



## Estudio experimental

El estudio experimental de esta práctica consta de cuatro partes. En cada una de ellas se describen todos los pasos que el alumno debe realizar, si tiene cualquier duda consulte con el profesor encargado de la sesión práctica. **En todo caso, antes de abandonar el laboratorio debe realizar el punto 66.**

### Pasos previos

1. Asegúrese de que su PC está conectado a la red de la ETSII.
2. Encienda su PC y arranque Windows 7.
3. Deshabilite el firewall de Windows.
4. Abra Internet Explorer y entre en Enseñanza Virtual. En la carpeta Laboratorio/Práctica 1/Archivos, encontrará dos ficheros que puede tener que utilizar más adelante. Cópielos en la carpeta **C:\Program Files (x86)\Tftpd32**. Asegúrese de que se quedan en esa carpeta o las descargas de archivos mediante TFTP no funcionarán correctamente. Cierre Internet Explorer.
5. Desconecte su PC de la red ETSII y conéctelo a LAB\_DTE, concretamente al SWITCH\_EUROPA (en G1.31) o al SWITCH\_SUDAMÉRICA (en G1.33). Compruebe que tiene conectividad de nivel físico observando que esté encendido el LED correspondiente a la boca de su switch.
6. Abra una ventana de Símbolo del sistema y ejecute el comando **ipconfig/all**, compruebe que la dirección IP de su PC empieza por 193, y anote su configuración IPv4 (dirección IP, máscara, puerta de enlace predeterminada y dirección IP servidor DNS). Compruebe que tiene conectividad a nivel de red con su router frontera.


### Primera parte: Configurando Wireshark y analizando PDUs

7. Arranque el analizador de protocolos Wireshark .
8. En el cuadro de etiquetado "Filter:", introduzca el filtro de visualización **http or dns**.
9. Observe cómo en el borde inferior de la ventana de Wireshark aparece el texto "Packets:" indicando el número total de tramas capturadas y el texto "Displayed:" indicando el número de tramas que han pasado el filtro de visualización y pueden verse en el listado de tramas. Si todo va bien, ahora estará capturando tramas (puede ver que el contador de "Packets" sigue creciendo, mientras que el contador de "Displayed" debería estar a valor "cero". Nótese, sin embargo, que existe la posibilidad de que algún proceso del sistema operativo genere algún tráfico DNS o algún protocolo derivado de HTTP, y le sea mostrado en la lista de tramas.
10. Abra una ventana del Símbolo del sistema, y ejecute el comando **ipconfig /flushdns** para borrar la caché DNS.
11. Abra el navegador MOZILLA FIREFOX  y borre su caché de páginas entrando en "Configuración/Avanzado/Red/Contenido web en caché -> Limpiar ahora", para eliminar cualquier página anterior que pudiera estar cargada en ella. Procure poner la ventana de Firefox con un tamaño no muy grande, de forma que pueda ver detrás la ventana de Wireshark y lo que está viéndose en el listado de tramas.
12. Reinicie la captura en Wireshark pulsando el icono de "RESTART" para eliminar cualquier tráfico capturado con anterioridad (se esté o no mostrando con el filtro de visualización que ha aplicado).
13. Usando FIREFOX, visite la página web <http://webserver.af.lab/lab3/paginasimple.html> para generar el tráfico de red que vamos a analizar.
14. Espere 30 segundos y, solo entonces, detenga la captura en Wireshark. Si no espera 30 segundos, la captura de tráfico podría estar incompleta y tendrá que volver a empezar desde el principio.
15. Si todo va bien, ahora Wireshark estará mostrándole, además del posible tráfico DNS de los procesos del Sistema Operativo, solamente 6 tramas, que serán: cuatro tramas al principio de la captura con el protocolo DNS (relacionadas con la resolución del nombre webserver.af.lab) y a continuación otras dos tramas con mensajes del protocolo HTTP (relacionadas con paginasimple.html). Si no es así, salga de Firefox, reinicie la captura en Wireshark pulsando el icono "RESTART" y vuelva al punto 10. Nota: es posible que haya alguna trama más, porque algún proceso del sistema operativo genere algún tráfico DNS, por algún protocolo derivado de HTTP, o por alguna retransmisión. Si le sobra alguna trama, puede ignorarla, pulsando el botón derecho del ratón sobre la trama e indicando la opción **"Ignore Packet"**.
16. Viendo simplemente la información del listado de tramas, conteste a las siguientes preguntas: ¿Cuál es la IP de su PC? ¿Cuál es la IP del servidor DNS al que FIREFOX pregunta por el nombre webserver.af.lab? ¿Cuál es la IP del servidor webserver.af.lab?
17. En Wireshark, vaya a File > Export Specified Packets y guarde en un archivo TODAS LAS TRAMAS CAPTURADAS ("All packets captured"). Fíjese en que podríamos escoger una opción en la que sólo se guardaran

las tramas visualizadas ("All packets displayed"), pero no queremos eso. El nombre de la captura puede ser "practica1ARcaptura1".

