Discover WLAN with Wireshark, AirPcap and WiSpy

Rolf Leutert, Leutert NetServices

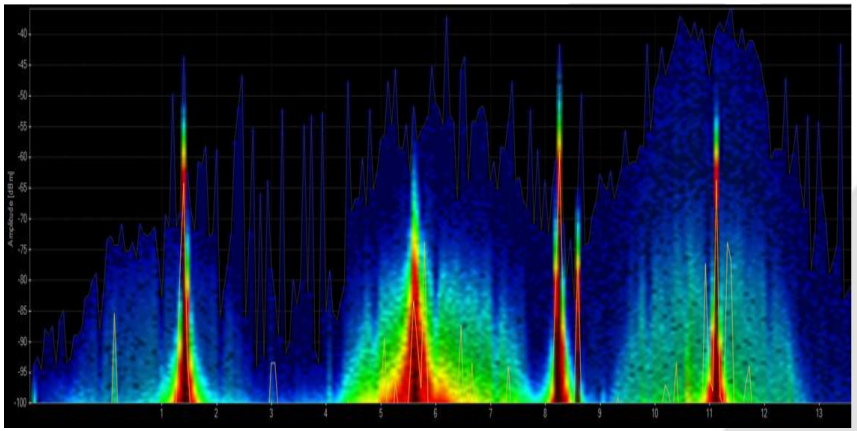
Discover WLAN with Wireshark, AirPcap and WiSpy

Session objectives:

- Learn what you can see on layer 1 and layer 2.
- Learn which tools can help you finding WLAN problems.
- Learn how Management- and Control frames assists you in root cause analysis.
- Learn how to customize Wireshark to show you specific WLAN information.

Discover WLAN with Wireshark, AirPcap and Wi-Spy

Troubleshooting WLANs comprises Layer 1 and Layer 2



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 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)

Layer 2 - Data Link Control

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

Client: 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

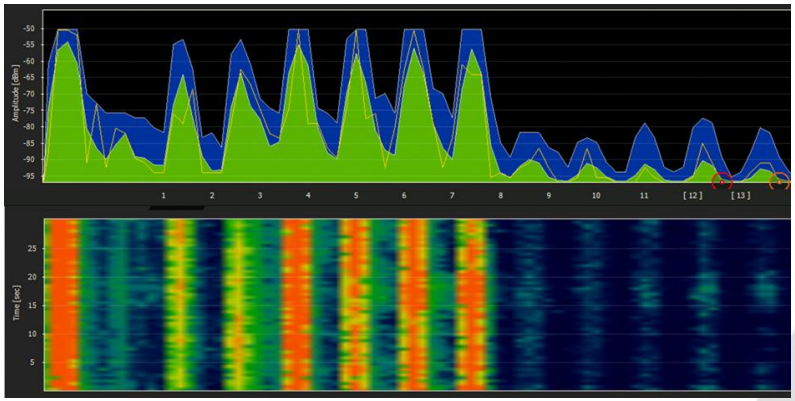
Wi-Spy® DBx spectrum scanner and Chanalizer® software displays and records all layer 1 signals in both 2.4 GHz and 5 GHz bands.

www.metageek.com

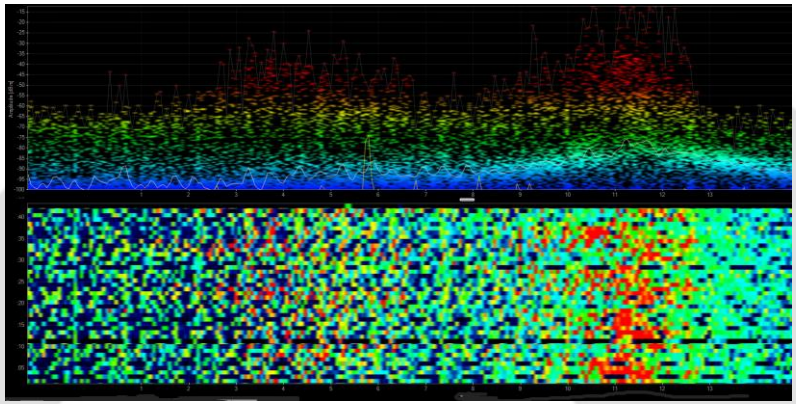
* ISM Industrial, Scientific and Medical
**UNII Unlicensed National Information Infrastructure

