Private DoH

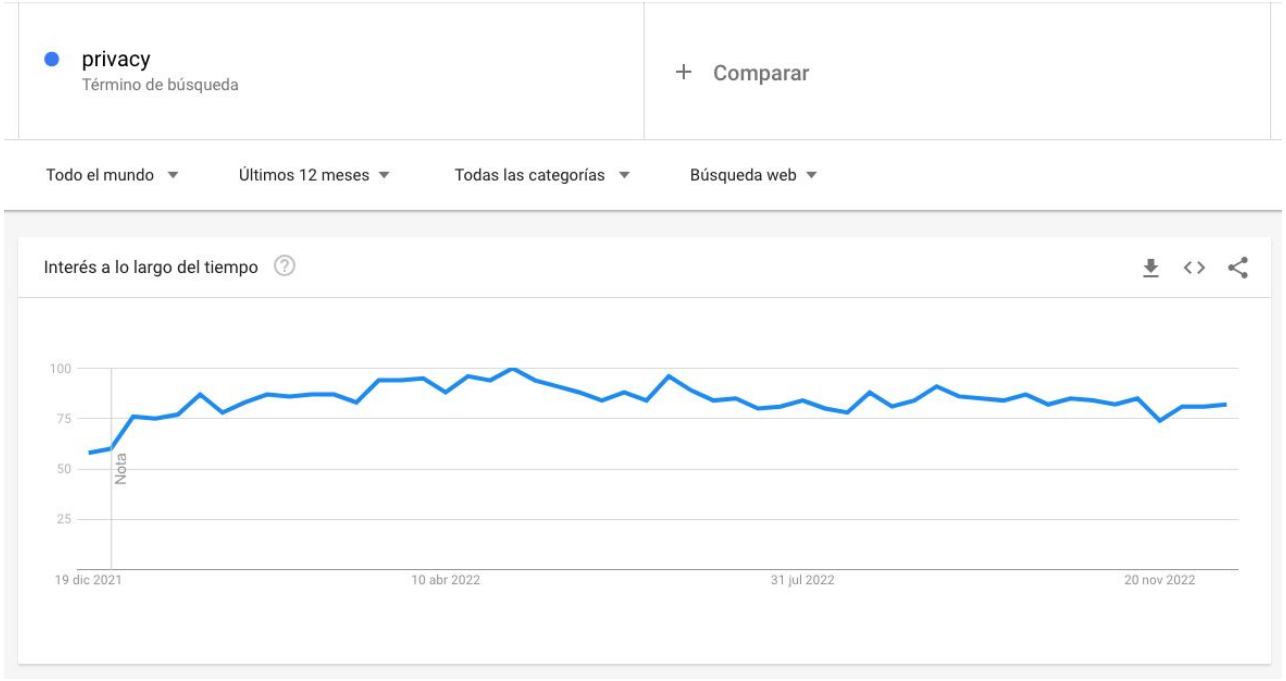
Nos presentamos

Cecilia Hortas

Camila Bojman

1 Motivación

¿Es importante la privacidad?



Interés a lo largo del tiempo

Los números reflejan el interés de búsqueda en relación con el valor máximo de un gráfico en una región y un periodo determinados. Un valor de 100 indica la popularidad máxima de un término, mientras que 50 y 0 indican que un término es la mitad de popular en relación con el valor máximo o que no había suficientes datos del término, respectivamente.

Primeras ideas

Nuestra aplicación va a trabajar con la **privacidad** de las consultas que se hacen para acceder a internet.

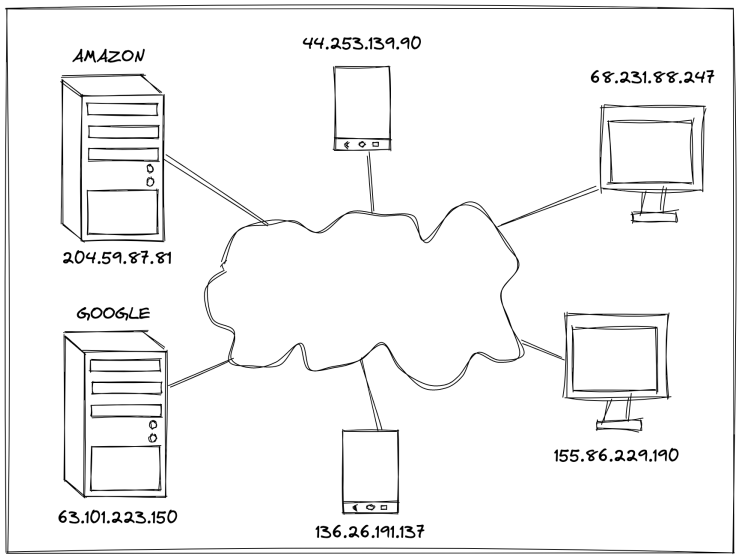
DNS

2

¿Qué es DNS?

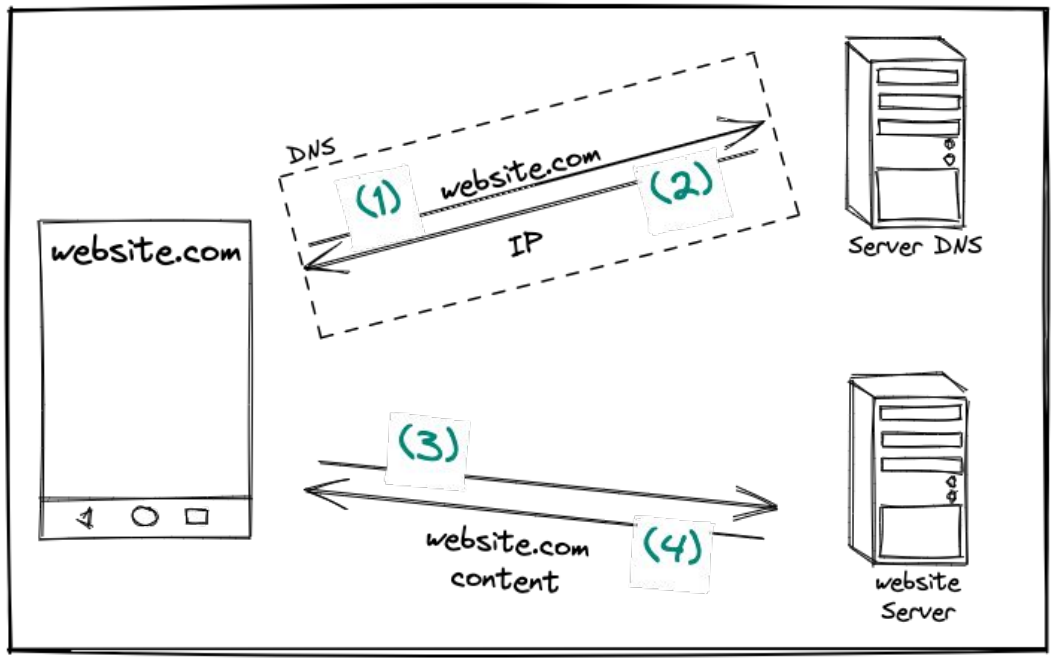
Domain Name System

Concepto básico de DNS



- Ser humano:
  - google.com
- Equipos con Internet:
  - Direcciones IP
- ¿Y cómo se consigue la IP correcta?
  - **DNS**

