HTTP

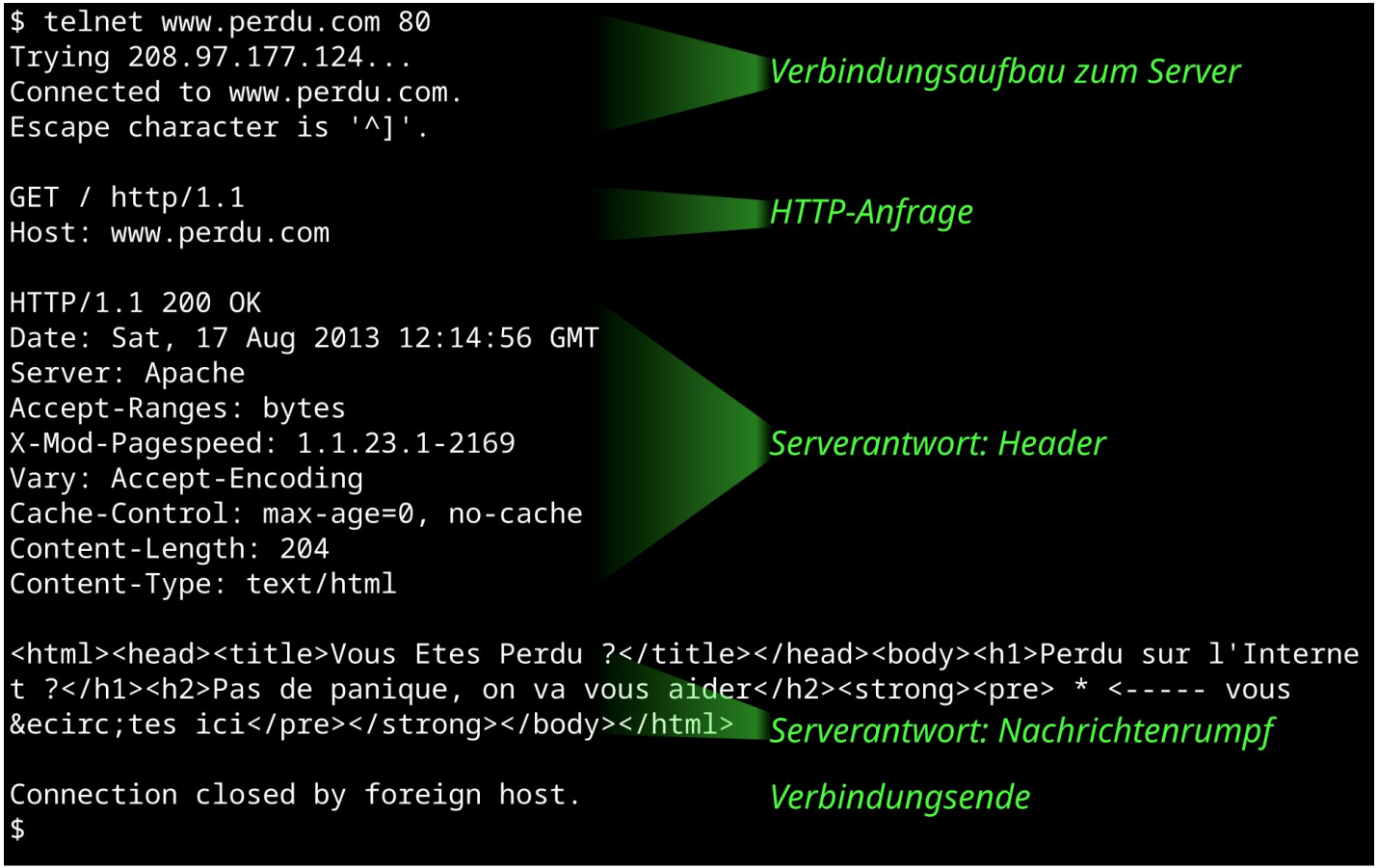
Hypertext Transfer Protocol

Agenda

1. Was ist HTTP?
2. Wie analysiere ich HTTP-Traffic?
3. Wie manipuliere ich Requests?
4. (Eigene Requests mit Python programmieren)

