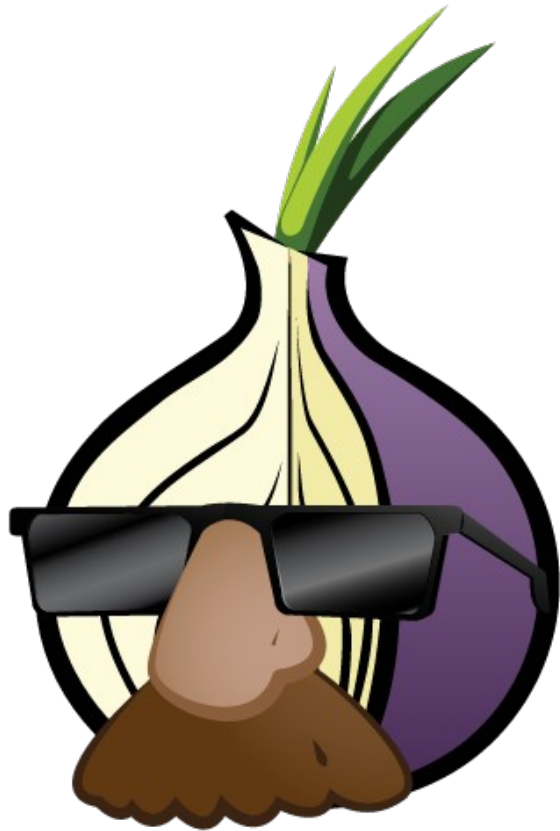


TORtilla con Cebolla



→ The Onion Router
&
The Deep Web

TORtilla con Cebolla


Marco Fernández Pranno

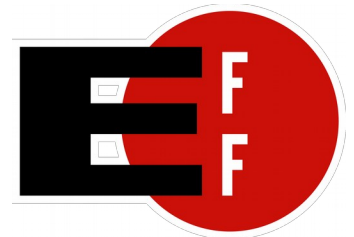
(Totally me)

(github.com/MarFerPra)



Qué os voy a contar ?

- Qué es TOR (Y ¿Por qué existe?)
- The Tor Foundation (+ EFF)
 - Free software saves the day
- Seguridad vs Privacida 
 - “Mass Surveillance and Targeted Surveillance”
- Darknet (Deep Web)
- ¿OPSEC? ¿Eso se come?



¿ Qué es TOR ?

- Navy → EFF → Tor Project Foundation
- Red distribuida (TCP)
- “Privacy by design” → No logs, no control
- Premio por la Free Software Foundation
- **Idea → Intermediarios no conocen el destino ni el origen de los paquetes.**

