NAVAJA NEGRA

TLS
Aumento de seguridad, disminución de privacidad

NAVAJA NEGRA

ReD

SecOpsDev
Formador, cuando me dejan

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

“arte de vivir en sociedad”

NAVAJA NEGRA

Como me gusta el olor a criptografía por la mañana

The Design and Implementation of the Tor Browser [DRAFT]

3.3. Adversary Capabilities - Attacks

The adversary can perform the following attacks from a number of different positions to accomplish various aspects of their goals. It should be noted that many of these attacks (especially those involving IP address leakage) are often performed by accident by websites that simply have JavaScript, dynamic CSS elements, and plugins. Others are performed by ad servers seeking to correlate users' activity across different IP addresses, and still others are performed by malicious agents on the Tor network and at national firewalls.

1. **Read and insert identifiers**

   The browser contains multiple facilities for storing identifiers that the adversary creates for the purposes of tracking users. These identifiers are most obviously cookies, but also include HTTP auth, DOM storage, cached scripts and other elements with embedded identifiers, client certificates, and even TLS Session IDs.

NAVAJA NEGRA

Ataques contra TLS

Defectos conceptuales

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

Primitivas criptográficas débiles

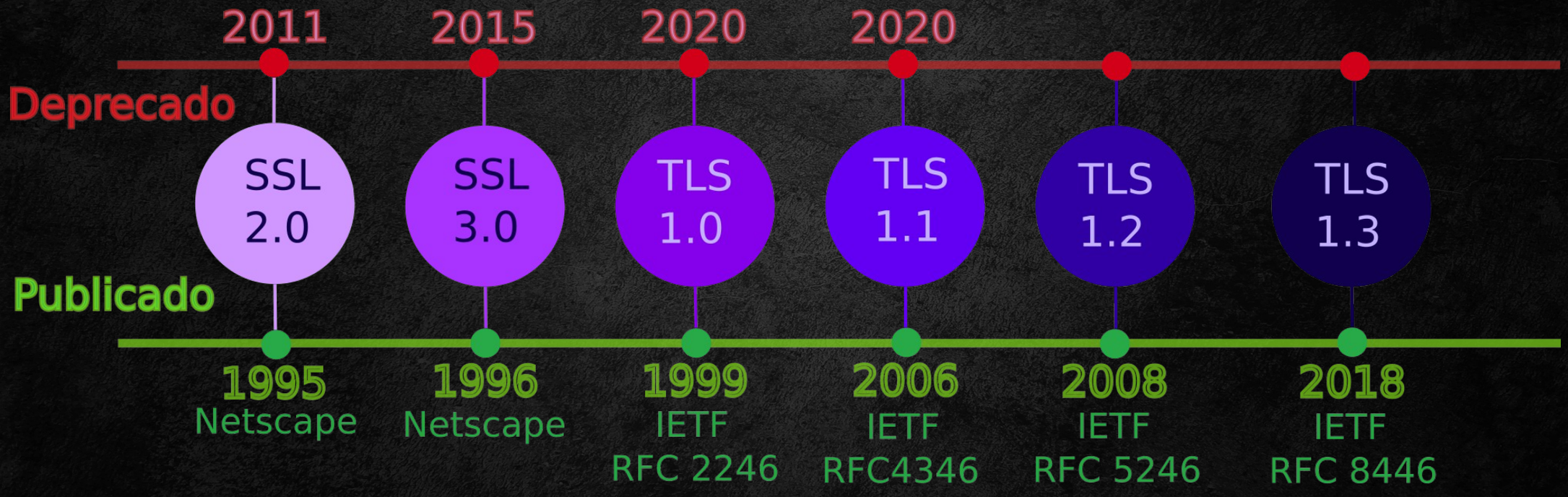
Sweet32, ROBOT, LUCKY13

Implementación de TLS

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

NAVAJA NEGRA

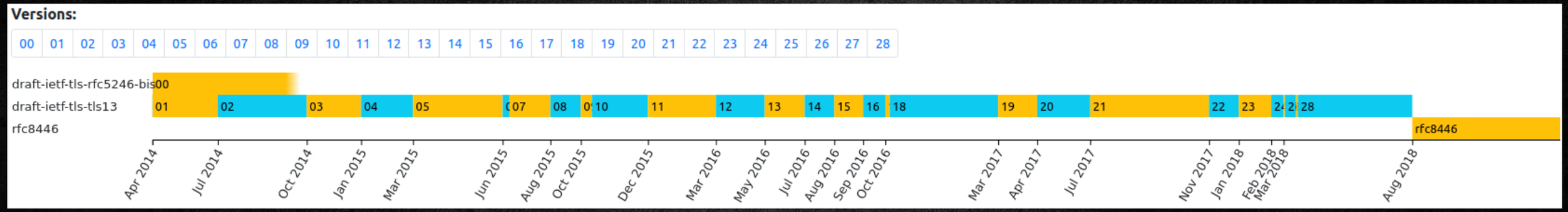
Historia de TLS



* Internet Engineering TaskForce

NAVAJA NEGRA

TLS 1.3



2013 Lista de deseos - Eric Rescorla

NAVAJA NEGRA

Que es SSL/TLS

Secure Socket Layer

Protocolo criptografico que provee seguridad sobre redes computacionales

Transport Layer Security

Sucesor al SSL

NAVAJA NEGRA

Uso de TLS

Web

HTTP + TLS = HTTPS

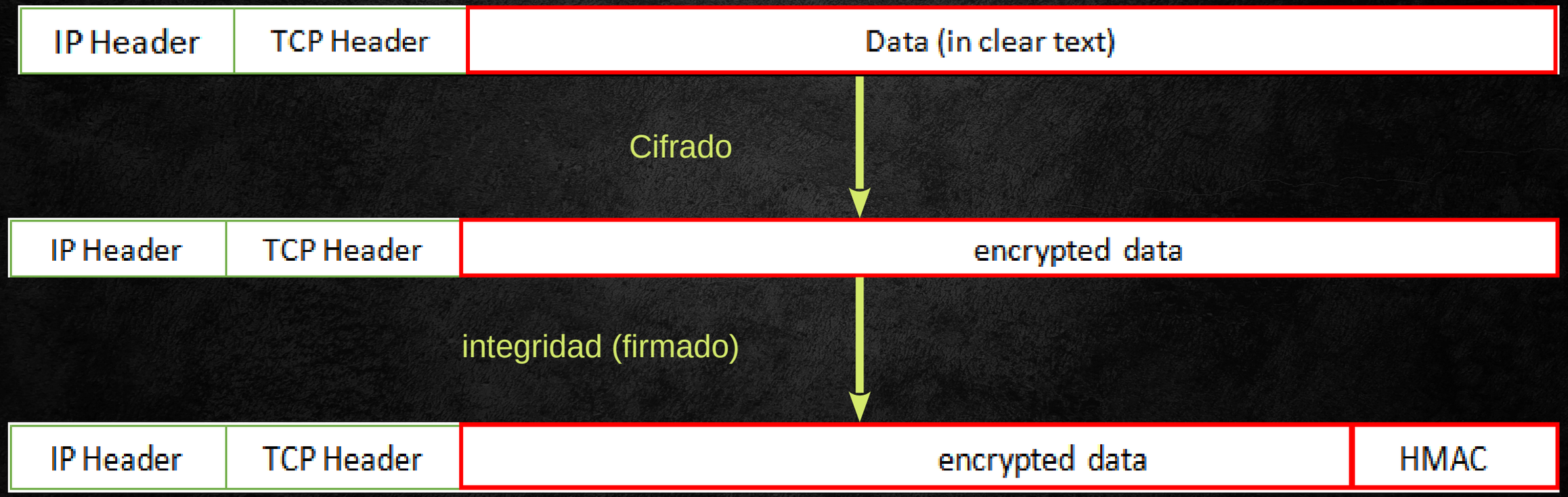
Email

SMTP + TLS = SMTPS

File Transfer

FTP + TLS = FTPS

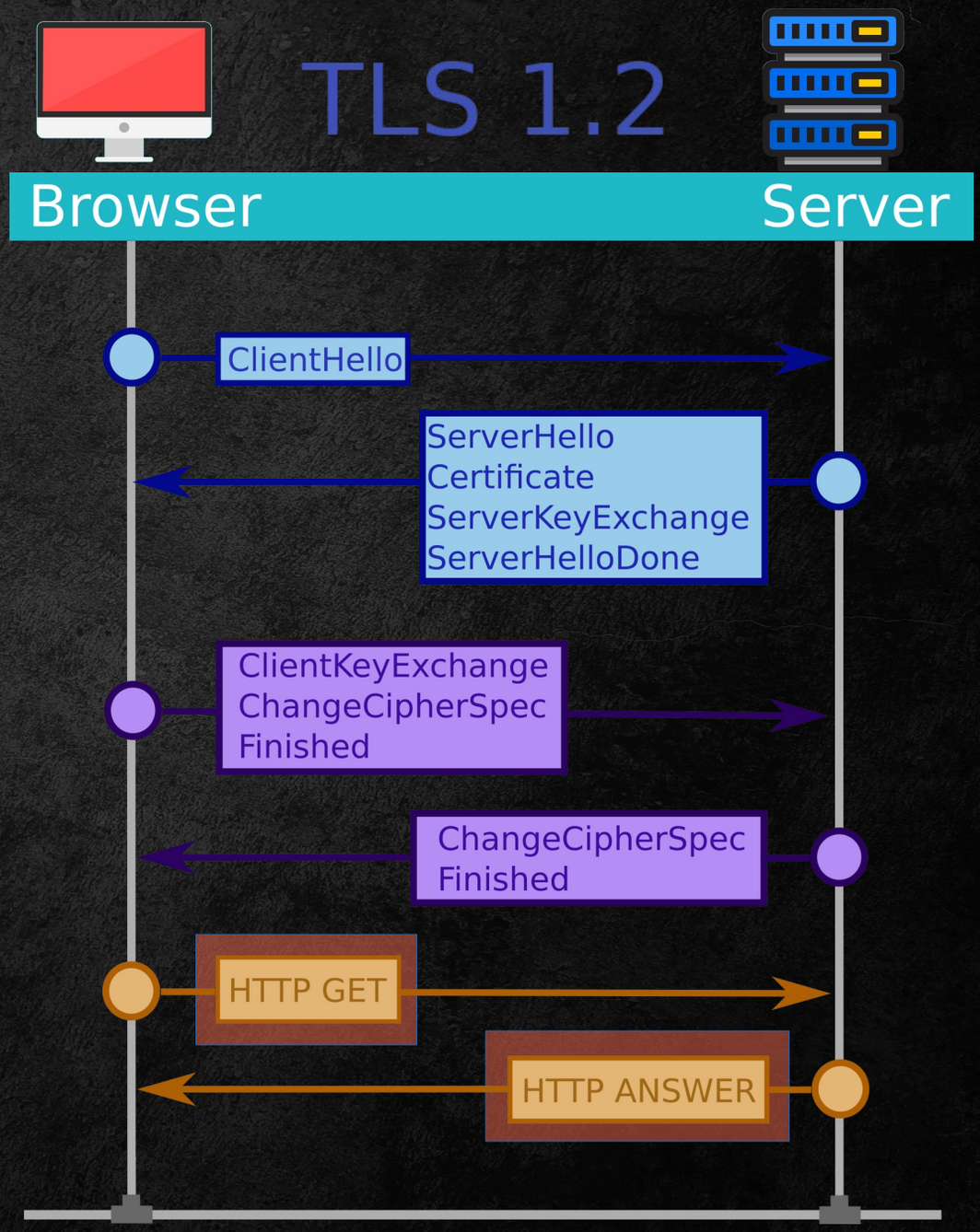
TLS


IP Header
TCP Header
Data (in clear text)
Cifrado
IP Header
TCP Header
encrypted data
integridad (firmado)
IP Header
TCP Header
encrypted data
HMAC

