PRÁCTICA 1: LAS APLICACIONES WEB y DNS

El objetivo de esta práctica es que conozcas a nivel básico el funcionamiento de dos aplicaciones muy utilizadas: la aplicación Web y la aplicación DNS. En particular, que te familiarices con su arquitectura y protocolos de aplicación. Para ello deberás leer detenidamente el libro de referencia y utilizar un programa analizador de protocolos (wireshark) para capturar los mensajes intercambiados entre los procesos de las aplicaciones distribuidas.

REQUISITOS ANTES DE COMENZAR LA PRÁCTICA 1

Para cumplir con los objetivos de aprendizaje es importante que cumplas todos los requisitos indicados antes de comenzar la realización de la práctica.

REQ #1. (45min). **Instalar el programa wireshark y realizar la práctica de familiarización con Wireshark (Practica0)**.

El software que vas a utilizar para analizar los mensajes intercambiados entre los procesos de aplicación se llama Wireshark. Después de haber realizado la práctica 0, debes dominar a nivel básico su funcionamiento y configuración. Recuerda que Wireshark captura todas las tramas que pasan por una de las tarjetas de red (NIC) de tu ordenador, y sabe interpretar y mostrarte las cabeceras de la mayoría de protocolos usados en la actualidad, incluyendo protocolos de nivel de enlace, red, transporte y aplicación. Por supuesto, HTTP y DNS se encuentran dentro de los protocolos de aplicación que sabe interpretar Wireshark.

REQ #2. (1hora). **Leer y entender la sección 2.2 del libro de referencia (La Web y http)**. Para ayudarte a discernir las ideas más importantes de la sección también puedes leer las transparencias que se encuentran al final del tema02 y que utilizará el profesor en la sesión de apoyo de la práctica. Si te quedan dudas, puedes resolverlas en la práctica.

REQ #3 (30min). **Leer y entender la sección 2.5 del libro de referencia (DNS** – El Servicio de Directorio de Internet). Para ayudarte a discernir las ideas más importantes de la sección también puedes leer las transparencias que utilizará el profesor en la sesión de apoyo de la práctica. Si te quedan dudas, puedes resolverlas en la práctica.

---------- PARTE I: LA APLICACIÓN WEB ----------

FUNDAMENTOS TEÓRICOS

Los indicados en la sección 2.2 del libro. Para profundizar en detalles del protocolo se puede consultar la norma RFC2612 si fuese necesario.

EJERCICIOS

A) INTERACCIÓN BÁSICA

Comenzaremos explorando el protocolo HTTP descargándonos un fichero HTML sencillo (no contiene referencias a otros objetos dentro de la página, como imágenes, etc…) de un servidor web. Haz lo siguiente:

1. Arranca un navegador (cliente del protocolo HTTP).
2. Arranca el analizador de protocolos Wireshark (req#1) *(no comiences la captura de paquetes todavía)*. Escribe "http" (sólo las letras, sin "") en el campo de fitrado para que sólo se vean los mensajes del protocolo HTTP en la ventana de captura de paquetes.
3. Espera un minuto y después comienza la captura de paquetes en Wireshark.
4. Introduce la siguiente dirección en el navegador: http://masai.us.es/index.html
5. Ya puedes parar la captura de paquetes en Wireshark.

La ventana de Wireshark debería ser parecida a la mostrada en la Figura 1.

