

WIRESHARK EDUCATION DAY – Olten CH 2026

Analyse von TLS-Handshakes

Benjamin Pfister

The Wireshark logo, featuring a stylized white shark fin icon above the word "WIRESHARK" in a bold, white, sans-serif font.

WIRESHARK

Sponsored by:  

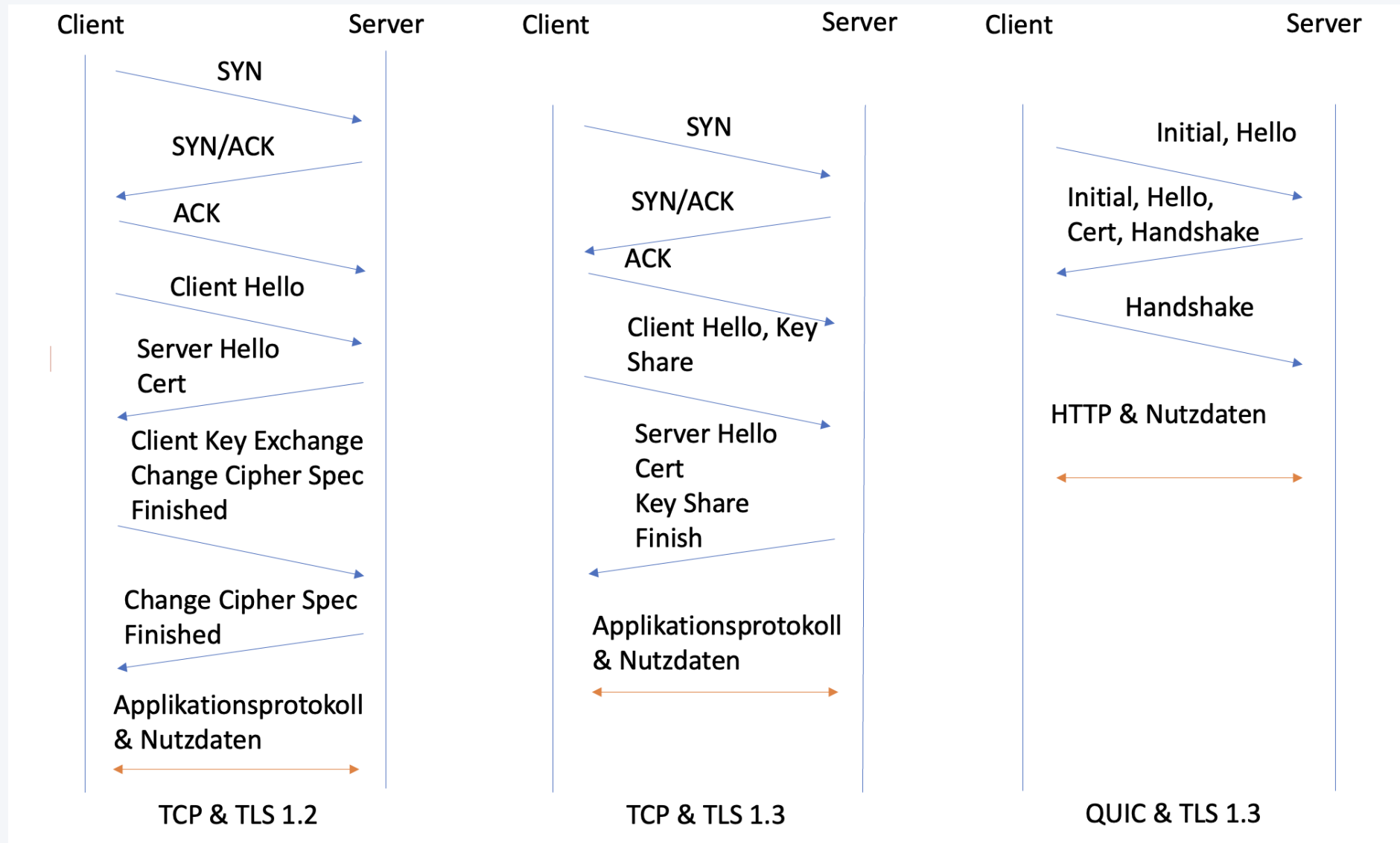


- Ablauf
- Zugrunde liegende Protokolle und Abhängigkeiten
- Handshake
- TLS Interception
- Erkennung Zielhosts trotz Verschlüsselung
- TLS-Entschlüsselung mit Session Key Methode

Ablauf



Ablauf Verbindungsaufbau



Ablauf Verbindungsaufbau



Wireshark capture of a connection setup (tcpbuf (3).pcap). The packet list shows the following sequence of events:

