WIRE**SHARK** Newsletter Juli 2013

Dieser Wireshark Newsletter von Leutert NetServices informiert Sie regelmässig in Kürze über wichtige Neuerungen im Zusammenhang mit dem führenden Open Source Analyser Wireshark und weiteren sinnvollen Netzwerkanalyse-Produkten.

Schlagzeilen:

- Markante Neuerungen in Wireshark ab Version 1.10.0
- 15 jähriges Wireshark Jubiläum am Sharkfest'13 in Kalifornien
- TCP Session Analyse mit Stream Graph erweitert
- Günstiger Monitoring Switch mit POE Pass-through
- Tipps, Tricks & Traces: Die Wireshark Display Filter Logik
- Hinweise: Wireshark Kurse und Präsentationen

Neue Features der Wireshark Versionen 1.8.3 bis 1.8.8

Neue Funktionen bis Release 1.8.2 wurden in den letzten Newslettern detailliert beschrieben. Die Versionen 1.8.3 bis 1.8.8 enthalten „nur" Protokollerweiterungen und Bug Fixes.

Unser Newsletter Archiv finden sie unter: www.wireshark.ch/de/wireshark-software/knowledge-base

Die wichtigsten Neuerungen ab Version 1.10.0

Mehr als 20 teilweise wichtige neue Funktionen wurden in dieser Version realisiert, welche das Einsatzgebiet und die Bedienung markant erweitern und verbessern.

Folgende ausgewählte Erweiterungen werden nachfolgend detailliert beschrieben:

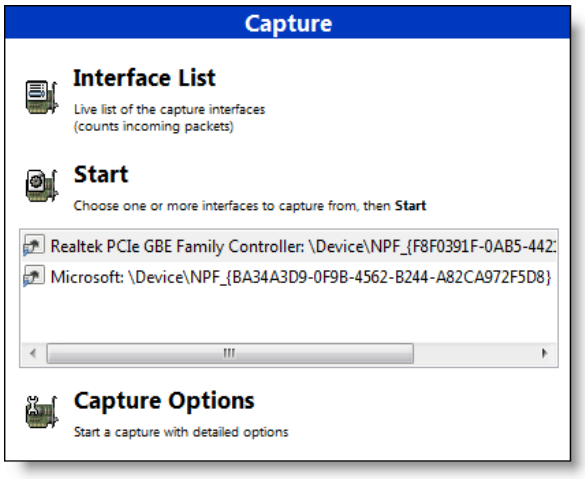
- Face Lifting: Neue Icons in Menüs und Toolbars
- Liste von DNS Namen im HOST-File Format
- Wireless Toolbar und Decryption Key Management verbessert
- Darstellung der TCP Graph Analyse verbessert
- Wireshark berechnet Antwortzeiten von HTTP Request/Response Dialogen
- TCP Window Scaling Faktor ist manuell einstellbar

Sämtliche V 1.10.0 Neuerungen im Textformat finden sie in den Release Notes:

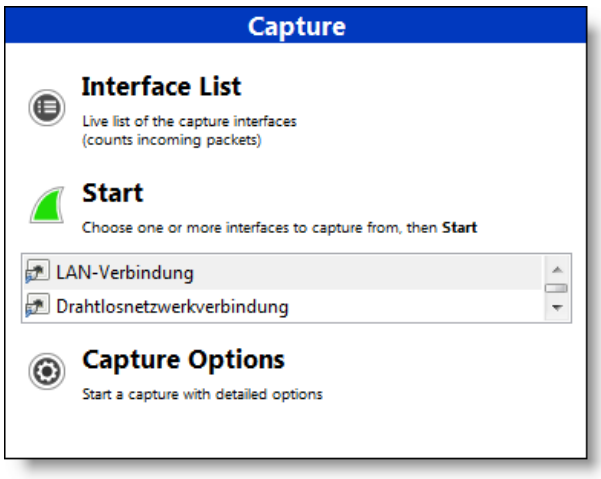
- http://www.wireshark.org/docs/relnotes/wireshark-1.10.0.html

Face Lifting

Nicht als Funktionserweiterung, sondern als Kosmetik können die neuen Icons bezeichnet werden, welche in den verschiedenen Menüs und Toolbars geändert wurden. Während die alten Icons eine Network Interface Card (NIC) kombiniert mit verschiedenen Symbolen zeigten, liessen sie sich doch bei kleiner Darstellung schlecht unterscheiden. (Wer von der jüngeren Generation weiss zudem noch wie eine NIC aussieht)



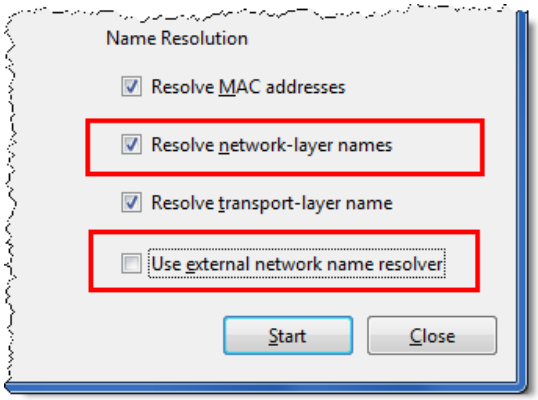
Alte Version mit NIC basierten Symbolen



Die neuen Icons sind besser zu unterscheiden

Liste von DNS Namen im HOST-File Format

Wireshark kann so konfiguriert werden, dass während der Aufzeichnung IP-Adressen durch Host Namen ersetzt werden. Dies kann mit zwei verschiedenen Methoden erreicht werden, welche unter den Capture Options ausgewählt werden können.

