

Escuela Superior de Tlahuelilpan

Área Académica de Ingenierías

**Tema: MODELO OSI** 

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

Periodo: Enero – Junio 2015

Material Didactico 2015 Programa Académico Lic. En Sistemas Computacionales





Escuela Superior de Tlahuelilpan

Área Académica de Ingenierías

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







### Escuela Superior de Tlahuelilpan

### Área Académica de Ingenierías

#### 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 (Direccio namiento lógico)

#### Nivel de Enlace de Datos Direccionamiento físico (MAC y LLC)

Nivel Físico Señal y transmisión binaria









Área Académica de Ingenierías

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.









Área Académica de Ingenierías

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





### Escuela Superior de Tlahuelilpan







Área Académica de Ingenierías

#### 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.







Área Académica de Ingenierías

### 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:







### Escuela Superior de Tlahuelilpan

#### Área Académica de Ingenierías

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...).







### Escuela Superior de Tlahuelilpan

#### Área Académica de Ingenierías

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.

		V	nesnark		
	the this year	Do Capture Analyze 3	patients perio		
	截氧聚(		6 😫 🛝 🐖 🖷	9 F	+
	Witter:		1.	+ Expression	- d simplar
Tramas	No., Time	Source	Destination	Protocol	into +
capturadas	\$2.5.83482 53.6.33487	2 65.54.52.42	103.108.109.305 219.155.155.259	109	stop > particage [ y2 Membership Repo
	54 6.45798	2 65.54.52.62	192.168.199.185	TCP	manp > partimage [
	50.6.54018	1 HonikaiPr 89175:00	Broedcast	MP	who has 152,368.1.
	50 6.35434	65.55.17.157	192.164.100.105	TO.	Atta a drive (161)
	59 7.63191	3 05.54.50.215	197.108.109.105	15460	The moderation man
Interpretación de trama seleccionada por nivel OSI	Frame 1 (327 Ethernet 11, Ethernet 11, Ethernet Prot Duser Datagram Duser Datagram Destateg Pro	bytes an wire, 327 byte Src: Sociesel 33:15:24 scal, Src: 382 388,300. Protocol, Src Part: bo (tecol	s captared) (00:06:01:33:75:24), 1 (192:168:100.1), dv otps (67), Dst Part;	Dit: HomAnij t: 192.160.1 Deotp: (68)	17_45:07:18_00:14:65: 01.99_(192.148.181.99
		0/22			
Vaciado hexadecimal	8000 68 15 05 4 8018 61 25 66 0 8628 65 63 68 4 8036 53 bc 00 0	45 af 19 00 06 51 33 fs 10 40 00 20 11 0e 47 00 13 00 44 01 25 af 77 02 10 00 00 c0 a0 65 63 c0	24 88 66 45 58 48 64 82 68 48 .9 81 85 88 39 62 82 10 65 63 88 08	2	96
	He 'Impeters)	OXIMUTY 635 Reckets	of Displayed M Marked	mullet	Madt

Wieasharl









### Escuela Superior de Tlahuelilpan

Área Académica de Ingenierías

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

111-pcap - Wiresbark						
Be EN See So Office Anico	Statistics transformer Dock. H	40		-		
發展發展與 圖 23 3	日日日キャイ	万业	0.04	QQQE		-
Pitas .		+ Ripe	ejon ting	Aceb		
Source	Destination	Pratacos	lafe.			-
148,202:10.13 Invertex.82:00:37 Invertex.93:84153	148.202.10.255 Broadcast Inventec.3cid6137	AGP AGP	who has 148,202	148.202.10.13 148.202.10.13	Tell 148.2 149101-09184	100
148.737.10.13 141.737.804.8 141.737.50.11 148.707.10.13 148.707.10.13	148.202.10.11 CINCOLOUGE 148.202.10.13 148.202.10.13	HTTP	HTTP/2	49340 [5:8, 40] 11470 [15:86] 12 11470 [2] 1 200 04 [12:4	C) Sequel Actor (D) (25) 201 (25) (1) (D) (10) (2) (D) (10) (2) (2) (D) (10) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	
148.202.10.13 148.202.10.13	148.202.10.211 148.202.10.211	NEWS	Martin Di-	ery is ordoless	ET. COM/(00) ET. COM/(00)	1
Crime delta from previou Ories delta from previou Ories since reference or Frame Number: 54 Frame Length: 670 bytes Capture Length: 670 bytes Capture Length: 670 bytes	s Captured frame: 0.00 s displayed frame: 0.0 first frame: 31.77367	0955000 : 00955000 0000 mecc	econt8] seconds] onds]			1
01000 0000 000 000 000 000 000 000 000	10 10	00 110 60 180 60 60 1	47. de 1 1. de 1 1. de ce	Profes Default		मा ग
Minicio B C m (b)21	teler. • 🙆 Novert 🚺	111 prop.		ne . Brittere	e 🕲 00.50	







