Analyzing WLANs with Wireshark & AirPcap

Sessions BU-5

Rolf Leutert

Consultant & Trainer | Leutert NetServices, Switzerland

SHARKFEST **'09**

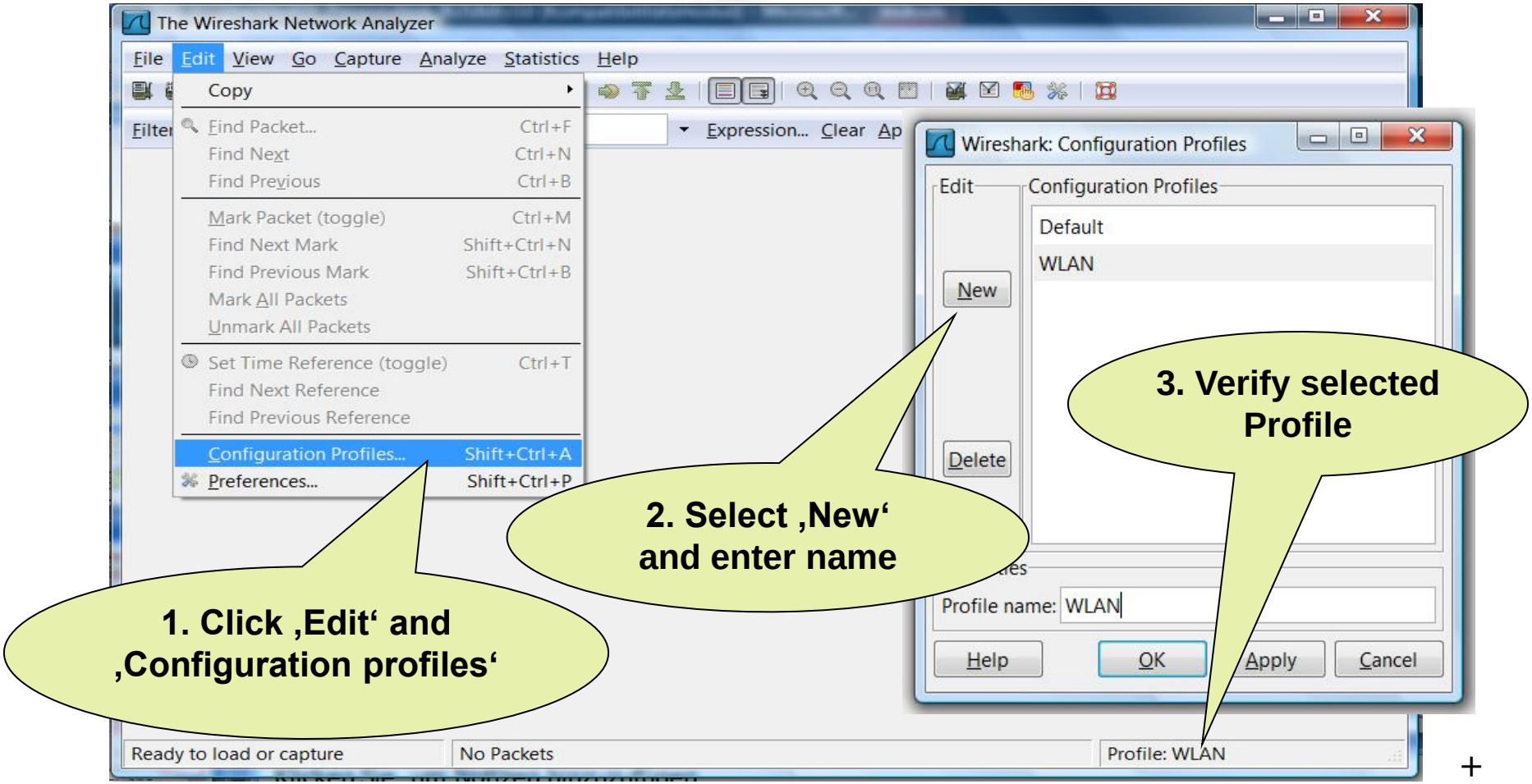
Stanford University

June 15-18, 2009

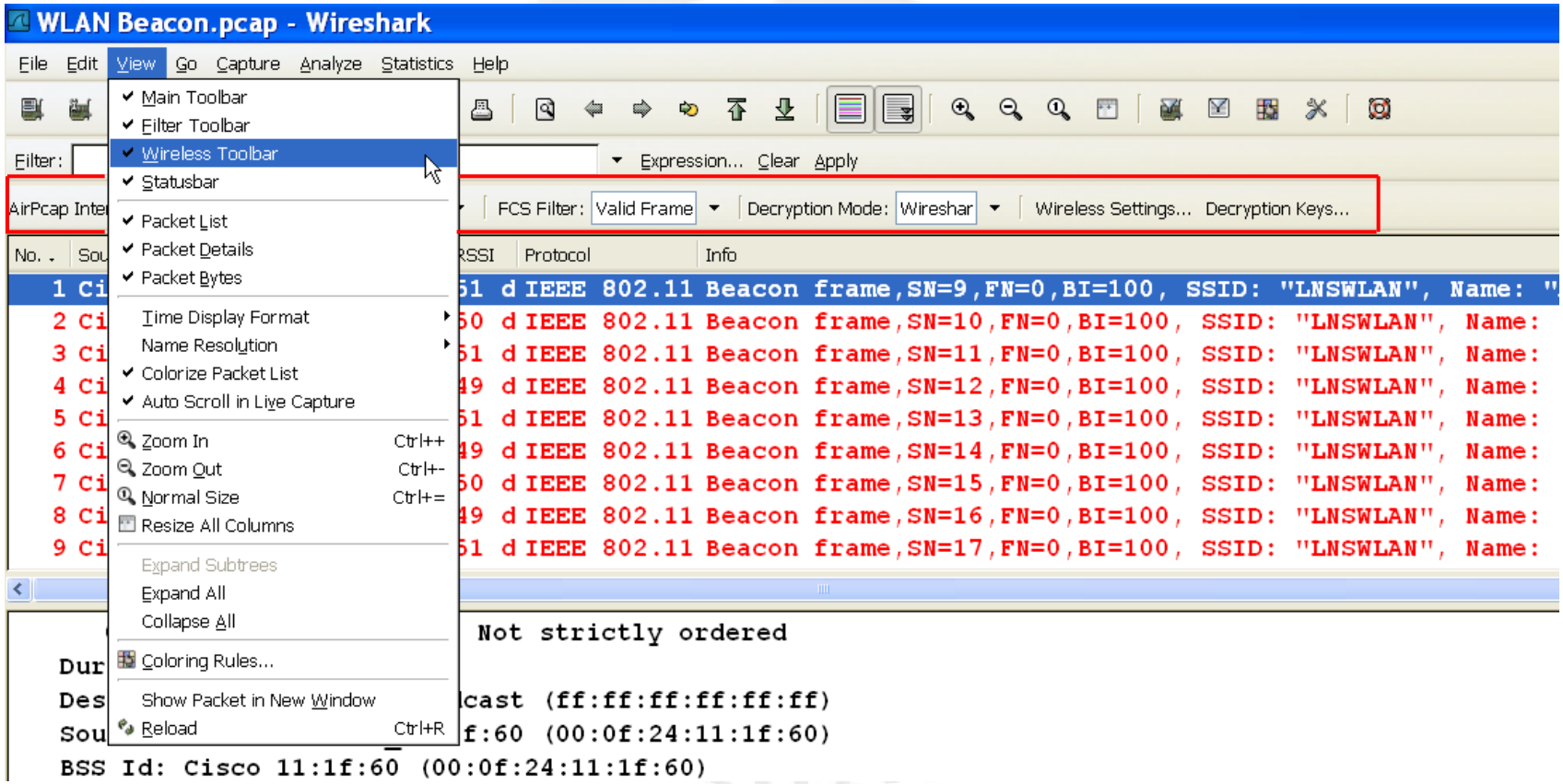
Agenda

- Setting up Wireshark with AirPcap
- Capturing WLAN data
- WLAN Management, Control & Data Frames
- WLAN Frame Formats
- Analyzing: Client can not associate
- Analyzing: Roaming problems
- Analyzing: Throughput issues
- Multiple-Input, Multiple-Output (MIMO)

