UNIVERSIDAD DE LAS FUERZAS ARMADAS
ESPE

Sistemas Operativos

Departamento de Ciencias de la Computación

Búsqueda de DNS

Estudiante:

Victor Camacho, Josué Merino, Martin Suquillo

Docente:

Ing. Washington Loza

Índice general

Índice de figuras

1. Objetivos

1.1. Objetivo General

Analizar el proceso de resolución de nombres de dominio mediante la consulta de servidores DNS extranjeros, utilizando herramientas de línea de comandos en sistemas Windows y Linux.

1.2. Objetivos Específicos

- Ejecutar y analizar consultas DNS en sistemas Windows y Linux mediante comandos, identificando la IP del servidor y el DNS que responde a la petición.
- Examinar la ruta de los paquetes de datos desde la computadora local hasta un servidor extranjero, observando los diferentes saltos en la red.

2. Desarrollo

2.1. DNS

El sistema de nombres de dominio (DNS) es básicamente una base de datos de información del host, el servicio que proporciona es información sobre el servidor de Internet. [1]

2.1.1. DNS Autoritativo

Proporciona un mecanismo de actualización que los desarrolladores utilizan para administrar sus nombres DNS públicos. De esta forma, responde a las consultas DNS convirtiendo los nombres de dominio en direcciones IP para que los equipos puedan comunicarse entre ellos. El DNS autoritativo tiene la autoridad final sobre el dominio y es responsable de brindar respuestas a servidores de DNS recurrente con la información de la dirección IP. [2]

2.1.2. DNS Recursivo

Los clientes normalmente no realizan consultas directamente a los servicios de DNS autoritativo. En su lugar, generalmente se conectan con otro tipo de servicio de DNS conocido como solucionador o un servicio de DNS recurrente. Este servicio funciona como un intermediario que obtiene la información del DNS por el cliente. Si un DNS recurrente tiene una referencia de DNS en caché o almacenada durante un período, entonces responde la consulta de DNS mediante el suministro de la información IP o la fuente. De lo contrario, pasa la consulta a uno o más servidores de DNS autoritativo para encontrar la información. [2]

2.2. Windows

Pasos :

