Fiuba
Facultad de Ingeniería
Universidad de Buenos Aires

Departamento de Computación
TA048 - REDES

Tarea Individual - 2° Cuatrimestre 2025

“Captura de “dig” con Wireshark”

Docente: José Ignacio Alvarez Hamelin

Alumna	Padrón	Email
Valdivia Wong, Angie Isabella	103727	avaldivia@fi.uba.ar

Fecha de entrega: 24/08/25

Comentarios:

I. Caso Iterativo:

Primero realicé la prueba en la terminal de **Linux Mint** utilizando el comando **+trace** con el dominio www.youtube.com. Lo que se observa es una especie de **“caminata DNS”**, donde la resolución comienza en los **servidores raíz**, continúa en los del **TLD .com**, luego pasa a los **servidores de youtube.com** y finalmente llega a la **respuesta definitiva** con la dirección solicitada. Este proceso puede apreciarse en las capturas de pantalla adjuntas, donde resalté las etapas principales con rectángulos.

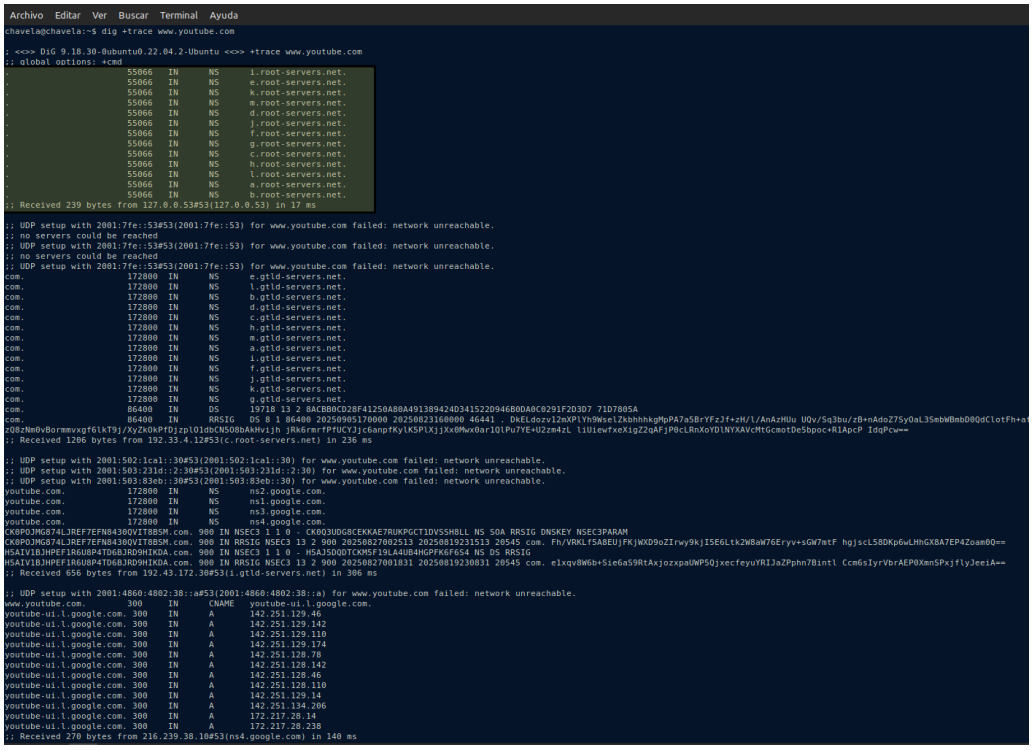


Figura 01: Se consulta a los servidores raices

Lo que interpreto es que el resolver local (127.0.0.53) me dió los Roots Servers, la raiz (.) no sabe la IP de www.youtube.com., pero me dice quién sabe sobre .com

