



Taller selfhosting mensajeria

CONTEXTO ACTUAL GEOPOLITICO

- La privacidad esta en juego
- Múltiples conflictos en Oriente Medio
- EEUU con cambio a tendencia proteccionista
- EUROPA : con múltiples gobiernos debiles
- RUSSIA : con CYBERGUERRA en áuge.







XI JINPING

HE DOES
NOT BELIEVE
IN PARTY'S
'COLLECTIVE'
LEADERSHIP...



Porcentajes de uso en españa

- Whatsapp: 95.6%
- Telegram: 39.9%
- Facebook 29.6%
- Instagram md 25.3%
- Teams: 19.1%
- Google chat: 6.2%
- Signal : 2.3%
- NO USAN! : 1.5%
- Otros : 3.6%
 - Xmpp
 - Irc
 - Matrix ...

¿ MENSAJERIA GRATIS ?

Cuando un producto es gratis,
normalmente el producto eres tú.

[https://www.youtube.com/watch?
v=pxWcNhR_Jp8](https://www.youtube.com/watch?v=pxWcNhR_Jp8)

¿De donde venimos ?



Aquellos que no recuerdan el pasado están
condenados a repetirlo.

—George Santayana

Historia de la mensajería | LOS 70 |

- 1971: Se envía el primer correo electrónico,
- 1973: Talkomatic en PLATO,
- 1978: Nace el CBBS (Bulletin Board System)



Historia de la mensajería | LOS 80 |

- 1980: Surgen chat relay
- 1998 : Msn microsoft
- 1983: Aparece el USENET
- 1986: Electronic Communications Privacy Act
- 1988: Se crea Internet Relay Chat (IRC),

