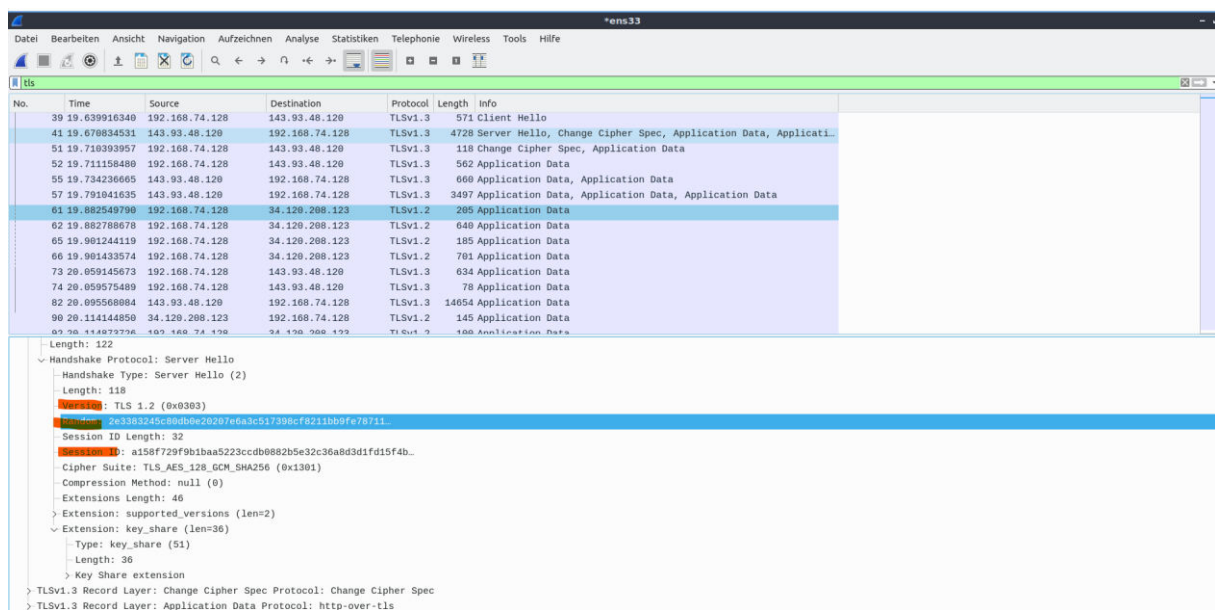


#### 14. Aufgabe: SSL in Wireshark

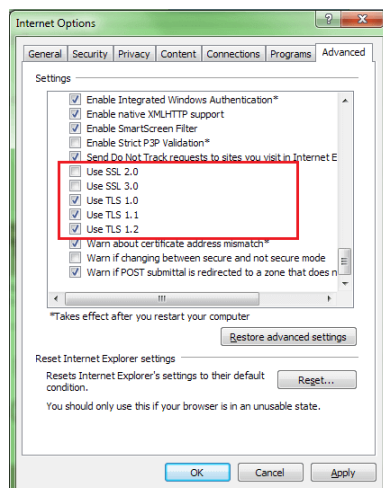
Zeichnen Sie den Zugriff auf die Seite <https://studip.hochschule-trier.de> mit Wireshark auf und beantworten Sie folgende Fragen:

- Wo finden Sie die verwendete SSL-Version im Mitschnitt? Wie können Sie die Version in Ihrem Browser konfigurieren?
- Zeigen Sie die im Handshake verwendeten Noncen.
- Zeigen Sie die im Handshake verwendete SessionID.
- Zeigen Sie die vorgeschlagenen Ciphersuites und die getroffene Auswahl. Wo können Sie die Vorschläge in Ihrem Browser konfigurieren?
- Zeigen Sie die vorgeschlagenen Komprimierungsverfahren und die getroffene Auswahl.
- Zeigen Sie alle ausgetauschten Zertifikate.
- Zeigen Sie die verwendeten Parameter der elliptischen Kurven (falls verwendet).
- Zeigen Sie die ausgetauschten Nachrichten des DH-Schlüsselaustauschs (falls vorhanden).