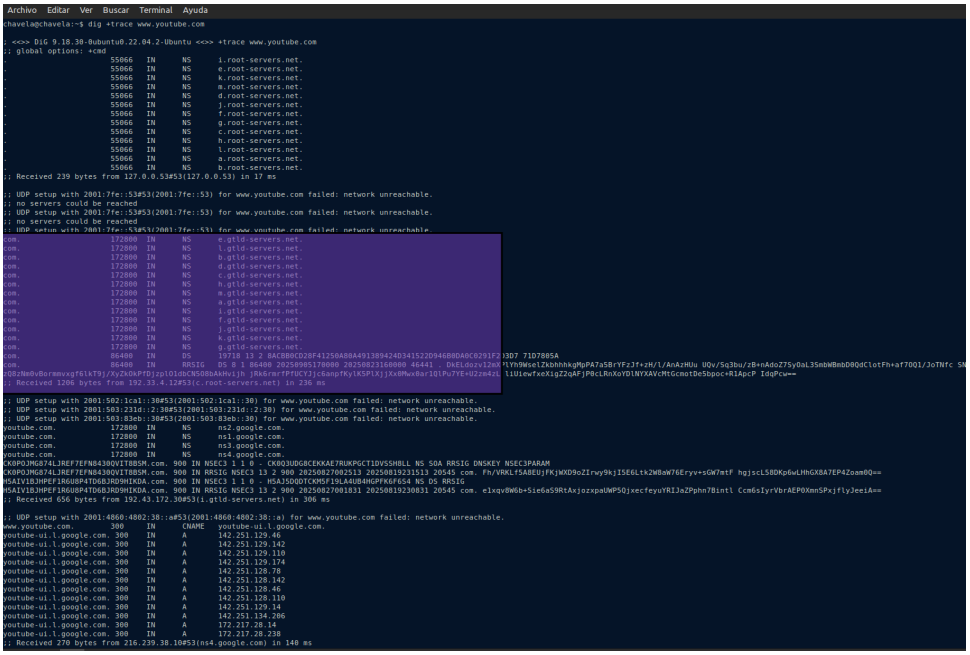


Figura 02: Se pasa a los .com

Acá me está diciendo “No sé la IP de www.youtube.com., pero los que saben sobre .com son estos NS” y me dan la lista de los TLD servers de .com

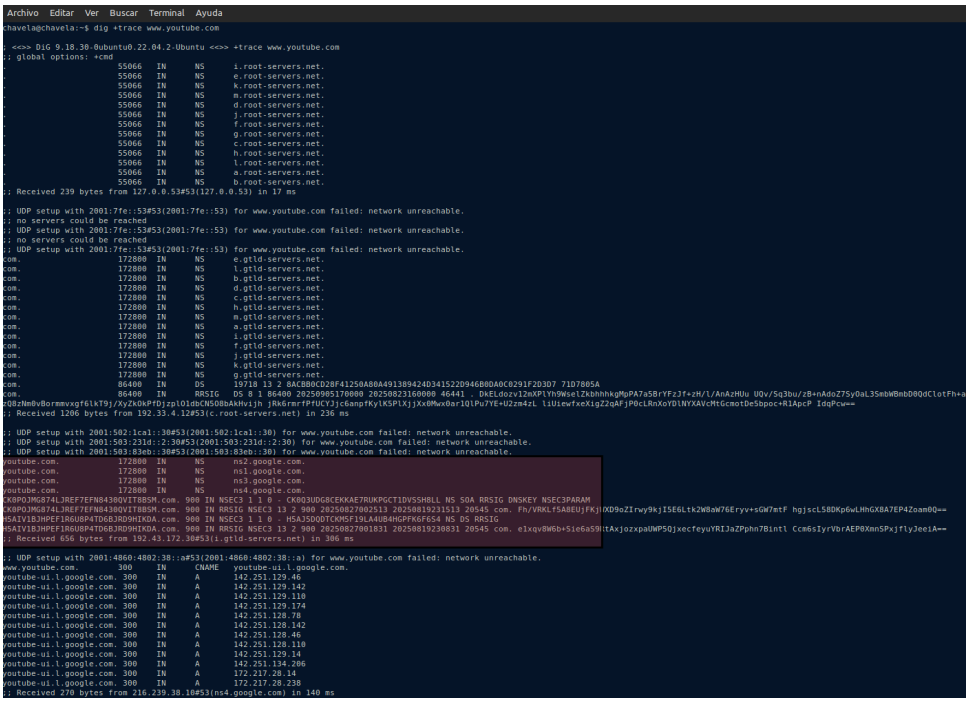


Figura 03: Delegación hacia youtube.com

Ahora un servidor de .com respondió “los servidores autoritativos de youtube.com. son los de Google (ns1.google.com , etc..)”

