
Universidad Carlos III de Madrid
Departamento de Ingeniería Telemática

Redes de Ordenadores

Práctica de concepto 1 – DNS

Grado en Ingeniería Informática

1. Objetivo

El objetivo de esta práctica es profundizar en el conocimiento del protocolo DNS, utilizando aplicaciones del sistema operativo (*nslookup*, *ipconfig*, *ifconfig*) así como un capturador de tráfico / analizador de paquetes (*Wireshark*).

2. Descripción

DNS juega un papel fundamental en el uso que hacemos de Internet, ya que su misión consiste en traducir los nombres de host a sus direcciones IP correspondientes. Esto nos facilita, entre otras cosas, recordar las direcciones de sitios web al permitir representar los hosts una forma intuitiva en el ámbito global de la red de redes.

Con el objetivo de hacer esta práctica fácil de realizar se han elegido una serie de aplicaciones existentes en los sistemas operativos *GNU Linux* y *Microsoft Windows* (la práctica puede hacerse en ambos sistemas operativos).

En primer lugar se explicará brevemente cómo utilizar la aplicación **nslookup**, relacionada con peticiones DNS. Tras dicha explicación y algunos ejemplos, se presentarán una serie de cuestiones a resolver. Seguidamente se explicarán las aplicaciones **ifconfig** (Linux) e **ipconfig** (Windows), relacionadas con la configuración del adaptador de red en los diferentes sistemas operativos. Finalmente se procederá a realizar una serie de capturas de tráfico con **Wireshark** a fin de analizar el comportamiento del protocolo DNS cuando se realizan peticiones a los servidores de nombres. Tras este punto se presentarán el resto de cuestiones evaluables para aprobar la práctica.

2.1. nslookup

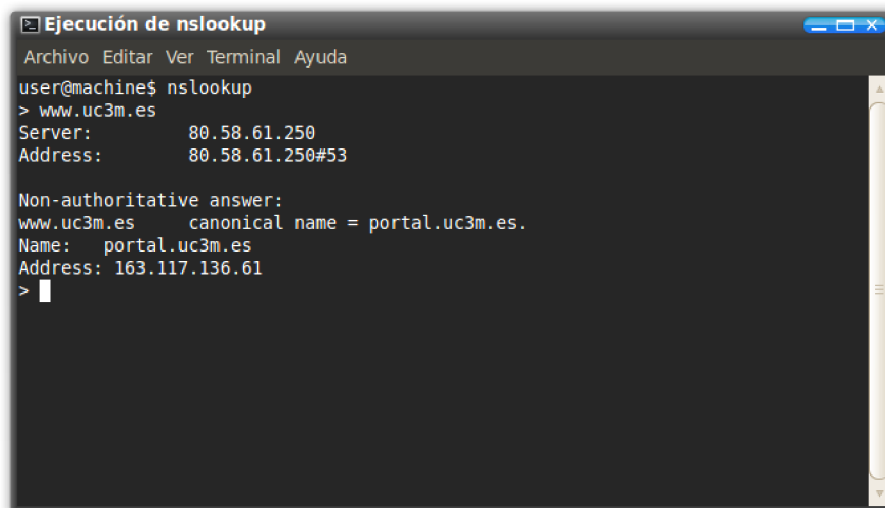
La aplicación *nslookup*, presente en diversos sistemas operativos, permite preguntar a los servidores de nombres del *Domain Name System* (DNS) por registros DNS, a fin de conocer, por ejemplo, la dirección IP de un servidor en base a su nombre, o si el DNS que tenemos configurado está funcionando correctamente. En este apartado vamos a aprender a utilizar la aplicación **nslookup** y a realizar pruebas con ella para averiguar la dirección IP de algunos servidores en Internet.