1. Abrimos la terminal de Windows:

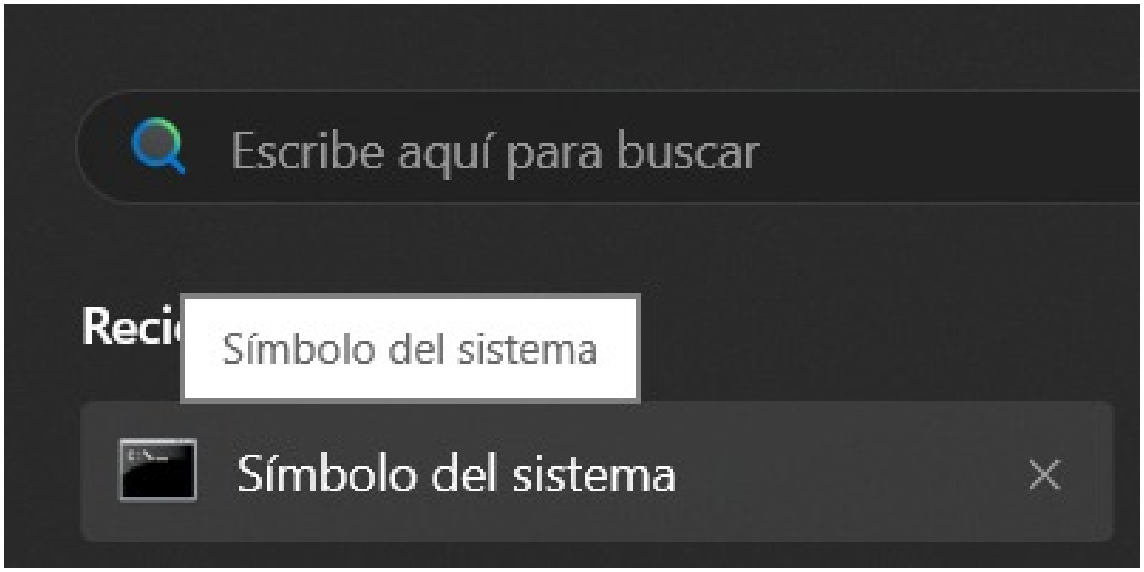

Figura 2.1: Terminal de Windows

2. Configuración Inicial del Servidor DNS Predeterminado:

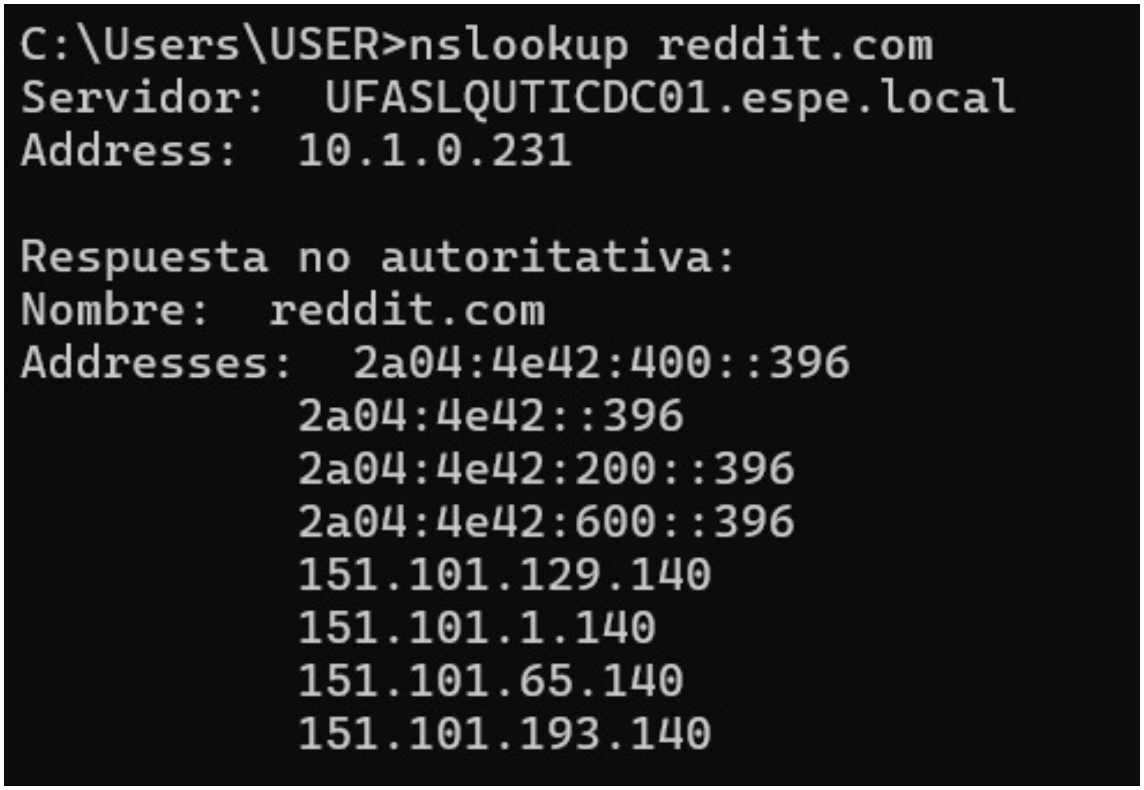

Figura 2.2: Configuración Inicial

Se configuró el servidor DNS predeterminado en el sistema. Para verificar la configuración del servidor DNS, se utilizó el comando **nslookup** sin parámetros adicionales. Como resultado, el servidor DNS predeterminado configurado fue "UFASLQUTICDC01.espe.local" con la dirección IP 10.1.0.231. Este servidor fue utilizado para todas las consultas DNS posteriores durante el laboratorio.

