



## LABS - Apuntes 1

Telematics (Universidad de Deusto)

# LAB 2: HTTP

## 1. La interacción básica HTTP GET/response

**1 ¿El navegador ejecuta HTTP versión 1.0 o 1.1? ¿Qué versión de HTTP funciona en el servidor?**

Tanto el cliente como el servidor tienen la versión http 1.1.

**2 ¿Qué idiomas (si los hay) indica el navegador que puede aceptar?**

En-us.

**3 ¿Cuál es la dirección IP de tu ordenador? Y ¿del servidor gaia.cs.umass.edu?**

Mi ordenador 192.168.1.102 y el del servidor 128.119.245.12

**4 ¿Cuál es el código de estado devuelto desde el servidor a tu navegador?**

200 OK

**5 ¿Cuál es la fecha de la última actualización del archivo HTML recuperado?**

23 de septiembre de 2003

**6 ¿Cuántos bytes han sido devueltos a tu navegador?**

73.

## *2. La interacción HTTP CONDITIONAL GET/response*

**8. Inspecciona el contenido de la primera solicitud HTTP GET desde el navegador al servidor. ¿Ves una línea "MODIFIED IF-Since" en el HTTP GET?**

No.

**9. Inspecciona el contenido de la respuesta del servidor. ¿El servidor devuelve explícitamente el contenido del archivo? ¿Cómo lo sabes?**

Sí, aparece en el line-based text data.

**10 Ahora inspecciona el contenido de la segunda petición HTTP GET desde el navegador al servidor. ¿Ves una línea "If-Modified-Since:" en el HTTP GET? Si es así, ¿qué información sigue al encabezado "If-Modified-Since:"?**

Sí, la fecha de la última modificación 23 de septiembre de 2003.

**11 ¿Cuál es el código de estado HTTP y frase devuelto por el servidor en respuesta a esta segunda HTTP GET? ¿El servidor devuelve explícitamente el contenido del archivo?**

Explícalo.

304 not modified, no vuelve a mostrar dos veces el mismo contenido si este no ha sido modificado.

## *3. Recuperando grandes documentos*

**12 ¿Cuántos mensajes petición HTTP GET fueron enviados por tu navegador?**

Hay un get.

**13 ¿Cuántos segmentos TCP conteniendo datos se necesitan para llevar a la única respuesta HTTP?**

[4 Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]

**14 ¿Cuál es el código de estado y la frase relacionada con la respuesta a la solicitud HTTP GET?**

200 OK.

**15 ¿Existen líneas de estado HTTP en los datos transmitidos asociados con una "continuación"?**

No.

#### ***4.Documentos HTML con Objetos Embebido***

**16 ¿Cuántas mensajes de petición HTTP GET fueron enviados por tu navegador? ¿A qué direcciones IP se enviaron éstas peticiones?**

3 get.

Ip's ==> 128.119.245.12 ^ 165.193.123.218 ^ 134.241.6.82

**17 ¿Puedes decir si el navegador descarga las dos imágenes en serie, o si fueron descargadas de los dos sitios web en paralelo? Explicalo.**

En serie se produce en diferentes tiempos.

#### ***5 HTTP Authentication***

**18 ¿Cuál es la respuesta del servidor (código de estado y frase) en respuesta al mensaje HTTP GET inicial de tu navegador?**

401 AUTHORIZATION REQUIRED.

**19 Cuando tu navegador envía el mensaje GET HTTP, por segunda vez, ¿el nuevo campo está incluido en el mensaje HTTP GET?**

AUTHORIZATION ESTA INCLUIDO EN EL HTTP EN EL SEGUNDO GET.

#### ***6.La sesión HTTP***

**1.Identificar las conexiones que se establecen entre clientes y servidores.**

Paquetes 4,10,12,41,42,48

**2.Identificar los segmentos TCP que participan en el establecimiento de la conexión**

syn,syn-ack,ack,psh-ack.

**3.¿Es la conexión que se establece entre el cliente y el servidor persistente o no persistente?**

La version http 1.1 siempre es persistente.

#### ***7. HTTP COOKIES***

**6. Identifica la trama que contienen las cookies en la captura anterior.**

Filtro http contains "Cookie"

**7. Comprueba si entre las cookies almacenada en tu navegador se encuentra la información contenida en la trama anterior.**

En ambas se ve informacion de yahoo.

#### ***8.Secure HTTP***

**8.Identifica los puertos utilizados por el servidor HTTPS**

filtro ssl

**9. ¿Es posible visualizar el contenido de la información?**

No debido a que esta encriptado.

## **LAB 3: DNS**

### **Captura 2**

**1. Busque la consulta DNS y mensajes de respuesta. ¿Se envían a través de UDP o TCP?**  
UDP

**2. ¿Cuál es el puerto de destino del mensaje de la consulta de DNS? ¿Cuál es el puerto de origen del mensaje de respuesta de DNS?**  
Origen 3163 Destino 53

**3. ¿A(enunciado pone en) qué dirección IP se envía el mensaje de consulta DNS? Utiliza ipconfig para averiguar la dirección IP de tu servidor DNS local. ¿Coinciden las dos direcciones IP?**  
Destinacion

**4. Examina el mensaje de respuesta de DNS. ¿Cuántas "respuestas" se ofrecen? ¿Qué significa el contenido de cada una de estas respuestas?**  
2 answer Rrs de tipo A. www.ietf.org: type A, class IN, addr 132.151.6.75 y www.ietf.org: type A, class IN, addr 65.246.255.51.

