



## Estudio experimental

El estudio experimental de esta práctica consta de tres 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. No olvide **guardar las capturas** que vaya realizando. Es imprescindible realizar el punto 37.

### Primera parte: Servicios de correo electrónico

1. Asegúrese de que su PC está conectado a la red ETSII.
2. Encienda su PC y arranque Windows 7.
3. Desactive el firewall de Windows.
4. Abra una ventana de **Símbolo del sistema** y ejecute en ella el comando **ipconfig /all**. Anote su dirección IP y su máscara de red.
5. Descargue el archivo smtp2021.pcap de Enseñanza Virtual y ábralo.
6. Observe la captura y conteste a las siguientes preguntas:
  - a. ¿Qué dirección IP tiene el servidor de correo?
  - b. ¿Qué protocolos observa entre cliente y servidor?
  - c. ¿Con qué puerto del servidor se ha establecido una conexión TCP? ¿Qué puerto ha abierto el cliente?
7. Seleccione el primer mensaje que el cliente de correo envía al servidor. ¿Qué tipo de mensaje es?
8. Con el mensaje anterior seleccionado, vaya a Analyze/Follow TCP Stream. De esta forma, podrá ver el diálogo SMTP entre cliente y servidor.
9. ¿Qué comandos SMTP envía el cliente al servidor? ¿Cuál es la dirección de correo del remitente?
10. Observe las cabeceras SMTP y conteste a las siguientes preguntas:
  - a. ¿Cuál es el nombre del remitente que le aparecerá al receptor del correo en su agente de correo?
  - b. ¿Cuál es la versión de MIME utilizada? ¿Qué permite la utilización de MIME?
  - c. ¿Lleva el correo algún archivo adjunto?
  - d. El texto original del correo incluía la frase "Esta prueba es la caña". ¿Por qué cree que no aparece así en Wireshark? ¿Podría verlo correctamente el destinatario?
11. Observe el segundo mensaje SMTP enviado por el cliente.
  - a. ¿Cuál es el tamaño del mensaje de correo?
  - b. ¿Quién es el remitente?
12. ¿Encuentra algún inconveniente en la forma de enviar los mensajes? ¿Se le ocurre alguna posible solución?

### Segunda parte: Sistema de Nombres de Dominio (DNS)

13. En la ventana del Símbolo del Sistema, ejecute el comando **ipconfig/flushdns**. De esta manera, borrará la caché DNS del sistema operativo.
14. 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.
15. Inicie una nueva captura de Wireshark y escriba el filtro **udp.port==53**. De esta manera, solo verá los mensajes con origen o destino en el puerto 53 (DNS).
16. Vaya a la página web [www.us.es](http://www.us.es). Espere unos 15 segundos y detenga la captura.
17. ¿Cuál es la dirección de su servidor DNS local? ¿Cuál es la dirección IP de la página web [www.us.es](http://www.us.es)?
18. Abra la petición DNS correspondiente a [www.us.es](http://www.us.es)
  - a. En el campo Flags, ¿qué significa que el primer bit sea cero?
  - b. ¿Qué indica el valor del bit Recursion Desired? ¿Qué tipo de búsqueda se realizará?
  - c. ¿Qué tipo de RR (Registro de Recurso) se puede observar? ¿Por qué?
19. Pulse con el botón derecho sobre el RR de tipo A correspondiente a [www.us.es](http://www.us.es), y seleccione Apply as Filter/Selected. ¿Qué ocurre?
20. Vuelva a poner el filtro del punto 15 y busque la petición DNS correspondiente a [api.instagram.com](http://api.instagram.com). ¿Cuál es el nombre canónico de dicho servidor? ¿Cómo lo sabe?
21. Abra otra ventana de MOZILLA FIREFOX , limpie otra vez el historial del navegador e introduzca la dirección IP correspondiente a [www.us.es](http://www.us.es) en el navegador. ¿qué ocurre? ¿Hay alguna petición DNS? ¿Por qué?