Área Académica de Ingenierías

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:







### Área Académica de Ingenierías

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:

29 111.p	ocap - Wireshark				
<u>File</u> Edit	t <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyz	e <u>S</u> tatistics Telephony <u>T</u> ools <u>H</u> e	elp		
		x 2 🔒   🔍 🗢 🔿	· · · · · · · · · · · · · · · · · · ·		¥ 🖻 🐔 🔹
Filter: to	p.stream eq 0		▼ Expression	Clear_ Apply	
	Source	Destination	Protocol - Info	)	_
	148.202.10.11	148.202.10.13	HTTP GET	Г / НТТР/1.1	
-	148.202.10.13	148.202.10.11	HTTP HTT	TP/1.1 200 OK (text/h1	tml)
	148.202.10.11	148.202.10.13	TCP 498	340 > http [SYN] Seq=0	Win=8192 Le
	148.202.10.13	148.202.10.11	TCP NUL	LD > 49840 [SYN, ACK] : 240 - http://www.ack] :	Seq=0 ACK=1
	148,202,10,11	148.202.10.13	TCP 498	340 > http [ACK] Seq=1	17 Ack=342 W
	148.202.10.13	148.202.10.11	TCP htt	tp > 49840 [FIN, ACK] 5	5eq=342 Ack=
	148.202.10.11	148.202.10.13	TCP 498	340 > http [ACK] Seq=61	17 Ack=343 W
	148.202.10.11	148.202.10.13	TCP 498	340 > http [RST, ACK] S	5eq=617 Ack=
0					
∙ Ca	 pture Length: 395 byt	es			
Ca [F	pture Length: 395 byt rame is marked: False	es			<u>)</u>
Ca [Fi [Pi	pture Length: 395 byt rame is marked: False rotocols in frame: et	es :] h:1p:tcp:http:data-text-	-lines]		<u>) (</u>
Ca [FI [PI [C	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: H1	es :] h:ip:tcp:http:data-text TP]	-lines]		<u> </u>
Ca) [F] [C] [C]	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: HI oloring Rule String:	es 2] h:1p:tcp:http:data-text- TP] http    tcp.port == 80]	-lines]		<u> </u>
Ca [F] [C] [C] = Ethe	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: H oloring Rule String: rnet II, Src: Invente	es 2] h:ip:tcp:http:data-text TP] http    tcp.port == 80] c_99:84:6a (00:a0:d1:99	-lines] :84:6a), Dst:	Inventec_8c:d6:37 (00	:1e:33:8c:df
Ca [Fi [Ci [Ci Ethe De	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: HI oloring Rule String: rnet II, Src: Invente stination: Inventec_2	es ] h:ip:tcp:http:data-text- TP] http    tcp.port == 80] :c_99:84:6a (00:a0:d1:99 :c:d6:37 (00:1e:33:86:d6	-lines] :84:6a), Dst: :37)	Inventec_8c:d6:37 (00	:1e:33:8c:d€
Ca [F] [C] [C] Ethe De	pture Length: 395 byt rame is marked: Falss rotocols in frame: et oloring Rule Name: HT oloring Rule String: rnet II, Src: Invente stination: Inventec_8	es -] h:ip:tcp:http:data-text- TP] http    tcp.port == 80] •c_99:84:6a (00:a0:d1:99 •c:d6:37 (00:1e:33:8c:d6	-lines] :84:6a), Dst: :37)	Inventec_8c:d6:37 (00	:1e:33:8c:df
