SharkFest '18 Europe

Troubleshooting WLANs (Part 1)

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

Rolf Leutert

Leutert NetServices
Switzerland
www.netsniffing.ch

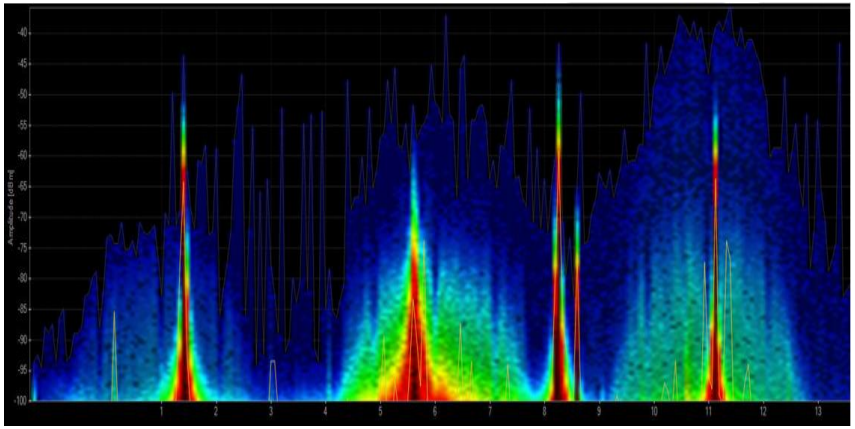
Rolf Leutert, El. Ing. HTL
Leutert NetServices
Zürich-Airport, Switzerland

- 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
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 how to use WiSpy to isolate layer 1 issues
- 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 !

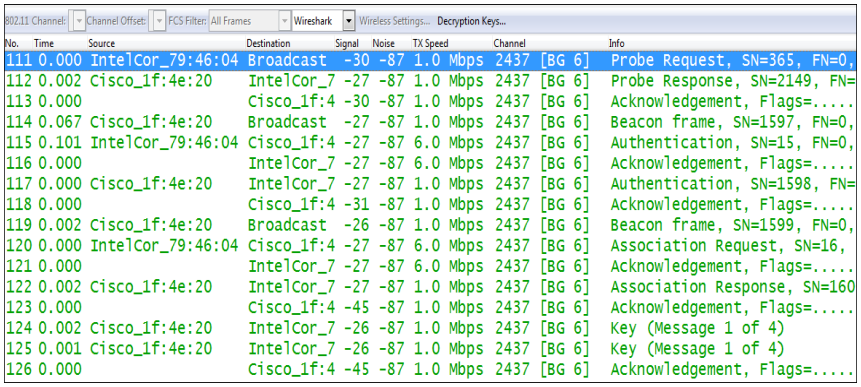


Layer 1 - Physical Access

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, WaveXpert

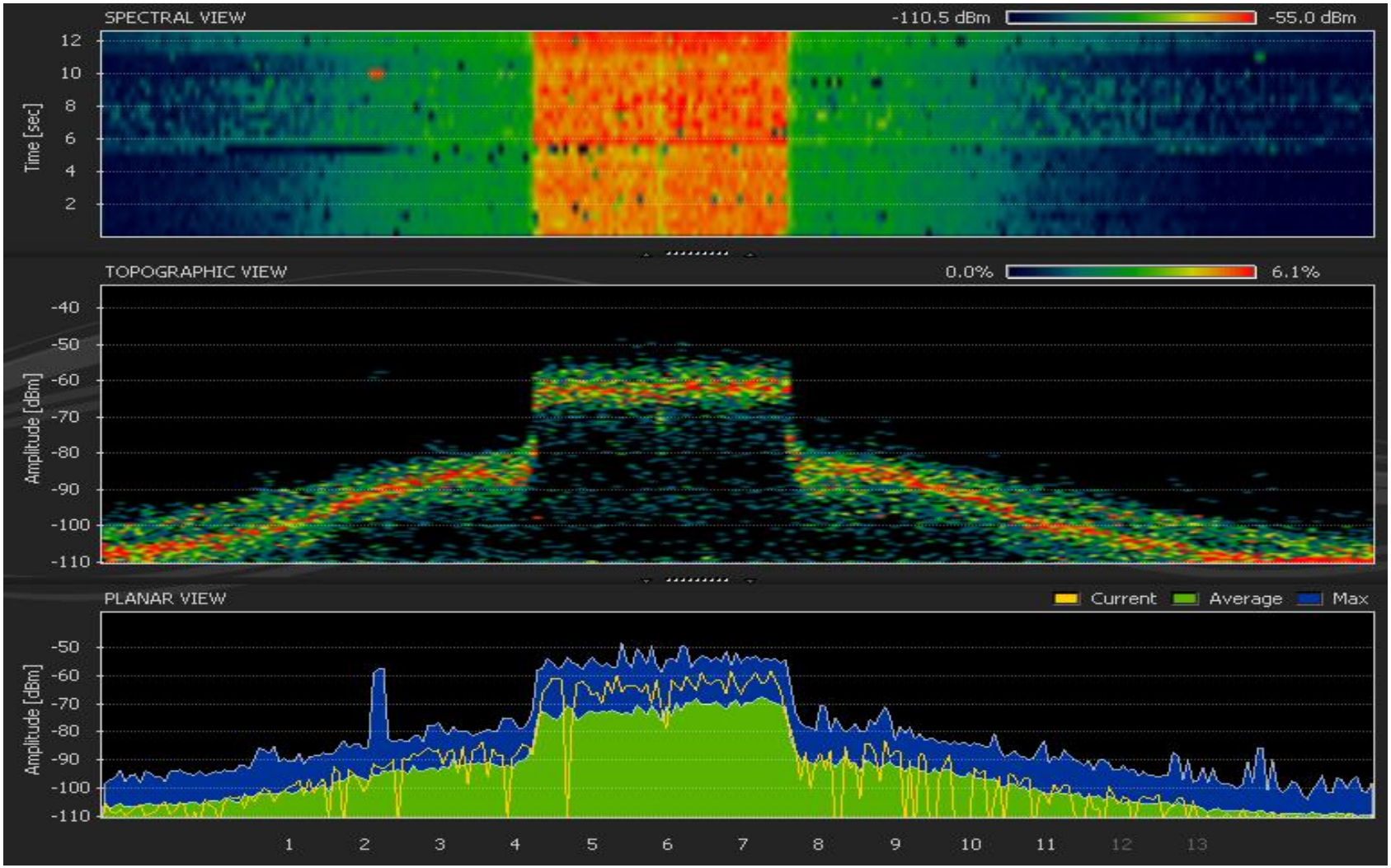
- WLAN Wi Fi devices are working in the 2.4 GHz ISM* and 5 GHz UNII** bands
- But both bands are free for any use, WiFi as well as non-WiFi devices
- Especially the 2.4 GHz band is often crowded with non-WiFi devices
- The only limitation is max. radiated power according to country regulations
- Non-WiFi 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 Chanalizer® software displays and records all layer 1 signals in both 2.4 GHz and 5 GHz bands.

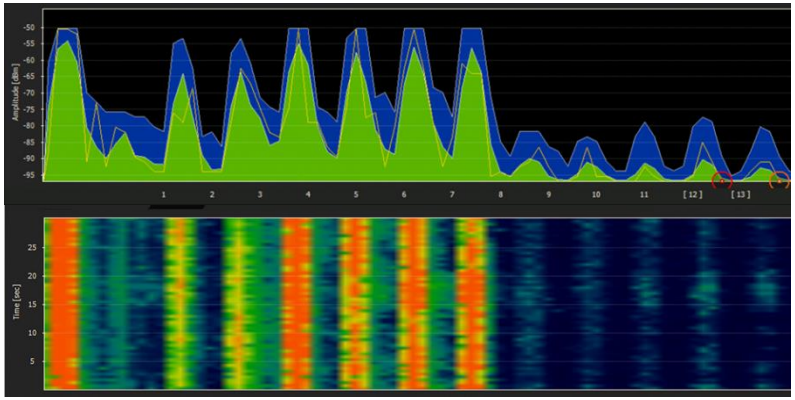
www.metageek.com

* ISM Industrial, Scientific and Medical
**UNII Unlicensed National Information Infrastructure

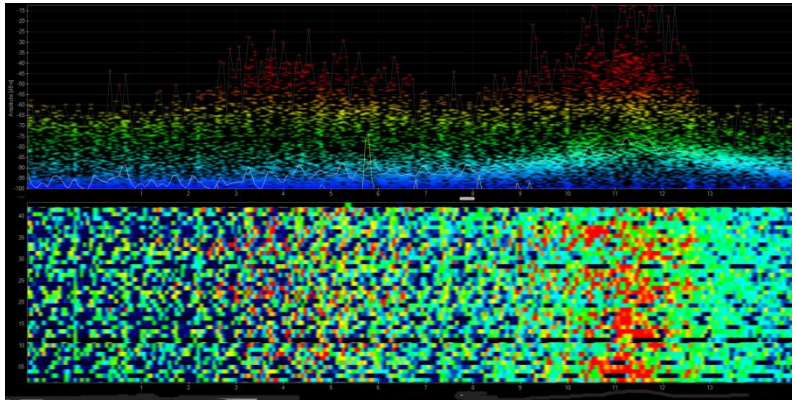
WiFi Device Signature in 2.4 GHz Band



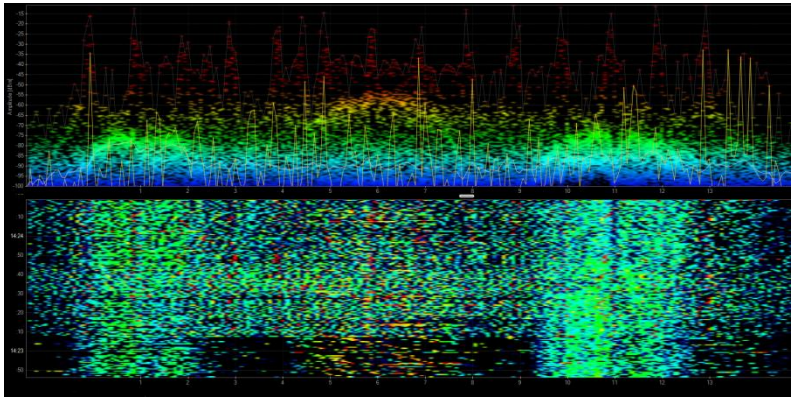
Non-WiFi Device Signatures in 2.4 GHz Band



