SharkFest ‘16 Europe

Troubleshooting WLANs (Part 1)

Layer 1 & 2 Analysis using WiSpy & AirPcap
19. October 2016

Welcome!

Rolf Leutert

Leutert NetServices
Switzerland
www.netsniffing.ch

#sf16eu

Introduction

LEUTERT NetServices

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

Sniffer Certified
MASTER

Wireshark University
WIRESHARK®
CERTIFIED
NETWORK ANALYST

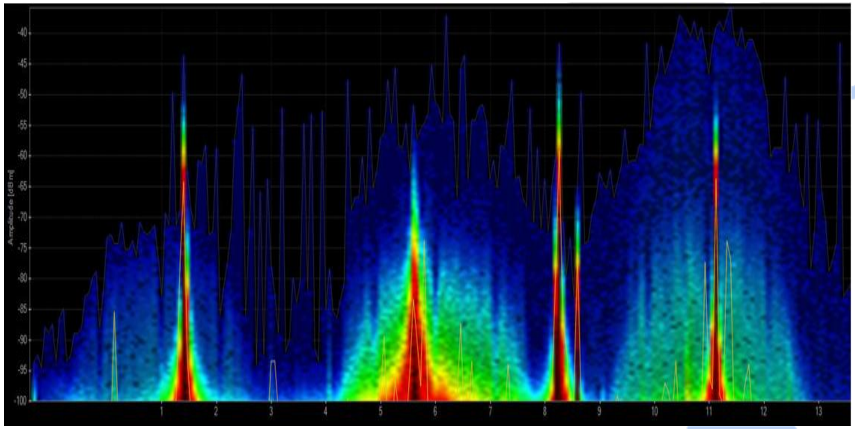
Session Objectives

- 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

Licensed by iStockphoto.com

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

Troubleshooting WLANs comprises Layer 1 and Layer 2

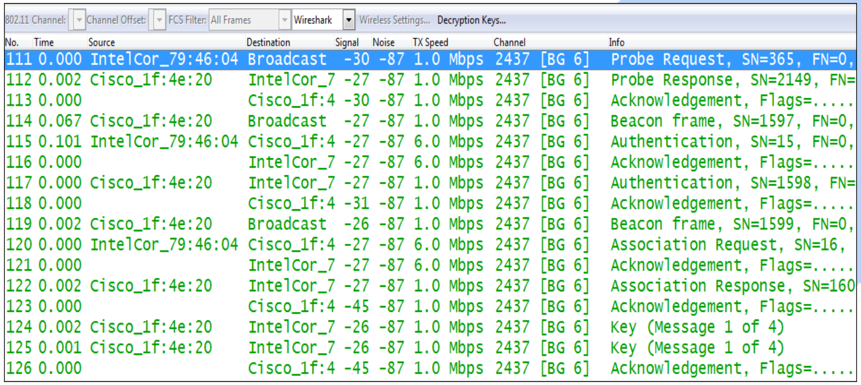


Layer 1 - Physical Access

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 Layer 1 Analysis

- 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 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

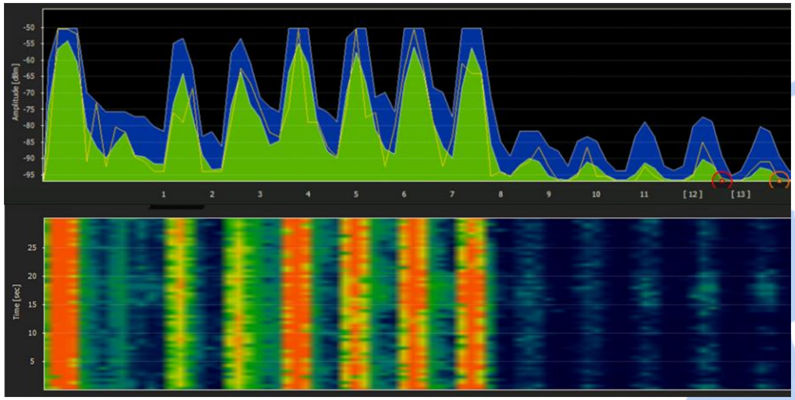
Wi-Spy® DBx spectrum scanner
and Chanalizer® software displays
and records all layer 1 signals in
both 2.4 GHz and 5 GHz bands.

www.metageek.com

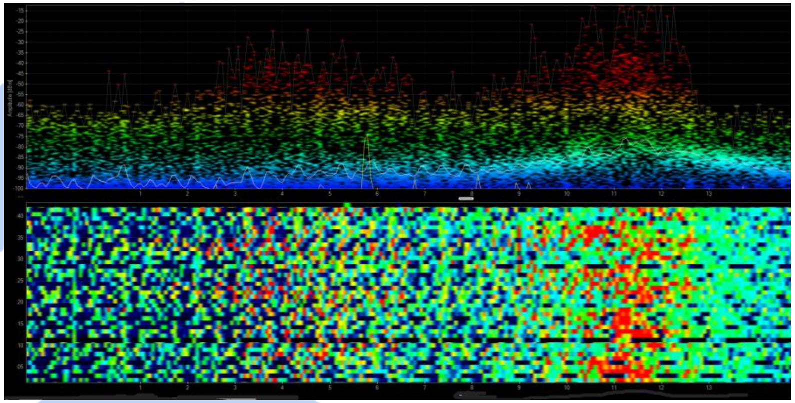
* ISM Industrial, Scientific and Medical
**UNII Unlicensed National Information Infrastructure

