Laboratorio 2.6.2: Uso de Wireshark™ para ver las unidades de datos del protocolo

Objetivos de aprendizaje

- Poder explicar el propósito de un analizador de protocolos (Wireshark).
- Poder realizar capturas básicas de la unidad de datos del protocolo (PDU) mediante el uso de Wireshark.
- Poder realizar un análisis básico de la PDU en un tráfico de datos de red simple.
- Experimentar con las características y opciones de Wireshark, como captura de PDU y visualización de filtrado.

Información básica

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para el diagnóstico de fallas de red, verificación, desarrollo de protocolo y software y educación. Antes de junio de 2006, Wireshark se conocía como Ethereal.

Un husmeador de paquetes (también conocido como un analizador de red o analizador de protocolos) es un software informático que puede interceptar y registrar tráfico de datos pasando sobre una red de datos. Mientras el flujo de datos va y viene en la red, el husmeador “captura” cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo a la RFC correcta u otras especificaciones.

Wireshark está programado para reconocer la estructura de los diferentes protocolos de red. Esto le permite mostrar la encapsulación y los campos individuales de una PDU e interpretar su significado.

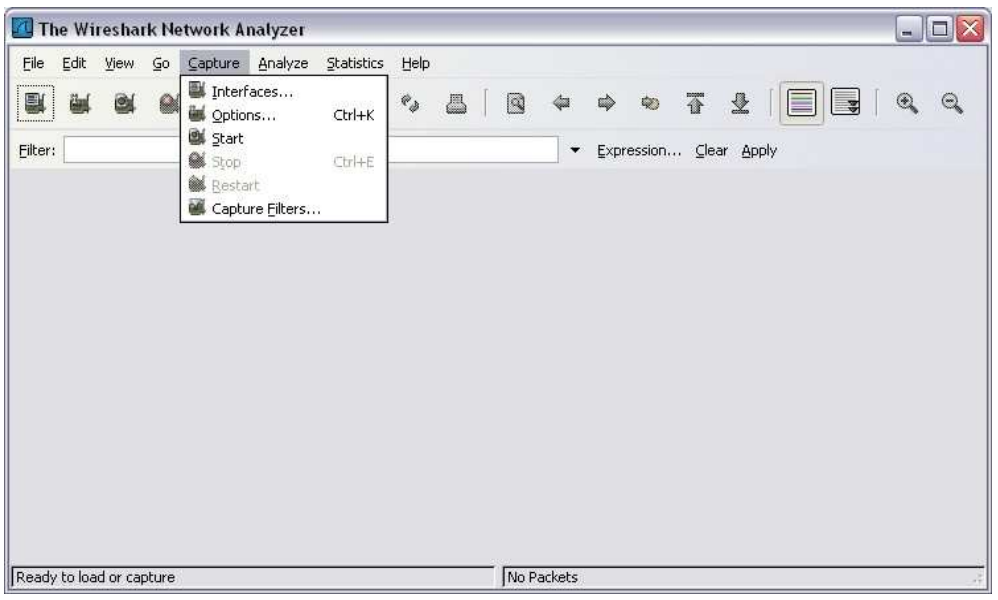
Es una herramienta útil para cualquiera que trabaje con redes y se puede utilizar en la mayoría de las prácticas de laboratorio en los cursos CCNA para el análisis de datos y el diagnóstico de fallas.

Para obtener más información y para descargar el programa visite: http://www.Wireshark.org

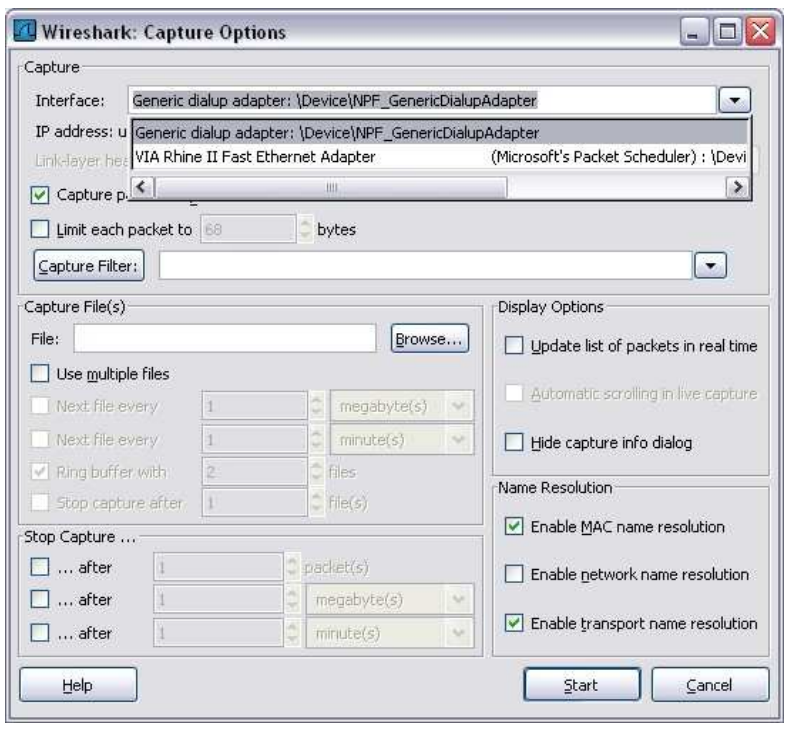
Escenario

Para capturar las PDU, la computadora donde está instalado Wireshark debe tener una conexión activa a la red y Wireshark debe estar activo antes de que se pueda capturar cualquier dato.

Cuando se inicia Wireshark, se muestra la siguiente pantalla.

