Basisinformationstechnologie II

Sommersemester 2023. 4: Rechnerkommunikation II

Protokolle, Anwendungen. *Basierend auf Jan Wieners' Folien*

Institut für Digital Humanities, Historisch-Kulturwissenschaftliche Informationsverarbeitung | Prof. Dr. Øyvind Eide | Slavina Stoyanova

Themenüberblick „Rechnerkommunikation II“

- „Warriors of the Net“
- HTTP
- HTTPS
- Anwendungsschicht
  - Email
    - SMTP
    - POP3
    - IMAP


Warriors of the Net

Fragen zum Kurzfilm

- Welche Informationen stehen auf dem Etikett des IP-Pakets?
- Wofür wird das Local Area Network (LAN) verwendet?
- Welche Aufgabe hat der Router?
- Was ist ein Proxy? Welche Aufgabe hat ein Proxy?
- Welche Aufgabe hat eine Firewall?
- Für welche Art von Paketen sind (im Film) die Eingänge 25 und 80 reserviert?

Themenüberblick II

- HTTP
- HTTPS
- Anwendungsschicht
  - Email
    - SMTP
    - POP3
    - IMAP

HTTP (Hypertext Transfer Protocol)	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Datenübertragung, Hypertext u. a.
Port:	80/TCP

HTTP im TCP/IP-Protokollstapel:

Anwendung	**HTTP**				
Transport	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Standards:	RFC 1945 (HTTP/1.0, 1996) RFC 2616 (HTTP/1.1, 1999)

HTTP (Hypertext Transfer Protocol)	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Datenübertragung, Hypertext u. a.
Port:	80/TCP

HTTP im TCP/IP-Protokollstapel:

Anwendung	**HTTP**				
Transport	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Standards:	RFC 1945 (HTTP/1.0, 1996) RFC 2616 (HTTP/1.1, 1999)

Ethernet, u.a.:

- ISO/OSI Modell:
  - Schicht 1 (Physik. Schicht) und
  - Schicht 2 (Sicherungsschicht)
- TCP/IP:

Ethernet im TCP/IP-Protokollstapel:

Anwendung	HTTP	IMAP	SMTP	DNS	...
Transport	TCP			UDP	
Internet	IP (IPv4, IPv6)				
Netzzugang	**Ethernet**				

HTTP (Hypertext Transfer Protocol)	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Datenübertragung, Hypertext u. a.
Port:	80/TCP

HTTP im TCP/IP-Protokollstapel:

Anwendung	**HTTP**				
Transport	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Standards:	RFC 1945 (HTTP/1.0, 1996) RFC 2616 (HTTP/1.1, 1999)

IPv4: 134.95.115.23
IPv6: Hex.-Not., 8 Blöcke, je 16 Bit

Ethernet, u.a.:

- ISO/OSI Modell:
  - Schicht 1 (Physik. Schicht) und
  - Schicht 2 (Sicherungsschicht)
- TCP/IP:

Ethernet im TCP/IP-Protokollstapel:

Anwendung	HTTP	IMAP	SMTP	DNS	...
Transport	TCP			UDP	
Internet	IP (IPv4, IPv6)				
Netzzugang	**Ethernet**				

HTTP (Hypertext Transfer Protocol)	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Datenübertragung, Hypertext u. a.
Port:	80/TCP

HTTP im TCP/IP-Protokollstapel:

Anwendung	**HTTP**				
Transport	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Standards:	RFC 1945 (HTTP/1.0, 1996) RFC 2616 (HTTP/1.1, 1999)

TCP: Transmission Control Protocol,
Verbindungsorientiertes Protokoll

IPv4: 134.95.115.23

IPv6: Hex.-Not., 8 Blöcke, je 16 Bit

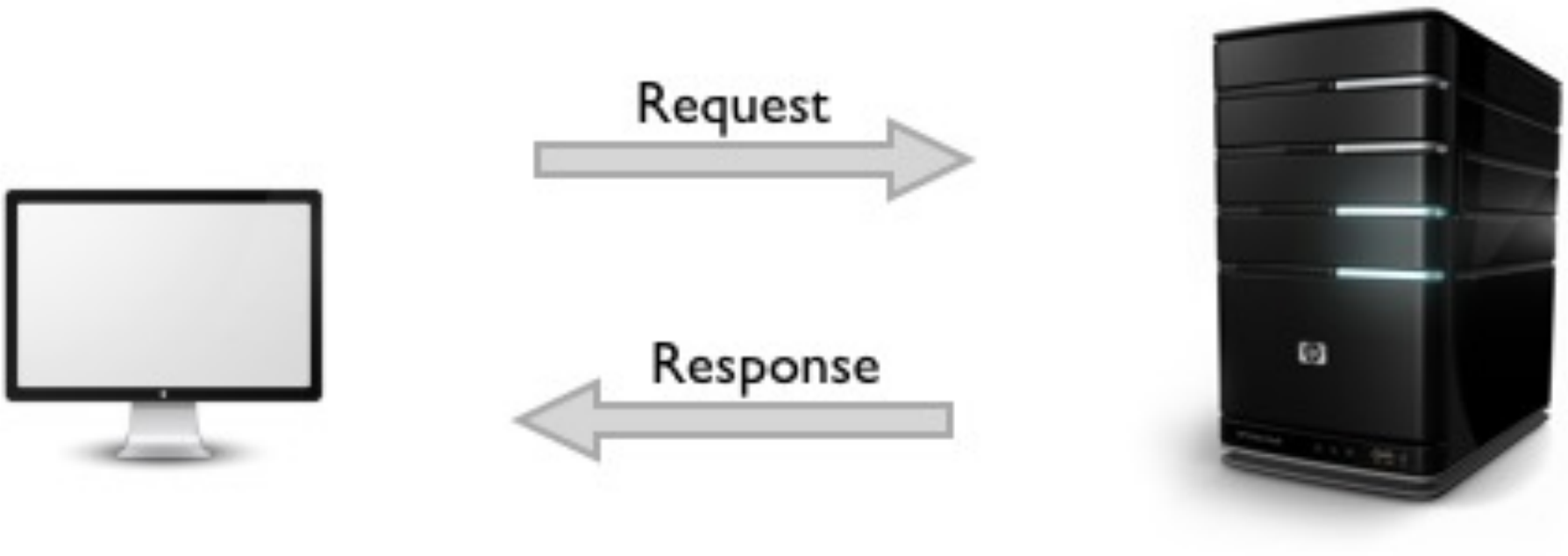
Ethernet, u.a.:

- ISO/OSI Modell:
  - Schicht 1 (Physik. Schicht) und
  - Schicht 2 (Sicherungsschicht)
- TCP/IP:

Ethernet im TCP/IP-Protokollstapel:

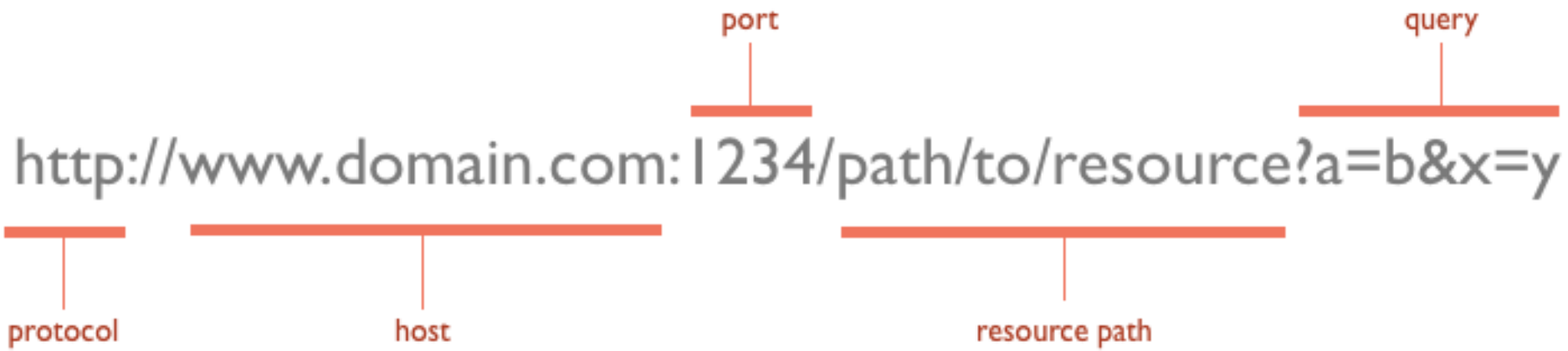
Anwendung	HTTP	IMAP	SMTP	DNS	...
Transport	TCP			UDP	
Internet	IP (IPv4, IPv6)				
Netzzugang	**Ethernet**				

