WIRE**SHARK Newsletter Februar 2025**

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**
- **Stratoshark**, der neue Bruder von **Wireshark**
- Das erste **PacketFest '25 in Zürich**

Tipps, Tricks & Traces:

- Kostengünstige, mobile **10 Gbit/s Aufzeichnungshardware**
- **Wireshark Profil** für **Encapsulated Frames**
- **Cool Commands**, kurze Video Clips zu den Themen **Wireshark**, **Cisco** usw.

Kurse & Events:

- Neuer **Wireshark** Kurs **The Packet Factor** bei **AnyWeb Training**
- Aktuelle **Kursdaten**

Neue Funktionen ab Wireshark Version 4

Display- zu Capture-Filter Übersetzer

- **Display- und Capture-Filter** haben aus historischen Gründen einen **unterschiedlichen Befehlssatz**

Capture Filter Syntax:

ether host 00:11:95:b7:e0:3e
ether src 00:11:95:b7:e0:3e
ether dst 00:11:95:b7:e0:3e

host 192.168.178.1
src host 192.168.178.1
dst host 192.168.178.1

net 192.168.178.0 mask 255.255.255.0
net 192.168.178/24

arp
not ip
tcp
udp port 138

Operators: not, and, or

http://wiki.wireshark.org/CaptureFilters

Display Filter Syntax:

eth.addr == 00:11:95:b7:e0:3e
eth.src == 00:11:95:b7:e0:3e
eth.dst == 01:00:5e:00:00:09

ip.addr == 192.168.178.1
ip.src == 192.168.178.1
ip.dst == 192.168.178.1

ip.addr == 192.168.178.0/24
ip.host contains "192.168.178"

arp
not ip
tcp
udp.port == 138

Operators: not, and, or

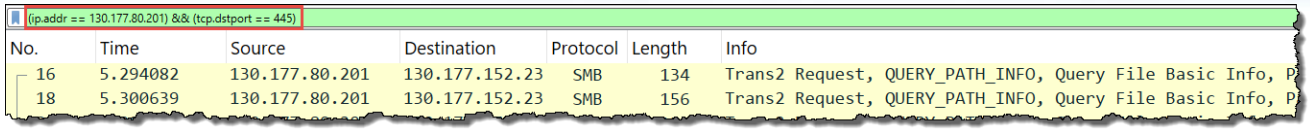
http://wiki.wireshark.org/DisplayFilters

- **Kursteilnehmer** fragen oft, ob es einen **Display- zu Capture-Filter Übersetzer** gibt? **Ja! Ab V4.4**

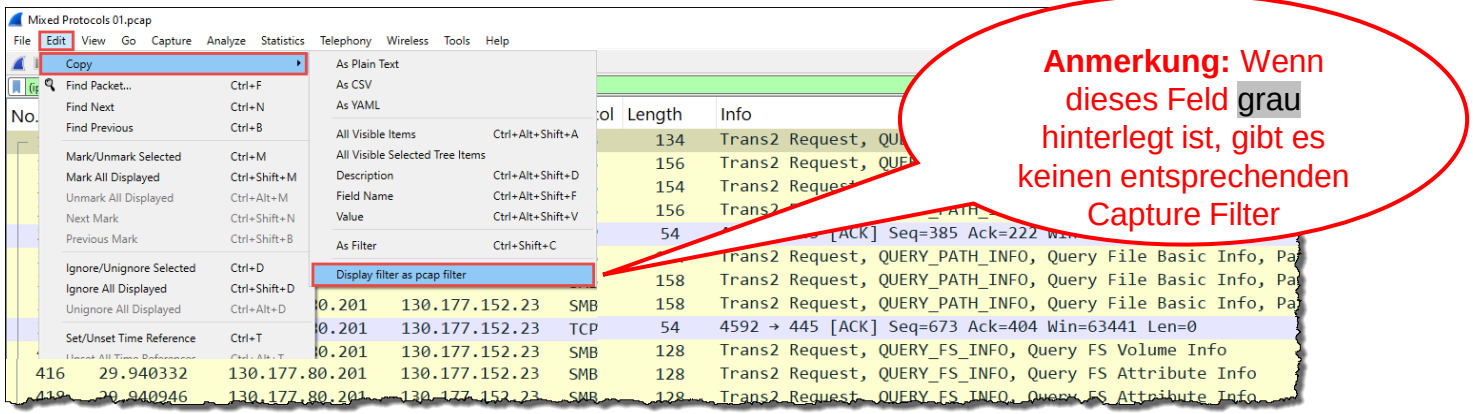
Neue Funktionen ab Wireshark Version 4

Display- zu Capture-Filter Übersetzer

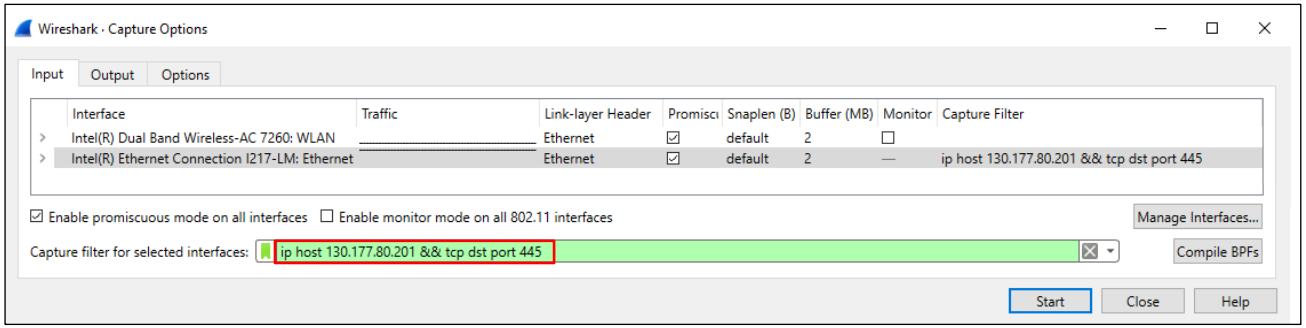
- Beispiel Display Filter: (ip.addr == 130.177.80.201) && (tcp.dstport == 445)



- Gehe zu → Edit → Copy → Display filter as pcap filter



- Gehe zu → Capture → Options Interface wählen und Filter mit rechtem Mausklick einfügen



