Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Kai Henken

Internetbasierte Tracking-Technologien

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Kai Henken

Internetbasierte Tracking-Technologien

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Bachelor of Science Angewandte Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr.-Ing. Martin Hübner
Zweitgutachter: Prof. Dr. Klaus-Peter Kossakowski

Eingereicht am: 13.10.2016

Kai Henken

Thema der Arbeit
Internetbasierte Tracking-Technologien

Stichworte
Internet, Tracking, Web-Tracking, Technologien, Verfahren, Protokolle, Kommunikation, Analyse, Identifizierung, Schutzmechanismen, Werkzeuge, Einstellungen, Erweiterungen, Firefox

Kurzzusammenfassung
In dieser Arbeit werden verschiedene Tracking-Technologien vorgestellt und deren Verfahren erklärt. Anschließend werden Methoden beschrieben, die dem Nutzer helfen, sich vor Tracking-Technologien zu schützen. Diese Schutzmechanismen wurden mit praktischen Messungen untersucht und deren Ergebnisse anhand verschiedener Kriterien verglichen und bewertet. Der Einsatz dieser Schutzmechanismen hat allerdings fast immer eine Einschränkung bei der Nutzung von Webseiten zur Folge.

Kai Henken

Title of the paper
Internet-based tracking-technologies

Keywords
Internet, tracking, web-tracking, technologies, procedures, protocols, communication, analysis, identification, protective mechanisms, tools, settings, extensions, Firefox

Abstract
This thesis describes different tracking technologies and their corresponding processes. In the following several methods are introduced which help the user to protect himself against various tracking technologies. These methods against tracking are evaluated and the results are compared and rated by using different criteria. However, in many cases the application of these protective mechanisms leads to limitations in the use of webpages.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABP	Adblock Plus
AH	Authentication Header
API	Application Programming Interface
cURL	Client for URLs
DES	Data Encryption Standard
DNS	Domain Name System
DNT	Do Not Track
DoD	Department of Defense
DTLS	Datagram Transport Layer Security
EFF	Electronic Frontier Foundation
ESP	Encapsulating Security Payload
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IMF	Internet Message Format
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet Service Provider
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
MDN	Message Disposition Notification
NAT	Network Address Translation
NS	Nameserver
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-shared Key
QUIC	Quick UDP Internet Connection
RTC	Real-Time Communication
SLAAC	Stateless Address Autoconfiguration
SOCKS	Socket Secure
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UIDH	Unique Identifier Header

URL	Uniform Resource Locator
VPN	Virtual Private Network
W3C	World Wide Web Consortium

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einleitung

Der Begriff “Internet der Dinge” bezeichnet die Weiterentwicklung der digitalen Vernetzung. Die Anzahl verschiedener Geräte, die miteinander über das Internet kommunizieren wächst stetig. Seit den Enthüllungen von Edward Snowden stehen Informationen der öffentlichkeit bereit, dass die Kommunikation durch staatliche Organisationen überwacht wird. Darüber hinaus versuchen Unternehmen, stets mehr Informationen über ihre Nutzer zu erfassen und zu verwerten.

1.1 Hinweis

Die Texte dieser Abschlussarbeit beinhalten aus Gründen der sprachlichen Vereinfachung und der besseren Lesbarkeit lediglich die männliche Form. Ungeachtet dessen, dass die männliche Form verwendet wird, beziehen sich diese Ausführungen gleichermaßen auf weibliche und männliche Personen.

1.2 Problemstellung

Die Nutzer kommen immer früher in Kontakt mit technischen Geräten, die Daten über einen Nutzer erheben können. Ein Teil der jüngeren Generationen nutzt sogar schon verschiedene Geräte, wie z.B. Smartphone, Tablet, Notebook und Computer. Eine Studie des BITKOM Vereins zeigt, dass bereits 65 Prozent aller Deutschen ab 14 Jahren ein Smartphone nutzen, 89 Prozent sind es bei den 14- bis 29- Jährigen (vgl. [Lut+15]).

Ein Großteil der Nutzer von diesen Geräten ist sich über den Umfang und die möglichen Folgen des Trackings und dem Verknüpfen der Informationen nicht bewusst, weil sie die Geräte samt der Technologien nicht als solche kennengelernt haben oder sie die Technologie nicht weiter hinterfragen. Außerdem sind die meisten Technologien so konzipiert, dass der Nutzer nicht ohne Weiteres feststellen kann, ob eine Datenerhebung stattfindet oder nicht.

1.3 Zielsetzung

Das Ziel dieser Arbeit ist es, einen fundierten Überblick über die Tracking-Technologien zu vermitteln. Dieser Überblick soll zeigen, dass viele verschiedene Möglichkeiten existieren, die Unternehmen, Organisationen oder auch staatliche Organisationen dazu nutzen können, um Nutzer zu tracken oder zu identifizieren.

Außerdem soll der Überblick dem Nutzer helfen herauszufinden, welche Geräte und Technologien ein Tracking ermöglichen. Danach bleibt es dem Nutzer überlassen, ob er sich mithilfe der vorhandenen Lösungen vor einem möglichen Tracking schützen möchte. Hierfür werden die Lösungen vorgestellt, untersucht und nach verschiedenen Kriterien bewertet.

1.4 Motivation

Die Menschen in der heutigen Zeit haben eine sehr große Auswahl an technischen Geräten, die sie nutzen und kaufen. Die meisten dieser Geräte können den Nutzern das Leben vereinfachen, aber viele dieser Geräte sind lediglich zur Unterhaltung und Motivierung zur Fitness gedacht.

Die Studie von BITKOM zeigt, dass schon Kinder im Alter von 6 bis 7 Jahren in Kontakt mit mehreren verschiedenen Geräten, wie z.B. Smartphone, Tablet, Notebook, Computer, etc., kommen und diese benutzen. Überwiegend sind es die Geräte der Eltern, die von den Kindern benutzt werden. Je älter die Kinder und Jugendlichen sind, desto höher ist der prozentuale Anteil unter ihnen, der diese Geräte besitzt und nutzt(siehe Tabelle 1.1). [BITKOM14]

Gerät	10 - 11 Jahre	12 - 13 Jahre	14 - 15 Jahre	16 - 18 Jahre
Smartphone	50%	84%	85%	88%
Laptop / Notebook	18%	41%	49%	60%
Desktop	16%	24%	32%	38%
Tablet	11%	23%	20%	16%

Tabelle 1.1: Ausschnitt der Nutzung von verschiedenen Geräten [BITKOM14]

Ein Großteil der Kinder, Jugendlichen und Erwachsenen ist sich nicht bewusst, dass es möglich ist, zum Beispiel ihr Nutzungsverhalten auf verschiedenen Geräten zu tracken. Werbeunternehmen versuchen ständig, aktuelle und ausführliche Informationen über die Nutzer zu erheben. Sie versuchen die Geräte eines Nutzers zu identifizieren und die erhobenen Informationen mit-

einander zu verknüpfen. Die Unternehmen und Organisationen aus anderen Tätigkeitsfeldern nutzen die Datenerhebung beispielsweise für interne Analysezwecke oder um Vorhersagen treffen zu können.

Unternehmen, die eine Datenerhebung der Nutzer vollziehen, bieten häufig ein Opt-out (zu dt. *sich gegen eine Datenerhebung entscheiden*) Verfahren an. Das Gegenteil vom Opt-out Verfahren ist das Opt-in Verfahren. Das Opt-in Verfahren ist meistens standardmäßig aktiviert. Nutzer, die eine Datenerhebung zulassen, möchten häufig das Unternehmen unterstützen oder andere Vorteile der Datenerhebung nutzen. Nutzer, die sich jedoch gegen eine Datenerhebung entscheiden, nutzen das Opt-out Verfahren, falls dieses vorhanden ist. Oder sie versuchen, sich mit anderen Lösungen vor der Datenerhebung zu schützen.

Es gibt unterschiedliche Gründe, weshalb ein Nutzer oder Unternehmen vermeiden möchte, dass eine Datenerhebung stattfindet:

Anonymität
: Sie wollen keine zusätzlichen Informationen Dritten überlassen, die ein detailliertes Bild über sie ermöglichen. Die weitere Datenerhebung soll ausschließlich in anonymisierter Form fortgesetzt werden.

Privatsphäre
: Ähnlich dem Punkt der Anonymität. Sie möchten genau beeinflussen können, welche Informationen Dritten zur Verfügung stehen. Beispielweise erhalten Dritte nur minimale oder manipulierte Informationen. Darüber hinaus möchten einige Anwender selbst die Erhebung von anonymisierten Informationen verhindern.

Performanz
: Sie möchten die Geräte oder Dienste möglichst performant nutzen können, sodass diese nicht durch überflüssige Zusatzfunktionen oder sogar Dritte gebremst werden.

Sicherheit
: Je ausführlicher die Informationen über den Nutzer sind, die von Dritten gesammelt werden, desto lukrativer sind diese Datensätze auch für Insider, Hacker oder weitere Dritte.

Dem Autor sind keine umfassenden und technologieübergreifenden Analysen der verschiedenen Tracking-Konzepte zum Zeitpunkt der Arbeit bekannt. Es werden einige Veröffentlichungen für die Ausarbeitung und Fundierung der Kapitel Grundlagen, Tracking-Technologien und Tracking-Schutzmechanismen verwendet.

Es wäre hilfreich, wenn eine Übersicht der verschiedenen Tracking-Technologien und der vorhandenen Lösungen existieren und veröffentlicht würde. Damit könnten sich Nutzer und Unternehmen einen Überblick verschaffen und sich ggf. vor dem Tracking mit den vorgeschlagenen und untersuchten Lösungen schützen können.

1.5 Themenabgrenzung

In dieser Arbeit werden ausschließlich die technische Realisierung verschiedener Tracking-Verfahren und mögliche Schutzmechanismen beschrieben und bewertet. Es wird nicht auf die Aspekte des Datenschutzes eingegangen, und es wird kein Ausblick auf künftige Verwendungsmöglichkeiten der durch Tracking erhaltenen Informationen gegeben.

1.6 Struktur der Arbeit

Die Arbeit glieder sich wie folgt: Im 2. Kapitel werden der Begriff des “Trackings” erläutert und die Ursachen genannt, weshalb eine Datenerhebung so interessant für Dritte ist. Anschließend werden im 3. Kapitel die verschiedenen Technologien des Trackings untersucht und reflektiert. Danach folgen im 4. Kapitel die Vorstellung, Untersuchung und Bewertung von vorhandenen Lösungen, die ein Tracking verhindern könnten.

2 Grundlagen

In diesem Kapitel werden die Definition und Bedeutung der folgenden Begriffe und Sätze erläutert.

2.1 Definition von Tracking

Tracking (zu dt. *die Verfolgung*) bedeutet das Nachführen oder Verfolgen von Objekten.

Tracking wird heutzutage in verschiedenen Bereichen genutzt. Es wird beispielweise in der Industrie in folgenden Kontexten verwendet:

Tracking
: Tracking wird im Allgemeinen zur Objekterfassung verwendet. Es wird z.B. im Bereich der Luftfahrt, Automobilbranche, Versand und vielen weiteren Bereichen genutzt. In diesem Kontext werden Objekte erfasst, wie z.B. Flugzeuge, Autos, Fußgänger, Pakete oder andere Objekte, und in ihrer Bewegung verfolgt.

Eyetracking
: Beim Eyetracking werden die Blickbewegungen des Auges mithilfe einer Kamera aufgezeichnet und analysiert.

Mousetracking
: Das Mousetracking erfolgt meistens per Software und es wird die Interaktion vom Mauszeiger eines Computers aufgezeichnet und analysiert.

Motion Tracking
: Beim Motion Tracking werden die Körperbewegungen einer oder mehrerer Personen erfasst und analysiert.

Web-Tracking
: Das Web-Tracking oder auch User-Tracking ist eine komplexe Form des Tracking. Es erfolgt über das Internet und sammelt Informationen über das Nutzerverhalten.

