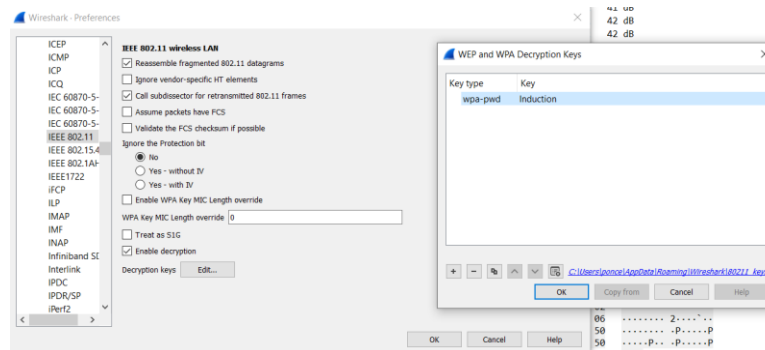


## Redes de área local inalámbricas (WLAN)

### • Ejercicio 1

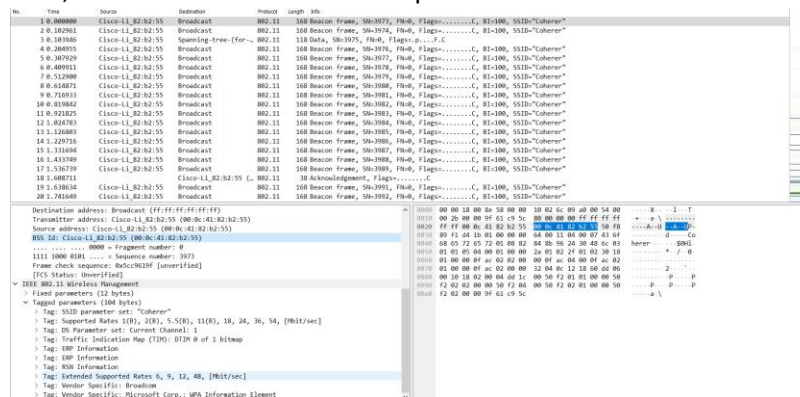
1. Descifra el contenido de las tramas capturadas a nivel IEEE 802.11 para visualizar su contenido.

En Wireshark, arriba en la pestaña **Edit-Preferences-Protocol-IEEE 802.11-Decryption keys** e introduciendo la clave *Induction* junto al tipo *wpa-pwd* podremos descifrar el contenido de las tramas.



2. No sabemos cuál es el SSID de la red donde se ha capturado el tráfico. ¿Cómo podríamos obtenerla?

Pinchando en una trama cualquiera, dentro de **IEEE 802.11 Wireless Management** podemos encontrar el SSID, tal como se muestra en la captura.



3. ¿A qué página web se está accediendo? ¿desde qué página se navega hasta llegar a ella?

Analizando el flujo TCP podemos conocer a qué página web se está accediendo.

Para esta primera captura observamos como se está enviando una petición a Wikipedia desde un navegador Mozilla Firefox y desde el buscador de Google, entre otras cosas.

```
GET /wiki/Landshark HTTP/1.1
Host: en.wikipedia.org
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.9) Gecko/20061206 Firefox/1.5.0.9
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png;*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.google.com/search?q=%22land+shark%22+candygram&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-US:official
```

Para cargar la página, es necesario además de cargar una imagen PNG. Por tanto, hacemos otra petición.

```
GET /fundraising/2006/meter.png HTTP/1.1
Host: upload.wikimedia.org
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.9) Gecko/20061206 Firefox/1.5.0.9
Accept: image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://en.wikipedia.org/wiki/Landshark
If-Modified-Since: Thu, 04 Jan 2007 04:40:01 GMT
If-None-Match: "5604440072312281207"
```

Tenemos una segunda conexión hacia una página web *snltranscripts.jt.org*.

```
GET /75/75daws2.phtml HTTP/1.1
Host: snltranscripts.jt.org
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.9) Gecko/20061206 Firefox/1.5.0.9
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.google.com/search?q=%22land+shark%22+candygram&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-US:official
```

Al acceder a la página, solicita cargar otra imagen y un anuncio:

```
GET /75/pics/75daws1.jpg HTTP/1.1
Host: snltranscripts.jt.org
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.9) Gecko/20061206 Firefox/1.5.0.9
Accept: image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://snltranscripts.jt.org/75/75daws2.phtml
Cookie: TRACKID=56d0e6a0999ed88037ba41b9e6830c78
```