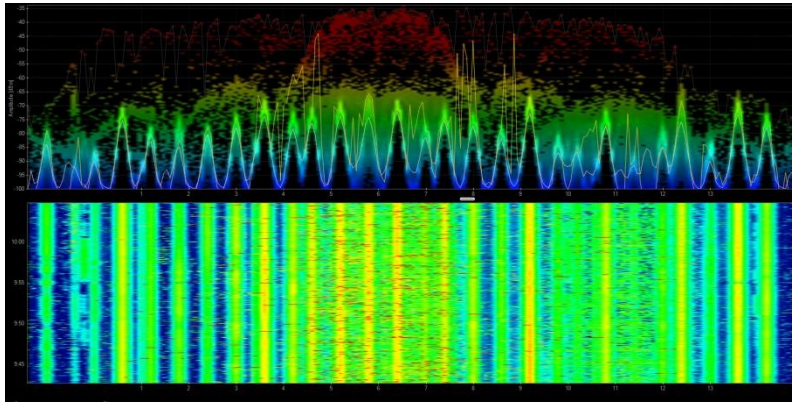
Home trainers in a fitness center



Microwave oven

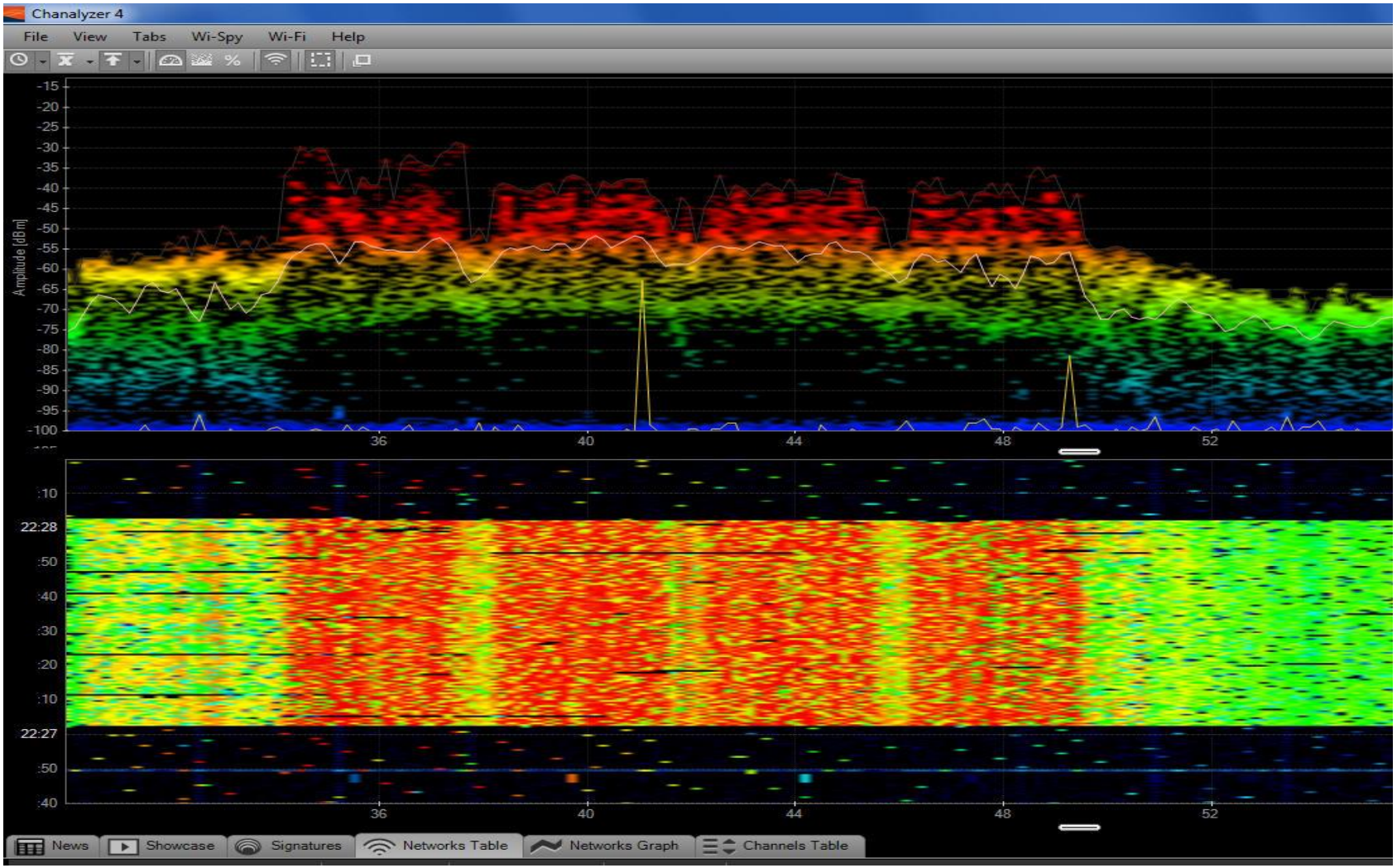


Remote control of model airplanes



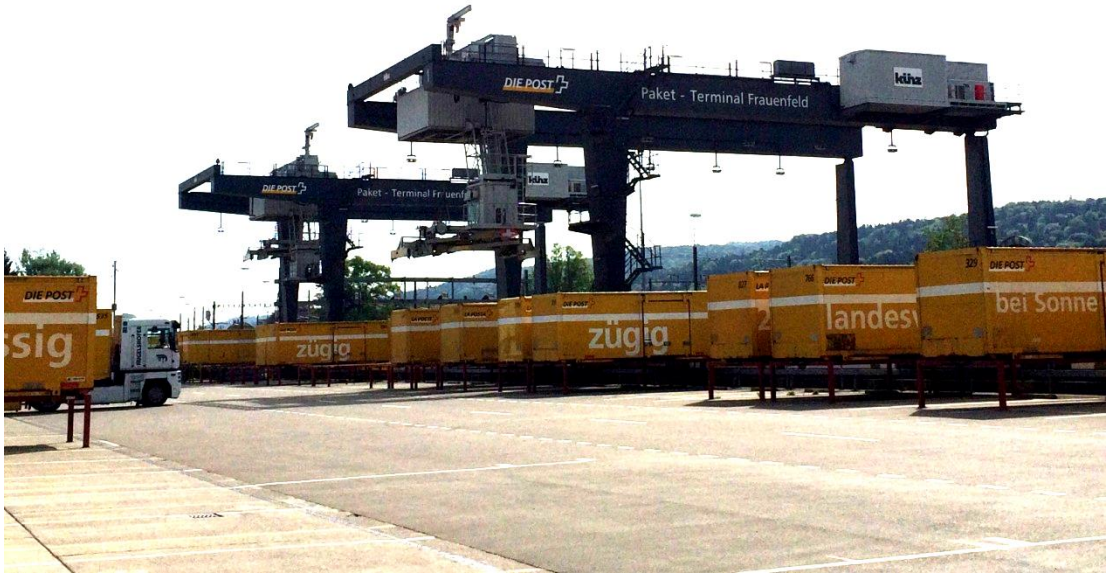
Wireless guitar

WiFi 802.11ac with four bonded channels in 5MHz Band



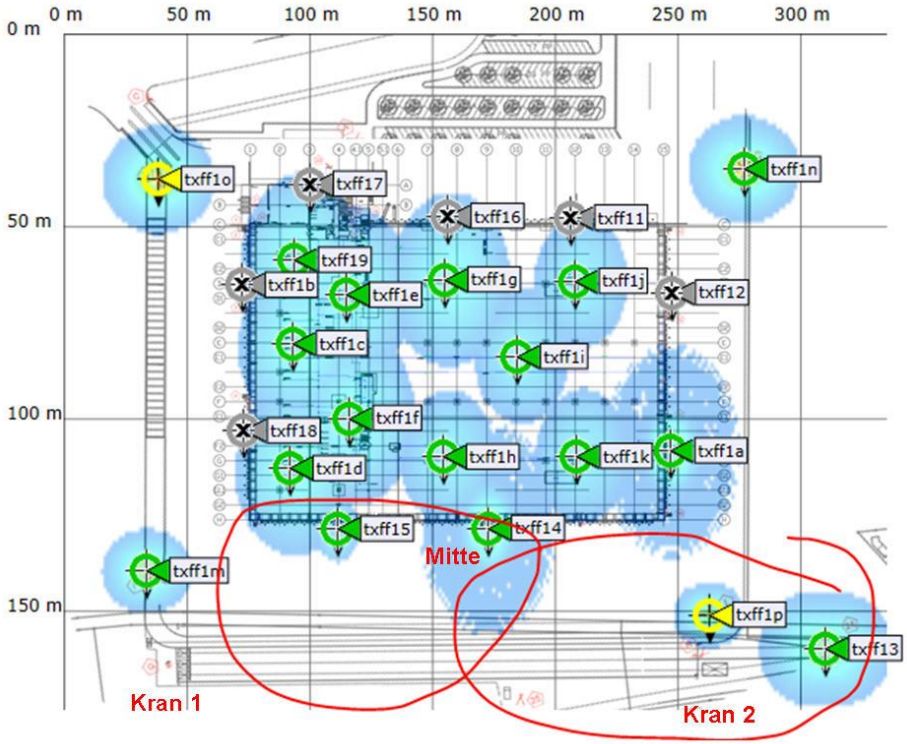
LIVE DEMONSTRATION
WI-SPY & CHANALYZER

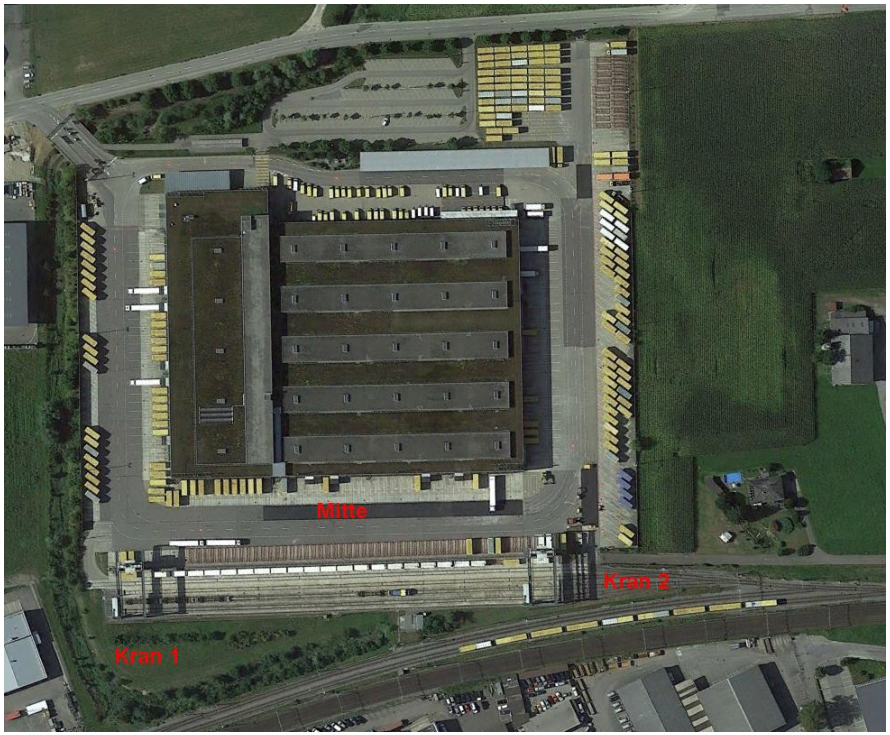
