

Redes Inalámbricas

Práctica con WhireShark I

Antonio J. Galán Herrera



Wireshark

Índice

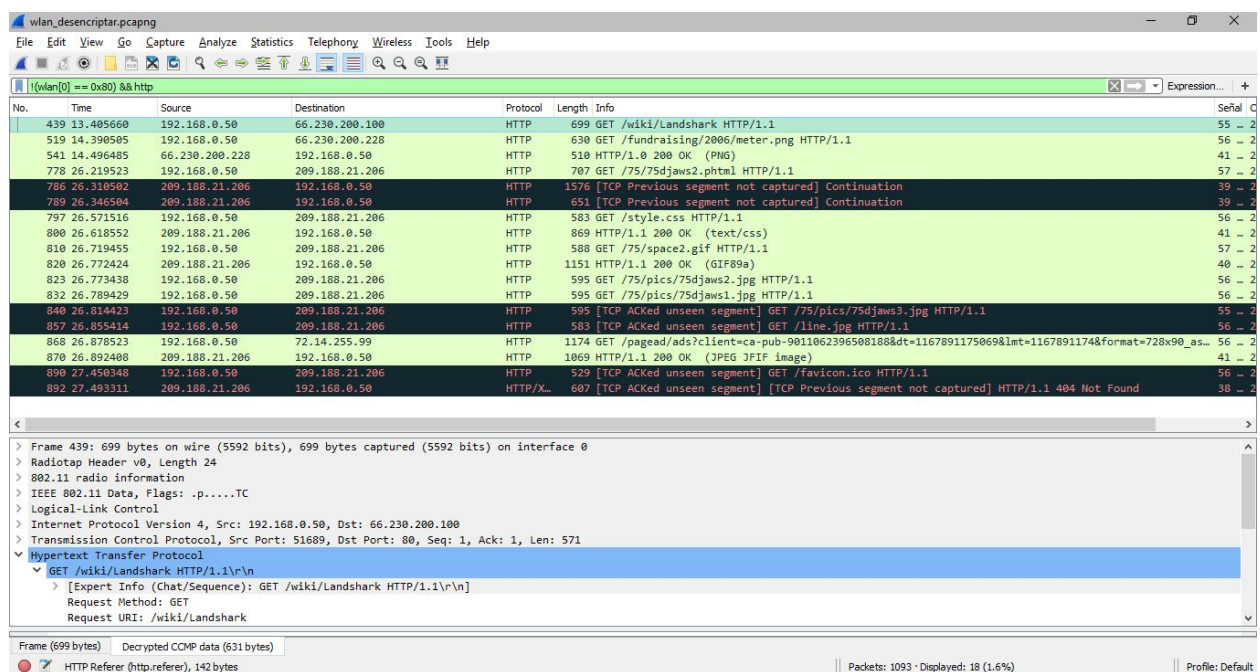
Quiz 1	2
Quiz 2	4
Quiz 3	6

Quiz 1

Desencripta el contenido de la traza [wlan_desencriptar.pcapng](#) usando la contraseña *Induction* y el SSID *Coherer* para saber a qué página web se está accediendo.

Para este ejercicio, se ha empleado el filtro `!(wlan[0] == 0x80) && http`, el primero para omitir los Beacons y el segundo para mostrar tramas del protocolo HTTP, ofreciendo una información mucho más concreta.

En esta imagen, se muestra la trama (430) que se ha usado para obtener la URL.



Y aquí, una vez abierta la trama, la localización de la información requerida.

The image shows a Wireshark packet capture window titled 'wlan_descriptar.pcapng'. The packet list on the left shows two packets. Packet 439 is selected, showing details of an HTTP GET request. The 'Hypertext Transfer Protocol' section is expanded, showing the request method (GET), URI (/wiki/Landshark), and version (HTTP/1.1). The 'Referer' field is highlighted, showing the URL: http://www.google.com/search?q=x22land+sharkx22+candygram&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-US:official. Annotations with arrows point to the 'Referer' field, indicating the page the user came from (Google), and the 'Full request URI' field, indicating the page the user is accessing (Wikipedia).

