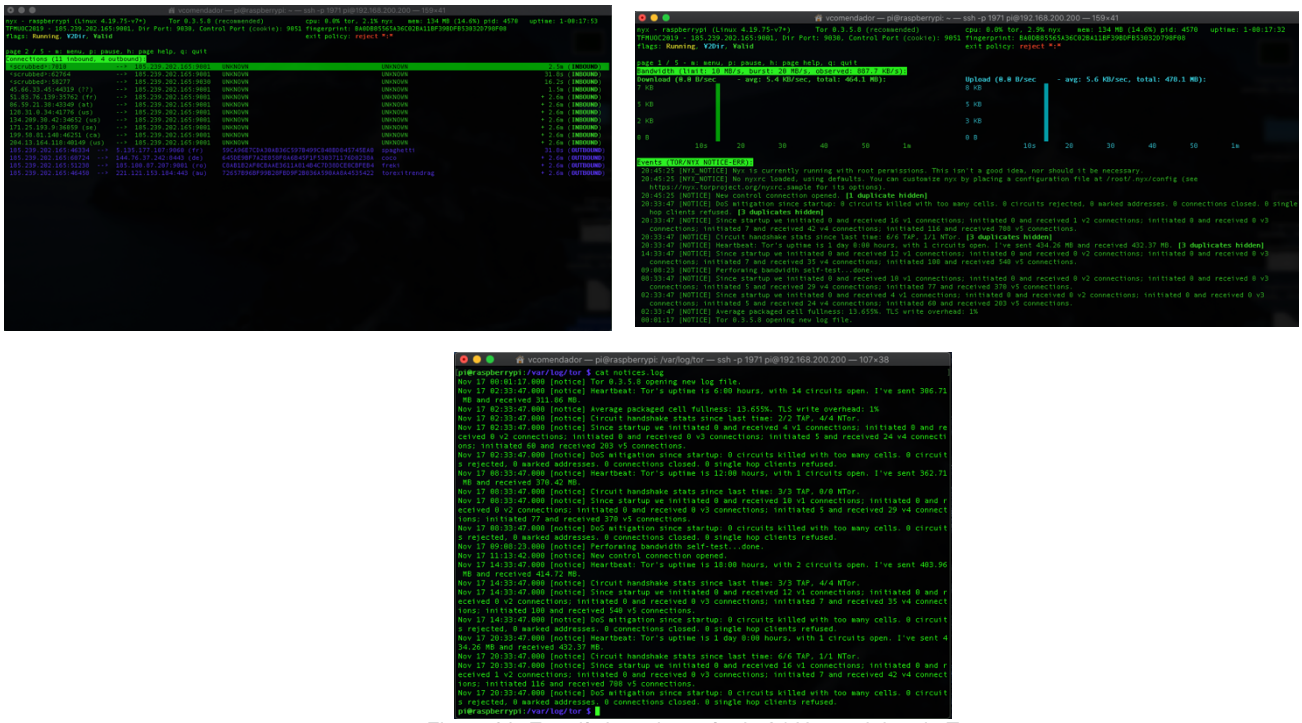


Figura 89: Estadísticas después de 24 Horas del nodo Tor.

En el segundo día de trabajo ininterrumpido de nuestro nodo, hemos vuelto a obtener las estadísticas en el log de Tor las cuales son:

Nov 18 20:33:47.000 [notice] Heartbeat: Tor's uptime is 2 days 0:00 hours, with 27 circuits open. I've sent 915.14 MB and received 906.84 MB.

Además, se ha otorgado un nuevo Flag a nuestro nodo, el cual es: **Fast**: Este nodo tiene mucho ancho de banda disponible. Por lo que las conexiones han aumentado considerablemente con respecto al primer día, adjuntamos capturas en las que podemos ver la barra en el lateral izquierdo de la lista de conexiones se encuentra a la mitad de la cantidad de conexiones que soporta el nodo, también observar el nuevo Flag obtenido:

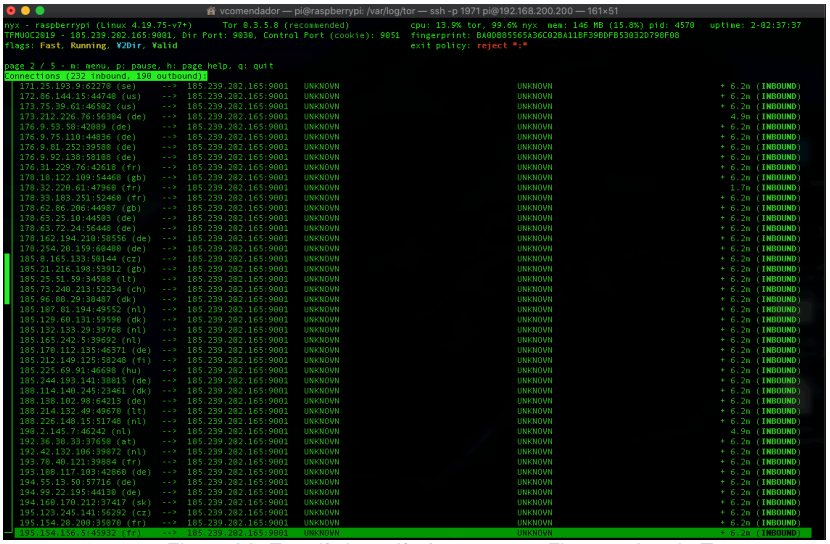


Figura 90: Estadísticas día 2 con nuevo Flag en el nodo Tor.

