Wireshark workshop cheatsheet

Sources:

https://www.wireshark.org/

Time format:

View -> Time Display Format

Decoding rules:

Analyze -> Decode As …

Analyze -> User Specified Decodes

Following Stream:

Analyze -> Follow TCP Stream

Analyze -> Follow SSL Stream

Display filter:

- http
- ssl
- tcp.port==5022
- ip.addr==10.0.5.65
- http.response.code >= 403
- ssl.record.version==0x0301
- ip.addr==10.0.13.81 and ssl
- tcp.port==443 || http
- not http and not ssl

Capture filter:

- ip
- ip6
- port 8050
- host 10.0.5.65
- not port 22
- tcp port 80 or tcp port 443
- not port 80 and not port 25 and host www.wireshark.org

SSL/TLS decryption:

Server private key (when DH/ECDH not used):

Edit -> Preferences -> Protocols -> SSL -> RSA keys list

Pre-Master Secret when using Firefox or Chrome:

User variable SSLKEYLOGFILE

Edit -> Preferences -> Protocols -> SSL -> (Pre)-Master-Secret log file