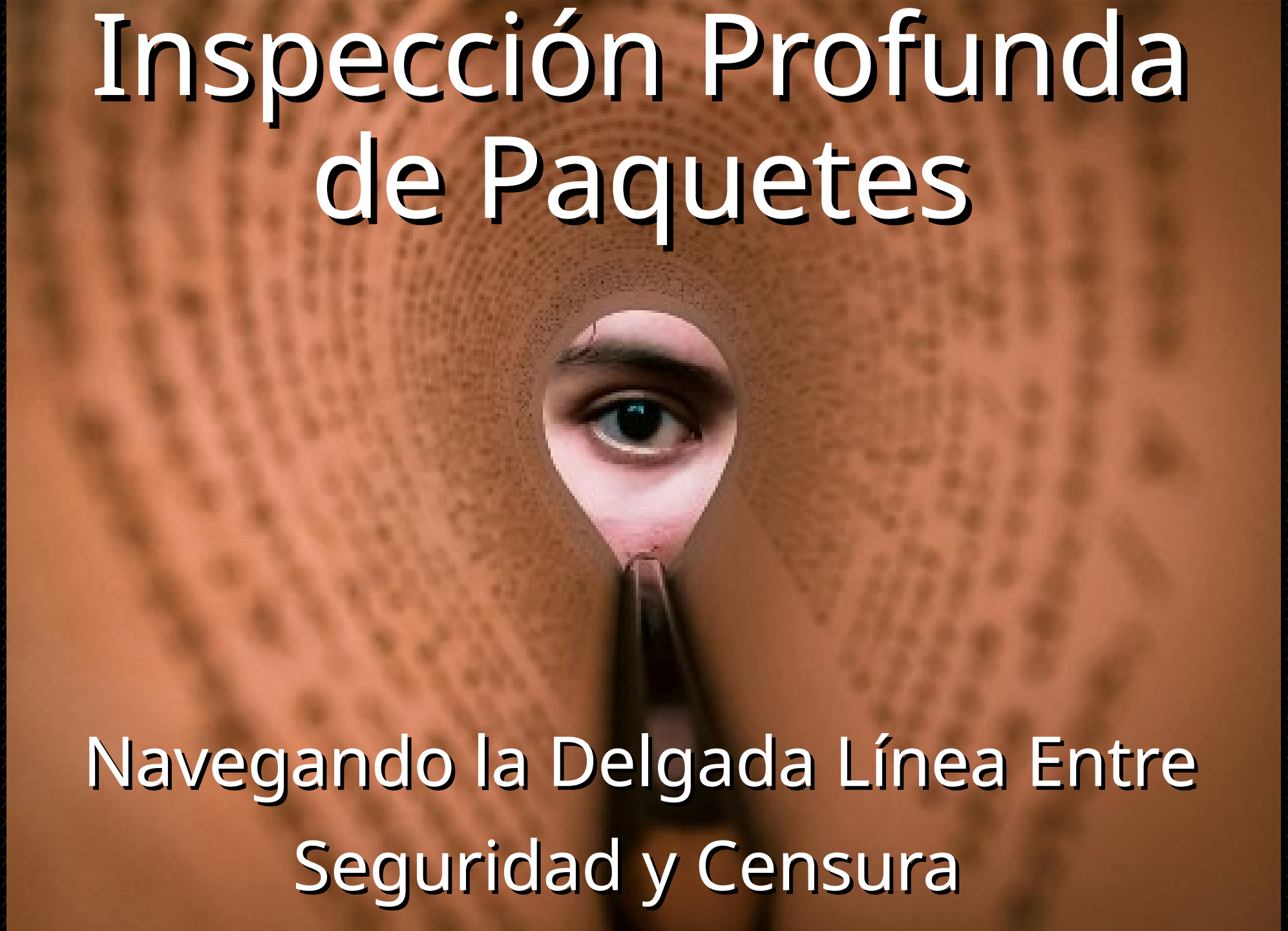
Inspección Profunda de Paquetes



Navegando la Delgada Línea Entre Seguridad y Censura

ReD

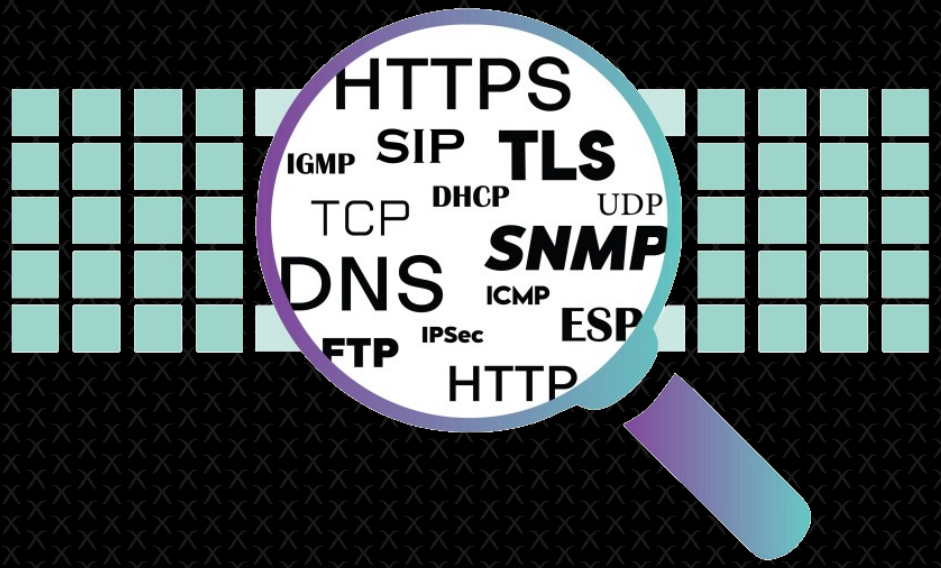
SecOpsDev
Formador, cuando me dejan

Activista tecnológico

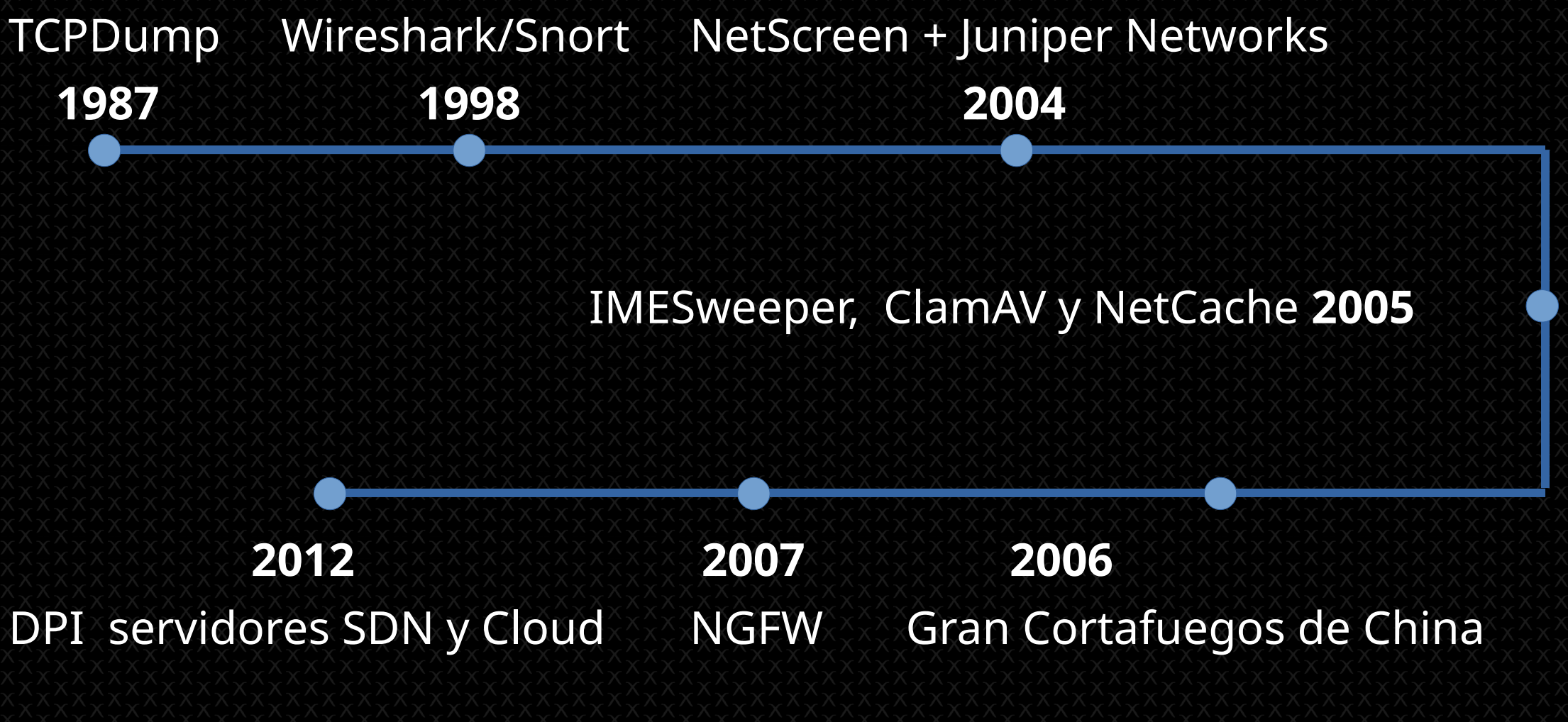
- Soberanía tecnológica
- Defensor de la privacidad
- Cofundador de Hacklabs y M4H

Motivación

DPI
Deep packet inspection



Evolución


TCPDump
1987
Wireshark/Snort
1998
NetScreen + Juniper Networks
2004
IMESweeper, ClamAV y NetCache 2005
2006
Gran Cortafuegos de China
2007
NGFW
2012
DPI servidores SDN y Cloud

DPI: ¿Qué es?

Inspección de paquetes con estado

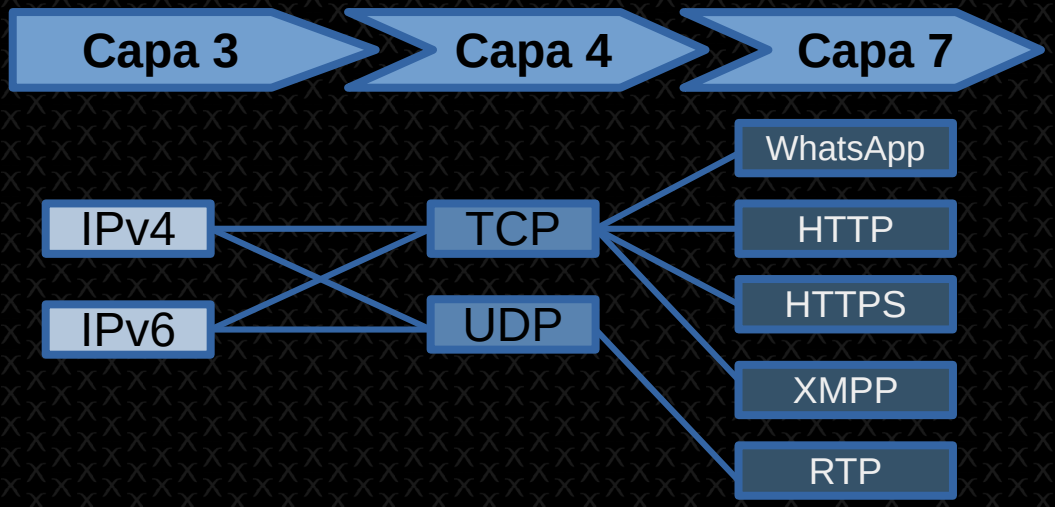
Mira el **header** y los **footer** del paquete

Inspección profunda de paquetes

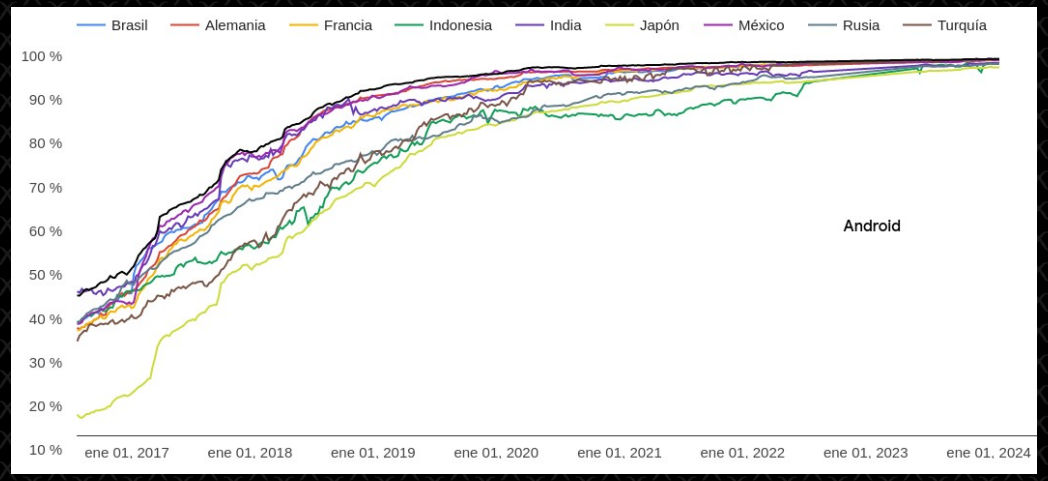
Examina la parte del **dato** del paquete