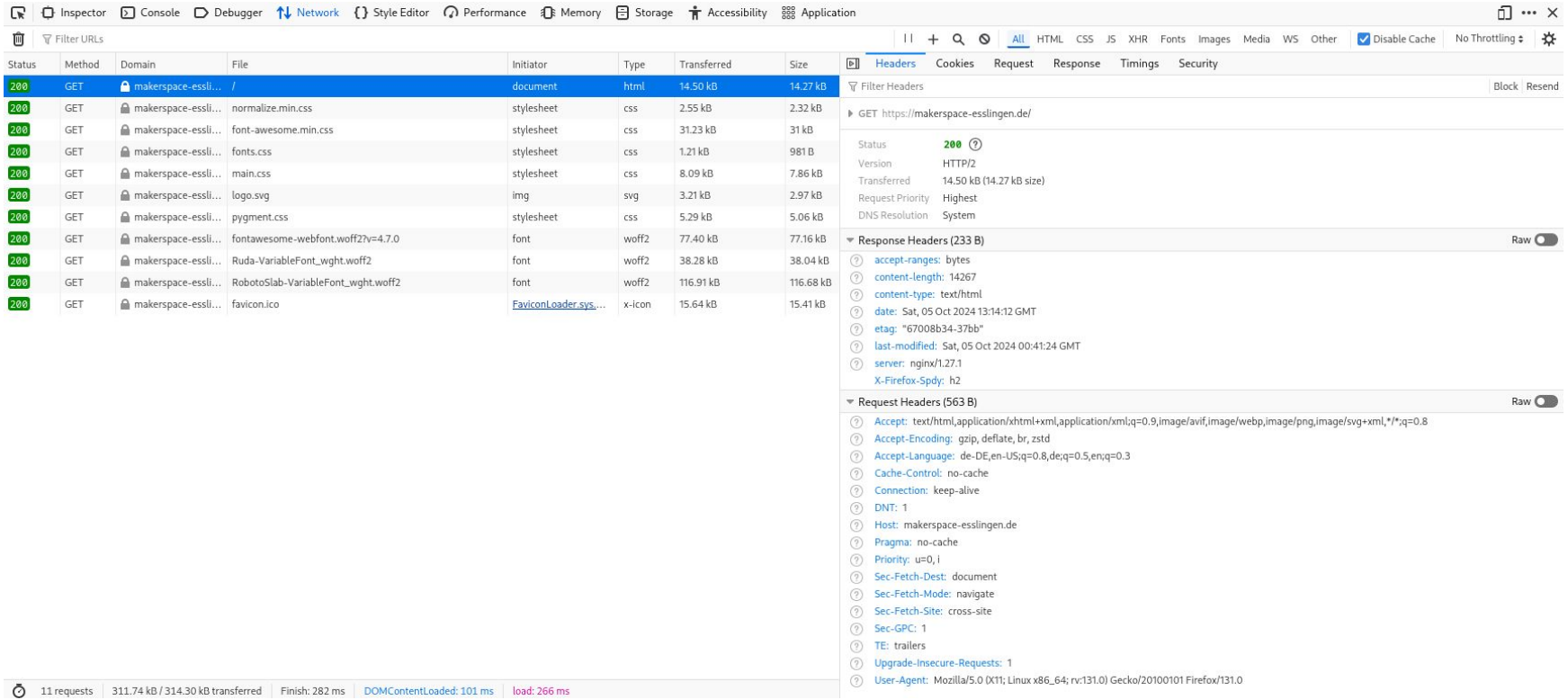
Was ist HTTP?

- Request-Response
  - Client schickt eine Anfrage
  - Server reagiert mit einer Antwort
- Stateless
  - Alle Anfragen sind voneinander unabhängig
  - Server speichert (normalerweise) keine Informationen von vorherigen Anfragen

