Wireless Sniffer

presented by
Rolf Leutert
Leutert NetServices

Ethereal ®

- Ethereal is a packet and protocol analyser for wired networks
- It decodes up to different 800 protocols
- It is freely available as open source and was released under the GNU General Public License
- It runs on all popular computing platforms, including Unix, Linux and Windows

Ethereal is registered trademark of Network Integration Services (NIS)

Ethereal ®

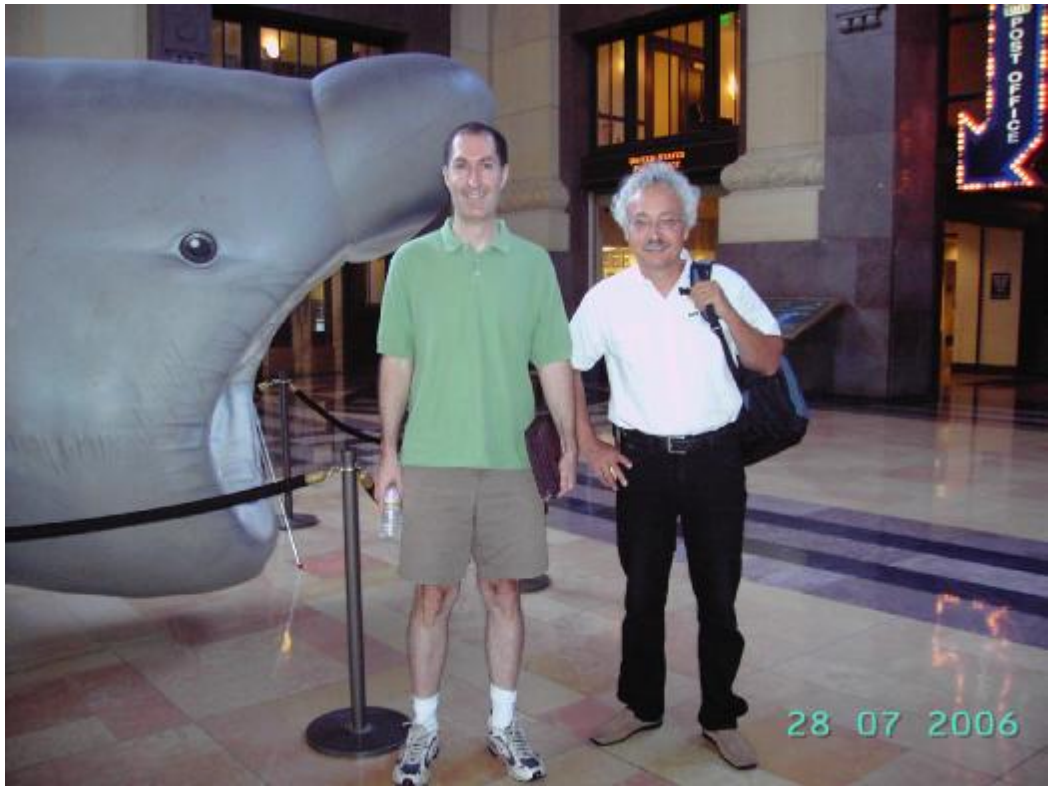
- The Ethereal project has been initiated in 1997 by Gerald Combs in Kansas City
- Gerald has found the name Ethereal in the dictionary – it stands for ‚from heaven‘
- In the meantime, more than 500 developers worldwide contributed to its programming protocol decoders (so called dissectors)
- Ethereal has been nominated as #1 packet sniffing tool by Insecure.org in June 2006 (http://sectools.org/sniffers.html)
- Q: What has Ethereal to do with Wireshark?

- A: Ethereal **is now** Wireshark
- Gerald Combs has changed his employer in 2006 and had to choose a new name for the project: Wireshark
- All developers worldwide have joined the new project and are supporting Wireshark
- Gerald Combs is now working with CACE Technologies, known as the developer of WinPcap driver

Wireshark name and logo are registered by Gerald Combs

„Sniffing problems a mile away“

is Gerald Combs‘ new slogan for Wireshark



Gerald Combs (left) und Rolf Leutert, July 2006 in Kansas City / USA

CACE TECHNOLOGIES

www.cacetech.com

- October 2006: CACE released the AirPcap
- AirPcap is the first open, affordable and easy to deploy WLAN (802.11b/g) packet capture solution for the Windows platform
- AirPcap comes as a USB 2.0 adapter, and it's been fully integrated with WinPcap and Wireshark
- AirPcap enables you to capture and analyze 802.11b/g wireless traffic, in-cluding control frames, management frames and power information

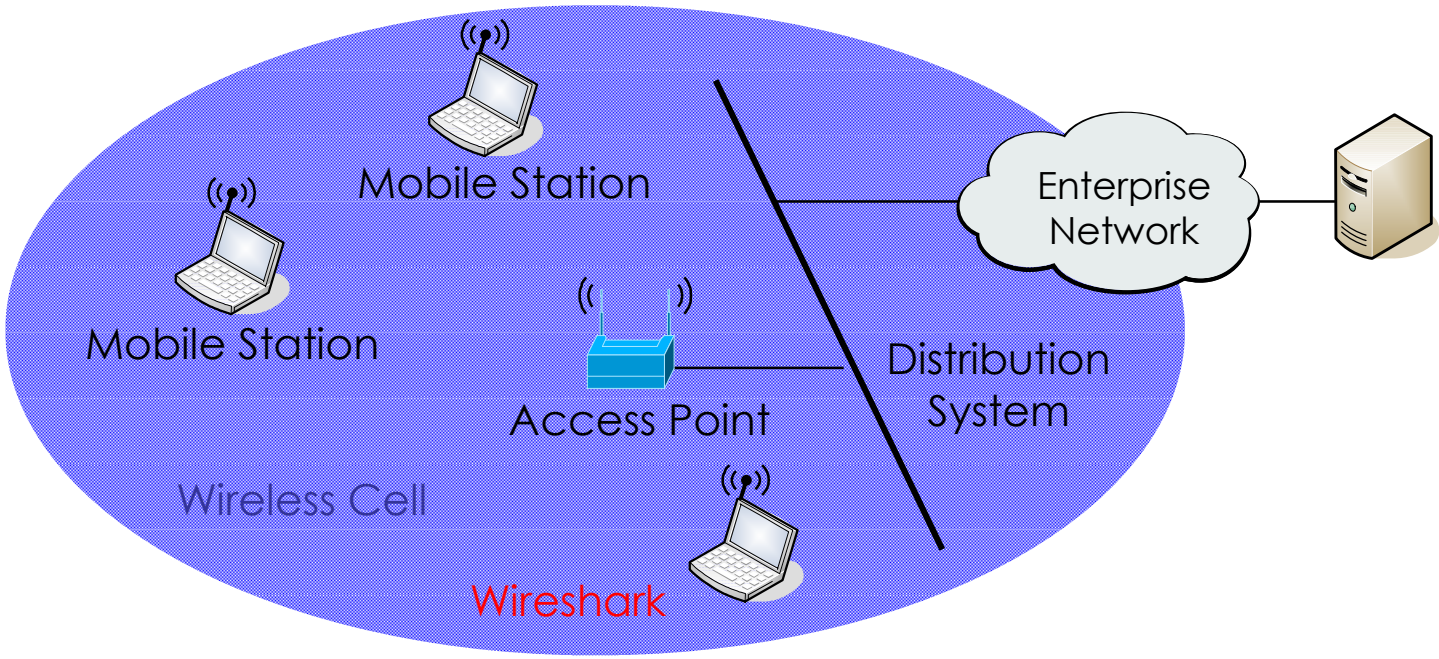
Why am I telling you this?

- Because you are responsible for the function, security and performance of your customers` wireless networks
- Because you can get a full function wire and wireless sniffer with expert knowledge at very low cost
- Because with Wireshark and AirPcap you can turn an ordinary notebook into a full function protocol analyser
- Because the first training worldwide with Wireshark and AirPcap is offered in Switzerland

Let me show you some highlights:

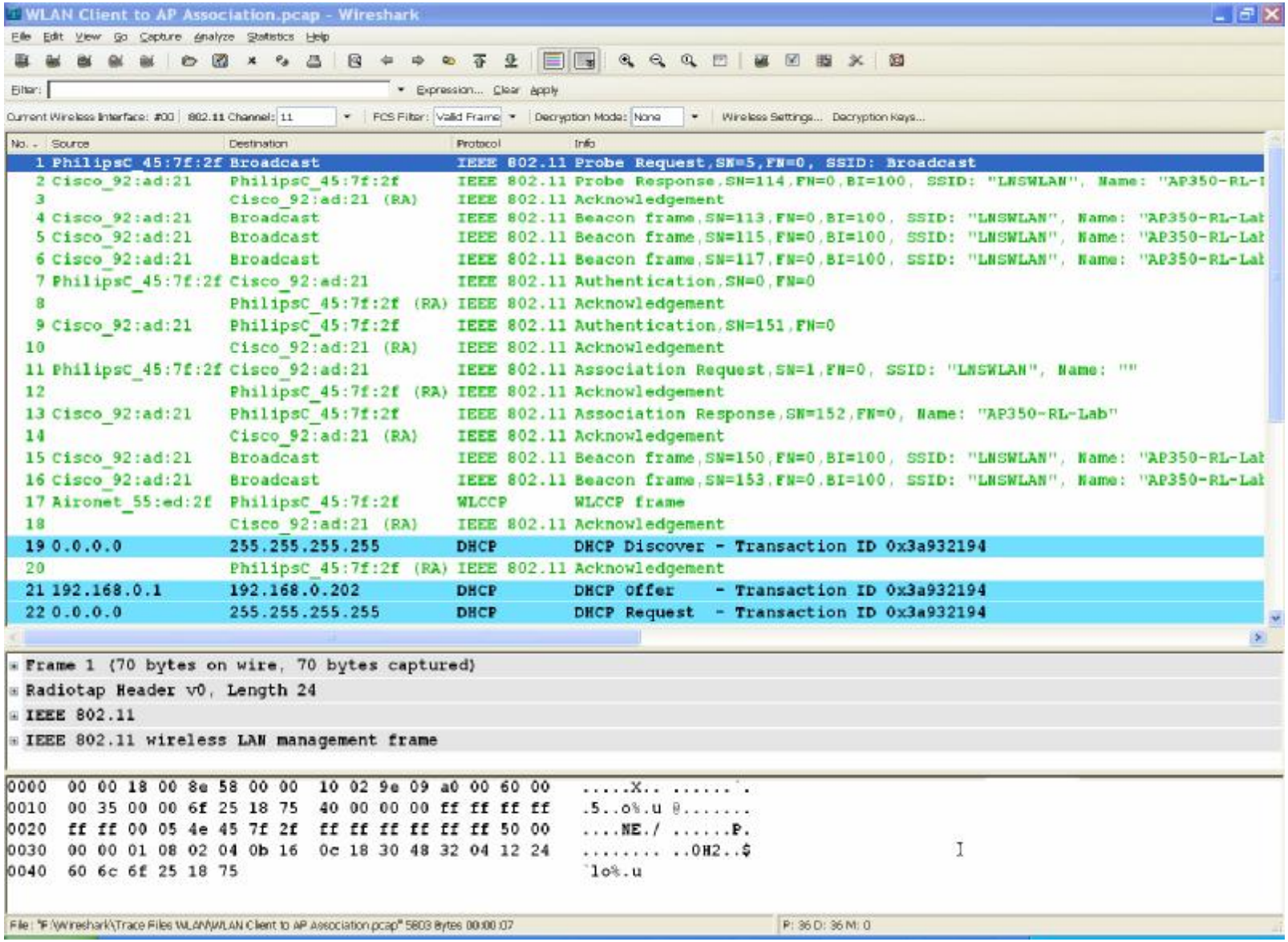
- Analysing management and control frames
- Analysing roaming problems
- Analysing performance problems in mixed 802.11b and g environment
- Analysing security issues
- Analysing VoIP Protocols
- Wireshark TCP/IP expert system

