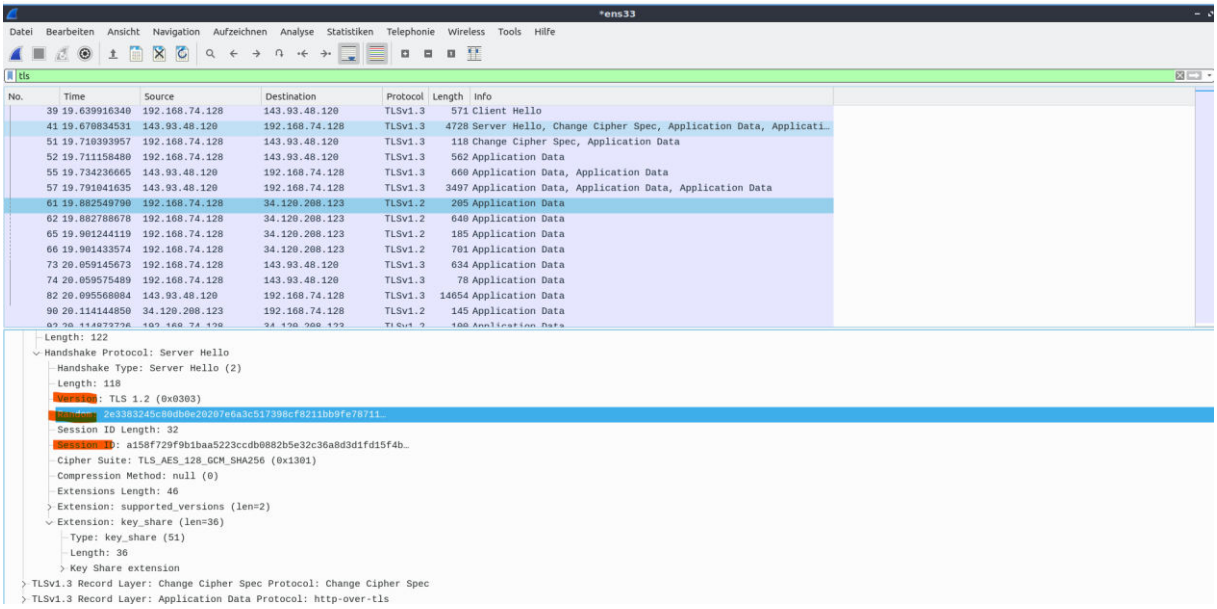
14. Aufgabe: SSL in Wireshark

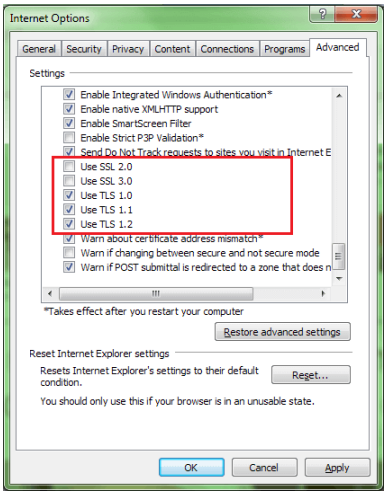
Zeichnen Sie den Zugriff auf die Seite https://studip.hochschule-trier.de mit Wireshark auf und beantworten Sie folgende Fragen:

- 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).