- Large logistic enterprise, depending on WLAN for day-to-day operations
- Two container cranes to load/unload trains require WLAN connections



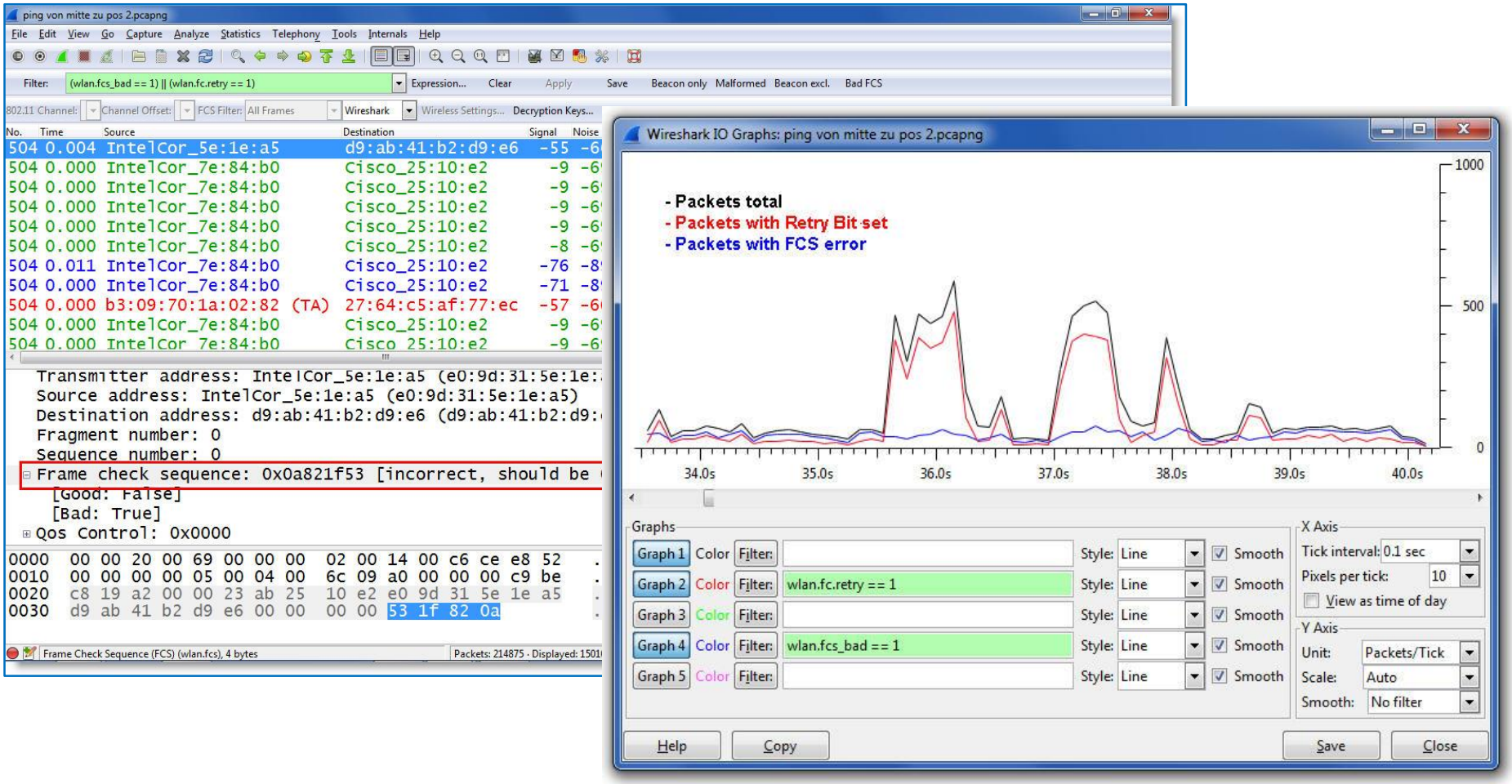
WLAN Layer 1 Analysis (Case one)

- 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



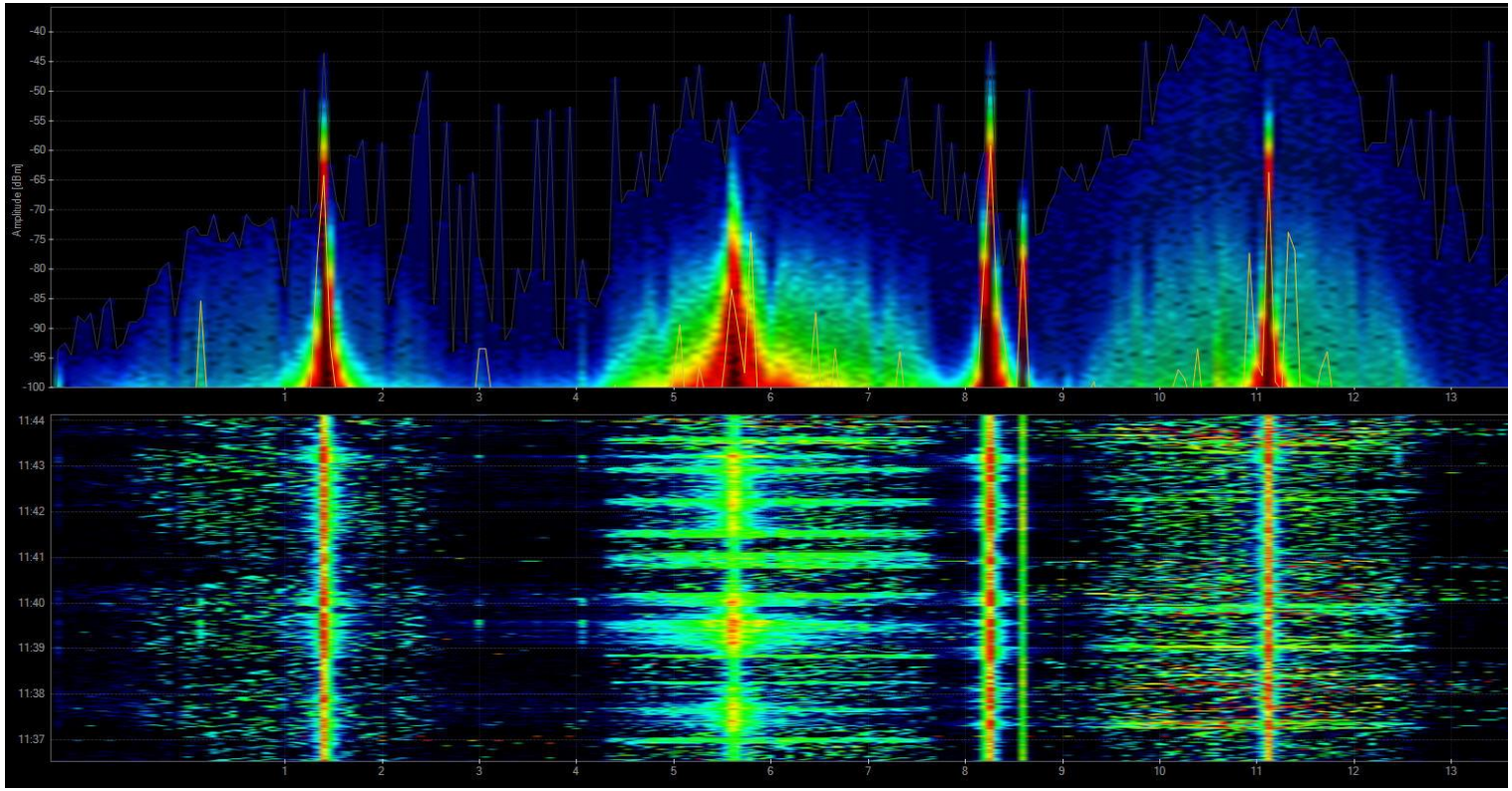


- Starting with layer 2 analysis near crane #2 in channels 1, 6, and 11
- Wireshark shows up to 70% of frames with bad FCS or the Retry Flag set



