

# Trabajo práctico dig

---

- Fecha de entrega: 7 de septiembre de 2024
- Materia: Redes (TA048)
- Curso: 02 Alvalrez Hamelin
- Nombre completo: Máximo Gismondi
- Padrón: 110119

## Consigna

Usar el comando "dig" con las opciones iterativa, autorizada y verborrágica capturando por la pantalla de la terminal y también mediante "Wireshark". Subirlo al Campus un informe en formato PDF.

## Introducción

En este trabajo práctico, nos vamos a centrar en la utilidad **dig** (Domain Information Groper). Esta utilidad permite realizar consultas a servidores DNS, proporcionando a los administradores de redes la capacidad de depurar la resolución de nombres de dominio y analizar el funcionamiento del protocolo DNS en situaciones específicas.

En esta ocasión, utilizaremos **dig** para consultar el servidor DNS asociado a **developer.mozilla.org**, un sitio que ofrece guías, referencias y herramientas principalmente para desarrolladores web. Analizaremos la traza de consultas, los servidores que responden, y otros detalles no solo a través de la línea de comandos, sino también con Wireshark, una aplicación que permite capturar y analizar cualquier tipo de paquete de red.

## Comando

Antes de empezar a enviar consultas a través de **dig**, vamos a entender como funciona el comando y la estructura del mismo. **dig** tiene la siguiente estructura:

```
dig [@server] [name] [type] [+opciones]
```

Donde:

- **@server**: Especifica el servidor DNS al que se le enviará la consulta. Si no se especifica, se utilizará el servidor DNS configurado en el sistema.
- **name**: Es el nombre de dominio que se desea consultar.
- **type**: Especifica el tipo de registro que se desea consultar. Si no se especifica, se asume que es un registro de tipo **A**.
- **+opciones**: Son opciones adicionales que se pueden utilizar para modificar el comportamiento de la consulta.

## Opciones

Para hacer una consulta iterativa, autorizada y verborrágica debemos utilizar las siguientes opciones:

- **+trace**: Realiza una consulta iterativa, mostrando la traza de consultas desde el servidor raíz hasta el servidor autoritativo.
- **+stats**: Muestra estadísticas de la consulta realizada.
- **+multiline**: Muestra la respuesta en formato de múltiples líneas.

No es necesario utilizar otras opciones ya que al usar **+trace** siempre se realiza una consulta iterativa y autorizada. Y la información adicional que se puede obtener con **+stats** y **+multiline** es suficiente para analizar la consulta ya que el modo verborrágico está activado por defecto.

## Servidor DNS

El servidor DNS que vamos a utilizar para realizar la consulta es **8.8.8.8**, el servidor DNS público de Google, que es muy utilizado por su velocidad y disponibilidad.

## Tipo de registro

El tipo de registro que vamos a consultar es **A**, que es el tipo de registro que nos permitirá obtener la dirección IP asociada al nombre de dominio y acceder al sitio web.

## Comando completo

Una vez que entendemos la estructura y las opciones que vamos a utilizar, el comando completo para realizar la consulta es el siguiente:

```
dig @8.8.8.8 developer.mozilla.org +trace +stats +multiline
```

## Captura por terminal

### Salida

Ejecutamos el comando en la terminal y redirigimos la salida a un archivo de texto para poder analizarla con más detalle. En el archivo **salida.txt** se encuentra la salida completa de la consulta.

### Análisis de la salida

Como dijimos, estaremos realizando una consulta iterativa y autorizada, por lo que la salida de la consulta se divide en varias partes. A continuación, analizaremos cada una de las partes de la salida:

1. **Consulta a los servidores raíz**: La primera parte de la salida muestra la consulta realizada a los servidores raíz para obtener la dirección de los servidores DNS autoritativos asociados al dominio **org..**

```
. 87203 IN NS e.root-servers.net.  
. 87203 IN NS d.root-servers.net.  
. 87203 IN NS c.root-servers.net.
```

```
.      87203 IN NS b.root-servers.net.
.      87203 IN NS j.root-servers.net.
.      87203 IN NS f.root-servers.net.
.      87203 IN NS l.root-servers.net.
.      87203 IN NS h.root-servers.net.
.      87203 IN NS k.root-servers.net.
.      87203 IN NS m.root-servers.net.
.      87203 IN NS i.root-servers.net.
.      87203 IN NS g.root-servers.net.
.      87203 IN NS a.root-servers.net.
```