Fase segunda de 3-8 días:

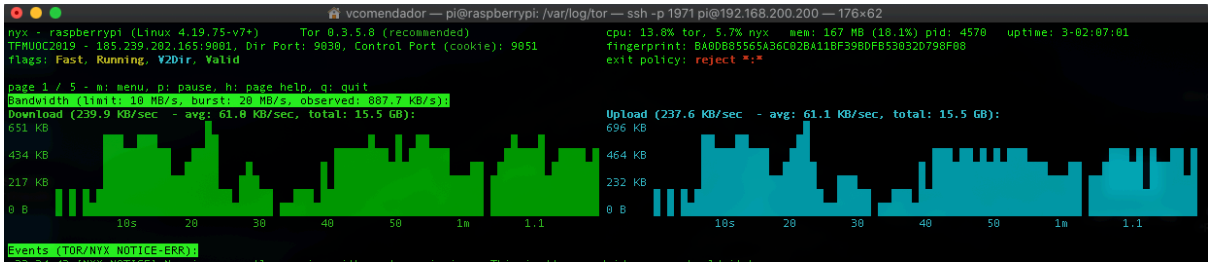
En el tercer día los logs indican:

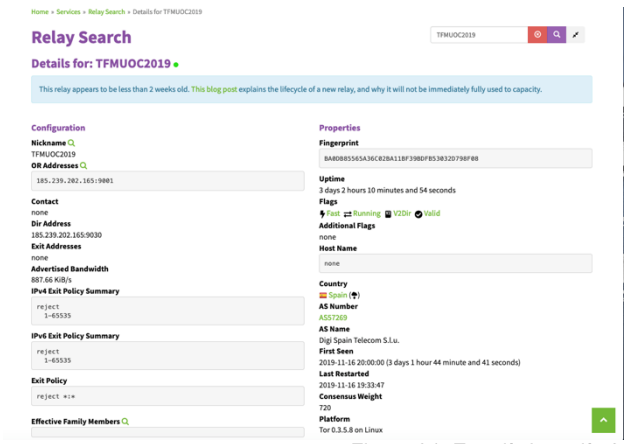
Nov 19 20:33:47.000 [notice] Heartbeat: Tor's uptime is 3 days 0:00 hours, with 260 circuits open. I've sent 11.38 GB and received 11.36 GB.

Nov 19 20:33:47.000 [notice] Circuit handshake stats since last time: 431/431 TAP, 9489/9489 NTor.

Nov 19 20:33:47.000 [notice] Since startup we initiated 0 and received 77 v1 connections; initiated 0 and received 24 v2 connections; initiated 0 and received 0 v3 connections; initiated 1021 and received 1224 v4 connections;

Podemos observar como nuestro nodo se va integrando en la Red Tor y obteniendo más trabajo y consideración dentro de ella, tanto a nivel de conexiones como de las graficas que nos ofrece Nyx así como desde la Web de Tor Metrics.





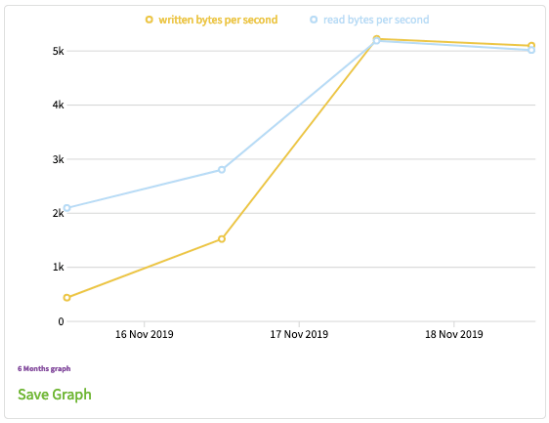


Figura 91: Estadísticas día 3 del nodo Tor.

En el cuarto día los logs nos muestran:

Nov 20 20:33:47.000 [notice] Heartbeat: Tor's uptime is 4 days 0:00 hours, with 316 circuits open. I've sent 28.31 GB and received 28.29 GB.

Nov 20 20:33:47.000 [notice] Circuit handshake stats since last time: 597/597 TAP, 14605/14605 NTor.

Nov 20 20:33:47.000 [notice] Since startup we initiated 0 and received 106 v1 connections; initiated 0 and received 77 v2 connections; initiated 0 and received 0 v3 connections; initiated 2353 and received 2918 v4 connections; initiated 21478 and received 22638 v5 connections.

Nov 20 20:33:47.000 [notice] DoS mitigation since startup: 0 circuits killed with too many cells. 0 circuits rejected, 0 marked addresses. 0 connections closed. 3 single hop clients refused.

Y su métrica con Nyx es:

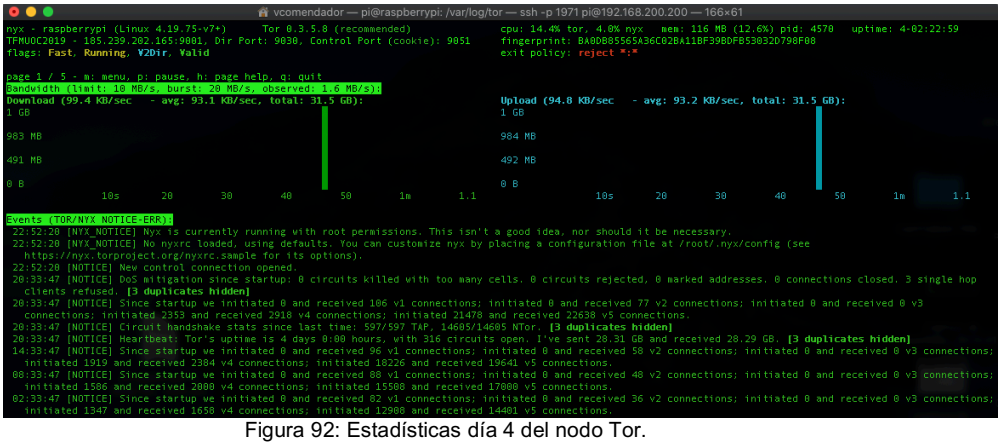


Figura 92: Estadísticas día 4 del nodo Tor.