No.	Time	Source	Destination	Protocol	Length	Info
439	13.485660	192.168.0.50	66.230.200.100	HTTP	699	GET /wiki/Landshark HTTP/1.1
519	14.390505	192.168.0.50	66.230.200.228	HTTP	630	GET /fundraising/2006/meter.png HTTP/1.1

Frame 439: 699 bytes on wire (5592 bits), 699 bytes captured (5592 bits) on interface 0

Radiotap Header v0, Length 24

802.11 radio information

IEEE 802.11 Data, Flags: .p.....TC

Logical-Link Control

Internet Protocol Version 4, Src: 192.168.0.50, Dst: 66.230.200.100

Transmission Control Protocol, Src Port: 51689, Dst Port: 80, Seq: 1, Ack: 1, Len: 571

Hypertext Transfer Protocol

GET /wiki/Landshark HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /wiki/Landshark HTTP/1.1\r\n]

Request Method: GET

Request URI: /wiki/Landshark

Request Version: HTTP/1.1

Host: en.wikipedia.org\r\n

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\r\n

Accept: text/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5\r\n

Accept-Language: en-us,en;q=0.5\r\n

Accept-Encoding: gzip,deflate\r\n

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

Referer: http://www.google.com/search?q=x22land+sharkx22+candygram&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-US:official\r\n

[Full request URI: http://en.wikipedia.org/wiki/Landshark]

[HTTP request 1/1]

01e0 61 6c 69 76 65 0d 0a 52 65 66 65 72 65 72 3a 26 alive R eferer:
01f0 60 74 7a 70 38 2f 21 77 77 77 2e 67 61 6f 67 6d http://w ww.googl
0200 65 2e 63 6f 6d 2f 73 65 61 72 63 68 3f 71 3d 25 s.com/se arch?q=x
0210 32 32 6c 61 6e 64 2b 73 68 61 72 6b 25 32 32 2b 22land+s harkx22+

Frame (699 bytes) Decrypted COMP data (631 bytes)

HTTP Referer (http:referer), 142 bytes

Packets: 1093 · Displayed: 18 (1.6%)

Profile: Default

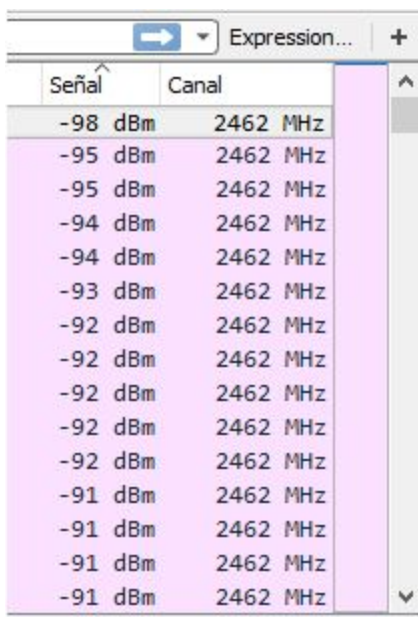
Quiz 2

Añade las columnas necesarias en la traza [wlan_signal.pcapng](#) y responde a las siguientes preguntas:

1. ¿Cuál es la señal recibida más baja?
2. Representa la evolución de la señal con una gráfica.
3. ¿Cuál es el canal que se está usando?
4. ¿Se produce algún cambio de canal?

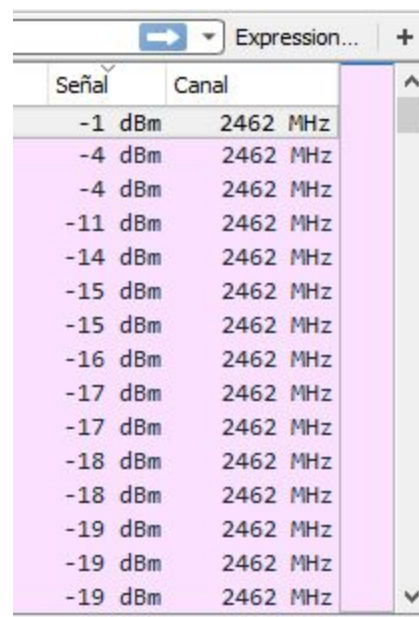
1. La señal más baja que está usando es de -98 dBm, y la mayor es -1 dBm.