NAVAJA NEGRA

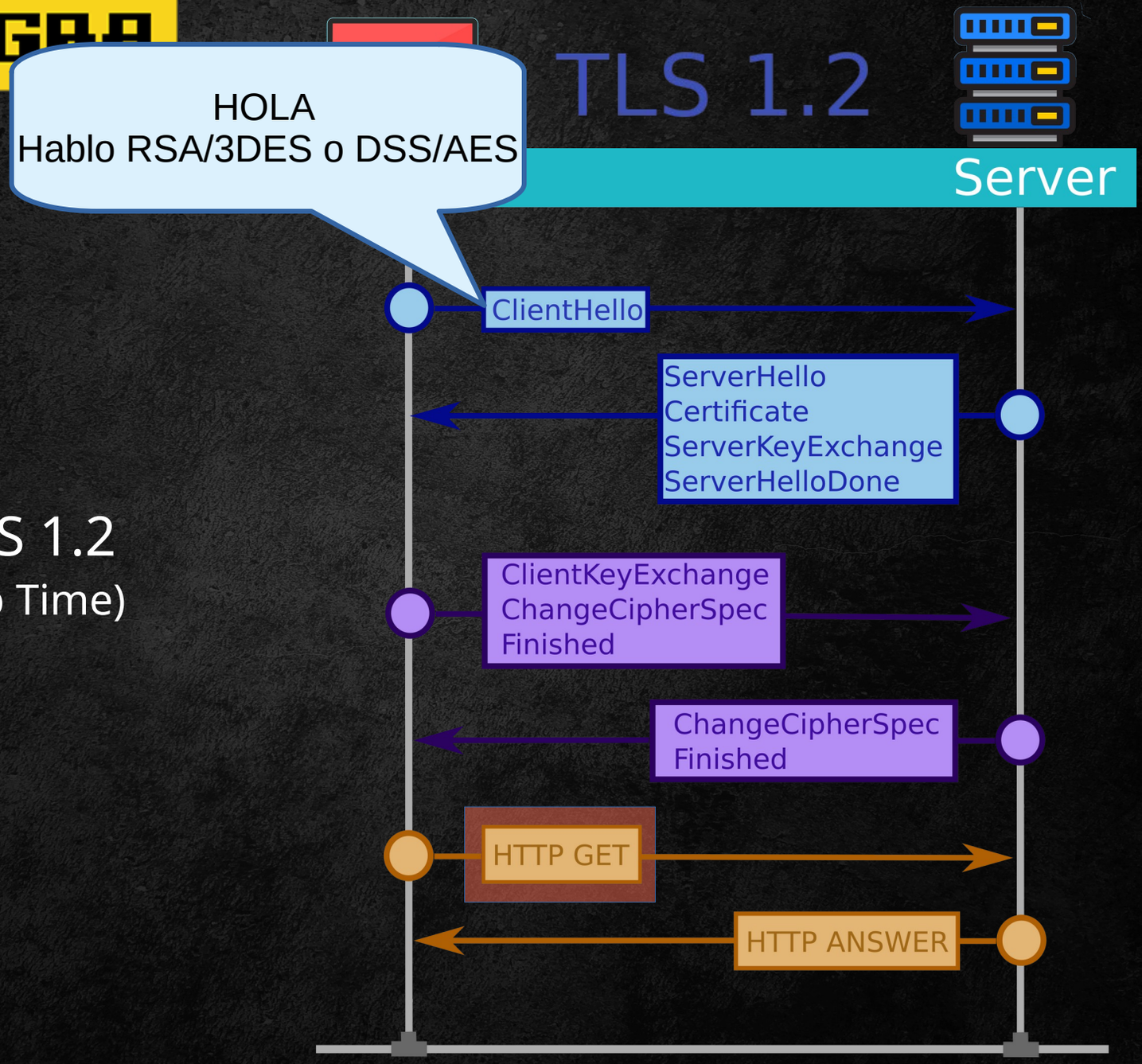
Handshake TLS 1.2

2 RTT (Round Trip Time)



Handshake TLS 1.2

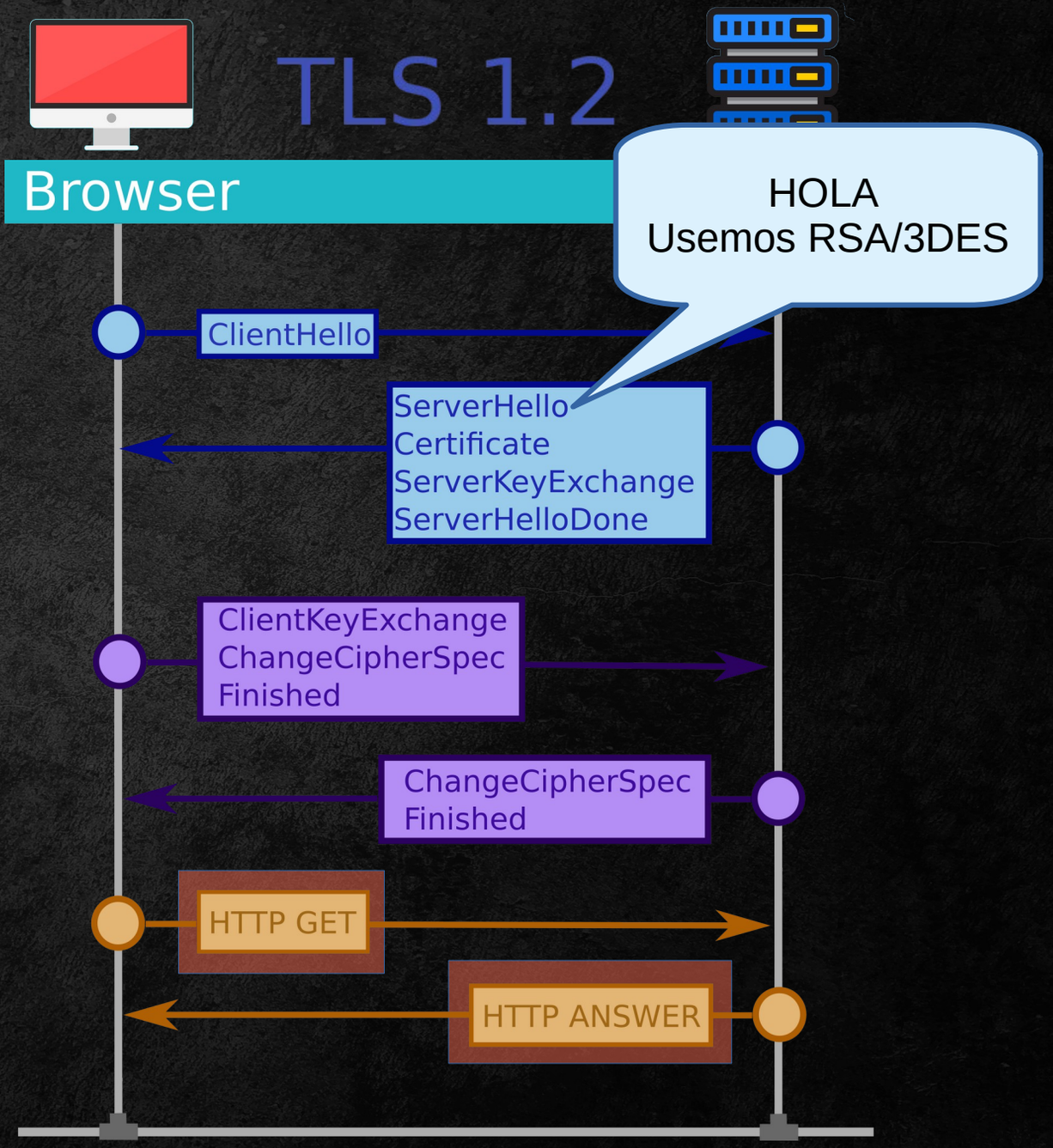
2 RTT (Round Trip Time)



NAVAJA NEGRA

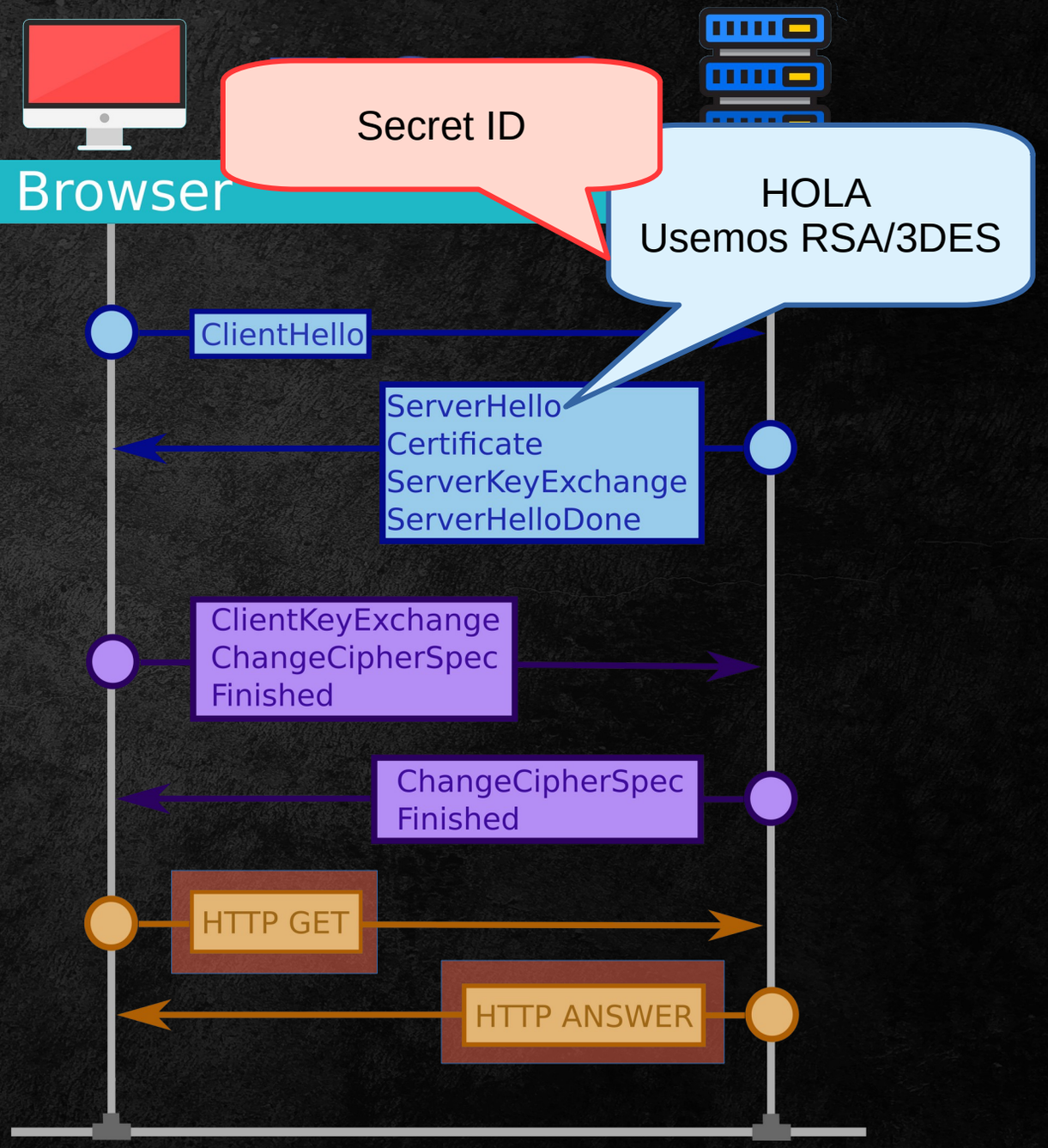
Handshake TLS 1.2

2 RTT (Round Trip Time)



NAVAJA NEGRA

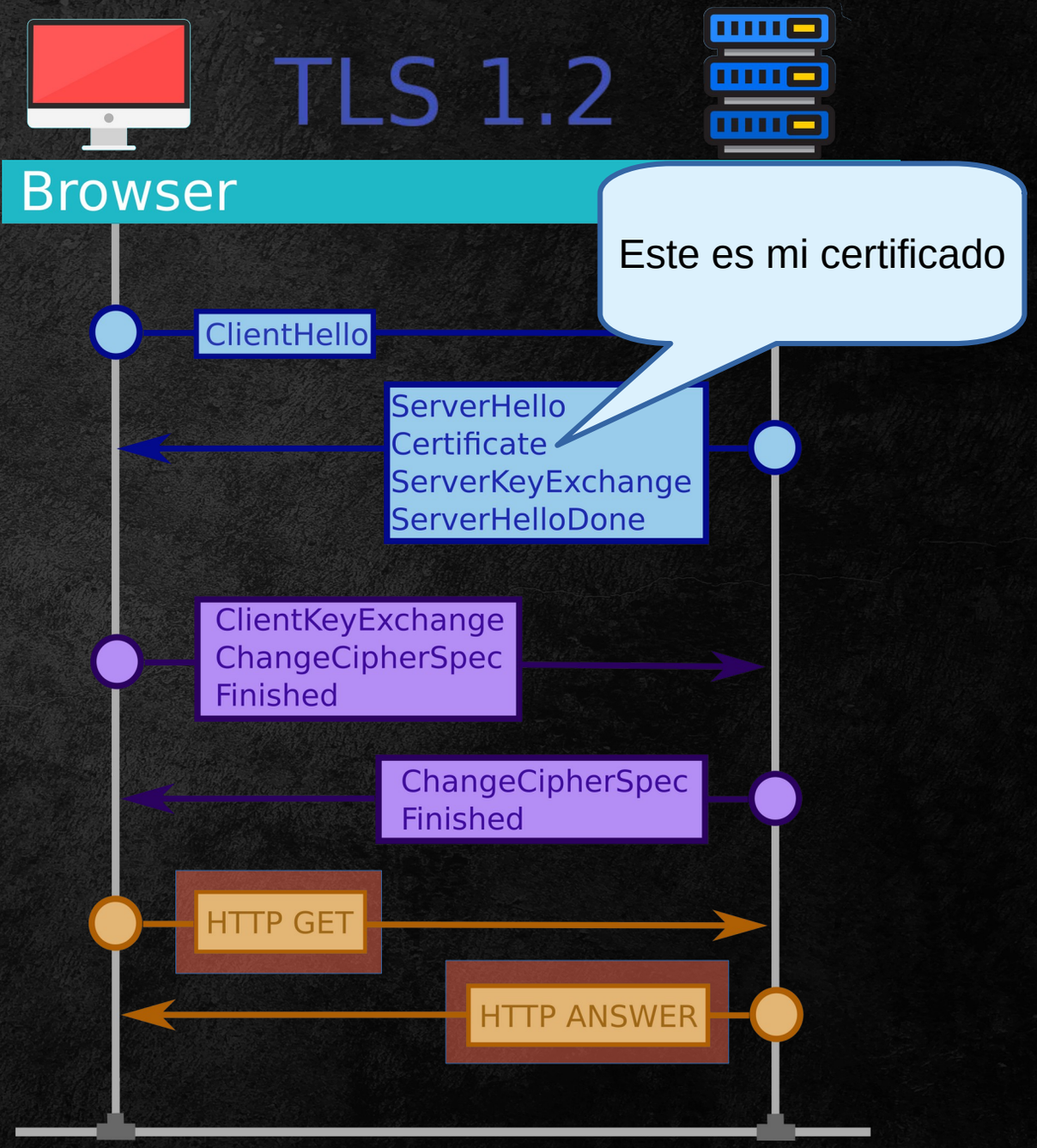
Handshake TLS 1.2
2 RTT (Round Trip Time)



NAVAJA NEGRA

Handshake TLS 1.2

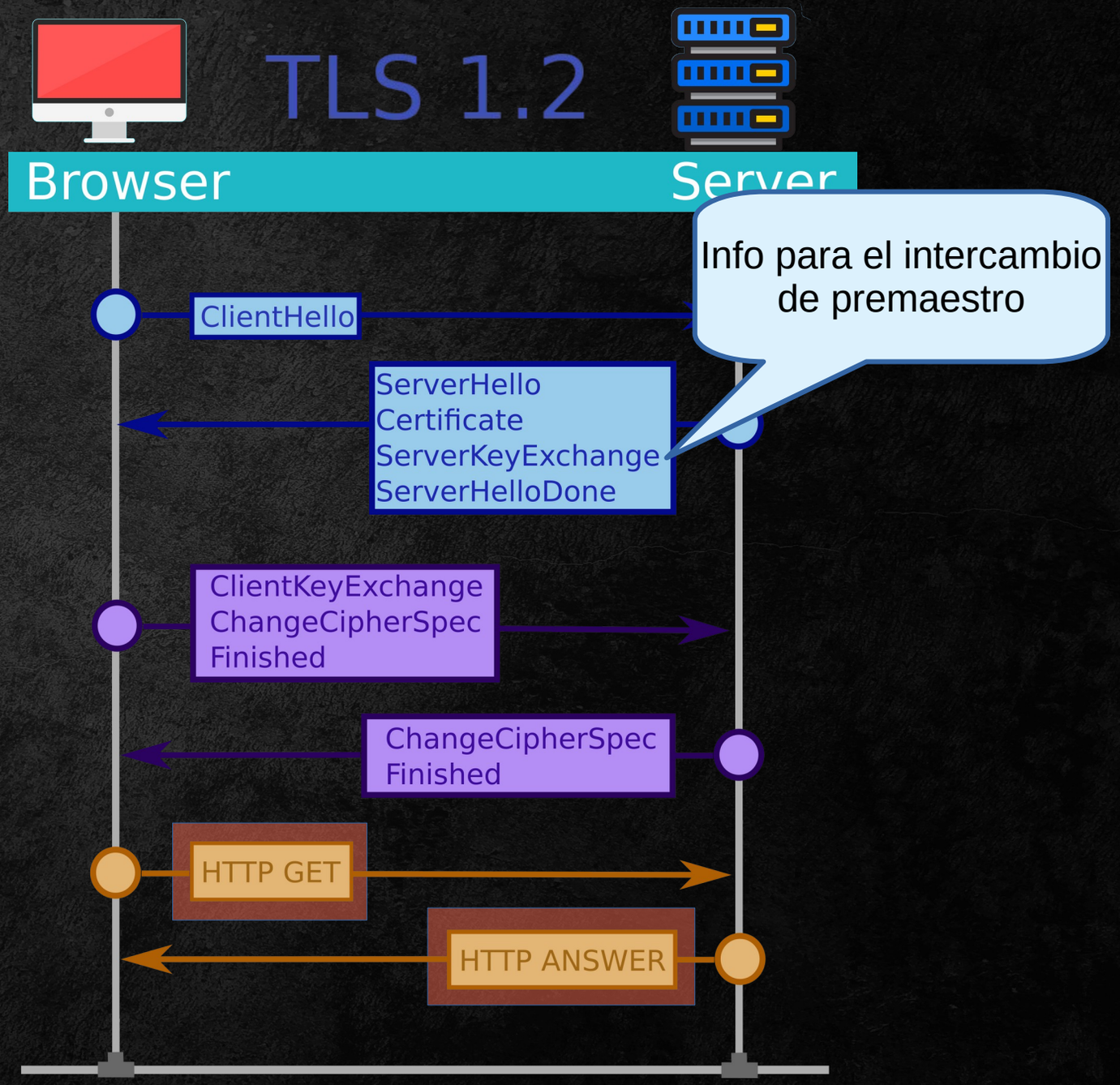
2 RTT (Round Trip Time)



