TIPOS DE CONSULTA EN UN SERVICIO DE DNS

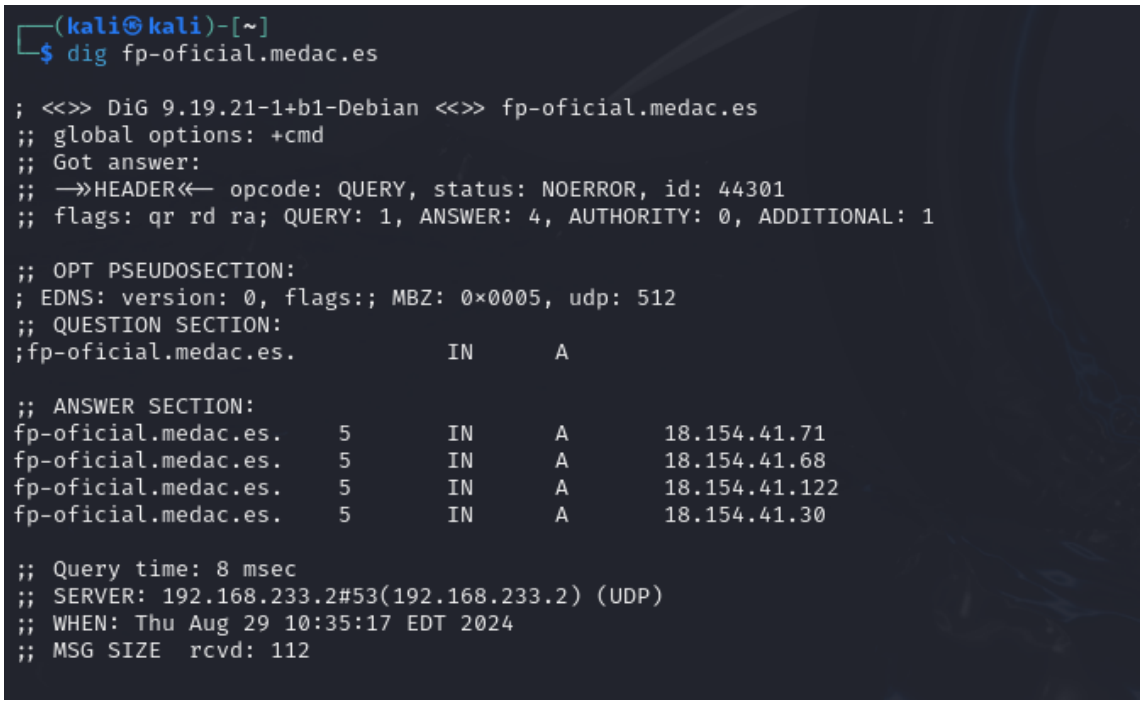
Ejecuta una máquina virtual de Kali Linux

1. Consulta Recursiva

Supón que deseas acceder al sitio web **https://fp-oficial.medac.es/ .**Tu ordenador hace una consulta recursiva al servidor DNS.

Ejemplo:

- Tu navegador envía la consulta recursiva a un servidor DNS recursor (por ejemplo, el servidor DNS de tu ISP).
- Si el servidor recursor no tiene la respuesta en su caché, consultará con los servidores raíz, luego con los servidores de nivel superior (TLD) .com, y finalmente con el servidor autoritativo de example.com.
- El servidor recursor obtiene la dirección IP y la devuelve a tu navegador.



Análisis del Resultado

Respuesta recibida:

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44301
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
```

- status: NOERROR: Indica que la consulta fue exitosa y no hubo errores.
- QUERY: 1: Una consulta fue realizada.
- ANSWER: 4: Se recibieron cuatro respuestas (cuatro direcciones IP en la sección de respuestas).
- AUTHORITY: 0: No se devolvieron registros de autoridad.
- ADDITIONAL: 1: Hay un registro adicional (generalmente relacionado con EDNS).

Sección de la Pregunta

```
;; QUESTION SECTION:
;fp-oficial.medac.es.           IN      A
```

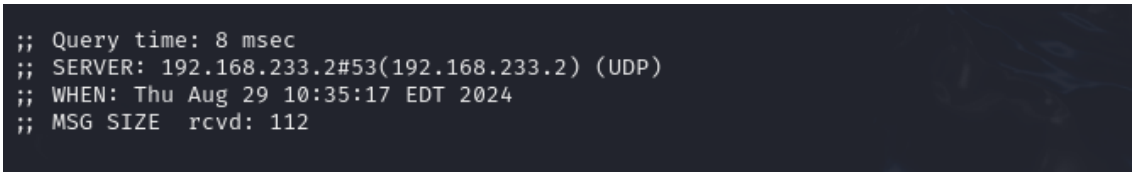
- Esta es la pregunta que hiciste: buscaste un registro A para el dominio fp-oficial.medac.es

Sección de Respuesta