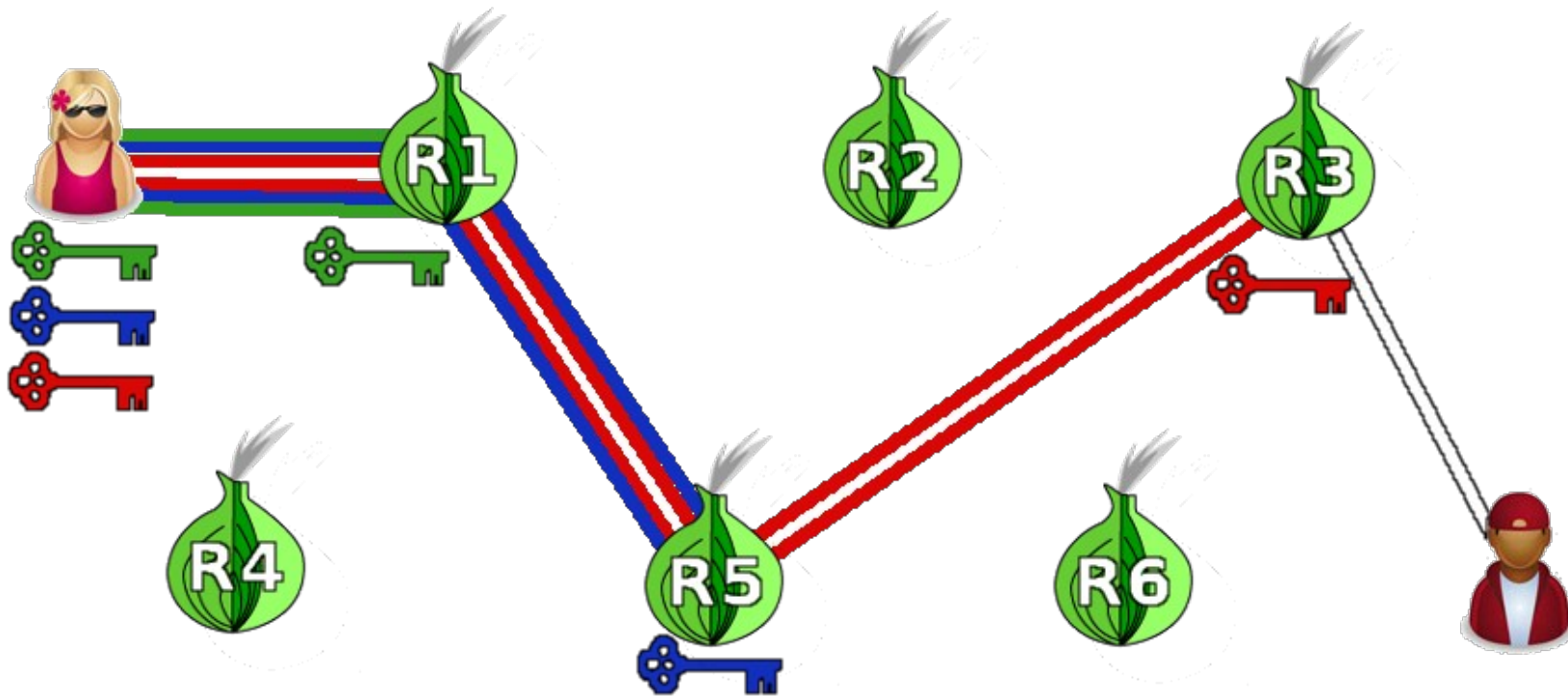
Ámbitos de uso:

- Conflictos políticos
- Restricciones en la difusión y/o acceso a la información
- Comunicaciones confidenciales

¿Qué es TOR ?


- Onion Routing:

- Nodo de entrada (**Guard**) → Nodo intermedio (**Relay**) → Nodo de Salida (**Exit node**)

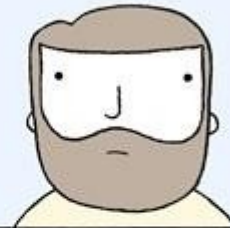


WILL WE FIND INTELLIGENT
LIFE?

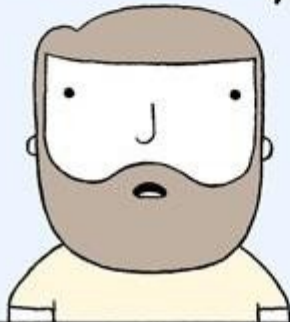
COULD IT BE RIGHT HERE
ON EARTH?



COULD IT
BE THIS
MAN?



I use TOR so
no one can
track me.



THE SEARCH CONTINUES

