

HTTP

Hypertext Transfer Protocol



Agenda

1. Was ist HTTP?
2. Wie analysiere ich HTTP-Traffic?
3. Wie manipulierte 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

```
$ telnet www.perdu.com 80
Trying 208.97.177.124...
Connected to www.perdu.com.
Escape character is '^['.
```

Verbindungsaufbau zum Server

```
GET / http/1.1
Host: www.perdu.com
```

HTTP-Anfrage

```
HTTP/1.1 200 OK
Date: Sat, 17 Aug 2013 12:14:56 GMT
Server: Apache
Accept-Ranges: bytes
X-Mod-Pagespeed: 1.1.23.1-2169
Vary: Accept-Encoding
Cache-Control: max-age=0, no-cache
Content-Length: 204
Content-Type: text/html
```

Serverantwort: Header

```
<html><head><title>Vous Etes Perdu ?</title></head><body><h1>Perdu sur l'Interne
t ?</h1><h2>Pas de panique, on va vous aider</h2><strong><pre> * <----- vous
&ecirc;tes ici</pre></strong></body></html>
```

Serverantwort: Nachrichtenrumpf

```
Connection closed by foreign host.
$
```

Verbindungsende



Wie analysiere ich HTTP-Traffic?

The screenshot shows the Chrome DevTools Network tab. The top toolbar includes icons for Inspector, Console, Debugger, Network, Style Editor, Performance, Memory, Storage, Accessibility, and Application. Below the toolbar is a filter for URLs. The main area displays a list of network requests with columns for Status, Method, Domain, File, Initiator, Type, Transferred, and Size. The first request is highlighted in blue, showing a 200 status for a GET request to the root of the domain. Below the list, the details for the selected response are shown, including headers and request headers.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	makerspace-essli...	/	document	html	14.50 kB	14.27 kB
200	GET	makerspace-essli...	normalize.min.css	stylesheet	css	2.55 kB	2.32 kB
200	GET	makerspace-essli...	font-awesome.min.css	stylesheet	css	31.23 kB	31 kB
200	GET	makerspace-essli...	fonts.css	stylesheet	css	1.21 kB	981 B
200	GET	makerspace-essli...	main.css	stylesheet	css	8.09 kB	7.86 kB
200	GET	makerspace-essli...	logo.svg	img	svg	3.21 kB	2.97 kB
200	GET	makerspace-essli...	pygment.css	stylesheet	css	5.29 kB	5.06 kB
200	GET	makerspace-essli...	fontawesome-webfont.woff2?v=4.7.0	font	woff2	77.40 kB	77.16 kB
200	GET	makerspace-essli...	Ruda-VariableFont_wght.woff2	font	woff2	38.28 kB	38.04 kB
200	GET	makerspace-essli...	RobotoSlab-VariableFont_wght.woff2	font	woff2	116.91 kB	116.68 kB
200	GET	makerspace-essli...	favicon.ico	FaviconLoader.sys...	x-icon	15.64 kB	15.41 kB

Response Headers (233 B)

- accept-ranges: bytes
- content-length: 14267
- content-type: text/html
- date: Sat, 05 Oct 2024 13:14:12 GMT
- etag: "67008b34-37bb"
- last-modified: Sat, 05 Oct 2024 00:41:24 GMT
- server: nginx/1.27.1
- X-Firefox-Spdy: h2

Request Headers (563 B)

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
- Accept-Encoding: gzip, deflate, br, zstd
- Accept-Language: de-DE,en-US;q=0.8,de;q=0.5,en;q=0.3
- Cache-Control: no-cache
- Connection: keep-alive
- DNT: 1
- Host: makerspace-esslingen.de
- Pragma: no-cache
- Priority: u=0,i
- Sec-Fetch-Dest: document
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Site: cross-site
- Sec-GPC: 1
- TE: trailers
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0

11 requests | 311.74 kB / 314.30 kB transferred | Finish: 282 ms | DOMContentLoaded: 101 ms | load: 266 ms



Wie analysiere ich HTTP-Traffic?

