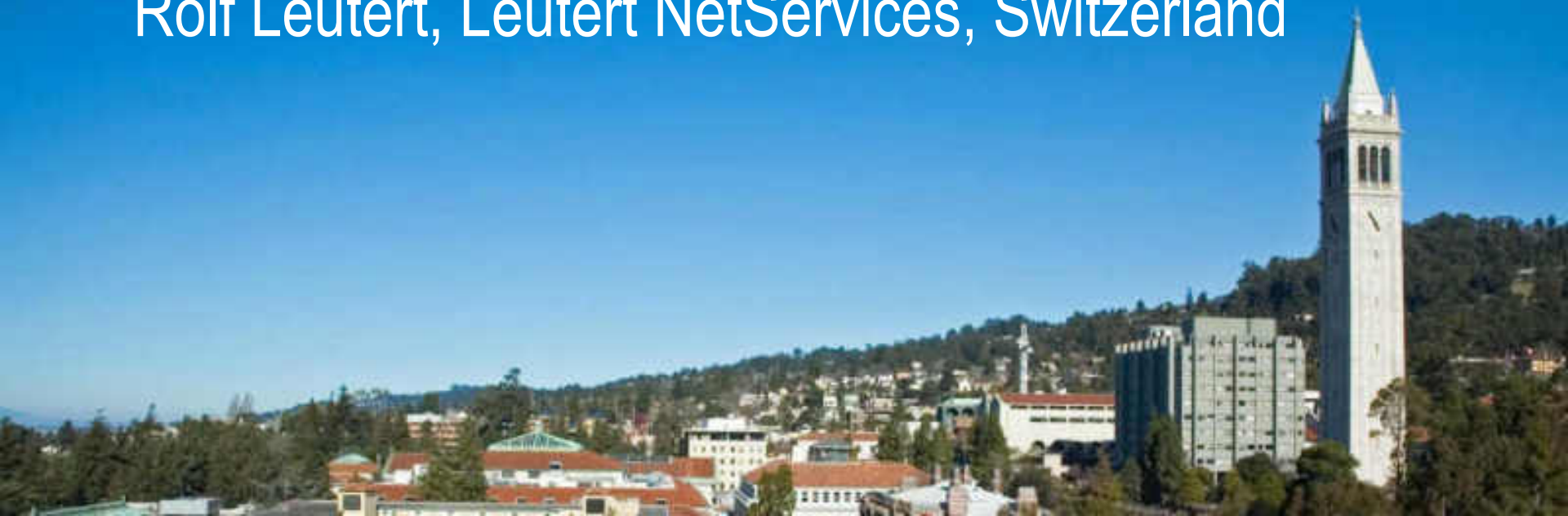# SHARKFEST '13

Wireshark Developer and User Conference

PA-12 WLAN Troubleshooting with Wireshark and AirPcap

Rolf Leutert, Leutert NetServices, Switzerland

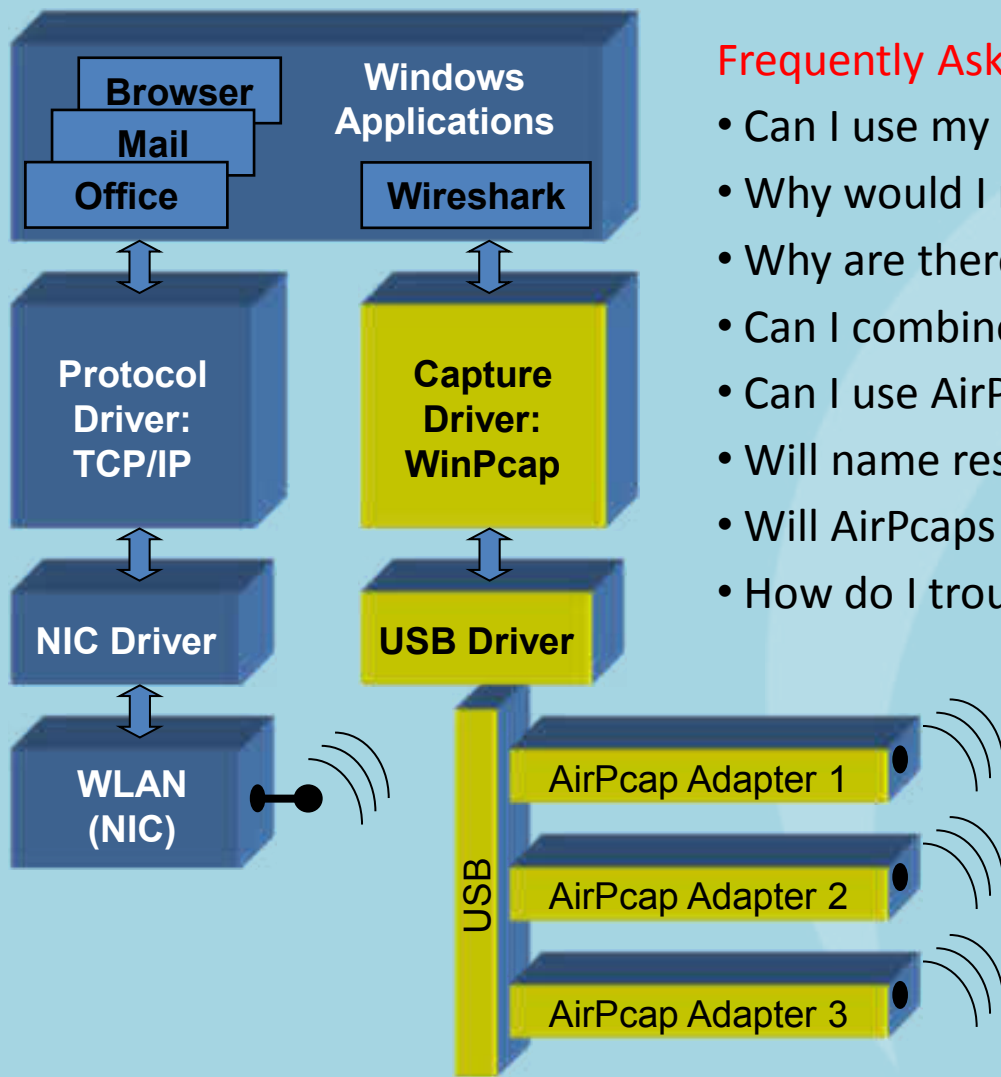# WLAN Troubleshooting with Wireshark and AirPcap

