WIRESHARK EDUCATION DAY – Olten CH 2026

Analyse von TLS-Handshakes

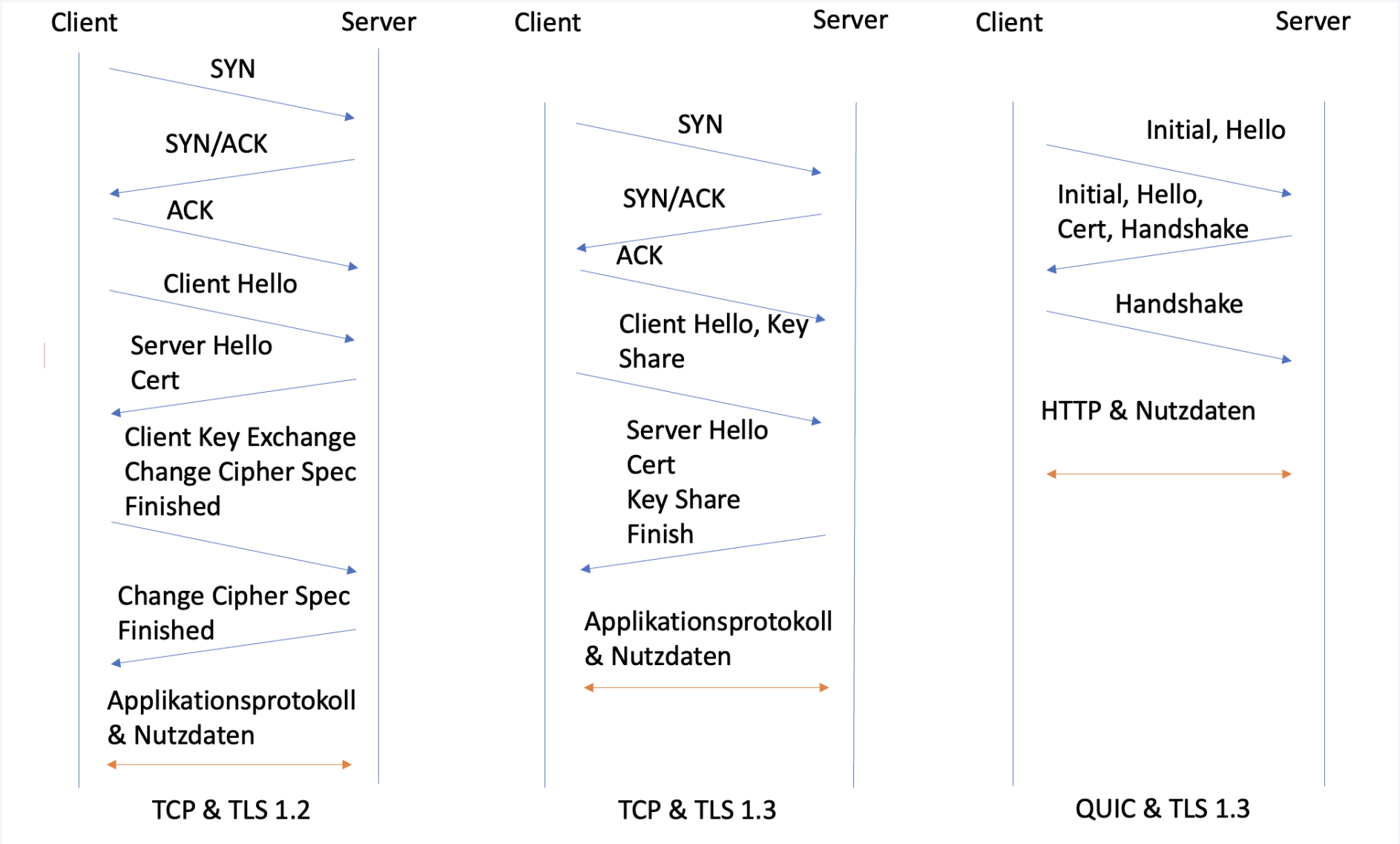
Benjamin Pfister

Überblick | Analyse von TLS-Handshakes

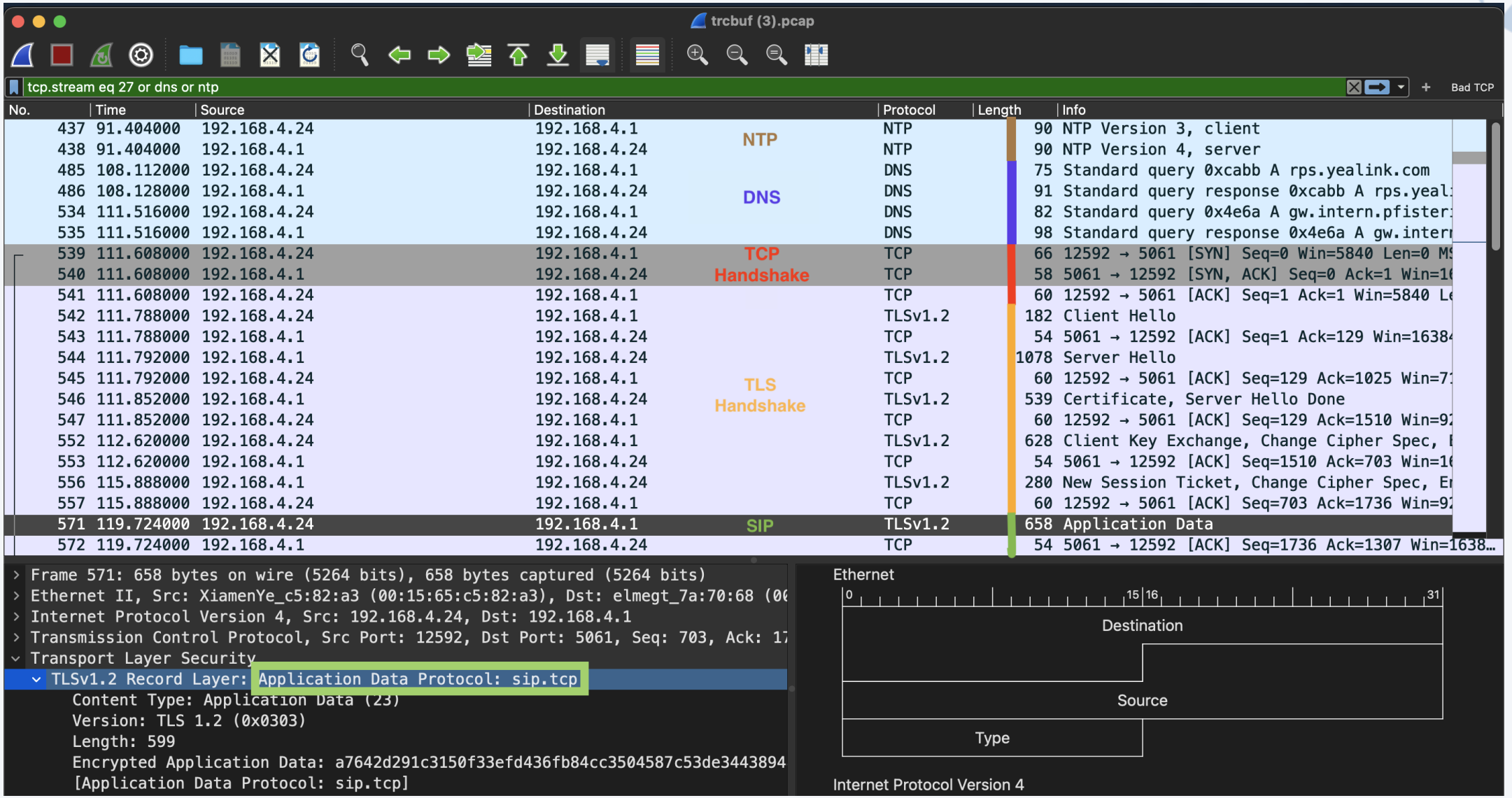
- Ablauf
- Zugrunde liegende Protokolle und Abhängigkeiten
- Handshake
- TLS Interception
- Erkennung Zielhosts trotz Verschlüsselung
- TLS-Entschlüsselung mit Session Key Methode

Ablauf

Ablauf Verbindungsaufbau



