WIRE**SHARK** Newsletter September 2012

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 1.80
- Gerald Combs am "Meet the Geek" Event in Zürich
- SharkFest'12 an der Universität von Berkeley in Kalifornien
- Capturing Control Plane Traffic in Cisco UCS
- Datenaufzeichnung in Virtuellen Maschinen
- Tipps, Tricks & Talks: Datenaufzeichnung mit zwei Interfaces
- Hinweise: Daten nächster Wireshark Kurse und Präsentationen

Neue Features der Wireshark Versionen 1.6.2 bis 1.8.2

Die Versionen 1.6.2 bis 1.6.10 enthalten Protokollerweiterungen und Bug Fixes. Markante neue Funktionen, welche teilweise schon lange auf der Wunschliste standen, wurden nun integriert. Einige dieser neuen Features werden hier vorgestellt. Weitere Informationen (nur Text) finden Sie in den gesammelten Release Notes unter: http://www.wireshark.org/docs/relnotes/

Die wichtigsten Neuerungen ab Version 1.8.0

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

Folgende Neuerungen werden nachfolgend detailliert beschrieben:

- Aufzeichnen von mehreren Interfaces
- Eigene Filter pro Interface
- Neues Fileformat pcap-ng
- Pcap-ng als Default File Format
- Freitext Felder für Notizen zu Files oder einzelnen Frames
- DNS Transaction ID neu im Frame Summary
- Quick Filter Buttons

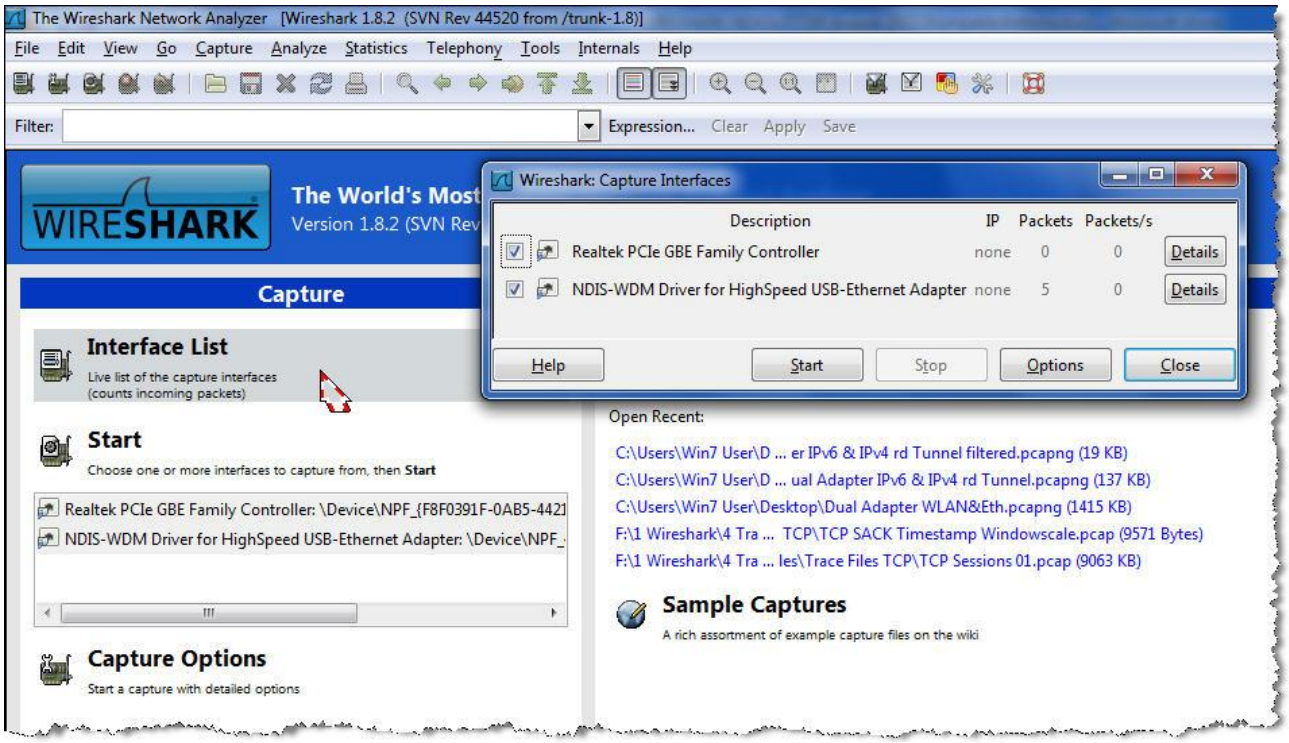
Weitere Neuerungen mit Kurzbeschrieb:

- TCP Timestamps Anzeige kann unter TCP Preferences nun ausgeschaltet werden.
  Diese Felder dienen der TCP Round-Trip Messung, sind jedoch keine grosse Hilfe bei der Fehlersuche und können deshalb neu in der Summary Zeile unterdrückt werden. „Ignore TCP Timestamps in summary"

- TCP Symptome „Fast Retransmission“ und „Retransmission“ neu in Kategorie „Notes“.
  Diese Symptome waren bisher in der Kategorie „Warning“, sind jedoch im TCP Ablauf normale Vorgänge.
- TCP Symptom „Windows Update“ wird nicht mehr mit Coloring Rule markiert.
  Diese wurden bisher als Fehlermeldung schwarz hinterlegt, sind jedoch im TCP Ablauf normale Vorgänge.
- TCP und UDP Header Checksum wird per Default nicht mehr geprüft.
  Führte zu häufigen, jedoch falschen Fehlermeldung bei Checksum Offloading. Diese Auslagerung der Checksum Berechnung an den Adapter ist bei neueren Ethernet Karten der Standard und beschleunigt die Verarbeitung der Frames.
- TCP Stream Index Definition wurde geändert.
  Wireshark erkennt TCP Sessions und filtert mit „Follow TCP Stream“ (rechte Maustaste) auf eine Session, der neue Filterstring dazu heisst „tcp.stream=0“
- Neue definierte Coloring Rules werden nun zuoberst auf der Liste eingetragen.
  Selbst definierte Coloring Rules wurden bisher zuunterst auf der Coloring Liste eingetragen; da die Liste von oben nach unten nach dem „first match“ Prinzip funktioniert, wurden die neuen Einträge oft durch bereits vorhandene „overruled“ und mussten manuell nach oben verschoben werden.
- GeoIP unterstützt nun auch IPv6.
  Bisher wurde für die geographische Darstellung von Adressen nur IPv4 unterstützt.
- File Export Funktion wurde verbessert.
  Die Export Funktionen wurden granularer gegliedert (siehe unter Menu File)
- „Decode As“ Einstellungen werden neu auch im Profil gespeichert
  Bisher wurden diese Einstellungen nicht im Profil abgespeichert und gingen deshalb beim Schliessen von Wireshark verloren.
- „Flow Graph“ übernimmt neu die Zeitdarstellung wie in Summary Window.
  Formatänderungen der „Time“ Kolonne im Summary Window werden nun auch in Flow Graph übernommen.
- „Time Shift“ Funktion ermöglicht es, die Zeitstempel von Frames zu verändern.
  Trace Files welche auf verschiedenen Geräten aufgenommen wurden, haben oft nicht synchrone Zeitstempel, beim „Mergen“ dieser Files nach Zeit stimmt dann die Reihenfolge der Pakete nicht. Mit dieser Funktion kann dies korrigiert werden.
- Expert LEDs Coloring Code
  Die Farbe des Expert LED/Button im Wireshark links unten signalisiert die höchste Stufe von Symptomen, welche in einer Aufzeichnung vom Protocol Expert detektiert wurden. Von CHAT (Blau), NOTES (Türkis), WARNINGS (Gelb) bis ERRORS (Rot). Beim Platzieren des Cursors auf dem Button wird neu die Erklärung des Farbcodes eingeblendet. Die Funktion dieses Expert Buttons finden Sie in unserem Newsletter März 2010
  http://www.wireshark.ch/download/Wireshark_Newsletter_2010_03.pdf

