

EJERCICIOS DE CAPTURA DE TRÁFICO

- 1) Tras realizar la captura, guardarla y reabrirla, nos encontramos con que solamente hay un paquete con el campo PO 53, como se aprecia en la siguiente diapositiva:

The image shows a Wireshark capture of network traffic. The main packet list pane displays a series of packets, with packet 53 highlighted. The packet details pane shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2804	3.038270	192.168.121.128	150.244.214.237	TCP	54	2804 → 80 [SYN] Seq=0 Win=512 Len=0
2804	5.054436	192.168.121.128	150.244.214.237	TCP	54	2804 → 80 [RST] Seq=1 Win=0 Len=0
2805	6.1038922	192.168.121.128	150.244.214.237	TCP	54	2805 → 80 [SYN] Seq=0 Win=512 Len=0
2805	8.1047237	192.168.121.128	150.244.214.237	TCP	54	2805 → 80 [RST] Seq=1 Win=0 Len=0
2806	10.2039944	192.168.121.128	150.244.214.237	TCP	54	2806 → 80 [SYN] Seq=0 Win=512 Len=0
2806	12.2049624	192.168.121.128	150.244.214.237	TCP	54	2806 → 80 [RST] Seq=1 Win=0 Len=0
2807	13.3049966	192.168.121.128	150.244.214.237	TCP	54	2807 → 80 [SYN] Seq=0 Win=512 Len=0
2807	15.3048881	192.168.121.128	150.244.214.237	TCP	54	2807 → 80 [RST] Seq=1 Win=0 Len=0
2808	16.4042297	192.168.121.128	150.244.214.237	TCP	54	2808 → 80 [SYN] Seq=0 Win=512 Len=0
2808	18.4050159	192.168.121.128	150.244.214.237	TCP	54	2808 → 80 [RST] Seq=1 Win=0 Len=0
2809	19.5043580	192.168.121.128	150.244.214.237	TCP	54	2809 → 80 [SYN] Seq=0 Win=512 Len=0
2809	21.5052527	192.168.121.128	150.244.214.237	TCP	54	2809 → 80 [RST] Seq=1 Win=0 Len=0
2810	22.6044659	192.168.121.128	150.244.214.237	TCP	54	2810 → 80 [SYN] Seq=0 Win=512 Len=0
2810	24.6055162	192.168.121.128	150.244.214.237	TCP	54	2810 → 80 [RST] Seq=1 Win=0 Len=0
2811	25.7045179	192.168.121.128	150.244.214.237	TCP	54	2811 → 80 [SYN] Seq=0 Win=512 Len=0
2811	27.7052028	192.168.121.128	150.244.214.237	TCP	54	2811 → 80 [RST] Seq=1 Win=0 Len=0
2812	28.8045858	192.168.121.128	150.244.214.237	TCP	54	2812 → 80 [SYN] Seq=0 Win=512 Len=0
2812	30.8054448	192.168.121.128	150.244.214.237	TCP	54	2812 → 80 [RST] Seq=1 Win=0 Len=0
29946	1.0000000	192.168.121.128	192.168.121.2	DNS	70	Standard query 0xdc7 A 150.244.214.237
53	2.0000000	192.168.121.128	192.168.121.2	DNS	86	Standard query response 0xdc7 A 150.244.214.237
57021	9.2028481	192.168.121.1	192.168.121.255	UDP	86	Source port: 57621 Destination port: 57621
80	4.054354	150.244.214.237	192.168.121.128	TCP	60	80 → 2804 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80	7.1047171	150.244.214.237	192.168.121.128	TCP	60	80 → 2805 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80	11.2049545	150.244.214.237	192.168.121.128	TCP	60	80 → 2806 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80	14.3048723	150.244.214.237	192.168.121.128	TCP	60	80 → 2807 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80	17.4050088	150.244.214.237	192.168.121.128	TCP	60	80 → 2808 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80	20.5052460	150.244.214.237	192.168.121.128	TCP	60	80 → 2809 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80	23.6055072	150.244.214.237	192.168.121.128	TCP	60	80 → 2810 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80	26.7052623	150.244.214.237	192.168.121.128	TCP	60	80 → 2811 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
80	29.8054373	150.244.214.237	192.168.121.128	TCP	60	80 → 2812 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Frame 2: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)

Ethernet II, Src: 00:50:56:f5:02:32 (00:50:56:f5:02:32), Dst: 00:0c:29:d1:c2:36 (00:0c:29:d1:c2:36)

Internet Protocol Version 4, Src: 192.168.121.2 (192.168.121.2), Dst: 192.168.121.128 (192.168.121.128)

User Datagram Protocol, Src Port: 53 (53), Dst Port: 29946 (29946)

Domain Name System (response)

0000 00 0c 29 d1 c2 36 00 50 56 f5 02 32 08 00 45 006.P.V..2..E.
0010 00 48 33 3e 00 00 11 93 93 c0 a8 79 02 c0 a8 ..H3>....y...
0020 79 00 00 35 74 fa 00 34 34 e6 dc e7 81 00 00 01 y..5t..4 4.....
0030 00 01 00 00 00 03 77 77 77 83 75 61 6d 02 65W ww.uam.e

File: /home/lubuntu/Desktop/... Packets: 30 - Displayed: 30 (100,0%) - Load time: 0:00.000

Profile: Default

2) El filtro utilizado es `ip and ip.len > 1000`. Una vez aplicado el filtro, se puede guardar la captura de manera normal, y se almacenaran solo los paquetes que cumplen los requisitos del filtro.