### Imagen

```
GET /pagead/ads?client=ca-pub-9011062396508188&dt=1167891175069&mt=1167891174&format=728x90_as&output=html&channel=8345570081&url=http%3A%2F%2Fsnltranscripts.jt.org%2F75%2F75daws2.phtml&color_bg=C0C0C0&color_text=000000&color_link=666666&color_url=3366FF&color_border=999999&ad_type=text_image&ref=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3D%2522land%2Bshark%2522%2Bcandygram%26start%3D0%26ie%3Dutf-8%26oe%3Dutf-8%26client%3Dfirefox-a%26rls%3Dorg.mozilla%3Aen-US%3Aofficial&cc=100&u_h=900&u_w=1440&u_ah=825&u_au=1440&u_cd=32&u_tz=-480&u_his=2&u_java=true&u_nplug=9&u_rmime=103 HTTP/1.1
Host: pagead2.googlesyndication.com
User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.9) Gecko/20061206 Firefox/1.5.0.9
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://snltranscripts.jt.org/75/75daws2.phtml
```

### Anuncio

## 4. ¿Qué tasa de transferencia hemos obtenido en la descarga del contenido de la web? ¿Qué versión de Wi-Fi se está empleando?

778.26.239523	192.168.0.50	209.180.21.200	HTTP	802.11	/75/75daws2.phtml HTTP
786.26.110592	209.180.21.200	192.168.0.50	HTTP	576	[TCP Previous segment not found]
786.26.110592	209.180.21.200	192.168.0.50	HTTP	583	[TCP Previous segment not found]
792.26.575556	192.168.0.50	209.180.21.200	HTTP	583	GET /style.css HTTP/1.1
800.26.618552	209.180.21.200	192.168.0.50	HTTP	809	HTTP/1.1 200 OK (text/css)
810.26.719455	192.168.0.50	209.180.21.200	HTTP	500	GET /75space2.gif HTTP/1.1
820.26.772434	209.180.21.200	192.168.0.50	HTTP	1151	HTTP/1.1 200 OK (GIF89a)
823.26.773438	192.168.0.50	209.180.21.200	HTTP	595	GET /75/pics/75daws1.jpg HTTP/1.1
832.26.789429	192.168.0.50	209.180.21.200	HTTP	595	GET /75/pics/75daws1.jpg HTTP/1.1
840.26.184843	192.168.0.50	209.180.21.200	HTTP	692	[TCP ACKed unseen segment]
857.26.855414	192.168.0.50	209.180.21.200	HTTP	583	[TCP ACKed unseen segment]
868.26.878523	192.168.0.50	72.14.255.99	HTTP	1174	GET /pagead/ads?client=ca-pub-9011062396508188&dt=1167891175069&mt=1167891174&format=728x90_as&output=html&channel=8345570081&url=http%3A%2F%2Fsnltranscripts.jt.org%2F75%2F75daws2.phtml&color_bg=C0C0C0&color_text=000000&color_link=666666&color_url=3366FF&color_border=999999&ad_type=text_image&ref=http%3A%2F%2Fwww.google.com%2Fsearch%3Fq%3D%2522land%2Bshark%2522%2Bcandygram%26start%3D0%26ie%3Dutf-8%26oe%3Dutf-8%26client%3Dfirefox-a%26rls%3Dorg.mozilla%3Aen-US%3Aofficial&cc=100&u_h=900&u_w=1440&u_ah=825&u_au=1440&u_cd=32&u_tz=-480&u_his=2&u_java=true&u_nplug=9&u_rmime=103 HTTP/1.1
870.26.892400	209.180.21.200	192.168.0.50	HTTP	1009	HTTP/1.1 200 OK (JPEG 3F1F)
880.26.825801	192.168.0.50	209.180.21.200	HTTP	852	[TCP ACKed unseen segment]
892.26.493111	209.180.21.200	192.168.0.50	HTTP/1.1	607	[TCP ACKed unseen segment]

Frame 868: 1174 bytes on wire (9392 bits), 1174 bytes captured (9392 bits) on interface unknown, id 6

> Radiotap Header v0, Length 24

> 802.11 radio information

PHY type: 802.11g (ERP) (6)

Proprietary mode: None (0)

Data rate: 54.0 Mb/s

Channel: 1

Frequency: 2412MHz

Signal strength (dB): 56 dB

> [Duration: 192us]

Tanto para la página web de Wikipedia como para *snltranscripts.jt.org*, la tasa es de 54 Mb/s y la versión Wi-Fi es 802.11g.

Toda la información se puede encontrar dentro de cada una de las tramas, es la pestaña *802.11 radio information*.

- Ejercicio 2

Añade las columnas necesarias para contestar rápidamente a las siguientes preguntas.

