

# WIRESHARK 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**



### Wireshark Is Healthy

Millions of lines of code ...3.6M or maybe 6.7M?

~ 1.5M Downloads / month ...on the servers we manage

~91% Windows, ~7% macOS ...again, on the servers we manage

4100 Discord users

3100 protocols, 269k fields

2400 authors

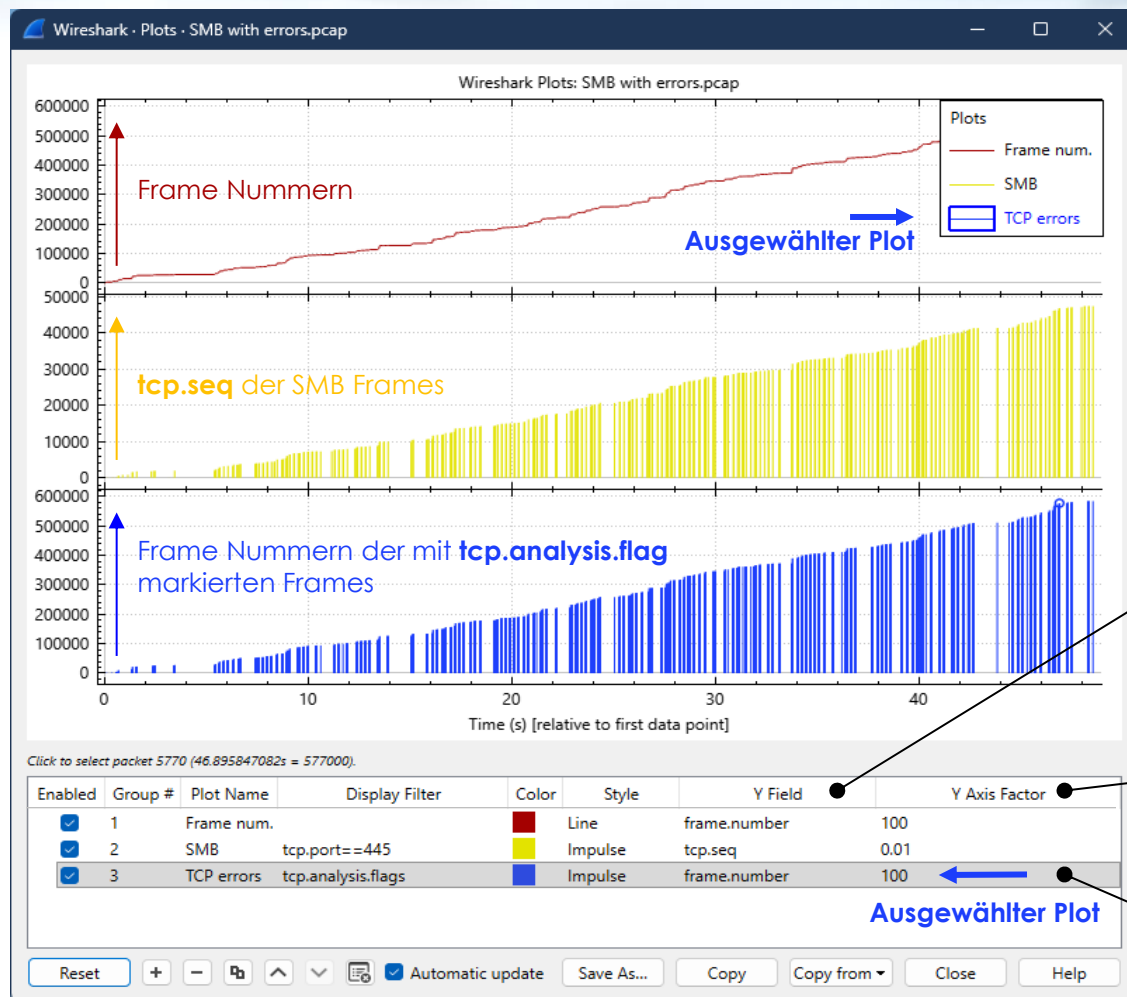
2 yearly conferences

1 certification

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.

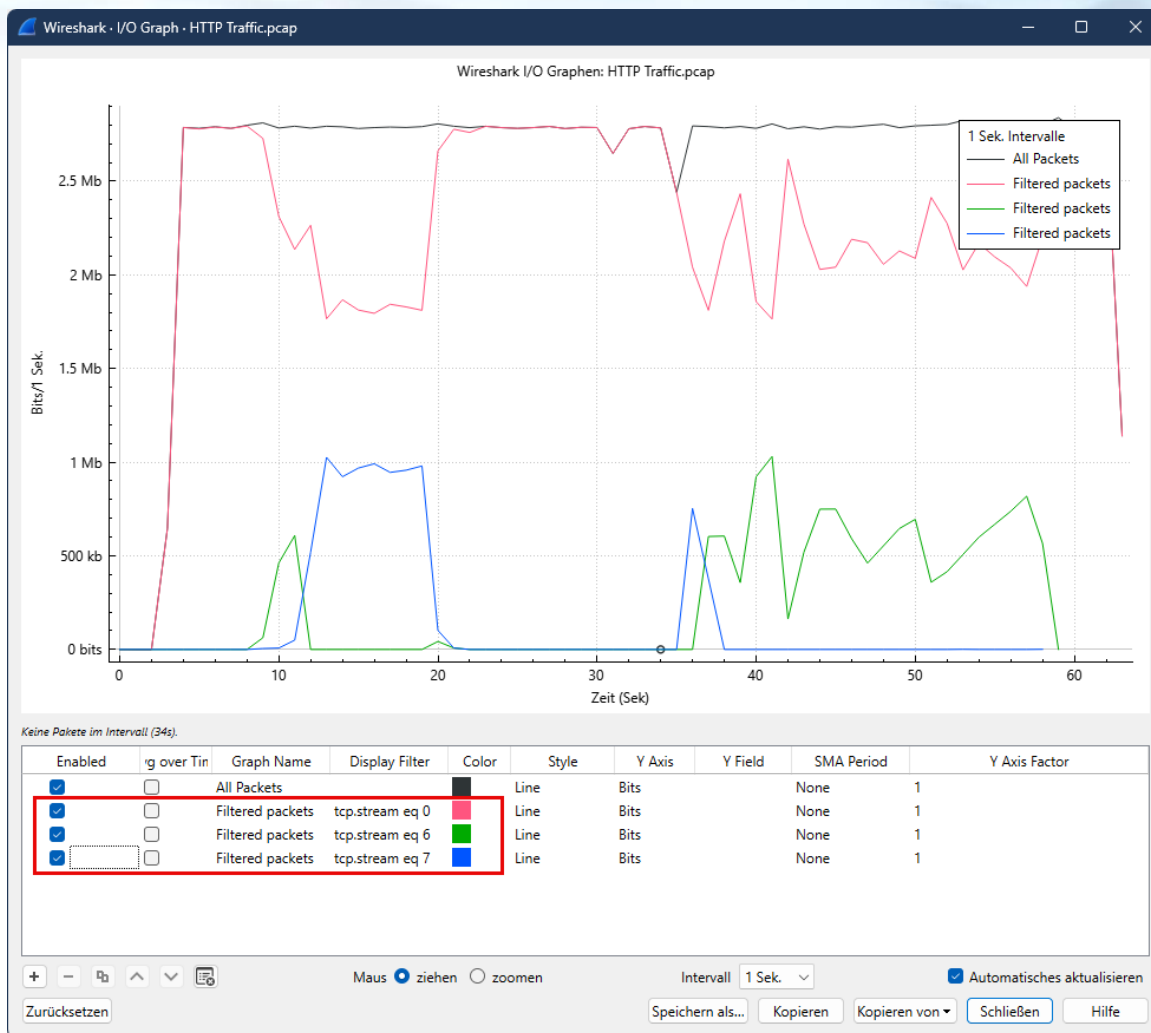
## Y Axis Factor (Multiplikator):