```
;; ANSWER SECTION:
fp-oficial.medac.es.    5       IN      A       18.154.41.71
fp-oficial.medac.es.    5       IN      A       18.154.41.68
fp-oficial.medac.es.    5       IN      A       18.154.41.122
fp-oficial.medac.es.    5       IN      A       18.154.41.30
```

- Esta sección muestra las direcciones IP asociadas con el dominio fp-oficial.medac.es.
- 18.154.41.71, 18.154.41.68, 18.154.41.122, 18.154.41.30: Son las direcciones IP que el servidor DNS devolvió para el dominio.
- TTL (Time To Live): 5: Indica que esta respuesta puede almacenarse en caché durante 5 segundos antes de necesitar ser actualizada.

Tiempo de Consulta y Servidor



- Query time: 8 msec: El tiempo que tomó obtener la respuesta fue de 8 milisegundos.
- SERVER: El servidor DNS que respondió a la consulta es 192.168.233.2.
- MSG SIZE rcvd: 112: El tamaño del mensaje de respuesta fue de 112 bytes.

2. Consulta Iterativa

Imagina que tu ordenador actúa como un cliente DNS (por ejemplo, en una configuración avanzada o durante el desarrollo). Realizas una consulta iterativa directamente a un servidor DNS.

Ejemplo:

Envías una consulta iterativa al servidor raíz.

El servidor raíz no tiene la dirección IP exacta de www.example.com, pero te redirige al servidor TLD .com.

Luego consultas el servidor TLD, que te redirige al servidor autoritativo de example.com.

Finalmente, consultas el servidor autoritativo que te da la dirección IP del dominio.

```
┌──(kali㉿kali)-[~]
└─$ dig 99.84.66.55 medac.es

; <<>> DiG 9.19.21-1+b1-Debian <<>> 99.84.66.55 medac.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 41883
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;99.84.66.55.                   IN      A

;; AUTHORITY SECTION:
.                       5       IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2024082900 1800 900 6048
00 86400

;; Query time: 27 msec
;; SERVER: 192.168.233.2#53(192.168.233.2) (UDP)
;; WHEN: Thu Aug 29 10:51:56 EDT 2024
;; MSG SIZE  rcvd: 115

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19164
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;medac.es.                      IN      A

;; ANSWER SECTION:
medac.es.               5       IN      A       18.154.41.71
medac.es.               5       IN      A       18.154.41.30
medac.es.               5       IN      A       18.154.41.68
medac.es.               5       IN      A       18.154.41.122

;; Query time: 75 msec
;; SERVER: 192.168.233.2#53(192.168.233.2) (UDP)
;; WHEN: Thu Aug 29 10:51:56 EDT 2024
;; MSG SIZE  rcvd: 101
```

Análisis del Resultado

Respuesta recibida: (dig 99.84.66.55 medac.es)

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 41883
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;99.84.66.55.                   IN      A
```

- status: NXDOMAIN: Indica que no se encontró un nombre de dominio llamado 99.84.66.55, lo cual tiene sentido porque es una dirección IP y no un nombre de dominio válido.
- QUESTION SECTION: La consulta preguntaba por 99.84.66.55 como un registro A, pero esto no es correcto porque una dirección IP no puede tener un registro A.

Segunda Consulta (medac.es)

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19164
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;medac.es.                      IN      A

;; ANSWER SECTION:
medac.es.               5       IN      A       18.154.41.71
medac.es.               5       IN      A       18.154.41.30
medac.es.               5       IN      A       18.154.41.68
medac.es.               5       IN      A       18.154.41.122
```

- status: NOERROR: Indica que la consulta para medac.es se resolvió correctamente.
- ANSWER SECTION: Esta sección muestra las cuatro direcciones IP asociadas con el dominio medac.es, que son las mismas que viste en consultas anteriores.

Consulta Inversa (Reverse DNS Lookup)

Supongamos que tienes la dirección IP 18.154.41.71 y quieres saber a qué nombre de dominio está asociada.

Ejemplo:

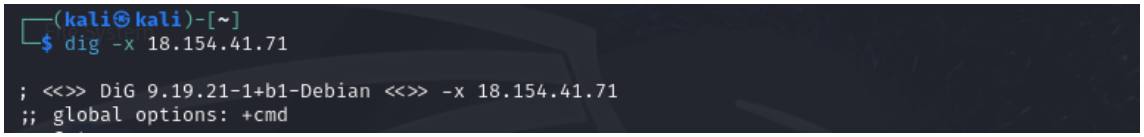
Envías una consulta inversa para 18.154.41.71 El servidor DNS consulta la zona inversa correspondiente (1.41.154.18.in-addr.arpa).

El servidor DNS devuelve el nombre de dominio asociado.