Filas ordenadas de menor a mayor señal.



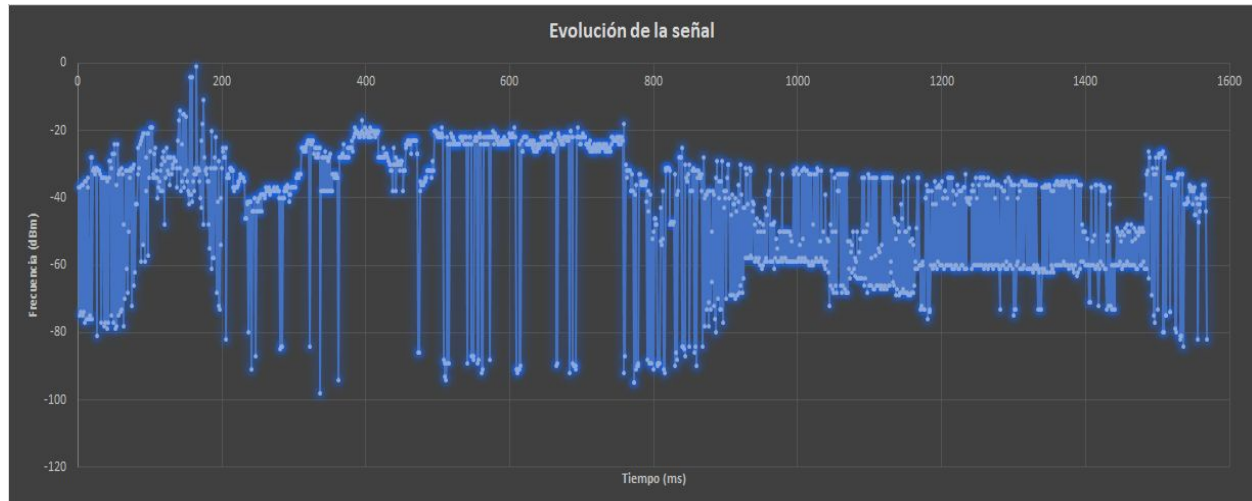
Señal	Canal
-98 dBm	2462 MHz
-95 dBm	2462 MHz
-95 dBm	2462 MHz
-94 dBm	2462 MHz
-94 dBm	2462 MHz
-93 dBm	2462 MHz
-92 dBm	2462 MHz
-92 dBm	2462 MHz
-92 dBm	2462 MHz
-92 dBm	2462 MHz
-92 dBm	2462 MHz
-91 dBm	2462 MHz
-91 dBm	2462 MHz
-91 dBm	2462 MHz
-91 dBm	2462 MHz

Filas ordenadas de mayor a menor señal.

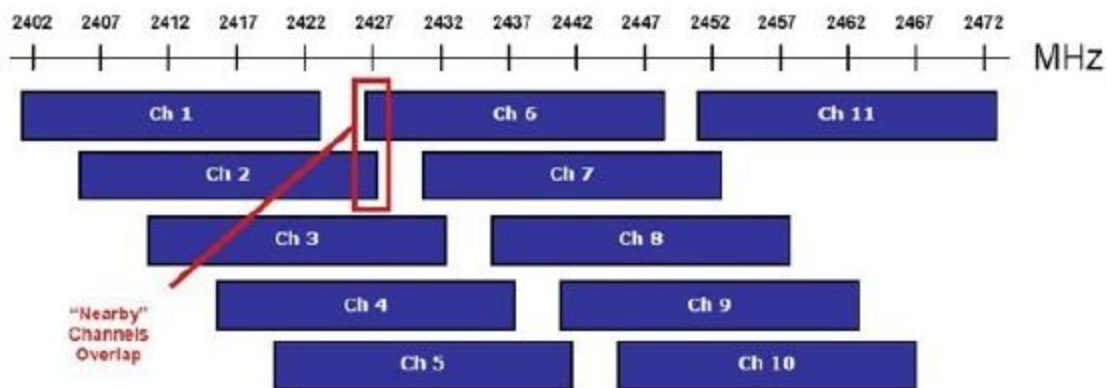


Señal	Canal
-1 dBm	2462 MHz
-4 dBm	2462 MHz
-4 dBm	2462 MHz
-11 dBm	2462 MHz
-14 dBm	2462 MHz
-15 dBm	2462 MHz
-15 dBm	2462 MHz
-16 dBm	2462 MHz
-17 dBm	2462 MHz
-17 dBm	2462 MHz
-18 dBm	2462 MHz
-18 dBm	2462 MHz
-19 dBm	2462 MHz
-19 dBm	2462 MHz
-19 dBm	2462 MHz