¿ Qué **NO** es TOR ?

- Bulletproof

TOR → Ocultar identidad

VPN's → Privacidad

- No actúa en capas superiores de la comunicación

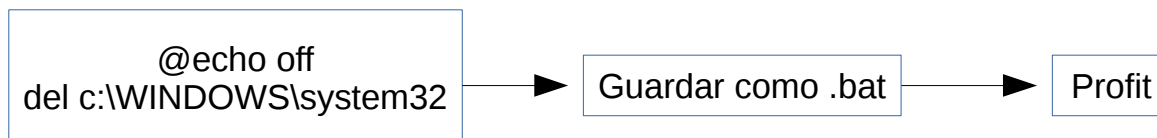
Tener en cuenta:

- Cookies
- Cabeceras HTTP
- Peticiones DNS no redireccionadas por TOR
- Plugins (Flash, Java, etc)

Soluciones

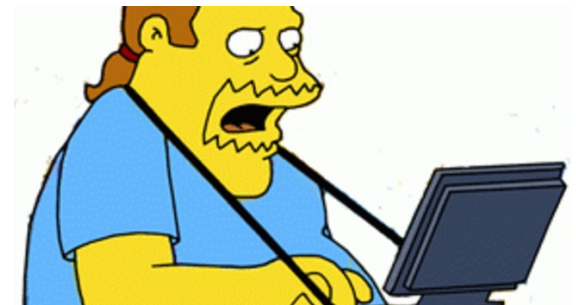
- Configurar correctamente el cliente
- No permitir tráfico fuera de TOR
- Siempre, siempre, SIEMPRE: HTTPS (HTTP + SSL)
- No permitir plugins
- Si una aplicación no soporta SOCKS: torify (Linux)

