

TOR: la internet oscura

Dr. Manuel Sánchez Rubio



<https://www.linkedin.com/in/sanchezrum>



@sanchezrum

¿Que es TOR? (I)?

- Es una red superpuesta sobre internet
- El intercambio de información no revela la identidad de los usuarios, es decir, su **IP**
- Mantiene la integridad y el secreto de la información que viaja por ella



¿Que es TOR? (II)?

- Es una red de alta latencia (retardos considerables), no es P2P y solo funciona con tráfico TCP
- Existen nodos de entrada, intermedios y de salida (puedes elegir que tipo quieres ser). Los nodos salida NO van cifrados
- Otras redes anónimas: Freenet Project, i2P, ZeroNet



¿Que es TOR? (III)?

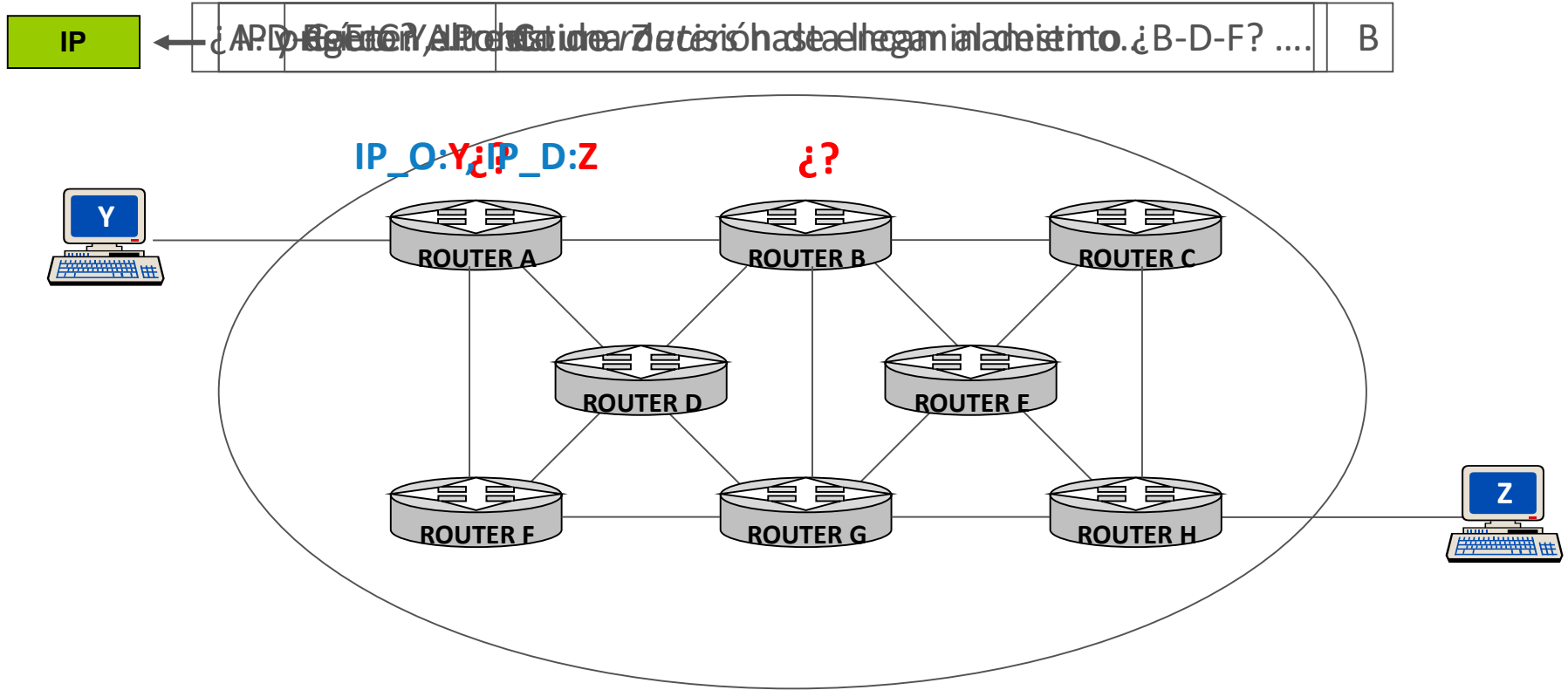
- Los servicios ocultos se identifican con un dominio
 - V2 (16 caracteres)
<https://nytimes3xbfgragh.onion/>
 - V3 (56 caracteres)
<https://7fa6xlti5joarlmkuhjaifa47ukgcwz6tfndgax45ocyn4rixm632jid.onion>