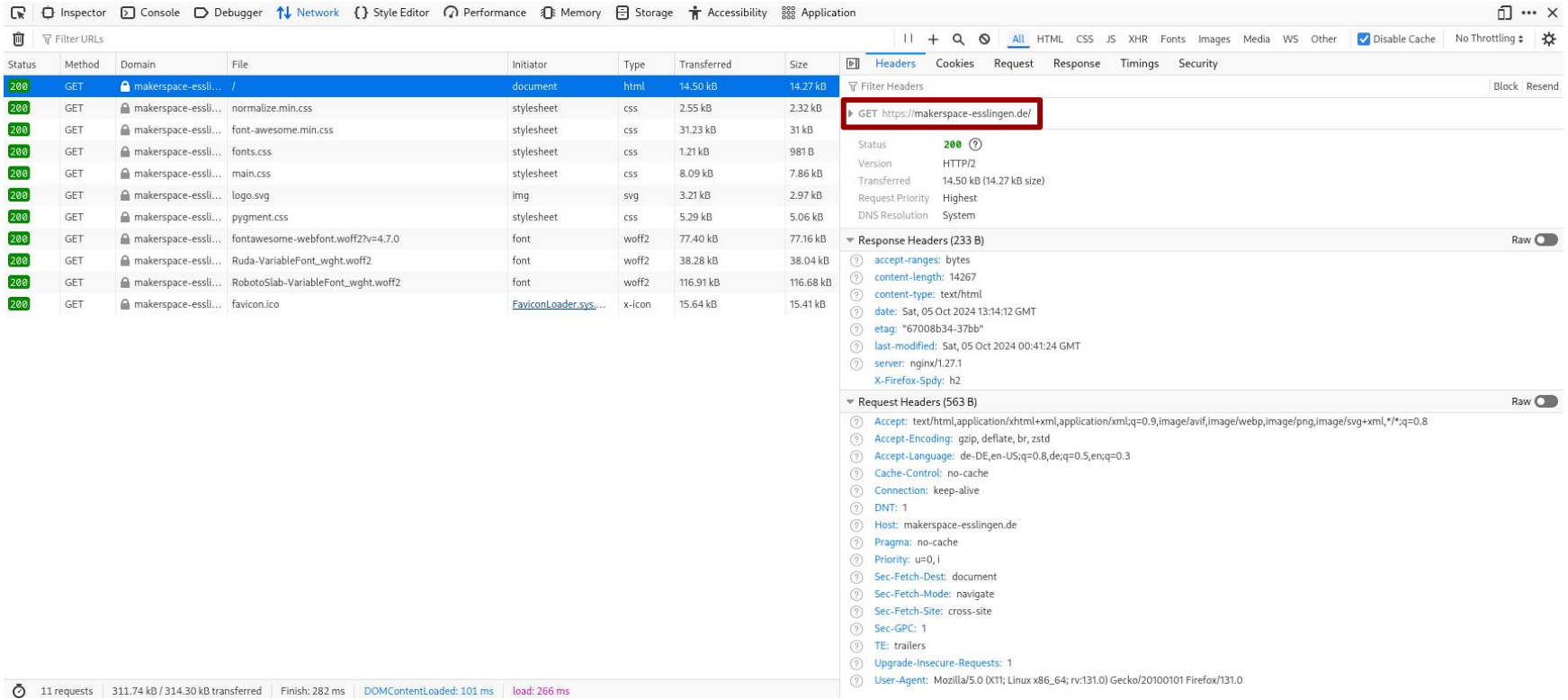


https://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol#/media/Datei:HTTP-Anfrage.svg

Wie analysiere ich HTTP-Traffic?