WLAN Layer 1 Analysis

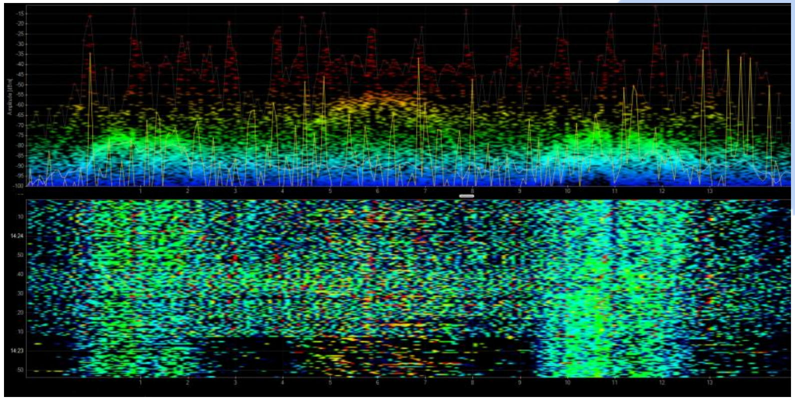
Non-WiFi Devices' Signatures



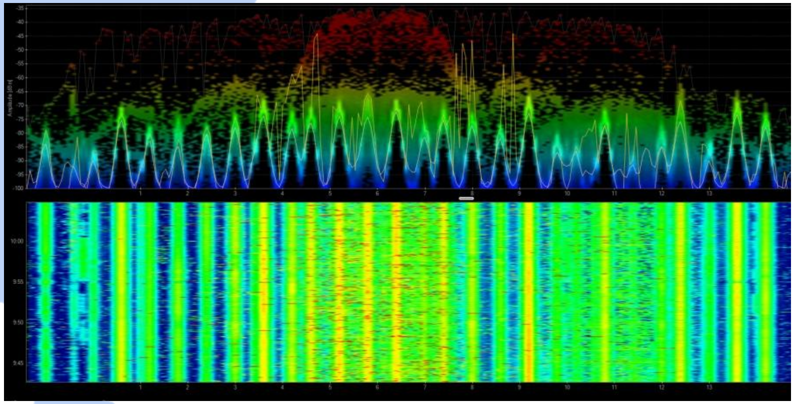
Home trainers in a fitness center



Microwave oven

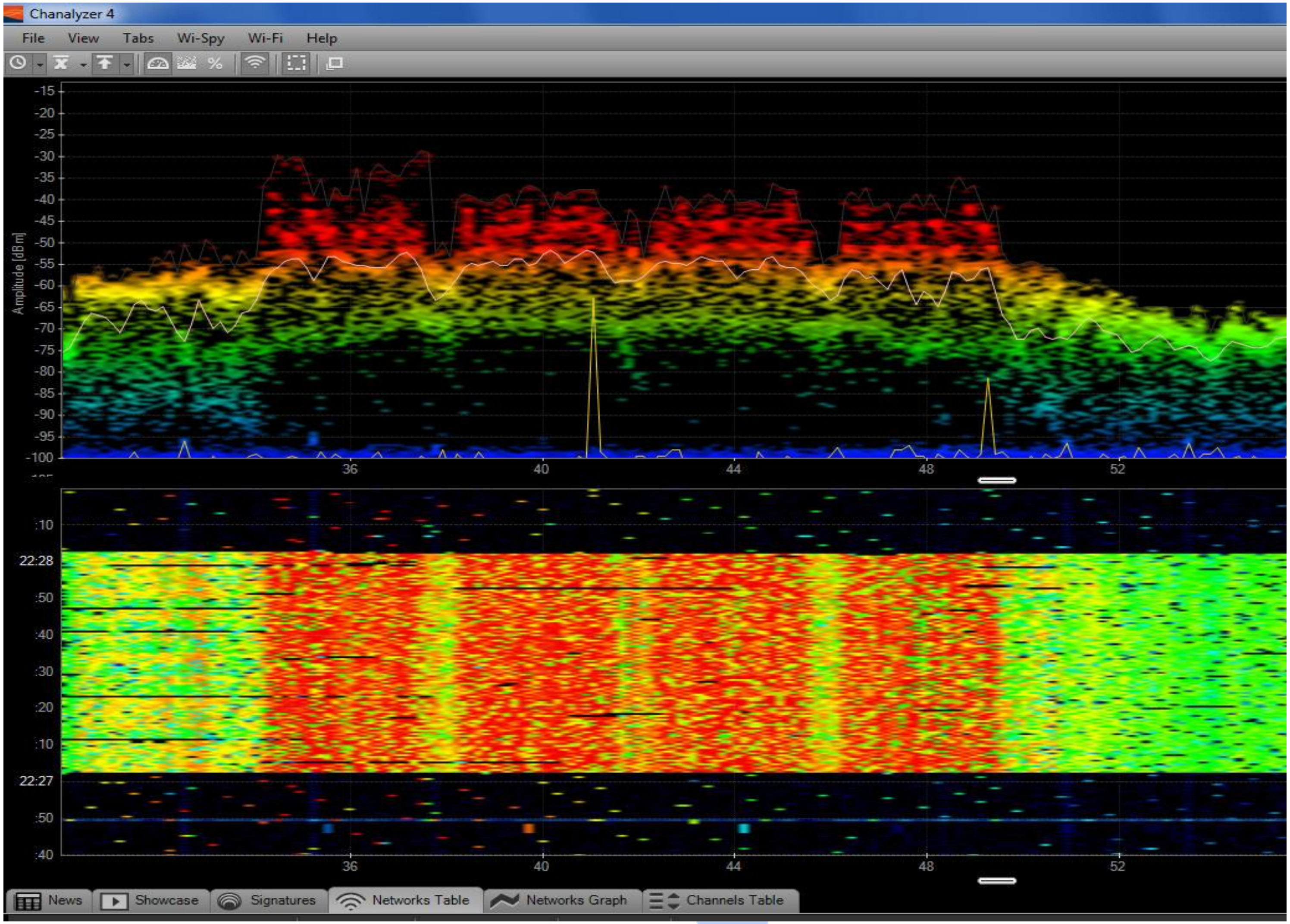


Remote control of model airplanes



Wireless guitar

Live Demo: WiSpy & Chanalyzer



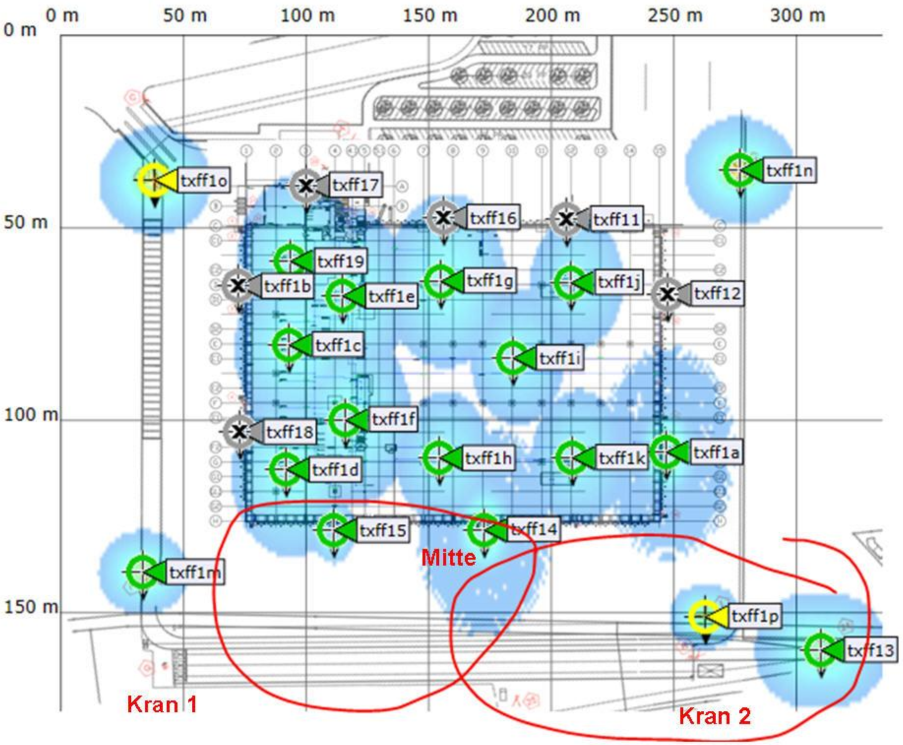
WiFi 802.11ac with four bonded channels

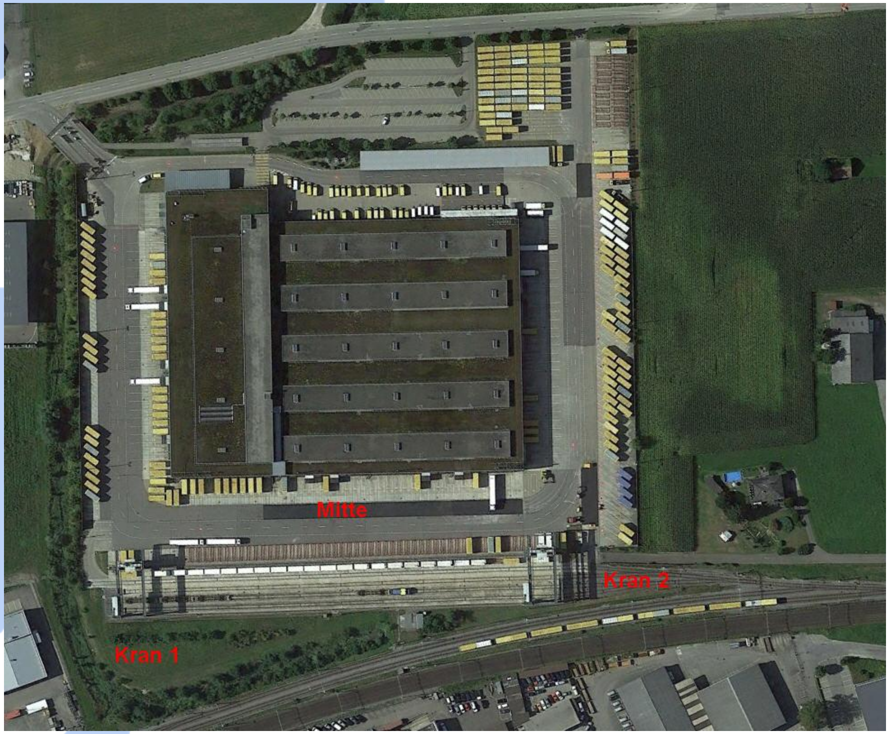
WLAN Layer 1 Analysis (Case one)

- 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)

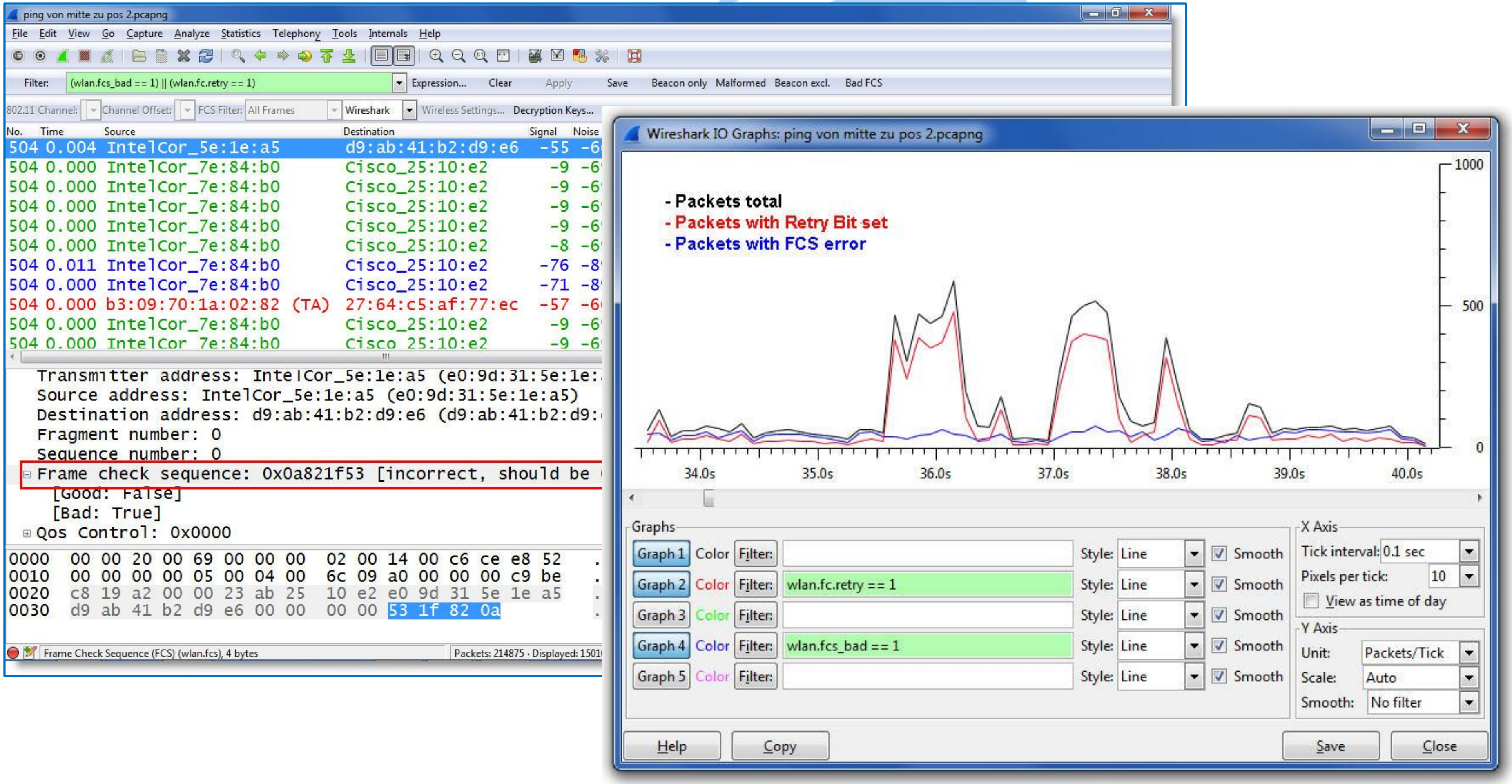
- User complain about log-in timeouts and disconnections during operations
- Crane #2 is hardly usable due to unreliable WLAN connection
- Tech-Support has already changed WiFi channels and added additional AP





WLAN Layer 1 Analysis (Case one)

- 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



ping von mitte zu pos 2.pcapng

Filter: (wlan.fcs_bad == 1) || (wlan.fc.retry == 1)