→ En Windows:



Tipos de nodos

- Onion Router (**OR**):
 - Routers y servidores de directorio
 - Entre sí mantienen TLS abiertas
 - Conexiones OR-OR → permanentes
- Onion Proxy (**OP**):
 - Software ejecutado por el usuario
 - Obtiene info de la red → establece caminos aleatorios
 - Canaliza el tráfico TCP a la red TOR
 - Conexiones OP-OR → no permanentes



Servicio de directorio:

Son OR con operadores de confianza/conocidos

Mantienen y difunden la BD con la información de los OR

Sólo se publican OR aprobados

→ Se monitorizan y aprueban de forma manual

Cuando un nuevo OR se conecta a la red, se define a sí mismo exponiendo su funcionamiento y capacidades:

→ Versión

→ Banda ancha

→ Política de enrutamiento (Si es *exit node*)

Claves OR:

Cada OR tiene una serie de pares de claves pública/privada

- *Identity Key*: firmar información sobre el propio OR, o como servicio de directorios
- *Onion Key*: cifra peticiones para establecer circuitos y negociar claves DH.
- *Connection Key*: usada en el *handshake TLS*. Se cambia cada 24 horas. En el handshake entre OR's se firma la CK con la IK, y se envía junto con la IK autofirmada

Células

- Paquetes de información con los que se comunican los nodos.

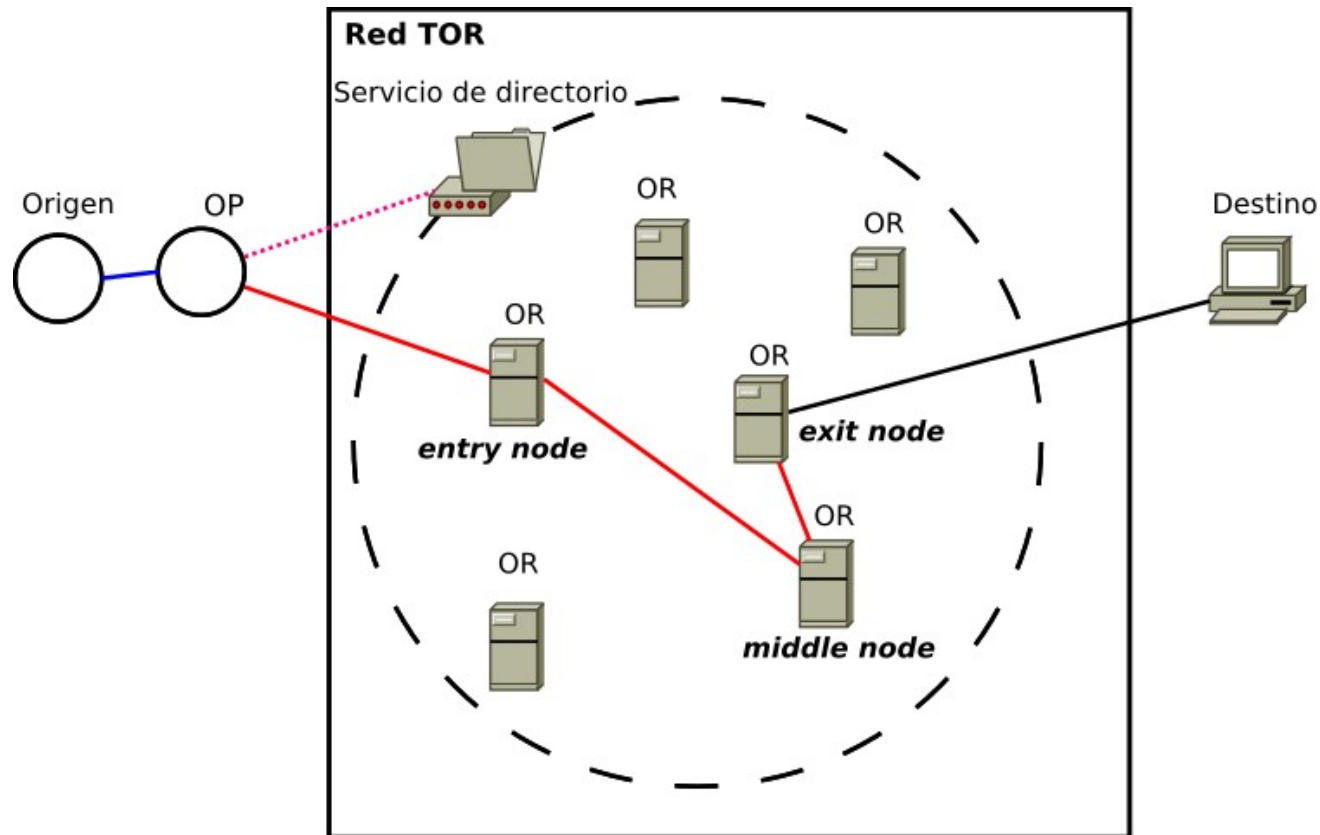
- circID: identificador del circuito
- CMD: comando → describe funcionalidad
 - C. de transmisión (*relay cell*)
 - C. de control (*control cell*)

