

Comunicaciones Seguras

Anonimato con Tor

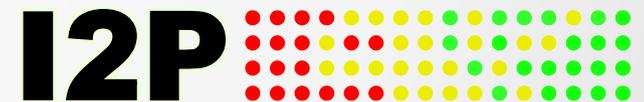
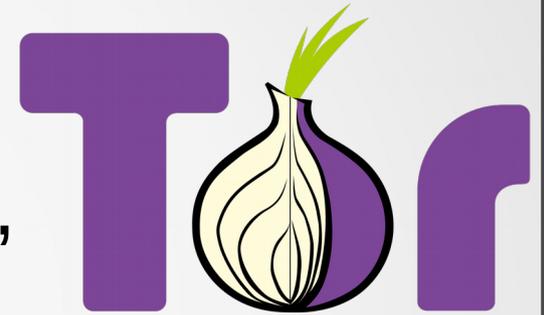
Rafael Bonifaz: rafael@bonifaz.ec

¿Por qué anonimato en Internet?

- Toda actividad en Internet deja huella
- Dirección IP
- Ubicación geográfica
- Búsquedas asociadas a una persona
- Hacer denuncias
- Filtrar información a Wikileaks
- Mucho más

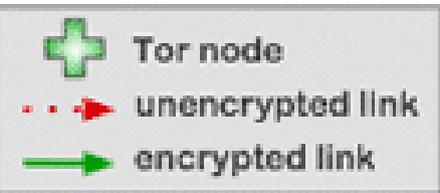
Opciones de anonimato

- Tor es la opción más reconocida y funciona solo con TCP
- I2P cumple objetivos similares a Tor, pero técnicamente diferente
 - Soporta TCP y UDP
- FreeNet es red de distribución de información descentralizada, resistente a la censura
- VPNs



¿Cómo Funciona Tor?

How Tor Works



Alice

Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.