Ablauf Verbindungsaufbau



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**

DNS-Auflösung

```
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 — Bad TCP

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 TSec…
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 TSec…

DNS-Auflösung

- 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

Socketaufbau

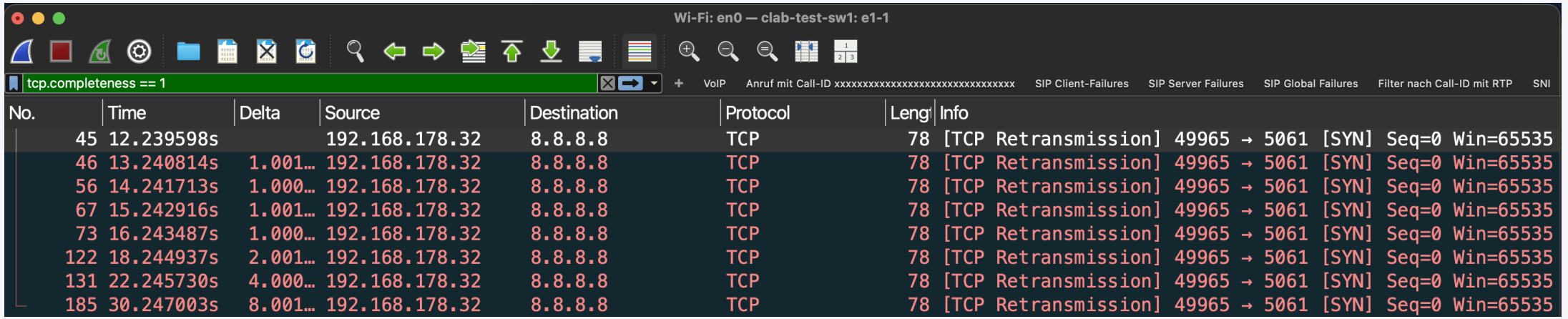
TCP Handshake erfolgreich