3. Consulta de Registros MX (Mail Exchanger) para el Dominio "reddit.com"

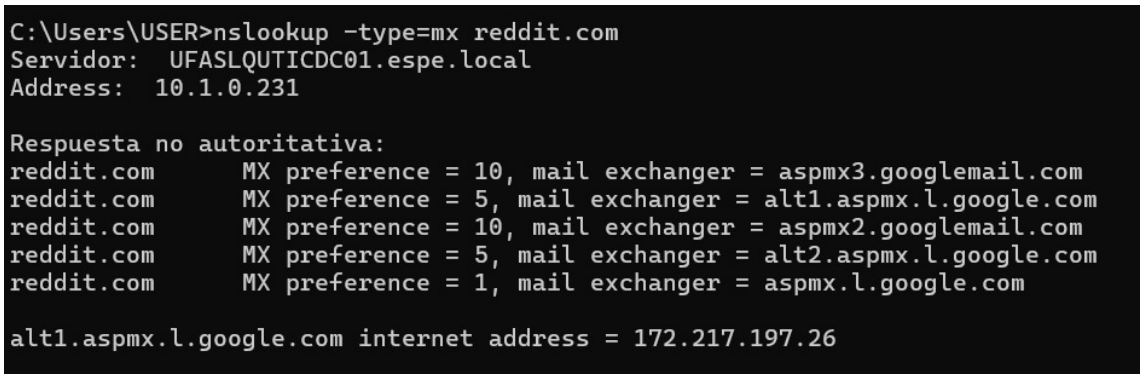

Figura 2.3: Consulta de Registros

Se realizó una consulta de tipo MX para el dominio "reddit.com" utilizando el comando nslookup -type=mx reddit.com. Este tipo de consulta proporciona información sobre los servidores de correo asociados al dominio solicitado. Los resultados obtenidos incluyeron varios registros MX, indicando los servidores de correo y sus respectivas prioridades de conexión. Los registros MX mostraron que los servidores de correo de "reddit.com" tienen distintas preferencias, con el servidor de mayor prioridad

4. Consulta de Direcciones IP para el Dominio "reddit.com"

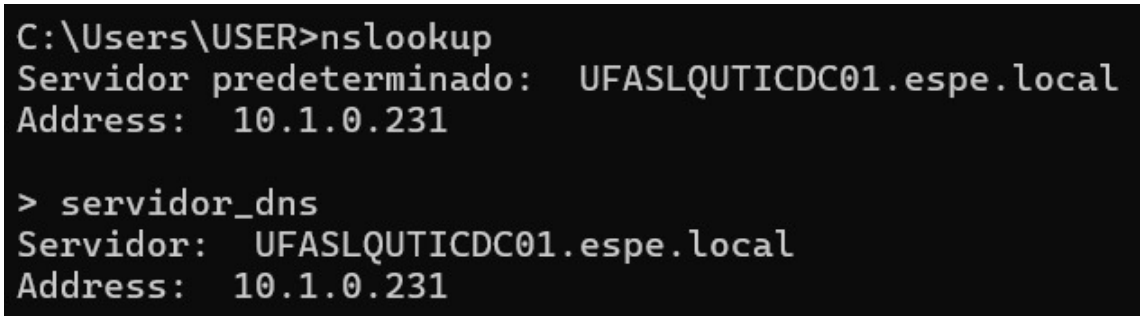

Figura 2.4: Consulta de Dirección IP

se realizó una consulta para obtener las direcciones IP asociadas al dominio "reddit.com" mediante el comando nslookup reddit.com. Como resultado, se obtuvieron varias direcciones IPv6 y IPv4. Las direcciones IPv6 obtenidas fueron de la forma "2a04:4e42:400::396", mientras que las direcciones IPv4 incluyeron "151.101.129.140z "151.101.65.140", entre otras. Estos registros indican las direcciones a las que se puede acceder para llegar al servidor correspondiente.

