



Made By ~ M4N14CK ~

Introducción

La dark web es una parte de internet que no está indexada por los motores de búsqueda tradicionales como Google, Bing o Yahoo. Para acceder a ella, se necesitan herramientas especiales, como el navegador Tor (The Onion Router). A diferencia de la surface web (la web superficial, que es accesible para todos) y la deep web (partes de internet no indexadas, como bases de datos privadas o intranets), la dark web es conocida por su anonimato y su uso tanto para actividades legítimas como ilegales.

Habiendo compartido esta información, quiero agradecerles por el apoyo que me ha permitido crear esta guía. Mi objetivo es ayudar a aquellos que sienten curiosidad por adentrarse en la dark web, pero también advertirles sobre los riesgos y desafíos que conlleva esta exploración. Para mí, personalmente, no fue una tarea fácil, ya que se requiere de ciertos enlaces .onion específicos para acceder a lugares más profundos y ocultos.

Estos enlaces pueden llevarte mucho más lejos de lo que imaginas, incluso a foros y sitios que albergan contenido extremadamente perturbador. No solo me refiero a temas conocidos como CP (contenido ilegal relacionado con menores) o Gore (contenido violento y sangriento), sino también a otros tipos de material desagradable, como la tortura de animales o actos de canibalismo. Por ejemplo, en algunos foros he llegado

a encontrar videos de un gato comiéndose a un gatito, lo cual es extremadamente impactante y difícil de procesar.

Acceso a Lugares Más Extraños e Illegales en la Dark Web

Se puede llegar a lugares mucho más extraños e ilegales en la dark web, pero solo si tienes los enlaces adecuados. Estos enlaces son altamente codiciados, ya que te permiten adentrarte en niveles más profundos y ocultos de la red. Si logras conseguir algún enlace valioso, podrías incluso venderlo.

Quizás te preguntes: "¿Por qué alguien pagaría por un simple enlace?" La respuesta es simple: conseguir este tipo de enlaces no es nada fácil. Requiere invertir horas y horas de búsqueda en la dark web, explorando foros, comunidades ocultas y mercados ilegales. Además, muchos de estos enlaces son efímeros, es decir, pueden desaparecer o cambiar en cualquier momento, lo que los hace aún más valiosos.

¿Por qué son tan difíciles de conseguir?

- **Acceso restringido:** Muchos de estos sitios no son públicos y solo se comparten entre usuarios de confianza o en círculos cerrados.
 - **Seguridad extrema:** Los administradores de estos sitios suelen implementar medidas de seguridad avanzadas para evitar ser detectados.
 - **Falta de indexación:** A diferencia de la web superficial, los sitios de la dark web no están indexados en motores de búsqueda, por lo que encontrar enlaces específicos requiere esfuerzo y paciencia.

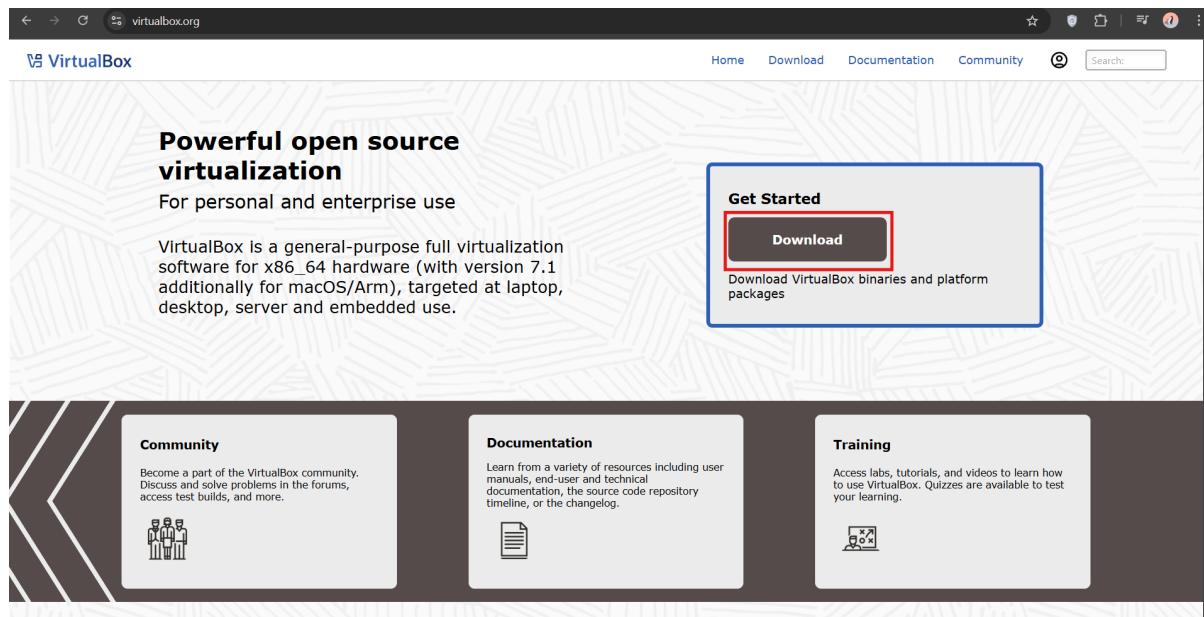
Una vez dada esta pequeña introducción, vamos a lo que realmente los interesa a muchos: **Cómo ingresar a la dark web**. En esta guía, les proporcionaré algunos enlaces que pueden ser útiles para comenzar. Sin embargo, quiero que tengan en cuenta que estos enlaces pueden cambiar o dejar de estar activos en cualquier momento. No puedo garantizar por cuánto tiempo estarán disponibles, así que les recomiendo que los utilicen lo más pronto posible.

Además, una vez que empiecen a navegar, podrán encontrar otros enlaces por su cuenta, lo que les permitirá explorar la dark web sin depender únicamente de los enlaces proporcionados en esta guía.

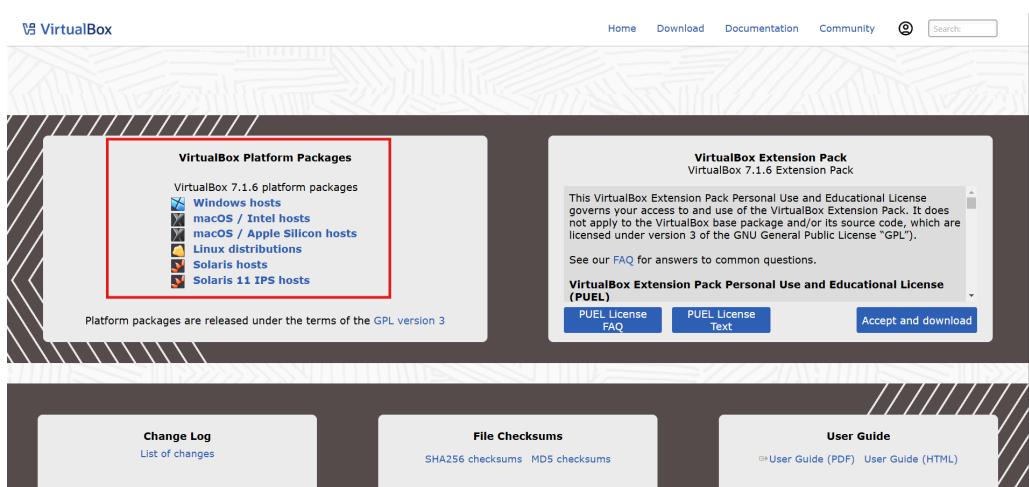
Instalación de Whonix

Para instalar Whonix, necesitaremos una máquina virtual (VM). En esta guía, utilizaremos VirtualBox, que pueden descargar desde su navegador preferido (Google, Firefox, etc.). A continuación, se muestra una imagen de referencia:

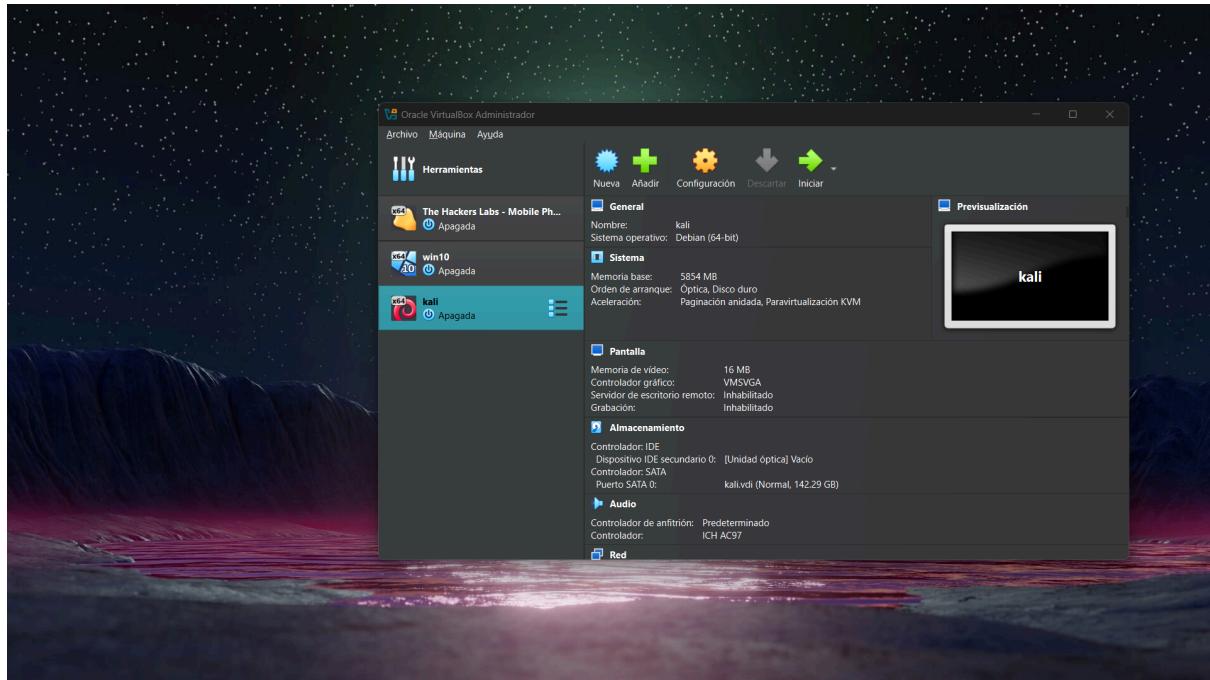
Se puede observar en la imagen que, para ingresar a la página de VirtualBox, simplemente deben escribir "**VirtualBox**" en el buscador y hacer clic en el primer enlace que aparezca. Con esto, podrán acceder directamente al sitio oficial. Una vez dentro, hagan clic en "**Download**" para iniciar la descarga.