DNS es la agenda telefónica de Internet



Nombres de dominio

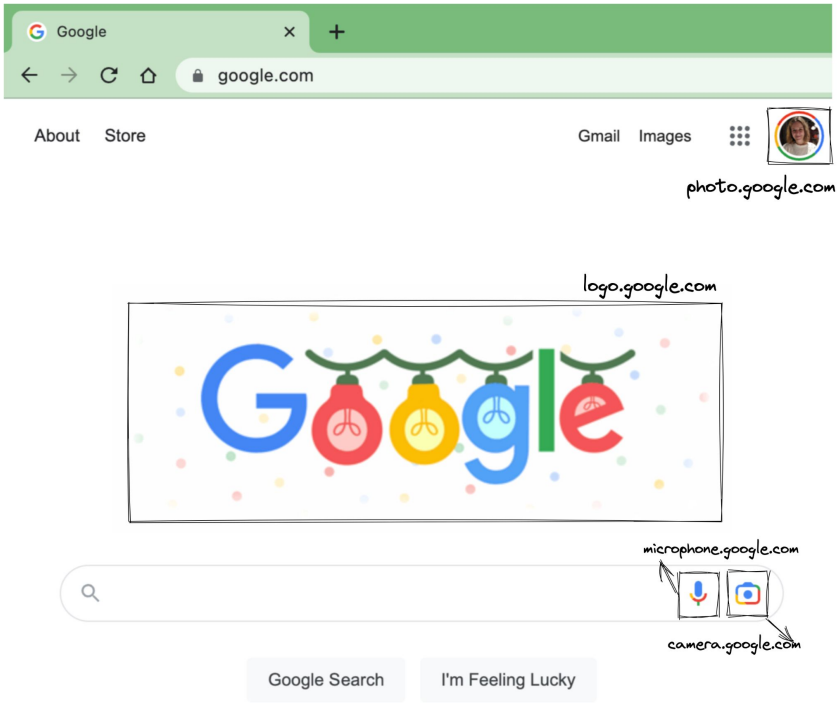
website.com

Direcciones IP

102.107.9.77

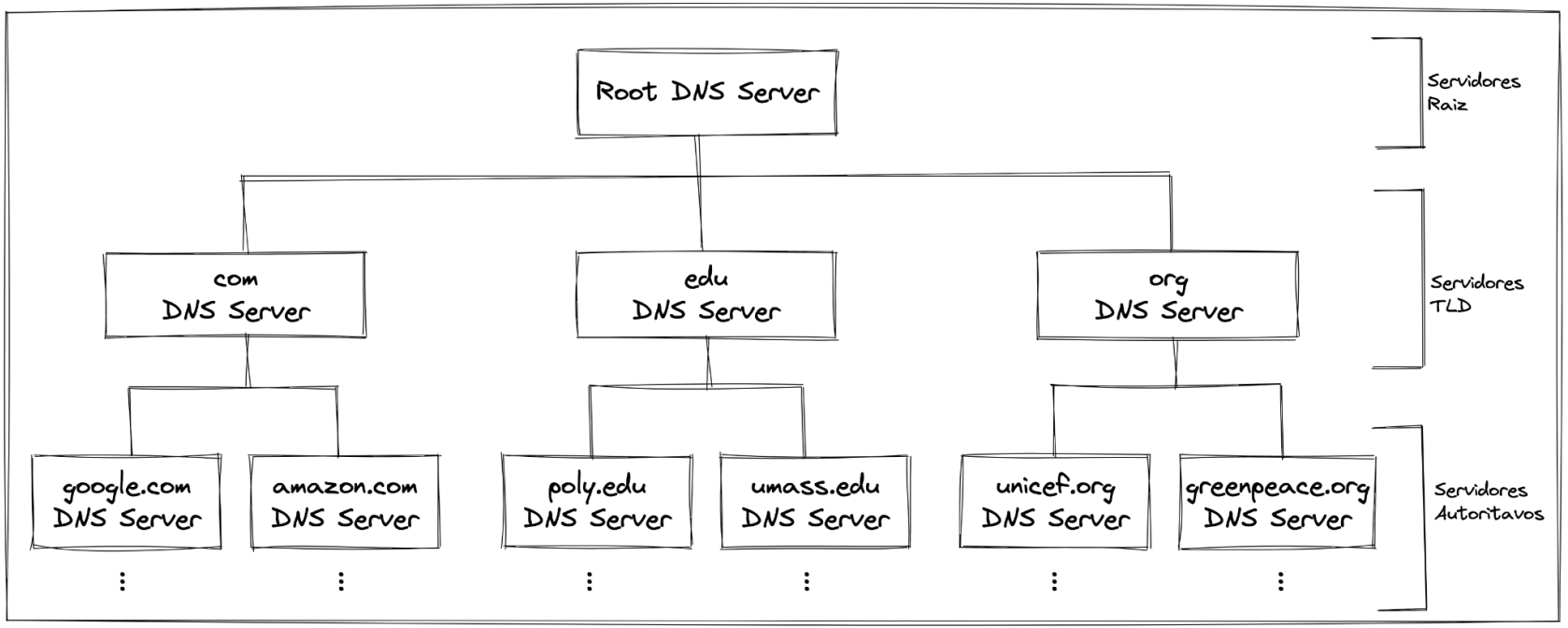
3 ¿Y cómo funciona?

Funcionamiento de DNS

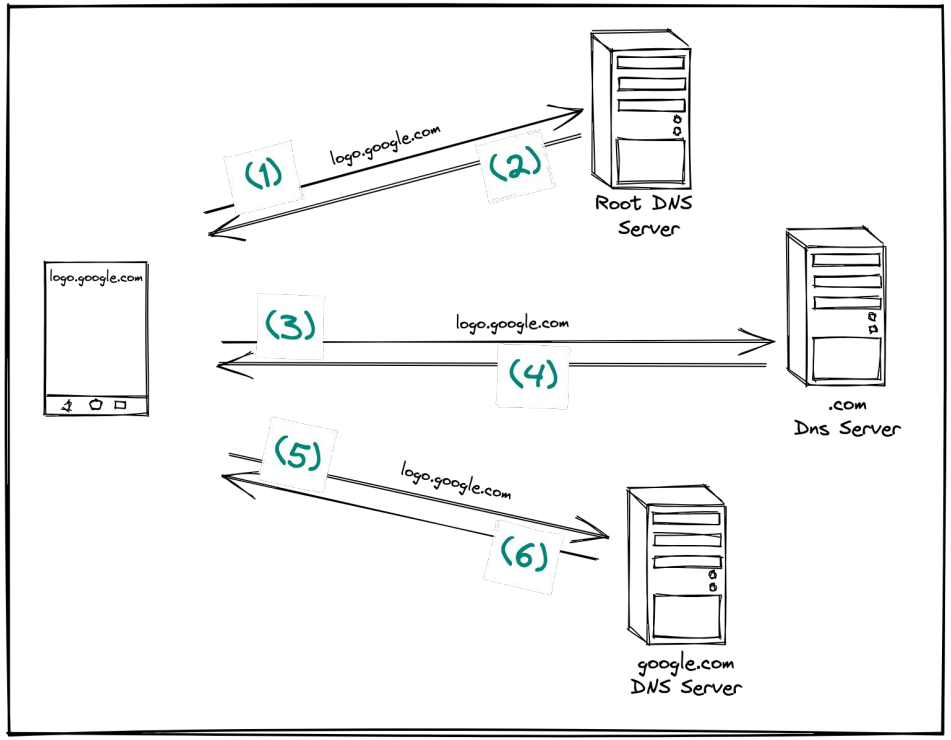


- Todo depende de DNS
- Segundo plano
- **¿Cómo escala?**
  - **Gran cantidad** de servidores
  - Organizados de forma **jerárquica**
  - **Distribuidos por el mundo**