WLAN Layer 1 Analysis

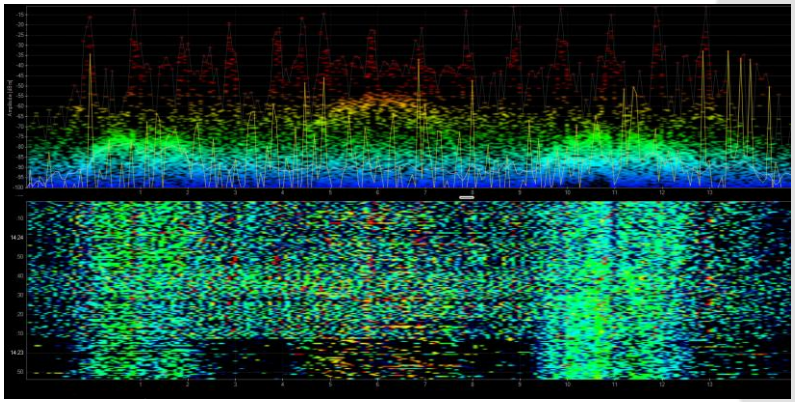
Non-WiFi Devices' Signatures



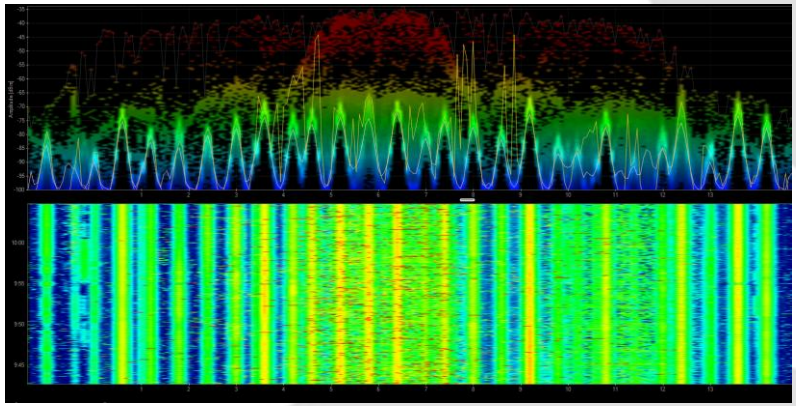
Home trainers in a fitness center



Microwave oven

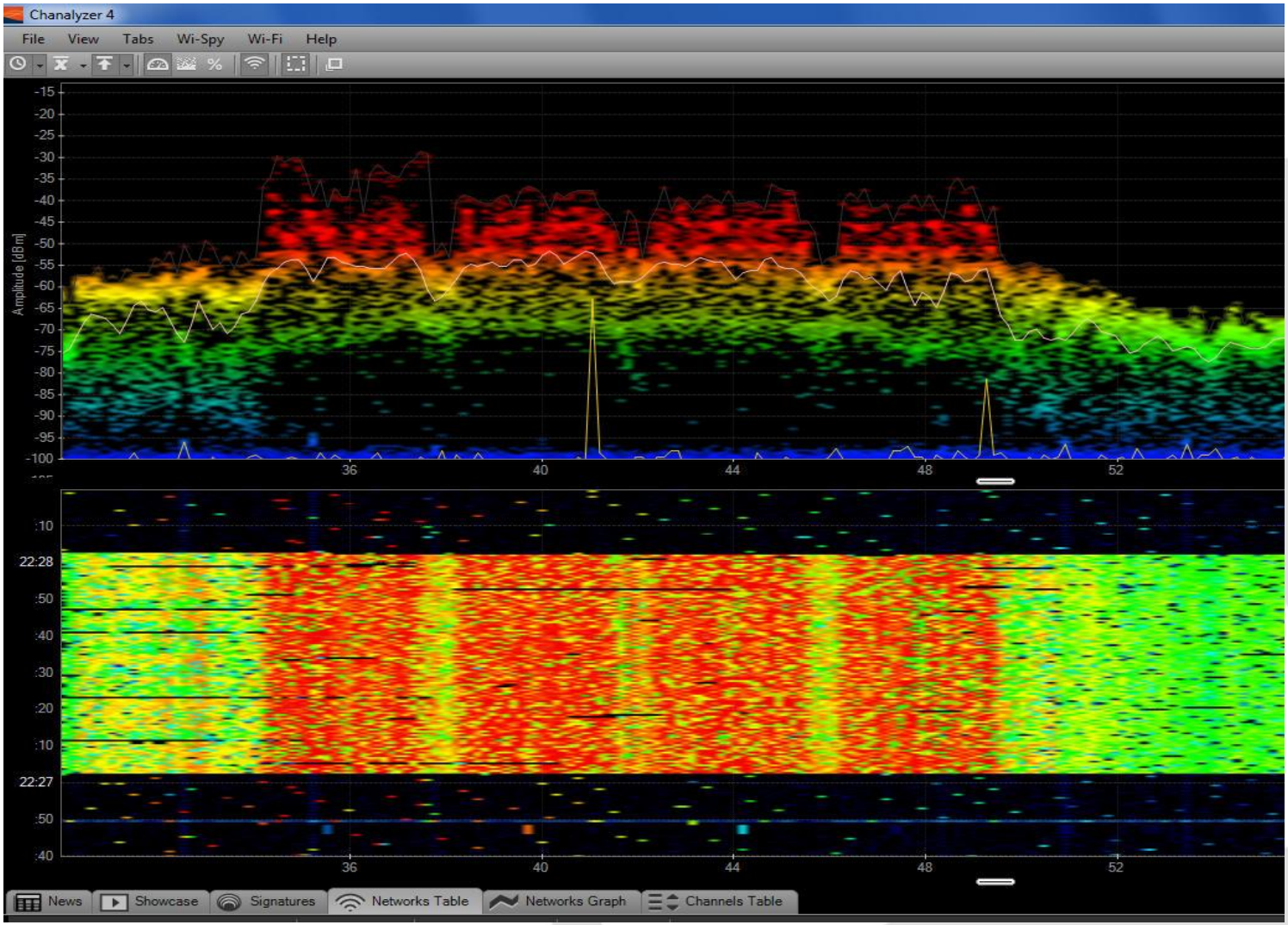


Remote control of model airplanes



Wireless guitar

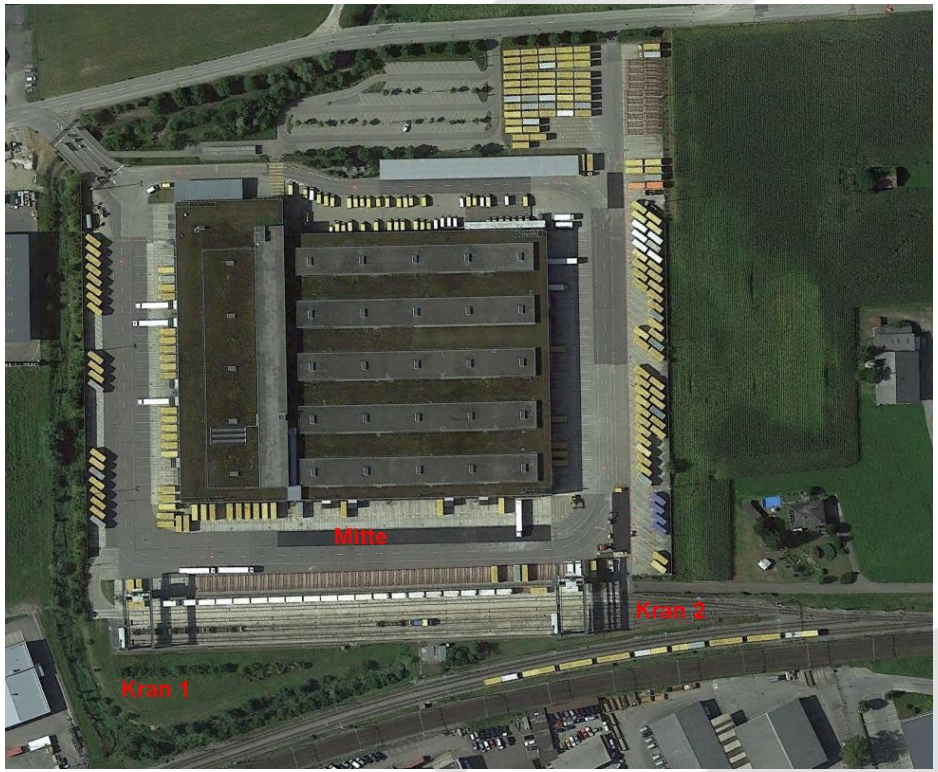
WLAN Layer 1 Analysis



WiFi 802.11ac with four bonded channels

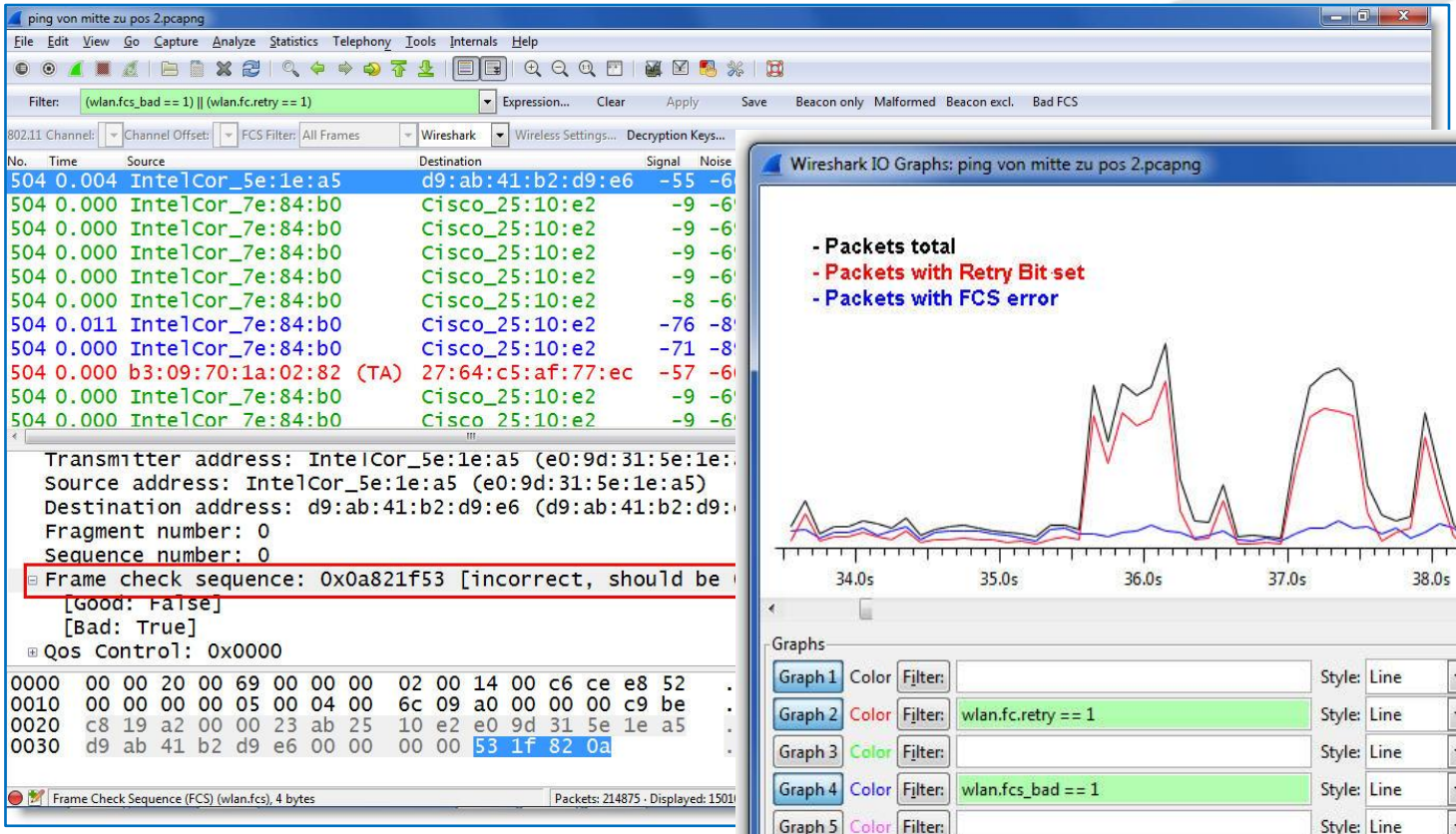
WLAN Layer 1 Analysis (Case one)

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



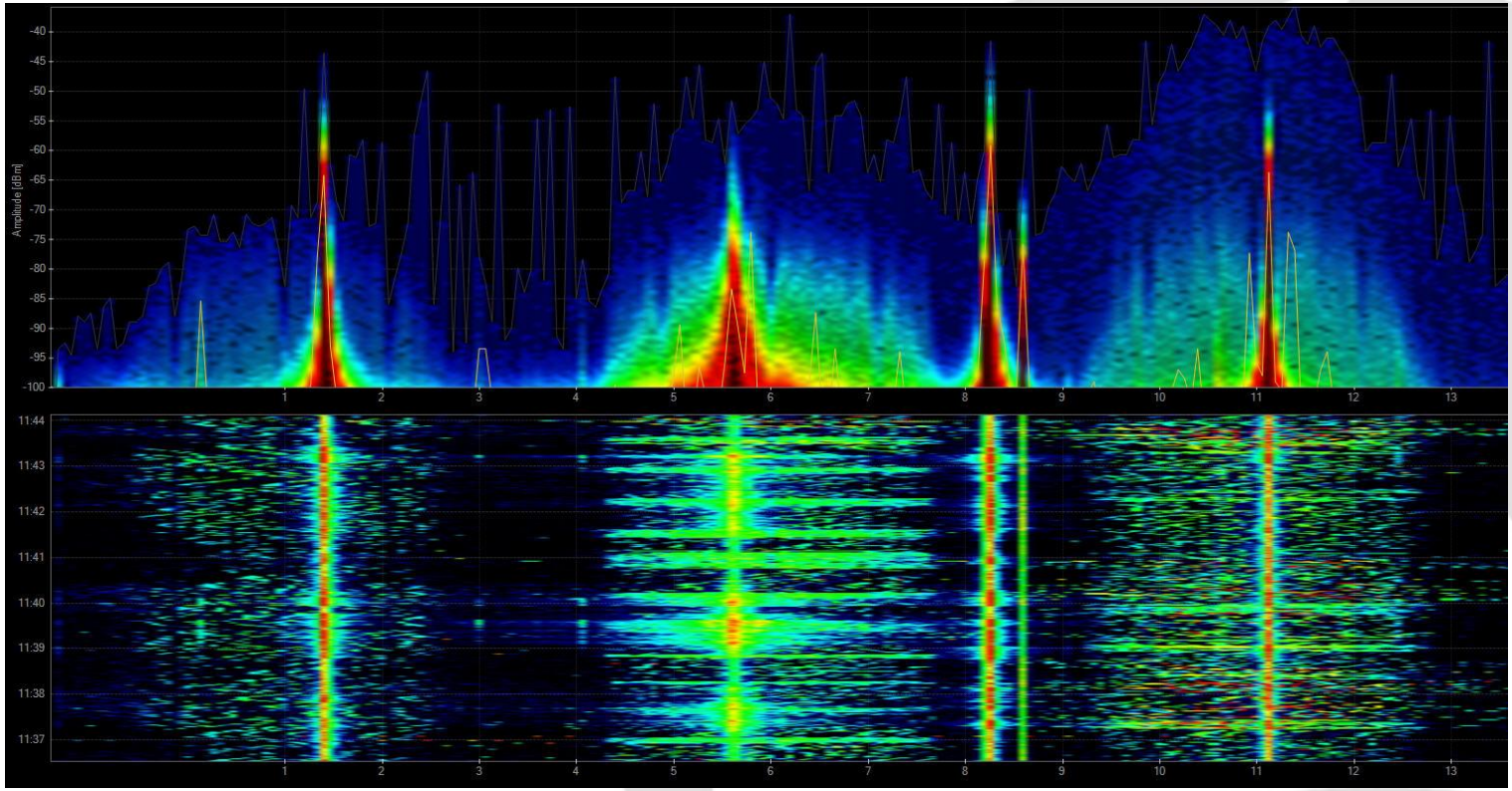
WLAN Layer 1 Analysis (Case one)

- 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



WLAN Layer 1 Analysis (Case one)

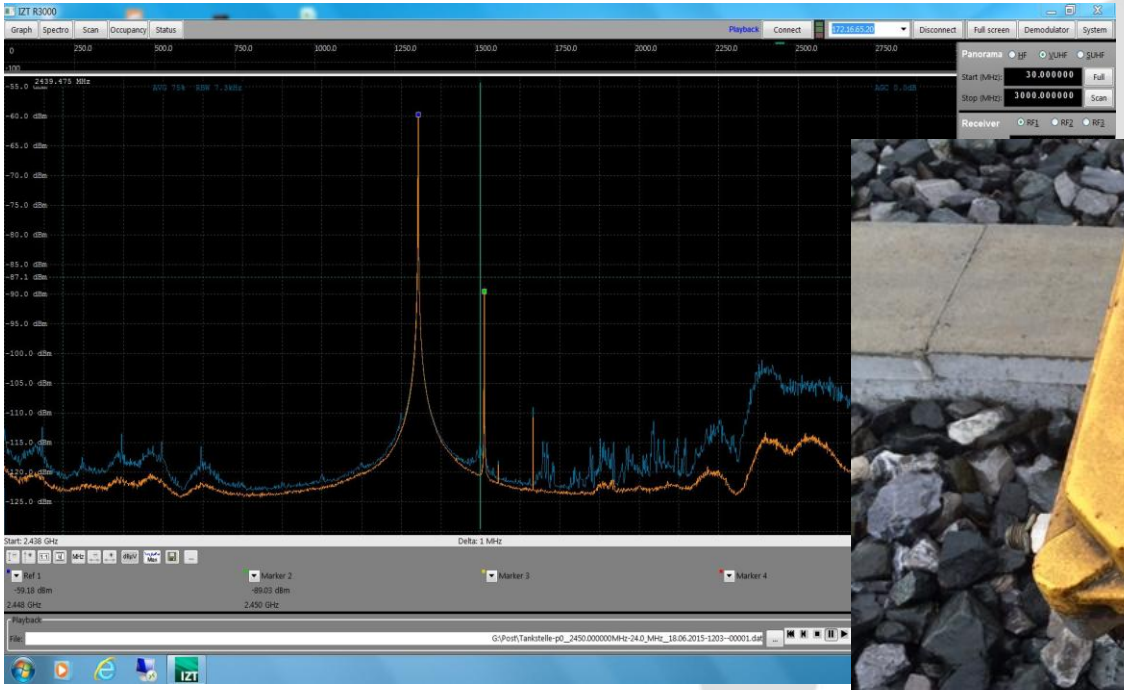
- Continuing with layer 1 analysis near crane #2 in 2.4 GHz band
- Strong interference with non-WiFi signals on all three channels detected