Una vez que hayan hecho clic en "**Download**", se les mostrará una lista de opciones. En este paso, deberán seleccionar el SO (Sistema Operativo) en el cual planean instalar la máquina virtual (VM). Elijan la opción que corresponda a su sistema operativo actual para continuar con la descarga.



Una vez que hayan descargado e instalado VirtualBox, debería aparecerles una interfaz similar a la siguiente:

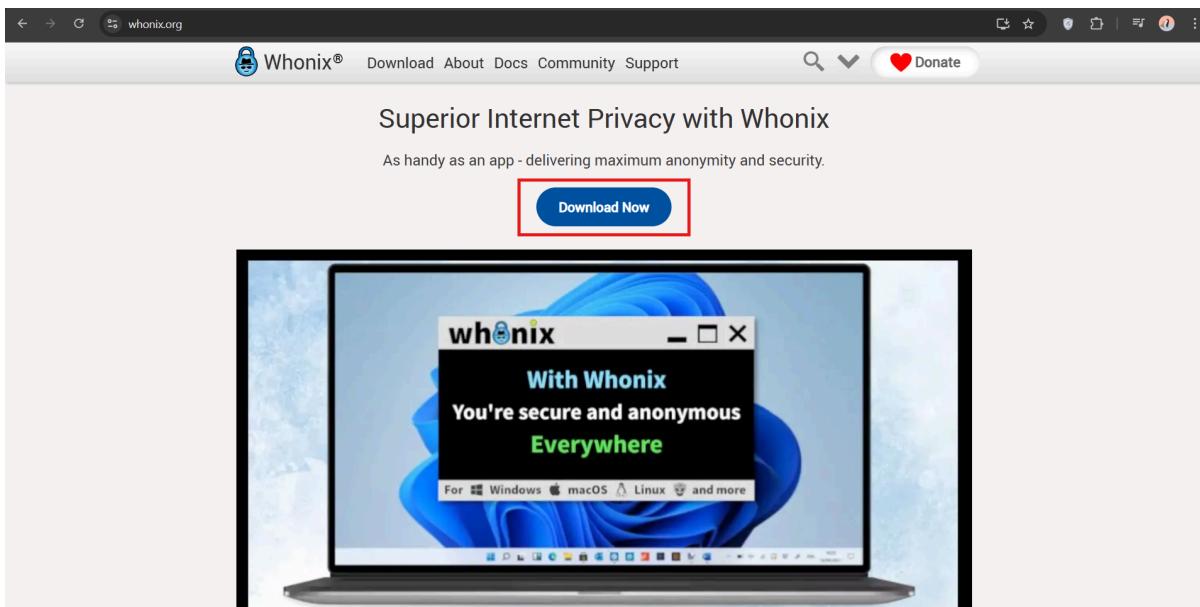


En esta pantalla, podrán ver las opciones para crear, configurar y gestionar sus máquinas virtuales. Esto les permitirá continuar con la instalación de Whonix u otros sistemas operativos dentro de la VM.

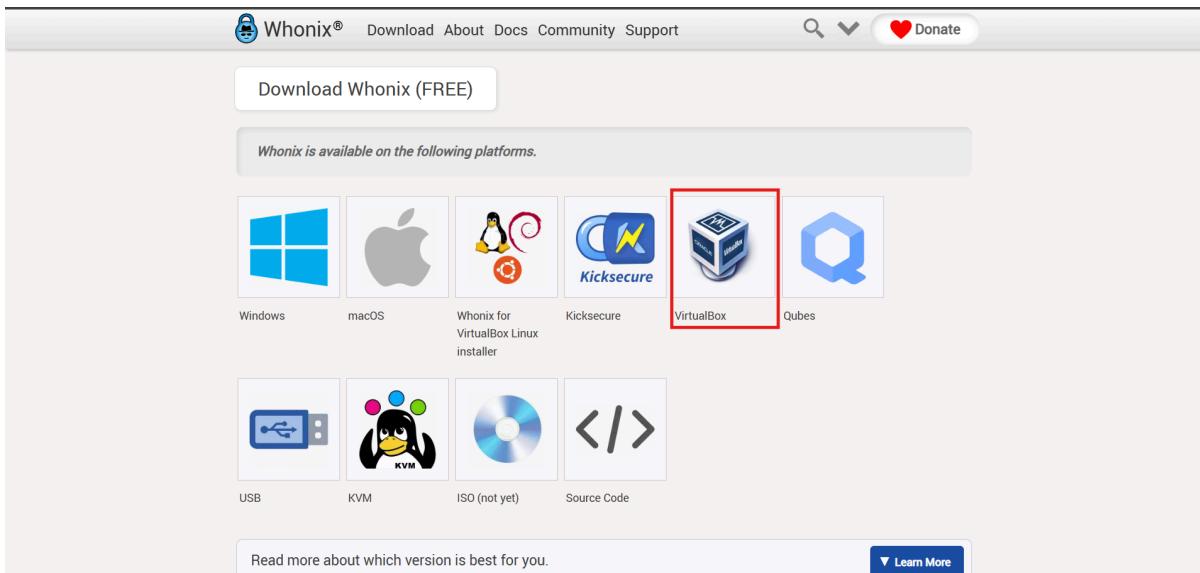
Instalando Whonix

Una vez configurado VirtualBox, para instalar Whonix:

Busquen "Whonix" en su navegador y entren al primer enlace. Dentro de la página, hagan clic en "**Download Now**".

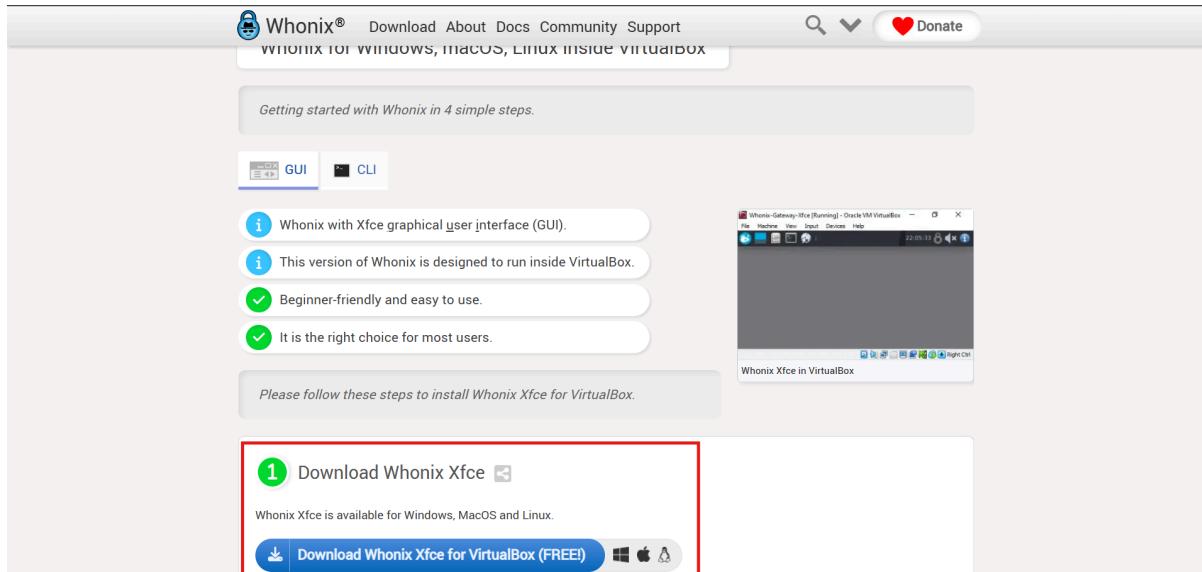


Una vez que hagan clic en "**Download**", les aparecerán varias opciones para instalar Whonix. En este caso, seleccionen la opción para VirtualBox. Esto les permitirá descargar los archivos necesarios para configurar Whonix en su máquina virtual.



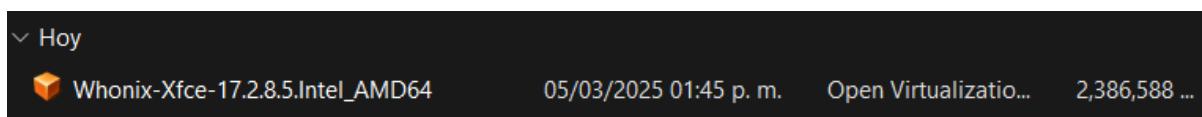
Ahora nos aparecerá la sección "**Getting started with Whonix in 4 simple steps**", que es un mini tutorial sobre cómo instalar Whonix. Sin embargo, lo que nos interesa es la parte que dice "**Download Whonix with Xfce**". Esta es la opción que debemos elegir por dos razones principales:

1. Es amigable para principiantes, ideal para quienes están comenzando.
2. Es la opción correcta para la mayoría de los usuarios.



Una vez que hayan descargado los archivos de Whonix, en su explorador de archivos (por ejemplo, en la carpeta de Descargas), les aparecerán los archivos descargados.

