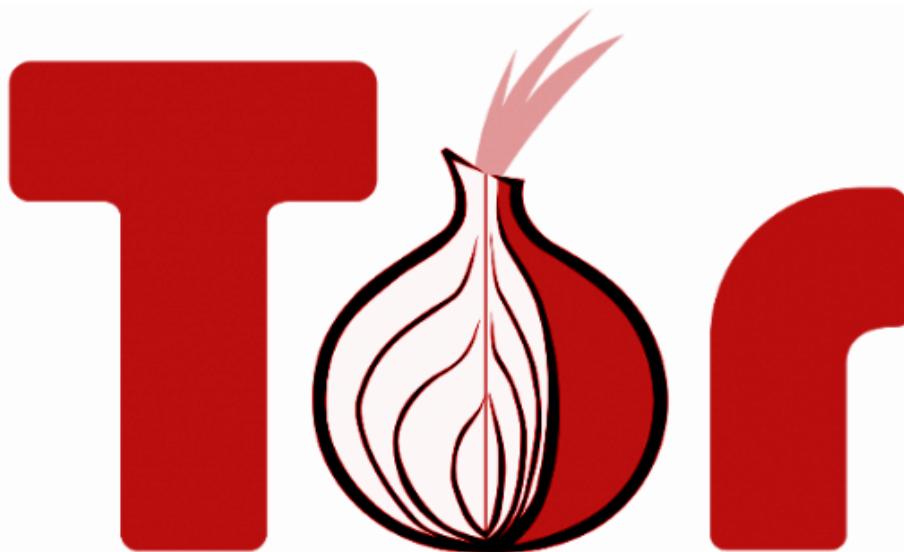


La Red Tor y La Deep Web



Pablo Merino Ávila
Adrián Ruiz López
Sergio Vela Pelegrina

Índice:

1- La Deep-Web y su Estructura.

2- La red TOR:

 2.1- Historia

 2.2- Componentes

 2.3- Funcionamiento Interno

 2.4- Riesgos de Uso

 2.5- Recomendaciones de Uso

 2.6- Dominios .onion

 2.7- Motores de Búsqueda.

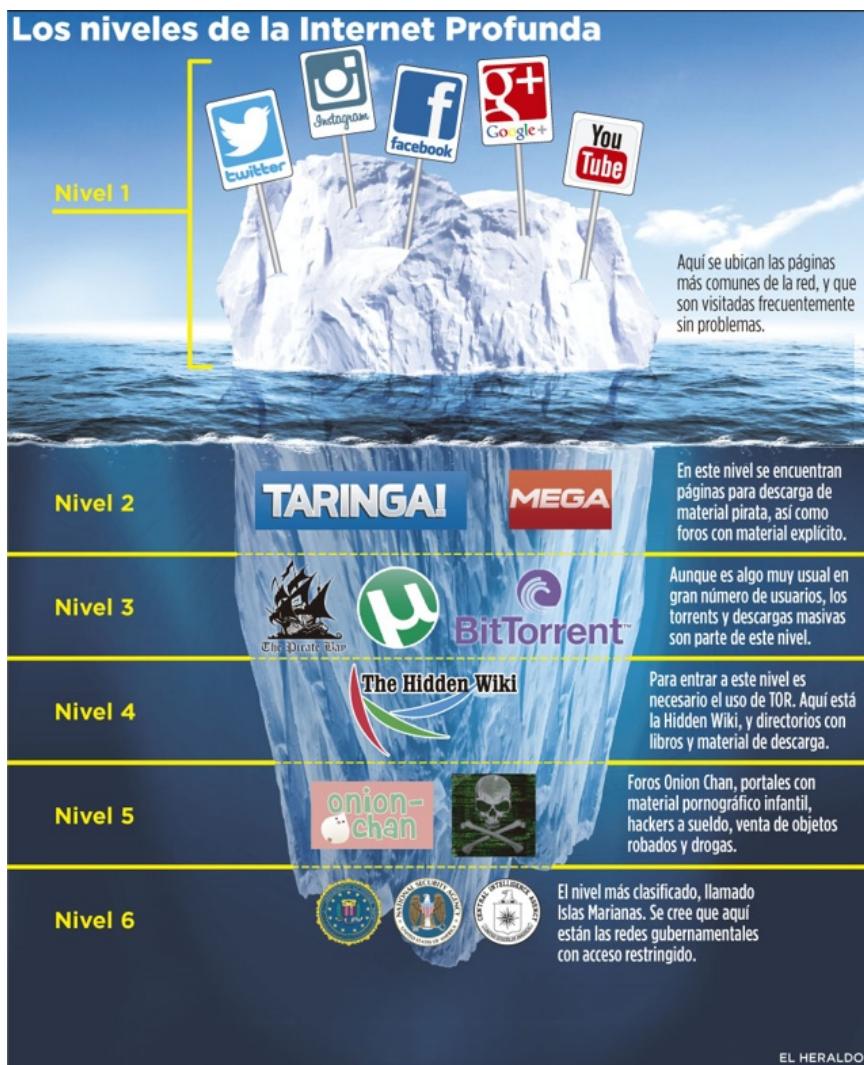
 2.8- Accediendo a la Deep Web.

