WIRE**SHARK Newsletter Januar 2026**

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 4.6**
- **MACsec** Verschlüsselung auf Ethernet Layer
- **X.509 Zertifikate** exportieren

Tipps, Tricks & Traces:

- **PDF-Grafiken** direkt mit Wireshark erstellen
- Wireshark zeigt **überlange Frames**, wo keine sind

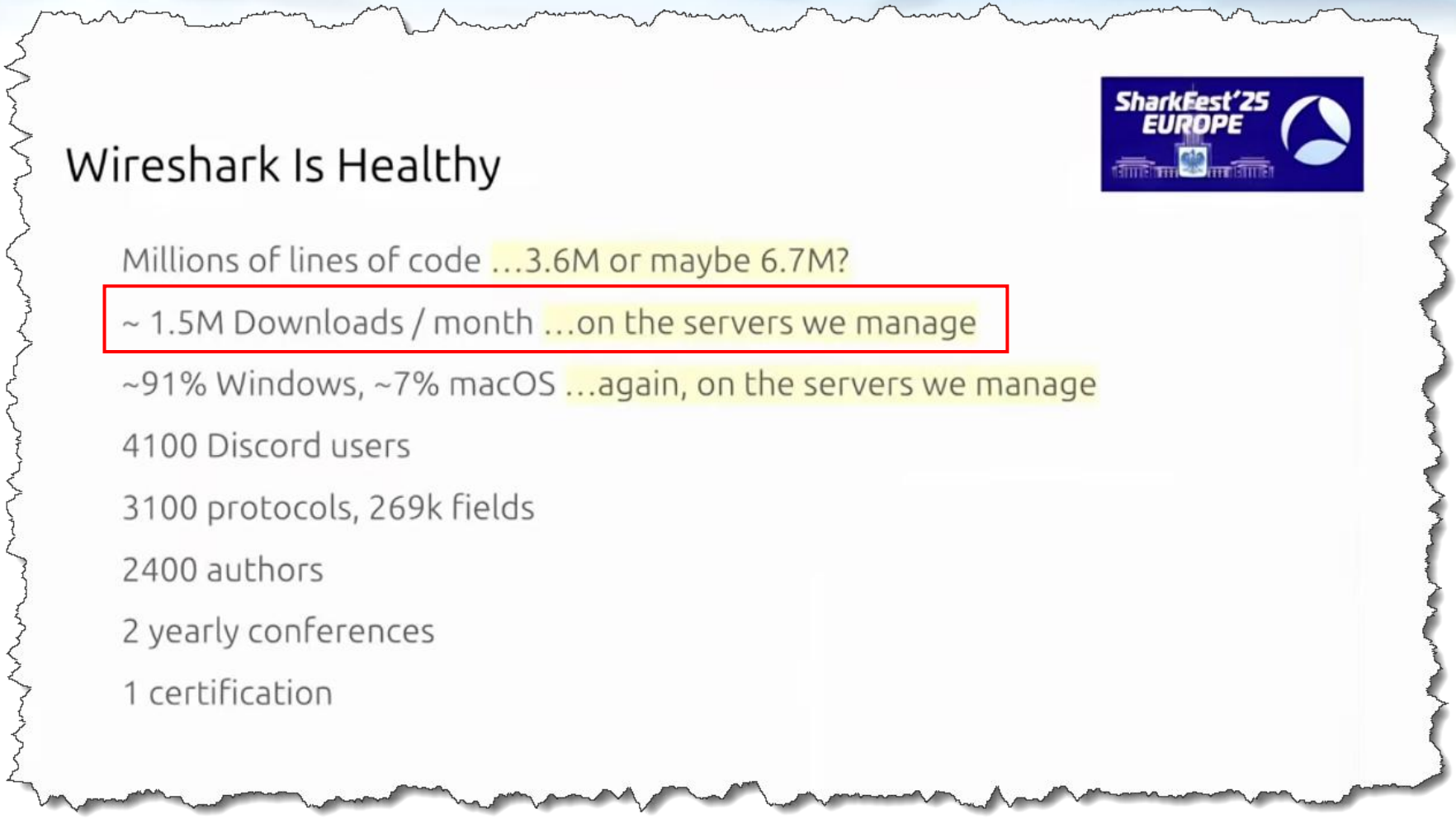
Kurse & Events:

- Aktuelle **Kursdaten** und andere **Wireshark Events**

Diese Schlagzeilen sind nur eine Auswahl; zahlreiche weitere Verbesserungen wurden vorgenommen.
Alle neuen 4.6 Funktionen auf https://www.wireshark.org/docs/relnotes/

Wireshark Update

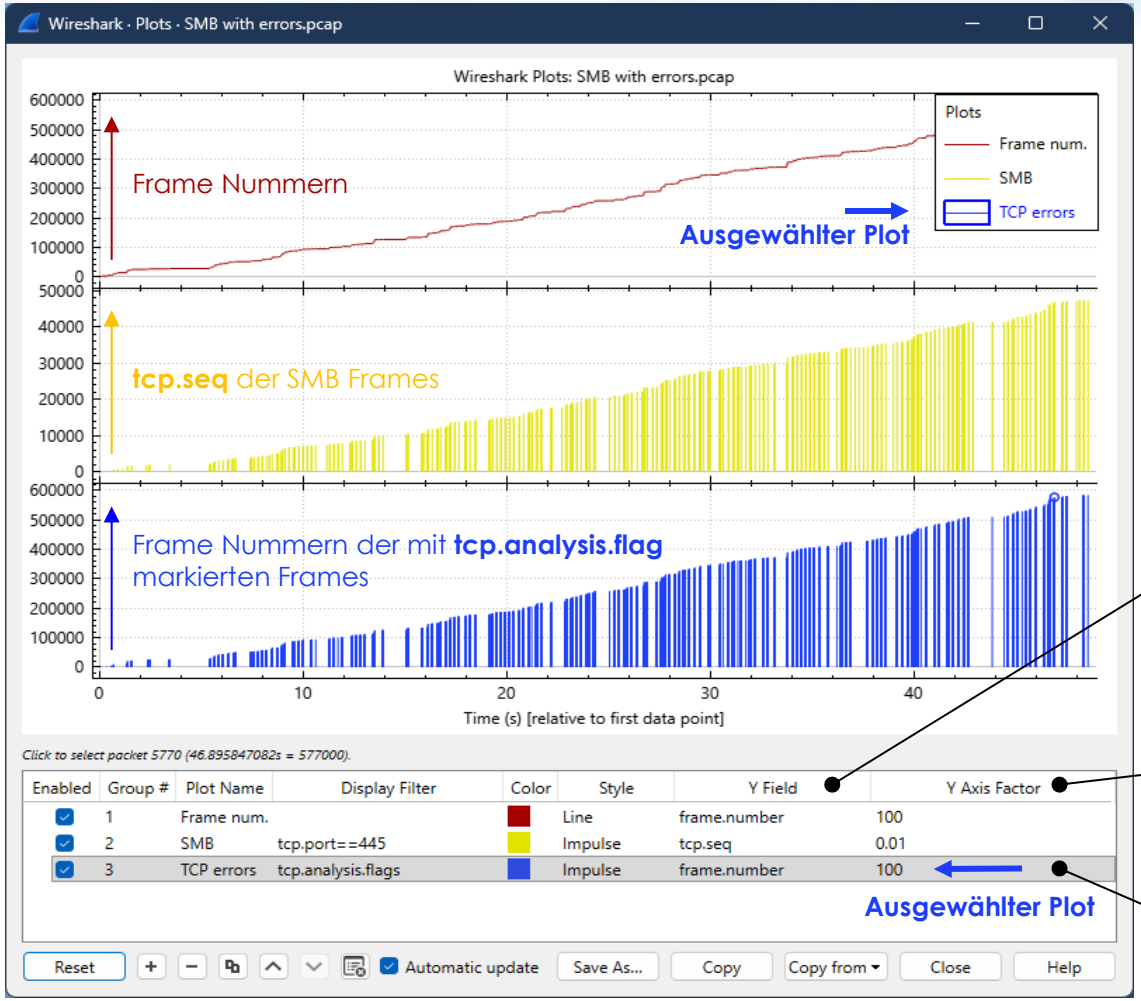
Immer wieder beeindruckend: **die Wireshark Statistik**



Quelle: Gerald Combs

Neue Plot Funktion

Trace File öffnen → Statistiken → Plots



- Die Funktion **Plots** zeigt den grafischen Verlauf beliebiger Werte.
- Jede Grafik zeigt den Wert des angegebenen Feldes (**Y-Feld)** zu jedem Zeitpunkt.
- Wenn man mit der Maus über das **→ ausgewählte Plot** fährt, werden die Paketnummern angezeigt.
- Ein **Links-Klick** auf eine Position führt zum entsprechenden Paket in der Wireshark-Paketliste.
- Ein rechter Mausklick in der Grafik zeigt die **Navigationshilfen.**

Y Field:

Parameter, der in der vertikalen Achse angezeigt werden soll.

