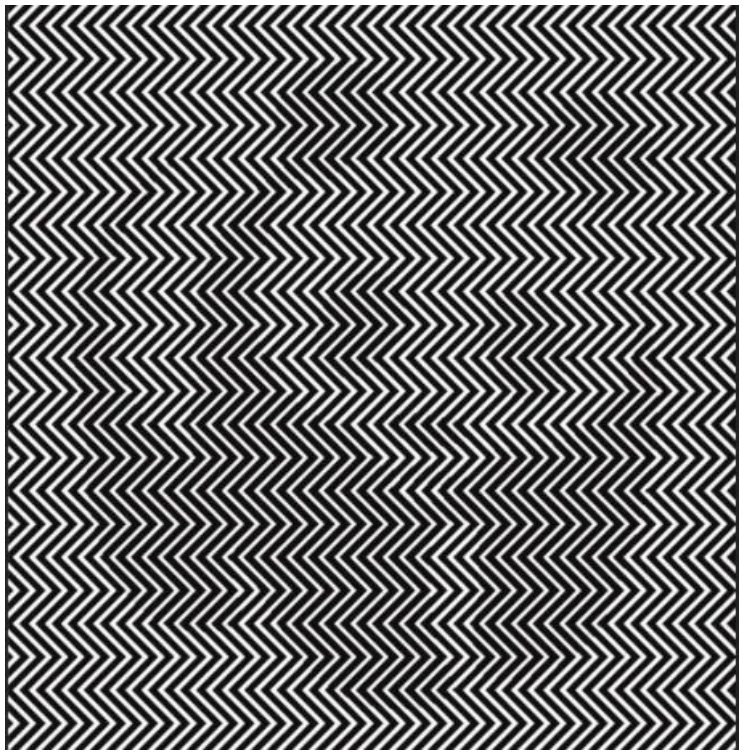
Vigilancia silenciosa
Lo que el cifrado NO esconde



¿Quién soy?

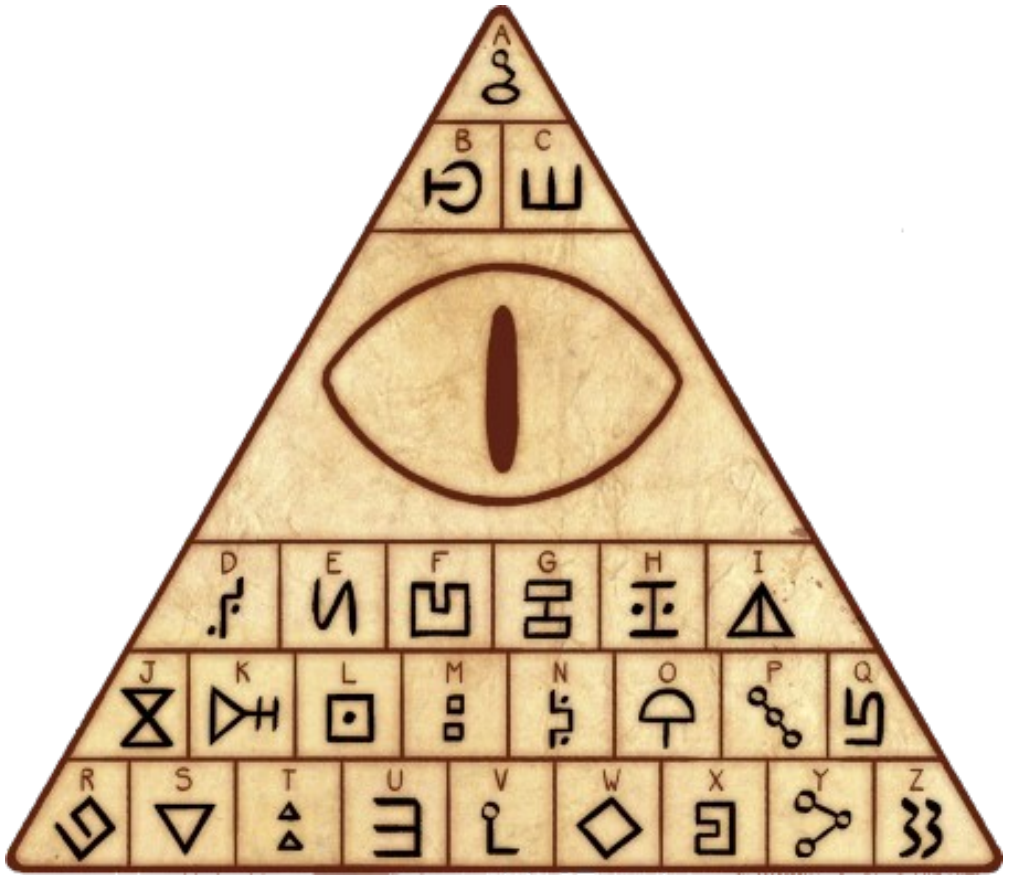
ReD

SecOpsDev

Formador, cuando me dejan

Activista tecnológico

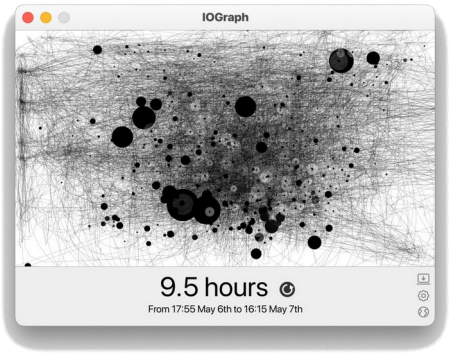
- ✔ Soberanía tecnológica
- ✔ Defensor de la privacidad
- ✔ Cofundador de Hacklabs y M4H

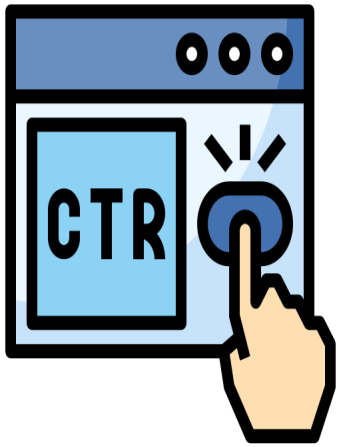


Si está cifrado es seguro

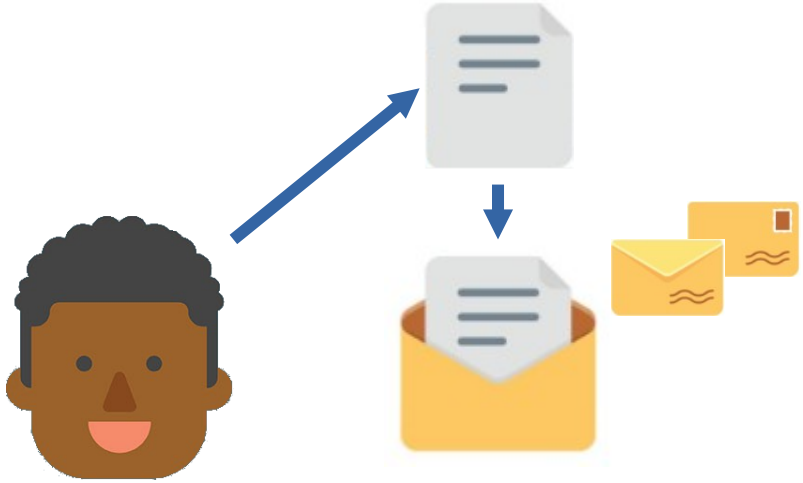
“tiene privacidad”