18. Para estar seguros de que hemos capturado el final de la conexión TCP, introduzca el filtro de visualización **tcp.flags.fin == 1** y observe que se muestran solo dos tramas y que ambas muestran en el campo Info el texto [FIN, ACK]. Si no es así es que algo ha salido mal y la captura no es válida. Quizá no esperó los 30 segundos necesarios antes de detener la captura en Wireshark. Va a tener que empezar de nuevo, así que debe cerrar Wireshark, cerrar FIREFOX y volver al paso 10.
19. ¿Cuál es el puerto usado por la aplicación cliente de su PC en la conexión con el servidor web? ¿Y el puerto usado por la aplicación servidora en el host remoto?
20. Escriba y aplique el filtro **dns**. ¿Cuántas peticiones DNS hay? ¿Qué RTT se observa para la primera petición? ¿Cuántas T\_PDUs del protocolo UDP se han intercambiado?
21. Escriba y aplique el filtro **not tcp**. Aparte del protocolo DNS, podrá ver que hay bastantes tramas que en este momento no nos interesan, por ejemplo de los protocolos ARP, RIPv1, STP, CDP, etc...
22. Escriba y aplique el filtro **tcp**. Debería ver solo tramas que en la columna "Protocol" muestran TCP o bien HTTP (recuerde que HTTP se encapsula dentro de TCP).
23. Elimine todas las retransmisiones y, en general, todas las tramas, que no se refieran a la carga de la página web.
24. Vuelva a a File > Export Specified Packets. Ahora, queremos salvar en disco solo las tramas que se están visualizando ("displayed") y que son las que nos interesan. Marcamos dentro de "Packet Range" las casillas "All packets" y "Displayed" para grabar todos los paquetes visualizados. Un buen nombre para el archivo sería "practica1ARcaptura2".
25. Acaba de grabar el archivo que nos interesa, pero aún tenemos cargado el anterior, el grande, con todas las tramas. Pulse el icono de la carpeta y cargue el fichero "practica1ARcaptura2".
26. Al cargar el fichero, cada una de las tramas lleva un segmento TCP. Nótese que aunque dos de ellas muestran HTTP en la columna "protocol", HTTP se encapsula dentro de TCP, por lo que TCP también está presente en esas tramas.
27. Observe los dos primeros segmentos TCP, los que aparecen marcados en el campo INFO con [SYN]. ¿En que se basa Wireshark para etiquetar esos segmentos con [SYN]? ¿Es por el hecho de ser los dos primeros segmentos de la captura? ¿O es porque hay algo especial en el interior de esos dos segmentos? Localice ese "algo especial" en el panel central (panel de detalles de trama).
28. Conteste a las siguientes preguntas:
  - a) ¿Qué tamaño tiene la A\_PDU enviada por el cliente?
  - b) ¿Qué tamaño tiene la A\_PDU enviada por el servidor?
  - c) ¿Qué aplicación es la primera que decide cerrar la conexión?

## Segunda Parte: Análisis de IP\_PDU, encapsulación

29. Seleccione la trama que corresponde a la petición DNS. Pulse sobre la primera trama y en detalle de trama pulse sobre el "+" que aparece al lado de Internet Protocol version 4 para ver los campos de la IP\_PDU de la IP\_PDU. Con la información mostrada, responda a estas preguntas: ¿Qué campo de la IP\_PDU indica que ha sido su PC el que ha enviado esta IP\_PDU? ¿Cuántos saltos como máximo podrá dar esta IP\_PDU para alcanzar al destino? Anote el valor del campo de la IP\_PDU que ha usado para responder a esta pregunta. ¿Qué campo de la IP\_PDU consulta Wireshark  para indicar que la IP\_PDU es del protocolo UDP?

## Tercera parte: TFTP

30. Esta parte de la práctica se realiza en pareja, junto con su compañero de al lado. Realice o no la acción correspondiente a cada punto, debe contestar a todas las preguntas.
31. Si está en el PC de la izquierda, ejecute el programa tftpd32, que se encuentra en el escritorio. Cambie la pestaña "Server interfaces" y seleccione su dirección IP. Después, entre en "Settings", En la pestaña "Global", deje únicamente el servidor TFTP como marcado. Posteriormente, entre en la pestaña TFTP y desmarque "Option negotiation". Pulse OK. Puede que el servidor le pida reiniciar. En ese caso, Pulse "Aceptar" e ignore la recomendación. En su lugar, lo que debe hacer es cambiar la pestaña "Current Directory", indicando el directorio en el que guardo los archivos del inicio de la práctica. Ya tiene su PC configurado como servidor TFTP.
32. Esté en el PC de la izquierda o de la derecha, inicie el programa Wireshark y empiece a capturar tráfico.
33. En el filtro de visualización, introduzca **tftp**.
34. Si está en el PC de la derecha, abra una ventana de **Símbolo del sistema**, déjela de tal manera que pueda observar dicha ventana al mismo tiempo que la captura de Wireshark y ejecute el comando **tftp IP\_de\_su\_compañero get Prueba1.txt**.
35. ¿A qué puerto se ha enviado este mensaje?
36. Observe los mensajes TFTP. Represente el diálogo entre cliente y servidor. ¿Cuántas tramas se han intercambiado?
37. ¿Está el servidor TFTP en su red? ¿Puede saber la dirección MAC del servidor?