Analysing management and control frames

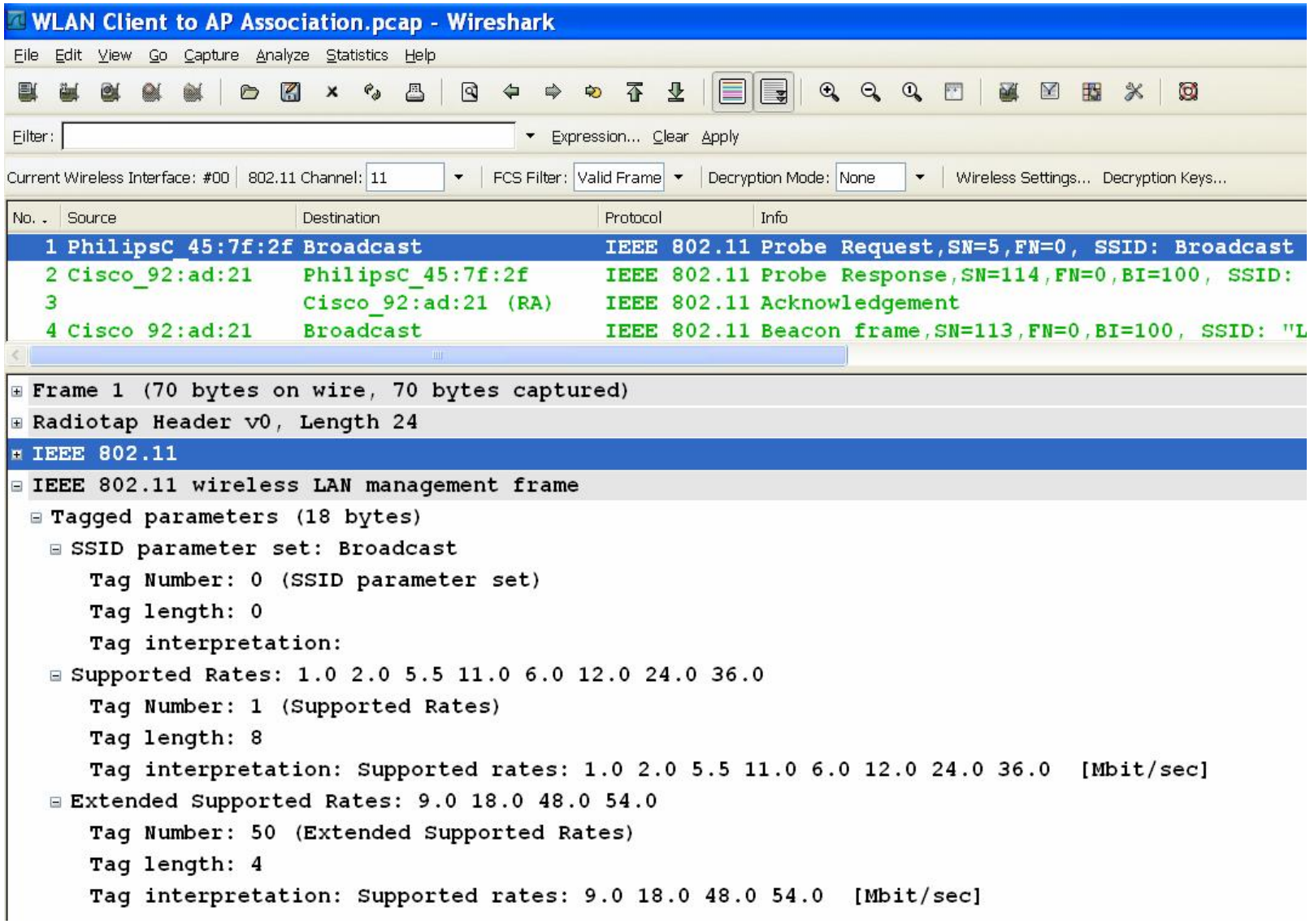


Place the Wireshark analyser anywhere within the cell, close to the access point

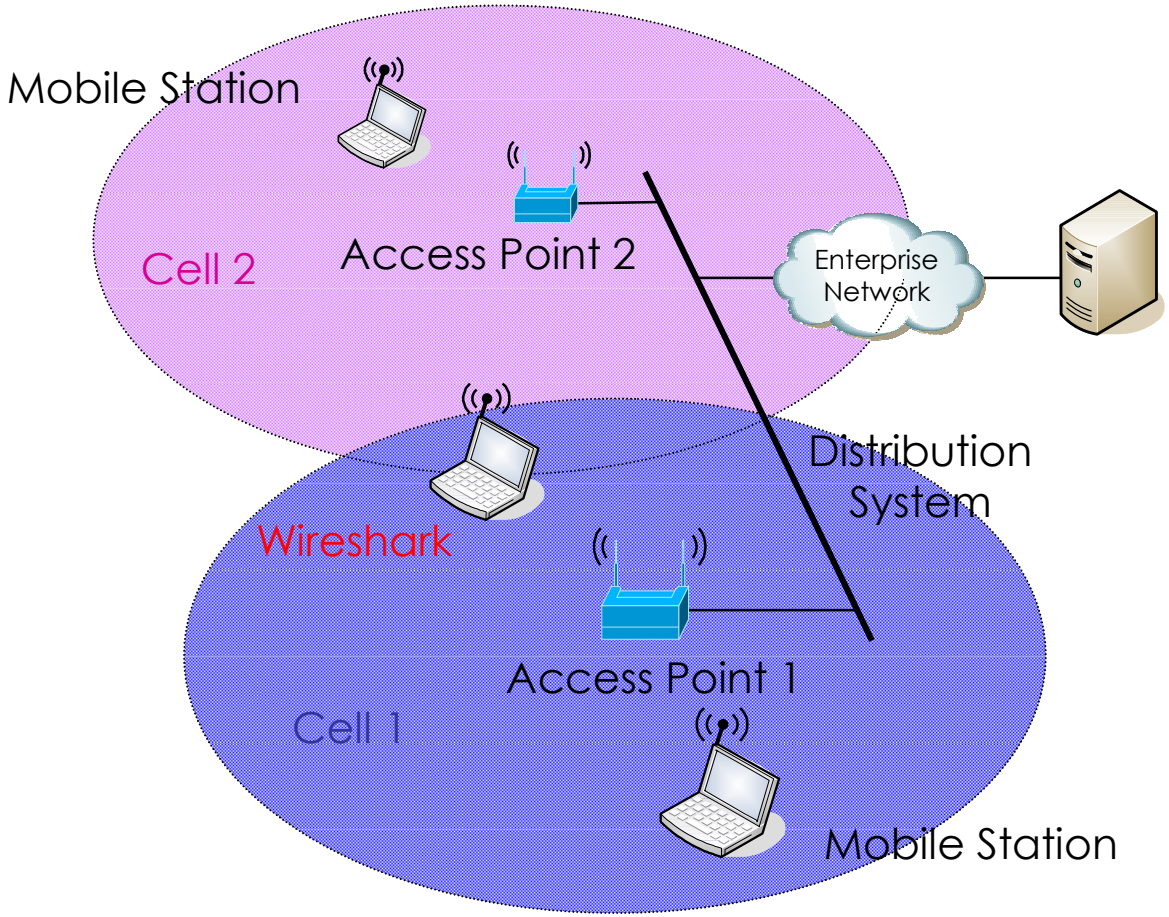
Analysing management and control frames



Analysing management and control frames



Analysing roaming problems

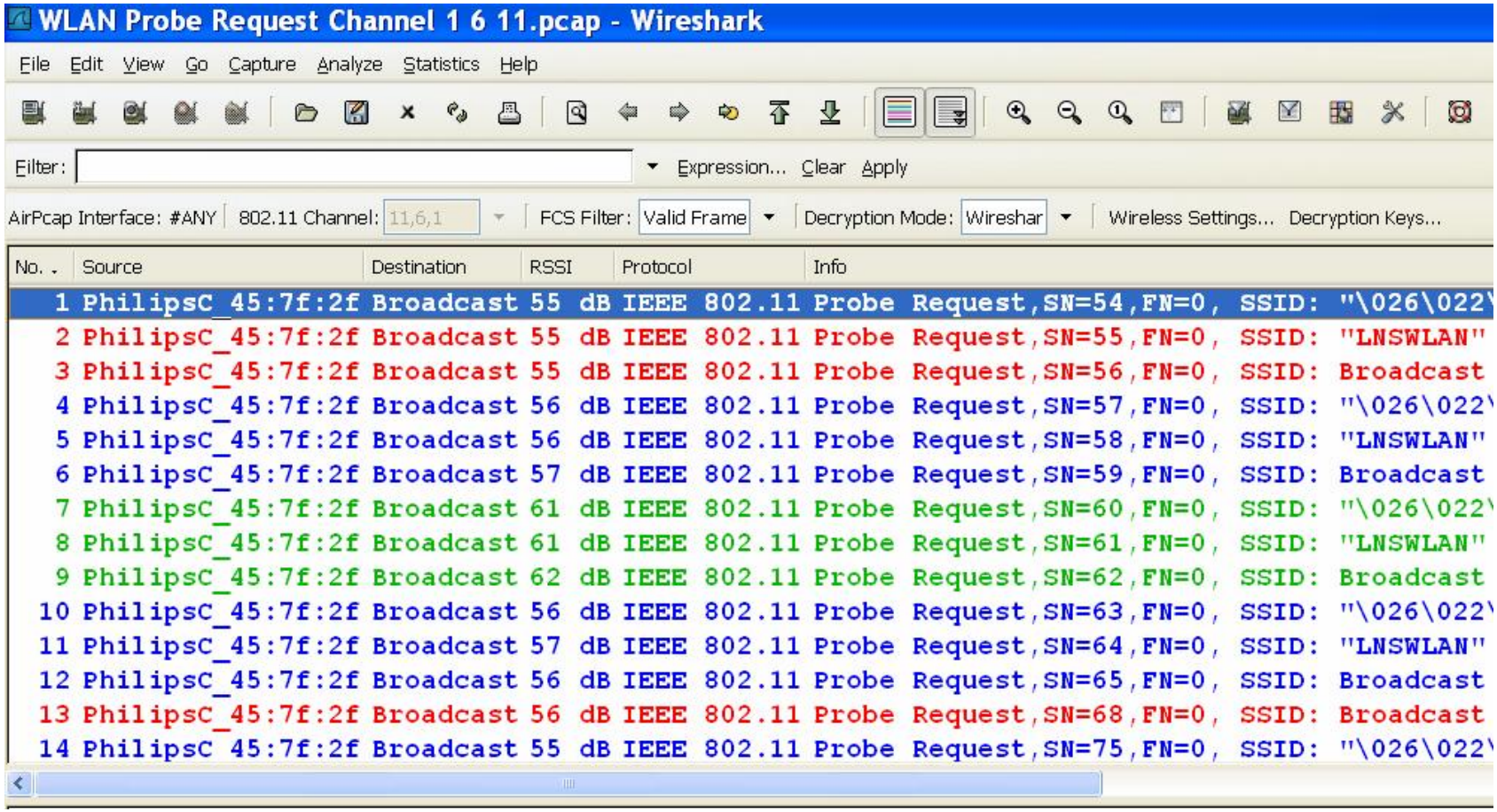


Place the Wireshark analyser in the overlapping zone of two or more access points

Analysing roaming problems

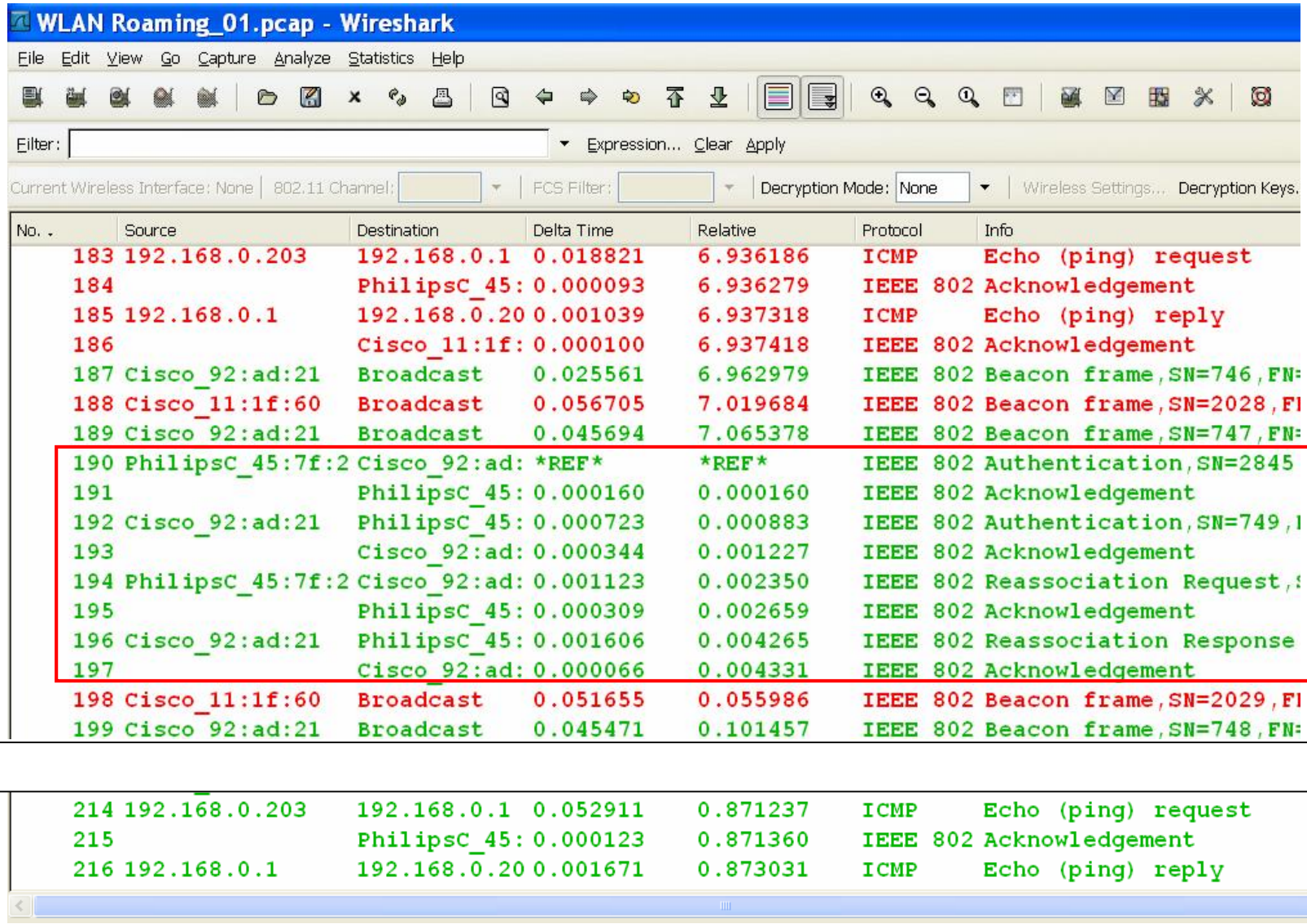
- Extended with a standard USB 2.0 hub, Wireshark can simultaneously capture packets in different radio cells
- Captured packets can be displayed in the same trace
- Packets can be colored to differentiate between channels