Esta consulta está firmada con RRSIG para verificar la autenticidad de la respuesta.

```
.      87203 IN RRSIG NS 8 0 518400 (
      20240920050000 20240907040000 20038 .
      U49XcWjPsd5CGorijfD033h3G+/3Nd2svHCIX60KUzrk
      46UMIU3B9Pbm0s/YCAUVvmD7gj4Zq0k+rXdGEUcysddn
      /oMRtNtIeNe92RwerClE8cUY3Klzulx3rLDghB5W7VLX
      3sy0l0U7XuA7aLSrHmB3tNWQzvXzErbMudKs0W+utzfQ
      1nYYGBDoLFrezaxm+sJHW1/+Mju5sXy5oXACr1ifq9TN
      uFCHfw6UcEW+wXd6MRjGfSdBPod5/bVgMg0hmbpVZ3gB
      u5eqwdBwPBRHQs+GuYlzh6PtJg7Z3W/6ZuCHd4YmoyBv
      W8Wm2ydUmbVSjiFeL9C6u9Ig2TFk/E10tQ== )
```

2. **Consulta a los servidores de nivel superior:** Luego de obtener la dirección de los servidores nivel superior asociados al dominio **org.**, necesitamos saber la dirección de los servidores autoritativos asociados al dominio **mozilla.org.**

```
org.      172800 IN NS a0.org.afilias-nst.info.
org.      172800 IN NS b0.org.afilias-nst.org.
org.      172800 IN NS c0.org.afilias-nst.info.
org.      172800 IN NS d0.org.afilias-nst.org.
org.      172800 IN NS a2.org.afilias-nst.info.
org.      172800 IN NS b2.org.afilias-nst.org.
org.      172800 IN NS c2.org.afilias-nst.info.
org.      172800 IN NS d2.org.afilias-nst.org.
org.      172800 IN NS a1.org.afilias-nst.info.
org.      172800 IN NS b1.org.afilias-nst.org.
org.      172800 IN NS c1.org.afilias-nst.info.
org.      172800 IN NS d1.org.afilias-nst.org.
```

Nuevamente firmada la respuesta para verificar la autenticidad de la misma.

```
org.      86400 IN RRSIG DS 8 1 86400 (
      20240920050000 20240907040000 20038 .
      nw5DAysKQIL8Xs0uznoeNjl6xG08XqPtWQID/Zes5T8j
```

```
5xgASM2Quykm90CNpRY2EPq++5UrKNHxK3g8YIjkezbp
JDJ+i7U1HGQINoEsh9VX0y0jsX0oKYkoAmf0l5SjIfx2
ARiHW2h7gTvnRtEihLV23mpJaiaDPaXRdE5MEKmkKEk
3l/jR7T3bvUL9FYcCnXCvK6IQpy1yeCUBGGb8+fr9Xbj
RYdBmeVrql8EDQCXo25SfkTgIN/deQy+bIYZl0pY7iMH
epood2sZB/NeqPaUvbG4WR0UCxgfjue+oos0oZTJT1TA
wpuUMGWHne8Ju6qm/8vsxRU19UukFAXTQA== )
```

3. **Consulta a los servidores autoritativos:** Una vez que tenemos la dirección de los servidores autoritativos, asociados a [mozilla.org](https://mozilla.org), realizamos la consulta a estos servidores para obtener que servidores DNS saben responder por el dominio [developer.mozilla.org](https://developer.mozilla.org).

```
mozilla.org. 3600 IN NS ns5-65.akam.net.
mozilla.org. 3600 IN NS ns1-240.akam.net.
mozilla.org. 3600 IN NS ns4-64.akam.net.
mozilla.org. 3600 IN NS ns7-66.akam.net.
```

4. **Consulta final al servidor autoritativo:** Finalmente, realizamos la consulta al servidor autoritativo para obtener la dirección IP asociada al nombre de dominio [developer.mozilla.org](https://developer.mozilla.org).

```
developer.mozilla.org. 60 IN CNAME
mdn.prod.mdn.prod.webservices.mozgcp.net.
```

Esto nos está indicando que el nombre de dominio [developer.mozilla.org](https://developer.mozilla.org) en realidad es un alias (CNAME) que apunta a otro nombre de dominio [mdn.prod.mdn.prod.webservices.mozgcp.net](https://mdn.prod.mdn.prod.webservices.mozgcp.net).

