Tema: MODELO OSI

Profesor: M. EN T. I. Mónica García Munguía

Periodo: Enero – Junio 2015

Programa Académico Lic. En Sistemas Computacionales

Material Didáctico 2015

Tema: Modelo OSI

Abstract One of the first theoretical issues that tend to be at the beginning of the courses of networks is the model with which have been structured in a data network transmissions, and describing the various layers that make up the network and the function they perform this model is known as the OSI model

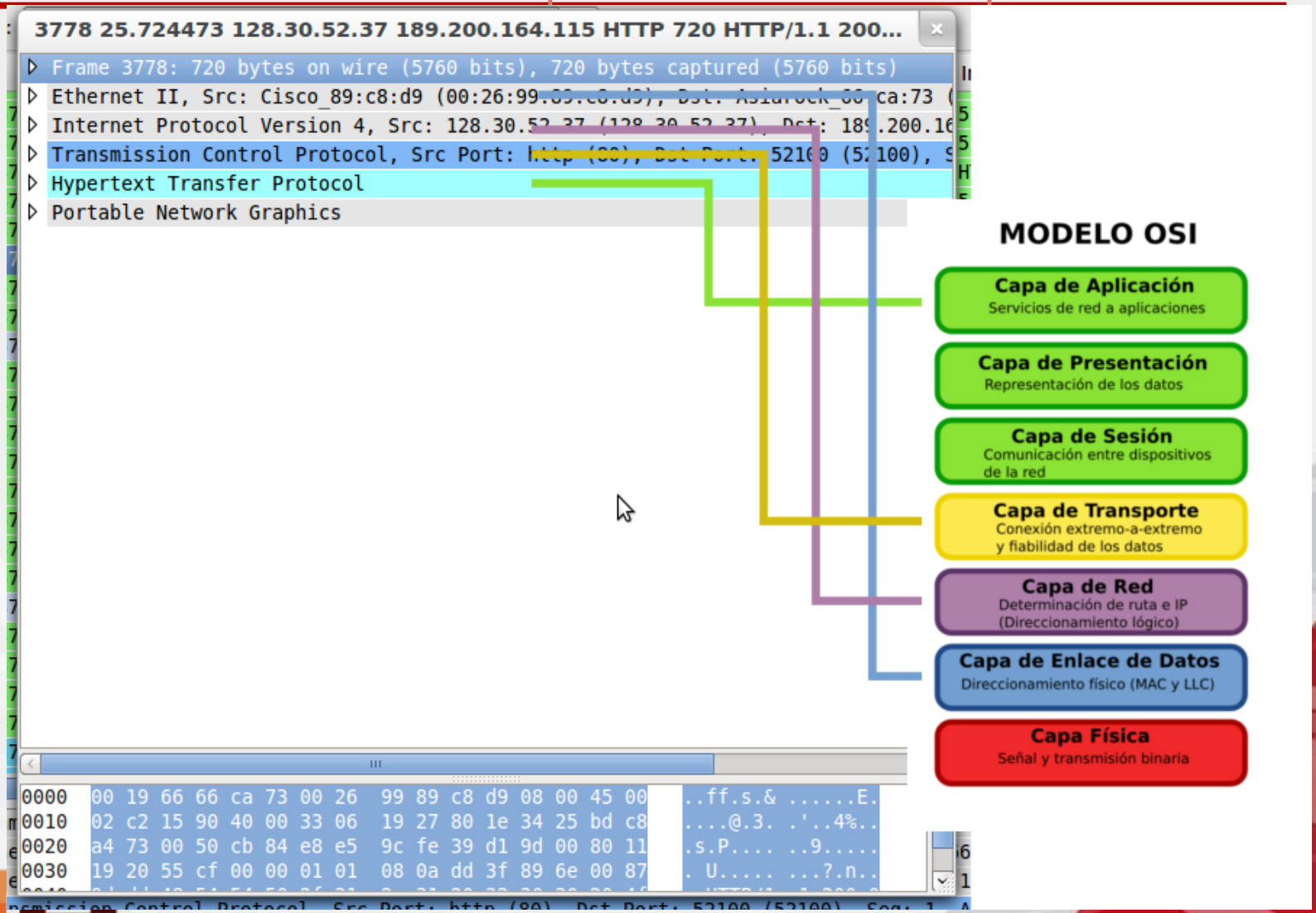
Keywords: **OSI, Network, Capas**


Nivel de Aplicación
Servicios de red a aplicaciones
Nivel de Presentación
Representación de los datos
Nivel de Sesión
Comunicación entre dispositivos de la red
Nivel de Transporte
Conexión extremo-a-extremo y fiabilidad de los datos
Nivel de Red
Determinación de ruta e IP (Direccionamiento lógico)
Nivel de Enlace de Datos
Direccionamiento físico (MAC y LLC)
Nivel Físico
Señal y transmisión binaria