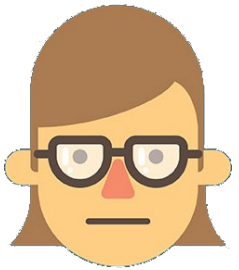
Cómo nos rastrean
Sospechosos habituales



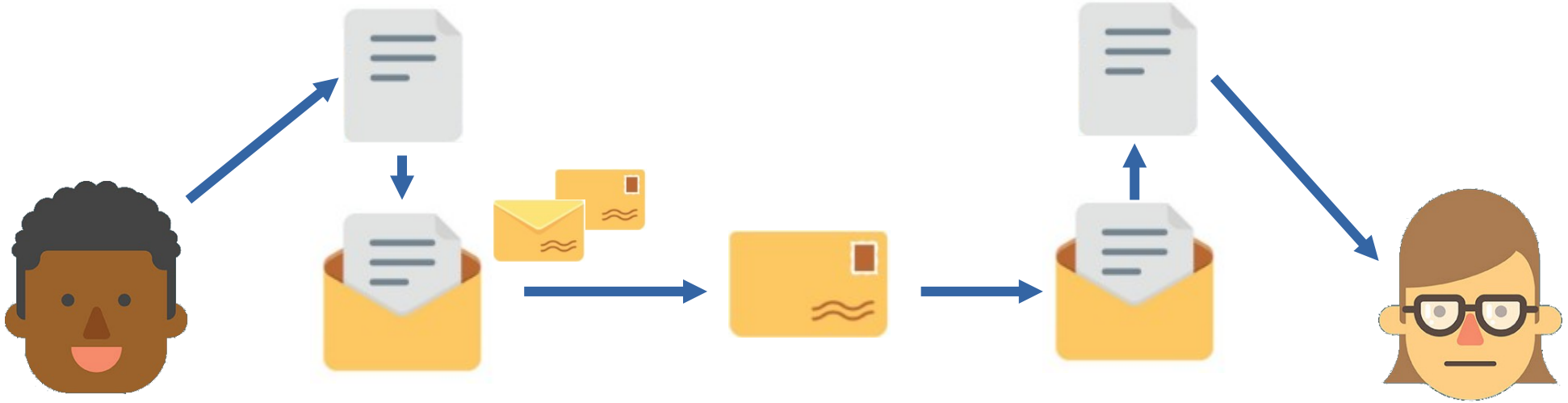


Comunicaciones

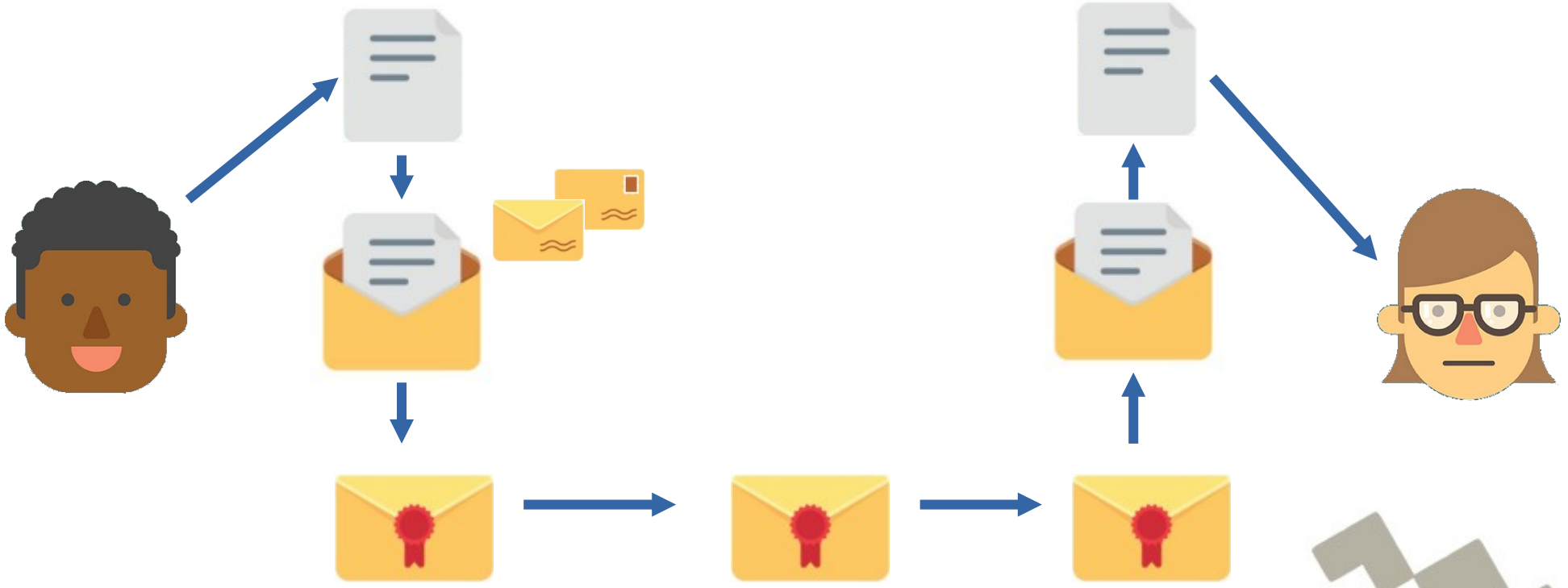




Comunicaciones



Comunicaciones



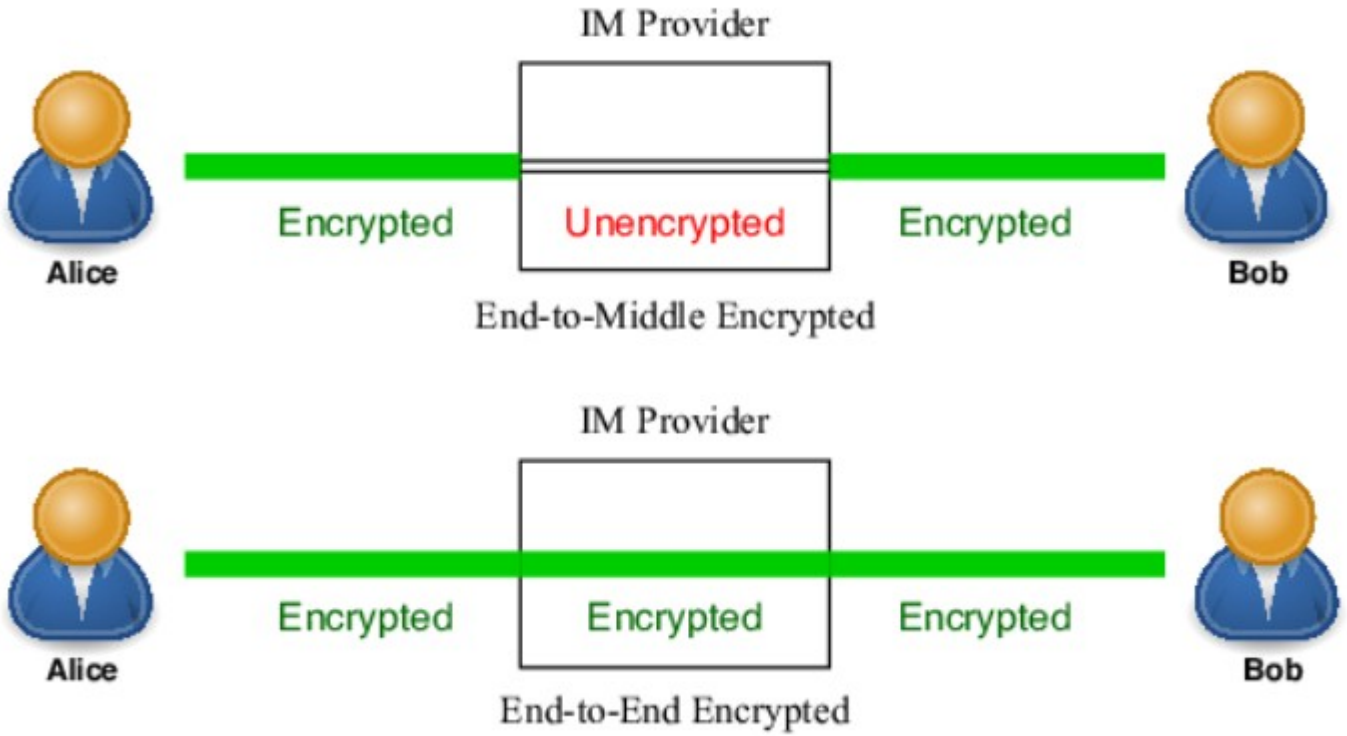
Tipo comunicación

En claro

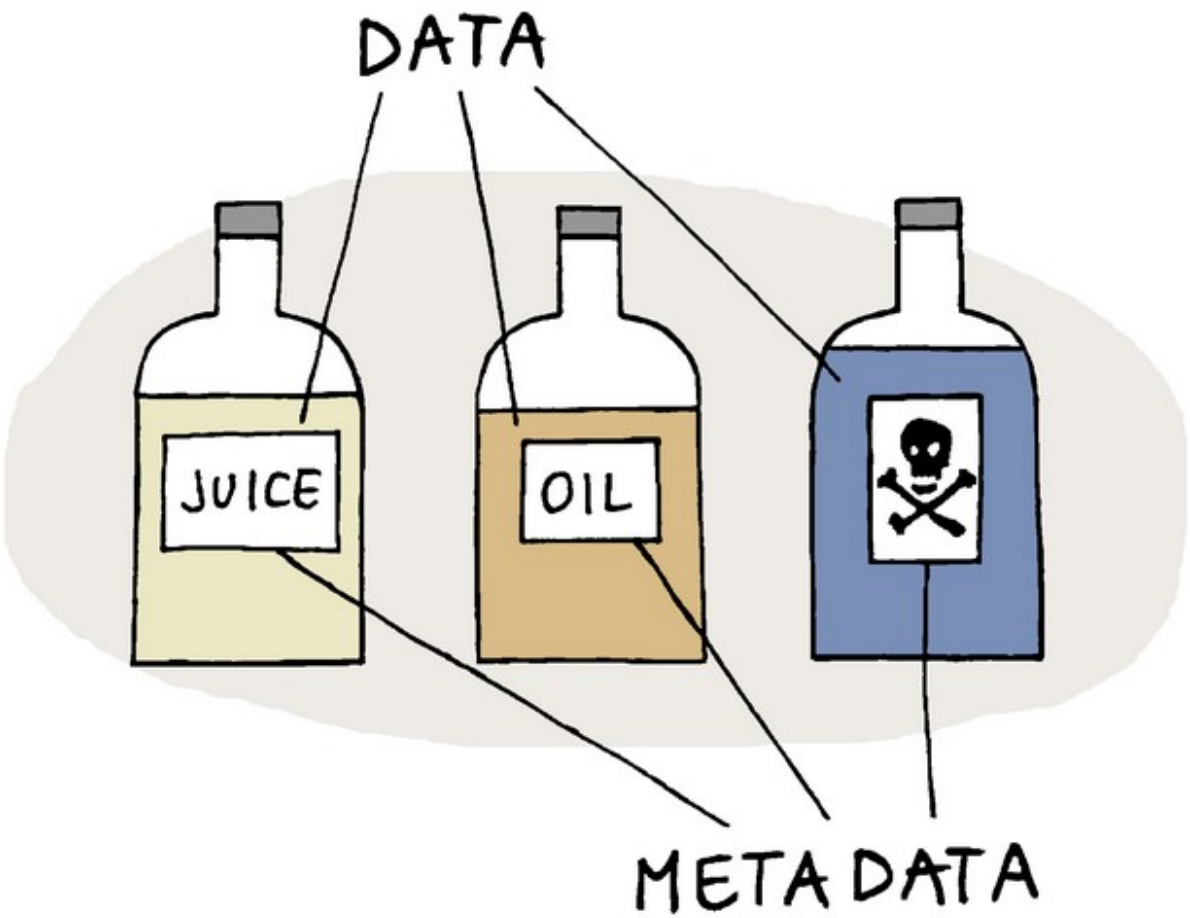
Tipo comunicación

Tipo comunicación

Cifrado E2EE



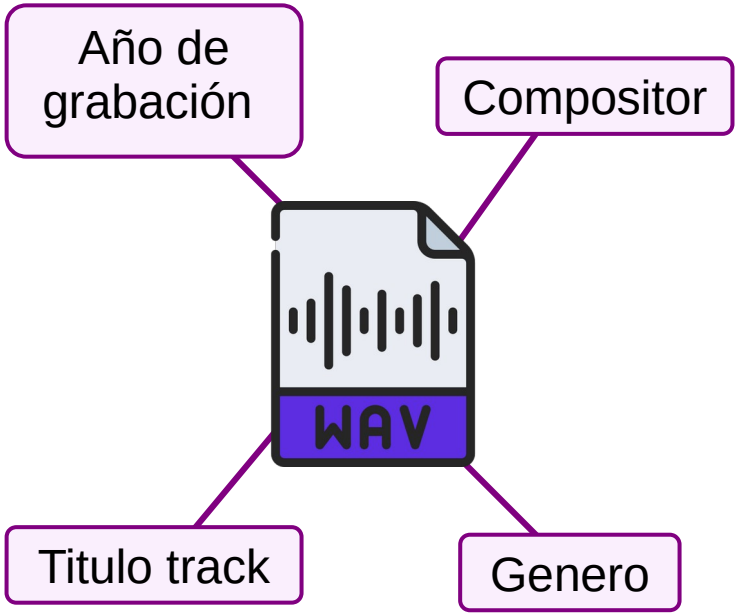
Metadatos en ficheros



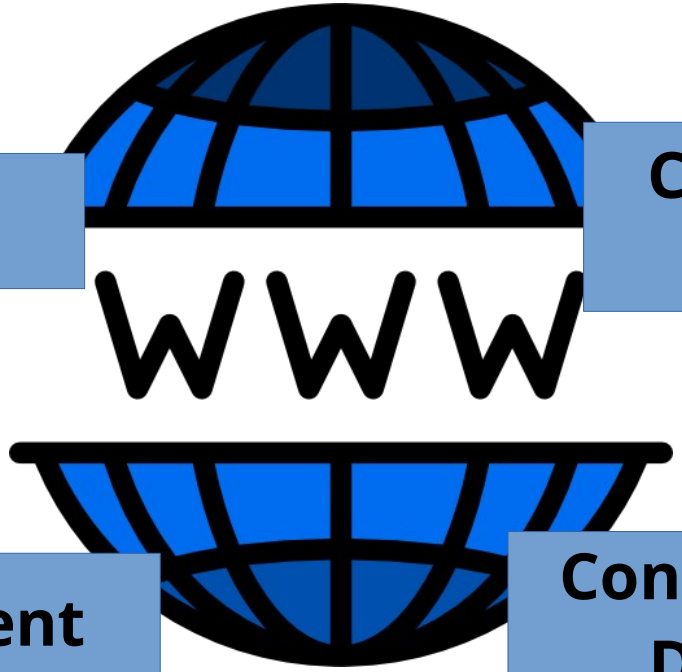
Dataedo /cartoon

PiotrDataedo

Metadatos en ficheros



Metadatos web



URL o URI

Cabeceras HTTP

User-Agent

Consultas DNS

Metadatos en tráfico

