WIRESHARK NEWSLETTER Juli 2008

Dieser Wireshark Newsletter 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 **PILOT,** die neue Software für Statistik und Reporting, der zweite Teil enthält die übliche Zusammenfassung und graphische Darstellungen über neue Funktionen in den Wireshark Versionen 1.0.1 und 1.0.2. sowie einen Hinweis auf die neue Webseite www.wireshark.ch

---

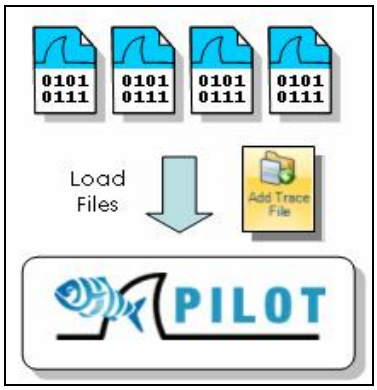
PILOT

"Network Analysis, Visualization and Reporting. Fully integrated with Wireshark™"

Der Name PILOT ist hergeleitet von den Pilotfischen, welche Haie begleiten und umschwärmen. Dies soll auf sinnige Weise die Nähe dieses Tools zu Wireshark symbolisieren.
PILOT erweitert die beschränkten graphischen Darstellungsmöglichkeiten von Wireshark auf ideale Weise und ist besonders geeignet für die statistische Verarbeitung und Erstellung von Reports.

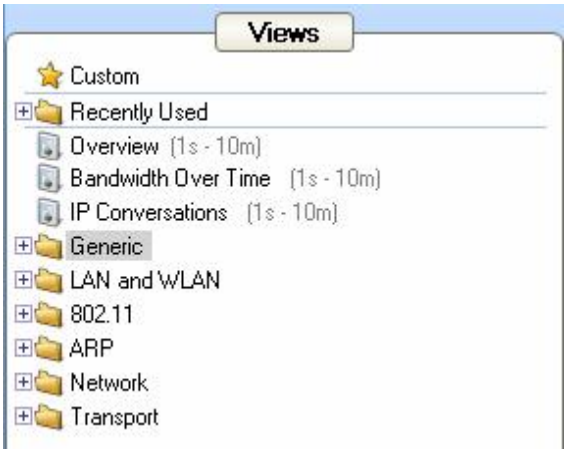
Die Firma **CACE Technologies**, die Trägerfirma von Wireshark, hat eine neue Software für die graphische Bearbeitung und Darstellung von Wireshark Tracefiles entwickelt. Besonderheiten dieses Tools sind die einfache Bedienung, die Integration mit Wireshark, die zahlreichen Reporting-Möglichkeiten und der günstige Preis.