**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.

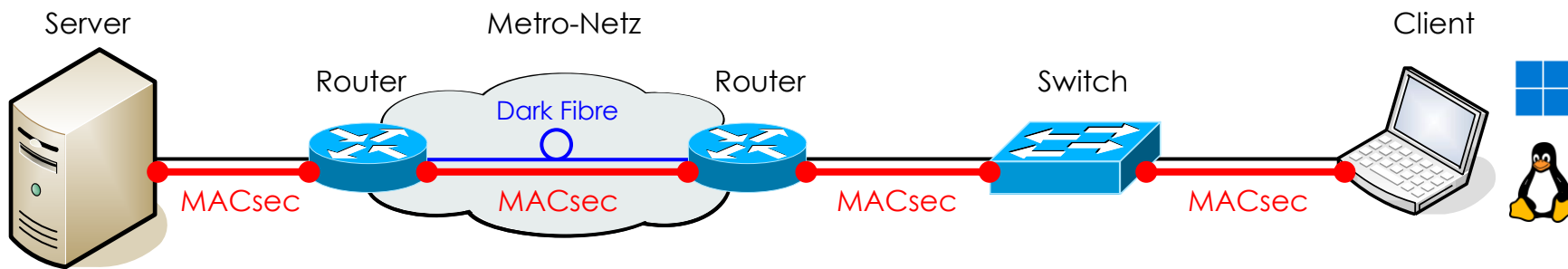
Firmen-interne Übertragungen sind oft ungesichert und bieten Angriffsmöglichkeiten auf Ethernet Ebene, z.B. bei **Dark-Fibre über öffentlichen Grund** zum Verbinden von Campus-Netzwerken zu einem Metropolitan Area Network.

**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**.



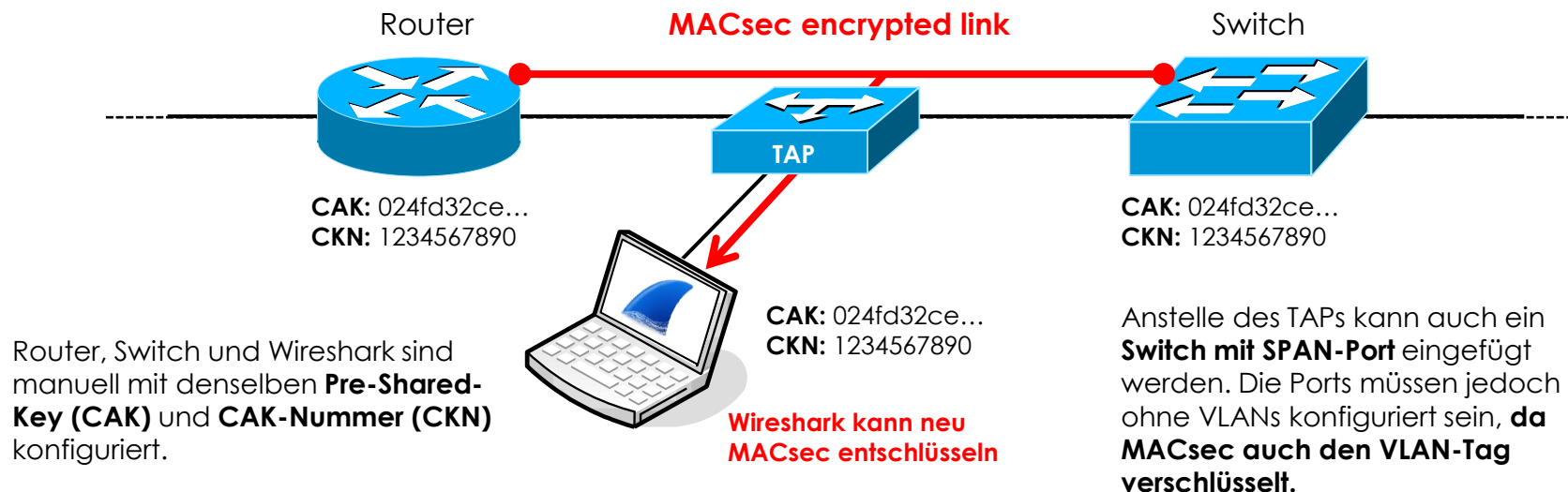
**MACsec** ist ein **Hop-by-Hop** Protokoll, d.h. die Daten werden **für jeden Link separat verschlüsselt**.

# 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.



# MACsec (Media Access Control Security)

## MACsec encrypted frames

MACsec\_ICMP\_encrypted01.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	VLAN ID	TTL	Protocol	Length	Info
1	0.000000	Routerboardc_94:85:97	LCFCElectron_39:d9:22			MACSEC	110	MACsec frame [UNVERIFIED]
2	0.000394	LCFCElectron_39:d9:22	Routerboardc_94:85:97			MACSEC	110	MACsec frame [UNVERIFIED]
3	0.417585	Routerboardc_0c:14:32	Nearest-non-TPMR-Bridge			EAPOL-MKA	138	Key Server, Live Peer List, MACsec SAK Use
4	0.417585	Routerboardc_94:85:9c	Nearest-non-TPMR-Bridge			EAPOL-MKA	138	Live Peer List, MACsec SAK Use
5	1.027085	Routerboardc_94:85:97	LCFCElectron_39:d9:22			MACSEC	110	MACsec frame [UNVERIFIED]
6	1.027399	LCFCElectron_39:d9:22	Routerboardc_94:85:97			MACSEC	110	MACsec frame [UNVERIFIED]
7	1.156905	Routerboardc_94:85:9c	Nearest-Customer-Bridge			MACSEC	85	MACsec frame [UNVERIFIED]
8	2.046843	Routerboardc_94:85:97	LCFCElectron_39:d9:22			MACSEC	110	MACsec frame [UNVERIFIED]
9	2.046843	LCFCElectron_39:d9:22	Routerboardc_94:85:97			MACSEC	110	MACsec frame [UNVERIFIED]
10	2.418978	Routerboardc_94:85:9c	Nearest-non-TPMR-Bridge			EAPOL-MKA	138	Live Peer List, MACsec SAK Use