Hemos explorado la información que podemos obtener de nuestro nodo en internet, y de Tor Metrics en su opción avanzada hemos obtenido los siguientes datos de nuestro nodo:

Figura 93: Información avanzada del nodo Tor.

En el quinto día los logs nos muestran:

Nov 21 20:33:47.000 [notice] Heartbeat: Tor's uptime is 5 days 0:00 hours, with 371 circuits open. I've sent 52.39 GB and received 52.34 GB.

Nov 21 20:33:47.000 [notice] Circuit handshake stats since last time: 591/591 TAP, 15006/15006 NTor.

Nov 21 20:33:47.000 [notice] Since startup we initiated 0 and received 133 v1 connections; initiated 0 and received 146 v2 connections; initiated 0 and received 2 v3 connections; initiated 4154 and received 4915 v4 connections; initiated 33931 and received 34198 v5 connections.

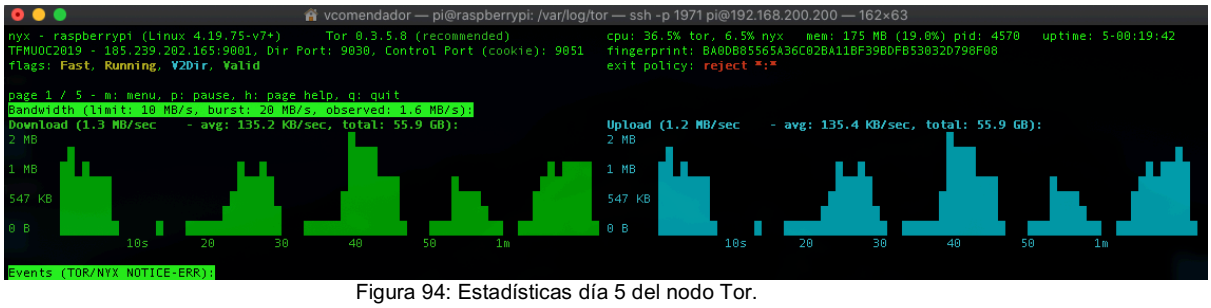


Figura 94: Estadísticas día 5 del nodo Tor.

En el sesto día los logs nos muestran:

Nov 22 20:33:47.000 [notice] Heartbeat: Tor's uptime is 6 days 0:00 hours, with 1433 circuits open. I've sent 86.40 GB and received 86.35 GB.

Nov 22 20:33:47.000 [notice] Average packaged cell fullness: 58.156%. TLS write overhead: 1%

Nov 22 20:33:47.000 [notice] Circuit handshake stats since last time: 7005/7005 TAP, 49086/49086 NTor.

Nov 22 20:33:47.000 [notice] Since startup we initiated 0 and received 158 v1 connections; initiated 0 and received 219 v2 connections; initiated 0 and received 3 v3 connections; initiated 5854 and received 8303 v4 connections; initiated 44021 and received 49481 v5 connections.

Nov 22 20:33:47.000 [notice] DoS mitigation since startup: 0 circuits killed with too many cells. 0 circuits rejected, 0 marked addresses. 0 connections closed. 11 single hop clients refused

Y hemos obtenido dos nuevos Flags:

HSDir: Este nodo es un directorio de servicio oculto v2. Esto significa que el nodo es un directorio de servicio oculto v2 si almacena y sirve descriptores de servicio ocultos v2, y tiene que poseer el indicador Estable y Rápido, también la autoridad tiene que detectar que ha estado funcionando durante al menos 96 horas.

Stable: Este nodo se considera estable por la gran cantidad de hora de funcionamiento correcto.

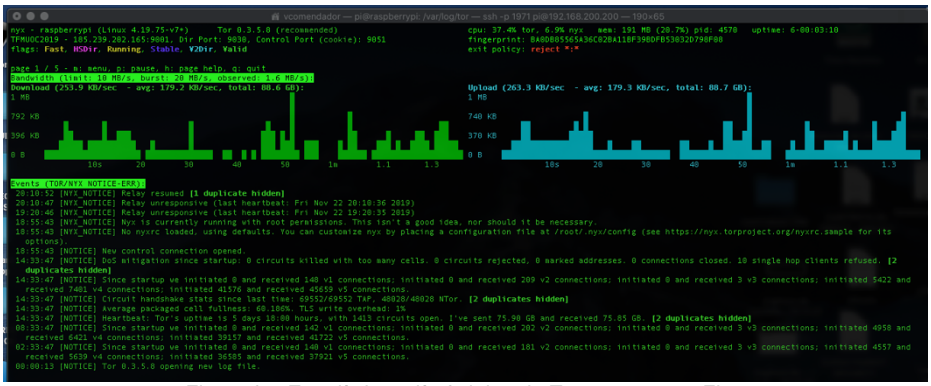


Figura 95: Estadísticas día 6 del nodo Tor con nuevos Flags.

