Estudio experimental

El estudio experimental de esta práctica consta de diez 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 el caso de no completar todas la partes del estudio experimental, antes de abandonar el laboratorio debe realizar el punto 68.

Debe completar en el laboratorio, al menos, las 7 primeras partes (páginas del 1 al 6). El resto de partes, (*introducción a Wireshark*) deben ser completadas por el alumno, bien en el laboratorio o bien en casa con ayuda de la captura del punto 56, será fundamental para poder completar el resto de prácticas.

Primera parte: Encender, restaurar, arrancar e identificar el PC

1. Encienda el PC. Al arrancar, se mostrará una pantalla con fondo blanco con un menú titulado “Menú del aula G1.31 y G1.33”. Si no le aparece esa pantalla debe avisar al profesor.
2. Seleccione en el menú la opción “Restaurar Imagen Windows 7 (64 bits)”. El proceso de restauración tarda bastantes minutos, por lo mientras se ejecuta puede aprovechar para empezar a leerse la segunda parte de la práctica y realizar los puntos 8 y 9.
3. Cuando vuelva a aparecer la misma pantalla con el menú del aula, seleccione la opción “Iniciar Sesión Windows 7 (64 bits)”.
4. Espere a que se cargue el SO Windows 7, inicie sesión con la clave **practicas**, y a continuación desactive el Firewall de Windows entrando en "Iniciar" > "Panel de control" > "Firewall de Windows" > ”Activar o Desactivar Firewall de Windows” y marcando las casillas correspondientes a los dos tipos de redes.
5. Los pasos del 1 al 4 tendrá que realizarlos en todas las prácticas de laboratorio de esta asignatura.
6. Observe que su PC tiene una etiqueta identificativa en el lateral, que dependiendo del laboratorio en el que se encuentre es diferente.
   Las etiquetas del laboratorio G1.31 son del tipo RED-X.
   Las etiquetas del laboratorio G1.33 son del tipo COM-X.
   Anote el código de la etiqueta identificativa de su PC.
7. Si ya ha hecho los puntos 8 y 9 de la segunda parte, continúe por el punto 10.

Segunda parte: Identificación de elementos del nivel físico de la red de acceso a Internet

Este laboratorio presenta unas características distintas a las aulas de ordenadores que se suelen utilizar en la ETSII. Por una parte, este laboratorio se comporta como un aula de ordenadores con acceso a Internet y, por otra parte, permite conectarse a una Intranet diseñada por el profesorado como se verá más adelante.

A continuación va a identificar elementos del nivel físico (cables, conectores, rosetas) que sirven para que su PC se conecte a la red de acceso a Internet de la Escuela (red ETSII).

8. Busque en la parte de atrás de su PC un cable que esté conectado al mismo. Sígalo y compruebe que acaba en una roseta empotrada en la pared cercana a su mesa. La roseta está a medio metro del suelo y justo debajo de ella hay uno o dos enchufes de corriente de color rojo. Esta roseta, externamente, se parece a las que se usan en la telefonía fija. El cable que ha localizado recibe coloquialmente el nombre de latiguillo, mide pocos metros y está acabado en ambos extremos por dos conectores RJ-45 macho (parecidos a los RJ-11, que son los utilizados en el teléfono fijo). Para que su PC pueda arrancar sin problemas, es importante comprobar antes de empezar cualquiera de las prácticas de la asignatura que dicho latiguillo esté conectado a la red ETSII, es decir, a esta roseta empotrada en la pared a medio metro de altura, debajo de su mesa y no a cualquier otra roseta. Compruebe que, efectivamente, está conectado a red ETSII.
9. La roseta a la que está conectado es una roseta doble, es decir, tiene dos puntos de conexión. Cada punto de conexión de cada roseta doble está etiquetado con un código único que sirve para identificar a este elemento de nivel físico y diferenciarlo de los otros puntos de conexión de otras rosetas. Tenga cuidado pues la etiqueta a veces está oculta por el conector del latiguillo. Anote el código de la etiqueta de su punto de conexión.
10. Para desconectar el latiguillo de la roseta empotrada debe presionar sobre una lengüeta que tiene el conector en uno de sus lados y tirar hacia fuera sin hacer fuerza. Desconecte ahora el latiguillo de la roseta empotrada en la pared. Observe el conector del latiguillo y podrá ver que existen 8 contactos metálicos distintos. Cada uno de estos contactos está unido a un cable que lo conecta a un contacto en el conector del otro extremo. Más adelante en el curso conocerá el funcionamiento de esta

interfaz física. El cable utilizado internamente en el latiguillo es igual al trozo de cable sin conectores que le ha suministrado el profesor. ¿Qué medio físico se está usando en la red ETSII?

11. Vuelva a conectar su latiguillo a la roseta con el código anotado en el punto 9.

12. ¿Qué tipo de red de acceso a Internet se usa en el aula?

13. ¿Qué tecnología se utiliza en este tipo de acceso?

14. ¿Según la nomenclatura vista en clase, qué nombre reciben los PC del aula?

Tercera parte: Comprobación configuración TCP/IP red de acceso a Internet (ipconfig)

La red ETSII sigue la arquitectura de Internet (TCP/IP). En esta arquitectura un sistema final (PC) requiere tener configurados, como mínimo, los siguientes **tres parámetros de nivel de red**:

- Una dirección de nivel de red propia (dirección IP) que lo identifique de manera única en Internet.
- La dirección de nivel de red de un router frontera que le de acceso a Internet, conocida en Windows como puerta de enlace predeterminada.
- Una máscara de subred.

(Nota: el significado y uso de estos parámetros se verá más adelante en la asignatura)

15. Los parámetros anteriores, y algunos más, forman parte de lo que se conoce como configuración TCP/IP. La configuración TCP/IP de un PC puede ser introducida manualmente o bien ser obtenida de forma automática por el propio PC. Si se hace de forma automática, la configuración TCP/IP se obtiene generalmente de un servidor DHCP usando el protocolo DHCP. Para ver la manera en la que se configura su PC siga estas instrucciones: haga clic con el botón derecho sobre el icono de **Red** presente en el escritorio y seleccione en el menú contextual la opción **Propiedades**. En la nueva ventana que le aparece haga clic en el texto **Conexión de área local** y en la ventana que le saldrá, titulada **Estado de Conexión de área local**, haga clic en el botón **Propiedades**. En la nueva ventana que aparece, busque, al final de un listado, el ítem **Protocolo de Internet versión 4 (TCP/IP v4),** selecciónelo y haga clic en el botón **Propiedades**. ¿De qué forma se configura TCP/IP en su PC? Cuando acabe cierre todas ventanas que le han aparecido.