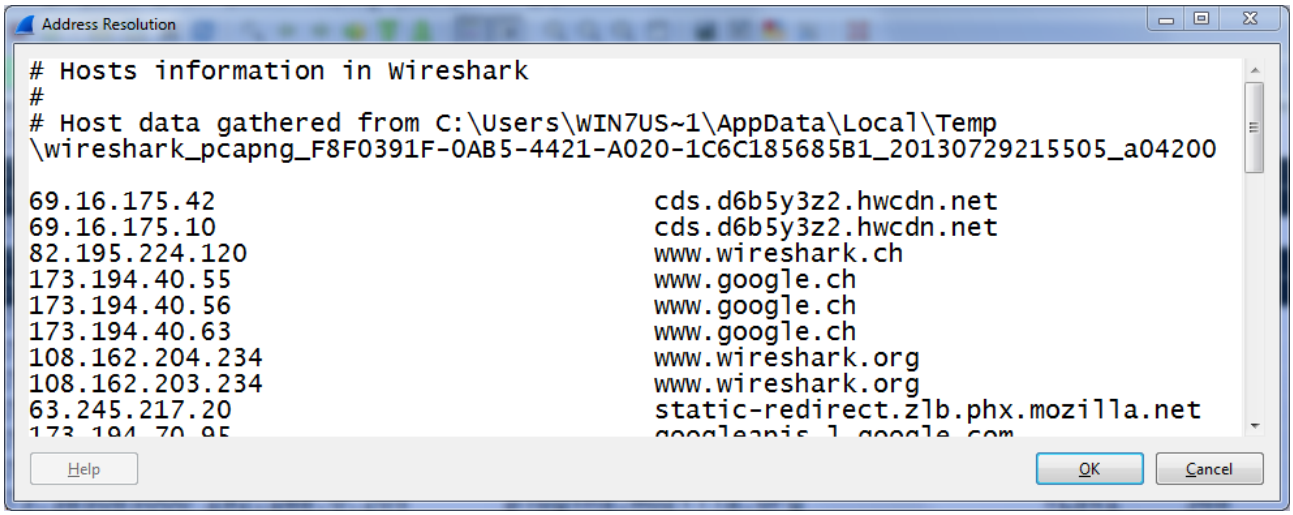


Die Option Resolve network-layer names analysiert die aufgezeichneten DNS Responses für die Namensauflösung.
→ Passive Namensauflösung

Mit der Option Use external network name resolver erzeugt Wireshark eigene DNS Queries für die Namensauflösung. Dazu muss die Wireshark unterliegende Plattform mit gültigen IP-Parametern inkl. DNS Adresse konfiguriert sein und auf dem DNS Server müssen Reversezonen konfiguriert sein.
→ Aktive Namensauflösung

Die von Wireshark aufgelösten DNS Namen (aktiv oder passiv) werden in einem Textfile aufgelistet. Diese Daten können mit Copy&Paste direkt in das sogenannten Hosts File kopiert werden, bei Windows OS normalerweise zu finden unter C:\Windows\System32\drivers\etc

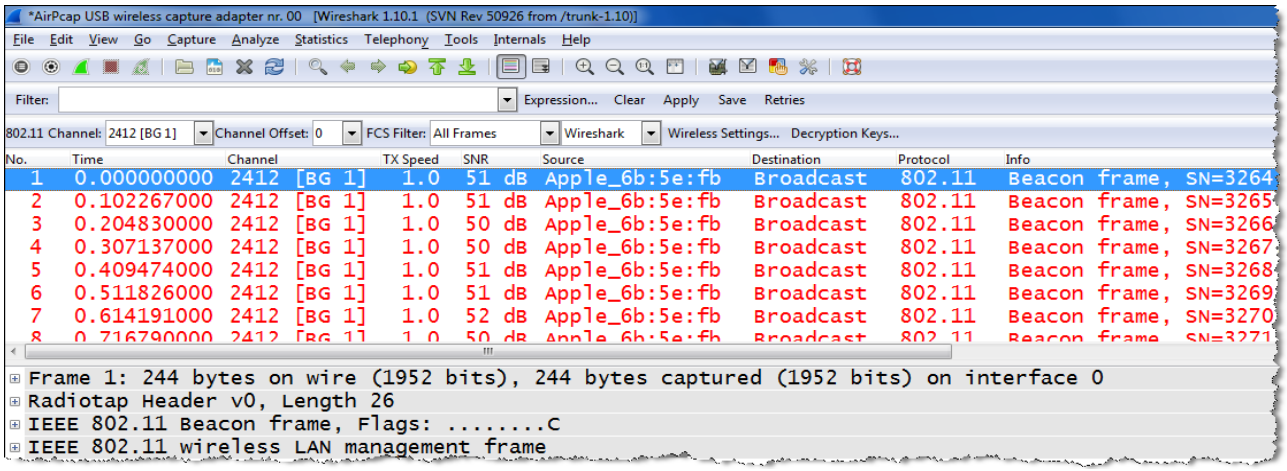
Diese neue Wireshark Funktion finden sie unter → Statistics → Show address resolution



Textfile mit den durch Wireshark gesammelten Host Namen

Wireless Toolbar und Decryption Key Management verbessert

Die Wireless Toolbar finden sie unter → View → Wireless Toolbar. Die Darstellung wurde optisch verbessert, zudem funktioniert das Abspeichern der Decryption Keys wieder einwandfrei.