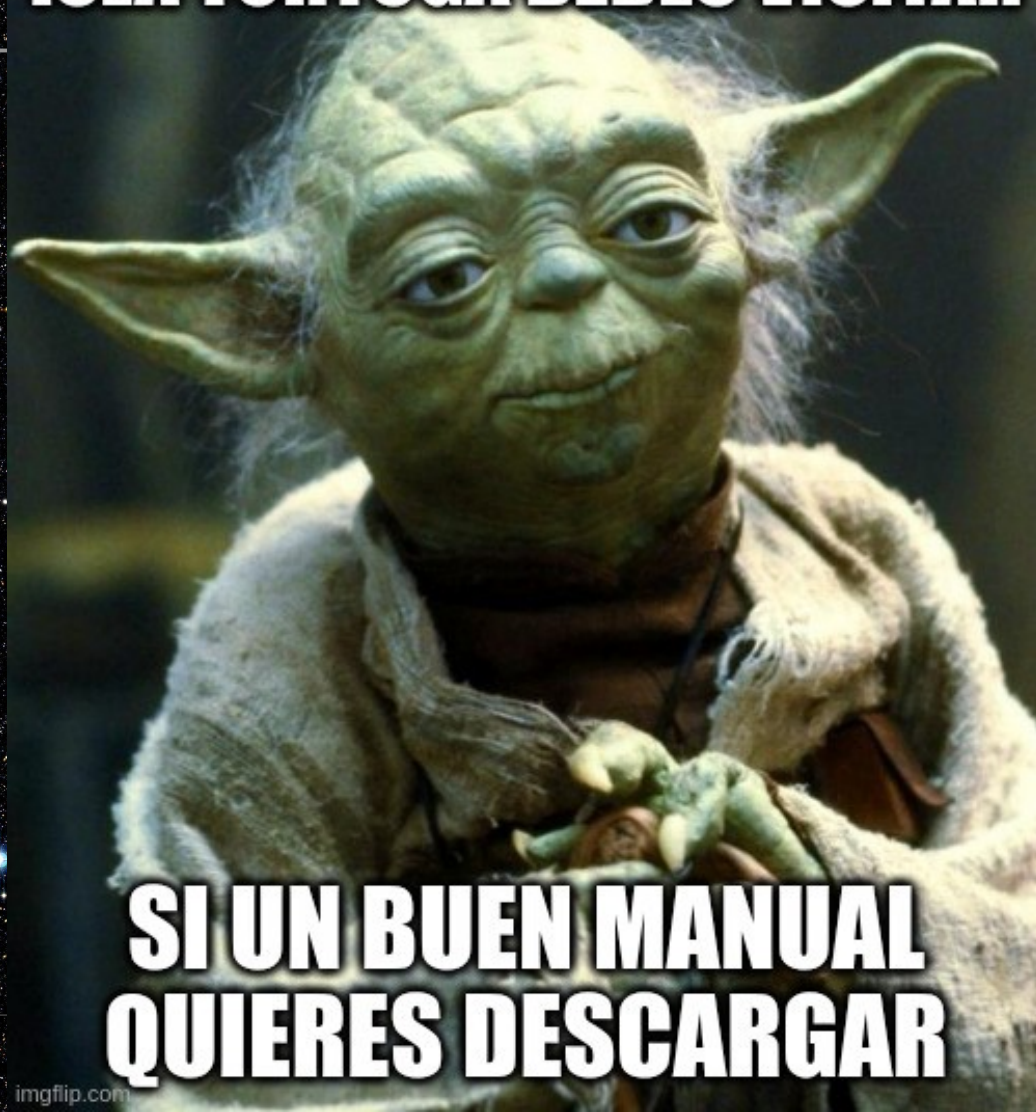
THE ECPA

ITS A TRAAAP

Historia de la mensajería | LOS 90 |

- 1996: ICQ, el primer mensajero popular
- 1996 : ISLA TORTUGA !
- 1998: AIM (AOL Instant Messenger)
- 1999: MSN Messenger
- 1999: La NSA intercepta MSN y AOL con ECHELON
- 1999: XMPP (jabber)

ISLA TORTUGA DEBES VISITAR



**SI UN BUEN MANUAL
QUIERES DESCARGAR**

Historia de la mensajería | 2000s |

- 2001 : 11s PATRIOT ACT
- 2002: Google lanza Gmail,
- 2002: Open fire (xmpp server) en java
- 2004: OTR , off-the-record
- 2004: Nace facebook
- 2007: Apple presenta el iPhone
- 2007: Arranca el proyecto PRISM
- 2009: WhatsApp
- 2010: Se lanza BBM (BlackBerry Messenger)