En la Web de Tor Metrics podemos observar los nuevo Flags concedidos por la autoridad, se adjunta captura:

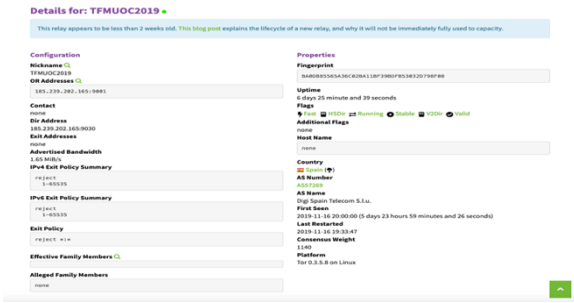


Figura 96: Estadísticas día 6 del nodo Tor Metrics con nuevos Flags.

En el sesto día los logs nos muestran:

Nov 23 20:33:47.000 [notice] Heartbeat: Tor's uptime is 7 days 0:00 hours, with 1310 circuits open. I've sent 119.93 GB and received 119.87 GB.

Nov 23 20:33:47.000 [notice] Average packaged cell fullness: 57.427%. TLS write overhead: 1%

Nov 23 20:33:47.000 [notice] Circuit handshake stats since last time: 1285/1285 TAP, 43543/43543 NTor.

Nov 23 20:33:47.000 [notice] Since startup we initiated 0 and received 183 v1 connections; initiated 0 and received 283 v2 connections; initiated 0 and received 3 v3 connections; initiated 7506 and received 11668 v4 connections; initiated 54105 and received 63953 v5 connections.

Las estadísticas conforman que continúan aumentando el trafico en nuestro nodo:

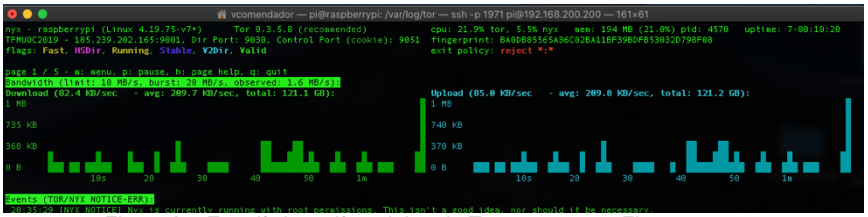


Figura 97: Estadísticas día 7 del nodo Tor con nuevos Flags.

Fase tercera de 8-68 días:

Se considera que nuestro nodo ya pertenece a la red Tor. En el octavo día los logs nos muestran:

Nov 24 20:33:47.000 [notice] Heartbeat: Tor's uptime is 8 days 0:00 hours, with 1093 circuits open. I've sent 149.82 GB and received 149.75 GB.

Nov 24 20:33:47.000 [notice] Average packaged cell fullness: 60.957%. TLS write overhead: 1%

Nov 24 20:33:47.000 [notice] Circuit handshake stats since last time: 2369/2369 TAP, 35258/35258 NTor.

Nov 24 20:33:47.000 [notice] Since startup we initiated 0 and received 218 v1 connections; initiated 0 and received 356 v2 connections; initiated 0 and received 6 v3 connections; initiated 9144 and received 14808 v4 connections; initiated 64349 and received 78344 v5 connections.

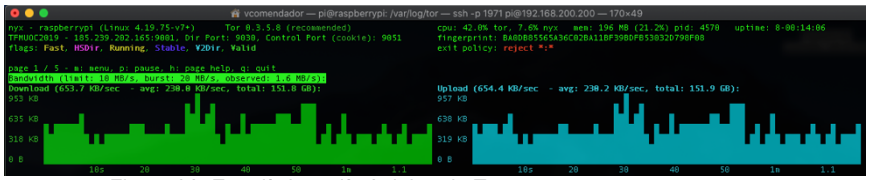


Figura 98: Estadísticas día 8 del nodo Tor.

Fase cuarta más de 68 días:

Aquí terminaría todo el ciclo nuestro nodo/relay.

En la Web de Tor Metrics hemos obtenido una grafica muy completa del papel que ha estado desarrollando nuestro nodo/relay dentó de la Red de Tor, exponemos la grafica.

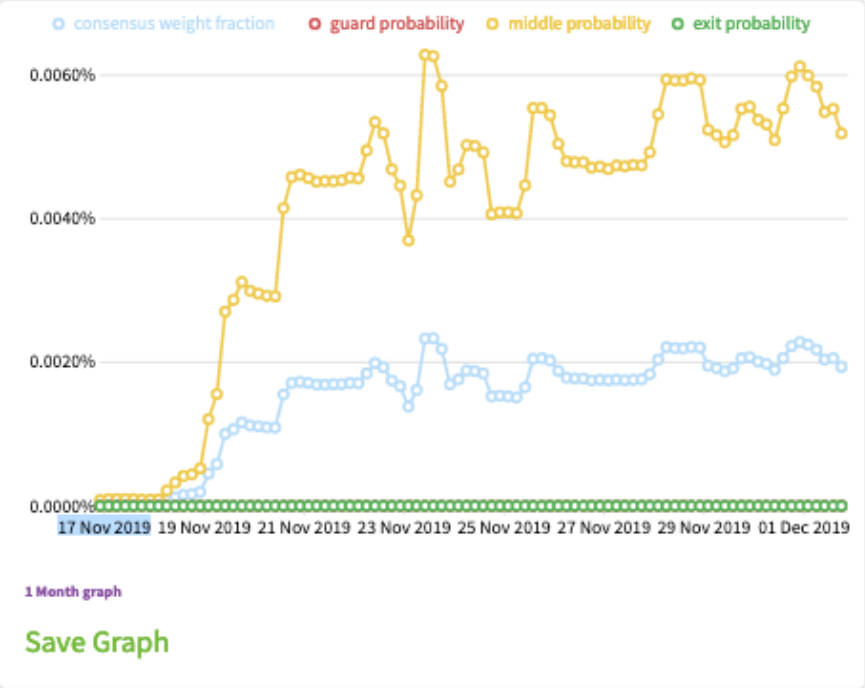


Figura 99: Estadísticas de evolución de nuestro nodo en la Red Tor.

