



“Secretaría De La Educación Superior”
“Instituto Tecnológico de Cancún”

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Laboratorio N#37 Wireshark

Alumno: Vargas Rodríguez Javier Jesús

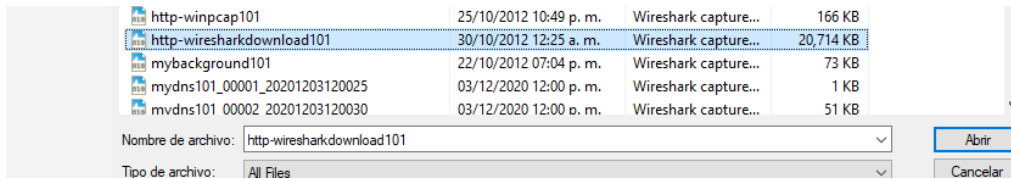
Maestro: Ismael Jiménez Sánchez

Fecha De Entrega: 6/Diciembre/2020

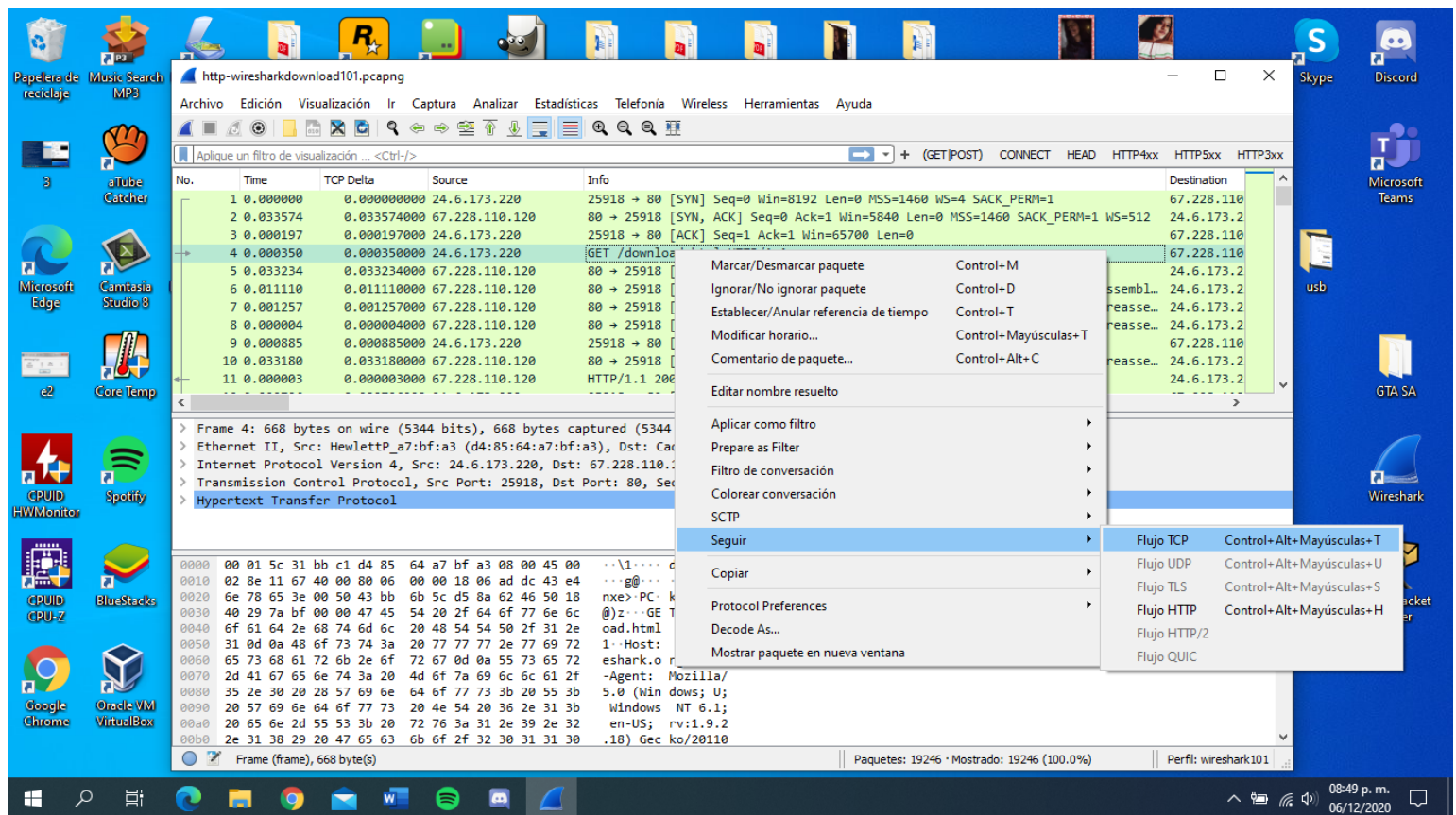
Horario: 5:00 pm – 6:00 pm

Laboratio N#37 – Usamos el reensamblaje para encontrar el mensaje HTTP oculto en un sitio web.

Paso 1 – Abrimos el archivo http-wiresharkdownload101.pcapng



Paso 2 – Los primeros 3 paquetes TCP para la conexión del servidor web. El frame 4 es el cliente. Solicitud GET para la pagina download.html. Haga clic con el botón derecho en el Frame 4 y seleccionar Seguir | Secuencia TCP



Paso 3 – Wireshark muestra la conversación sin los encabezados Ethernet, IP o TCP. Desplazarse por el Stream para buscar el mensaje oculto Gerald Combs, creador de wireshark se encuentra en el servidor y comienza con X-SLOGAN.