Funcionamiento DPI

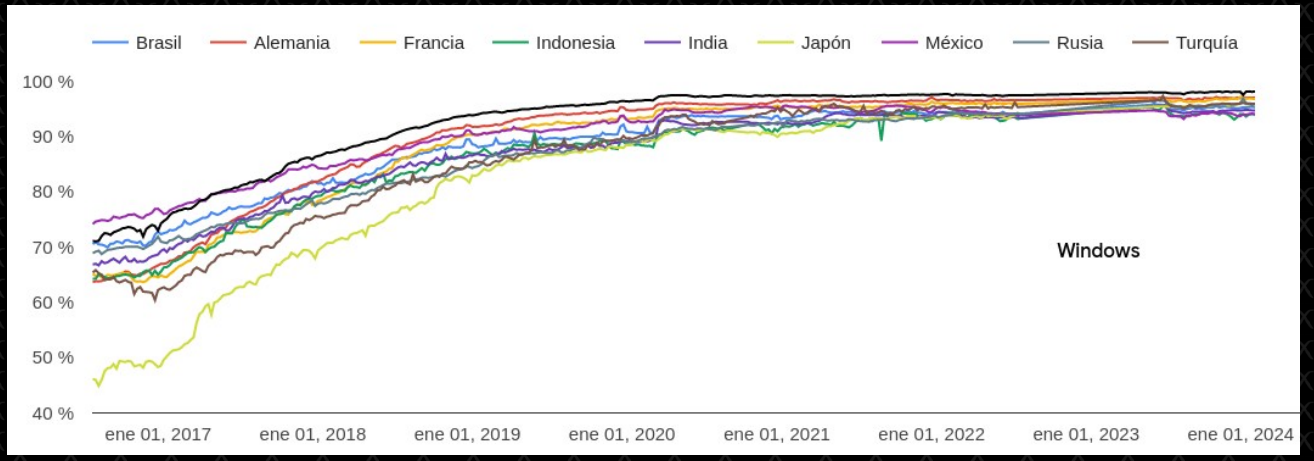
- Captura de paquetes
- Análisis de contenido
- Acción basada en el análisis
  - Permitir
  - Bloquear
  - **Ralentizar**
  - **Acelerar**
  - Registrar
  - Redireccionar



Tráfico cifrado



95% tráfico Chrome HTTPS

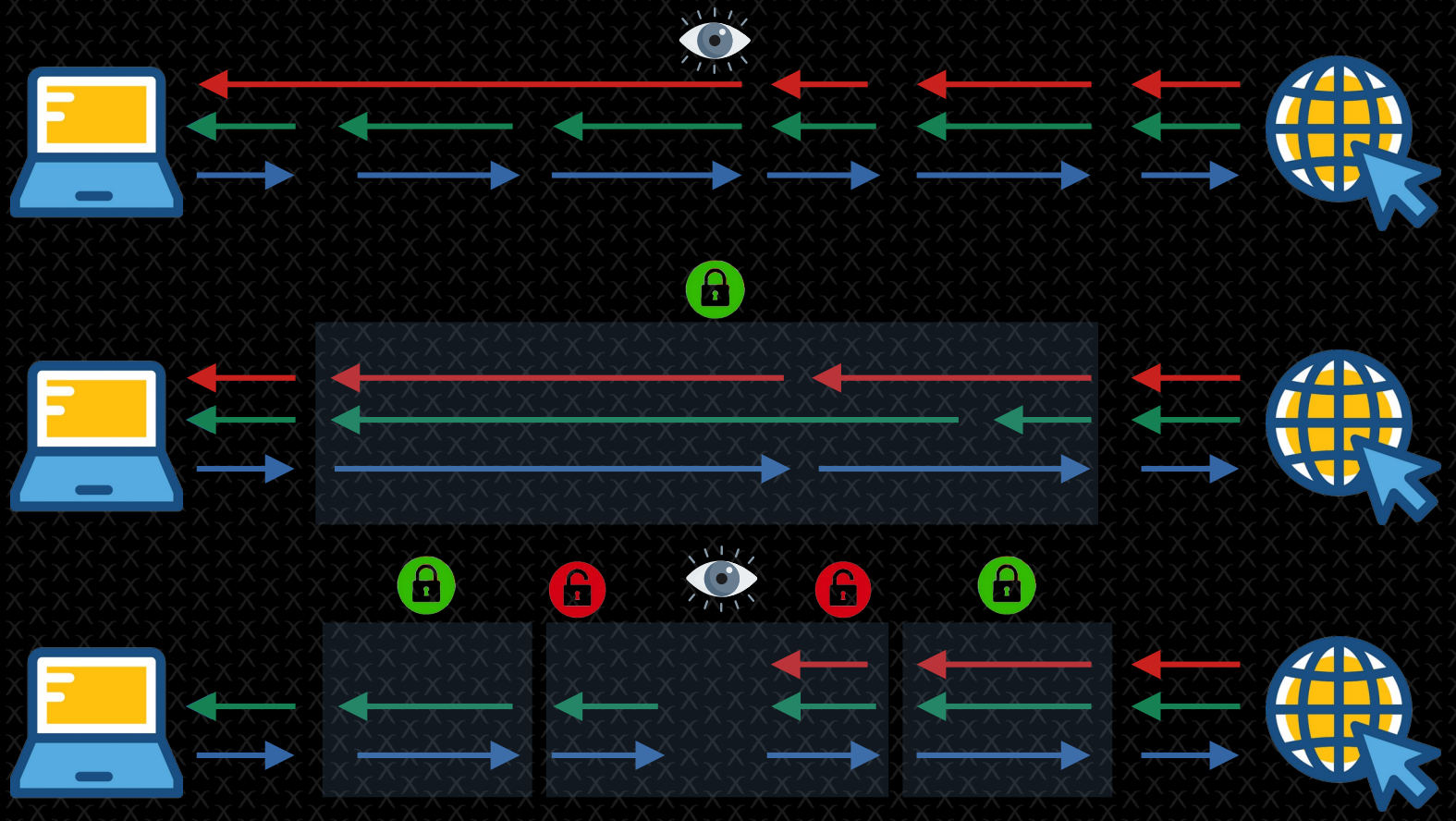


Tipos análisis con DPI

Trafico sin cifrar

Trafico cifrado

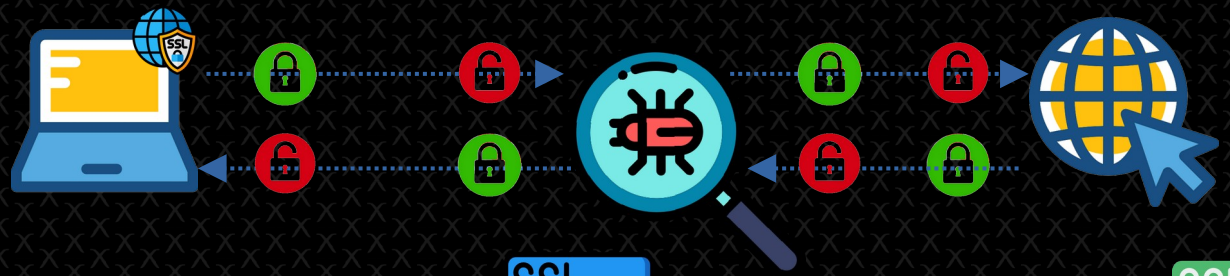
Trafico cifrado descifrado



Rotura de cifrado en DPI

SSL/TLS Interception

Trafico cifrado con inspección TLS



Subject: **feliz1984.com**
Issur: **compañía CA**

Subject: **feliz1984.com**
Issur: **Oficial CA**

Usos legítimos

Usos legítimos

Calidad de servicio (QoS)
Modelado de tráfico
Requisitos regulatorios

Usos legítimos

Publicidad personalizada
Diferenciación de servicios
Análisis de subscriptores

Calidad de servicio (QoS)
Modelado de tráfico
Requisitos regulatorios

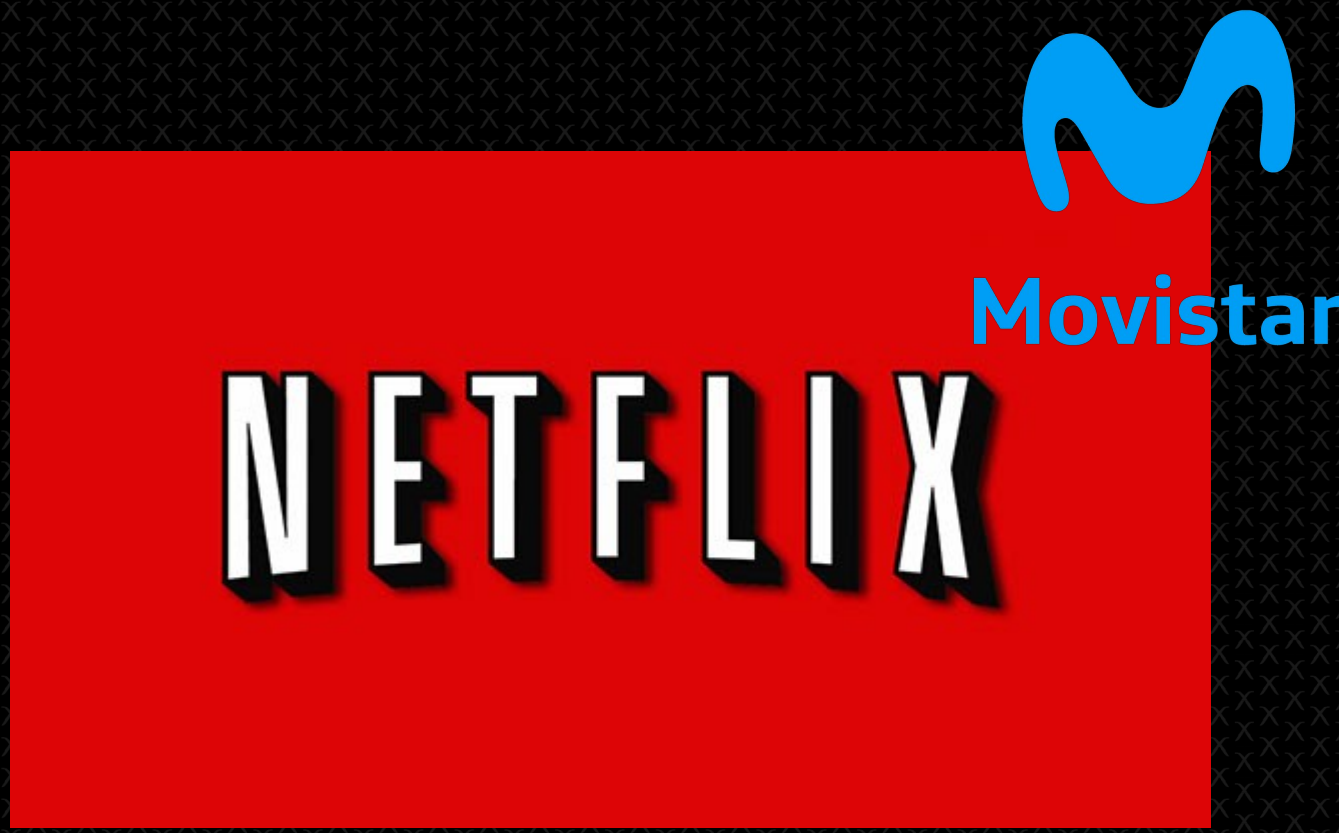
Usos legítimos

Publicidad personalizada
Diferenciación de servicios
Análisis de subscriptores

Calidad de servicio (QoS)
Modelado de tráfico
Requisitos regulatorios

En el lado del mal

Violación de la privacidad

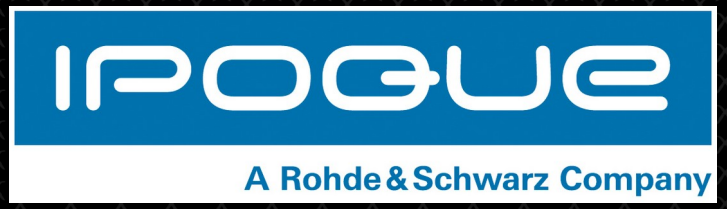


Movistar

En el lado del mal

Violación de la privacidad

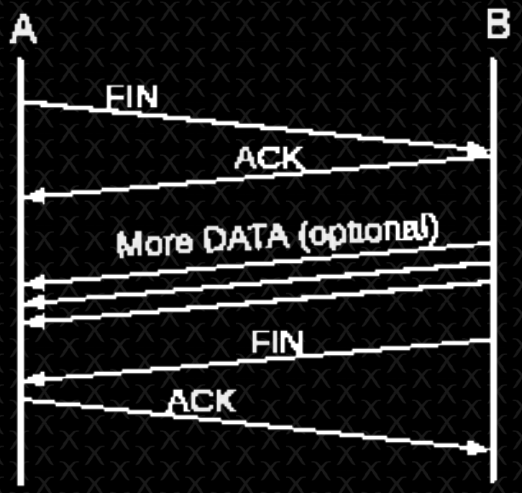
Herramientas con DPI



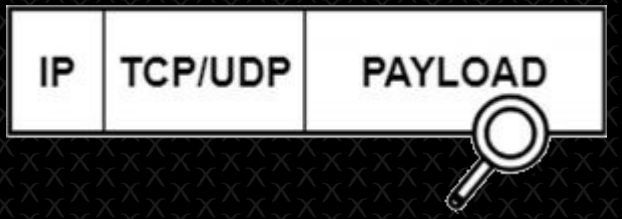
Técnicas sin cifrado

- **Inspección Basada en Metadatos**
- Identificación de Protocolos basada en Heurísticas
- Fingerprinting de Aplicaciones
- **Análisis de Comportamiento**
- Análisis de Certificados de Seguridad

Técnicas con cifrado



- Inspección de Payload
- Reensamblado de flujos
- **Decodificación de Protocolos Personalizados**



Técnicas específicas

Inspección de Tráfico:
→ **Mensajería Instantánea**
→ **Peer-to-Peer**
→ **Cloud**
→ **Vídeo (Multicast)**
→ **VoIP**
→ **DNS**

