

Nombres: Jesús Rodríguez Heras, Juan Pedro Rodríguez Gracia y Gabriel Fernando Sánchez Reina.

## Práctica 9: Wireshark

1.) Al lanzar el comando ping a “google.es” podemos ver como en wireshark se muestran paquetes ICMP desde la máquina que lanza el ping hasta el servidor y la respuesta del servidor a la máquina.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The status bar at the top indicates the capture is running on 'wlan0' and shows the current time as 'jue, 17 de may, 17:03'. The packet list pane shows a series of ICMP Echo (ping) requests and replies. The packet details pane for the selected packet (No. 54) shows the following structure:

- Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: Cisco\_f5:22:20 (18:e7:28:f5:22:20), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (reply/gratuitous ARP)

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 ff ff ff ff ff 18 e7 28 f5 22 20 08 06 00 01 ..... (." ....
0010 08 00 06 04 00 02 00 cd fe d6 61 1d 0a b6 6e 98 ..... ..a...n.
0020 00 cd fe d6 61 1d 0a b6 6e 98 .....a...n.
```

En cuanto a los filtros, podemos filtrar por IP, por MAC, por protocolo de red utilizado, etc. Incluso tenemos una opción que nos permite descifrar el nombre del origen/destino de la conexión.

2.) Vamos a realizar este ejercicio con nuestros equipos lanzando un ping a “google.es”.

a) Según el campo “Opcode”, mediante el cual se puede saber si es una petición o una respuesta en función del número que sea (1=petición, 2=respuesta).

b) La IP de la puerta de enlace es: 10.182.1.1 y su MAC es: C0:25:5C:AC:A3:20.

c) La está suministrando la propia puerta de enlace.

d) Utilizando la herramienta Nmap o con el propio Wireshark podemos lanzar una petición de respuesta a un comando ping y saber la dirección de las posibles víctimas que tenemos en la red.

e) Con el comando “wireshark fichero\_recogida.pcapng” podemos abrirlo con wireshark.