HTTP: Client / Server Modell



Quelle: http://net.tutsplus.com/tutorials/tools-and-tips/http-the-protocol-every-web-developer-must-know-part-1/

HTTP: Uniform Resource Locator (URL)

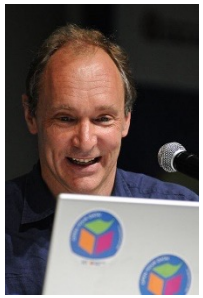


Quelle: http://net.tutsplus.com/tutorials/tools-and-tips/http-the-protocol-every-web-developer-must-know-part-1/

HTTP: Uniform Resource Locator (URL)

Drei Standards:

- HTTP
- HTML
- URLs

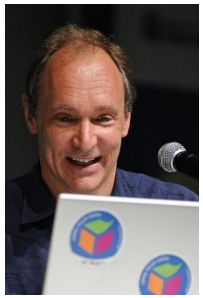


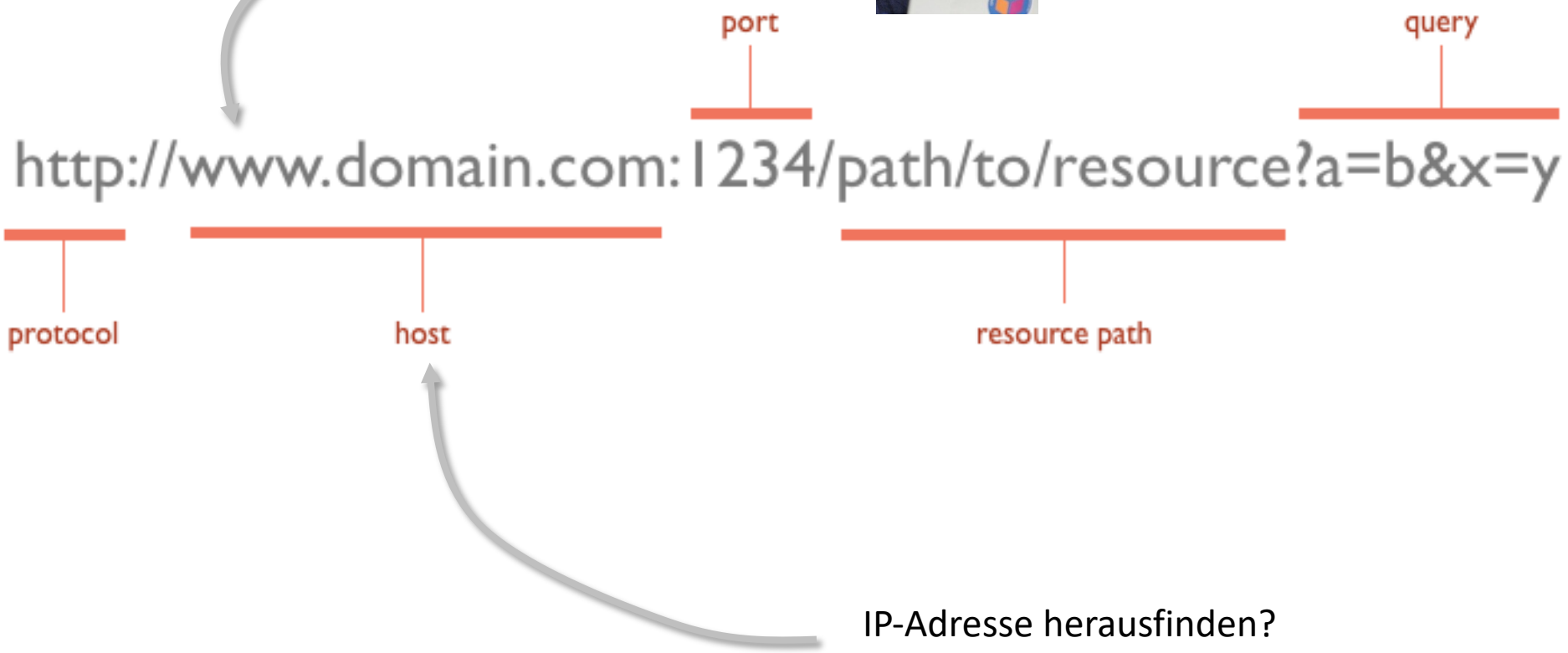
Quelle: http://net.tutsplus.com/tutorials/tools-and-tips/http-the-protocol-every-web-developer-must-know-part-1/

HTTP: Uniform Resource Locator (URL)

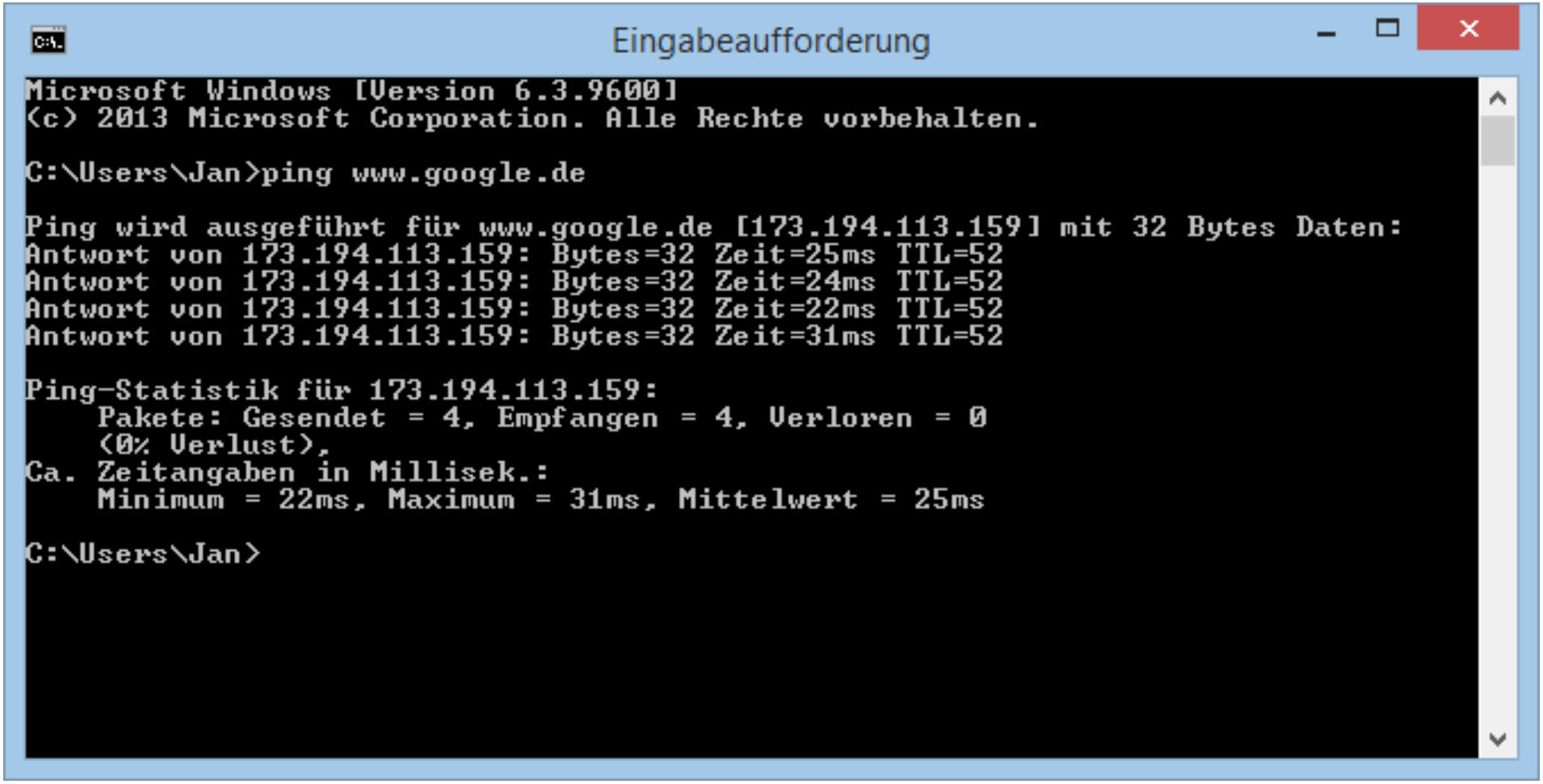
Drei Standards:

- HTTP
- HTML
- URLs





Quelle: http://net.tutsplus.com/tutorials/tools-and-tips/http-the-protocol-every-web-developer-must-know-part-1/


Eingabeaufforderung
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Alle Rechte vorbehalten.
C:\Users\Jan>ping www.google.de
Ping wird ausgeführt für www.google.de [173.194.113.159] mit 32 Bytes Daten:
Antwort von 173.194.113.159: Bytes=32 Zeit=25ms TTL=52
Antwort von 173.194.113.159: Bytes=32 Zeit=24ms TTL=52
Antwort von 173.194.113.159: Bytes=32 Zeit=22ms TTL=52
Antwort von 173.194.113.159: Bytes=32 Zeit=31ms TTL=52
Ping-Statistik für 173.194.113.159:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 22ms, Maximum = 31ms, Mittelwert = 25ms
C:\Users\Jan>

SpoookyJS. Ein multiagentenbasiertes JavaScript-Framework zur flexiblen Implementation digitaler browserbasierter Brettspiele und spielübergreifender künstlicher Intelligenz

Wieners, Jan Gerrit (2014) *SpoookyJS. Ein multiagentenbasiertes JavaScript-Framework zur flexiblen Implementation digitaler browserbasierter Brettspiele und spielübergreifender künstlicher Intelligenz*. Dissertation, Universität zu Köln.