> Frame 1: Packet, 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF\_{34DD7944-9011-42A0-A43E-B074DD2B8950}, id 0

Ethernet II, Src: Routerboardc\_94:85:97 (d4:01:c3:94:85:97), Dst: LCFCElectron\_39:d9:22 (28:d2:44:39:d9:22)

> Destination: LCFCElectron\_39:d9:22 (28:d2:44:39:d9:22)

> Source: Routerboardc\_94:85:97 (d4:01:c3:94:85:97)

Type: 802.1AE (MACsec) (0x88e5)

[Stream index: 0]

802.1AE Security Tag

> 0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C

.... 01 = AN: 0x1

Short length: 0

Packet number: 52290

System Identifier: Routerboardc\_94:85:9c (d4:01:c3:94:85:9c)

Port Identifier: 1

ICV: 2ed11b2d13e1458ffa2072703281c48f

> [Verification Info]

Data (66 bytes)

MACsec Header

ICV Trailer

Ethernet header → Not encrypted

MACsec header and encrypted PING data  
→ No VLAN tag nor higher protocols visible

Integrity Check Value (ICV) added to  
verify that data has not been altered

0000	28 d2 44 39 d9 22 d4 01 c3 94 85 97 88 e5 2d 00	(.D9:".. .....
0010	00 00 cc 42 d4 01 c3 94 85 9c 00 01 f2 93 19 b1	...B.... .....
0020	72 36 49 a6 28 8e 43 11 d7 f1 26 f6 6f 0a df f5	r6I.(.C. .&.o...
0030	e8 31 c1 b0 e7 ca 8a 6b 2b 6e 99 14 8c 00 00 34	.1.....k +n.....4
0040	b7 89 c1 cc 8f 87 79 81 56 a5 40 cf cd 16 79 b9	.....y. V.@...y.
0050	27 1e c3 2d f3 1d 39 62 7a ad e6 e7 b8 3c 2e d1	'.....9b z.....<..
0060	1b 2d 13 e1 45 8f fa 20 72 70 32 81 c4 8f	...E... rp2...

MACsec Header (14 Bytes)

Encrypted Data (66 Bytes)

ICV Trailer (16 Bytes)

# MACsec (Media Access Control Security)

## MACsec frames decrypted with Wireshark

3\_MACsec\_ICMP\_VLAN200\_with\_Key\_Negotiation\_CKN1234567890.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	VLAN ID	TTL	Protocol	Length	Info
→ 8	2.059203	192.168.0.211	192.168.200.50	200	126	ICMP	110	Echo (ping) request id=0x0001, seq=35552/57482, ttl=126 (reply in 9)
← 9	2.059484	192.168.200.50	192.168.0.211	200	64	ICMP	110	Echo (ping) reply id=0x0001, seq=35552/57482, ttl=64 (request in 8)
10	2.891802	Routerboardc_0c:14:32	Nearest-Bridge	1		LLDP	181	MA/04:f4:1c:0c:14:2a IN/vlan1 121 SysN=MikroTik Switch SysD=MikroTik RouterOS
11	3.069032	192.168.0.211	192.168.200.50	200	126	ICMP	110	Echo (ping) request id=0x0001, seq=35553/57738, ttl=126 (reply in 12)
12	3.069523	192.168.200.50	192.168.0.211	200	64	ICMP	110	Echo (ping) reply id=0x0001, seq=35553/57738, ttl=64 (request in 11)
13	3.352772	Routerboardc_94:85:9c	Nearest-Bridge	1		LLDP	184	MA/d4:01:c3:94:85:96 IN/vlan1 121 SysN=MikroTik Router SysD=MikroTik RouterOS

> Frame 8: Packet, 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF\_{34DD7944-9011-42A0-A43E-B074DD2BB950}, id 0

▼ Ethernet II, Src: Routerboardc\_94:85:97 (d4:01:c3:94:85:97), Dst: LCFCElectron\_39:d9:22 (28:d2:44:39:d9:22)

> Destination: LCFCElectron\_39:d9:22 (28:d2:44:39:d9:22)

> Source: Routerboardc\_94:85:97 (d4:01:c3:94:85:97)  
Type: 802.1AE (MACsec) (0x88e5)  
[Stream index: 3]

> 802.1AE Security Tag

Decrypted Data: 810000c808004500003c7c3700007e017633c0a800d3c0a8c8320800c27a00018ae06162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 200

> Internet Protocol Version 4, Src: 192.168.0.211, Dst: 192.168.200.50

> Internet Control Message Protocol

0000 81 00 00 c8 08 00 45 00 00 3c 7c 37 00 00 7e 01 .....E. <|7...~

0010 76 33 c0 a8 00 d3 c0 a8 c8 32 08 00 c2 7a 00 01 v3.....2...z..

0020 8a e0 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e ..abcdef ghijklmn

0030 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 opqrstuv wabcdfg

0040 68 69 hi

**Decrypted headers and fields:**

- 8100 2 Bytes Ethertype 8100 (VLAN)
- 00c808004500003c7c3700007e017633c0a800d3c0a8c832 4 Bytes VLAN Header with Ethertype 0800 (IP)
- 0800c27a00018ae06162636465666768696a6b6c6d6e6f7071727374757677616263646566676869 20 Bytes IP Header
- 0800c27a00018ae0 8 Bytes ICMP Header
- 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869 32 Bytes ICMP Payload

Packet (110 bytes)    Decrypted Data (66 bytes)

