

# Wireshark Captura

## Protocolo 802.11

### Contenido

Introducción.....	2
Lectura de paquetes.....	2
Paquete 1.....	2
Paquete 10.....	3
Paquete 270.....	3
Atacar utilizando el archivo .pcap.....	5

## Introducción.

Debido a que mi tarjeta de red no puede cambiar a modo monitor, el profesor me ha indicado un fichero .pcap a analizar.

En este caso, la intención es ampliar y conocer un poco más a fondo como funciona el protocolo Wi-Fi.

## Lectura de paquetes.

The screenshot shows the Wireshark interface with the file 'investigation.pcap' open. The packet list on the left shows 16 packets. The first packet (No. 1) is selected, and its details are expanded in the right pane. The details pane shows the following information:

- Supported Rates: 24 (0x30), 36 (0x48), 54 (0x6c)
- Tag: DS Parameter set: Current Channel: 2
- Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
- Tag: ERP Information
- Tag: Vendor Specific: Microsoft Corp.: WPS
- Tag: Vendor Specific: Broadcom

The status bar at the bottom indicates: 'Barker Preamble Mode (wlan.er...barker\_preamble\_mode), 1 byte | Packets: 133068 - Displayed: 133068 (100.0%) | Profile: Default'

### Paquete 1.

Su tipo de encapsulado es IEEE 802.11 Wireless LAN (WLAN) capturado el 17 de septiembre de 2010 a las 15:56:41.085 UTC, con una longitud de fragmento de 105 bytes (840 bits). El destinatario

Joaquim Chagas Neto CCIEX

es Broadcast y la dirección de origen proviene de CiscoLinksys\_61:00:d0.

La BSSID corresponde a la de CiscoLinksys\_61:00:d0.

El SSID se corresponde con "Ment0rNet", con un soporte para 1, 2, 5.5, 11, 18, 24, 36, 54 Mbit/seg. Utiliza el canal 2 para comunicarse.

Además, el ERP no se encuentra definido.

En Tag Vendor Specific vemos que menciona a Microsoft Corp. WPS y el tipo WPS, por lo que deducimos que es un Wifi Protected Setup, pero más abajo nos indica que no está configurado.

#### Paquete 10.

En este paquete veo un request por parte de SenaoInterna\_33:a9:55 con el subtipo: Request-to-send.

En sus flags encontramos el DS Status que nos indica que la red puede estar utilizando el modo AD-HOC y que la data no está protegida.

#### Paquete 270.

En el apartado info veo un Probe Response. Analizando un poco veo la dirección del receptor, destinatario y el transmisor, respectivamente, CIMSYS\_33:44:55, CIMSYS\_33:44:55 y CiscoLinksys\_61:00:d0.

En los parámetros podemos observar de nuevo la SSID "Ment0rNet" en el canal 2 con el ERP no definido y el WPS no configurado.

Pero en este caso nos aporta más información que en los otros paquetes; su UUID E, manufacturer, model name, model number, serial number, primary device type y el nombre del dispositivo.

- ❖ El UUID Enrollee es 138140001dd211b29fffc67e816b4bfb.
- ❖ El Manufacturer Linksys.
- ❖ El nombre del modelo Router.
- ❖ El número del modelo WRT54G2.

Joaquim Chagas Neto CCIEX

- ❖ El serial number CSV01J334883.
- ❖ El tipo de dispositivo nos indica la categoría de Network Infrastructure.
- ❖ El nombre del dispositivo es Wireless-G Router.
- ❖ El Vendedor es Broadcom.

The screenshot shows the Wireshark interface with a packet capture of a Probe Response. The packet list shows a 211-byte Probe Response (SN=3804) from CIMSYS\_33:44:55. The packet details pane shows the IEEE 802.11 frame structure, including the MAC address CIMSYS\_33:44:55, the SSID 'SenaoInterna\_33:a9:...', and the Vendor Specific Element (VSE) containing the device information.

No.	Time	Source	Destination	Protocol	Length	Info
264	2010-09-17 15:57:01.486640	S...	SenaoInterna_33:a9:...	802.11	16	Request-to-send, Flags=...
265	2010-09-17 15:57:01.494896	C...	CIMSYS_33:44:55	802.11	211	Probe Response, SN=3801, FM...
266	2010-09-17 15:57:01.527601	S...	SenaoInterna_33:a9:...	802.11	10	Acknowledgement, Flags=...
267	2010-09-17 15:57:01.574704	S...	SenaoInterna_33:a9:...	802.11	10	Acknowledgement, Flags=...
268	2010-09-17 15:57:01.621293	S...	SenaoInterna_33:a9:...	802.11	10	Acknowledgement, Flags=...
269	2010-09-17 15:57:01.642289	S...	SenaoInterna_33:a9:...	802.11	10	Acknowledgement, Flags=...
270	2010-09-17 15:57:01.683314	C...	CIMSYS_33:44:55	802.11	211	Probe Response, SN=3804, FM...
271	2010-09-17 15:57:01.683311	C...	CiscoLinksys_61:00:...	802.11	10	Acknowledgement, Flags=...
272	2010-09-17 15:57:01.712496	C...	CiscoLinksys_61:00:...	802.11	30	Authentication, SN=3, FN=0,
273	2010-09-17 15:57:01.712498	C...	CIMSYS_33:44:55 (00...	802.11	10	Acknowledgement, Flags=...
274	2010-09-17 15:57:01.713009	C...	CIMSYS_33:44:55	802.11	41	Authentication, SN=3805, FM...
275	2010-09-17 15:57:01.713521	C...	CiscoLinksys_61:00:...	802.11	10	Acknowledgement, Flags=...
276	2010-09-17 15:57:01.715569	C...	CiscoLinksys_61:00:...	802.11	55	Association Request, SN=4,
277	2010-09-17 15:57:01.715570	C...	CIMSYS_33:44:55 (00...	802.11	10	Acknowledgement, Flags=...
278	2010-09-17 15:57:01.716593	C...	CIMSYS_33:44:55	802.11	57	Association Response, SN=38...
279	2010-09-17 15:57:01.716594	C...	CiscoLinksys_61:00:...	802.11	10	Acknowledgement, Flags=...

