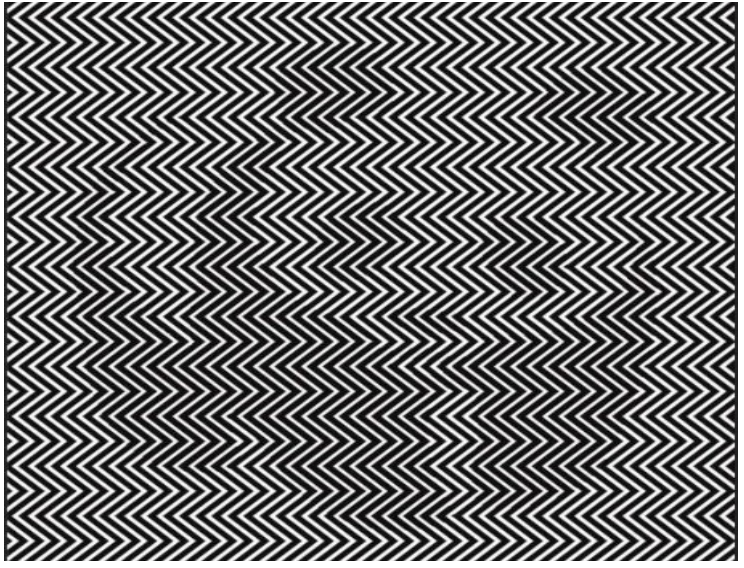
Vigilancia silenciosa
Lo que el cifrado NO esconde



Ahora es personal

¿Quién soy?