No.	Time	Source	Destination	Protocol	Length	Info
437	91.404000	192.168.4.24	192.168.4.1	NTP	90	NTP Version 3, client
438	91.404000	192.168.4.1	192.168.4.24	NTP	90	NTP Version 4, server
485	108.112000	192.168.4.24	192.168.4.1	DNS	75	Standard query 0xcabb A rps.yealink.com
486	108.128000	192.168.4.1	192.168.4.24	DNS	91	Standard query response 0xcabb A rps.yealink.com
534	111.516000	192.168.4.24	192.168.4.1	DNS	82	Standard query 0x4e6a A gw.intern.pfister.com
535	111.516000	192.168.4.1	192.168.4.24	DNS	98	Standard query response 0x4e6a A gw.intern.pfister.com
539	111.608000	192.168.4.24	192.168.4.1	TCP	66	12592 → 5061 [SYN] Seq=0 Win=5840 Len=0 MSS=60
540	111.608000	192.168.4.1	192.168.4.24	TCP	58	5061 → 12592 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0
541	111.608000	192.168.4.24	192.168.4.1	TCP	60	12592 → 5061 [ACK] Seq=1 Ack=1 Win=5840 Len=0
542	111.788000	192.168.4.24	192.168.4.1	TLSv1.2	182	Client Hello
543	111.788000	192.168.4.1	192.168.4.24	TCP	54	5061 → 12592 [ACK] Seq=1 Ack=129 Win=16384 Len=0
544	111.792000	192.168.4.1	192.168.4.24	TLSv1.2	1078	Server Hello
545	111.792000	192.168.4.24	192.168.4.1	TCP	60	12592 → 5061 [ACK] Seq=129 Ack=1025 Win=7680 Len=0
546	111.852000	192.168.4.1	192.168.4.24	TLSv1.2	539	Certificate, Server Hello Done
547	111.852000	192.168.4.24	192.168.4.1	TCP	60	12592 → 5061 [ACK] Seq=129 Ack=1510 Win=9216 Len=0
552	112.620000	192.168.4.1	192.168.4.24	TLSv1.2	628	Client Key Exchange, Change Cipher Spec, Encrypted
553	112.620000	192.168.4.1	192.168.4.24	TCP	54	5061 → 12592 [ACK] Seq=1510 Ack=703 Win=16384 Len=0
556	115.888000	192.168.4.1	192.168.4.24	TLSv1.2	280	New Session Ticket, Change Cipher Spec, Encrypted
557	115.888000	192.168.4.24	192.168.4.1	TCP	60	12592 → 5061 [ACK] Seq=703 Ack=1736 Win=9216 Len=0
571	119.724000	192.168.4.24	192.168.4.1	TLSv1.2	658	Application Data
572	119.724000	192.168.4.1	192.168.4.24	TCP	54	5061 → 12592 [ACK] Seq=1736 Ack=1307 Win=16384 Len=0

The packet details pane for packet 571 (Application Data) shows:

- Frame 571: 658 bytes on wire (5264 bits), 658 bytes captured (5264 bits)
- Ethernet II, Src: XiamenYe_c5:82:a3 (00:15:65:c5:82:a3), Dst: elmege_7a:70:68 (00:0c:29:7a:70:68)
- Internet Protocol Version 4, Src: 192.168.4.24, Dst: 192.168.4.1
- Transmission Control Protocol, Src Port: 12592, Dst Port: 5061, Seq: 703, Ack: 1736, Win: 9216, Len: 658
- Transport Layer Security
 - TLSv1.2 Record Layer: Application Data Protocol: sip.tcp
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 599
 - Encrypted Application Data: a7642d291c3150f33efd436fb84cc3504587c53de3443894 [Application Data Protocol: sip.tcp]

The packet bytes pane shows the Ethernet frame structure:

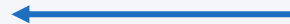
- Ethernet
 - Destination: 00:0c:29:7a:70:68
 - Source: 00:15:65:c5:82:a3
 - Type: 0x0800 (IPv4)
- Internet Protocol Version 4

Zugrunde liegende Protokolle und Abhängigkeiten

Zugrunde liegende Protokolle und Abhängigkeiten

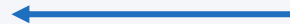


DNS-Auflösung



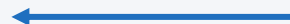
DNS-Methoden
DNS-Server
Firewallfreigaben

Socket-Aufbau



Bidirektionales Routing
Firewall

TLS-Handshake



Version & Ciphers (Verschlüsselung & Signatur)
Gültigkeitszeit Zertifikat (NTP)
CN, SAN und Verwendungszweck Zertifikat
Vertrauenswürdige Zertifizierungsstelle
TLS Interception



```
[pfister@wlc Resources % dig vaf.de. @192.168.178.1 +tcp  
;; Connection to 192.168.178.1#53(192.168.178.1) for vaf.de. failed: connection refused.
```

```
dig vaf.de. @8.8.8.8 +tcp  
vaf.de.                3600      IN      A       217.160.170.221
```

(dns and tcp) or tcp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
141	4.283376	192.168.178.22	192.168.178.1	TCP	78	64659 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=150494748...
142	4.286399	192.168.178.1	192.168.178.22	TCP	60	53 → 64659 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
286	16.193122	192.168.178.22	8.8.8.8	TCP	78	64669 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=102433362...
287	16.211633	8.8.8.8	192.168.178.22	TCP	74	53 → 64669 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM=...
288	16.211839	192.168.178.22	8.8.8.8	TCP	66	64669 → 53 [ACK] Seq=1 Ack=1 Win=131584 Len=0 TSval=1024333646 TSecr=...
289	16.212021	192.168.178.22	8.8.8.8	DNS	103	Standard query 0x05d2 A vaf.de OPT
290	16.228591	8.8.8.8	192.168.178.22	TCP	66	53 → 64669 [ACK] Seq=1 Ack=38 Win=65536 Len=0 TSval=3962821185 TSecr=...
291	16.232836	8.8.8.8	192.168.178.22	DNS	119	Standard query response 0x05d2 A vaf.de A 217.160.170.221 OPT
292	16.232898	192.168.178.22	8.8.8.8	TCP	66	64669 → 53 [ACK] Seq=38 Ack=54 Win=131520 Len=0 TSval=1024333667 TSecr=...
293	16.233561	192.168.178.22	8.8.8.8	TCP	66	64669 → 53 [FIN, ACK] Seq=38 Ack=54 Win=131520 Len=0 TSval=1024333667...
294	16.249872	8.8.8.8	192.168.178.22	TCP	66	53 → 64669 [FIN, ACK] Seq=54 Ack=39 Win=65536 Len=0 TSval=3962821206 ...
295	16.250035	192.168.178.22	8.8.8.8	TCP	66	64669 → 53 [ACK] Seq=39 Ack=55 Win=131520 Len=0 TSval=1024333685 TSecr=...