PORQUE TE CHIVASTE EDWARD

ERAS EL ELEGIDO

Historia de la mensajería | LOS 90 |

- 2011: Lulzsec Hackea AOL comprometiendo miles de usuarios
- 2013: Nace Telegram con E2EE
- 2013: LEAKS SNOWDEN xkeylogger y PRISM
- 2013: xmpp y skype comprometidos + VAULT 7
- 2014: Matrix
- 2017 : SCUTTLEBUT
- 2017 : SIGNAL



OPCIONES ACTUALES

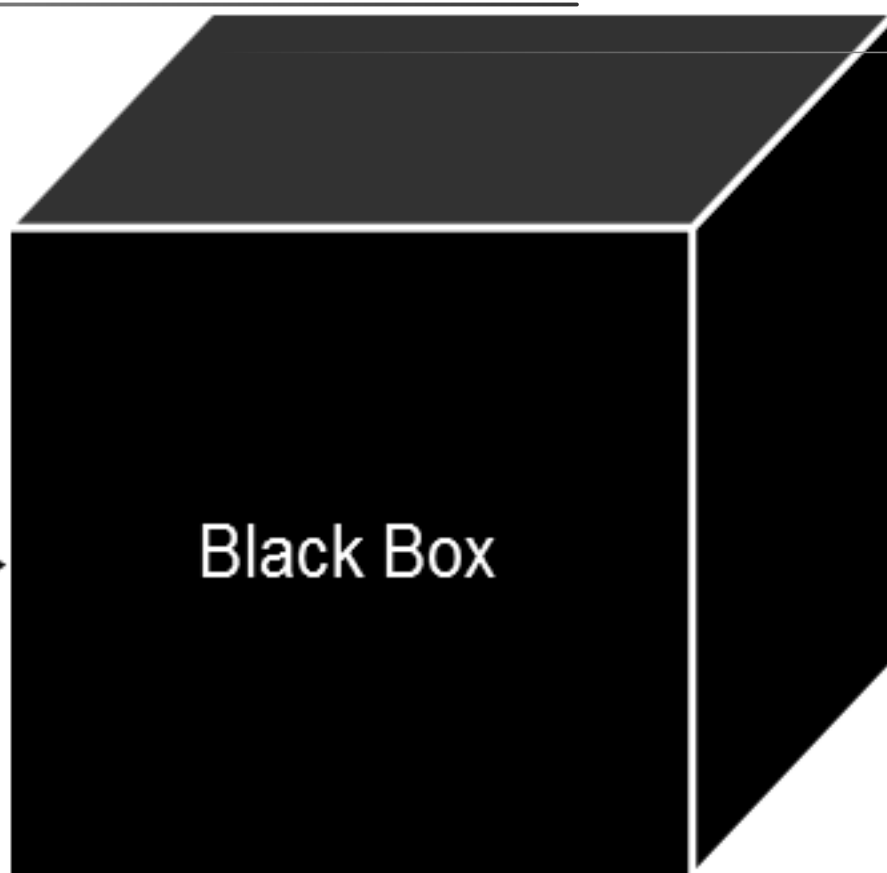
• Signal	- Software libre	- Centralizado
• Xmpp	- Software libre	- Descentralizado
• Matrix	- Software libre	- Federado
• Briar	- Software libre	- Peer-to-peer
• Tox	- Software libre	- Peer-to-peer
• Simplex	- Software libre	- Peer-to-peer
• OASIS	- Software libre	- Federado & Peer-to-peer