The screenshot shows the Network tab of a web browser's developer tools. The top toolbar includes icons for Inspector, Console, Debugger, Network, Style Editor, Performance, Memory, Storage, Accessibility, and Application. Below the toolbar, there are tabs for Headers, Cookies, Request, Response, Timings, and Security. The main area displays a list of network requests with columns for Status, Method, Domain, File, Initiator, Type, Transferred, and Size. The first request is highlighted in blue, and its details are shown in the right-hand pane. The details pane is divided into Filter Headers, Response Headers (233 B), and Request Headers (563 B). The Request Headers section is expanded, showing various headers such as Accept, Accept-Encoding, Accept-Language, Cache-Control, Connection, DNT, Host, Pragma, Priority, Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site, Sec-GPC, TE, Upgrade-Insecure-Requests, and User-Agent.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	makerspace-essli...	/	document	html	14.50 kB	14.27 kB
200	GET	makerspace-essli...	normalize.min.css	stylesheet	css	2.55 kB	2.32 kB
200	GET	makerspace-essli...	font-awesome.min.css	stylesheet	css	31.23 kB	31 kB
200	GET	makerspace-essli...	fonts.css	stylesheet	css	1.21 kB	981 B
200	GET	makerspace-essli...	main.css	stylesheet	css	8.09 kB	7.86 kB
200	GET	makerspace-essli...	logo.svg	img	svg	3.21 kB	2.97 kB
200	GET	makerspace-essli...	pygment.css	stylesheet	css	5.29 kB	5.06 kB
200	GET	makerspace-essli...	fontawesome-webfont.woff2?v=4.7.0	font	woff2	77.40 kB	77.16 kB
200	GET	makerspace-essli...	Ruda-VariableFont_wght.woff2	font	woff2	38.28 kB	38.04 kB
200	GET	makerspace-essli...	RobotoSlab-VariableFont_wght.woff2	font	woff2	116.91 kB	116.68 kB
200	GET	makerspace-essli...	favicon.ico	FaviconLoader.sys...	x-icon	15.64 kB	15.41 kB

11 requests | 311.74 kB / 314.30 kB transferred | Finish: 282 ms | DOMContentLoaded: 101 ms | load: 266 ms



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?

The screenshot shows the Network tab of a web browser's developer tools. The top part displays a list of requests with columns for Status, Method, Domain, File, Initiator, Type, Transferred, and Size. The first request is highlighted in blue, showing a 200 status for a GET request to the root of the domain. Below this, the details for the selected response are shown, including the Request Headers (563 B) and Response Headers (233 B). The Request Headers section is highlighted with a red box.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	makerspace-essli...	/	document	html	14.50 kB	14.27 kB
200	GET	makerspace-essli...	normalize.min.css	stylesheet	css	2.55 kB	2.32 kB
200	GET	makerspace-essli...	font-awesome.min.css	stylesheet	css	31.23 kB	31 kB
200	GET	makerspace-essli...	fonts.css	stylesheet	css	1.21 kB	981 B
200	GET	makerspace-essli...	main.css	stylesheet	css	8.09 kB	7.86 kB
200	GET	makerspace-essli...	logo.svg	img	svg	3.21 kB	2.97 kB
200	GET	makerspace-essli...	pygment.css	stylesheet	css	5.29 kB	5.06 kB
200	GET	makerspace-essli...	fontawesome-webfont.woff2?v=4.7.0	font	woff2	77.40 kB	77.16 kB
200	GET	makerspace-essli...	Ruda-VariableFont_wght.woff2	font	woff2	38.28 kB	38.04 kB
200	GET	makerspace-essli...	RobotoSlab-VariableFont_wght.woff2	font	woff2	116.91 kB	116.68 kB
200	GET	makerspace-essli...	favicon.ico	FaviconLoader.sys...	x-icon	15.64 kB	15.41 kB

Request Headers (563 B)

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
- Accept-Encoding: gzip, deflate, br, zstd
- Accept-Language: de-DE,en-US;q=0.8,de;q=0.5,en;q=0.3
- Cache-Control: no-cache
- Connection: keep-alive
- DNT: 1
- Host: makerspace-esslingen.de
- Pragma: no-cache
- Priority: u=0,i
- Sec-Fetch-Dest: document
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Site: cross-site
- Sec-GPC: 1
- TE: trailers
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0



