DNS

Fundamentos de DNS e introducción a DNSSEC

Carlos Martínez, Lacnic
Nicolás Antoniello, ICANN

Semana de Nombres de Dominio en LAC
24 de Noviembre de 2020

¿Para qué DNS ?

Nombres y Números (o direcciones)

- Los dispositivos se identifican (de forma única) a través de Internet mediante direcciones IP (de la misma forma que usamos números de teléfono para identificar terminales telefónicas o dispositivos móviles en una red de telefonía).

  IPv4: 192.0.2.7
  IPv6: 2001: db8 :: 7

- Aunque los números son fáciles de usar para las máquinas, el cerebro humano tiende a preferir recordar nombres.

- Luego viene el Sistema de Nombres de Dominio (DNS) para traducir o asociar nombres a números… para que la gente pueda recordar y usar nombres mientras los dispositivos siguen usando números como identificadores.

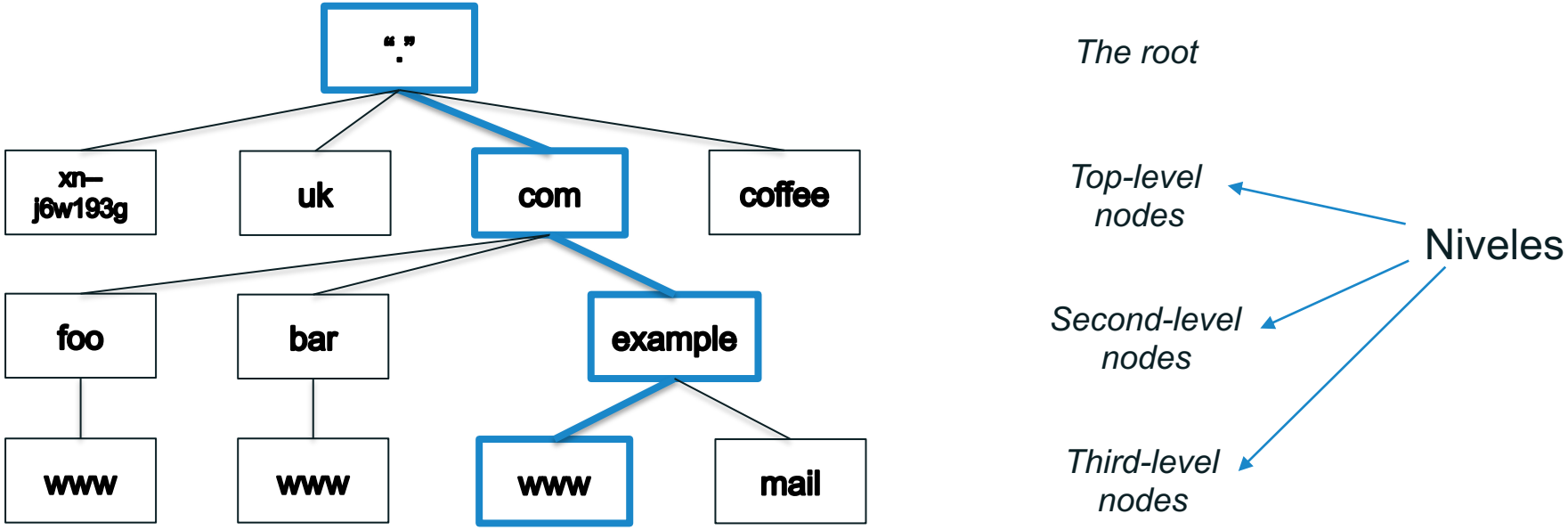
Resolución de Nombres

- El mapéo de nombres a direcciones IP (y direcciones IP a nombres) es lo que denominamos *resolución de nombres*.
- La resolución de nombres en los primeros años de Internet utilizaba un archivo de texto sin formato llamado HOSTS.TXT
  - Misma función pero formato ligeramente diferente al anterior /etc/hosts
  - Mantenido de forma centralizada por el NIC (Network Information Center) en el Stanford Research Institute (SRI)
  - Los administradores de red enviaban las actualizaciones por correo electrónico
- El objetivo era que todos tuvieran la última versión del archivo
  - Lanzado una vez por semana
  - Descargable vía FTP

Características del DNS …

Nombres de Dominio

- La estructura de la base de datos DNS es un árbol invertido llamado *espacio de nombres (**domain names**)* (piense en DNS como un enorme almacén distribuido para almacenar información destinada a ser accesible para cualquier persona en Internet).
- Cada nodo (excepto la raíz) tiene una etiqueta llamada nombre de dominio.
- Ese nombre de dominio se crea secuenciando etiquetas de nodo desde un nodo específico hasta la raíz, separadas por puntos (esta identificación inequívoca de un nombre de dominio a menudo se denomina nombre de dominio completo (***fully qualified domain name: FQDN***).

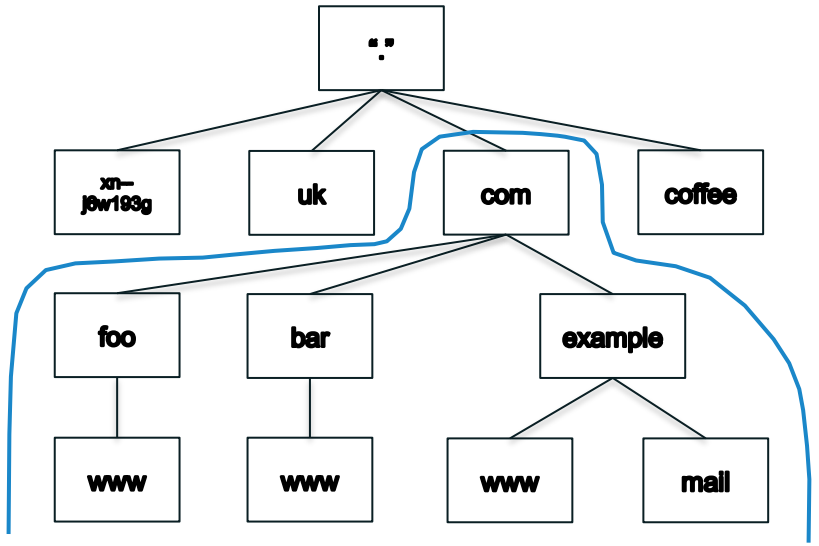


Dominios y Delegación de Administración (Zonas)

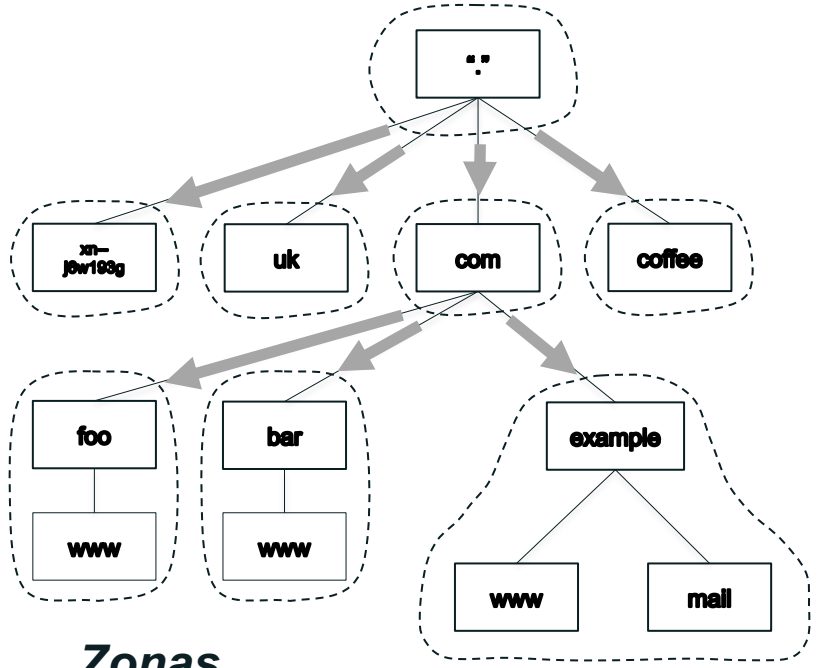
- Ahora, si administramos un enorme almacén distribuido de información, destinado a ser accesible para cualquier persona en Internet, necesitaremos ayuda para operarlo y algunos estándares para poder almacenar, administrar e intercambiar esa información.
- Y ahí viene la definición del ***dominio*** y la posibilidad de ***delegar*** la gestión de partes (***zonas***) del almacén (DNS) para permitir la administración distribuida (por eso las divisiones administrativas se denominan zonas).
- Entonces, una zona sería un estante en nuestro almacén para almacenar datos. Mientras que un dominio se define como un nodo y todo lo que está debajo de él (todo el subárbol debajo de un nodo).

La ***delegación*** crea zonas:
- La zona de delegación se denomina ***Padre***.
- La zona delegada es la ***Hija***.

Algunos de los datos almacenados en zonas:
- Dirección IPv4 para un nombre (A)
- Dirección IPv6 para un nombre (AAAA)
- Servidor de correo para un nombre (MX)



Dominio "**com**"



Zonas

Proceso de resolución de nombres de dominio…

Definiciones

- Recordar que el DNS es una base de datos distribuida:
  - Los datos se mantienen localmente (en nuestro enorme almacén distribuido) pero están disponibles a nivel mundial.

- ***Resolver*** (o servidores recursivos): envían consultas (son como proveedores de servicios encargados de buscarnos los datos, para no tener que buscarlos nosotros mismos en los estantes del almacén).

- ***Servidores autoritativos***: responden consultas (las cajas o contenedores en los estantes de nuestro almacén que contienen todos los datos).

- El ***proceso de resolución*** es la implementación de la traducción de una dirección IP a un nombre de dominio, o más general, obtener la respuesta para una consulta específica.

