

## Actividad 2: Protocolos y DNS

1. Analizar los paquetes que se transmiten al conectarse a un servidor web.

Utilizando el sitio web local desarrollado en la Actividad 1, realizar un informe con los encabezados y paquetes enviados y recibidos por el navegador web.

Identificar los datos del cliente y del servidor (Sistema Operativo, IP y todos los datos que pueda obtener). ¿Qué tanto confiaría en estos datos transmitidos? ¿Cuáles se pueden modificar y cuáles no?

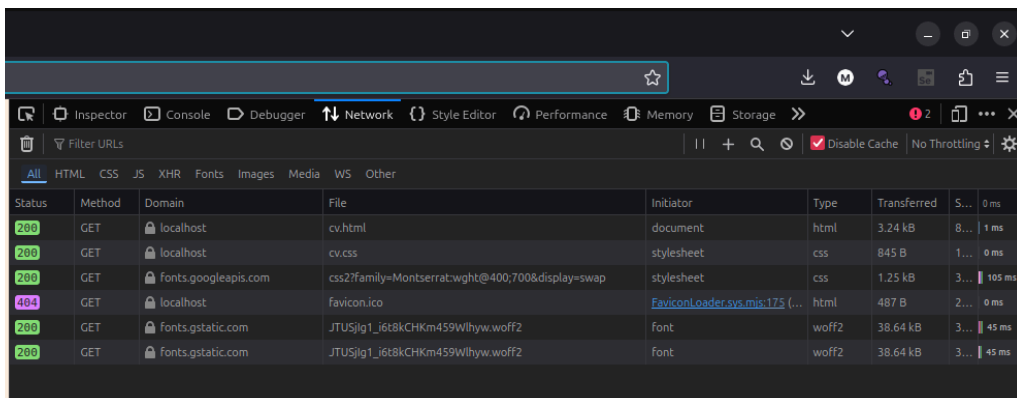
2. Analizar la resolución DNS

Utilizando la línea de comandos resolver los siguientes puntos:

- a. Determine la dirección IP del servidor `www.caece.edu.ar`
- b. Averigüe qué servidor tiene asignada la dirección IP `69.171.230.68`
- c. Averigüe los servidores de correo de GMAIL
- d. Informar los servidores de nombre (ns) del dominio `w3c.org`
- e. Si hubiese algún problema con el DNS de CAECE y quisiera enviar un email a alguna cuenta `@caece.edu.ar`, ¿A qué IP debería enviar esos correos electrónicos?
- f. ¿Cuánto tiempo almacenará en cache su DNS local la dirección IP de `php.net`? Pregunte varias veces a su DNS local por esta dirección. ¿Qué observa en el TTL del registro de recurso?
- g. ¿Cómo podemos saber si un servidor está usando balanceo de carga? Mencione algún ejemplo.

### Desarrollo

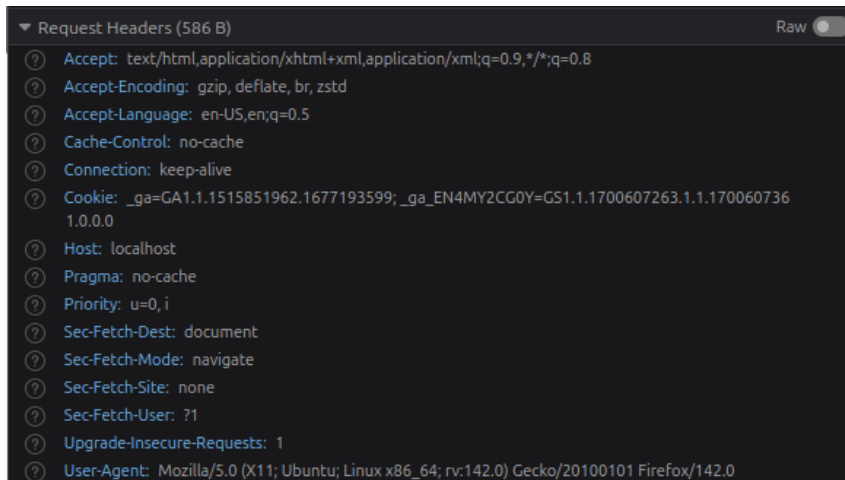
1. Inspeccionando la página y entrando a la sección de Network podemos ver las peticiones que realizó el navegador. En el caso de mi página son las siguientes:



