cyber camp

CYBERSECURITY EVENT

2016

Manuel Guerra y Fco J.Rodriguez

GOBIERNO DE ESPAÑA | MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

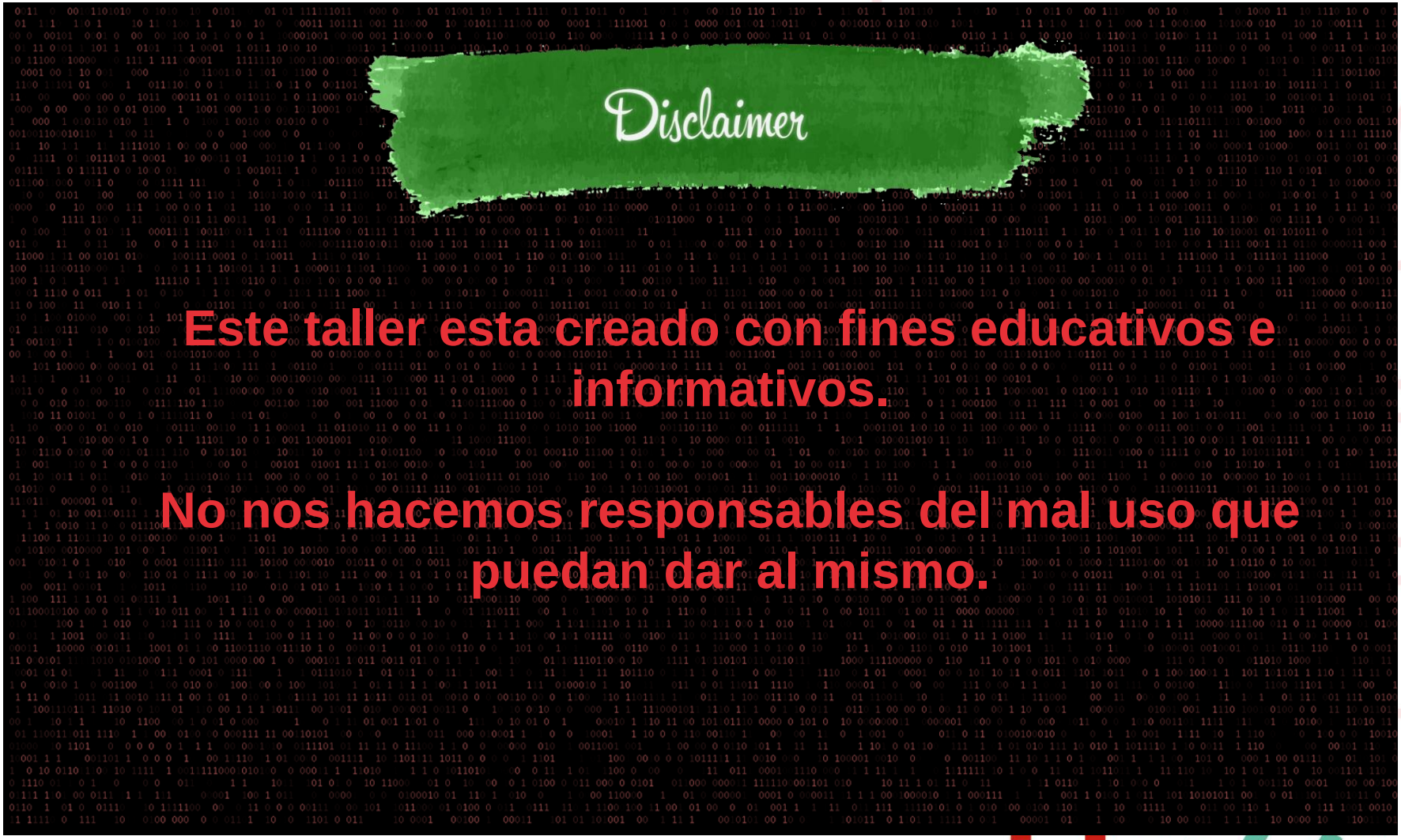
incibe_ TRABAJANDO POR LA CONFIANZA DIGITAL

CyberCamp.es

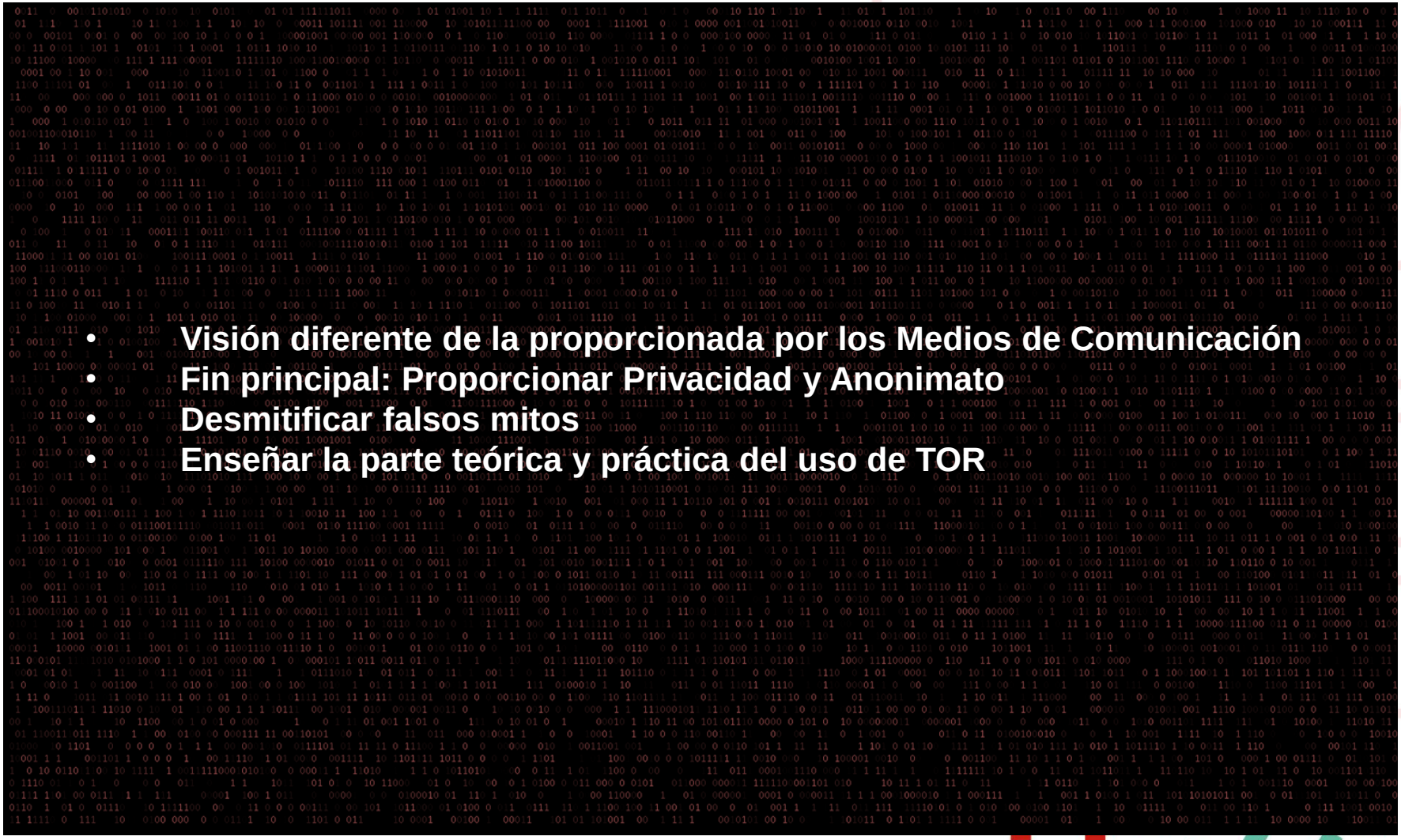
Ponentes


incibe_
cyber camp
CYBERSECURITY EVENT
2016
Francisco J. Rodríguez
Instituto Nacional de Ciberseguridad de España
Manuel Guerra
Unidad de Investigación Tecnológica de la Policía Nacional

Disclaimer

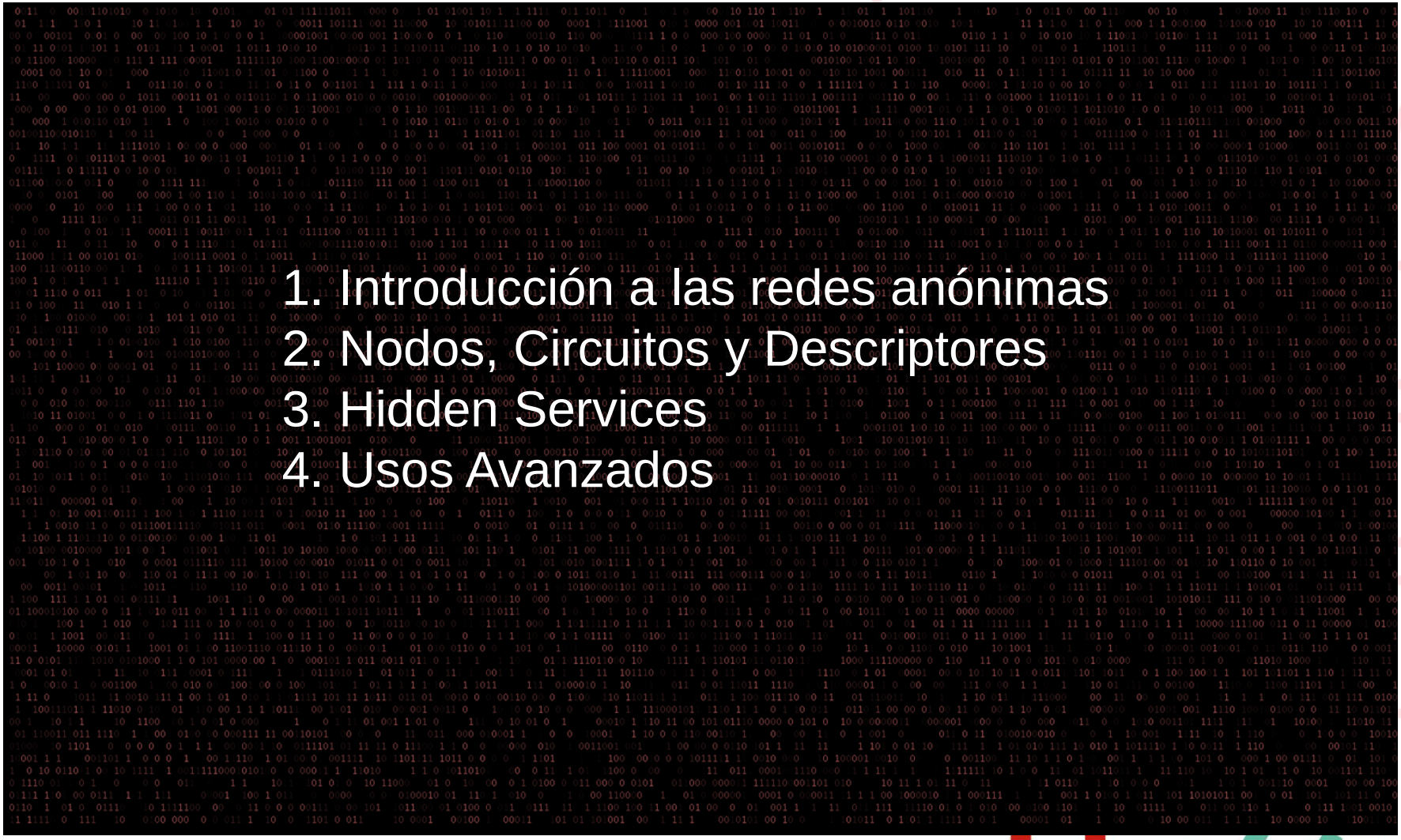

Disclaimer
Este taller esta creado con fines educativos e informativos.
No nos hacemos responsables del mal uso que puedan dar al mismo.

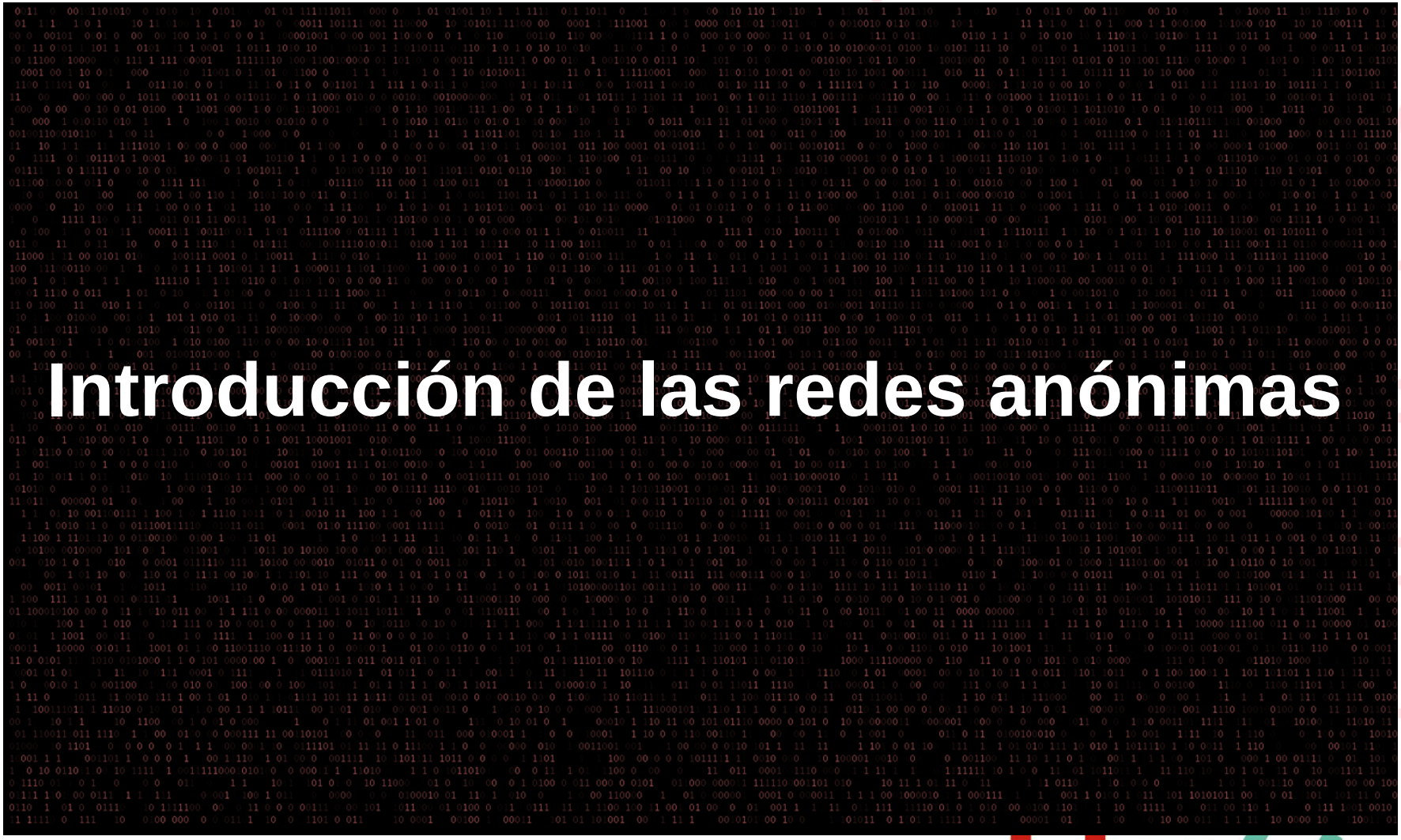
Objetivo del Taller



- Visión diferente de la proporcionada por los Medios de Comunicación
- Fin principal: Proporcionar Privacidad y Anonimato
- Desmitificar falsos mitos
- Enseñar la parte teórica y práctica del uso de TOR

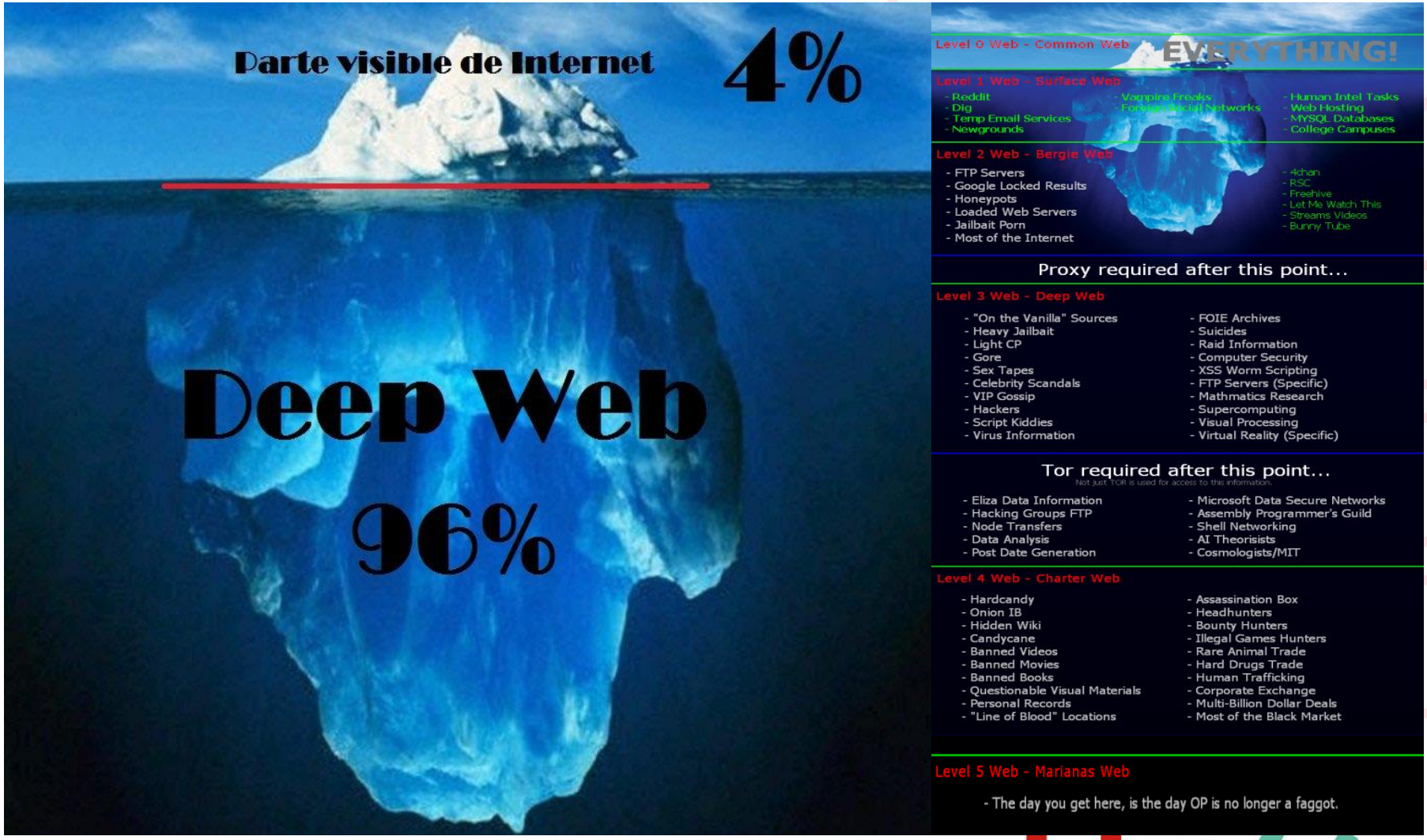
Estructura del Taller





Introducción de las redes anónimas

Todos conocemos esta imagen

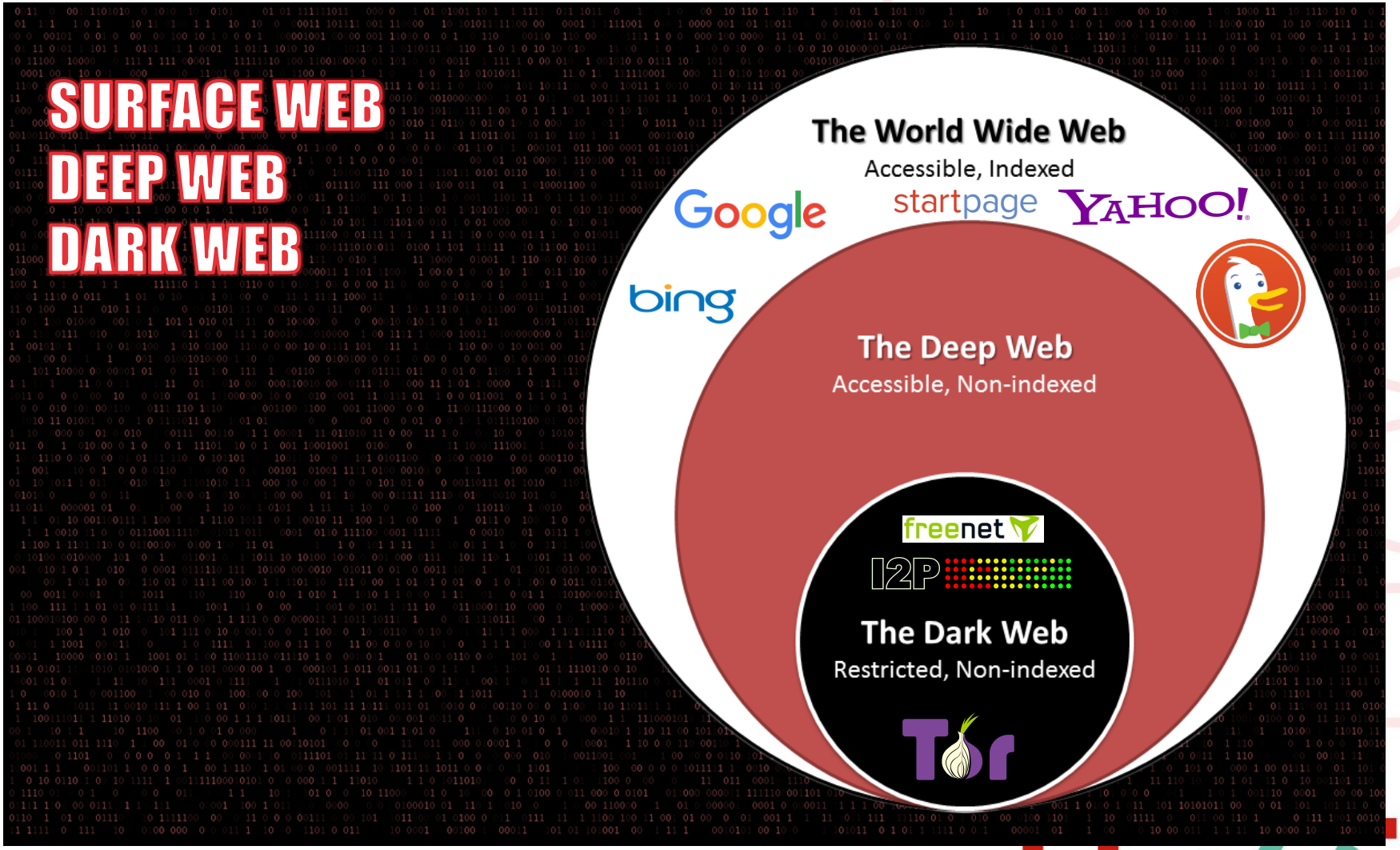


Empieza la cuenta atras


BÓRRALO DE
TU MENTE

Desaprender.