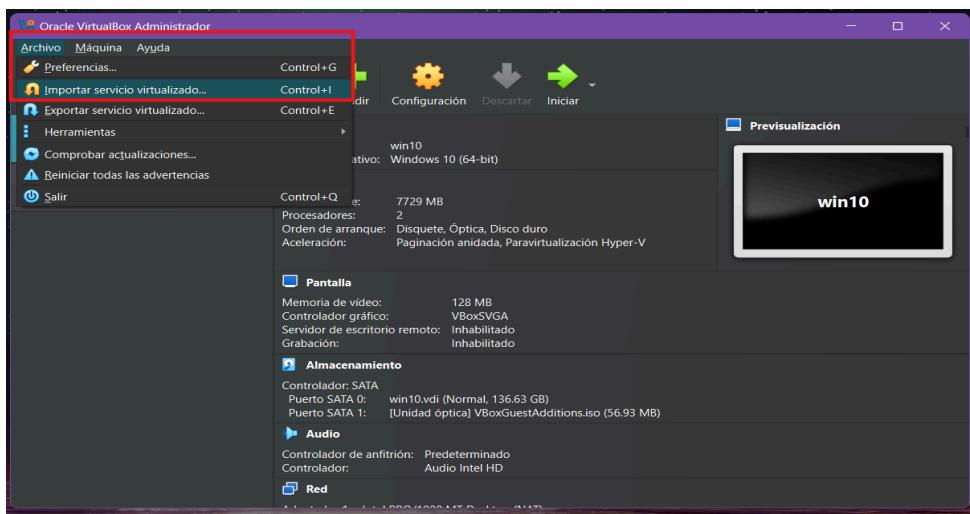
En este caso, deberían ver algo similar a esto:



Ahora, lo que deben hacer es abrir VirtualBox (VB) y seguir estos pasos:

En la barra superior, haga clic en la pestaña que dice "Archivo".

Les aparecerá un menú desplegable con varias opciones. Selecciónen "Importar servicio virtualizado", como se muestra en este ejemplo:

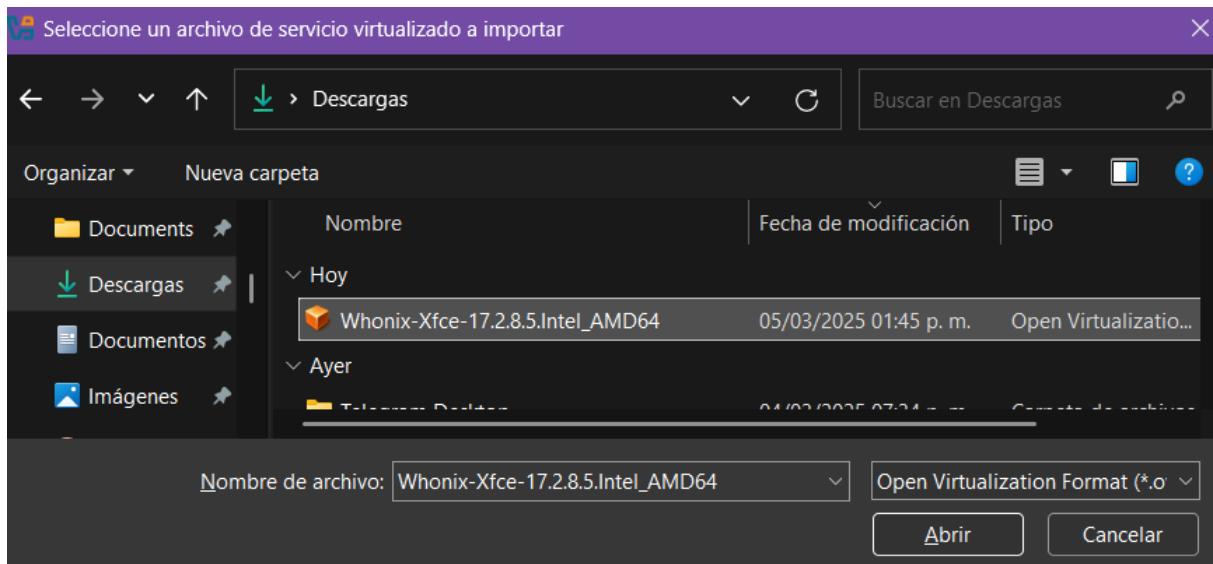


Ahora les aparecerá una ventana titulada "**Importar servicio virtualizado**". En esta ventana, deben hacer lo siguiente:

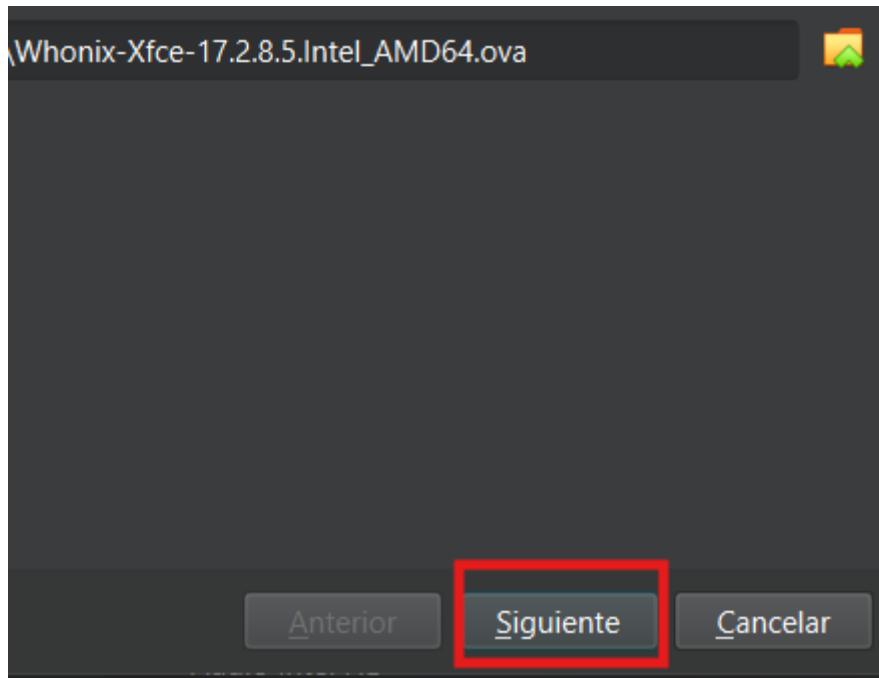
Seleccionen la opción que dice "**Importar archivo**", como se muestra en este ejemplo:



Buscan donde esta el archivo a exportar lo seleccionan y listo a si como en este ejemplo:



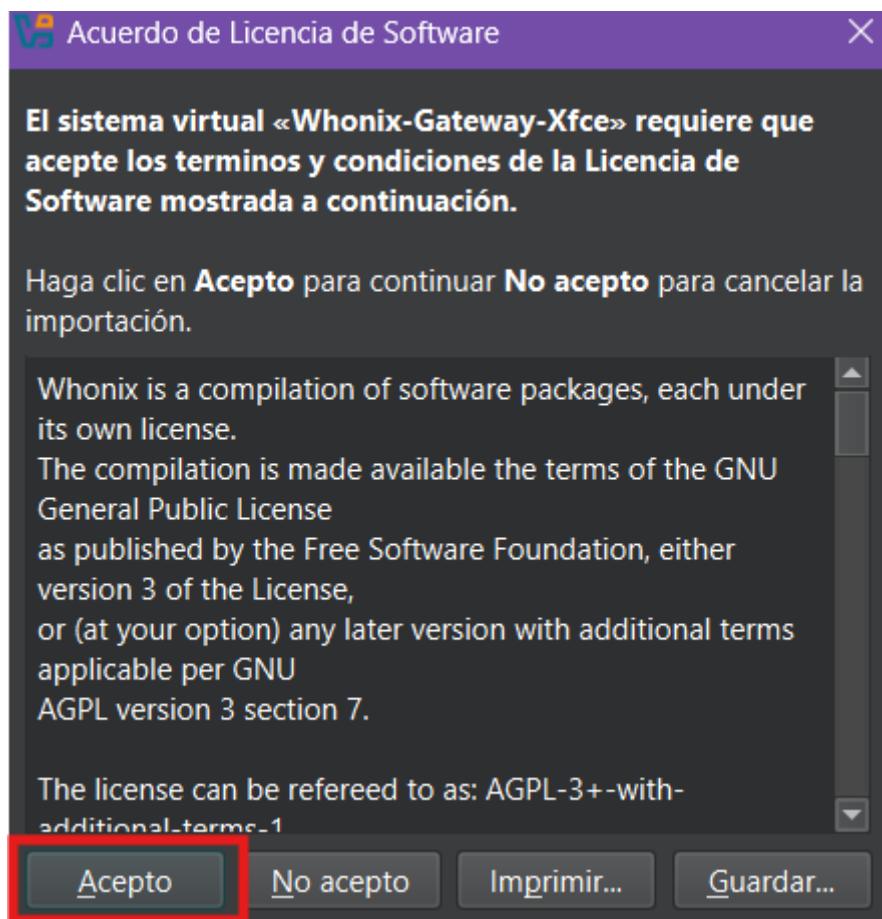
Ahora solo le dan a siguiente



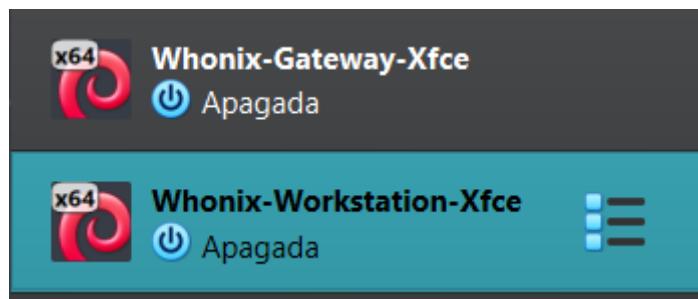
Ahora en esta parte pueden hacer algunas configuraciones como agregarle mas RAM o CPU pero eso ya lo haremos después ahora solo le dan en Terminar y listo.