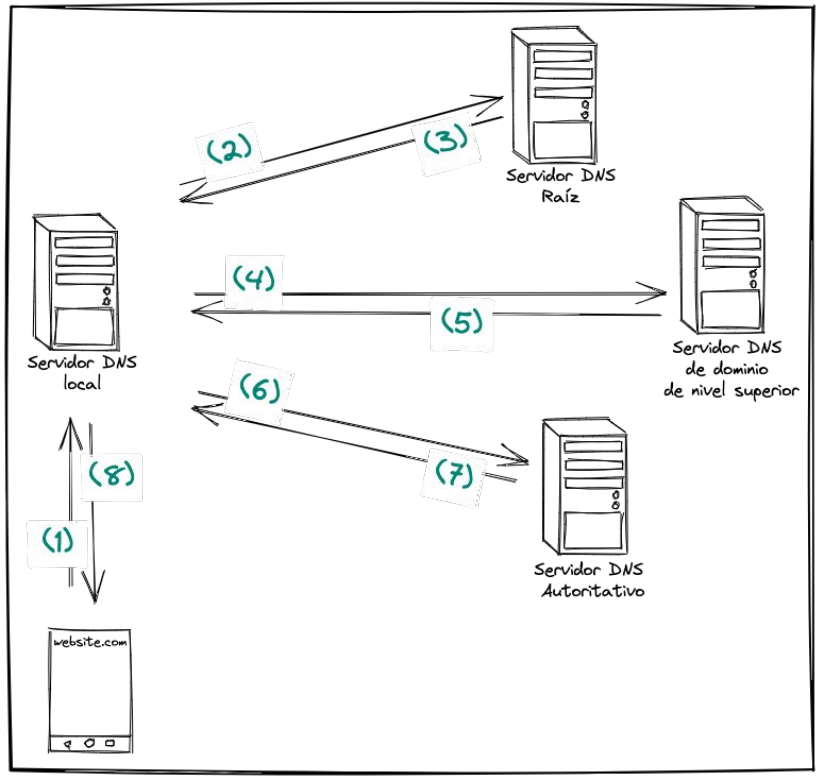
Jerarquía DNS



Jerarquía DNS



ISP (Internet Service Provider)



- Acceso a internet

  Ejemplos ISP: Fibertel, Telecentro, IPlan.

- Servidores DNS locales. Brindan:
  - Servicios de **resolución DNS**.
  - Cache DNS.

4 Public DNS

Irrupción de Public DNS

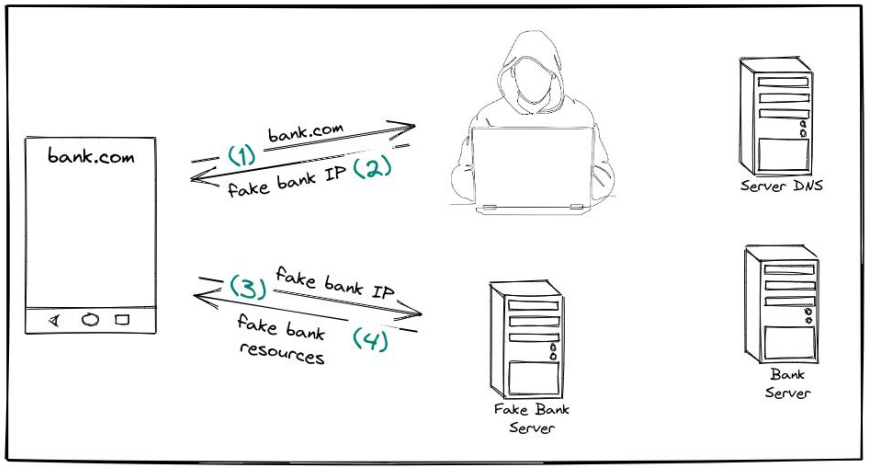
- Servicio de DNS **gratuito** ofrecido por algunas empresas.
- Son ampliamente utilizados por su:
  - Performance
  - Redundancia
- ¿Pero qué obtienen a cambio las empresas? Los **patrones de conducta de internet** de cada uno de los usuarios.

5

Alternativa a DNS

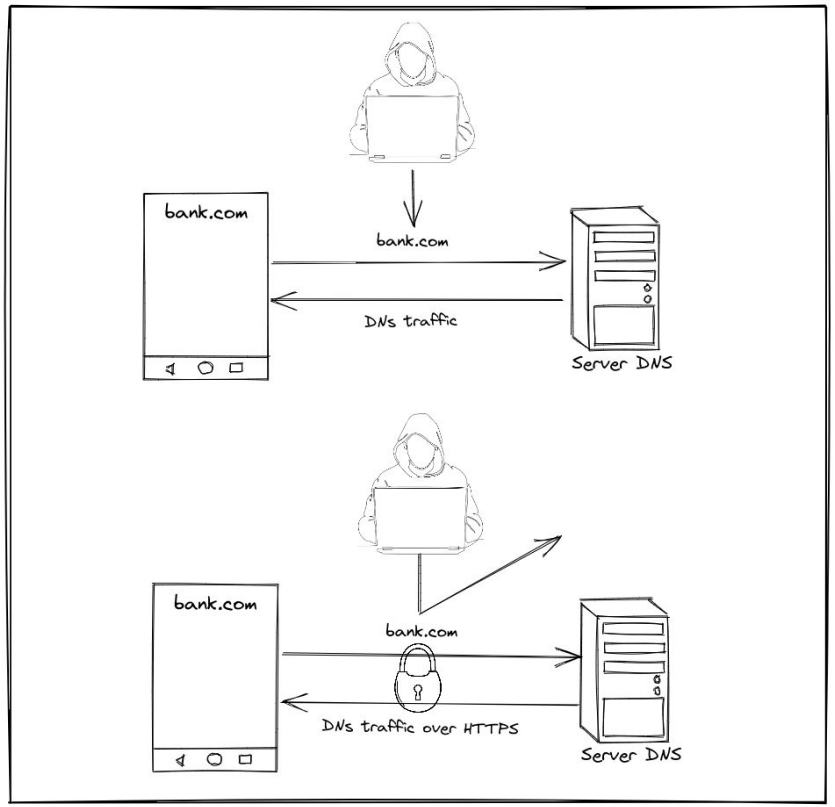
DoH

Seguridad en DNS



- DNS no garantiza **autenticación**, **confidencialidad e integridad**.
- Expone a los usuarios a diversas amenazas como ataques man-in-the-middle.

DoH (DNS over HTTPS)



- Las consultas y respuestas de DNS se **cifran** y se envían a través del protocolo HTTPS (TCP) en lugar de UDP.
- DoH garantiza que los atacantes **no puedan alterar** el contenido de las consultas DNS.

Ventajas y desventajas

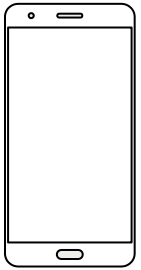
Ventajas

- Previene ataques *man-in-the-middle*.
- Las empresas que proveen DoH suelen tener gran capacidad de procesamiento.

Desventajas

- DoH concentra la mayoría de los datos de DNS con las grandes empresas.

