WIRESHARK NEWSLETTER April 2008
Spezialausgabe SHARKFEST'08 in Los Altos, California

Dieser Wireshark Newsletters von Leutert NetServices informiert Sie regelmässig in Kürze über wichtige Neuerungen im Zusammenhang mit dem führenden Open-Source-Analyser Wireshark.

Der erste Teil dieses Newsletters berichtet über das **SHARKFEST'08**, der zweite Teil enthält die übliche Zusammenfassung und graphische Darstellungen über neue Funktionen in der Wireshark Version 1.0.

SHARKFEST'08

Sie wurde von vielen Fachleuten mit Spannung und Interesse erwartet, die erste Wireshark Developer- und User-Konferenz, welche vom 31. März bis 2. April 08 stattfand, und um es vorweg zu nehmen: Sie war ein voller Erfolg. Im malerischen Foothill College, Los Altos Hills, California, trafen sich Core-Entwickler, Network Analyse Gurus, Trainer und Anwender zu diesem Gipfeltreffen.

Die Anwesenden repräsentierten ein Who's Who der Netzwerkanalyse-Szene:

- Gerald Combs (creator of **Ethereal/Wireshark**)
- Loris Degioanni (creator of **WinPcap**; creator of **Pilot**)
- Gianluca Varenni (creator of **WinPcap**; creator of **TurboCap**)
- Thomas D'Otreppe (creator of the **Aircrack-NG** suite)
- Scott Haugdahl (BitCricket; creator of **PacketScrubber**; former CTO WildPackets)
- Mike Kershaw (creator of **Kismet**)
- Fyodor, aka Gordon Lynn (creator of **NMap**)
- Mike Pennacchi (**packet guru**; Network Protocol Specialist)
- Laura Chappell (Founder of **Wireshark U**)
- Joe Bardwell (**packet guru**; Connect 802)
- John Bruno (CEO of **CACE Technologies**)
- Wireshark **Core Developers** from around the World

Ein besonderes Highlight war auch der Vortrag des Keynote Speakers Dr. **Vinton Cerf**, PhD, Google Vice President and Chief Internet Evangelist, welcher von vielen als Vater des Internets bezeichnet wird.

Neben einem spannenden Rückblick auf die Wireshark/Ethereal-Entstehungsgeschichte wurden viele interessante Details und ein Ausblick in die Zukunft präsentiert – und dies mit viel Humor und der bekannten amerikanischen Lockerheit.

Hier einige Key Figures:

- 9+ years in development
- 600+ developers
- 900+ protocols
- 6 hosting providers
- 3 domains
- 2 names
- 1.5 million lines of code
- 300,000 downloads per month (unglaublich!!!)

Angekündigte Neuerungen und Produkte

Eines steht fest: **Wireshark wird ‚Open Source' bleiben!** Eine Frage/Sorge, die mir häufig zu Ohren kommt, kann damit klar beantwortet werden: Der Geist, von dem dieses erstaunliche Tool getragen wird, ist ungebrochen. Zudem besitzen viele Entwickler weltweit die Rechte an Teilen des Source Codes und würden sich mit allen Mitteln gegen eine Kommerzialisierung von Wireshark zur Wehr setzen.

CACE Technologies (ausgesprochen wie CASE) bildet die Trägerfirma für Wireshark und wird ihren Markt noch vermehrt mit Zusatzservices und –Produkten (wie AirPcap) ausbauen.
Zwei neue Produkte wurden in diesem Zusammenhang angekündigt, welche demnächst auf den Markt kommen werden:

- **PILOT,** eine besonders benutzerfreundliche Software für Visualisierung, Reporting und statistische Darstellung von Wireshark Tracefiles. Integriert mit Wireshark und besonders geeignet für grosse Datenmengen im Bereich von <100MBytes.

- **Gigabit Hardware Adapter** für die Analyse von Gigabit Full/Duplex mit Datenmengen, welche von heutigen Notebooks leistungsmässig nicht verarbeitet werden können.

Ich hatte die Gelegenheit, die Draft-Version von PILOT zu testen und bin erstaunt über die intuitive Benutzerführung dieses Tools. Leutert NetServices wird in einem der nächsten Newsletter im Detail über Bedienung und Funktionalität berichten, sobald diese Produkte erhältlich sein werden.

