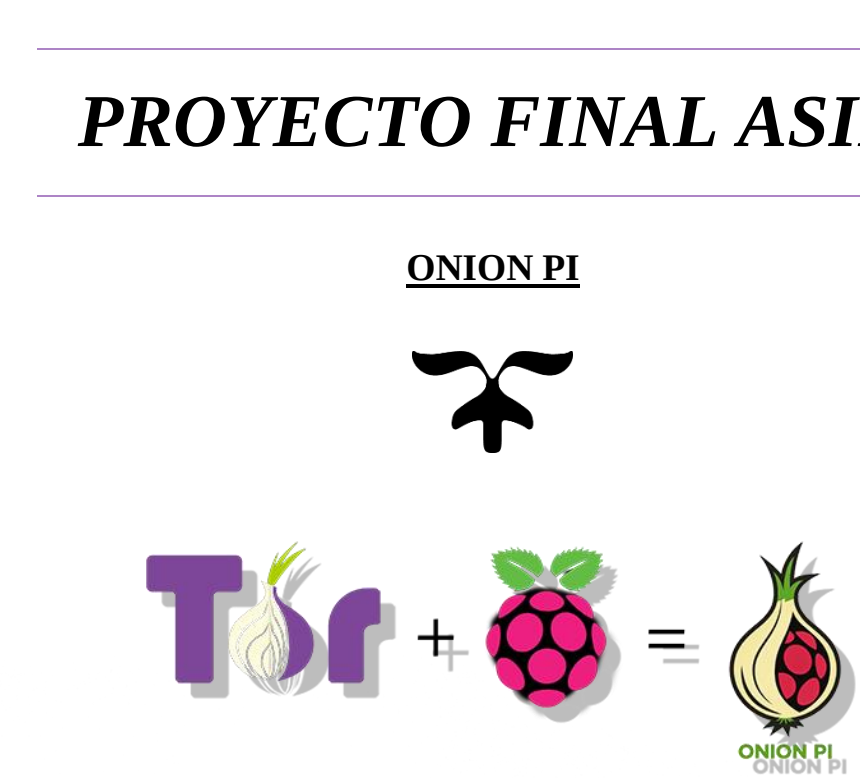
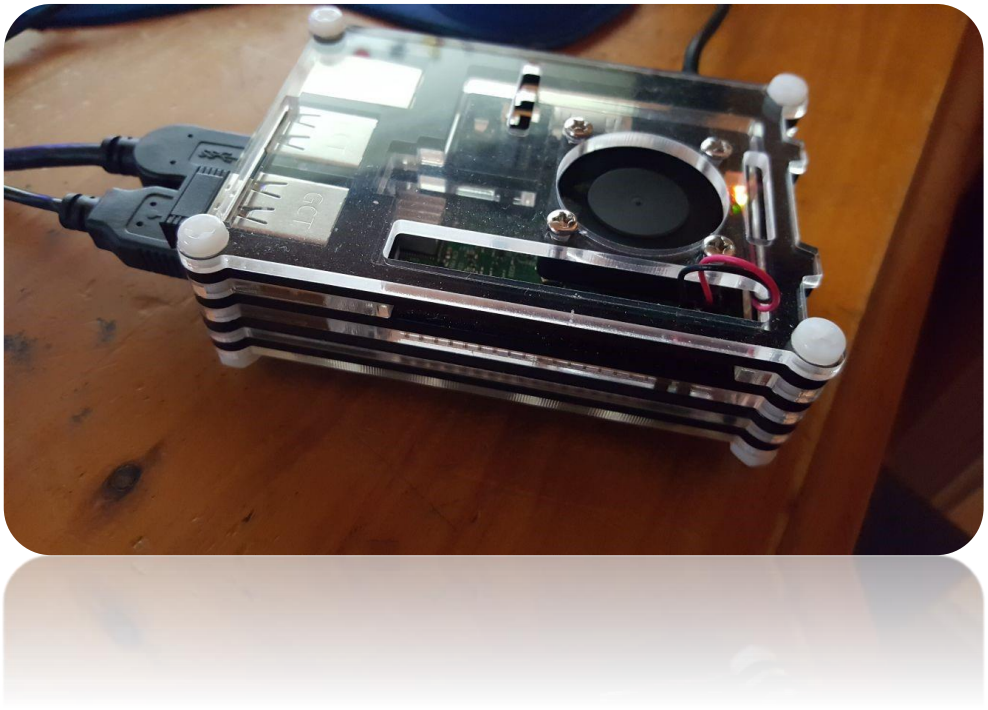
PROYECTO FINAL ASIR

ONION PI





14 DE MARZO DE 2018

PROYECTO FINAL ASIR
ANDRÉS CORTÉS ESCOBEDO

INDICE

1.- Descripción del proyecto, y tecnologías que vamos a aprender o investigar.

Tor + Raspberry Pi 3 = Onion Pi

Onion Pi es la unión de Tor (The Onion Router) implementado en un dispositivo Raspberry Pi. Se trata de un punto de acceso wifi que te proporciona conexión a la **red Tor.**

Este proyecto nació con la idea de poder crear una red TOR eficiente, económico y totalmente funcional.

Demostraremos que se pueden ofrecer un punto de acceso que se pueda llevar a cualquier lado y poder tener una navegación anónima protegiéndonos de internet, haciendo competencia a un ordenador/servidor convencional, con una inversión inicial reducida y un coste energético mínimo. Aunque a un nivel funcional menor (ya que mi capital económico es limitado), con un gasto reducido se puede llegar a crear una red TOR.

Este proyecto está orientado a las empresas que han empezado o quienes tienen una economía limitada, y para aquellos que buscan un producto de calidad, de reducidas dimensiones y que tenga coste económico mucho más bajo que usar un ordenador convencional.

Las tecnologías que vamos a aprender o investigar son:

- **El funcionamiento de la red Tor**
- **Documentación Tor**
- **Raspberry Pi**
- **Sistema operativo Raspbian**

2.- Relación de nuestro proyecto con las asignaturas del ciclo formativo de ASIR: Sistemas Operativos, Redes, Servicios en Red, Empresa, Seguridad, Aplicaciones Web, Bases de datos, etc.

Este proyecto tiene relación con las siguientes asignaturas :

- **Sistemas operativos**
- **Redes y Servicios en Red**
- **Seguridad en Red**

3.- Objetivos que perseguimos con el proyecto, contestando a estas preguntas: ¿Qué vamos a aprender?, ¿Qué queremos conseguir?, ¿Qué necesidades cubriría en una empresa?

¿Qué vamos a aprender?

Vamos aprender la nueva tecnología "**Raspberry Pi**" su funcionamiento, y que con algo tan pequeño, podemos hacer las mismas funciones como las de un servidor obviamente con sus limitaciones, pero a un costo muy reducido comparado con un servidor convencional, por otro lado el sistema operativo de Raspberry Pi, que se llama "**Raspbian**" que es el recomendado para la optimización de este pequeño ordenador, basado en Debian Jessie, que para usuarios de cultura media en informática se le hará más fácil el uso de la terminal que es de Linux.

La tecnología TOR son las siglas de '**The Onion Router**', la red de comunicaciones superpuesta a Internet y basada en un sistema de enrutamiento por capas, que permite al usuario conectarse a la Red haciendo uso de una serie de nodos intermedios (proporcionados por otros usuarios de la red) posibilitando así mantener la integridad y el anonimato de las conexiones realizadas a través de los mismos, de manera similar a una VPN, es decir hace la función de una **red TOR**

Iptables es el corta fuegos que viene implementado en Linux con el cual obtenemos una implementación en la seguridad que se encargara de controlar las comunicaciones entre la red y el exterior, denegando o permitiendo los paquetes de datos que mediante reglas se irán filtrando.

Por último, gracias al servicio de **hostapd** podemos tener un punto de acceso con nuestra raspberry pi que podemos configurar mediante el archivo de configuración, y como tenemos el modelo raspberry pi B no hará falta una antena usb, porque este tipo ya tiene una integrada, aunque si queremos que nuestra máquina tenga más alcance pues si sería necesaria.

¿Qué queremos conseguir?

El objetivo principal es probar que con poco dinero y usando la tecnología Rasberry, podemos dar servicio a las empresas, cubriendo la necesidad de navegar de forma segura, privada, de una manera económica y funcional.

¿Qué beneficios tiene usar nuestro proyecto en una empresa?

Onion pi, trata de hacer un punto de acceso el cual conectará a nuestro router y nos dará acceso a internet. Además, podremos evitar un seguimiento o realizar el bloqueo de sitios por parte del proveedor de internet local, alojar servicios dentro de la red sin necesidad de revelar la ubicación del sitio… Todo ello encaminado para garantizar una comunicación de forma segura con otra persona.

TOR esconde el origen y el destino de todo el tráfico que éste genera, por lo que oculta nuestra identificación, que buscamos, y por donde navegamos. Al esconder el destino de su tráfico también te ayuda a saltarte la censura, e incluso a acceder a sitios bloqueados en tu región por cualquier motivo.

Por otro lado, también tenemos un ahorro económico tanto de consumo como de precio ya que este "mini ordenador" en comparación con un ordenador/servidor es mucho más barato.

Puesto que los datos en una empresa es el núcleo fundamental de la misma, la principal ventaja que tendría este proyecto sería la gran seguridad que ofrecería en la comunicación, ya que ésta sería muy difícil ser robada o interceptada por ciberdelincuentes.

4.- Necesidades: Software, hardware, documentales, libros, y temporalización (cuanto tiempo se estima que nos va a llevar cada parte del proyecto).

Parte hardware

COMPONENTE	PROVEEDOR	CANTIDAD	PRECIO FINAL
Raspberry pi 3 Modelo B	**Amazon**	**1**	**36.00**
Cargador de 5V/2.5 + 3x Disipador + Ventilador + Cable micro usb con conector on/off	**Amazon**	**1**	**15.00**
Tarjeta SD (32 Gb)	**Amazon**	**1**	**12.00**
Cable Ethernet.	**Amazon**	**1**	**5.00**
Cable HDMI	**Amazon**	**1**	**6.00**

- Raspberry Pi 3 Modelo B
- Adaptador de corriente que proporcione una salida de 5V y 1A.
- Tarjeta SD (32 Gb) con Raspbian instalado.
- Cable Ethernet.
- Cable HDMI para conectar a un monitor a la raspberry

¿Qué es Raspberry Pi?

Es un ordenador del tamaño de una tarjeta de crédito. Consta de una placa base sobre la que se monta un procesador, un chip gráfico y memoria RAM. Fue lanzado en 2006 por la Fundación Raspberry Pi con el objeto de estimular la enseñanza de informática en las escuelas de todo el mundo.

¿Es un ordenador completo?

Sí, con la excepción de que no incluye el cable de alimentación, la caja ni el disco duro, para el que se utiliza una tarjeta de memoria microSD. Otros periféricos como el teclado, el ratón o el receptor wifi pueden conectarse vía USB. También se precisa de un monitor, como es lógico.