ReD

SecOpsDev

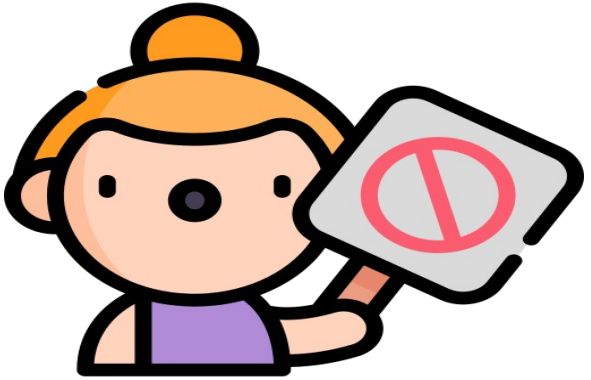
Formador, cuando me dejan

Activista tecnológico

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

Aprendiz de investigador

A quién puede interesar



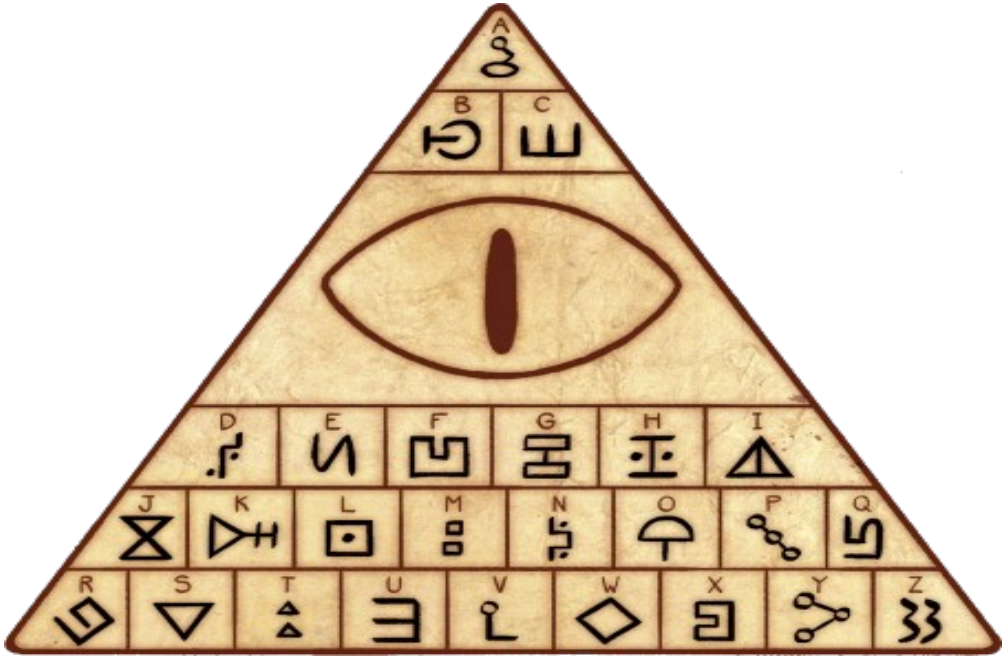
Activistas

Periodistas

Juristas

A quién puede interesar

A todos

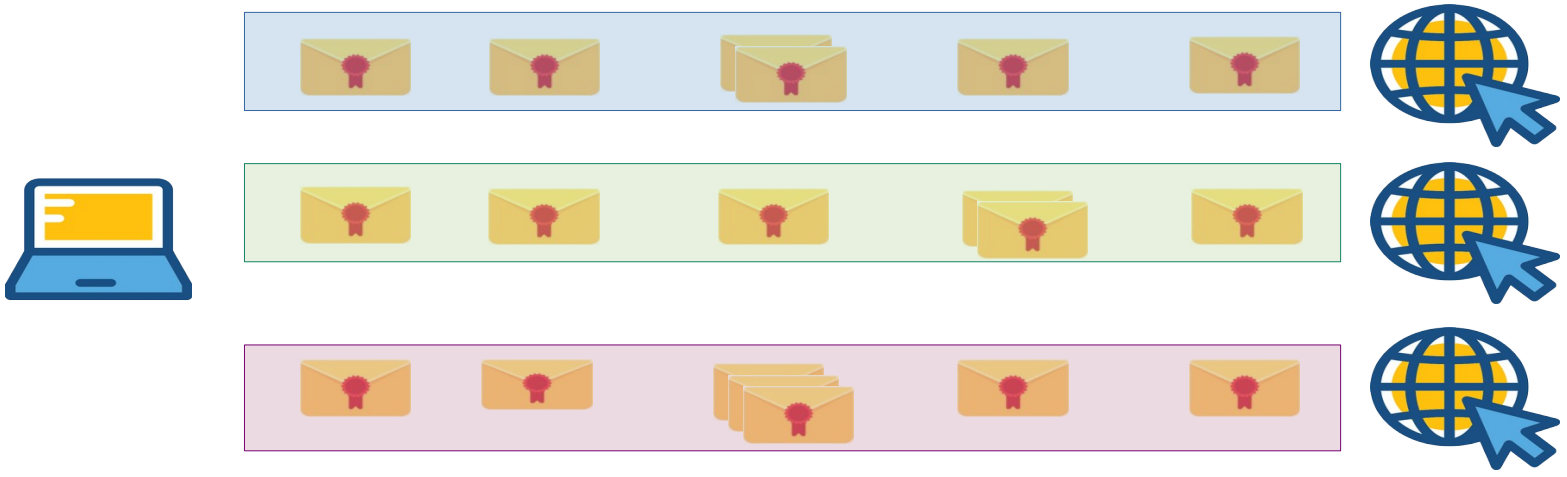


Si está cifrado es seguro

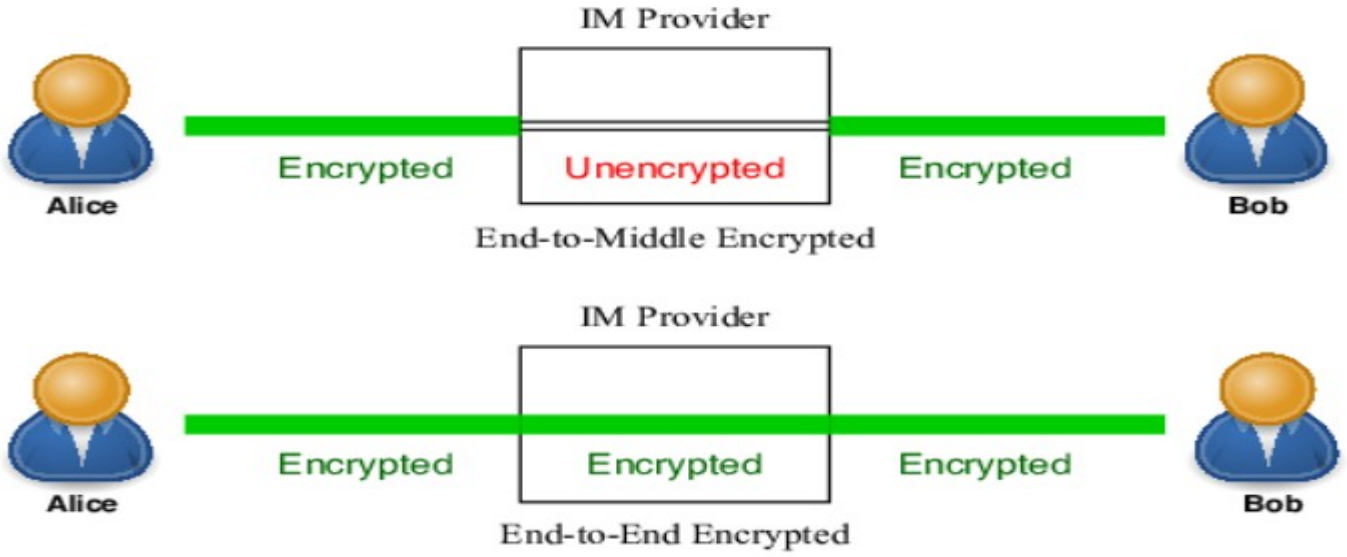
“tiene privacidad”

Comunicación en claro

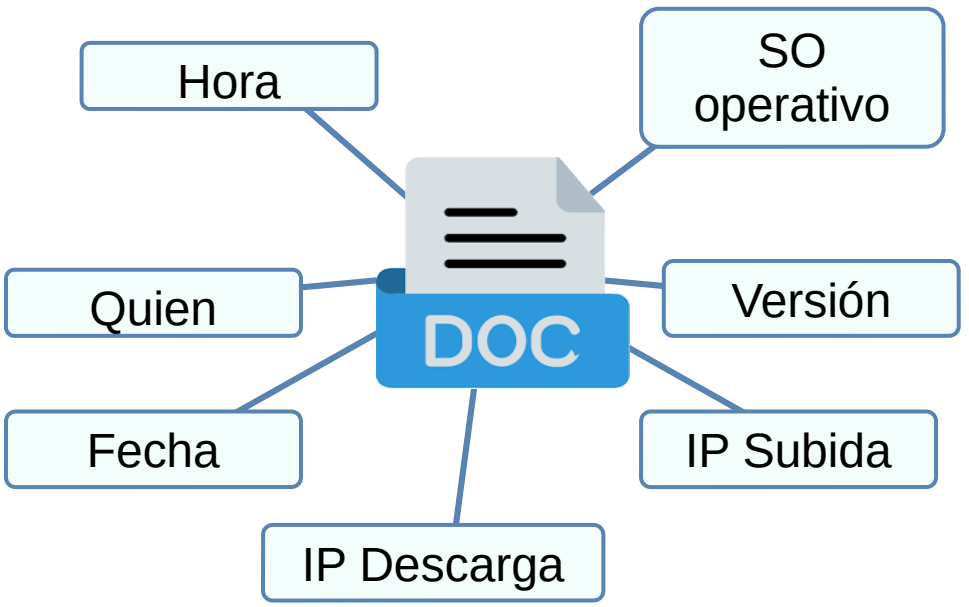
Comunicación cifrada

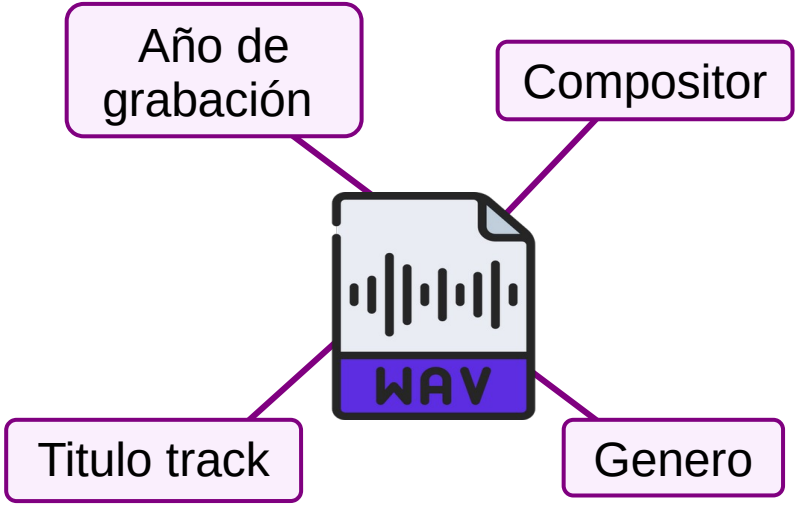


Cifrado E2EE



Metadatos en ficheros





Metadatos en el trafico

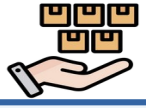
Metadatos en el trafico

Duración

Timestamp

Tipo

Direcciones



Paquetes # Datos

TTL

IP/Puerto

Attachments

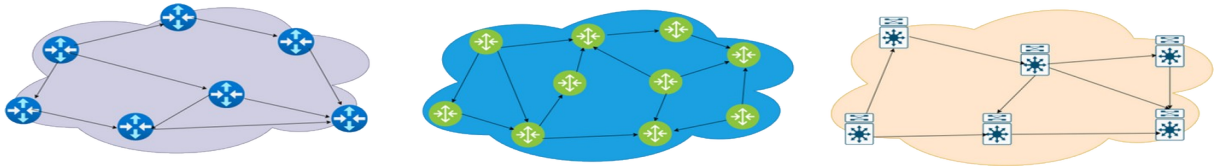
Flags

Certificados

Protocolos

Metadatos - Análisis

Topología de red (nodos principales)