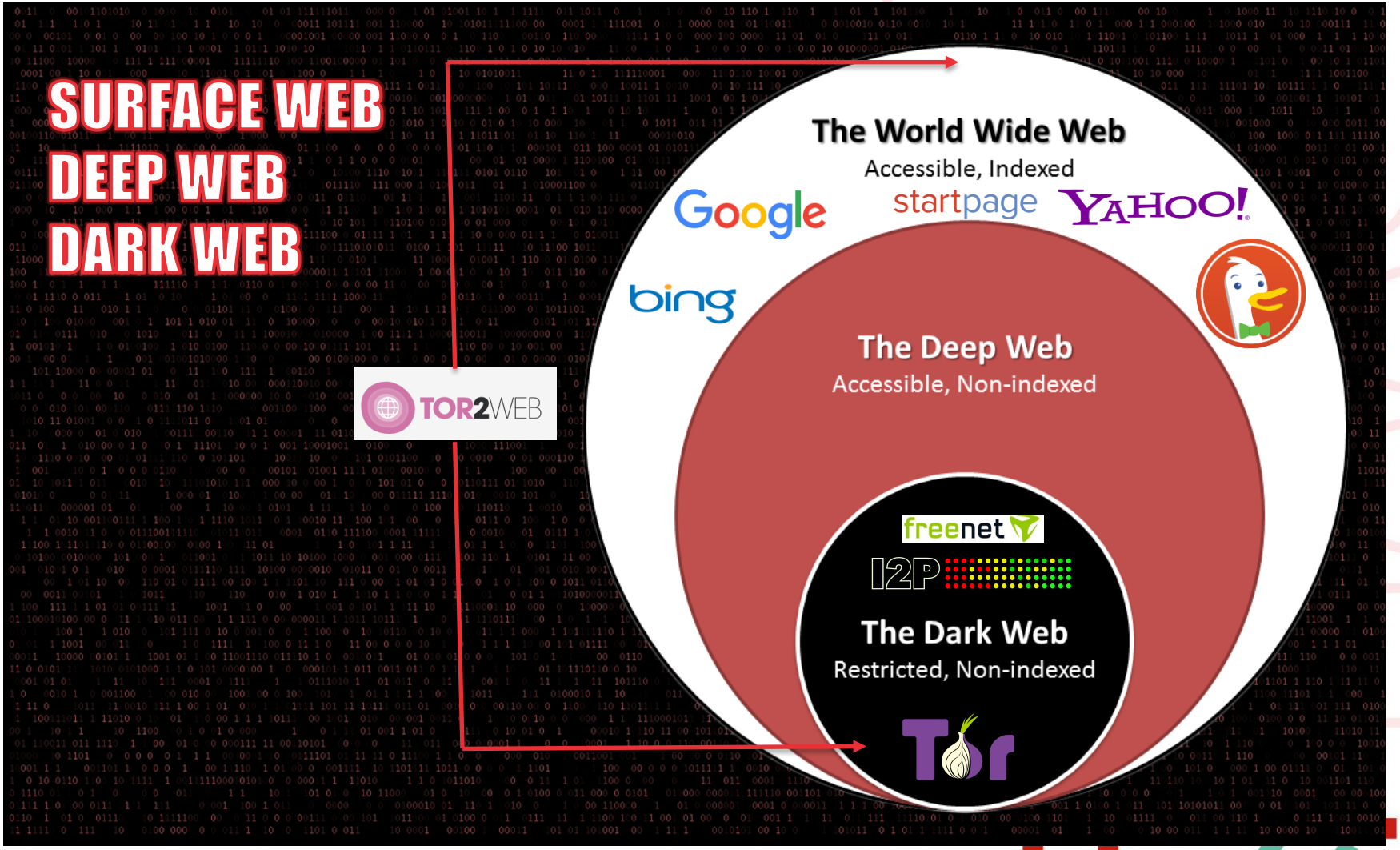
Surface / Deep / Dark Web



Deep Web

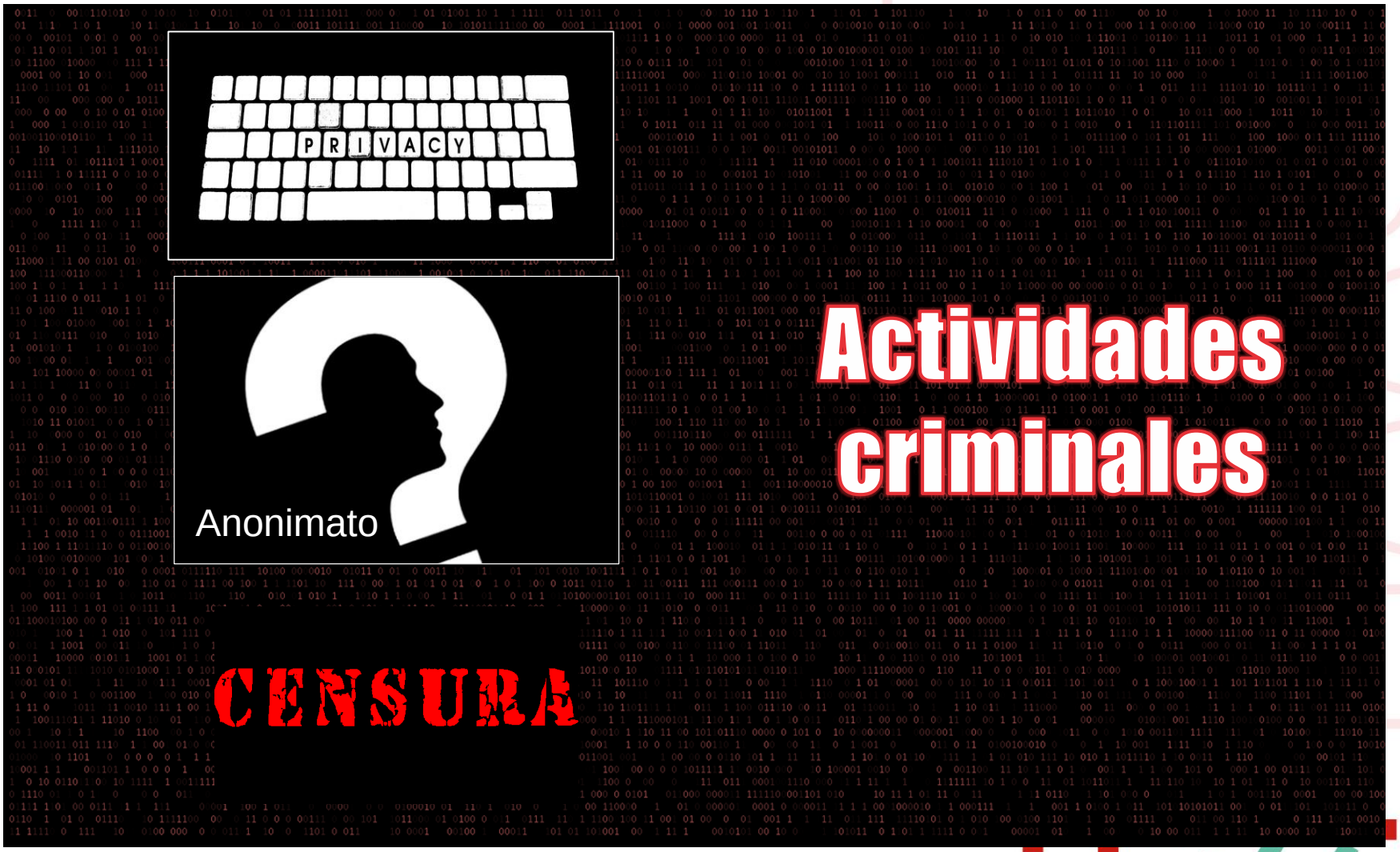
- Páginas web Dinámicas
- Páginas bloqueadas (Capcha, pragma no-cache, Robots.txt)
- Sitios no linkados o enlazados
- Sitios Privados (Acceso mediante usuario y contraseña)
- Páginas que el buscador decidió no indexar
- Documentos con formatos no indexables
- Indexados, pero no accesibles con criterios de búsqueda convencionales
- Sitios con nombres de dominio no controlados por IANA (Emercoin, Namecoin, name.space …)

