SharkFest ’19 Europe

Troubleshooting WLANs (Part 1)

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

Rolf Leutert

Leutert NetServices
Switzerland
www.netsniffing.ch

Introduction

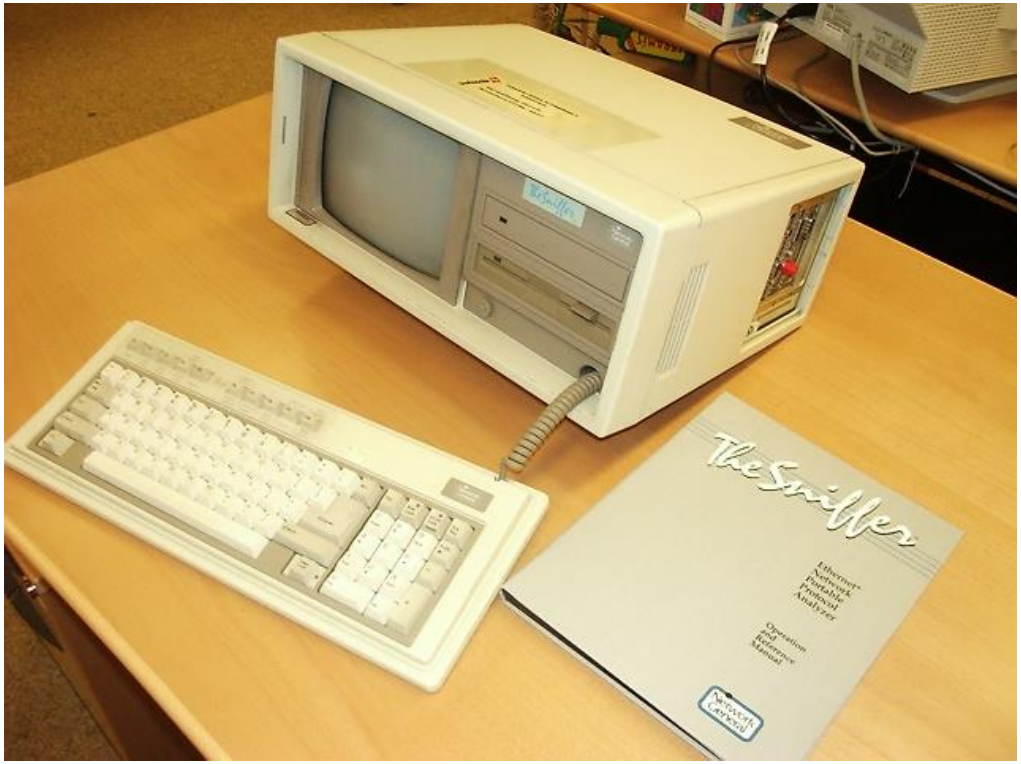
Rolf Leutert, El. Eng. HTL
Leutert NetServices
Zürich-Airport, Switzerland

- 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

The original “Sniffer”

Sniffer® has been registered as trademark in 1989


The Sniffer
The Sniffer
Ethernet Network Portable Protocol Analyzer
Operation and Reference Manual
Network General

- First **Network General Sniffer** in Switzerland
- Bought 1988 by Swissair airline to analyse **Token-Ring**
- Compaq Portable, DOS Version 1.30 / 256 KByte Capture Buffer
- Price US $ 30’000 (and more for each decoder)
- No trainings available (Sniffer University started in 1997)

Session Content

Session One

- Analysing Layer 1 (Physical Access) with Spectrum Analyser
- Use case: Finding the source interfering with a WLAN
- Wi-Fi Scanners: Free tools, their functions and limitations
- Analysing Layer 2: Capturing Wi-Fi packets with built in WLAN cards
- Using the Radiotap and PPI pseudo-header information
- Wi-Fi Access Control with CSMA/CA
- Capturing multiple Wi-Fi channels (for analysing roaming problems)

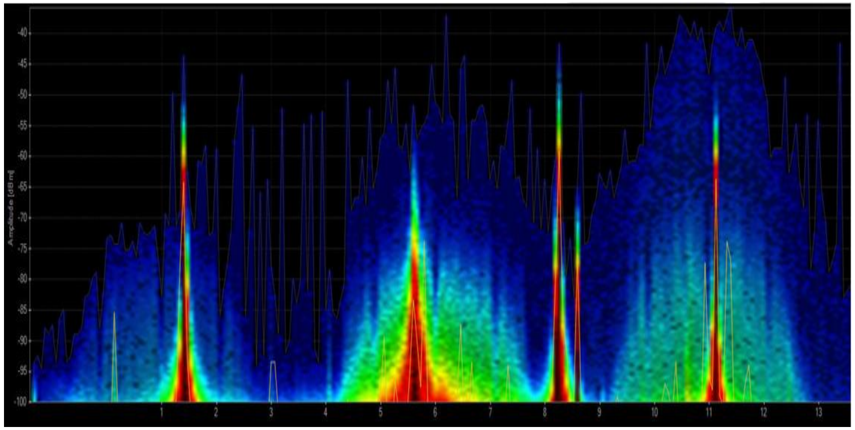
Session Two

- WLAN Layer 2 Analysis using 802.11 Mgmt. & Control frames
- The four different IEEE 802.11 Frame Formats
- WiFi Data Transmission & Retransmission
- Management Frames: Beacon, Probe Request & Response
- Management Frames: Authentication & Association
- Control Frames: Request to Send / Clear to Send
- Decrypting WEP, WPA & WPA2 PSK
- Use case: Isolating a Client roaming problem
- Analysing 802.11n/ac Frame Aggregation A-MSDU & A-MPDU