Para ejecutar **nslookup** sólo hay que hacer lo siguiente:

- En **GNU Linux utilizando Gnome** como gestor de ventanas
 - Pulsar **Alt+F2**
 - Escribir **gnome-terminal** y pulsar **intro**
 - Escribir en el terminal **nslookup** y pulsar **intro**.
- En **Microsoft Windows**
 - Pulsar el **botón de inicio**

- Si es *Windows XP o anterior*, pulsar **ejecutar**
- Si es *Vista o superior*, hacer **click** en el **campo de búsqueda**
- Escribir **cmd** y pulsar **intro**
- Escribir en la consola de comandos **nslookup** y pulsar **intro**.

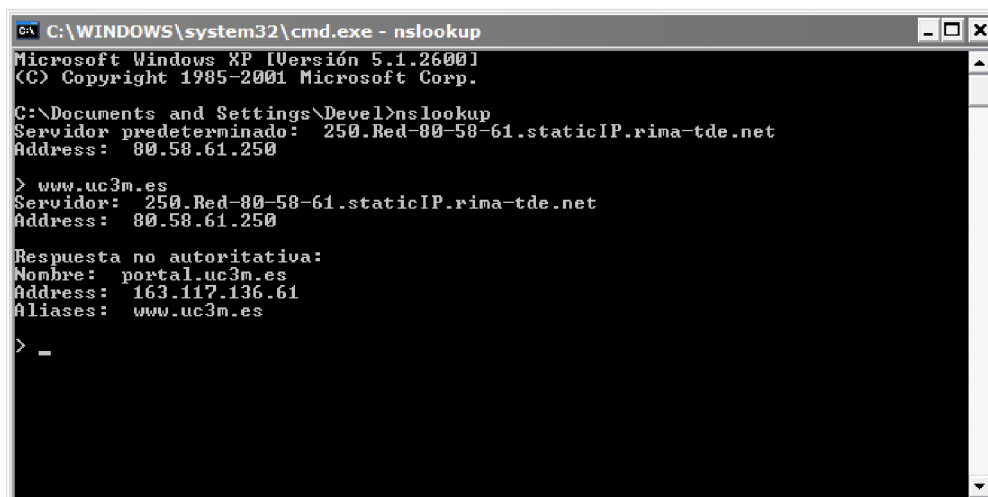
A continuación se muestran un par de capturas con la ejecución de nslookup y la resolución de la dirección IP para el sitio www.uc3m.es en GNU Linux y en Microsoft Windows.

A terminal window titled "Ejecución de nslookup" showing the execution of the nslookup command in a Linux environment. The prompt is "user@machine\$". The user enters "nslookup", followed by "> www.uc3m.es". The output shows the server address as 80.58.61.250 and the canonical name as portal.uc3m.es with its IP address 163.117.136.61.

```
Ejecución de nslookup
Archivo Editar Ver Terminal Ayuda
user@machine$ nslookup
> www.uc3m.es
Server:      80.58.61.250
Address:     80.58.61.250#53

Non-authoritative answer:
www.uc3m.es  canonical name = portal.uc3m.es.
Name:   portal.uc3m.es
Address: 163.117.136.61
>
```

Fig. - Ejecución de nslookup en Linux

A Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe - nslookup" showing the execution of the nslookup command. The prompt is "C:\Documents and Settings\Devel>". The user enters "nslookup", followed by "> www.uc3m.es". The output shows the server address as 250.Red-80-58-61.staticIP.rima-tde.net and the canonical name as portal.uc3m.es with its IP address 163.117.136.61.

```
C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Devel>nslookup
Servidor predeterminado: 250.Red-80-58-61.staticIP.rima-tde.net
Address: 80.58.61.250

> www.uc3m.es
Servidor: 250.Red-80-58-61.staticIP.rima-tde.net
Address: 80.58.61.250

Respuesta no autoritativa:
Nombre: portal.uc3m.es
Address: 163.117.136.61
Aliases: www.uc3m.es
> _
```

Fig. - Ejecución de nslookup en Windows

Para finalizar la ejecución de **nslookup**, sólo hay que escribir **exit** y pulsar **intro**.