Aufzeichnung von mehreren Interfaces

Was im Wireshark für WLAN schon immer möglich war, die gleichzeitige Aufzeichnung von verschiedenen Frequenz-Kanälen mit Hilfe von mehreren AirPcap Adaptern, ist nun auch mit mehreren Ethernet Karten möglich - eine Funktion, welche schon länger auf der Wunschliste der Wireshark Benutzer und Entwickler stand. Dies eröffnet völlig neue Möglichkeiten in der Analyse: So können zum Beispiel Daten vor und nach einem Firewall, Router oder Switch aufgezeichnet werden; oder Daten im WLAN und gleichzeitig nach dem Access Point auf der wired Seite.

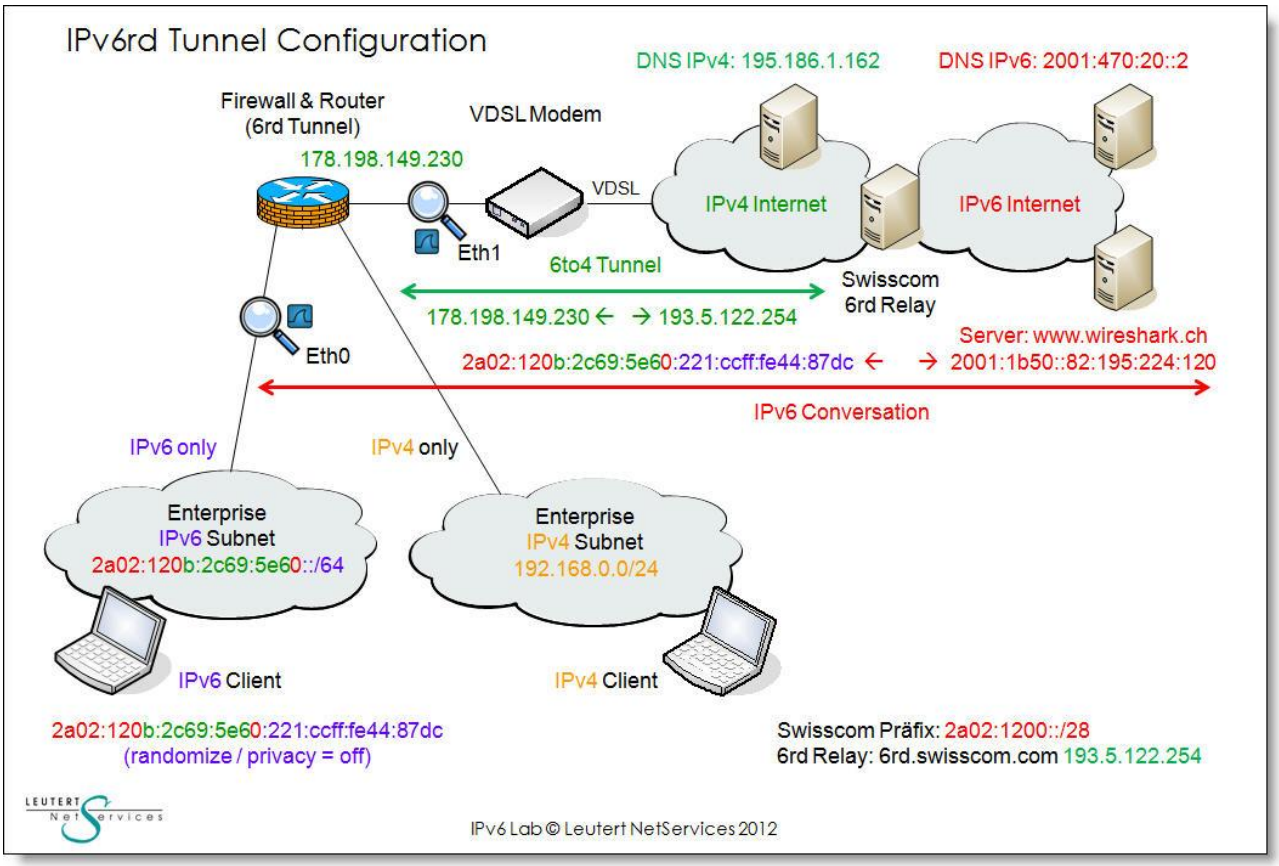


Auswahl von mehreren Interfaces für die Aufzeichnung

Da Notebooks meistens nur über einen Ethernet Anschluss verfügen, kann z.B. eine handelsübliche Ethernet Express Card oder ein Ethernet USB Adapter zur Erweiterung verwendet werden.

