WIRE**SHARK** Newsletter Januar 2016

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

Schlagzeilen:

- Wireshark Version 2.0
- Hinweise: Wireshark Kurse und Präsentationen
- SharkFest'16 auch in Europa

Markante Verbesserungen in Wireshark Version 2.0

Mit dieser neuen Version wird die grösste Überarbeitung von Wireshark seit dem Namenswechsel von Ethereal im Jahr 2006 eingeführt. Die meisten Anwendungen verwenden zum Darstellen von Grafiken, Menüs, Pop-Up-Fenstern usw. zusätzliche Hilfsprogramme. Ethereal und Wireshark v1.x basieren auf dem Open Source Graphical Tool Kit GTK+ von www.gtk.org.

Die Wireshark Core-Entwickler unter der Leitung von Ethereal Gründer Gerald Combs sahen in dem Toolkit QT ("cute") von www.qt.io bessere Entwicklungsmöglichkeiten für die Zukunft und migrierten Wireshark in hunderten von Arbeitsstunden auf diese neue Plattform. Ein herzliches Dankeschön gebührt den vielen Freiwilligen für ihre enorme Leistung. Die meisten Neuerungen wirken im Hintergrund, aber auch für den Benutzer ergeben sich zahlreiche Verbesserungen.

- Vereinfachtes Graphical User Interface (GUI)
- Unterstützung von verschiedenen Betriebssystemen
- Menüs in verschiedenen Sprachen (auch Deutsch)
- Verbesserte Grafiken mit mehr Funktionen
- Markieren zusammengehörender Pakete
- Intelligenter Scrollbar
- USB Interfaces

Vereinfachtes Graphical User Interface (GUI)

Die offensichtlichste Veränderung ist die neue Welcome Page. Diese wurde stark vereinfacht und ermöglicht einen schnelleren Einstieg zum Aufzeichnungsvorgang oder den Zugriff auf zuvor geöffnete Trace Files.
Alle vom WinPcap Driver detektierten Interfaces werden gelistet und zeigen neu die Aktivität mit sogenannten Spark Lines. Ein Doppelklick auf ein Interface genügt und der Capture-Vorgang wird gestartet.
Weitere wichtige Funktionen wie Capture und Display Filter sind ebenfalls direkt auf der Einstiegs-seite konfigurierbar. (Bild 1).

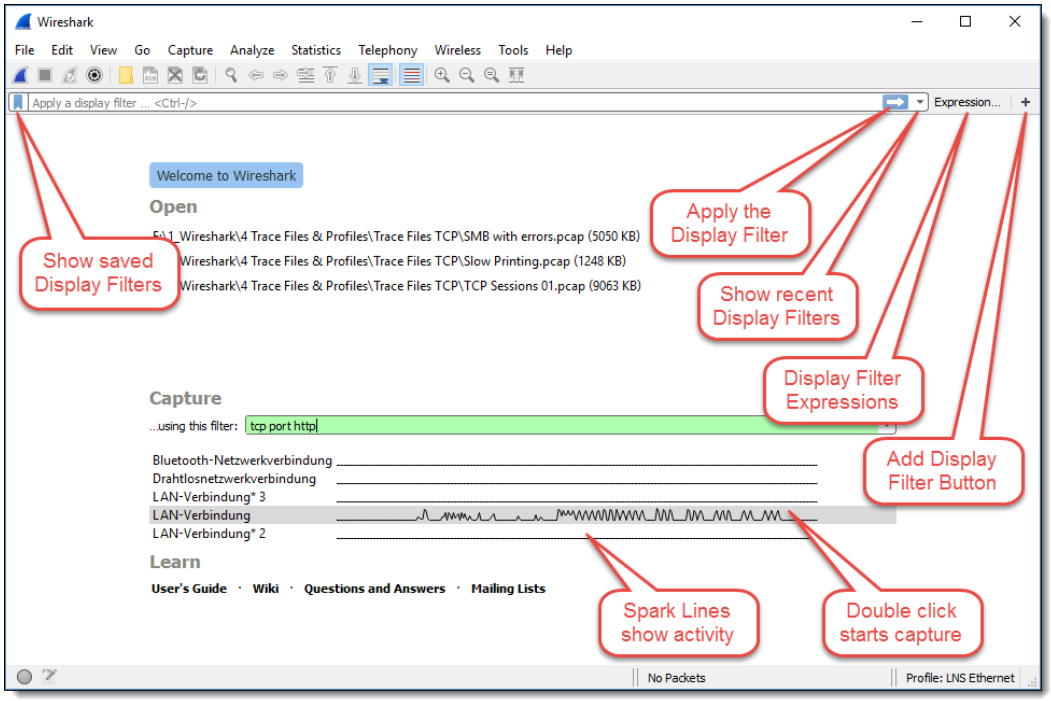


Bild 1: Neue, stark vereinfachte Welcome Page

Die bestehenden Wireshark Profile werden von 2.0 übernommen. Wer den Umstieg noch hinauszögern will: Das alte GTK+ GUI wird als Wireshark Legacy noch bis Version 2.2 unterstützt werden. Beide Versionen können auch gleichzeitig installiert werden, dies erleichtert den Umstieg.