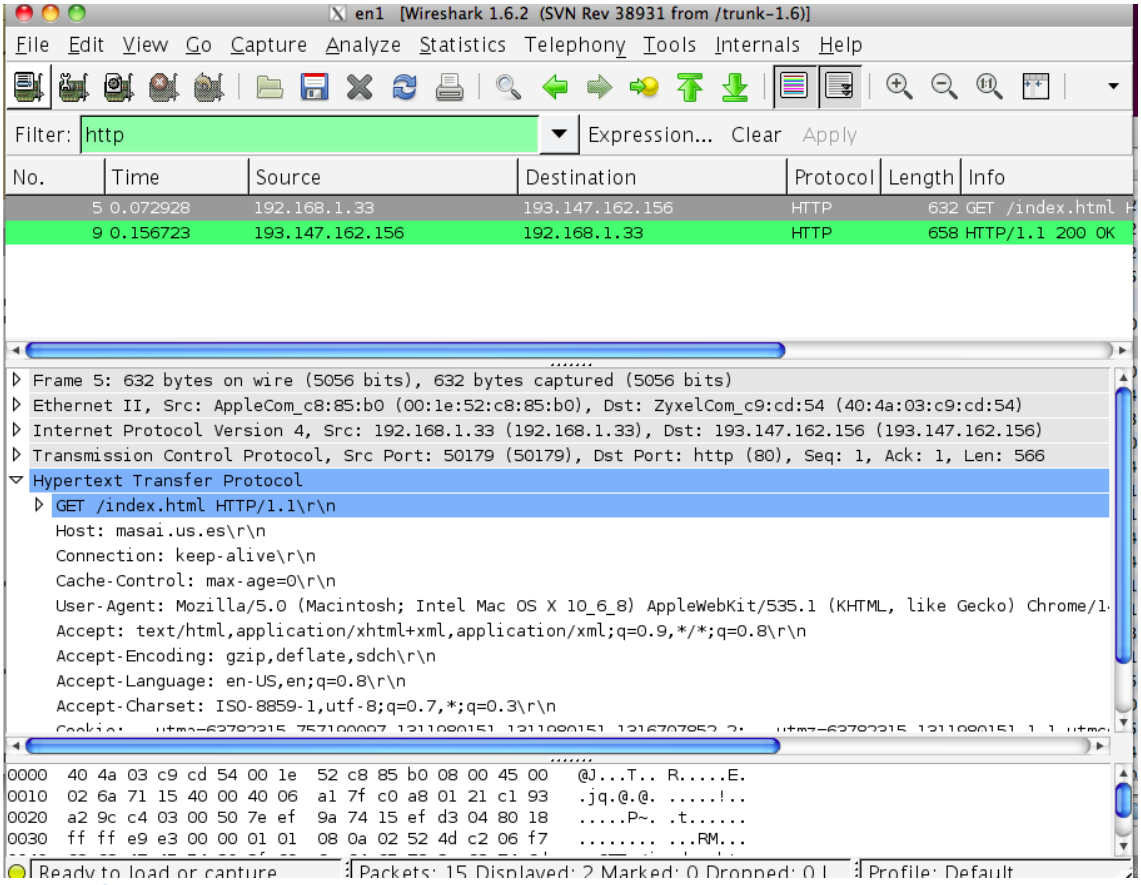

Ilustración 1. Captura de pantalla de Wireshark

Los paquetes capturados deberían mostrar tanto la petición (mensaje GET) como la correspondiente respuesta. En el ejemplo mostrado en la Figura 1, se puede apreciar el contenido del mensaje GET (desde tu navegador hacia el servidor `masai.us.es`).

Recuerda que los mensajes del protocolo de aplicación HTTP van encapsulados dentro de segmentos TCP, los cuales a su vez viajan encapsulados dentro de datagramas IP, que a su vez viajan dentro de las tramas Ethernet o WiFi (según la NIC que hayas utilizado para conectarte a Internet). Wireshark muestra apiladas las cabeceras de todos estos protocolos, pero nosotros ahora estamos interesados principalmente en analizar la información del protocolo de aplicación HTTP, por lo tanto, en principio minimizaremos la información mostrada sobre el resto de protocolos.

Puede que en tu captura no aparezcan sólo mensajes idénticos a los mostrados en la Figura 1. Ten en cuenta varias cosas para explicar esto:

(a) Wireshark captura todo el tráfico que lea la tarjeta de red y por lo tanto, en un enlace de acceso múltiple puedes capturar paquetes de otros compañeros (a eso se le llama modo de funcionamiento promiscuo). Para averiguar cuál es la IP de tu ordenador puedes utilizar el comando `ipconfig /all` en Windows o en Linux `/sbin/ifconfig`. Puedes indicar en el filtro de Wireshark que sólo incluya los paquetes con origen o destino en tu ordenador con el filtro " http && ip.addr==193.147.162.146" (donde 193.147.162.146 debe ser reemplazado con la IP de tu ordenador).

(b) Si no obtienes al menos, los dos mensajes anteriores (GET y 200 OK), puede que tu navegador ya haya guardado la página (si lo has intentado anteriormente) en su caché local y ahora utilice la cabecera conditional-get para asegurarse de su copia local esta actualizada. Para solucionar esto, simplemente debes decirle al navegador que borre los datos en su caché.