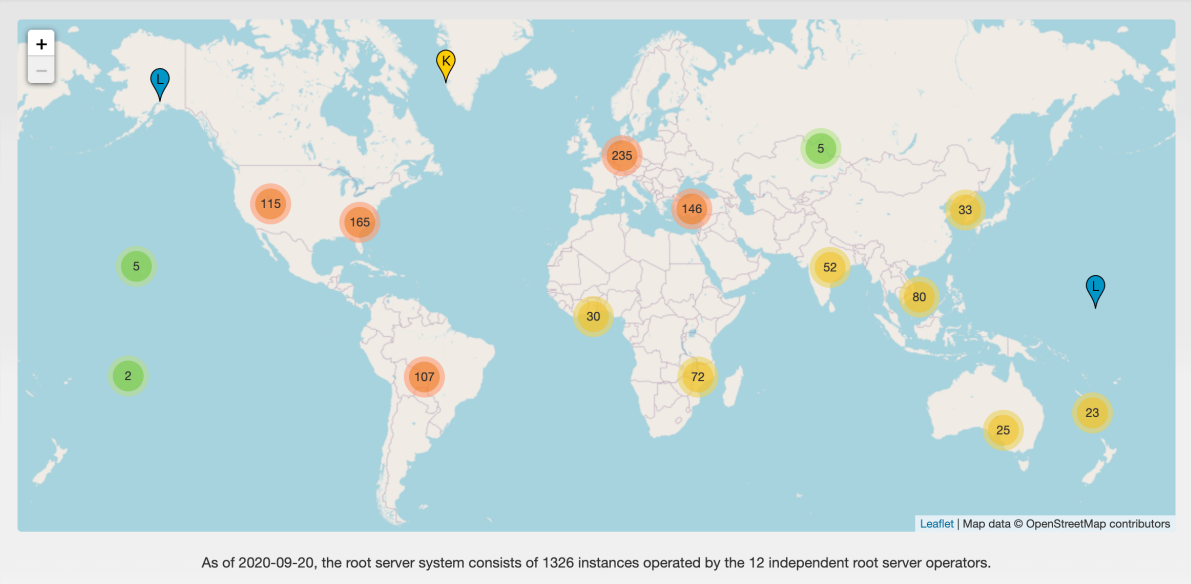
Optimizando el Sistema

- ***Almacenamiento en caché***: básicamente, estos proveedores de servicios (resolutores) pueden recordar la información que encuentran en el almacén para no tener que volver a buscarla cada vez que alguien solicita lo mismo (así que recuerde que el almacenamiento en caché ocurre en los resolutores).

- ***Replicación***: es aconsejable mantener varias copias de nuestros estantes (todas con la misma información) para poder colocarlas lo más cerca posible de los proveedores de servicios (recursivos). Por lo tanto, proporciona menos tiempos de resolución (el almacenamiento de información está más cerca), equilibrio de carga (ya que proporciona acceso a diferentes estantes en lugar de todos los mismos) y, por supuesto, hace que todo el sistema sea más robusto y resistente.

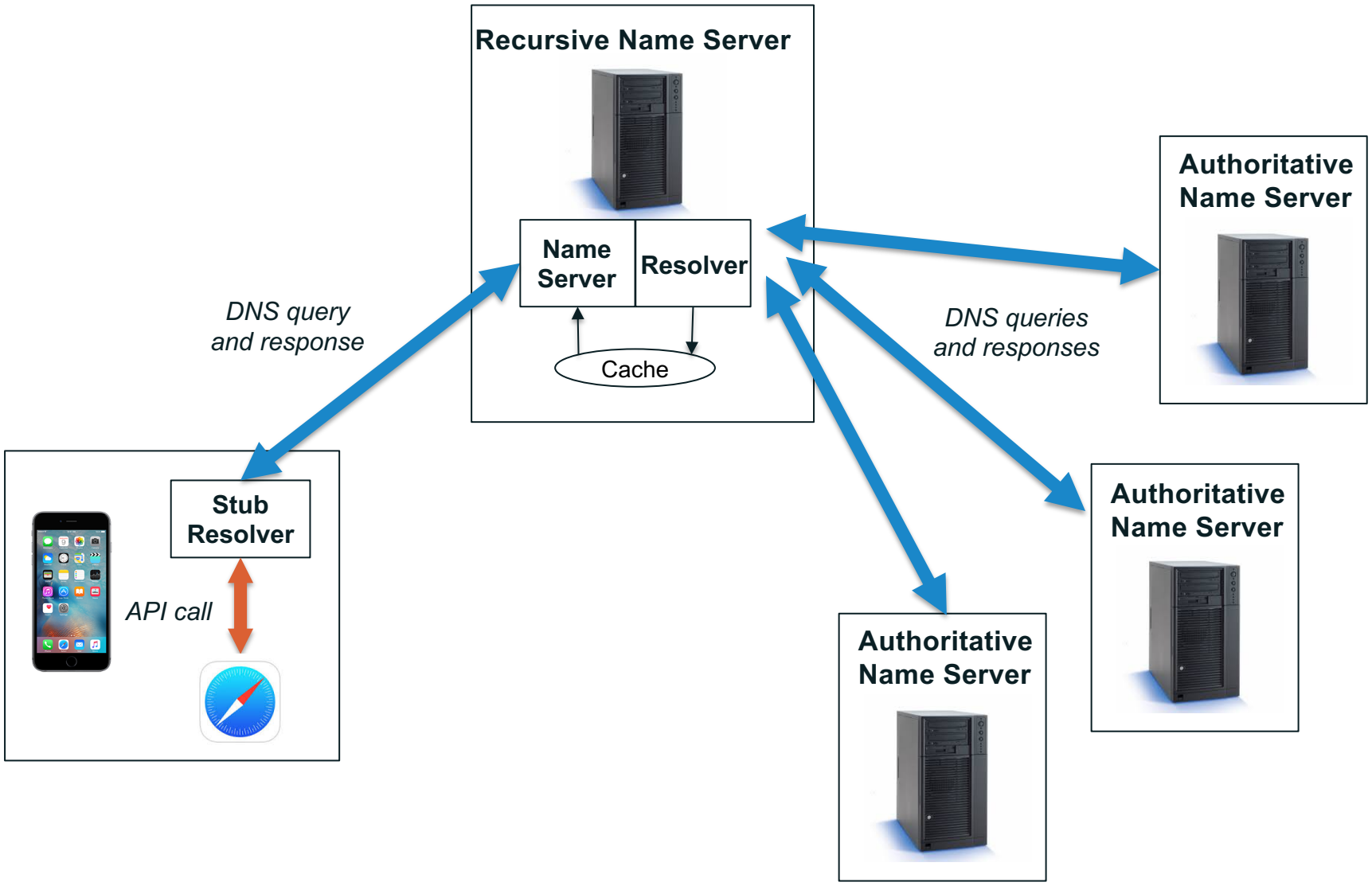
P: ¿Cuántos servidores DNS existen?
R: ¿Muchos miles…?

P: Y, por ejemplo, ¿cuántos servidores raíz DNS existen?
R: Según https://root-servers.org/ hay 1326 copias de la zona raíz para 2020-09-20.



As of 2020-09-20, the root server system consists of 1326 instances operated by the 12 independent root server operators.

Componentes del DNS



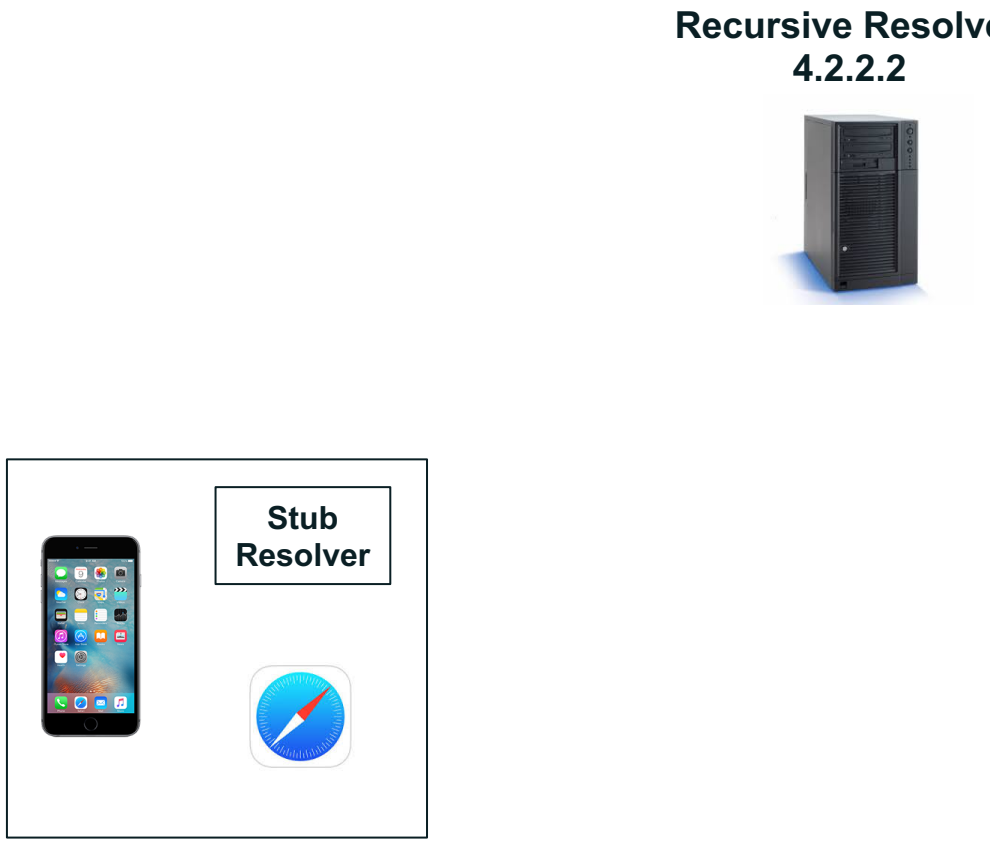
Antes de ver el proceso de resolución

Pero primero…

- ¿Cómo se inicia el proceso de resolución si no hay datos locales en el *recursivo*? (usted es el proveedor de servicios de resolución, por lo que necesita saber por dónde empezar a buscar en el almacén)
- Suponga que el caché de resolución se encuentra vacío (por lo que no tiene ninguna información de búsqueda anterior).
- No hay más remedio que comenzar en la zona raíz (el estante que contiene los datos de los dominios de nivel superior).
- Los servidores de nombres raíz son los servidores *autoritativos* para la zona raíz.
- Pero, ¿cómo encuentra un *recursivo* las direcciones IP de los servidores de nombres raíz?
- Deben estar pre-configuradas (de hecho, la mayoría del software DNS viene precargado con una versión actualizada del archivo llamado archivo contiendo esa información).
- No hay forma de descubrirlos (¿problema de huevo-gallina?).
- Un archivo dentro del servidor recursivo (resolver) llamado ”root hints file" contiene los nombres y direcciones IP de los servidores de nombres raíz.
- https://www.iana.org/domains/root/files