Esto significa que si realmente queremos obtener la dirección IP asociada al nombre de dominio [developer.mozilla.org](https://developer.mozilla.org), debemos realizar una nueva consulta a este nuevo nombre de dominio.

5. **Consulta adicional:** En este caso podemos realizar la consulta de forma iterativa, es decir, realizar una nueva consulta al servidor autoritativo asociado al nombre de dominio [mdn.prod.mdn.prod.webservices.mozgcp.net](https://mdn.prod.mdn.prod.webservices.mozgcp.net) para obtener la dirección IP asociada al nombre de dominio [developer.mozilla.org](https://developer.mozilla.org). Pero como el proceso es el mismo, podemos pasar directamente a la consulta final y obtener la dirección IP.

Para eso podemos hacer la siguiente consulta:

```
dig @8.8.8.8 mdn.prod.mdn.prod.webservices.mozgcp.net +short
```

La opción **+short** no elimina la información adicional dejando solo que nos interesa, en este caso la dirección IP asociada al nombre de dominio

**mdn.prod.mdn.prod.webservices.mozgcp.net.** y por ende al nombre de dominio **developer.mozilla.org.**

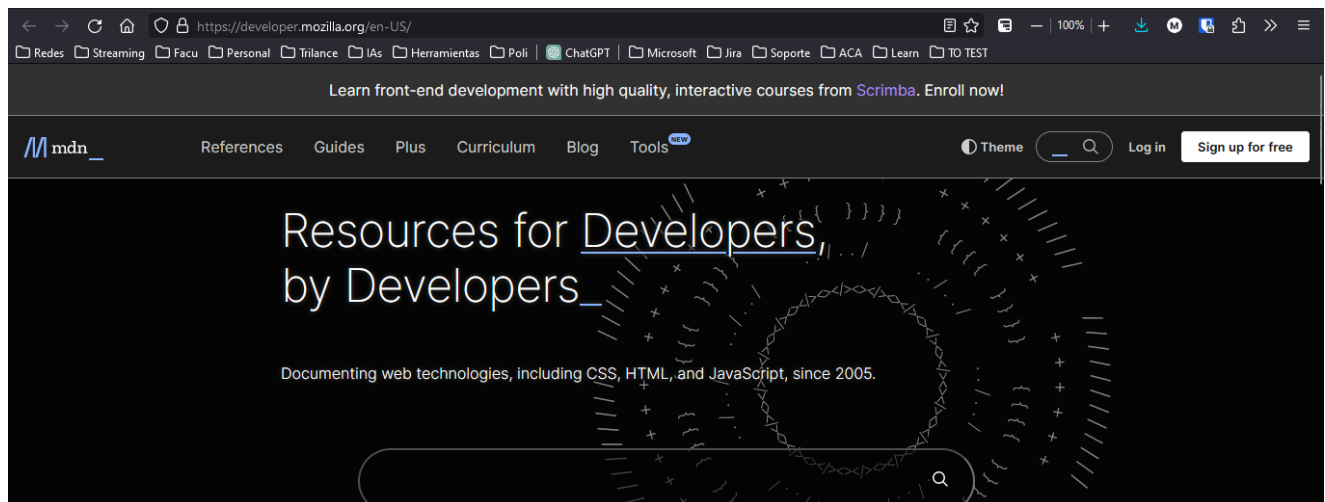
```
mdn.prod.mdn.prod.webservices.mozgcp.net. 174 IN A 34.111.97.67
```

Por lo que la dirección IP asociada al nombre de dominio **developer.mozilla.org.** es **34.111.97.67** y con esta dirección IP podemos acceder al sitio web.

## Información adicional

Además de la información seleccionada, dig nos muestra información adicional sobre la consulta realizada, como las estadísticas de la consulta, los servidores que respondieron, los tiempos de respuesta, los tamaño de los paquetes, entre otros. Muy buena información para comprender lo que realmente comprende la consulta.