circID	2 bytes
CMD	1 byte
Payload	509 bytes

Etapas de la comunicación

- Aplicación → SOCKS → Cliente (*Onion Proxy*) → Red *Onion Routers*
- Solicitud al servicio de directorio → información sobre la red.
- Elección aleatoria de nodos: *entry node*, *middle relay* y *exit node*.
- Generación del camino de forma sucesiva:
 - Generación de claves → Diffie-Hellman + RSA
- Encapsulamiento *onion* a través del camino → Exit node → Destino

Etapas de la comunicación



- Tráfico SOCKS de tráfico TCP
- Tráfico bidireccional de células sobre TLS
- Tráfico TCP
- Tráfico HTTP

Puntos de encuentro

Punto de contacto entre entidades de la red.

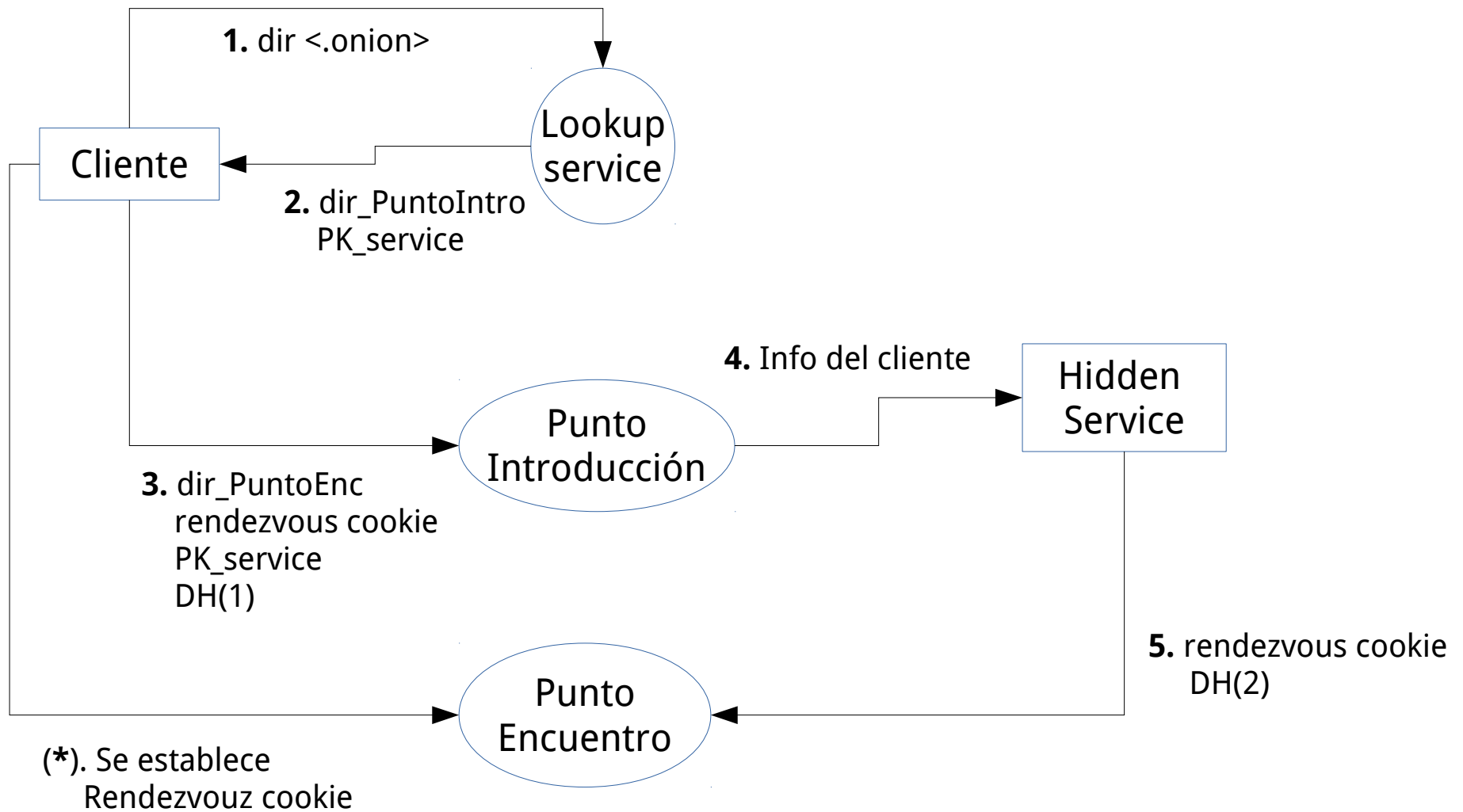
Cada extremo de la comunicación envía sus mensajes a un servidor intermediario.