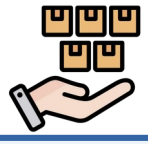
Metadatos en tráfico

Duración

Tiempo

Tipo

Direcciones



Paquetes
Datos

TTL

Timestamp

IP/Puerto

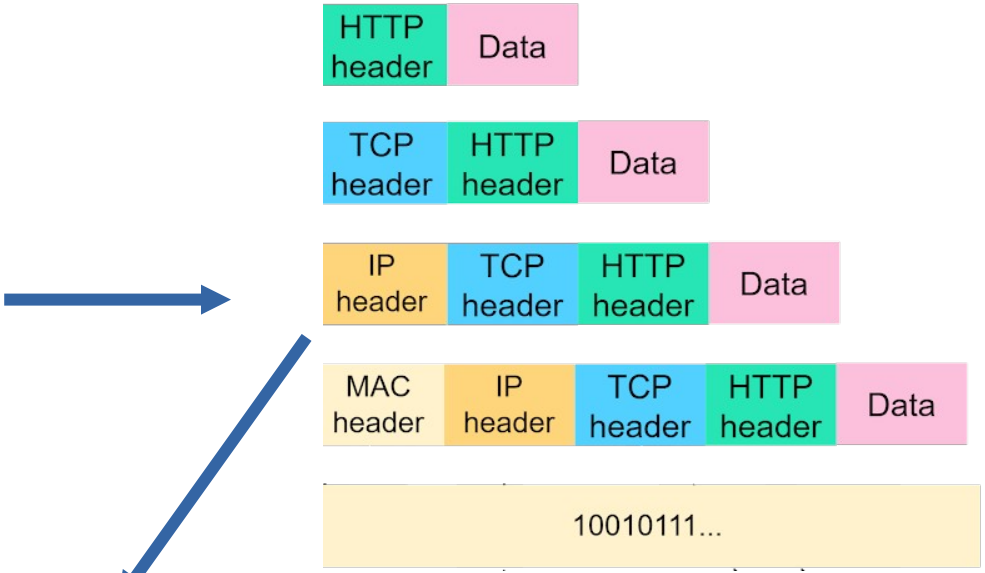
Attachments

Flags

Certificados

Protocolos

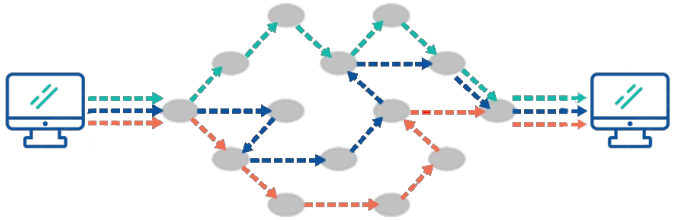
Metadatos



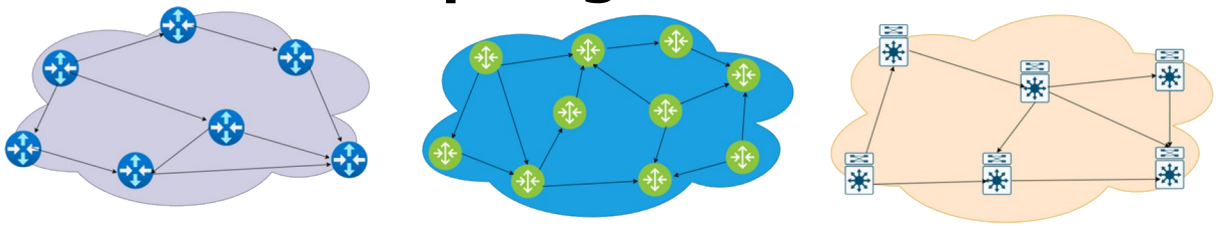
VER 4 bits	HEL 4 bits	Sevice Type 8 bits	Total Length 16 bits	
Datagram Identification 16 bits			Flags 3 bits	Fragment offset 13 bits
Time To Live 8 bits		Protocol 8 bits	Header Checksum 16 bits	
Source IP Address 32 bits				
Destination IP Address 32 bits				
Options				

Metadatos - Análisis

Tráfico



Topología de red

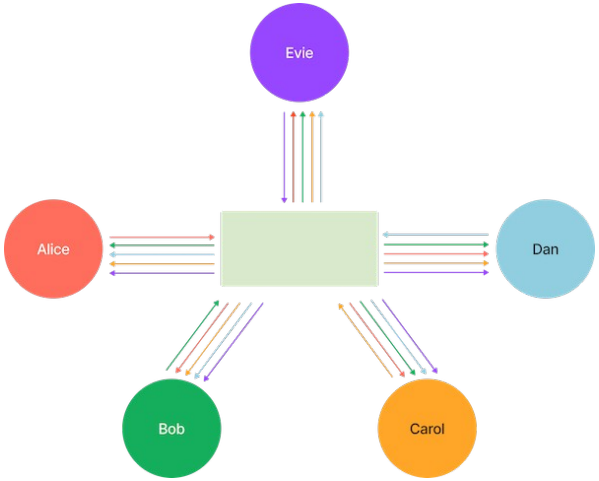