NO SON OPCIONES , PORFAVOR!

- Privativos , Centralizados , modelo de negocio...
- Telegram : Pavel y la ciudad del amor.
- Whatsapp , mr suk con sus colaboradores
- DM instagram , mr zuk con sus homofobias
- Snapchat ... entre broma y broma 2 cazas

QUE NO SON OPCIONES HE DICHO

Input



Black Box

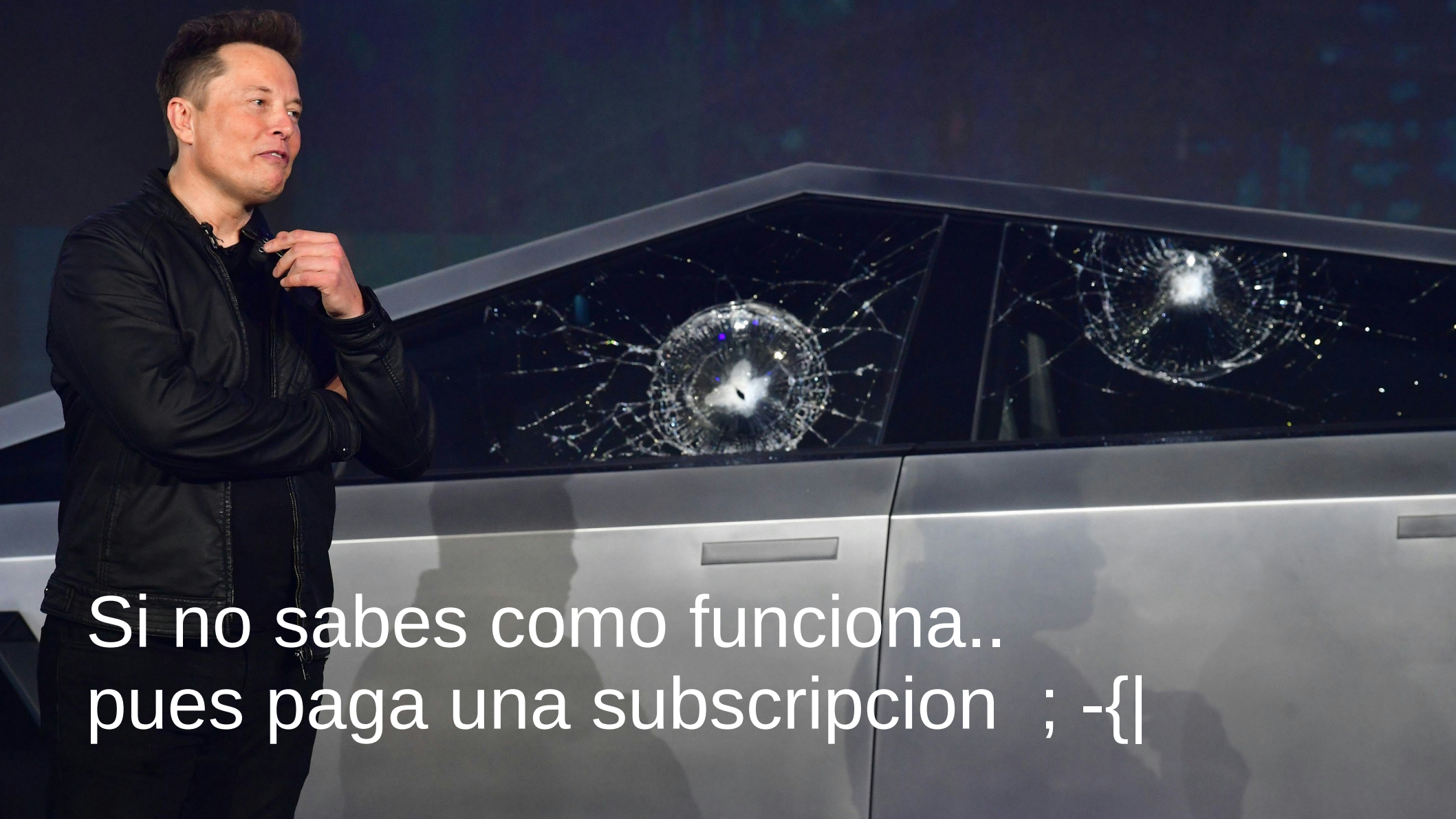


Output

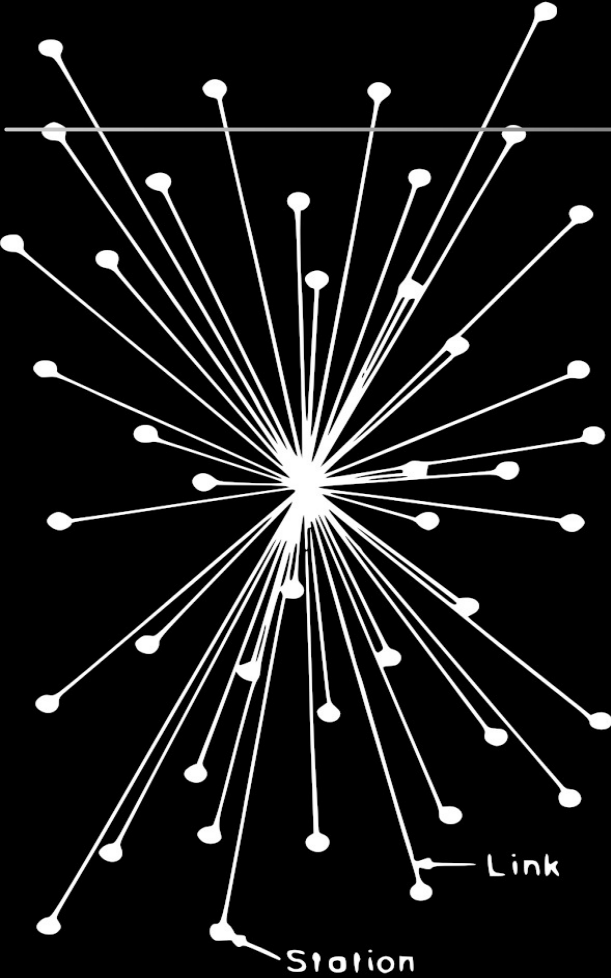
Internal behavior of the code is unknown