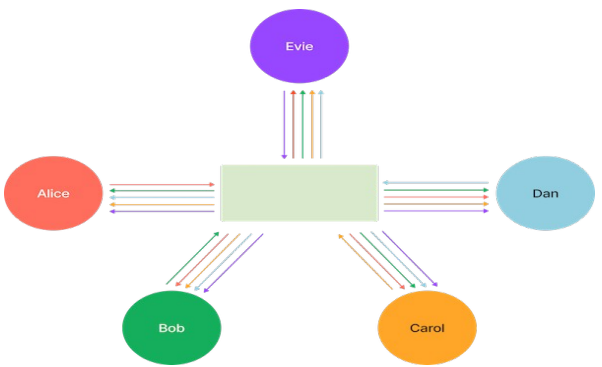


Donde ocurre la comunicación (geolocalización)

Metadatos - Análisis

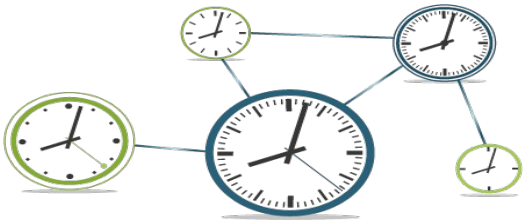
Tamaño de paquetes

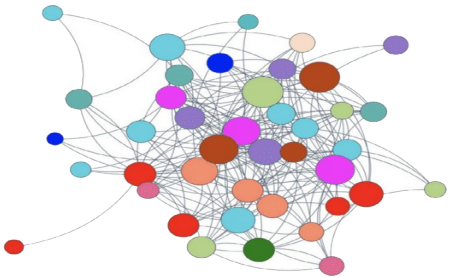
Correlación (activismo)



Metadatos - Análisis

Frecuencia de conexiones (servicios)





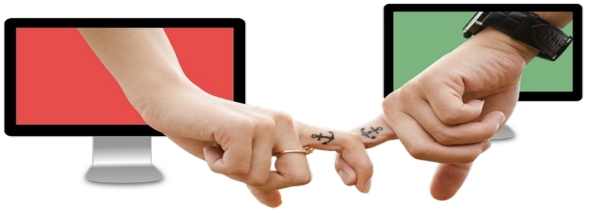
Duración de las Conexiones (periodicidad)

Huella dactilar (identificación)

Metadatos - Análisis

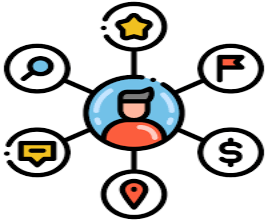
Información del Certificado

Patrones de handshake
y renegociación



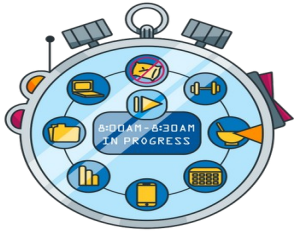
Metadatos – Resultados finales

Perfilado detallado



Identificación indirecta

Correlación de perfiles



Saber rutinas y hábitos (Sexting)

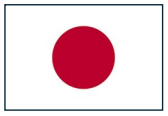
Los metadatos son tan valiosos como el contenido

Cómo están las cabezas

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

TICSA

SORM

G10 Gesetz

BÜPF

CALEA

MITA

Interceptación Legal (LI)

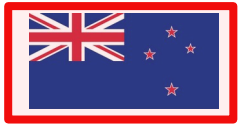
Investigatory Powers Act

Telecommunications (Interception and Access) Act

Ley de Interce
Comunic

Loi relative au renseignement

Indian Telegraph Act y IT Act



TICSA

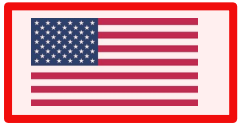
Five eyes

SORM

G10 Gesetz

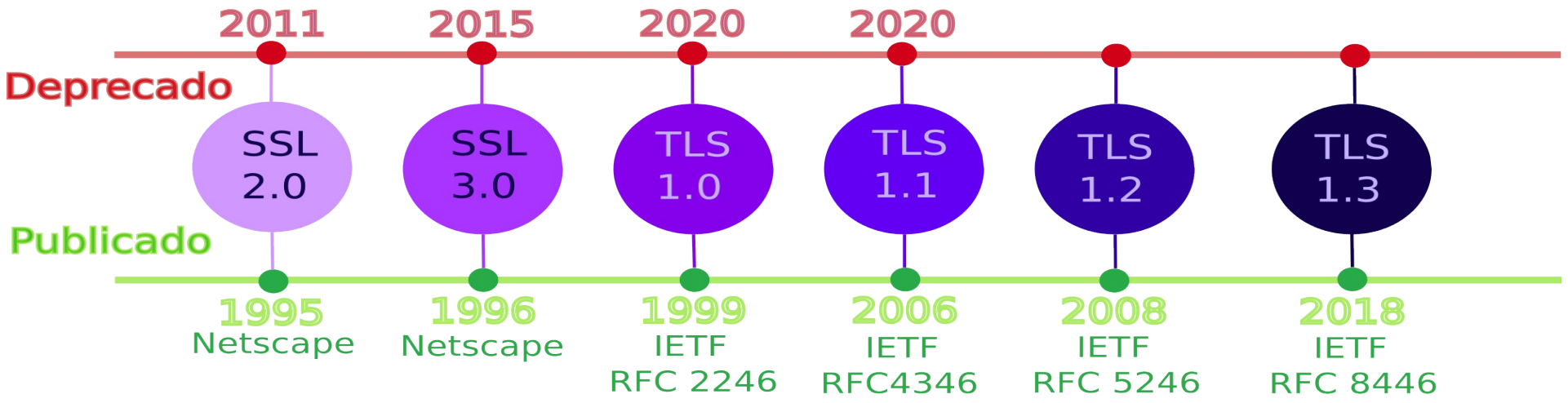
BÜPF

CALEA



MITA

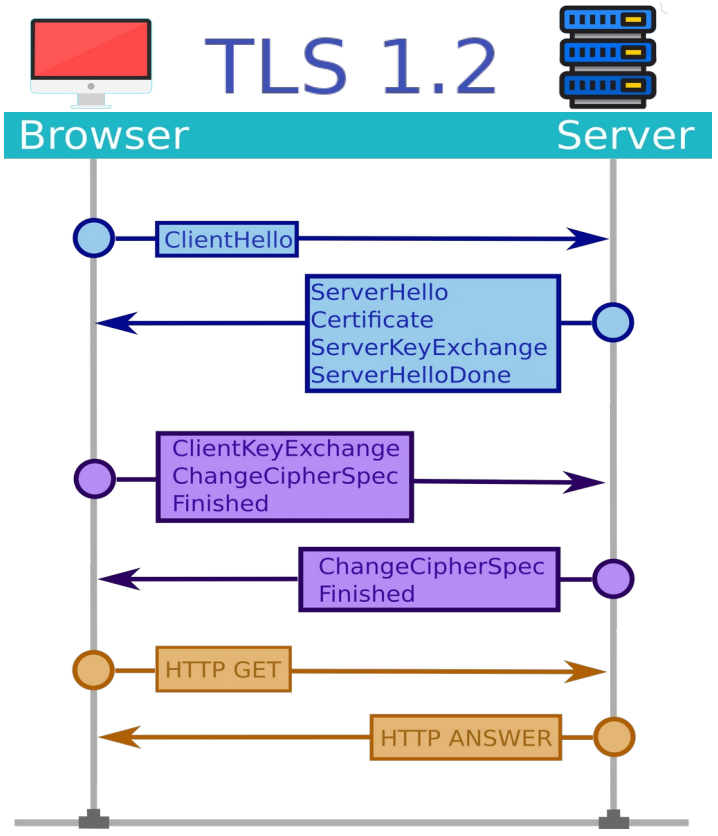
Historia del cifrado (TLS)