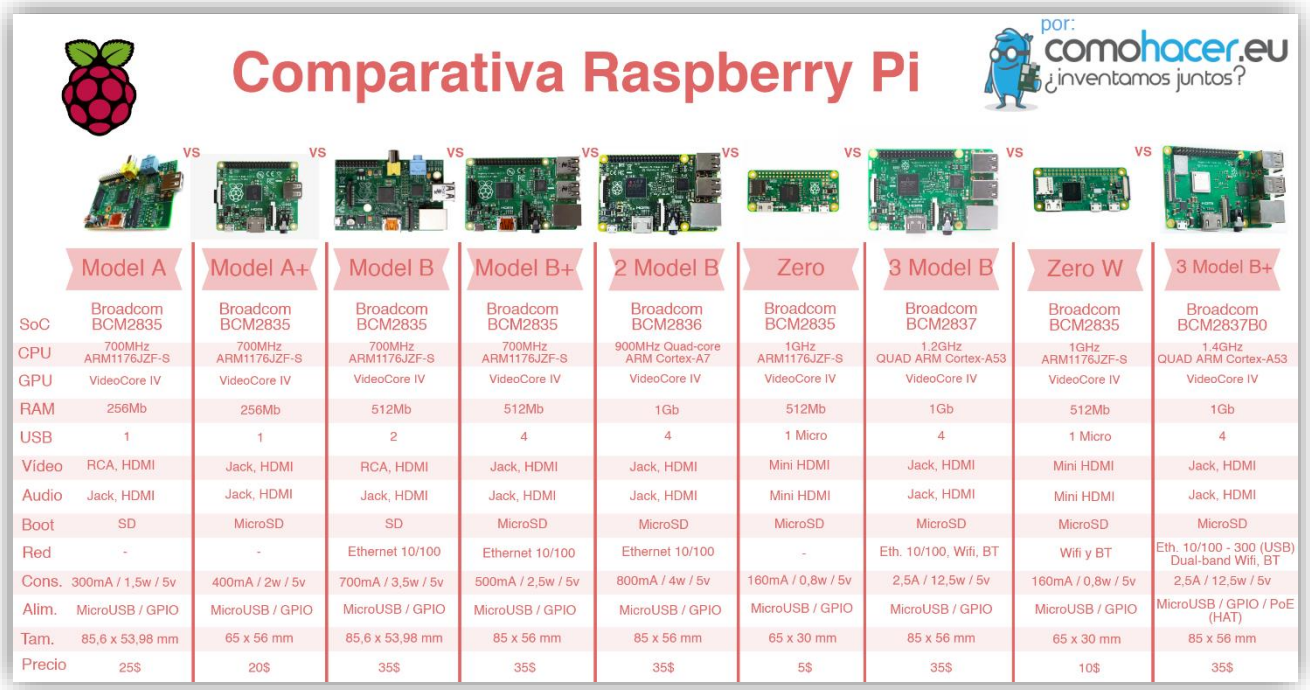
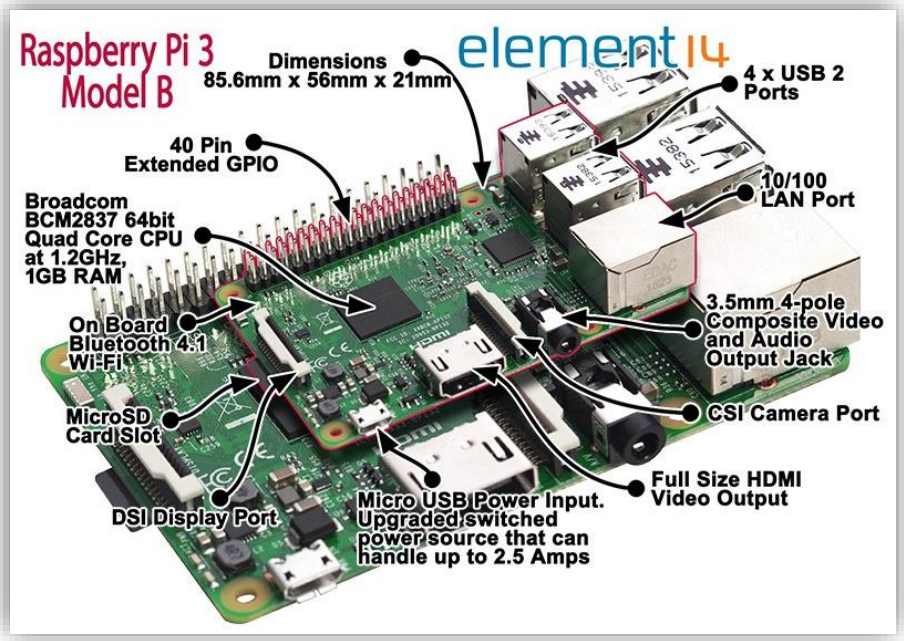


Tabla comparativa de los distintos tipos de Raspberrys que hay en el mercado.



(Esquema de Raspberry Pi modelo B, la expongo ya que es la que voy a usar en el proyecto.)

¿Cuánto cuesta?

Su precio oscila entre los 25 y los 38 euros, según el modelo que se elija. Hay dos, A y B, (**raspberry 1**) que comparten una serie de características, como el chip, el procesador gráfico, las entradas/salidas y la capacidad para reproducir vídeo en 1080p. El modelo B es más caro ya que tiene mejores prestaciones en comparación con el A.

¿Es potente?

El procesador funciona a 1.2 GHz y puede acelerar gráficos 3D por hardware. Más o menos como el ordenador que tenías en 2003, con la salvedad de que puedes ver películas en alta definición.

¿Qué sistema operativo emplea?

Se pueden instalar un buen puñado de ellos, la mayoría basados en el kernel de Linux. Algunos de los más conocidos son Android, Firefox OS, Raspbian, OpenWebOS o Unix. También se pueden cargar interfaces gráficas similares a Windows, de modo que la curva de aprendizaje del sistema no es demasiado pronunciada.

¿Puede utilizarlo cualquiera?

Cualquiera que tenga unas nociones básicas de Linux o sea capaz de identificar un problema y buscarlo en Google, podrá utilizar Raspberry Pi. Su complejidad es directamente proporcional a la ambición que se muestre en su aplicación práctica. En cualquier caso la instalación base es asequible y en internet campan cientos de programas empaquetados que dotan a la placa de una u otra funcionalidad.

¿En qué se diferencia de mi viejo ordenador?

Raspberry Pi es la esencia de tu viejo ordenador y, por lo tanto, tiene ciertas limitaciones. Es terriblemente lento cargando las páginas web (al menos en el navegador por defecto) o retocando una fotografía, y de ninguna manera será capaz de ejecutar un videojuego actual. No obstante, a diferencia del antiguo PC, la tecnología es obsoleta, que no vieja. Las piezas no están recicladas, sino que tienen el ciclo de vida intacto. Además, gracias a su tamaño y a las virtudes del código abierto, es una máquina con infinitas posibilidades creativas.

Parte software

- **Servicio DHCP**
- **Servicio hostapd**
- **TOR**
- **IPTABLES**
- **Navegador TOR**

Servicio DHCP

Es un conjunto de reglas para dar direcciones IP y opciones de configuración a ordenadores y estaciones de trabajo en una red. Una dirección IP es un número que identifica de forma única a un ordenador en la red, ya sea en una red corporativa o en Internet.

La dirección IP puede ser asignada estáticamente (manualmente) por el administrador o asignada dinámicamente por un servidor central.

Funcionamiento de DHCP

DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC) el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN. Esta tecnología reduce el trabajo de un administrador, que de otra manera tendría que visitar todos los ordenadores o estaciones de trabajo uno por uno. Para introducir la configuración IP consiste en la IP, máscara, puerta de enlace, DNS, etc.

Un servidor DHSC (*DHCP Server*) es un equipo en una red que está corriendo un servicio DHCP. Dicho servicio se mantiene a la escucha de peticiones broadcast DHCP. Cuando una de estas peticiones es oída, el servidor responde con una dirección IP y opcionalmente con información adicional.

Modos en DHCP

Existen 3 modos en DHCP para poder asignar direcciones IP a otros equipos:

1 – Asignación manual: El administrador configura manualmente las direcciones IP del cliente en el servidor DCHP. Cuando la estación de trabajo del cliente pide una dirección IP, el servidor mira la dirección MAC y procede a asignar la que configuró el administrador.

2 – Asignación automática: Al cliente DHCP (ordenador, impresora, etc.) se le asigna una dirección IP cuando contacta por primera vez con el DHCP Server. En este método la IP es asignada de forma aleatoria y no es configurada de antemano.

3 – Asignación dinámica: El servidor DHCP asigna una dirección IP a un cliente de forma temporal. Digamos que es entregada al client Server que hace la petición por un espacio de tiempo. Cuando este tiempo acaba, la IP es revocada y la estación de trabajo ya no puede funcionar en la red hasta que no pida otra.

Conclusión:

DHCP es un protocolo diseñado principalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP está activo en un servidor donde se centraliza la gestión de la direcciones IP de la red. Hoy en día, muchos sistemas operativos incluyen este servicio dada su importancia.

Servicio hostapd

Es un servicio que hace que nuestra tarjeta Wi-Fi se comporte como un punto de acceso.

TOR

Antes de hablar de TOR, quiero hacer un pequeño inciso sobre la diferencia de **Proxy**, **VPN** y de **TOR**

¿Qué es un Proxy?

Un Proxy, al igual que una VPN, dirige tu tráfico a través de otra computadora, en vez de la tuya. Aunque hay servidores proxy públicos y privados, solo los proxies privados, usualmente de pago, proporcionan todo tipo de estabilidad y confiabilidad.

Inconvenientes:

Hoy en día, los principales protocolos proxy en uso son SOCKS y HTTP/HTTPS. Los proxies SOCKS y HTTP no ofrecen encriptación, mientras que HTTPS ofrece proxies con el mismo nivel de encriptación que cualquier sitio web SSL. Sin embargo, los proxies no están diseñados para proteger todo tu tráfico en Internet, normalmente solo el del navegador. Además, muchos proxies pasan la dirección IP original del usuario al sitio de destino, haciendo que no sean adecuados para los usuarios conscientes de su seguridad y privacidad. Finalmente, los proxies deben ser configurados de forma individual para cada aplicación (email, navegador, aplicaciones de terceros) y algunas aplicaciones no son compatibles con los proxies.

¿Qué es VPN?

Una Red Privada Virtual (Vitrual Private Network) es una conexión de red que te permite crear una conexión segura con otra ubicación, por lo tanto, te permite aparecer como si estuvieras en otro lugar. Tu computadora crea un túnel virtual encriptado con el servidor VPN y toda tu navegación aparece como si viniera del servidor VPN. Todo el tráfico de Internet pasa por este túnel encriptado, evitando que tu información esté expuesta a mirones entre tu computadora y el servidor de VPN.

Inconvenientes:

Es imperativo que elijas un servicio de VPN de calidad que no almacene datos o registros de las comunicaciones. En caso de que una agencia del gobierno demande al proveedor de VPN que revele sus registros, los usuarios no podrán quedar expuestos. Además, es importante que el servicio de VPN implemente un balance de cargas y aleatorización de servidores adecuadas para que los usuarios siempre se conecten con un servidor de VPN diferente.

¿Qué es TOR?

TOR es una sigla formada por las palabras “The Onion Router”. La traducción de la palabra The Onion Router vendría a ser enrutador cebolla.

TOR no es más que un proyecto de software libre cuya función es hacer que las comunicaciones entre un cliente y un servidor se hagan mediante lo que se denomina el enrutamiento de cebolla.

Nota: En uno de los apartados de este artículo se explica de forma detallada el funcionamiento del enrutamiento de cebolla.

Objetivos de la red TOR

TOR originariamente fue creado por el ejército de los Estados Unidos con fines militares a mediados de los años 90. Actualmente TOR es gestionado por un grupo de voluntarios que tienen los siguientes objetivos:

- Preservar la privacidad cuando navegamos por Internet.
- Mantener las comunicaciones anónimas y seguras.
- Asegurar la integridad de la información transmitida por Internet.
- Proteger la libertad de los usuarios de Internet.
- Evitar que pueda ser monitorizada y registrada nuestra actividad en Internet.
- Evitar la censura que determinados países aplican sobre sus ciudadanos.

A pesar de las buenas intenciones de TOR hay que remarcar que también hay gente que utiliza la red TOR para actividades ilegales como por ejemplo:

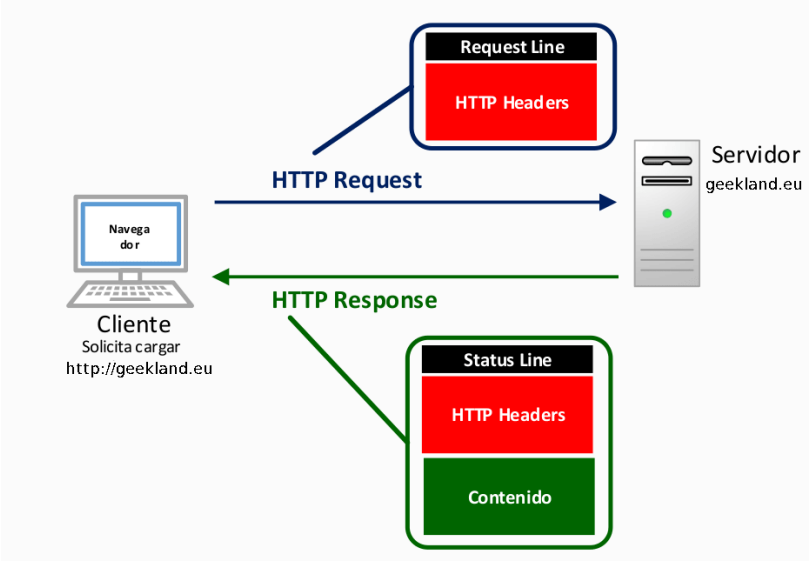
- Compraventa de sustancias prohibidas.
- Compraventa de armas.
- Distribución pornografía infantil.
- Contratación de sicarios.