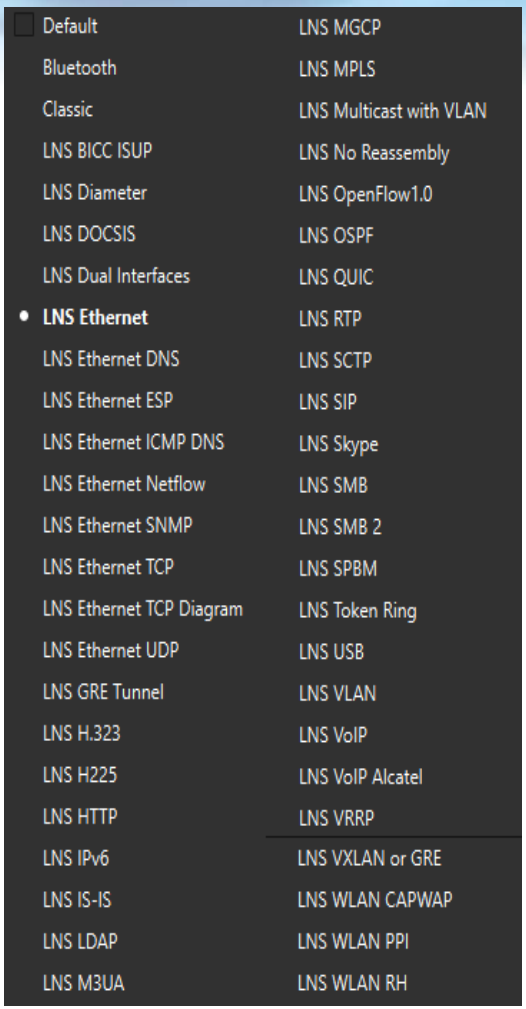
Neue Funktionen ab Wireshark Version 4

Automatic Profile Switching

- **Wireshark Profile** sind eine sehr nützliche Funktion, sie ermöglichen die Darstellung zu personalisieren indem die Anzeige mit eigenen **Spalten, Filter-Knöpfen, Farben** usw. an die Bedürfnisse angepasst werden kann.
- Sinnvoll ist z.B. ein eigenes **Profil für jedes der verschiedenen Protokolle.**
- **Profile** können **importiert und exportiert** werden, und lassen so auf einfache Weise auf weitere Computer verteilen (linke Maustaste im Wireshark Feld rechts unten).
- Im **Internet** gibt es zahlreiche **vorgefertigte Profile**, die bei Bedarf runtergeladen werden können.
- Mein Kollege **Walter Hofstetter** hat eine übersichtliche **Liste** dieser Profile erstellt; daraus sind die Eigenschaften der verschiedenen Profile ersichtlich.
- Dies ermöglicht, die Eignung eines Profils zu beurteilen, **ohne dieses installieren zu müssen.** Die Liste ist als PDF **hier** abrufbar.

Wireshark bietet eine **neue Funktion: Automatic Profile Switching**

- Diese ermöglicht das **automatische Aktivieren eines Profils** beim Öffnen eines Trace Files.
- Als **Zusatz zum Profil** wird ein entsprechender **Filter** konfiguriert, damit wird beim Öffnen eines Trace Files das entsprechende Profil aktiviert.

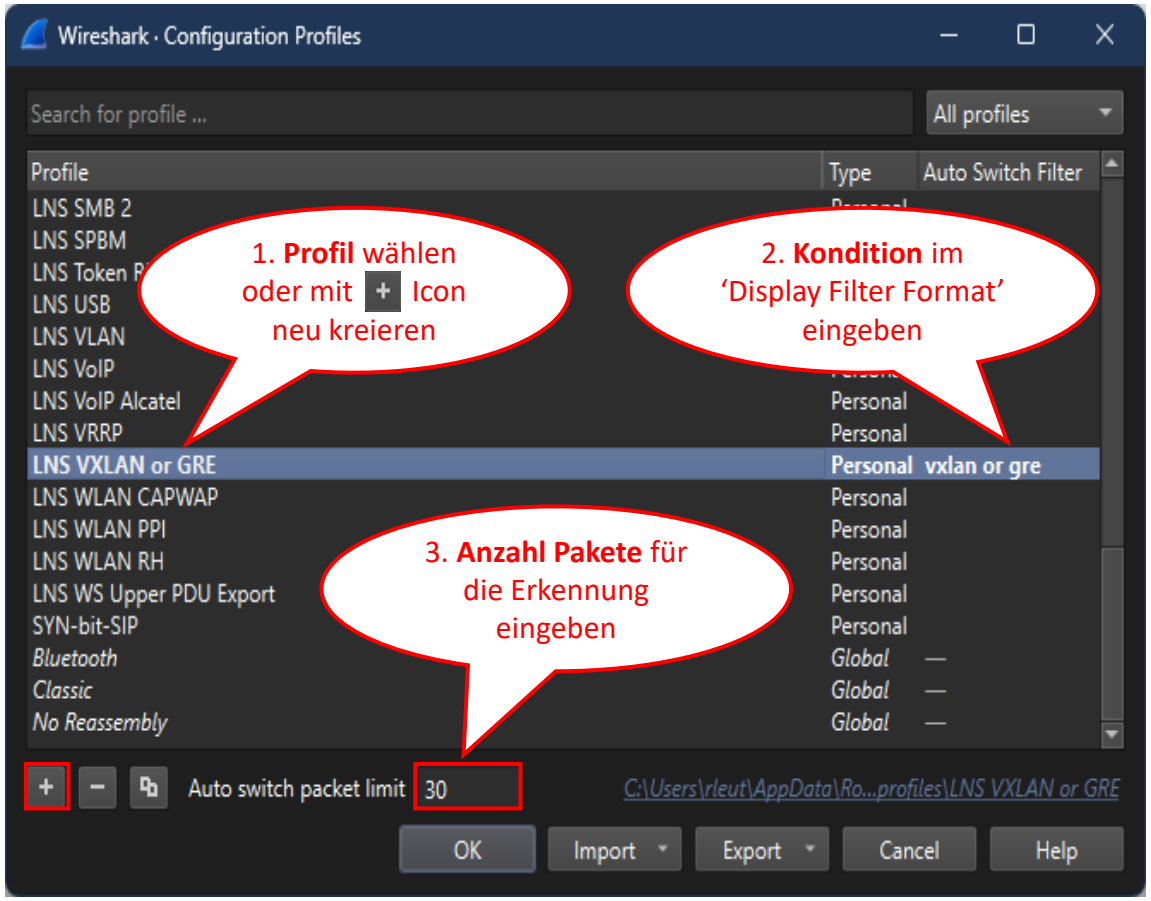


Meine Wireshark Profile

Neue Funktionen ab Wireshark Version 4

Automatic Profile Switching

- Diese Funktion aktiviert beim Öffnen eines Trace Files **automatisch ein entsprechendes Profil.**
- Zum Einrichten: **Wireshark** rechts unten im Feld **Profile → Rechte Maus Taste → Manage Profiles**



Die Protokolle **VXLAN** und **GRE-Tunnel** enthalten beide **äussere und innere Adressfelder.** (Wie so ein Profil erstellt wird, ist ab Seite 17 erklärt.)

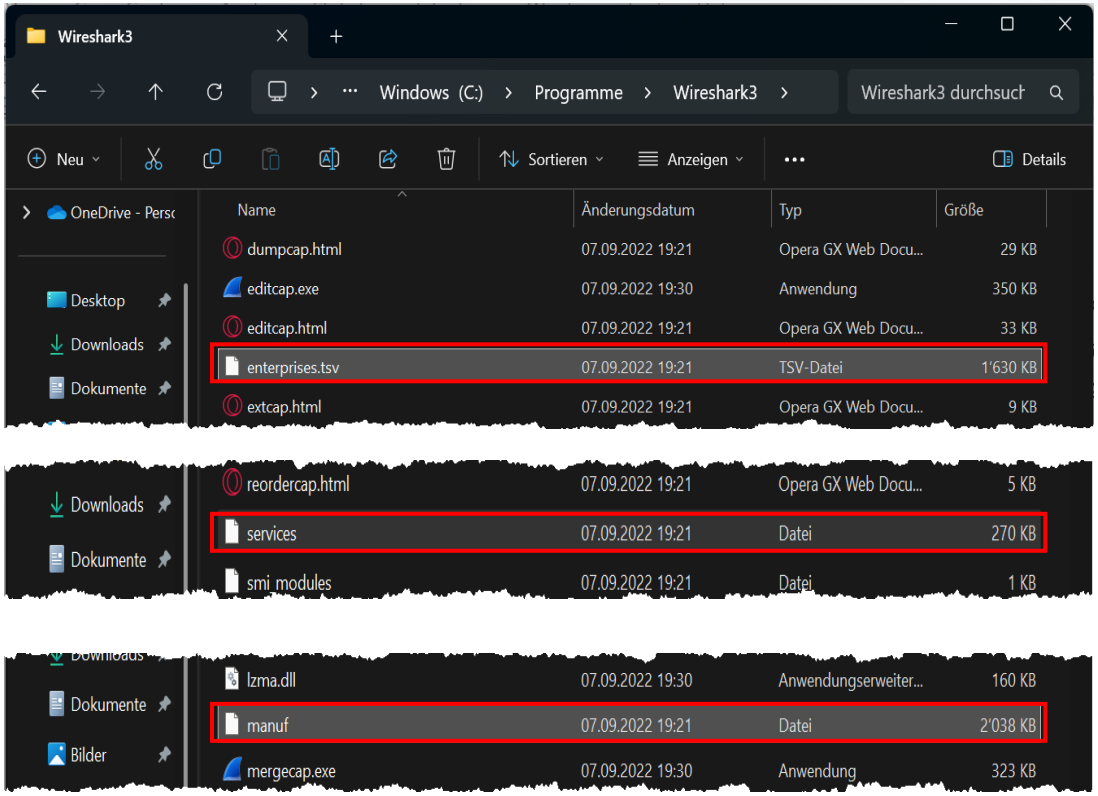
Zum Einrichten lässt sich als **Kondition** ein beliebiger **Display Filter** eingeben. Nach diesem sucht **Wireshark** beim Öffnen eines Trace Files in der eingegebenen Anzahl von Paketen.