En las capturas se puede apreciar que el cliente está utilizando la infraestructura de *Telefónica de España*, donde el servidor predeterminado es **80.58.61.250**. Si se ejecuta el comando nslookup sin

especificar el servidor DNS, entonces se manda la petición al servidor DNS configurado por defecto en el sistema operativo (ver apartado 2.2).

Existen varias formas de ejecutar nslookup. Ahora vamos a ver algunas de ellas:

nslookup nombre_de_host

Ejemplo: **nslookup www.uc3m.es**

Al ejecutar este comando, nslookup está pidiendo al servidor de nombres por defecto “*por favor, envíame la dirección IP para el host www.uc3m.es*”. Como se puede apreciar en las anteriores capturas de pantalla, la respuesta a este comando muestra dos tipos de información:

1. El nombre y la dirección IP del servidor DNS que proporciona la respuesta.
2. La respuesta en sí, que consiste en el nombre y la dirección IP de www.uc3m.es.

nslookup -type=tipo_registro nombre_de_dominio

Ejemplo: **nslookup -type=NS uc3m.es**

En el ejemplo se ha utilizado como tipo de registro **NS (Name Servers)**, es decir, se han solicitado los registros correspondientes a los servidores de nombres para el dominio uc3m.es (*authoritative servers*). Al igual que en el caso anterior, la respuesta muestra una serie de tipos de información:

1. El nombre y la dirección IP del servidor DNS que proporciona la respuesta.
2. Los servidores de nombres del dominio sobre el que se ha preguntado. Aunque estos sean *authoritative servers* para dicho dominio, se puede dar el caso que en la respuesta aparezca *non-authoritative*. Esto es así porque la respuesta a nuestra *query* procede de la caché de algún servidor en lugar de venir de algún servidor de tipo *authoritative*.
3. La dirección IP de los *authoritative servers*.

nslookup nombre_de_host servidor_DNS

Ejemplo: **nslookup www.uc3m.es vortex.uc3m.es**

En el ejemplo se está indicando a nslookup que envíe la petición al servidor DNS pasado por parámetro (vortex.uc3m.es). De esta forma, la petición DNS se ejecutará sobre ese servidor en lugar del servidor configurado por defecto en el sistema operativo.

NOTA: para ver las diferentes opciones soportadas por nslookup, ejecutar nslookup, y en el *prompt* de la aplicación (>) introducir **help** y pulsar **intro**. También puede resultar útil la siguiente referencia: <http://elouai.com/nslookup-reference.php>

NOTA2: existe otra herramienta más avanzada que `nslookup` utilizada para el mismo propósito. Su nombre es “**dig**” (*Domain Information Groper*) y aunque viene por defecto en muchas de las distribuciones GNU Linux, no lo hace con los sistemas operativos de Microsoft. Es por ello el motivo de elegir **nslookup** en lugar de **dig** para la realización de la práctica.

2.1.1. Cuestiones (parte 1 de 5)

- 1) Ejecuta `nslookup` para obtener la dirección IP del dominio de la **Agencia Tributaria Española**.
- 2) Ejecuta `nslookup` para obtener los *authoritative servers* de **Yahoo**.
- 3) Ejecuta `nslookup` para determinar los servidores de correo de la **Universidad Carlos III**.