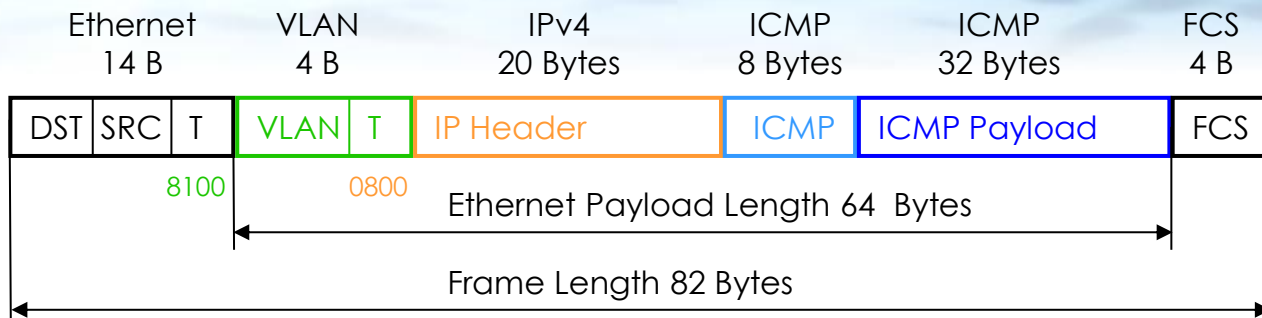
Decrypted Data (macsec.decrypted\_data), 66 bytes

Packets: 429

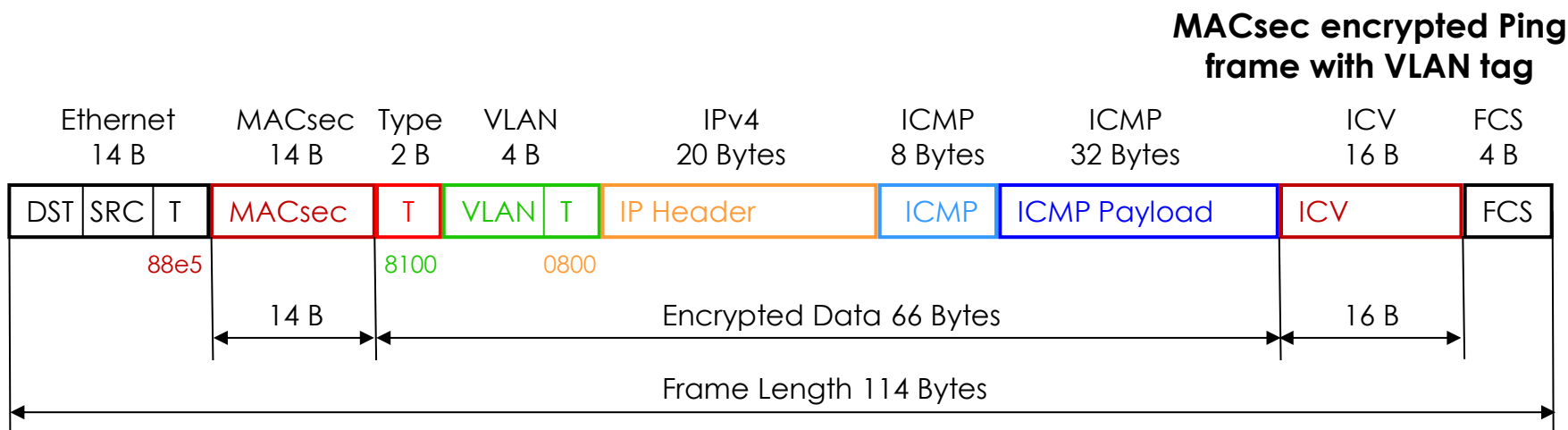


# MACsec (Media Access Control Security)

## MACsec frame format



Unencrypted Ping frame with VLAN tag



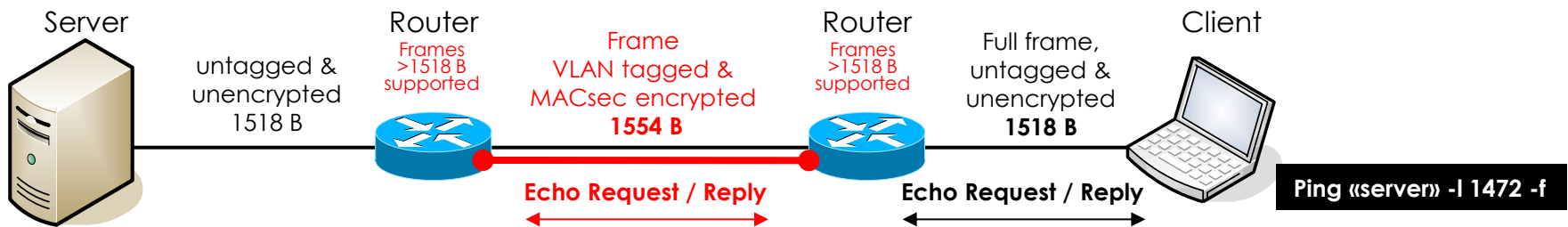
- **MACsec** verlängert Frames **ohne** VLAN-Tag um **30 Bytes**, Frames **mit** VLAN-Tag um **32 Bytes**
- Z.B. ein **Ping mit VLAN** wird durch die Verschlüsselung von **82 Bytes** auf **114 Bytes** vergrößert

➤ 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**.



MACsec\_oversized\_ICMP\_VLAN200\_with\_Negotiation.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	VLAN ID	TTL	Protocol	Length	Info
→ 110	35.038581	192.168.0.211	192.168.200.50	200	126	ICMP	1550	Echo (ping) request id=0x0001, seq=64667/39932, ttl=126 (reply in 111)
← 111	35.039615	192.168.200.50	192.168.0.211	200	64	ICMP	1550	Echo (ping) reply id=0x0001, seq=64667/39932, ttl=64 (request in 110)
→ 116	36.048042	192.168.0.211	192.168.200.50	200	126	ICMP	1550	Echo (ping) request id=0x0001, seq=64668/40188, ttl=126 (reply in 117)
← 117	36.048919	192.168.200.50	192.168.0.211	200	64	ICMP	1550	Echo (ping) reply id=0x0001, seq=64668/40188, ttl=64 (request in 116)

> Frame 110: Packet, 1550 bytes on wire (12400 bits), 1550 bytes captured (12400 bits) on interface \Device\NPF\_{34DD7944-9011-42A0-A43E-B074DD2BB950}

> Ethernet II, Src: Routerboardc\_94:85:97 (d4:01:c3:94:85:97), Dst: LCFCElectron\_39:d9:22 (28:d2:44:39:d9:22)

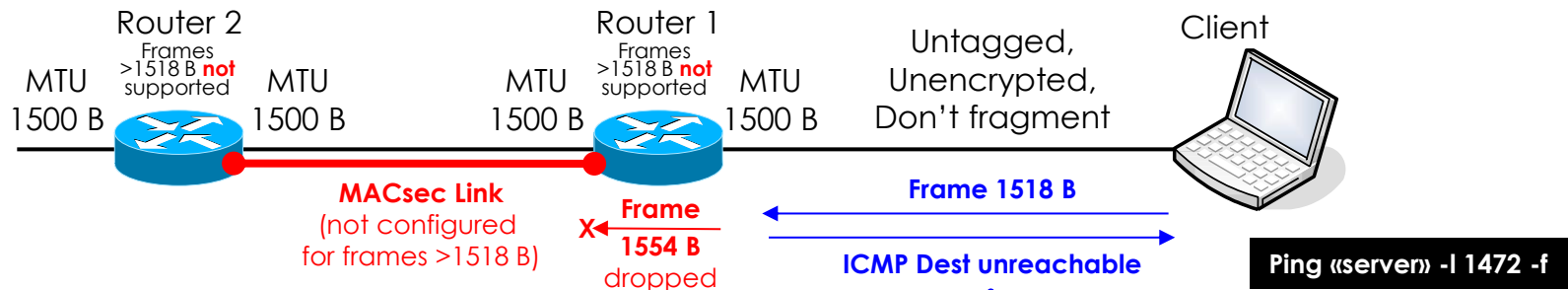
➤ Damit **Wireshark** Frames >1518 Bytes anzeigt, muss der Ethernet Adapter für **Jumbo Frames** konfiguriert sein.