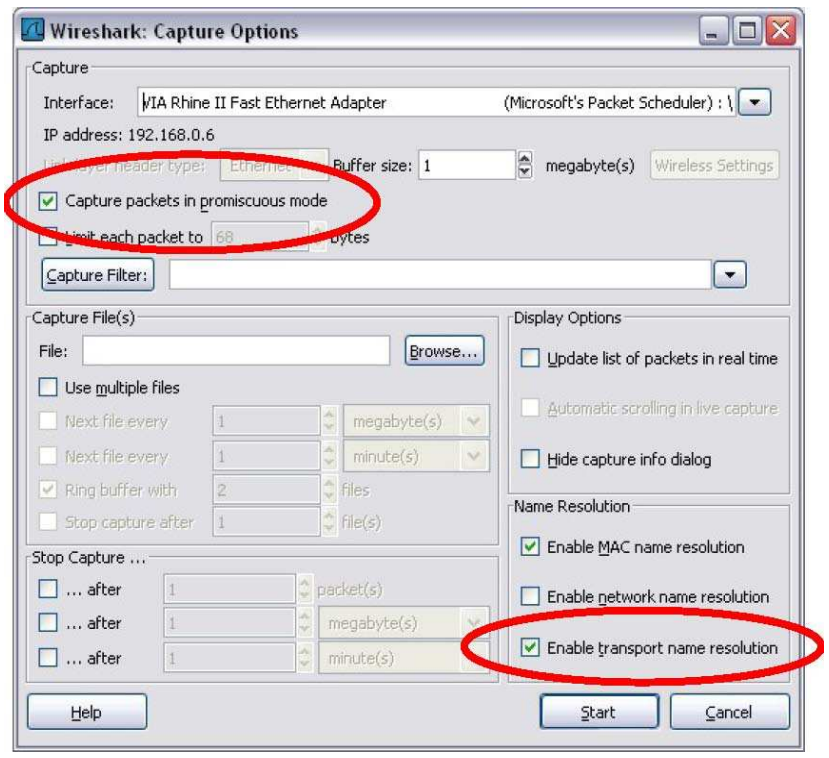


Para empezar con la captura de datos es necesario ir al menú **Capture** y seleccionar **Options**. El cuadro de diálogo **Options** provee una serie de configuraciones y filtros que determinan el tipo y la cantidad de tráfico de datos que se captura.



Primero, es necesario asegurarse de que Wireshark está configurado para monitorear la interfaz correcta. Desde la lista desplegable **Interface**, seleccione el adaptador de red que se utiliza. Generalmente, para una computadora, será el adaptador Ethernet conectado.

Luego se pueden configurar otras opciones. Entre las que están disponibles en **Capture Options,** merecen examinarse las siguientes dos opciones resaltadas.



Configurar Wireshark para capturar paquetes en un modo promiscuo.

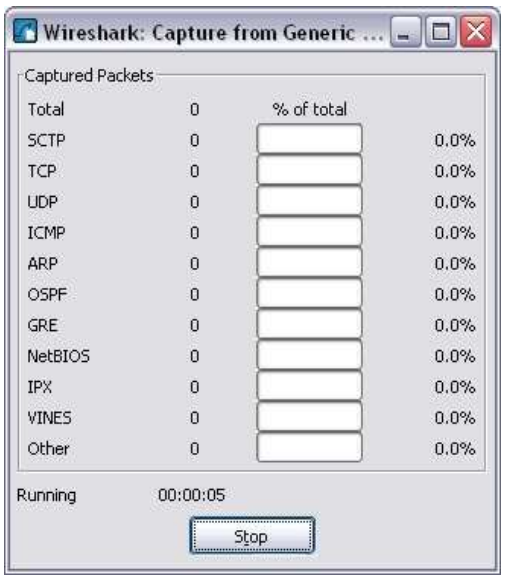
Si esta característica NO está verificada, sólo se capturarán las PDU destinadas a esta computadora. Si esta característica está verificada, se capturarán todas las PDU destinadas a esta computadora Y todas aquellas detectadas por la NIC de la computadora en el mismo segmento de red (es decir, aquellas que “pasan por” la NIC pero que no están destinadas para la computadora). Nota: La captura de las otras PDU depende del dispositivo intermediario que conecta las computadoras del dispositivo final en esta red. Si utiliza diferentes dispositivos intermediarios (hubs, switches, routers) durante estos cursos, experimentará los diferentes resultados de Wireshark.

Configurar Wireshark para la resolución del nombre de red

Esta opción le permite controlar si Wireshark traduce a nombres las direcciones de red encontradas en las PDU. A pesar de que esta es una característica útil, el proceso de resolución del nombre puede agregar más PDU a sus datos capturados, que podrían distorsionar el análisis.

También hay otras configuraciones de proceso y filtrado de captura disponibles.

Haga clic en el botón **Start** para comenzar el proceso de captura de datos y una casilla de mensajes muestra el progreso de este proceso.



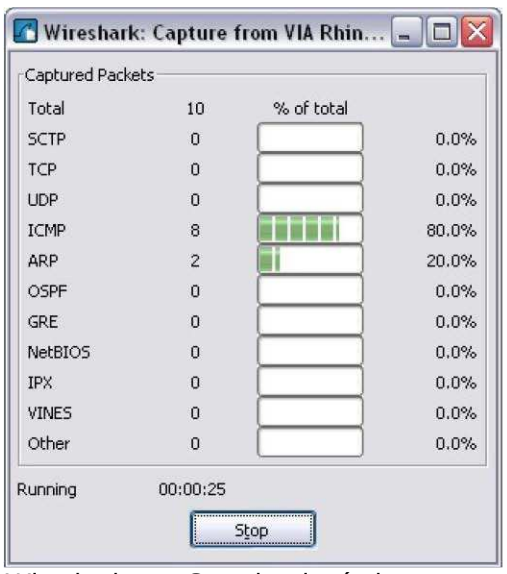
Mientras se capturan las PDU, los tipos y números se indican en la casilla de mensajes.

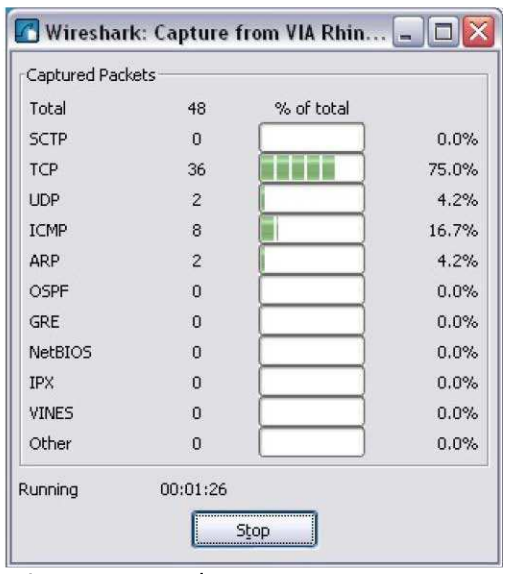
Los ejemplos de arriba muestran la captura de un proceso ping y luego el acceso a una página Web. Si hace clic en el botón **Stop**, el proceso de captura termina y se muestra la pantalla principal. La ventana de visualización principal de Wireshark tiene tres paneles.