Donde ocurre la comunicación

Metadatos - Análisis

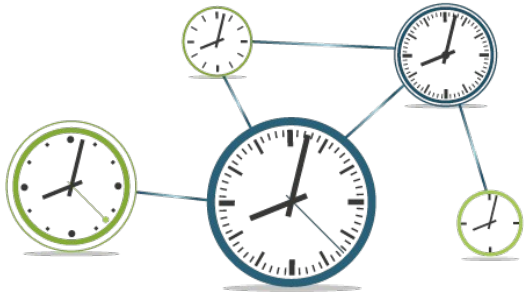
Tamaño de paquetes

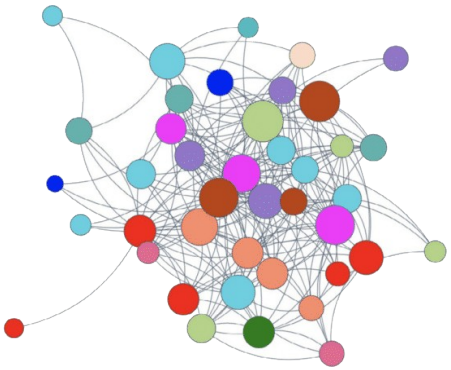
Correlación



Metadatos - Análisis

Frecuencia de conexiones





Duración de las conexiones

Huella dactilar

Metadatos - Análisis

Información del Certificado

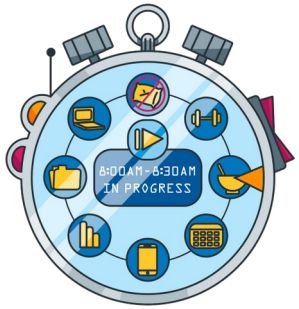
Patrones de handshake y renegociación

Metadatos
Resultados finales

Perfilado detallado

Identificación indirecta

Correlación de perfiles



Saber rutinas y hábitos

Análisis de metadatos

- **Inspección profunda de paquetes (DPI)**
- **Sistemas de análisis de tráfico de red (NTA)**