Si les aparece este mensaje solo denle en aceptar



Una vez hecho esto en su Virtual Box les tendra que aparecer 2 maquinas



Las dos máquinas mencionadas, **Whonix-Gateway-Xfce** y **Whonix-Workstation-Xfce**, son componentes clave del sistema **Whonix**, que está diseñado para proporcionar **privacidad y anonimato** en línea.



Whonix-Gateway-Xfce: Esta máquina actúa como un gateway (puerta de enlace) que dirige todo el tráfico de Internet a través de la red Tor. Su función principal es asegurar que todas las conexiones estén enrutadas a través de Tor, lo que ayuda a proteger la identidad y la ubicación del usuario. Al estar "apagada", significa que actualmente no está en funcionamiento.



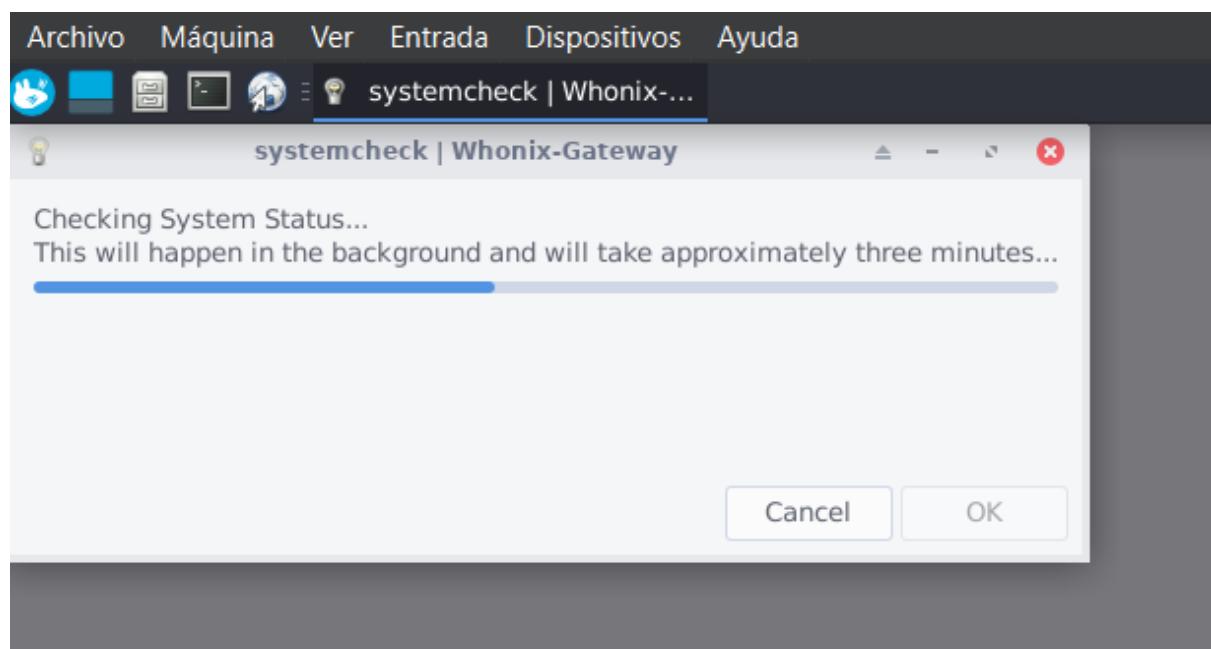
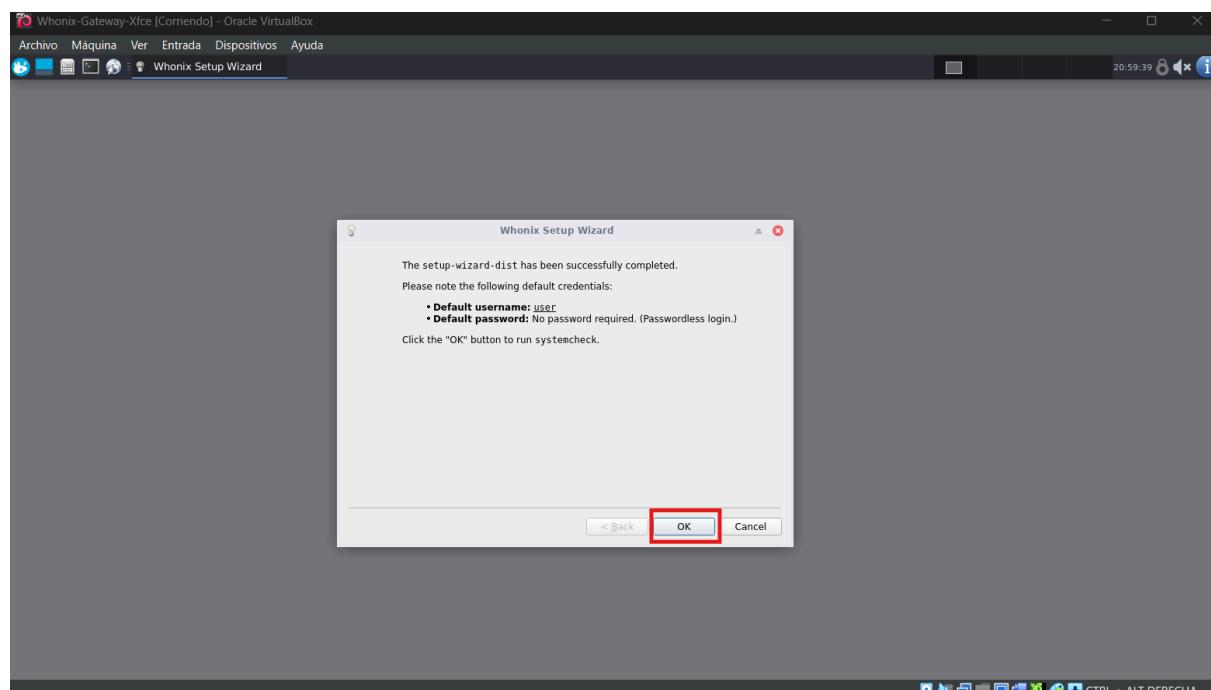
Whonix-Workstation-Xfce: Esta es la máquina donde el usuario realiza sus actividades, como navegar por Internet o usar aplicaciones. Está aislada de la red directa y solo se comunica con el exterior a través del Whonix-Gateway. Esto añade una capa adicional de seguridad, ya que incluso si la Workstation está comprometida, la identidad del usuario sigue protegida por el Gateway. Al estar "apagada", indica que no está activa en este momento.

En el sistema Whonix, el orden de activación de las máquinas es importante para garantizar que el tráfico de red se enrute correctamente a través de Tor.

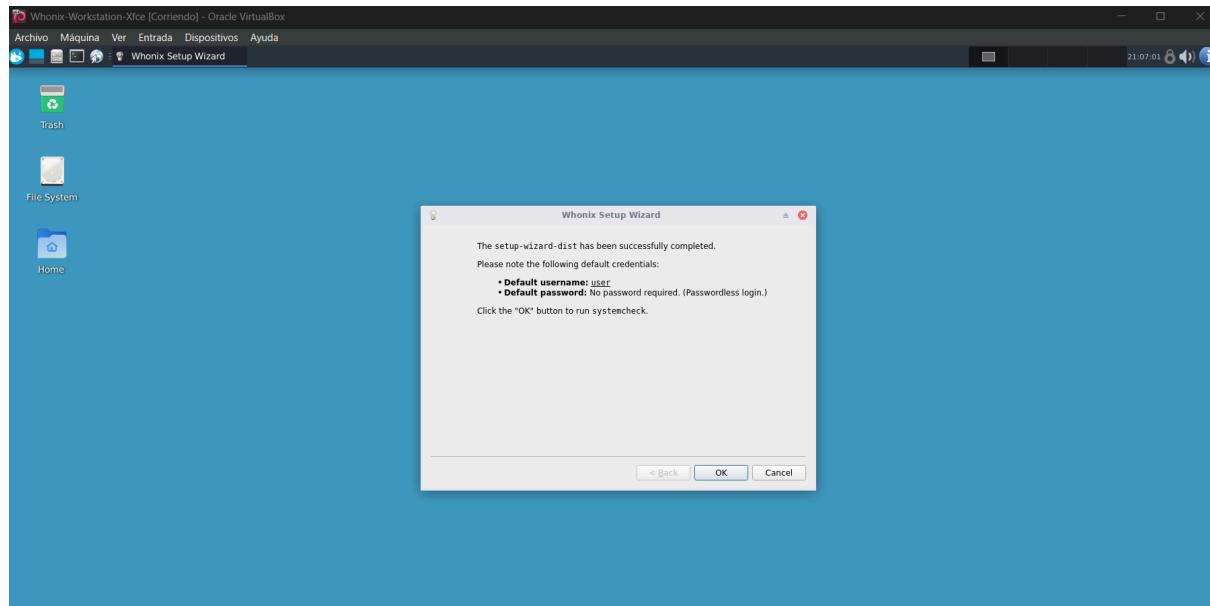
1. **Whonix-Gateway-Xfce:** Debes activar primero esta máquina. El Gateway es el componente que maneja la conexión a la red Tor y asegura que todo el tráfico de Internet pase a través de ella. Sin el Gateway en funcionamiento, la Workstation no podrá conectarse a Internet de manera segura.
 2. **Whonix-Workstation-Xfce:** Una vez que el Gateway esté activo y funcionando correctamente, puedes activar la Workstation. Esta máquina depende del Gateway para todas sus conexiones a Internet, por lo que es crucial que el Gateway esté en funcionamiento antes de iniciar la Workstation.