NAVAJA NEGRA

Handshake TLS 1.2

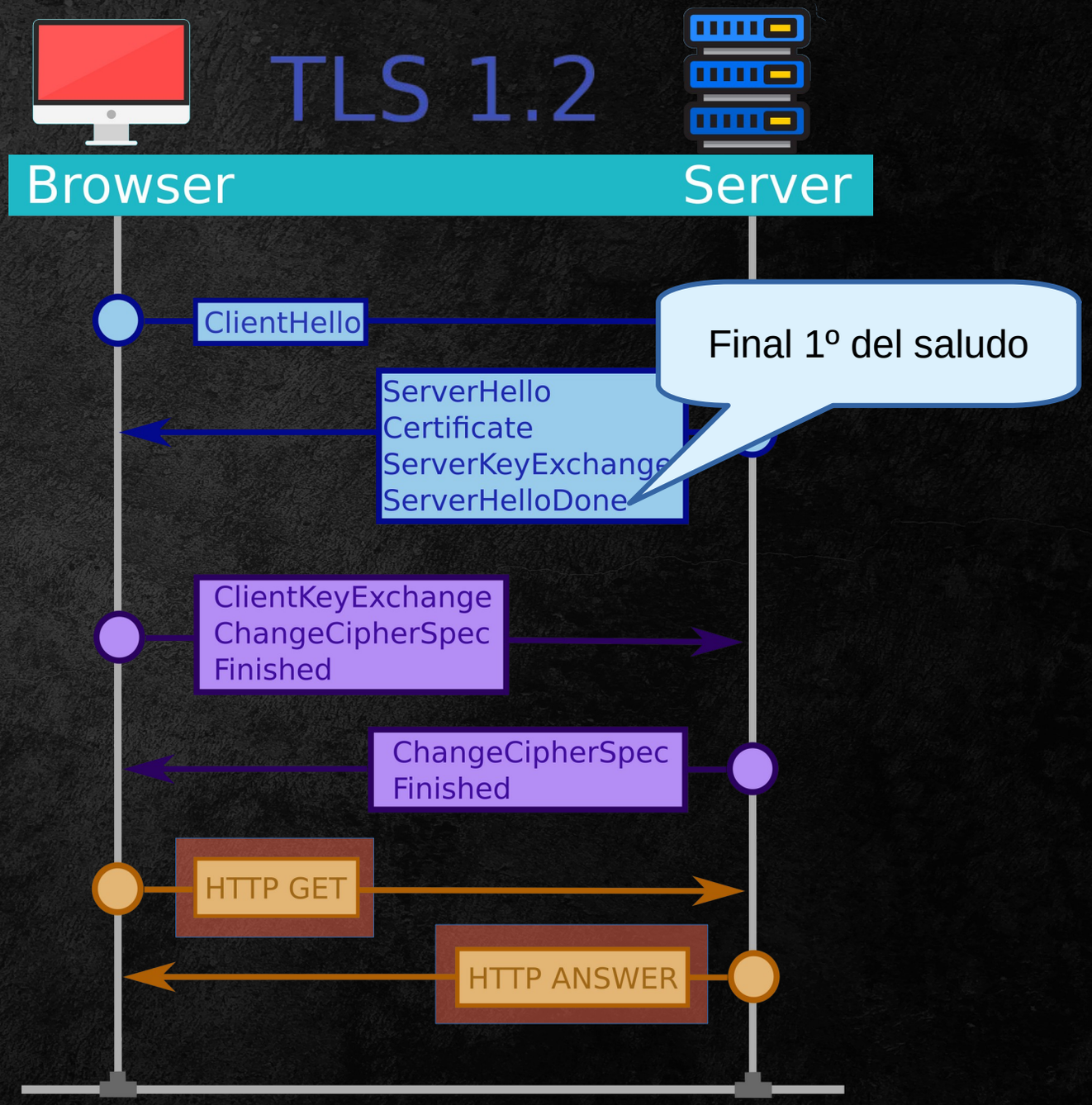
2 RTT (Round Trip Time)



NAVAJA NEGRA

Handshake TLS 1.2

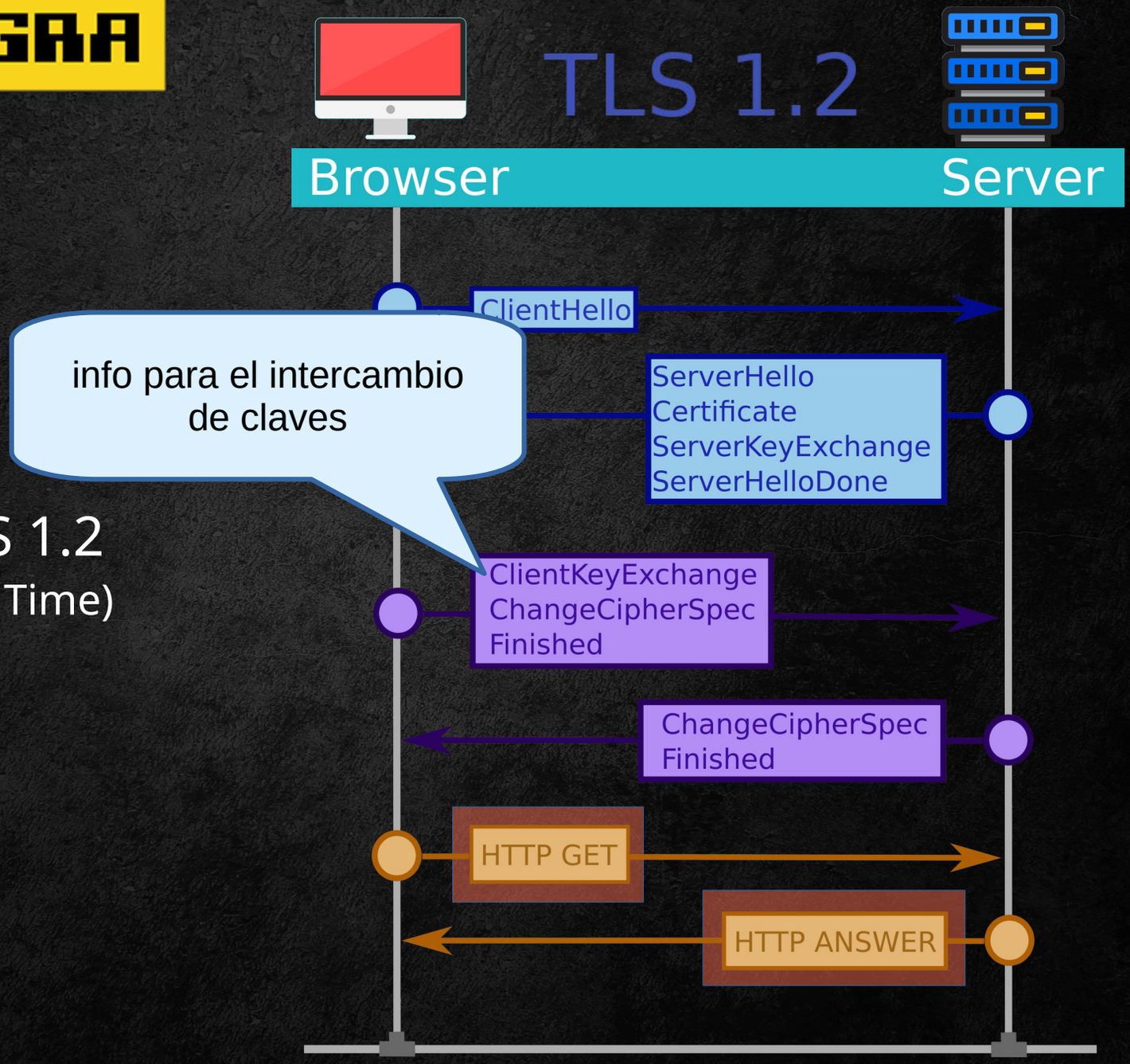
2 RTT (Round Trip Time)



NAVAJA NEGRA

Handshake TLS 1.2

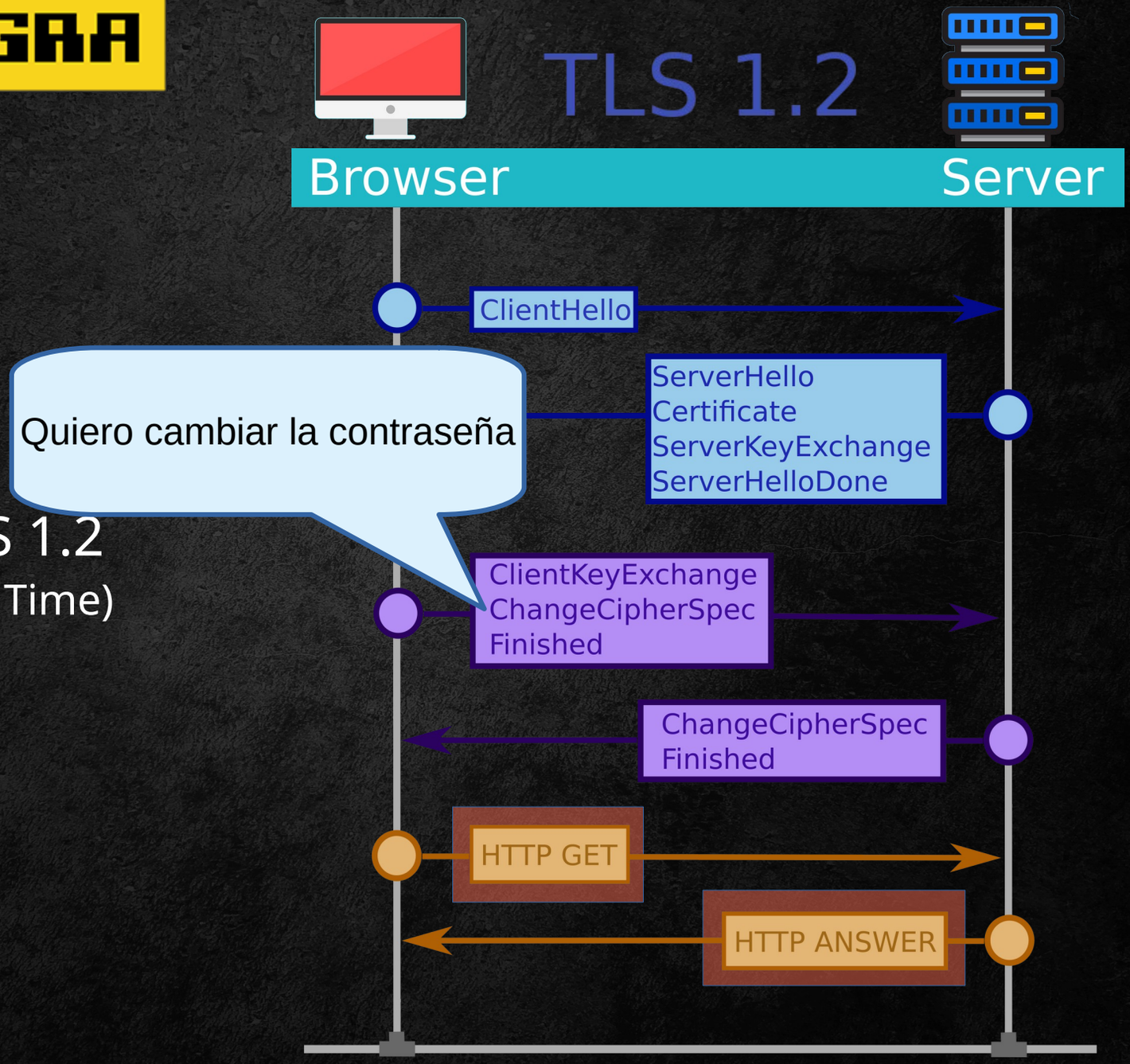
2 RTT (Round Trip Time)



NAVAJA NEGRA

Handshake TLS 1.2

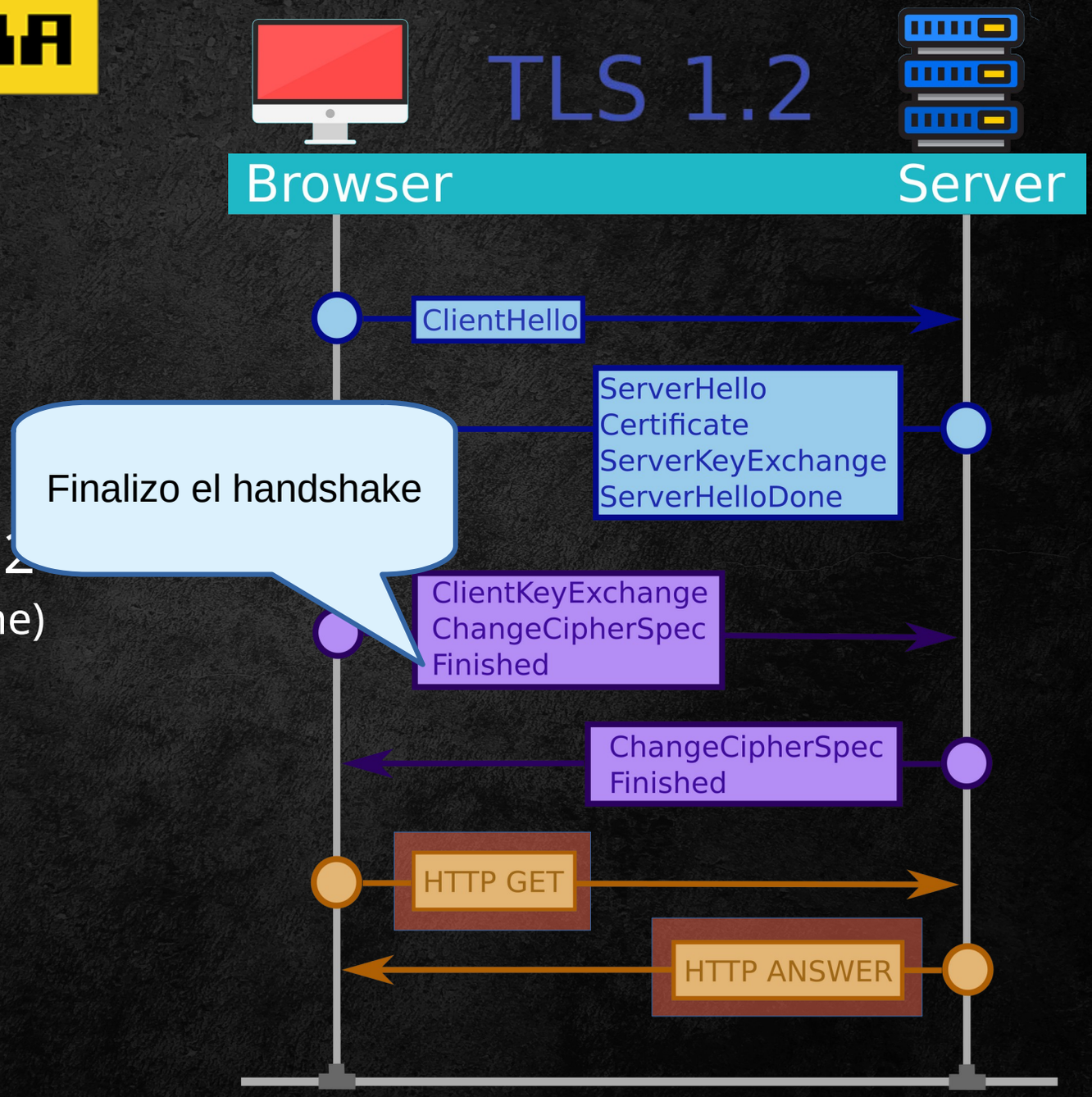
2 RTT (Round Trip Time)