Proxy Web Tor2Web

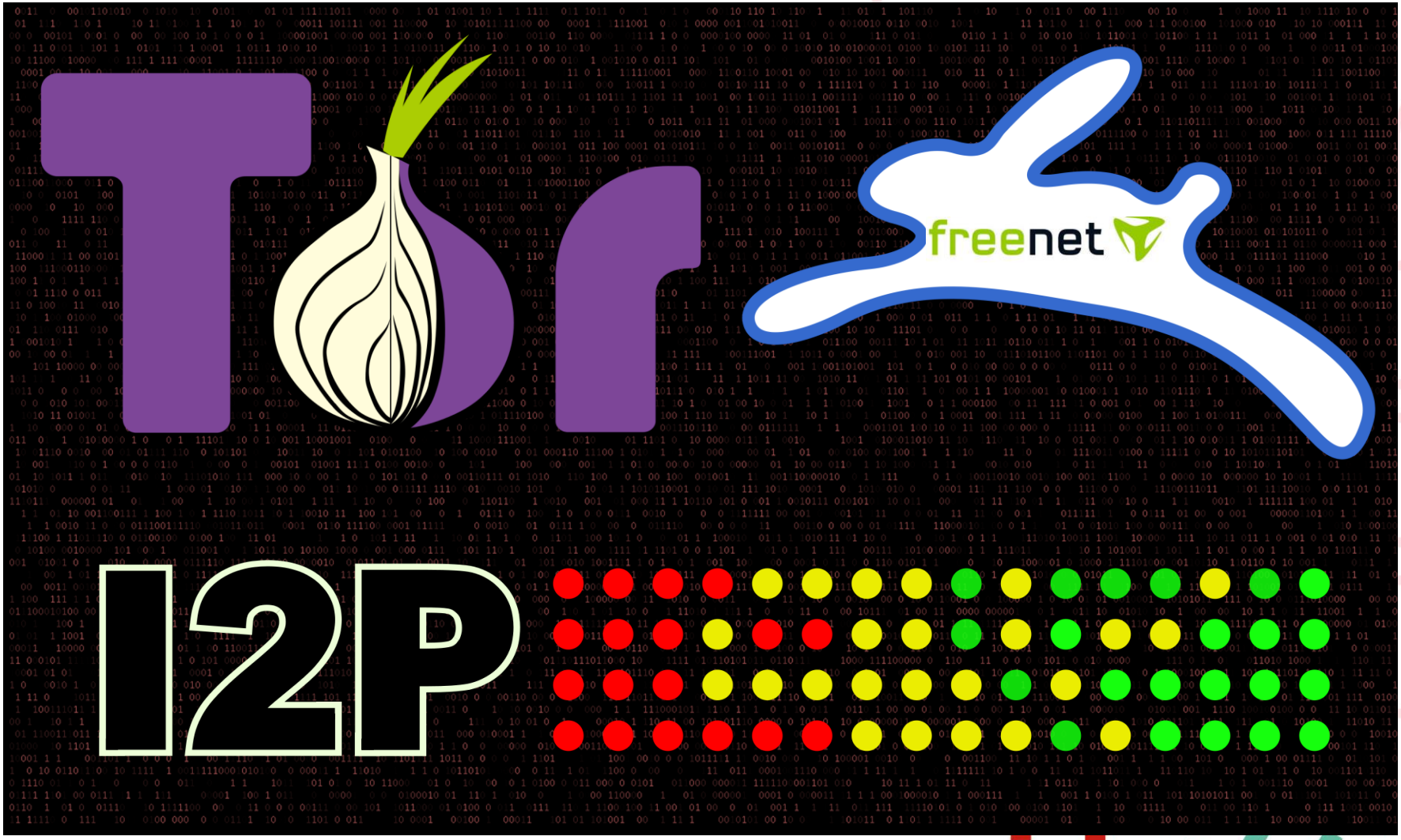


Desmintiendo el Iceberg

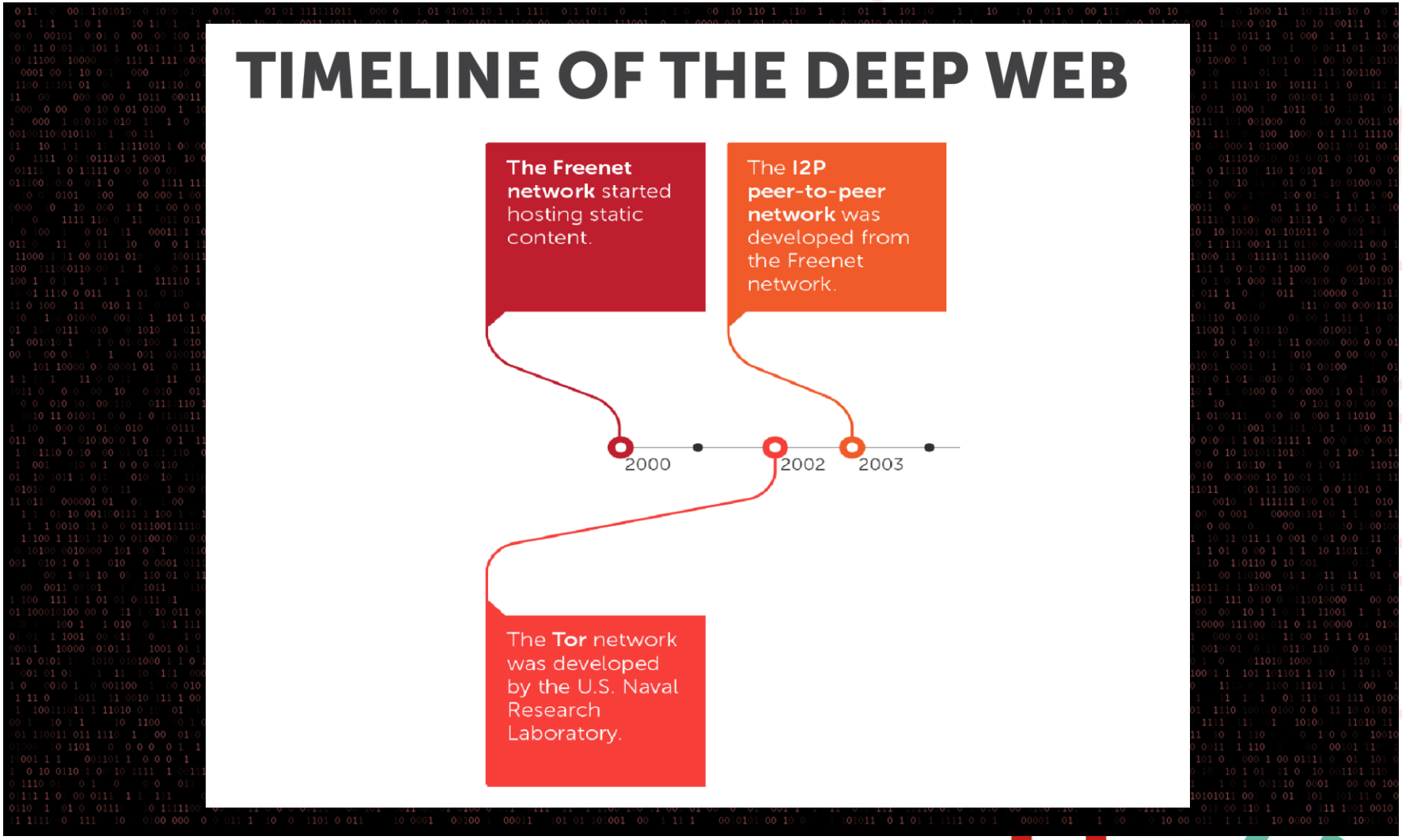
Las 2 caras de la moneda: usos de TOR



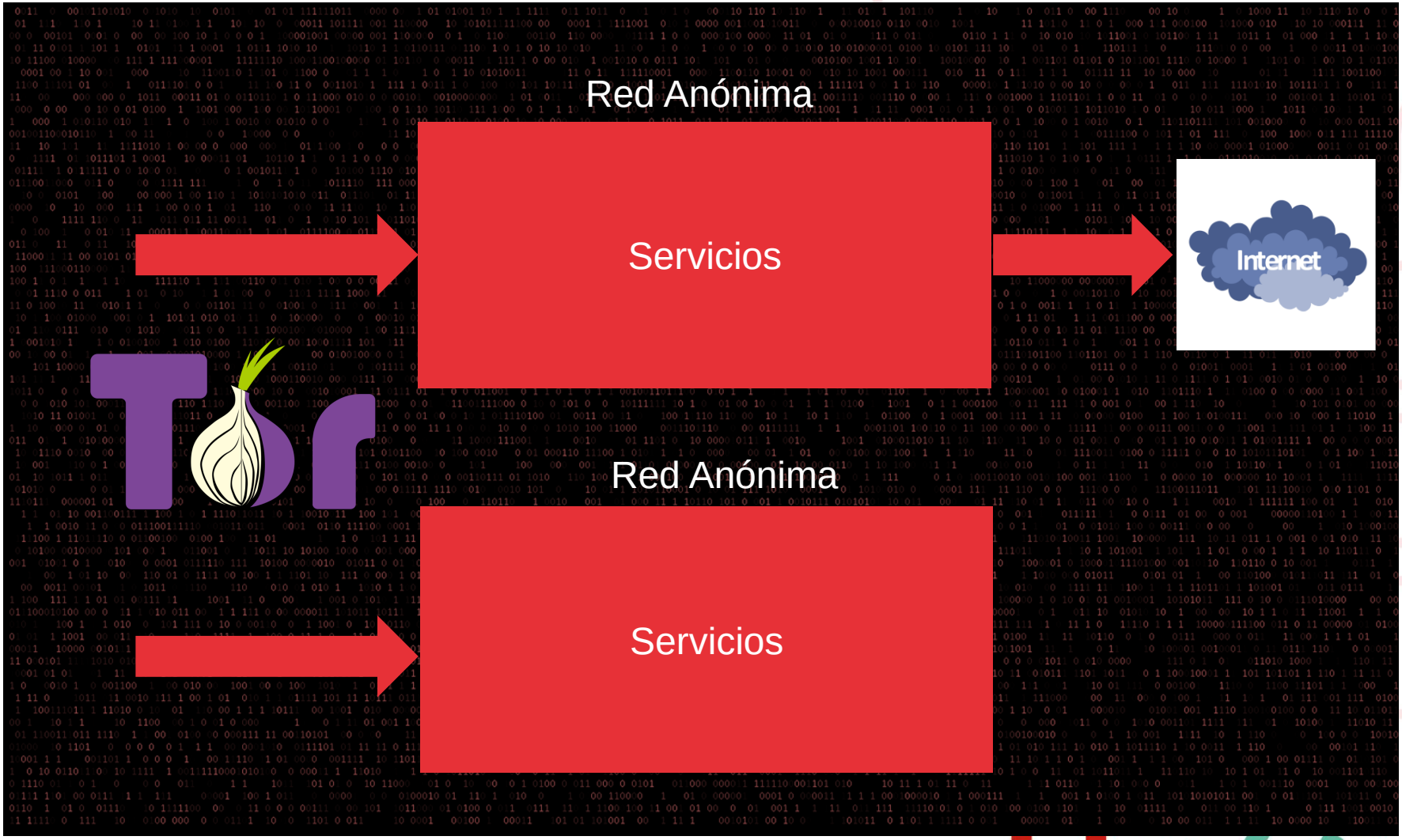
Redes anónimas más conocidas



Cronología redes anónimas



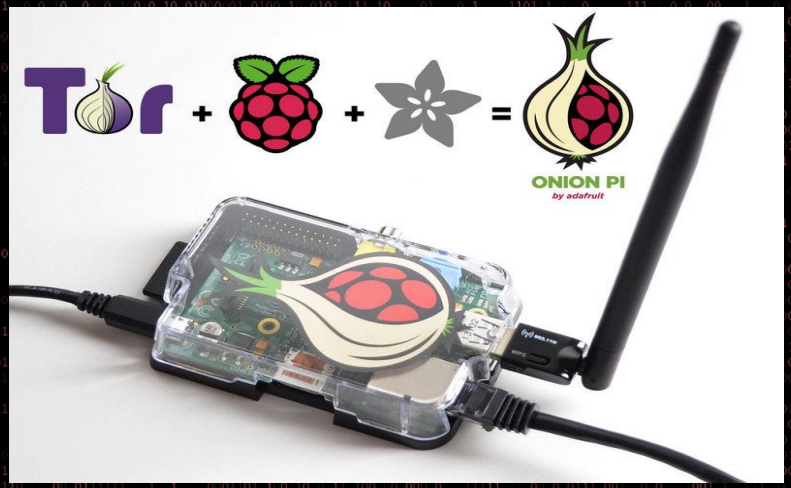
Outproxy/Inproxy



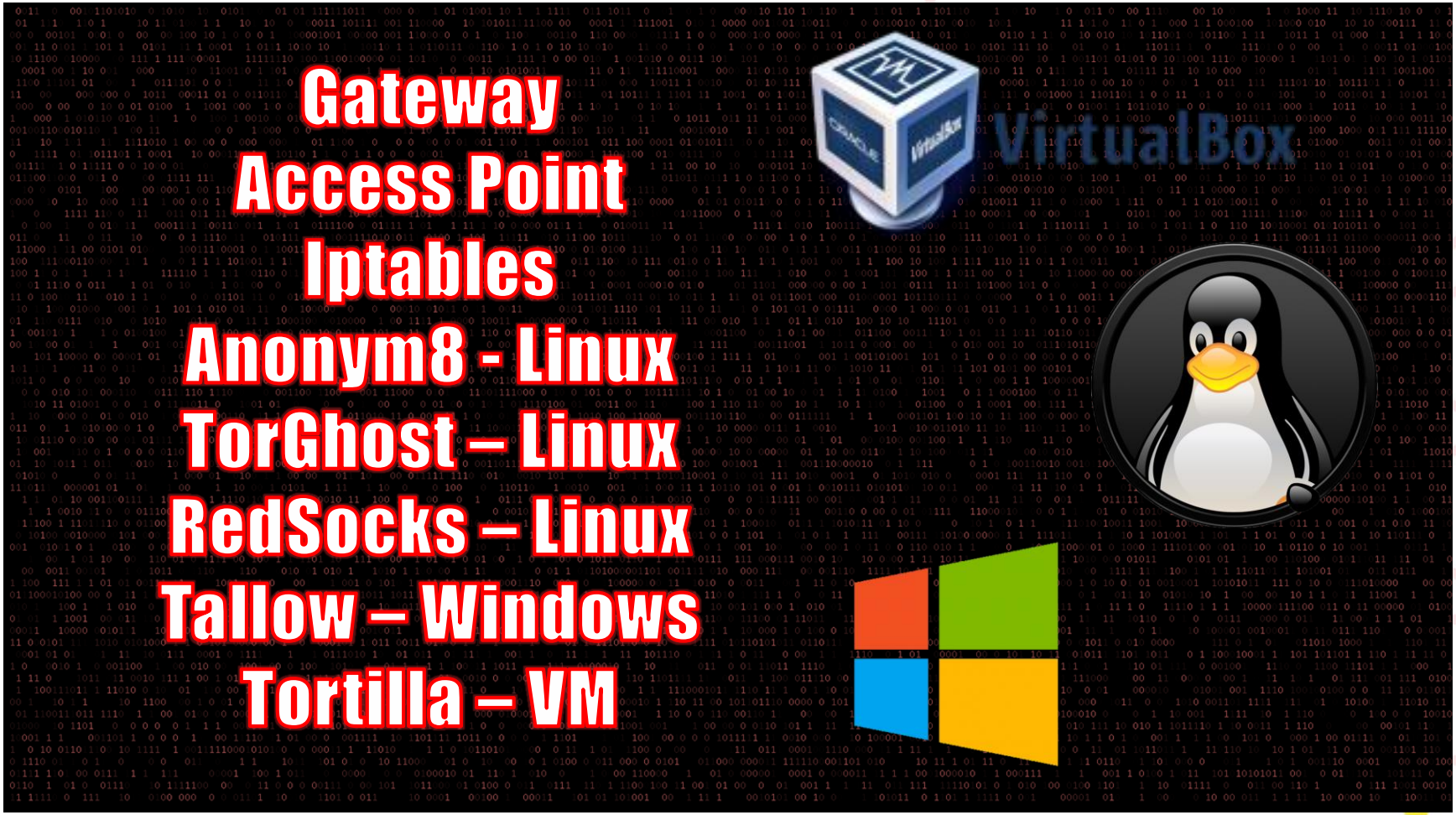
Otras redes y herramientas

Distribuciones Linux

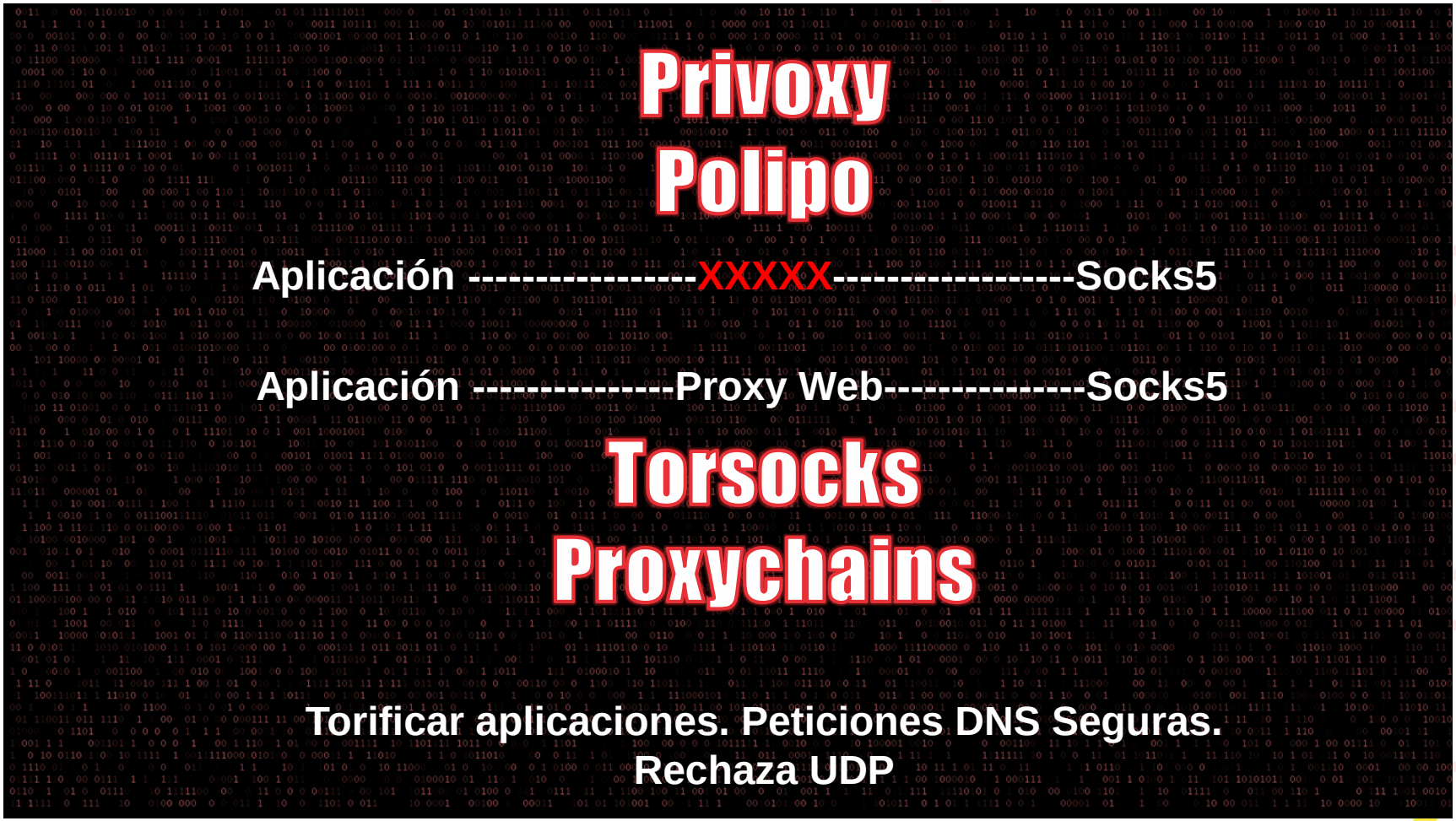
Routers con VPN -TOR / OnionPi / Tor Phone



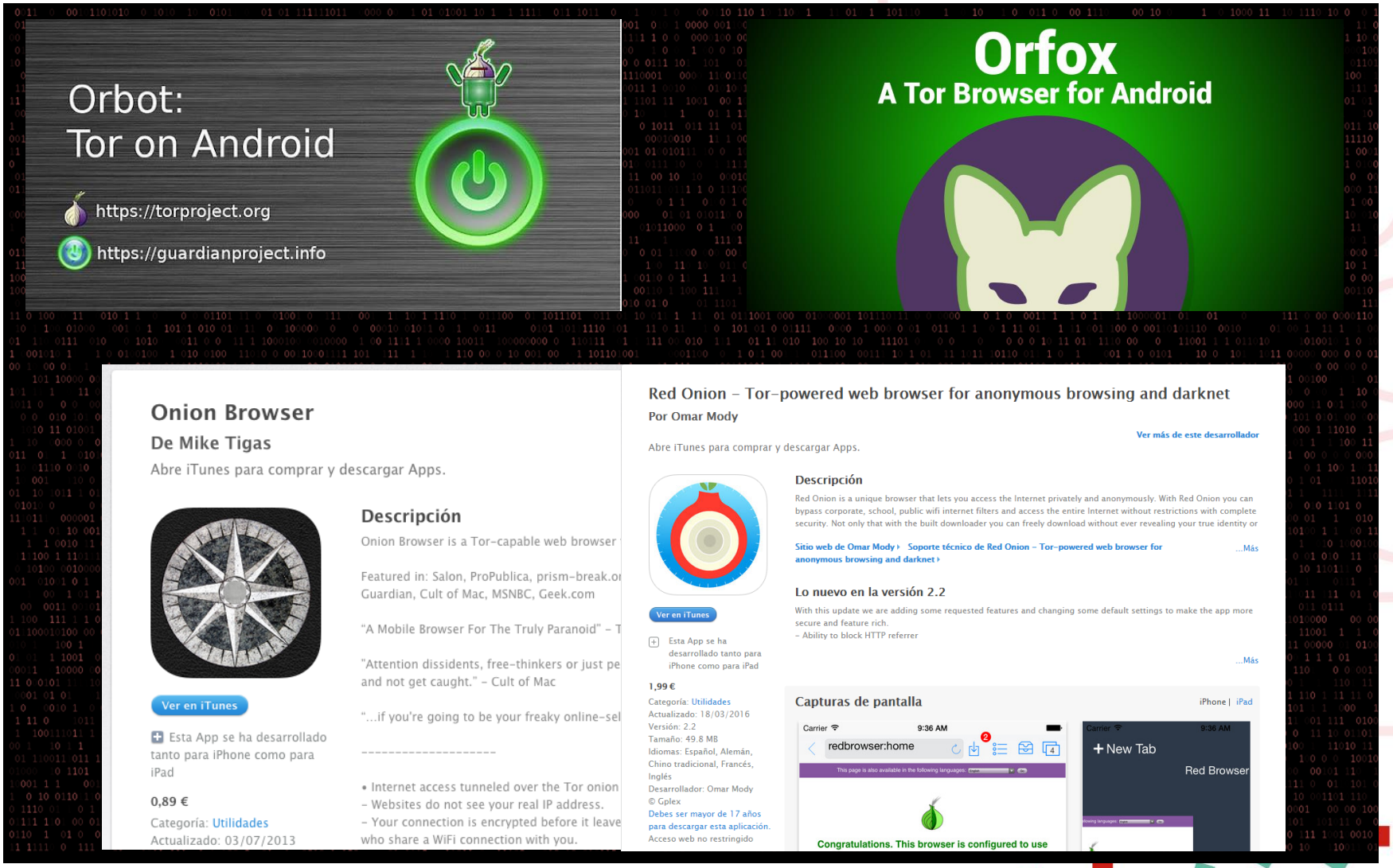
Enrutar tráfico por TOR



Aplicaciones por Tor



TOR en IOS y Android



Origen de TOR

Proyecto Onion Routing (Laboratorio de investigación naval de EEUU)

Patrocinado por la EFF (Electronic Frontier Fountation) hasta nov 2005

Tor project (Sin animo de lucro para la investigación y educación)

Tor (The Onion Router) ha conseguido que la ICANN le **conceda el TLD .onion**, haciéndose así dueña del dominio .onion. Onion es cebolla en inglés, y esta palabra hace mención a la forma de enrutar que emplea la red Tor, denominado enrutado cebolla.

[a-z 2-7] x 16.onion

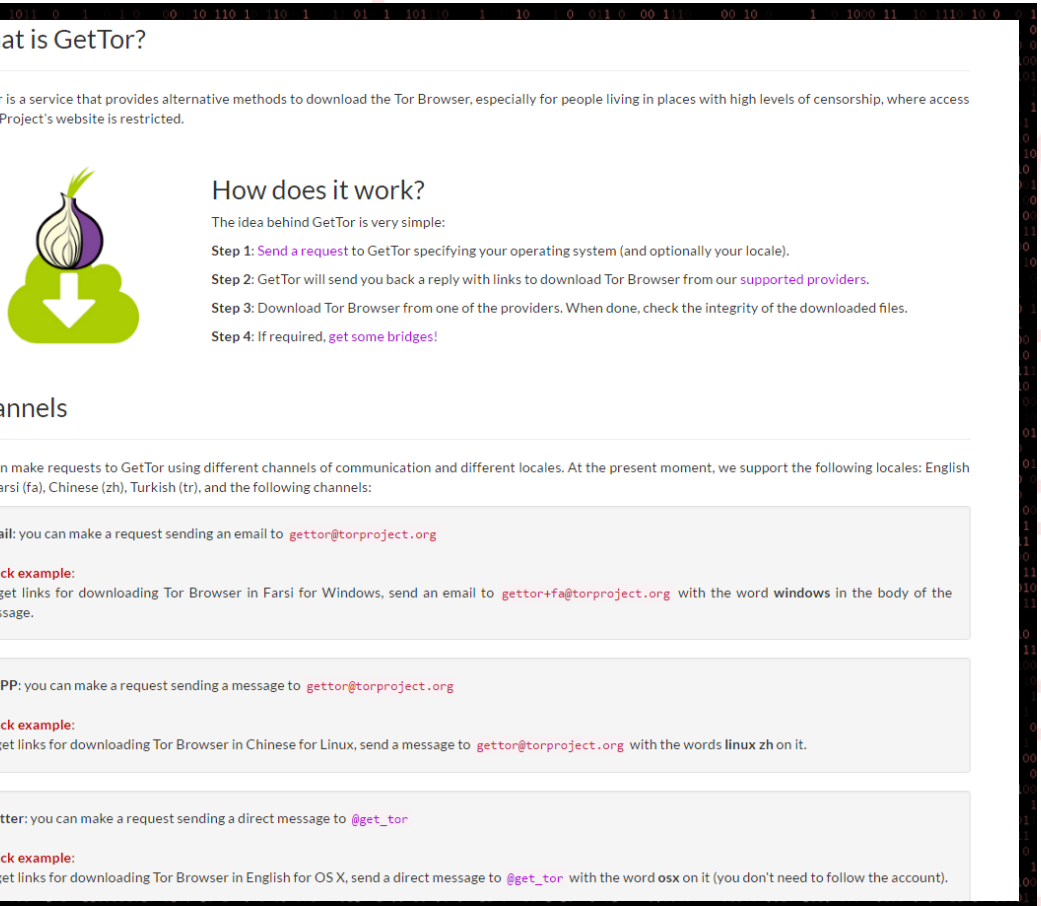
dfhe345cnvkf8756.onion

Obtener TOR. Alternativa GetTOR.Otros

Apt-get

Yum

Sources



What is GetTor?

GetTor is a service that provides alternative methods to download the Tor Browser, especially for people living in places with high levels of censorship, where access to Tor Project's website is restricted.

How does it work?

The idea behind GetTor is very simple:

Step 1: Send a request to GetTor specifying your operating system (and optionally your locale).

Step 2: GetTor will send you back a reply with links to download Tor Browser from our supported providers.

Step 3: Download Tor Browser from one of the providers. When done, check the integrity of the downloaded files.

Step 4: If required, get some bridges!

Channels

You can make requests to GetTor using different channels of communication and different locales. At the present moment, we support the following locales: English (en), Farsi (fa), Chinese (zh), Turkish (tr), and the following channels:

Email: you can make a request sending an email to `gettor@torproject.org`

Quick example:
To get links for downloading Tor Browser in Farsi for Windows, send an email to `gettor+fa@torproject.org` with the word **windows** in the body of the message.

XMPP: you can make a request sending a message to `gettor@torproject.org`

Quick example:
To get links for downloading Tor Browser in Chinese for Linux, send a message to `gettor@torproject.org` with the words **linux zh** on it.

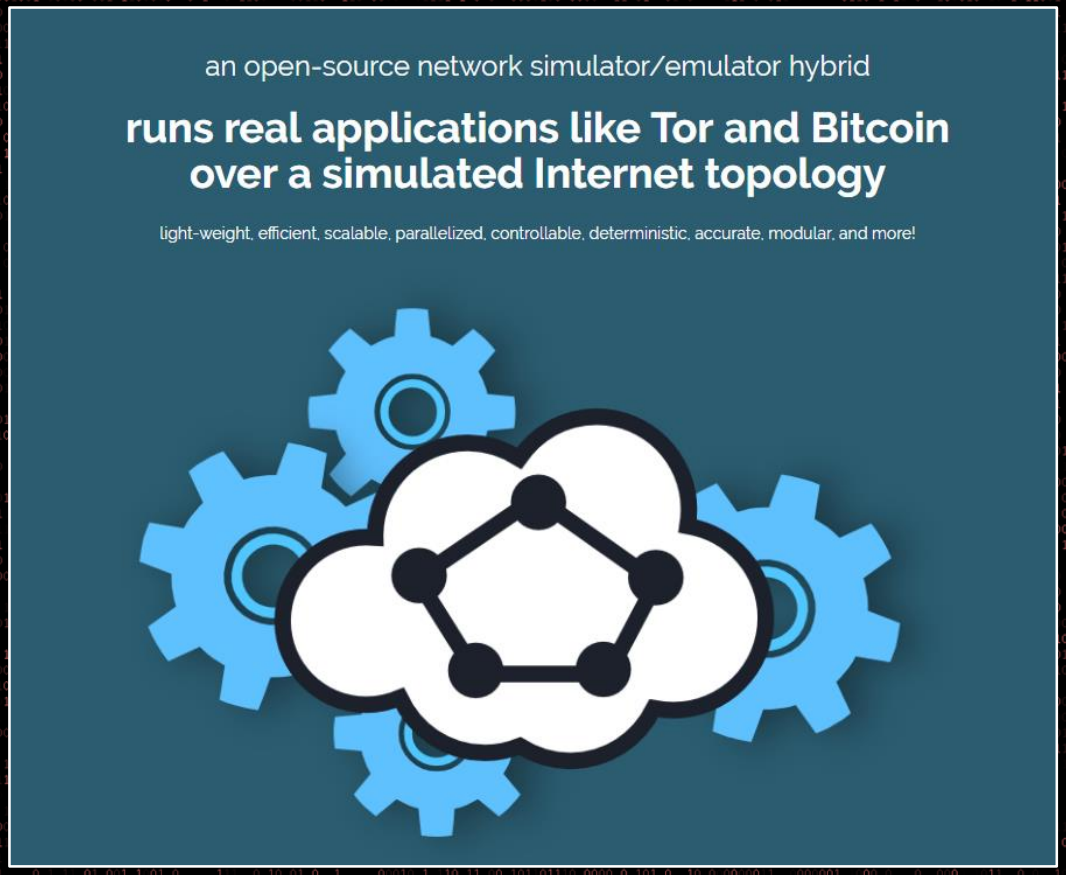
Twitter: you can make a request sending a direct message to `@get_tor`

Quick example:
To get links for downloading Tor Browser in English for OS X, send a direct message to `@get_tor` with the word **osx** on it (you don't need to follow the account).