Hemos procedido a la desconexión de nuestro nodo/relay y observamos como el sistema de estadísticas de Tor Metrics mantiene todos los datos de nuestro nodo, mostrando el tiempo que estuvo operativo, así como el que lleva fuera de línea de la Red Tor.

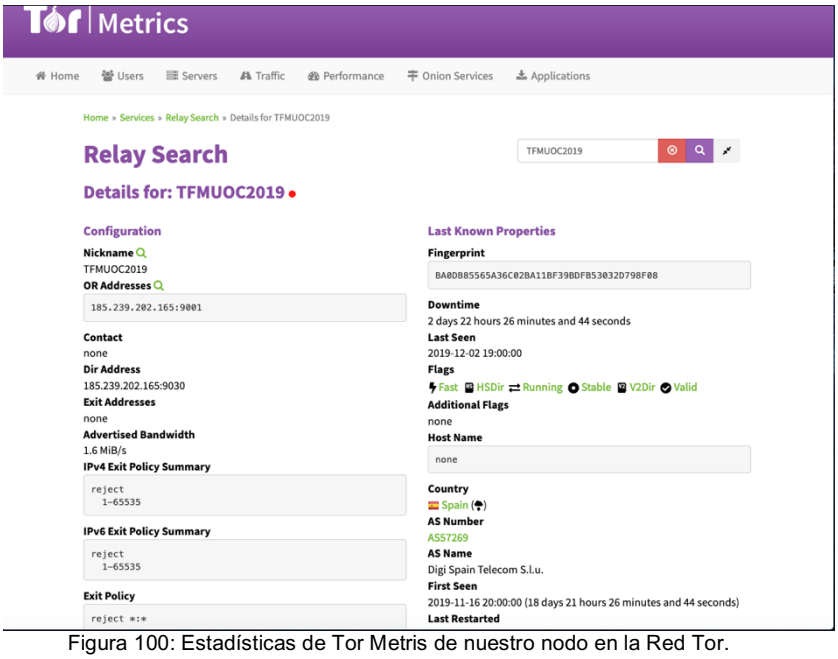


Figura 100: Estadísticas de Tor Metris de nuestro nodo en la Red Tor.

6. Conclusiones y líneas de futuro

6.1. Conclusiones

A lo largo del transcurso de este Trabajo Fin de Master, hemos podido descubrir y entender el significado de las palabras Deep Web, percibiendo y descubriendo que este submundo se compone por muchísimas más cosas que simples Web de contenido ilegal o delictivo.

Siempre como creencia extendida popularmente y determinadas publicaciones que elevaban a niveles muy altos tanto los contenidos y actividades ilegales dentro de estas redes. En nuestra investigación hemos visto que efectivamente este tipo de redes alberga un porcentaje de este tipo de contenido ilegales, los cuales tiene una gran repercusión mediática, pero no todo el contenido ni todo el usuario que se conecta es para realizar actos ilícitos, hemos comprobado que en paralelo a este ecosistema de ilegalidades existe otro totalmente licito y digno de explorar.
Mediante tres redes de anonimato hemos podido investigar el interesante mundo del anonimato, llegado a la conclusión de que muchas informaciones, afirmaciones y experiencias narradas en la Surface Web, son un engaño a la sociedad, ya que hablaban de niveles dentro de un iceberg, de la marianas Web, etc. y no hemos encontrado nada de esto.

El procesamiento de un nodo de salida Tor es arduo y precisa de unos requerimientos mínimos bastante elevados como es un gran ancho de banda que se logra mediante una línea de fibra óptica de gran capacidad, elevada potencia de computación y una integración de sistemas de seguridad óptimos.

Para profundizar más en el conocimiento de estas redes de anonimato y que como no también sirven para saltarse la cesura de algunos países, hemos implementado como investigación practica un nodo/relay de la Red Tor que es la más popular de las tres estudiadas. De las diferentes maneras de funcionamiento de este nodo, hemos optado por la de nodo intermedio y evitar ser un nodo de salida, ya que este ultimo tipo es muy comprometido, ya que en esta red el nodo de salida no encripta el trafico si no que va en claro, pudiendo saber el origen de las peticiones. La Red Tor cuida mucho los nodos de entrada y salida, ya que son los más buscados para ser atacados y obtener la ubicación real de algunos sitios Wb no muy licito.
La ISP que hemos usado no nos ha restringido el acceso a la red Tor, alguno si cortan este tipo de trafico cuando lo detectan.

Tor ofrece un alto grado de seguridad para proteger el anonimato del usuario, pero también sufre algún tipo de vulnerabilidad, aunque la comunidad que desarrolla Tor esta siempre alerta para corregir posibles fallos y parchear su solución. Podemos decir que entre los gobiernos y los

desarrolladores de Tor se relaza una lucha de protección de sus usuarios y las autoridades de descubrir quien esta detrás de este anonimato para detenerlo.

