



# SharkFest '17 Europe

## Troubleshooting WLANs (Part 1)

Layer 1 & 2 Analysis Using AirPcap, Wi-Spy & Other Tools

8. November 2017



Rolf Leutert

Leutert NetServices

Switzerland

[www.netsniffing.ch](http://www.netsniffing.ch)



Rolf Leutert, El. Ing. HTL  
Leutert NetServices  
Zürich-Airport, Switzerland

- Network Analysis & Troubleshooting
- Protocol Trainings TCP/IP, WLAN, VoIP, IPv6
- Wireshark® Certified Network Analyst 2010
- Wireshark® Instructor since 2006
- Sniffer® certified Instructor since 1990

[leutert@netsniffing.ch](mailto:leutert@netsniffing.ch)  
[www.netsniffing.ch](http://www.netsniffing.ch)

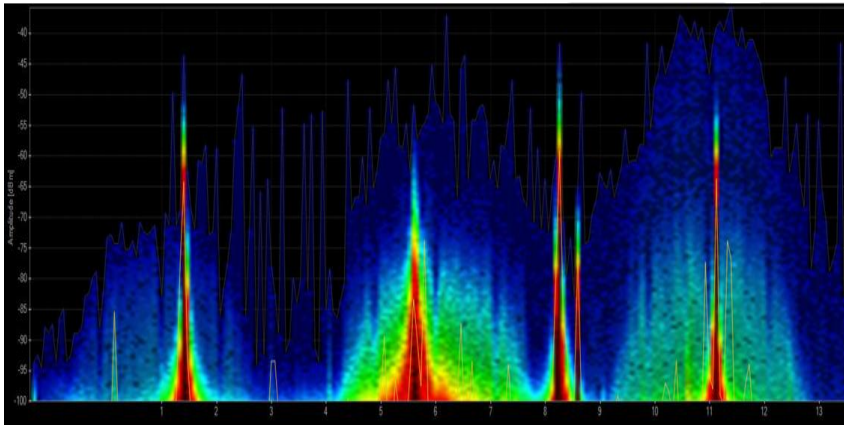




- Learn what you can see on WLAN layer 1 and layer 2
- Learn which tools can help you finding WLAN problems
- Learn which tool supports which layer
- Learn how to use Radiotap and PPI header information
- Learn how to customize Wireshark to show you specific WLAN information



Troubleshooting wireless networks is a demanding task and requires detailed understanding of important functions on layer 1 and 2 !



## Layer 1 - Physical Access

FH, DSSS, OFDM, coding, modulation, bands, channels, frequencies, noise, signal strength, interferences etc.

**Clients:** WiFi and non-WiFi devices like surveillance cameras, remote control, microwave, health gadgets etc.

**Tools:** Spectrum Analyser (e.g. Wi-Spy)

No.	Time	Source	Destination	Signal	Noise	Tx Speed	Channel	Info
111	0.000	IntelCor_79:46:04	Broadcast	-30	-87	1.0 Mbps	2437 [BG 6]	Probe Request, SN=365, FN=0,
112	0.002	Cisco_1f:4e:20	IntelCor_7	-27	-87	1.0 Mbps	2437 [BG 6]	Probe Response, SN=2149, FN=
113	0.000		Cisco_1f:4	-30	-87	1.0 Mbps	2437 [BG 6]	Acknowledgement, Flags=.....
114	0.067	Cisco_1f:4e:20	Broadcast	-27	-87	1.0 Mbps	2437 [BG 6]	Beacon frame, SN=1597, FN=0,
115	0.101	IntelCor_79:46:04	Cisco_1f:4	-27	-87	6.0 Mbps	2437 [BG 6]	Authentication, SN=15, FN=0,
116	0.000		IntelCor_7	-27	-87	6.0 Mbps	2437 [BG 6]	Acknowledgement, Flags=.....
117	0.000	Cisco_1f:4e:20	IntelCor_7	-27	-87	1.0 Mbps	2437 [BG 6]	Authentication, SN=1598, FN=
118	0.000		Cisco_1f:4	-31	-87	1.0 Mbps	2437 [BG 6]	Acknowledgement, Flags=.....
119	0.002	Cisco_1f:4e:20	Broadcast	-26	-87	1.0 Mbps	2437 [BG 6]	Beacon frame, SN=1599, FN=0,
120	0.000	IntelCor_79:46:04	Cisco_1f:4	-27	-87	6.0 Mbps	2437 [BG 6]	Association Request, SN=16,
121	0.000		IntelCor_7	-27	-87	6.0 Mbps	2437 [BG 6]	Acknowledgement, Flags=.....
122	0.002	Cisco_1f:4e:20	IntelCor_7	-27	-87	1.0 Mbps	2437 [BG 6]	Association Response, SN=160
123	0.000		Cisco_1f:4	-45	-87	1.0 Mbps	2437 [BG 6]	Acknowledgement, Flags=.....
124	0.002	Cisco_1f:4e:20	IntelCor_7	-26	-87	1.0 Mbps	2437 [BG 6]	Key (Message 1 of 4)
125	0.001	Cisco_1f:4e:20	IntelCor_7	-26	-87	1.0 Mbps	2437 [BG 6]	Key (Message 1 of 4)
126	0.000		Cisco_1f:4	-45	-87	1.0 Mbps	2437 [BG 6]	Acknowledgement, Flags=.....

## Layer 2 - Data Link Control

WiFi Standards 802.11 a/b/g/n/ac framing, management, access control, security, encryption etc.

**Clients:** WiFi compatible devices only

**Tools:** Wireshark, AirPcap, Scanners



- ▶ WLAN (WiFi) devices are working in the 2.4 GHz ISM\* and 5 GHz UNII\*\* bands
- ▶ But both bands are free for any use, WiFi as well as non-WiFi devices
- ▶ Especially the 2.4 GHz band is often crowded with non-WiFi devices
- ▶ The only restriction is max. radiated power according to country regulations
- ▶ Non-WiFi clients use any kind of modulation and may interfere with WiFi
- ▶ Layer 2 tools like Wireshark can not detect non-WiFi devices
- ▶ Spectrum analyzers scan the bands and show shape and strength of all signals

Wi-Spy® DBx spectrum scanner and Chanalyzer® software displays and records all layer 1 signals in both 2.4 GHz and 5 GHz bands.

[www.metageek.com](http://www.metageek.com)

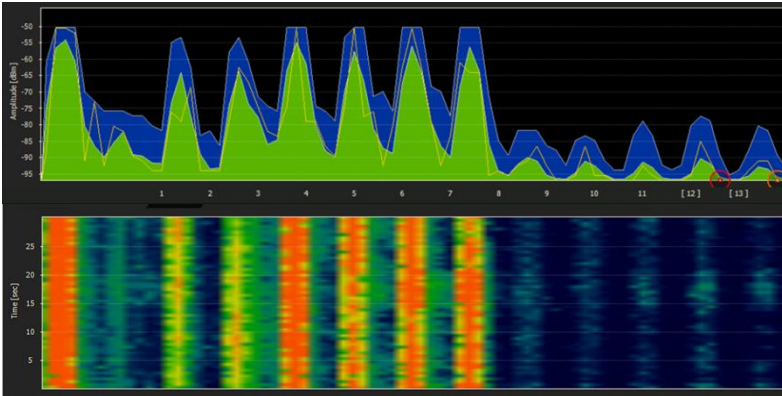
\* ISM Industrial, Scientific and Medical