■ DNS-Abfrage

- `dns.flags.response == False`

■ DNS A-Record-Abfrage

- `dns.qry.type == 1`

- `dns.qry.name == "profitap.com"`

■ HTTPS Record-Abfrage

- `dns.qry.type == 65`

■ Antworten

- `dns.flags.response == True` oder `dns.resp.type`

■ Antwort auf A-Record

- `dns.a == 192.0.2.1`



TCP Handshake erfolgreich

```
pfister@Mac ~ % nmap -p 443 192.168.178.6
Starting Nmap 7.99 ( https://nmap.org ) at 2026-04-06 12:58 +0200
Nmap scan report for rechnung.intern.pfisterit.de (192.168.178.6)
Host is up (0.0096s latency).

PORT      STATE SERVICE
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

TCP Handshake nicht erfolgreich

```
[pfister@wlc Resources % telnet vaf.de 5061
Trying 217.160.170.221...
```

Beispiel Fehlerfall

Wi-Fi: en0 — clab-test-sw1: e1-1

tcp.completeness == 1

No.	Time	Delta	Source	Destination	Protocol	Leng	Info
45	12.239598s		192.168.178.32	8.8.8.8	TCP	78	[TCP Retransmission] 49965 → 5061 [SYN] Seq=0 Win=65535
46	13.240814s	1.001...	192.168.178.32	8.8.8.8	TCP	78	[TCP Retransmission] 49965 → 5061 [SYN] Seq=0 Win=65535
56	14.241713s	1.000...	192.168.178.32	8.8.8.8	TCP	78	[TCP Retransmission] 49965 → 5061 [SYN] Seq=0 Win=65535
67	15.242916s	1.001...	192.168.178.32	8.8.8.8	TCP	78	[TCP Retransmission] 49965 → 5061 [SYN] Seq=0 Win=65535
73	16.243487s	1.000...	192.168.178.32	8.8.8.8	TCP	78	[TCP Retransmission] 49965 → 5061 [SYN] Seq=0 Win=65535
122	18.244937s	2.001...	192.168.178.32	8.8.8.8	TCP	78	[TCP Retransmission] 49965 → 5061 [SYN] Seq=0 Win=65535
131	22.245730s	4.000...	192.168.178.32	8.8.8.8	TCP	78	[TCP Retransmission] 49965 → 5061 [SYN] Seq=0 Win=65535
185	30.247003s	8.001...	192.168.178.32	8.8.8.8	TCP	78	[TCP Retransmission] 49965 → 5061 [SYN] Seq=0 Win=65535

Handshake



TLS-Handshake | Ablauf bis TLS 1.2



- Client Hello = Vorschlag TLS-Version & Cipher Suites
 - `tls.handshake.type == 1`
- Server Hello = Annahme/Ablehnung TLS-Version & Cipher Suites, Zufallszahl & Übersendung TLS-Zertifikat
 - `tls.handshake.type == 2`
- Client Key Exchange = Pre-Master Secret wird übersendet
 - `tls.handshake.type == 16`
- Change Cipher Spec = Wechsel auf generierte Session-Schlüssel
 - `tls.record.content_type == 20`

163	14.238440	192.168.178.22	192.168.178.1	TLSv1.2	263	Client Hello
164	14.240559	192.168.178.1	192.168.178.22	TCP	60	5061 → 49363 [ACK] Seq=1 Ack=210 Win=16384 Len=
707	18.524603	192.168.178.1	192.168.178.22	TLSv1.2	1078	Server Hello
708	18.524686	192.168.178.22	192.168.178.1	TCP	54	49363 → 5061 [ACK] Seq=210 Ack=1025 Win=65535 Len=
709	18.528784	192.168.178.1	192.168.178.22	TLSv1.2	1141	Certificate, Server Key Exchange, Server Hello I
710	18.528872	192.168.178.22	192.168.178.1	TCP	54	49363 → 5061 [ACK] Seq=210 Ack=2112 Win=65535 Len=