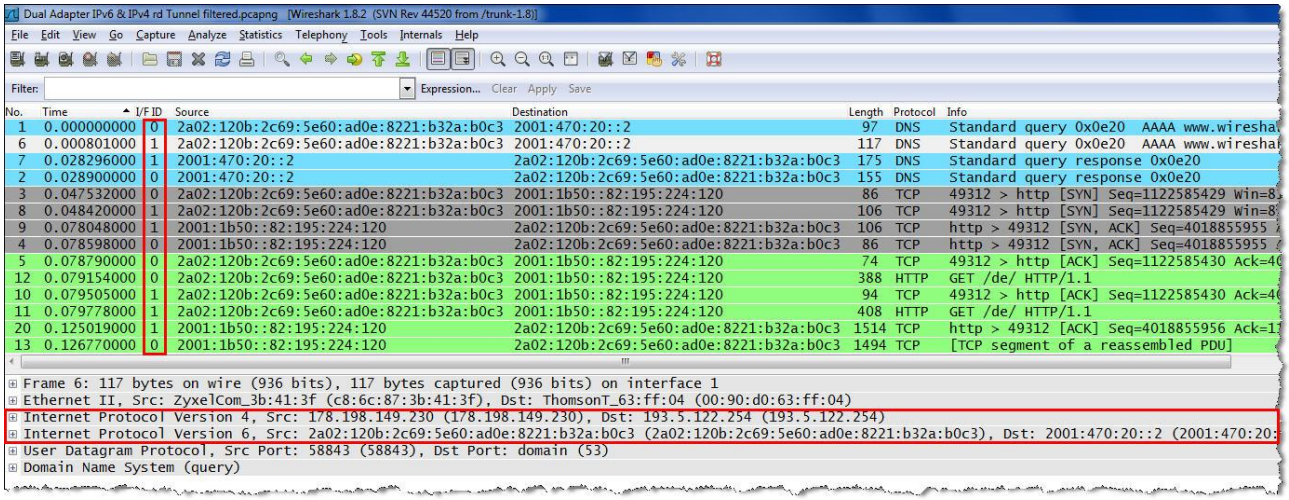
Eine von vielen sinnvollen Anwendungen zeigt das folgende Beispiel: In einem gemischten Umfeld mit IPv4 und IPv6 werden die Daten vor (Eth0) und nach (Eth1) dem Router aufgezeichnet. Der Router bildet Richtung Internet einen IPv6 RD Tunnel und verpackt IPv6 in IPv4 Frames. Dies ermöglicht es, sowohl die „native IPv6 Frames“ als auch die verpackten Daten im selben Tracefile darzustellen und zu analysieren.

Bemerkung: Beachten Sie bitte auch die Framenummern im Wireshark Screenshot, sie sind nicht sequenziell, da die Frames nach der Time Kolonne sortiert sind. Mehr dazu in unserer Rubrik Tipps, Tricks & Talks weiter unten im Newsletter.



IPv6rd Testlab mit zwei Wireshark Messpunkten

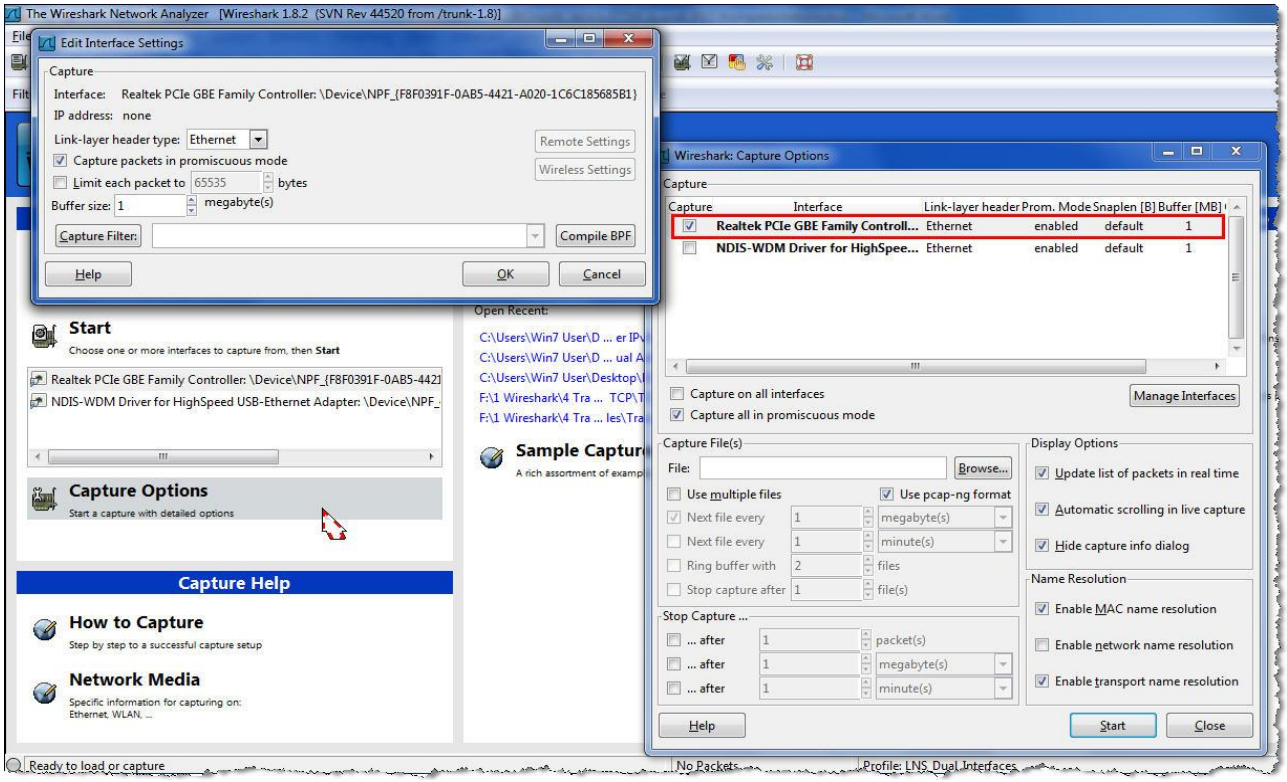
Die Interface IDs **0** und **1** werden (nur) im neuen Fileformat Pcap-ng mit abgespeichert und ermöglichen die Anzeige in einer eigenen Kolonne. In dieser Anordnung werden alle Frames doppelt aufgezeichnet, die Frames mit I/F ID 0 sind native IPv6, die Frames mit I/F ID 1 sind die in IPv4 verpackten Frames:



*Die Frames **vor** (I/F ID 0) und **nach** (I/F ID 1) dem Tunnel Router*

Eigene Capture Optionen pro Interface

Bei der Aufzeichnung vom mehreren Interfaces z.B. in verschiedenen Subnetzen kann es sinnvoll sein, auch verschiedene Capture Filter anzuwenden. Dies ist durchaus möglich, die Funktion ist nur etwas versteckt zu finden:
Beim Mausklick auf die „Capture Options" öffnet sich das Capture Option Panel mit den verfügbaren Interfaces. Durch Doppelklick auf eines der Interfaces öffnet sich ein weiteres Panel mit den einstellbaren Optionen für das ausgewählte Interface.