Funcionamiento de la red tor

Para comprender como funciona TOR primero tenemos que entender el funcionamiento del enrutamiento tradicional.

Funcionamiento del enrutamiento tradicional

Si nos conectamos a internet de forma habitual y queremos visitar una página web, se establecerán varias conexiones directas entre nuestro navegador y el servidor que aloja la página que web para poder obtener el contenido que queremos.



Así de este modo si nos queremos conectar a https://geekland.eu nuestro navegador enviará directamente una petición al servidor de https://geekland.eu.

Cuando se reciba la petición, el servidor analizará el contenido de las cabeceras http (HTTP Headers) de nuestra petición para saber el contenido que tiene que proporcionar.

Seguidamente el servidor nos responderá con otras cabeceras http (HTTP Headers) mas el contenido que queremos visualizar o descargar.

Una vez detallado el sistema de enrutamiento tradicional podremos ver que presenta varios problemas:

1. En muchas ocasiones la totalidad del proceso no incluye ningún mecanismo de cifrado. Por lo tanto un atacante podría interceptar y/o modificar el contenido que visualizamos o descargamos en nuestro ordenador.
2. Aunque el servidor al que nos conectemos use https seguiremos teniendo problemas. El protocolo https no cifra las cabeceras http. Por lo tanto si un atacante intercepta nuestro tráfico no podrá ver su contenido, pero si podrá saber de donde vienen y donde van los datos interceptados.

Para solucionar estos 2 problemas que acabamos de citar podemos usar el enrutamiento de cebolla que nos proporciona TOR.

Funcionamiento del enrutamiento cebolla

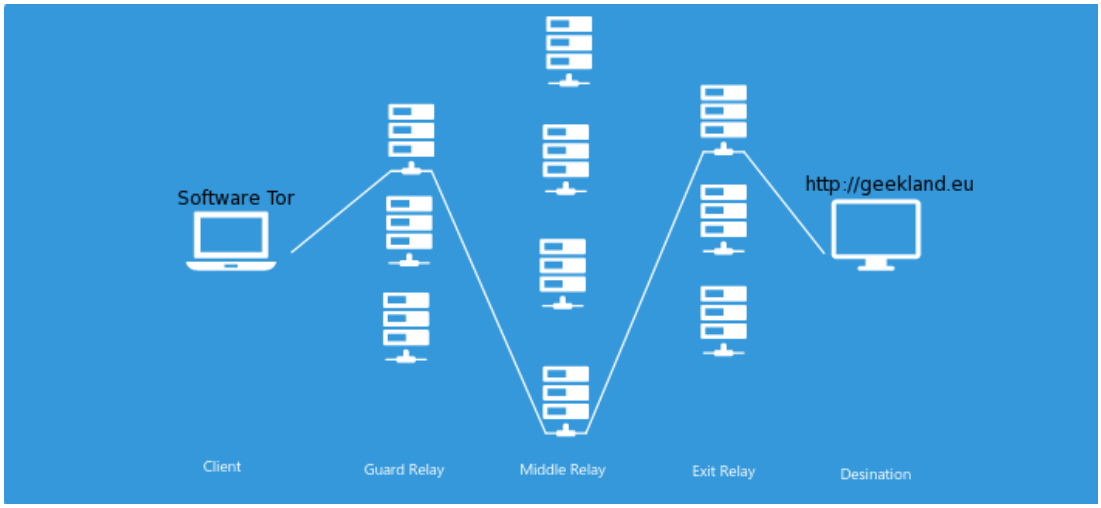
Para entender bien el funcionamiento del enrutamiento de Cebolla lo podemos dividir en tres partes.

1. La primera parte consiste en el establecimiento de la ruta a seguir para poder obtener y/o enviar un contenido.
2. La segunda etapa será el proceso de cifrado de la totalidad de la información que queremos enviar y/o obtener.
3. La tercera y última etapa consistirá en ir descifrando de forma progresiva la totalidad de información que queremos enviar y/o obtener.

Seguidamente explicaremos de forma detallada cada una de las etapas.

Establecimiento de la ruta en el enrutamiento de cebolla

En la siguiente imagen podemos ver una representación gráfica de la ruta que se establece cuando usamos el enrutamiento de cebolla (The Onion Router).



Supongamos que existe un Cliente (Client) que podemos ser nosotros y queremos conectarnos a un destino (Destination) que puede ser la página Web https://geekland.eu

Lo primero que observamos es que en este caso la conexión entre nuestro navegador y el servidor de destino no es directa. Existen multitud de puntos intermedios de conexión denominados nodos (Relays).

Nota: En la actualidad la red Tor dispone de aproximadamente 7000 nodos que son seleccionados de forma aleatoria. Cuanto mayor sea el número de nodos mayor será la privacidad ofrecida por Tor y su velocidad de navegación.

Nota: Los nodos de la red TOR acostumbran a ser públicos y cualquiera de nosotros pueda crear y gestionar uno. Lo único que necesitamos es disponer de un software y de un buen ancho de banda en nuestra casa.

Obtención del los nodos disponibles de la red tor

En el momento que queremos conectarnos a una página web con el enrutado de cebolla, el primer paso que realizará el Software TOR de nuestro ordenador es conectarse a Internet para obtener el listado de la totalidad de nodos disponibles en la red.

El listado de nodos obtenidos será usado para crear una ruta de conexión aleatoria.

Conexión con el nodo de entrada

Una vez obtenido el listado, el Software TOR seleccionará un nodo de entrada (Guard relay).

A continuación el software TOR se conectará de forma segura con el nodo de entrada usando el protocolo TLS. Una vez establecida la conexión segura se creará una clave de sesión 1 entre el software TOR de nuestro ordenador y el nodo de entrada (Guard relay).

Conexión con los nodos intermedios

Para extender la ruta, el software TOR de nuestro ordenador usará la clave de sesión 1 para cifrar un mensaje que enviará al nodo de entrada (Guard relay). Cuando el nodo de entrada reciba el mensaje lo descifrará y de esta forma descubrirá el nodo intermedio (Middle Relay) al que se tiene que contactar.

Acto seguido el nodo inicial establece una conexión segura con el nodo intermedio mediante el protocolo TLS. Una vez establecida la conexión, el nodo de entrada cifra un mensaje con la clave de sesión 1 en el que informa al software TOR que se ha establecido la conexión entre el nodo entrada y el nodo intermedio.

Al llegar el mensaje del nodo entrada (Guard Relay) al Software TOR se descifra y al confirmarse la conexión entre nodos se establece una clave de sesión 2 entre el software TOR y el nodo intermedio (Middle Relay).

Conexión con el nodo de salida

Finalmente el Software TOR selecciona un nodo de salida (Exit Relay). Una vez seleccionado el nodo se cifra esta información con la clave de sesión 1 y con la clave de sesión 2.

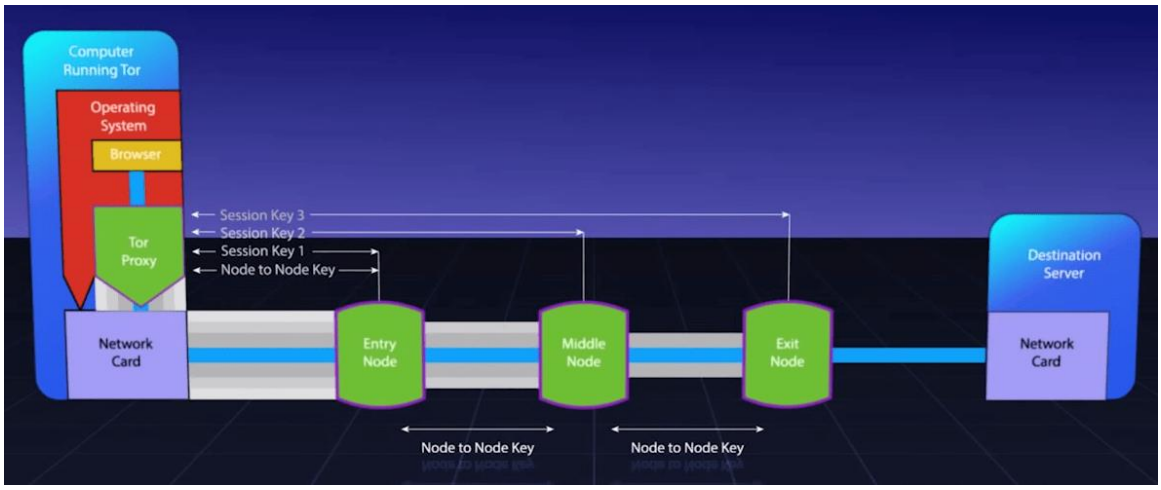
El mensaje que contiene el nodo de salida se envía desde el Software TOR al nodo de entrada. En el nodo de entrada se descifra parte del mensaje con la clave de sesión 1 y a posteriori se envía el al nodo intermedio.

Una vez el mensaje llega al nodo intermedio se usa la clave de sesión 2 para descifrar totalmente el mensaje. Acto seguido el nodo intermedio establecerá una conexión segura con el nodo salida (Exit Relay) mediante el protocolo TLS.

Al establecerse la conexión se informará de forma segura al Software TOR de nuestro ordenador que la conexión entre el nodo intermedio y el nodo de salida se ha establecido. Acto seguido se creará una clave de sesión 3 entre el software TOR y el nodo de Salida.

Finalmente el nodo de salida de la red TOR será el encargado de contactar con el destino que en nuestro caso será https://geekland.eu

Seguidamente pueden ver una representación gráfica de todo el proceso que acabamos de comentar.



Una vez definida la ruta ya podemos pasar a ver el procedimiento de cifrado usado por TOR.

Nota. Como medida de seguridad cada 10 minutos se establecerá una nueva ruta de conexión de forma automática. En los archivos de configuración de TOR podremos modificar este tiempo o si lo precisamos también podemos forzar que se establezca una ruta de forma manual.

Método de cifrado de la red TOR

Una vez establecida la ruta cifraremos la totalidad de contenido de nuestra petición.

La totalidad del contenido de nuestra petición estará cifrado mediante criptografía asimétrica. Su funcionamiento es el siguiente:

Antes de entrar en el nodo de entrada la totalidad de nuestra información se cifra por capas del siguiente modo:

Nota: Procedimiento suponiendo que hay en nodo de entrada, un nodo intermedio y un nodo de salida.

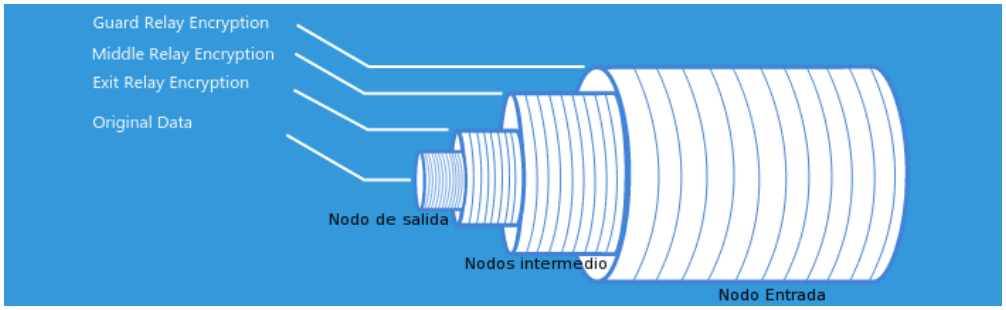
1. Se usa la clave pública del nodo de salida para cifrar la totalidad de contenido de nuestra petición. De esta forma añadimos una capa de cifrado y aseguramos que únicamente el último nodo podrá descifrar nuestro mensaje.
2. Al mismo tiempo se usa la clave pública del nodo intermedio y de este modo se aplica una segunda capa de cifrado a nuestra petición.
3. Finalmente se usa la clave pública del nodo de entrada para añadir una tercera capa de cifrado a nuestra petición.

