Redes de Ordenadores

GRADO EN INGENIERÍA INFORMÁTICA

**Lr - DNS**

**Curso** 2020/2021

Jorge Rodríguez Fraile, 100405951, Grupo 81, [100405951@alumnos.uc3m.es](mailto:100405951@alumnos.uc3m.es)

Índice

[Cuestiones de nslookup 3](#_Toc55048614)

[Cuestiones escenario 1: Web-surfing 4](#_Toc55048615)

[Cuestiones escenario 2: nslookup 6](#_Toc55048616)

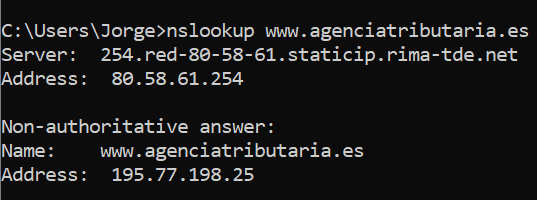
[Cuestiones escenario 3: nslookup 8](#_Toc55048617)

[Cuestiones escenario 4: nslookup 9](#_Toc55048618)

# Cuestiones de nslookup

1. Ejecuta nslookup para obtener la dirección IP del dominio de la **Agencia Tributaria Española.**

Su dirección IP de dominio es 195.77.198.25



1. Ejecuta nslookup para obtener los *authoritative servers* de **Yahoo**.

Los servidores autoritarios para yahoo.com, con su nombre y dirección IP son:

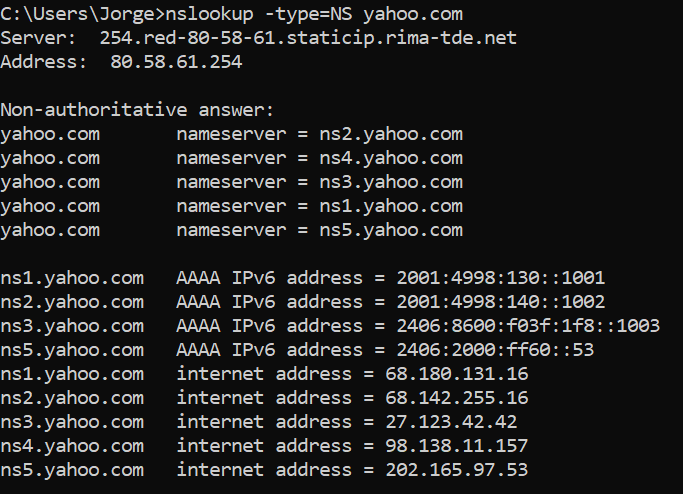
ns1.yahoo.com 68.180.131.16

ns2.yahoo.com 68.142.255.16

ns3.yahoo.com 27.123.42.42

ns4.yahoo.com 98.138.11.157

ns5.yahoo.com 202.165.97.53



1. Ejecuta nslookup para determinar los servidores de correo de la **Universidad Carlos III**

Los servidores obtenidos del tipo MX, los de intercambio de correo, para uc3m.es son:

aspmx.l.google.com internet address = 142.250.13.26

aspmx.l.google.com AAAA IPv6 address = 2a00:1450:400c:c0c::1a

alt1.aspmx.l.google.com internet address = 209.85.233.26

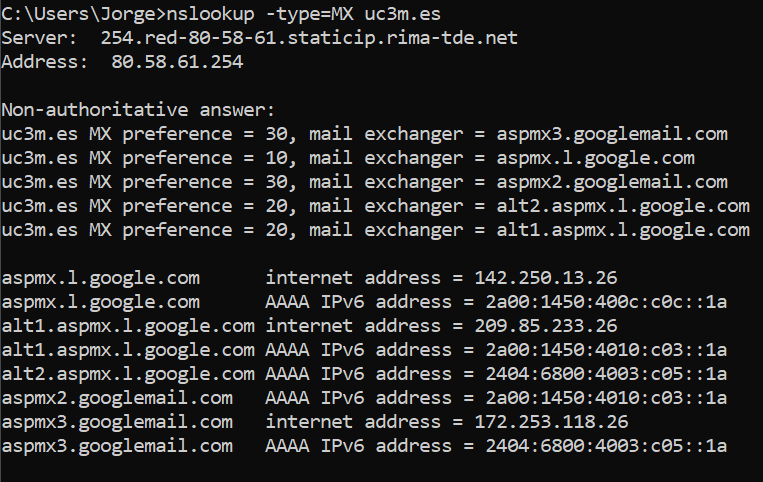
alt1.aspmx.l.google.com AAAA IPv6 address = 2a00:1450:4010:c03::1a