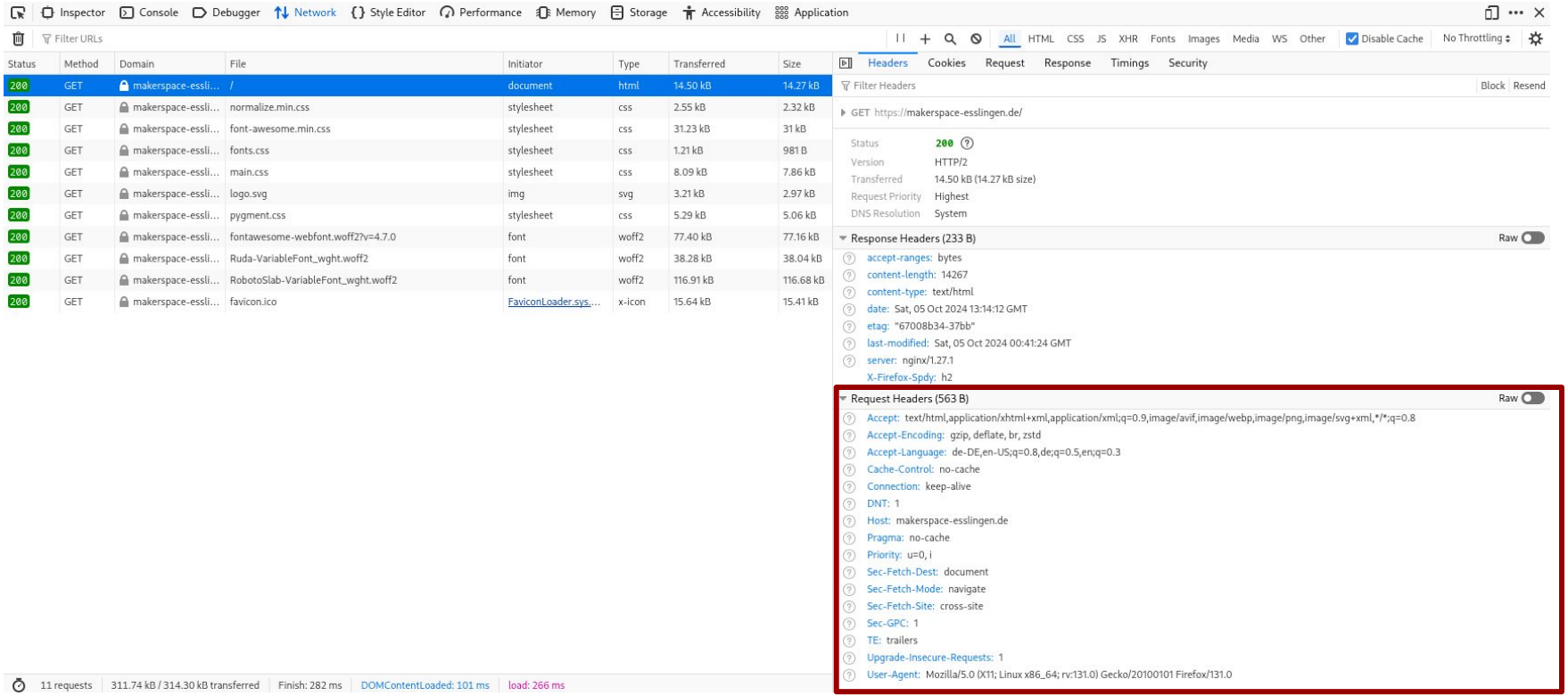
Wie analysiere ich HTTP-Traffic?



Anfragemethoden

- **GET**: Abruf einer Ressource (z. B. einer Webseite).
- **POST**: Übermittlung von Daten an den Server (z. B. bei einem Formular).
- **PUT**: Aktualisierung einer Ressource.
- **DELETE**: Löschen einer Ressource.
- **HEAD**: Abrufen der Metadaten einer Ressource (ohne den eigentlichen Inhalt).
- **PATCH**: Teilweises Update einer Ressource.
- und weitere: **TRACE, OPTIONS, CONNECT**

Wie analysiere ich HTTP-Traffic?



Headers

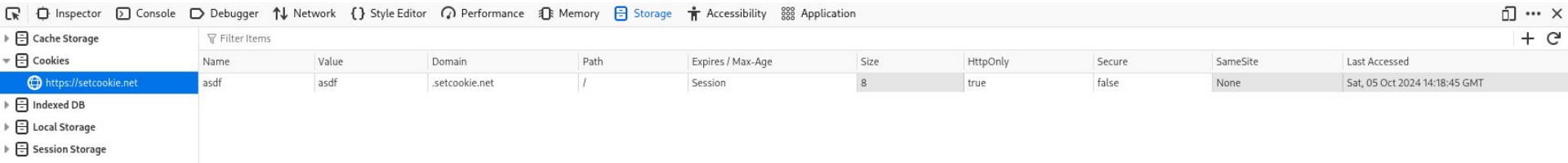
User-Agent: Identifiziert den Client, der die Anfrage stellt (z.B. den Webbrowser).