2.2. ifconfig / ipconfig

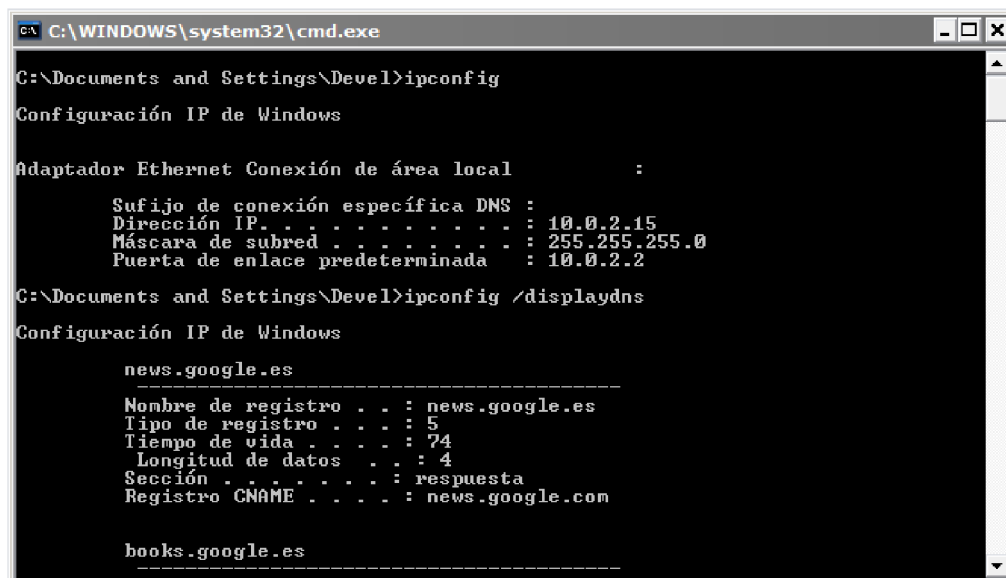
Las aplicaciones de línea de comandos **ifconfig** (*GNU Linux / UNIX*) e **ipconfig** (*Windows*) permiten, entre otras cosas, mostrar información específica, como la correspondiente a la configuración de TCP/IP, los servidores DNS configurados, la dirección física, etc. de uno o varios adaptadores de red pertenecientes al equipo en el que se ejecuta el comando.

2.2.1. ipconfig

Al igual que `nslookup`, existen varias formas de ejecutar `ipconfig`. A continuación se mostrarán algunas opciones que pueden resultar útiles:

ipconfig /all

Muestra la información completa para todos los adaptadores del sistema. Esto es, aparte del nombre y tipo de adaptador, muestra la información de configuración TCP/IP (IP, máscara, puerta de enlace predeterminada), los servidores DNS configurados, posible duración de concesiones (*leases*) DHCP, etc.



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Devel>ipconfig

Configuración IP de Windows

Adaptador Ethernet Conexión de área local :

    Sufijo de conexión específica DNS :
    Dirección IP. . . . . : 10.0.2.15
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada : 10.0.2.2

C:\Documents and Settings\Devel>ipconfig /displaydns

Configuración IP de Windows

    news.google.es
    -----
    Nombre de registro . . : news.google.es
    Tipo de registro . . . : 5
    Tiempo de vida . . . . : 74
    Longitud de datos . . . : 4
    Sección . . . . . : respuesta
    Registro CNAME . . . . : news.google.com

