



Capturing Wireless

Capturing Wireless

» What is Wireless?

» Capturing wireless with Wireshark

- Ready to go by default

» Special setup

- Wireshark setup
- Configuration of wireless NIC on wireless LAN (WLAN)

Capturing Wireless

Filter: Expression... Clear Apply Save TCP Full

802.11 Channel: Channel Offset: FCS Filter: All Frames None Wireless Settings... Decryption Keys...

No.	Time	Source	Destination	Protocol	Expert	Length	Info
1	0.000000	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
2	0.102961	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
3	0.103946	Cisco-Li_82:b2:55	Spanning-tree-(for-	802.11		118	Data, SN=3975,
4	0.204955	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
5	0.307929	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
6	0.409911	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
7	0.512900	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
8	0.614871	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
9	0.716933	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
10	0.819842	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
11	0.921825	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
12	1.024783	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,
13	1.126803	Cisco-Li_82:b2:55	Broadcast	802.11		168	Beacon frame,

Flags: 0x10
Data Rate: 1.0 Mb/s
Channel frequency: 2412 [BG 1]
Channel type: 802.11b (0x00a0)
... ..0... = Turbo: False
... ..1... = Complementary Code Keying (CCK): True
... ..0... = Orthogonal Frequency-Division Multiplexing (OFDM): False
... ..1... = 2 GHz spectrum: True
... ..0... = 5 GHz spectrum: False
... ..0... = Passive: False
... ..0... = Dynamic CCK-OFDM: False
... ..0... = Gaussian Frequency Shift Keying (GFSK): False
... ..0... = GSM (900MHz): False
... ..0... = Static Turbo: False
... ..0... = Half Rate Channel (10MHz Channel width): False
... ..0... = Quarter Rate Channel (5MHz channel width): False
Signal Quality: 84
Antenna: 0
SSI signal: 43 dB

Capturing Wireless

» Problems you may encounter

- Incorrect SSID
- Channel problem
- Other

» Tools you can use

- You can set up a Wireshark filter to capture WLAN specific traffic and use the WLAN Traffic option on the Statistics menu
- Specialized toolbar

Capturing Wireless

Wireshark: WLAN Traffic Statistics: wpa-Induction.pcap

Network Overview - No Filter

BSSID	Ch.	SSID	% Packets	Beacons	Data Packets	Probe Req	Probe Resp	Auth	Deauth	Other
ff:ff:ff:ff:ff:3f		<Broadcast>	0.14 %	0	0	0	0	0	0	0
5a:17:e9:a9:be:27		<Broadcast>	0.14 %	0	0	0	0	0	0	0
65:78:f7:b7:60:a9		<Broadcast>	0.41 %	0	0	0	0	0	0	0
65:78:f7:b7:30:84		<Broadcast>	0.14 %	0	0	0	0	0	0	0
98:d3:04:64:fa:55		<Broadcast>	0.14 %	0	1	0	0	0	0	0
Cisco-Li_82:b2:55	1	Coherer	97.95 %	398	284	4	26	2	0	0

Selected Network

Address	% Packets	Data Sent	Data Received	Probe Req	Probe Resp	Auth	Deauth	Other	Comment
11:5a:08:13:2c:86	100.00 %	0	0	0	0	0	0	1	
18:9d:f4:e6:d1:7a	100.00 %	0	0	0	0	0	0	1	

☒ Name resolution ☒ Limit to display filter ☒ Only show existing networks

Help Copy Close

Questions?