```
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

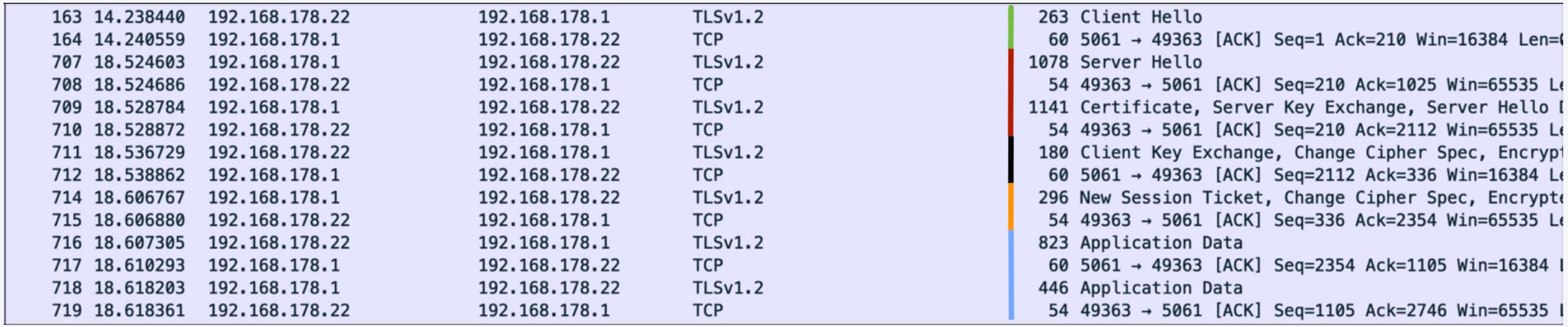


No.	Time	Delta	Source	Destination	Protocol	Leng	Info
45	12.239598s		192.168.178.32	8.8.8.8	TCP	78	[TCP Retransmission] 49965 → 5061 [SYN] Seq=0 Win=65535
46	13.240814s	1.001…	192.168.178.32	8.8.8.8	TCP	78	[TCP Retransmission] 49965 → 5061 [SYN] Seq=0 Win=65535
56	14.241713s	1.000…	192.168.178.32	8.8.8.8	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