6 Nuestra aplicación



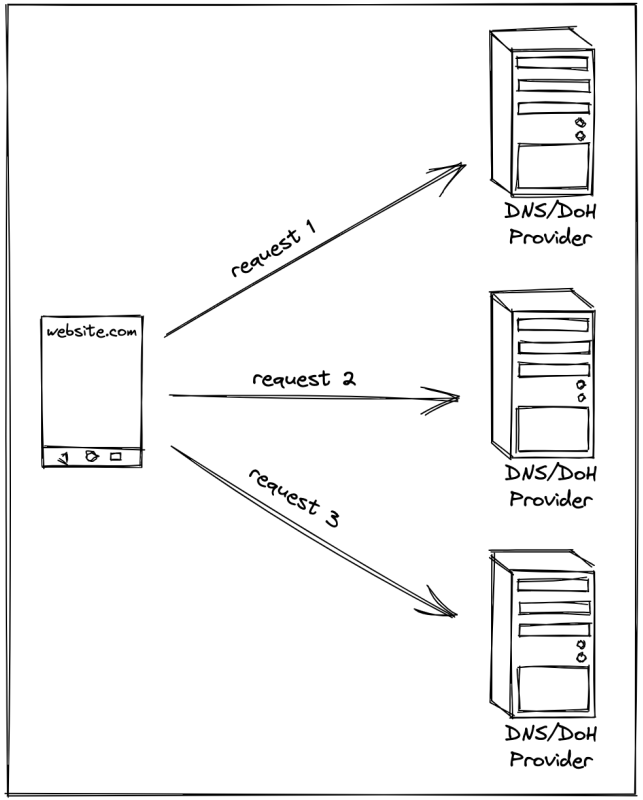
PDoH

Propósito de la aplicación

Buscamos mejorar el rendimiento de la resolución de DNS procurando atributos de calidad:

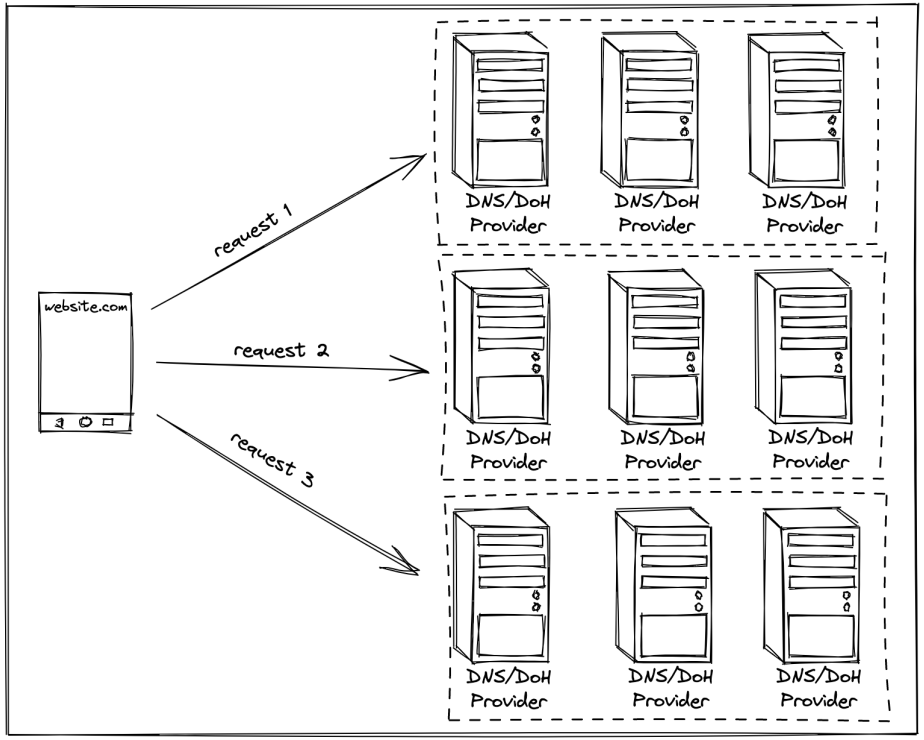
- Seguridad → DoH
- Privacidad → Sharding
- Performance → Racing

Sharding



- Cada proveedor tiene solamente un subconjunto de las consultas DNS del cliente.
- Si usamos únicamente sharding puede suceder que el proveedor DNS seleccionado sea lento para una localización en particular.

Racing



- Enfoque redundante
- Distintos servicios DNS compiten entre sí (racing).

Aplicación móvil

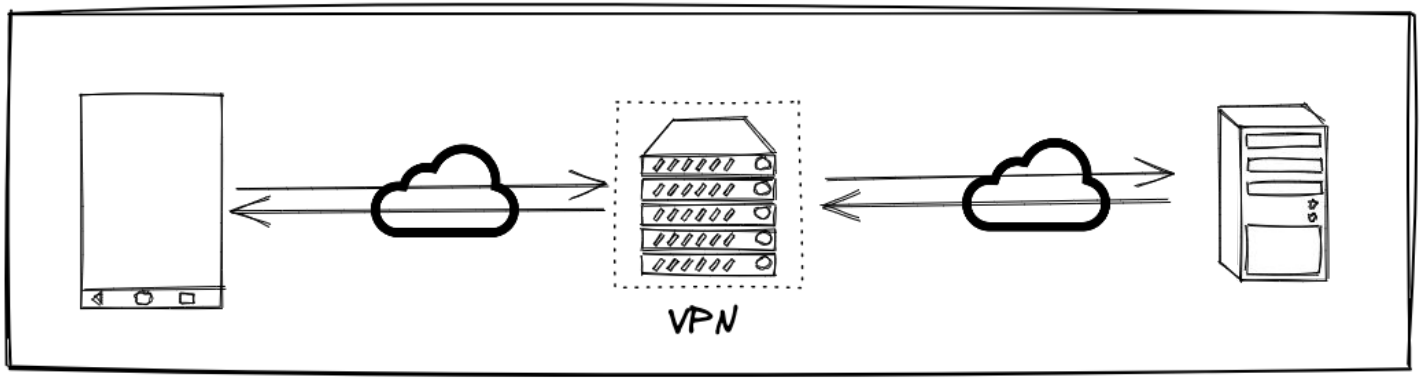
- A diferencia de los entornos desktop, los entornos móviles requieren del permiso sudo para capturar mensajes de la red.
  - Caso contrario, se debería “rootear” el celular.

- Solución: uso de la clase nativa Android `VpnService`.

7 Arquitectura

VPN local

- Objetivo: actuar como intermediario entre el cliente y el servidor, de manera **transparente** para el cliente.



VPN en nuestra aplicación

- Objetivo: interceptar todas las consultas DNS que hace el cliente para dirigirlas a los distintos servidores.

- No se utilizará un servidor externo por 2 motivos:
  - Tendría la información de las consultas
  - Alteraría la selección de proveedores

Idea básica del procesamiento

- Se capturan todos los paquetes que entran al celular y se identifican cuáles son los paquetes UDP y TCP a procesar.
  - Campo en el header IPv4.