+

Troubleshooting WLANs comprises Layer 1 and Layer 2

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

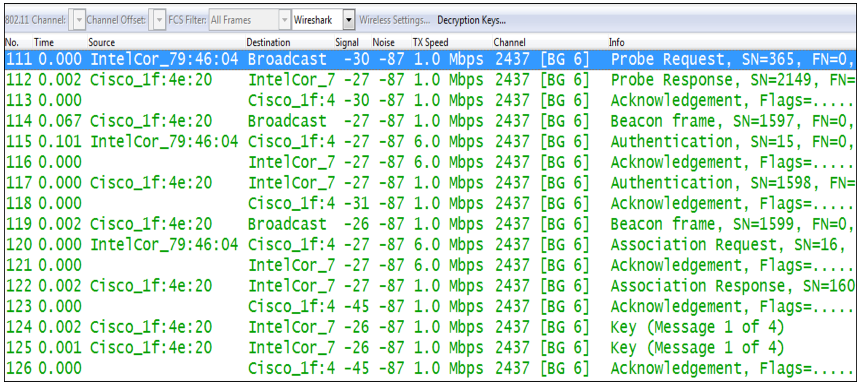


Layer 1 - Physical Access

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)



```
802.11 Channel: ▾ Channel Offset: ▾ FCS Filter: All Frames ▾ Wireshark ▾ Wireless Settings... Decryption Keys...
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 Layer 1 Analysis

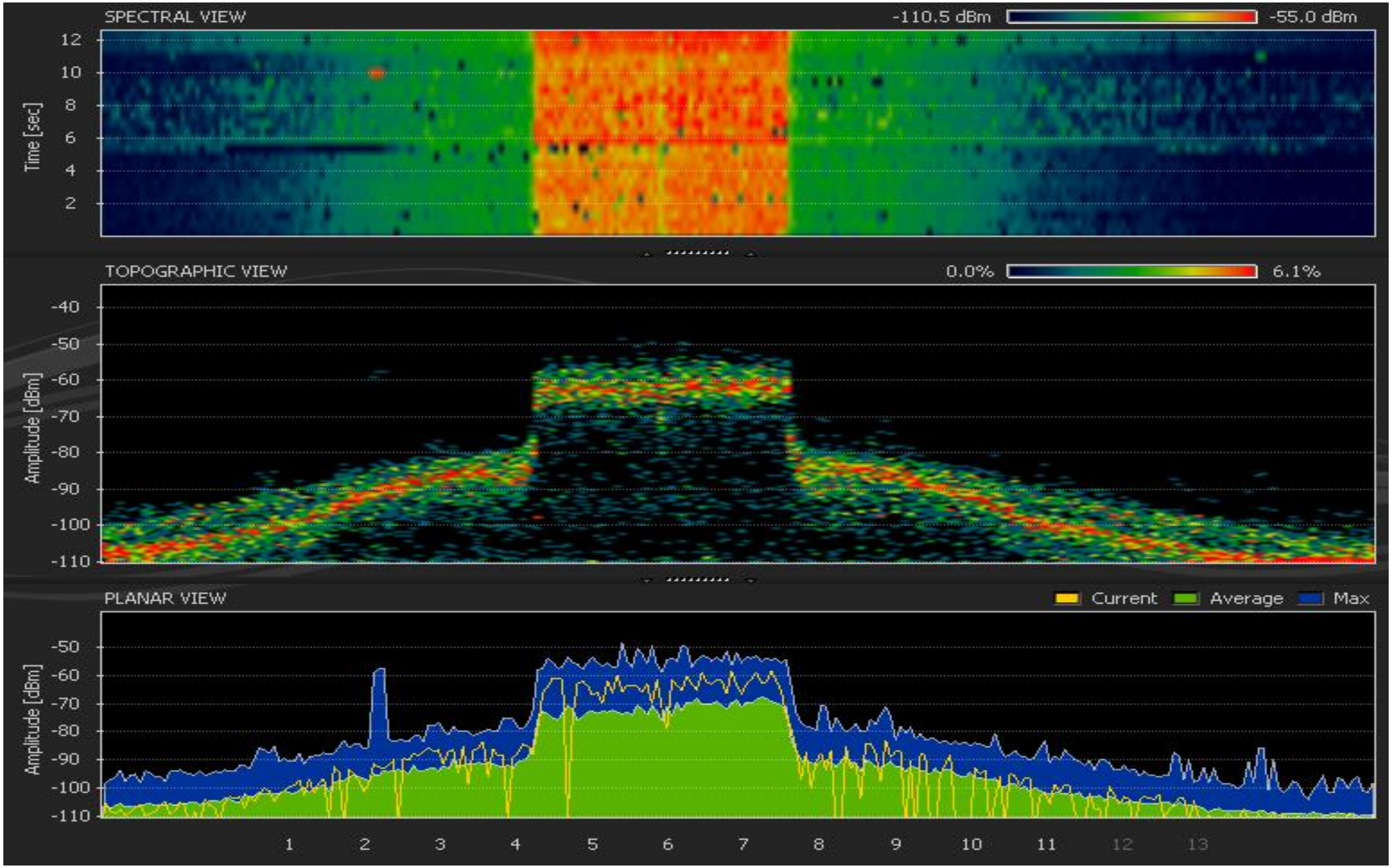
- WLAN Wi Fi devices are working in the 2.4 GHz ISM* and 5 GHz UNII** bands
- But both bands are free for any use, WiFi as well as non-WiFi devices
- Especially the 2.4 GHz band is often crowded with non-WiFi devices
- The only limitation is max. radiated power according to country regulations
- Non-WiFi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

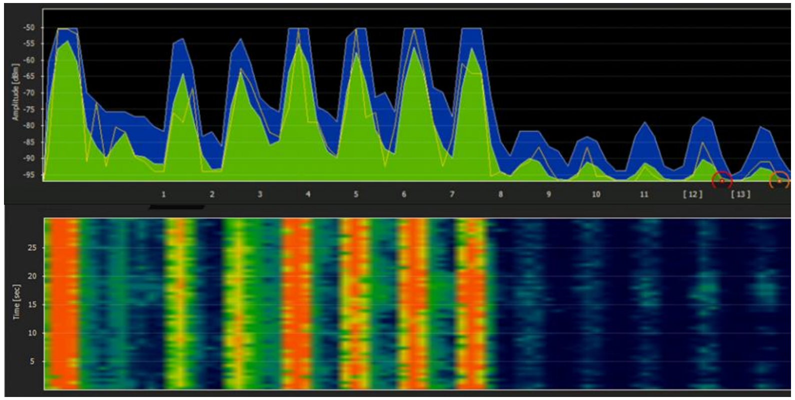
* ISM Industrial, Scientific and Medical
**UNII Unlicensed National Information Infrastructure

WiFi Device Signature in 2.4 GHz Band

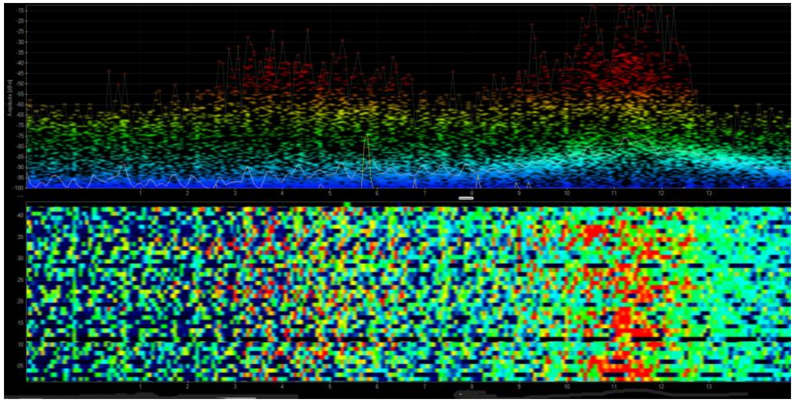


WLAN Layer 1 Analysis

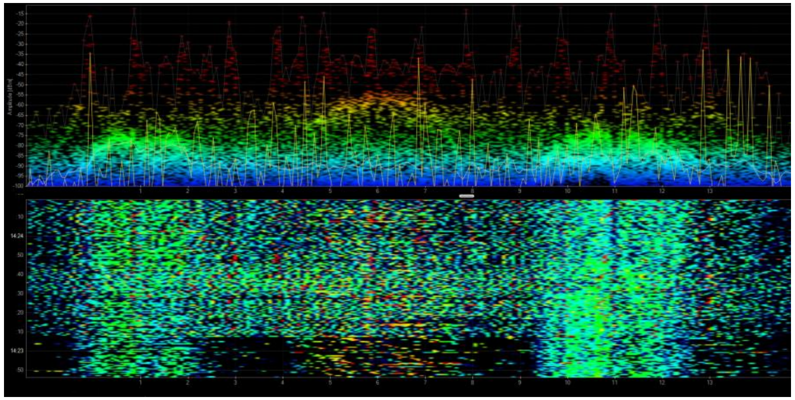
Non-WiFi Device Signatures in 2.4 GHz Band



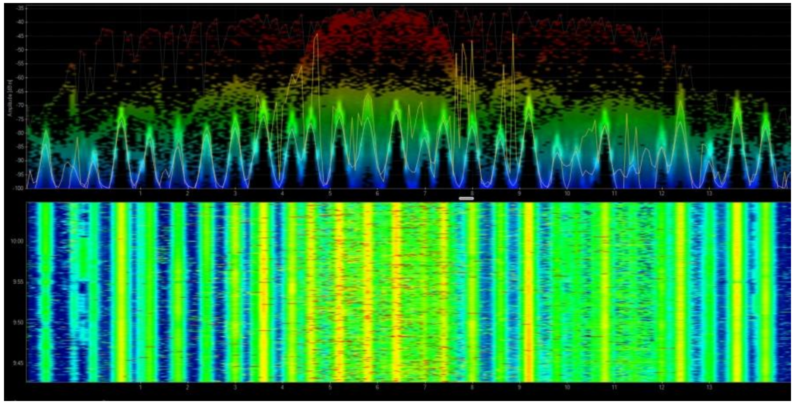
Home trainers in a fitness center



Microwave oven



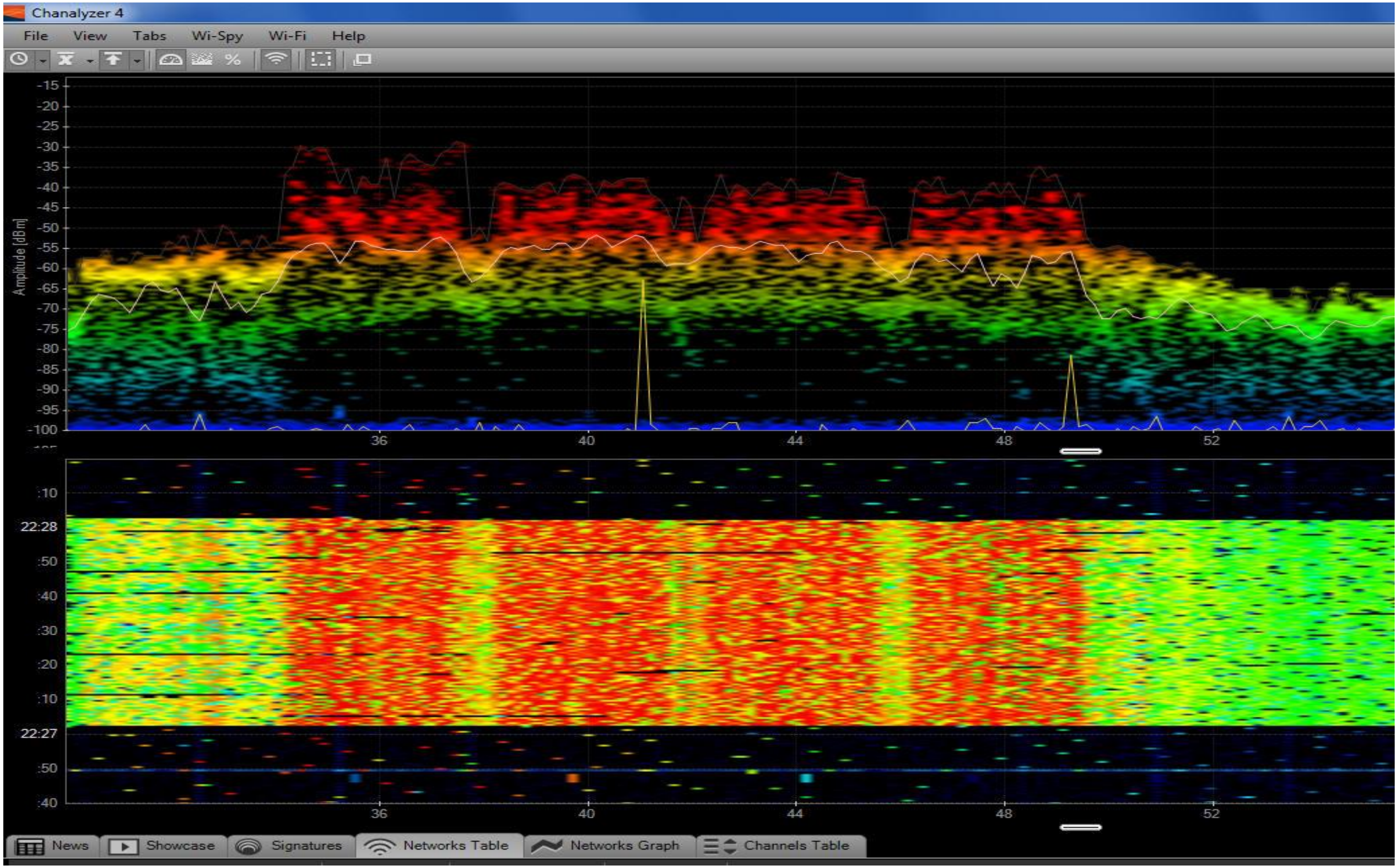
Remote control of model airplanes



Wireless guitar

Live Demo: Wi-Spy & Chanalyzer

WiFi 802.11ac with four bonded channels in 5MHz Band

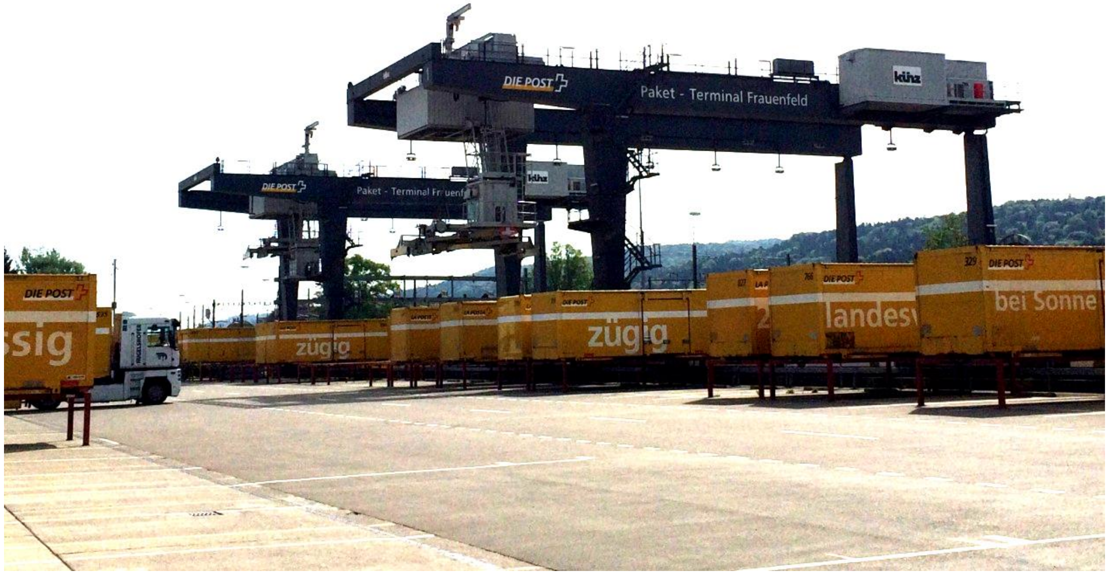


Live Demo: Wi-Spy & Chanalyzer

LIVE DEMONSTRATION
WI-SPY & CHANALYZER

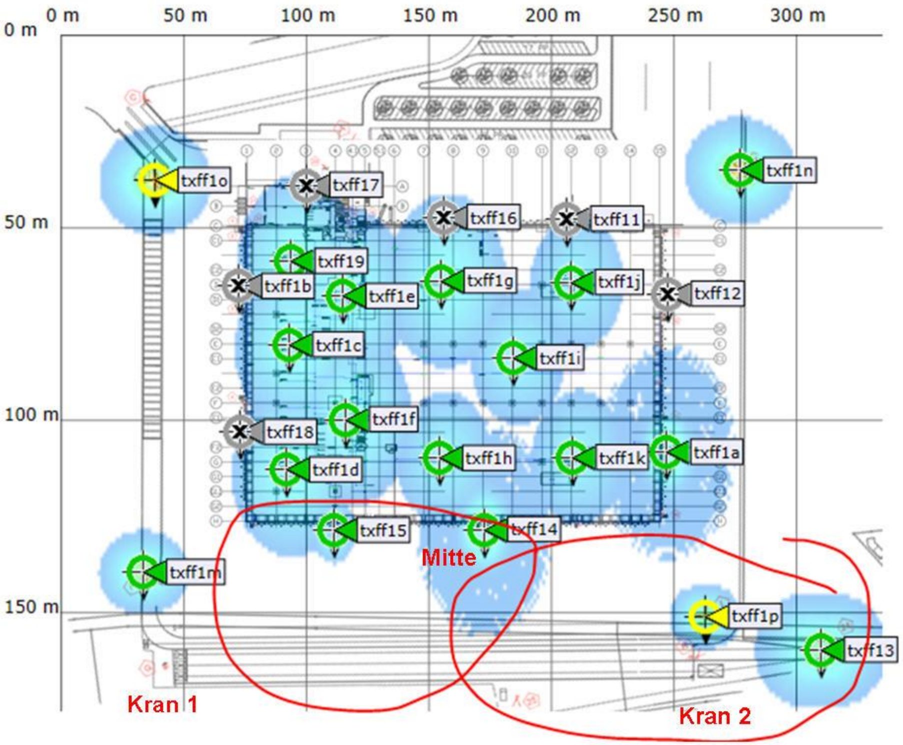
WLAN Layer 1 Analysis (Case one)

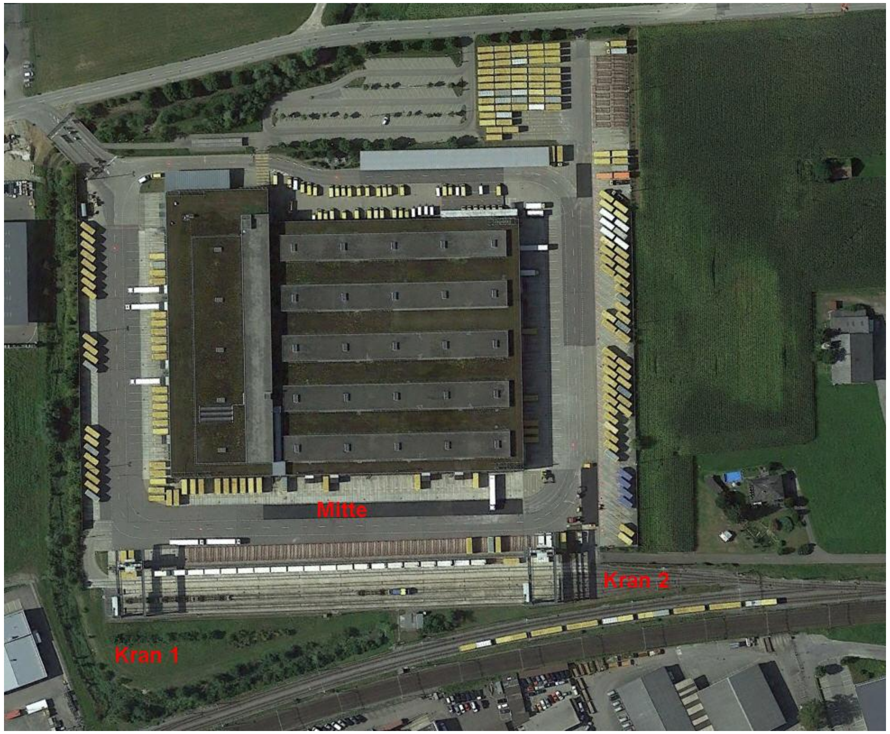
- Large logistic enterprise, fully depending on WLAN for day-to-day operations
- Two container cranes to load/unload trains require WLAN connections



WLAN Layer 1 Analysis (Case one)

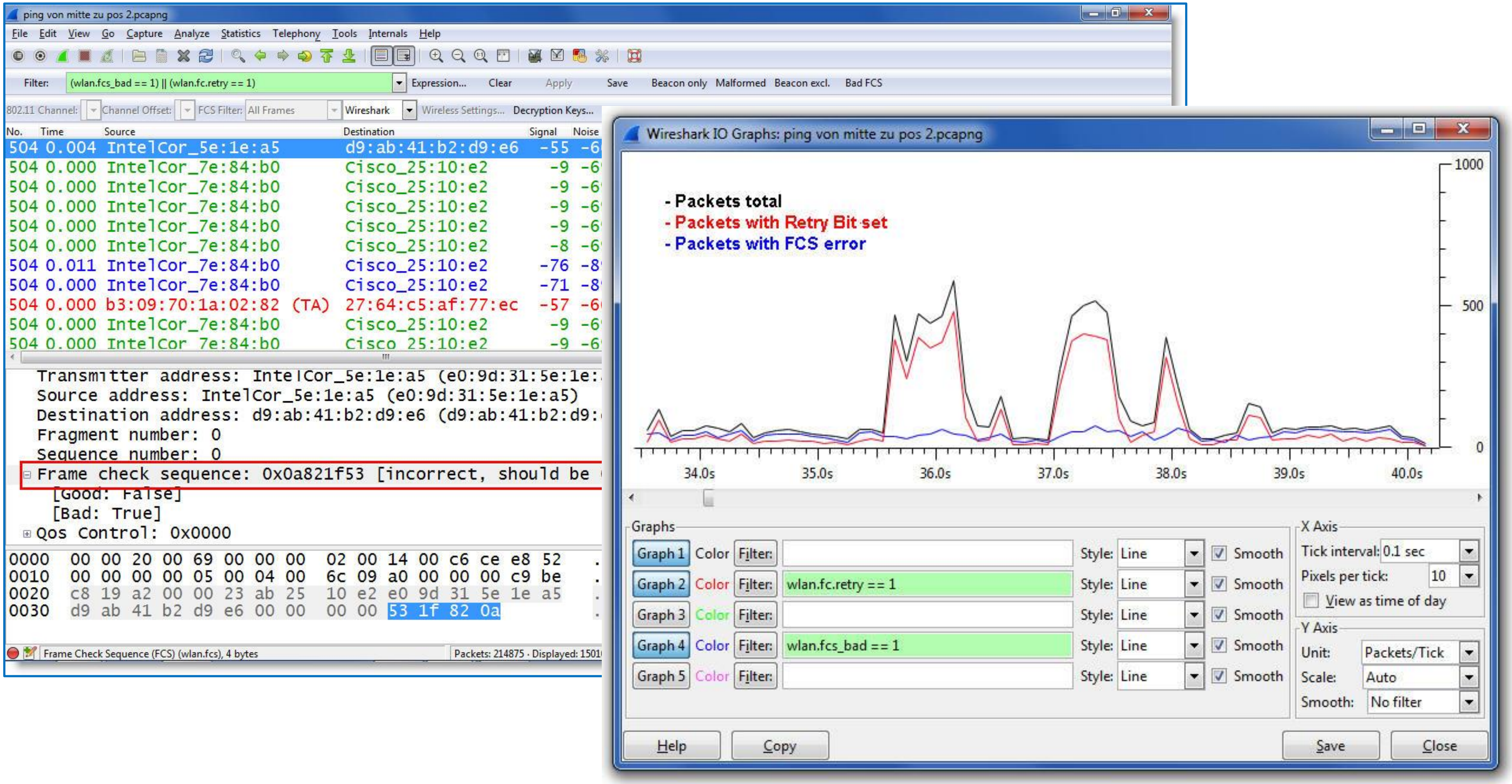
- User complain about log-in timeouts and disconnections during operations