2. La representación gráfica de la evolución de la señal es la siguiente, donde puede apreciarse que la señal oscila entre los -1 dBm y los -98 dBm, como se indicó en la respuesta anterior.

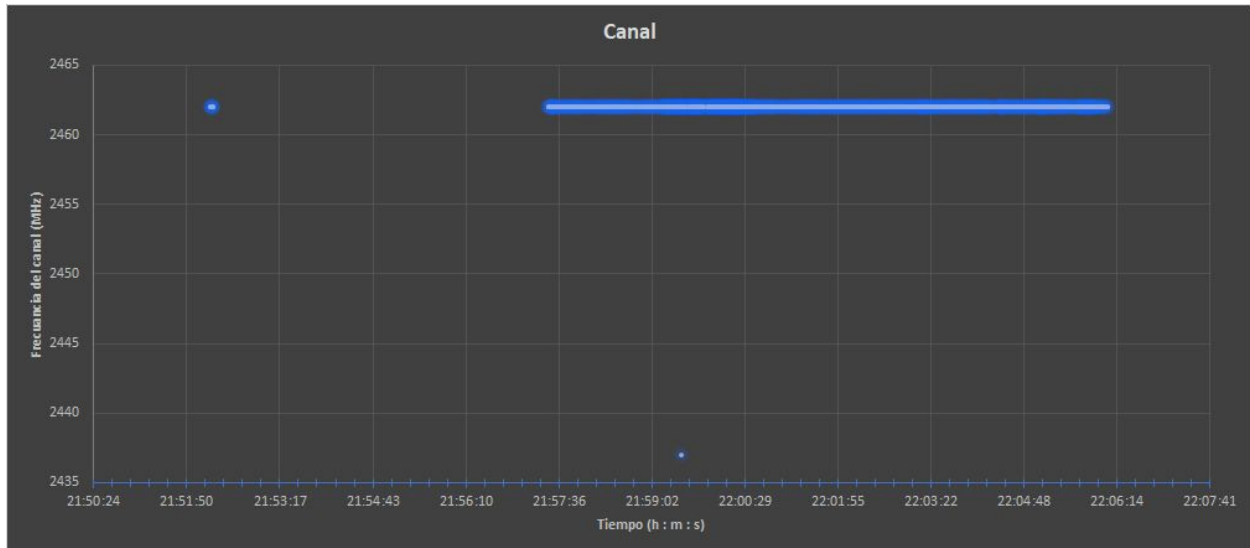


3. Se está usando el canal 11, ya que es el canal correspondiente para la frecuencia que se está usando, que es 2462 MHz.



4. Sí, a las 21:59:30 (a los 437 segundos de haber empezado la captura con WhireShark) puede observarse un cambio de frecuencia, pasando de 2462 MHz a 2437 MHz. Esto indica que se produce un cambio del canal. Concretamente, pasa del canal 11 al canal 6 (como puede apreciarse en la imagen del apartado anterior).

Nota: la captura empieza a las 21:52:12.



Quiz 3

Utiliza la traza [wlan_problem.pcapng](#) para saber qué tipo de tráfico contiene.

¿Cuál es el problema?

El tráfico que contiene la traza corresponde a tráfico broadcast, apreciándose dicha información en la columna «destino».

Por otro lado, el problema se trata de una incorrecta validación del checksum en las tramas erróneas, donde cabe destacar que tanto la señal como la longitud de la trama difieren ampliamente respecto a los valores de las tramas correctas.

Esto da a entender que la distancia respecto al dispositivo destino es la causante, dando lugar a una pérdida de información por el camino en el envío provocando que la longitud de la trama variase junto a la señal.

En la imagen puede observarse la localización del error marcado en rojo en la trama que se ha abierto (493).