alt2.aspmx.l.google.com AAAA IPv6 address = 2404:6800:4003:c05::1a

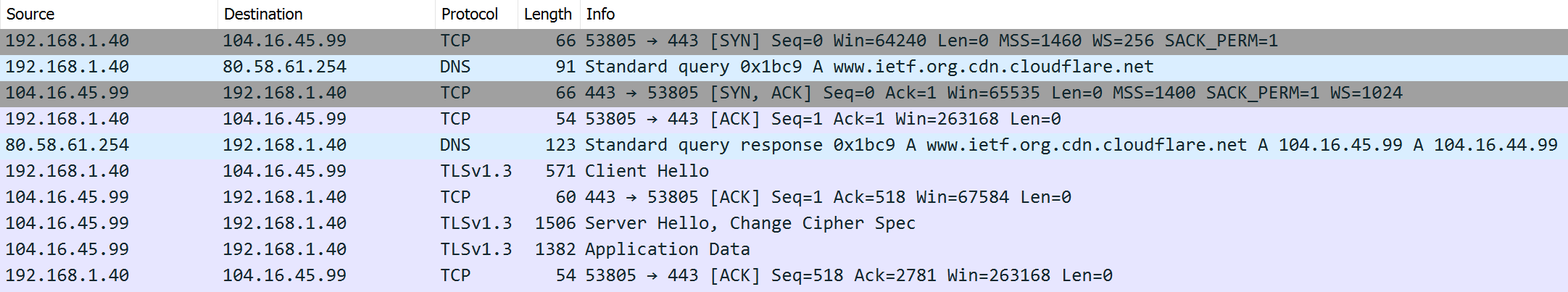
aspmx2.googlemail.com AAAA IPv6 address = 2a00:1450:4010:c03::1a

aspmx3.googlemail.com internet address = 172.253.118.26

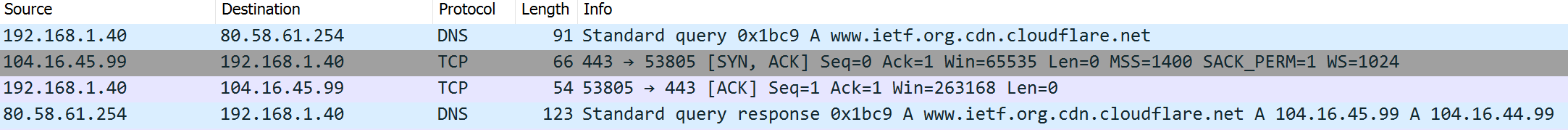
aspmx3.googlemail.com AAAA IPv6 address = 2404:6800:4003:c05::1a



# Cuestiones escenario 1: Web-surfing



1. Localiza los mensajes de petición y respuesta DNS. ¿Son enviados sobre TCP o sobre UDP?



Son enviados con UDP.



1. ¿Cuál es el puerto de destino para el mensaje de petición DNS? ¿Cuál es el puerto de origen del mensaje respuesta?

Puerto destino de la petición: 53

Puesto origen de la respuesta: 53

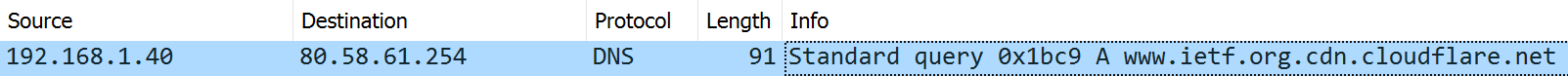




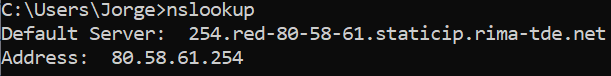
1. ¿A qué dirección IP se envió la petición DNS? Utiliza alguna de las aplicaciones del sistema comentadas anteriormente para determinar la dirección IP del servidor DNS configurado en el equipo. ¿Coinciden ambas direcciones?