Dieses Profil wird sich automatisch aktivieren, wenn in den ersten 30 Paketen das **VXLAN-** oder **GRE-Protokoll** erkannt wird.

Ein Profil kann mit dem Icon kopiert,
oder mit dem Icon gelöscht werden.

Neue Funktionen ab Wireshark Version 4

Um die **Aufstartzeit** von Wireshark zu verbessern, wurden untenstehende Dateien kompiliert, im **Wireshark-Code integriert** und sind deshalb im Wireshark Programm Ordner **nicht mehr editierbar.**



Bis Wireshark Version 3:

Die Datei **enterprises.tsv** enthielt die „SMI Network Management Private Enterprise Codes“, die von Wireshark bei der Namensauflösung beispielsweise in den Protokollen **Diameter** und **NetFlow** verwendet wurde.

Wireshark verwendete die Datei **services**, um Portnummern in Namen zu übersetzen.
z.B. **Port 443 TCP/UDP → HTTPS**

Die Datei **manuf** wurde von Wireshark zur Übersetzung von MAC-Adressen zu Herstellernamen verwendet.
z.B. **00:01:D7 → F5Networks**

Ab Version 4: Wireshark zeigt die Standard **manuf** Liste neu unter **→ Tools → MAC Address Blocks**

Unter diesem **Link** zeigt **Laura Chappell** wie weiterhin eine eigene **manuf** Datei erstellt werden kann.

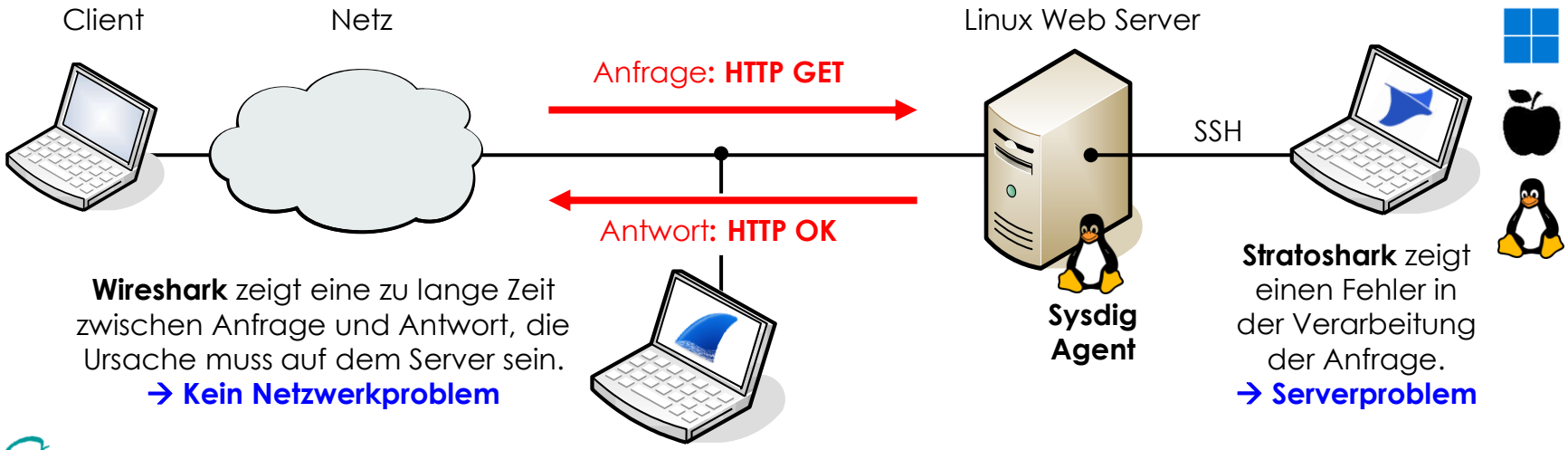
Stratoshark

Stratoshark ist ein neues **Open Source Tool**, welches die Aktivitäten, z.B. **innerhalb eines Servers** überwachen und analysieren kann.

Die Software zeichnet **Befehle und Transaktionen** zwischen den **Applikationen** und zum **Betriebssystem** (aktuell nur für LINUX), sogenannte **System Calls,** auf.

Dies hilft Applikationsentwicklern und Systembetreuern, die **System-internen Abläufe** mitzuverfolgen, **Fehler** und **Sicherheitslücken erkennen und beheben zu können.**

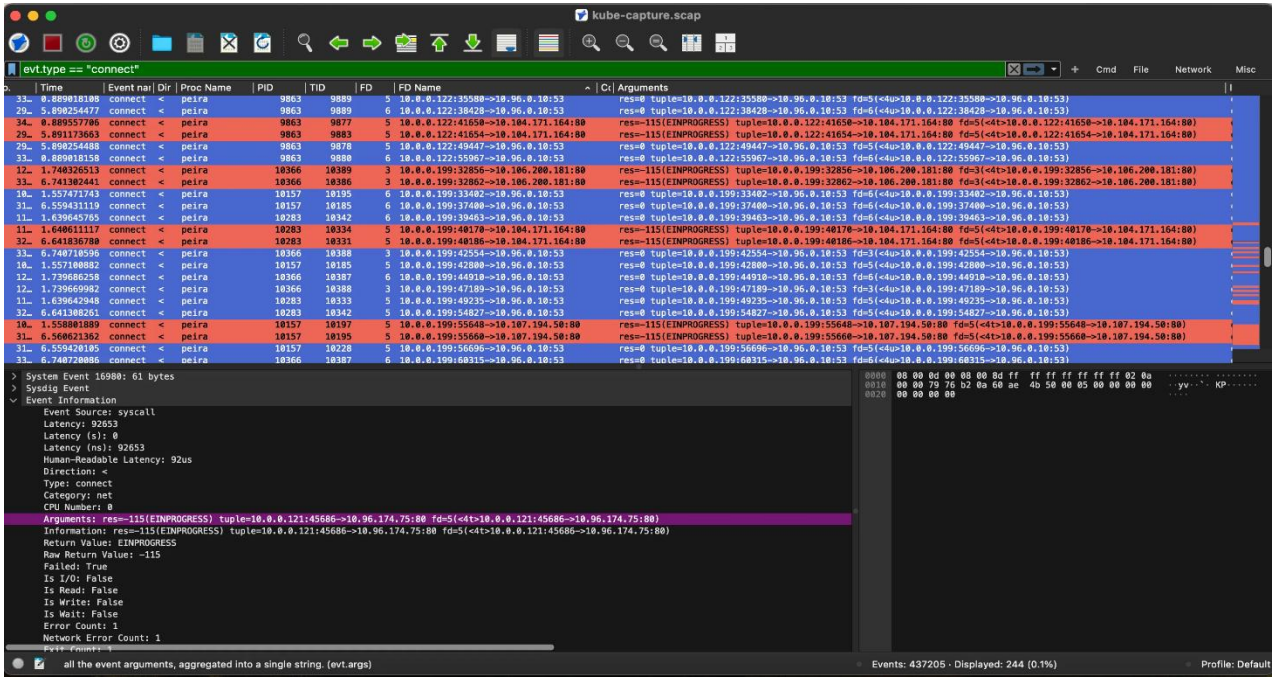
Stratoshark ist die ideale Ergänzung zu **Wireshark** für die Eingrenzung von Problemursachen.
Beispiel: Ein Benutzer klagt über lange Antwortzeiten des Web-Servers: **Netzwerk oder Server?**



