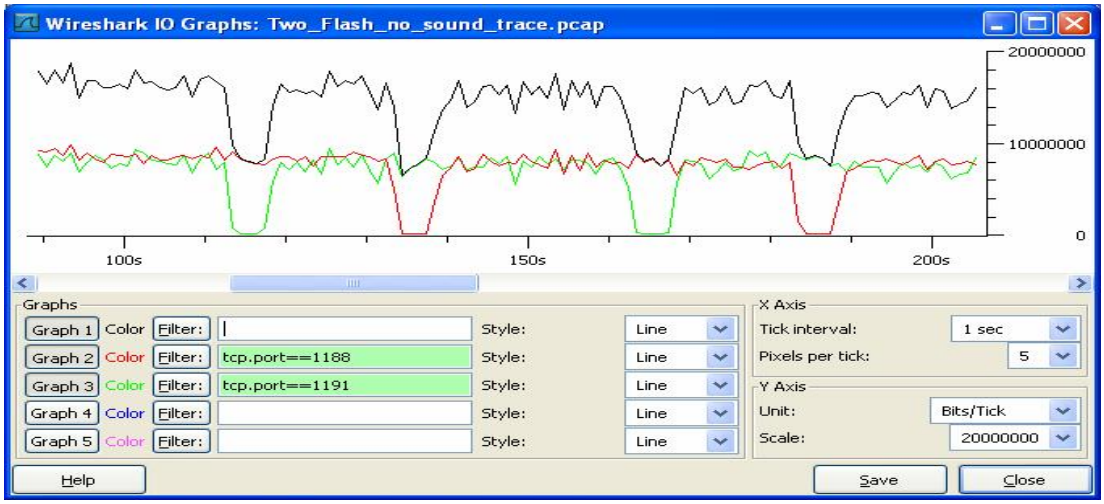
LEUTERT NetServices

WIRESHARK NEWSLETTER Januar 2008

Dies ist der erste des von nun an regelmässig erscheinenden Wireshark Newsletters von Leutert NetServices. Er informiert Sie in Kürze über wichtige Neuerungen im Zusammenhang mit dem führenden Open-Source Analyser Wireshark.

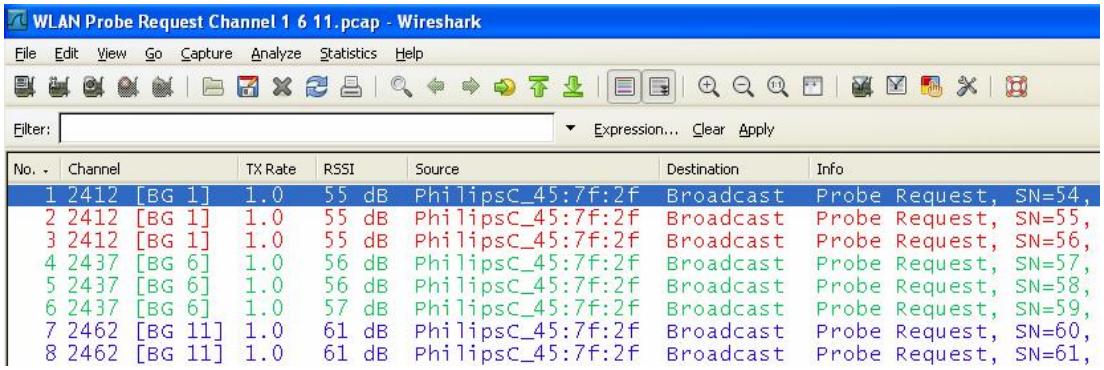
Neue Features der Wireshark Version 0.99.7 (erhältlich seit 18.12.07)
Dies ist nur eine Auswahl der Neuerungen, sämtliche Details inklusive Informationen über Bugfixes finden Sie im Release Note auf http://www.wireshark.org/

- Die beliebte Funktion **IO Graphs** hat neue Display Optionen und die Grafik lässt sich nun in verschiedenen Bildformaten (png, bmp, jpec etc.) exportieren.