WLAN Layer 1 Analysis (Case one)

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



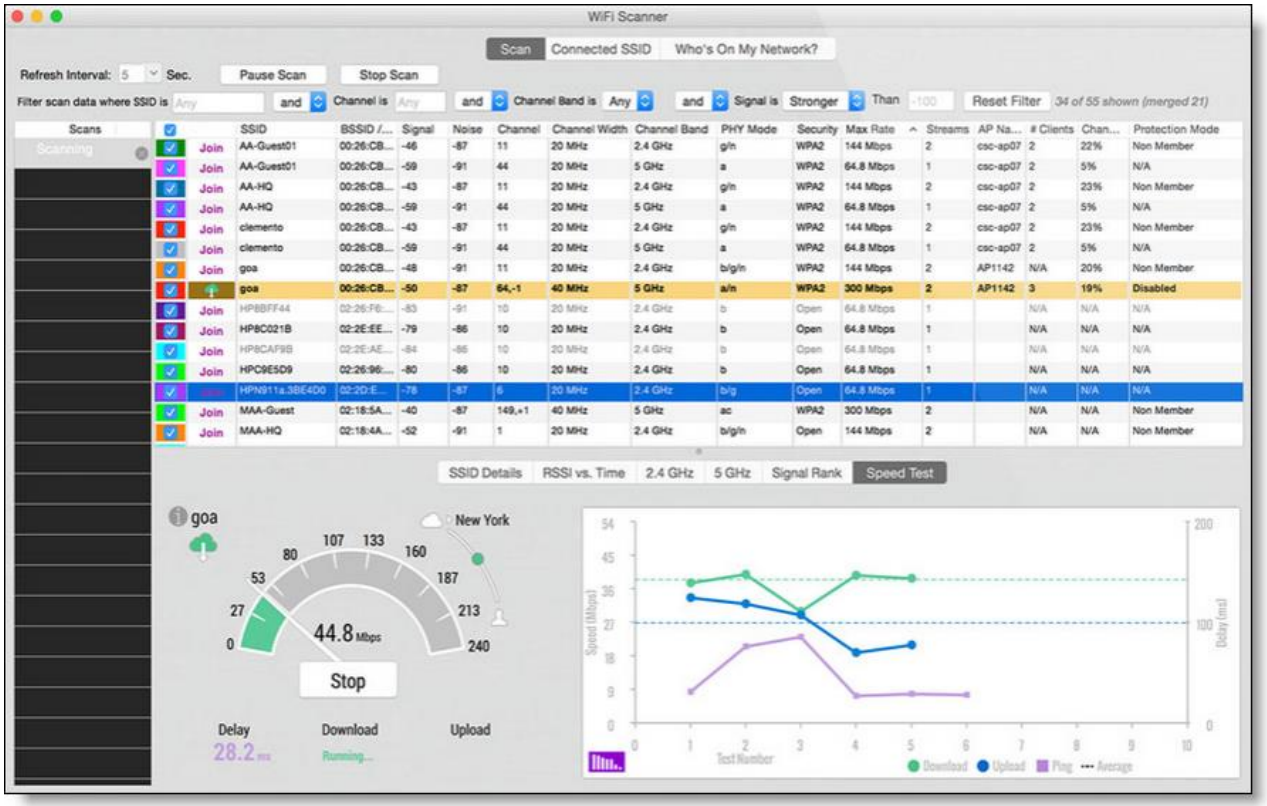
- Signal source is outside of customers campus' → Swiss radio authority informed
- If this transmitting power is within legal limits → Change to 5 GHz band required

- Swiss radio authority (BAKOM) scanned the 2.4 GHz band with their own tool
- They detected a strongly interfering signal caused by a 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



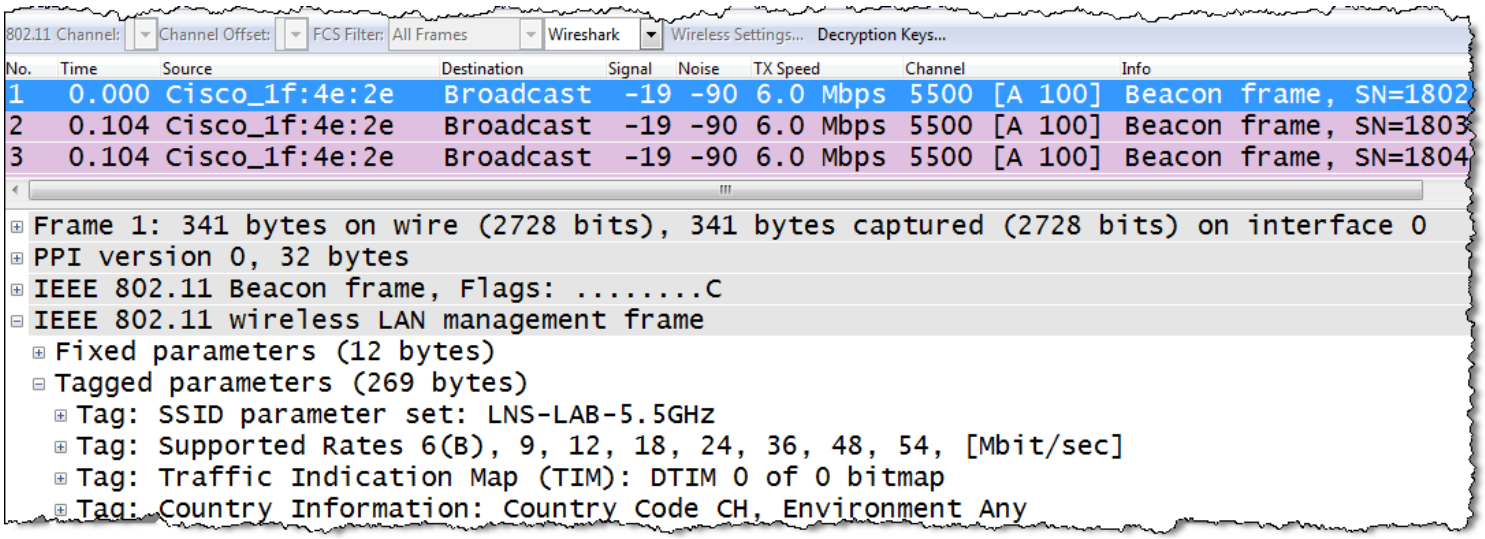
WiFi Scanners (just a few popular ones)

	Acrylic WiFi scanner	www.acrylicwifi.com
	Ekahau HeatMapper	www.ekahau.com
	inSSIDer	www.metageek.com
	NetStumbler	www.netstumbler.com
	Wifi Analyzer (Android)	play.google.com
	WifiInfoView	www.nirsoft.net
	WifiScanner	wifiscanner.sourceforge.net
	Wifi Scanner	www.apple.com/osx/apps/app-store

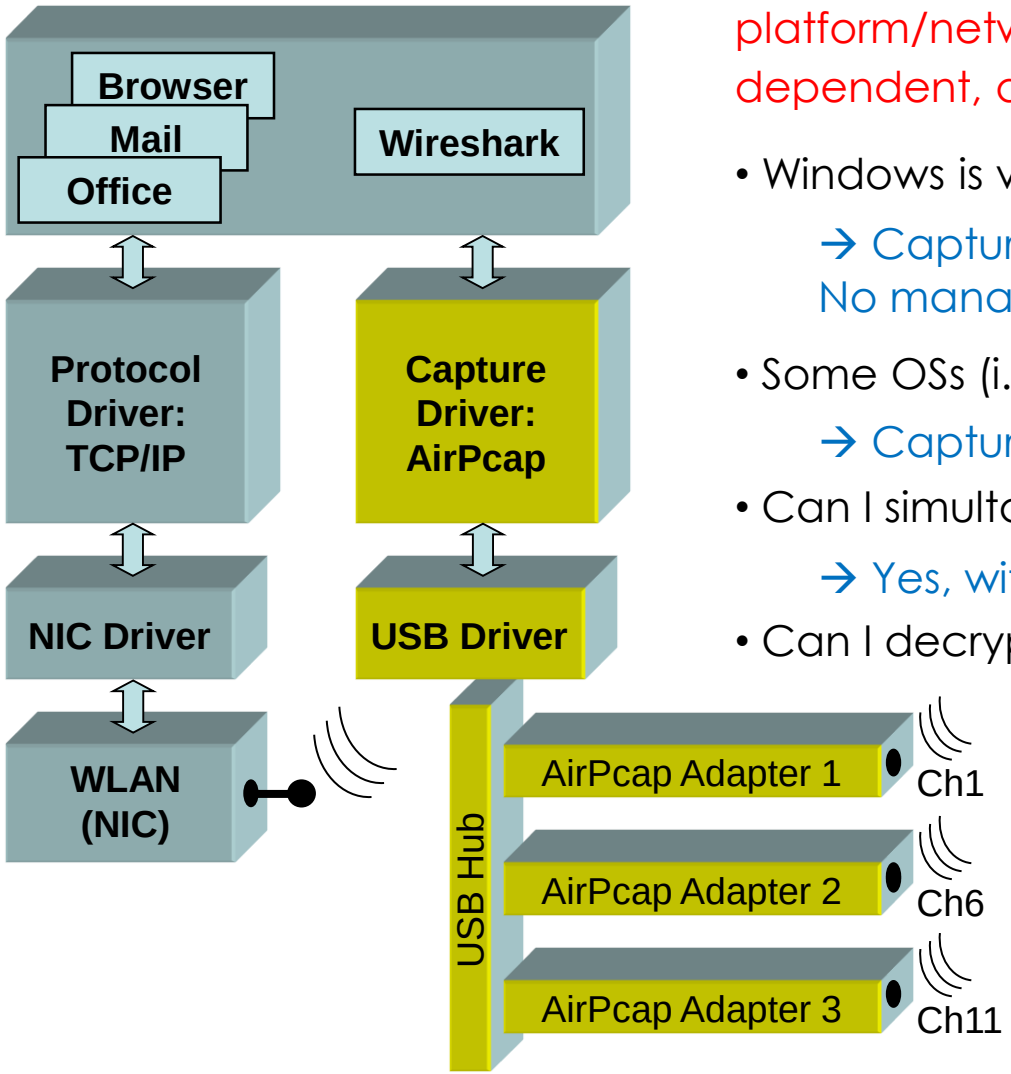
Remark: Apple IOS (iPhone/iPad) has locked direct access to the WiFi interface for stability and other unknown reasons. Jailbreak is required to install and run WiFi Scanner apps on these devices.