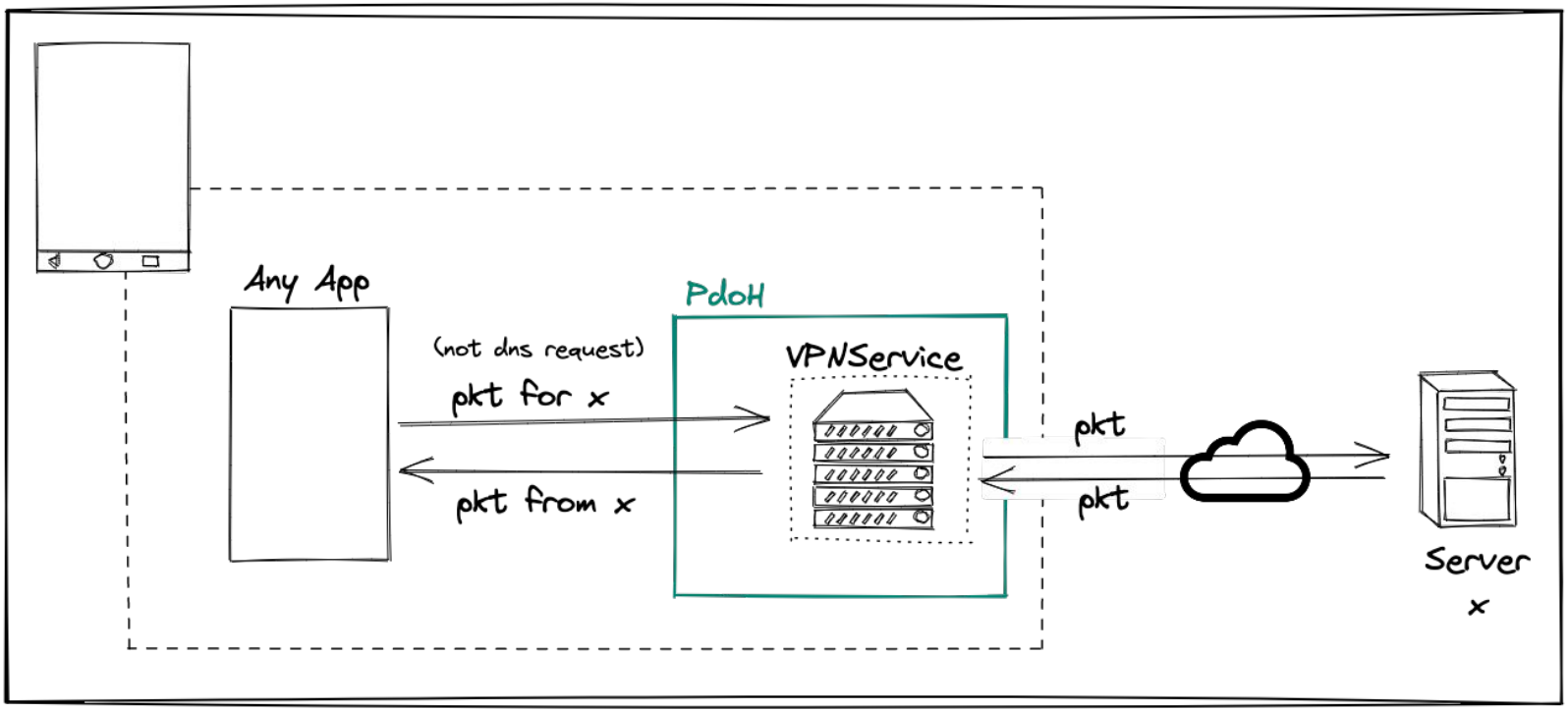
- Paquete DNS: todo paquete UDP cuyo destino sea el puerto 53.
  - Campo en el header UDP.

Un poco más sobre el procesamiento

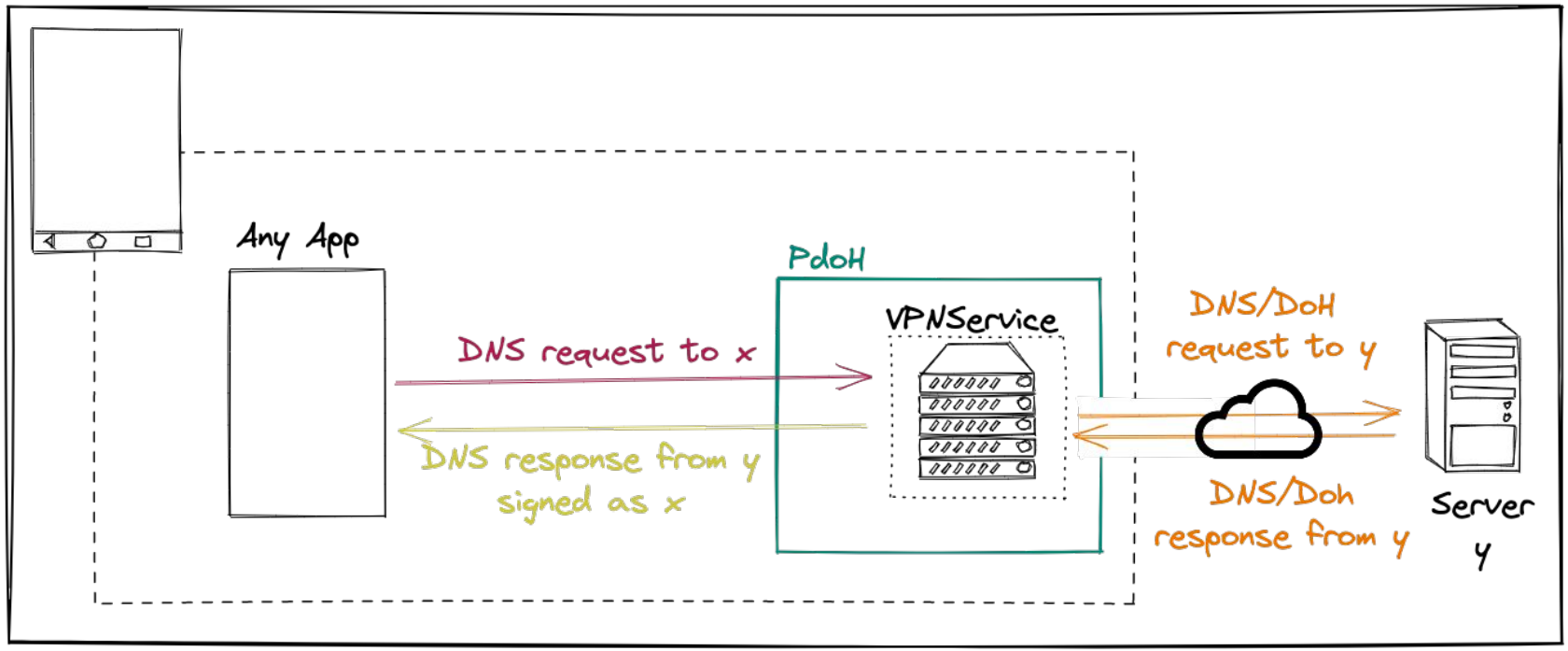
A bajo nivel, la VPN se materializa en 2 *files descriptors*:

- Un **file descriptor** desde donde se leen los bytes entrantes que se pueden mapear a paquetes TCP, UDP o DNS.
- Un **file descriptor** donde se escriben los bytes que representan al paquete procesado.