(c) Puede que el navegador solicite otro GET buscando el objeto favicon.ico. Esto es simplemente la referencia a un icono que se mostrará en el navegador al lado de la dirección web. Simplemente ignora este mensaje y su correspondiente respuesta.

(d) Recuerda que puedes decirle a Wireshark que ignore los paquetes que desees. Para ello selecciona un paquete en la ventana donde se listan los paquetes capturados y, con el botón derecho del ratón, puedes indicar que se elimine (ignore) dicho paquete de la lista mostrada.

Si después de 10 minutos no logras tener una captura satisfactoria, puedes descargarte un archivo de capturas de http://masai.us.es/practica1/Bloque1captura. Carga este archivo con tu Wireshark para continuar la práctica (menú Archivo/File). **Aún así, pregúntale al profesor el día de la práctica para averiguar por qué no has logrado hacer la captura. En el examen de prácticas seguramente tendrás que realizar capturas y no podrás preguntarle al profesor**.

Inspecciona la información del primer mensaje HTTP GET y su correspondiente respuesta. Recuerda que el protocolo se encuentra definido en la norma RFC 2616 y que siempre puedes consultar dicha norma ante dudas. También puedes consultar otras puentes como wikipedia (p.ej. https://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol) o w3c. Cuando estés respondiendo deberías tener visible el contenido de ambos mensajes (petición y respuesta), e indicar en qué parte del mensaje (campo del mensaje) has encontrado la respuesta a las siguientes preguntas.

1. ¿Tu navegador esta ejecutando la versión del protocolo HTTP 1.0 o 1.1? ¿Qué versión del protocolo HTTP esta ejecutando el servidor?
2. ¿Qué idiomas preferiría el navegador en los documentos solicitados?
3. ¿Cuál es la dirección IP de tu ordenador?¿cuál es la dirección IP del servidor Web?
4. ¿Cuál es el código de estado (status code) indicado en la respuesta del servidor?
5. ¿Cuándo ha sido modificado por última vez el objeto index.html en el servidor?
6. ¿Cuántos bytes de "contenido" viajan en el mensaje de respuesta del servidor? (el "contenido" es el campo *cuerpo del mensaje*, donde viaja encapsulado el objeto solicitado por el cliente)
7. ¿Qué frases puedes observar en el texto HTML del contenido del mensaje que hayas visto a través del navegador?
8. Observa que en el objeto que viaja como contenido dentro del cuerpo del mensaje existen marcas del lenguaje HTML. Por ejemplo la marca <H1> indica que lo que se escriba después debe representarse en el navegador con un tamaño de letra apropiado para una cabecera. </H1> indica el final de la marca. ¿Qué otras marcas observas en el objeto?

B) LA INTERACCIÓN GET/RESPUESTA CON CONDITIONAL GET

Además de los proxys o caché web, los navegadores también tienen su caché local donde almacenan los objetos que reciben de los servidores. Antes de continuar esta práctica, asegúrate de borrar la caché del navegador que estés usando (para hacer esto en *Internet Explorer*, selecciona *Tools->Internet Options ->Delete file*; en *Firefox* selecciona Tools ->*Clear Private Data*). Ahora haz lo siguiente.

- Arranca el navegador y asegúrate de borrar su caché local.
- Arranca Wireshark (si lo habías cerrado) y comienza una nueva captura de paquetes.
- Introduce la siguiente dirección en el nagevador: http://masai.us.es/index.html . El navegador mostrará la página del ejercicio anterior.
- Rápidamente, haz click en el botón de refrescar la página actual (o reescribe la misma dirección) en el navegador.
- Para la captura de paquetes en WireShark, e introduce "http" en la ventana de filtrado, para que sólo se muestren los paquetes capturados que contengan mensajes del protocolo HTTP.

Nota: si no logras realizar la captura satisfactoriamente después de 5 min., puedes descargártela de http://masai.us.es/practica1/Bloque2captura No olvides preguntar al profesor que te explique por qué no has podido realizar la captura.
Responde a las siguientes preguntas:

9. Inspecciona el contenido de la primera petición HTTP GET del navegador. ¿Ves la línea de cabecera "IF-MODIFIED-SINCE" en dicha petición?
10. Inspecciona el contenido de la primera respuesta del servidor (respuesta a la petición anterior). Mira el cuerpo del mensaje. ¿Devuelve el servidor la página web solicitada en su respuesta?