Shallot - <https://github.com/katmagic/Shallot>

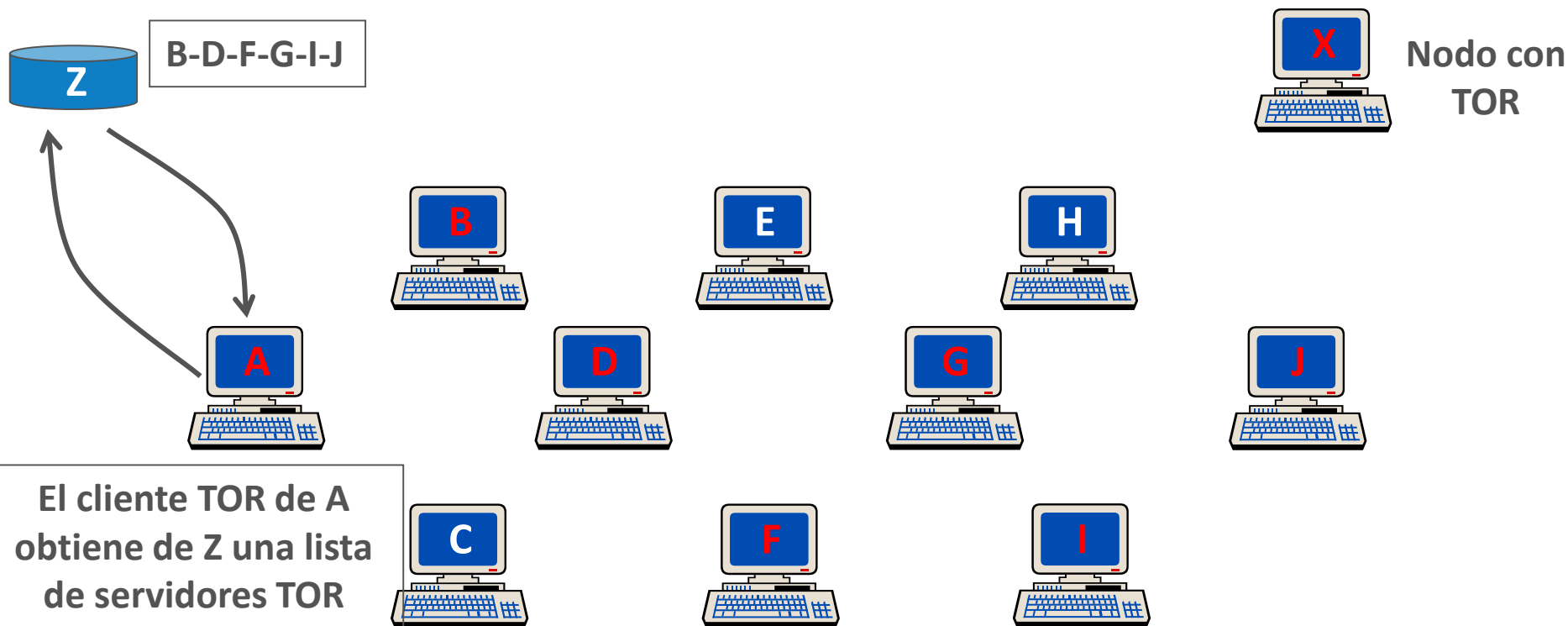
Scallion - <https://github.com/lachesis/scallion>

Generan automáticamente dominios .onion hasta dar con una a nuestro gusto.

¿Como funciona Internet?



¿Como funciona TOR? (I)