Detección de **Tunneling** encapsulado

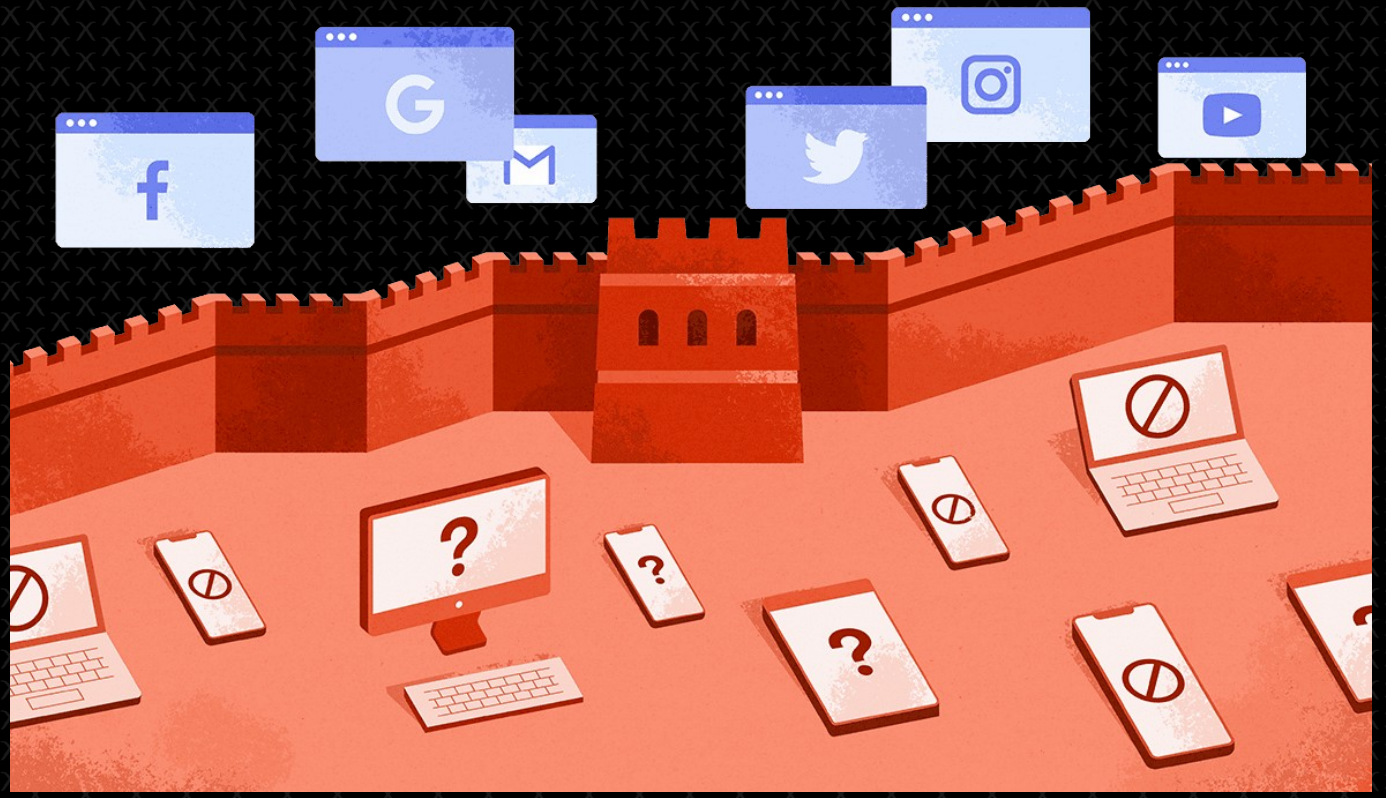
Censura

Importancia de la censura

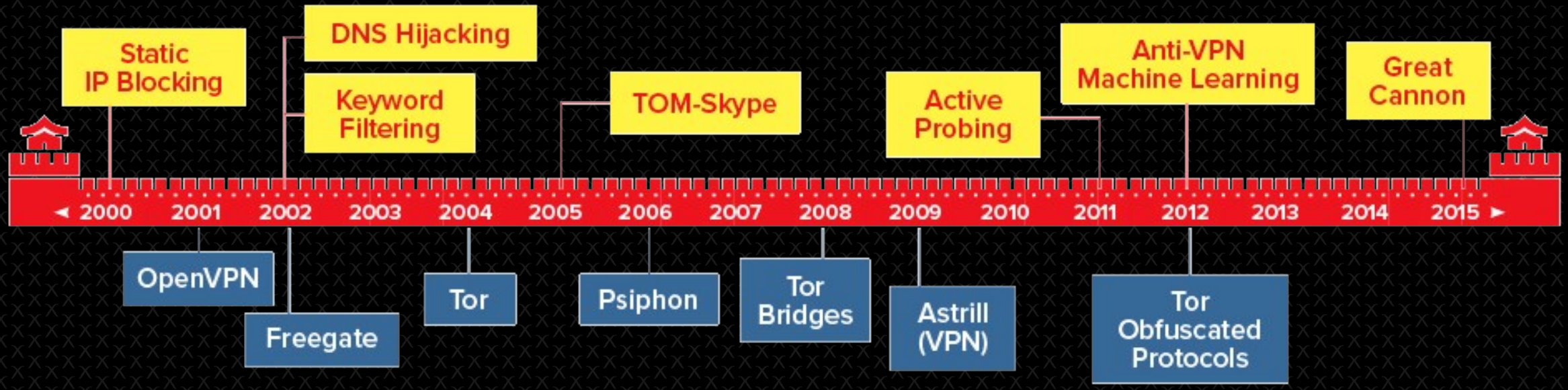
RFC 9505

Great Firewall (GFW)

金盾工程 (Proyecto Escudo Dorado)

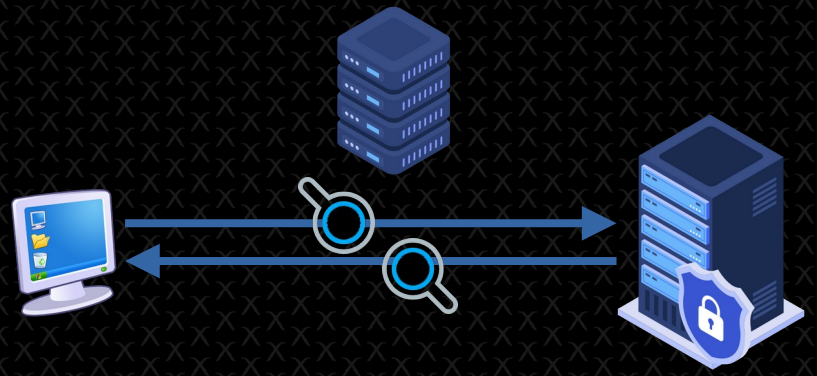


Great Firewall (GFW)

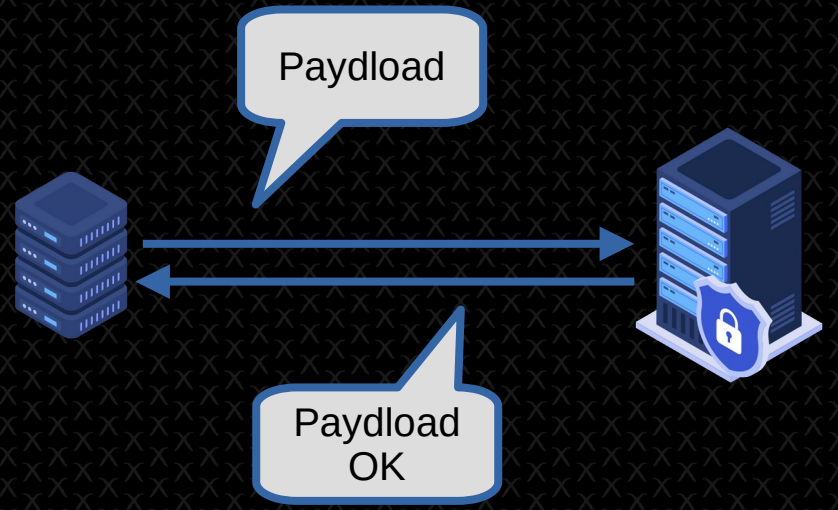


Evolución bloqueo

Inspección pasiva no intrusiva



Sondeo activo



Inspección pasiva tráfico cifrado

5 conjuntos de heurísticas rudimentarias

Exención de entropía <50% de 1

Exención de caracteres ASCII imprimibles 0x20–0x7e

- ◇ Los primeros 6 bytes son imprimibles
- ◇ Más de la mitad de los bytes son imprimibles
- ◇ Contiene más de 20 bytes imprimibles contiguos

Exención de Protocolos Comunes

- ◇ HTTP
- ◇ TLS

Inspección pasiva tráfico cifrado

5 conjuntos de heurísticas rudimentarias

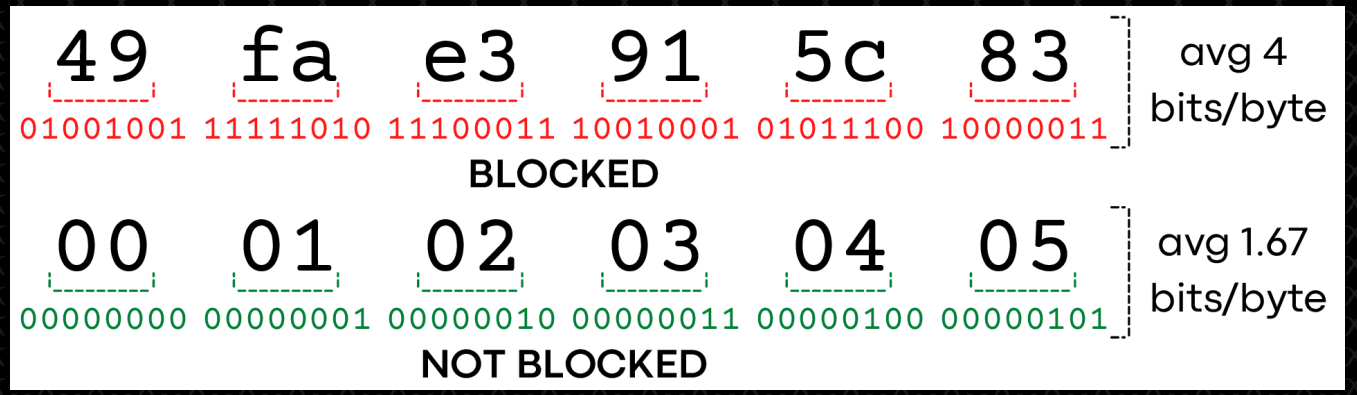
Exención de entropía <50% de 1

Exención de caracteres ASCII imprimibles 0x20–0x7e

- Los primeros 6 bytes son imprimibles
- Más de la mitad de los bytes son imprimibles
- Contiene más de 20 bytes imprimibles contiguos

Exención de Protocolos Comunes

- HTTP
- TLS



Inspección pasiva tráfico cifrado

5 conjuntos de heurísticas rudimentarias

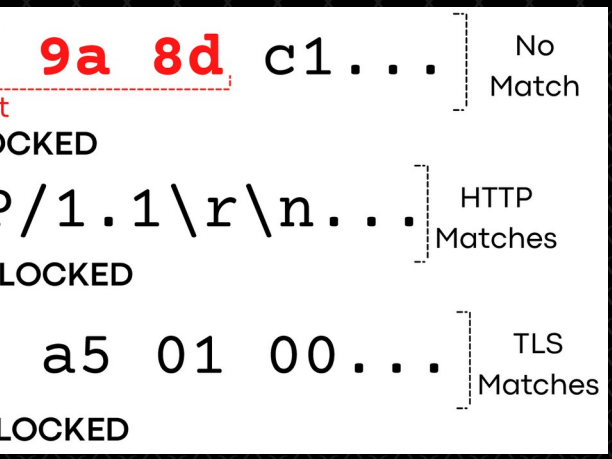
Exención de entropía <50% de 1

Exención de caracteres ASCII imprimibles 0x20–0x7e

- ◇ Los primeros 6 bytes son imprimibles
- ◇ Más de la mitad de los bytes son imprimibles
- ◇ Contiene más de 20 bytes imprimibles contiguos

Exención de Protocolos Comunes

- ◇ HTTP
- ◇ TLS



Inspección pasiva tráfico cifrado

5 conjuntos de heurísticas rudimentarias

Exención de entropía <50% de 1

Exención de caracteres ASCII imprimibles 0x20–0x7e

- Los primeros 6 bytes son imprimibles
- Más de la mitad de los bytes son imprimibles
- Contiene más de 20 bytes imprimibles contiguos

Exención de Protocolos Comunes

- HTTP
- TLS

Inspección pasiva tráfico cifrado

5 conjuntos de heurísticas rudimentarias

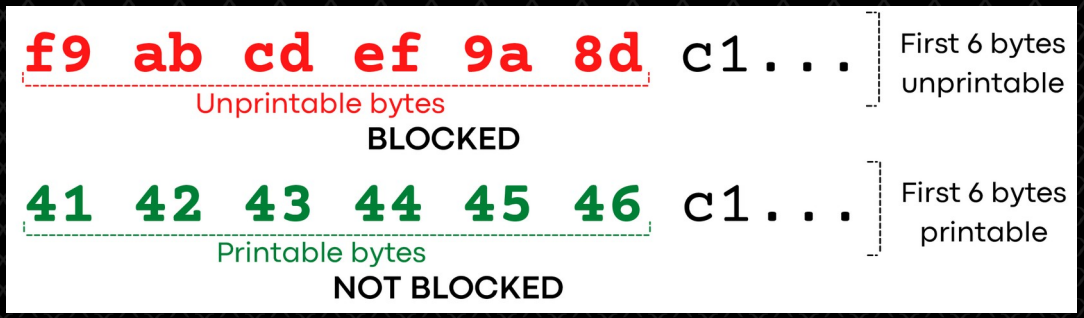
Exención de entropía <50% de 1

Exención de caracteres ASCII imprimibles 0x20–0x7e

- ◇ Los primeros 6 bytes son imprimibles
- ◇ Más de la mitad de los bytes son imprimibles
- ◇ Contiene más de 20 bytes imprimibles contiguos