Status	Method	Domain	File	Initiator	Type	Transferred	S...	0 ms
200	GET	localhost	cv.html	document	html	3.24 kB	8...	1 ms
200	GET	localhost	cv.css	stylesheet	css	845 B	1...	0 ms
200	GET	fonts.googleapis.com	css2?family=Montserrat:wght@400;700&display=swap	stylesheet	css	1.25 kB	3...	105 ms
404	GET	localhost	favicon.ico	FaviconLoader.sys.mjs:175 (...)	html	487 B	2...	0 ms
200	GET	fonts.gstatic.com	JTUSjlg1_i6t8kCHKm459Wlhyw.woff2	font	woff2	38.64 kB	3...	45 ms
200	GET	fonts.gstatic.com	JTUSjlg1_i6t8kCHKm459Wlhyw.woff2	font	woff2	38.64 kB	3...	45 ms

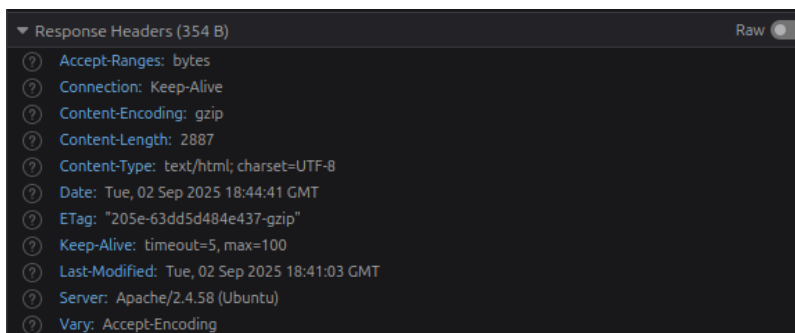
La primera petición que aparece es la del archivo “cv.html” a través del método GET. Como mi archivo está en el servidor y no tiene ningún problema responde con el código de estado 200 (ok). El tipo de la respuesta es html y proviene del dominio localhost.

El encabezado de la petición es el siguiente:



Podemos ver datos como el lenguaje, el host (localhost), la prioridad, el tipo de conexión, entre otros campos.

El encabezado de la respuesta es el siguiente:



Podemos ver la longitud de la respuesta, el tipo (texto/html), la fecha, el servidor (Apache), entre otros campos.

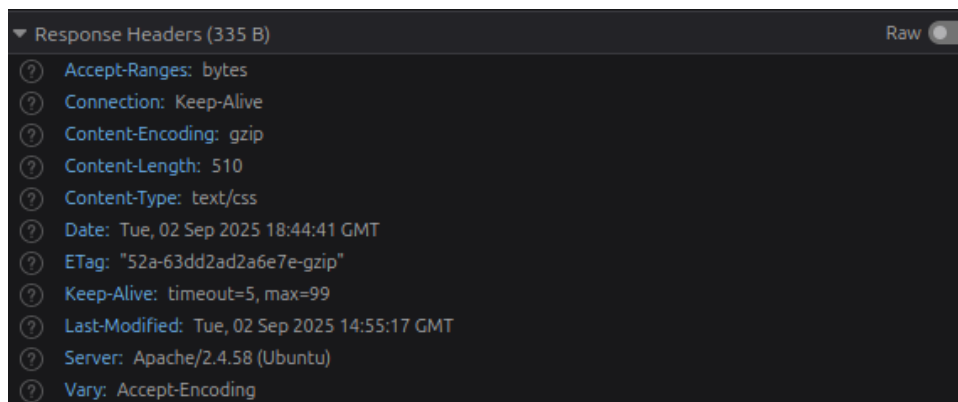
La segunda petición es la de los estilos. En la cabecera de mi archivo html tengo un link a un archivo llamado “cv.css”, por lo tanto, el navegador realiza la petición del mismo a través de del método GET al localhost.

