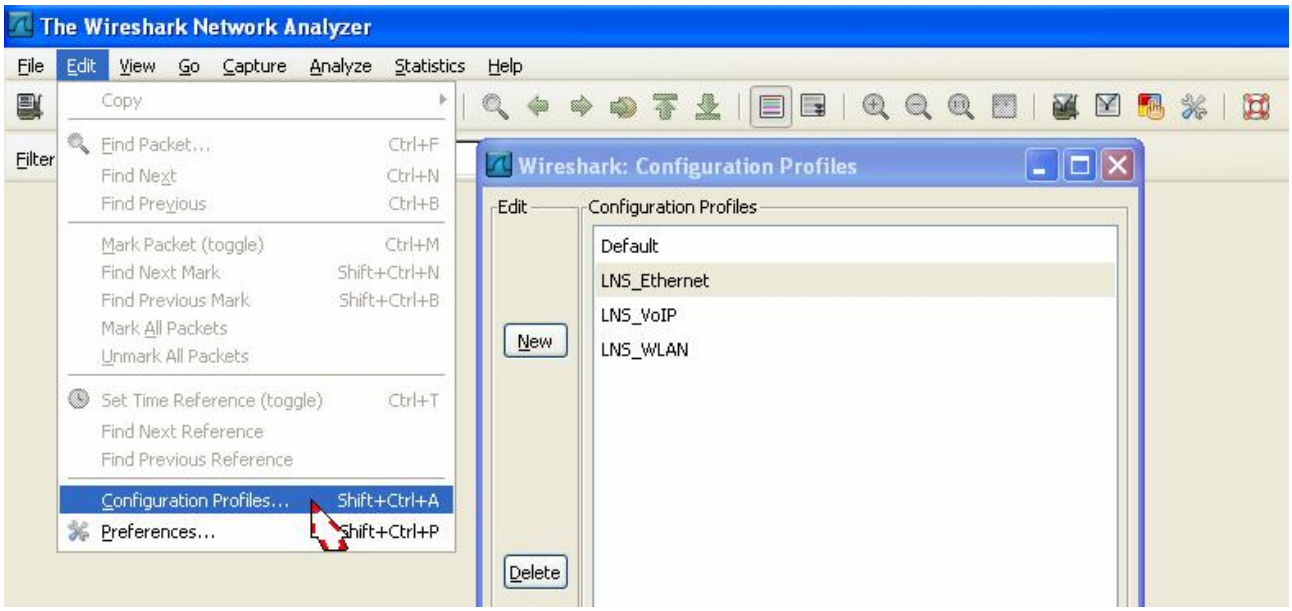
LEUTERT NetServices

WIRESHARK NEWSLETTER März 2008

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

Neue Features der Wireshark Version 0.99.8 (erhältlich seit 27.2.08)
Dies ist nur eine Auswahl der Neuerungen, sämtliche Details inklusive Informationen über Bugfixes finden Sie im Release Note auf http://www.wireshark.org/

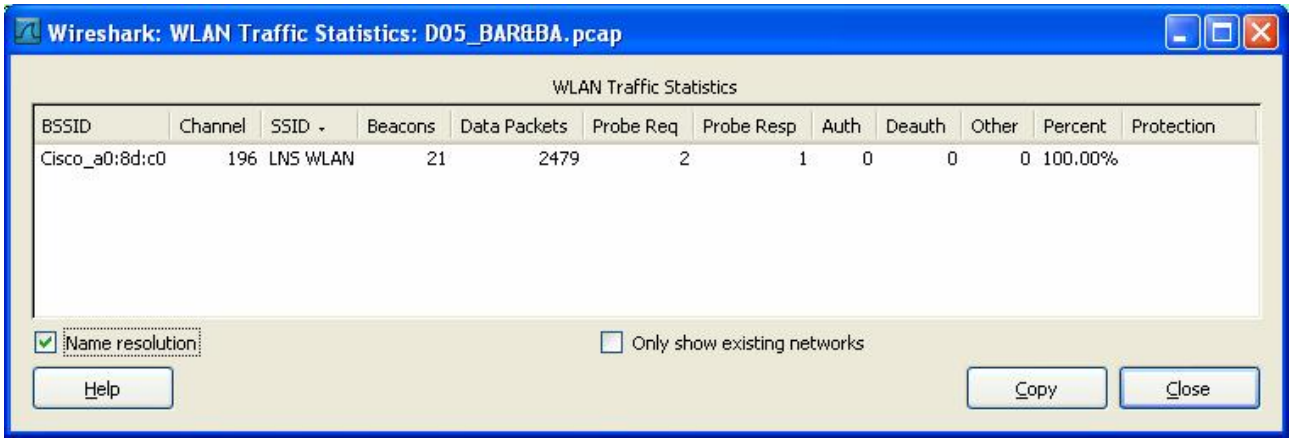
- Die neue Funktion **‚Configuration Profiles'** erlaubt das Abspeichern verschiedener Wireshark Konfigurationen unter frei wählbaren Profil-Namen. Abgespeichert werden alle unter ‚Edit Preferences' vorgenommenen, individuellen Anpassungen wie ‚Columns', Layout, Coloring Rules, Protocol Settings etc. Je nach Anwendung kann so schnell zwischen verschiedenen Profilen gewechselt werden.