711	18.536729	192.168.178.22	192.168.178.1	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypt
712	18.538862	192.168.178.1	192.168.178.22	TCP	60	5061 → 49363 [ACK] Seq=2112 Ack=336 Win=16384 Len=
714	18.606767	192.168.178.1	192.168.178.22	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypt
715	18.606880	192.168.178.22	192.168.178.1	TCP	54	49363 → 5061 [ACK] Seq=336 Ack=2354 Win=65535 Len=
716	18.607305	192.168.178.22	192.168.178.1	TLSv1.2	823	Application Data
717	18.610293	192.168.178.1	192.168.178.22	TCP	60	5061 → 49363 [ACK] Seq=2354 Ack=1105 Win=16384 Len=
718	18.618203	192.168.178.1	192.168.178.22	TLSv1.2	446	Application Data
719	18.618361	192.168.178.22	192.168.178.1	TCP	54	49363 → 5061 [ACK] Seq=1105 Ack=2746 Win=65535 Len=



Wireshark · Packet 163 · SIP-TLS_Softphone_PBX_Corre

✓ Cipher Suites (38 suites)

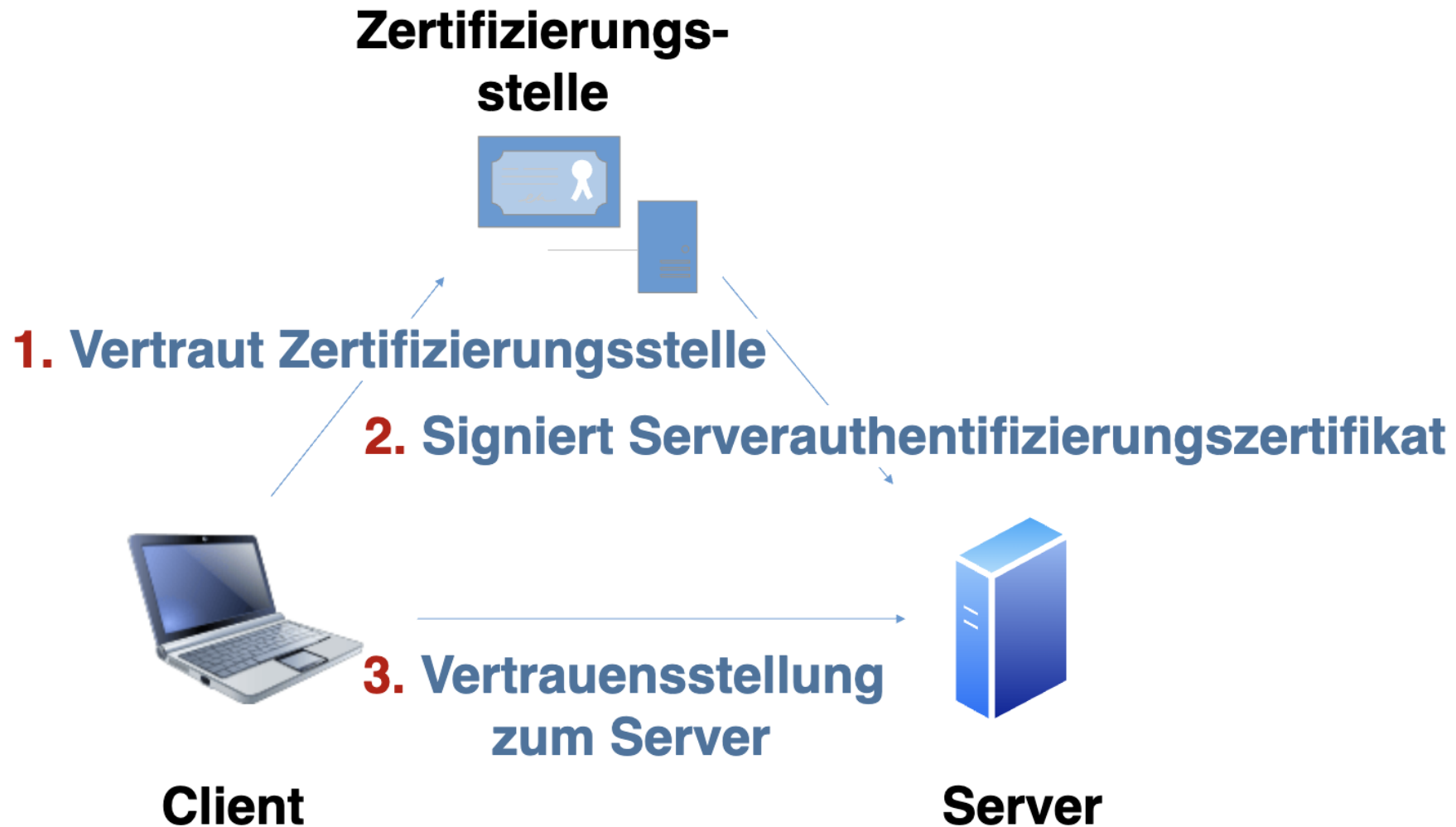
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
- Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
- Cipher Suite: TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Wireshark · Packet 707 · SIP-TLS_Softphone_PBX_Correct.pcapng

Length: 61

✓ Handshake Protocol: Server Hello

- Handshake Type: Server Hello (2)
- Length: 57
- Version: TLS 1.2 (0x0303)
- Random: 7afbdb1475ddeb11a7827be6ecff2f0082d0d2085defb97ff129648527e05e0c
- Session ID Length: 0
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)



TLS-Handshake | Zertifikate



Wireshark

File

Edit

View

Go

Capture

Analyze

Statistics

Telephony

Wireless

Tools

Help

Open

Open Recent

Merge...

Import from Hex Dump...

Close

Save

Save As...

File Set

Export Specified Packets...

Export Packet Dissections

Export Packet Bytes...

Export PDUs to File...

Strip Headers...

Export TLS Session Keys...

Export Objects

Print...

Wi-Fi: en0 — clab-test-sw1: e1-1

1235 Certificate, Server Key Exchange, Server Hello Done

No.	Time	Destination	Protocol	
822	3.0	192.168.178.32	TLSv1.3	
823	3.0	192.168.178.32	TCP	
824	3.0	192.168.178.32	TLSv1.3	
825	3.0	192.168.178.32	TLSv1.3	
826	3.0	192.168.178.32	TLSv1.3	
827	3.0	192.168.178.32	TCP	
828	3.0	192.168.178.32	TLSv1.3	
829	3.0	192.168.178.32	TLSv1.3	
830	3.0	192.168.178.32	TCP	
831	3.0	192.168.178.32	TLSv1.2	
832	3.0	192.168.178.32	TCP	
833	3.0	192.168.178.32	TCP	
834	3.0	192.168.178.32	TLSv1.2	
835	3.0	192.168.178.32	TCP	
836	3.0	192.168.178.32	TCP	
837	3.0	192.168.178.32	TCP	
838	3.016960s	192.168.178.32	TCP	
839	3.017048s	192.168.178.32	TCP	
840	3.017658s	192.168.178.32	TCP	
841	3.020174s	query.reachit.de	TCP	
842	3.020176s	query.reachit.de	TCP	
843	3.020178s	query.reachit.de	TCP	
844	3.020261s	192.168.178.32	TCP	
845	3.020739s	192.168.178.1	TCP	

pfister@Mac Downloads % openssl x509 -in 00a853bb726684aaae7499bee54dd47ad2.cer -text

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