Es gibt keine klare Definition des Web-Trackings. Deshalb stützt sich die Arbeit auf die Definition des Web-Trackings im Sinne der Erhebung und Analyse von Nutzerdaten mithilfe von

technischen Geräten. Zur Datenerhebung werden verschiedene Internetdienste genutzt, welche die Nutzerdaten aus unterschiedlichen Gründen sammeln, zusammenführen und analysieren. Die Internetdienste verfolgen unterschiedliche Ziele bei der Nutzung dieser Daten. Diese könnten z.B. zur Weiterentwicklung des Dienstes, Erstellung von Statistiken, Vorhersagen des Nutzerverhaltens oder aber auch für kommerzielle Zwecke verwendet werden. [BBDI13]

Die internetbasierten Tracking-Technologien ermöglichen, dass Nutzer eindeutig identifiziert werden können. Dazu werden die digitalen Spuren des Nutzers verwendet, die eindeutige Identifikatoren beinhalten. Damit ist es möglich, einen Nutzer auch ohne ohne lokal gespeicherte Informationen (beispielsweise einen Cookie) zu identifizieren. [BBDI13]

2.2 Internet of Things (IoT)

Was ist das "Internet of Things" (zu dt. *Internet der Dinge*)? Das Internet der Dinge hat keine klare Definition. Es beschreibt die Kommunikation von "intelligenten" Geräten [Sha+16]. Andere Begriffe, die Ähnliches beschrieben haben, haben sich lediglich nicht durchsetzen können, weil der technologische Fortschritt dies nicht zuließ.

Seit 2010 kam es zu einem stärkeren Wachstum der Geräte [Mor14], die zum Internet der Dinge zählen. Die folgenden drei Faktoren waren dafür ausschlaggebend:

1. Breitbandverbindungen und Funk-Netzwerke sind weiter verbreitet und die dazugehörigen Kosten sind gesunken.
2. Die Kosten für Funk-Sensoren und -Chips sind gesunken, weshalb die Hersteller diese direkt in die Geräte einbauen.
3. Es ist inzwischen möglich, die unstrukturierten Daten zu speichern, tracken und analysieren.

Die "Libelium Smart World" (siehe Abbildung 2.1) zeigt eine mögliche Zukunft, wie sich das Internet der Dinge entwickeln und genutzt werden könnte. Jedes dieser Geräte sendet Informationen über das Internet, diese Informationen werden automatisch ausgewertet. Daraus können verschiedene Sicherheitsrisiken entstehen. Zum einen wird unberechtigter Zugriff und Missbrauch von persönlichen Daten ermöglicht und zum anderen werden Angriffe auf andere Systeme vereinfacht. [FTC2015]

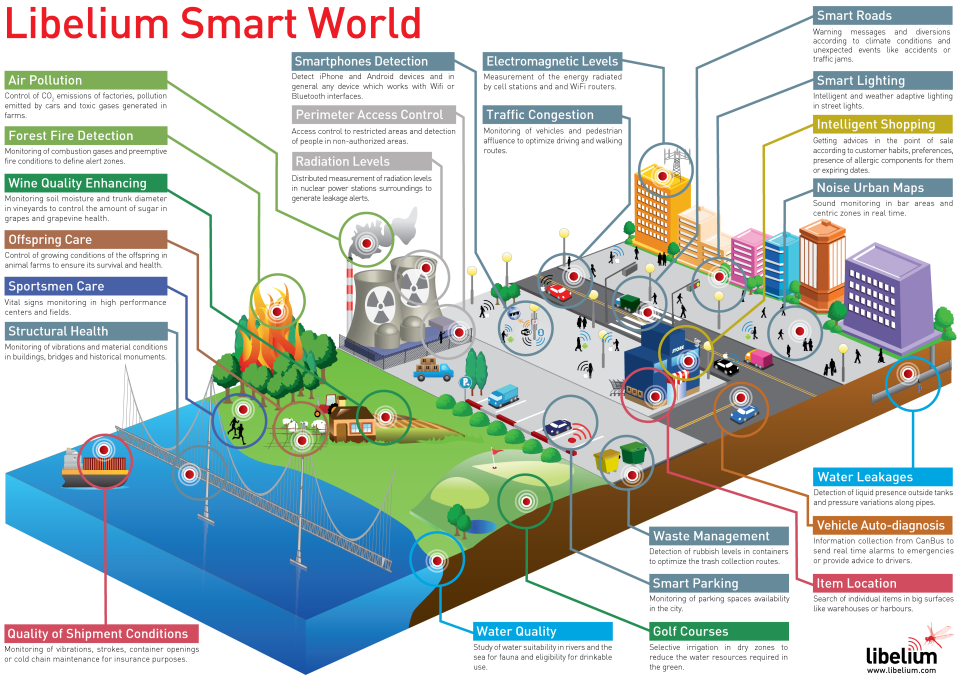


Abbildung 2.1: Libelium Smart World[1]: Eine mögliche Zukunft vom "Internet der Dinge"

Laut Prognosen von Gartner steigt die Zahl der IoT-Geräte in den nächsten Jahren noch um ein Vielfaches. Allein in diesem Jahr sollen täglich 5,5 Millionen Geräte hinzukommen. Bis 2020 werden es voraussichtlich fast 20,8 Milliarden Geräte sein (siehe Tabelle 2.1) [Gartner15].

Kategorie	2014	2015	2016	2020
Verbraucher	2.277	3.023	4.024	13.509
Business: branchenübergreifend	632	815	1.092	4.408
Business: branchenspezifisch	898	1.065	1.276	2.880
Gesamt	3.807	4.902	6.392	20.797

Tabelle 2.1: Internet of Things: Geräte[2] [Gartner15]

[1] Quelle: `http://www.libelium.com/top_50_iot_sensor_applications_ranking/#show_infographic` (Abruf: 25.04.2016)

[2] Die Anzahl Geräte in Millionen.

2.3 “Daten sind das neue Öl”

Durch die internetbasierten Tracking-Technologien und das Internet der Dinge wird der Traffic, der über die Internet-Knoten verläuft, in den nächsten Jahren noch weiter ansteigen. Anhand der Statistik (siehe Abbildung 2.2), die z.B. der Internet-Knoten von DE-CIX zur Verfügung stellt, ist es möglich, sich ein grobes Bild vom Datenaufkommen der letzten fünf Jahre bis heute im Internet zu machen. Dieser Internet-Knoten ist nach Datendurchsatz und angeschlossenen ISPs einer der größten der Welt.

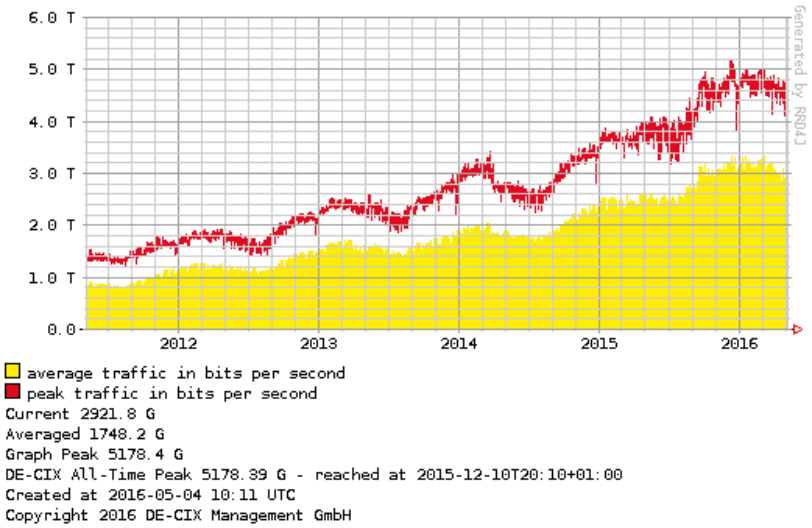


Abbildung 2.2: DE-CIX[1]: Traffic vom Internet-Knoten Frankfurt

Bereits im Jahre 1990 wurden Unmengen an Daten gesammelt und diese Daten wurden mithilfe von systematischen Analysen ausgewertet. Damals waren die Daten jedoch aus einer wesentlich geringeren Anzahl von Quellen und es war lediglich möglich, Analysen auf Daten aus der Vergangenheit zu erstellen. Aus diesen Ergebnissen wurden Prognosen erstellt, die im Unternehmen dazu verwendet wurden, die Ziele und strategische Entscheidungen zu optimieren. Die Prognosen waren jedoch ungenau, sodass sie zu einer unsicheren Zukunft führten. [Bü13]

Die heutigen Geräte und Technologien können umfangreiche Datenmengen innerhalb von kürzester Zeit sammeln und zur Verfügung stellen. Dazu kommt noch, dass die Nutzer verschiedene Dienste im Internet nutzen und weitere Daten und Informationen hinterlassen, indem sie die

[1]Quelle: `https://www.de-cix.net/about/statistics/` (Abruf: 04.05.2016)

Produkte oder Dienste der Unternehmen nutzen. Die Informationen reichen von Nachrichten bis persönliche Daten wie Namen, Orte oder sogar Gesundheitsdaten. Die allgemeine Problematik dabei für die Unternehmen und Organisationen ist, dass die Daten aus verschiedenen Quellen stammen, unterschiedlich schnell zur Verfügung stehen, unvorhersagbar und unstrukturiert ankommen. Zu Zeiten von "Big Data" [Bü13] ist dies inzwischen ein geringeres Problem, da alle Daten gesammelt und anschließend analysiert werden können. Mithilfe dieser Informationen können zum Beispiel neue Produkte und weitere Dienstleistungen entwickelt werden.

Es gibt heute viele Unternehmen, die ihre Produkte und Dienste kostenlos oder gegen einen geringen Betrag zur Verfügung stellen. Musterbeispiele von Unternehmen sind hierfür Google [Kep13] und Facebook [Sol11]. Bei diesen Unternehmen wird der Nutzer zum Produkt, da die Unternehmen die Informationen der Nutzer benötigen und verwenden, um den Nutzer möglichst zielgerichtete Werbung zu zeigen oder ihm kostenpflichtige Produkte und Dienste anbieten zu können.

2.4 Big Brother Awards

Passend und erwähnenswert zum Thema dieser Arbeit ist der "Big Brother Award" [PI], der ein Negativpreis für Unternehmen, Organisationen und Personen ist. Es gibt ihn bereits seit dem Jahre 1998. Erst nur in England, aber danach auch in verschiedenen Ländern, in denen er von Vereinen und Organisationen organisiert und verliehen wird. Der "Digitalcourage e.V." übernimmt diese Aufgabe für Deutschland. Der Preis wird denjenigen verliehen, "die in besonderer Weise und nachhaltig die Privatsphäre von Menschen beeinträchtigen oder persönliche Daten Dritten zugänglich machen". [Dig]

3 Tracking-Technologien

3.1 Allgemein

Generell kann beim Tracking zwischen zustandsbehafteten und zustandslosen Trackings unterschieden werden. In der wissenschaftlichen Arbeit [MM12] werden die beiden Klassifizierungen des Trackings differenziert. Beim zustandsbehafteten Tracking werden zusätzliche Informationen vom Betreiber der Webseite beim Nutzer gespeichert. Die Speicherung der Informationen kann beispielsweise durch Cookies (siehe Kapitel 3.1.5), Benutzerdaten und den lokalen Speicher des Browsers erfolgen. Beim zustandslosen Tracking werden die Informationen genutzt, die der Nutzer dem Betreiber der Webseite zur Verfügung stellt. Die Arbeit [Eck10] zeigt, dass der Fingerprint (siehe Kapitel 3.1.4) des Browsers von 83,6% der Besucher eindeutig war. Bei Besuchern, die Adobe Flash oder eine Java Virtual Machine aktiviert hatten, war der Fingerprint sogar zu 94,2% eindeutig. Dazu wurden die Fingerprints von 470.161 Teilnehmern, die die Webseite `panopticlick.eff.org` besucht hatten, untersucht.

3.1.1 Metadaten

Metadaten sind Informationen, die der Nutzer, wenn überhaupt, nur unter bestimmten Umständen zu Gesicht bekommt. Es sind zusätzliche Informationen innerhalb der Daten bzw. der Dateien, welche die Merkmale und Eigenschaften der Daten beinhalten. Aus diesem Grunde sind sie auch nicht notwendig, um die Daten verwenden zu können. Diese Informationen fallen überall im digitalen Bereich an, sei es nur ein Zeitstempel oder ähnliches.

Als einfaches Beispiel für Metadaten dienen die Eigenschaften eines Word-Dokuments. Diese beinhalten zusätzlich zu dem Inhalt des Dokuments noch weitere Informationen, die teilweise in der Abbildung 3.1 ersichtlich werden.