PDF - Eingereichte Version
Download (8Mb) | Vorschau

Kurzfassung/Abstract

Künstliche Intelligenz in digitalen Spielen ist zumeist Anwendungsdomäne komplexer spielspezifischer Softwarelösungen mangelnder Erweiterbarkeit. Die vorliegende Arbeit beschäftigt sich mit der Konzeption und Realisierung des JavaScript-Frameworks SpoookyJS, das die vereinfachte Erstellung browserbasierter digitaler Brettspiele ermöglicht. Entwickelt als Multiagentensystem, bietet SpoookyJS künstliche Gegner in den umgesetzten Spielen und fungiert als Test- und Entwicklungsumgebung für die Forschung um spielübergreifende artifizielle Entscheidungsfindung.

Publikationsform: Hochschulschrift (Dissertation)

Autoren:

Autorenname	E-Mail-Adresse
Wieners, Jan Gerrit	jan@jan-wieners.de

URN: urn:nbn:de:hbz:38-59711

Themen: Informatik, Datenverarbeitung
Philosophie
Technik, Technologie

Freie Schlagwörter:

Keywords	Language
Computational Intelligence, Digitale Brettspiele, General Game Playing, Künstliche Intelligenz, Monte Carlo Spielbaumsuche	Deutsch

Fakultät: Philosophische Fakultät

Einrichtung/Fakultät/Seminar/Institut: Philosophische Fakultät > Historisch - Kulturwissenschaftliche Informationsverarbeitung

Sprache: Deutsch

Jahr: 28 Oktober 2014

Datumstyp: Veröffentlichung

Tag der mündlichen Prüfung: 14 Januar 2015

Status des Volltextes: Öffentlich

Weitere URLs:
- http://www.spoookyjs.de
- http://www.jan-wieners.de/dissertation

Datum der Hinterlegung: 19 Feb 2015 10:07:58

Gutachter

Name des Gutachters	Akademischer Titel des Gutachters
Thaller, Manfred	Prof. Dr.
Förtsch, Reinhard	Prof. Dr.

URI: http://kups.ub.uni-koeln.de/id/eprint/5971

URN:NBN RESOLVER FÜR DEUTSCHLAND UND SCHWEIZ

- URN-Resolver
- URL-Resolver
- Registrierte Namensräume
- Partnerinstitutionen
- Beispiele

- URN-Administration
- Deutsche Nationalbibliothek

Information über die URN

U R N	**urn:nbn:de:hbz:38-59711**
Verantwortliche Institution	Universitäts- und Stadtbibliothek Köln
Erstellt / Geändert	2015-02-19 / 2015-02-26

Zugriff auf die Ressource

Bitte kontaktieren Sie die verantwortliche Institution, falls eine der gelisteten URLs nicht funktionieren sollte

1. U R L	**http://kups.ub.uni-koeln.de/5971/**

2. U R L	**http://d-nb.info/106755307X/34**

Neuer Glanz für das Markenzeichen von Guinness

4. Mai 2016 | 31 Kommentare

MEISTGELESEN (30 TAGE)

Die neuen Audi-Ringe – Vorsprung durch Flat Design 26.489 Aufrufe

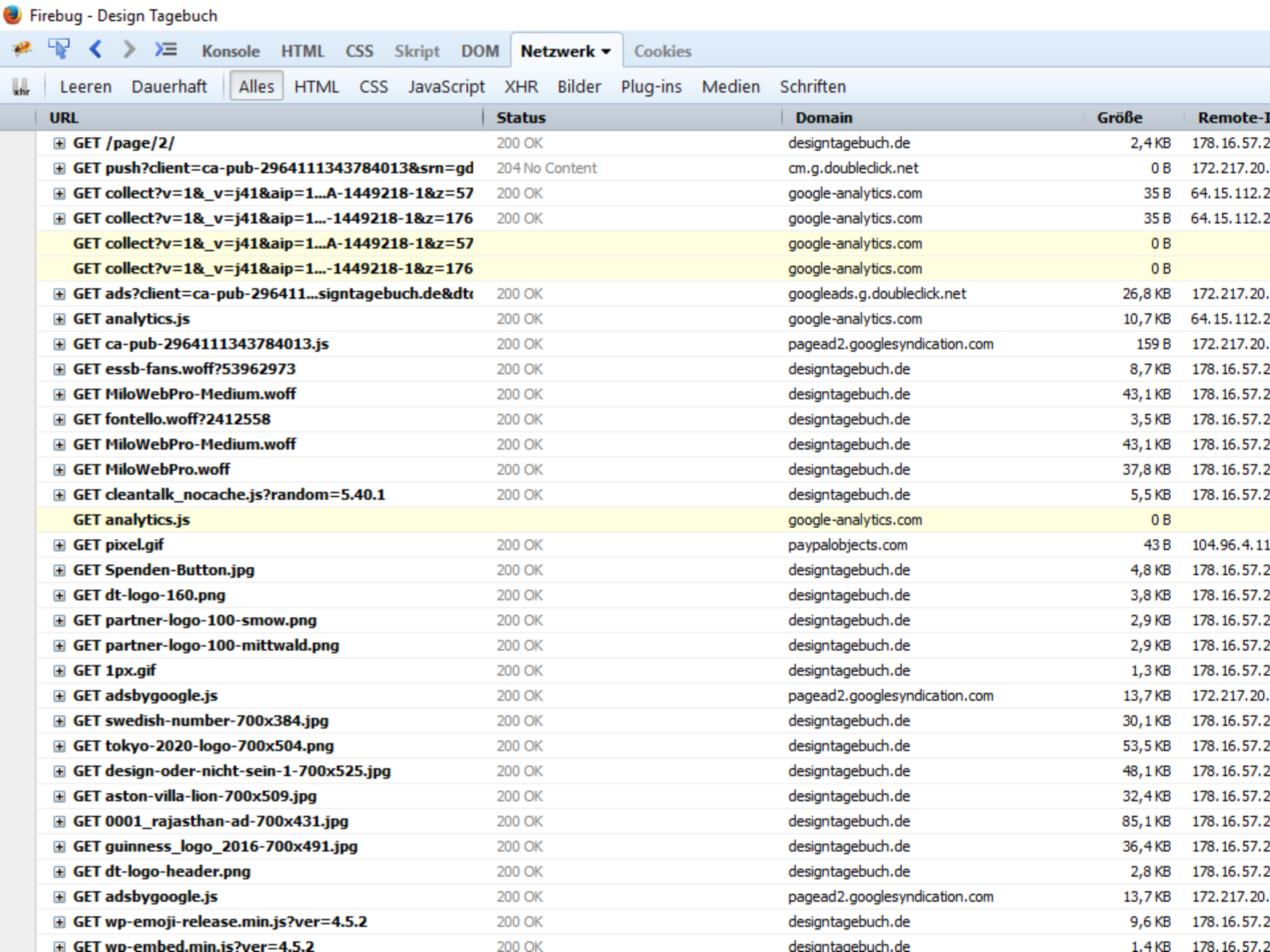
Neuer Markenauftritt für Bosch 12.800 Aufrufe

Die neue australische 5-Dollar-Banknote, Erbrochenes, und wie auf schlechten Stil schlechtes Design folgt 9.241 Aufrufe

Einführung der 9. Schweizer Banknotenserie – so sieht die neue 50-Franken-Note aus 8.426 Aufrufe