La petición se envió a la dirección: 80.58.61.254

Wireshark:



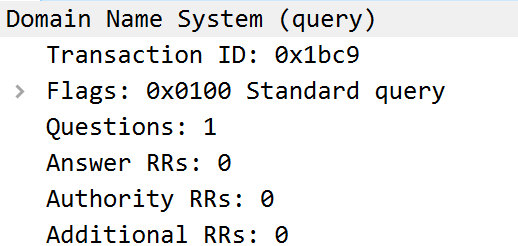
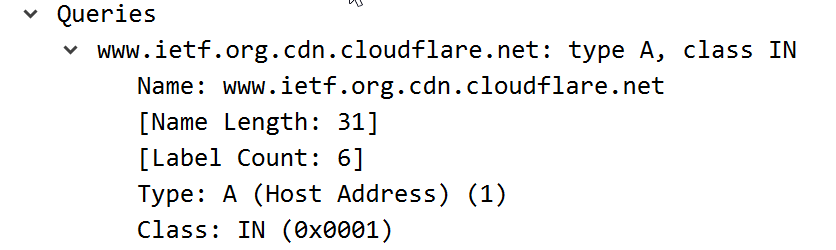
nslookup:



Ambas coinciden.

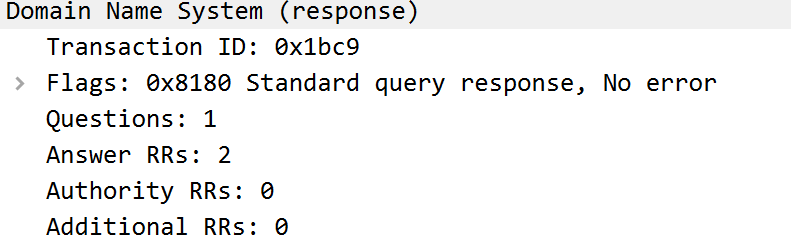
1. Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene el mensaje de petición alguna respuesta (answer)?

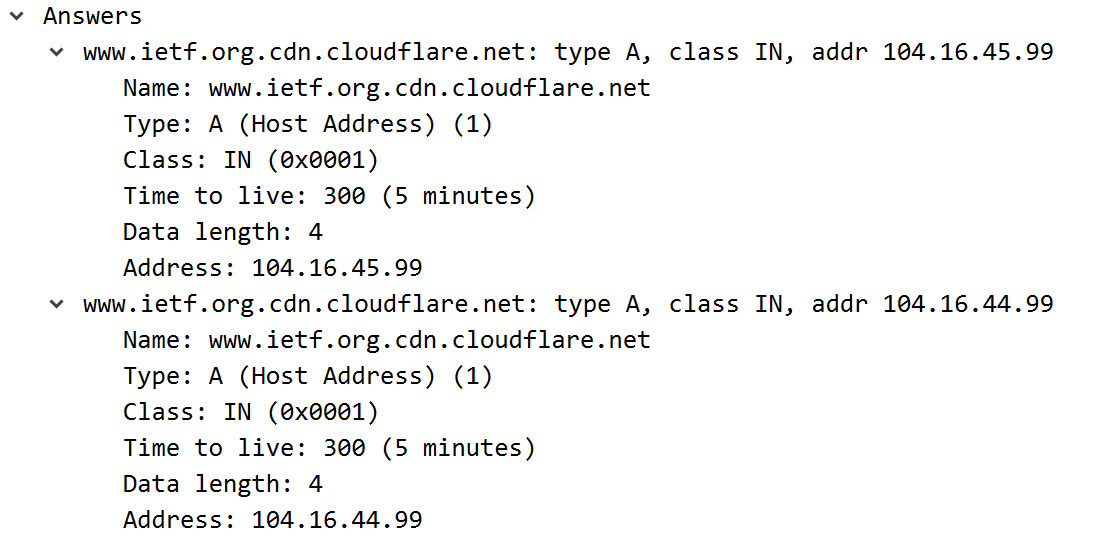
Es de tipo A, dado el nombre del servidor obtenemos su dirección IP. No contienen ninguna respuesta la petición.