The image shows a Wireshark packet capture window titled 'wlan_problem.pcapng'. The packet list pane at the top shows several IEEE 802.11 frames. Packet 493 is selected, and its details pane is expanded. The details pane shows the structure of the IEEE 802.11 frame, including the Frame Control field, Duration, Receiver and Destination addresses, Transmitter and Source addresses, BSS ID, Fragment number, and Sequence number. A red highlight is placed over the 'Frame check sequence' field, which contains the value '0x0101027f'. A red error message is displayed below this field: '[Expert Info (Error/Malformed): Bad checksum [should be 0x69ee5d57]]'. The error message also indicates the severity level is 'Error' and the group is 'Malformed'. The packet bytes pane at the bottom shows the raw data of the frame, with the sequence number field (00 00) highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info	Signal	Channel
493	07:04:42.948049	D-Link_cc:a3:ea	LiteonTe_58:2b:0d	802.11	110	Probe Response, SN=2720, FN=0, Flags=...R..., BI=100, SSID=wsu	-96 dBm	
492	07:04:42.946928	D-Link_cc:a3:ea	LiteonTe_58:2b:0d	802.11	120	Probe Response, SN=2720, FN=0, Flags=...C..., BI=100, SSID=wsu	-95 dBm	
488	07:04:42.636930	D-Link_cc:a3:ea	LiteonTe_58:2b:0d	802.11	120	Probe Response, SN=2716, FN=0, Flags=...C..., BI=100, SSID=wsu	-78 dBm	
473	07:04:40.870449	D-Link_cc:a3:ea	IntelCor_d0:27:d7	802.11	120	Probe Response, SN=2698, FN=0, Flags=...C..., BI=100, SSID=wsu	-77 dBm	
278	07:04:19.424740	D-Link_cc:a3:ea	IntelCor_d0:27:d7	802.11	120	Probe Response, SN=2402, FN=0, Flags=...C..., BI=100, SSID=wsu	-96 dBm	
204	07:04:10.825550	D-Link_cc:a3:ea	IntelCor_d0:27:d7	802.11	120	Probe Response, SN=2312, FN=0, Flags=...R..., BI=100, SSID=wsu	-79 dBm	
203	07:04:10.822425	D-Link_cc:a3:ea	IntelCor_d0:27:d7	802.11	120	Probe Response, SN=2312, FN=0, Flags=...C..., BI=100, SSID=wsu	-96 dBm	
202	07:04:10.821047	D-Link_cc:a3:ea	IntelCor_d0:27:d7	802.11	120	Probe Response, SN=2311, FN=0, Flags=...R..., BI=100, SSID=wsu	-95 dBm	

Frame 493: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0

Radiotap Header v0, Length 20

802.11 radio information

IEEE 802.11 Probe Response, Flags: ...R...

Type/Subtype: Probe Response (0x0005)

Frame Control Field: 0x5008

.000 0001 0011 1010 = Duration: 314 microseconds

Receiver address: LiteonTe_58:2b:0d (00:22:5f:58:2b:0d)

Destination address: LiteonTe_58:2b:0d (00:22:5f:58:2b:0d)

Transmitter address: D-Link_cc:a3:ea (00:13:46:cc:a3:ea)

Source address: D-Link_cc:a3:ea (00:13:46:cc:a3:ea)

BSS Id: D-Link_cc:a3:ea (00:13:46:cc:a3:ea)

.... .. 0000 = Fragment number: 0

1010 1010 0000 = Sequence number: 2720

Frame check sequence: 0x0101027f incorrect, should be 0x69ee5d57

[Expert Info (Error/Malformed): Bad checksum [should be 0x69ee5d57]]

[Bad checksum [should be 0x69ee5d57]]

[Severity level: Error]

[Group: Malformed]

[FCS Status: Bad]

IEEE 802.11 wireless LAN

Fixed parameters (12 bytes)

Tagged parameters (58 bytes)

0020 46 cc a3 ea 00 13 46 cc a3 ea 00 00 e9 5f 20 80 F.....F... ..

Sequence number (wlan.seq), 2 bytes

Packets: 1388 · Displayed: 62 (4.5%)

Profile: Default