Stratoshark

Stratoshark wurde entwickelt von der Firma **sysdig**, Marktführer im Bereich **Monitoring von Cloud and Containers.**
Sysdig ist auch der Sponsor von **Wireshark** und **Gerald Combs**, der Gründer von Wireshark, ist dort seit 2022 der **Director of Open Source**. (siehe Newsletter 2023)

Genial ! Stratoshark verwendet dasselbe GUI wie Wireshark, dadurch werden sich Wireshark Benutzer schnell zurechtfinden. Es sind bereits zahlreiche Video-Clips als Einführung verfügbar; das von **Ross Bagurdes** mag ich besonders https://youtu.be/Uz97DZmwRSM

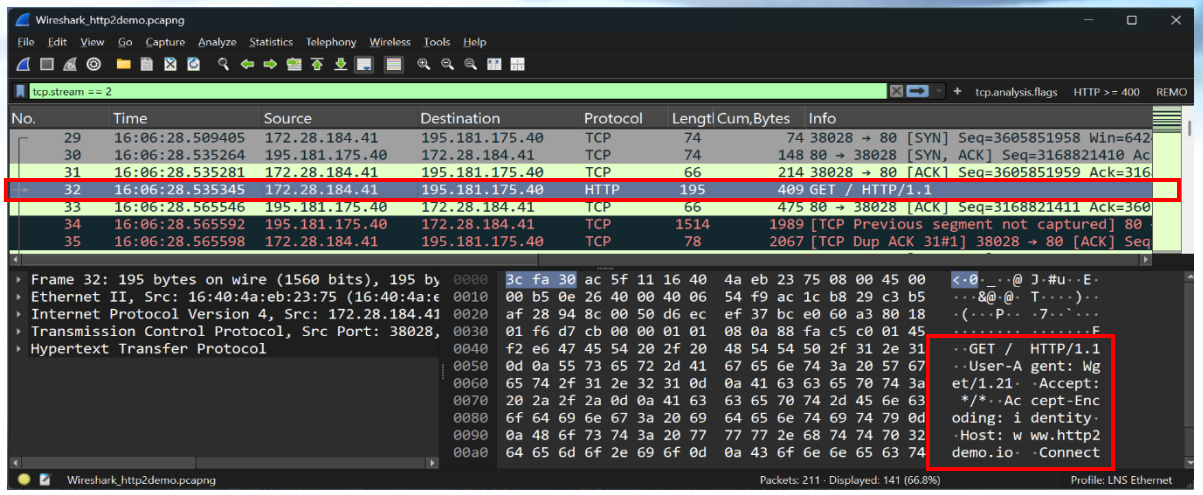


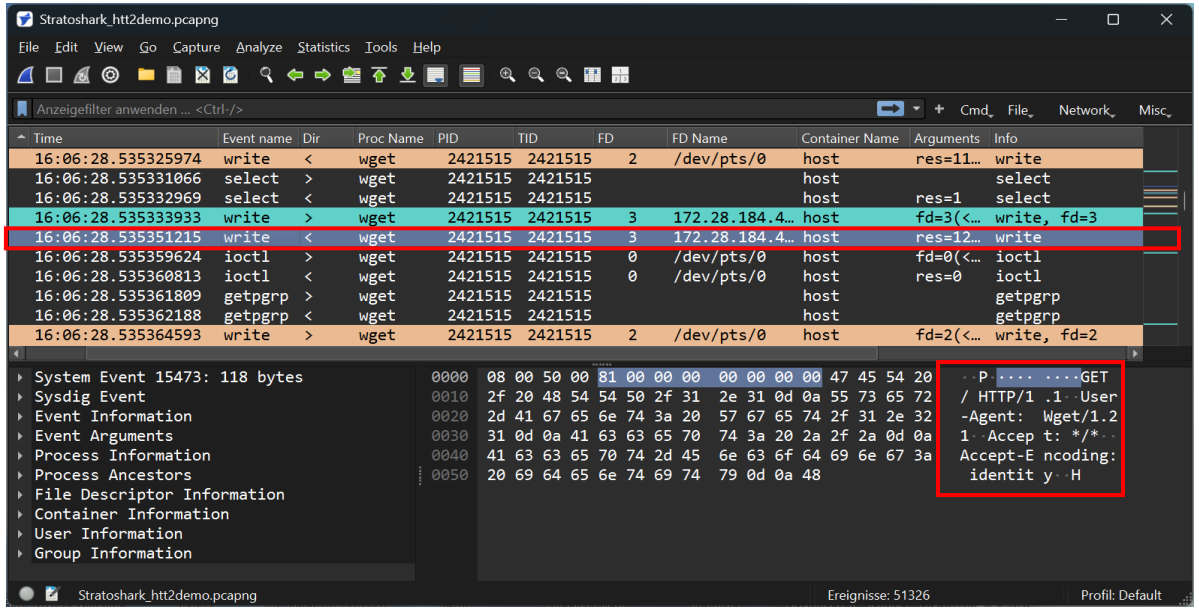
Stratoshark öffnet **Event Files** mit den Extensions **.scap** (von sysdig) und **.pcapng** (Wireshark)

Hier zeigt **Stratoshark** (Windows Version) einen **HTTP 404 Error**, aufgezeichnet auf einem **Linux Web Server.**