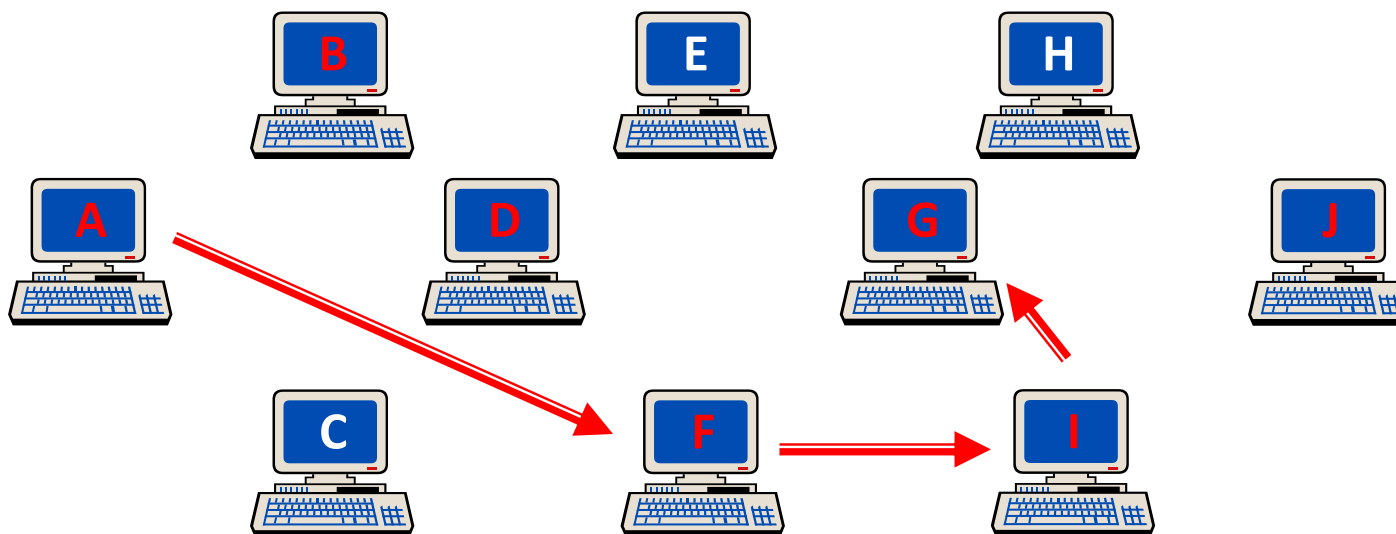


¿Como funciona TOR? (II)

De esta lista de servidores TOR, el nodo TOR A para poder llegar a su destino (G) decide al azar, cuantos va a usar (por ejemplo A-F-I-G)



Nodo con
TOR



¿Como funciona TOR? (III)

TOR funciona como un sistema de **cifrado asimétrico**.

Cada usuario posee dos claves; la **clave pública**, que se puede enviar a cualquier persona y la **clave privada**, solo conocida por el usuario.

Solo lo cifrado con una clave pública puede ser descifrado con la clave privada.

Un remitente usa la clave pública del destinatario para cifrar el mensaje, el cual solo puede ser descifrado con la clave privada del destinatario, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo.

Este cifrado está basado en la factorización de números primos.

¿Como funciona TOR? (y VI)



Hola soy A +

G

=

$E_{G,A}$



Vete a G

$E_{G,A}$

=

$E_{G,I}$

$E_{G,A}$



Vete a I

$E_{G,I}$

$E_{G,A}$

=

$E_{G,I}$

$E_{G,I}$

$E_{G,A}$

CLAVE PÚBLICA

F

I

G

$E_{G,I}$

$E_{G,I}$

$E_{G,A}$

?



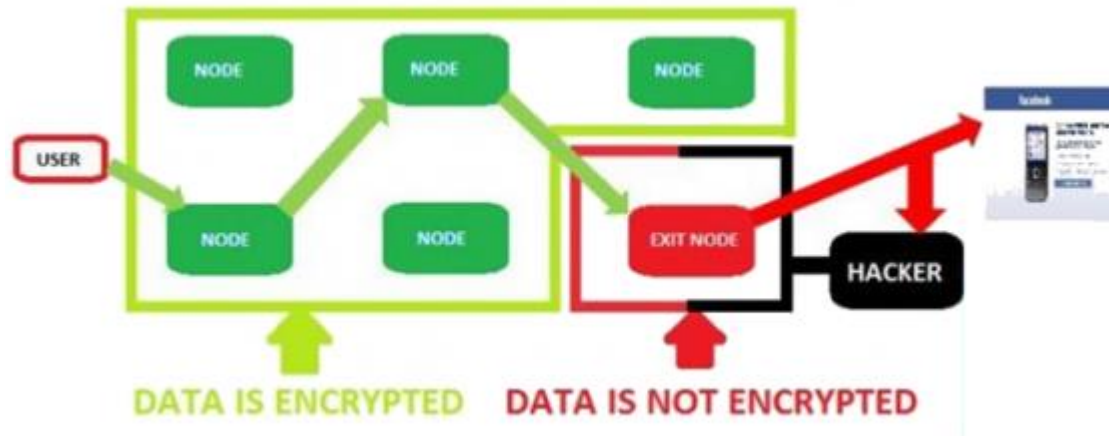
Vete a I

¿Por que se ha vuelto tan popular?

- Proporciona anonimato
- La gente usa Tor para evitar que sitios de internet aprendan sus hábitos de navegación
- Acceso a contenido bloqueado por los ISP
- Permite a usuarios publicar un sitio web y otros servicios sin necesidad de revelar desde donde se publica (anonymous, pedofilia, hackers...). **Deepweb**
- Los periodistas pueden comunicarse desde zonas en conflicto, sin temor a ser detectados
- Evasion de grandes firewalls en países con censura (China)

¿Pero TOR es seguro?

- **Tor garantiza el anonimato, pero no la privacidad.** Si alguien está escuchando el tráfico en el punto de salida, puede leer la información.



Navegando la deepweb



¿Como conectarnos a TOR?

- Instala Tor: www.torproject.org
- Conectar

Basado en Firefox ESR

Incluye extensiones:

- TorButton
- TorLauncher
- NoScript
- HTTPS Everywhere Firefox
- ProxyTOR garantiza la seguridad de los usuarios



- Disponible para Windows, MacOS, Linux y Android
- Cuando finaliza una sesión, borra los datos sensibles relacionados a la privacidad (cookies, historial de navegación, etc)

...antes, unas medidas de seguridad

- Instala Privoxy. Capacidades avanzadas de filtrado que mejoran la ocultación y elimina banners, popups...etc
- No instales pluggins, no habilites nada (flash, realplayer, quicktime...)
- Estando conectado no abras ningún documento
- Para evitar la censura en un País *hostil* o de tu ISP, conéctate a través de un Bridge Relay (obtener en <https://bridges.torproject.org/bridges>)
- Usa HTTPS
- Instala la extensión NoScript para bloquear la ejecución de código Javascript

¿Como navegar?