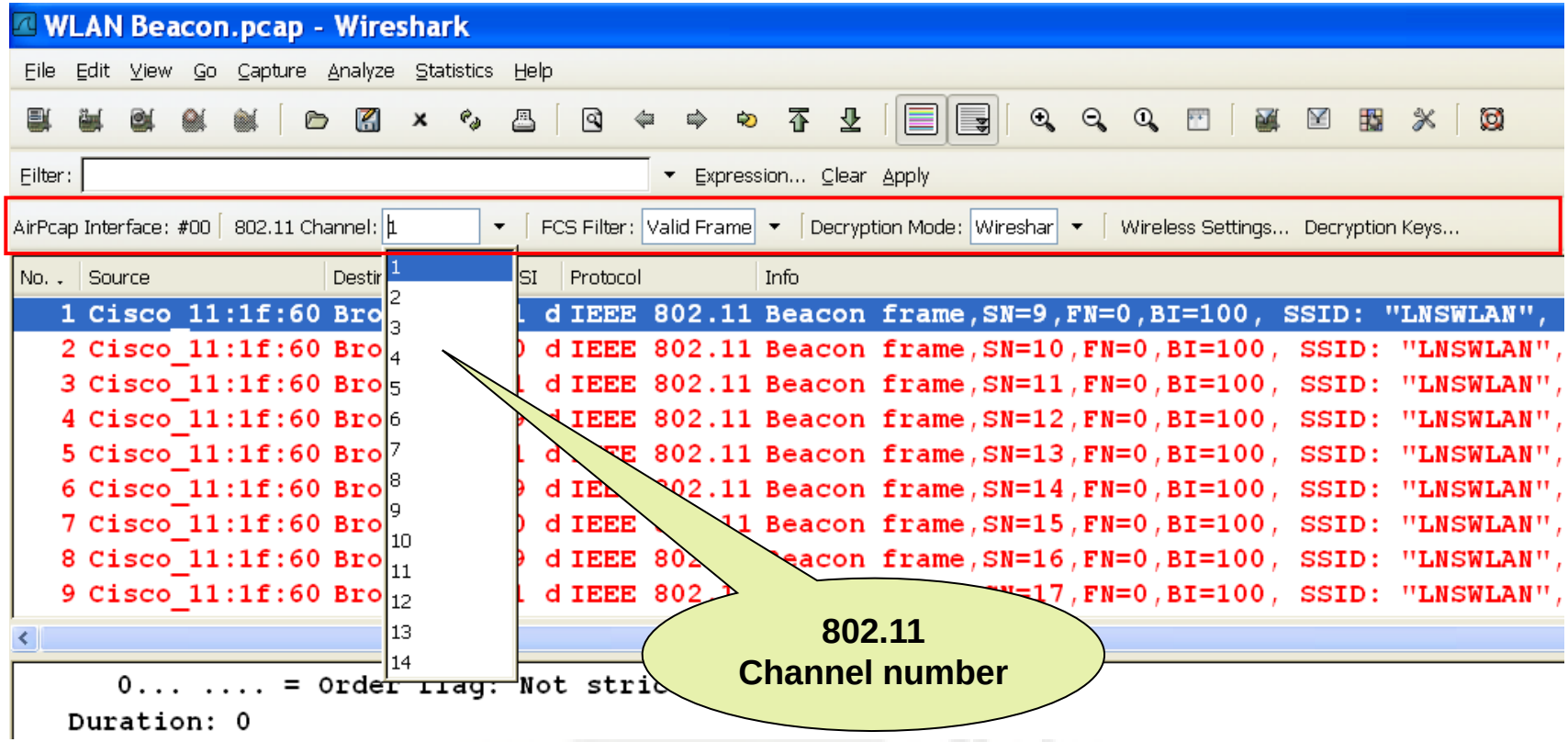
Creating a WLAN profile



The Wireless Toolbar

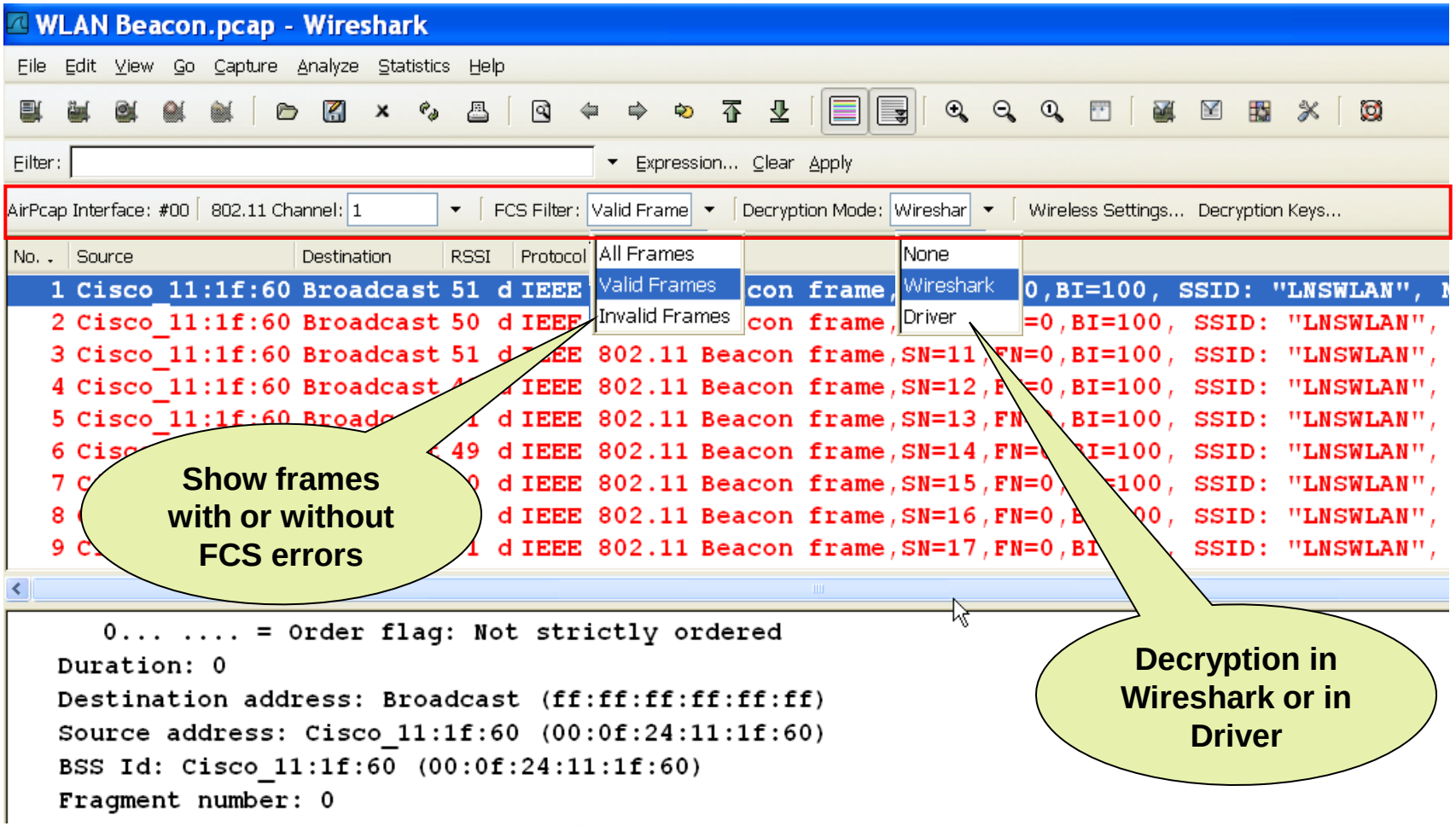


The Wireless Toolbar

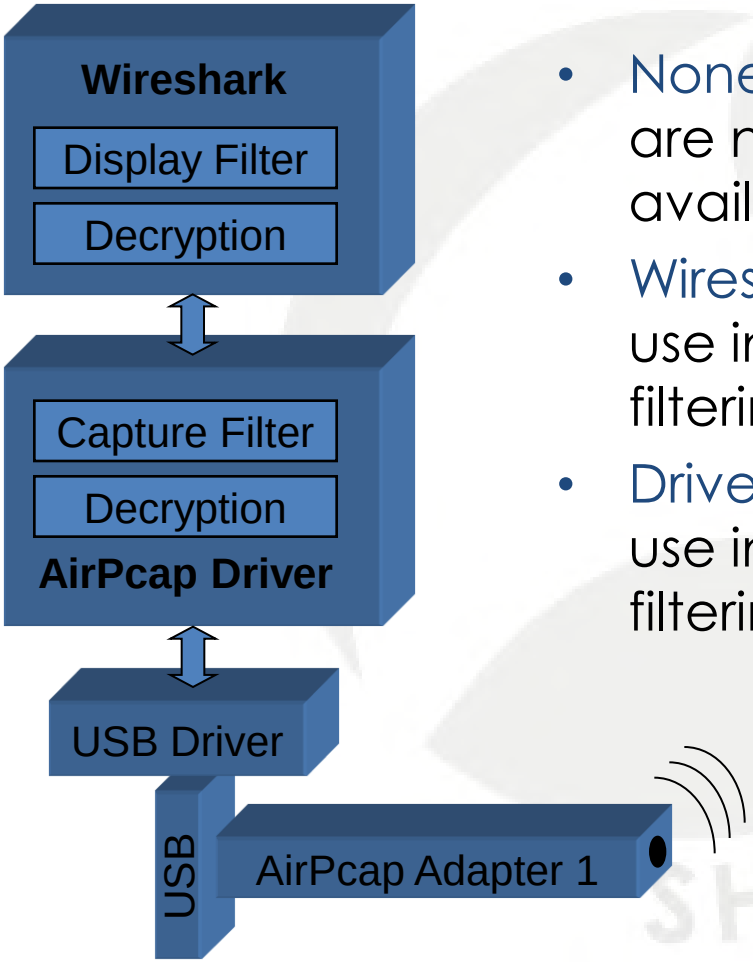


- Channel number can be changed during capturing

The Wireless Toolbar

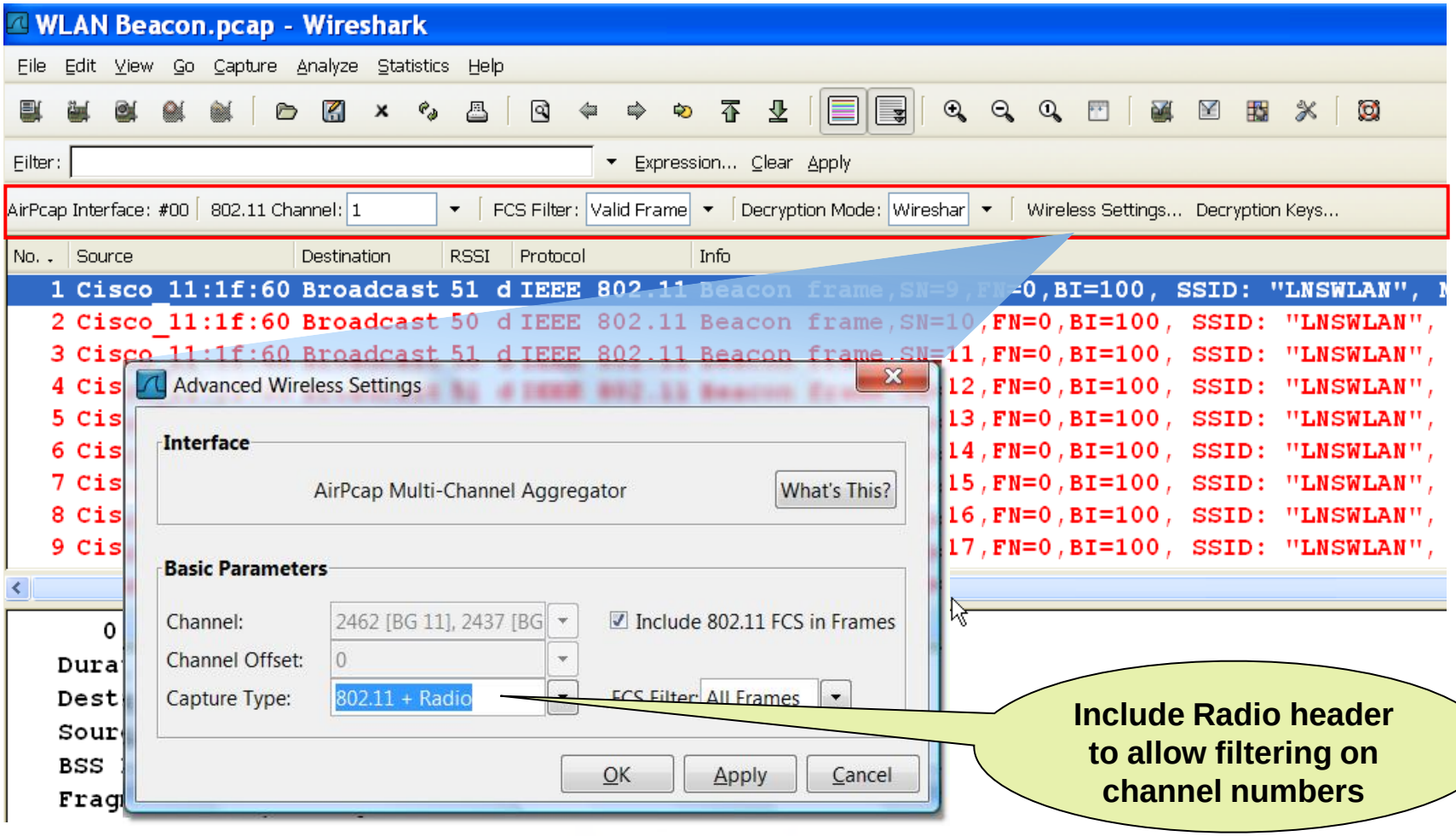


Decryption Modes

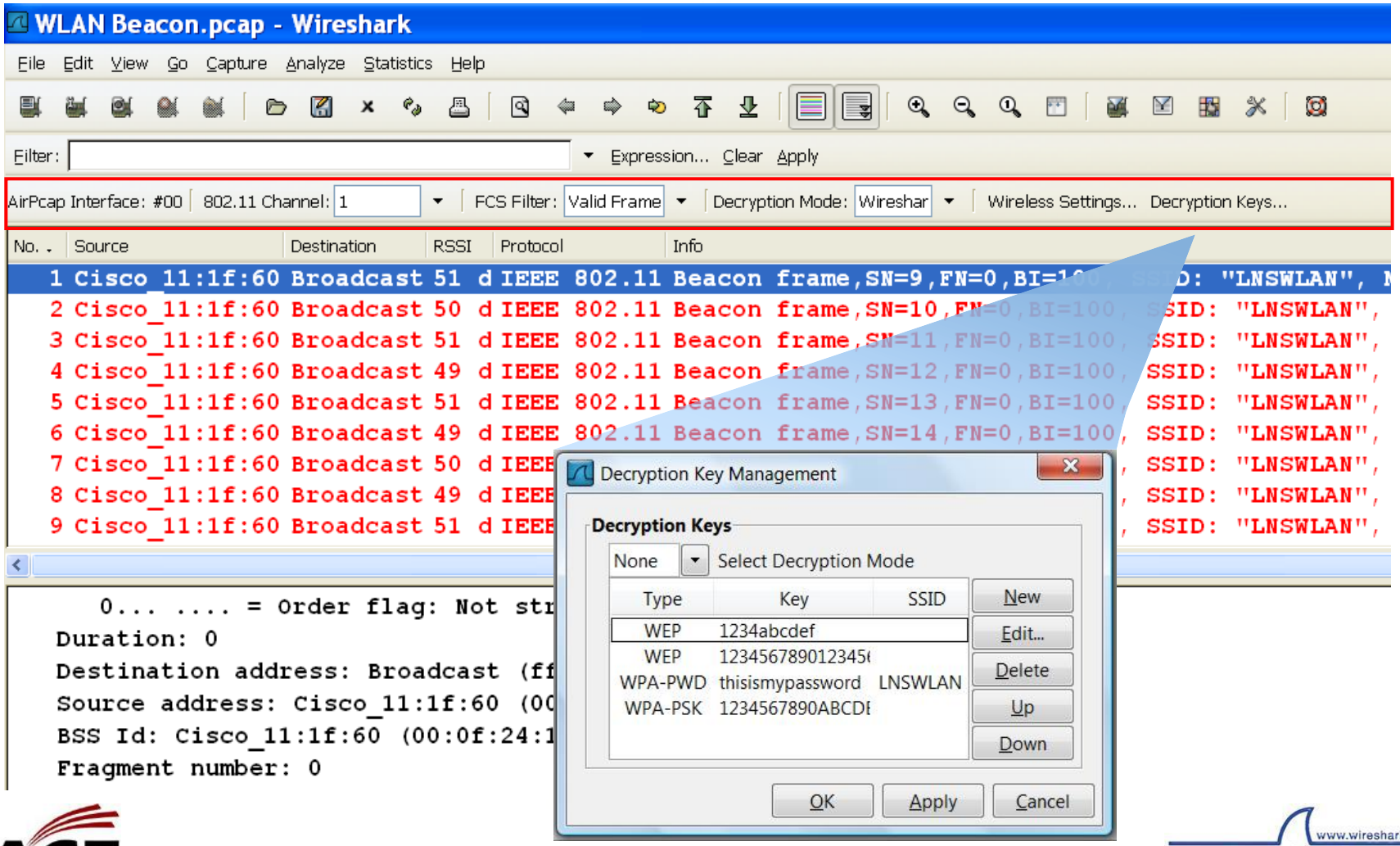


- None: no decryption - use if packets are not encrypted or if key is not available
- Wireshark: decryption in Wireshark – use in combination with display filtering
- Driver: decryption in AirPcap driver – use in combination with capture filtering only

The Wireless Toolbar



The Wireless Toolbar



Decryption Keys

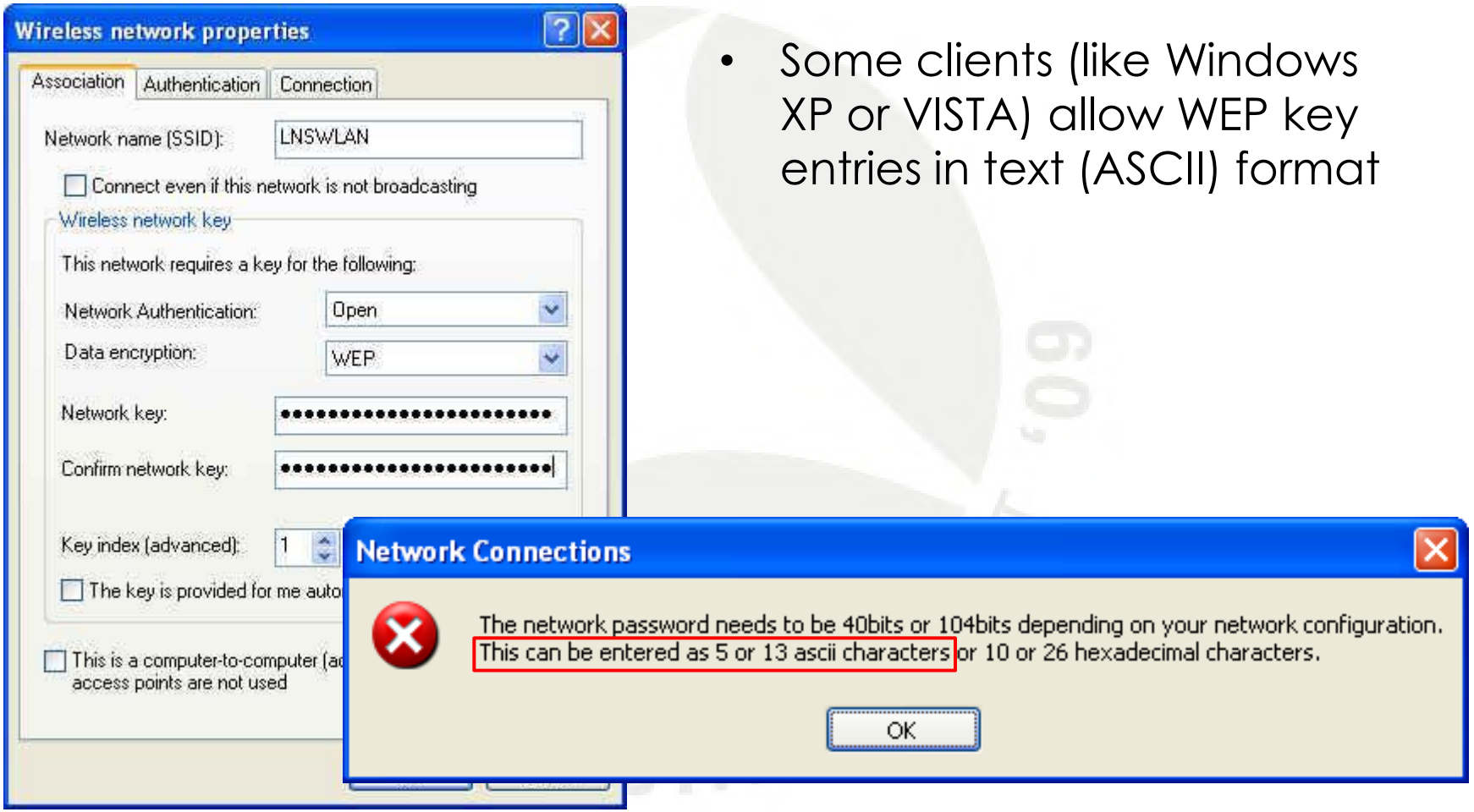
- Wireshark supports decryption of WEP, WPA1 and WPA2 with static shared keys:

- WEP Key formats:

Keys					
light *	5 ASCII	Character	5x8bit =	40 + 24 bit IV =	64 bit Key
1234ABCDEF	10 HEX	Character	10x4bit =	40 + 24 bit IV =	64 bit Key
lightningstar *	13 ASCII	Character	13x8bit =	104 + 24 bit IV =	128 bit Key
123456..ABCDEF	26 HEX	Character	26x4bit =	104 + 24 bit IV =	128 bit Key

* Wireshark does not support text entries for WEP keys, use a Text-to-HEX converter like www.swingnote.com/tools/texttohex.php

Decryption Keys



- Some clients (like Windows XP or VISTA) allow WEP key entries in text (ASCII) format

Decryption Keys

- WPA-PWD (Password)

Key	SSID
thisismypassword	LNSWLAN

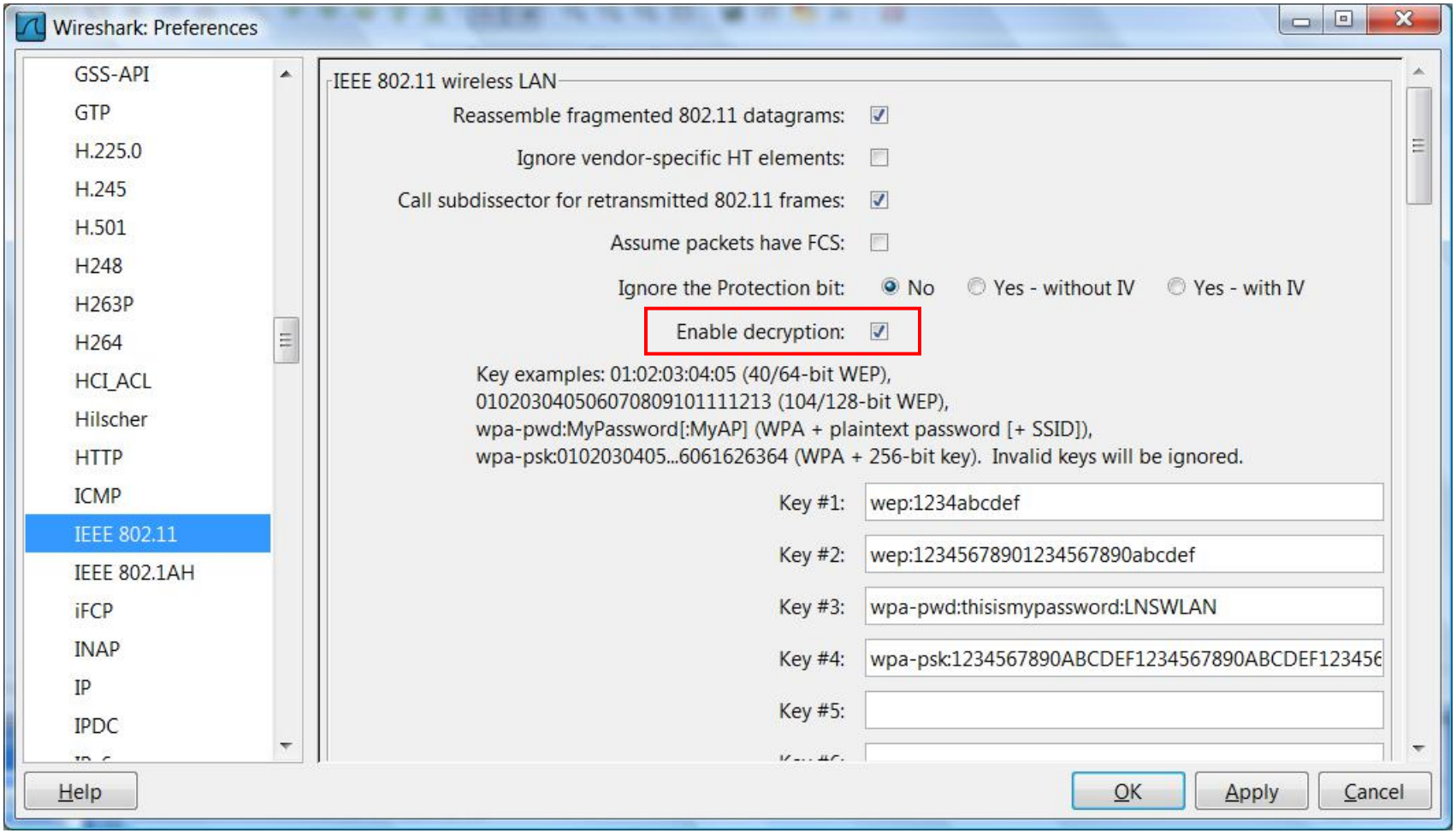
8 to 63 ASCII character password and SSID

- WPA-PSK (Pre-shared-key)