Wireshark - Seguir flujo TCP (tcp.stream eq 0) - http-wiresharkdownload101.pcapng

GET /download.html HTTP/1.1
Host: www.wireshark.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.18) Gecko/20110614 Firefox/3.6.18
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Cookie: __utma=87653150.190379794.1311185717.1311454861.1311475252.3; __utmc=87653150; __utmz=87653150.1311475252.3.6.utmcsrc=google|utmccn=(organic)|utmcmd=organic|utmctr=wireshark%20bug%202234; __utmb=87653150.3.10.1311475252

HTTP/1.1 200 OK
Date: Sun, 24 Jul 2011 02:43:21 GMT
Server: Apache/2.2.14 (Ubuntu)
Last-Modified: Wed, 20 Jul 2011 22:53:12 GMT
Accept-Ranges: bytes
X-Mod-Pagespeed: 0.9.11.5-312
Vary: Accept-Encoding
Content-Encoding: gzip
X-Slogan: Sniffing the glue that holds the Internet together.
Cache-control: max-age=0, no-cache, no-store
Content-Length: 5457
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

.....<kw.....8S.I...9.e.m3
L...K..D.X.d'.....\$......*..ei.....}.k....z}I..'.Rsc..N..N..].....75R.
%I[y.....B...w.(...J\$.7H.Z{...HH.a.Ex.h.?OB.~.%S#*...c..9\$.b...G...q...\$.j
.O<...l..Y...K.H.A.i.N...p..f.....T9.z..4...../.....@.....J..?..q,dBR.nY..|....)?
L...;

Paquete 6.1 cliente pkt.5 servidor pkt.1 cambio.Clic para seleccionar.

Conversación completa (6518 bytes) Show data as ASCII Secuencia 0

Buscar: Filtrar esta secuencia Imprimir Save as... Atrás Cerrar Ayuda

Frame (frame), 668 byte(s) Paquetes: 19246 - Mostrado: 16 (0.1%) Perfil: wireshark101

Paso 4 – Este no es el único mensaje oculto en la sesión de navegación web, ahora que conocemos el mensaje comienza con “X – Slogan”.

Hacemos clic en el botón cerrar y luego en el botón borrar para eliminar el filtro TCP.

The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request. The packet list shows three frames, with frame 21 selected. The packet details pane shows the structure of the frame: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data of the frame, which is a GIF image.

No.	Time	TCP Delta	Source	Info	Destination
6	0.000000	0.011110000	67.228.110.120	80 → 25918 [ACK] Seq=1 Ack=615 Win=7168 Len=1460 [TCP segment of a reassembl...	24.6.173.220
21	0.342493	0.001377000	67.228.110.120	HTTP/1.1 200 OK (GIF89a)	24.6.173.220
28	0.303759	0.006065000	2607:f0d0:2001:e:1::...	HTTP/1.1 200 OK (GIF89a)	2002:1806:adcc::1

Frame 21: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface unknown, id 0

- Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
- Internet Protocol Version 4, Src: 67.228.110.120, Dst: 24.6.173.220
- Transmission Control Protocol, Src Port: 80, Dst Port: 25919, Seq: 1, Ack: 650, Len: 478
- Hypertext Transfer Protocol
- CompuServe GIF, Version: GIF89a

Paquetes: 19246 · Mostrado: 3 (0.0%) | Perfil: wireshark101

Paso 5 - Hacemos clic derecho en los otros 2 frames desplazados y seleccionamos Seguir | Secuencia TCP para examinar encabezados HTTP entre Host.

The screenshot shows the Wireshark interface with the 'Follow TCP Stream' window open. The window displays the raw data of the selected packet, which is a GIF image. The window also shows the packet details pane and the packet bytes pane. The 'Follow TCP Stream' window is titled 'Seguir flujo TCP (tcp.stream eq 2) · http-wiresharkdownload101.pcapng'.

GET /image/ipv4.gif?id=1068963279 HTTP/1.1
Host: ipv4.wireshark.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.18) Gecko/20110614 Firefox/3.6.18
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.wireshark.org/download.html
Cookie: __utma=87653150.190379794.1311185717.1311454861.1311475252.3; __utmc=87653150.1311475252.3.6.utmcsrc=google|utmcn=(organic)|utmcmd=organic|utmcctr=wireshark%20bug%202234; __utmb=87653150.4.10.1311475252

HTTP/1.1 200 OK
Date: Sun, 24 Jul 2011 02:43:21 GMT
Server: Apache/2.2.14 (Ubuntu)
Vary: Host
Last-Modified: Wed, 20 Jul 2011 22:53:22 GMT
Accept-Ranges: bytes
Content-Length: 43
Link: <http://www.wireshark.org/image/ipv4.gif>; rel="canonical"
X-Slogan: Sniffing the glue that holds the Internet together.
Cache-control: public, max-age=600
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: image/gif

GIF89a.....!.....D..;

Paquete 21: cliente pkt.1 servidor pkt.1 cambio. Clic para seleccionar.

Conversación completa (1127 bytes) Show data as ASCII Secuencia 2

Buscar: Buscar siguiente

Paquetes: 19246 · Mostrado: 11 (0.1%) | Perfil: wireshark101

Paso 6 – Hacemos clic en cerrar la ventana cuando se haya terminado de ver las corrientes.