Das File **404Error.scap** ist als Demo verfügbar auf GitHub

Wireshark kombiniert mit Stratoshark



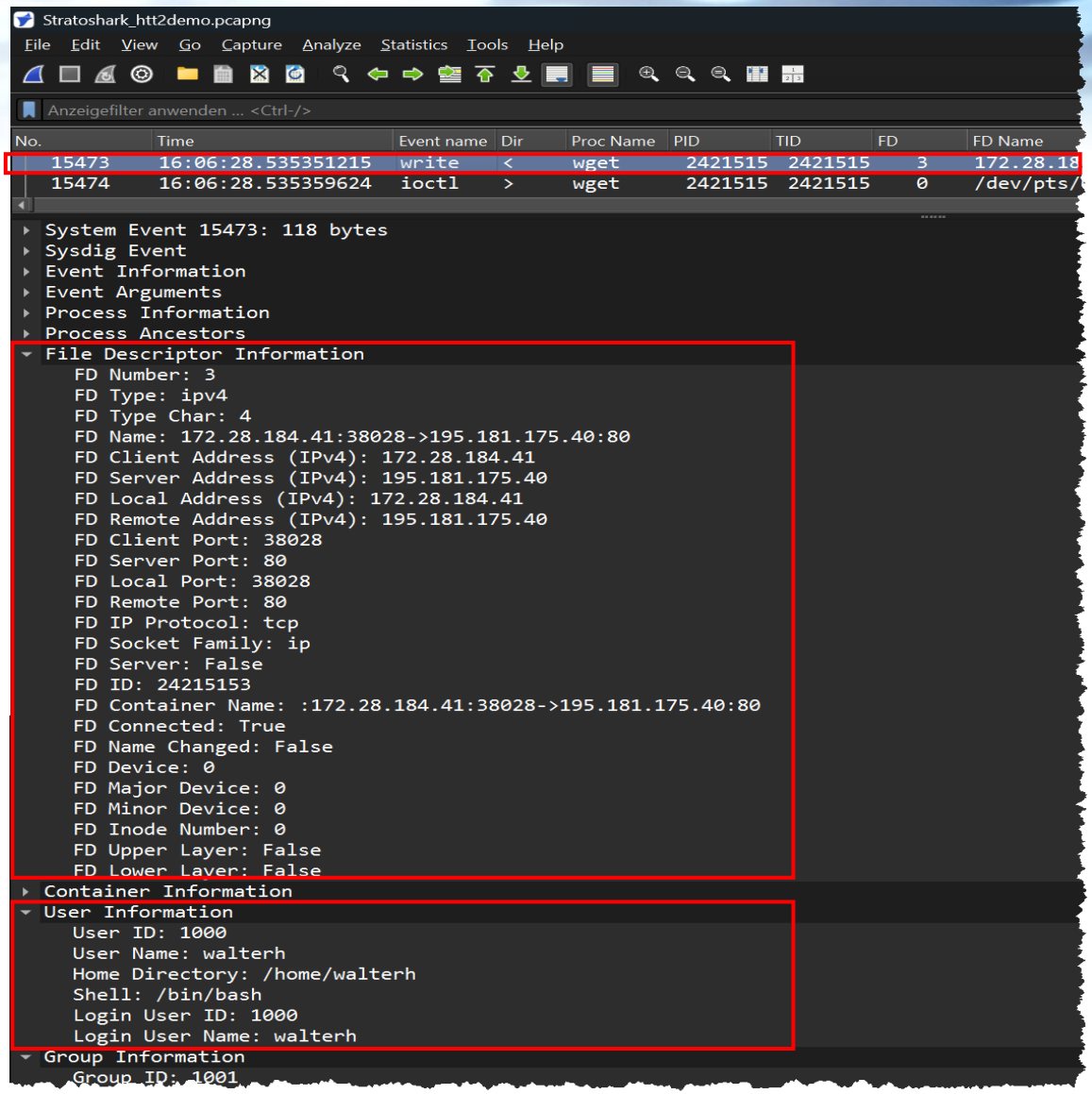


Zugriff auf eine Webseite, gleichzeitig aufgezeichnet mit **Wireshark** und **Stratoshark** *(Danke Walter Hofstetter)*

Wireshark zeigt den **Frame** **HTTP Get** als Zugriff auf eine Webseite.

Stratoshark zeigt denselben **HTTP Get** als **Event** mit IP-Adressen, Process ID, Thread ID und vielen weiteren Details.

Stratoshark Detail Fenster



In der Übersicht zeigt **Stratoshark** anstelle von Paketen pro Zeile einen **System Event.**

Die Zeilen im **Detail Fenster** können aufgeklappt werden und zeigen einen erstaunlichen Detaillierungsgrad.

STRATOSHARK
System Call and Event Log Analyzer

Obschon noch im **Pre-Release** Stadium, zeigt **Stratoshark** bereits sein riesiges Potenzial.

Vielen Dank an **Gerald Combs, Loris Degioanni** und ihr Team für dieses grossartige Tool.

PacketFest '25 in Zürich

News für die **ntop- und Wireshark-Community**: Am **8. und 9. Mai** findet das erste **PacketFest** statt.

PacketFest ist eine zweitägige technische Veranstaltung, bei der die ntop- und Wireshark-Community zusammenkommt, um Themen wie Netzwerküberwachung, Troubleshooting, Cybersicherheit und Open-Source-Technologien zu diskutieren.

Das Hauptziel der Veranstaltung besteht darin, zu zeigen, wie diese aktuellen Herausforderungen mit Hilfe bevorzugter Tools effektiv angegangen werden können.

Eine wertvolle Möglichkeit mit Gleich-gesinnten in Kontakt zu treten, Erfahrungen auszutauschen und die **neuesten Funktionen von ntop und Wireshark** zu erfahren.

Walter Hofstetter: Paketguru der ersten Stunde, wird zeigen, wie mit Wireshark **Cyber Threats** erkannt werden können.
Rolf Leutert: Ich werde Erkenntnisse aus **40 Jahren Paketanalyse** schildern und neue Wireshark Funktionen zeigen.

Es erwarten Sie zahlreiche weitere interessante Themen und Anwenderberichte.
Der Gründer von Wireshark, **Gerald Combs,** wird zugeschaltet folgenden Beitrag präsentieren
"Wiresharchaeology: How it started and where we're headed"

PacketFest '25 in Zürich

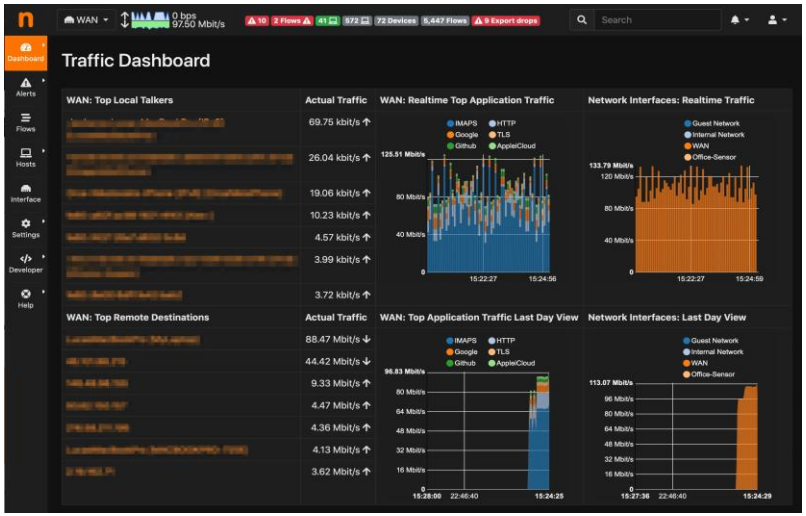
Dank des Hauptsponsors **ntop** können die Teilnahmekosten minimal gehalten werden.
Bei schneller **Anmeldung** bis 28. Feb. **CHF 125.-**, ab 1. März **CHF 150.-** (inkl. Mittagessen und Pausenverpflegung).

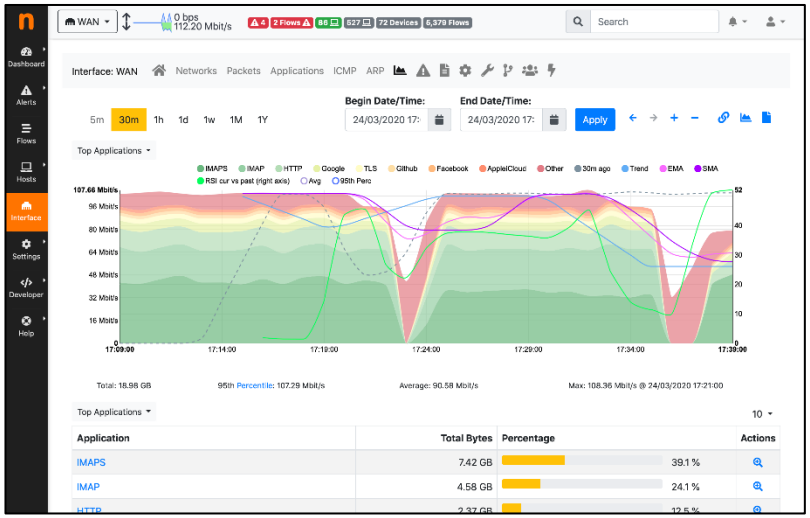
Vor dem PacketFest findet **am 7. Mai** die **Pre-Conference** mit einem **ntopng Training** statt. Die Anzahl Teilnehmer ist beschränkt. Die Teilnahme ist in den Kosten vom PacketFest **eingeschlossen**.