Optionen wie Capture Filter sind pro Interface konfigurierbar

Neues File Format .pcapng

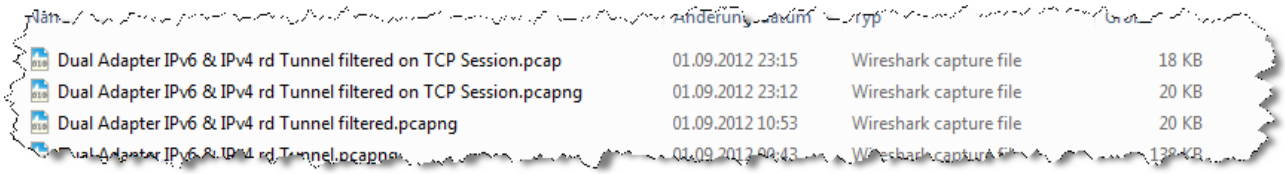
Schon seit einigen Wireshark Versionen steht dieses neue Fileformat als Option zur Verfügung und wurde während dieser Zeit getestet und verbessert. Mit Version 1.8 wird nun pcap-ng (next generation) definitiv eingeführt. Das neue Format enthält zahlreiche Verbesserungen und speichert gegenüber dem pcap Format mehr Informationen mit den eigentlichen Frames ab.
Das Pcap File Format wurde vor langer Zeit zusammen mit TCPdump und dem Driver LibPcap definiert und wird weiterhin unterstützt werden. Nicht zuletzt da TCPdump millionenfach in Geräten wie Firewalls, Routers Unix Servers etc. standardmässig installiert ist.

Die wichtigsten Information, welche im neuen Fileformat zusätzlich abgespeichert werden:

- Über DNS aufgelöste Namen zu IP Adressen (auch IPv6)
- Interface I/D
- Freitext Notizen zum File
- Freitext Notizen zu einzelnen Frames
- Beim Aufzeichnen verlorene Frames (Dropped Packets)
- Beim Aufzeichnen aktive Capture Filter

Pcap-ng als Default File Format

Ab Wireshark Version 1.8 wird pcap-ng als Default Format beim Abspeichern von Files verwendet. Aus Gründen der Rückwärtskompatibilität wird jedoch das pcap Format weiterhin zur Speicherung angeboten. Diese Option ist neu unter dem Menupunkt File -> Export Specified Packets…
Files mit dem alten pcap Format können mit Wireshark geöffnet und z.B. mit Freitext Notizen versehen als pcap-ng neu abgespeichert werden; dies sogar unter demselben Namen, so dass es sinnvoll ist, die z.B. im Windows 7 per Default unterdrückten File Extensions einzublenden.

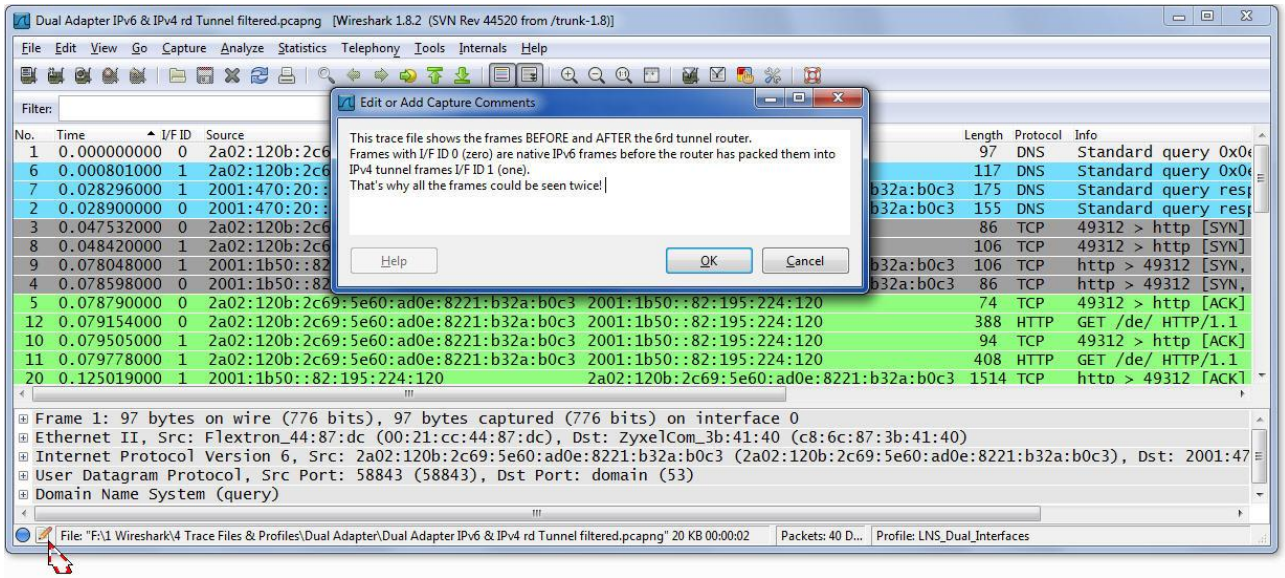


*Filenamen **mit** File Extensions in Windows 7*

Bemerkung: Wenn Wireshark Version 1.8 auf einem Gerät installiert wird, auf dem noch keine ältere Wireshark Version installiert war, wird pcap-ng die Default Einstellung für abzuspeichernde Files.
Wenn jedoch bereits eine frühere Wireshark Version installiert ist, und sie wählen bei dem Upgrade die Option „Profile beibehalten“, wird die File Format Einstellung gemäss Profil der Vorgängerversion übernommen, d.h. Sie müssen die Speichereinstellung u.U. auf das neue Fileformat ändern.

Freitext Felder für Notizen zu Files oder einzelnen Frames

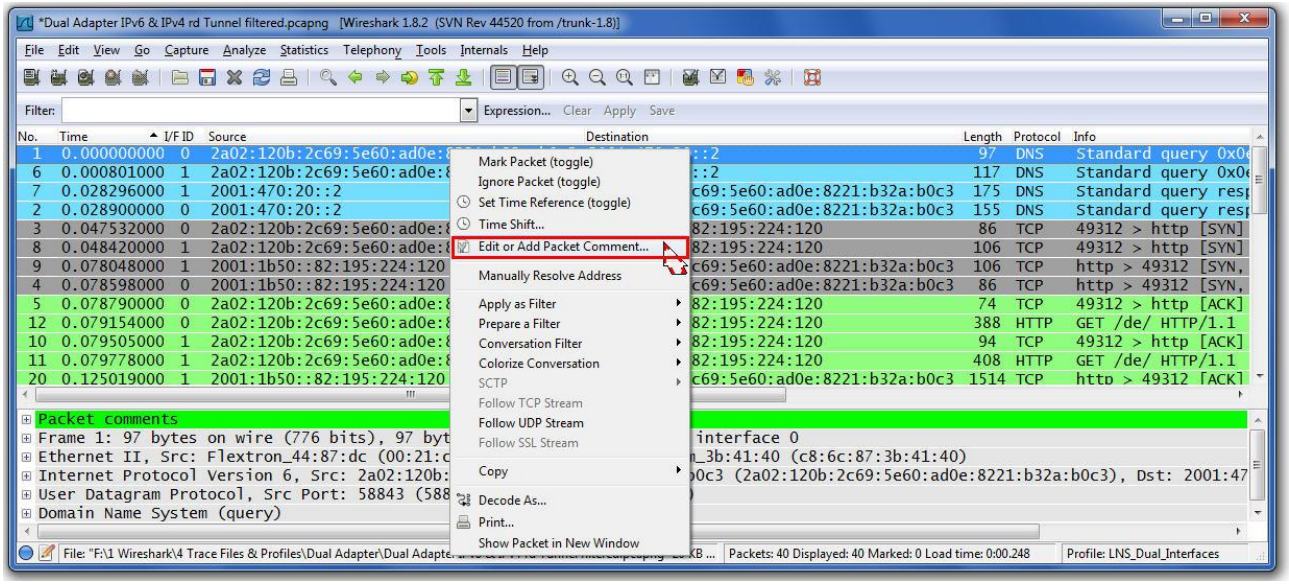
Eine weitere Wireshark Funktion, welche oft gewünscht wurde, das Kommentieren eines ganzen Tracefiles oder einzelner Frames, ist nun mit dem neuen Fileformat pcap-ng verfügbar. Diese erweist sich als sehr nützlich, wenn Tracefiles/Frames für die Speicherung mit Text versehen werden sollen oder ein File zur Analyse an weitere Personen weitergeleitet werden soll. Die Funktion File Comment ist über den Read/Edit Comment Button links unten im Wireshark abzurufen.