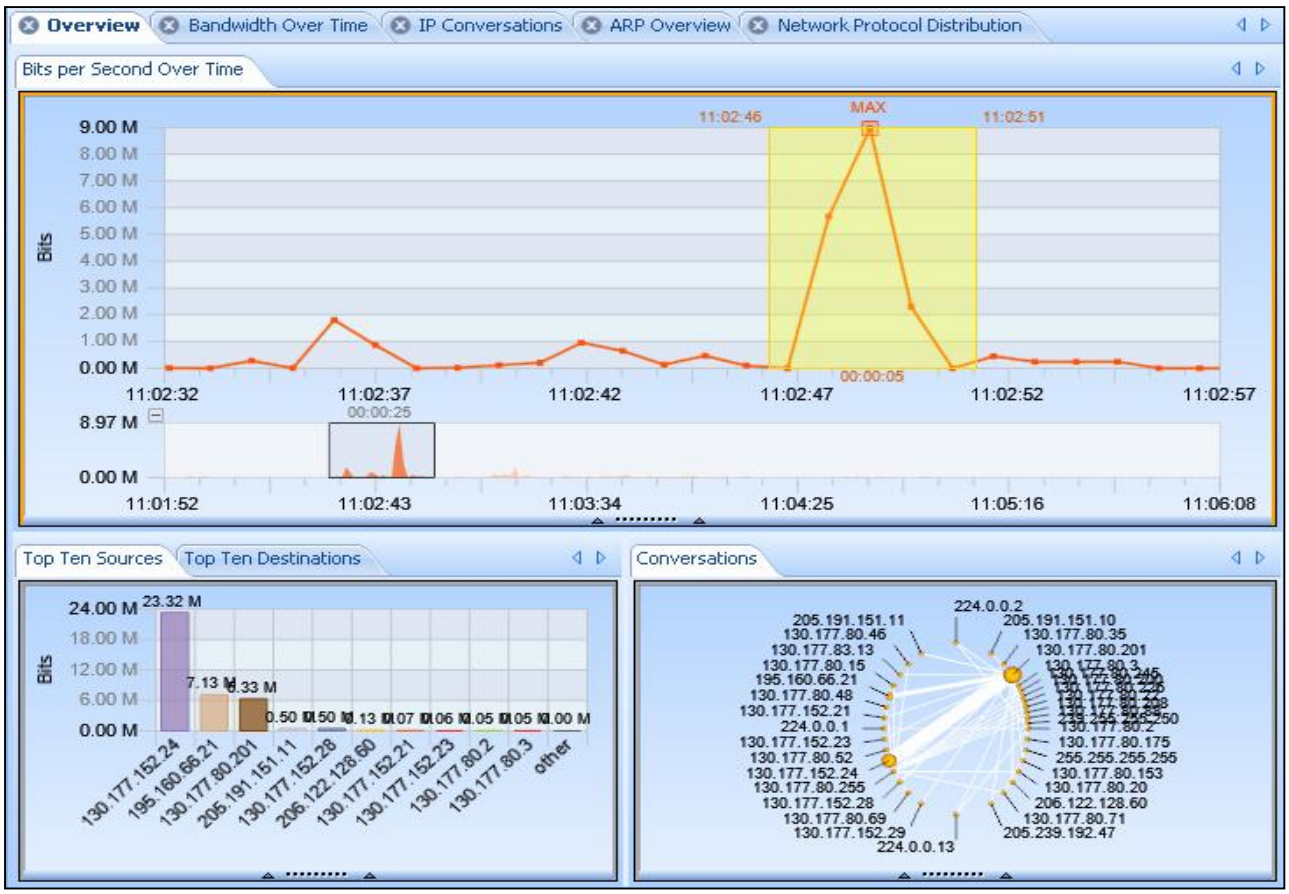
Features



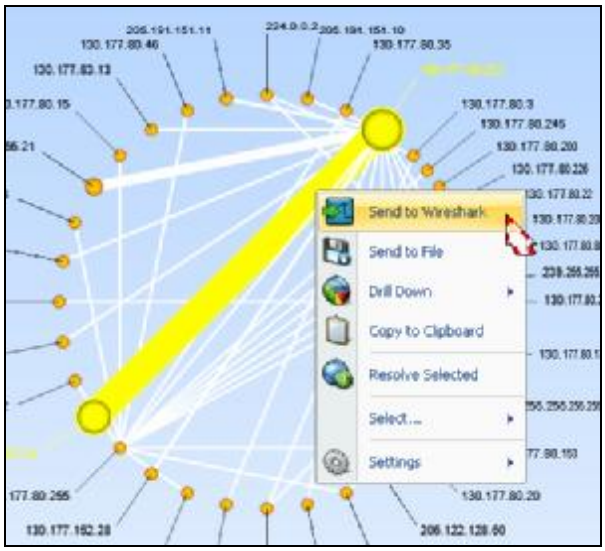
Wireshark Tracefiles werden durch einfaches Click & Drop in die PILOT Software importiert. Eine weitere Möglichkeit ist auch, vom PILOT direkt den Wireshark zu starten und Daten online darzustellen.
PILOT zeigt nicht den detaillierten Inhalt einzelner Datenpakete (dazu dient weiterhin Wireshark), sondern analysiert die wichtigsten Werte wie Adressen (MAC und IP), Framegrössen, Protokolle, Conversations usw. und stellt diese in übersichtlichen Diagrammen dar.