a8:53:bb:72:66:84:aa:ae:74:99:be:e5:4d:d4:7a:d2

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36

Validity

Not Before: Dec 2 00:00:00 2025 GMT

Not After : Jan 2 23:59:59 2027 GMT

Subject: CN=responder.wt.heise.de

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:a3:49:37:5a:11:21:20:aa:29:98:98:79:9b:61:

Wireshark · Export · X509AF object list

Text Filter: heise.de

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
834	responder.wt.heise.de	application/pkix-cert	1716 bytes	00a853bb726684aaae7499bee54dd47ad2.cer
1002	data-fb7f8b3ae8.heise.de	application/pkix-cert	1294 bytes	0637821d8379267d804c...

Help

Preview

Save All

Close

Save

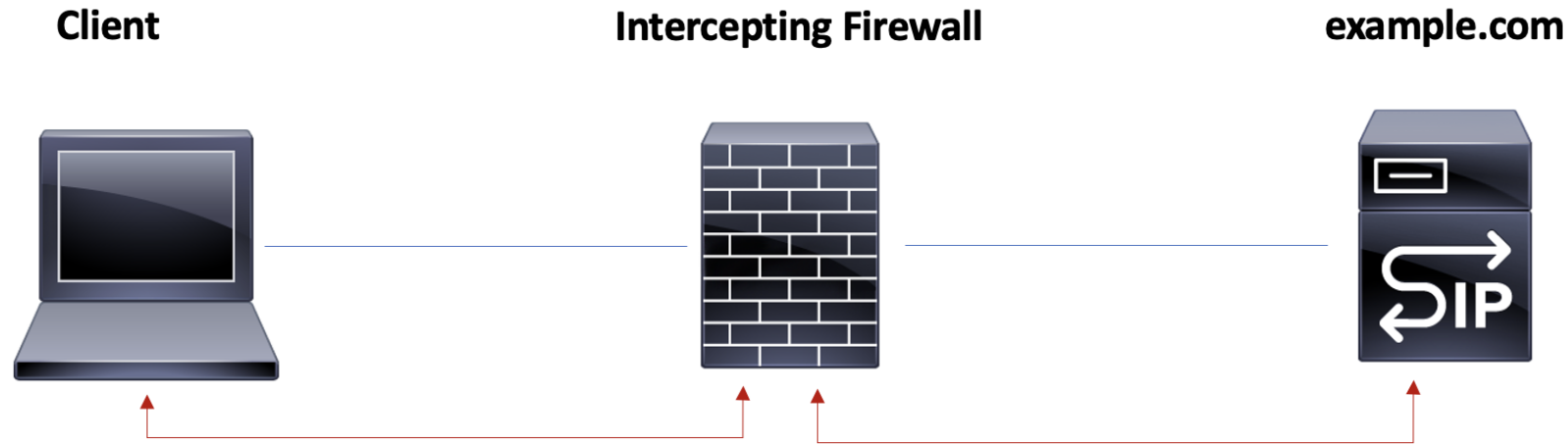
TLS Interception



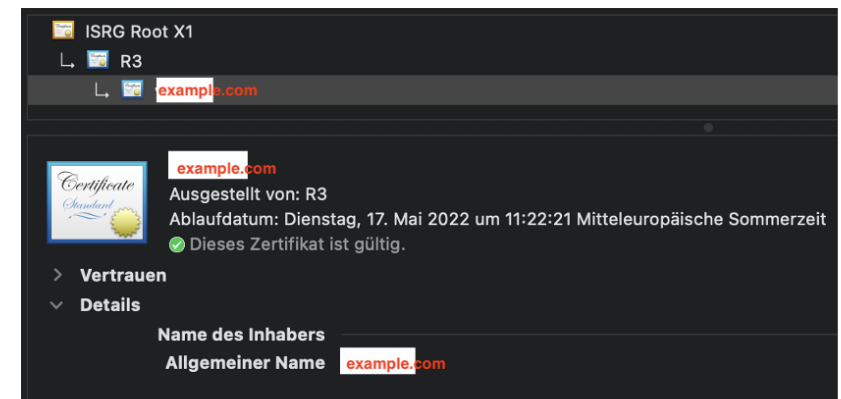
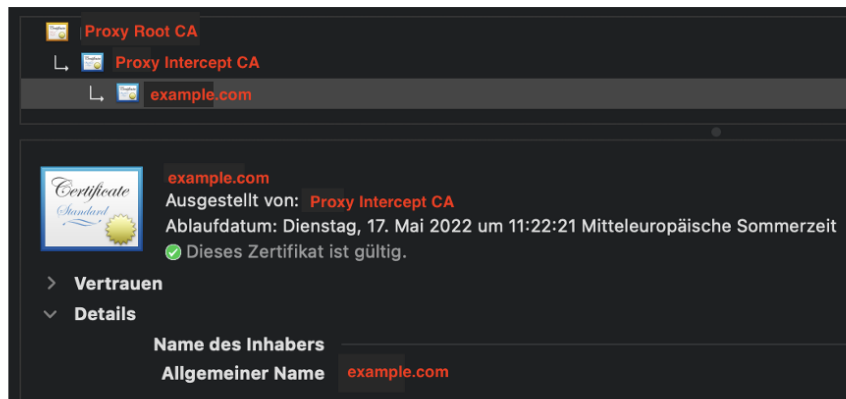
TLS-Handshake | Zertifikate bei Interception



Client muss Proxy Root CA als vertrauenswürdige CA bekannt sein



Firewall bricht TLS-Session auf und tauscht Serverauthentifizierungszertifikat.





Zertifikats-Viewer: www.pfisterit.de

Allgemein

Details

Zertifikathierarchie

▼ Sectigo Public Server Authentication Root R46

▼ Sectigo Public Server Authentication CA DV R36

www.pfisterit.de

Zertifikatfelder

▼ Zertifikat

Version

Seriennummer

Algorithmus für Zertifikatsignatur

Aussteller

▼ Gültigkeit

Nicht vor

Nicht nach

Feldwert

22.07.26, 01:59:59 MESZ

Exportieren...

The Ultimate PCAP v20250325.pcapng

ntp

Time

Source

Destination

Protocol

Lengt

Info

2349

247148590...

192.168.121.40

78.46.107.140

NTP

94

NTP Version 3, client

2350

247148590...

78.46.107.140

192.168.121.40

NTP

94

NTP Version 3, server

Frame 2350: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface unknown, id 85

Ethernet II, Src: Cisco_9e:11:41 (00:14:69:9e:11:41), Dst: Cisco_df:e7:c1 (00:16:47:df:e7:c1)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 121

Internet Protocol Version 4, Src: 78.46.107.140, Dst: 192.168.121.40

User Datagram Protocol, Src Port: 123, Dst Port: 123

Network Time Protocol (NTP Version 3, server)

> Flags: 0x1c, Leap Indicator: no warning, Version number: NTP Version 3, Mode: server

[\[Request In: 2349\]](#)

[Delta Time: 0.007001000 seconds]

Peer Clock Stratum: secondary reference (2)

Peer Polling Interval: 10 (1024 seconds)

Peer Clock Precision: -19 (0.000001907 seconds)

Root Delay: 0.011566 seconds

Root Dispersion: 0.036118 seconds

Reference ID: 192.53.103.108

Reference Timestamp: Mar 3, 2017 19:41:42.937027587 UTC

Origin Timestamp: Mar 3, 2017 19:57:26.698613687 UTC

Receive Timestamp: Mar 3, 2017 19:57:26.699470358 UTC

Transmit Timestamp: Mar 3, 2017 19:57:26.699541750 UTC

Wireshark Education Day – Olten CH 2026

18

Test TLS Handshake