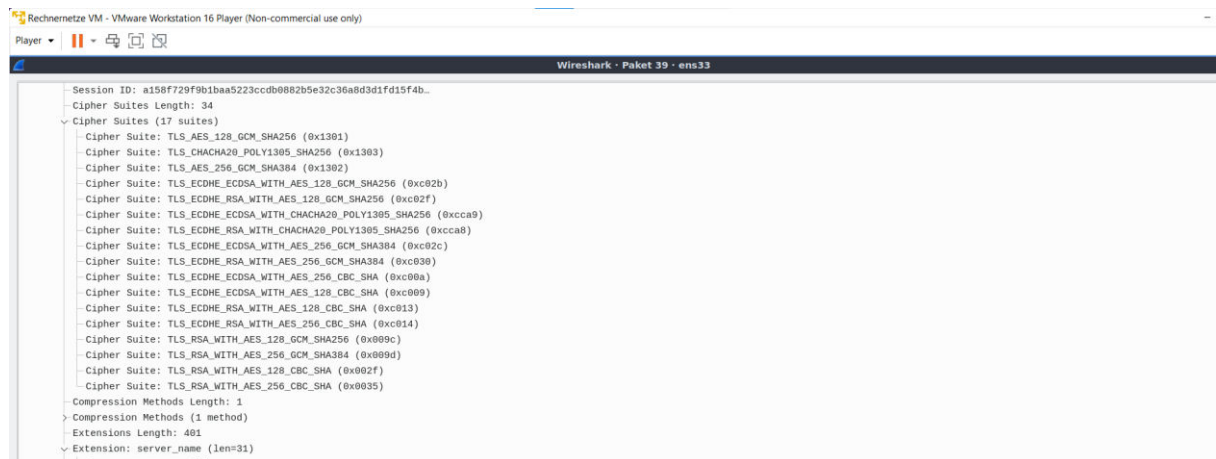
1,2 und 3 siehe rot



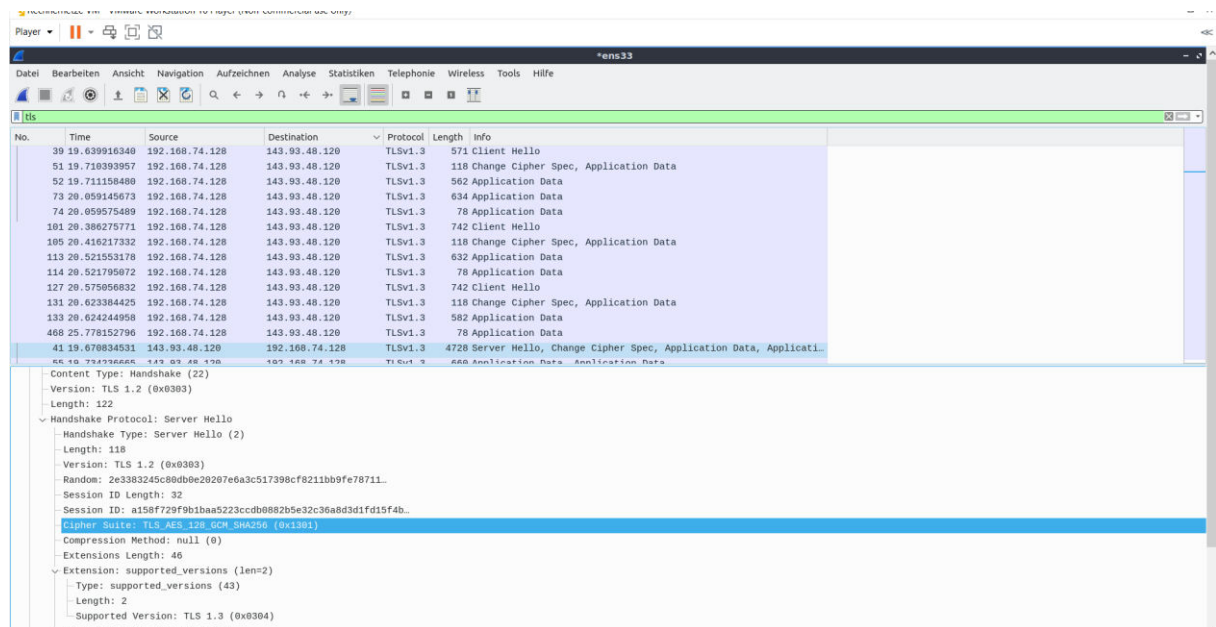
In Google



## 4. Auswahl client



## Schlussendlich gewählte



## In Google

Über eine **Blacklist** müssen die Cipher als Parameter direkt beim Start übergeben werden. Entsprechende Hexcodes müssen zunächst aus dem Quellcode extrahiert werden.

