Extensiones de seguridad para el sistema de nombres de dominio (DNSSEC)

En días pasados por Twitter dimos cuenta de la novedad de que el Centro de Información de Red de Venezuela (NIC.VE) tenía un nuevo alias en esa red social y que el WHOIS estaba funcionando por línea de comandos (durante un tiempo solo se podía consultar por la página web de ese organismo):

https://twitter.com/ks7000/status/1244993626180067330

¡Artículo en construcción!

La persona que nos recordó acerca del nuevo valor de los dominios web venezolanos es la Licenciada Lenis Querales, quien actualizó su tutorial al respecto (creación, renovación, configuración DNS, etc.)

https://twitter.com/Shcove1/status/1244995999048839168

Gracias a ella recordamos de revisar el estado del dominio de Internet *(en adelante simplemente "dominio")* nic.ve en sí mismo (por medio de WHOIS) y nos percatamos que ahora tiene DNSKEY ***¿pero qué es esto?*** Pues sigan leyendo nuestro artículo de hoy...

Advertencia.

> No trabajamos para ningún gobierno de país alguno. La imagen que encabeza este artículo la he elegido porque la práctica que haremos será sobre ese dominio en particular. En todo caso esta entrada es publicada de manera única, y exclusivamente, **con propósitos didácticos.**
>
> ¡Quedan avisadas y avisados!



¿Qué es DNSSEC?

Si quieren la explicación completa pueden leerla con total calma en Wikipedia, yo he colaborado en la redacción de dicho artículo y recomiendo su lectura. Sin embargo por acá tenemos otra manera y estilo de trabajar así que lo expresaré en mis propias palabras.

[SVG: DNS en el mundo real (Wikipedia https://commons.wikimedia.org/wiki/File:DNS_en_el_mundo_real.svg)]

DNS en el mundo real (Wikipedia https://commons.wikimedia.org/wiki/File:DNS_en_el_mundo_real.svg)

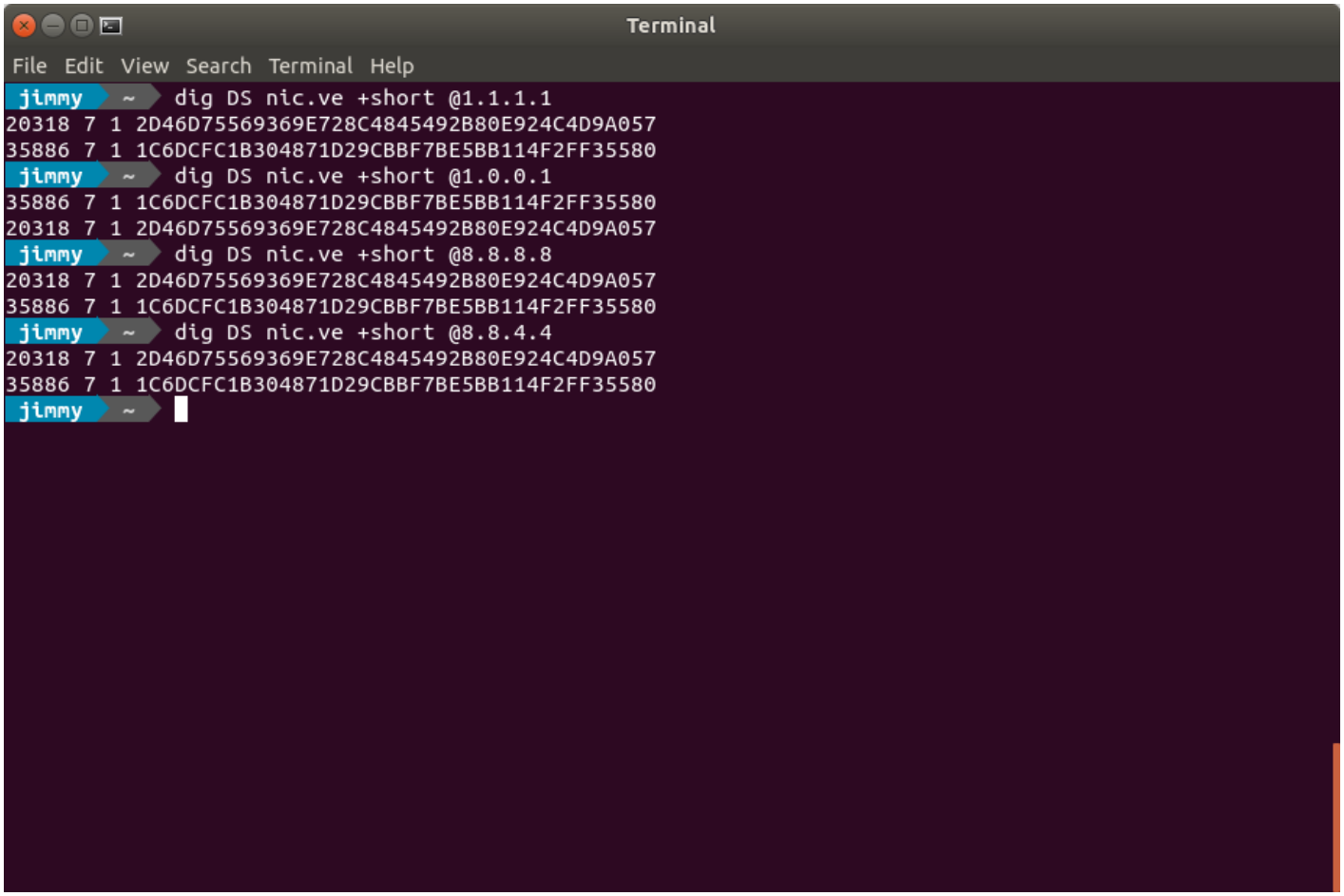
El gráfico anterior, tomado de Wikipedia, ilustra rápidamente como un ordenador resuelve un dominio de Internet. «Resolver un dominio de Internet» significa convertir "el nombre" del sitio o página web a una o varias direcciones IPv4 o IPv6. ¿Recuerdan lo que es el HTTP? ¿Recuerdan el uso de HTTPS, página web segura para conectar a bancos y entidades financieras?