```
pfister@mbp ~ % openssl s_client -connect profitap.com:443
Connecting to 217.160.0.226
[CONNECTED(00000005)]
depth=2 C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication Root R46
verify return:1
depth=1 C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36
verify return:1
depth=0 CN=*.profitap.com
verify return:1
---
Certificate chain
 0 s:CN=*.profitap.com
  i:C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36
  a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
  v:NotBefore: Nov 27 00:00:00 2025 GMT; NotAfter: Dec 11 23:59:59 2026 GMT
 1 s:C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36
  i:C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication Root R46
  a:PKEY: RSA, 3072 (bit); sigalg: sha384WithRSAEncryption
  v:NotBefore: Mar 22 00:00:00 2021 GMT; NotAfter: Mar 21 23:59:59 2036 GMT
 2 s:C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication Root R46
  i:C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority
  a:PKEY: RSA, 4096 (bit); sigalg: sha384WithRSAEncryption
  v:NotBefore: Mar 22 00:00:00 2021 GMT; NotAfter: Jan 18 23:59:59 2038 GMT
 3 s:C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority
  i:C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA Certificate Services
  a:PKEY: RSA, 4096 (bit); sigalg: sha384WithRSAEncryption
  v:NotBefore: Mar 12 00:00:00 2019 GMT; NotAfter: Dec 31 23:59:59 2028 GMT
---
```

Test TLS Handshake



