



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 ®

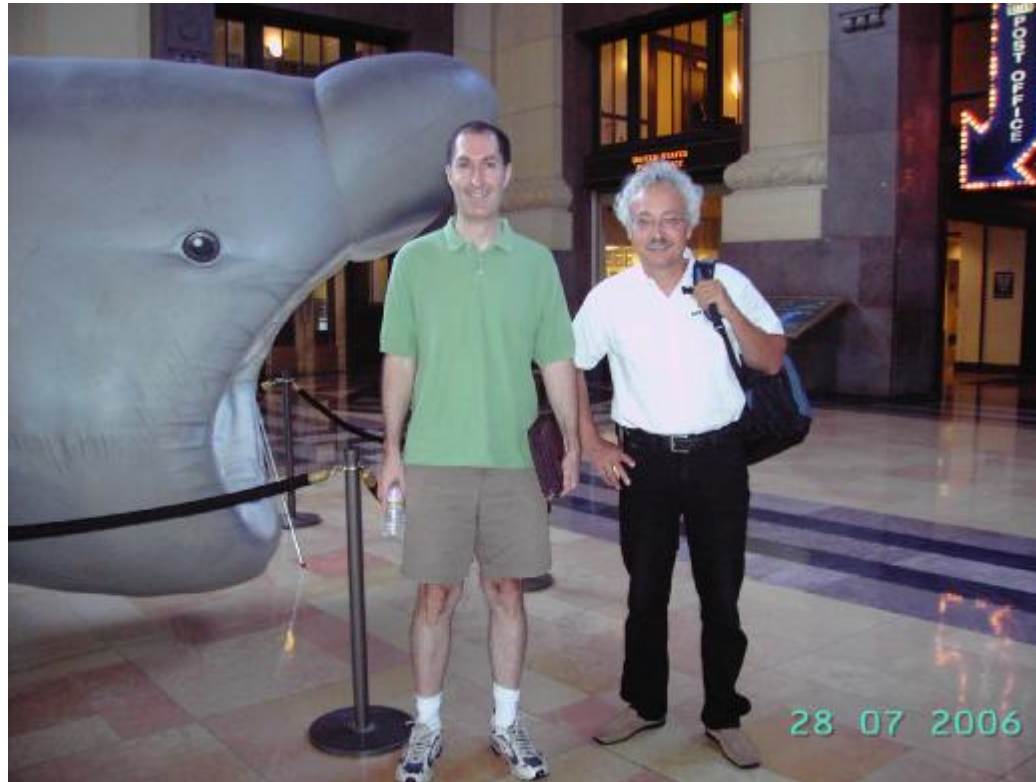
- The Ethereal project has been initiated in 1997 by Gerald Combs in Kansas City
- Gerald has found the name Ethereal in the dictionary – it stands for *‘from heaven’*
- In the meantime, more than 500 developers worldwide contributed to its programming protocol decoders (so called dissectors)
- Ethereal has been nominated as #1 packet sniffing tool by [Insecure.org](http://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



- 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, including control frames, management frames and power information



Why am I telling you this?

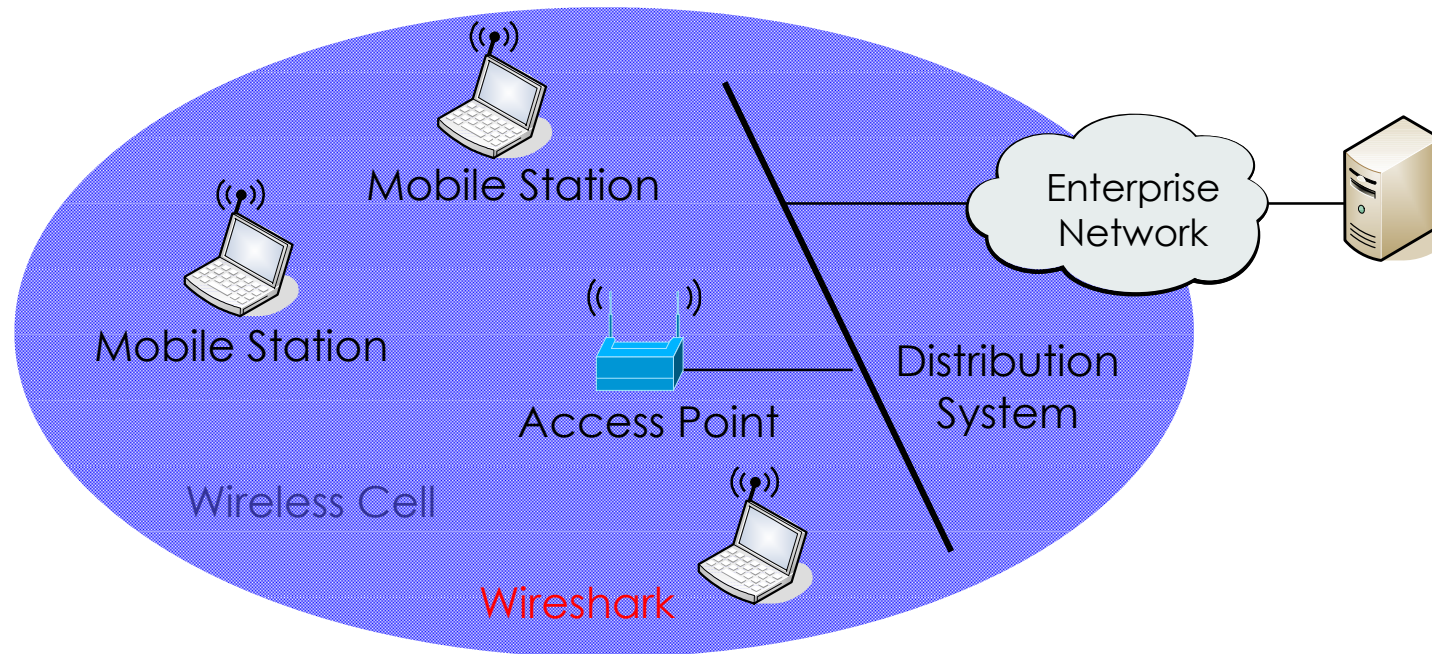
- Because you are responsible for the function, security and performance of your customers` wireless networks
- Because you can get a full function wire and wireless sniffer with expert knowledge at very low cost
- Because with Wireshark and AirPcap you can turn an ordinary notebook into a full function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

The screenshot shows a Wireshark capture of a WLAN client-to-AP association process. The interface is 'WLAN Client to AP Association.pcap - Wireshark'. The packet list pane shows 22 packets. Packet 1 is a Probe Request from PhilipsC_45:7f:2f to Broadcast. Packets 2-3 are a Probe Response and its Acknowledgement. Packets 4-6 are Beacon frames from Cisco_92:ad:21 to Broadcast. Packets 7-8 are an Authentication sequence. Packets 9-10 are another Authentication sequence. Packets 11-12 are an Association Request and its Acknowledgement. Packet 13 is an Association Response from Cisco_92:ad:21 to PhilipsC_45:7f:2f. Packets 14-16 are Beacon frames. Packet 17 is a WLCCP frame from Aironet_55:ed:2f to PhilipsC_45:7f:2f. Packets 18-19 are an Acknowledgement and a DHCP Discover from 0.0.0.0 to 255.255.255.255. Packet 20 is an Acknowledgement for the DHCP Discover. Packet 21 is a DHCP Offer from 192.168.0.1 to 192.168.0.202. Packet 22 is a DHCP Request from 0.0.0.0 to 255.255.255.255.