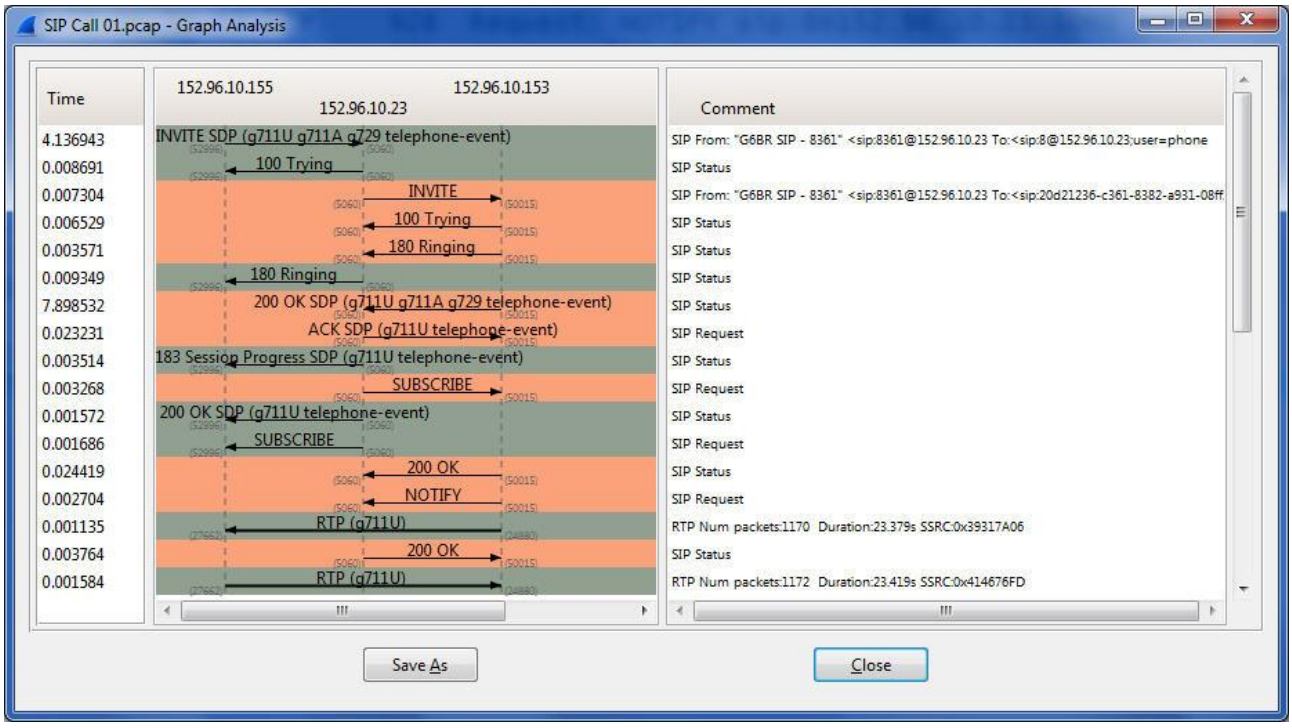


Wireless Management Frames aufgezeichnet mit AirPcap Adapter

Wireshark kann Daten entschlüsseln, welche mit WEP, WPA und WPA2 verschlüsselt sind. Dies unter der Bedingung, dass diese mit einem statischen Key konfiguriert sind (Personal Mode) und der Key für die Decryption zur Verfügung steht (während oder nach der Aufzeichnung).

Darstellung von Graph Analysis verbessert

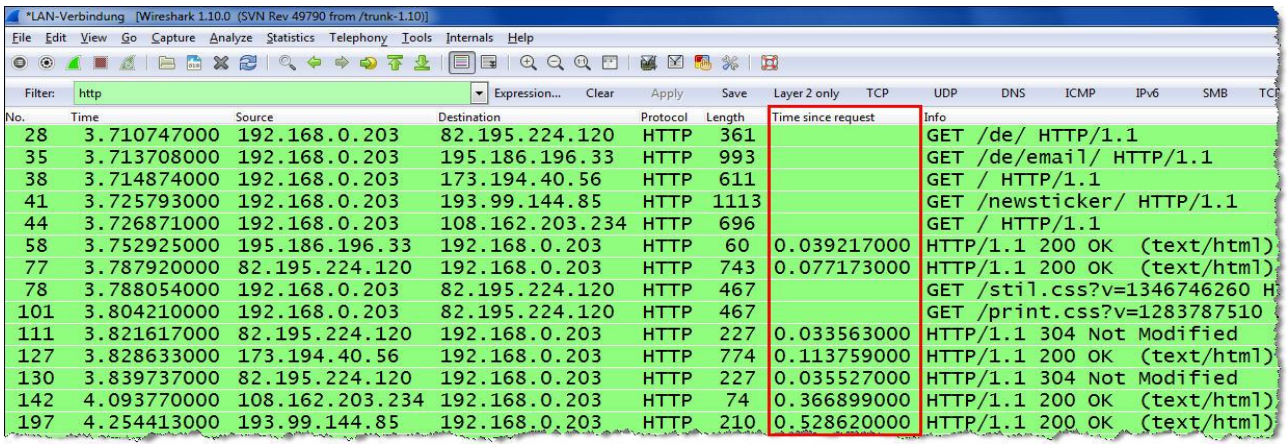
Die praktische grafische Darstellung von Konversationen wurde verbessert, die Grösse lässt sich nun beliebig verändern. Diese Funktion finden sie unter → Statistics → Flow Graph



Darstellung eines VoIP Calls mit SIP Signaling und RTP mit Flow Graph

Wireshark berechnet Antwortzeiten von HTTP Request/Response Dialogen

Das neue Feld Time since request finden sie in jedem HTTP Response Frame. Rechter Mausklick auf das Feld und Wahl von Apply as Column generiert eine eigene Kolonne. Für die Berechnung muss die Reassemblierung in den TCP Preferences eingeschaltet sein (ist die Default Einstellung).



Übersichtliche Darstellung der Antwortzeiten in einer eigenen Kolonne

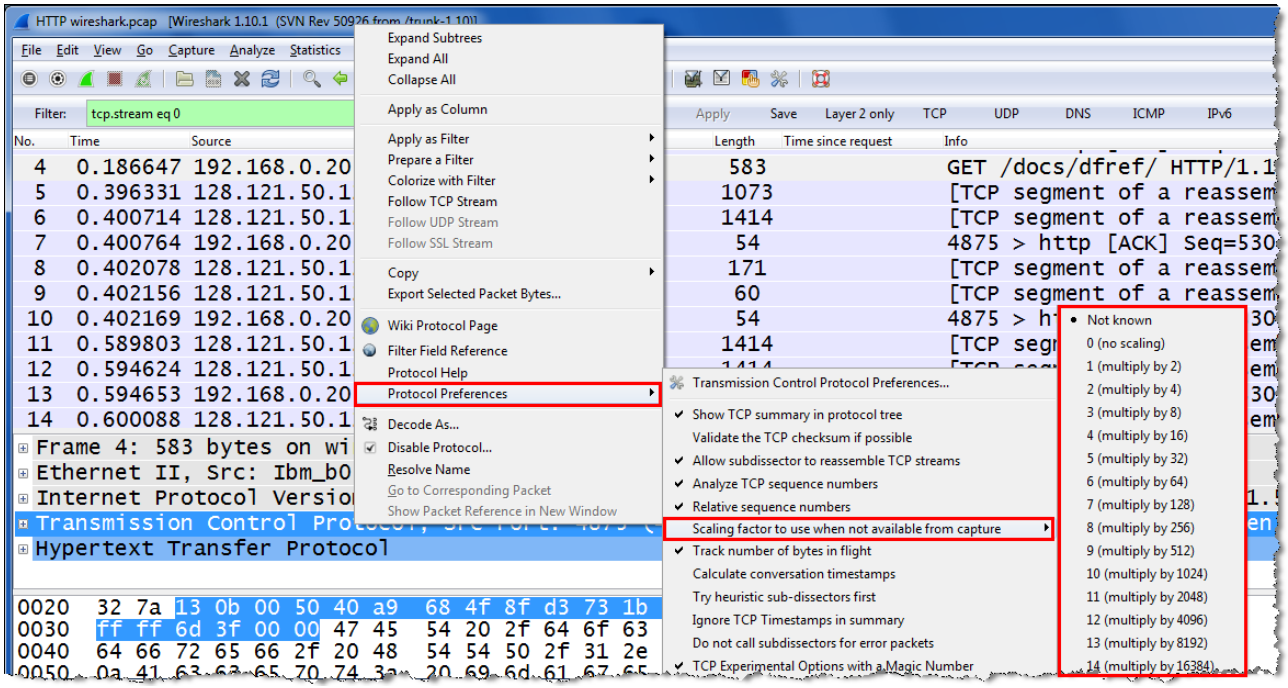
Wireshark setzt mit diesen HTTP Antwortzeiten die Entwicklung in Richtung Application Performance Analyse fort, ein Wunsch, welcher von zahlreichen Benutzern gewünscht wird. Entsprechende Analysen unterstützt Wireshark auch bereits für das SMB Protokoll.