El encabezado de la petición es:



En este caso, a diferencia de la petición anterior, tenemos un campo llamado “referer” que indica la dirección del recurso que realizó la petición, en este caso el archivo cv.html.

El encabezado de la respuesta es:



Los campos son los mismos que en la petición anterior nada más varían la longitud de la respuesta y el tipo, ahora es text/css.

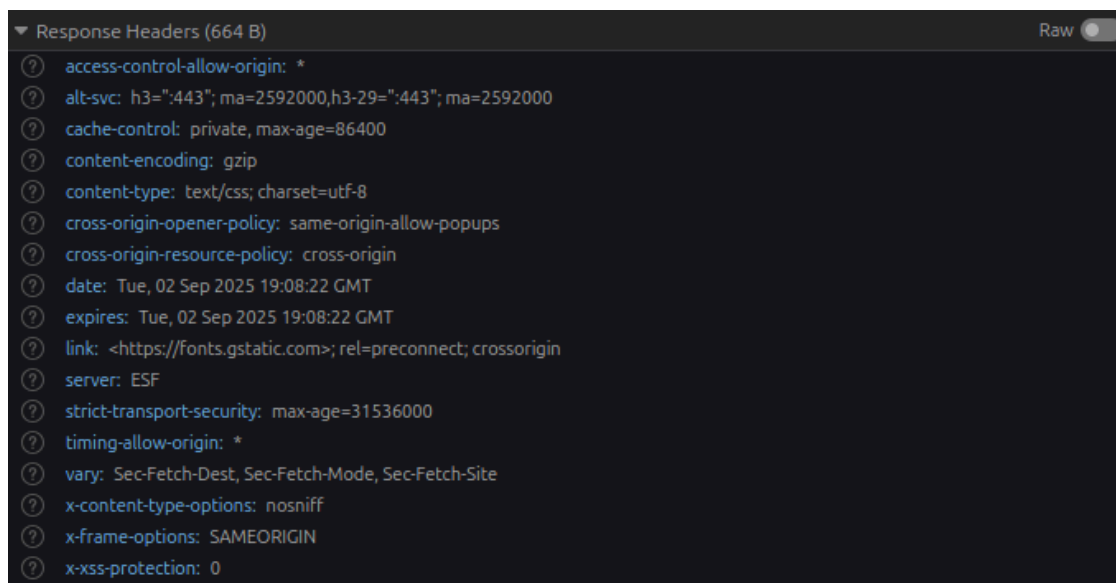
La tercera petición que se realiza es la de la fuente que utilicé: Montserrat. Opté por no descargarla e incluir un link en el head de mi archivo html, es por eso que el navegador realiza la petición. Dejando el cursor sobre el dominio nos permite ver la IP destino de font.googleapis.com: 172.217.28.10. También vemos que el servicio está en el puerto 443.

El encabezado de la petición es:



Al igual que en la petición anterior, el navegador realiza la petición a fonts.googleapis.com porque utilizo una fuente externa. Podemos observar que en este caso el campo referer solo dice <http://localhost/> y no <http://localhost/cv.html> como en el caso anterior. Investigando encontré que el navegador recorta el origen cuando hace peticiones fuera de localhost para más seguridad.