**5. Considera el paquete TCP SYN enviado por tu nodo inmediatamente a continuación de la consulta. ¿La dirección IP de destino del paquete SYN corresponde con alguna de las direcciones IP proporcionadas en el mensaje de respuesta de DNS (podrías explicarlo)?**  
--

**6 . Esta página web contiene imágenes. Antes de recuperar cada imagen, ¿envía el nodo nuevas consultas DNS? ¿por qué?**  
Las DNS no incluyen ningun archivo de foto a si que en este caso no.

### **Captura 3**

**7. Examina el mensaje de consulta DNS. ¿Qué "Tipo" de consulta DNS es?** Tipo A

**8. Examina el mensaje de respuesta DNS. ¿Qué contenido hay en el campo respuestas y autoridades?**  
Respuestas ==> www.mit.edu: type A, class IN, addr 18.7.22.83

Actividades ==> Authoritative nameservers

Captura 4

**9. Examina el mensaje de respuesta de DNS. ¿Qué MIT servidores nombre proporciona el mensaje de respuesta?**

Respuestas ==> copia pega... answers

**10. ¿En este mensaje de respuesta se proporcionan también las direcciones IP de los servidores de nombres del MIT?**

Si te los da la respuesta entre corchete.

CAPTURA 5

**11. ¿A qué dirección IP se envía el mensaje de consulta DNS? ¿Es la dirección IP de tu servidor DNS local por defecto? Si no fuera así, ¿a quién corresponde la dirección IP?**

Destination, es la misma.

**12. Examina el mensaje de respuesta de DNS. ¿Cuántas " autoridades " se informan? ¿Qué significa el contenido cada una de estas respuestas?**

En este caso como no dice nada, se define de cada response.

## **LAB 4: FTP**

### ***1. FTP***

**1. Explica los mensajes intercambiados entre el servidor y el cliente en el proceso de identificación de un usuario. Identifica todos los mensajes intercambiados entre el cliente y el relacionado con la captura de la interfaz de servidor.**

**2. La contraseña no se muestra en la interfaz, pero ¿el nombre de usuario y contraseña se intercambiaron de alguna manera protegidos o se envían como texto sin formato?**

**3. Explica los mensajes intercambiados (identificando cada comando y las acciones que ha llevado a cabo el receptor ...) como resultado de un comando "dir" para mostrar el contenido de una carpeta.**

**4. Explica el intercambio de mensajes (comandos y respuestas) que se han producido como consecuencia del comando "get" para recuperar un archivo.**

# **LAB 5 : TCP**

## **1.** *Un primer vistazo a la traza capturada*

**1. ¿Cuál es la dirección IP y número de puerto TCP utilizado por el equipo cliente (HTTP fuente -cliente ) que está transfiriendo el archivo a gaia.cs.umass.edu ?**

192.168.160.26

61258

**2. ¿Cuál es la dirección IP del gaia.cs.umass.edu ?**

128.119.245.12

**3. ¿Qué números de puerto de envío y recepción aparecen en los segmentos TCP para esta conexión ?**

80 y 61258

## **3. Fundamentos TCP**

**4. ¿Cuál es el número de secuencia del segmento TCP SYN que se utiliza para iniciar la conexión TCP entre el equipo cliente y gaia.cs.umass.edu ?**

Seq = 0

**5. ¿Qué hay en el segmento que identifica el segmento como un segmento SYN ?**

Flags: 0x002 (syn)

**6. ¿Cuál es el número de secuencia del segmento SYN ACK enviado por gaia.cs.umass.edu al equipo cliente en respuesta al SYN ?**

Seq = 0

**7. ¿Cuál es el valor del campo de acuse de recibo en el segmento SYN ACK ?**

1.

**8. ¿Cómo gaia.cs.umass.edu determinar ese valor?**

Esta determinado con el numero de secuencia +1.

**9. ¿Qué hay en el segmento que identifica el segmento como segmento SYN ACK ?**

Flags: 0x012 (SYN, ACK)

**10. ¿Cuál es el número de secuencia del segmento TCP contiene el comando HTTP POST?**

164041

**12. Teniendo en cuenta la diferencia de tiempo entre el envío de cada segmento TCP y la recepción de su reconocimiento, ¿cuál es el valor RTT para cada uno de los seis segmentos? ¿Cuál es el valor EstimatedRTT después de la recepción de cada ACK? Supongamos que el valor de la EstimatedRTT es igual a la medida de RTT para el primer segmento, y luego se calcula utilizando la ecuación EstimatedRTT en la página 249 para todos los segmentos posteriores.**

**grafico**

**13. ¿Cuál es la longitud de cada uno de los seis primeros segmentos TCP ?** La longitud de cada uno de los primeros segmentos TCP es 708. Los siguientes segmentos son todos 1514.

**14. ¿Cuál es la cantidad mínima de espacio de búfer disponible anunciada en el recibido por toda la traza?** La cantidad mínima de espacio de búfer disponible se indica como 65535. El remitente nunca se limita porque nunca alcanzamos la capacidad total de la ventana.

**15. ¿Hay segmentos retransmitidos en el archivo de seguimiento?**

**16. ¿Cuántos datos reconoce el receptor normalmente en un ACK ? ¿Puedes identificar un caso en el que el receptor reconoce todos los demás segmentos recibidos?**

El receptor suele tener 432 bits. Hay casos en los que el receptor recibe todos los demás segmentos. Esto se muestra cuando se produce más de un ack en una fila.

**17. ¿Cuál es el rendimiento (bytes transferidos por unidad de tiempo) para la conexión TCP?**

El rendimiento se puede calcular utilizando el valor del último ack (149,629), el primer número de secuencia (1) dividido por el tiempo transcurrido desde el primer fotograma (1.6) = 93517.6 bps.