## Ingreso al sitio web



El navegador me hace directamente la traducción de la IP a la URL del sitio web.

## Captura de Wireshark

Si ejecutamos el comando mientras hacemos una captura de los paquetes, podremos ir viendo en tiempo real cómo se realizan las consultas y las respuestas de los servidores DNS. Para esto simplemente empezamos a capturar y cortamos al finalizar la consulta.

Una vez que tenemos la captura, podemos filtrar los paquetes para ver solo los relacionados con la consulta DNS. Para esto utilizamos el filtro **dns** en la barra de filtros de Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.057811	192.168.0.251	190.55.154.137	DNS	76	Standard query 0x35ba A wpad.acacoo.net
3	0.076107	190.55.154.137	192.168.0.251	DNS	155	Standard query response 0x35ba A wpad.acacoo.net SOA a.gtld-servers.net
4	0.076406	192.168.0.251	190.55.154.137	DNS	69	Standard query 0xea77 A wpad.home
5	0.079826	192.168.0.251	190.55.154.137	DNS	76	Standard query 0xe70b A wpad.acacoo.net
6	0.095615	190.55.154.137	192.168.0.251	DNS	144	Standard query response 0xea77 No such name A wpad.home SOA a.root-servers.net
7	0.097337	190.55.154.137	192.168.0.251	DNS	155	Standard query response 0xe70b No such name A wpad.acacoo.net SOA a.gtld-servers.net
8	0.097743	192.168.0.251	190.55.154.137	DNS	69	Standard query 0x837b A wpad.home
11	0.133761	190.55.154.137	192.168.0.251	DNS	144	Standard query response 0x837b No such name A wpad.home SOA a.root-servers.net
18	0.669892	192.168.0.251	8.8.8.8	DNS	82	Standard query 0x28fb NS <Root> OPT
19	0.709322	8.8.8.8	192.168.0.251	DNS	567	Standard query response 0x28fb NS <Root> NS b.root-servers.net NS m.root-servers.net NS e.root-servers.net NS c
20	0.711812	192.168.0.251	190.55.154.137	DNS	78	Standard query 0xda15 AAAA b.root-servers.net

Lo primero que observamos es la consulta al servidor DNS de Google donde hacemos la consulta por los DNS raíz y nos devuelve el registro NS de cada uno de ellos junto con la firma RRSIG. Por eso las 14 respuestas.

19	0.709322	8.8.8.8	192.168.0.251	DNS	567	Standard query response 0x28fb NS <Root> NS b.root-servers.net NS m.root-servers.net NS e.root-servers.net NS c
20	0.711812	192.168.0.251	190.55.154.137	DNS	78	Standard query 0xda15 AAAA b.root-servers.net
21	0.711823	192.168.0.251	190.55.154.137	DNS	78	Standard query 0x8b6a A b.root-servers.net
24	0.730569	190.55.154.137	192.168.0.251	DNS	106	Standard query response 0xda15 AAAA b.root-servers.net AAAA 2001:1b8:10::b
25	0.734019	190.55.154.137	192.168.0.251	DNS	94	Standard query response 0x8b6a A b.root-servers.net A 170.247.170.2
26	0.736060	192.168.0.251	190.55.154.137	DNS	78	Standard query 0x18cd A m.root-servers.net
27	0.736113	192.168.0.251	190.55.154.137	DNS	78	Standard query 0x43b6 AAAA m.root-servers.net
28	0.755650	190.55.154.137	192.168.0.251	DNS	106	Standard query response 0x43b6 AAAA m.root-servers.net AAAA 2001:dc3::35
29	0.761982	190.55.154.137	192.168.0.251	DNS	94	Standard query response 0x18cd A m.root-servers.net A 202.12.27.33
30	0.764531	192.168.0.251	190.55.154.137	DNS	78	Standard query 0xc149 AAAA e.root-servers.net
31	0.764531	192.168.0.251	190.55.154.137	DNS	78	Standard query 0x27cf A e.root-servers.net
32	0.780787	190.55.154.137	192.168.0.251	DNS	106	Standard query response 0xc149 AAAA e.root-servers.net AAAA 2001:500:a8::e
33	0.780888	192.168.0.251	181.47.248.146	DNS	78	Standard query 0xc149 AAAA e.root-servers.net
34	0.781016	192.168.0.251	181.47.248.146	DNS	78	Standard query 0x27cf A e.root-servers.net
35	0.785300	190.55.154.137	192.168.0.251	DNS	94	Standard query response 0x27cf A e.root-servers.net A 192.203.230.10
36	0.788103	192.168.0.251	190.55.154.137	DNS	78	Standard query 0xa672 AAAA d.root-servers.net
37	0.788157	192.168.0.251	190.55.154.137	DNS	78	Standard query 0x7568 A d.root-servers.net