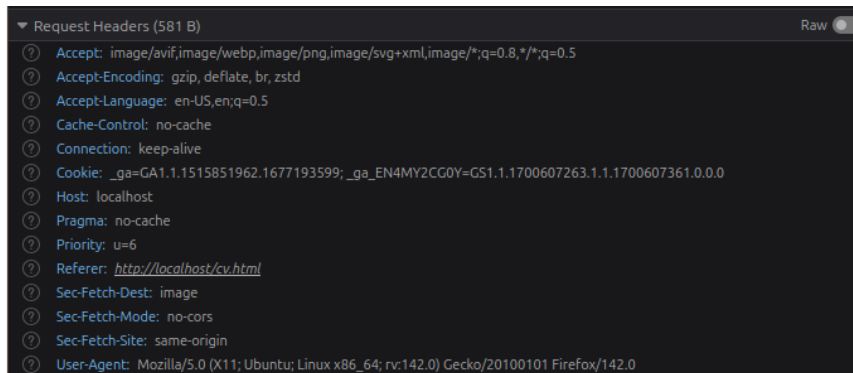
El encabezado de la respuesta es:



Los campos más diferentes a los que venía viendo y me llamaron la atención son: access-control-allow-origin, en este caso al tener un asterisco nos indica que permite el acceso desde cualquier página, link <https://fonts.gstatic.com>; rel=preconnect; crossorigin, que le sugiere al navegador que realice una “preconexión” antes de necesitarlo y strict-transport-security: max-age=31536000, que le indica al navegador que tiene que usar siempre HTTPS con este dominio y expira en 1 año.

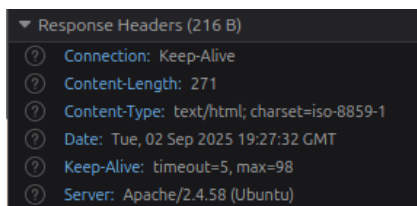
La cuarta petición que se realiza, con el método GET, es al dominio localhost y del archivo favicon.ico. En este caso la respuesta tiene un código de 404 (not found) ya que no definí ningún ícono para mi página.

El encabezado de la petición es:



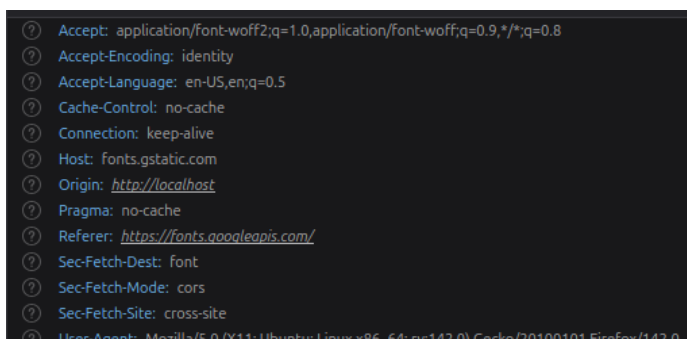
Podemos ver nuevamente que el campo referer indica la página local. En este caso se esperaba una imagen con el formato avif/webp/png/svg, lo indica el campo Accept.

El encabezado de la respuesta es:



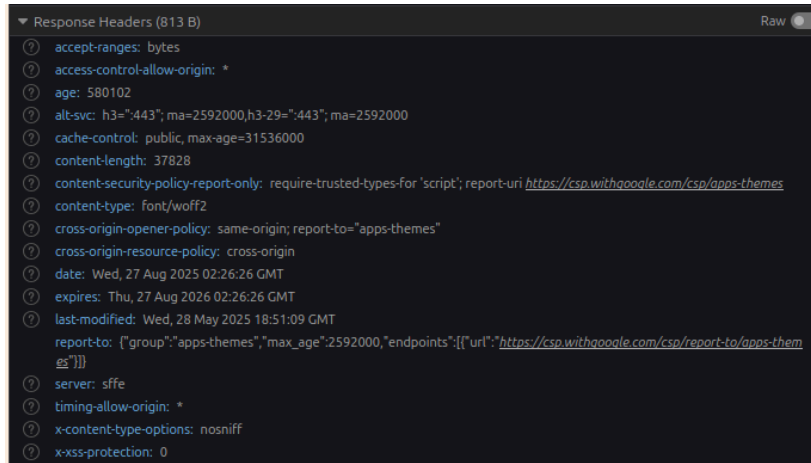
Por último, las peticiones 5 y 6 son iguales y hacen referencia a los archivos que contienen las fuentes en sí. Las peticiones se hacen al dominio fonts.gstatic.com, que tiene la IP 142.251.128.35. Aparece duplicado porque utilicé pesos distintos entonces se requieren dos fuentes (aunque pertenezcan al mismo origen).