Headers

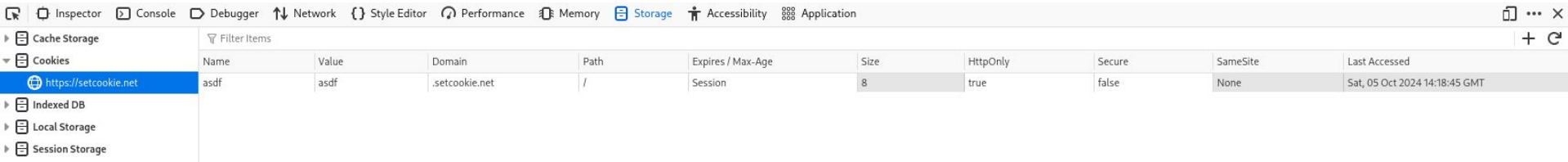
User-Agent: Identifiziert den Client, der die Anfrage stellt (z.B. den Webbrowser).

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



The screenshot shows the Chrome DevTools Storage Inspector. The left sidebar lists storage types: Cache Storage, Cookies, Indexed DB, Local Storage, and Session Storage. The 'Cookies' section is expanded, showing a single cookie for the URL 'https://setcookie.net'. The main pane displays a table of cookie details.

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?

The screenshot shows the Network tab of a browser's developer tools. A table lists various requests, with the first row highlighted in blue. A red box highlights the status column, showing '200' for all requests. The details pane on the right shows the response headers and request headers for the selected request.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	makerspace-essli...	/	document	html	14.50 kB	14.27 kB
200	GET	makerspace-essli...	normalize.min.css	stylesheet	css	2.55 kB	2.32 kB
200	GET	makerspace-essli...	font-awesome.min.css	stylesheet	css	31.23 kB	31 kB
200	GET	makerspace-essli...	fonts.css	stylesheet	css	1.21 kB	981 B
200	GET	makerspace-essli...	main.css	stylesheet	css	8.09 kB	7.86 kB
200	GET	makerspace-essli...	logo.svg	img	svg	3.21 kB	2.97 kB
200	GET	makerspace-essli...	pygment.css	stylesheet	css	5.29 kB	5.06 kB
200	GET	makerspace-essli...	fontawesome-webfont.woff2?v=4.7.0	font	woff2	77.40 kB	77.16 kB
200	GET	makerspace-essli...	Ruda-VariableFont_wght.woff2	font	woff2	38.28 kB	38.04 kB
200	GET	makerspace-essli...	RobotoSlab-VariableFont_wght.woff2	font	woff2	116.91 kB	116.68 kB
200	GET	makerspace-essli...	favicon.ico	FaviconLoader.sys...	x-icon	15.64 kB	15.41 kB

Response Headers (233 B)

- accept-ranges: bytes
- content-length: 14267
- content-type: text/html
- date: Sat, 05 Oct 2024 13:14:12 GMT
- etag: "67008b34-37bb"
- last-modified: Sat, 05 Oct 2024 00:41:24 GMT
- server: nginx/1.27.1
- X-Firefox-Spdy: h2

Request Headers (563 B)

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
- Accept-Encoding: gzip, deflate, br, zstd
- Accept-Language: de-DE,en-US;q=0.8,de;q=0.5,en;q=0.3
- Cache-Control: no-cache
- Connection: keep-alive
- DNT: 1
- Host: makerspace-esslingen.de
- Pragma: no-cache
- Priority: u=0,i
- Sec-Fetch-Dest: document
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Site: cross-site
- Sec-GPC: 1
- TE: trailers
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0

11 requests | 311.74 kB / 314.30 kB transferred | Finish: 282 ms | DOMContentLoaded: 101 ms | load: 266 ms

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?