- Crane #2 is hardly usable due to unreliable WLAN connection
- Tech-Support has already changed WiFi channels and added additional AP





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
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save Beacon only Malformed Beacon excl. Bad FCS
Wireless Settings... Decryption Keys...
Wireshark IO Graphs: ping von mitte zu pos 2.pcapng
- Packets total
- Packets with Retry Bit set
- Packets with FCS error
1000
500
0
34.0s
35.0s
36.0s
37.0s
38.0s
39.0s
40.0s
Help
Copy
Save
Close

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

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

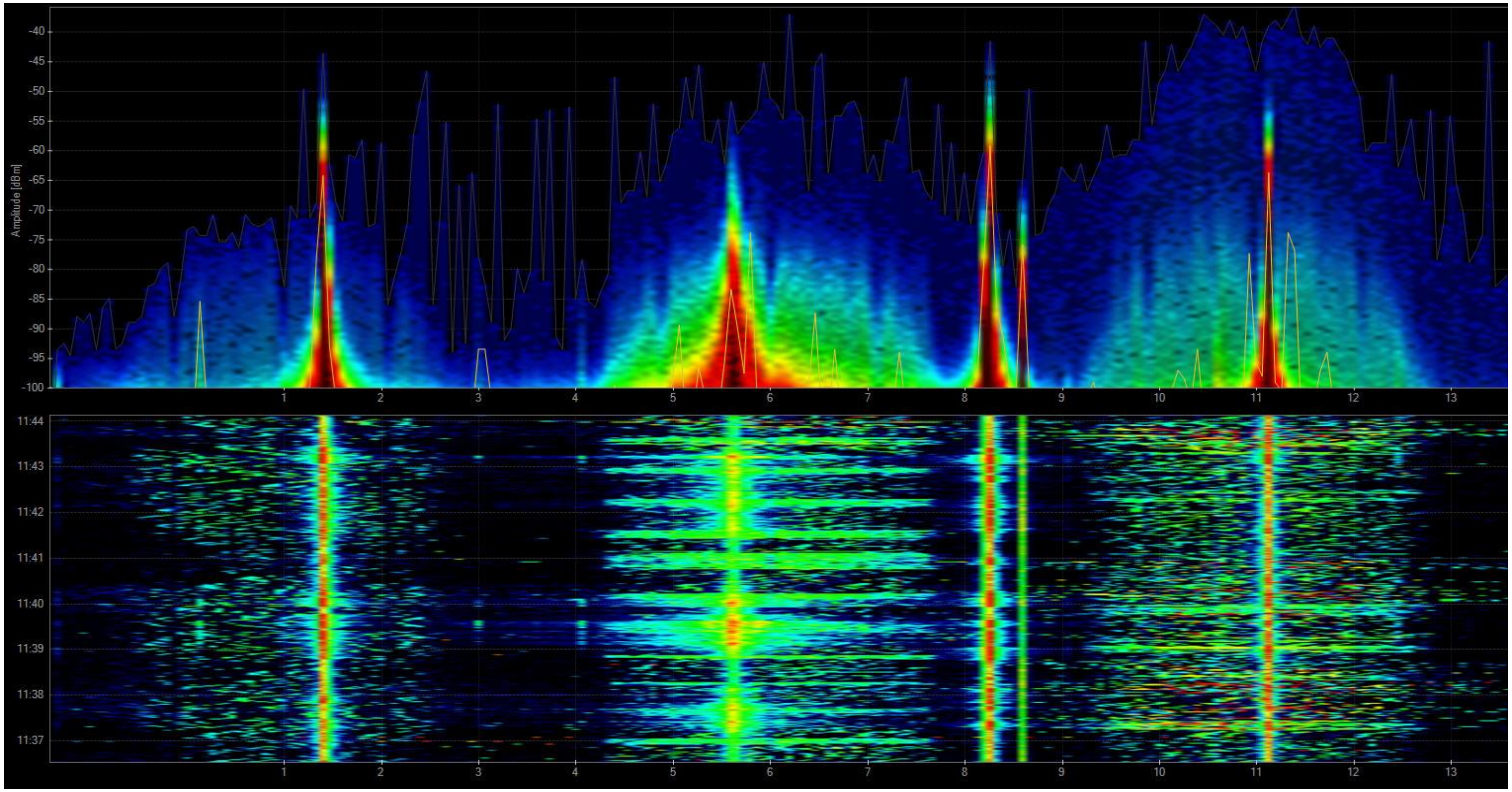
Tick interval: 0.1 sec
Pixels per tick: 10
□ View as time of day

Y Axis

Unit: Packets/Tick
Scale: Auto
Smooth: No filter

WLAN Layer 1 Analysis (Case one)

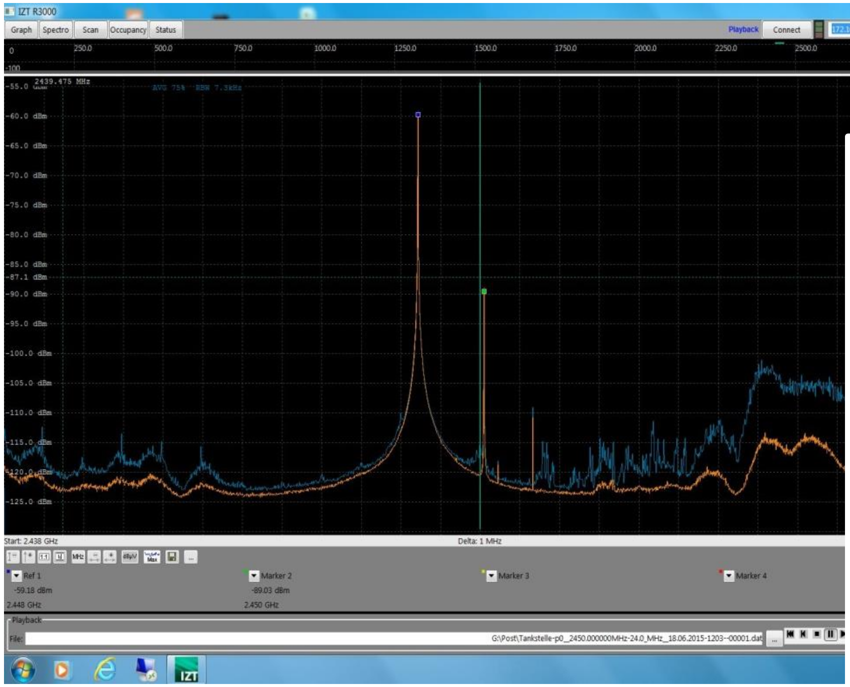
- Continuing with layer 1 analysis near crane #2 in 2.4 GHz band
- Strong interference with a non-WiFi signals on all three channels detected



- 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



BAKOM scan result

Traffic monitoring induction loop

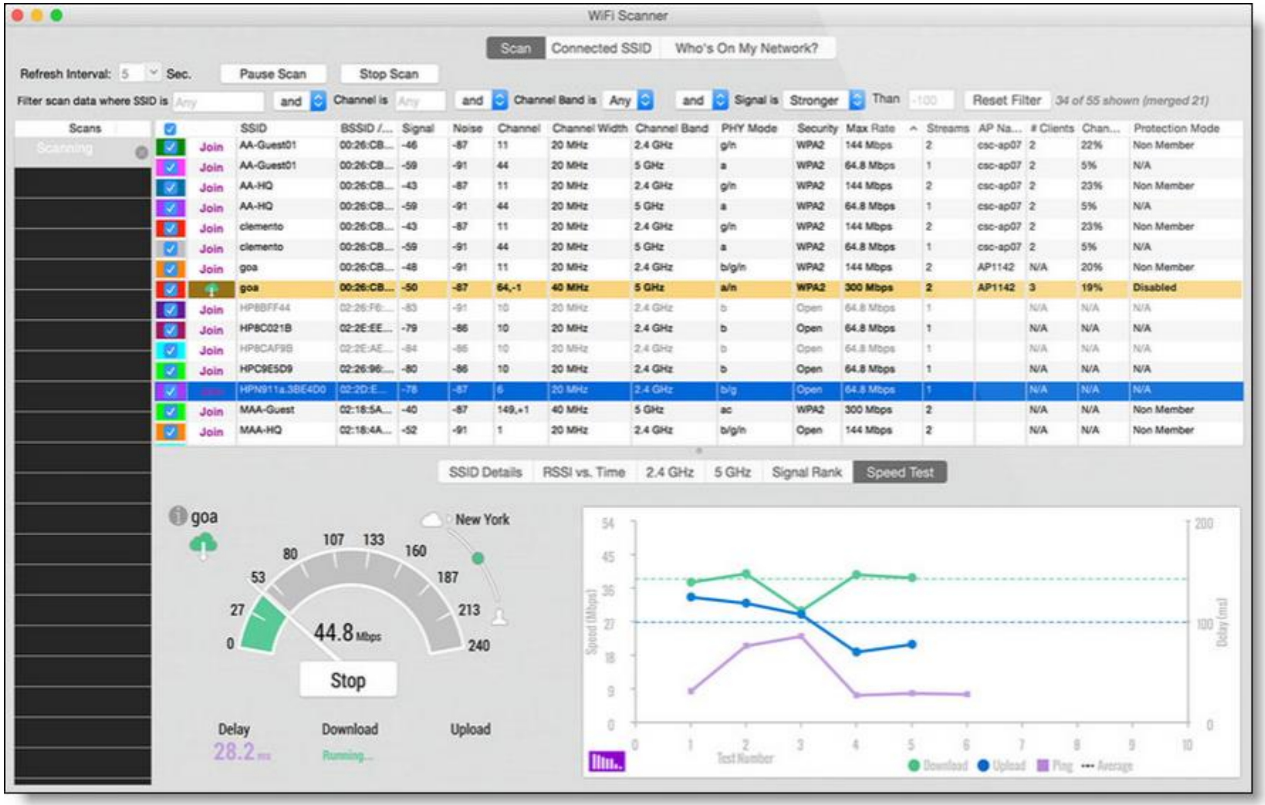
WiFi Scanners (just a few popular ones)

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 (MacOS)	www.apple.com/mac/

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.

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



WiFi Scanner

Scan | Connected SSID | Who's On My Network?

Refresh Interval: 5 Sec. | Pause Scan | Stop Scan

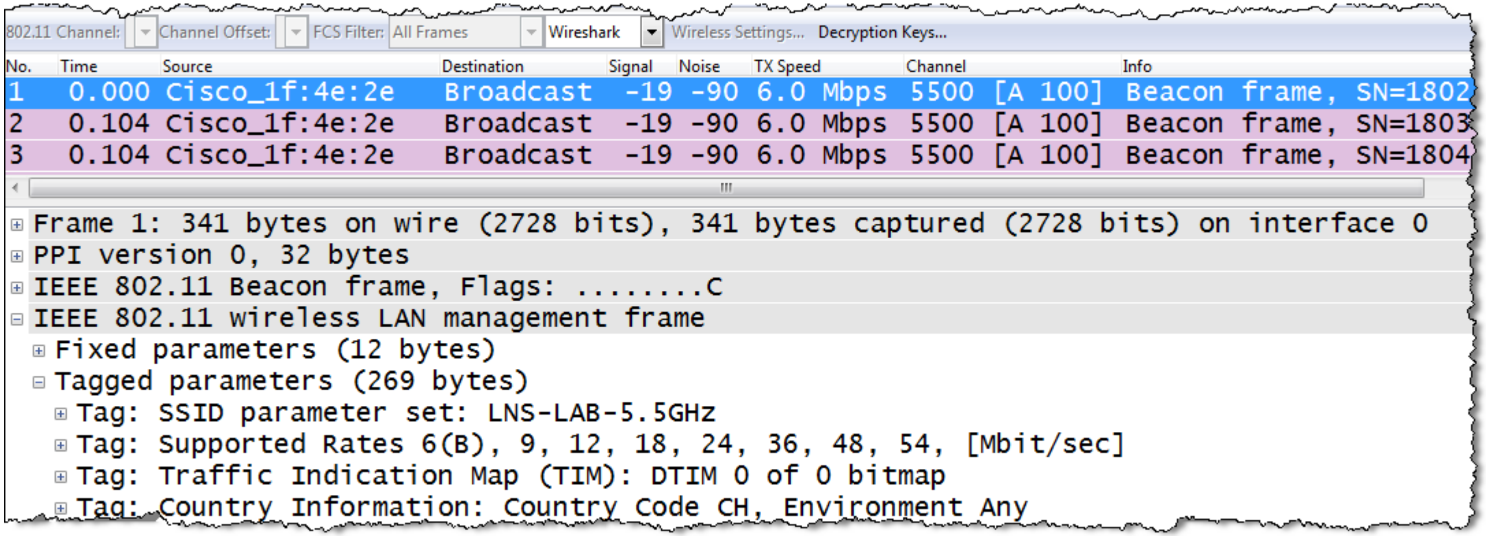
Filter scan data where SSID is Any and Channel is Any and Channel Band is Any and Signal is Stronger Than -100 | Reset Filter | 34 of 55 shown (merged 21)

☑		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

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



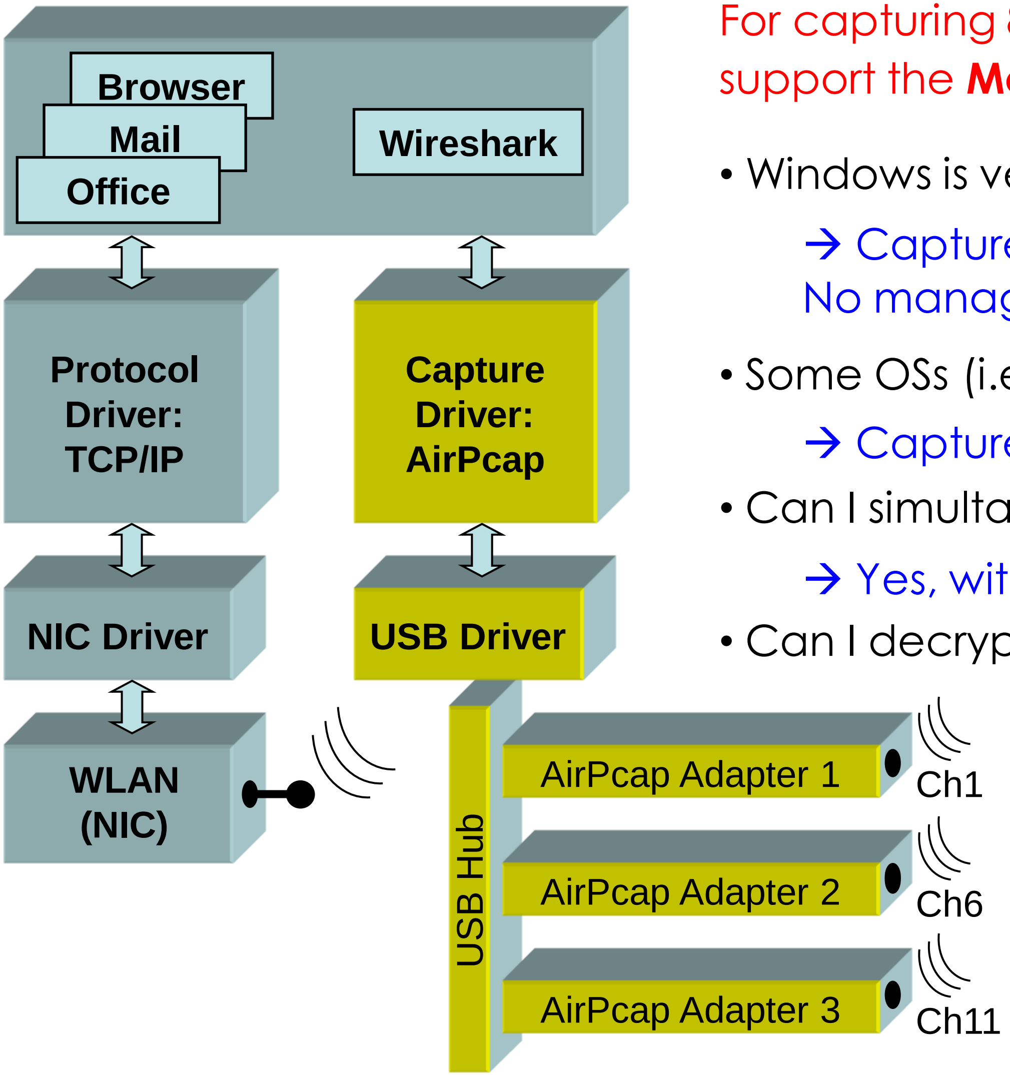
802.11 Channel: | Channel Offset: | FCS Filter: All Frames | Wireshark | Wireless Settings... | Decryption Keys...