El panel de Lista de PDU (o Paquete) ubicado en la parte superior del diagrama muestra un resumen de cada paquete capturado. Si hace clic en los paquetes de este panel, controla lo que se muestra en los otros dos paneles.
El panel de detalles de PDU (o Paquete) ubicado en el medio del diagrama, muestra más detalladamente el paquete seleccionado en el panel de Lista del paquete.

El panel de bytes de PDU (o paquete) ubicado en la parte inferior del diagrama, muestra los datos reales (en números hexadecimales que representan el binario real) del paquete seleccionado en el panel de Lista del paquete y resalta el campo seleccionado en el panel de Detalles del paquete.

Cada línea en la Lista del paquete corresponde a una PDU o paquete de los datos capturados. Si seleccionó una línea en este panel, se mostrarán más detalles en los paneles “Detalles del paquete” y “Bytes del paquete”. El ejemplo de arriba muestra las PDU capturadas cuando se utilizó la utilidad ping y cuando se accedió a





http://www.Wireshark.org. Se seleccionó el paquete número 1 en este panel.

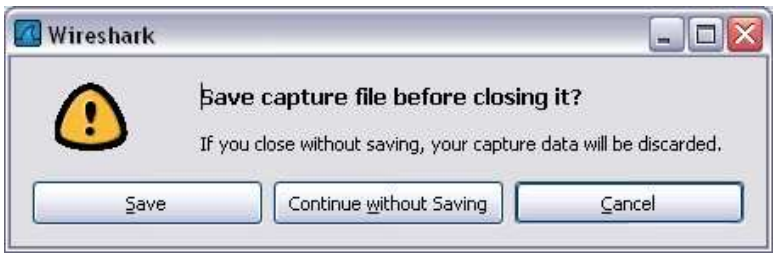
El panel Detalles del paquete muestra al paquete actual (seleccionado en el panel “Lista de paquetes”) de manera más detallada. Este panel muestra los protocolos y los campos de protocolo de los paquetes seleccionados. Los protocolos y los campos del paquete se muestran con un árbol que se puede expandir y colapsar.

El panel Bytes del paquete muestra los datos del paquete actual (seleccionado en el panel “Lista de paquetes”) en lo que se conoce como estilo “hexdump”. En esta práctica de laboratorio no se examinará en detalle este panel. Sin embargo, cuando se requiere un análisis más profundo, esta información que se muestra es útil para examinar los valores binarios y el contenido de las PDU.

La información capturada para las PDU de datos se puede guardar en un archivo. Ese archivo se puede abrir en Wireshark para un futuro análisis sin la necesidad de volver a capturar el mismo tráfico de datos. La información que se muestra cuando se abre un archivo de captura es la misma de la captura original.

Cuando se cierra una pantalla de captura de datos o se sale de Wireshark se le pide que guarde las PDU

capturadas.



Si hace clic en **Continue without Saving** se cierra el archivo o se sale de Wireshark sin guardar los datos capturados que se muestran.

Tarea 1: Captura de PDU mediante ping

Paso 1: Después de asegurarse de que la topología y configuración de laboratorio estándar son correctas, inicie Wireshark en un equipo en un módulo de laboratorio.

Configure las opciones de captura como se describe arriba en la descripción general e inicie el proceso de captura.

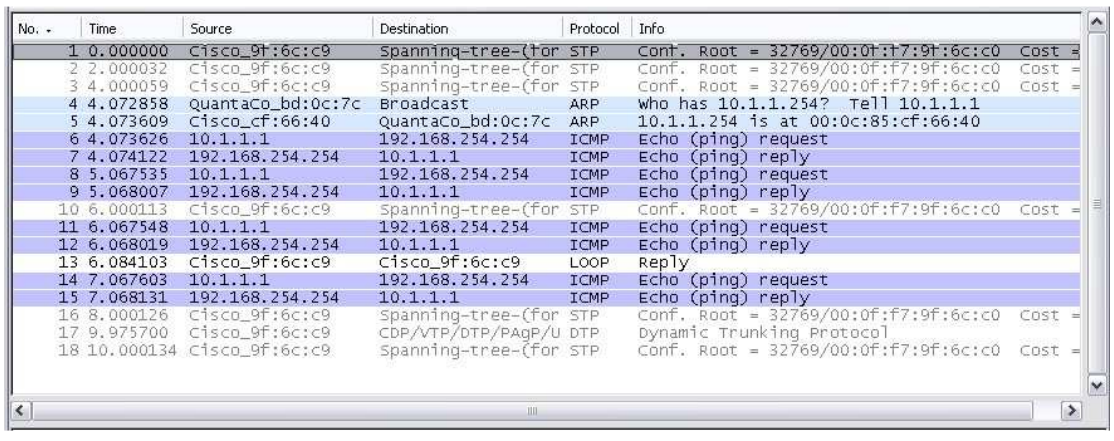
Desde la línea de comando del equipo, haga ping en la dirección IP de otra red conectada y encienda el dispositivo final en la topología de laboratorio. En este caso, haga ping en Eagle Server utilizando el comando ping **192.168.254.254**.

Después de recibir las respuestas exitosas al ping en la ventana de línea de comandos, detenga la captura del paquete.

Paso 2: Examine el panel Lista de paquetes.