Diese Technologie kann und wird auch beim internetbasierten Tracking genutzt. Viele Webseiten nutzen beispielsweise Werkzeuge zur Web-Analyse [Akk16], womit es dem Anbieter der Webseite möglich ist, eine genaue Analyse und Auswertung bezüglich des Besucherverhaltens

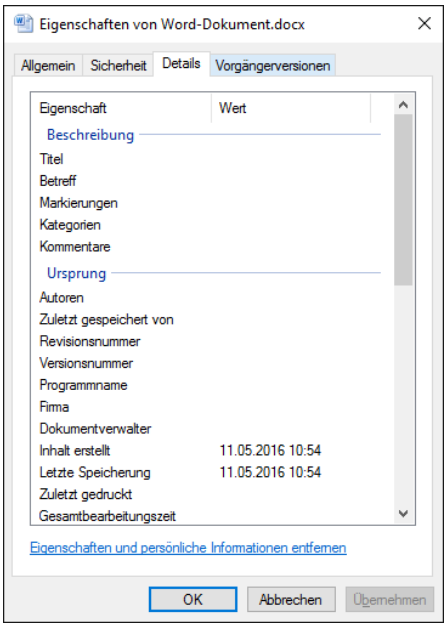


Abbildung 3.1: Eigenschaften eines Word Dokuments

machen zu können. Diese Werkzeuge können unter anderem die Metadaten der HTTP(S)-Anfragen auswerten und dadurch z.B. feststellen, aus welchen Land der Besucher stammen könnte. Außerdem kann festgestellt werden, welche Browser, welches Betriebssystem und welche Plugins vom Besucher verwendet wurden und mehr.

3.1.2 Nachladen von Objekten

Bei diesem Verfahren wird die Technik des Web Beacons [RBE03] verwendet. Beim Web Beacon wird beispielsweise ein winziges Bild ($\approx$ 1x1 Pixel groß), das meistens transparent oder in der Farbe des Hintergrunds ist, eingebunden. Öffnet nun der Nutzer das Dokument, die E-Mail oder die Webseite, in dem der Web Beacon eingebaut ist, dann wird das Bild automatisch vom Webserver (siehe Kapitel 3.3.1) nachgeladen - sofern das Nachladen nicht verhindert wird.

3.1.3 Einbinden von Referral-Links

Referral-Links unterscheiden sich kaum zu normalen Links, sie beinhalten in der aufzurufenden URL zusätzliche Parameter. Werbeunternehmen nutzen dieses Verfahren [Lee09] mithilfe von Webservern (siehe Kapitel 3.3.1), damit sie weitere Informationen über einen Besucher erhalten.

Dies ist möglich durch die Parameter, die vom Unternehmen vergeben werden. Diese sind eindeutig und personalisiert oder mit anderen Informationen verknüpft.

3.1.4 Fingerprint

Beim Fingerprinting werden häufig mehrere verschiedene Merkmale eines Nutzers verknüpft. Die Kombination der Merkmale bildet meistens ein eindeutiges Wiedererkennungsmerkmal des Nutzers, das als Fingerprint (zu dt. *Fingerabdruck*) bezeichnet wird. Mithilfe dieses Fingerprints ist der Nutzer solange identifizierbar bis er eines der ursprünglichen Merkmale verändert wird und sich dadurch der gebildete Fingerprint ändert.

Beim Canvas Fingerprinting [MS12] wird das Rendern von Schriftarten genutzt. Das Rendern der Schriftart ist abhängig von der Konfiguration des Browsers, vom Betriebssystem, vom Grafikkarten Treiber, von der Grafikkarte und der Einstellung des Bildschirms. Vom Ergebnis des Renderns wird ein kryptografischer Hash-Wert gebildet und dieser wird als eindeutiger Fingerprint verwendet.

3.1.5 Cookies

Cookies werden dazu verwendet, um einen Nutzer bei einem weiteren Besuch der Webseite eindeutig identifizieren zu können. Es existieren unterschiedliche Arten von Cookies. Ursprünglich wurden Cookies in Form von Textdateien (siehe Abbildung 3.2) gespeichert. Alternativ sind noch die Möglichkeiten vorhanden Cookies im Flash-Speicher abzulegen oder den Cache des Browsers als eine Art Cookie zu verwenden. Als Webseiten-Betreiber ist es möglich, den HTTP-Antworten einen sogenannten ETag [W3CETag] als HTTP-Kopfzeile hinzuzufügen und diesen als eine Art Cookie zu verwenden.

```
Name: remid
Inhalt: 1539958357804419587
Host: .bild.de
Pfad: /
Senden für: Jeden Verbindungstyp
Gültig bis: Donnerstag, 31. Dezember 2037 23:55:55 GMT
```

Abbildung 3.2: Beispiel eines Cookies in Form einer Textdatei

3.2 Protokolle

Für ein besseres Verständnis, in welchem Zusammenhang die Protokolle zueinanderstehen, ist die Darstellung in der vier Schichtenarchitektur des Department of Defense (DoD) sinnvoll. Diese Schichtenarchitektur ist im [RFC1122] definiert. Im DoD-Schichtenmodell lassen sich die betrachteten Technologie gut darstellen - siehe dazu Tabelle 3.1.

Nr.	Schicht	Dienste / Protokolle / Anwendungen		
4	Anwendung	HTTP	HTTPS	DNS
3	Transport	TCP		UDP
2	Internet	IP (IPv4 / IPv6)		
1	Netzzugriff	Ethernet		

Tabelle 3.1: DoD-Schichtenmodell der betrachteten Protokolle

3.2.1 Internet Protocol Version 4 (IPv4)

Eine IP-Adresse ist immer eindeutig, sie ist die Grundlage, damit Rechner in einem Netzwerk kommunizieren können. Sie bildet auch die Grundlage für viele Tracking-Technologien, weil es mit ihr möglich ist, einen Nutzer bzw. einen Anschluss zu identifizieren. Im übertragenen Sinne könnte eine IP-Adresse mit der Anschrift einer Wohnung bzw. eines Hauses verglichen werden. Sie besteht aus einem Netzanteil (Ort, Postleitzahl und Straße) und einem Hostanteil (Hausnummer).

Beispiel IPv4 Adresse: `31.18.132.172`

Bei dieser Beispiel IP Adresse könnte es wie in Tabelle 3.2 aussehen.

Netzanteil:	`31.18`
Hostanteil:	`132.172`

Tabelle 3.2: Netz- und Hostanteil

Der Netzanteil könnte für irgendeine Straße in Hamburg stehen und mithilfe des Hostanteils ist die genaue Identifizierung des Anschlusses bekannt. Es könnte sogar sein, dass der Hostanteil `132.173` dem nächsten Anschluss entspricht, der nur eine Hausnummer weiter liegt.

Dem Internet Service Provider (ISP) ist es überlassen, wie dieser seinen Kunden die IP-Adressen zuweist. Es gibt Provider, bei denen die Kunden täglich eine neue IP erhalten, jedoch gibt es

auch andere Provider, bei denen sich die IP nur wöchentlich oder monatlich ändert. Zu dem gibt es auch die Möglichkeit, eine statische bzw. permanente IP zu erhalten.

Das IPv4 Protokoll wurde bereits im Jahre 1980 im [RFC760] definiert. Das Protokoll war für die rasche Entwicklung des Internets nicht entwickelt worden. Daher wurde im Jahre 1994 das Network Address Translation (NAT) Verfahren im [RFC1631] veröffentlicht, das es ermöglicht hat, mehrere Geräte im Internet mit einem Anschluss bzw. einer IP-Adresse zu versorgen. Durch dieses Verfahren ist keine direkte Kommunikation zwischen den Endgeräten möglich, da die Datenpakete durch den Router mit einer Adressabbildung (private und öffentliche Adresse) an das entsprechende Endgerät durchgereicht werden. Ein weiterer Effekt dieses Verfahrens ist auch, dass keine direkte Identifikation der einzelnen Geräte hinter einem Anschluss möglich ist, da im Internet lediglich die Adresse des Routers öffentlich ist.

3.2.2 Internet Protocol Version 6 (IPv6)

IPv6 ist der Nachfolger von IPv4 und es wurde ein erster Entwurf im Dezember 1995 im [RFC1883] veröffentlicht. Es wurden mit dem Protokoll die Fehler von IPv4 weitestgehend korrigiert. Der wichtigste Aspekt war die Adressknappheit von IPv4, die im September 2012 von RIPE NCC [RIPE12] verkündet wurde, da der letzte /8 Adress-Block ($\hat{=}$ 16.777.214 nutzbare Host-Adressen) angebrochen wurde. Der aktuelle Stand der noch verfügbaren IPv4 Adressen ist in Abbildung 3.3 ersichtlich.

Diese Tatsache hat dazu geführt, dass die Anbieter den Kunden zeitnah IPv6 zur Verfügung stellen. Es gibt auch alternativ Lösungen für Kunden, denen die Anbieter keine IPv6 Kommunikation zur Verfügung gestellt haben. Diese konnten beispielweise IPv6 Tunnelbroker oder Gateways nutzen, um eine IPv6 Adresse besuchen zu können.

IPv6 bietet jedoch im Vergleich zu IPv4 noch bessere Möglichkeiten zur Identifizierung der einzelnen Geräte und somit auch der Nutzer. Es stehen genügend IP-Adressen zur Verfügung, damit jedes Gerät eine eindeutige Adresse im Internet erhalten kann, sodass das NAT Verfahren nicht mehr benötigt wird. Wechselt ein mobiles Gerät - beispielweise ein Handy, Notebook oder Tablet - das Netzwerk ist es je nach Einstellung des Gerätes mittels Stateless Address Autoconfiguration (SLAAC) über verschiedene Netzwerke hinweg zu identifizieren.

SLAAC kann zur Identifizierung verwendet werden, wenn die automatische Konfiguration der IPv6-Adresse gewünscht ist und diese nicht zentral vergeben und gespeichert wird. Da-

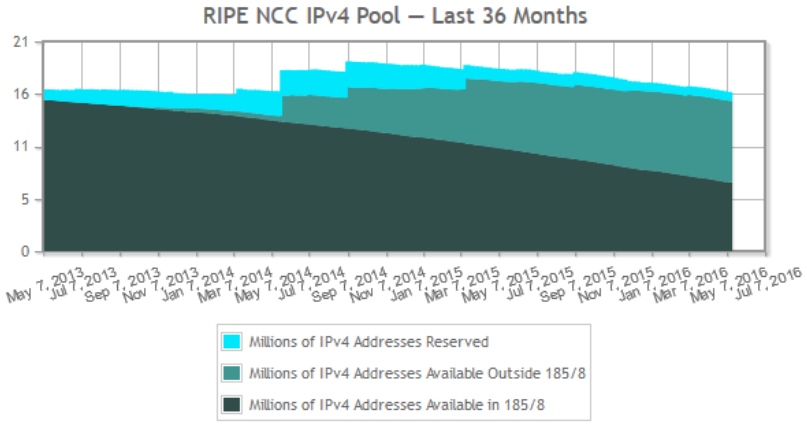


Abbildung 3.3: RIPE NCC[1]: Ausschöpfung des IPv4 Adresspools

durch wird sichergestellt, dass ein Gerät auf jeden Fall eine IP-Adresse erhält. Wie das SLAAC Verfahren funktioniert, lässt sich anhand eines Beispiels gut erklären.

Beispiel IPv6 Adresse: `fe80::8638:38ff:fe60:5dcc`

Diese IPv6 Adresse besteht aus zwei 64 Bit Blöcken - dem Präfix (*link prefix*) und dem Suffix (*interface identifier*) (siehe Abbildung 3.4).

```
|        64 bits          |        64 bits          |
+-------------------------+-------------------------+
|          fe80::         |  8638:38ff:fe60:5dce    |
|      link prefix        |  interface identifier   |
+-------------------------+-------------------------+
```

Abbildung 3.4: IPv6-Paket: Präfix und Suffix

Das Präfix `fe80::` (ungekürzt: `fe80:0000:0000:0000:`) entspricht dem Netzwerk und ist in diesem Beispiel eine link-lokale IPv6 Adresse. Das Suffix `8638:38ff:fe60:5dcc` entspricht dem EUI-64 Format [RFC4862] und enthält die zugewiesene Unternehmens ID und Hersteller Erweiterungs-Kennung.