\*\*UNII Unlicensed National Information Infrastructure

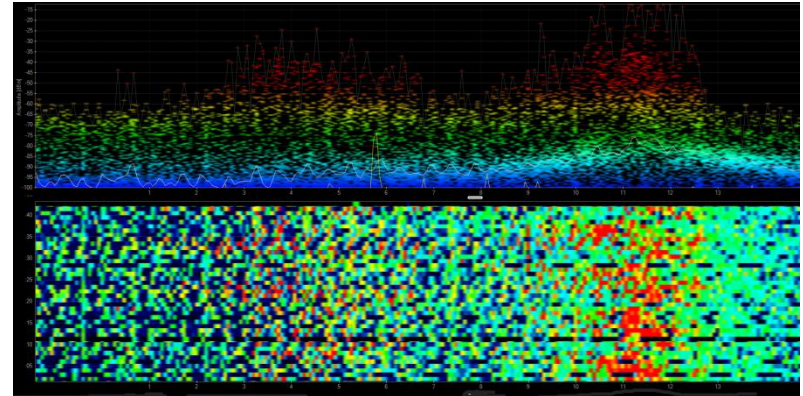




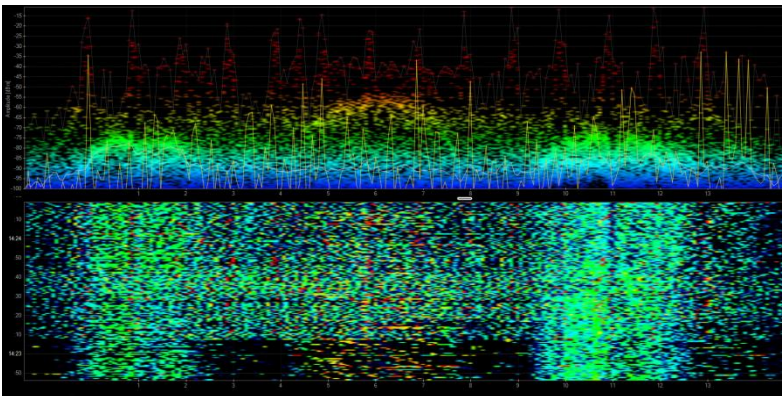
## Non-WiFi Devices' Signatures



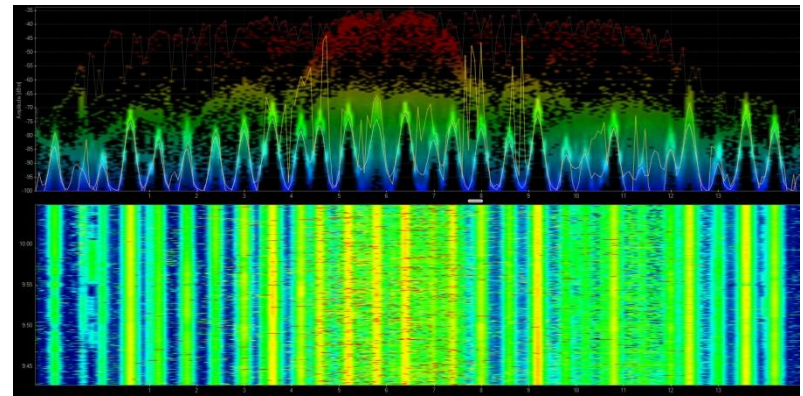
Home trainers in a fitness center



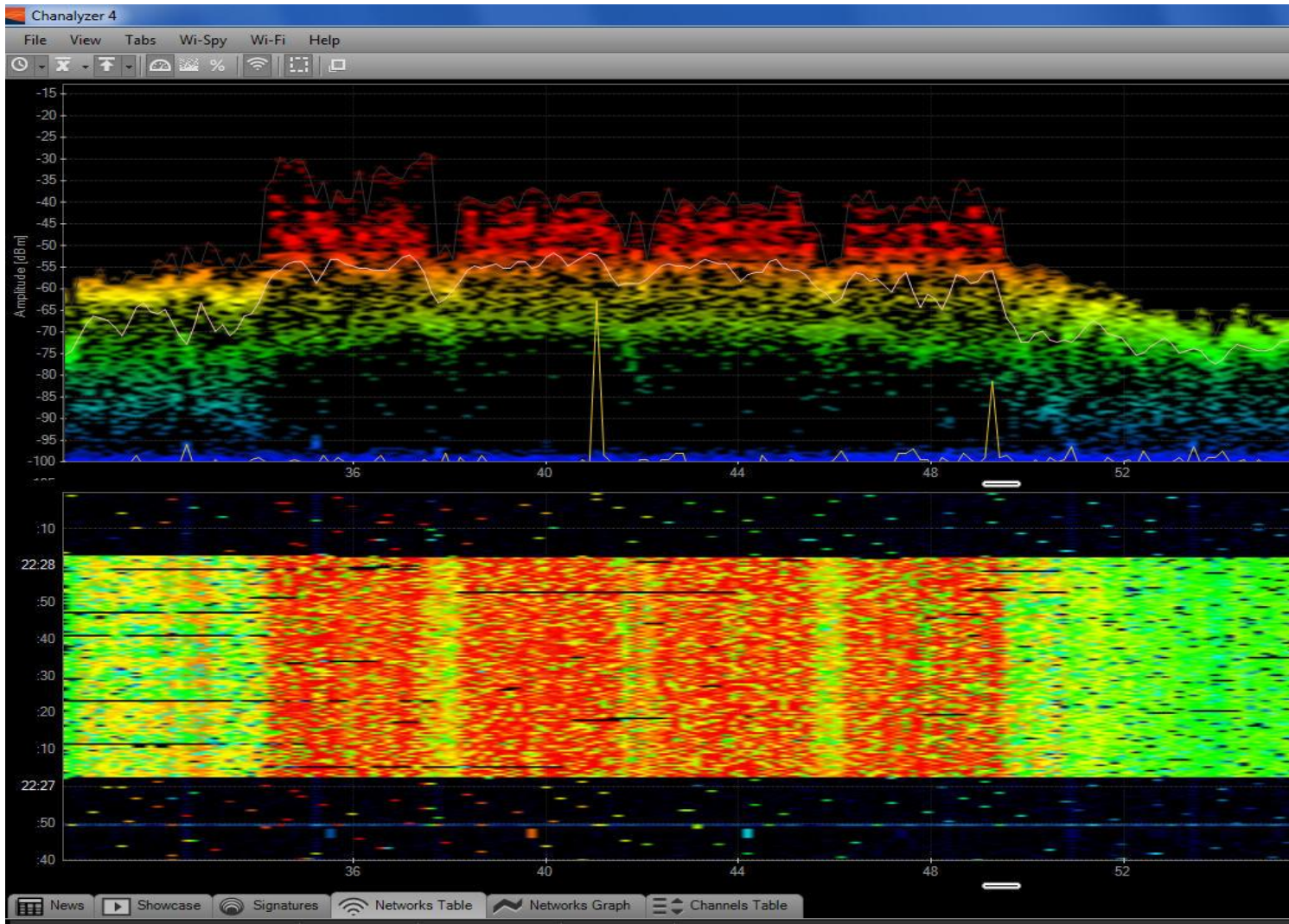
Microwave oven



Remote control of model airplanes



Wireless guitar



WiFi 802.11ac with four bonded channels



**LIVE DEMONSTRATION  
WI-SPY & CHANALYZER**



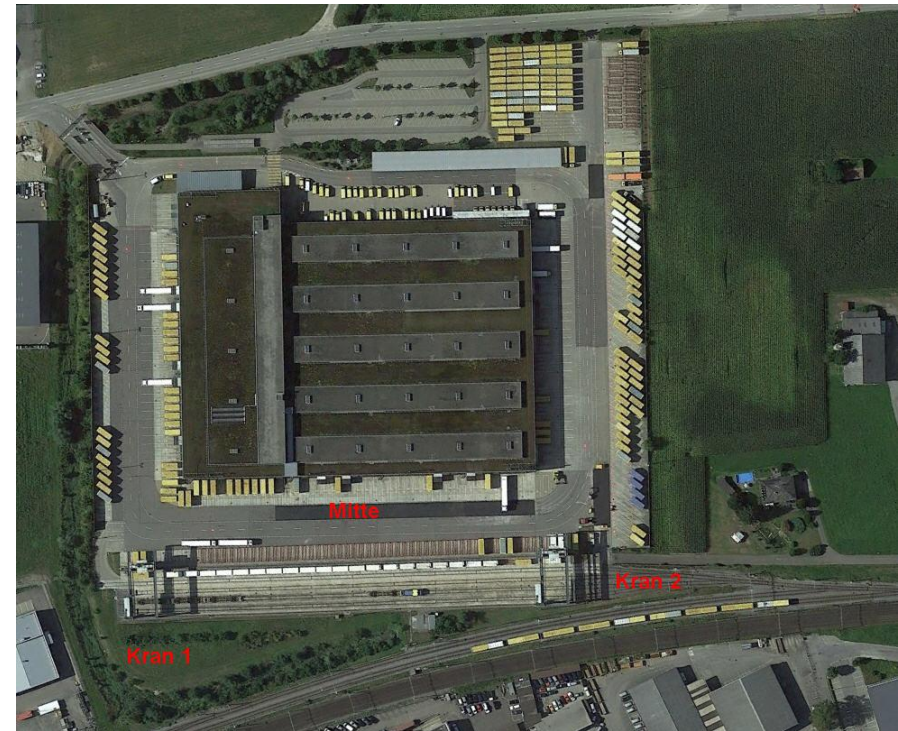