Finales Logo der Olympischen Sommerspiele in Tokio 2020 gekürt 6.156 Aufrufe

EMPFEHLUNGEN


Firebug - Design Tagebuch
Konsole HTML CSS Skript DOM Netzwerk Cookies
Leeren Dauerhaft Alles HTML CSS JavaScript XHR Bilder Plug-ins Medien Schriften
URL Status Domain Größe Remote-I
GET /page/2/ 200 OK designtagebuch.de 2,4 KB 178.16.57.2
GET push?client=ca-pub-2964111343784013&srn=gd 204 No Content cm.g.doubleclick.net 0 B 172.217.20.
GET collect?v=1&_v=j41&aip=1...A-1449218-1&z=57 200 OK google-analytics.com 35 B 64.15.112.2
GET collect?v=1&_v=j41&aip=1...-1449218-1&z=176 200 OK google-analytics.com 35 B 64.15.112.2
GET collect?v=1&_v=j41&aip=1...A-1449218-1&z=57 google-analytics.com 0 B
GET collect?v=1&_v=j41&aip=1...-1449218-1&z=176 google-analytics.com 0 B
GET ads?client=ca-pub-296411...signtagebuch.de&dt 200 OK googleads.g.doubleclick.net 26,8 KB 172.217.20.
GET analytics.js 200 OK google-analytics.com 10,7 KB 64.15.112.2
GET ca-pub-2964111343784013.js 200 OK pagead2.googlesyndication.com 159 B 172.217.20.
GET essb-fans.woff?53962973 200 OK designtagebuch.de 8,7 KB 178.16.57.2
GET MiloWebPro-Medium.woff 200 OK designtagebuch.de 43,1 KB 178.16.57.2
GET fontello.woff?2412558 200 OK designtagebuch.de 3,5 KB 178.16.57.2
GET MiloWebPro-Medium.woff 200 OK designtagebuch.de 43,1 KB 178.16.57.2
GET MiloWebPro.woff 200 OK designtagebuch.de 37,8 KB 178.16.57.2
GET cleantalk_nocache.js?random=5.40.1 200 OK designtagebuch.de 5,5 KB 178.16.57.2
GET analytics.js google-analytics.com 0 B
GET pixel.gif 200 OK paypalobjects.com 43 B 104.96.4.11
GET Spenden-Button.jpg 200 OK designtagebuch.de 4,8 KB 178.16.57.2
GET dt-logo-160.png 200 OK designtagebuch.de 3,8 KB 178.16.57.2
GET partner-logo-100-smow.png 200 OK designtagebuch.de 2,9 KB 178.16.57.2
GET partner-logo-100-mittwald.png 200 OK designtagebuch.de 2,9 KB 178.16.57.2
GET 1px.gif 200 OK designtagebuch.de 1,3 KB 178.16.57.2
GET adsbygoogle.js 200 OK pagead2.googlesyndication.com 13,7 KB 172.217.20.
GET swedish-number-700x384.jpg 200 OK designtagebuch.de 30,1 KB 178.16.57.2
GET tokyo-2020-logo-700x504.png 200 OK designtagebuch.de 53,5 KB 178.16.57.2
GET design-oder-nicht-sein-1-700x525.jpg 200 OK designtagebuch.de 48,1 KB 178.16.57.2
GET aston-villa-lion-700x509.jpg 200 OK designtagebuch.de 32,4 KB 178.16.57.2
GET 0001_rajasthan-ad-700x431.jpg 200 OK designtagebuch.de 85,1 KB 178.16.57.2
GET guinness_logo_2016-700x491.jpg 200 OK designtagebuch.de 36,4 KB 178.16.57.2
GET dt-logo-header.png 200 OK designtagebuch.de 2,8 KB 178.16.57.2
GET adsbygoogle.js 200 OK pagead2.googlesyndication.com 13,7 KB 172.217.20.
GET wp-emoji-release.min.js?ver=4.5.2 200 OK designtagebuch.de 9,6 KB 178.16.57.2
GET wp-embed.min.js?ver=4.5.2 200 OK designtagebuch.de 1,4 KB 178.16.57.2

Firebug - Design Tagebuch

Konsole HTML CSS Skript DOM **Netzwerk** Cookies

Leeren Dauerhaft Alles HTML CSS JavaScript XHR Bilder Plug-ins Medien Schriften

URL	Status	Domain	Größe	Remote-IP
GET /page/2/	200 OK	designtagebuch.de	2,4 KB	178.16.57.240

Header Antwort HTML Cache Cookies

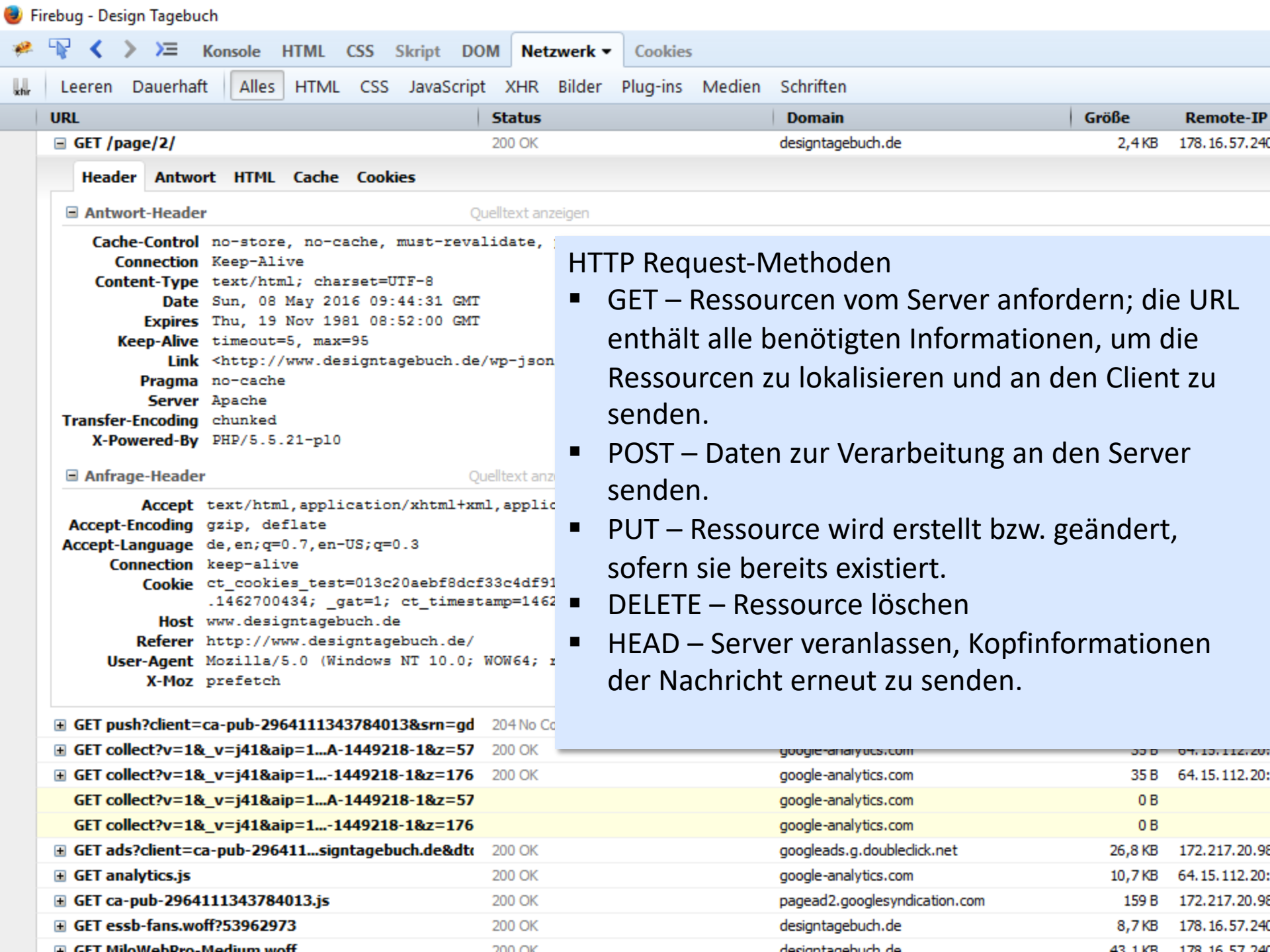
Antwort-Header Quelltext anzeigen

Cache-Control	no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection	Keep-Alive
Content-Type	text/html; charset=UTF-8
Date	Sun, 08 May 2016 09:44:31 GMT
Expires	Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive	timeout=5, max=95
Link	<http://www.designtagebuch.de/wp-json/>; rel="https://api.w.org/"
Pragma	no-cache
Server	Apache
Transfer-Encoding	chunked
X-Powered-By	PHP/5.5.21-pl0