Das "`c`" in diesem Beispiel ist die Kennzeichnung für die Hersteller ID (siehe Abbildung 3.5) und enthält `8638:38`, dies ist die Hersteller ID für Samsung. Die Kennzeichnung von "`g`" entspricht einem Einzel-/Gruppen Bit. Darauf folgen die Bits für `ff:fe`, die statisch festgelegt

[1]Quelle: `https://www.ripe.net/publications/ipv6-info-centre/about-ipv6/ipv4-exhaustion/ipv4-available-pool-graph` (Abruf: 13.05.2016)

```
|0               1|1               3|3               4|4               6|
|0               5|6               1|2               7|8               3|
+-----------------+-----------------+-----------------+-----------------+
|      8638       |      38ff       |      fe60       |      5dce       |
|0010000110111110|0011100011111111|1111111001100000|0101110111001110|
|cccccc1gcccccccc|cccccccc11111111|11111110mmmmmmmm|mmmmmmmmmmmmmmmm|
+-----------------+-----------------+-----------------+-----------------+
```

Abbildung 3.5: IPv6-Pakets: Suffix - Hexadezimal und Binär

sind. Zum Schluss folgt die Kennzeichnung von "m" - im genannten Beispiel `60:5dce`, diese Bits entsprechen der Hersteller Erweiterungs-Kennung. Die Hersteller ID und die Hersteller Erweiterungs-Kennung ergeben die MAC-Adresse des Netzwerkanschlusses. Wechselt eines dieser Geräte, das SLAAC aktiviert hat, das Netzwerk, so ändert sich lediglich das Präfix des Netzwerkes und es ist leicht, dieses Gerät wieder zu identifizieren. Außerdem ist es mit der MAC-Adresse möglich, den Hersteller des Gerätes herauszufinden, sollte sie nicht verändert worden sein.

3.2.3 Domain Name System (DNS)

Jedes Gerät, das an ein Netzwerk angeschlossen wird, erhält vom Router, sofern der Router so konfiguriert ist, eine IP-Adresse und verweist auf einen Nameserver (NS). Dieser Nameserver wird häufig vom ISP bereitgestellt und übermittelt dessen Adresse. Es ist auch möglich, solange die Einstellungen nicht deaktiviert oder gesperrt sind, eigene oder fremde Nameserver beim Router oder direkt am Endgerät zu hinterlegen.

Der Nameserver wird zur Namensauflösung im Netzwerk und im Internet verwendet. Möchte der Nutzer oder das Gerät beispielweise ein Datenpaket bzw. eine Anfrage an einen Webserver senden, so wird überprüft, ob das System den Hostnamen des Webservers auflösen kann. Dazu wird als erstes der DNS-Cache vom Betriebssystem überprüft, ob ein entsprechenden Eintrag vorhanden ist. Sollte kein entsprechender Eintrag für den Hostnamen vorhanden sein, wird eine DNS-Anfrage (siehe Tabelle 3.3a) an den Nameserver gesendet.

Die Antwort, die das Betriebssystem auf die DNS-Anfrage vom Nameserver erhält, enthält den Typ der Anfrage und die dazu gehörigen Daten. Die Daten (siehe Tabelle 3.3b) enthalten den Hostname (*name*), die IP-Adresse (*address*) und die Lebenszeit (*ttl*) bzw. Gültigkeitsdauer der Daten in Sekunden (für den DNS-Cache).

Typ	Daten
A	name: haw-hamburg.de

(a) DNS-Anfrage

Typ	Daten
A	name: haw-hamburg.de address: 134.28.219.2 ttl: 600

(b) DNS-Antwort

Tabelle 3.3: DNS-Informationen von haw-hamburg.de (Abrufdatum: 20.05.2016)

Der Auszug (siehe Abbildung 3.6) aus einer dnsmasq Server Protokollierung, zeigt eine Anfrage (Zeile 1) an den Nameserver und dessen Antwort (Zeile 2):

```
1 May 20 11:25:37 dnsmasq[467]: query[A] www.google.com from 10.0.0.25
2 May 20 11:25:37 dnsmasq[467]: config www.google.com is 172.217.19.36
```

Abbildung 3.6: DNS-Anfrage (dnsmasq)

Anhand der DNS-Anfragen oder einer Protokollierung ist es für die Betreiber von Nameservern möglich, ein Profil der Nutzer anzulegen. Durch das Profil ist es beispielweise möglich, das Surfverhalten auszuspähen, d.h. der Betreiber kann sehen, wann welcher Nutzer nach welchem Hostname gefragt hat. Sollte das Betriebssystem die Einträge nicht oder nur für einen kurzen Zeitraum (abhängig von deren Lebenszeit) zwischenspeichern, desto genauer wird das Bild des Nutzers.

Wissenschaftler des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit und der Universität Hamburg haben in einer wissenschaftlichen Arbeit [HBF13] demonstriert, dass es möglich ist, Nutzer mit verhaltensbasiertem Tracking zu identifizieren. Dies haben sie mithilfe von DNS gezeigt. Sie haben dazu einen Datensatz mit DNS-Anfragen von mehr als 3600 Nutzern über zwei Monate genutzt. An diesem Datensatz wurden drei verschiedene Methoden getestet und mit der besten Methode ist es ihnen gelungen, bis zu 85,4 Prozent der Daten mit dem Nutzer zu verknüpfen.

3.2.4 Hypertext Transfer Protocol (HTTP)

HTTP wird dazu genutzt, um Webdienste zur Verfügung zu stellen. Besucht ein Nutzer nun eine Webseite mit einem Browser, so sendet dieser eine HTTP-Anfrage an den Webserver. Der Webserver bearbeitet diese Anfrage und sendet seine HTTP-Antwort zurück.

Eine HTTP-Anfrage samt Steuerinformationen einer Standardinstallation von Mozilla Firefox (Version 46.0.1) mit aktivierter DNT Funktion zeigt Abbildung 3.7:

```
1  GET / HTTP/1.1
2  Host: haw-hamburg.de
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko
       /20100101 Firefox/46.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;
       q=0.8
5  Accept-Language: de,en-US;q=0.7,en;q=0.3
6  Accept-Encoding: gzip, deflate
7  DNT: 1
8  Connection: keep-alive
```

Abbildung 3.7: HTTP-Anfrage (Mozilla Firefox)

Zum Vergleich: Eine einfache HTTP-Anfrage von cURL, einem Kommandozeilen-Programm zum Übertragen von Dateien:

```
1 GET / HTTP/1.1
2 User-Agent: curl/7.38.0
3 Host: haw-hamburg.de
4 Accept: */*
```

Abbildung 3.8: HTTP-Anfrage (cURL)

Bei diesem einfachen Vergleich zwischen Abbildung 3.7 und 3.8 wird bereits deutlich, dass die Anwendungen unterschiedlich viele Informationen über den Nutzer, dessen Betriebssystem und Anwendung preisgeben. HTTP-Anfragen von Mozilla Firefox enthalten ein detaillierteres Muster (Abbildung 3.7, Zeile 3 - 6) als die von cURL (Abbildung 3.7, Zeile 2). Mithilfe dieser Informationen kann beispielsweise der Betreiber des Webservers detaillierte Profile der Nutzer anlegen.

3.2.5 Hypertext Transfer Protocol Secure (HTTPS)

Bei HTTPS erfolgt die Kommunikation mit HTTP in einer Ende-zu-Ende-verschlüsselten Sitzung. Die Sitzung wird mittels Secure Socket Layer (SSL) oder besser dessen Nachfolger Transport Layer Security (TLS) geschützt [RFC2818], denn SSL gilt inzwischen als veraltet und unsicher [MDK14].

Die Verschlüsselung stellt sicher, dass der Datenverkehr nur vom Client und Server entschlüsselt werden kann. Also ist es weiterhin für den Betreiber der Server möglich, die bei HTTPS anfallenden Daten zu erheben. Aber für Dritte, wie beispielsweise dem ISP, ist es nicht mehr möglich, die Kommunikation in Klartext mitzulesen.

Jedoch ist es Forschern von Universitäten [Mue+16] gelungen, anhand der Nutzdaten von HTTPS das Betriebssystem, den Browser und die aufgerufene HTTPS Anwendung des Nutzers zu identifizieren. Dazu haben sie einen Datensatz mit mehr als 20.000 markierten Sitzungen verwendet und hatten bei der Identifizierung eine Genauigkeit von bis zu 96,06 Prozent.

3.3 Kommunikation

3.3.1 Webserver

Betreiber von Webservern haben meisten die Protokollierung aktiviert, um beispielweise Störfälle oder Angriffe feststellen und ihnen vorbeugen zu können. Dazu werden ankommende Pakete und Logs analysiert.

Eine Zeile aus einer Apache Webserver Protokollierung sieht wie folgt aus:

```
31.18.132.172 - - [20/May/2016:14:48:50 +0200] "GET / HTTP/1.1" 200
   20 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko
   /20100101 Firefox/46.0"
```

Abbildung 3.9: Apache Webserver Protokollierung

In der Protokollierung (siehe Abbildung 3.9) werden die meisten der Informationen, die der Betreiber durch die HTTP-Anfragen von den Nutzern erhalten kann, bereits bei Standardeinstellungen gespeichert. Mit diesen Daten können diverse Statistiken erstellt werden oder es kann das Nutzerverhalten analysiert und ausgewertet werden.

Zur Auswertung der Logs können beispielweise kostenfreie Analyse-Werkzeuge, wie AWStats, Analog oder Webalizer verwendet werden. Es besteht auch die Möglichkeit, sich ein Analyse-Werkzeug zu kaufen oder ein eigenes zu programmieren. Aber die kostenfreien Werkzeuge bieten auch eine sehr umfangreiche Auswertung der Logs mithilfe von verschiedenen Darstellungen (siehe Abbildung 3.10) an.

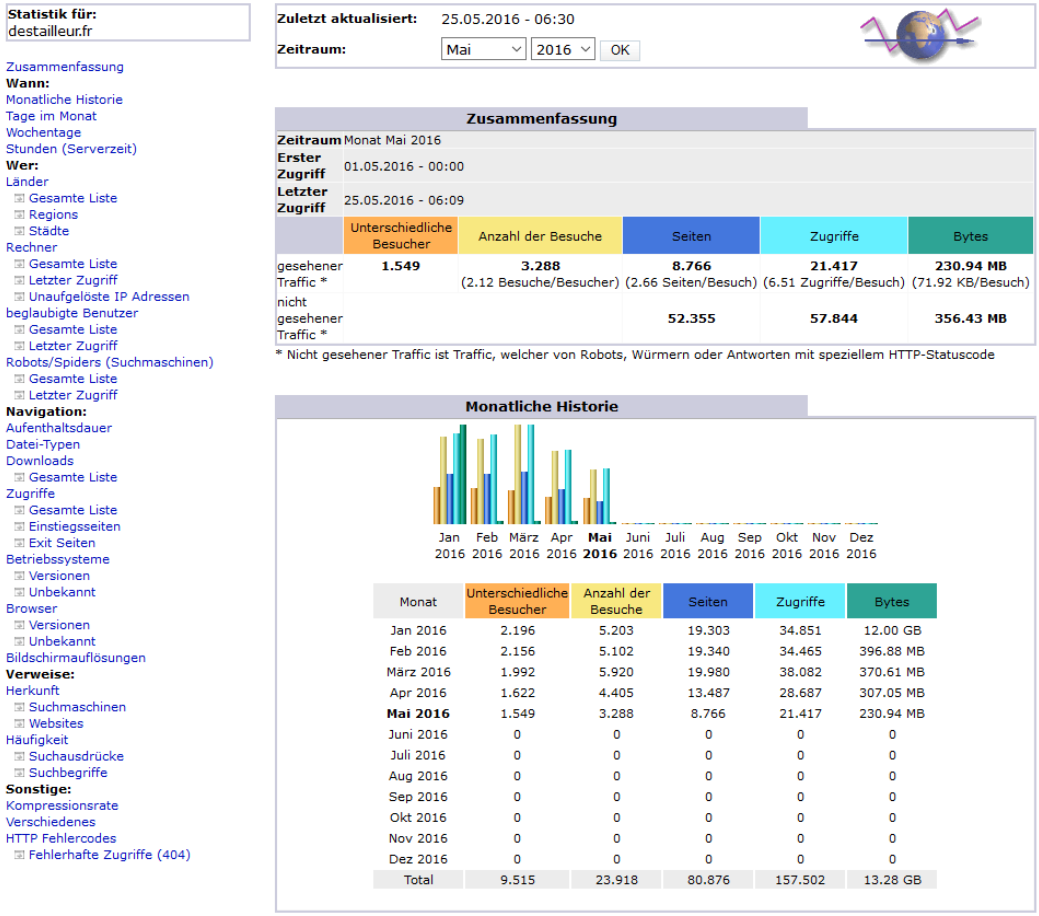


Abbildung 3.10: AWStats[1]: Auswertung der HTTP Logs

[1]Quelle: `http://www.nltechno.com/awstats/awstats.pl?config=destailleur.fr` (Abruf: 25.05.2016)

Die Informationen, die man durch HTTP-Anfragen erhält, reichen vielen Webseiten-Betreibern noch nicht aus, da sie noch detailliertere Auswertungen und Analysen über die Besucher ihrer Webseite haben möchten. Solche Betreiber binden dann auf ihren Webseiten weitere Analyse-Werkzeuge wie beispielsweise Google Analytics oder Piwik (siehe Abbildung 3.11) ein.