1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF

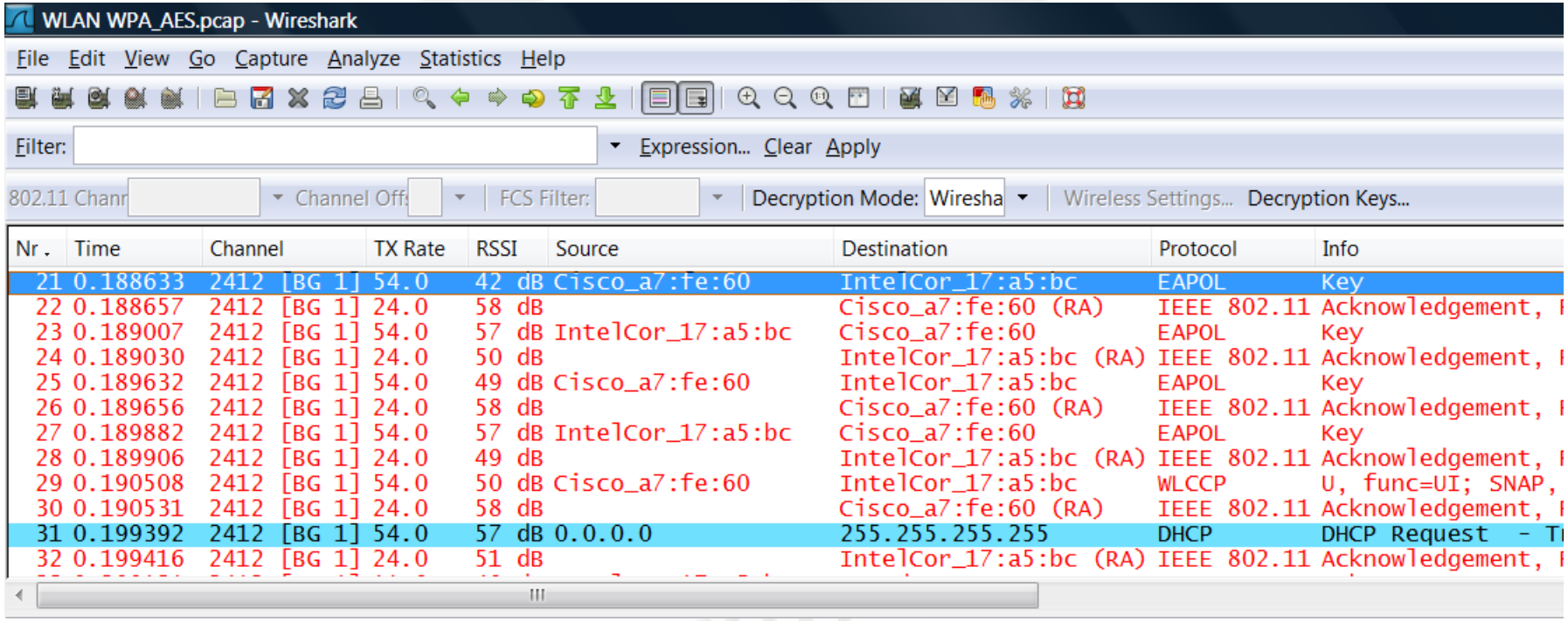
exact 64 long HEX character string

Decryption Keys

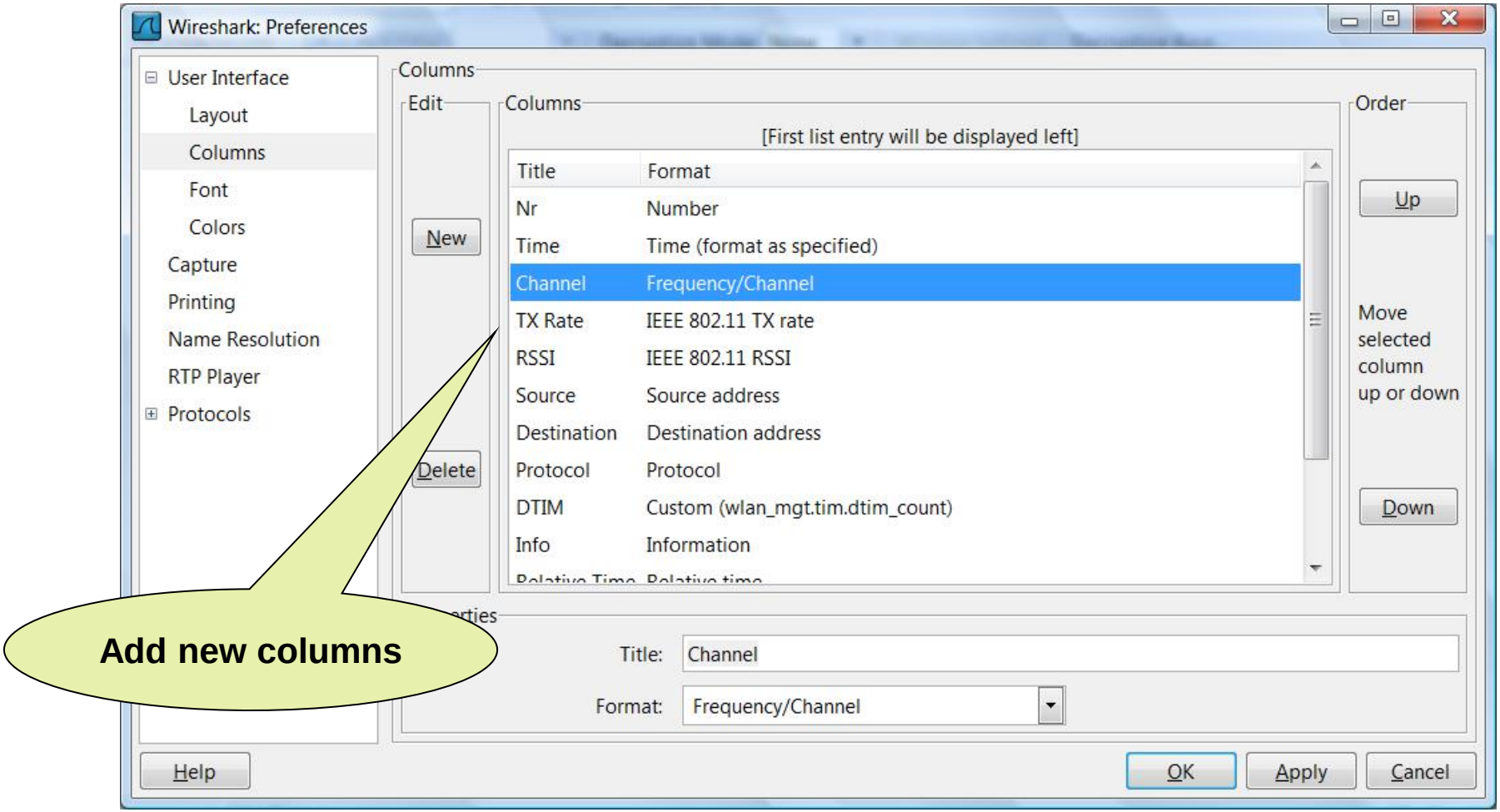


Decryption Keys

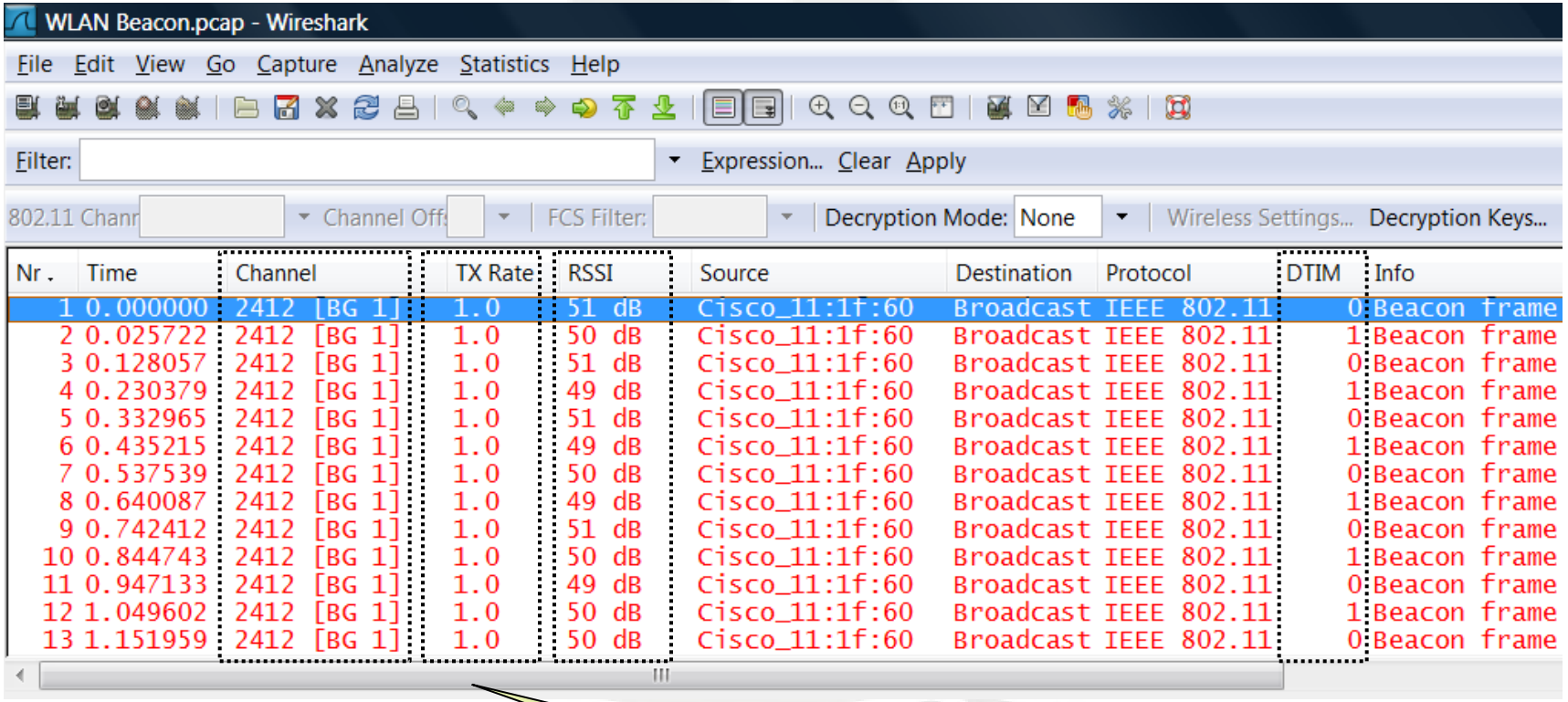
- In order to decrypt WPA, you also need to capture the key negotiation process during connection setup