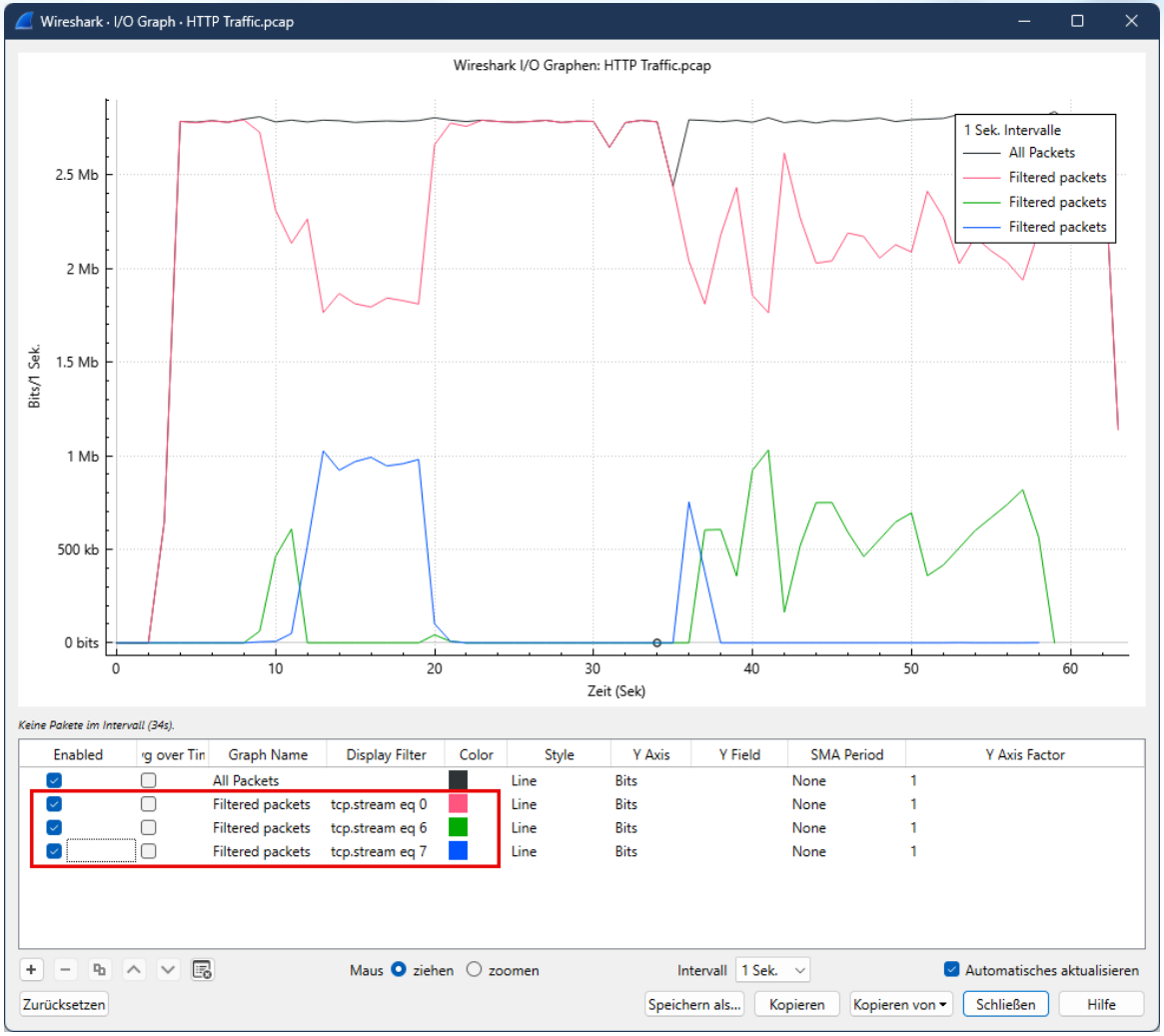
Y Axis Factor (Multiplikator):

100 → Graph Y Werte x 100
0.01 → Graph Y Werte x 0.01
100→ Graph Y Werte x 100
(Dient dazu, die Darstellung vertikal zu skalieren)

Der für die detaillierte Analyse **ausgewählte Plot**

Die I/O Graph Funktion

Trace File öffnen → Statistiken → I/O Graph



- Die nicht mehr neue, aber immer noch praktische Funktion **I/O Graph** zeigt den Bandbreitenanteil von frei definierbaren Grössen.
- Im Beispiel die Bandbreite eines **Links (2.8 Mbps)** und den **Anteil** der Datenraten der einzelnen **TCP-Streams.**

Die Navigation ist wie bei **Plots:**

- Wenn man mit der Maus über die Grafik fährt, wird die **Paketnummer** des ausgewählten Plots zu einem bestimmten Zeitpunkt angezeigt.
- Ein **Links-Klick** auf das Diagramm führt Sie zum entsprechenden Paket in der Wireshark-Paketliste.
- Ein rechter Mausklick in der Grafik zeigt die **Navigationshilfen.**

MACsec (Media Access Control Security)

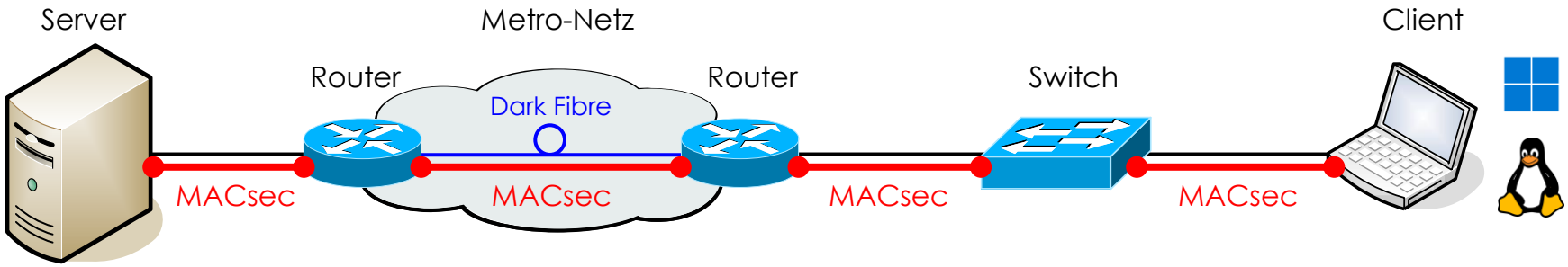
Gesicherte Übertragung auf der Routing- oder Applikationsschicht ist heute weit verbreitet **(IPsec, TLS)** und verhindert zuverlässig Bedrohungen wie Man-in-the-Middle-Angriffe, Mitschneiden von Datenpaketen und Replay-Angriffe.

Firmen-interne Übertragungen sind oft ungesichert und bieten Angriffsmöglichkeiten auf Ethernet Ebene, z.B. bei **Dark-Fibre über öffentlichen Grund** zum Verbinden von Campus-Netzwerken zu einem Metropolitan Area Network.

MACsec stellt auf Layer 2 (Ethernet Frame Layer) gesicherte Verbindungen zwischen **Routern, Switches und Endgeräten** her.

Im Gegensatz zu **IPSec** und **TLS** sind in einem **MACsec** Paket **alle Felder verschlüsselt**, d.h. auch Protokolle wie **DHCP, ARP, LLDP, NDP, VLAN, LACP.** Nur der **Ethernet Header** (MAC-Source, MAC-Destination, Ethertype) ist lesbar.

Der Anlass, warum **MACsec** als Thema in diesem Newsletter behandelt wird: dieses Protokoll kann ab **Wireshark Version 4.6 entschlüsselt werden**.



MACsec ist ein **Hop-by-Hop** Protokoll, d.h. die Daten werden **für jeden Link separat verschlüsselt**.

MACsec (Media Access Control Security)

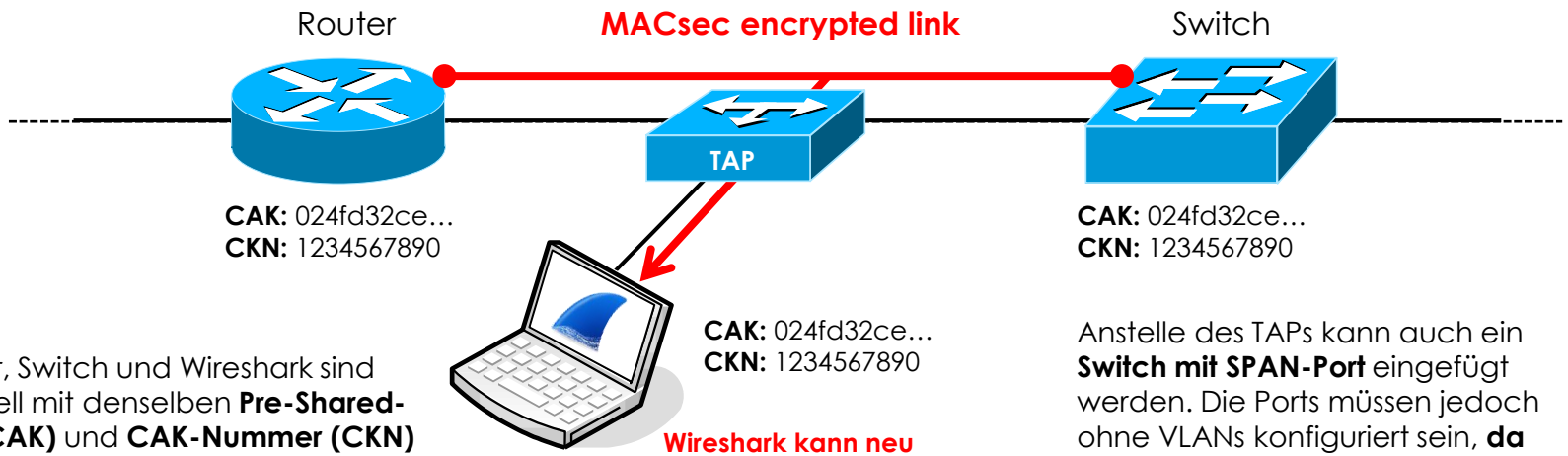
- **MACsec** ist mit **EAP IEEE 802.1X** (Radius-Protokoll) zur Authentifizierung kombinierbar und arbeitet unabhängig von Sicherheitsprotokollen höherer Ebenen wie **IPSec** oder **TLS**.
- **MACsec** ist kein neu definiertes Protokoll, der **Standard IEEE 802.1AE-2018** existiert schon länger.
- In jüngster Zeit wird **MACsec** jedoch vermehrt in **Routern, Switches** und auch auf **Endgeräten** verfügbar.