No.	Source	Destination	Protocol	Info
1	PhilipsC_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=5, FN=0, SSID: Broadcast
2	Cisco_92:ad:21	PhilipsC_45:7f:2f	IEEE 802.11	Probe Response, SN=114, FN=0, BI=100, SSID: "LNSWLAN", Name: "AP350-RL-I
3	Cisco_92:ad:21	Cisco_92:ad:21 (RA)	IEEE 802.11	Acknowledgement
4	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=113, FN=0, BI=100, SSID: "LNSWLAN", Name: "AP350-RL-Lat
5	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=115, FN=0, BI=100, SSID: "LNSWLAN", Name: "AP350-RL-Lat
6	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=117, FN=0, BI=100, SSID: "LNSWLAN", Name: "AP350-RL-Lat
7	PhilipsC_45:7f:2f	Cisco_92:ad:21	IEEE 802.11	Authentication, SN=0, FN=0
8	PhilipsC_45:7f:2f (RA)	PhilipsC_45:7f:2f	IEEE 802.11	Acknowledgement
9	Cisco_92:ad:21	PhilipsC_45:7f:2f	IEEE 802.11	Authentication, SN=151, FN=0
10	Cisco_92:ad:21 (RA)	PhilipsC_45:7f:2f	IEEE 802.11	Acknowledgement
11	PhilipsC_45:7f:2f	Cisco_92:ad:21	IEEE 802.11	Association Request, SN=1, FN=0, SSID: "LNSWLAN", Name: ""
12	PhilipsC_45:7f:2f (RA)	PhilipsC_45:7f:2f	IEEE 802.11	Acknowledgement
13	Cisco_92:ad:21	PhilipsC_45:7f:2f	IEEE 802.11	Association Response, SN=152, FN=0, Name: "AP350-RL-Lab"
14	Cisco_92:ad:21 (RA)	PhilipsC_45:7f:2f	IEEE 802.11	Acknowledgement
15	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=150, FN=0, BI=100, SSID: "LNSWLAN", Name: "AP350-RL-Lat
16	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=153, FN=0, BI=100, SSID: "LNSWLAN", Name: "AP350-RL-Lat
17	Aironet_55:ed:2f	PhilipsC_45:7f:2f	WLCCP	WLCCP frame
18	Cisco_92:ad:21 (RA)	PhilipsC_45:7f:2f	IEEE 802.11	Acknowledgement
19	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x3a932194
20	PhilipsC_45:7f:2f (RA)	PhilipsC_45:7f:2f	IEEE 802.11	Acknowledgement
21	192.168.0.1	192.168.0.202	DHCP	DHCP Offer - Transaction ID 0x3a932194
22	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x3a932194

Frame 1 (70 bytes on wire, 70 bytes captured)
 Radiotap Header v0, Length 24
 IEEE 802.11
 IEEE 802.11 wireless LAN management frame

```

0000 00 00 18 00 8e 58 00 00 10 02 9e 09 a0 00 60 00  ....X.. .....
0010 00 35 00 00 6f 25 18 75 40 00 00 00 ff ff ff ff  .5..o%.u @.....
0020 ff ff 00 05 4e 45 7f 2f ff ff ff ff ff ff 50 00  ...NE./ .....P.
0030 00 00 01 08 02 04 0b 16 0c 18 30 48 32 04 12 24  .... ..0H2..$
0040 60 6c 6f 25 18 75                                `lo%.u
    
```

File: F:\Wireshark\Trace Files\WLAN\WLAN Client to AP Association.pcap 5803 Bytes 00:00:07 | P: 36 D: 36 M: 0

Analysing management and control frames

WLAN Client to AP Association.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

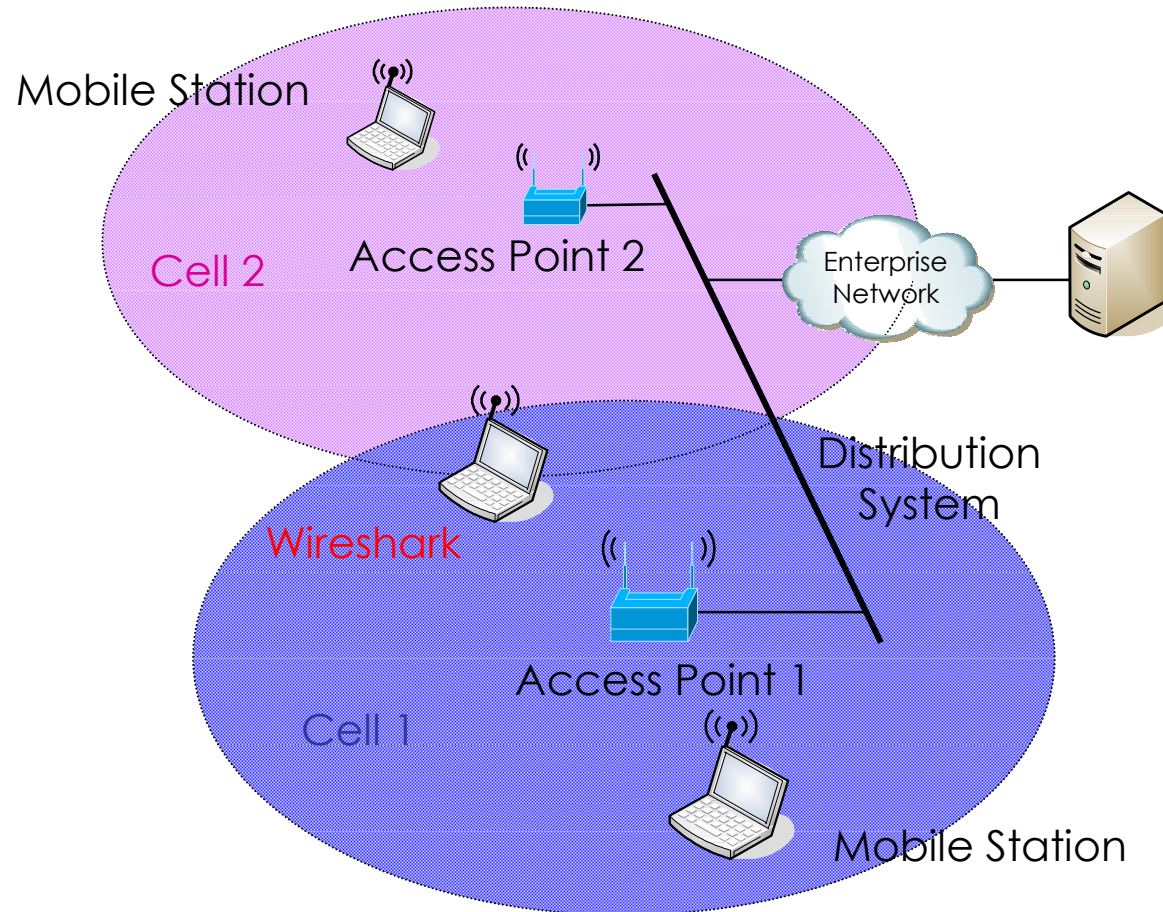
Current Wireless Interface: #00 802.11 Channel: 11 FCS Filter: Valid Frame Decryption Mode: None Wireless Settings... Decryption Keys...

