

Práctica WLAN: Parte 1

Cristina Díaz García

Noviembre 2018



Índice

Índice general	1
1. Quiz 1	2
2. Quiz 2	2
3. Quiz 3	3

1. Quiz 1

Se está accediendo a la página *en.wikipedia.org*, pasando por *wikimedia* y *pagead2.googlesyndication.com*.

427	13.267707	192.168.0.50	68.87.76...	DNS	138	Standard query 0x605b A en.wikipedia.org
503	14.256515	192.168.0.50	68.87.76...	DNS	142	Standard query 0xca51 A upload.wikimedia.org
807	26.709443	192.168.0.50	68.87.76...	DNS	151	Standard query 0x8c12 A pagead2.googlesyndication.com

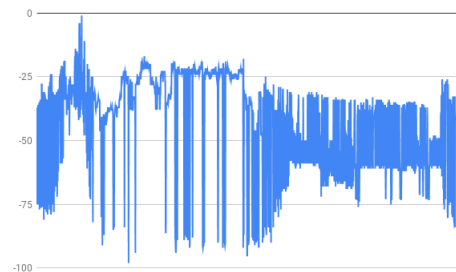
Topic / Item
HTTP Requests by HTTP Host
upload.wikimedia.org
/fundraising/2006/meter.png
snltranscripts.jt.org
/style.css
/line.jpg
/favicon.ico
/75/space2.gif
/75/pics/75d jaws3.jpg
/75/pics/75d jaws2.jpg
/75/pics/75d jaws1.jpg
/75/75d jaws2.phtml
pagead2.googlesyndication.com
/pagead/ads?client=ca-pub-9011062396508188&dt=1167891175069&mt=1167891174&format=728x90_as&output=html&channel=8345570081&url=http%3A%2F%2Fsnltranscripts.jt.org%
en.wikipedia.org
/wiki/Landshark
239.255.255.250:1900
*

2. Quiz 2

La señal más baja es aquella de la que más se pierde la señal, y mientras más mayor el valor absoluto del RSSI negativo, mayor es la pérdida de señal.

No.	Time	Source	Destination	Protocol	Length	Info	Señal
337	438.725511	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-98 dBm
772	491.540517	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-95 dBm
773	491.543930	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-95 dBm
362	440.792136	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-94 dBm
511	463.861638	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-94 dBm
510	463.860515	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-93 dBm
561	471.870400	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-92 dBm
610	475.973673	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-92 dBm
683	483.232132	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-92 dBm
758	489.495028	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-92 dBm
815	498.523657	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-92 dBm
241	427.606382	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-91 dBm
562	471.872314	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-91 dBm
609	475.971764	192.168.0.1	192.168.0.1	ICMP	128	Echo (ping)	-91 dBm

La gráfica de la evolución temporal es la siguiente:



Siempre está en el canal 11 excepto en el paquete 322, que está en el 6, como podemos comprobar:

wlan_radio.channel == 11							Expression...	
No.	Time	Source	Destination	Protocol	Length	Info		
1	0.000000	192.168.0.106	192.168.0...	ICMP	128	Echo (ping) request id=0x0001, seq=21/5376, ttl=128 (reply in 2)		
2	0.000921	192.168.0.1	192.168.0...	ICMP	128	Echo (ping) reply id=0x0001, seq=21/5376, ttl=127 (request in 1)		
3	1.002244	192.168.0.106	192.168.0...	ICMP	128	Echo (ping) request id=0x0001, seq=22/5632, ttl=128 (reply in 4)		
4	1.003233	192.168.0.1	192.168.0...	ICMP	128	Echo (ping) reply id=0x0001, seq=22/5632, ttl=127 (request in 3)		
5	2.005228	192.168.0.106	192.168.0...	ICMP	128	Echo (ping) request id=0x0001, seq=23/5888, ttl=128 (reply in 6)		
6	2.006113	192.168.0.1	192.168.0...	ICMP	128	Echo (ping) reply id=0x0001, seq=23/5888, ttl=127 (request in 5)		
7	3.007252	192.168.0.106	192.168.0...	ICMP	128	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (reply in 8)		
8	3.008476	192.168.0.1	192.168.0...	ICMP	128	Echo (ping) reply id=0x0001, seq=24/6144, ttl=127 (request in 7)		
9	313.634923	192.168.0.106	192.168.0...	ICMP	128	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 10)		
10	313.635844	192.168.0.1	192.168.0...	ICMP	128	Echo (ping) reply id=0x0001, seq=25/6400, ttl=127 (request in 9)		
11	314.637023	192.168.0.106	192.168.0...	ICMP	128	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 12)		
12	314.637964	192.168.0.1	192.168.0...	ICMP	128	Echo (ping) reply id=0x0001, seq=26/6656, ttl=127 (request in 11)		
13	315.639015	192.168.0.106	192.168.0...	ICMP	128	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (no response found)		
14	316.639073	192.168.0.106	192.168.0...	ICMP	128	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (no response found)		