11. Ahora inspecciona el contenido de la segunda petición HTTP GET del navegador. ¿Ves una línea de cabecera "IF-MODIFIED-SINCE"? ¿qué información viaja como valor de la cabecera?
12. ¿Cuál es el código de estado y la frase devuelta como respuesta en el servidor a la segunda petición HTTP GET? ¿devuelve el servidor explícitamente el objeto solicitado en su respuesta?

C) PETICIÓN DE DOCUMENTOS QUE CONTIENEN REFERENCIAS A OTROS OBJETOS

En los ejemplos anteriores, la página web solicitada consiste en un único objeto (un único fichero html de pequeño tamaño). Veamos qué ocurre cuando solicitamos un documento de mayor tamaño que a su vez incluye referencias a varios objetos.

Haz lo siguiente.

- Arranca el navegador y asegúrate de que borras su caché local.
- Arranca WireShark (si lo habías cerrado) y comienza una nueva captura de paquetes.
- Introduce la siguiente dirección en el nagevador: http://masai.us.es/research/ . El navegador mostrará una página web que incluye una referencia a varios objetos de tipo imagen.
- Para la captura de paquetes en WireShark y asegúrate de que sólo se muestran los paquetes con información del protocolo HTTP.

Nota: si no has logrado realizar la captura en 5 min., puedes descargarte una de http://masai.us.es/practica1/Bloque3captura **.Aún así, pregúntate por qué no has logrado hacer la captura ya que tu problema persiste**.

Ahora responde a las siguientes preguntas:

13. ¿cuántas peticiones GET han sido realizadas por parte del navegador?¿qué objeto se pedía en cada petición?¿el servidor ha respondido positivamente a todas las peticiones?
14. Cuantas tramas han tenido que ser recibidas por el cliente para obtener toda la página web solicitada (documento en html más todos los objetos referenciados en la página)? (fíjate en la línea justo entre el comienzo del texto de la cabecera HTTP y TCP para ver si la información mostrada ha sido consecuencia del reensamblaje de varios segmentos o no). ¿qué tamaño en bytes tiene la página web recibida?.

Nota: ten en cuenta que la respuesta del documento base (.html) requiere de la recepción y reensamblado de múltiples paquetes lo que puede provocar que en wireshark se muestren mensajes aparentemente fuera del orden lógico ya que un mensaje no se mostrará como completamente recibido hasta que no se hayan recibido por completo todos sus fragmentos.

Redirección con Location

La web http://tinyurl.com acorta el tamaño de URLs de gran longitud a través de la creación de alias más cortos. Para ello simplemente crea los alias y los almacena en una base de datos. Cuando recibe la petición de uno de estos alias devuelve una cabecera de redirección con la dirección original. Por ejemplo, la URL http://trajano.us.es/docencia/FundamentosDeInternet puede ser reducida a http://tinyurl.com/ppjg97v . Capture los mensajes recibidos al conectarse a la dirección anterior y compruebe que se recibe una respuesta HTTP/1.1 301 Moved Permanently con la línea de cabecera **Location** indicando la dirección original. Para ello puede enviar lo siguiente (se recomienda escribirlo previamente en un editor como emacs).

Pruebe si quiere a realizar una conexión con servidor web de tinyurl.com pero a través del programa telnet en lugar de un navegador (el programa telnet se ejecuta desde la línea de comandos del sistema operativo Linux. Si usas Windows necesitas instalar el programa putty). Telnet es un terminal remoto y por lo tanto, las teclas que pulsemos serán enviadas al servidor a través de la conexión tcp especificada(es como si escribiesemos directamente la APDU que genera el cliente)

Una vez tenga disponible el terminal, escriba:

```
%> telnet tinyurl.com 80
```

Una vez conectado, pruebe a escribir

```
POST /ppjg97v HTTP/1.1
Host:tinyurl.com
Content-Length:0
```

(presione un par de veces <ENTER> al terminar de escribir)

RESPUESTAS A LOS EJERCICIOS

En el documento de *RespuestasP1* tienes las respuestas que ha obtenido el profesor. Estas respuestas fueron capturadas en el curso 15/16 y debido a cambios posteriores en la configuración del servidor, puede que en algunos ejercicios la respuesta obtenida no sea exactamente la mostrada (pero sí parecida).

EXAMEN DE AUTO-EVALUACIÓN

Instrucciones

- *Arranque un navegador (diferente al que ya tiene arrancado con la enseñanza virtual) y borre la caché y cookies del navegador*.
- *Puede arrancar otro navegador para consultar el protocolo http (p*.e. en http://www.w3.org/Protocols/rfc2616/rfc2616.html)
- *Prepare Wireshark para realizar una nueva captura de tramas por su interfaz Ethernet*.

