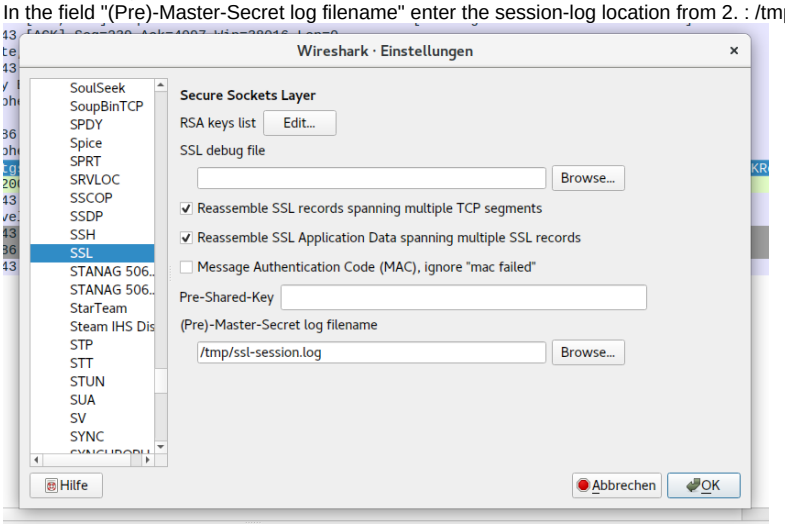
1 Inspecting HTTPS communication between TextGridLab and server with Wireshark

As the communication between TextGridLab and Server is encrypted with TLS using ECDHE (or DHE as fallback) for Key-Exchange, its not directly sniffable with Wireshark. To observe the HTTP traffic one needs to get hold of the SSL session keys. This is possible by adding java libraries like jSSLKeyLog or extract-ssl-secrets to the TextGridLab startup. This will drop the SSL session keys to a place where Wireshark could use them for TLS decryption. Here is how its done, with extract-ssl-secrets.jar as an example, jSSLKeyLogin.jar usage is analogous:

1. Download https://github.com/neykov/extract-ssl-secrets/releases/download/v2.0.0/extract-ssl-secrets-2.0.0.jar
2. Edit the textgridlab.ini, add a line

```
-javaagent:/path-to/extract-ssl-secrets-2.0.0.jar=/tmp/ssl-session.log
```

3. In Wireshark: go to EditPreferences, from Protocols choose SSL
4. In the field "(Pre)-Master-Secret log filename" enter the session-log location from 2. : /tmp/ssl-session.log



5. start a capture to textgridlab.org, the following capture filter should do: "tcp port https and host textgridlab.org"
6. start the TextGridLab and observe the traffic