802.11 Channel: Channel Offset: FCS Filter: All Frames Wireshark

```
No.  Time   Source                      Destination           Signal  Noise
504 0.004 IntelCor_5e:1e:a5            d9:ab:41:b2:d9:e6      -55  -6
504 0.000 IntelCor_7e:84:b0            Cisco_25:10:e2         -9   -6
504 0.000 IntelCor_7e:84:b0            Cisco_25:10:e2         -9   -6
504 0.000 IntelCor_7e:84:b0            Cisco_25:10:e2         -9   -6
504 0.000 IntelCor_7e:84:b0            Cisco_25:10:e2         -9   -6
504 0.000 IntelCor_7e:84:b0            Cisco_25:10:e2         -8   -6
504 0.011 IntelCor_7e:84:b0            Cisco_25:10:e2         -76  -8
504 0.000 IntelCor_7e:84:b0            Cisco_25:10:e2         -71  -8
504 0.000 b3:09:70:1a:02:82 (TA)       27:64:c5:af:77:ec      -57  -6
504 0.000 IntelCor_7e:84:b0            Cisco_25:10:e2         -9   -6
504 0.000 IntelCor_7e:84:b0            Cisco_25:10:e2         -9   -6
```

```
  Transmitter address: IntelCor_5e:1e:a5 (e0:9d:31:5e:1e:
  Source address: IntelCor_5e:1e:a5 (e0:9d:31:5e:1e:a5)
  Destination address: d9:ab:41:b2:d9:e6 (d9:ab:41:b2:d9:
  Fragment number: 0
  Sequence number: 0
⊟ Frame check sequence: 0x0a821f53 [incorrect, should be
    [Good: False]
    [Bad: True]
⊞ Qos Control: 0x0000
```

```
0000  00 00 20 00 69 00 00 00  02 00 14 00 c6 ce e8 52
0010  00 00 00 00 05 00 04 00  6c 09 a0 00 00 00 c9 be
0020  c8 19 a2 00 00 23 ab 25  10 e2 e0 9d 31 5e 1e a5
0030  d9 ab 41 b2 d9 e6 00 00  00 00 53 1f 82 0a
```

Frame Check Sequence (FCS) (wlan.fcs), 4 bytes — Packets: 214875 · Displayed: 1501

Wireshark IO Graphs: ping von mitte zu pos 2.pcapng

Graphs

Graph 1	Color	Filter:		Style: Line	☑ Smooth
Graph 2	Color	Filter:	wlan.fc.retry == 1	Style: Line	☑ Smooth
Graph 3	Color	Filter:		Style: Line	☑ Smooth
Graph 4	Color	Filter:	wlan.fcs_bad == 1	Style: Line	☑ Smooth
Graph 5	Color	Filter:		Style: Line	☑ Smooth

X Axis

Tick interval: 0.1 sec

Pixels per tick: 10

□ View as time of day

Y Axis

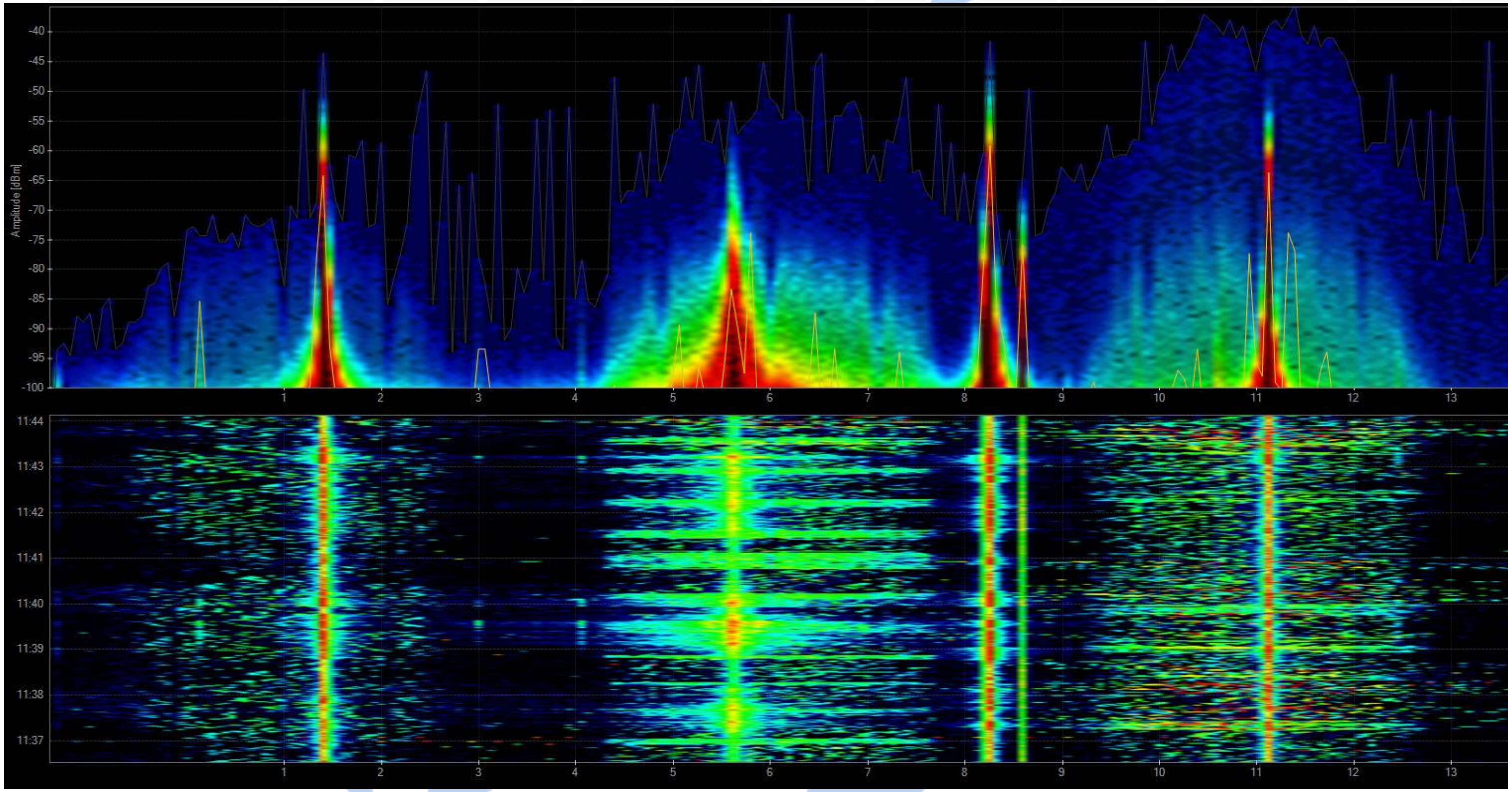
Unit: Packets/Tick

Scale: Auto

Smooth: No filter

WLAN Layer 1 Analysis (Case one)

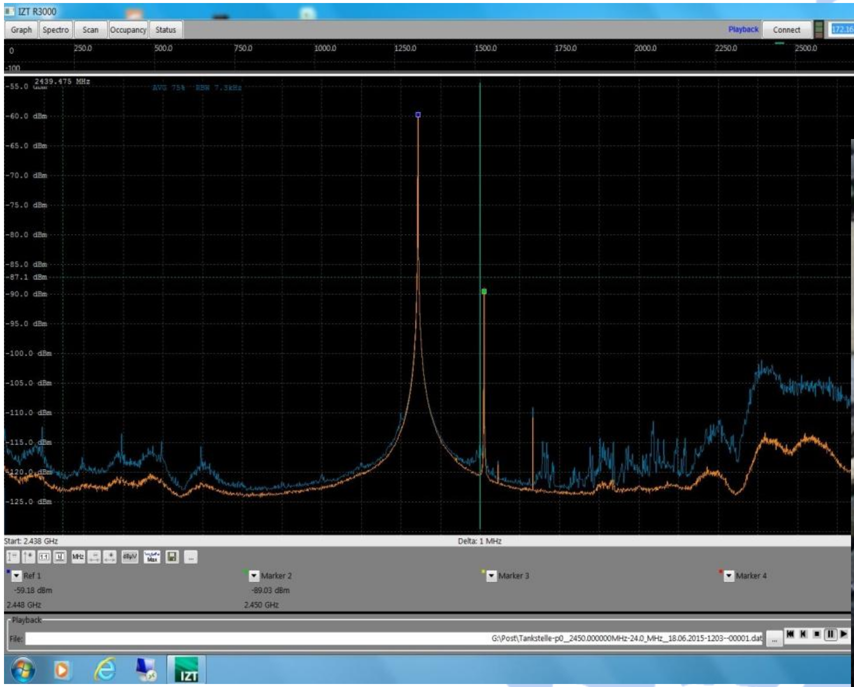
- Continuing with layer 1 analysis near crane #2 in 2.4 GHz band
- Strong interference with non-WiFi signals on all three channels detected



- 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

WLAN Layer 1 Analysis (Case one)