```
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!

Capturing 802.11 Packets



For capturing 802.11 traffic the **WLAN NIC** needs to support the **Monitor Mode!** (HW & driver dependent)

- 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

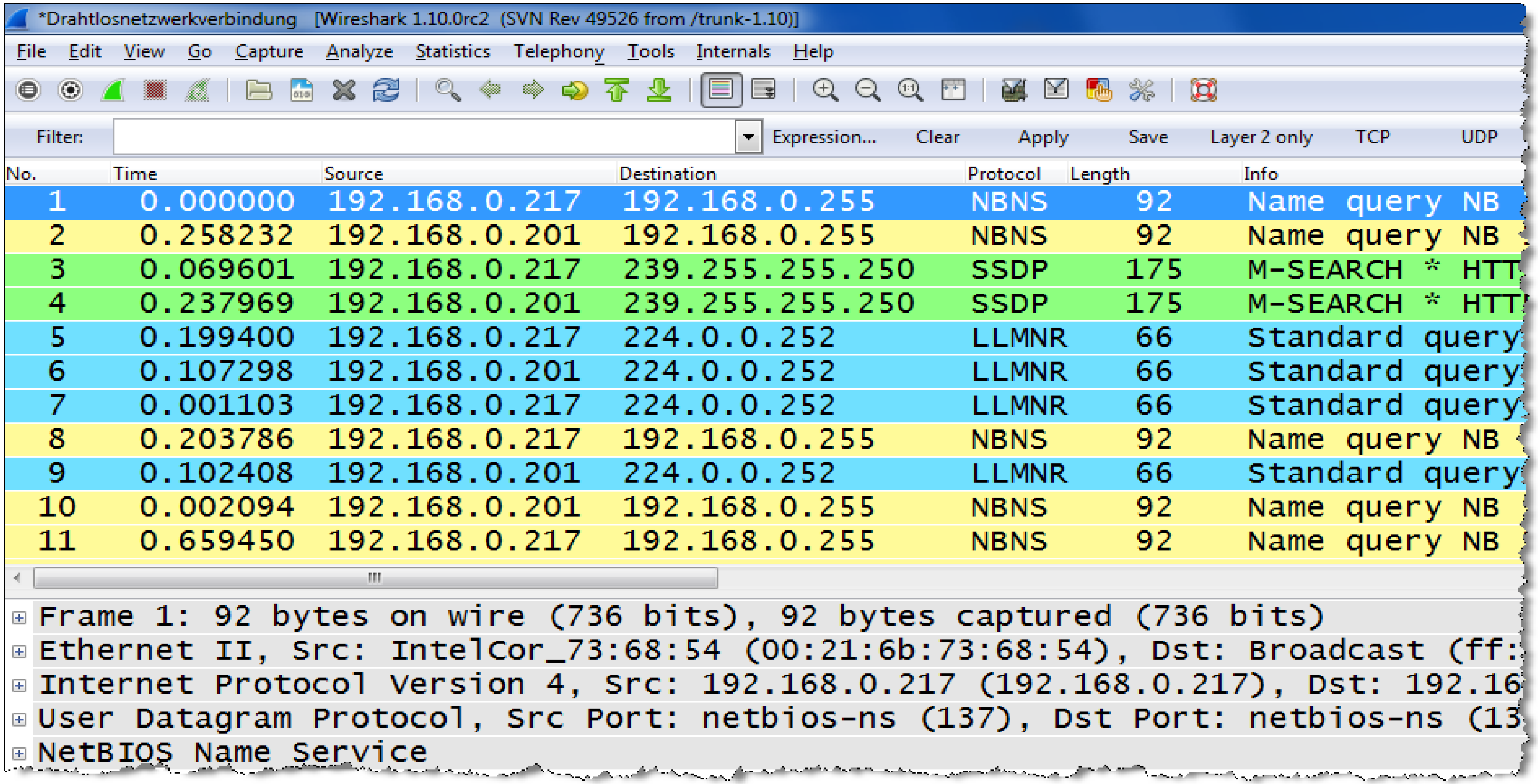
More information:
wiki.wireshark.org/CaptureSetup/WLAN

+

Capturing 802.11 Packets

- WLAN NICs not supporting Monitor Mode may display faked Ethernet frames only
- Only Data frames, no Radio / WLAN header and no Mgmt. / Ctrl. Frames
- Only own traffic and broadcast frames are captured (no promiscuous mode)

→ These WLAN NICs are not suitable for Wi-Fi capturing and analysing!