# 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



No.	Time	Source	Destination	VLAN ID	TTL	Protocol	Length	Info
1	0.000000	192.168.0.211	192.168.100.50		128	ICMP	1514	Echo (ping) request id=0x0001, seq=14712/30777
2	0.001802	192.168.0.100	192.168.0.211		64...	ICMP	590	Destination unreachable (Fragmentation needed)

```

> Frame 2: Packet, 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{81480ECC-E8BC-4E52-BBDE-B...}
> Ethernet II, Src: Routerboardc_94:85:96 (d4:01:c3:94:85:96), Dst: JiapengHuaxi_32:d5:34 (c8:4d:44:32:d5:34)
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 192.168.0.211
> Internet Control Message Protocol
  > Type: Destination unreachable (3)
    Code: 4 (Fragmentation needed)
  
```

- 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](#)

No.	Time	Source	Destination	VLAN	TTL	Protocol	Length	Info
1	0.000000	Routerboardc_0c:14:32	Nearest-non-TPMR-Bridge			EAPOL-MKA	94	Key Server, Potential Peer List
2	0.000576	Routerboardc_94:85:9c	Nearest-non-TPMR-Bridge			EAPOL-MKA	94	Live Peer List
3	1.998934	Routerboardc_0c:14:32	Nearest-non-TPMR-Bridge			EAPOL-MKA	170	Key Server, Live Peer List, MACsec SAK Use, Distributed SAK
4	1.999116	Routerboardc_94:85:9c	Nearest-non-TPMR-Bridge			EAPOL-MKA	94	Live Peer List
5	2.001033	Routerboardc_94:85:9c	Nearest-non-TPMR-Bridge			EAPOL-MKA	138	Live Peer List, MACsec SAK Use
6	7.069001	Routerboardc_94:85:97	LCFCElectron_39:d9:22	200		ARP	78	Who has 192.168.200.50? Tell 192.168.200.1
7	7.069240	LCFCElectron_39:d9:22	Routerboardc_94:85:97	200		ARP	96	192.168.200.50 is at 28:d2:44:39:d9:22
8	7.205273	192.168.0.211	192.168.200.50	200	126	ICMP	1550	Echo (ping) request id=0x0001, seq=64672/41212, ttl=126 (req
9	7.205856	192.168.200.50	192.168.0.211	200	64	ICMP	1550	Echo (ping) reply id=0x0001, seq=64672/41212, ttl=64 (req

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.

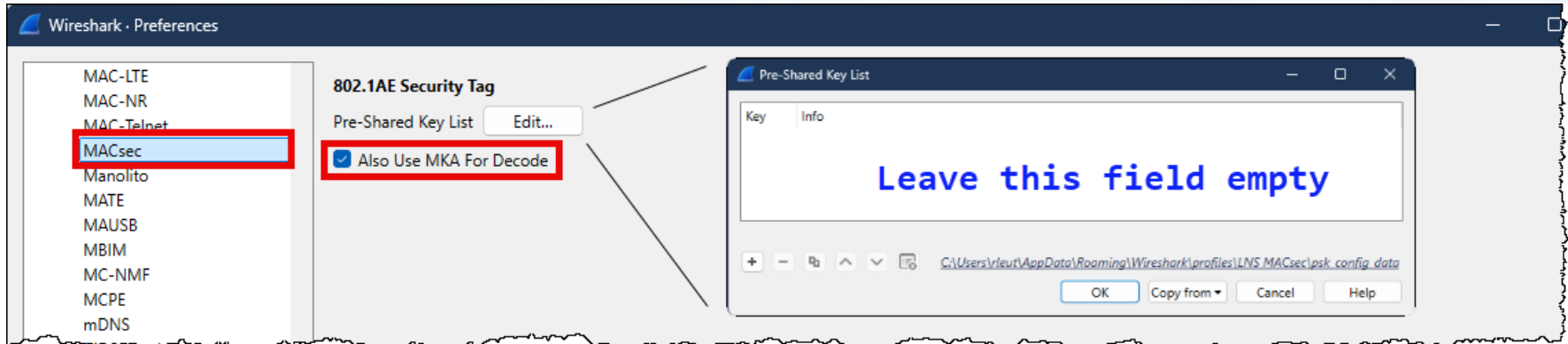
<b>CAK</b>	Connectivity Association Key (PSK) (must be 32 or 64 Hex digits and the same on both devices (and Wireshark)
<b>CKN</b>	CAK Name (must be an even number of Hex digits and the same on both devices (and Wireshark)
<b>EAPOL</b>	Extensible Authentication Protocol over LAN
<b>MKA</b>	MACsec Key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



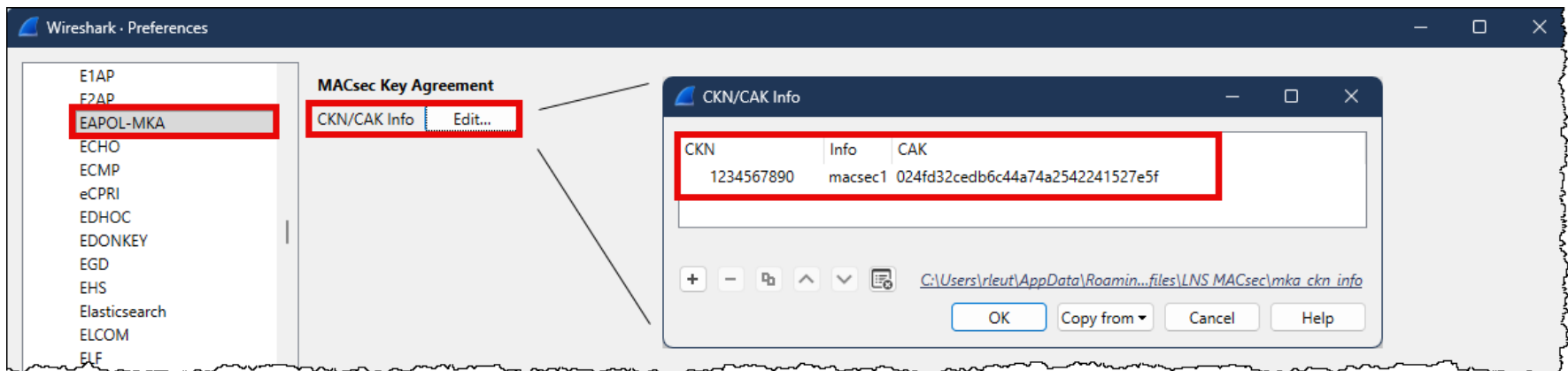
# MACsec (Media Access Control Security)

