

PROTOCOLO HTTP – LABORATORIO WIRESHARK

En el presente laboratorio trabajaremos varios aspectos del protocolo HTTP, a saber:

- Solicitudes básicas con GET
- GET condicional
- Documentos HTML con objetos embebidos
- Autenticación en HTTP

a. Solicitudes básicas con GET

En esta primera parte del laboratorio se accederá a un documento HTML muy sencillo, sin objetos embebidos. Para ello:

- Inicie su navegador web.
- Inicie Wireshark y comience la captura de paquetes. En el campo de filtro escriba `http` para filtrar solamente el tráfico HTTP.
- Navegue a la siguiente dirección: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>
- El navegador mostrará una página web muy sencilla, de una sola línea.
- Detenga la captura en Wireshark.

Busque en la captura el paquete que contiene la orden GET. Selecciónelo, dé clic derecho y escoja la opción Follow -> TCP Stream. Aparecerá una ventana donde se verá todo el texto intercambiado por el cliente y el servidor durante la conversación. Note que el texto enviado por el cliente aparecerá en rojo, y las respuestas del servidor en azul. Conteste las siguientes preguntas:

1. ¿Cuál versión de HTTP emplea su navegador? ¿Cuál versión emplea el servidor?
2. ¿Cuáles idiomas (si aparecen) puede aceptar su navegador del servidor?
3. ¿Cuál es la dirección IP de su computador? ¿Y del servidor `gaia.cs.umass.edu`?
4. ¿Cuál es el código de estado que regresa el servidor a su navegador?
5. ¿Cuándo fue modificado por última vez el archivo al cual accedió en el servidor?
6. ¿Cuántos bytes de contenido fueron retornados por el servidor?

b. GET condicional

En la clase, se vio que la mayoría de los navegadores prefiere hacer un GET condicional cuando se está accediendo a una página web, para poder aprovechar el caché del navegador. En esta parte de la práctica se podrá apreciar este mecanismo en acción. Para ello:

- Borre el caché de su navegador.
- Inicie la captura en Wireshark. Emplee el filtro `http`.

- Navegue a la siguiente página: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html> . Se desplegará una página web muy sencilla de 5 líneas.
- Presione el botón de refresco en el navegador, para volver a cargar la página.
- Detenga la captura en Wireshark. Se podrán apreciar dos solicitudes GET en la captura.

Conteste las siguientes preguntas:

7. Revise el contenido de la primera solicitud HTTP GET. ¿Hay algún encabezado IF-MODIFIED-SINCE?
8. Revise el contenido de la primera respuesta del servidor. ¿Qué código de estado retornó el servidor? ¿El servidor envió explícitamente el contenido de la página web? ¿Cómo puede demostrarlo?
9. Ahora revise el contenido de la segunda solicitud HTTP GET. ¿Hay algún encabezado IF-MODIFIED-SINCE? Si lo hay, ¿qué información aparece a continuación?
10. Revise el contenido de la segunda respuesta del servidor. ¿Qué código de estado retornó el servidor? ¿El servidor envió explícitamente el contenido de la página web? Explique.

c. Documentos HTML con objetos embebidos

En esta sección estudiaremos qué ocurre cuando el navegador descarga una página con objetos embebidos, en este caso, imágenes que pueden estar en el mismo servidor, o en otro. Para ello:

- Inicie la captura con Wireshark. Emplee el filtro http.
- Acceda a la siguiente página: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html> . Se cargará una página con dos imágenes. La primera (el logo de Pearson) reside en `gaia.cs.umass.edu`. La segunda (la tapa de un libro) reside en `kurose.cslash.net`.
- Una vez que las imágenes carguen, detenga la captura en Wireshark.

Conteste las siguientes preguntas:

11. ¿Cuántas solicitudes GET envió su navegador? ¿A cuáles direcciones IP fueron enviadas las solicitudes GET?
12. ¿Podría decir si las imágenes fueron descargadas en serie, o en paralelo? Explique.

d. Autenticación HTTP

Finalmente se estudiará el proceso de autenticación básica de HTTP, que permite crear sitios web protegidos con usuario y contraseña de una manera muy sencilla y a la vez insegura. Para ello:

- Inicie la captura con Wireshark. Emplee el filtro http.

- Navegue a la siguiente dirección: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html . Cuando se le solicite, introduzca wireshark-students como usuario, y network como contraseña. Si todo sale bien, aparecerá una página web de dos líneas.
- Detenga la captura en Wireshark. Se podrán observar dos solicitudes GET.

Conteste las siguientes preguntas:

13. ¿Cuál es el código de respuesta a la primera solicitud GET de su navegador?
14. Cuando su navegador envía el GET por segunda vez, ¿qué encabezado adicional se incluye con la solicitud?
15. Decodifique la cadena que aparece a continuación del encabezado nuevo empleando un decodificador Base64 (puede buscar uno en Google). ¿Qué cadena de texto aparece al decodificar la cadena original?