- *Capture con Wireshark el intercambio de mensajes que ocurre entre su navegador y el servidor web al acceder a la siguiente URL: http://masai.us.es/p01test/*
- *Pare la captura en Wireshark en cuanto vea completa la página solicitada por su navegador.*

Analizando la captura anterior (filtre para que sólo se muestre el tráfico del protocolo *http*) responder a la siguientes preguntas:

(1) ¿cuántos bytes tiene el objeto /index.html que envía el servidor?

(a) **1.425** (b) 1.680 (c) 495 (d) ninguna de las otras

(2) ¿cuántas peticiones de tipo GET de imágenes se producen hasta que finalmente obtengo la página completa del Dpto de Ingeniería Telemática? (excluya las peticiones del objeto /favicon.ico si se produjesen)

(a) 2 **(b) 4** (c) 8 (d) ninguna de las anteriores.

(3) ¿cuál es el nombre del software del proceso servidor? (nombre y versión)

(a) **Apache/2.4.6 (CentOS) PHP/5.4.16**
(b) Apache/12.1.2 (Safari)
(c) Mozilla/5.0
(d) Firefox/1.2

(4) ¿cierra el servidor la conexión después de enviar el objeto /graficos/dit.gif ?

(a) Si, el servidor usa conexiones no persistentes
(b) No, el servidor usa conexiones persistentes
(c) Si, el servidor no usa conexiones persistentes
(d) no se puede averiguar con los datos de la captura.

(5) ¿cuándo fue la última vez que se modificó el objeto /index.html en el servidor?

(a) Fri, 17 Nov 2017 18:37:15 GMT
(b) Fri, 25 Oct 2013 09:23:11 GMT
(c) Thu, 24 Oct 2013 10:12:11 GMT
(d) ninguna de las otras

¿QUÉ DEBERÍAS SABER A PARTIR DE AHORA?

- Poner en marcha Wireshark y realizar una captura del tráfico que circula por cualquier NIC de tu equipo
- Saber interpretar y usar el interfaz de Usuario de Wireshark
- Saber identificar la dirección IP y puerto origen y destino de cada mensaje y saber mirar cuál es la dirección IP de la NIC que utiliza tu equipo para su conexión a Internet.
- Saber leer el contenido de los mensajes del protocolo http
- Conocer la estructura básica de las peticiones y respuestas vistas en la práctica.
- Conocer las cabeceras vistas en la práctica y saber buscar información sobre nuevas cabeceras
- Conocer el funcionamiento del Conditional GET
- Conocer el funcionamiento de las COOKIES

PARTE II: DNS

PARTE I : LA APLICACIÓN DNS

JERARQUÍA DE SERVIDORES DE NOMBRES (15min)

Ya debes estar familiarizado con la estructura del Sistema de Nombres de Dominio (DNS) como una base de datos distribuida y un protocolo cliente/servidor para la realización de peticiones y obtención de respuestas de servidores DNS.

Recuerda que los servidores DNS pueden ser clasificados en diferentes niveles jerárquicos:

- Locales[1]: los de tu ISP, a los que tu host realiza las peticiones.
- Autorizados (authoritative), los servidores de una organización que mantienen información actualizada de los nombres de todas las máquinas que existen dentro del dominio de dicha organización (p.ej. *us.es*).

NIVEL	NOMBRE DEL SERVIDOR	DIRECCIÓN IP
ROOT (en España)	-	-
TLD (es)	-	-
Autorizado (us.es)	-	-
Local	-	-

- De Nivel Superior de un dominio (Top-Level Domain). A veces los DNS locales no tienen la dirección IP o el nombre de los servidores autorizados de un dominio y por ello deben consultar a servidores de nivel superior (p.ej. .es) o bien a un servidor raíz. Estos servidores de nivel jerárquico superior mantienen y almacenan las direcciones y nombres de los servidores autorizados dentro de su dominio.
- Raiz (root). Son servidores que deberían siempre ayudar en la resolución de un nombre. Mantienen y almacenan información sobre otros servidores DNS de Internet (p.ej. los servidores TLD o servidores autorizados).

Una vez resuelta la petición, el servidor DNS local envía al cliente la respuesta, que también guarda en su caché durante un tiempo predeterminado.