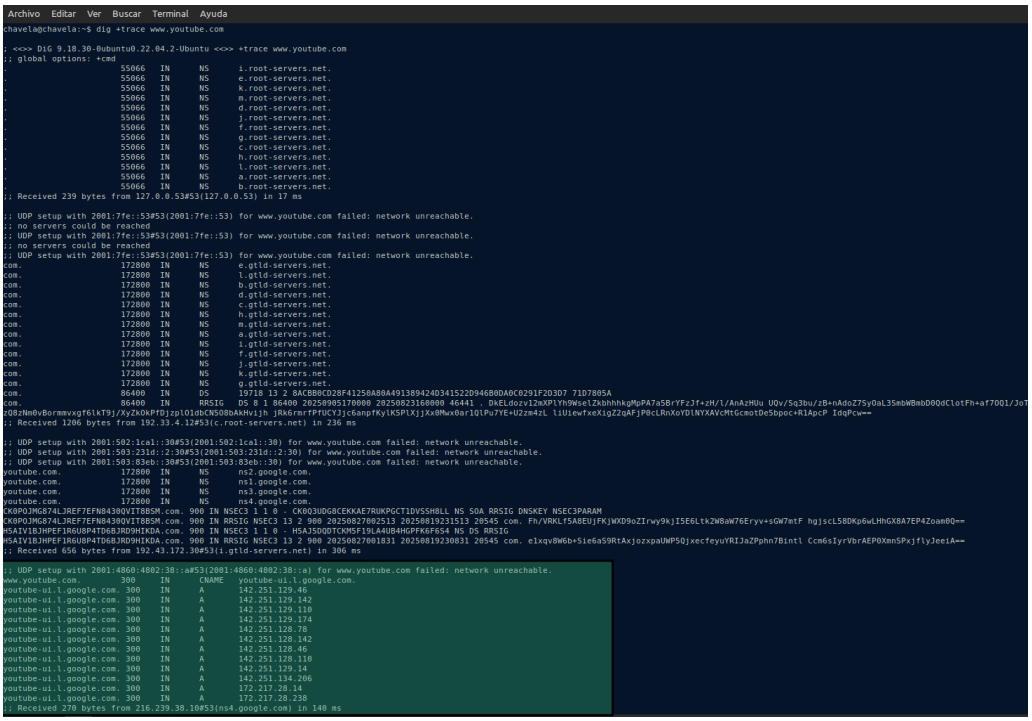
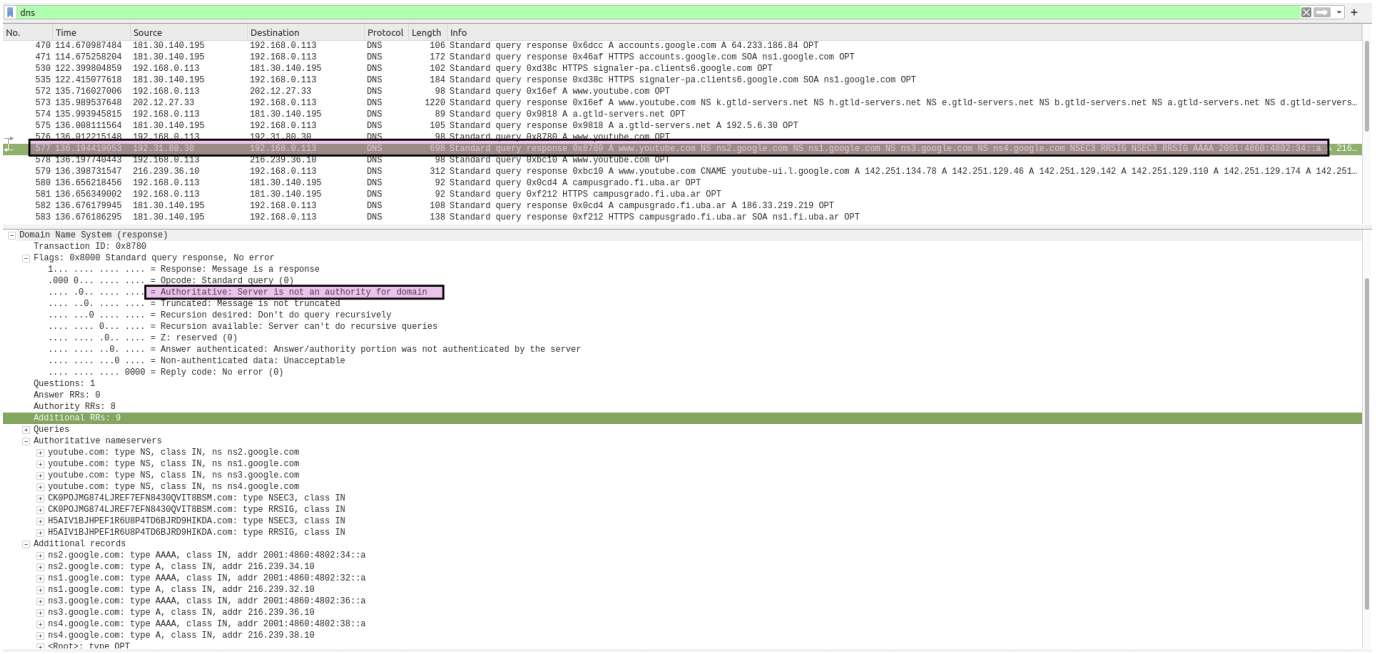