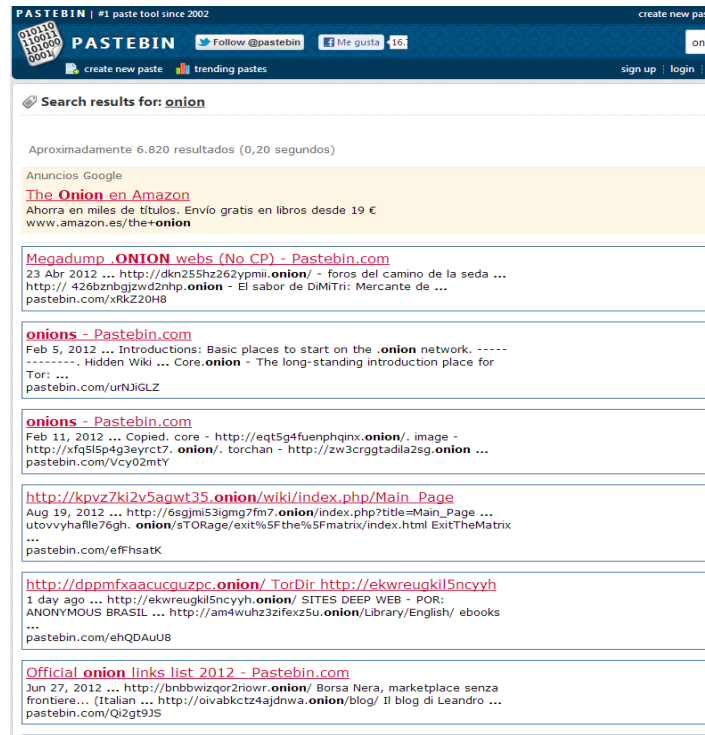
- ¿Y Google? -> NO EXISTE
- ¿Dónde Buscar?
 - Dentro de Tor:
 - Torch
 - Boca a Boca
 - Pastebin
 - Hidden Wiki

– Fuera de Tor:

- Ahmia
- Helios
- Predator

Pastebin

- Entra en pastebin.com y encuentras links a páginas TOR



The screenshot shows the Pastebin website interface. At the top, there's a navigation bar with the Pastebin logo, social media links, and a search bar. Below the navigation bar, there's a search results section for the query 'onion'. The results show approximately 6,820 results. The first result is an advertisement for 'The Onion en Amazon'. The second result is a link to 'Megadump .ONION webs (No CP) - Pastebin.com'. The third result is a link to 'onions - Pastebin.com'. The fourth result is a link to 'onions - Pastebin.com'. The fifth result is a link to 'http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page'. The sixth result is a link to 'http://dppmfxaacucguzpc.onion/ TorDir http://ekwreugkil5ncyvh'. The seventh result is a link to 'Official onion links list 2012 - Pastebin.com'.

PASTEBIN | #1 paste tool since 2002 create new paste

create new paste trending pastes sign up | login | my

Search results for: **onion**

Aproximadamente 6.820 resultados (0,20 segundos)

Anuncios Google

The Onion en Amazon
Ahorra en miles de títulos. Envío gratis en libros desde 19 €
www.amazon.es/the+onion

Megadump .ONION webs (No CP) - Pastebin.com
23 Abr 2012 ... <http://dkn255hz262ypmii.onion/> - foros del camino de la seda ...
<http://426bznbgjzwd2nhp.onion/> - El sabor de DiMiTri: Mercante de ...
pastebin.com/xRkZ20H8

onions - Pastebin.com
Feb 5, 2012 ... Introductions: Basic places to start on the .onion network. ----
-----, Hidden Wiki ... Core.onion - The long-standing introduction place for
Tor: ...
pastebin.com/urNjIGLZ

onions - Pastebin.com
Feb 11, 2012 ... Copied. core - <http://eqt5g4fuenphqinx.onion/>. image -
<http://xfq5l5p4g3eyrct7.onion/>. torchan - <http://zw3crggtadlla2sg.onion/> ...
pastebin.com/Vcy02mtY

http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page
Aug 19, 2012 ... http://6sgjmi53img7fm7.onion/index.php?title=Main_Page ...
utovvyhaffe76gh. onion/sTORage/exit%5Fthe%5Fmatrix/index.html ExitTheMatrix
...
pastebin.com/effhsatK

<http://dppmfxaacucguzpc.onion/> TorDir <http://ekwreugkil5ncyvh>
1 day ago ... <http://ekwreugkil5ncyvh.onion/> SITES DEEP WEB - POR:
ANONYMOUS BRASIL ... <http://am4wuhz3zifexz5u.onion/Library/English/> ebooks
...
pastebin.com/ehQDAuU8