### Tercera parte: Control de errores a nivel de red. ICMP

22. Esta tercera parte de la práctica está estructurada por parejas, por lo que tendrá que realizar algunas acciones de esta práctica contando con su compañero/a. Las respuestas deben ser dadas por ambos miembros de la pareja, realicen ellos la acción o no.
23. **Si está en el laboratorio G1.31**, desconecte su PC de la red ETSII y conéctelo a la intranet del laboratorio, concretamente al SWITCH\_EUROPA (si está en el PC de la izquierda) o al SWITCH\_ASIA (si está en el PC de la derecha). **Si está en el laboratorio G1.33**. Si es así, desconecte su PC de la red ETSII y conéctelo a la intranet del laboratorio, concretamente al SWITCH\_SUDAMÉRICA (si está en el PC de la izquierda) o al SWITCH\_NORTEAMÉRICA (si está en el PC de la derecha).
24. Abra una ventana de Símbolo del sistema y ejecute en ella el comando `ipconfig /all`. Anote su dirección IP.
25. Inicie el programa Wireshark y empiece a capturar tráfico. En el filtro de visualización, introduzca **`icmp and not tcp.port==2008`**. El SO está ejecutando un proceso que utiliza el puerto 2008. Este tráfico generado por este proceso no nos interesa y de ahí que realicemos este filtrado.
26. Haga un ping desde el Símbolo del Sistema a su puerta de enlace por defecto.
27. Observe el mensaje ICMP asociado a una de las peticiones de eco en Wireshark
  - a. ¿Cuál es el valor del campo Tipo del mensaje ICMP?
  - b. En la cabecera IP del mensaje, identifique el valor del campo protocolo.
  - c. ¿Cuál es la longitud de la ICMP\_UD?
28. Observe el mensaje ICMP asociado a una de las respuestas de eco en Wireshark
  - a. ¿Cuál es el valor del campo Tipo del mensaje ICMP?
29. Ejecute el comando `ping -n 3 -l 500 dirección_IP_de_su_compañero/a`.
  - a. ¿Cuántas peticiones de eco realiza ahora? ¿Le responden a las peticiones?
  - b. ¿Cuál es el tamaño de la ICMP\_UD ahora?
  - c. ¿Cuál es el RTT entre su PC y el de su compañero?
30. Ejecute el comando `ping -l 1200 -f dirección_IP_de_su_compañero/a`. (Compruebe antes que Wireshark está capturando tráfico).
  - a. ¿Qué ocurre ahora?
  - b. ¿Hay algún flag de la cabecera IP de la petición de eco activado? ¿Cuál?
  - c. ¿Le llega algún mensaje ICMP? Si es así, ¿cuáles son su tipo y código? ¿Quién se lo envía?
  - d. ¿Cuál es la MTU de la red problemática? ¿Cómo lo sabe?
31. Guarde la captura anterior e inicie una nueva captura en Wireshark. Ponga un filtro de visualización (**`icmp or tftp and not tcp.port==2008`**).
32. Ejecute **`tftp 200.200.200.200 get file.txt`** desde el Símbolo del sistema.
  - a. ¿Qué ocurre? ¿Qué mensajes ICMP ha capturado?
  - b. ¿Quién es el emisor de los mensajes ICMP? ¿A qué cree que son debidos estos mensajes?
  - c. ¿Cuáles son los Tipos y Códigos de estos mensajes?
33. Si está vd. en el PC de la derecha, ejecute **`tftp dirección_IP_de_su_compañero/a get file.txt`** desde el Símbolo del sistema y observe la captura de Wireshark.
  - a. ¿Qué ocurre? ¿Por qué?
  - b. ¿Qué mensajes ICMP aparecen? ¿Cuáles son sus Tipos y Códigos?
34. Si está en el PC de la izquierda, ponga en marcha el servidor TFTP (Tftpd32, que se encuentra en el Escritorio). Basta seleccionar el interfaz que corresponde a su dirección IP.
35. Si está vd. en el PC de la derecha, vuelva a ejecutar **`tftp dirección_IP_de_su_compañero/a get file.txt`**.
  - a. ¿Hay algún error a nivel de red?
  - b. ¿Se ha desarrollado el protocolo de aplicación normalmente?
  - c. ¿Ha podido descargarse el archivo? ¿Por qué?
36. Ejecute `tracert dirección_IP_de_su_compañero/a`.
  - a. ¿Qué mensajes ICMP aparecen?
  - b. ¿Cuáles son sus Tipos y Códigos?
  - c. ¿Cuántos routers atraviesa la última petición de eco? ¿Cuáles son las direcciones IP de dichos routers?
37. 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 de red.