Freitext Kommentar zu einem Capture File

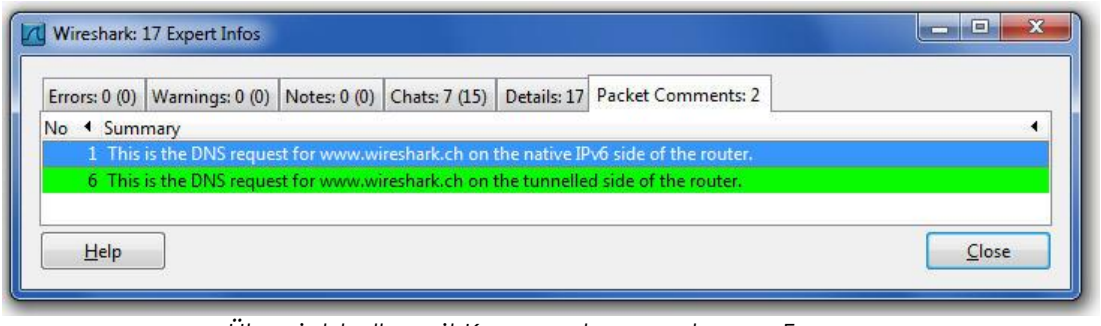
Der Text zu einem Capture File ist auch unter der Menuposition Statistics -> Summary einzusehen.

Einzelne Frames können ebenfalls mit Kommentar versehen werden, dies durch rechten Mausklick auf den gewünschten Frame und Wahl der Option „Edit or Add Packet Comment…“



Einzelne Frames können zusätzlich mit Kommentar versehen werden

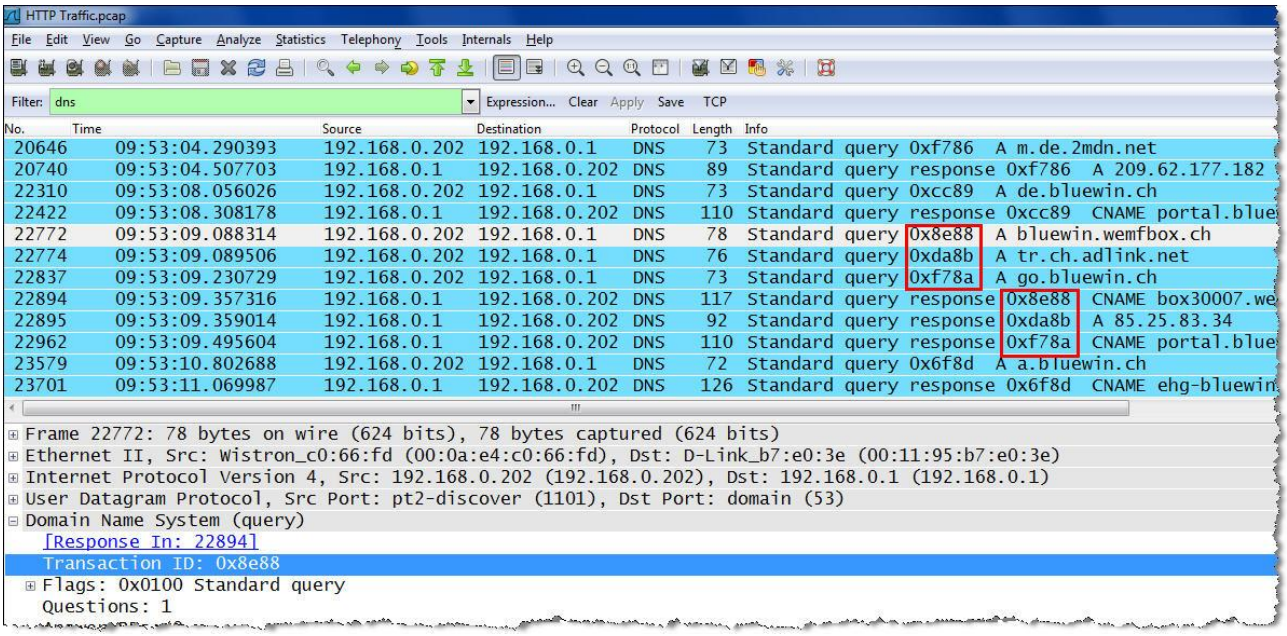
Der Text ist unter den einzelnen Frames sichtbar, kann aber durch Mausklick auf den Expert Button (links unten) und Auswahl der Position „Packet Comments“ auch als Übersicht dargestellt werden.



Übersicht aller mit Kommentar versehenen Frames

DNS Transaction ID neu auch im Frame Summary

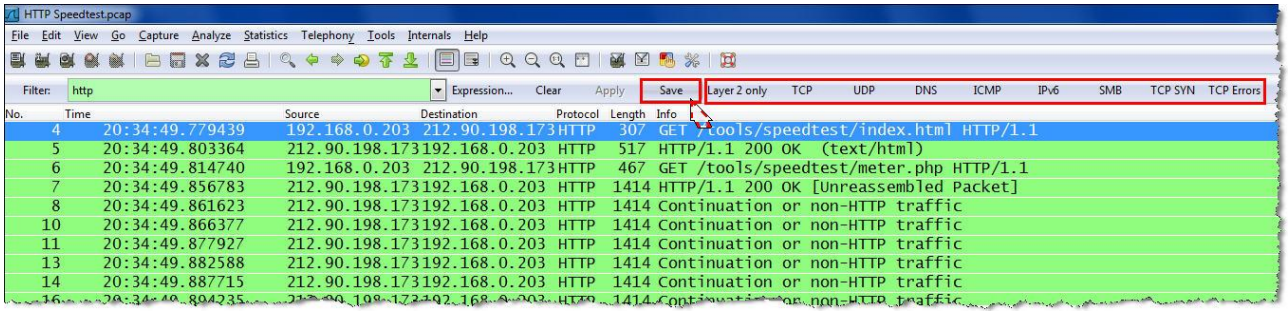
Jeder „DNS Query“ enthält eine Transaction ID, welche im „DNS Query Response“ als Referenz zur Anfrage wiederum mitgesendet wird. Bisher war diese Transaction ID nur im Packet Detail Window zu sehen. Um die Zuordnung der Antworten zur Anfrage zu erleichtern, wird diese Transaction ID neu auch im Packet Summary Window angezeigt. Dies beschleunigt die Suche nach einer DNS Antwort auf eine Anfrage, da diese u.U. erst viele Frames später eintreffen kann.