WELL THERE'S YOUR PROBLEM

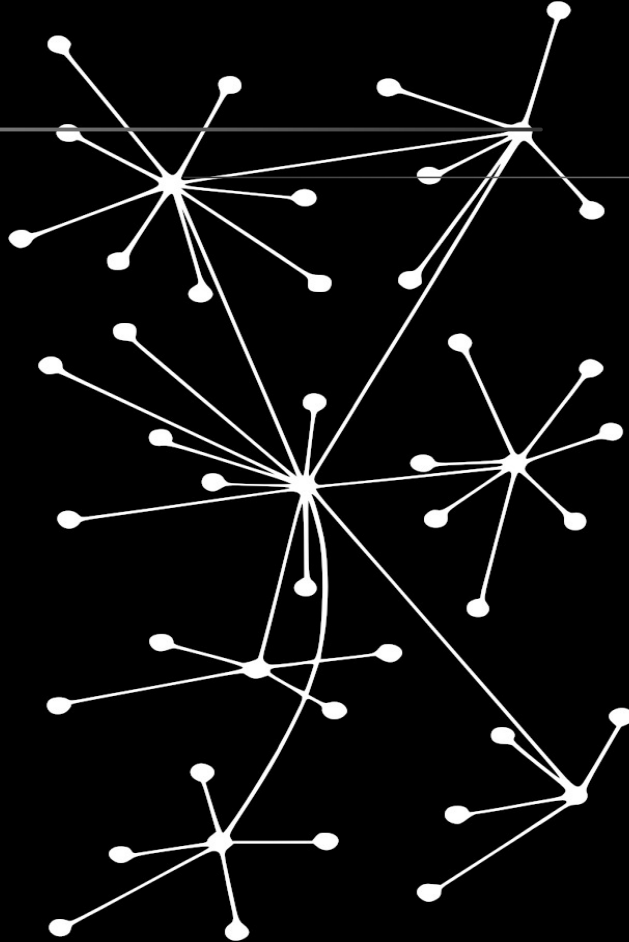




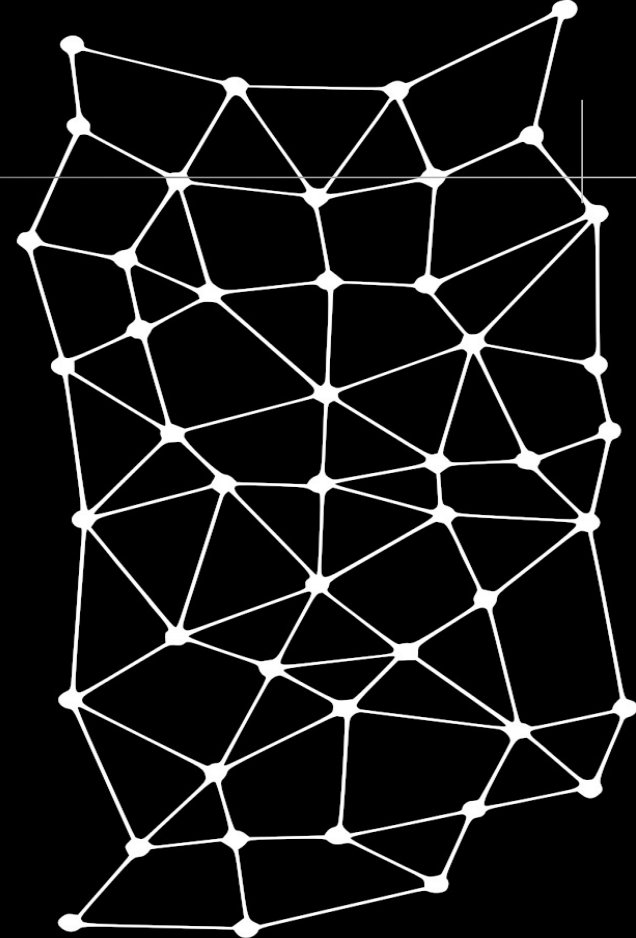
Si no sabes como funciona..
pues paga una subscripcion ; -{



CENTRALIZED
(A)



DECENTRALIZED
(B)



DISTRIBUTED
(C)

FIG. 1 — Centralized, Decentralized and Distributed Networks

MENSAJERIA CENTRALIZADA



- Todo pasa por un nodo maestro.



Single point of failure

SYSTEM FAILURE

error 235553261...pending.....
fatal ER # 5444167QW32Z_ws @%\$\$

- Y si ese nodo falla ? O es hackeado ?

MENSAJERIA DESCENTRALIZADA

TIENE VARIOS NODOS QUE
VALIDAN. NO DEPENDE DE
UN SERVIDOR CENTRAL.

MENSAJERIA FEDERADA

LOS NODOS QUE VALIDAN SE
APOYAN ENTRE ELLOS CON
PROTOCOLOS DE RED COMO
SCUTTELBUT O GOSSIP

La importancia del cifrado

- Cifras porque tienes
algo que ocultar ?

~NO , cifro porque
la privacidad es un Derecho !