Official onion links list 2012 - Pastebin.com
Jun 27, 2012 ... <http://bnbbwizqor2niowr.onion/> Borsa Nera, marketplace senza
frontiere... (Italian ... <http://oivabkctz4ajdnwa.onion/blog/> Il blog di Leandro ...
pastebin.com/Qi2gt9JS

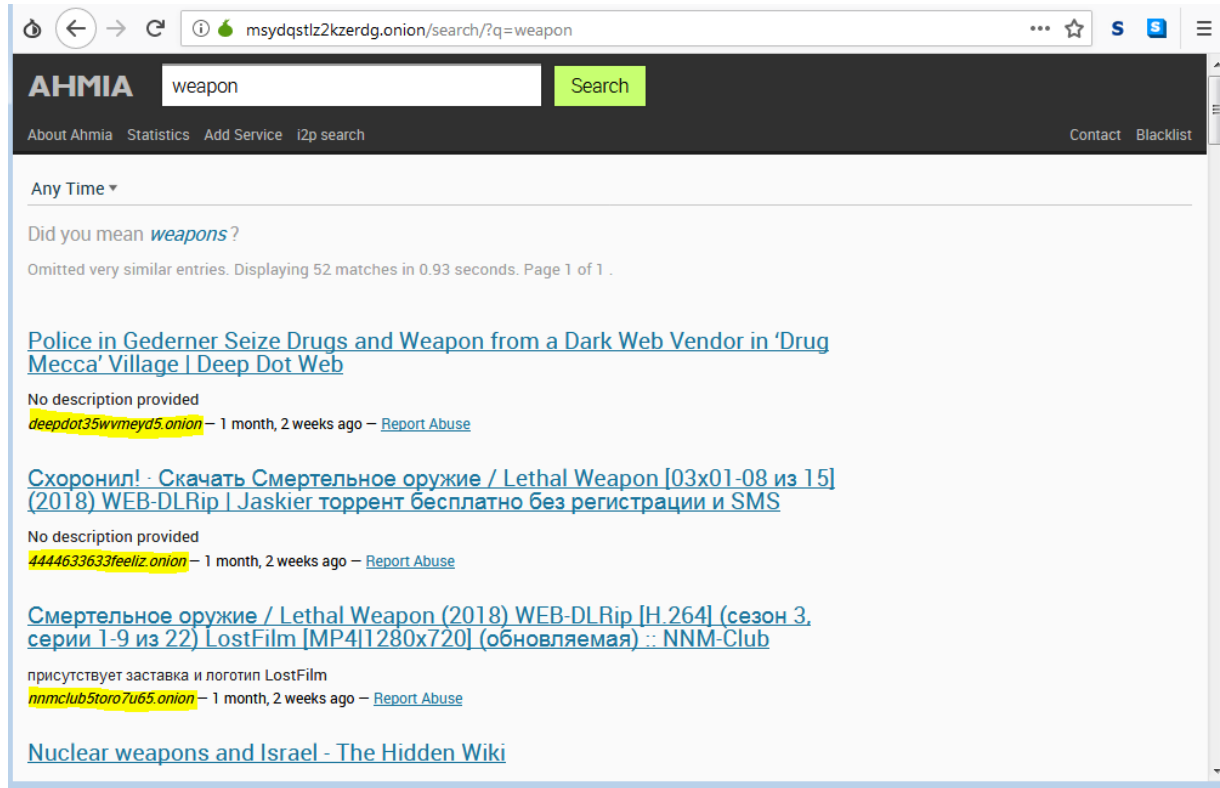
Torch

- Torch: <http://xmh57jrznw6insl.onion>



Ahmia

- Ahmia: <http://msydstlz2kzerdg.onion>



Predator

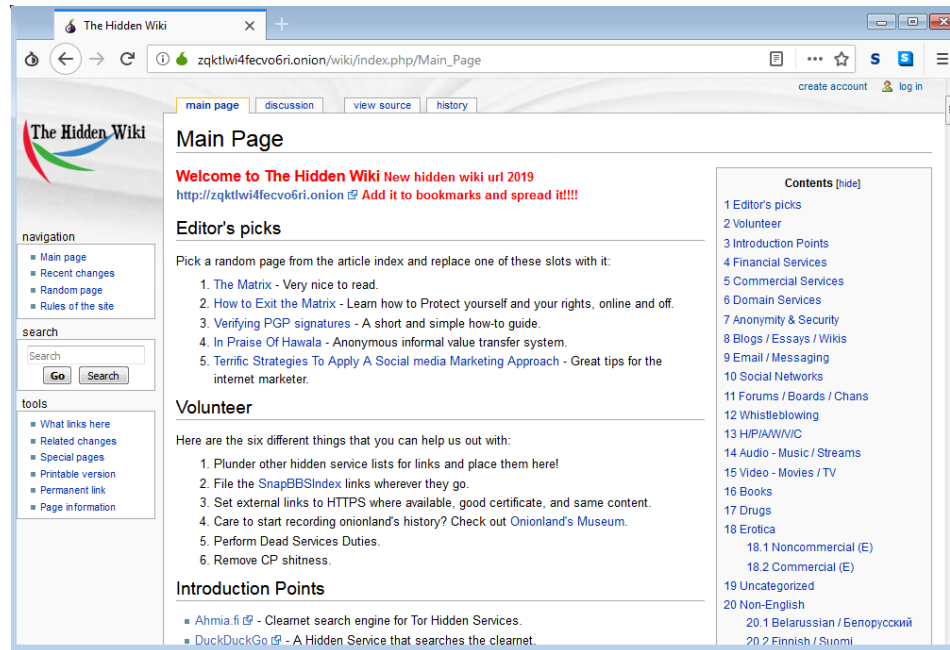
- Nuestra pequeña contribución...