Figura 04: Respuesta Final

Entonces, se observa que www.youtube.com no tiene IP directa, es un alias llamado ***CNAME*** a ***youtube-ui.l.google.com*** , y ese nombre sí tiene un monton de direcciones IP (***A***) y la respuesta la dió ns4.google.com que es **autoritativo** para youtube.com.

Usando la herramienta wireshark:



Analizando el caso de Standard query response mirando las pestañas del Domain Name System:

- En la parte resaltada indica que el servidor **NO es autoritativo** , respetando en la otra terminal el comando de:

  dig +trace www.youtube.com

- Pero mas abajo me muestra los servers que sí son Autoritativos y que es lo mismo mostrado en las terminales (imágenes anteriores) que son mas completos.
- Si tomo uno de esos servers autoritativos y lo filtro en el wireshark me tiene que salir que es autoritativo , eso se va analizar en la siguiente sección.

II. Caso Autorizada:

Para este caso probé directamente con el comando ***"dig"***

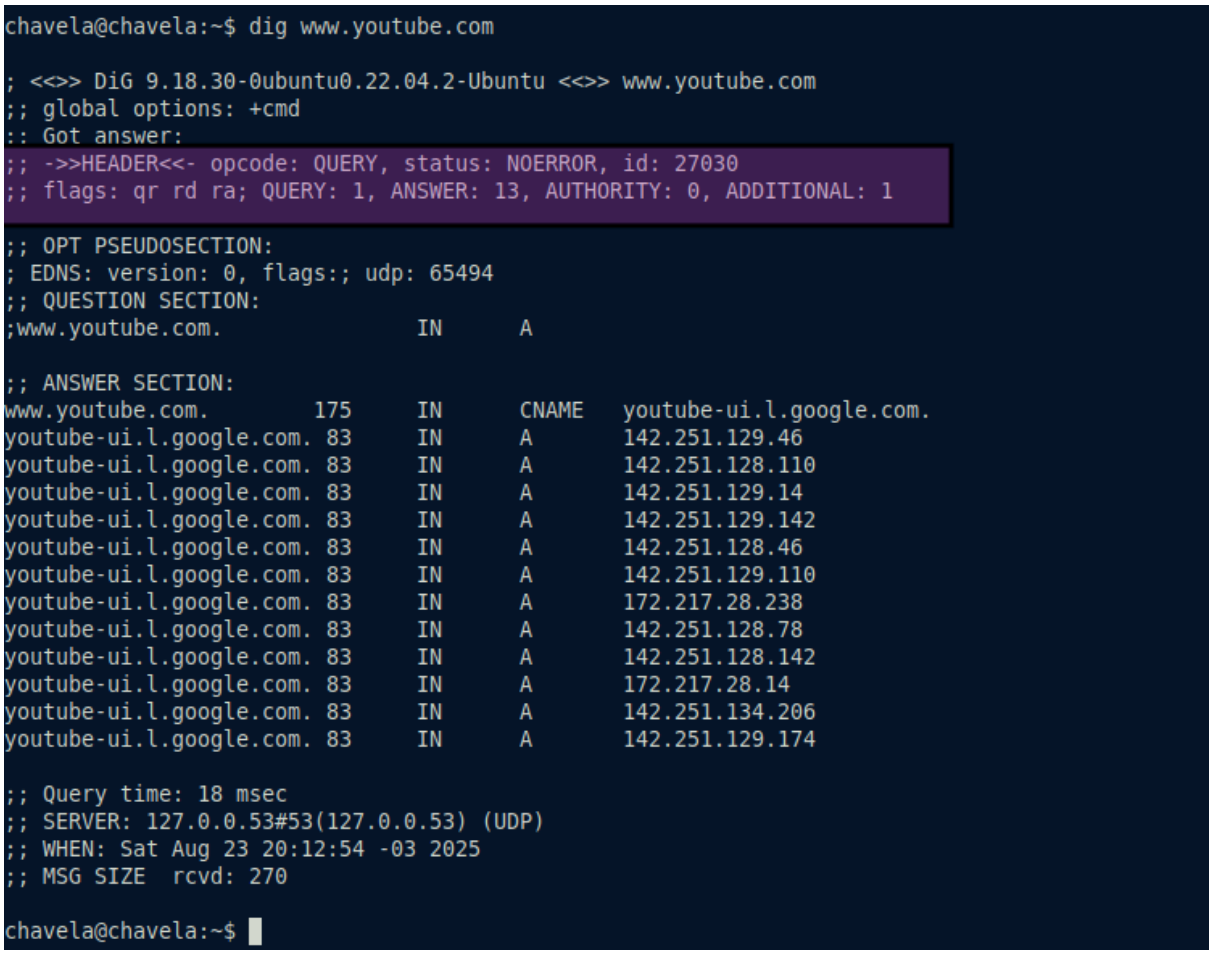


Figura 05: Consultando un registro normal

Como se observa en la parte resaltada en los flags no aparece ***" aa "*** que significa que fue una respuesta no autoritativa .

Entonces hago lo siguiente:

```
chavela@chavela:~$ dig NS youtube.com +short
ns3.google.com.
ns4.google.com.
ns1.google.com.
ns2.google.com.
chavela@chavela:~$ dig @ns1.google.com www.youtube.com

