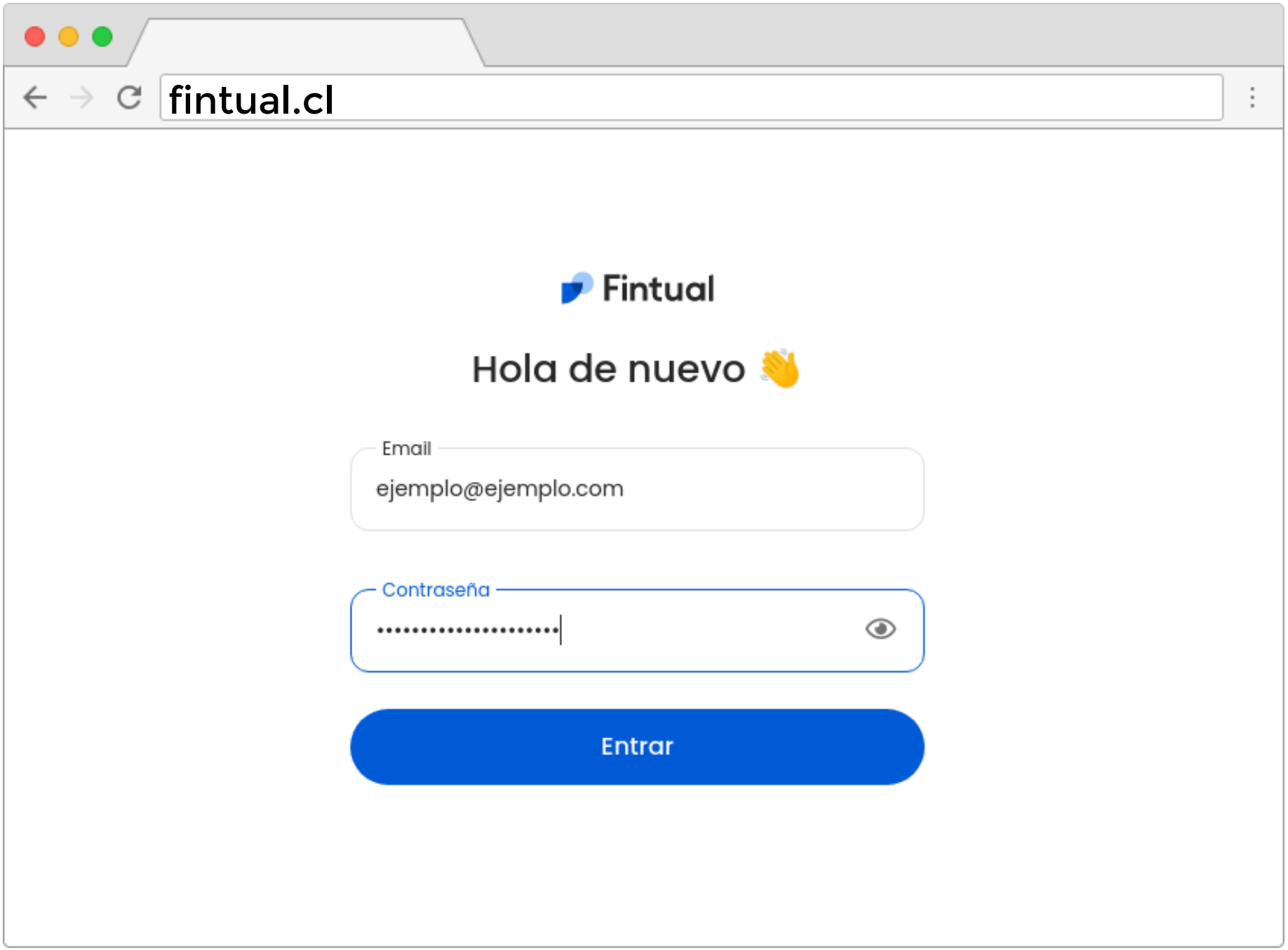
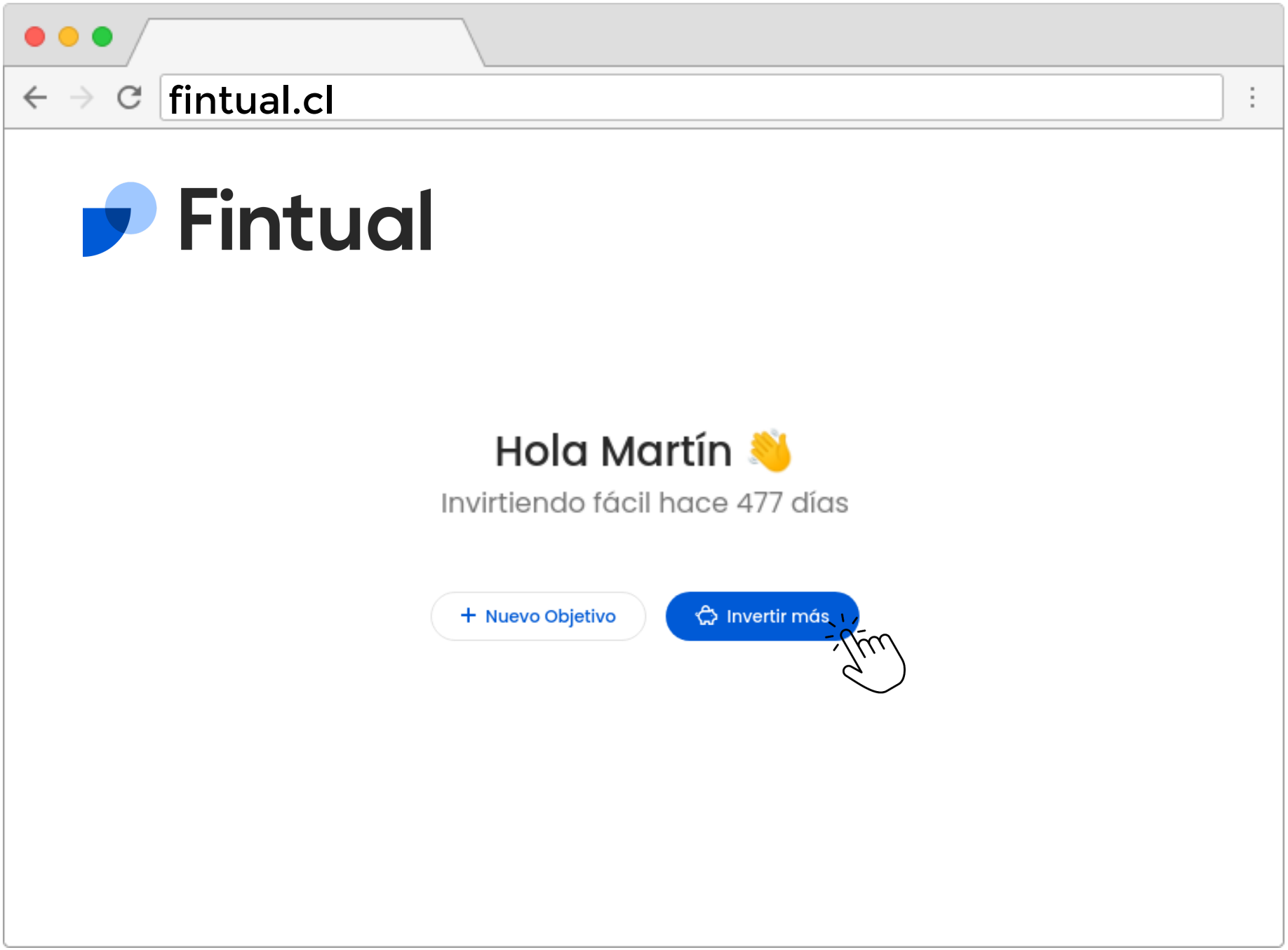
IIC3253