PREDATOR

Hidden Wiki

- Buscador alojado en la Deep Web



<http://zqkltwi4fecvo6ri.onion>

¿Que oculta la Hidden Wiki?

- Chat, email...

Email / Messaging

See also: The compendium of clear net [Email](#) providers.

- [secMail.pro](#) - Complete mail service that allows you to send and receive mails without violating your privacy.
- [Mail2Tor](#) - Mail2Tor is a free anonymous e-mail service made to protect your privacy.
- [Elude.in](#) - Elude.in is a privacy based email service and a Bitcoin/Monero exchange.
- [TorBox](#) - This is a hidden mailbox service only accessible from TOR without connection with public internet.
- [BitMessage](#) - Connects bitmessage and e-mail services. Registration only available using the clearweb link.
- [Protonmail](#) - Swiss based e-mail service, encrypts e-mails locally on your browser. Free and paid accounts.
- [TorGuerrillaMail](#) - Disposable Temporary E-Mail Address.
- [Chat with strangers](#) - Talk to random users anonymously.
- [CTemplar](#) - First ever high end fully encrypted tor email service

¿Que oculta la Hidden Wiki?

- Discusiones politicas

Political Advocacy

- [Men of Action](#) - Volunteer who fights the good side of revolutions and wars
- [Heidenwut](#) - Politics, Occultism, Spy vs Spy, Revolution!! [clearnet](#)
- [BuggedPlanet.Info](#) - Information on Telecommunication Interception Comp
- [PURE EUROPE](#) - Cleanse Europe of the dirt! **Sponsored by HighTimes**
- [Keep Internet Open!](#) - Small unofficial AnonOps site, currently instructing
- [A website](#) - Free speech advocacy. (About 50% uptime.)
- [paraZite #2nd](#), [clearnet 301 redirector](#) - [paraZite](#): Illicit activities advoc
- [Neutering NOT Org](#), [clearnet](#) - Why Non-Human Beings Should NOT Be
- [House of Anonymous](#) - Satirical manifesto regarding anonymous. **Sponsc**
- [paraZite #1st](#), [clearnet 301 redirector](#) - [paraZite](#): Illicit activities advoc
- [FREEFOR](#) - USA-based FREEdom FORces developing a turnkey distribu
- [The Movement of torism](#) - New activist group organized in OnionSpace. S
- [Wake up Europe!](#) - This is a call to arms!

...y el dinero?

Bitcoin lo crea Satoshi Nakamoto en 2009, es open source y no lo dirige persona alguna o empresa.

Silk Road, le da el espaldarazo definitivo como un método de blanqueo y compras ilegales a nivel mundial.

No todo es malo en bitcoin, es usado por inmigrantes para enviar dinero exento de comisiones a sus países, o como “moneda refugio” en países con la inflación disparada (Argentina)

...y el dinero?

ABC Serrano fue el primer centro comercial de Madrid con cajero Bitcoin



...Vayamos de compras!!






Año 2012

1 gram MDMA Excellent Quality



Price 7.32117 BTC

 \$ 97.52  £ 60.00  € 73.96

Ship from United Kingdom

Ship to Worldwide




Stock 6

Created in 2012-09-22 06:40 UTC

Last update 2012-12-16 15:05 UTC

Your balance isn't enough to buy this item! Please deposit the needed funds before.

Description

 1 grams | "Kryptonite" | Excellent Quality  MDMA 

Product

This listing is for 1 grams of **AMAZING Quality** Kryptonite MDMA.

This is superbly made very very strong, high quality MDMA.

The gram comes as one whole rock, very transparent and very clean.

(MDMA over time breaks down and becomes brittle, causing impurities inside the rocks, which leads to a white dusty oxide forming on the outside layer, and it no longer being transparent.)

Shipping

As with all my products I'll provide fast, stealth, and discreet packaging/shipping.

- Please visit my profile for info on myself and my business.