## 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).



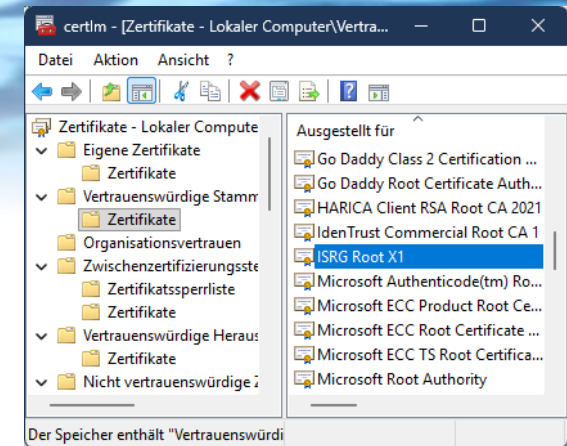
No.	Time	Source	Destination	Server Name	TTL	Protocol	Length	Info
1	0.000000	HP-EliteBook-840	www.netsniffing.ch		128	TCP	66	50358 → 443 [SYN] Seq=275952904 Win=64240 Len=0
2	0.006402	www.netsniffing.ch	HP-EliteBook-840		54	TCP	66	443 → 50358 [SYN, ACK] Seq=3296870161 Ack=275952904
3	0.006484	HP-EliteBook-840	www.netsniffing.ch		128	TCP	54	50358 → 443 [ACK] Seq=275952905 Ack=3296870161
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=275953422
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=275953422
8	0.015137	www.netsniffing.ch	HP-EliteBook-840		54	TCP	1230	443 → 50358 [PSH, ACK] Seq=3296873082 Ack=275953422
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=329687511
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], PRIOR
14	0.194379	HP-EliteBook-840	www.netsniffing.ch		128	HTTP2	483	HEADERS[15]: GET /de/, WINDOW_UPDATE[15]
15	0.199702	www.netsniffing.ch	HP-EliteBook-840		54	TCP	60	443 → 50358 [ACK] Seq=3296875113 Ack=27595440

Mit Wireshark entschlüsselte HTTP-Daten

# X.509 Zertifikat exportieren

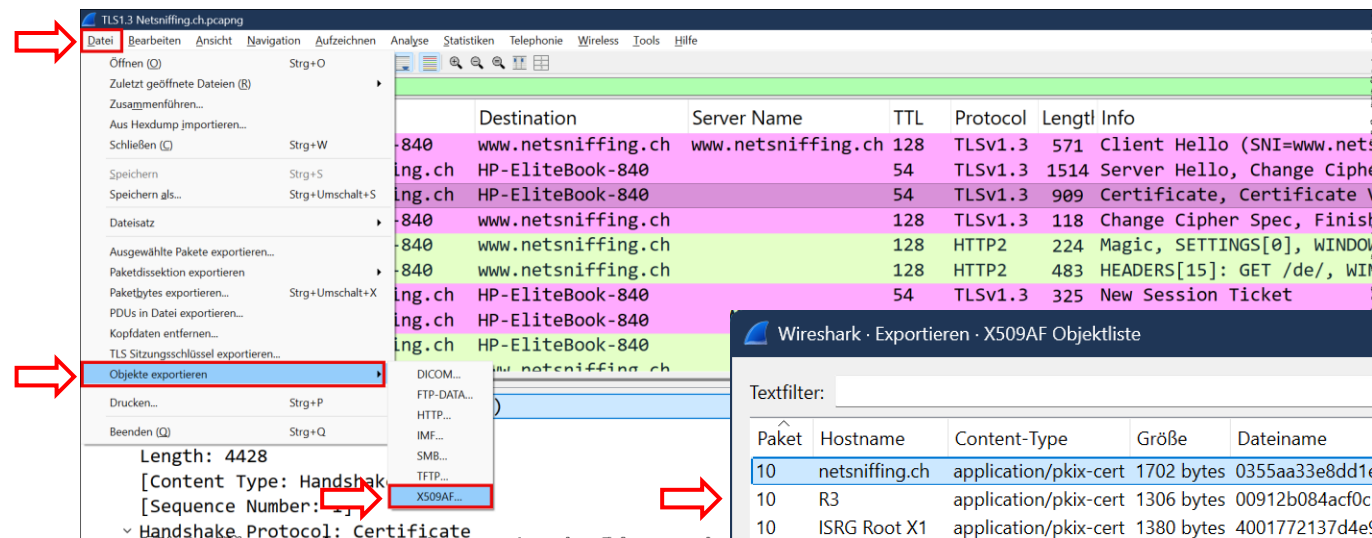
## ➤ Was ist der Nutzen, X.509 Zertifikate exportieren zu können?

- 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!



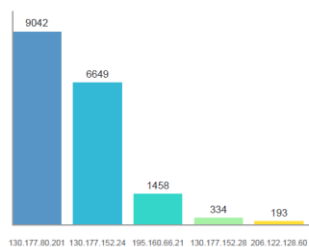
# Tipps, Tricks & Traces

## PacketReporter: PDF-Grafiken direkt mit Wireshark erstellen

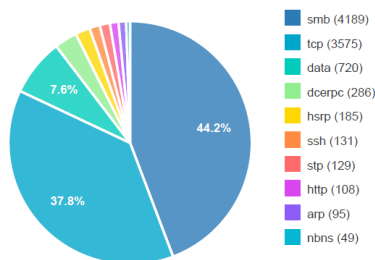
- Mein Wireshark Buddy [Walter Hofstetter](#) hat mit LUA Script eine nützliche Erweiterung erstellt.
- Von einem Trace File lassen sich rund ein Dutzend Grafiken direkt in ein PDF-File exportieren.