Anfrage-Header Quelltext anzeigen

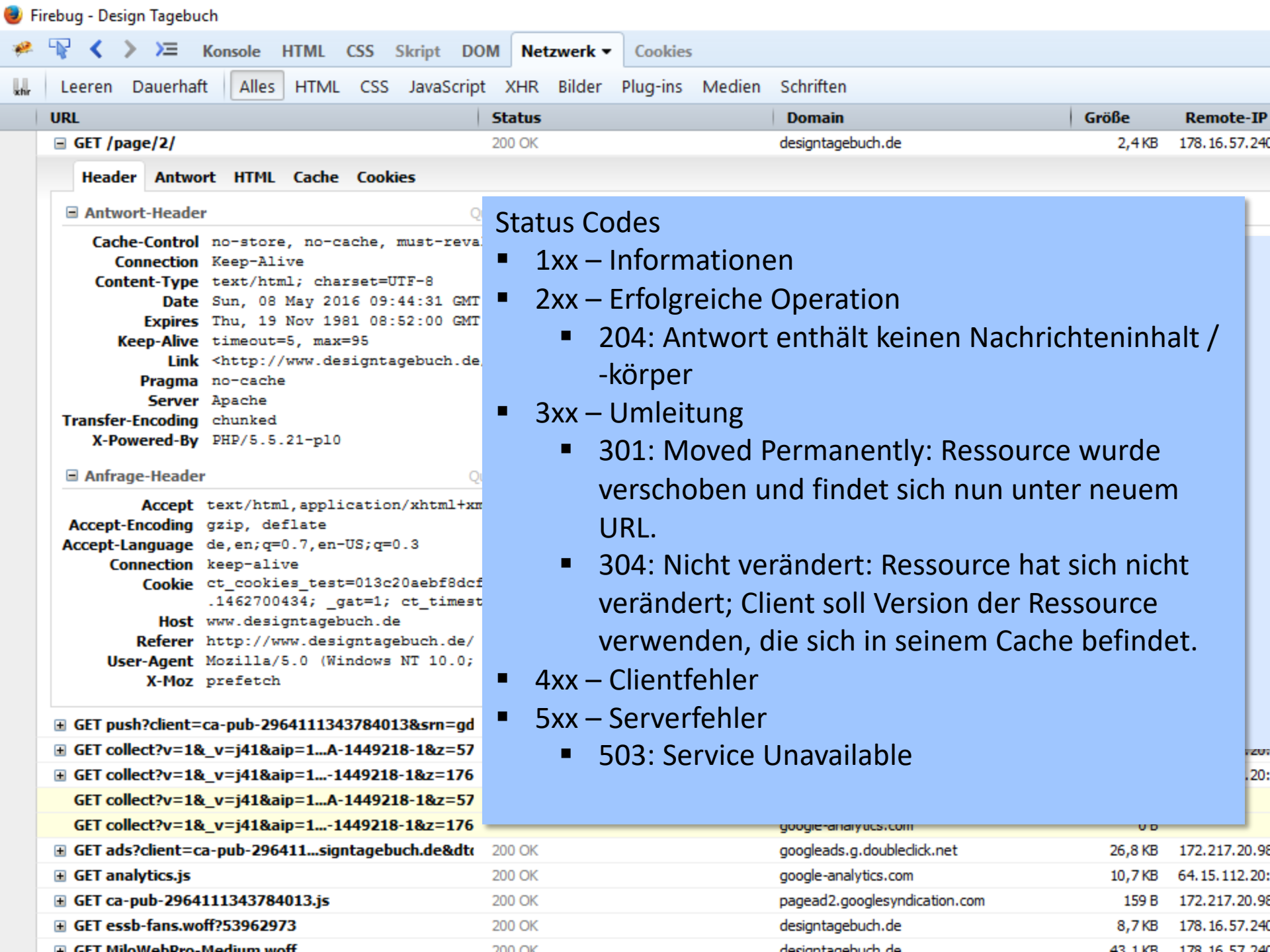
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding	gzip, deflate
Accept-Language	de,en;q=0.7,en-US;q=0.3
Connection	keep-alive
Cookie	ct_cookies_test=013c20aebf8dcf33c4df9187ab47b1fc; PHPSESSID=roc249kcg86mtelm7dggn8ksd4; _ga=GA1.2.1631352634.1462700434; _gat=1; ct_timestamp=1462700433; ct_checkjs=1698036306
Host	www.designtagebuch.de
Referer	http://www.designtagebuch.de/
User-Agent	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
X-Moz	prefetch

GET push?client=ca-pub-2964111343784013&srn=gd	204 No Content	cm.g.doubleclick.net	0 B	172.217.20.13
GET collect?v=1&_v=j41&aip=1...A-1449218-1&z=57	200 OK	google-analytics.com	35 B	64.15.112.20:
GET collect?v=1&_v=j41&aip=1...-1449218-1&z=176	200 OK	google-analytics.com	35 B	64.15.112.20:
GET collect?v=1&_v=j41&aip=1...A-1449218-1&z=57		google-analytics.com	0 B	
GET collect?v=1&_v=j41&aip=1...-1449218-1&z=176		google-analytics.com	0 B	
GET ads?client=ca-pub-296411...signtagebuch.de&dt	200 OK	googleads.g.doubleclick.net	26,8 KB	172.217.20.98
GET analytics.js	200 OK	google-analytics.com	10,7 KB	64.15.112.20:
GET ca-pub-2964111343784013.js	200 OK	pagead2.googlesyndication.com	159 B	172.217.20.98
GET essb-fans.woff?53962973	200 OK	designtagebuch.de	8,7 KB	178.16.57.240
GET MiloWebPro-Medium.woff	200 OK	designtagebuch.de	43,1 KB	178.16.57.240



HTTP Request-Methoden

- GET – Ressourcen vom Server anfordern; die URL enthält alle benötigten Informationen, um die Ressourcen zu lokalisieren und an den Client zu senden.
- POST – Daten zur Verarbeitung an den Server senden.
- PUT – Ressource wird erstellt bzw. geändert, sofern sie bereits existiert.
- DELETE – Ressource löschen
- HEAD – Server veranlassen, Kopfinformationen der Nachricht erneut zu senden.


Firebug - Design Tagebuch
Konsole HTML CSS Skript DOM Netzwerk Cookies
Leeren Dauerhaft Alles HTML CSS JavaScript XHR Bilder Plug-ins Medien Schriften
URL Status Domain Größe Remote-IP
GET /page/2/ 200 OK designtagebuch.de 2,4 KB 178.16.57.240
Header Antwort HTML Cache Cookies
Antwort-Header
Cache-Control no-store, no-cache, must-reva
Connection Keep-Alive
Content-Type text/html; charset=UTF-8
Date Sun, 08 May 2016 09:44:31 GMT
Expires Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive timeout=5, max=95
Link <http://www.designtagebuch.de
Pragma no-cache
Server Apache
Transfer-Encoding chunked
X-Powered-By PHP/5.5.21-pl0
Anfrage-Header
Accept text/html,application/xhtml+xm
Accept-Encoding gzip, deflate
Accept-Language de,en;q=0.7,en-US;q=0.3
Connection keep-alive
Cookie ct_cookies_test=013c20aebf8dcf
.1462700434; _gat=1; ct_timest
Host www.designtagebuch.de
Referer http://www.designtagebuch.de/
User-Agent Mozilla/5.0 (Windows NT 10.0;
X-Moz prefetch
GET push?client=ca-pub-2964111343784013&srn=gd
GET collect?v=1&_v=j41&aip=1...A-1449218-1&z=57
GET collect?v=1&_v=j41&aip=1...-1449218-1&z=176
GET collect?v=1&_v=j41&aip=1...A-1449218-1&z=57
GET collect?v=1&_v=j41&aip=1...-1449218-1&z=176
GET ads?client=ca-pub-296411...signtagebuch.de&dt 200 OK googleads.g.doubleclick.net 26,8 KB 172.217.20.98
GET analytics.js 200 OK google-analytics.com 10,7 KB 64.15.112.20
GET ca-pub-2964111343784013.js 200 OK pagead2.googlesyndication.com 159 B 172.217.20.98
GET essb-fans.woff?53962973 200 OK designtagebuch.de 8,7 KB 178.16.57.240
Status Codes
1xx – Informationen
2xx – Erfolgreiche Operation
204: Antwort enthält keinen Nachrichteninhalt / -körper
3xx – Umleitung
301: Moved Permanently: Ressource wurde verschoben und findet sich nun unter neuem URL.
304: Nicht verändert: Ressource hat sich nicht verändert; Client soll Version der Ressource verwenden, die sich in seinem Cache befindet.
4xx – Clientfehler
5xx – Serverfehler
503: Service Unavailable