PGP
TOR
OTR
FTW

0xCRYPTOPARTY.IN

CIFRADO Y PROTOLOS

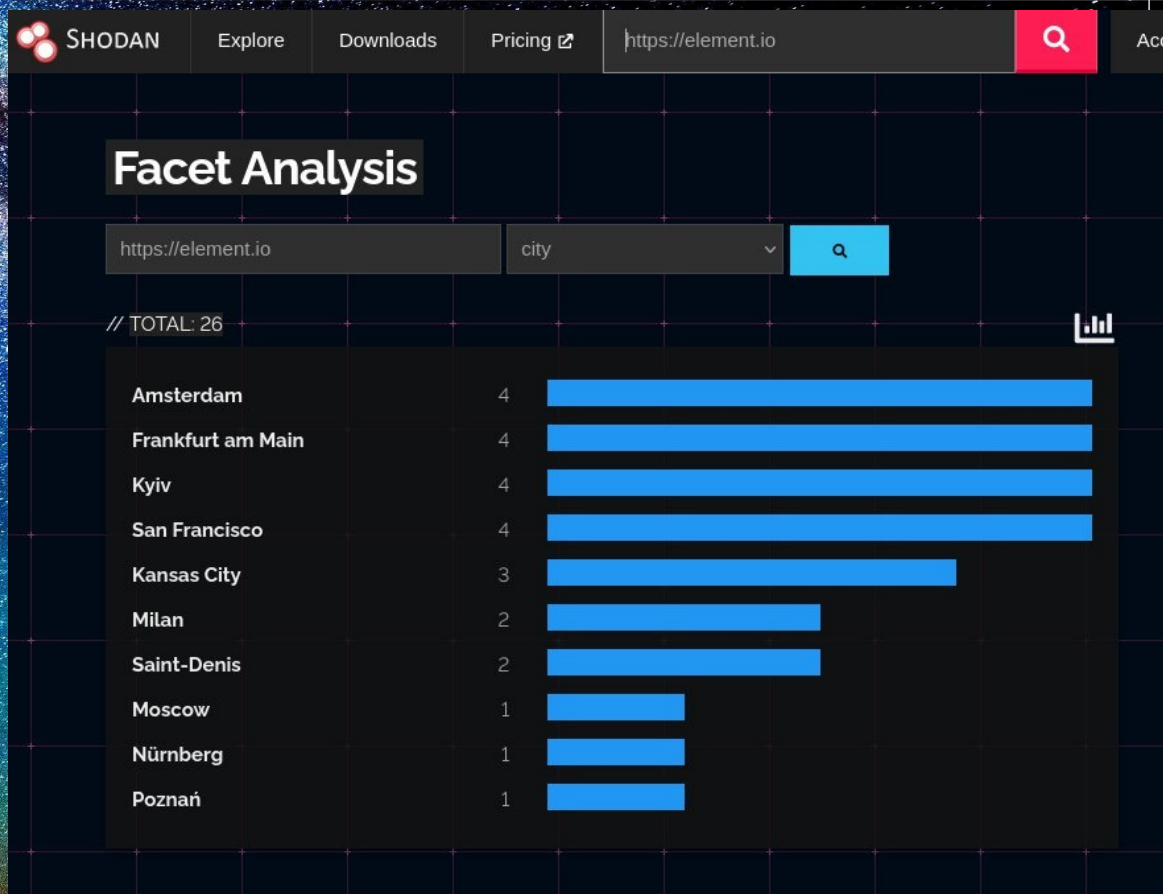
- SHA256
- OMEMO
- PGP
- OTR
- E2EE
- P2P con NACL
- SCUTTLEBUT
- PFS
- X25519
- Curvas elipticas

MATRIX

- INSTALAR **SYNAPSE**
- TENER UN ROUTER
- TENER UN DOMINIO o IP FIJA FUERA DEL CGNAT
- CLIENTE (ELEMENT , ROCKET.CHAT , NEOCHAT)

Shodan.io -> analizar servidores

- Es element del MOSSAD ?
- Element vende datos ?
- Es matrix seguro ?



XMPP

- INSTALAR PROSODY
- TENER UN ROUTER
- DOMINIO O IP FUERA DEL CGNAT
- CLIENTE (CONVERSATIONS)

IRC

- Internet relay chat
- Mensajes temporales
- Salas publicas y privadas
- Anonimo
- Multiuser sencillo (se puede cambiar de nick)

OASIS

- Federada
- Descentralizada
- Cifrado
poscuantico
- Incensurable
- Chat privados
- Persistente



COMMANDOS INSTALACION

```
sudo apt-get install git curl  
curl -sL http://deb.nodesource.com/setup\_22.x | sudo bash -  
sudo apt-get install -y nodejs  
git clone https://code.03c8.net/KrakensLab/oasis  
cd oasis  
npm install .  
npm run start
```

code.03c8.net

KrakensLab/oasis

[PROD] SolarNET.HuB (SNH) - The Project Network - Oasis

PARA DUDAS O DEBATES

sito0@riseup.net

- Dance like no one is watching
- Encrypt like everyone is.
- XMPP : sito0@conversations.im
- OASIS : cant find me if i dont let you ; -)

Ni con OSINT JAJAJA que la fuerza os ACOMPAÑE

MESSAGE WARS

Generated by Font-Generator.com

THE END

Generated by Font-Generator.com