- Der Fokus liegt hier auf der **MACsec Konfiguration von Wireshark** und nicht auf Netz- und Endgeräten.
- Die **Einrichtung auf Netz- und Endgeräten** ist herstellerspezifisch; dazu sind im Internet viele Beiträge verfügbar.

→ Z.B. Netzwerkverschlüsselung mit MACsec zwischen Switch und Endgerät von Benjamin Pfister, 10 Nov. 2025

Wireshark bietet mit der neuen Funktion wertvolle Unterstützung bei der Implementierung von MACsec.

→ Zur Demonstration wird hier die einfachste **MACsec** Konfiguration nur mit **PSK** (ohne 802.1X) verwendet.

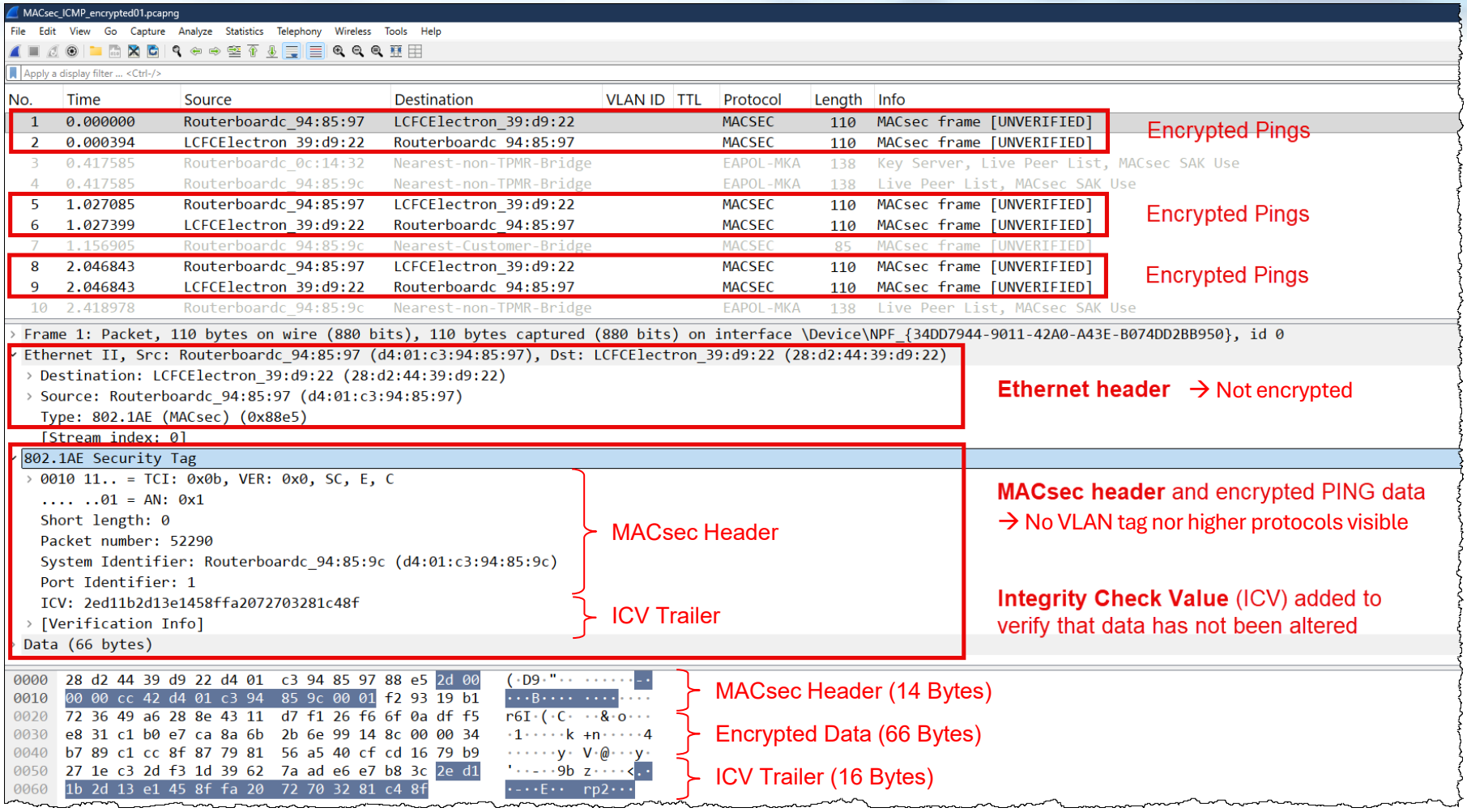


Router, Switch und Wireshark sind manuell mit denselben **Pre-Shared-Key (CAK)** und **CAK-Nummer (CKN)** konfiguriert.

Anstelle des TAPs kann auch ein **Switch mit SPAN-Port** eingefügt werden. Die Ports müssen jedoch ohne VLANs konfiguriert sein, **da MACsec auch den VLAN-Tag verschlüsselt.**

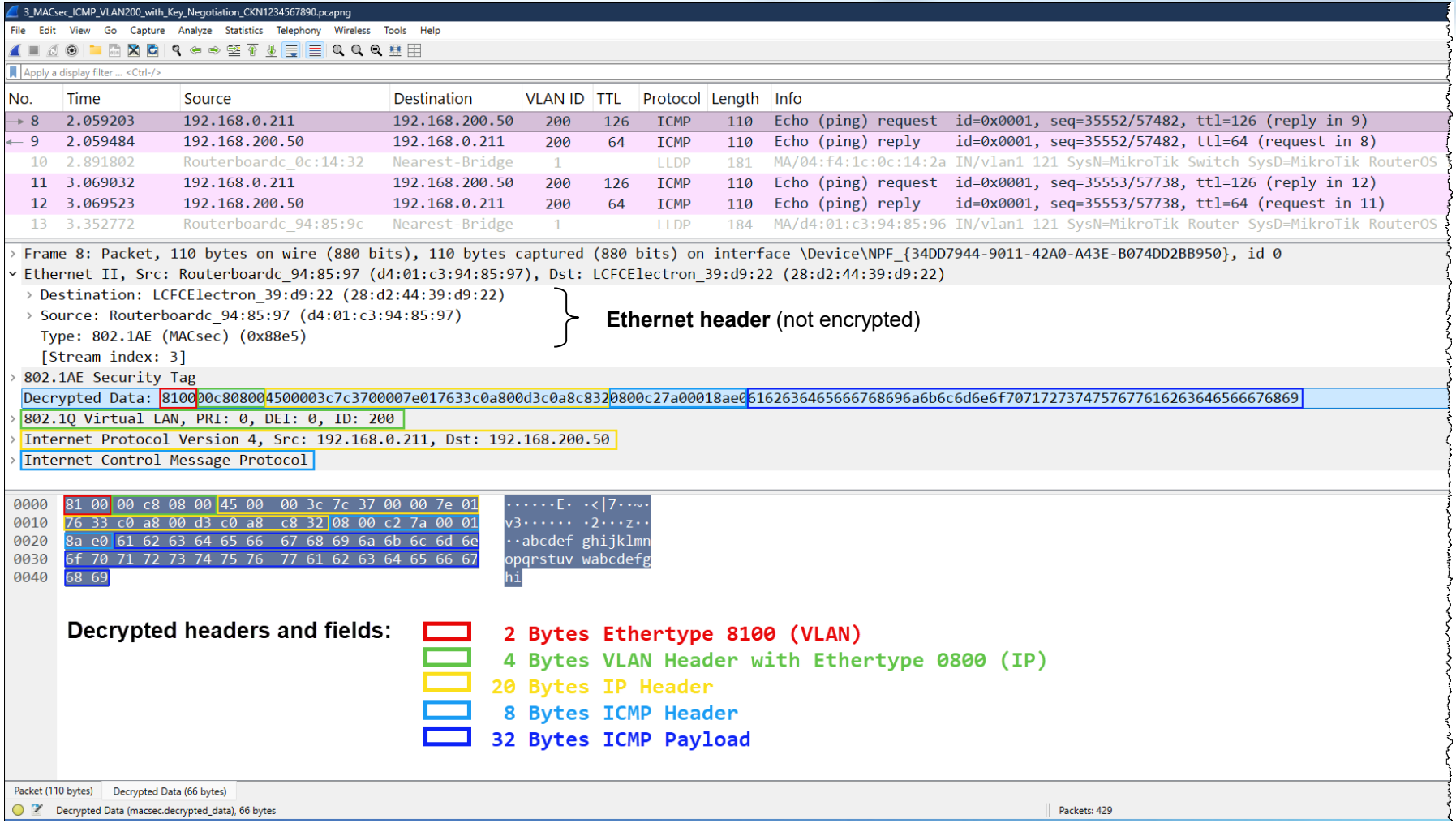
MACsec (Media Access Control Security)

MACsec encrypted frames



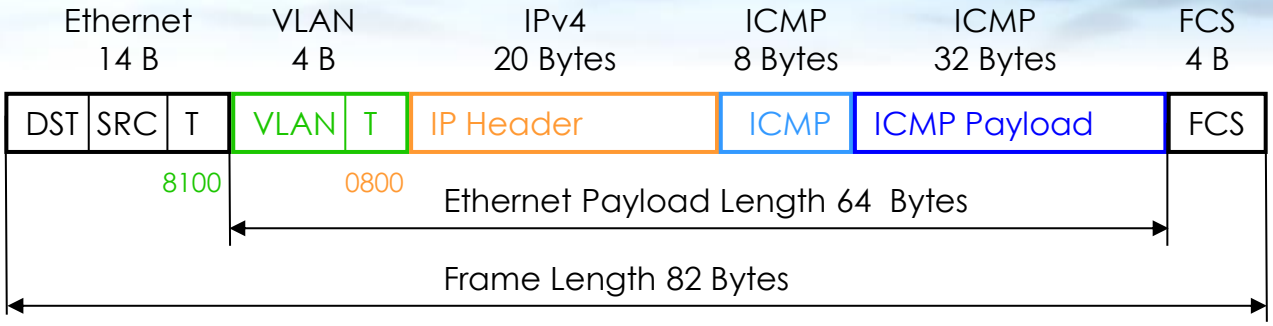
MACsec (Media Access Control Security)