Happy buying

Drug Market, Drogas

DrugMarket

Shopping Cart (1) | Messages (0) | Orders (0) | Account (฿0.0000)
Logged in as deanOliver Logout

Drugs 2303
Cannabis 579
Dissociatives 53
Ecstasy 325
Opioids 83
Prescription 253
Psychedelics 467
Steroids/PEDs 245
Stimulants 298

1 GR Pure Cocaine

Tipos

Nota de los usuarios

Destino posible

Item info:

seller	frankmatthews 97.6
ships from	Netherlands
ships to	Worldwide
category	Cocaine

add to cart discuss 0 report

Precio

price

฿0.0239

postage options:

free shipping worldwide no shipping to usa (฿0.000)

Pure Cocaine straight off the brick!

Reviews: [Click here for more](#)

★★★★★ 2 days, 2 hours

Looks the ticket - trusted seller - not bad delivery for over xmas and international!

★★★★★ 2 days, 7 hours

Black Market



[\(more photo\)](#)

PTR GREEN GI SPECIAL EDITION .308 G3

Caliber: .308 Winchester / 7.62x51mm NATO
Capacity: One 20 round magazine included
Barrel: 18" Match Grade Barrel, 1:10 twist rate
Length: 40.5"
Weight: 9.5 pounds

\$890 (0.2453 BTC)

amount



[\(more photo\)](#)

CENTURY ZASTAVA N-PAP M70 AK-47

Caliber: 7.62x39mm
Capacity: Two 30 round magazines included
Barrel: 16.25" Hammer Forged Barrel, 1:10" twist
Dimensions: 36" long
Weight: 7.9 pounds

\$590 (0.1626 BTC)

amount



[\(more photo\)](#)

KRIISS VECTOR SDP .45 ACP SPECIAL DUTY PISTOL


Caliber: .45 ACP
Capacity: One 13 round magazine included
Barrel: 5.5", 1:16" twist, threaded muzzle
Length: 16"
Weight: ~5.4 pounds

\$1450 (0.3996 BTC)

amount

Asesinos a sueldo

Hitman Network



We are a team of 3 contract killers working in the US (+Canada) and in the EU. Once you made a "purchase" we will reply to you within 1-2 days, contract will be completed within 1-3 weeks depending on target.

Only rules: no children under 16 and no top 10 politicians.

Product	Price	Quantity
We kill your target in the USA/Canada	10000 USD = <input type="text"/> \$	<input type="text" value="1"/> x Buy now
We kill your target in the European Union	12000 USD = <input type="text"/> \$	<input type="text" value="1"/> x Buy now

Compra de cuentas Pay-Pal

Prices

PayPal account with 100USD sending limit with fake contact info, e-mail account, etc. – 3 BTC

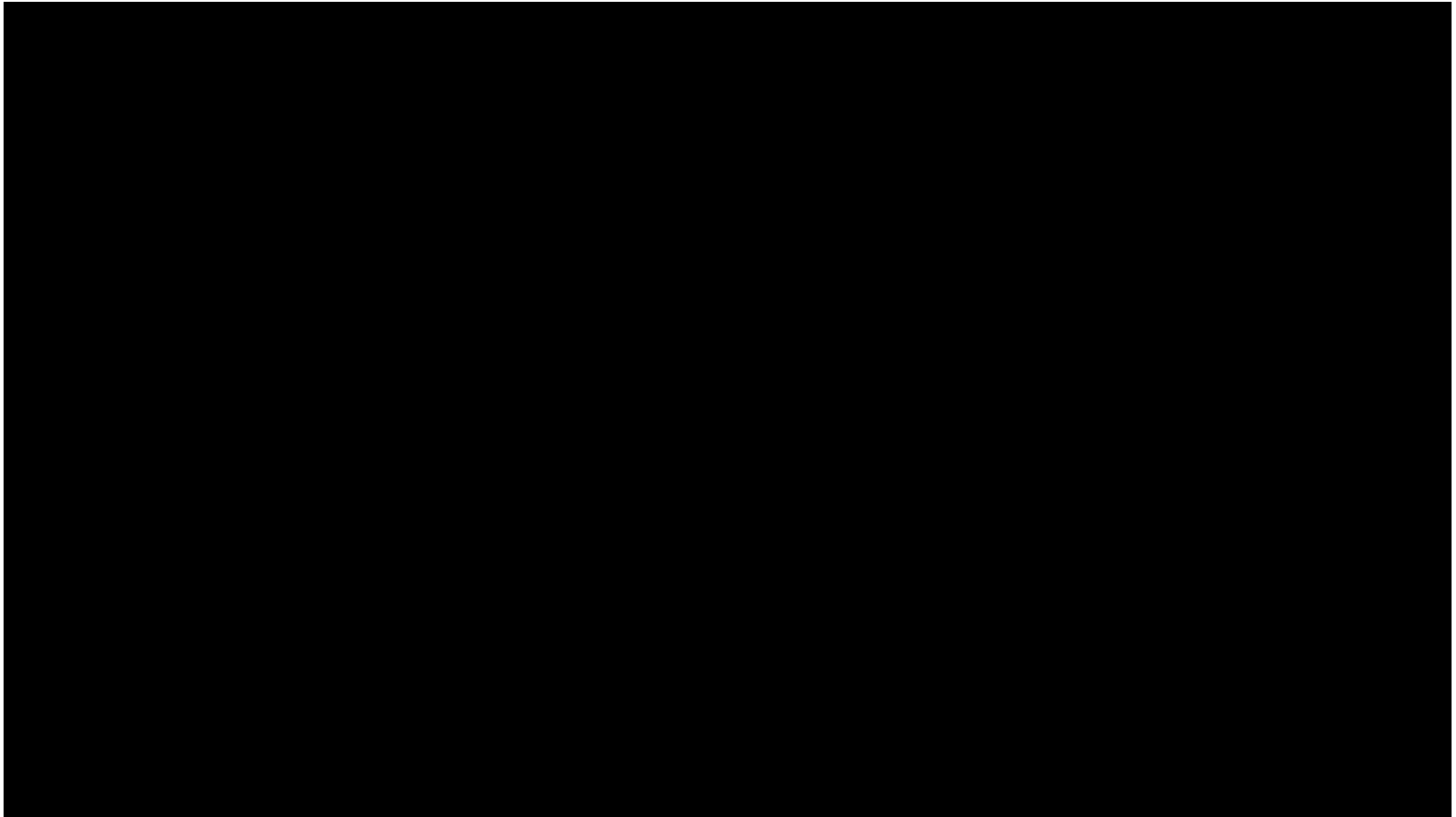
PayPal account with 2000USD sending limit with fake contact info, VCC, e-mail account, etc. [MOST POPULAR] – 10 BTC