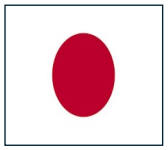
Metadatos del paquete

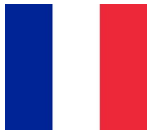
Carga útil

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


MITA

SORM 

G10 Gesetz 

BÜPF 

CALEA 

SSL/TLS

Conjuntos de algoritmos “suites de cifrado"

- Algoritmos de intercambio de claves
- Algoritmos de autenticación
- Algoritmos de cifrado de datos
- Funciones de hash (integridad)

ECDHE-ECDSA-AES128-GCM-SHA256

SSL/TLS

ECDHE_DES_AES_128_CBC_SHA

ECDHE_ECDSA_AES_128_GCM_SHA256

ECDH_RC4_WITH_AES_128_GCM_SHA256

DHE_RSA_WITH_AES_256_GCM_SHA384

RSA_WITH_3DES_CBC_SHA

DHE_ECDSA_WITH_AES_128_CBC_MD5_P256

ECDHE-ECDSA-AES128-GCM-SHA256

SSL/TLS

ECDHE_DES_AES_128_CBC_SHA

ECDHE_ECDSA_AES_128_GCM_SHA256

ECDH_RC4_WITH_AES_128_GCM_SHA256

DHE_RSA_WITH_AES_256_GCM_SHA384

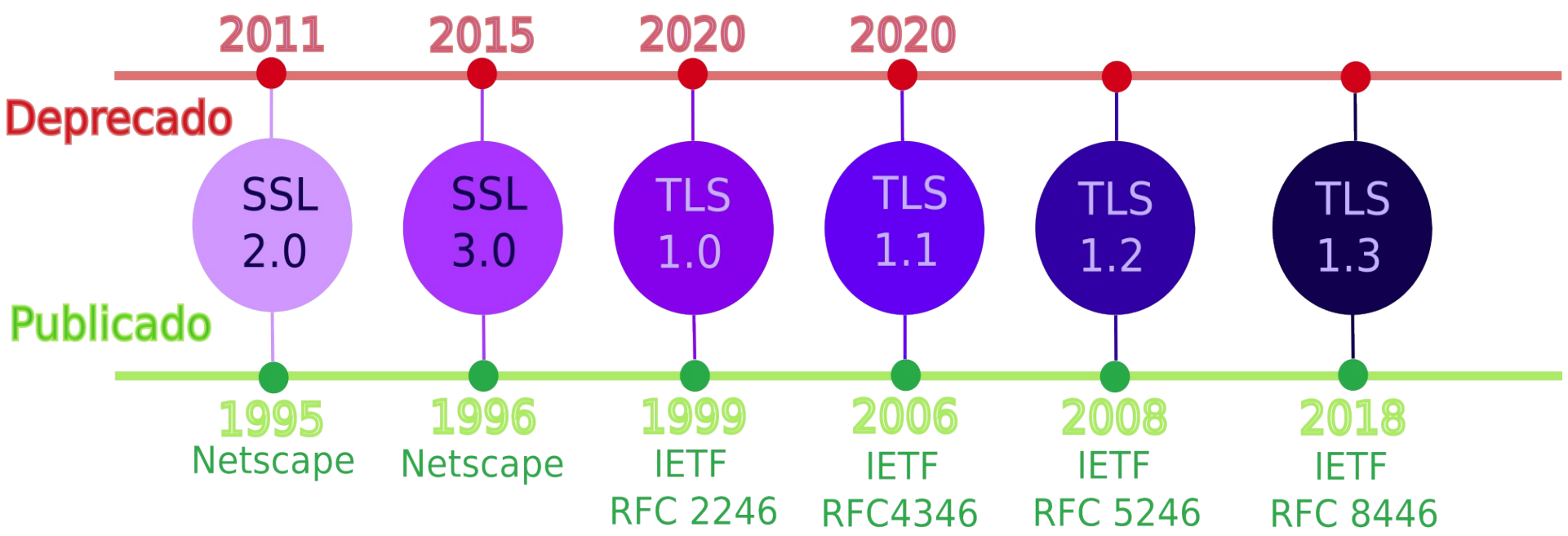
RSA_WITH_3DES_CBC_SHA

DHE_ECDSA_WITH_AES_128_CBC_MD5_P256

"No oculta metadatos de las comunicaciones"