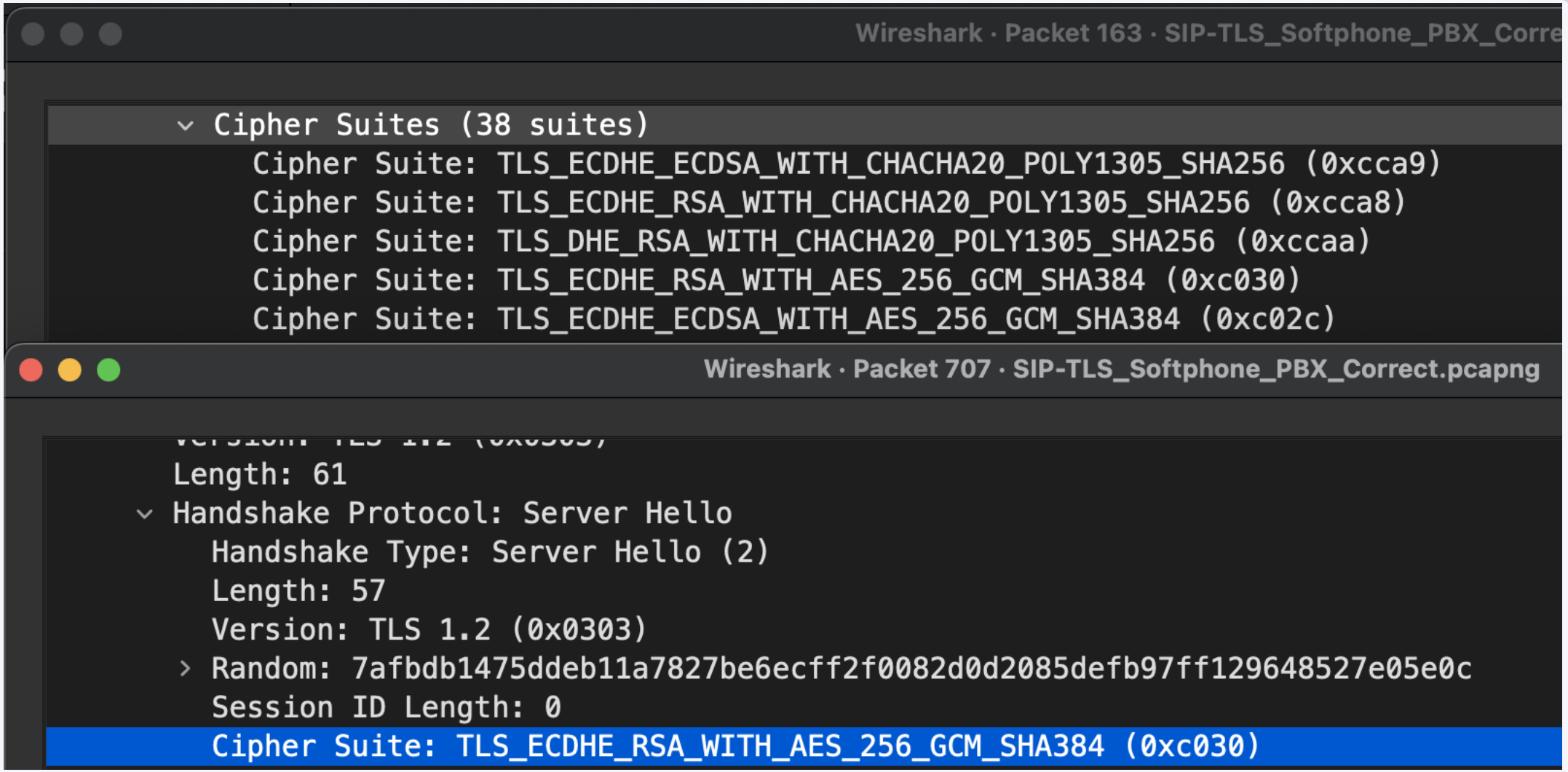
Handshake

TLS-Handshake | Ablauf bis TLS 1.2

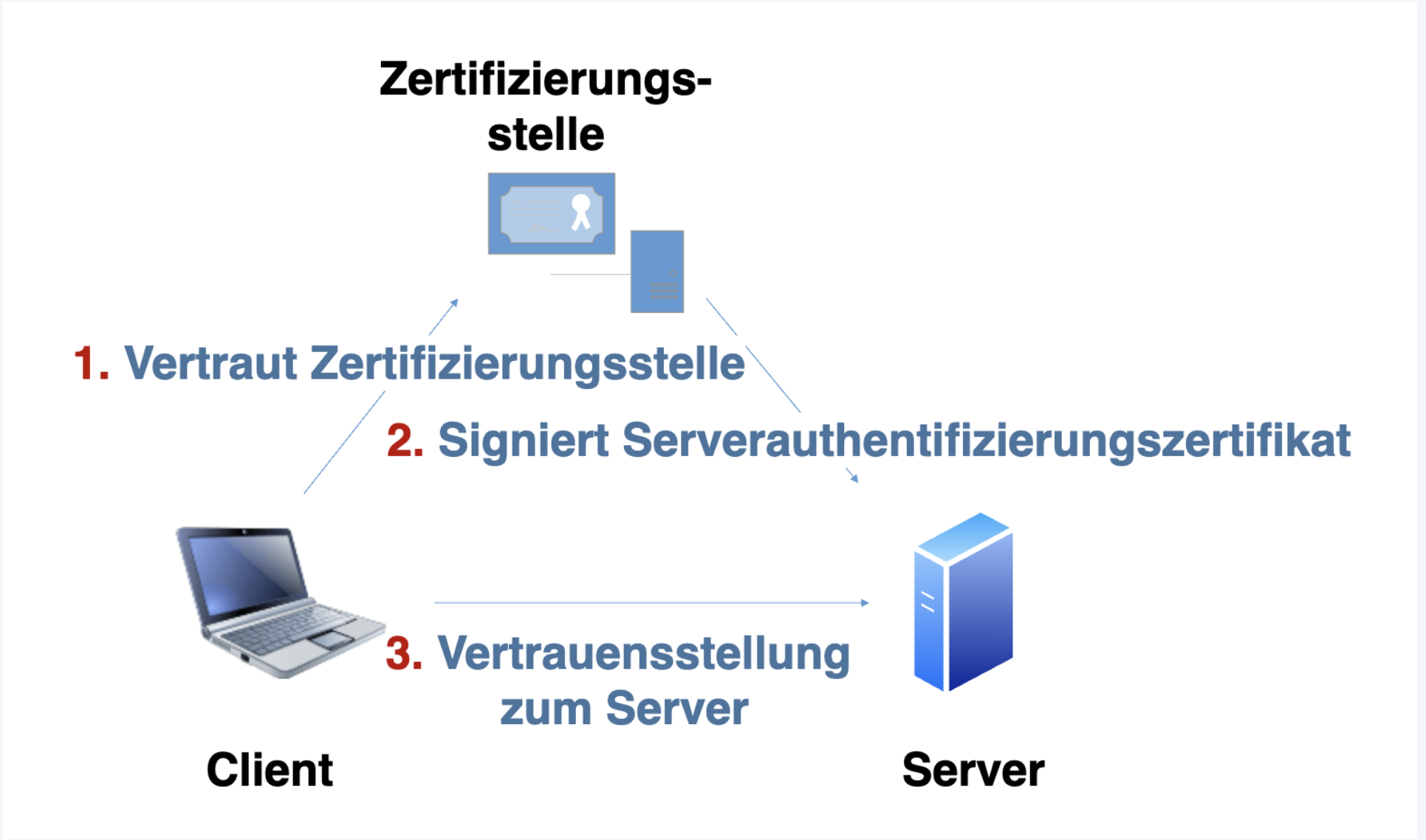
- Client Hello = Vorschlag TLS-Version & Cipher Suites
  - tls.handshake.type == 1
- Server Hello = Annahme/Ablehnung TLS-Version & Cipher Suites, Zufallszahl & Übersendung TLS-Zertifikat
  - tls.handshake.type == 2
- Client Key Exchange = Pre-Master Secret wird übersendet
  - tls.handshake.type == 16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