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



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



Capturing 802.11 traffic with **built-in NICs** is very platform/network adapter/driver/libpcap dependent, and might not be possible at all !

- Windows is very limited here:

  → Captures only broadcasts & your own traffic
  No management/control frames, fake Ethernet

- Some OSs (i.e. MAC OS) support Monitor Mode

  → Captures all traffic and provides Radio Infos

- Can I simultaneously capture multiple channels?

  → Yes, with external hardware

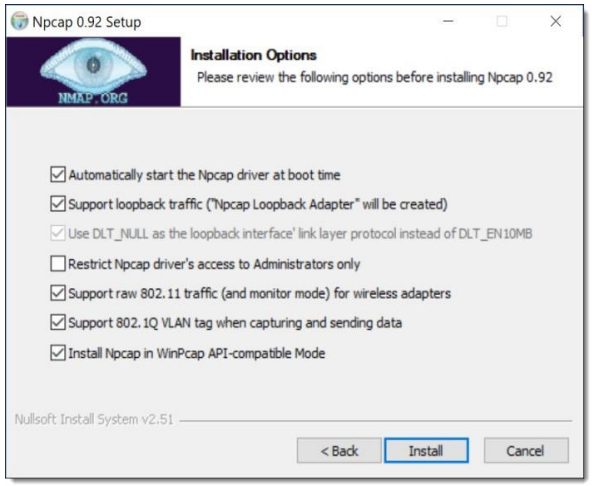
- Can I decrypt 802.11 data packets?

  → Yes, if shared keys are used, if the key is available and the key negotiation process is captured

More information:
wiki.wireshark.org/CaptureSetup/WLAN

Capturing 802.11 Packets (Links)

https://wiki.wireshark.org/CaptureSetup/WLAN



Windows:

- Npcap is an update of WinPcap using NDIS 6 and has many added features https://nmap.org/npcap/#download
- Instruction link: https://wiki.wireshark.org/CaptureSetup/WLAN#Starting_from_Windows_Vista:_Npcap

Linux:

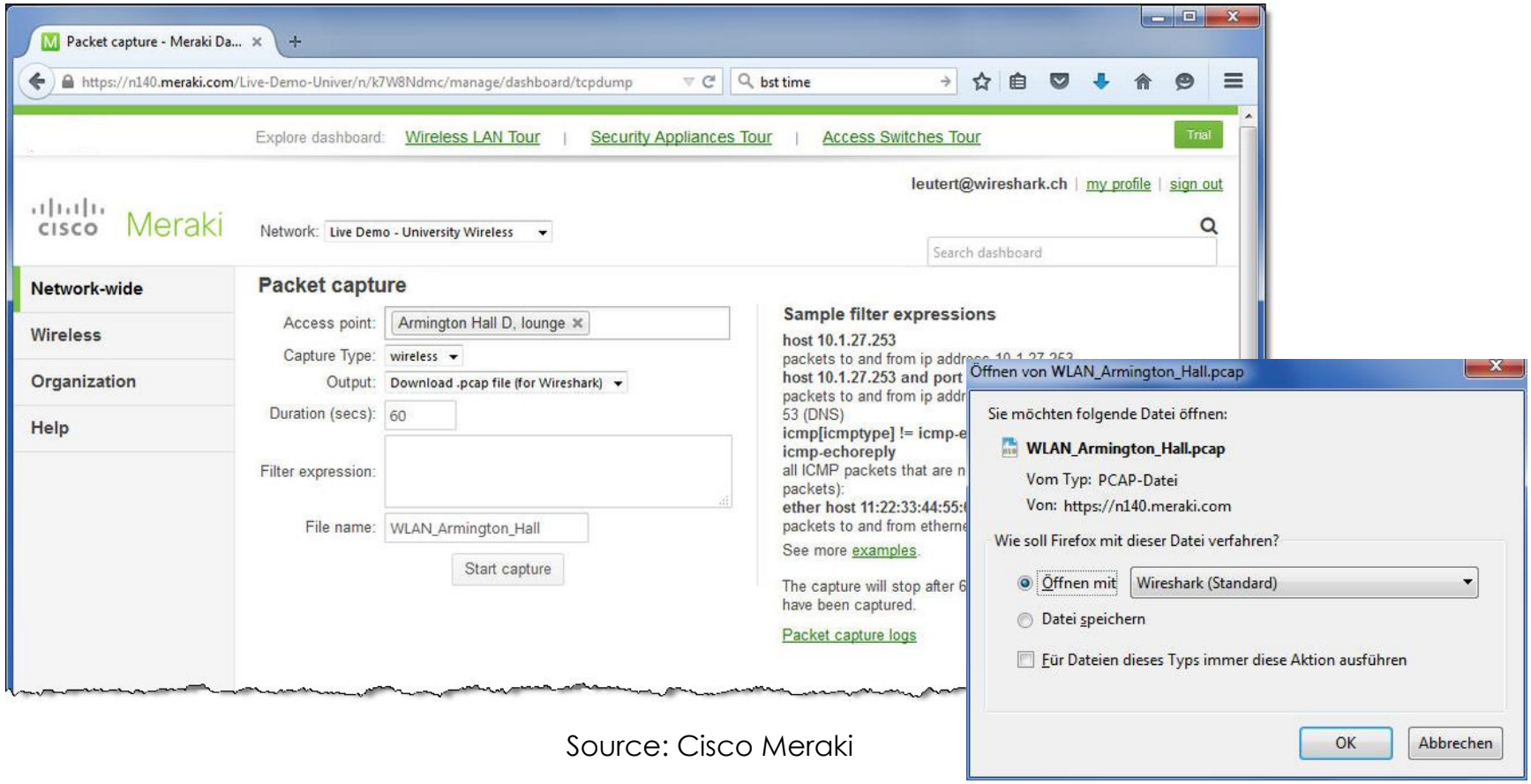
- Instruction link: https://wiki.wireshark.org/CaptureSetup/WLAN#Linux
- Existing Linux Wireless drivers: https://wireless.wiki.kernel.org/en/users/drivers

MAC OS:

- Instruction link: https://wiki.wireshark.org/CaptureSetup/WLAN#Mac_OS_X
- Free Airtool for Wireshark captures from Mac's built-in Wi-Fi adapter: https://www.adriangranados.com/apps/airtool

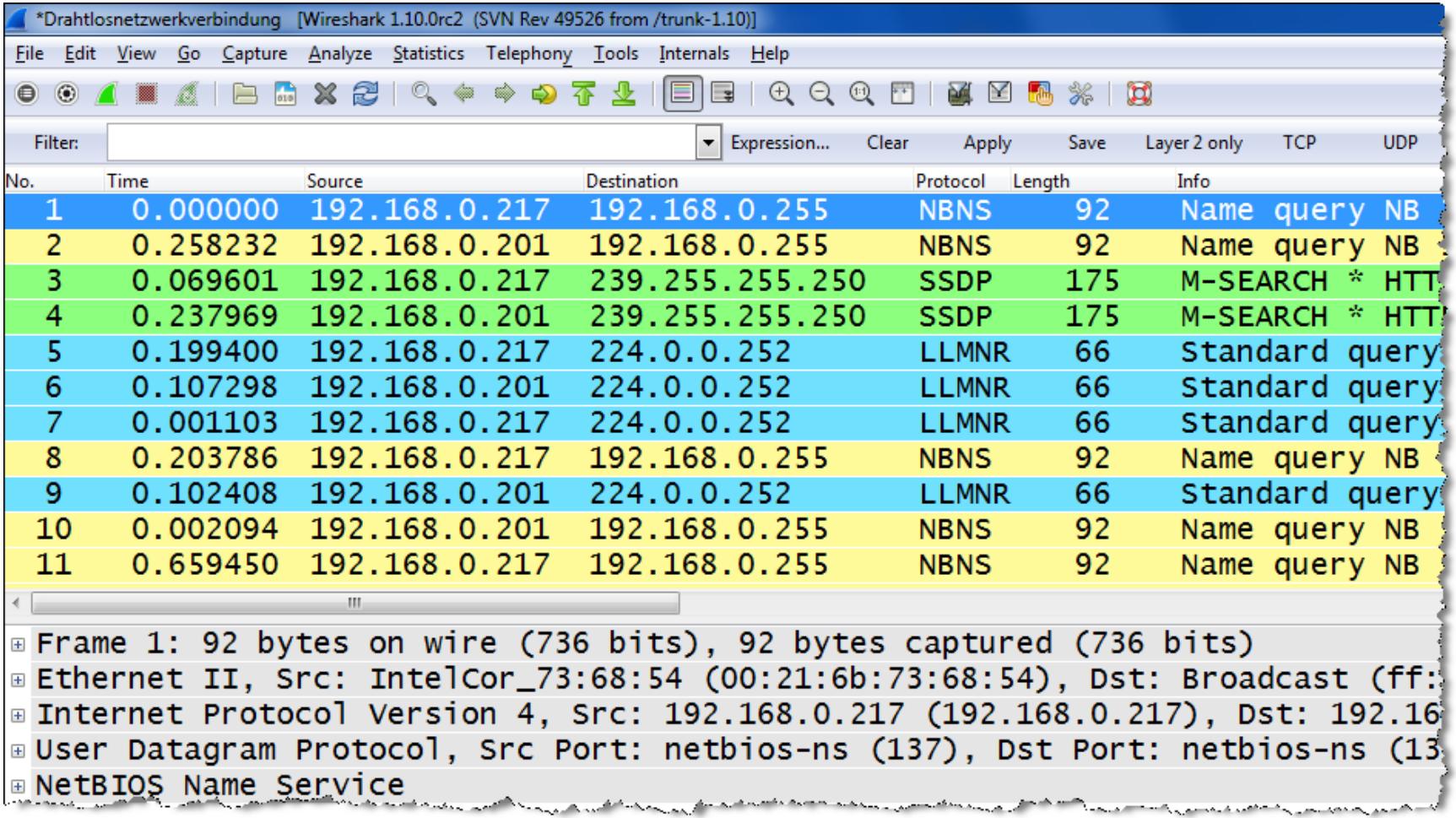
Most of newer Access Points offer remote controlled packet capture features