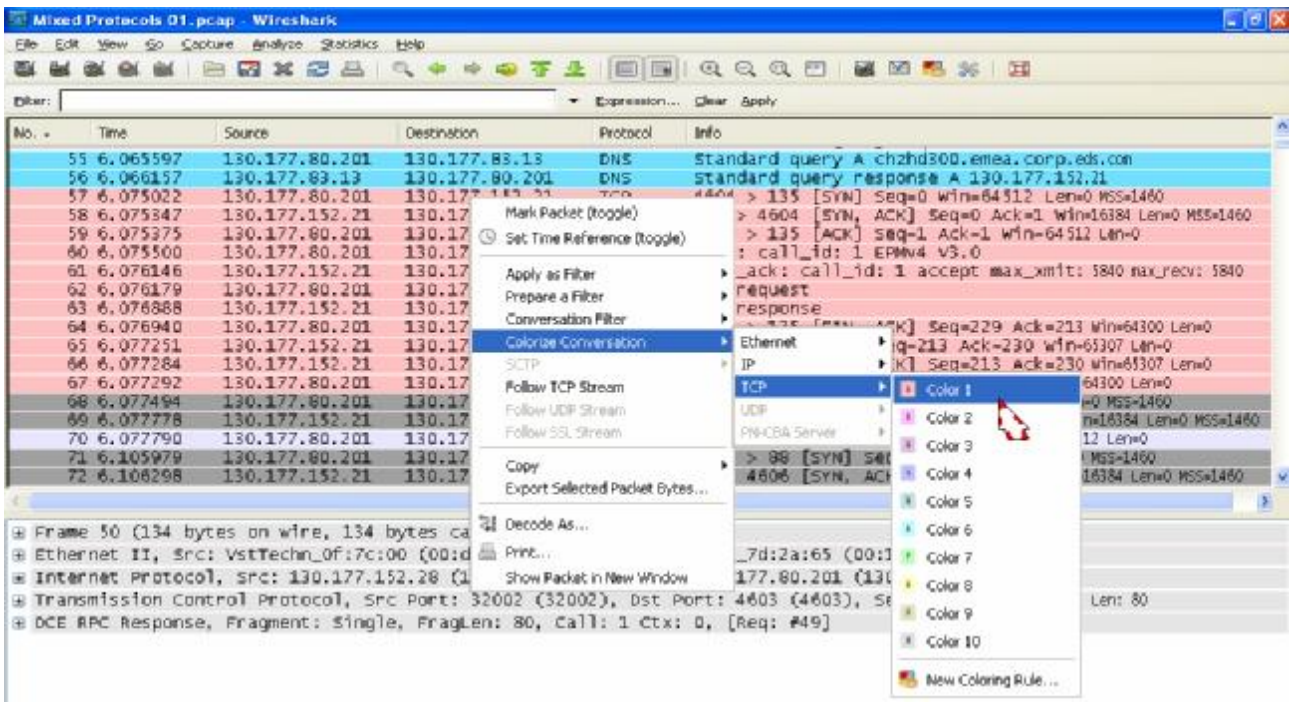
Leider können die Anpassungen, welche Sie eventuell bereits durchgeführt haben, nicht in ein neues Profil abgespeichert werden, da diese dem ‚Default Profile' zugeordnet sind. Es muss zuerst ein neues Profil eröffnet werden (welches mit den Default Einstellungen startet) und die Änderungen dann in diesem Profil vorgenommen werden. (Ein kleiner Zusatzaufwand)

- **Neu decodierte Protokolle** (neben zahlreichen Erweiterungen von bereits decodierten):
AiroPeek Remote Capture, China Mobile Point to Point, Distributed Lock Manager 3, EUTRAN X2 Application Protocol, FOUNDATION Fieldbus, International Passenger Airline Reservation System/Airline Link Control, Microsoft DirectPlay, Path Computation Element communication Protocol, Real Time Messaging Protocol, S1 Application Protocol, Scripting Service Protocol, Societe Internationale de Telecommunications Aeronautiques, Unisys Transmittal System, Wi-fi Protected Setup

Unter **à Statistic à WLAN Traffic** finden Sie eine neue Liste über WLAN Aktivitäten einer oder mehreren Kanälen. Die Statistik zeigt neben der MAC Adressen und SSIDs der Access-Points auch den Anteil der wichtigsten Management- und Daten Frames.