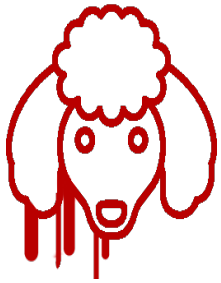
ECDHE-ECDSA-AES128-GCM-SHA256

Historia de TLS



*** Internet Engineering TaskForce**

Ataques contra TLS



Defectos conceptuales

3SHAKE, TLS Renego MITM, CANICHE, ATOLLADERO, FENÓMENO, POODLE, LOGJAM, FREAK

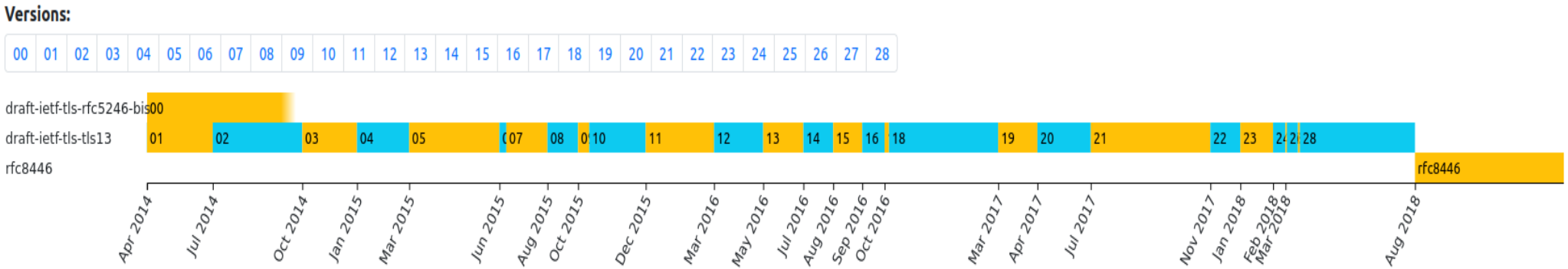
Primitivas criptográficas débiles

Sweet32, ROBOT, LUCKY13

Implementación de TLS

BEAST, Faulty CBC padding , CRIMEN, BREACH, TIME, HEIST, SLOTH, DROWN ATTACK, SMACK, ROCA, HEARTBLEED, ALPACA

Historia de TLS 1.3



2013 Lista de deseos - Eric Rescorla

TLS 1.3

Algoritmos de hash antiguos

MD5, SHA-1

Sistemas de cifrado antiguos

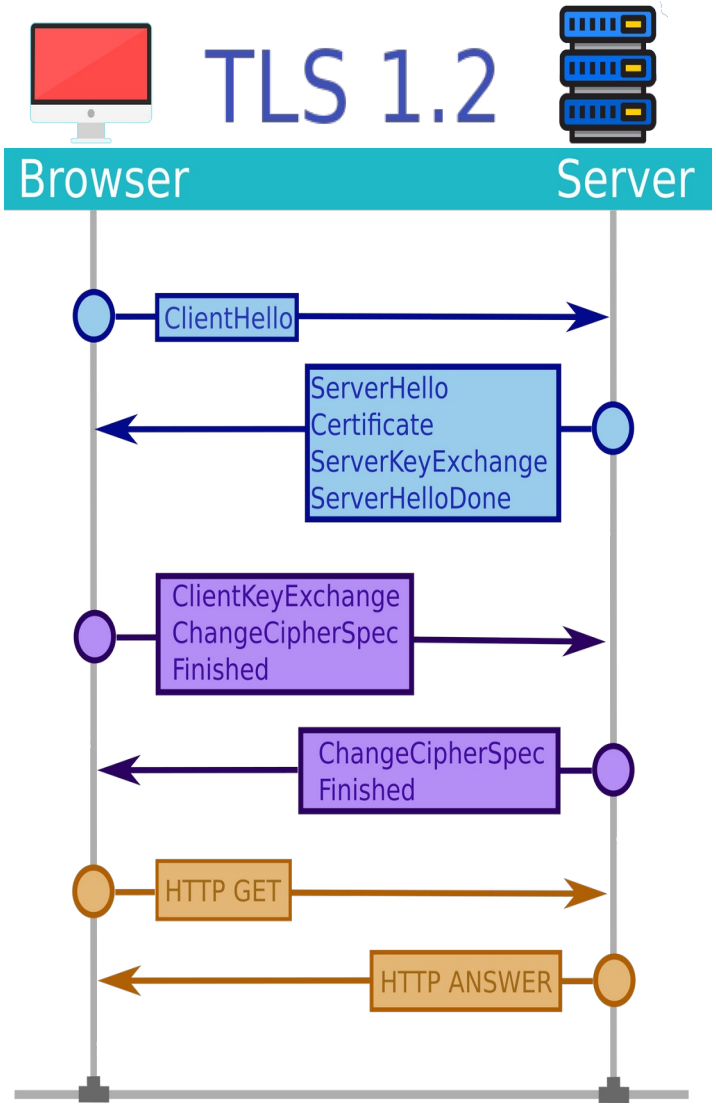
RC4, DES, 3DES

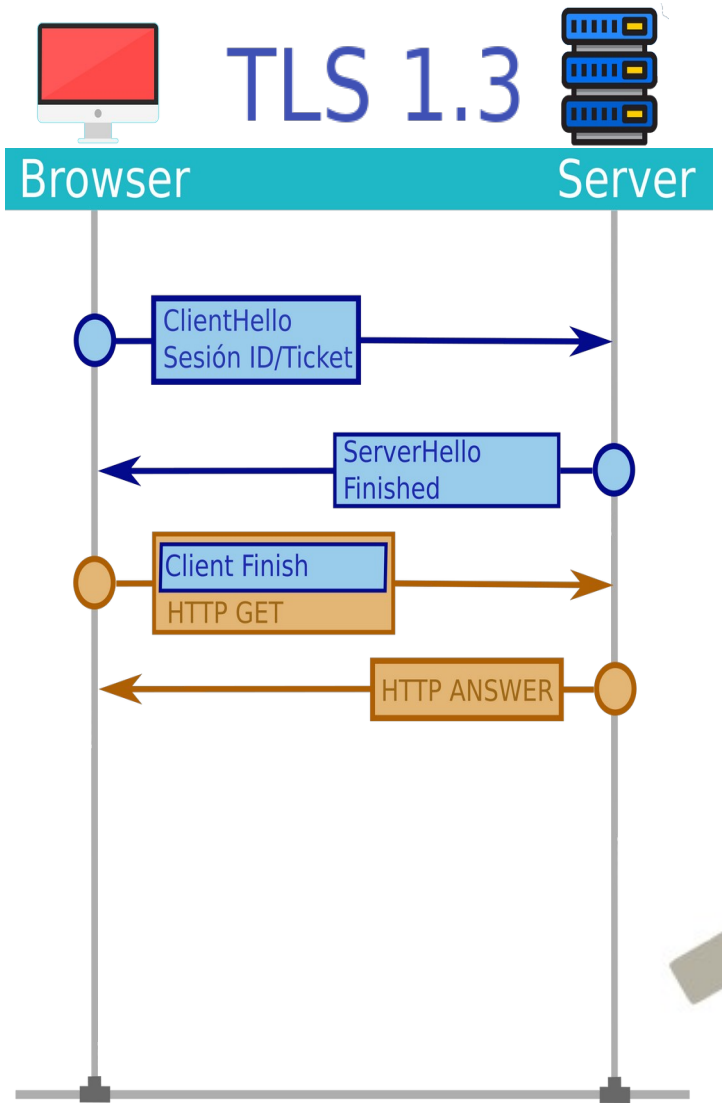
Cifadro simétrico que utiliza modos de bloque CBC

AES-CBC

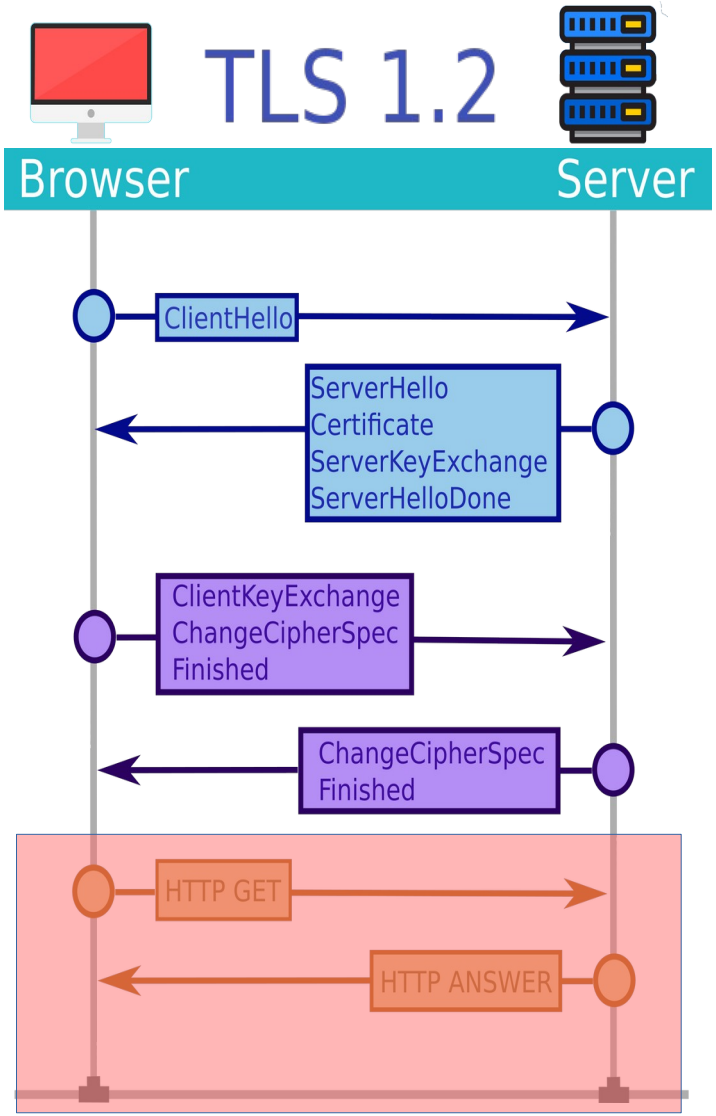
Grupos Diffie-Hellman arbitrarios no efímeros

