Práctica 1: Wireshark

1. Abre el programa Wireshark y captura todas las tramas durante un minuto aproximadamente. En ese tiempo, abre el navegador, carga varias páginas, realiza una búsqueda en el Google…

2. ¿Cuántas tramas has capturado? Aproximadamente, ¿cuántas tramas por segundo han pasado por la tarjeta de red de tu equipo?

3. Guarda todas las tramas capturadas en el fichero prac1.cap

4. Selecciona una trama cualquiera, por ejemplo, la nº 123. ¿Cuántos bytes ocupa? ¿Y la trama que fue capturada en el segundo 5.0000?

5. Busca una trama que en el campo protocolo tenga “HTTP”. ¿En qué color aparece? ¿Qué protocolo de nivel de enlace utiliza? ¿Y en el nivel de red? ¿Y en el de transporte?

6. Busca una trama cuya dirección MAC origen sea tu dirección MAC. ¿A quién va destinada?

7. Mirando las opciones de captura, realiza las siguientes capturas:
    a. Capturar tramas durante 20 segundos únicamente.
    b. Capturar tramas de manera que cada 500 KB capturados vayan a un nuevo fichero de nombre ejer9.cap
    c. Capturar únicamente 50 tramas.

8. Indica para qué sirve cada uno de los botones de la barra de herramientas:

Práctica 1: Wireshark (II) : Búsqueda de tramas Ethernet

Empleando el panel de expresiones para filtrar las tramas del Wireshark, realiza las siguientes búsquedas tras haber capturado durante un minuto las tramas de circulan por la tarjeta de red de tu equipo:

9. Tramas que mi tarjeta de red envía.

10. Tramas que van dirigidas a mi tarjeta de red.

11. Tramas que mi tarjeta de red envía a la dirección de broadcast.

12. Tramas que no van destinadas a mi tarjeta de red.

13. Tramas cuyo tipo no sea 0x0800.

14. Tramas que mi tarjeta de red envía y cuyo tipo no sea 0x0800.

15. Tramas cuya longitud sea superior a 1500 bytes.

16. Tramas que mi tarjeta de red envía o recibe.

17. Tramas enviadas a mi equipo por la tarjeta de red de cualquier compañero, y que sean superiores a 300 bytes.

18. Tramas cuya dirección destino sea una dirección MAC de multicast o de broadcast.

19. Tramas enviadas a mi tarjeta de red por una tarjeta de red cualquiera fabricada por “Dell Computers”. Consulta información sobre los OUI en:

    http://es.wikipedia.org/wiki/OUI
    http://standards.ieee.org/regauth/oui/index.shtml
    http://www.wireshark.org/tools/oui-lookup.html

Práctica 1: Wireshark (III) : Protocolo IP

Empleando el panel de expresiones para filtrar las tramas del Wireshark, realiza las siguientes búsquedas tras haber capturado tramas de circulan por la tarjeta de red de tu equipo:

20. Datagramas cuya IP destino sea la del router.
21. Datagramas cuya IP origen sea la de tu propio equipo.
22. Datagramas cuya IP destino sea la del router, y su versión de IP sea 4.
23. Datagramas cuya longitud de la cabecera IP sea distinta de 20 bytes.
24. Datagramas con longitud total entre 500 y 1000 bytes.
25. Datagramas con un TTL mayor que 10.
26. Datagramas que vayan dirigidos a un nivel de transporte UDP.
27. Datagramas con un desplazamiento distinto a 0.
28. Datagramas destinados a tu equipo que utilicen TCP en el nivel de transporte.
29. Averigua las direcciones de los servidores DNS que empleas en tu conexión. Localiza los datagramas enviados o recibidos por un servidor DNS. ¿En qué color aparecen en el Wireshark? ¿Qué protocolo de transporte utilizan?

Práctica 1: Wireshark (IV) : Protocolos TCP y UDP

30. Escribe la expresión para mostrar todas las tramas que salgan de tu equipo, empleen como protocolo de transporte TCP y vayan dirigidas al puerto 80 de cualquier servidor.