Content-Type: Gibt an, um welche Art von Daten es sich handelt (z.B. text/html, application/json).

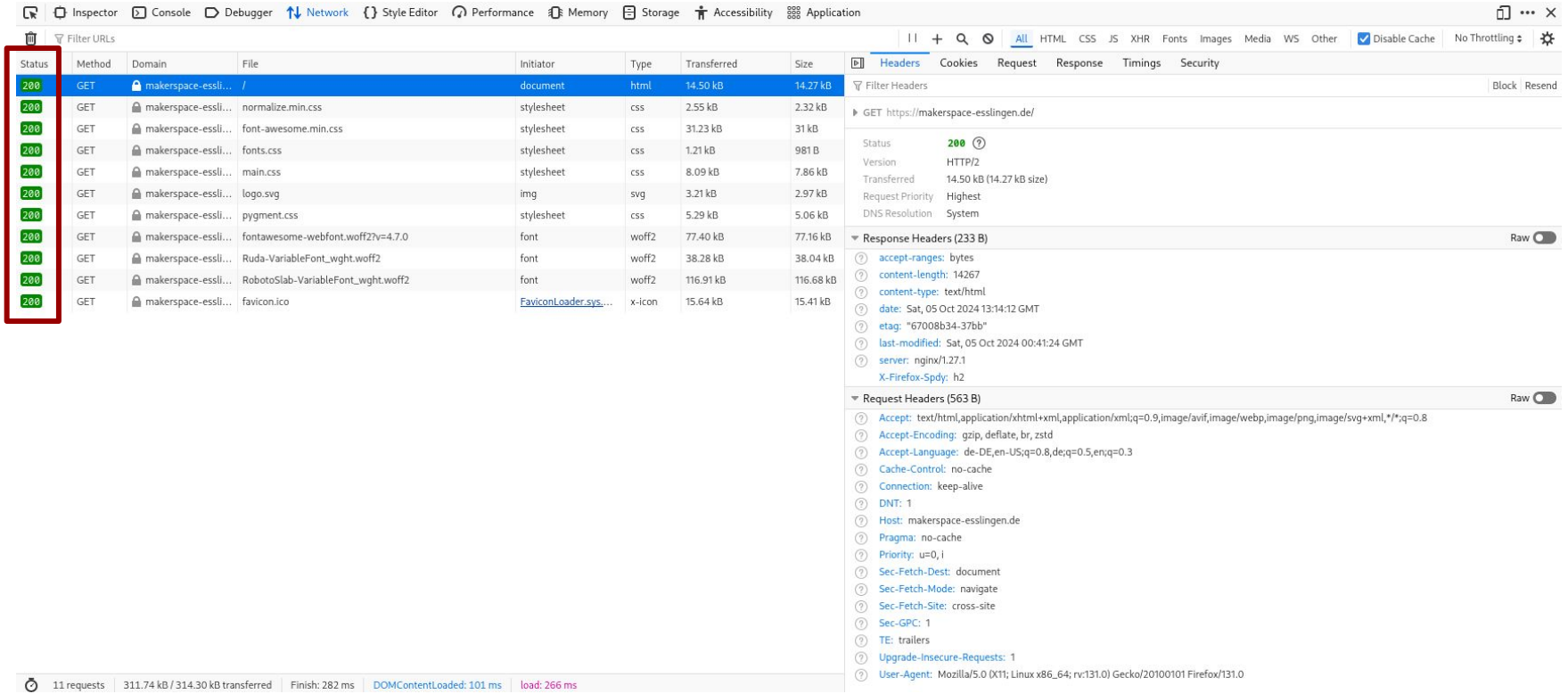
Cookie: Kann Informationen über eine Sitzung oder Benutzereinstellungen enthalten.

und viele weitere…

Cookies


Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cache Storage
Cookies
https://setcookie.net
Indexed DB
Local Storage
Session Storage
Filter Items
Name
Value
Domain
Path
Expires / Max-Age
Size
HttpOnly
Secure
SameSite
Last Accessed
asdf
asdf
.setcookie.net
/
Session
8
true
false
None
Sat, 05 Oct 2024 14:18:45 GMT

Wie analysiere ich HTTP-Traffic?