    books.google.es
    -----
```

Fig. - Ejemplo de ejecución ipconfig

`ipconfig /displaydns`

Muestra las entradas almacenadas en la caché local de DNS junto con su tiempo de vida (TTL) o de validez, tipo de registro, longitud de los datos, etc.

`ipconfig /flushdns`

Vacía todas las entradas de la caché local de DNS y una vez hecho eso, carga las entradas almacenadas en fichero de hosts.

2.2.2. `ifconfig`

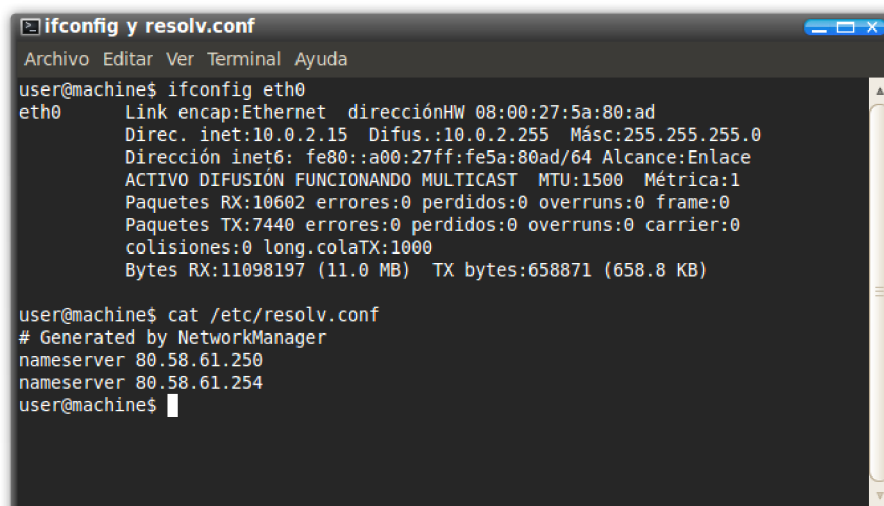
Para *ifconfig* también existen una serie de parámetros que pueden resultar de utilidad. Muchos de ellos requieren privilegios administrativos (superusuario) para poder ser ejecutados, pero en concreto, los que sirven para obtener información de uno o varios adaptadores se pueden utilizar desde cualquier usuario del sistema.

Si escribimos en un terminal `ifconfig` y pulsamos **intro**, obtendremos la lista de los adaptadores de red del sistema y su configuración asociada.

Si escribimos en el terminal `ifconfig nombre_adaptador`, lo que obtendremos será únicamente la configuración del adaptador de red cuyo nombre es "*nombre_adaptador*".

Para conocer las *direcciones de los servidores DNS configurados* en el sistema en la mayoría de las distribuciones GNU Linux, se puede consultar el fichero `/etc/resolv.conf`. O lo que es lo mismo, ejecutar en un terminal `cat /etc/resolv.conf`

Una forma de limpiar la caché DNS almacenada en el sistema consiste en reiniciar el servicio de red. Para ello hacen falta permisos de superusuario. Para reiniciar el servicio de red, escribir en un terminal `sudo /etc/init.d/networking restart`. Hay que tener en cuenta que *en los laboratorios no se disponen de los permisos necesarios* para llevar a cabo esta acción.



```
ifconfig y resolv.conf
Archivo Editar Ver Terminal Ayuda
user@machine$ ifconfig eth0
eth0      Link encap:Ethernet  direcciónHW 08:00:27:5a:80:ad
          Direc. inet:10.0.2.15  Difus.:10.0.2.255  Másc:255.255.255.0
          Dirección inet6: fe80::a00:27ff:fe5a:80ad/64 Alcance:Enlace
          ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
          Paquetes RX:10602 errores:0 perdidos:0 overruns:0 frame:0
          Paquetes TX:7440 errores:0 perdidos:0 overruns:0 carrier:0
          colisiones:0 long.colaTX:1000
          Bytes RX:11098197 (11.0 MB)  TX bytes:658871 (658.8 KB)

user@machine$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 80.58.61.250
nameserver 80.58.61.254
user@machine$
```

Fig. - Ejecución de `ifconfig` y consulta de `resolv.conf`

2.3. Captura de tráfico DNS con Wireshark

Wireshark es un potente analizador de paquetes y capturador de tráfico *open source* y multiplataforma. Puede obtenerse gratuitamente desde: <http://www.wireshark.org/download.html>

En este apartado lo vamos a utilizar para observar el comportamiento del protocolo DNS en varios escenarios.



Fig. - Ventana principal de Wireshark v1.2.7 en GNU Linux

NOTA: Normalmente para realizar capturas de paquetes hace falta cambiar el modo de funcionamiento del adaptador de red a lo que se conoce como modo “*promiscuo*”. *Wireshark* lleva a cabo esta acción de manera automática (siempre que el adaptador lo soporte), pero para ello requiere permisos de administrador. En los laboratorios de Telemática se han configurado una serie de políticas de seguridad de forma que los alumnos puedan capturar paquetes mediante *Wireshark* (al menos en las cuentas de Linux). Para ejecutar *Wireshark*, ejecutar en un terminal:

```
xhost +  
sudo wireshark
```

En cualquier caso se *recomienda la instalación de la aplicación en los PCs propios para evitar problemas.*

2.3.1. Escenario 1: *Web-surfing*

En este apartado vamos a realizar una captura de tráfico mientras accedemos a una dirección web mediante un navegador de Internet. Una vez realizada la captura, analizaremos los resultados.

Pasos a seguir:

1. Abrir un navegador (Internet Explorer, Firefox, Opera, IceApe...) y limpiar la caché.
2. Limpiar la caché DNS del sistema, ya sea mediante *ipconfig* o *reiniciando el servicio de red*.
3. Abrir *Wireshark* e introducir "*ip.addr==ip_del_equipo*" en el campo **filtro**, donde *ip_del_equipo* es la IP asociada al computador en el que se está ejecutando *Wireshark*. Este filtro elimina los paquetes que ni son originados ni están destinados al equipo.
4. Iniciar la captura de paquetes con Wireshark.
5. Con el navegador, visitar la dirección: <http://www.ietf.org>
6. Detener la captura de paquetes.

NOTA: si no se ha visitado previamente el sitio, no hace falta llevar a cabo los pasos 1 y 2.

2.3.2. Cuestiones (parte 2 de 5): *Web-surfing*

- 4) Localiza los mensajes de petición y respuesta DNS. ¿Son enviados sobre TCP o sobre UDP?
- 5) ¿Cuál es el puerto de destino para el mensaje de petición DNS? ¿Cuál es el puerto de origen del mensaje respuesta?
- 6) ¿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?
- 7) Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene el mensaje de petición alguna respuesta (*answer*)?
- 8) Examina el mensaje de respuesta DNS. ¿Cuántas respuestas contiene? ¿Qué contiene cada una de esas respuestas?
- 9) 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?
- 10) Esta página web contiene imágenes. ¿Antes de descargar cada imagen se realizan nuevas peticiones DNS?

2.3.3. Escenario 2: *nslookup*

Ahora vamos a probar con *nslookup*. Sigue las siguientes instrucciones:

1. Comienza una captura de paquetes nueva, indicando el mismo filtro que en el escenario 1 (*ip.addr==ip_del_equipo*).
2. Introduce en un terminal el comando **nslookup www.uc3m.es**
3. Detén la captura de paquetes.

Deberías obtener una traza parecida a la que se muestra en la siguiente captura de pantalla.

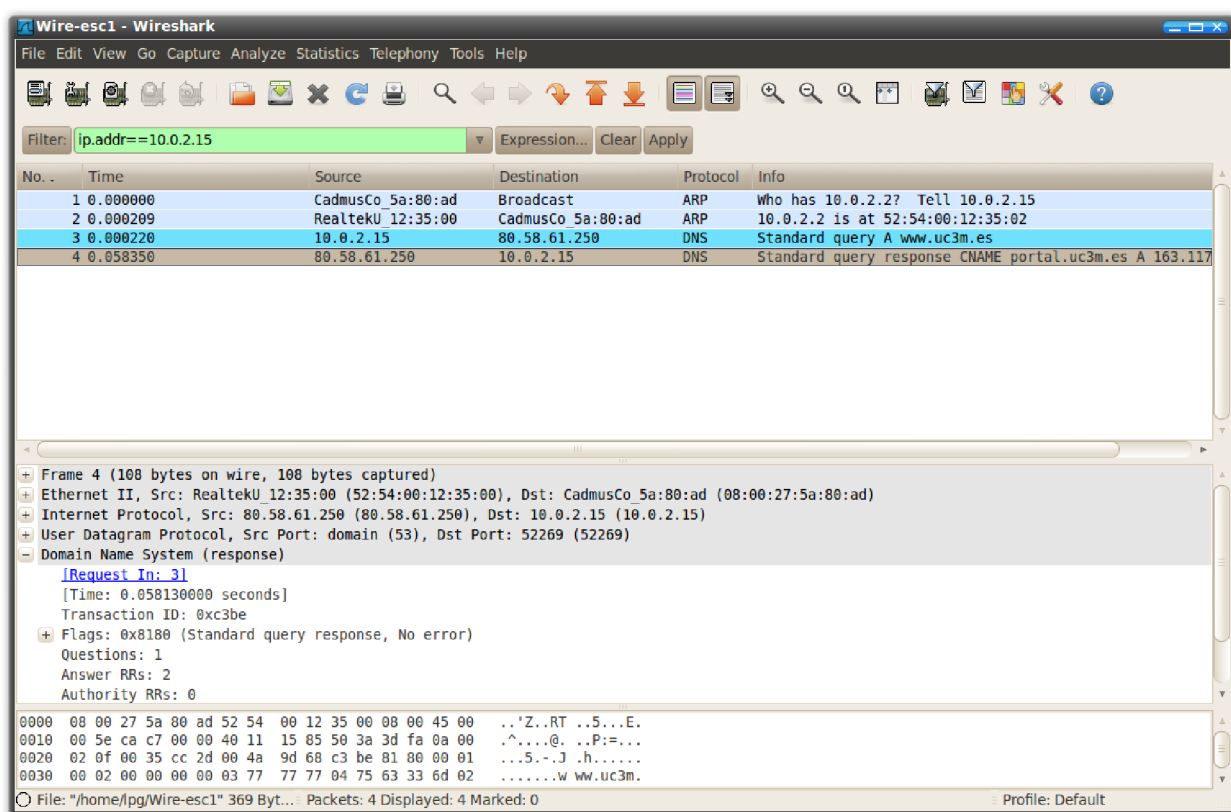