Troubleshooting WLAN problems can be a very challenging task. The wireless media is known to be unreliable. Signal interferences, low signal areas or overloaded cells are just a few of possible issues.

In addition, the compatibility between the different IEEE standards and the vendor's way of implementation is not always granted.

Having so many factors potentially impacting the performance of a wireless LAN, a systematic root-cause analysis will be more promising than the trial and error method.

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Browser
Mail
Office

Windows Applications

Wireshark

Protocol Driver: TCP/IP

Capture Driver: WinPcap

NIC Driver

USB Driver

WLAN (NIC)

USB

AirPcap Adapter 1

AirPcap Adapter 2

AirPcap Adapter 3

Frequently Asked Questions:

- Can I use my built-in WLAN NIC with Wireshark?
- Why would I need AirPcaps to analyze WLAN?
- Why are there different types of AirPcaps?
- Can I combine different types of AirPcaps?
- Can I use AirPcaps to join a WLAN?
- Will name resolution work with AirPcaps?
- Will AirPcaps show me Radio Interferences?
- How do I troubleshoot encrypted WLANs?

WLAN Troubleshooting with Wireshark and AirPcap

Capturing with built-in WLAN card

Windows Applications
- Browser
- Mail
- Office
- Wireshark

Protocol Driver: TCP/IP

NIC Driver
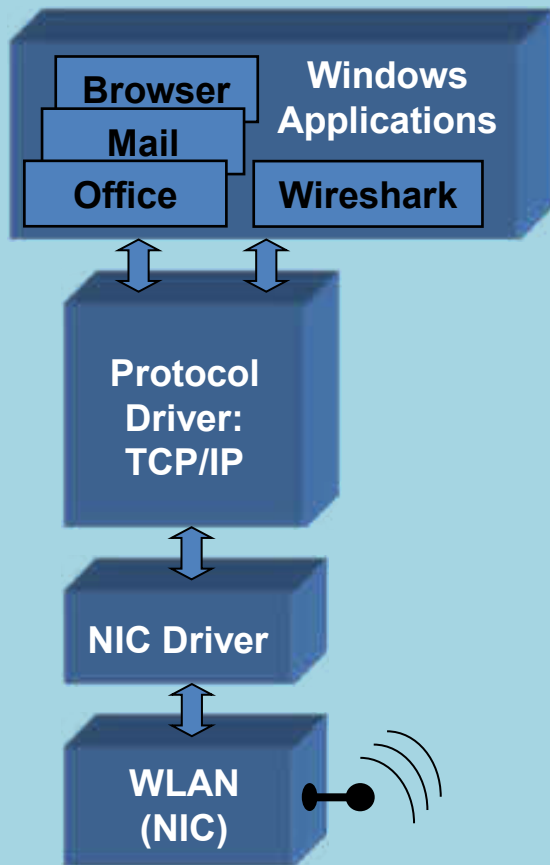
WLAN (NIC)

Frequently Given Answers:

- Yes you can use the built in WLAN NIC with Wireshark!

But with a lot of restrictions:

- No promiscuous mode, only the own traffic visible
- Frames will be displayed in Ethernet format
- No radio information like SNR, channel no, speed etc.
- One channel only, not suitable for roaming analysis

And the biggest limitation:

- No management or control frames visible!
- But these are the ones you need for troubleshooting

(Exception: under Linux some NICs support more features)

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Capturing with built-in WLAN card

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

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Capturing with AirPcap Adapters