https://gettor.torproject.org/

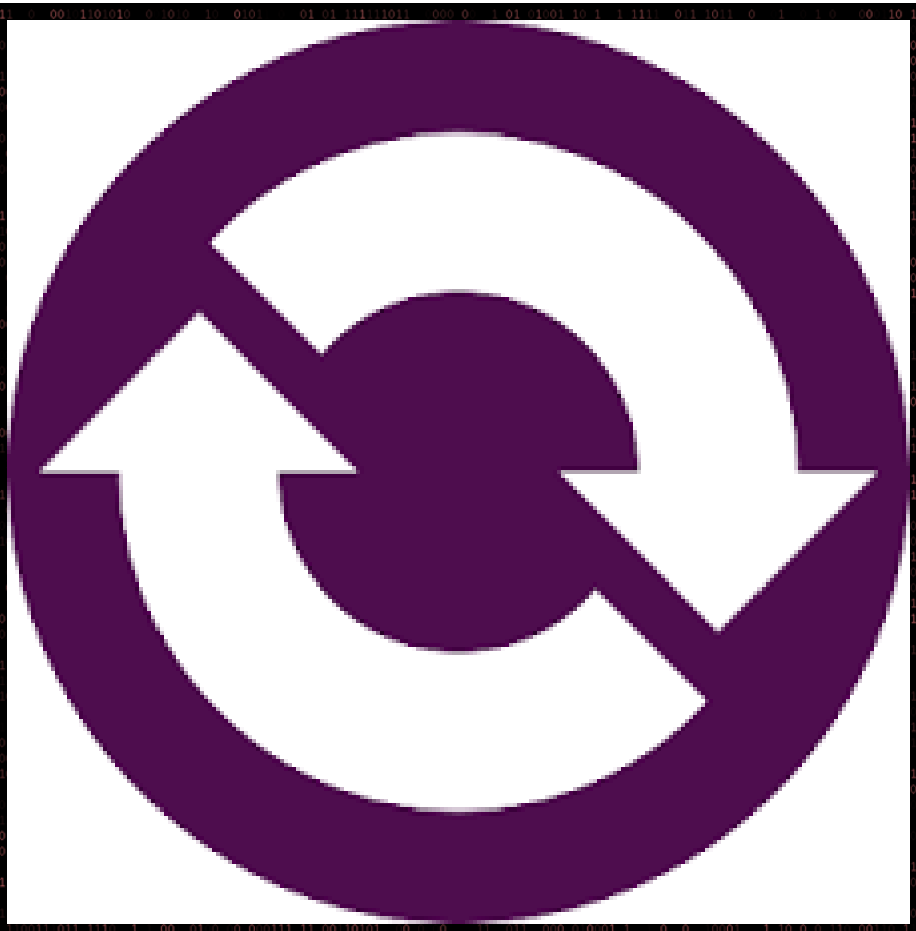
Guía Oficial TOR

Emulando TOR: Shadow y Chutney



https://gitweb.torproject.org/chutney.git

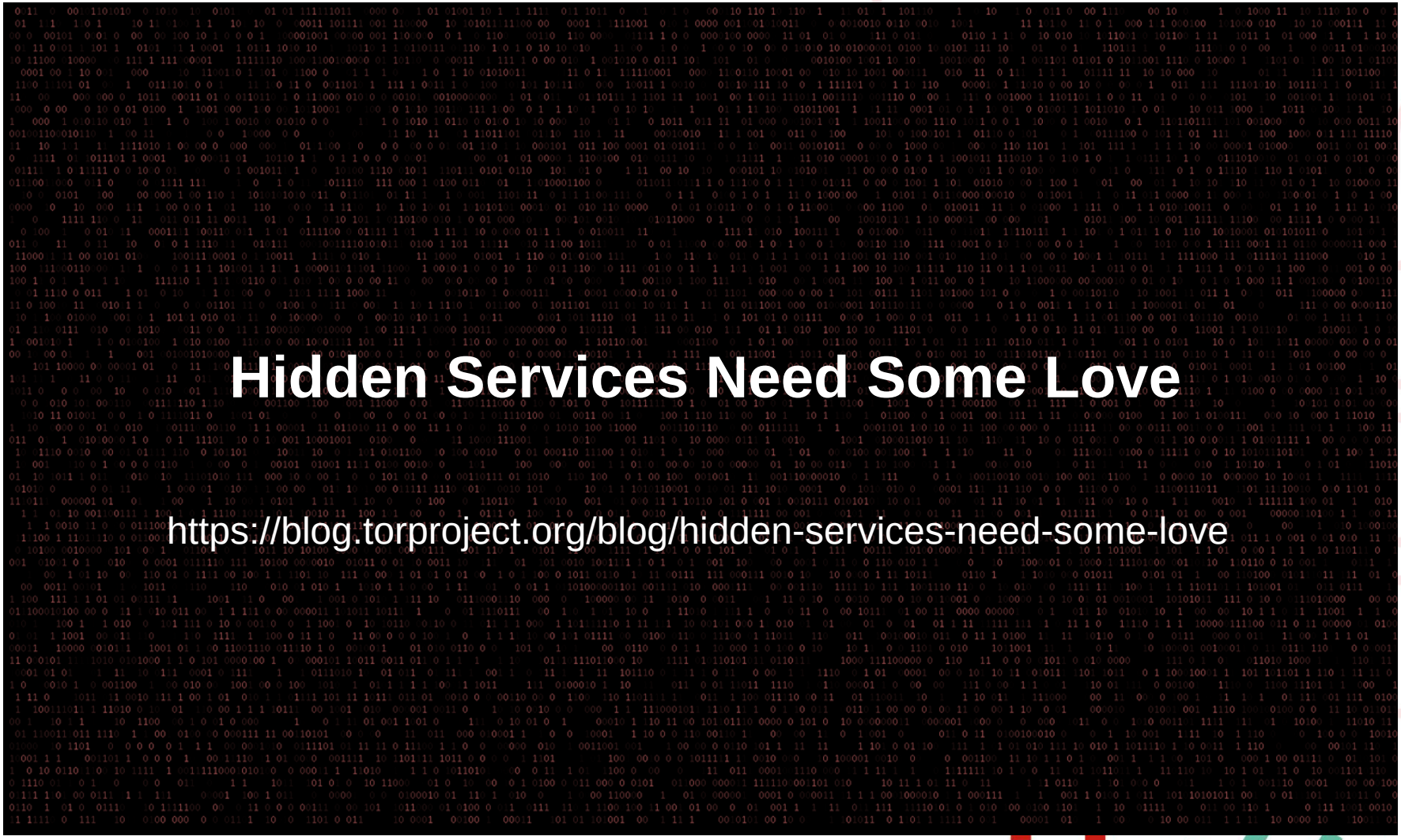
Sigaint / OnionShare / Tor Messenger



https://onionshare.org/

http://sigaintevyh2rzvw.onion/
http://torbox3uiot6wchz.onion/

Vulnerabilidades en TOR



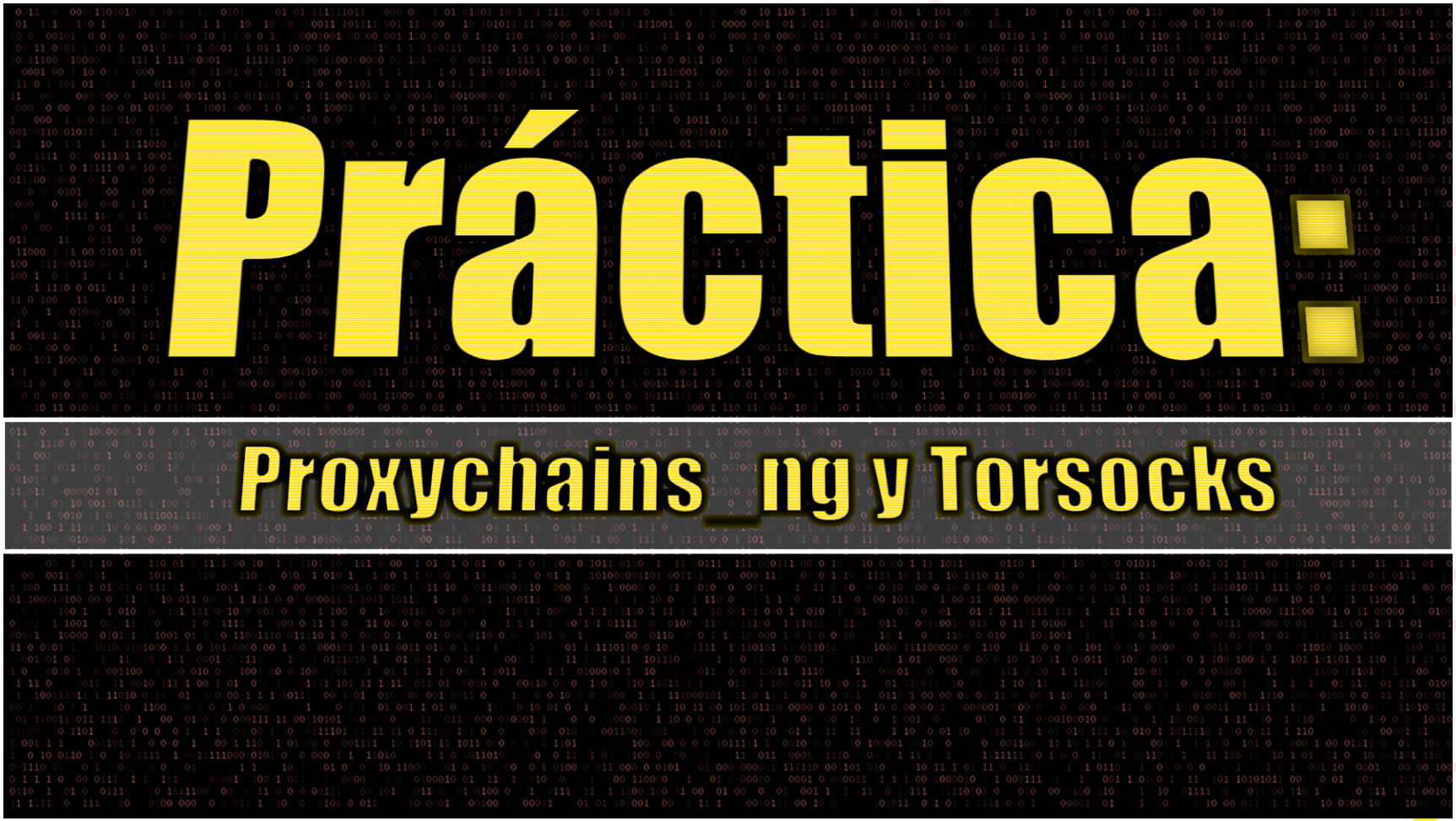
Práctica


Práctica:
Instalación de Tor Browser.
Instalación Instancia TOR


Práctica:
Configuración Red TOR y Nivel de Seguridad en Tor Browser

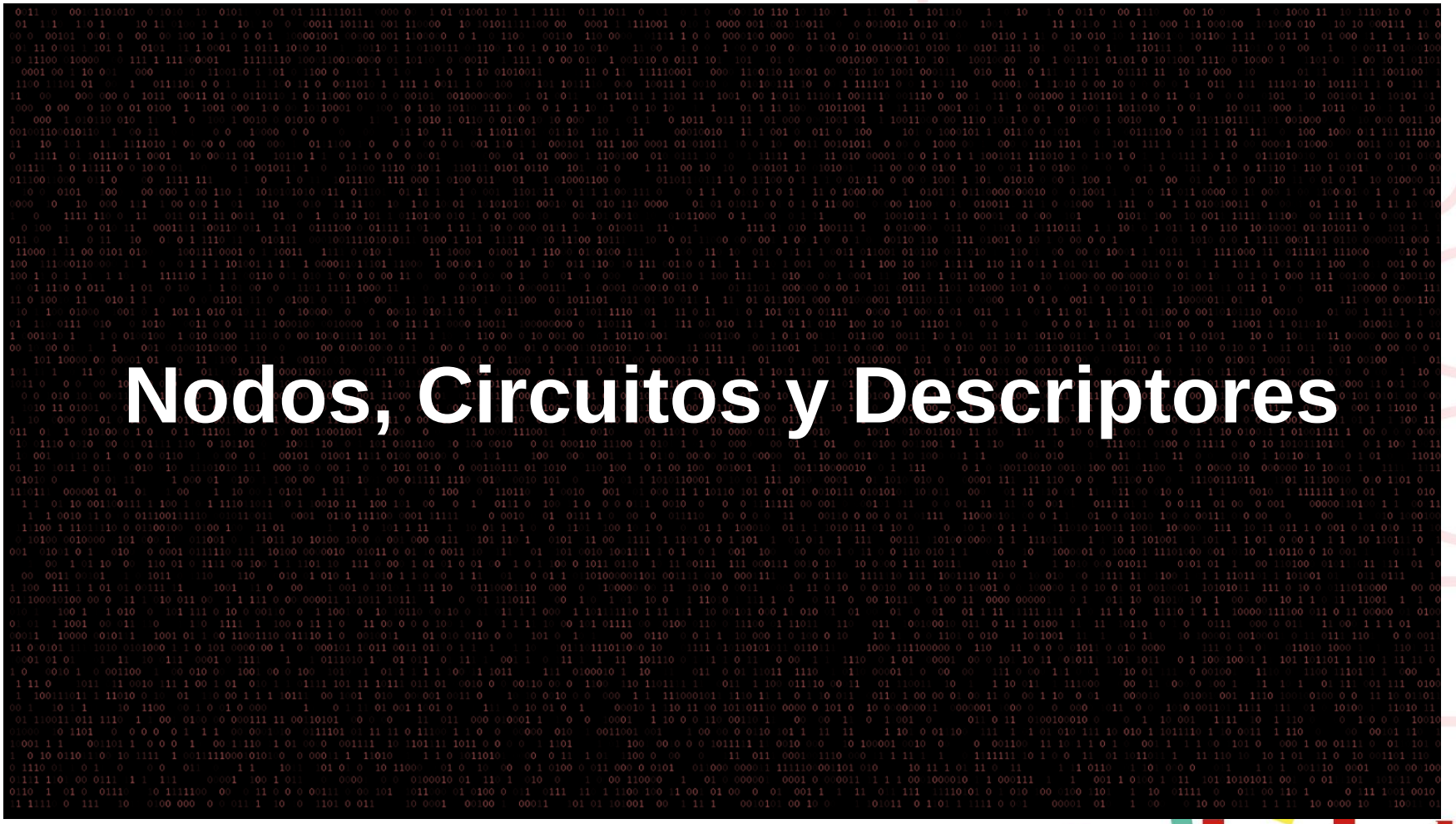
Práctica

Práctica



Práctica

Práctica



Nodos, Circuitos y Descriptores

Autoridades de directorio

Tor es una red centralizada y gestionada por un conjunto de servidores confiables.

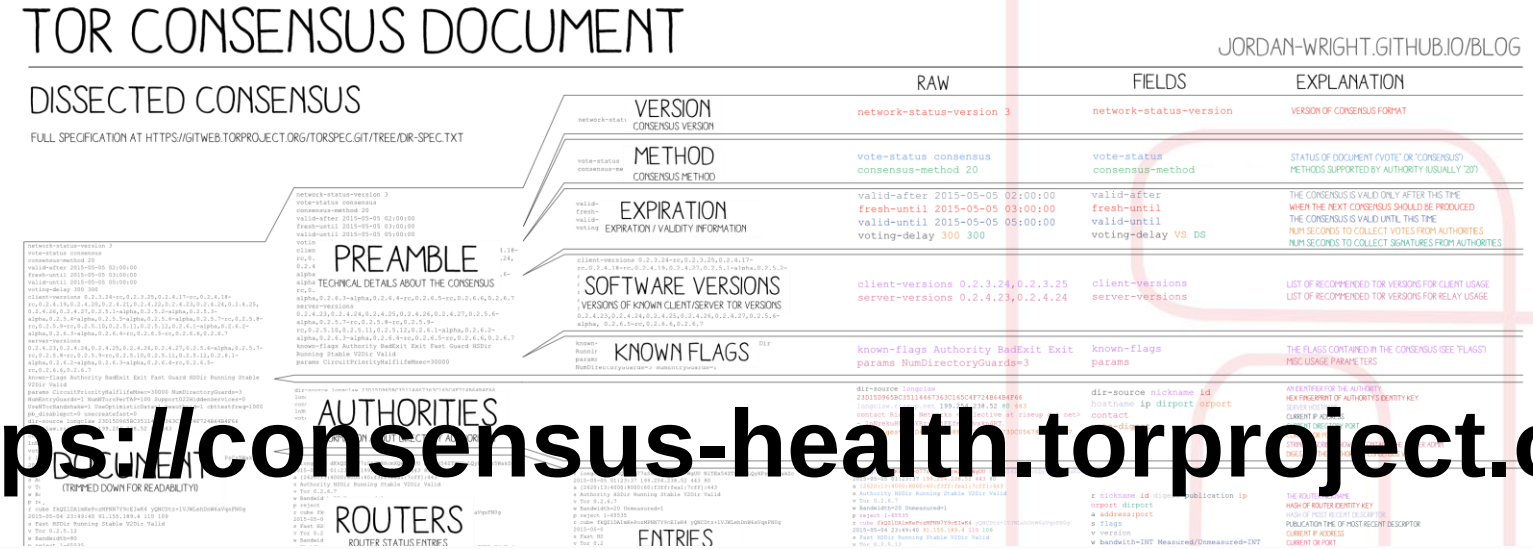
Autoridades de directorio:

- Garantizan el correcto funcionamiento de la red
- Gestionan la configuración de la red.
- Gestionan Rendimiento de la red
- Aportan Estadísticas
- Generan el documento de consenso (Información nodos que forman la red TOR)

flag:Authority

Nickname	Bandwidth	Uptime	Country	IP	Flags	ORPort	DirPort	Type
dizum	2.46 MB/s	10d 23h		194.109.206.212		443	80	Relay
maatuska	51.2 KB/s	18d 21h		171.25.193.9		80	443	Relay
Bifroest	472.35 KB/s	18d 2h		37.218.247.217		443	80	Relay
dannenberg	2.1 MB/s	1d 20h		193.23.244.244		443	80	Relay
tor26	76.8 KB/s	17d 20m		86.59.21.38		443	80	Relay
Faravahar	514.84 KB/s	4d 14h		154.35.175.225		443	80	Relay
moria1	512 KB/s	9d 11h		128.31.0.34		9101	9131	Relay
longclaw	38.91 KB/s	3d 23h		199.254.238.53		443	80	Relay
gabelmoo	40.96 KB/s	9d 21h		131.188.40.189		443	80	Relay

Documento de Consenso



https://consensus-health.torproject.org/

Resumen proceso de votación

1- Recibir Descriptores

Cada nodo genera un descriptor con sus datos (Nombre,Ip,SO..) y lo envia a cada Autoridad de Directorio

2 - Creación de Status-Vote

Cada Autoridad de directorio incluye otros datos como las Flags de cada nodo entre otros y lo envia al resto de Autoridades

3 - Computo del consenso

Se procesan todos los votos y se genera el documento de consenso.