Una vez entendido lo anterior, que es de suma importancia, asegúrense de dominar estos pasos, ya que son clave para instalar y configurar Whonix correctamente. Esto les permitirá utilizar la plataforma de manera segura y aprovechar al máximo sus funciones de privacidad y anonimato. ¡Practiquen y no duden en revisar los pasos las veces que necesiten!

Ahora activamos la primera máquina la cual es el **Whonix-Gateway-Xfce** les aparecerá un mensaje el cual es para hacer un systemcheck así que solo le dan en ok



Una vez hecho esto activamos la otra máquina la cual es **Whonix-Workstation-Xfce** y al igual que el gateway hace exactamente lo mismo por lo que no es necesario que vuelva a poner imágenes de lo anterior.

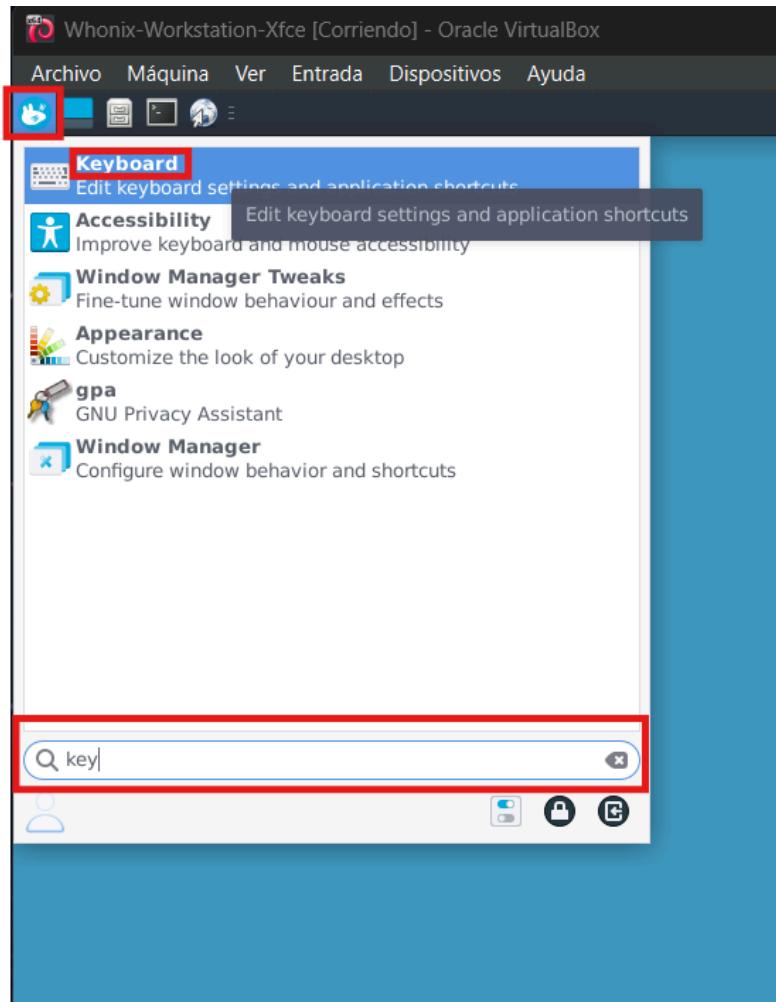


Esto sería todo de la instalación de whonix.

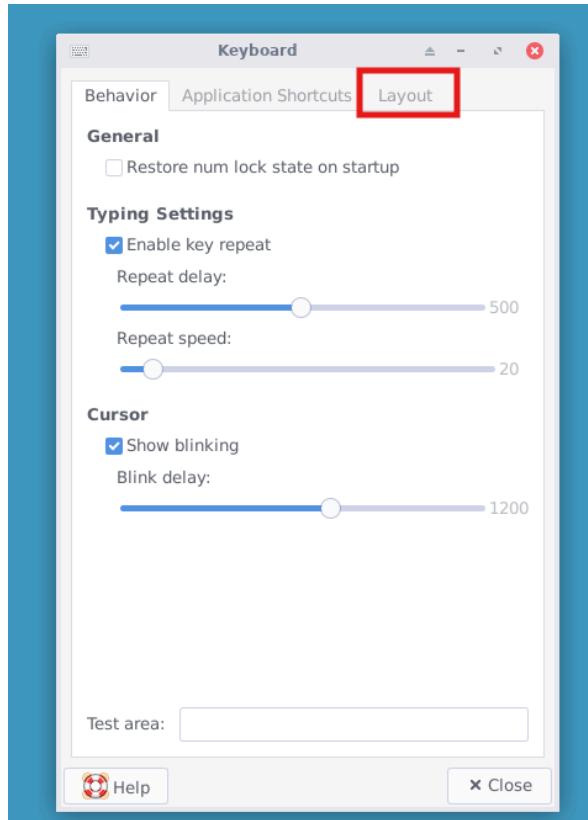
Configurando el entorno de Whonix

Lo primero que haremos es **cambiar el idioma del teclado**, ya que, por defecto, Whonix viene configurado con un teclado en inglés. Esto puede ser un problema para usuarios de Latinoamérica (y otros países) porque algunas teclas no coinciden con la distribución del teclado físico, lo que dificulta el uso de la terminal y otras aplicaciones.

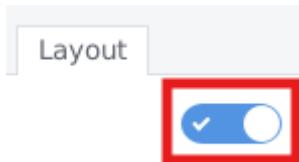
Para esto le damos click al icono que tiene la cara de un ratón luego le dan click en la barra de búsqueda y pondrán la palabra **key** y una vez puesto eso les saldrá la opción **Keyboard** y proceden a darle click a **Keyboard**.



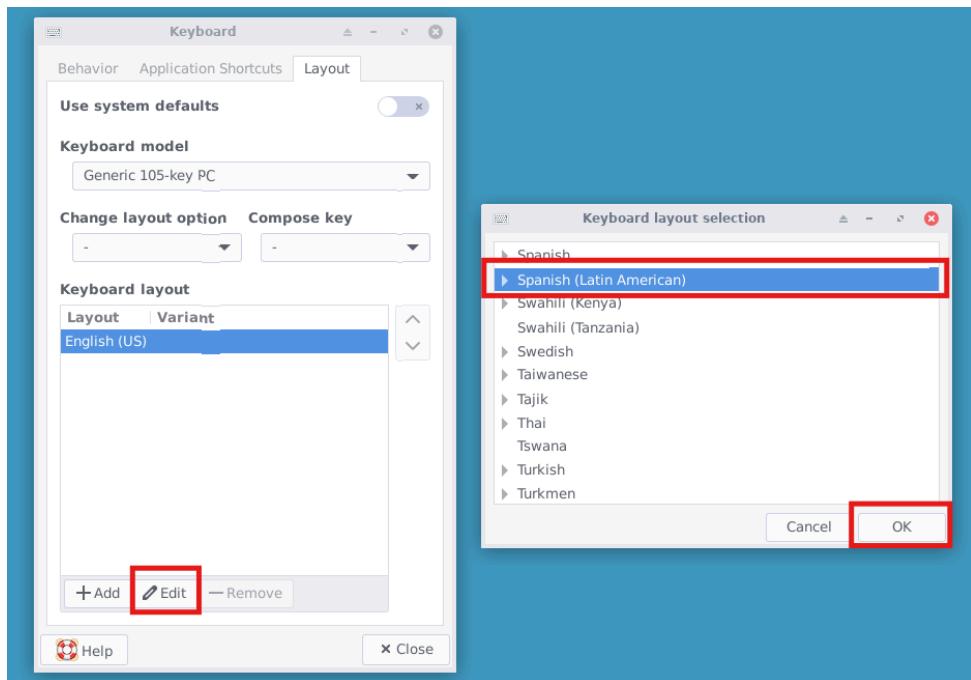
Les aparecerá esta ventana y le darán click en **Layout**



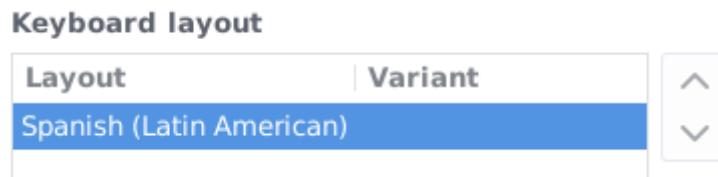
Una vez hecho eso ahora le darán click a ese switch para hacer los cambios en la aplicación



Una vez hecho esto le dan a **Edit** y les aparecerá otra ventana y en esa nueva ventana buscarán la palabra **spanish(Latin American)** una vez seleccionado le darán en **ok**



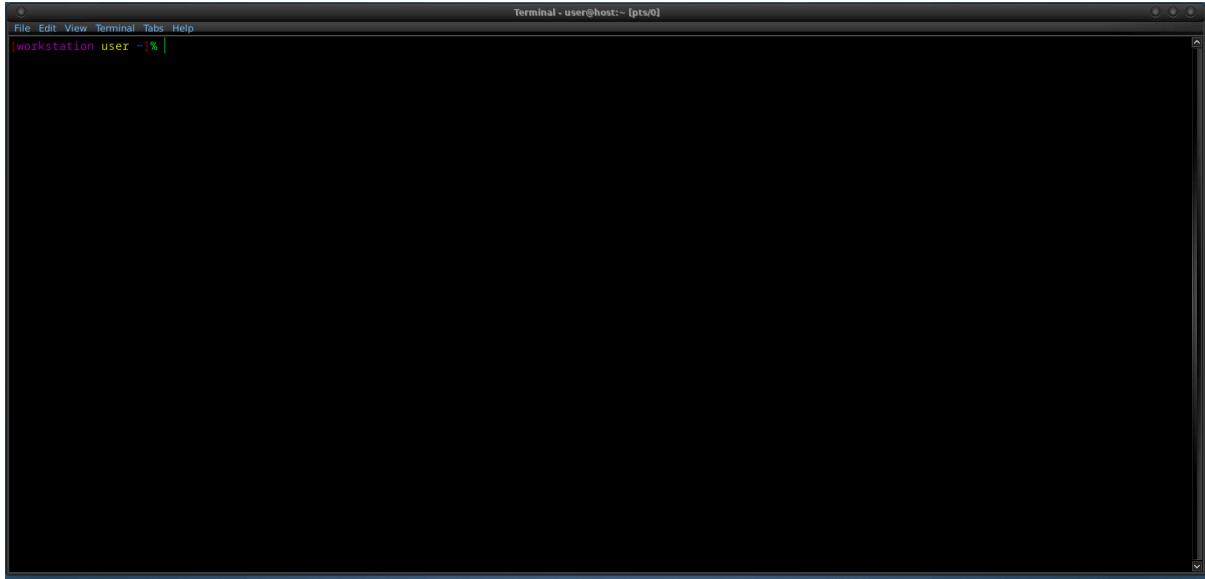
Basicamente así es como quedaría



Configurando la terminal e instalando comandos en Whonix

Ahora que el teclado está configurado correctamente en Whonix, podemos utilizar algunos comandos en la terminal para verificar que la conexión a Tor esté funcionando correctamente y asegurarnos de que no haya fugas de información (como la dirección IP real o consultas DNS).