*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

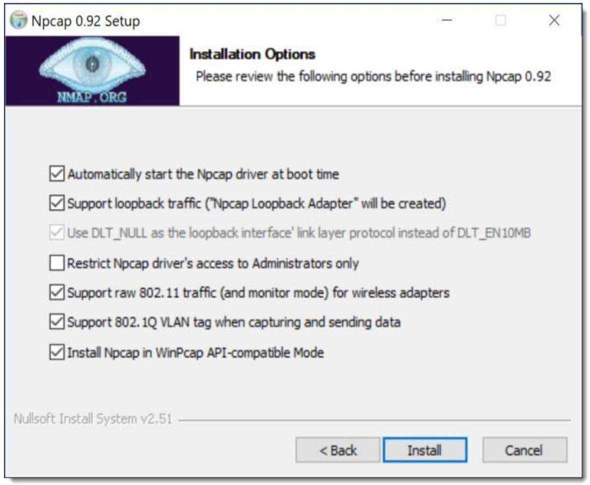
```
⊞ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
⊞ Ethernet II, Src: IntelCor_73:68:54 (00:21:6b:73:68:54), Dst: Broadcast (ff:
⊞ Internet Protocol Version 4, Src: 192.168.0.217 (192.168.0.217), Dst: 192.16
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (13
⊞ NetBIOS Name Service
```

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



Npcap 0.92 Setup

Installation Options

Please review the following options before installing Npcap 0.92

☑ Automatically start the Npcap driver at boot time

☑ Support loopback traffic ("Npcap Loopback Adapter" will be created)

☑ Use DLT_NULL as the loopback interface' link layer protocol instead of DLT_EN10MB

□ Restrict Npcap driver's access to Administrators only

☑ Support raw 802.11 traffic (and monitor mode) for wireless adapters

☑ Support 802.1Q VLAN tag when capturing and sending data

☑ Install Npcap in WinPcap API-compatible Mode

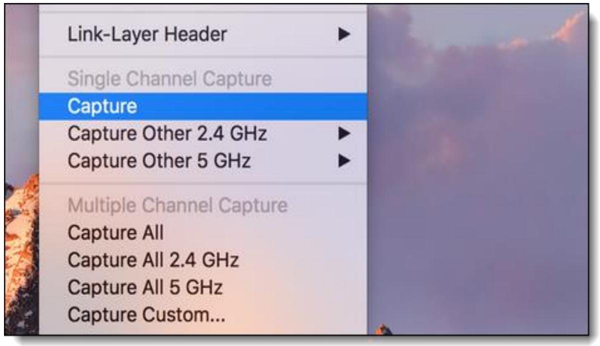
Linux:

- 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

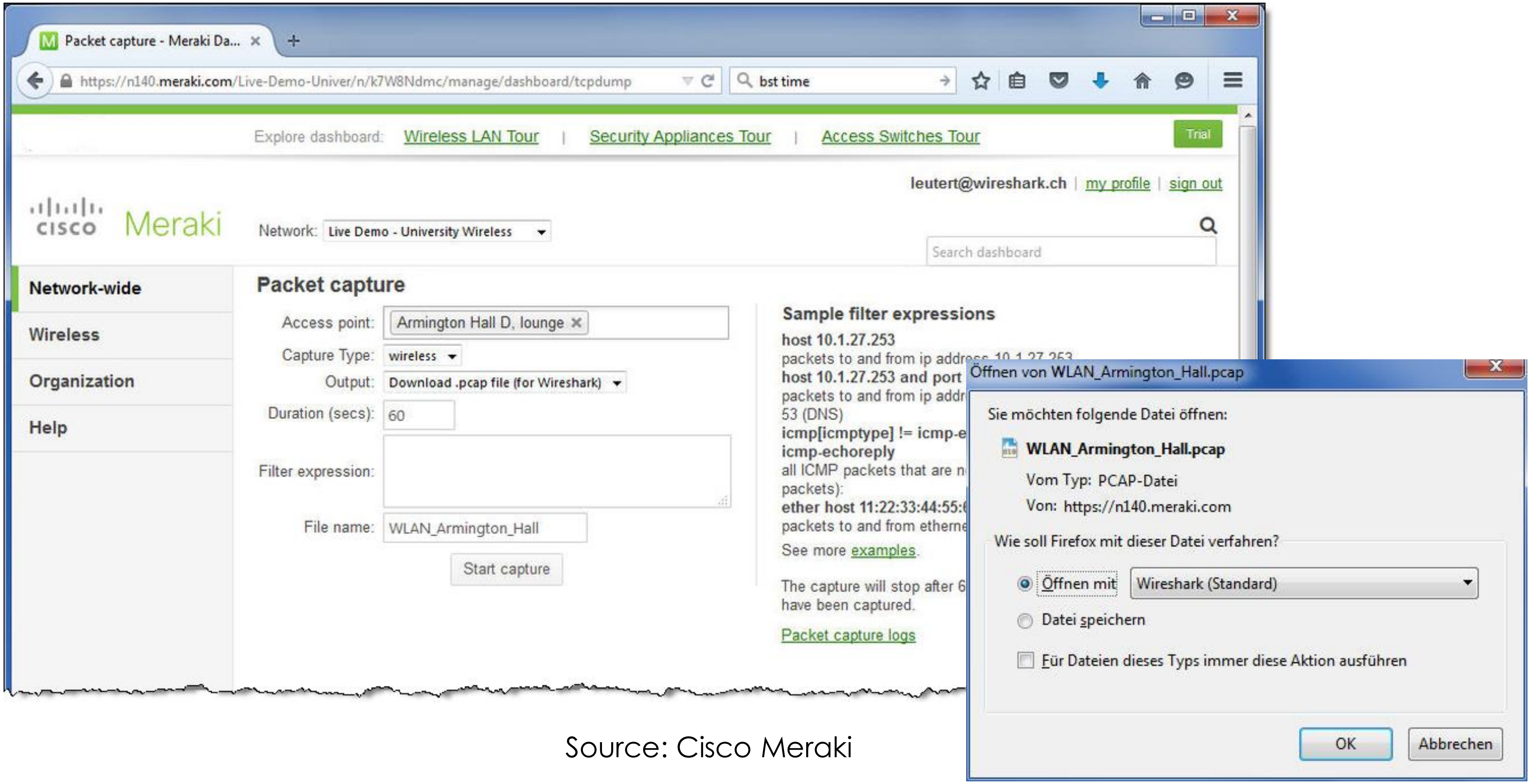
Airtool



Capturing 802.11 Packets on Access Points

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



Packet capture - Meraki Da...

https://n140.meraki.com/Live-Demo-Univer/n/k7W8Ndmc/manage/dashboard/tcpdump

bst time

Explore dashboard: Wireless LAN Tour | Security Appliances Tour | Access Switches Tour

Trial

leutert@wireshark.ch | my profile | sign out

cisco Meraki

Network: Live Demo - University Wireless

Search dashboard

Network-wide
Wireless
Organization
Help

Packet capture

Access point: Armington Hall D, lounge ×
Capture Type: wireless
Output: Download .pcap file (for Wireshark)
Duration (secs): 60
Filter expression:
File name: WLAN_Armington_Hall

Start capture

Sample filter expressions

host 10.1.27.253
packets to and from ip address 10.1.27.253
host 10.1.27.253 and port
packets to and from ip addr
53 (DNS)
icmp[icmptype] != icmp-e
icmp-echoreply
all ICMP packets that are n
packets)
ether host 11:22:33:44:55:
packets to and from etherne
See more examples.

The capture will stop after 6
have been captured.

Packet capture logs

Öffnen von WLAN_Armington_Hall.pcap

Sie möchten folgende Datei öffnen:

WLAN_Armington_Hall.pcap
Vom Typ: PCAP-Datei
Von: https://n140.meraki.com

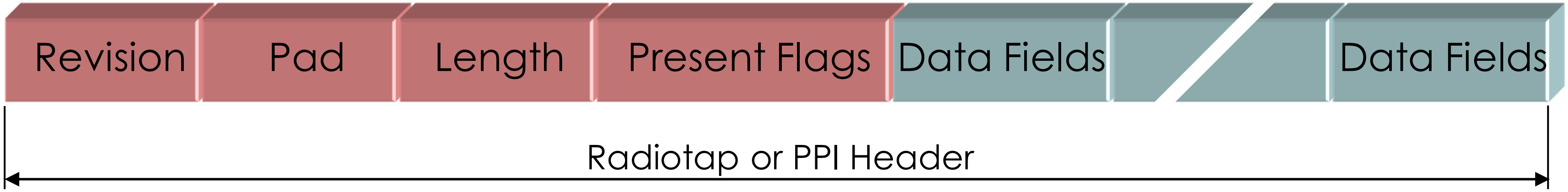
Wie soll Firefox mit dieser Datei verfahren?

● Öffnen mit Wireshark (Standard)
○ Datei speichern
□ Für Dateien dieses Typs immer diese Aktion ausführen

OK Abbrechen

Source: Cisco Meraki

The Radiotap and PPI pseudo-header



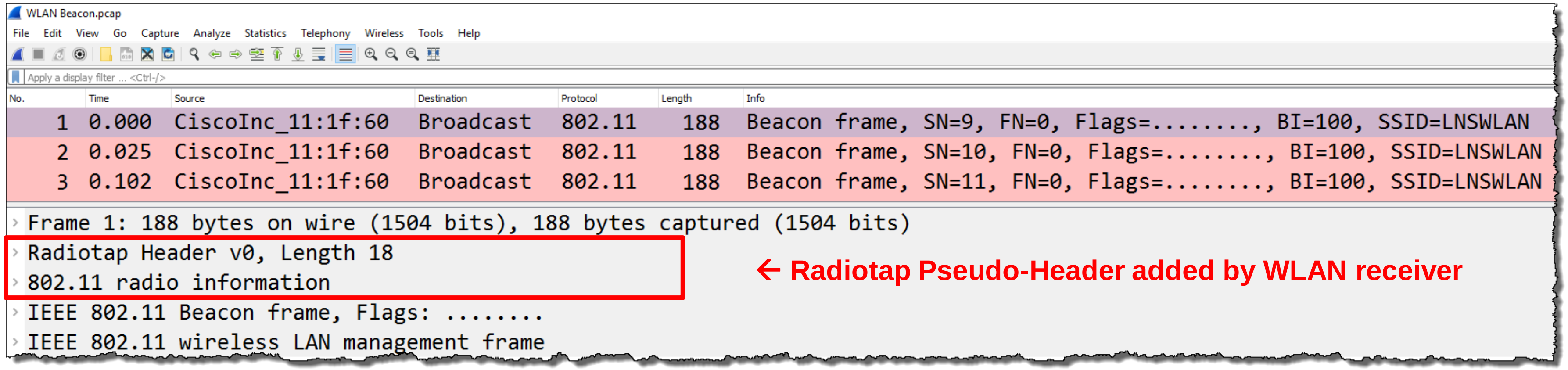
- The Radiotap or the PPI (Per Packet Information) are so called *Link-layer pseudo-headers* because they are not transmitted with the frame.
- They are added by the driver during reception and contain additional radio information about the incoming frame.
- Provides Receive Signal Strength, bit rate, 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