Con nuestro nodo/ hemos capturado trafico y hemos descubierto dentro de Tor que tipos de nodos se conectaban con el, también hemos detectado otros nodos intermedios que se conectaban con nosotros.

6.2.Líneas de futuro

Podríamos seguir investigando sobre otro tipo de redes similares a las estudiadas en este proyecto.
En nuestro estudio hemos navegado por tres de las más conocidas, ni que decir tiene que la que más destaca es Tor ya que es muy popular y tiene mucho contenido.
Pero otra gran línea de investigación para profundizar mucho más seria la red Freenet, que como hemos visto es una red de distribución de información descentralizada y resistente a la censura, inicialmente se identifica con algún grado más de segura que la mencionada red Tor pero con una velocidad mucho menor.

Otra opción que seria interesante investigar para evitar la censura es **Ultrasurf** [39], al cual es una herramienta que fue diseñada en sus orígenes para usuarios de Internet en China continental, donde Internet está muy censurada y las actividades de los usuarios de Internet son monitorizadas.

Hemos detectado algunos nombres de redes de anonimato, pero creemos que son proyectos abandonados, o no tiene muchos seguidores, ya que la información es del año 2016 como **PrivaTegrity** o **Riffle**

Otra línea de exploración también muy interesante seria la búsqueda de vulnerabilidades y ataques sobre estas redes, pudiendo así estudiarlas desde otra óptica y verificar sus eficacias ante diferentes intentos de romper su anonimato.

Seria muy interesante también, abrir otra línea de investigación sobre la tecnología **Blockchain** (Cadena de bloques: columna vertebral sobre la cual descansan las arquitecturas de las criptomonedas) y la relevancia de la misma. Su creador, bajo el seudónimo de Satoshi Nakamoto, pretendía crear un proyecto con un objetivo principal: que las transacciones económicas entre dos personas no necesiten de un organismo central o ningún tipo de intermediario. Usando estas formas de pago se podría estudiar algún ejemplo, como el uso por parte de los cibercriminales en la red y la complejidad que una investigación por parte de las Fuerzas y Cuerpos de Seguridad del Estado deberían abordar ante esta tecnología.

Bibliografía

• **Web:** PUCP. http://red.pucp.edu.pe/wp-content/uploads/biblioteca/Castells_internet.pdf [1]

- **Libro**: Eduardo Casas Herrer, La Red Oscura (En las Sombras de Internet) XcUDI 31/08/17 [2]

• **Web:** YouTube CINCIBE. https://www.youtube.com/watch?v=PYu9Zkwmhw0&t=1s [3]

• **Web:** Blogthingkbig,com. https://blogthinkbig.com/surface-web-deep-web-darknet-se-diferencian [4]

• **Web:** Wikipedia. https://es.wikipedia.org/wiki/Internet_de_las_cosas [5]

• **Web:** Buscador SHODAN. https://www.shodan.io [6]

• **Web:** Internet live stats. https://www.internetlivestats.com/ [7]

• **Web:** Wikipedia. https://en.wikipedia.org/wiki/Deep_web [8]

• **Web:** Wikipedia. https://danielmiessler.com/study/internet-deep-dark-web/ [9]

• **Web:** Wikipedia. https://es.wikipedia.org/wiki/I2P [10]

• **Web:** INCIBE. https://www.incibe-cert.es/blog/redes-anonimas-mas-alla-de-tor [11]

• **Web:** I2P. https://geti2p.net/es/docs/how/tech-intro [12]

• **Web:** FreeNet. https://freenetproject.org/ [13]

• **Web:** INCIBE. https://www.incibe-cert.es/blog/redes-anonimas-mas-alla-de-tor [14]

• **Web:** Yolanda Corral. https://www.yolandacorral.com/tor-vs-freenet/ [15]

• **Web:** Tor. https://www.torproject.org/es/ [16]

• **Web:** Periodismos Actual. https://periodismoactual.com/que-es-la-red-tor-y-como-funciona [17]

• **Web:** Tor. https://tormap.void.gr/ [18]

• **Web:** Tor. https://tb-manual.torproject.org/es/onion-services/ [19]

• **Web:** Tor. https://support.torproject.org/es/onionservices/onionservices-2/ [20]

• **Web:** Tor. https://www.genbeta.com/seguridad/llega-la-nueva-generacion-de-onion-services-con-mayor-privacidad-y-seguridad-para-la-red-tor [21]

• **Web:** Q4OS. https://www.q4os.org/ [22]

• **Web:** I2P. https://geti2p.net/es/ [23]

• **Web:** FreeNet. https://freenetproject.org/ [24]

• **Web:** Wikipedia. https://es.wikipedia.org/wiki/Whonix [25]

• **Web:** Whonix. https://www.whonix.org/ [26]

• **Web:** Luis Llamas. https://www.luisllamas.es/modelos-de-raspberry-pi/ [27]

• **Web:** Wikipedia. https://es.wikipedia.org/wiki/Raspbian [28]

• **Web:** RaspBerry. https://www.raspberrypi.org/downloads/ [29]

• **Web:** RaspBerry para torpes. https://raspberryparatorpes.net/instalacion/poner-la-direccion-ip-fija-en-raspbian-pixel/ [30]

• **Web:** RaspBerry. https://www.raspberrypi.org/documentation/remote-access/ssh/ [31]

• **Web:** Tor. https://2019.www.torproject.org/docs/tor-manual.html [32]

• **Web:** Diego Calvo. http://www.diegocalvo.es/capturar-paquetes-en-linux-con-tcpdump/ [33]