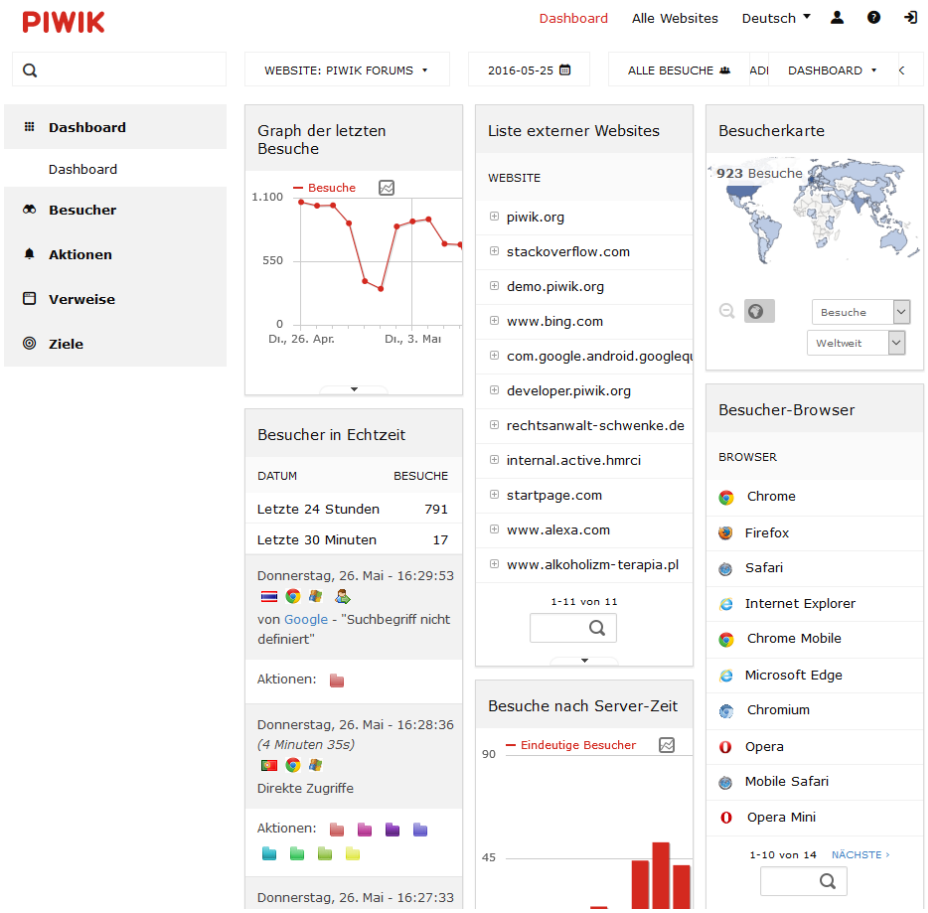


Abbildung 3.11: Piwik[1]: Auswertung der Webseiten Besucher

Diese Werkzeuge werden per JavaScript in die Webseite eingebunden und im Browser des Webseiten Besuchers ausgeführt. Dadurch können weitere Daten der offenen Browsersitzung erhoben werden wie beispielsweise das Bewegungs- / Klickverhalten der Maus und Informationen der genutzten Plugins.

[1]Quelle: `https://demo.piwik.org/` (Abruf: 26.05.2016)

3.3.2 E-Mail

Es existieren verschiedene Technologien, die es ermöglichen, zusätzliche Informationen über einen Nutzer zu erheben. Sie unterscheiden sich in der Anwendung, wie die Daten erhoben werden, und in dem Umfang, welche Daten erhoben werden können.

Internet Message Format (IMF)

Im Internet Message Format (IMF) Standard wird die Struktur einer E-Mail definiert. Der Standard [RFC5322] beschreibt unter anderem den Aufbau der Steuerinformationen einer E-Mail. Diese können zusätzliche Informationen beinhalten, die nicht zwingend für den Versand einer E-Mail benötigt werden, und somit Informationen über den Nutzer preisgeben könnten.

Ein Auszug des Quelltextes einer E-Mail, die mit Thunderbird (Version 45.1.0) versendet worden ist:

```
1 To: kai.henken@haw-hamburg.de
2 From: Kai Henken <kai.henken@haw-hamburg.de>
3 Message-ID: <1f4131b1-2786-c440-d669-c987f1d4d957@haw-hamburg.de>
4 Date: Sun, 29 May 2016 18:12:27 +0200
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko
     /20100101 Thunderbird/45.1.0
6 MIME-Version: 1.0
7 Content-Type: text/plain; charset=utf-8; format=flowed
8 Content-Transfer-Encoding: 7bit
```

Abbildung 3.12: Quelltext Ausschnitt einer E-Mail (Thunderbird)

Zum Vergleich: Ein Auszug des Quelltextes (siehe Abbbildung 3.13) einer E-Mail, die mit dem Webmailer der HAW versendet worden ist.

Bei dem Vergleich zwischen den Abbildungen 3.12 und 3.13 zeigt sich ein ähnliches Verhalten wie bei den zuvor betrachteten HTTP-Anfragen. Mozilla Thunderbird bindet beispielsweise standardmäßig den “User-Agent” (Abbildung 3.12, Zeile 5) ein, der einige Informationen des absendenden Systems preisgibt. Der Webmailer hingegen gibt lediglich zusätzlich preis, dass die Sprache des Inhalts vom Nutzer deutsch (Abbildung 3.13, Zeile 7) ist. Des Weiteren enthält der Quelltext des Webmailers einige Steuerinformationen, die nicht verwendet worden sind (Abbildung 3.13, Zeile 3 “Subject:” und 8 - 10 “X-MS-*”).

```
From: "Henken, Kai" <Kai.Henken@haw-hamburg.de>
To: "Henken, Kai" <Kai.Henken@haw-hamburg.de>
Subject:
Thread-Index: AdG5xfCgfbIsm6RRRlepafIYjKFbfQ==
Date: Sun, 29 May 2016 18:19:56 +0200
Message-ID: <7C4F94DD6B4E9B459E3B434C8576E7E018F20629@MB01.
    mailcluster.haw-hamburg.de>
Content-Language: de-DE
X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator:
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
MIME-Version: 1.0
```

Abbildung 3.13: Quelltext Ausschnitt einer E-Mail (HAW Webmailer)

Message Disposition Notification (MDN)

Der Standard [RFC3798] von Message Disposition Notification (MDN) definiert zusätzliche Felder in den Steuerinformationen von Internet Message Format (siehe Abbildung 3.14).

```
Disposition-Notification-To: Kai Henken <kai.henken@haw-hamburg.de>
```

Abbildung 3.14: MDN Steuerinformation in einer E-Mail

Dies ermöglicht, wie der Name "Disposition-Notification" [RFC3798] bereits verrät, eine Benachrichtigung über die Verteilung einer E-Mail. Mögliche Benachrichtigungen sind beispielsweise das Öffnen beziehungsweise Anzeigen des Inhalts, Drucken oder Löschen der E-Mail. Je nach Einstellung des Mailservers oder -Clients kann diese Benachrichtigung unterbunden werden, ansonsten wird diese automatisch versendet.

3.3.3 Audio

Es existieren Tracking-Technologien, die mithilfe von nicht hörbaren Tönen und Frequenzen Informationen zwischen Geräten austauschen können. Diese Töne und Frequenzen werden auch als "Audio Beacon" (zu Deutsch *Audio-Leuchtfeuer*) bezeichnet.

Unternehmen können dieses Verfahren [Cha15] nutzen, um beispielsweise Kunden beim Betreten des Geschäfts die passende Werbung auf seinem Gerät anzeigen zu lassen. Dazu

benötigt der Kunde lediglich ein Gerät, das die Töne und Frequenzen empfängt und eine App, die im Hintergrund laufen kann und mit dem dazu passenden Werbeunternehmen kooperiert (siehe Abbildung 3.15) ein.

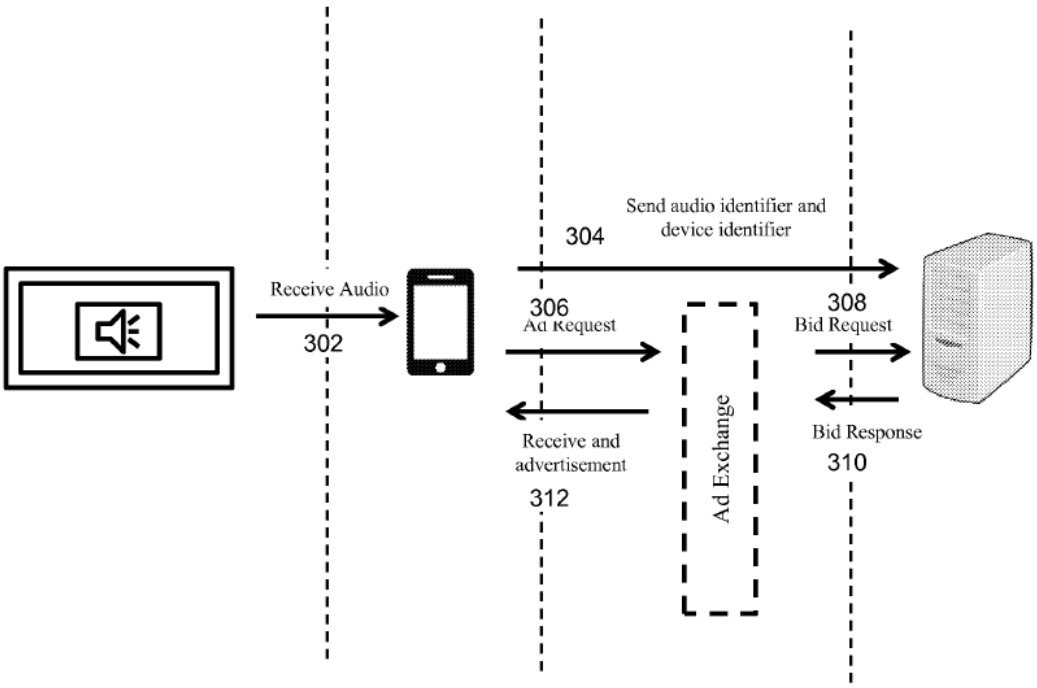


Abbildung 3.15: Patent US2015/0215668 A1 [Cha15]

Ein Werbeunternehmen, das diese Technologie nutzt, ist beispielsweise SilverPush. SilverPush stellt für Entwickler eine Bibliothek zur Verfügung, wodurch SilverPush in eine App eingebunden werden kann. Außerdem hat SilverPush eine Demo App und zwei Beispiel Sounds zur Verfügung gestellt. Der Sicherheitsberater Kevin Finisterre [Fin15] hat die App, den Code und die Beispiele von SilverPush analysiert und hat die von SilverPush genutzten Frequenzen feststellen können. Der Buchstabe 'A' entspricht der Frequenz von 18 kHz, der nächste Buchstabe ist jeweils um 75 Hertz höher, daher entspricht 19,75 kHz dem Buchstaben 'Z'.