3- La moneda de Pago de la Deep-Web: El Bitcoin

El concepto de "Deep Web" o de "Internet profunda" es cada vez más popular y está captando más y más usuarios de la red. Internet es una fuente inagotable de información y que buscadores como Google, Yahoo o Bing nos presentan miles de resultados simplemente basándonos en los términos o palabras clave que tecleamos.

1. La estructura de la Deep web

Como hemos comentado, para poder entender mejor qué es la Deep web es necesario imaginarla como un iceberg compuesto por 5 niveles, cada cual más profundo.



El **primer nivel** o también llamado Surface Web se corresponde con la parte de la red a la que se accede desde los motores de búsqueda tradicionales (google, yahoo bing entre otros) Internet visible, aquella que está indexada y fácilmente rastreable.

El **segundo nivel** ya supone estar por debajo de la superficie. Se considera que a este acceden quienes tienen la edad determinada para poder entrar al contenido de las páginas incluidas en él. Aquí, la información ya no se encuentra indexada, ni visible ni rastreada por los motores de búsqueda tradicionales.

El **tercer nivel** ya se conoce propiamente como la Deep Web. Y en este, ya se empieza a encontrar parte del contenido que roza la ilegalidad. Aquí, ya se requiere de un proxy específico para poder acceder, es decir, navegar por dicha parte de la web.

El **cuarto nivel** es considerado como el nivel más profundo conocido dentro de la Deep Web al que comúnmente un usuario puede acceder. Aquí, la mayoría de contenido se considera ilegal.

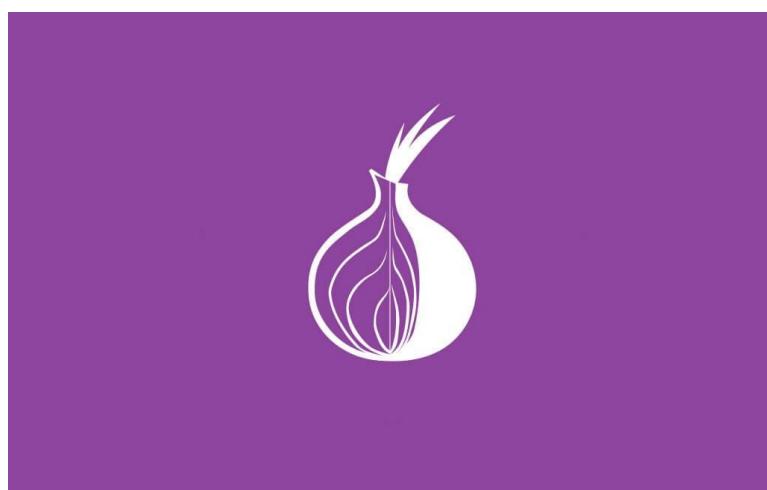
Se entiende que una vez superados estos primeros cuatro niveles se procede el acercamiento a la base del iceberg que se corresponde con la Darknet o Internet oscura. A partir de aquí donde se encuentra una pequeña parte de la deep web. Se dice que en este es donde están los sitios a los que únicamente se puede acceder a través de un software especial como es Tor. Se estaría en el definido como un **quinto nivel**.

A partir de aquí, se puede hablar del Mariana's Web o dark web, como símil al nombre de la fosa más profunda del mundo. Ello es consecuencia del desconocimiento de la verdadera profundidad y contenido de este nivel. Se puede identificar como el mundo de los hackers, en el que solo se conoce la existencia de redes de carácter privado con acceso restringido, en el que no existe ningún tipo de norma ni seguridad.