NAVAJA NEGRA

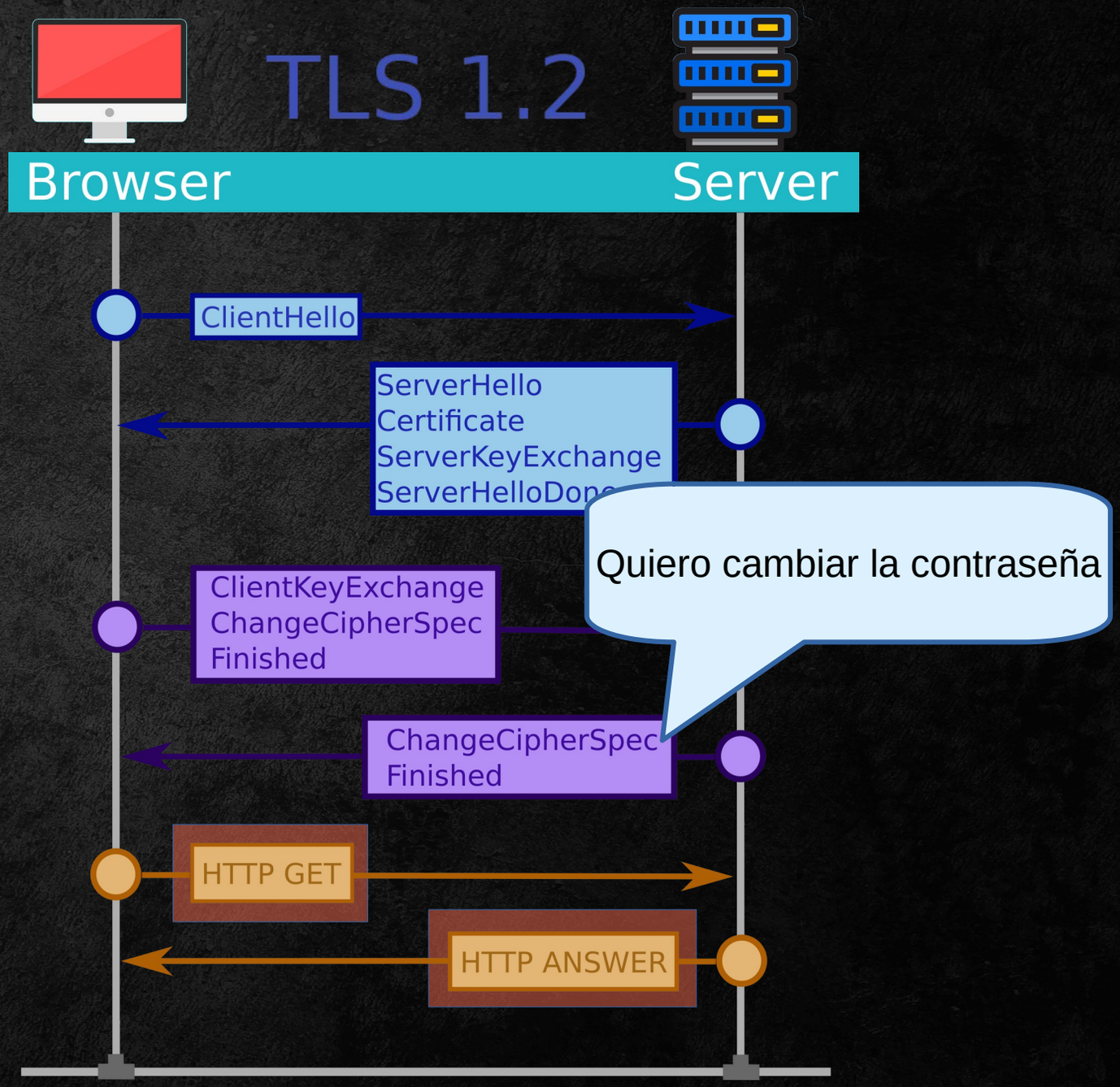
Handshake TLS 1.2

2 RTT (Round Trip Time)



NAVAJA NEGRA

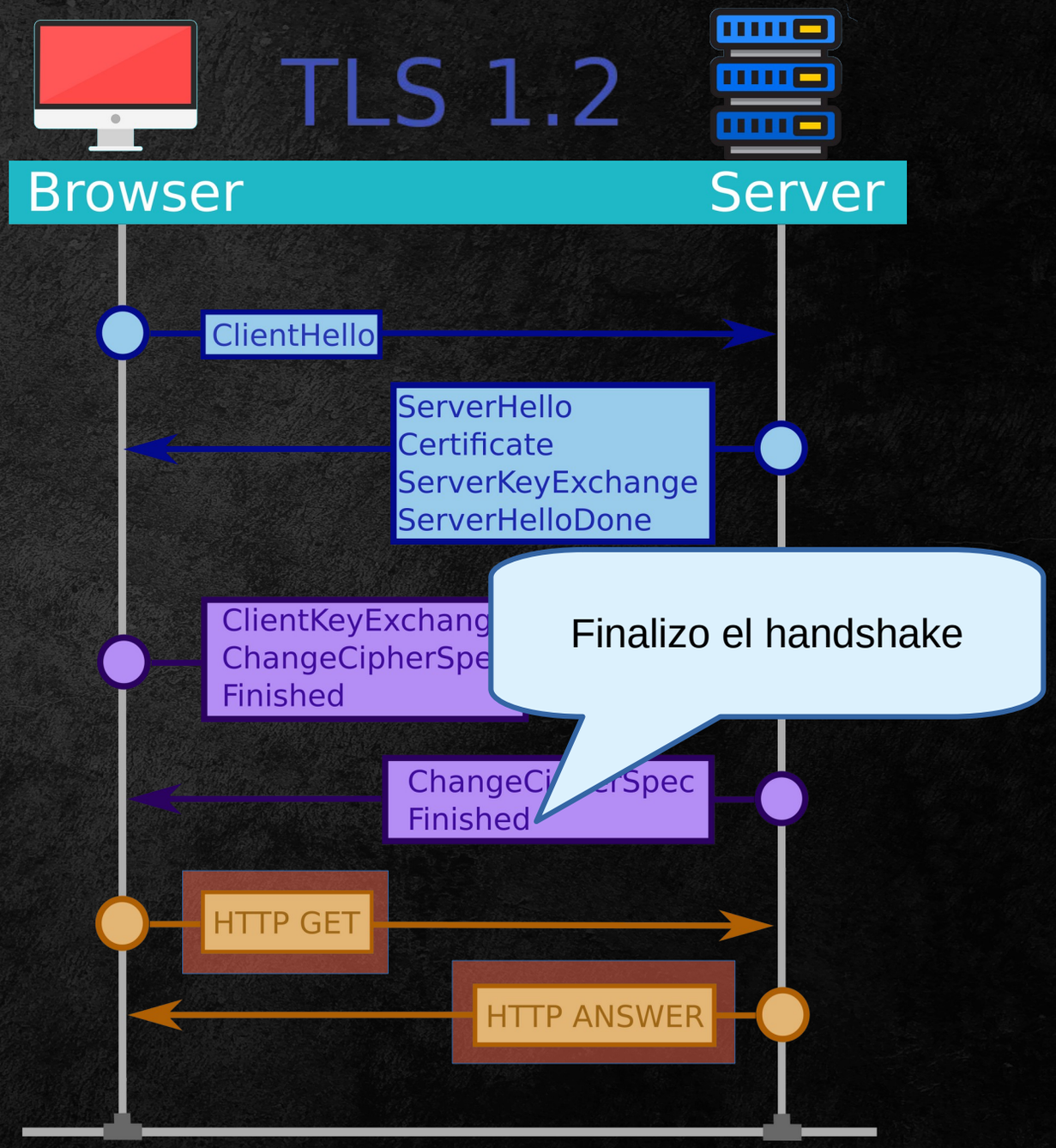
Handshake TLS 1.2
2 RTT (Round Trip Time)



NAVAJA NEGRA

Handshake TLS 1.2

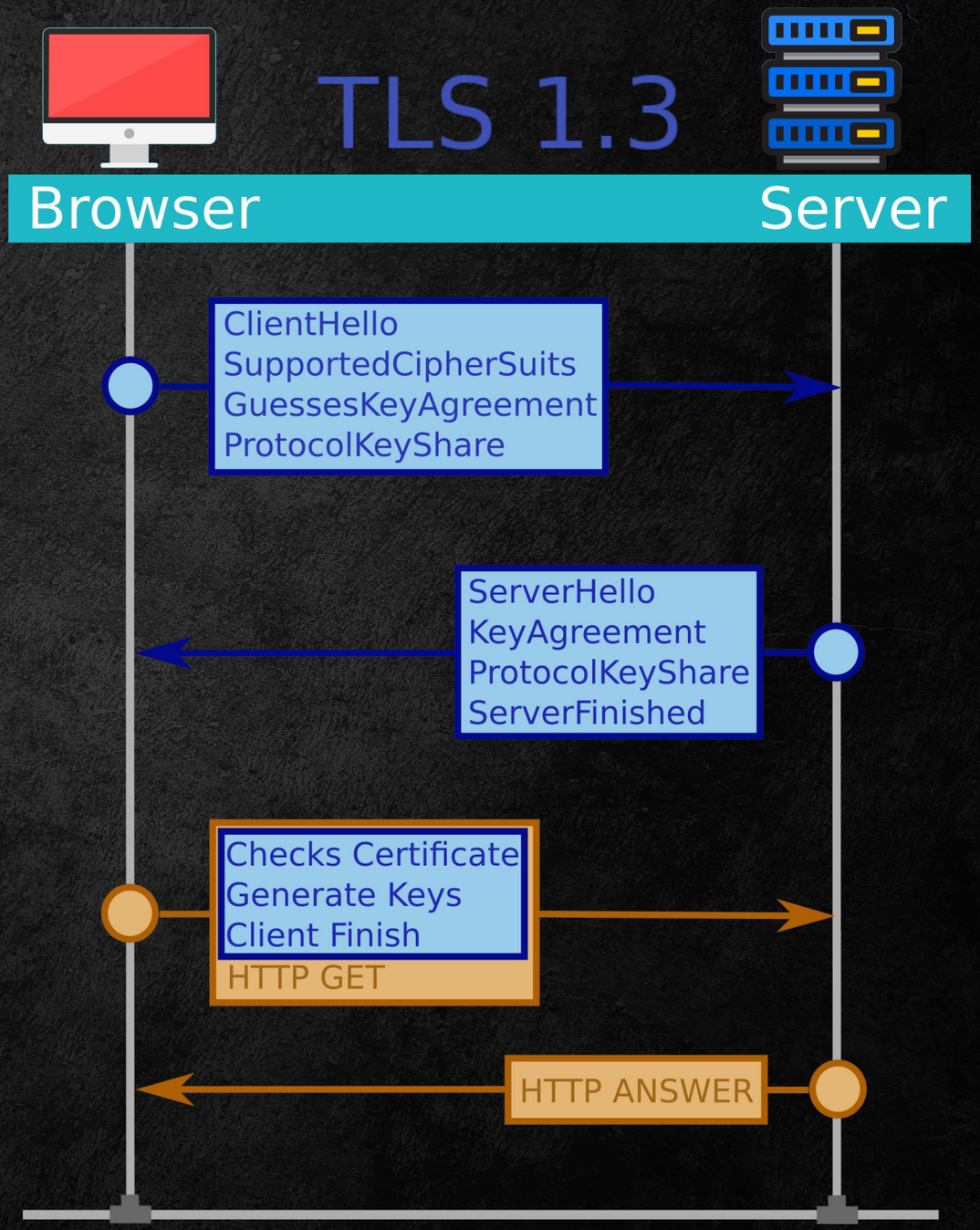
2 RTT (Round Trip Time)