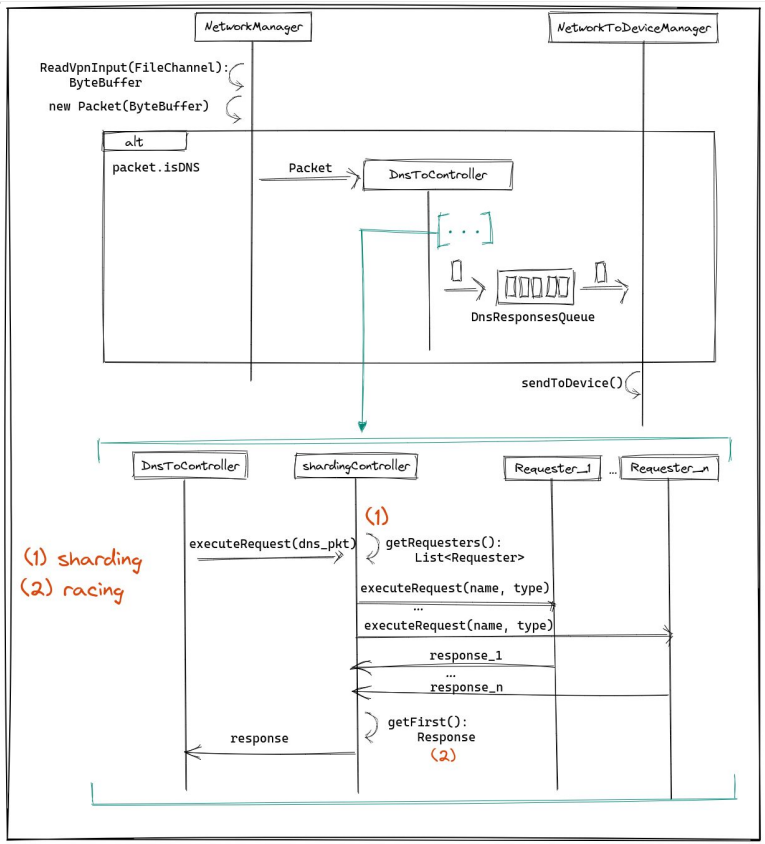
Flujo de paquetes no DNS



Flujo de paquetes DNS



Procesamiento de paquetes DNS



Sharding y racing

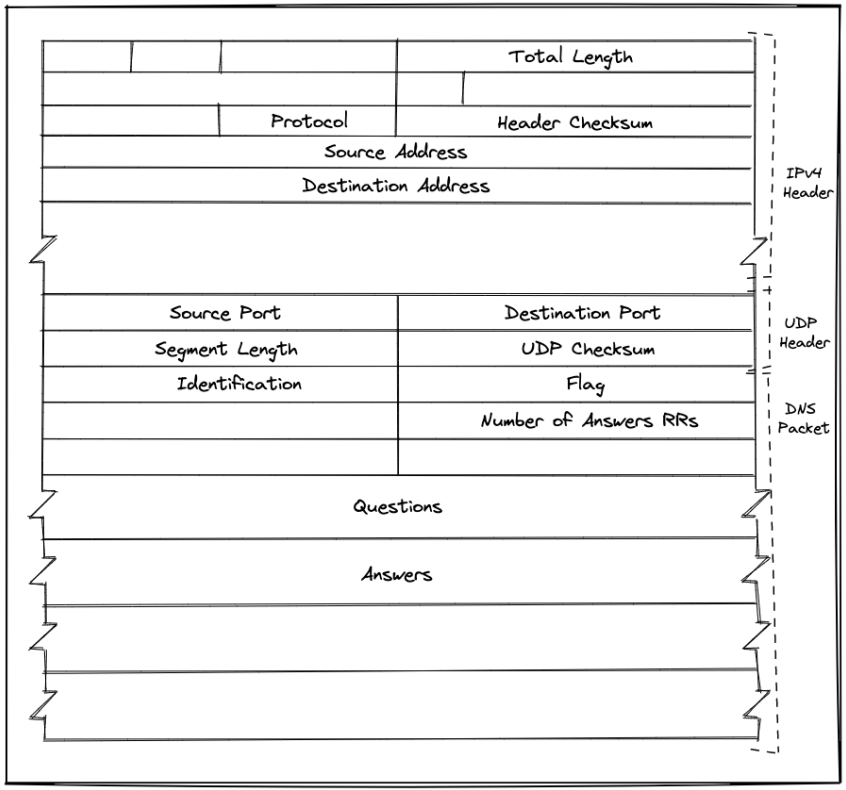
Cada paquete DNS se procesa al enviarse a una cantidad de proveedores configurables mediante la UI → Sharding

- Disposición de tantos grupos como combinaciones sean posibles con los proveedores existentes.
- Algoritmo de Round-Robin para elegir el grupo.

El resultado de la ejecución será el que devuelva el proveedor que resuelva primero la request → Racing