2.3. Linux

```
[g7@localhost ~]$ dig +trace google.com

; <<>> DiG 9.16.23-RH <<>> +trace google.com
;; global options: +cmd
.                       41160   IN      NS      k.root-servers.net.
.                       41160   IN      NS      h.root-servers.net.
.                       41160   IN      NS      m.root-servers.net.
.                       41160   IN      NS      d.root-servers.net.
.                       41160   IN      NS      f.root-servers.net.
.                       41160   IN      NS      b.root-servers.net.
.                       41160   IN      NS      e.root-servers.net.
.                       41160   IN      NS      c.root-servers.net.
.                       41160   IN      NS      l.root-servers.net.
.                       41160   IN      NS      g.root-servers.net.
.                       41160   IN      NS      a.root-servers.net.
.                       41160   IN      NS      i.root-servers.net.
.                       41160   IN      NS      j.root-servers.net.
;; Received 824 bytes from 10.0.2.3#53(10.0.2.3) in 25 ms
```

Figura 2.5: dig +trace google.com

El comando dig +trace google.com muestra cómo se resuelve el nombre de dominio google.com a su dirección IP paso a paso:

1. dig primero pregunta a los servidores raíz de DNS sobre google.com.
2. Los servidores raíz (k.root-servers.net, h.root-servers.net, etc.) no tienen la respuesta final, pero saben quién maneja los dominios .com y los redirigen allí.
3. La última línea dice que la respuesta vino de 10.0.2.3 en 25 ms. Esta es la dirección de nuestro servidor DNS configurado.

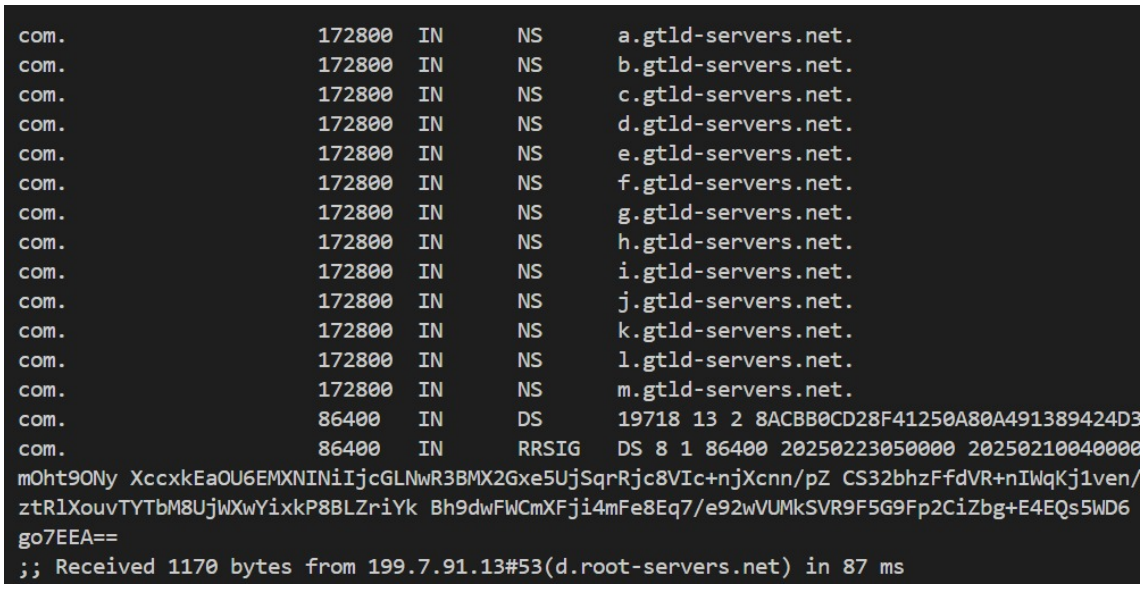

Figura 2.6: Respuesta del servidor 1

4. Ahora, dig pregunta a los servidores responsables del dominio de nivel superior .com (ej., a.gtld-servers.net, b.gtld-servers.net, etc.).