Existen bases de datos públicas donde se listan los servidores de la jerarquía anteriormente descrita. Por ejemplo en http://www.root-servers.org se puede encontrar información sobre los servidores raíz. En la propia página de la IANA, en http://www.iana.org/domains/root/db/ se puede encontrar información sobre los servidores TLD, y en http://whois.domaintools.com/ se puede encontrar información sobre los servidores de nombres de una organización (servidores autorizados de un dominio).

[1] Puedes consultar la dirección IP del Servidor DNS local que atiende las peticiones de tu equipo mirando en la configuración de red de tu equipo (p.ej. en Windows con el comando ipconfig /all , o en linux en el fichero /etc/resolv.conf).

1) Usando las referencias anteriores u otras que encuentres, rellena un nombre de un servidor DNS de cada uno de los tipos vistos en la tabla que sigue a continuación:

En la web http://www.nic.es se puede consultar la lista de Organizaciones de tipo *Registrar* (agentes registradores) que pueden registrar nombres dentro del dominio .es. Encuentra el nombre de al menos dos empresas de este tipo.

PROGRAMA CLIENTE DNS (15min)

Normalmente, el servicio DNS es solicitado por otras aplicaciones cuando el usuario escribe el nombre de un host en lugar de su IP (p.ej. al escribir la URL en un navegador web). Sin embargo los sistemas operativos también ofrecen un programa cliente DNS para que sea utilizado directamente por los usuarios. Por ejemplo, windows usa el programa nslookup mientras que Linux o mac os x utilizan un programa llamado host, o alternativamente otro programa llamado dig.

nslookup es un programa cliente DNS accesible a los usuarios del sistema operativo Windows. Abre un terminal (ejecuta cmd para obtener una ventana con un terminal) y prueba resolver los siguientes nombres de máquinas.

- masai.us.es
- www.hotmail.es

Mira la ayuda del programa nslookup o host en tu sistema antes de usarlo para conocer todas las posibilidades de uso. En Windows ejecute %>nslookup y entre en el modo interactivo y después ejecute >? Para ver la ayuda (p.e. >set type=NS filtra en las respuestas los registros de tipo NS; >exit sale del modo interactivo) Después intenta responder a las siguientes preguntas:

2) En la primera consulta al DNS (la de masai.us.es), ¿cuál es la IP del servidor local DNS que responde? ¿cuál es la dirección IP de masai.us.es?

3) En la segunda consulta DNS, ¿cuál es el nombre canónico del host www.hotmail.es?

4) En la segunda consulta DNS ¿hay una única dirección IP asociada al nombre o varias? Si hubiese más de una, ¿qué dirección IP tienen los hosts que pueden responder a cualquiera de los nombres asociados a www.hotmail.es?

CAPTURA DE MENSAJES DEL PROTOCOLO DNS (15min)

Los mensajes DNS de petición y respuesta tienen el mismo formato (la misma sintaxis), mostrada en la Figura 1. Recuerda que los RR son tuplas del tipo (name, value, type, ttl) y que en función del tipo de mensaje (campo type), los campos name

y value tienen diferente significado [2]. Puedes encontrar información detallada sobre el protocolo y los Registros de Recursos (RR) en http://www.zytrax.com/books/dns/ch15/ o bien en la norma correspondiente http://www.ietf.org/rfc/rfc1035.txt .

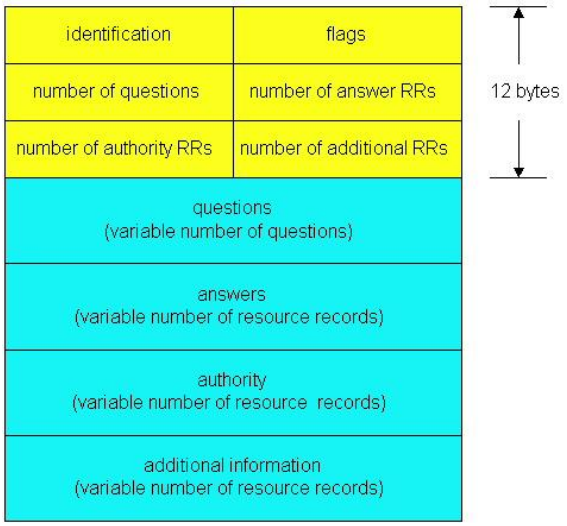

Ilustración 2. Formato genérico de los mensajes del protocolo DNS

En el primero de los dos enlaces anteriores puedes ver en detalle la cabecera del mensaje DNS. El resto del mensaje está compuesto de por un conjunto de Registros de Recursos que viajarán en los campos correspondientes según la naturaleza del registro (p.ej. si es una consulta irá en el campo questions, si son de respuesta irán en answers o additional information, salvo si son del tipo NS que irán en el campo authority).