Statuscodes

1xx - Informationen
2xx - Erfolgreiche Operation
3xx - Umleitung
4xx - Client Fehler
5xx - Server Fehler

Beispiele für Statuscodes

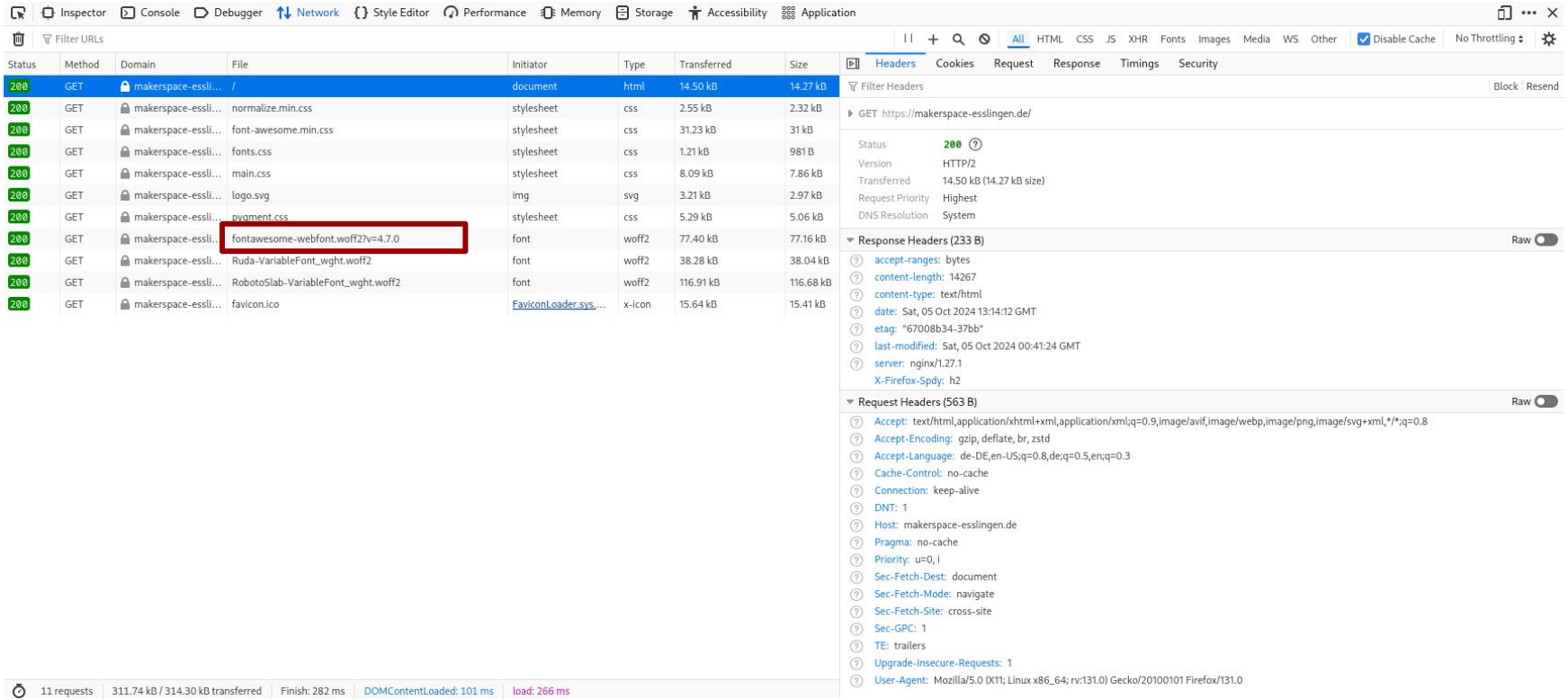
200 OK: Die Anfrage war erfolgreich.

301 Moved Permanently: Die Ressource wurde dauerhaft verschoben.

404 Not Found: Die Ressource wurde nicht gefunden.

500 Internal Server Error: Ein Fehler auf dem Server ist aufgetreten.

Wie analysiere ich HTTP-Traffic?



