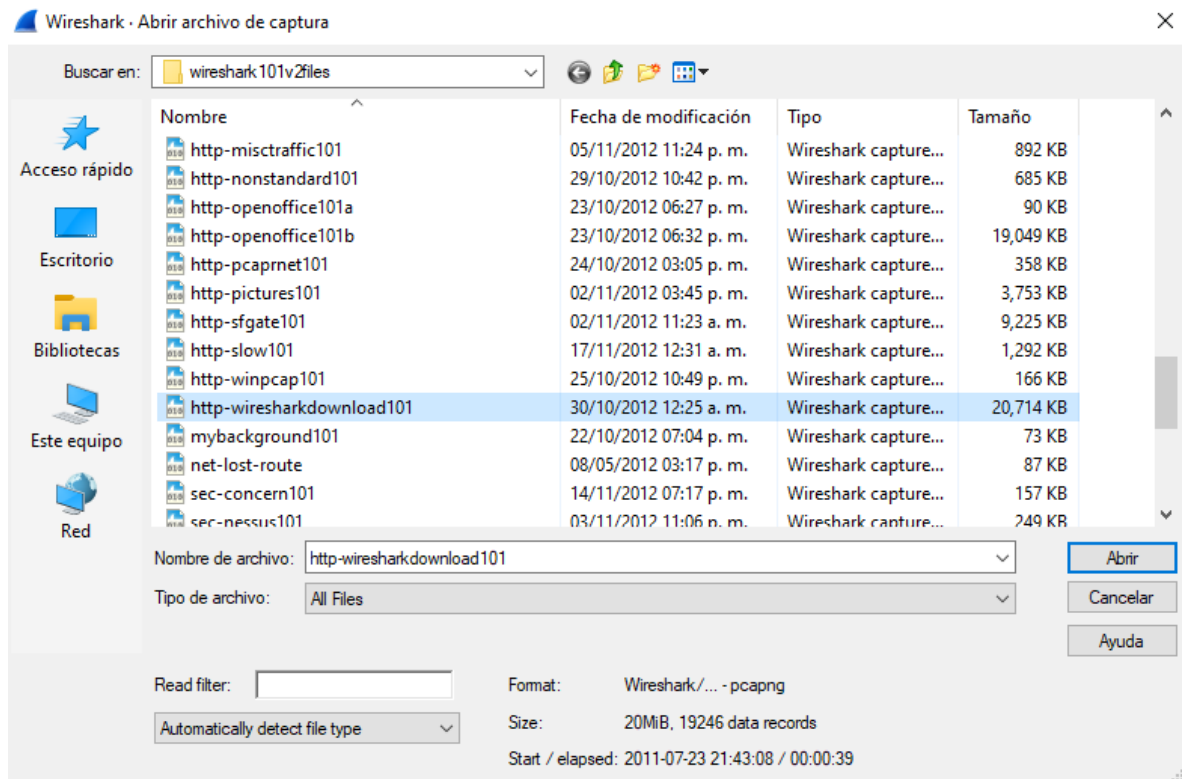


Lab 37

Abriremos el archivo “http-wiresharkdownload101.pcapng”



Veremos que los primeros tres paquetes son el protocolo TCP para la conexión del servidor web y el cuarto es la solicitud GET del cliente para la pagina download.html, daremos clic derecho en el paquete 4 y después en follow y flujo de TCP

The screenshot displays the Wireshark interface with a packet capture named 'http-wiresharkdownload101.pcapng'. The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Coloring Rule Name	Info
1	0.000000	24.6.173.220	67.228.110.120	TCP	HTTP	25918 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.033574	67.228.110.120	24.6.173.220	TCP	HTTP	80 → 25918 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
3	0.000197	24.6.173.220	67.228.110.120	TCP	HTTP	25918 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.000350	24.6.173.220	67.228.110.120	HTTP	HTTP	GET /download.html HTTP/1.1
5	0.033234	67.228.110.120	24.6.173.220	TCP	HTTP	80 → 25918 [ACK] Seq=1 Ack=615 Win=7168 Len=0

