1. Introducción a DNS.

El protocolo de resolución de nombres de dominio DNS (*Domain Name System*) se emplea para traducir las direcciones IP de los equipos a nombres de dominio de la forma *www.dominio.com* y viceversa, de modo que sea más fácil de recordar para las personas.

Su funcionamiento y utilidad es similar al de una agenda telefónica. Es bastante complicado para una persona recordar los números de teléfono de todos nuestros contactos, sin embargo, nos resulta mucho más fácil recordar sus nombres. De este modo, cuando queremos llamar a uno de nuestros amigos, buscamos su nombre en la agenda, automáticamente nuestro teléfono obtiene el número al cual realizar la llamada.

En el caso de Internet, cuando queremos acceder a una determinada web, sería imposible memorizar las direcciones IP de todas nuestras páginas favoritas, pero sí recordamos sus nombres. Cuando introducimos el nombre del dominio que queremos visitar, el software de nuestro ordenador realiza una serie de consultas para averiguar cuál es la IP de dicho dominio antes de poder obtener el contenido de la página que queremos visitar.

Podemos ver un ejemplo sencillo con la utilidad ***ping***. Cuando hacemos *ping* a un determinado dominio se puede observar cuál es la dirección IP de este. En la *Figura 1* se puede ver la dirección IP del dominio *www.google.com*.

```
PING www.google.com (142.250.200.100) 56(84) bytes of data.
64 bytes from mad41s13-in-f4.1e100.net (142.250.200.100): icmp_seq=1 ttl=115 time=21.6 ms

--- www.google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 21.681/21.681/21.681/0.000 ms
```

Figura 1: Dirección IP de google.com.

También es posible averiguar el nombre de dominio a partir de una dirección IP, a este proceso se conoce como **resolución DNS inversa**.

El protocolo DNS establece las reglas de comunicación entre el servidor de nombres de dominio y los clientes para realizar la resolución de la dirección IP del dominio. El protocolo se encuentra descrito en numerosos RFC, aunque un punto de comienzo puede ser el **RFC 6195**, que revisa el estado y realiza recomendaciones de buenas prácticas en la implementación del protocolo.

RFC 6895. Domain Name System (DNS) IANA Considerations.
https://tools.ietf.org/html/rfc6895

Para profundizar más en el funcionamiento del protocolo DNS y su seguridad, recomendamos consultar la **Guía de seguridad en servicios DNS** elaborada por el INCIBE.

Guía de seguridad en servicios DNS. INCIBE 2014.
https://www.incibe-cert.es/blog/guia-dns

1.1. Estructura de nombres de dominio.

La estructura de nombres de dominio, conocida como FQDN (*Fully Qualified Domain Name*), es un sistema jerárquico que permite localizar de forma exacta un recurso a través del protocolo DNS. Los nombres de dominio se leen de derecha a izquierda, comenzando por la zona raíz del dominio, simbolizado por un punto (.) que habitualmente se obvia al escribir el nombre de dominio. Por ejemplo, el dominio ***subdominio.dominio.es.*** se estructura del siguiente modo:

- Comienza con la zona raíz representada por el . que se puede obviar.
- Continúa con el dominio de nivel superior ***es*** o TLD (*Top Level Domain*).
- Después tenemos el dominio de segundo nivel ***dominio*** o SLD *(Second Level Domain*) que es un subdominio del TLD.
- Por último, tenemos el dominio de tercer nivel ***subdominio***, que a su vez es un subdominio del SLD. El número de niveles no tiene límite pero DNS establece un límite en el número de caracteres que puede tener un nombre de dominio que es de 255 caracteres en total.