URL-Parameter

https://makerspace-esslingen.de/theme/fonts/fontawesome-webfont.woff2?v=4.7.0

- Daten als Teil der URL
- ?Parameter1=Wert1&Parameter2=Wert2

Body-Parameter

```
POST /wiki/Spezial:Search HTTP/1.1
Host: de.wikipedia.org
Content-Type: application/x-www-form-urlencoded
Content-Length: 24

search=Katzen&go=Artikel
```

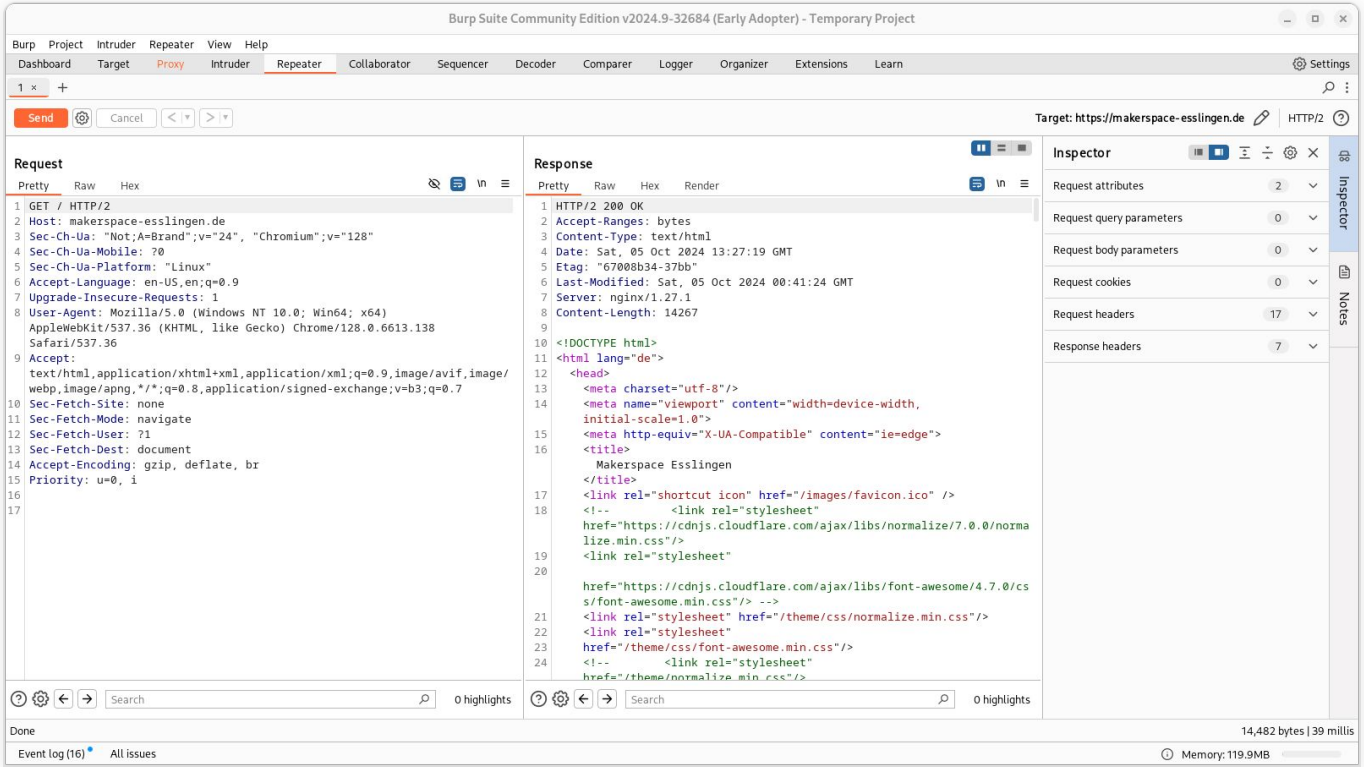
URL-Encoding

https://duckduckgo.com/?q=Schw%C3%B6rfest&t=newext&atb=v406-1

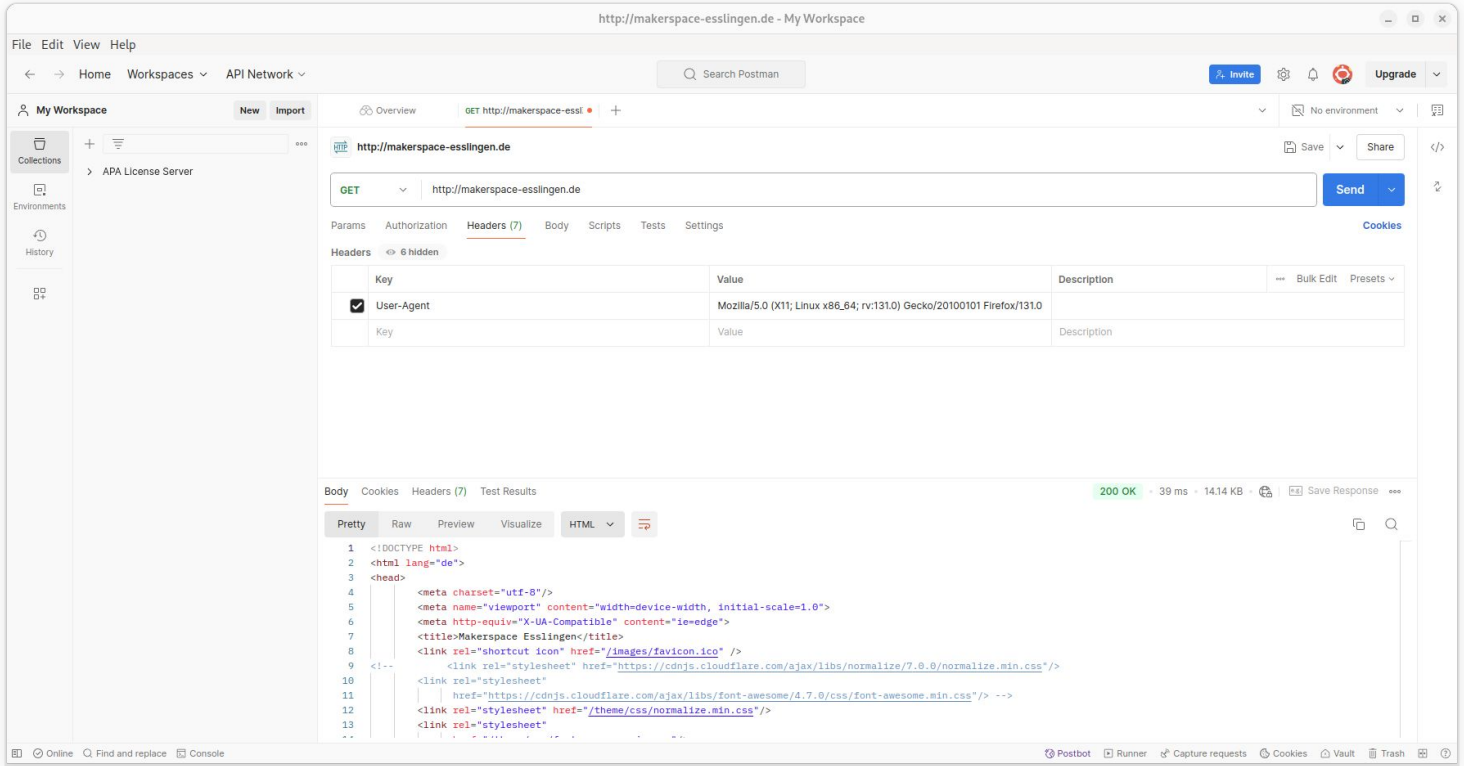
␣	"	%	-	.	<	>	\	^	_	`	{	|	}	~	£	€
%20	%22	%25	%2D	%2E	%3C	%3E	%5C	%5E	%5F	%60	%7B	%7C	%7D	%7E	%C2%A3	%E2%82%AC

https://de.wikipedia.org/wiki/URL-Encoding
https://www.urldecoder.io/

Wie manipuliere ich Requests? (BurpSuite)



Wie erstelle ich eigene Requests? (Postman)



Eigene Requests mit Python programmieren

https://github.com/domyos/python-requests-demo

```
python3 -m venv venv
. venv/bin/activate
pip3 install requests
```

https://docs.python-requests.org/en/latest/user/quickstart/