1. Examina el mensaje de respuesta DNS. ¿Cuántas respuestas contiene? ¿Qué contiene cada una de esas respuestas?

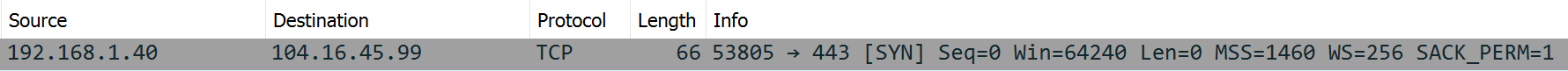
Contiene 2 respuestas, ambas sobre el mismo servidor, que nos proporcionan las IP que podemos utilizar para comunicarnos, 104.16.45.99 y 104.16.44.99.





1. Considera el siguiente paquete TCP SYN enviado por tu host. ¿Se corresponde la IP de destino a alguna de las direcciones IP contenidas en el mensaje de respuesta DNS?

El mensaje de SYN lo envía a la dirección 104.16.45.99, que era una de las respuestas a la petición.



1. Esta página web contiene imágenes. ¿Antes de descargar cada imagen se realizan nuevas peticiones DNS?

No, no se hace ninguna petición DNS más en el periodo capturado.

# Cuestiones escenario 2: nslookup

1. ¿Cuál es el puerto destino para el mensaje de petición DNS? ¿Cuál es el puerto origen del mensaje respuesta DNS?

Puerto destino de la petición: 53

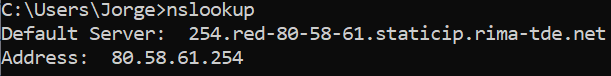
Puesto origen de la respuesta: 53



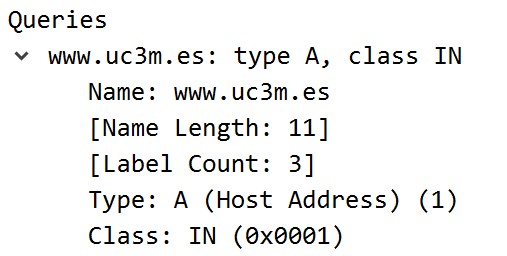
1. ¿A qué dirección IP se envía el mensaje de petición DNS? ¿Se corresponde esa IP con la configurada en el equipo para el servidor DNS por defecto?

La petición se envía a 80.58.61.254, que se corresponde con la por defecto del sistema.

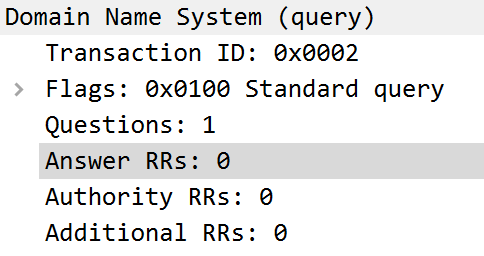




1. Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene dicho mensaje alguna respuesta (answer)?

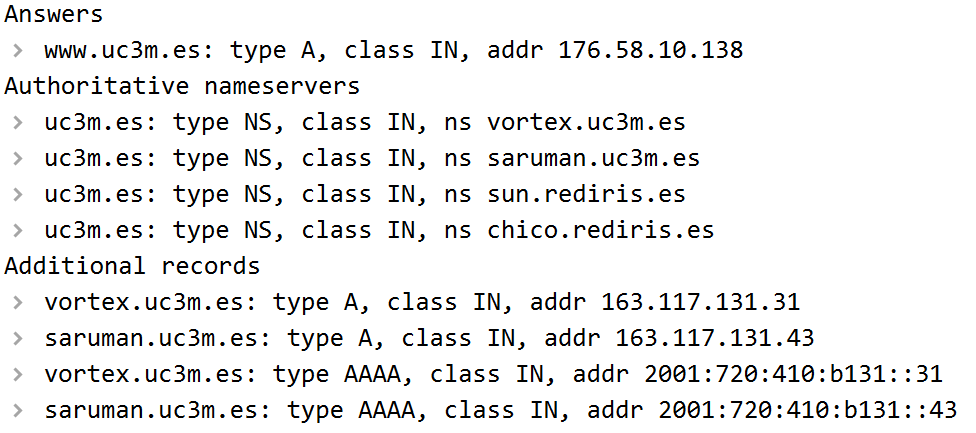
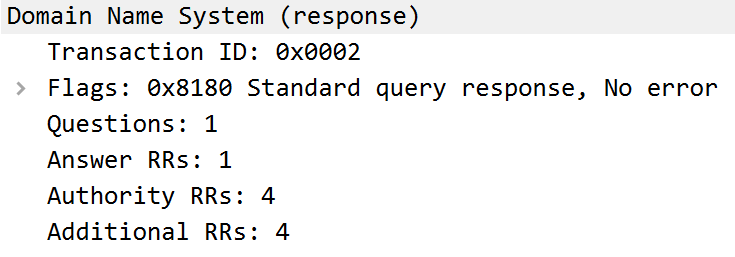
El registro es de tipo A, correspondencia nombre e IP. 