16. Para ver los parámetros de la configuración TCP/IP de su PC puede utilizar el comando **ipconfig**, disponible en la mayoría de los SO Windows. Abra una ventana de **Símbolo del sistema** y ejecute en ella el comando **ipconfig /all** para ver toda la configuración TCP/IP de su PC. Puede abrir una ventana de **Símbolo del sistema** haciendo doble clic sobre el icono presente en el escritorio o bien mediante "Inicio" > "Todos los programas" > "Accesorios" > "Símbolo del sistema". Tenga en cuenta que la única información del comando ipconfig que nos va a interesar es la relativa al **Adaptador de Ethernet Conexión de área local**, por lo que no debe prestar atención a la información de los otros dos adaptadores etiquetados **Adaptador de túnel**. Por otro lado, tenga en cuenta que el comando **ipconfig** "a secas" ofrece un resumen con la información más importante de la configuración TCP/IP, pero que para verla toda hace falta el comando **ipconfig /all**.

17. ¿Cuál es la dirección IPv4 asignada a su PC? Observe que el cuarto número que aparece en la dirección IP coincide con el número que aparece en la etiqueta identificativa de su PC (la que anotó en el punto 5).

18. ¿Cuál es la máscara de subred?

19. ¿Cuál es la dirección IP de su puerta de enlace predeterminada (router frontera)?

20. ¿Cuál es la dirección IP del servidor DHCP?

21. La configuración TCP/IP obtenida automáticamente desde un servidor no tiene normalmente una validez "infinita" sino que el servidor nos concede una "licencia" de uso que expira al cabo de un tiempo (aunque podemos ir renovando dicha "licencia" de uso). ¿Cuántas horas o minutos de "licencia" de uso tiene su PC sobre la configuración TCP/IP actual?

22. Indique lo que ocurre al ejecutar el comando **ipconfig /release** en una ventana de **Símbolo del sistema**, (fíjese bien en los tres parámetros básicos de su configuración TCP/IP). A continuación ejecute también el comando **ipconfig /all** y piense en lo que ha conseguido al hacer el "release" de la configuración (liberación).

23. Indique lo que ocurre al ejecutar el comando **ipconfig /renew** (fíjese bien en los tres parámetros básicos de su configuración TCP/IP). A continuación ejecute también el comando **ipconfig /all** y piense en lo que ha conseguido al hacer el "renew" de la configuración (renovación).

24. En el área de notificación de la barra de tareas existe un icono que informa sobre el estado de la **Conexión de área local**, cambiando a veces su aspecto. Si hace clic sobre ese icono y luego clic sobre **Abrir Centro de redes y recursos compartidos** y a continuación hace clic en el texto **Conexión de área local** le aparecerá una ventana titulada **Estado de Conexión de área local** en la que podrá ver el estado de la conexión. ¿Cuál es el ancho de banda (R) de su conexión?

25. Desconecte el latiguillo de la roseta de la pared y observe que el icono cambia de aspecto. Además, si mueve el ratón sobre el icono le aparece un mensaje y si hace clic sobre él también podrá ver un mensaje. Fíjese bien en esos mensajes informativos y en el aspecto del icono.
26. Conecte de nuevo el latiguillo y observe que el icono vuelve a cambiar de aspecto. Además, si mueve el ratón sobre el icono le aparece un mensaje y si hace clic sobre él también podrá ver un mensaje. Fíjese bien en esos mensajes informativos y en el aspecto del icono.
27. ¿Es posible saber si el cable está conectado/desconectado observando este icono? Esto sería una prueba de funcionamiento del nivel físico, conocida como "conectividad de nivel físico".

Cuarta parte: Conectividad a nivel 3. Retardo ida y vuelta (ping)

El comando **ping** sirve para probar que dos equipos que tengan implementado el nivel de red (sistemas finales y routers) pueden intercambiar entre ellos las PDU de ese nivel (R_PDU), es decir, permite realizar una prueba de conectividad de nivel de red. Al ejecutar este comando desde un equipo origen hacia un equipo destino, el origen envía al destino una R_PDU especial (**solicitud de eco**), que cuando la recibe está obligado a responder al origen con otra R_PDU especial (**respuesta de eco**).

28. El comando **ping** se debe ejecutar en una ventana de **Símbolo del sistema** y requiere como parámetro obligatorio la dirección IP o el nombre del equipo destino. Haga un **ping** desde su PC usando como equipo destino su router frontera (véase el punto 19). Por defecto, el comando **ping** de Windows 7 envía cuatro R_PDUs al equipo destino, es decir, realiza cuatro pruebas de conectividad de nivel de red. El comando ping nos muestra en pantalla una línea de información para cada una de las cuatro solicitudes de eco enviadas. Si de una solicitud de eco ha recibido una respuesta de eco, la línea de información empieza por "Respuesta desde" y a continuación aparece la IP del equipo que nos ha enviado la R_PDU. ¿Cuántas respuestas del router frontera ha recibido el comando **ping** que acaba de ejecutar?

29. ¿Es obligatorio que en el otro extremo (equipo destino) exista una entidad par de nivel de red para que el comando **ping** reciba respuesta?

30. ¿Utiliza el comando **ping** los servicios de algún nivel para enviar la R_PDU? En caso afirmativo indique el nombre del nivel y el porqué.

31. Haga un **ping** al equipo 8.8.8.8. Observe como en la información que ofrece el comando **ping** cuando recibe la respuesta de cada una de las solicitudes de eco informa del tiempo transcurrido desde que se inició el envío de la R_PDU en el equipo origen hasta que se recibió la R_PDU de respuesta de eco. Comprueba si las cuatro solicitudes han obtenido respuesta y si lo han hecho en el mismo tiempo.
32. La R_PDU en su viaje de ida y vuelta atraviesa varios nodos intermedios (routers), cada uno de los cuales contribuye con su retardo nodal al retardo que nos muestra el comando **ping**. ¿Qué fuentes de retardo contribuyen al retardo nodal?