Proceso de Resolución

El *stub resolver* del teléfono está configurado para enviar consultas al servidor recursivo con la dirección IP 4.2.2.2

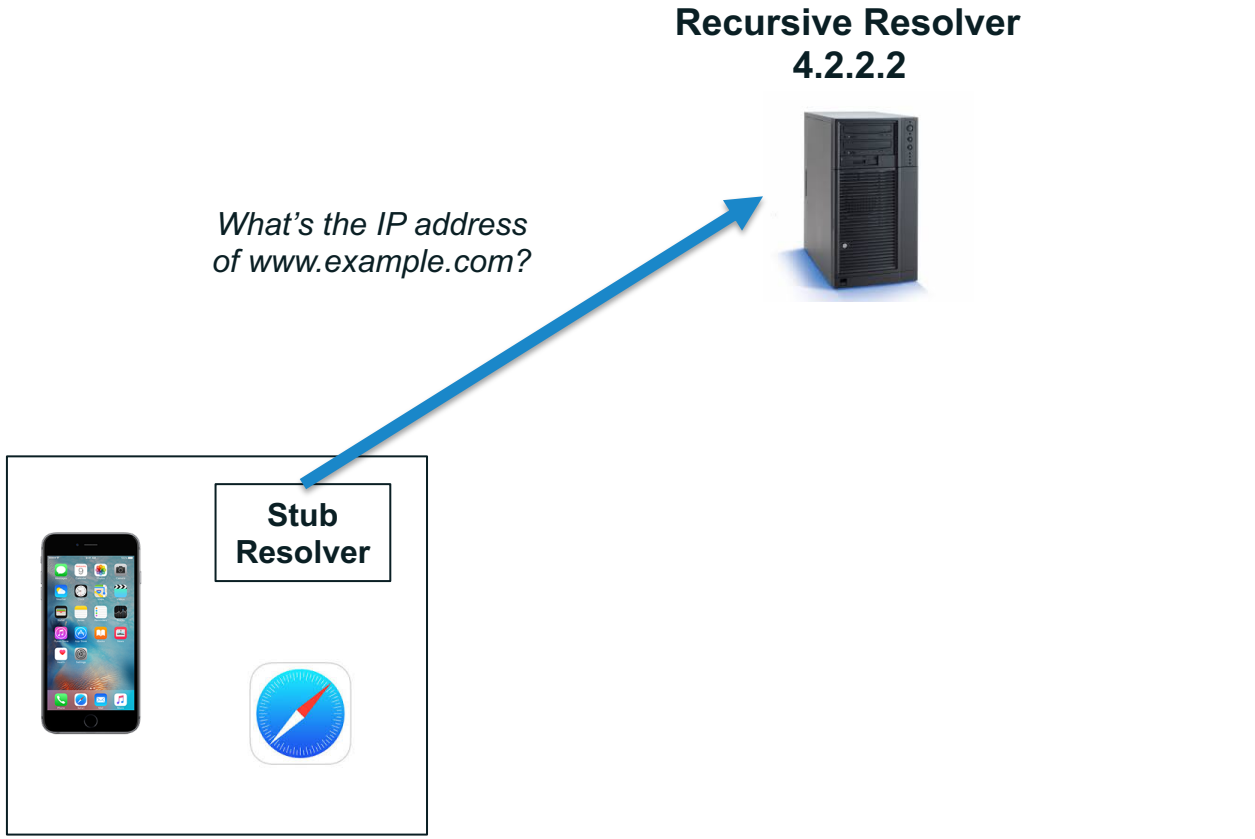


Proceso de Resolución

Un usuario escribe www.example.com en Safari, que luego llama a la función del *stub resolver* para resolver el nombre

Proceso de Resolución

El *stub resolver* del teléfono envía una consulta para www.example.com, IN, A a 4.2.2.2



Proceso de Resolución

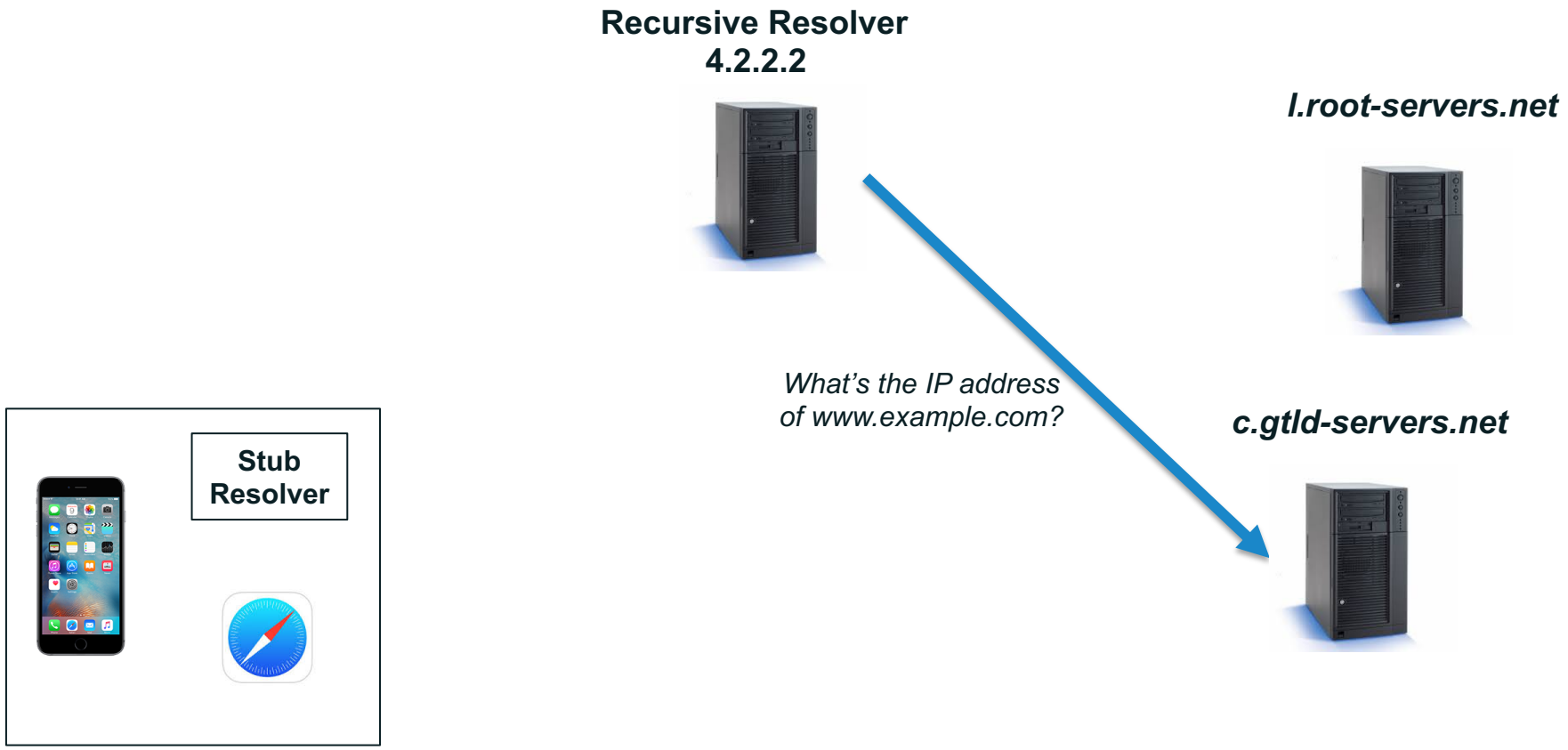
El servidor recursivo 4.2.2.2 no tiene datos almacenados en caché para www.example.com, por lo que consulta un servidor raíz