Ca [F] [C] [C] Ethe De	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: HT oloring Rule String: rnet II, Src: Invente stination: Inventec_8	es :] h:ip:tcp:http:data-text- TP] http    tcp.port == 80] :c_99:84:6a (00:a0:d1:99 :c:d6:37 (00:1e:33:8c:d6 a0. d1 99 84 63 08 00 45	-lines] :84:6a), Dst: :37)	Inventec_8c:d6:37 (00	:1e:33:8c:d(
Ca [F] [C] [C] Ethe De ( 0000 C	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: H oloring Rule String: rnet II, Src: Invente stination: Inventec_8 00 1e 33 8c d6 37 00 1. 7d 0e f7 40 00 80	es :] h:ip:tcp:http:data-text TP] http    tcp.port == 80] :c_99:84:6a (00:a0:d1:99 :c:d6:37 (00:1e:33:8c:d6 a0 d1 99 84 6a 08 00 45 06 ac d7 94 ca 08 00 45	-lines] :84:6a), Dst: :37) 0037. ca .l.@.	Inventec_8c:d6:37 (00	:1e:33:8c:d€
Ca [F] [C] [C] Ethe De (0000 C 0000 C 0000 C	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: H oloring Rule String: rnet II, Src: Invente stination: Inventec_8 00 1e 33 8c d6 37 00 01 7d 0e f7 40 00 80 3a 0b 00 50 c2 b0 49	es 1) h:ip:tcp:http:data-text TP] http    tcp.port == 80] c_99:84:6a (00:a0:d1:99 tc:d6:37 (00:1e:33:8c:d6 0 a0 d1 99 84 6a 08 00 45 06 ac d7 94 ca 08 00 45 06 ac d7 94 ca 08 00 45 06 b8 6c 1f b6 ec 50	-lines] :84:6a), Dst: :37) 0037. ca .}.@ 18P1	Inventec_8c:d6:37 (00	:1e:33:8c:dt
Ca [F] [C] [C] [C] [C] [C] [C] [C] [C] [C] [C	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: H oloring Rule String: rnet II, Src: Invente stination: Inventec_8 00 le 33 8c d6 37 00 01 70 0e f7 40 00 80 03 00 00 50 c2 b0 49 01 00 2f f2 00 00 48	es ] h:ip:tcp:http:data-text- TP] http    tcp.port == 80] :c_99:84:6a (00:a0:d1:99 :c:d6:37 (00:1e:33:8c:d6 a0 d1 99 84 6a 08 00 45 26 ac d7 94 ca 0a 0d 94 00 b5 b8 cc 1f b6 ec 50 54 50 2f 31 2e 31 20 54 50 2f 31 2e 31 20 55 50 2f 30 2f	-lines] :84:6a), Dst: :37) 0037. ca .}.@ 18P.II 32H	Inventec_8c:d6:37 (00	:1e:33:8c:d(
Ca [F [P [C] [C] Ethe 0000 C 0010 C 0020 C 0030 C 0030 C 0030 C	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: HT oloring Rule String: rnet II, Src: Invente stination: Inventec_8 00 1e 33 8c d6 37 00 01 7d 0e f7 40 00 80 01 00 2f f2 00 00 48 30 30 20 4f 4b 0d 0a 02 30 21 27 20 4d 61	es :] h:1p:tcp:http:data-text- TP] http    tcp.port == 80] :c_99:84:6a (00:a0:d1:99 :c:d6:37 (00:1e:33:8c:d6 a0 d1 99 84 6a 08 00 45 06 ac d7 94 ca 0a 0d 94 00 b5 b8 6c 1f b6 ec 50 54 54 50 2f 31 2e 31 20 24 54 50 2f 31 2e 31 20 54 54 50 2f 31 2e 31 20 55 36 2f 31 2e 31 20 56 36 2f 30 2e 31 2e 31 20 56 36 2f 30 2e 31 2e 31 20 56 36 2f 30 2e 31 2e 30 20 56 36 2f 30 2e 31 2e 31 2e 30 56 36 2f 30 2e 31 2e 31 2e 30 56 36 2f 30 2e 31 2e 31 2e 30 56 36 2f 30 2e 31 2e 31 2e 30 56 36 2f 30 2e 32 2e 32 2e 32 2e 32 2e 30 56 36 2f 30 2e 30 56 36 2f 30 2e 31 2e 31 2e 30 56 36 2f 30 2e 31 2e 31 2e 30 56 36 2f 30 2e 31 2e 31 56 36 2f 30 2e 31 2e 30 56 36 2f 30 2e 30 56 36 2f 30 56 36 36 2f 30 56 36 3f 30 56 3f	-lines] :84:6a), Dst: :37) 0037. ca .