No contiene ninguna respuesta la petición.

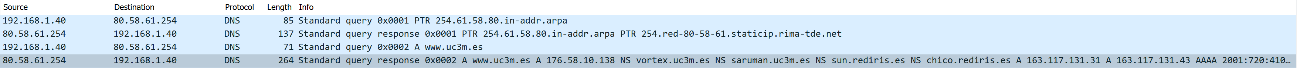


1. Examina el mensaje de respuesta DNS. ¿Cuántas respuestas contiene? ¿Qué contiene cada una de esas respuestas?

Contiene 1 respuesta, la dirección IP del nombre [www.uc3m.es](http://www.uc3m.es), y además contiene 4 nombres de servidores de nombres y las direcciones IPv4 y IPv6 de dos de ellos.



1. Adjunta una captura de pantalla



# Cuestiones escenario 3: nslookup

1. ¿A qué dirección IP se envía el mensaje de petición DNS? ¿Se corresponde esa IP con la configurada en el equipo para el servidor DNS por defecto?

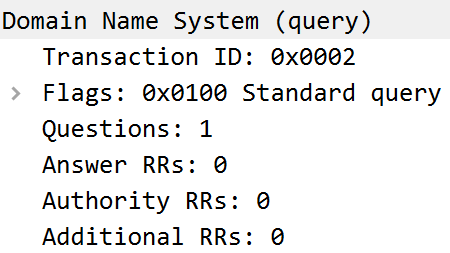
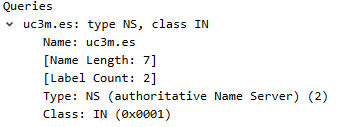
Se envía a la dirección 80.58.61.254. Se corresponde con la IP configurada en el equipo por defecto. 



1. Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene dicho mensaje alguna respuesta (answer)?

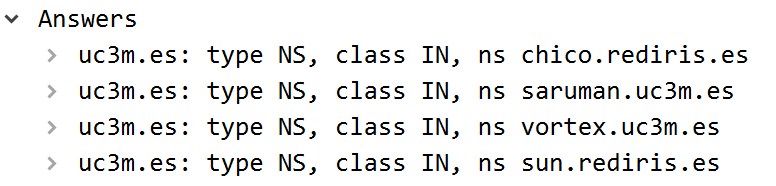
El registro es de tipo NS, que proporcionan la correspondencia del nombre de dominio con los servidores de nombres.

No contiene ninguna respuesta la petición.



1. Examina el mensaje de respuesta DNS. ¿Qué servidores de nombres aparecen en el mensaje de respuesta para la Universidad Carlos III? ¿Proporciona esta respuesta las direcciones IP de dichos servidores?

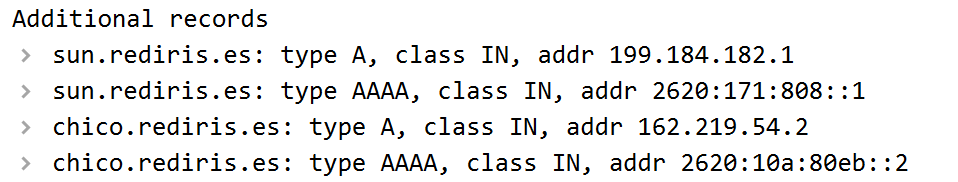
Servidores de nombres: vorteX.uc3m.es, saruman.uc3m.es, sun.rediris.es, chico.rediris.es