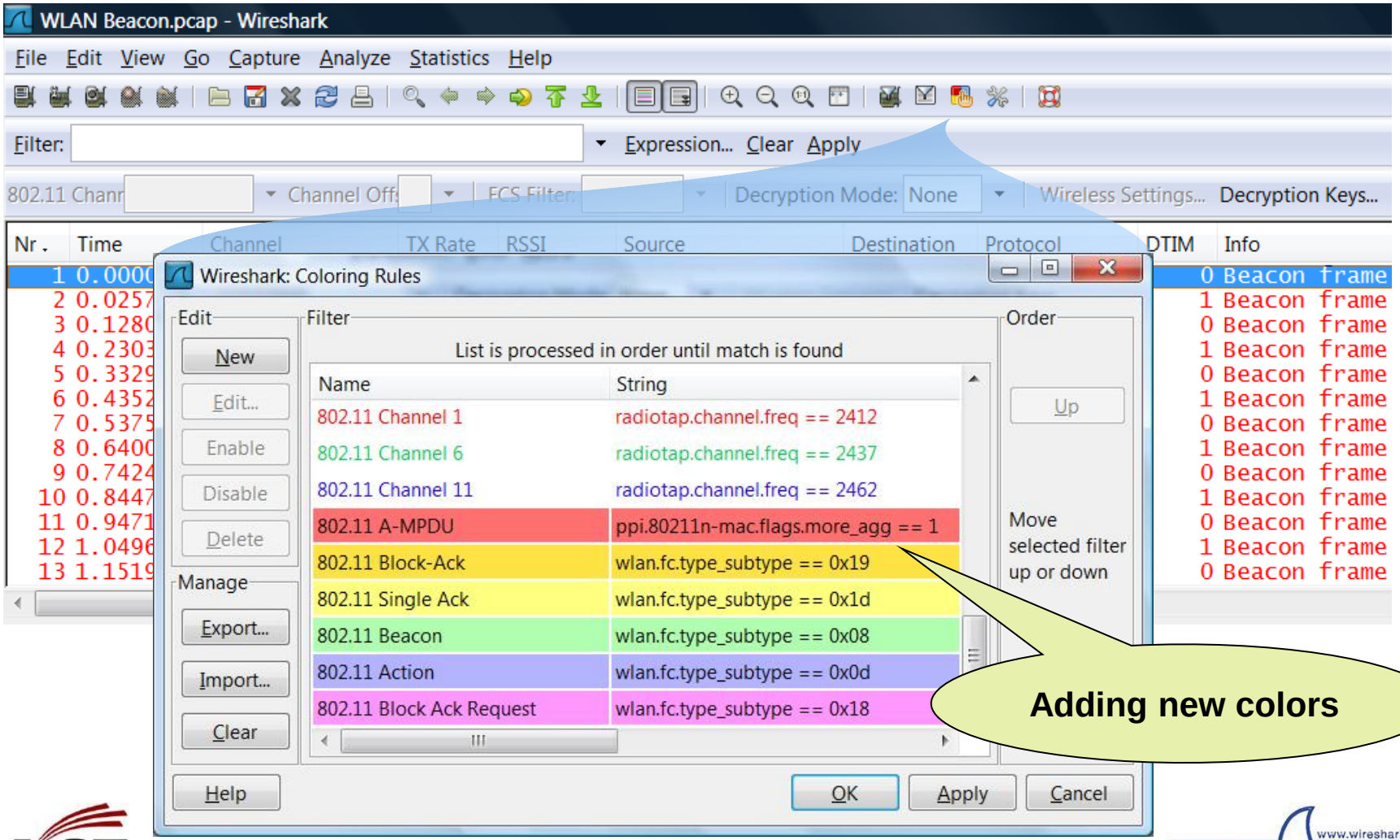
Tuning display for WLAN



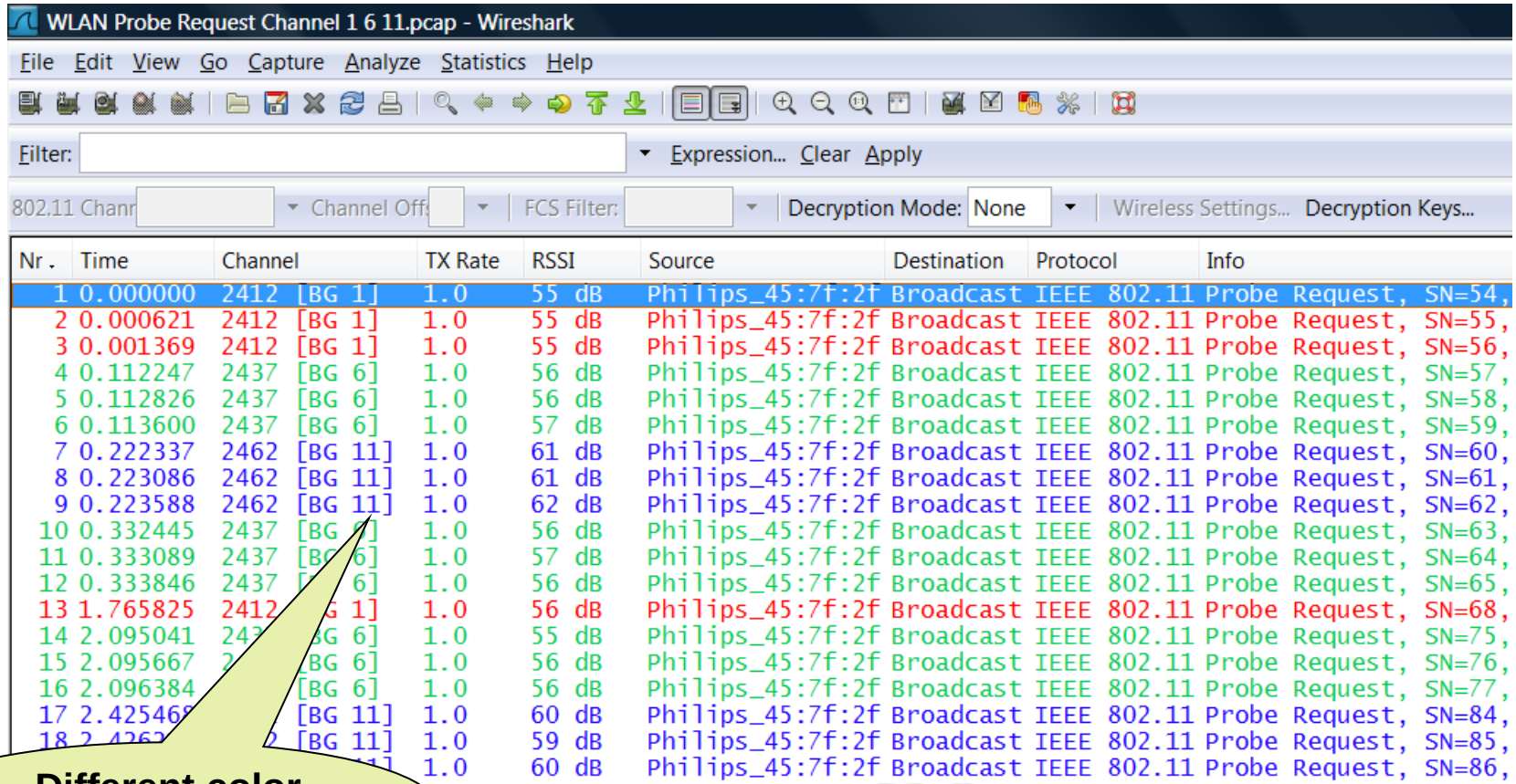
Tuning display for WLAN



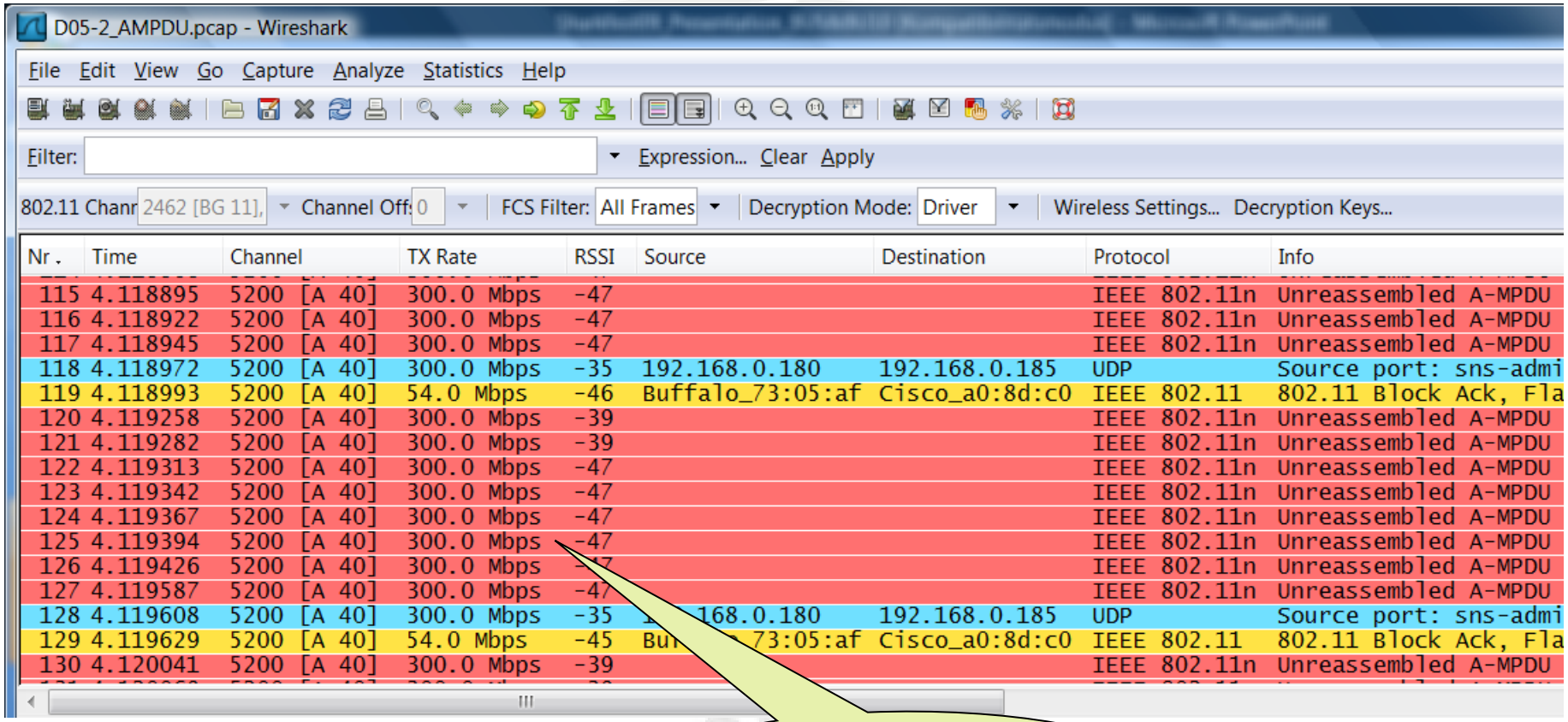
Tuning display for WLAN



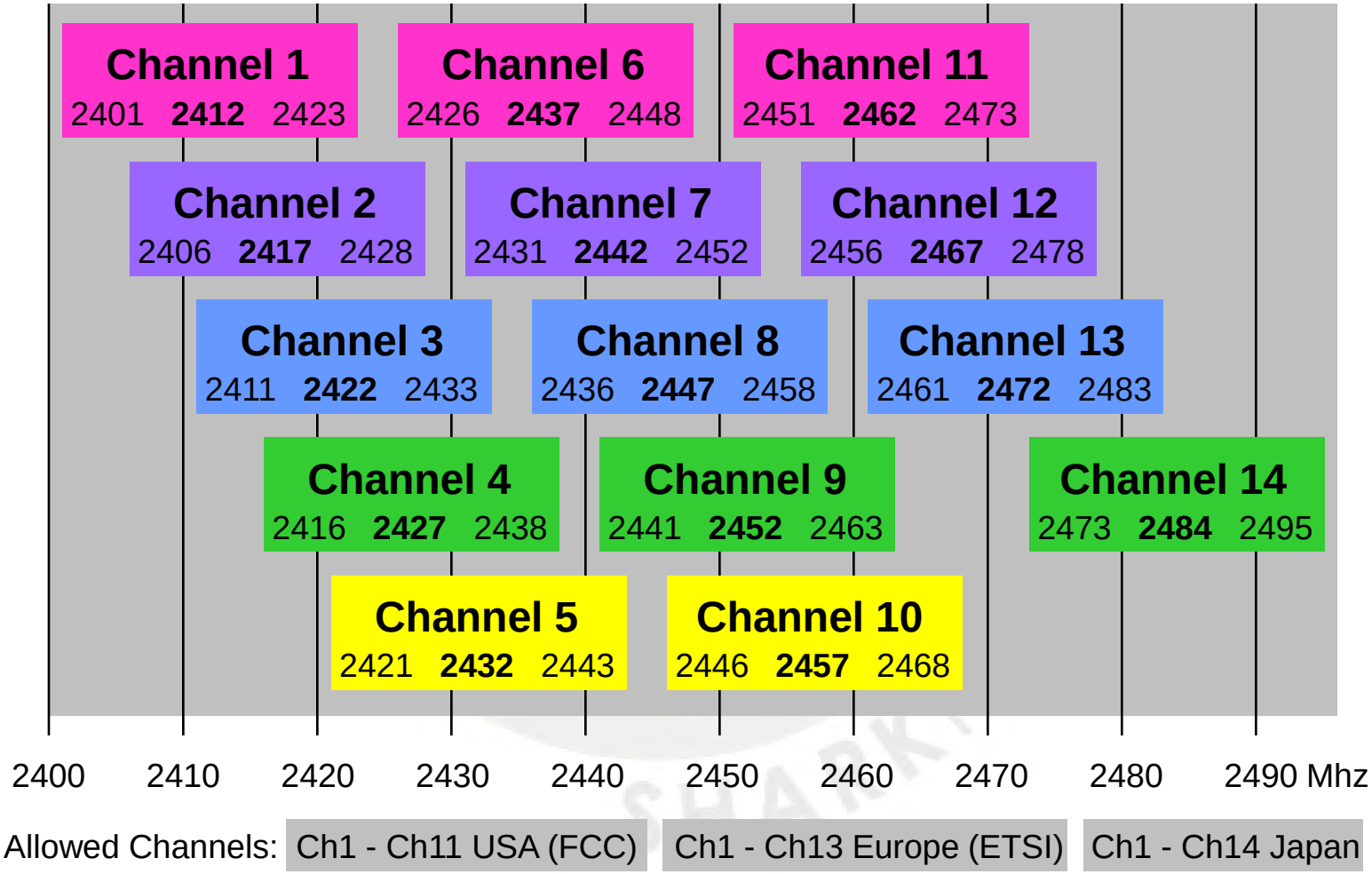
Tuning display for WLAN



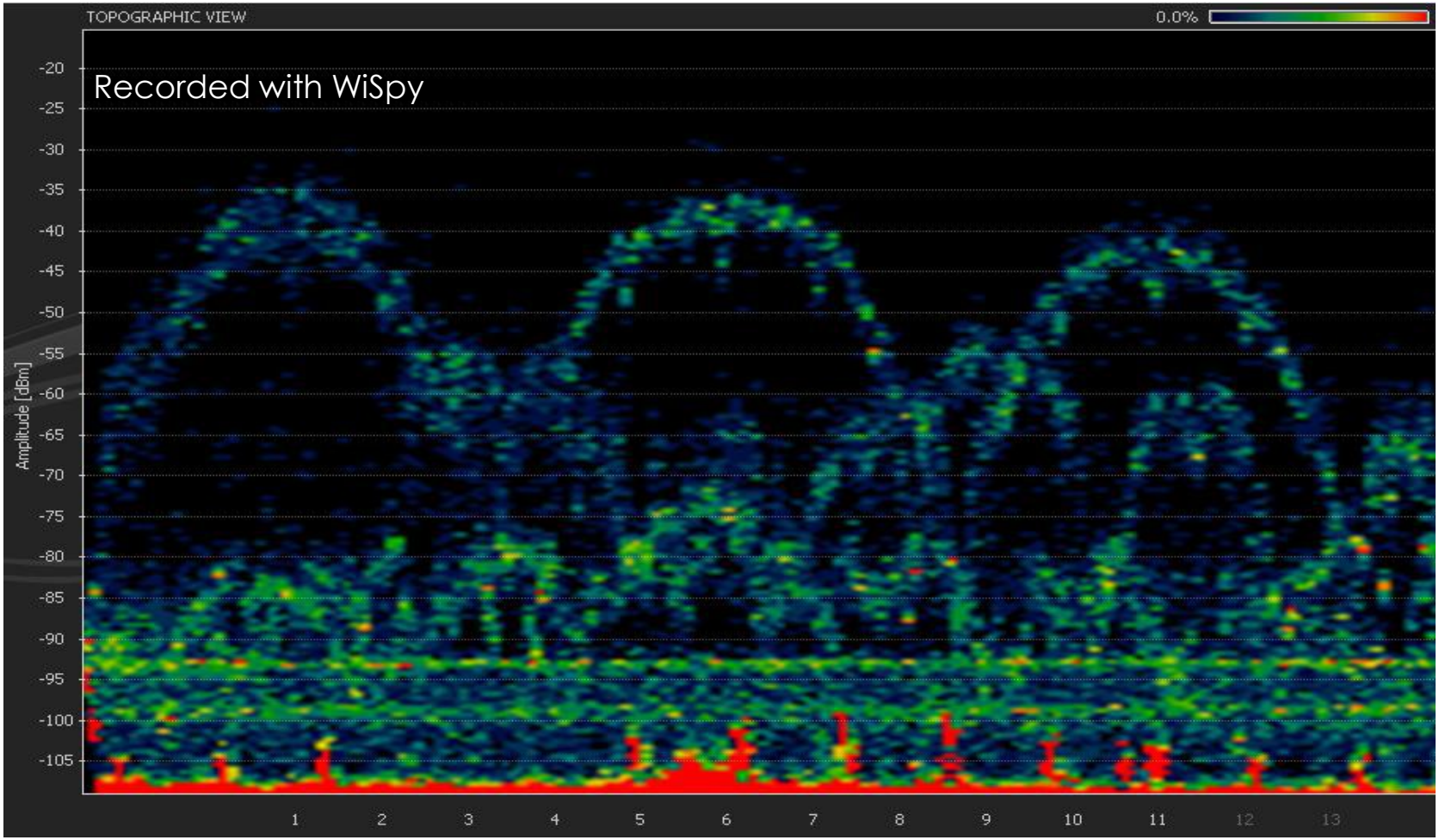
Tuning display for WLAN



802.11b/g Channel Allocation



802.11b/g Channel Allocation



WLAN Management Frames

- Beacon
- Probe request and response
- Authentication
- Deauthentication
- Association request and response
- Reassociation request and response
- Disassociation

These frames are used to establish and maintain communications within a single radio cell (channel)

WLAN Control & Data Frames

Control Frames
- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledge
- Power Save Poll

These frames control the access to the shared media

Data Frames
- Data
- Null Function

These frames transport data or are use for keep alives

WLAN Management Frames

Beacon

- Marks the presence of an Access Point (AP)
- Sent 10 times / seconds (default)
- Carries BSSID, MAC address etc. of AP
- Indicates capabilities of AP (speeds etc.)
- Indicates type and need for encryption
- Keeps mobile clients time synchronized
- Carries optional vendor specific info
- and much more

WLAN Management Frames

Probe Request / Response

- Purpose is to find an Access Point
- Probe Request are always sent by client
- Probe Requests are sent in all channels

- Access Point replies with Probe Response
- Probe Response contains same info fields like Beacon

Remark: In 'Passive Mode' no Probe Request are sent by the client, channels are scanned for Beacons (saves power)

WLAN Management Frames

Authentication

- Initially two methods definded:
  - 'Open Authentication'
  - 'Shared Key Authentication'
- Obsolete methods (unsecure)
- 802.1x Authentication' is mostly used today

Deauthentication

- Sent if a station or the Access Point wishes to terminate secure communications

WLAN Management Frames

Association Request

- A station is applying to be registered with an Access point
- A single station can only be associated with one Access Point

Association Response

- Reply from AP to confirm association

Dissassociation

- Sent to release an association

WLAN Management Frames

Reassociation Request

- Sent by a roaming station to the new Access Point
- Station lists the present Access Point in the Request as a reference

Reassociation Response

- Reply from the Access Point to confirm new association

WLAN Control Frames

Request to Send (RTS)

- Sent by a station or Access Point to reserve a time slot for transmission
- Used after a number of not acknowledged transmissions
- Used in mixed b/g/n cells and hidden node situations to prevent collisions

Clear to Send (CTS)

- Reply to confirm the requested time slot

WLAN Control Frames

Acknowledge

- Sent by a station or Access Point to confirm successful reception of a packet

Power Save Poll

- Sent by a station in sleep mode to fetch packets stored in Access Point

WLAN Data Frames

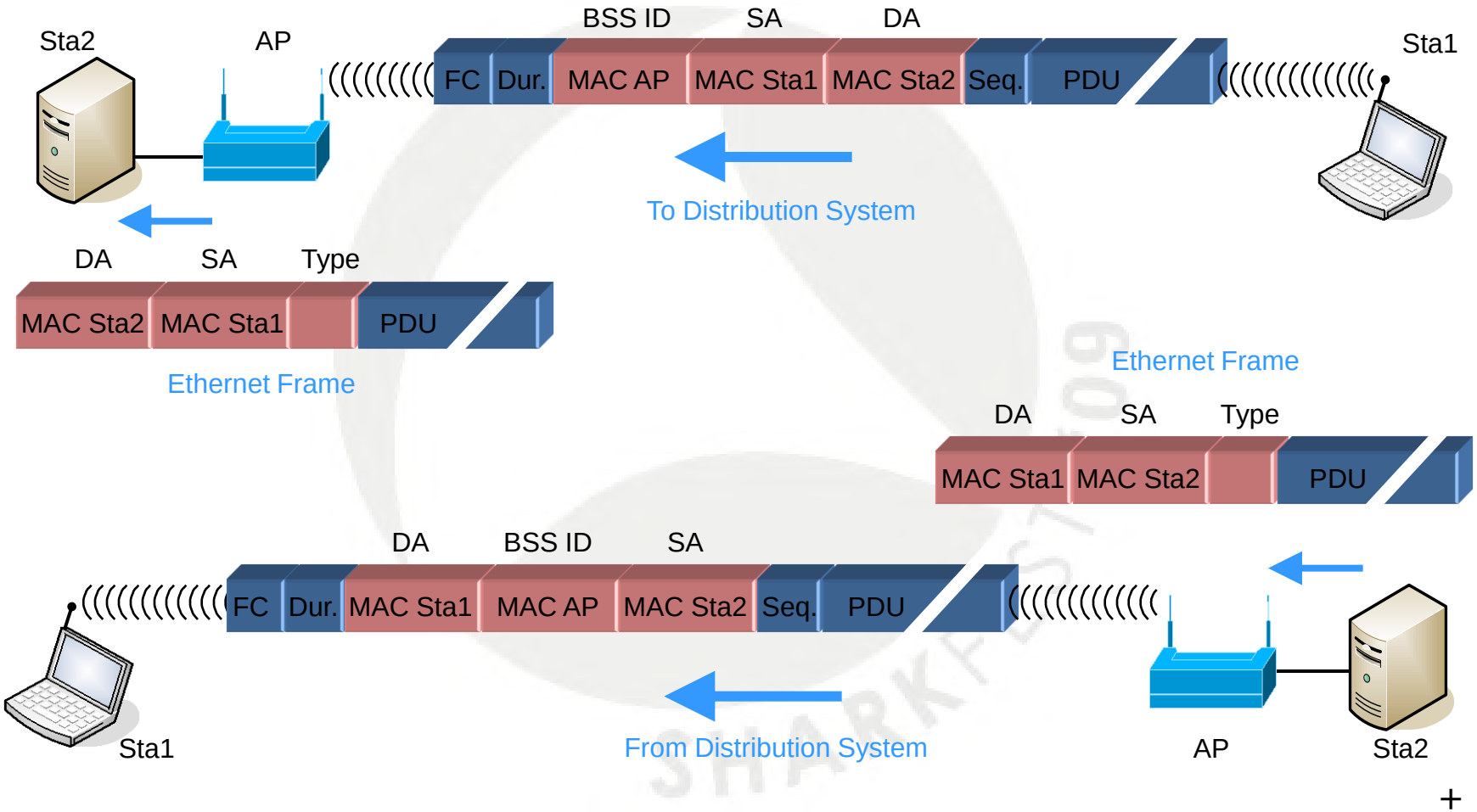
Data

- Data frames may be encrypted or in clear text
- Data frames may contain 802.11 QOS control for Voice over WLAN

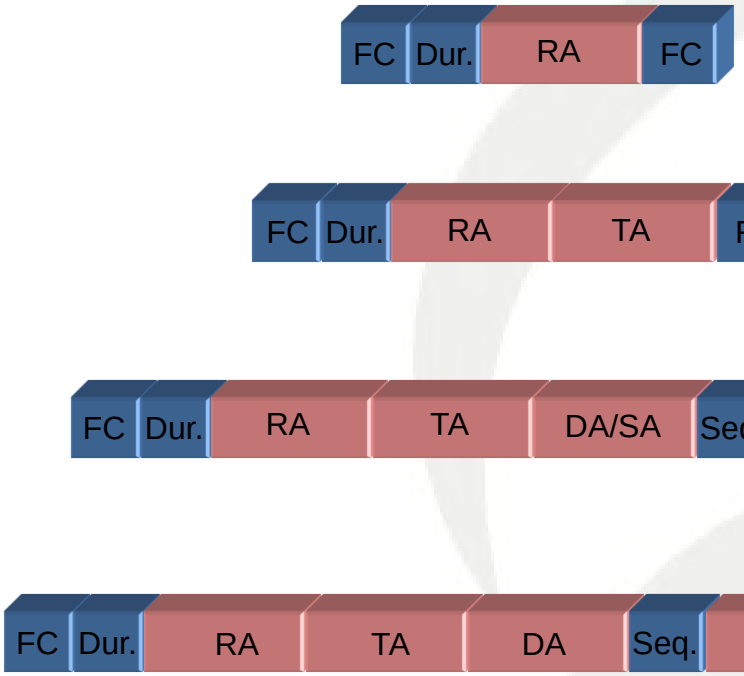
Null Function

- Data frame containing no data
- Used for keep-alives or signaling power save condition