8 Paquete DNS

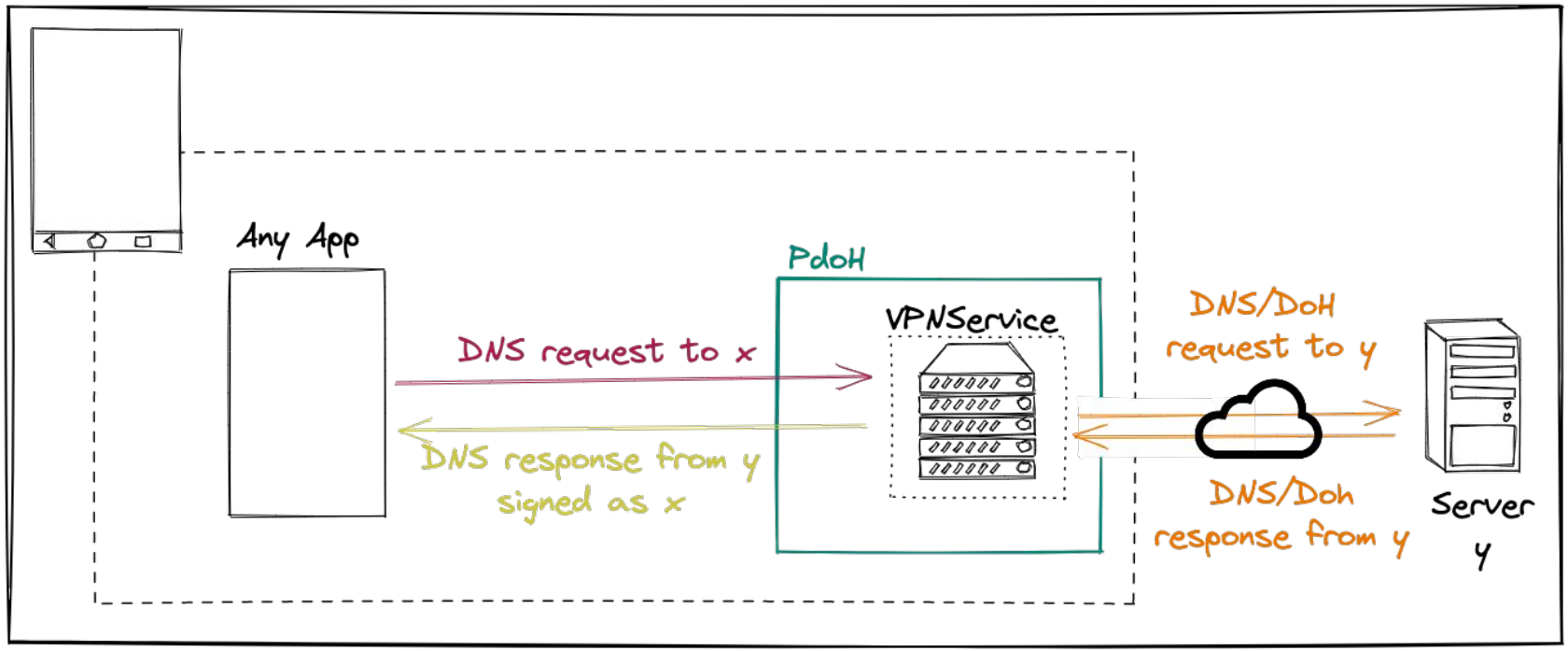
Construcción de paquetes DNS



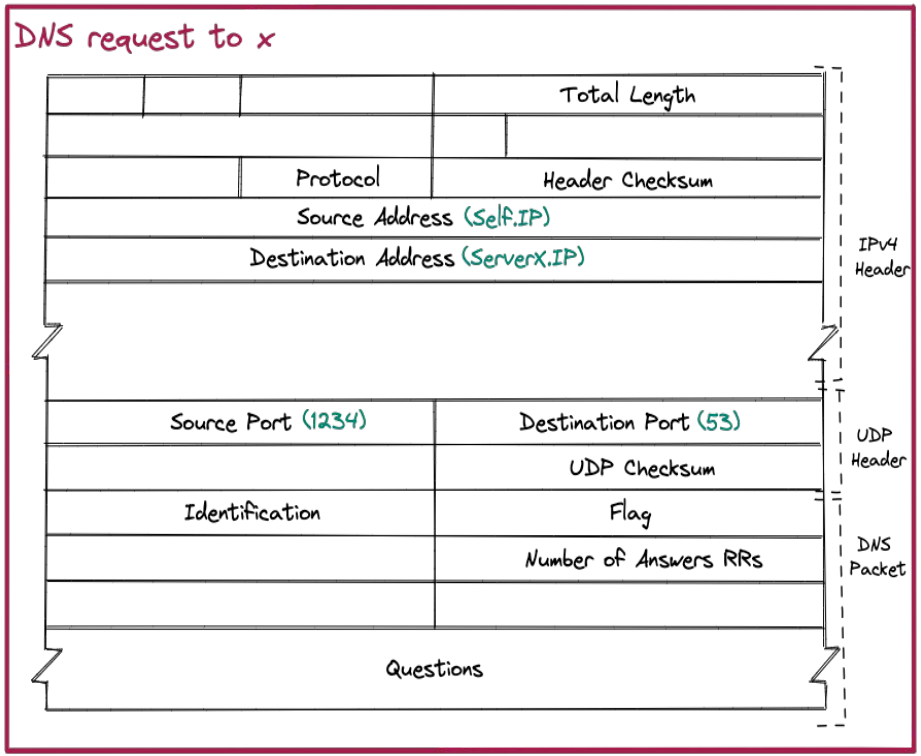
Un paquete DNS se constituye de:

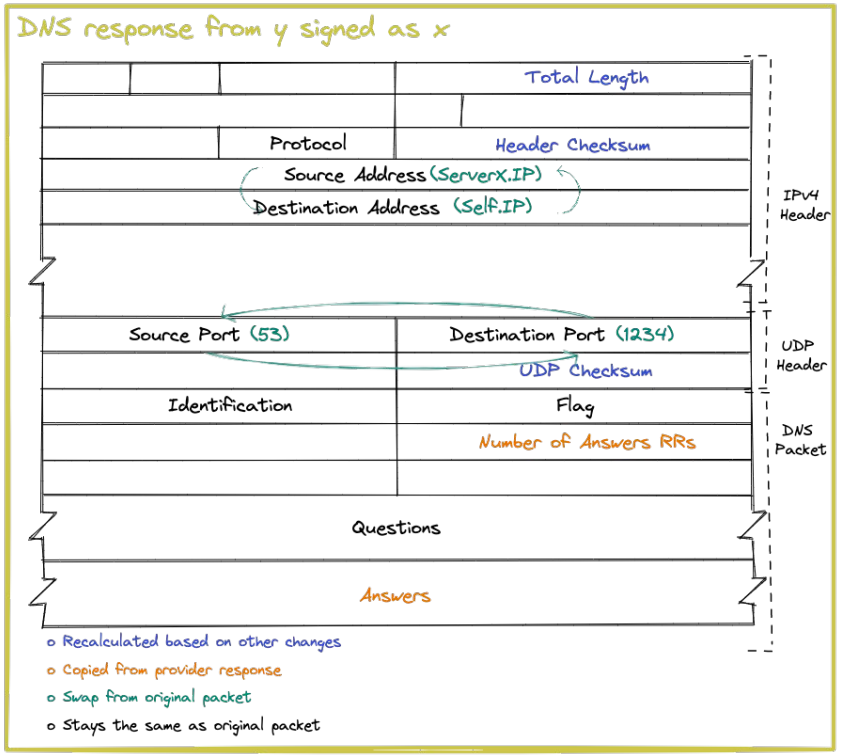
- Header IPV4
- Header UDP
- Header DNS
- Preguntas y respuestas DNS

Flujo de paquetes DNS



Modificaciones al paquete DNS





9 Configuraciones

Configuración DoH

Disponibles los proveedores: Cloudflare, Google y Quad9.

Cantidad de servidores disponibles para racing: 2 o 3

- 2 proveedores: {Google, Cloudflare}, {Google, Quad9} y {Cloudflare, Quad9}.
- 3 proveedores: {Google, Cloudflare, Quad9}.

Cuando mayor sea la cantidad de proveedores, más son las probabilidades de tener mejor performance pero se ve perjudicada la privacidad.

Configuración DNS

Alrededor de 200 servidores públicos disponibles pero pueden **no estar activos**.

- Solución: ping periódico a los proveedores que mantiene una lista de proveedores activos.

→ **Proveedor activo**: se calculan los grupos disponibles para hacer sharding agregando a este proveedor.

→ **Proveedor no activo**: se elimina de todos los grupos existentes.

Ping periódico

Primer enfoque: ping tradicional como paquete ICMP.

- Resultado: todos los proveedores activos ❌
- Responden el ping ICMP pero no están activos.

Enfoque final: request DNS falso con un host determinado por configuración (UUID).

- Request capturado por la VPN pero se identifica y se procesa como un paquete UDP para no ciclar infinitamente.

Implementación DNS

- Necesidad de identificar los paquetes DNS capturados por la VPN.
  - No podemos modificar el host porque es relevante en la consulta ❌
  - Agregamos una segunda consulta con un host configurable (UUID).

- Overhead en el procesamiento.

Configuración Both

- Ensamble de las implementaciones DoH y DNS.
- Se arman grupos con los proveedores DNS y DoH y se determina cuál elegir con el algoritmo round-robin.