Proporciona las direcciones IPv4 y IPv6 de dos de ellos:

sun.rediris.es: 199.184.182.1 y 2620:171:808::1

chico.rediris.es: 162.219.54.2 y 2620:10a:80eb::2



1. Adjunta una captura de pantalla



# Cuestiones escenario 4: nslookup

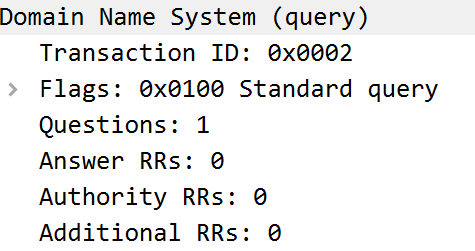
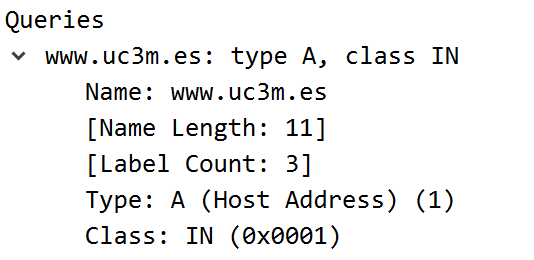
1. ¿A qué dirección IP se envía el mensaje de petición DNS? ¿Se corresponde esa IP con la configurada en el equipo para el servidor DNS por defecto? Si no lo es, ¿a qué dirección IP se corresponde?

La petición se envía a 163.117.131.31. No se trata de la que tiene por defecto el sistema, , ya que lo hemos especificado en el comando. La IP se corresponde al servidor de nombres, vortex.uc3m.es, con IP 163.117.131.31 que la hemos tenido que solicitar.



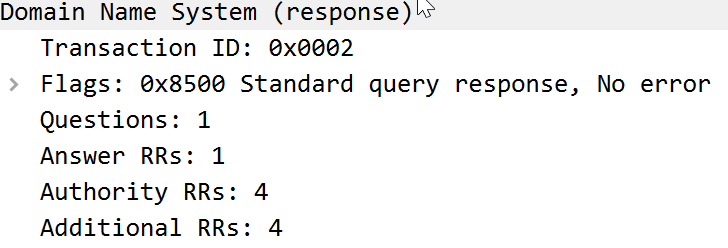
1. Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene dicho mensaje alguna respuesta (answer)?

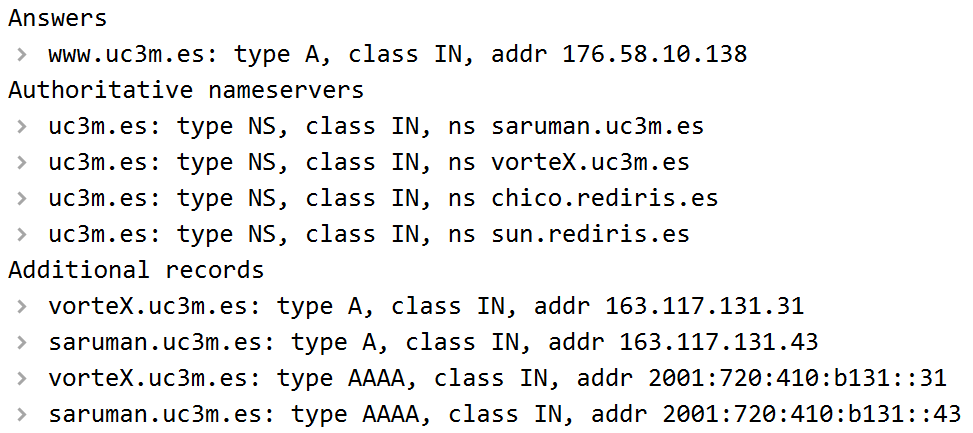
El registro es de tipo A, queremos la IP ligada al nombre [www.uc3m.es](http://www.uc3m.es). No contienen ninguna respuesta.



1. Examina el mensaje de respuesta DNS. ¿Cuántas respuestas contiene? ¿Qué contiene cada una de esas respuestas?

Contiene una sola respuesta, la dirección IP del nombre de dominio solicitado, 176.58.10.138. Aunque también incluye los servidores de nombre y algunas de sus direcciones IP.





1. Adjunta una captura de pantalla