Windows Applications

Wireshark

Capture Driver: WinPcap

USB Driver

USB

AirPcap Adapter 1

AirPcap Adapter 2

AirPcap Adapter 3
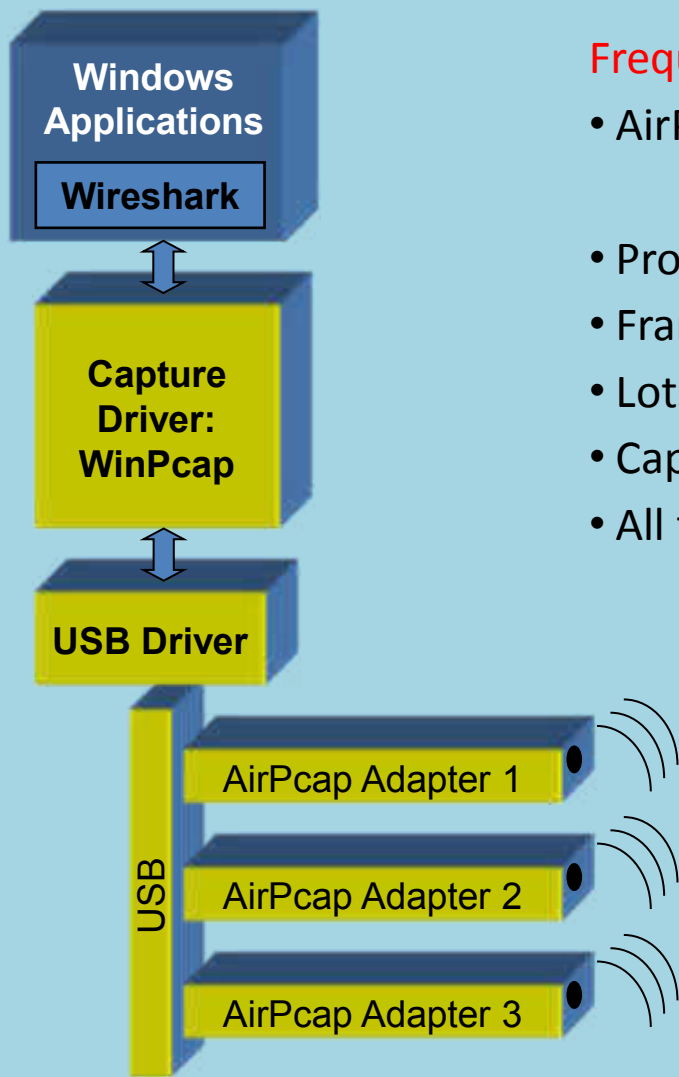
Frequently Given Answers:

• AirPcaps support the following features:

• Promiscuous mode, all traffic in a radio cell visible

• Frames will be displayed original WLAN format

• Lots of radio information like SNR, channel no, speed etc.

• Capturing in multiple channels with multiple adapters

• All frame types visible (Data, Management and Control)

WLAN Troubleshooting with Wireshark and AirPcap

Different AirPcap Adapters

AirPcap Classic
802.11b/g

AirPcap TX
802.11b/g
+ Frame injection

AirPcap NX
802.11a/b/g/n

Frequently Given Answers:
- Different AirPcaps for different 802.11 standards
- Different features at different costs
- Different AirPcaps can be combined together
- AirPcaps can not join a WLAN, are for capturing only
- Name resolution will not work for above reason
- Radio interferences can not be detected directly with AirPcaps
- Supported by all popular Windows versions up to Win7
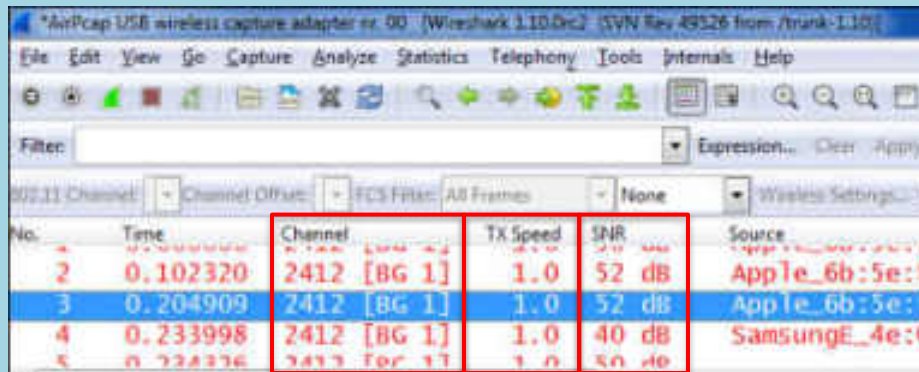
New features within near future:
- 802.11ac standard support
- Win 8 drivers
- USB 3.0 support for NX (Classic and TX today)
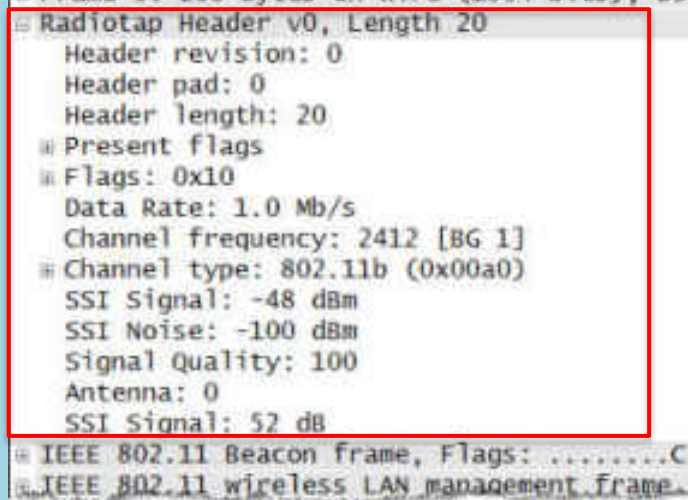
www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Additional Wireshark Columns