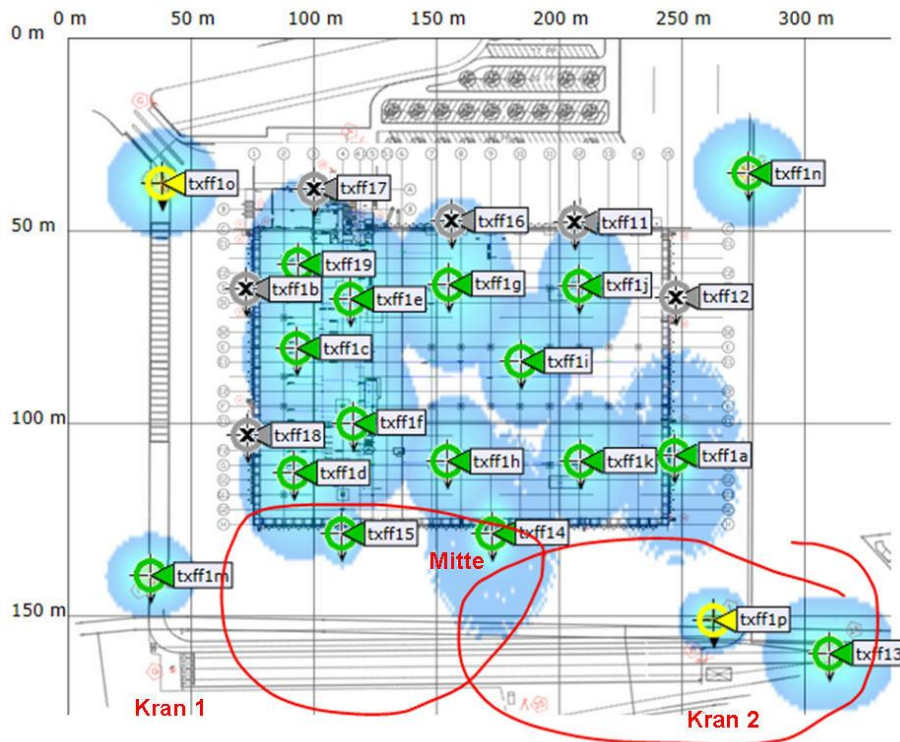


- Large logistic enterprise, **depending on WLAN** for day-to-day operations
- Two container cranes to load/unload trains require WLAN connections



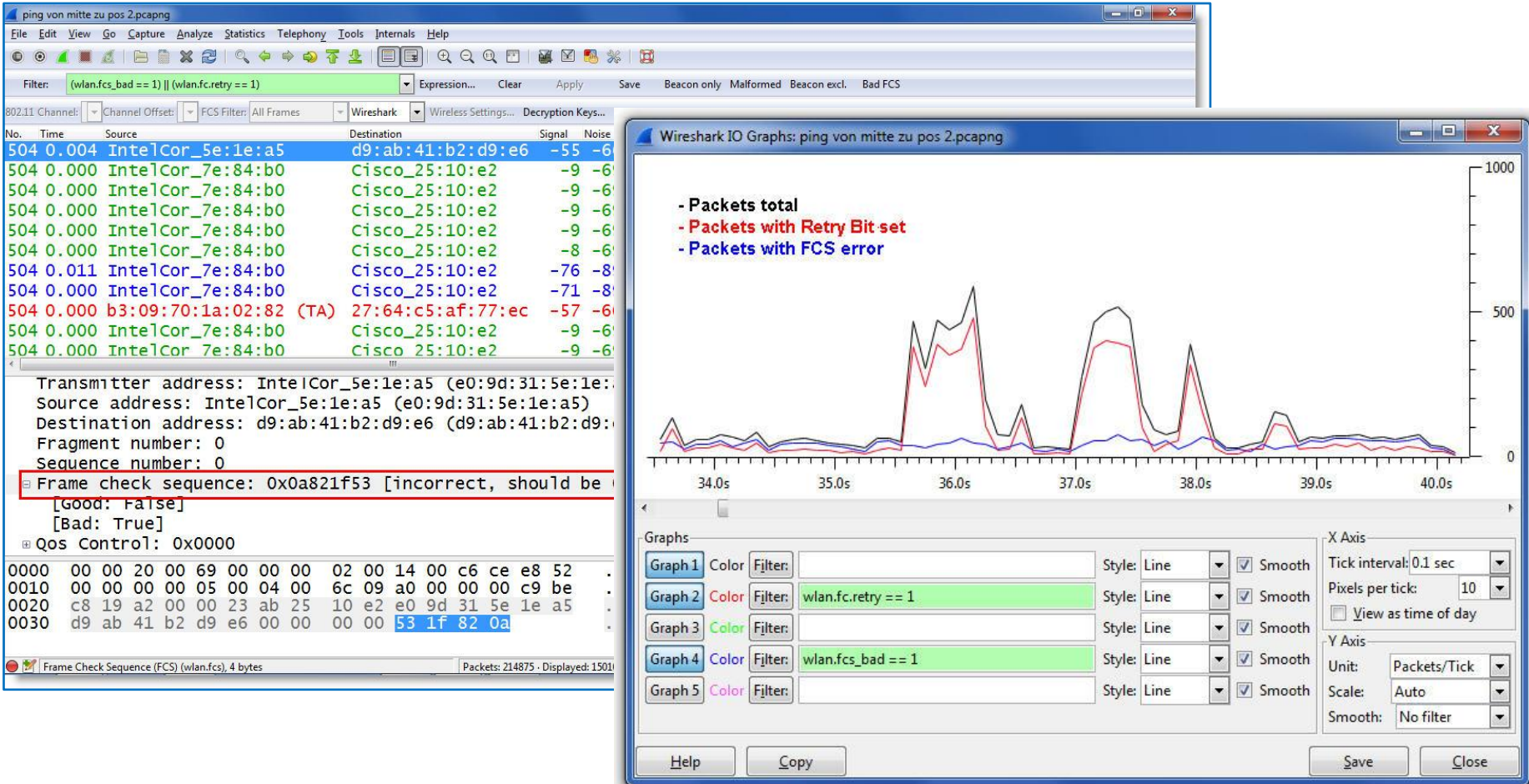


- ▶ User complain about log-in **timeouts** and **disconnections** during operations
- ▶ Crane #2 is hardly usable due to **unreliable WLAN connection**
- ▶ Tech-Support has already changed WiFi channels and **added additional AP**