Einige Beispiele

2. Top 10 IP Addresses

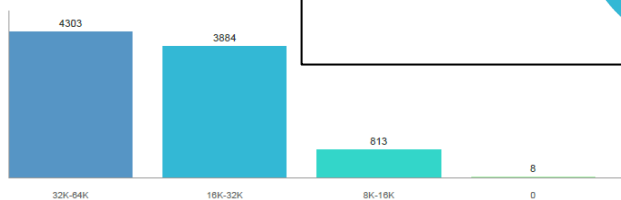


3. Top Protocols and Applications

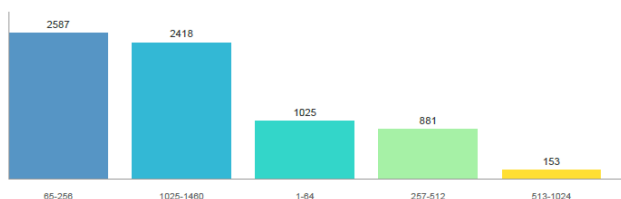


11. TCP Analysis

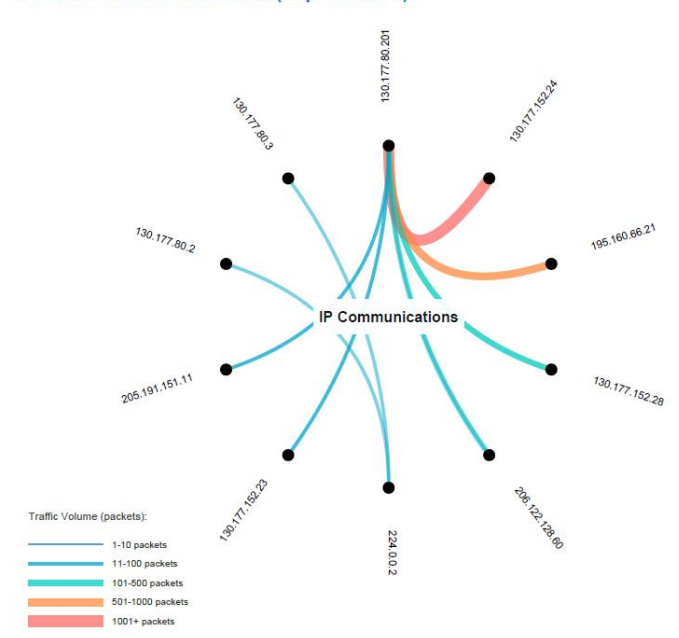
11.1 TCP Window Size Distribution



11.2 TCP Segment Size Distribution

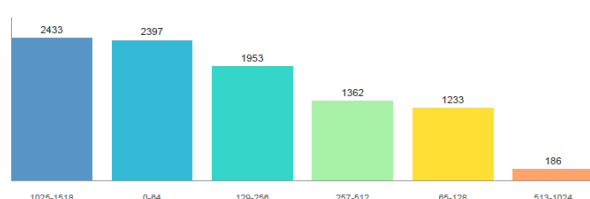


4. IP Communication Matrix (Top 10 Hosts)



9. MAC Layer Analysis

9.2 Frame Size Distribution







# Tipps, Tricks & Traces

17

## PDF-Grafiken direkt mit Wireshark erstellen

- **PacketReporter** und Installationsanleitungen für **Windows/MAC/Linux** sind auf [GitHub](#) verfügbar.

The screenshot shows the GitHub repository 'netwho / PacketReporter' with the file 'PacketReporter-v0.2.5.zip' highlighted. Below it, a Windows File Explorer window is open, showing the contents of the 'PacketReporter-v0.2.5\installers\windows' folder. The files listed are:

Name	Änderungsdatum	Typ	Größe
install.ps1	19.01.2026 15:03	Windows PowerShell-Skript	12 KB
install.sh	19.01.2026 15:03	SH-Datei	6 KB
Logo.png	19.01.2026 15:03	PNG-Datei	94 KB
packet_reporter.lua	19.01.2026 15:03	LUA-Datei	106 KB
packet_reporter.txt	19.01.2026 15:03	Textdokument	1 KB
requirements.md	19.01.2026 15:03	MD-Datei	13 KB
WINDOWS_QUICK_INSTALL_MANUAL_de.pdf	19.01.2026 15:03	Adobe Acrobat Document	385 KB
WINDOWS_QUICK_INSTALL_MANUAL_en.pdf	19.01.2026 15:03	Adobe Acrobat Document	383 KB

The 'WINDOWS\_QUICK\_INSTALL\_MANUAL\_de.pdf' file is highlighted in red. To the right of the File Explorer, a 'Download' button is visible with a red box around the download icon.