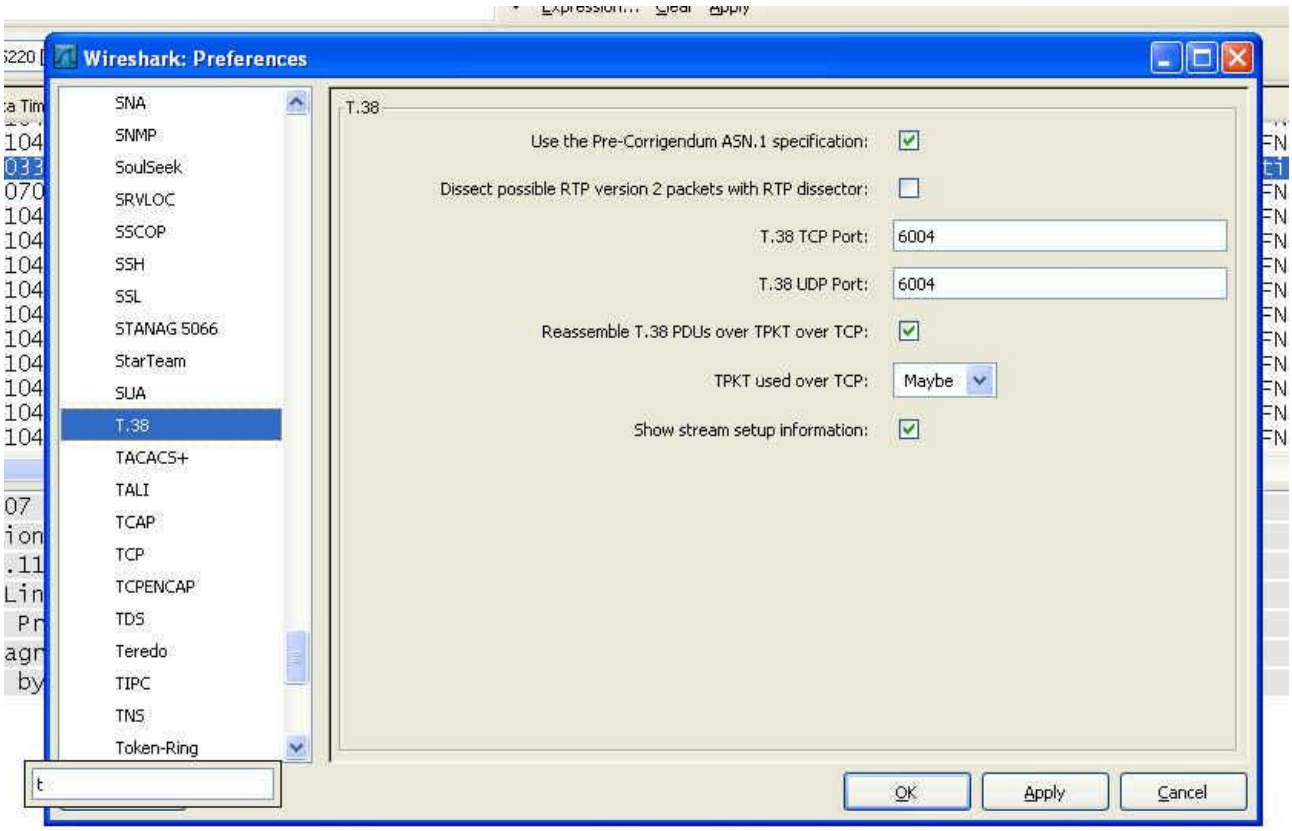


Neue, temporäre **'Coloring rules'** lassen sich nun mit wenigen Mausklicks anwenden, so dass z.B. eine bestimmte TCP Session hervorgehoben werden kann. Einfach rechter Mausklick auf einen TCP SYN Frame anwenden und mit **à Colorize Conversation à TCP à Color** die gewünschte Farbe wählen. Ein Trace mit zahlreichen TCP Sessions wird dadurch wesentlich übersichtlicher dargestellt:



Bug Report. Ein kleiner Fehler, welcher jedoch nur die Bedienung des Wireshark beeinträchtigt, hat sich in Version 99.8 eingeschlichen und wurde von Leutert NetServices bereits gemeldet.

Unter **à Edit Preferences à Protocols** lässt sich keinen String wie z.B. TCP eingeben, sondern nur noch einen einzelnen Charakter, danach bleibt die Eingabe für einige Sekunden blockiert.



Weitere interessante Infos:

- Trainings von Leutert NetServices werden neu auch in Deutschland von **ExperTeach GmbH** angeboten, eine renommierte Firma im Bereich IT-Seminare mit den Spezialgebieten Netzwerktechnik und Telekommunikation.
  http://www.experteach.de/classroomtraining/steckbriefe/classroomtraining_steckbrief_WISH.php

Soviel für den Moment, der nächste Newsletter wird über das **SharkFest.08** in Kalifornien berichten. Einige interessante Neuerungen können erwartet werden.

Mit freundlichen Grüssen
Rolf Leutert / Leutert NetServices
März 2008

http://www.cacetech.com/SHARKFEST.08/

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