Una vez finalizada la etapa de cifrado nuestra petición entra en el nodo de entrada y empezará la transmisión y descifrado de nuestra petición.

Proceso de descifrado de nuestra petición

Una vez seleccionada la ruta y cifrada la totalidad de nuestra información, TOR realizará las siguientes acciones:

1. La totalidad de información de nuestra petición y/o mensaje entra dentro del nodo de entrada. Usando la clave privada del nodo de entrada quitaremos la primera de las 3 capas de cifrado. Como el mensaje aún tiene dos capas de cifrado será completamente imposible que el nodo inicial pueda ver nuestro contenido.
2. Seguidamente nuestra petición y/o mensaje se dirigirá al nodo intermedio. Allí usaremos la clave privada del nodo intermedio para quitar la segunda de las 3 capas de cifrado.
3. Para finalizar en el nodo de salida se usará la clave privada del nodo de salida para quitar la última de las capas de cifrado de nuestra petición. Una vez nuestro mensaje está sin cifrar se procederá a la entrega de nuestra petición al servidor, y el servidor nos dará respuesta repitiendo de nuevo el procedimiento que acabamos de describir.



Representación del proceso de descifrado del mensaje

Beneficios obtenidos al usar el enrutado cebolla de la red tor

Una vez conocemos el funcionamiento de la red TOR resulta fácil deducir que su uso implica lo siguiente:

1. Ninguno de los nodos conoce la ruta completa de nuestra petición. Únicamente conocen el nodo que les suministra nuestra petición y el nodo al que le envían nuestra petición. Este hecho es bueno para mejorar nuestra privacidad.
2. Ninguno de los nodos, a excepción del nodo final, puede consultar el contenido o información que estamos enviando o recibiendo. Este es debido a que cada uno de los nodos va quitando una capa de cifrado y hasta que no llegamos al nodo de salida hay capas de cifrado.
3. Nuestra petición o información tiene que pasar forzosamente por los nodos establecidos inicialmente. En caso contrario no se podrá descifrar nuestra petición y por lo tanto nunca obtendremos una respuesta del servidor.
4. Cada uno de los nodos únicamente conoce la información que necesita saber que es la la clave privada para poder descifrar nuestra petición y el siguiente nodo en el que se tiene que enviar la información. Así de este modo aunque un nodo intermedio estuviera comprometido no pasaría absolutamente nada.

   Gracias a estos 4 puntos tenemos ciertas garantías que al usar la red TOR y el enrutado de cebolla podemos mejorar considerablemente nuestra privacidad en la red.

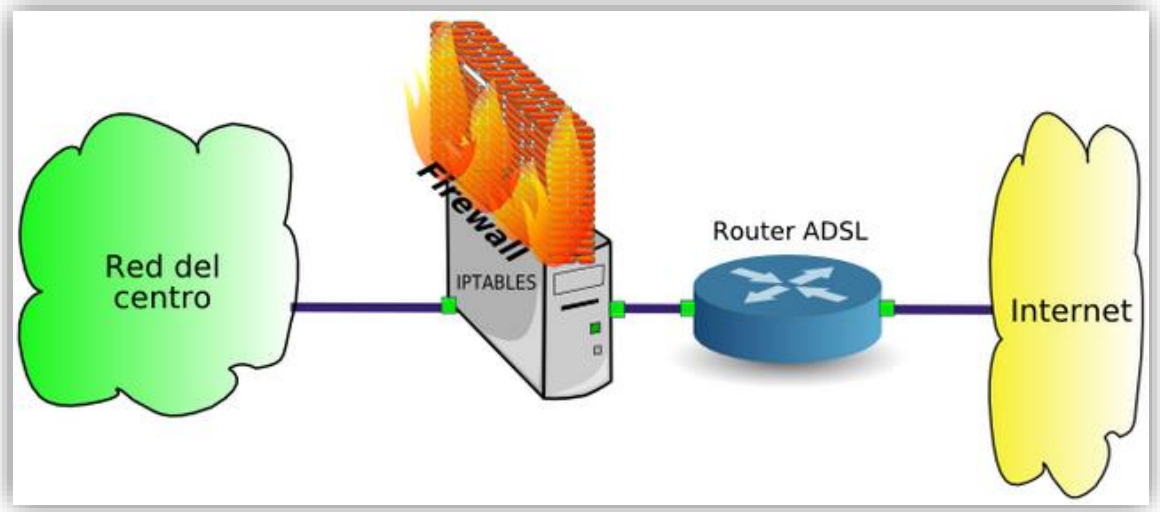
IPTABLES

¿Qué es y para qué se usa?

El cortafuegos utilizado para gestionar las conexiones en Linux es iptables.

Las posibilidades de iptables son prácticamente infinitas y un administrador que quiera sacarle el máximo provecho, puede realizar configuraciones extremadamente complejas.

Para simplificar, diremos que básicamente, iptables permite crear reglas que analizarán los paquetes de datos que entran, salen o pasan por nuestra máquina, y en función de las condiciones que establezcamos, tomaremos una decisión que normalmente será permitir o denegar que dicho paquete siga su curso.



El cortafuegos controla las comunicaciones entre la red y el exterior

Para crear las reglas, podemos analizar muchos aspectos de los paquetes de datos. Podemos filtrar paquetes en función de:

Tipo de paquete de datos

- Tipo INPUT: paquetes que llegan a nuestra máquina
- Tipo OUTPUT: paquetes que salen de nuestra máquina
- Tipo FORWARD: paquetes que pasan por nuestra máquina

Interfaz por la que entran (-i = input) o salen (-o = output) los paquetes

- eth0, eth1, wlan0, ppp0, …

IP origen de los paquetes (-s = source)

- IP concreta, ej: 10.0.1.3
- Rango de red, ej: 10.0.1.0/8

IP destino de los paquetes (-d = destination)

- IP concreta, ej: 10.0.1.3
- Rango de red, ej: 10.0.1.0/8

Protocolo de los paquetes (-p = protocol)

- Tcp, udp, icmp…

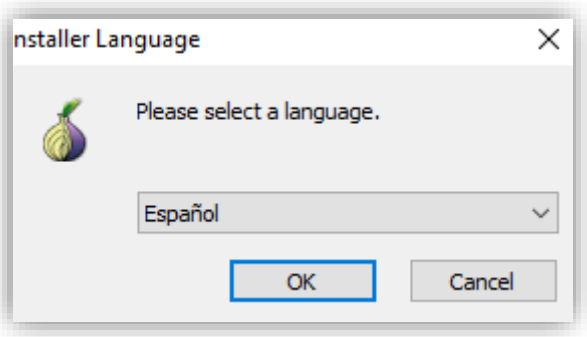
Hacer NAT (modificar IP origen y destino para conectar nuestra red a otra red o a Internet) y…

- Filtrar antes de enrutar: PREROUTING
- Filtrar después de enrutar: POSTROUTING

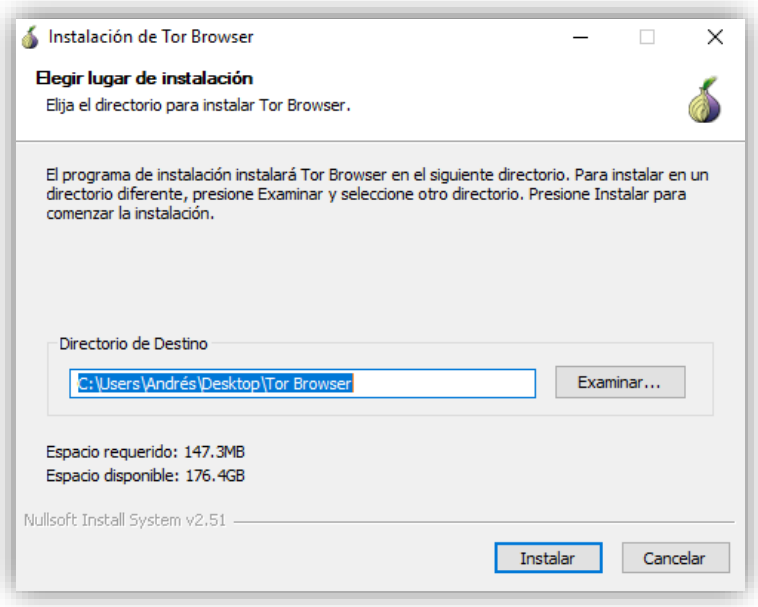
Navegador TOR

Descargamos desde el navegador TOR, desde la página TorProject (https://www.torproject.org/download/download-easy.html.es)

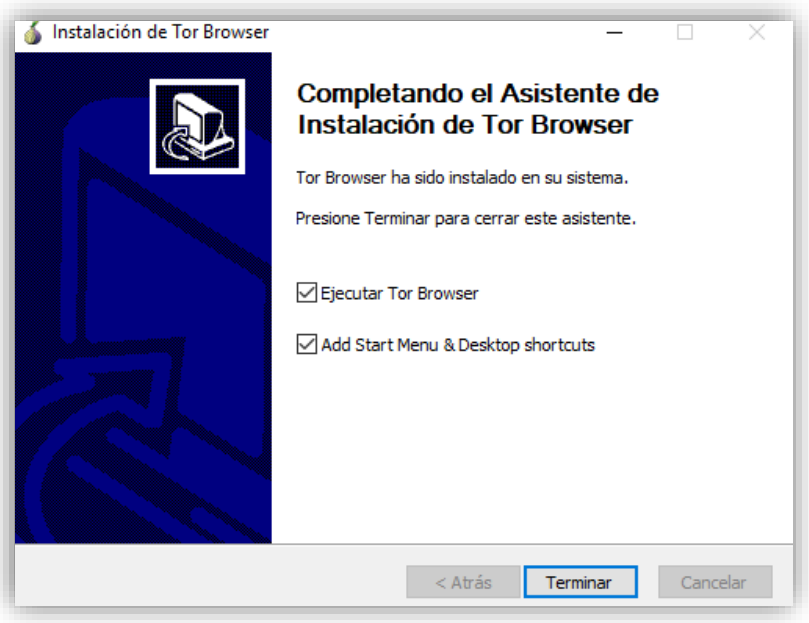
Se abrirá una pequeña ventana preguntando qué idioma desea utilizar para el Navegador Tor. Hay varios para elegir. Elija el idioma que desee y haga clic en el botón OK.



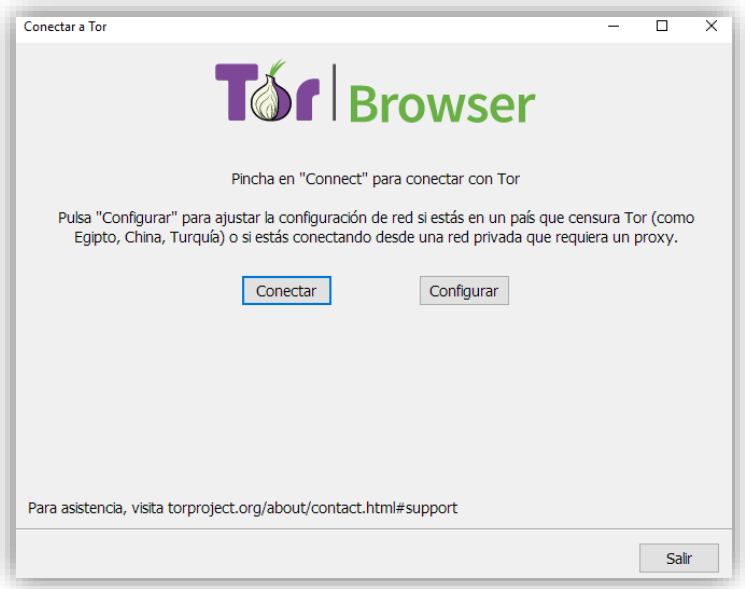
Encontrará una nueva ventana que le indicará dónde se instalará Tor Browser. La ubicación predeterminada es su escritorio. Puede cambiarlo a una ubicación diferente si se desea, pero por ahora mantenga el valor predeterminado.



