WIRE**SHARK** Newsletter August 2011

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-Tools.

Schlagzeilen:

RIVERBED übernimmt Sponsorschaft von Wireshark

riverbed Think fast.™

„Der Hai ist im Flussbett gelandet!“ Diese Meldung schockte weltweit die Wireshark Benutzer- und Entwicklergemeinde, als im Oktober 2010 bekannt wurde, dass die Firma RIVERBED Technology die Firma CACE Technologies, den bisherigen Sponsor von Wireshark übernommen hatte. Schnell wurde die Situation mit der ORACLE Akquisition von OpenOffice verglichen, die Kommerzialisierung und damit das Ende von Wireshark prophezeit.
Seither hat sich die Szene etwas beruhigt, und es gibt verlässliche Anzeichen, dass sich diese berechtigten Befürchtungen nicht bewahrheiten werden. Ich hatte anlässlich des SharkFests`11 im Juni in Kalifornien die Möglichkeit, an Presseinterviews mit Riverbed Keypersonen teilzunehmen und möchte Ihnen meinen Eindruck schildern.

Riverbed Technology ist mit ihren Steelhead-Produkten Marktführer (Gartner Bericht vom Dezember 2010) im Bereich Wide Area Network Optimization und ermöglicht die effiziente Ausnutzung von Bandbreiten für verschiedene, auf TCP/UDP/IP basierende Protokolle. Man kann davon ausgehen, dass eine wirkungsvolle Optimierungstechnik profundes Wissen dieser Protokolle auf Packet Ebene voraussetzt, d.h. für diese Entwicklungsingenieure ist Wireshark das Grundwerkzeug. Was weniger bekannt ist: Der Hauptentwickler von TCPdump und LibPcap (Urformen der Paketaufzeichnung im Unix Bereich), Steve McCanne, ist CTO bei Riverbed und damit verantwortlich für die technische Entwicklung dieser Produkte.

Sharkfest'11, Stanford University, California
Three 'Packet Gurus' on board(v.l.):

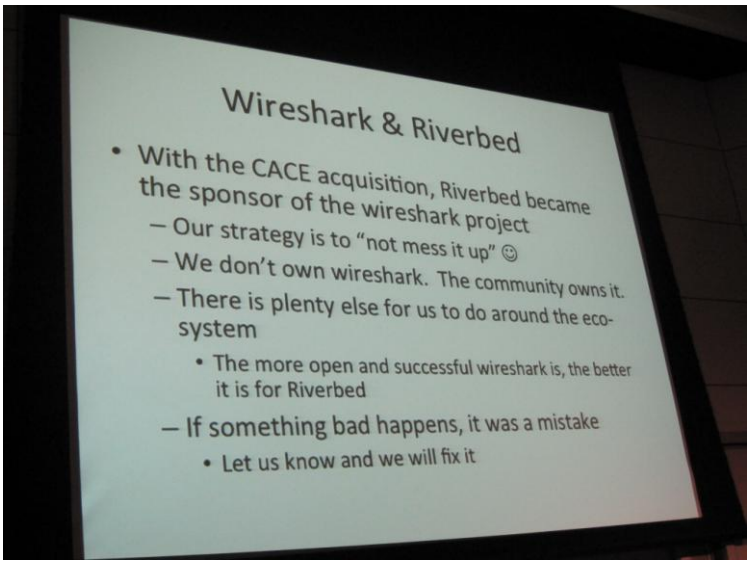
Steve McCanne (CTO Riverbed, Entwickler von TCPdump und LibPcap),
Loris Degioanni (Senior Director of Technology Riverbed, Entwickler von WinPcap) und
Gerald Combs (Open Source Projects, Entwickler von Wireshark)

Mit der Übernahme von CACE kamen auch Loris Degioanni (WinPcap) und Gerald Combs (Wireshark) und das gesamte CACE Pilot Entwicklungsteam an Bord von Riverbed. Im Fokus standen vor allem auch die kommerziellen Produkte Shark Appliance und **CACE Pilot**, Riverbed plant die Integration dieser Funktionen in Ihre eigenen Produktelinien Steelhead und Cascade Monitoring. Die CACE Pilot Software, beliebt als Ergänzung von Wireshark für die Analyse von grossen Tracefiles, wird weiterhin als Stand-alone Version unter dem Namen Cascade Pilot Personal Edition angeboten. Eine 30-tägige Testlizenz erhalten Sie unter:
http://www.riverbed.com/us/contact/try-and-evaluate-pilot-pe.php

Auch nach der Übernahme der CACE Produkte und Wireshark betont Riverbed, die Unabhängigkeit der Open Source Software garantieren zu wollen.

Gemäss Loris Degioanni, ehemaliger Teilhaber von CACE, war dies auch eine der Vertragsbedingungen für die Übernahme.

Steve McCanne formulierte dieses Versprechen in seiner Eröffnungs-Präsentation am Sharkfest'11 wie folgt: **(siehe Slide rechts).**



Weitere Informationen zu diesem Thema finden Sie in der aktuellen Computerwoche:
http://www.computerwoche.de/netzwerke/tk-netze/2488520/

Meine persönliche Meinung:
Nach den Eindrücken beim Besuch des Sharkfest'11, verschiedenen Gesprächen und Diskussionen bin ich persönlich davon überzeugt, dass die Unabhängigkeit von Wireshark als Open Source-Projekt durch die Übernahme von Riverbed nicht gefährdet ist.
Die Beteuerungen von Riverbed sind glaubhaft, und die sehr zurückhaltende Präsenz von Riverbed als Sponsor am Sharkfest'11 werte ich als erster Beweis, dass diese Versprechen auch eingehalten werden. Gerald Combs hat es auch geschafft, die weltweit verteilten Core-Entwickler im Open Source-Projekt zu behalten, zudem glaube ich an seine Fähigkeit die Unabhängigkeit bewahren zu können. Wireshark ist immer noch sein Baby, auch wenn es schon lange den Kinderschuhen entwachsen ist.

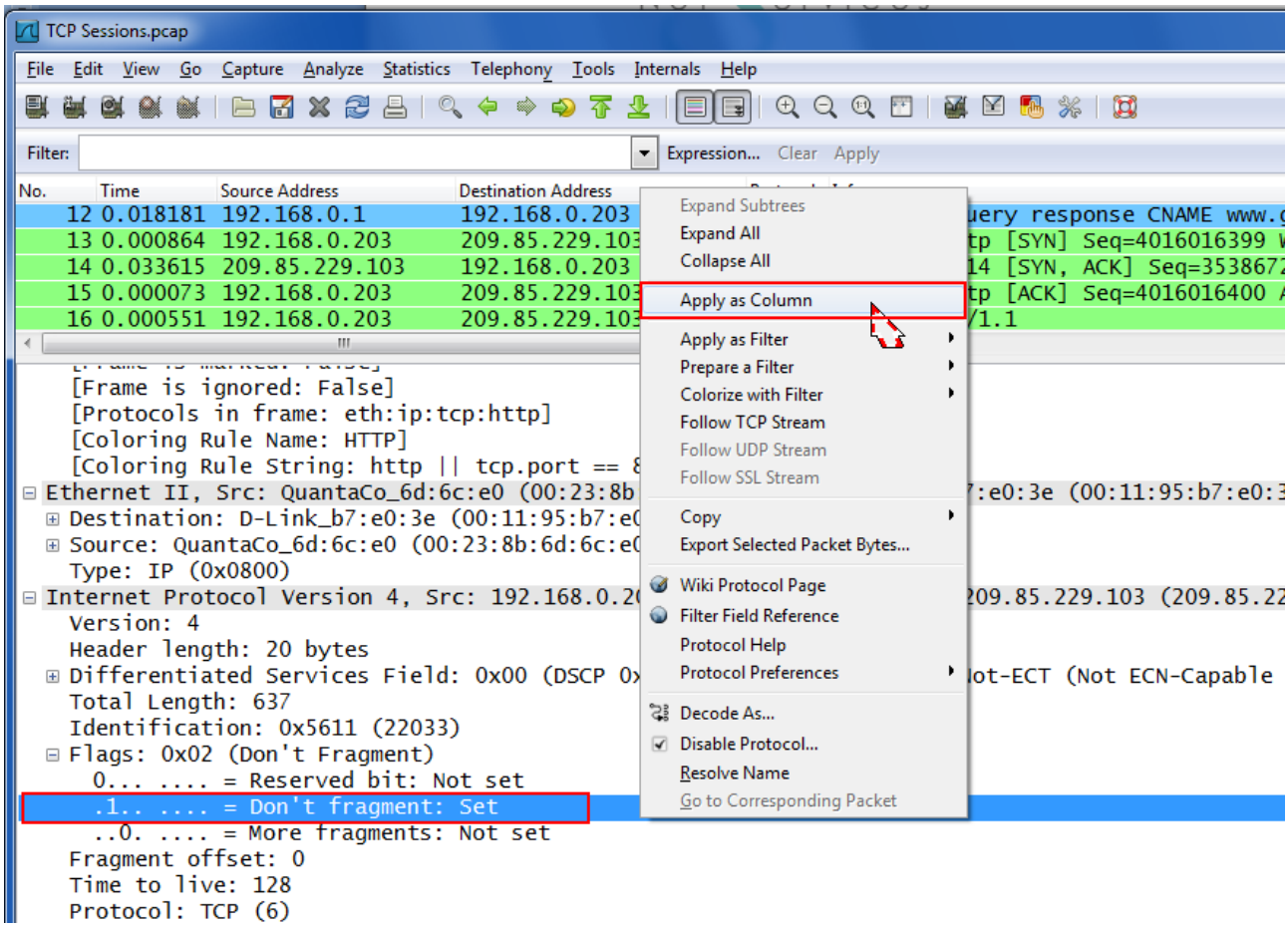
Neue Features der Wireshark Versionen 1.2.7 bis 1.6.1

Die meisten dieser Versionen enthalten Protokollerweiterungen und Bug Fixes. Wireshark hat einen sehr hohen Grad an Professionalität und Stabilität erreicht. Die Erweiterungen und Verbesserungen betreffen deshalb vorwiegend die Bedienbarkeit und die Optimierung der Darstellung. Einige dieser

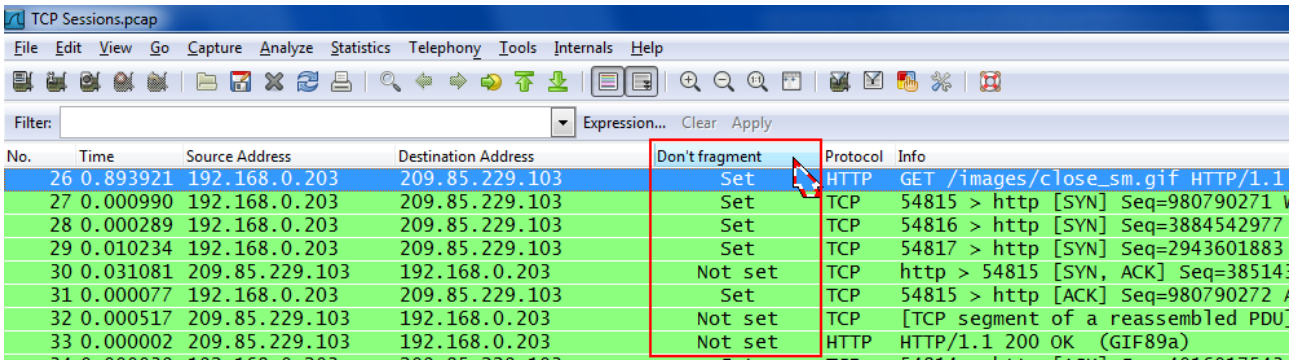
neuen Features werden hier vorgestellt. Detaillierte Informationen (nur Text) finden Sie in den gesammelten Release Notes unter: http://www.wireshark.org/docs/relnotes/

Verbessertes Column Handling

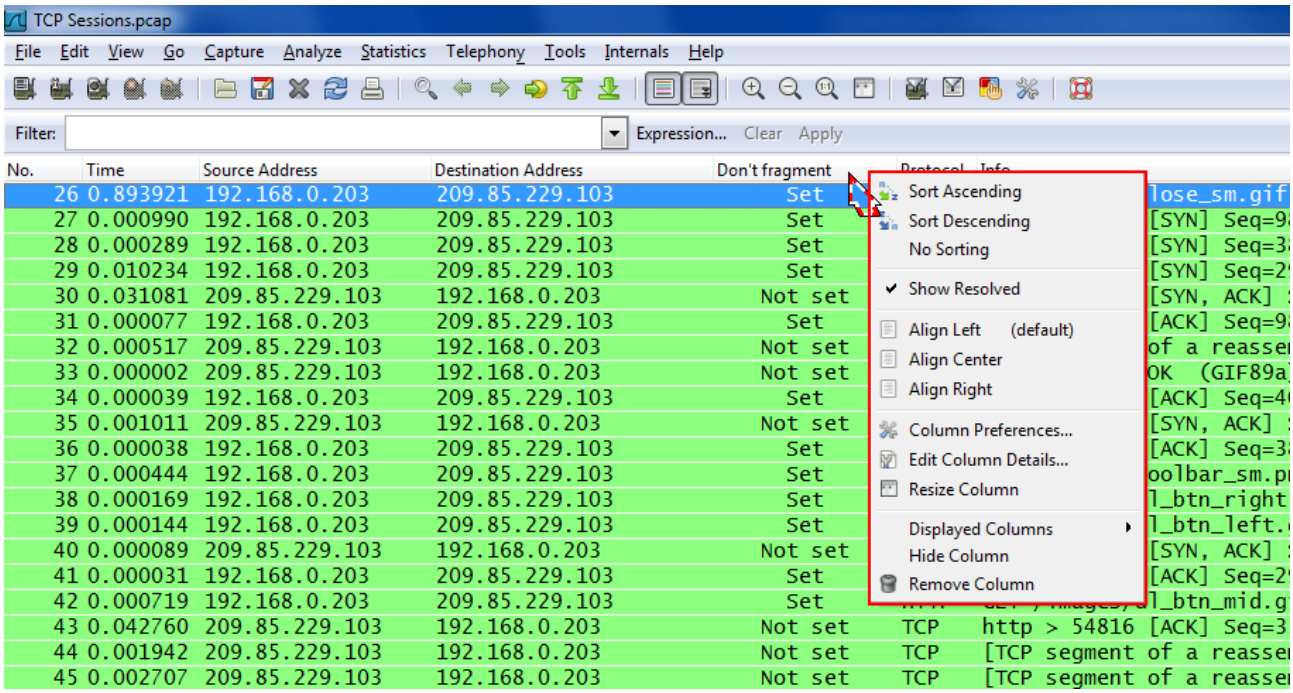
Neue Kolonnen müssen nicht mehr über das Menü Preferences hinzugefügt werden, sondern können mit rechtem Mausklick auf das entsprechende Protokollfeld direkt ausgewählt werden.



Die neue Kolonne befindet sich ganz rechts und kann durch Drag & Drop (neu) im Kolonnentitel horizontal an die gewünschte Position verschoben werden.

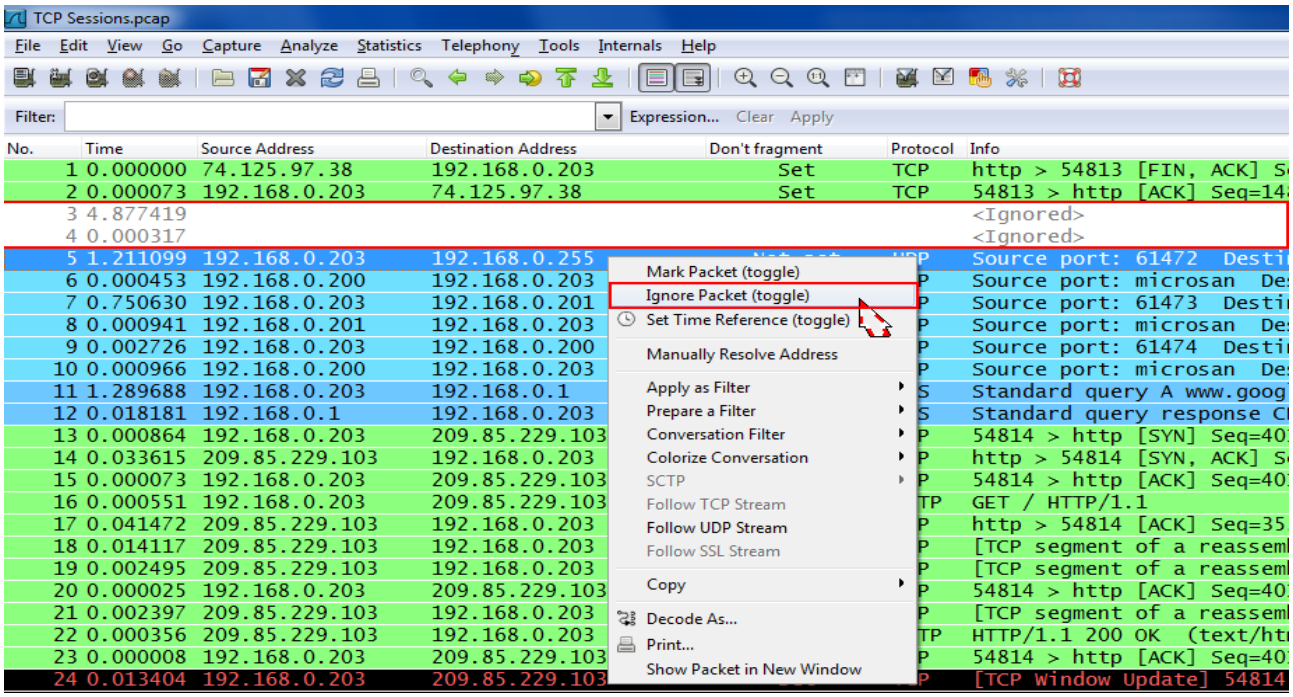


Rechter Mausklick im Kolonnentitel zeigt neue Optionen für die Darstellung dieser Kolonne

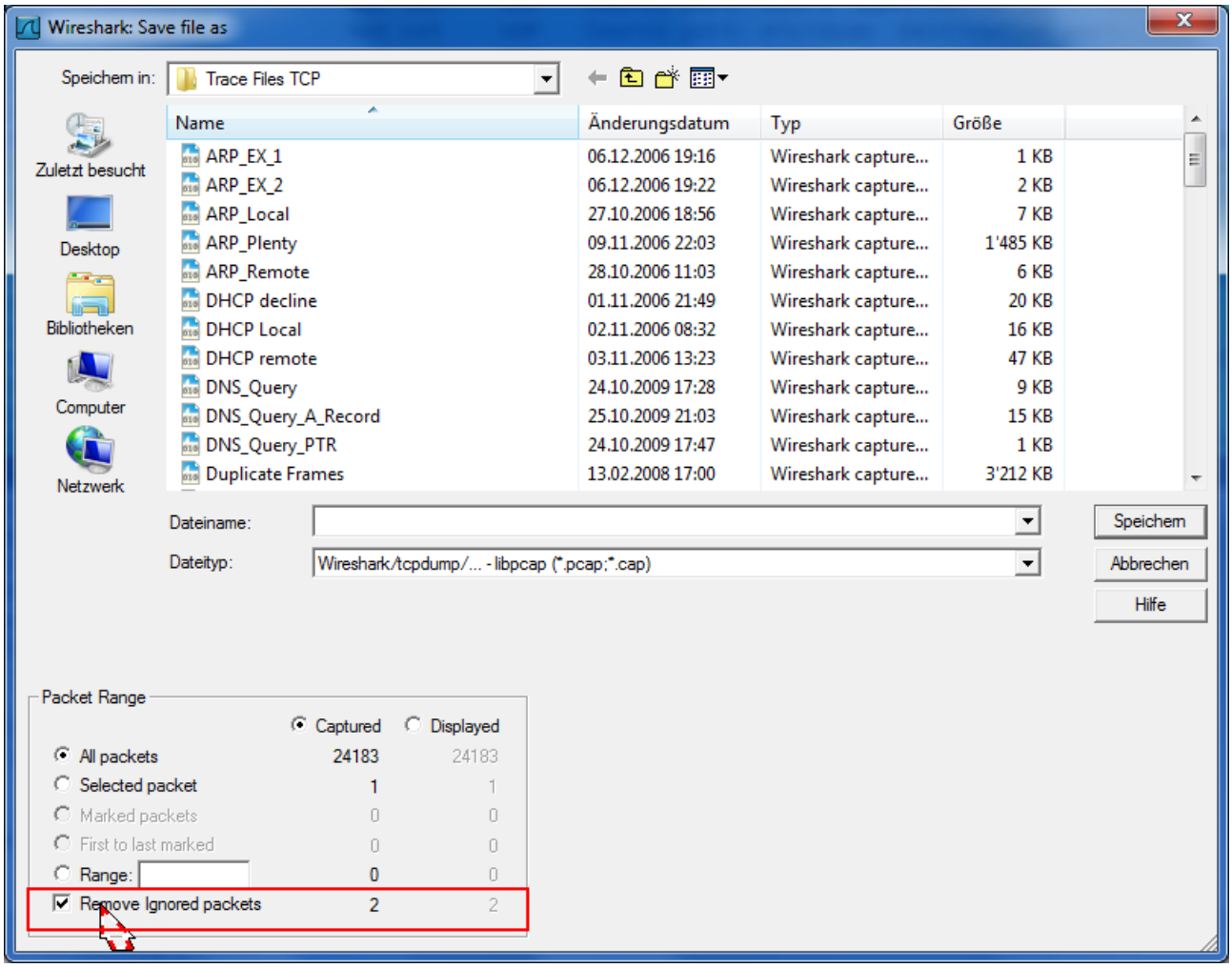


Unterdrücken ausgewählter Frames

Eine neue Funktion ermöglicht es, Frames individuell auszublenden, z.B. für Dokumentation usw.
Rechter Mausklick auf einem angewählten Frame zeigt die neue Funktion „Ignore Packet“



Beim „Speichern unter“ können die als “Ignored Packet” angewählten Frames entfernt werden.



Neue Navigation innerhalb einer TCP/UDP Konversation

Enthält ein Tracefile mehrere TCP Sessions oder UDP Conversations, kann mit zwei neuen Tastenkombinationen zum nächsten oder vorherigen, dazugehörenden Frame gesprungen werden. Die Navigation ist einfach: Einen Frame der TCP Session oder UDP Conversation anklicken und mit den Tastenkombinationen nach oben oder unten springen. Dabei wird auf den nächsten Frame mit gleichem IP Adress-Paar und TCP/UDP Port-Paar gesprungen.

Tastenkombinationen:

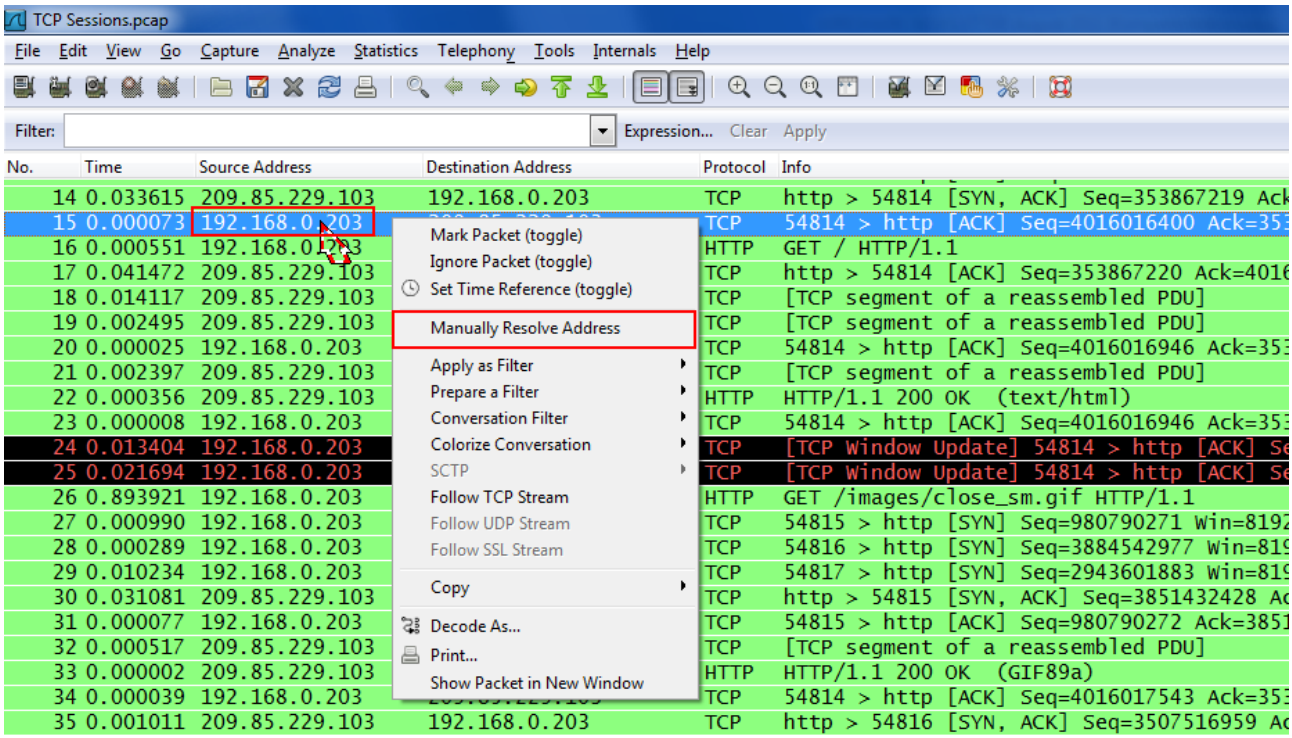
Ctrl , (Control und Komma) springt nach oben zum vorigen Frame der TCP/UDP Konversation

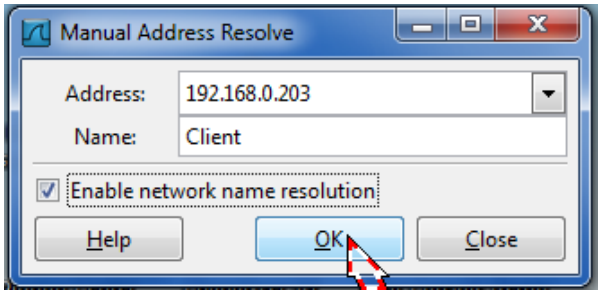
Ctrl . (Control und Punkt) springt nach unten zum nächsten Frame der TCP/UDP Konversation

Selektive Namensauflösung oder -Zuordnung

Diese neue Funktion erlaubt es, bei Bedarf nachträglich aus einem Tracefile heraus IP Adressen via DNS aufzulösen, oder wenn dies nicht möglich ist, manuell Namen zuzuordnen. Diese werden in der Wireshark-internen Namensliste abgespeichert und bleiben bis zum Schliessen von Wireshark erhalten.

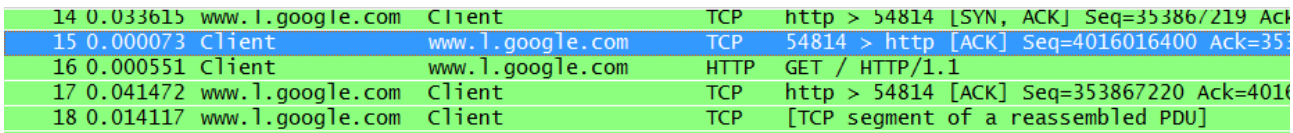
Rechter Mausklick auf einer Source oder Destination IP Adresse zeigt die neue Funktion „Manually Resolve Address“





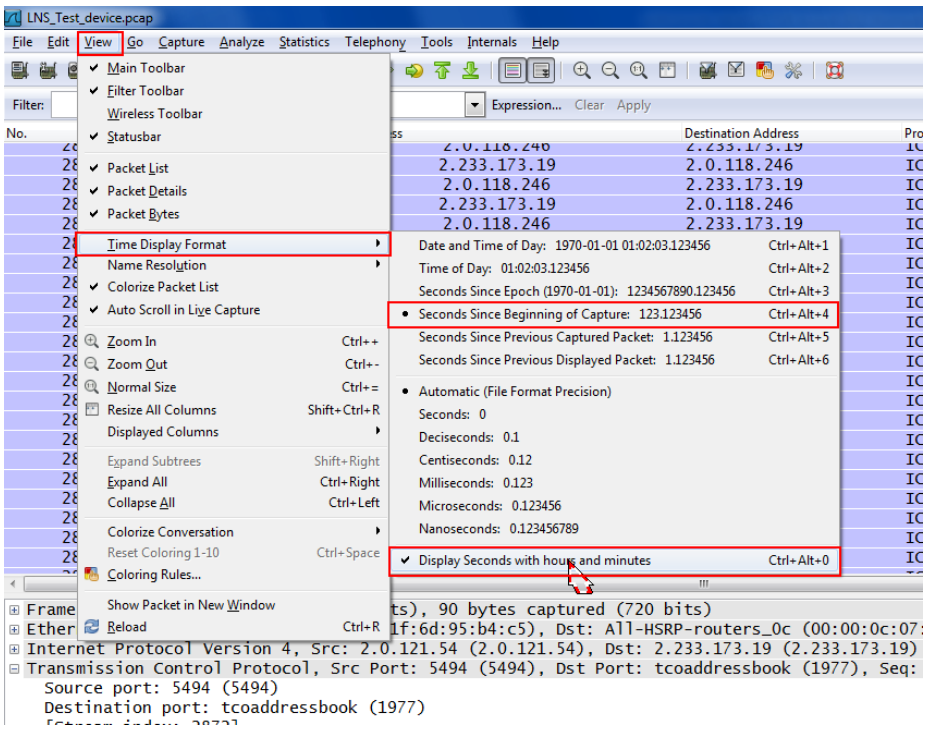
Für die Namensauflösung per DNS benötigt Wireshark Netzwerkanschluss und eine gültige DNS IP Adresse.

Wireshark versucht, die IP Adresse mit Reverse Lookup beim DNS Server aufzulösen. Gelingt dies nicht, wird der eingegebene Namen verwendet (siehe Bild unten).

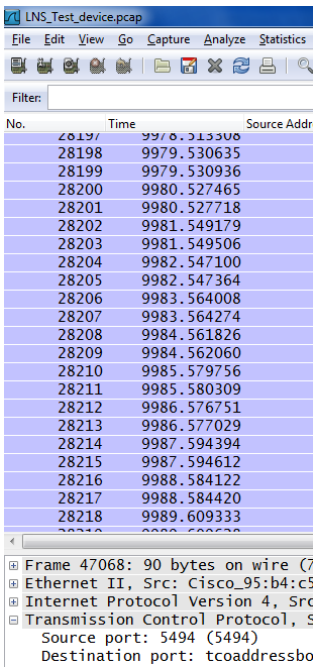


Neue Darstellung des Zeitstempels in Stunden, Minuten, Sekunden

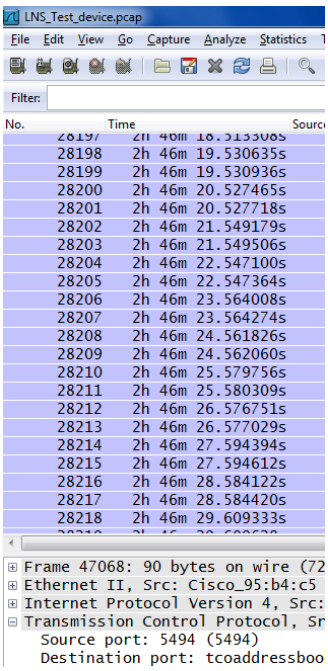
Das Zeitformat kann anstatt nur in Sekunden nun auch in Stunden, Minuten und Sekunden dargestellt werden:



Zeitformat in Sekunden



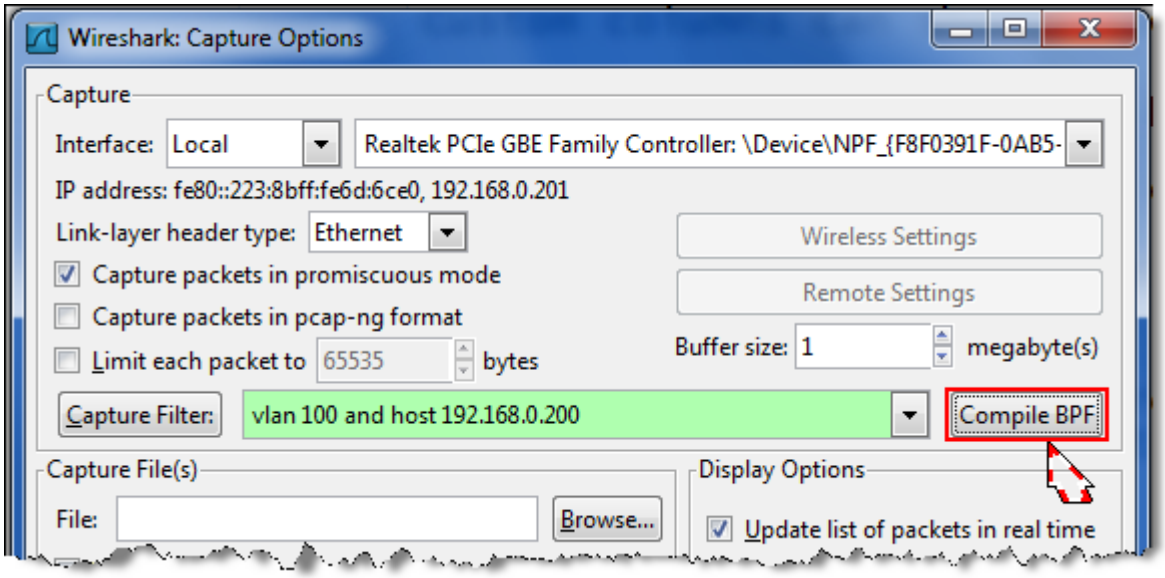
Zeit in Std./Min./Sek.



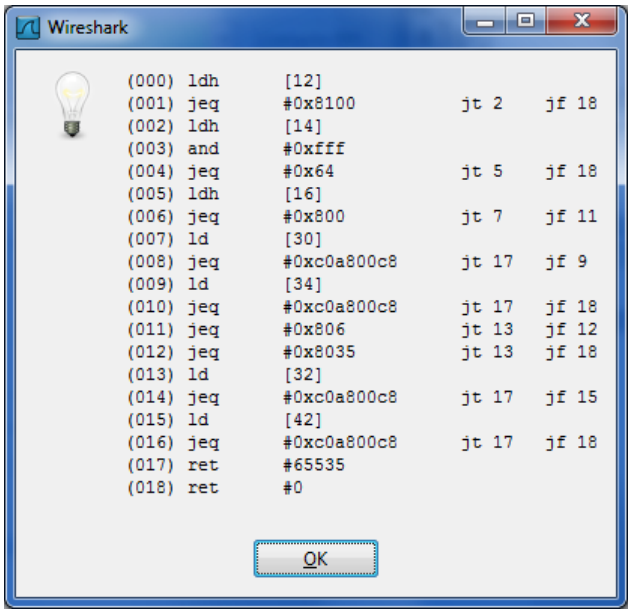
Syntax-Prüfung nun auch bei Capture Filtern

Die bewährte und beliebte Syntax-Prüfung wurde neu auch für Capture Filter eingeführt.

Roter Hintergrund = Filter ungültig Grüner Hintergrund = Filter gültig



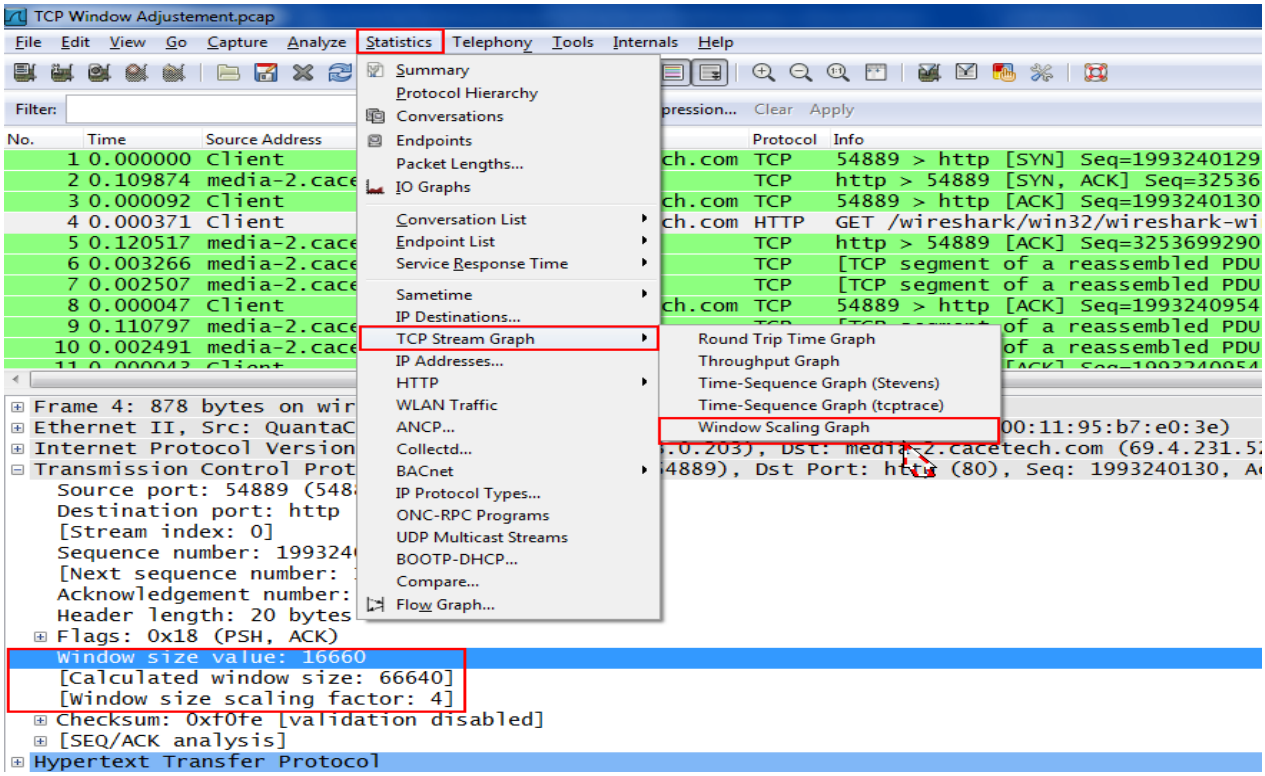
Zusätzlich ist es neu möglich, den Compiled Berkeley Packet Filter Code (BPF) anzuzeigen.



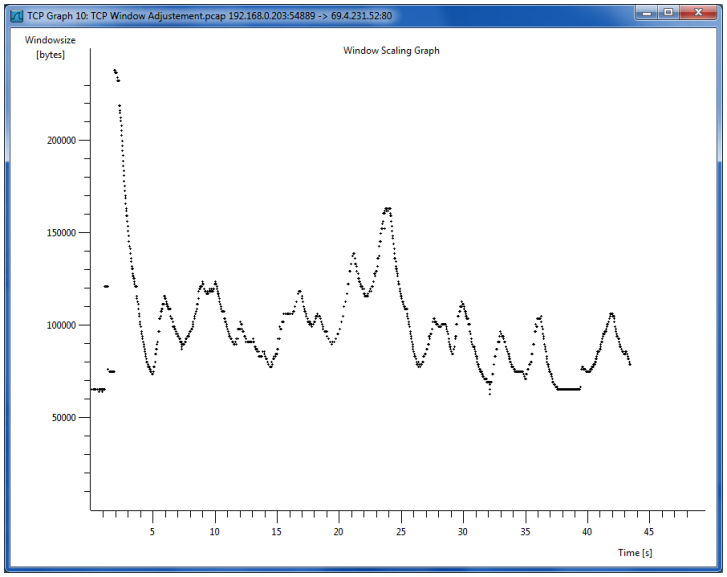
Hinweis: Die Capture Filter Syntax ist dieselbe wie diejenige von TCPdump. Auf dem Internet finden Sie viele weitere Details dazu, ein informativer Link ist auch www.gearbit.com

Neue TCP Window Scaling Optionen

Im Detail-Fenster wird neu die TCP Window Size sowohl „unscaled“ als auch „scaled“ angezeigt



Die neue Grafik „Window Scaling Graph“ zeigt den Verlauf der TCP Window Size



Die Grafik zeigt die Veränderung der TCP Window Size während einer TCP Session.

Der Client variiert den Wert zwischen ca. 60 KByte bis rund 240 KByte während der TCP Session von rund 45 Sekunden Dauer.

Der Window Scaling Faktor ist vier.

Wireshark Certified Network Analyst (WCNA)

Wireshark University
WIRESHARK®
CERTIFIED
NETWORK ANALYST

Die Wireshark University unter Leitung der renommierten Laura Chappell hat den neuen WCNA lanciert. Der Titel soll die Troubleshooting-Fähigkeit sowie das entsprechende Protokoll- und Wireshark Know-how unter Beweis stellen.
Dies kommt dem Bedürfnis der Netzwerkindustrie nach immer mehr zertifiziertem Netzwerk Know-how entgegen.

Der Test kann sowohl weltweit in Testcentern der Firma Kryterion http://www.kryteriononline.com als auch online am PC (mit Kameraüberwachung) durchgeführt werden.
WCNA besteht jedoch nicht nur aus einer einmaligen Prüfung, sondern bietet auf Wunsch auch die Möglichkeit, fortlaufend Sessions und Prüfungen zu absolvieren. Das entsprechende Programm heisst Continuing Professional Education (CPE) und bietet die Möglichkeit, CPE-Kreditpunkte zu sammeln.

Mehr Informationen über das umfangreiche Programm und die Schritte zur Zertifizierung finden Sie unter: http://www.wiresharktraining.com/certification

Der WCNA Test kostet US$ 299.

Erster Erfahrungsbericht:

Pascal Deller und Rolf Leutert von Leutert NetServices haben im September 2010 unter den ersten in Europa diesen Test erfolgreich absolviert, hier unsere Beurteilung:

Sehr detaillierte Kenntnisse von TCP Session Auf- und Abbau, Windows Size, Flags, Retransmission, Sequence Numbers, Duplicate Acks, Zero Window usw. sind notwendig.

Auch Kenntnisse weiterer Protokolle wie ARP, IPv4, UDP, DHCP, ICMP, RTP, DNS, POP, SMTP, HTTP und FTP werden verlangt. Einige Fragen beziehen sich auf Bereiche wie WLAN, VoIP und Security.

Im Bereich Wireshark werden gute Kenntnisse der zahlreichen Möglichkeiten vorausgesetzt. Die Fragen betreffen Themen wie etwa Display und Capture Filter, Round-Trip Berechnungen, Coloring Rules, Capture Options, Display Options, Profiles, Preferences usw.

Der Test kann insgesamt als recht anspruchsvoll beurteilt werden. Ohne gute Kenntnisse oder entsprechende Vorbereitungen ist wohl kein erfolgreiches Absolvieren möglich.

Unsere TCP/IP-Kurse vermitteln Ihnen die notwendigen Grundlagen, und mit der entsprechenden Anwendung in der Praxis sollten Sie jedoch gut gerüstet sein.

Im Weiteren wird von Laura Chappel über Internet ein „Exam Preparation Guide“ angeboten, mehr Informationen und Bestellung unter: http://www.wiresharkbook.com/epg/

Tipps, Tricks & Talks

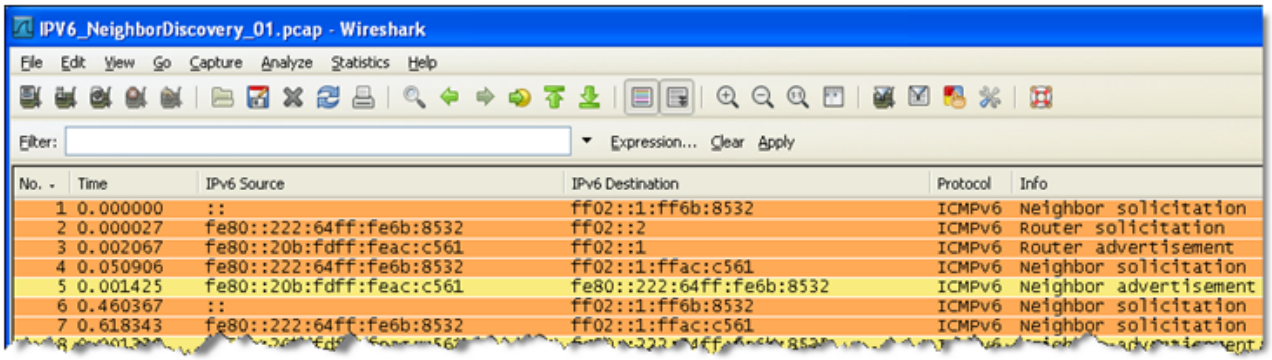
IPv6 entdecken mit Wireshark

Das grosse Interesse an unseren Kurzeinführungen von ½ bis 1 Tag, aber auch die Nachfrage nach unseren praktischen IPv6 Lab-Kursen zeigt: IPv6 ist nun definitiv zum Thema geworden. Während kleinere Firmen sicher noch abwarten können, werden IPv6-Kenntnisse von ISPs, Geräteherstellern und Netzwerkintegratoren in Kürze vorausgesetzt werden.
Die vorausgesagte jahrelange Koexistenz von IPv4- und IPv6-Netzen wird die Komplexität erhöhen und den Betrieb, den Unterhalt und die Fehlersuche noch anspruchsvoller werden lassen.

Wireshark kann natürlich auch in diesem Bereich wertvolle Unterstützung leisten, sämtliche Felder des IPv6 Headers werden bereits decodiert und dargestellt. Unterschiede bestehen jedoch nicht nur im Protokoll, auch viele Prozesse wurden neu definiert; nachfolgend einige Screenshots aus unserem IPv6-Kurs, welche einige der neue Abläufe zeigen.

Der Client erfragt den IPv6 Network Prefix vom Router und bildet die IPv6 Adresse selbst.

Frame #	
1	Duplicate Address Detection after Link-Local autoconfiguration
2	Router Discovery
3	Router Advertisement and global address autoconfiguration
4	Neighbor Discovery (searching for Router MAC)
5	Neighbor Advertisement (reply from Router with MAC)
6	Duplicate Address Detection with acquired global address

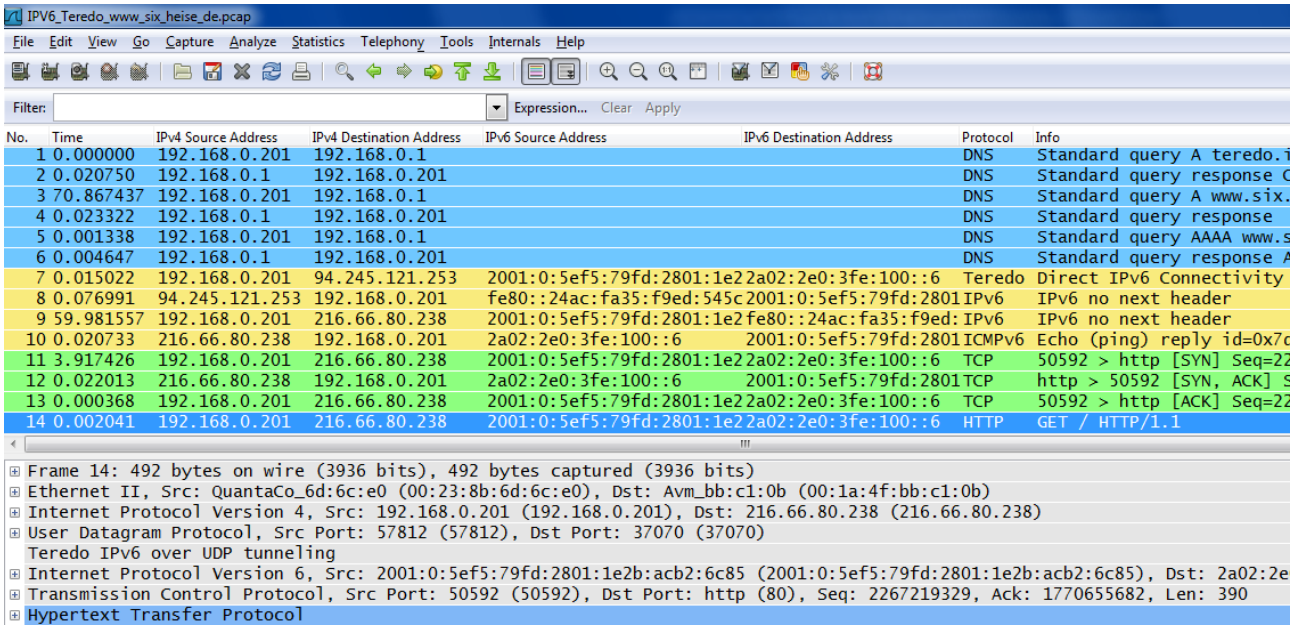


Quelle: Kurs ‚IPv6 Analyse mit Wireshark' von Leutert NetServices

Das beim IPv4 verwendete ARP Protokoll sowie Broadcast werden beim IPv6 nicht mehr eingesetzt. Für die Suche nach der MAC Adresse einer Zielstation wird die „Neighbor Solicitation" verwendet.

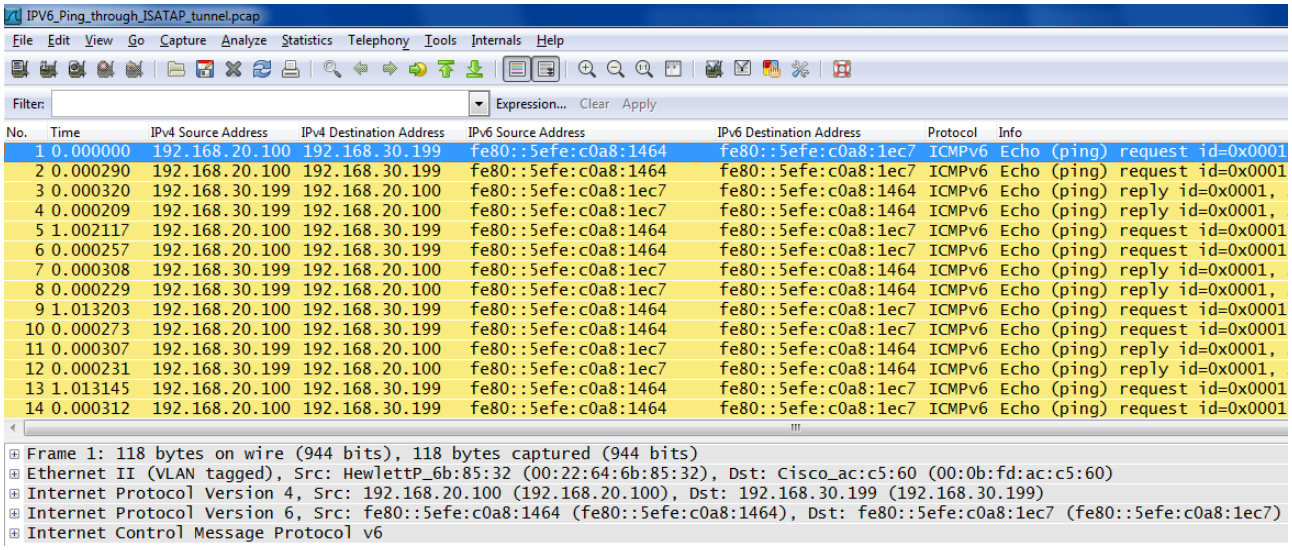
Tunneling-Mechanismen werden während der Migration häufig einsetzt werden, Sie ermöglichen den Transport von IPv6-Paketen über die bestehende IPv4-Infrastruktur. Wireshark kann die IPv4- und IPv6-Adressen kombiniert darstellen. Ideal für die Analyse von Tunnels.

Der Aufbau eines TEREDO Tunnels



Quelle: Kurs ‚IPv6 Analyse mit Wireshark' von Leutert NetServices

Ping durch einen ISATAP Tunnel



Quelle: Kurs ‚IPv6 Analyse mit Wireshark' von Leutert NetServices

Der ISATAP Tunnel verwendet eine IPv6 „Link Local Address", diese enthält in den letzten 4 Bytes die IPv4 Adresse (in HEX).

Hinweise

Die nächsten öffentlichen Wireshark Kurse und Präsentationen

Gerne offerieren wir Ihnen interne Kurse oder Tech-Sessions nach ihren Wünschen zu den aufgeführten Themen.

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

---

Einführungskurse:

Net Analyse – Protokollanalyse mit Wireshark

Datum:	26.09.2011 – 27.09.2011 (2 Tage)
Ort:	Studerus, Schwerzenbach
Kurs-Details und Anmeldung bei	Studerus

IPv6 – Einstieg zum IPv6 Protokoll

Datum:	31.10.2011 (1 Tag)
Ort:	Studerus, Schwerzenbach
Kurs-Details und Anmeldung bei	Studerus

WLAN – Analyse

Datum:	12.12.2011 – 13.12.2011 (2 Tage)
Ort:	Studerus, Schwerzenbach
Kurs-Details und Anmeldung bei	Studerus

Lab basierende Kurse

IPv6 Workshop mit Wireshark

Datum:	19.09.2011 – 20.09.2011 (2 Tage)
Ort:	Hochschule Rapperswil INS, Rapperswil
Kurs-Details und Anmeldung bei	Hochschule Rapperswil

VoIP Protokollvertiefung mit Wireshark

Datum:	17.10.2011 – 18.10.2011 (2 Tage)
Ort:	Hochschule Rapperswil INS, Rapperswil
Kurs-Details und Anmeldung bei	Hochschule Rapperswil

WLAN Netzwerkanalyse mit Wireshark und AirPcap

Datum:	05.12.2011 – 07.12.2011 (3 Tage)
Ort:	Hochschule Rapperswil INS, Rapperswil
Kurs-Details und Anmeldung bei	Hochschule Rapperswil

TCP/IP Netzwerkanalyse mit Wireshark

Datum:	21.11.2010 - 23.11.2010 (3 Tage)
Ort:	Hochschule Rapperswil INS, Rapperswil
Kurs-Details und Anmeldung bei	Hochschule Rapperswil

Es freut uns, Sie in einem unserer Kurse zu begrüssen.

Besten Dank für Ihr Interesse
Mit freundlichen Grüssen Rolf Leutert