```
┌──(kali㉿kali)-[~]
└─$ dig -x 18.154.41.71

; <<>> DiG 9.19.21-1+b1-Debian <<>> -x 18.154.41.71
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51093
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 512
;; QUESTION SECTION:
;71.41.154.18.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
71.41.154.18.in-addr.arpa. 5    IN      PTR     server-18-154-41-71.mad53.r.cloudfront.net.

;; Query time: 163 msec
;; SERVER: 192.168.233.2#53(192.168.233.2) (UDP)
;; WHEN: Thu Aug 29 11:01:22 EDT 2024
;; MSG SIZE  rcvd: 110
```

Análisis del Resultado

Respuesta recibida: (dig -x 18.154.41.71)

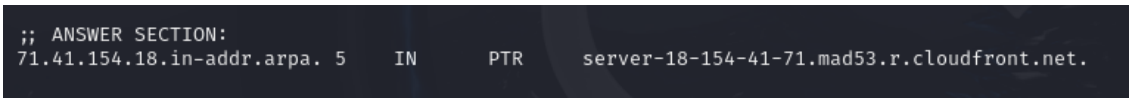


- Este es el comando que ejecutaste: dig -x 18.154.41.71, donde -x indica que se trata de una consulta inversa (Reverse DNS Lookup).

Respuesta Recibida

- status: NOERROR: Significa que la consulta fue exitosa y no hubo errores.
- ANSWER: 1: Se recibió una respuesta en la sección de respuesta, lo cual indica que se encontró un nombre de dominio asociado con la IP.

Sección de la Pregunta



- 71.41.154.18.in-addr.arpa.: Este es el nombre invertido de la dirección IP que estás investigando.
- 5: Es el TTL (Time To Live), que indica cuánto tiempo puede ser almacenada en caché esta respuesta.
- PTR: Este es el tipo de registro que mapea una dirección IP a un nombre de dominio.
- server-18-154-41-71.mad53.r.cloudfront.net.: Este es el nombre de dominio asociado con la dirección IP 18.154.41.71. En este caso, pertenece a un servidor de Amazon CloudFront, un servicio de distribución de contenido (CDN).

Tiempo de Consulta y Servidor

```
;; Query time: 163 msec
;; SERVER: 192.168.233.2#53(192.168.233.2) (UDP)
;; WHEN: Thu Aug 29 11:01:22 EDT 2024
;; MSG SIZE  rcvd: 110
```

- Query time: 163 msec: El tiempo que tomó para resolver la consulta fue de 163 milisegundos.
- SERVER: 192.168.233.2: El servidor DNS que resolvió la consulta.
- MSG SIZE rcvd: 110: El tamaño del mensaje de respuesta fue de 110 bytes.

Consulta No Recursiva

Si configuras una consulta no recursiva, tu servidor DNS no buscará más allá de su caché.

Ejemplo:

Envías una consulta no recursiva para www.medac.es

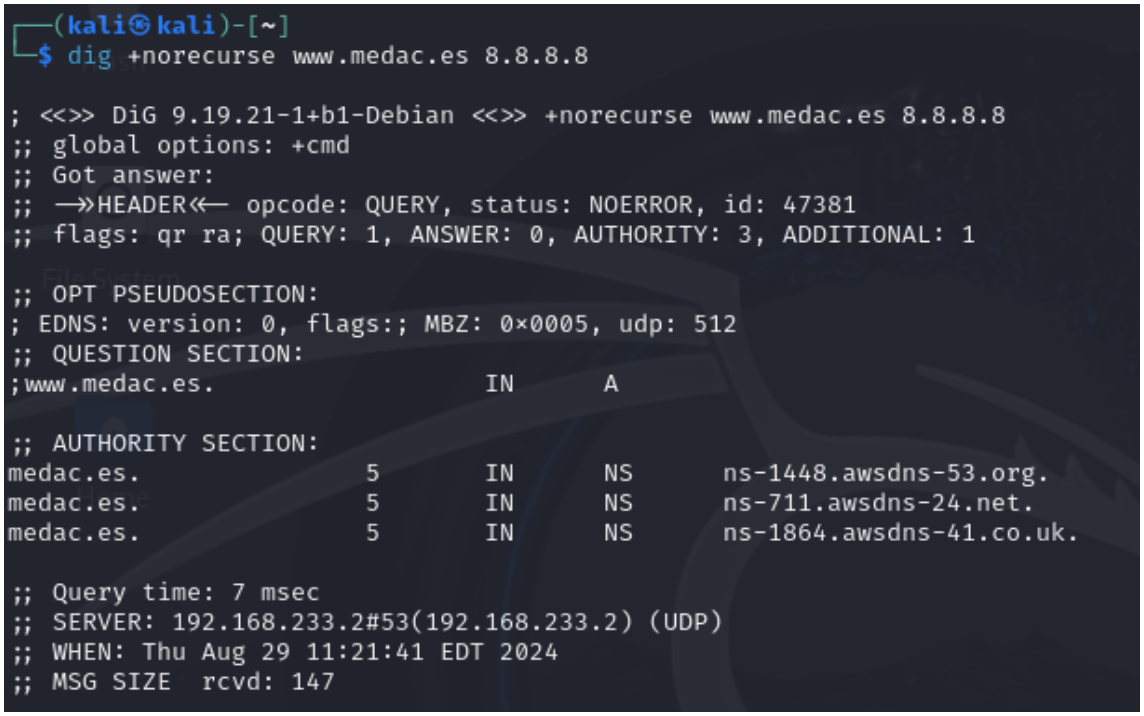
El servidor DNS responde únicamente con la información en su caché.

Si no tiene la información, devuelve un error o una respuesta parcial.