No.	Source	Destination	Protocol	Info
1	PhilipsC_45:7f:2f	Broadcast	IEEE 802.11	Probe Request, SN=5, FN=0, SSID: Broadcast
2	Cisco_92:ad:21	PhilipsC_45:7f:2f	IEEE 802.11	Probe Response, SN=114, FN=0, BI=100, SSID:
3		Cisco_92:ad:21 (RA)	IEEE 802.11	Acknowledgement
4	Cisco_92:ad:21	Broadcast	IEEE 802.11	Beacon frame, SN=113, FN=0, BI=100, SSID: "L

Frame 1 (70 bytes on wire, 70 bytes captured)

- Radiotap Header v0, Length 24
- IEEE 802.11
 - IEEE 802.11 wireless LAN management frame
 - Tagged parameters (18 bytes)
 - SSID parameter set: Broadcast
 - Tag Number: 0 (SSID parameter set)
 - Tag length: 0
 - Tag interpretation:
 - Supported Rates: 1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0
 - Tag Number: 1 (Supported Rates)
 - Tag length: 8
 - Tag interpretation: Supported rates: 1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 [Mbit/sec]
 - Extended Supported Rates: 9.0 18.0 48.0 54.0
 - Tag Number: 50 (Extended Supported Rates)
 - Tag length: 4
 - Tag interpretation: Supported rates: 9.0 18.0 48.0 54.0 [Mbit/sec]

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

WLAN Probe Request Channel 1 6 11.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

AirPcap Interface: #ANY 802.11 Channel: 11,6,1 FCS Filter: Valid Frame Decryption Mode: Wireshar Wireless Settings... Decryption Keys...

No.	Source	Destination	RSSI	Protocol	Info
1	PhilipsC_45:7f:2f	Broadcast	55 dB	IEEE 802.11	Probe Request, SN=54, FN=0, SSID: "\026\022\
2	PhilipsC_45:7f:2f	Broadcast	55 dB	IEEE 802.11	Probe Request, SN=55, FN=0, SSID: "LNSWLAN"
3	PhilipsC_45:7f:2f	Broadcast	55 dB	IEEE 802.11	Probe Request, SN=56, FN=0, SSID: Broadcast
4	PhilipsC_45:7f:2f	Broadcast	56 dB	IEEE 802.11	Probe Request, SN=57, FN=0, SSID: "\026\022\
5	PhilipsC_45:7f:2f	Broadcast	56 dB	IEEE 802.11	Probe Request, SN=58, FN=0, SSID: "LNSWLAN"
6	PhilipsC_45:7f:2f	Broadcast	57 dB	IEEE 802.11	Probe Request, SN=59, FN=0, SSID: Broadcast
7	PhilipsC_45:7f:2f	Broadcast	61 dB	IEEE 802.11	Probe Request, SN=60, FN=0, SSID: "\026\022\
8	PhilipsC_45:7f:2f	Broadcast	61 dB	IEEE 802.11	Probe Request, SN=61, FN=0, SSID: "LNSWLAN"
9	PhilipsC_45:7f:2f	Broadcast	62 dB	IEEE 802.11	Probe Request, SN=62, FN=0, SSID: Broadcast
10	PhilipsC_45:7f:2f	Broadcast	56 dB	IEEE 802.11	Probe Request, SN=63, FN=0, SSID: "\026\022\
11	PhilipsC_45:7f:2f	Broadcast	57 dB	IEEE 802.11	Probe Request, SN=64, FN=0, SSID: "LNSWLAN"
12	PhilipsC_45:7f:2f	Broadcast	56 dB	IEEE 802.11	Probe Request, SN=65, FN=0, SSID: Broadcast
13	PhilipsC_45:7f:2f	Broadcast	56 dB	IEEE 802.11	Probe Request, SN=68, FN=0, SSID: Broadcast
14	PhilipsC_45:7f:2f	Broadcast	55 dB	IEEE 802.11	Probe Request, SN=75, FN=0, SSID: "\026\022\