Pues bien, DNSSEC va de lo mismo: certificados digitales públicos que pueden ser comprobados por terceros en una cadena de confianza. En el caso de los navegadores web la cadena de confianza comienza con el propio navegador que al instalarlo tiene sus propios certificados iniciales de confianza para ganar tiempo, rapidez. **Este artículo trata de comprobar dicho mecanismo pero en DNSSEC,** utilizando como ejemplo el dominio de Internet nic.ve que encabeza la entrada.

Consultar si un dominio posee DNSSEC

Abriremos una ventana terminal e introduciremos el siguiente comando:

```
dig DS nic.ve +short @1.1.1.1
```



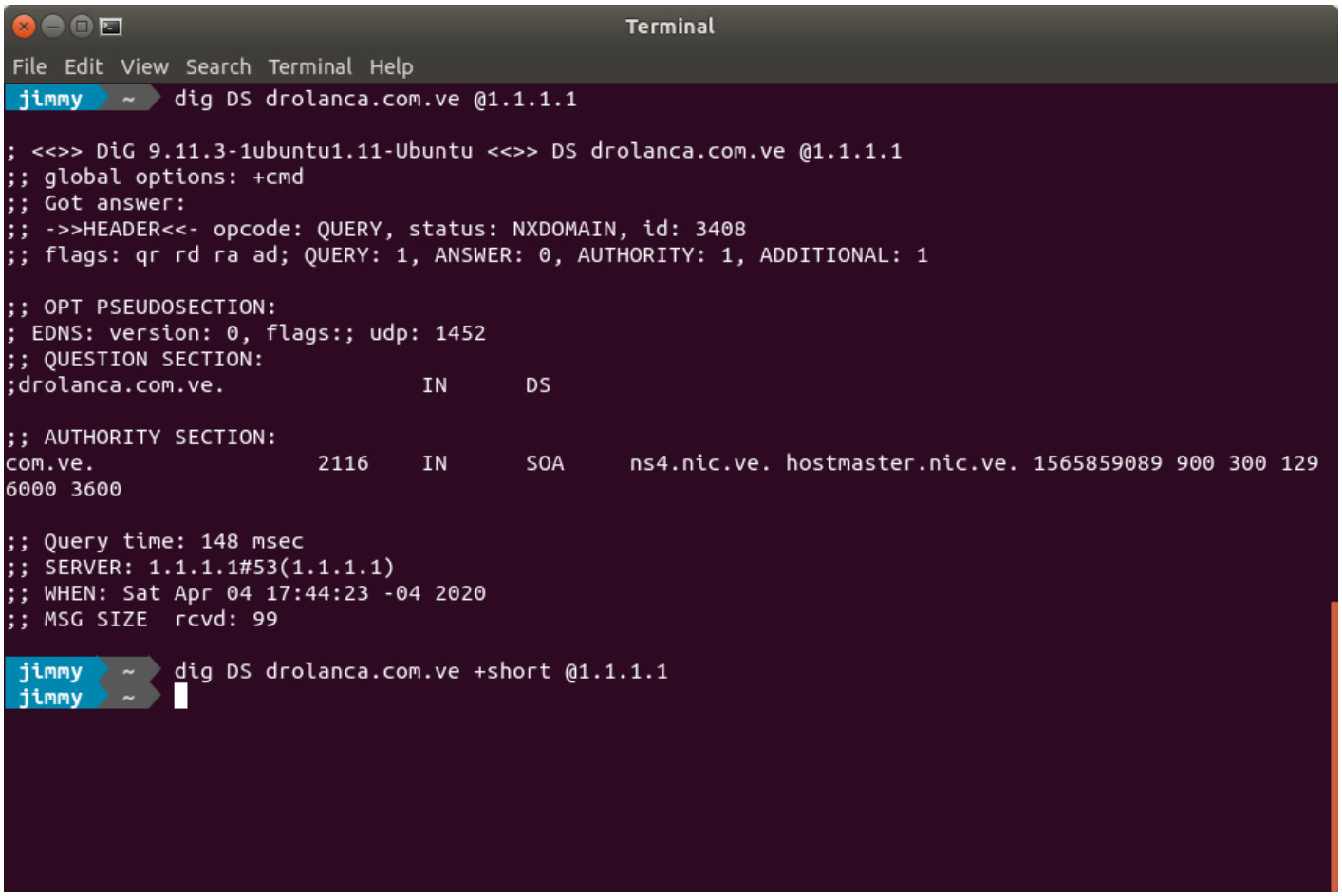
dig DS nic.ve +short @1.1.1.1

Explico:

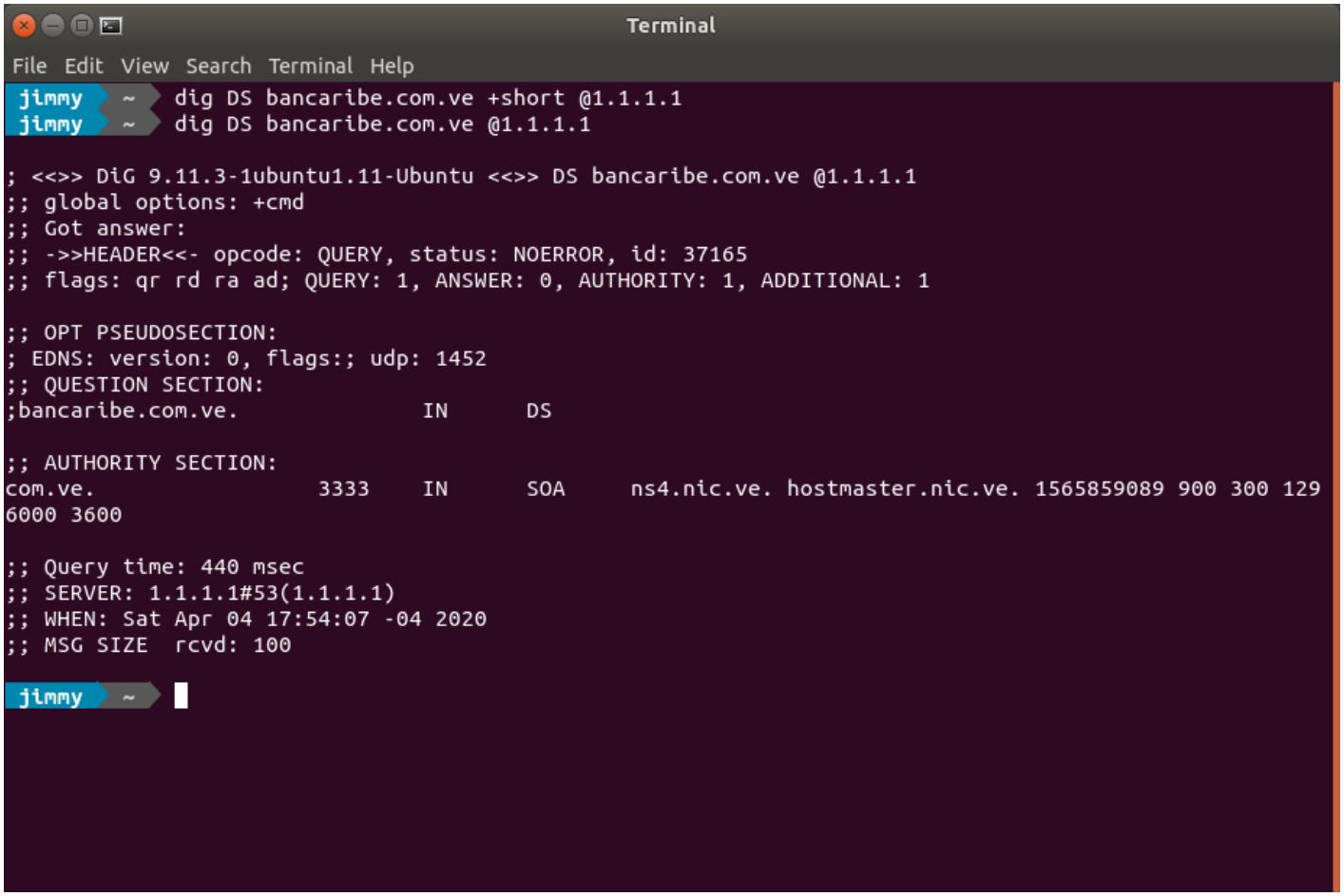
- **dig**: el ejecutable que indagará a un servidor DNS, ya veremos cuál.
- **DS**: en inglés *Delegation Signer*, uno de los cuatro tipos especiales de registro para DNSSEC (pueden consultar en Wikipedia el resto de ellos). Es un archivo de zona firmado digitalmente, en este caso delegado.
- **nic.ve**: pues el dominio que nos interesa y ocupa, por ahora.
- **+short**: parámetro de **dig**, necesario para que nos entregue la información justa.
- **@1.1.1.1**: son los DNS de la empresa **Cloudflare**. Es una historia larga de contar pero, esencialmente, APNIC (Centro de Información de la Red de Asia y el Pacífico, uno de los cinco registradores de dominios principales a nivel mundial), tenía reservadas las direcciones IPv4 *muy singulares* para propósitos de estudio y precisamente fueron encomendadas a Cloudflare para ello. La otra dirección es **1.0.0.1**, la cual, como ven, es muy singular -y fácil de recordar-.

- **@8.8.4.4**: en este caso pertenece a la empresa Google, el DNS principal es **8.8.8.8** y viene funcionando desde el año 2009.

Como ustedes pueden ver, consultamos a cuatro diferentes resolutores de dominio y devuelven los mismos valores, aunque no en el mismo orden. A continuación presento dos capturas de pantalla consultando el dominio de una droguería y un banco, ambos de Venezuela y con los que trabajo día a día, fíjense también qué sucede cuando obviamos el parámetro **+short**:

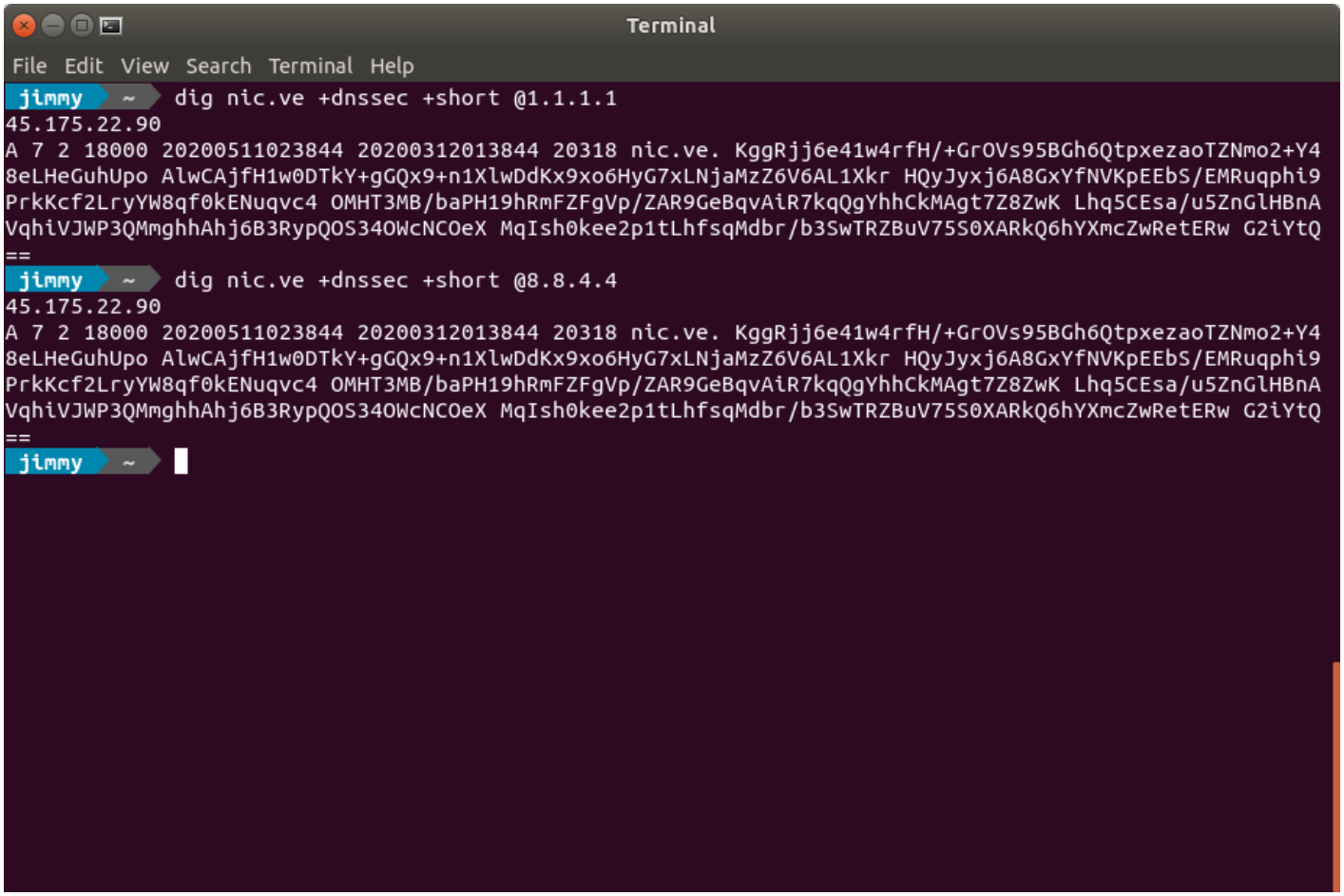


dig DS drolanca.com.ve +short @1.1.1.1



dig DS bancaribe.com.ve +short @1.1.1.1

Si tiene DNSSEC ¿cuál es su DNSKEY?



dig nic.ve +dnssec +short @1.1.1.1

Abriremos una ventana terminal e introduciremos el siguiente comando:

```
dig nic.ve +dnssec +short @1.1.1.1
```