Primero abrimos una terminal con la combinación de teclas **ctrl + alt + t** una vez hecho esto nos abrirá una terminal ejemplo:



Si ustedes alguna vez han utilizado alguna distribución de linux basado en debian entonces se les hará muy fácil utilizar la terminal pues los comandos son exactamente los mismos por lo que hacer hacer ciertas modificaciones no será un problema.

El primer comando que ingresamos es **sudo apt update && sudo apt upgrade -y** esto es para actualizar el sistema ejemplo:

```
1/1 ▾ + 🔍 ✎
[workstation user ~] % sudo apt update && sudo apt upgrade -y
Get:1 tor+https://deb.whonix.org/bookworm InRelease [61.2 kB]
Hit:2 tor+https://deb.debian.org/debian bookworm InRelease
Get:3 tor+https://deb.kicksecure.com/bookworm InRelease [62.0 kB]
Get:4 tor+https://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Get:5 tor+https://deb.whonix.org/bookworm/main amd64 Packages [13.6 kB]
Get:6 tor+https://fasttrack.debian.net/debian bookworm-fasttrack InRelease [12.9 kB]
Get:7 tor+https://deb.kicksecure.com/bookworm/main amd64 Packages [34.0 kB]
Get:8 tor+https://deb.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Get:9 tor+https://deb.debian.org/debian bookworm-backports InRelease [59.4 kB]
Get:10 tor+https://deb.debian.org/debian bookworm-security/main amd64 Packages [246 kB]
Get:11 tor+https://deb.debian.org/debian bookworm-backports/non-free amd64 Packages.diff/Index [17.3 kB]
Get:12 tor+https://deb.debian.org/debian bookworm-backports/main amd64 Packages.diff/Index [63.3 kB]
Get:13 tor+https://deb.debian.org/debian bookworm-backports/non-free amd64 Packages T-2025-03-06-2027.58-F-2025-03-06-2027.58.pdiff [264 B]
Get:13 tor+https://deb.debian.org/debian bookworm-backports/non-free amd64 Packages T-2025-03-06-2027.58-F-2025-03-06-2027.58.pdiff [264 B]
Get:14 tor+https://deb.debian.org/debian bookworm-backports/main amd64 Packages T-2025-03-07-2014.23-F-2025-03-06-0204.45.pdiff [1921 B]
Get:14 tor+https://deb.debian.org/debian bookworm-backports/main amd64 Packages T-2025-03-07-2014.23-F-2025-03-06-0204.45.pdiff [1921 B]
Fetched 675 kB in 5s (141 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
59 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  linux-headers-6.1.0-31-amd64 linux-headers-6.1.0-31-common linux-image-6.1.0-31-amd64 privleap python3-pam
The following packages will be upgraded:
  base-files bind9-dnsutils bind9-host bind9-libbs bsdxtrautils bsutils dist-base-files dnsutils eject fdisk gstreamer1.0-plugins-base
  gstreamer1.0-plugins-good helper-scripts libavahi-client3 libavahi-common-data libavahi-common3 libavlki libehm15 libfdisk1 libglib2.0-0
```

Una vez que se haya actualizado el sistema pondremos otro comando el cual nos ayudará a verificar el estado de tor el cual es este comando **sudo service tor status** ejemplo:

```
[workstation user ~]% sudo service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; enabled; preset: enabled)
   Drop-In: /usr/lib/systemd/system/tor.service.d
             └─50_anon_ws_disable_stacked_tor.conf
     Active: active (exited) since Sat 2025-03-08 01:53:56 UTC; 22min ago
       Main PID: 1019 (code=exited, status=0/SUCCESS)
         CPU: 10ms

Mar 08 01:53:56 host systemd[1]: Starting tor.service - Anonymizing overlay network for TCP (multi-instance-master)...
Mar 08 01:53:56 host systemd[1]: Finished tor.service - Anonymizing overlay network for TCP (multi-instance-master).
[workstation user ~]%
```

- **tor.service:**

Es un servicio que permite usar la red Tor, una red que ayuda a navegar de forma anónima y segura.

- **Loaded:**

El servicio está cargado y configurado para iniciarse automáticamente (está "habilitado").

- **Active:**

El servicio está activo, pero en este caso, ya terminó su tarea y se marcó como "exited" (finalizado correctamente).

- **Última actividad:**

El servicio se inició y finalizó el 8 de marzo de 2025 a las 01:53:56 UTC.

- **Logs:**

Muestra que el servicio se inició y finalizó correctamente en ese momento.

En dado caso de que a ustedes no les aparezca como en la imagen lo cual sería algo completamente extraño pues tendrán que ejecutar este comando **sudo service tor start** y **sudo service tor status** y con eso lograran verificar si el servicio de tor ahora está activado.

Podemos también usar la herramienta torsocks para verificar nuestra conectividad.

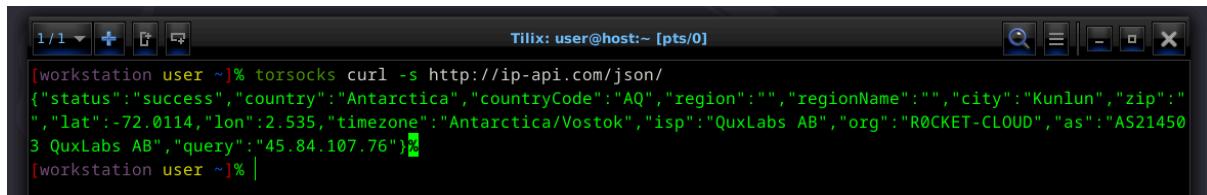
¿Qué es torsocks?

Torsocks es una herramienta que permite redirigir el tráfico de aplicaciones a través de la red Tor. Esto es útil para asegurarte de que las conexiones de una aplicación específica estén siendo enrutadas correctamente a través de Tor, lo que añade un nivel adicional de privacidad y anonimato.

Sabiendo esto pasemos a hacer la verificación utilizando torsocks y otros métodos para asegurarnos de que nuestra conexión a través de la red Tor esté funcionando correctamente.

Verificar la dirección IP y mas información

Usa curl para verificar tu dirección IP pública a través de Tor:



```
1/1 Tiliix: user@host:~ [pts/0]
[workstation user ~]% torsocks curl -s http://ip-api.com/json/
{"status":"success","country":"Antarctica","countryCode":"AQ","region":"","regionName":"","city":"Kunlun","zip":"
","lat":-72.0114,"lon":2.535,"timezone":"Antarctica/Vostok","isp":"QuxLabs AB","org":"ROCKET-CLOUD","as":"AS21450
3 QuxLabs AB","query":"45.84.107.76")%}
[workstation user ~]%
```

Desglosamos más esto:

El comando **torsocks curl -s http://ip-api.com/json/** combina dos herramientas poderosas (torsocks y curl) para realizar una solicitud HTTP a través de la red Tor y obtener información sobre la dirección IP que estás utilizando.

1. torsocks

- torsocks es una herramienta que redirige el tráfico de una aplicación a través de la red Tor. En este caso, se utiliza para asegurarse de que la solicitud HTTP realizada por curl pase a través de Tor, lo que garantiza que la conexión sea anónima y que la dirección IP visible sea la de un nodo de salida de Tor.

2. curl

- curl es una herramienta de línea de comandos utilizada para transferir datos desde o hacia un servidor. En este caso, se utiliza para hacer una solicitud HTTP GET a la URL especificada (<http://ip-api.com/json/>).

3. -s (opción de curl)

- La opción -s (silent) le dice a curl que opere en modo silencioso, lo que significa que no mostrará progreso ni mensajes de error. Esto es útil cuando solo te interesa el resultado de la solicitud y no quieres que se muestre información adicional en la terminal.

4. <http://ip-api.com/json/>

- Esta es la URL a la que se realiza la solicitud. ip-api.com es un servicio que devuelve información sobre la dirección IP desde la cual se realiza la solicitud. Al acceder a <http://ip-api.com/json/>, el servicio devuelve un objeto JSON con detalles como:
 - La dirección IP.
 - El país, región y ciudad asociados con la IP.
 - El proveedor de servicios de Internet (ISP).
 - La zona horaria.
 - Las coordenadas geográficas (latitud y longitud).