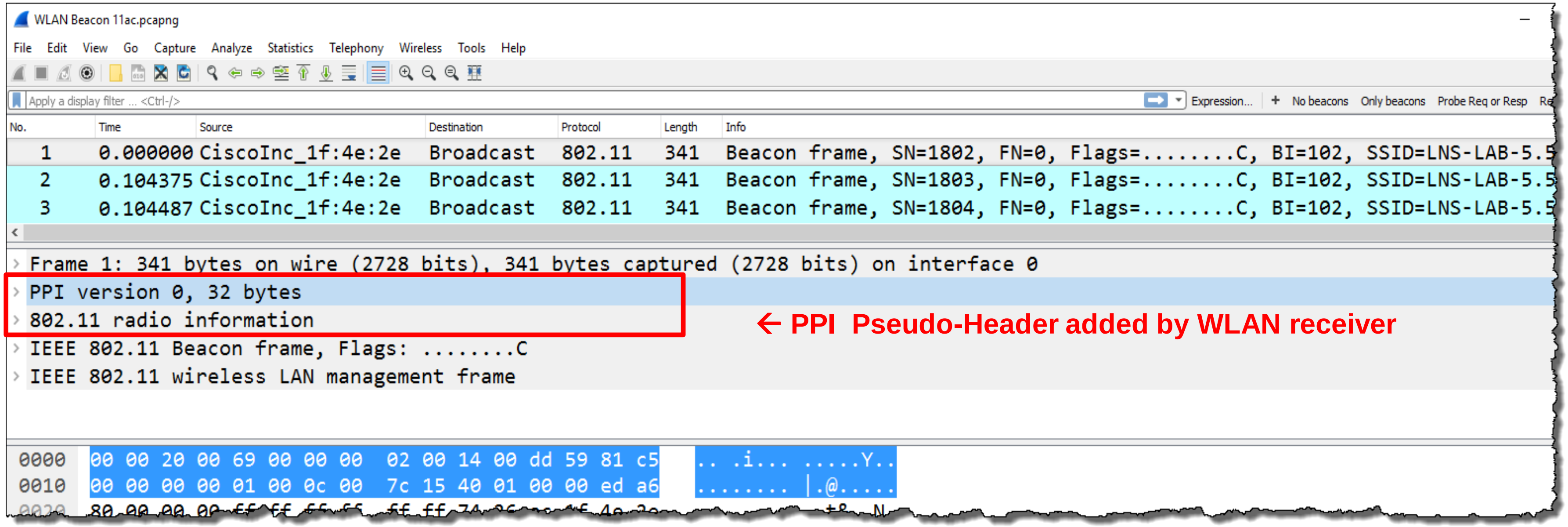
The Radiotap and PPI pseudo-header



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 WLAN receiver



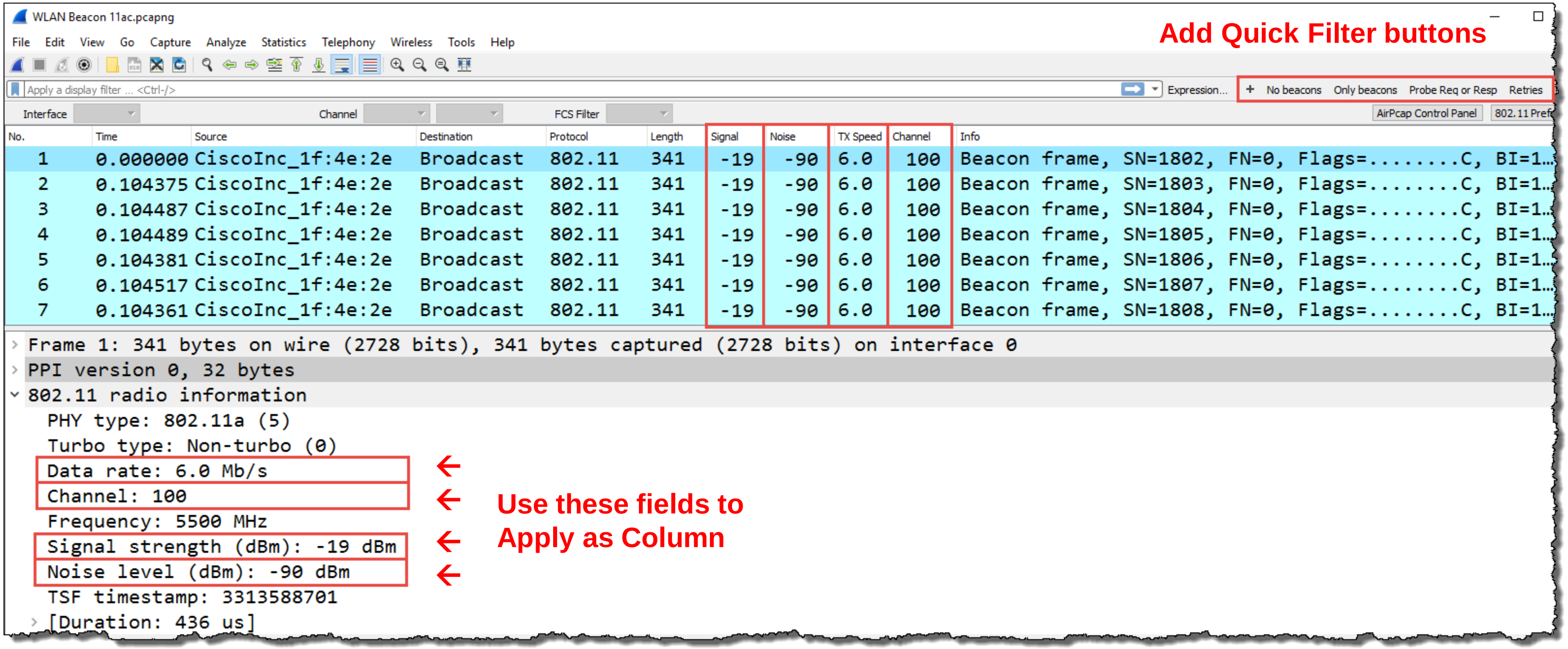
WLAN Beacon 11ac.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
No beacons
Only beacons
Probe Req or Resp
Re

```
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
```

← 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

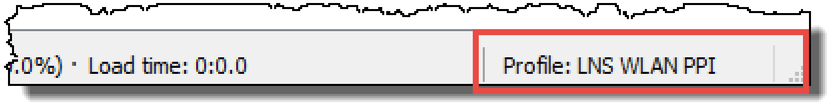

WLAN Beacon 11ac.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+ No beacons Only beacons Probe Req or Resp Retries
Interface
Channel
FCS Filter
AirPcap Control Panel
802.11 Pref