- AirPcaps add a Radiotap Header with useful information to each captured frame
- Verify that the Radio option is turned on

Use the fields to add columns for:
- Channel #, TX Speed, SNR

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Frame Types Overview

The Management Frames:

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

The Control Frames:
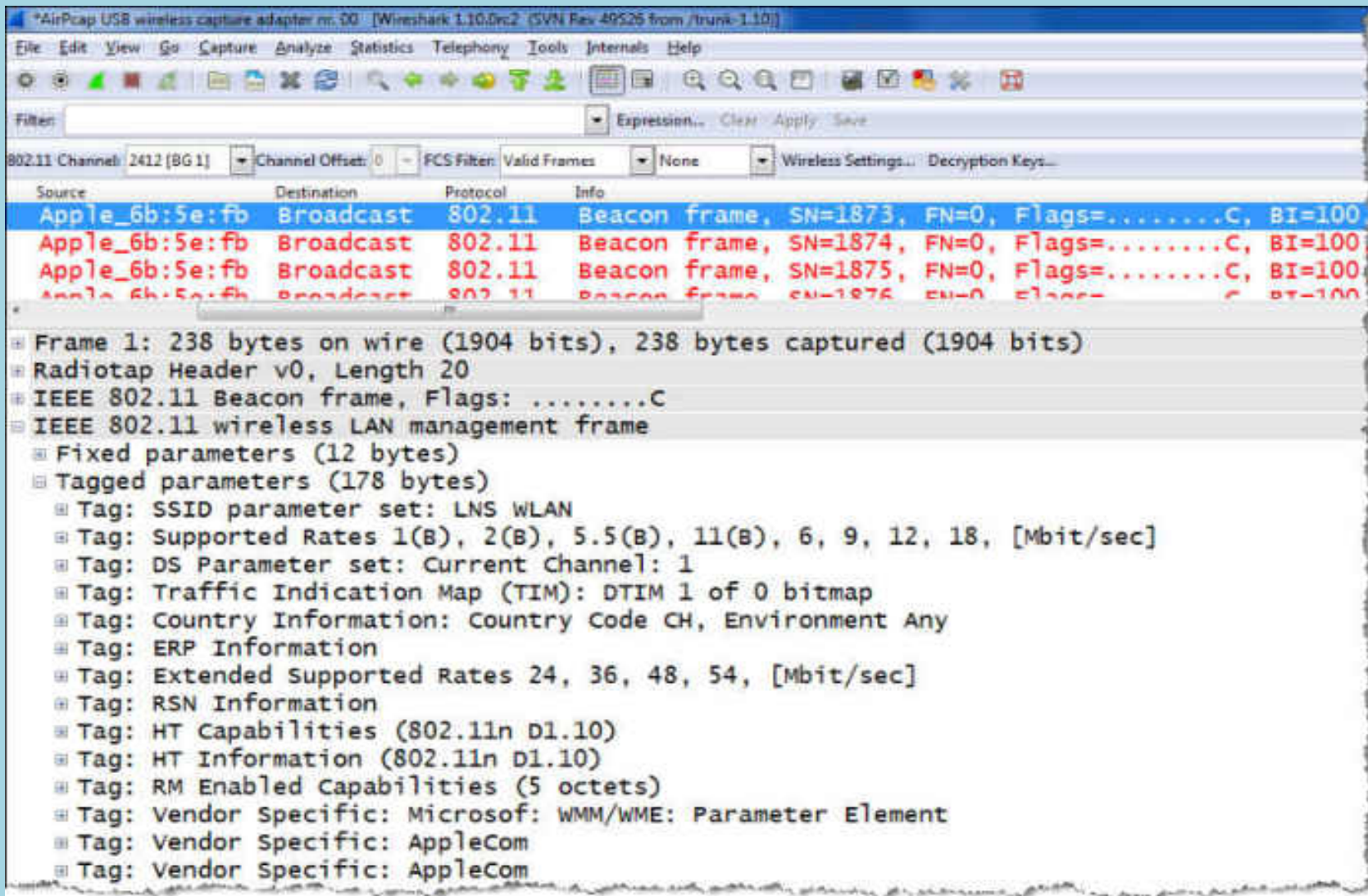
- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledge / Block Acknowledge Request / Block Acknowledge
- Power Save Poll

The Data Frames:

- Data
- Null Function

WLAN Troubleshooting with Wireshark and AirPcap

Frame Type: Beacon

© Leutert NetServices 2013

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Probe Request / Probe Response

© Leutert NetServices 2013

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Authentication Request / Authentication Response

© Leutert NetServices 2013

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Association Request / Association Response

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: EAPOL Key Messages

WLAN Troubleshooting with Wireshark and AirPcap

Frame Type: Action

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Decrypted Data Frame followed by Block Acknowledge