WLAN Frame Formats



WLAN Frame Formats



Acknowledge, Clear to Send

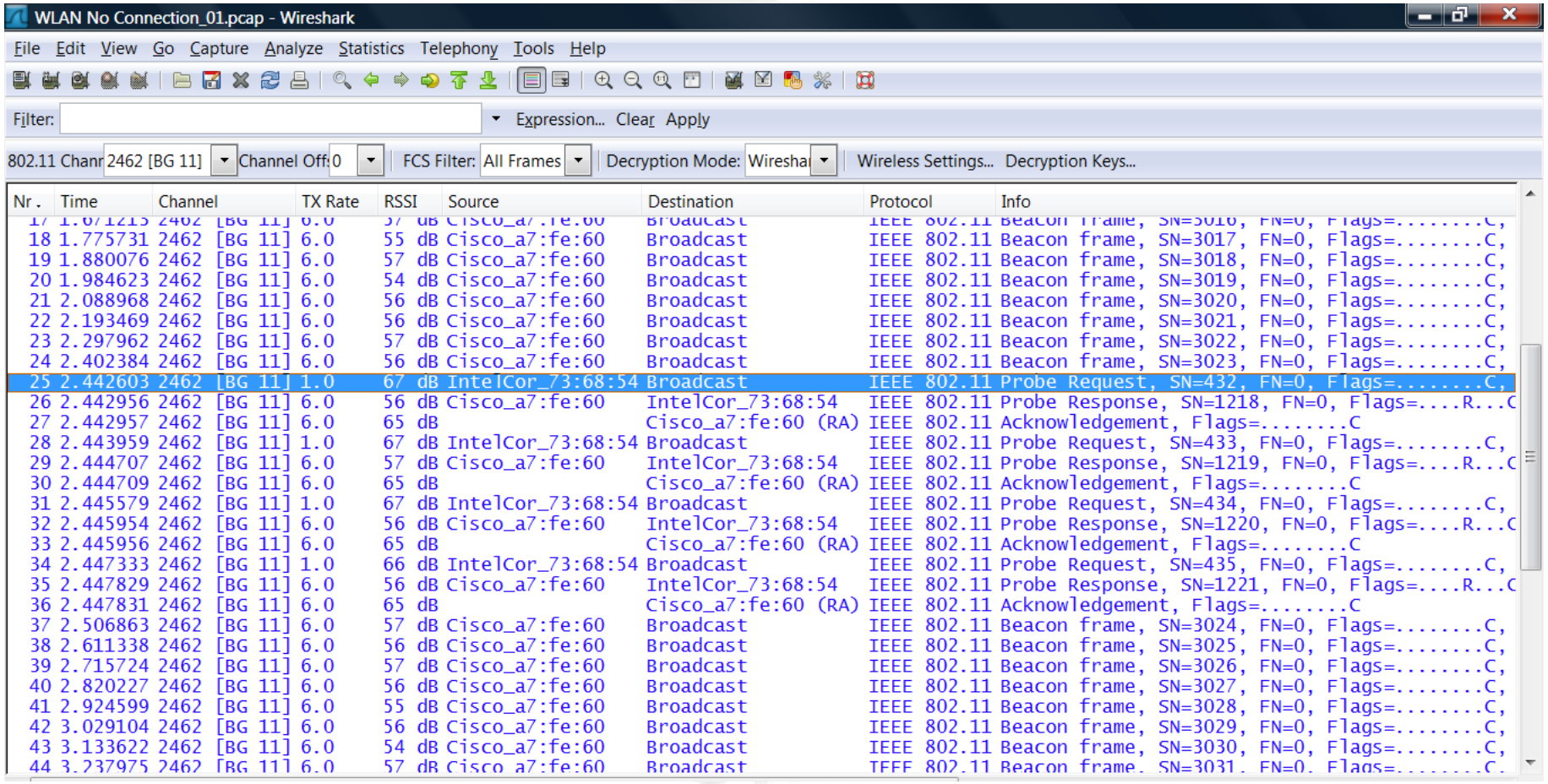
Request to Send

Data Frame, Beacon, Probe Request, Probe Response, Authentication, Deauthentication, Association, Reassociation, Disassociation

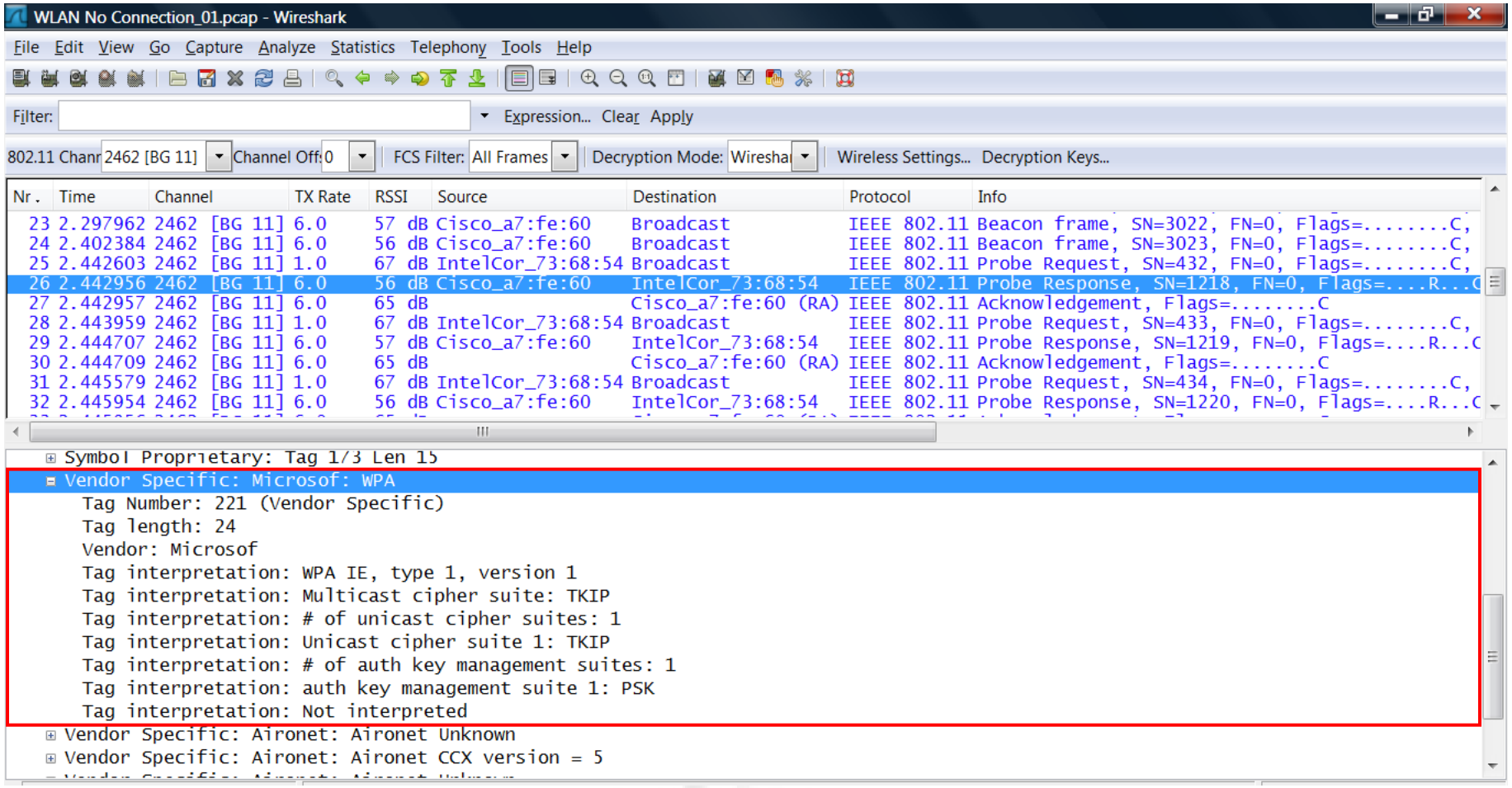
Data Frame through repeater

FC = Frame Control, Dur. = Duration, RA = Receiver Address, TA = Transmitter Address; DA = Destination Address, SA = Source Address, Seq. = Sequence, PDU = Protocol Data Unit, FC = Frame Check Sequence

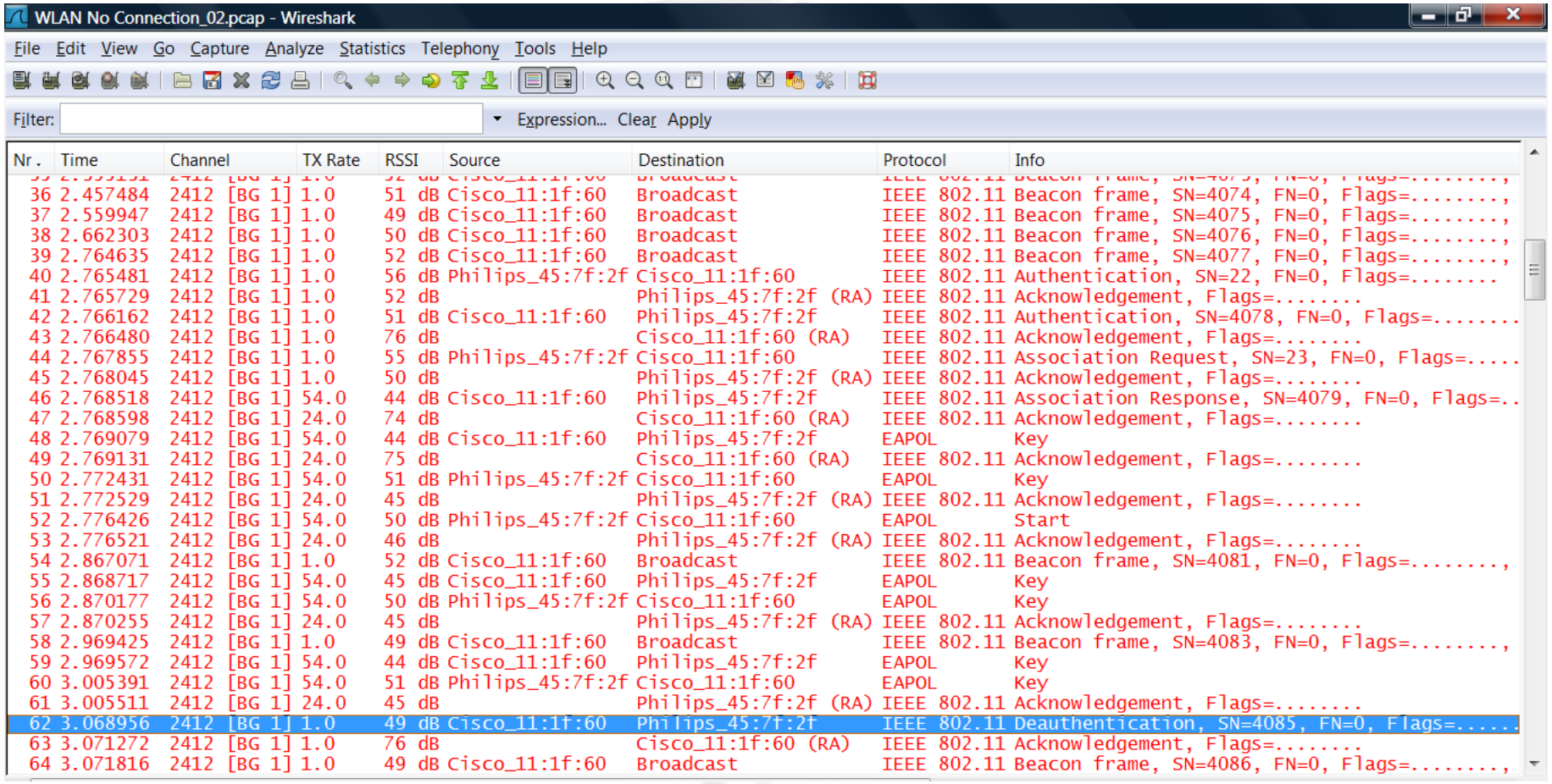
Client can not associate - Case one



Client can not associate - Case one

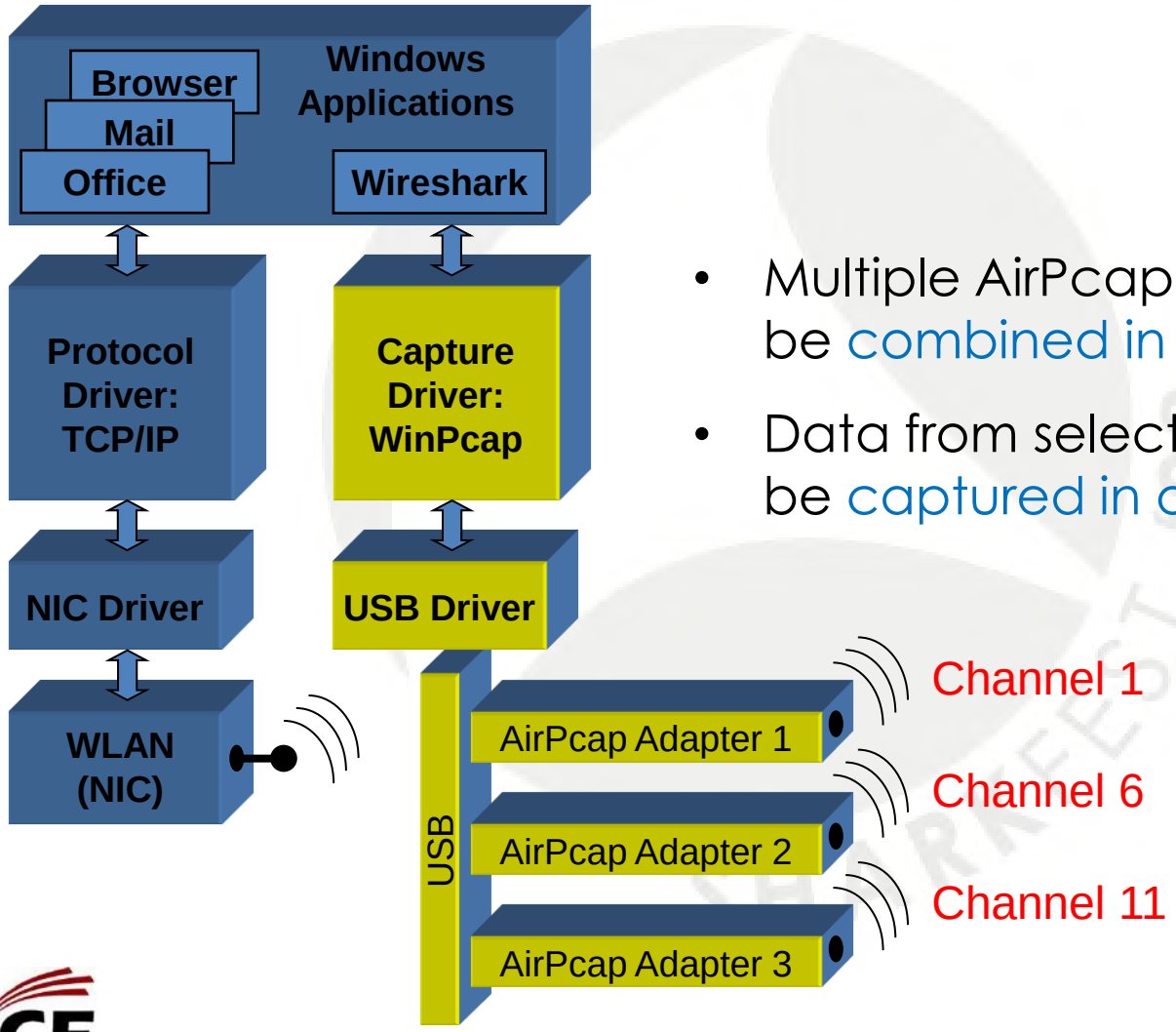


Client can not associate - Case two



Nr.	Time	Channel	TX Rate	RSSI	Source	Destination	Protocol	Info
36	2.457484	2412 [BG 1]	1.0	51 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4074, FN=0, Flags=........,
37	2.559947	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4075, FN=0, Flags=........,
38	2.662303	2412 [BG 1]	1.0	50 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4076, FN=0, Flags=........,
39	2.764635	2412 [BG 1]	1.0	52 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4077, FN=0, Flags=........,
40	2.765481	2412 [BG 1]	1.0	56 dB	Philips_45:7f:2f	Cisco_11:1f:60	IEEE 802.11	Authentication, SN=22, FN=0, Flags=........
41	2.765729	2412 [BG 1]	1.0	52 dB		Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=........
42	2.766162	2412 [BG 1]	1.0	51 dB	Cisco_11:1f:60	Philips_45:7f:2f	IEEE 802.11	Authentication, SN=4078, FN=0, Flags=........
43	2.766480	2412 [BG 1]	1.0	76 dB		Cisco_11:1f:60 (RA)	IEEE 802.11	Acknowledgement, Flags=........
44	2.767855	2412 [BG 1]	1.0	55 dB	Philips_45:7f:2f	Cisco_11:1f:60	IEEE 802.11	Association Request, SN=23, FN=0, Flags=.....
45	2.768045	2412 [BG 1]	1.0	50 dB		Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=........
46	2.768518	2412 [BG 1]	54.0	44 dB	Cisco_11:1f:60	Philips_45:7f:2f	IEEE 802.11	Association Response, SN=4079, FN=0, Flags=..
47	2.768598	2412 [BG 1]	24.0	74 dB		Cisco_11:1f:60 (RA)	IEEE 802.11	Acknowledgement, Flags=........
48	2.769079	2412 [BG 1]	54.0	44 dB	Cisco_11:1f:60	Philips_45:7f:2f	EAPOL	Key
49	2.769131	2412 [BG 1]	24.0	75 dB		Cisco_11:1f:60 (RA)	IEEE 802.11	Acknowledgement, Flags=........
50	2.772431	2412 [BG 1]	54.0	51 dB	Philips_45:7f:2f	Cisco_11:1f:60	EAPOL	Key
51	2.772529	2412 [BG 1]	24.0	45 dB		Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=........
52	2.776426	2412 [BG 1]	54.0	50 dB	Philips_45:7f:2f	Cisco_11:1f:60	EAPOL	Start
53	2.776521	2412 [BG 1]	24.0	46 dB		Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=........
54	2.867071	2412 [BG 1]	1.0	52 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4081, FN=0, Flags=........,
55	2.868717	2412 [BG 1]	54.0	45 dB	Cisco_11:1f:60	Philips_45:7f:2f	EAPOL	Key
56	2.870177	2412 [BG 1]	54.0	50 dB	Philips_45:7f:2f	Cisco_11:1f:60	EAPOL	Key
57	2.870255	2412 [BG 1]	24.0	45 dB		Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=........
58	2.969425	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4083, FN=0, Flags=........,
59	2.969572	2412 [BG 1]	54.0	44 dB	Cisco_11:1f:60	Philips_45:7f:2f	EAPOL	Key
60	3.005391	2412 [BG 1]	54.0	51 dB	Philips_45:7f:2f	Cisco_11:1f:60	EAPOL	Key
61	3.005511	2412 [BG 1]	24.0	45 dB		Philips_45:7f:2f (RA)	IEEE 802.11	Acknowledgement, Flags=........
62	3.068956	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Philips_45:7f:2f	IEEE 802.11	Deauthentication, SN=4085, FN=0, Flags=.....
63	3.071272	2412 [BG 1]	1.0	76 dB		Cisco_11:1f:60 (RA)	IEEE 802.11	Acknowledgement, Flags=........
64	3.071816	2412 [BG 1]	1.0	49 dB	Cisco_11:1f:60	Broadcast	IEEE 802.11	Beacon frame, SN=4086, FN=0, Flags=........,