Die so genannten **‚Views'** bilden das Herzstück des PILOTs. Dutzende von Graphs und Charts können auf intuitive Weise auf ein Tracefile gezogen werden, und innert Sekunden wird die entsprechende Darstellung aufgebaut.
Die Anzahl dieser Views wird laufend erweitert werden, die nächste Serie mit Schwerpunkt VLANs ist bereits angekündigt. Dies ermöglicht gezielte Auswertung auf verschiedenen Layers, ohne aufwändige Filter zu setzen.



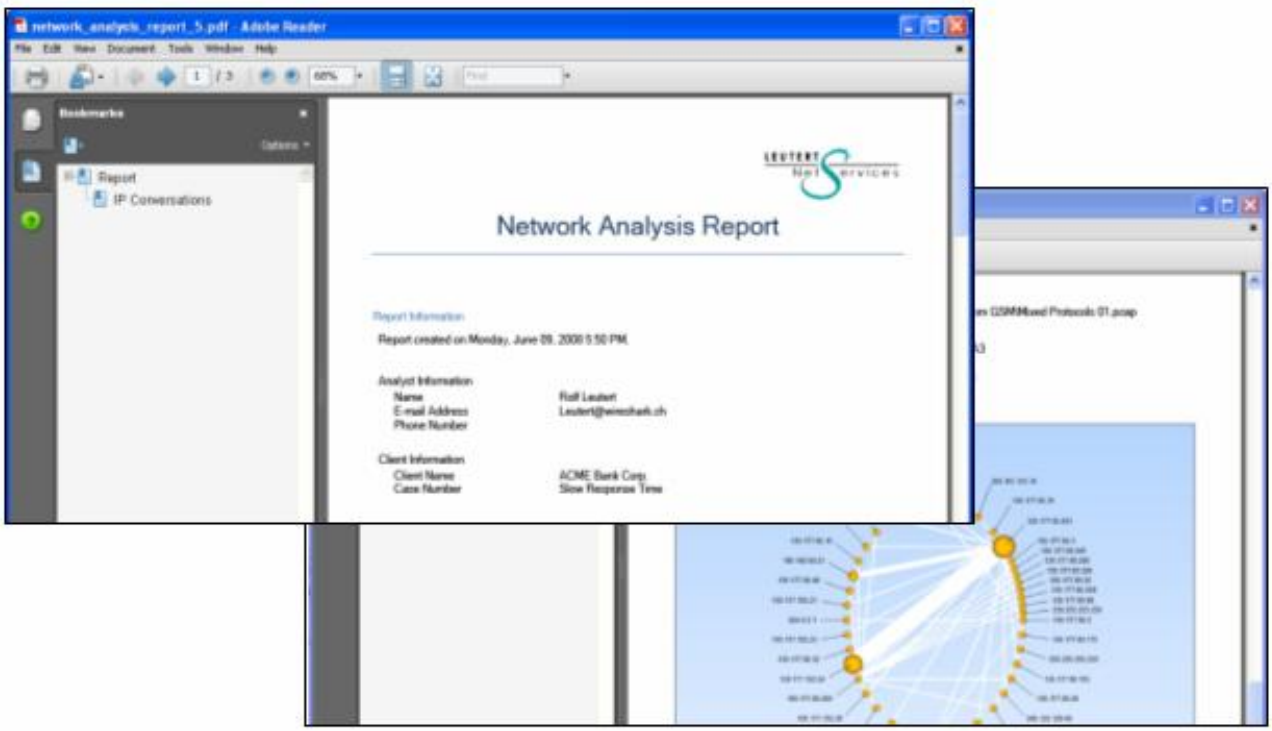


Verschiedene Views wie der Bandbreitenverlauf über die Zeit, Top-Talkers sortiert nach Volumen oder das beliebte Conversation-Kreisdiagramm zeigen im Überblick den Verlauf in einem Tracefile. Aus jedem dieser Diagramme können Bereiche markiert und mit einem Mausklick zur genaueren Analyse an den Wireshark geschickt werden.



