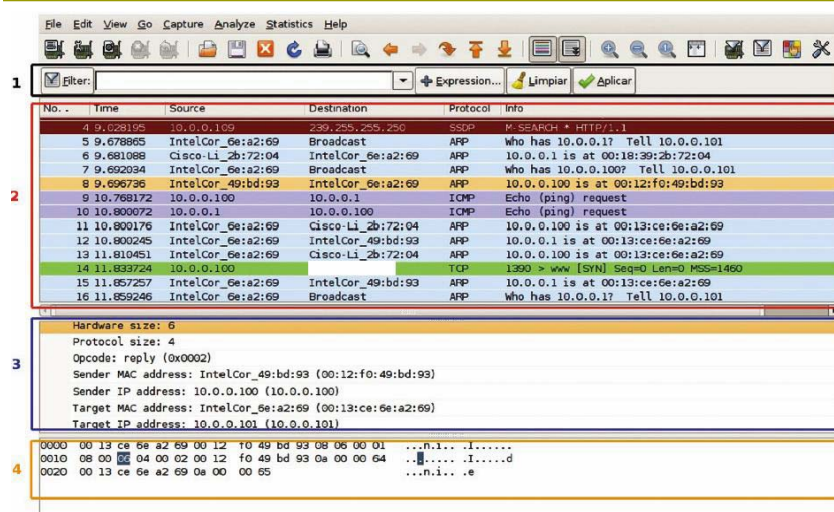


WIRESHARK Secciones



Zonas de información

- ❑ Zona de listado de los paquetes capturados con información de:
 - Numero de Frame, tiempo en segundos de la captura, Origen, Destino, protocolo involucrado y por último un campo de información extra que previamente Wireshark a decodificado.
- ❑ Zona de muestra de datos del Frame capturado. En este caso Frame 23 o captura 23 (las enumera secuencialmente) nos da información de todos los protocolos involucrados en la captura:
 - En campo **Frame** nos muestra información completa de la trama capturada. Tamaño total, etc. A continuación Ethernet II que nos muestra la **cabecera Ethernet II** que a su vez pertenece a la capa de enlace de datos:
 - ❑ 0000 00 04 75 ed 89 c3 00 14 22 5f a9 25 08 00
 - Nos muestra parte de la cabecera de la trama Ethernet II, en este caso:
 - ❑ **Destino** 6 bytes 00 04 75 ed 89 c3 : MAC destino
 - ❑ **Origen** 6 bytes 00 14 22 5f a9 25 : MAC origen
 - ❑ **Tipo** 2 bytes 08 00 : protocolo que viaja en la parte de datos de la trama en este caso **IP**. 0x0800.
- ❑ Zona de protocolos: en este ejemplo vemos Internet Protocol y TCP
- ❑ Internet Protocol con los datos de la cabecera del datagrama IP:
 - 0000 45 00 02 93 e1 8f 00 00 80 06 6f b2 d9 7e 4b de E.....o...~K.
0010 c0 a8 01 1e
- ❑ Transmission Control Protocol. (TCP):
 - 0000 00 50 12 67 21 9e b2 a5 99 28 f1 c8 50 18 fd b2 .P.g!....(.P...
0010 f5 79 00 00 .y..
 - Información del **Puerto de origen, destino, número de secuencia**, etc.
 - **TCP Segment Data**, con todo el contenido del campo Data del segmento TCP.