MACsec frames decrypted with Wireshark



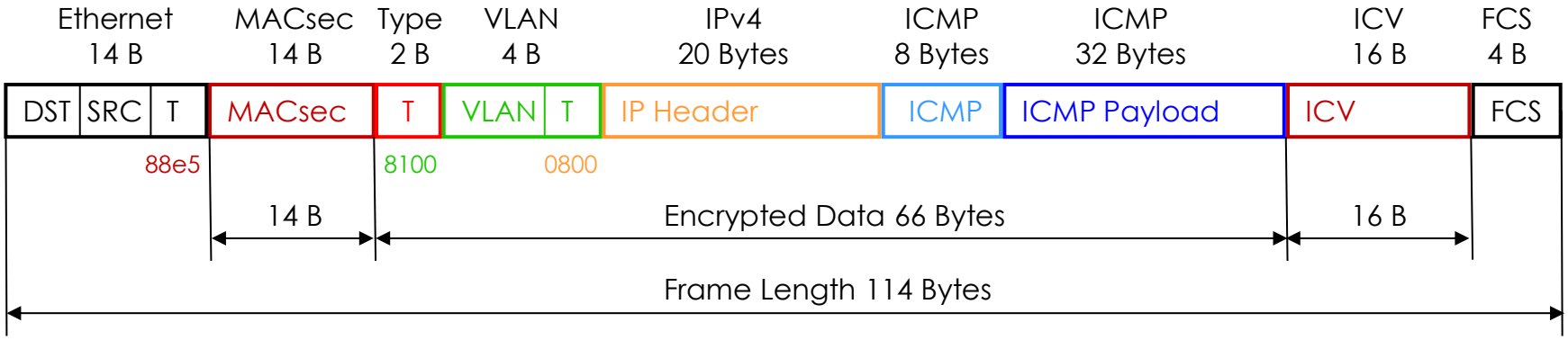
MACsec (Media Access Control Security)

MACsec frame format



Unencrypted Ping frame with VLAN tag

MACsec encrypted Ping frame with VLAN tag



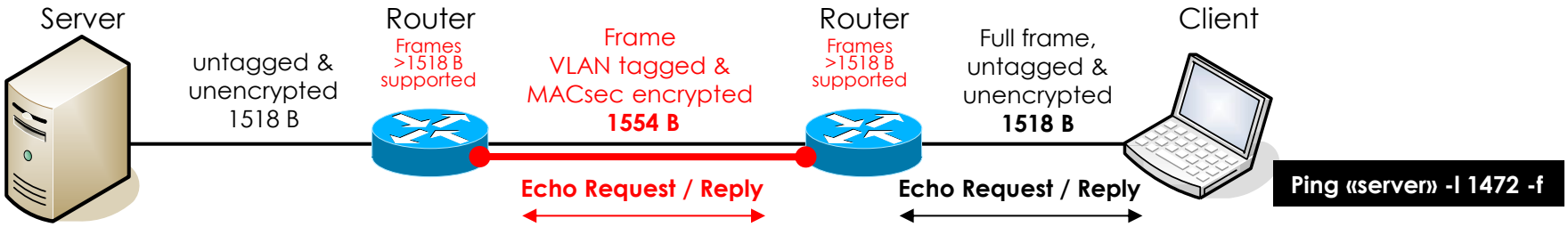
- **MACsec** verlängert Frames **ohne** VLAN-Tag um **30 Bytes**, Frames **mit** VLAN-Tag um **32 Bytes**
- Z.B. ein **Ping mit VLAN** wird durch die Verschlüsselung von **82 Bytes** auf **114 Bytes** vergrössert

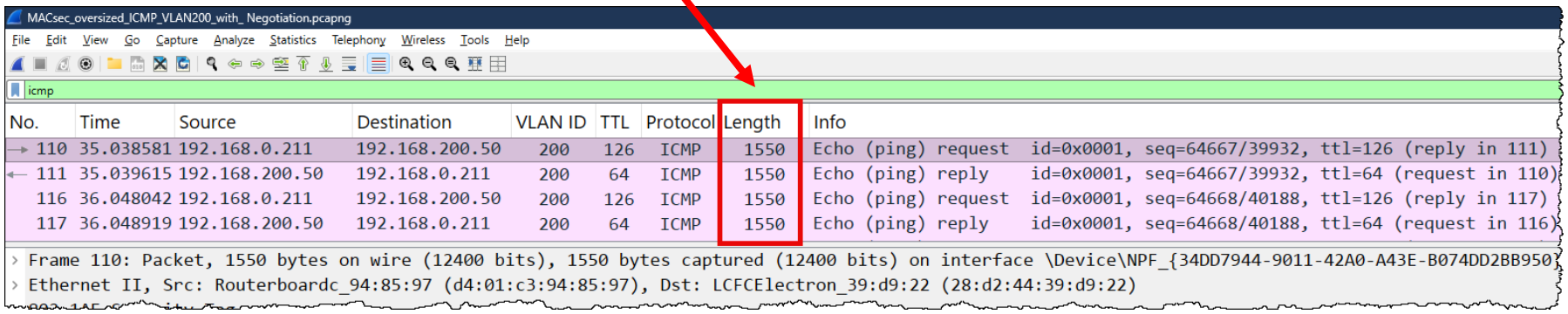
➢ Beachten: **Wireshark** zeigt die Frame Länge **ohne die 4 Bytes FCS** (das FCS-Feld wird oft von der NIC entfernt)

Frame Size vs. MTU

- **Maximum Transmission Unit** (MTU) und **Ethernet Frame Grösse** werden oft vermischt oder verwechselt.
- Die default **Ethernet MTU** (payload) ist **≤1500 Bytes.** Die Frame Länge ist **≤1518 B** (mit Ethernet Header und FCS)
- Protokolle wie **VLAN, VPN, GRE, VXLAN, CAPWAP, MACsec** usw. fügen zusätzliche Header den Frames hinzu.
- Frames **>1518 Bytes** können im Netz verworfen werden und zu schwierig einzugrenzenden Problemen führen.
- Mit den **PING-Optionen** kann die MTU einer Verbindung End-zu-End und ohne Fragmentierung getestet werden.
- Unter Windows generiert `ping 1.1.1.1 -l 1472 -f` einen **vollen Frame (1518 B)** und testet **Routing und MTU.**

MACsec addiert 30 - 36 Bytes und erzeugt (bei einem bereits vollen Frame) einen **überlangen Frame.**





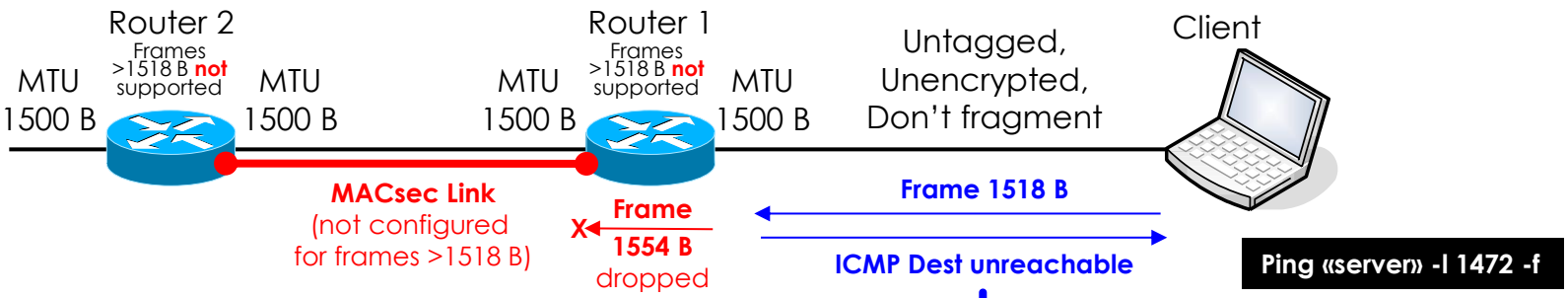
➢ Damit **Wireshark** Frames >1518 Bytes anzeigt, muss der Ethernet Adapter für **Jumbo Frames** konfiguriert sein.

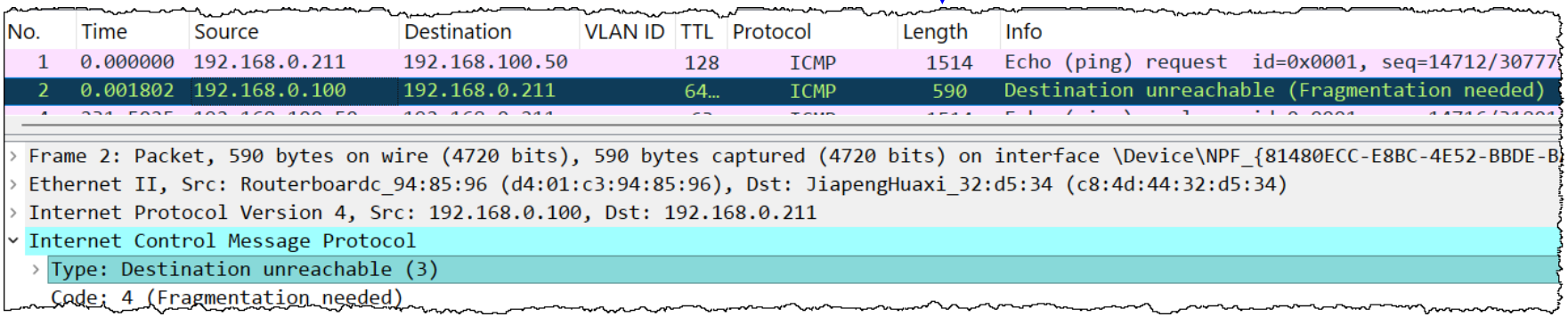
MACsec (Media Access Control Security)

Maximum Transmission Unit (MTU)

- Ist bei einem Router ein Frame grösser als die **MTU des Ausgangs-Links,** wird er den **Frame fragmentieren**.
- Bei einigen Protokollen (z.B. SMB) sind die Frames jedoch per default als **don't fragment** markiert.
- Ein zu grosser Frame wird dann verworfen und eine **ICMP** (Fragmentation needed) an den Sender geschickt.