Leider werden die Filtersettings nicht kopiert, dazu verwendet man weiterhin ein Screencopy-Tool wie z.B SnagIt. (Übrigens, haben Sie's schon mal probiert: IO Graphs läuft auch live während der Aufzeichnung und ergibt einen guten Überblick über die aktuelle Lastkurve auf dem Netz!)

- Bei der Analyse von **WLAN** mit **AirPcap** besteht neu die Möglichkeit die **Channel-No** pro Frame in einer Kolonne direkt im Packet-List Window anzuzeigen:



LEUTERT NetServices
Phone +41 79 430 55 23
leutert@wireshark.ch
www.wireshark.ch
Steigstrasse 28
CH-8307 Effretikon

- Neu ist auch die Funktion **Follow UDP-Stream**, funktioniert gleich wie Follow TCP-Stream.
- Einzelne **Coloring Rules** können neu temporär ausgeschaltet werden, ohne dass sie wie bisher gelöscht werden müssen.
- Gefiltert werden kann neu beim **SNMP** direkt auf den **OID** (Object Identifier).

- **Neu decodierte Protokolle** (neben zahlreichen Erweiterungen von bereits decodierten):

ANSI TCAP, application/xcap-error (MIME type), CFM, DPNSS, EtherCAT, ETSI e2/e4, H.282, H.460, H.501, IEEE 802.1ad and 802.1ah, IMF (RFC 2822), RSL, SABP, T.125, TNEF, TPNCP, UNISTIM, Wake on LAN, WiMAX ASN Control Plane, X.224

- Im Moment noch inoffiziell verfügbar von Leutert NetServices ist eine Version von Wireshark welche Aufzeichnung über einen **InfiniBand Adpater** decodiert. Bitte setzen Sie sich bei Bedarf mit uns in Verbindung.

Weitere interessante Infos:

Vom 31. März bis 2. April 08 findet im Foothill College, Los Altos Hills, California das **SHARKFEST ´08**, die erste Wireshark Developer- und User-Konferenz statt. Es erwarten Sie viele interessante Beiträge zu den Themen Network Analysis, Troubleshooting, Security usw.
Im Anhang finden Sie die detallierte Sharkfest Agenda.

Rolf Leutert von Leutert NetServices wird dort eine Session über die Analyse des neuen Standards **WLAN 802.11n (MIMO)** mit dem AirPcap N Adapter präsentieren. Es würde uns freuen Sie dort begrüssen zu dürfen. Mehr Details finden Sie unter: http://www.cacetech.com/SHARKFEST.08/

Der erste **Wireshark VoIP Analyse Kurs** von Leutert NetServices findet am 28./29. Januar 2008 an der Hochschule für Technik Rapperswil statt. Es sind noch Plätze frei, Details und Anmeldung unter: http://www.mylearning.ch/voip/sniffer/

Ab diesem Jahr finden Wireshark Kurse von Leutert NetServices neu auch in **Österreich**, **Neuseeland** und **Australien** statt, bitte melden Sie sich bei Bedarf bei uns.

Die öffentlichen Wireshark Kurse TCP/IP und WLAN finden weiterhin bei **Comicro-Netsys** statt. Details und Anmeldung unter: http://www.comicro.ch/g3.cms/s_page/51000

Soviel für den Moment, wir wünschen Ihnen ein erfolgreiches 2008 und viele 'conclusive Traces' mit Wireshark.