## Bsp

```
chrome --cipher-suite-  
blacklist=0x0001,0x0002,0x0004,0x0005,0x0017,0x0018,0xc002,0xc007,  
0xc00c,0xc011,0xc016,0xff80,0xff81,0xff82,0xff83
```

Es wird kein Komprimierungsverfahren verwendet

Rechneretze VM - VMware Workstation 16 Player (Non-commercial use only)

Player

tls

No.	Time	Source	Destination	Protocol	Length	Info
39	19.639916340	192.168.74.128	143.93.48.120	TLSv1.3	571	Client Hello
41	19.670834531	143.93.48.120	192.168.74.128	TLSv1.3	4728	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
51	19.710393957	192.168.74.128	143.93.48.120	TLSv1.3	118	Change Cipher Spec, Application Data
52	19.711158480	192.168.74.128	143.93.48.120	TLSv1.3	562	Application Data
55	19.734236665	143.93.48.120	192.168.74.128	TLSv1.3	660	Application Data, Application Data
57	19.791041635	143.93.48.120	192.168.74.128	TLSv1.3	3497	Application Data, Application Data, Application Data
61	19.882549790	192.168.74.128	34.120.208.123	TLSv1.2	205	Application Data
62	19.882788678	192.168.74.128	34.120.208.123	TLSv1.2	640	Application Data
65	19.901244119	192.168.74.128	34.120.208.123	TLSv1.2	185	Application Data
66	19.901433574	192.168.74.128	34.120.208.123	TLSv1.2	701	Application Data
73	20.009145673	192.168.74.128	143.93.48.120	TLSv1.3	634	Application Data
74	20.009575489	192.168.74.128	143.93.48.120	TLSv1.3	78	Application Data
82	20.095560804	143.93.48.120	192.168.74.128	TLSv1.3	14654	Application Data
90	20.114144850	34.120.208.123	192.168.74.128	TLSv1.2	145	Application Data
93	20.114873726	192.168.74.128	34.120.208.123	TLSv1.2	100	Application Data

Length: 512

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 508

Version: TLS 1.2 (0x0303)

Random: 47b79f32d0b089eb7d1a91e3d8a333d491a723b0e2b28eec..

Session ID Length: 32

Session ID: a1b8f729f9b1baa5223ccdb0882b5e32c36a8d3d1fd15f4b..

Cipher Suites Length: 34

Cipher Suites (17 suites)

Compression Methods Length: 1

Compression Methods (1 method)

Compression Method: null (0)

Extensions Length: 401

Extension: server\_name (len=31)

Type: server\_name (0)

Length: 31

Server Name Indication extension

Extension: extended\_master\_secret (len=0)

Type: extended\_master\_secret (23)

Befehl **Certificate:**

*ssl.handshake.type == 11*

Rechneretze VM - VMware Workstation 16 Player (Non-commercial use only)

Player

timv1.pcapng

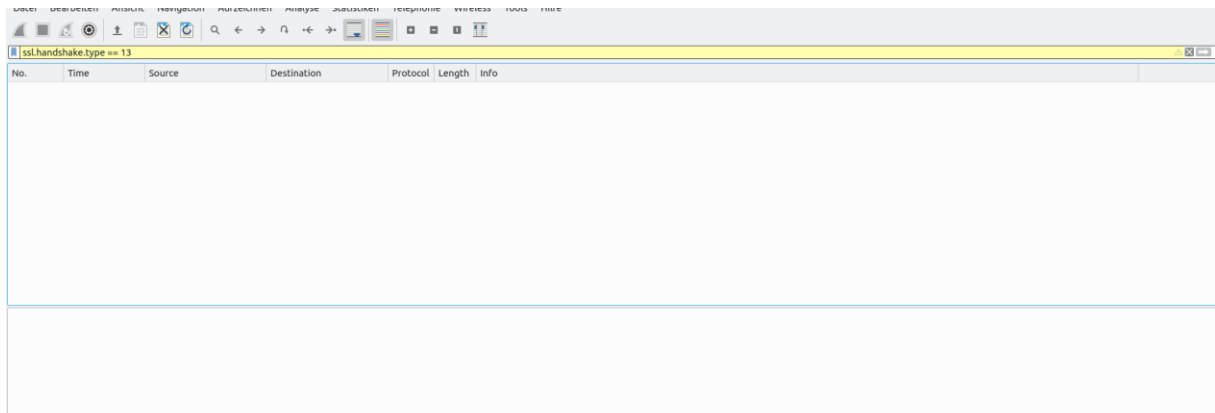
Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