2. La Red Tor

2.1 Historia

Es un acrónimo de The Onion Router, es decir el enrutamiento de cebolla. Este es un proyecto que busca el poder crear una red de comunicaciones distribuida de baja latencia por encima de la capa de Internet de manera que nunca se revelen los datos de los usuarios que la utilizan, manteniéndose, así como una red privada y anónima. El uso u objetivo más destacado de este proyecto es evitar la censura de determinados contenidos que están bloqueados en internet por ciertos países o causas. Es la red distribuida más famosa y utilizada como herramienta de privacidad y anonimato en Internet.

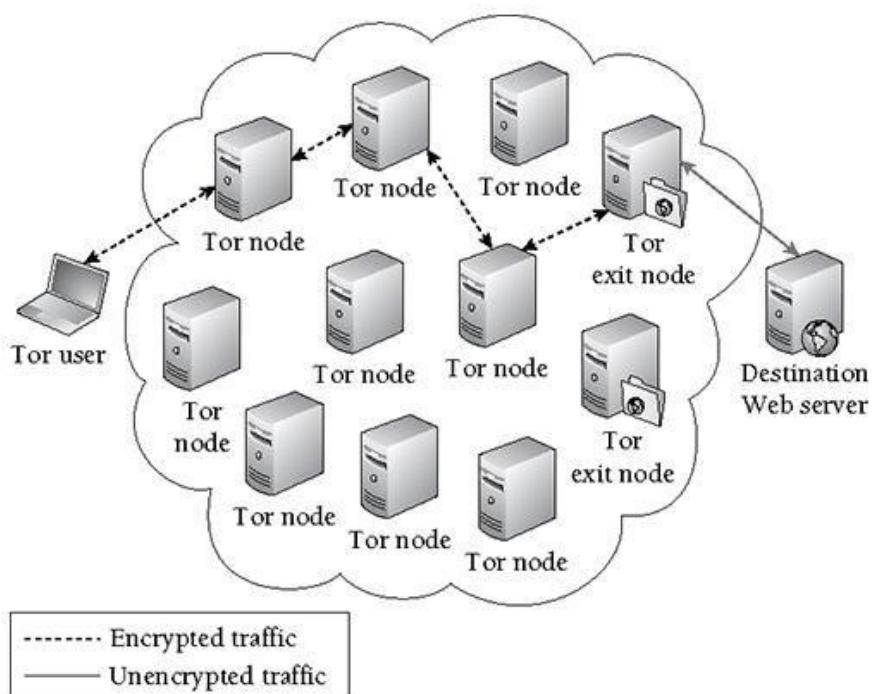


El nombre de dicha red es dado por el tipo de comportamiento que utiliza, estructurado en capas que la conforman el cual permite un acceso a un contenido saltando de una capa a otra capa más profunda impidiendo que las páginas por las que se navega identifiquen la IP desde la cual se accede.

2.2 Componentes de la Red Tor:

La red está compuesta por un conjunto de nodos los cuales se comunican a través del protocolo SSL/TLS (cada nodo mantiene una conexión TLS con el resto de nodos).

Dicho protocolo garantiza las propiedades como la privacidad o la autenticación. También mantiene la integridad ya que los mensajes incluyen un MAC lo que posibilita verificar su no modificación antes de su llegado al destino final. También se mantiene la disponibilidad de los datos ya que la integridad es una condición de la disponibilidad, por lo que si se rompe la información no estará disponible.



Existen dos tipos de nodos: Los **nodos OR o onion routers** (tor-relays), que actúan a modo de encaminadores así como servidores de directorio. Estos mantienen una conexión con cada uno de los otros OR, la cual nunca se cierra conscientemente si no es por inactividad.

Y, por otra parte, los **nodos OP o onion proxy** (Tactical Technology Collective Front Line Defenders, 2016) que se basan en la obtención de información del servicio directorio, crear circuitos aleatoriamente mediante la red así como de control de las conexiones de las aplicaciones de los usuarios. Lo característico de los nodos es que estos son voluntarios, es decir, cualquier persona puede participar en la red Tor como un nodo más configurando su ordenador

Si accedemos desde nuestro navegador tor y obtenemos nuestra ip, en algunos casos, el nodo de tor tiene instalado un servicio web y podemos observar el mensaje:

CUALESMIIP.COM

CUAL ES MI IP | ROUTERS WIRELESS | ROUTERS ENTRADAS

Gestión anuncios WiFi

Cual es mi IP

Tu IP real es **176.10.104.240**
(tor1e1.digitale-gesellschaft.ch)
 No navegas a través de proxy

This is a Tor Exit Router | Digitale Gesellschaft | 176.10.104.240

DIGITALE GESELLSCHAFT

This is a Tor Exit Router

Tor Overview
 Tor Abuse FAQ
 Tor Legal FAQ
 Abuse

This is a Tor Exit Router

Most likely you are accessing this website because you had some issue with the traffic coming from this IP. This router is part of the [Tor Anonymity Network](#), which is dedicated to [providing privacy](#) to people who need it most: average computer users. This router IP should be generating no other traffic, unless it has been compromised.