Analyzing Roaming Problems



- Multiple AirPcap adapters can be combined in one logical I/F
- Data from selected channels will be captured in one trace file

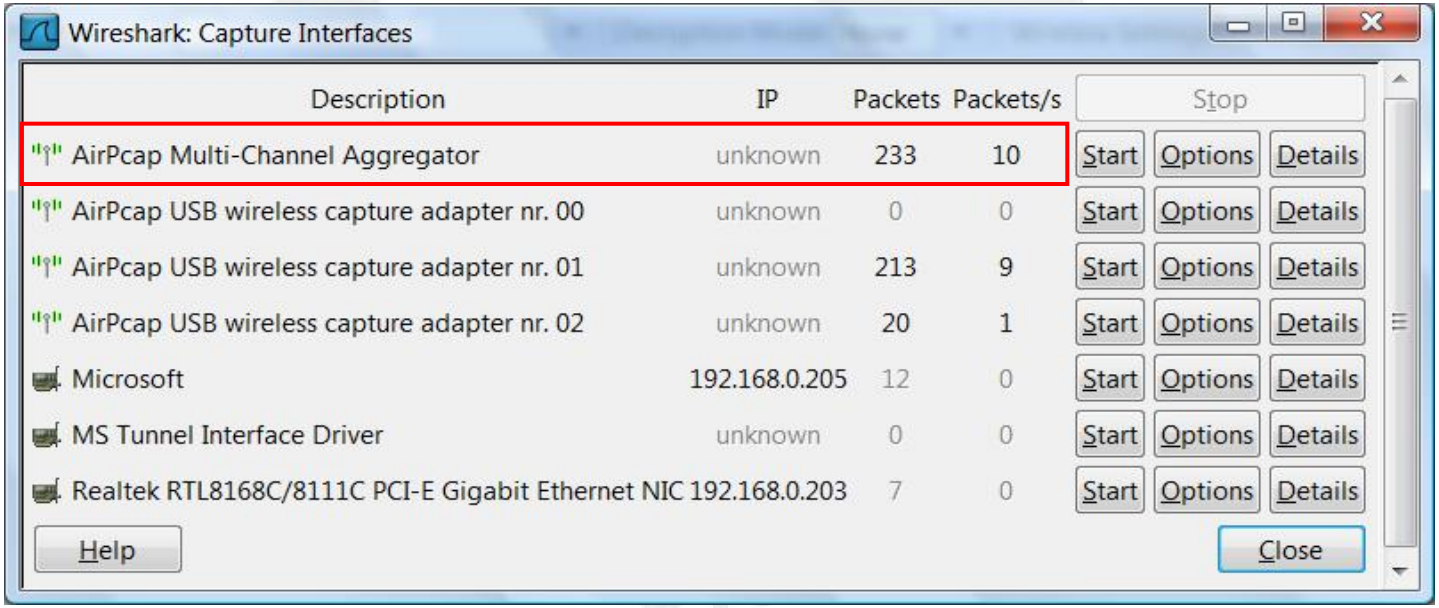
Analyzing Roaming Problems

- Mounting USB hub and AirPcap adapters on a notebook gives you a mobile solution to capture roaming processes

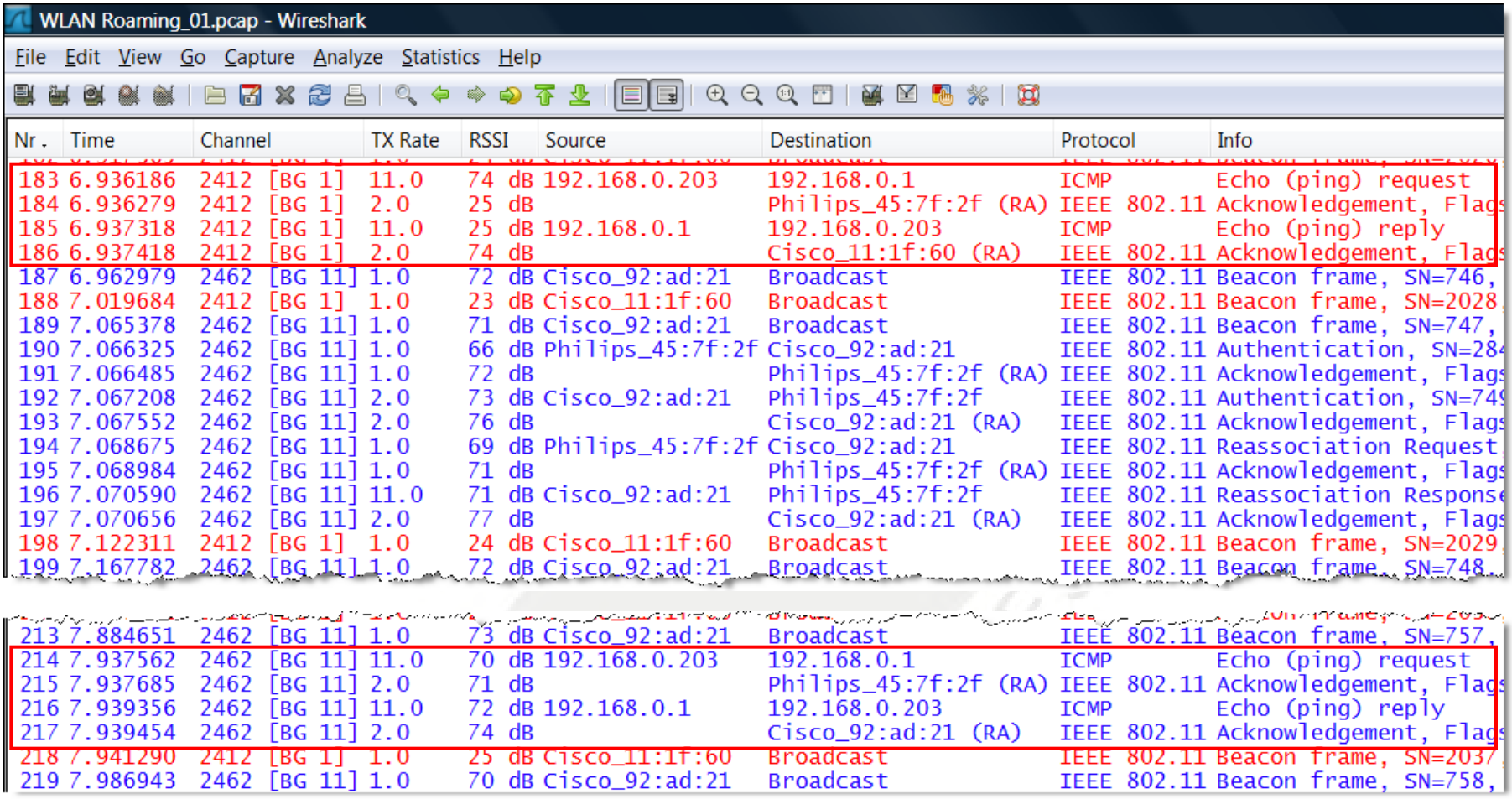
- Roaming problems are quite complex to analyze
- In order to capture the roaming event, you have to follow the roaming client as close as possible
- Set a display filter to BEACONs and MAC address of roaming client

Combining multiple Airpcap adapters

- More than one AirPcap adapter will be automatically combined in the AirPcap Multi-Channel Aggregator
- Channel numbers must be configured individually on each adapter



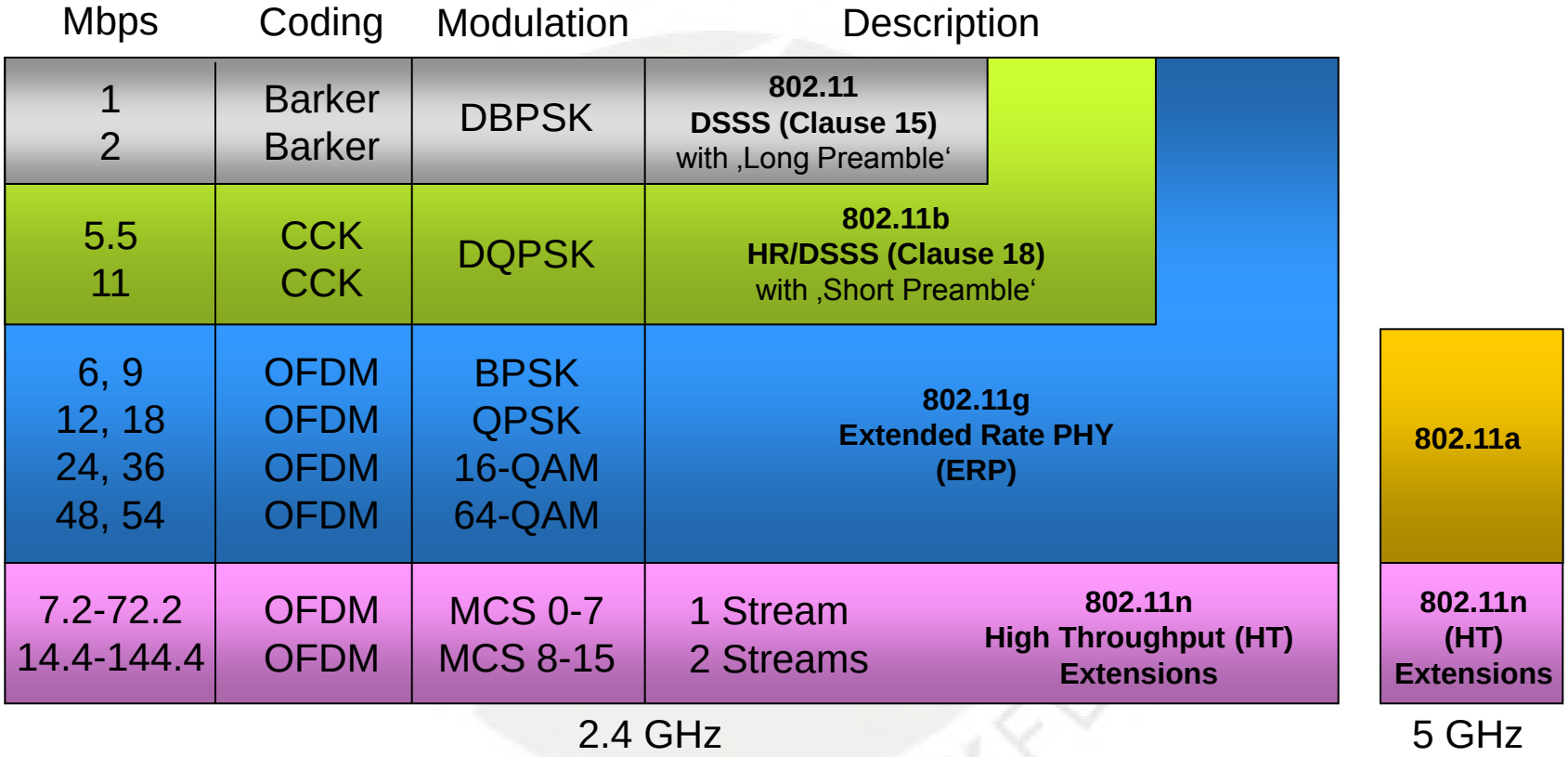
Roaming Client



Throughput Analysis

- Throughput will always be an issue in WLANs
- A radio cell is a shared media with half duplex conversation
- Indicated throughput (i.e. 54Mbps) are maximum values and are only achieved under optimal conditions
- Data throughput is around 50% of cell throughput
- Presence of old 802.11b-only client will reduce cell throughput significantly

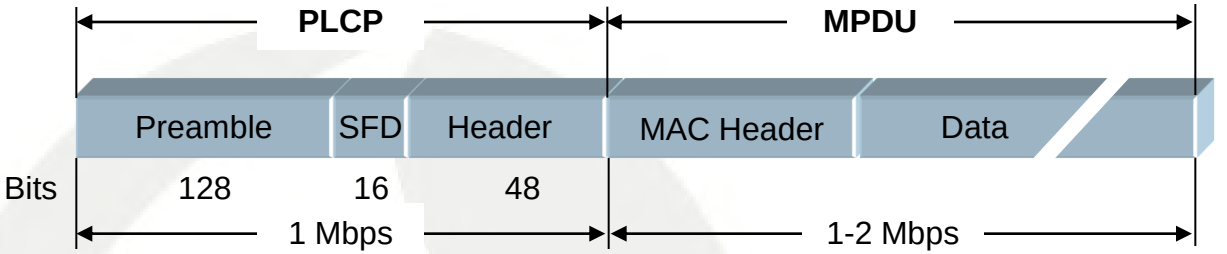
Overview WLAN Standards



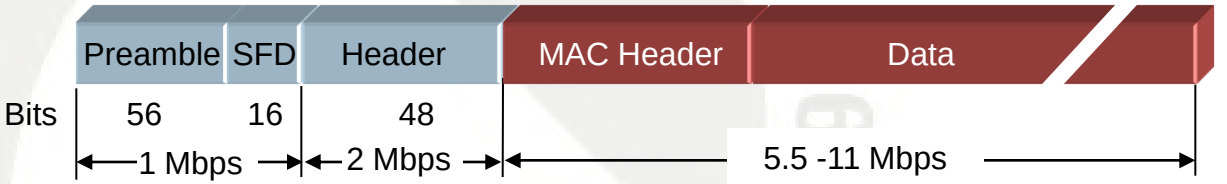
CCK = Complementary Code Keying
DBPSK = Differential Binary Phase-Shift Keying
DQPSK = Differential Quadrature Phase-Shift Keying
OFDM = Orthogonal Frequency Division Multiplexing
BPSK = Binary Phase-Shift Keying
QPSK = Quadrature Phase-Shift Keying
QAM = Quadrature Amplitude Modul.
MCS = Modulation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

Overview Frame Types (2.4 GHz)

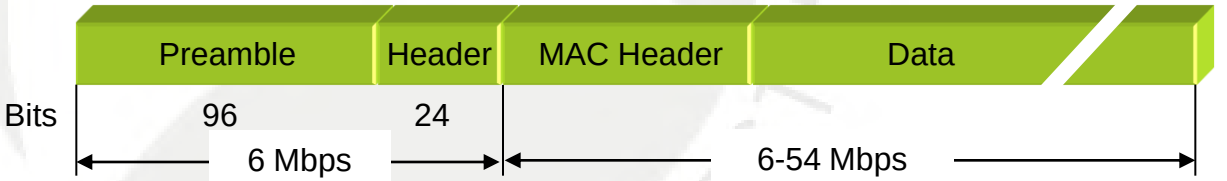
802.11 DSSS with
‚Long Preamble'
Barker Code



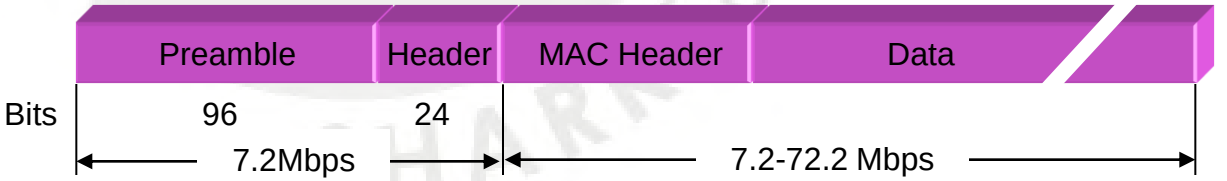
802.11b HR/DSSS with
‚Short Preamble'
Barker / CCK