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> @ns1.google.com www.youtube.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18640
;; flags: qr aa rd; QUERY: 1, ANSWER: 14, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.youtube.com.               IN      A

;; ANSWER SECTION:
www.youtube.com.        300     IN      CNAME   youtube-ui.l.google.com.
youtube-ui.l.google.com. 300    IN      A       142.251.134.78
youtube-ui.l.google.com. 300    IN      A       172.217.28.238
youtube-ui.l.google.com. 300    IN      A       142.251.129.46
youtube-ui.l.google.com. 300    IN      A       142.251.129.142
youtube-ui.l.google.com. 300    IN      A       142.251.129.110
youtube-ui.l.google.com. 300    IN      A       142.251.129.174
youtube-ui.l.google.com. 300    IN      A       142.251.128.78
youtube-ui.l.google.com. 300    IN      A       142.251.128.142
youtube-ui.l.google.com. 300    IN      A       142.251.128.46
youtube-ui.l.google.com. 300    IN      A       142.251.128.110
youtube-ui.l.google.com. 300    IN      A       142.251.129.14
youtube-ui.l.google.com. 300    IN      A       142.251.134.206
youtube-ui.l.google.com. 300    IN      A       172.217.28.14

;; Query time: 39 msec
;; SERVER: 216.239.32.10#53(ns1.google.com) (UDP)
;; WHEN: Sat Aug 23 20:21:53 -03 2025
;; MSG SIZE  rcvd: 286

chavela@chavela:~$
```