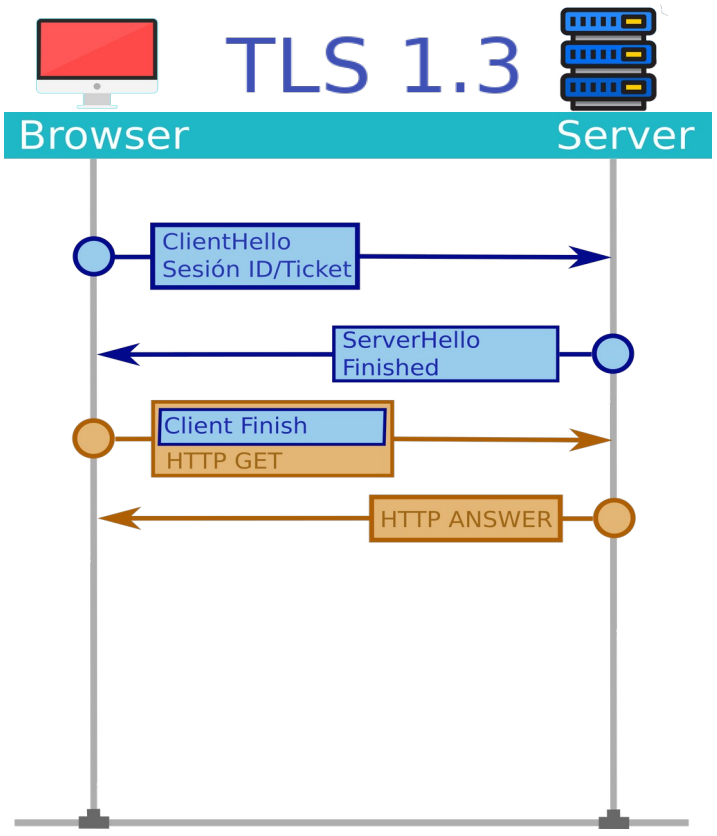


*** Internet Engineering TaskForce**

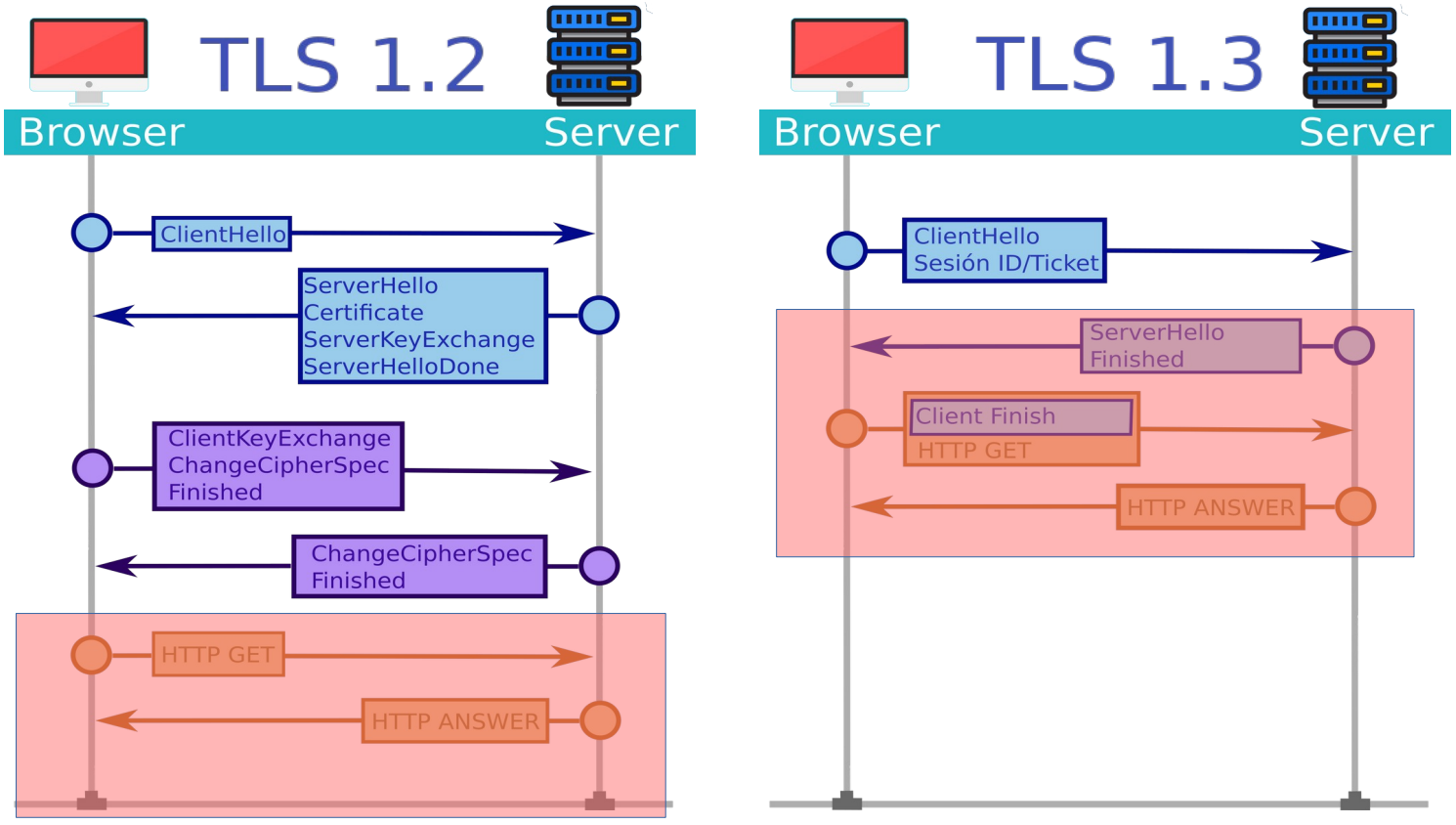
Borrador TLS 1.3
Abr 2014 - Ago 2018

Handsake TLS 1.2 y 1.3

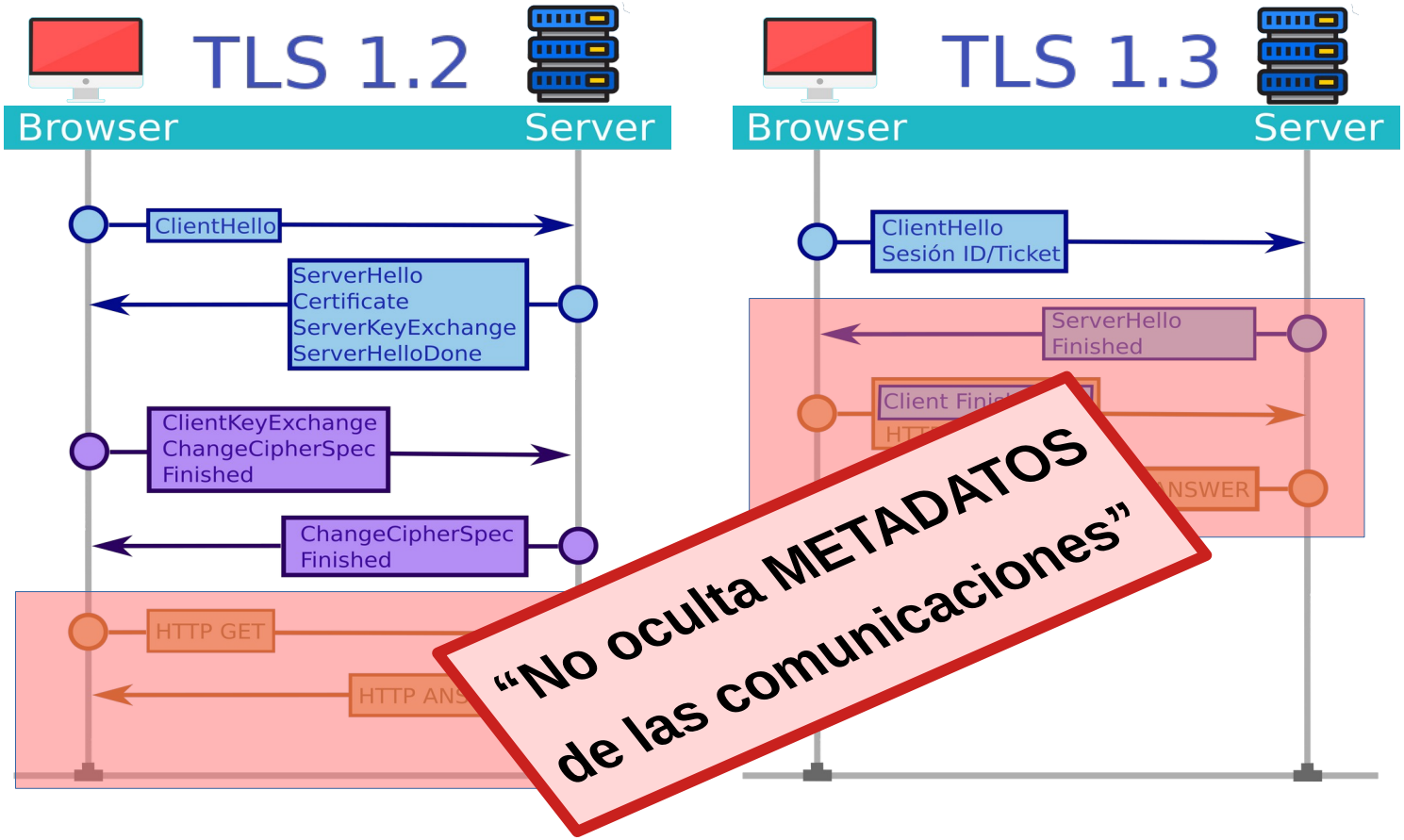




Handsake TLS 1.2 y 1.3



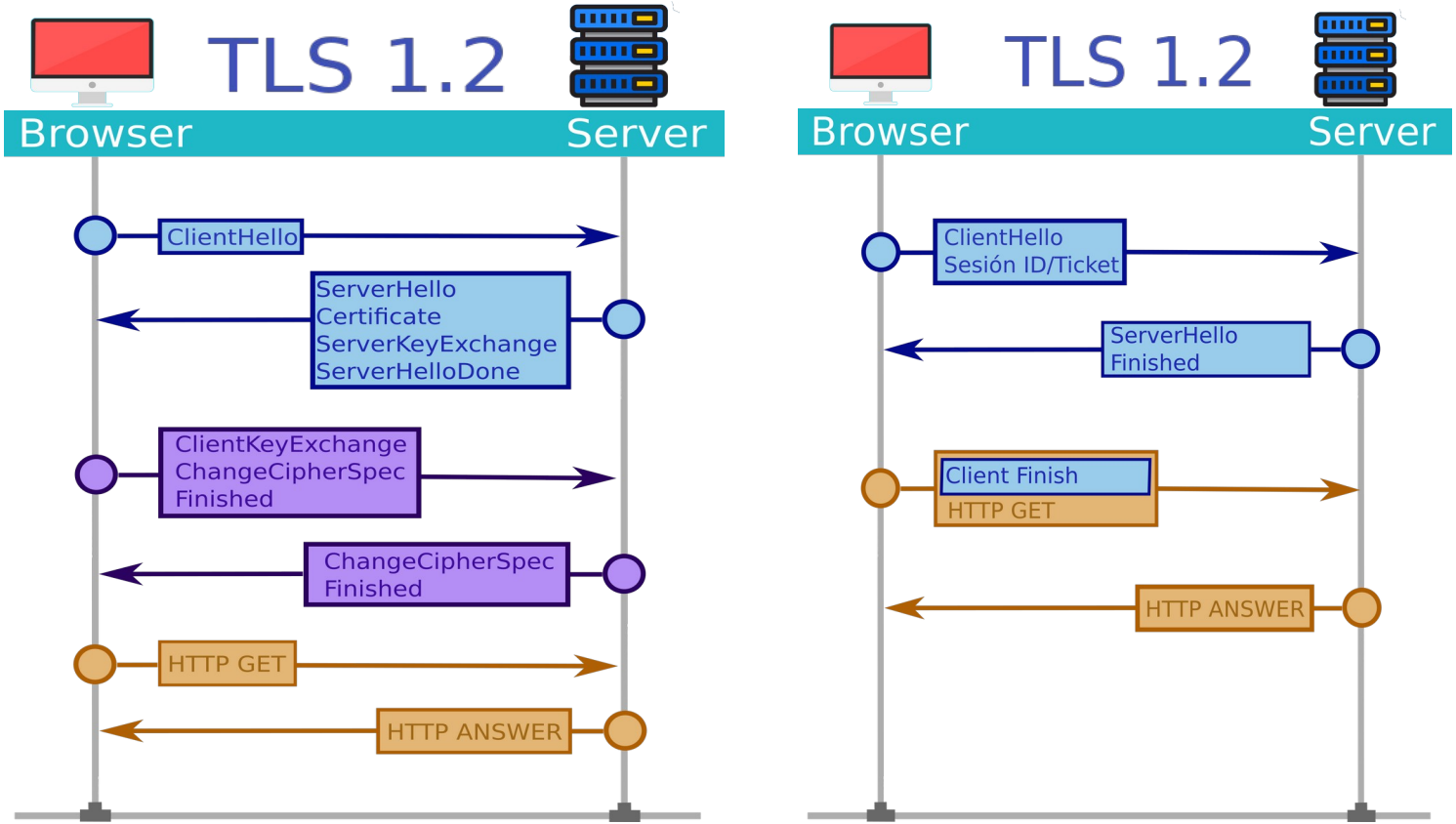
Handsake TLS 1.2 y 1.3



TLS 1.3 el más rápido

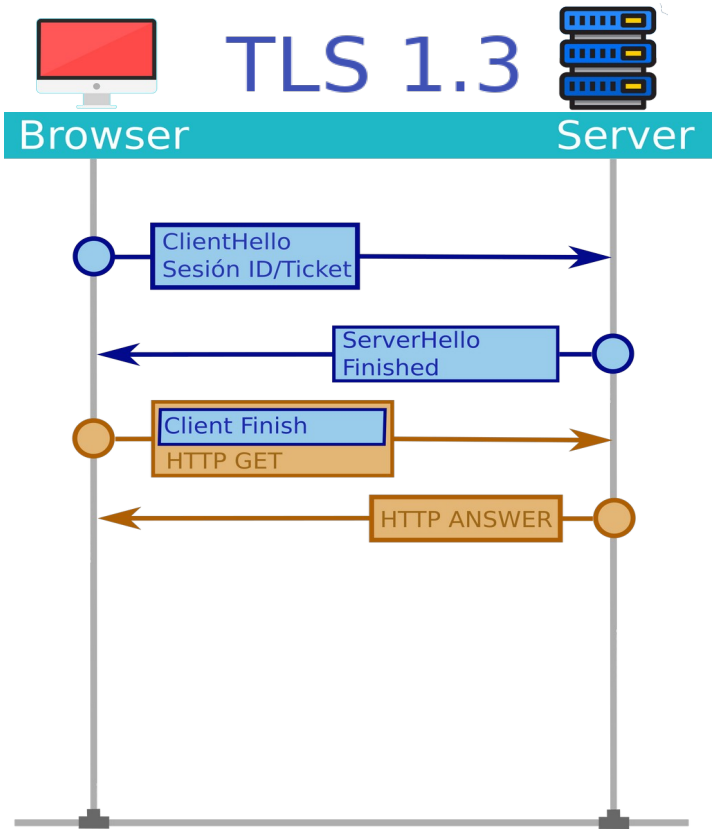
TLS 1.3 el más rápido

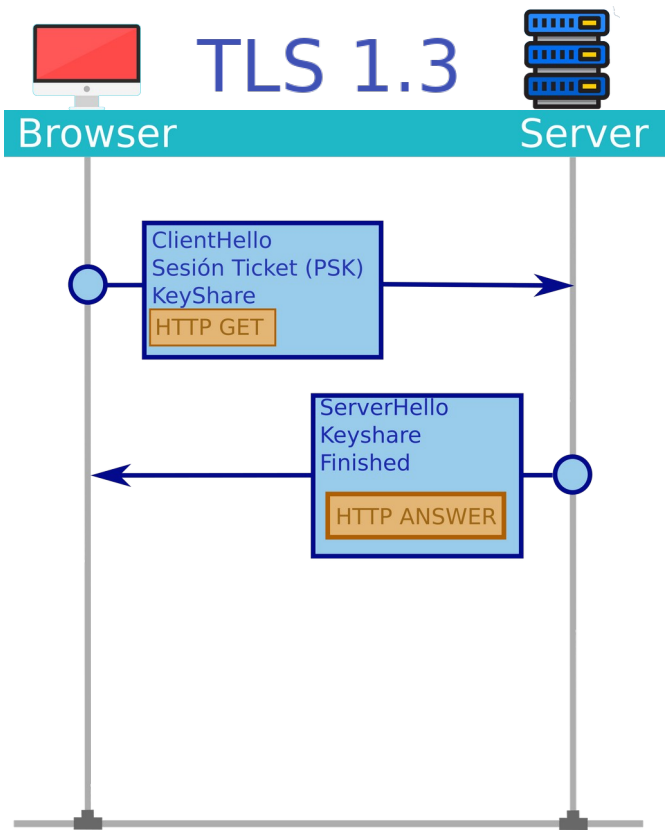
Cacheo de TLS 1.2



Session ids/tickets
2 RTT → 1RTT

Cacheo de TLS 1.3





PKS

1 RTT → 0RTT

Siguiendo usuarios por TLS