- 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

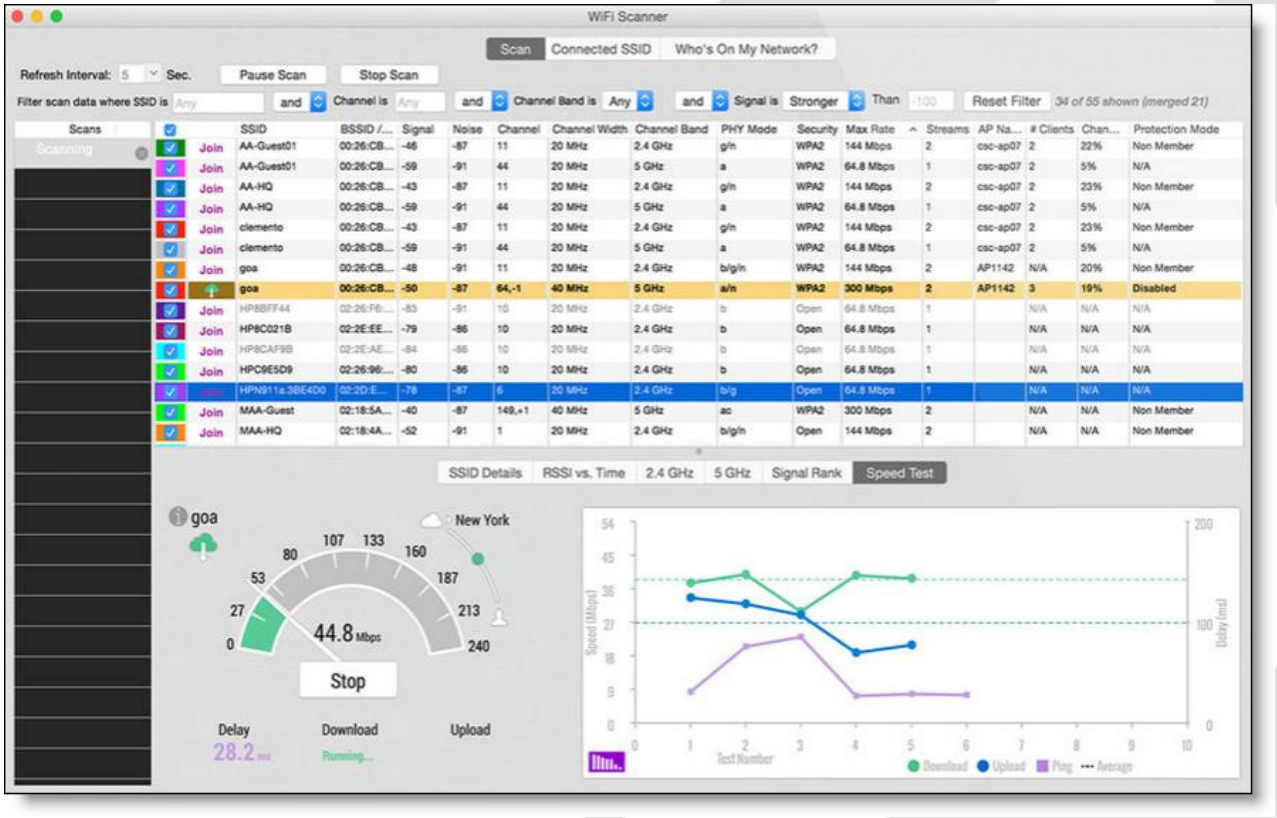


BAKOM scan result

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



WiFi Scanners (just a few popular ones)

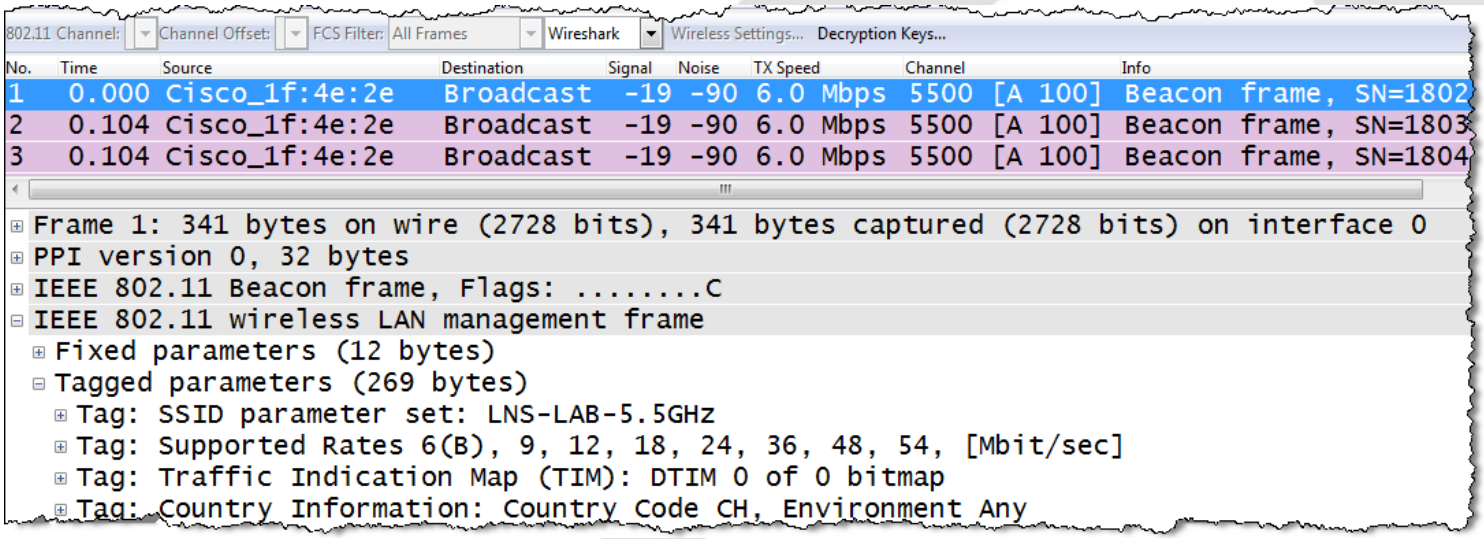
ACRYLIC WiFi	Acrylic WiFi scanner	www.acrylicwifi.com
ekahau	Ekahau HeatMapper	www.ekahau.com
	inSSIDer	www.metageek.com
	NetStumbler	www.netstumbler.com
	Wifi Analyzer (Android)	play.google.com
	WifiInfoView	www.nirsoft.net
WifiScanner	WifiScanner	wifiscanner.sourceforge.net
	Wifi Scanner	www.apple.com/osx/apps/app-store

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



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

WLAN Layer 2 Analysis

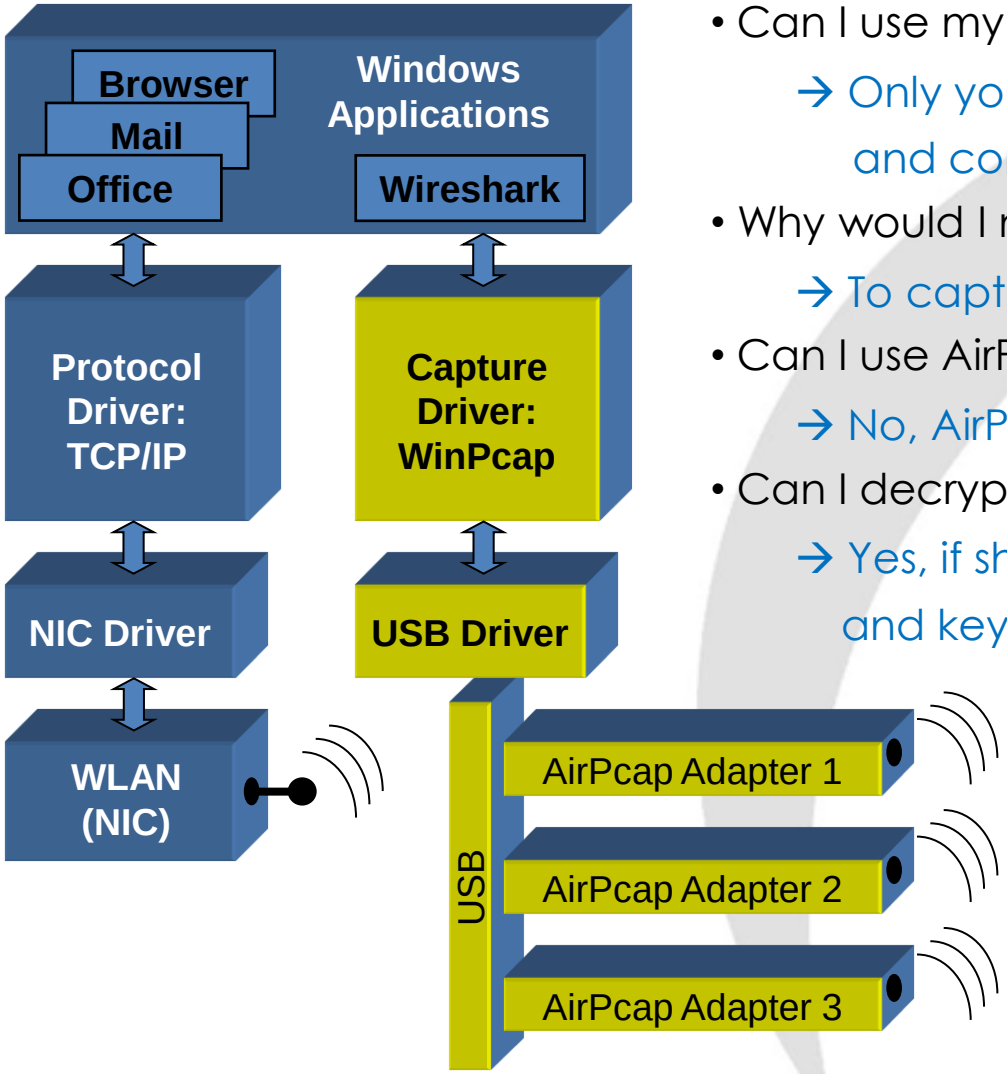
Key features:

- 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

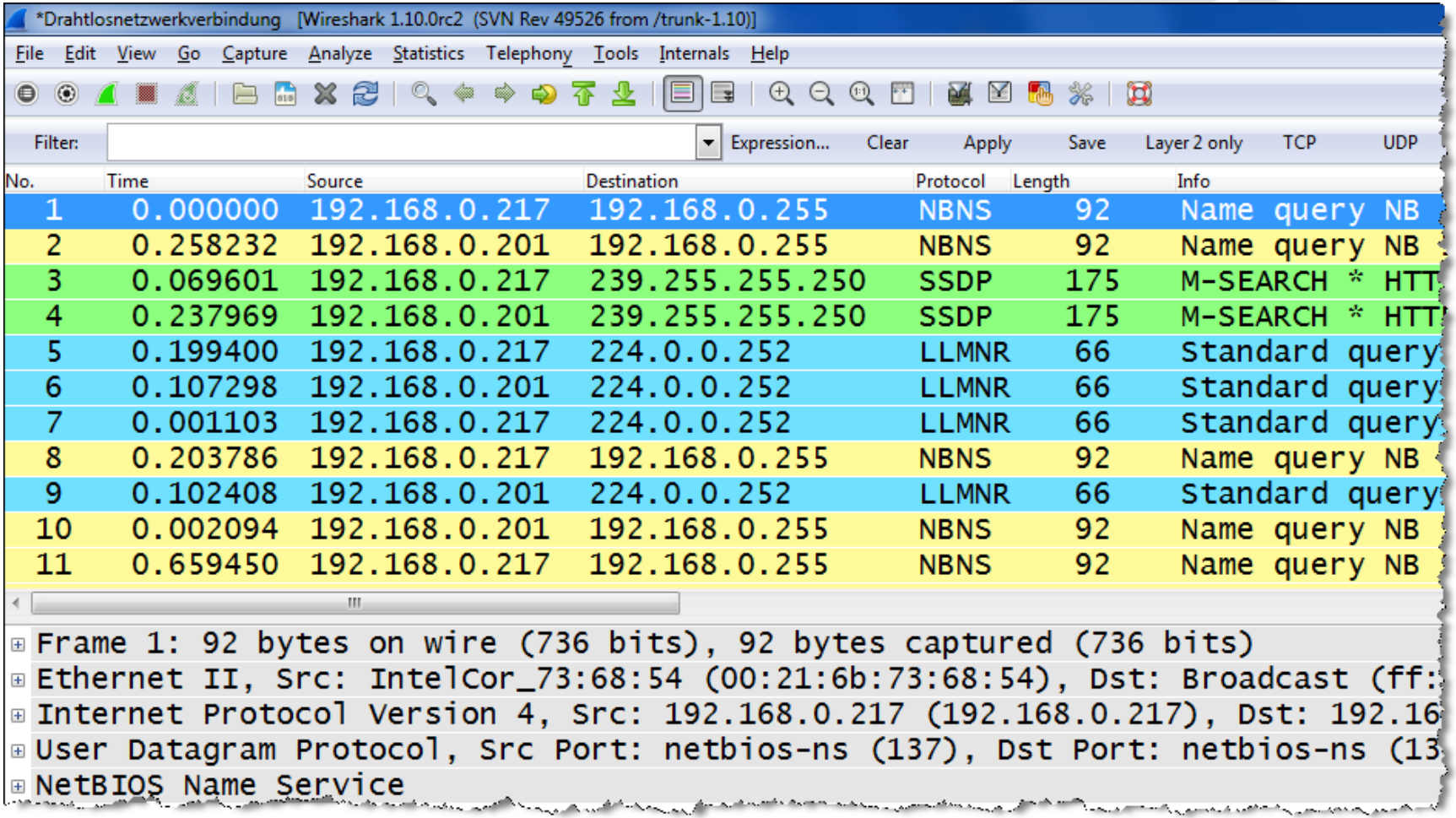


Frequently Asked Questions:

- 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

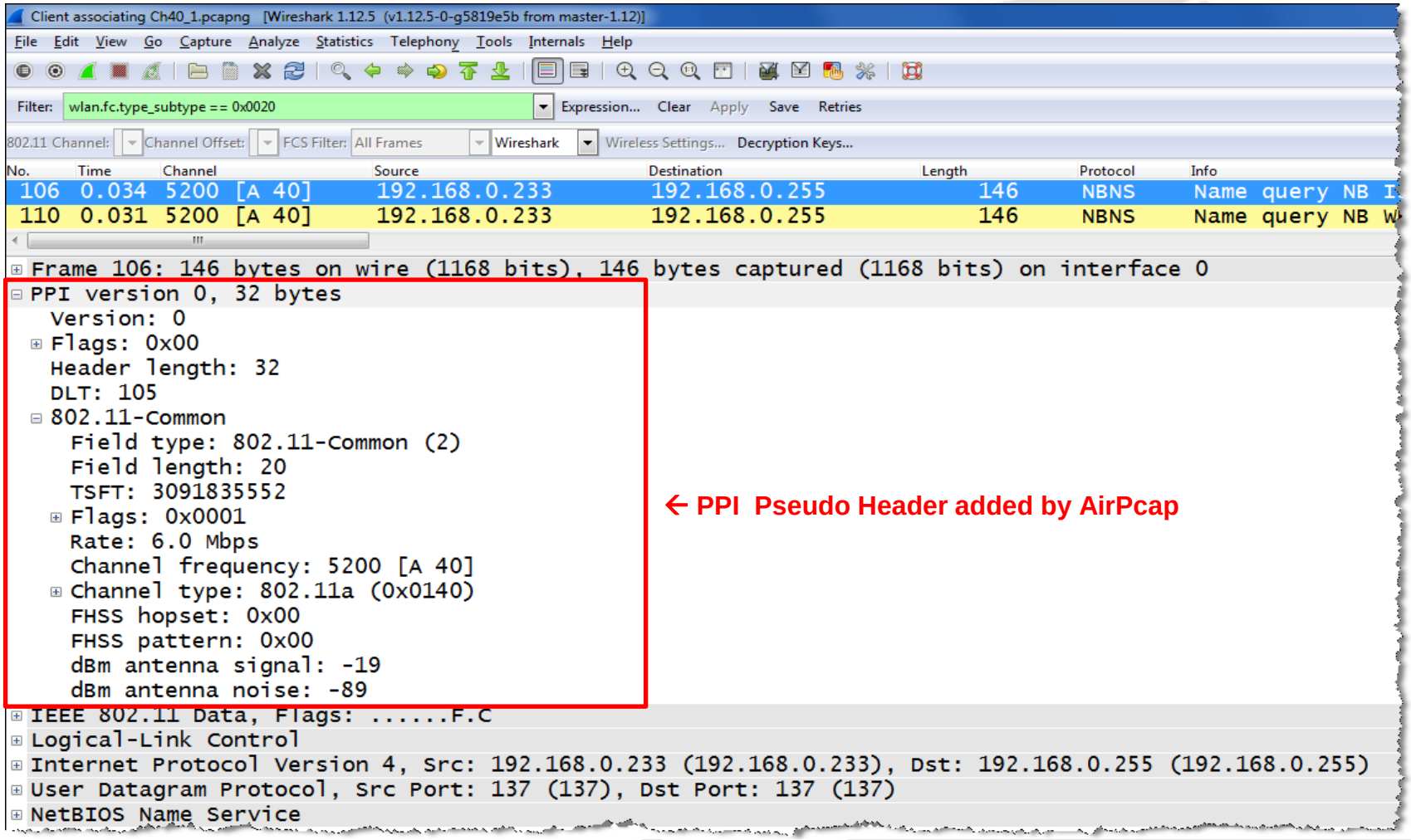
WLAN Layer 2 Analysis

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



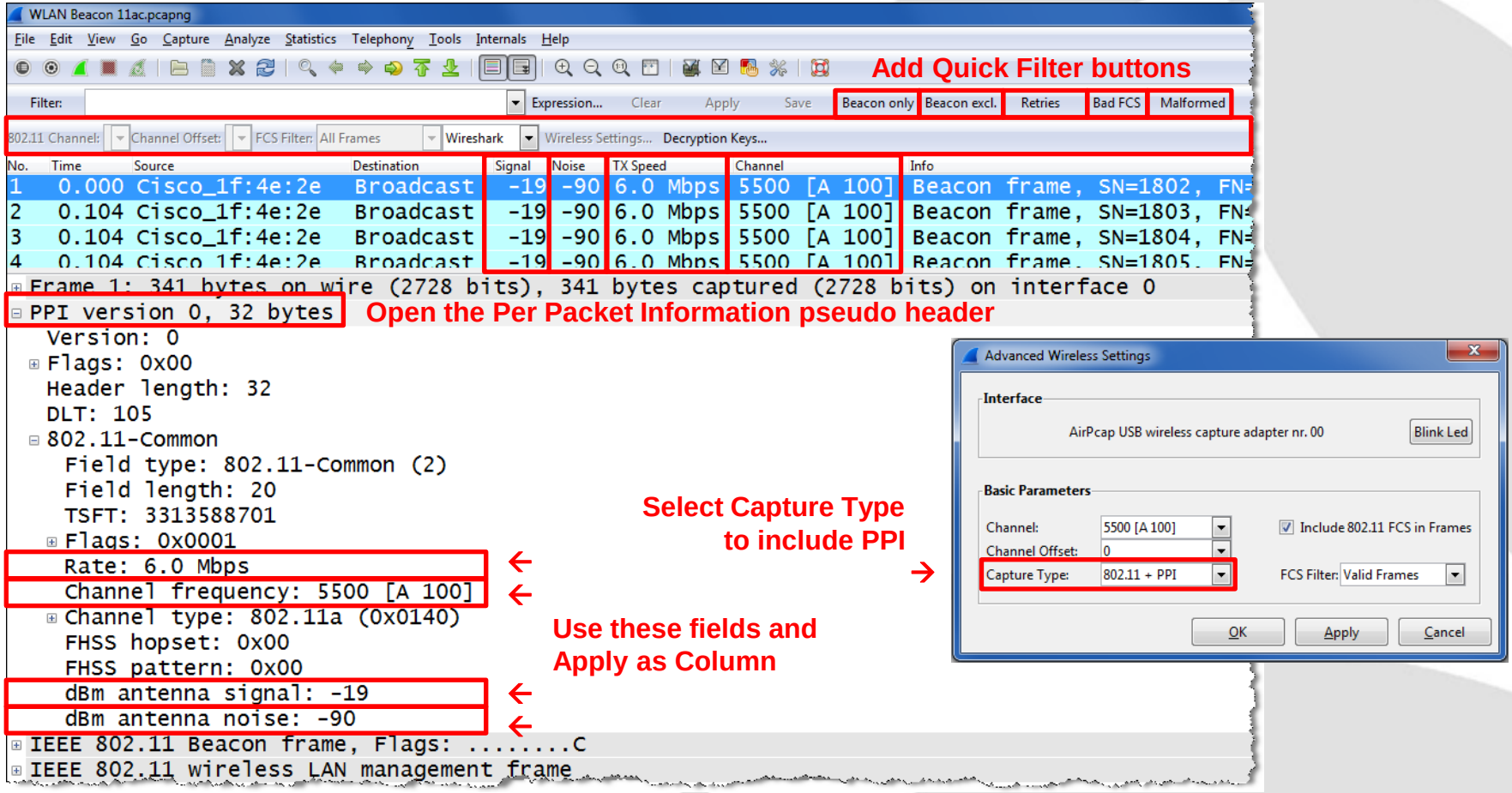
WLAN Layer 2 Analysis

- AirPcap is adding a Radio Tap or PPI (Per Packet Information) pseudo header
- The Pseudo-Header contains helpful infos like channel no, signal strength etc.