- 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



172.16.65.20

Panorama ○ HF ● VUHF ○ SUHF

Start (MHz): 30.000000

Stop (MHz): 3000.000000

Receiver ● RF1 ○ RF2 ○ RF3

Start: 2.438 GHz

Delta: 1 MHz

Ref 1: -59.18 dBm, 2.448 GHz

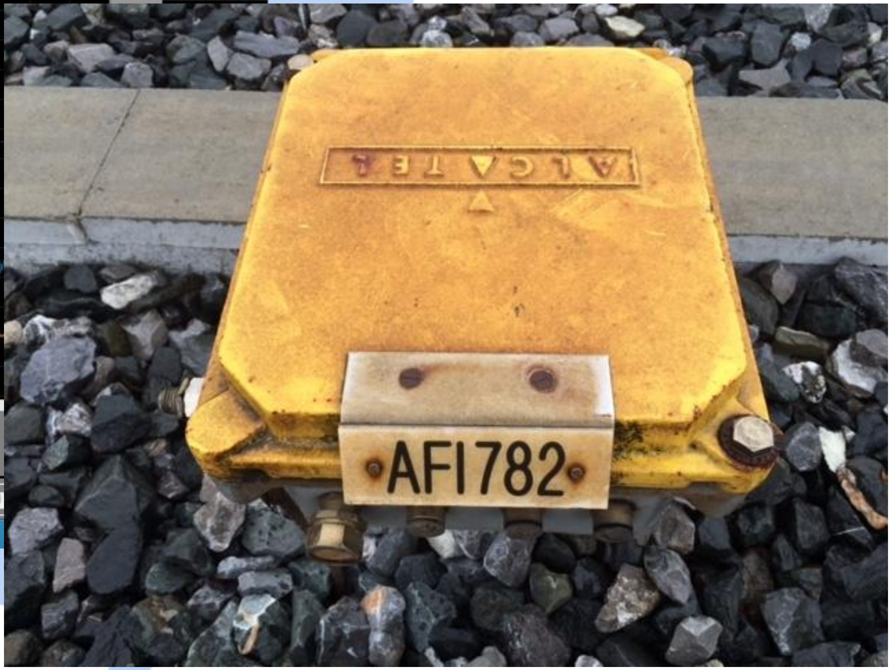
Marker 2: -89.03 dBm, 2.450 GHz

Marker 3

Marker 4

File: G:\Post\Tankstelle-p0__2450.000000MHz-24.0_MHz__18.06.2015-1203--00001.dat

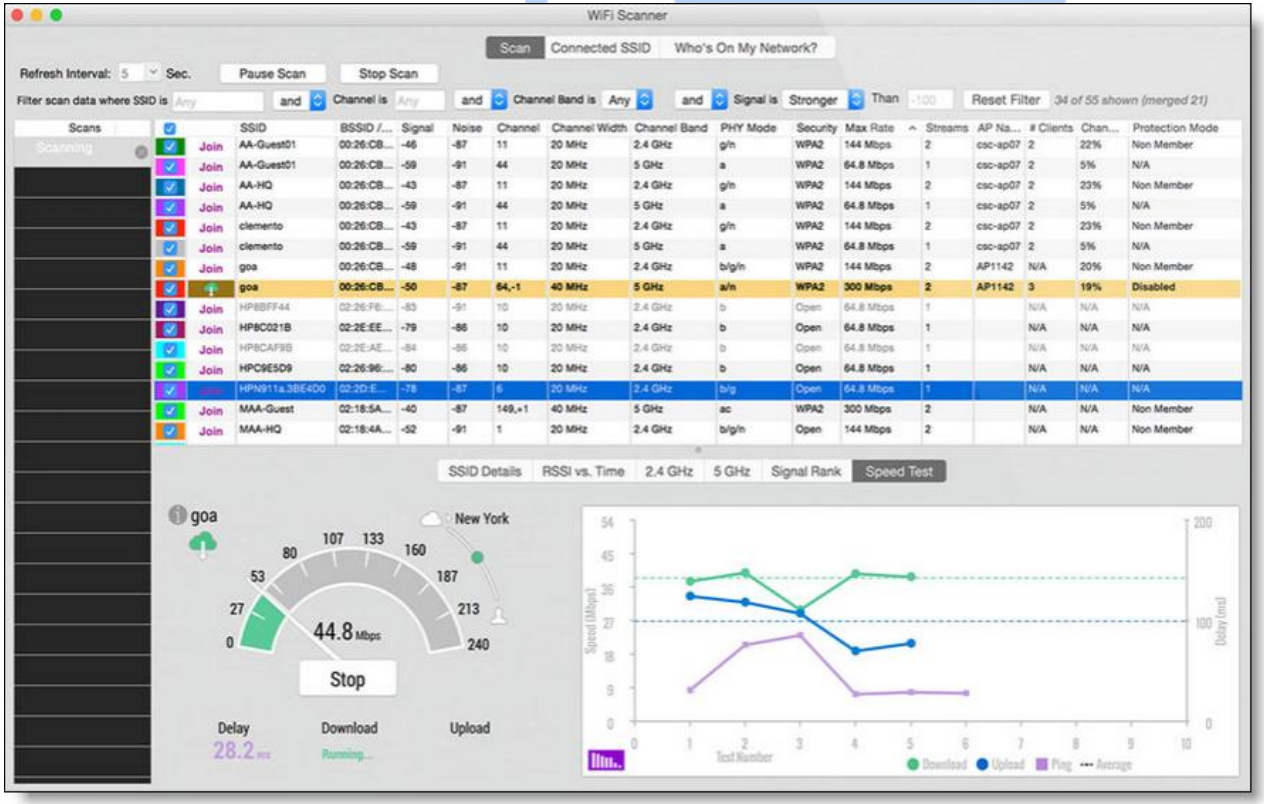
BAKOM scan result



Traffic monitoring induction loop

WiFi Scanners

- 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



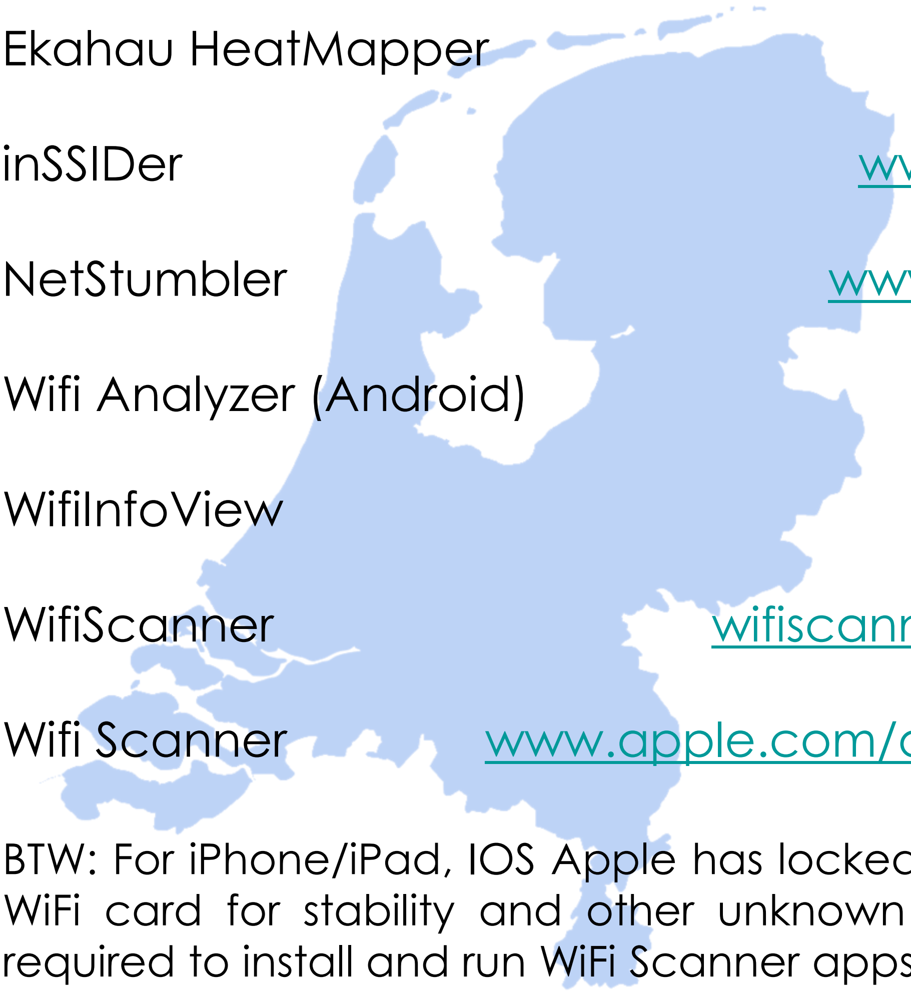
Refresh Interval: 5 Sec.

Filter scan data where SSID is Any and Channel is Any and Channel Band is Any and Signal is Stronger Than -100

34 of 55 shown (merged 21)

☑		SSID	BSSID /...	Signal	Noise	Channel	Channel Width	Channel Band	PHY Mode	Security	Max Rate	Streams	AP Na...	# Clients	Chan...	Protection Mode
☑	Join	AA-Guest01	00:26:CB...	-46	-87	11	20 MHz	2.4 GHz	g/n	WPA2	144 Mbps	2	csc-ap07	2	22%	Non Member
☑	Join	AA-Guest01	00:26:CB...	-59	-91	44	20 MHz	5 GHz	a	WPA2	64.8 Mbps	1	csc-ap07	2	5%	N/A
☑	Join	AA-HQ	00:26:CB...	-43	-87	11	20 MHz	2.4 GHz	g/n	WPA2	144 Mbps	2	csc-ap07	2	23%	Non Member
☑	Join	AA-HQ	00:26:CB...	-59	-91	44	20 MHz	5 GHz	a	WPA2	64.8 Mbps	1	csc-ap07	2	5%	N/A
☑	Join	clemento	00:26:CB...	-43	-87	11	20 MHz	2.4 GHz	g/n	WPA2	144 Mbps	2	csc-ap07	2	23%	Non Member
☑	Join	clemento	00:26:CB...	-59	-91	44	20 MHz	5 GHz	a	WPA2	64.8 Mbps	1	csc-ap07	2	5%	N/A
☑	Join	goa	00:26:CB...	-48	-91	11	20 MHz	2.4 GHz	b/g/n	WPA2	144 Mbps	2	AP1142	N/A	20%	Non Member
☑		goa	00:26:CB...	-50	-87	64,-1	40 MHz	5 GHz	a/n	WPA2	300 Mbps	2	AP1142	3	19%	Disabled
☑	Join	HP8BFF44	02:26:F6:...	-83	-91	10	20 MHz	2.4 GHz	b	Open	64.8 Mbps	1		N/A	N/A	N/A
☑	Join	HP8C021B	02:2E:EE...	-79	-86	10	20 MHz	2.4 GHz	b	Open	64.8 Mbps	1		N/A	N/A	N/A
☑	Join	HP8CAF9B	02:2E:AE...	-84	-86	10	20 MHz	2.4 GHz	b	Open	64.8 Mbps	1		N/A	N/A	N/A
☑	Join	HPC9E5D9	02:26:96:...	-80	-86	10	20 MHz	2.4 GHz	b	Open	64.8 Mbps	1		N/A	N/A	N/A
☑		HPN911a.3BE4D0	02:2D:E...	-78	-87	6	20 MHz	2.4 GHz	b/g	Open	64.8 Mbps	1		N/A	N/A	N/A
☑	Join	MAA-Guest	02:18:5A...	-40	-87	149,+1	40 MHz	5 GHz	ac	WPA2	300 Mbps	2		N/A	N/A	Non Member
☑	Join	MAA-HQ	02:18:4A...	-52	-91	1	20 MHz	2.4 GHz	b/g/n	Open	144 Mbps	2		N/A	N/A	Non Member

WiFi Scanners (just a few popular ones)