Domain Name System (response)				0030	00 0e 00 00 00 01 00 00 02 01 00 00 02 00 01
Transaction ID: 0x28fb				0040	00 01 54 a3 00 14 01 62 0c 72 6f 6f 74 2d 73 65
Flags: 0x81a0 Standard query response, No error				0050	72 76 65 72 73 03 6e 65 74 00 00 00 02 00 01 00
Questions: 1				0060	01 54 a3 00 04 01 6d c0 1e 00 00 02 00 01 00 01
Answer RRs: 14				0070	54 a3 00 04 01 65 c0 1e 00 00 02 00 01 00 01 54
Authority RRs: 0				0080	a3 00 04 01 64 c0 1e 00 00 02 00 01 00 01 54 a3
Additional RRs: 1				0090	00 04 01 69 c0 1e 00 00 02 00 01 00 01 54 a3 00
Queries				00a0	04 01 61 c0 1e 00 00 02 00 01 00 01 54 a3 00 04
<Root>: type NS, class IN				00b0	01 66 c0 1e 00 00 02 00 01 00 01 54 a3 00 04 01
Name: <Root>				00c0	6b c0 1e 00 00 02 00 01 01 54 a3 00 04 01 67
[Name Length: 6]				00d0	c0 1e 00 00 02 00 01 00 01 54 a3 00 04 01 68 c0
[Label Count: 1]				00e0	1e 00 00 02 00 01 00 01 54 a3 00 04 01 63 c0 1e
Type: NS (2) (authoritative Name Server)				00f0	00 00 02 00 01 00 01 54 a3 00 04 01 6c c0 1e 00
Class: IN (0x0001)				0100	00 02 00 01 00 01 54 a3 00 04 01 6a c0 1e 00 00
Answers				0110	2e 00 01 00 01 54 a3 01 13 00 02 00 00 00 07 e9
<Root>: type NS, class IN, ns.b.root-servers.net				0120	00 66 ad aa 1a 66 4f 78 80 a6 46 00 88 fh 40 43

Luego podemos revisar las consultas a los servidores de nivel superior y los servidores autoritativos.

96	1.027236	190.55.154.137	192.168.0.251	DNS	106	Standard query response 0x7da0 AAAA j.root-servers.net AAAA 2001:503:c27::2:30
97	1.027236	190.55.154.137	192.168.0.251	DNS	94	Standard query response 0x197e A j.root-servers.net A 192.58.128.30
98	1.028263	192.168.0.251	192.36.148.17	DNS	104	Standard query 0xc0e9 A developer.mozilla.org OPT
99	1.024017	192.36.148.17	192.168.0.251	DNS	863	Standard query response 0xc0e9 A developer.mozilla.org NS a2.org.afiliat-nst.info NS d0.org.afiliat-nst.org
100	1.025828	192.168.0.251	190.55.154.137	DNS	83	Standard query 0xf1fd AAAA a2.org.afiliat-nst.info
101	1.025828	192.168.0.251	190.55.154.137	DNS	83	Standard query 0xf1fd AAAA a2.org.afiliat-nst.info
137	1.245457	192.168.0.251	199.249.120.1	DNS	120	Standard query 0xbbf6 A developer.mozilla.org OPT
138	1.465235	199.249.120.1	192.168.0.251	DNS	689	Standard query response 0xbbf6 A developer.mozilla.org NS ns4-64.akam.net NS ns5-65.akam.net NS ns7-66.akam.net

Finalmente, podemos ver la consulta al servidor autoritativo y la respuesta con la dirección IP asociada al nombre de dominio **developer.mozilla.org**.