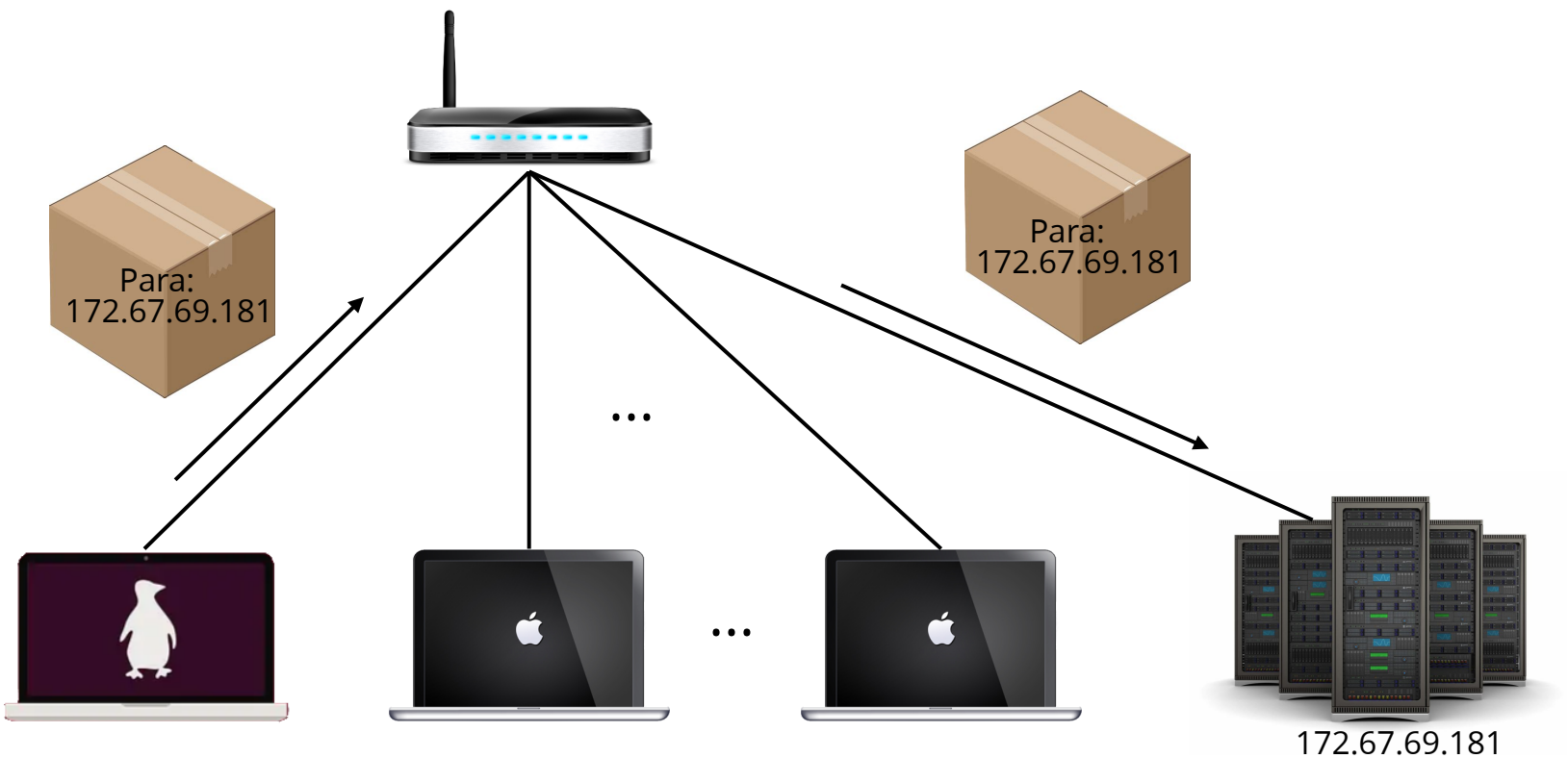
Seguridad en la Web


fintual.cl
Fintual
Hola de nuevo 👋
Email
ejemplo@ejemplo.com
Contraseña
Entrar

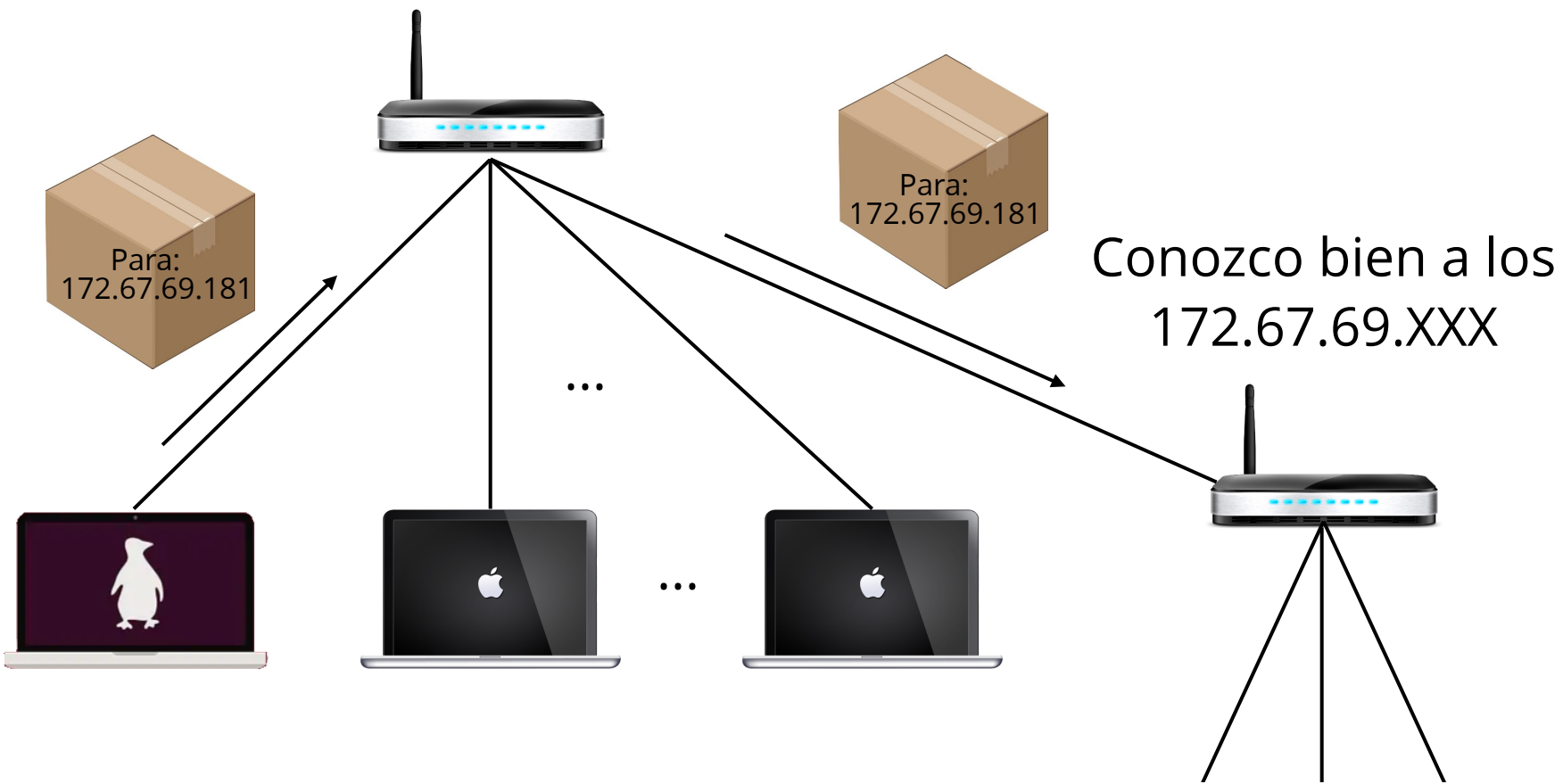

fintual.cl
Fintual
Hola Martín 👋
Invirtiendo fácil hace 477 días
+ Nuevo Objetivo
Invertir más

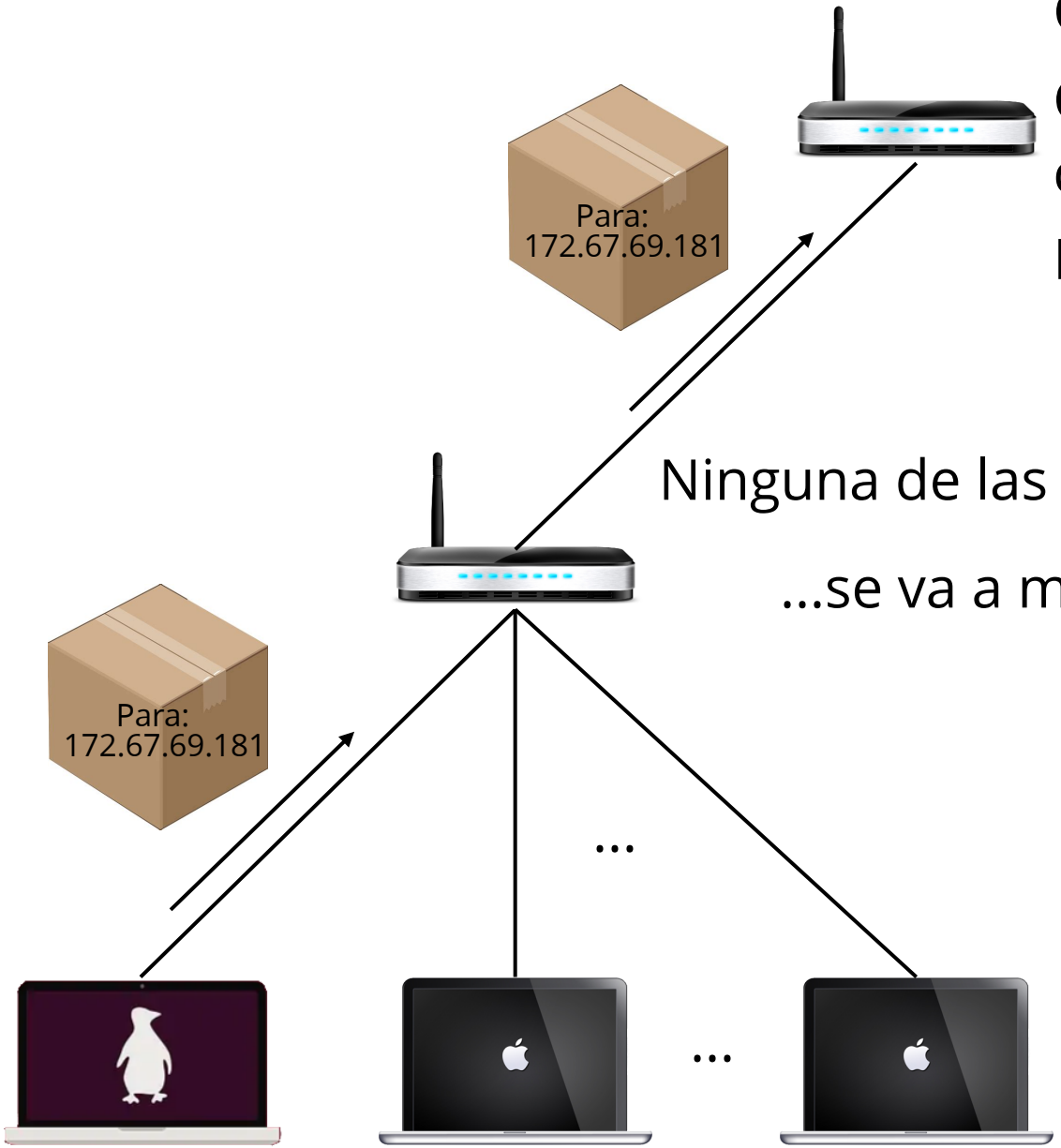

THAT'S IT?
TOO EASY.

Conozco esa dirección?



Conozco a alguien que conozca esa dirección?





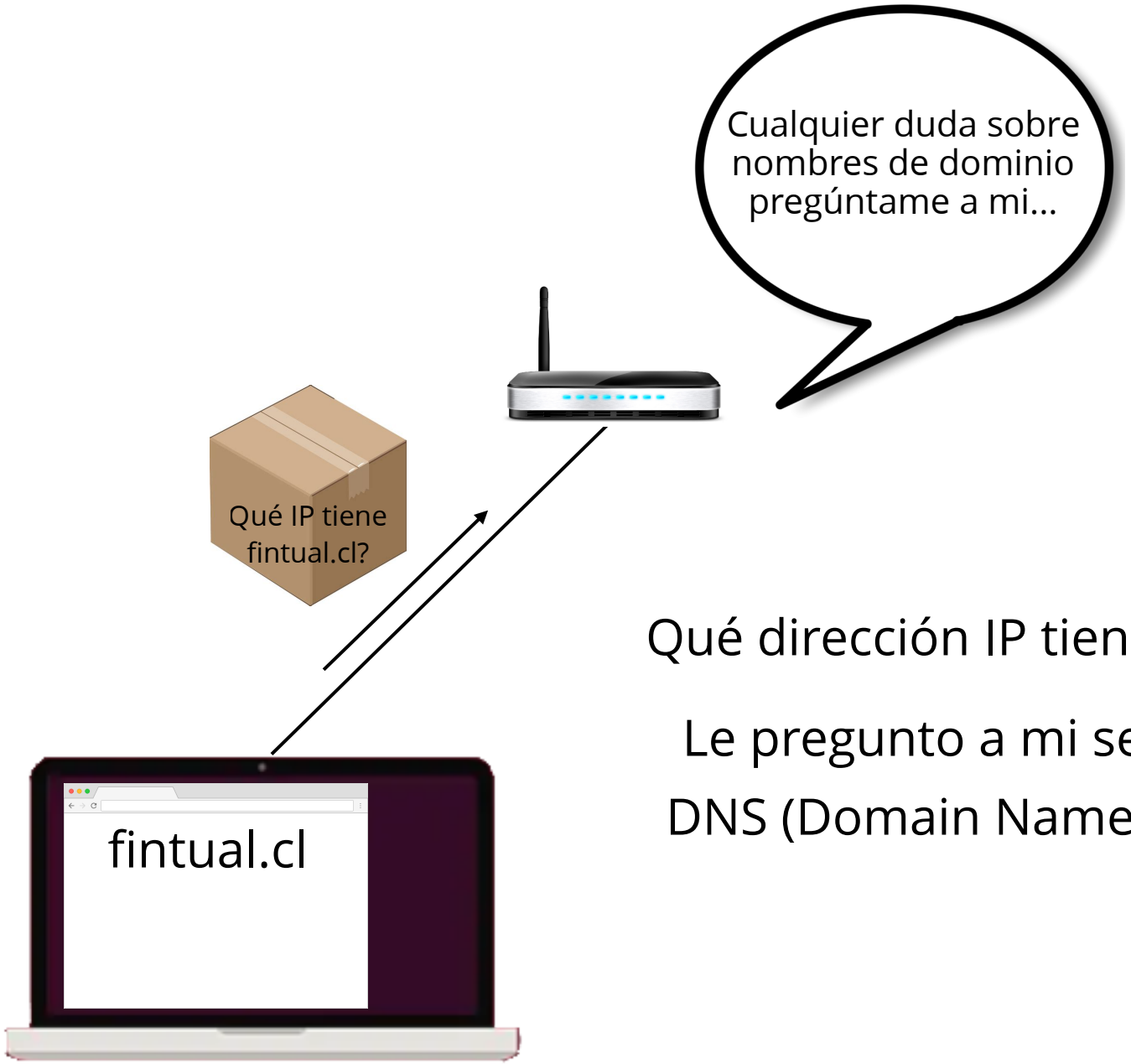
Conozco esa dirección?