Mit freundlichen Grüssen
Rolf Leutert / Leutert NetServices
Januar 2008

LEUTERT NetServices
Phone +41 79 430 55 23
leutert@wireshark.ch
www.wireshark.ch
Steigstrasse 28
CH-8307 Effretikon

LEUTERT NetServices

SHARKFEST '08 AGENDA March 31st – April 2nd | Foothill College | Los Altos Hills, CA

Monday March 31	Developer Track	Track 1	Track 2
8:00am - 9:00am	Continental Breakfast		
9:00am - 10:15am	Welcome Keynote Opening Remarks: John Bruno, CACE Technologies CEO Presenters: Gerald Combs, Wireshark Creator, Loris Degioanni, AirPcap Creator, Gianluca Varenni, WinPcap Master, Laura Chappell, Founder, Protocol Analysis Institute and Wireshark University		
10:15am - 10:30am	*Break*	*Break*	*Break*
10:30am - 12:00pm	Hackathon Kickoff with Gerald Combs, Dir. of Open Source Projects, CACE Technologies	T1-1 I've downloaded Wireshark...Now what? Instructor: Betty DuBois, Wireshark U	T2-1 Analyzer Placement and Baseline Techniques Instructor: Tony Fortunato, Wireshark U
12:00pm - 12:45pm	*Lunch*	*Lunch*	*Lunch*
12:45pm - 2:00pm	D01 Advanced Scripting and Command Line Usage with tshark and Related Utilities Instructor: Sake Blok , Wireshark Core Developer	T1-2 The Virtue of Continuous, Complete Packet Capture &Stream-to-Storage for Enhanced Network Forensics Capability Instructor: Paal Tveit, VP of Engineering, Solera Networks	T2-2 Analyzing the TCP/IP Resolution Processes - Port, Name, Route and Hardware Address Resolution Instructor: Laura Chappell, WSU
2:00pm - 2:15pm	*Break*	*Break*	*Break*
2:15pm - 3:30pm	D02 Writing Your Own Wireshark Packet Dissectors - INTRODUCTION Instructor:TBD	T1-3 Case Studies: Solving Network Performance Problems with Wireshark Instructor: Laura Chappell, WSU	T2-3 Legal Issues of Packet Analysis Instructor: Jimmy Garcia, Supervisor, High Tech Investigation Division, Los Angeles Office of the District Attorney
3:30pm - 3:45pm	*Break*	*Break*	*Break*
3:45pm - 5:00pm	D03 Writing Your Own Wireshark Packet Dissectors - ADVANCED Instructor: Guy Harris, Wireshark Core Developer	T1-4 Expose VOIP Problems Using Wireshark Instructor: Sean Walberg	T2-4 Trace File Analysis - Identifying Wire Latency, Client Latency and Server Latency Issues (Includes Charting Techniques) Instructor: Laura Chappell, WSU
6:00pm - 7:00pm	Internet Safety for Kids: Predator Tactics, Classification and Protection		

LEUTERT NetServices

SHARKFEST '08 AGENDA March 31st – April 2nd | Foothill College | Los Altos Hills, CA

Tuesday April 1	Developer Track	Track 1	Track 2
8:00am - 9:00am	Continental Breakfast		
9:00am - 10:15am	D04 Writing your own Packet Capture Tool with WinPcap and AirPcap - Part 1 Instructor: Gianluca Varenni, Developer and WinPcap Maestro, CACE Technologies	T1-5 Introduction to WLAN Analysis Instructor: Joe Bardwell, Founder, Connect 802 Corporation	T2-5 Advanced Capture and Display Filtering Instructor: Tony Fortunato, WSU
10:15am - 10:30am	*Break*	*Break*	*Break*
10:30am - 12:00pm	D05 Analysing WLAN 802.11N MIMO with AirPcap N Instructor: Rolf Leutert, Leutert NetServices	T1-6 Tutorial: Leveraging Wireshark for Wireless Network Analysis using AirPcap Instructor: Joshua Wright, Aruba	T2-6 Trace File Analysis - The Elephant Coming From Behind: Full Window, Window Update and TCP Keepalives Instructor: Betty DuBois, WSU
12:00pm - 12:45pm	*Lunch*	*Lunch*	*Lunch*
12:45pm - 2:00pm	D06 802.11 Packet Dissection with AirPcap and WinPcap Instructor: Dustin Johnson, Developer, CACE Technologies	T1-7 WLAN Analysis & Security Instructor: Thomas D'Otreppe, Aircrack-NG Creator	T2-7 An Introduction to Network Forensics - Identifying Reconnaissance and Attacks on the Network Instructor: Laura Chappell, WSU
2:00pm - 2:15pm	*Break*	*Break*	*Break*
2:15pm - 3:30pm	D07 Programming and Extending the Wireshark User Interface Presenter: Ulf Lamping, Wireshark Core Developer	T1-8 Non-Intrusive Out-of-Band Network Monitoring utilizing a Data Access Switch Instructor: Patrick Leong, CTO, Gigamon Systems LLC	T2-8 Trace File Analysis - Packet Loss, Retransmissions, Fast Retransmissions, Duplicate ACKs, ACK Lost Segment and Out-of-Order Packets (Includes Charting Techniques) Instructor: Laura Chappell, WSU
3:30pm - 3:45pm	*Break*	*Break*	*Break*
3:45pm - 5:00pm	Birds of a Feather Session WinPcap Do's and Don'ts Moderator: Gianluca Varenni, CACE	T1-9 Wireshark Enhancement Product SURPRISE Presentation!	T2-9 Top 10 Tips and Tasks Instructor: Betty DuBois, WSU