Para la comparación de tamaño entre el paquete IP y su protocolo, adjuntamos la siguiente captura, en la que se puede observar que existe una diferencia de 14 Bytes entre ambos tamaños. Esto se cumple también en el resto de paquetes IP.

The screenshot shows the Wireshark 1.10.6 interface. The filter bar at the top contains the expression `ip and ip.len > 1000`. The packet list pane shows a series of TCP segments, all with a length of 1514 bytes. The packet details pane for the selected packet (Frame 23) shows the following structure:

- Frame 23: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
- Ethernet II, Src: 00:50:56:f9:78:41 (00:50:56:f9:78:41), Dst: 00:0c:29:7c:d0:46 (00:0c:29:7c:d0:46)
- Internet Protocol Version 4, Src: 150.244.214.237 (150.244.214.237), Dst: 192.168.182.129 (192.168.182.129)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 - Total Length: 1500
 - Identification: 0x2262 (8802)
 - Flags: 0x00
 - Fragment offset: 0
 - Time to live: 128

The packet bytes pane shows the raw data of the packet, starting with the Ethernet II header and the IP header.

3) Para añadir la nueva columna, vamos al menú 'Edit'->'Preferences'. Una vez ahí, entramos en 'User Interface'->'Columns', y creamos una nueva columna dándole a 'Añadir'. El nombre será interarrival, y el tipo de campo será 'Delta Time'. Adjuntamos captura de pantalla con la columna añadida.

The screenshot shows the Wireshark 1.10.6 interface. The packet list table at the top displays a series of TCP segments from source 150.244.214.237 to destination 192.168.182.129. A new column, 'interarrival', has been added to the table, showing the time interval between each packet. The packet details pane for packet 23 shows the following structure:

- Frame 23: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
- Ethernet II, Src: 00:50:56:f9:78:41 (00:50:56:f9:78:41), Dst: 00:0c:29:7c:d0:46 (00:0c:29:7c:d0:46)
- Internet Protocol Version 4, Src: 150.244.214.237 (150.244.214.237), Dst: 192.168.182.129 (192.168.182.129)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 - Total Length: 1500
 - Identification: 0x2262 (8802)
 - Flags: 0x00
 - Fragment offset: 0
 - Time to live: 128

The packet bytes pane at the bottom shows the raw data of the packet, including the Ethernet II header, IP header, and TCP header.

4) Entrando en Preferences, editamos la columna de Time, y cambiamos su tipo a Absolute date and time, quedando la columna como se ve reflejado en la siguiente diapositiva

The screenshot displays the Wireshark 1.10.6 interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The filter bar shows the filter 'ip and ip.len > 1000'. The packet list table is populated with 20 packets, all of which are TCP segments from 150.244.214.237 to 192.168.182.129. The packet details pane for packet 23 shows the following structure:

- Ethernet II, Src: 00:50:56:f9:78:41 (00:50:56:f9:78:41), Dst: 00:0c:29:7c:d0:46 (00:0c:29:7c:d0:46)
- Internet Protocol Version 4, Src: 150.244.214.237 (150.244.214.237), Dst: 192.168.182.129 (192.168.182.129)
- Version: 4
- Header Length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 1500
- Identification: 0x2262 (8802)
- Flags: 0x00
- Fragment offset: 0
- Time to live: 128

The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates 'Ready to load or capture', 'Packets: 6934 · Displayed: 2803 (40,4%) · Dropped: 0 (0,0%) · Load time: 0:00.128', and 'Profile: Default'.

5) Introducimos el filtro udp e iniciamos la captura. Una vez finalizada, comprobamos que los únicos paquetes capturados son los que aparecen en la siguiente captura.

The screenshot shows the Wireshark 1.10.6 interface. The filter bar at the top is set to 'udp'. The packet list shows two captured packets, both DNS. The selected packet (No. 2) is a UDP response from 192.168.182.129 to 192.168.182.2. The packet details pane shows the Ethernet II header, Internet Protocol Version 4 header, and the selected UDP protocol (17). The packet bytes pane shows the raw data in hexadecimal and ASCII.

Pk	No.	Time	Source	Destination	Protocol	Length	Info
32283	1	2018-09-21 14:51:39.015434000	192.168.182.129	192.168.182.2	DNS	70	53 Standard query 0xcfc A www.uam 0.000000000
53	2	2018-09-21 14:51:39.015906000	192.168.182.2	192.168.182.129	DNS	86	32283 Standard query response 0xcfc , 0.000472000

Packet details for the selected packet (No. 2):

- Ethernet II, Src: 00:0c:29:7c:d0:46 (00:0c:29:7c:d0:46), Dst: 00:50:56:f9:78:41 (00:50:56:f9:78:41)
- Internet Protocol Version 4, Src: 192.168.182.129 (192.168.182.129), Dst: 192.168.182.2 (192.168.182.2)
- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
- Total Length: 56
- Identification: 0x231c (8988)
- Flags: 0x02 (Don't Fragment)
- Fragment offset: 0
- Time to live: 64
- Protocol: UDP (17)

Packet bytes (hex/ascii):

```
0000 00 50 56 f9 78 41 00 0c 29 7c d0 46 08 00 45 00 .PV.xA..)|.F..E.
0010 00 38 23 1c 40 00 40 11 29 c4 c0 a8 b6 81 c0 a8 .8#.@.@.).....
0020 b6 02 7e 1b 00 35 00 24 6d ea cf 5c 01 00 00 01 ..~..5.$ m.\....
0030 00 00 00 00 00 00 03 77 77 77 03 75 61 6d 02 65 .....w ww.uam.e
0040 73 00 00 01 00 01 S.....
```