El panel Lista de paquetes en Wireshark debe verse ahora parecido a éste:

Observe los paquetes de la lista de arriba. Nos interesan los números de paquetes 6, 7, 8, 9, 11, 12, 14 y 15. Localice los paquetes equivalentes en la lista de paquetes de su equipo.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	Who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Si el usuario realizó el Paso 1 A de arriba, haga coincidir los mensajes que se muestran en la ventana de línea de comandos cuando el ping se ejecutó con los seis paquetes capturados por Wireshark. Responda lo siguiente desde la lista de paquetes Wireshark:

¿Qué protocolo se utiliza por ping? **ICMP**

¿Cuál es el nombre completo del protocolo? **Internet Control Messages Protocol**

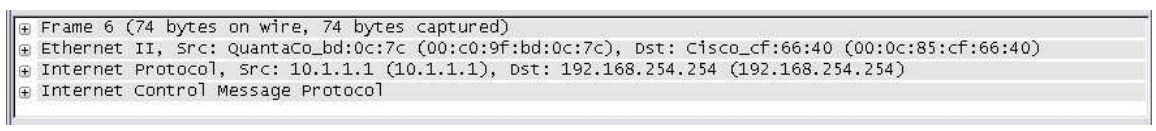
¿Cuáles son los nombres de los dos mensajes ping? **El de envio es: Echo (ping) request, y el de respuesta es: Echo (ping) reply**

¿Las direcciones IP de origen y destino que se encuentran en la lista son las que esperaba? **Sí** / No

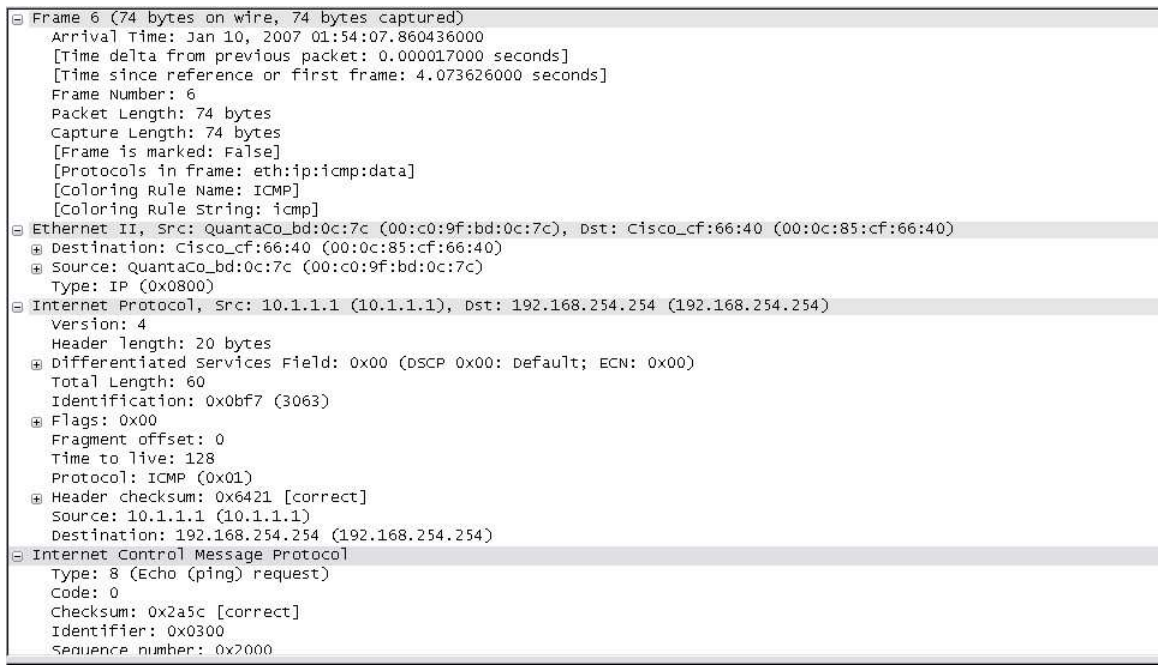
¿Por qué? **Porque en los mensajes de petición aparece la ip de mi equipo como origen y como destino la dirección a la que hice el ping, y en los mensajes de respuesta la inversa.**

Paso 3: Seleccione (resalte) con el mouse el primer paquete de solicitud de eco en la lista.

El panel de Detalles del paquete mostrará ahora algo parecido a:



Haga clic en cada uno de los cuatro "**+**" para expandir la información. El panel de Detalles del paquete será ahora algo parecido a:



Como puede ver, los detalles de cada sección y protocolo se pueden expandir más. Tómese el tiempo para leer esta información. En esta etapa del curso, puede ser que no entienda completamente la información que se muestra, pero tome nota de la que sí reconozca.

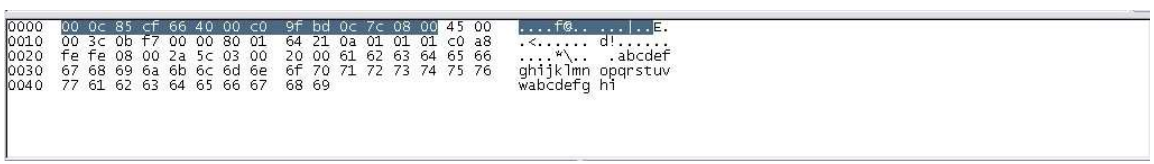
Localice los dos tipos diferentes de "Origen" y "Destino". ¿Por qué hay dos tipos?
Nos lo indica por mac adress, y por IP, por que las mac corresponden a la capa de red y la IP a la capa de internet.

¿Cuáles son los protocolos que están en la trama de Ethernet?
Ethernet II

Si selecciona una línea en el panel de Detalles del paquete, toda o parte de la información en el panel de Bytes del paquete también quedará resaltada.

Por ejemplo, si la segunda línea (+ Ethernet II) está resaltada en el panel de detalles, el panel de Bytes resalta ahora los valores correspondientes.

Esto muestra los valores binarios particulares que representan la información de la PDU. En esta etapa del curso no es necesario entender esta información en detalle.



Paso 4: Vaya al menú Archivo y seleccione Cerrar. Haga clic en **Continue without Saving** cuando se muestre esta casilla de mensaje.