4 - Distribución del consenso

Cada autoridad distribuye en concenso a los clientes y a los directorios de cache

Flags asignadas a nodos

Authority
Exit
Fast
Guard
HSDir
Running
Stable
Named
Unnamed
Valid V2dir

Aggregate Network Statistic Summary | Graphs / Details		
Total Bandwidth of displayed Routers [GBytes/s]	2.993	
Total Number of Routers	7151	100%
Routers in Current Query Result Set	930	13.01%
Total Number of 'Authority' Routers	9	0.1%
Total Number of 'Bad Directory' Routers	0	0%
Total Number of 'Bad Exit' Routers	4	0.1%
Total Number of 'Exit' Routers	930	13%
Total Number of 'Fast' Routers	5969	83.5%
Total Number of 'Guard' Routers	2398	33.5%
Total Number of 'Hibernating' Routers	2	0%
Total Number of 'Named' Routers	0	0%
Total Number of 'Stable' Routers	6021	84.2%
Total Number of 'Running' Routers	7151	100%
Total Number of 'Valid' Routers	7151	100%
Total Number of 'V2Dir' Routers	4733	66.2%
Total Number of 'Directory Mirror' Routers	4733	66.2%

http://blog.kamaluk.com/post/60948276326/tor-flags

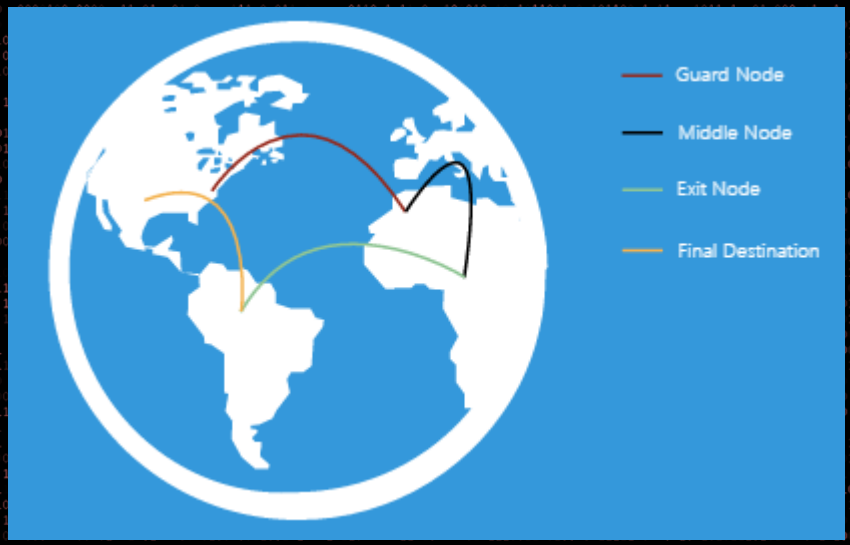
Tipos de repetidores / Nodos

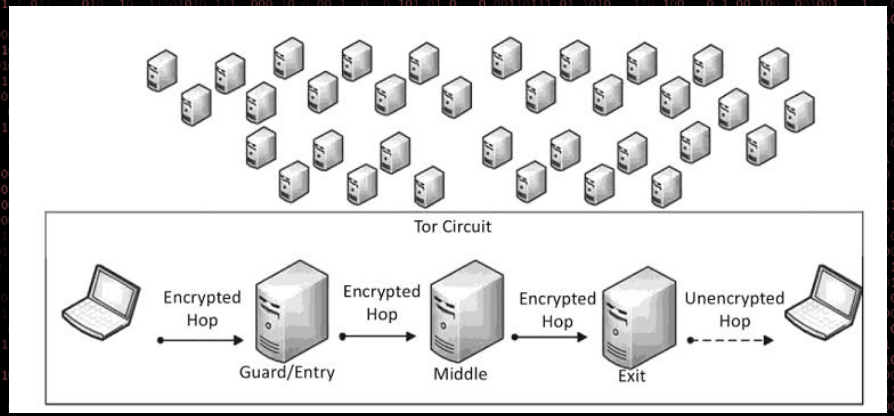
Guard/Entry Node

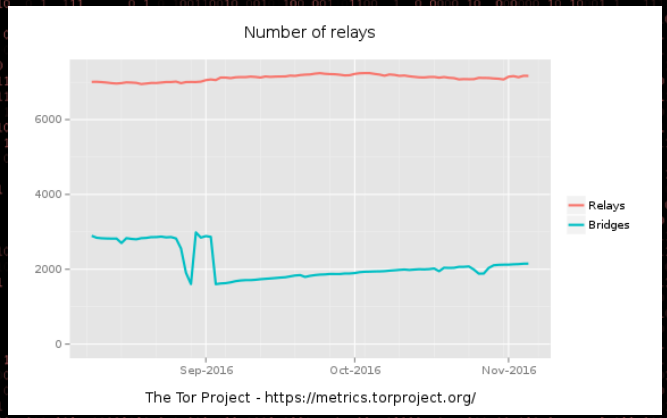
Middle Node

Exit Node

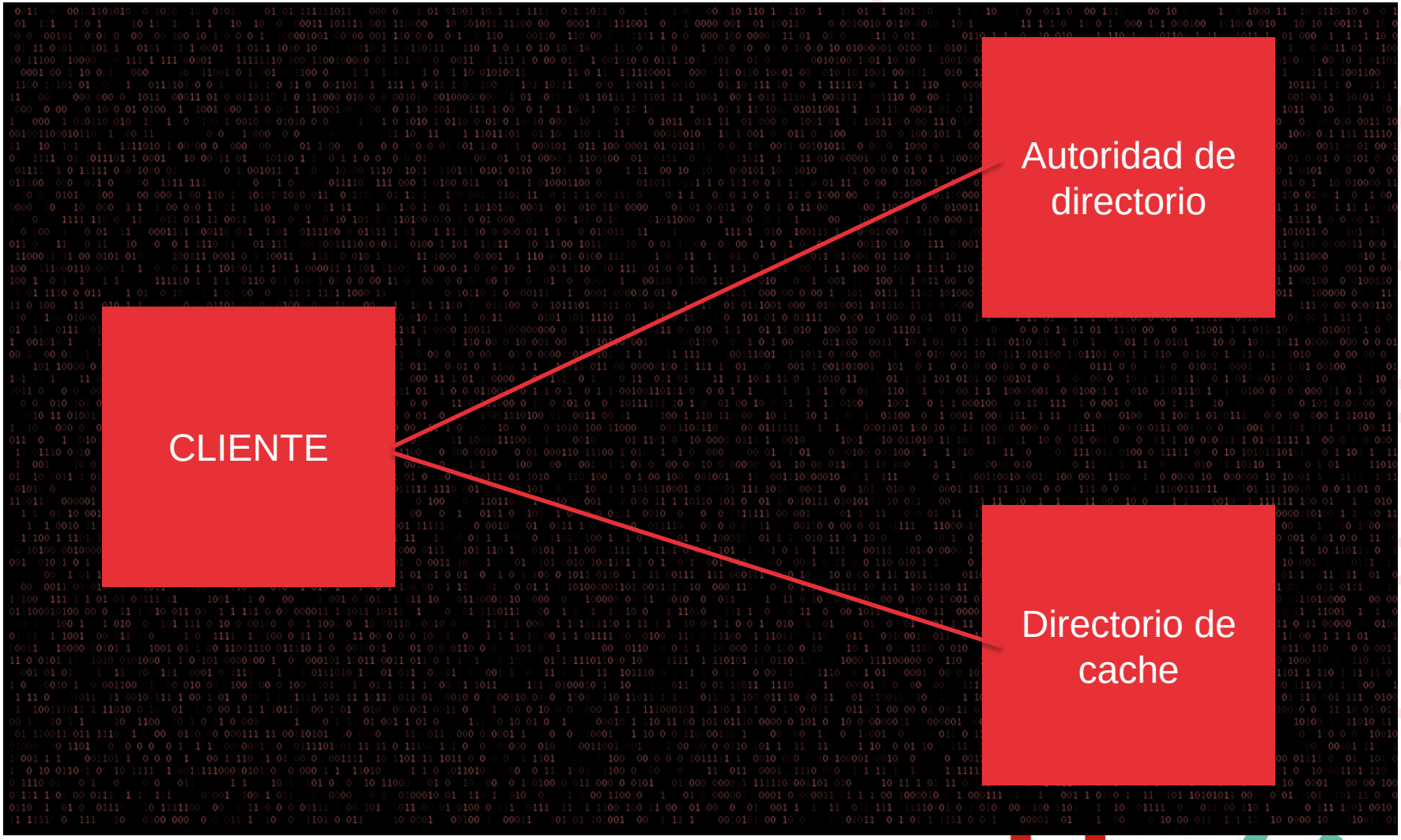
Brigde







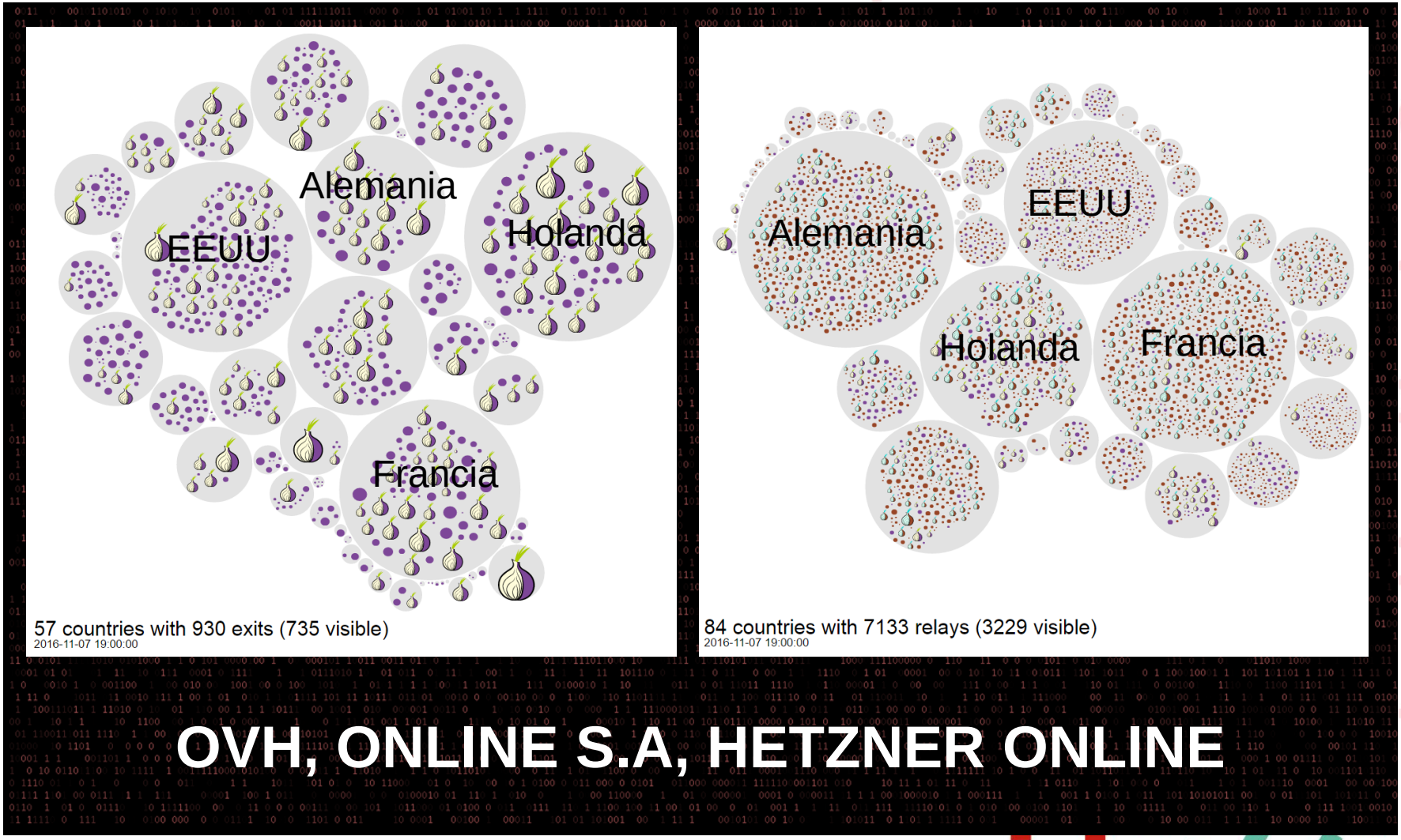
Directorios de cache



Mapeados de Nodos a nivel Mundial

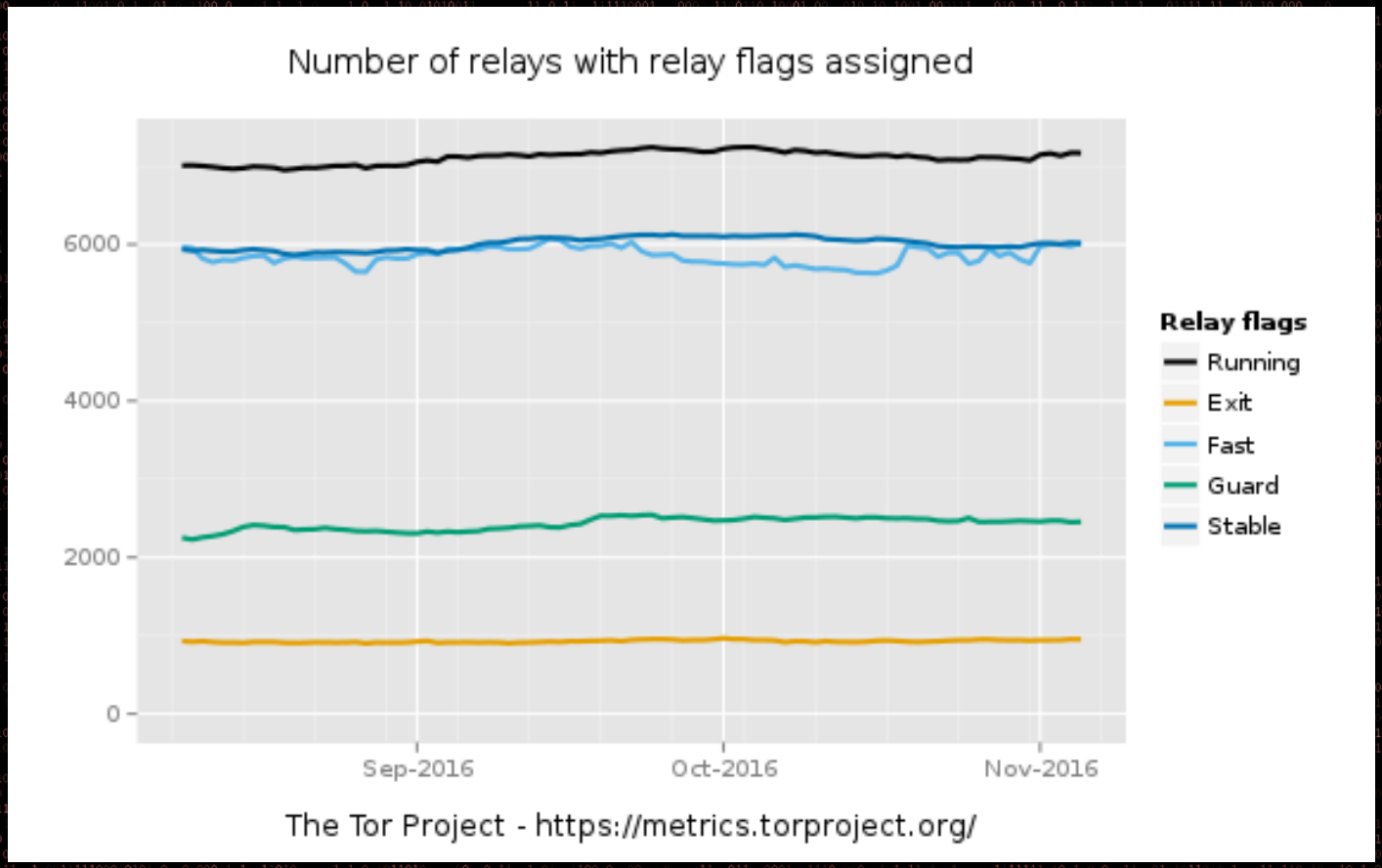
TorFlow

Estadísticas de Nodos por Paises / ASN

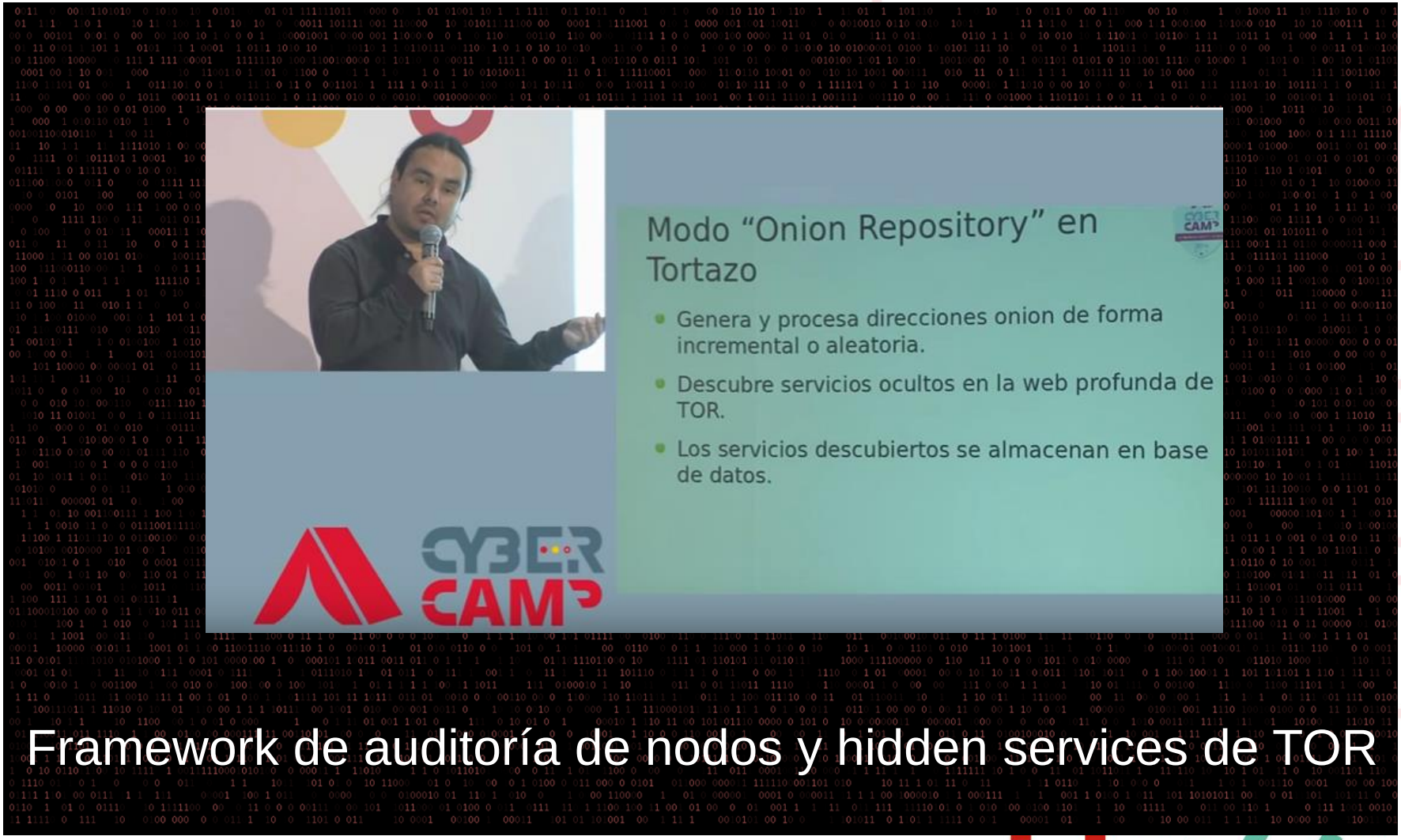


OVH, ONLINE S.A, HETZNER ONLINE

Estadísticas de tipos de nodos



Auditoria de Nodos. Tortazo



Framework de auditoría de nodos y hidden services de TOR

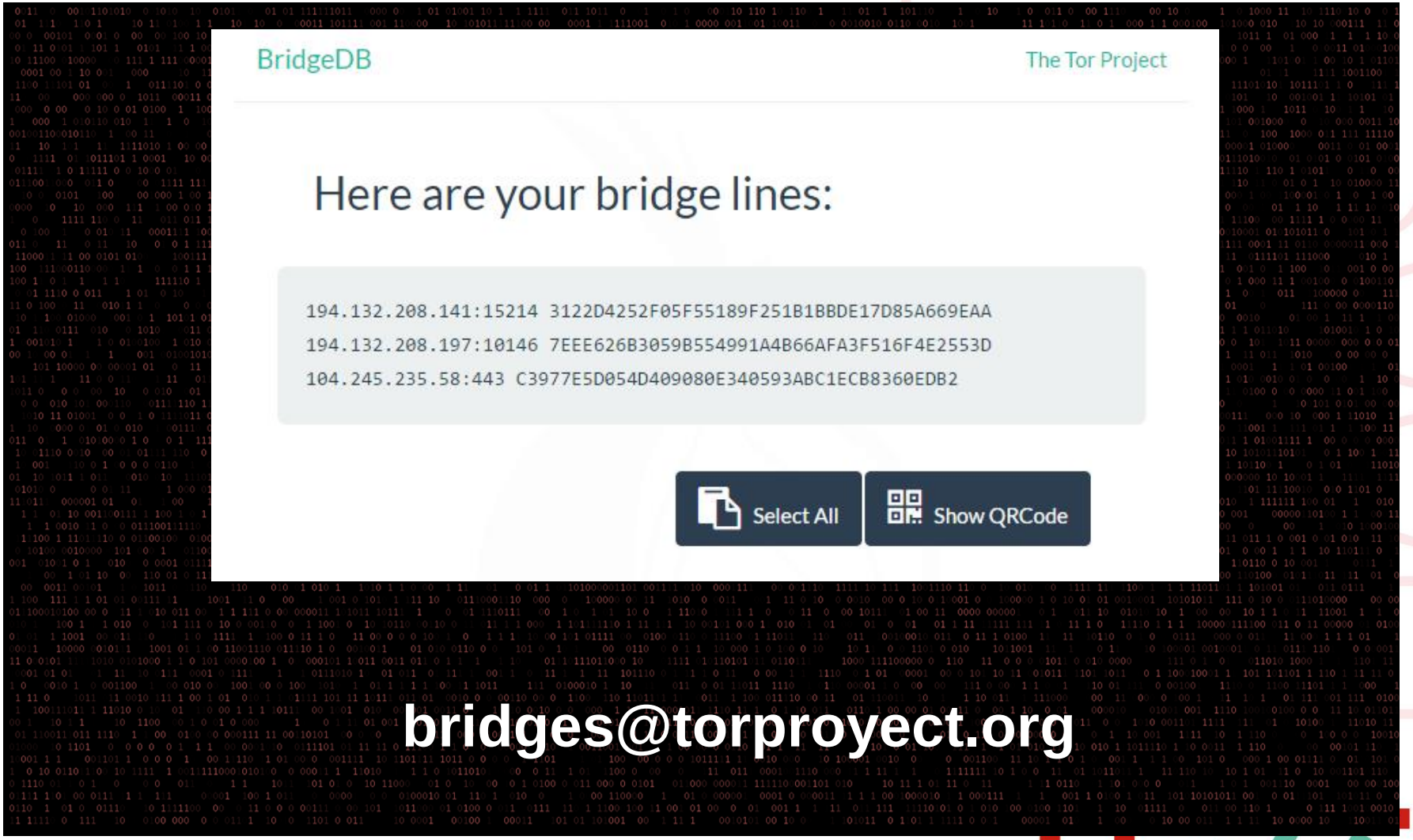
Práctica


Práctica:
Configuración de TOR como Servicio
(Repetidor Interno)