LEUTERT NetServices
Phone +41 79 430 55 23
leutert@wireshark.ch
www.wireshark.ch
Steigstrasse 28
CH-8307 Effretikon

LEUTERT NetServices

SHARKFEST '08 AGENDA March 31st – April 2nd | Foothill College | Los Altos Hills, CA

Wednesday April 2	Developer Track	Track 1	Track 2
8:00am - 9:00am	Continental Breakfast		
9:00am - 10:15am	Roundtable R01 Trace File Formats and Packet Meta Information Moderator: Gianluca Varenni, CACE Technologies	T1-10 Expose VOIP Problems Using Wireshark Instructor: Sean Walberg	T2-10 Trace File Analysis - Case Studies: Samples of Wireshark in Action Instructor: Betty DuBois, WSU
10:15am - 10:30am	*Break*	*Break*	*Break*
10:30am - 12:00pm	D08 Advanced HTTP, SSL, and SMB Analysis Instructor: Ronnie Sahlberg, Wireshark Core Developer	T1-11 WLAN Analysis & Security Instructor: Mike Kershaw, Kismet Creator	T2-11 Trace File Analysis - Analyzing HTTP Traffic Behavior (Commands, Responses, Data Reassembly, Reporting) Instructor: Tony Fortunato, WSU
12:00pm - 12:45pm	*Lunch*	*Lunch*	*Lunch*
12:45pm - 2:00pm	Panel Discussion R02 The Future of Open Source Network Tools Panel Moderator: Mike Pennachi, Network Protocol Specialists, LLC Panel Participants: Fyodor, Founder, insecure.org CEO, PacketTrap Loris Degioanni, CTO, CACETechnologies	T1-12 SCTP/SIGTRAN & SSL Protocol Overview Instructor: Michael Tuexen, Wireshark Core Developer	T2-12 Complementary Tools - Honeypots, Keyloggers, Host Forensic Tools, etc. Instructor: Laura Chappell, WSU
2:00pm - 2:15pm	*Break*	*Break*	*Break*
2:15pm - 3:30pm	D09 File & Disk-Sharing Protocols Instructor: Richard Sharpe, Wireshark Core Developer	T1-13 Tapping Basics Instructor: Chris Bihary, Network Critical	T2-13 Trace File Analysis - Infected Systems (Worms, Backdoors, etc.) Instructor: Laura Chappell, WSU
3:30pm - 3:45pm	*Break*	*Break*	*Break*
3:45pm - 5:00pm	Roundtable R03 Wireshark Roadmap Moderator: Gerald Combs, Director, Open Source Projects, CACE Technologies	T1-14 Birds of a Feather Session: Wireshark in the Enterprise Moderator: Sebastian Tandel, Wireshark Core Developer	CONFERENCE ENDS