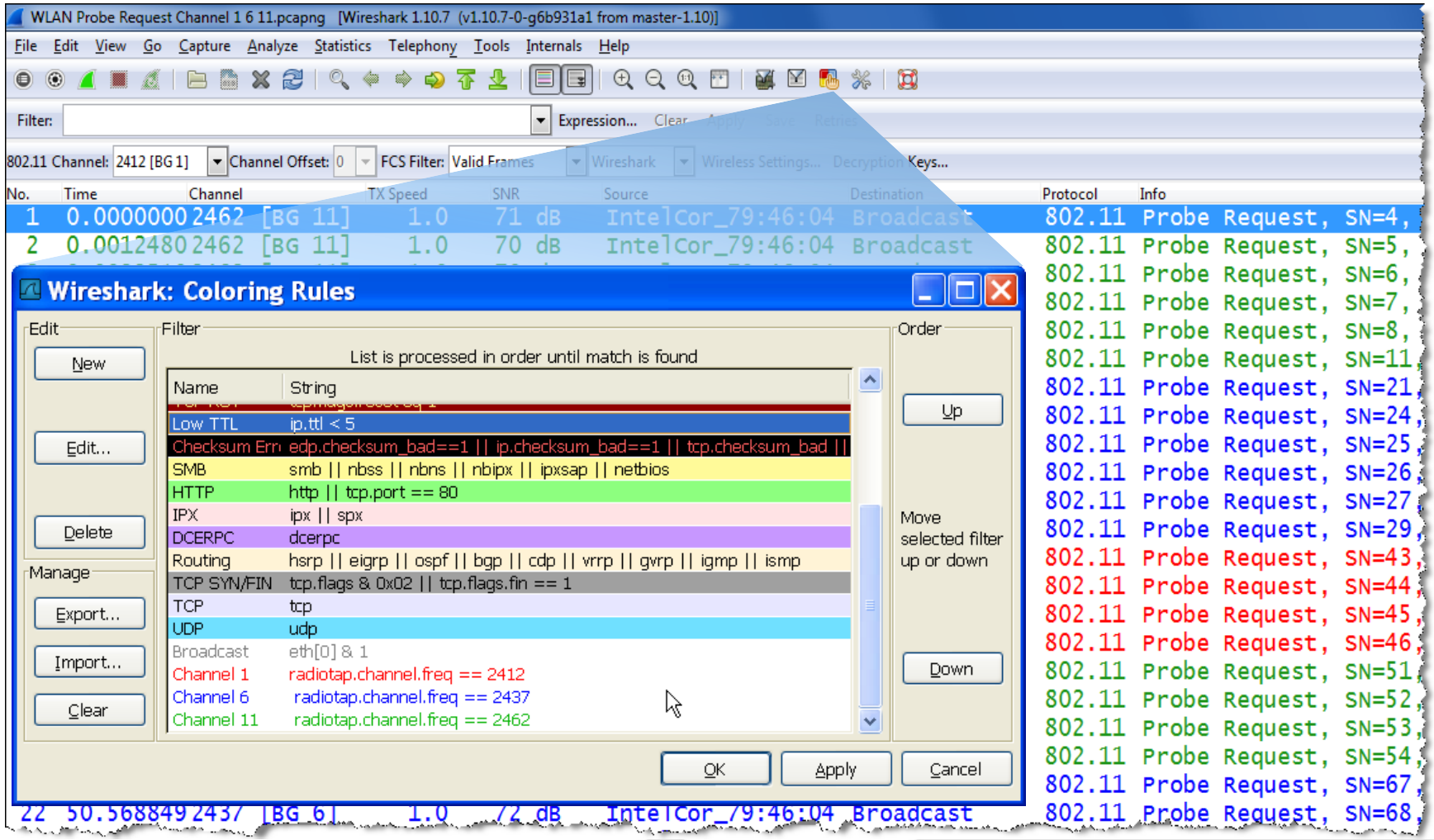
Customize Wireshark for WLAN Analysis

- Create a new profile and customize your Wireshark before analyzing WLANs
- Turn on Wireless Toolbar and add columns with useful layer 1 information
- Configure AirPcap to add a Pseudo Header (PPI) to each frame at reception



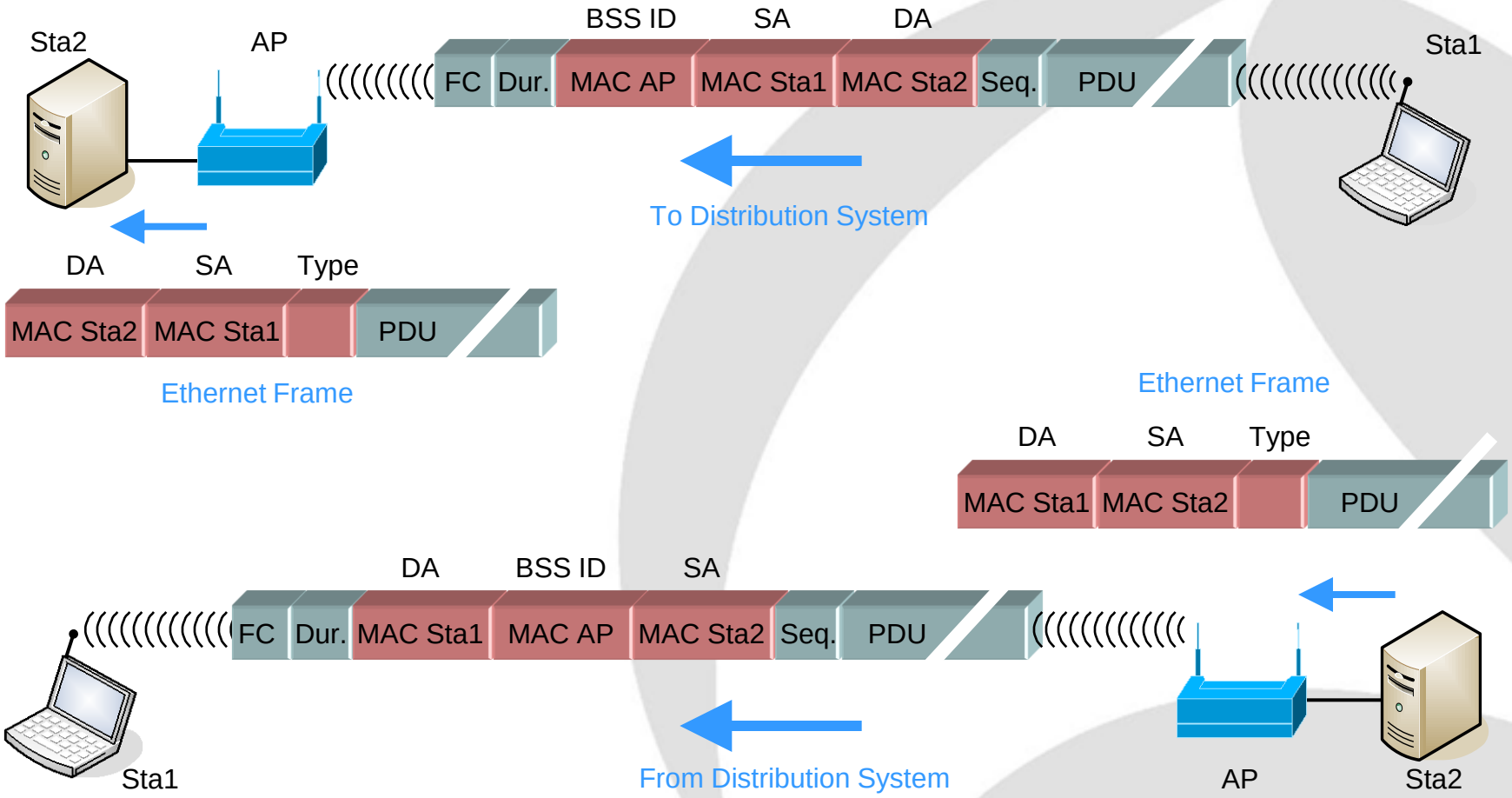
Customize Wireshark for WLAN Analysis

- Adding a coloring rule per channel enhances readability



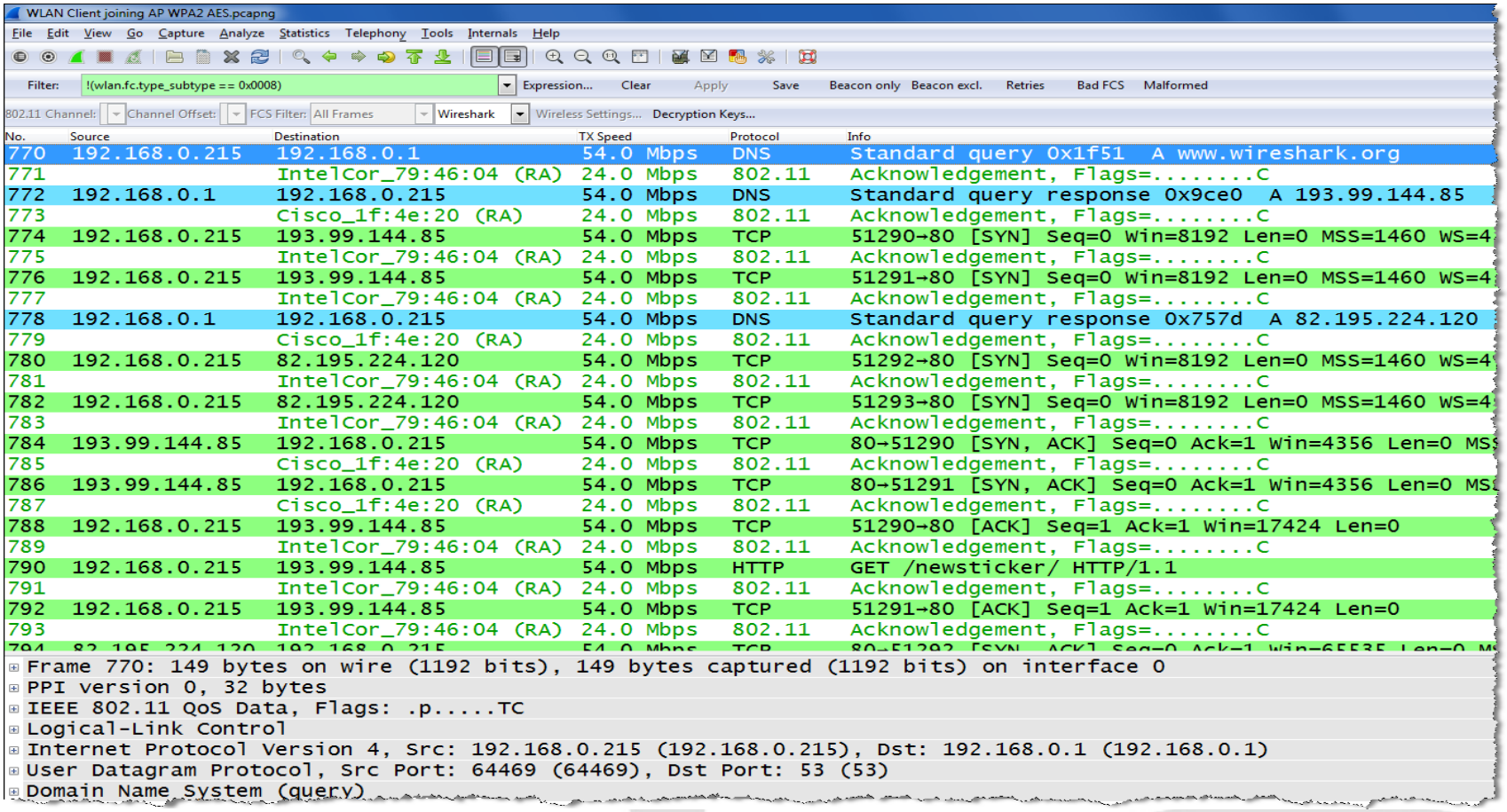
WLAN Layer 2 Analysis

- 802.11 frames look different from Ethernet frames
- WLAN frames have from one to four MAC addresses



WLAN Layer 2 Analysis

Data Transmission (single packets)