Router 1 kann den **überlangen Frame** nicht weiterleiten und schickt eine ICMP an den Sender





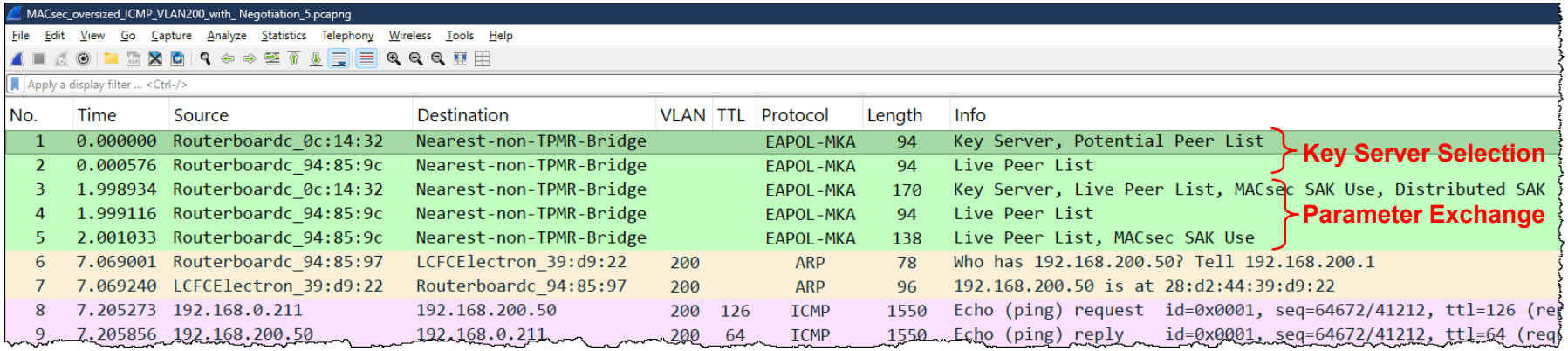
➢ Um diese Situation zu vermeiden, die **Frame Grösse** auf den **MACsec Interfaces** auf z.B. **1560 Bytes** erhöhen

MACsec (Media Access Control Security)

Initial Negotiation Process

- **MACsec ist ein Punkt-Punkt-Protokoll**; als erstes wird mit einem **Two-Way Handshake** der Key-Server festgelegt.
- Das Gerät mit der **tieferen MAC-Adresse** wird zum **Key-Server** und initiiert die nächste Phase.
- Der Key-Server berechnet mit dem **CAK** Wert und einer **zufälligen Zahl** den **Session-Key (SAK).**
- Danach werden im **Three-way Handshake** der **verschlüsselte Session Key** und andere Parameter ausgetauscht.

→ Mehr Details auf Frame level unter Cisco MKA, MACsec Key Agreement Exchange, on the wire



MACsec decrypted with Wireshark

→ Die Frames können entschlüsselt werden, wenn **Wireshark** mit den **CAK / CKN** Werten konfiguriert ist **und die 5 Frames beim MACsec Aufbau** mitaufgezeichnet werden.

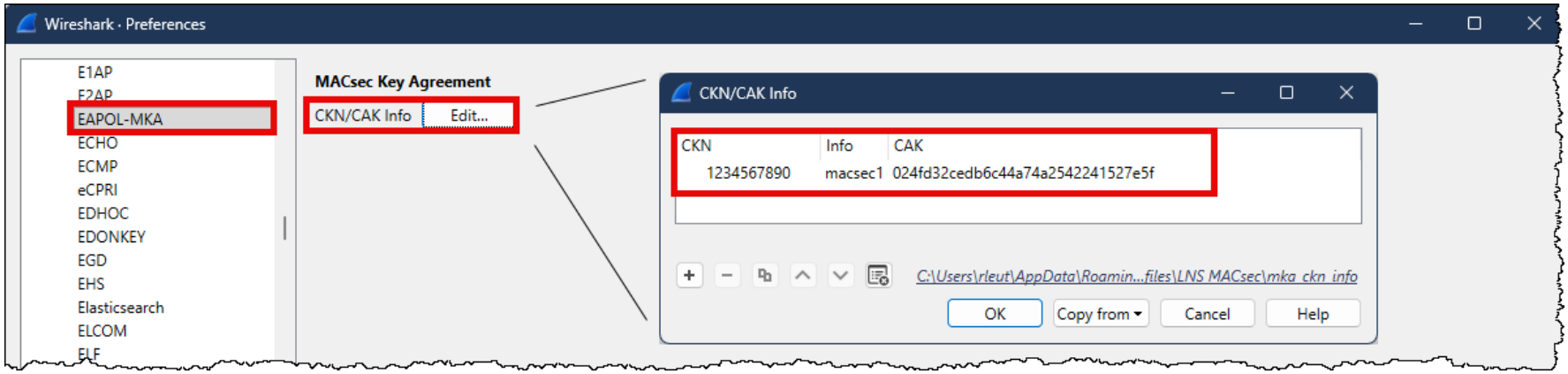
CAK	Connectivity Association Key (PSK) (must be 32 or 64 Hex digits and the same on both devices (and Wireshark)
CKN	CAK Name (must be an even number of Hex digits and the same on both devices (and Wireshark)
EAPOL	Extensible Authentication Protocol over LAN
MKA	MACsec Key Agreement (EAPOL extension for MACsec)
SAK	Secure Association Key (Session key derived from the CAK and used to encrypt data sent between devices)

MACsec (Media Access Control Security)

Wireshark MACsec Configuration

→ Edit → Preferences → Protocols → **MACsec**

→ Edit → Preferences → Protocols → **EAPOL-MKA**



Mit obigen Einstellungen kann Wireshark MACsec Frames entschlüsseln.

X.509 Zertifikat exportieren

- Das **Zertifikat** ist ein wichtiger Bestandteil von aktuellen Verschlüsselungen (HTTPS).
- Es enthält u.a. den **Public Key, Herausgeber, Digitale Signatur** usw. und wird von **TCP/TLS (und QUIC)** u.a. für die Authentisierung des Zielservers verwendet.
- **Diese Protokolle** gelten (mit langen Schlüsseln) aktuell allgemein als **unknackbar**.
- D.h. es gibt **keine Möglichkeit,** zwischen Client und Server aufgezeichnete Daten **innerhalb eines verwertbaren Zeitraumes** zu entschlüsseln.
- Für die Netzwerk-Fehlereingrenzung mit Wireshark genügen jedoch in den meisten Fällen die **unverschlüsselten TCP-Layer-Informationen** (QUIC verwendet jedoch UDP).
- Für **Applikations-Entwicklung und -Fehlersuche** wären jedoch **entschlüsselte HTTP-Daten** von Vorteil.
- Die **Entschlüsselung von TLS mit Wireshark** ist nur möglich, wenn ein **Zugriff auf den Client** besteht.
- Der Browser auf dem Client kann so konfiguriert werden, dass der **Session-Key in eine Datei gespeichert** wird.

➢ **Wird diese Datei in Wireshark importiert, können die Daten entschlüsselt werden** (Anleitungen auf YouTube).

No.	Time	Source	Destination	Server Name	TTL	Protocol	Length	Info
1	0.000000	HP-EliteBook-840	www.netsniffing.ch		128	TCP	66	50358 → 443 [SYN] Seq=275952904 Win=64240 Le
2	0.006402	www.netsniffing.ch	HP-EliteBook-840		54	TCP	66	443 → 50358 [SYN, ACK] Seq=3296870161 Ack=27
3	0.006484	HP-EliteBook-840	www.netsniffing.ch		128	TCP	54	50358 → 443 [ACK] Seq=275952905 Ack=32968701
4	0.009104	HP-EliteBook-840	www.netsniffing.ch	www.netsniffing.ch	128	TLSv1.3	571	Client Hello (SNI=www.netsniffing.ch)
5	0.015032	www.netsniffing.ch	HP-EliteBook-840		54	TCP	60	443 → 50358 [ACK] Seq=3296870162 Ack=2759534
6	0.015137	www.netsniffing.ch	HP-EliteBook-840		54	TLSv1.3	1514	Server Hello, Change Cipher Spec, Encrypted
7	0.015137	www.netsniffing.ch	HP-EliteBook-840		54	TCP	1514	443 → 50358 [ACK] Seq=3296871622 Ack=2759534
8	0.015137	www.netsniffing.ch	HP-EliteBook-840		54	TCP	1230	443 → 50358 [PSH, ACK] Seq=3296873082 Ack=27
9	0.015184	HP-EliteBook-840	www.netsniffing.ch		128	TCP	54	50358 → 443 [ACK] Seq=275953422 Ack=329687425
10	0.017140	www.netsniffing.ch	HP-EliteBook-840		54	TLSv1.3	909	Certificate, Certificate Verify, Finished
11	0.017191	HP-EliteBook-840	www.netsniffing.ch		128	TCP	54	50358 → 443 [ACK] Seq=275953422 Ack=329687517
12	0.193761	HP-EliteBook-840	www.netsniffing.ch		128	TLSv1.3	118	Change Cipher Spec, Finished
13	0.194308	HP-EliteBook-840	www.netsniffing.ch		128	HTTP2	224	Magic, SETTINGS[0], WINDOW_UPDATE[0], PRIORI
14	0.194379	HP-EliteBook-840	www.netsniffing.ch		128	HTTP2	483	HEADERS[15]: GET /de/, WINDOW_UPDATE[15]
15	0.199703	www.netsniffing.ch	HP-EliteBook-840		54	TCP	60	443 → 50358 [ACK] Seq=3296875113 Ack=2759540