Proceso de Resolución

El servidor raíz devuelve una referencia a .com

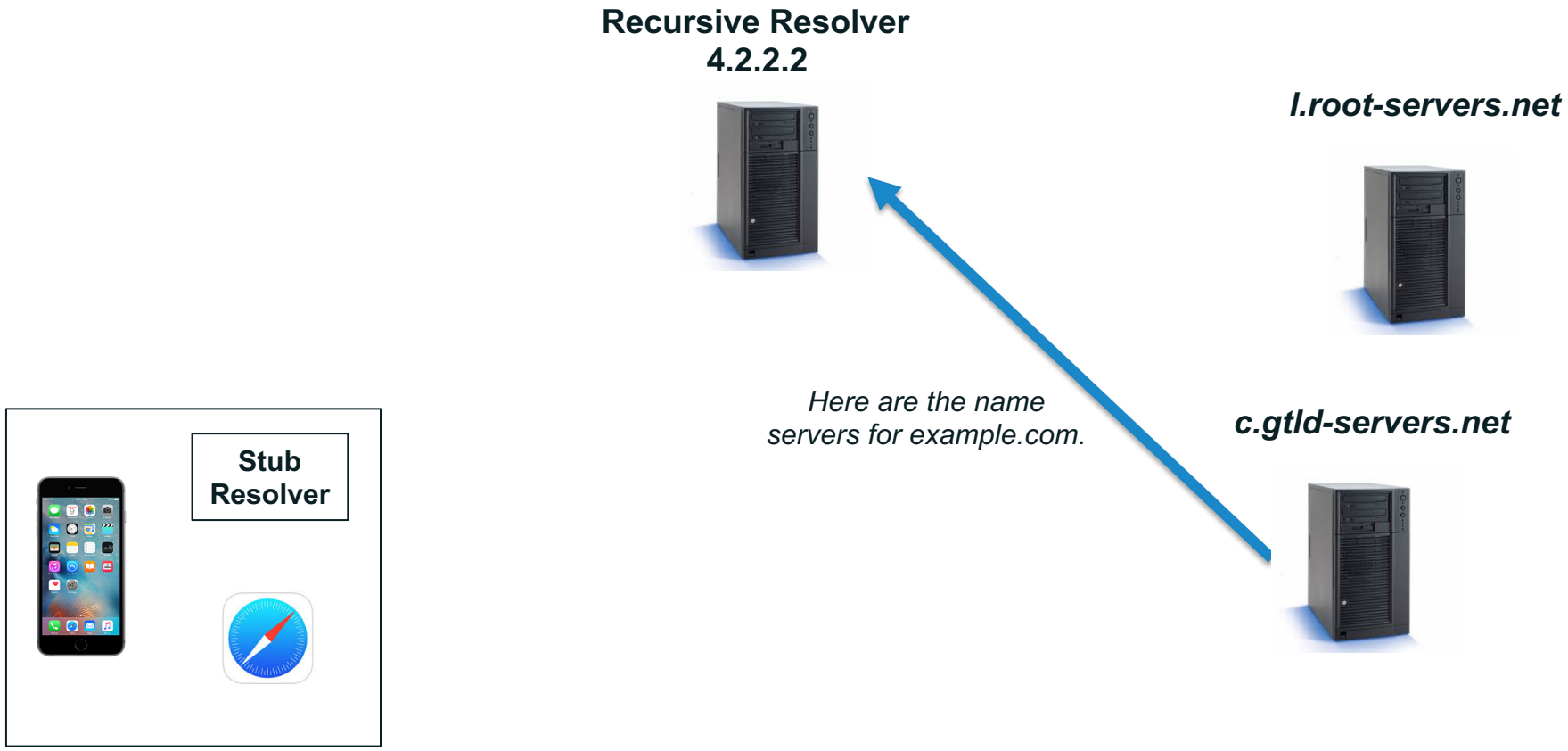
Proceso de Resolución

El servidor recursivo consulta al servidor .com



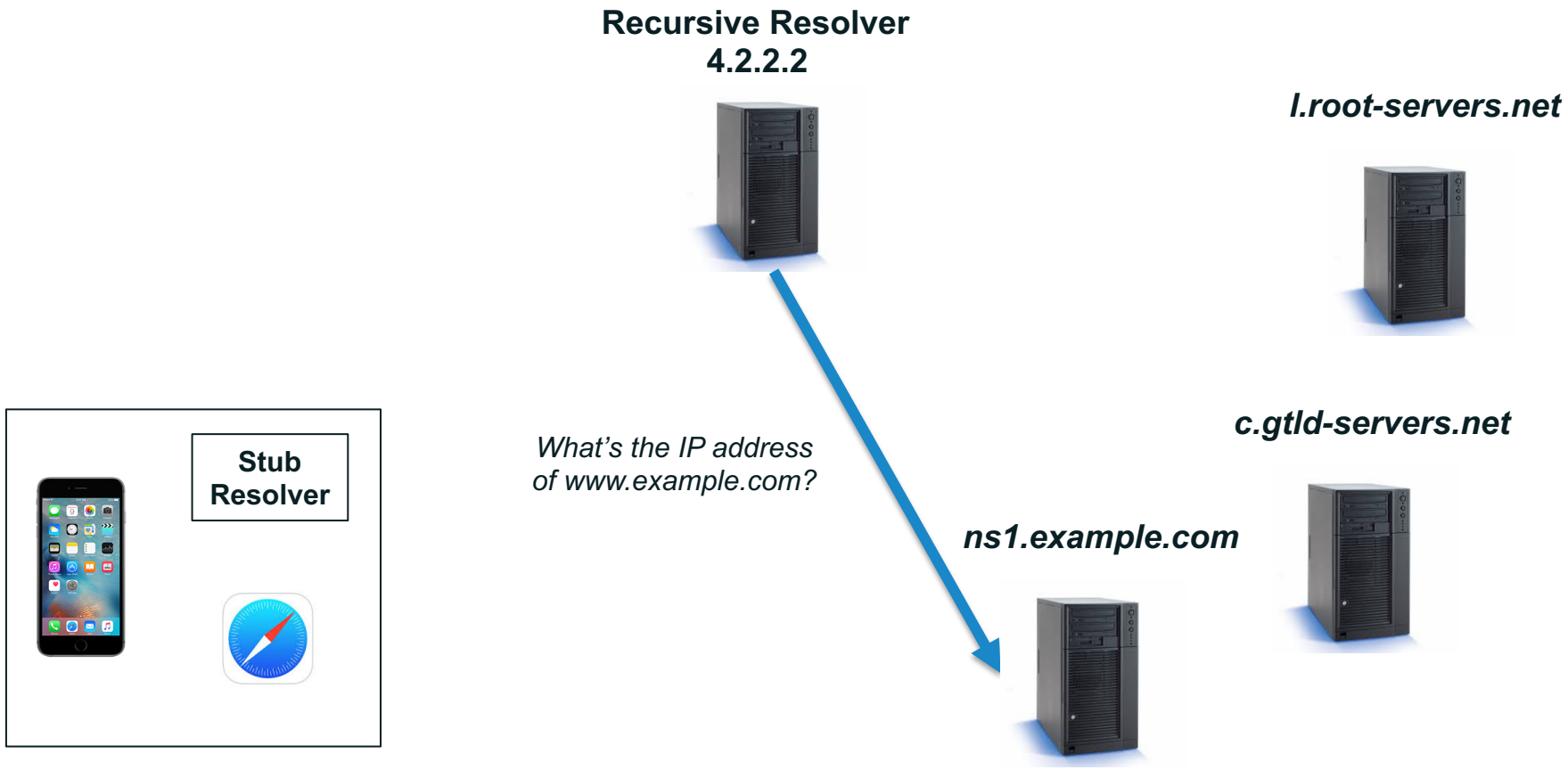
Proceso de Resolución

El servidor .com devuelve una referencia a example.com



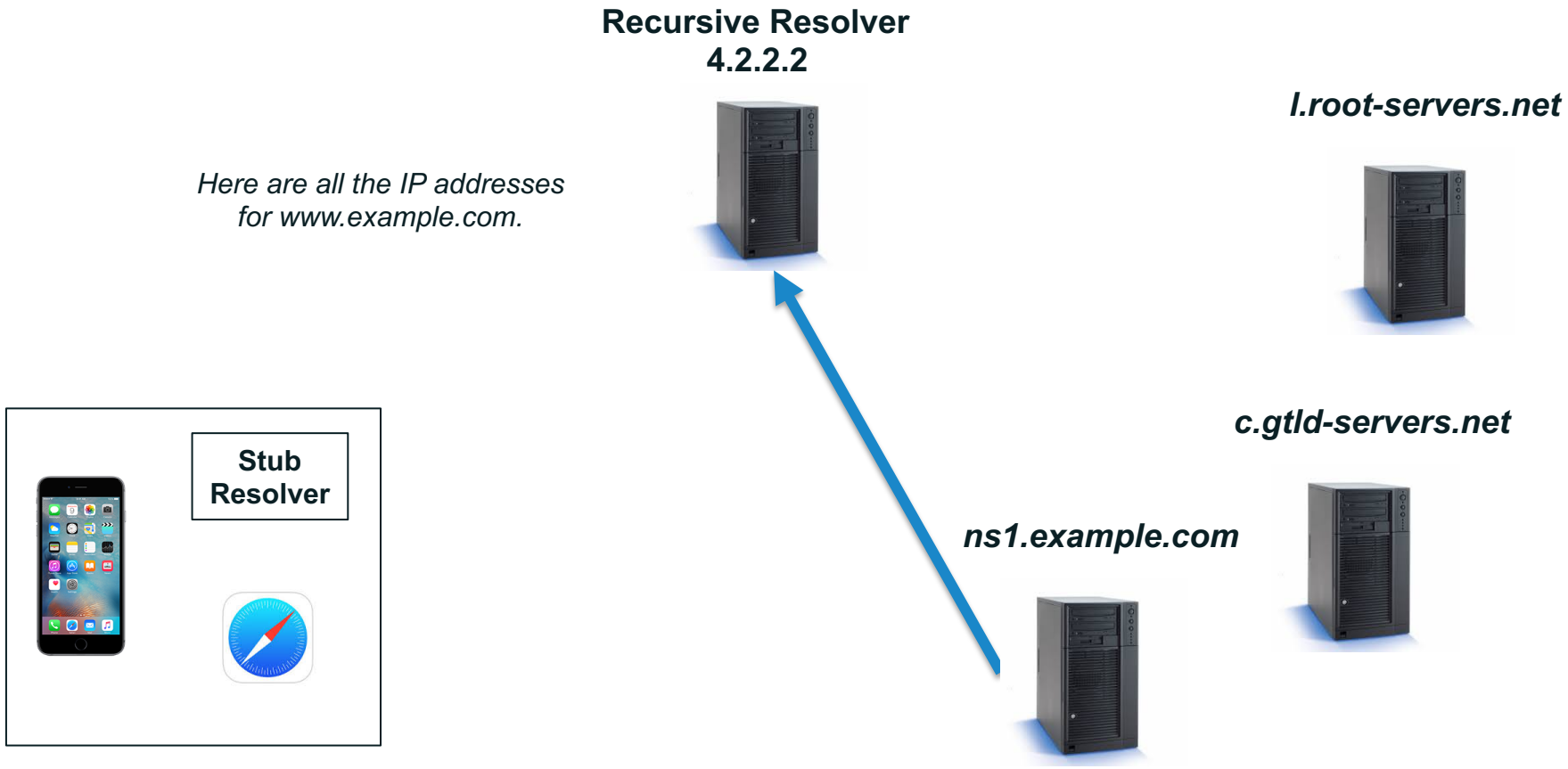
Proceso de Resolución

El servidor recursivo consulta al servidor de example.com



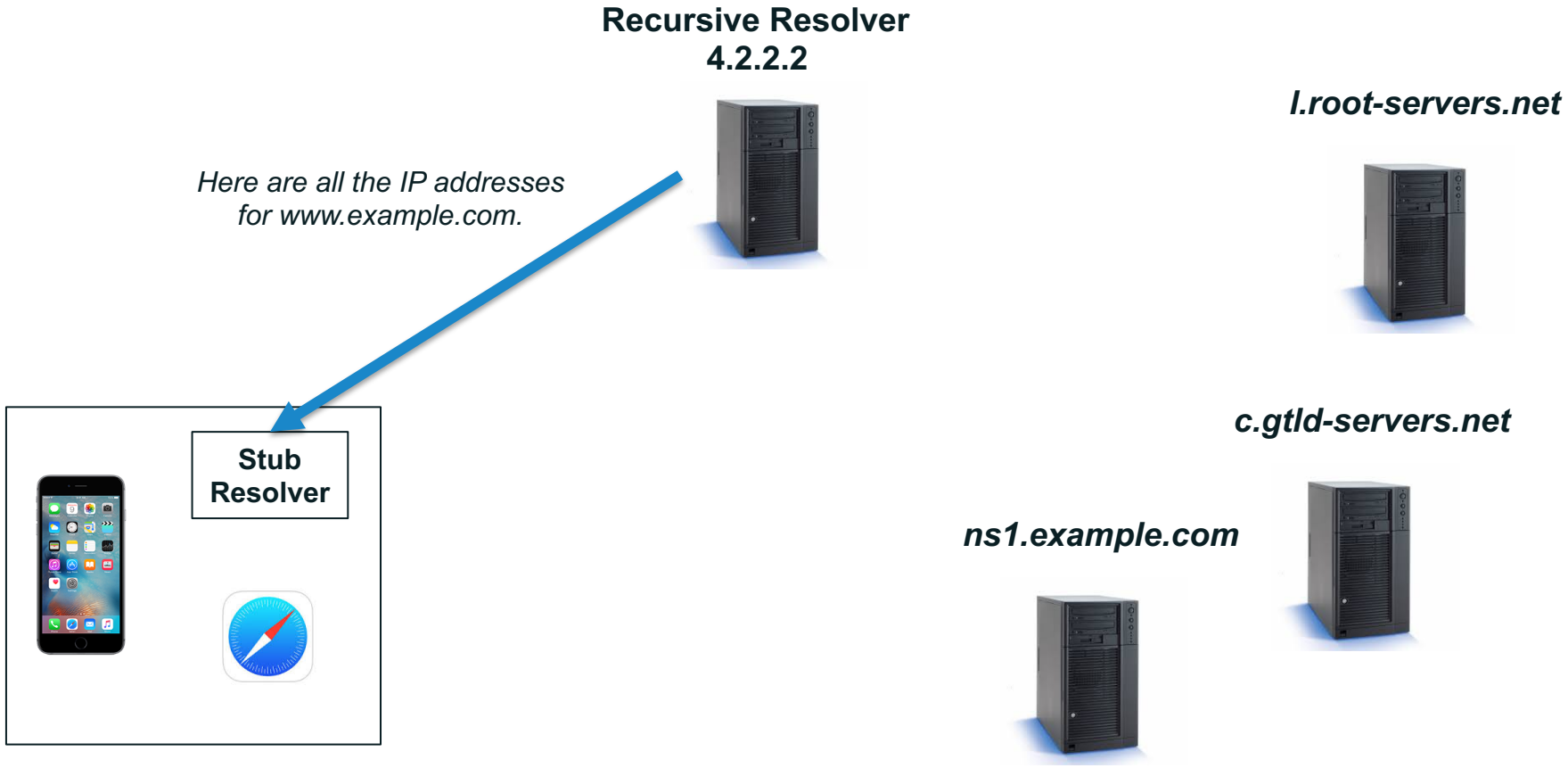
Proceso de Resolución

El servidor example.com devuelve la respuesta a la consulta porque él es el *autoritativo* para example.com