Analysing roaming problems



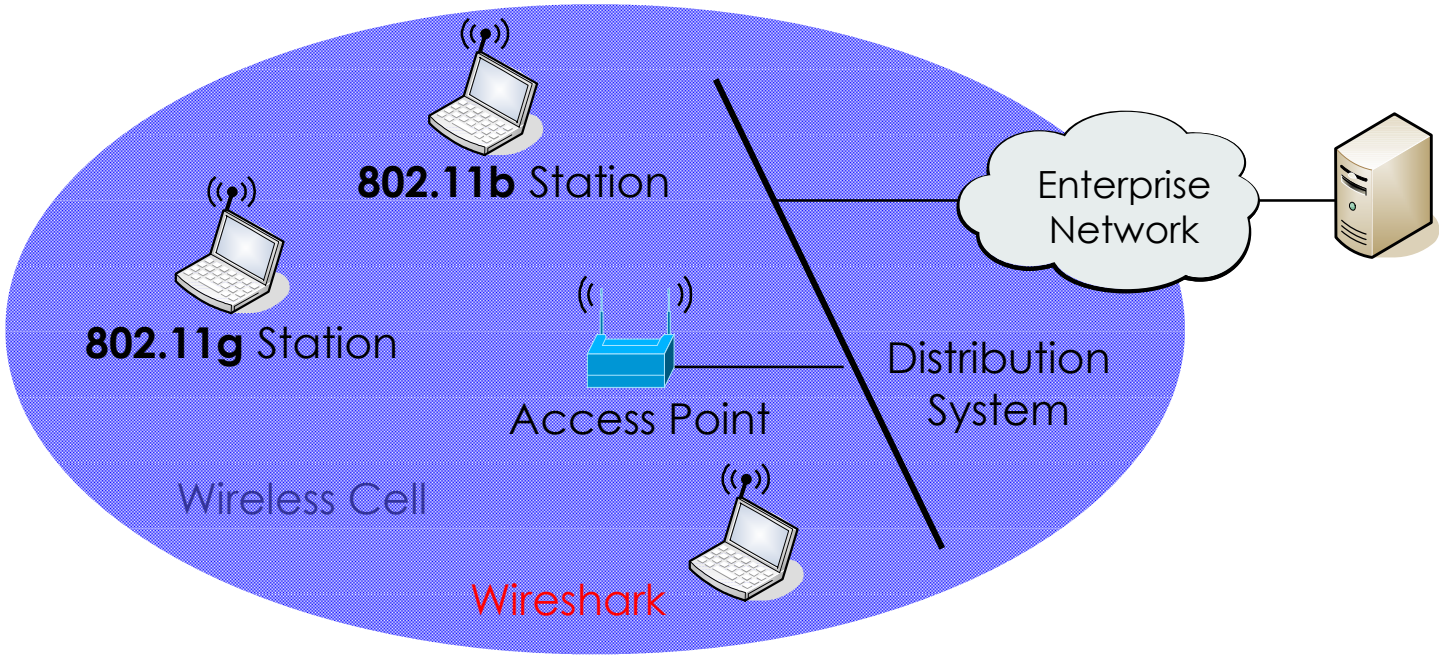
Simultaneous packet capture in channel 1, 6 and 11

Analysing roaming problems



Analysing mixed 802.11b and g environments

802.11b (DSSS) and 802.11g (OFDM) can run simultaneously in the same cell

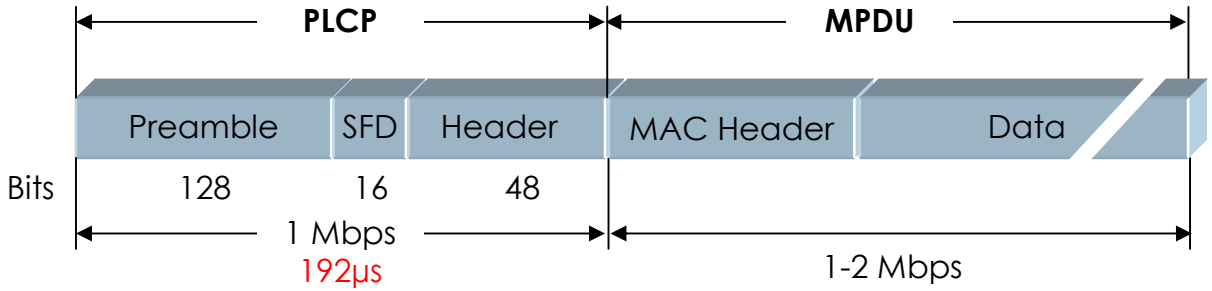


Problem: Stations using DSSS cannot 'hear' stations using OFDM!

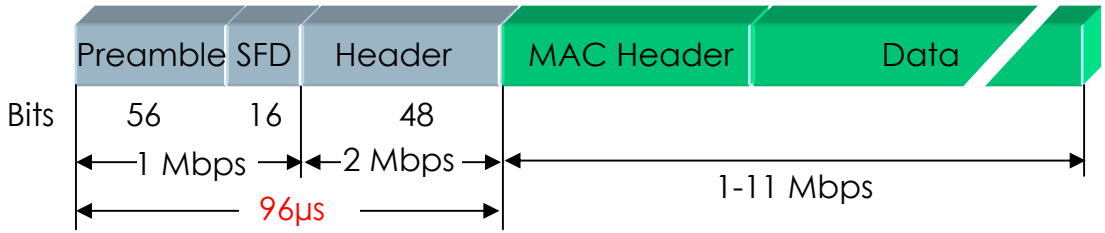
Analysing mixed 802.11b and g environments

DSSS and OFDM packet formats are NOT compatible

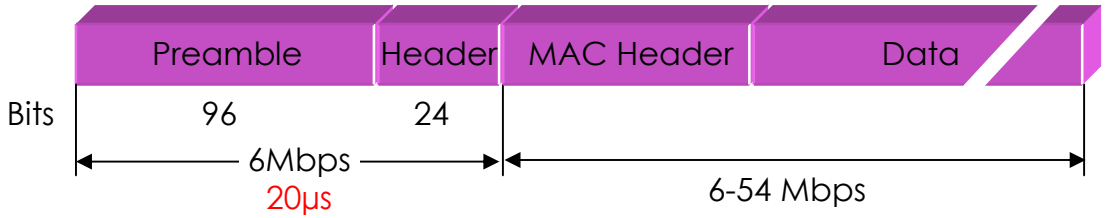
802.11 DSSS with
‚Long Preamble'
Barker Code



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



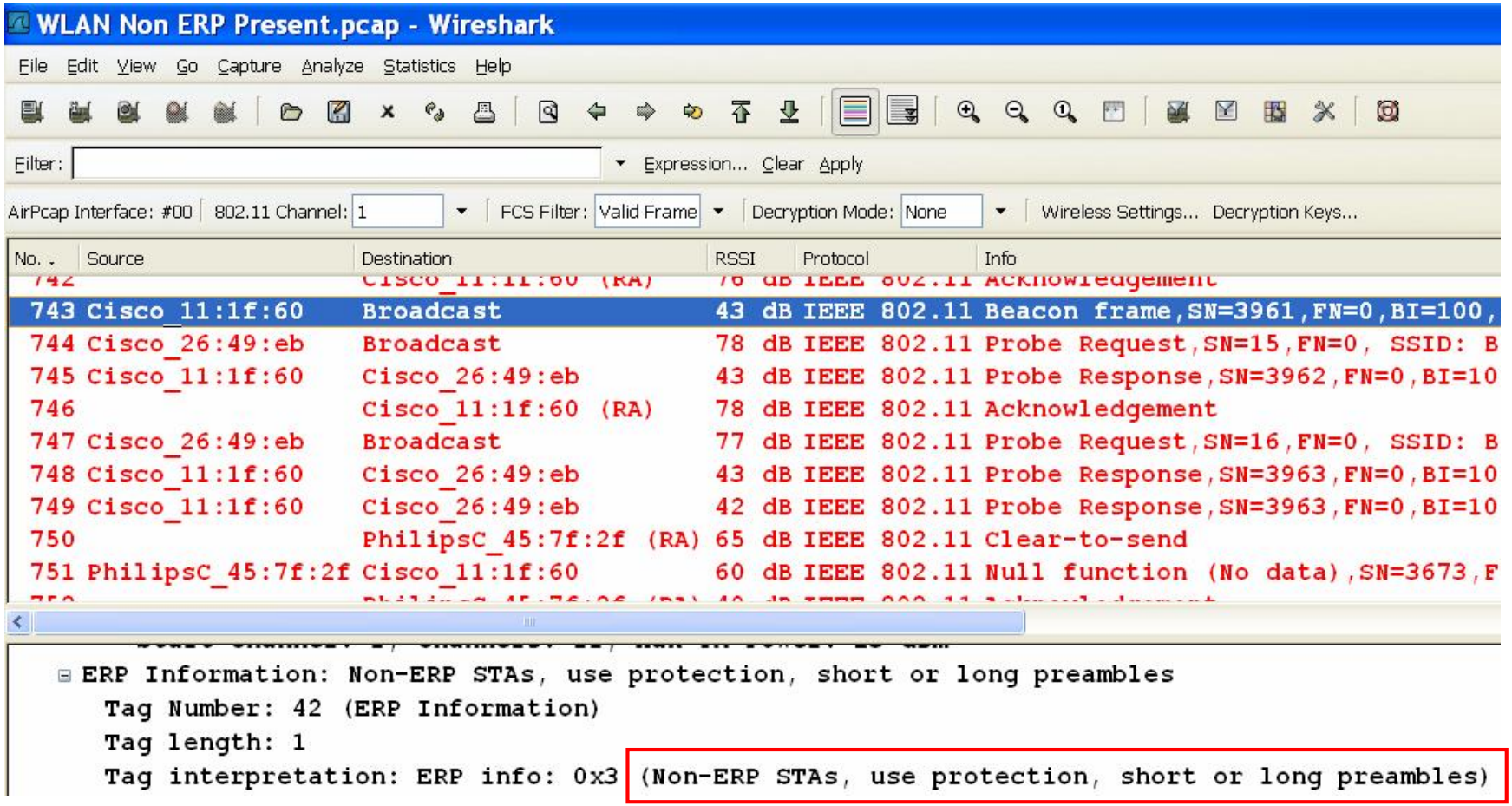
802.11g (ERP)
Extended Rate PHY
new Frame Format
OFDM