No.	Time	Source	Destination	Protocol	Length	Info	Tx rate	Channel	Frequency	Signal
1	0.000000	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	48.0	11	2462MHz	-37 dBm
2	0.000021	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	36.0	11	2462MHz	-75 dBm
3	1.002244	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	48.0	11	2462MHz	-37 dBm
4	1.003213	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	36.0	11	2462MHz	-74 dBm
5	2.000228	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	48.0	11	2462MHz	-36 dBm
6	2.000613	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	36.0	11	2462MHz	-75 dBm
7	3.007252	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	48.0	11	2462MHz	-36 dBm
8	3.008426	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	36.0	11	2462MHz	-74 dBm
9	11.649223	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	54.0	11	2462MHz	-35 dBm
10	11.653444	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	36.0	11	2462MHz	-77 dBm
11	11.657923	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	54.0	11	2462MHz	-35 dBm
12	11.657964	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	36.0	11	2462MHz	-76 dBm
13	11.659015	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	54.0	11	2462MHz	-34 dBm
14	11.659073	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	54.0	11	2462MHz	-37 dBm
15	11.659289	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	36.0	11	2462MHz	-76 dBm
16	11.659289	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	36.0	11	2462MHz	-76 dBm
17	11.659336	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	24.0	11	2462MHz	-75 dBm
18	11.712296	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	54.0	11	2462MHz	-28 dBm
19	11.712425	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	48.0	11	2462MHz	-28 dBm
20	11.713115	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	2.0	11	2462MHz	-76 dBm
21	11.713438	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	54.0	11	2462MHz	-32 dBm
22	11.713787	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	48.0	11	2462MHz	-31 dBm
23	11.713112	192.168.0.106	192.168.0.1	ICMP	128	Echo (ping) request	36.0	11	2462MHz	-33 dBm

5. ¿Cuál es la señal recibida más baja? (RSSI)

Es la de la trama 337 con un valor de -98 dBm.

No.	Time	Source	Destination	Protocol	Length	Info	Tx rate	Channel	Frequency	Signal
337	438.725511	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	1.0	11	2462MHz	-98 dBm
772	491.549517	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	1.0	11	2462MHz	-95 dBm
773	491.549398	192.168.0.1	192.168.0.106	ICMP	128	Echo (ping) reply	1.0	11	2462MHz	-95 dBm

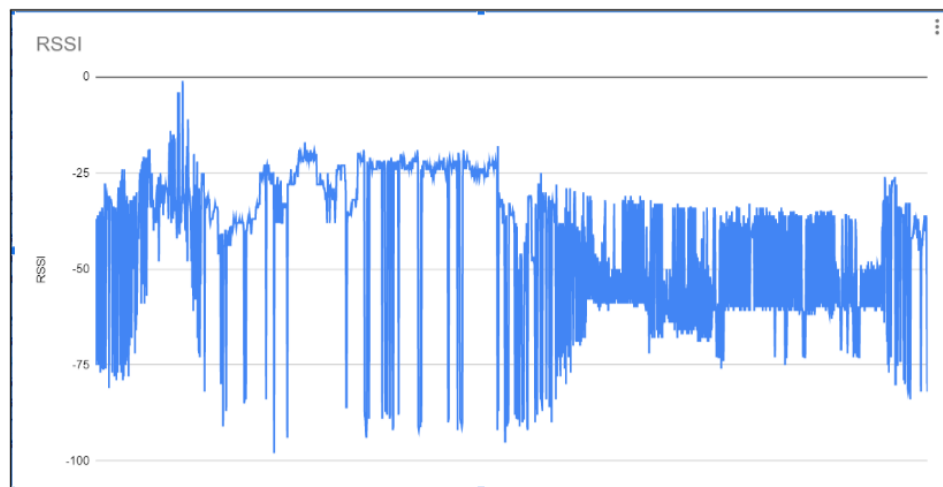
6. ¿Qué canal está usando? ¿A qué frecuencia se corresponde?

Está usando el canal 11 con una frecuencia de 2462 MHz.

7. ¿Hay cambio de canal? ¿Por qué crees que se cambia a ese o esos canales?

En la trama 332 se produce un cambio de canal al 6 debido a interferencias que se encuentran en la banda de los 2.4 GHz.

8. Representa con una gráfica en Excel evolución temporal de la señal.



- **Ejercicio 3**

**9. ¿Qué tipo de tráfico contiene la traza?**

La traza contiene en su gran mayoría tramas de gestión, en especial del tipo Beacon, Probe Request y Probe Response.

[illegible]

**10. ¿Cuál es el problema? Señala las tramas afectadas y cuándo ocurre.**

Tenemos problemas con alguna de las tramas que presentan pérdida de información y algunas corruptas con errores del tipo Malformed Packet.

The screenshot displays the Wireshark interface with packet 6 selected. The left pane shows the packet list and details. The right pane shows the raw packet data in hexadecimal and ASCII. A red box highlights the error message: "Malformed Packet: 1024.000.0.0: length of contained line exceeds length of containing line". Below this, the raw data is shown in hexadecimal and ASCII, with a group of bytes highlighted as "Malformed".

**11. En base a los parámetros estudiados en los ejercicios anteriores, ¿a qué puede deberse?**

Se debe al RSSI. Es decir, la potencia de la señal es lo suficientemente baja como para que se produzcan caídas y cortes en la comunicación.