TCP Window Scaling Faktor ist manuell einstellbar

Die Window Scaling Option ermöglicht es, die Grösse des TCP-Eingangsbuffers bis auf 1 GByte zu vergrössern (TCP Extensions gemäss RFC 1323). Diese Option wird zwischen Client und Server beim Aufbau einer TCP Session während des 3-way Handshakes (SYN, SYN-ACK, ACK) ausgehandelt. Der Wireshark Expert berücksichtigt den ausgehandelten Faktor bei den Windows-Size Berechnungen und Fehlermeldungen.

Wird die Aufzeichnung mit Wireshark erst nach dem TCP 3-way Handshake gestartet, fehlt diese Information. Falschmeldungen des Wireshark Experts können die Folge sein. Neu kann der Scaling Factor manuell konfiguriert werden. Der richtige Wert muss dabei empirisch ermittelt werden, am besten durch die Verwendung des TCP Stream Graph. Gute TCP Kenntnisse wie sie auch in unseren Kursen vermittelt werden, sind dazu jedoch erforderlich.

Betätigen Sie einen rechten Mausklick auf dem TCP Header im Detail Fenster
und folgen Sie den Menü-Positionen gemäss Screenshot:



Manuelle Einstellung des TCP Scaling Faktors beim Fehlen des 3-way Handshakes

15-jähriges Wireshark Jubiläum am Sharkfest'13 in Kalifornien

Im Jahr 1998 startete Gerald Combs unter dem Namen Ethereal die Entwicklung einer grafischen Protokoll-Analysesoftware und stellte diese als Open-Source zur Verfügung. Nur fünf Protokolle im TCPdump Format .pcap wurden im ersten Release, basierend auf Linux und Solaris, unterstützt.
Gerald und seiner Frau (von ihr stammt der Name Wireshark) wurde in einem humorvollen Filmbeitrag entsprechend Ehre und Dank bekundet, woraufhin Gerald den Dank unmittelbar an die grosse Entwicklergemeinde weitergab.

Aktuell unterstützt Wireshark die Decodierung von mehr als 1'000 Protokollen, kann nach über 140'000 verschiedenen Protokollfelder filtern und wird Monat für Monat rund 500'000 mal von der Webseite heruntergeladen. Ein Erfolgsprojekt, welches auch schon mehrmals als Musterbeispiel für Open-Source ausgezeichnet wurde.

Mehr Informationen zur Geschichte und Entwicklung von Wireshark finden sie unter Heise Online:

http://www.heise.de/netze/meldung/15-Jahre-Wireshark-Auf-zum-Internet-der-Dinge-1910320.html

Rolf Leutert präsentierte dieses Jahr u.a. zum ersten Mal eine Session zum Thema SMB 3 Protokoll. Microsoft ist bestrebt, mit der neusten Version des Server Message Block Protokolls vermehrt Einzug in die virtualisierte Server Umgebung zu halten. Das grosse Interesse an der Präsentation scheint das Potential zu bestätigen.

Sämtliche SharkFest'13 Beiträge (teilweise mit Video) sind abrufbar unter:

http://sharkfest.wireshark.org/sharkfest.13/index.html

Die Wireshark Entwicklung geht rasant weiter, freiwillige Entwickler arbeiten an der Decodierung neuer Protokolle (sogenannten Dissectors) wie HDMI Control-Bus, Industrial Protocols usw.

Eine Migration, welche Gerald Combs als MAC Fan besonders am Herzen liegt, ist der Wechsel der grafischen Darstellung von GTK (Graphical Tool Kit) auf QT als Open-Source Cross Plattform. QT (Kiu:ti) soll das Wireshark GUI besser an das spezifische Look and Feel der verschiedenen Betriebssysteme anpassen.
Damit würde Wireshark auf den MACs endlich ohne das in die Jahre gekommene X.11 GUI funktionieren können.
Auch Ideen für die Unterstützung weiterer Plattformen wie Android oder Apple IOS werden diskutiert und warten auf freiwillige Helfer.

Ethernet Jubiläum

Rich Seifert (l.) und Rolf Leutert

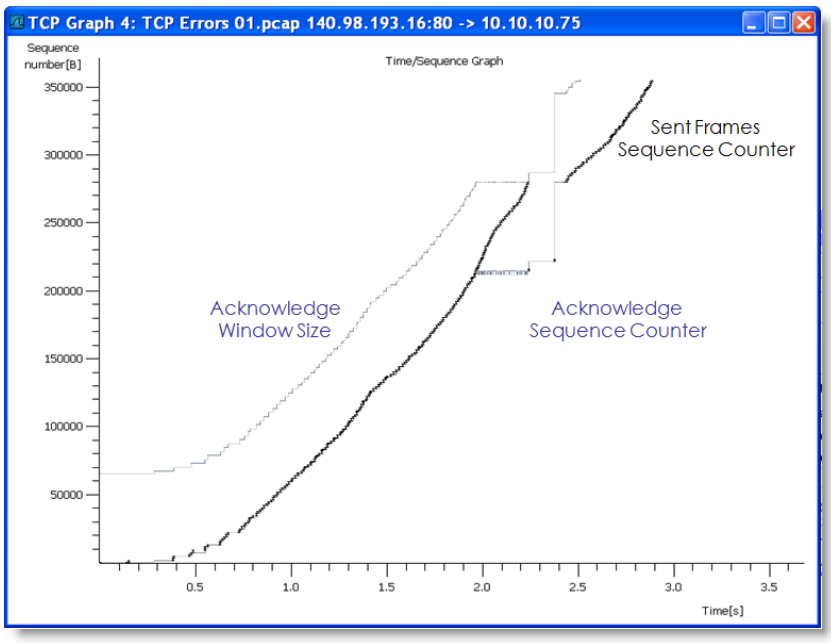
Geburtstag feiert dieses Jahr auch Ethernet, vor 40 Jahren auf Grund einer ersten Skizze von Bob Metcalfe bei Xerox entstanden. Keynote Speaker am Sharkfest'13 war auch Rich Seifert, einer der drei Entwickler der ersten Ethernet Spezifikation (DIX) und Erfinder des Yellow-Cables.
Nur wenige Techniken in der IT erreichen ein so hohes Alter, da scheinen doch einige Überlegungen mit Weitblick getroffen worden zu sein.
Rich berichtete auf seine humorvolle Weise über die Anfänge der Erfolgsgeschichte, welche Entscheide offenbar richtig waren, aber auch was er heute anders lösen würde.