Quinta parte: Identificación de elementos del nivel físico de la Intranet del laboratorio

La Intranet del laboratorio, LAB_DTE, es una red que se comporta igual que Internet pero en un entorno controlado por los profesores. En ella aparecen los mismos elementos hardware (enlaces cableados e inalámbricos, routers,...) y software (protocolos, aplicaciones en red,..) que podemos encontrar en Internet. La tecnología usada para conectarnos a la Intranet es la misma que se usa en una red de acceso Institucional o Empresarial, es decir, se usa tecnología Ethernet.

La Intranet del laboratorio sigue la normativa vigente con respecto al cableado estructurado, es decir, sigue la forma correcta en la que se debe realizar el tendido de cables para instalar una red en un edificio. Todos estos aspectos son tareas que pertenecen al nivel físico en la arquitectura en capas. Un objetivo del cableado estructurado es centralizar en uno o varios puntos de un edificio (**armarios de interconexión**) toda la **electrónica de red** (dispositivos de diferentes niveles del modelo OSI que permiten realizar un conjunto de funciones bien conocidas), la cual normalmente se encuentra montada en un **bastidor (rack)**. El otro objetivo es centralizar el acceso al **cableado de red**, por lo que desde unos **paneles de parcheo** ubicados en los armarios de interconexión parten cables que se distribuyen por todo el edificio, terminando cada uno de ellos en un **punto de conexión** a la red dentro de una **roseta** que, normalmente, estará ubicada en la pared.

En la Intranet del laboratorio, las rosetas podemos verlas en la pared más cercana a nuestra mesa. Se trata de una roseta doble de montaje superficial (no empotrada) situada a una altura bastante superior al borde la mesa en la que se encuentra nuestro PC. Desde cada una de las rosetas parten dos cables, ocultos por la canaleta horizontal que se ve en la pared, hacia un par de paneles de parcheo situados en una de las paredes del laboratorio. Nótese que son dos cables porque la roseta tiene dos puntos de conexión. Cerca de los paneles de parcheo hay un bastidor (rack) en el que está montada la electrónica de red. Por motivos prácticos y de facilidad de acceso a los diversos elementos a la hora de hacer las prácticas, en el laboratorio los paneles de parcheo están atornillados a la pared en lugar de estar ubicados en el bastidor (rack) y además el bastidor no está fijo en un punto y protegido dentro de un armario de interconexión, sino que tiene ruedas y se puede acceder a él fácilmente.

A continuación va a identificar elementos del nivel físico (paneles de parcheo, rosetas, latiguillos) que sirven para que su PC se conecte a la Intranet del laboratorio.

33. En la pared más cercana a su mesa, a una altura superior al borde de la mesa podrá encontrar varias rosetas cuadradas de color crema. Cada roseta es doble y alberga en su interior dos puntos de conexión, accesibles desde su parte inferior. En el frontal de la roseta hay dos etiquetas identificativas, una por cada uno de los dos puntos de conexión. El identificador de la etiqueta izquierda sigue el formato "A XX" y el de la derecha es "B XX". Escoja una roseta cuadrada para realizar la práctica y anote el código que aparece en la etiqueta de la izquierda, con el formato "A XX". Como norma general, el punto de conexión etiquetado con "A XX" se va a utilizar para conectarse a la Intranet del laboratorio y el etiquetado con "B XX" se usa para otras tareas de configuración de la electrónica de red. Como ya hemos dicho, de las rosetas parten cables ocultos por una canaleta que las conectan con los paneles de parcheo de la pared. Un panel de parcheo es un dispositivo de nivel físico que permite agrupar en un único punto muchos puntos de conexión dispersos por el laboratorio. Desde un punto de vista externo podemos ver "n" puntos de conexión idénticos a los que podemos ver en las rosetas. Cada punto de conexión del panel de parcheo se conoce como **puerto** y cada uno de ellos tiene una etiqueta identificativa idéntica a la que aparece en el punto de conexión del otro extremo del cable (en la roseta).

34. Busque en la pared del laboratorio (entrando en él, a mano derecha) los paneles de parcheo que hay. Fíjese bien en la numeración de los puertos. ¿Cuántos paneles de parcheo hay y cuántos puertos tiene cada uno?

35. Localice en uno de los paneles de parcheo el puerto etiquetado con un identificador que sigue el formato "A XX" y que sea igual al que usted apuntó en el apartado 33.

36. Podrá ver, cerca de los paneles de parcheo un bastidor (rack) con diversos equipos, algunos de los cuales están conectados a los paneles de parcheo. Dependiendo del laboratorio en que se encuentre usted, los equipos que encontrará en el rack serán diferentes.
En el rack del **laboratorio G1.31** podrá encontrar un equipo etiquetado **HUB_ASIA**, mientras que en el rack del **laboratorio G1.33** podrá encontrar un equipo etiquetado **HUB_NORTEAMERICA**.

37. Localice en el rack el **HUB_ASIA** o el **HUB_NORTEAMERICA**. Fíjese en que este dispositivo tiene en su frontal muchos puertos, similares a los del panel de parcheo, y unos indicadores LED, uno por cada puerto. El LED asociado a un puerto sólo se encenderá si hay un cable conectado en ese puerto y, además, el equipo detecta que hay conectividad a nivel físico con un equipo ubicado en el otro extremo. Un PC normal suele tener también un LED con la misma finalidad, justo al lado del conector en el que enchufamos el latiguillo que nos une a la red. En los PC del laboratorio esa funcionalidad la implementa el LED inferior que aparece a la derecha del conector, en este caso sólo se enciende en color verde o naranja si la R es 100 Mbps o 1Gbps, cuando R ese 10 Mbps no se ilumina, por lo que no nos es útil para probar la conectividad a nivel físico, teniendo que recurrir a pruebas como la que hicimos en el apartado 27. El HUB es un dispositivo de nivel físico, más adelante en el curso conocerá su funcionamiento.

38. ¿Qué indicadores LED hay encendidos en el HUB que localizó en el apartado anterior?

39. Localice en el laboratorio el código identificativo del PC (formato RED-X o COM-X) que está conectado al puerto 16 del HUB que localizó en el apartado 37.