Exención de Protocolos Comunes

- ◇ HTTP
- ◇ TLS



Ataque de sondeo activo

Cargas útiles contra servidor **2011**

2012 Conjunto cifrado TLS

Sondeos contra protocolos **2015**

2019 Detección de ShadowSocks

Detecciones masivas **2021**

Ataque de sondeo activo

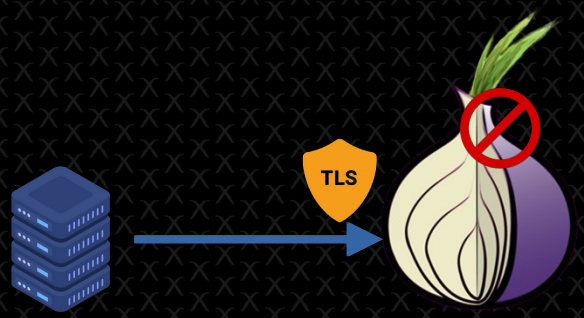
Cargas útiles contra servidor **2011**

2012 Conjunto cifrado TLS

Sondeos contra protocolos **2015**

2019 Detección de ShadowSocks

Detecciones masivas **2021**



Ataque de sondeo activo

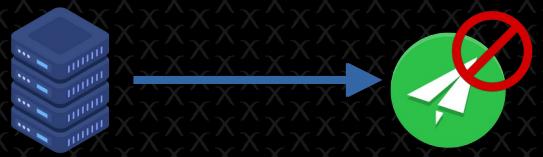
Cargas útiles contra servidor **2011**

2012 Conjunto cifrado TLS

Sondeos contra protocolos **2015**

2019 Detección de ShadowSocks

Detecciones masivas **2021**



Ataque de sondeo activo

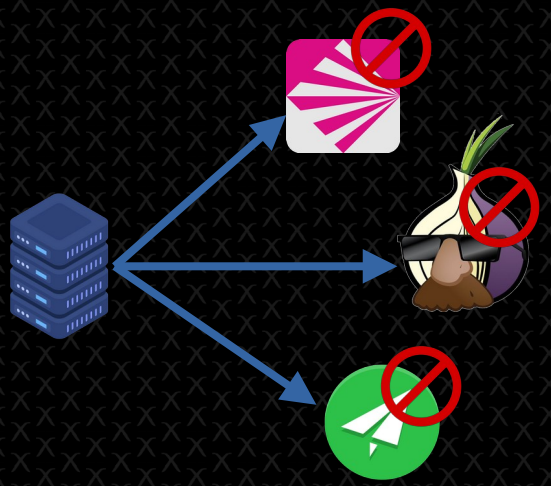
Cargas útiles contra servidor **2011**

2012 Conjunto cifrado TLS

Sondeos contra protocolos **2015**

2019 Detección de ShadowSocks

Detecciones masivas **2021**



Sondeo activo
Ataque y defensa

- TTL de los cortes
- Peticiones SNI

- Lectura infinita
- Fronting de app

Sondeo activo
Ataque y defensa

- TTL de los cortes
- Peticiones SNI

- Lectura infinita
- Fronting de app



Bloqueo

Probabilístico 26%

Estratégico No Cloud populares

Tupla de 3 durante 180 seg

Sin censura residual fijo

Daño colateral 0,6%

Bloqueo

Solo descarta cliente servidor
UDP no se ve afectado
El número de puerto no tiene valor

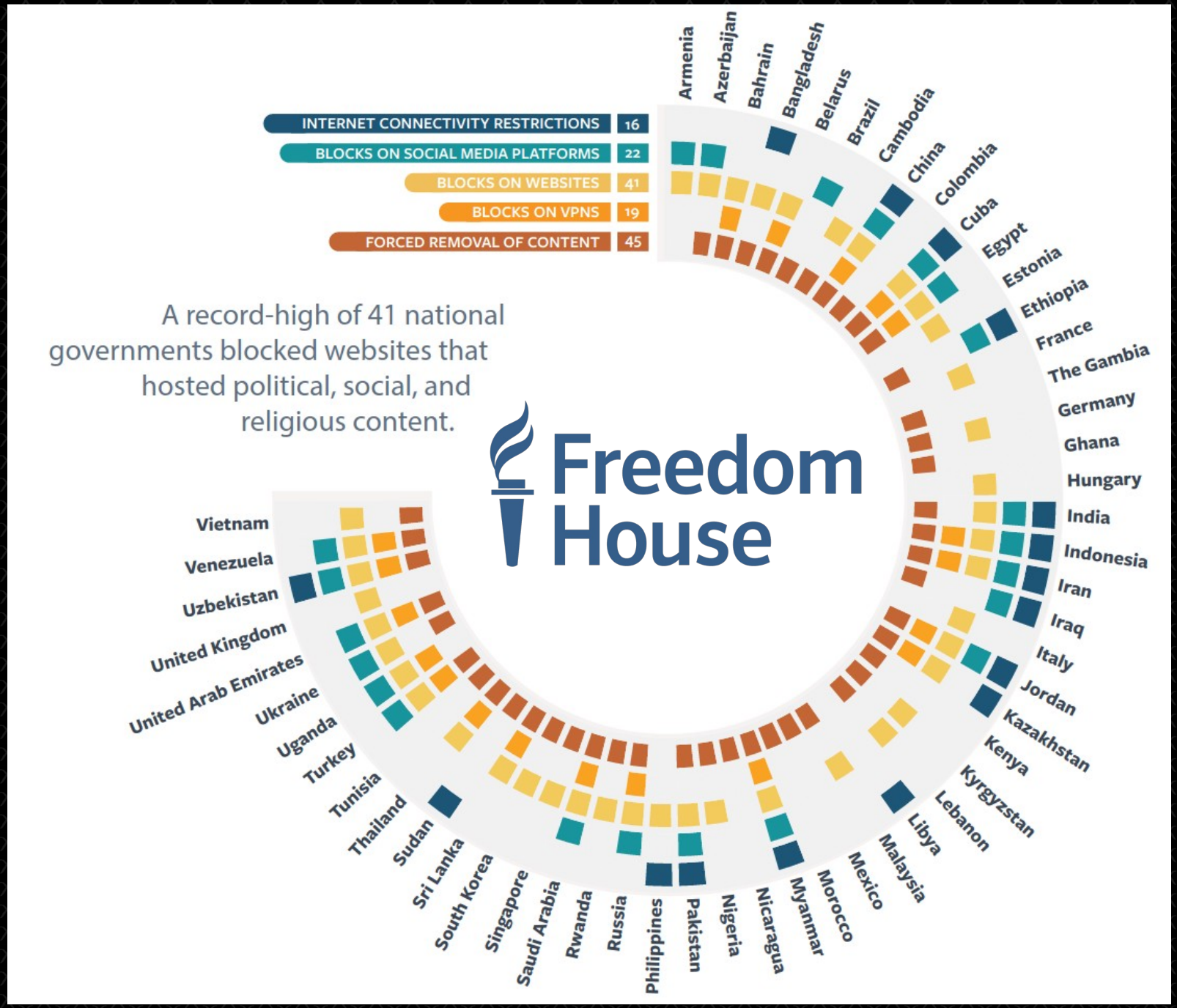
Esquivar bloqueos

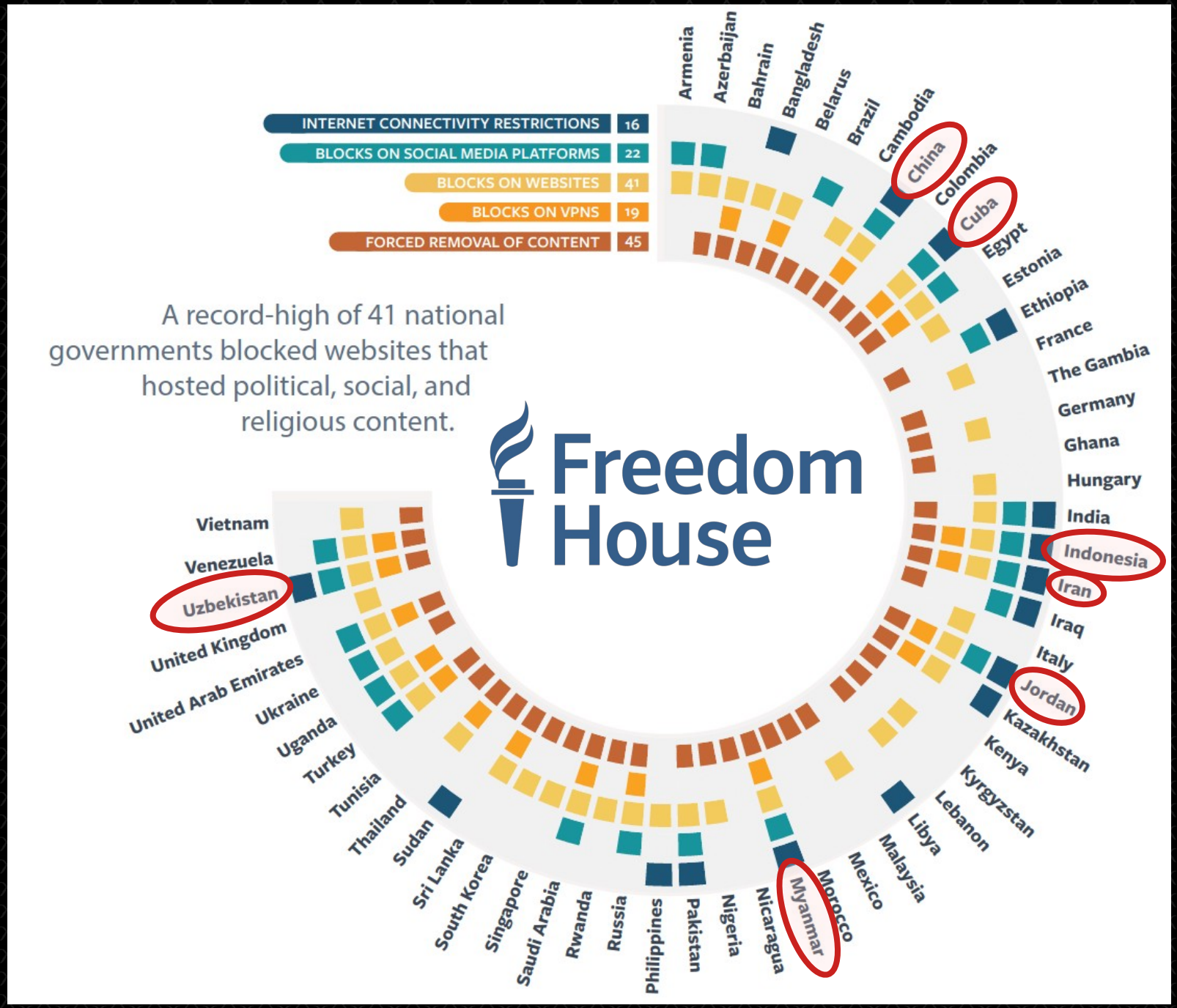
Aprovecharnos del gestión de recursos

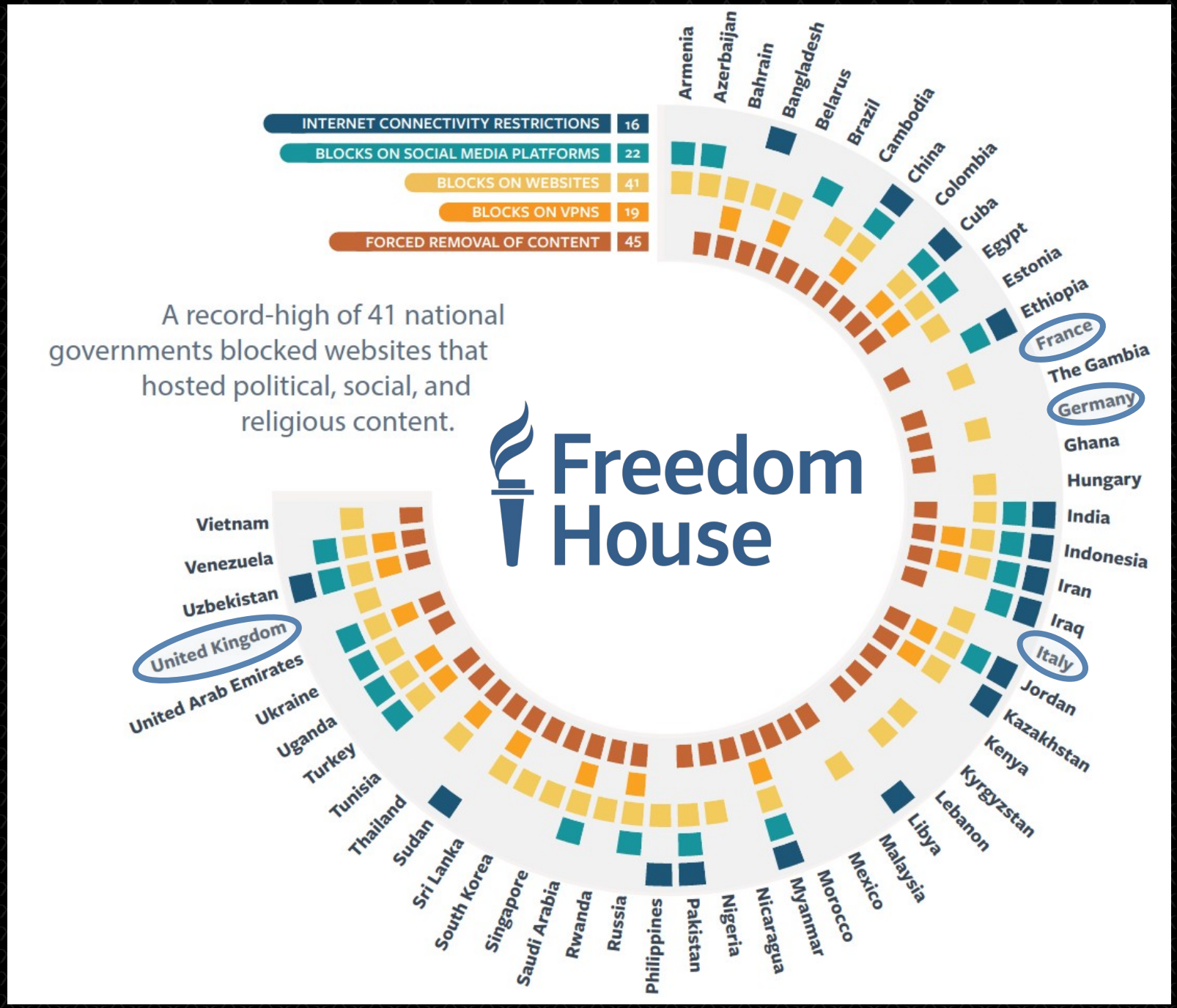
→ Modificación del prefijo de los paquetes