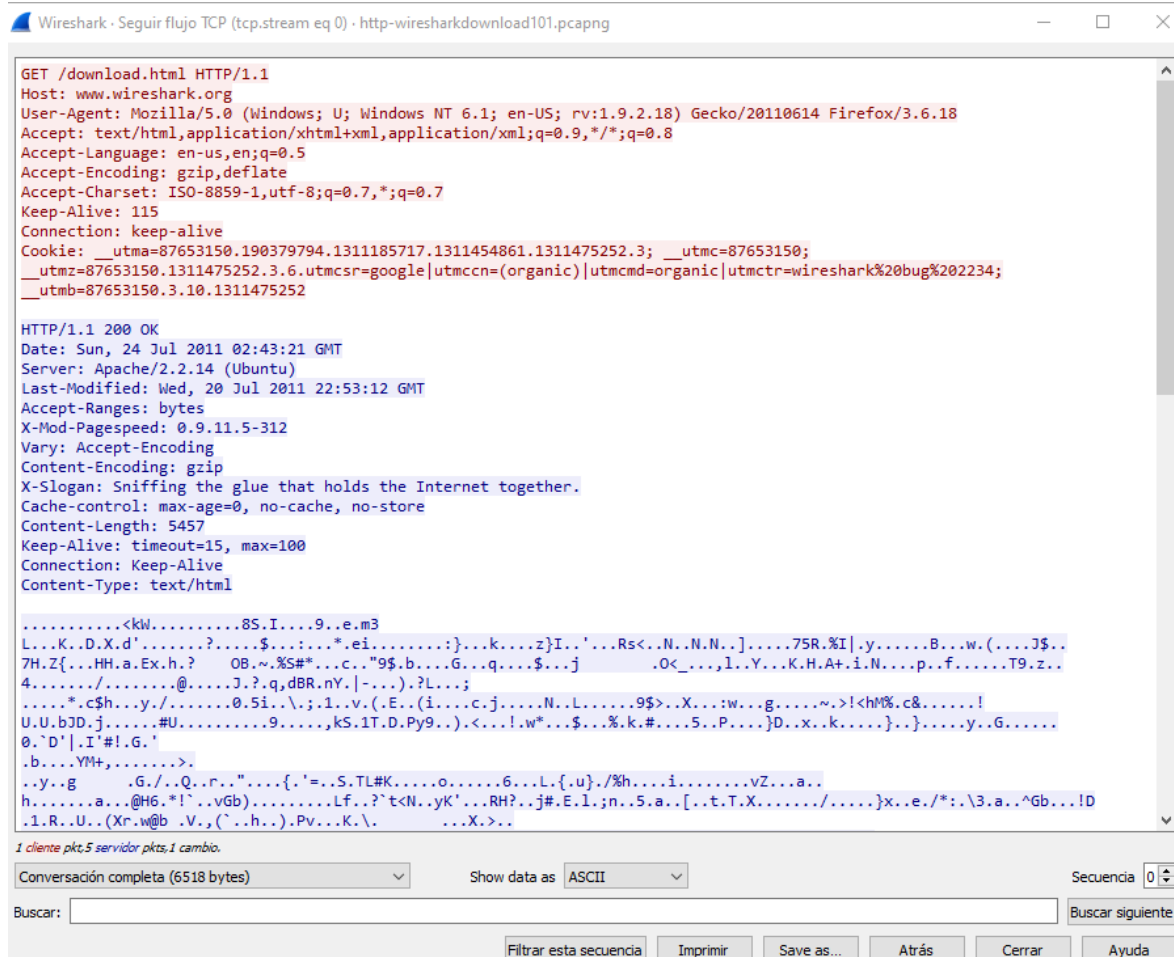
The packet details pane for packet 4 shows the following structure:

- Ethernet II, Src: Intel E100 (08:00:00:00:00:00), Dst: Intel E100 (08:00:00:00:00:00)
- Internet Protocol Version 4, Src: 24.6.173.220, Dst: 67.228.110.120
- Transmission Control Protocol, Src Port: 25918, Dst Port: 80, Seq: 1, Ack: 1, Win: 65700, Len: 0
- Hypertext Transfer Protocol, Method: GET, Path: /download.html, Version: 1.1

A right-click context menu is open over packet 4, with the 'Seguir' (Follow) option selected. The submenu shows the following options:

- Flujo TCP (Control+Alt+Mayúsculas+T)
- Flujo UDP (Control+Alt+Mayúsculas+U)
- Flujo TLS (Control+Alt+Mayúsculas+S)
- Flujo HTTP (Control+Alt+Mayúsculas+H)
- Flujo HTTP/2
- Flujo QUIC

El programa nos mostrará la conversación sin los encabezados de Ethernet, IP o TCP, navegaremos por la ventana hasta encontrar el mensaje oculto de Gerald Combs, creador de Wireshark, el cual se encuentra en el flujo del servidor que comienza con “X-Slogan”



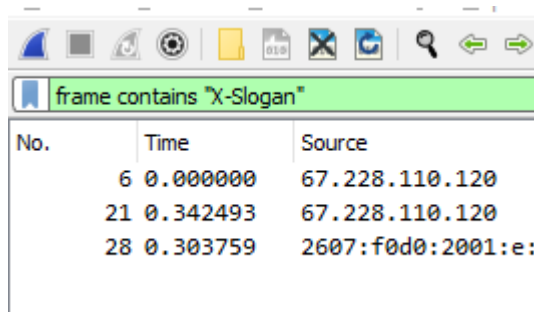
```
GET /download.html HTTP/1.1
Host: www.wireshark.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.18) Gecko/20110614 Firefox/3.6.18
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: 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.utmcsr=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'.....?.....$.e.i.....}...k...z}I...'..Rs<..N..N.N..].....75R.%I|.y.....B...w.(...J$.
7H.Z{...HH.a.Ex.h.? 0B.~.%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$..y./.....0.5i..\.;1..v.(.E..(i...c.j.....N..L.....9$>..X...:w...g.....~>|<hM%.c&.....!
U.U.bJD.j.....#U.....9.....,kS.1T.D.Py9..).<...!w*...$...%k.#...S...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.T.X...../.....}x..e./*:. \3.a..^Gb...!D
.l.R..U..(Xr.w@b .V.,('..h..).Pv...K..\. ...X.>..
```

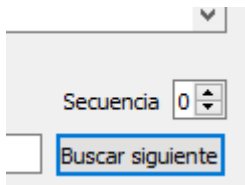
Una vez que cerremos esta ventana, borraremos el filtro de seguimiento de flujo TCP

Y escribiremos frame contains “X-Slogan”.



No.	Time	Source
6	0.000000	67.228.110.120
21	0.342493	67.228.110.120
28	0.303759	2607:f0d0:2001:e:

Daremos clic derecho sobre los paquetes, después en seguir y flujo de TCP para examinar los encabezados intercambiados entre hosts, utilizaremos las flechas de navegación de la secuencia para pasar entre secuencias



Utilizará esta función en su proceso de análisis, esto en lugar de desplazarnos por un archivo de seguimiento y examinar cada paquete uno por uno, siga los flujos TCP, UDP o SSL.