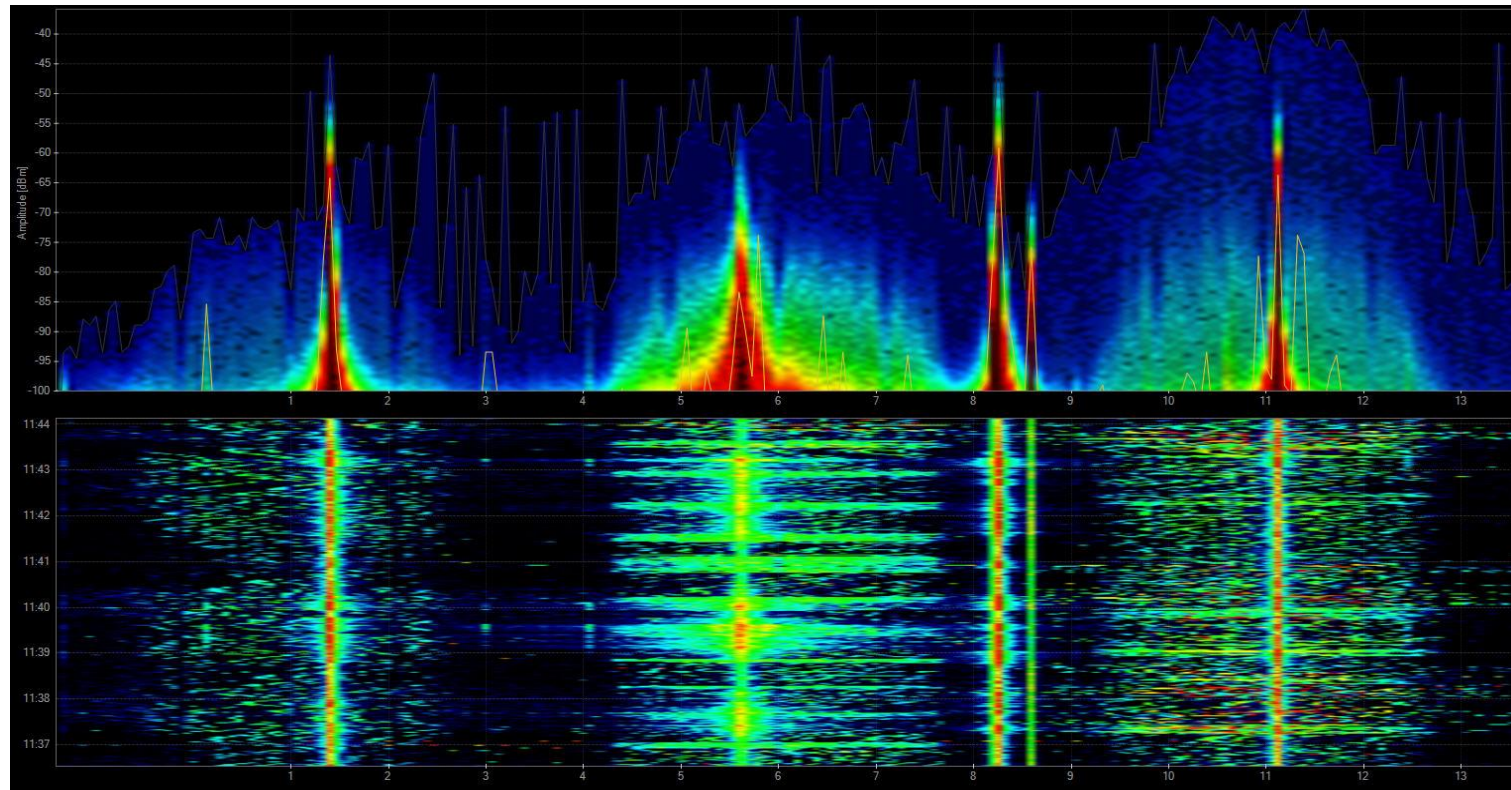


- Starting with **layer 2** analysis near crane #2 in channels 1, 6, and 11
- Wireshark shows up to **70%** of frames with **bad FCS** or the **Retry Flag** set





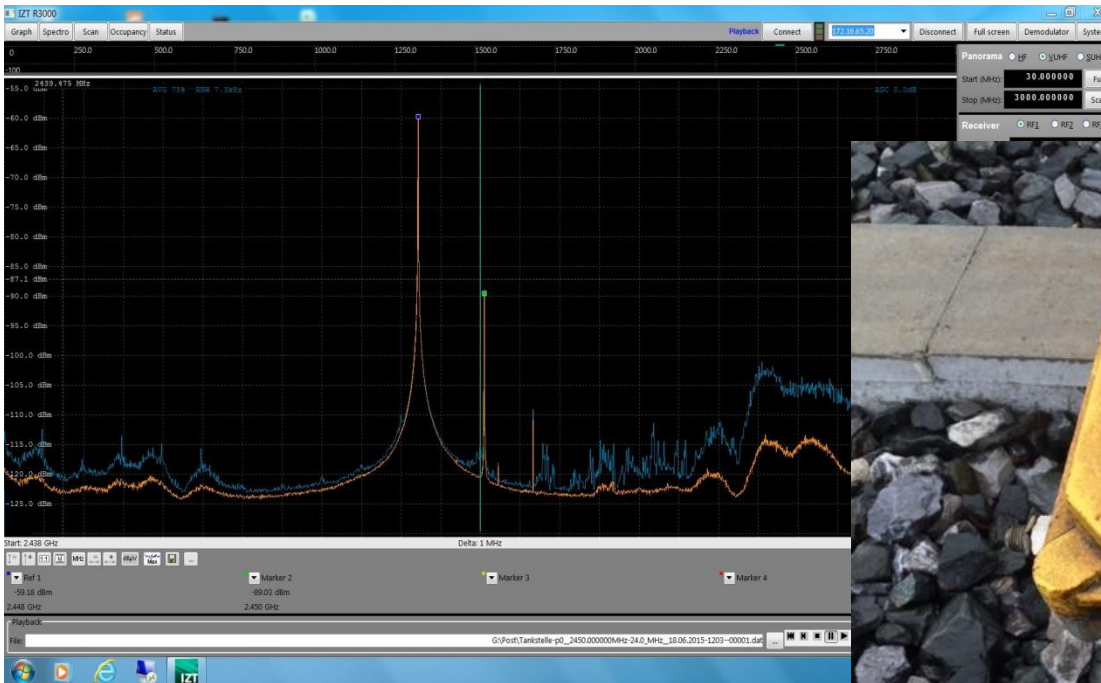
- Continuing with **layer 1** analysis near crane #2 in 2.4 GHz band
- Strong interference with **non-WiFi signals** on all three channels detected



- Signal source is outside of customers campus' → Swiss radio authority informed
- If this transmitting power is within legal limits → Change to 5 GHz band required



- Swiss radio authority (BAKOM) scanned the 2.4 GHz band with their own tool
- Strong interfering signal caused by a **defective railway induction loop**