38. Ahora, si está en el PC de la derecha, abra una ventana de **Símbolo del sistema** y ejecute el comando **tftp IP\_de\_su\_compañero get Textolargo.txt**.
39. Abra el primer mensaje TFTP. ¿Cuáles son los protocolos de aplicación, transporte y red utilizados, respectivamente?
40. Observando únicamente la captura en Wireshark, ¿puede saber cuántos bytes tiene el fichero Textolargo.txt?
41. Observe el primer bloque de datos enviado por el servidor. ¿Cuántos bytes del fichero viajan en dicho bloque?
42. ¿Cuántos bytes tiene la TFTP\_PDU? ¿Por qué no coincide con el número de bytes enviados? Indique cómo lo ha calculado.
43. Si está en el PC de la izquierda, cierre el servidor TFTP.
44. Si está en el PC de la derecha, ejecute el comando **dir** y compruebe que los archivos descargados están en el directorio.

#### Cuarta parte: FTP

45. Inicie una nueva captura de Wireshark. No la pare hasta que se le indique expresamente.
46. Es posible que aparezca cierto tráfico no deseado relacionado con otros procesos. Para eliminarlo, puede escribir en el filtro de visualización, escriba **tcp.port==21 or tcp.port==20**. De esta forma, solo verá el tráfico que genera FTP en el puerto 21 (control) y el puerto 20 (datos).
47. Abra una ventana de Símbolo del Sistema y déjela de tal manera que pueda observar dicha ventana al mismo tiempo que la captura de Wireshark.
48. Ejecute el comando **ftp ftpserver.af.lab** en la ventana del Símbolo del Sistema.
49. Compare lo que ocurre en el programa (ftp en el Símbolo del Sistema) y en la comunicación (protocolo FTP en Wireshark).
50. El nombre de usuario es igual a la etiqueta que está en el frontal de su ordenador, exceptuando el guion. Si, por ejemplo, está en el ordenador COM-105 del laboratorio G1.33, su usuario es com105 y su password es comcom105. Si está en el ordenador RED-13, del G1.31, su usuario es red13 y su password es redred13.
51. Al introducir nombre de usuario y password, ¿qué comandos del protocolo FTP observa?
52. ¿Cuál es el mensaje de bienvenida del servidor?
53. Observe el primer mensaje que aparece en este momento en la captura en Wireshark. ¿Qué tipo de mensaje es? ¿Cuál es la dirección IP del servidor FTP? ¿Y su dirección MAC? ¿A qué puerto del servidor se conecta el cliente? ¿Cuál es el puerto abierto por la aplicación cliente?
54. Entre en el directorio download mediante el comando **cd download**. ¿Qué secuencia de comandos/respuestas FTP tiene lugar?
55. Descargue el archivo copyright.txt mediante el comando **get copyright.txt**
56. ¿Qué secuencia de comandos/respuesta del protocolo ftp provoca la ejecución del comando get en la línea de comandos?
57. Preste atención al comando PORT. Fíjese en que los parámetros del comando son 6 números separados por comas. Los cuatro primeros corresponden a los octetos que conforman la dirección IP del cliente. Los dos últimos (X e Y) están referidos al número de puerto. El cliente abrirá el puerto  $256 \times X + Y$  para la conexión de datos. Calcule el puerto que abrirá el cliente para la conexión de datos mediante esa fórmula.
58. Observe la conexión de datos que se establece para descargar el fichero. ¿Se está trabajando en modo activo o en modo pasivo? ¿Por qué?
59. ¿Qué puerto está utilizando el servidor para enviar los datos? ¿Y para recibir los comandos y mandar las respuestas?
60. ¿Cuántas tramas se han intercambiado hasta ahora para realizar la transferencia completa del archivo? ¿Qué diferencias observa con el diálogo que se establecería en TFTP?
61. Encuentre los mensajes que contienen el contenido del archivo. ¿Cuántos bytes tiene el archivo descargado?
62. ¿Cuánto tiempo ha durado la conexión de datos? Para ello, debe medir el tiempo que hay desde el SYN de la conexión de datos hasta el ACK al FIN de dicha conexión.
63. Ejecute el comando **dir**. ¿Cuál es la secuencia de comandos/respuesta del protocolo FTP que la ejecución de dir provoca?
64. Ejecute el comando **bye**. ¿Qué ocurre? ¿Con qué mensaje responde el servidor FTP? ¿Cree que este mensaje es configurable por el administrador del servidor?
65. Pare ahora la captura de Wireshark. ¿Cuántas conexiones TCP se han establecido en esta cuarta parte y por qué?
66. Cierre Wireshark, desconecte su PC de la Intranet del laboratorio y vuelva a conectarlo a la red de acceso a Internet (red ETSII) en la misma roseta en la que estaba y apague el PC. Vuelva a dejar en su sitio el latiguillo que conectó al switch.