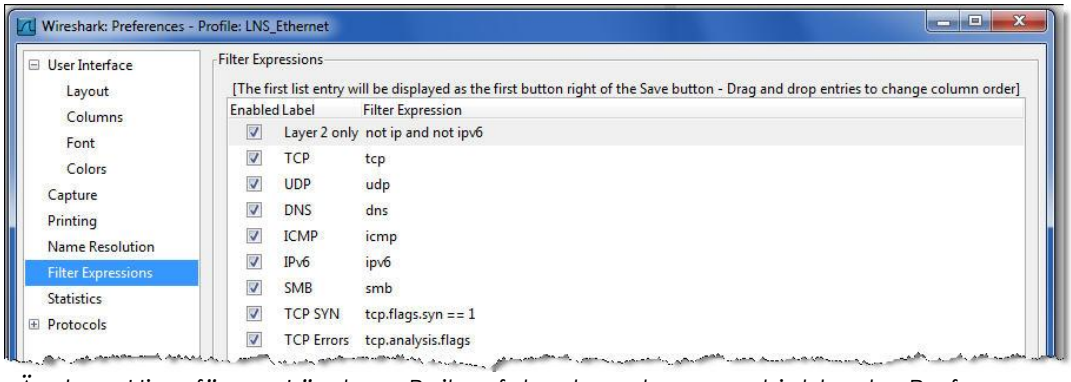
Die DNS Transaction ID wird nun auch im Packet Summary angezeigt

Quick Filter Buttons

Eine weitere neue Funktion, welche den Einsatz von Display Filtern noch komfortabler gestaltet. Häufig verwendete Filter Strings lassen sich durch einfaches Klicken auf den „Save" Button in der Filterzeile als „Quick Filter Button" abspeichern. Wie die meisten Konfigurationsänderungen in Wireshark werden auch diese Settings automatisch im aktuellen Profil abgespeichert.



Quick Filter Buttons ermöglichen „One Click Filtering"



Ändern, Hinzufügen, Löschen, Reihenfolge tauschen geschieht unter Preferences

Gerald Combs am "Meet the Geek" Event in Zürich

Am 6. Februar 2012 genossen Wireshark-Begeisterte aus der Schweiz, Deutschland und Österreich ein besonderes Event: den Besuch von **Gerald Combs** in Zürich. An der Veranstaltung "Meet the Geek" im Hotel Hilton Zürich Airport ergab sich die einmalige Gelegenheit, den Gründer des Open Source Tools live zu erleben.
Auf unterhaltsame Weise plauderte Gerald über die ereignisreiche Geschichte des Netzwerkanalyse-Tools, vom ehemaligen Ethereal bis zum heutigen Wireshark.

Der seltene Gast (Gerald reist sehr ungern) aus Davis, Kalifornien, informierte generell über spannende Details des Open Source Systems hinter Wireshark und stellte markante Features der kommenden Version vor.

Wireshark gilt weltweit als Musterbeispiel eines äusserst erfolgreichen Open Source Projekts, das alle kommerziellen Mitbewerbsprodukte in kürzester Zeit auf die hinteren Ränge verwies und es heute auf die erstaunliche Zahl von rund 500'000 Downloads pro Monat bringt

Gerald wurde von vielen Teilnehmern als sehr sympathisch und authentisch empfunden.

Gerald Combs, Gründer von Wireshark

Mehr Informationen und Fotos unter http://www.wireshark.ch/de/wireshark-software/events

SharkFest'12 an der Universität von Berkeley in Kalifornien

Bereits zum fünften Mal, jedoch erstmals an der Universität von Berkeley in Kalifornien, fand vom 24. bis 27. Juni 2012 die jährliche Wireshark Developer und User Conference statt. Das Sharkfest hat sich inzwischen zu einem Treffen von Wireshark Experten aus allen Kontinenten etabliert und bietet Sessions über die praktische Anwendung von Wireshark für Protokollanalyse und Troubleshooting.

Rolf Leutert von Leutert NetServices präsentierte im Advanced Track Sessions zu den Themen:

A-3: Tuning Win7 Using Wireshark's TCP Stream Graph (case study)

A-5: Analyzing WLAN Roaming Problems (case study)

Sämtliche Präsentationen sind verfügbar unter: http://sharkfest.wireshark.org/sharkfest.12/

Capturing Control Plane Traffic in Cisco UCS

Die Funktion ist wenig bekannt, aber trotzdem sehr praktisch; sie ermöglicht das Aufzeichnen von Daten direkt auf dem Control Plane der CISCO Unified Computing und Server (UCS) Familie. Dadurch kann der interne Datenverkehr zur Server-Steuereinheit, der sogenannten Fabric Interconnect (FI), ohne umständliches Anschliessen eines externen Gerätes analysiert werden.

Das integrierte Tool heisst „Ethanalyser", basiert auf dem Wireshark Open Source Code und unterstützt Capture- und Display-Filters. Die aufgezeichneten Daten können als Text im CLI angezeigt werden oder zur besseren Verarbeitung als .pcap File exportiert und mit Wireshark geöffnet werden.

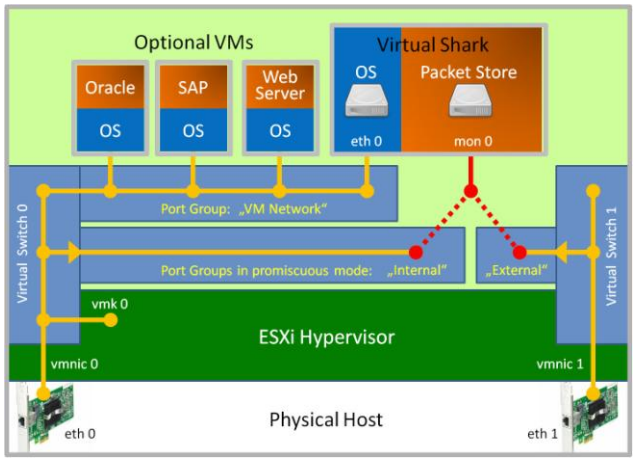
Mehr Informationen über die umfangreichen Möglichkeiten finden Sie unter:
http://jeffsaidso.com/2012/07/capturing-control-plane-traffic-in-ucs/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+JeffSaidSo+%28Jeff+Said+So%29&utm_content=Google+Reader

oder im PDF Dokument:
http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps11541/white_paper_c11-673817.pdf

Besten Dank an M. Fischer von SWISS TXT Schweizerische Teletext AG für den Hinweis auf dieses Tool.

