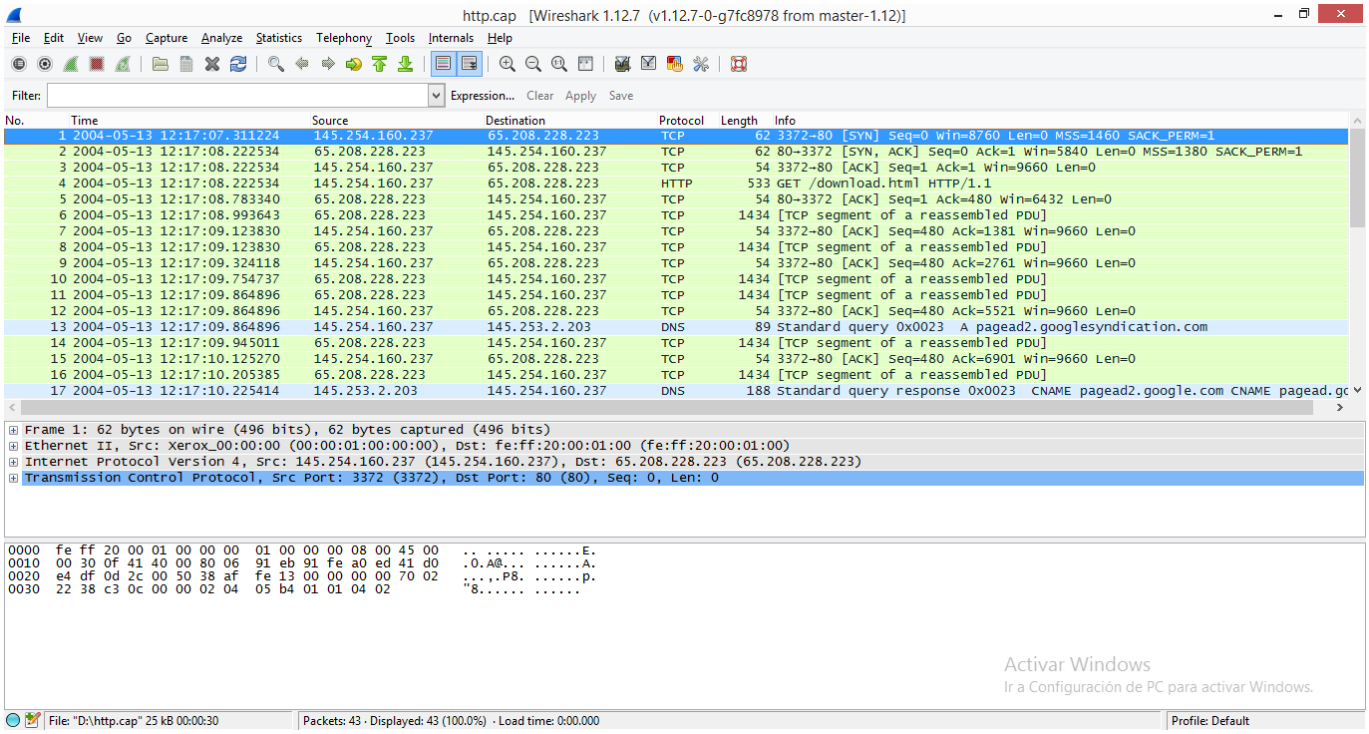
Introducción a Wireshark

Una herramienta básica para observar los mensajes intercambiados entre aplicaciones es un analizador de protocolos (packet sniffer). Un analizador de protocolos es un elemento pasivo, únicamente observa mensajes que son transmitidos y recibidos desde y hacia un elemento de la red, pero nunca envía él mismo mensajes. En su lugar, un analizador de protocolos recibe una copia de los mensajes que están siendo recibidos o enviados en el terminal donde está ejecutándose.