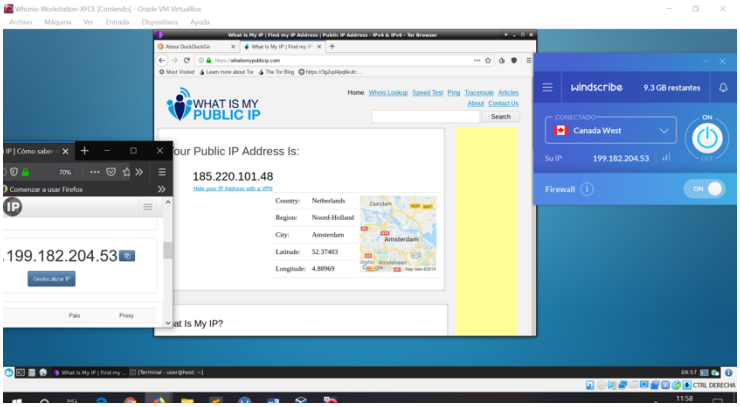
• **Web:** Tor Nyx. https://nyx.torproject.org/ [34]

• **Web:** Tor. https://gitweb.torproject.org/torspec.git/tree/dir-spec.txt?id=a442ab92e84a044ffe90cad37cd517e0f98e1bea#n2229 [35]
• **Web:** Tor. https://community.torproject.org/relay/setup/post-install/ [36]
• **Web:** Tor. https://blog.torproject.org/lifecycle-new-relay [37]
• **Web:** Tor Metrics. https://metrics.torproject.org/ [38]
• **Web:** Ultrasurf. https://ultrasurf.us/ [39]

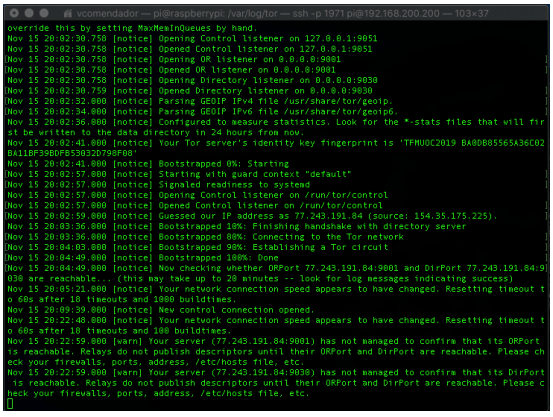
Anexo

Procederemos ahora a exponer algunos elementos que hemos usado, pero no se han detallado en el documento, o algún tipo de inconveniente que se nos ha producido al implementar o ejecutar algún aplicativo.

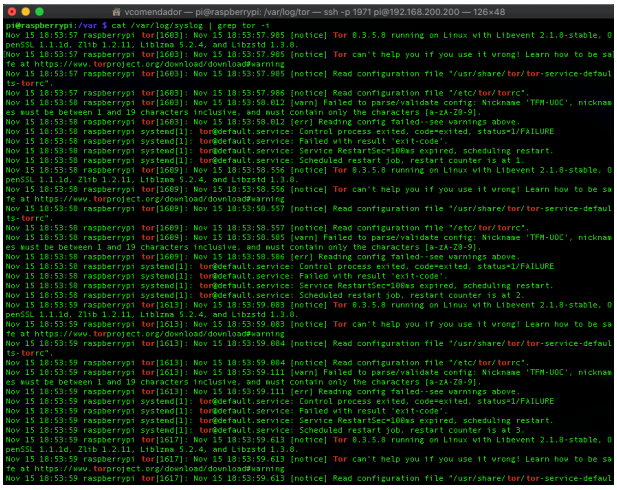
Para realizar el punto 3 del documento hemos usado una VPN para tunelizar todo el trafico que se genera al conectarnos a cualquier red de anonimato, protegiendo así mucho más nuestra identidad y nuestra IP de origen. La VPN usada a sigo Windscribe, seguramente adjuntamos una captura donde vemos el cliente de la VPN conectado en Canadá, una página Web que geo-localiza la IP y muestra Canadá, también podemos observar que ya estamos conectados a Tor, mediante Whonix y tenemos IP y conexión con la red Tor.



A la hora de ejecutar el servicio de Tor en la Raspberry, obtuvimos varios avisos de que no se podrían conectar con los puertos especificados en el trorc, así que, tras una pequeña investigación por Internet, detectamos que no teníamos abiertos estos puertos en nuestro router, lo solucionamos haciendo un Port Forwarding en el mismo. Adjuntamos pantalla con el log donde se ve el error.



Una vez solucionado el problema de comunicaciones, tuvimos otro error al indicar el nombre de nodo. Ya que utilizamos en primer momento un guion para separa dos palabras y la red Tor no permite ningún tipo de símbolo, adjuntamos captura del log con el error del nombre.