→ El *Rendezvous Point* los redirecciona de forma segura para que establezcan una conexión canónica y se identifiquen.

Hidden services

- Proveedores de servicios sobre la red TOR
- **Creación de un hidden service:**
 - Generación de claves RSA (pública/privada)
 - Envío de clave pública a *introduction points*
- Dirección: “{hash}.onion” → 16 caracteres resultado de aplicar una función hash sobre la clave pública.

Conexión cliente → Hidden Service

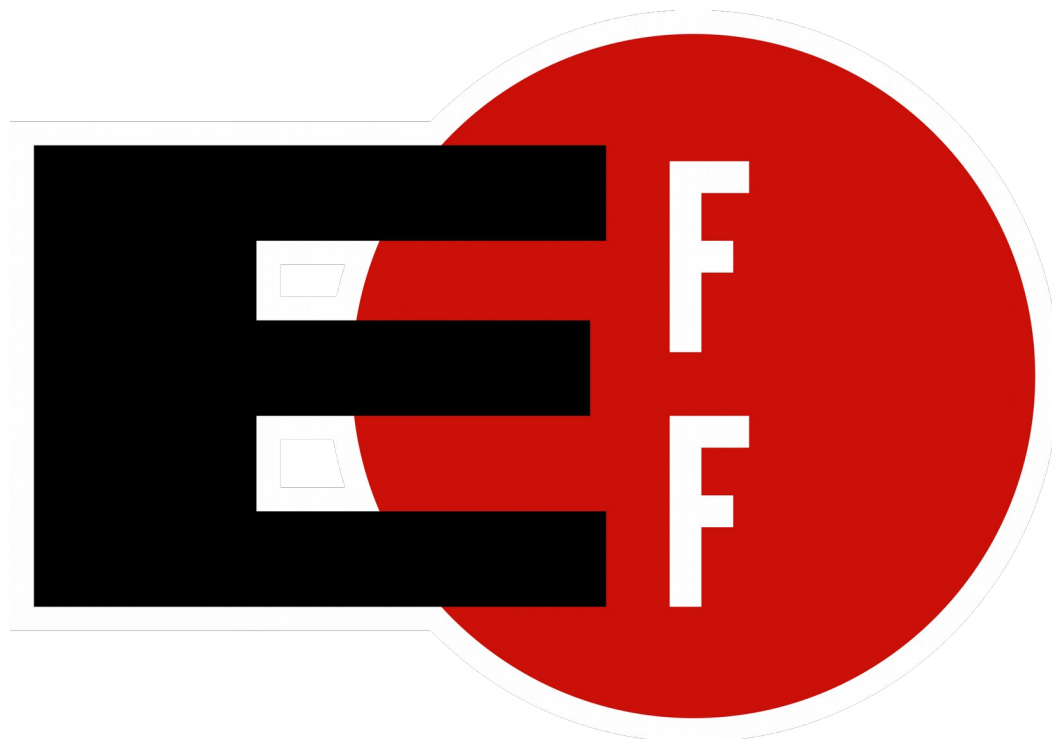


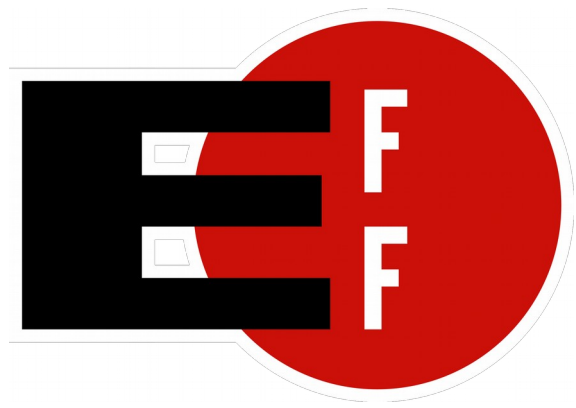
Weak points

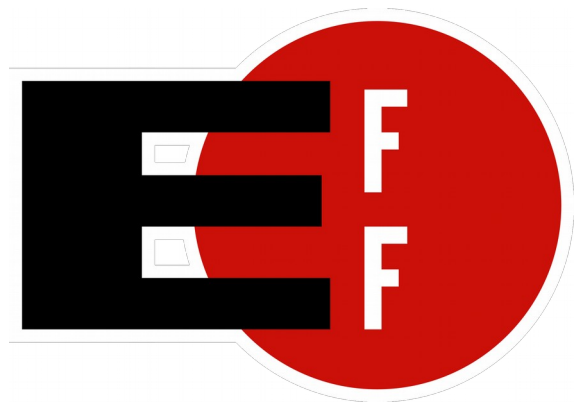
- Principalmente *Correlation attacks*
- Controlar un gran número de nodos hace posible:
 - Ataques por estimación de rutas e identificación de usuarios
 - Denegación de servicio
- Crackeo de claves de cifrado → “posible”.

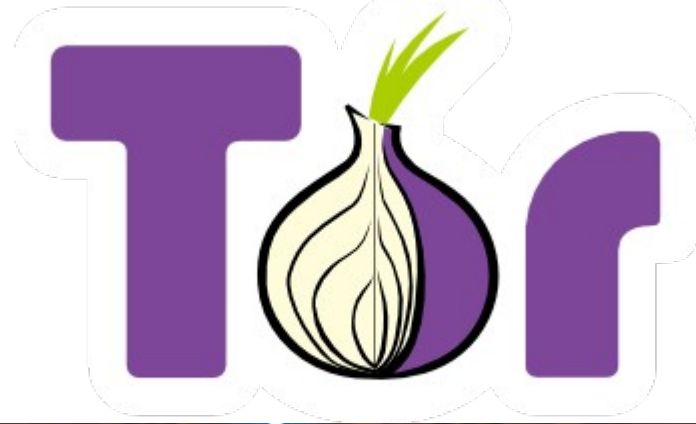
¿ Por qué existe TOR?

Garantizar la libertad de uso y de expresión de internet











Tor Browser



TAILS



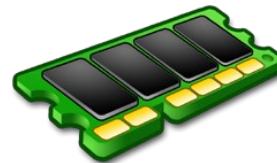
Orbot



**HTTPS
Everywhere**



Shadow



Tor-ramdisk

Darknet (Deep web)