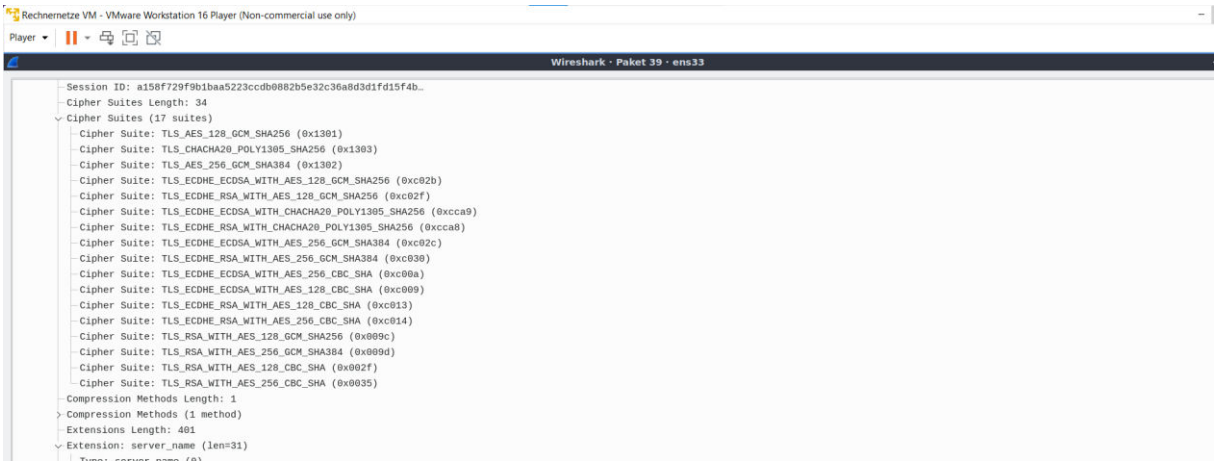
1,2 und 3 siehe rot



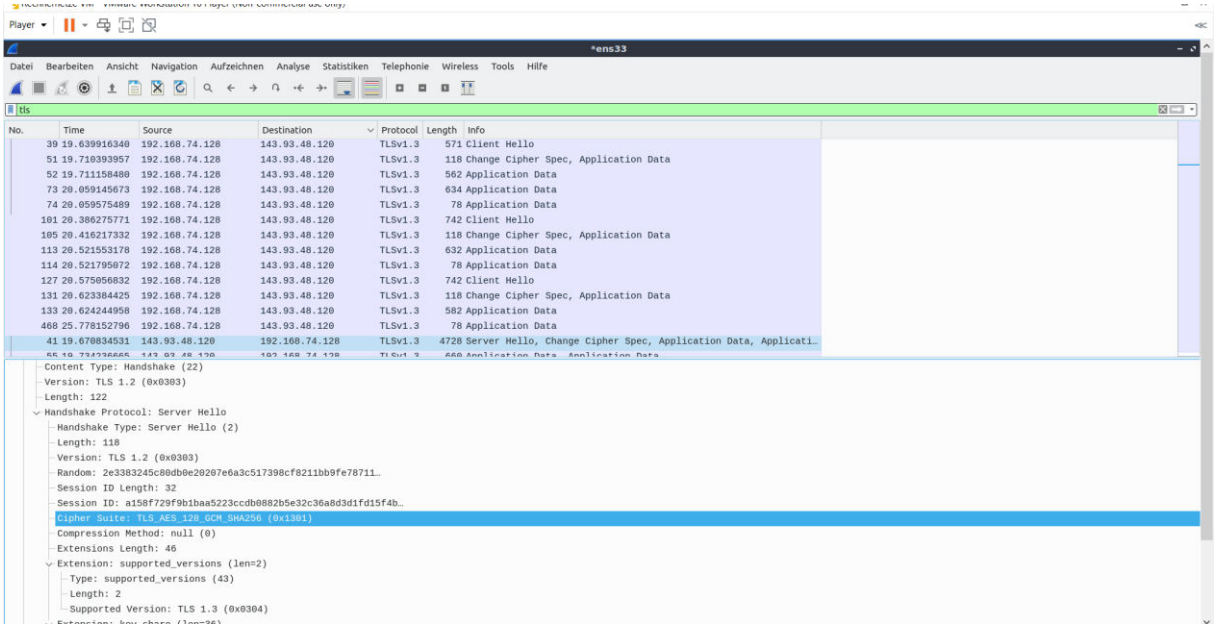
In Google



4. Auswahl client



Schlussendlich gewählte



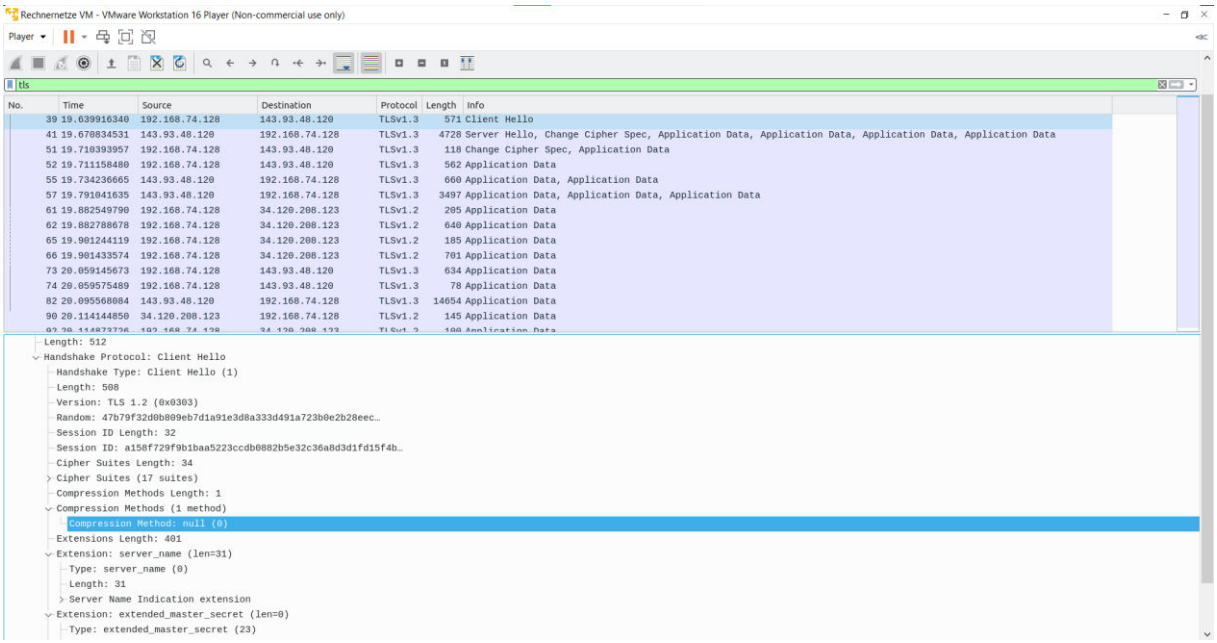
In Google