Sexta parte: Conexión a la Intranet del laboratorio

40. Desconecte su latiguillo de la roseta de la pared (la de debajo de la mesa, de la red ETSII).

41. Conecte el latiguillo a la roseta que escogió en el apartado 33, en el punto de conexión de la izquierda, etiquetado según el formato "A XX".

42. Observe el icono de notificación  y compruebe si existe conectividad a nivel físico. Explique si es posible en estas condiciones que algún equipo pueda responder a un **ping** enviado desde su equipo.

43. Pídale al profesor un nuevo latiguillo y conecte un extremo al panel de parcheo, en el puerto que tenga la misma etiqueta (formato "A XX") que el punto de conexión al que conectó el latiguillo de su PC en el apartado 41.

44. Conecte el otro extremo de ese latiguillo a cualquier puerto libre del **HUB_ASIA** o del **HUB_NORTEAMERICA**.

45. ¿De qué formas puede comprobar que existe conectividad a nivel físico entre su PC y el HUB del apartado anterior?

46. En la Intranet del laboratorio, al igual que en la red de acceso a Internet, los PC conectados a ella requieren de una configuración TCP/IP específica que se obtiene automáticamente de un servidor DHCP. Realice los pasos oportunos para obtener de forma automática la nueva configuración TCP/IP de su PC (Pista: repase lo que hizo en los apartados 22 y 23 para hacer un "liberar" y un "renovar" la configuración TCP/IP). Compruebe que la configuración TCP/IP de su PC no coincide con la que tenía en la tercera parte de la práctica. (Avise al profesor en el caso de que sí coincida). Es probable que durante el proceso de conexión a la Intranet del laboratorio le haya aparecido una ventana llamada “Establecer ubicación de red”. Si eso ocurre escoja con doble clic la opción “Red de trabajo” y cierre luego dicha ventana.

47. ¿Cuál es ahora el ancho de banda (R) de su conexión?

48. ¿Por qué cree que no coincide el ancho de banda actual con el del apartado 24?

Séptima parte[1]: Retardo salto a salto (tracert)

Tracert es un comando que sirve para ver por qué routers pasan las R_PDU en el camino de ida desde un equipo origen hasta un equipo destino. El comando **tracert** se ejecuta en el equipo origen en una ventana de **Símbolo del sistema** y, de forma parecida al comando **ping**, el único parámetro obligatorio es la dirección IP del equipo destino.

La salida del comando **tracert** nos muestra una línea por cada uno de los routers que forman parte del camino desde el origen al destino. El primer router es el más cercano al origen. Cada línea asociada a un router muestra los retardos de ida y vuelta (en ms) de tres R_PDU que han llegado a dicho router y han vuelto al equipo origen.

La última línea es diferente, puesto que muestra información del equipo destino y no de los routers intermedios.

El comando **tracert** utiliza para obtener toda esta información unas técnicas más complejas que las usadas por el comando **ping**, las cuales veremos más adelante, durante el curso.

49. Si su equipo es del tipo **RED-X** ejecute el comando **tracert** dirigido al equipo destino **com-101.nam.lab** y si su equipo es del tipo **COM-X** ejecute el comando **tracert** dirigido al equipo destino **red-10.as.lab**. Nota: sepa que los equipos **com-101.nam.lab** y **red-10.as.lab** son sistemas finales conectados a la Intranet.

50. Observe la salida del comando **tracert** y diga cuántos routers hay en el camino desde su PC al equipo destino. Realice un gráfico en el que represente a los dos sistemas finales y los routers intermedios si estos están conectados unos a otros mediante enlaces de comunicación cableados. En el gráfico debe indicar el retardo de ida y vuelta mínimo que hay entre el sistema final origen y cada uno de los routers que hay en el camino hacia el sistema final destino, así como el retardo de ida y vuelta mínimo del sistema final origen al destino. Avise al profesor para que le revise el gráfico.

[1] Si no le diera tiempo a realizar esta parte del estudio experimental en el laboratorio puede hacerlo en casa. Sólo tiene que hacer el **tracert** dirigido a **8.8.8.8**. Puede venir a las tutorías de su profesor/a de prácticas a revisar si los resultados son correctos. Para ello debe traer la salida del comando.

51. Explique por qué los retardos de ida y vuelta a los routers que aparece en la gráfica del apartado 50 van aumentando conforme nos alejamos del origen.

52. Usando la gráfica que ha realizado en el apartado 50, estime el retardo de ida y vuelta entre el primer router y el segundo router, el segundo y el tercero y así sucesivamente hasta alcanzar al sistema final destino. Anótelo en el gráfico que ha realizado en el apartado 50.

53. Si suponemos que el factor más influyente en el retardo de ida y vuelta entre dos equipos adyacentes es el ancho de banda del enlace entre ambos, ordene de menor a mayor el ancho de banda de los enlaces que intervienen en el camino del **tracert** que ha ejecutado y anótelo en el gráfico del apartado 50 indicando con R1 el menor ancho de banda y Rn el de mayor, siendo *n* el número de enlaces. Avise al profesor para que le revise el gráfico.

Octava parte[2]: Familiarización analizador Wireshark

Wireshark es un programa que, ejecutado en un sistema final es capaz de capturar todo el tráfico de red recibido o enviado por dicho sistema a través de su interfaz de red, es decir, las tramas o E_PDUs que llegan o salen de la interfaz de red del equipo en el que se esté ejecutando. Es una herramienta de gran utilidad, pues no sólo captura el tráfico sino que además es capaz de analizarlo mostrando al usuario información detallada de los protocolos de cada uno de los niveles (desde el nivel de enlace de datos hasta el nivel de aplicación). Es por ello que recibe el nombre de analizador de protocolos.

54. Haga doble clic en el icono del escritorio para arrancar el analizador de protocolos **Wireshark**. En la Figura 1 se muestra la pantalla inicial que aparece al arrancar Wireshark y la Tabla 1 muestra un resumen de los iconos de Wireshark que más se van a utilizar en las prácticas.