Frame 321: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0
PPI version 0, 32 bytes
802.11 radio information
PHY type: 802.11b (4)
Data rate: 1,0 Mb/s
Channel: 11
Frequency: 2462MHz
Signal strength (dBm): -23dBm
Noise level (dBm): -100dBm
[Duration: 896µs]
IEEE 802.11 Data. Flags:R..TC
00 00 20 00 00 00 00 00 02 00 14 00 00 00 00 00 ... 1 ...

wlan_signal.pcapng Packets: 1568 · Displayed: 1567 (99.9%) Profile: Default

!wlan_radio.channel == 11							Expression...	
No.	Time	Source	Destination	Protocol	Length	Info		
322	437.723424	192.168.0.106	192.168.0...	ICMP	128	Echo (ping) request id=0x0001, seq=148/37888, ttl=128 (no response found!)		

Frame 322: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface 0
PPI version 0, 32 bytes
802.11 radio information
PHY type: 802.11b (4)
Data rate: 1,0 Mb/s
Channel: 6
Frequency: 2437MHz
Signal strength (dBm): -84dBm
Noise level (dBm): -100dBm
[Duration: 896µs]
IEEE 802.11 Data. Flags:R..TC
00 00 20 00 00 00 00 00 02 00 14 00 00 00 00 00 ... 1 ...

wlan_signal.pcapng Packets: 1568 · Displayed: 1 (0.1%) Profile: Default

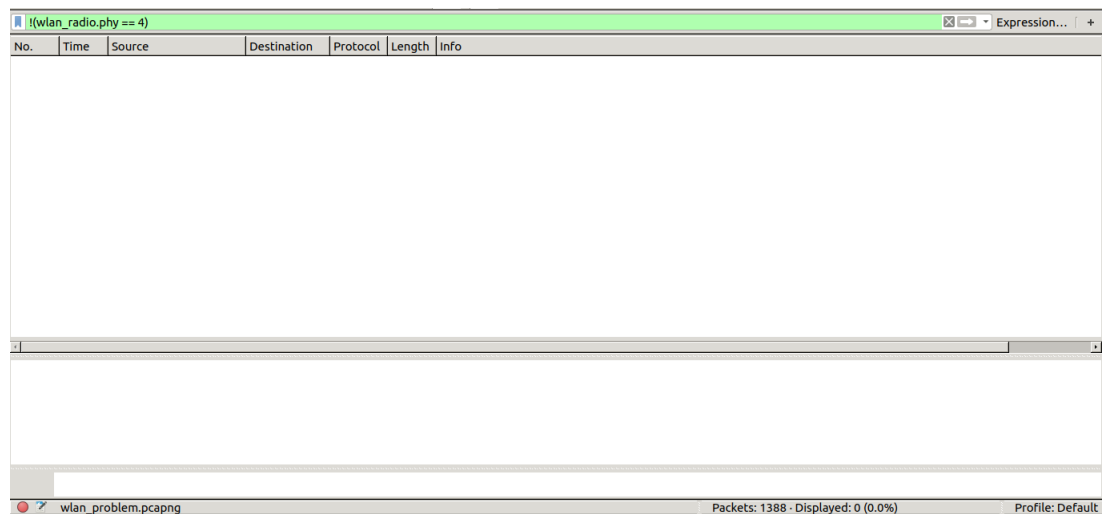
3. Quiz 3

En este ejercicio el problema es que ciertos paquetes tienen errores en con el checksum o el payload.