Conozco a alguien que conoce esa dirección?

Ni idea, default route...

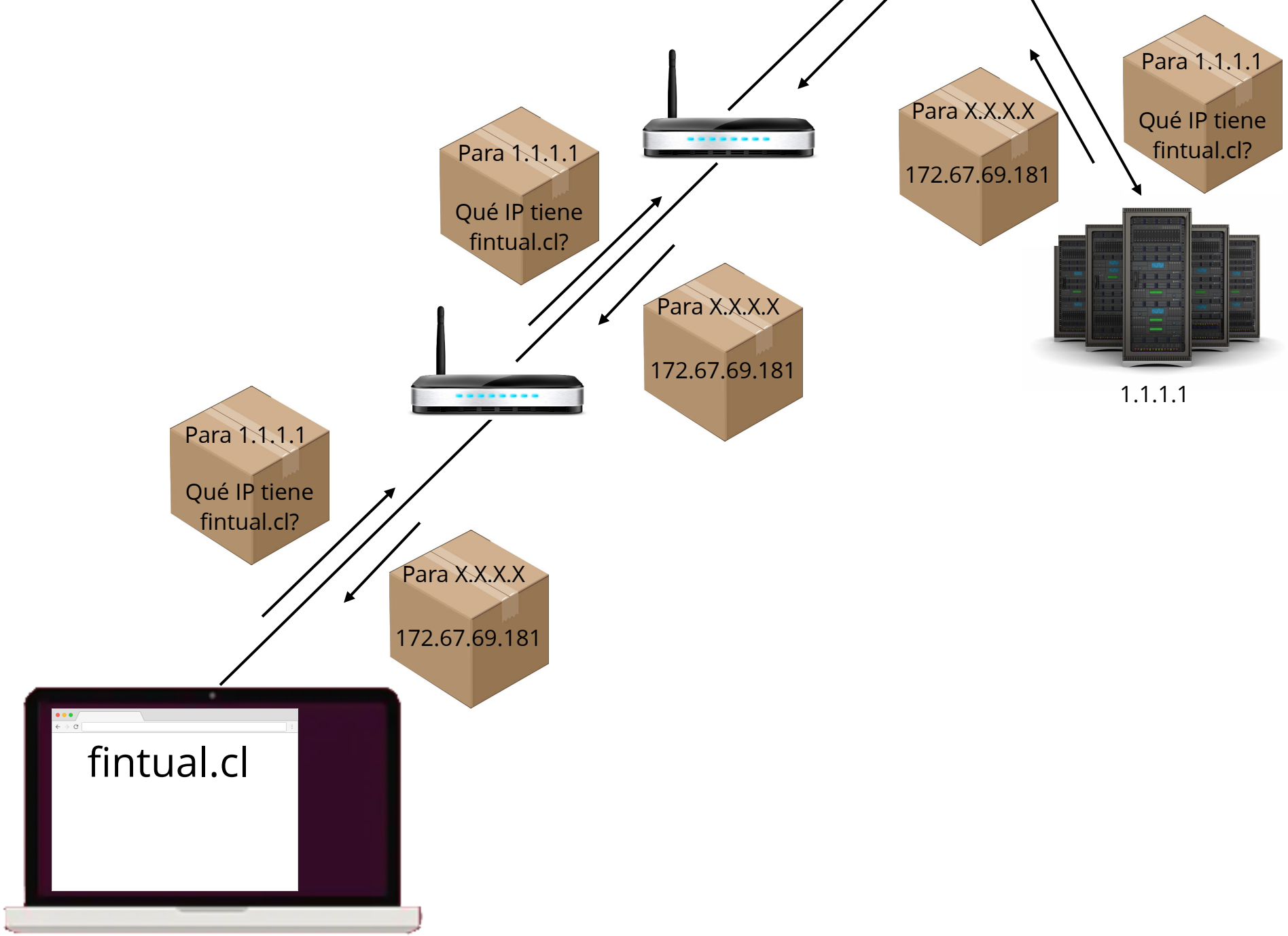
Ninguna de las anteriores...

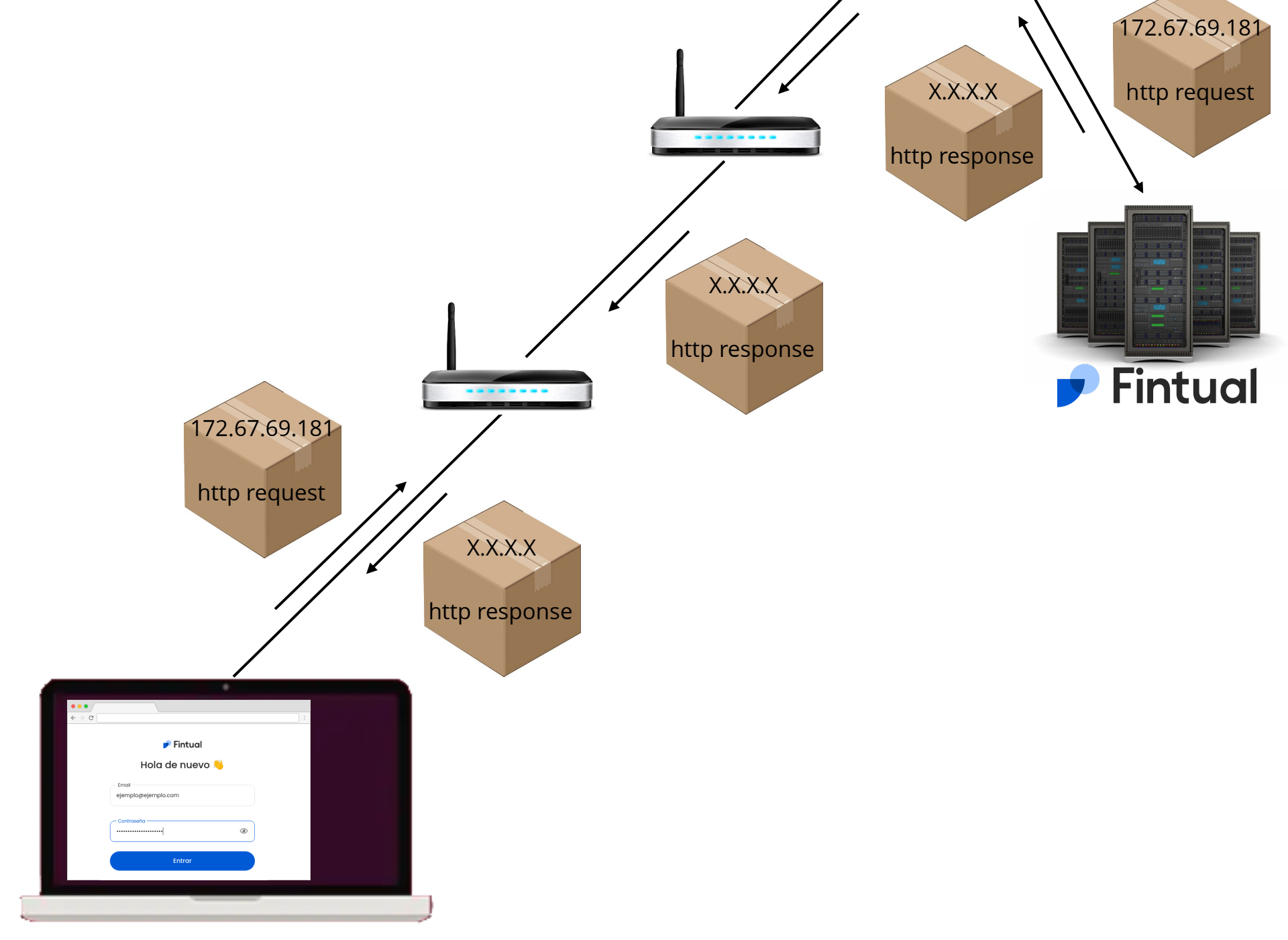
...se va a mi "default route"



Qué dirección IP tiene fintual.cl?

Le pregunto a mi servidor de DNS (Domain Name System)...

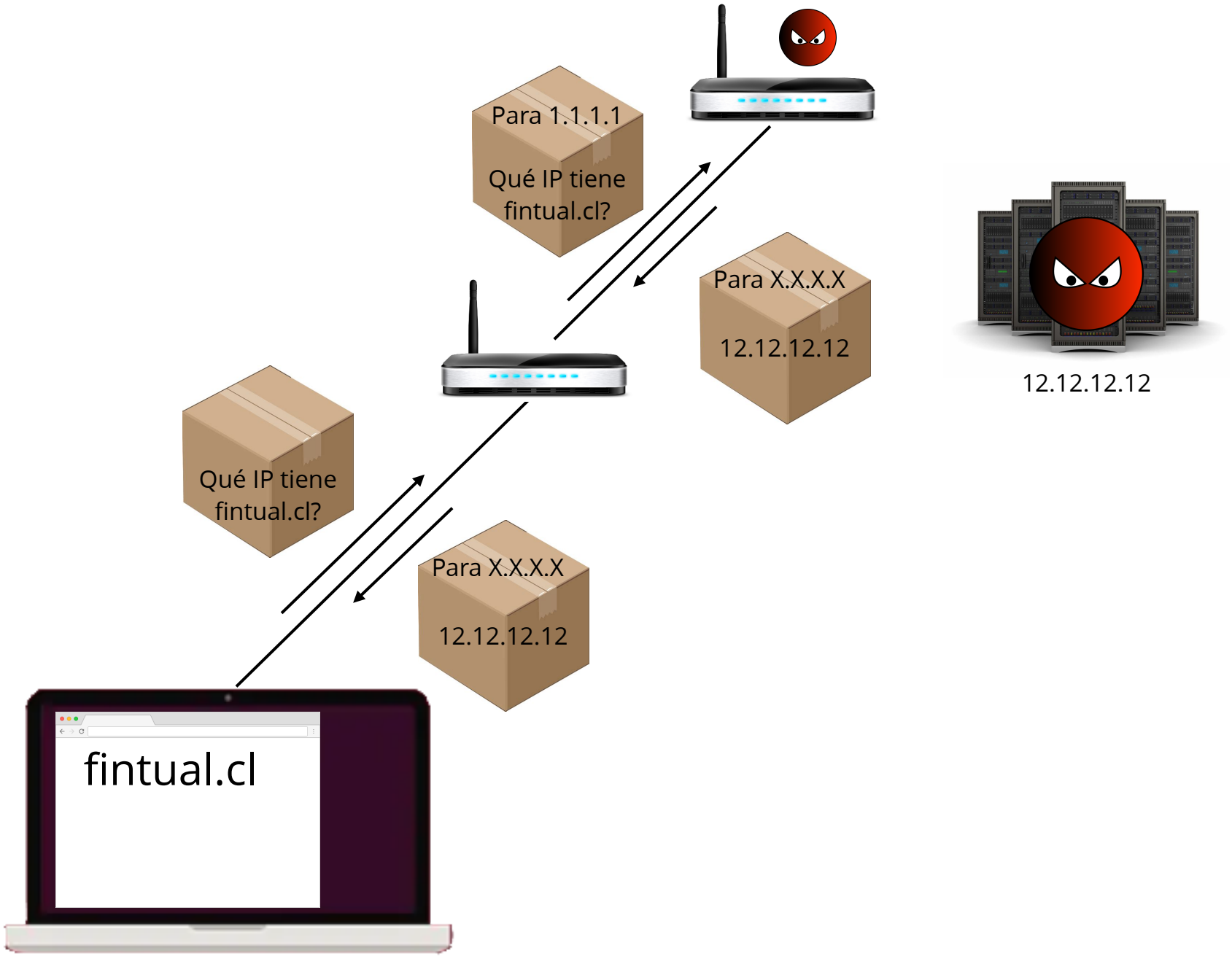

Para 1.1.1.1
Qué IP tiene fintual.cl?
Para X.X.X.X
172.67.69.181
Para 1.1.1.1
Qué IP tiene fintual.cl?
Para X.X.X.X
172.67.69.181
1.1.1.1
Para 1.1.1.1
Qué IP tiene fintual.cl?
Para X.X.X.X
172.67.69.181
fintual.cl