5. Estos servidores tampoco tienen la dirección IP final de google.com, pero saben qué servidores manejan el dominio google.com.

6. La respuesta vino del servidor d.root-servers.net en 87 ms.

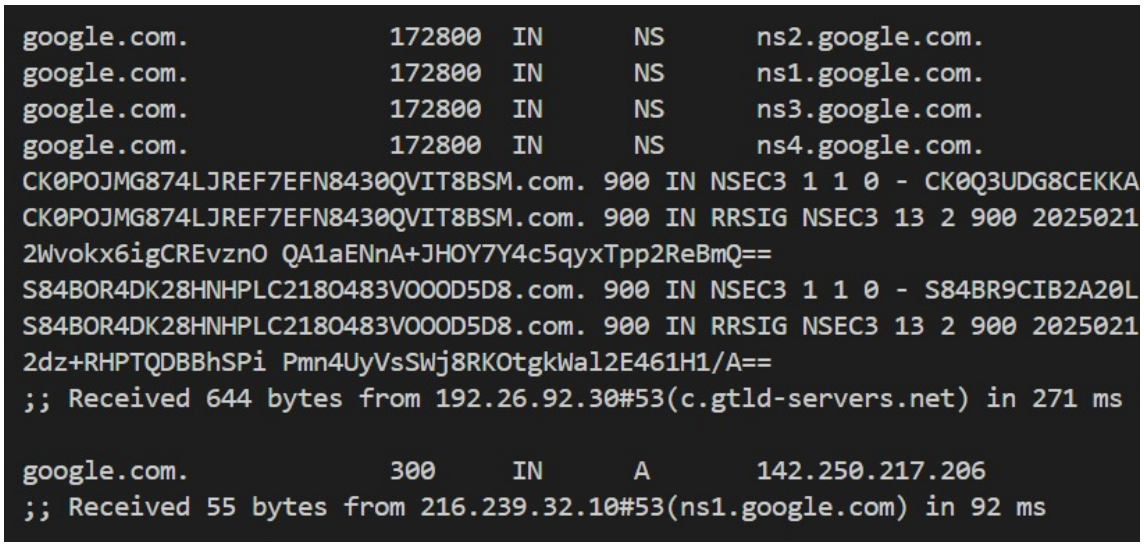

Figura 2.7: Respuesta del servidor 2

7. Ahora dig pregunta a los servidores específicos de google.com (ns1.google.com, ns2.google.com, etc.).

8. Estos servidores tienen la dirección IP de google.com y la devuelven.

9. La respuesta vino del servidor c.gtld-servers.net en 271 ms. 10. Finalmente, los servidores de google.com responden con la dirección IP 142.250.217.206.

10. La respuesta vino de ns1.google.com en 92 ms.

3. Conclusiones

- A través de los comandos, se pudo comprobar que los sistemas operativos pueden resolver nombres de dominio a direcciones IP de manera eficiente, utilizando servidores DNS específicos.
- El uso de comandos en Windows y en Linux permitió visualizar la ruta que siguen los paquetes de datos hasta llegar al servidor extranjero. Se observó que los paquetes atraviesan múltiples nodos intermedios antes de llegar a su destino, lo que influye en la latencia y el tiempo de respuesta de la conexión.
- Se evidenció que la ubicación del servidor DNS impacta en los tiempos de respuesta, ya que servidores ubicados en otras regiones pueden generar una mayor latencia. Esto resalta la importancia de utilizar servidores DNS óptimos para mejorar la velocidad y estabilidad de la conexión a Internet.

Bibliografía

[1] Liu, C., & Albitz, P. (2006). DNS and Bind. .º'Reilly Media, Inc.".

[2] ¿Qué es DNS? – Introducción a DNS - AWS. (s.f.). Amazon Web Services, Inc. `https://aws.amazon.com/es/route53/what-is-dns/`