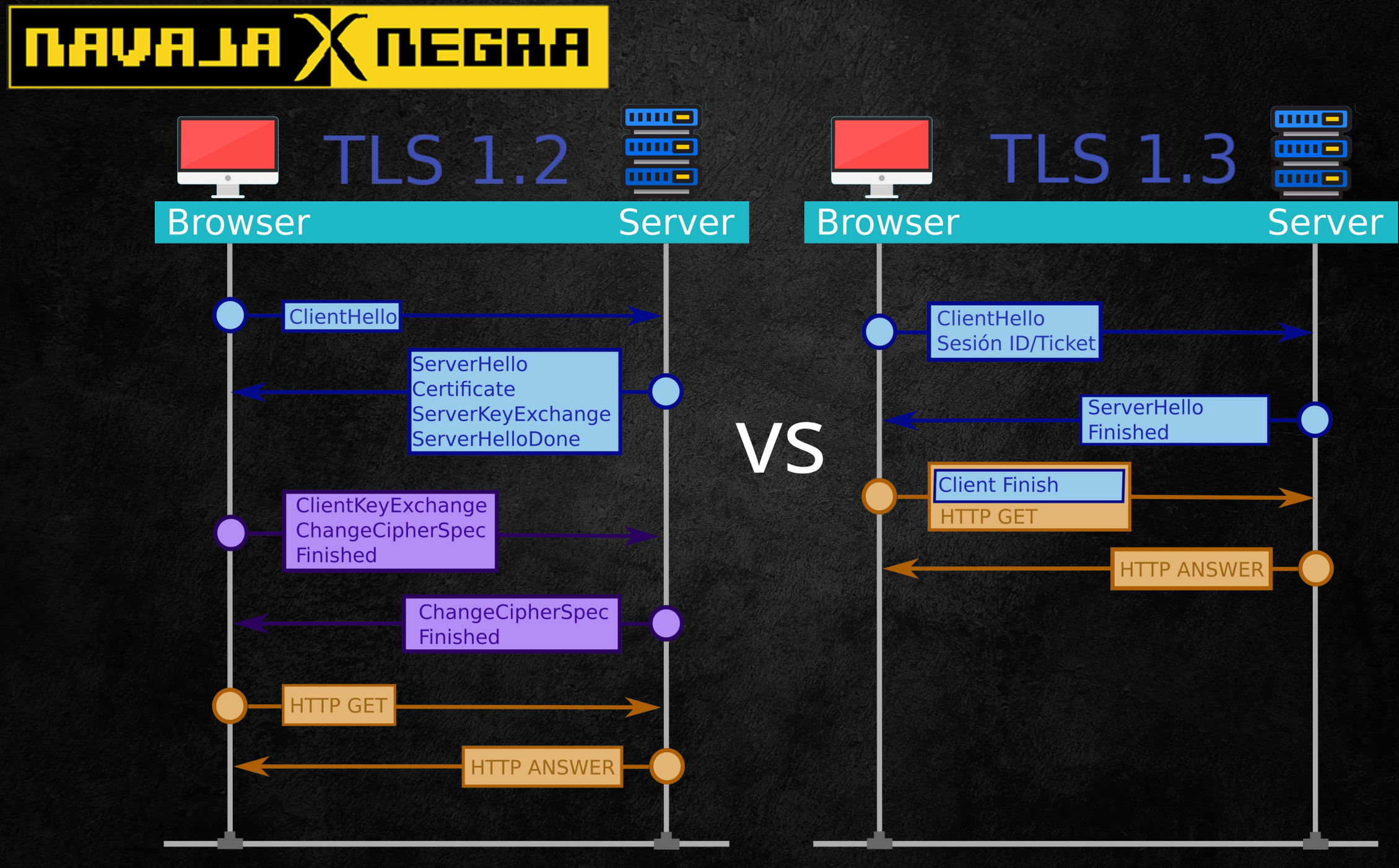


NAVAJA NEGRA

Handshake TLS 1.3

1 RTT (Round Trip Time)




NAVAJA NEGRA
TLS 1.2
Browser
Server
ClientHello
ServerHello
Certificate
ServerKeyExchange
ServerHelloDone
ClientKeyExchange
ChangeCipherSpec
Finished
ChangeCipherSpec
Finished
HTTP GET
HTTP ANSWER
VS
TLS 1.3
Browser
Server
ClientHello
Sesión ID/Ticket
ServerHello
Finished
Client Finish
HTTP GET
HTTP ANSWER

NAVAJA NEGRA

TLS 1.3

ssl

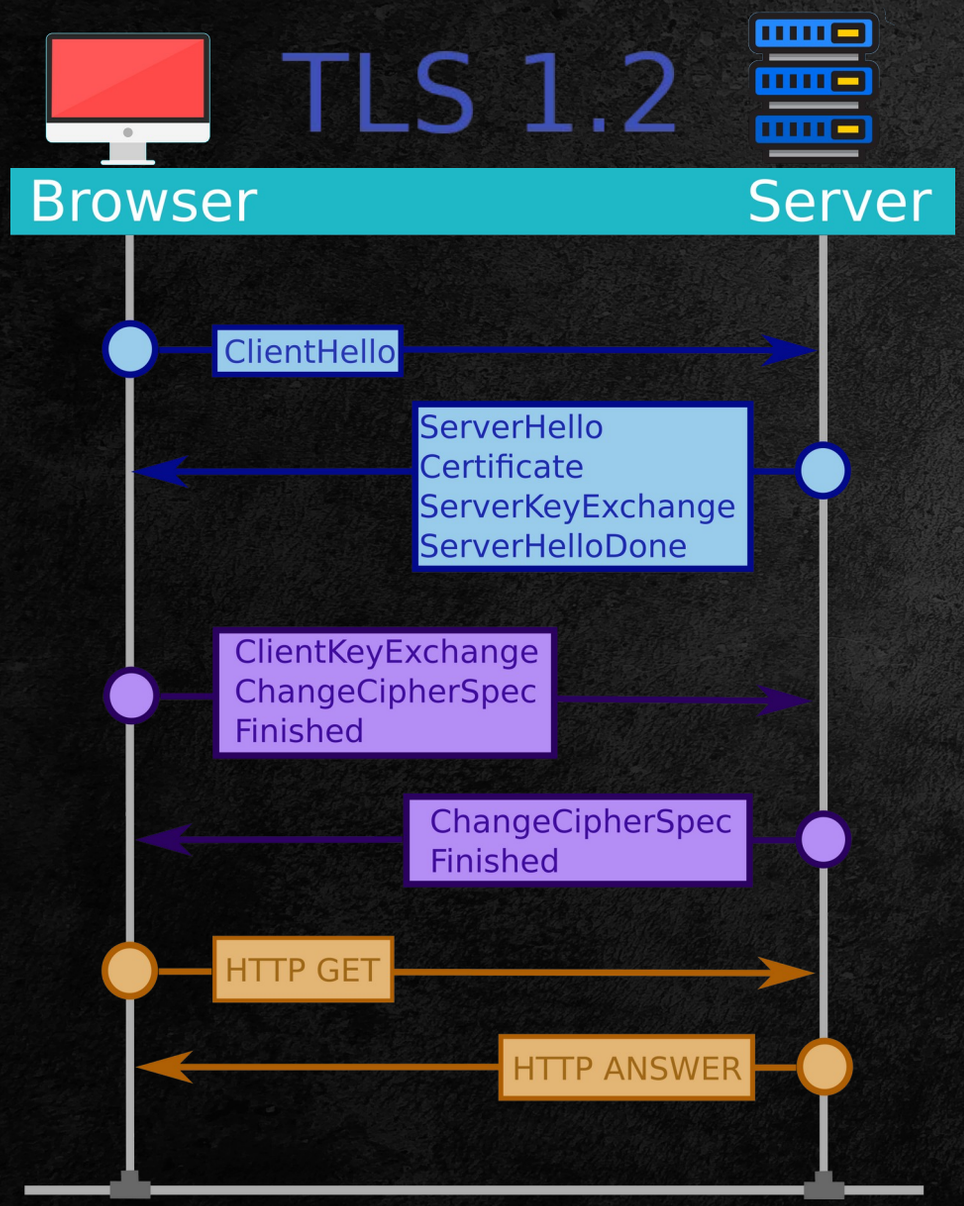
No.	Time	Source	Destination	Protocol	Length	Info
4	0.000509	127.0.0.1	127.0.0.1	TLSv1.3	299	Client Hello
6	0.008516	127.0.0.1	127.0.0.1	TLSv1.3	2299	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, App…
8	0.009185	127.0.0.1	127.0.0.1	TLSv1.3	146	Change Cipher Spec, Application Data
9	0.009564	127.0.0.1	127.0.0.1	TLSv1.3	321	Application Data

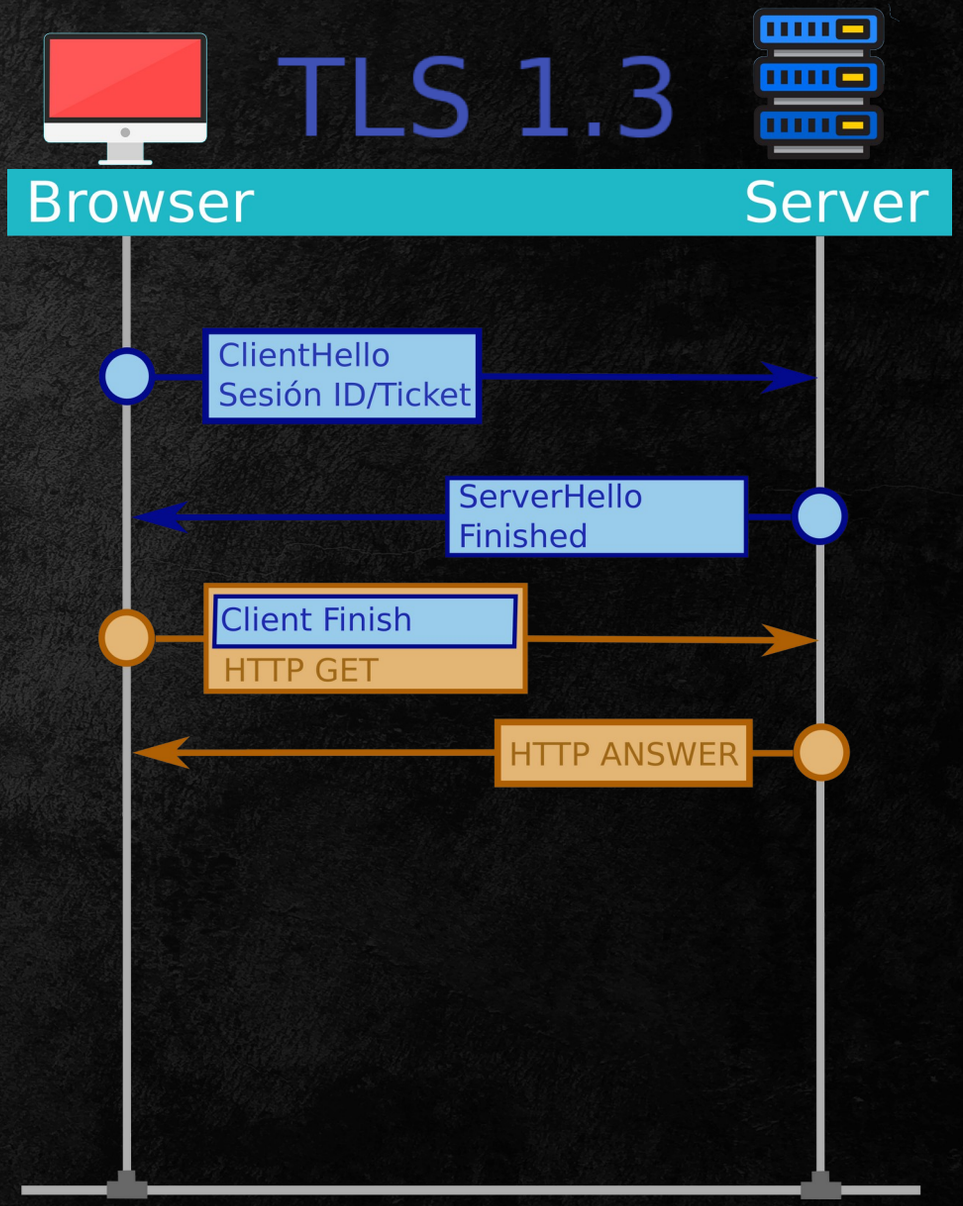
TLS 1.2

ssl

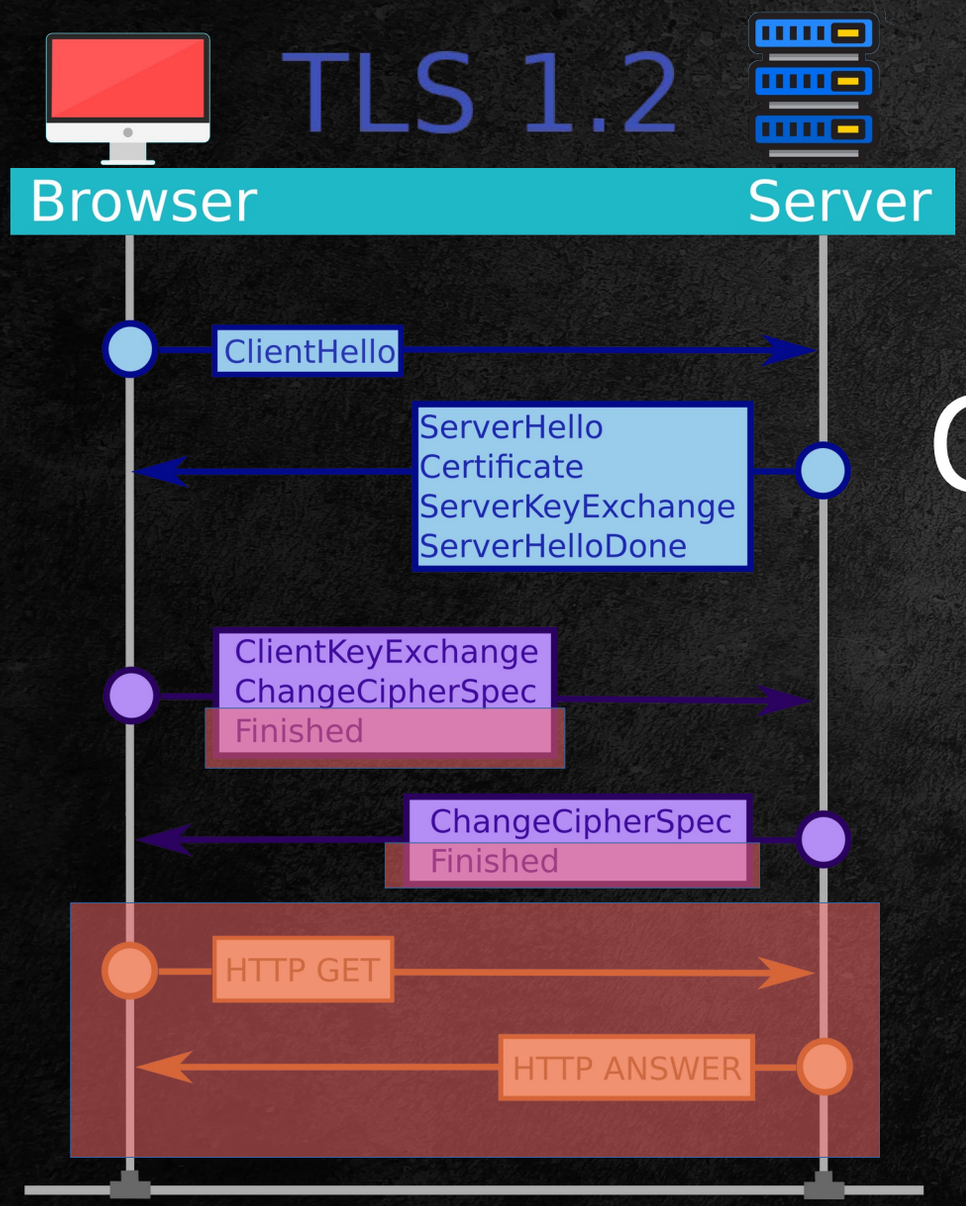
No.	Time	Source	Destination	Protocol	Length	Info
4	0.000508	127.0.0.1	127.0.0.1	TLSv1.2	377	Client Hello
6	0.007982	127.0.0.1	127.0.0.1	TLSv1.2	2142	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8	0.008630	127.0.0.1	127.0.0.1	TLSv1.2	159	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9	0.008886	127.0.0.1	127.0.0.1	TLSv1.2	292	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
10	0.008955	127.0.0.1	127.0.0.1	TLSv1.2	329	Application Data
12	7.041511	127.0.0.1	127.0.0.1	TLSv1.2	150	Application Data