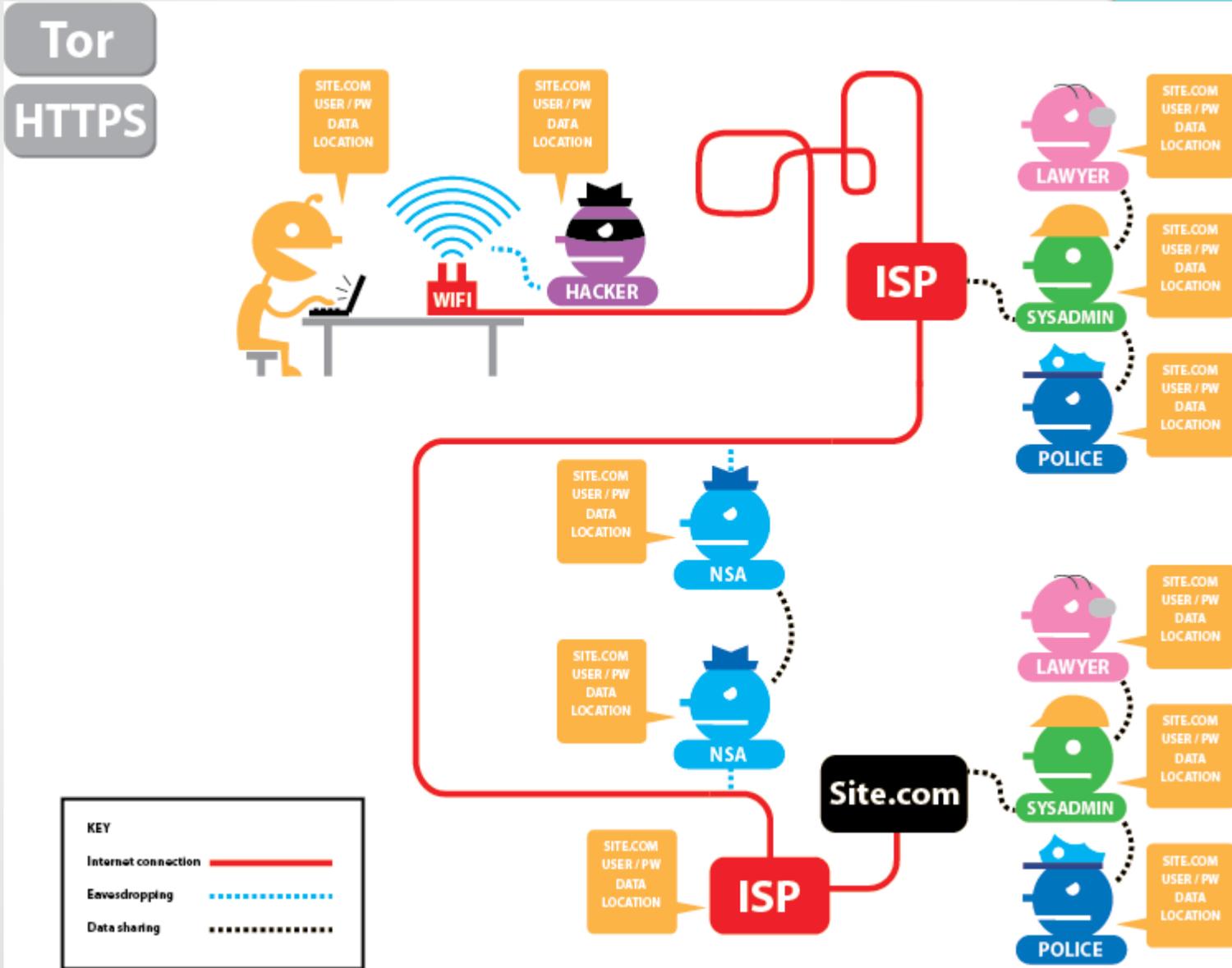


Jane

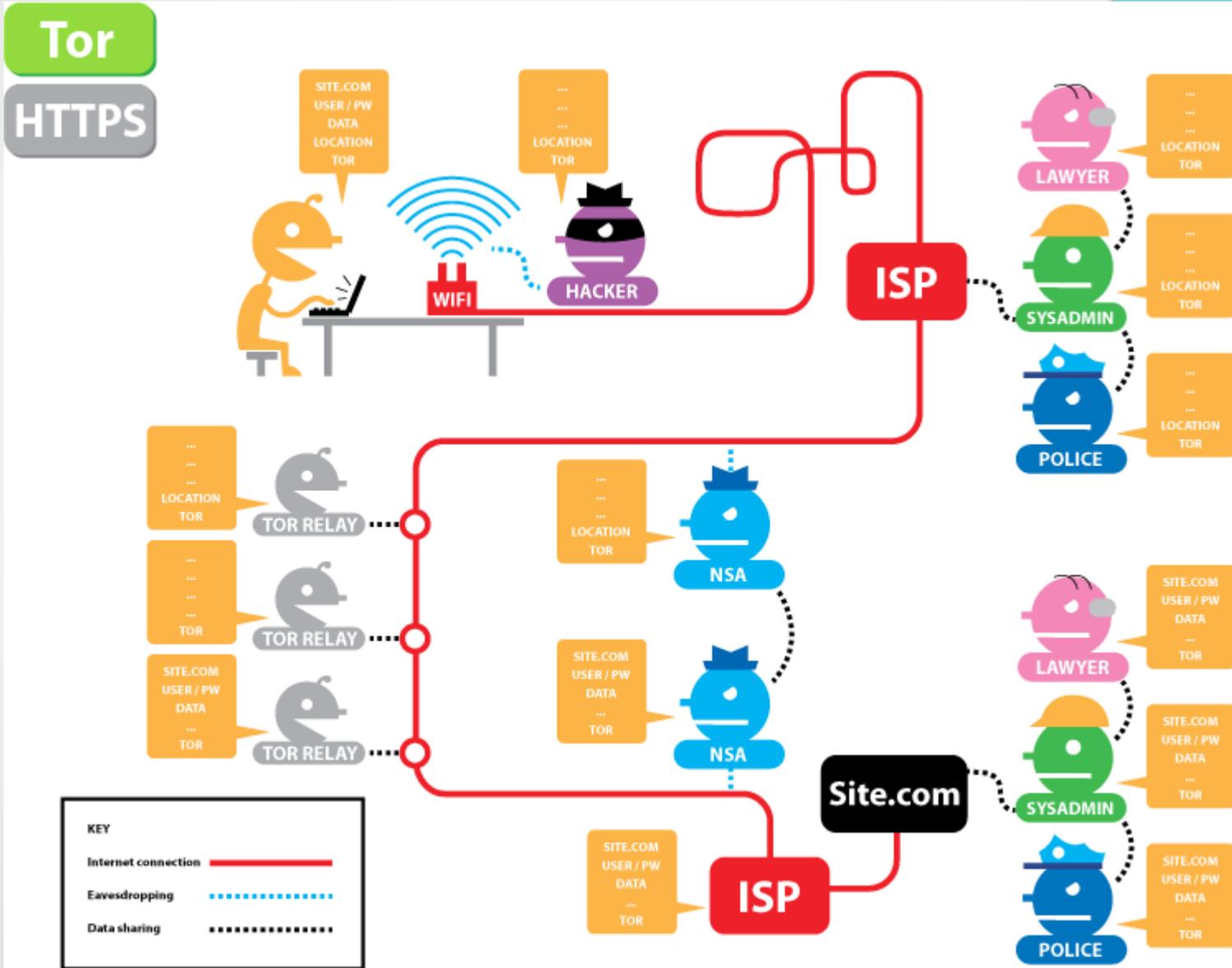


Bob

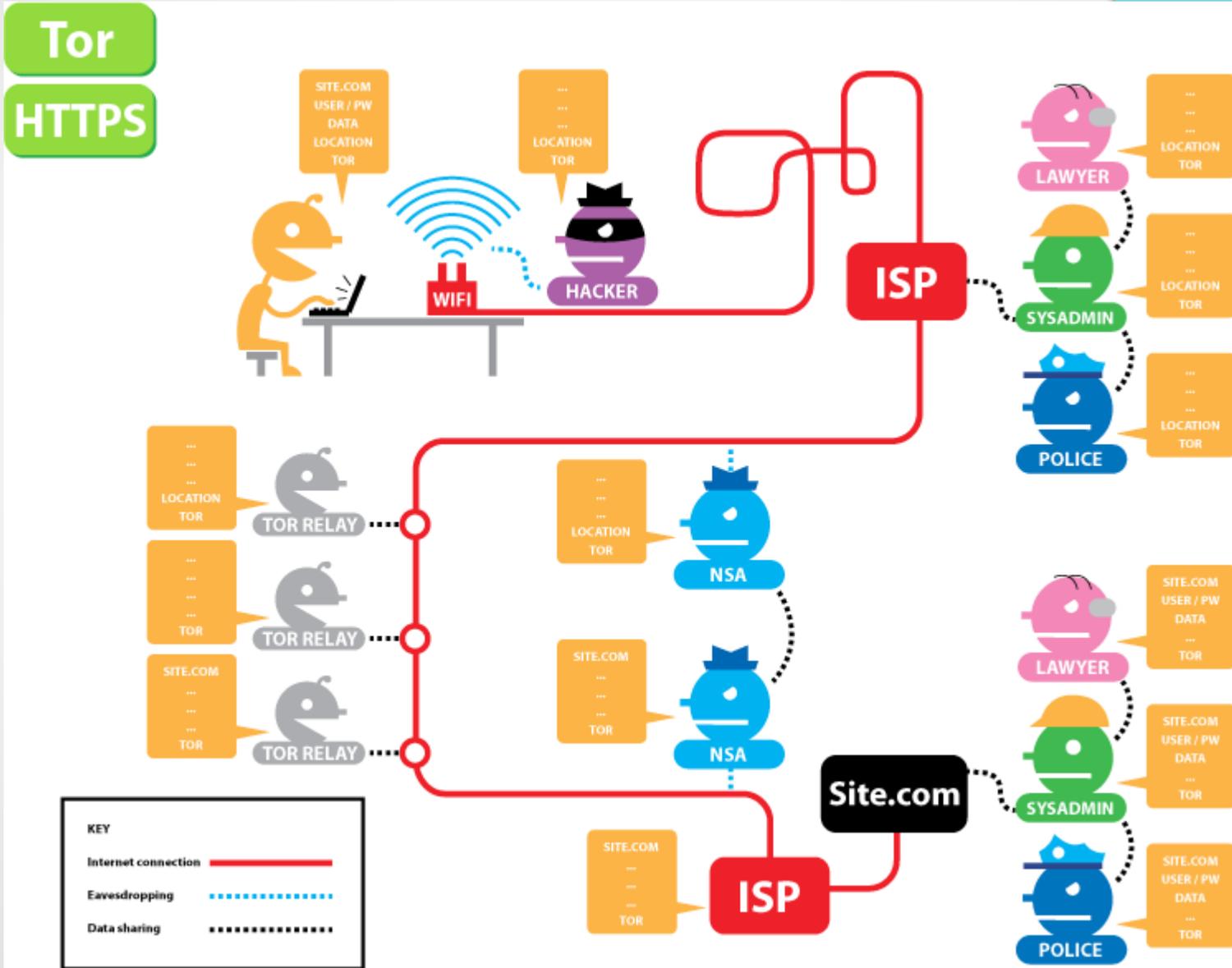
Sin Tor y sin HTTPS



Con Tor y sin HTTPS



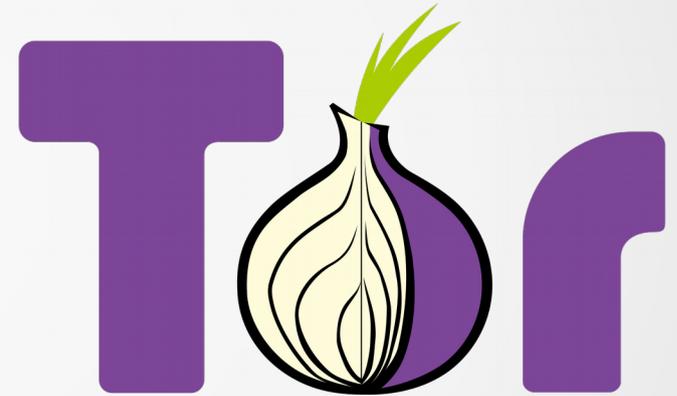
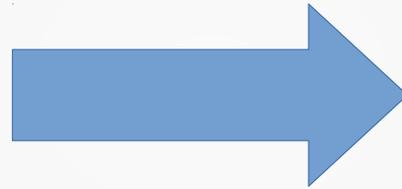
Con Tor y sin HTTPS



Tor y servicios ocultos