Está compuesto principalmente de dos elementos: una librería de captura de paquetes, que recibe una copia de cada trama de enlace de datos que se envía o recibe, y un analizador de paquetes, que muestra los campos correspondientes a cada uno de los paquetes capturados. Para realizar esto, el analizador de paquetes ha de conocer los protocolos que está analizando de manera que la información mostrada sea coherente. Es decir, si capturamos un mensaje HTTP, el analizador de paquetes ha de saber que este mensaje se encuentra encapsulado en un segmento TCP, que a su vez se encuentra encapsulado en un paquete IP y éste a su vez en una trama de Ethernet.


http.cap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 2004-05-13 12:17:07.311224 145.254.160.237 65.208.228.223 TCP 62 3372→80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
2 2004-05-13 12:17:08.222534 65.208.228.223 145.254.160.237 TCP 62 80→3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM=1
3 2004-05-13 12:17:08.222534 145.254.160.237 65.208.228.223 TCP 54 3372→80 [ACK] Seq=1 Ack=1 Win=9660 Len=0
4 2004-05-13 12:17:08.222534 145.254.160.237 65.208.228.223 HTTP 533 GET /download.html HTTP/1.1
5 2004-05-13 12:17:08.783340 65.208.228.223 145.254.160.237 TCP 54 80→3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
6 2004-05-13 12:17:08.993643 65.208.228.223 145.254.160.237 TCP 1434 [TCP segment of a reassembled PDU]
7 2004-05-13 12:17:09.123830 145.254.160.237 65.208.228.223 TCP 54 3372→80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
8 2004-05-13 12:17:09.123830 65.208.228.223 145.254.160.237 TCP 1434 [TCP segment of a reassembled PDU]
9 2004-05-13 12:17:09.324118 145.254.160.237 65.208.228.223 TCP 54 3372→80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
10 2004-05-13 12:17:09.754737 65.208.228.223 145.254.160.237 TCP 1434 [TCP segment of a reassembled PDU]
11 2004-05-13 12:17:09.864896 65.208.228.223 145.254.160.237 TCP 1434 [TCP segment of a reassembled PDU]
12 2004-05-13 12:17:09.864896 145.254.160.237 65.208.228.223 TCP 54 3372→80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
13 2004-05-13 12:17:09.864896 145.254.160.237 145.253.2.203 DNS 89 Standard query 0x0023 A pagead2.googlesyndication.com
14 2004-05-13 12:17:09.945011 65.208.228.223 145.254.160.237 TCP 1434 [TCP segment of a reassembled PDU]
15 2004-05-13 12:17:10.125270 145.254.160.237 65.208.228.223 TCP 54 3372→80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0
16 2004-05-13 12:17:10.205385 65.208.228.223 145.254.160.237 TCP 1434 [TCP segment of a reassembled PDU]
17 2004-05-13 12:17:10.225414 145.253.2.203 145.254.160.237 DNS 188 Standard query response 0x0023 CNAME pagead2.google.com CNAME pagead.g
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Internet Protocol Version 4, Src: 145.254.160.237 (145.254.160.237), Dst: 65.208.228.223 (65.208.228.223)
Transmission Control Protocol, Src Port: 3372 (3372), Dst Port: 80 (80), Seq: 0, Len: 0
0000 fe ff 20 00 01 00 00 00 01 00 00 00 08 00 45 00 .. ..E.
0010 00 30 0f 41 40 00 80 06 91 eb 91 fe a0 ed 41 d0 .0.A@... ......A.
0020 e4 df 0d 2c 00 50 38 af fe 13 00 00 00 00 70 02 ...,.P8. ......p.
0030 22 38 c3 0c 00 00 02 04 05 b4 01 01 04 02 "8..... ......
Activar Windows
Ir a Configuración de PC para activar Windows.
File: "D:\http.cap" 25 kB 00:00:30
Packets: 43 · Displayed: 43 (100.0%) · Load time: 0:00.000
Profile: Default