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

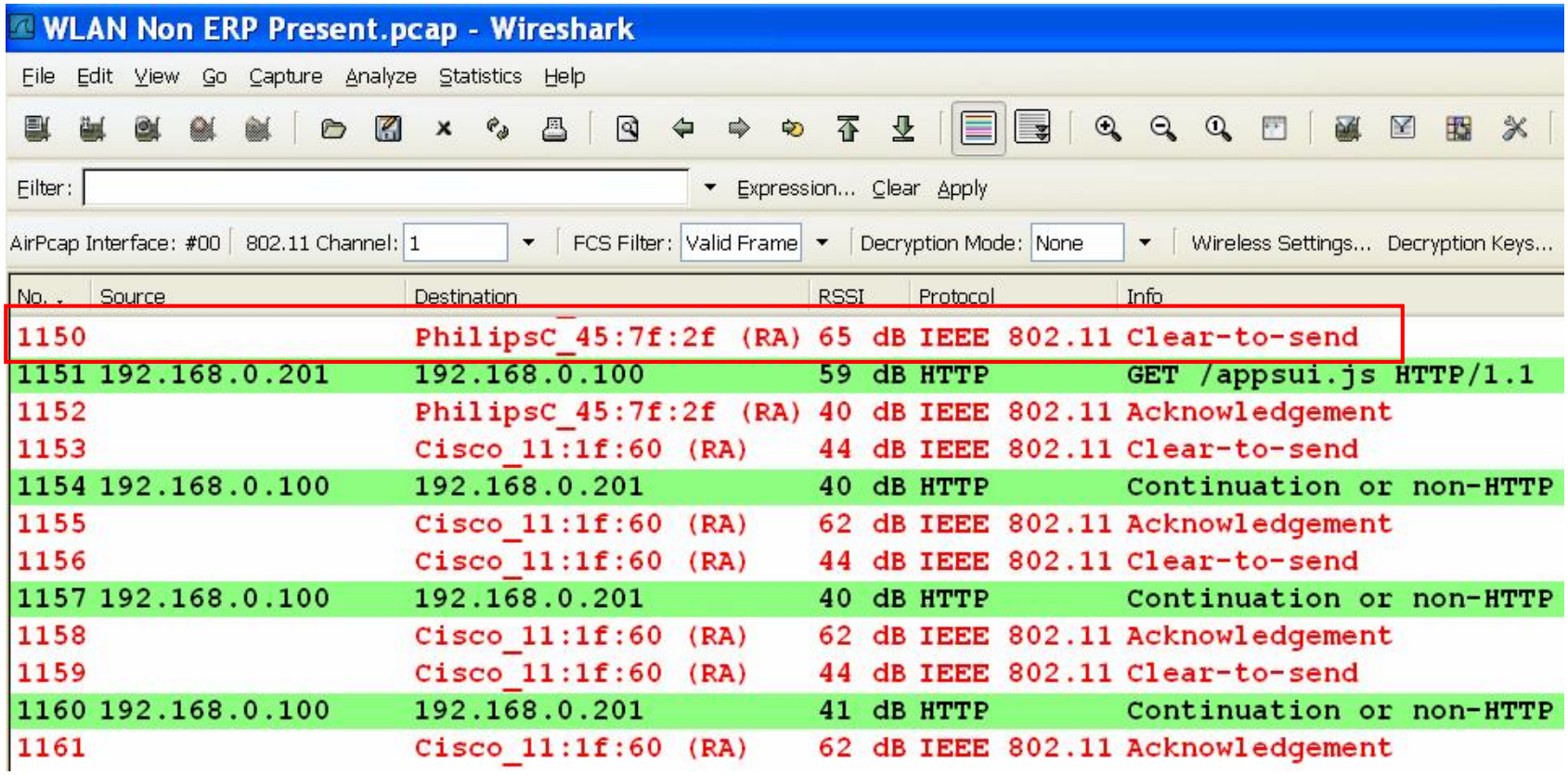
Analysing mixed 802.11b and g environments

Access point indicates in 'Beacon' if DSSS stations are present



Analysing mixed 802.11b and g environments

OFDM stations changes to 'Protected Mode'



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

Analysing mixed 802.11b and g environments

Reduced data throughput in mixed environments

	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

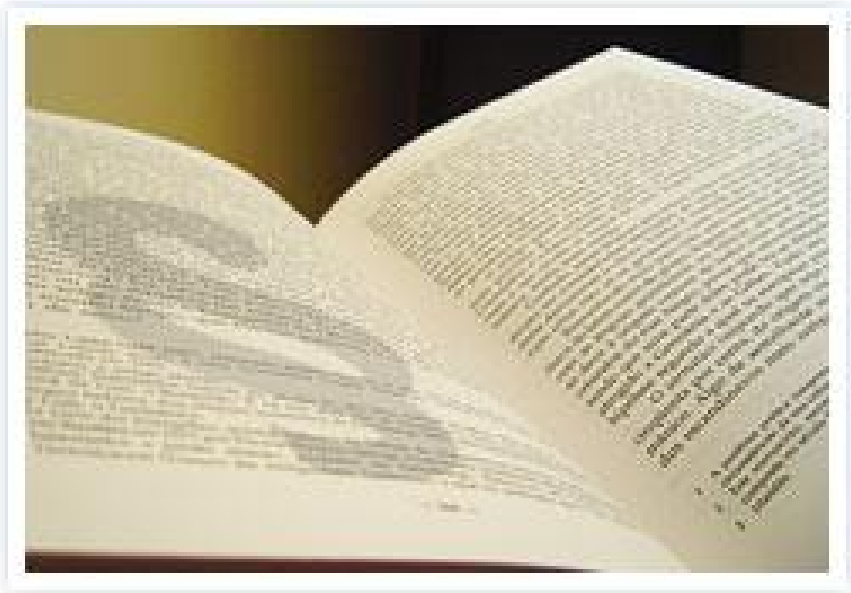
Analysing security issues

Judgement of Landgericht Hamburg 26.7.2006

Source: http://www.lexexakt.de/glossar/lghamburg2006-07-26.php

Providers of an unsecured WLAN are liable and can be prosecuted for illegal activities like music downloading, spamming etc.

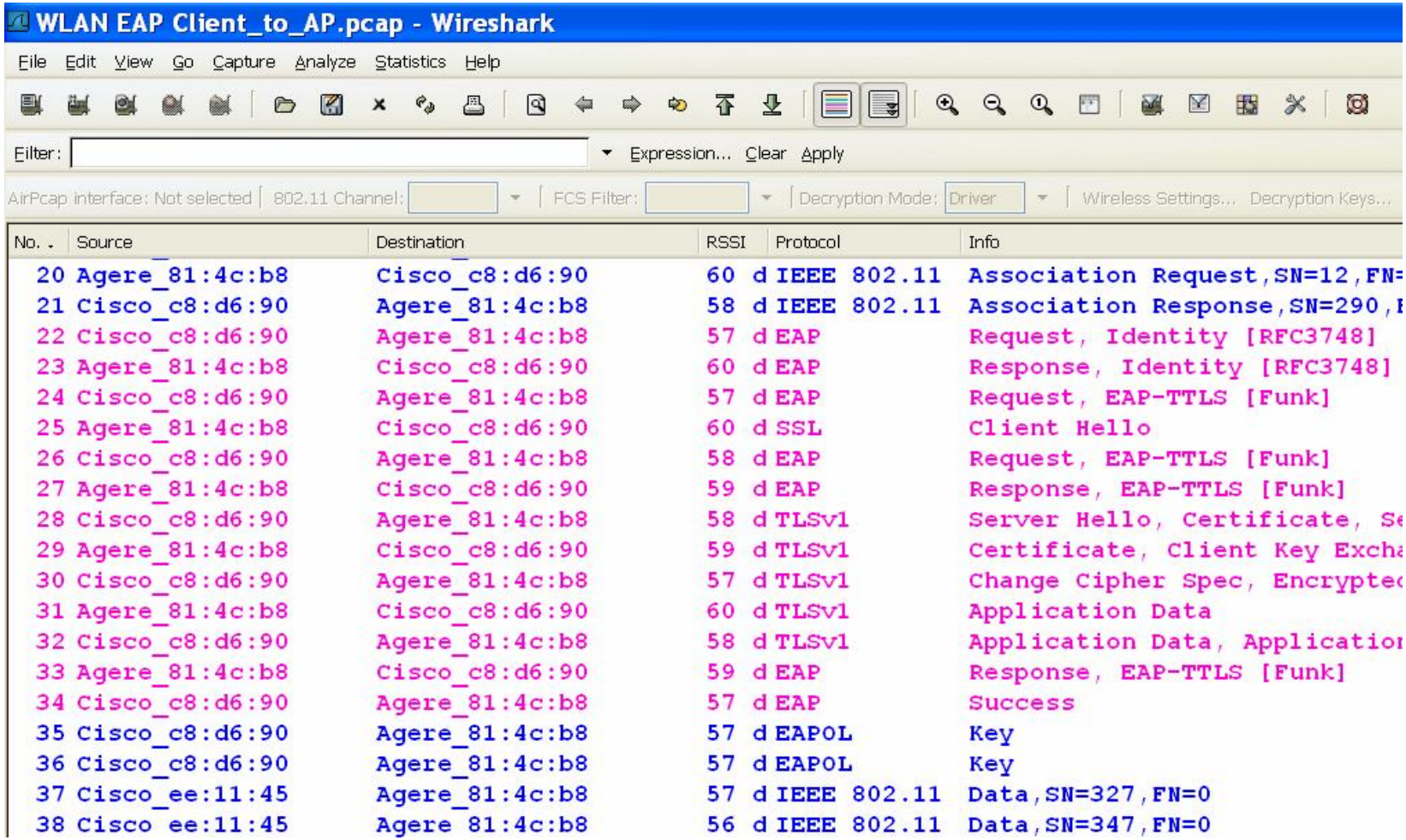
A German company has been sued and adjudged for illegal music downloading through an unsecured WLAN by a third party.