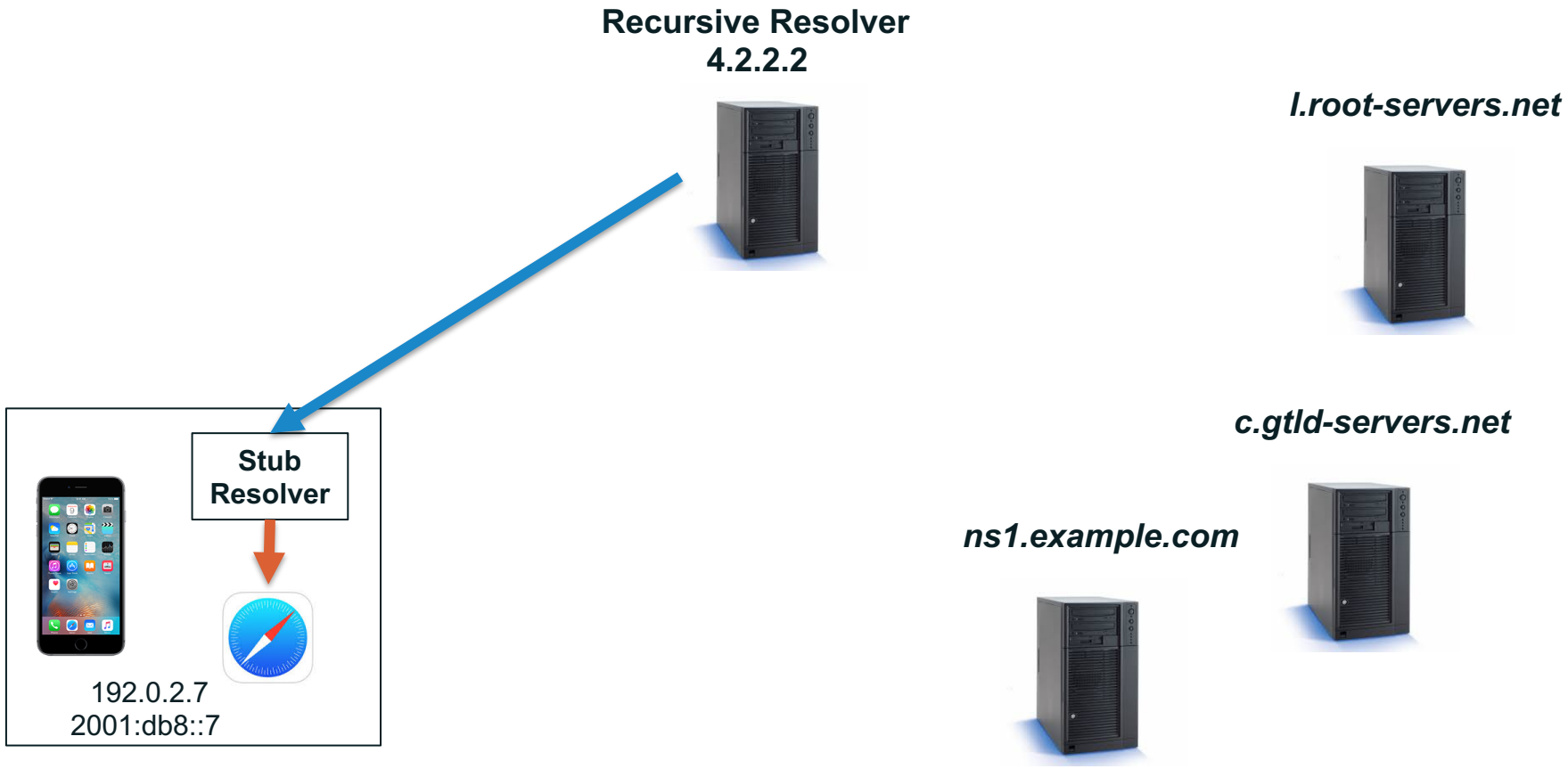
Proceso de Resolución

El servidor recursivo devuelve la respuesta a la consulta al *stub resolver*



Proceso de Resolución

El *stub resolver* devuelve las direcciones IP a Safari



Proceso de Resolución

- Después de la consulta anterior, el servidor recursivo en 4.2.2.2 ahora sabe:
  - Nombres y direcciones IP de los servidores .com
  - Nombres y direcciones IP de los servidores de example.com
  - Direcciones IP para www.example.com
- Almacena en caché todos esos datos para que pueda responder consultas futuras rápidamente, sin repetir todo el proceso de resolución.