También podemos utilizar este otro comando para verificar nuestra conexión: **torsocks curl <https://check.torproject.org>**

```
[workstation user ~]% torsocks curl https://check.torproject.org
<!doctype html>
<html lang="en_US">
<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>

    Congratulations. This browser is configured to use Tor.

  </title>
  <link rel="icon" type="image/x-icon" href="/torcheck/img/tor-not.png" />
  <style>
    html { height: 100%; }
```

Por último utilizaremos el comando whonixcheck el cual es una herramienta específica del sistema operativo Whonix, que está diseñado para proporcionar un alto nivel de privacidad y anonimato al utilizar la red Tor.

```
[workstation user ~]% whonixcheck
[INFO] [systemcheck] Connected to Tor.
[INFO] [systemcheck] Whonix is produced independently of, with no guarantee from, The Tor Project. https://www.whonix.org
[INFO] [systemcheck] Whonix APT Repository: Enabled.
When the Whonix team releases BOOKWORM updates,
they will be AUTOMATICALLY installed (when you run apt-get dist-upgrade)
along with updated packages from the Debian team. Please
read https://www.whonix.org/wiki/Trust to understand the risk.
If you want to change this, use:
    sudo repository-dist
```

¿Qué hace whonixcheck?

El comando **whonixcheck** realiza una serie de pruebas para asegurarse de que:

- **El tráfico está siendo enrutado correctamente a través de Tor:** Verifica que no haya fugas de tráfico fuera de la red Tor.
 - **El sistema Whonix está configurado correctamente:** Comprueba que las configuraciones de red y seguridad estén aplicadas adecuadamente.
 - **No hay problemas de conectividad con Tor:** Detecta si hay errores en la conexión a la red Tor.

Entiendo que todos los comandos son para verificar su conectividad pero es que es lo mas importante puesto a que una fuga puede exponerlos demasiado y mas si tienen el JS(javaScript) activado ya que algunas paginas pueden sacar mucha informacion con solo un script pero en si los demas comandos que se pueden utilizar en la terminal son los mismos que se usan debian por ejemplo:

sudo apt update && sudo apt upgrade

sudo apt install -y

sudo apt list

Esto seria todo sobre la terminal

Hidden Wiki

¿Qué es, por qué se creó y por qué no es un buen lugar para comenzar en la dark web?

La Hidden Wiki es uno de los directorios más conocidos dentro de la deep web, creado como una especie de "página de inicio" para navegar por sitios .onion. Surgió como una herramienta para facilitar el acceso a diversos servicios y contenidos en la red Tor, desde foros de discusión hasta mercados ilegales.



thehidden2.wiki
<https://thehidden2.wiki>

...

[Hidden Wiki » 100+ Active Dark Web Links 2025 » TheHidden2....](#)

The Hidden Wiki was a dark web wiki that featured links to .onion sites on the main page. The first Hidden Wiki was a website that could only be reached by using Tor and, therefore must use the .onion pseudo-top-level domain. The site's main page provided a community-maintained directory of links...

[Silk Road](#) · [Blog](#) · [Tor Web Browser](#) · [Hidden Wiki](#) · [History](#) · [Dark Web Guide](#)



hidden.wiki
<https://hidden.wiki>

...

[The Original Hidden Wiki - All Types Of Dark Web Links Here](#)

Hidden wiki is a website that has a link to all the hidden wiki and secret/illicit works, for example, tax evasion, contract killing, cyber-attacks for hire, etc. The hidden wiki is a set of links of websites, but a lot more additional websites are there on the Dark web which don't appear on the hidden wiki. HOW THE...

La verdad no es para nada difícil encontrar la hidden wiki ya que en si solo es poner en el buscador de DuckDuckGo **hidden wiki** y ya te saldrán varias páginas de la hidden wiki.

No importa a cual se le de click ya que hacen casi lo mismo pues son los mismos links aunque hoy en día esta la **hidden2.wiki** la cual se presenta como una versión moderna de lo que antes era la **hiddenwiki**.

The deep web is much bigger than the regular internet: it makes up 90% of everything on the internet; it has secret networks, databases, and sites that need passwords. Most of the stuff on the deep web is okay, but it's hidden because of technical reasons, not because it's bad! In contrast, the dark web and the hidden wiki is intentionally concealed and accessed via anonymity tools like Tor. While facilitating criminal activities, the dark web enables free speech, journalism, and dissent in oppressive regimes. So, privacy comes at both a cost and benefit to society.

Hidden Wiki can also be accessed using <https://hidden-wiki.onion>

Hidden Search Engines

- [OnionIndex Search Engine](#) – OnionIndex Search Engine
- [DuckDuckGo](#) – DuckDuckGo Search Engine
- [OnionLand](#) – OnionLand Search
- [Tordex](#) – Tordex
- [Torch](#) – Torch
- [Ahmia](#) – Ahmia
- [MetaGer](#) – MetaGer – German Search
- [haystak](#) – haystak

Store Links

- [Tor Shop](#) – Tor Shop – Multi Vendor Marketplace | Build-in Escrow
- [BlackMart](#) – BlackMart
- [Caribbean Cards](#) – Caribbean Cards
- [Psy Shop](#) – Psy Shop – Drugs Market
- [Cordzilla](#) – Cordzilla
- [21Million Club](#) – 21 Million Club

- » Dark Web Digest – November 2024 Edition
- » Dark Web Digest – October 2024 Edition
- » Dark Web Digest – September 2024 Edition
- » Dark Web Digest – August 2024 Edition
- » Dark Web Digest – July 2024 Edition
- » Dark Web Digest – June 2024 Edition
- » Dark Web Digest – May 2024 Edition
- » Dark Web Digest – April 2024 Edition
- » Dark Web Digest – March 2024 Edition
- » Dark Web Digest – February 2024 Edition
- » Dark Web Digest – January 2024 Edition
- » Dark Web Digest – December 2023 Edition
- » Anonymized Payment Methods Are Essential on the Hidden Wiki Markets
- » Dark Web Digest – November 2023 Edition
- » Dangers Lurking on the Dark Web or the

Forums / Social / Chat

- [dread](#) – dread
- [Deutschland im Deep Web Forum](#) – Deutschland im Deep Web Forum
- [Hidden Answers](#) – Hidden Answers
- [SuprBay](#) – SuprBay: The PirateBay Forum
- [Rutor](#) – Rutor
- [Lolita City](#) – Lolita City
- [Endchan](#) – Endchan
- [Raddle](#) – Raddle
- [MadIRC](#) – MadIRC
- [The Stock Insiders](#) – The Stock Insiders
- [Facebook](#) – Facebook
- [Ableonion](#) – Ableonion
- [Adamant](#) – Adamant Decentralized messenger
- [-/xss.is](#) – XSS.is – Russian Hacking Forum
- [HackTown](#) – HackTown
- [NZ Darknet Forum](#) – NZ Darknet Market Forums
- [The Calyx Institute \(Jabber\)](#) – The Calyx Institute (Jabber)
- [ANONYMOUS'z FORUM](#) – ANONYMOUS'z FORUM

Más de la mitad de estos links no sirven

Ya con esto sabemos que la hidden wiki es una porquería para encontrar buenos links y sobre todo perder el tiempo con sus links muertos puede que muchos de nosotros hayamos intentado buscar buenos links en ese lugar pues es el lugar principal al cual todos acuden cuando se menciona la deep web pero lamentablemente con los años esta famosa página ha decaído mucho por lo que como se ha mencionado antes no es un buen lugar para comenzar.

pero no se preocupen porque más adelante es donde comienza la aventura puesto que yo voy a dar ciertos links .onion los cuales les puede gustar y ademas les dire el cómo se podrán mover a través de la dark web y la verdad moverse es sencillo pero encontrar ciertas páginas la verdad no lo es ya que la mayor parte serán scam y lo más probable es que en ciertos sitios los links estan caidos.

Esto seria todo sobre la Hidden Wiki

Hidden Links

Para comenzar necesitar acceder a este link:

<http://wclekwrf2aclunlmuikf2bopusjfv66jlhwgtgbiy5nw524r6ngoid.onion/>

ese es el link para entrar a la página Hidden Links y una vez que lo hayan puesto en su navegador les aparecerá algo como esto:

Please solve the CAPTCHA to continue:

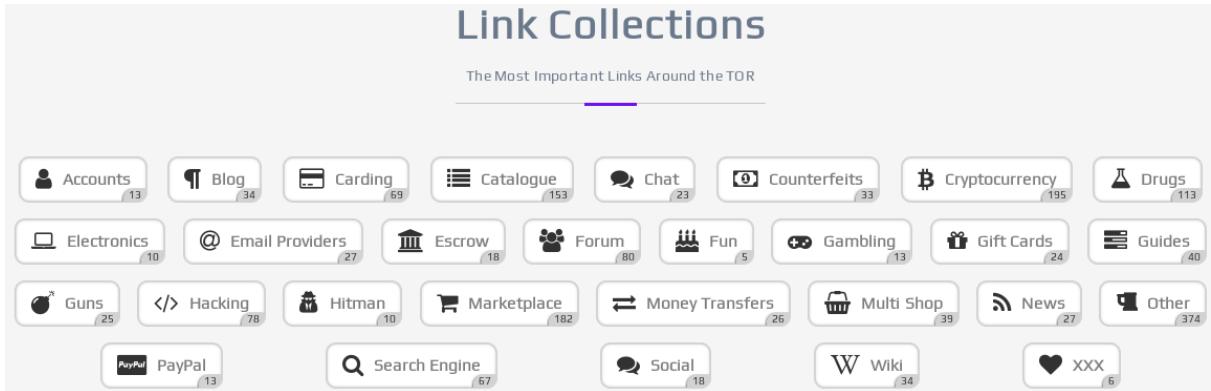
d1aa0

Una vez que Resuelvan el captcha podrán acceder a todo el contenido que les proporciona la página