Tarea 2: Captura de FTP PDU

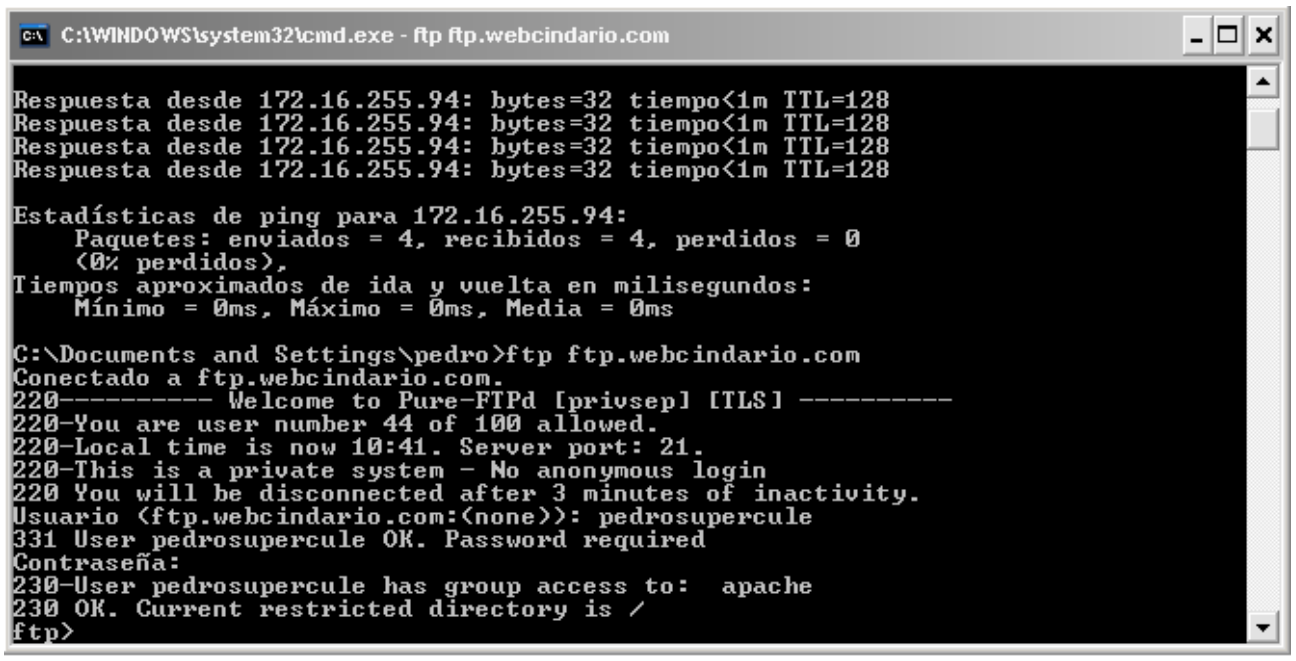
Paso 1: Inicie la captura de paquetes.

Considerando que Wireshark sigue en funcionamiento desde los pasos anteriores, inicie la captura de paquetes haciendo clic en la opción **Iniciar** en el menú **Capture** de Wireshark.

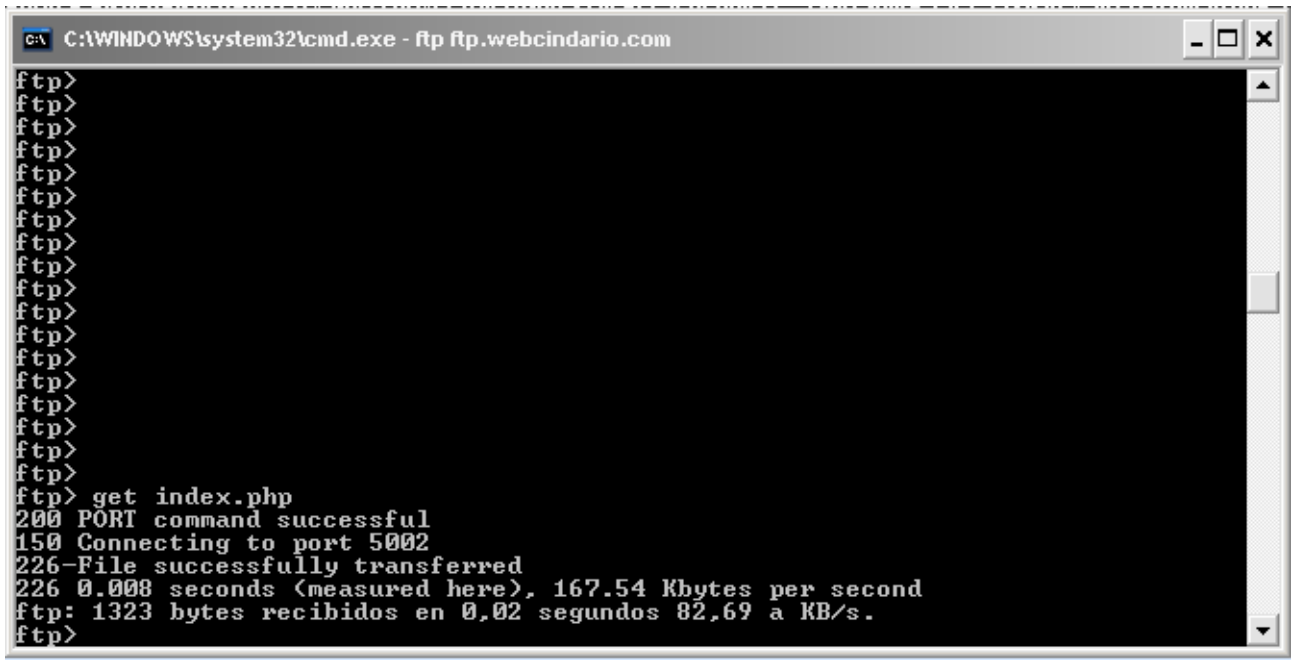
~~**“** Ingrese **ftp 192.168.254.254** en la línea de comandos del equipo donde se ejecuta Wireshark.~~

~~Cuando se establezca la conexión, ingrese **anonymous** como usuario, sin ninguna contraseña. ID del usuario: **anonymous** Password: <INTRO> También se puede iniciar sesión con id de usuario **cisco** y contraseña **cisco.”**~~

Nota importante: Dado que el servidor que nos indican en la práctica no está operativo, en mi caso he realizado este proceso conectando al servidor ftp de mi hosting **ftp.webcindario.com,** con mi usuario **pedrosupercule** y mi contraseña **********.**



Una vez que inició sesión con éxito, ingrese **get `index.php`** y presione la tecla ingresar <INTRO>. Con esa operación comenzará la descarga del archivo desde el servidor ftp. El resultado será similar a:



Una vez que la descarga del archivo se haya completado, ingrese **quit**

```
ftp> quit
```

Una vez que los archivos se hayan descargado exitosamente, detenga la captura PDU en Wireshark.