BAKOM scan result

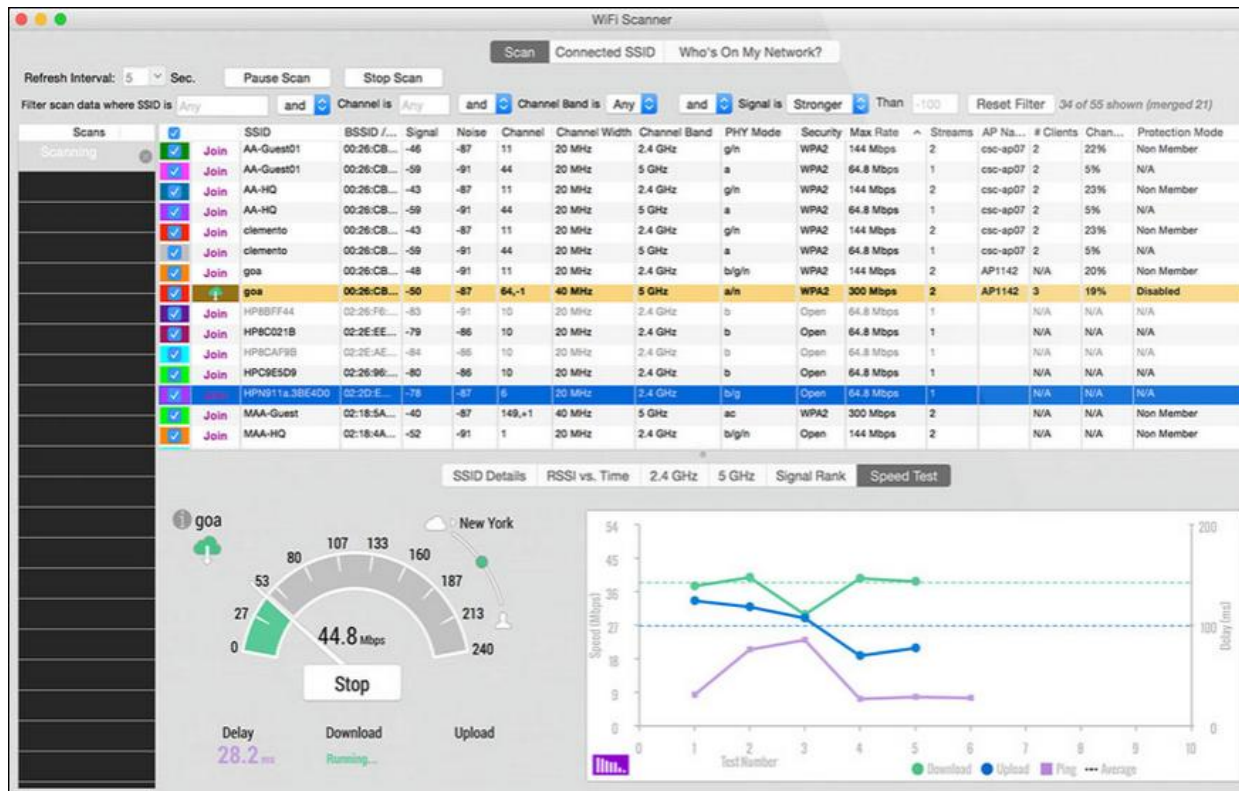


Traffic monitoring induction loop





- WiFi scanners show you available access points with lots of information like SSID, channel no, channel width, max. rate, security mode etc.
- Some tools are able to perform throughput simulations
- No adapter required, WiFi scanners are using internal WLAN cards





Acrylic WiFi scanner

[www.acrylicwifi.com](http://www.acrylicwifi.com)



Ekahau HeatMapper

[www.ekahau.com](http://www.ekahau.com)



inSSIDer

[www.metageek.com](http://www.metageek.com)



NetStumbler

[www.netstumbler.com](http://www.netstumbler.com)



Wifi Analyzer (Android)

[play.google.com](http://play.google.com)



WifiInfoView

[www.nirsoft.net](http://www.nirsoft.net)



WifiScanner

[wifiscanner.sourceforge.net](http://wifiscanner.sourceforge.net)



Wifi Scanner

[www.apple.com/osx/apps/app-store](http://www.apple.com/osx/apps/app-store)



Remark: Apple IOS (iPhone/iPad) has locked direct access to the WiFi interface for stability and other unknown reasons. Jailbreak is required to install and run WiFi Scanner apps on these devices.



All these tools have the following **limitations** in common:

- Scanning on **layer 2**, therefore **only WiFi** devices can be detected.
- Non-802.11 sources like surveillance cameras etc. are **invisible**.
- WiFi scanners read data from **Beacon** and other **management frames**

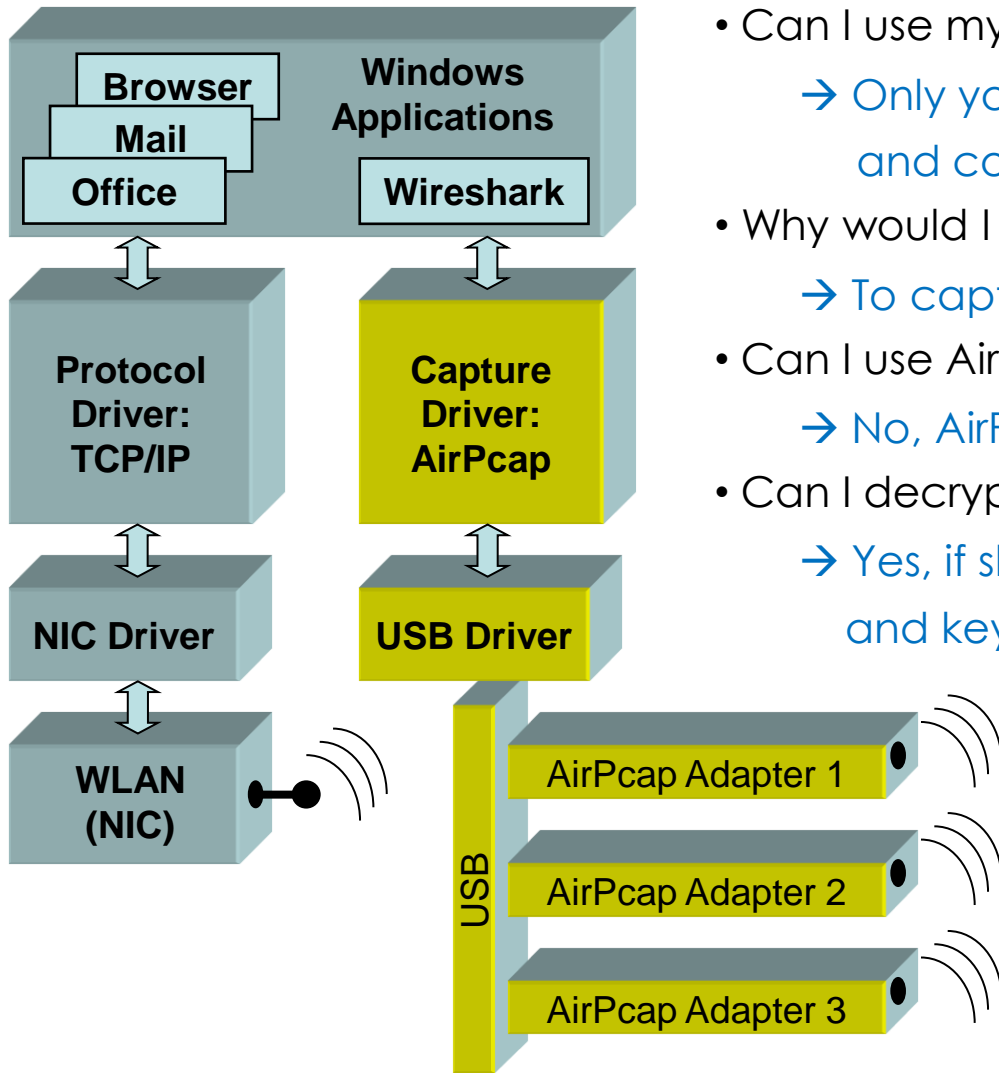
No.	Time	Source	Destination	Signal	Noise	TX Speed	Channel	Info
1	0.000	Cisco_1f:4e:2e	Broadcast	-19	-90	6.0 Mbps	5500 [A 100]	Beacon frame, SN=1802
2	0.104	Cisco_1f:4e:2e	Broadcast	-19	-90	6.0 Mbps	5500 [A 100]	Beacon frame, SN=1803
3	0.104	Cisco_1f:4e:2e	Broadcast	-19	-90	6.0 Mbps	5500 [A 100]	Beacon frame, SN=1804

Frame 1: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface 0

- PPI version 0, 32 bytes
- IEEE 802.11 Beacon frame, Flags: .....C
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters (12 bytes)
  - Tagged parameters (269 bytes)
    - Tag: SSID parameter set: LNS-LAB-5.5GHZ
    - Tag: Supported Rates 6(B), 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    - Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    - Tag: Country Information: Country Code CH, Environment Any

WiFi Scanners will not provide any information if Beacon frames interfere with non 802.11 devices on layer 1!





## Frequently Asked Questions:

- Can I use my built-in WLAN NIC with Wireshark?  
→ Only your own traffic and no management and control frames will be captured
- Why would I need multiple AirPcaps?  
→ To capture roaming processes
- Can I use AirPcaps to join a WLAN?  
→ No, AirPcaps are monitoring devices only.
- Can I decrypt data with AirPcap adapter?  
→ Yes, if shared keys are used, key is available and key negotiation is captured

MAC OS X and some Linux Drivers also support WLAN monitoring:  
<http://linuxwireless.org/en/users/Drivers>



- ▶ Capturing with the built-in WLAN NIC may display faked Ethernet frames only
- ▶ Only Data frames and no Radio or WLAN header will be seen

\*Drahtlosnetzwerkverbindung [Wireshark 1.10.0rc2 (SVN Rev 49526 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:  Expression... Clear Apply Save Layer 2 only TCP UDP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.217	192.168.0.255	NBNS	92	Name query NB
2	0.258232	192.168.0.201	192.168.0.255	NBNS	92	Name query NB
3	0.069601	192.168.0.217	239.255.255.250	SSDP	175	M-SEARCH * HTT
4	0.237969	192.168.0.201	239.255.255.250	SSDP	175	M-SEARCH * HTT
5	0.199400	192.168.0.217	224.0.0.252	LLMNR	66	Standard query
6	0.107298	192.168.0.201	224.0.0.252	LLMNR	66	Standard query
7	0.001103	192.168.0.217	224.0.0.252	LLMNR	66	Standard query
8	0.203786	192.168.0.217	192.168.0.255	NBNS	92	Name query NB
9	0.102408	192.168.0.201	224.0.0.252	LLMNR	66	Standard query
10	0.002094	192.168.0.201	192.168.0.255	NBNS	92	Name query NB
11	0.659450	192.168.0.217	192.168.0.255	NBNS	92	Name query NB

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)

- Ethernet II, Src: IntelCor\_73:68:54 (00:21:6b:73:68:54), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.168.0.217 (192.168.0.217), Dst: 192.168.0.255
- User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
- NetBIOS Name Service



The image shows the Wireshark interface with three callout boxes indicating the steps to configure AirPcap:

- 1. Turn on Wireless Toolbar**: A callout points to the **View** menu in the top toolbar.
- 2. Click on AirPcap Control Panel**: A callout points to the **AirPcap Control Panel** button in the top toolbar.
- 3. Configure AirPcap Settings**: A callout points to the **AirPcap Control Panel** dialog box, which is open and shows the **Basic Configuration** section. This section includes:
  - Interface: AirPcap USB wireless capture adapter nr. 00
  - Model: AirPcap Nx
  - Transmit: yes
  - Media: 802.11 a/b/g/n
  - Channel: 2412 MHz [BG 1]
  - Extension Channel: 0
  - Capture Type: 802.11 + PPI
  - FCS Filter: Valid Frames
  - Include 802.11 FCS in Frames



- ▶ You may have to start Wireshark in [Admin Mode](#) to see the AirPcap I/Fs
- ▶ Verify the settings on the [Capture Interfaces](#) pane

Wireshark · Capture Interfaces

Input Output Options

Interface	Traffic	Link-layer Header	Promi:	Snaplen	Buffer (MB)	Monitor Mode	Capture Filter
AirPcap USB wireless capture adapter nr. 00		Per-Packet Information	<input checked="" type="checkbox"/>	default	2	—	
<b>AirPcap Multi-Channel Aggregator</b>		Per-Packet Information	<input checked="" type="checkbox"/>	default	2	—	
AirPcap USB wireless capture adapter nr. 01		Per-Packet Information	<input checked="" type="checkbox"/>	default	2	—	
AirPcap USB wireless capture adapter nr. 02		Per-Packet Information	<input checked="" type="checkbox"/>	default	2	—	
> Bluetooth-Netzwerkverbindung			<input checked="" type="checkbox"/>	default	2	—	
Drahtlosnetzwerkverbindung		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> LAN-Verbindung* 3		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> LAN-Verbindung		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> LAN-Verbindung* 2		Eth	<input checked="" type="checkbox"/>	default	2	—	

Enable promiscuous mode on all interfaces

Capture filter for selected interfaces:

Manage Interfaces... Compile BPFs

**Start** Close Help

**1. Select Virtual Adapter**

**2. Press to Start Capturing**



## Key features:

- ▶ Radio cells use **one or multiple 20 MHz channels** (n/ac) to increase throughput
- ▶ Each radio cell is a **shared media** and is controlled by an Access Point (AP)
- ▶ A mobile client can be associated with **only one AP** at the time
- ▶ Radio cell access is controlled by **managements and control frames**
- ▶ Wireshark with AirPcap can **capture and analyze** these frames
- ▶ Understanding of these frames is crucial for **WLAN troubleshooting**

AirPcap Nx 802.11a/b/g/n USB - adapter works with **Wireshark** and captures Wi-Fi packets in both 2.4 GHz and 5 GHz bands.

[www.riverbed.com/products/](http://www.riverbed.com/products/)

**END-OF-AVAILABILITY  
JANUARY 1ST, 2018**





## Softing IT Networks introduces new multi-channel Wireless Analyzer

- Includes 4 wireless adapter with 16 integrated antennas
- Supports 4x4 MIMO up to IEEE 802.11ac Wave 2 up to 800 Mbps
- USB-C type connector for data and unit power
- 2.4 GHz or 5 GHz version available
- Notebook with Linux OS (Ubuntu)
- Creates .pcapng files incl. Radiotap

Price target: below EUR 2'000

Availability: planned for 1<sup>st</sup> Qu. 2018

## Planned features:

- 4 channel bonding (up to 1730 Mbps)
- Dual band support (2.4 and 5 GHz)
- Optional integrated battery
- Supporting most Linux's and Mac OS



Multi-Channel WLAN Analyzer



**Joint development of:**  
**Softing IT Networks GmbH**  
85540 Haar, Germany and  
**GHMT AG**  
66450 Bexbach, Germany





802.11n

802.11n/ac Physical Rate Table (Mbps)									
Number of Streams	Modulation	Antennas		Spatial Streams	Maximum Rate (Mbps)				Band Support
		Tx	Rx		1 Ch.	2 Ch.	4 Ch.	8 Ch.	
One Stream*	64-QAM	1	1	1	72	150	n.a.	n.a.	2.4 & 5 GHz
Two Streams*	64-QAM	2	2	2	144	300	n.a.	n.a.	2.4 & 5 GHz
Three Streams	64-QAM	3	3	3	216	450	n.a.	n.a.	2.4 & 5 GHz
Four Streams	64-QAM	4	4	4	288	600	n.a.	n.a.	2.4 & 5 GHz

\* AirPcap Nx supports Legacy, HT20 or HT40 mode (no SGI & Greenfield mode)



802.11ac  
Wave 1

One Stream	256-QAM	1	1	1	86	200	433	n.a.	5 GHz
Two Streams	256-QAM	2	2	2	173	400	866	n.a.	5 GHz
Three Streams	256-QAM	3	3	3	289	600	1300	n.a.	5 GHz



802.11ac  
Wave 2

One Stream	256-QAM	1	1	1	86	200	433	866	5 GHz
Two Streams	256-QAM	2	2	2	173	400	866	1730	5 GHz
Three Streams	256-QAM	3	3	3	289	600	1300	2600	5 GHz
Four Streams	256-QAM	4	4	4	385	800	1730	3470	5 GHz
Eight Streams	256-QAM	8	8	8	770	1600	3470	6930	5 GHz

Softing WLAN Analyzer will support up to 4 channels per WLAN adapter



Softing WLAN Analyzer configuration menu including **Longterm Monitoring** feature:

- Using **Dumpcap** to write packets directly to a file without starting Wireshark
- Creates an individual **pcapng file** per WLAN adapter, a new one every **5 Minutes**
- Packet size (Snaplen) is set to **500 Bytes**

GHMT Channel Settings

Available adapters:

Adapter No.	Channel No.	Channel Options
wlan1	36	HT40+
wlan2	40	HT40+
wlan3	44	HT20
wlan4	48	HT20

Buttons: Set Channels, Set Channels and start Wireshark menu, Set Channels and start Wireshark capturing, Start Longterm Monitoring

Count available adapters: 4

Wireshark - Capture Interfaces

Input Output Options

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (M)	Monito	Capture Filter
▶ wlan0		Ethernet	<input checked="" type="checkbox"/>	default	2	<input type="checkbox"/>	
wlan1		802.11 plus radiotap header	<input checked="" type="checkbox"/>	default	2	<input type="checkbox"/>	
wlan2		802.11 plus radiotap header	<input checked="" type="checkbox"/>	default	2	<input type="checkbox"/>	
wlan3		802.11 plus radiotap header	<input checked="" type="checkbox"/>	default	2	<input type="checkbox"/>	
wlan4		802.11 plus radiotap header	<input checked="" type="checkbox"/>	default	2	<input type="checkbox"/>	
any		Linux cooked	<input checked="" type="checkbox"/>	default	2	—	
▶ Loopback: lo		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
eth0		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
bluetooth0		Bluetooth HCI ... pseudo-header	<input checked="" type="checkbox"/>	default	2	—	
nflg		Linux netfilter log messages	<input checked="" type="checkbox"/>	default	2	—	

Enable promiscuous mode on all interfaces

Capture filter for selected interfaces:

Buttons: Manage Interfaces..., Compile BPFs, Help, Close, Start







Channels 36,40,44,48.pcapng [Frank Lindner - Wireless Applications - GHMT AG]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + NoBeacon

No.	Time	Source	Destination	Channel	TX Rate	Size	RSSI	Protocol	Info
56...	87.916435	Apple_03:2c:9f	Apple_a9:3b:31	36	24	74	-64 dBm	802...	Null function (No data), SN=3...
56...	87.916445		Apple_03:2c:9...	36	24	60	-85 dBm	802...	Acknowledgement, Flags=.....
56...	87.916435	Apple_03:2c:9f	Apple_a9:3b:31	40	24	74	-64 dBm	802...	Null function (No data), SN=3...
56...	87.916445		Apple_03:2c:9...	40	24	60	-77 dBm	802...	Acknowledgement, Flags=.....
56...	87.962199	Apple_a9:3b:31	Broadcast	36	6	310	-82 dBm	802...	Beacon frame, SN=3744, FN=0,
56...	88.064576	Apple_a9:3b:31	Broadcast	36	6	310	-83 dBm	802...	Beacon frame, SN=3745, FN=0,
56...	88.137439	Apple_b2:4c:4d	Broadcast	36	6	157	-70 dBm	802...	Probe Request, SN=18, FN=0, F
56...	88.137927	Apple_a9:3b:31	Apple_b2:4c:4d	36	6	304	-81 dBm	802...	Probe Response, SN=3746, FN=0
56...	88.137967		Apple_a9:3b:3...	36	6	60	-70 dBm	802...	Acknowledgement, Flags=.....
56...	88.157919	Apple_b2:4c:4d	Broadcast	36	6	157	-71 dBm	802...	Probe Request, SN=19, FN=0, F
56...	88.158431	Apple_a9:3b:31	Apple_b2:4c:4d	36	6	304	-81 dBm	802...	Probe Response, SN=3748, FN=0
56...	88.158439		Apple_a9:3b:3...	36	6	60	-71 dBm	802...	Acknowledgement, Flags=.....
56...	88.166872	Apple_a9:3b:31	Broadcast	36	6	310	-82 dBm	802...	Beacon frame, SN=3747, FN=0,
56...	88.270088	Apple_b2:4c:4d	Broadcast	48	6	157	-58 dBm	802...	Probe Request, SN=24, FN=0, F
56...	88.181768	Apple_b2:4c:4d	Broadcast	40	6	157	-38 dBm	802...	Probe Request, SN=20, FN=0, F
56...	88.290585	Apple_b2:4c:4d	Broadcast	48	6	157	-57 dBm	802...	Probe Request, SN=25, FN=0, F
56...	88.202162	Apple_b2:4c:4d	Broadcast	40	6	157	-38 dBm	802...	Probe Request, SN=21, FN=0, F
56...	88.225988	Apple_b2:4c:4d	Broadcast	44	6	157	-64 dBm	802...	Probe Request, SN=22, FN=0, F
56...	88.269272	Apple_a9:3b:31	Broadcast	36	6	310	-81 dBm	802...	Beacon frame, SN=3749, FN=0,

▶ Frame 5620: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0  
▶ Radiotap Header v0, Length 50  
▶ 802.11 radio information  
▶ IEEE 802.11 Null function (No data), Flags: ...P...T

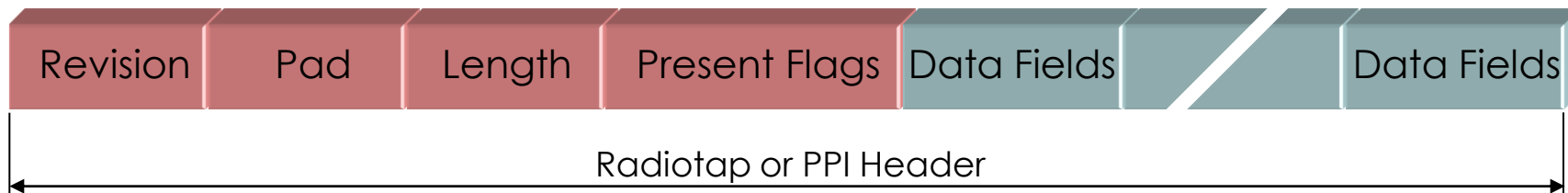
```
0000 00 00 32 00 2f 40 00 a0 20 08 00 a0 20 08 00 a0  ..2./@..  ... ..
0010 20 08 00 a0 20 08 00 00 84 28 86 0f 00 00 00 00  ... .. (. ....
0020 00 30 3c 14 40 01 c5 00 00 00 c3 00 b7 01 bd 02  .0<.@...  ....
0030 c0 03 48 11 2c 00 20 c9 d0 a9 3b 31 e0 5f 45 03  ..H,..  ..;1_E.
0040 2c 9f 20 c9 d0 a9 3b 31 90 16  ,. ....;1 ..
```

Channels 36,40,44,48 Packets: 6173 · Displayed: 6173 (100.0%) Profile: WLAN 3.3 LNS

Simultaneous capturing in channels 36, 40, 44 & 48



**LIVE DEMONSTRATION  
SOFTING WLAN ANALYZER**



- ▶ Radiotap or the newer PPI (Per Packet Information) are so called *pseudo-headers* because they are not transmitted with the frame.
- ▶ They are added by the driver during reception and contain additional radio information about the frame.
- ▶ Receive signal strength, bit rate, channel number and other fields are added
- ▶ These fields can be added as columns in Wireshark and support troubleshooting
- ▶ Some other driver (i.e. MAC OS X) may also add these headers

More detailed information:

Radiotap: <http://www.radiotap.org/Radiotap>

PPI manual: [http://www.cacotech.com/documents/PPI\\_Header\\_format\\_1.0.1.pdf](http://www.cacotech.com/documents/PPI_Header_format_1.0.1.pdf)



WLAN Beacon.pcap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000	CiscoInc_11:1f:60	Broadcast	802.11	188	Beacon frame, SN=9, FN=0, Flags=....., BI=100, SSID=LNSWLAN
2	0.025	CiscoInc_11:1f:60	Broadcast	802.11	188	Beacon frame, SN=10, FN=0, Flags=....., BI=100, SSID=LNSWLAN
3	0.102	CiscoInc_11:1f:60	Broadcast	802.11	188	Beacon frame, SN=11, FN=0, Flags=....., BI=100, SSID=LNSWLAN

> Frame 1: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)

- > Radiotap Header v0, Length 18
- > 802.11 radio information
- > IEEE 802.11 Beacon frame, Flags: .....
- > IEEE 802.11 wireless LAN management frame

**← Radiotap Pseudo-Header added by AirPcap Classic**

WLAN Beacon 11ac.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	CiscoInc_1f:4e:2e	Broadcast	802.11	341	Beacon frame, SN=1802, FN=0, Flags=.....C, BI=102, SSID=LNS-LAB-5.5
2	0.104375	CiscoInc_1f:4e:2e	Broadcast	802.11	341	Beacon frame, SN=1803, FN=0, Flags=.....C, BI=102, SSID=LNS-LAB-5.5
3	0.104487	CiscoInc_1f:4e:2e	Broadcast	802.11	341	Beacon frame, SN=1804, FN=0, Flags=.....C, BI=102, SSID=LNS-LAB-5.5

> Frame 1: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface 0

- > PPI version 0, 32 bytes
- > 802.11 radio information
- > IEEE 802.11 Beacon frame, Flags: .....C
- > IEEE 802.11 wireless LAN management frame

**← PPI Pseudo-Header added by AirPcap NX**

```

0000 00 00 20 00 69 00 00 00 02 00 14 00 dd 59 81 c5  ..i... ..Y..
0010 00 00 00 00 01 00 0c 00 7c 15 40 01 00 00 ed a6  .....|.@....
0020 80 00 00 00 ff ff ff ff ff ff 7a 05 00 05 4e 2e  +R.N
  
```



- Create a Wireshark profile for WLAN settings
- Add columns with radio information values from the PPI header
- Add specific Quick Filter buttons with management & control frames

**Add Quick Filter buttons**

No.	Time	Source	Destination	Protocol	Length	Signal	Noise	TX Speed	Channel	Info
1	0.000000	CiscoInc_1f:4e:2e	Broadcast	802.11	341	-19	-90	6.0	100	Beacon frame, SN=1802, FN=0, Flags=.....C, BI=1...
2	0.104375	CiscoInc_1f:4e:2e	Broadcast	802.11	341	-19	-90	6.0	100	Beacon frame, SN=1803, FN=0, Flags=.....C, BI=1...
3	0.104487	CiscoInc_1f:4e:2e	Broadcast	802.11	341	-19	-90	6.0	100	Beacon frame, SN=1804, FN=0, Flags=.....C, BI=1...
4	0.104489	CiscoInc_1f:4e:2e	Broadcast	802.11	341	-19	-90	6.0	100	Beacon frame, SN=1805, FN=0, Flags=.....C, BI=1...
5	0.104381	CiscoInc_1f:4e:2e	Broadcast	802.11	341	-19	-90	6.0	100	Beacon frame, SN=1806, FN=0, Flags=.....C, BI=1...
6	0.104517	CiscoInc_1f:4e:2e	Broadcast	802.11	341	-19	-90	6.0	100	Beacon frame, SN=1807, FN=0, Flags=.....C, BI=1...
7	0.104361	CiscoInc_1f:4e:2e	Broadcast	802.11	341	-19	-90	6.0	100	Beacon frame, SN=1808, FN=0, Flags=.....C, BI=1...

> Frame 1: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface 0  
 > PPI version 0, 32 bytes  
 > 802.11 radio information  
   PHY type: 802.11a (5)  
   Turbo type: Non-turbo (0)  
   Data rate: 6.0 Mb/s  
   Channel: 100  
   Frequency: 5500 MHz  
   Signal strength (dBm): -19 dBm  
   Noise level (dBm): -90 dBm  
   TSF timestamp: 3313588701  
 > [Duration: 436 us]

Use these fields to Apply as Column

0.0%) · Load time: 0:0.0

Profile: LNS WLAN PPI



To add different **channel colors** select → View → Coloring Rules...

WLAN Probe Request Channel 1 6 11.pcapng

File Edit **View** Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	TA	RA	Data rate (Mb/s)	Channel	SNR	Length	Info
1	0.000	IntelCor_79:46:04	Broadcast	1	11	-29 dBm	122	Probe Request, SN=4,
2	0.001	IntelCor_79:46:04	Broadcast	1	11	-30 dBm	122	Probe Request, SN=5,
3	0.001	IntelCor_79:46:04	Broadcast	1	11	-30 dBm	108	Probe Request, SN=6,
4	0.000	IntelCor_79:46:04	Broadcast	1	11	-30 dBm		
5	0.033	IntelCor_79:46:04	Broadcast	1	11	-31 dBm		
6	0.003	IntelCor_79:46:04	Broadcast	1	11	-31 dBm		
7	0.107	IntelCor_79:46:04	Broadcast	1	6	-32 dBm		
8	0.038	IntelCor_79:46:04	Broadcast	1	6	-33 dBm		
9	0.012	IntelCor_79:46:04	Broadcast	1	6	-30 dBm		
10	0.003	IntelCor_79:46:04	Broadcast	1	6	-31 dBm		
11	0.003	IntelCor_79:46:04	Broadcast	1	6	-38 dBm		
12	0.013	IntelCor_79:46:04	Broadcast	1	6	-32 dBm		
13	0.145	IntelCor_79:46:04	Broadcast	1	1	-37 dBm		
14	0.001	IntelCor_79:46:04	Broadcast	1	1	-38 dBm		
15	0.001	IntelCor_79:46:04	Broadcast	1	1	-40 dBm		
16	0.001	IntelCor_79:46:04	Broadcast	1	1	-43 dBm		

Wireshark · Coloring Rules · LNS WLAN RadioTap

Name	Filter
<input checked="" type="checkbox"/> Bad TCP	tcp.analysis.flags
<input checked="" type="checkbox"/> HSRP State Change	hsrp.state != 8 && hsrp.state != 16
<input checked="" type="checkbox"/> Spanning Tree Topology Change	stp.type == 0x80
<input checked="" type="checkbox"/> OSPF State Change	ospf.msg != 1
<input checked="" type="checkbox"/> ICMP errors	icmp.type eq 3    icmp.type eq 4    icmp.type eq 5
<input checked="" type="checkbox"/> ARP	arp
<input checked="" type="checkbox"/> ICMP	icmp    icmpv6
<input checked="" type="checkbox"/> TCP RST	tcp.flags.reset eq 1
<input checked="" type="checkbox"/> TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && ! ip.multicast)
<input type="checkbox"/> Checksum Errors	cdp.checksum_bad==1    edp.checksum_bad==1
<input checked="" type="checkbox"/> SMB	smb    nbss    nbns    nbpx    ipxsap    netbios
<input checked="" type="checkbox"/> HTTP	http    tcp.port == 80
<input checked="" type="checkbox"/> IPX	ipx    spx
<input checked="" type="checkbox"/> DCERPC	dcerpc
<input checked="" type="checkbox"/> Routing	hsrp    eigrp    ospf    bgp    cdp    vrrp    gre
<input checked="" type="checkbox"/> TCP SYN/FIN	tcp.flags & 0x02    tcp.flags.fin == 1
<input checked="" type="checkbox"/> TCP	tcp
<input checked="" type="checkbox"/> UDP	udp
<input checked="" type="checkbox"/> Broadcast	eth[0] & 1
<input checked="" type="checkbox"/> Channel 1	radiotap.channel.freq == 2412
<input checked="" type="checkbox"/> Channel 6	radiotap.channel.freq == 2437
<input checked="" type="checkbox"/> Channel 11	radiotap.channel.freq == 2462



## 802.11 Frame Types Overview

### Management Frames:

- Beacon
- Probe Request & Response
- Authentication & Deauthentication
- Association & Disassociation
- Reassociation Request & Response
- Action

### Control Frames:

- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledge / Block Acknowledge Request / Block Acknowledge
- Power Save Poll

### Data Frames:

- Data
- Null Function



# SharkFest '17 Europe

*That's it for part 1, hope to see you back for:*

## **Troubleshooting WLANs (Part 2)**

*Hot News: Including KRACK !!!*