→ Alteración de la entropía

No solo censuran los "malos"


INTERNET CONNECTIVITY RESTRICTIONS 16
BLOCKS ON SOCIAL MEDIA PLATFORMS 22
BLOCKS ON WEBSITES 41
BLOCKS ON VPNS 19
FORCED REMOVAL OF CONTENT 45
A record-high of 41 national governments blocked websites that hosted political, social, and religious content.
Freedom House
Armenia
Azerbaijan
Bahrain
Bangladesh
Belarus
Brazil
Cambodia
China
Colombia
Cuba
Egypt
Estonia
Ethiopia
France
The Gambia
Germany
Ghana
Hungary
India
Indonesia
Iran
Iraq
Italy
Jordan
Kazakhstan
Kenya
Kyrgyzstan
Lebanon
Libya
Malaysia
Mexico
Morocco
Myanmar
Nicaragua
Nigeria
Pakistan
Philippines
Russia
Rwanda
Saudi Arabia
Singapore
South Korea
Sri Lanka
Sudan
Thailand
Tunisia
Turkey
Uganda
Ukraine
United Arab Emirates
United Kingdom
Uzbekistan
Venezuela
Vietnam


INTERNET CONNECTIVITY RESTRICTIONS 16
BLOCKS ON SOCIAL MEDIA PLATFORMS 22
BLOCKS ON WEBSITES 41
BLOCKS ON VPNS 19
FORCED REMOVAL OF CONTENT 45
A record-high of 41 national governments blocked websites that hosted political, social, and religious content.
Freedom House
Armenia
Azerbaijan
Bahrain
Bangladesh
Belarus
Brazil
Cambodia
China
Colombia
Cuba
Egypt
Estonia
Ethiopia
France
The Gambia
Germany
Ghana
Hungary
India
Indonesia
Iran
Iraq
Italy
Jordan
Kazakhstan
Kenya
Kyrgyzstan
Lebanon
Libya
Malaysia
Mexico
Morocco
Myanmar
Nicaragua
Nigeria
Pakistan
Philippines
Russia
Rwanda
Saudi Arabia
Singapore
South Korea
Sri Lanka
Sudan
Thailand
Tunisia
Turkey
Uganda
Ukraine
United Arab Emirates
United Kingdom
Uzbekistan
Venezuela
Vietnam


INTERNET CONNECTIVITY RESTRICTIONS 16
BLOCKS ON SOCIAL MEDIA PLATFORMS 22
BLOCKS ON WEBSITES 41
BLOCKS ON VPNS 19
FORCED REMOVAL OF CONTENT 45
A record-high of 41 national governments blocked websites that hosted political, social, and religious content.
Freedom House
Armenia
Azerbaijan
Bahrain
Bangladesh
Belarus
Brazil
Cambodia
China
Colombia
Cuba
Egypt
Estonia
Ethiopia
France
The Gambia
Germany
Ghana
Hungary
India
Indonesia
Iran
Iraq
Italy
Jordan
Kazakhstan
Kenya
Kyrgyzstan
Lebanon
Libya
Malaysia
Mexico
Morocco
Myanmar
Nicaragua
Nigeria
Pakistan
Philippines
Russia
Rwanda
Saudi Arabia
Singapore
South Korea
Sri Lanka
Sudan
Thailand
Tunisia
Turkey
Uganda
Ukraine
United Arab Emirates
United Kingdom
Uzbekistan
Venezuela
Vietnam

No solo censuran los "malos"

Interceptación legal (LI)

Investigatory Powers Act

Telecommunications (Interception and Access) Act

Ley de Interceptación de Comunicaciones

Loi relative au renseignement

Indian Telegraph Act y IT Act

SORM

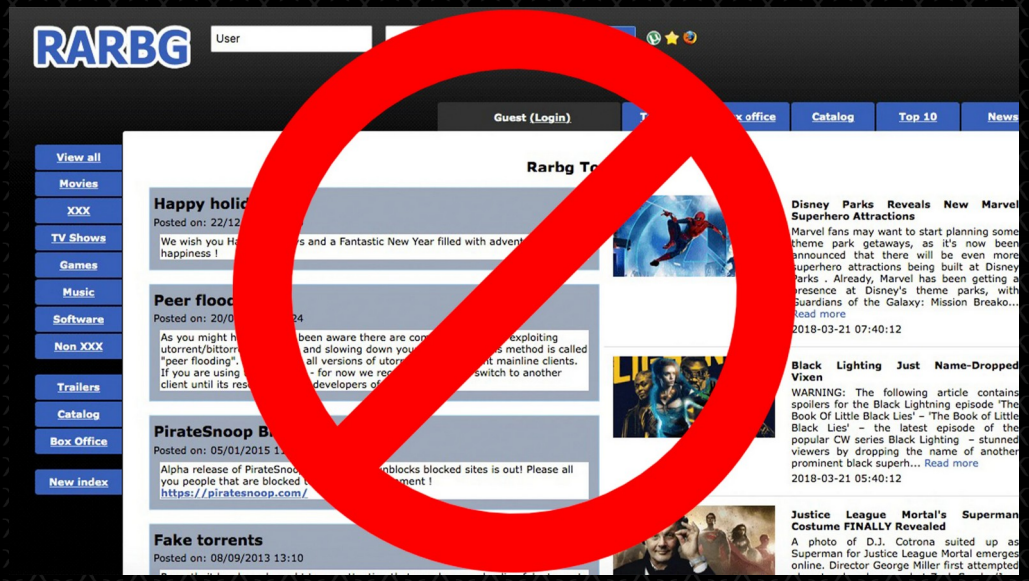
G10 Gesetz

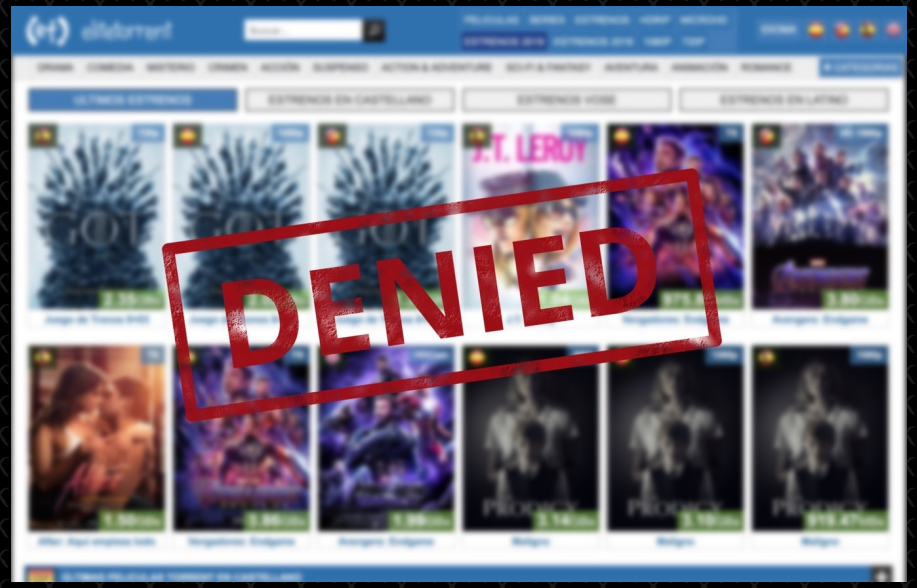
BÜPF

CALEA

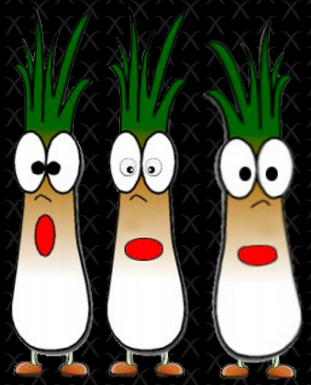
MITA

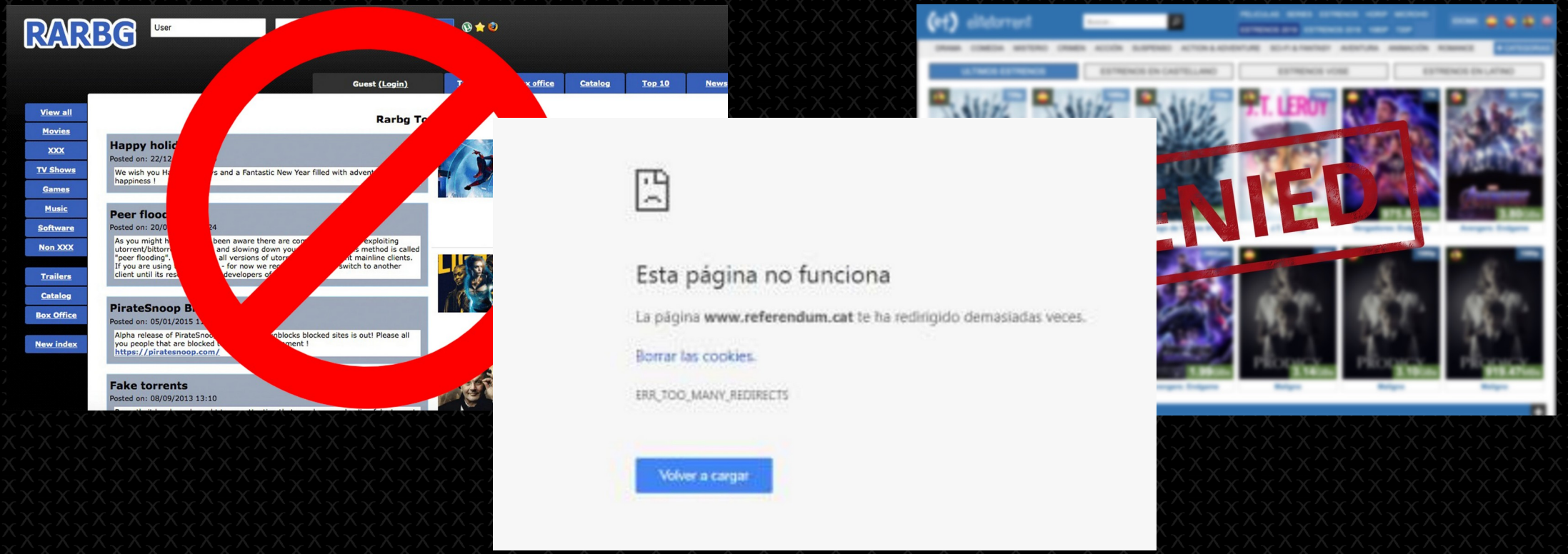
Otras censuras



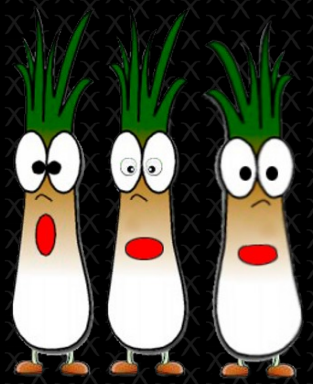


Otras censuras

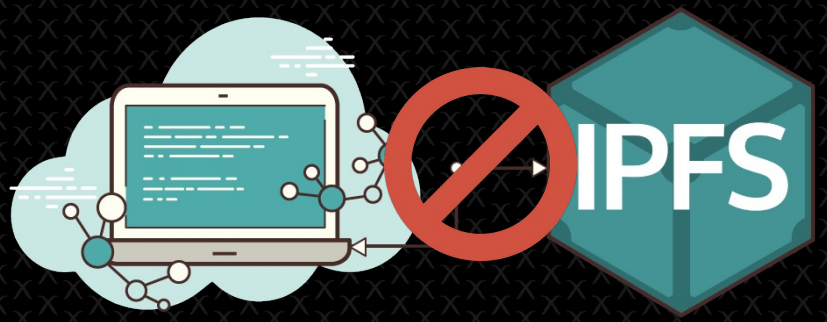




Censura en Cataluña



onvotar.garantiespelreferendum.com
www.referendum.fun

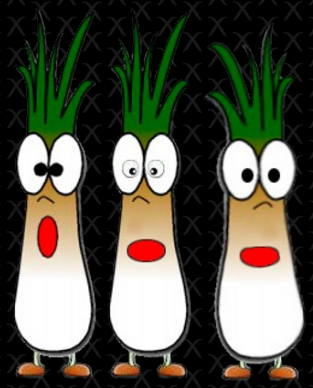


Bloqueo de las solicitudes HTTP
Bloqueo de las solicitudes HTTPS

https://gateway.ipfs.io/ipns/qmzxwebjbvkgdgakdypquxx4kc5tcwbvur4iyzrtml8xcr/#1Oct"