Información sobre FQDN en Wikipedia. [ENG]
https://en.wikipedia.org/wiki/Fully_qualified_domain_name

En cuanto a los TLD, existen distintos tipos:

- **Organizaciones genéricas** (gTLD – *Generic Top Level Domain*). Se conocen como genéricos por razones históricas y la lista ha sufrido cambios a lo largo de los años. En la actualidad se consideran dominios gTLD a *com*, *org*, *net*, *info*, *name* y *pro*.
- **Localizados geográficamente** (ccTLD – *Country Code Top Level Domain*). Pertenecen a países o regiones, están definidos por ISO 3166-1) : *es*, *pt*, *fr*, etc.
- **Dominios patrocinados** (sTLD – *Sponsored Top Level Domain*). Son dominios propuestos por alguna agencia o fundación independiente (*aero*, *mobi*, *cat*, *edu*, *gov*). Los dominios patrocinados *int*, *edu*, *gov* y *mil* inicialmente pertenecían a la categoría gTLD.
- **Dominios para pruebas** (tTLD – *Test Top Level Domai*n). Son dominios *test* empleados para pruebas en el desarrollo de los protocolos. No se encuentran accesibles en los directorios raíz.

1.2. Gestión de los nombres de dominio.

IANA (*Internet Assigned Numbers Authority*) es el organismo encargado de la gestión de los servidores raíz. También es el organismo encargado de gestionar los TLD y supervisar la creación de nuevos TLD.

IANA delega la gestión de cada TLD en una **autoridad de registro**. Por ejemplo, los dominios geográficos (gTLD) son gestionados, normalmente, por cada país. En España, el **organismo**

REDES *(red.es*) es la autoridad de registro de los dominios *es*, que realiza esta función a través de ***dominios.es*** (https://www.dominios.es).

A su vez, la autoridad de registro de un TLD delega en otras entidades llamados **agentes registradores** (*registrars*) los servicios de contratación y gestión de dominios para el público en general. En la página web de *dominios.es* se puede consultar la lista completa de agentes registradores para los dominios *es*.

1.3. Registros Regionales de Internet.

Puesto que DNS traduce nombres de dominio en direcciones IP, estas también deben gestionarse y asignarse de algún modo. IANA delega la gestión de bloques IP a los **Registros Regionales de Internet** (RIR, *Regional Internet Registry*).

Estas organizaciones están encargadas de la distribución, venta, gestión de direcciones IP. Ofrecen información útil para identificar rangos de direcciones IP de una entidad y sistemas autónomos (AS, *Autonomous System*), los routers de direccionamiento en la red pública.

Hay diferentes RIR que gestionan un área geográfica concreta: APNIC (Asia), RIPE (Europea), ARIN (América), AfricNIC (África) y LacNIC (Latinoamérica y Caribe). Por tanto, en nuestra investigación, cuando obtenemos datos de direcciones IP podemos consultar más información de ellas en los diferentes RIR, en nuestro caso será más habitual usar RIPE.

Página web y base de datos de RIPE. [ENG]
https://www.ripe.net/

1.4. Zonas DNS.

La estructura de nombres de dominio es un árbol jerárquico, sin embargo, esto no representa exactamente cómo funciona el sistema de nombres de dominio. Una consulta DNS para un determinado nombre de dominio es resuelto por el **servidor de nombres autorizado** (*authoritative name server*) para la zona DNS a la que pertenece dicho dominio.

Las zonas DNS se utilizan para organizar la gestión de la información de un determinado dominio y subdominios. Una zona DNS puede tener uno o varios servidores de nombres autorizados, y puede gestionar más de un dominio.

Artículo de Cloudflare. ¿Qué es una zona DNS?
https://www.cloudflare.com/es-es/learning/dns/glossary/dns-zone/

La información de todos los nombres de dominio no está almacenada en un único servidor, está distribuida en zonas. La zona raíz está compuesta por 13 servidores raíz gestionados por la IANA,

desde *a.root-servers.net* hasta *m.root-servers.net*. Estos servidores son los encargados de resolver las consultas de las zonas de los dominios de primer nivel (TLD), como los dominios genéricos (gTLD) *com*, *net*, *edu*, o los dominios de países (ccTLD) como *es*, *fr*, *uk*, etc.