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]
```

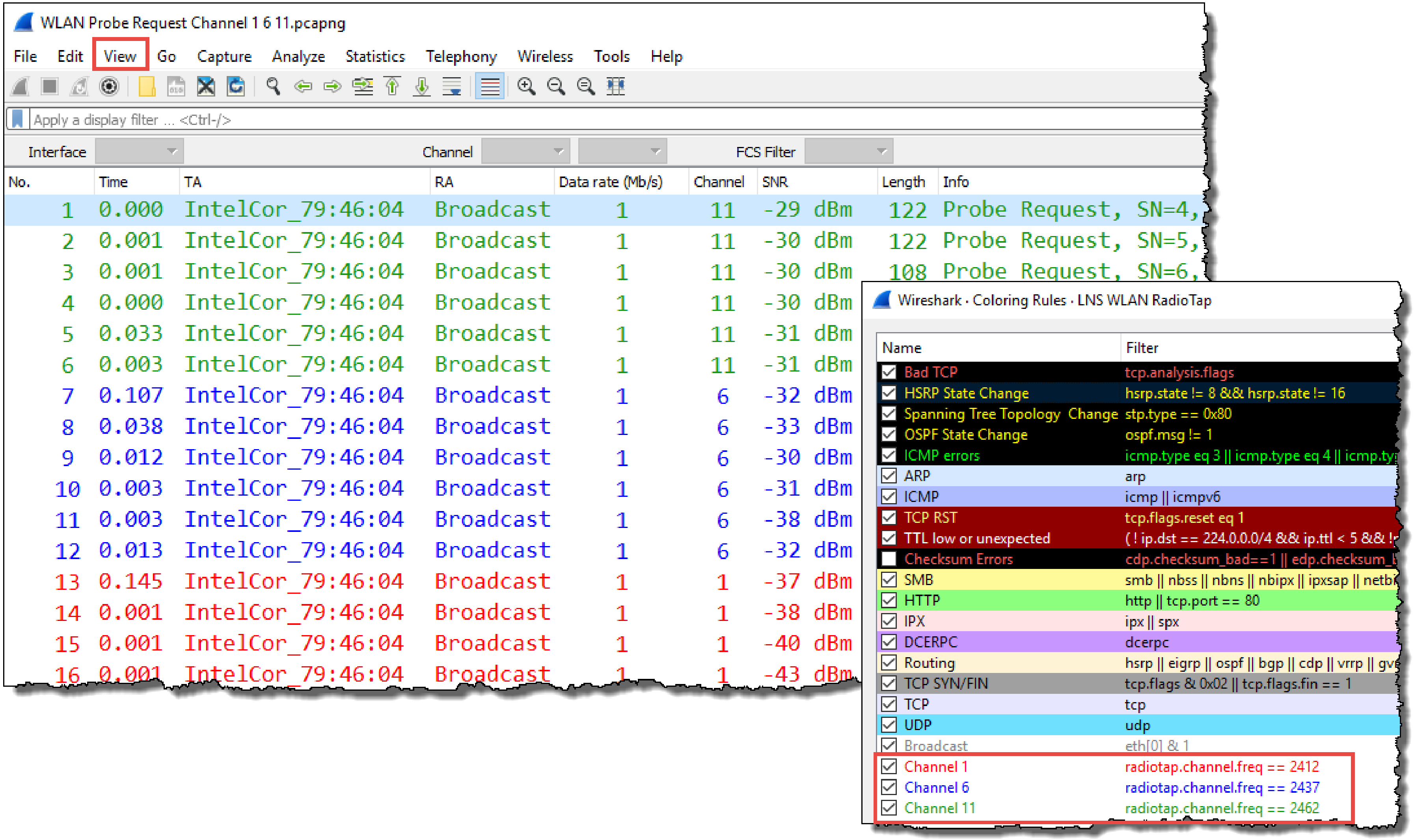
Use these fields to Apply as Column


.0%) · Load time: 0:0.0

Profile: LNS WLAN PPI

Customize Wireshark for WLAN analysis

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

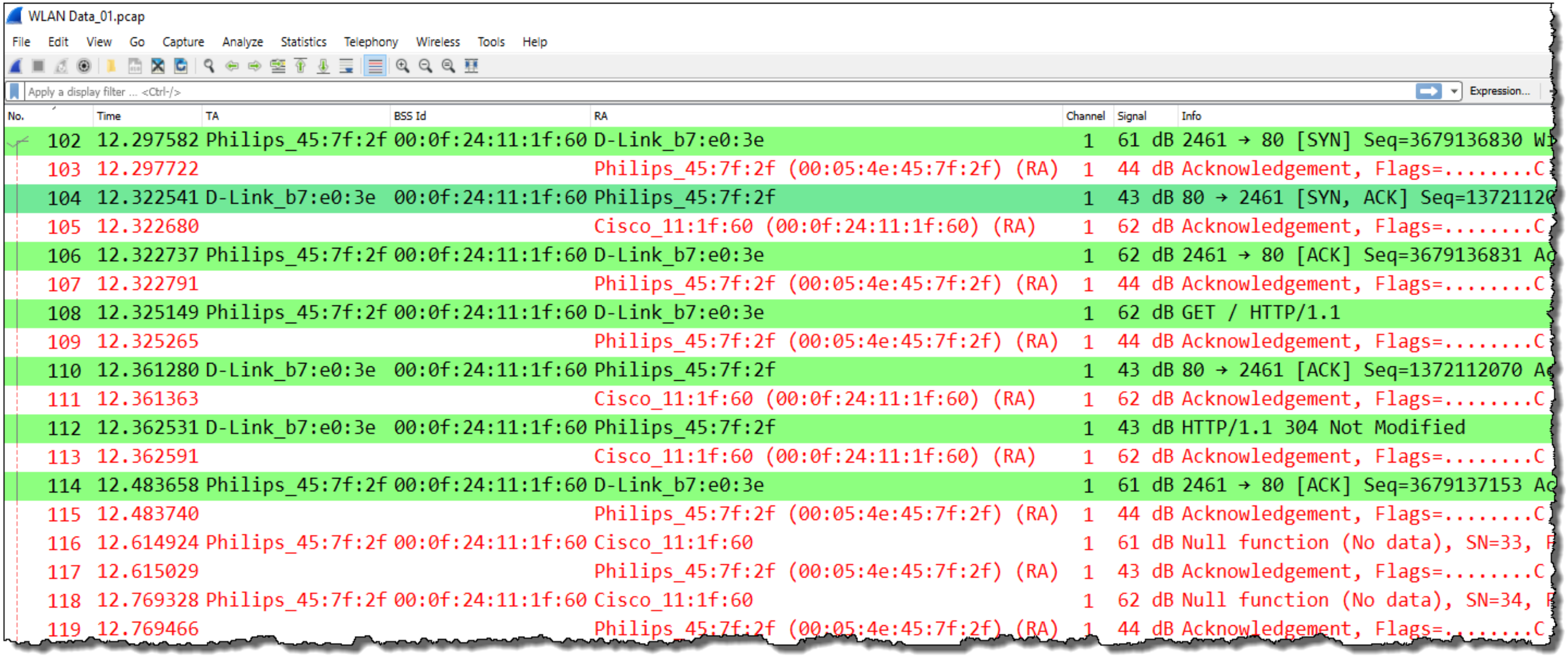

WLAN Probe Request Channel 1 6 11.pcapng
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter … <Ctrl-/>
Interface
Channel
FCS Filter
Wireshark · Coloring Rules · LNS WLAN RadioTap

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		

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

Analysing WiFi Data Transmission

- In non-aggregation mode each packet is acknowledged individually
- The acknowledge frame follows immediately after each data frame
- The (single) acknowledge has no source address field


WLAN Data_01.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

No.	Time	TA	BSS Id	RA	Channel	Signal	Info
102	12.297582	Philips_45:7f:2f	00:0f:24:11:1f:60	D-Link_b7:e0:3e	1	61 dB	2461 → 80 [SYN] Seq=3679136830 Wi
103	12.297722			Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	1	44 dB	Acknowledgement, Flags=........C
104	12.322541	D-Link_b7:e0:3e	00:0f:24:11:1f:60	Philips_45:7f:2f	1	43 dB	80 → 2461 [SYN, ACK] Seq=13721120
105	12.322680			Cisco_11:1f:60 (00:0f:24:11:1f:60) (RA)	1	62 dB	Acknowledgement, Flags=........C
106	12.322737	Philips_45:7f:2f	00:0f:24:11:1f:60	D-Link_b7:e0:3e	1	62 dB	2461 → 80 [ACK] Seq=3679136831 Ac
107	12.322791			Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	1	44 dB	Acknowledgement, Flags=........C
108	12.325149	Philips_45:7f:2f	00:0f:24:11:1f:60	D-Link_b7:e0:3e	1	62 dB	GET / HTTP/1.1
109	12.325265			Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	1	44 dB	Acknowledgement, Flags=........C
110	12.361280	D-Link_b7:e0:3e	00:0f:24:11:1f:60	Philips_45:7f:2f	1	43 dB	80 → 2461 [ACK] Seq=1372112070 Ac
111	12.361363			Cisco_11:1f:60 (00:0f:24:11:1f:60) (RA)	1	62 dB	Acknowledgement, Flags=........C
112	12.362531	D-Link_b7:e0:3e	00:0f:24:11:1f:60	Philips_45:7f:2f	1	43 dB	HTTP/1.1 304 Not Modified
113	12.362591			Cisco_11:1f:60 (00:0f:24:11:1f:60) (RA)	1	62 dB	Acknowledgement, Flags=........C
114	12.483658	Philips_45:7f:2f	00:0f:24:11:1f:60	D-Link_b7:e0:3e	1	61 dB	2461 → 80 [ACK] Seq=3679137153 Ac
115	12.483740			Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	1	44 dB	Acknowledgement, Flags=........C
116	12.614924	Philips_45:7f:2f	00:0f:24:11:1f:60	Cisco_11:1f:60	1	61 dB	Null function (No data), SN=33, F
117	12.615029			Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	1	43 dB	Acknowledgement, Flags=........C
118	12.769328	Philips_45:7f:2f	00:0f:24:11:1f:60	Cisco_11:1f:60	1	62 dB	Null function (No data), SN=34, F
119	12.769466			Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	1	44 dB	Acknowledgement, Flags=........C

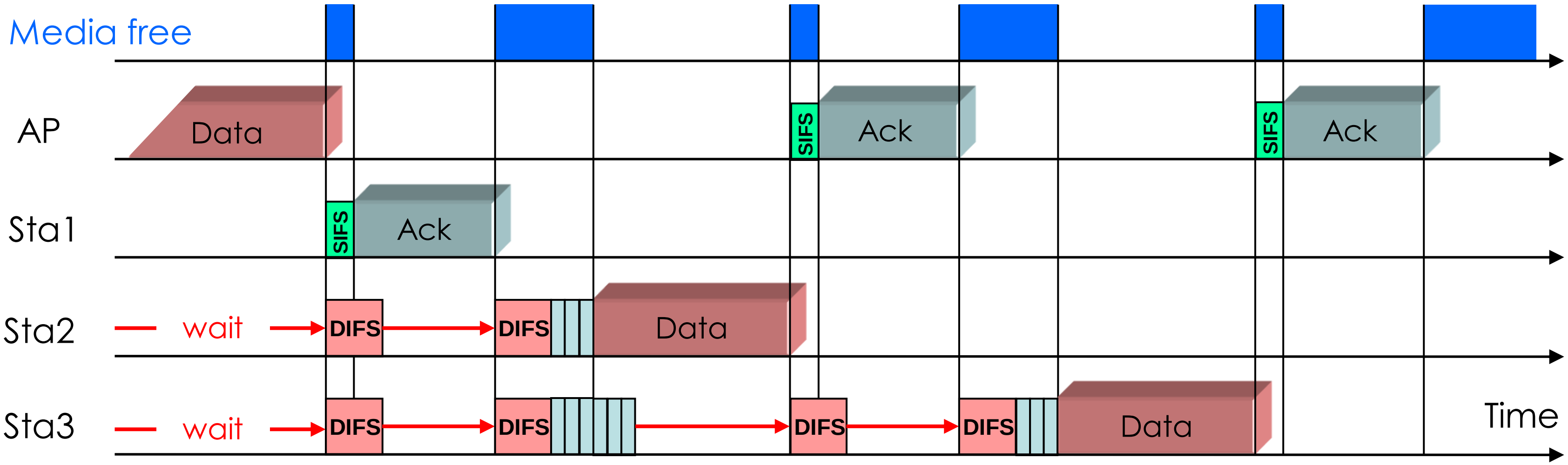
Access Control with CSMA/CA

- 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 holds 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

Capturing 802.11 Packets in multiple Channels

Wi-Fi basic features:

- Each radio cell is a shared media and is controlled by an Access Point (AP)
- A radio cell access is controlled by managements and control frames
- A mobile client can be associated with only one AP at the time
