# Webservices

## HTTP-Header analysieren

Das geht am einfachsten mittels **curl** auf einem Linux:

```
# curl -Is https://www.google.de
```

Antwort:

```
HTTP/1.1 200 OK
Date: Sat, 07 Dec 2019 17:10:55 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
Server: gws
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: 1P_JAR=2019-12-07-17; expires=Mon, 06-Jan-2020 17:10:55 GMT;
path=/; domain=.google.de
Set-Cookie: NID=193=aFX44JBE-vFTxbutUsfqQU0d7_kl3oJf-
xXp8iLHaJdMy9wcXVPOgBLeLIXNdO-PWsW-U_h___zJcsWKwkqW1z68f4PdeDTXlX0UpwCHZ-
t9j1j4k-IEDxkUpKKZyjaqMZM7VAreaLgo_q6iKIZTnHBgoHAsesjF-SduZSCbSew;
expires=Sun, 07-Jun-2020 17:10:55 GMT; path=/; domain=.google.de; HttpOnly
Transfer-Encoding: chunked
Alt-Svc: quic=":443"; ma=2592000; v="46,43",h3-Q050=":443"; ma=2592000,h3-
Q049=":443"; ma=2592000,h3-Q048=":443"; ma=2592000,h3-Q046=":443";
ma=2592000,h3-Q043=":443"; ma=2592000
Accept-Ranges: none
Vary: Accept-Encoding
```

## SSL/TLS-Analyse

Ich nutze für die Analyse den OpenSSL-Client.

> https://sourceforge.net/projects/openssl/

### Beispiel unter Windows

```
openssl.exe s_client -connect 192.168.100.173:8080
[...]
---
SSL handshake has read 1287 bytes and written 484 bytes
```

```
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1
    Cipher    : ECDHE-RSA-AES256-SHA
    Session-ID:
5F46000078CFFF3B27D85D4F1531F0321A6749E1B537E8C9D600904CB9E07C3E

    Session-ID-ctx:
    Master-Key:
82D6B5A9127FCA29C0513B75BC0B1221DE300E6481CE99E123A3E606F0AA50EB
21B010838B5C1F5E7A0C769F084FD2A6
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1634114167
    Timeout   : 300 (sec)
    Verify return code: 21 (unable to verify the first certificate)
---
HTTP/1.1 500 Internal Server Error
Server: Webserver/2.35.3.0
Date: Wed, 13 Oct 2021 08:36:17 GMT
Content-Length: 0
Connection: close

read:errno=0
```

From:
https://wikinet.webby.hetzel-netz.de/ - **Sebastians IT-Wiki**

Permanent link:
**https://wikinet.webby.hetzel-netz.de/netzwerk:webservices**

Last update: **2021/10/13 08:49**