Beispiel: Im Kreisdiagramm lässt sich eine bestimmte Conversation markieren. Mit einem rechten Mausklick werden diese Daten vom Wireshark geöffnet, in einem neuen File abgespeichert oder detaillierter untersucht.
Dies dauert selbst bei grossen Datenmengen wie z.B. 500'000 Paketen nur wenige Sekunden. Dieselbe Filter-Funktion kann im Wireshark bis einige Minuten dauern, da sämtliche Frames analysiert werden.
Subnetzmasken können automatisch detektiert oder manuell konfiguriert werden.

PILOT bietet umfangreiche Reporting-Möglichkeiten. Sämtliche Views lassen sich in einem Bericht zusammenfassen und mit Kommentar versehen. Folgende Formate werden unterstützt: PDF Report, ZIP Package, Excel Spreadsheet, Word Document, Text File und HTML Page.



Direkt im PILOT kann das Layout gewählt und das Firmenlogo in den Report kopiert werden.

Dies sind nur einige Highlights aus den umfangreichen Möglichkeiten von PILOT in Verbindung mit Wireshark. Auf der Webseite von CACE Technologies finden Sie weitere Informationen und ein kurzes Intro-Video: http://www.cacetech.com/products/pilot.htm

PILOT ist im Gegensatz zu Wireshark eine kommerziell vertriebene Software, entwickelt von CACE Technologies. Lizenzen werden jedoch im Vergleich zu ähnlichen Produkten zu einem sehr günstigen Preis abgegeben. Die Lizenz wird auf eine Hardware-Plattform limitiert.

Einführungspreise gültig bis September 2008:

PILOT Single-Seat License mit Updates während 12 Monaten CHF 1'320.00
mit Updates während 36 Monaten CHF 1'880.00

PILOT/AirPcap Ex Package (Single-Seat License mit 1 AirPcap EX a/b/g Adapter)
mit Updates während 12 Monaten CHF 1'780.00
mit Updates während 36 Monaten CHF 2'340.00

PILOT/AirPcap Ex 3-Pack Package (Single-Seat License mit 3 AirPcap EX a/b/g Adapter)
mit Updates während 12 Monaten CHF 2'698.00
mit Updates während 36 Monaten CHF 3'259.00

Bestellung auf unserer Webseite www.wireshark.ch
Lieferung und Registrierung von PILOT erfolgen per Internet direkt durch CACE Technologies.
Lieferung von AirPcap Adaptern durch Leutert NetServices. Alle Preise verstehen sich ohne MwSt.

Neue Features der Wireshark Version 1.0.1 und 1.0.2 (erhältlich seit 30.6.08 und 10.7.08)

Die beiden Versionen enthalten vorwiegend ‚Bug Fixes', beheben einige Crash-Situationen und erweitern das Dekodieren von bestehenden Protokollen.

- **Erweiterungen an bestehenden Protokollen**

ACTRACE, BACnet BVLC, BOOTP, E212, iSCSI, IUA, LDAP, MGCP, MIKEY, MSMMS, RMI, RPC, RTCP, RTP, SIP, SNMP, TCP, UNIStim, WiMAX

Neue Webseite von Leutert NetServices und wireshark.ch

Die beiden Webseiten wurden zusammengeführt und übersichtlich gestaltet. Neu besteht auch die Möglichkeit, Produkte wie PILOT, AirPcap und WiSpy Adapter direkt zu bestellen.

Wir freuen uns über Ihren Besuch auf www.wireshark.ch

Mit freundlichen Grüssen Rolf Leutert