Censura en Cataluña

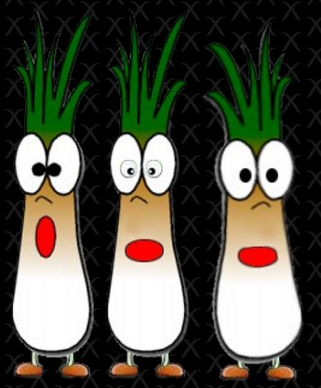
HTTP



No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	46682 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850521864 TSecr=0 WS=128
2	0.054014	147.135.130.181	192.168.1.121	TCP	53	76	80 → 46682 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251601665 TSecr=1850521864 WS=128
3	0.054066	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850521877 TSecr=1251601665
4	0.054205	192.168.1.121	147.135.130.181	HTTP	64	145	GET / HTTP/1.1
5	0.068480	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ZeroWindow] 80 → 46682 [ACK] Seq=1 Ack=80 Win=0 Len=0
6	0.069180	147.135.130.181	192.168.1.121	TCP	249	1506	[TCP segment of a reassembled PDU]
7	0.069214	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1453 Win=32128 Len=0 TSval=1850521881 TSecr=1251601665
8	0.069239	147.135.130.181	192.168.1.121	HTTP	249	221	HTTP/1.1 403 Forbidden (text/html)
9	0.069247	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
10	0.069829	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [FIN, ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
11	0.083563	147.135.130.181	192.168.1.121	TCP	249	56	80 → 46682 [FIN, ACK] Seq=1620 Ack=80 Win=128 Len=0
12	0.083596	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=81 Ack=1621 Win=35072 Len=0 TSval=1850521885 TSecr=1251601665
13	0.123655	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1453 Win=0 Len=0
14	0.123670	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
15	0.123671	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
16	0.123672	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1621 Win=0 Len=0

Censura en Cataluña

HTTP

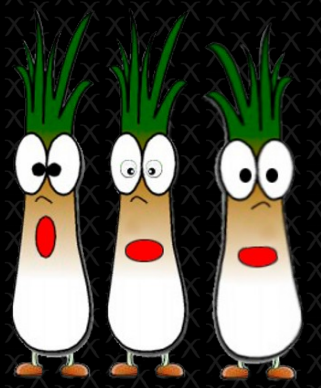


1 192.168.1.121 147.135.130.181 TCP 64

No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	46682 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850521864 TSecr=0 WS=128
2	0.054014	147.135.130.181	192.168.1.121	TCP	53	76	80 → 46682 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251601665 TSecr=1850521864 WS=128
3	0.054066	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850521877 TSecr=1251601665
4	0.054205	192.168.1.121	147.135.130.181	HTTP	64	145	GET / HTTP/1.1
5	0.068480	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ZeroWindow] 80 → 46682 [ACK] Seq=1 Ack=80 Win=0 Len=0
6	0.069180	147.135.130.181	192.168.1.121	TCP	249	1506	[TCP segment of a reassembled PDU]
7	0.069214	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1453 Win=32128 Len=0 TSval=1850521881 TSecr=1251601665
8	0.069239	147.135.130.181	192.168.1.121	HTTP	249	221	HTTP/1.1 403 Forbidden (text/html)
9	0.069247	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
10	0.069829	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [FIN, ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
11	0.083563	147.135.130.181	192.168.1.121	TCP	249	56	80 → 46682 [FIN, ACK] Seq=1620 Ack=80 Win=128 Len=0
12	0.083596	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=81 Ack=1621 Win=35072 Len=0 TSval=1850521885 TSecr=1251601665
13	0.123655	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1453 Win=0 Len=0
14	0.123670	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
15	0.123671	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
16	0.123672	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1621 Win=0 Len=0

Censura en Cataluña

HTTP

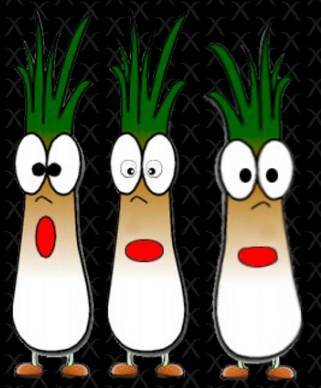


2 147.135.130.181 192.168.1.121 TCP 53

No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	46682 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850521864 TSecr=0 WS=128
2	0.054014	147.135.130.181	192.168.1.121	TCP	53	76	80 → 46682 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251601665 TSecr=1850521864 WS=128
3	0.054066	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850521877 TSecr=1251601665
4	0.054205	192.168.1.121	147.135.130.181	HTTP	64	145	GET / HTTP/1.1
5	0.068480	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ZeroWindow] 80 → 46682 [ACK] Seq=1 Ack=80 Win=0 Len=0
6	0.069180	147.135.130.181	192.168.1.121	TCP	249	1506	[TCP segment of a reassembled PDU]
7	0.069214	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1453 Win=32128 Len=0 TSval=1850521881 TSecr=1251601665
8	0.069239	147.135.130.181	192.168.1.121	HTTP	249	221	HTTP/1.1 403 Forbidden (text/html)
9	0.069247	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
10	0.069829	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [FIN, ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
11	0.083563	147.135.130.181	192.168.1.121	TCP	249	56	80 → 46682 [FIN, ACK] Seq=1620 Ack=80 Win=128 Len=0
12	0.083596	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=81 Ack=1621 Win=35072 Len=0 TSval=1850521885 TSecr=1251601665
13	0.123655	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1453 Win=0 Len=0
14	0.123670	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
15	0.123671	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
16	0.123672	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1621 Win=0 Len=0

Censura en Cataluña

HTTP

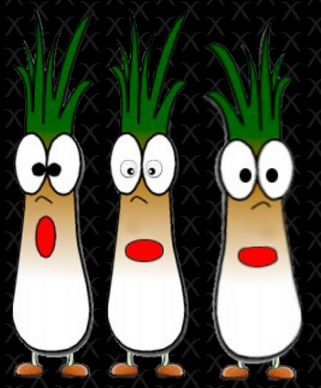


5 147.135.130.181 192.168.1.121 TCP 249

No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	46682 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850521864 TSecr=0 WS=128
2	0.054014	147.135.130.181	192.168.1.121	TCP	53	76	80 → 46682 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251601665 TSecr=1850521864 WS=128
3	0.054066	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850521877 TSecr=1251601665
4	0.054205	192.168.1.121	147.135.130.181	HTTP	64	145	GET / HTTP/1.1
5	0.068480	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ZeroWindow] 80 → 46682 [ACK] Seq=1 Ack=80 Win=0 Len=0
6	0.069180	147.135.130.181	192.168.1.121	TCP	249	1506	[TCP segment of a reassembled PDU]
7	0.069214	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1453 Win=32128 Len=0 TSval=1850521881 TSecr=1251601665
8	0.069239	147.135.130.181	192.168.1.121	HTTP	249	221	HTTP/1.1 403 Forbidden (text/html)
9	0.069247	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
10	0.069829	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [FIN, ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
11	0.083563	147.135.130.181	192.168.1.121	TCP	249	56	80 → 46682 [FIN, ACK] Seq=1620 Ack=80 Win=128 Len=0
12	0.083596	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=81 Ack=1621 Win=35072 Len=0 TSval=1850521885 TSecr=1251601665
13	0.123655	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1453 Win=0 Len=0
14	0.123670	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
15	0.123671	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
16	0.123672	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1621 Win=0 Len=0

Censura en Cataluña

HTTP



8 147.135.130.181 192.168.1.121 HTTP 249 221 HTTP/1.1 403

No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	46682 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850521864 TSecr=0 WS=128
2	0.054014	147.135.130.181	192.168.1.121	TCP	53	76	80 → 46682 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251601665 TSecr=1850521864 WS=128
3	0.054066	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850521877 TSecr=1251601665
4	0.054205	192.168.1.121	147.135.130.181	HTTP	64	145	GET / HTTP/1.1
5	0.068480	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ZeroWindow] 80 → 46682 [ACK] Seq=1 Ack=80 Win=0 Len=0
6	0.069180	147.135.130.181	192.168.1.121	TCP	249	1506	[TCP segment of a reassembled PDU]
7	0.069214	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1453 Win=32128 Len=0 TSval=1850521881 TSecr=1251601665
8	0.069239	147.135.130.181	192.168.1.121	HTTP	249	221	HTTP/1.1 403 Forbidden (text/html)
9	0.069247	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
10	0.069829	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [FIN, ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
11	0.083563	147.135.130.181	192.168.1.121	TCP	249	56	80 → 46682 [FIN, ACK] Seq=1620 Ack=80 Win=128 Len=0
12	0.083596	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=81 Ack=1621 Win=35072 Len=0 TSval=1850521885 TSecr=1251601665
13	0.123655	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1453 Win=0 Len=0
14	0.123670	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
15	0.123671	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
16	0.123672	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1621 Win=0 Len=0

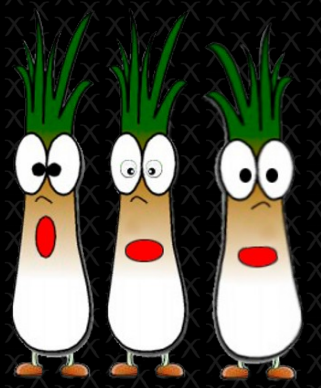
Censura en Cataluña

HTTP

11	147.135.130.181	192.168.1.121	TCP	249	FIN, ACK
12	192.168.1.121	147.135.130.181	TCP	64	ACK
13	147.135.130.181	192.168.1.121	TCP	53	RST

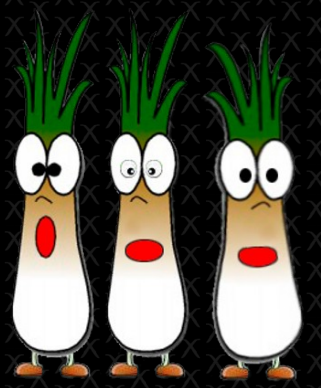
No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	46682 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850521864 TSecr=0 WS=128
2	0.054014	147.135.130.181	192.168.1.121	TCP	53	76	80 → 46682 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251601665 TSecr=1850521864 WS=128
3	0.054066	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850521877 TSecr=1251601665
4	0.054205	192.168.1.121	147.135.130.181	HTTP	64	145	GET / HTTP/1.1
5	0.068480	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ZeroWindow] 80 → 46682 [ACK] Seq=1 Ack=80 Win=0 Len=0
6	0.069180	147.135.130.181	192.168.1.121	TCP	249	1506	[TCP segment of a reassembled PDU]
7	0.069214	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1453 Win=32128 Len=0 TSval=1850521881 TSecr=1251601665
8	0.069239	147.135.130.181	192.168.1.121	HTTP	249	221	HTTP/1.1 403 Forbidden (text/html)
9	0.069247	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
10	0.069829	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [FIN, ACK] Seq=80 Ack=1620 Win=35072 Len=0 TSval=1850521881 TSecr=1251601665
11	0.083563	147.135.130.181	192.168.1.121	TCP	249	56	80 → 46682 [FIN, ACK] Seq=1620 Ack=80 Win=128 Len=0
12	0.083596	192.168.1.121	147.135.130.181	TCP	64	66	46682 → 80 [ACK] Seq=81 Ack=1621 Win=35072 Len=0 TSval=1850521885 TSecr=1251601665
13	0.123655	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1453 Win=0 Len=0
14	0.123670	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
15	0.123671	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1620 Win=0 Len=0
16	0.123672	147.135.130.181	192.168.1.121	TCP	53	56	80 → 46682 [RST] Seq=1621 Win=0 Len=0

Censura en Cataluña



```
HTTP/1.1 403 Forbidden
Content-Type: text/html; charset="utf-8"
Content-Length: 1510
Connection: Close

<!DOCTYPE html PUBLIC \"-//W3C//DTD HTML 4.01//EN\">
<html>
  <head>
    <meta charset="utf-8"/>
    <title>
      PHISHING_TSOL_MENSAJE_1
    </title>

  </head>
  <body>
    <CENTER>
      <h1 id="causa" name="PHISHING_TSOL_MENSAJE_1">
      </h1>
      <script type="text/javascript">
        var name = document.getElementById("causa").getAttribute('name')
            var text = ""
                switch (name) {
                  case 'PHISHING_TSOL_MENSAJE_1":
                    text = "Judicial_Guardia_Civil"
                      window.location.replace("http://paginaintervenida.edgesuite.net");
                    break;
                  case 'Administrativo_Ley_del_Juego":
                    text = "Administrativo_Ley_del_Juego"
                      window.location.replace("http://195.235.52.40");
                    break;
                  case 'Judicial_Guardia_Civil":
                    text = "Judicial_Guardia_Civil"
                      window.location.replace("http://paginaintervenida.edgesuite.net");
                    break;
                  case 'Judicial_Policia_Nacional":
                    text = "Judicial_Policia_Nacional"
                      window.location.replace("http://webbloqueadaporpolicianacional.com");
                    break;
                  default:
                    text = "ERROR 404 - File url1 not found";
                }
        document.getElementById("causa").innerHTML = text
      </script>
    </CENTER>
  </body>
</html>
```

Censura en Cataluña

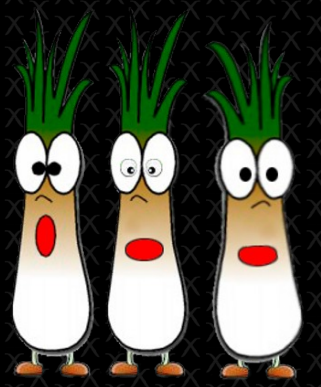


```
HTTP/1.1 403 Forbidden
Content-Type: text/html; charset="utf-8"
Content-Length: 1510
Connection: Close

<!DOCTYPE html PUBLIC \"-//W3C//DTD HTML 4.01//EN\">
<html>
  <head>
    <meta charset="utf-8"/>
    <title>
      PHISHING_TSOL_MENSAJE_1
    </title>

  </head>
  <body>
    <CENTER>
      <h1 id="causa" name="PHISHING_TSOL_MENSAJE_1">

yId("causa").getAttribute('name')

ENSAJE_1":
ardia_Civil"
eplace("http://paginaintervenida.edgesuite.net");

Ley_del_Juego":
ivo_Ley_del_Juego"
eplace("http://195.235.52.40");

a_Civil":
ardia_Civil"
eplace("http://paginaintervenida.edgesuite.net");

a_Nacional":
licia_Nacional"
eplace("http://webbloqueadaporpolicianacional.com");

 File url1 not found";

).innerHTML = text

    </CENTER>
  </body>
</html>
```