DNSSEC

Vulnerabilidades de DNS

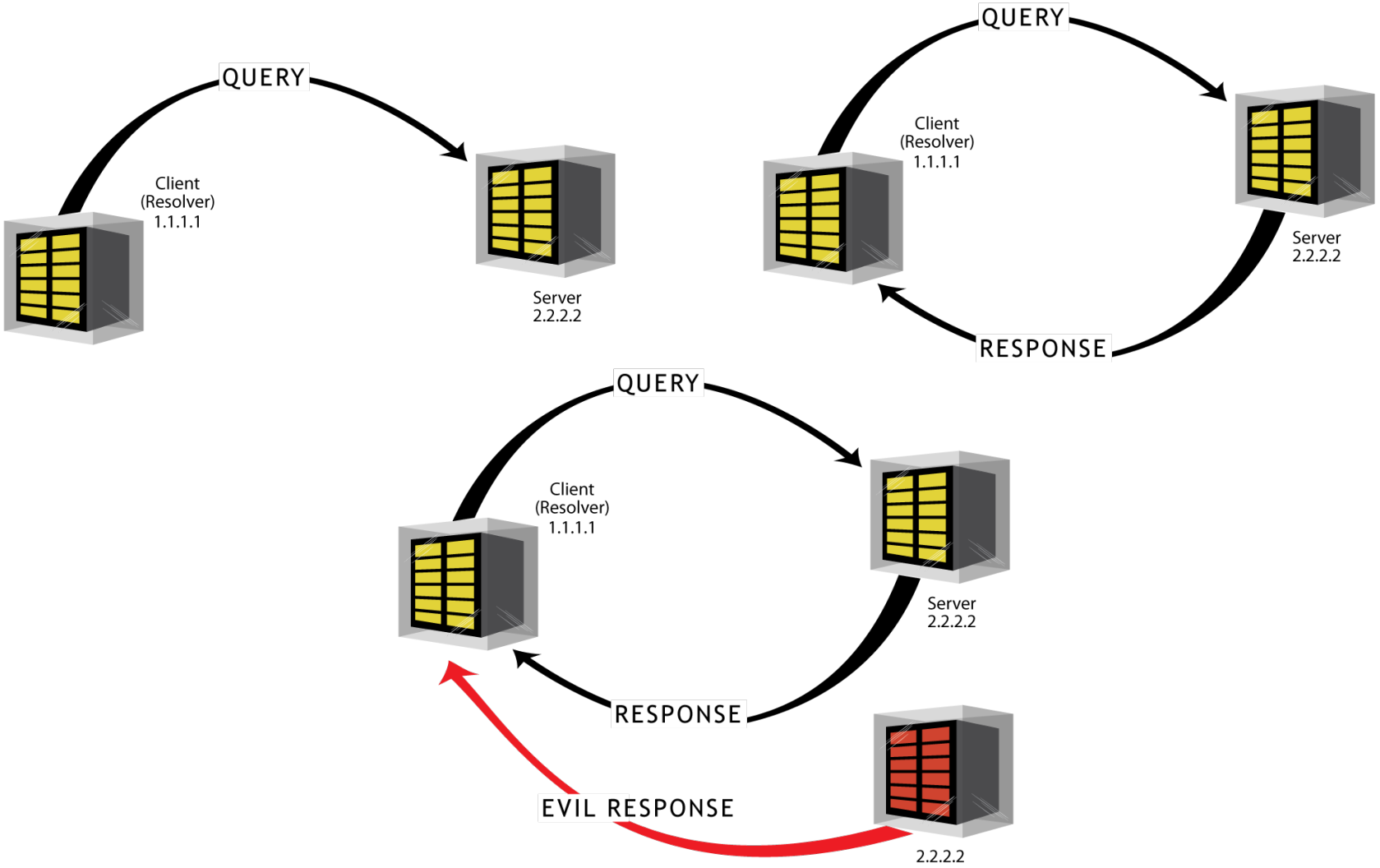
- ***La estructura básica del DNS (década de 1970) no tenía en cuenta los problemas de seguridad.***
  - ***Enfoque: rendimiento.***
  - ***Principio: confianza.***

3 areas de vulnerabilidades

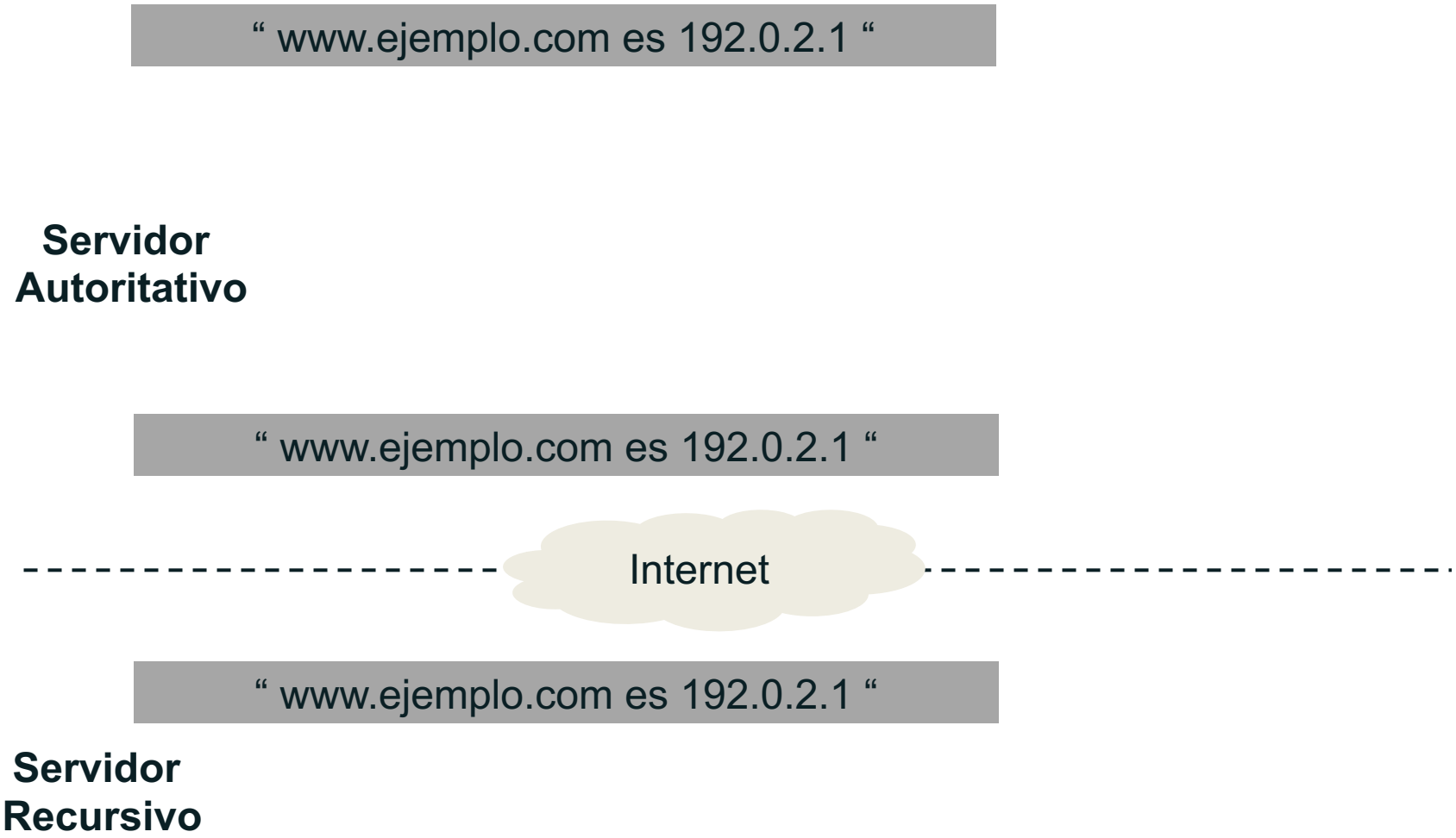
- ***Confidencialidad***
  - ***Acceso no deseado de información a terceros***
- ***Disponibilidad***
  - ***Pérdida de capacidad de acceso***
- ***Integridad***
  - ***Modificación o destrucción no deseada***

← DNSSEC actúa aquí

Vulnerabilidades de DNS



Visión General (sin DNSSEC)



Qué es DNSSEC? …

… lo que hace

- DNSSEC utiliza criptografía de clave pública y firmas digitales para proporcionar:
  - Autenticación de origen de los datos
  - Integridad de los datos
- DNSSEC ofrece protección contra la falsificación de datos de DNS

… lo que NO hace

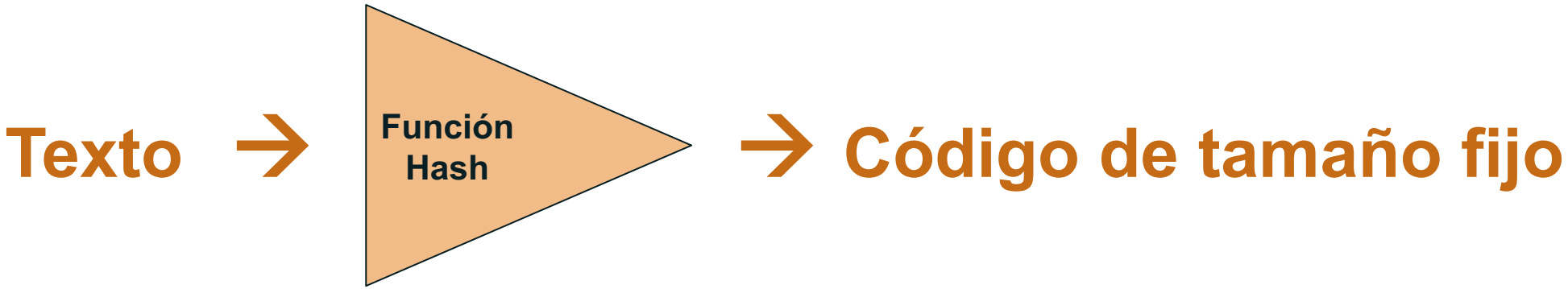
- Proveer confidencialidad en el intercambio de datos de DNS
- Evitar algunos ataques dirigidos al software de DNS o los sistemas
  - DDoS

Como funciona?