Los encabezados de petición en ambos casos son así:



Podemos observar que espera un archivo en formato woff/woff2, como es externo se declara el origen sólo como localhost (sin la ruta completa).

Los encabezados de respuesta en ambos casos son:



Considero que los datos que vienen de grandes compañías como google en este caso son confiables, todo lo relacionado con el cliente es fácilmente modificable y por ende no es seguro. Algunos campos que considero que se pueden modificar son: el User-Agent, el Accept / Accept-Language, el Referer, Origin. En todos los casos utilizando una aplicación como Postman se podrían modificar los campos o incluso utilizando Javascript.

En cambio, algunos de los campos que no se pueden modificar son: el estado de la respuesta, el content-type, el content-length, el server, el Access-Control-Allow-Origin.

2.

a.

```
maga@maga-desktop: ~  
maga@maga-desktop:~$ dig www.caece.edu.ar  
  
; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> www.caece.edu.ar  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 159  
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 65494  
;; QUESTION SECTION:  
;www.caece.edu.ar.          IN      A  
  
;; ANSWER SECTION:  
www.caece.edu.ar.          60      IN      CNAME   190.210.98.5.iplan.toservers.com.  
190.210.98.5.iplan.toservers.com. 600 IN A      190.210.98.5  
  
;; Query time: 417 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)  
;; WHEN: Wed Sep 03 11:21:08 -03 2025  
;; MSG SIZE rcvd: 107
```

Utilizando la herramienta dig con el nombre del servidor obtenemos información dentro de la cual podemos ver que la IP es 190.210.98.5.

b.

```
maga@maga-desktop:~$ dig -x 69.171.230.68

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> -x 69.171.230.68
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 264
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;68.230.171.69.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
68.230.171.69.in-addr.arpa. 3600 IN      PTR      fwdproxy-cco-068.fbsv.net.

;; Query time: 840 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Sep 03 11:26:54 -03 2025
;; MSG SIZE rcvd: 94
```

Para conseguir el nombre del servidor que tiene asignada esa IP tenemos que realizar la misma consulta pero utilizando la opción `-x` para hacer la resolución inversa. En este caso obtuvimos el server con el nombre: `fwdproxy-cco-068.fbsv.net`

c.

```
maga@maga-desktop:~$ dig gmail.com MX

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> gmail.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59904
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;gmail.com.                IN      MX

;; ANSWER SECTION:
gmail.com.      1008    IN      MX      20 alt2.gmail-smtp-in.l.google.com.
gmail.com.      1008    IN      MX      5  gmail-smtp-in.l.google.com.
gmail.com.      1008    IN      MX      40 alt4.gmail-smtp-in.l.google.com.
gmail.com.      1008    IN      MX      30 alt3.gmail-smtp-in.l.google.com.
gmail.com.      1008    IN      MX      10 alt1.gmail-smtp-in.l.google.com.

;; Query time: 10 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Sep 03 14:12:38 -03 2025
;; MSG SIZE rcvd: 161
```

Podemos ver que gmail.com tiene 5 servidores de mail.

d.

```
maga@maga-desktop:~$ dig w3c.org NS

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> w3c.org NS
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 24396
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;w3c.org.                IN      NS

;; ANSWER SECTION:
w3c.org.                10800   IN      NS      ns-139-c.gandi.net.
w3c.org.                10800   IN      NS      ns-225-a.gandi.net.
w3c.org.                10800   IN      NS      ns-206-b.gandi.net.

;; Query time: 136 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Sep 03 14:15:57 -03 2025
;; MSG SIZE rcvd: 114
```