- Some allow capturing during operation, other must be put into monitor mode
- Even cloud controlled APs (i.e. Meraki) support capturing on wire- or wireless side

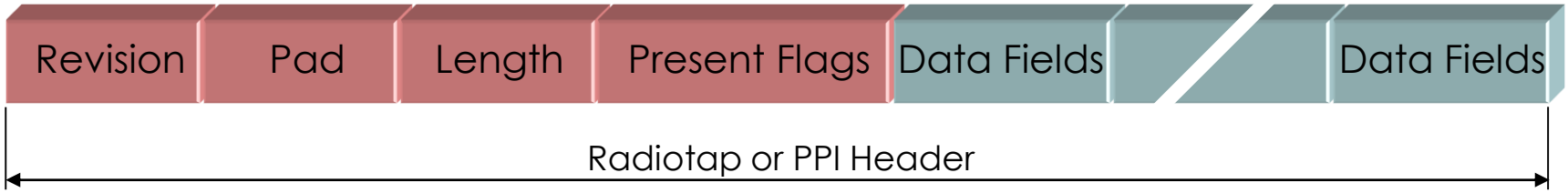


Source: Cisco Meraki

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

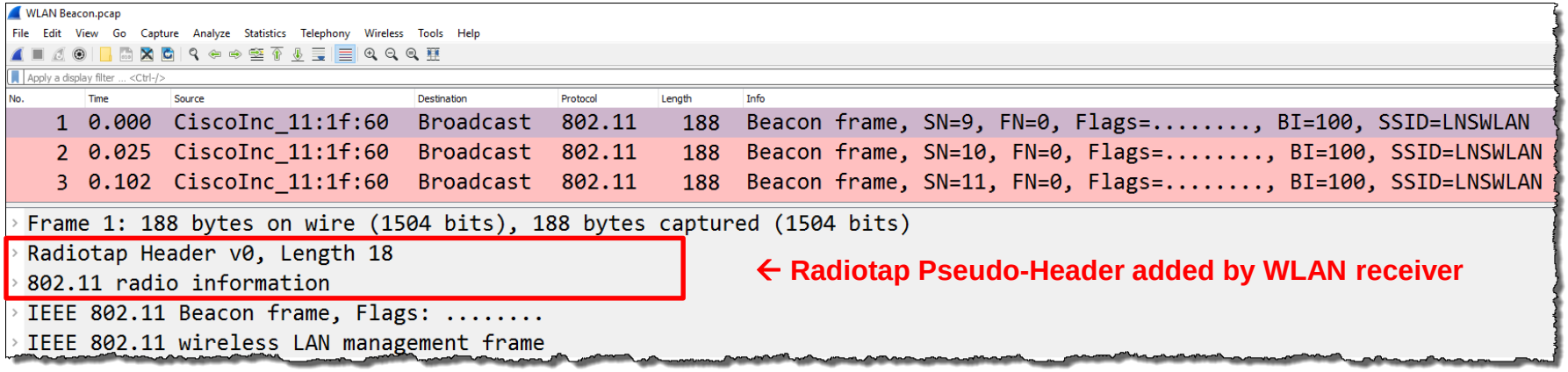


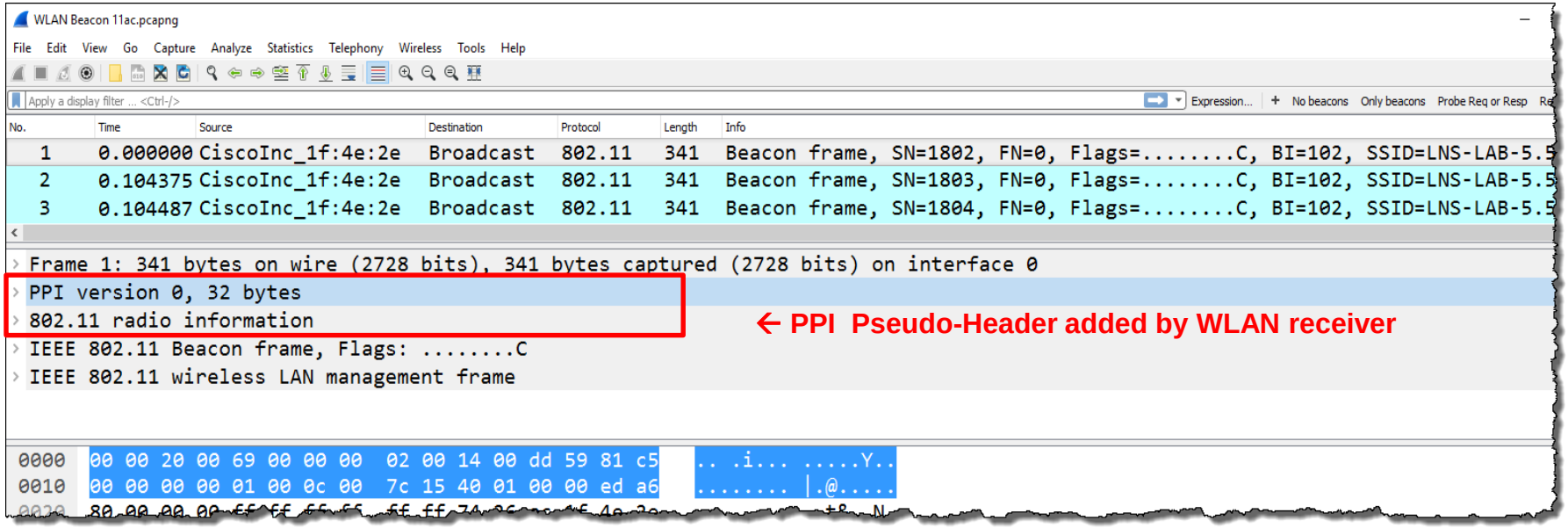
The Radiotap and PPI pseudo-header



- The Radiotap or the PPI (Per Packet Information) are so called *Link-layer 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 incoming frame.
- Provides Receive Signal Strength, bit rate, channel number and other fields
- These fields can be used as columns in Wireshark and support troubleshooting
- Some drivers (i.e. MAC OS) offer a selection of different Link-layer headers, however, the Radiotap header is the most widely supported type.

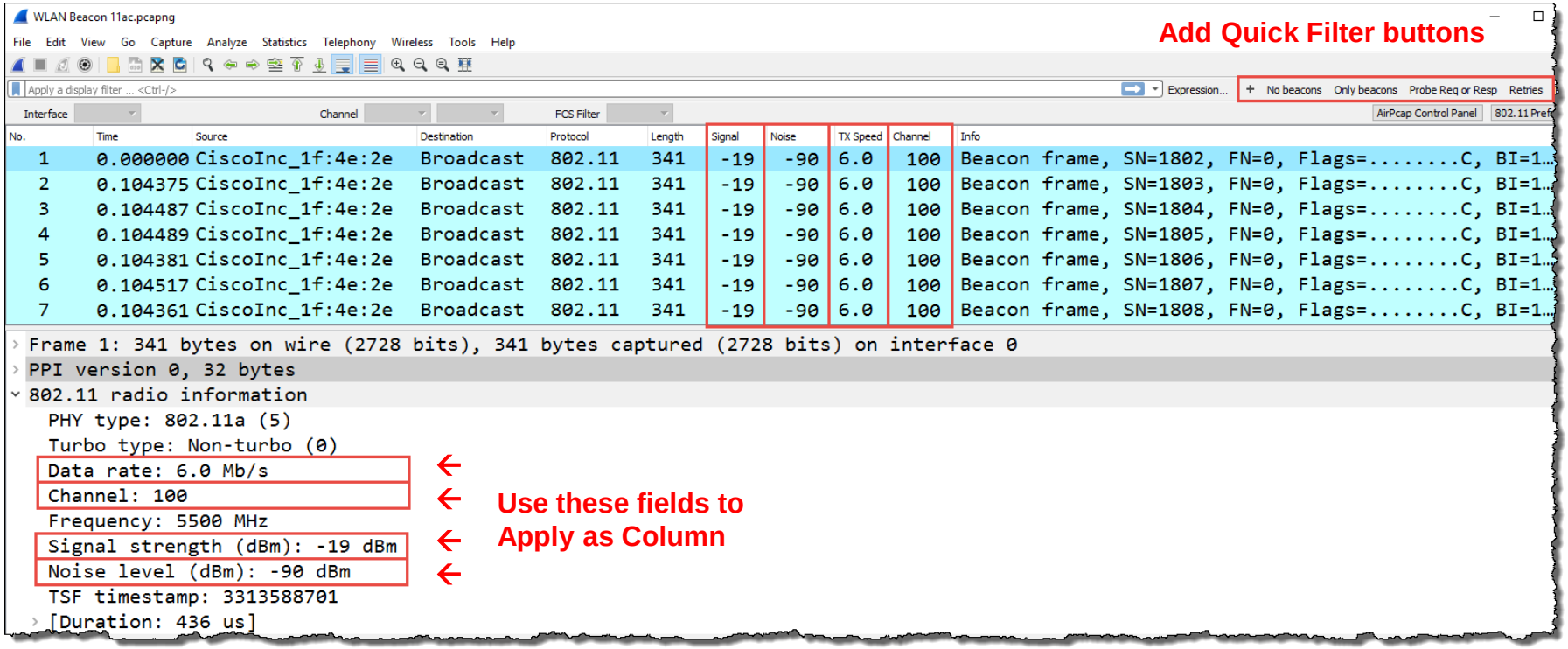
More detailed information:
Radiotap: https://www.radiotap.org/
List of Pseudo-headers: https://www.adriangranados.com/blog/link-layer-header-types