802.11g (ERP)
Extended Rate PHY
OFDM

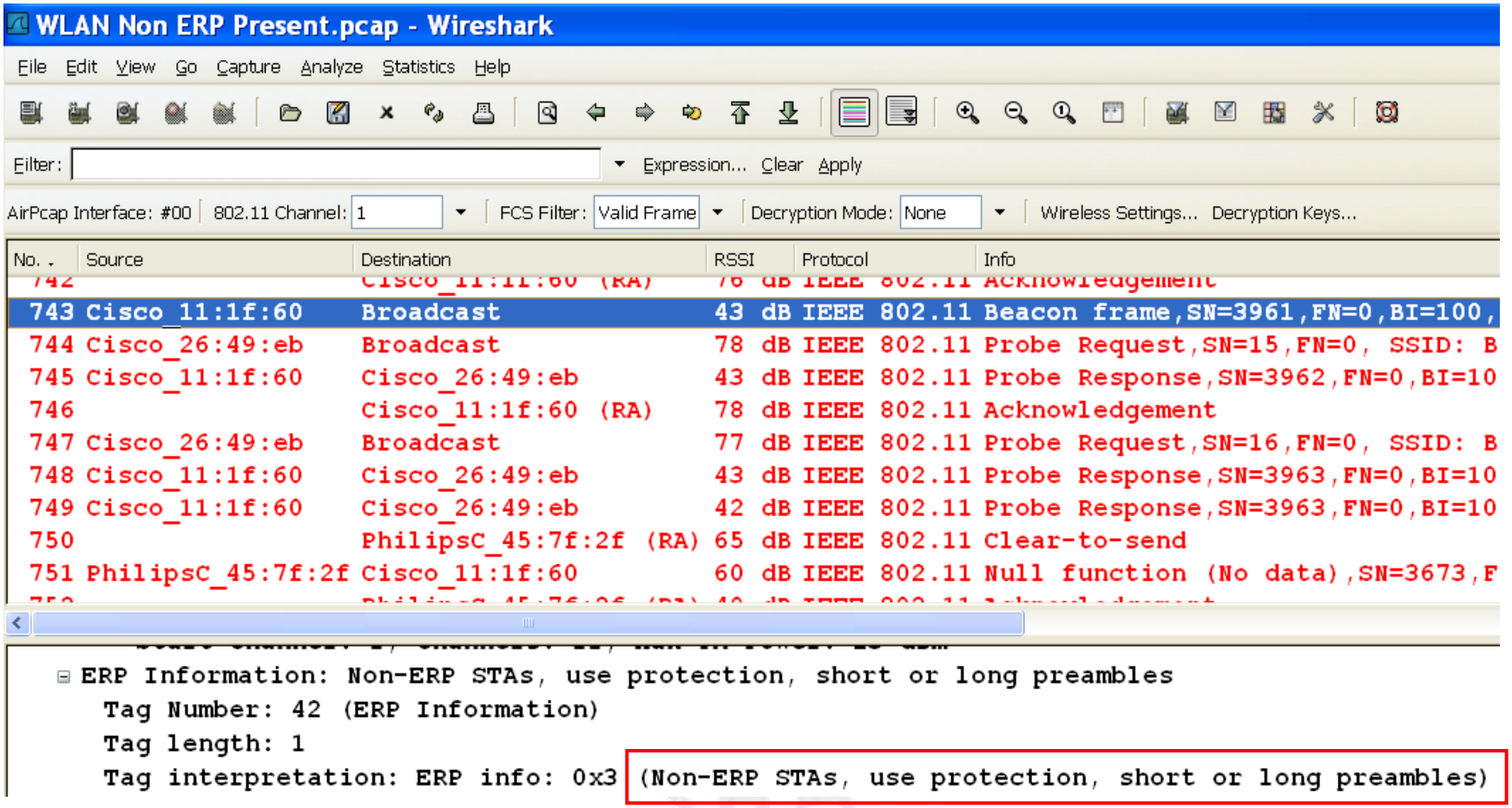


802.11n (HT)
High Throughput
extended OFDM

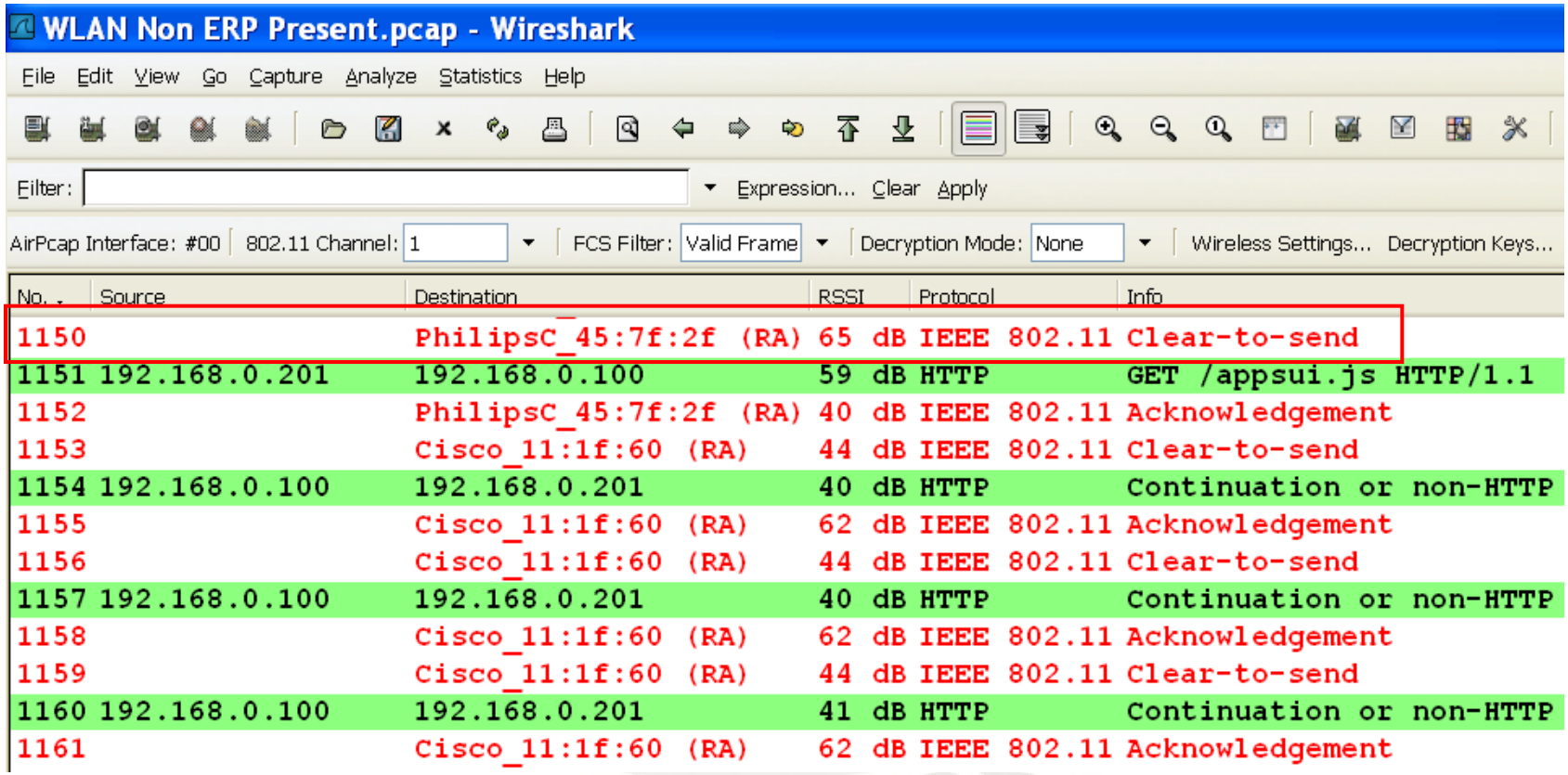


PLCP = Physical Layer Convergence Protocol
MPDU = MAC Layer Protocol Data Unit

Throughput Analysis



Throughput Analysis



OFDM (ERP) stations are sending control frames **‚Clear-to send to self'** (CTS-to-self) before each data frame to reserve time slot

Throughput Analysis

- Reduced data throughput in mixed environment

	Data Rate (Mbps)	Approximate Throughput (Mbps)	Throughput as a Percentage of 802.11b Throughput
802.11b	11	6	100%
802.11g—with 802.11b clients in cell (CTS/RTS)	54	8	133%
802.11g—with 802.11b clients in cell (CTS-to-self)	54	13	217%
802.11g (no 802.11b clients in cell)	54	22	367%
802.11a	54	25	417%

Source: Cisco Systems

Throughput improvement:
Upgrade of all 802.11b stations to 802.11g

Channel Allocation 5 GHz Band

Frequency Band	Channel ID	FCC (GHz)	ETSI (GHz)	MKK (GHz)
Lower Band UNII-1	34	--	--	5.170
	36	5.180	5.180	--
	38	--	--	5.190
	40	5.200	5.200	--
	42	--	--	5.210
	44	5.220	5.220	--
	46	--	--	5.230
	48	5.240	5.240	--
Middle Band UNII-2	52	5.260*	5.260	5.260
	56	5.280*	5.280	5.280
	60	5.300*	5.300	5.300
	64	5.320*	5.320	5.320
High Band UNII-2 extended	100	5.500*	5.500	5.500
	104	5.520*	5.520	5.520
	108	5.540*	5.540	5.540
	112	5.560*	5.560	5.560
	116	5.580*	5.580	5.580
	120	5.600*	5.600	5.600
	124	5.620*	5.620	5.620
	128	5.640*	5.640	5.640
	132	5.660*	5.660	5.660
	136	5.680*	5.680	5.680
	140	5.700*	5.700	5.700
Upper Band UNII-3/ISM	149	5.745	--	--
	153	5.765	--	--
	157	5.785	--	--
	161	5.805	--	--
ISM	165	5.825	--	--

Available non-overlapping channels	
FCC (USA and Canada)	24
ETSI (Europe)	19
MKK (Japan)	19

Transmit Power Control (TPC) required for	
FCC (USA and Canada)	Band 2,2e
ETSI (Europe)	Band 1,2,2e
MKK (Japan)	Band 1,2,2e

Dynamic Frequency Selection (DFS) required for	
FCC* (USA and Canada)	Band 2,2e
ETSI (Europe)	Band 1,2,2e
MKK (Japan)	Band 1,2,2e

Some channels only allowed for inhouse use

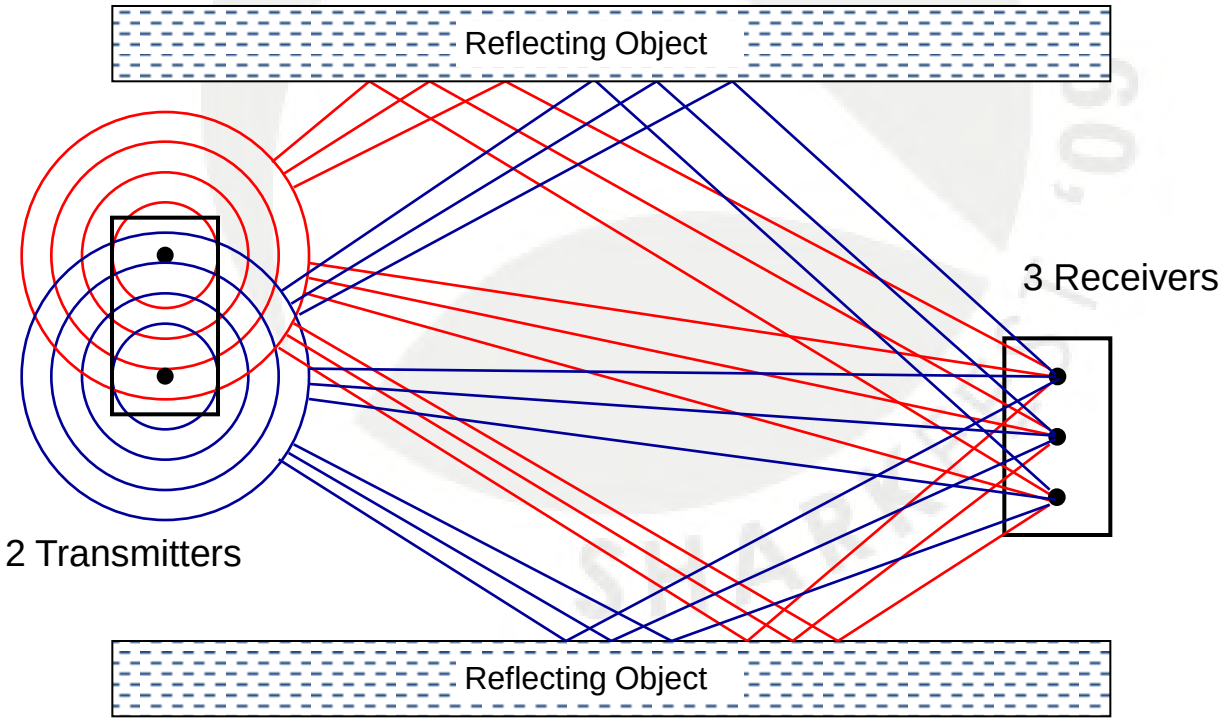
*New stricter FCC DFS2 rules valid off July 20, 2007

Multiple-Input, Multiple-Output (MIMO)

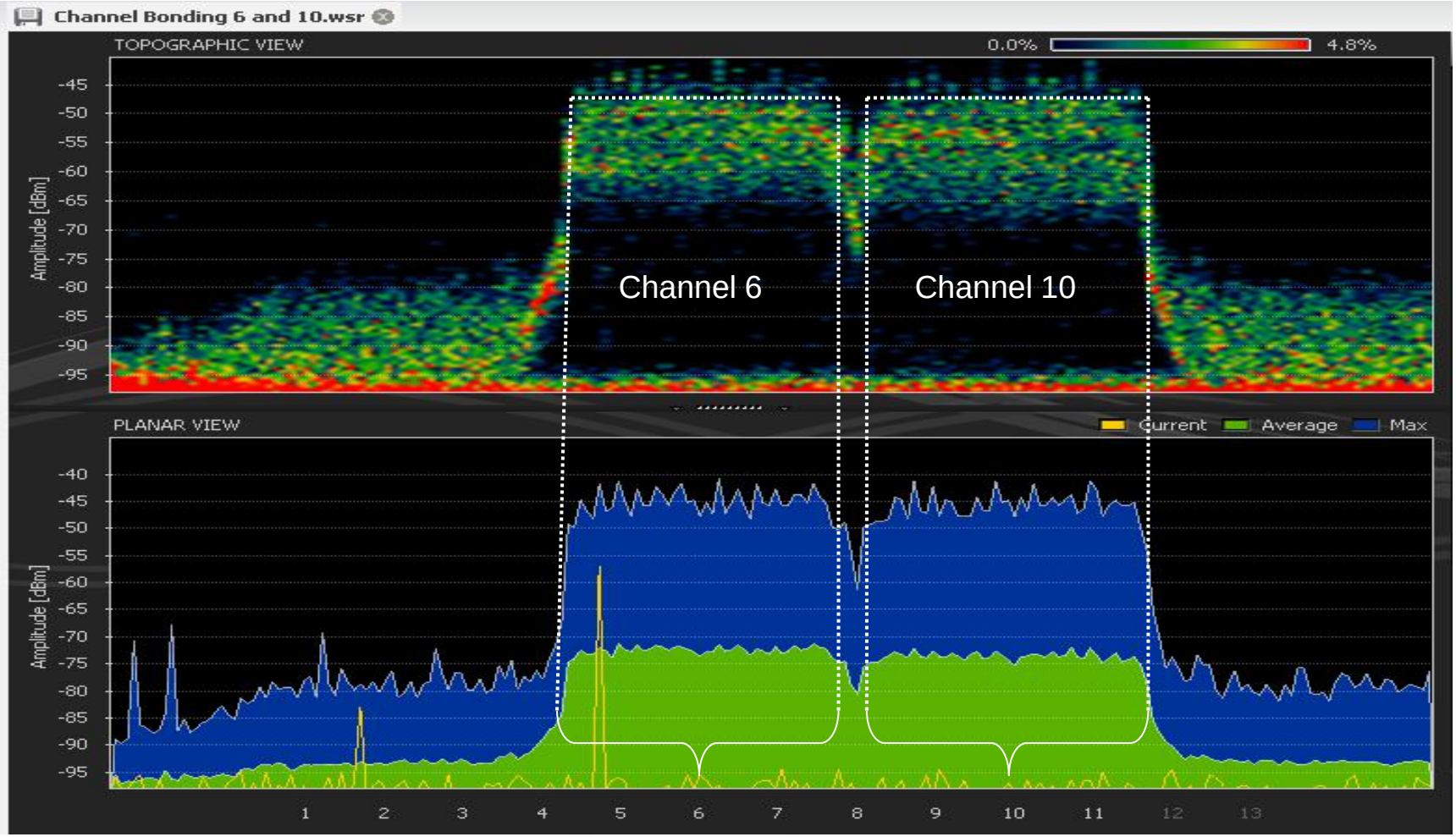
- 802.11n introduces lots of new WLAN technologies
- Physical layer improvements with new ODFM
- MIMO supports multiple streams within one channel
- Channel bonding combines two adjacent channels
- Frame aggregation allows large frames or streaming packets
- Block acknowledges replaces ping pong procedure
- With two streams and two channels up to 300 Mbps
- Future product will support four streams and up to 600 Mbps

Multiple Streams (Spatial Multiplexing)

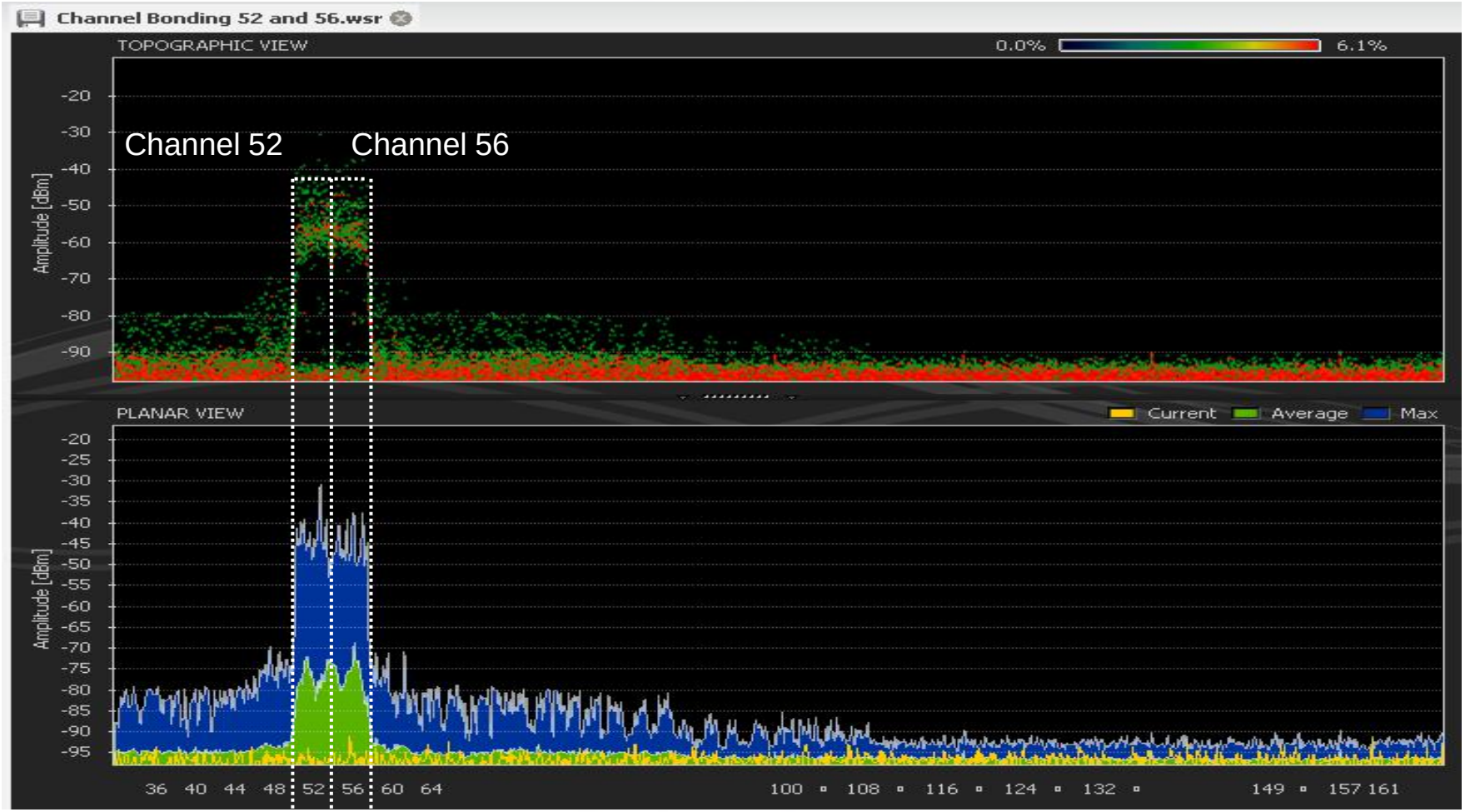
- A signal stream is broken down into multiple signal streams, each is transmitted from a different antenna.
- Each of these "spatial" streams arrives at the receiver with different amplitude (signal strength) and phase.