```
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
```

```
Protocol: TLSv1.3
```

```
Server public key is 2048 bit
```

```
This TLS version forbids renegotiation.
```

```
Compression: NONE
```

```
Expansion: NONE
```

```
No ALPN negotiated
```

```
Early data was not sent
```

```
Verify return code: 0 (ok)
```

```
---
```

```
---
```

```
Post-Handshake New Session Ticket arrived:
```

```
SSL-Session:
```

```
Protocol   : TLSv1.3
```

```
Cipher     : TLS_AES_256_GCM_SHA384
```

```
Session-ID: 82B33392426FA1523B935901F05B745107809274E84108A3886A97E54C7E1E76
```

```
Session-ID-ctx:
```

```
Resumption PSK: F035E274509D21B28AE673D9825D94627E736036870E5653676924BE6A5F9
```

```
PSK identity: None
```

```
PSK identity hint: None
```

```
SRP username: None
```

```
TLS session ticket lifetime hint: 300 (seconds)
```

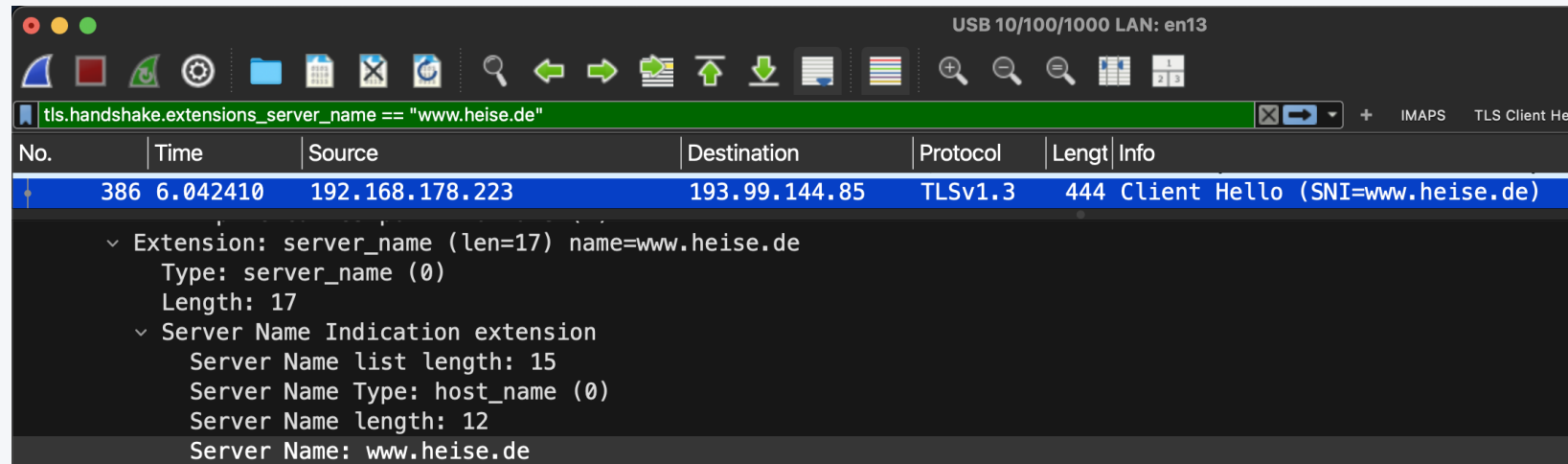
Erkennung Zielhosts trotz Verschlüsselung

Erkennung Zielhosts trotz Verschlüsselung



■ SNI-Extension

- In TLS Client-Hello
- `tls.handshake.extension.type == 0`
- `tls.handshake.extensions_server_name == www.heise.de`



Erkennung Zielhosts trotz Verschlüsselung



■ DNS-Antwort auf A-Record

■ Vorwärts

■ dns.resp.name contains "heise.de"

■ Rückwärts

■ dns.a == 192.0.2.1

TLS-Entschlüsselung mit Session Key Methode

TLS-Entschlüsselung mit Session Key Methode



[t] Wi-Fi: en0

http.request.method == "GET"

SIP Client-Failures SIP Server-Failures SIP Global-Failures VoIP Filter nach Call-ID mit RTP Filter nach Call-ID ohne RTP Fehlerhafter TCP-Socketaufbau Pakete mit SDP DTMF-Töne im RTP HTTP OK

No.	Time	Ak	Source	Destination	Protocol	Len	Info
9711	134.268165	...	192.168.178.124	77.247.84.129	HTTP	91	GET /2507/sp_19