Práctica

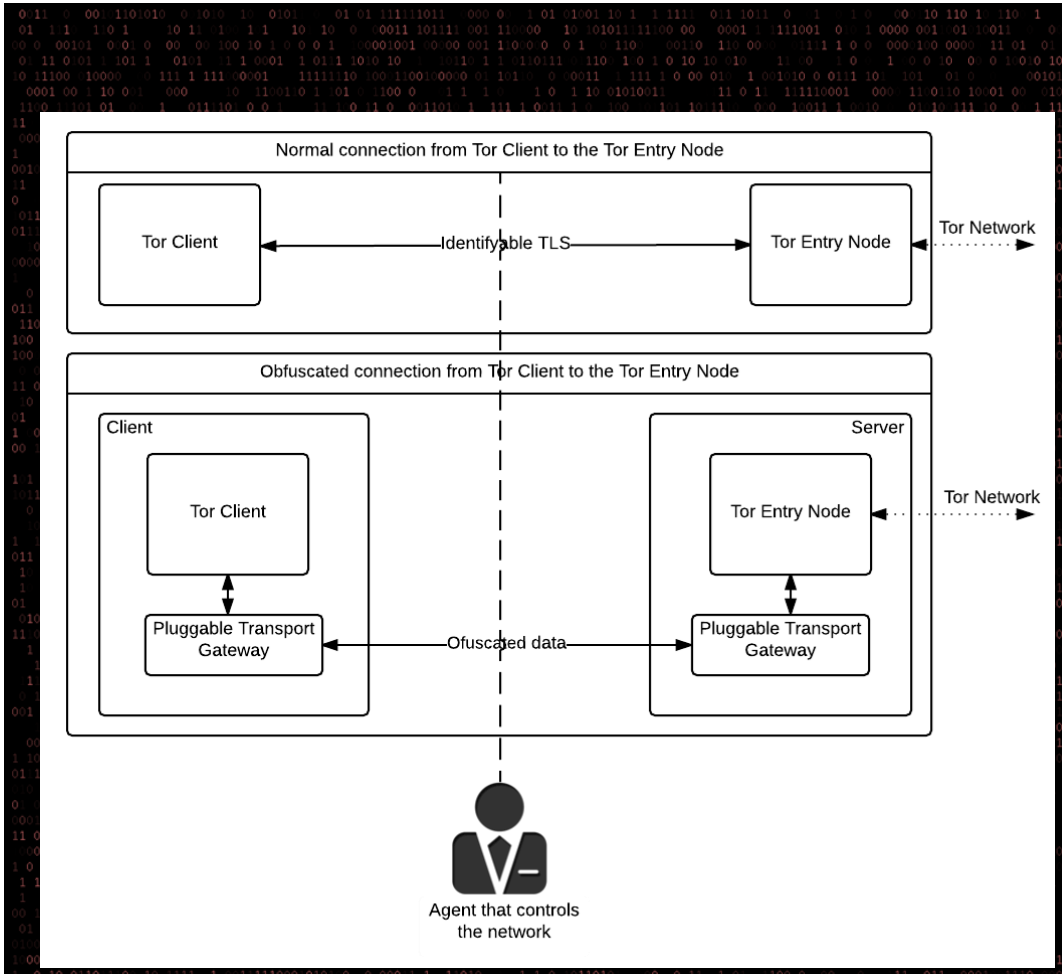
Práctica

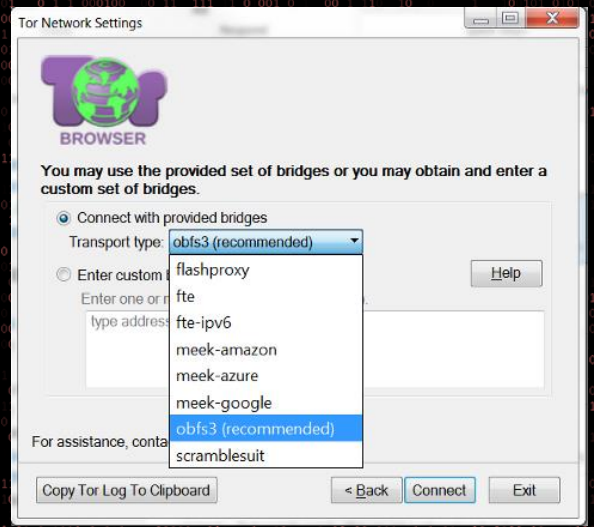
Bloqueo de TOR: Bridges



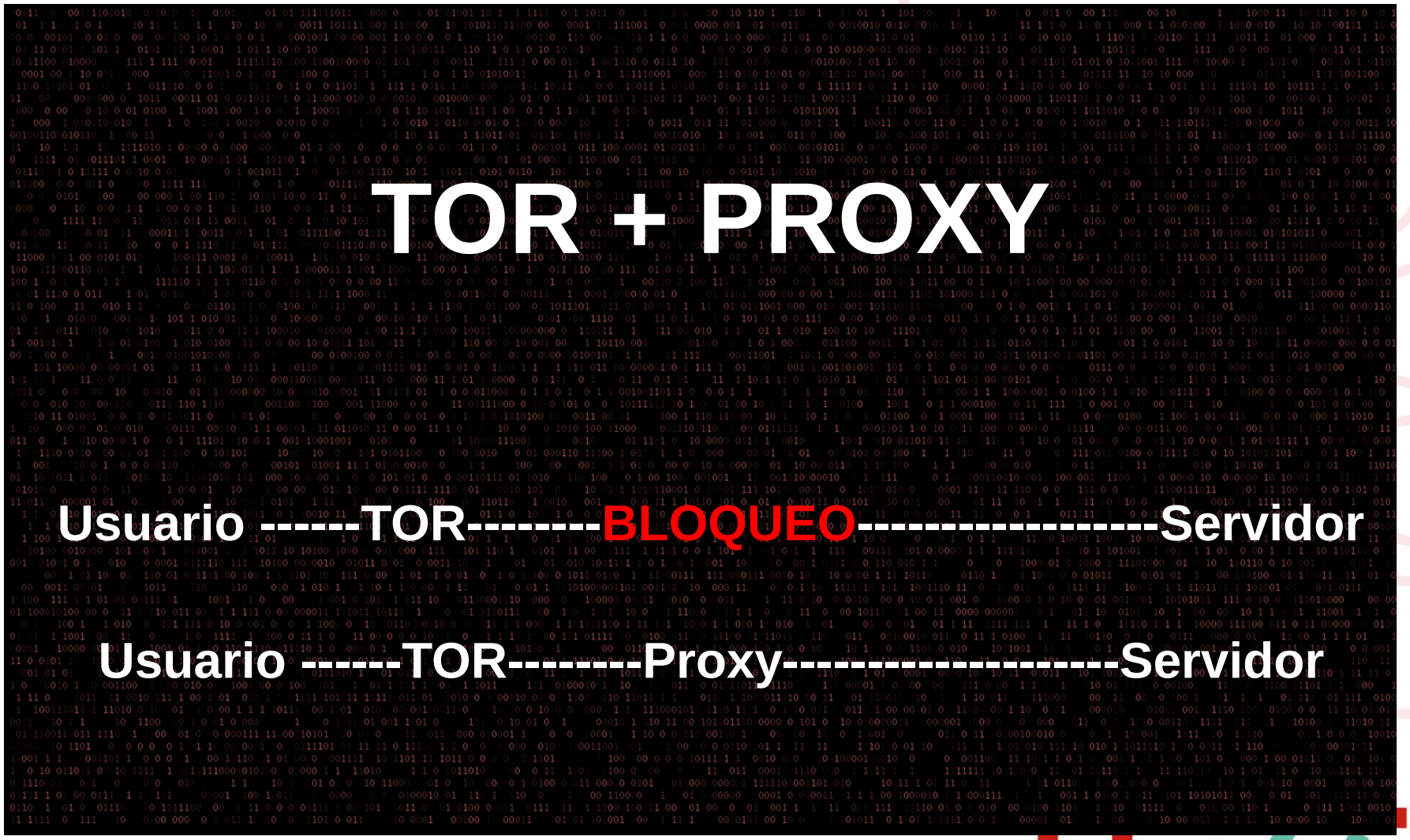
bridges@torproyect.org

Bloqueo de TOR: Pluggable Transport





Bloqueo de TOR: Proxy



Práctica


Práctica:
Solicitar Bridges: BrigdesDB y
bridges@torproject

Práctica

Práctica


Práctica:
Ofuscación de Tráfico: Pluggable Transport

Descriptores y Tipos.

Descriptor Type	Description
Server Descriptor	Information that relays publish about themselves. Tor clients once downloaded this information, but now they use microdescriptors instead.
ExtraInfo Descriptor	Relay information that Tor clients do not need in order to function. This is self-published, like server descriptors, but not downloaded by default.
Microdescriptor	Minimalistic document that just includes the information necessary for Tor clients to work.
Network Status Document	Though Tor relays are decentralized, the directories that track the overall network are not. These central points are called **directory authorities**, and every hour they publish a document called a **consensus** (aka, network status document). The consensus in turn is made up of **router status entries**.
Router Status Entry	Relay information provided by the directory authorities including flags, heuristics used for relay selection, etc.
Hidden Service Descriptor	Information pertaining to a **Hidden Service**. These can only be **queried through the tor process**.