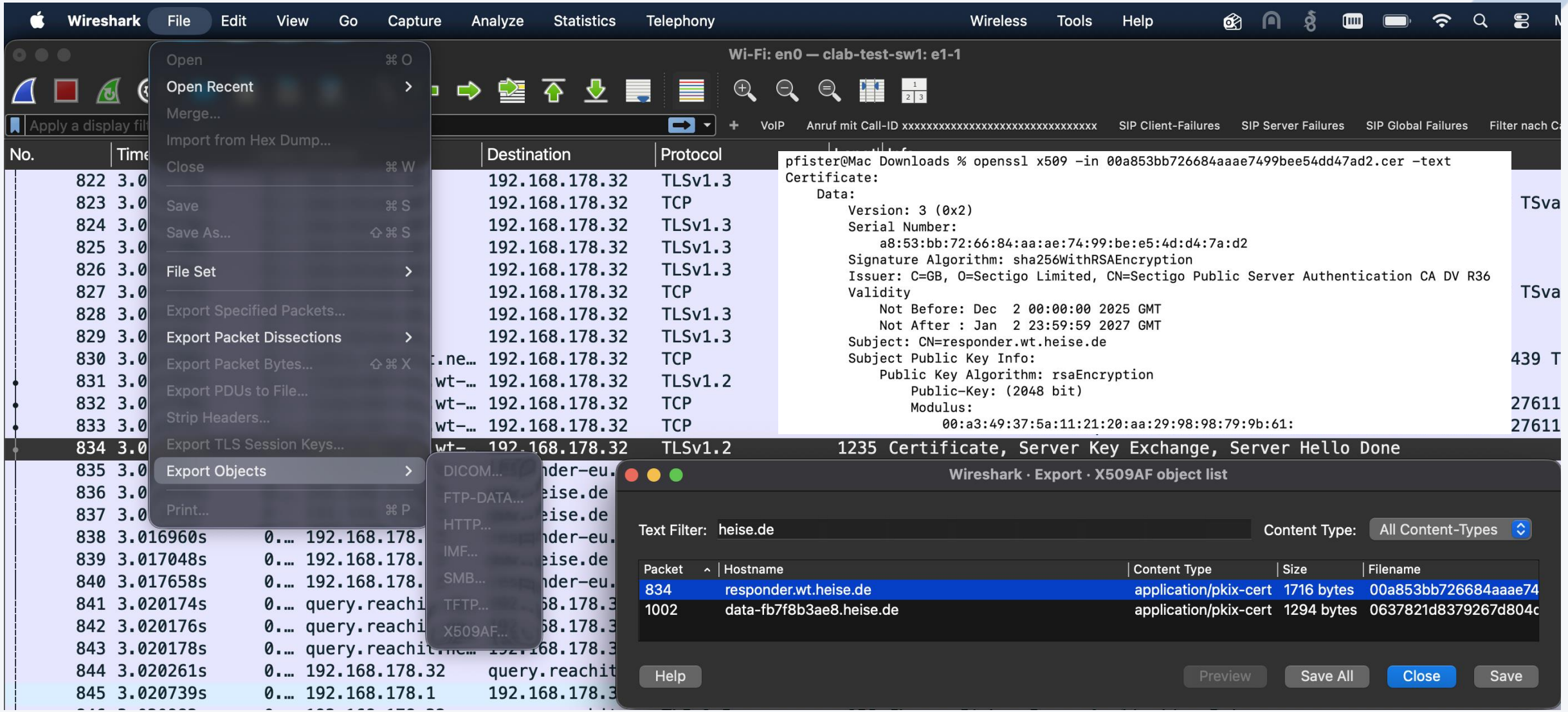
TLS-Handshake | Ciphers



TLS-Handshake | Zertifikate



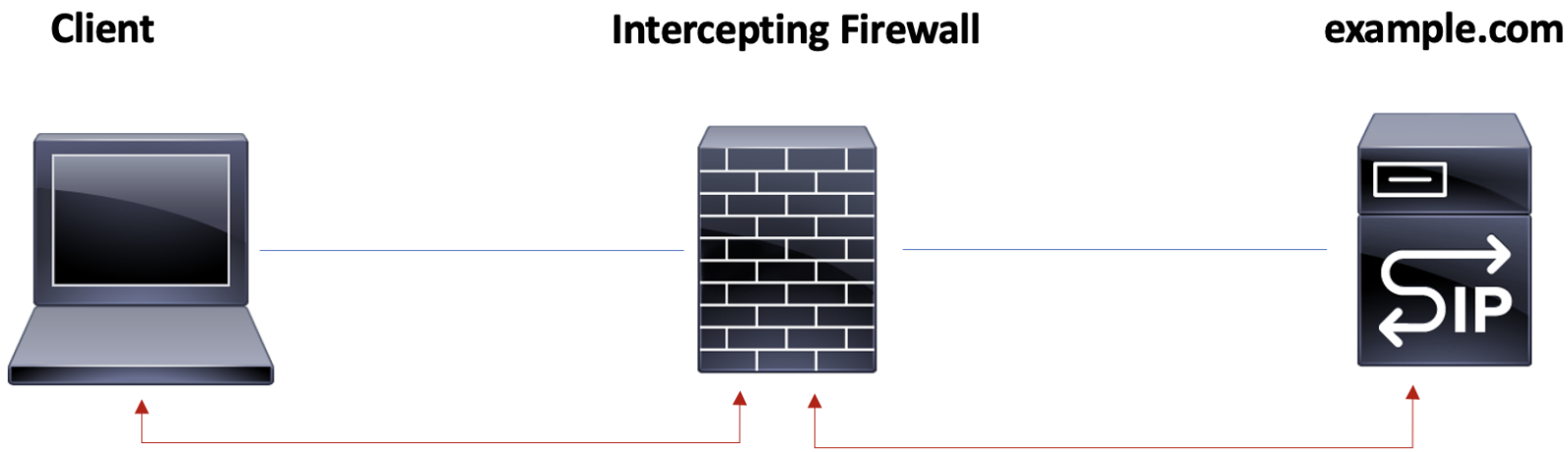
TLS-Handshake | Zertifikate



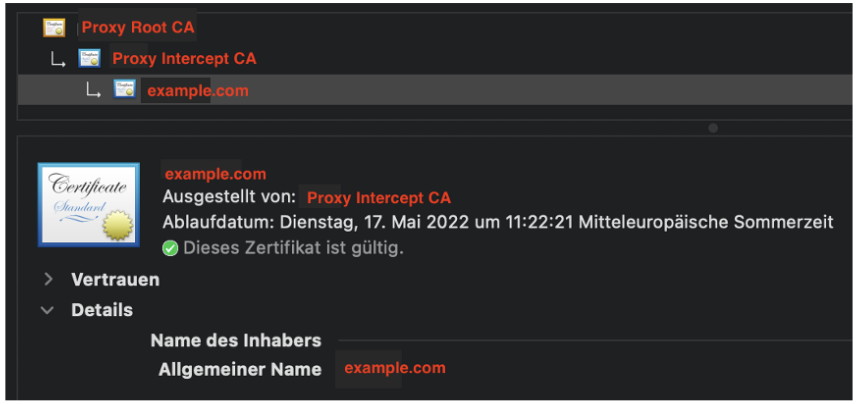
TLS Interception

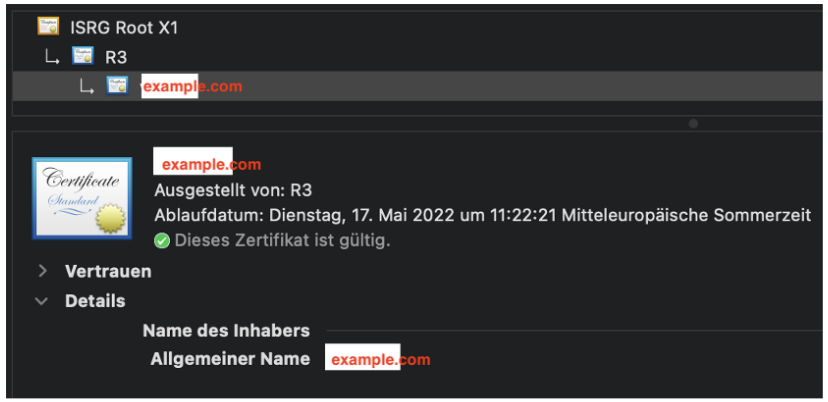
TLS-Handshake | Zertifikate bei Interception