Fig. - Traza del escenario 2 en Wireshark

2.3.4. Cuestiones (parte 3 de 5): *escenario 2 (nslookup)*

- 11) ¿Cuál es el puerto destino para el mensaje de petición DNS? ¿Cuál es el puerto origen del mensaje respuesta DNS?
- 12) ¿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?
- 13) Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene dicho mensaje alguna respuesta (*answer*)?

- 14) Examina el mensaje de respuesta DNS. ¿Cuántas respuestas contiene? ¿Qué contiene cada una de esas respuestas?
- 15) Adjunta una captura de pantalla.

2.3.5. Escenario 3: *nslookup*

Repite el experimento del escenario 2, pero en esta ocasión utiliza el comando:

nslookup -type=NS uc3m.es

2.3.6. Cuestiones (parte 4 de 5): *escenario 3 (nslookup)*

- 16) ¿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?
- 17) Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene dicho mensaje alguna respuesta (*answer*)?
- 18) 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?
- 19) Adjunta una captura de pantalla.

2.3.7. Escenario 4: *nslookup*

Repite el experimento del escenario 3, pero en esta ocasión utiliza el comando:

nslookup www.uc3m.es vortex.uc3m.es

2.3.8. Cuestiones (parte 5 de 5): *escenario 4 (nslookup)*

- 20) ¿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?
- 21) Examina el mensaje de petición DNS. ¿De qué tipo es el registro DNS? ¿Contiene dicho mensaje alguna respuesta (*answer*)?
- 22) Examina el mensaje de respuesta DNS. ¿Cuántas respuestas contiene? ¿Qué contiene cada una de esas respuestas?
- 23) Adjunta una captura de pantalla.

3. Entrega

- Para considerar la práctica válida, se deberán contestar **correctamente al menos 12** cuestiones.
- Las respuestas a las cuestiones se entregarán mediante un formulario online en la actividad habilitada al efecto en Aula Global 2.
- Las capturas de pantalla realizadas durante la práctica se adjuntarán en un documento pdf y se entregará en la actividad habilitada al efecto en Aula Global 2. El nombre de dicho fichero debe seguir el siguiente formato:

RO-PdC1-[Campus][Grupo]-[NIA].pdf

Tal que:

Campus	letra 'L' o 'C' correspondiente al campus (<i>Leganés</i> o <i>Colmenarejo</i>).
Grupo	grupo (80, 81, 82, 83, 84, 85, 89).
NIA	número identificador del alumno.

Ejemplo válido: **RO-PdC1-L81-100055221.pdf**