HTTP: Argumentübergabe

Beispiel: Formulareingabe im Browser

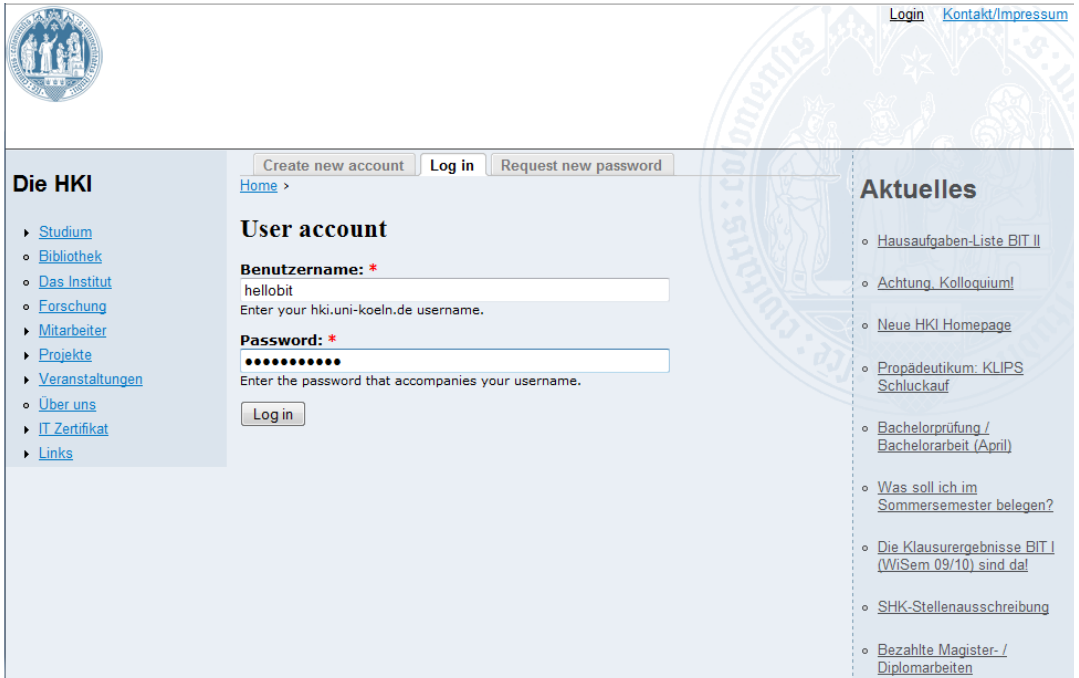
- GET
  - Informationen sind Teil der URL; Übergabe von Paaren aus Argument und Wert
    Beispiel Google Suche:
    http://www.google.de/#hl=de&source=hp**&q=hello+world**&aq=f&aqi=g10&aql=&oq=&gs_rfai=&fp=8889134438f330ab
- POST
  - Informationen (Argument-/Wert Paare) werden unverschlüsselt(!) im Hintergrund (in den HTTP Kopfdaten) übertragen

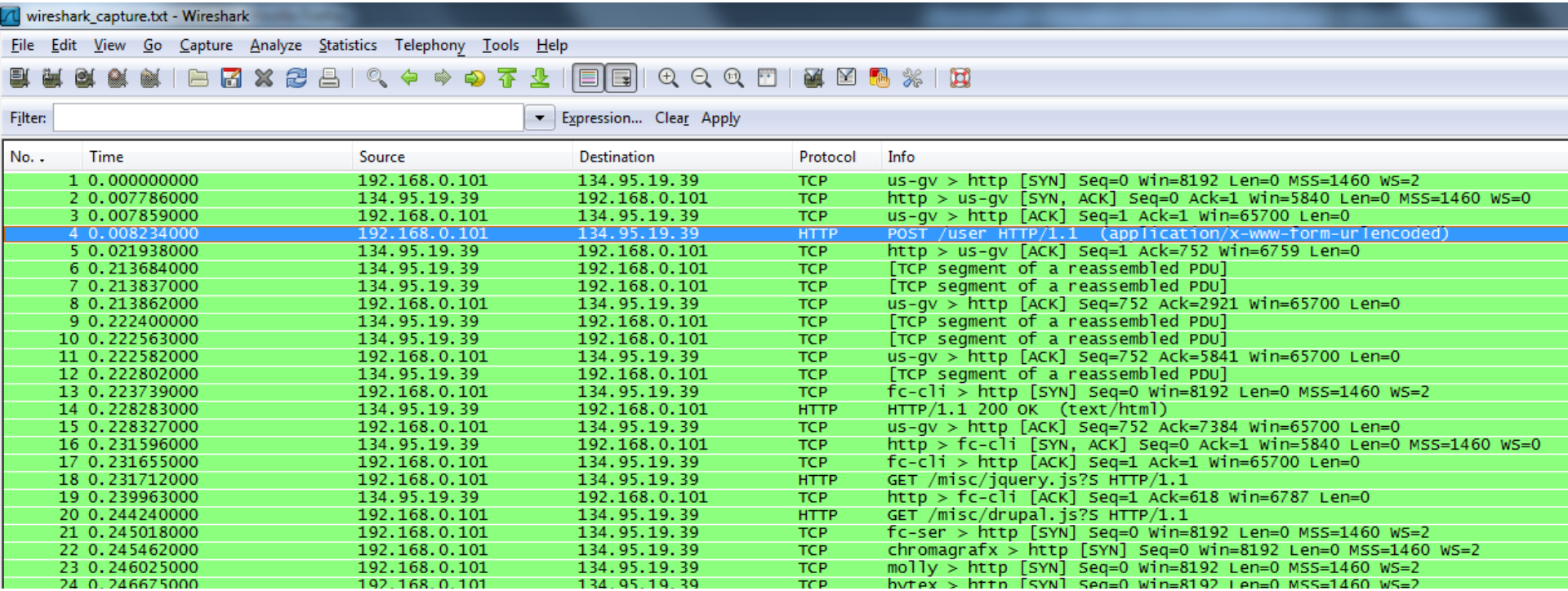
HTTP und die Sicherheit…

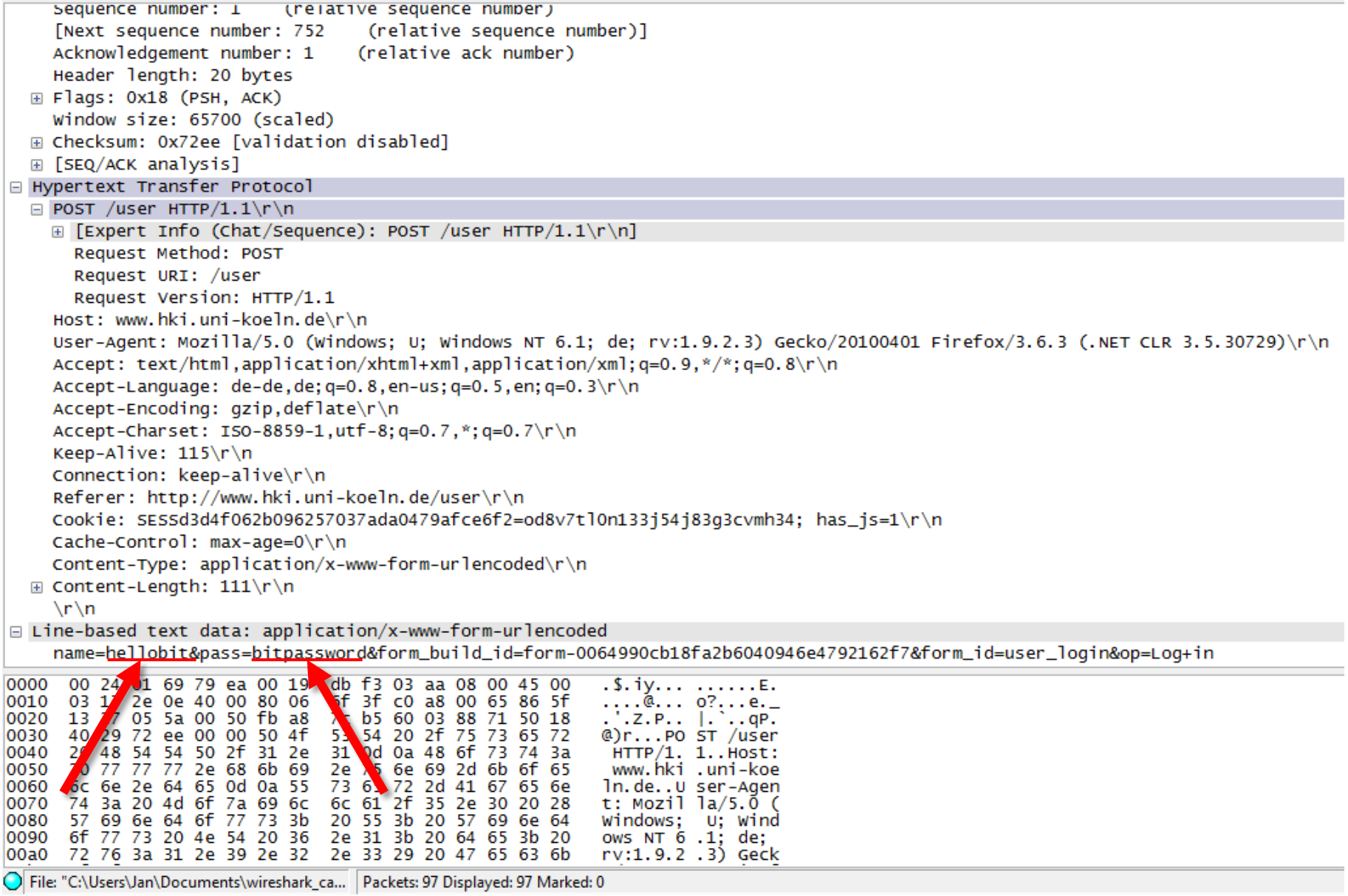
HTTP Sicherheit: Wireshark

Packet Sniffing mit Wireshark
(http://www.wireshark.org/)