Simultaneous packet capture in channel 1, 6 and 11

Analysing roaming problems

WLAN Roaming_01.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

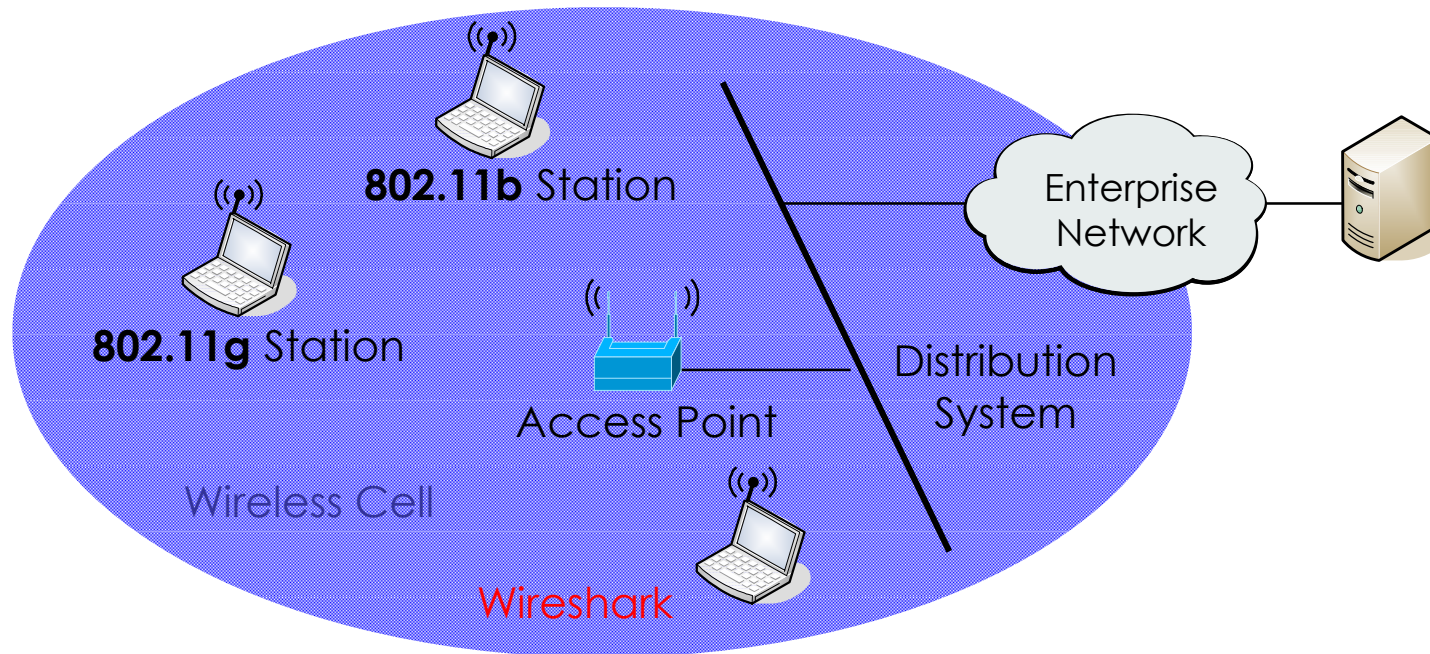
Filter: Expression... Clear Apply

Current Wireless Interface: None | 802.11 Channel: | FCS Filter: | Decryption Mode: None | Wireless Settings... Decryption Keys.

No. .	Source	Destination	Delta Time	Relative	Protocol	Info
183	192.168.0.203	192.168.0.1	0.018821	6.936186	ICMP	Echo (ping) request
184		PhilipsC_45:	0.000093	6.936279	IEEE 802	Acknowledgement
185	192.168.0.1	192.168.0.20	0.001039	6.937318	ICMP	Echo (ping) reply
186		Cisco_11:1f:	0.000100	6.937418	IEEE 802	Acknowledgement
187	Cisco_92:ad:21	Broadcast	0.025561	6.962979	IEEE 802	Beacon frame, SN=746, FN:
188	Cisco_11:1f:60	Broadcast	0.056705	7.019684	IEEE 802	Beacon frame, SN=2028, FI
189	Cisco_92:ad:21	Broadcast	0.045694	7.065378	IEEE 802	Beacon frame, SN=747, FN:
190	PhilipsC_45:7f:2	Cisco_92:ad: *REF*		*REF*	IEEE 802	Authentication, SN=2845
191		PhilipsC_45:	0.000160	0.000160	IEEE 802	Acknowledgement
192	Cisco_92:ad:21	PhilipsC_45:	0.000723	0.000883	IEEE 802	Authentication, SN=749, I
193		Cisco_92:ad:	0.000344	0.001227	IEEE 802	Acknowledgement
194	PhilipsC_45:7f:2	Cisco_92:ad:	0.001123	0.002350	IEEE 802	Reassociation Request, s
195		PhilipsC_45:	0.000309	0.002659	IEEE 802	Acknowledgement
196	Cisco_92:ad:21	PhilipsC_45:	0.001606	0.004265	IEEE 802	Reassociation Response
197		Cisco_92:ad:	0.000066	0.004331	IEEE 802	Acknowledgement
198	Cisco_11:1f:60	Broadcast	0.051655	0.055986	IEEE 802	Beacon frame, SN=2029, FI
199	Cisco_92:ad:21	Broadcast	0.045471	0.101457	IEEE 802	Beacon frame, SN=748, FN:
214	192.168.0.203	192.168.0.1	0.052911	0.871237	ICMP	Echo (ping) request
215		PhilipsC_45:	0.000123	0.871360	IEEE 802	Acknowledgement
216	192.168.0.1	192.168.0.20	0.001671	0.873031	ICMP	Echo (ping) reply

Analysing mixed 802.11b and g environments

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

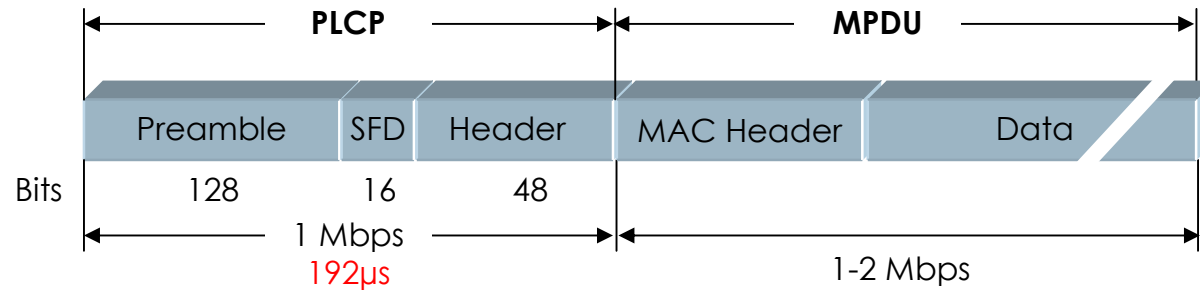


Problem: Stations using DSSS cannot 'hear' stations using OFDM!