WLAN security is not an option anymore!

Analysing security issues

Key exchange process can be analysed

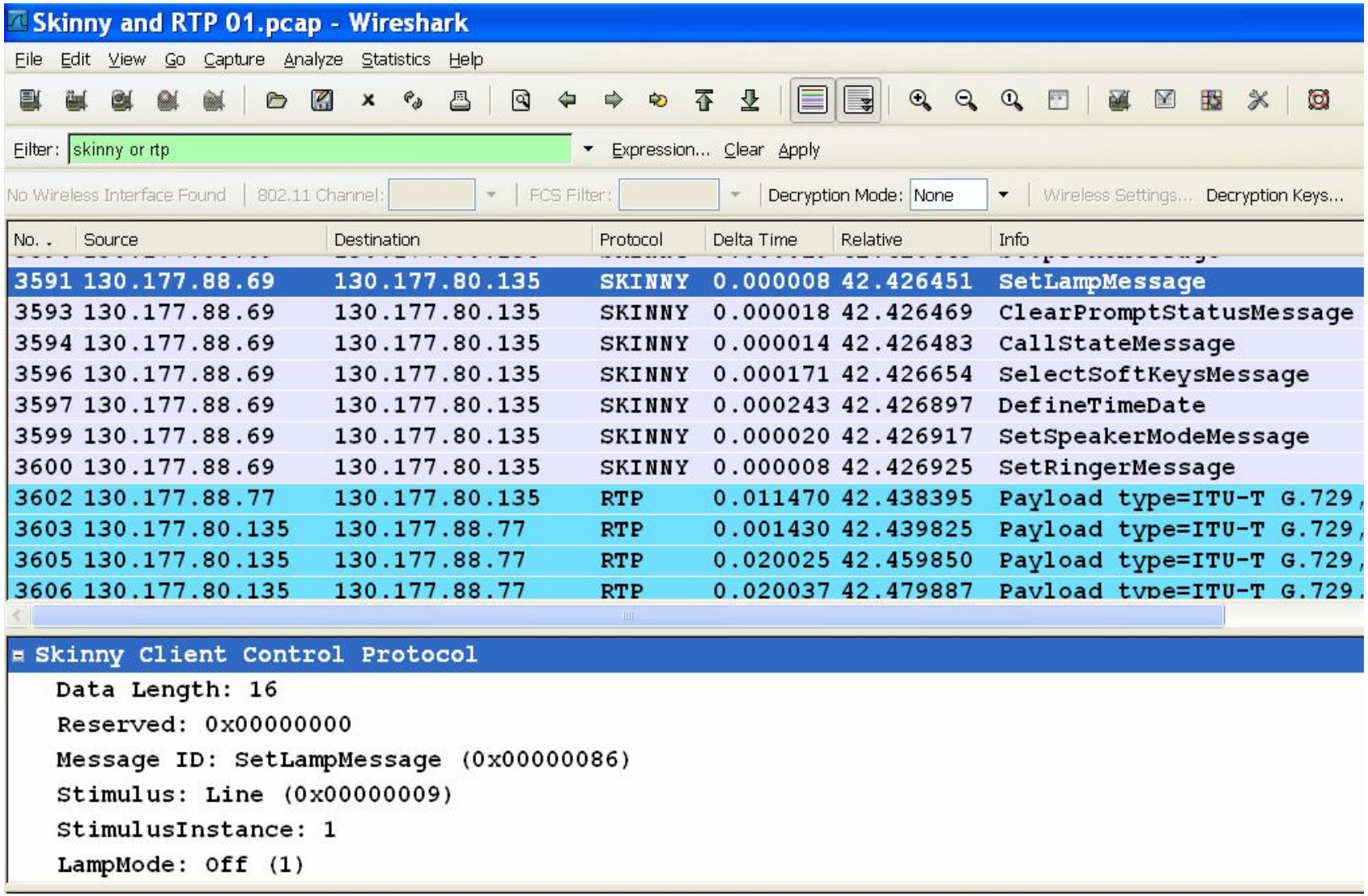


To make the picture complete:

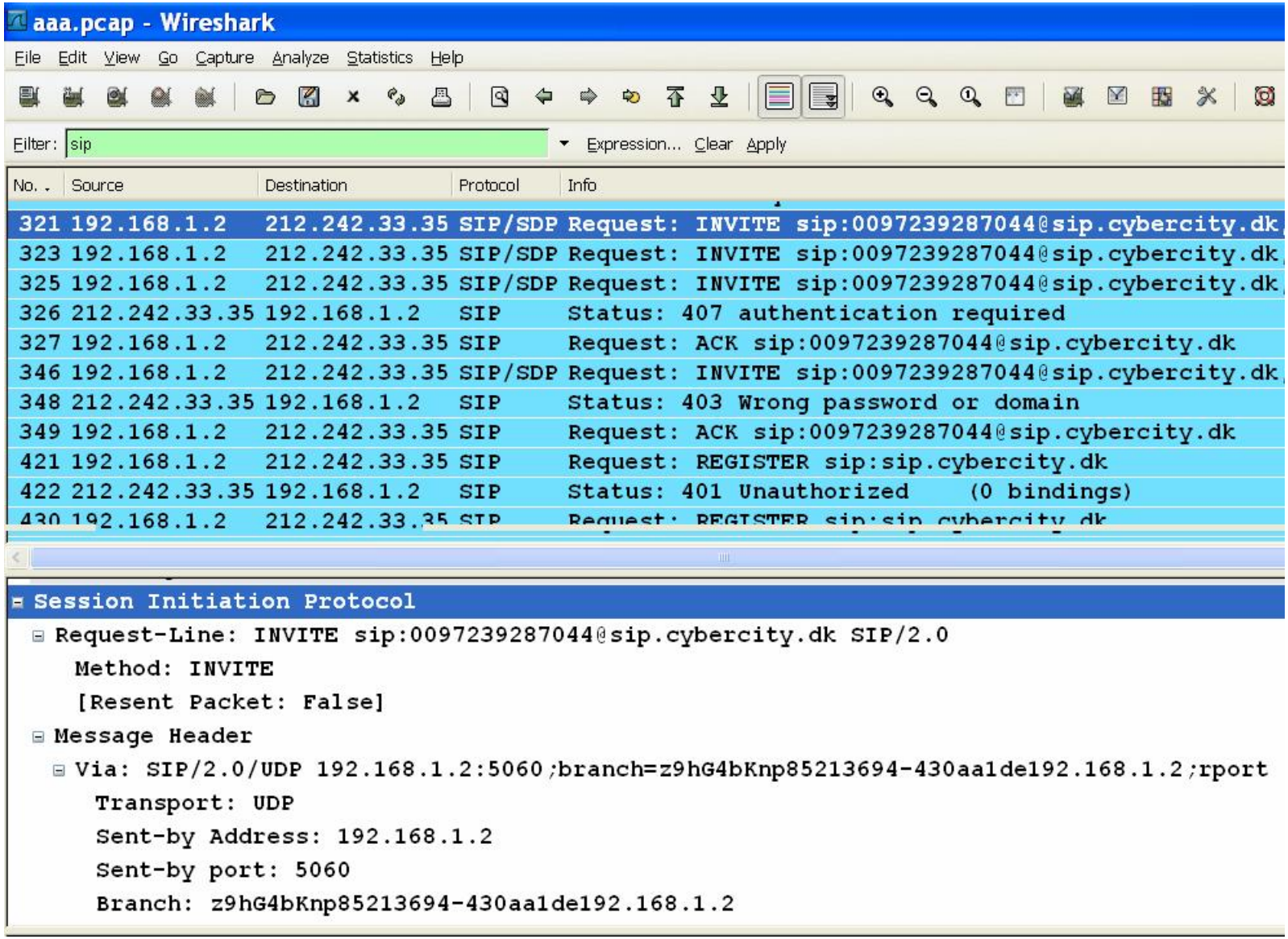
- Wireshark is also analysing all popular VoIP protocols like Skinny, SIP, MGCP etc.
- Moreover, Wireshark has an excellent expert knowledge system which assists you in bulk data analysing
- And Wireshark has very powerful filter possibilities

Let me give you some examples...