If you are a Swiss law enforcement official please read also the background information available in [German](#) and [French](#).

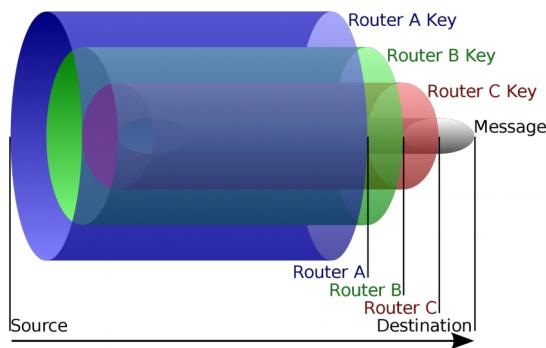
How Tor Works: click here for more information.

Tor sees use by many important segments of the population, including journalists, Chinese dissidents, whistleblowers, activists, whistle blowers, abuse victims, stalker targets, the US military, and law enforcement, just to name a few. While Tor is not designed for malicious computer users, it is true that they can use the network for malicious ends. In reality however, the actual amount of [abuse](#) is quite low. This is largely because criminals and hackers have significantly better access to privacy and anonymity than do the regular users whom they prey upon. Criminals can and do use Tor to commit far larger and more [powerful attacks](#) than Tor on a daily basis. Thus, in the mind of the founders of the organization Digital Society, the social need for easily accessible censorship-resistant private, anonymous communication trumps the risk of unskilled bad actors, who are almost always more easily uncovered by traditional police work than by extensive monitoring and surveillance anyway.

In terms of applicable law, Tor routers explicitly do not contain identifiable routing information about the source of a packet, and no single node can determine both the origin and destination of a given transmission.

The Digital Society is not a communication service provider (CSP) or a provider of defined communication services according Art. 2 of the Federal Act on the Surveillance of Post and Telecommunications from March 16th 2016 (SPTA, SR 780.1). Therefore the association is not required by law to comply with Art. 21 f and 26 f SPTA. There is no obligation to provide information or for data retention. In fact under Swiss privacy law it is forbidden to collect personal data (as IP addresses) as long as it is not transparent, of legitimate purpose and proportionate.

El uso de la criptografía de clave asimétrica es la que impide que cada nodo pueda conocer los otros nodos del circuito con los que no se comunica directamente, siendo el único conocedor, el software Tor del equipo desde el que se accede.



La autenticación es garantizada a través de la criptografía de llave pública, en cuanto a que una de las partes de la comunicación ha de autenticarse para el envío de los datos. El servidor se autentica enviando un certificado SSL firmado por una autoridad certificadora asegurándose que solo el servidor tiene la clave privada. Si no se produce esta la confidencialidad tampoco ya que la comunicación no será segura.

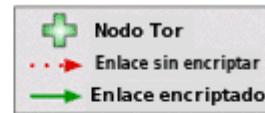
2.3 Funcionamiento interno de Tor:

1 Paso: El software del usuario construye un circuito de conexiones cifradas a través de nodo disponibles en la red, seleccionando tres. Cada uno solo conoce el nodo que le dio los datos y al que le entrega los datos, no teniendo conocimiento de la ruta completa de los datos transferidos.



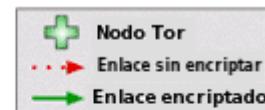
2 Paso: . Una vez el software de Tor selecciona la ruta aleatoria y cifrada se procede a la transferencia de cualquier tipo de dato hasta llegar al servidor de la web que se quiere visitar. Como cada relé o nodo no conoce más que el salto realizado en el circuito no puede vincular el predecesor y sucesor de la conexión.

Ef Cómo Funciona Tor: 2



3 Paso: El software Tor utiliza el mismo circuito en las conexiones realizadas durante unos diez minutos. Una vez transcurridos estos se concede un nuevo circuito, evitando así que se puedan vincular sus acciones realizadas con las que realizará.