Mit Wireshark entschlüsselte HTTP-Daten

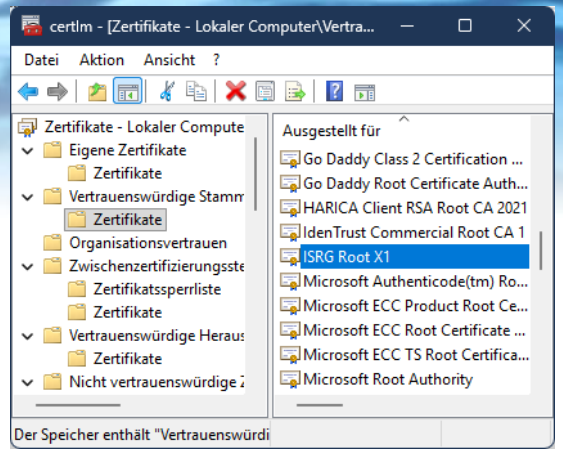
X.509 Zertifikat exportieren

➢ Was ist der Nutzen, X.509 Zertifikate exportieren zu können?

- Beim **TLS-Handshake** schickt der Server **sein X.509 Zertifikat** an den Client.
- Es enthält **keine geheimen Informationen**, muss aber verifiziert werden.
- Ein **Client mit Browser** kann die Echtheit des Server-Zertifikats mit Hilfe der lokalen **Certificates List** überprüfen und es annehmen oder ablehnen.

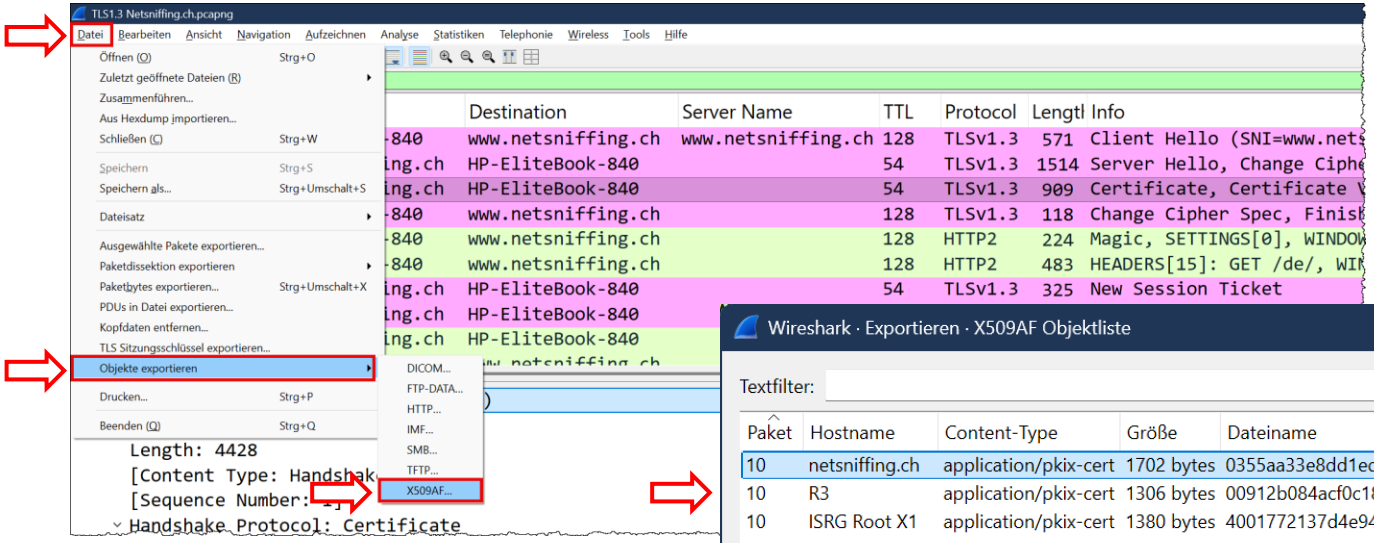
➢ Bei Clients **ohne Certificates List** (Firewalls, Drucker, IoT-Geräte usw.) muss ein Zertifikat **manuell importiert werden**.

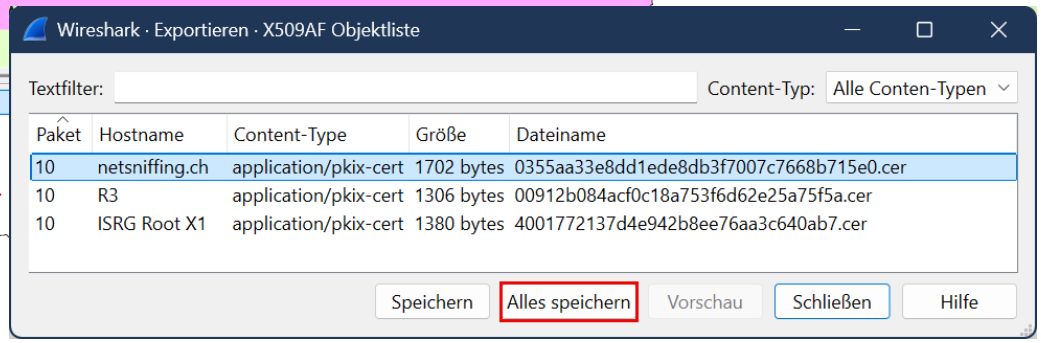
- Die **X.509 Zertifikate** haben das Format **.cer, .crt oder .pem**



Windows → Run: certlm.msc

➢ Von Wireshark exportierte X.509 Zertifikate können auf andere Geräte übertragen werden.





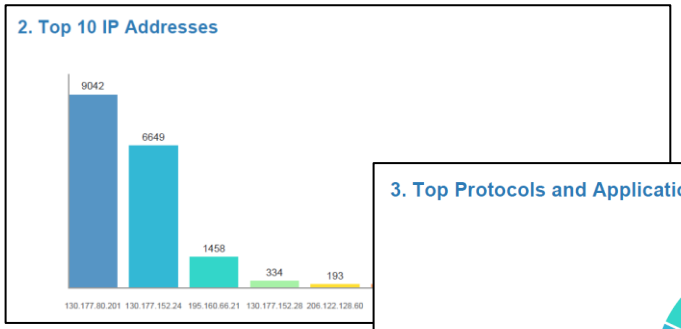
Anmerkung:
Ab TLS1.3 sind Zertifikate auch verschlüsselt, d.h. ohne Session-Key vom Client nicht sichtbar und nicht exportierbar!

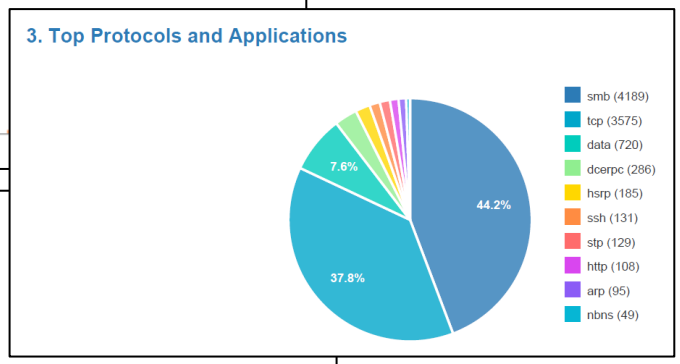
Tipps, Tricks & Traces

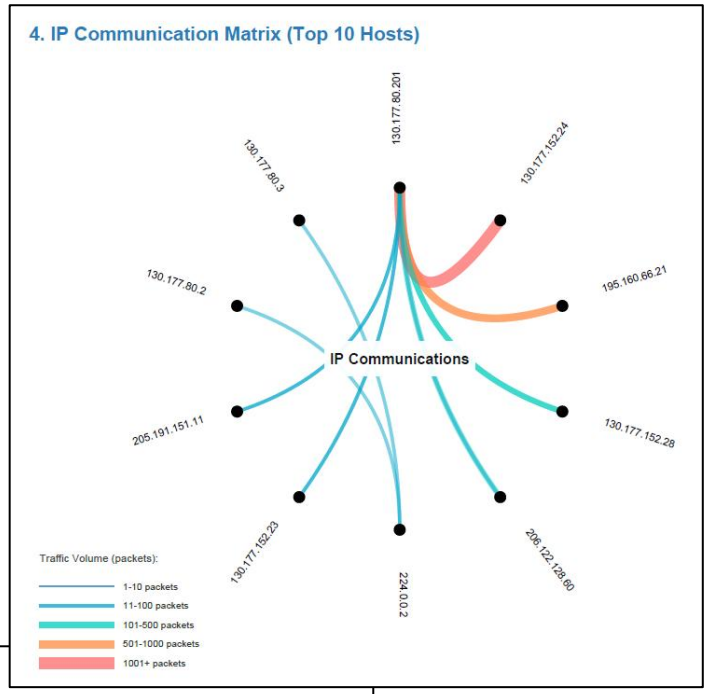
PacketReporter: PDF-Grafiken direkt mit Wireshark erstellen

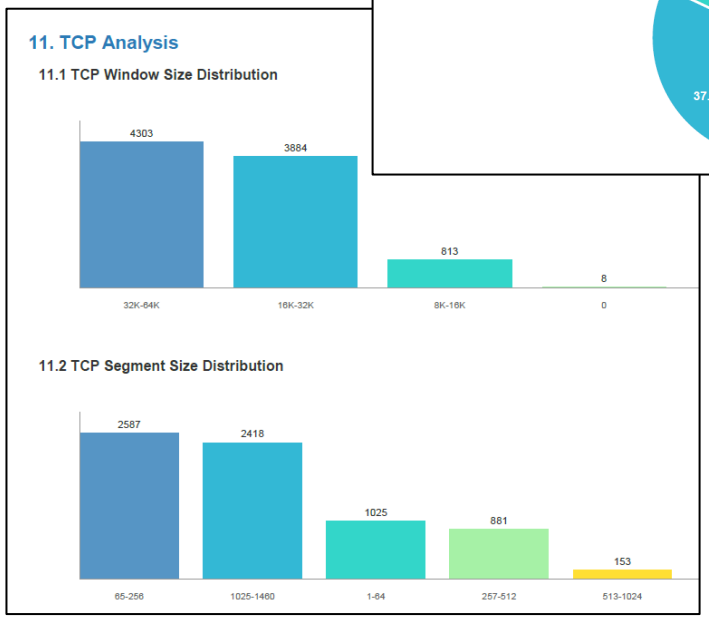
- Mein Wireshark Buddy Walter Hofstetter hat mit LUA Script eine nützliche Erweiterung erstellt.
- Von einem Trace File lassen sich rund ein Dutzend Grafiken direkt in ein PDF-File exportieren.

