



**TECNOLÓGICO
NACIONAL DE MÉXICO**



INSTITUTO TECNOLÓGICO DE CANCÚN

SISTEMAS COMPUTACIONALES

MATERIA: Fundamentos de Telecomunicaciones

PROFESOR: ING. ISMAEL JIMÉNEZ SÁNCHEZ

LABORATORIO: 37

Alumno:

SARRAGOT PASTRANA WILIAM ADRIEN

LAB 37: UTILICE EL REENSAMBLAJE PARA ENCONTRAR EL MENSAJE HTTP OCULTO DE UN SITIO WEB

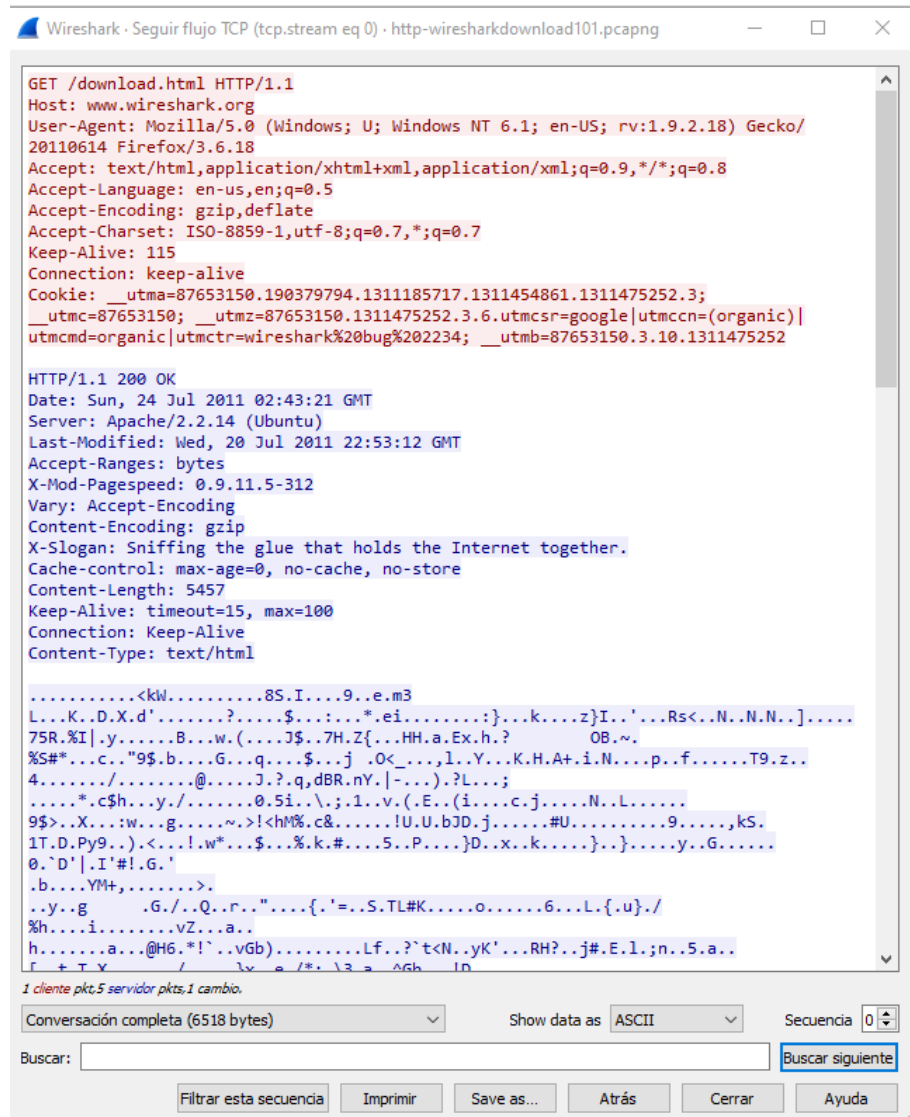
Paso 1: Abra `http-wireharkdownload101.pcapng`

Paso 2: Los primeros tres paquetes son el protocolo de enlace TCP para la conexión del servidor web. El marco 4 es la solicitud GET del cliente para la página `download.html`. Haga clic con el botón derecho en el marco 4 y seleccione seguir, flujo TCP.