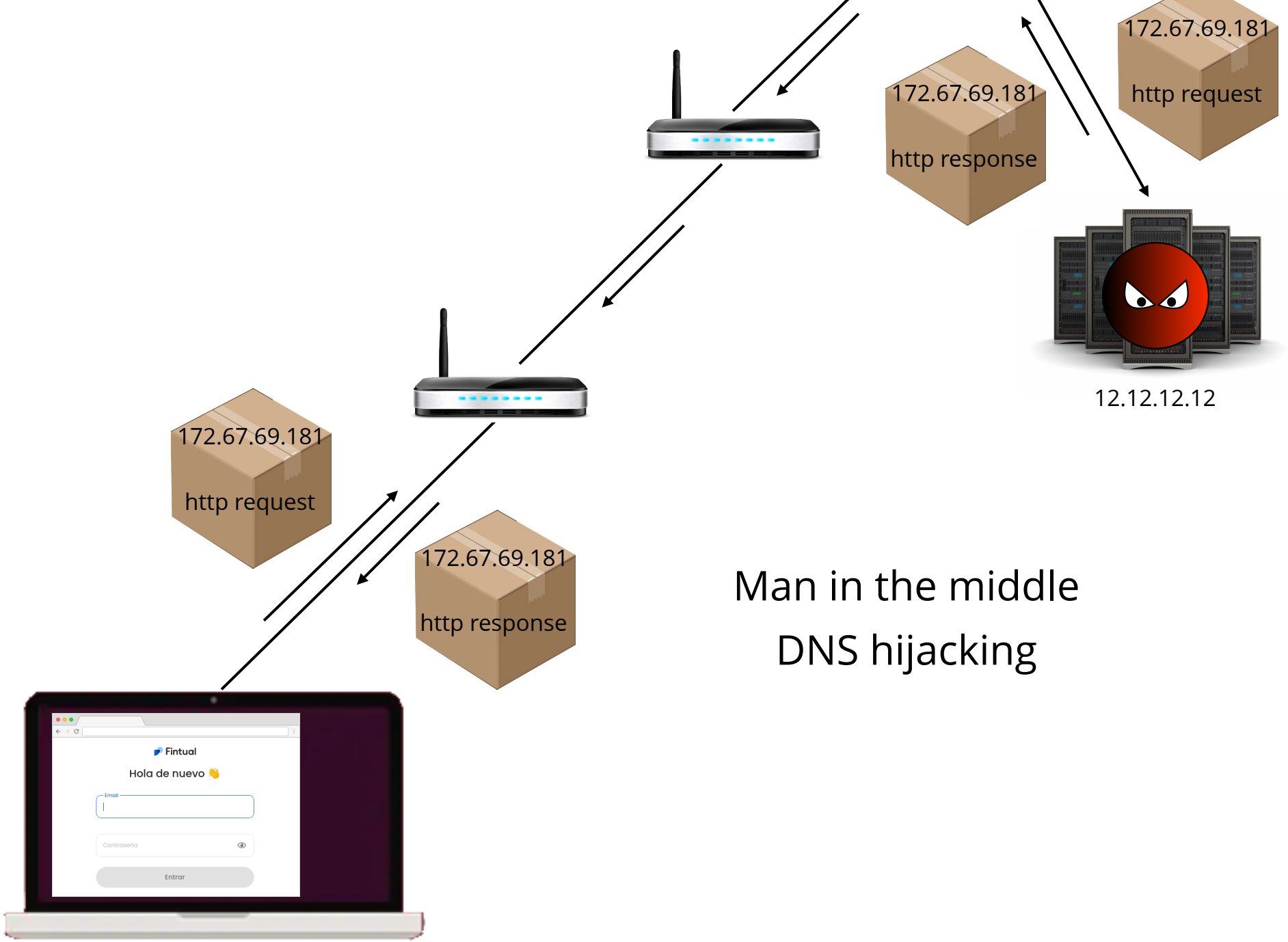

172.67.69.181
http request
X.X.X.X
http response
X.X.X.X
http response
172.67.69.181
http request
X.X.X.X
http response
Fintual
Fintual
Hola de nuevo 👋
Email
ejemplo@ejemplo.com
Contraseña
Entrar

Llegamos...

Vamos bien?

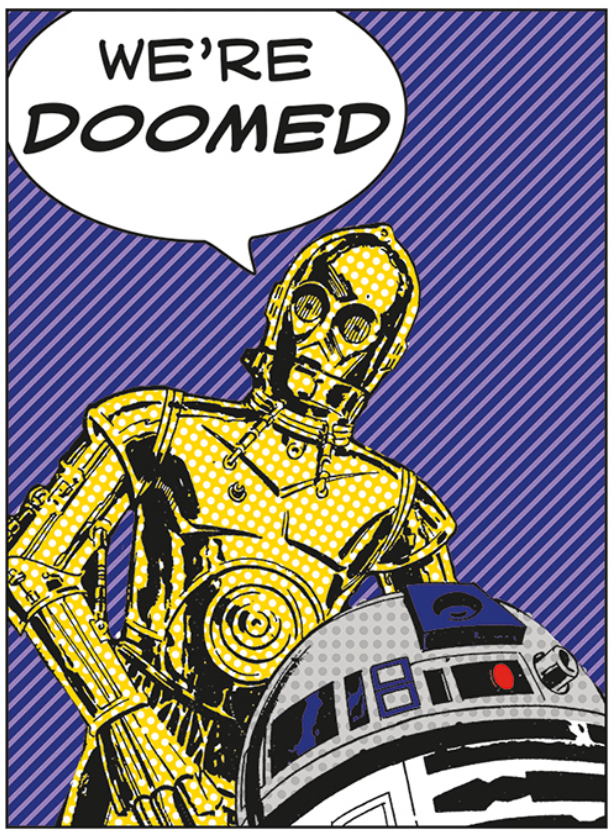
¿Problemas de seguridad?


Para 1.1.1.1
Qué IP tiene fintual.cl?
Para X.X.X.X
12.12.12.12
Qué IP tiene fintual.cl?
Para X.X.X.X
12.12.12.12
fintual.cl
12.12.12.12



Man in the middle
DNS hijacking

Soluciones?



Public-key crypto to the rescue

Fintual

Public key

Public key

Seguro y autentificado

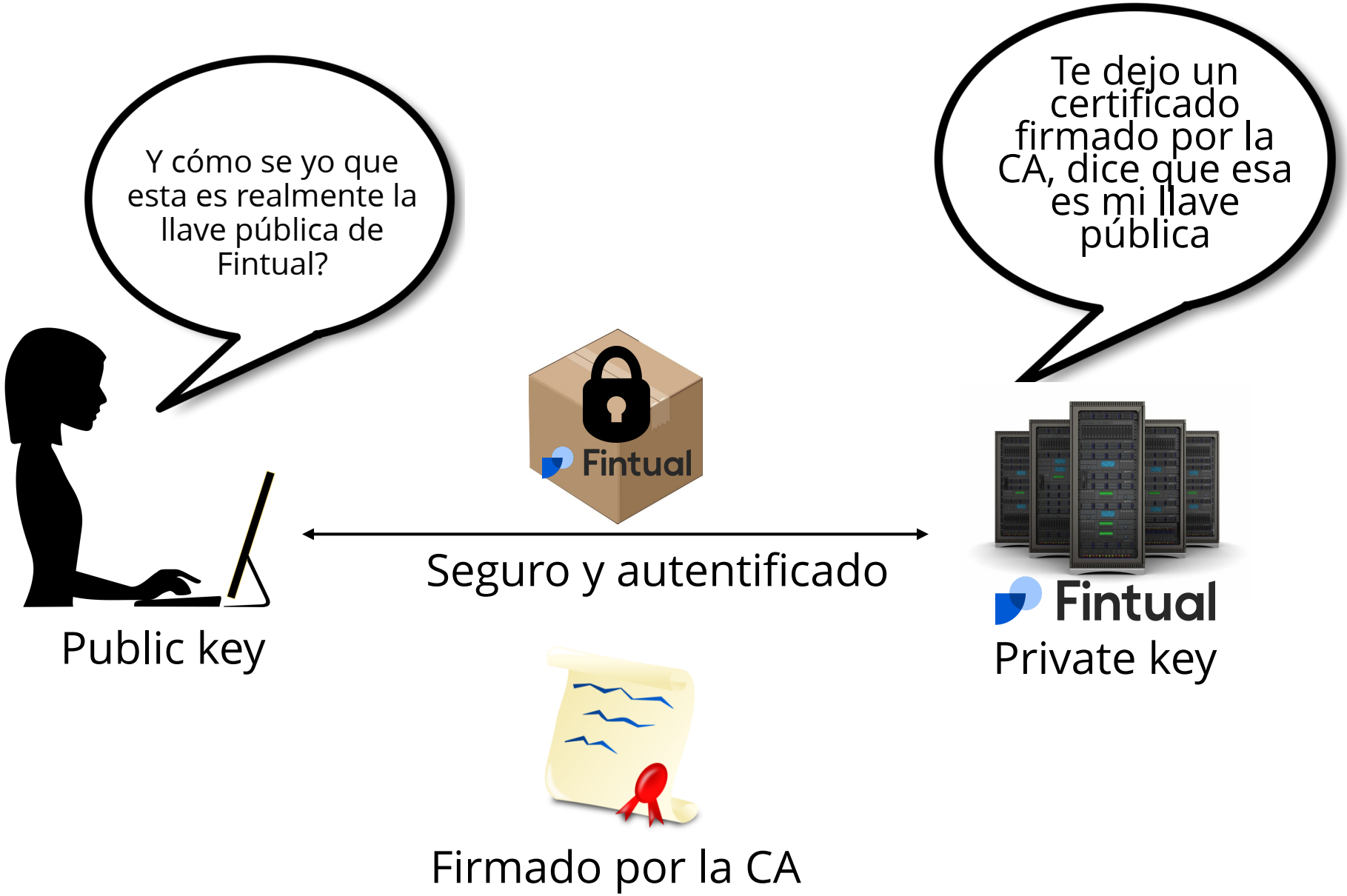
Fintual

Private key

Problemas?