- **Estudio de la universidad de Hamburgo**
- **Funciona como cookie**

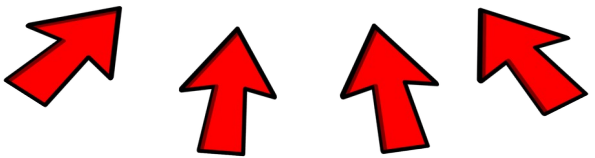
- **Seguimiento por PSK desde el servidor (da igual IP)**

Siguiendo usuarios por TLS

Tiempo max	**10,080 min (7 días)**
Recomendado TLS 1.2	**3 min**
Recomendado TLS 1.3	**5 min**

Siguiendo usuarios por TLS

Tiempo max	**10,080 min**
Recomendado TLS 1.2	**3 min**
Recomendado TLS 1.3	**5 min**



Siguiendo usuarios por TLS

- El navegador también gestiona la caché
- Ataque de prolongación
- 5 minutos como máximo
- Si cierran navegador se borra cache

Siguiendo usuarios por TLS

- El navegador también gestiona la caché
- Ataque de prolongación
- 5 minutos como máximo
- Si cierran navegador se borra cache

Siguiendo usuarios por TLS

- El navegador también [illegible]na la caché
- Ataque de [illegible]
- 5 minutos [illegible]o máximo
- Si cierran navegador se borra cache

Siguiendo usuarios por TLS

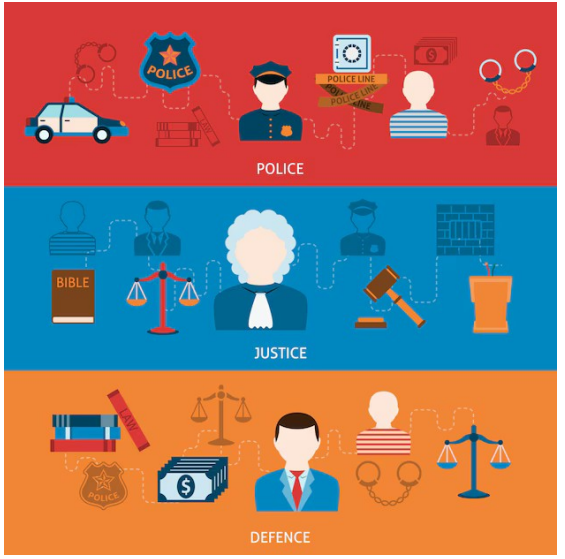
- **Siempre activada**
- **Navegador “no se reinicia”**
- **Posible cacheo constante**

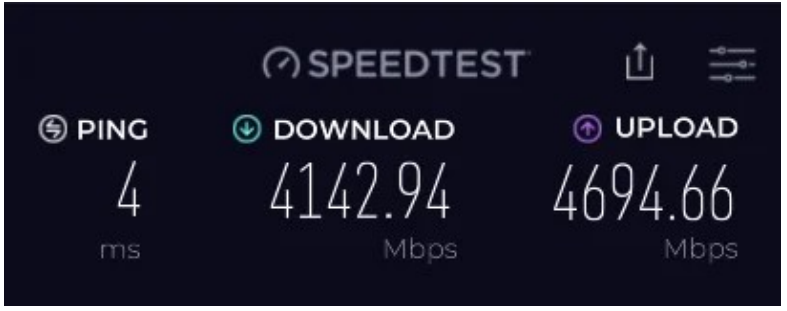
Siguiendo usuarios por TLS

- **Siempre activada**
- **Navegador “no se reinicia”**
- **Posible cacheo constante**