El proceso de instalación se completa cuando ve una ventana que indica que ha completado el proceso de instalación. Si hace clic en el botón Finalizar, el Navegador TOR se iniciará de inmediato y los accesos directos de "Inicio TOR Navegador" se agregarán al Menú Inicio y al Escritorio.



La primera vez que el Navegador TOR arranque en su computadora, aparecerá una ventana que le permitirá modificar algunos ajustes si es necesario. Es probable que tenga que regresar y hacer algunos cambios en los ajustes de configuración, pero continúe y trate de conectarse a la red TOR haciendo un clic al botón de Conectar/Connect.



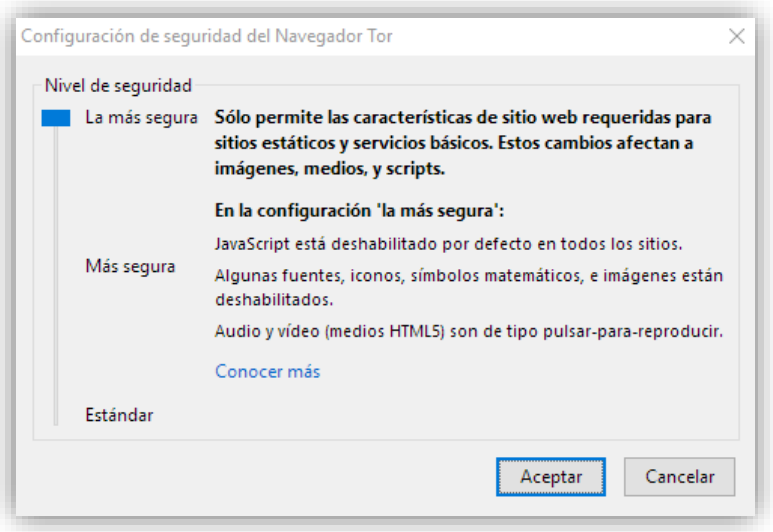
La primera vez que el Navegador TOR inicie, le damos a conectar, ya que configuraremos TOR, desde raspberry, y nos encargaremos nosotros de crear el proxy.

Haga clic en el logo de la cebolla TOR en la parte superior izquierda del navegador, luego a la configuración de Privacidad y Seguridad.

Algunas opciones de un navegador web normal pueden hacerle vulnerable a un ataque intruso del tipo “ataque por intermediario”. Otras características han tenido errores de software o “bugs” en ellas que han revelado la identidad de los usuarios.

Deslizando los niveles de Seguridad al nivel más alto desactiva estas características. Esto lo hará más seguro de los atacantes que pueden interferir con su conexión de Internet o aprovechar nuevos errores en estas características.

Desafortunadamente, al desactivar estas características puede hacer que algunos sitios web no se desplieguen por completo. El nivel bajo por defecto está bien para una protección diaria, pero lo puede elevar si está preocupado por atacantes sofisticados, o si no le molesta que algunos sitios web no se desplieguen correctamente.

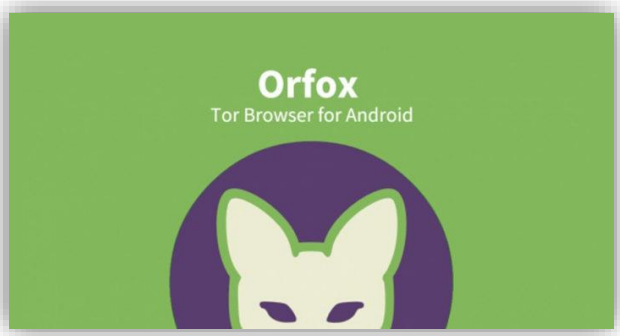


Consejos a la hora de navegar con TOR

- Usá el Navegador TOR
- No uses torrent sobre TOR
- No habilites ni instales plugins en el navegador
- Usá versiones HTTPS de los Sitios
- No abras documentos, descargados de TOR mientras estes online
- Deshabilitar javascript de todos los sitios
- Deshabilitar reproducción automática en medios multimedia
- No maximizar la ventana del navegador puede permitir a los sitios web determinar el tamaño del monitor, lo que puede usar para rastrearnos.

Nota :

The Guardian Project, los responsables del navegador de escritorio ultra-seguro **TOR**, han lanzado **Orfox**, la versión para dispositivos Android.



Documentación

- **Adafruit**
- **TOR**
- **Rasperry Pi**
- **Raspbian**

Temporalización : 40 horas aproximadas

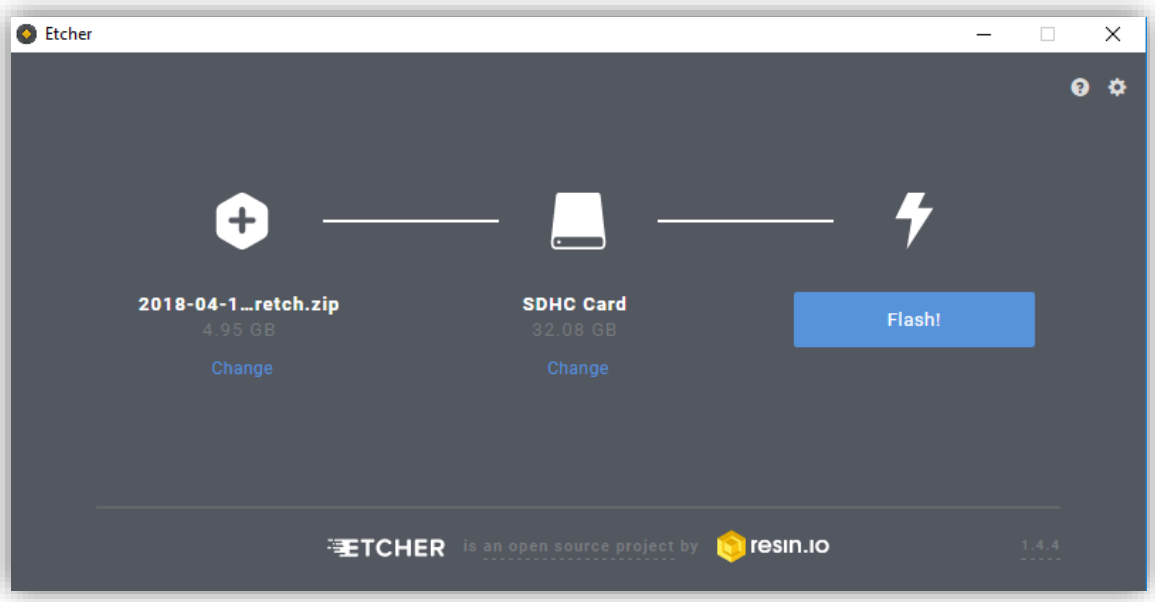
5. Configuración paso a paso de Onion Pi.

Pasos iniciales

Lo primero que debemos hacer es instalar el sistema operativo en nuestro Raspberry Pi. En nuestro caso hemos utilizado la última versión de **Raspbian**.

Para ello vamos a usar el software llamado **Etcher,** es una aplicación gratuita y de código abierto desarrollada para facilitar en todo lo posible la grabación de imágenes ISO, IMG y otros formatos comprimidos directamente y de forma segura a memorias USB y tarjetas de memoria.

Tiene una interfaz sencilla con seleccionar la imagen, el dispositivo de almacenamiento y presionar flash.



Una vez instalado el sistema operativo en nuestro micro SD, la insertamos en nuestra raspberry y la encendemos y esperamos a que se inicie Raspbian.

Una vez configurado y con el dispositivo funcionando y conectado a Internet mediante RJ-45 actualizamos las fuentes de software, las aplicaciones y el sistema tecleando:

```
sudo apt-get update -y
sudo apt-get upgrade -y
sudo apt-get dist-upgrade -y
```

***apt-get update**: actualiza la lista de paquetes disponibles y sus versiones, pero no instala o actualiza ningún paquete. Esta lista la coge de los servidores con repositorios que tenemos definidos en el *sources.list*, es decir, donde se enlistan las "fuentes" o "repositorios" disponibles de los paquetes de software candidatos a ser: actualizados, instalados, removidos

***apt-get upgrade**: una vez el comando anterior ha descargado la lista de software disponible y la versión en la que se encuentra, podemos actualizar dichos paquetes usando este comando: apt-get upgrade. Instalará las nuevas versiones respetando la configuración del software cuando sea posible (esta es la maravilla de este tipo de sistemas).

***apt-get dist-upgrade**: es un actualizador completo diseñado para simplificar la actualización entre publicaciones de Debian. Utiliza un sofisticado algoritmo para diseñar el mejor conjunto de paquetes a instalar, actualizar y eliminar para así obtener cuanto sea posible de la última publicación.

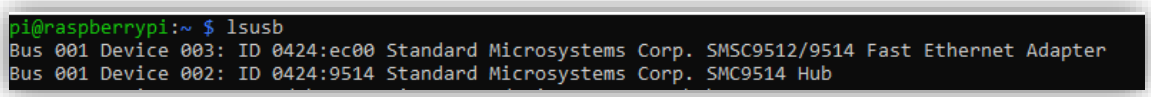
***Uso el comodin **–y** (yes) para que acepte todas las peticiones que pida la terminal

Una vez con nuestro sistema actualizado podemos seguir con la configuración de nuestra Raspberry Pi para funcionar como un punto de acceso.

Comprobar que nuestra tarjeta USB Wi-Fi es detectada y funciona en modo AP (Punto de Acceso)

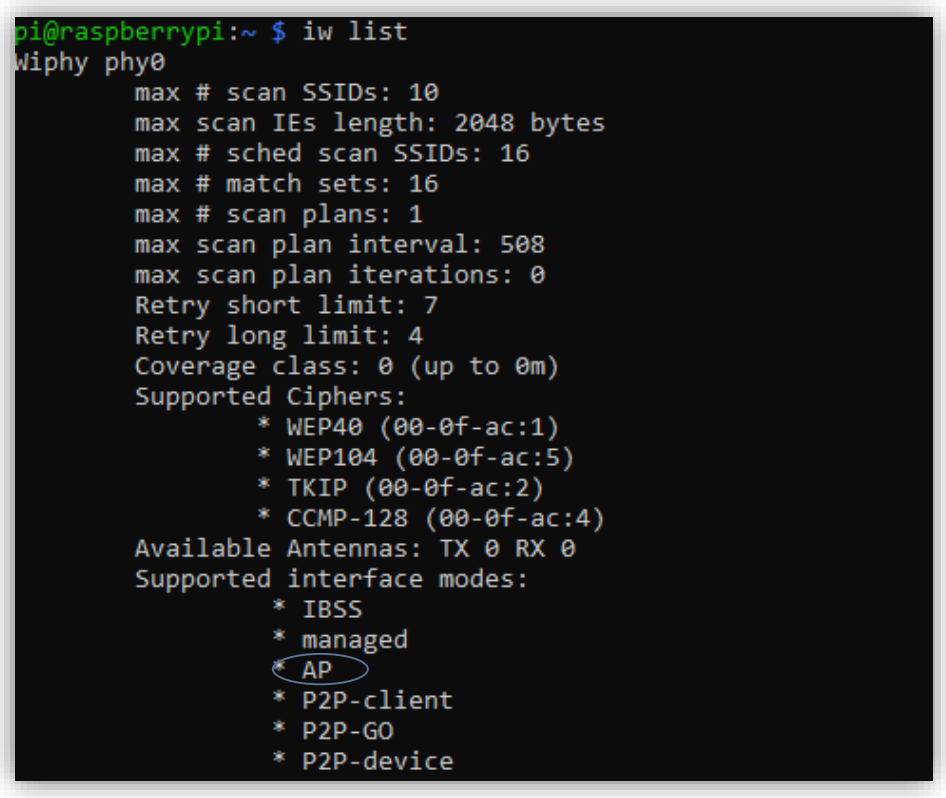
Lo primero que haremos será comprobar que el dispositivo detecta la tarjeta. Para ello tecleamos:

```
Lsusb
```



Y nos debería aparecer allí listada. Una vez que aparece ejecutaremos otro comando para comprobar que la tarjeta Wi-Fi puede funcionar en **modo AP** (punto de acceso):

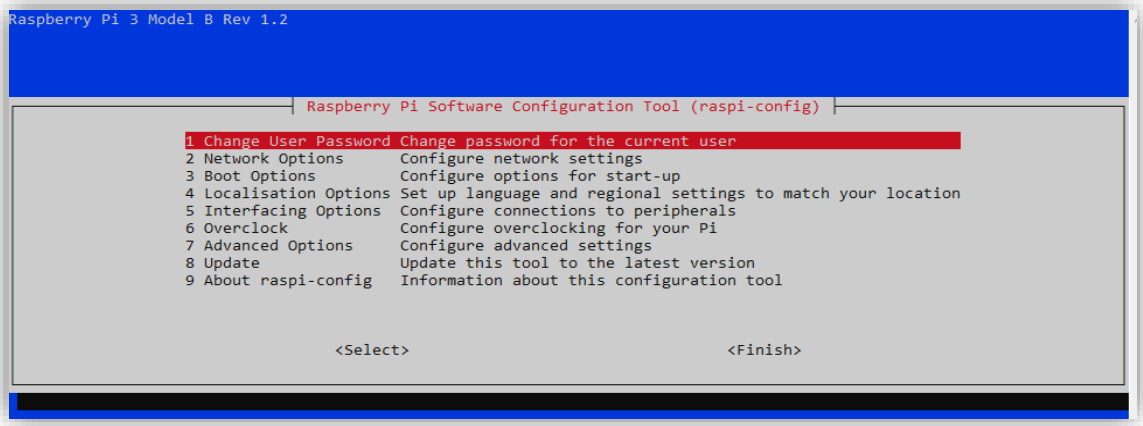
```
iw list
```



Si en el resultado que nos aparece en pantalla podemos ver la línea: Modes: **AP**, la tarjeta es compatible para realizar esta configuración, de lo contrario, debemos buscar otra tarjeta cuyo chipset permita configurarla como **punto de acceso**, o AP.