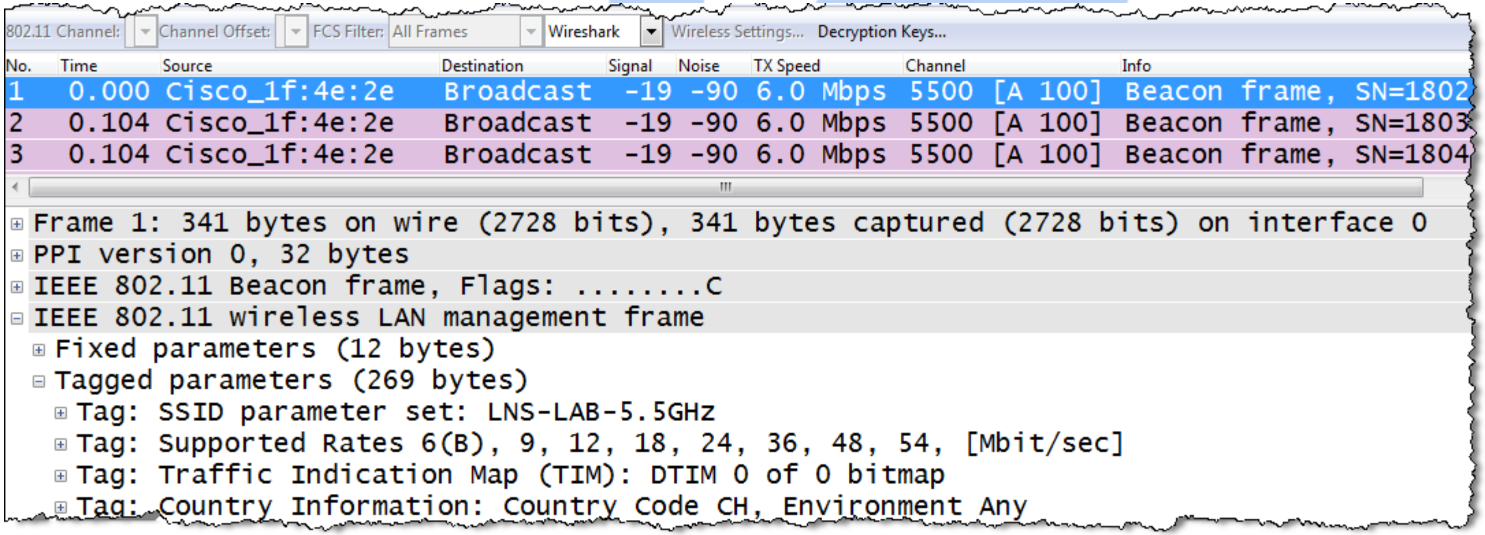
Acrylic WiFi scanner	www.acrylicwifi.com
Ekahau HeatMapper	www.ekahau.com
inSSIDer	www.metageek.com
NetStumbler	www.netstumbler.com
Wifi Analyzer (Android)	play.google.com
WifiInfoView	www.nirsoft.net
WifiScanner	wifiscanner.sourceforge.net
Wifi Scanner	www.apple.com/osx/apps/app-store

BTW: For iPhone/iPad, IOS Apple has locked direct access to the WiFi card for stability and other unknown reasons. Jailbreak is required to install and run WiFi Scanner apps on these devices.

WiFi Scanners

All these tools have the following limitations in common:

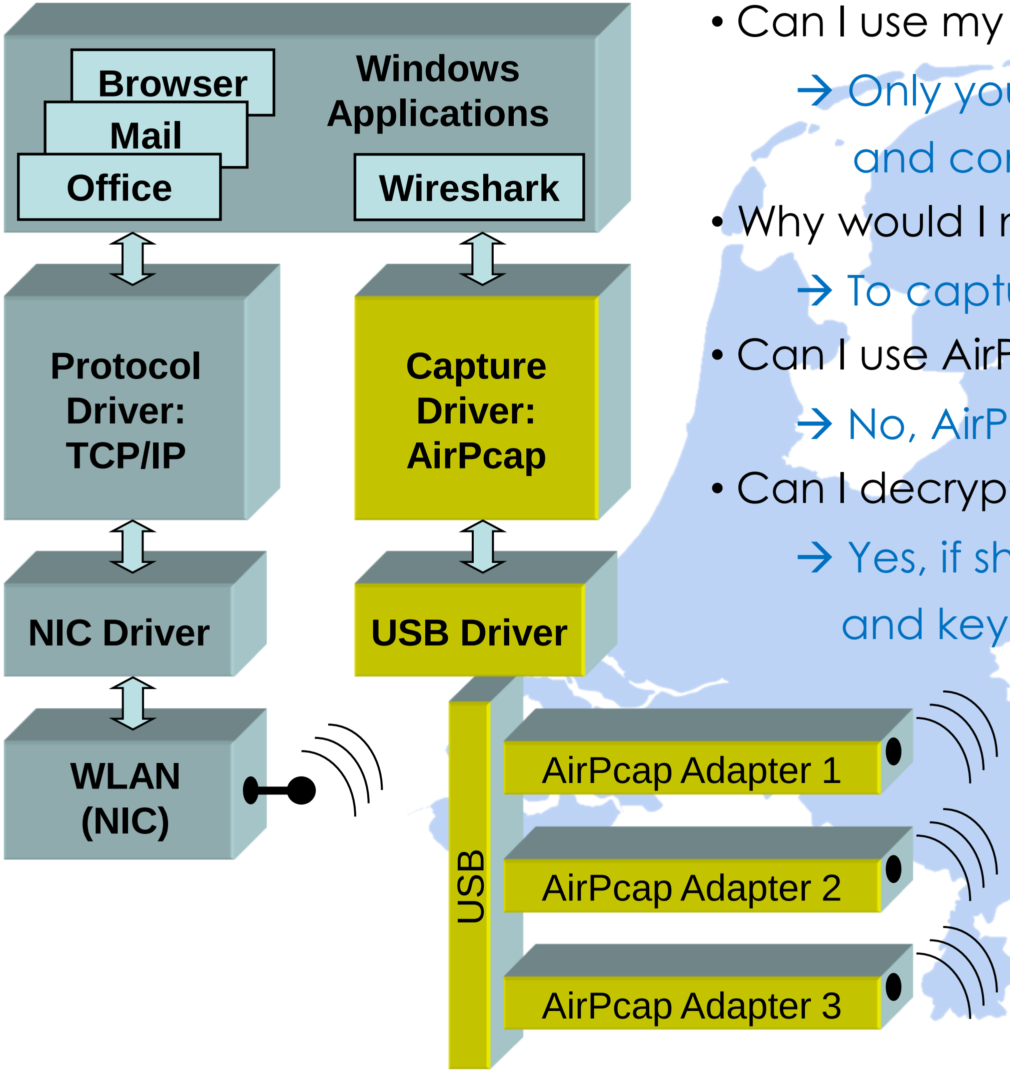
- Scanning on layer 2, therefore only WiFi devices can be detected.
- Non-802.11 sources like surveillance cameras etc. are invisible.
- WiFi scanners read data from Beacon and other management frames



```
802.11 Channel:   Channel Offset:   FCS Filter: All Frames   Wireshark   Wireless Settings...  Decryption Keys...

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!

WLAN Layer 2 Analysis



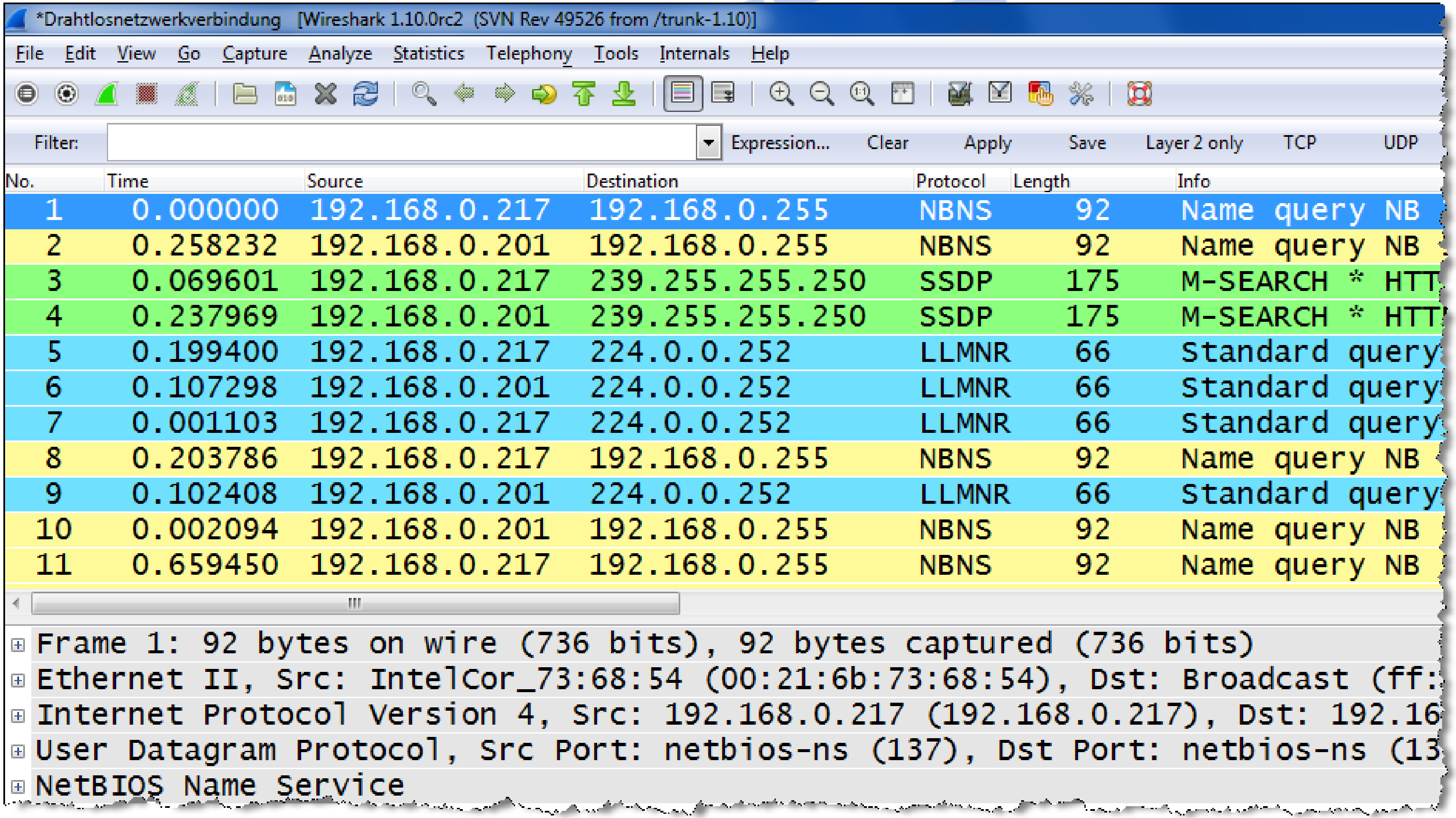
Frequently Asked Questions:

- 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

WLAN Layer 2 Analysis

- 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)]

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:
⊞ Internet Protocol Version 4, Src: 192.168.0.217 (192.168.0.217), Dst: 192.16
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (13
⊞ NetBIOS Name Service
```