A qué nos enfrentamos

Adversarios increíblemente poderosos





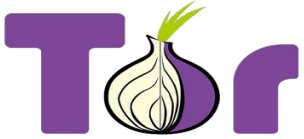
“Necesidad” de baja latencia y gran ancho de banda

Técnicas para combatirlo

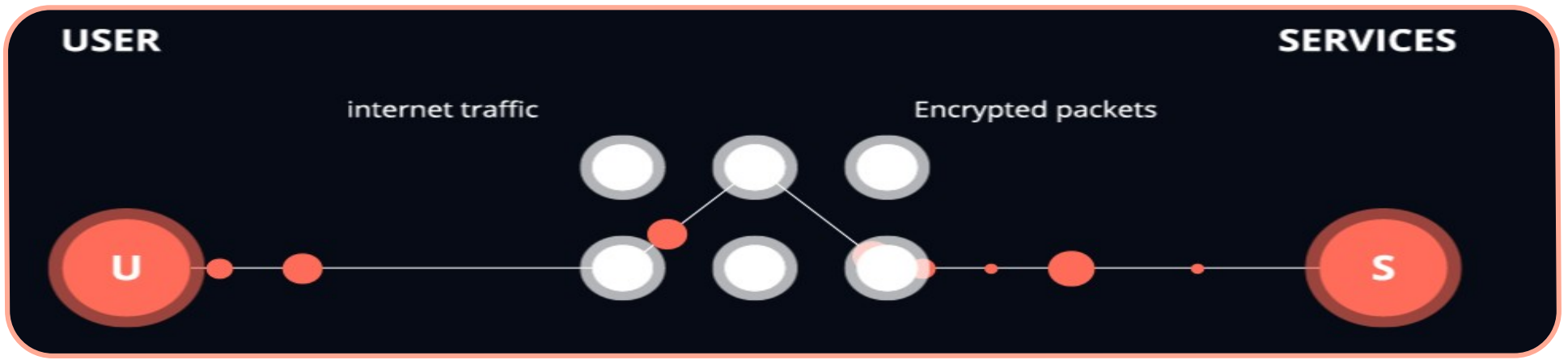
- **Relleno de Paquetes (Padding)**
- **Tráfico "Chaff" o Relleno de Ruido**
- **Tiempos de Transmisión Aleatorizados**
- **Redirigir tráfico por nodos intermedios**
- **Tráfico cifrado a través de múltiples saltos**

VPNs

Redes enrutadas anónimas



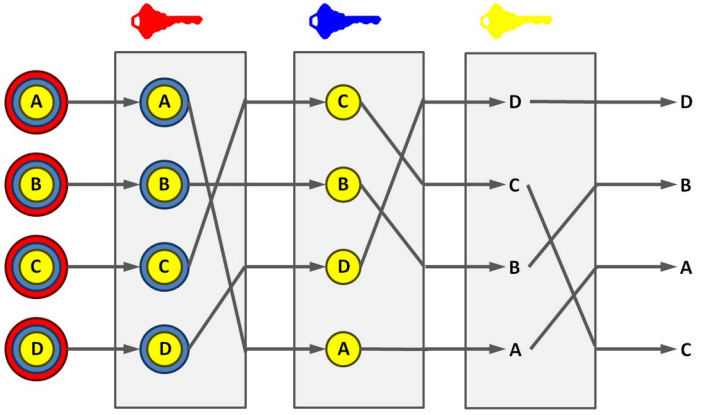
Redes enrutadas anónimas



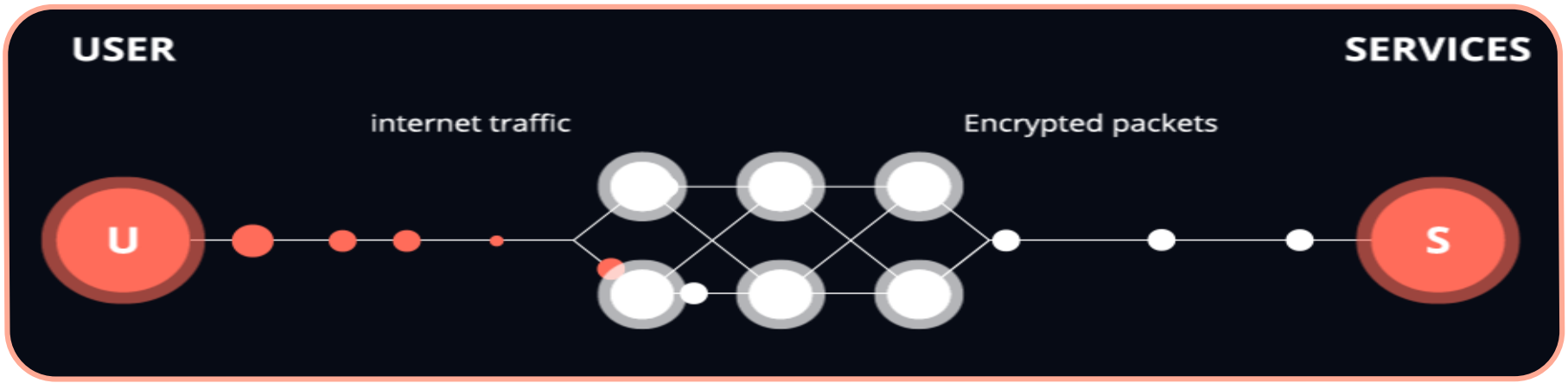
Redes MixNets

David Chaum
1981 "Correo Electrónico de rastro oculto, Direcciones de Regreso, y Seudónimos Digitales”