Este dominio ha sido intervenido y se encuentra a disposición de la Autoridad Judicial

This domain name has been seized pursuant to a seizure warrant under the Judicial Authority and is under its administration

Censura en Cataluña



```
HTTP/1.1 403 Forbidden
Content-Type: text/html; charset="utf-8"
Content-Length: 1510
Connection: Close

<!DOCTYPE html PUBLIC \"-//W3C//DTD HTML 4.01//EN\">
<html>
  <head>
    <meta charset="utf-8"/>
    <title>
      PHISHING_TSOL_MENSAJE_1
    </title>

  </head>
  <body>
    <CENTER>
      <h1 id="causa" name="PHISHING_TSOL_MENSAJE_1">
```

Este dominio ha sido intervenido y se encuentra a disposición de la Autoridad Judicial

This domain name has been seized pursuant to a seizure warrant under the Judicial Authority and is under its administration

GOBIERNO DE ESPAÑA

DOMINIO INTERVENIDO POR ORDEN JUDICIAL

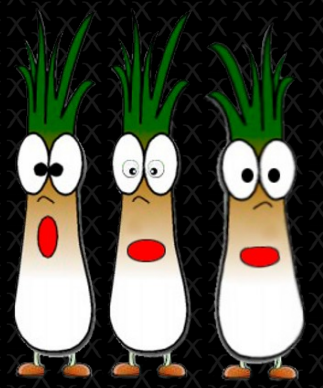
POLICIA NACIONAL DE ESPAÑA

THIS DOMAIN NAME HAS BEEN SEIZED PURSUANT TO A JUDICIAL WARRANT

SPANISH NATIONAL POLICE

Censura en Cataluña

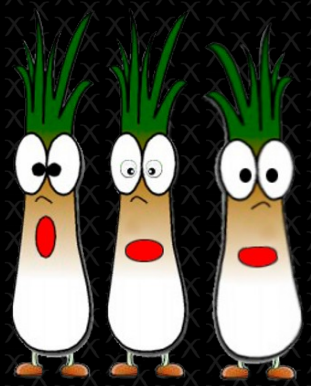
HTTPS



No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	34988 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850466514 TSecr=0 WS=128
2	0.000355	192.168.1.121	147.135.130.181	TCP	64	74	34990 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850466514 TSecr=0 WS=128
3	0.052211	147.135.130.181	192.168.1.121	TCP	52	76	443 → 34988 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251546316 TSecr=1850466514 WS=128
4	0.052257	192.168.1.121	147.135.130.181	TCP	64	66	34988 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850466527 TSecr=1251546316
5	0.052275	147.135.130.181	192.168.1.121	TCP	52	76	443 → 34990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251546316 TSecr=1850466514 WS=128
6	0.052282	192.168.1.121	147.135.130.181	TCP	64	66	34990 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850466527 TSecr=1251546316
7	0.052543	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
8	0.052663	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
9	0.082159	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34988 [RST, ACK] Seq=1 Ack=105204425 Win=0 Len=0
10	0.082190	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34990 [RST, ACK] Seq=1 Ack=1430621405 Win=0 Len=0
11	3.168047	192.168.1.121	147.135.130.181	TCP	64	74	34992 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850467306 TSecr=0 WS=128
12	3.168182	192.168.1.121	147.135.130.181	TCP	64	74	34994 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850467306 TSecr=0 WS=128
13	3.222239	147.135.130.181	192.168.1.121	TCP	53	76	443 → 34992 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251547108 TSecr=1850467306 WS=128
14	3.222290	192.168.1.121	147.135.130.181	TCP	64	66	34992 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850467319 TSecr=1251547108
15	3.222312	147.135.130.181	192.168.1.121	TCP	53	76	443 → 34994 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251547108 TSecr=1850467306 WS=128
16	3.222325	192.168.1.121	147.135.130.181	TCP	64	66	34994 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850467319 TSecr=1251547108
17	3.222504	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
18	3.222600	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
19	3.252269	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34992 [RST, ACK] Seq=1 Ack=1120449859 Win=0 Len=0
20	3.252297	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34994 [RST, ACK] Seq=1 Ack=537856325 Win=0 Len=0

Censura en Cataluña

HTTPS

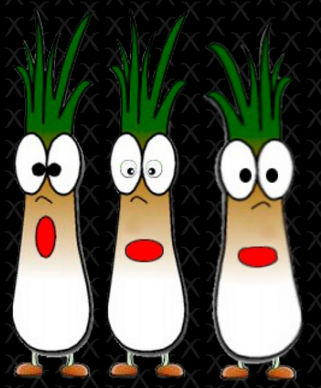


1 192.168.1.121 147.135.130.181 TCP 64

No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	34988 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850466514 TSecr=0 WS=128
2	0.000355	192.168.1.121	147.135.130.181	TCP	64	74	34990 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850466514 TSecr=0 WS=128
3	0.052211	147.135.130.181	192.168.1.121	TCP	52	76	443 → 34988 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251546316 TSecr=1850466514 WS=128
4	0.052257	192.168.1.121	147.135.130.181	TCP	64	66	34988 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850466527 TSecr=1251546316
5	0.052275	147.135.130.181	192.168.1.121	TCP	52	76	443 → 34990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251546316 TSecr=1850466514 WS=128
6	0.052282	192.168.1.121	147.135.130.181	TCP	64	66	34990 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850466527 TSecr=1251546316
7	0.052543	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
8	0.052663	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
9	0.082159	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34988 [RST, ACK] Seq=1 Ack=105204425 Win=0 Len=0
10	0.082190	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34990 [RST, ACK] Seq=1 Ack=1430621405 Win=0 Len=0
11	3.168047	192.168.1.121	147.135.130.181	TCP	64	74	34992 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850467306 TSecr=0 WS=128
12	3.168182	192.168.1.121	147.135.130.181	TCP	64	74	34994 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850467306 TSecr=0 WS=128
13	3.222239	147.135.130.181	192.168.1.121	TCP	53	76	443 → 34992 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251547108 TSecr=1850467306 WS=128
14	3.222290	192.168.1.121	147.135.130.181	TCP	64	66	34992 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850467319 TSecr=1251547108
15	3.222312	147.135.130.181	192.168.1.121	TCP	53	76	443 → 34994 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251547108 TSecr=1850467306 WS=128
16	3.222325	192.168.1.121	147.135.130.181	TCP	64	66	34994 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850467319 TSecr=1251547108
17	3.222504	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
18	3.222600	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
19	3.252269	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34992 [RST, ACK] Seq=1 Ack=1120449859 Win=0 Len=0
20	3.252297	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34994 [RST, ACK] Seq=1 Ack=537856325 Win=0 Len=0

Censura en Cataluña

HTTPS

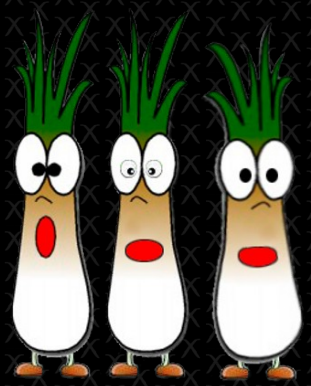


3 147.135.130.181 192.168.1.121 TCP 52

No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	34988 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850466514 TSecr=0 WS=128
2	0.000355	192.168.1.121	147.135.130.181	TCP	64	74	34990 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850466514 TSecr=0 WS=128
3	0.052211	147.135.130.181	192.168.1.121	TCP	52	76	443 → 34988 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251546316 TSecr=1850466514 WS=128
4	0.052257	192.168.1.121	147.135.130.181	TCP	64	66	34988 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850466527 TSecr=1251546316
5	0.052275	147.135.130.181	192.168.1.121	TCP	52	76	443 → 34990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251546316 TSecr=1850466514 WS=128
6	0.052282	192.168.1.121	147.135.130.181	TCP	64	66	34990 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850466527 TSecr=1251546316
7	0.052543	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
8	0.052663	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
9	0.082159	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34988 [RST, ACK] Seq=1 Ack=105204425 Win=0 Len=0
10	0.082190	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34990 [RST, ACK] Seq=1 Ack=1430621405 Win=0 Len=0
11	3.168047	192.168.1.121	147.135.130.181	TCP	64	74	34992 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850467306 TSecr=0 WS=128
12	3.168182	192.168.1.121	147.135.130.181	TCP	64	74	34994 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850467306 TSecr=0 WS=128
13	3.222239	147.135.130.181	192.168.1.121	TCP	53	76	443 → 34992 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251547108 TSecr=1850467306 WS=128
14	3.222290	192.168.1.121	147.135.130.181	TCP	64	66	34992 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850467319 TSecr=1251547108
15	3.222312	147.135.130.181	192.168.1.121	TCP	53	76	443 → 34994 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251547108 TSecr=1850467306 WS=128
16	3.222325	192.168.1.121	147.135.130.181	TCP	64	66	34994 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850467319 TSecr=1251547108
17	3.222504	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
18	3.222600	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
19	3.252269	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34992 [RST, ACK] Seq=1 Ack=1120449859 Win=0 Len=0
20	3.252297	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34994 [RST, ACK] Seq=1 Ack=537856325 Win=0 Len=0

Censura en Cataluña

HTTPS

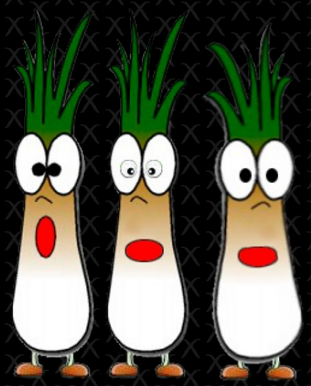


8 192.168.1.121 147.135.130.181 SSL 64 Client Hello

No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	34988 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850466514 TSecr=0 WS=128
2	0.000355	192.168.1.121	147.135.130.181	TCP	64	74	34990 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850466514 TSecr=0 WS=128
3	0.052211	147.135.130.181	192.168.1.121	TCP	52	76	443 → 34988 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251546316 TSecr=1850466514 WS=128
4	0.052257	192.168.1.121	147.135.130.181	TCP	64	66	34988 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850466527 TSecr=1251546316
5	0.052275	147.135.130.181	192.168.1.121	TCP	52	76	443 → 34990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251546316 TSecr=1850466514 WS=128
6	0.052282	192.168.1.121	147.135.130.181	TCP	64	66	34990 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850466527 TSecr=1251546316
7	0.052543	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
8	0.052663	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
9	0.082159	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34988 [RST, ACK] Seq=1 Ack=105204425 Win=0 Len=0
10	0.082190	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34990 [RST, ACK] Seq=1 Ack=1430621405 Win=0 Len=0
11	3.168047	192.168.1.121	147.135.130.181	TCP	64	74	34992 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850467306 TSecr=0 WS=128
12	3.168182	192.168.1.121	147.135.130.181	TCP	64	74	34994 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850467306 TSecr=0 WS=128
13	3.222239	147.135.130.181	192.168.1.121	TCP	53	76	443 → 34992 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251547108 TSecr=1850467306 WS=128
14	3.222290	192.168.1.121	147.135.130.181	TCP	64	66	34992 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850467319 TSecr=1251547108
15	3.222312	147.135.130.181	192.168.1.121	TCP	53	76	443 → 34994 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251547108 TSecr=1850467306 WS=128
16	3.222325	192.168.1.121	147.135.130.181	TCP	64	66	34994 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850467319 TSecr=1251547108
17	3.222504	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
18	3.222600	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
19	3.252269	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34992 [RST, ACK] Seq=1 Ack=1120449859 Win=0 Len=0
20	3.252297	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34994 [RST, ACK] Seq=1 Ack=537856325 Win=0 Len=0

Censura en Cataluña

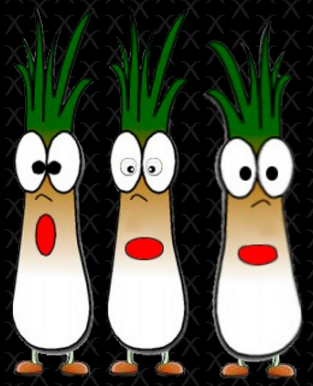
HTTPS



9	147.135.130.181	192.168.1.121	TCP	249	RST, ACK

No.	Time	Source	Destination	Protocol	ttl	Length	Info
1	0.000000	192.168.1.121	147.135.130.181	TCP	64	74	34988 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850466514 TSecr=0 WS=128
2	0.000355	192.168.1.121	147.135.130.181	TCP	64	74	34990 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850466514 TSecr=0 WS=128
3	0.052211	147.135.130.181	192.168.1.121	TCP	52	76	443 → 34988 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251546316 TSecr=1850466514 WS=128
4	0.052257	192.168.1.121	147.135.130.181	TCP	64	66	34988 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850466527 TSecr=1251546316
5	0.052275	147.135.130.181	192.168.1.121	TCP	52	76	443 → 34990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251546316 TSecr=1850466514 WS=128
6	0.052282	192.168.1.121	147.135.130.181	TCP	64	66	34990 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850466527 TSecr=1251546316
7	0.052543	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
8	0.052663	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
9	0.082159	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34988 [RST, ACK] Seq=1 Ack=105204425 Win=0 Len=0
10	0.082190	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34990 [RST, ACK] Seq=1 Ack=1430621405 Win=0 Len=0
11	3.168047	192.168.1.121	147.135.130.181	TCP	64	74	34992 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850467306 TSecr=0 WS=128
12	3.168182	192.168.1.121	147.135.130.181	TCP	64	74	34994 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1850467306 TSecr=0 WS=128
13	3.222239	147.135.130.181	192.168.1.121	TCP	53	76	443 → 34992 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251547108 TSecr=1850467306 WS=128
14	3.222290	192.168.1.121	147.135.130.181	TCP	64	66	34992 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850467319 TSecr=1251547108
15	3.222312	147.135.130.181	192.168.1.121	TCP	53	76	443 → 34994 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1452 SACK_PERM=1 TSval=1251547108 TSecr=1850467306 WS=128
16	3.222325	192.168.1.121	147.135.130.181	TCP	64	66	34994 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1850467319 TSecr=1251547108
17	3.222504	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
18	3.222600	192.168.1.121	147.135.130.181	SSL	64	269	Client Hello
19	3.252269	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34992 [RST, ACK] Seq=1 Ack=1120449859 Win=0 Len=0
20	3.252297	147.135.130.181	192.168.1.121	TCP	249	56	[TCP ACKed unseen segment] 443 → 34994 [RST, ACK] Seq=1 Ack=537856325 Win=0 Len=0