55. Puede iniciar una captura de diversas formas. La primera forma es seleccionar en la pantalla inicial de Wireshark (si no estuviera ya seleccionada), la **Conexión de área local** y luego hacer clic en **Start**. Otra manera es hacer clic sobre el icono que aparece en el menú. Y la otra manera es hacer clic en el icono del menú para abrir una ventana en la que aparece el listado de todas las interfaces de red que se pueden usar, seleccionar la que nos interesa (la **Conexión de área local** descrita como **Realtek PCIe GBE Family Controller**) y luego pulsar el botón **Start**. Sabiendo esto, ponga a Wireshark a capturar tráfico usando el método que prefiera. Si todo lo ha hecho bien, le aparecerá en una ventana las tramas que en ese momento están llegando o saliendo de su PC, las cuales están siendo capturadas por . Avise al profesor antes de continuar.

56. Abra Mozilla Firefox y acceda con el navegador a la página **http://www.redes.lab** ubicada en un servidor web de la Intranet del laboratorio.

57. Espere 20 segundos y detenga la captura de Wireshark haciendo clic en el icono . Guarde la captura en un fichero para llevársela cuando acabe la práctica. Para ello haga clic sobre el icono , introduzca el nombre del fichero y luego sobre guardar. Para cargar esta captura previa sólo tendría que abrirla pulsando sobre el icono e indicar la ubicación del fichero con la captura para que Wireshark la muestre.

[2] Si no le diera tiempo a realizar esta parte del estudio experimental en el laboratorio puede hacerlo en casa. Puede utilizar la captura que le adjuntamos "**LAB1-exp-redeslab.pcapng**" o hacer su propia captura. Sólo tiene que instalar Wireshark en su equipo (dejando las opciones de instalación "por defectgo") y abrir la siguiente página web: **http://www.dte.us.es/personal/smartin/lab3/paginasimple.html** de Internet en vez de la indicada en el estudio experimental.

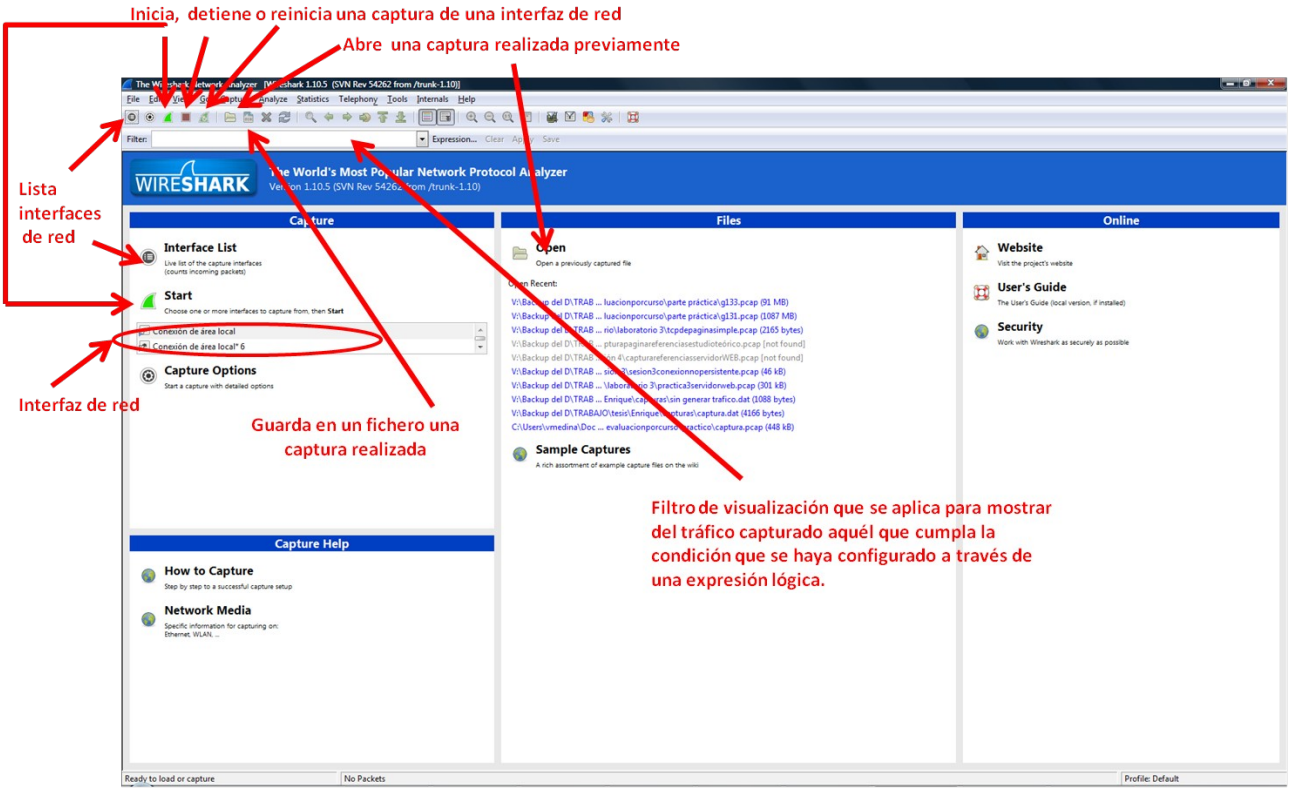

Figura 1: Pantalla inicial al arrancar Wireshark.

	Muestra las interfaces disponibles para capturar		Reinicia una captura (detiene la actual e inicia una nueva).
	Detiene una captura		Inicia una captura
	Abre un fichero con una captura previa		Guarda un fichero con la captura actual

Tabla 1: Iconos de Wireshark más utilizados.

58. Fíjese en las tres partes (listado de tramas, detalles de tramas y octetos que forman la trama) de la ventana principal donde se visualiza la captura que ha realizado . En la Figura 2 se puede consultar lo que se muestra en cada parte.

59. Muévase por el **listado de tramas** y, usando la información que aparece en "Protocol" busque tramas que encapsulen PDUs de los protocolos típicos de Internet cuyas siglas averiguó en el último apartado del estudio teórico. Fíjese en que si hace clic en el nombre de la columna "Protocol" ordenará el listado de tramas por este campo). Tenga en cuenta que a nivel de enlace todas las tramas capturadas usan el protocolo Ethernet.