}0. 18P.II 12H 69 00 OK 24 12 MO	Inventec_8c:d6:37 (00	:1e:33:8c:d(
Ca [F] [C] [C] [C] [C] [C] [C] [C] [C] [C] [C	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: HI oloring Rule String: rnet II, Src: Invente stination: Inventec_8 00 1e 33 8c d6 37 00 11 7d 0e f7 40 00 80 03a 0b 00 50 c2 b0 49 11 00 2f f2 00 00 48 30 30 20 4f 4b 0d 0a 20 30 21 22 30 4d 61 20 30 41 23 34 4d 61	es ) h:1p:tcp:http:data-text TP] http    tcp.port == 80] c_99:84:6a (00:a0:d1:99 c:d6:37 (00:1e:33:8c:d6 a0 d1 99 84 6a 08 00 45 06 ac d7 94 ca 0a 0d 94 00 b5 b8 6c 1f b6 ec 50 54 54 50 2f 31 2e 31 20 44 61 74 65 3a 20 46 72 72 00 21 20 21 20 31 21 CAR Packets: 79 Displayed: 9Ma	-lines] :84:6a), Dst: :37) 0037. ca	Inventec_8c:d6:37 (00 jE. jP. TTP/1.12 D ate: Fri Profile: Default	:1e:33:8c:d6
Cai [F] [P] [C] [C] [C] [C] [C] [C] [C] [C] [C] [C	pture Length: 395 byt rame is marked: False rotocols in frame: et oloring Rule Name: H oloring Rule String: rnet II, Src: Invente stination: Inventec_8 00 1e 33 8c d6 37 00 11 7d 0e f7 40 00 80 0a 0b 00 50 c2 b0 49 01 00 2f f2 00 00 49 01 00 2f f2 00 00 49 03 03 02 0 2f 42 00 40 41 (Documents and Settings\FAMILI	es es i) h:ip:tcp:http:data-text- TP] http    tcp.port == 80] ic_99:84:6a (00:a0:d1:99 ic:d6:37 (00:1e:33:8c:d6 a0 d1 99 84 6a 08 00 45 06 ac d7 94 ca 08 00 45 06 ac d7 94 ca 08 00 45 06 ac d7 94 ca 08 00 45 27 20 23 20 21 20 20 21 24 61 74 65 3a 20 46 72 27 20 23 20 21 20 20 21 _CAR Packets: 79 Displayed: 9 Ma	-lines] :84:6a), Dst: :37) 0037. ca .}.6 18PI 32/H 69 00 OK 24 13 M3 rked: 0	Inventec_8c:d6:37 (00	:1e:33:8c:dt







Área Académica de Ingenierías

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

### Ejemplo









Escuela Superior de Tlahuelilpan

Área Académica de Ingenierías

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

#### Ejemplo









### Escuela Superior de Tlahuelilpan

Área Académica de Ingenierías

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











Área Académica de Ingenierías

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









Área Académica de Ingenierías

# Bibliografía

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