Censura en Cataluña



Análisis finales

Telefónica

vodafone

HTTP 404

Bypaseando DPI

Técnicas

- Ofuscación de Tráfico
- Encapsulación
- Tunelización
- Cifrado Selectivo de Partes del Tráfico
- Fragmentación de Paquetes
- Redirección y Manipulación de Tráfico
- Inyección de Paquetes Falsos y Redundancia en Tráfico
- Refraction Networking
- Uso de Proxies (Proxy Usage)
- Multiplexación de Tráfico
- Uso de Multipath Routing
- Separación de Datos en Múltiples Flujos
- Cambio de Tiempos de Paquetes
- Uso de Redes Anónimas
- Cambio Dinámico de Protocolo
- Uso de Protocolos No Convencionales
- Envío de RST con TTL del DPI

Técnicas

- Ofuscación de Tráfico
- Encapsulación
- Tunelización
- **Cifrado Selectivo de Partes del Tráfico**
- Fragmentación de Paquetes
- Redirección y Manipulación de Tráfico
- Inyección de Paquetes Falsos y Redundancia en Tráfico
- Refraction Networking
- Uso de Proxies (Proxy Usage)
- Multiplexación de Tráfico
- Uso de Multipath Routing
- Separación de Datos en Múltiples Flujos
- **Cambio de Tiempos de Paquetes**
- Uso de Redes Anónimas
- Cambio Dinámico de Protocolo
- Uso de Protocolos No Convencionales
- **Envío de RST con TTL del DPI**

Soluciones Anti DPI

GoodbyeDPI

Demergi

DPIGuard

Cloak

Soluciones Anti DPI

WireGuard

Cifrado Total del Tráfico
Usa UDP en lugar de TCP
No usa un Handshake Visible
Paquetes Indistinguibles

Cloak

GoodbyeDPI

Demergi

DPIGuard

Soluciones Anti DPI

Cifrado Total del Tráfico
Usa UDP en lugar de TCP
No usa un Handshake Visible
Paquetes Indistinguibles

Soluciones Anti DPI

Usa WebRTC para ofuscar el tráfico
Ofuscación y camuflaje del tráfico

Soluciones Anti DPI

Ofuscación de protocolos
Multiplexación de tráfico
Encapsulación en diferentes protocolos

Geneva

Genetic Evasion

Algoritmo genético

Acciones básicas a nivel de paquete:

- Eliminar
- Duplicar
- Fragmentar
- Manipular

Se compone de:

- Algoritmo genético
- Motor de estrategia

Geneva

Genetic Evasion

NO ANONIMIZACIÓN
NO CIFRADO
NO PROTECCIÓN CONTRA CENSURA

Preservando la privacidad

BlindBox (2015) **PrivDPI** (2019) **P2DPI** (2021)

Se cifra datos
Se opera con firmas

Preservando la privacidad

BlindBox (2015) **PrivDPI** (2019) **P2DPI** (2021)

Calculo Multipartito seguro (MPC)
Criptografia Homomórfica

Preservando la privacidad

BlindBox (2015) **PrivDPI** (2019) **P2DPI** (2021)

Criptografía homomórfica ligera
Filtrado de patrones
Privacidad diferencial

Jugando con DPIs

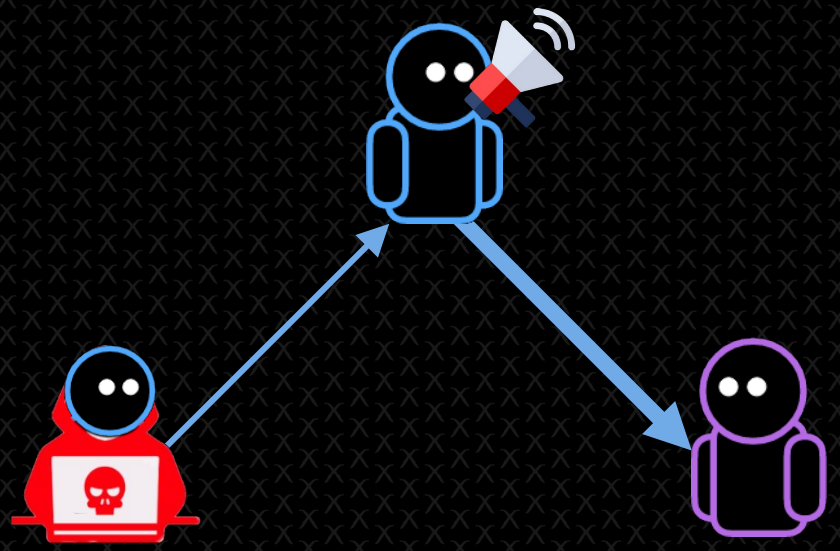
Amplificacion DOS tipo deflection:

- Primer ataque TCP no SYN
- Primer ataque basado en HTTP
- TCP > UDP
- Posible amplificación infinita

Jugando con DPIs

Amplificacion DOS tipo deflection:

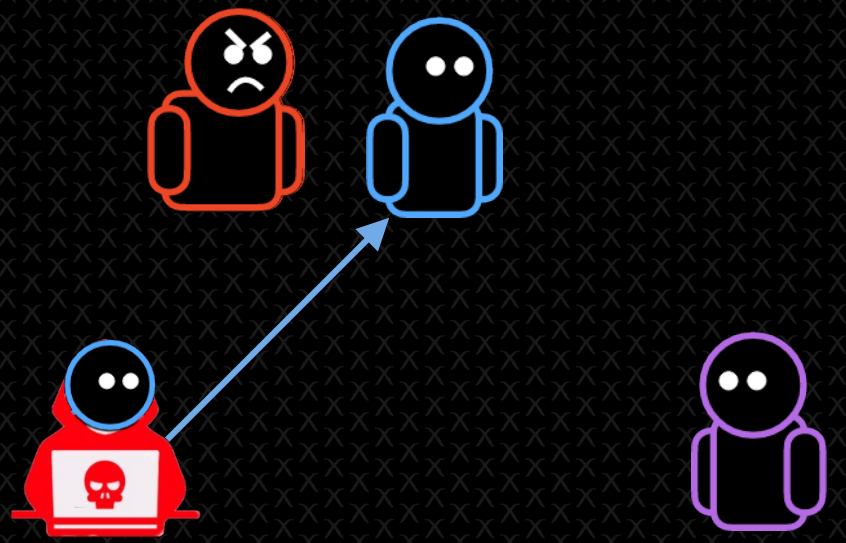
- Primer ataque TCP no SYN
- Primer ataque basado en HTTP
- TCP > UDP
- Posible amplificación infinita



Jugando con DPIs

Amplificacion DOS tipo deflection:

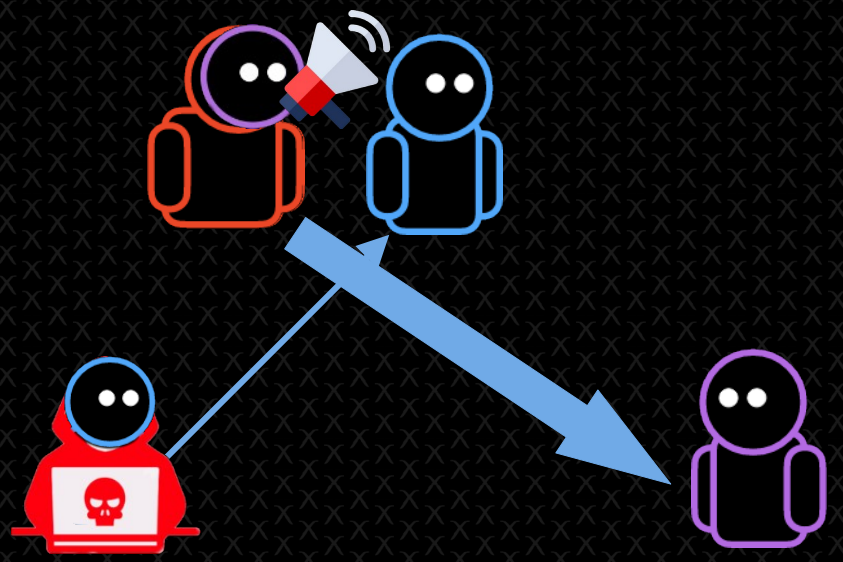
- Primer ataque TCP no SYN
- Primer ataque basado en HTTP
- TCP > UDP
- Posible amplificación infinita



Jugando con DPIs

Amplificacion DOS tipo deflection:

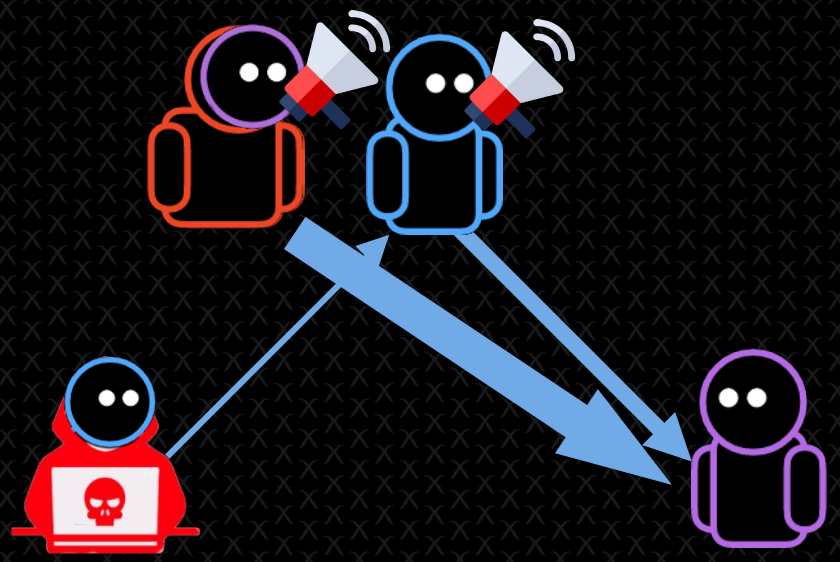
- Primer ataque TCP no SYN
- Primer ataque basado en HTTP
- TCP > UDP
- Posible amplificación infinita



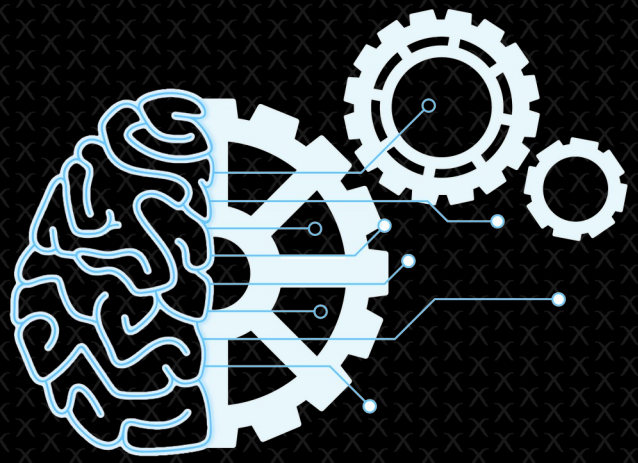
Jugando con DPIs

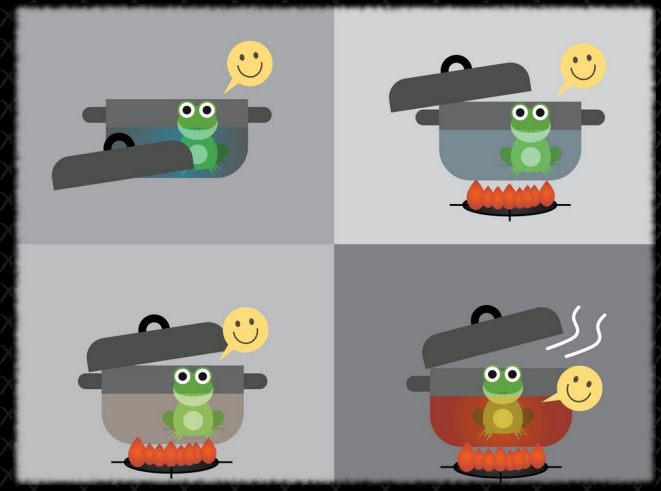
Amplificacion DOS tipo deflection:

- Primer ataque TCP no SYN
- Primer ataque basado en HTTP
- TCP > UDP
- Posible amplificación infinita



Conclusiones





Gracias

OONI

Qurium
THE MEDIA FOUNDATION

Freedom House

Tor®
TorProject.org

¿Preguntas?

 @feliz1984@mastodon.social

 @ReD.1984

 red@feliz1984.com