WLAN Layer 2 Analysis with AirPcap

Key features:

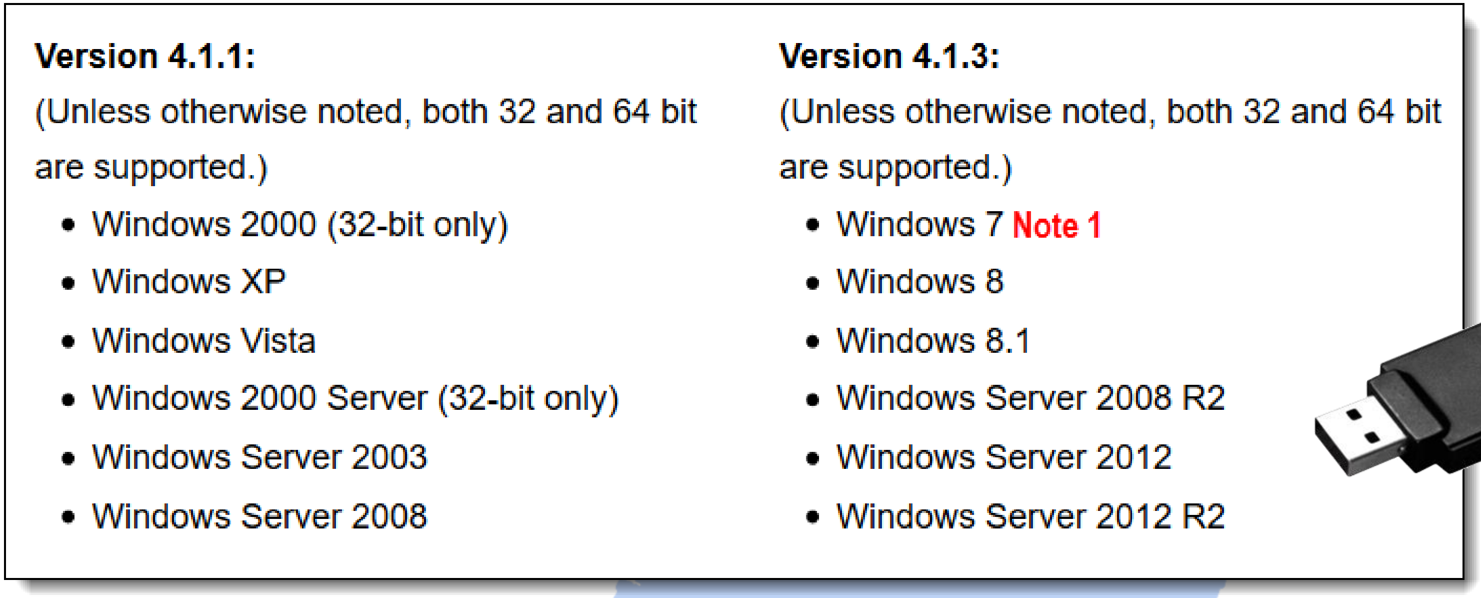
- Radio cells use one or multiple 20 MHz channels (n/ac) to increase throughput
- Each radio cell is a shared media and is controlled by an Access Point (AP)
- A mobile client can be associated with only one AP at the time
- Radio cell access is controlled by managements and control frames
- Wireshark 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 WiFi packets in both 2.4 GHz and 5 GHz bands.

www.riverbed.com/products/

WLAN Layer 2 Analysis with AirPcap

AirPcap Nx Driver Support:



Version 4.1.1:

(Unless otherwise noted, both 32 and 64 bit are supported.)

- Windows 2000 (32-bit only)
- Windows XP
- Windows Vista
- Windows 2000 Server (32-bit only)
- Windows Server 2003
- Windows Server 2008

Version 4.1.3:

(Unless otherwise noted, both 32 and 64 bit are supported.)

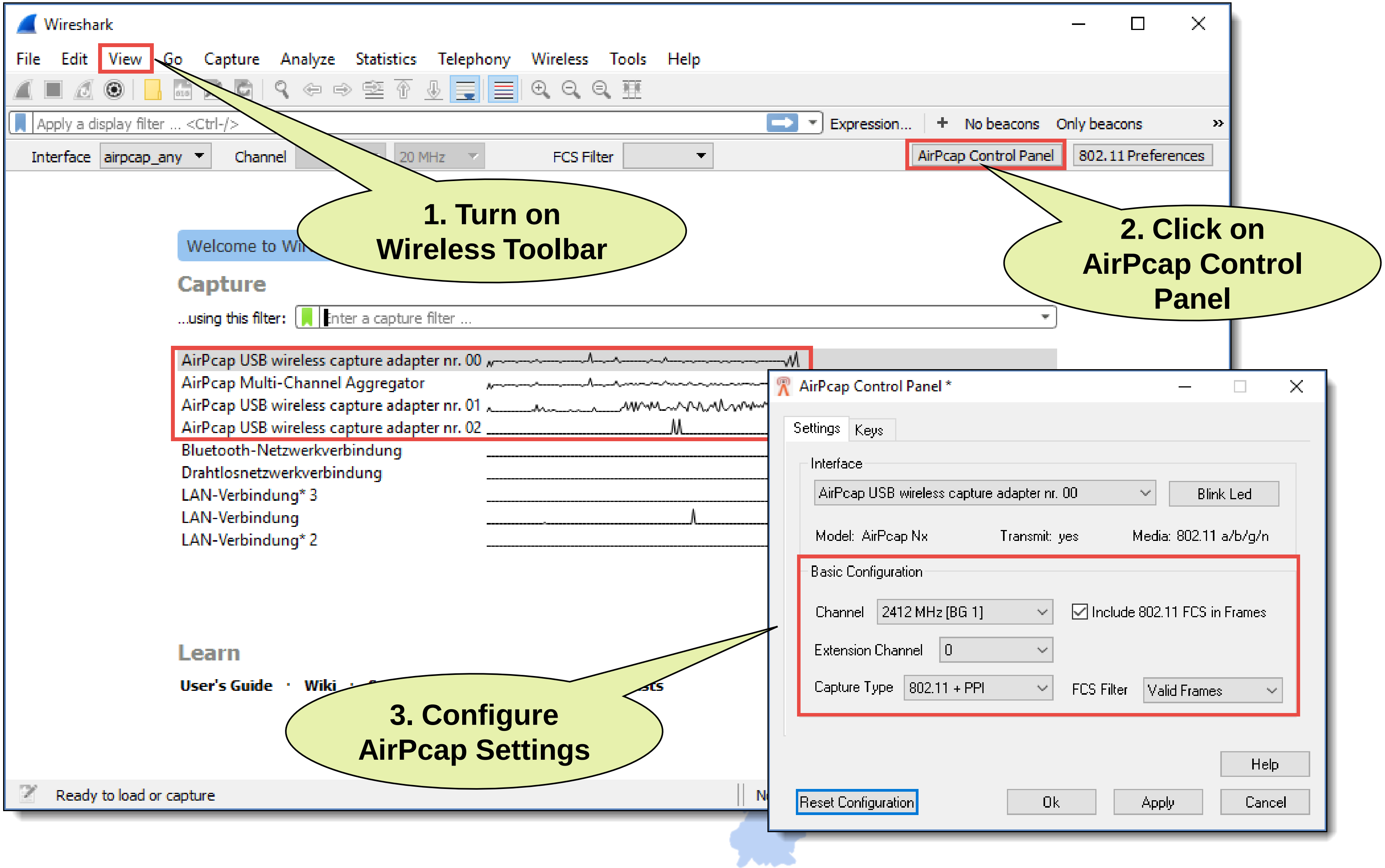
- Windows 7 **Note 1**
- Windows 8
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Chart notes:

[1] Windows 7 does not officially support USB 3.0, so inserting an AirPcap adapter into some USB 3.0 interfaces may crash a system. When an AirPcap Nx adapter is inserted into a USB 3.0 port of Intel Series 7 or 8 chipset, Windows 7 will crash. Some third-party USB 3.0 controllers, for example, Fresco Logic xHCI (USB3) Controller FL1100 Series or VIA USB eXtensible Host Controller, works fine.