Den vollständigen Artikel finden sie auf Heise Online:

http://www.heise.de/netze/meldung/Ethernet-Pionier-Wir-haben-drei-Dinge-richtig-gemacht-1924725.html

TCP Session Analyse mit Stream Graph erweitert

Die grafische Darstellung einer TCP Half-Session erleichtert die Analyse und ist in Wireshark schon seit längerer Zeit verfügbar:
→ Frame wählen → Statistics → TCPStreamGraph → Time-Sequence Graph (tcptrace)

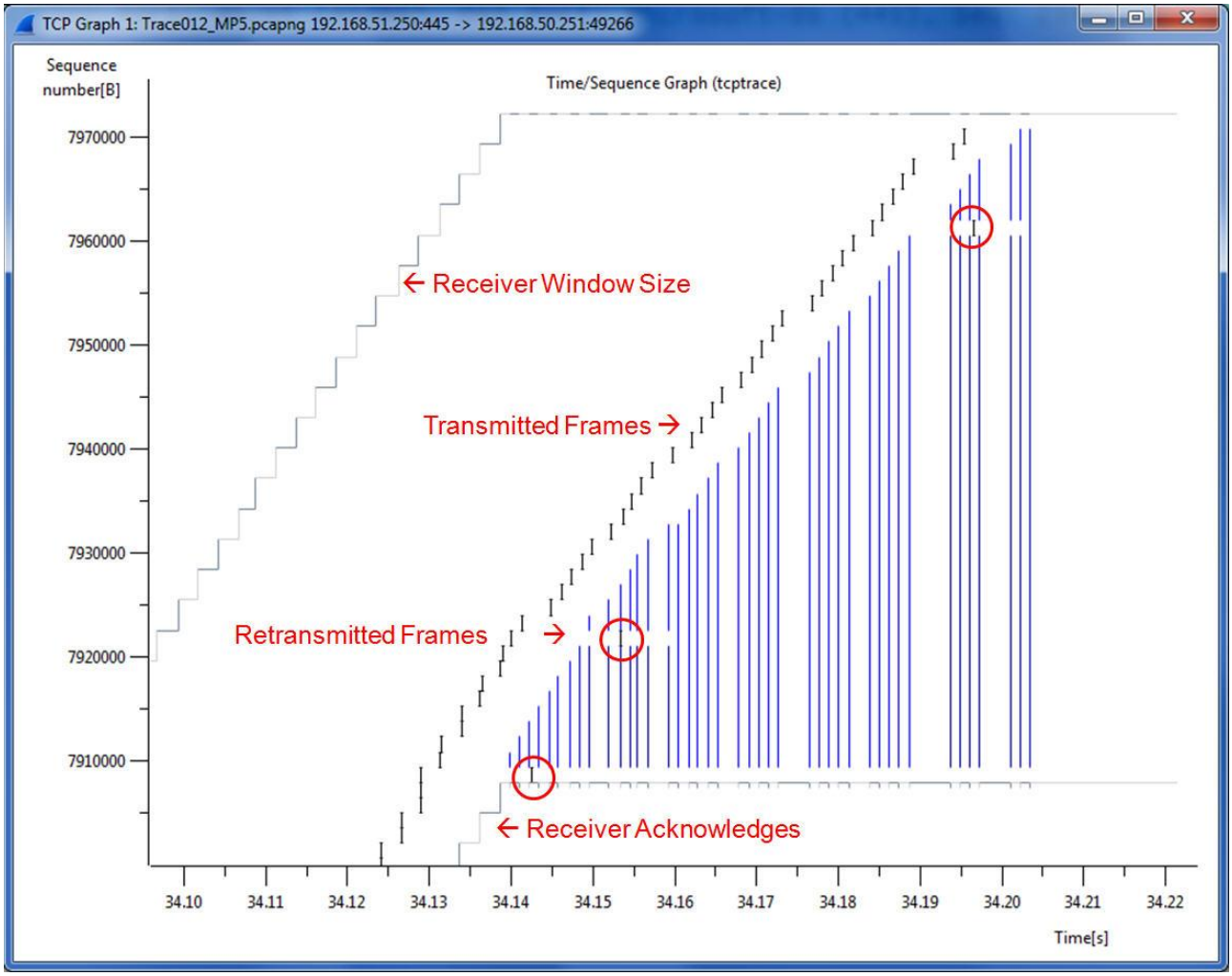


Grafische Darstellung von TCP (Quelle: TCP Kurs von Leutert NetServices)

Diese Grafik wurde ein weiteres Mal verbessert und zeigt nun noch mehr Details, z.B. werden nun auch Selective Acknowledge dargestellt. SACKs sind Teil der TCP Extensions RFC 1323 und ermöglichen es dem Empfänger, in den Acknowledges selektiv fehlende Frames und die danach bereits empfangenen Frames zu bestätigen. Dies verbessert den TCP Durchsatz bei langen Laufzeiten markant, da der Sender gezielt nur die fehlenden Frames nachzuliefern hat.

Erklärungen:
Die empfangenen Pakete nach einem fehlenden Frame werden in den senkrechten blauen Linien mit den Lücken für die fehlenden Frames dargestellt. Die einzelnen kurzen vertikalen Linien mit den Querenden stellen die übertragenen Pakete dar. Nachgelieferte Frames sind innerhalb der blauen Linien zu sehen (eingekreist), worauf mit gewisser Verzögerung durch die Netzlaufzeit die Lücken in den Selective Acknowledges geschlossen werden. Die Ausnahme bildet die erste Retransmission (rechts unten), welche auch nach der zweiten Übertragung nicht bestätigt wird und damit die Session blockiert.