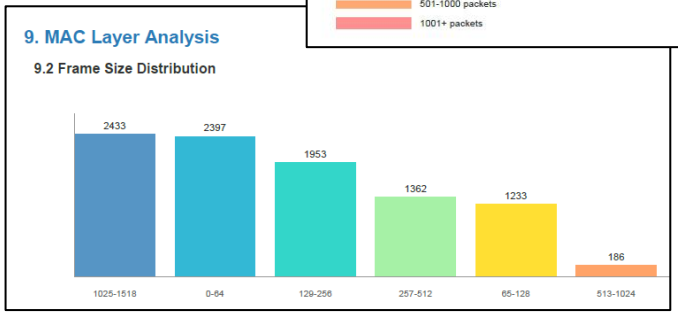
Einige Beispiele







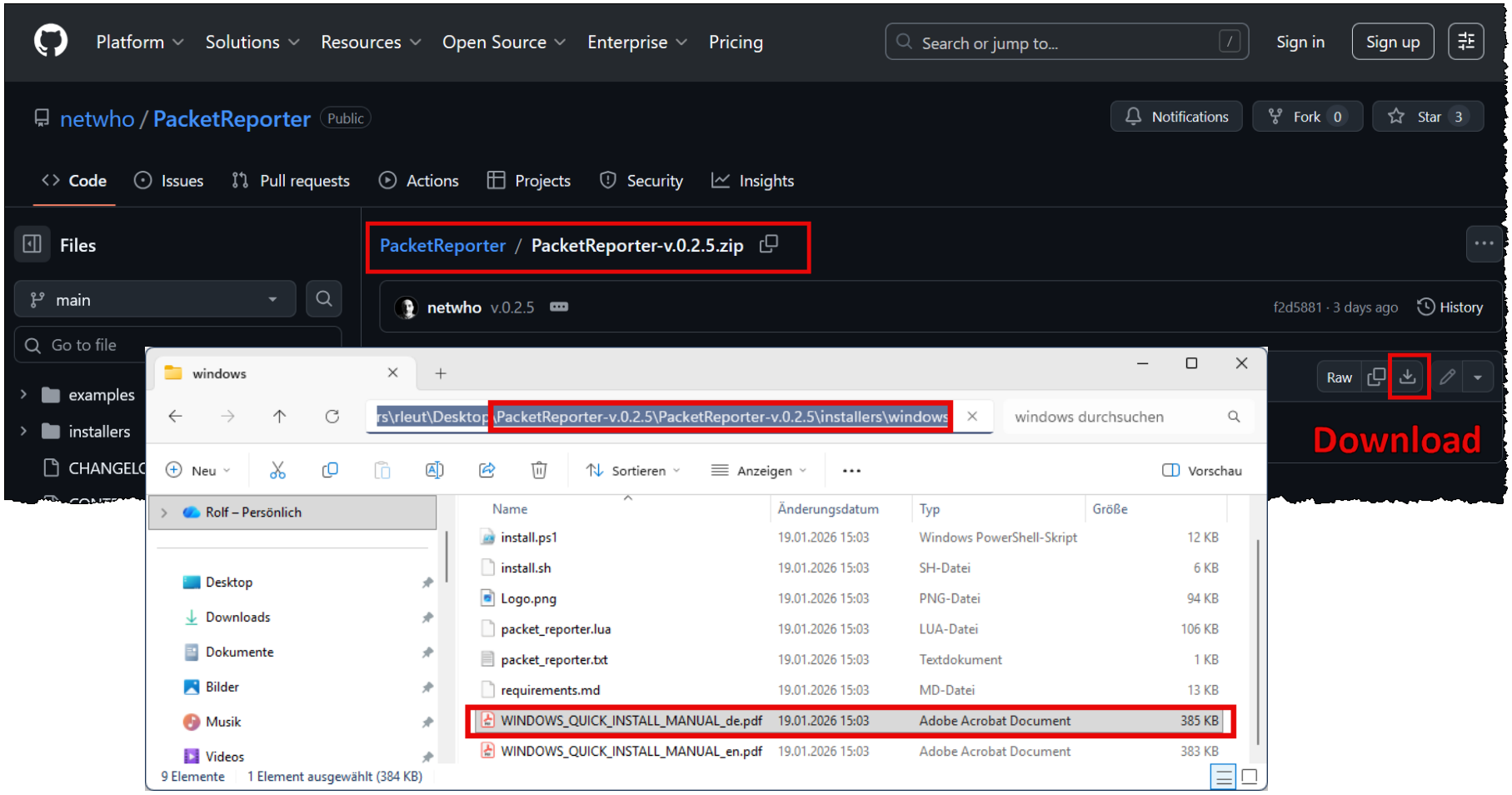




Tipps, Tricks & Traces

PDF-Grafiken direkt mit Wireshark erstellen

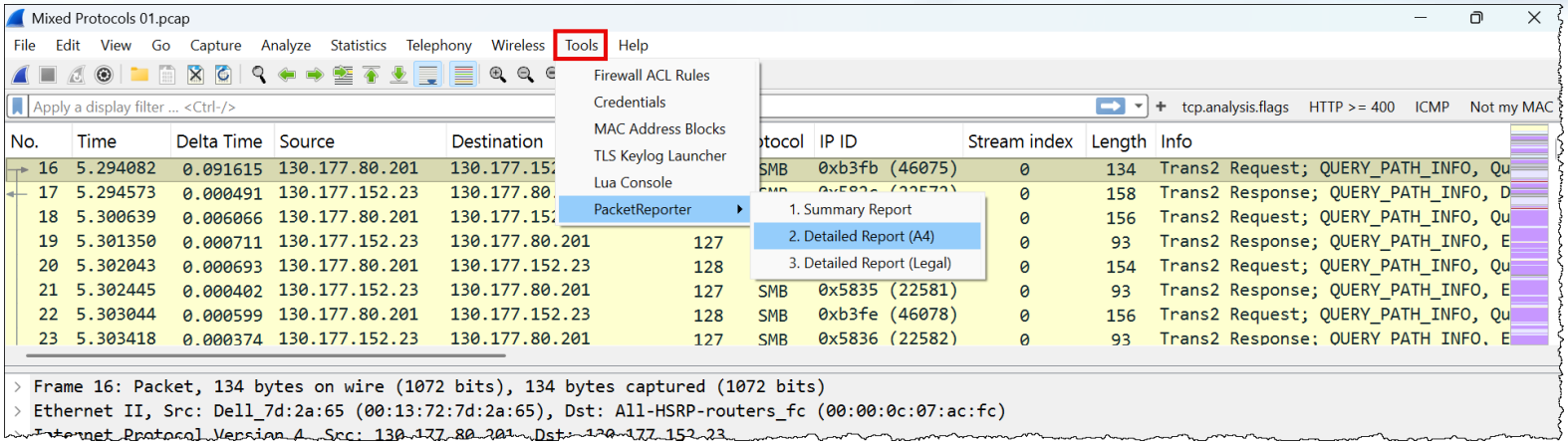
- **PacketReporter** und Installationsanleitungen für **Windows/MAC/Linux** sind auf **GitHub** verfügbar.



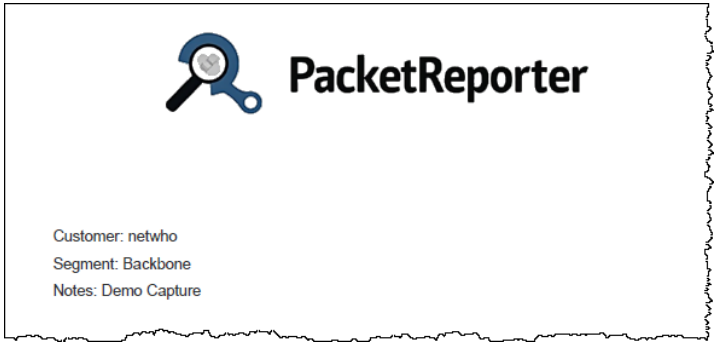
Tipps, Tricks & Traces

PDF-Grafiken direkt mit Wireshark erstellen

- Unter Tools einen **Reporttyp** wählen, dann im Pop-up Fenster **Export PDF** Knopf betätigen.