- **Pcap-NG,** ein neues Format für Trace Files, ist wohl die spannendste Ankündigung was die zukünftigen Möglichkeiten von Wireshark betrifft. Es wird neu möglich sein, neben den reinen Raw-Daten zusätzliche Information vergleichbar zu Meta-Daten abzuspeichern. D.h. dass zum Beispiel Zusatzinformationen wie Resolved DNS Names, Free Text Notations, Filter Settings usw. zusammen mit den Frames gespeichert werden können und damit beim Öffnen des Files wieder zur Verfügung stehen. Dieses Fileformat wird auch das gleichzeitige Aufzeichnen von mehreren Interfaces unterstützen (was beim USB AirPcap Adapter ja bereits möglich ist).

Soviel vom SHARKFEST'08.
Sämtliche **Präsentationen** können im PDF Format herunter geladen werden:
http://www.cacetech.com/SHARKFEST.08/

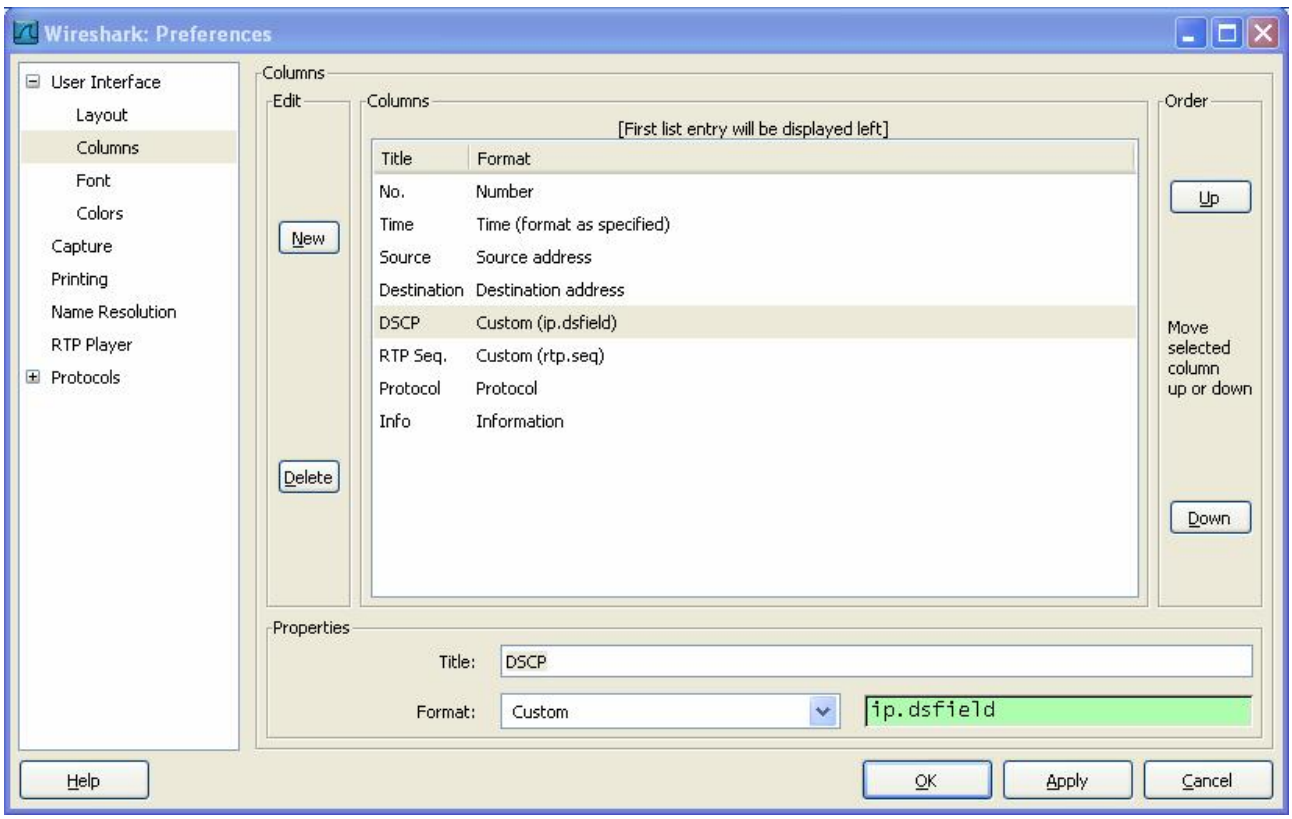
Die Präsentation von Leutert NetServices über **802.11n MIMO Analyse** direkt unter:
D05_Leutert_Analysing 802.11n MIMO.pdf

Neue Features der Wireshark Version 1.0.0 (erhältlich seit 31.3.08)