Como tenemos que usar sudo (**Permisos de administrador**), debemos de cambiar la contraseña por la que tiene por defecto, se puede cambiar entrando en la configuración de raspberry pi, tecleando :

```
sudo raspi-confi
```



Seleccionamos la primera opción que es para cambiar de contraseña.

Instalar software necesario y dependencias

La mayor parte del software necesario viene por defecto instalado en **Raspbian**, aunque los únicos que podrían darnos problemas son el servidor **DHCP**, el servicio de creación de puntos de acceso (**hostapd**), y el firewall **IPTABLES** que podemos instalar manualmente (en caso de no estar disponible) tecleando:

```
sudo apt-get install isc-dhcp-server hostapd -y

  sudo apt-get install iptables-persistant -y
```

Una vez llegados a este punto podemos reiniciar nuestro Raspberry para empezar con la configuración.

Configuración

Todas las configuraciones se realizan desde el terminal, a modo texto. Nosotros vamos a utilizar el editor **nano**.

```
sudo nano /etc/dhcp/dhcpd.conf
```

El servidor DHCP de ISC se configura a través del fichero ***/etc/dhcp/dhcpd.conf***, el cual es un fichero de texto que contiene declaraciones y estamentos, y estos últimos pueden ser estamentos condicionales, opciones y parámetros. Con todo esto, lo que se pretende es:

- Especificar el comportamiento del servidor a través de parámetros.
- Definir los valores que se enviarán a los clientes, fundamentalmente a través de opciones (también pueden usarse algunos parámetros).
- Determinar cómo el servidor interactuará con otros servicios (DNS, OMAPI y parejas DHCP failover)
- Describir los segmentos de red que constituyen toda la red física, tanto los que el servidor atiende como los que no.

Las ***declaraciones*** se evalúan una sola vez, concretamente cuando se arranca el servidor y se lee el fichero de configuración, guardándose todo su contenido en una base de datos en la memoria RAM. Los ***estamentos*** se evalúan cada vez que se recibe una petición por parte de un cliente, y será el ámbito en el que aparezca el *estamento* el que determine si se evaluará o no para un cliente dado.

Las opciones y los parámetros normalmente son manipulados de la misma forma, con la diferencia de que los parámetros indican cómo trabajará el servidor DHCP y las opciones qué información se enviará a los clientes.

En este punto se va a explicar el papel que cumplen muchas de las distintas declaraciones y estamentos que podemos escribir en él.

Algunos convenios de este fichero son los siguientes:

- El signo # comienza un comentario hasta el final de la línea y puede ponerse en cualquier lugar.
- No se distingue entre mayúsculas y minúscula.
- Todos los estamentos deben acabar con el signo de punto y coma (;). Las declaraciones que definen un ámbito mediante los signos { y } no finalizan en punto y coma.

En este archivo debemos buscar una serie de líneas. Las siguientes están por defecto sin comentar, las comentamos con una almohadilla # delante de manera que dejen de estar habilitadas quedando de la siguiente manera:

```
#option domain-name "example.org";
#option domain-name-servers ns1.example.org,  ns2.example.org;
```

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
#option domain-name "example.org";
#option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;
```

***Lo comentamos por si vamos a usar algún nombre de dominio.**

Buscaremos el elemento #authoritative; que por defecto estará comentado y lo descomentamos para activarlo, quedando:

```
authoritative;
```

```
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;
```

***Lo vamos a descomentar para usar el servidor dhcp para la red local**

Para finalizar configuraremos la red en la que funcionará el servidor DHCP (en nuestro ejemplo en la red 192.168.100.1). Para ello nos situamos al final del documento y añadimos:

```
#Rango IP

subnet 192.168.100.0 netmask 255.255.255.0{
option broadcast-address 192.168.100.255;
default-lease-time 600;
max-lease-time 7200;
option domain-name "local";
option routers 192.168.100.1;
option domain-name-servers 192.168.100.1;
range 192.168.100.133 192.168.100.193;
}
```

Guardamos los cambios y cerramos el archivo.

Vamos a editar el fichero **/etc/default/isc-dhcp-server** para indicar la interfaz de escucha del DHCP:

```
sudo nano /etc/default/isc-dhcp-server
```

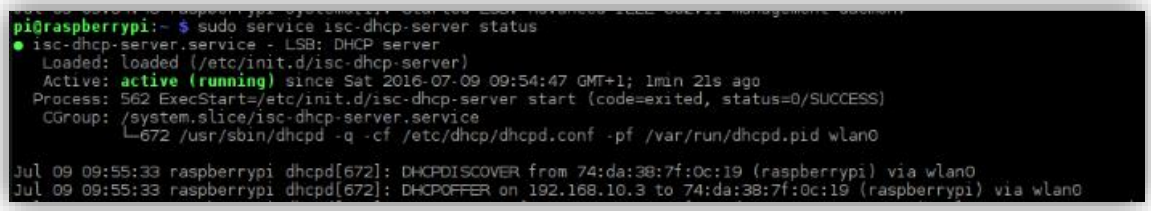
Como el ordenador va a usar el servidor DHCP y tiene más de una interfaz de red, puede que necesitemos que éste no trabaje por todas las interfaces, es decir, que sólo atienda peticiones por **IPV4**. Para hacer esto debemos modificar la variable ***INTERFACES,*** que escuche estas peticiones por la interfaz **wlan0** que es la red wifi

```
INTERFACES="wlan0"
```

Comprobamos que el servidor DHCP esté en funcionamiento con el comando :

```
sudo service isc-dhcp-service status
```

(previamente haberlo reiniciado o iniciado)



El servidor DHCP ya está configurado.

Configurar la conexión WLAN y Ethernet

Lo primero que haremos será desconectar la tarjeta Wi-Fi. Para ello tecleamos:

```
sudo ifdown wlan0
```

***Ifdown quita una interfaz de red, colocándola en un estado donde no puede transmitir ni recibir datos.**

A continuación abriremos el fichero "dhcpcd.conf":

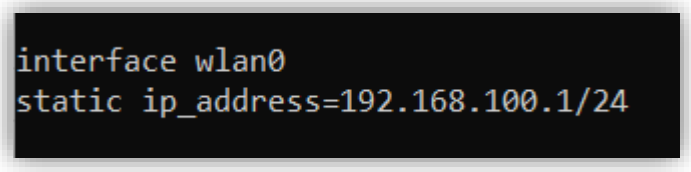
Es el fichero para configurar las interfaces de red, en este caso para poner wlan0 como IP estática, es decir, es una IP asignada a un dispositivo y nunca se modifica, entonces si la raspberry se reinicia o se apaga seguirá teniendo la misma IP.

```
sudo nano /etc/dhcpcd.conf
```

Y lo configuraremos de la siguiente manera:

```
interface wlan0
static ip_address=192.168.100.1/24
```

***/24** = hace referencia a la máscara de red, es decir, 255.255.255.0



Para aplicar los cambios al momento debemos teclear:

```
sudo ifconfig wlan0 192.168. 2.1
```

Es para activar la interfaz que anteriormente habíamos desactivado, le indicamos la ip que quiere que use la interfaz.

Configurar el punto de acceso

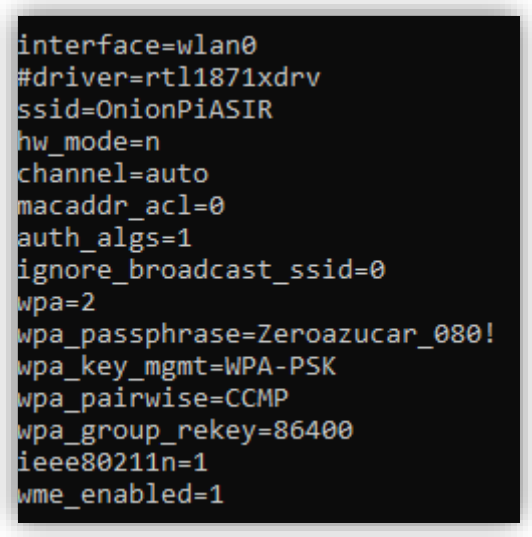
Una vez más, editaremos otro fichero tecleando:

Crearemos un fichero que se encargará de la configuración del punto de acceso en este caso lo podemos llamar "**hostapd.conf**", dentro del directorio de hostapd.ho

```
sudo nano /etc/hostapd/hostapd.conf
```

Crearemos una red protegida con contraseña para mayor seguridad. Crea un nuevo fichero con la siguiente línea:

```
interface=wlan0
#driver=rtl1871xdrv
ssid=OnionPiASIR
hw_mode=n
channel=auto
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase= Zeroazucar_080!
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_group_rekey=86400
ieee80211n=1
wme_enabled=1
```



A continuación detallaré el contenido mostrado:

- **interface=wlan0**: nombre de la interfaz que vamos a utilizar como punto de acceso
- **driver= rtl871xdrv**: El que he usado aquí, el rtl871xdrv es genérico.
- **ssid=xxxxx**: nombre que le vamos a dar a nuestro punto de acceso
- **hw_mode=n**: modo de red usado por la red wifi. Puede ser a (11mbps), b (22mbps) y g (54mbps). El modo n (104mbps) se configura aparte, con otro parámetro.
    - **`ieee80211n=1`** si está a 1, el modo de la wifi es el n (104mbps)
- **channel=auto**: canal usado la red wifi creada. Debe estar entre 1 y 11, pero recordemos los canales se superponen físicamente en el espacio de frecuencias, y

que los canales óptimos para que no existan conflictos son 1, 6 y 11. Versiones modernas de hostapd permite el valor "auto", de tal forma que se busca el canal menos saturado dentro del entorno donde esté la red wifi.

- **macaddr_acl=0**: con valor 1 activa el filtro MAC en el punto de acceso, puesto a 0 lo desactiva.

- **ignore_broadcast_ssid=0**: Para desactivar que este la ssid oculta.

- **1** = oculta la difusión del SSID de la red wifi. De esta manera ningún dispositivo normal podrá verla en su lista de redes wifi y solo podrá conectarse a ella dando su nombre exacto.

- **auth_algs=1**: algoritmo de autenticación (bit 0 = Open System Authentication, bit 1 = Shared Key Authentication)

- **wpa=2**: Para utilizar el cifrado WPA2

- **wpa_passphrase=xxxxx**: clave para acceder a nuestro punto de acceso.

- **wpa_key_mgmt**=WPA-PSK WPA-PSK-SHA256: algoritmos de gestión de claves aceptados.

- **wpa_pairwise=CCMP** es un protocolo de encriptación de IEEE 802.11i. Es obligatorio en el estándar WPA2.

- **wpa_group_rekey=86400.** Es el número de segundos del intervalo de renovación de la clave WPA. Cada cierto tiempo se aplica un "rekeying" (Cambio de llaves encriptadas).

- **wme_enabled=1** si está a 1, se activa el modo WME para funcionalidad HT (higth throughput-alto rendimiento) completa. Esto activa sistemas más potentes de modulación de la señal y uso de frecuencias que permite alcanzar velocidades más altas.

Para finalizar con la configuración abrimos un nuevo archivo de configuración tecleando:

```
sudo nano /etc/default/hostapd
```

Este fichero se encarga de la configuración de hostapd, por lo que descomentamos y cambiamos la línea #DAEMON_CONF="" por:

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

Para que recoja la configuración de nuestro punto de acceso que hemos creado anteriormente.

Guardamos y cerramos el archivo para finalizar. Ya casi hemos finalizado, sólo quedan unos ajustes menores y configurar Raspbian para que todo esto se ejecute al inicio del sistema de forma automática.

Volvemos a descomentar la línea y poner la misma ruta en el siguiente fichero tecleamos:

```
sudo nano /etc/init.d/hostapd
```

Cuando se inicie el sistema y carge el servicio hostapd recoja la configuración de nuestro punto de acceso.

Una de las posibilidades que nos ofrece **GNU/Linux** es la de poder actuar como enrutador, es decir, recibir paquetes, decidir la ruta de estos y reenviarlos por cualquiera de las interfaces de red existentes. Para hacerlo necesitamos modificar el parámetro del kernel denominado **ip_forward.**

El fichero de configuración **/etc/sysctl.conf** se utiliza para establecer algunos parámetros del kernel y que estos se mantengan entre sucesivos arranques del sistema, es decir, que los cambios sean persistentes. Esto es equivalente a cambiar valores en los archivos del directorio virtual /proc/sys, sólo que con este último método los cambios se pierden al apagar el sistema.

El nombre completo del parámetro que debemos modificar para que el equipo funcione como router se denomina **net.ipv4.ip_forward**, y su valor debe ser **1**. Para que este cambio se mantenga al reiniciar el sistema, editamos el fichero **/etc/sysctl.conf.**

editaremos este fichero tecleando:

```
sudo nano /etc/sysctl.conf
```

Y añade la siguiente línea al final del archivo:

```
net.ipv4.ip_forward=1
```

Tras este cambio reiniciamos el sistema y el equipo ya funcionará a partir de ahora como router; pero podemos hacer el cambio en caliente y ahorrarnos el reinicio. Hay varias formas de hacer esto:

- Directamente poniendo el 1 en el fichero del directorio */proc/sys* que se encarga de este parámetro. La forma de descubrir el fichero relacionado con un parámetro concreto del fichero */etc/sysctl.conf* es siempre la misma. Todos los ficheros están en */proc/sys*, y los puntos del parámetro separan directorios hasta el último que separa el nombre del fichero, de esta manera, el fichero que buscamos es el ***/proc/sys/net/ipv4/ip_forward***. Podemos escribir un 1 de la siguiente forma, sin necesidad de abrirlo con un editor:

```
sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"
```

Ejecuta las siguientes líneas para crear la traducción de red entre el puerto Ethernet eth0 y el puerto wifi wlan0 :

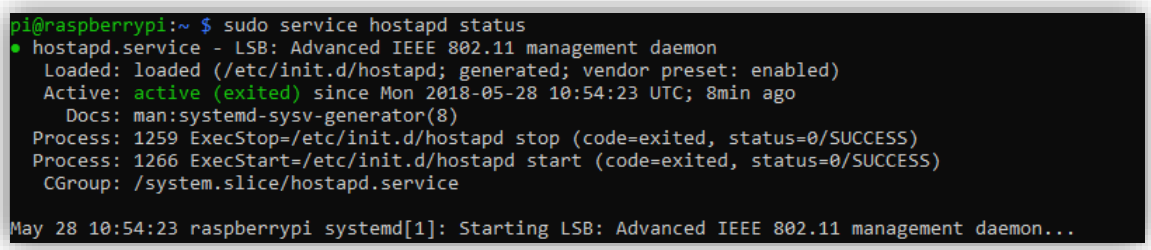
```
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state
              RELATED,ESTABLISHED -j ACCEPT

   sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

Para que toda la magia se arranque al iniciar con la herramienta ***iptables-persistent*** que instalamos al principio, hay que ejecutar lo siguiente:

```
sudo sh -c "iptables-save > /etc/iptables/rules.v4"
```

Comprobamos si el servicio de hostapd está activo tecleamos:

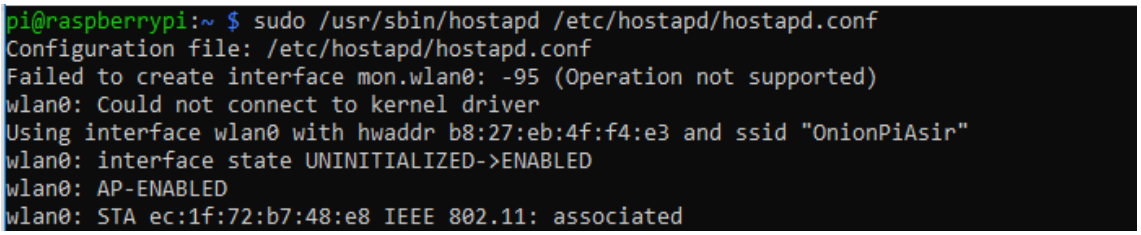
```
sudo service hostapd status
```



Por último, para ver que todo funciona correctamente:

```
sudo /usr/sbin/hostapd /etc/hostapd/hostapd.conf
```

Esto ejecuta hostapd manualmente con nuestro archivo de configuración.



Podemos buscar con nuestro ordenador o móvil para ver que nos encontraremos una nueva red wifi en este caso llamada "**OnionPiASIR**" y podremos acceder a internet.

El servicio hostapd ya está configurado.

Configurar TOR

Ya tenemos configurado nuestro punto de acceso, ahora toca configurar proxy anónimo con TOR.

Ahora toca instalar **TOR,** tecleamos:

```
sudo apt-get install tor -y
```

Ejecuta el siguiente comando:

```
sudo nano /etc/tor/torrc
```

Y pega el siguiente código con el que empezamos a configurar la red justo debajo de la línea que pone ##https://www.torproject.org/docs#torrc:

```
##
## Tor will look for this file in various places based on your platform:
## https://www.torproject.org/docs#torrc

Log notice file /var/log/tor/notices.log
VirtualAddrNetwork 10.192.0.0/10
AutomapHostsSuffixes .onion,.exit
AutomapHostsOnResolve 1
TransPort 9040
TransListenAddress 192.168.100.1
DNSPort 53
DNSListenAddress 192.168.100.1
```

- **Log notice file /var/log/tor/notices.log**: Este fichero aun no estará creado pero lo ponemos previamente, que indica que nos registre en este fichero todos los mensajes sobre TOR como por ejemplo los errores que tenga.

- **VirtualAddrNetwork 10.192.0.0/10**: la dirección de red que usará para salir y con la cual será identificada fuera de la red.

- **AutomapHostsOnResolve 1**: Cuando esta opción está habilitada, y obtenemos una solicitud para resolver una dirección que finaliza con uno de los sufijos de **AutomapHostsSuffixes**.

- **AutomapHostsSuffixes .onion,.exit**: En esta opción añadimos los sufijos que queramos buscar con TOR, la lista de sufijos ira separada por comas.

- **TransPort 9040 y DNSPort 53:** Esto le indicará a TOR que reenvíe el tráfico redirigido al puerto 9040 y reenvíe las solicitudes del servidor de nombres de dominio en el puerto 53.

- **TransListenAddress 192.168.100.1 y DNSListenAddress 192.168.100.1:** Tanto la dirección IP como el DNS escuchara por la misma dirección 192.168.100.1

Cambia las tablas de enrutamiento IP para que las conexiones a través de la interfaz WiFi (wlan0) sean enrutadas a través del software TOR. Escribe lo siguiente para eliminar las reglas antiguas de la tabla IP NAT:

```
sudo iptables -F
sudo iptables -t nat –F
```

Las siguientes configuraciones nos permitirán, por este orden, acceder a través de SSH agregando una excepción para el puerto 22, enrutar el DNS desde el adaptador wlan0 al puerto interno 53 y por último, enrutar todo el tráfico TCP del adaptador wlan0 al puerto 9400 (TransPort en nuestro torrc):

```
sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 22 -j REDIRECT --to-ports 22
sudo iptables -t nat -A PREROUTING -i wlan0 -p udp --dport 53 -j REDIRECT --to-ports 53
sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --syn -j REDIRECT --to-ports 9040
```

Lo guardaremos en nuestro antiguo archivo NAT para conservar toda la configuración, así se cargará automáticamente cuando se configure la red al reiniciar:

```
sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"
```

Crea los ficheros de log necesarios para hacer "**debug**", es decir, para que el sistema escriba errores si los hay y poder saber qué es lo que está pasando. Con las siguientes instrucciones lo creamos, le asignamos el usuario y le damos permisos.

```
sudo touch /var/log/tor/notices.log
sudo chown debian-tor /var/log/tor/notices.log
sudo chmod 644 /var/log/tor/notices.log
```

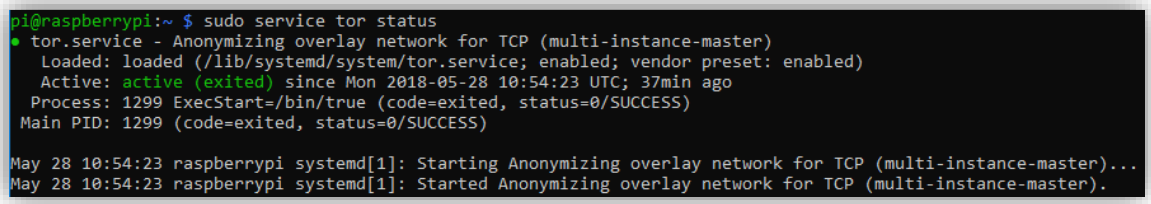
Comprobamos que existen con:

```
ls -l /var/log/tor
```

y arranca el servicio manualmente:

```
sudo service tor start
```

Comprueba que todo ha ido bien y que el servicio está levantado:



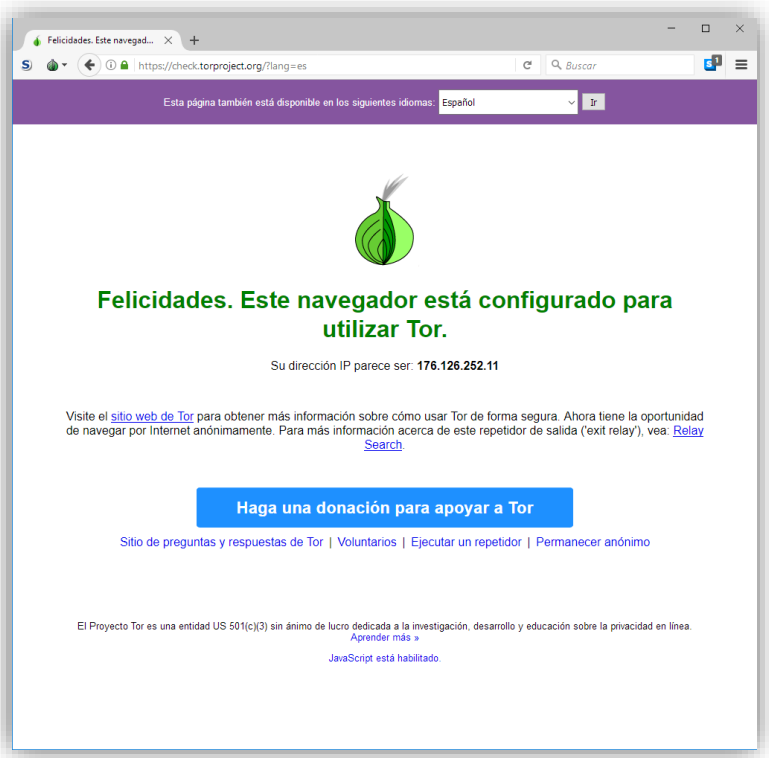
Y, por último que se ejecute en los siguientes arranques, ejecutamos lo siguiente con todos los servicios usados:

```
sudo update-rc.d tor enable
sudo update-rc.d isc-dhcp-server enable
sudo update-rc.d hostapd enable
```