161	1.554820	190.55.154.137	192.168.0.251	DNS	104	Standard query response 0x/0d9 AAAA ns1-240.akam.net AAAA 2000:1401:2::f0
162	1.554820	190.55.154.137	192.168.0.251	DNS	92	Standard query response 0xd712 A ns1-240.akam.net A 193.108.91.240
163	1.556396	192.168.0.251	193.108.91.240	DNS	120	Standard query 0x5a0d A developer.mozilla.org OPT
164	1.605340	193.108.91.240	192.168.0.251	DNS	146	Standard query response 0x5a0d A developer.mozilla.org CNAME mdn.prod.mdn.prod.webservices.mozgcp.net OPT

Class: IN (0x0001)			
Answers			
developer.mozilla.org: type CNAME, class IN, cname mdn.prod.mdn.prod.webservices.mozgcp.net			
Name: developer.mozilla.org			
Type: CNAME (5) (Canonical NAME for an alias)			
Class: IN (0x0001)			
Time to live: 60 (1 minute)			
Data length: 42			
CNAME: mdn.prod.mdn.prod.webservices.mozgcp.net			

Como vemos la respuesta final, nos indica que el nombre de dominio **developer.mozilla.org** es un alias como habíamos visto anteriormente y que apunta a otro nombre de dominio **mdn.prod.mdn.prod.webservices.mozgcp.net**.

Hasta aquí llega la consulta de **dig**, pero como vimos anteriormente, podemos realizar una nueva consulta para obtener la dirección IP asociada al nombre de dominio

mdn.prod.mdn.prod.webservices.mozgcp.net. y por ende al nombre de dominio developer.mozilla.org..

Current filter: dns					
No.	Time	Source	Destination	Protocol	Length Info
21	1.271807	192.168.0.251	8.8.8.8	DNS	123 Standard query 0x4be3 A mdn.prod.mdn.prod.webservices.mozgcp.net OPT
22	1.322962	8.8.8.8	192.168.0.251	DNS	127 Standard query response 0x4be3 A mdn.prod.mdn.prod.webservices.mozgcp.net A 34.111.97.67 OPT

```
Type: A (1) (Host Address)
Class: IN (0x0001)
  Answers
    mdn.prod.mdn.prod.webservices.mozgcp.net: type A, class IN, addr 34.111.97.67
      Name: mdn.prod.mdn.prod.webservices.mozgcp.net
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 600 (10 minutes)
      Data length: 4
      Address: 34.111.97.67
  Additional records
```

Como vemos, obtenemos la misma IP que habíamos obtenido anteriormente por consola: 34.111.97.67.

Acá termina la consulta y podemos ver todo el proceso de resolución de nombres de dominio a través de la captura de Wireshark en el archivo [wireshark.pcapng](#) y [wireshark\\_adicional.pcapng](#). Tenemos muchas más consultas intermedias a los servidores DNS y las respuestas correspondientes. Entre ellas todos los servidores raíz que terminamos ignorando ya que otros respondieron antes.

## Conclusión

Dig es una utilidad muy interesante para entender y depurar el funcionamiento del protocolo DNS. Nos permite realizar consultas de forma iterativa y autorizada, obteniendo información detallada sobre los servidores que responden a nuestras consultas y los registros asociados a los nombres de dominio.

Particularmente esta dirección a consultar era una dirección especial ya que no nos devolvía directamente la dirección IP asociada al nombre de dominio sino un alias al que debíamos consultar para obtener la dirección IP final. Este ejemplo nos permitió entender más en profundidad el orden en el que el protocolo DNS resuelve las consultas y cómo se realiza la resolución de nombres de dominio en la práctica.

Por último, la captura de Wireshark nos enseña que es realmente una herramienta muy poderosa para cualquier administrador de red o ingeniero. Nos permite ver bit a bit todo el tráfico de la computadora y aunque a primera vista a veces no se entienda mucho, podemos excavar (dig 😊) en los paquetes y entender las comunicaciones que se están realizando en la red.

Como comentario personal, me sorprende la velocidad con la que se resuelven las consultas DNS y estoy convencido que aunque no probe mucho el uso de las respuestas cacheadas, es un gran ahorro de tiempo y recursos para el internet en general.

## Bibliografía

- [IBM dig command](#): me permitió entender la estructura del comando [dig](#) y las opciones que se pueden utilizar.