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

Bsp

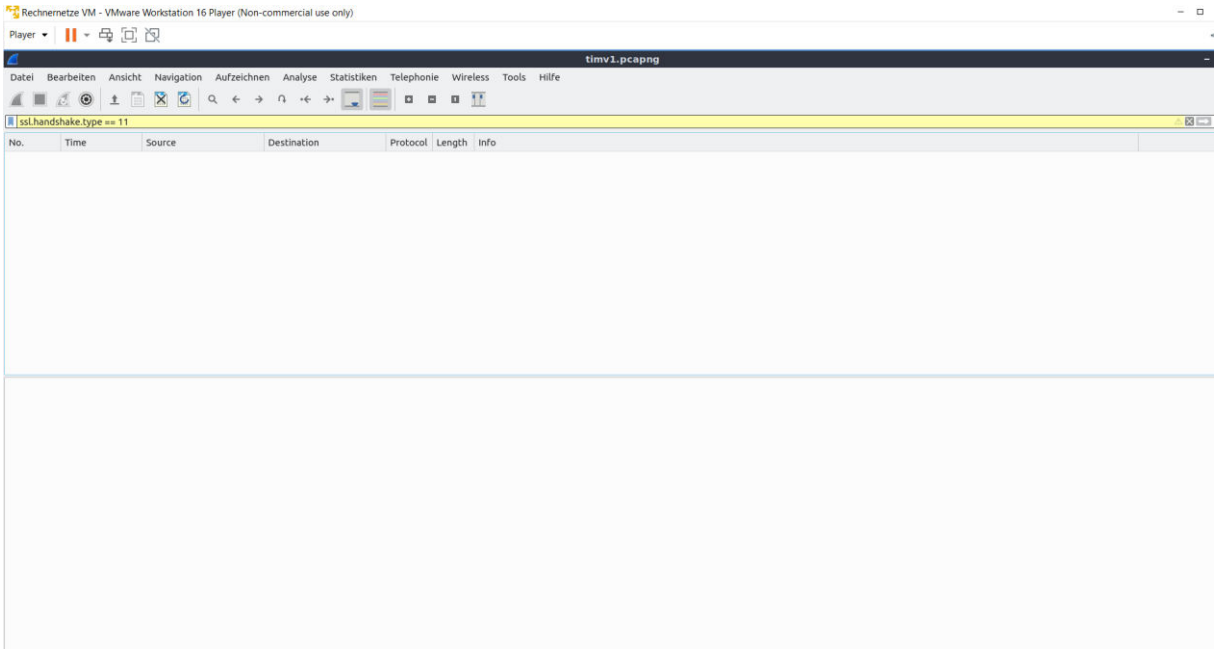
```
chrome --cipher-suite-
blacklist=0x0001,0x0002,0x0004,0x0005,0x0017,0x0018,0xc002,0xc007
,0xc00c,0xc011,0xc016,0xff80,0xff81,0xff82,0xff83
```