https://stem.torproject.org/tutorials/mirror_mirror_on_the_wall.html

Práctica

Práctica

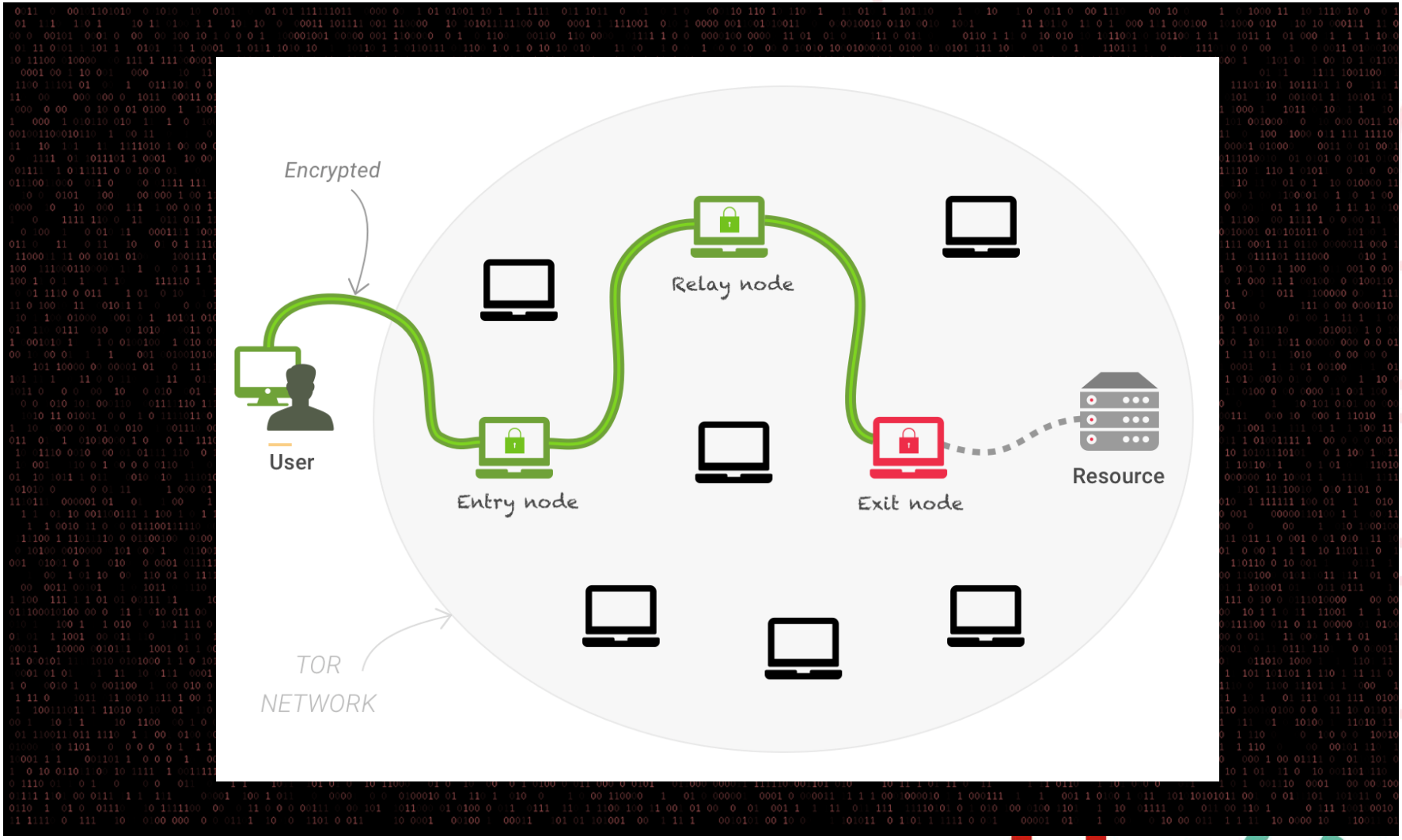
Práctica

Práctica

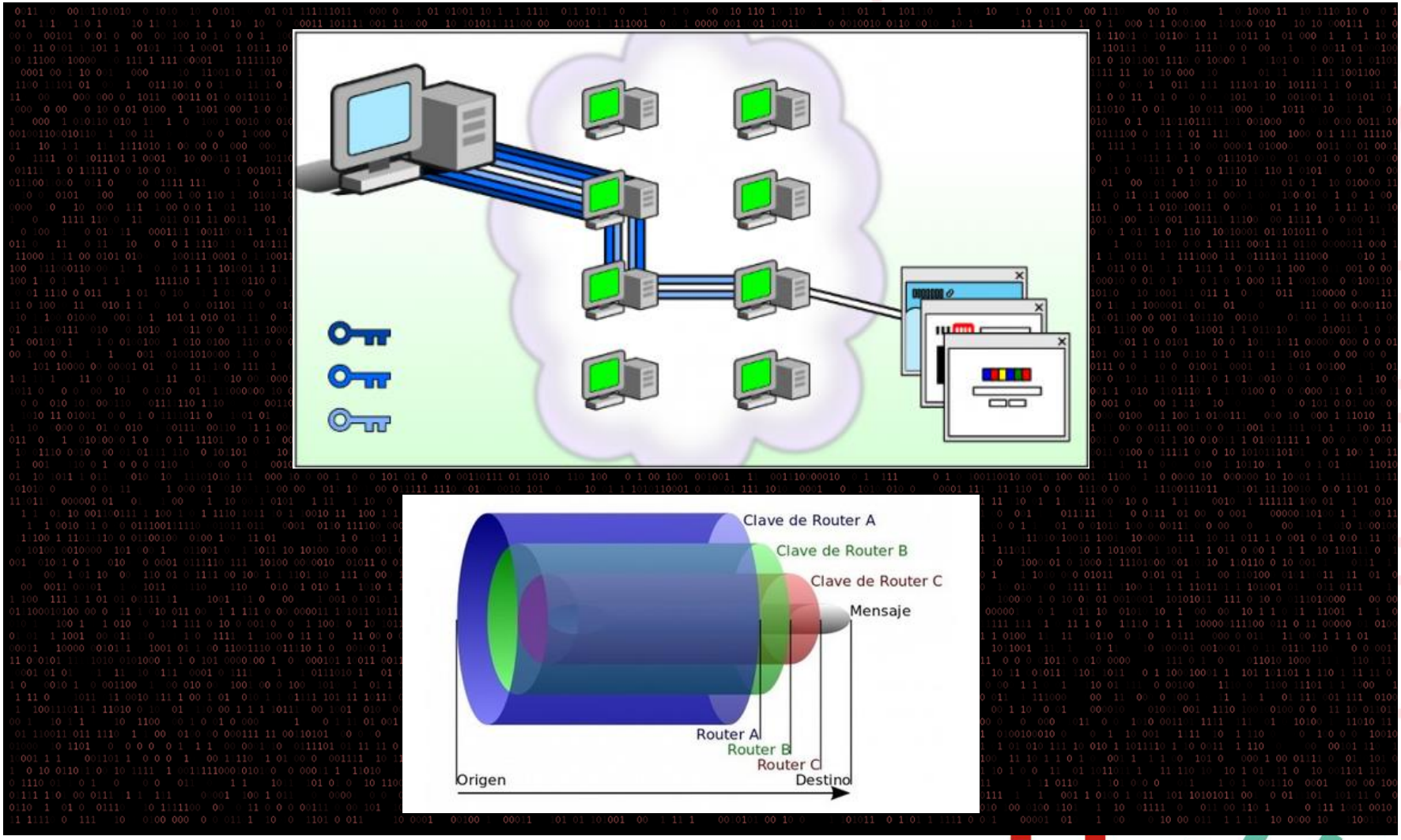
Práctica

Práctica

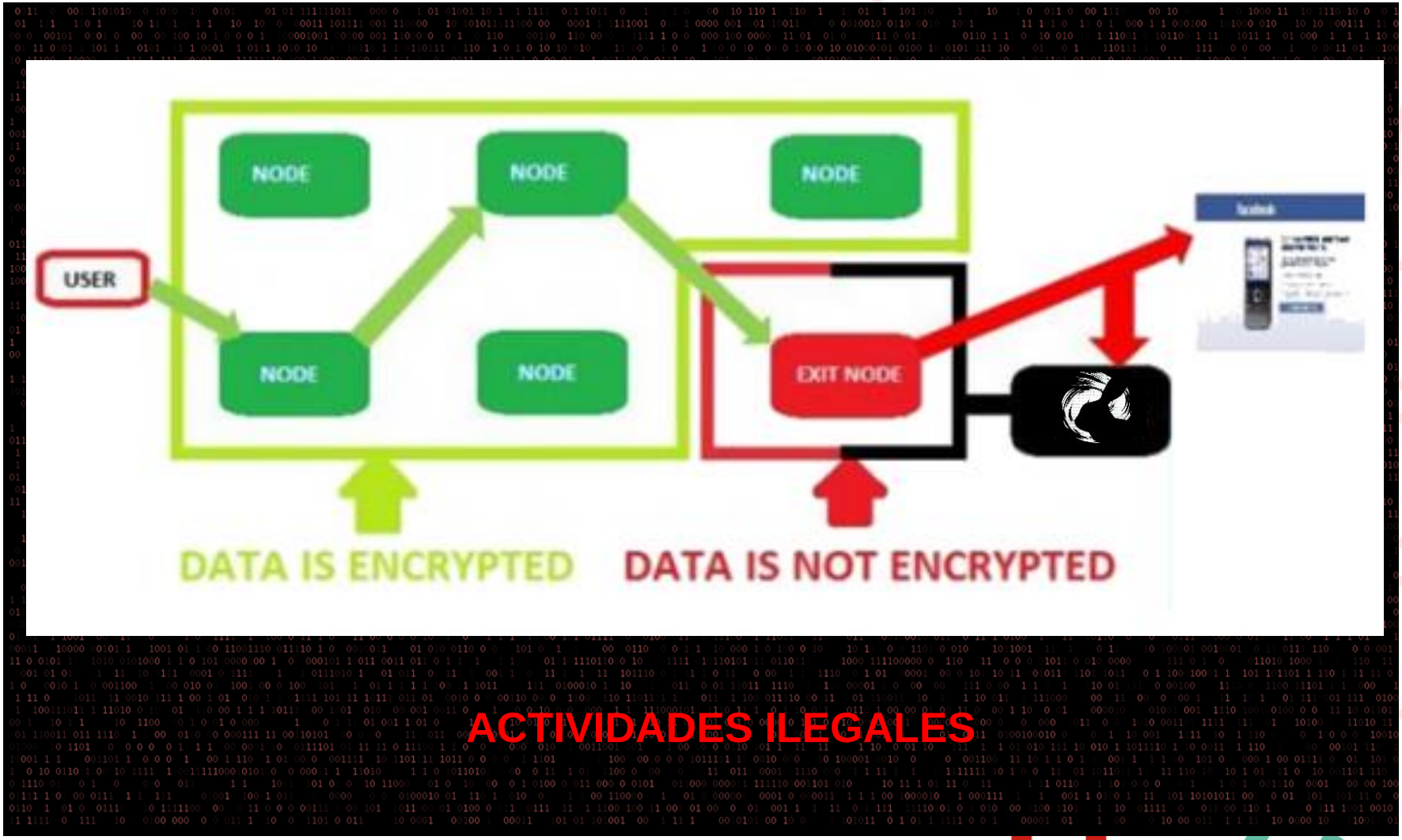
Circuitos por defecto



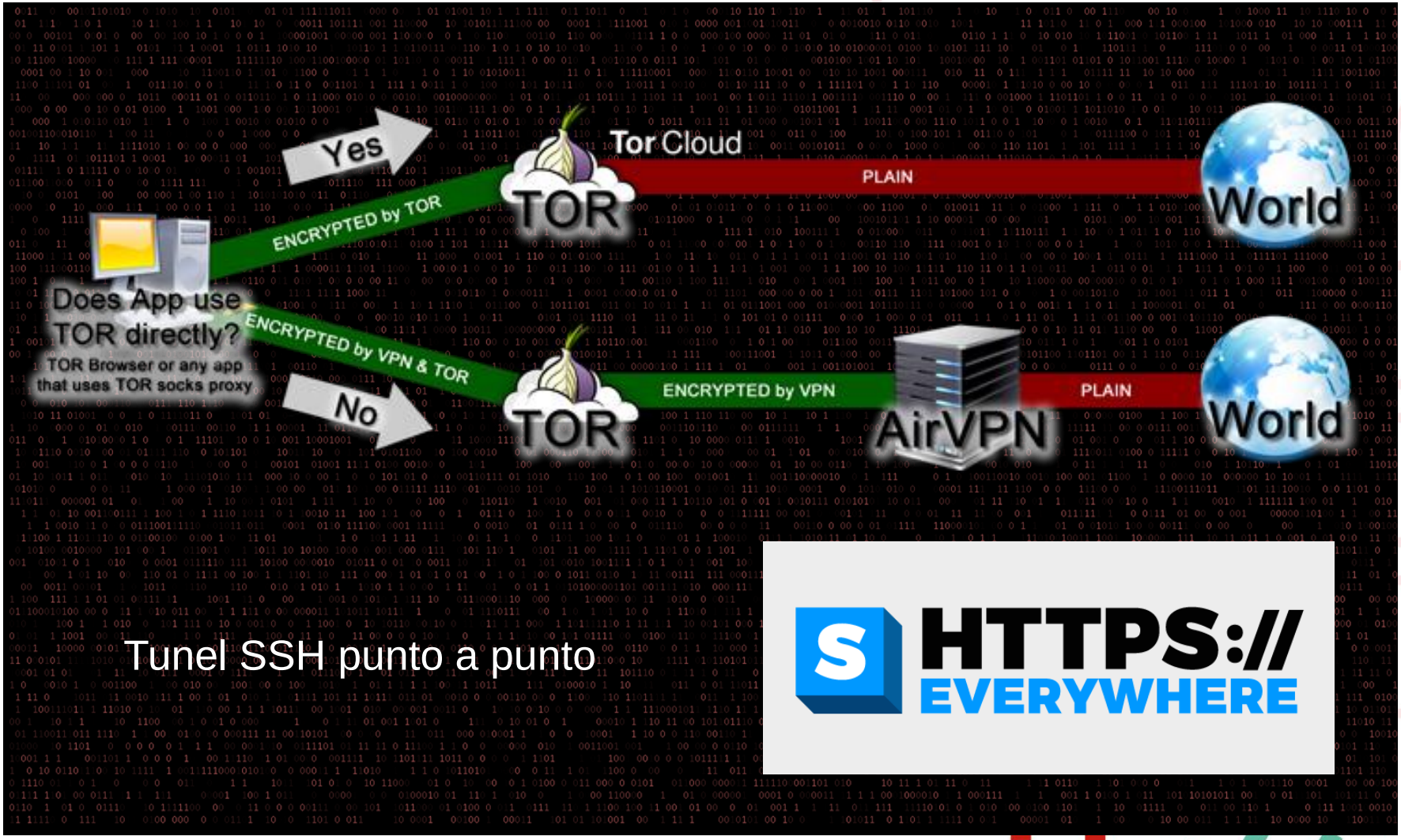
Cifrado de información



Problemática del nodo de salida



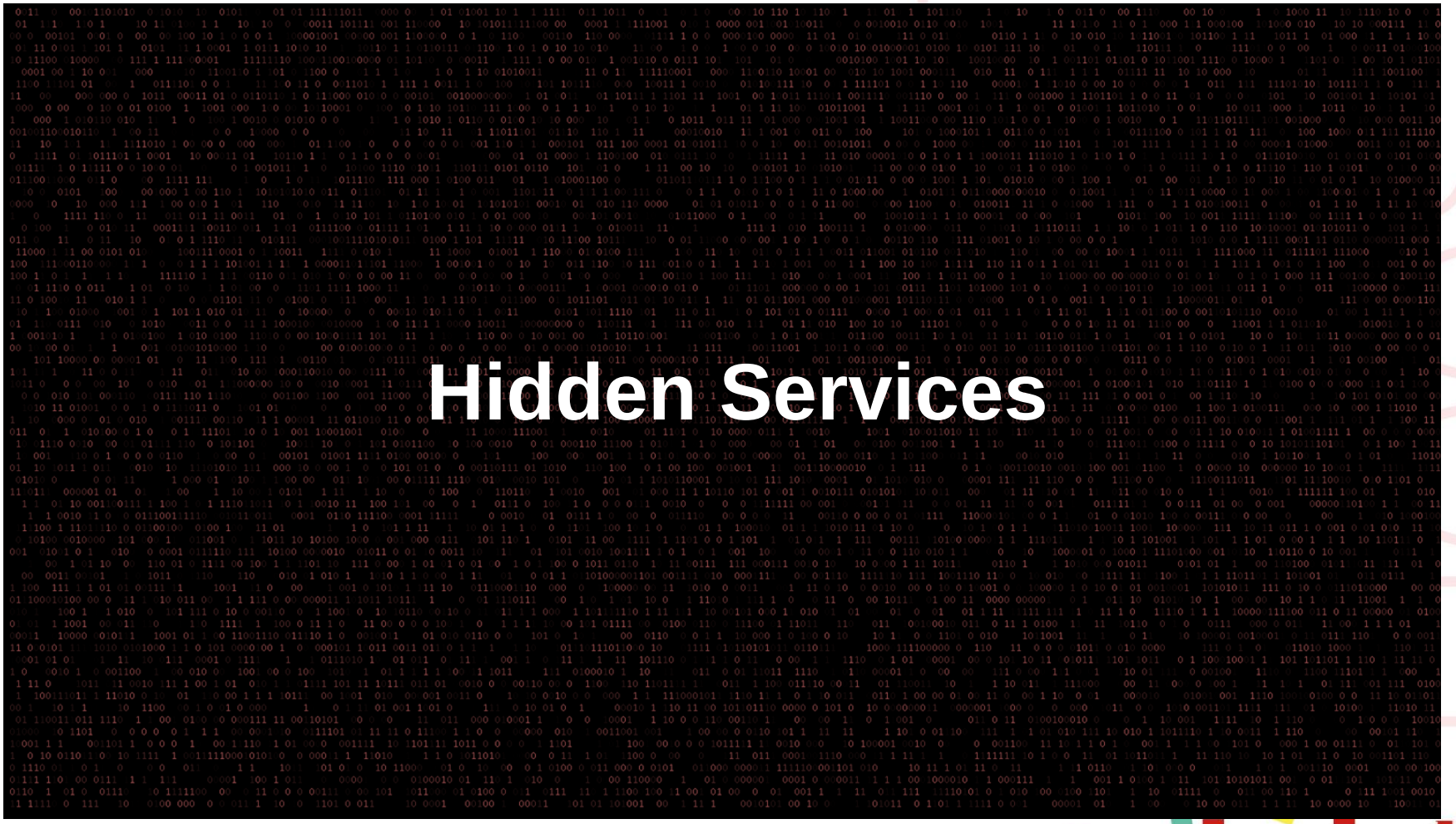
HTTPS/SSH/VPN sobre TOR



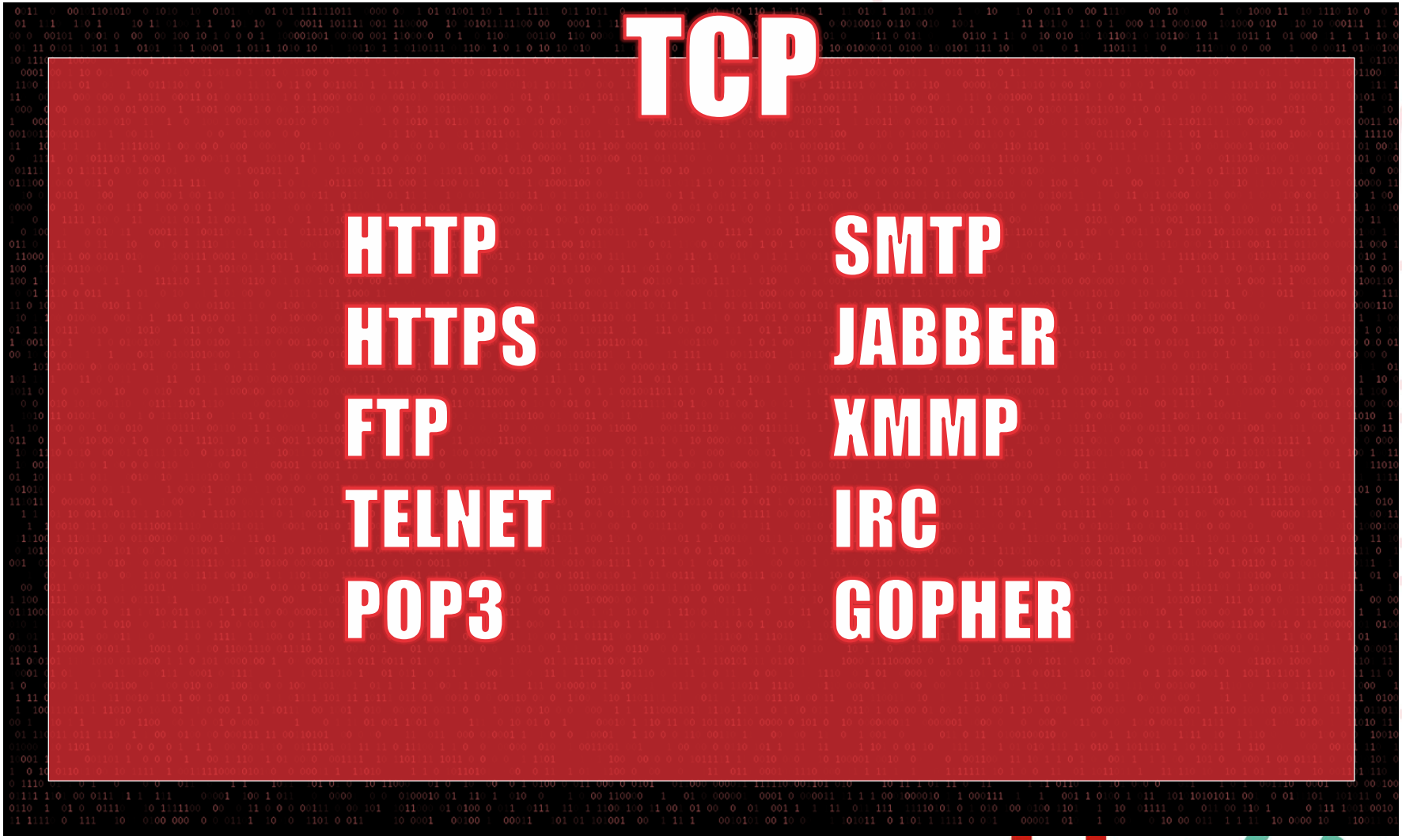
Práctica

Práctica

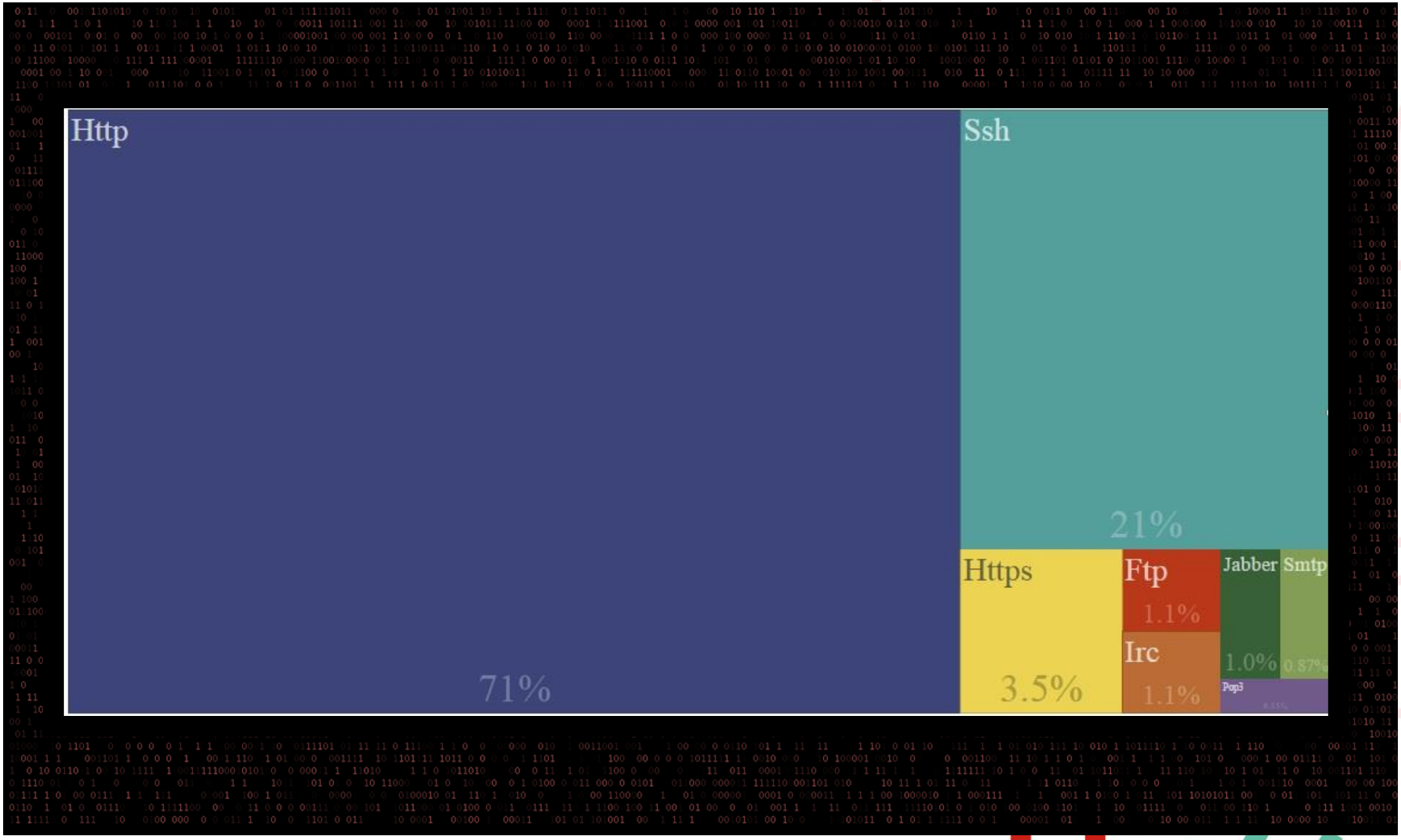
Práctica


Hidden Services

Hidden Services. Servicios expuestos en TOR

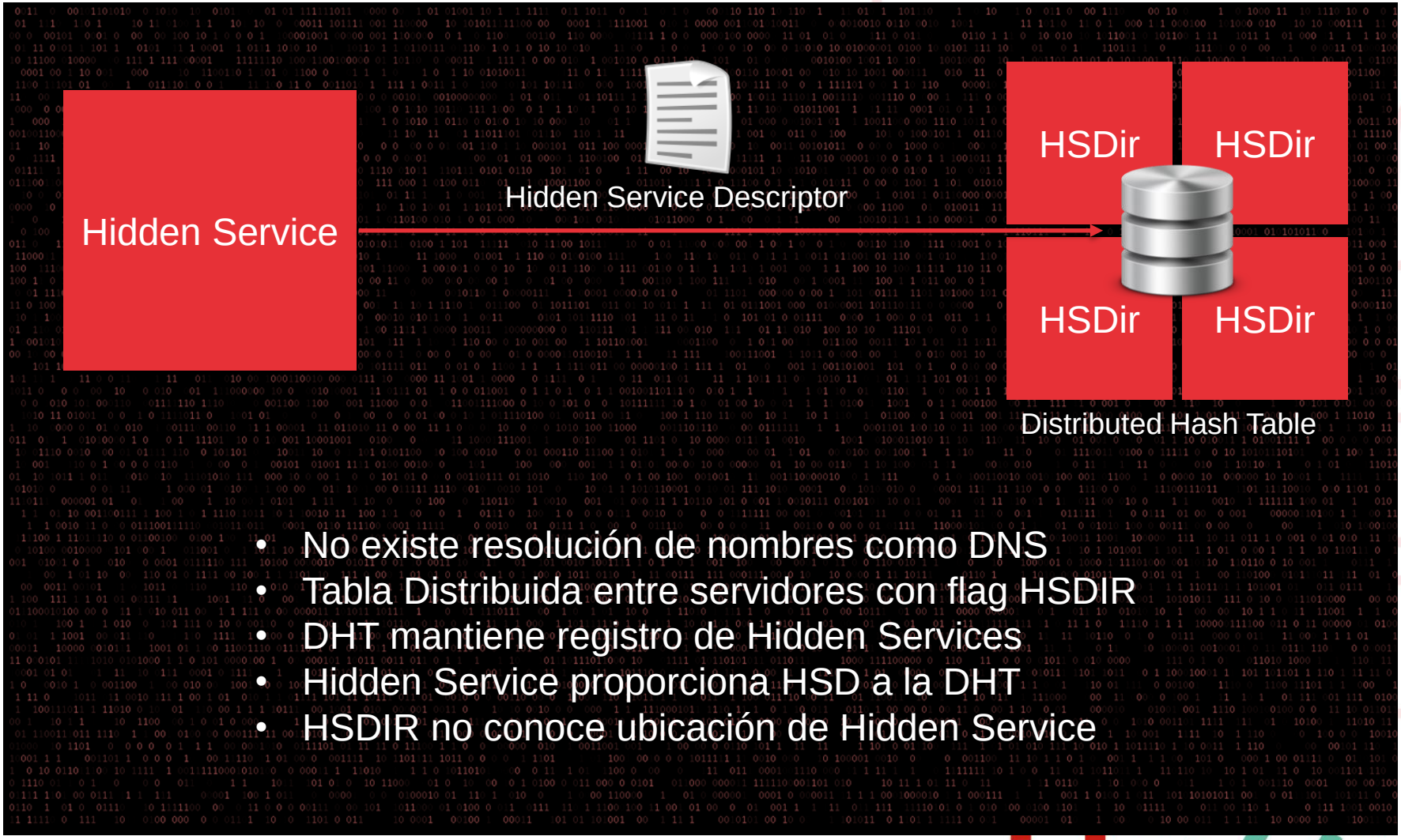


Resultado estudio 200.000 Onion



Donde se despliegan los Hidden Services

No DNS. Hidden Service Directory. DHT

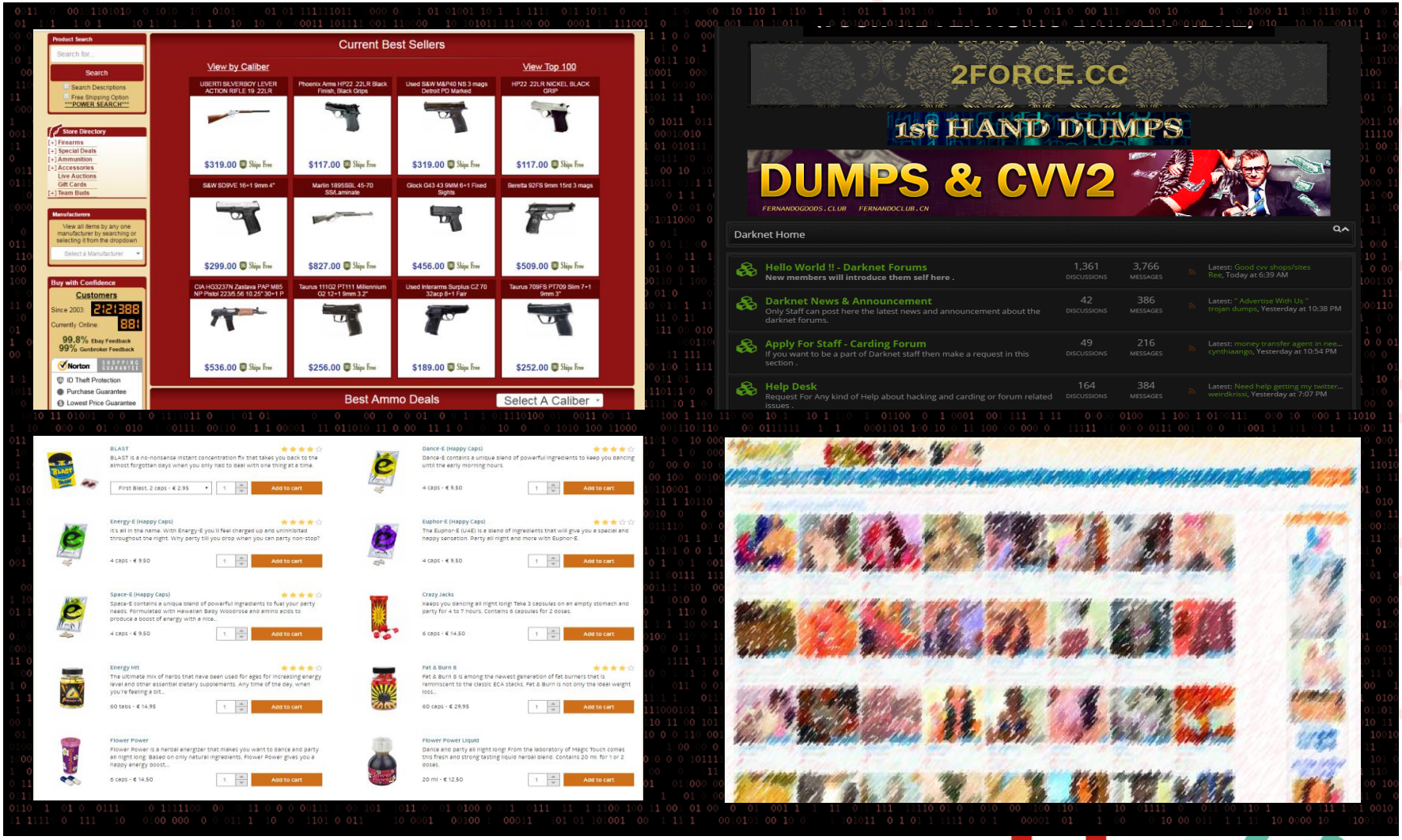


- No existe resolución de nombres como DNS
- Tabla Distribuida entre servidores con flag HSDIR
- DHT mantiene registro de Hidden Services
- Hidden Service proporciona HSD a la DHT
- HSDIR no conoce ubicación de Hidden Service