Datenaufzeichnung in Virtuellen Maschinen

Immer häufiger wird von Kunden das Bedürfnis, auf Virtuellen Maschinen Daten aufzeichnen zu können, an uns herangetragen. Natürlich ist es möglich, Wireshark auf einem virtuellen Server zu installieren und laufen zu lassen, dies führt jedoch oft zu riesigen Datenmengen und grossen Tracefile (bis Terabytes), welche vom Wireshark nicht mehr geöffnet und verarbeitet werden können. Die Firma **RIVERBED** (Träger von Wireshark) bietet kommerzielle Produkte, welche in diesem Bereich zum Einsatz kommen. **Shark Appliances** unterstützen 10 Gigabit Ethernet Karten und bieten Speicherplatz bis 32 Terabytes.



Virtual Shark basierend auf VMware

Neu ist nun unter dem Namen **„Virtual Shark"** eine Software erhältlich, welche direkt auf VMware aufsetzt und durch Zugriff auf den virtuellen Switch den internen Datenverkehr aufzeichnen kann.
Eine weitere Anwendung ist die Installation von Virtual Shark auf einer beliebigen Hardware, welche dann als kostengünstige Probe im Netz verteilt an kritischen Stellen Daten aufzeichnet und speichert. Der Zugriff erfolgt über die **PILOT Console**, in welcher Wireshark integriert ist.
Mehr Infos auf unserer Webseite unter: www.wireshark.ch/de/produkte/virtual-shark

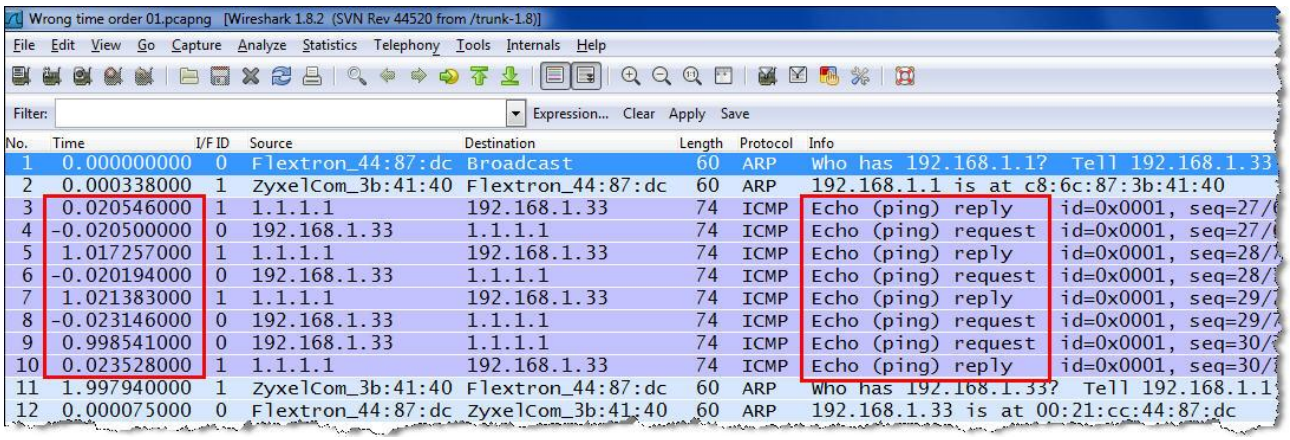
Tipps, Tricks & Talks

Datenaufzeichnung mit zwei (oder mehr) Interfaces

Wie bereits erwähnt, bietet diese neue Funktion viele neue Einsatzgebiete, da Aufzeichnungen von mehreren Interfaces ins selbe Tracefile „gemergt" werden. Bei der Analyse von Full-Duplex Verbindungen kommen auch häufig TAPs als Abgriff zum Einsatz, welche dann für den Rx und Tx Verkehr je einen separaten Ausgang zur Verfügung stellen. Diese beiden Datenströme können nun auf einfache Weise mit zwei Ethernet Interfaces in ein Tracefile gespeichert werden.

Das Ganze hat jedoch gewisse Tücken, die durch die Art und Weise bedingt sind, wie die Daten in das Tracefile gespeichert werden. Diese Aufgabe wird nicht von Wireshark erledigt, sondern durch die darunter liegenden Treiber LibPap (bei Unix, Linux) und WinPcap (bei Windows)und DumpCap.

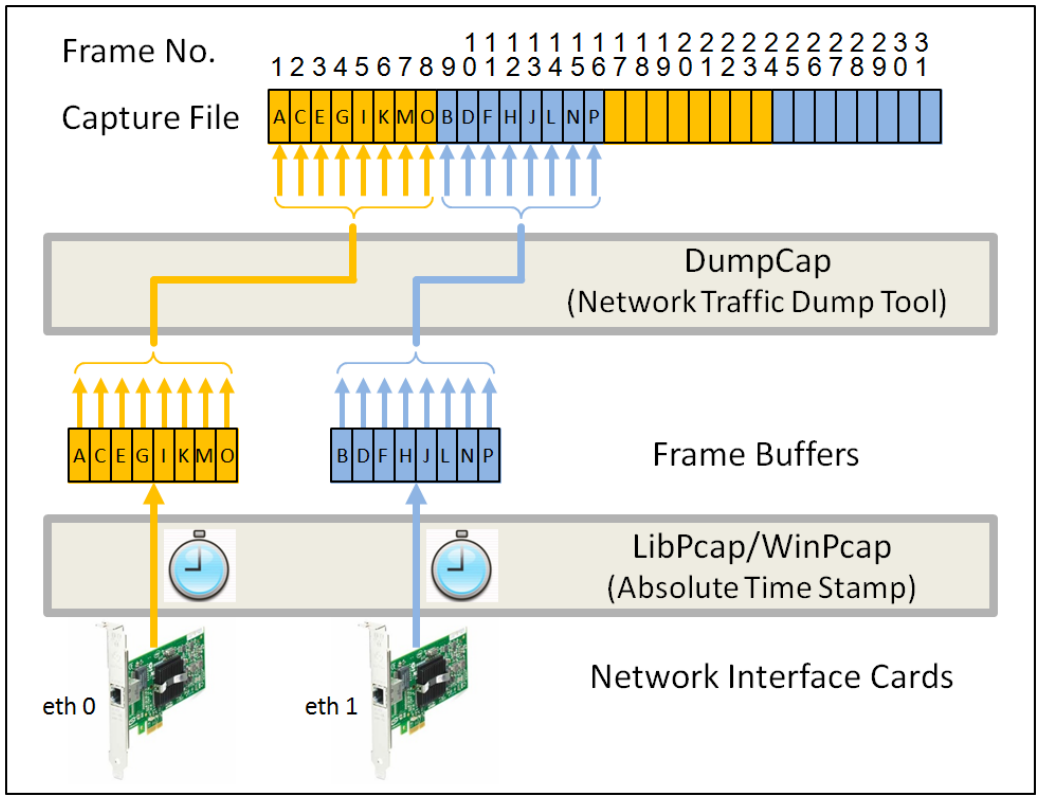
Folgendes Tracefile wurde ab einem Full-Duplex TAP mit zwei Interfaces aufgezeichnet und zeigt den Dialog in beide Richtungen. Beachten sie besonders die negativen Delta Zeiten in der Time Kolonne und die Echo (Ping) Replies vor den Echo (Ping) Requests! Da wurden Frames in ihrer Reihenfolge vertauscht. Was ist die Ursache und wie kann dies korrigiert werden?