Es wird kein Komprimierungsverfahren verwendet



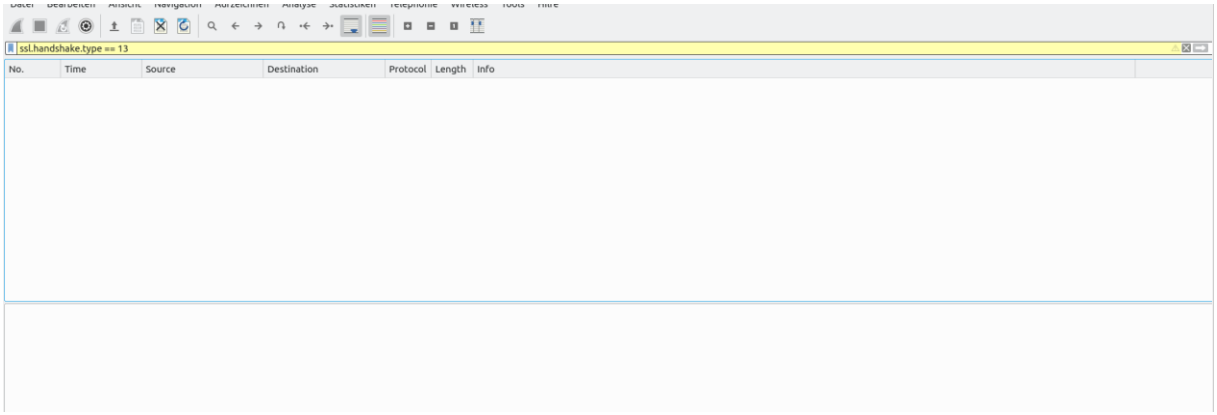
Befehl **Certificate:**

ssl.handshake.type == 11

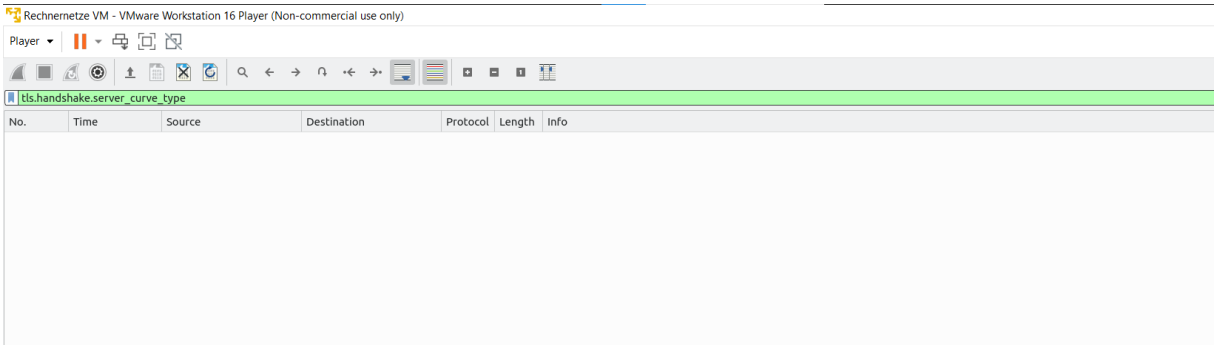


CertificateRequest

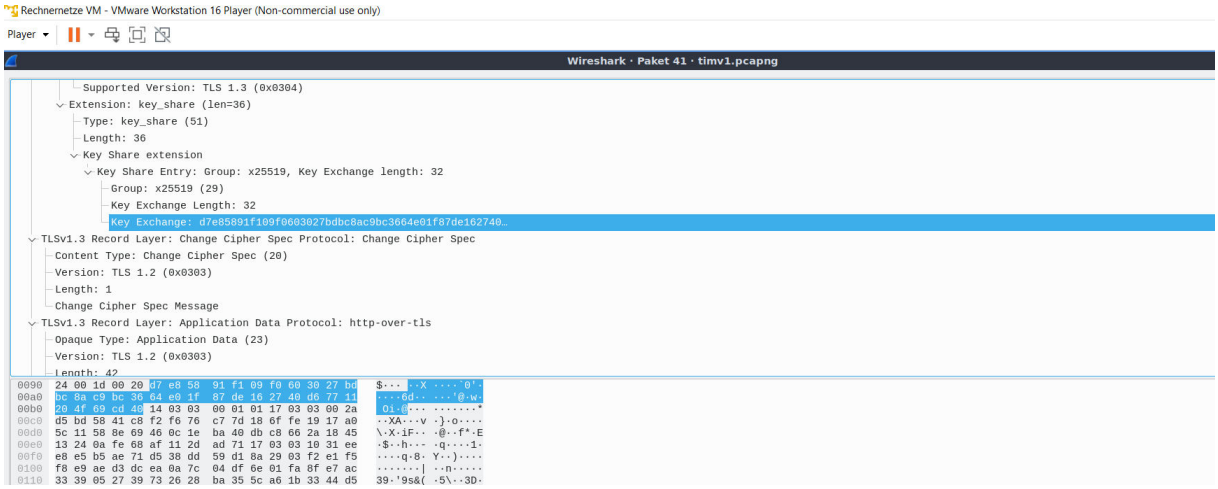
ssl.handshake.type == 13



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



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