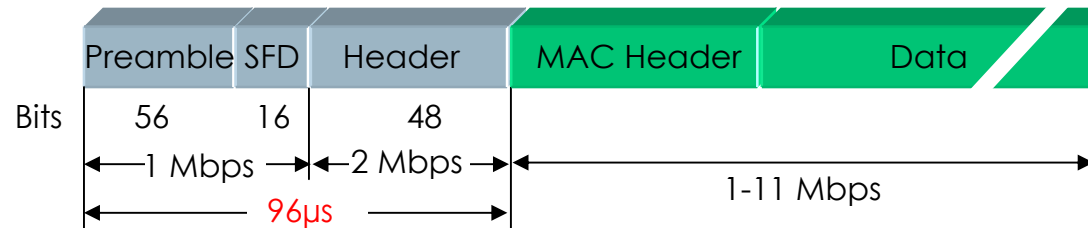
Analysing mixed 802.11b and g environments

DSSS and OFDM packet formats are NOT compatible

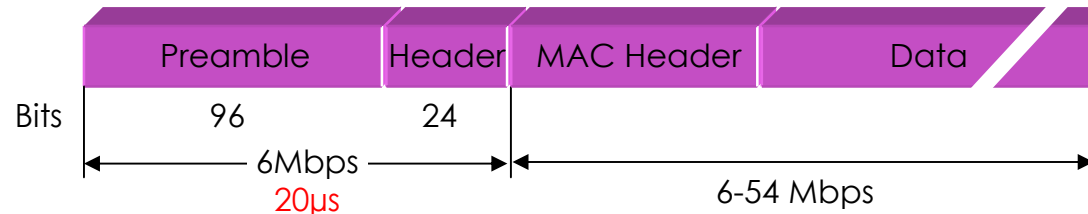
802.11 DSSS with
,Long Preamble'
Barker Code



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

The image shows a Wireshark capture of WLAN traffic. The main pane displays a list of frames. Frame 743 is highlighted, showing a Beacon frame from Cisco_11:1f:60 to Broadcast. The protocol is IEEE 802.11. The info pane below shows the ERP information: Non-ERP STAs, use protection, short or long preambles. The tag number is 42, and the tag length is 1. The tag interpretation is ERP info: 0x3 (Non-ERP STAs, use protection, short or long preambles).

No.	Source	Destination	RSSI	Protocol	Info
742		CISCO_11:1f:60 (RA)	76 dB	IEEE 802.11	Acknowledgement
743	Cisco_11:1f:60	Broadcast	43 dB	IEEE 802.11	Beacon frame, SN=3961, FN=0, BI=100,
744	Cisco_26:49:eb	Broadcast	78 dB	IEEE 802.11	Probe Request, SN=15, FN=0, SSID: B
745	Cisco_11:1f:60	Cisco_26:49:eb	43 dB	IEEE 802.11	Probe Response, SN=3962, FN=0, BI=10
746		Cisco_11:1f:60 (RA)	78 dB	IEEE 802.11	Acknowledgement
747	Cisco_26:49:eb	Broadcast	77 dB	IEEE 802.11	Probe Request, SN=16, FN=0, SSID: B
748	Cisco_11:1f:60	Cisco_26:49:eb	43 dB	IEEE 802.11	Probe Response, SN=3963, FN=0, BI=10
749	Cisco_11:1f:60	Cisco_26:49:eb	42 dB	IEEE 802.11	Probe Response, SN=3963, FN=0, BI=10
750		PhilipsC_45:7f:2f (RA)	65 dB	IEEE 802.11	Clear-to-send
751	PhilipsC_45:7f:2f	Cisco_11:1f:60	60 dB	IEEE 802.11	Null function (No data), SN=3673, F

ERP Information: Non-ERP STAs, use protection, short or long preambles
Tag Number: 42 (ERP Information)
Tag length: 1
Tag interpretation: ERP info: 0x3 (Non-ERP STAs, use protection, short or long preambles)

Analysing mixed 802.11b and g environments

OFDM stations changes to 'Protected Mode'

WLAN Non ERP Present.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

AirPcap Interface: #00 802.11 Channel: 1 FCS Filter: Valid Frame Decryption Mode: None Wireless Settings... Decryption Keys...

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
1159		Cisco_11:1f:60 (RA)	44 dB	IEEE 802.11	Clear-to-send
1160	192.168.0.100	192.168.0.201	41 dB	HTTP	Continuation or non-HTTP
1161		Cisco_11:1f:60 (RA)	62 dB	IEEE 802.11	Acknowledgement

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

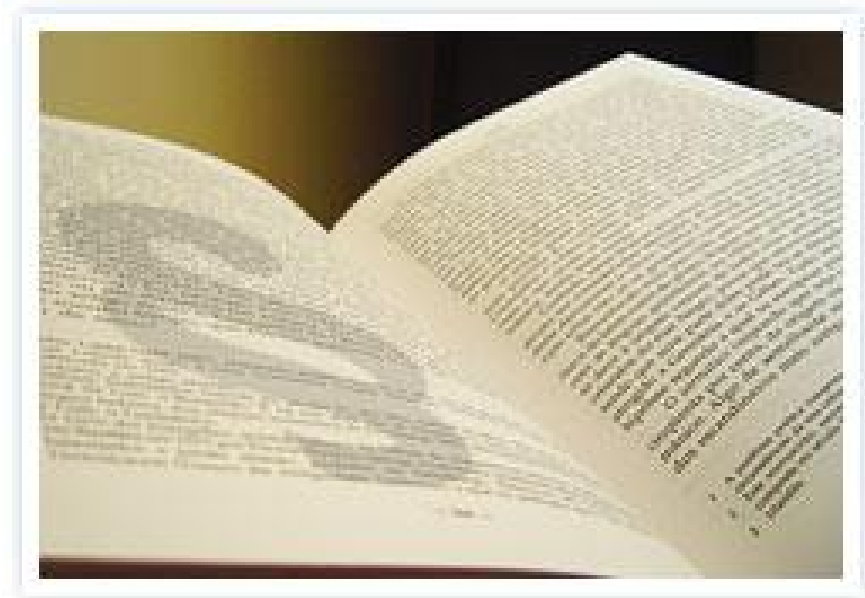
Analysing security issues

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

WLAN EAP Client_to_AP.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

AirPcap interface: Not selected | 802.11 Channel: | FCS Filter: | Decryption Mode: Driver | Wireless Settings... Decryption Keys...