HTTP Login auf hki.uni-koeln.de mit Benutzername „hellobit“ und Passwort „bitpassword“




wireshark_capture.txt - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000000 192.168.0.101 134.95.19.39 TCP us-gv > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
2 0.007786000 134.95.19.39 192.168.0.101 TCP http > us-gv [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 WS=0
3 0.007859000 192.168.0.101 134.95.19.39 TCP us-gv > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
4 0.008234000 192.168.0.101 134.95.19.39 HTTP POST /user HTTP/1.1 (application/x-www-form-urlencoded)
5 0.021938000 134.95.19.39 192.168.0.101 TCP http > us-gv [ACK] Seq=1 Ack=752 Win=6759 Len=0
6 0.213684000 134.95.19.39 192.168.0.101 TCP [TCP segment of a reassembled PDU]
7 0.213837000 134.95.19.39 192.168.0.101 TCP [TCP segment of a reassembled PDU]
8 0.213862000 192.168.0.101 134.95.19.39 TCP us-gv > http [ACK] Seq=752 Ack=2921 Win=65700 Len=0
9 0.222400000 134.95.19.39 192.168.0.101 TCP [TCP segment of a reassembled PDU]
10 0.222563000 134.95.19.39 192.168.0.101 TCP [TCP segment of a reassembled PDU]
11 0.222582000 192.168.0.101 134.95.19.39 TCP us-gv > http [ACK] Seq=752 Ack=5841 Win=65700 Len=0
12 0.222802000 134.95.19.39 192.168.0.101 TCP [TCP segment of a reassembled PDU]
13 0.223739000 192.168.0.101 134.95.19.39 TCP fc-cli > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
14 0.228283000 134.95.19.39 192.168.0.101 HTTP HTTP/1.1 200 OK (text/html)
15 0.228327000 192.168.0.101 134.95.19.39 TCP us-gv > http [ACK] Seq=752 Ack=7384 Win=65700 Len=0
16 0.231596000 134.95.19.39 192.168.0.101 TCP http > fc-cli [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 WS=0
17 0.231655000 192.168.0.101 134.95.19.39 TCP fc-cli > http [ACK] Seq=1 Ack=1 Win=65700 Len=0
18 0.231712000 192.168.0.101 134.95.19.39 HTTP GET /misc/jquery.js?S HTTP/1.1
19 0.239963000 134.95.19.39 192.168.0.101 TCP http > fc-cli [ACK] Seq=1 Ack=618 Win=6787 Len=0
20 0.244240000 192.168.0.101 134.95.19.39 HTTP GET /misc/drupal.js?S HTTP/1.1
21 0.245018000 192.168.0.101 134.95.19.39 TCP fc-ser > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
22 0.245462000 192.168.0.101 134.95.19.39 TCP chromagrafx > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
23 0.246025000 192.168.0.101 134.95.19.39 TCP molly > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2


Sequence number: 1 (relative sequence number)
[Next sequence number: 752 (relative sequence number)]
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes
Flags: 0x18 (PSH, ACK)
Window size: 65700 (scaled)
Checksum: 0x72ee [validation disabled]
[SEQ/ACK analysis]
Hypertext Transfer Protocol
POST /user HTTP/1.1\r\n
[Expert Info (Chat/Sequence): POST /user HTTP/1.1\r\n]
Request Method: POST
Request URI: /user
Request Version: HTTP/1.1
Host: www.hki.uni-koeln.de\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; de; rv:1.9.2.3) Gecko/20100401 Firefox/3.6.3 (.NET CLR 3.5.30729)\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3\r\n
Accept-Encoding: gzip,deflate\r\n
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
Keep-Alive: 115\r\n
Connection: keep-alive\r\n
Referer: http://www.hki.uni-koeln.de/user\r\n
Cookie: SESSd3d4f062b096257037ada0479afce6f2=od8v7tl0n133j54j83g3cvmh34; has_js=1\r\n
Cache-Control: max-age=0\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 111\r\n
\r\n
Line-based text data: application/x-www-form-urlencoded
name=hellobit&pass=bitpassword&form_build_id=form-0064990cb18fa2b6040946e4792162f7&form_id=user_login&op=Log+in
0000 00 24 01 69 79 ea 00 19 db f3 03 aa 08 00 45 00 .$.iy... ......E.
0010 03 1 2e 0e 40 00 80 06 6f 3f c0 a8 00 65 86 5f ....@... o?...e._
0020 13 7 05 5a 00 50 fb a8 7 b5 60 03 88 71 50 18 .'.Z.P.. |.`..qP.
0030 40 29 72 ee 00 00 50 4f 53 54 20 2f 75 73 65 72 @)r...PO ST /user
0040 2 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1. 1..Host:
0050 77 77 77 2e 68 6b 69 2e 6 6e 69 2d 6b 6f 65 www.hki .uni-koe
0060 6c 6e 2e 64 65 0d 0a 55 73 6 72 2d 41 67 65 6e ln.de..U ser-Agen
0070 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
0080 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e 64 Windows; U; Wind
0090 6f 77 73 20 4e 54 20 36 2e 31 3b 20 64 65 3b 20 ows NT 6 .1; de;
00a0 72 76 3a 31 2e 39 2e 32 2e 33 29 20 47 65 63 6b rv:1.9.2 .3) Geck
File: "C:\Users\Jan\Documents\wireshark_ca... Packets: 97 Displayed: 97 Marked: 0

HTTPS FTW!

→ https://www.ksk-koeln.de

HTTPS (Hypertext Transfer Protocol Secure)	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Verschlüsselte Datenübertragung
Port:	443/TCP

HTTPS im TCP/IP-Protokollstapel:

Anwendung	HTTP				
Transport	SSL/TLS				
	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Standards:	RFC 2818 (HTTP Over TLS, 2000)


Let's Encrypt
Dokumentation
Hilfe bekommen
Spenden
Über uns
Sprachen
Eine Non-Profit-Organisation, die TLS-Zertifikate für
260 Millionen Websites bereitstellt.
Lesen Sie unseren Jahresbericht 2021
Loslegen
Sponsern
AUS UNSEREM BLOG (AUF ENGLISCH)
19.05.2022
Nurturing Continued Growth of Our Oak CT Log
Only five organizations run a Certificate Transparency log, and the Let's Encrypt log is the only fully open source stack.
Mehr lesen
28.04.2022
TLS Beyond the Web: How MongoDB Uses Let's Encrypt for Database-to-Application Security
MongoDB uses millions of Let's Encrypt certs for critical workloads.
Mehr lesen
HAUPTSPONSOREN UND SPENDER
mozilla
cisco
EFF
OVHcloud
chrome
Internet Society
Meta
aws
IdenTrust
FORD FOUNDATION
shopify
THE BEST RUN SAP
AUTOMATTIC
Akamai
ALA American Library Association
cyon
infomaniak
HOSTPOINT
SiteGround
VULTR
PlanetHoster
fastly
3CX
SQUARESPACE
HawkHost
thebestvpn
JIMDO
VTEX

about certbot

What's Certbot?

Certbot is a free, open source software tool for automatically using Let's Encrypt certificates on manually-administrated websites to enable HTTPS.

Certbot is made by the Electronic Frontier Foundation (EFF), a 501(c)3 nonprofit based in San Francisco, CA, that defends digital privacy, free speech, and innovation.

Is Certbot right for me?

If you're looking to add the security and privacy benefits of an HTTPS certificate to your website, you may not need Certbot. Many hosting providers have internal tools to enable HTTPS. Before using Certbot, check if your hosting provider is one of them.

Certbot might be right for you if you:

+ have comfort with the command line ,
+ have an HTTP website that's already online , with port 80 open ,
+ and administer your website via a dedicated server , virtual private server , or cloud-hosted server , which you can access via ssh , and have the ability to sudo .