- Existen sitios del tipo <http://abcxyz.onion> que son accesibles solo a través de Tor
- La comunicación es siempre cifrada
- Parte importante de la Deepweb, Darknet, etc.
- El servidor nunca sabe desde donde se conectan los clientes
- La ubicación del servidor es secreta
- Wikileaks: <http://wlupld3ptjvsgwqw.onion>

Tor permite ocultar metadatos



La NSA y Tor

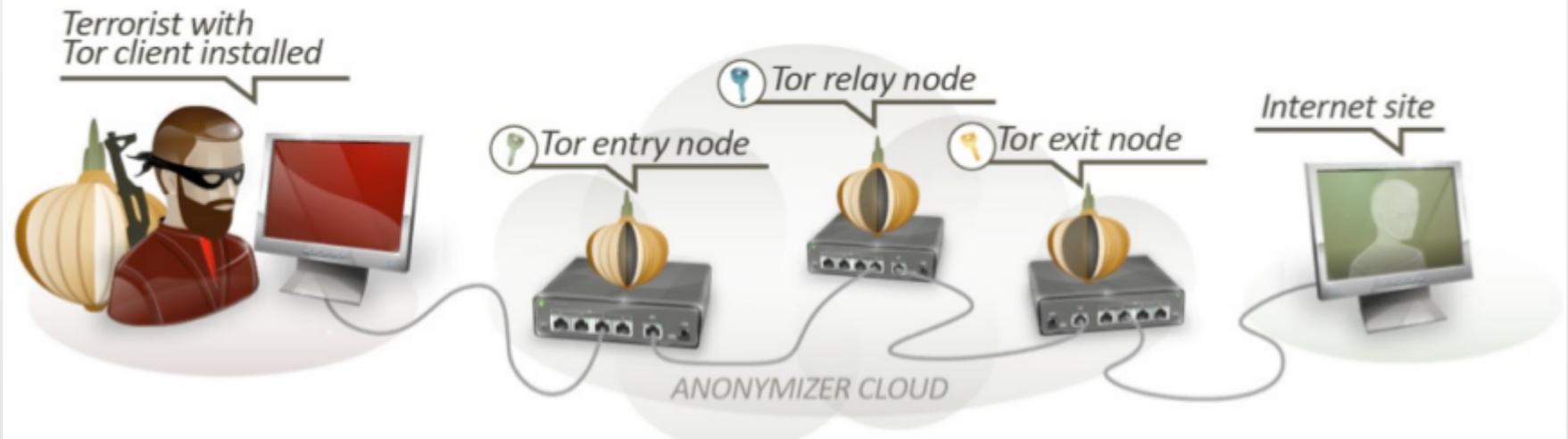
- Tor es financiado principalmente por el gobierno de EEUU
- Tor es software libre
- Tor es una red con miles de nodos
- Los nodos se seleccionan de forma aleatoria en el cliente
- Según presentación filtrada por Snowden para la NSA “Tor Stincks”