HOSTNAME	IP ADDRESSES	OPERATOR
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	Verisign, Inc.
b.root-servers.net	199.9.14.201, 2001:500:200::b	University of Southern California, Information Sciences Institute
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	Verisign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Figura 2: Listado de los 13 servidores raíz con sus direcciones IPv4 e IPv6. Fuente: https://www.iana.org/domains/root/servers

Cada una de estas zonas TLD tiene múltiples servidores de nombres autorizados que son registrados en los servidores raíz correspondientes. De este modo, cuando el servidor raíz recibe una consulta sobre un determinado dominio, aunque este no conozca cuál es la respuesta (cuál es la dirección IP de este nombre de dominio) sí conoce cuál es el servidor de nombres autorizado para dicho dominio por lo que puede responder para que se dirija la consulta a este. En las siguientes secciones se explica todo este proceso de manera práctica.

1.5. Tipos de registros DNS.

Para comprender las consultas DNS es importante saber que la información DNS se guarda en **registros de distinto tipo**:

- **A** (*Address*). Registro para traducir nombres de hosts a direcciones IPv4.
- **AAAA** (*Address*). Similar al anterior, pero para traducir nombres a direcciones IPv6.
- **CNAME** (*Canonical Name*). Se usa para crear nombres de hosts adicionales, o alias, para los host de un dominio. Empleado cuando se corren múltiples servicios (FTP, HTTP…) en un servidor con una sola IP. Cada servicio tiene su propia entrada DNS (*ftp.ejemplo.com* y *www.ejemplo.com*). También se utiliza cuando hay múltiples servidores HTTP en el mismo host, con diferentes nombres.
- **NS** (*Name Server*). Establece la asociación entre un nombre de dominio y el servidor o servidores de nombres autorizados que almacenan la información de ese dominio.

- **MX** (*Mail eXchange*). El registro de intercambio de correo asocia el nombre de dominio a los servidores de correo disponibles para ese dominio.
- **PTR** (*PoinTeR*). También conocido como registro inverso, ya que su funcionamiento es lo opuesto al registro A, traduciendo direcciones IP a nombres de dominio.
- **SOA** (*Start Of Authority*). Proporciona información sobre el servidor DNS primario de la zona.
- **HINFO** (*Host Information*). Descripción del host. Permite conocer información del tipo de máquina y sistema operativo.
- **TXT** (*Text*). Información textual, permite a los dominios identificarse de modo arbitrario.
- **LOC** (*Location*). Permite indicar las coordenadas GPS del dominio.
- **WKS**. Obsoleto en favor de SRV.
- **SRV** (*Services*). Permite indicar los servicios que ofrece el dominio (definido en el RFC 2782 y actualizado posteriormente en RFC 6335 y 8553).
- **SPF** (*Sender Policy Framework*). Este registro especifica los hosts que están autorizados a enviar correo desde el dominio dado. Se utiliza para identificar correos falsificados y/o spam.

1.6. El proceso iterativo de una consulta DNS.

Cuando un equipo cliente trata de comunicarse con otra máquina a través de un nombre de dominio, el equipo cliente necesita averiguar en primer lugar cuál es la IP correspondiente a dicho nombre de dominio. La primera parada es el equipo local, es decir, consultar si nuestro propio equipo conoce la respuesta, el encargado de dar la respuesta es el *Local DNS Resolver*.

En Linux, el fichero */etc/hosts* es un fichero de texto plano que almacena traducciones estáticas de nombres de dominio, por lo que es el primer lugar donde se consulta por el *local DNS Resolver*. En sistemas operativos Windows, el fichero se sitúa en *C:\Windows\System32\drivers\etc\hosts*.

```
127.0.0.1 localhost
192.168.57.5 www.miejemplo.com miejemplo.com ftp.miejemplo.com
10.5.0.2 www.trustedsite.com trustedsite.com
10.5.0.3 www.evilsite.com evilsite.com
```

Si la respuesta no está en el equipo local, la consulta se trasladará al **servidor DNS local**, que normalmente será el servidor DNS de nuestro proveedor de Internet, o aquél que tengamos configurado. Algunos de los servidores DNS públicos más utilizados son los servidores DNS de Google (8.8.8.8 y 8.8.4.4) o de Cloudflare (1.1.1.1).