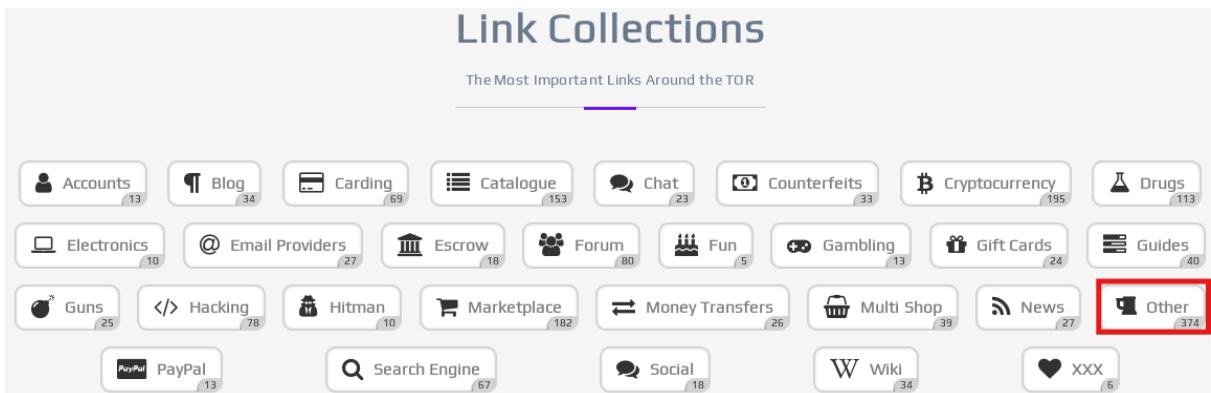
The screenshot shows the homepage of the Hidden Links website. At the top, there's a purple header bar with the "HIDDEN LINKS" logo on the left and navigation links for "DIRECTORY", "ADD LINK", "DASHBOARD", "ABOUT", and "ADVERTISING" on the right. Below the header, there are several promotional banners: one for "Cryptonium" featuring Bitcoin and Ethereum icons, another for "CLONED CREDIT CARDS" with a "SAFETY GUARANTEED" badge, and a third for "100% Valid Cards". A red banner at the bottom of the header area states: "A critical payment bug has been found. Every link owner who used it without reporting will be banned." In the main content area, there's a message encouraging users to participate in drug flow research on "DrugRoutes" and noting that it is anonymous. Another message cautions against sending emails to link owners asking for money, stating that Hidden Links NEVER send such emails. It also mentions that the catalogue is FREE FOR ALL. DO NOT SEND MONEY TO SCAMMERS!!!. Below this, a welcome message says: "Welcome to the Hidden Links - smart DW links collection. We carefully select every link to make you enjoy every second spend in Deepweb. Feel free to submit the link you are inspired of - together we can create the Best DW links catalogue." There are several links to other dark web sites like "KEVIN.SEC > Hire a Hacker", "DarkDir", "Mike's Grand Store", "Latest", "Popular", "Random", "S Dark", "MEGA Wallets Real Shop", and "Team Premium".

Me encantaría explicar todo el contenido que brinda esa página pero es demasiado y no quiero extender más esta guía pero ustedes pueden explorar la página y ver todo el contenido que ofrece ojo que puede que algunos links no estén funcionando pero lo que les voy a mostrar les va a servir mucho para que puedan moverse por la darkweb hasta este punto ya no estamos en la deepweb dado a que su contenido es mucho más fuerte e ilegal.

En la página bajamos un poco y nos aparecerá algo como esto:



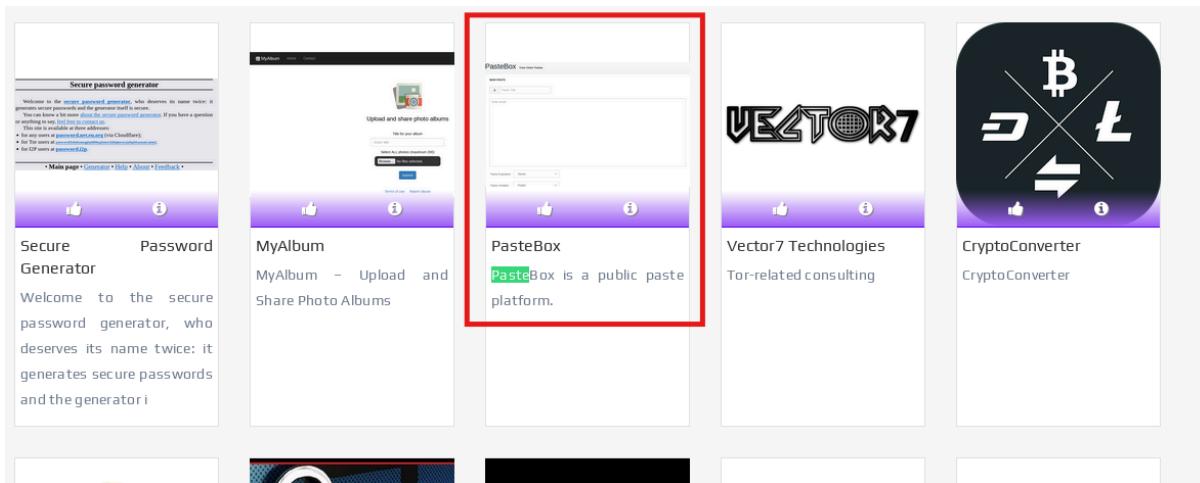
Como su mismo título lo dice son una colección de links ustedes pueden revisar uno por uno y ver que contienen pero en esta ocasión iremos a esta parte:



Una vez hecho esto les aparecerá toda una sección con muchos links:

The screenshot shows the "Other" section of the Link Collections website. It displays a grid of cards, each representing a different link or service. The cards are arranged in two rows. The first row contains five cards: 1. Books, courses and art Library / Book (with a painting icon). 2. Oniongen Vanity v3 Address (with a green background and a white onion icon). 3. PASTE LINK – Free resource from censorship (with a blue link icon). 4. Anon Hosting – Free hosting provider (with a green onion icon). 5. NoScript Pastebin Darkweb Share your text in Darknet (with a black background and a small preview window). The second row contains five cards: 1. 8chan One of the oldest and most (with a 8chan logo icon). 2. MEGA Tor FileShare MEGAtor is a free and (with a screenshot of the MEGA interface). 3. Genuine UK citizenship papers (with a British flag icon). 4. Fuck Facebook Search engine for stolen (with a screenshot of the Fuck Facebook search results). 5. MetaTor – Russian imageboard (with a dark-themed imageboard interface icon).

Pero lo que más vamos a buscar son los **pastebins** ejemplo:



PasteBox View Older Pastes Guest

NEW PASTE

Paste Title: A

hello world

Paste Expiration: Never

Paste Visibility: Public

Password (Optional):

Encrypt in database

WI+ZC QR code | Enter Code | Paste

RECENT PASTES

- Order Bitcoin[...]
- [...]
- Buy[...]
- Buy Documents[...]
- OnionWay - Onion[...]
- LINKS!
- WU Transfer[...]
- Emploment and[...]
- Real and fake[...]
- Buy Real Degree[...]

En este sitio podrás compartir cualquier tipo de contenido ya y publicarlo de forma pública o privada e incluso ponerle contraseña y decidir cuando cuaduacara. Pero aparte de todo eso tu tambien podras ver lo que otras personas publicaron aun que algunas seran spam o estafas hay otras que te pueden llevar a otros sitios y explorar.

RECENT PASTES

Order Bitcoin[...]	
[...]	
Buy[...]	
Buy Documents[...]	
OnionWay - Onion[...]	
LINKS!	
WU Transfer,[...]	
Emploments and[...]	
Real and fake[...]	
Buy Real Degree,[...]	

En esta parte solo le dan click a **RECENT PASTES** y podrán ver lo que se ha publicado recientemente. Cómo se logra apreciar hay varias publicaciones y en una de estas hay una que se llama Links y puede que esto nos ayude a encontrar mas cosas a si que entramos a este pero voy a pasar su link ya que lo más probable es que ya no esté.

PasteBox [View Older Pastes](#) Guest

PASTES ARCHIVE

Show 10 entries Search:

PASTE TITLE	PASTE TIME
Order Bitcoin Wallets	03/6/2025 08:54:02
Order,Passports, Drivers Licenses, ID Cards, Visas,[...]	03/3/2025 01:37:55
Buy International Passports and Identity cards,Visas.[...]	03/3/2025 01:27:36
Buy Documents Onlin	02/26/2025 04:41:28
OnionWay - Onion search engine	02/25/2025 05:55:11
LINKS!	02/25/2025 00:51:43
WU Transfer, Money Gram, Clone Credit Cards, Passport,[...]	02/25/2025 00:36:08
Emploments and citizenship papers or identification[...]	02/25/2025 00:26:00
Real and fake documents, passports and identities,[...]	02/24/2025 22:12:27
Buy Real Degree, Buy Real Diploma, Buy Real Transcript[...]	02/24/2025 22:12:07

Showing 1 to 10 of 10,000 entries

Previous 1 2 3 4 5 ... 1000 Next

PasteBox is a public paste platform.
Login or Register to edit, delete and keep track of your pastes and more.

RECENT PASTES

Order Bitcoin[...]	
[...]	
Buy[...]	
Buy Documents[...]	
OnionWay - Onion[...]	
LINKS!	
WU Transfer,[...]	
Emploments and[...]	
Real and fake[...]	
Buy Real Degree,[...]	

Una vez dentro podremos observar cuánta gente lo miró dia, año y ahora de la publicación y sobre todo el link que dejo:



LINKS! GUEST ON 25TH FEBRUARY 2025 12:51:43 AM

1. <http://darkmond65ucj7scvxquhmm2nbfm5tvkqj75xpf7czat73j67yute7ad.onion>

este seria el link: <http://darkmond65ucj7scvxquuhm2nbm5tvkqi75xpf7czat73j67yute7ad.onion/>

y bueno esto seria todo la verdad quisiera continuar con más pero la verdad hacer esto me a tomado días y horas y aunque mucha gente lo pueda ver como muy poco o casi nada eso puede decir que nunca en su vida han hecho guias o tutoriales pero bueno a mi lo que me gustaría es que compartieran esta guía para aquellos que tienen dudas sobre la dark web sin nada mas que decir espero que disfruten leyendo mientras hacen los pasos eso es todo de mi parte SALUDOS.