Das **Open-Source-Tool ntopng** der Firma **ntop** wird für die webbasierte Überwachung des Netzwerkverkehrs sowie der Sicherheitsaspekte eingesetzt und bietet u.a. folgende Funktionen:

- Passives Erfassen des Netzwerkverkehrs
- Sammeln von Netzwerkflüssen (NetFlow, sFlow usw.)
- Überwachen von ausgewählten Netzwerkgeräten
- Überwachen der Netzwerkinfrastruktur über SNMP

ntopng zeigt nicht nur Verkehrsstatistiken, sondern analysiert auch den Verkehr, zieht Schlussfolgerungen zum beobachteten Verkehrstyp und meldet Überschreitungen von Cybersicherheitsmetriken.



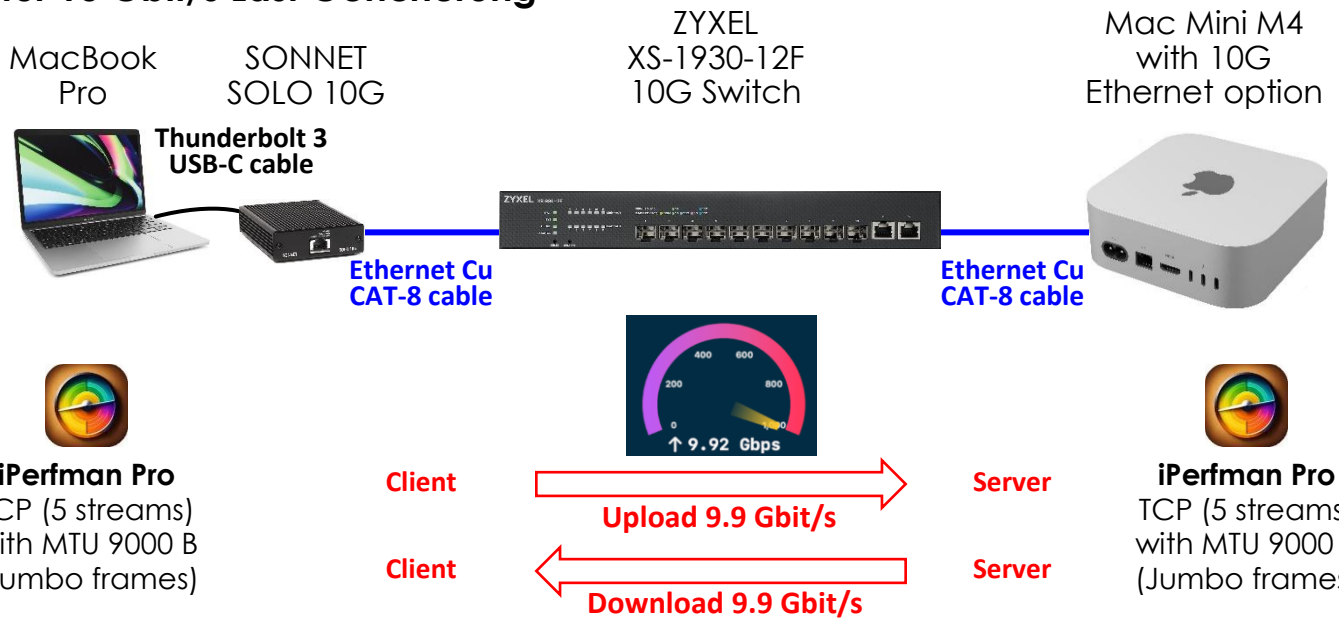


Tipps, Tricks & Traces

Kostengünstige, mobile 10 Gbit/s Aufzeichnungshardware

- Erst seit wenigen Monaten ist der neue **Mac Mini M4** von Apple auf dem Markt und setzt beim **Preis-Leistungs-Verhältnis neue Massstäbe** (CHF 900.- mit 512GB SSD und 10 Gbit Ethernet Option)
- Ein Kursteilnehmer brachte mich auf die Idee zu untersuchen, ob sich damit eine kostengünstige, **mobile Capture Unit für Wireshark** mit bis zu 10 Gbit/s realisieren lässt.
- Die erste Herausforderung war es, eine Testanordnung zu erstellen, die in der Lage ist die volle Datenrate von **10 Gbit/s zu generieren.**
- Ein erster Versuch mit einem künstlich erzeugten Switch **Spanning-Tree-Loop** ergab nur ca. 2 Gbit/s.
- Mit **iPerfman Pro** (eine GUI-Version des bekannten Tools **iPerf3**) und optimierten TCP-Parametern konnte Volllast auf dem 10 Gbit Ethernet generiert werden.

Testlayout für 10 Gbit/s Last Generierung



Tipps, Tricks & Traces

Kostengünstige, mobile 10 Gbit/s Aufzeichnungshardware

- Das Ziel war es zu ermitteln, **wieviel Prozent** der 9.9 Gbit/s der **Mac Mini** aufzuzeichnen vermag.
- Aus verschiedenen Gründen (wegen zusätzliche CPU-Last, Ethernet Offloading-Funktionen usw.) ist es in der Praxis **nicht empfohlen,** Wireshark auf dem Sender oder Empfänger aufzeichnen zu lassen.
- Zur Vereinfachung des Testlayouts und in Ermangelung eines zweiten Mac Mini wurde hier (entgegen der Empfehlung) **trotzdem mit Wireshark auf dem Mac Mini aufgezeichnet**, gleichzeitig zum laufenden **iPerfman Pro**.
- Die Resultate waren erstaunlich: **Kein Frameverlust während der gesamten Aufzeichnung!**

Testlayout für 10 Gbit/s Aufzeichnung

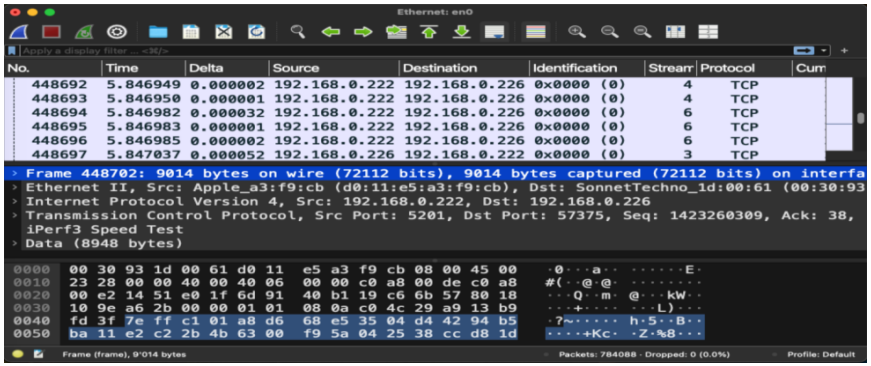
Mac Mini M4
with 10G
Ethernet option

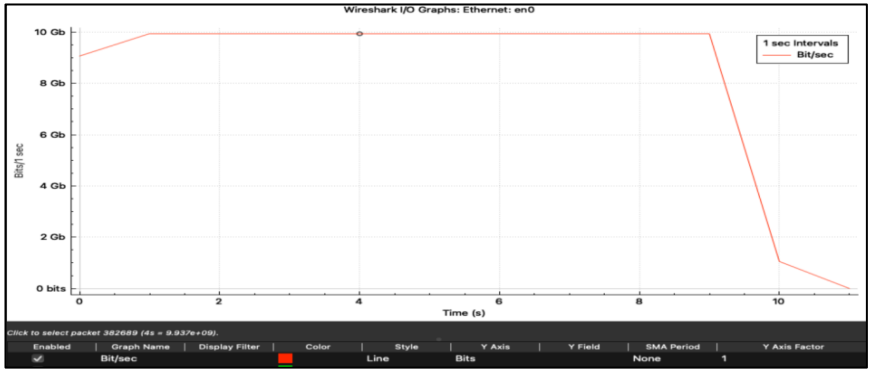
Ethernet Cu
CAT-8 cable

iPerfman Pro
TCP (5 streams)
with MTU 9000 B
(Jumbo frames)

No dropped Frames!