Este servidor DNS realiza el proceso iterativo de consultar a los servidores autorizados de cada zona hasta que obtiene la respuesta adecuada. Vamos a simular este proceso iterativo utilizando el comando *dig*. Este comando nos permite realizar consultas DNS a un servidor de nuestra

elección, además se puede configurar también el tipo de consulta que se desea realizar. El formato del comando es el siguiente:

dig @server dominio tipo

- ***server***. Es el nombre o dirección IP del servidor DNS al que se desea consultar.
- ***dominio***. El nombre de dominio sobre el que realizamos la consulta.
- ***tipo***. El tipo de registro DNS que se desea consultar (ANY, A, MX, NS, SIG, etc.). Si no se indica nada, se consulta por defecto el registro A.

Vamos a averiguar la dirección IP del dominio *www.example.com*. Comenzamos consultando a uno de los servidores raíz, hemos elegido el servidor *k*, por estar gestionado por RIPE y, por tanto, más cerca geográficamente. El siguiente cuadro muestra la respuesta obtenida (se han omitido algunos elementos en las diferentes respuestas).

```
$ dig @k.root-servers.net www.example.com

;; QUESTION SECTION:
;www.example.com. IN A

;; AUTHORITY SECTION:

com. 172800 IN NS b.gtld-servers.net.
com. 172800 IN NS j.gtld-servers.net.
com. 172800 IN NS k.gtld-servers.net.

;; ADDITIONAL SECTION:
b.gtld-servers.net. 172800 IN A 192.33.14.30
j.gtld-servers.net. 172800 IN A 192.48.79.30
k.gtld-servers.net. 172800 IN A 192.52.178.30
```

Una respuesta DNS puede tener cuatro secciones:

- ***Question***. Aquí aparecen los campos de la pregunta que se ha realizado al servidor de nombres.
- ***Answer***. Esta sección contiene la respuesta a la pregunta que se ha realizado, es decir, la dirección IP del nombre de dominio que se ha consultado.
- ***Authority***. Esta sección contiene los servidores de nombres autorizados para responder la pregunta realizada.
- ***Additional***. Esta sección contiene información relacionada con la consulta pero no es estrictamente la respuesta a la pregunta.

Por tanto, de los resultados de la consulta anterior no hemos obtenido la respuesta que íbamos buscando, pero hemos obtenido un listado de servidores de nombres autorizados (registros NS en la sección *authority*) para la zona *.com*, qué si pueden contestar a nuestra pregunta, por ejemplo *k.gtld-servers.net*, por lo que debemos trasladar nuestra consulta a alguno de ellos. Además, en la sección *additional* nos indica cuál es la dirección IP de cada uno de estos servidores autorizados.

```
$ dig @k.gtld-servers.net www.example.com

;; QUESTION SECTION:
;www.example.com. IN A

;; AUTHORITY SECTION:
example.com. 172800 IN NS a.iana-servers.net.
example.com. 172800 IN NS b.iana-servers.net.
```

Al igual que antes, el servidor responsable de la zona *.com* no conoce la respuesta, pero conoce cuáles son los servidores autorizados para la zona *example.com*, estos son *a.iana-servers.net* y *b.iana-servers.net*, por lo que les trasladamos la pregunta a uno de ellos.

```
$ dig @a.iana-servers.net www.example.com

;; QUESTION SECTION:
;www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 86400 IN A 93.184.216.34
```

Finalmente, hemos obtenido la respuesta, En la sección Answer podemos ver que la dirección IP del nombre de dominio *www.example.com* es 93.184.216.34.

Los servidores de nombres locales guardan las consultas previas que les han realizado en una caché, con lo que no siempre será necesario realizar el proceso iterativo completo. La siguiente vez que el servidor DNS local reciba una consulta para el dominio *www.example.com*, ofrecerá la respuesta inmediatamente, acelerando el proceso de consultas enormemente. Estos registros se guardan en la caché por un tiempo definido, por lo que cuando expiran son eliminados de la misma. Esto permite poder actualizar los datos de los nombres de dominio, este proceso suele tardar entre 24 y 48 horas, hasta que los cambios se propagan por todos los servidores mientras expiran los datos almacenados en sus cachés.