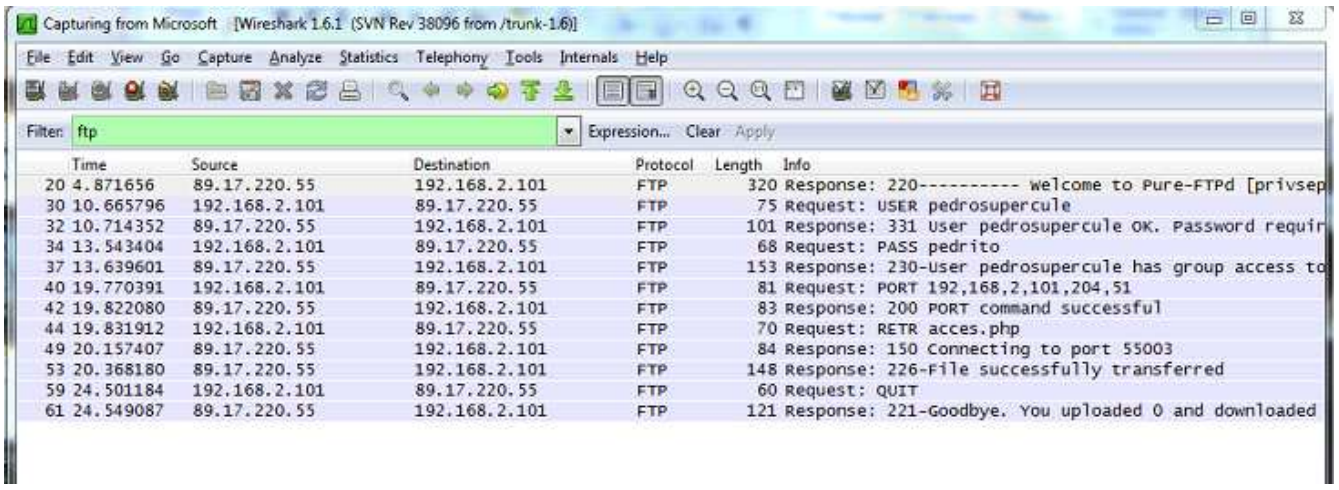
Paso 2: Aumente el tamaño del panel de Lista de paquetes de Wireshark y desplácese por las PDU que se encuentren en la lista.

Localice y tome nota de las PDU asociadas con la descarga del archivo. Éstas serán las PDU del protocolo TCP de Capa 4 y del protocolo FTP de Capa 7.

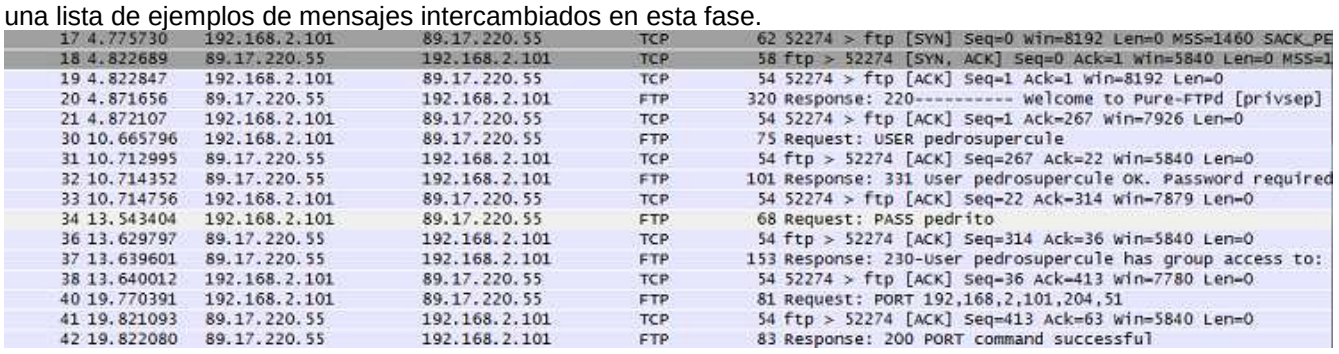
17	4.775730	192.168.2.101	89.17.220.55	TCP	62 52274 > ftp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PE
18	4.822689	89.17.220.55	192.168.2.101	TCP	58 ftp > 52274 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1
19	4.822847	192.168.2.101	89.17.220.55	TCP	54 52274 > ftp [ACK] Seq=1 Ack=1 Win=8192 Len=0
20	4.871656	89.17.220.55	192.168.2.101	FTP	320 Response: 220---------- Welcome to Pure-FTPd [privsep]
21	4.872107	192.168.2.101	89.17.220.55	TCP	54 52274 > ftp [ACK] Seq=1 Ack=267 Win=7926 Len=0
30	10.665796	192.168.2.101	89.17.220.55	FTP	75 Request: USER pedrosupercule
31	10.712995	89.17.220.55	192.168.2.101	TCP	54 ftp > 52274 [ACK] Seq=267 Ack=22 Win=5840 Len=0
32	10.714352	89.17.220.55	192.168.2.101	FTP	101 Response: 331 User pedrosupercule OK. Password required
33	10.714756	192.168.2.101	89.17.220.55	TCP	54 52274 > ftp [ACK] Seq=22 Ack=314 Win=7879 Len=0
34	13.543404	192.168.2.101	89.17.220.55	FTP	68 Request: PASS pedrito
36	13.629797	89.17.220.55	192.168.2.101	TCP	54 ftp > 52274 [ACK] Seq=314 Ack=36 Win=5840 Len=0
37	13.639601	89.17.220.55	192.168.2.101	FTP	153 Response: 230-User pedrosupercule has group access to:
38	13.640012	192.168.2.101	89.17.220.55	TCP	54 52274 > ftp [ACK] Seq=36 Ack=413 Win=7780 Len=0
40	19.770391	192.168.2.101	89.17.220.55	FTP	81 Request: PORT 192,168,2,101,204,51
41	19.821093	89.17.220.55	192.168.2.101	TCP	54 ftp > 52274 [ACK] Seq=413 Ack=63 Win=5840 Len=0
42	19.822080	89.17.220.55	192.168.2.101	FTP	83 Response: 200 PORT command successful
43	19.822477	192.168.2.101	89.17.220.55	TCP	54 52274 > ftp [ACK] Seq=63 Ack=442 Win=7751 Len=0
44	19.831912	192.168.2.101	89.17.220.55	FTP	70 Request: RETR acces.php
45	19.916225	89.17.220.55	192.168.2.101	TCP	54 ftp > 52274 [ACK] Seq=442 Ack=79 Win=5840 Len=0
49	20.157407	89.17.220.55	192.168.2.101	FTP	84 Response: 150 Connecting to port 55003
50	20.157815	192.168.2.101	89.17.220.55	TCP	54 52274 > ftp [ACK] Seq=79 Ack=472 Win=7721 Len=0
53	20.368180	89.17.220.55	192.168.2.101	FTP	148 Response: 226-File successfully transferred
54	20.368500	192.168.2.101	89.17.220.55	TCP	54 52274 > ftp [ACK] Seq=79 Ack=566 Win=7627 Len=0
59	24.501184	192.168.2.101	89.17.220.55	FTP	60 Request: QUIT
60	24.548243	89.17.220.55	192.168.2.101	TCP	54 ftp > 52274 [ACK] Seq=566 Ack=85 Win=5840 Len=0
61	24.549087	89.17.220.55	192.168.2.101	FTP	121 Response: 221-Goodbye. You uploaded 0 and downloaded 2
62	24.549492	192.168.2.101	89.17.220.55	TCP	54 52274 > ftp [ACK] Seq=85 Ack=633 Win=7560 Len=0
63	24.549681	89.17.220.55	192.168.2.101	TCP	54 ftp > 52274 [FIN, ACK] Seq=633 Ack=85 Win=5840 Len=0
64	24.549757	192.168.2.101	89.17.220.55	TCP	54 52274 > ftp [ACK] Seq=85 Ack=634 Win=7560 Len=0
65	24.565116	192.168.2.101	89.17.220.55	TCP	54 52274 > ftp [FIN, ACK] Seq=85 Ack=634 Win=7560 Len=0
66	24.612210	89.17.220.55	192.168.2.101	TCP	54 ftp > 52274 [RST] Seq=634 Win=0 Len=0