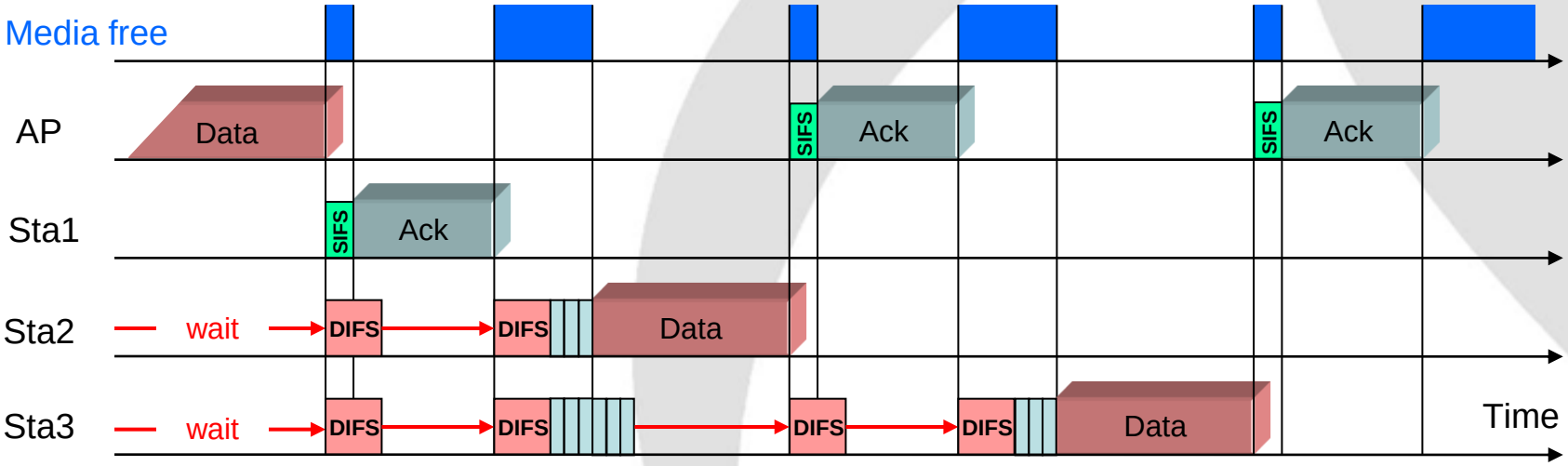


- Acks must follow immediately after a Data frame and have no source address.

WLAN Layer 2 Analysis

- Access method Carrier Sense, Multiple Access w. Collision Avoidance CSMA/CA
- Different time spaces control the access to the shared media

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)



- If media is free, each station waits DIFS and a random number of Slot Times

WLAN Layer 2 Analysis

Frame Types Overview

Management Frames:

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

Control Frames:

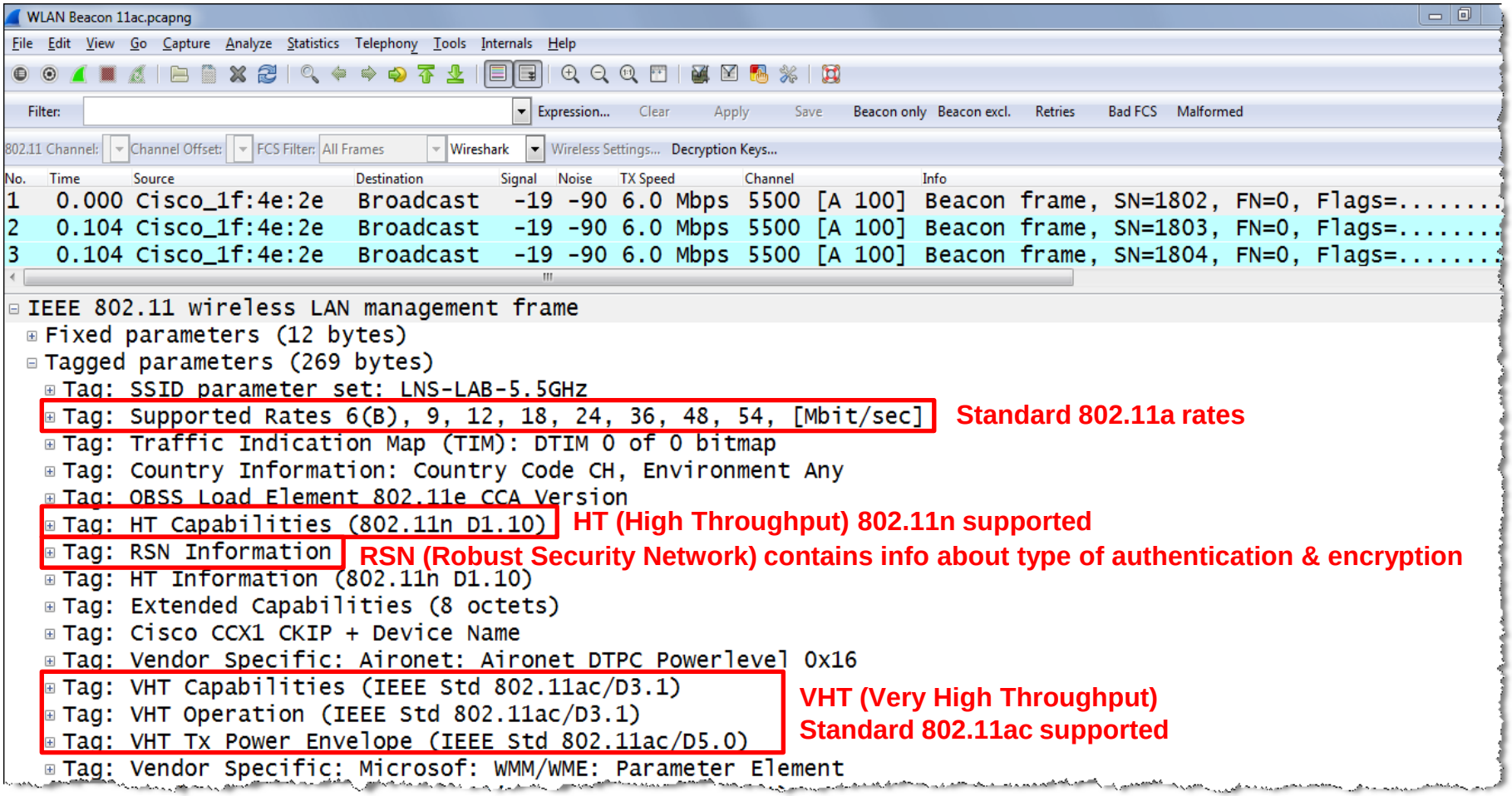
- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledge / Block Acknowledge Request / Block Acknowledge
- Power Save Poll

Data Frames:

- Data
- Null Function

WLAN Layer 2 Analysis

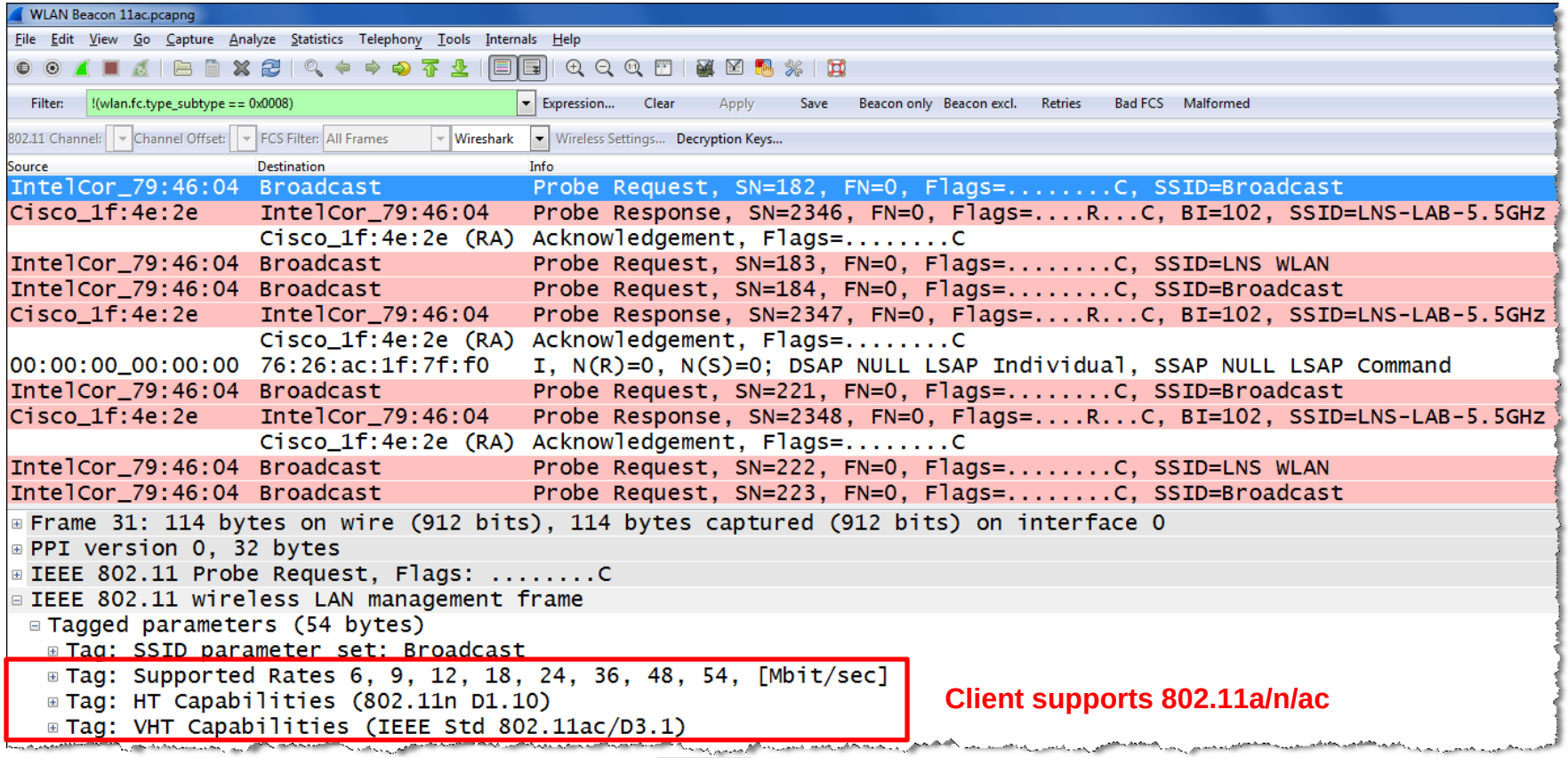
Beacon Tags



- Beacons tags contain information about supported and required features

WLAN Layer 2 Analysis

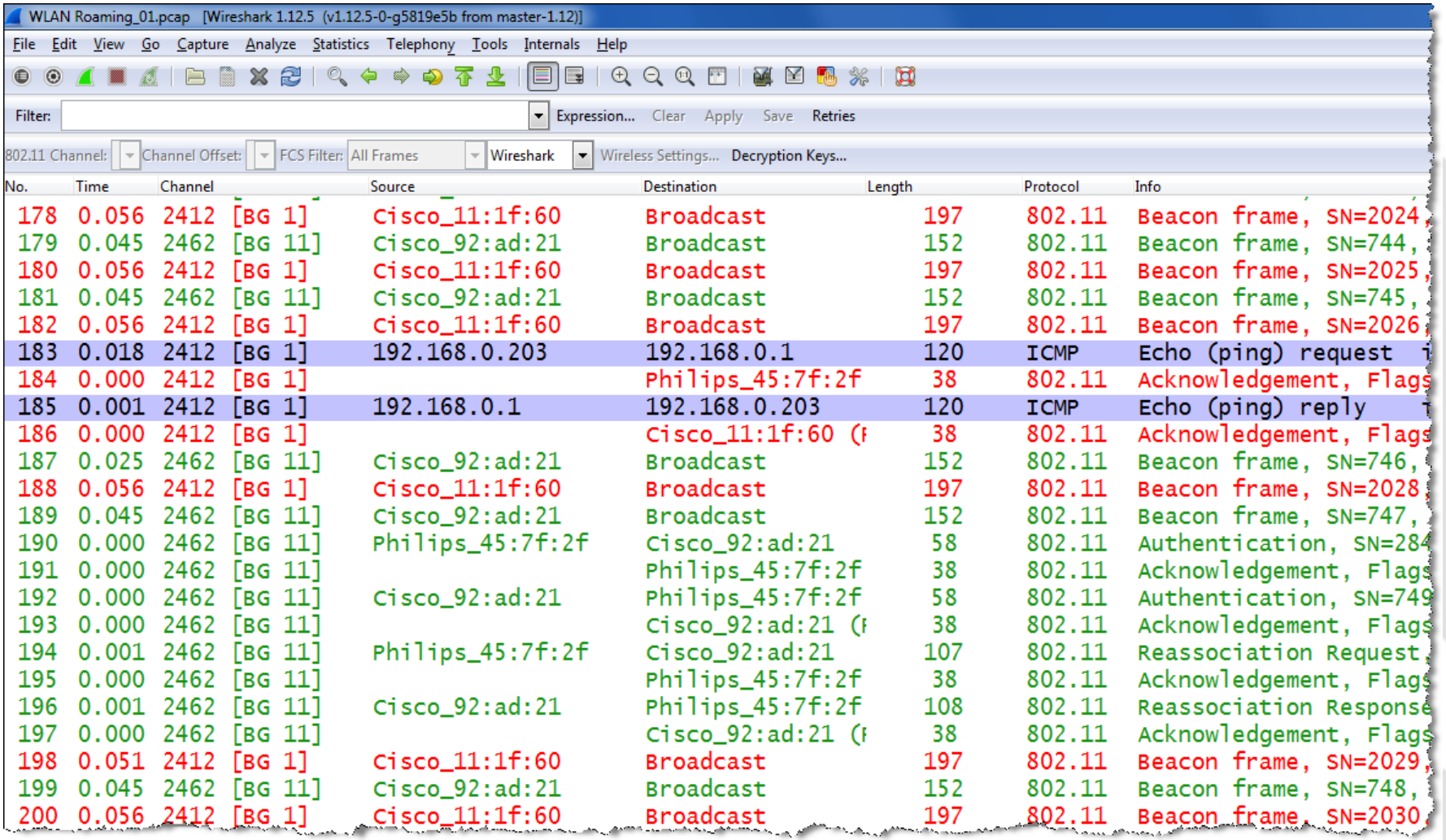
Probe Request / Probe Response



- Clients scans for Access Points through all channels using Probe Request
- Probe Request contains client features and specific or broadcast SSID
- Access Points reply with Probe Response, containing same fields as Beacon

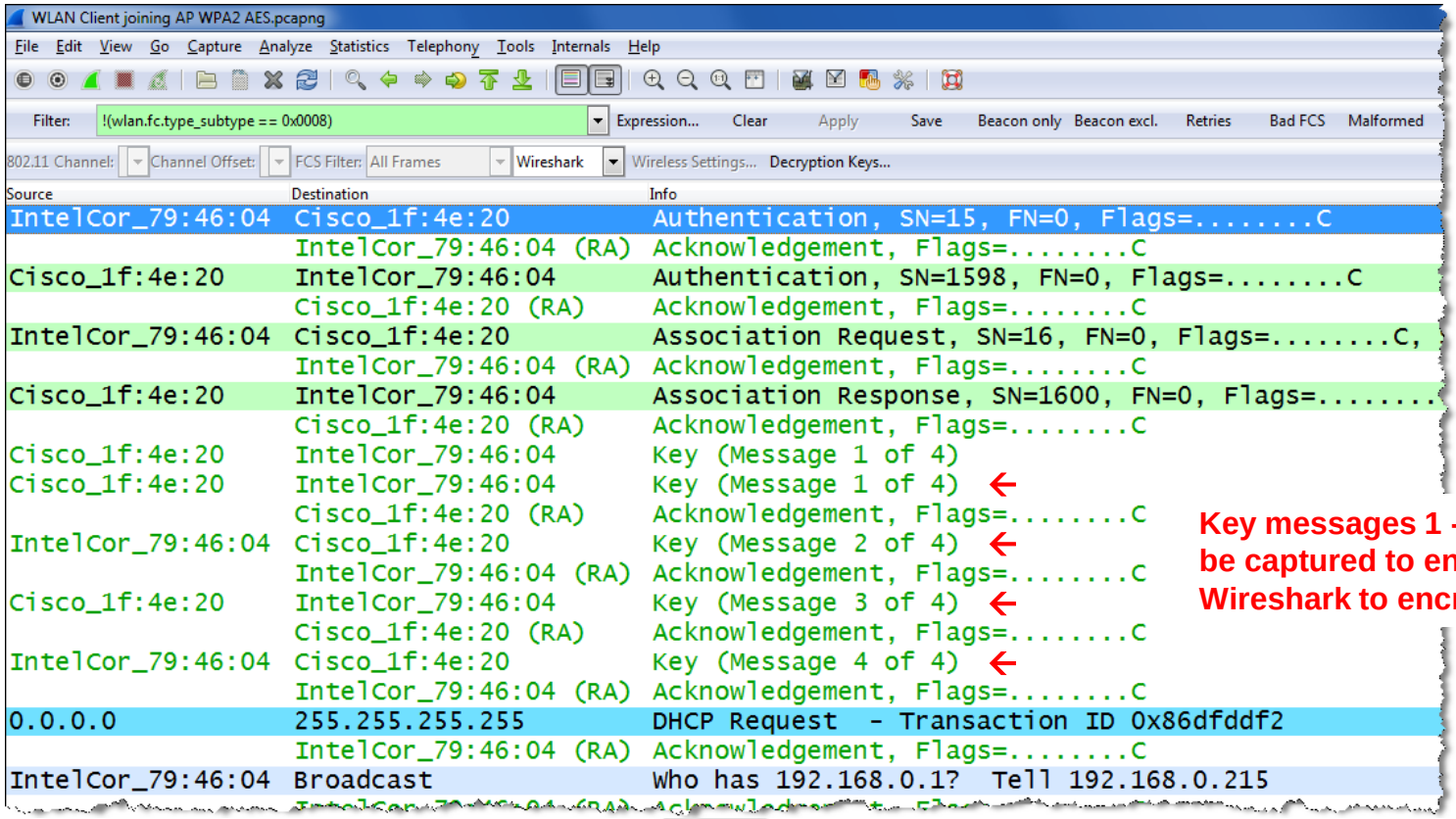
WLAN Layer 2 Analysis

- Following a roaming client with two AirPcap adapters



WLAN Layer 2 Analysis

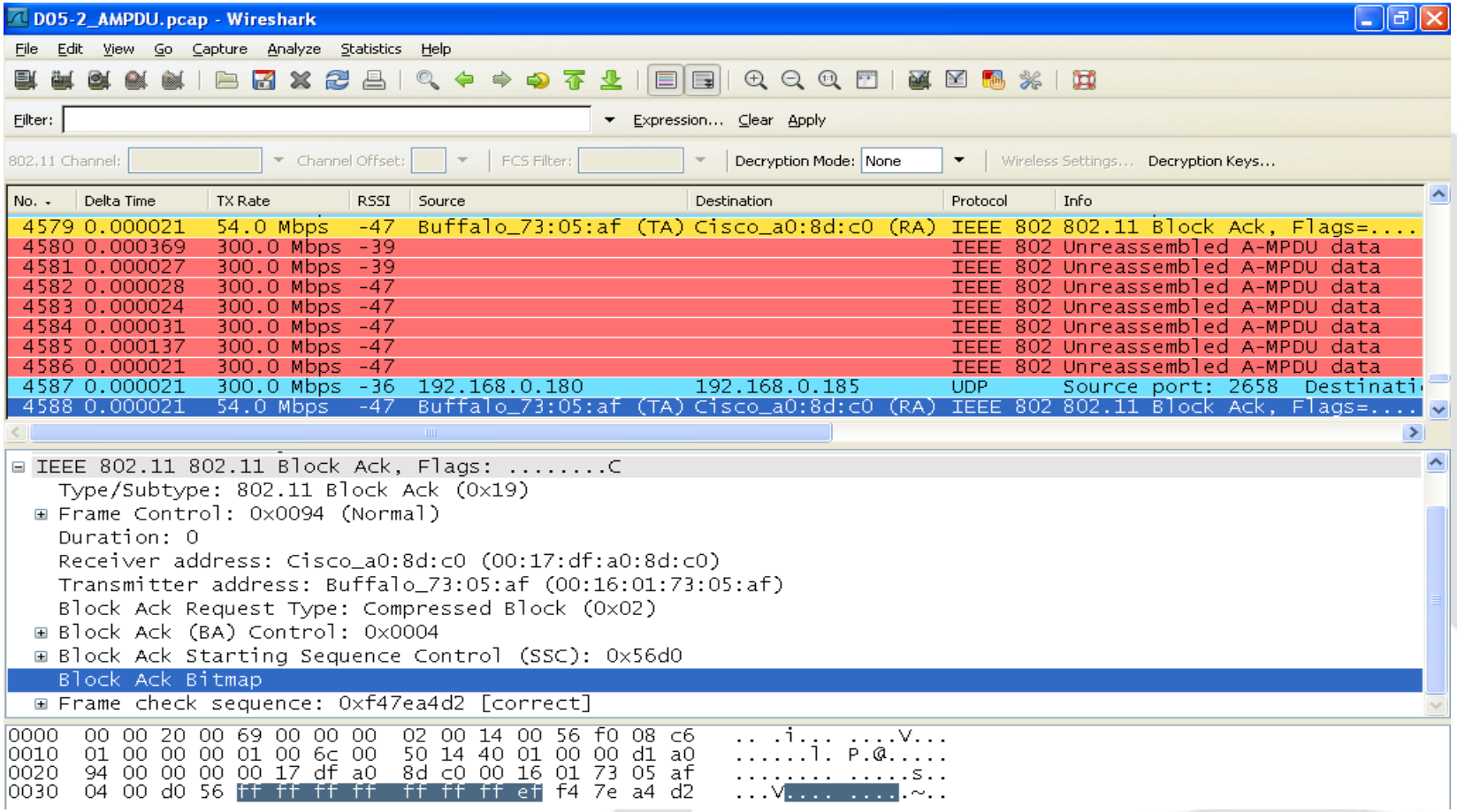
Association Request / Association Response



- Authentication is old WEP legacy stuff; still there, but has no function.
- Clients associates with Access Point and negotiates WPA session key.
- All frames are acknowledged or retransmitted by the sender.