- WEP and WPA1/2 personal mode (shared key) can be decrypted by Wireshark
- To enable WPA decryption, the key negotiation process must be captured too
- Shared Key decryptions is possible during capturing or offline from a stored file

www.wireshark.ch
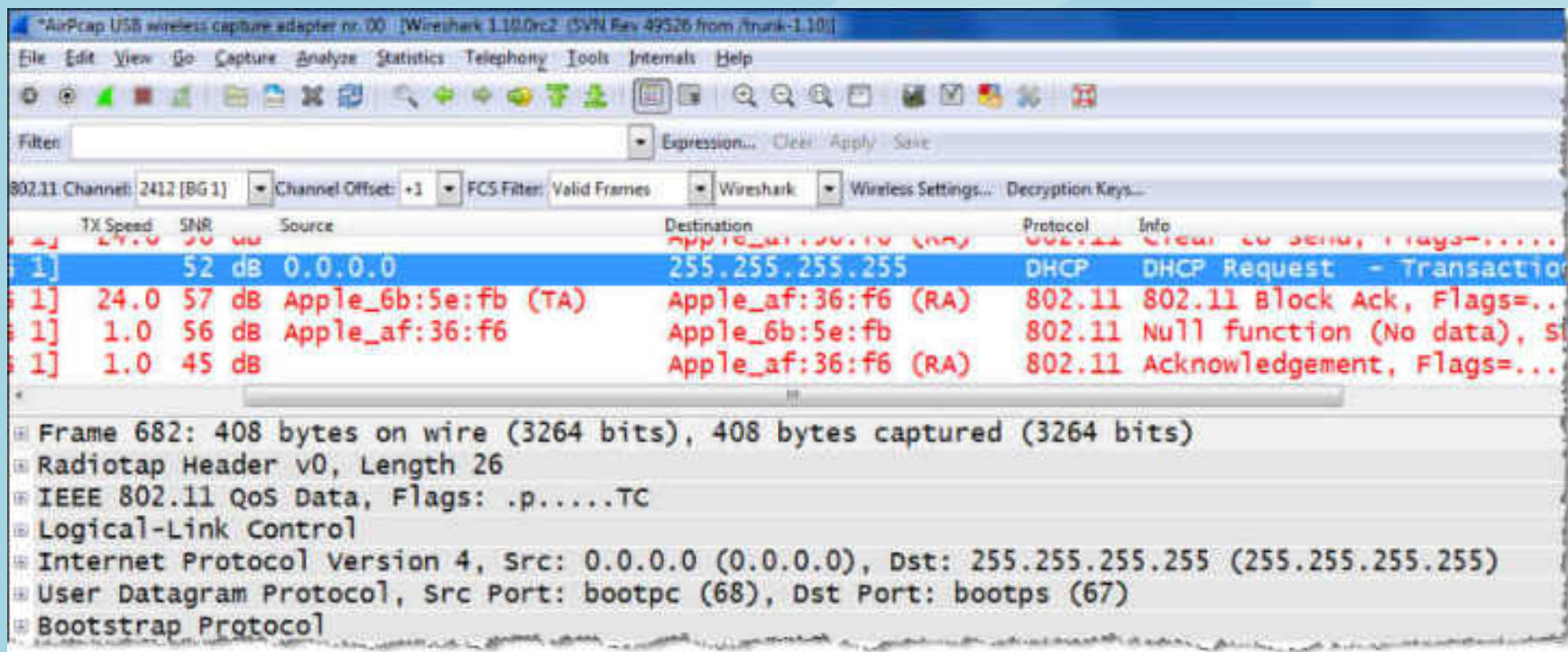
WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Null Function Data followed by Acknowledge

- The Null Function frame is often used as keep-alive message from the client
- Another purpose is to inform the AP if the client is changing the power save status