NAVAJA NEGRA

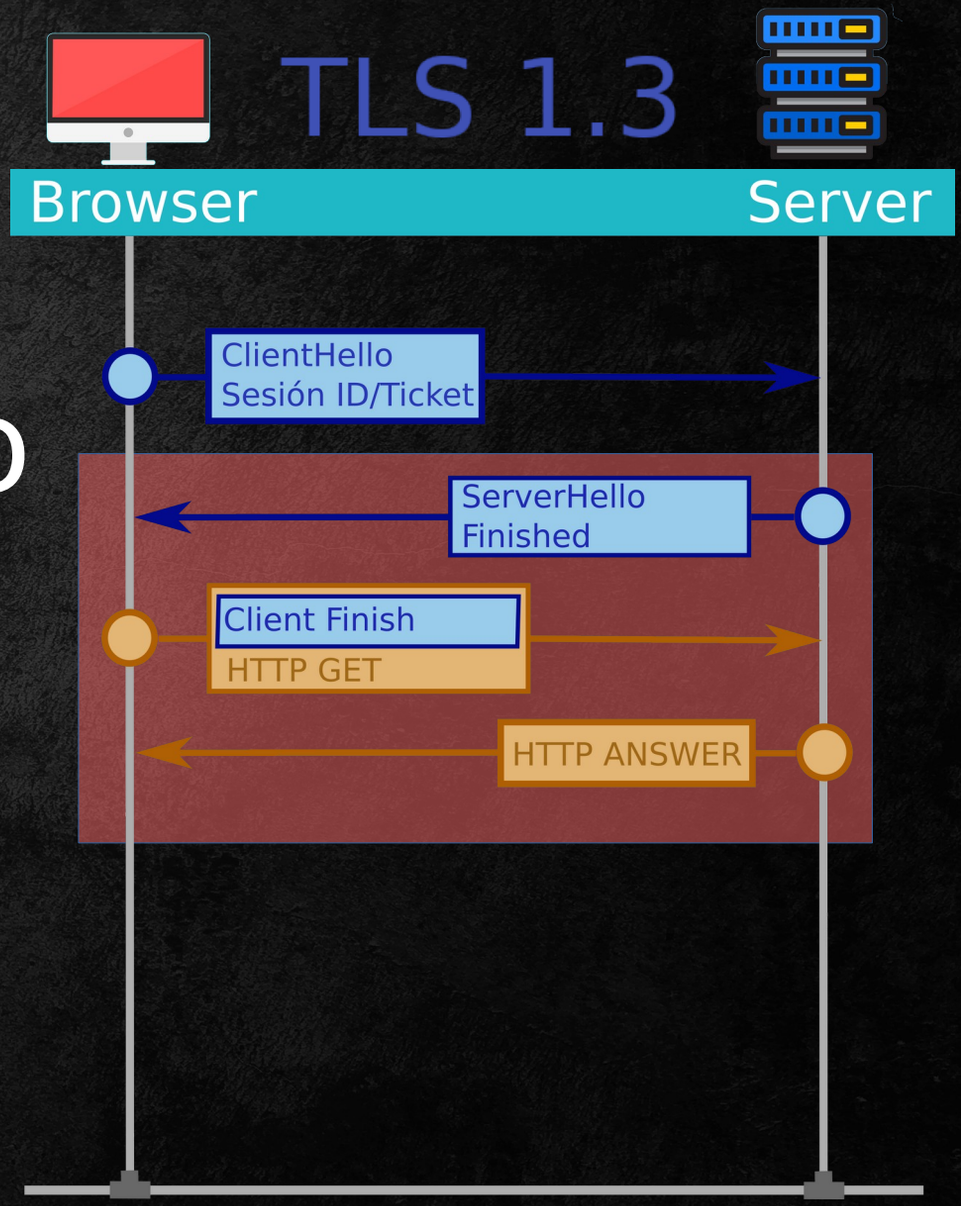




NAVAJA NEGRA



Cifrado



NAVAJA NEGRA

No key exchange

Forward Secrecy

~~**RSA**~~

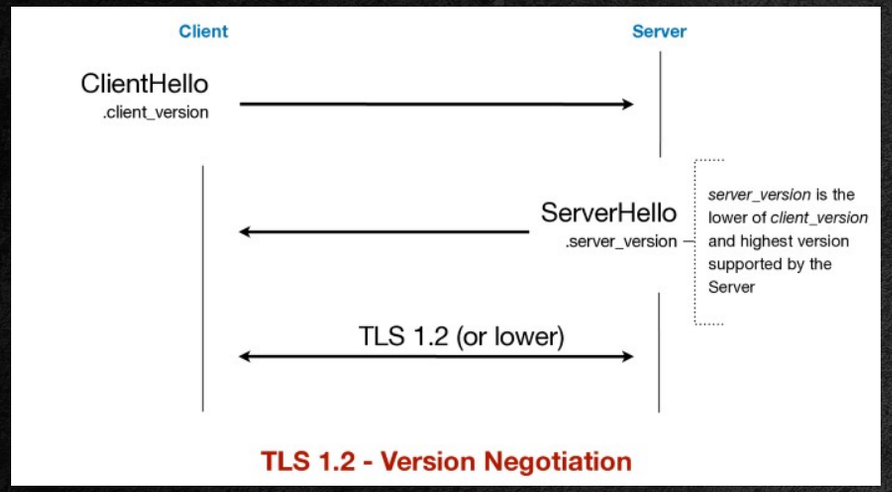
~~**Diffie-hellman**~~

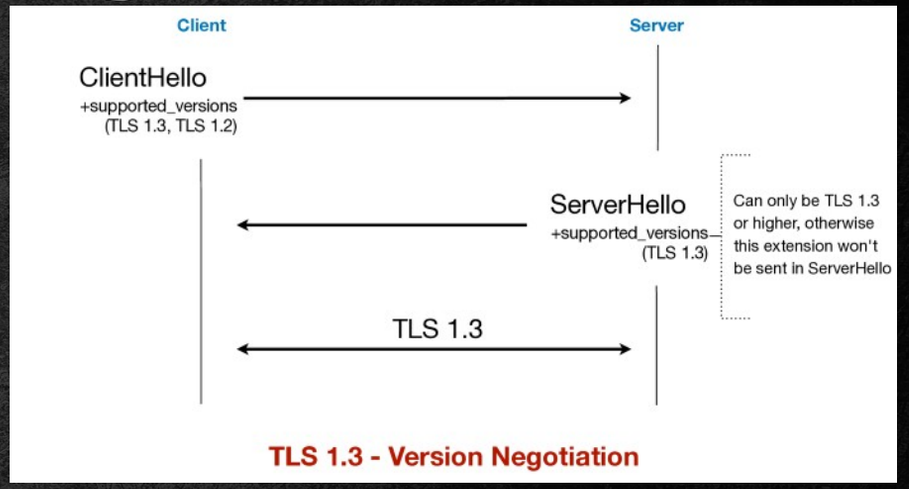
Conjuntos de cifrado

TLS 1.2
37 conjuntos de cifrado
319 adicionales heredados

TLS 1.3
5 conjuntos de cifrado

Anti Downgrade





"44 4F 57 4E 47 52 44 01"

D O W N G R D 01

NAVAJA NEGRA

Algoritmos de hash antiguos

- MD5
- SHA-1

Sistemas de cifrado antiguos

- RC4
- DES
- 3DES

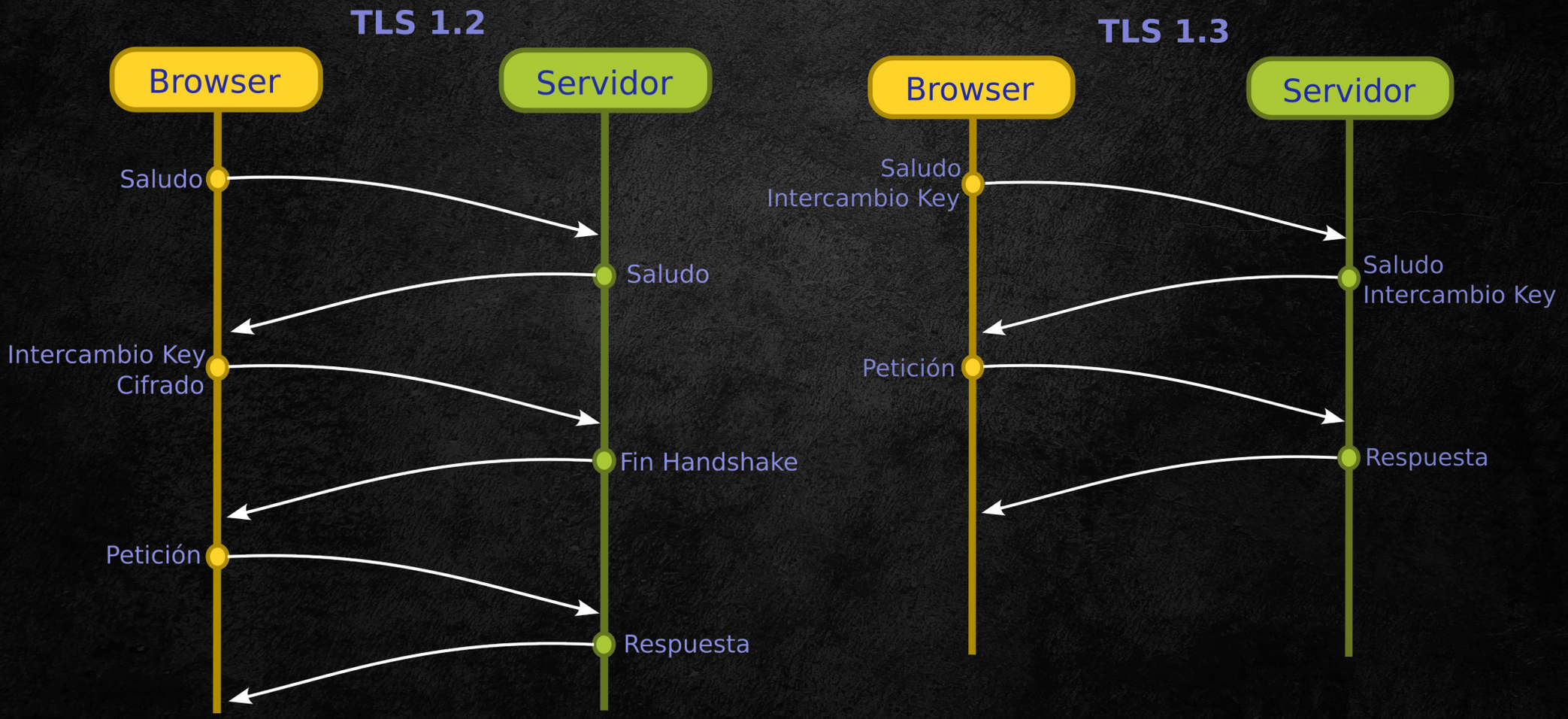
Cifadro simetrico que utiliza modos de bloque CBC

- AES-CBC

Grupos Diffie-Hellman arbitrarios no efímeros

NAVAJA NEGRA

TLS (Simplificado)



The Design and Implementation of the Tor Browser [DRAFT]

3.3. Adversary Capabilities - Attacks

The adversary can perform the following attacks from a number of different positions to accomplish various aspects of their goals. It should be noted that many of these attacks (especially those involving IP address leakage) are often performed by accident by websites that simply have JavaScript, dynamic CSS elements, and plugins. Others are performed by ad servers seeking to correlate users' activity across different IP addresses, and still others are performed by malicious agents on the Tor network and at national firewalls.

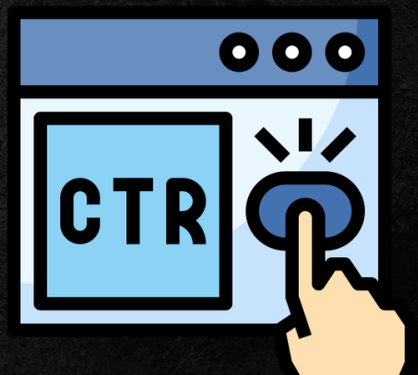
1. **Read and insert identifiers**

   The browser contains multiple facilities for storing identifiers that the adversary creates for the purposes of tracking users. These identifiers are most obviously cookies, but also include HTTP auth, DOM storage, cached scripts and other elements with embedded identifiers, client certificates, and even TLS Session IDs.

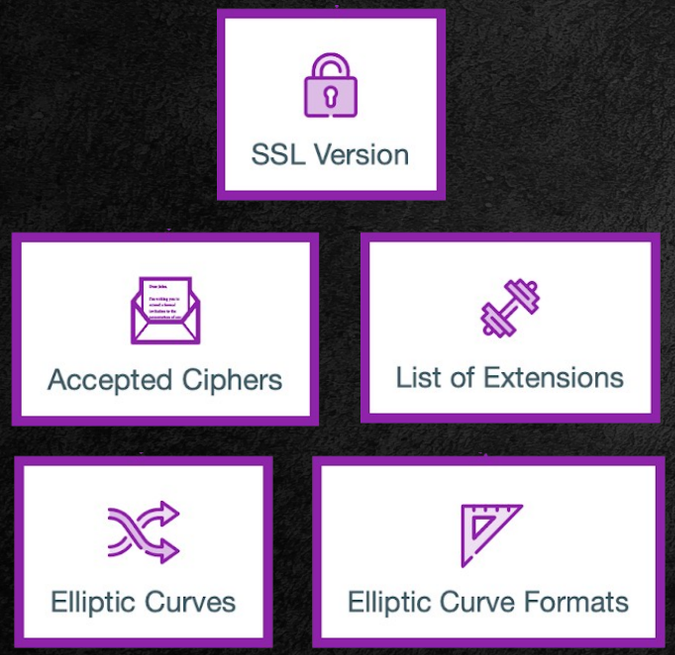
NAVAJA NEGRA

Como nos rastrean

- Cookies
- Web beacons (Web bug)
- Session replay scripts
- Account tracking
- Browser fingerprinting
- Canvas elements
- Cross-domain content
- Supercookies
- Favicons
- Mouse tracking
- Cross-device tracking
- Click-through rate
- Javascript tracking code
- Social media



Perfilado grupos usuarios TLS




```
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 224
  ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 220
      Version: TLS 1.2 (0x0303)
    ▶ Random
      Session ID Length: 0
      Cipher Suites Length: 38
    ▶ Cipher Suites (19 suites)
      Compression Methods Length: 1
    ▶ Compression Methods (1 method)
      Extensions Length: 141
    ▶ Extension: server_name
    ▶ Extension: elliptic_curves
    ▶ Extension: ec_point_formats
    ▶ Extension: signature_algorithms
    ▶ Extension: next_protocol_negotiation
    ▶ Extension: Application Layer Protocol
    ▶ Extension: status_request
    ▶ Extension: signed_certificate_timestam
    ▶ Extension: Extended Master Secret
```

Significant, key - value order is!