Tu equipo tiene una caché local donde guarda las resoluciones realizadas con anterioridad hasta su fecha de caducidad. Antes de continuar la práctica conviene que borres el contenido de tal caché (en windows[3], ejecuta cmd.exe y ejecuta en el terminal el comando ipconfig /flushdns).

Ahora vamos a capturar los mensajes DNS que se generan cuando un programa (en nuestro caso ping) recibe el nombre de una máquina en lugar de su dirección IP. Haz lo siguiente:

- Borra la caché DNS local de tu equipo.
- Abre un nuevo terminal de línea de comandos (en windows ejecuta cmd).
- Abre Wireshark e introduce "ip.addr==<IP_tu_equipo>"
- Comienza la captura de paquetes en wireshark

[2] Puede consultar una lista completa de los tipos de RR existentes en https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml o en http://en.wikipedia.org/wiki/List_of_DNS_record_types

[3] Consulta en http://www.whatsmydns.net/flush-dns.html cómo borrar la caché DNS de tu sistema operativo.

- Escribe en terminal ping www.cs.umn.edu
- Espera un par de segundos y para la captura de paquetes en wireshark.

Si después de 5 minutos no logras tener una captura satisfactoria, puedes descargarte un archivo de capturas de http://masai.us.es/practica2/capturaDNS Carga este archivo con tu Wireshark para continuar la práctica (menú Archivo/File). No obstante, pídele a tu profesor que te ayude a realizar la captura.

Examina el contenido de los mensajes del protocolo DNS y responde a las siguientes preguntas:

5) Localiza los mensajes de petición y respuesta del protocolo DNS relacionados con la resolución del nombre www.cs.umn.edu. ¿Son enviados mediante TCP o UDP? ¿cuál es el puerto destino para el mensaje de petición DNS? ¿Cuál es el puerto asociado a un servidor DNS?

6) Examina el primer mensaje de petición DNS que genera tu equipo. ¿Qué tipo de registro de recurso viaja en el campo "query"? ¿Contiene el mensaje de petición DNS alguna respuesta en el campo "answers"?

7) Examina el mensaje de respuesta a la petición anterior. ¿Cuántos registros viajan en el campo "respuestas" (answers)? ¿Para qué sirve cada una de esas respuestas? ¿Cuál es el nombre real –canónico- de www.cs.umn.edu? ¿Cuál es la IP resuelta?

8) Mira en el resto de campos de la respuesta. ¿Cómo se llama el servidor DNS autorizado para el dominio umn.edu ?

RESPUESTAS A LOS EJERCICIOS

En el documento de *RespuestasP1* tienes las respuestas que ha obtenido el profesor.

EXAMEN DE AUTO-EVALUACIÓN

1) Indique el nombre canónico que corresponde al nombre www.facebook.com

a) www.facebook.com b) facebook.com **c) star.c10r.facebook.com** d) ninguna de las otras respuestas

2) Indique la dirección IP de un servidor público de correo electrónico del dominio us.es

a) 192.163.175.40 **b) 193.147.175.80** c) 172.154.56.12 d) ninguna de las anteriores.

3) Indique la dirección IP de algún servidor DNS del dominio facebook.com

RESPUESTA 1: 69.171.239.11

4) Averigüe el nombre de una máquina que responda como servidora de correo electrónico para el dominio isotrol.com (si hubiese vários nombres, elegir sólo uno)

respuesta: ASPMX.L.GOOGLE.com

¿QUÉ DEBERÍAS SABER A PARTIR DE AHORA?

- Saber la estructura de los mensajes del protocolo DNS. En particular, entender y saber interpretar los 4 campos de longitud variable.
- Saber consultar las direcciones IP de máquinas partiendo de su nombre registrado.
- Conocer el proceso de resolución de nombres entre diferentes servidores
- Conocer la estructura de la base de datos distribuida de DNS
- Conocer el proceso a seguir para registrar un nuevo nombre de dominio en un DNS