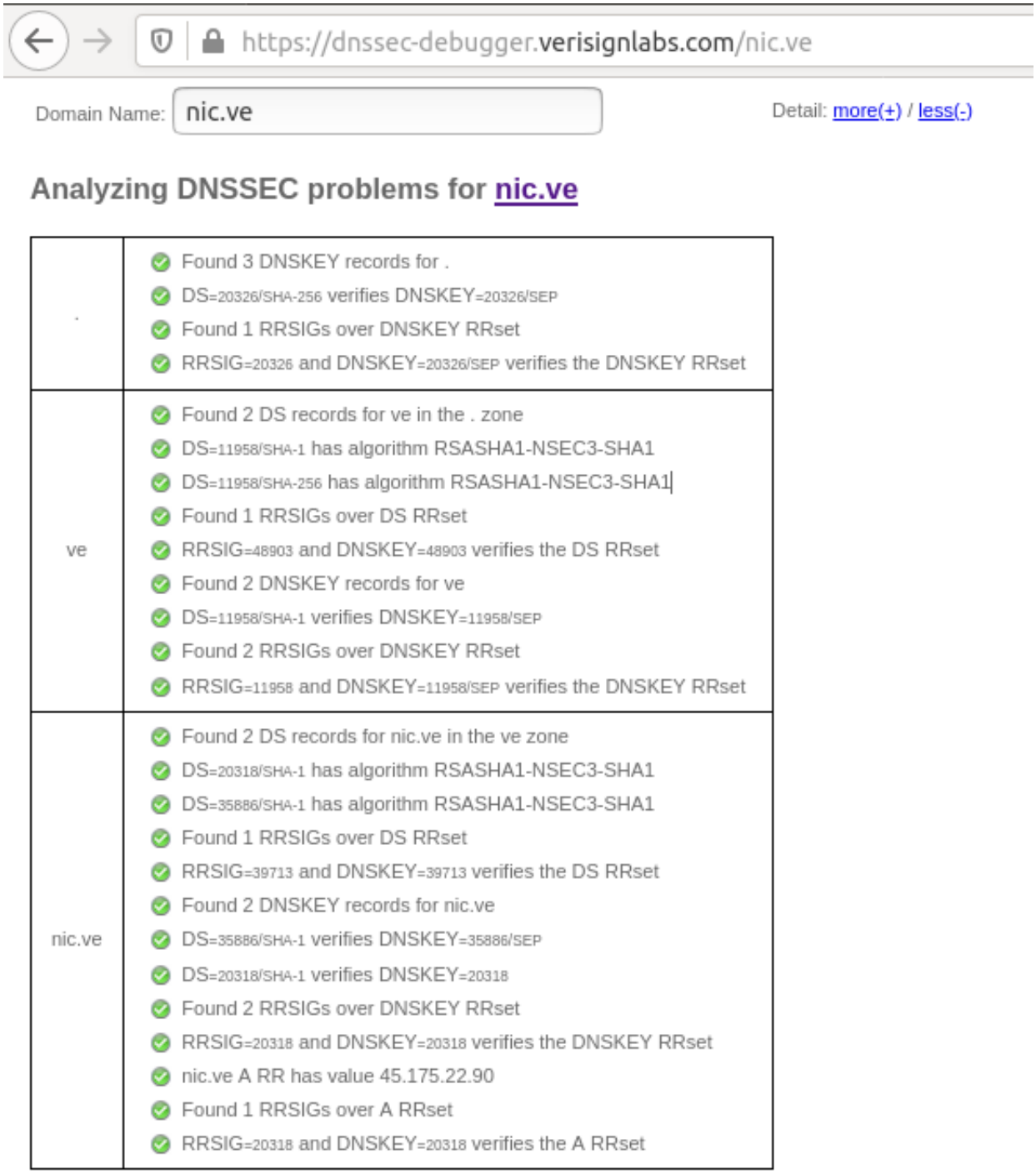
Explico:

- **dig**: el ejecutable que indagará a un servidor DNS, ya veremoos cuál.
- **nic.ve**: pues el dominio que nos interesa y ocupa, por ahora.
- **+dnssec**: parámetro de **dig** para indicarle que nos devuelva ese valor.
- **+short**: parámetro de **dig**, necesario para que nos entregue la información justa.
- **@1.1.1.1**: son los servidores de la empresa **Cloudflare**. Es una historia larga de contar pero, esencialmente, APNIC (Centro de Información de la Red de Asia y el Pacífico) uno