Perfilado grupos usuarios TLS

Lee Brotherston
2015
Opensource

→

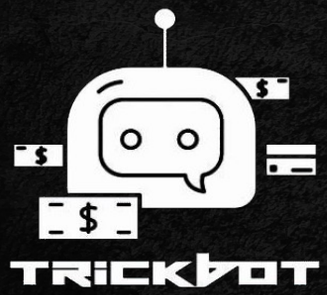
John Althouse
Jeff Atkinson
Josh Atkins

→

JA3
JA3S

→

IDS/IPS
SIEM

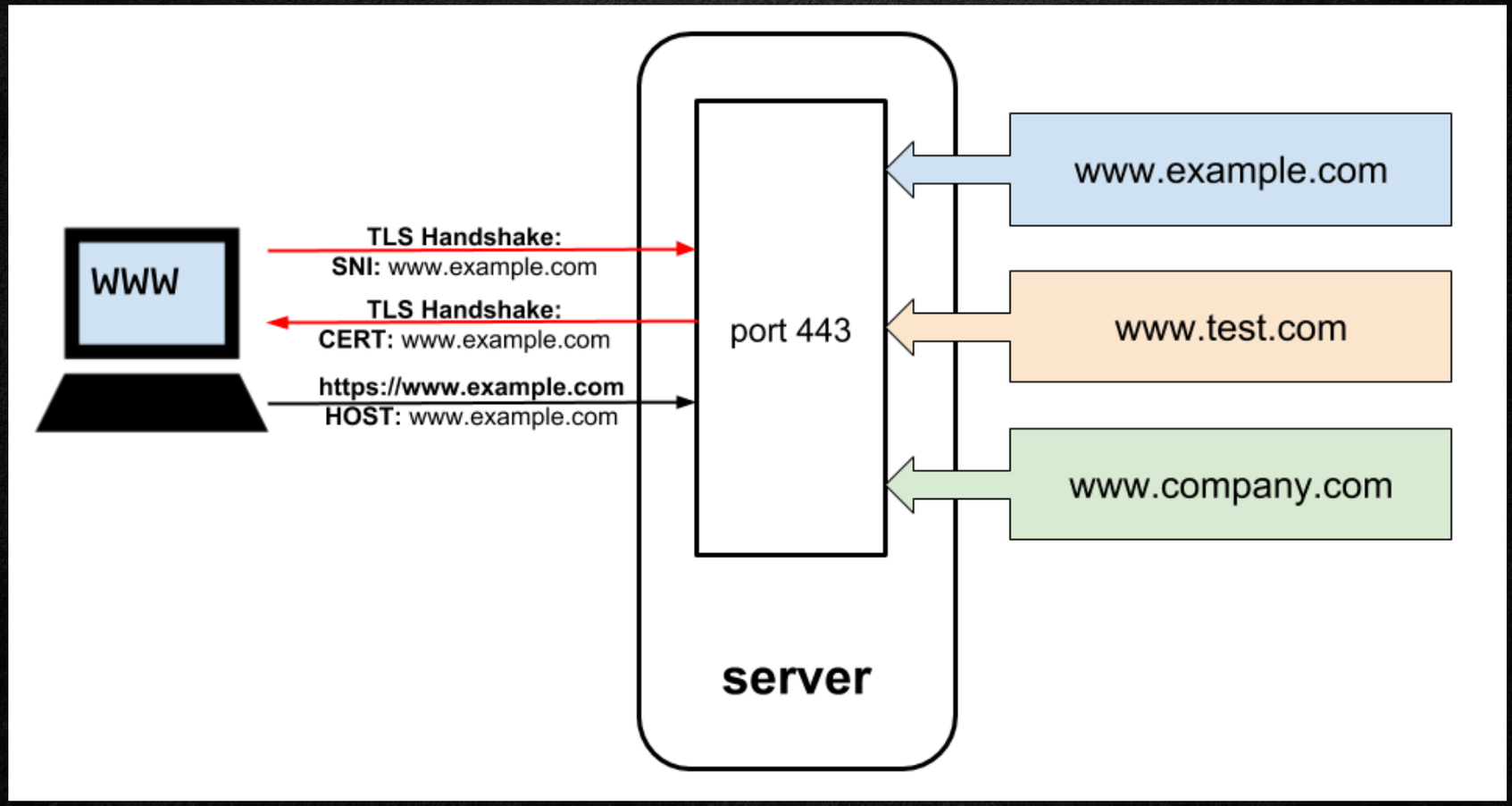


6734f37431670b3ab4292b8f60f29984

e7d705a3286e19ea42f587b344ee6865

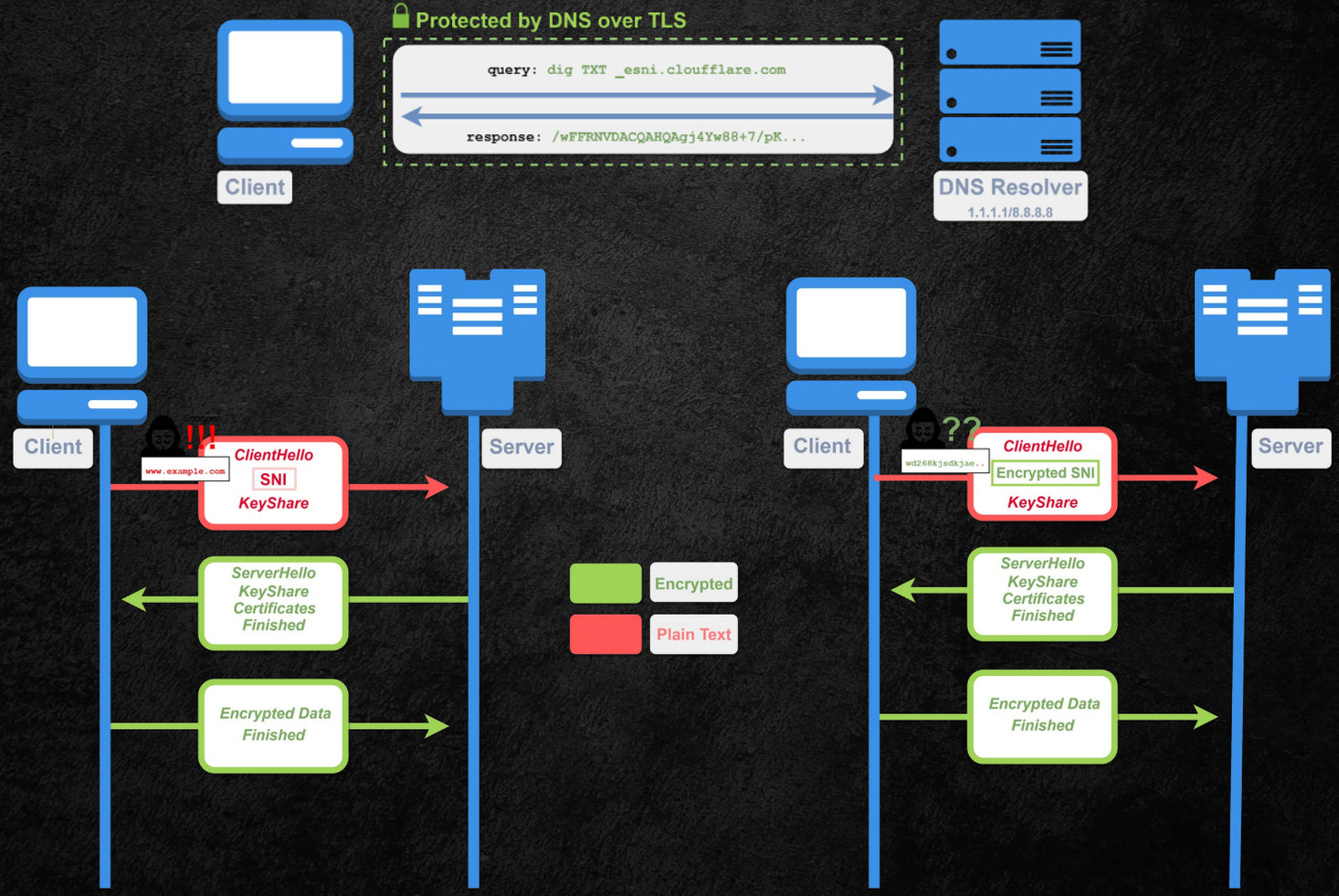
Cipher-Stunting

Perfilado por SNI

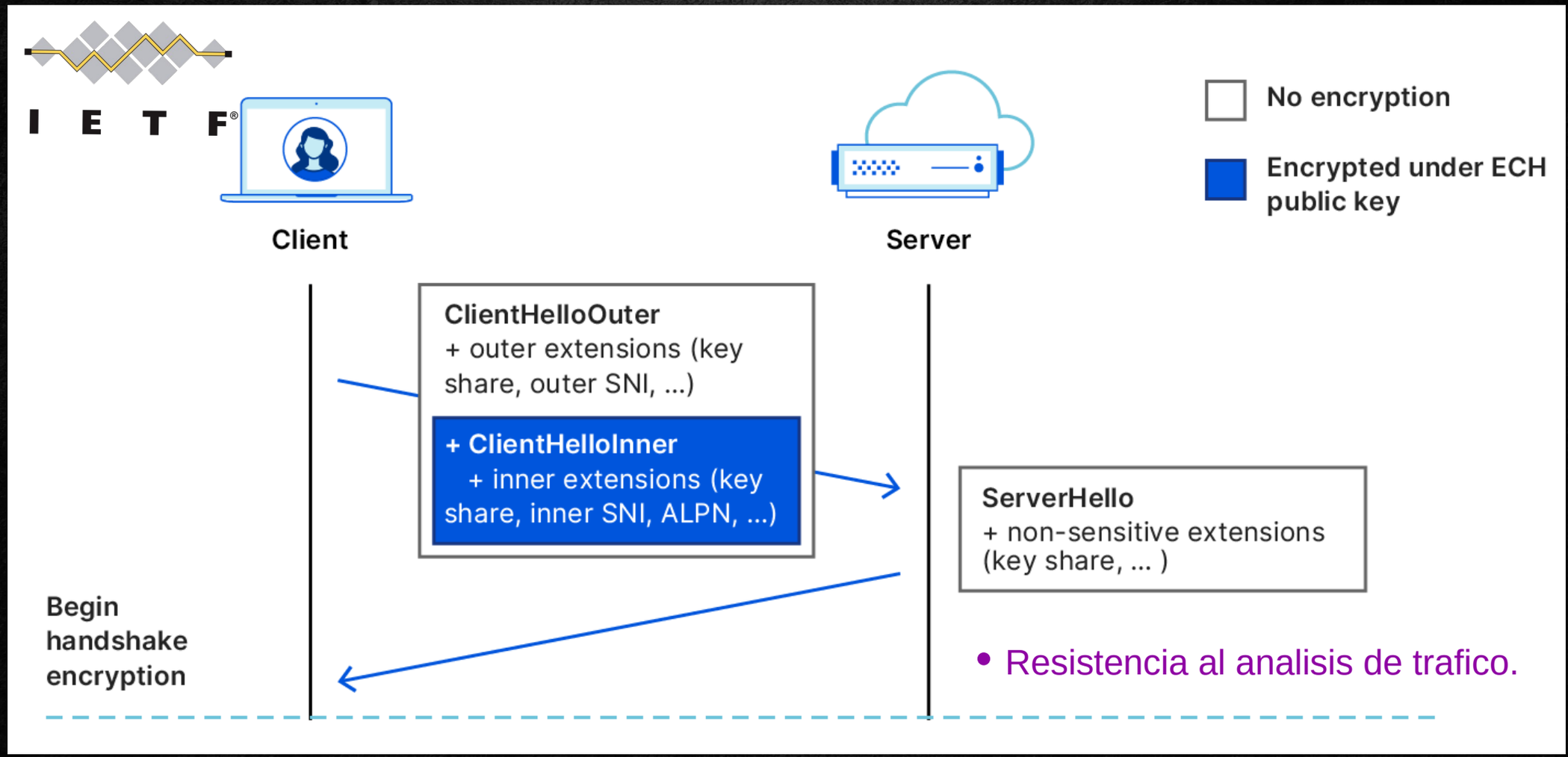


NAVAJA NEGRA

Extension eSNI



Extension ECH



- Resistencia al analisis de trafico.

NAVAJA NEGRA

Extension ECH

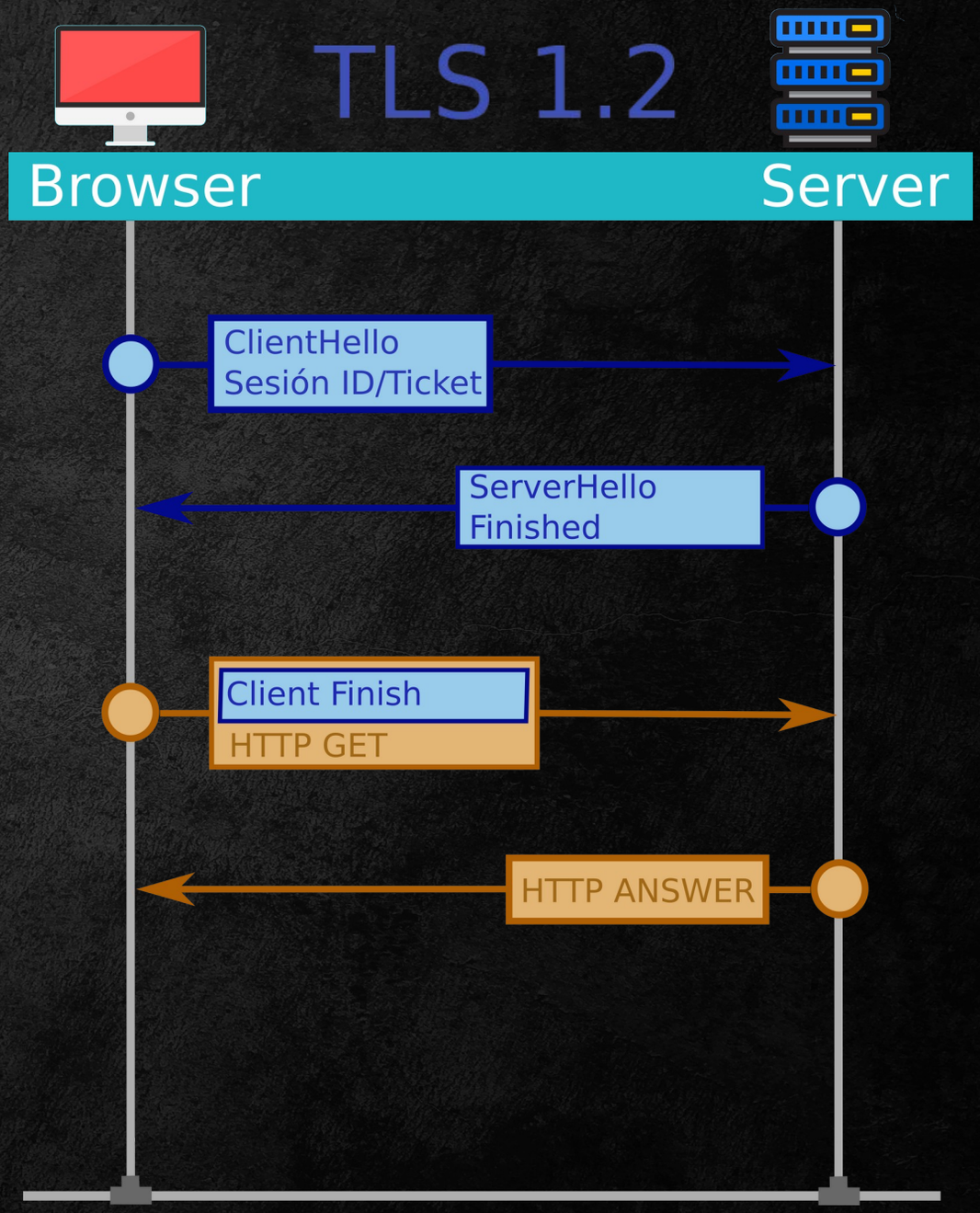
- Firefox 85 cambia eSNI por ECH (limitaciones)
- ECH va por el borrador 13
- En el borrador 10 TLS (2015) se planteó