9.9 Gigabit/s Throughput

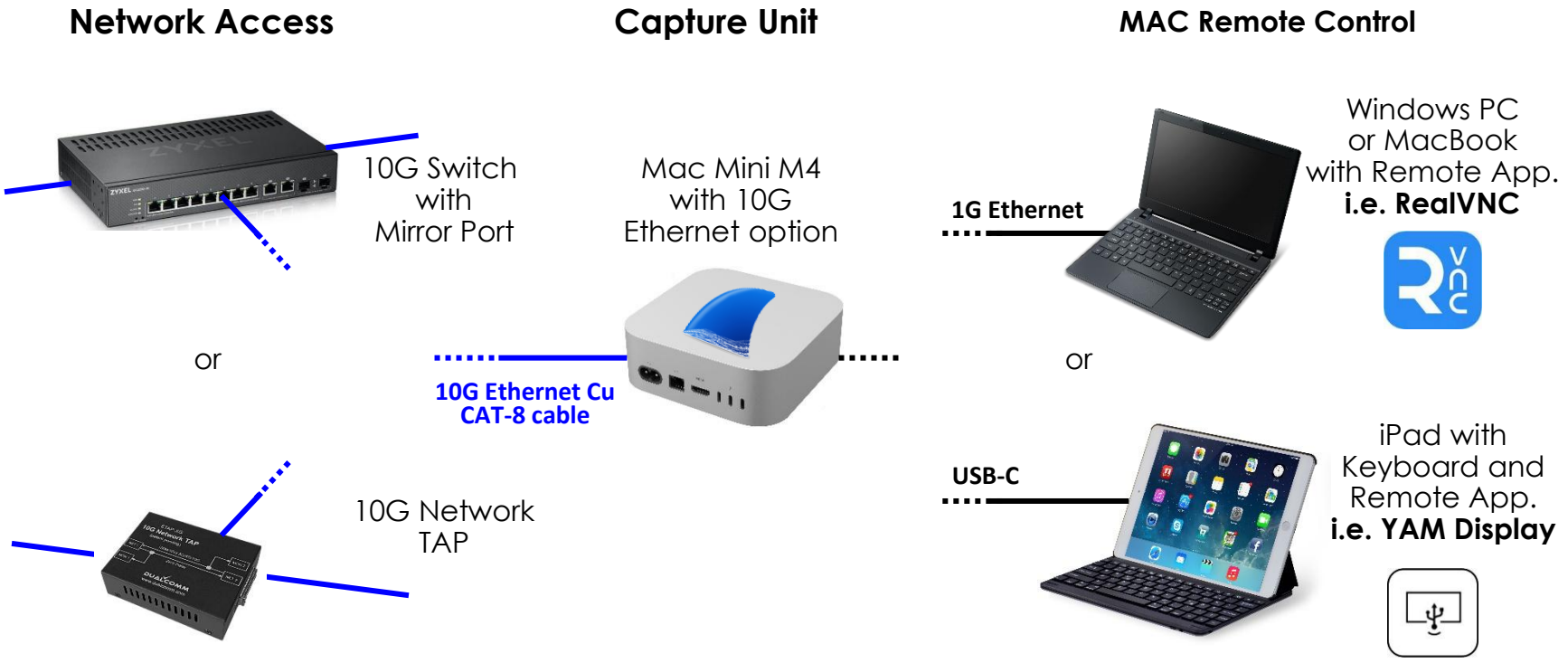




Tipps, Tricks & Traces

Kostengünstige, mobile 10 Gbit/s Aufzeichnungshardware

- Der Mac Mini braucht zur Bedienung externes Zubehör wie **Monitor, Keyboard und Maus**.
- Für eine portable Variante sind jedoch **möglichst wenig Zusatzgeräte** erwünscht.
- Ein **remote Zugriff** auf den Mac Mini von einem **MacBook** oder **Windows PC** ist dabei ideal.
- Eine andere Variante mit einem **iPad mit Keyboard** und USB-C Kabel ist ebenfalls möglich.
- In der Praxis würde der Mac Mini an den **Mirror Port eines Switches** oder an einen **10G TAP** angeschlossen.
- Mit entsprechenden Konvertern kann die Konfiguration auch für **10G Fiber** eingesetzt werden.



Tipps, Tricks & Traces

Kostengünstige, mobile 10 Gbit/s Aufzeichnungshardware

Zusammenfassung

- In der verwendeten Konfiguration zeigten die Aufzeichnungen **keinen Paketverlust** bei **vollem 10 Gbit Durchsatz**. Die guten gemessenen Resultate sind **nur ein Snapshot** in einer künstlich aufgebauten Umgebung, geben jedoch einen ersten Eindruck über die Leistungsfähigkeit des **Mac Mini als Capture Unit**.
- Kommerziell erhältliche 10G Capture Appliances bieten noch **zusätzliche Funktionen wie graphische Darstellungen/Statistiken und mehr.** Dies jedoch zu einem mindestens 5-fachen Preis gegenüber der Mac Mini Variante. Diese Kosten lassen sich bei nur gelegentlichem Gebrauch oft nicht rechtfertigen.
- Leider hatte ich bis jetzt noch keine Gelegenheit, diese Konfiguration mit dem Mac Mini in einem **Live-Netzwerk praktisch zu testen**. Ich werde dies jedoch beim nächsten Troubleshooting-Einsatz bei einem Kunden mit 10 Gigabit Netzwerk nachholen.
- Ein 10 Gigabit Netzwerk ist in der Regel so dimensioniert, dass eine volle Auslastung nur selten erreicht wird (und sonst müsste es auf 40 Gigabit aufgerüstet werden). Deshalb kann angenommen werden, dass die Mac Mini Variante auch in einem 10 Gigabit Live-Netzwerk gute Resultate liefern kann.
- Im Weiteren gilt es zu beachten, dass ein 10G Ethernet (wie auch 1G Ethernet) immer **Full-Duplex** unterstützt, d.h. der maximal nutzbare Durchsatz beträgt 10 Gbit pro Richtung, total also **20 Gbit/s**. Dies würde natürlich den Einsatzbereich des Mac Mini übersteigen.