Verified PayPal account, including fake contact info, associated e-mail account, etc. – 15 BTC

Hacked PayPal account, with linked bank account, e-mail account – Contact for price ***NONE IN STOCK***

Unlimited access/speed PPTP VPN with setup help included [HOT] – 15 BTC ***NO LONGER AVAILABLE FOR NOW***

Contratar un hacker



Santiago Cervera entrega al juez sus ordenadores, tabletas y móviles

EP / NAVARRA | Día 21/12/2012 - 16.42h

TEMAS RELACIONADOS

► Santiago Cervera

► El exdiputado fue imputado la semana pasada en la investigación por un supuesto chantaje al presidente de Caja Navarra



EFE

E-mail

- ProtonMail: protonirockerxow.onion



The image shows the ProtonMail login interface. At the top is the ProtonMail logo. Below it is the heading "INICIO DE SESIÓN" with a user icon. There are two input fields: "Nombre de usuario" and "Contraseña" with an eye icon for toggling visibility. A white button labeled "INICIAR SESIÓN" is below the fields. A link for help or alternative versions is present: "¿No puede para entrar? Obtenga [ayuda](#) o pruebe [con otra versión](#)." Below this is a link for new users: "¿Nuevo en ProtonMail?" followed by a white button labeled "CREAR CUENTA". The background is a blue gradient with a mountain silhouette.

Herramientas - Mail2TOR

**CREACIÓN DE UNA CUENTA
DE CORREO EN
TOR**

Herramientas - OnionShare

OnionShare:
Compartir archivos a través de la red tor



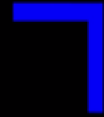
Herramientas – Crear un servicio oculto




Crawling



BUSCA TOR



Silk Road

**Silk Road**
anonymous market

messages 0 | orders 0 | account B0

Search

Go

Shop by Category

Drugs 4,086

- Cannabis 983
- Dissociatives 77
- Ecstasy 318
- Opioids 350
- Other 157
- Precursors 18
- Prescription 901
- Psychedelics 587
- Stimulants 405

Apparel 82

Art 5

Books 778

Collectibles 15

Computer equipment 42

Custom Orders 27

Digital goods 369


Drug paraphernalia 152

Electronics 36


Erotica 296

Fireworks 5


Food 4




100 x Anadrol 50MG
Oxymetholone (sealed)
\$12.41




1 gram MDMA
\$5.89




1/2g Cocaine
\$5.44




10 Pieces White Heart
130-150mg MDMA Content
\$4.49




Red and White Filter (10
packs x 20 cigarettes)
\$1.90



VEGA 100mg Sildenafil
citrate 4 tablets
\$1.50



10 gram Santa Maria
\$11.58



1/4 oz G13
\$8.13

Otros "supermercados" clausurados

[Silk Road](#) era en 2011 el "Amazon de las drogas" y otros productos clandestinos.

Las fuerzas de seguridad desmontaron otros *súpermercados*, como [AlphaBay](#), Hansa o Wall Street Market, pero no han sido tan notorios.

No olvidéis que nosotros no estamos en el lado oscuro



Muchas gracias