- Standard channel width is 20 MHz, channels should not overlap
- 802.11n/ac supports bonding of adjacent channels to 40/80/160 MHz width
- A mobile client can change to other AP with the same SSID (seamless roaming)
- Following a roaming client requires capturing in multiple channels simultaneously

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

+

Capturing 802.11 Packets with WaveXpert

- 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 power
  - **WaveXpert 1** dual band 2.4 GHz and 5 GHz
  - **WaveXpert 2** single band 5 GHz (up to 160MHz)
  - Creates pcapng files incl. Radiotap header

-
  - Regular price: EUR 2’490
  - Intro price: EUR 1’950 (till 15. Nov. 2019)

Multi-Channel WLAN Sniffer

- Requirements:
  - LINUX notebook with USB-C (Thunderbolt 3)
  - Supporting Ubuntu/Mint Linux’s

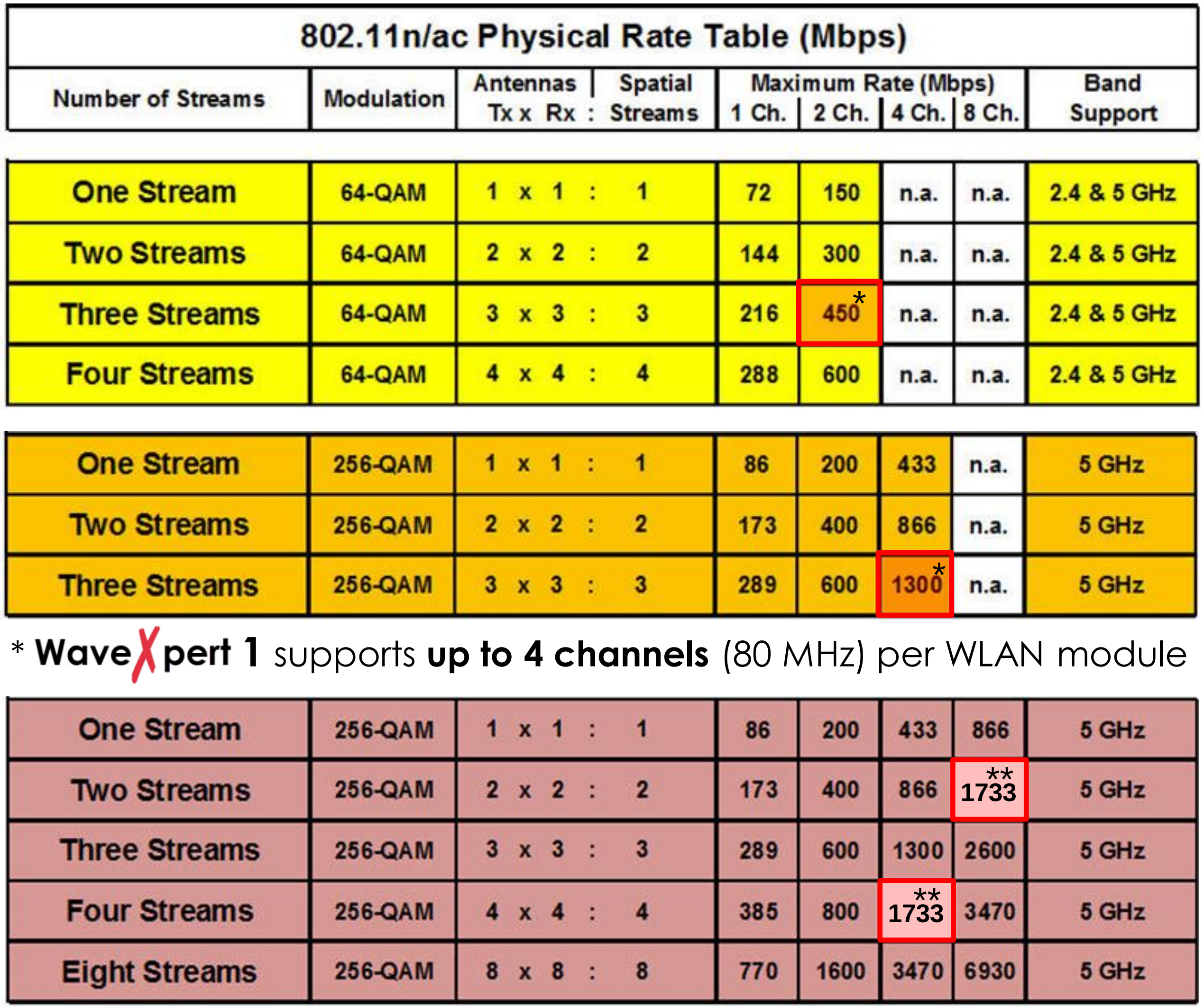
https://itnetworks.softing.com/wireless-lan/wavexpert/

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)

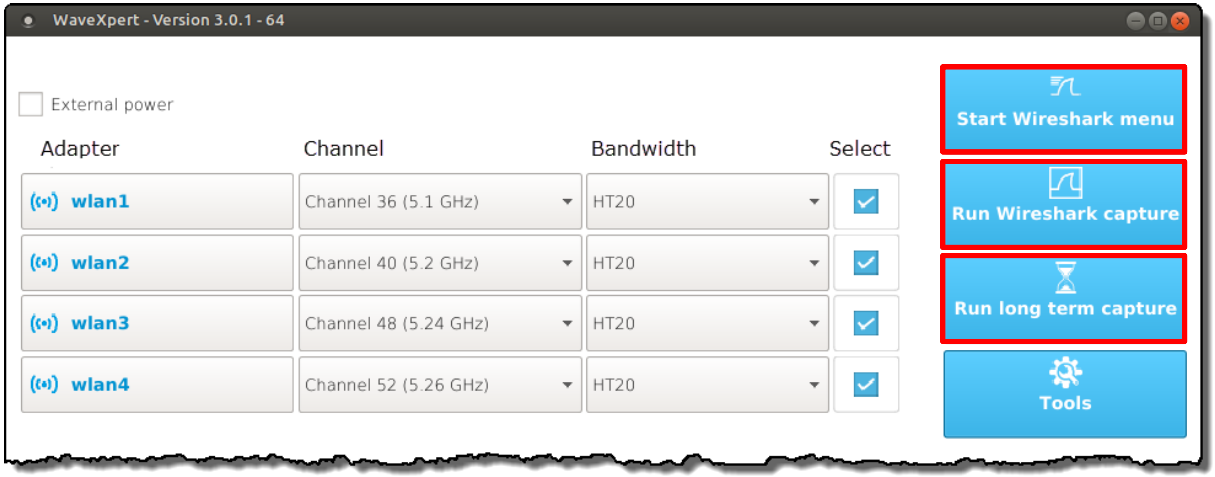
	Number of Streams	Modulation	Antennas Tx x Rx	Spatial : Streams	Maximum Rate (Mbps) 1 Ch.	 2 Ch.	 4 Ch.	 8 Ch.	Band Support
802.11n	One Stream	64-QAM	1 x 1	1	72	150	n.a.	n.a.	2.4 & 5 GHz
	Two Streams	64-QAM	2 x 2	2	144	300	n.a.	n.a.	2.4 & 5 GHz
	Three Streams	64-QAM	3 x 3	3	216	450*	n.a.	n.a.	2.4 & 5 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	**1733	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	**1733	3470	5 GHz
	Eight Streams	256-QAM	8 x 8	8	770	1600	3470	6930	5 GHz

* **WaveXpert 1** supports **up to 4 channels** (80 MHz) per WLAN module

** **WaveXpert 2** supports **up to 8 channels** (160 MHz) per WLAN module

Capturing 802.11 Packets with WaveXpert

WaveXpert configuration menu allows to select up to four adapters for capturing

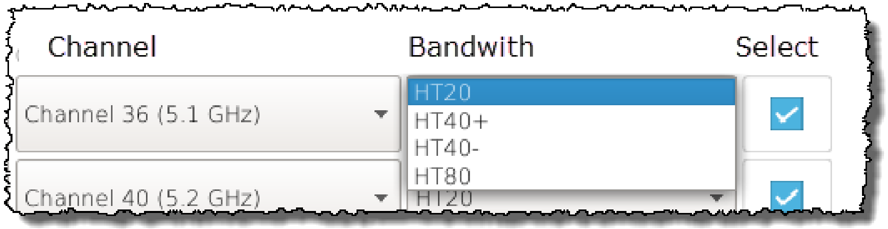


WaveXpert - Version 3.0.1 - 64

□ External power

Adapter	Channel	Bandwidth	Select
wlan1	Channel 36 (5.1 GHz)	HT20	☑
wlan2	Channel 40 (5.2 GHz)	HT20	☑
wlan3	Channel 48 (5.24 GHz)	HT20	☑
wlan4	Channel 52 (5.26 GHz)	HT20	☑

- Each adapter supports Bandwidth up to 80MHz (four 20MHz channels bonded)

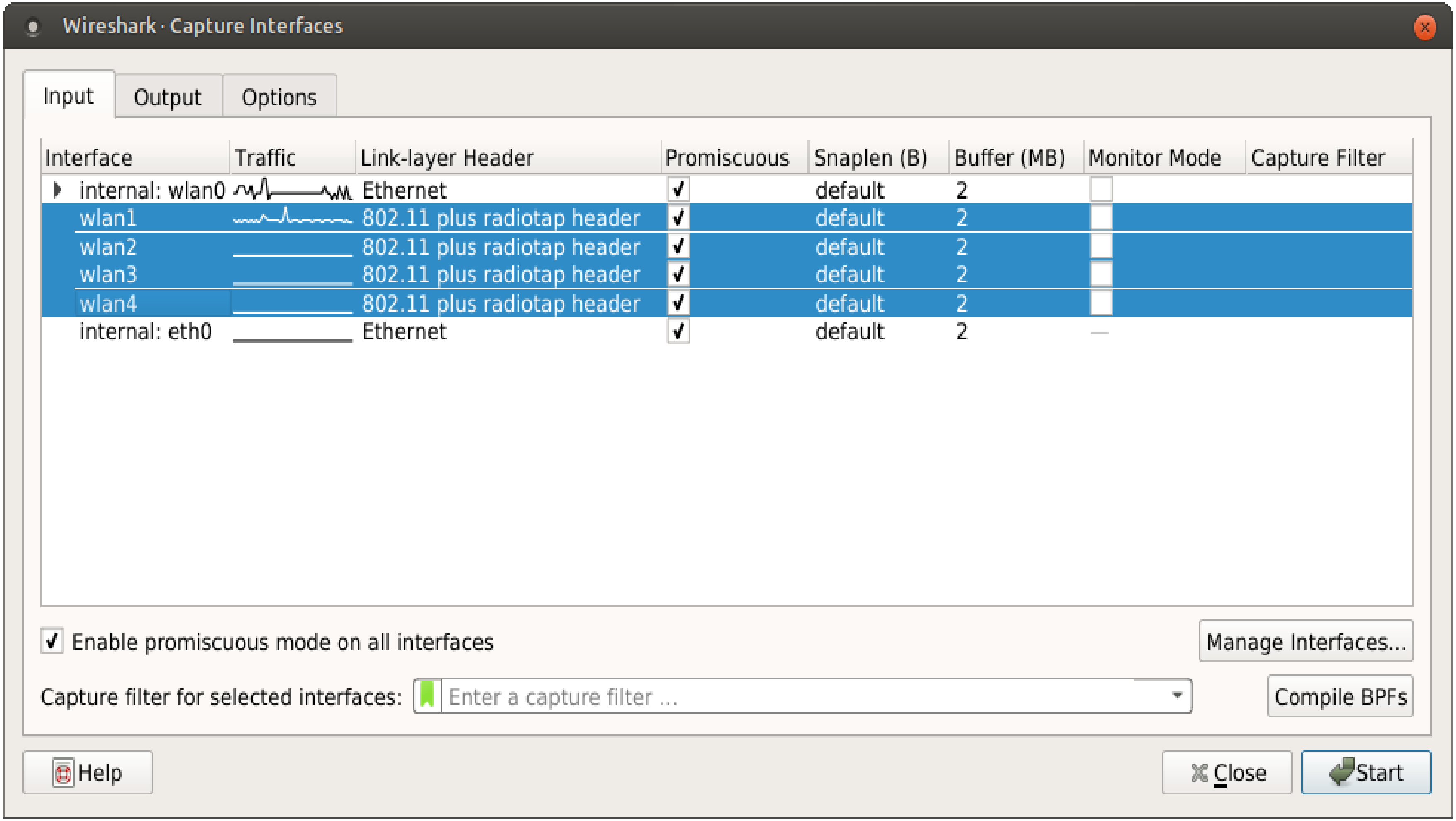


Channel	Bandwith	Select
Channel 36 (5.1 GHz)	HT20 HT40+ HT40- HT80	☑
Channel 40 (5.2 GHz)	HT20	☑

- Long Term stores packets directly to files, without starting Wireshark
- Creates an individual pcapng file per WLAN adapter
- Creates a new file per adapter every 5 minutes
- Packet size (Snaplen) is set to 500 Bytes

Capturing 802.11 Packets with WaveXpert

- The WaveXpert adapters and configurations will be imported to Wireshark for capturing



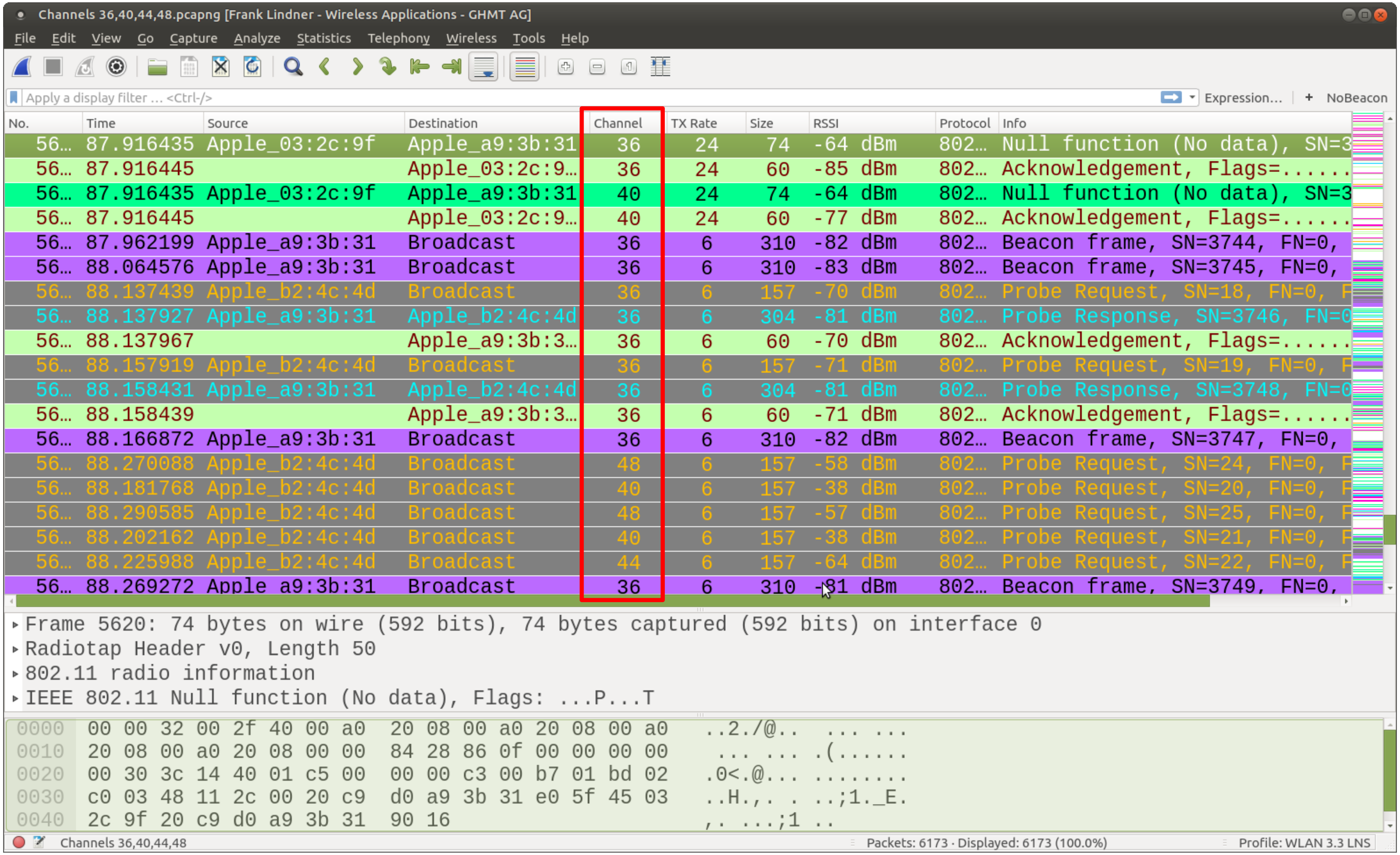
Wireshark · Capture Interfaces

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter
internal: wlan0		Ethernet	☑	default	2	□	
wlan1		802.11 plus radiotap header	☑	default	2	□	
wlan2		802.11 plus radiotap header	☑	default	2	□	
wlan3		802.11 plus radiotap header	☑	default	2	□	
wlan4		802.11 plus radiotap header	☑	default	2	□	
internal: eth0		Ethernet	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter …

Capturing 802.11 Packets with WaveXpert



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

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

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 all over Europe