www.wireshark.ch
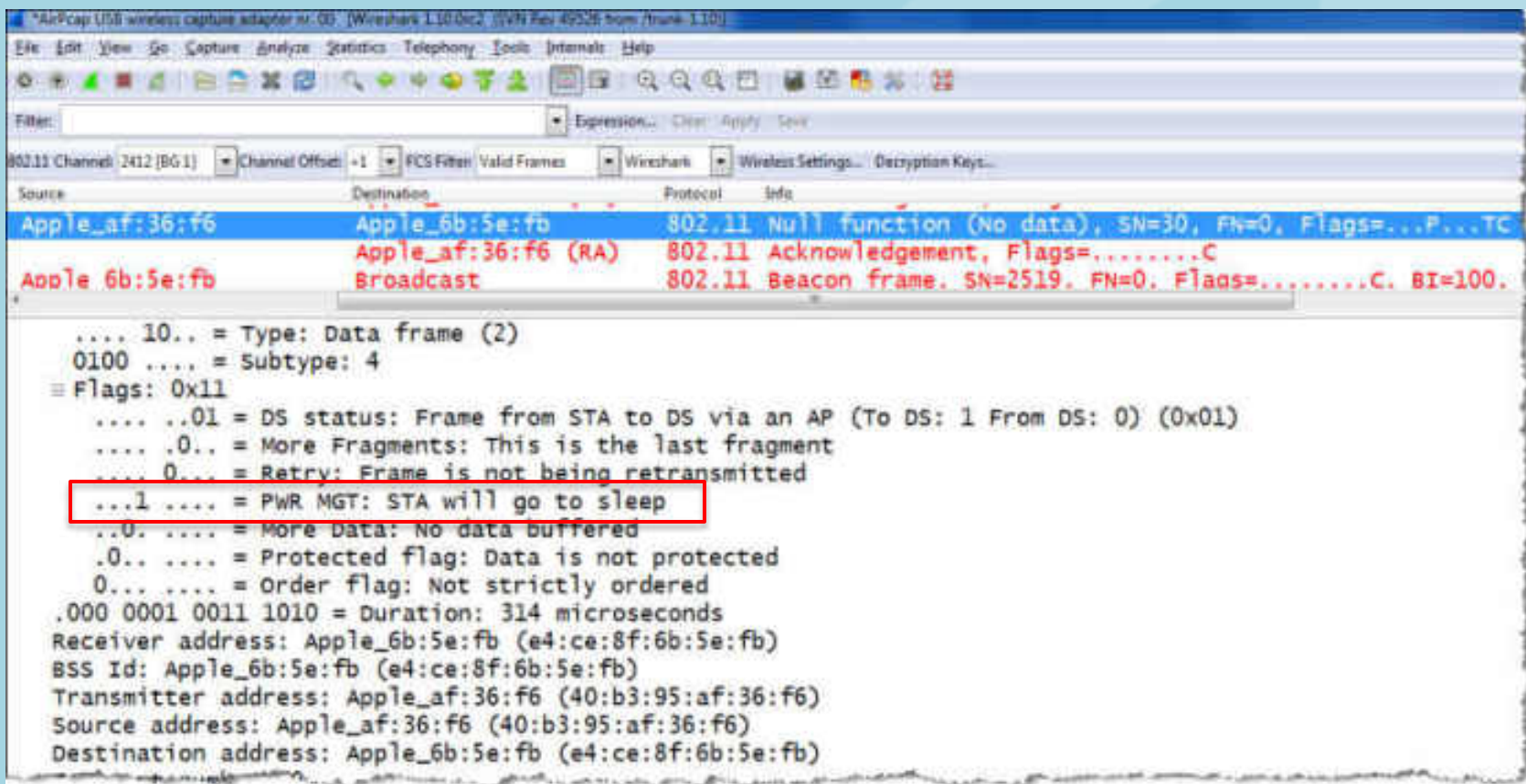
WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Request-to-send (RTS) and Clear-to-send (CTS)

- RTS /CTS are used to reserve airtime in hidden node situations or busy networks
- Another purpose is to hinder old clients from interfering with clients of new standards

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Data and Acknowledges

- In the air, every Data frame is acknowledged or otherwise retransmitted
- 802.11 a/b/g every single Data frame is acknowledged. 802.11n introduced Block Acks
- Single Acks must follow immediately after a Data frame and have no source address

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Filter on Retransmitted frames

- Retransmitted frames are marked with the Retry Bit by the sender
- Create a Display Filter on retransmitted frames and save it as a Quick Filter Button
- Watch the percentage of retransmitted versus original frames in the bottom line

© Leutert NetServices 2013 www.wireshark.ch
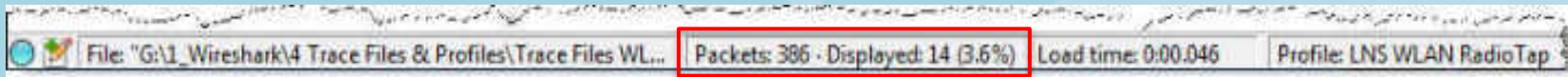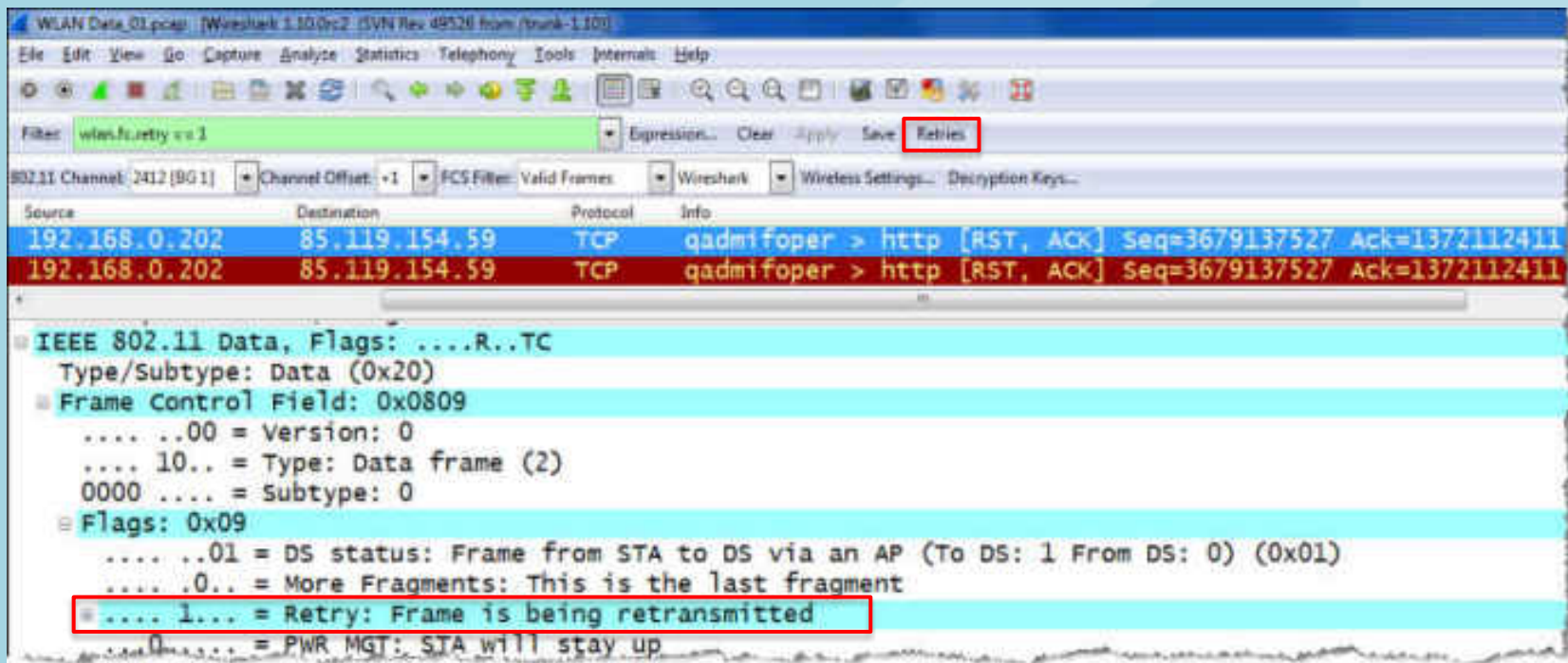
WLAN Troubleshooting with Wireshark and AirPcap