Client muss Proxy Root CA als vertrauenswürdige CA bekannt sein

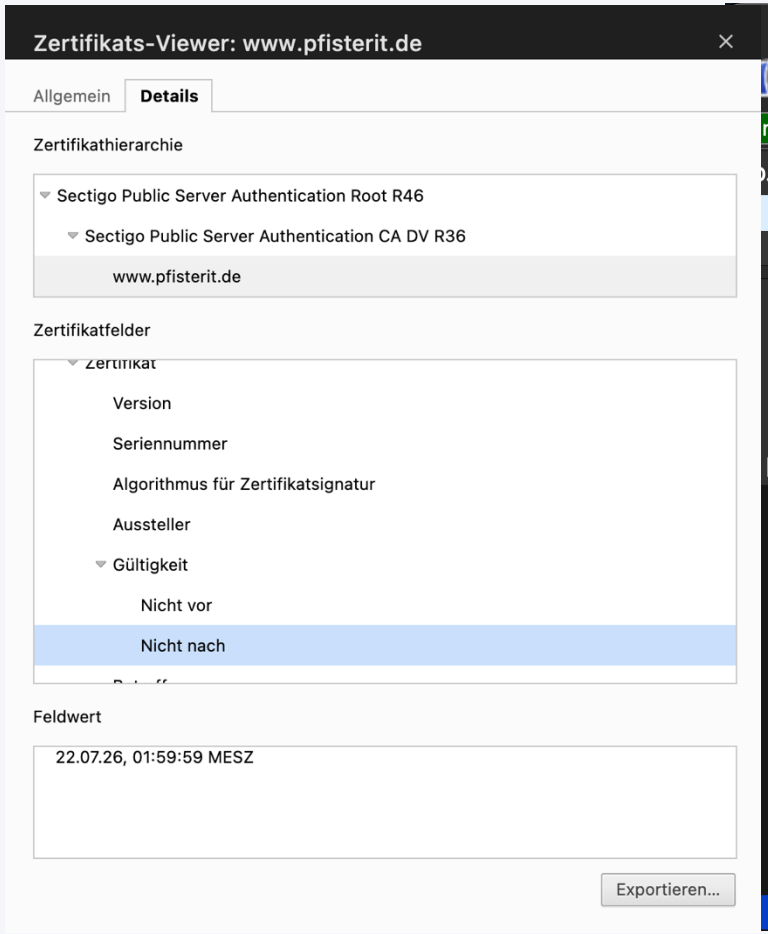


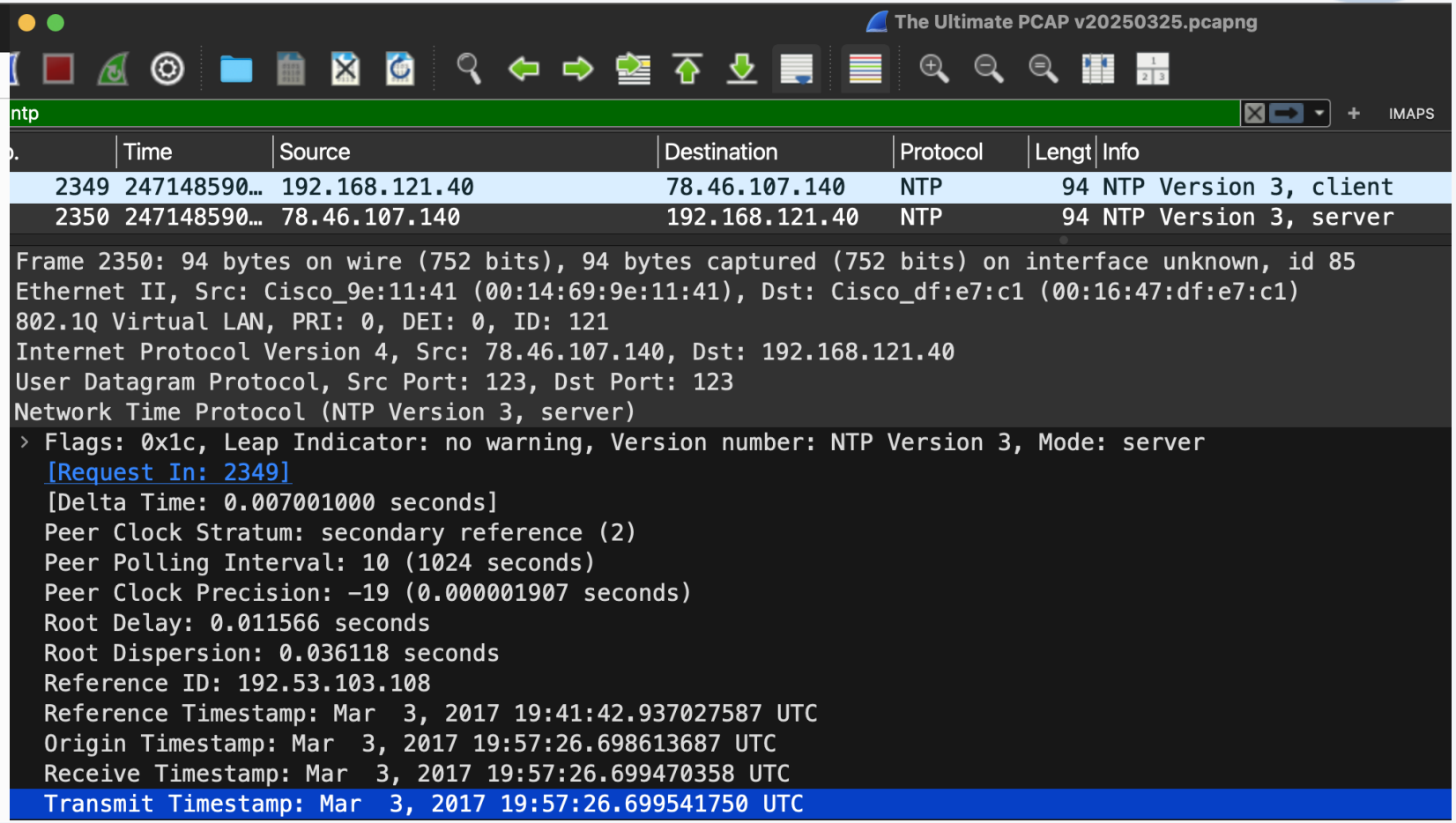
Firewall bricht TLS-Session auf und tauscht Serverauthentifizierungszertifikat.