WLAN Layer 2 Analysis

Data Transmission (multiple packets in aggregation mode)

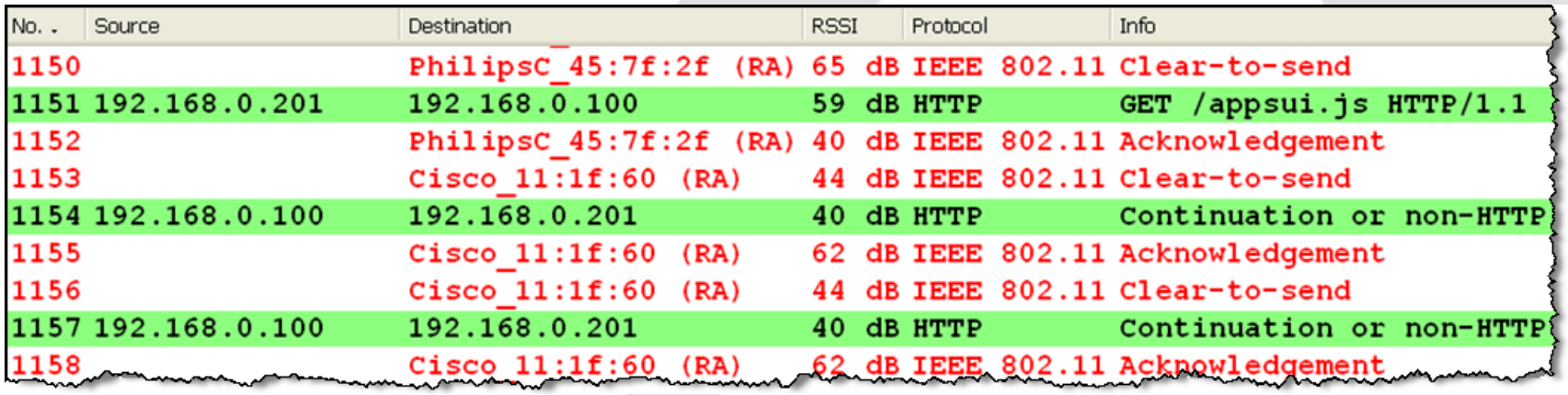


- 802.11n/ac supports up to 64 packet in a burst with a single Block Acknowledge.
- Block Ack contains Bitmap to ack only good packets, other will be sent again.

WLAN Layer 2 Analysis

Interoperability between WLAN generations

- Interoperability between 802.11b/g/n and 802.11a/n/ac is granted.
- Mixed operations come at a cost: lower throughput.
- Indicated throughput values are valid for non-mixed environment and small cells.
- Clients at the border of cells transmit at low speed and use longer airtime.
- Shrink your cell size and gain bandwidth by disabling lower rates in Access Points.
- Try to get rid of old clients (especially B-only) before upgrading your APs.



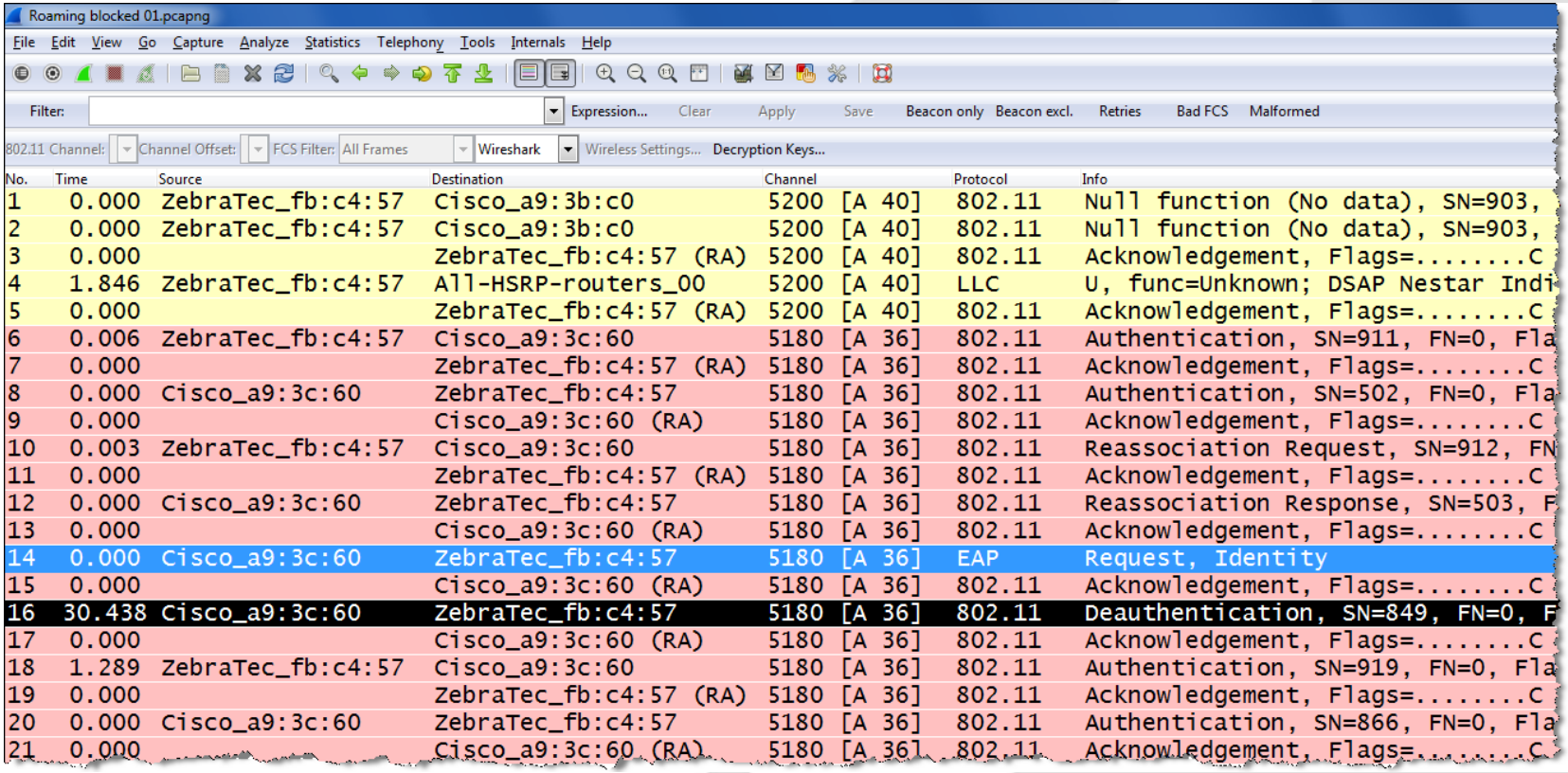
No.	Source	Destination	RSSI	Protocol	Info
1150		PhilipsC_45:7f:2f (RA)	65 dB	IEEE 802.11	Clear-to-send
1151	192.168.0.201	192.168.0.100	59 dB	HTTP	GET /appsui.js HTTP/1.1
1152		PhilipsC_45:7f:2f (RA)	40 dB	IEEE 802.11	Acknowledgement
1153		Cisco_11:1f:60 (RA)	44 dB	IEEE 802.11	Clear-to-send
1154	192.168.0.100	192.168.0.201	40 dB	HTTP	Continuation or non-HTTP
1155		Cisco_11:1f:60 (RA)	62 dB	IEEE 802.11	Acknowledgement
1156		Cisco_11:1f:60 (RA)	44 dB	IEEE 802.11	Clear-to-send
1157	192.168.0.100	192.168.0.201	40 dB	HTTP	Continuation or non-HTTP
1158		Cisco_11:1f:60 (RA)	62 dB	IEEE 802.11	Acknowledgement

- Old clients must be silenced with Request-to-Send / Clear-to-send (RTS/CTS) or Clear-to-Send-Self (CTS-Self) frames sent before each data frame.
- This process will significantly reduce the total cell throughput.

WLAN Layer 2 Analysis (Case two)

Customer problem analyzed and solved with Wireshark and AirPcap

- User is complaining about sporadic hangers in bar code scanners, up to minutes
- Vendors of mobile clients and access points are finger pointing, since month.
- Problem could be assigned to bar code vendor by analyzing trace files.



No.	Time	Source	Destination	Channel	Protocol	Info
1	0.000	ZebraTec_fb:c4:57	Cisco_a9:3b:c0	5200 [A 40]	802.11	Null function (No data), SN=903,
2	0.000	ZebraTec_fb:c4:57	Cisco_a9:3b:c0	5200 [A 40]	802.11	Null function (No data), SN=903,
3	0.000		ZebraTec_fb:c4:57 (RA)	5200 [A 40]	802.11	Acknowledgement, Flags=.....C
4	1.846	ZebraTec_fb:c4:57	All-HSRP-routers_00	5200 [A 40]	LLC	U, func=Unknown; DSAP Nestar Indi
5	0.000		ZebraTec_fb:c4:57 (RA)	5200 [A 40]	802.11	Acknowledgement, Flags=.....C
6	0.006	ZebraTec_fb:c4:57	Cisco_a9:3c:60	5180 [A 36]	802.11	Authentication, SN=911, FN=0, Fla
7	0.000		ZebraTec_fb:c4:57 (RA)	5180 [A 36]	802.11	Acknowledgement, Flags=.....C
8	0.000	Cisco_a9:3c:60	ZebraTec_fb:c4:57	5180 [A 36]	802.11	Authentication, SN=502, FN=0, Fla
9	0.000		Cisco_a9:3c:60 (RA)	5180 [A 36]	802.11	Acknowledgement, Flags=.....C
10	0.003	ZebraTec_fb:c4:57	Cisco_a9:3c:60	5180 [A 36]	802.11	Reassociation Request, SN=912, FN
11	0.000		ZebraTec_fb:c4:57 (RA)	5180 [A 36]	802.11	Acknowledgement, Flags=.....C
12	0.000	Cisco_a9:3c:60	ZebraTec_fb:c4:57	5180 [A 36]	802.11	Reassociation Response, SN=503, F
13	0.000		Cisco_a9:3c:60 (RA)	5180 [A 36]	802.11	Acknowledgement, Flags=.....C
14	0.000	Cisco_a9:3c:60	ZebraTec_fb:c4:57	5180 [A 36]	EAP	Request, Identity
15	0.000		Cisco_a9:3c:60 (RA)	5180 [A 36]	802.11	Acknowledgement, Flags=.....C
16	30.438	Cisco_a9:3c:60	ZebraTec_fb:c4:57	5180 [A 36]	802.11	Deauthentication, SN=849, FN=0, F
17	0.000		Cisco_a9:3c:60 (RA)	5180 [A 36]	802.11	Acknowledgement, Flags=.....C
18	1.289	ZebraTec_fb:c4:57	Cisco_a9:3c:60	5180 [A 36]	802.11	Authentication, SN=919, FN=0, Fla
19	0.000		ZebraTec_fb:c4:57 (RA)	5180 [A 36]	802.11	Acknowledgement, Flags=.....C
20	0.000	Cisco_a9:3c:60	ZebraTec_fb:c4:57	5180 [A 36]	802.11	Authentication, SN=866, FN=0, Fla
21	0.000		Cisco_a9:3c:60 (RA)	5180 [A 36]	802.11	Acknowledgement, Flags=.....C

WLAN technology coming soon…

802.11n

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
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

* AirPcap Nx supports 802.11n with up to two Spatial Streams (2x2:2) in Legacy, HT20 or HT40 mode (no SGI & Greenfield mode)

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

WLAN technology coming soon…

Unofficially announced: A new AirPcap adapter from riverbed

Supporting Short Guard Interval (SGI), 3x3 MIMO, AC and more…
Planned availability: early 2016

Product Requirements	Atheros AR9342 with Qualcomm/Atheros QCA9880
3x3 MIMO	X
USB 3.0 (5Gbps or 640MB/s)	USB 2.0 (480Mbps or 60MB/s)
802.11ac (Theoretical max. 6,933Mbps or 900MB/s - Up to 8x 866.7Mbps channels)	X
802.11abgn (802.11n max. 600MB/s)	X
Win8	
External Antenna	3
USB stick form factor	External USB Enclosure
Short Guard Interval	X
Channel Support	2.412-2.472Ghz, 5.180-5.825Ghz, TBD

Source: Riverbed Technology (specs. without commitment)

Thank you for your attention

Rolf Leutert, Leutert NetServices, www.wireshark.ch