Identifique los tres grupos de PDU asociados con la transferencia del archivo.

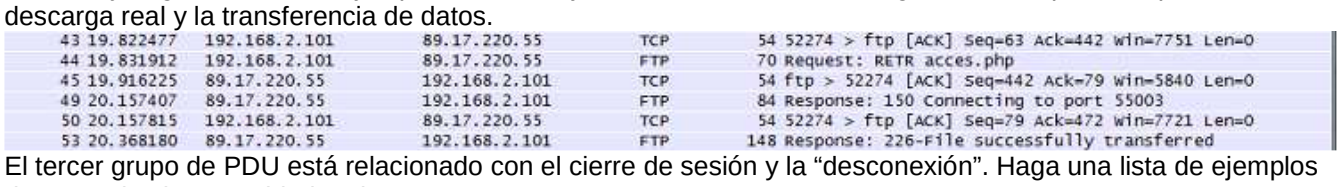
Si realizó el paso de arriba, haga coincidir los paquetes con los mensajes y las indicaciones en la ventana de línea de comandos FTP.



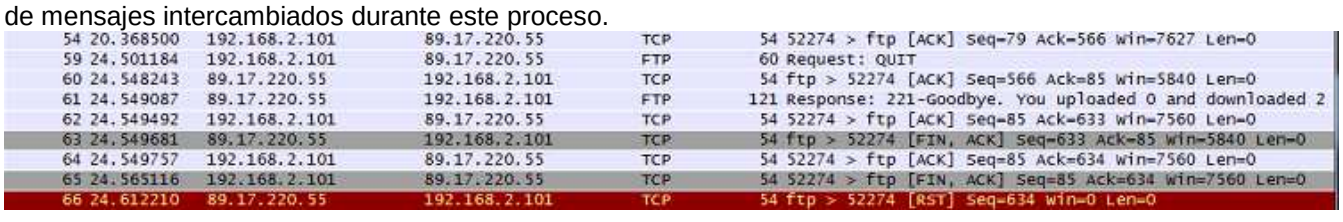
El primer grupo está asociado con la fase “conexión” y el inicio de sesión en el servidor. Haga una lista de ejemplos de mensajes intercambiados en esta fase.



Localice y haga una lista de ejemplos de mensajes intercambiados en la segunda fase, que es el pedido de descarga real y la transferencia de datos.



El tercer grupo de PDU está relacionado con el cierre de sesión y la “desconexión”. Haga una lista de ejemplos de mensajes intercambiados durante este proceso.



Localice los intercambios TCP recurrentes a través del proceso FTP. ¿Qué característica de TCP indica esto?

Establece una conexión con el servidor ftp sincronizando nuestro puerto 52274 con el 21 del servidor para utilizar durante la conexión

Paso 3: Examine los Detalles del paquete.

Seleccione (resalte) un paquete de la lista asociada con la primera fase del proceso FTP.
Observe los detalles del paquete en el panel de Detalles.

¿Cuáles son los protocolos encapsulados en la trama?

Protocols in frame: eth:ip:tcp

Resalte los paquetes que contengan el nombre de usuario y contraseña.
Examine la porción resaltada en el panel Byte del paquete.

Aparece claramente en texto el nombre de ususario y su contraseña

¿Qué dice esto sobre la seguridad de este proceso de inicio de sesión FTP?

Que durante la fase de conexión no se encriptan los datos de usuario y password y en cuanto a seguridad si alguien está realizando un sniffer de la red podrá ver nuestros datos con el problema que ello conlleva.

Resalte un paquete asociado con la segunda fase. Desde cualquier panel, localice el paquete que contenga el nombre del archivo.

El nombre del archivo es:**index.php**

Resalte un paquete que contenga el contenido real del archivo. Observe el texto simple visible en el panel Byte.

Se aprecia RETR index.php (solicitamos el archivo index.php)

Resalte y examine en los paneles Detalles y Byte; algunos de los paquetes intercambiados en la tercera fase de la descarga del archivo. ¿Qué características distinguen al contenido de estos paquetes?

Indica que cerramos la conexión (logout), y se aprecia los bytes que hemos subido y bajado al servidor.

Cuando termine, cierre el archivo Wireshark y continúe sin guardar.

Tarea 3: Captura de HTTP PDU

Paso 1: Inicie la captura de paquetes.

Considerando que Wireshark sigue en funcionamiento desde los pasos anteriores, inicie la captura de paquetes haciendo clic en la opción **Iniciar** en el menú **Captura** de Wireshark.

Nota: Si se continúa desde pasos anteriores de esta práctica de laboratorio, no es necesario configurar las opciones de captura.

“Inicie un navegador Web en el equipo donde ejecuta Wireshark. Ingrese el URL de Eagle Server **example.com** o ingrese la dirección IP-192.168.254.254. Una vez que la página Web se haya descargado por completo, detenga la captura del paquete Wireshark.”