existen herramientas que permiten examinar a detalle lo que ocurre dentro de una red, de modo que se puede ver no solo los datos que se deseaban emitir, si no también los datos y parámetros usados y generados por cada etapa de la transmisión, es al examinar estos que las razones de la estructura del modelo OSI quedan claras. Una de estas herramientas es el analizador de paquetes de red.

Una muestra de esto puede verse en la figura, en la cual se capturo un paquete de una transferencia HTTP y las diferentes secciones mostradas en Wireshark se conectaron con su capa correspondiente del modelo OSI.

Wireshark si muestra algo que podría corresponderse con la capa física, esto no es del todo correcto, puesto que la capa física no se indica por las tramas emitidas, si no por frecuencias y voltajes eléctricos y es mas fácil de visualizar con un osciloscopio


3778 25.724473 128.30.52.37 189.200.164.115 HTTP 720 HTTP/1.1 200...
Frame 3778: 720 bytes on wire (5760 bits), 720 bytes captured (5760 bits)
Ethernet II, Src: Cisco_89:c8:d9
Internet Protocol Version 4, Src: 128.30.52.37
Transmission Control Protocol, Src Port:
Hypertext Transfer Protocol
Portable Network Graphics
0000 00 19 66 66 ca 73 00 26 99 89 c8 d9 08 00 45 00
0010 02 c2 15 90 40 00 33 06 19 27 80 1e 34 25 bd c8
0020 a4 73 00 50 cb 84 e8 e5 9c fe 39 d1 9d 00 80 11
0030 19 20 55 cf 00 00 01 01 08 0a dd 3f 89 6e 00 87
MODELO OSI
Capa de Aplicación
Servicios de red a aplicaciones
Capa de Presentación
Representación de los datos
Capa de Sesión
Comunicación entre dispositivos de la red
Capa de Transporte
Conexión extremo-a-extremo y fiabilidad de los datos
Capa de Red
Determinación de ruta e IP (Direccionamiento lógico)
Capa de Enlace de Datos
Direccionamiento físico (MAC y LLC)
Capa Física
Señal y transmisión binaria

Ethernet - Capa de enlace de datos: La función de Ethernet es proporcionar los mecanismos para el direccionamiento *físico* manejando a nivel tarjeta de red a donde deben de enviarse los paquetes.
Internet Protocol - Capa de red: Maneja como se direcionan los paquetes a nivel software, permitiendo cambiar el hardware sin modificar el sistema en si.
Transfer Control Protocol - Capa de Transporte: Permite las transferencias orientadas a conexión y la fiabilidad del sistema.
Capa de aplicación - HTTP: En esta capa están los protocolos que ya cumplen una función y envían datos que son usados o solicitados por aplicaciones.

ANÁLISIS DE RED CON WIRESHARK

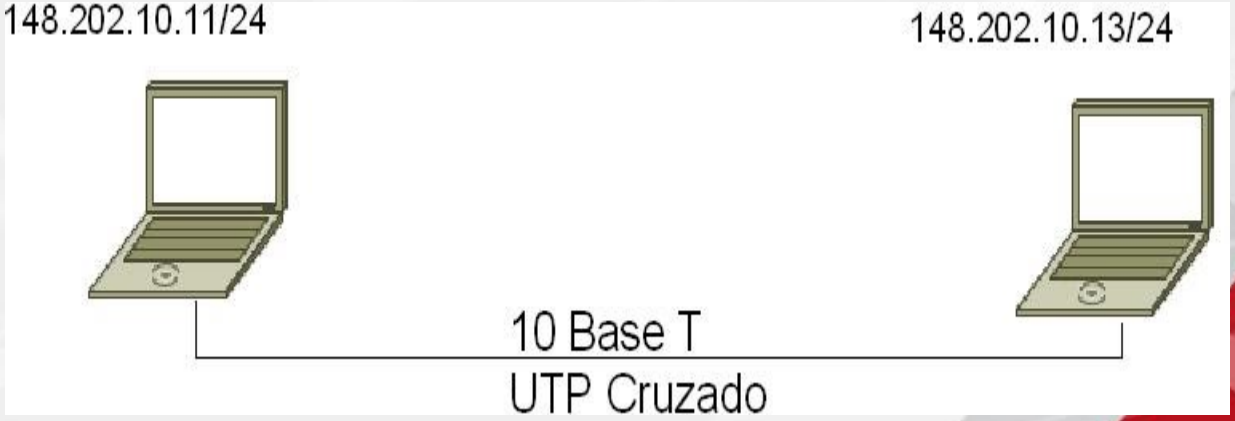
MATERIAL:

2 computadoras con Wireshark, Apache y Navegador de Internet instalados.

1 cable UTP para Ethernet cruzado.

DESARROLLO:

1. conectamos las dos computadoras entre sí con el cable UTP para Ethernet cruzado como se muestra en la siguiente figura:



2. Luego configuramos nuestra IP de la computadora, “Dirección IP” escribimos en una de las computadora 148.202.10.11 y en la otra computadora en el mismo campo escribimos 148.202.10.13 y en el campo donde dice “Máscara de subred” escribimos en ambas computadoras 255.255.255.0, todos los demás campos dejarlos en blanco, aceptar y cerrar las Conexiones de red.

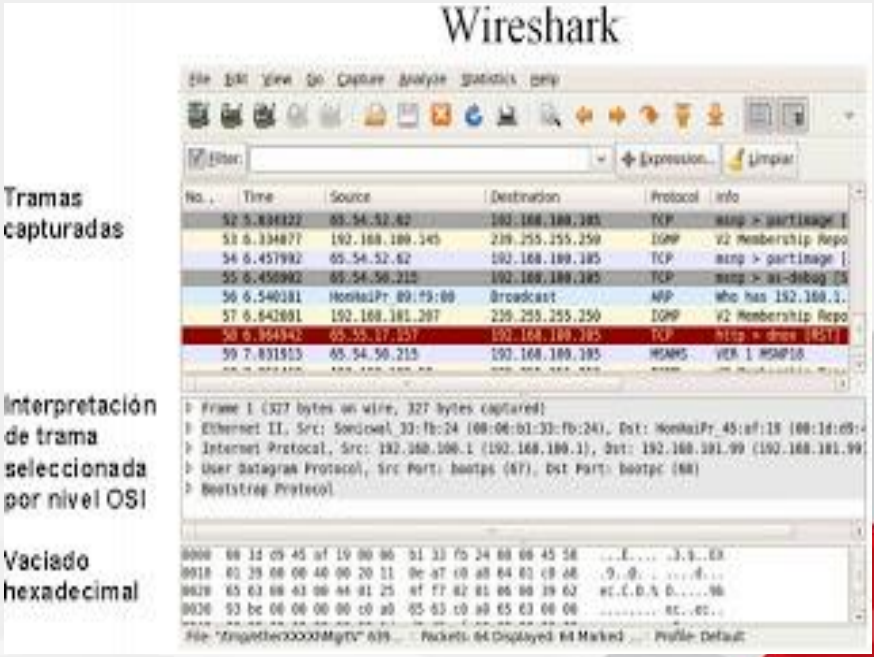
3. Desactivar en ambas computadoras todo software p2p o cualquiera que acceda a Internet de forma automática (ejemplos: MSN. Ares, limewire, skype, etc...).

Desactivar todos los firewall que estén corriendo en los equipos, incluyendo los que se encuentran en los programas antivirus como parte de su funcionalidad.