Ef Cómo Funciona Tor: 3



Este tipo de enrutamiento produce la ralentización de la carga de los accesos. Por esta razón, puede considerarse que la conexión es más lenta que cuando se accede a los navegadores tradicionales.

2.4 Riesgos del uso de la red Tor:

La parte donde la red Tor es vulnerable es en los nodos de salida, y es que todo el tráfico que viaja desde el nodo de salida a Internet va sin cifrar, por lo que se podría realizar un Man In The Middle para capturar toda la información. [Aquí](#) tenemos encontrar un video muy interesante, donde se analiza durante 24h un nodo tor de salida.

Respecto a los errores del usuario destacamos:

- Uso incorrecto del sistema, accediendo a contenidos, direcciones u objetos con ejecutables incrustados que desvén la comunicación, provocando una fuga en el mecanismo del sistema y se darían a conocer las direcciones IP reales de los usuarios.
- El acceso a sitios web HTTP los nodos de salida pueden ver los paquetes que circulan por ellos, podrían ser sometidos a seguimientos y control. El HTTPS es seguro, evitando que los nodos de salida accedan al contenido transportado, siempre y cuando los servidores a los que accede el cliente sean confiables y se corrobore siempre la veracidad de sus certificados.
- Los problemas propios de Tor se centran en su propio diseño, pudiendo afectar a la privacidad de los usuarios. Por una parte, que los usuarios sean redireccionados a servidores especiales mediante operadores de telecomunicaciones puede facilitar ataques MitM (Man-in-the-Middle) . Estos son conocidos como ataques de correlación de extremo a extremo (end-to-end) ya que el atacante al controlar los dos extremos puede correlacionar las IP con las peticiones enviadas al servidor. Se pueden distinguir entre los de tiempo, estudiando los patrones de temporización, y los de tamaño, mediante el recuento de paquetes.

2.5 Recomendaciones de Uso:

- Ejecutar Tor desde una máquina virtual, aislará nuestra máquina física del malware que abunda en este tipo de webs. Se recomienda la utilización de Tails debido a la cantidad de medidas de seguridad disponibles como puede ser, forzar la totalidad de conexiones salientes.
- se advierte la necesidad de utilizar otras medidas de seguridad que complementen esa carencia, tales como servidores proxy, VPN o cambiar la dirección MAC.
- LLevar a cabo el acceso desde una red pública (o no tan pública..) y no desde el propio router
- Otra sería la inactivación de herramientas del ordenador como son la cámara y el micrófono.

2.6 Dominios .onion :

Hay que tener en cuenta que la Internet Profunda, al ser una red alternativa, las páginas tendrán direcciones (URL) con formato distinto al habitual. Un ejemplo de este tipos de direcciones es : “ <http://am4wuhz3zifexz5u.onion/> ”

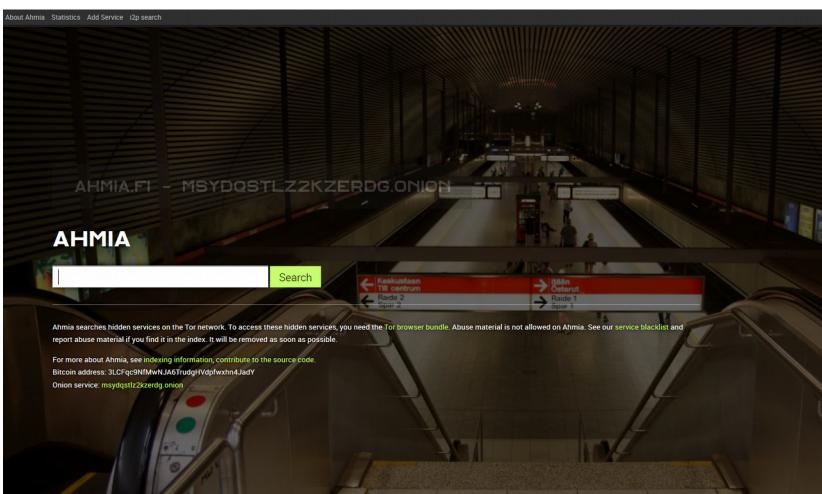
Se les conoce como identificadores conformados por una combinación de 16 caracteres alfanuméricos incomprensibles derivados de la llave pública del servicio oculto. Este número se conformará con cualquier letra del alfabeto y partir de números decimales que empiecen por 2 y acaben por 7 por lo que se obtiene un número de 80 bit en base 32.