El tráfico del primer host que se ve en el archivo de seguimiento, el cliente en este caso, se muestra en rojo El tráfico del segundo host que se ve en el archivo de seguimiento, el servidor en este caso, se muestra en azul.

Paso 3:

Wireshark muestra la conversación sin los encabezados ethernet, ip o TCP, desplácese por la secuencia para buscar el mensaje oculto de gerald combs, creador wirehark. Se encuentra en la secuencia del servidor y comienza con X-Slogan. X-SLOGAN: Esnifando el pegamento que une a Internet



```
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.utmsr=google|utmccn=(organic)|utmcmd=organic|utmctr=wireshark%20bug%202234; __utmb=87653150.3.10.1311475252

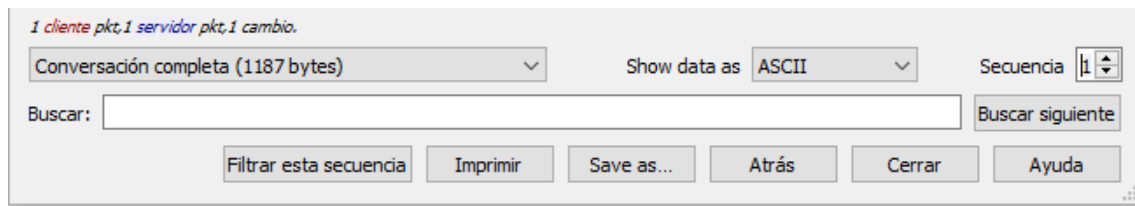
HTTP/1.1 200 OK
Date: Sun, 24 Jul 2011 02:43:21 GMT
Server: Apache/2.2.14 (Ubuntu)
Last-Modified: Wed, 20 Jul 2011 22:53:12 GMT
Accept-Ranges: bytes
X-Mod-Pagespeed: 0.9.11.5-312
Vary: Accept-Encoding
Content-Encoding: gzip
X-Slogan: Sniffing the glue that holds the Internet together.
Cache-control: 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'.....?.....$......*..ei.....:}...k.....z}I...Rs<..N..N..N.].....
75R.%I|.y.....B...w.(....J$.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...;
.....*.c$h...y./.....0.Si..\.j.1..v.(.E..(i...c.j.....N..L.....
9$>..X...:w...g.....~.~!<hM%.c&.....!U.U.bJD.j.....#U.....9.....,kS.
1T.D.Py9..).<...!w*...$.%.k.#....5..P....}D..x.k.....}.}.....y..G.....
0.'D'|.I'#!.G.'
.b....YM+,.....>.
..y..g      .G./..Q..r..".....{.'=.S.TL#K.....O.....6...L.{.u.}/
%h.....i.....vZ...a..
h.....a...@H6.*!'..vGb).....Lf..?*'t<N..yK'...RH?...j#.E.l;n..5.a..
[ + T Y / \ x a / * + \ 3 a ^ G b 1 D

1 cliente pkt, 5 servidor pkts, 1 cambio.
```

Paso 4: Este no es el único mensaje oculto en la sesión de navegación web. Ahora que sabe que el mensaje comienza con "X-slogan", ¿cómo podría hacer que Wireshark muestre cada cuadro que tiene este ACII? Haga clic en el botón cerrar y en el botón borrar para eliminar el filtro de flujo TCP Aplicar el marco del filtro de visualización que contiene "X-Slogan"

Paso 5: Haga clic derecho en los otros dos marcos mostrados y seleccione Seguir, Flujo TCP para examinar los encabezados HTTP intercambiados entre el host. ¿Encontraste el otro?



Paso 6: Limpieza de Lan, haga clic en el botón Cerrar en las siguientes ventanas de Steam TCP cuando haya terminado de seguir las secuencias