NOTA: En mi caso conecto a **jovellanos.esp.st**

Paso 2: Aumente el tamaño del panel de Packet List de Wireshark y desplácese por las PDU que se encuentren en la lista.

Localice e identifique los paquetes TCP y HTTP asociados con la descarga de la página Web.

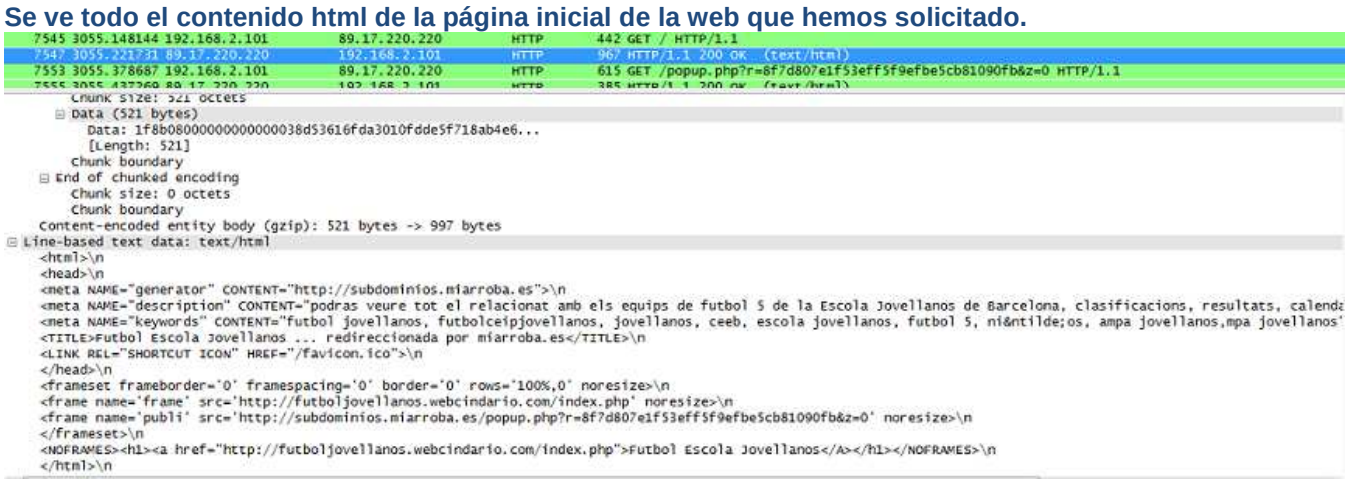
Observe el parecido entre este intercambio de mensajes y el intercambio FTP.

Establece una conexión con el servidor ftp sincronizando nuestro puerto 51911 con el 80 del servidor para utilizar durante la conexión, y se van solicitando las paginas html y las imágenes de la pagina secuencialmente.

Paso 3: En el panel Packet List, resalte un paquete HTTP que tenga la notación “(text/html)” en la columna Información.

En el panel Detalles del paquete, haga clic en “+” al lado de “**Line-based text data: html**” ¿Cuándo esta información expande lo que se muestra?

Se ve todo el contenido html de la página inicial de la web que hemos solicitado.



Examine la porción que resaltó en el panel Byte. Esto muestra los datos HTML que contiene el paquete.

Cuando termine, cierre el archivo Wireshark y continúe sin guardar.

Tarea 4: Reflexión

Considere lo que puede proveer Wireshark sobre la información de encapsulación referida a los datos de red capturados. Relacione esto a los modelos de la capa OSI y TCP/IP. Es importante que el usuario pueda reconocer y relacionar tanto los protocolos representados como la capa de protocolo y los tipos de encapsulación de los modelos con la información provista por Wireshark.

Como hemos visto con Wireshark, seleccionando un UDP podemos ver parte de su estructura de capas OSI, ya que en los detalles en la etiqueta frame están los datos relacionados con la capa de “enlace de datos” del modelo OSI, en la etiqueta Ethernet II será lo referido a la capa de “Red” del modelo OSI (i las dos anteriores se corresponden a la capa de RED del modelo TCP/IP), en la etiqueta de Internet protocol va todo lo referido a la capa de “Internet”, de ambos modelos, en la etiqueta Transimission Transfer Protocol lo referido a la capa de “Transporte”, de ambos modelos, y en la capa de Hypertext Transfer Protocol va lo referido a las capas OSI de “Aplicación, presentación y sesión” que se corresponden a la capa “Aplicación” del modelo TCP/IP

Tarea 5: Desafío

Analice cómo podría utilizar un analizador de protocolos como Wireshark para:

(1) diagnosticar fallas de una página Web para descargar con éxito un navegador de un equipo

(2) identificar el tráfico de datos en una red requerida por los usuarios.

(1) Como podemos ver en los detalles de una conexión utilizando el portocolo HTTP, se puede apreciar si el contenido html es el mismo accediendo desde diferentes navegadores, en caso de que apreciemos que dicho código es diferente en alguna de las peticiones de pagina web realizada por uno de los navegadores podremos detectar con cual realizar la solicitud de pagina en concreto, para saber a que navegador corresponde la petición lo podemos ver en los detalles contenidos en la etiqueta Hypertext Transfer Protocol->GET viendo el contenido de User-Agent (nos indica el navegador y el sistema operativo que realiza la petición).

Comentar, que si nosotros fueramos un servidor Web, podríamos ver que tipo de clientes nos solicitan paginas (sabríamos sus User Agent), también podríamos ver si se nos hacen peticiones a la web desde un user agent que no sea un navegador para protegerla de ataques masivos o robo de datos, etc.

(2) Teniendo en cuenta que disponemos de la IP asignada a dicho usuario, podemos controlar todas las líneas UDP en las que sea como origen o como destino aparezca dicha IP, para ver las conexiones que esta realizando con otras IP, y ver que acciones se están realizando, por ejemplo podemos ver si se le esta realizando una intrusión externa, si esta realizando tareas no consentidas (por ejemplo hay empresas que no dejan realizar descargas de archivos a sus empleados), podríamos ver que archivos esta descargando via ftp y desde donde, etc.

Tarea 6: Limpieza

A menos que el instructor le indique lo contrario, salga de Wireshark y apague el equipo correctamente.