Release notes:
https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html

WLAN Layer 2 Analysis with AirPcap


Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression… + No beacons Only beacons
AirPcap Control Panel
802.11 Preferences
Welcome to Wi
Capture
Learn
User's Guide · Wiki
Ready to load or capture
AirPcap Control Panel *
Settings Keys
Blink Led
Help
Reset Configuration Ok Apply Cancel

Interface: airpcap_any Channel: 20 MHz FCS Filter:

...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

Interface: AirPcap USB wireless capture adapter nr. 00

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

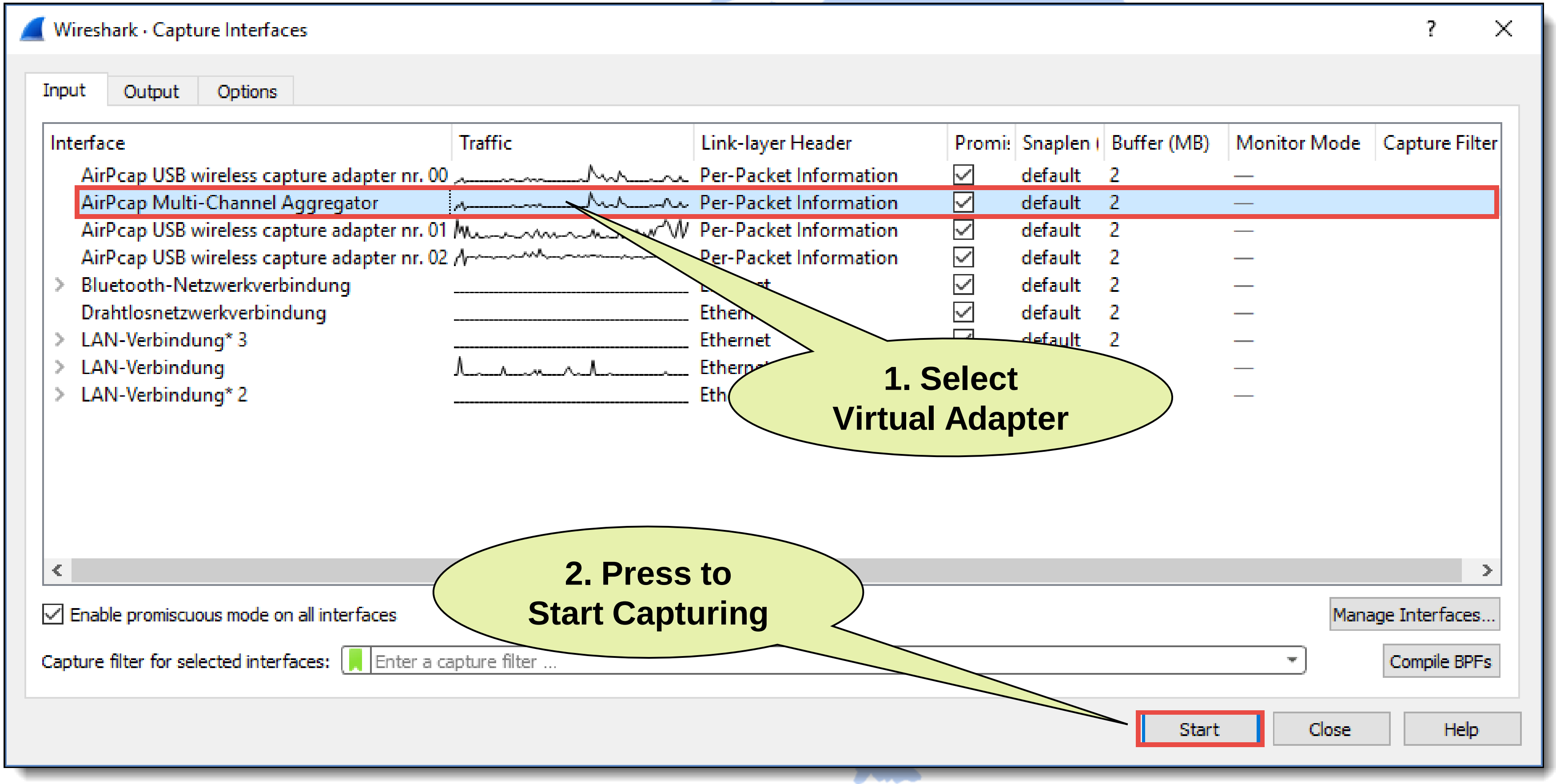
1. Turn on Wireless Toolbar

2. Click on AirPcap Control Panel

3. Configure AirPcap Settings

WLAN Layer 2 Analysis with AirPcap

- 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

Interface	Traffic	Link-layer Header	Promi:	Snaplen (	Buffer (MB)	Monitor Mode	Capture Filter
AirPcap USB wireless capture adapter nr. 00		Per-Packet Information	☑	default	2	—	
AirPcap Multi-Channel Aggregator		Per-Packet Information	☑	default	2	—	
AirPcap USB wireless capture adapter nr. 01		Per-Packet Information	☑	default	2	—	
AirPcap USB wireless capture adapter nr. 02		Per-Packet Information	☑	default	2	—	
Bluetooth-Netzwerkverbindung			☑	default	2	—	
Drahtlosnetzwerkverbindung		Ethern	☑	default	2	—	
LAN-Verbindung* 3		Ethernet	☑	default	2	—	
LAN-Verbindung		Etherne				—	
LAN-Verbindung* 2		Eth				—	

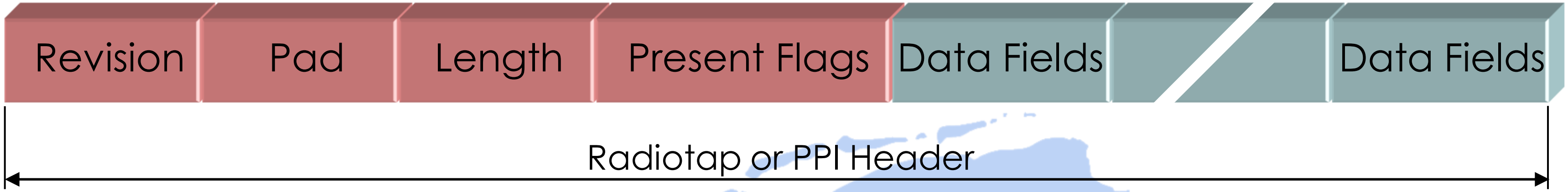
☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

1. Select Virtual Adapter

2. Press to Start Capturing

The AirPcap Radiotap and PPI pseudo-header



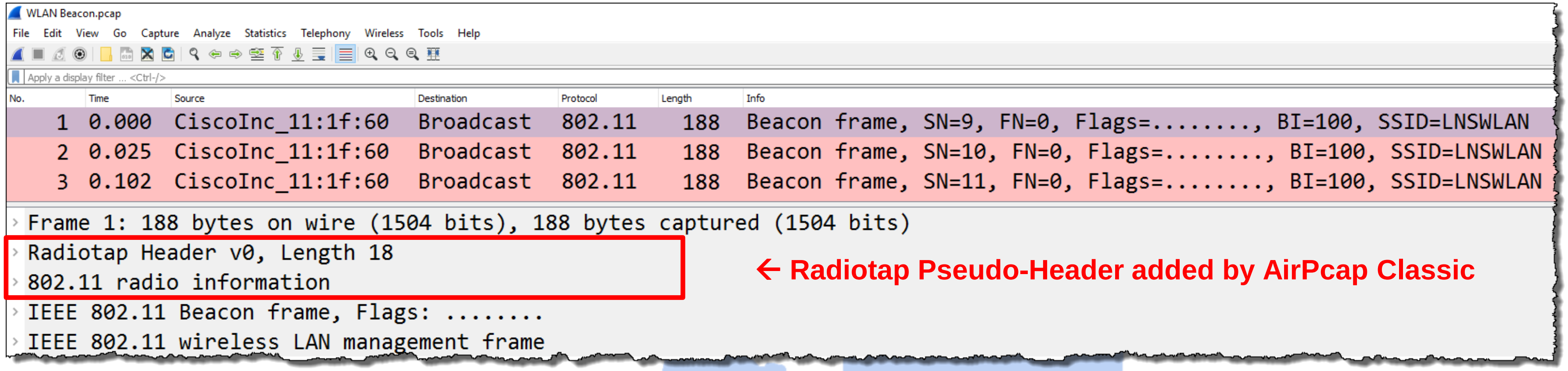
- Radiotap or the newer PPI (Per Packet Information) are so called *pseudo-headers* because they are not transmitted with the frame.
- They are added by the driver during reception and contain additional radio information about the frame.
- Receive signal strength, bit rate, channel number and other 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

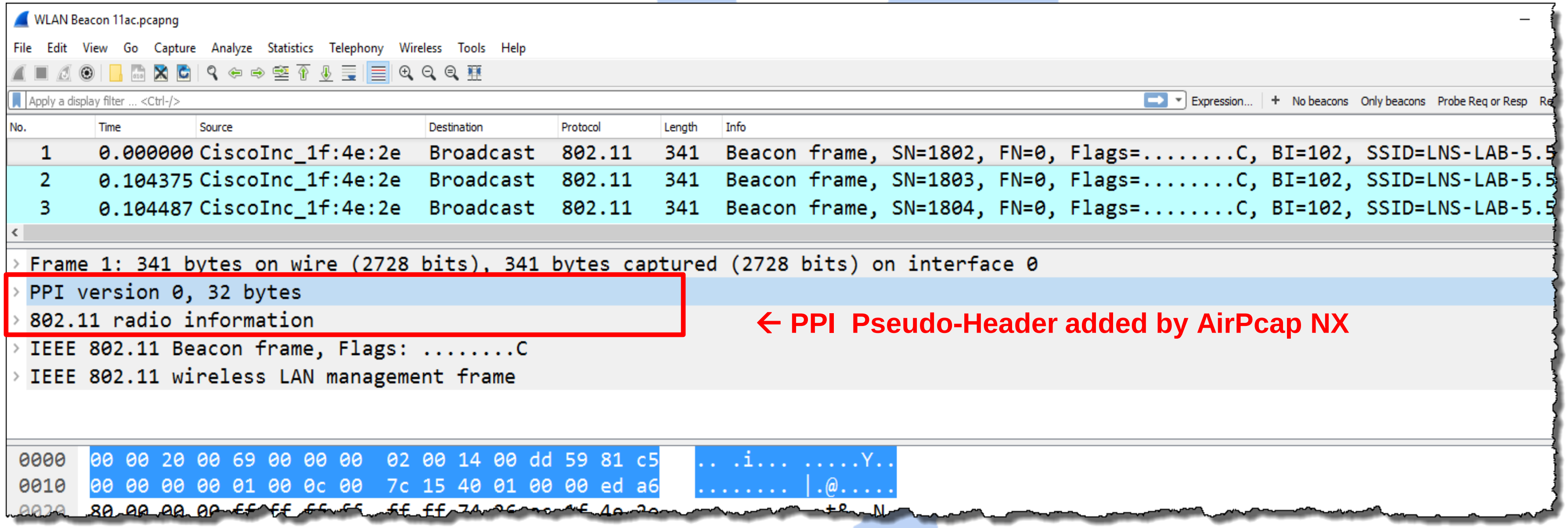
PPI manual: http://www.cacetech.com/documents/PPI_Header_format_1.0.1.pdf