ssl.handshake.type == 11

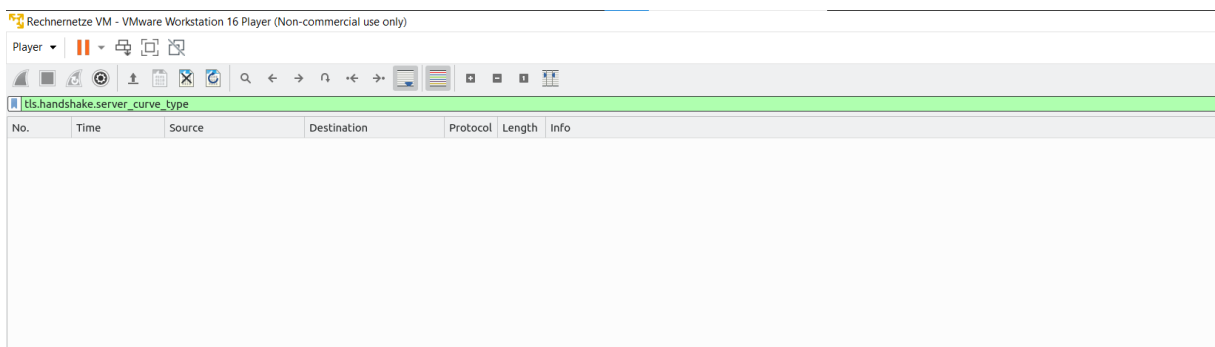
No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

**CertificateRequest**

`ssl.handshake.type == 13`



Es wurden keine Zertifikate übermittelt oder angefragt. Dieser Schritt ist Optional



Der filter zeigt mir alle packages mit ECC an. Es wird also keine verwendet

Rechnernetze VM - VMware Workstation 16 Player (Non-commercial use only)

Player ▾ || 🖨️ 📄 📶

Wireshark · Paket 41 · timv1.pcapng

- Supported Version: TLS 1.3 (0x0304)
  - Extension: key\_share (len=36)
    - Type: key\_share (51)
      - Length: 36
    - Key Share extension
      - Key Share Entry: Group: x25519, Key Exchange length: 32
        - Group: x25519 (29)
          - Key Exchange Length: 32
          - Key Exchange: d7e85891f109f0693027dbbc8ac9bc3664e01f87de162740...
  - TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    - Content Type: Change Cipher Spec (20)
      - Version: TLS 1.2 (0x0303)
        - Length: 1
      - Change Cipher Spec Message
    - TLSv1.3 Record Layer: Application Data Protocol: http-over-tls
      - Opaque Type: Application Data (23)
        - Version: TLS 1.2 (0x0303)
          - Length: 42

0090	24 00 1d 00 20 d7 e8 58 91 f1 09 f0 60 30 27 bd	\$... ..X...0..
00a0	ac 8a c9 bc 30 14 c9 17 0c 10 27 00 00 77 11	...6d...{bwc
00b0	20 1f 69 c0 a8 14 03 03 00 01 01 17 03 03 00 2a	0b... ..
00c0	05 bd 58 41 c8 f2 f6 76 c7 7d 18 6f fe 19 17 a0	..XA...v...o...
00d0	5c 11 58 8e 69 40 0c 1e ba 40 db c8 66 2a 18 45	\.X.iF...@..f*.E
00e0	13 24 0a fe 08 af 11 2d ad 71 17 03 03 10 31 ee	.\$..h...q...1.
00f0	e8 e5 b5 ae 71 d5 38 dd 59 d1 8a 29 03 f2 e1 f5	...q-B.Y...)
0100	f8 e9 ae d3 dc ea 0a 7c 04 df 6e 01 fa 8f e7 ac	..... ..n....
0110	33 39 05 27 39 73 26 28 ba 35 5c a6 1b 33 44 d5	39..9s&(-5...3D.

Könnte auch sein das keine verschickt wurden wenn nicht danach gefragt wurde da