No. .	Source	Destination	RSSI	Protocol	Info
20	Agere_81:4c:b8	Cisco_c8:d6:90	60	d IEEE 802.11	Association Request, SN=12, FN=
21	Cisco_c8:d6:90	Agere_81:4c:b8	58	d IEEE 802.11	Association Response, SN=290, I
22	Cisco_c8:d6:90	Agere_81:4c:b8	57	d EAP	Request, Identity [RFC3748]
23	Agere_81:4c:b8	Cisco_c8:d6:90	60	d EAP	Response, Identity [RFC3748]
24	Cisco_c8:d6:90	Agere_81:4c:b8	57	d EAP	Request, EAP-TTLS [Funk]
25	Agere_81:4c:b8	Cisco_c8:d6:90	60	d SSL	Client Hello
26	Cisco_c8:d6:90	Agere_81:4c:b8	58	d EAP	Request, EAP-TTLS [Funk]
27	Agere_81:4c:b8	Cisco_c8:d6:90	59	d EAP	Response, EAP-TTLS [Funk]
28	Cisco_c8:d6:90	Agere_81:4c:b8	58	d TLSv1	Server Hello, Certificate, Se
29	Agere_81:4c:b8	Cisco_c8:d6:90	59	d TLSv1	Certificate, Client Key Excha
30	Cisco_c8:d6:90	Agere_81:4c:b8	57	d TLSv1	Change Cipher Spec, Encrypted
31	Agere_81:4c:b8	Cisco_c8:d6:90	60	d TLSv1	Application Data
32	Cisco_c8:d6:90	Agere_81:4c:b8	58	d TLSv1	Application Data, Application
33	Agere_81:4c:b8	Cisco_c8:d6:90	59	d EAP	Response, EAP-TTLS [Funk]
34	Cisco_c8:d6:90	Agere_81:4c:b8	57	d EAP	Success
35	Cisco_c8:d6:90	Agere_81:4c:b8	57	d EAPOL	Key
36	Cisco_c8:d6:90	Agere_81:4c:b8	57	d EAPOL	Key
37	Cisco_ee:11:45	Agere_81:4c:b8	57	d IEEE 802.11	Data, SN=327, FN=0
38	Cisco_ee:11:45	Agere_81:4c:b8	56	d IEEE 802.11	Data, SN=347, FN=0



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

Skippy and RTP 01.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: **skippy or rtp** Expression... Clear Apply

No Wireless Interface Found | 802.11 Channel: | FCS Filter: | Decryption Mode: None | Wireless Settings... Decryption Keys...

No.	Source	Destination	Protocol	Delta Time	Relative	Info
3591	130.177.88.69	130.177.80.135	SKIPPY	0.000008	42.426451	SetLampMessage
3593	130.177.88.69	130.177.80.135	SKIPPY	0.000018	42.426469	ClearPromptStatusMessage
3594	130.177.88.69	130.177.80.135	SKIPPY	0.000014	42.426483	CallStateMessage
3596	130.177.88.69	130.177.80.135	SKIPPY	0.000171	42.426654	SelectSoftKeysMessage
3597	130.177.88.69	130.177.80.135	SKIPPY	0.000243	42.426897	DefineTimeDate
3599	130.177.88.69	130.177.80.135	SKIPPY	0.000020	42.426917	SetSpeakerModeMessage
3600	130.177.88.69	130.177.80.135	SKIPPY	0.000008	42.426925	SetRingerMessage
3602	130.177.88.77	130.177.80.135	RTP	0.011470	42.438395	Payload type=ITU-T G.729
3603	130.177.80.135	130.177.88.77	RTP	0.001430	42.439825	Payload type=ITU-T G.729
3605	130.177.80.135	130.177.88.77	RTP	0.020025	42.459850	Payload type=ITU-T G.729
3606	130.177.80.135	130.177.88.77	RTP	0.020037	42.479887	Payload type=ITU-T G.729

Skippy Client Control Protocol

- Data Length: 16
- Reserved: 0x00000000
- Message ID: SetLampMessage (0x00000086)
- Stimulus: Line (0x00000009)
- StimulusInstance: 1
- LampMode: Off (1)

Analysing VoIP protocols

The screenshot shows a Wireshark capture of SIP traffic. The filter is set to 'sip'. The packet list shows several SIP messages between 192.168.1.2 and 212.242.33.35. The details pane shows the structure of an INVITE message.

No.	Source	Destination	Protocol	Info
321	192.168.1.2	212.242.33.35	SIP/SDP	Request: INVITE sip:0097239287044@sip.cybercity.dk
323	192.168.1.2	212.242.33.35	SIP/SDP	Request: INVITE sip:0097239287044@sip.cybercity.dk
325	192.168.1.2	212.242.33.35	SIP/SDP	Request: INVITE sip:0097239287044@sip.cybercity.dk
326	212.242.33.35	192.168.1.2	SIP	Status: 407 authentication required
327	192.168.1.2	212.242.33.35	SIP	Request: ACK sip:0097239287044@sip.cybercity.dk
346	192.168.1.2	212.242.33.35	SIP/SDP	Request: INVITE sip:0097239287044@sip.cybercity.dk
348	212.242.33.35	192.168.1.2	SIP	Status: 403 Wrong password or domain
349	192.168.1.2	212.242.33.35	SIP	Request: ACK sip:0097239287044@sip.cybercity.dk
421	192.168.1.2	212.242.33.35	SIP	Request: REGISTER sip:sip.cybercity.dk
422	212.242.33.35	192.168.1.2	SIP	Status: 401 Unauthorized (0 bindings)
430	192.168.1.2	212.242.33.35	SIP	Request: REGISTER sip:sip.cybercity.dk

Session Initiation Protocol

- Request-Line: INVITE sip:0097239287044@sip.cybercity.dk SIP/2.0
 - Method: INVITE
 - [Resent Packet: False]
- Message Header
 - Via: SIP/2.0/UDP 192.168.1.2:5060 ;branch=z9hG4bKnp85213694-430aa1de192.168.1.2 ;rport
 - Transport: UDP
 - Sent-by Address: 192.168.1.2
 - Sent-by port: 5060
 - Branch: z9hG4bKnp85213694-430aa1de192.168.1.2

Analysing VoIP protocols

SIP_CALL_RTP_G711 - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: mgcp

No.	Source	Destination	Protocol	Info
492	200.57.7.202	200.57.7.195	MGCP	RSIP 12218 aaln/4@CPG2 MGCP 1.0 NCS 1.0
493	200.57.7.195	200.57.7.202	MGCP	400 12218 OK
546	200.57.7.195	200.57.7.202	MGCP	AUEP 10506 aaln/1@cpg2 MGCP 1.0 NCS 1.0
547	200.57.7.202	200.57.7.195	MGCP	200 10506 OK
548	200.57.7.195	200.57.7.202	MGCP	AUEP 10507 aaln/1@cpg1 MGCP 1.0 NCS 1.0
549	200.57.7.202	200.57.7.195	MGCP	200 10507 OK
1754	200.57.7.202	200.57.7.195	MGCP	NTFY 12219 aaln/1@CPG2 MGCP 1.0 NCS 1.0
1756	200.57.7.195	200.57.7.202	MGCP	200 12219 OK
1758	200.57.7.195	200.57.7.202	MGCP	RQNT 10508 aaln/1@cpg2 MGCP 1.0 NCS 1.0
1759	200.57.7.195	200.57.7.202	MGCP	RQNT 10509 aaln/1@cpg2 MGCP 1.0 NCS 1.0
1760	200.57.7.202	200.57.7.195	MGCP	200 10508 OK

Media Gateway Control Protocol

RSIP (RestartInProgress)
 Transaction ID: 12218
 Endpoint: aaln/4@CPG2
 Version: MGCP 1.0 NCS 1.0
[\[The response to this request is in frame 493\]](#)

Parameters
 RestartMethod (RM): restart

Wireshark expert system

The screenshot displays the Wireshark interface for a file named 'TCP Errors 01.pcap'. The main window is divided into three panes: the top pane shows a list of 15 packets, the middle pane shows the details of the selected packet (User Datagram Protocol), and the bottom pane shows the expert info window.