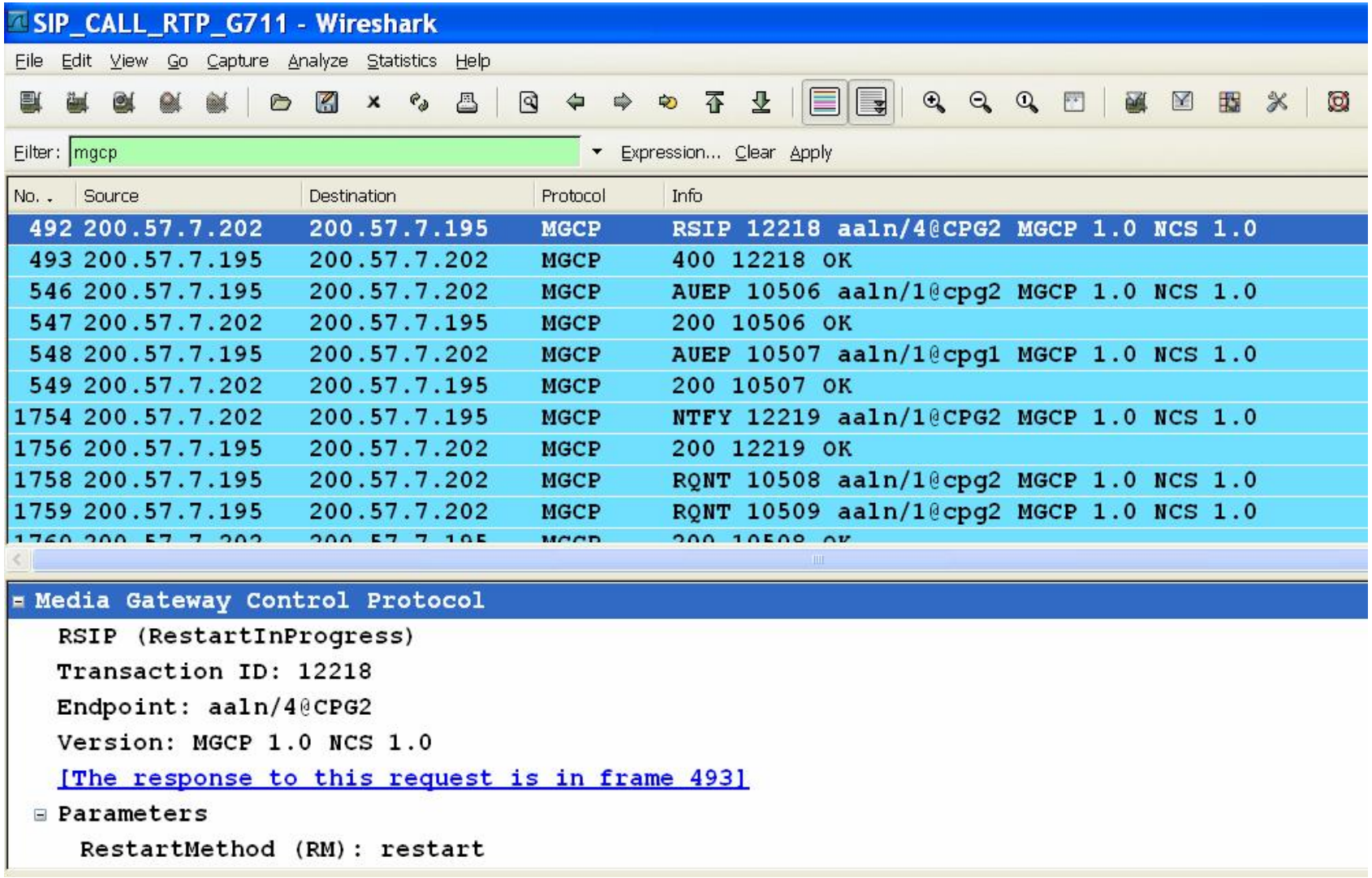
Analysing VoIP protocols



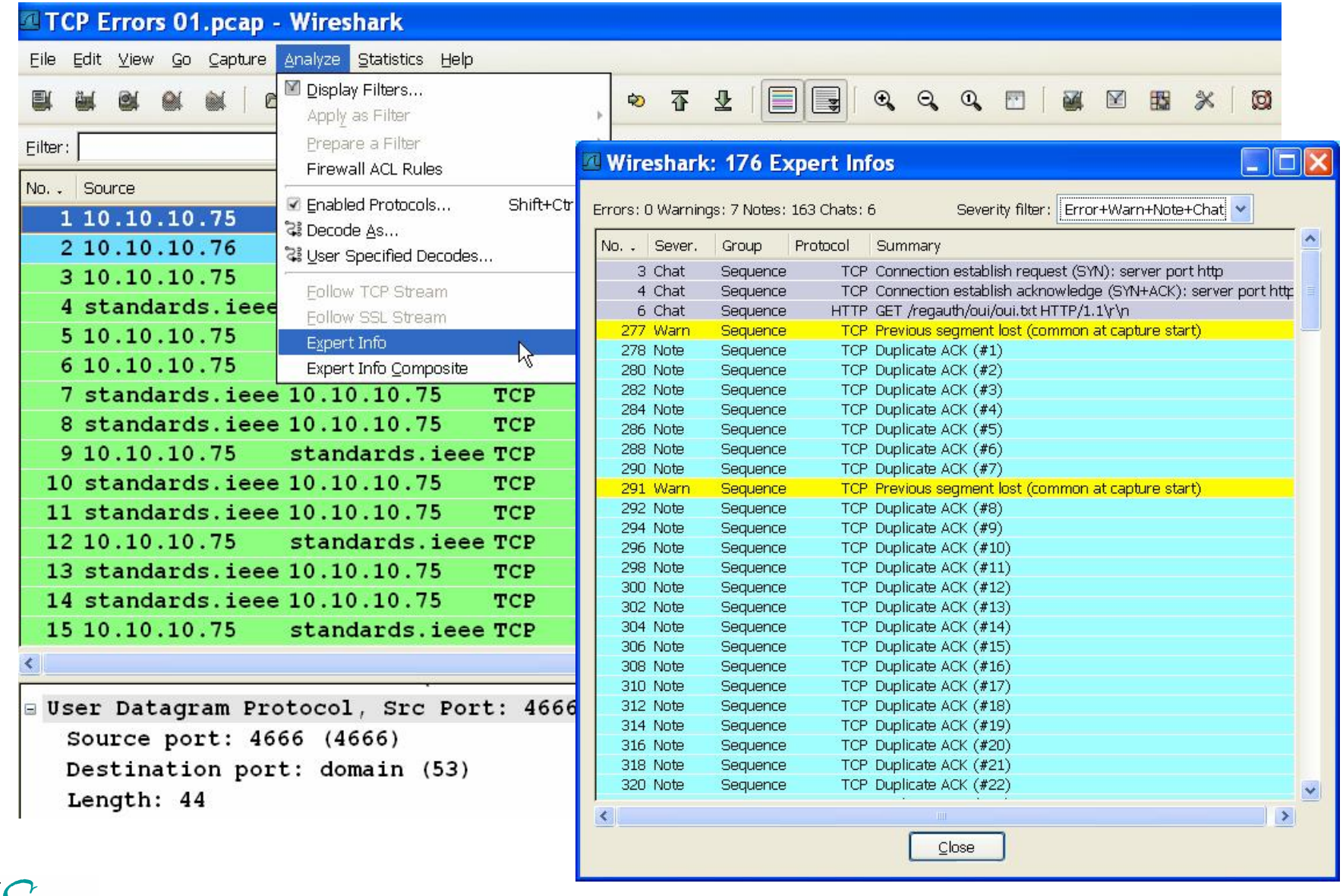
Analysing VoIP protocols



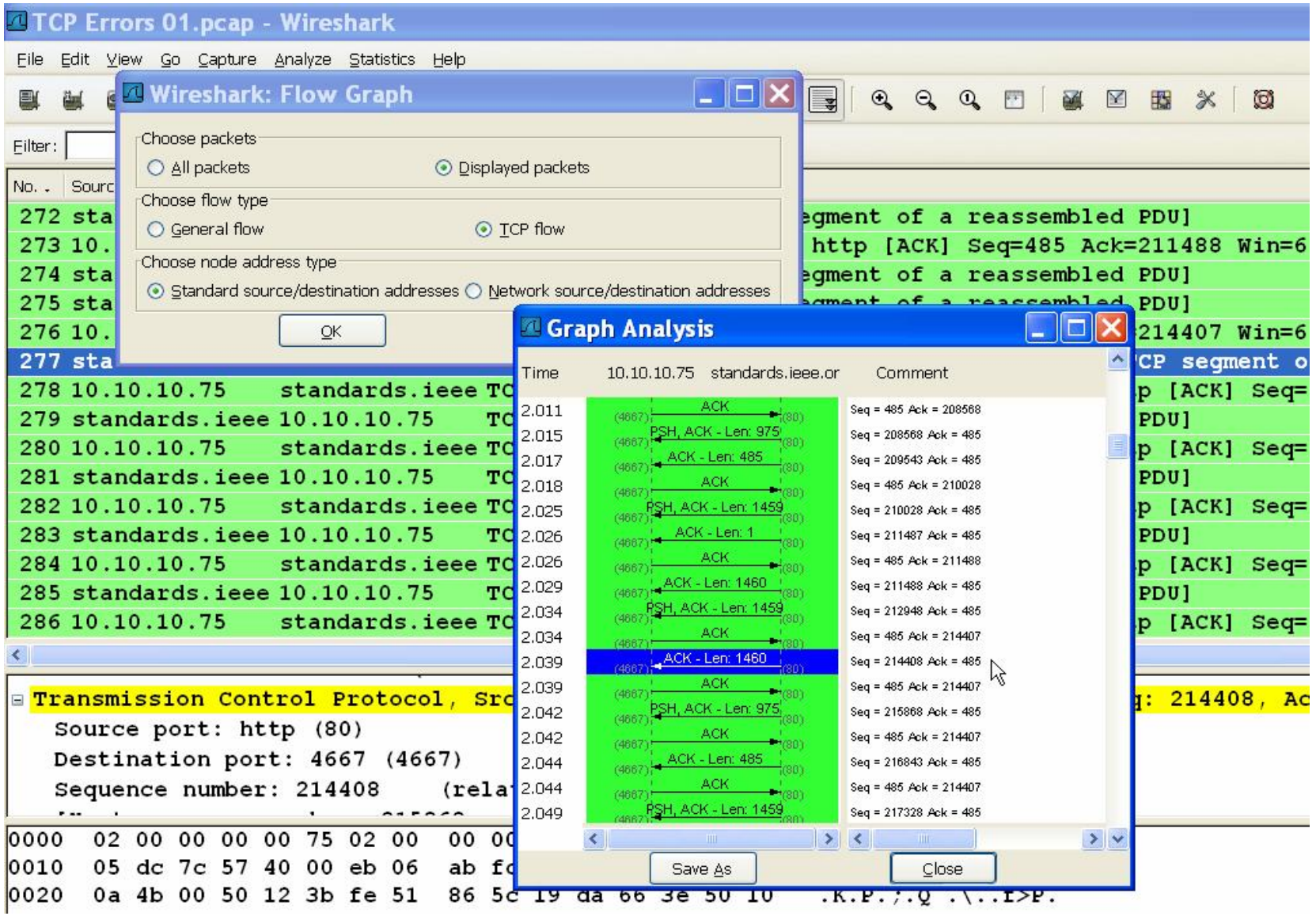
Analysing VoIP protocols



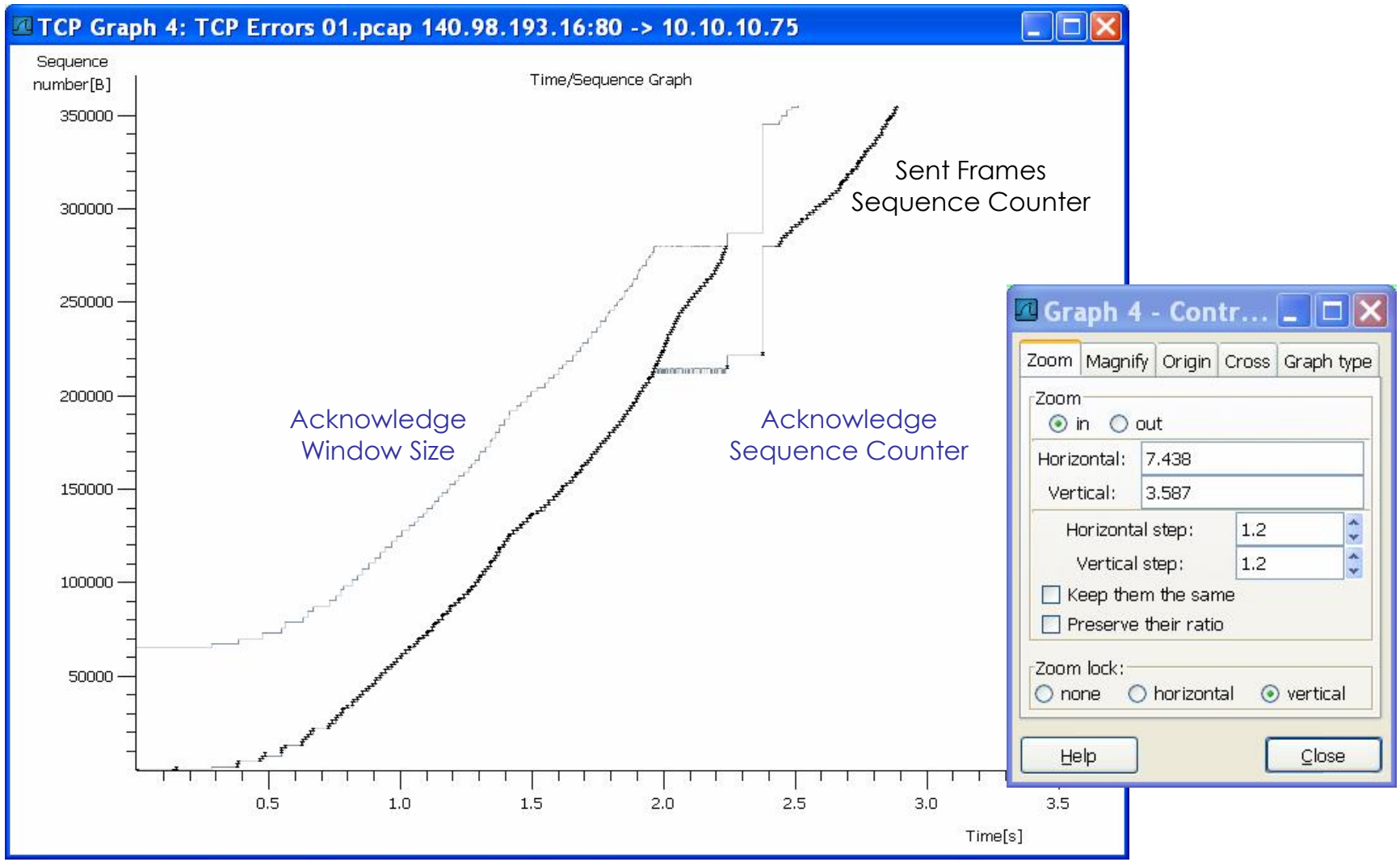
Wireshark expert system



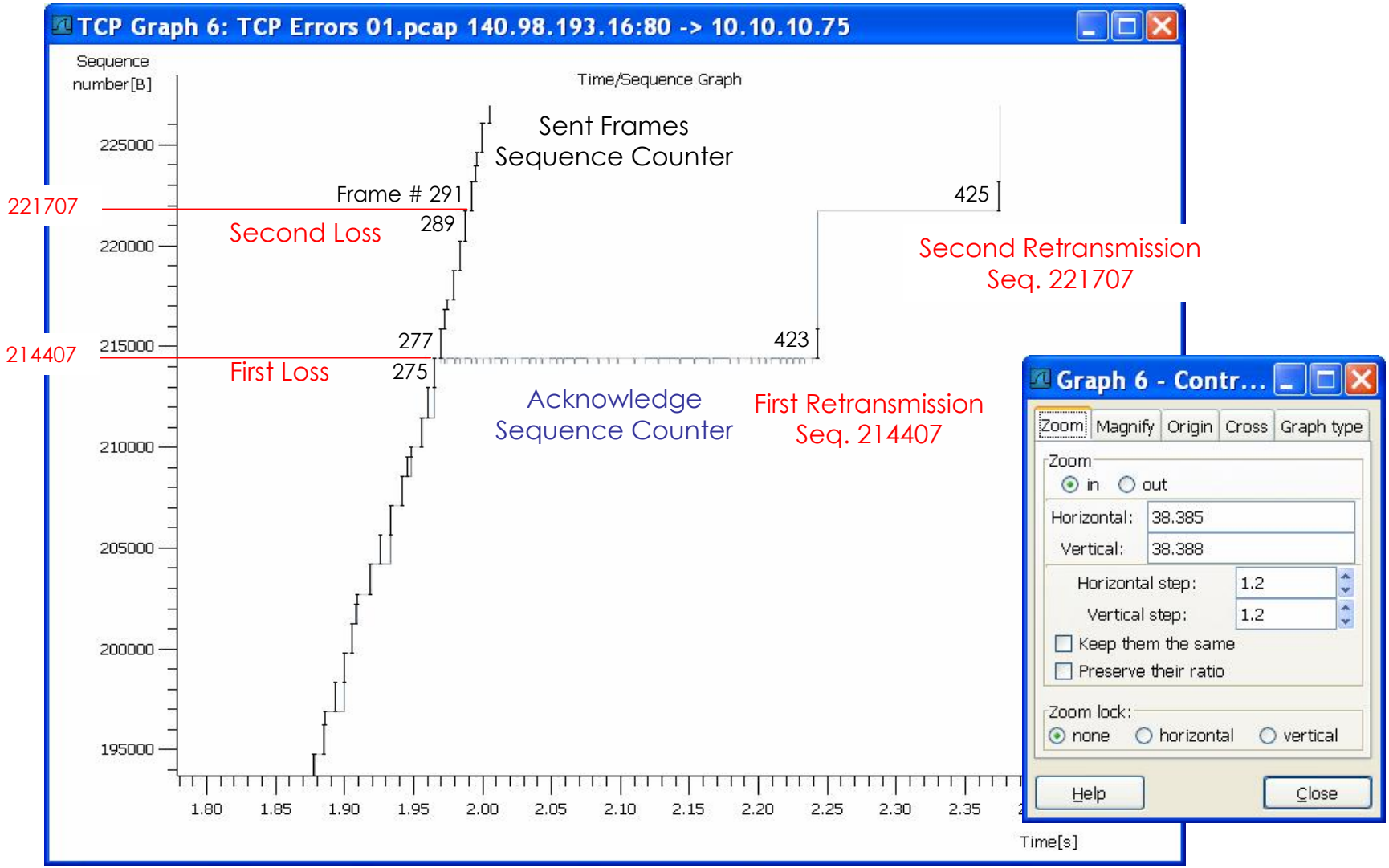
Wireshark expert system



Wireshark expert system



Wireshark expert system



To summarize:

- Wireshark is a sophisticated tool for analysing and troubleshooting network problems
- Wireshark in combination with AirPcap has unique features like simultaneous capturing in different 802.11b/g channels
- Due to its open source background Wireshark has unlimited potential to adopt to future technology changes
- Wireshark has best cost/benefit ratio
- Wireshark trainings are available to acquire in-depth skills and knowledge

The End

Thank you for your attention

I would enjoy to meet you again in one of our trainings

Rolf Leutert
Leutert Netservices
www.wireshark.ch