TLS-Handshake | NTP





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
---
```

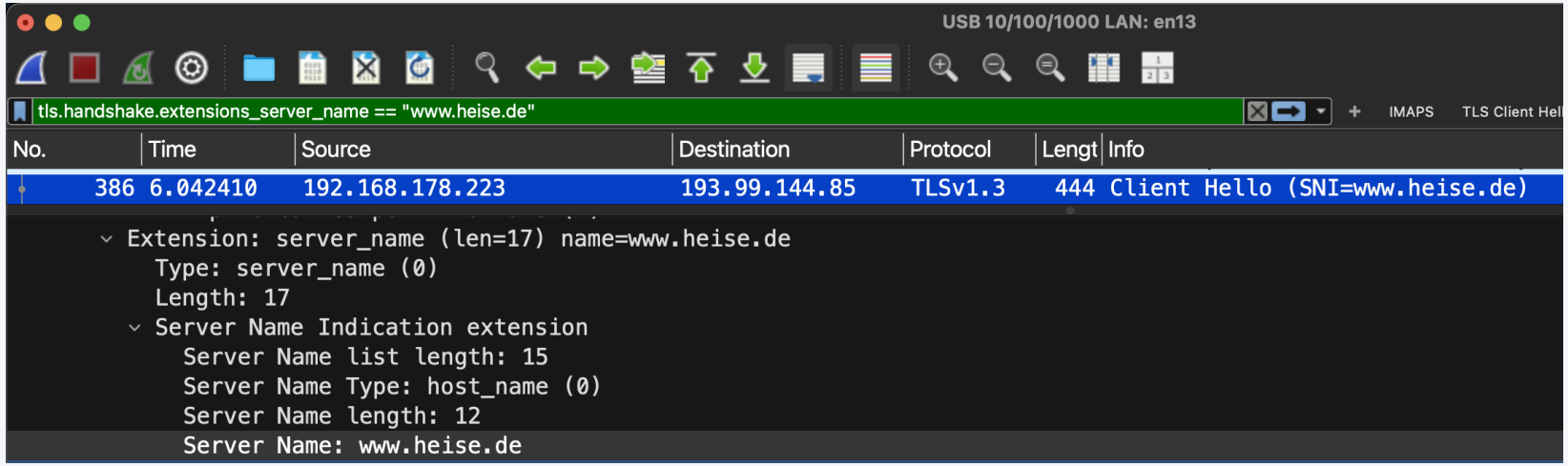
Test TLS Handshake