31. Escribe la expresión para mostrar todas las tramas que empleen UDP en el nivel de transporte y usen un puerto que no sea “bien conocido”.

Práctica 1: Wireshark (V) :
Opciones avanzadas del Wireshark

32. **Conversaciones TCP:** Captura las tramas al abrir la web de Google. Cuando acabes, haz clic sobre una de las tramas de la conexión TCP establecida y ve al menú *Analyze*, *Follow TCP stream*. Allí podrás ver la "conversación" mantenida entre cliente y servidor, señaladas con colores distintos. Los comandos que aparecen son comandos del protocolo HTTP. ¿Por qué palabra empiezan siempre las peticiones HTTP del cliente? ¿Qué forma tiene la primera línea de las respuestas HTTP del servidor? Graba toda la conversación como un fichero de texto ej32.txt. Ahora captura las tramas mientras te conectas a un servidor FTP (por ejemplo ftp.rediris.es). Navega entre las distintas carpetas. Cuando termines, selecciona alguna trama etiquetada como FTP, comprueba a qué puerto del servidor se dirige, y vuelve a la opción *Analyze*, *Follow TCP stream*. Indica el nombre de algunos comandos FTP que envía el cliente.

33. **Filtros predefinidos:** Ve al menú *Analyze*, *Display Filters*. Allí pueden verse algunos filtros con sus expresiones ya escritas, para mostrar tramas que frecuentemente suelen seleccionarse. Selecciona el filtro para capturar todas las tramas que usen el puerto 80 bien sea para TCP o UDP. Observa que la expresión se escribe automáticamente, y que algunas expresiones tienen una forma más reducida que las que hemos ido empleando. Crea un nuevo filtro llamado ej33 que permita mostrar todas las tramas que usen el puerto 21 en TCP.

34. **Edición de la coloración de las reglas**: Menú *View*, *Coloring Rules* (o el botón correspondiente de la barra de herramientas). Modifica la coloración de la regla que muestra en verde los paquetes HTTP, para que los muestre con fondo de color naranja.

35. **Guardar tramas en fichero:** Utilizando la opción *File*, *Save As*, haz que se guarden en ficheros (ej35a.pcap, ej35b.pcap, etc) las tramas que se te indican:

a. Todas las tramas de la captura.
b. Sólo los mensajes DNS de la captura.
c. Sólo la última trama de la captura.
d. Las tramas 5, 12 y 20 (usa el botón derecho sobre las tramas para marcarlas, y el menú *Edit* , *Unmark* para desmarcarlas cuando haga falta).
e. Todas las tramas comprendidas entre los segundos 1 y 2 de la captura.
f. Exporta las tramas 20 y 40 a un fichero de texto (*File*, *Export*), y en su contenido debe guardarse la información general de cada trama, sin detalles. ¿Cuánto ocupa el fichero?
g. Exporta a un fichero de texto las mismas tramas que en el ejercicio anterior, pero guardando ahora todo el contenido de las tramas. ¿Cuánto ocupa el fichero?

36. **Estadísticas:** Mirando la información que aparece en el menú *Statistics*, submenús *Summary*, *Protocol Hierarchy*, *Packet Length* e *IP Addresses* , contesta a las siguientes preguntas:

¿Cuál ha sido el tamaño medio de una trama durante la captura?
¿Qué porcentaje de paquetes han sido mensajes DNS?
¿Cuál ha sido la velocidad media durante la captura (bytes/seg)?
¿Cuántos bytes en total corresponden a segmentos TCP?
¿Qué porcentaje de paquetes fueron Ethernet?
¿Cuál ha sido la longitud de paquete más utilizada?
¿Con cuántas IP diferentes has interactuado? Quitando la tuya, ¿cuál ha sido la que más veces ha aparecido durante la captura?
¿Qué porcentaje de veces se han utilizado puertos TCP? ¿Y UDP?