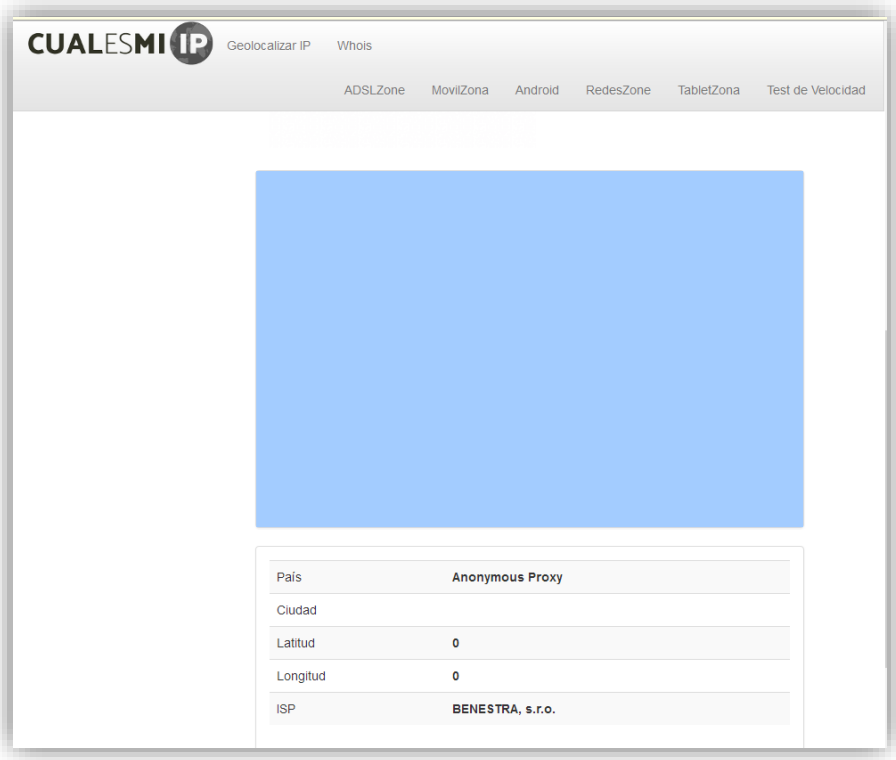
Ahora sólo falta probarlo. Conectar cualquier otro equipo con WiFi a la red recién creada, y usar el navegador de **TOR** o en dispositivos móviles será necesario usar **Orfox**.

Para comprobar que el proxy está funcionando, una de las formas más rápidas es visitando un sitio web como **https://check.torproject.org/** que mostrará tu dirección IP tal como la ve la web y también nos dirá si está en funcionamiento nuestro proxy y si podemos usar TOR.

TOR ya está configurado.



Y si hacemos una comprobación de nuestra geolocalización de nuestra dirección IP, nos mostrará lo siguiente.



Nos no podrá mostrar donde estamos ubicados, ya que no sabe dónde corresponde nuestra dirección IP, nos dirá que estamos usando un proxy anónimo.

Un ejemplo claro que podemos usar nuestra Onion Pi es para navegar por la Deep web, ahora bien:

¿Qué es la deep web?

El concepto de deep web es sencillo. La deep web es aquella parte de la red que contiene material, información y páginas web que no están indexadas en ninguno de los buscadores existentes como pueden ser **bing, google, yahoo**, etc. Así en el hipotético caso que los buscadores pudieran indexar la totalidad de contenido en la web significaría que desaparecería la deep web.

No obstante esto es imposible ya que muchas de las páginas y documentos están hechos de tal forma que no puedan ser indexables, ya sea porque están protegidos con contraseña, porqué están realizados en formatos no indexables como por ejemplo páginas realizadas completamente en flash, sin contenido html, etc.

¿Qué tamaño tiene la deep web?

Muchos de vosotros quedareis sorprendidos en saber que la deep web presenta mucho más contenido que la web superficial que nosotros podemos acceder. Según datos de la Wikipedia en el año 2000 la internet superficial tenía un tamaño de 167 Terabytes mientras que la deep web tenía un tamaño de 7500 Terabytes lo que significa que el contenido de la deep web era 45 veces superior a la información que teníamos acceso en aquel momento. Actualmente a día de hoy la universidad de **California en Berkeley** estima que el tamaño real de la red profunda es de 91.000 Terabytes.

¿Qué podemos encontrar en la deep web?

Todo lo que hay en la deep web no podemos decir que sea intrínsecamente malo. Podemos encontrar contenido interesante y diverso como por ejemplo:

Contenido almacenado por los gobiernos de distintos países.

Organizaciones que almacenan información. Por ejemplo la **NASA** almacena información acerca de las investigaciones científicas que realiza. Otro de información almacenada puede ser datos meteorológicos, datos financieros, directorios con información de personas, etc.

Multitud de bases de datos de distinta índole. Las bases de datos representan un % muy importante de la información almacenada en la **deep web**.

- **Foros de temáticas diversas**.

No obstante también nos podemos encontrar contenido muy desagradable como por ejemplo los siguientes:

- **Venta de drogas.**
- **Pornografía.**
- **Mercado negro de sicarios.**

Documentos clasificados como por ejemplo los de **wikileaks**. (Bueno diría que esto malo no es.)

- **Foros de crackers en busca de víctimas.**
- **Phishers, spammers, botnet agents, en busca de víctimas.**
- **Páginas para comprar o fabricar armas.**
- **Piratería de libros, películas, música, software, etc.**

Nota: Afortunadamente el contenido que se acaba de describir representa un % muy pequeño de lo que es la deep web. Este tipo de contenido se clasifica dentro de una sub categoría de la deep web denominada darknet.

Nota: Cabe destacar que el 90% de contenido que existe en la deep web es accesible para la totalidad de usuarios.

Cuando accedemos a la Deep web, nos percataremos de que todos los enlaces terminará con el dominio .onion.

¿Qué son los dominios .onion?

Es un pseudo dominio de nivel superior genérico que indica una dirección IP anónima accesible por medio de la **red TOR**.

Las direcciones son resultado de una combinación de 16 caracteres alfanuméricos generados sistemáticamente basándose en una clave pública cuando TOR es configurado. Esa combinación de 16 caracteres puede ser creada con cualquier letra del alfabeto y con dígitos decimales que empiecen por 2 y acaben en 7 representando así un número de 80-bit en base 32.

Forman parte de la **Deep Web**. Aunque tales direcciones no son en realidad DNS, los buscadores web pueden acceder a sitios .onion usando proxy y enviando la solicitud a través de servidores de la red TOR. El objetivo de usar este sistema es hacer que tanto el distribuidor de información como el receptor sean difícilmente trazables, ya sea entre ellos, o por un tercero.

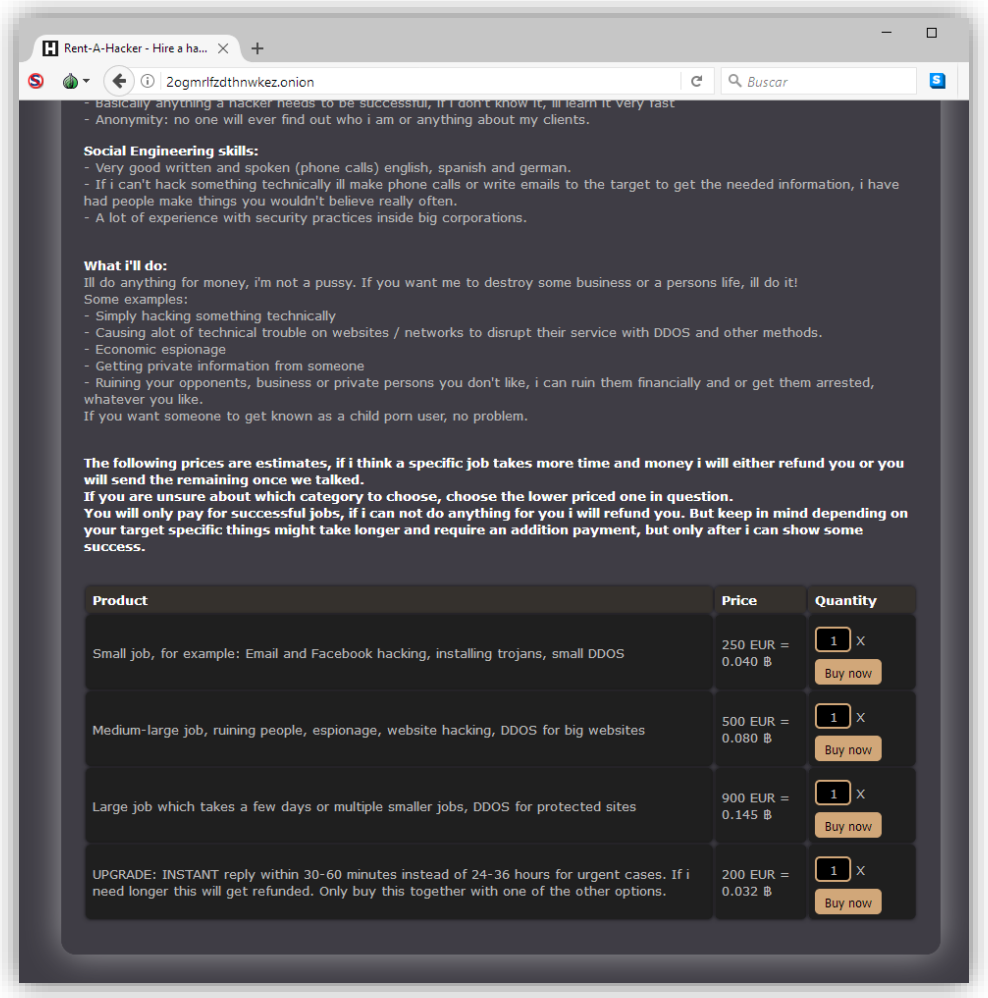
En la web de la "superficie" podemos hacer un seguimiento, o encontrar webs por medio de buscadores. En la Deep Web no hay buscadores, (sólo algunos facilitadores), el usuario

debe conocer la web que va a visitar, muchas veces bajo contraseña. En la Deep Web se puede encontrar el contenido de la web tradicional pero también todo aquello que no aparece en ella.

Imagen de los tipos de niveles que encontramos en la Deep Web.

Ejemplo:

Buscando por la Deep Web, encontramos a un hacker que vende sus servicios a cambio de bitcoins para hacer ataques DDOS, “hacker Facebook”, instalar troyanos….



6. Bibliografía

- https://www.torproject.org/about/overview.html.es
- https://www.torproject.org/docs/documentation.html
- https://www.welivesecurity.com/la-es/2014/07/02/navegacion-anonima-tor-herramienta-cuidadosos-o-cibercriminales/
- https://learn.adafruit.com/onion-pi/do-more-dot-dot-dot
- http://histinf.blogs.upv.es/2013/12/18/raspberry-pi/
- https://www.raspberrypi.org/forums/viewtopic.php?t=77879
- https://es.scribd.com/doc/225682222/Raspberry-Pi-Guia-Del-Usuario-2da-Ed-en-Espanol
- https://blog.desdelinux.net/iptables-para-novatos-curiosos-interesados/
- https://www.raspberrypi.org/forums/viewtopic.php?t=111887
- https://arenlasysadmin.wordpress.com/2013/05/05/ejecutar-script-arranque-linux/
- http://maslinux.es/ejecucion-de-comandos-y-scripts-en-el-inicio-y-reinicio-en-gnulinux/
- http://www.raspbian.org/RaspbianForums
- http://www.rpi.uroboros.es/sistema.html#5
- http://www.g2khosting.com/blog/iptables-que-es-y-para-que-se-usa/
- https://www.ecured.cu/Tor
- https://tonet666p.wordpress.com/category/hostapd/
- http://www.ordenadores-y-portatiles.com/dhcp.html
- https://blogthinkbig.com/que-es-la-deep-web