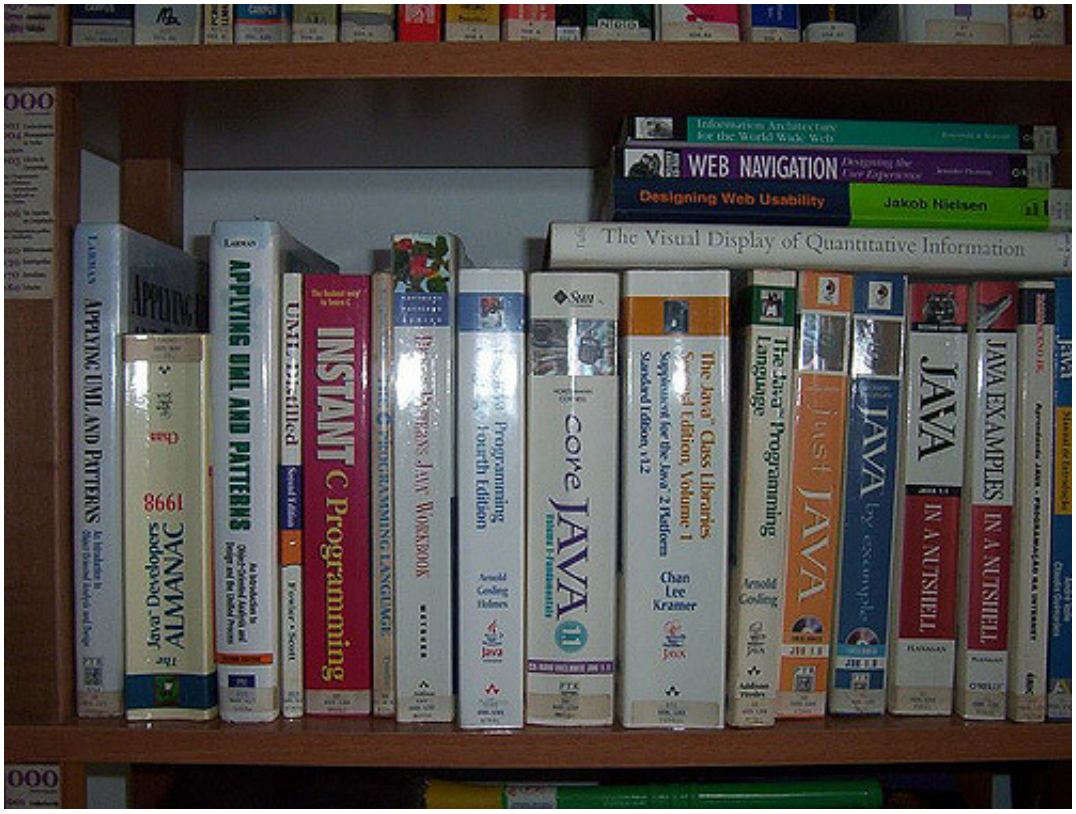
de los cinco registradores de dominios principales a nivel mundial tenía reservadas las direcciones IPv4 *muy singulares* para propósitos de estudio y precisamente fueron encomendadas a Cloudflare para ello. La otra dirección es **1.0.0.1**, la cual, como ven, es muy singular y fácil de recordar.

- **@8.8.4.4**: en este caso pertenece a la empresa Google, el DNS principal es **8.8.8.8** y viene funcionando desde el año 2009.

Como



Analizando problemas en DNSSEC para nic.ve



Fuentes consultadas

En idioma castellano

- «DNSSec por Eduardo Collado».
- «DNSSEC (ICANN wiki)».
- «».

En idioma francés

- «».

- «».
- «».

En idioma inglés



- «How to test and validate DNSSEC using dig command line».
- «What is a KSK, ZSK, RRSIG?».
- «What is the Chain of Trust?».
- «Caching with DNSMasq and optionally with DNSSEC».
- «dnsmasq (Archlinux wiki)».
- «DNSSEC (Archlinux wiki)».
- «https://www.digitalocean.com/community/tutorials/how-to-use-dig-whois-ping-on-an-ubuntu-vps-to-query-dns-data»



Crédito de la imagen Gerd Altmann, trabajo, licencia de uso:Pixabay