Y cómo se yo que esta es realmente la llave pública de Fintual?
Fintual
Seguro y autentificado
Fintual
Public key
Private key

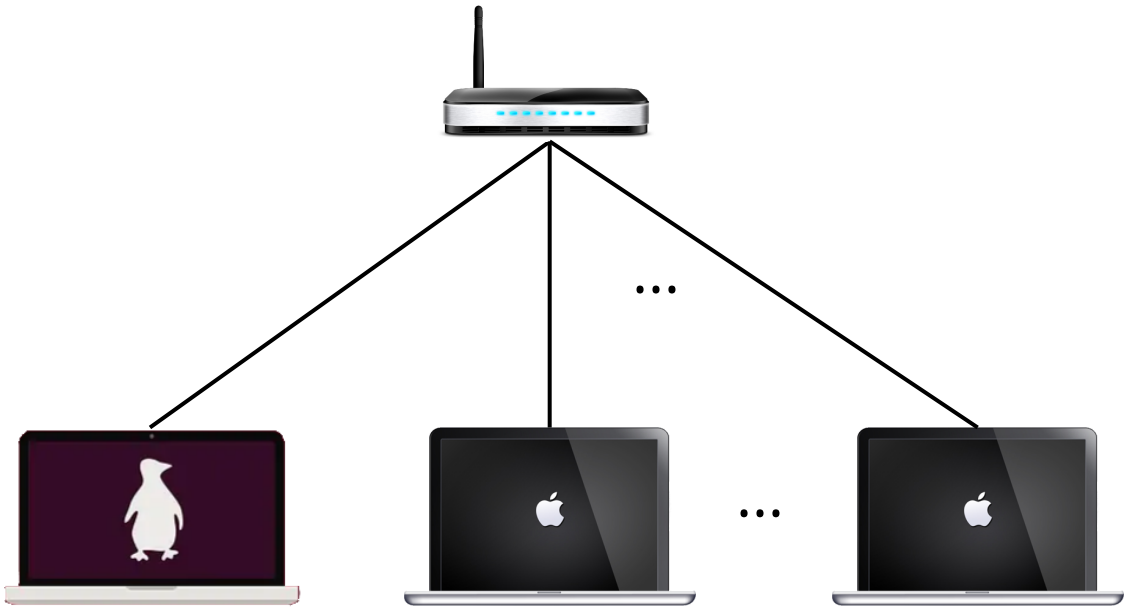
Certificate Authorities (CAs)


Y cómo se yo que esta es realmente la llave pública de Fintual?
Te dejo un certificado firmado por la CA, dice que esa es mi llave pública
Fintual
Seguro y autentificado
Public key
Fintual
Private key
Firmado por la CA

¿Más problemas?


Y cómo sé yo cuál es la llave pública de la CA?


DO NOT
QUESTION
AUTHORITY


CA's public key
CA's public key
CA's public key

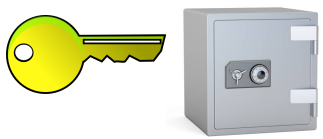

PUBLIC AUTHORITY


Y cómo se yo que esta es realmente la llave pública de Fintual?
Te dejo un certificado firmado por la CA, dice que esa es mi llave pública
Fintual
Seguro y autentificado
Public key
Fintual
Private key
Firmado por la CA

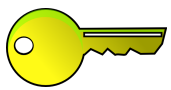
¿Cómo se obtiene este certificado?

Let's Encrypt

Free SSL For All

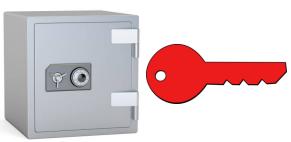


Quisiera sacar certificados para fintual.com, aquí mi llave pública



Primero, no te vayas a equivocar, firma <nonce> con la llave privada

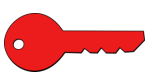
Además, tienes que poner este <nonce2> en fintual.com/<nonce3>



Listo!

Todo en orden!

Bacán! me darías un certificado para asegurar fintual.com con esta otra llave pública?



Firmado, verificar con

Listo!

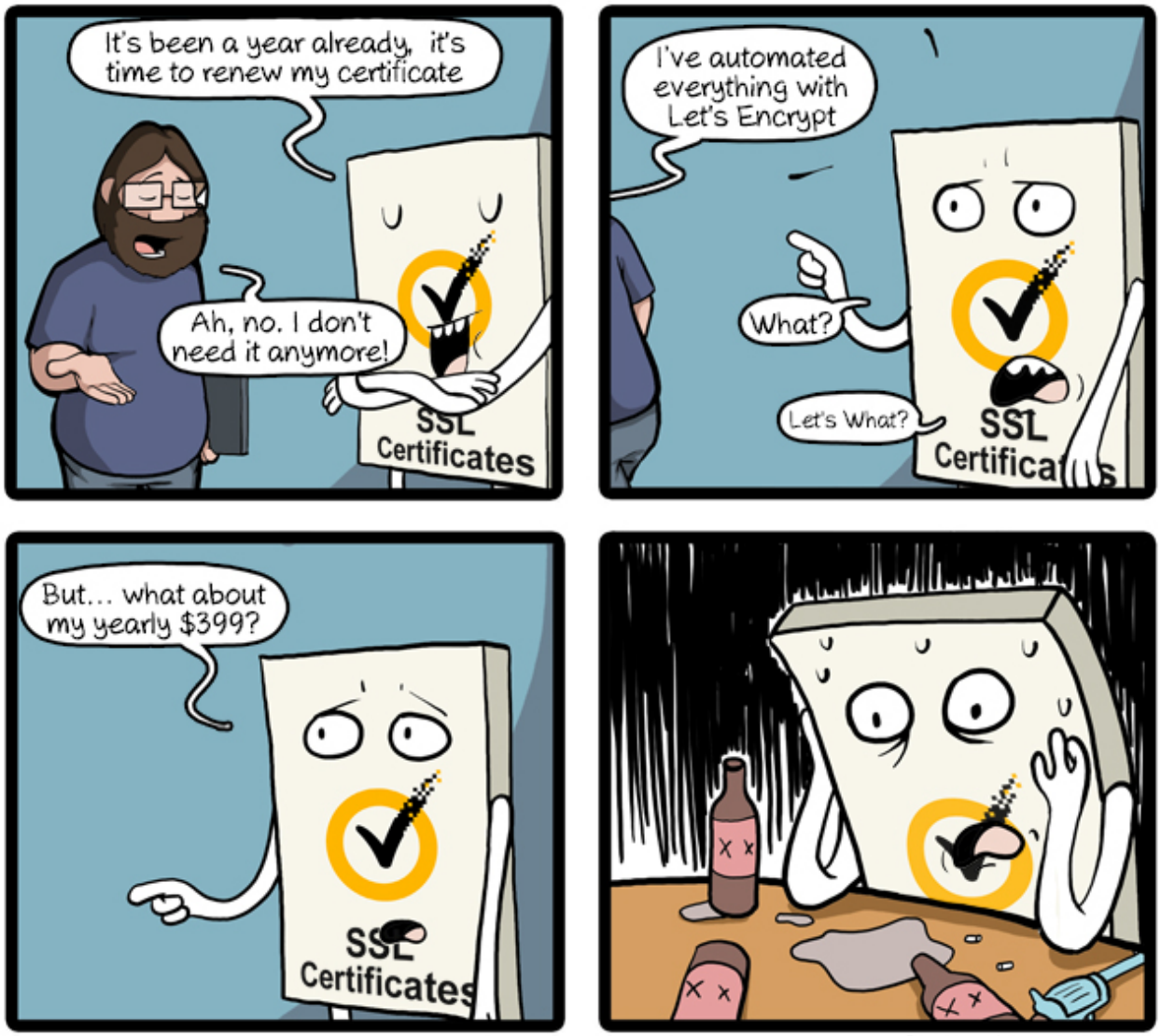
Gracias!

Estos certificados son bastante más complejos en estructura, pero el flujo anterior resume cómo se obtienen

Teniendo certeza de que estoy hablando con el dueño del sitio y tengo la llave pública, aseguramos la sesión con DH

https://tls12.ulfheim.net/

para (muchísimos) más detalles


It's been a year already, it's time to renew my certificate
Ah, no. I don't need it anymore!
SSL Certificates
I've automated everything with Let's Encrypt
What?
Let's What?
SSL Certificates
But... what about my yearly $399?
SSL Certificates
CommitStrip.com