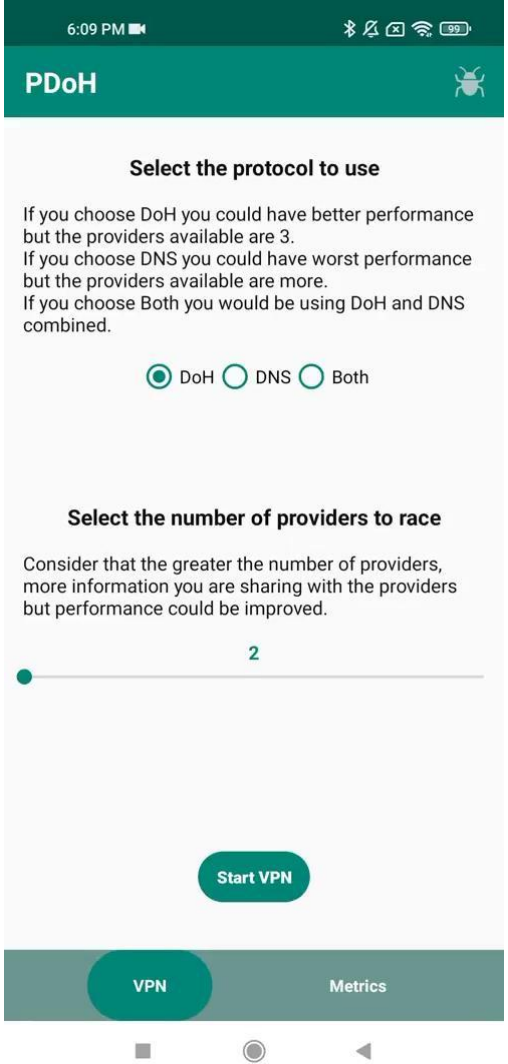
10 Demo

Demo

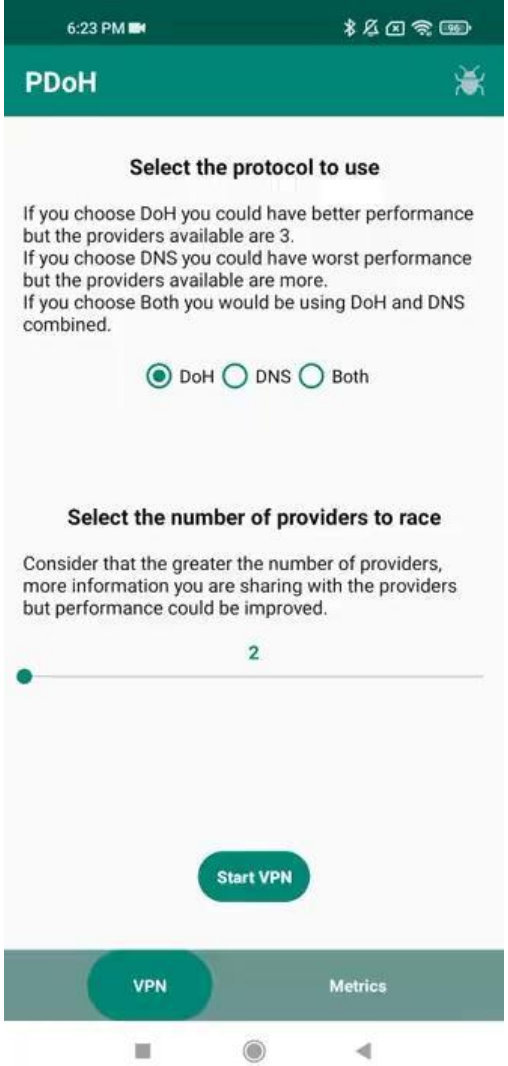
- Configuración DoH
- Configuración DNS
- Configuración Both
- Casos borde

- ¿Qué vamos a verificar?
  - Celular tiene internet
  - Métricas disponibles

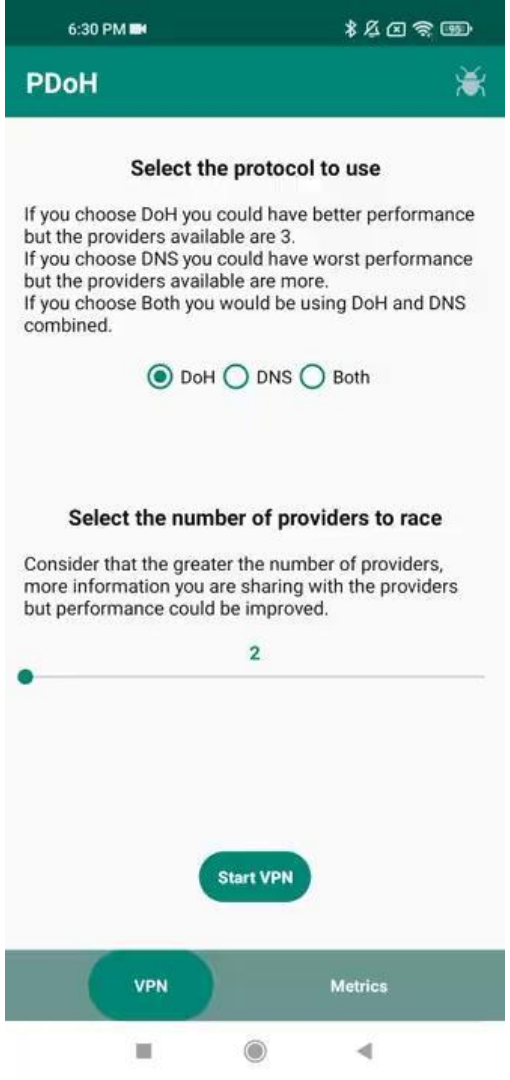
DoH


6:09 PM
PDoH
Select the protocol to use
If you choose DoH you could have better performance but the providers available are 3.
If you choose DNS you could have worst performance but the providers available are more.
If you choose Both you would be using DoH and DNS combined.
DoH
DNS
Both
Select the number of providers to race
Consider that the greater the number of providers, more information you are sharing with the providers but performance could be improved.
2
Start VPN
VPN
Metrics

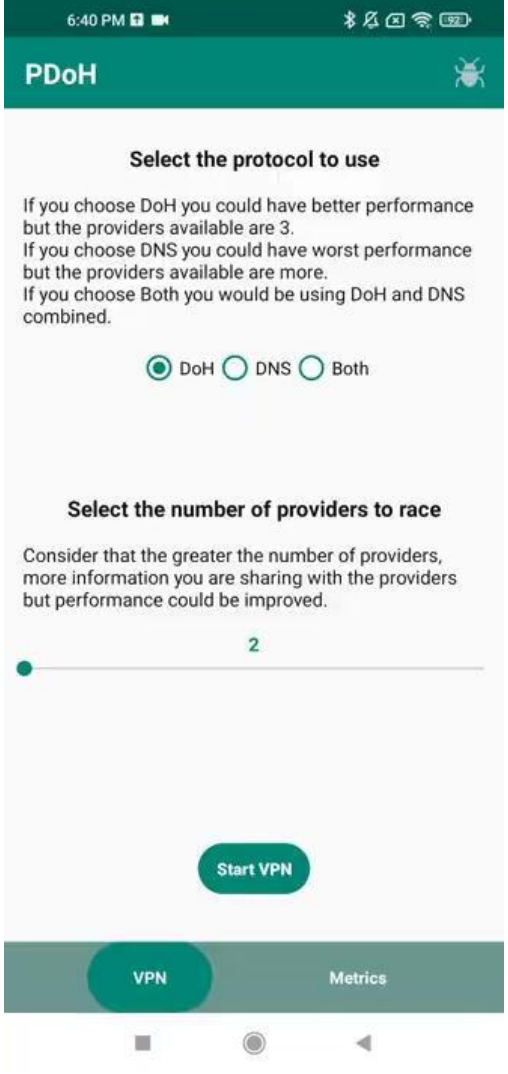
DNS


6:23 PM
PDoH
Select the protocol to use
If you choose DoH you could have better performance but the providers available are 3.
If you choose DNS you could have worst performance but the providers available are more.
If you choose Both you would be using DoH and DNS combined.
DoH
DNS
Both
Select the number of providers to race
Consider that the greater the number of providers, more information you are sharing with the providers but performance could be improved.
2
Start VPN
VPN
Metrics

Both


6:30 PM
PDoH
Select the protocol to use
If you choose DoH you could have better performance but the providers available are 3.
If you choose DNS you could have worst performance but the providers available are more.
If you choose Both you would be using DoH and DNS combined.
DoH
DNS
Both
Select the number of providers to race
Consider that the greater the number of providers, more information you are sharing with the providers but performance could be improved.
2
Start VPN
VPN
Metrics

Casos borde


6:40 PM
PDoH
Select the protocol to use
If you choose DoH you could have better performance but the providers available are 3.
If you choose DNS you could have worst performance but the providers available are more.
If you choose Both you would be using DoH and DNS combined.
DoH
DNS
Both
Select the number of providers to race
Consider that the greater the number of providers, more information you are sharing with the providers but performance could be improved.
2
Start VPN
VPN
Metrics

11 Lecciones

Lecciones aprendidas

- Armado de la respuesta DNS
- Sólo 3 proveedores DoH
- Android cerraba la aplicación después de 1 hora
  - Notificación
  - Memory leak

12 Trabajo futuro

¿Qué más podría tener la aplicación?

- Soporte IPv6
- Configuración de proveedores
- Más métricas
- ODoH (Oblivious DoH)
- iOS

13 Conclusiones

Beneficios de la aplicación

- Uso de los beneficios de DoH para preservar la privacidad del patrón de conductas del usuario
- Implementación de sharding y racing
- Posibilidad de utilizar una configuración DNS o DoH
- Métricas disponibles para analizar el comportamiento de la aplicación

14 ¿Preguntas?

15 Gracias totales

Muchas gracias por escucharnos!

Les dejamos el QR para bajarse la aplicación si les gustó.

Solo para Android