Das Problematische für die Nutzer bei dieser Technologie ist, dass aktuell keine Opt-Out Möglichkeit existiert und kaum bekannt ist, wo die Technologie bereits eingebunden worden ist. Außerdem ermöglicht die Technologie ein geräteübergreifendes Tracking [Cal+15], wodurch die einzelnen Tracking Profile der Geräte synchronisiert werden könnten und das nutzende Unternehmen sehr umfassende Informationen über einen Nutzer erhalten würde.

Dabei muss lediglich das empfangende Gerät mit dem Internet verbunden sein und das ausstrahlende Gerät des Audio Beacons könnte beispielsweise auch ein Fernseher, Radio oder Lautsprecher sein.

3.4 Provider

Provider haben viele verschiedene Möglichkeiten, einen Nutzer zu tracken, weil sie die Datenpakete vom Nutzer entgegennehmen und zum Ziel weiterleiten. Dadurch ist es möglich, unverschlüsselte Datenpakete auszuwerten und zu analysieren wie bei zuvor beschriebenen Tracking-Technologien.

Internet

Die Internet Service Provider, wie beispielsweise Telekom, Vodafone, Kabel Deutschland und viele mehr, stellen ihren Kunden gegen ein Entgelt einen Internetzugang zur Verfügung. In 2014 hat der amerikanische ISP Verizon [HA14] gezeigt, dass ihm dieses Entgelt wohl nicht genügt. Verizon hat bei dem unverschüsselten Datenverkehr seiner Kunden eine zusätzliche HTTP-Steuerinformation mit der Bezeichnung Unique Identifier Header (UIDH) (siehe Abbildung 3.16) zur Nutzeridentifikation hinzugefügt. Es basiert auf der Tracking-Technologie in Kapitel 3.2.4.

```
GET / HTTP/1.1
User-Agent: curl/7.38.0
Host: haw-hamburg.de
Accept: */*
X-UIDH: 12345
```

Abbildung 3.16: HTTP-Steuerinformationen: UIDH [LP14]

Ein weiterer amerikanischer Anbieter (AT&T) [Hil14] hat eine ähnliche Technologie getestet, um seine Nutzer eindeutig identifizieren zu können. Die HTTP-Steuerinformationen (siehe Abbildung 3.16) unterscheiden sich in ihrer Bezeichnung. Verizon verwendet *X-UIDH* und AT&T verwendet *x-up-subno* [abu14]. Ergänzend dazu hat AT&T diesen sogenannten "Supercookie" nur an ihre Mobilfunk-Kunden verteilt, und es existierte eine Opt-Out Möglichkeit.

4 Tracking-Schutzmechanismen

Es existieren bereits verschiedene Webseiten, die Sammlungen von Werkzeugen für die verschiedenen Themen und Bereiche zusammengestellt haben. Diese Webseiten führen Werkzeuge auf, die eine Identifizierung des Users erschweren. Es werden teilweise die proprietären Produkte genannt und direkt dazu eine passende freie - meist Open Source - Alternative.

cryptoparty.in
: Cryptoparty ist eine dezentrale, globale Initiative mit dem Ziel, die grundlegendsten Kryptographie-Softwares und ihre Konzepte des Einsatzes der breiten Öffentlichkeit vorzustellen.

prism-break.org
: PRISM-Break ist ein Open-Source-Projekt zur Reduzierung der möglichen Auswirkungen der staatlichen Internet-Überwachung. Es werden Open Source Empfehlungen für beliebte proprietäre Software und Dienstleistungen genannt.

privacytools.io
: Private und staatlich geförderte Organisationen und Unternehmen können Ihre Online-Aktivitäten überwachen und aufzeichnen. privacytools.io bietet Wissen und die Werkzeuge, die Privatsphäre gegen die globale Massenüberwachung zu schützen.

Es wurde eine Testseite (siehe Anhang A.1) verwendet, um die verschiedenen Schutzmechanismen untersuchen und bewerten zu können. Dazu wurden mit dieser Testseite stichprobenartig Messungen durchgeführt.

4.1 Werkzeuge zur Verschleierung

Die hier vorgestellten Werkzeuge dienen zur Verschleierung der Herkunft von Datenpaketen. Teilweise unterstützen die Werkzeuge zusätzliche Filterfunktionen, wodurch beispielsweise Tracking vermindert werden kann.

4.1.1 Übersicht

Die folgende Tabelle fasst die Bewertung der einzelnen Schutzmechanismen zusammen. Die ersten drei Kriterien werden in der Motivation (siehe Kapitel 1.4) definiert. Unter Nutzung wird die Benutzbarkeit des Schutzmechanismus und der Webseite bewertet. Unter Einrichtung wird lediglich die Installation oder Konfiguration betrachtet. Die Übersicht befindet sich jeweils zu Beginn der Unterkapitel der Tracking-Schutzmechanismen (Kapitel 4.2.1 und 4.3.1).

Werkzeuge	Anonymität & Privatsphäre	Sicherheit & Schutz	Performanz	Nutzung	Einrichtung
VPN					
Proxy					
Tor					

(a)

Symbol	Bedeutung
	neutral
	gut / einfach
	schlecht / schwer

(b) Legende

Tabelle 4.1: Werkzeug: Übersicht

4.1.2 Virtual Private Network (VPN)

Mithilfe von VPN-Verbindungen ist es möglich, in einem durch Verschlüsselung gesicherten Tunnel den gesamten Datenverkehr über eine öffentlich zugängliche Infrastruktur, beispielsweise das Internet, umzuleiten. Dadurch werden die Endpunkt des Tunnels zum Ein- bzw. Ausgang des Datenverkehrs.

Es existieren drei VPN-Typen, die detaillierter im wissenschaftlichen Artikel “VPN-Virtual Private Networks” von W. Böhmer [Bö02] beschrieben werden. Unternehmen und Organisationen nutzen häufig die VPN-Typen End-to-Site (“Remote-Access-VPN”) und Site-to-Site (“Intranet-VPN”). Andere Nutzer verwenden meist nur den VPN-Typ End-to-End (“Extranet-VPN”).

End-to-Site

Das End-to-Site- oder auch Remote-Access-VPN wird beispielsweise von Unternehmen genutzt, damit Heimarbeitsplätze oder Mitarbeiter mit mobilen Endgeräten auf Ressourcen des Unternehmensnetzwerkes zugreifen können (siehe Abbildung 4.1).

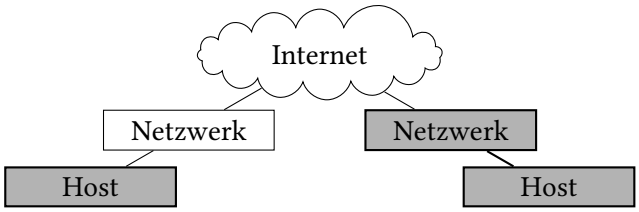


Abbildung 4.1: Werkzeug: VPN - End-to-Site[1]

Site-to-Site

Das Site-to-Site-, Network-to-Network- oder auch Branch-Office-VPN kann dazu genutzt werden, um mehrere Netzwerke über das Internet sicher miteinander zu verbinden (siehe Abbildung 4.2). Unternehmen nutzen dies, um beispielsweise Außenstellen oder Niederlassungen in einem virtuellen Netzwerk zusammenzufassen.

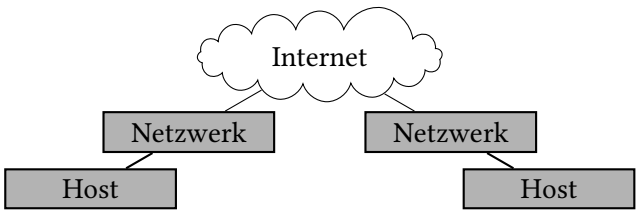


Abbildung 4.2: Werkzeug: VPN - Site-to-Site[1]

End-to-End

Das End-to-End-, Host-to-Host- oder auch Remote-Desktop-VPN beschreibt eine Verbindung zwischen lediglich zwei Hosts (siehe Abbildung 4.3). Dieser Verbindungs-Typ wird beispielsweise von VPN-Anbietern genutzt.

[1]Die grau hinterlegten Knoten kommunizieren miteinander.

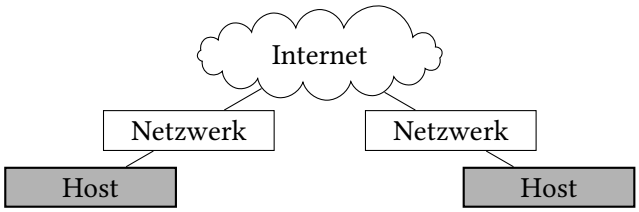


Abbildung 4.3: Werkzeug: VPN - End-to-End[1]

Es existieren verschiedene Protokolle, die bei einem VPN-Tunnel genutzt werden können. Diese unterscheiden sich in der Einrichtung, Sicherheit und Performanz.

IPsec

Das Internet Protocol Security (IPsec) ist definiert im [RFC4301] und erweitert das Internet Protocol mit Mechanismen zur Authentifizierung und Verschlüsselung. Es gilt als sicher und kann nur IP-Pakete tunneln. Es verwendet das Konzept der Vertrauensstellung, das grundlegend für IPsec ist. Die Vertrauensstellung reguliert die Kommunikation der Endpunkte. Die Endpunkte können einzelne Hosts oder aber auch Router sein, die zur Verbindung zweier Netze verwendet werden. Die Konfiguration von IPsec ist aufwändig, je komplexer die Vertrauensstellung ist desto höher ist der Konfigurationsaufwand. Um die Kommunikation zwischen zwei Stationen zu realisieren, müssen diese Stationen die folgende Informationen austauschen: Art der Übertragung, Verschlüsselungsalgorithmus, Schlüssel, Gültigkeitsdauer der Schlüssel.

Die Mechanismen zur Authentifizierung und Verschlüsselung - Authentication Header (AH) [RFC4302] und Encapsulating Security Payload (ESP) [RFC4303] - können unabhängig voneinander verwendet werden. Beim AH werden lediglich die Integrität und Echtheit der Daten sichergestellt. Durch den ESP werden die Daten verschlüsselt übertragen. Bei beiden Protokollen werden keine bestimmten Verfahren vorgeschrieben, daher ist es notwendig, dass die Endpunkte dieselben Verfahren verwenden. Außerdem ist darauf zu achten, dass die Datensicherheit abhängig vom Verschlüsselungsalgorithmus ist.

PPTP

Das Point-to-Point Tunneling Protocol (PPTP) ist definiert im [RFC2637] und gilt als unsicher. Es wurde von mehreren Unternehmen entwickelt, unter anderem von Microsoft, weshalb es hauptsächlich in Microsoft-Betriebssystemen zum Einsatz kommt und die

[1] Die grau hinterlegten Knoten kommunizieren miteinander.

Authentisierung des Remote Access Servers für Microsoft Windows NT genutzt wurde. Die Schwachstelle des Protokolls ist die Authentifizierung [Sch12]. Dort wird das Authentifizierungsverfahren MSCHAPv2 eingesetzt und dieses verwendet den gebrochenen Verschlüsselungsalgorithmus DES (Data Encryption Standard).

L2TP

Das Layer Two Tunneling Protocol (L2TP) ist definiert im [RFC2661]. Es basiert auf PPTP und Layer Two Forwarding (L2F) und kann jedes beliebige Netzwerkprotokoll in einen PPP-Rahmen verpacken. L2TP unterstützt eine Authentifizierung durch einen Pre-shared Key (PSK) oder zertifikatsbasiert. Eine eigene Verschlüsselungskomponente besitzt das Protokoll nicht. Um eine Verschlüsselung zu verwenden, wird meistens IPsec eingesetzt.

L2TP over IPsec

"L2TP using IPsec" bzw. L2TP over IPsec ist definiert im [RFC3193]. Durch die Kombination der beiden Protokolle werden die Nachteile der Protokolle aufgehoben. Dadurch ist es möglich, jedes beliebige Netzwerkprotokoll mit einer höchstmöglichen Sicherheit zu übertragen.

VPN over SSL

Der OpenVPN [OpenVPN] Client nutzt beispielsweise VPN over SSL - wie aus dem Namen ersichtlich wird eine TLS/SSL Verbindung verwendet. Es ist vergleichsweise einfach einzurichten. Die Authentifizierung der Nutzer kann entweder mittels PSK oder zertifikatsbasiert erfolgen. Es existieren zwei verschiedene Netzwerkmodi, die verschiedene Vor- und Nachteile besitzen. Beim Bridging-Modus werden alle Datenpakete durch den Tunnel übertragen, da ein vollständiges Tunneln des Ethernet-Frames erfolgt. Beim Routing-Modus werden ausschließlich IP-Pakete durch den Tunnel übertragen.