Fintual
Seguro y autentificado
Fintual

https://fintual.cl

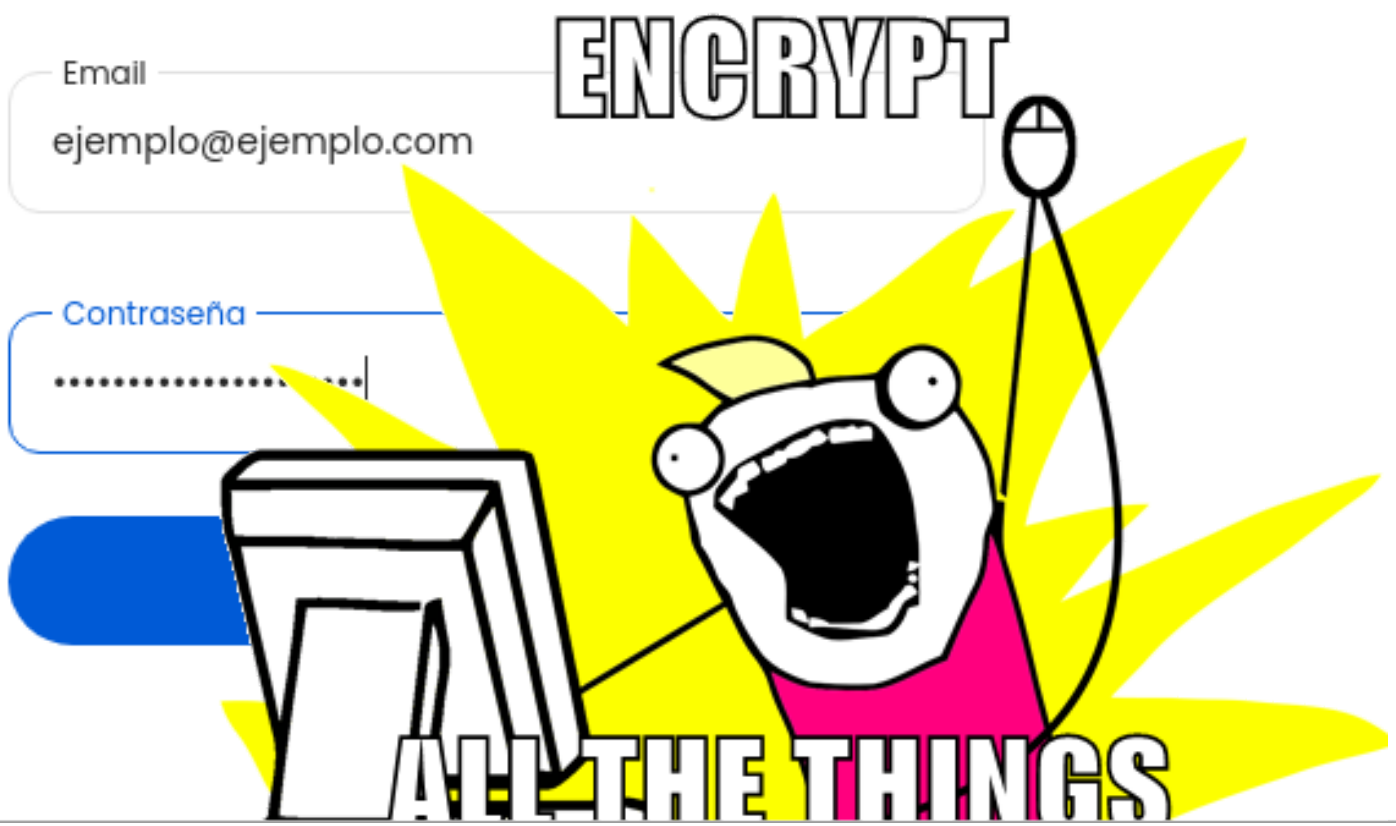
Fintual

Hola de nuevo 👋

Email

ejemplo@ejemplo.com

Contraseña



Ruteo IP

DNS

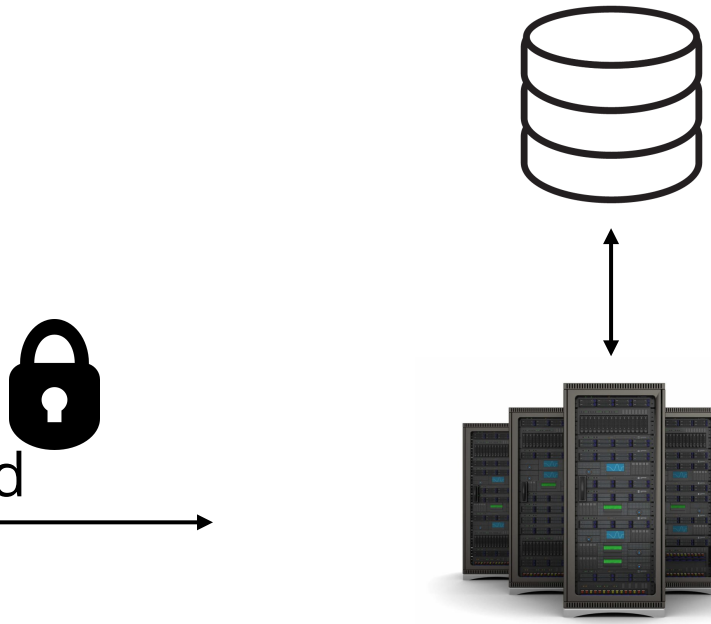
Https

Autoridades Certificadoras

Vamos bien?

Todavía?

Usuario, password

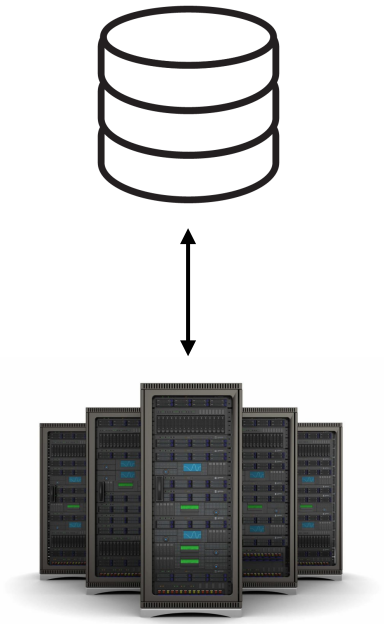


Fintual

Es cierto que este usuario tiene este password?

Correo	Password
atac@ble.com	1Cl4v3muyM4l4
vulner@ble.cl	1Cl4v3P3s1m4

Cualquier persona que gane acceso a la base de datos podría ver correos y contraseñas...



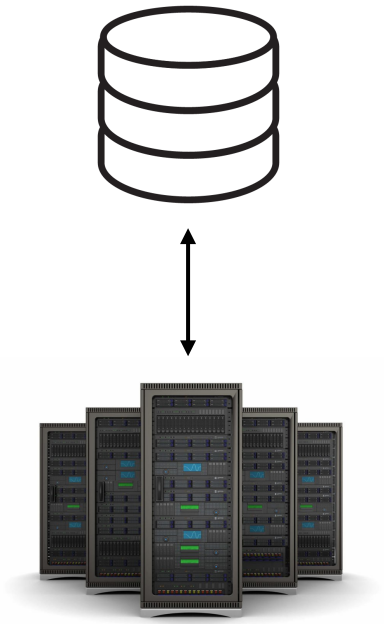
Fintual

Es cierto que este usuario tiene este password?

¿Cómo lo arreglamos?

Correo	SHA256(password)
atac@ble.cl	ef52045429b9094900170095d91e2bb6b78c514b
vulner@ble.cl	30df6af7eb3dd9e5b9944020440b9fc6d325beec

Mejor, pero todavía hay problemas...



Fintual

Es cierto que este usuario tiene este password?

Rainbow Tables

Las 500.000 Contraseñas más comunes de 2021

123456	356a192b7913b04c54574d18c28d46e6395428ab
123456789	da4b9237bacccdf19c0760cab7aec4a8359010b0
picture1	77de68daecd823babbb58edb1c8e14d7106e83bb
password	1b6453892473a467d07372d45eb05abc2031647a
12345678	ac3478d69a3c81fa62e60f5c3696165a4e5e6ac4
111111	c1dfd96eea8cc2b62785275bca38ac261256e278
123123	902ba3cda1883801594b6e1b452790cc53948fda
12345	da4b9237bacccdf19c0760cab7aec4a8359010b0
1234567890	77de68daecd823babbb58edb1c8e14d7106e83bb
...	...

Correo	**SHA256(password)**
atac@ble.cl	ef52045429b9094900170095d91e2bb6b78c514b
vulner@ble.cl	30df6af7eb3dd9e5b9944020440b9fc6d325beec

Hay algún hash de mi rainbow table en la tabla de usuarios?

Cómo arreglamos esto?

Correo	**Salt**	**Hash(password || Salt)**
c@lidad.cl	fz4/fho#hg%gjs	ef52045429b9094900170095d91e2bb6b78c514b
mejor@s.cl	zxc$f4(w@hvg>	30df6af7eb3dd9e5b9944020440b9fc6d325beec

Por qué no podemos atacar con rainbow tables?

Hagámoslo todavía más desagradable para los atacantes!

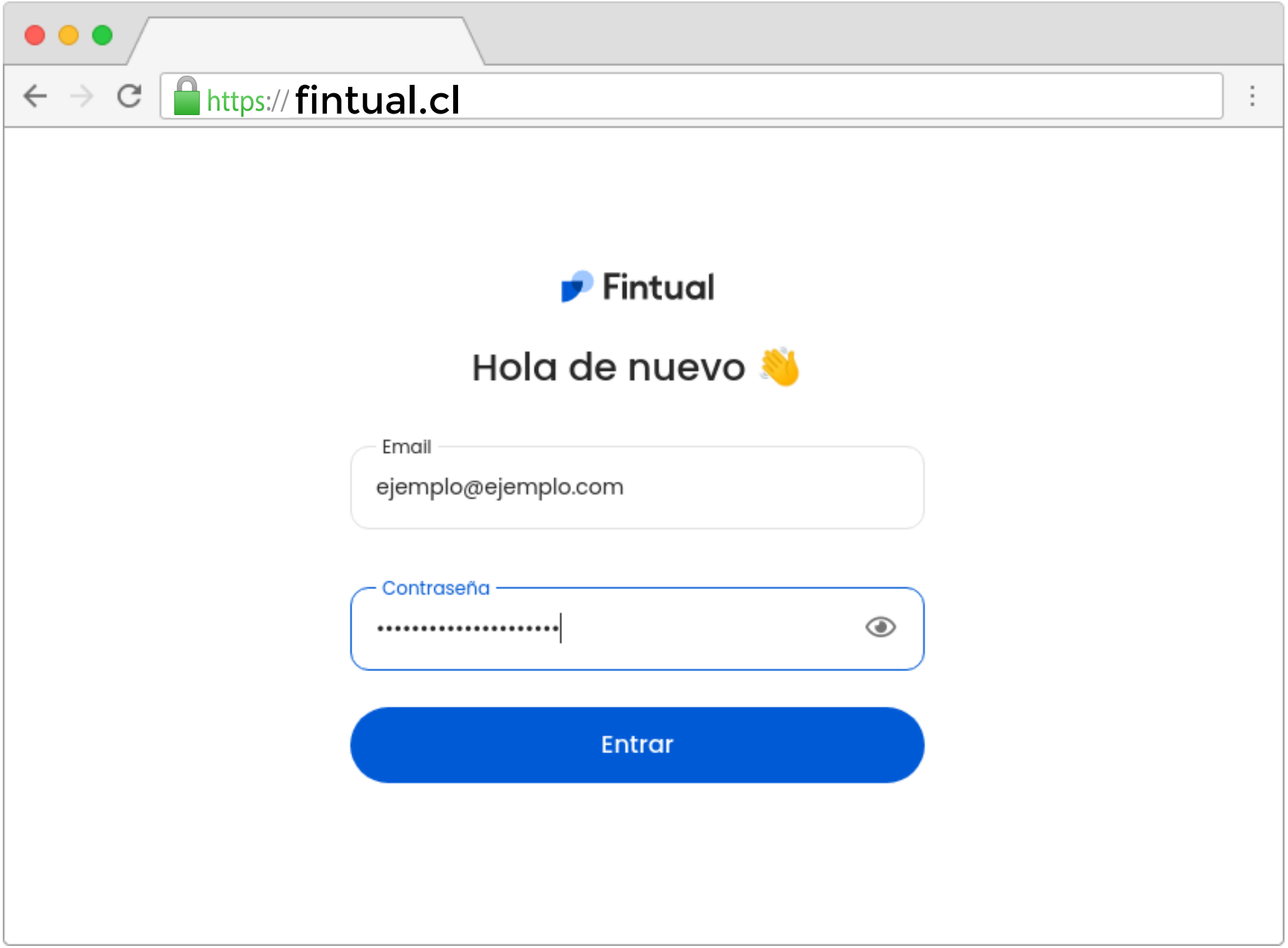
Correo	**HKDF(password)**
impec@ble.cl	pbkdf2_sha256$260000$W0U57Kqw5UDvasFO0YQccX$GAbxNa/PfEtEnS3APi5eV356wpdkfo3baQNdGsNn2e8=
inmejor@ble.cl	pbkdf2_sha256$260000$JxxEv17MH36GQeNaoqScmQ$5vfidwdL96PEWmaZMH3WrVPkoNXoMcO6JrOUKK24vf8=