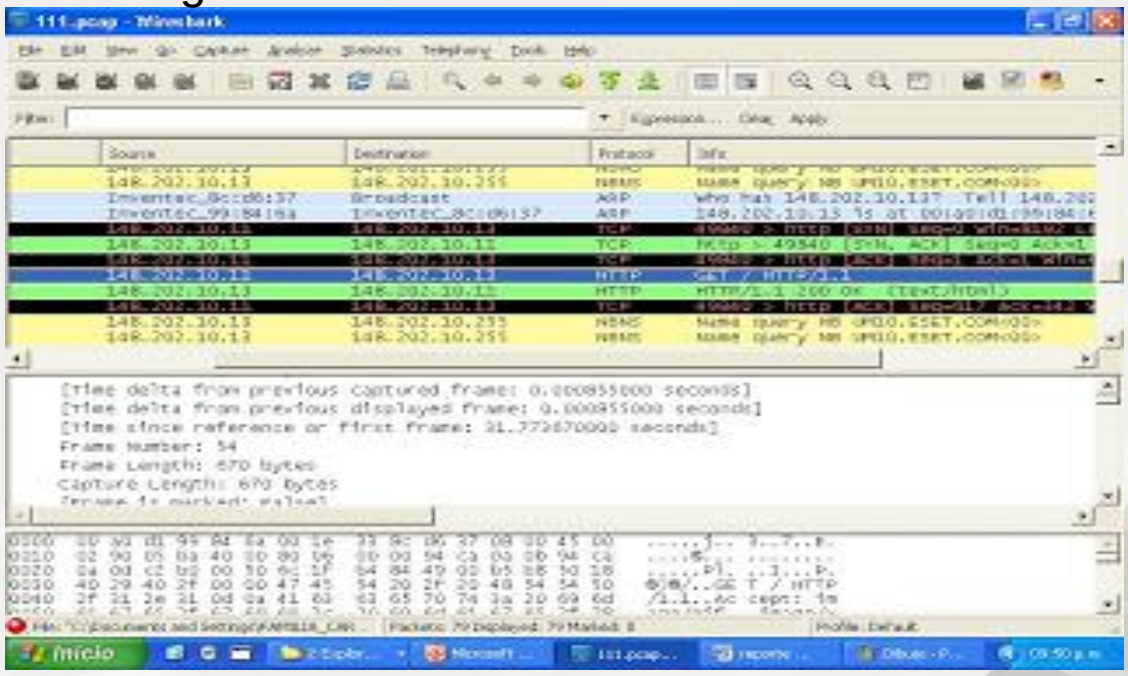
5. Desactivar otras conexiones de red inalámbricas como WiFi, 3G, etc...

6. Realizar pings de una computadora a otra para verificar que el tráfico de los paquetes es exitoso

Abrimos Wireshark y elegimos interfaz Ethernet cableada. Posteriormente iniciamos la captura de la sesión http.



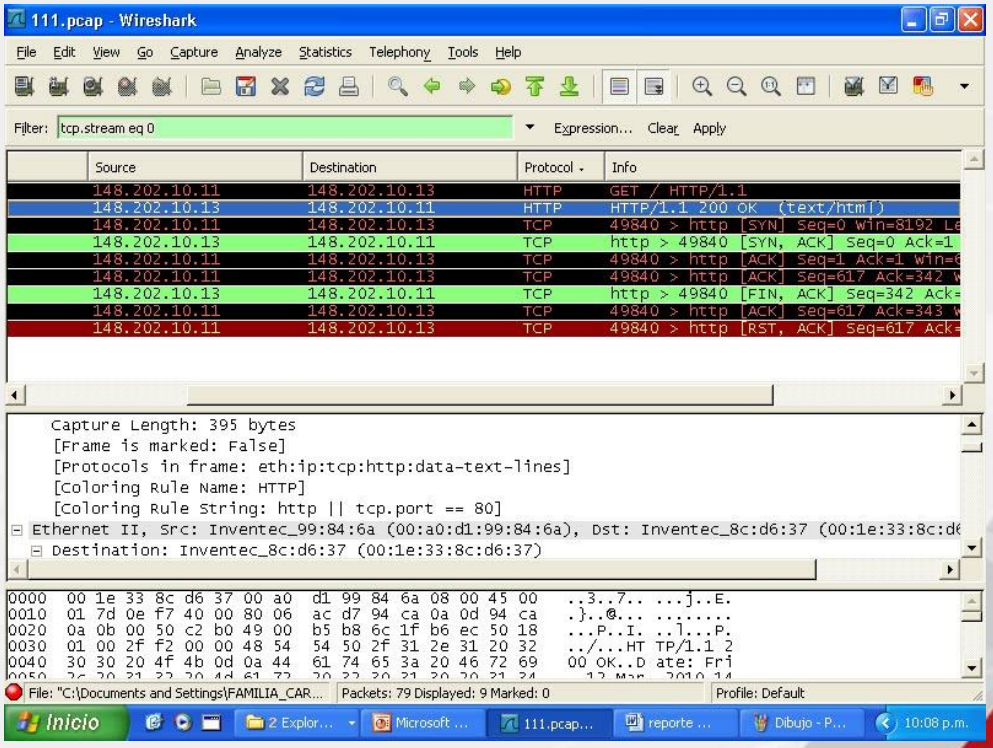
La sesión que capturada inmediatamente después de hacer los pings fue la siguiente:



La sesión que capturamos tal como está contiene paquetes como imágenes y otros elementos que mandamos de un equipo a otro, si mandamos mucho contenido de este tipo nuestra sesión se ve muy contaminada de elementos, los cuales pueden ser de tipo ACK (color gris en la imagen), NBNS (color amarillo), TCP y HTTP que son las que nos interesan aparecen en negro y verde respectivamente.

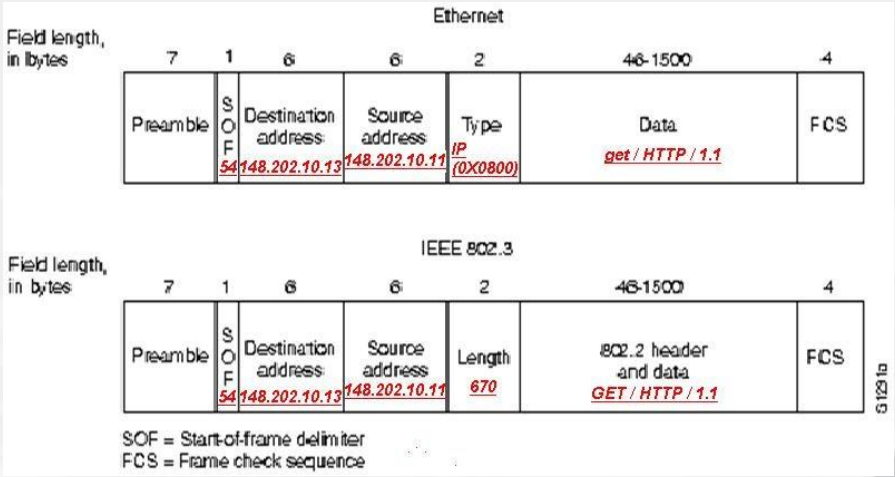
Para limpiar nuestra sesión de estos elementos y quedarnos solo con la información de TCP y HTTP hacemos lo siguiente:

De las tramas capturadas elegimos la primera de Protocolo TCP y le damos clic derecho -> elegimos “Follow TCP stream” y veremos como nos quedamos únicamente con las tramas de Protocolo TCP y HTTP que son las que nos interesan, la sesión ya filtrada luce así:



En una tabla registra la información que obtuvimos de nuestra sesión para la trama de Ethernet tal y como esta conformado el paquete.

Ejemplo



Elabora la tabla que describea el encabezado IP de un paquete e incluye los datos de cada campo respecto a la captura

Ejemplo

Formato de encabezado IPv4

Bits 0 – 3	4 – 7	9 – 15	16 – 31
Versión: *4*	Header length: *20 bytes*	Type of service: *0X00*	Total length: *656*
Identification: *0X05ba (1466)*		Flags: *0X02*	Fragment offset: *0*
Time to live: *128*	Protocol: *TCP (0X06)*		Header checksum: *0X0000*
32–bit source address: *10010100.11001010.00001010.00001011 (148.202.10.11)*			
32–bit destinatio address: *10010100.11001010.00001010.00001101 (148.202.10.13)*			
Options			Padding

Elabora la tabla que describa el encabezado de TCP del mismo paquete e incluye los datos de cada campo respecto a la captura
Ejemplo

TCP Header

Source Port (16) 49840			Destination Port (16) 80
Sequence Number (32) 1			
Acknowledgement Number (32) 1			
Data offset	Reserved (6)	Flags (6) 0X18	Window (16) 65700
Checksum (16) 0X402f			Urgent (16)
Options and Padding			
Data (Varies)			

Elabora tus conclusiones y coméntalas en clase con tus compañeros y el maestro

Bibliografía

Merino, B. (2011). *ANÁLISIS DE TRÁFICO CON.* España: INTECO-CERT.