DTLS

Das Datagram Transport Layer Security (DTLS) Protokoll ist definiert im [RFC6347]. [RFC6347] orientiert sich sehr stark TLS1.2 und versucht dieses möglichst genau abzubilden. Der Grundgedanke bei DTLS ist die Konstruktion "TLS over datagram". Das Problem bei UDP ist, dass Pakete verloren gehen können oder neugeordnet werden müssen. DTLS führt eine eigene Sequenznummer ein, damit dieses Problem behoben wird. DTLS wird beispielsweise vom Cisco AnyConnect Client verwendet.

QUIC

Das Quick UDP Internet Connection [QUIC] Protokoll ist aktuell noch ein Entwurf von Google. QUICs Funktionalität ist gleichwertig zu der Kombination aus TCP, TLS

und HTTP/2. Es verwendet das UDP-Protokoll, wodurch das Protokoll gegenüber der klassischen Variante ein Geschwindigkeits- und Bandbreiten-Vorteil hat.

Es ist abhängig vom Anwender, welche VPN-Schutzmechanismen ihm zur Verfügung stehen und welche er nutzen möchte. Es wäre beispielweise möglich, dass jemand das VPN des Arbeitgebers oder der Organisation auch für private Zwecke nutzen könnte. Sollte der Arbeitgeber den Datenverkehr analysieren und überwachen, dann könnte er jedoch auch einige Information über den Arbeitnehmer erhalten. Alternativ existieren noch die Möglichkeiten, öffentliche und kostenfreie VPN-Anbieter (beispielsweise vpnbook.com) zu nutzen. Die Webseite vpngate.net stellt eine umfangreiche Liste von kostenfreien VPN-Servern zur Verfügung. Außerdem ist auch noch die Möglichkeit vorhanden, sich ein Abonnement bei einem kommerziellen VPN-Anbieter zu beschaffen.

Einige dieser VPN-Anbieter bewerben ihre VPNs mit einer hohen Bandbreite sowie mit den Merkmalen, dass sie nur sehr wenige Daten, nur abrechnungsrelevante Daten oder überhaupt keine Daten speichern. Außerdem bieten kommerzielle VPN-Anbieter mittlerweile mit einem eigenen VPN-Client häufig den eigenen DNS-Server an und eine weitere Option, um Werbung zu blockieren.

Bewertungskriterien

Anonymität & Privatsphäre

Die Anonymität ist nur bedingt sichergestellt. Häufig wird der gesamte Datenverkehr über den VPN-Server übertragen. Der ISP sieht den verschlüsselten Datenverkehr zu den genutzten VPN-Servern. Es ist abhängig vom VPN-Anbieter, wie dieser die anfallenden Daten und Informationen des Nutzers verwendet, speichert, löscht oder ggf. anonymisiert.

Wenn der VPN-Anbieter die Verbindungsdaten protokolliert und der Nutzer ein Abonnement mit persönlichen Informationen besitzt - dies können Informationen zum Nutzer oder zur Bezahlung sein - ist es für den VPN-Anbieter möglich, den Nutzer zu identifizieren. Ansonsten ist eine Identifizierung durch den VPN-Anbieter nur über die IP-Adresse oder über eine Auswertung des Datenverkehrs möglich.

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne VPN	9.44	5.25	5.65	5.19	5.27	6.16
	Ø VPN	19.54	13.27	6.27	6.83	7.72	10.73
ohne Cache	ohne VPN	13.51	9.72	9.99	9.82	10.02	10.61
	Ø VPN	40.55	21.47	12.21	13.87	14.08	20.44

(a) Performanz[2]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne VPN	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit VPN	5.00	11.00	87.27	74.33	1.00	6.13	6.20

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne VPN	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit VPN	65.15	4.00	0.00	2.92	6.00	2.00	0.00	79.87

(c) Tracker

Tabelle 4.2: Werkzeug: VPN[1]

Dritte können beispielsweise über die HTTP-Logs folgende Informationen über den Nutzer erhalten:

Abruf		Wert
IP-Adresse	ohne VPN	31.18.132.134
	mit VPN	176.126.237.217
Host	ohne VPN	ip1f128486.dynamic.kabel-deutschland.de
	mit VPN	ws197180.vpn.haw-hamburg.de

Tabelle 4.3: Werkzeug: VPN[3] - Anonymität & Privatsphäre

Sicherheit & Schutz

Der Nutzer muss dem VPN-Anbieter vertrauen, so wie er seinem ISP vertraut, dass dieser verantwortungsvoll mit den vom Nutzer angegebenen Daten umgeht. Je nach VPN-Anbieter ist der Schutz sehr hoch, da die Verbindung häufig über VPN-Server erfolgt, die von vielen Nutzern gleichzeitig genutzt werden. Daher wird die Identifizierung eines Nutzers anhand der IP-Adresse erschwert.

[1] Details zu den Messungen befinden sich im Anhang A.2 und A.3.
[2] Werte entsprechen der Ladezeit in Sekunden.
[3] Weitere Details, wie die Informationen des Browsers, befinden sich im Anhang A.4.

Performanz

Die Performanz ist im Wesentlichen vom VPN-Server, dessen Bandbreite und Auslastung abhängig. Ein Performanz-Verlust wird der Nutzer haben, weil der Datenverkehr über weitere Verbindungspunkte geleitet wird.

Der durchschnittliche Performanz-Verlust wird ersichtlich in der Tabelle 4.2a und ist relativ gering, da die Ladezeit lediglich von 6.16 auf 10.73 Sekunden ($\approx$ 57 Prozent) ansteigt. Bei deaktiviertem Cache steigt jedoch die durchschnittliche Ladezeit von 10.61 auf 20.44 Sekunden ($\approx$ 93 Prozent).

Die Studie [NBV09] zeigt, dass die Performanz des VPNs nicht nur abhängig vom verwendeten Server, Protokoll und der Verschlüsselung sondern auch vom Betriebssystem ist - getestet wurden Windows Server 2003, Windows Vista und Linux Fedora Core 6. Bei dem Datendurchsatz ist mal Windows performanter als Linux und umgekehrt gewesen. Anders sieht das aber bei der Initiierung der Verbindung aus: in diesem Fall benötigte Linux zwischen 1.0 bis 1.7ms während alle Messungen bei Windows unter 0.6ms waren.

Nutzung

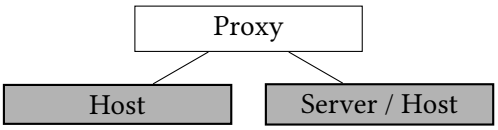
Die Nutzung eines VPNs ist je nach Typ mit einem geringen Aufwand verbunden. Die Verbindung des Typs Site-to-Site ist meistens dauerhaft aktiviert. Bei den Typen End-to-Site und End-to-End ist es meistens notwendig, dass der Nutzer sich mittels Benutzername und Passwort in der VPN-Anwendung authentifizieren muss.

Einrichtung

Die Einrichtung ist für den Nutzer nur mit einem geringen bis mittelmäßigen Aufwand verbunden, weil die VPN-Typen, die im Unternehmen genutzt werden, vom Unternehmen eingerichtet werden. Bei dem VPN-Typ End-to-End benötigt der Nutzer eine Anwendung, die bei kommerziellen Anbietern häufig bereits konfiguriert ist und bei kostenlosen Anbietern häufig mithilfe einer Anleitung in wenigen Schritten eingerichtet ist.

4.1.3 Proxy

Generell arbeitet ein Proxy als Vermittler. In Abbildung 4.4 ist die Kommunikation über einen Proxy beispielhaft abgebildet. Als Vermittler kann der Proxy einige zusätzliche Funktionen übernehmen wie beispielsweise das Filtern, Bearbeiten, Zwischenspeichern oder Anonymisieren von Anfragen. Das Verfahren zur Anonymisierung wird in dem Artikel “Anonymität und Authentizität im World Wide Web” [FM98] ausführlich behandelt.



Host	Proxy	Server / Host
sendet Anfrage	leitet Anfrage weiter	verarbeitet Anfrage
verarbeitet Antwort	leitet Antwort weiter	sendet Antwort

Abbildung 4.4: Werkzeug: Proxy - Kommunikation zweier Hosts[1]

Jedes Kommunikationsprotokoll besitzt einen eigenen Proxy-Server. Es existiert kein Proxy-Server, der alle Protokolle unterstützt. Es gibt jedoch die Möglichkeit, einen SOCKS-Proxy zu verwenden. Mithilfe des SOCKS-Protokolls, das in Version 5 im [RFC1928] definiert ist, ist es möglich, alle Datenpakete und Protokolle über einen Proxy-Server zu übertragen. Die Datenübertragung bei der Nutzung von Proxy-Servern ähnelt sehr stark der von VPN-Servern, jedoch wird der Datenverkehr bei Proxies nicht immer verschlüsselt. Diese Arbeit beschäftigt sich lediglich mit dem Prinzip von Proxies und zeigt das Verfahren nur exemplarisch.

Proxy-Server können in drei Schutzklassen [XROXY] der Privatsphäre unterteilt werden, die sich wie folgt definieren lassen:

Transparent
: Die Datenpakete werden unverändert weiter vermittelt. Es wird außerdem noch mitgeteilt, dass der Absender einen Proxy verwendet. Dies erfolgt häufig über eine HTTP-Kopfzeile.

Distorting
: Die Datenpakete werden verändert, wodurch verhindert werden soll, dass der Empfänger den Absender identifizieren kann. Es existiert eine Mitteilung, dass ein Proxy verwendet wird.

Anonymous
: Die Datenpakete werden wie bei der Schutzklasse Distorting verändert. Jedoch entfällt die Mitteilung über die Verwendung eines Proxy.

Bewertungskriterien

Die Bewertung unterscheidet sich kaum von den Bewertungen beim Tracking-Schutzmechanismus VPN in Kapitel 4.1.2. Im Wesentlichen unterscheidet sich diese in der Hinsicht, dass der Nutzer seinen Datenverkehr auf verschiedene Anbieter verteilen kann. Es wäre beispielweise

[1] Die grau hinterlegten Knoten kommunizieren miteinander.

möglich, für jede Anwendung einen eigenen Anbieter zu nutzen, sofern die Anwendungen dies unterstützten.

Anonymität & Privatsphäre

Die Anonymität und Privatsphäre sind teilweise sichergestellt - abhängig von der Proxy-Klasse (siehe Tabelle 4.4). Diese geben unterschiedlich viele Informationen über den Datenverkehr und den Nutzer preis. Der erzielte Grad der Anonymität hängt ab von dem genutzten Protokoll und den Proxy-Servern sowie der Anzahl der Anbieter. Weiterhin ist es auch hier dem Anbieter überlassen, wie dieser den Datenverkehr verarbeitet ggf. speichert.

Sicherheit & Schutz

Gleichbleibend wie in Kapitel 4.1.2. Bei Nutzung vieler und verschiedener Proxy-Anbieter erhöht sich jedoch das Risiko, dass die Daten sich weiter verbreiten.

Je nach Server und Einstellung bzw. der Klassifikation ist es möglich, dass der Empfänger mehr Informationen vom Nutzer des Proxy-Servers sieht. Da die Server häufig von mehreren Nutzern genutzt werden, wird die Identifizierung über die IP-Adresse erschwert. Des Weiteren wäre es möglich, mit verschiedenen Anwendungen unterschiedliche Proxies zu verwenden, wodurch der Anbieter lediglich den Datenverkehr einer Anwendung analysieren könnte und nicht den kompletten Datenverkehr.

Performanz

Die Performanz ist stark abhängig von der Einrichtung und Nutzung der Proxies. Ähnlich wie in Kapitel 4.1.2 wird der Nutzer bei der jeweiligen Anwendung und den dafür genutzten Anbieter einen geringen bis großen Performanz-Verlust haben können. Es ist aber möglich, die anfallende Last der verschiedenen Anwendungen auf verschiedene Proxy-Server zu verteilen, um die Performanz zu verbessern. Außerdem kann man einen Performanz-Vorteil erzielen, wenn der Proxy von mehreren Nutzern verwendet wird und diese die gleichen Webseiten besuchen, wodurch der Proxy beispielsweise die Webseiten-Antworten zwischenspeichern kann und nicht erneut die Webseiten-Anfrage versenden muss.