La NSA y Tor



Stinks (U)

Analytics: Circuit Reconstruction (S//SI)



<https://edwardsnowden.com/2013/10/04/tor-stinks-presentation/>

¿Cómo obtener Tor?

- Se descarga desde <https://www.torproject.org/>
 - Importante verificar que se use https
- Se recomienda utilizar Tor Browser
 - Firefox modificado con Tor incluido
- En distribuciones basadas en Debian se puede usar el paquete **torbrowser-launcher**
- Se puede instalar Tor sin navegador
 - Utilizar para otros programas sin necesidad de abrir navegador

Manos a la obra

software libre (Software) en DuckDuckGo - Navegador Tor

Archivo Editar Ver Historial Marcadores Herramientas Ayuda

software libre (Softw... x + 1

https://duckduckgo.com/?t=disconnect&x=%2Fhtml&q=software+libre&ia=abo | Buscar

2

3

5

4

6

Nueva identidad (nueva instancia y conexiones de Tor) Ctrl+Mayús.+U
Nuevo circuito Tor para este sitio Ctrl+Mayús.+L
Configuración de privacidad y seguridad...
Configuración de red Tor...
Comprobar actualización del Navegador Tor...

Circuito Tor para este sitio (duckduckgo.com):
Este navegador
Holanda (Países Bajos) (83.162.202.182)
Francia (51.254.218.247)
Dinamarca (185.129.62.63)
Internet

Libre is a generic library for real-time communications with asynchronous I/O support (BSD Revised, Voip, SIP, RTP, ICE).
Más en Freshmeat

Free software - Wikipedia, the free encyclopedia
Free software, freedom-respecting software, software libre, or libre software is computer software distributed under terms that allow users to run the software for ...
en.wikipedia.org/wiki/Software_libre

LibreOffice - Free download and software reviews - CNET ...
LibreOffice is a free suite of apps for creating text documents, spreadsheets, presentations, and more, which you can then save in Microsoft Office formats.
download.cnet.com/LibreOffice/3000-18483_4-75337651.html

Software Libre (spanish audio) - YouTube

Enviar comentarios

En colaboración con YAHOO!

Interfaz navegador Tor

- 1) Botón Tor: configuración de Tor
- 2) Nueva identidad: cierra y abre Tor desde cero
Nuevo circuito: nuevo circuito para ese sitio
- 3) Configuración de privacidad y de red
- 4) Comprobar actualizaciones
- 5) Configuración de Noscript
- 6) Nodos por los que pasa el circuito a través de Tor

Tor en celular

- Se instala el paquete **Orbot** desde **F-droid** o **Google Play**
- Puede funcionar como proxy transparente
- Orfox equivale al navegador de Tor
- Aplicaciones como Twidere, Covnersations,
- **Un celular es un terminal vulnerable**

Problemas al usar Tor

- No todas las páginas funcionan
- Hay que resolver captchas
- Cloudfare
- Es más lento
- Cada vez es más difícil abrir un correo

Correo electrónico amigable con tor

- [Bitmessage.ch](https://bitmessage.ch/) - <https://bitmessage.ch/>
- [Cock.li](https://cock.li/) - <https://cock.li/> (various domains available).
- Mail2Tor: <http://mail2tor2zyjdctd.onion/>
- RiseUp - <https://help.riseup.net/> (need invite).
- Sigaint - <http://sigaint.org/> <http://sigaintevyh2rzvw.onion/>
- Tutanota - <https://tutanota.com> (48 hours to check you).
- Unseen.is - <https://www.unseen.is/> (requires secondary e-mail address; can be slow to load).
- VFEMail - <https://vfemail.net/>

Tomado lista de correo Tor

<https://lists.torproject.org/cgi-bin/mailman/listinfo/tor-talk>