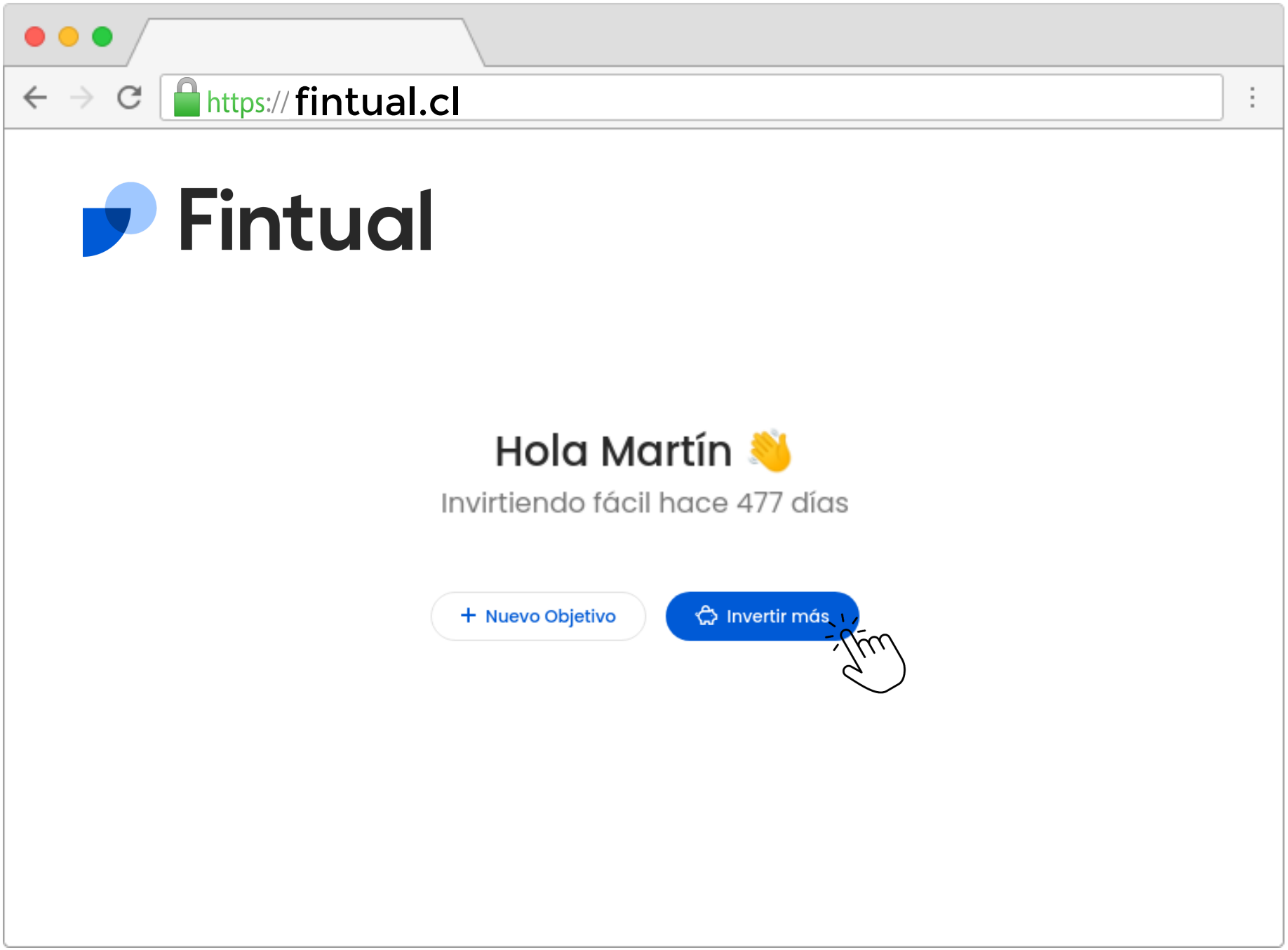
Usuario, password

Fintual

Es cierto que este usuario tiene este password?

¡Ganamos acceso!


https://fintual.cl
Fintual
Hola de nuevo 👋
Email
ejemplo@ejemplo.com
Contraseña
Entrar


https:// fintual.cl
Fintual
Hola Martín 👋
Invirtiendo fácil hace 477 días
+ Nuevo Objetivo
Invertir más

Quiero invertir más

¿Cómo lo arreglamos?

Usuario, password

`a7d88f9...360as9df`

Fintual

<Token> de sesión, en cada request envíamelo para saber que eres tú

¿Dónde lo guardamos?

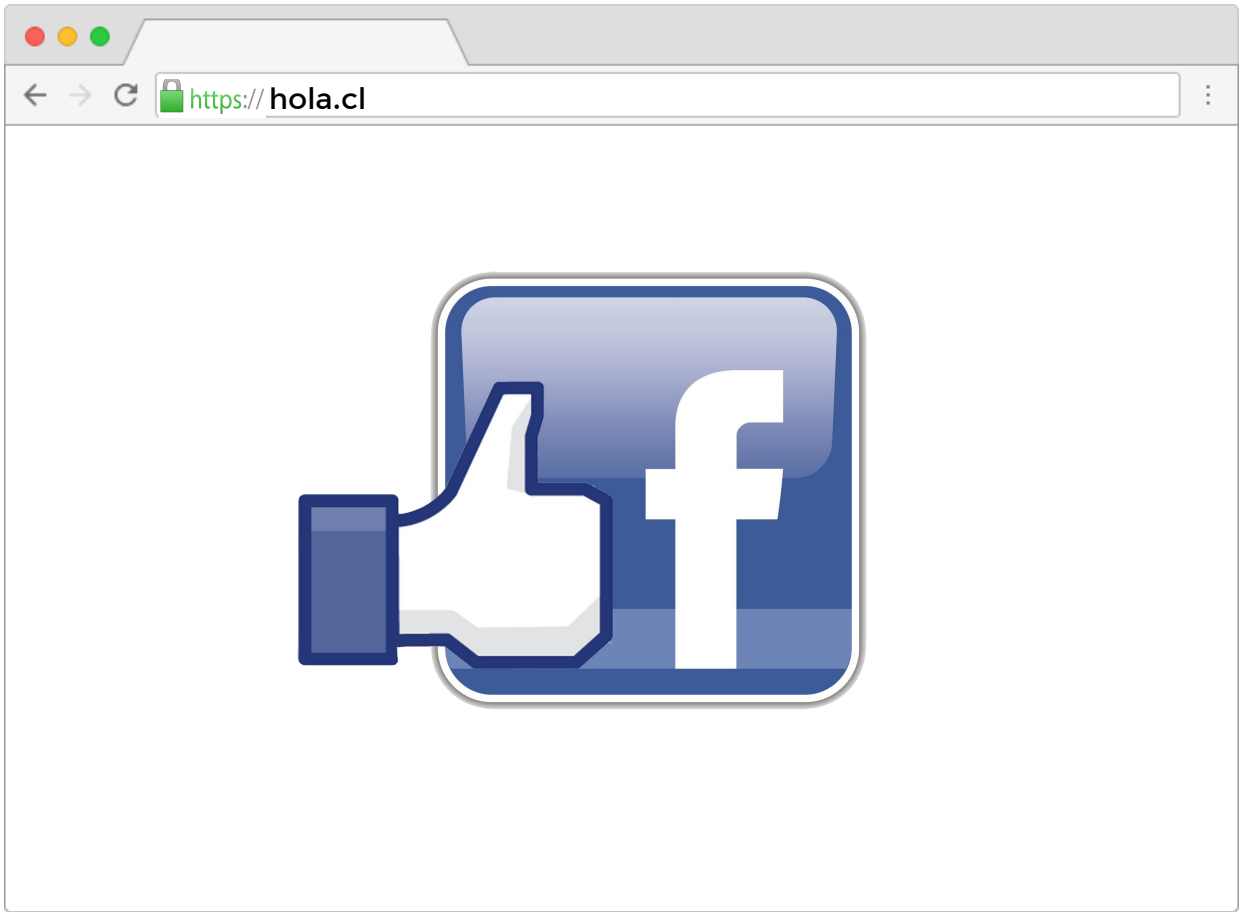
¿Opciones?

Variable en JavaScript

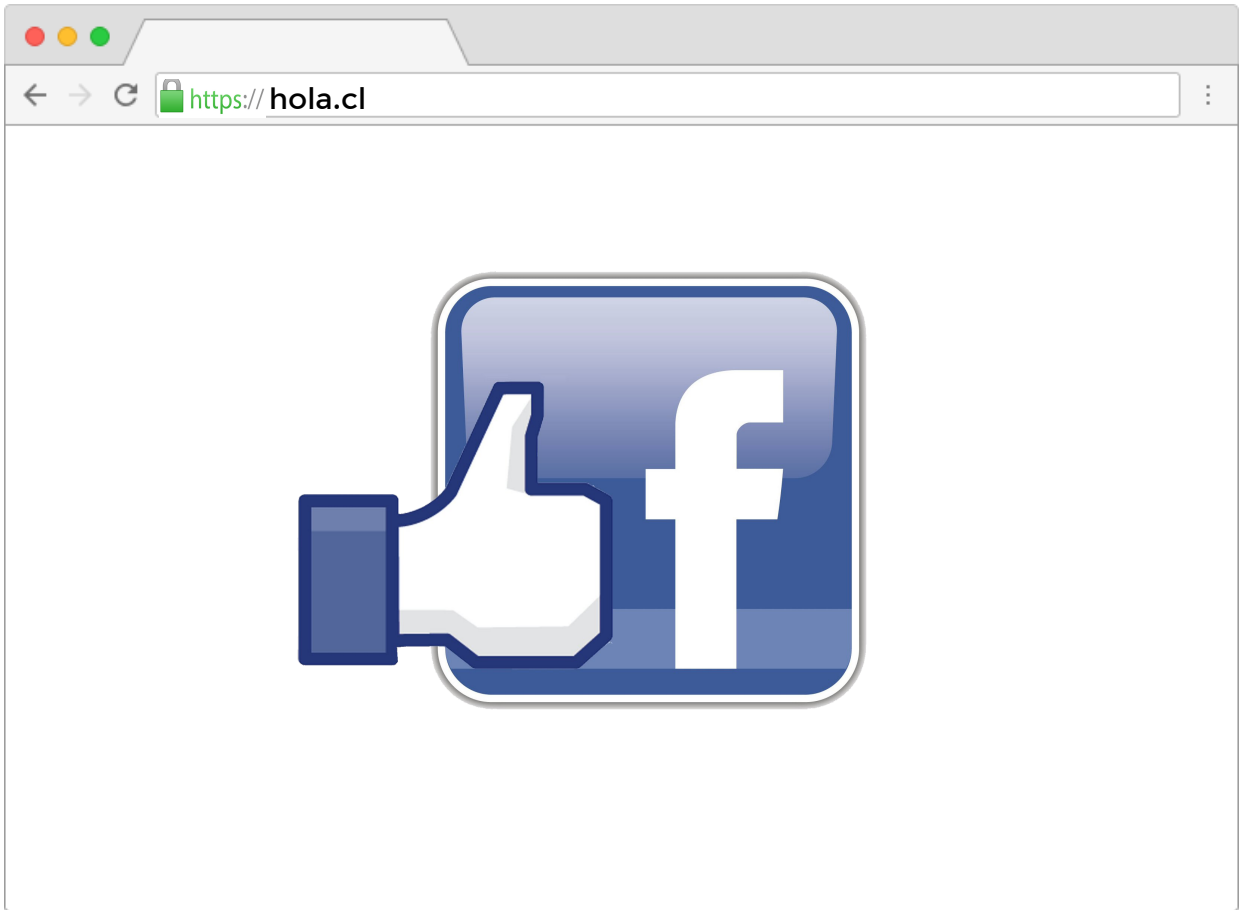
LocalStorage

Cookie

Variable en JavaScript	Muy volátil, difícil de saber si se cambia 
LocalStorage	Podría ser buena idea, ¿pero qué pasa si alguna librería en mi *node_modules* está infectada? 
Cookies	Suena razonable. ¿Qué problema podríamos tener?  HTTP_ONLY: Para que no la pueda leer el JS