Tipps, Tricks & Traces

Erstellen eines VXLAN Profils

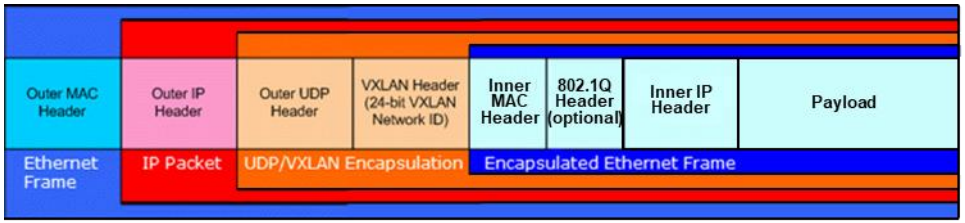
- Zahlreiche Protokolle sind **enkapsuliert**, ein Ethernet Frame wird zum Transport in ein **weiteres Protokoll gepackt**.
- Diese Pakete enthalten **mehrere MAC- und IP-Adressen**, die **des Original Frames** und die **des Tunnel-Protokolls.**
- Die Felder werden auch als **Innere** (Inner) **und Äussere** (Outer) **Header** bezeichnet.
- **Welche dieser Adressen zeigt nun Wireshark** beim Öffnen eines solchen Trace Files?
- Per Default zeigt **Wireshark die Adressen des Original Frames** (Inner Header), und nicht die des Tunnel-Protokolls.

→ Mit einem entsprechenden Profil, **lassen sich alle Adressfelder anzeigen.**

Encapsulated or Tunneled Protocols:

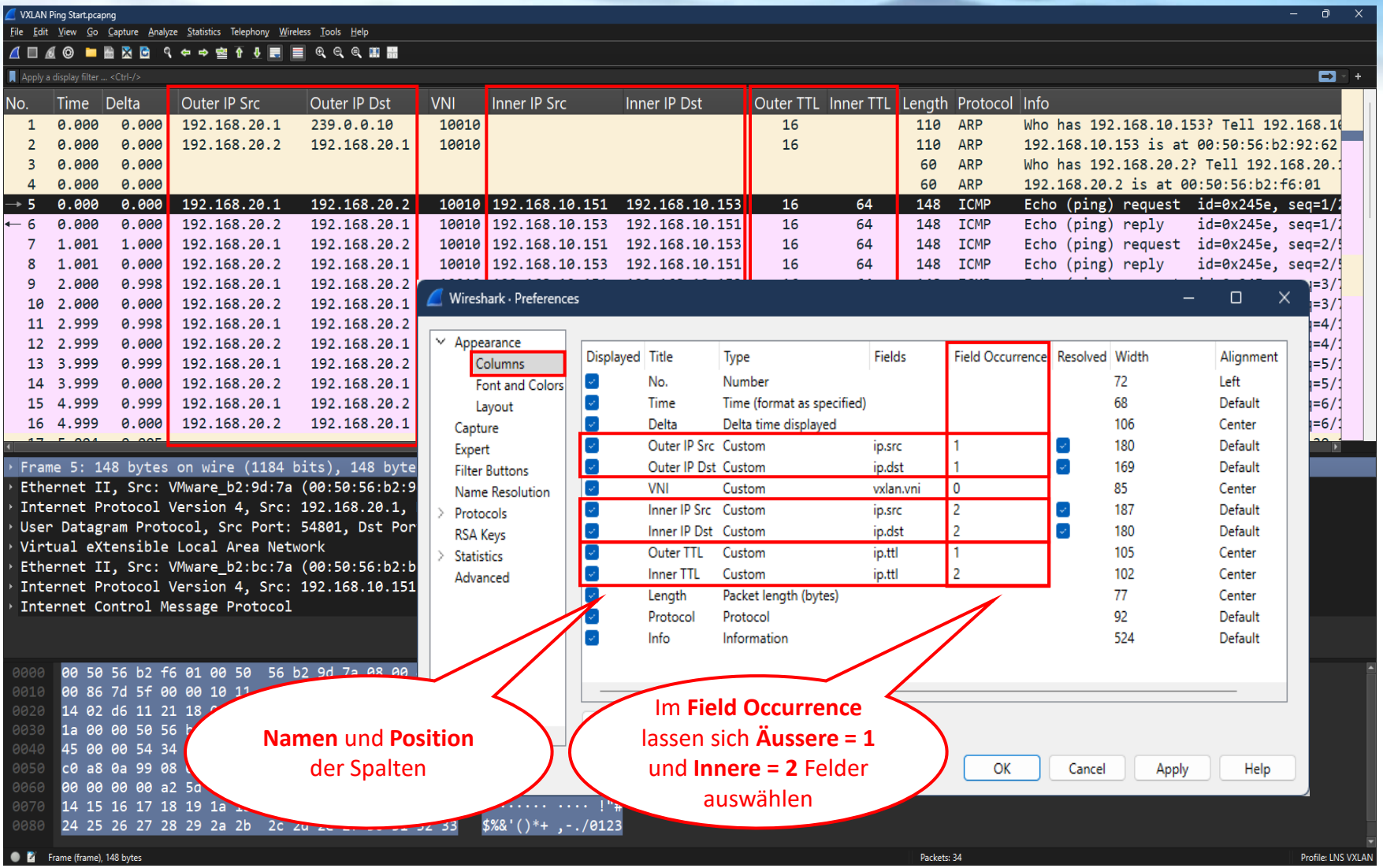
- **GRE tunnel** (Generic Routing Encapsulation)
- **CAPWAP tunnel** (Control And Provisioning of Wireless Access Points)
- **ICMP messages** (Internet Control Message Protocol)
- **IP in IP** (i.e., IPv4 in IPv6)
- **VPN** (Virtual Private Network)
- **VXLAN** (Virtual Extensible LAN)

VXLAN encapsulated frame with **Inner** and **Outer** MAC and IP headers



Tipps, Tricks & Traces

Erstellen eines VXLAN Profils



Tipps, Tricks & Traces

Diverses

Cool Commands

- Auf der Webseite von **AnyWeb Training** in Zürich werden ab **12. März 2025** kurze Video-Clips mit **Cool Commands** aufgeschaltet.
- Da werden auf kurze und prägnante Weise neue und praktische Befehle aus den Bereichen **Wireshark**, **Cisco**, **Python** und **Linux** erklärt.
- Den Termin notieren oder sich für den AnyWeb Training Newsletter **registrieren**.

The Packet Factor – neuer Wireshark Kurs zum Thema Network Security

- Mein langjähriger Kollege **Walter Hofstetter** ist Autor und Leiter dieses Kurses und eine Koryphäe auf dem Gebiet **Netzwerk-Analyse und -Security**.
- Der Kurs **The Packet Factor** zeigt, wie Wireshark im Bereich **Intrusion Detection and Prevention** auf Paketebene zur Erkennung von Netzwerk-Manipulationen und -Attacken eingesetzt werden kann.
- Es gibt in dieser Kombination und diesem Detaillierungsgrad aktuell **keinen vergleichbaren Kurs** auf dem Markt. Mehr Details und Anmeldung bei **AnyWeb Training** in Zürich

→ **Walter**, wann entwickeln wir den ersten **Stratoshark Kurs?**

Unsere Wireshark-Protokoll-Kurse & andere Events

- **PacketFest '25 in Zürich** **8.-9.05.2025** → Zur Anmeldung PacketFest '25
  Pädagogische Hochschule Zürich → **Garantierte Durchführung**

- **Öffentliche Kurse in der Schweiz**
  AnyWeb Training in Zürich → Zur Anmeldung bei AnyWeb
  TCP/IP Analyse mit Wireshark **11.-13.03.2025** → **Garantierte Durchführung**

  Studerus in Schwerzenbach → Zur Anmeldung bei Studerus
  VoIP Analyse mit Wireshark **20.03.2025**

- **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 öffentlichen Kurse** → Kurse Leutert NetServices

Unsere 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.

Hier unser Newsletter Archiv. Es würde uns freuen, Sie in einem unserer Kurse begrüssen zu können.

Have fun and enjoy sniffing, Rolf Leutert