Where to capture WLAN frames

• The physical location within a radio cell is relevant for your capturing results

Rules of thumb

For analyzing problems in a single cell:
• Stay near the Access Point
• All traffic flows through the AP
• Clients must not hear each other

For analyzing roaming problems:
• Stay near the roaming client
• Capture with multiple AirPcaps
• Use Beacons to define your location

SSID: LNSWLAN
Channel 1

Enterprise
Network

Distribution
System

SSID: LNSWLAN
Channel 6

www.wireshark.ch
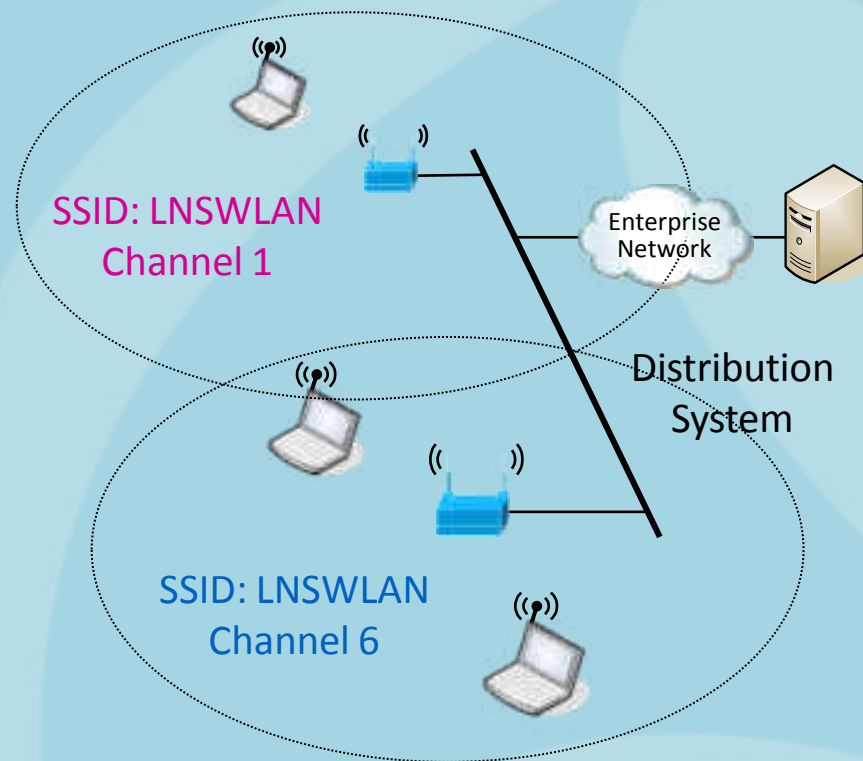
WLAN Troubleshooting with Wireshark and AirPcap