9746	134.273436	...	192.168.178.124	77.247.84.129	HTTP	91	GET /2507/sp_19
9750	134.274639	...	192.168.178.124	77.247.84.129	HTTP	91	GET /2507/sp_19
9755	134.277790	...	192.168.178.124	77.247.84.129	HTTP	91	GET /2507/sp_19
9803	134.296266	...	192.168.178.124	77.247.84.129	HTTP	91	GET /2507/sp_19
9972	134.312727	...	192.168.178.124	77.247.84.129	HTTP	82	GET /7618/sp_VI
10154	134.390506	...	192.168.178.124	77.247.84.129	HTTP	1...	GET /3998/120_6
10194	134.420572	...	192.168.178.124	136.243.25.80	HTTP	7...	GET /120_600/50
10918	137.739491	...	192.168.178.124	35.210.72.234	HTTP	8...	GET /push_sync?

> Frame 10918: 810 bytes on wire (6480 bits), 810 bytes captured (6480 bits) on interface en0, id 0

> Ethernet II, Src: 8a:c7:67:59:50:a6 (8a:c7:67:59:50:a6), Dst: Ubiquiti_2e:cf:ff (28:70:4e:2e:cf:ff)

> Internet Protocol Version 4, Src: 192.168.178.124, Dst: 35.210.72.234

> Transmission Control Protocol, Src Port: 51465, Dst Port: 443, Seq: 3318, Ack: 8416, Len: 744

> [2 Reassembled TCP Segments (2152 bytes): #10917(1408), #10918(744)]

> Transport Layer Security

> Hypertext Transfer Protocol

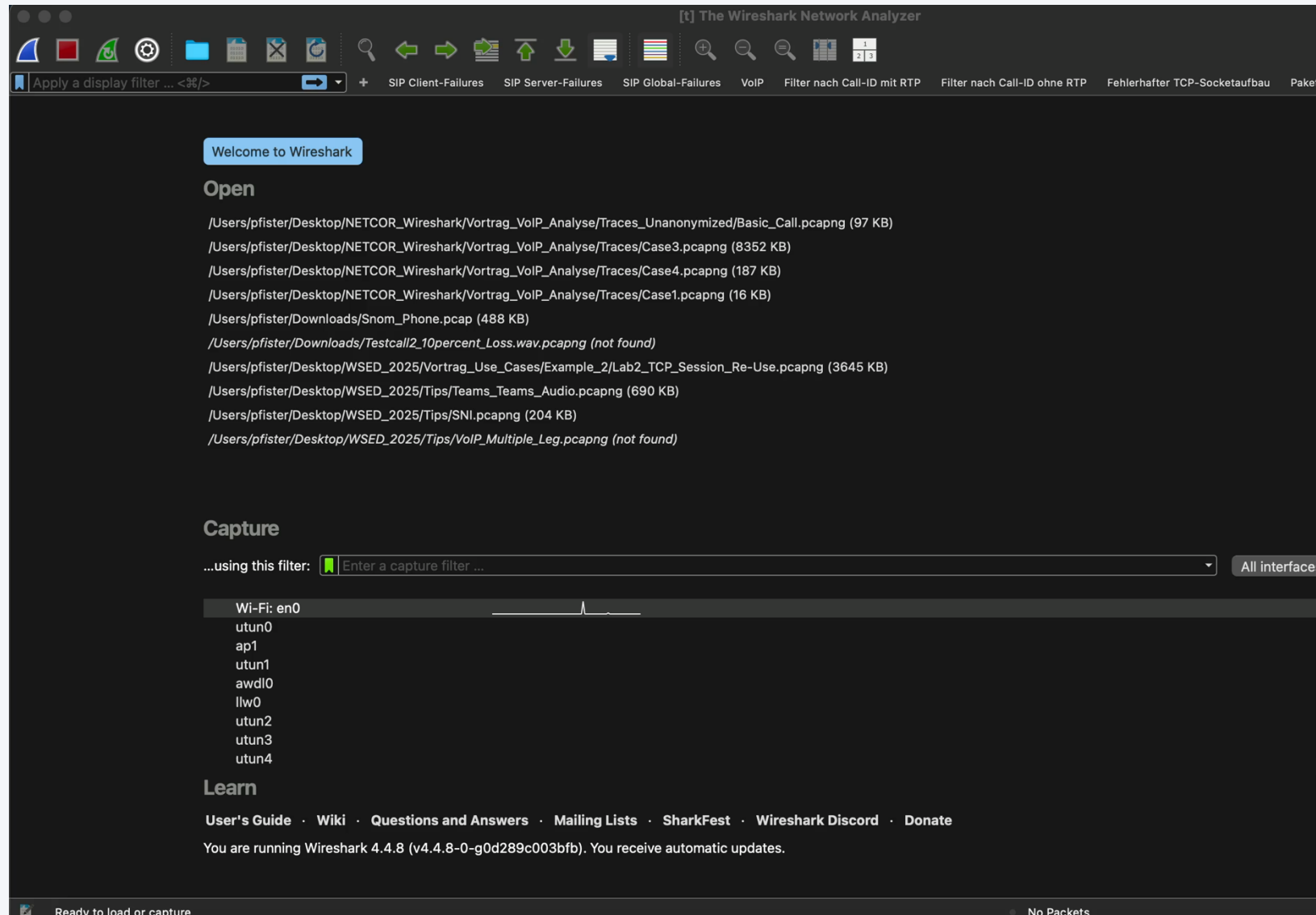
> [...] GET /push_sync?iframe=1&gdpr_consent=CQVNjgAQVNjgAAGABCENB0FsAP_gAAAAAYgKEBBBCpMDGFAMDBVAJgASYAU19gBIEQAAACBA

> Request Method: GET

> Request URI [...]: /push_sync?iframe=1&gdpr_consent=CQVNjgAQVNjgAAGABCENB0FsAP_gAAAAAYgKEBBBCpMDGFAMDBVAJgASYAU19g

> Request Version: HTTP/1.1

TLS-Entschlüsselung mit Session Key Methode



Bildquellen



■ Pexels <https://www.pexels.com/de-de/>

■ Unsplash <https://unsplash.com/de>

Vielen Dank!

WIRESHARK

Benjamin Pfister

[linkedin.com/in/benjamin-pfister-90136b298](https://www.linkedin.com/in/benjamin-pfister-90136b298)