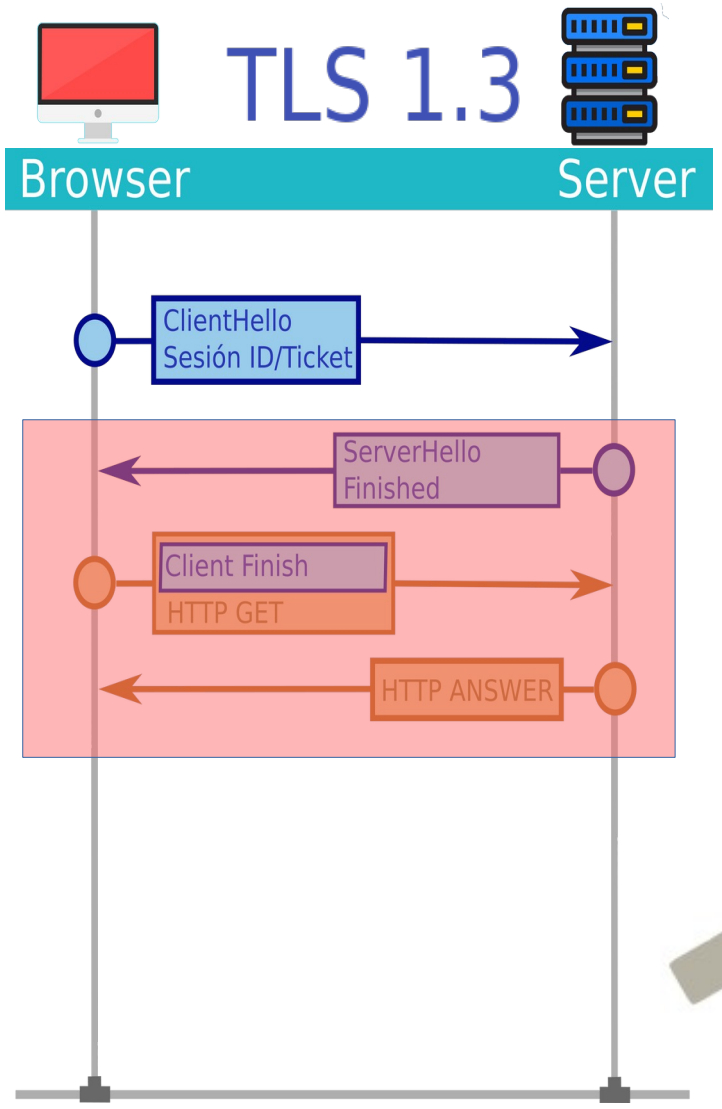
Comparativa TLS





Comparativa TLS





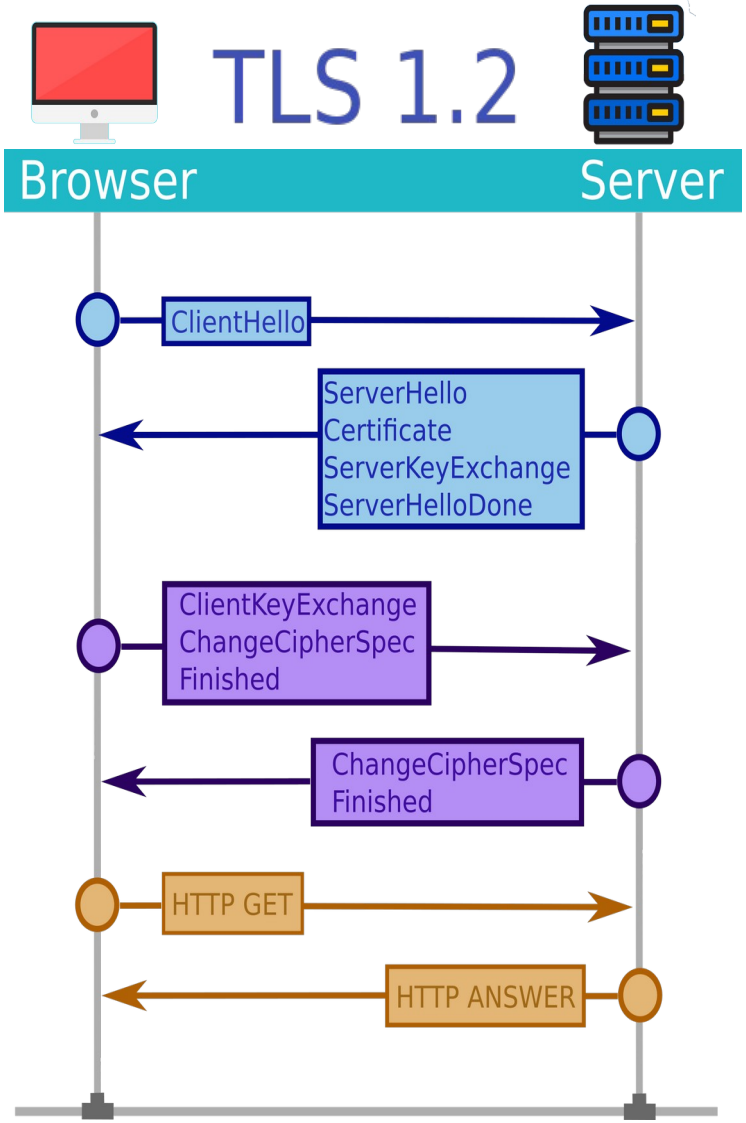
TLS más rápido

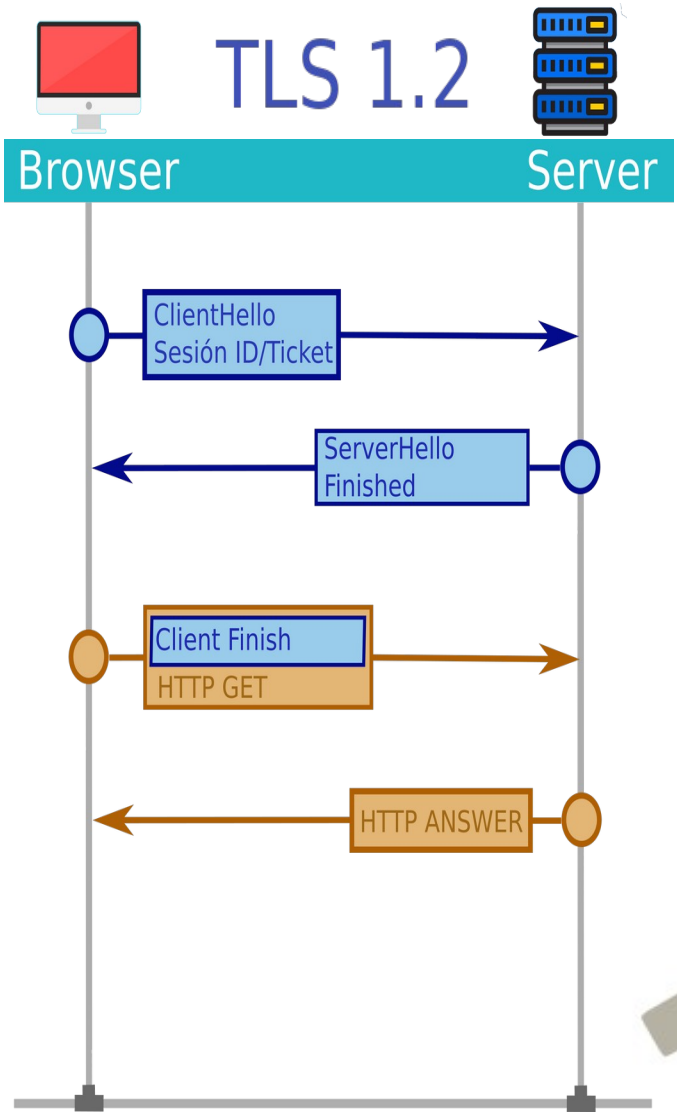
TLS más rápido

Google

Meta

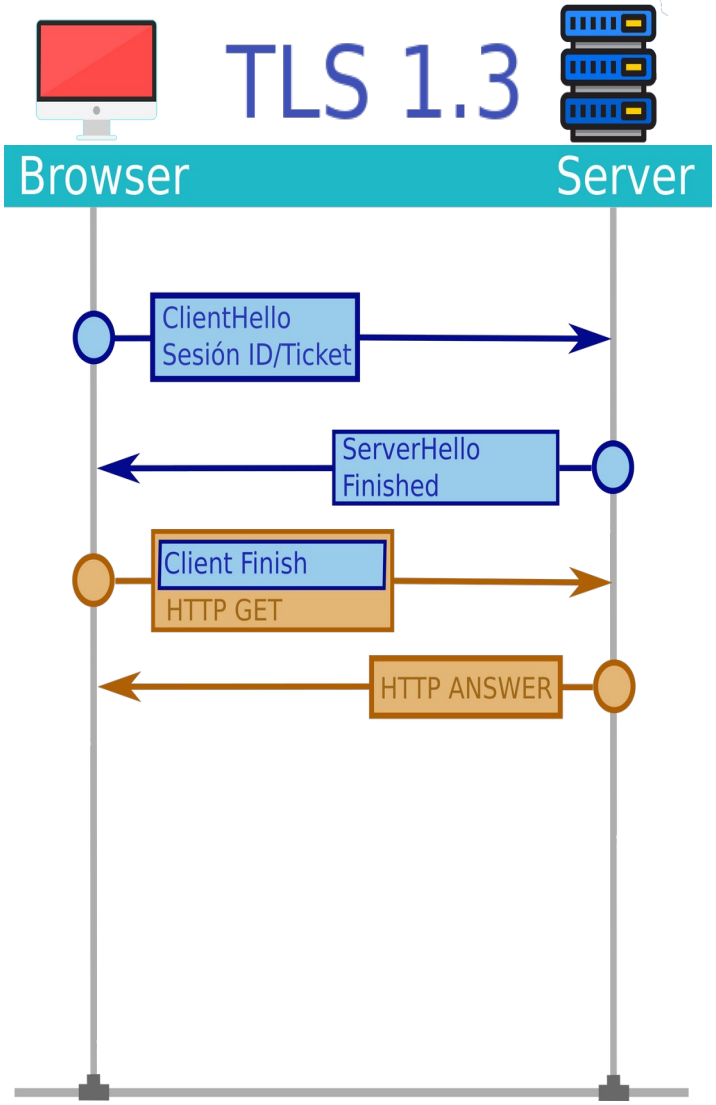
Cacheo TLS 1.2

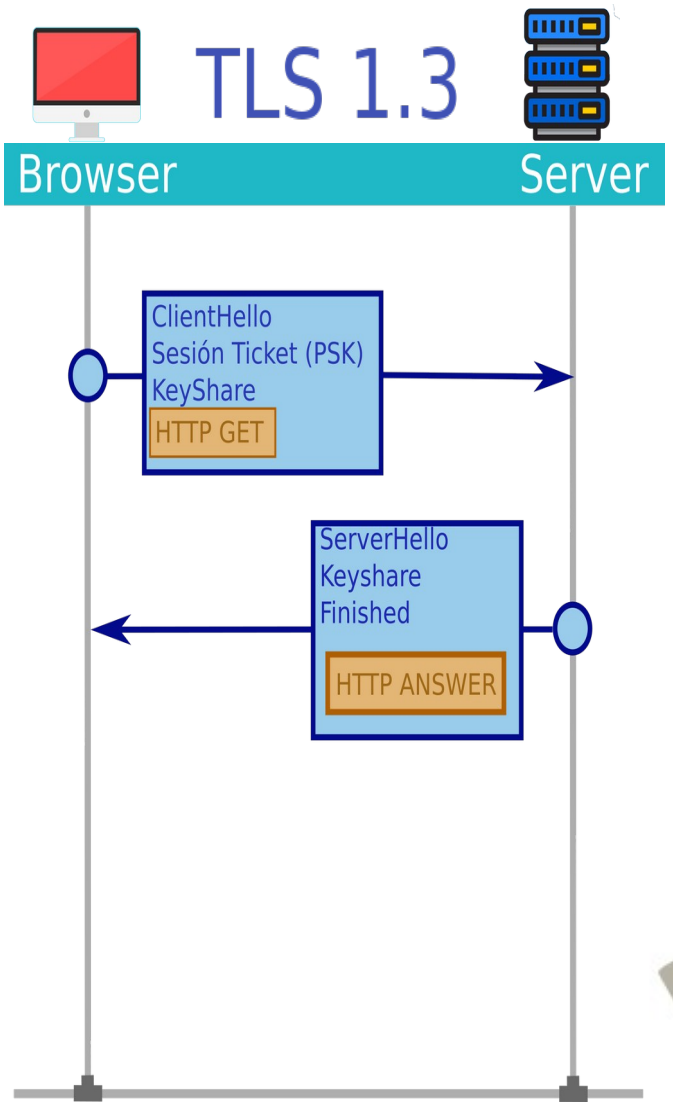




Session ids/tickets
2 RTT → 1RTT

Cacheo TLS 1.3





PKS

1 RTT → 0RTT

Siguiendo usuarios Reanudación

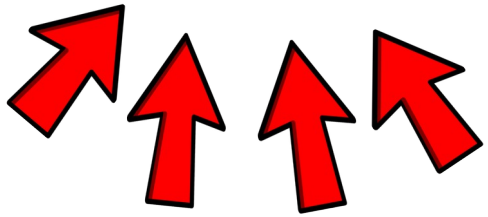
- Estudio de la universidad de Hamburgo
- Funciona como cookie
- Seguimiento por PSK desde el servidor (da igual IP)

Siguiendo usuarios
Reanudación

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

Siguiendo usuarios
Reanudación

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



Siguiendo usuarios
Reanudación

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

Siguiendo usuarios
Reanudación

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

Se complica “demasiado”

Siguiendo usuarios
Reanudación

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

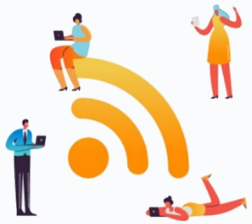
Siguiendo usuarios
Reanudación

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

Interés en perfilado

orange™

TrustPid



utiq

Interés en perfilado

TrustPid

Ayudando a mantener Internet gratis

El contenido online suele ser gratuito gracias a la publicidad, los muros de pago y las suscripciones utilizando direcciones de correo electrónico registradas.

Al dar tu consentimiento a TrustPid, ayudas a mantener el contenido de Internet gratuito.

Interés en perfilado

Qué podemos hacer

- **Uso de herramientas de anonimización**
- **Minimización de metadatos**
- **Educación y concienciación**

Debemos buscar tecnologías y políticas que minimicen la recopilación de metadatos y aseguren que su uso sea transparente y ético.

Los metadatos son tan valiosos como el contenido

Gracias

¿Preguntas?

 @feliz1984@mastodon.social

 @ReD.1984

 red@feliz1984.com