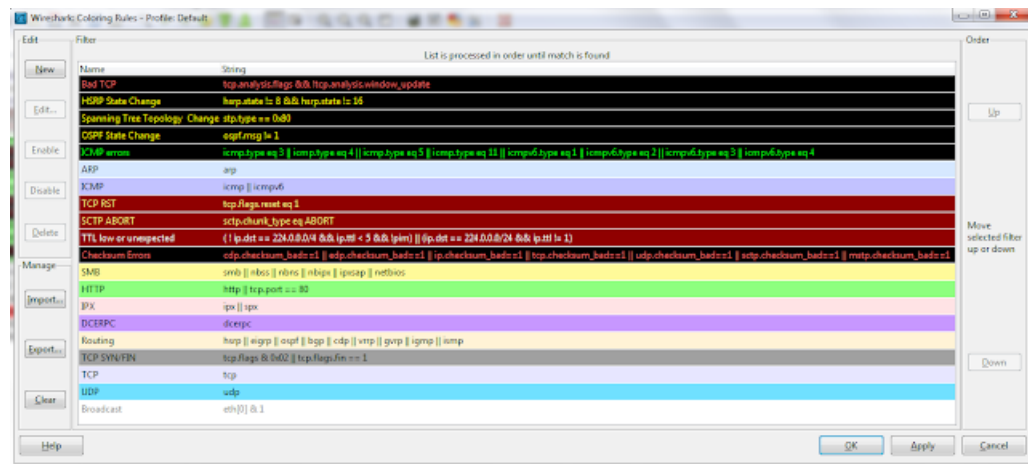
[ws.expert.group == "Malformed"]							Expression...	+
No.	Time	Source	Destination	Protocol	Length	Info		
60.921	D-Link_cc:a3:ea	Broadcast	802.11	99	Beacon frame, SN=2067, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
71.023	D-Link_cc:a3:ea	Broadcast	802.11	111	Beacon frame, SN=2068, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
293.276	D-Link_cc:a3:ea	Broadcast	802.11	75	Beacon frame, SN=2091, FN=0, Flags=....., BI=100, SSID=wsu			
313.481	D-Link_cc:a3:ea	Broadcast	802.11	101	Beacon frame, SN=2093, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
546.143	D-Link_cc:a3:ea	Broadcast	802.11	115	Beacon frame, SN=2121, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
596.655	D-Link_cc:a3:ea	Broadcast	802.11	73	Beacon frame, SN=2126, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
738.293	D-Link_cc:a3:ea	Broadcast	802.11	67	Beacon frame, SN=2142, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
748.396	D-Link_cc:a3:ea	Broadcast	802.11	79	Beacon frame, SN=2143, FN=0, Flags=....., BI=100, SSID=wsu[Malformed Packet]			
768.601	D-Link_cc:a3:ea	Broadcast	802.11	105	Beacon frame, SN=2145, FN=0, Flags=....., BI=100, SSID=wsu[Malformed Packet]			
9610.95	D-Link_cc:a3:ea	Broadcast	802.11	81	Beacon frame, SN=2170, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
9911.16	D-Link_cc:a3:ea	Broadcast	802.11	107	Beacon frame, SN=2172, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
12714.33	D-Link_cc:a3:ea	Broadcast	802.11	107	Beacon frame, SN=2284, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
14816.38	D-Link_cc:a3:ea	Broadcast	802.11	123	Beacon frame, SN=2227, FN=0, Flags=....., BI=100, SSID=wsu[Malformed Packet]			
15216.79	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2233, FN=0, Flags=....., BI=100, SSID=wsu[Malformed Packet]			
15518.63	D-Link_cc:a3:ea	Broadcast	802.11	413	Data, SN=2263, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
17821.09	D-Link_cc:a3:ea	Broadcast	802.11	77	Beacon frame, SN=2291, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
17921.19	D-Link_cc:a3:ea	Broadcast	802.11	89	Beacon frame, SN=2292, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
18124.48	D-Link_cc:a3:ea	Broadcast	802.11	145	Beacon frame, SN=2284, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
Frame 152: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0								
Interface id: 0 (unknown)								
Encapsulation type: IEEE 802.11 plus radiotap radio header (23)								
Arrival Time: Sep 10, 2009 07:04:04.907479000 CEST								
[Time shift for this packet: 0.000000000 seconds]								
Epoch Time: 125255844.907479000 seconds								
0000 00 00 14 00 ee 18 00 00 10 02 6c 09 a0 00 b2 9c1.....								
wlan_problem.pcapng							Packets: 1388 - Displayed: 127 (9.1%)	Profile: Default