Bemerkung:
Die rot markierten Einträge sind Ergänzungen und in der Original Grafik nicht vorhanden.



Darstellung von TCP Selective Acknowledges (SACK) und Retransmissions

Günstiger Monitoring Switch mit POE Pass-through

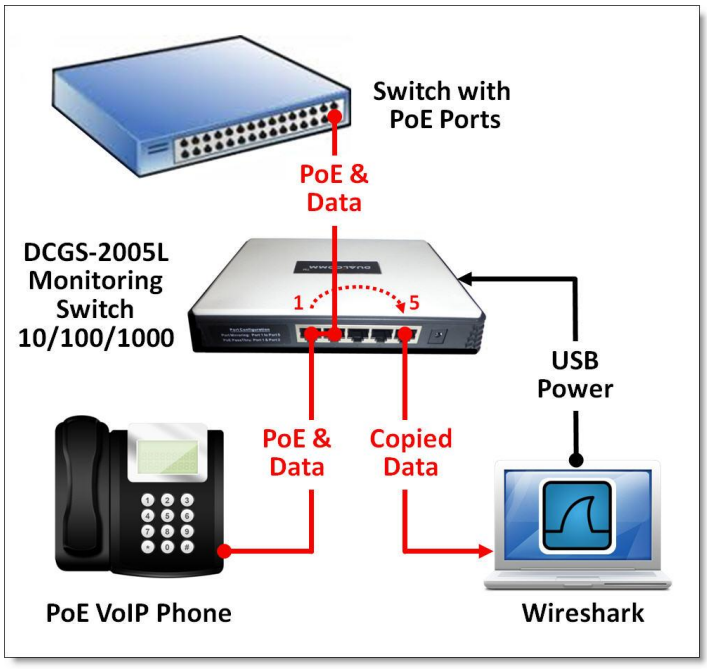
Leutert NetServices bietet auch einige ausgewählte kommerzielle Analyseprodukte im Verkauf an. Alle unsere Produkte finden sie unter: http://www.wireshark.ch/de/produkte/

Neu im Programm ist ein mobiler kostengünstiger Monitoring Switch der Firma Dualcomm USA, welcher in die Notebook-Tasche jedes Field Engineers passt.

Nicht immer ist der Zugriff auf einen Switch zum Konfigurieren eines Mirror/Span Ports für das Abgreifen des Datenverkehrs möglich. Z.B. Kunden, welche ihre Netzwerkinfrastruktur durch Dritte betreuen lassen, haben in der Regel keinen Konfigurations-Zugriff auf die Router und Switches.

Der DCGS-2005L ist ein fix geschalteter Ethernet Monitoring Switch für das Aufzeichnen mit 10/100/1000 Mbit/sec. Half & Full Duplex. Der Switch wird einfach in die Verbindung zwischen einem Endgerät und dem Switchport eingefügt und kopiert den Datenverkehr von und zum Endgerät auf einen fix verdrahteten Monitor Port, an welchem ein Network Analyser (z.B. Wireshark) angeschlossen wird.

Durch die Power-over-Ethernet (PoE) pass-through Funktion ist es möglich, auch PoE Endgeräte wie VoIP Telefone, WLAN Access Points, IP Kameras usw. anzuschliessen und mit Strom zu versorgen. Der Monitoring Switch selbst wird durch die Verbindung zu einem USB Port des Notebooks mit Strom versorgt, dadurch entfällt die Notwendigkeit für ein externes Netzteil.
Diese Konfiguration ermöglicht z.B. auch die Aufzeichnung des Boot-Vorganges eines PoE Gerätes wie VoIP Telefon, WLAN Access-Point inkl. die Parameter-Aushandlung über CDP oder LLDP mit dem Switch.



Der Verkaufspreis pro Switch beträgt CHF 160.00 (exkl. MwSt.) und ist ab Lager lieferbar.

Beim Wireshark Einführungskurs bei der Firma Studerus AG ist ein Monitoring Switch eingeschlossen. Anmeldung unter: http://www.studerus.ch/de/training/detail/net-analyse

Tipps, Tricks & Traces

Die Wireshark Display Filter Logik

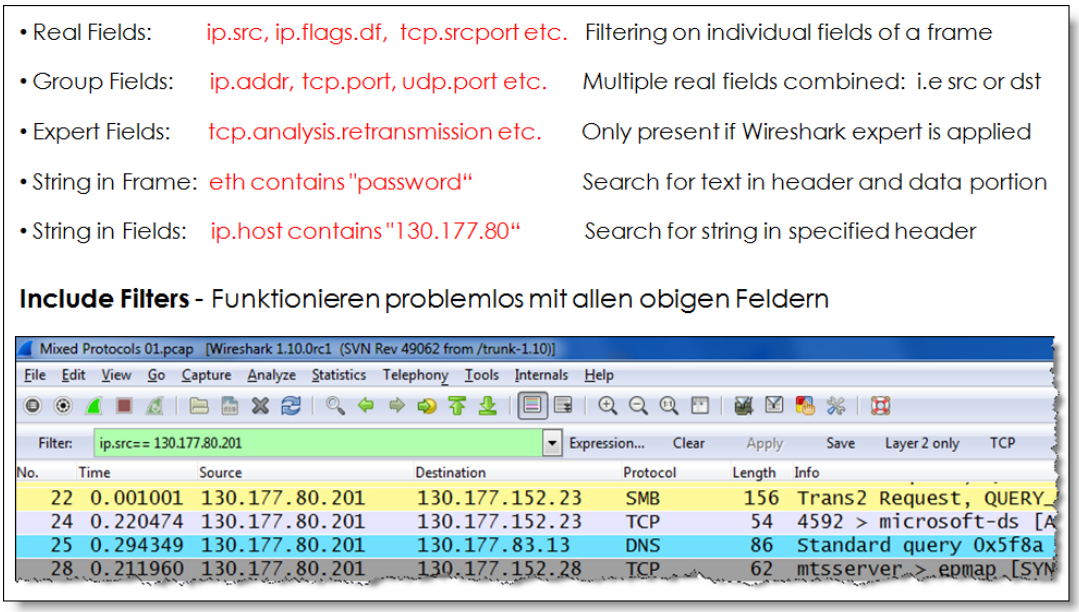
Die Wireshark Display Filter basieren auf einer ausgeklügelten Logik und funktionieren auf der Verbindung von Feldnamen und variablen Werten, z.B.: ip.src == 128.121.50.122
Die sogenannten Dissectors zerlegen sämtliche Protokolle in kleinstmögliche Einheiten, die sogenannten Header Fields (inzwischen über 140'000). Die Felder haben je nach Bedeutung unterschiedliche Grössen, so besteht z.B. das Don't Fragment Feld gerade mal aus einem Bit. Beim Anwählen eines Feldes erscheint der Feldnamen unten links in Klammern (ip.flags.df).