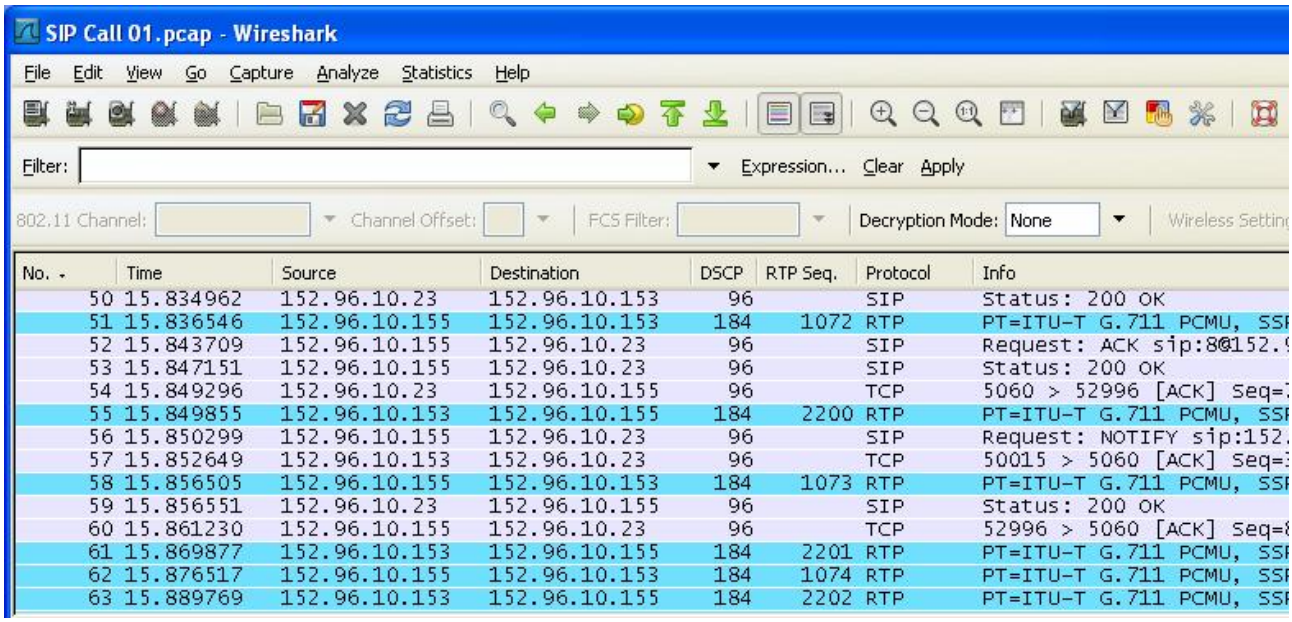
Endlich, nach neun Jahren Entwicklung ist es soweit, die **Version 1.0.0** wurde präzis auf das Datum des SharkFest'08 fertig gestellt. Auch diesmal wurden wieder neben zahlreichen neuen Protokollen auch einige neue Funktionen implementiert, einige ‚kosmetische' Verbesserungen angebracht und einige Schwachstellen korrigiert.

Dies ist nur eine Auswahl der Neuerungen, sämtliche Details inklusive Informationen über Bugfixes finden Sie im Release Note auf http://www.wireshark.org/

- Die neue Funktion **‚Custom Columns'** erlaubt das Darstellen von Werten, welche nicht bereits zur Auswahl für eine Spalte zur Verfügung stehen. Dadurch lassen sich wichtige Variablen für eine spezifische Analyse übersichtlich anzeigen.



In diesem VOIP-Beispiel wurden die Spalten ‚DSCP' für die Priorisierung und die ‚RTP Seq.' Nummern eingefügt:



- **Neu decodierte Protokolle**
  IEEE 802.15.4, Infiniband, Parallel Redundancy Protocol, RedBack Lawful Intercept, Xcsl

- **Erweiterungen an bestehenden Protokollen**
  AFS, ALCAP, ATM, BACapp, CIGI, DCC (renamed from DCCP), DCCP (renamed from DCP), DCERPC SPOOLSS, DCERPC NT, DHCP, DirectPlay, EtherCAT, FIX, GIOP, GTP, H.248, HTTP, ICMPv6, ICQ, IPv6, ISIS, JXTA, NCP, P_Mul, PCAP, PKIX1Explicit, PTP, RADIUS, Roofnet, RTCP, RTMPT, RTP, RX, SABP, SCSI OSD, sFlow, SMPP, SNMP, SSCOP, TAPA, TIPC, TPNCP, UNISTIM, X.25, X.509sat, XML

- **Neues Icon für Trace Files** (um sie nicht mit dem Wireshark Shortcut zu verwechseln)

Soviel für den Moment, viel Erfolg mit Wireshark
Mit freundlichen Grüssen
Rolf Leutert / Leutert NetServices
April 2008