60. Haga clic en cada trama del listado de tramas que encapsule a uno de los protocolos de los encontrados en el apartado 59 y, aprovechando la información mostrada en la parte "detalle de la trama", realice un gráfico en el que se muestren los niveles de la arquitectura TCP/IP que se utilizan, empezando por el de más alto nivel y terminando en el de enlace, e indique para cada nivel el protocolo que usa.

Novena Parte: Continuando con el aprendizaje del manejo del analizador Wireshark

Wireshark es capaz de utilizar los servicios de DNS para, en sus diversas ventanas, mostrarnos siempre nombres de host y dominio, en lugar de mostrarnos las direcciones IP equivalentes, en el formato numérico xxx.xxx.xxx.xxx habitual. Esa característica nos será de mucha utilidad en esta práctica. Entre en "Edit" → "Preferences", pulse "Name Resolution" en el panel de la izquierda, **active** la opción **"Resolve Network (IP) addresses"**. Wireshark también es capaz de mostrarnos, en lugar de los números de puerto TCP y UDP, el nombre del protocolo que usa habitualmente dicho número de puerto. En esta práctica concreta no nos interesa habilitar esta funcionalidad de Wireshark. Entre en "Edit" → "Preferences", pulse "Name Resolution" en el panel de la izquierda, **desactive** la opción **"Resolve Transport Name"** y pulse **"OK"** para cerrar la ventana y que tengan efecto los cambios.

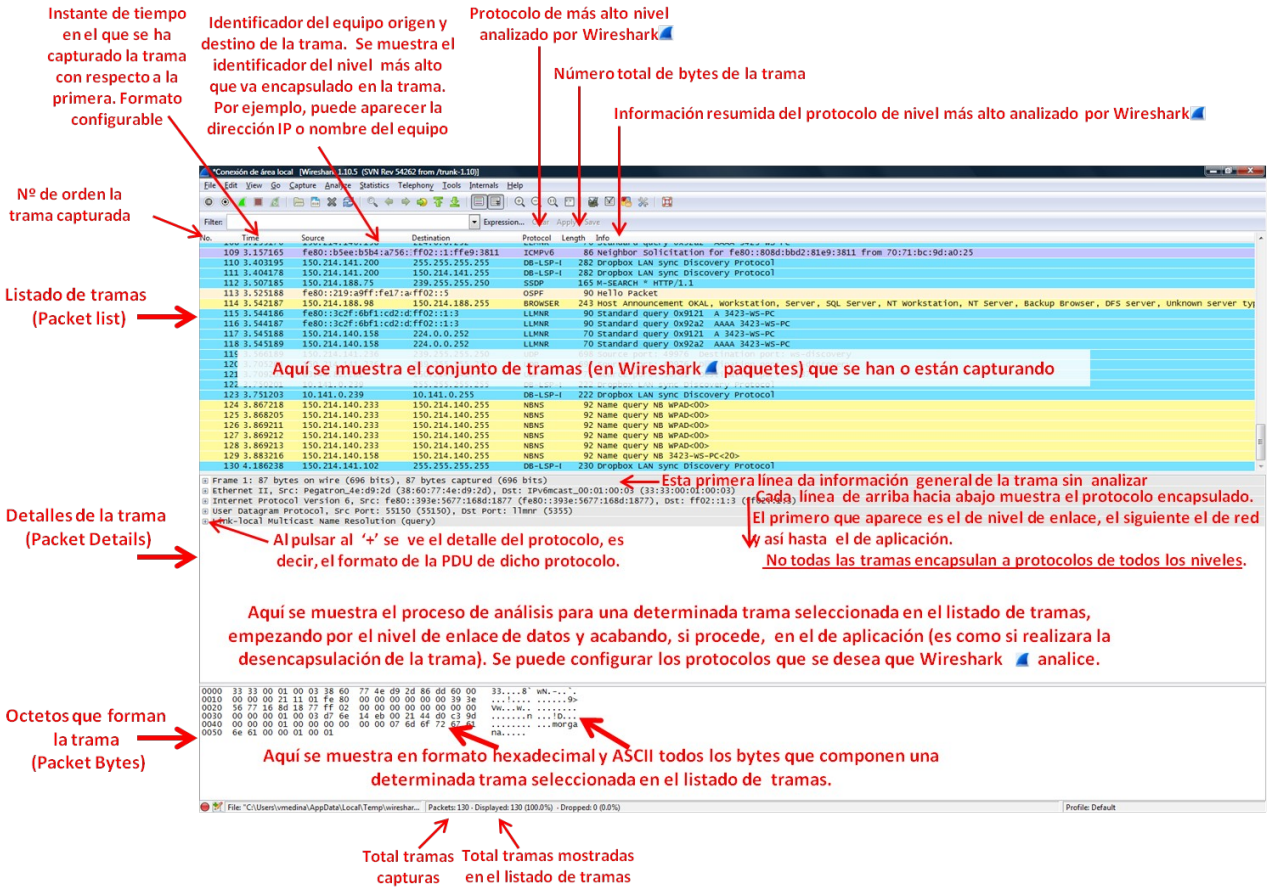

Figura 2: Descripción de las diferentes partes que componen la herramienta.

En el listado de tramas podemos ver mucha información de cada trama, organizada en columnas. Las que aparecen por defecto son:

- La primera columna se llama "No." y nos muestra el número de orden en el que se han ido capturando las tramas, de la 1 a la N.
- La segunda columna se llama "Time" y en ella Wireshark nos muestra, en segundos, información temporal del instante en que fue capturada esa trama. Por defecto este tiempo se mide desde el instante en que se capturó la primera trama, por lo que en la trama número 1 es 0.000000.
- La columna "Source" muestra información del equipo que envió la trama (o el que envió alguna PDU encapsulada en dicha trama, depende de cómo hayamos configurado Wireshark).
- La columna "Destination" es análoga a la anterior, mostrándonos información del equipo destino.
- La columna "Protocol" muestra información de protocolo de más alto nivel encapsulado en esa trama y que es capaz de analizar.
- La columna "Length" muestra el número de bytes de la trama. En la última sesión de laboratorio se verá qué campos de la trama (E_PDU) incluye.
- La columna "Info" muestra información resumida del protocolo de más alto nivel que es capaz de analizar en esa trama.