```
┌──(kali㉿kali)-[~]
└─$ dig +norecurse www.medac.es 8.8.8.8

; <<>> DiG 9.19.21-1+b1-Debian <<>> +norecurse www.medac.es 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47381
;; flags: qr ra; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 512
;; QUESTION SECTION:
;www.medac.es.                  IN      A

;; AUTHORITY SECTION:
medac.es.               5       IN      NS      ns-1448.awsdns-53.org.
medac.es.               5       IN      NS      ns-711.awsdns-24.net.
medac.es.               5       IN      NS      ns-1864.awsdns-41.co.uk.

;; Query time: 7 msec
;; SERVER: 192.168.233.2#53(192.168.233.2) (UDP)
;; WHEN: Thu Aug 29 11:21:41 EDT 2024
;; MSG SIZE  rcvd: 147

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 14751
;; flags: qr ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 512
;; QUESTION SECTION:
;8.8.8.8.                       IN      A

;; AUTHORITY SECTION:
.                       5       IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2024082900 1800 900 6048
00 86400

;; Query time: 3 msec
;; SERVER: 192.168.233.2#53(192.168.233.2) (UDP)
;; WHEN: Thu Aug 29 11:21:41 EDT 2024
;; MSG SIZE  rcvd: 111
```

Análisis del Resultado

Respuesta recibida: (dig +norecurse www.medac.es 8.8.8.8)



- Comando: dig +norecurse www.medac.es 8.8.8.8 consulta el servidor DNS de Google (8.8.8.8) para resolver el nombre de dominio www.medac.es sin permitir la resolución recursiva (+norecurse).
- HEADER: status: NOERROR indica que la consulta fue procesada correctamente sin errores.
- ANSWER: No hay respuesta directa en la sección de respuesta (ANSWER: 0), lo que significa que el servidor DNS de Google no devolvió una dirección IP para www.medac.es en esta consulta.
- AUTHORITY: La consulta devuelve una lista de servidores DNS autoritativos (NS) para el dominio medac.es. Esto significa que para obtener la respuesta, el servidor te indica que debes consultar uno de estos servidores autoritativos: ns-1448.awsdns-53.org, ns-711.awsdns-24.net, ns-1864.awsdns-41.co.uk.

Segunda respuesta

```
;; Got answer:
;; →»HEADER«← opcode: QUERY, status: NXDOMAIN, id: 14751
;; flags: qr ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 512
;; QUESTION SECTION:
;8.8.8.8.                       IN      A

;; AUTHORITY SECTION:
.                       5       IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2024082900 1800 900 6048
00 86400

;; Query time: 3 msec
;; SERVER: 192.168.233.2#53(192.168.233.2) (UDP)
;; WHEN: Thu Aug 29 11:21:41 EDT 2024
;; MSG SIZE  rcvd: 111
```

- HEADER: status: NXDOMAIN indica que el dominio consultado no existe. Aquí parece que hubo una consulta errónea intentando resolver 8.8.8.8 como un dominio, lo cual no es correcto ya que 8.8.8.8 es una dirección IP.

- AUTHORITY: Se muestra el servidor autoritativo para la raíz (.), lo que indica que el sistema DNS no pudo encontrar ningún dominio asociado con la consulta.