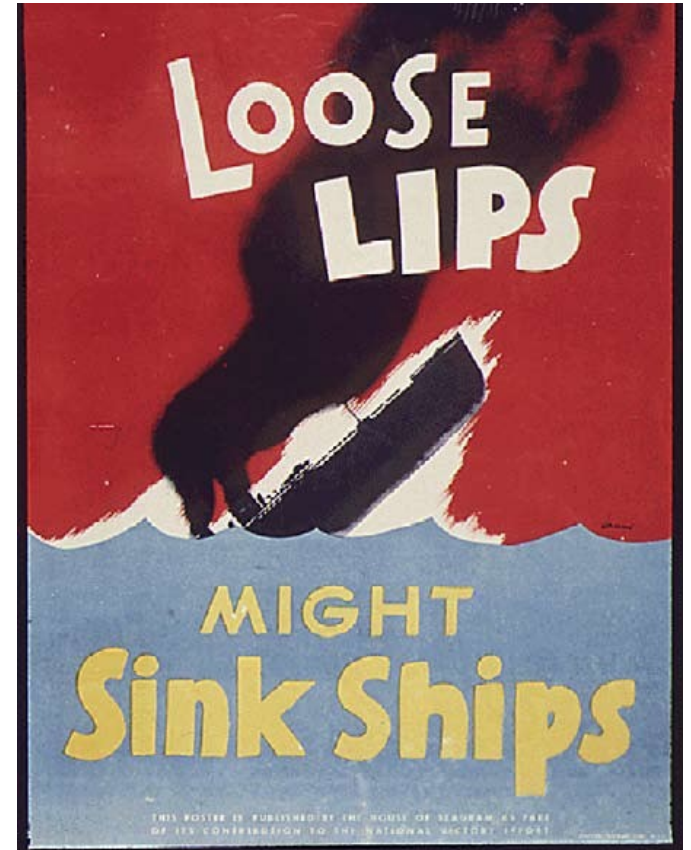
- Hidden services
- Difusión de información
- Bitcoin → Mixers
- Mercado negro
- Otras redes cifradas que ofuscan identidad
 - I2P
 - Freenet

“Seguridad” || “Privacidad”

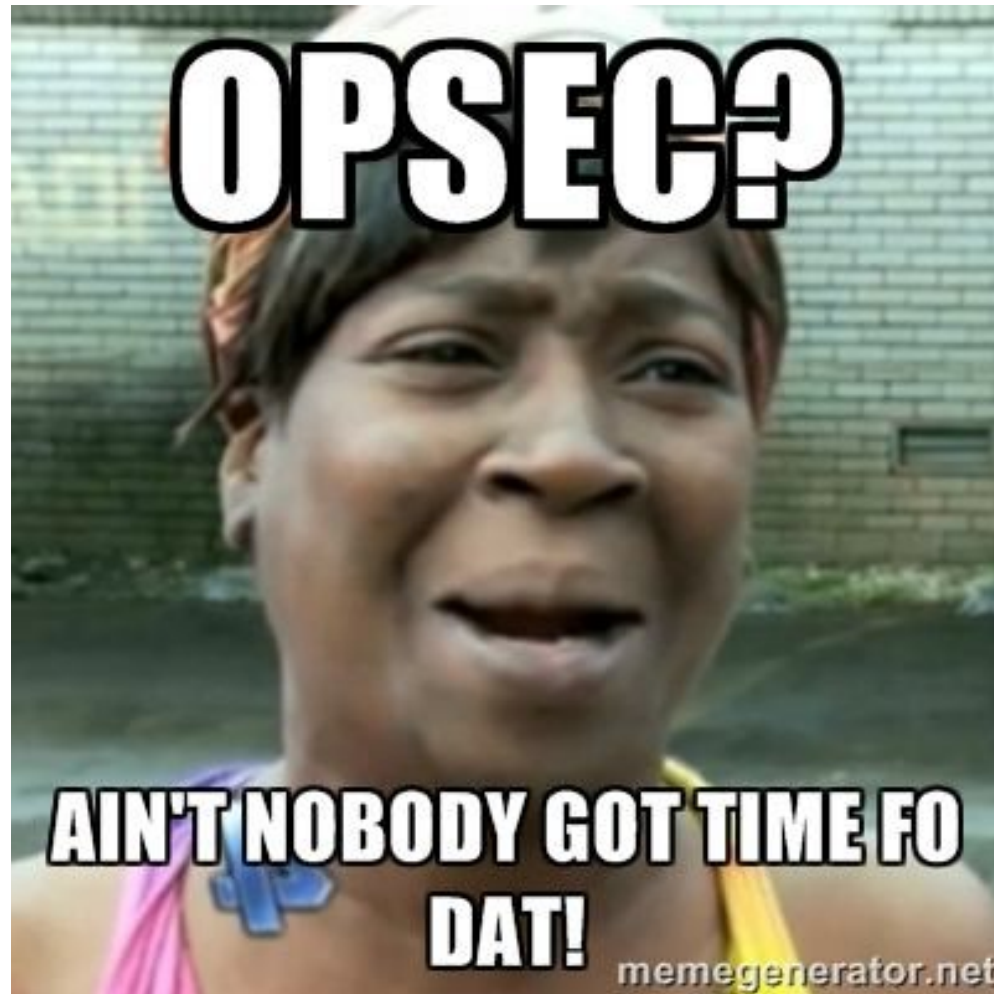


¿OPSEC? ¿Eso se come?