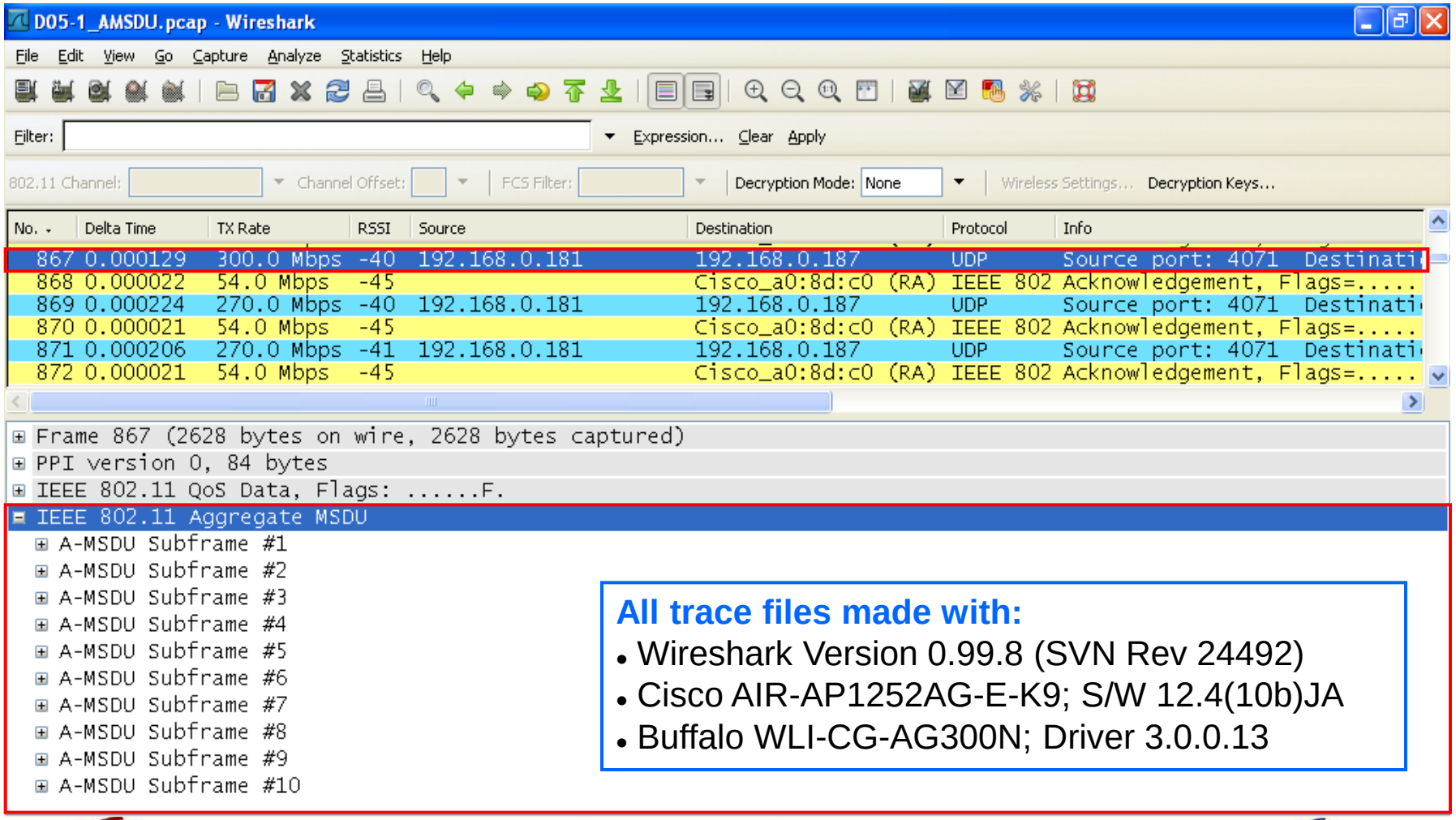
Channel Bonding 2.4 GHz Band



Channel Bonding 5 GHz Band



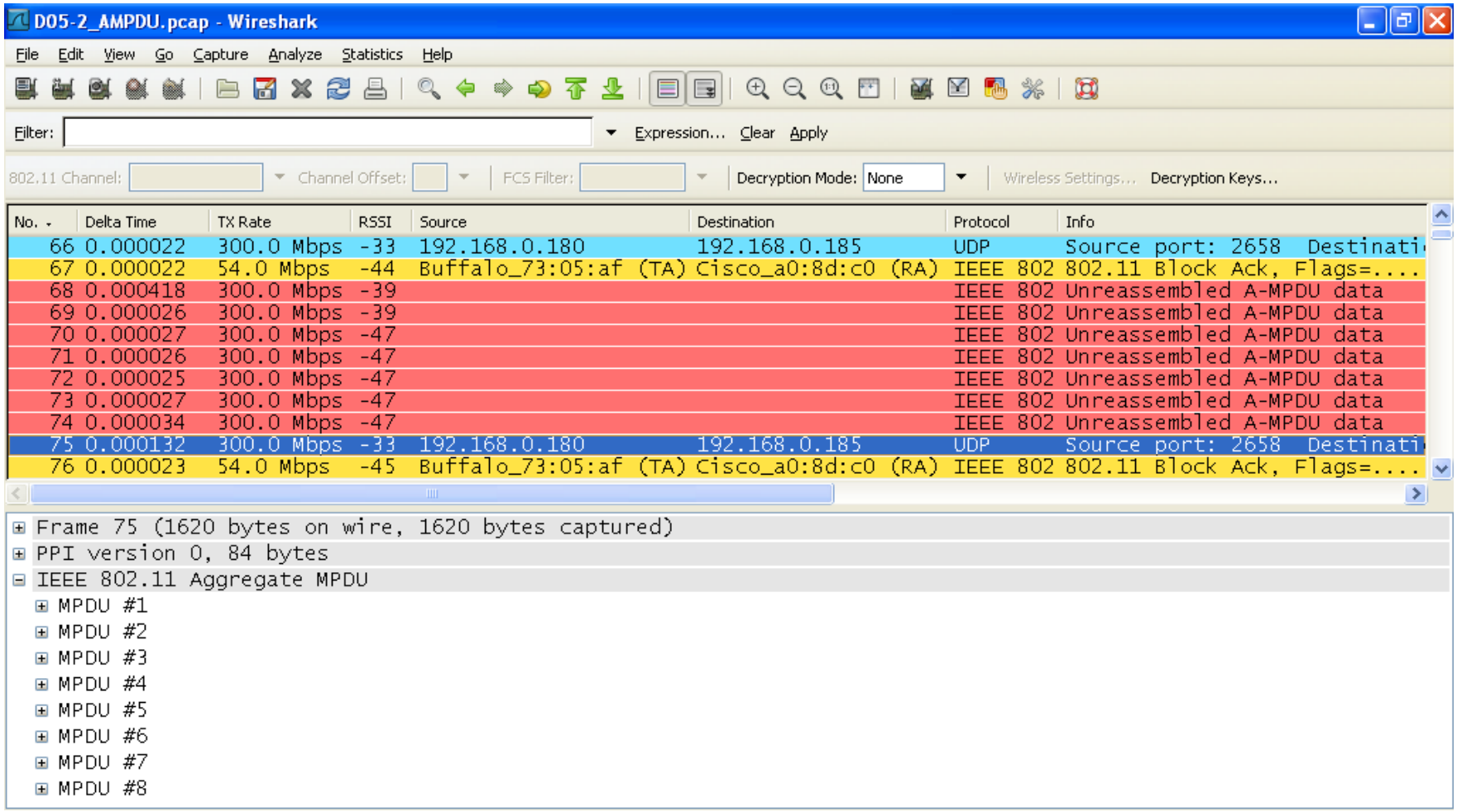
Aggregate-MAC Service Data Unit (A-MSDU)



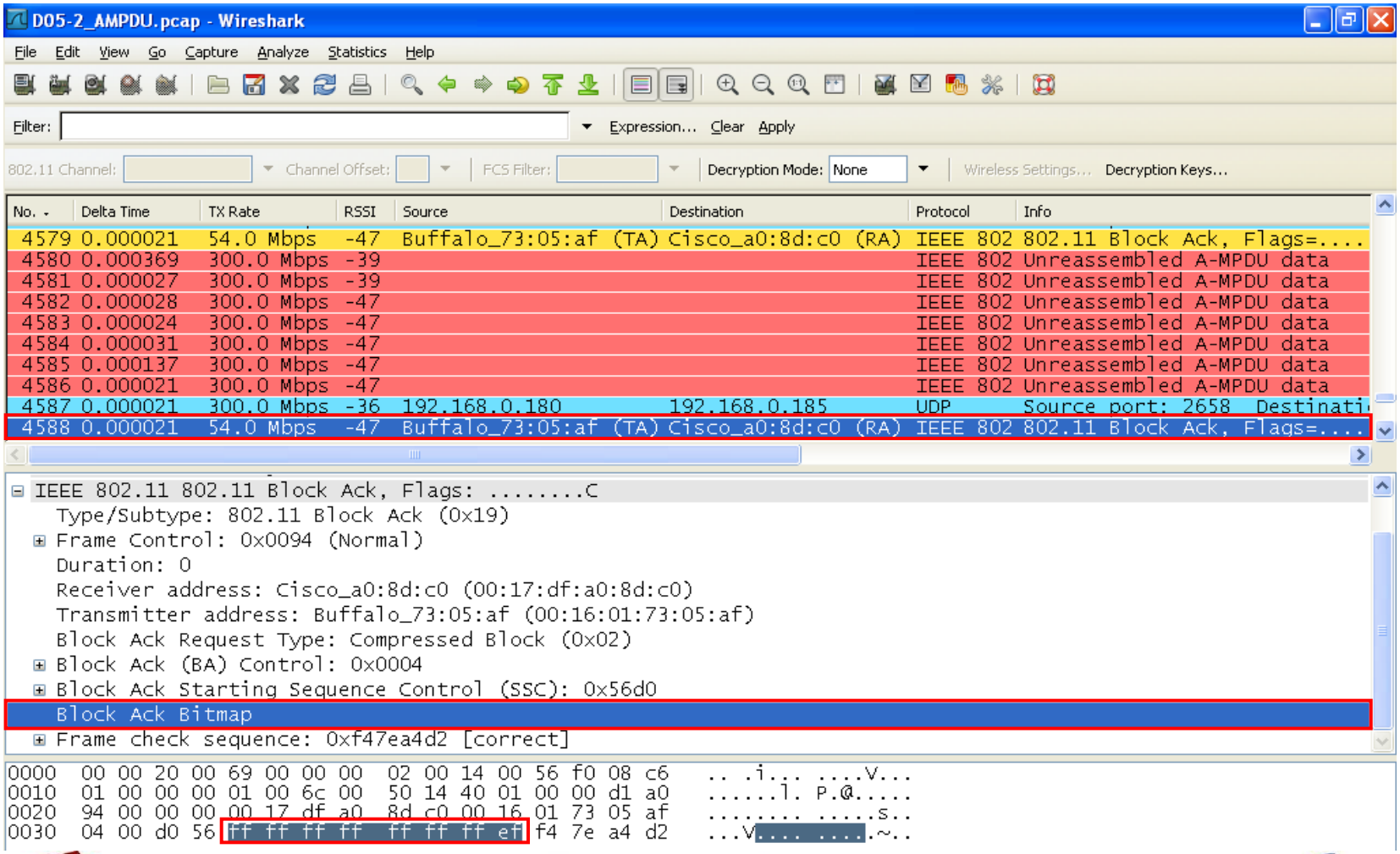
All trace files made with:

- Wireshark Version 0.99.8 (SVN Rev 24492)
- Cisco AIR-AP1252AG-E-K9; S/W 12.4(10b)JA
- Buffalo WLI-CG-AG300N; Driver 3.0.0.13

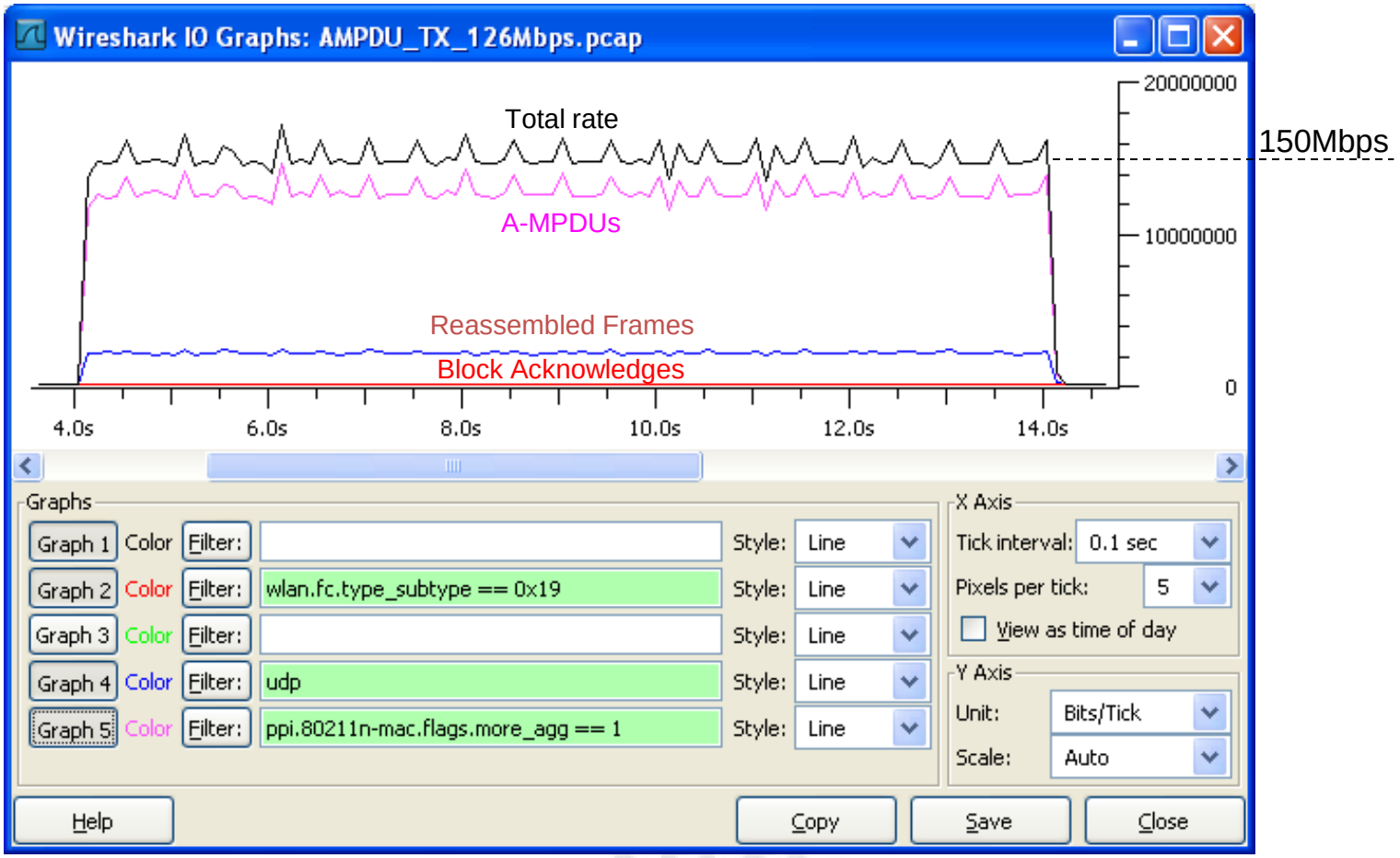
Aggregate-MAC Protocol Data Unit (A-MPDU)



Block Acknowledges



802.11n Throughput analysis



UDP bandwidth measurement with **IPerf** indicates throughput of 126Mbps

Thank you for your attention

Please fill in the evals

Trace files are available on request from:

Rolf Leutert
Leutert NetServices
leutert@wireshark.ch