vcomendador — pi@raspberrypi: /var/log/tor — ssh -p 1971 pi@192.168.200.200 — 126×48
pi@raspberrypi:/var $ cat /var/log/syslog | grep tor -i
Nov 15 18:53:57 raspberrypi tor[1603]: Nov 15 18:53:57.985 [notice] Tor 0.3.5.8 running on Linux with Libevent 2.1.8-stable, O
penSSL 1.1.1d, Zlib 1.2.11, Liblzma 5.2.4, and Libzstd 1.3.8.
Nov 15 18:53:57 raspberrypi tor[1603]: Nov 15 18:53:57.985 [notice] Tor can't help you if you use it wrong! Learn how to be sa
fe at https://www.torproject.org/download/download#warning
Nov 15 18:53:57 raspberrypi tor[1603]: Nov 15 18:53:57.985 [notice] Read configuration file "/usr/share/tor/tor-service-defaul
ts-torrc".
Nov 15 18:53:57 raspberrypi tor[1603]: Nov 15 18:53:57.986 [notice] Read configuration file "/etc/tor/torrc".
Nov 15 18:53:58 raspberrypi tor[1603]: Nov 15 18:53:58.012 [warn] Failed to parse/validate config: Nickname 'TFM-UOC', nicknam
es must be between 1 and 19 characters inclusive, and must contain only the characters [a-zA-Z0-9].
Nov 15 18:53:58 raspberrypi tor[1603]: Nov 15 18:53:58.012 [err] Reading config failed--see warnings above.
Nov 15 18:53:58 raspberrypi systemd[1]: tor@default.service: Control process exited, code=exited, status=1/FAILURE
Nov 15 18:53:58 raspberrypi systemd[1]: tor@default.service: Failed with result 'exit-code'.
Nov 15 18:53:58 raspberrypi systemd[1]: tor@default.service: Service RestartSec=100ms expired, scheduling restart.
Nov 15 18:53:58 raspberrypi systemd[1]: tor@default.service: Scheduled restart job, restart counter is at 1.
Nov 15 18:53:58 raspberrypi tor[1609]: Nov 15 18:53:58.556 [notice] Tor 0.3.5.8 running on Linux with Libevent 2.1.8-stable, O
penSSL 1.1.1d, Zlib 1.2.11, Liblzma 5.2.4, and Libzstd 1.3.8.
Nov 15 18:53:58 raspberrypi tor[1609]: Nov 15 18:53:58.556 [notice] Tor can't help you if you use it wrong! Learn how to be sa
fe at https://www.torproject.org/download/download#warning
Nov 15 18:53:58 raspberrypi tor[1609]: Nov 15 18:53:58.557 [notice] Read configuration file "/usr/share/tor/tor-service-defaul
ts-torrc".
Nov 15 18:53:58 raspberrypi tor[1609]: Nov 15 18:53:58.557 [notice] Read configuration file "/etc/tor/torrc".
Nov 15 18:53:58 raspberrypi tor[1609]: Nov 15 18:53:58.585 [warn] Failed to parse/validate config: Nickname 'TFM-UOC', nicknam
es must be between 1 and 19 characters inclusive, and must contain only the characters [a-zA-Z0-9].
Nov 15 18:53:58 raspberrypi tor[1609]: Nov 15 18:53:58.586 [err] Reading config failed--see warnings above.
Nov 15 18:53:58 raspberrypi systemd[1]: tor@default.service: Control process exited, code=exited, status=1/FAILURE
Nov 15 18:53:58 raspberrypi systemd[1]: tor@default.service: Failed with result 'exit-code'.
Nov 15 18:53:58 raspberrypi systemd[1]: tor@default.service: Service RestartSec=100ms expired, scheduling restart.
Nov 15 18:53:58 raspberrypi systemd[1]: tor@default.service: Scheduled restart job, restart counter is at 2.
Nov 15 18:53:59 raspberrypi tor[1613]: Nov 15 18:53:59.083 [notice] Tor 0.3.5.8 running on Linux with Libevent 2.1.8-stable, O
penSSL 1.1.1d, Zlib 1.2.11, Liblzma 5.2.4, and Libzstd 1.3.8.
Nov 15 18:53:59 raspberrypi tor[1613]: Nov 15 18:53:59.083 [notice] Tor can't help you if you use it wrong! Learn how to be sa
fe at https://www.torproject.org/download/download#warning
Nov 15 18:53:59 raspberrypi tor[1613]: Nov 15 18:53:59.084 [notice] Read configuration file "/usr/share/tor/tor-service-defaul
ts-torrc".
Nov 15 18:53:59 raspberrypi tor[1613]: Nov 15 18:53:59.084 [notice] Read configuration file "/etc/tor/torrc".
Nov 15 18:53:59 raspberrypi tor[1613]: Nov 15 18:53:59.111 [warn] Failed to parse/validate config: Nickname 'TFM-UOC', nicknam
es must be between 1 and 19 characters inclusive, and must contain only the characters [a-zA-Z0-9].
Nov 15 18:53:59 raspberrypi tor[1613]: Nov 15 18:53:59.111 [err] Reading config failed--see warnings above.
Nov 15 18:53:59 raspberrypi systemd[1]: tor@default.service: Control process exited, code=exited, status=1/FAILURE
Nov 15 18:53:59 raspberrypi systemd[1]: tor@default.service: Failed with result 'exit-code'.
Nov 15 18:53:59 raspberrypi systemd[1]: tor@default.service: Service RestartSec=100ms expired, scheduling restart.
Nov 15 18:53:59 raspberrypi systemd[1]: tor@default.service: Scheduled restart job, restart counter is at 3.
Nov 15 18:53:59 raspberrypi tor[1617]: Nov 15 18:53:59.613 [notice] Tor 0.3.5.8 running on Linux with Libevent 2.1.8-stable, O
penSSL 1.1.1d, Zlib 1.2.11, Liblzma 5.2.4, and Libzstd 1.3.8.
Nov 15 18:53:59 raspberrypi tor[1617]: Nov 15 18:53:59.613 [notice] Tor can't help you if you use it wrong! Learn how to be sa
fe at https://www.torproject.org/download/download#warning
Nov 15 18:53:59 raspberrypi tor[1617]: Nov 15 18:53:59.613 [notice] Read configuration file "/usr/share/tor/tor-service-defaul