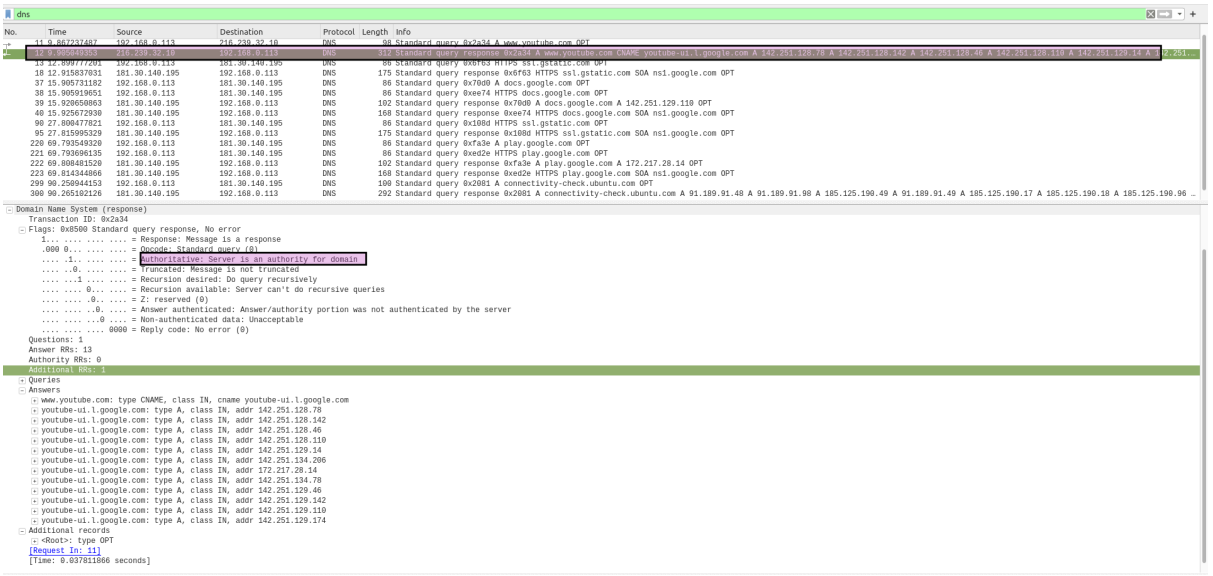
Figura 06: Forzar consulta a servidores autoritativos

Lo que hice ahí fue averiguar primero que me muestre la lista de servidores autoritativos del dominio, luego:

```
chavela@chavela:~$ dig NS youtube.com +short
ns3.google.com.
ns4.google.com.
ns1.google.com.
ns2.google.com.
chavela@chavela:~$ dig @ns1.google.com www.youtube.com

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> @ns1.google.com www.youtube.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18640
;; flags: qr aa rd; QUERY: 1, ANSWER: 14, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.youtube.com.               IN      A

;; ANSWER SECTION:
www.youtube.com.        300     IN      CNAME   youtube-ui.l.google.com.
youtube-ui.l.google.com. 300    IN      A       142.251.134.78
youtube-ui.l.google.com. 300    IN      A       172.217.28.238
youtube-ui.l.google.com. 300    IN      A       142.251.129.46
youtube-ui.l.google.com. 300    IN      A       142.251.129.142
youtube-ui.l.google.com. 300    IN      A       142.251.129.110
youtube-ui.l.google.com. 300    IN      A       142.251.129.174
youtube-ui.l.google.com. 300    IN      A       142.251.128.78
youtube-ui.l.google.com. 300    IN      A       142.251.128.142
youtube-ui.l.google.com. 300    IN      A       142.251.128.46
youtube-ui.l.google.com. 300    IN      A       142.251.128.110
youtube-ui.l.google.com. 300    IN      A       142.251.129.14
youtube-ui.l.google.com. 300    IN      A       142.251.134.206
youtube-ui.l.google.com. 300    IN      A       172.217.28.14

;; Query time: 39 msec
;; SERVER: 216.239.32.10#53(ns1.google.com) (UDP)
;; WHEN: Sat Aug 23 20:21:53 -03 2025
;; MSG SIZE  rcvd: 286

chavela@chavela:~$
```

Una vez que haya elegido a uno de ellos (ns1.google.com) le pregunto directamente al servidor DNS autoritativo de Google (que maneja youtube.com) y en la salida se nota que aparece la flag **“ aa ”** que significa Authoritative Answer.

Usando la herramienta wireshark:



Analizando el caso de Standard query response mirando las pestañas del Domain Name System:

- En la parte resaltada indica que el servidor **Si es autoritativo** , respetando en la otra terminal el comando de:

  dig @ns1.google.com www.youtube.com

- En la pestaña de Answers incluye un registro CNAME que indica que www.youtube.com es un alias de youtube-ui.l.google.com
- Asi mismo se observa varios registros “A” asociados a diferentes direcciones IP de youtube-ui.l.google.com
- Esto muestra la verdadera relación jerárquica entre el nombre solicitado y su dominio dentro de Google, la consulta autorizada devuelve la respuesta oficial desde el servidor que tiene la autoridad sobre el dominio

III. Caso Verborragico:

En este caso noté que solo muestra información adicional sobre el proceso de la consulta DNS , en mi caso como el sistema operativo es una versión más actualizada tuve que poner mas flags en los comandos para que me muestre detalles más específicos:

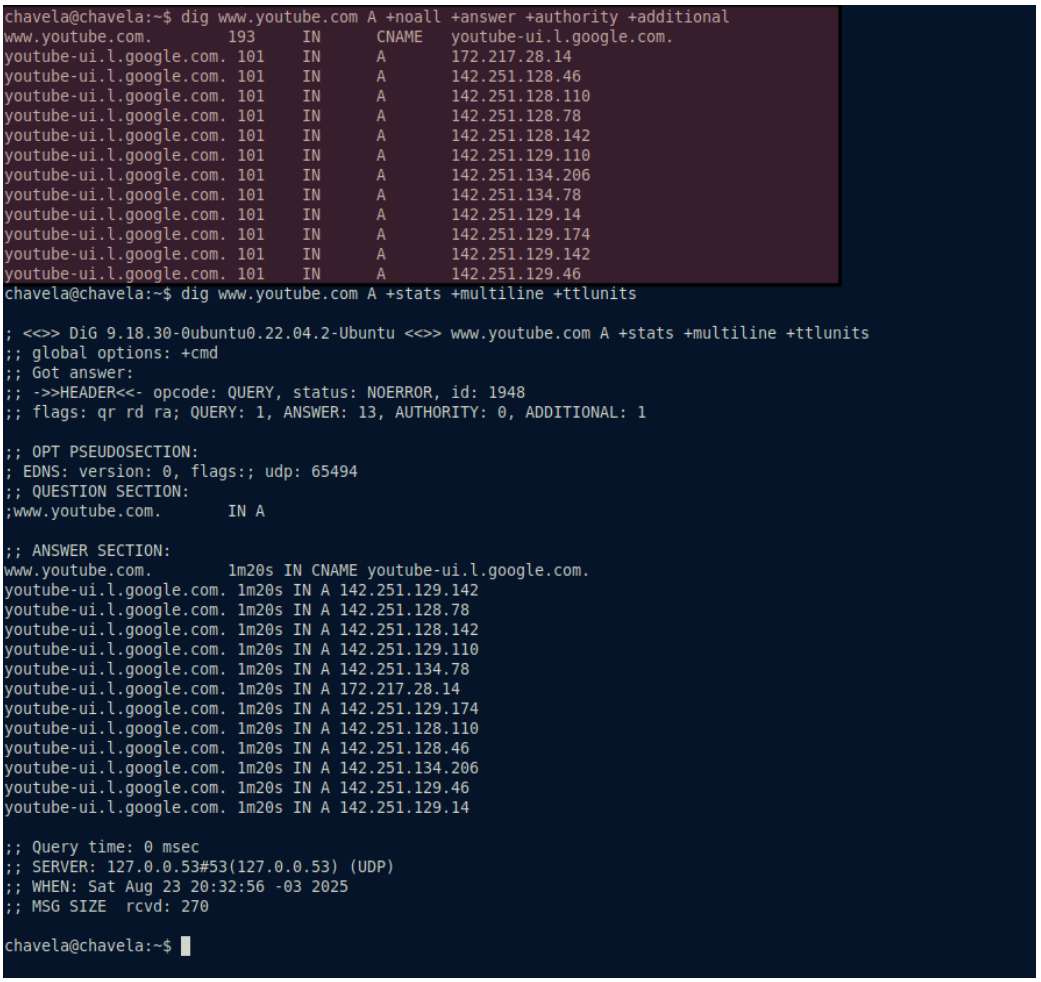


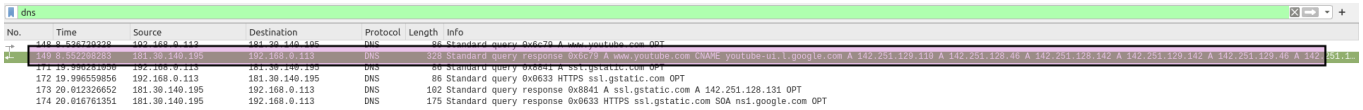
Figura 08: Captura con +noall +answer +authority +additional