- Función “Hash”
- Par de Calves (o llaves) (Pública e Privada)
- Firma Digital

Función “Hash”

- Convierte información en una serie de caracteres de longitud fija.




```
Este equipo no tiene copa del mundo  →  5d242b5294d72df332ca2c492d2c0b9b

Este equipo tiene copa del mundo  →  e3d688adde84cf3e3fa493466dadba89
```

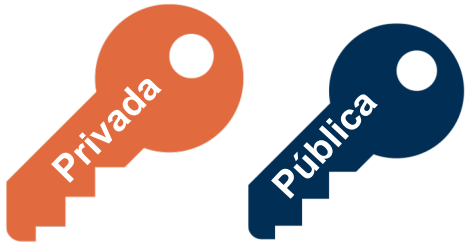
Criptografía de llaves Públicas

- Encriptación simétrica
  - 1 llave para encriptar y desencriptar

- Encriptación asimétrica **(DNSSEC utiliza esta)**
  - 1 llave para encriptar + 1 llave para desencriptar
    - 1 llave privada
    - 1 llave pública

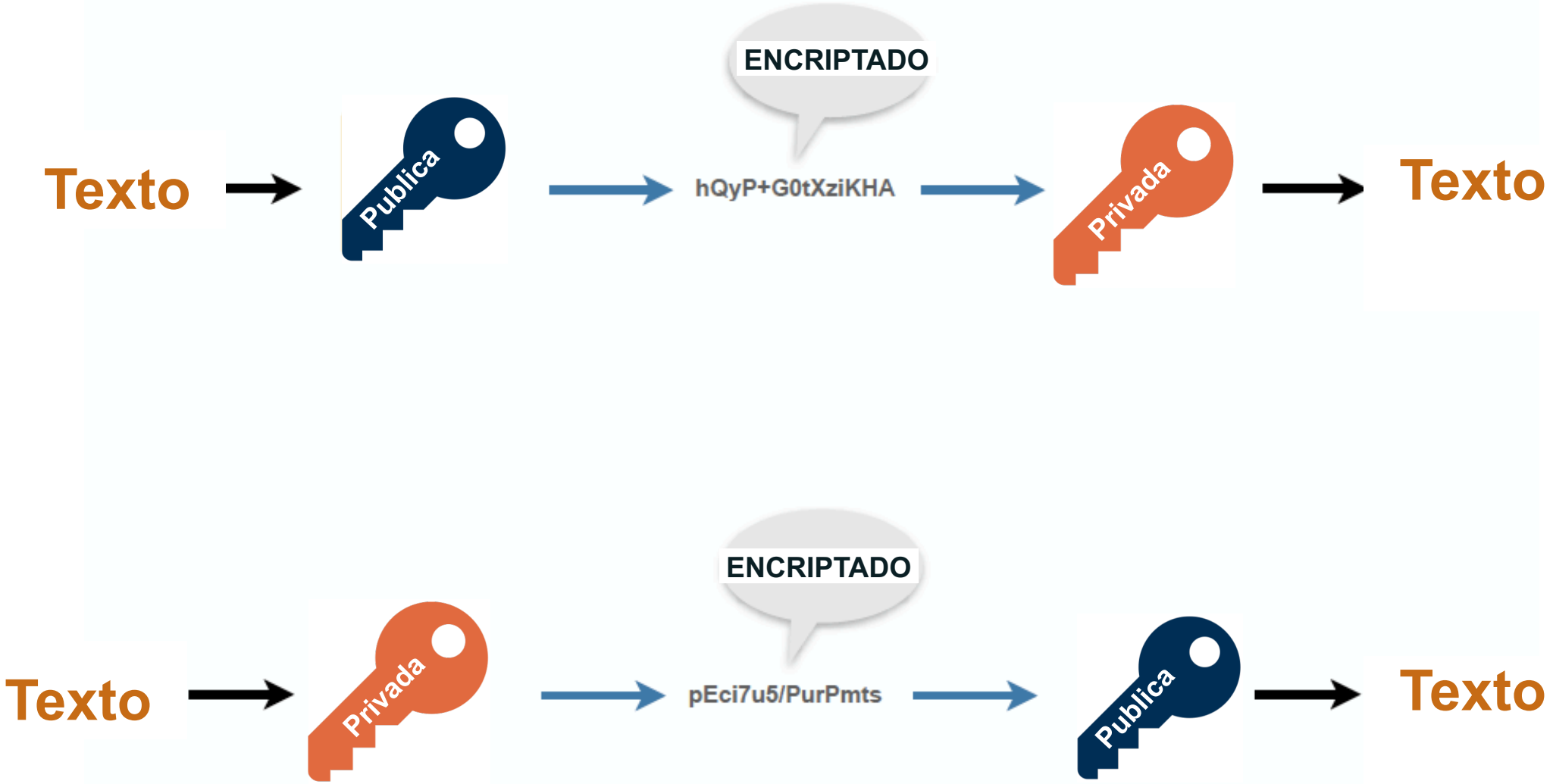
Llaves de encriptación

- **Par de llaves**
  - **Llave privada**
  - **Llave pública**



- **El contenido cifrado con una clave solo se puede descifrar con la otra.**
  - La clave pública puede "abrir" el contenido cifrado con la clave privada y viceversa.

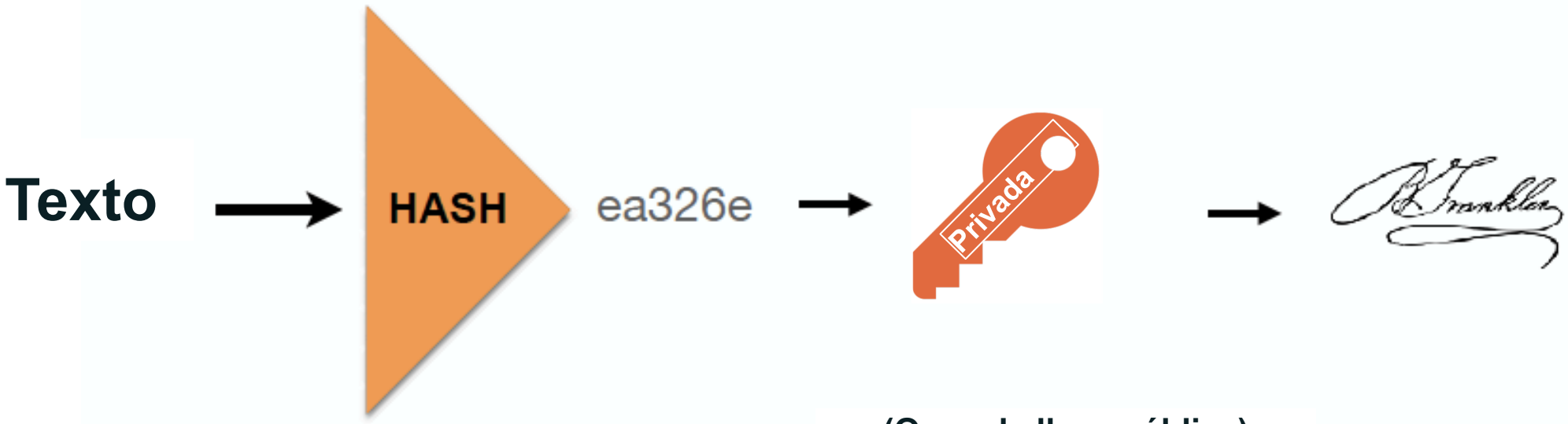
Llaves de encriptación



Firmas digitales

- Si combinamos hashes con cifrado de clave pública, tenemos una firma digital
- Generamos un hash y luego lo encriptamos con una clave