Es posible quitar y añadir columnas de información al listado de tramas, para adaptarlo a nuestras necesidades en cada momento. Será interesante añadir dos nuevas columnas que nos presenten información de los puertos de origen y de destino de las T_PDU de los protocolos TCP y UDP. Con esto podremos identificar el número de puerto usado para identificar al proceso de aplicación cliente y servidor en una trama que encapsule protocolos hasta el nivel de aplicación. Para hacerlo debe seguir estas instrucciones:

61. Entre en "Edit" → "Preferences", y pulse en la rama "Columns" (dentro de "User Interface" en el panel de la izquierda).

62. Pulse el botón "Add" una vez para añadir una nueva columna.

63. Haga clic en el texto "New column" que ha aparecido, y edítelo escribiendo como título de la nueva columna el texto "SrcPort" y pulsando "Intro" en el teclado.

64. En el campo "Field Type" debe seleccionar de la lista desplegable el valor "Src Port (unresolved).

65. Repita los pasos b), c) y d) para crear otra columna con título "DstPort" y que tenga "Dest Port (unresolved)" de "Field Type".
66. Pulse "OK" para cerrar la ventana "Preferences".
67. Observe que en el listado de tramas aparecen las dos nuevas columnas en la parte de la derecha (si no puede verlas desplácese hacia la derecha). Utilice el ratón para reordenar las columnas y colocar las dos nuevas delante de la columna "Info" o bien ajuste el ancho de la columna "Info" para que se muestren todas ellas en pantalla sin tener que desplazarse.

Como ya sabe, la ventana principal de Wireshark está dividida en tres paneles. Ya hemos repasado el panel superior, el listado de tramas. Los otros dos paneles están muy relacionados con el panel superior, pues nos muestran información de la trama que hayamos seleccionado en el listado de tramas.

El panel central, "Detalles de la trama", muestra diversa información de la trama y de su contenido, de forma ordenada y estructurada por niveles. En primer lugar se muestra información de la trama completa y luego se va mostrando información de cada uno de los niveles, empezando desde el nivel de enlace, a continuación red, transporte y aplicación (si es que aparecen todos, cosa que no siempre ocurre). En cada línea hay un "+" a la izquierda para desplegar la información del protocolo asociada a cada nivel (una vez interpretada por la herramienta). No toda la información que aparece de un determinado protocolo forma realmente parte de dicho protocolo. A veces Wireshark añade información que ha determinado como resultado de un análisis que ha realizado a nivel global, en cuyo caso esta información aparece entre corchetes [ ]. Por otro lado, tampoco todo lo que aparece detrás de un "+" es necesariamente un protocolo. Por ejemplo, Wireshark es capaz de analizar diferentes formatos de ficheros como GIF, PNG, JPG, etc. y los muestra a la derecha de un "+". Seleccione con el ratón una trama que en la columna "Protocol" muestre HTTP y fíjese en los nombres de los protocolos que aparecen en el panel central.

El panel inferior, "Bytes de la trama", muestra un volcado en hexadecimal y en ASCII del contenido de la trama seleccionada. Los datos en hexadecimal (en la parte izquierda) se presentan en filas de 16 bytes, junto con una primera columna que indica la posición relativa (dentro de la trama) del primer octeto de la fila. Si en el panel central se hace clic en alguno de los niveles (o en algún campo dentro de estos) se resaltan con fondo oscuro en el panel inferior los bytes asociados a aquello sobre lo que hemos hecho clic. Al revés también funciona, pulsando sobre bytes del panel inferior y viendo en el panel central como se selecciona el campo de información correspondiente. Haga clic en "detalles de trama" en "Hipertext Transfer Protocol" para seleccionar el protocolo HTTP. ¿Qué información aparece en ASCII en "bytes de tramas"? Pulse sobre el "+" que aparece al lado de "Hipertext Transfer Protocol" en "detalles de trama", observará el contenido de la HTTP_PDU. Haga clic varias veces en diferentes líneas de cabecera y observe como se ve en ASCII esa información. ¿Cómo se muestra en ASCII los códigos de control '\r' y '\n"?

Respecto a las marcas de tiempo, mostradas en la columna "Time" del listado de tramas, la primera trama tiene por defecto la marca 0.000000 segundos y el resto de marcas van incrementándose respecto a esta. No obstante, es posible establecer una marca de referencia en cualquier trama de forma que sea el "cero" para todas las tramas a continuación de ella, que verán su marca de tiempo modificado considerando esa referencia, lo cual es útil para medir tiempos entre tramas desde una primera que será la que tomemos como "referencia". Para ello seleccionamos la trama que queremos marcar como referencia con clic-derecho y elegimos "Set Time Reference (Toggle)", apareciendo ***REF*** en esa trama y modificándose el tiempo de las tramas siguientes. Si repetimos la operación se quita la referencia de esa trama. Tenga en cuenta que puede haber varias "referencias locales" en el listado de tramas.

Fíjese que en el listado de tramas hay varias tramas que contienen PDUs del protocolo HTTP (fíjese en el valor de la columna "Protocol"). Concretamente, debe encontrar una trama que muestre en la columna "Info" que contiene una petición GET del protocolo HTTP.

La petición GET la ha emitido el proceso cliente, que está asociado a un determinado puerto en el host origen ("source host"). Gracias a la columna SrcPort (puerto fuente o puerto origen) podemos averiguar con facilidad el número de puerto asociado al proceso cliente.

Compruebe que el valor numérico de la columna DstPort de la trama que encapsula el GET es el valor habitual usado por un proceso servidor del protocolo HTTP. Anótelo.

Compruebe también que en la columna “Destination” NO aparece como nombre del servidor www.redes.lab sino otro distinto (webserver.af.lab). Esto es debido a que www.redes.lab es un alias de webserver.af.lab, es decir, ambos son nombres asociados al mismo sistema final. El nombre principal se conoce como CNAME o nombre canónico en la terminología DNS (Canonical NAME) y es el que aparece en la columna “Destination”. Anote la correspondencia entre el nombre canónico y el alias del servidor web.

Ahora vamos a hacer que la trama con el GET pase a ser la "referencia temporal" con respecto a la cual medir los tiempos de captura de las tramas capturadas detrás de ella. Para ello seleccione dicha trama haciendo clic sobre ella con el botón derecho del ratón y seleccione en el menú contextual que le aparece la opción "Set Time Reference (Toggle)". Fíjese que ahora esa trama no tiene marca de tiempo en la columna "Time" sino que aparece el texto ***REF*.** Es posible anular esta operación repitiendo los mismos pasos que hemos dado sobre esa trama.