El tráfico es todo 802.11:

[wlan_radio.phy == 4]							Expression...	+
No.	Time	Source	Destination	Protocol	Length	Info		
10.000	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2058, FN=0, Flags=.....C, BI=100, SSID=wsu			
20.409	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2062, FN=0, Flags=.....C, BI=100, SSID=wsu			
30.511	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2063, FN=0, Flags=.....C, BI=100, SSID=wsu			
40.716	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2065, FN=0, Flags=.....C, BI=100, SSID=wsu			
50.819	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2066, FN=0, Flags=.....C, BI=100, SSID=wsu			
60.921	D-Link_cc:a3:ea	Broadcast	802.11	99	Beacon frame, SN=2067, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
71.023	D-Link_cc:a3:ea	Broadcast	802.11	111	Beacon frame, SN=2068, FN=0, Flags=....., BI=100, SSID=wsu[Packet size limited dur			
81.126	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2069, FN=0, Flags=.....C, BI=100, SSID=wsu			
91.228	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2070, FN=0, Flags=.....C, BI=100, SSID=wsu			
101.331	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2071, FN=0, Flags=.....C, BI=100, SSID=wsu			
111.433	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2072, FN=0, Flags=.....C, BI=100, SSID=wsu			
121.475	IntelCor_d0:27:d7	Broadcast	802.11	69	Probe Request, SN=276, FN=0, Flags=.....C, SSID=wsu			
131.478	D-Link_cc:a3:ea	IntelCor_...	802.11	120	Probe Response, SN=2073, FN=0, Flags=.....C, BI=100, SSID=wsu			
141.479	D-Link_cc:a3:ea	IntelCor_...	802.11	120	Probe Response, SN=2073, FN=0, Flags=.....R..C, BI=100, SSID=wsu			
151.535	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2074, FN=0, Flags=.....C, BI=100, SSID=wsu			
161.638	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2075, FN=0, Flags=.....C, BI=100, SSID=wsu			
171.740	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2076, FN=0, Flags=.....C, BI=100, SSID=wsu			
181.843	D-Link_cc:a3:ea	Broadcast	802.11	126	Beacon frame, SN=2077, FN=0, Flags=.....C, BI=100, SSID=wsu			
Frame 1: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0								
Radiotap Header v0, Length 20								
802.11 radio information								
PHY type: 802.11b (4)								
Short preamble: False								
Data rate: 1.0 Mb/s								
Channel: 1								
0010 11 00 00 05 00 00 00 00 ff ff ff ff ff ff 00 1313.....								
PHY type (wlan_radio.phy)							Packets: 1388 - Displayed: 1388 (100.0%)	Profile: Default



Todo el tráfico coloreado de blanco es de tipo broadcast (802.11) y el negro de tipo error en el checksum.



Referencias

[1] *Coloring rules*, <http://manualwireshark.blogspot.com/>.