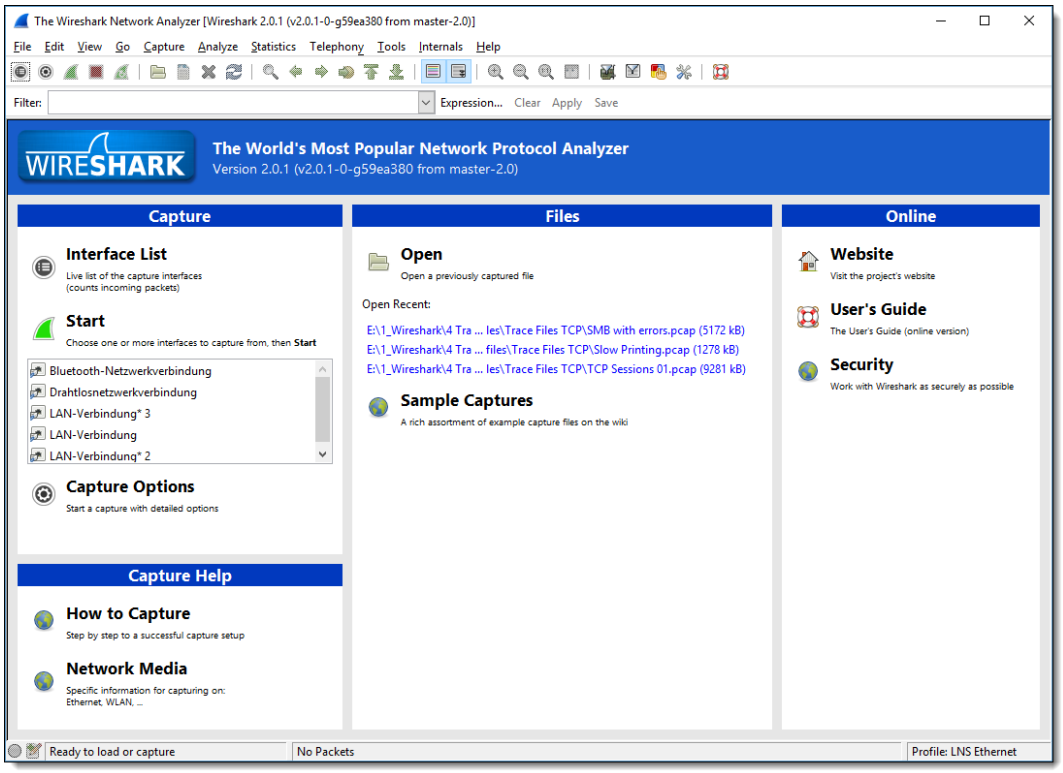


Bild 2: Wireshark Legacy 2.0 mit herkömmlichem GUI

Unterstützung von verschiedenen Betriebssystemen

Wireshark hat seit langem schon verschiedene Betriebssysteme unterstützt, auf einigen jedoch nur unter Verwendung einer zusätzlichen Grafiksoftware wie z.B. X11 x.org/wiki.
Mit der Verwendung von QT kann Wireshark nun auch auf dem MAC OS native (ohne X11) installiert werden; dies zur grossen persönlichen Freude von Gerald Combs als erklärter MAC Fan.

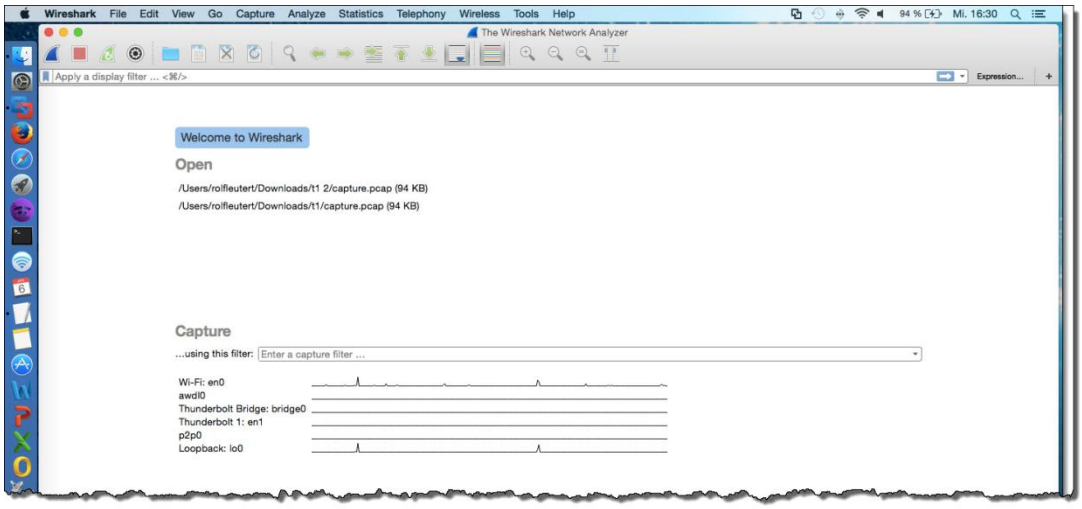


Bild 3: Wireshark 2.0 läuft nun ohne X11 auch auf MAC OS X

Nein! Vorläufig noch keine Unterstützung von Android und Apple IOS. Eine detaillierte Liste von mehr als 20 unterstützen Betriebssystemen ist unter folgendem Link zu finden:
https://www.wireshark.org/docs/wsdg_html_chunked/ChIntroPlatforms.html

Menüs in verschiedenen Sprachen (auch Deutsch)

Schon lange auf der Wunschliste von den weltweiten Wireshark Benutzern stand die Unterstützung von verschiedenen Sprachen. Die Auswahl soll noch erweitert werden, aktuell angeboten werden neben Englisch nun auch: Chinesisch, Französisch, Deutsch, Italienisch, Japanisch und Polnisch.

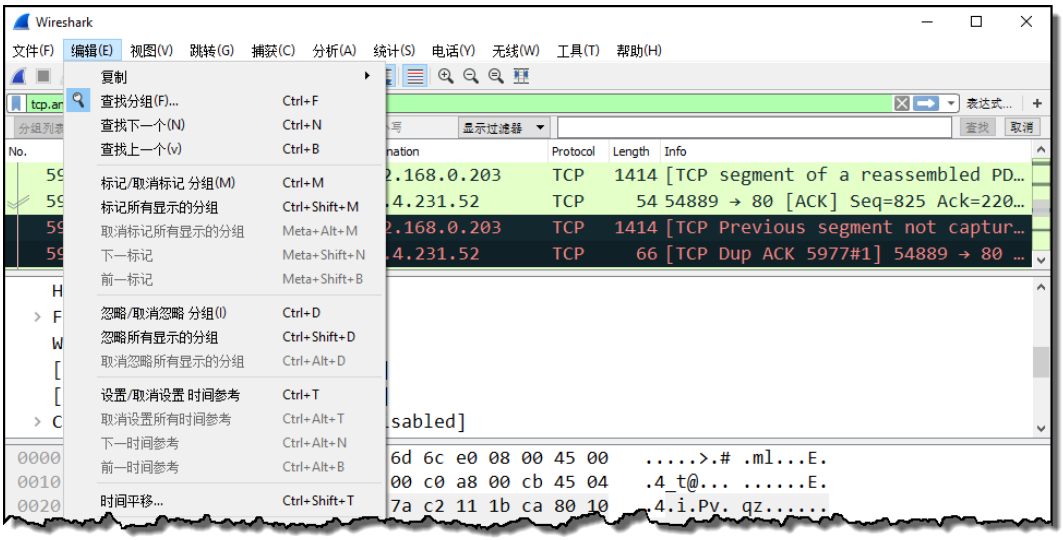


Bild 4: Wireshark 2.0 auf Chinesisch

Die Spracheinstellung findet man unter → Bearbeiten → Einstellungen → Darstellung → Sprache
oder in der englischen Version unter → Edit → Preferences → Appearance → Language
Die Grundeinstellung der Sprache übernimmt Wireshark beim Installieren von der Systemeinstellung.
Falls Sie aus der chinesischen Darstellung nicht mehr zurückfinden 😊 → Ctrl+Shift+P

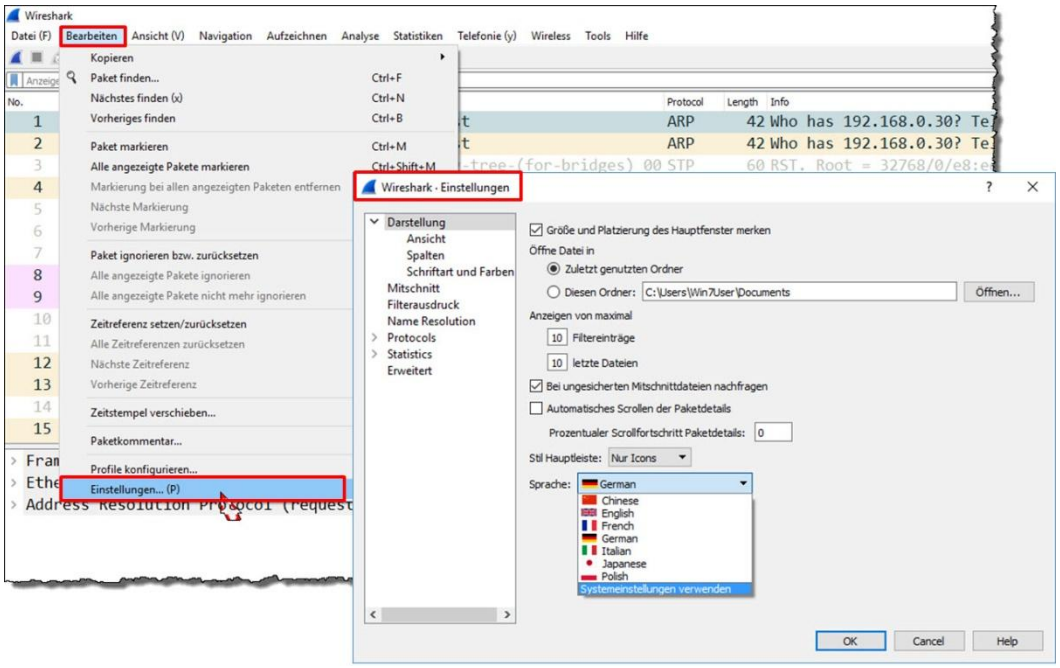


Bild 5: Sprachauswahl

Verbesserte Grafiken mit mehr Funktionen

Die beliebte Darstellung → Statistics → I/O Graph wurde markant verbessert, viele Funktionen hinzugefügt, und die Anzahl der Grafikkurven ist praktisch nicht mehr limitiert. Zudem kann die Grafik mehrmals gleichzeitig geöffnet und als PDF, PNG, JPEG, BMP oder CVS gespeichert werden.

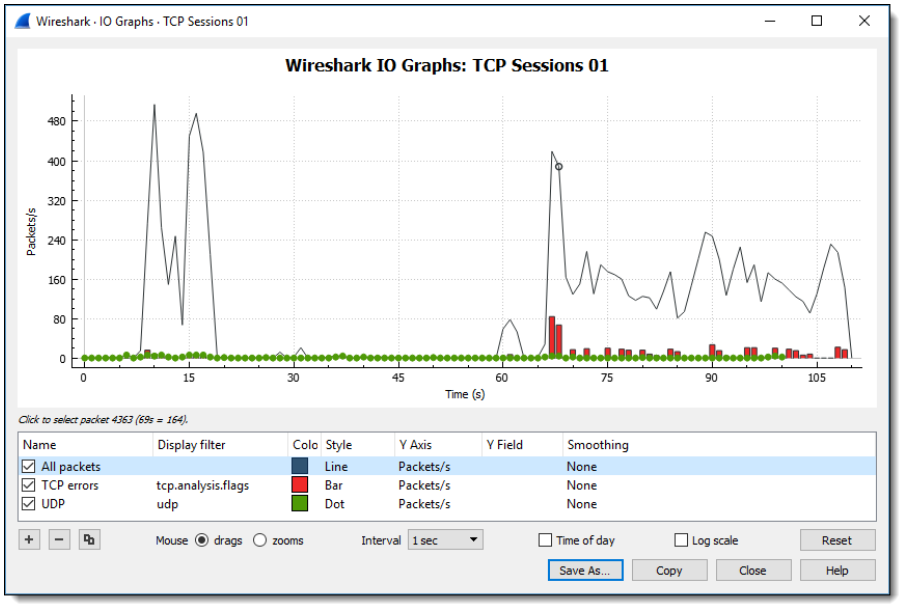


Bild 6: I/O Graph mit vielen neuen Funktionen

Wesentliche Verbesserungen erfuhr auch die für die TCP Analyse unverzichtbare Grafik TCPtrace, (welche natürlich auch in unseren Kursen detailliert behandelt wird 😉). Der Vergleich zeigt neben der besseren Darstellung auch die neuen, zusätzlich in die Grafik direkt eingebunden Funktionen.

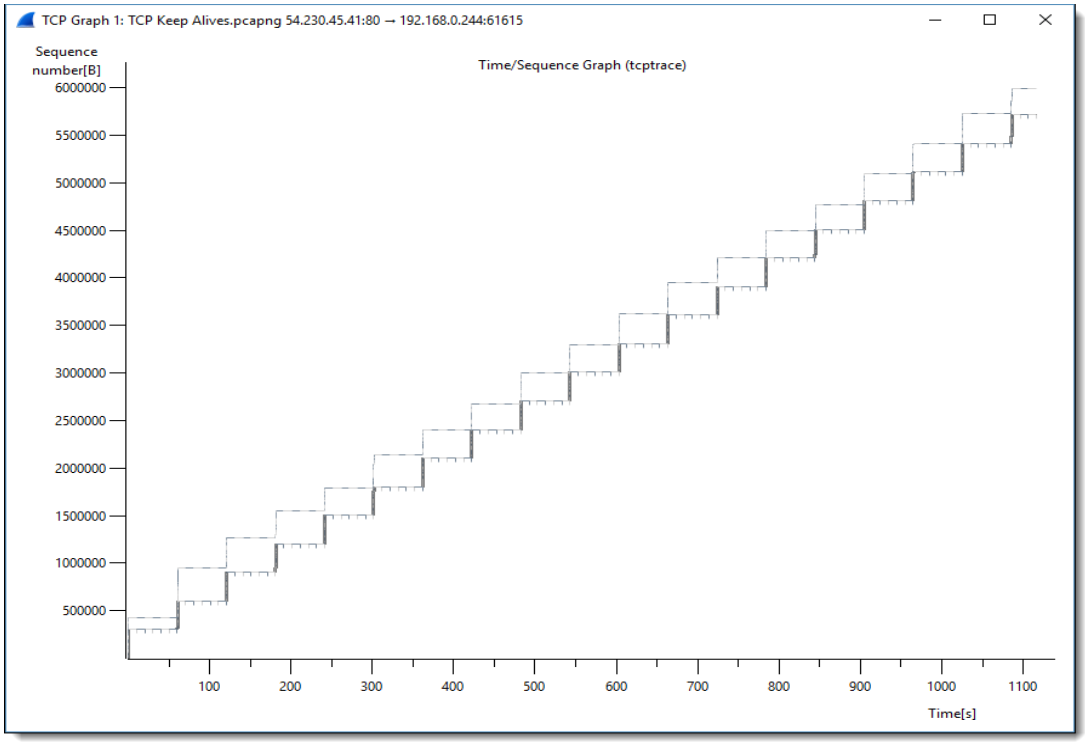


Bild 7: TCPtrace, alte Darstellung

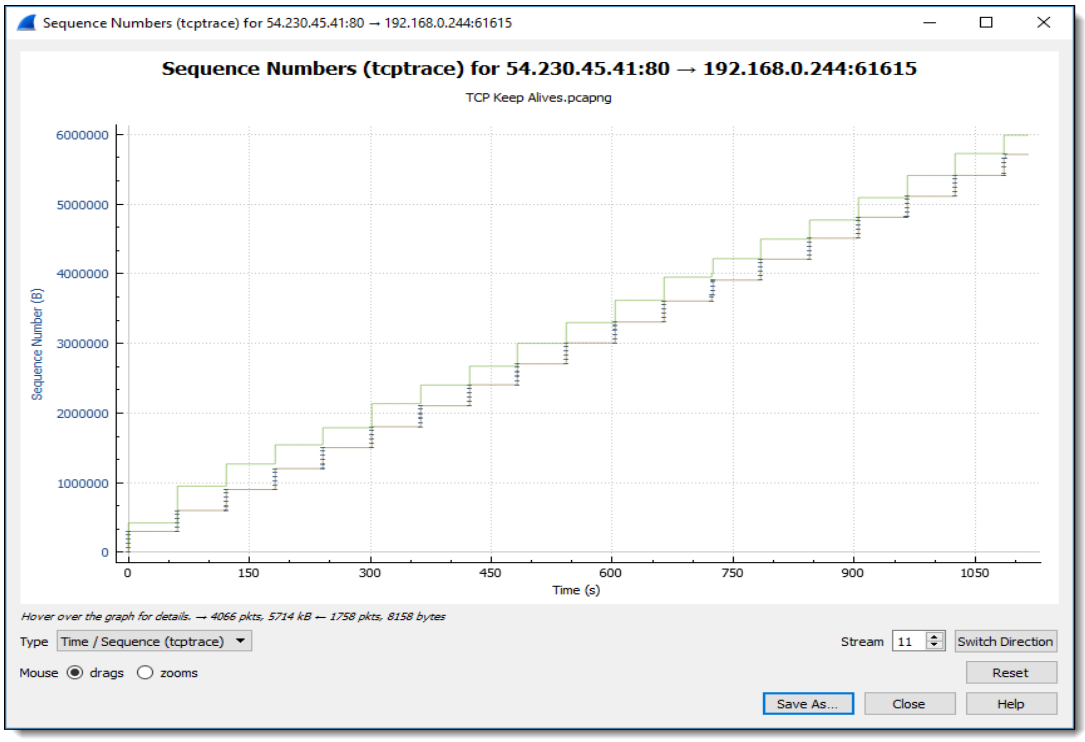


Bild 8: TCPtrace, neue Darstellung

Markieren zusammengehörender Pakete

Viele Protokolle wie DHCP, DNS usw. basieren auf einem Anfrage - Antwort Dialog, andere wie HTTP oder SMB verwenden eine TCP Session für die zuverlässige Übertragung grosser Datenmengen. Die Pakete folgen jedoch meistens nicht unmittelbar hintereinander, da auf dem Netz in der Regel mehrere Kommunikationen gleichzeitig aktiv sind.
Wireshark 2.0 markiert zusammengehörende Pakete (related Packets) eines Dialogs oder einer TCP Session und erleichtert dadurch die Analyse bei grossen Datenmengen.

Bild 9 zeigt in Frame 81 eine DNS Anfrage, in der Spalte ganz links markiert mit einem Pfeil nach rechts. Die zugehörende Antwort findet sich im Frame 85 und ist mit einem Pfeil nach links markiert.

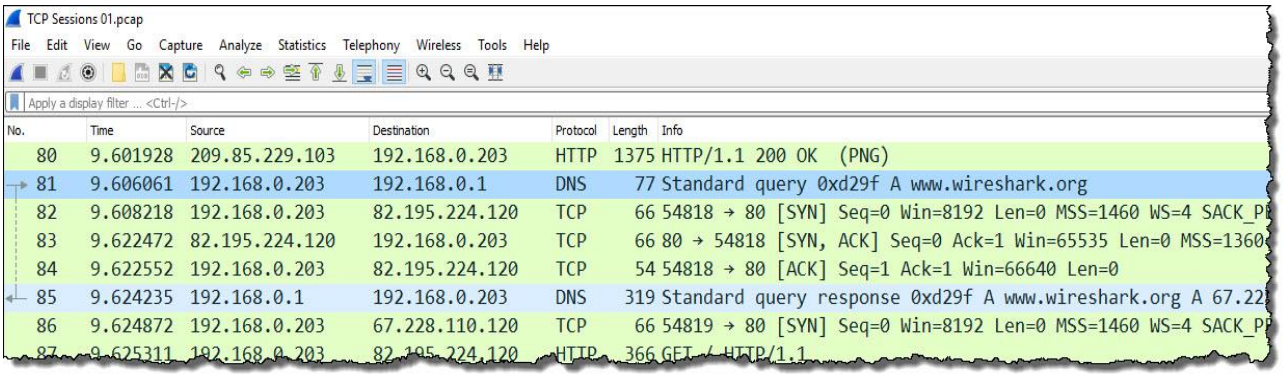


Bild 9: Markierte DSN Anfrage und Antwort

Wird mit dem Cursor ein Paket angewählt, welches Teil einer TCP Session darstellt, werden alle zu dieser Session gehörende Pakete links mit einer durchgehenden, vertikalen Linie markiert. Pakete, welche nicht zu dieser Session gehören, werden mit einer gestrichelten Linie markiert.

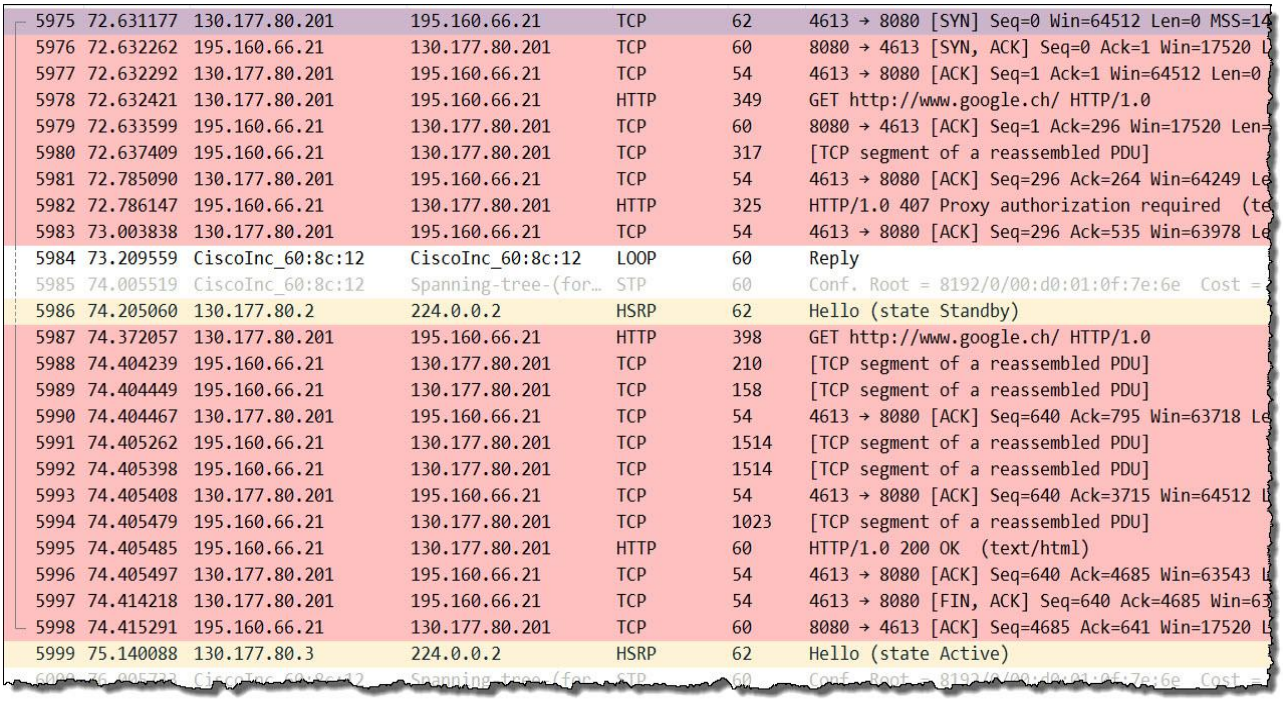
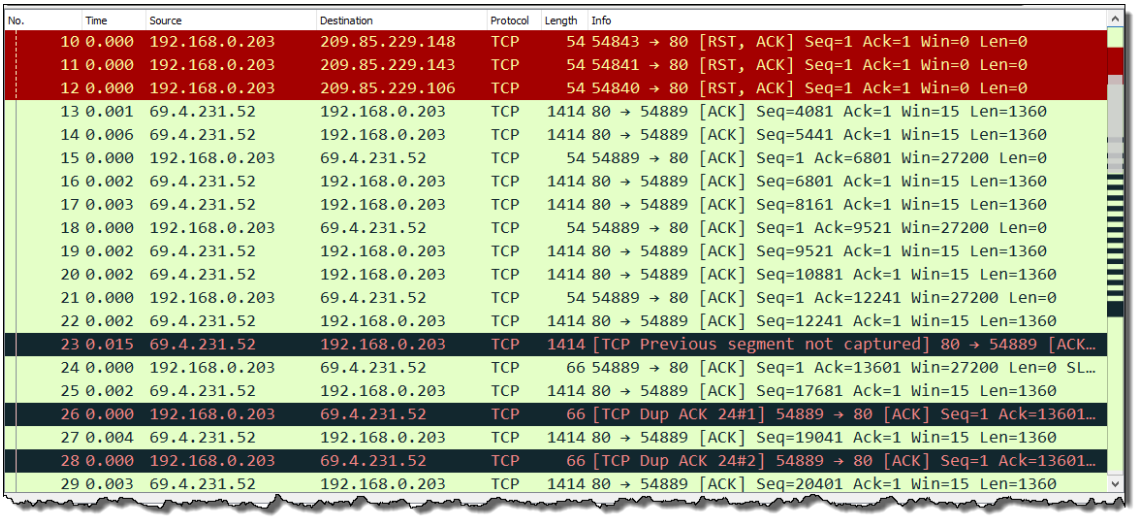


Bild 10: Mit einer durchgehenden Linie markierte Pakete einer TCP Session

Intelligenter Scrollbar

Die herkömmliche Funktion des Scrollbars am rechten Rand von Wireshark ist selbst erklärend, neu wurde dieser jedoch mit „Intelligenz“ versehen. Die Farbcodierung ist nun dieselbe, wie sie zum Einfärben der verschiedenen Frames verwendet wird → View → Coloring Rules.
D.h. jeder Frame entspricht neu im Scrollbar einer horizontalen Linie mit derselben Farbe.
Z.B. schwarz eingefärbte Frames stellen beim Wireshark Pakete mit Fehlern dar, diese werden im Scrollbar ebenfalls als schwarze horizontale Linie angezeigt und lassen sich dadurch schneller auffinden.

Bild 11: Scrollbar



No.	Time	Source	Destination	Protocol	Length	Info
10	0.000	192.168.0.203	209.85.229.148	TCP	54	54843 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	0.000	192.168.0.203	209.85.229.143	TCP	54	54841 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	0.000	192.168.0.203	209.85.229.106	TCP	54	54840 → 80 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	0.001	69.4.231.52	192.168.0.203	TCP	1414	80 → 54889 [ACK] Seq=4081 Ack=1 Win=15 Len=1360
14	0.006	69.4.231.52	192.168.0.203	TCP	1414	80 → 54889 [ACK] Seq=5441 Ack=1 Win=15 Len=1360
15	0.000	192.168.0.203	69.4.231.52	TCP	54	54889 → 80 [ACK] Seq=1 Ack=6801 Win=27200 Len=0
16	0.002	69.4.231.52	192.168.0.203	TCP	1414	80 → 54889 [ACK] Seq=6801 Ack=1 Win=15 Len=1360
17	0.003	69.4.231.52	192.168.0.203	TCP	1414	80 → 54889 [ACK] Seq=8161 Ack=1 Win=15 Len=1360
18	0.000	192.168.0.203	69.4.231.52	TCP	54	54889 → 80 [ACK] Seq=1 Ack=9521 Win=27200 Len=0
19	0.002	69.4.231.52	192.168.0.203	TCP	1414	80 → 54889 [ACK] Seq=9521 Ack=1 Win=15 Len=1360
20	0.002	69.4.231.52	192.168.0.203	TCP	1414	80 → 54889 [ACK] Seq=10881 Ack=1 Win=15 Len=1360
21	0.000	192.168.0.203	69.4.231.52	TCP	54	54889 → 80 [ACK] Seq=1 Ack=12241 Win=27200 Len=0
22	0.002	69.4.231.52	192.168.0.203	TCP	1414	80 → 54889 [ACK] Seq=12241 Ack=1 Win=15 Len=1360
23	0.015	69.4.231.52	192.168.0.203	TCP	1414	[TCP Previous segment not captured] 80 → 54889 [ACK…
24	0.000	192.168.0.203	69.4.231.52	TCP	66	54889 → 80 [ACK] Seq=1 Ack=13601 Win=27200 Len=0 SL…
25	0.002	69.4.231.52	192.168.0.203	TCP	1414	80 → 54889 [ACK] Seq=17681 Ack=1 Win=15 Len=1360
26	0.000	192.168.0.203	69.4.231.52	TCP	66	[TCP Dup ACK 24#1] 54889 → 80 [ACK] Seq=1 Ack=13601…
27	0.004	69.4.231.52	192.168.0.203	TCP	1414	80 → 54889 [ACK] Seq=19041 Ack=1 Win=15 Len=1360
28	0.000	192.168.0.203	69.4.231.52	TCP	66	[TCP Dup ACK 24#2] 54889 → 80 [ACK] Seq=1 Ack=13601…
29	0.003	69.4.231.52	192.168.0.203	TCP	1414	80 → 54889 [ACK] Seq=20401 Ack=1 Win=15 Len=1360

Bild 12: Der neue Scrollbar ermöglicht schnelles Auffinden nach Farbcodes

USB Interfaces

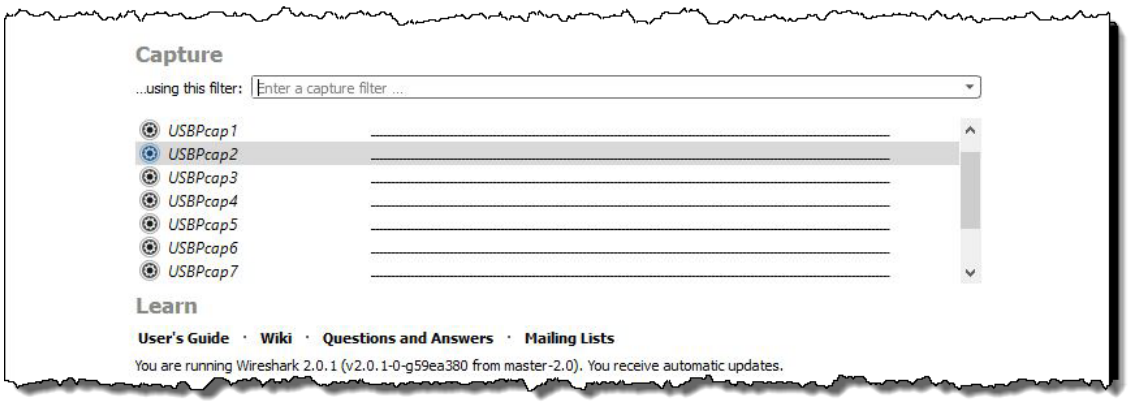


Bild 13: Die USB Interfaces mit Spark Lines (siehe auch Bild 1 auf Seite 2)

Bei der Installation von Wireshark 2.0 wird die Möglichkeit angeboten, den USBPcap Driver zu installieren. Die detektierten USB Schnittstellen werden dann auf der Welcome Page aufgelistet, und mit Doppelklick auf ein bestimmtes Interface wird die Aufzeichnung gestartet.

Im Bild 14 ist der Verbindungsaufbau mit einem USB Harddrive vom Hersteller Brinell dargestellt.