The AirPcap Radiotap and PPI pseudo-header


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 AirPcap Classic**

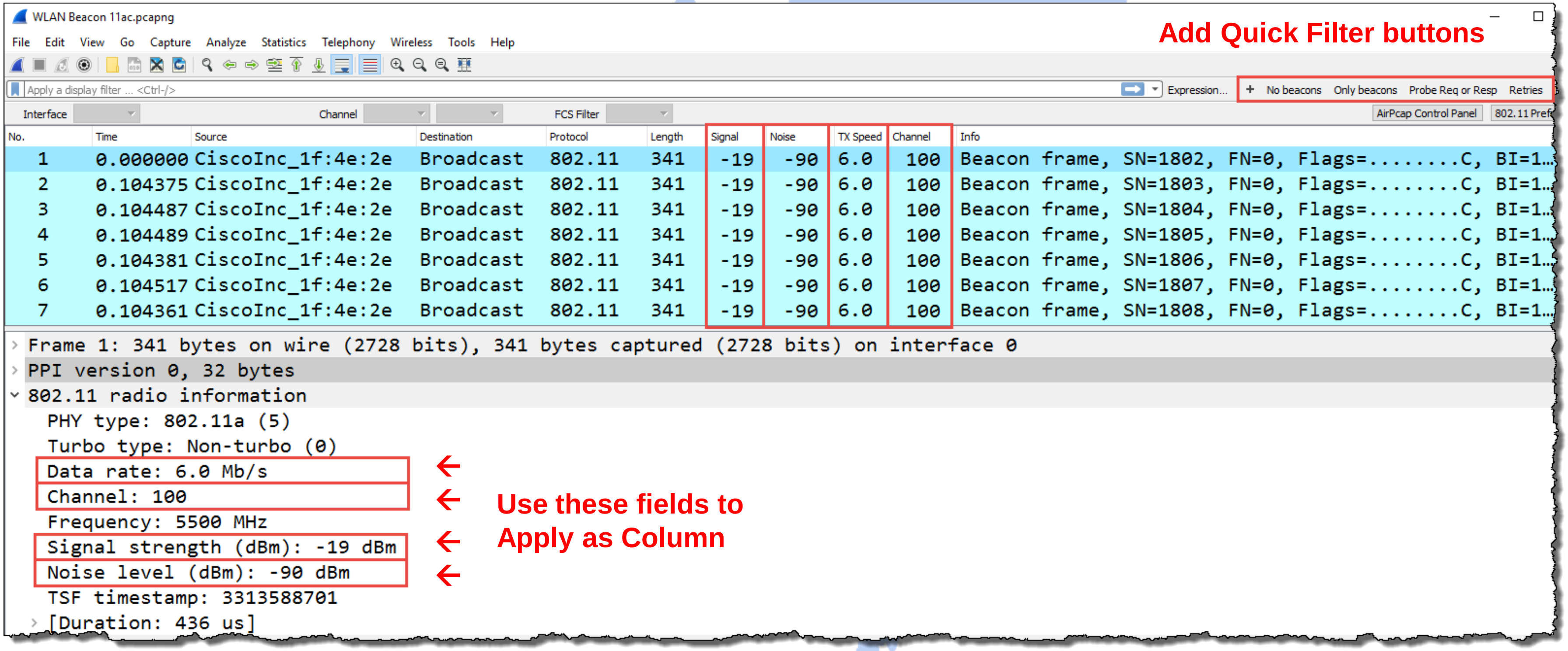

WLAN Beacon 11ac.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
No beacons
Only beacons
Probe Req or Resp
Re

```
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   ........ |.@.....
0020  80 00 00 00 ff ff ff ff  ff ff 74 26 ac 1f 4e 2e   ........ ..t&...N.
```

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

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



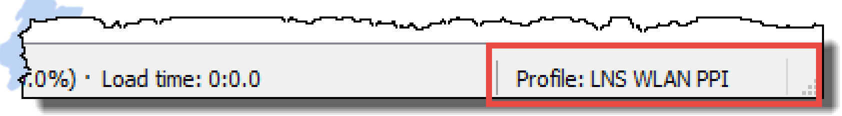
WLAN Beacon 11ac.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+ No beacons Only beacons Probe Req or Resp Retries
Interface
Channel
FCS Filter
AirPcap Control Panel
802.11 Pref

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
v 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]
```

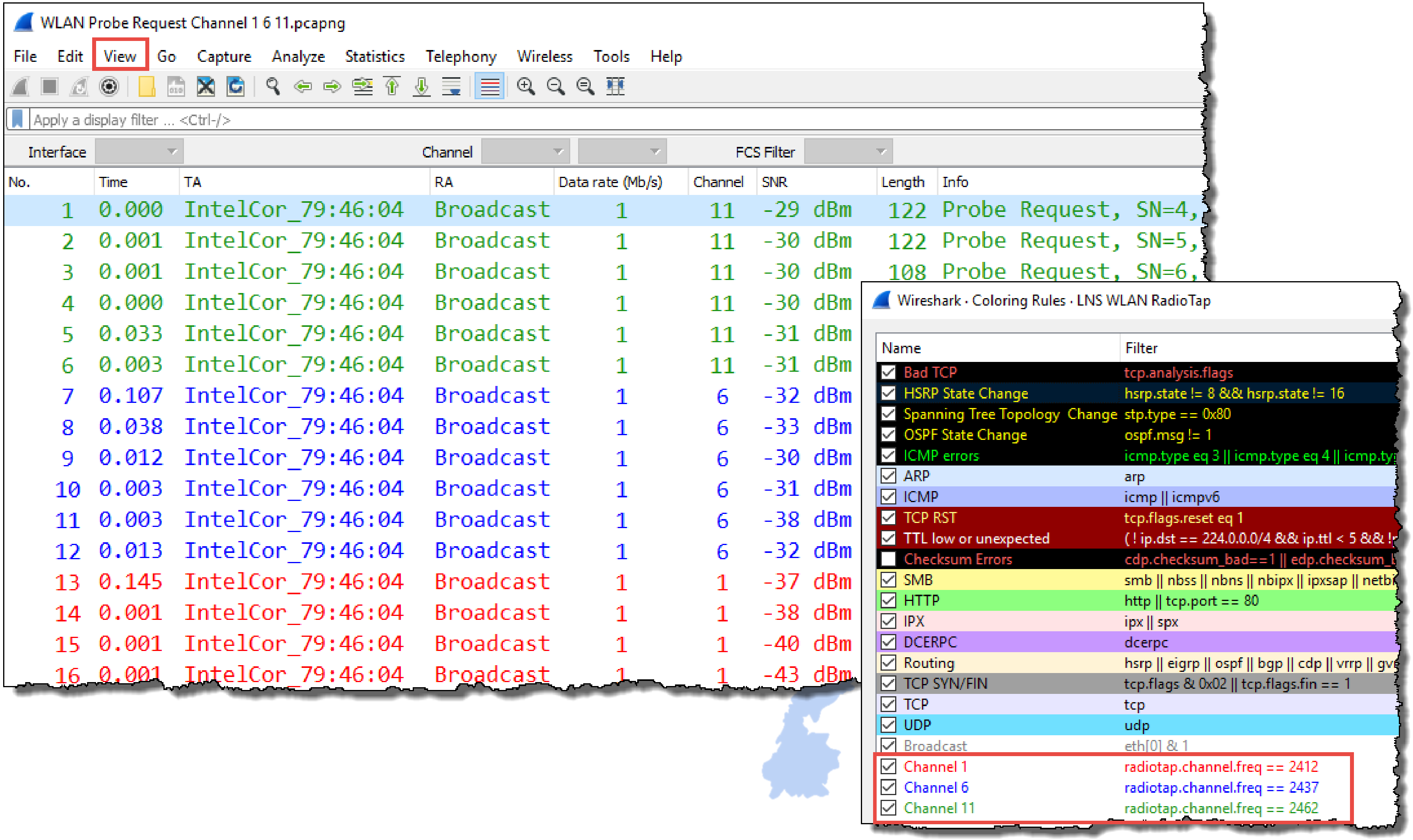
Use these fields to Apply as Column



```
.0%) · Load time: 0:0.0      Profile: LNS WLAN PPI
```

Customize Wireshark for WLAN analysis

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



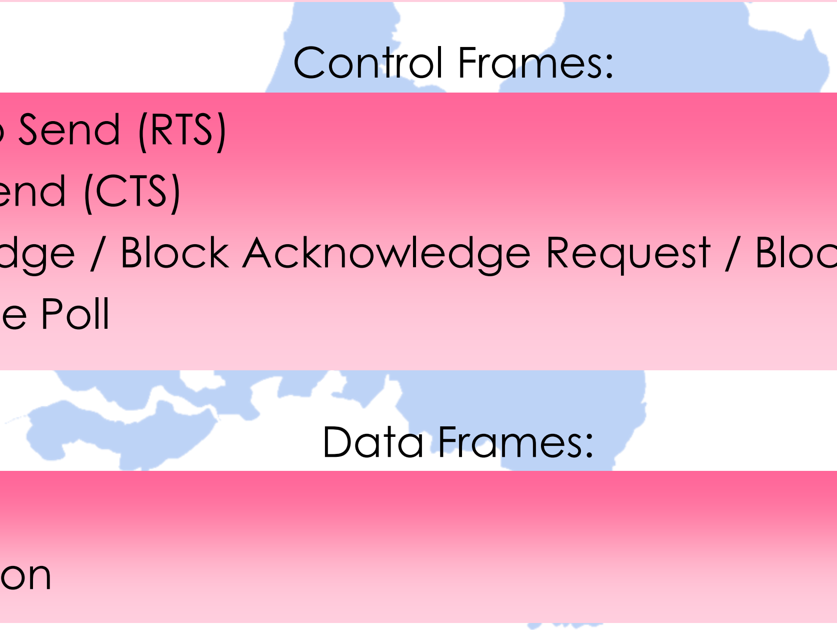
WLAN Probe Request Channel 1 6 11.pcapng

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

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 ‘16 Europe

That’s it for part 1 !
Let’s have a break and
hope to see you back for:

Troubleshooting WLANs (Part 2)

Troubleshooting WLANs using 802.11 Management & Control Frames
19. October 2016

Rolf Leutert
Leutert NetServices
Switzerland
www.netsniffing.ch

#sf16eu