WLAN Beacon.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
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 WLAN receiver

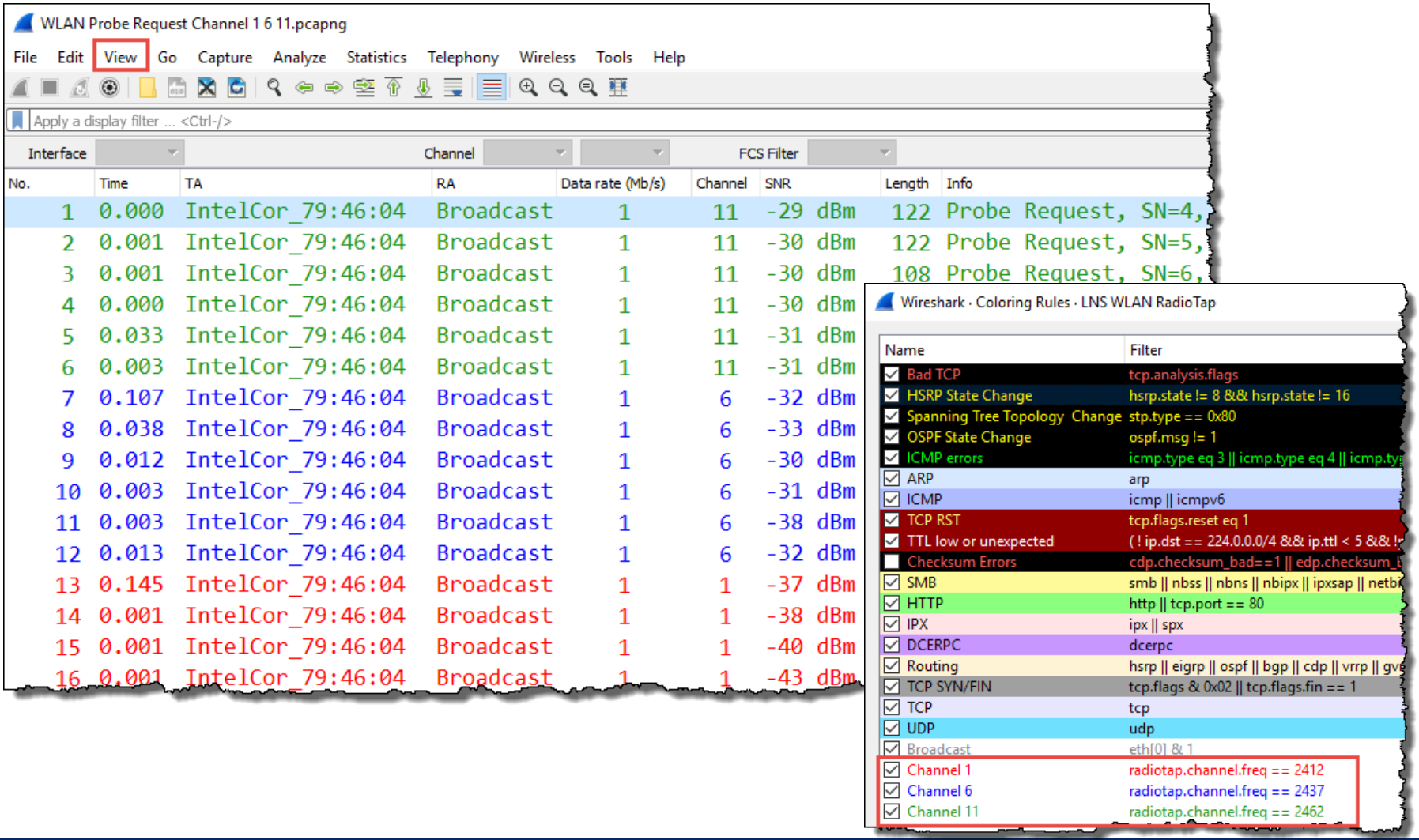

WLAN Beacon 11ac.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression... No beacons Only beacons Probe Req or Resp
No. Time Source Destination Protocol Length Info
1 0.000000 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, 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
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 .... |.@.....
← PPI Pseudo-Header added by WLAN receiver

Customize Wireshark for WLAN analysis

- 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

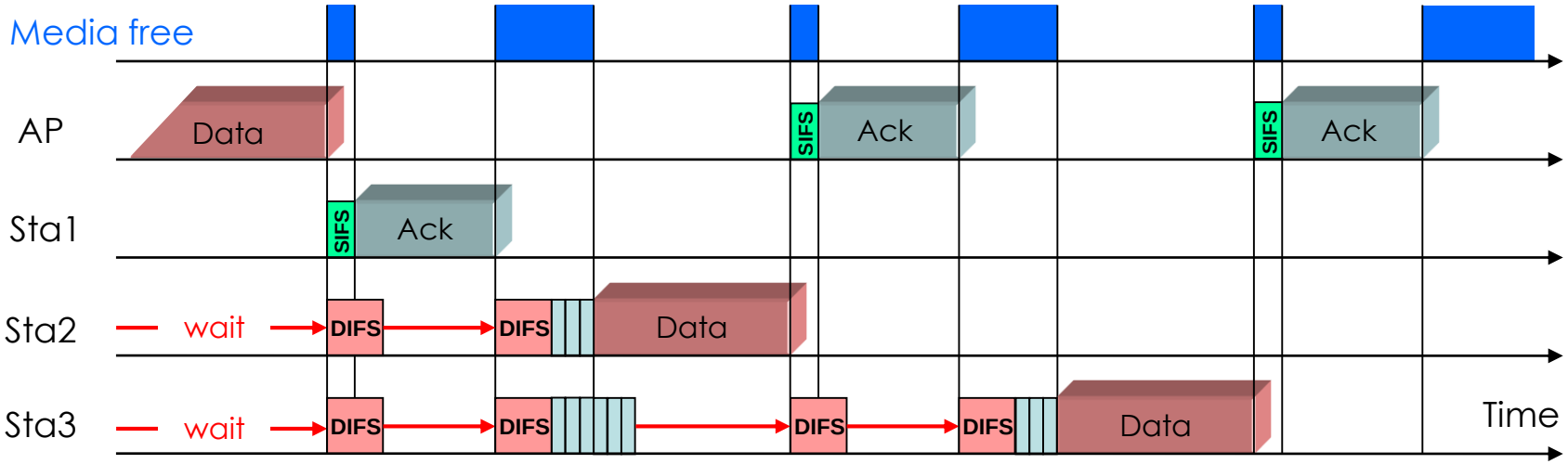


To add different channel colors select → View → Coloring Rules…

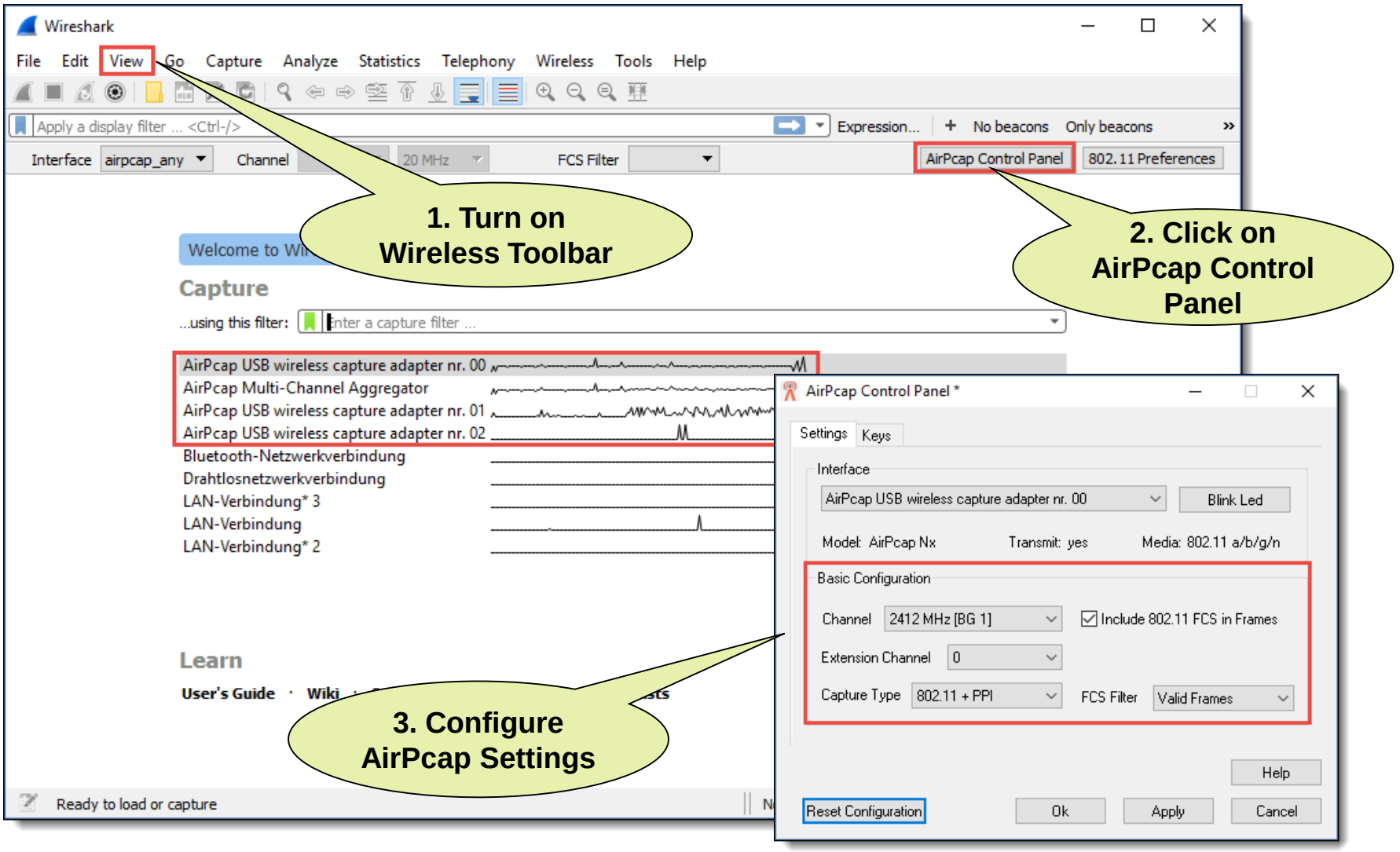


CSMA/CA offers different Inter Frame Spaces (IFS) to control media access:

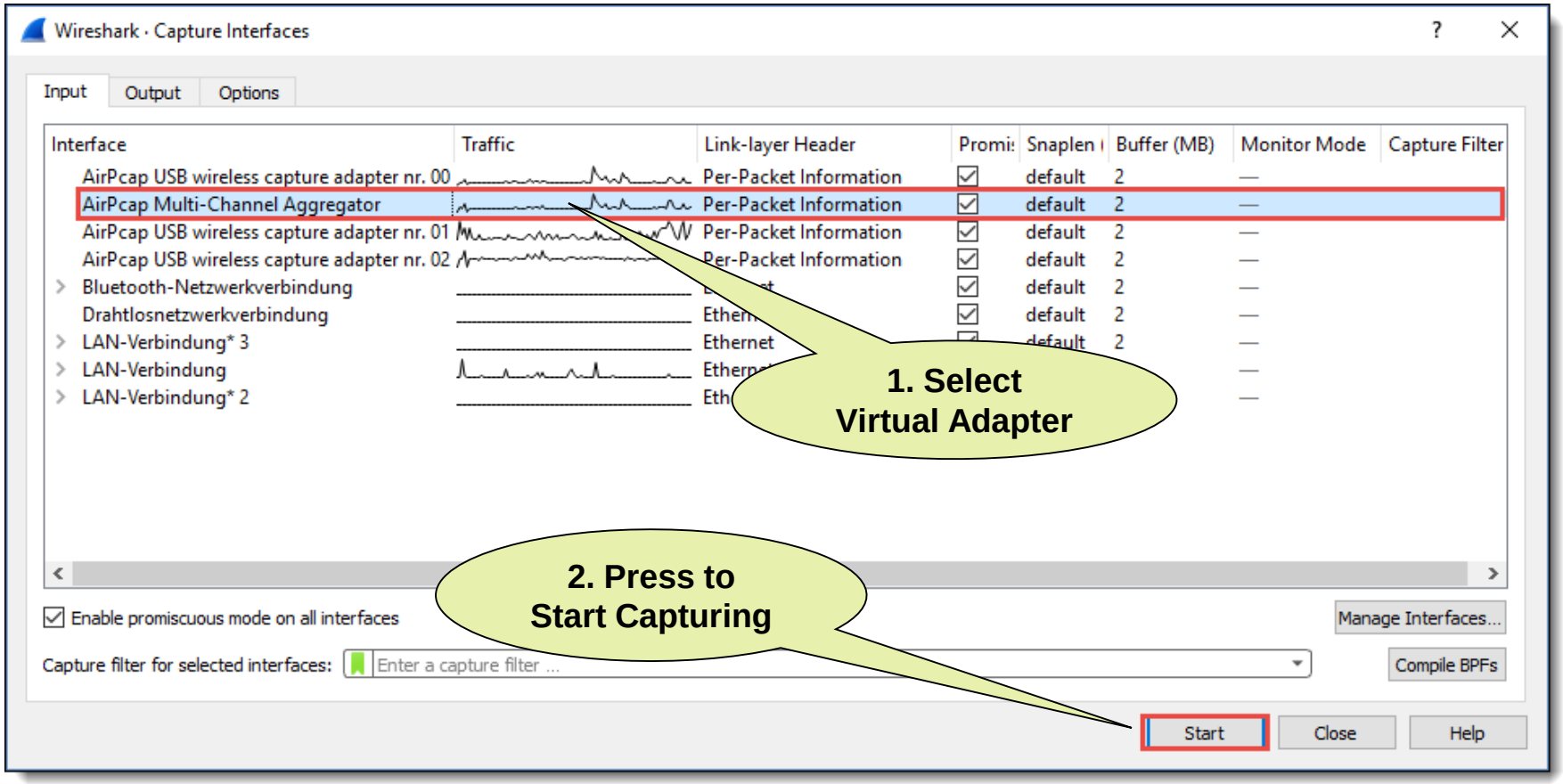
SIFS (Short Inter Frame Space)	802.11b/g = 10 µs 802.11a = 16 µs
DIFS (DCF Inter Frame Space) (2x Slot time + SIFS)	802.11b=50µs 802.11g=28µs 802.11a=34µs
Slot Time 802.11b = 20 µs (max. 31x)	**Short Slot Time** 802.11a/g = 9 µs (max. 15x)



- Stations can send anytime if media is free, but hold back if media is busy.
- If air becomes free, stations are waiting DIFS and a random number of Slot Times before sending
- Receiving stations verify Frame Check Sequence, if OK are sending ACK after SIFS


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression... + No beacons Only beacons
Interface airpcap_any Channel 20 MHz FCS Filter
AirPcap Control Panel
802.11 Preferences
1. Turn on Wireless Toolbar
2. Click on AirPcap Control Panel
Capture
...using this filter: Enter a capture filter ...
AirPcap USB wireless capture adapter nr. 00
AirPcap Multi-Channel Aggregator
AirPcap USB wireless capture adapter nr. 01
AirPcap USB wireless capture adapter nr. 02
Bluetooth-Netzwerkverbindung
Drahtlosnetzwerkverbindung
LAN-Verbindung* 3
LAN-Verbindung
LAN-Verbindung* 2
Learn
User's Guide · Wiki
Ready to load or capture
AirPcap Control Panel *
Settings Keys
Interface
AirPcap USB wireless capture adapter nr. 00
Blink Led
Model: AirPcap Nx
Transmit: yes
Media: 802.11 a/b/g/n
Basic Configuration
Channel 2412 MHz [BG 1]
Include 802.11 FCS in Frames
Extension Channel 0
Capture Type 802.11 + PPI
FCS Filter Valid Frames
3. Configure AirPcap Settings
Help
Reset Configuration
Ok
Apply
Cancel

- You may have to start Wireshark in Admin Mode to see the AirPcap I/Fs
- Verify the settings on the Capture Interfaces pane



Key features:

- WiFi radios can use 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 WiFi packets in both 2.4 GHz and 5 GHz bands.

END-OF-AVAILABILITY JANUARY 1ST 2018

- Softing IT Networks introduces the new WaveXpert
  - Includes 4 wireless adapter with 16 integrated antennas
  - Supports 4x4 MIMO up to IEEE 802.11ac Wave 2
  - USB-C type plug for data and unit power
  - 2.4 GHz or 5 GHz versions available
  - 4 x 4 : 4 up to 4 Channels (1'730 Mbps)
  - 2 x 2 : 2 up to 8 Channels (1'730 Mbps)
  - pcapng files incl. Radiotap header

Multi-Channel WLAN Sniffer

- Retail price: EUR 1'950
  Availability: planned for 1st Qu. 2019

- Requirements:
  - LINUX notebook and USB-C (Thunderbolt 3)
  - Supporting most Linux's and Mac OS

Joint development of:

Softing IT Networks GmbH
85540 Haar, Germany and
GHMT AG
66450 Bexbach, Germany

Supported maximum capture rates

802.11n/ac Physical Rate Table (Mbps)								
Number of Streams	Modulation	Antennas Tx x Rx : Spatial Streams		Maximum Rate (Mbps) 1 Ch.	2 Ch.	4 Ch.	8 Ch.	Band Support
802.11n								
One Stream*	64-QAM	1 x 1 :	1	72	150	n.a.	n.a.	2.4 & 5 GHz
Two Streams*	64-QAM	2 x 2 :	2	144	300 *	n.a.	n.a.	2.4 & 5 GHz
Three Streams	64-QAM	3 x 3 :	3	216	450	n.a.	n.a.	2.4 & 5 GHz
Four Streams	64-QAM	4 x 4 :	4	288	600	n.a.	n.a.	2.4 & 5 GHz
802.11ac Wave 1								
One Stream	256-QAM	1 x 1 :	1	86	200	433	n.a.	5 GHz
Two Streams	256-QAM	2 x 2 :	2	173	400	866	n.a.	5 GHz
Three Streams	256-QAM	3 x 3 :	3	289	600	1300	n.a.	5 GHz
802.11ac Wave 2								
One Stream	256-QAM	1 x 1 :	1	86	200	433	866	5 GHz
Two Streams	256-QAM	2 x 2 :	2	173	400	866	1730 **	5 GHz
Three Streams	256-QAM	3 x 3 :	3	289	600	1300	2600	5 GHz
Four Streams	256-QAM	4 x 4 :	4	385	800	1730 **	3470	5 GHz
Eight Streams	256-QAM	8 x 8 :	8	770	1600	3470	6930	5 GHz

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

** Softing WaveXpert supports up to 8 channels per WLAN adapter

802.11Frame 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 '18 Europe

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

Troubleshooting WLANs (Part 2)

Troubleshooting WLANs using
802.11 Management & Control Frames

WLAN Trainings with Wireshark & WaveXpert available in Germany and Switzerland