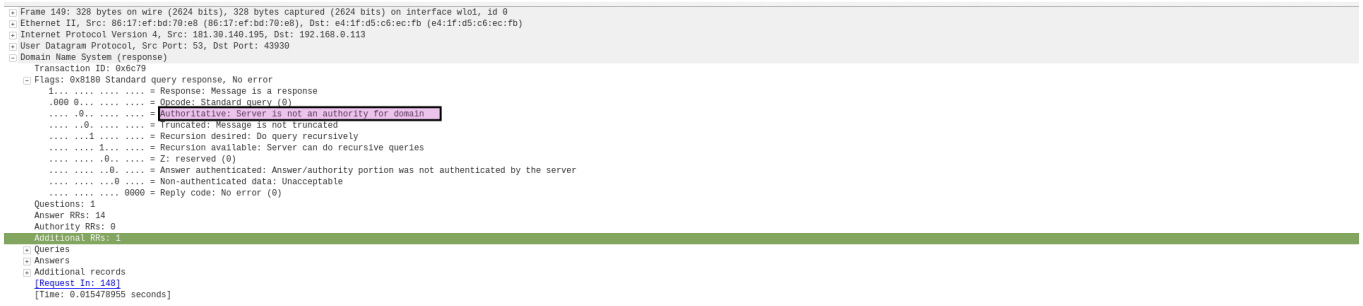
Solo muestra las secciones **ANSWER / AUTHORITY / ADDITIONAL**, Se puede ver que, aparecen los servidores que tienen la autoridad sobre el dominio youtube.com Es decir, ahí se listan cuáles son los **nameservers oficiales de Google** que se encargan de responder por ese dominio.
También, gracias a la opción ***+additional,*** se muestran las direcciones IP de esos **servidores autoritativos**.

Usando otro comando ***+stats +multiline +ttlunits*** y el ***wireshark:***

```
chavela@chavela:~$ dig www.youtube.com A +noall +answer +authority +additional
www.youtube.com.        193     IN      CNAME   youtube-ui.l.google.com.
youtube-ui.l.google.com. 101    IN      A       172.217.28.14
youtube-ui.l.google.com. 101    IN      A       142.251.128.46
youtube-ui.l.google.com. 101    IN      A       142.251.128.110
youtube-ui.l.google.com. 101    IN      A       142.251.128.78
youtube-ui.l.google.com. 101    IN      A       142.251.128.142
youtube-ui.l.google.com. 101    IN      A       142.251.129.110
youtube-ui.l.google.com. 101    IN      A       142.251.134.206
youtube-ui.l.google.com. 101    IN      A       142.251.134.78
youtube-ui.l.google.com. 101    IN      A       142.251.129.14
youtube-ui.l.google.com. 101    IN      A       142.251.129.174
youtube-ui.l.google.com. 101    IN      A       142.251.129.142
youtube-ui.l.google.com. 101    IN      A       142.251.129.46
chavela@chavela:~$ dig www.youtube.com A +stats +multiline +ttlunits

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> www.youtube.com A +stats +multiline +ttlunits
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1948
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.youtube.com.       IN A

;; ANSWER SECTION:
www.youtube.com.        1m20s IN CNAME youtube-ui.l.google.com.
youtube-ui.l.google.com. 1m20s IN A 142.251.129.142
youtube-ui.l.google.com. 1m20s IN A 142.251.128.78
youtube-ui.l.google.com. 1m20s IN A 142.251.128.142
youtube-ui.l.google.com. 1m20s IN A 142.251.129.110
youtube-ui.l.google.com. 1m20s IN A 142.251.134.78
youtube-ui.l.google.com. 1m20s IN A 172.217.28.14
youtube-ui.l.google.com. 1m20s IN A 142.251.129.174
youtube-ui.l.google.com. 1m20s IN A 142.251.128.110
youtube-ui.l.google.com. 1m20s IN A 142.251.128.46
youtube-ui.l.google.com. 1m20s IN A 142.251.134.206
youtube-ui.l.google.com. 1m20s IN A 142.251.129.46
youtube-ui.l.google.com. 1m20s IN A 142.251.129.14

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sat Aug 23 20:32:56 -03 2025
;; MSG SIZE  rcvd: 270

chavela@chavela:~$
```

Figura 09: Captura con +stats +multiline +ttlunits





En las consultas realizadas se observa que las respuestas obtenidas son **no autoritativas**, ya que el bit AA (Authoritative Answer) se encuentra en 0.

Esto ocurre porque el servidor que respondió no es dueño de la zona youtube.com, sino que actúa como servidor recursivo (en este caso el 127.0.0.53 del sistema o el resolver al que reenvía las consultas).
Una respuesta autoritativa solo se obtiene cuando la consulta se dirige directamente a un servidor autoritativo del dominio, como por ejemplo **ns1.google.com** visto anteriormente.