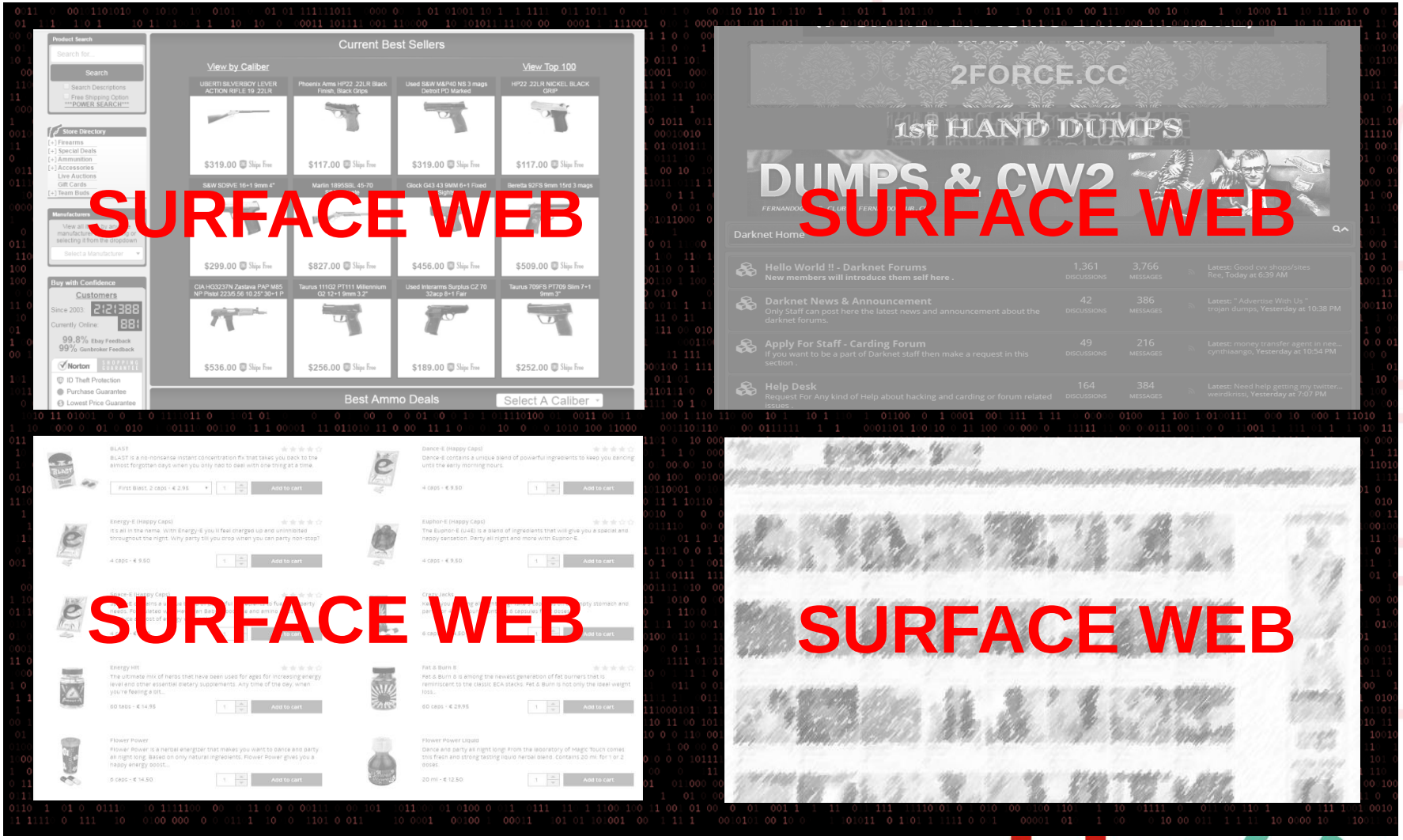
Buscadores / Acceso a TOR desde Proxy Web

Dirección onion + .to .cab .city .link

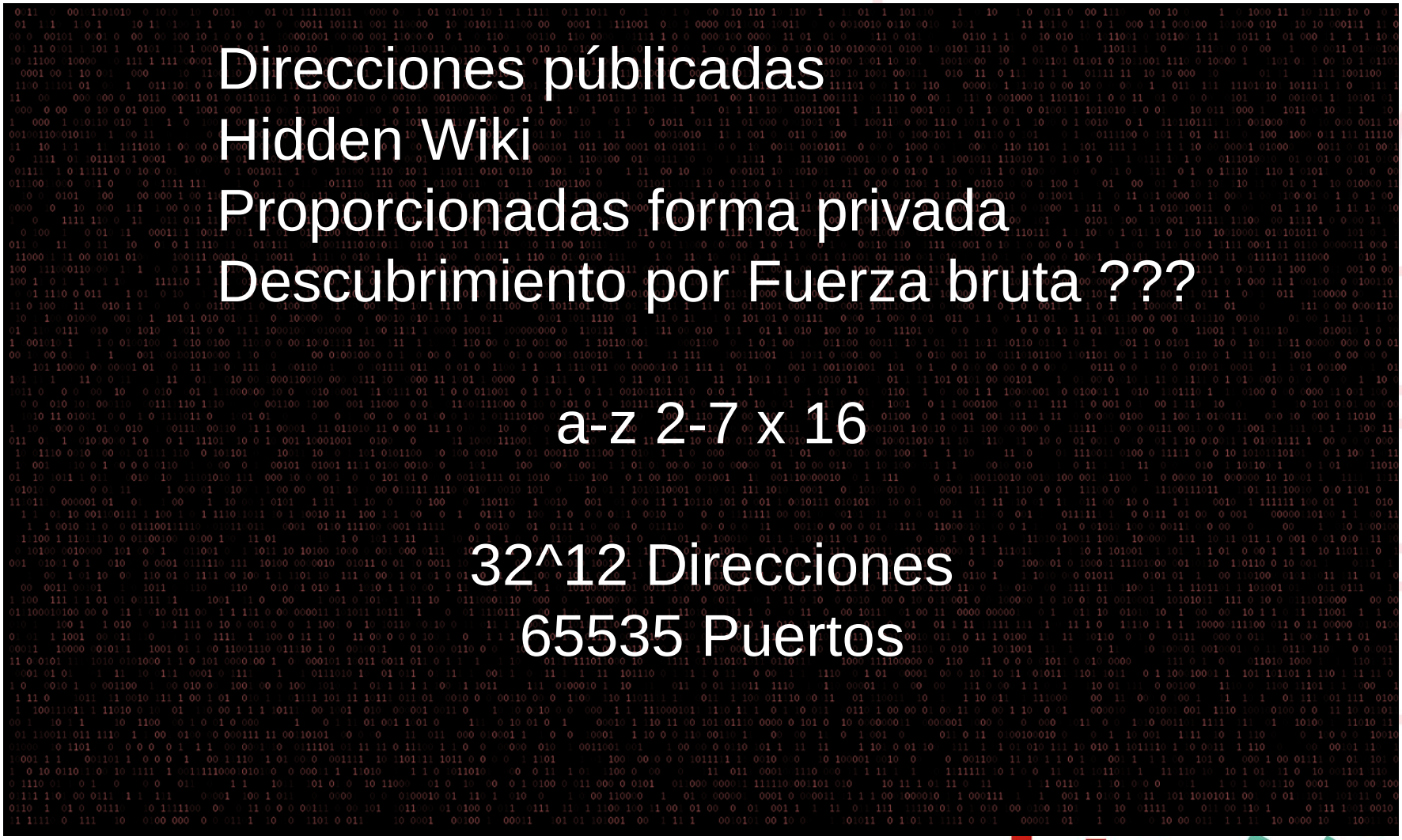
Cibercrimen en TOR



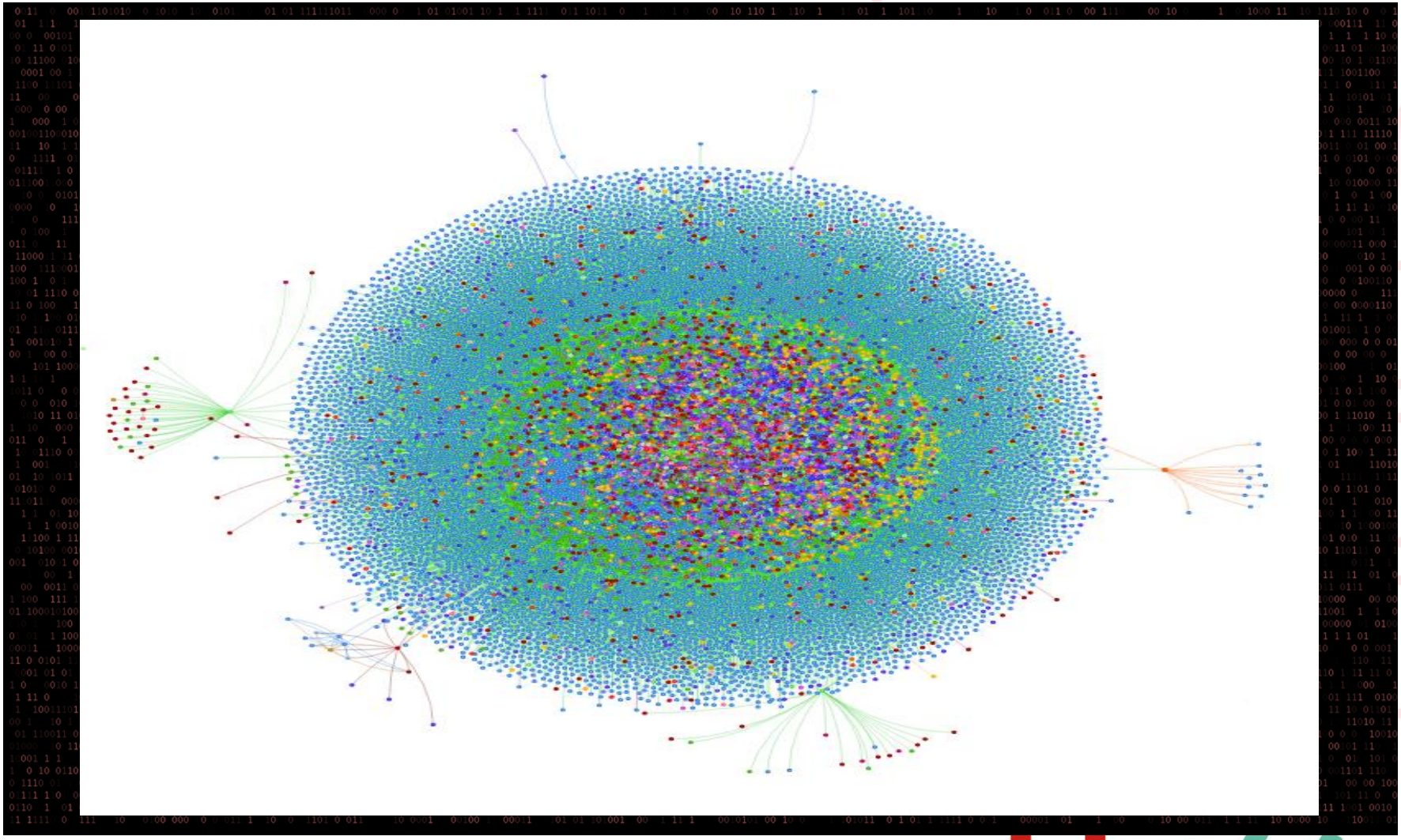
Cibercrimen en TOR / Surface WEB



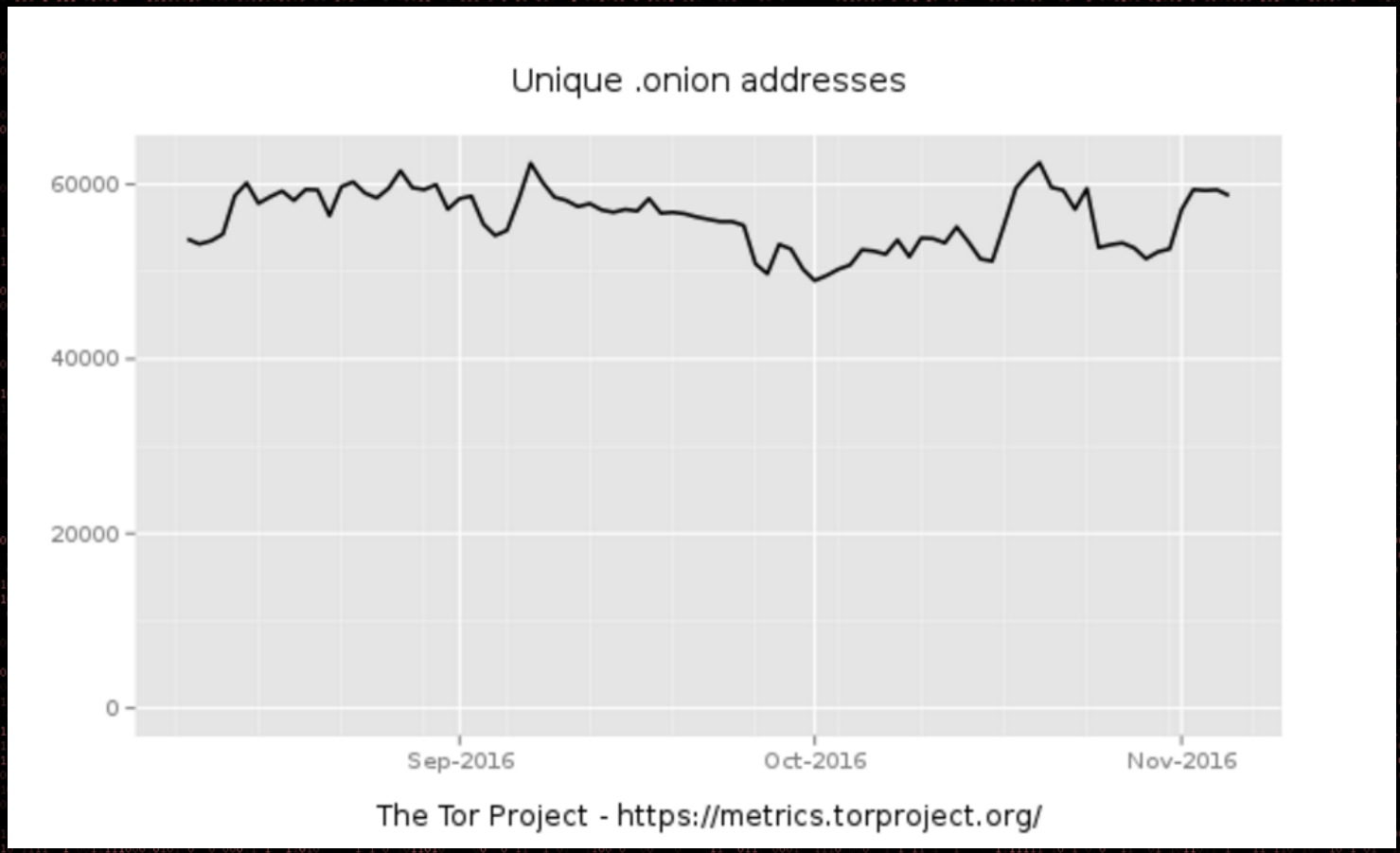
Dificultad de obtener nuevos Hidden Services



Relación Hidden Services Web detectados



Gráfica Onions en TOR



Leaks IP. Desanonimización de Onions. Onionscan

Auditoria de nuestros Hidden Service

Práctica

Práctica

Práctica


Práctica:
Servicio Onion con múltiples direcciones

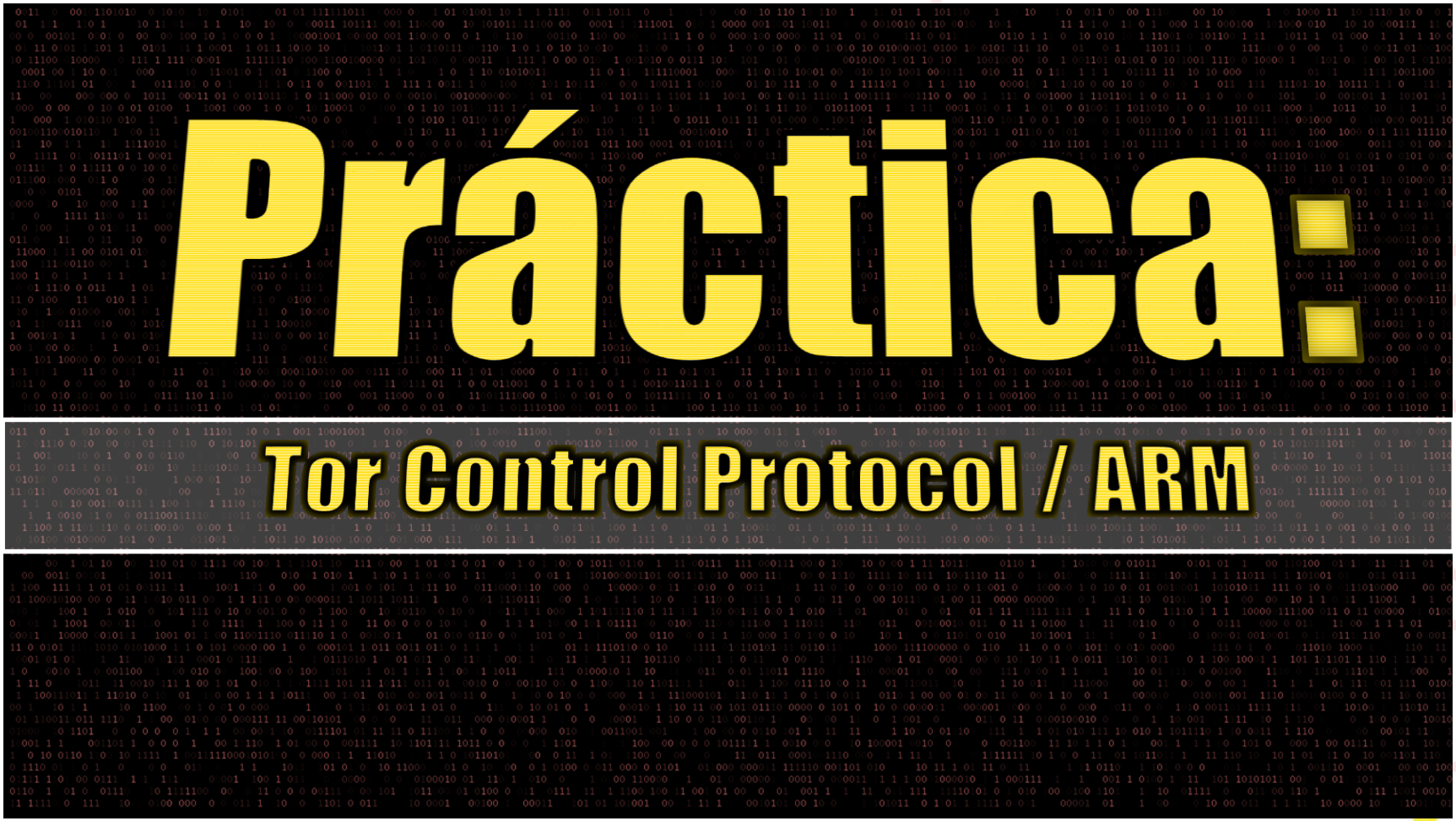
Bloque 4

Acceso Programático con Stem y TXTorCON

Tor Control Protocol / ARM

- 3.1. SETCONF
- 3.2. RESETCONF
- 3.3. GETCONF
- 3.4. SETEVENTS
- 3.5. AUTHENTICATE
- 3.6. SAVECONF
- 3.7. SIGNAL
- 3.8. MAPADDRESS
- 3.9. GETINFO
- 3.10. EXTENDCIRCUIT
- 3.11. SETCIRCUITPURPOSE
- 3.12. SETROUTERPURPOSE
- 3.13. ATTACHSTREAM
- 3.14. POSTDESCRIPTOR
- 3.15. REDIRECTSTREAM
- 3.16. CLOSESTREAM
- 3.17. CLOSECIRCUIT
- 3.18. QUIT
- 3.19. USEFEATURE
- 3.20. RESOLVE
- 3.21. PROTOCOLINFO
- 3.22. LOADCONF
- 3.23. TAKEOWNERSHIP
- 3.24. AUTHCHALLENGE
- 3.25. DROPGUARDS

TOR-ARM


Práctica:
Tor Control Protocol / ARM

Para más información:Torspec

https://gitweb.torproject.org/torspec.git/tree

¿ PREGUNTAS ?

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
incibe_
TRABAJANDO POR LA CONFIANZA DIGITAL

CyberCamp.es

Gracias por su atención

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL