# WIRE**SHARK Newsletter Januar 2023**

Liebe Kunden und Wireshark Freunde

Dieser Wireshark Newsletter von Leutert NetServices informiert Sie unregelmässig über Neuerungen im Zusammenhang mit dem Open Source Analyzer Wireshark und weiteren Netzwerkanalyse-Produkten.


## Schlagzeilen

News:

- Neue Funktionen ab **Wireshark Version 4**
- **Sysdig** ist neuer Sponsor von Wireshark
- Update zum **QUIC-Protokoll**
- Webinar: **Wird QUIC der Nachfolger von TCP?**

Tipps, Tricks & Traces:

- Installieren eines **LUA-Plugins** für **HFA-Protokoll**
- Verschiedene Wireshark Versionen nutzen

Kurse & Events:

- **AnyWeb Training** ist neuer Wireshark-Kursanbieter für die Schweiz
- Neuer Trainer bei **Arrow ECS GmbH**, unserem Kursanbieter in Wien
- Webinar: **Troubleshooting WLANs mit Wireshark**
- Aktuelle **Kursdaten**

# Neue Funktionen ab Wireshark Version 4

Die meisten Veränderungen bei der Wireshark Version 4 geschahen im Hintergrund:

- Die markanteste Neuerung ist der Upgrade der Grafikbibliothek von Qt 5 auf Qt 6.
- Qt (auch Qiute genannt) ermöglicht die Unterstützung verschiedener Betriebssysteme.

- Wireshark unterstützt ab Version 4.0 nur noch 64-Bit Prozessoren, die letzte Version die noch 32-Bit unterstützt, ist 3.6.10. Diese wird noch einige Jahre unterstützt werden.

- Obige Änderungen sind vor allem eine Vereinfachung für die Entwickler, da Wireshark doch schon aus mehr als 3 Millionen Code-Zeilen besteht und mehr als 2'000 Protokolle decodiert.

- Zu viele Erweiterungen wurden beim Upgrade auf Version 4.0 eingeführt, um diese alle hier aufzuführen. Alle Details sind unter https://www.wireshark.org/docs/relnotes/ abrufbar.

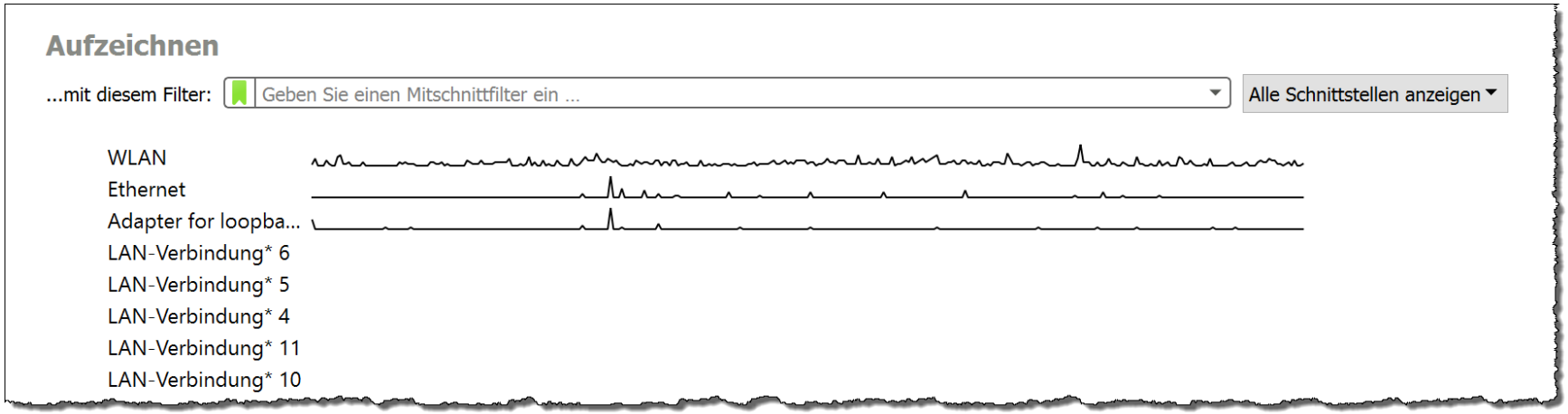
- Ein 18 Min. langes Video mit dem Wireshark Gründer Gerald Combs und einem der Core Entwickler Roland Knall ist abrufbar unter https://www.youtube.com/watch?v=3HdKhen0Gqw

- So markante Änderungen bedeuten auch immer, dass neue Bugs auftauchen.
- Die Versionen 4.0.1 und 4.0.2 enthalten deshalb bereits erste Bug Fixes.

# Neue Funktionen ab Wireshark Version 4

## Änderungen auf dem Start-Bildschirm

- Die Anordnung der vom Npcap Driver entdeckten Capture Interfaces wurde geändert.
- Neu werden die aktiven Interfaces immer zuoberst angezeigt.
- Dies vereinfacht die Übersicht, auf welchen Interfaces aktuell Datenverkehr aktiv ist.

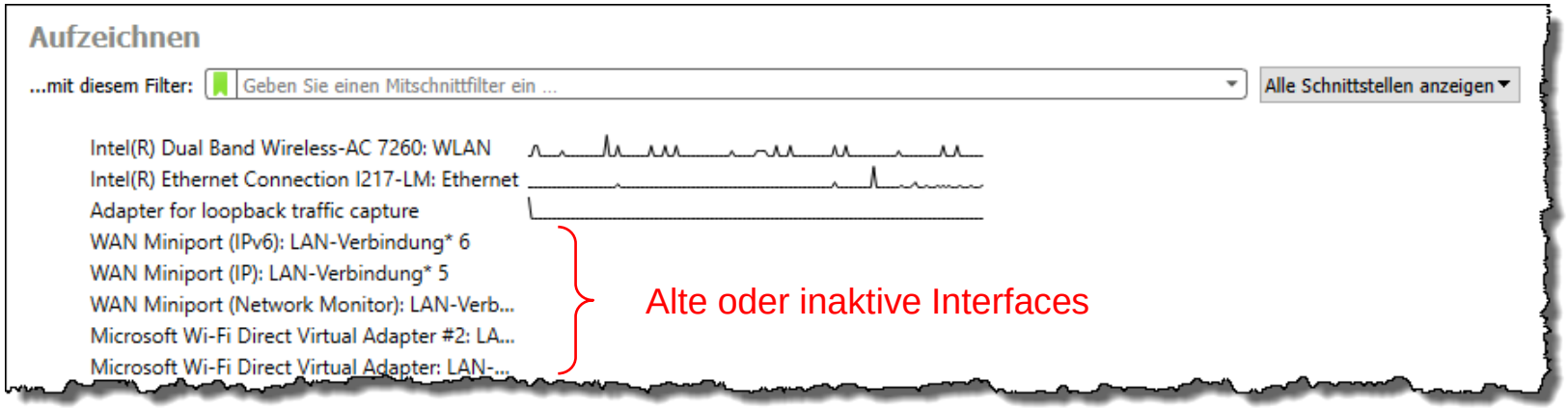



- Inaktive Interfaces können auch ausgeblendet werden (siehe nächste Seite).

# Neue Funktionen ab Wireshark Version 4

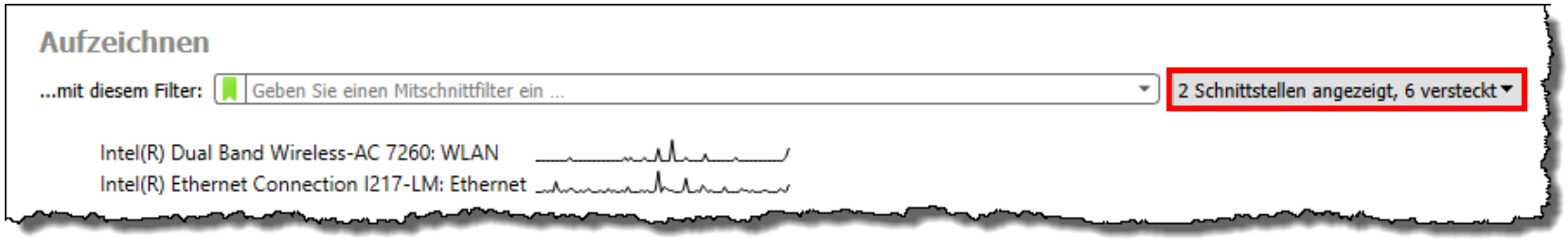
## Ausblenden inaktiver Interfaces

- Beim Aufstarten von Wireshark sucht der Windows Driver Npcap nach NDIS 6 Interfaces.
- Dabei werden oft auch alte und nicht aktive Interface Drivers entdeckt und gelistet.
- Um diese zu entfernen wäre ein Eingriff ins entsprechende Betriebssystem notwendig.




- Wireshark kann diese Interfaces nicht entfernen, jedoch deren Anzeige unterdrücken:

**→ Aufzeichnen → Optionen → Schnittstellen verwalten** → Inaktive Interfaces ausblenden



# Neue Funktionen ab Wireshark Version 4

## Paketanzeige-Bereich

- Sniffer-Oldies (like myself ☺) erinnern sich noch an den ersten Sniffer™ von Network General
- Auch Gerald Combs, der Gründer von Ethereal (heute Wireshark), hatte während seinem Studium mit dem original Sniffer gearbeitet, dieser inspirierte ihn zur Entwicklung von Ethereal.

*Token-Ring Sniffer 1986*

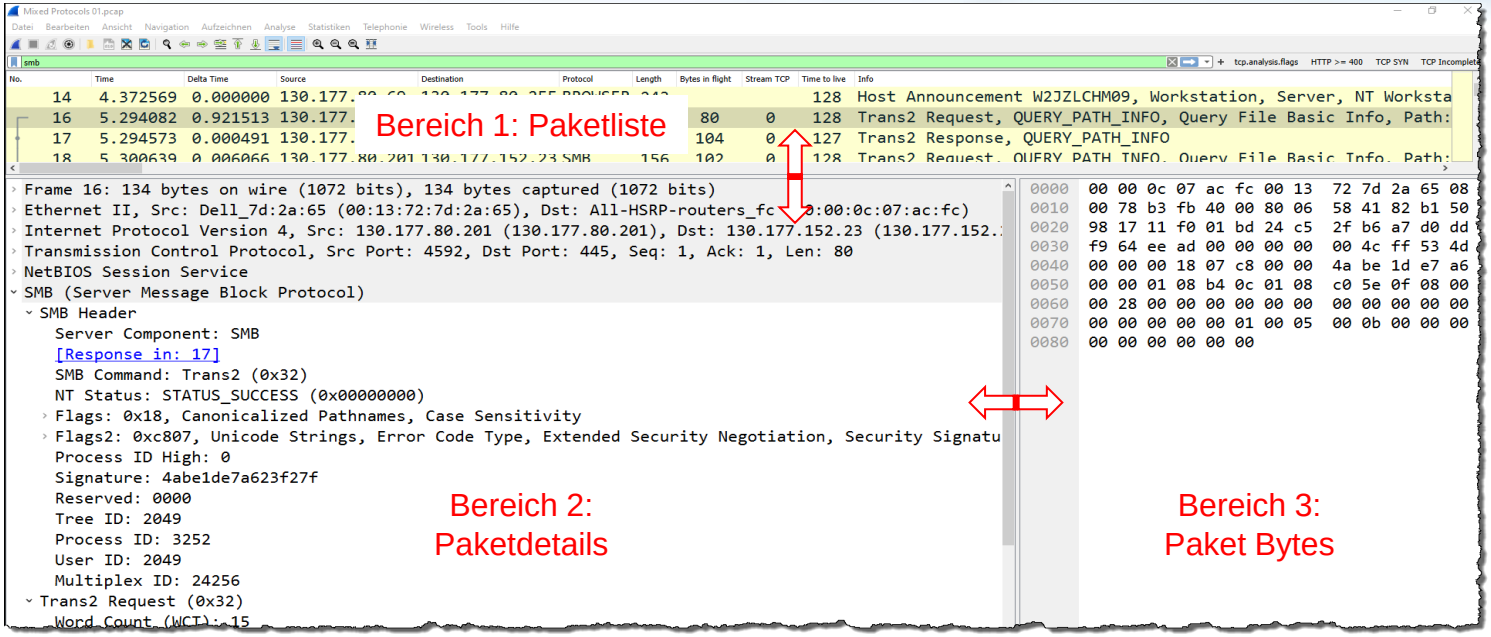
```
SUMMARY   Rel time     From Mary                    From Tom
   59        7.582  NETBIOS      +Mary             NET Find name TOMPC<03>
   60        7.593                                 NET Name TOMPC<03> recognized
   61        7.603  NET D=02 S=04 Session initialize
   63        7.613                                 NET D=04 S=02 Session confirm
   65        7.629  NET D=02 S=04 Data

DETAIL
 SMB:  Return code = 0,0 (OK)
 SMB:  Originator = "MARYXTSV"
 SMB:  Destination = "TOMPC"
 SMB:  [Message text]
 SMB:
                              Frame 65 of 84
HEX                                                                    ASCII
 0020  FF 53 4D 42 D0 00 00 00  00 00 00 00 00 00 00 00  .SMB............
 0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
 0040  00 23 00 04 4D 41 52 59  58 54 53 56 00 04 54 4F  .#..MARYXTSV  TO
 0050  4D 50 43 00 01 0F 00 48  65 6C 6C 6F 20 74 68 65  MPC....Hello the
 0060  72 65 20 54 6F 6D                                re Tom
                              Frame 65 of 84

                    Use TAB to select windows
1       2 Set      4 Zoom  5        6Disply 7 Prev  8 Next          10 New
  Help    mark       in     Menus   options  frame   frame          capture
```

*Sniffer-Paketanzeige (Quelle Wikipedia)*

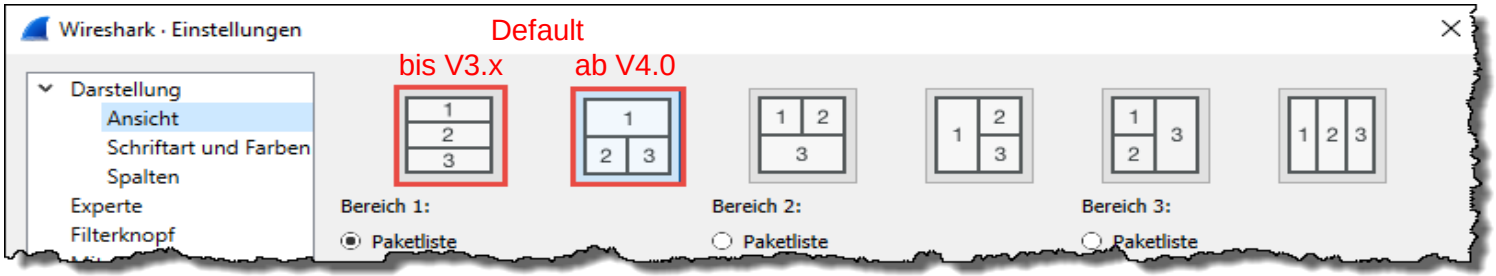
- Vom Sniffer hat Gerald Combs die Paketdarstellung mit den drei Bereichen übernommen.
- Diese Darstellung wurde bis und mit Wireshark Version 3 als Default beibehalten, natürlich erweitert mit den graphischen Möglichkeiten eines modernen GUIs.

# Neue Funktionen ab Wireshark Version 4

- Die neue Grundeinstellung zeigt die drei Bereiche neu angeordnet.
- Dies entspricht offenbar der von den meisten Wireshark-Benutzern bevorzugten Anordnung.



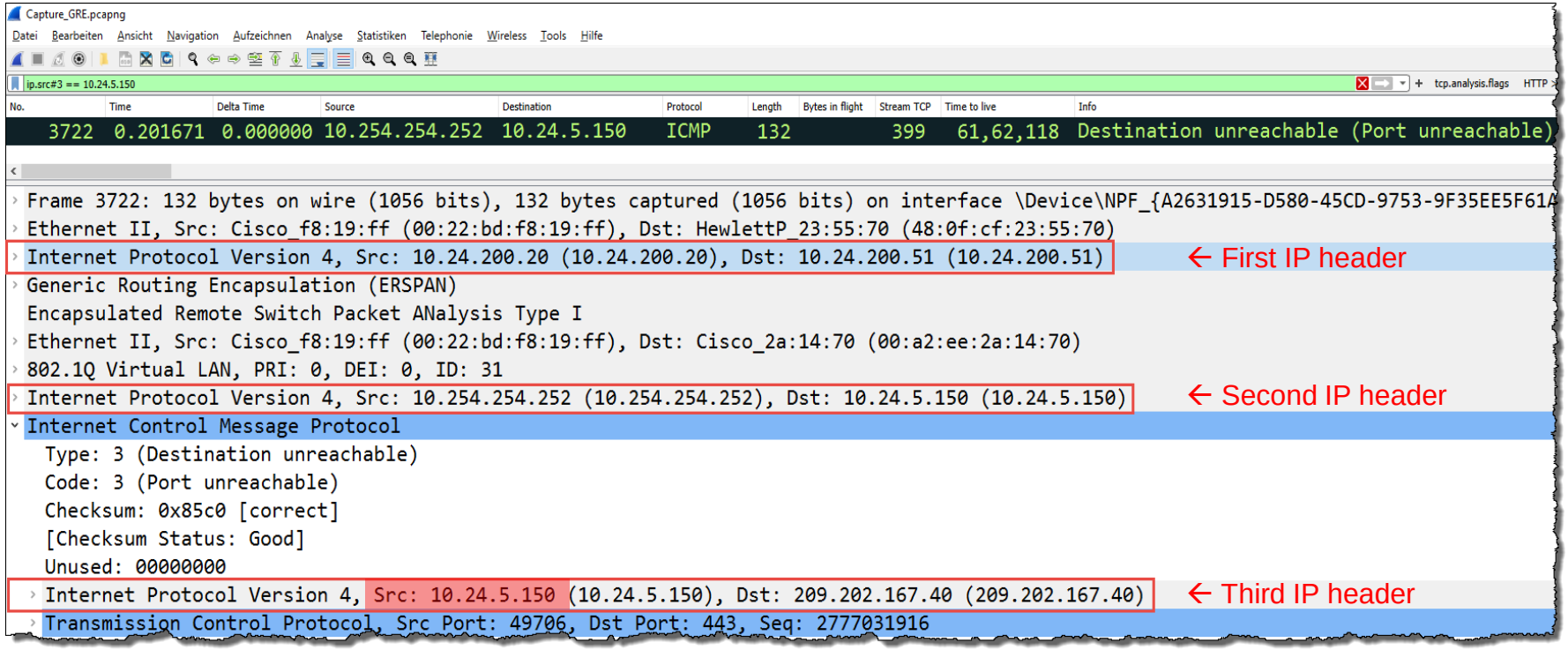

- Unter → Bearbeiten → Einstellungen → Ansicht kann die Bereichs-Anordnung gewählt werden.



# Neue Funktionen ab Wireshark Version 4

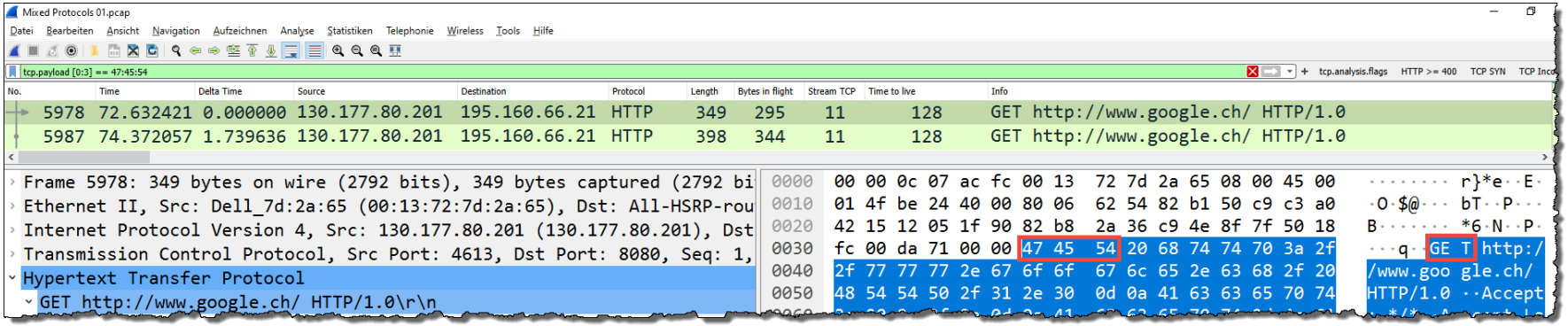
## Display Filter Erweiterungen (hier nur die Wichtigsten)

- Zahlreiche Tunnel Protokolle enthalten dieselben Felder mehrmals, z.B. MAC- oder IP-Adressen.
- GRE, VXLAN usw. enthalten ein äusseres und ein inneres MAC- oder IP-Adressen-Paar.
- Neu kann spezifiziert werden, auf welches Adress-Paar gefiltert werden soll (Layer operator #).
- Z.B. enthalten ICMP Destination unreachable Pakete über GRE sogar drei IP-Adressen-Paare.
- Der Filter `ip.src#3 == 10.24.5.150` filtert im dritten IP-Header auf die gesuchte IP-Adresse.

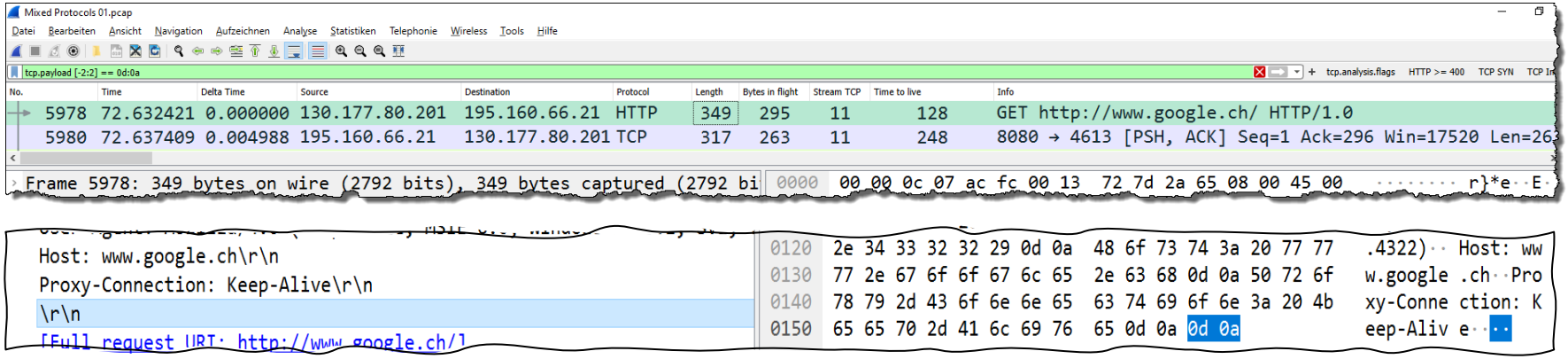


# Neue Funktionen ab Wireshark Version 4

- Neu ist es möglich, auf Bytes im TCP-Payload zu filtern
- Dazu muss auch die Position der Bytes (Offset) spezifiziert werden.
- Der Filter `tcp.payload [0:3] == 47:45:54` filtert auf die ersten drei Bytes im TCP-Payload




- Der Filter `tcp.payload [-2:2] == 0d:0a` filtert auf die letzten zwei Bytes im TCP-Payload



# Neue Funktionen ab Wireshark Version 4

**Mit dem sogenannten Membership Operator können Mehrfach-Filter vereinfacht werden.**

- Die Werte innerhalb { } bilden die Members, auf welche ein bestimmtes Feld geprüft wird.
- Die aufgelisteten Member-Werte müssen mit einem Komma separiert werden.
- Der Filter `tcp.port in {80, 443, 8080}` zeigt alle Pakete mit den spezifizierten TCP-Ports.
- Gleiches Resultat wie der Filter `tcp.port == 80 || tcp.port == 443 || tcp.port == 8080`
- Der Filter `tcp.port in {1 .. 1023}` zeigt alle Pakete mit TCP-Ports im Well known Bereich.

Weitere praktische Beispiele:

- Der Filter `ip.addr in {10.0.0.5 .. 10.0.0.9, 192.168.1.1..192.168.1.9}` zeigt IP-Ranges
- Der Filter `http.request.method in {"HEAD", "GET"}` zeigt alle HTTP HEAD und GET Meldungen
- Der Filter `dns and frame.time_delta in {1 .. 10.5}` zeigt DNS Antworten im Delta-Bereich

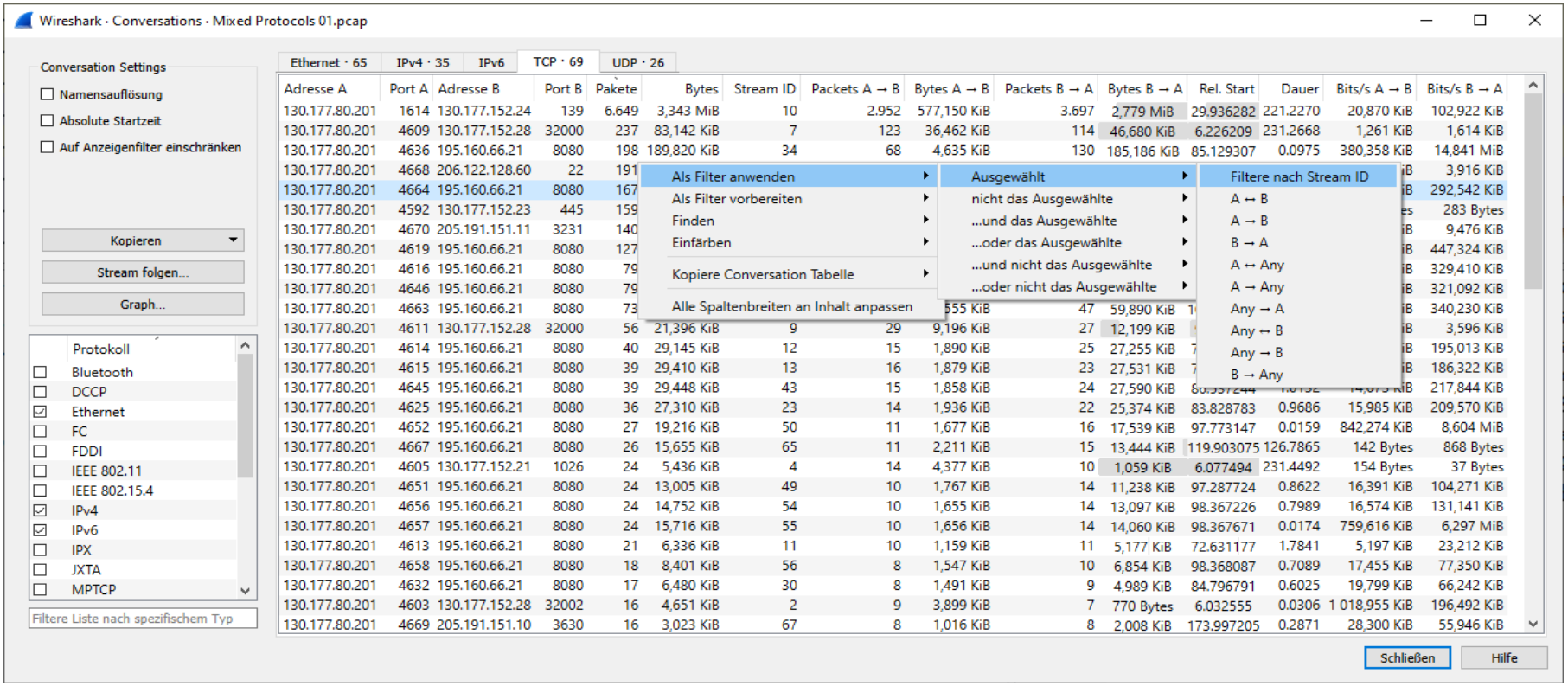
**Mit dem Slice Operator kann auf HEX-Werte an einer definierten Position gefiltert werden:**

- Der Filter `eth.src [0:3] == 00:0b:fc` prüft die ersten drei Bytes im Ethernet (Vendor Code)
- Der Filter `frame [12:2] <05:dc` zeigt nur IEEE 802.3 Ethernet Logical Link Control (LLC) Pakete

→ Der Text-Filter muss neu immer mit Gänsefüsschen frame contains "xxx" geschrieben werden.

# Neue Funktionen ab Wireshark Version 4

- Die Liste unter → **Statistiken → Verbindungen** hat nun neue Parameter und Funktionen.
- Die Darstellung zeigt eine Übersicht aller Verbindungen auf den verschiedenen Layern.
- Jede Kolonne lässt sich nach wie vor auf- oder absteigend sortieren
- Die Rechte Maustaste auf einer beliebigen Zeile führt direkt zu den Filtermöglichkeiten.




*Das Conversation Panel: der beste Ausgangspunkt zum Filtern auf Verbindungen auf verschiedenen Schichten*

# Sysdig neuer Haupt-Sponsor von Wireshark

**Im Januar 2022 übernahm die Firma Sysdig die Wireshark-Sponsorschaft von Riverbed.**

- Das Open-Source Projekt Wireshark basiert auf freiwilligen Softwareprogrammieren rund um den Globus, die kostenlos die Weiterentwicklung von Wireshark fördern.
- Unter der Leitung von Gerald Combs hat sich ein Team von ca. 20 Core-Entwicklern gebildet, welches über wichtige Wireshark Entwicklungsschritte entscheidet.


- Ursprünglich lief Ethereal nur auf Linux/Unix basierten Betriebssystemen mit dem Libpcap-Driver.
- Einer der wichtigsten Schritte von Wireshark war die Unterstützung des Windows-Betriebssystems.
- Der Italiener **Loris Degioanni** entwickelte als PhD-Arbeit an der Universität in Turin **WinPcap.**
- Dieser WinPcap-Driver ermöglichte erst den Betrieb von Ethereal/Wireshark unter Windows.
- Ab 2006 arbeiteten Gerald und Loris zusammen unter CACE Technologies in Kalifornien.
- 2014 gründete Loris **Sysdig**, die erste Firma spezialisiert auf Monitoring von Cloud and Containers.
- Nun hat Sysdig (System Digging) Gerald und die Sponsorschaft von Wireshark übernommen.

**Eine ideale Kombination, die von der Wireshark Community sehr begrüsst wurde und den Fortbestand von Wireshark für lange Zeit garantieren wird.** 👍👍👍

# Neue Spende-Möglichkeit an die Wireshark Foundation

**Bei der Übernahme der Sponsorschaft von Wireshark durch Sysdig wurde auch die Wireshark Foundation neu aufgestellt.**

- Das Wireshark Logo und das Finne Symbol sind eingetragene Handelsmarken der Wireshark Foundation.


- Die Wireshark Foundation, mit Gerald Combs als Präsident, ist nun eine gemeinnützige Organisationen zur Förderung von Wissenschaft.
- Registriert nach amerikanischem Recht unter 501(c)3 non profit organisation ist es der Wireshark Foundation nun möglich, zum Steuerabzug berechtigte Spenden entgegenzunehmen.


- Alle Aktivitäten von Leutert NetServices basieren seit 2006 vollständig auf Wireshark; wir haben bereits eine grosszügige Spende ausgerichtet und werden dies auch in Zukunft regelmässig tun.
- Wenn Wireshark auch in Ihrem täglichen Geschäft eine wichtige Rolle spielt, ermuntern wir auch Sie dies zu honorieren. Die Spenden werden für die laufenden Betriebskosten verwendet.

→ Neu eingerichtet wurde auch ein Wireshark Shop mit zahlreichen Werbeartikeln.

# QUIC Update

https://quicwg.org/

In meinem letzten Newsletter vom April 2021 habe ich zum ersten Mal über das neue QUIC Protokoll berichtet, das von IETF im Mai 2021 standardisiert wurde.

- Während zu diesem Zeitpunkt QUIC in vielen Browsern noch manuell aktiviert werden musste, ist QUIC in den aktuellen Browsern per default aktiv und wird sogar gegenüber TCP bevorzugt.
- Inzwischen konnte ich QUIC bereits bei einigen Kunden vorstellen; die einstündige Einführung, aufgezeichnet durch die Firma onway, ist als Webinar bei YouTube abrufbar.
- Die Bevorzugung von QUIC durch die Browser hat das neue Protokoll (meistens als HTTP/3 oder H3 bezeichnet) weiter etabliert, wie auch der Bericht von Heise Online vom Juli 2022 zeigt.

→ Es ist also höchste Zeit, sich als Netzwerker mit QUIC vertraut zu machen. Wireshark starten, mit der Webseite von YouTube verbinden, und Sie werden das QUIC Protokoll in Aktion sehen.

**Wegen den eingeschränkten Filter-Möglichkeiten empfehlen jedoch viele Security Device Hersteller immer noch, das QUIC-Protokoll zu sperren (UDP Ports 80 & 443).** (Stand Juni 2022)

- Checkpoint: NO QUIC security profile. (Recommended to block it)
- Cisco: QUIC Fingerprinting possible in Secure Firewall V7.3.
- Palo Alto: No QUIC security profile. (Recommended to block it)
- Fortinet: No QUIC security profile. (Recommended to block it)
- Sophos: No QUIC security profile. (Recommended to block it)
- F5 Networks: QUIC support in experimental status.
- SonicWall: No QUIC security profile. (Recommended to block it)

# QUIC Update

- Einige Quellen melden aktuell bereits einen QUIC-Anteil von ca. 25% des Internet-Verkehrs.
- Inzwischen ist es klar: QUIC wird sich neben TCP etablieren, die Entwicklung steht erst am Anfang und wird rasant weitergetrieben.
- **SMB over QUIC** für Windows-Umgebung steht nun zur Verfügung (Danke Herbert G. für die Links)

  https://learn.microsoft.com/de-de/windows-server/storage/file-server/smb-over-quic

  https://www.windowspro.de/roland-eich/smb-over-quic-windows-server-2022-nutzen
- **DNS over QUIC** (DoQ) ist da, und viele weitere Applikationen werden für QUIC vorbereitet.

→ **Es bleibt die Schwierigkeit, das QUIC- Protokoll auf herkömmliche Art zu analysieren.**

**Hier einige Zitate aus einer QUIC-Beschreibung** (die Beste die ich bisher fand)

*<< If QUIC takes much more importance in the future, the troubleshooting of the network engineers will be deeply modified >>*

*<< With QUIC (without the session keys) most of the flows are encrypted and parameters used for the troubleshooting is hidden >>*

*<< The tracking of packet loss, latency, jitter, out of order, congestion window, etc. is impossible >>*

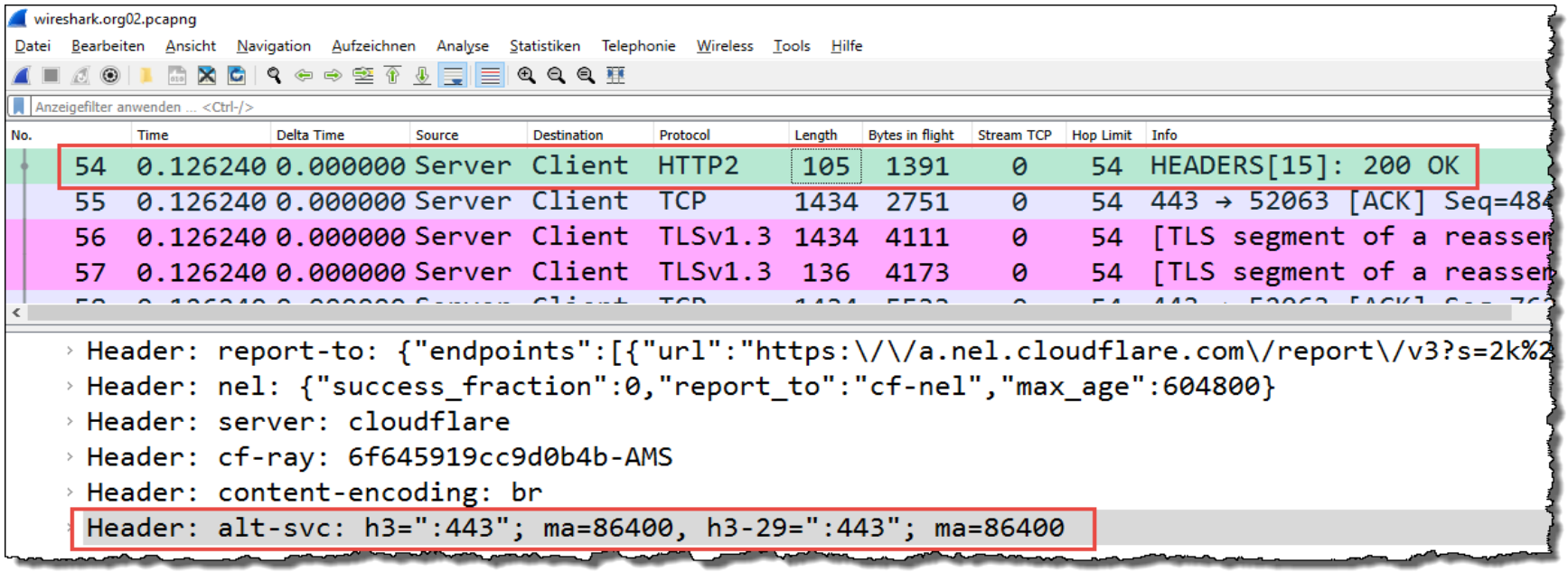
*<< QUIC also has a huge impact on network security devices. It's why all security devices providers will slow down the deployment of QUIC >>*

Quelle: https://blogit.michelin.io/quic-analysis-a-udp-based-multiplexed-and-secure-transport/

# QUIC Update

## Neue Service Binding Parameter (SVCB) für QUIC in DNS

- Die Frage lautet: Wie erkennt ein QUIC-fähiger Client, ob der Zielserver auch QUIC unterstützt?
- Die Antwort: Beim ersten Kontakt mit einem Server verwendet der Client TCP.
- Der Server signalisiert dann in HTTPS-Antworten, dass auch H3 (QUIC) unterstützt wird.
- H3 Unterstützung wird im HTTP Header im Feld **alt-svc** (alternate services) spezifiziert:

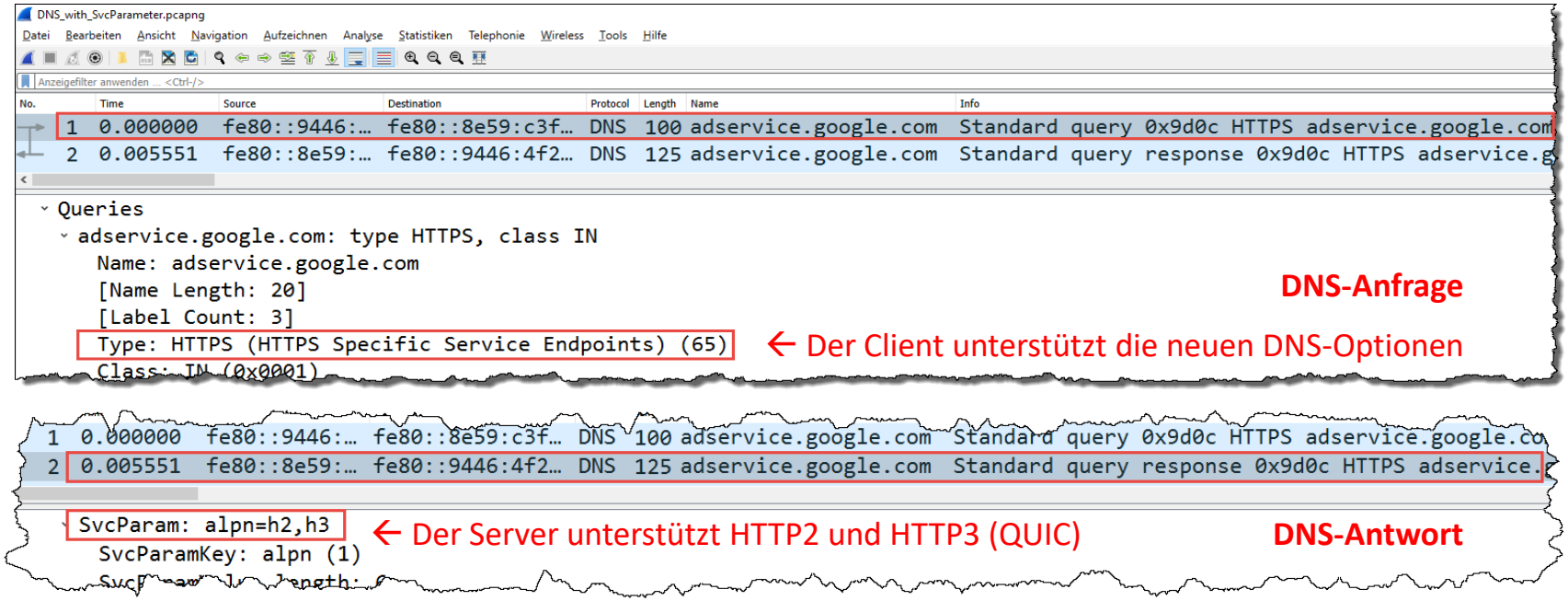



- Der Client wechselt dann **on the fly** auf QUIC und beendet die bestehende TCP-Session.
- Der Client speichert diese Information und kontaktiert den Server fortan direkt mit QUIC.

# QUIC Update

## Neue Service Binding (SVCB) Parameter für QUIC in DNS

- Um den Umweg über TCP auszuschalten, wurden im DNS neue Service Parameter definiert.
- Diese SVCBs sind noch IETF Drafts, teilweise jedoch bereits implementiert (z.B. Cloudflare DNS)
- Der DNS Resolver des Clients signalisiert in der DNS-Anfrage, ob diese Optionen unterstützt sind.

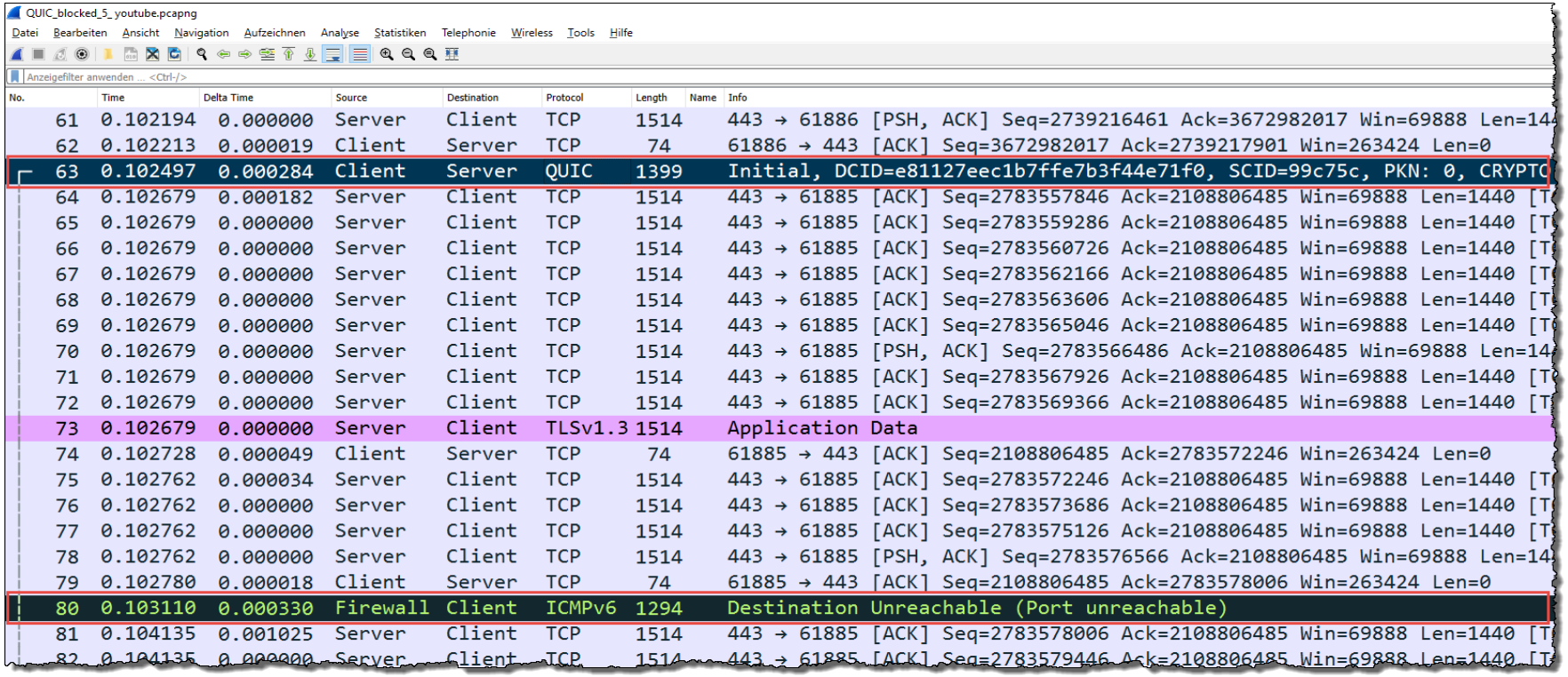



- Das Feld Application Layer Protocol Negotiation (ALPN) zeigt, dass dieser Server H3 unterstützt.
- D.h. der Client kann den Server direkt mit H3 (QUIC) kontaktieren, ohne den Umweg über TCP.
- Der Filter dns.svcb.svcparam.key zeigt alle DNS-Antworten mit den neuen Parametern.

# QUIC Update

## Blockieren von QUIC in Firewalls

- Wie bereits erwähnt, sind die meisten Firewall-Hersteller noch nicht QUIC-Ready und empfehlen die von QUIC verwendeten Ports UDP/80 und UDP/443 zu sperren.
- Solange noch keine Server existieren, die nur noch QUIC unterstützen, stellt dies kein Problem dar.
- Der Client verbindet über TCP mit dem Server, versucht jedoch sporadisch mit QUIC zu verbinden.




- Die Firewall reagiert mit ICMP (port unreachable) und die TCP-Verbindung bleibt bestehen.

# Quick UDP Internet Connections (QUIC)

## Zusammenfassung und Ausblick

- Die Wireshark-Analyse wird durch folgende QUIC Eigenschaften wesentlich schwieriger:
  - Starke Verschlüsselung mit TLS 1.3
  - Zahlreiche unterschiedliche Header und Frame-Formate
  - Die meisten Felder im Header haben variable Grössen
  - Mehrere und unterschiedliche Pakete im gleichen Frame sind möglich (vergleichbar mit SCTP)
  - Drei verschiedene Paketgruppen mit eigenem Paketzähler und eigenen Bestätigungen
  - Mehrere, parallele Streams im selben Frame, begrenzt nur durch die max. Ethernet Framelänge
  - Filtern auf einen Stream wird dadurch verunmöglicht, da Wireshark nur ganze Frames filtern kann
  - IP-Adresse und UDP-Port können während der Verbindung geändert werden (für Roaming)
  - Und viele Eigenschaften mehr…
- Der QUIC Rollout betrifft nicht nur Server und Clients, auch Firewalls, Loadbalancer etc.
- Implementierungsprobleme in vielen Komponenten basierend auf TCP sind zu erwarten
- Umso wichtiger werden QUIC-Kenntnisse und Analysemöglichkeiten mit Wireshark
- Die Wireshark-Decodierung ist noch nicht komplett, und ein Expert-System fehlt (noch)

- Aktuell standen mir noch keine Tracefiles mit Übertragungsfehlern zur Verfügung
- Ich werde QUIC-Updates und Fehlersituationen in weiteren Newslettern behandeln

⇨ **Feedback und QUIC-Tracefiles sind von euch Sniffern gerne willkommen** ⇦

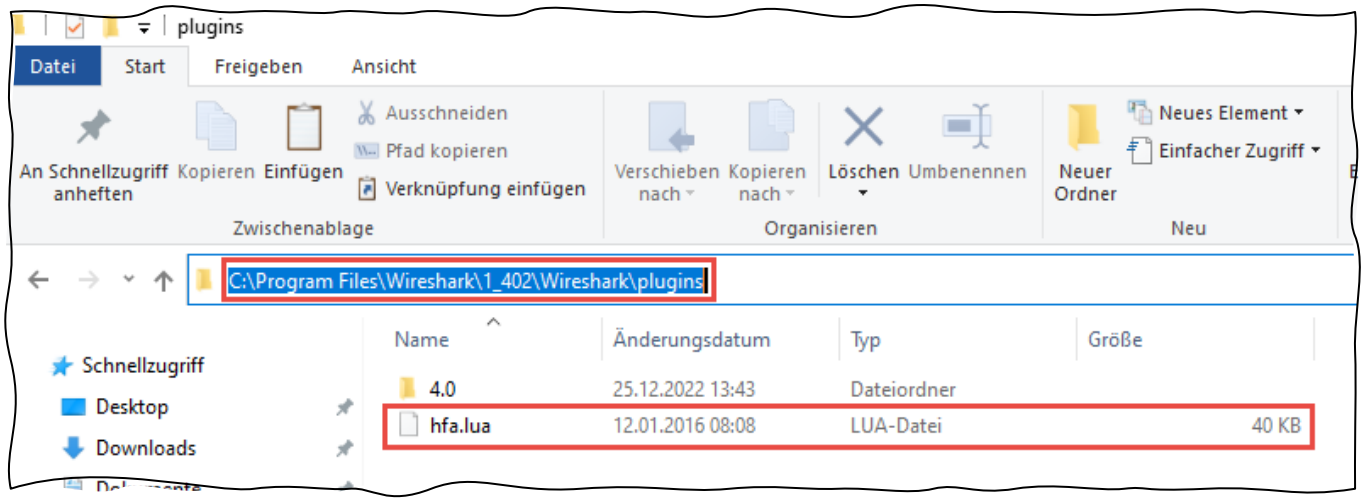
# Tipps, Tricks & Traces

## VoIP: Installieren eines LUA-Plugins für HFA-Protokoll

- Zahlreiche meiner VoIP-Kunden setzen in den Kundennetzwerken neben SIP auch das UNIFY-proprietäre **HFA** (**H**iPath **F**eature **A**ccess) Protokoll ein.
- Wireshark hat (noch) keinen HFA-Dissector und kann HFA deshalb nicht decodieren.
- Mit der Scriptsprache LUA lässt sich ein eigener Decoder schreiben und in Wireshark installieren.
- Jonas Köritz (Deutschland) hat ein HFA LUA-Plugin entwickelt, welches HFA decodiert.

→ Die hfa.lua Datei herunterladen und in den Wireshark\plugins Ordner kopieren.

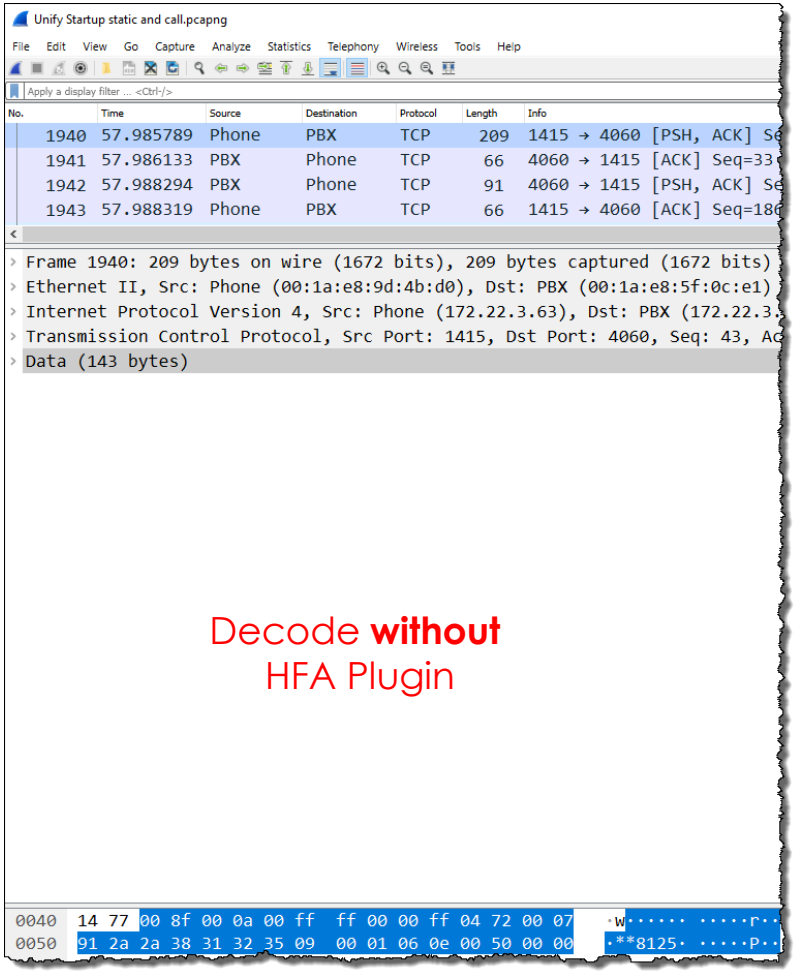
→ Im Wireshark unter → Analyse → Lua Plugins neu laden klicken oder Wireshark neu starten.

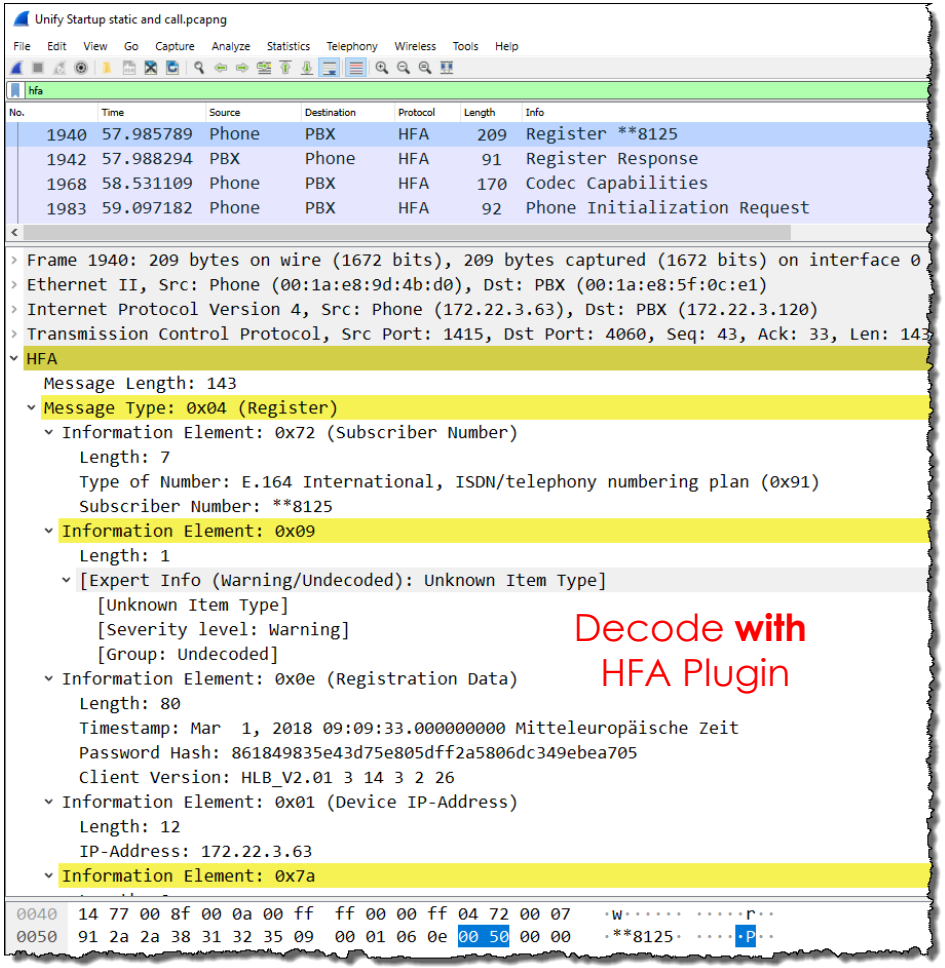


# Tipps, Tricks & Traces

## VoIP: Installieren eines LUA-Plugins für HFA-Protokoll

- Leider decodiert das LUA-Plugin nicht alle Felder (gelb markiert), aber für die Analyse gut genug.

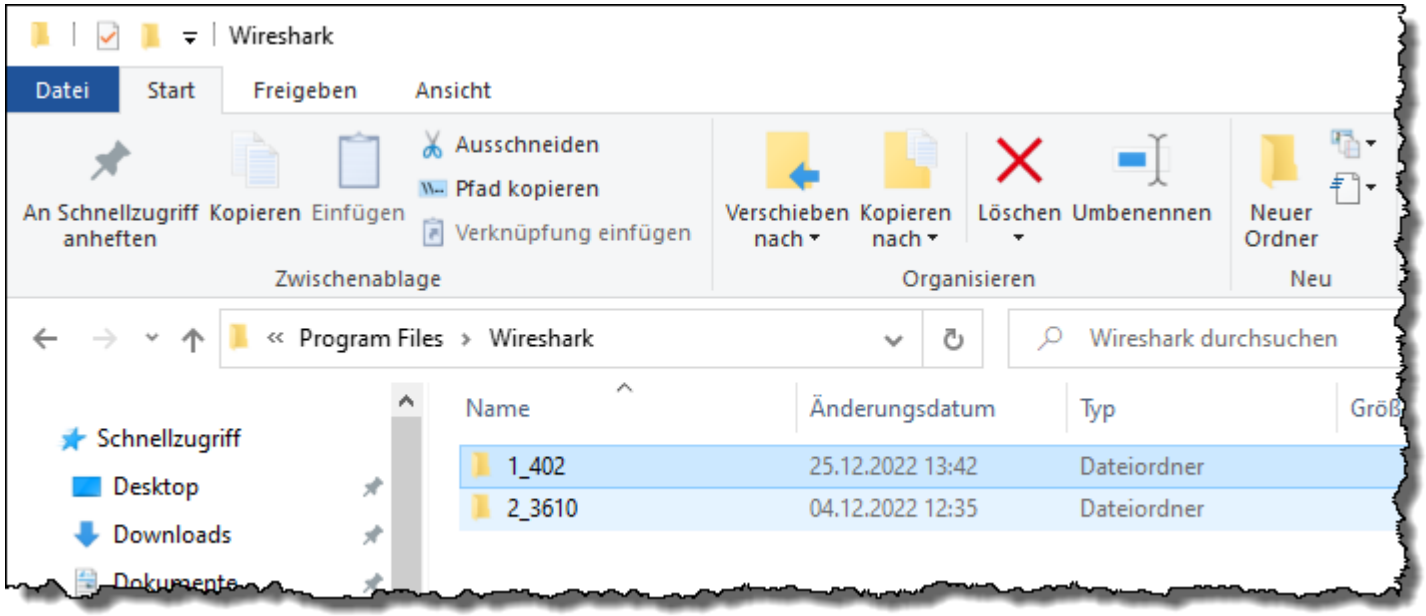


# Tipps, Tricks & Traces

## Installieren von mehreren Wireshark Versionen

- Leider ist nicht garantiert, dass Plugins bei Wireshark Versionswechseln immer noch funktionieren.
- Aus solchen Gründen kann es erwünscht sein, mehrere Wireshark-Versionen zu installieren.
- Wireshark startet Per Default immer die erste Version im Program Files Ordner.
- Mit einer Desktop-Verknüpfung kann die gewünschte Version direkt ausgewählt werden.
- Wireshark kann auch mehrfach gestartet werden und gleichzeitig aktiv sein.




Wireshark 4.0.2

Wireshark 3.6.10

# Unsere Wireshark-Protokoll-Kurse & andere Events

## AnyWeb Training – neuer Schulungspartner in der Schweiz

In der Regel führen wir unsere Wireshark Schulungen als Firmenkurse bei Kunden durch, was sich schon ab vier Teilnehmern lohnt. Da jedoch viele kleinere Unternehmen ihre Netzwerktechniker ebenfalls in Protokollwissen und Wireshark Troubleshooting ausbilden möchten, bieten wir in Deutschland, Österreich und der Schweiz auch öffentliche Kurse an.

Wir freuen uns, Ihnen unseren neuen Schulungspartner für die Schweiz vorstellen zu können: AnyWeb Training. Die sehr ambitionierte Firma ist seit 1996 offizieller Cisco Learning Partner und hat sich mit ihren praxisorientierten Kursen den Ruf eines hoch kompetenten Schulungsanbieters erarbeitet. Die Wireshark-Kursdaten für 2023 sind bereits aufgeschaltet und können ab sofort gebucht werden. Die Kurse werden von Leutert NetServices durchgeführt.

## Neuer Trainer bei unserem Kursanbieter ARROW in Wien

Im Laufe dieses Jahres wird sich unser langjähriger Wireshark Trainer Herbert Grabmeyer in den wohlverdienten Ruhestand zurückziehen. Herbert wurde von den Kursteilnehmern für seine hohe Fachkompetenz sehr geschätzt, und wir danken ihm für die professionelle Zusammenarbeit.

Als Nachfolger wird Robert Bihlmeyer unsere lizenzierten Wireshark-Kurse bei Arrow ECS GmbH durchführen. Robert ist erfahrener VMware-Trainer und kennt sich auch mit Wireshark bestens aus. Die Wireshark-Kursdaten für 2023 sind bereits aufgeschaltet und können ab sofort gebucht werden. Wir heissen Robert herzlich willkommen und wünschen ihm viel Erfolg.

# Unsere Wireshark-Protokoll-Kurse & andere Events

- **Öffentliche Kurse in der Schweiz** → Zur Anmeldung bei AnyWeb
  Bei AnyWeb Training in Zürich
- **Öffentliche Kurse in Österreich** → Zur Anmeldung bei ARROW
  Bei Arrow ECS GmbH in Wien
- **Öffentliche Kurse in Deutschland** → Zur Anmeldung bei ALSO
  Remote Kurse bei ALSO
- **Übersicht aller öffentliche Kurse** → Kurse Leutert NetServices

Unser Spezialität sind Firmenkurse oder Tech-Sessions nach ihren Wünschen zu den Themen:

- **Einführung Netzwerkanalyse, Wireshark Tipps & Tricks, TCP/IP, QUIC, WLAN, VoIP und IPv6**
- YouTube Webinar (1h) **Troubleshooting WLANs mit Wireshark** aufgezeichnet durch onway.


Die Präsentationen der in Europa und den USA durchgeführten Shark**Fest** Konferenzen sind abrufbar unter:
Europa: https://sharkfesteurope.wireshark.org/retrospective
USA: https://sharkfestus.wireshark.org/retrospective

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

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

**Have fun and enjoy sniffing**, Rolf Leutert