Hashing + Encriptación = Firma Digital

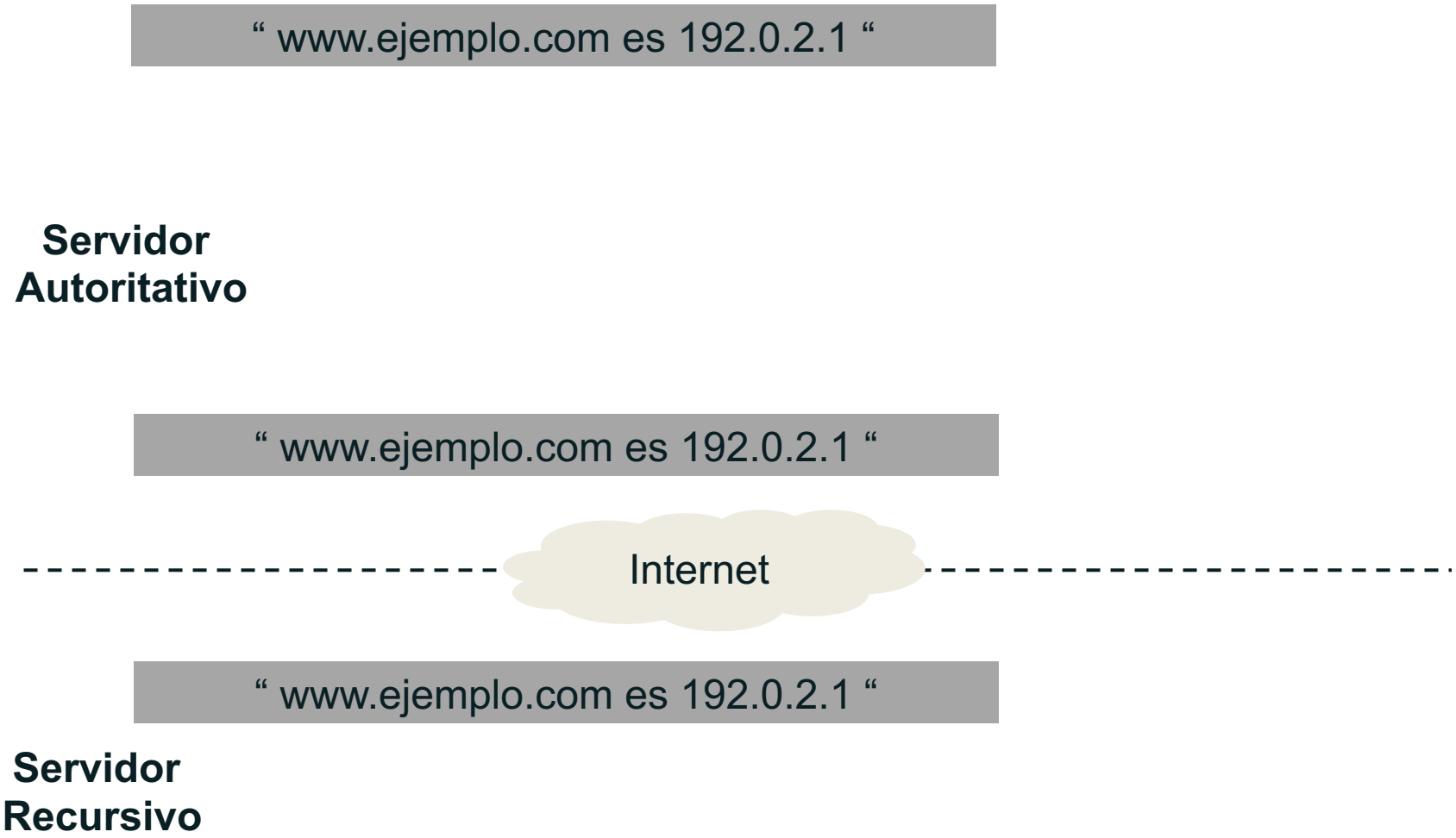


(O con la llave pública)

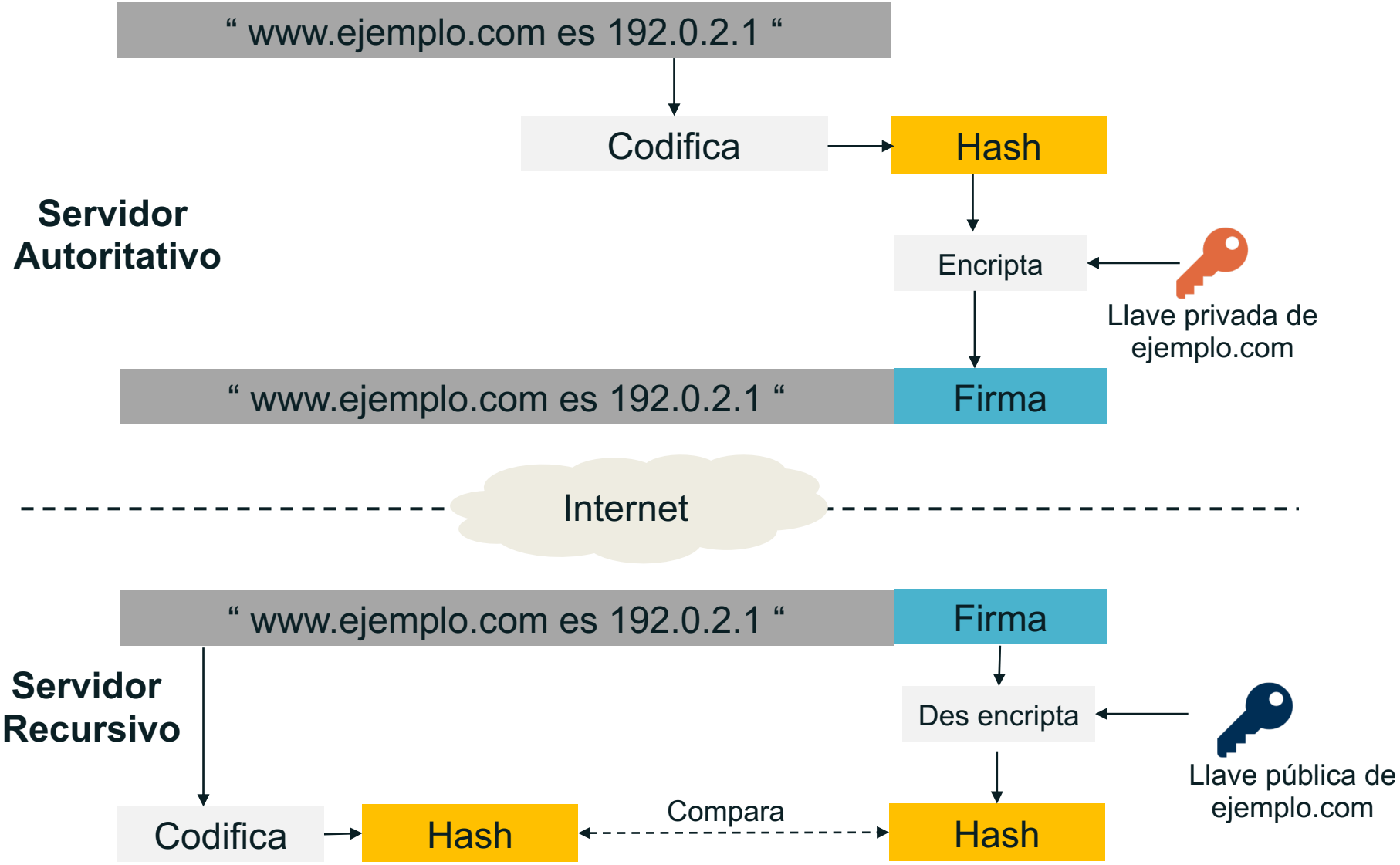
Verificando la autenticidad de las firmas

- Des encriptamos el mensaje
  - Obtenemos el hash.
- Convertir el mensaje original en un hash
- Comparar con el hash recibido
- Si los 2 hashes coinciden, el mensaje no se ha modificado.

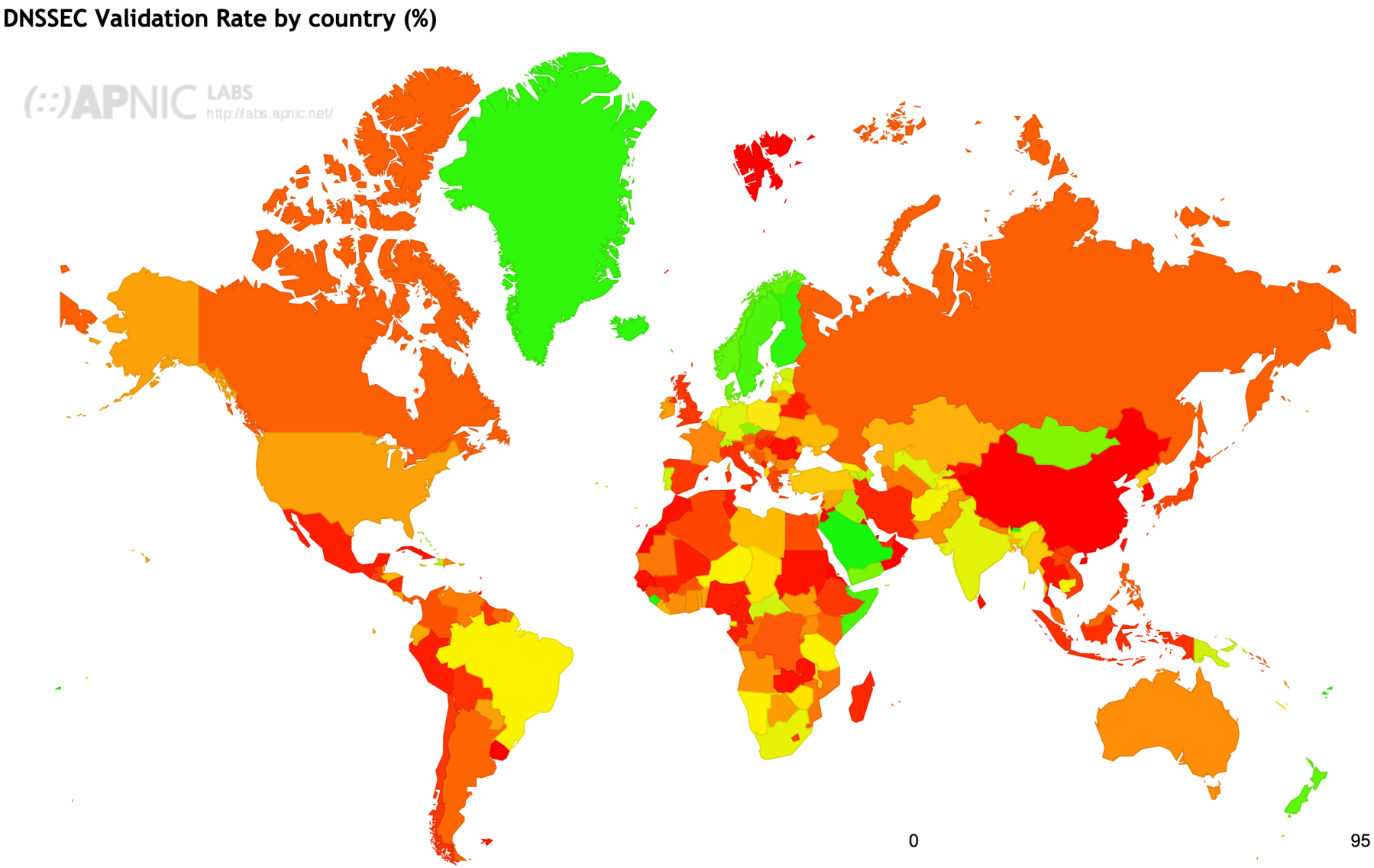
Visión General (sin DNSSEC) - recordando -



Visión General (con DNSSEC)



Validación DNSSEC en servidores recursivos, por país



https://stats.labs.apnic.net/dnssec

Gracias … preguntas?