- TL; DR:
 - STFU
 - No dar a nadie poder sobre uno mismo
 - Evitar contaminación entre identidades
 - Paranoia proactiva



¿OPSEC? ¿Eso se come?



Bad OPSEC:



- Silk Road:

→ “Amazon/Ebay” de material ilegal

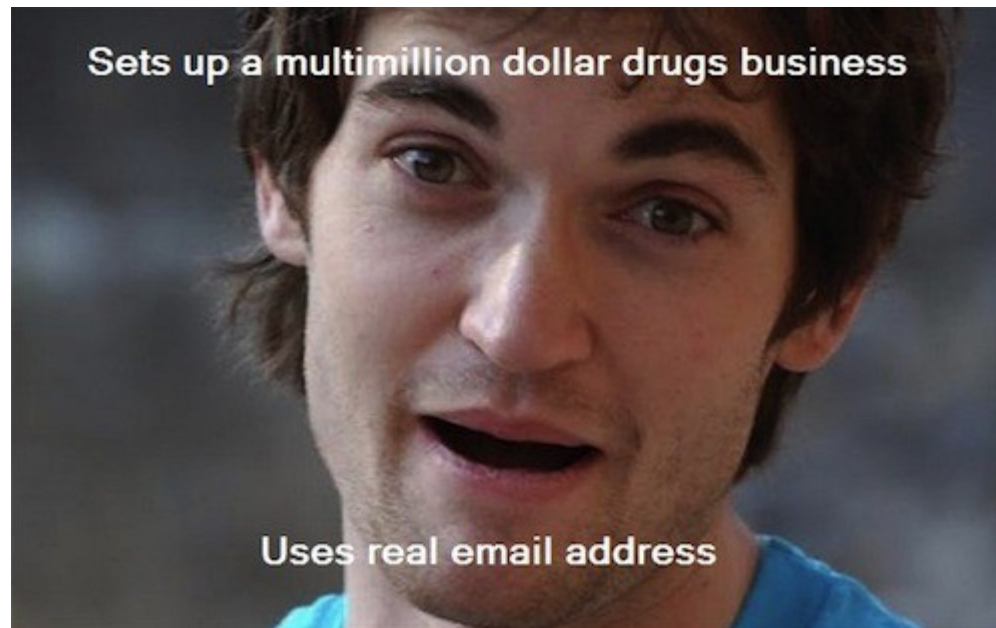
→ 1200 millones de \$ en transacciones

→ Figura de DPR

(*Dread Pirate Roberts*)

Bad OPSEC:

- Dread Pirate Roberts → Ross Ulbricht



Bad OPSEC:

- Lulz Sec



¿ Qué hacer?

- NO hacer el idiota por la darknet
- Promover la imagen e intención real detrás de TOR
- Mantener un OR en casa (?)

ó

- Donar a → www.torservers.net

Enlaces de interés y bibliografía

- [A message from George Orwell, to everyone on the Internet](#)
- [Safety on the TOR network](#)
- [How Tor Users Got Caught](#)
- [Real time tor metrics](#)
- [Real time TOR network's flow](#)
- [Traffic Correlation on Tor by Realistic Adversaries](#)
- [Deanonymizing Tor](#)
- [Raspberry Pi as a Tor Relay and Help Others Browser Anonymously](#)
- [Majority of Tor crypto keys could be broken by NSA](#)
- [NSA attains the Holy Grail of spying, decodes vast swaths of Internet traffic](#)
- [NSA Chief Stakes Out Pro-Encryption Position, in Contrast to FBI](#)
- [70% Of global Internet traffic goes through Northern Virginia](#)

Enlaces de interés y bibliografía

- [Design of a blocking-resistant anonymity system - Tor Project technical report](#)
- [Tor: The Second-Generation Onion Router](#)
- [Tor Protocol Specification](#)
- [Tor Rendezvous Specification](#)