Podemos ver que los servidores de nombre son: ns-139-c.gandi.net, ns-225-a.gandi.net y ns-206-b.gandi.net

e.

```
maga@maga-desktop:~$ dig caece.edu.ar MX

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> caece.edu.ar MX
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 56435
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;caece.edu.ar.          IN      MX

;; ANSWER SECTION:
caece.edu.ar.          300     IN      MX      10 aspmx3.googlemail.com.
caece.edu.ar.          300     IN      MX      10 aspmx4.googlemail.com.
caece.edu.ar.          300     IN      MX      10 aspmx5.googlemail.com.
caece.edu.ar.          300     IN      MX      5 alt1.aspmx.l.google.com.
caece.edu.ar.          300     IN      MX      5 alt2.aspmx.l.google.com.
caece.edu.ar.          300     IN      MX      1 aspmx.l.google.com.
caece.edu.ar.          300     IN      MX      10 aspmx2.googlemail.com.

;; Query time: 9 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Sep 03 14:26:17 -03 2025
;; MSG SIZE rcvd: 220
```



En caso de que el servidor DNS de CAECE esté caído y queramos mandar un mail, lo haríamos a alguno de sus servidores de mail, por ejemplo el que tiene el nombre de dominio aspmx4.googlemail.com. Para conseguir la IP realizamos la siguiente consulta:

```
maga@maga-desktop:~$ dig aspmx3.googlemail.com

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> aspmx3.googlemail.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7168
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 65494
;; QUESTION SECTION:
;aspmx3.googlemail.com.      IN      A

;; ANSWER SECTION:
aspmx3.googlemail.com.  285     IN      A      142.250.102.26

;; Query time: 1 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Wed Sep 03 14:39:19 -03 2025
;; MSG SIZE rcvd: 66
```

Lo que nos da el número de IP: 142.250.102.26

- f. Realizando una consulta al sitio php.net vemos que el TTL es de 300s, este campo indica también cuánto tiempo va a quedar guardada la IP en el caché local. Esto lo podemos comprobar porque si seguimos haciendo la consulta el TTL cada vez es menor:

```
maga@maga-desktop:~$ dig php.net TTL

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> php.net TTL
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4028
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 65494
;; QUESTION SECTION:
;php.net.                  IN      A

;; ANSWER SECTION:
php.net.                  300     IN      A      185.85.0.29
```

```
maga@maga-desktop:~$ dig php.net

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> php.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44827
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;php.net.                IN      A

;; ANSWER SECTION:
php.net.                 223     IN      A      185.85.0.29
```

- g. Una forma de determinar si un servidor tiene balanceo de carga es buscando si para el mismo nombre de dominio vemos que hay varias IPs, es decir, varios registros del tipo A.

Por ejemplo, si consultamos los registros A de youtube obtenemos lo siguiente:

```
maga@maga-desktop:~$ dig www.youtube.com

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> www.youtube.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49797
;; flags: qr rd ra; QUERY: 1, ANSWER: 17, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.youtube.com.        115     IN      CNAME   youtube-ui.l.google.com.
youtube-ui.l.google.com. 115     IN      A       142.251.129.14
youtube-ui.l.google.com. 115     IN      A       142.251.129.110
youtube-ui.l.google.com. 115     IN      A       142.251.128.78
youtube-ui.l.google.com. 115     IN      A       142.251.134.206
youtube-ui.l.google.com. 115     IN      A       142.251.128.110
youtube-ui.l.google.com. 115     IN      A       142.251.128.46
youtube-ui.l.google.com. 115     IN      A       142.251.129.174
youtube-ui.l.google.com. 115     IN      A       172.217.173.238
youtube-ui.l.google.com. 115     IN      A       142.250.79.110
youtube-ui.l.google.com. 115     IN      A       142.251.128.142
youtube-ui.l.google.com. 115     IN      A       142.251.128.142
```

Otro ejemplo que se me ocurrió consultar es el dominio de Paulina Cocina, y descubrí que tiene varias IPs también:

```
maga@maga-desktop:~$ dig www.paulinacocina.net +short
172.67.70.222
104.26.14.209
104.26.15.209
```