Verschiedene Verfahren wie VLAN, QinQ, MPLS usw. fügen zwischen Ethernet- und IP-Header Felder von variabler Länge ein, dadurch verändert sich die Position (Offset, in Bytes) aller nachfolgenden Felder innerhalb dieses Paketes.

Der Display Filter funktioniert unabhängig vom Offset eines Feldes, im Gegensatz zum Capture Filter.

Capture Filter (basierend auf TCPdump) arbeiten nach dem Offset&Value Prinzip und funktionieren deshalb nicht bei variablen Positionen einer Kondition. Z.B. der Filter src host 128.121.50.122 wird in einem Netzwerk mit VLAN Tags nicht mehr greifen und muss angepasst werden. Die Syntax lautet dann entsprechend: vlan and src host 128.121.50.122

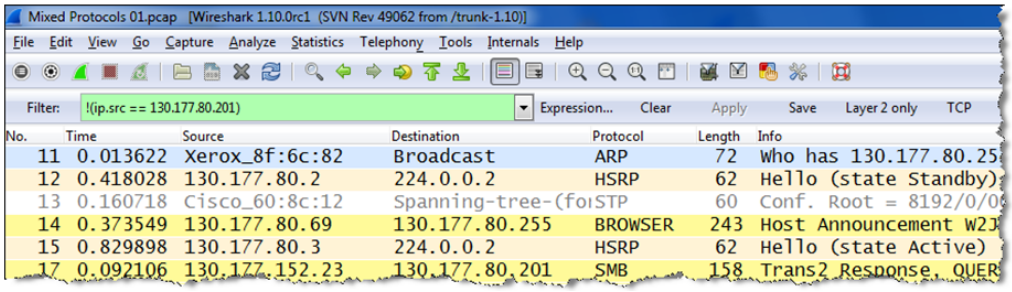
Um die Filterfunktion zu erweitern, kann Wireshark neben den Real Fields auf weitere Felder filtern; diese sind nicht als Feld im Frame enthalten, sondern werden von Wireshark generiert.



Die verschiedenen Display Filter (Quelle: TCP Kurs von Leutert NetServices)

Alle verschiedenen Filtertypen funktionieren problemlos beim sogenannten Include Filter, d.h. ein Paket muss das angegebene Feld mit Wert enthalten.
Etwas komplizierter wird es mit dem Exclude Filter, d.h. die gesuchten Pakete dürfen das angegebene Feld mit Wert nicht enthalten.

Exclude Filters - Zeigen oft unerwartete Resultate



Ein Filter soll Frames zeigen, welche nicht von der spezifizierten IP Adresse stammen:

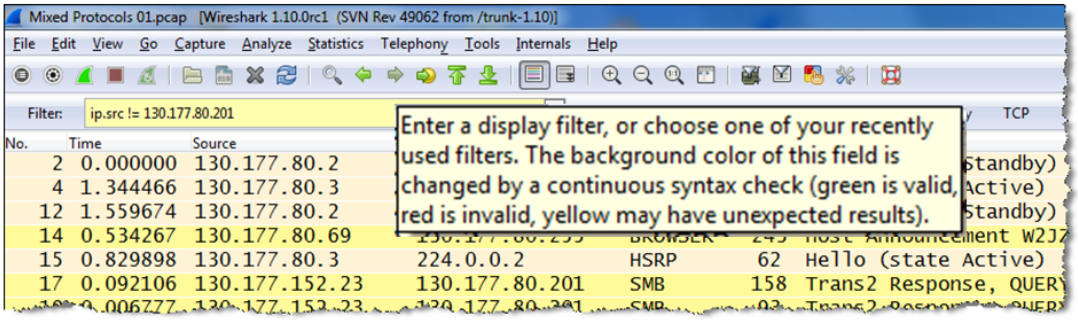
• Der Filter !(ip.src == 130.177.80.201) oder not (ip.src == 130.177.80.201) zeigt alle Frames, welche kein IP Source Feld mit der spezifizierten Adresse enthalten.

• Da Protokolle wie ARP, STP usw. dieses Feld ebenfalls nicht enthalten, werden diese Frames auch angezeigt! Resultat zeigt mehr als die gewünschten Frames!

Exclude Filter sind tricky (Quelle: TCP Kurs von Leutert NetServices)

Der korrekte Filter würde lauten, ip and not ip.src == 130.177.80.201 oder ip.src != 130.177.80.201
Die Syntax != entspricht dabei not equal. Bei diesem Filter erscheint jedoch ein gelber Hintergrund als Warnung, dass das Filterresultat nicht eindeutig sein könnte.

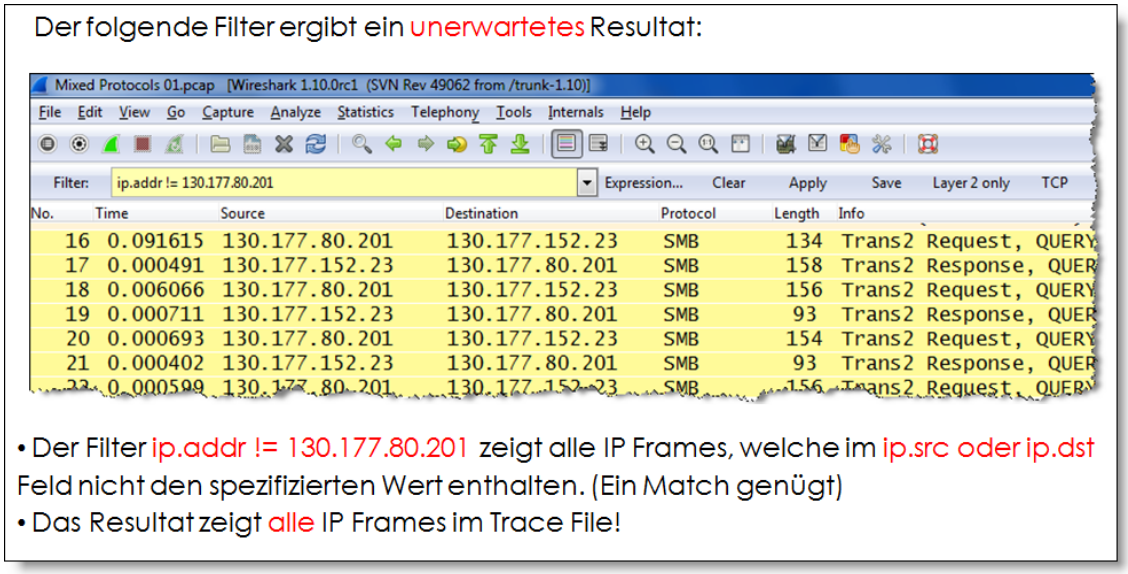
Der folgende Filter ergibt das erwartete Resultat:



• Der gelbe Filter-Hintergrund weist jedoch darauf hin, dass das Resultat unter Umständen nicht eindeutig sein könnte!

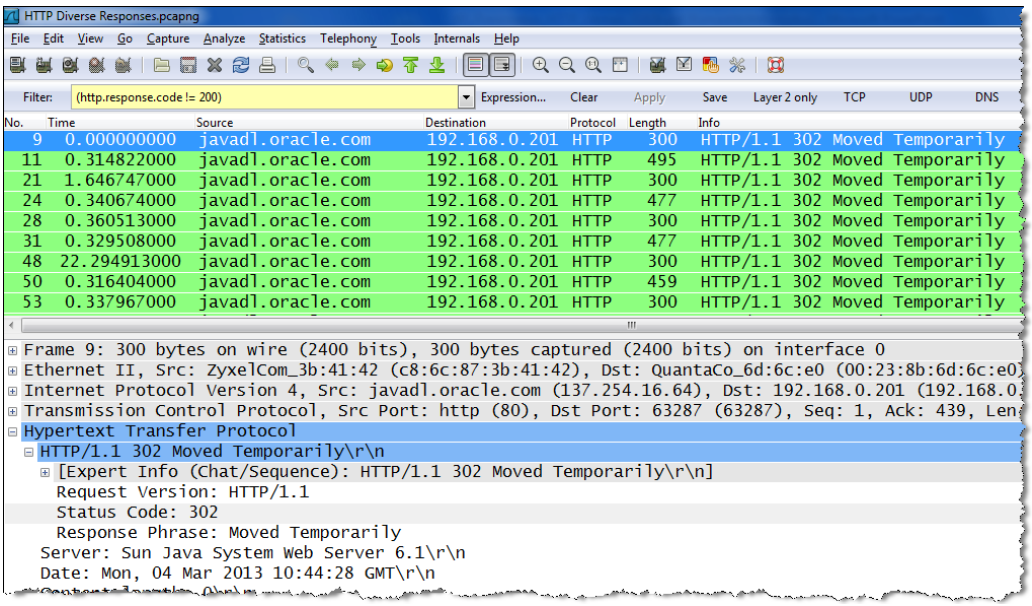
Gelber Background als Warnung (Quelle: TCP Kurs von Leutert NetServices)

Erklärung: Der Filter ip.src != 130.177.80.201 sucht nach dem ersten IP Source Address Feld, welches nicht die spezifizierte Adresse enthält, erachtet die Bedingung als erfüllt und zeigt das Paket an. Ist das gesuchte Feld im selben Frame weitere Male vorhanden (z.B. in gewissen ICMP Frames), werden diese Felder nicht mehr geprüft.
D.h. der Filter auf die Gruppenadresse ip.addr != 130.177.80.201 wird nicht funktionieren, da diese Felder in der Regel innerhalb eines Paketes mehrmals vorkommen.



Falsches Resultat bei != Filter auf Gruppenadresse (Quelle: TCP Kurs von Leutert NetServices)

Schlussfolgerung: Filter, welche die Syntax != (nicht gleich) enthalten, funktionieren trotz gelber Warnung einwandfrei, wenn gewährleistet ist, dass das gesuchte Feld innerhalb eines Paketes nur ein einziges Mal vorhanden ist. Dies ist bei den meisten Real Fields gegeben, jedoch nicht bei Group Fields oder anderen Feldern.



Beispiel eines sinnvollen != Display Filters

Hinweise:

Öffentliche Präsentationen und Wireshark Kurse

Tun Sie sich und Ihren Mitarbeiter etwas Sinnvolles und buchen Sie uns z.B. für eine eintägige Einführung zu IPv6, einem Update zu Wireshark oder dem Thema Ihrer Wahl aus den aufgeführten Kursen. Wir garantieren Ihnen einen lehrreichen Anlass.

Präsentationen und Events:

Das Studerus Technology Forum geht dieses Jahr in die vierte Runde und hat sich als Event sowohl für wertvolle Weiterbildung als auch unterhaltsame Keynotes bereits etabliert. Interessierte aus Fachhandel und Anwender-unternehmen treffen sich im WTC Zürich Oerlikon zu einem spannenden TEFO-Mix aus Wissensvermittlung, Praxistipps u. Networking.
Leutert NetServices wird eine praxisorientierte Session zum Thema Netzwerk-Analyse mit Wireshark präsentieren.

Der Anlass ist kostenlos, mehr Infos und Anmeldung unter http://www.studerus.ch/de/tefo/

Wireshark Einführungen und Kurse

Gerne offerieren wir Ihnen zu den aufgeführten Themen interne Kurse oder Tech-Sessions nach ihren Wünschen (mit oder ohne Lab-Sessions):

- Netzwerkanalyse allgemein
- TCP/IP Netzwerkanalyse mit Wireshark
- WLAN Netzwerkanalyse mit Wireshark und AirPcap
- VoIP Analyse mit Wireshark
- IPv6 Netzwerkanalyse mit Wireshark

Die komplette Liste aller öffentlichen Kurse auch in Österreich und Deutschland finden Sie auf unserer Webseite http://www.wireshark.ch/de/wireshark-kurse/oeffentliche-kurse

Es würde uns freuen, Sie in einem unserer Kurse begrüssen zu können.

Besten Dank für Ihr Interesse
Mit freundlichen Grüssen Rolf Leutert