Estas empiezan por http ya que siguen siendo una página web pero terminan con ".onion". Es considerado como un dominio de nivel superior virtual, el cual muestra una dirección anónima a la cual se accede a través de Tor, a diferencia de los otros dominios de nivel superior como .com o .org a las que se puede acceder sin este (Castaño Apaza, 2014). El formato completo del mismo sería "x.y.onion", el cual si es desglosado se identifica la "x" como la cookie de 28 autorización y "y" se encarga de codificar el hash de la clave pública. Un ejemplo de dirección .onion podría ser "http://silkroad7rn2puhj.onion/", que se correspondería con el servidor de la página The Silk Road 3.0. Por tanto, estos sitios web tienen nombres de dominio registrados con una raíz diferente a la del Sistema de Nombres de Dominio (DNS) por lo que los nombres de los host se han introducido con un registrador alternativo al de la Corporación de Internet para Nombres y Números Asignados (ICANN)

La principal finalidad de este sistema es garantizar la irrastreabilidad, a diferencia de lo que ocurre en la Web que navegamos habitualmente, ya que en esta se realizan fácilmente seguimientos y se pueden trazar las rutas seguidas por los usuarios.

2.7 Motores de Búsqueda en la Deep Web:

Tal y como se ha especificado anteriormente, la Deep Web no utiliza los buscadores tradicionales por lo que ha desarrollado sus propios tipos de buscador, específicamente diseñados para la red Tor. Entre estos, destaca especialmente el llamado Torch, TorSearch, Duck Go o Grams (se considera el Google de la DeepWeb).



Lo más normal es consultar las webs conocidas como wikis que se utilizan como directorios específicos a partir de los cuales conocemos los servicios que se ocultan en la red Tor. The Hidden Wiki es la principal ya que esta recoge una lista con una amplia clasificación de los servicios ocultos con sus correspondientes direcciones. Pero hay que tener en cuenta que, con el fin de garantizar esa privacidad buscada, los enlaces van variando de pseudo-dominio, teniendo que revisarse continuamente para garantizar su actualización. Aunque también hay que recordar que se puede acceder a esta wiki desde el propio Google. Además también se encuentran otras páginas que sin ser consideradas como wikis presentan listados de enlaces .onion actualizadas.

The screenshot shows a dark-themed website for 'Hidden Wiki | Tor .onion urls directories'. At the top, there's a navigation bar with links for 'HOME', 'HIDDEN WIKI ONION URLs TOR LINK DIRECTORY', and 'MORE DEEP WEB ARTICLES'. A search bar and an RSS feed link are also present. The main content area features a post titled 'Hidden Wiki .onion Urls Tor Link Directory' from September 21, 2013. The post discusses how to browse .onion Deep Web links using Tor Browser and lists various hidden services and search engines. On the right side, there's a sidebar with 'Recent Posts' and 'Recent Comments' sections, as well as an 'Archives' section with links to specific months.

2013
09.21

Hidden Wiki .onion Urls Tor Link Directory

Category: / Tags: no tag / Add Comment

To browse .onion Deep Web links, install Tor Browser from <http://torproject.org/>

Hidden Service lists and search engines

<http://3g2upl4pq6kufc4m.onion/> – DuckDuckGo Search Engine
<http://xmh57jzrnmw6ns1.onion/> – TORCH – Tor Search Engine
http://zqktlw4fecvo6ri.onion/wiki/index.php/Main_Page – Uncensored Hidden Wiki
<http://32rlckwuurif4dv.onion/> – Onion URL Repository
<http://e266al32vpuorbyg.onion/bookmarks.php> – Dark Nexus
<http://5plvsgydwv2gce.onion/> – Seeks Search
<http://2vlqpcqjihmd5r2.onion/> – Gateway to Freenet
<http://nlmymchrmlmbnii.onion/> – Is It Up?
<http://kpynyym6xqi7wz2.onion/links.html> – ParaZite
<http://wikis5auuihwq5.onion/> – Onion Wiki – 650+ working 05.2017 deep web links
<http://kpwz7ki2v5agwt35.onion/> – The Hidden Wiki
<http://idnxcnkn4qt76tg.onion/> – Tor Project: Anonymity Online
<http://torlinkbgs6aabns.onion/> – TorLinks
<http://jh32yy5zgayyyts3.onion/> – Hidden Wiki . Onion Urls
<http://wikijernta4qgg2.onion/> – Hidden Wiki – Tor Wiki
<http://xdagkrnwpc7aaytzh.onion/> – Anonet Webproxy
http://3fyb44wdhnd2ghhl.onion/wiki/index.php?title=Main_Page – All You're Wiki – clone of the clean hidden wiki that went down with freedom hosting
<http://3fyb44wdhnd2ghhl.onion/> – All You're Base
<http://j6imw42ur6dpcl3.onion/> – TorProject Archive
<http://p3igkncehackgtib.onion/> – TorProject Media
<http://kbhpodlnfx3clb4.onion/> – Tor Search
<http://cipollatnumrrahd.onion/> – Cipolla 2.0 (Italian)
<http://dpmfxkaacucuzpc.onion/> – TorDir – One of the oldest link lists on Tor