Packet List:

No.	Source
1	10.10.10.75
2	10.10.10.76
3	10.10.10.75
4	standards.ieee
5	10.10.10.75
6	10.10.10.75
7	standards.ieee 10.10.10.75
8	standards.ieee 10.10.10.75
9	10.10.10.75 standards.ieee
10	standards.ieee 10.10.10.75
11	standards.ieee 10.10.10.75
12	10.10.10.75 standards.ieee
13	standards.ieee 10.10.10.75
14	standards.ieee 10.10.10.75
15	10.10.10.75 standards.ieee

Packet Details (User Datagram Protocol):

- Source port: 4666 (4666)
- Destination port: domain (53)
- Length: 44

Expert Info Window (176 Expert Infos):

Errors: 0 Warnings: 7 Notes: 163 Chats: 6 Severity filter: Error+Warn+Note+Chat

No.	Sever.	Group	Protocol	Summary
3	Chat	Sequence	TCP	Connection establish request (SYN): server port http
4	Chat	Sequence	TCP	Connection establish acknowledge (SYN+ACK): server port http
6	Chat	Sequence	HTTP	GET /regauth/oui/oui.txt HTTP/1.1\r\n
277	Warn	Sequence	TCP	Previous segment lost (common at capture start)
278	Note	Sequence	TCP	Duplicate ACK (#1)
280	Note	Sequence	TCP	Duplicate ACK (#2)
282	Note	Sequence	TCP	Duplicate ACK (#3)
284	Note	Sequence	TCP	Duplicate ACK (#4)
286	Note	Sequence	TCP	Duplicate ACK (#5)
288	Note	Sequence	TCP	Duplicate ACK (#6)
290	Note	Sequence	TCP	Duplicate ACK (#7)
291	Warn	Sequence	TCP	Previous segment lost (common at capture start)
292	Note	Sequence	TCP	Duplicate ACK (#8)
294	Note	Sequence	TCP	Duplicate ACK (#9)
296	Note	Sequence	TCP	Duplicate ACK (#10)
298	Note	Sequence	TCP	Duplicate ACK (#11)
300	Note	Sequence	TCP	Duplicate ACK (#12)
302	Note	Sequence	TCP	Duplicate ACK (#13)
304	Note	Sequence	TCP	Duplicate ACK (#14)
306	Note	Sequence	TCP	Duplicate ACK (#15)
308	Note	Sequence	TCP	Duplicate ACK (#16)
310	Note	Sequence	TCP	Duplicate ACK (#17)
312	Note	Sequence	TCP	Duplicate ACK (#18)
314	Note	Sequence	TCP	Duplicate ACK (#19)
316	Note	Sequence	TCP	Duplicate ACK (#20)
318	Note	Sequence	TCP	Duplicate ACK (#21)
320	Note	Sequence	TCP	Duplicate ACK (#22)

Wireshark expert system

The screenshot displays the Wireshark interface with several windows open. The main window shows a packet list with a filter applied. A 'Wireshark: Flow Graph' dialog is open, allowing selection of packets and flow types. A 'Graph Analysis' window is also open, showing a detailed view of a TCP flow with a sequence of ACK and PSH, ACK packets. The packet list shows a sequence of packets from 272 to 286, with a detailed view of a Transmission Control Protocol segment.

Wireshark: Flow Graph

Choose packets:
 All packets Displayed packets

Choose flow type:
 General flow ICP flow

Choose node address type:
 Standard source/destination addresses Network source/destination addresses