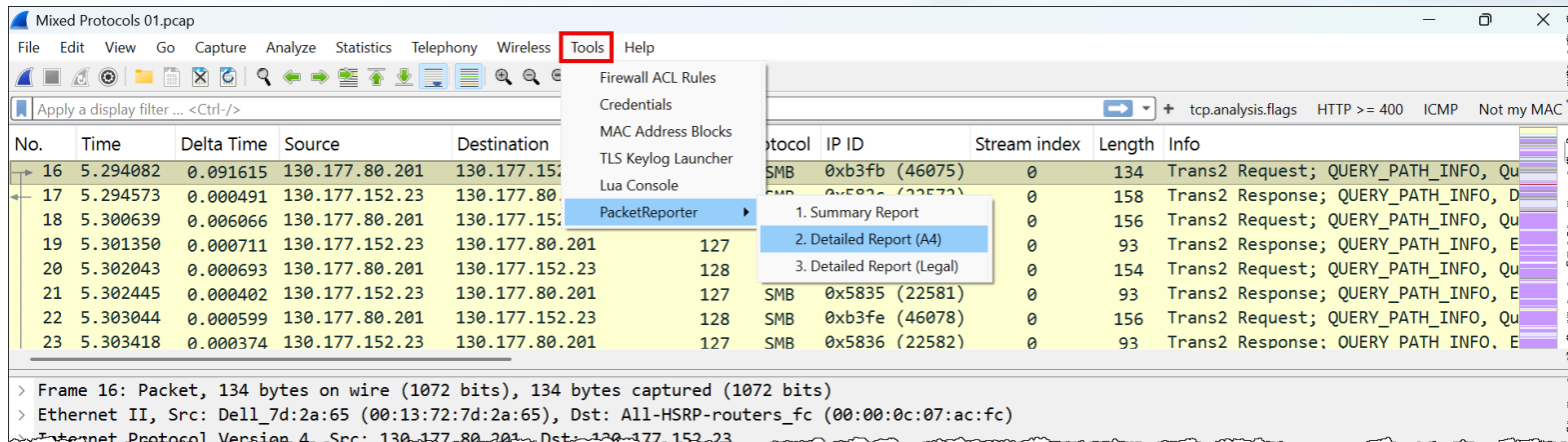
Download



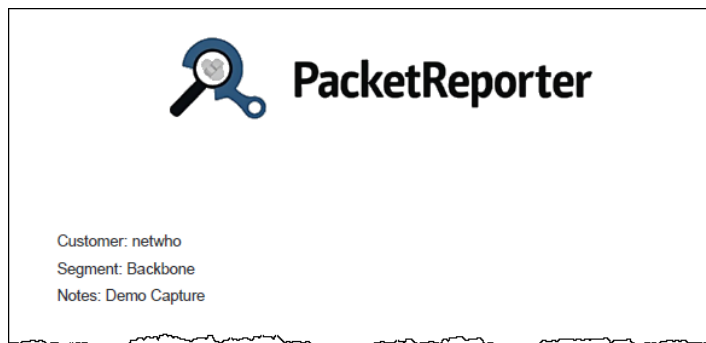
# Tipps, Tricks & Traces

## 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](mailto:walter.hofstetter@netwho.ch) kontaktieren.

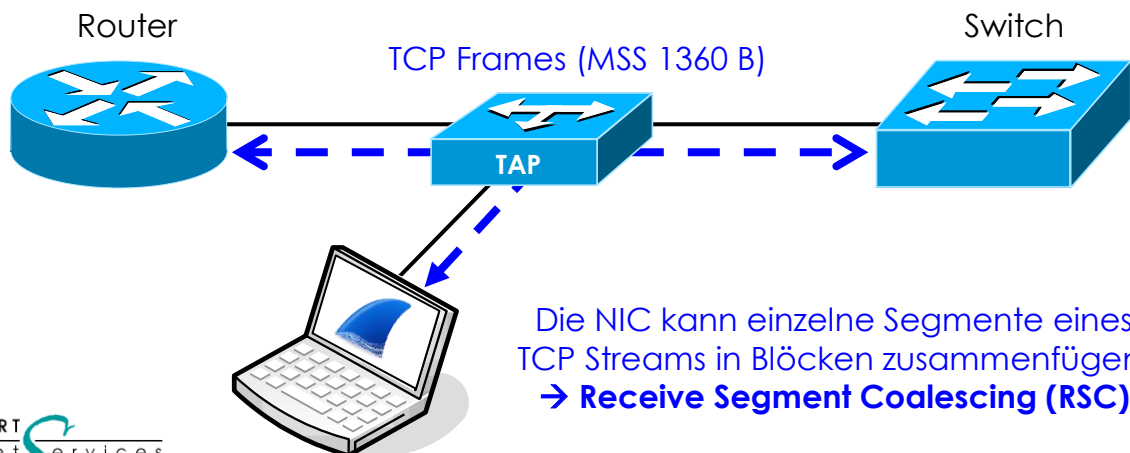


# Tipps, Tricks & Traces

## 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**.

No.	Time	Source	Destination	Protocol	Time to Live	Length	Info
21	3.986	192.168.0.204	82.195.224.120	TCP	128	66	55211 → 49701 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
22	3.996	82.195.224.120	192.168.0.204	TCP	55	66	49701 → 55211 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 WS=0 SACK_PERM=1
23	3.996	192.168.0.204	82.195.224.120	TCP	128	54	55211 → 49701 [ACK] Seq=1 Ack=1 Win=4194304 Len=0
24	3.997	192.168.0.204	82.195.224.120	FTP-DATA	128	2774	FTP Data: 2720 bytes (PASV) (STOR wireshark-win32-1.2.5.exe)
25	4.045	82.195.224.120	192.168.0.204	TCP	55	60	49701 → 55211 [ACK] Seq=1 Ack=2721 Win=63920 Len=0
26	4.045	192.168.0.204	82.195.224.120	FTP-DATA	128	5494	FTP Data: 5440 bytes (PASV) (STOR wireshark-win32-1.2.5.exe)
27	4.094	82.195.224.120	192.168.0.204	TCP	55	60	49701 → 55211 [ACK] Seq=1 Ack=5441 Win=61200 Len=0
28	4.094	192.168.0.204	82.195.224.120	FTP-DATA	128	5494	FTP Data: 5440 bytes (PASV) (STOR wireshark-win32-1.2.5.exe)



Wireshark zeigt Datenblöcke zusammengefügt aus mehreren 1360 B grossen TCP-Segmenten

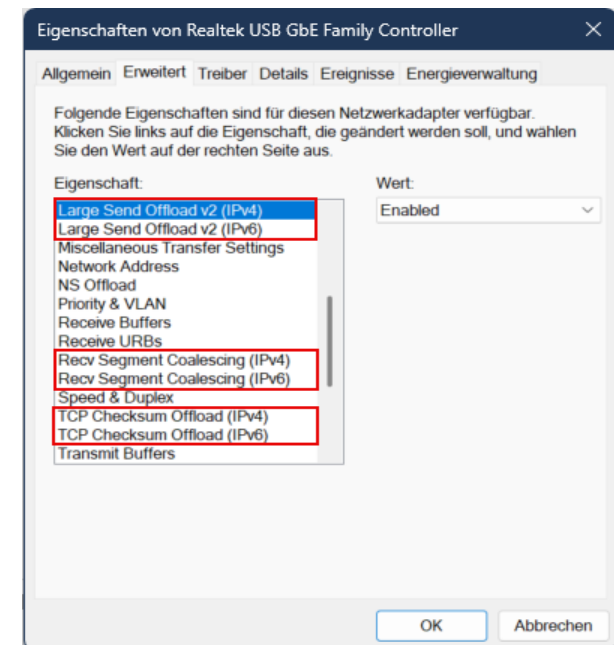
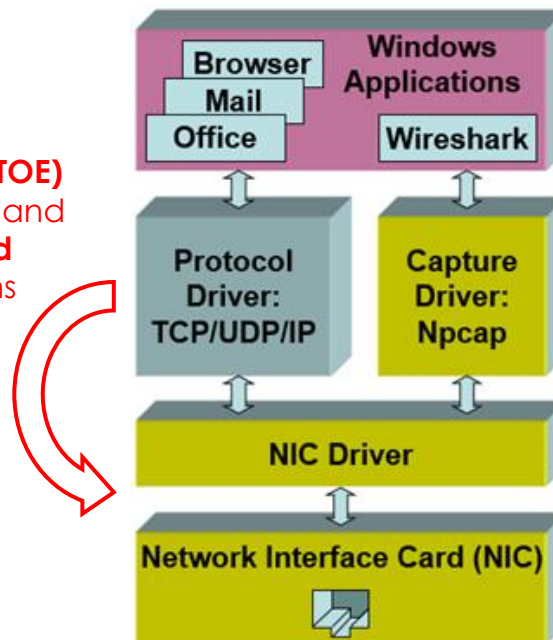


# Tipps, Tricks & Traces

## 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**



**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](#).