NAVAJA NEGRA

Sistemas de cacheo TLS 1.2
2 RTT → 1 RTT

Session ids/tickets (ServerHello)

- Número aleatorio
- Algoritmos de sec
- Parametros de sec

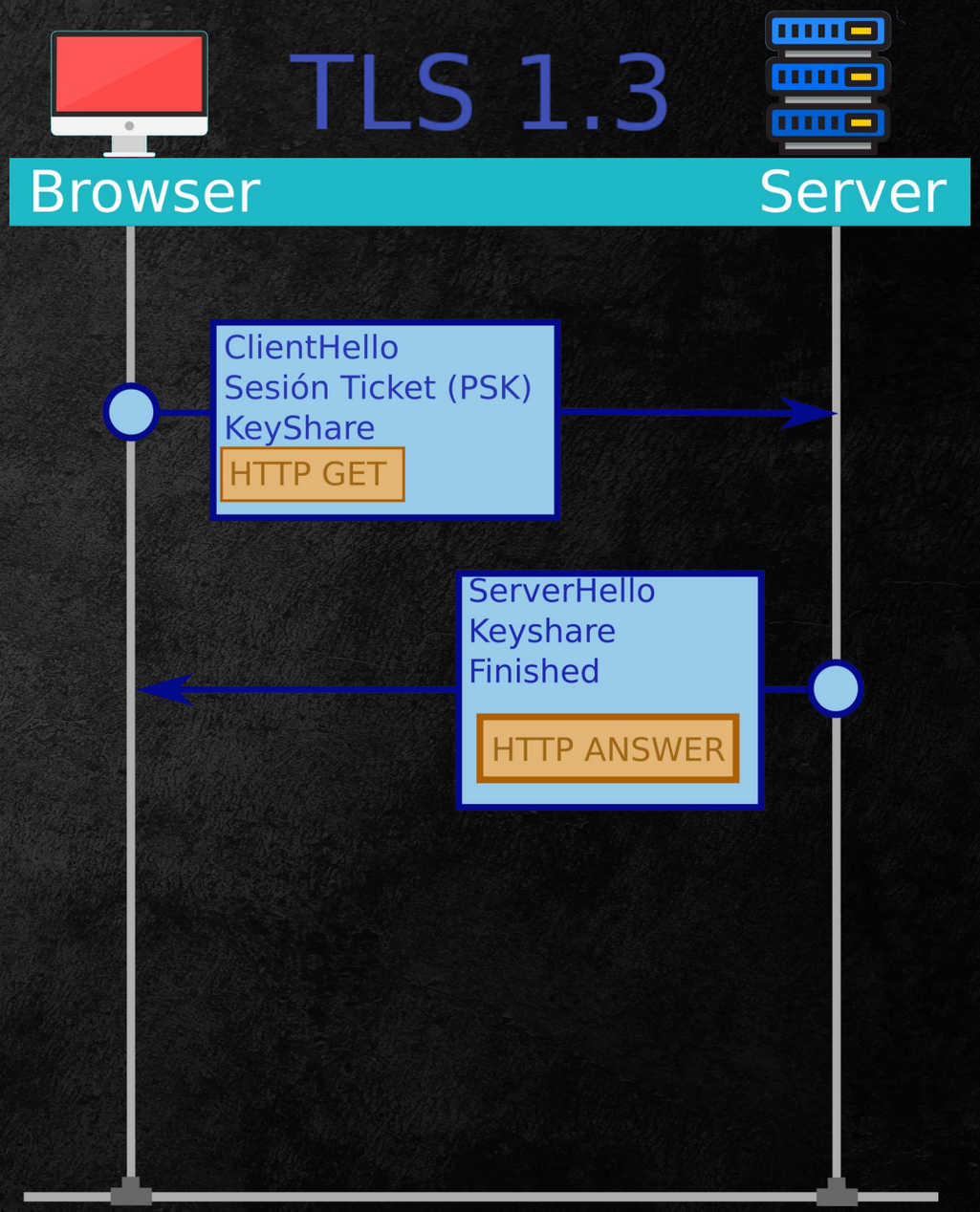


NAVAJA NEGRA

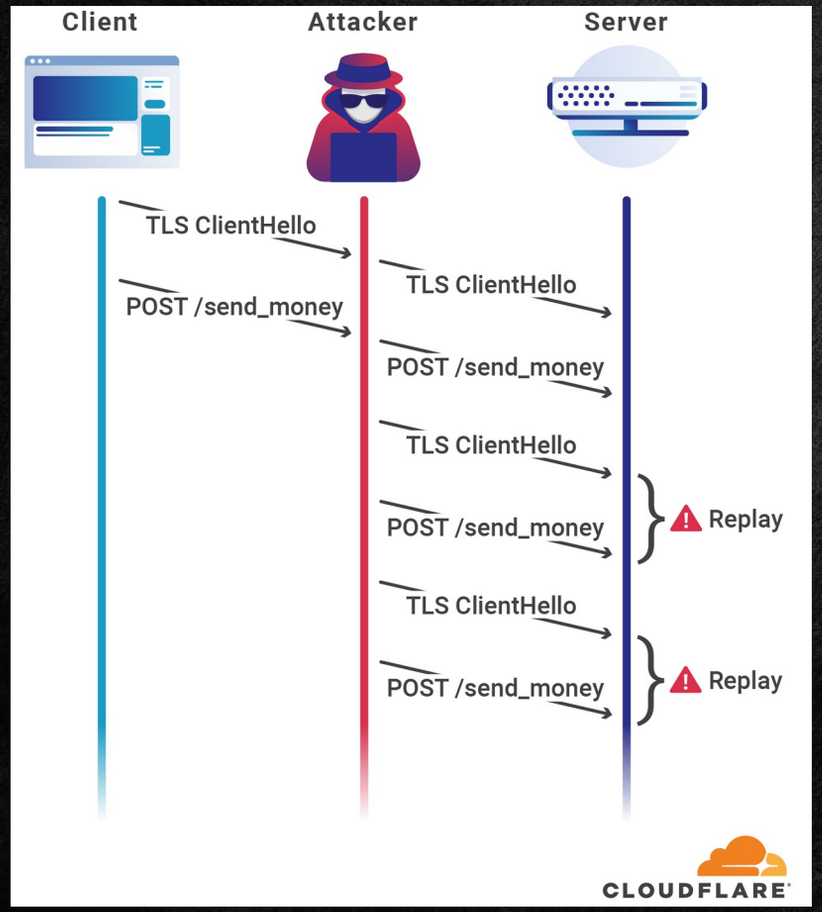
Sistemas de cacheo TLS 1.3
1 RTT → 0 RTT

PSK

Simpre cifrado



Replay en TLS 1.3



Solucion:

Solo operaciones idempotentes:

NO POST y similares

SI GET y similares

Error 425 (too early) para notificarlo

Seguimiento de usuarios con reanudación

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

Seguimiento de usuarios con reanudación

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

Seguimiento de usuarios con reanudación

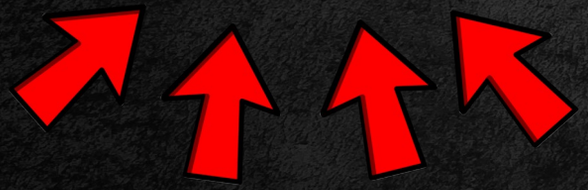
Tiempo max	10,080 Min
Recomendado TLS 1.2	3 min
Recomendado TLS 1.3	5 min

Seguimiento de usuarios con reanudación

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

Seguimiento de usuarios con reanudación

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



Seguimiento de usuarios con reanudación

El navegador también gestiona la caché

Ataque de prolongación

Si cierran navegador se borra cache

Seguimiento de usuarios con reanudación

El navegador también gestiona la caché

Ataque de prolongación

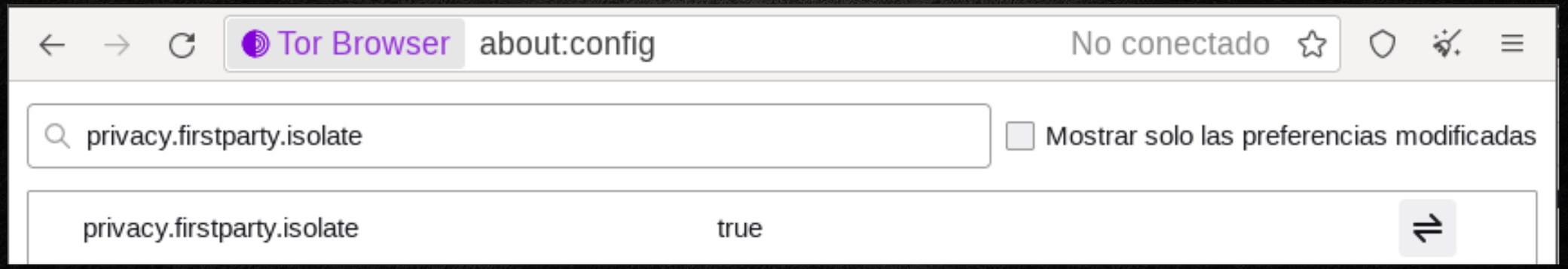
Si cierran navegador se borra cache

Se complica “demasiado”

Seguimiento de usuarios con reanudación

- Aplicaciones siempre activas
- Navegador “no se reinicia”
- Posible cacheo constante

Conclusiones



Conclusiones

Despertar el gusanillo con TLS

Seguridad no es siempre igual a privacidad

TLS 1.3 no es menos seguro, han dado otras prioridades

NAVAJA NEGRA

Internacional

EL PAÍS

OFENSIVA DE RUSIA EN UCRANIA >

Rusia bloquea medios extranjeros y redes sociales con una nueva ley que castiga con cárcel "la desinformación"

NAVAJA NEGRA

Internacional

cárcel

CincoDías

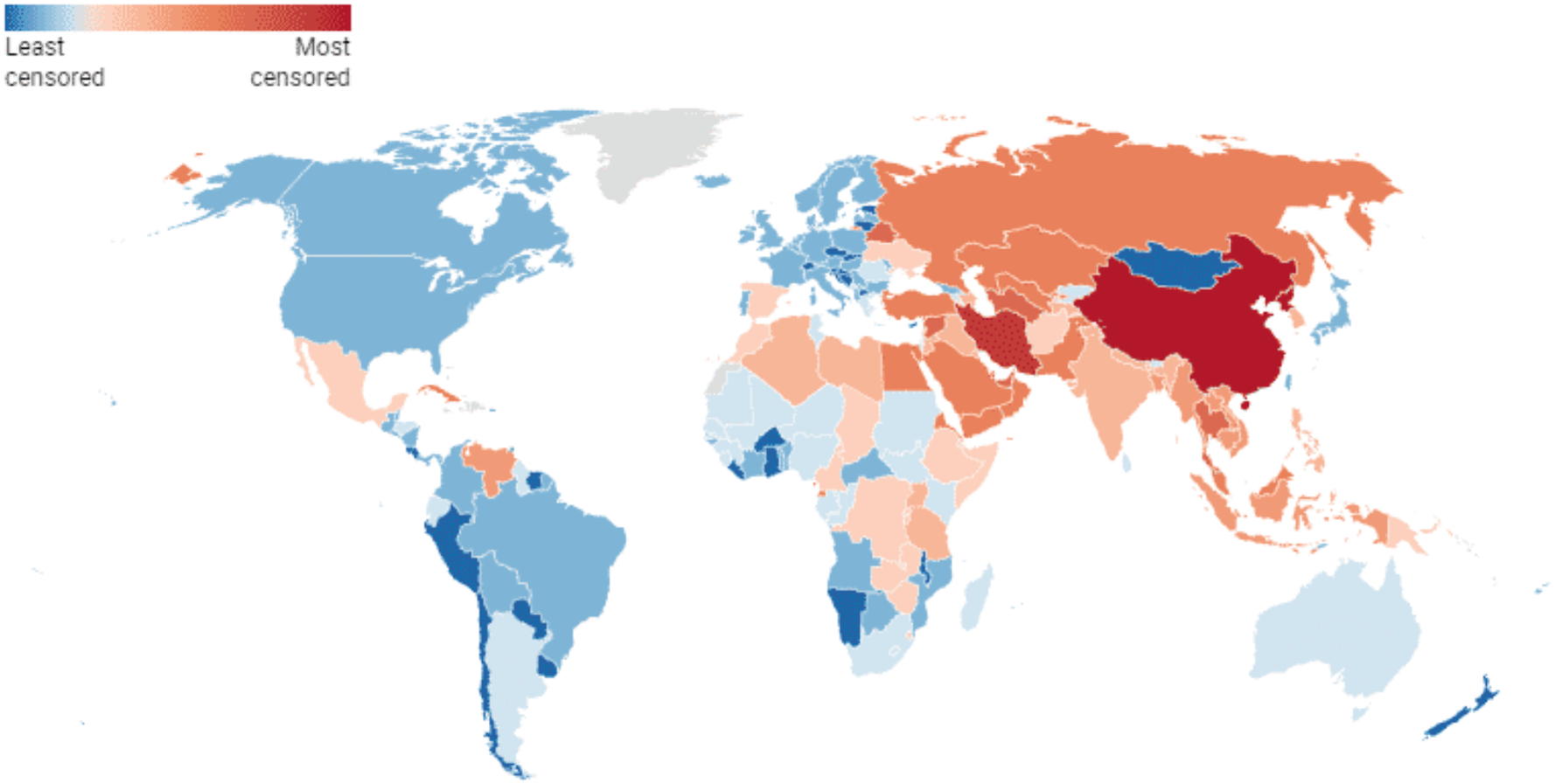
EL PAÍS ECONOMÍA

El 'splinternet' y cómo puede limitar el acceso a la web

Países como Rusia, China o Corea del Norte bloquean contenidos y redirigen el tráfico de la red

NAVAJA NEGRA

Which countries are the most censored in the world?



NAVAJA NEGRA

NAVAJA NEGRA

Somos un producto

The Telegraph

Apple under fire over iPhone encryption tech

Vodafone, Telefonica, Orange and T-Mobile have joined a running battle between tech giants and regulators

NAVAJA NEGRA

Somos un producto

orange™

SFR

TrustPid

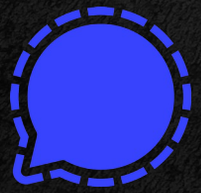
Telefónica

NAVAJA NEGRA

Gracias

¿¿Preguntas??


red@nosoloaulas.com


@ReD.1984