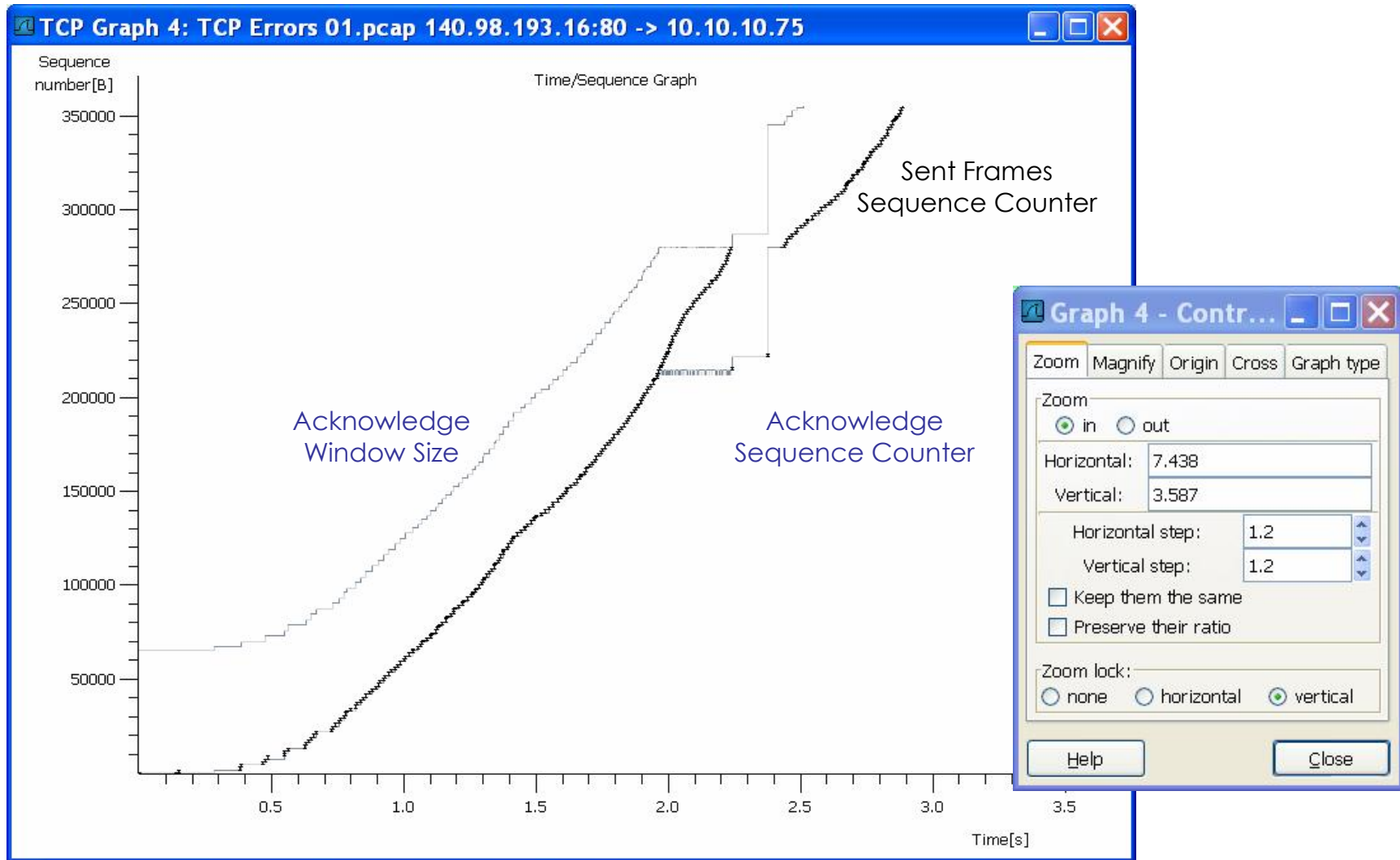
Graph Analysis

Time	10.10.10.75	standards.ieee.or	Comment
2.011	(4667)	(80)	Seq = 485 Ack = 208568
2.015	(4667)	(80)	Seq = 208568 Ack = 485
2.017	(4667)	(80)	Seq = 209543 Ack = 485
2.018	(4667)	(80)	Seq = 485 Ack = 210028
2.025	(4667)	(80)	Seq = 210028 Ack = 485
2.026	(4667)	(80)	Seq = 211487 Ack = 485
2.026	(4667)	(80)	Seq = 485 Ack = 211488
2.029	(4667)	(80)	Seq = 211488 Ack = 485
2.034	(4667)	(80)	Seq = 212948 Ack = 485
2.034	(4667)	(80)	Seq = 485 Ack = 214407
2.039	(4667)	(80)	Seq = 214408 Ack = 485
2.039	(4667)	(80)	Seq = 485 Ack = 214407
2.042	(4667)	(80)	Seq = 215868 Ack = 485
2.042	(4667)	(80)	Seq = 485 Ack = 214407
2.044	(4667)	(80)	Seq = 216843 Ack = 485
2.044	(4667)	(80)	Seq = 485 Ack = 214407
2.049	(4667)	(80)	Seq = 217328 Ack = 485

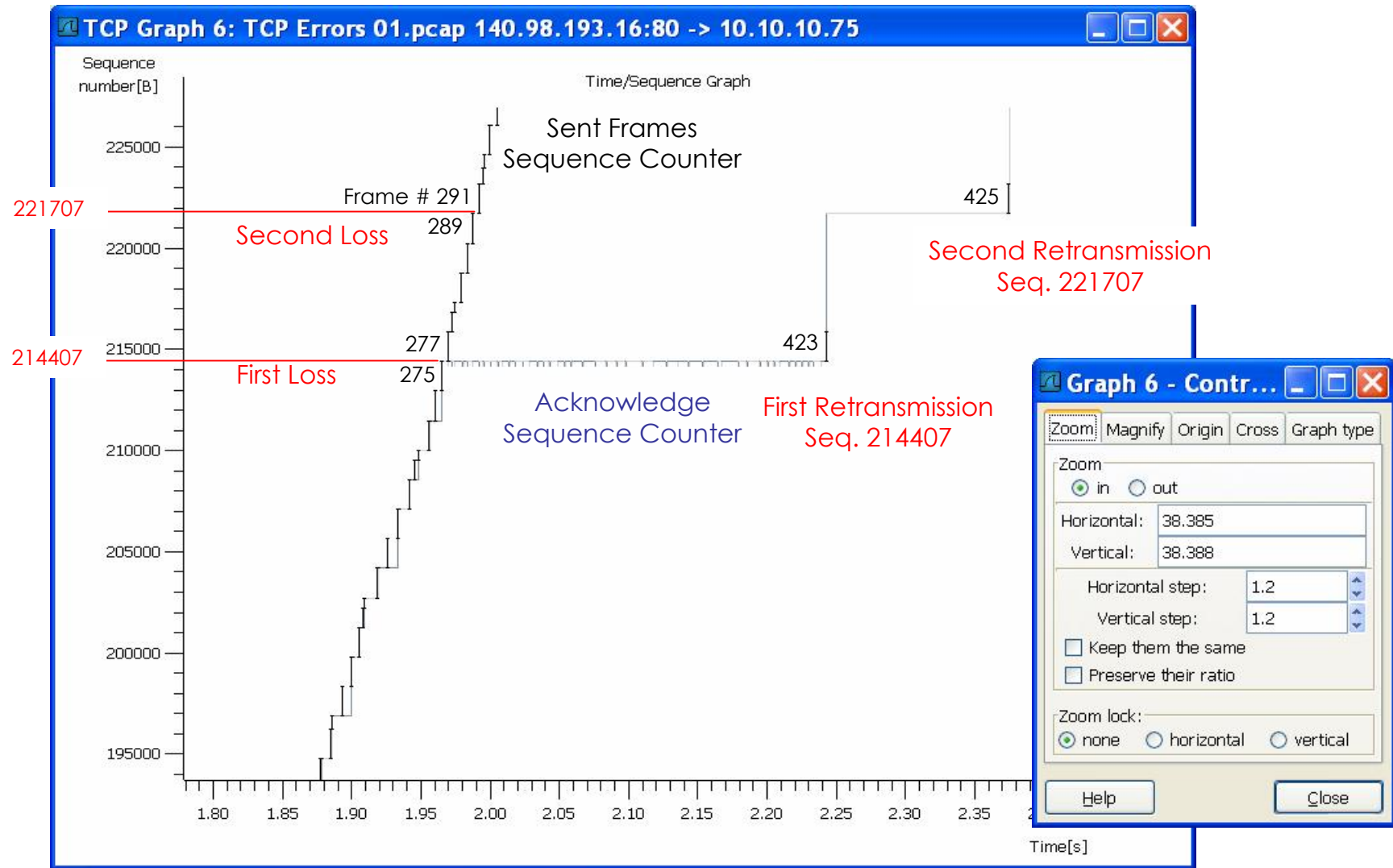
Transmission Control Protocol, Src...

Source port: http (80)
Destination port: 4667 (4667)
Sequence number: 214408 (rela...

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 802.11 b/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