- Unter **%USERPROFILE%\.packet_reporter** können Report-Logo und -Text geändert werden



Default **Report-Logo** und -**Text**

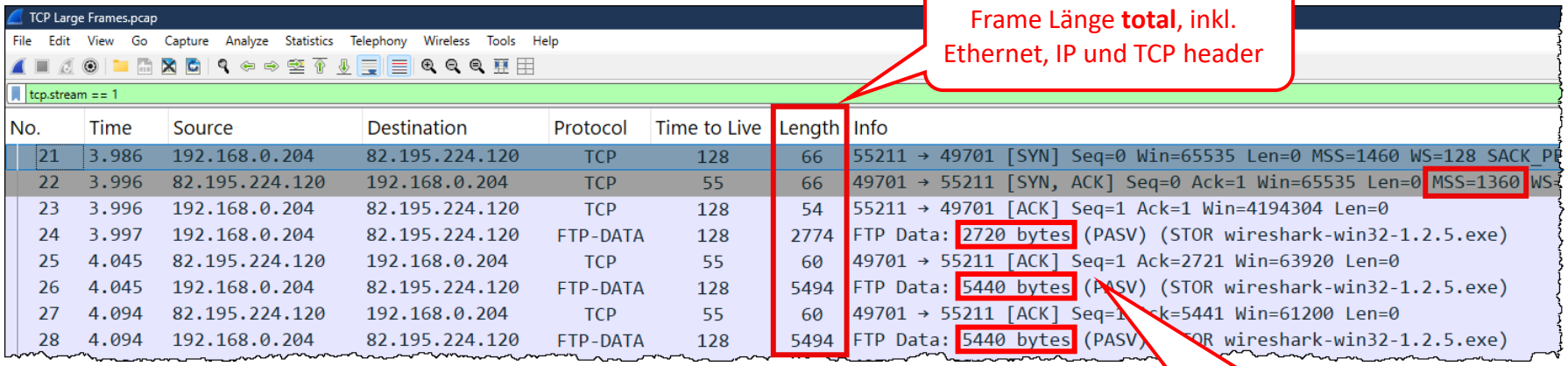
➢ Für Anregungen oder Unterstützung direkt walter.hofstetter@netwho.ch kontaktieren.

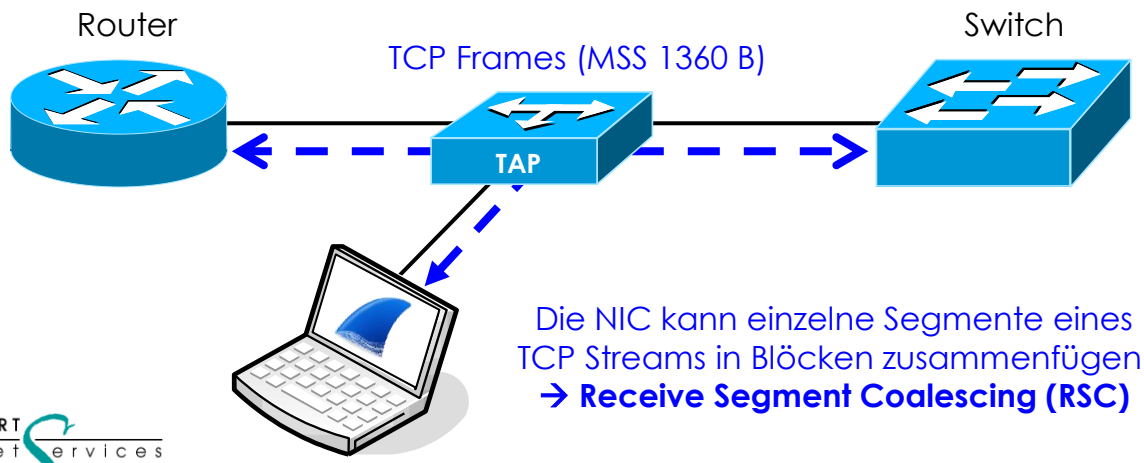
Tipps, Tricks & Traces

Wireshark zeigt überlange Frames, wo keine sind!

- Wireshark Aufzeichnungen direkt **auf dem Sender oder Empfänger** eines TCP Streams sind **nicht empfohlen**.
- Wireshark zeigt dann oft **grosse Frame Längen**, obschon die **TCP-MSS** z.B. mit **≤1360 B** ausgehandelt wurde.
- Immer öfter tritt dieser Effekt jedoch auch beim Aufzeichnen an einem **TAP** oder **SPAN-Port** auf.

→ **Grund:** Aktuelle NICs unterstützen **das Zusammenfügen** von empfangenen **TCP-Segmenten zu Datenblöcken**.





Die NIC kann einzelne Segmente eines TCP Streams in Blöcken zusammenfügen.
→ **Receive Segment Coalescing (RSC)**

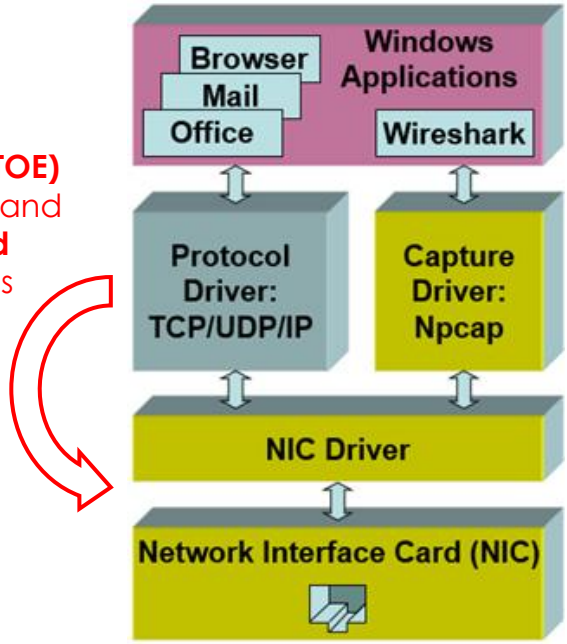
Tipps, Tricks & Traces

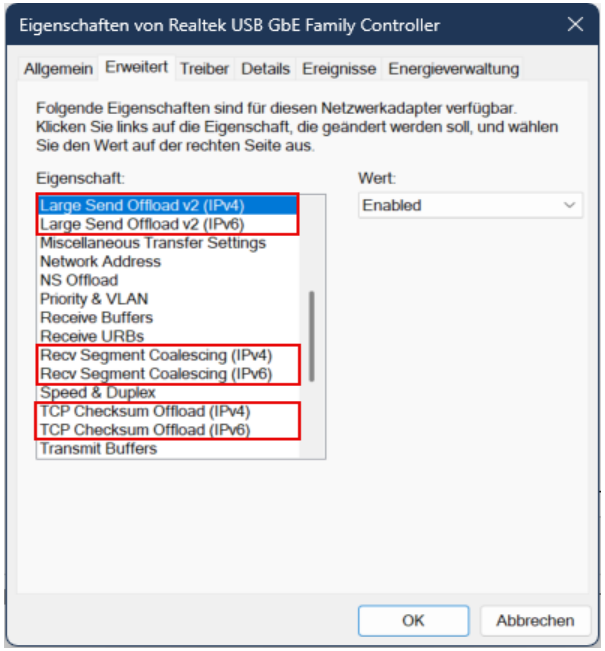
Wireshark zeigt überlange Frames, wo keine sind!

- Um die CPU zu entlasten, werden vermehrt rechenintensive Prozesse an den **Ethernet-Adapter (NIC) ausgelagert**.
- Die NIC **fragmentiert TCP-Blöcke** (beim Senden) und **fügt TCP-Segmente in Blöcken zusammen** (beim Empfangen)
- Der **Npcap Driver** erhält die Daten in **Block-Form**, d.h. **vor dem Fragmentieren** und **nach dem Zusammenfügen.**
- **Wireshark** zeigt deshalb die Grösse der **TCP-Daten-Blöcke** und nicht die wahre Frame-Grösse auf dem Ethernet.
- Werden diese **TOE-Funktionen** ausgeschaltet, kann dies die CPU-Leistung bei normalem Gebrauch beeinflussen.

➢ **Empfehlung:**
- Die TOE-Parameter bei der **NIC für den normalen PC-Gebrauch nicht verändern.**
- Zum Aufzeichnen mit Wireshark eine **zweite NIC** (z.B. einen **USB Ethernet Dongle**) verwenden, und **nur da** die TOE-Funktionen ausschalten.

TCP Offload Engine (TOE)
NICs take over more and more sending **and** receiving functions





Unsere Wireshark-Protokoll-Kurse & andere Events

Öffentliche Kurse in der Schweiz

AnyWeb Training in Zürich **TCP/IP-Analyse mit Wireshark** Vorbereitung	**4.-6. Mai 2026**	→ Zur Anmeldung bei AnyWeb
AnyWeb Training in Zürich **WLAN-Netzwerkanalyse mit Wireshark**	**02.-03. Feb. 2026**	→ Zur Anmeldung bei AnyWeb ✓ **Garantierte Durchführung**
Studerus in Schwerzenbach **VoIP-Analyse mit Wireshark**	**02. Juni 2026**	→ Zur Anmeldung bei Studerus

Öffentliche Kurse in Österreich

Bei Arrow ECS GmbH in Wien	**Diverse Daten**	→ Zur Anmeldung bei ARROW

Öffentliche Kurse in Deutschland

Remote Kurse bei ALSO Deutschland	**Diverse Daten**	→ Zur Anmeldung bei ALSO

SharkFest'26 US	Nashville, Tennessee	**18. - 23. Juli 2026**	https://sharkfest.wireshark.org/sfus/
SharkFest'26 Europe	Brüssel, Belgien	**2. - 6. Nov. 2026**	https://sharkfest.wireshark.org/sfeu/

Gerne senden wir Ihnen ein Angebot für einen **Firmenkurs** oder eine **Tech-Session** zu den Themen:

Einführung Netzwerkanalyse, Wireshark Tipps & Tricks, TCP/IP, QUIC, WLAN, VoIP und IPv6

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

Have fun and enjoy sniffing! Rolf Leutert. Unser Newsletter Archiv.