- **Mixmaster (1995)**
- **Mixminion (2003)**

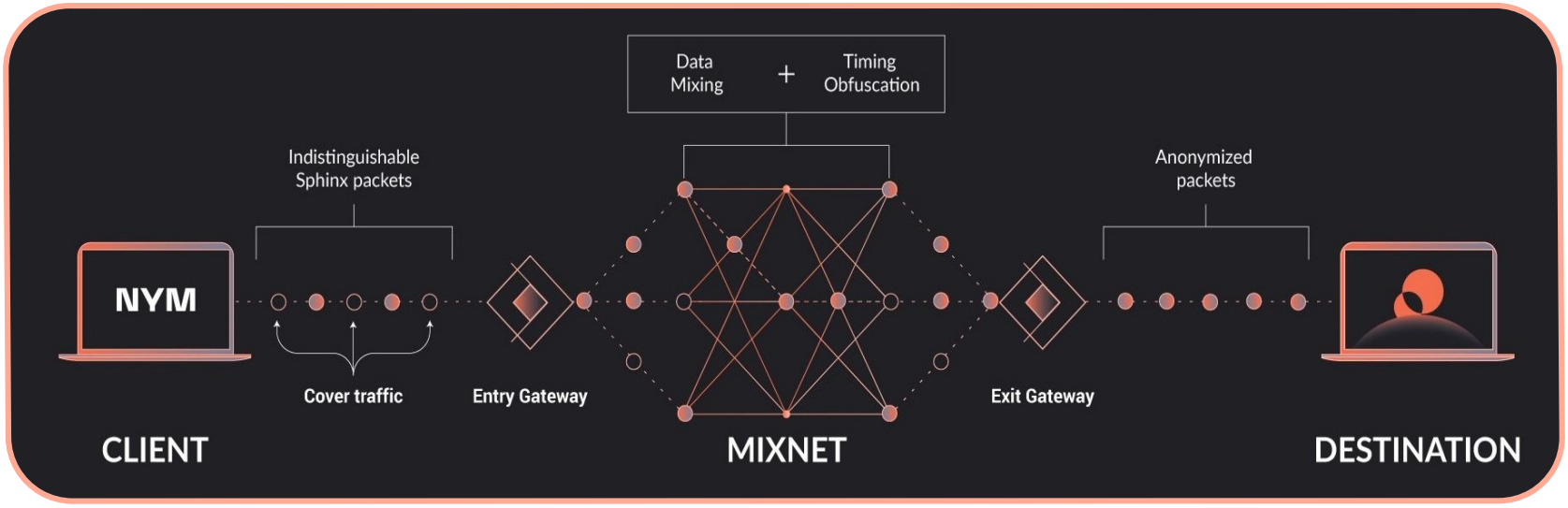


Redes MixNets

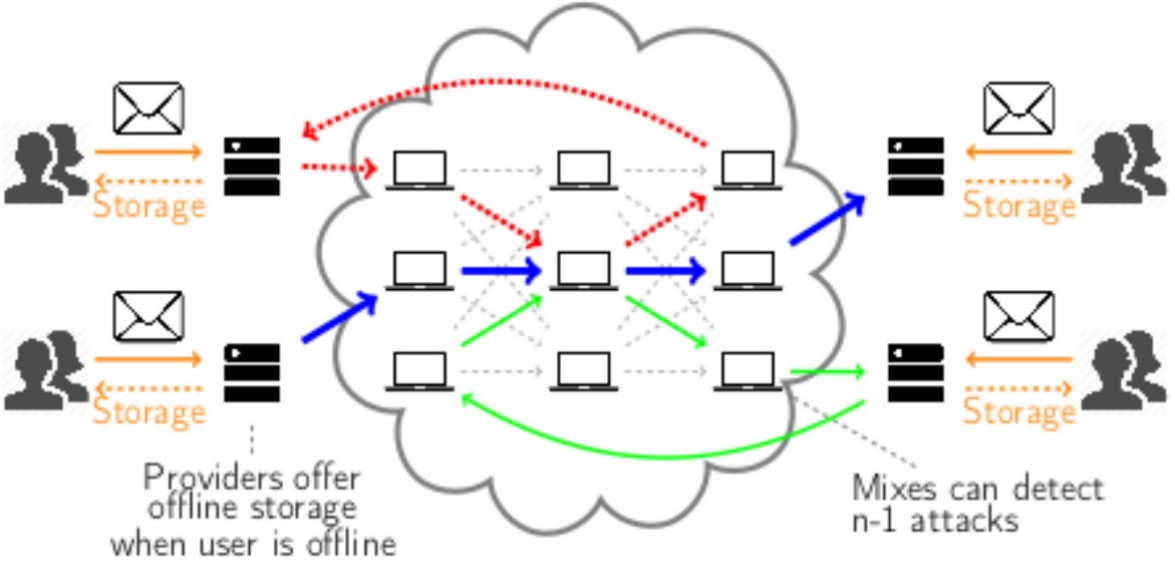


NYM

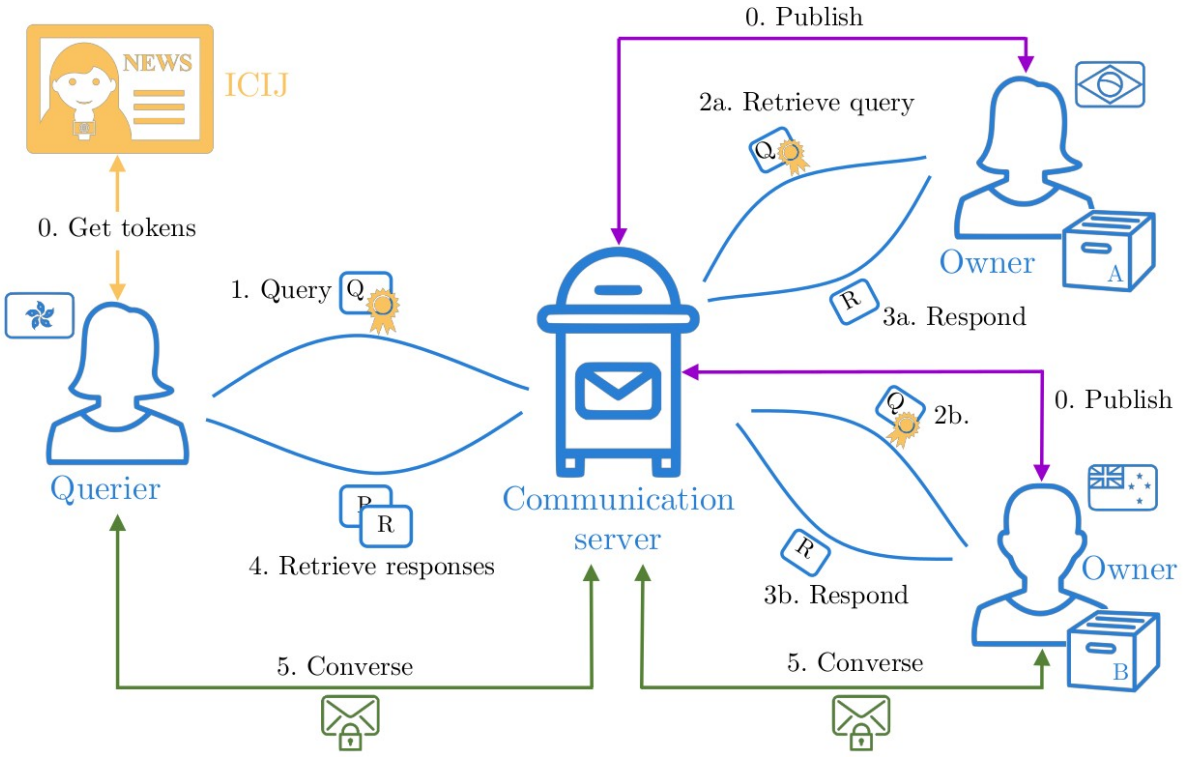
Nym


Data Mixing
+
Timing Obfuscation
Indistinguishable Sphinx packets
Anonymized packets
NYM
Cover traffic
Entry Gateway
Exit Gateway
CLIENT
MIXNET
DESTINATION

Katzenpost


Storage
Storage
Storage
Storage
Providers offer
offline storage
when user is offline
Mixes can detect
n-1 attacks

DataShare Network



Paranoia como forma de vida

Gracias!!

¿Preguntas?

 @feliz1984@mastodon.social

 red@feliz1984.com

 ReD.1984