Packet 270 details:

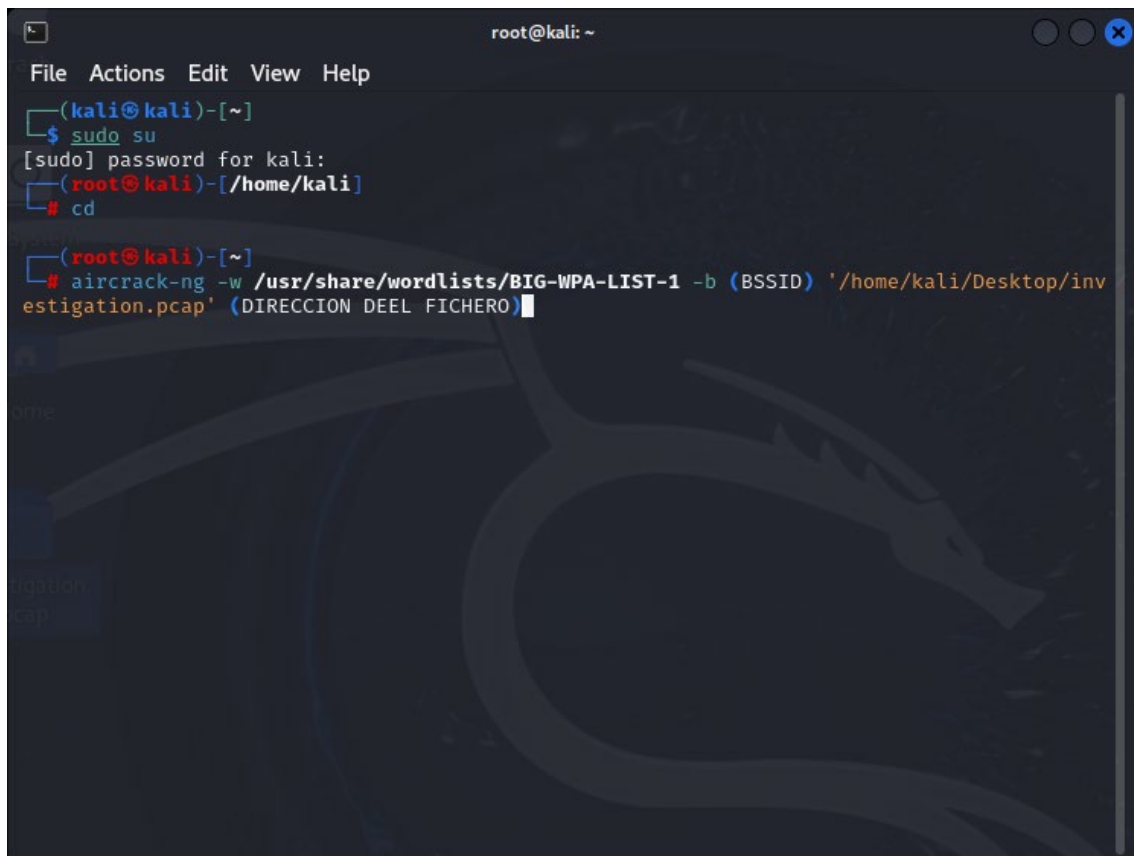
- Data Element Type: UUID E (0x1047)
- Data Element Length: 16
- UUID Enrollee: 138140001dd211b29fffc67e816b4bfb
- Manufacturer: Linksys
  - Data Element Type: Manufacturer (0x1021)
  - Data Element Length: 7
  - Manufacturer: Linksys
- Model Name: Router
  - Data Element Type: Model Name (0x1023)
  - Data Element Length: 6
  - Model Name: Router
- Model Number: WRT54G2
  - Data Element Type: Model Number (0x1024)
  - Data Element Length: 7
  - Model Number: WRT54G2
- Serial Number: CSV01J334883
  - Data Element Type: Serial Number (0x1042)
  - Data Element Length: 12
  - Serial Number: CSV01J334883
- Primary Device Type
  - Data Element Type: Primary Device Type (0x1054)
  - Data Element Length: 8
  - Primary Device Type: 00060050f2040001
  - Category: Network Infrastructure (0x00006)
  - Subcategory: AP (0x00001)
- Device Name: Wireless-G Router
  - Data Element Type: Device Name (0x1011)
  - Data Element Length: 17

Text item (text), 12 bytes | Packets: 133068 · Displayed: 133068 (100.0%) | Profile: Default

## Atacar utilizando el archivo .pcap.

Para ello simplemente necesitaremos la suite de aircrack-ng, el BSSID o MAC de la red en cuestión y el archivo .pcap.

Ejecutamos aircrack-ng con los parámetros -w /usr/share/wordlists/ y -b que corresponde con el BSSID a atacar junto con el fichero .pcap.

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the following commands and output:

```
(kali@kali)~[~]  
$ sudo su  
[sudo] password for kali:  
(root@kali)~[/home/kali]  
# cd  
  
(root@kali)~[~]  
# aircrack-ng -w /usr/share/wordlists/BIG-WPA-LIST-1 -b (BSSID) '/home/kali/Desktop/investigation.pcap' (DIRECCION DEEL FICHERO)
```

The terminal background features a faint, stylized dragon logo, which is the Kali Linux logo. The cursor is at the end of the last command line.