Graphical presentation of Radio Signal Strength with Wireshark IO Graphs

- Using the field radiotap.db_antsignal from two AirPcap NX tuned in two channels
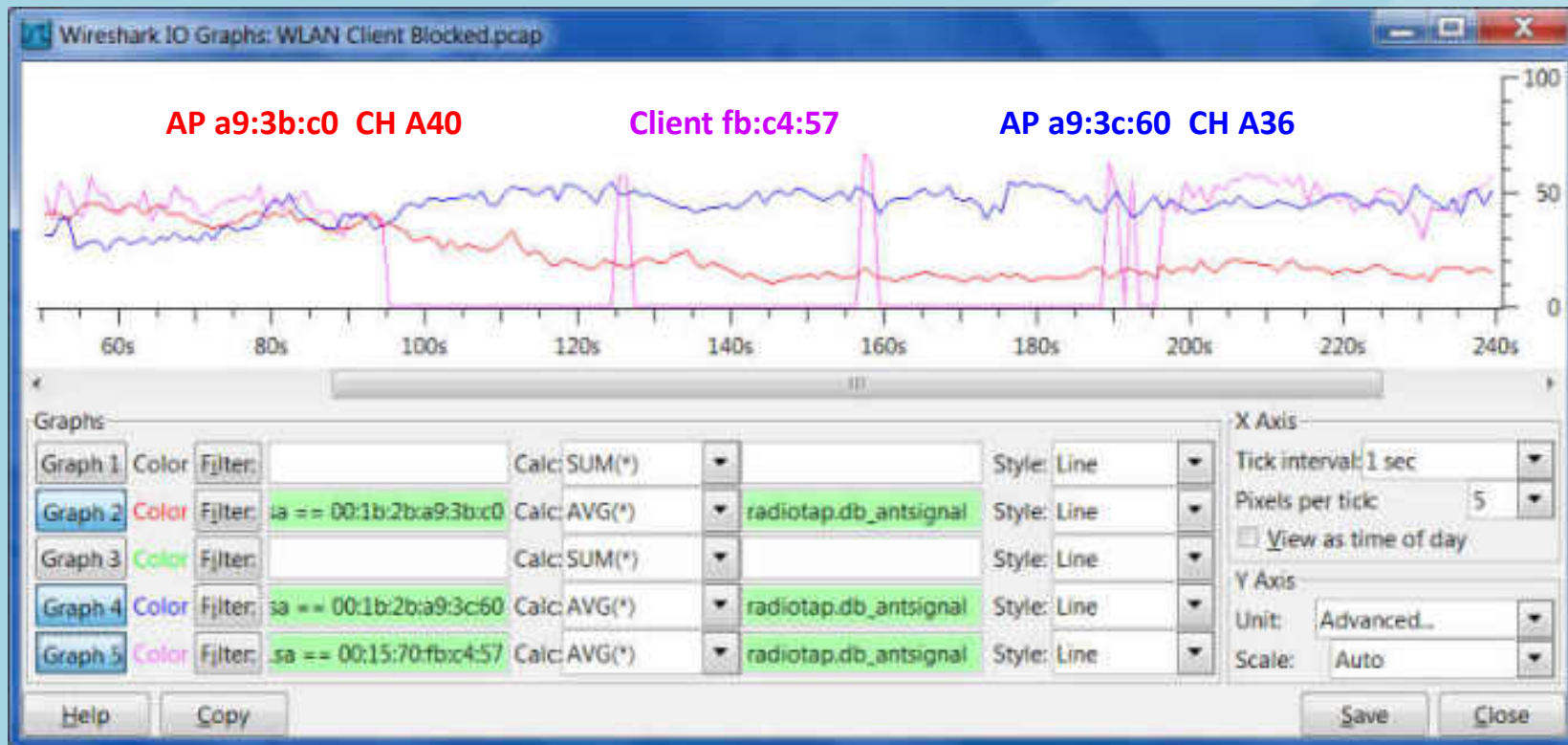
Graph 2 Color Filter: wlan.sa == 00:1b:2b:a9:3b:c0 → Access Point in Channel A40
Graph 4 Color Filter: wlan.sa == 00:1b:2b:a9:3c:60 → Access Point in Channel A36
Graph 5 Color Filter: wlan.sa == 00:15:70:fb:c4:57 → Mobile Client followed with Wireshark

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Overview of WLAN standards

Mbps	Coding	Modulation	Description		
1 2	Barker Barker	DBPSK	**802.11** **DSSS (Clause 15)** with ‚Long Preamble'		
5.5 11	CCK CCK	DQPSK	**802.11b** **HR/DSSS (Clause 18)** with ‚Short Preamble'		
6, 9 12, 18 24, 36 48, 54	OFDM OFDM OFDM OFDM	BPSK QPSK 16-QAM 64-QAM	**802.11g** **Extended Rate PHY** **(ERP)**		**802.11a**
7.2-72.2 14.4-144.4	OFDM OFDM	MCS 0-7 MCS 8-15	1 Stream 2 Streams	**802.11n** **High Troughput (HT)** **Extensions**	

2.4 GHz   **5 GHz**

CCK = Complementary Code Keying   BPSK = Binary Phase-Shift Keying
DBPSK = Differential Binary Phase-Shift Keying   QPSK = Quadrature Phase-Shift Keying
DQPSK = Differential Quadrature Phase-Shift Keying QAM = Quadrature Amplitude Modul.
OFDM = Orthogonal Frequency Division Multiplexing   MCS = Modulation Coding Scheme

www.wireshark.ch

WLAN Troubleshooting with Wireshark and AirPcap

Outlook to WLAN products and standards

- 802.11n products using 4 streams will go up to 600 Mbps (PHY data rate)
- 802.11n products using Beamforming to focus RF energy and improve radio signal
- 802.11z Direct Link Setup to allow direct client to client communication
- 802.11w Management Frame Protection to increase security level against intruders

- 802.11ac 5G WiFi is an improvement to 802.11n. Uses 5GHz band and defines up to a maximum of 6.93 Gbps with up to 8 streams and up to 8 bonded channels (160 MHz)

802.11ac 5G WiFi logo

802.11ad WiGig logo

- 802.11ad WiGig for short range WLANs using 60GHz band with up to 7Gbps

www.wireshark.ch

Thank you for your attention

© SeaPics.com

Hope you learned something useful

Rolf Leutert, Leutert NetServices, www.wireshark.ch