Ejemplo Zonas de Información

[Untitled] - Wireshark					
File Edit View Go Capture Analyze Statistics Help					
Expression... New Bookmarks					
No.	Time	Source	Destination	Protocol	Info
19	20.999999	217.126.75.222	192.168.1.30	IGMP	v2 Membership query
20	21.053335	0e11:5f:a9:25	Broadcast	ARP	who has 192.168.1.12? Tell 192.1
21	21.482221	192.168.1.30	239.255.255.250	IGMP	v2 Membership report
22	21.530214	192.168.1.30	224.0.0.9	IGMP	v2 Membership report
23	21.850315	217.126.75.222	192.168.1.30	ICMP	Echo (ping) of a reassembled PK
24	21.92808	217.126.75.222	192.168.1.30	TCP	[TCP segment of a reassembled PK
Frame 23 (673 bytes on wire (673 bytes captured))					
Arrival Time: Feb 14, 2008 11:00:21.113714000					
[Time delta from previous captured frame: 0.662299000 seconds]					
[Time delta from previous displayed frame: 0.662299000 seconds]					
[Time since reference or first frame: 18.192313000 seconds]					
Frame number: 23					
Frame Length: 673 bytes					
Capture Length: 673 bytes					
[Frame is marked: False]					
[Protocols in Frame: eth:ip:tcp:icmp]					
[Coloring rule Name: HTTP]					
[Coloring rule string: http tcp.port == 80]					
[Click on the "Details" pane to expand the details pane]					
[Click on the "Packet Bytes" pane to expand the packet bytes pane]					
Destination: 3Com.ed:89:c3 (00:04:73:ed:89:c3)					
Source: dell.sf:a9:25 (00:14:22:5f:a9:25)					
Type: IP (0x0800)					
Internet Protocol, Src: 217.126.75.222 (217.126.75.222), Dst: 192.168.1.30 (192.168.1.30)					
Transmission Control Protocol, Src Port: http (80), Dst Port: 4711 (4711), Seq: 1, Ack: 590, Len: 619					
Source port: http (80)					
Destination port: 4711 (4711)					
Sequence number: 1 (relative sequence number)					
Next sequence number: 620 (relative sequence number)					
Acknowledgement number: 590 (relative ack number)					
Header length: 20 bytes					
Flags: 0x18 (PSH, ACK)					
Window size: 64946					
Checksum: 0x4370 (correct)					
0000 00 04 75 ed 89 c3 00 14 22 5f a9 25 08 00 45 00 00.....0x0800..					
0010 02 99 42 8f 00 00 00 0f 02 09 7d 4b 06 c0 a80.....					
0020 01 1e 00 50 12 67 21 9e b2 45 99 28 f1 c8 50 18P.g...(.P.					
0030 f0 b2 f5 79 00 00 48 54 54 50 2f 31 2e 31 20 32 ...y..HT 19/1.1.2					
0040 30 30 20 4f 4b 0d 0a 44 63 74 63 3a 20 54 68 75 00 0c.0 ates: Thu					
0050 2c 20 31 34 20 46 65 62 20 32 30 30 38 20 30 39 , 14 Feb 2008 09					
0060 3a 15 37 3a 32 36 20 47 4d 54 0d 0a 53 65 72 76 157.26 G MT, Serv					
0070 65 72 3a 20 41 70 63 63 68 65 2f 32 2e 30 2e 36 er: Apac he/2.0.6					
0080 31 20 28 37 69 64 33 32 29 20 6d 6f 64 5f 73 73 1 (win32) mod_ss					
0090 6c 2f 32 2e 30 2e 36 31 20 4f 70 65 6e 53 53 4c /2.0.61. openSL					
00a0 2f 30 2e 39 2e 37 6d 20 50 48 50 2f 34 2e 33 2e /0.9.7m PHP/4.3.					
00b0 31 31 0d 0a 58 2d 50 6f 77 65 72 63 64 2d 42 79 31.x-no word-by					
00c0 3a 20 50 48 50 2f 34 2e 34 2e 37 0d 0a 53 65 74 : PHP/4.4.7..set					
00d0 2d 42 6f 6f 69 65 3a 20 70 69 70 62 62 32 6d -Cook:1e phpb2m					
00e0 79 73 75 6c 5f 64 61 74 61 3d 61 25 33 41 32 25 ysql_dat a=x3A2X					
00f0 33 41 21 37 42 75 23 33 41 31 31 25 33 41 21 32 3AN789K3 Al1X3AK2					
0100 32 63 75 6f 6c 6f 6f 69 6e 69 64 21 32 32 25 2autolog tntC2K					
0110 33 42 75 25 33 41 33 32 25 33 41 25 32 32 63 32 385N3A32 N3AN2c2					
0120 65 62 36 30 30 30 66 38 36 36 32 64 64 33 37 63 6e600F9 662d97C					
0130 63 33 63 35 38 63 34 65 30 63 37 63 66 63 25 32 c3c58c4e 0c7afAN2					
0140 32 25 33 42 72 25 33 41 36 25 33 41 25 32 32 75 2K38N3A 0NAN22u					
0150 73 65 72 6d 64 25 32 32 25 33 42 6d 75 33 41 34 ser1CN22 N3AN3A4					