Marketplace Financial

<http://torbrokerge7zxgq.onion/> – TorBroker – Trade securities anonymously with bitcoin, currently supports nearly 1000 stocks and ETFs

Recent Posts

- Recent downtime of the hidden wiki in march 2017 May 8, 2017
- The Hidden Wiki 2015 January 8, 2015
- thehiddenwiki.org moved to a new server because of DDOS January 8, 2015
- Silk Road 2 got shut down and owner 'Defcon' arrested November 7, 2014
- BBC Horizon showing thehiddenwiki.org in documentary about the deep web September 15, 2014
- Silk Road shutdown, domain seized, DPR arrested (October 2, 2013
- Botnet still slowing down Tor but situation is getting better September 30, 2013
- Check out this new hidden wiki alternative September 4, 2013
- Tor network under huge DDOS September 3, 2013
- Hidden Wiki Videos August 29, 2013

Recent Comments

Archives

- May 2017
- January 2015
- November 2014

2.8 Accediendo a la Deep Web:

EuCanna - First Class Cannabis Healthcare

rst04hutlefirefq.onion

EuCanna

First Class Cannabis Healthcare

Products Info Login Register EuCanna.com

Buds | Oil | Ointment | Suppositories | Creams | Bath Melts

Soaps | CannaCaps | Edibles | Special Offers

Medical Grade Cannabis Buds

We stock high quality hydroponic and organic cannabis. We are experienced professional cannabis growers who place emphasis on the medicinal value rather than the quantity we produce. This is why you will frequently see strains listed with a 50/50 indica-sativa ratio, as these strains are best for making the Rick Simpson Oil.

Product	Price	Quantity
3.5g Organic White Russian	42 EUR = 0.006 B	<input type="text" value="1"/> X <button>Buy now</button>
7g Organic White Russian	80 EUR = 0.011 B	<input type="text" value="1"/> X <button>Buy now</button>
14g Organic White Russian	147.5 EUR = 0.020 B	<input type="text" value="1"/> X <button>Buy now</button>
3.5g Organic Chronic	42 EUR = 0.006 B	<input type="text" value="1"/> X <button>Buy now</button>
7g Organic Chronic	80 EUR = 0.011 B	<input type="text" value="1"/> X <button>Buy now</button>
14g Organic Chronic	147.5 EUR = 0.020 B	<input type="text" value="1"/> X <button>Buy now</button>

ng... Connecting... Kamagra ... Connecting... Connecting... Connecting... Connecting... Connecting... Connecting...

Kamagra For Bitcoin

Products About us FAQs Register Login

Kamagra Tablets

Kamagra 100mg Generic Viagra™ Tablets are a very popular, successful and widely accepted treatment for erectile dysfunction. Manufactured by Ajanta Pharma in clinical 'clean room' conditions, Kamagra is produced to a high quality standard to ensure safety and effectiveness. Patients using Kamagra regularly report successful intercourse and generally continue to use the treatment. The effective treatment time of Kamagra is 4 - 6 hours but many GPs report longer effective times. The active ingredient of Kamagra is Sildenafil Citrate. It belongs to the PDE-5 family of vasodilators. These drugs work by dilating the blood vessels in the body; particularly around the genital area. This in turn, allows stronger blood flow to enable an erection to take place. Kamagra is not an aphrodisiac and stimulation will be required to develop an erection.