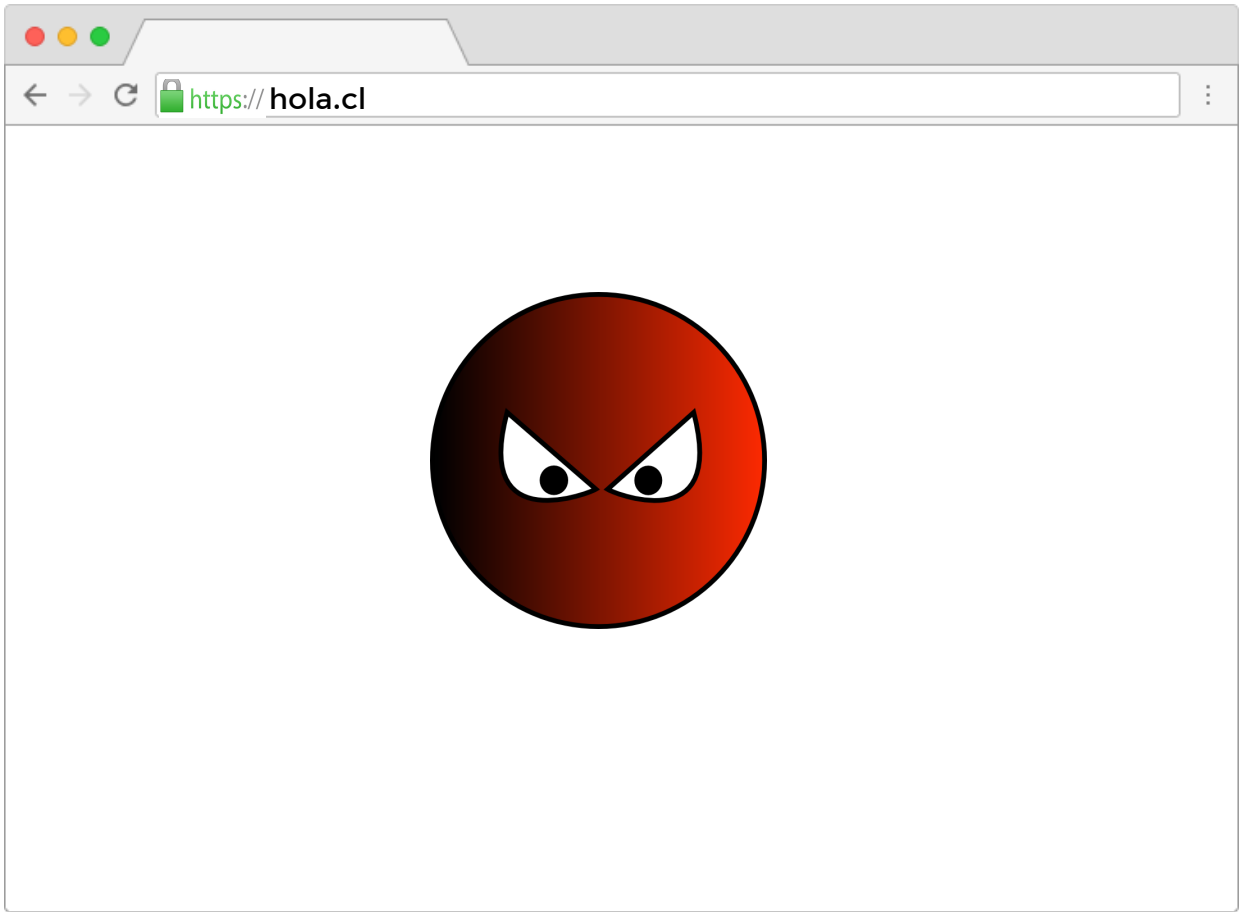
Le estoy dando un like a hola.cl!!



¡Soy yo dando un like!
(Acá van mis cookies)

¡Perfecto!

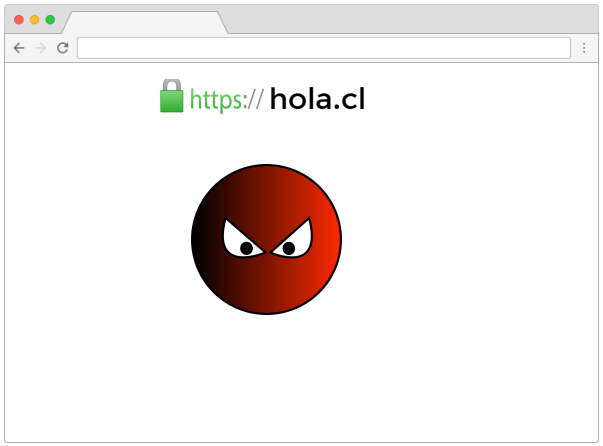
¿Problemas?

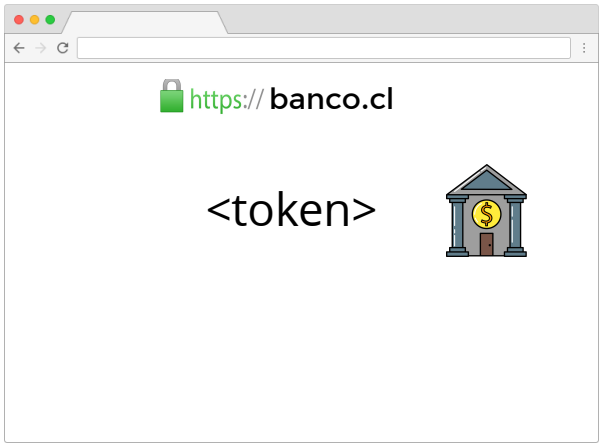


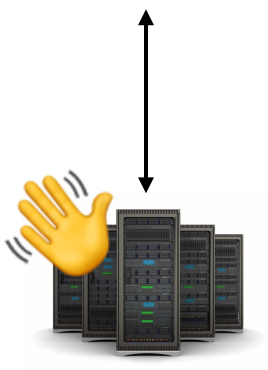
Cross-site
reference forgery

Quiero hacer esta transferencia,
(Acá van mis cookies)

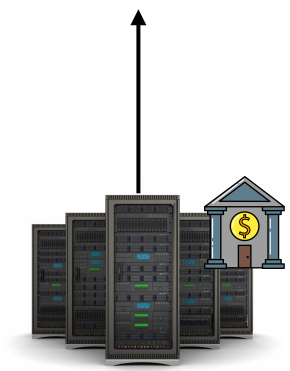
¡Perfecto!







Quiero transferir
(Acá van mis cookies)



user_id	token
1	f2...e4
27	a0...15

Para hacer algo "delicado",
mándame siempre el token

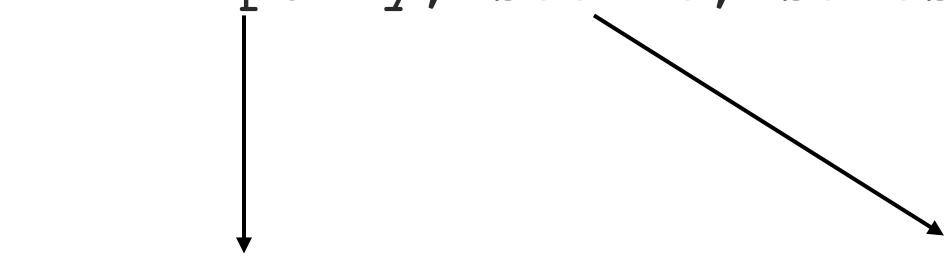
Cross-site reference forgery token

A.K.A. **csrf_token**

Esta es la forma "tradicional" de mitigar CSRF

Actualmente (desde ~2020) hay mejores formas de protegerse de estos ataques

```
Set-Cookie: SESSION_TOKEN=ad94...e10;
  HttpOnly; Secure; SameSite=Strict
```



Inaccesible por JS

Sólo se envía por HTTPS

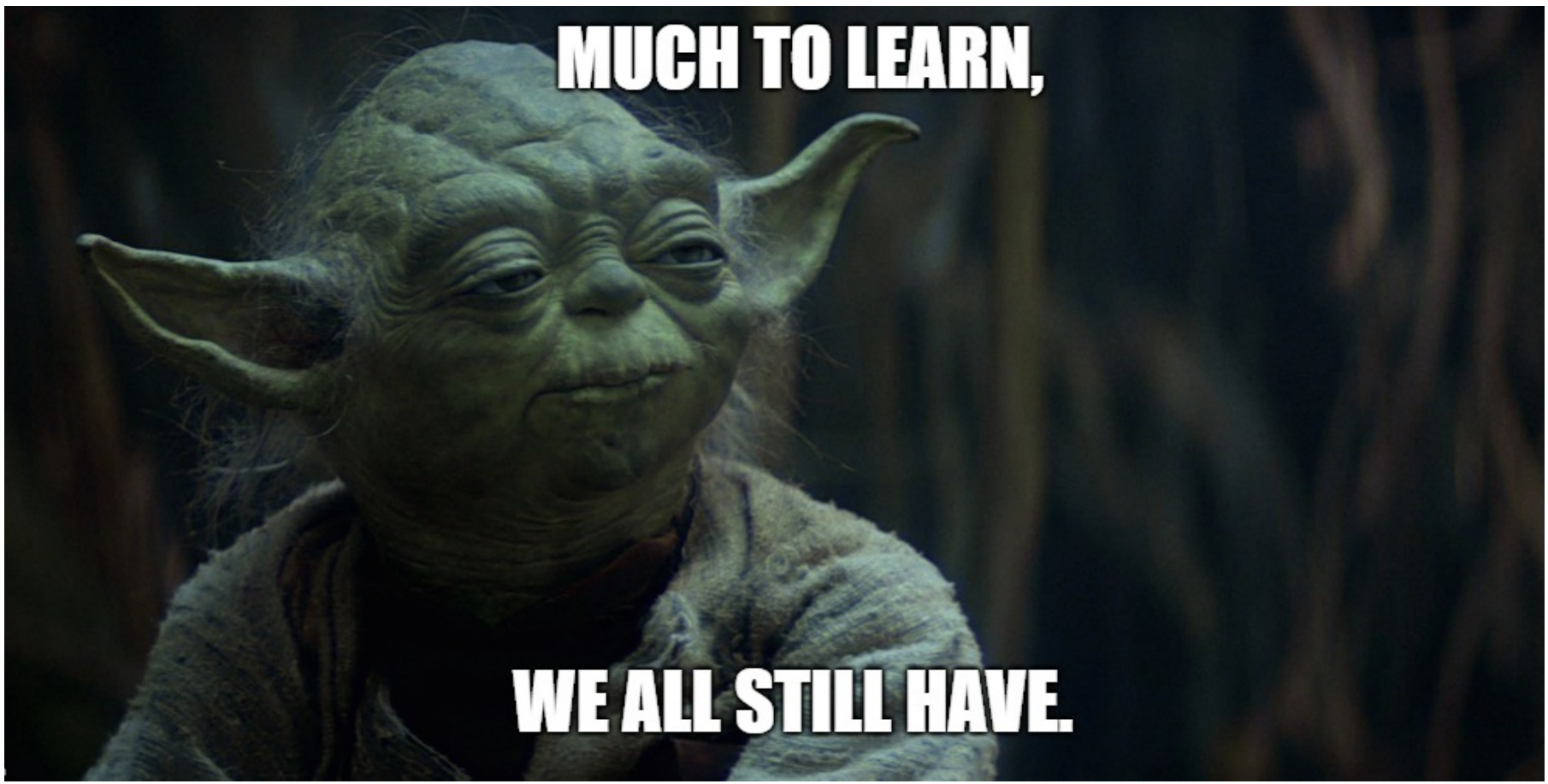
SameSite

El atributo SameSite de una cookie puede tener tres valores

None: La cookie se manda siempre (default hasta ~2020)

Strict: La cookie se manda sólo si el request se inició en el mismo sitio.

Lax: La cookie se manda en requests iniciados por el mismo sitio, y en requests iniciados por otros sitios en los que **cambia la url en la barra de direcciones**



Pero ya tenemos las herramientas necesarias...