If you're ready to use Certbot, we provide customized instructions for your setup at the Certbot Instructions page.

Certbot renews certificates every 60 days. For more information about how Certbot works and for community managed resources, check out our Get Help page.

For more information around the codebase for Certbot and how to get involved as a developer, check out our Contribute to Certbot page.

Certbot is part of EFF's larger effort to encrypt the entire Internet. Websites need to use HTTPS to secure the web. Along with HTTPS Everywhere, Certbot aims to build a network that is more structurally private, safe, and protected against censorship.

Anwendungsschicht: Email

…Protokolle?

Email: Protokolle & Co.

Absenden / Weiterleiten von Ema

SMTP → Simple Mail Transfer Protocol

SMTP im TCP/IP-Protokollstapel:

Anwendung	SMTP				
Transport	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Standard:	RFC 5321

Abholen von Emails

POP3 (Post Office Protocol Version 3)	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Abholen von E-Mail vom Provider
Port:	110/TCP 995/TCP (Verschlüsselt)

POP3 im TCP/IP-Protokollstapel:

Anwendung	POP3				
Transport	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Standards:	RFC 1939 (POP3, 1996)

Internet Message Access Protocol	
Familie:	Internetprotokollfamilie
Einsatzgebiet:	Lesen und Verwalten von E-Mails
Ports:	143/TCP[1] 993/TCP (nur mit TLS)

IMAP im TCP/IP-Protokollstapel:

Anwendung	IMAP				
Transport	TCP				
Internet	IP (IPv4, IPv6)				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...

Standard:	RFC 3501

Email: Sicherheit

POP3 / SMTP / IMAP: ggf. ungesichert / unverschlüsselt

„Wenn die Regierungen in früheren Zeiten die Privatsphäre der Bürger verletzen wollten, mußten sie einen gewissen Aufwand betreiben, um die Briefpost abzufangen, unter Dampf zu öffnen und zu lesen oder Telefongespräche abzuhören und womöglich zu protokollieren. […]
Heute ersetzt die Elektronische Post allmählich die herkömmliche Briefpost […]. Im Gegensatz zur Briefpost sind E-Mails unglaublich leicht abzufangen und auf interessante Stichwörter hin elektronisch zu prüfen. Das läßt sich ohne weiteres, routinemäßig, automatisch und nicht nachweisbar in großem Maßstab bewerkstelligen.“

(Phil Zimmermann, zitiert nach Singh, Simon: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. Deutscher Taschenbuch Verlag. München. 2000. S. 357.)

Email: Sicherheit

Vgl. golem.de: http://www.golem.de/news/ueberwachung-millionfache-e-mail-filterung-der-geheimdienste-ohne-richter-1202-90072.html (27.02.2012):

„Laut einem Bericht des Parlamentarischen Kontrollgremiums (PKG) haben die Geheimdienste Verfassungsschutz, Bundesnachrichtendienst und Militärischer Abschirmdienst (MAD) im Jahr 2010 die Inhalte von Millionen E-Mails durchsucht und dabei in über 37 Millionen elektronischen Nachrichten verdächtige Suchbegriffe gefunden. Die Versechsfachung gegenüber dem Vorjahr sei der Zunahme von Spam geschuldet, hieß es zur Begründung. Gesucht wurde nach rund 15.300 Begriffen aus den Bereichen Terrorismus, Massenvernichtungswaffen und Schleusung. In nur 213 Fällen ergaben sich durch die millionfache E-Mail-Überwachung verwertbare Hinweise für die Geheimdienste.“

Pretty Good Privacy (PGP), Anwendungsschicht

```
-----BEGIN PGP MESSAGE----- […]
qANQR1DBwEwD4PSJmhZ2mJoBB/oDkeTMBP+qTZCbrH0x+ltec/FpCwYLrojTKR4O
he1qjeJshaR5j6B0tpYeLGiRf/4OfkKNNDCmRjkT9ofRCgv5GO9sz6WOeZiMWhjU
hT1LF8K84xLvCeXPIwdFNThF3vFktuMTy1fDfl/nFDSjXsigD/3mmbHmN0S9bbUE
XfEaceWPSiHqIZME9Mr57LeySCag2LVBtAVFN4+aMRH9q/YDB4KKXlUcmIR4z64K
WU4fFpdQ7Bp30JCi4L/1R3d9AQgnhdgnv253yYJ1qS+XcVxCcXVEHaChcfUcoNWs
4puujwCdTrcFIEuF9iJeszVxWKFFNOkq9GbQ6w//F/a0tVs2wcBMA24E5h1oRymC
AQf8CzQOAQcJspYpeiD1eibRptJTEFiELgylFmO7lEwGhpUQgfmP9EYBnbuYYMF1
Hr3rWEcZBqVqk6C0XEo04H/I4QXr47wRQEYiiSEo088J6eY2PUySOAnv/ITqC0zq
zv2u+/qGrwiexgqYkLbzh0Yz4LxPZJPUcmoEE/eySfuVUldupxqbBAGZaMLzDNxW
IyETP4zK4NjAzy4NbDmU7A3hF0cBY4BZwapd+o1sbxuZ7PVgAqi1gNF3favGb/u0
KwzevoKFxf1nyePnQwTkQYvG49Eb2vEa0DEVnvpZZvUUPFigqD2X1052pqDrafZ0
eZAqFPCvGVSb8Tgg6wOtZxtgDcHATANGok9/6C2khQEIAJ5CHLfef8DR+e+3mjxL
OkcL+JzD6O3JMIK6iylaLrc/sKsZUUC0JTbvm6KdQU4IheTQkS0t0IEvYO652NL+
PMHmQ4qmyX/natFyUlZOlTGJzhLP/n659Uq4zZg9dmDHNZZPvH/ShvPDBJLacKTO
s5fHxswh9EDjlp+zlfUm8M1C7dGMoKhyciqtl4rK7Ag5/YyRR+kZFA3RFwIFRjyM […]
-----END PGP MESSAGE-----
```

PGP IM PARLAMENT

Warum mein Abgeordneter keine PGP-Mail öffnen kann

Offiziell fordert das Europäische Parlament *"Ende-zu-Ende-Verschlüsselung als Selbstverständlichkeit"*. Sucht man jedoch eine Möglichkeit, seinem Abgeordneten eine verschlüsselte E-Mail zu senden, trifft man auf ahnungslose Politiker, frustrierte Mitarbeiter und eine sehr vorsichtige IT-Abteilung - und das in Berlin genau wie in Brüssel.

E-Mail-Verschlüsselung gibt es seit Jahrzehnten. Seit der Veröffentlichung von GnuPG im Jahr 1997 unter der GNU Public License steht sie prinzipiell jedem zur kostenfreien Nutzung offen. Und trotzdem scheint diese sichere Art der elektronischen Kommunikation für die meisten Politiker und politischen Institutionen weiterhin Neuland zu sein.

Die Frage ist dabei, wie sich Wähler mit sensiblen Anliegen auf sichere Art und Weise an ihre politischen Vertreter wenden können. Könnten Whistleblower eine Politikerin sicher auf Missstände hinweisen? Bei dem weitreichenden Hackerangriff auf den Deutschen Bundestag im Frühsommer 2015 wurden immerhin gigabyteweise E-Mails unerlaubt kopiert. Eigentlich müsste man annehmen, dass in den Parlamenten eine ganze Horde von IT-Experten an Lösungen für die sichere Kommunikation unserer Abgeordneten arbeitet. Wir

Ein Ausschnit aus dem PGP-Key des EU-Abgeordneten Jan Philipp Albrecht - nur wenige Abgeordnete sind so erreichbar. (Bild: Golem.de)

Artikel: PGP IM PARLAMENT
Warum mein Abgeordneter keine PGP-Mail öffnen kann

Inhalt:
- Ende-zu-Ende-Verschlüsselung im EU-Parlament?
- Pilotprojekt für S/MIME läuft, Zukunft ungewiss

Datum: 26.4.2016, 12:04

Autor: Jan Weisensee

Themen: PGP, Bundesregierung, E-Mail, EU, Ende-zu-Ende-Verschlüsselung, Exchange, Groupware, NSA, Spionage, Verschlüsselung

Bildnachweise

- https://commons.wikimedia.org/wiki/File:Universitat_zu_Koln_Hauptgebaude_ost.jpg
- http://causeitsallaboutthepayno.tumblr.com/post/131746453874/im-currently-listening-to-adeles-new
- www.giphy.com
- http://www.elandroidelibre.com/wp-content/uploads/2015/11/spam.jpg
- http://www.golem.de/news/pgp-im-parlament-warum-mein-abgeordneter-keine-pgp-mail-oeffnen-kann-1604-120506.html
- https://ec.europa.eu/commission/2014-2019/oettinger_en