The screenshot shows the Chrome DevTools Network tab. The top toolbar includes icons for Inspector, Console, Debugger, Network, Style Editor, Performance, Memory, Storage, Accessibility, and Application. Below the toolbar, there are tabs for Headers, Cookies, Request, Response, Timings, and Security. The main area is divided into a list of requests on the left and a detailed view of the selected request on the right.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	makerspace-essli...	/	document	html	14.50 kB	14.27 kB
200	GET	makerspace-essli...	normalize.min.css	stylesheet	css	2.55 kB	2.32 kB
200	GET	makerspace-essli...	font-awesome.min.css	stylesheet	css	31.23 kB	31 kB
200	GET	makerspace-essli...	fonts.css	stylesheet	css	1.21 kB	981 B
200	GET	makerspace-essli...	main.css	stylesheet	css	8.09 kB	7.86 kB
200	GET	makerspace-essli...	logo.svg	img	svg	3.21 kB	2.97 kB
200	GET	makerspace-essli...	ryoment.css	stylesheet	css	5.29 kB	5.06 kB
200	GET	makerspace-essli...	fontawesome-webfont.woff2?v=4.7.0	font	woff2	77.40 kB	77.16 kB
200	GET	makerspace-essli...	Ruda-VariableFont_wght.woff2	font	woff2	38.28 kB	38.04 kB
200	GET	makerspace-essli...	RobotoSlab-VariableFont_wght.woff2	font	woff2	116.91 kB	116.68 kB
200	GET	makerspace-essli...	favicon.ico	FaviconLoader.sys...	x-icon	15.64 kB	15.41 kB

The selected request (fontawesome-webfont.woff2?v=4.7.0) is highlighted with a red box. The details panel on the right shows the following information:

- Status: 200
- Version: HTTP/2
- Transferred: 14.50 kB (14.27 kB size)
- Request Priority: Highest
- DNS Resolution: System
- Response Headers (233 B):
 - accept-ranges: bytes
 - content-length: 14267
 - content-type: text/html
 - date: Sat, 05 Oct 2024 13:14:12 GMT
 - etag: "67008b34-37bb"
 - last-modified: Sat, 05 Oct 2024 00:41:24 GMT
 - server: nginx/1.27.1
 - X-Firefox-Spdy: h2
- Request Headers (563 B):
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
 - Accept-Encoding: gzip, deflate, br, zstd
 - Accept-Language: de-DE,en-US;q=0.8,de;q=0.5,en;q=0.3
 - Cache-Control: no-cache
 - Connection: keep-alive
 - DNT: 1
 - Host: makerspace-esslingen.de
 - Pragma: no-cache
 - Priority: u=0,i
 - Sec-Fetch-Dest: document
 - Sec-Fetch-Mode: navigate
 - Sec-Fetch-Site: cross-site
 - Sec-GPC: 1
 - TE: trailers
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/2010101 Firefox/131.0



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 manipulierte ich Requests? (BurpSuite)

The screenshot displays the Burp Suite interface with the 'Repeater' tab selected. The target is set to 'https://makerspace-esslingen.de'. The 'Request' pane shows a GET request to the root path. The 'Response' pane shows an HTTP/2 200 OK response with HTML content. The 'Inspector' pane on the right shows the request and response headers.

Request

```
1 GET / HTTP/2
2 Host: makerspace-esslingen.de
3 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "Linux"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.138
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
  webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Priority: u=0, i
16
17
```

Response

```
1 HTTP/2 200 OK
2 Accept-Ranges: bytes
3 Content-Type: text/html
4 Date: Sat, 05 Oct 2024 13:27:19 GMT
5 Etag: "67008b34-37bb"
6 Last-Modified: Sat, 05 Oct 2024 00:41:24 GMT
7 Server: nginx/1.27.1
8 Content-Length: 14267
9
10 <!DOCTYPE html>
11 <html lang="de">
12 <head>
13 <meta charset="utf-8"/>
14 <meta name="viewport" content="width=device-width,
  initial-scale=1.0">
15 <meta http-equiv="X-UA-Compatible" content="ie=edge">
16 <title>
  Makerspace Esslingen
  </title>
17 <link rel="shortcut icon" href="/images/favicon.ico" />
18 <!-- <link rel="stylesheet"
  href="https://cdnjs.cloudflare.com/ajax/libs/normalize/7.0.0/normalize.min.css"/>
19 <link rel="stylesheet"
  href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css"/> -->
20 <link rel="stylesheet" href="/theme/css/normalize.min.css"/>
21 <link rel="stylesheet" href="/theme/css/font-awesome.min.css"/>
22 <link rel="stylesheet"
  href="/theme/css/font-awesome.min.css"/>
23 <!-- <link rel="stylesheet"
  href="/theme/normalize.min.css"/>
24
```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 0
- Request headers: 17
- Response headers: 7

Done
Event log (16) All issues

14,482 bytes | 39 millis
Memory: 119.9MB

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/>