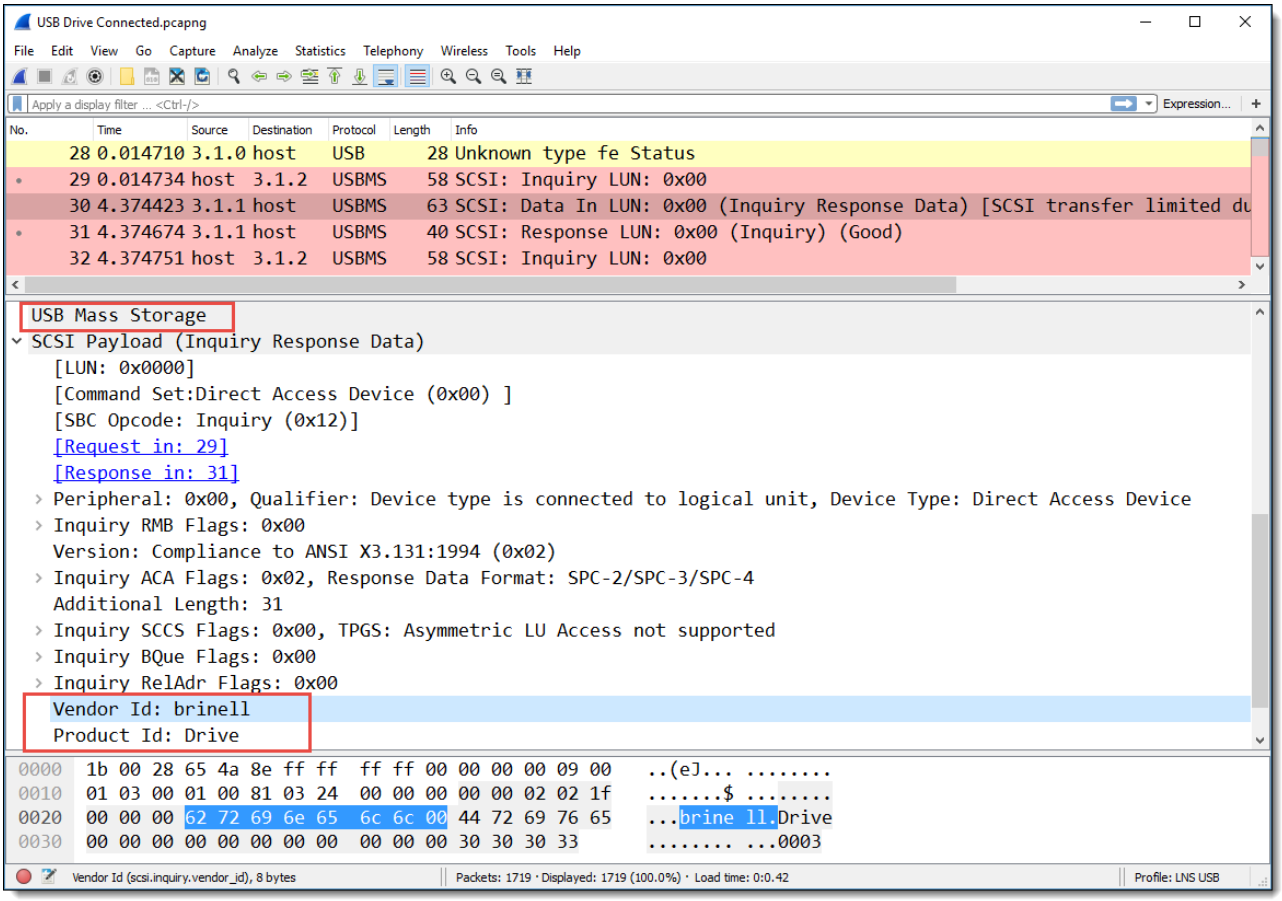


Bild 14: Aufzeichnung des Verbindungsaufbaus zu einem USB Harddrive

Zusammenfassung

Jede Umstellung ist auch mit Umgewöhnung, d.h. Aufwand verbunden und deshalb bleibt man gerne mit Werkzeugen, die man kennt (ich z.B. arbeite noch mit Office 2007). Die Umstellung auf Wireshark 2.0 bedeutet auch, dass gewisse Funktionen nicht mehr am gewohnten Ort zu finden sind; ausser der umgestalteten Welcome Page ist dies jedoch nur für wenige Funktionen der Fall.
Ich arbeite seit kurzer Zeit nur noch mit Version 2.0 und habe mich bereits umgewöhnt; die neuen Funktionen, die bereinigten Menüs und die besseren Grafiken sind den Aufwand in jedem Fall wert.

In diesem Newsletter wurden nur die wichtigsten Neuerungen vorgestellt, zahlreiche weitere Details wurden nicht behandelt – sie gilt es selbst zu entdecken. Viele weitere Informationen finden Sie auf dem Web, z.B. im Blog von Gerald Combs:
https://blog.wireshark.org/2015/11/let-me-tell-you-about-wireshark-2-0/

Hinweise:

Öffentliche Präsentationen und Wireshark Kurse

SharkFest'16 auch in Europa

Bereits seit dem Jahr 2008 findet in Kalifornien, USA, einmal pro Jahr die Wireshark User & Developer Conference, genannt SharkFest, statt. Leutert NetServices war von Anfang an vertreten und präsentiert regelmässig Sessions zu verschiedenen Themen wie Protokollanalyse und Troubleshooting.
Immer wieder wurden die Organisatoren angefragt, ob dieser Event nicht auch mal in Europa durchgeführt werden könnte. Nun scheint es so weit zu sein: noch nicht offiziell bestätigt, jedoch bereits in der groben Planung, soll dieses Jahr, vermutlich im Oktober in Holland, ein SharkFest Europe stattfinden. Sobald mehr Details bekannt sind, werden wir Sie auf unserer Webseite unter www.wireshark.ch/de/news und im nächsten Newsletter informieren. Auf einen persönlichen Kontakt an diesem Event würden wir uns sehr freuen.

Sämtliche Präsentationen von früheren SharkFest Events finden sie unter:
https://sharkfest.wireshark.org/retrospective.html

Wireshark Einführungen und Kurse

Alle unsere Kurse werden bereits mit Wireshark 2.0 durchgeführt. Gönnen Sie sich und Ihren Mitarbeiter etwas Sinnvolles und buchen Sie uns z.B. für eine eintägige Einführung zu IPv6, einem Update zu Wireshark 2.0 oder dem Thema Ihrer Wahl aus den aufgeführten Kursen. Wir garantieren Ihnen einen lehrreichen Anlass.

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

- Netzwerkanalyse allgemein
- TCP/IP Netzwerkanalyse mit Wireshark
- WLAN Netzwerkanalyse mit Wireshark, AirPcap und WiSpy
- 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

Unser Newsletter Archiv finden sie unter: http://www.wireshark.ch/de/wireshark-infos/newsletter

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

Besten Dank für Ihr Interesse
Mit freundlichen Grüssen Rolf Leutert