Product	Price	Quantity
Kamagra 100mg x 12	15 GBP = 0.002 B	<input type="text" value="1"/> X <button>Buy now</button>
Kamagra 100mg x 24	28 GBP = 0.004 B	<input type="text" value="1"/> X <button>Buy now</button>
Kamagra 100mg x 52	50 GBP = 0.008 B	<input type="text" value="1"/> X <button>Buy now</button>
Kamagra 100mg x 100	78 GBP = 0.012 B	<input type="text" value="1"/> X <button>Buy now</button>

Kamagra Oral Jelly

Kamagra Oral Jelly is a popular and effective treatment for erectile dysfunction. Unlike hard-to-swallow tablets, Kamagra Jelly sachets can be simply squeezed out onto a spoon and swallowed easily. Kamagra Oral Jelly is manufactured clinically in clean room facilities by Ajanta Pharma. Kamagra Jelly is supplied in a range of flavours and quantities may include mint, chocolate, banana, orange, mango, strawberry, pineapple and vanilla. A selection of mixed flavours will be sent in every order. Unfortunately, we are unable to send specific flavours. Kamagra Jelly is quickly absorbed into the body and patients report faster response times from 20 mins. Kamagra Oral Jelly has an effective treatment time of 4 - 6 hours but many GPs report longer times. The active ingredient of Kamagra Oral Jelly is Sildenafil Citrate. It belongs to the PDE-5 family of vasodilators. These drugs work by dilating the blood vessels in the body; particularly around the genital area. This in turn, allows stronger blood flow to enable an erection to take place. Kamagra Jelly is not an aphrodisiac and stimulation will be required to develop an erection.

Product	Price	Quantity
Kamagra Oral Jelly 100mg x 7	18 GBP = 0.003 B	<input type="text" value="1"/> X <button>Buy now</button>
Kamagra Oral Jelly 100mg x 14	35 GBP = 0.005 B	<input type="text" value="1"/> X <button>Buy now</button>

[Board index](#) < Preteens (6-12yo) This area is NOW LOCKED you can use to cross post and view but can not post new topics < Preteen girls

Preteen girls

FORUM	TOPICS	POSTS	LAST POST
Photos Pictures of preteen girls (6-12yo)	21	132	Re: Animated GIF th by gregory Tue Mar 20, 2018 2:18
Videos Videos of preteen girls (6-12yo)	31	178	Re: Serie -- The Ur by DarkHead Sat Mar 31, 2018 2:52

[Board index](#) The team Delete all board cookies

7haz75ietrhjds3j.onion/main3.php

Search Login Reg

All natural spanking:

Album: Boys Date: 02/16/2012 Owner: Gallery Administrator Size: 155 items Views: 244620	Album: Birthdays and playful Date: 02/16/2012 Owner: Gallery Administrator Size: 204 items Views: 190239	Album: Uploads Your uploads Date: 02/16/2012 Owner: Gallery Administrator Size: 1225 items (7407 items total) Views: 248505 	Album: Girls #1 Date: 02/16/2012 Owner: Gallery Administrator Size: 82 items (95 items total) Views: 342384 Comments: 1
Album: Girls #2 Date: 02/16/2012 Owner: Gallery Administrator Size: 153 items Views: 653782 Comments: 1	Album: Videos Date: 02/16/2012 Owner: Gallery Administrator Size: 9 items (10 items total) Views: 655225 Comments: 1	Forum Date: 03/06/2012	Album: Unlisted backup of old files Date: 05/13/2015 Owner: Gallery Administrator Size: 15 items (464 items total) Views: 34327

Page: 1

3. La Moneda de Pago de la Deep Web: El Bitcoin



Venimos hablando de lo que nos podemos encontrar navegando por la **deep web**, ahora bien, todo tiene un coste y esto no es una excepción.

Como hemos comentado anteriormente, **TOR** se centra básicamente en el anonimato, por tanto, tiene poco sentido que se hagan transferencias de dinero real.

Por lo tanto, la solución ideal para realizar transacciones es el **Bitcoin**.

Estamos hablando de una moneda virtual, no controlada por ningún gobierno.

Es un **protocolo** y red **P2P** que se utiliza como **criptomoneda, sistema de pago y mercancía**.

Dicha moneda virtual, ofrece un gran abanico de posibilidades, que hace factible la comisión de delitos dado el anonimato, la mayor privacidad respecto a otras operaciones y la no existencia de esos límites en la cantidad de dinero.

Un claro ejemplo en el que se hizo uso de esta moneda es el virus **WannaCry**, el cual fue un ciberataque masivo a miles de empresas, entre ellas Telefónica, es uno de estos tipos de cibersecuestros por los que los criminales piden un rescate en **bitcoins** a cambio de liberar los equipos.