```
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

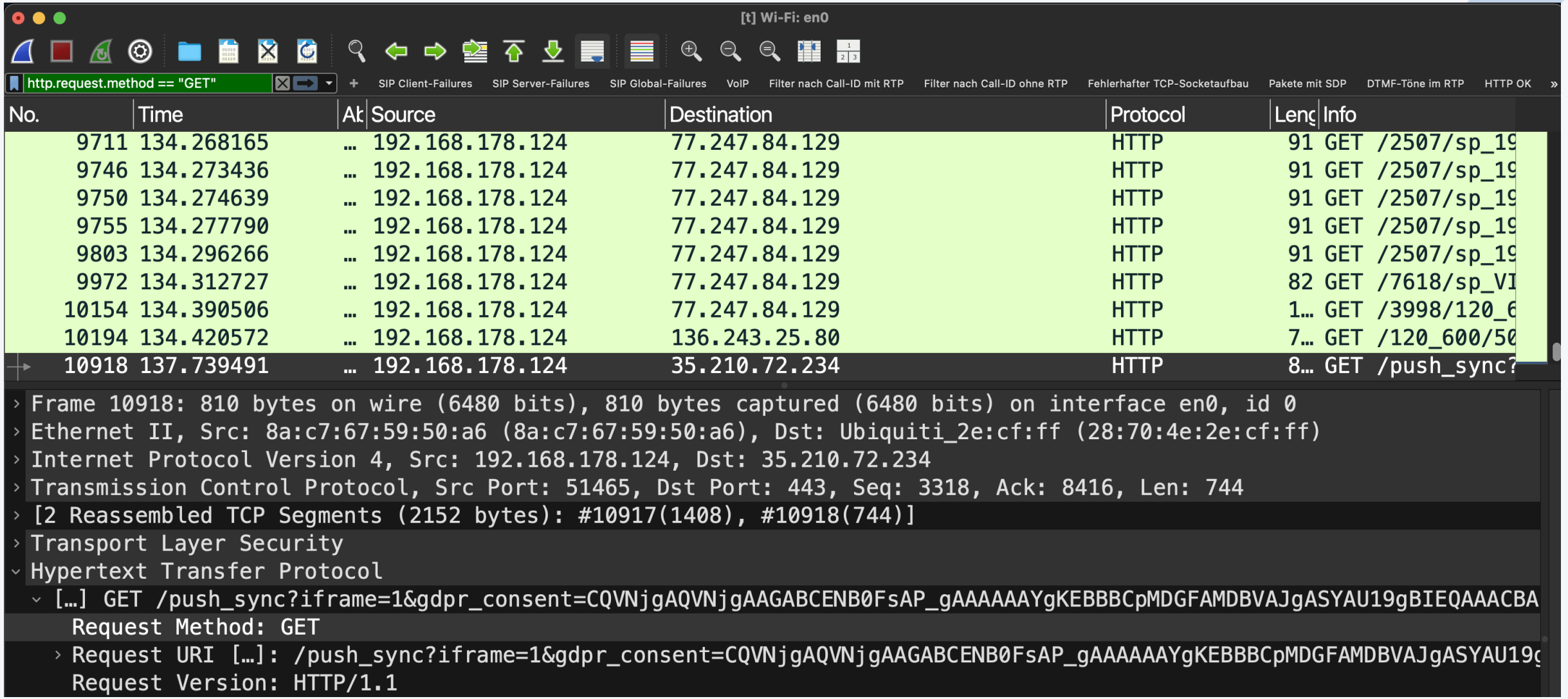


Erkennung Zielhosts trotz Verschlüsselung

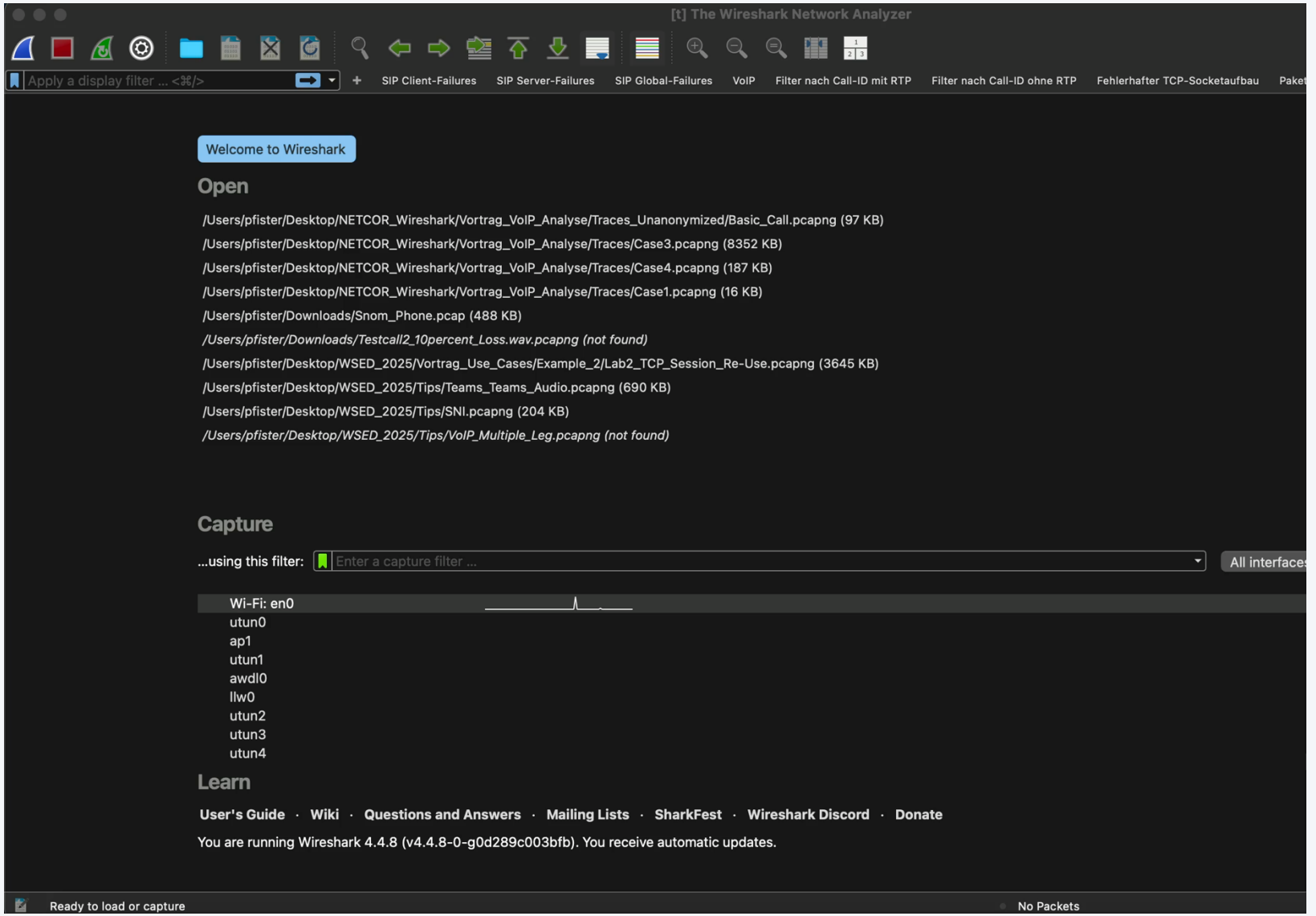
- DNS-Antwort auf A-Record
  - Vorwärts
    - dns.resp.name contains "heise.de“
  - Rückwärts
    - dns.a == 192.0.2.1

TLS-Entschlüsselung mit Session Key Methode

TLS-Entschlüsselung mit Session Key Methode



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