Negative Delta Times und Ping Replies vor den Ping Requests

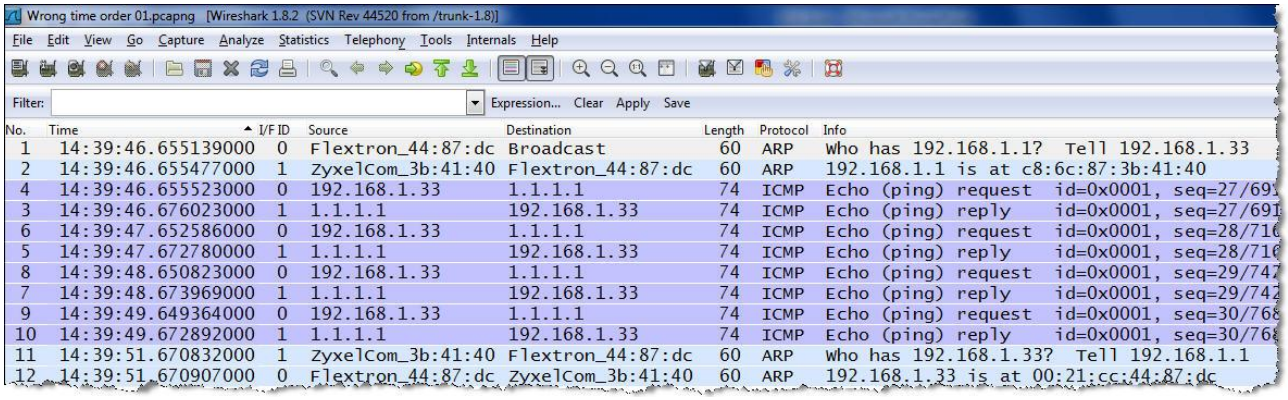
Die Ursache liegt in der Art und Weise wie die Frames im Capture File abgespeichert werden. Dies wird in folgender Darstellung aufgezeigt. Die von der NIC eingelesenen Frames werden von LibPcap/WinPcap mit einem Zeitstempel versehen und im Buffer abgelegt. Der Zeitstempel basiert auf der Absoluten Zeit (Datum und Zeit)des Hostsystems (System Clock).
Die Buffer werden in Intervallen von DumpCap geleert und die Frames im Capture File abgelegt. Angenommen die Frames seinen gemäss ihrer alphabetischen Reihenfolge eingetroffen, also B unmittelbar nach A, D nach C usw. Da die Frames aus dem Buffer nicht nach ihrem Zeitstempel sondern als Block ins File geschrieben werden, kann dies dazu führen, dass zwei Frames, welche zeitmässig nahe beieinander liegen (z.B. A und B), im Capture File relativ weit auseinander abgelegt sind.
Wireshark öffnet das File und nummeriert die Frames in der Reihenfolge wie sie abgelegt wurden, dadurch erhält B die Frame Nummer 9, obwohl er zeitlich zwischen A und C datiert ist. Dies führt zu

den negativen Delta Times, da diese basierend auf dem Zeitstempel der Frames berechnet werden.



Die Ursache von negativen Delta Times

Die Korrekturmassnahme ist einfach (wenn man weiss wie), die Time Kolonne wird auf die Darstellung „Time of Day" umgestellt (unter View -> Time display Format) und die Frames durch Mausklick in das Titelfeld der Time Kolonne nach der absoluten Zeit neu sortiert.



Tracefile sortiert nach der „Time of Day" ordnet Frames in der richtigen Reihenfolge

Abgespeichert werden die Frames jedoch wiederum nach ihrer Nummer, d.h. beim erneuten Öffnen des Tracefiles sind sie wieder nach ihrer Framenummer sortiert.

Hinweise: Die nächsten öffentlichen Präsentationen, Events und Wireshark Kurse

Tun Sie sich und Ihren Mitarbeiter etwas Gutes 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:

Bereits zum dritten Mal lädt Sie Studerus AG zum erfolgreichen "Technology Forum" ein. Die zahlreichen Präsentationen bieten in parallelen Tracks wiederum eine grosse Auswahl an interessanten Themen rund ums Netzwerk mit Fokus auf Security, Wireless-LAN, VoIP, Virtualisierung etc.
Leutert NetServices wird eine praxisorientierte Session zum Thema Wireless-Analyse mit Wireshark präsentieren.

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

Einführungskurse:

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

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

Net Analyse – Protokollanalyse mit Wireshark (wird durchgeführt)

Datum:	17.09.2012 – 18.09.2012 (2 Tage)
Ort:	Studerus, Schwerzenbach
Kurs-Details und Anmeldung bei	Studerus

IPv6 – Einstieg zum IPv6 Protokoll

Datum:	30.11.2012 (1 Tag)
Ort:	Studerus, Schwerzenbach
Kurs-Details und Anmeldung bei	Studerus

Lab basierende Kurse:

TCP/IP Netzwerkanalyse mit Wireshark (wird durchgeführt)

Datum:	03.12.2012 – 05.12.2012 (3 Tage)
Ort:	Hochschule Rapperswil INS, Rapperswil
Kurs-Details und Anmeldung bei	Hochschule Rapperswil

WLAN Netzwerkanalyse mit Wireshark und AirPcap

Datum:	26.11.2012 – 27.11.2012 (2 Tage)
Ort:	Hochschule Rapperswil INS, Rapperswil
Kurs-Details und Anmeldung bei	Hochschule Rapperswil

IPv6 Fundamentals, Workshop mit Wireshark

Datum:	Daten für 2013 in Vorbereitung (2 Tage)
Ort:	Hochschule Rapperswil INS, Rapperswil
Kurs-Details und Anmeldung bei	Hochschule Rapperswil

VoIP Protokollvertiefung mit Wireshark

Datum:	Auf Anfrage (2 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