Localice, detrás de la trama del GET, una trama que encapsule la respuesta HTTP a dicho GET. En la columna "Info" de la respuesta debe aparecer la línea de estado "HTTP/1.1 200 OK" o bien la línea de estado "HTTP/1.1 304 Not modified", dependiendo de las circunstancias en que se generó el GET con Mozilla Firefox.

Compruebe que en la respuesta se usan los mismos puertos que en la solicitud, pero puerto origen es ahora puerto destino y viceversa.

Compruebe que ocurre lo mismo con los valores de las columnas "Source" y "Destination".

Como hemos hecho que la trama del GET sea la referencia temporal de todas las tramas que le siguen, es muy fácil medir el tiempo transcurrido entre la emisión del GET y la recepción de la respuesta.

¿Cuánto vale el RTT entre su PC y el servidor web www.redes.lab?

Wireshark es capaz de, a partir de una trama cualquiera que contenga una T_PDU del protocolo TCP (o UDP), localizar todas las demás T_PDU que se transmitieron en la misma conexión TCP que ella (o en el caso de UDP, las T_PDU entre el mismo cliente y servidor usando una determinada pareja de puertos UDP). Gracias a eso puede mostrarnos el flujo de bytes transmitidos a través de esa conexión TCP por los procesos cliente y servidor (o el intercambio de A_PDUs en el caso de UDP). Seleccione la trama del GET haciendo clic sobre ella con el botón derecho del ratón y seleccione en el menú contextual que le aparece la herramienta "Follow TCP Stream". (Nota: Para UDP sería "Follow UDP Stream")

En la ventana "Follow TCP Stream" podemos ver en color rosa los bytes enviados por el proceso cliente y de color morado los bytes enviado por el proceso servidor. Si el cliente y el servidor mantienen un diálogo "largo" a través de una misma conexión (como en las conexiones HTTP persistentes) podría verse como se van alternando los mensajes del cliente y del servidor.

Décima parte: Filtros de visualización

En el cuadro de texto etiquetado "Filter:" que aparece bajo la barra de iconos de Wireshark puede escribir una expresión lógica con una determinada sintaxis, que hace que se muestren en el listado de tramas sólo aquellas que hacen que la expresión lógica sea cierta. Esta expresión lógica recibe el nombre de "filtro" y sólo afecta a lo que se muestra en el listado de trama, es decir, ni elimina una trama ya capturada ni tampoco es tenido en cuenta a la hora de decidir si una trama debe o no capturase. Se trata sólo de un filtro de visualización ("display filter") y no de un filtro de captura ("capture filter").

Hay muchas expresiones de filtrado que podemos introducir para cada protocolo reconocido por Wireshark. Puede ver todas las expresiones que hay para cada protocolo, haciendo clic en el botón "Expression...", pero si conoce la expresión puede escribirla directamente en el cuadro de texto "Filter:". Wireshark va mostrando una ayuda con las expresiones compatibles con lo que ya lleva escrito e incluso las autocompleta a medida que las escribe. Si la expresión es correcta aparecerá con fondo VERDE y si es incorrecta el fondo será ROJO. Para que Wireshark utilice el filtro que acabamos de escribir, es necesario pulsar sobre "Apply", opción que podemos ver a la derecha del filtro. Si deseamos volver a ver todas las tramas basta con pulsar sobre "Clear". Pulse ahora sobre "Clear" si el cuadro de texto "Filter:" mostrase algún filtro. Algunas expresiones básicas son:

- "ip.addr == 193.1.10.1", que muestra tramas que contienen R_PDUs cuya dirección IP origen o destino sea la 193.1.10.1.
- "tcp.port == 80", para mostrar el tráfico con número de puerto origen o destino el 80.
- "udp.port == 53", que hace lo mismo pero con UDP.
- "ip.src" y "ip.dst" son parecidos a "ip.addr" pero sólo se fijan en que la IP especificada esté en el origen o en el destino.
- "tcp.dstport" y "tcp.srcport" se fijan solamente en el puerto destino o el origen.
- "http", "dns", "tcp", "udp" y "icmp" son expresiones sencillas que hacen que sólo se muestren tramas que encapsulen PDUs de esos protocolos.

Es posible construir expresiones lógicas complejas combinando expresiones sencillas con los operadores lógicos "and", "or" y "not". Por ejemplo "http or dns" captura tramas que hacen que la expresión lógica "combinada" sea cierta. Es decir, aquellas que hacen que "http" sea cierta y también aquellas que hacen que "dns" sea cierta. También es posible utilizar el operador "contains" que permite buscar cadenas dentro de la PDU de un protocolo, por ejemplo, "http contains GET" permitiría ver todas las tramas que encapsulan PDUs HTTP que contienen la palabra "GET". Otro ejemplo con este operador sería "dns contains www" que nos dejaría ver solo las tramas con PDUs DNS en las que aparezca la cadena "www".

Fíjese que si marca una trama como referencia temporal con ***REF*** (recuerde el apartado), esa trama siempre se visualiza en el listado de tramas, sea cual sea el filtro de visualización aplicado.

Si no tiene una captura hecha que le llene completamente el listado de tramas, haga una nueva generando el tráfico de red que sea necesario y luego detenga la captura.
Escriba un filtro sencillo, como "http", "tcp", "udp", etc. y aplíquelo.
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.
Haga clic en "Clear" para borrar el filtro de visualización y volver a ver todas las tramas capturadas.
Aplique un filtro que muestre sólo el tráfico de nivel de red con origen o destino la dirección IP de su PC.

68. Cierre wireshark y el navegador, o y cualquier otra ventana que haya abierta en su PC.
Desconecte su PC de la Intranet del laboratorio.
Conecte su PC a la red de acceso a Internet (red ETSII) en el mismo punto de conexión y roseta del apartado 9.
Apague el PC.
Vuelva a dejar en su sitio el latiguillo que conectó al **HUB_ASIA** o al **HUB_NORTEAMÉRICA**.
Devuelva el trozo de cable sin conectores que se le entregó, dejándolo en la de la mesa del profesor.