Nutzung

Der Aufwand für die Nutzung von Proxies ist relativ gering, da sie häufig keine zusätzlichen Authentifizierung-Mechanismen besitzen.

Einrichtung

Die Anwendung muss die Verwendung eines Proxies unterstützen und der Proxy muss bei jeder Anwendung eingestellt werden. Alternativ bieten manche Anwendungen die

HTTP-Kopfzeile	Wert
Hostname	promail.vpshosting.com.hk
Proxy	180.235.133.27
Proxy Type	1.1 VPS12 (squid/3.1.23)
HTTP_VIA	1.1 VPS12 (squid/3.1.23)
HTTP_X_FORWARDED_FOR	31.18.132.134

(a) Transparent-Proxy

HTTP-Kopfzeile	Wert
Hostname	fc.57.32a9.ip4.static.sl-reverse.com
Proxy Type	1.1 www.dev1.beautifulyou.boots.co.uk
HTTP_VIA	1.1 www.dev1.beautifulyou.boots.co.uk

(b) Distorting-Proxy

HTTP-Kopfzeile	Wert
Hostname	ip-89-250-207-195.rev.snt.net.pl

(c) Anonymous-Proxy

Tabelle 4.4: Werkzeug: Proxy - Anonymität & Privatsphäre[1]

Einstellung an, dass sie die Proxy-Einstellung des Systems verwenden. Es existieren auch sogenannte Webproxies. Webproxies besitzen eine Weboberfläche, über die der Nutzer andere Webseiten besuchen kann. Die Webseite proxy.org bietet beispielsweise eine Sammlung von Webproxies an.

4.1.4 Tor

Das Tor Projekt [Tor] dient zur Anonymisierung der Nutzer. Es wird beispielsweise von Personen verwendet, um Webseiten besuchen zu können, die durch den ISP oder eine Regierung gesperrt sind. Es ist möglich, den Nutzern, Webseiten und andere Dienste zur Verfügung zu stellen ohne deren Standort preiszugeben. Zum Beispiel können Journalisten es nutzen, um mit Whistleblowern und Regimekritikern zu kommunizieren. Außerdem können sie es zur Kommunikation mit ihrer Organisation im Ausland verwenden.

Die Verwendung von Tor schützt vor der üblichen Internet-Überwachung bzw. der Analyse des Datenverkehrs. Bei der Analyse wird sich zunutze gemacht, dass die Quelle und das Ziel des Datenverkehrs lesbar sind. Dadurch können Rückschlüsse auf das Verhalten und die Interessen des Nutzers erfolgen. Der Datenverkehr wird unterteilt in Steuerinformationen und Nutzlast bzw. dem Dateninhalt. Sobald der Dateninhalt verschlüsselt ist, kann dieser nicht

[1] Weitere Details zu den HTTP-Anfragen und -Antworten befinden sich im Anhang A.5.

mehr zur Analyse verwendet werden. Es ist jedoch noch möglich, dass die Steuerinformationen ausgewertet werden und davor möchte das Tor Projekt die Nutzer schützen.

Das Tor Netzwerk unterstützt TCP-Datenströme sowie jede Anwendung, die SOCKS unterstützt.

Wie funktioniert Tor?

Schritt 1

Der Nutzer Alice erhält von einem Verzeichnis-Server eine Liste von Tor Knoten (siehe Abbildung 4.5).

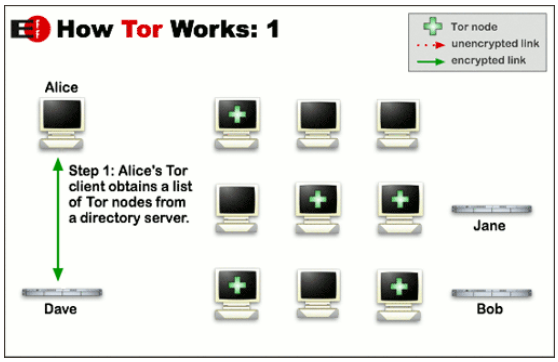


Abbildung 4.5: Werkzeug: Tor[1] - How Tor Works: 1

Schritt 2

Bei der Kommunikation zwischen Alice und Bob (siehe Abbildung 4.6) generiert der Tor Client einen zufälligen Pfad durch das Tor Netzwerk. Die Kommunikation innerhalb des Tor Netzwerkes erfolgt verschlüsselt. Die Tor Knoten kennen niemals den gesamten Pfad des Paketes, weil der Client für jeden Knoten des Pfades einen eigenen Verschlüsselungs-Schlüssel aushandelt und mindestens 3 Tor Knoten verwendet werden. Die Tor Knoten wissen bei der Zustellung des Paketes lediglich woher es stammt und wohin es zugestellt werden soll. Für eine Verbindung wird aus Performanzgründen derselbe Pfad bis zu circa 10 Minuten lang verwendet.

Schritt 3

Bei der Kommunikation zwischen Alice und Jane (siehe Abbildung 4.7) generiert der Tor Client einen weiteren zufälligen Pfad durch das Tor Netzwerk.

[1] Quelle: `https://www.torproject.org/about/overview.html.en` (Abruf: 18.09.2016)

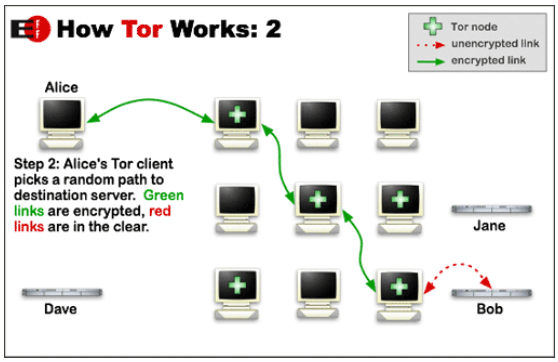


Abbildung 4.6: Werkzeug: Tor[1] - How Tor Works: 2

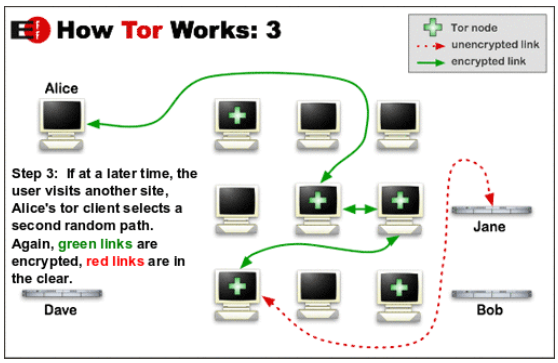


Abbildung 4.7: Werkzeug: Tor[1] - How Tor Works: 3

Lediglich die Kommunikation innerhalb des Tor Netzwerkes ist durch Verschlüsselung geschützt. Die Kommunikation außerhalb des Tor Netzwerkes - zwischen Tor Knoten und Ziel ist nicht geschützt. Auf diesem Teilpfad ist es möglich, die Nutzlast zu verschlüsseln. Aber es besteht weiterhin die Möglichkeit, den Nutzer über die Steuerinformationen zu identifizieren (siehe Kapitel 4.2 und 4.3).

Bewertungskriterien

Anonymität & Privatsphäre

Die Anonymität im Tor Netzwerk ist hoch. Jeder Nutzer kann Tor herunterladen und kostenfrei nutzen. Die Tor Knoten werden von verschiedenen privaten Personen sowie einigen Institutionen bereitgestellt.

[1]Quelle: `https://www.torproject.org/about/overview.html.en` (Abruf: 18.09.2016)

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Tor	156.68	65.10	63.18	127.68	1524.25	387.38
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Tor	190.73	132.28	201.50	214.43	3468.80	841.55

(a) Performanz[2]

	Typ	html	css	images	js	flash	xhr	other	media	fonts
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00	0.00	0.00
	mit Tor	8.00	11.40	123.80	79.80	1.80	4.40	8.60	1.00	0.20

(b) Anfragen

	Typ	Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Tor	72.20	4.20	0.00	2.20	6.00	4.00	0.00	88.40

(c) Tracker

Tabelle 4.5: Werkzeug: Tor[1]

Die Privatsphäre ist sehr hoch. Das Prinzip von Tor ähnelt mehreren hintereinander geschalteten Anonymous-Proxies (siehe Abbildung 4.6). Der Datenverkehr im Tor Netzwerk ist verschlüsselt und die einzelnen Knoten kennen niemals den gesamten Pfad im Netzwerk. Eine bekannte Schwäche des Tor Netzwerkes ist die Anzahl der bereitgestellten Knoten, die von einer Person oder Institution stammen. Fließt eine Kommunikation nur über Knoten eines Betreibers, dann kann der Betreiber den Pfad der Kommunikation identifizieren.

Sicherheit & Schutz

Es fallen keine persönlichen Daten beim Herunterladen oder Ausführen von Tor an, daher können sich diese auch nicht unwissentlich weiterverbreiten.

Performanz

Die Ladezeit ist sehr langsam (siehe Tabelle 4.5a). Die Anfragen benötigen im Schnitt 10- bis 20-mal länger im Vergleich zur direkten Kommunikation (ohne Tor). Bei einer Abfrage benötigte das Tor Netzwerk sogar 300-mal länger. Der Nutzer kann die Performanz nicht beeinflussen, da er den Pfad der Kommunikation durch das Tor Netzwerk nicht steuern kann.

[1] Details zu den Messungen befinden sich im Anhang A.2 und A.6.
[2] Werte entsprechen der Ladezeit in Sekunden.

Nutzung

Tor ist sehr einfach zu nutzen. Der Nutzer muss lediglich den Tor Browser oder Client starten und schon wird eine Verbindung zum Tor Netzwerk aufgebaut.

Einrichtung

Es existieren zwei Varianten, die sich ein Nutzer herunterladen kann. Einmal das Tor Browser Paket, das den Tor Browser beinhaltet. Dieser basiert auf Firefox und hat bereits einen Tor Client integriert. Der Browser besitzt außerdem noch eine Erweiterung von Tor, die die Sicherheitseinstellung des Browsers mithilfe von vier vorgegebenen Profilen konfiguriert. Ferner existieren die Erweiterungen Disconnect (siehe Kapitel 4.3.8), HTTPS Everywhere (siehe Kapitel 4.3.4) und NoScript (siehe Kapitel 4.3.16). Das andere Paket beinhaltet lediglich den Tor Client. Der Nutzer muss den SOCKS-Proxy bei den Anwendungen einstellen sofern diese über das Tor Netzwerk kommunizieren sollen.

4.2 Einstellungen für den Browser

In dieser Arbeit liegt der Fokus auf dem Webbrowser Mozilla Firefox. Dieser ist ein freier Browser und der am meisten genutzte Browser in Deutschland (siehe Abbildung 4.8). Es ist möglich, dem Browser durch Erweiterungen, sogenannte “Add-ons”, weitere Funktionen (beispielsweise Skript- und Werbeblocker) hinzuzufügen.

Einstellungen

Einige der Browser Hersteller gehen dazu über, Funktionen von Erweiterungen nativ in den Browser zu integrieren. Dazu gehören Erweiterungen, die die Privatsphäre des Nutzers schützen wie beispielsweise Werbeblocker und Blocker für weitere Tracking-Mechanismen. Als erster Browser Hersteller hat Mozilla [Moz15] diese Änderung im November 2015 verkündet und den Funktionsumfang des “Privaten Modus” vom Firefox mit einen Werbe- und Trackingblocker erweitert. Auch der Opera Browser [Op15D] wurde im Mai 2016 um einen nativen Werbeblocker erweitert, der unter anderem das Laden von Webseiten beschleunigt. Ein Monat danach wurde diese Änderung auch für den mobilen Opera Browser [Op15M] übernommen, wodurch der Nutzer bei der Übertragung Datenvolumen sparen kann.

Die Standardeinstellungen eines Browsers beinhalten häufig Einstellungen, mit denen sich ein Nutzer leichter identifizieren lässt. Daher existieren im Internet verschiedene Webseiten, wie beispielsweise eine vom BSI [BSIDB], die dem Nutzer Informationen, Tipps und Empfehlungen zu den verschieden Browsern zur Verfügung stellen.

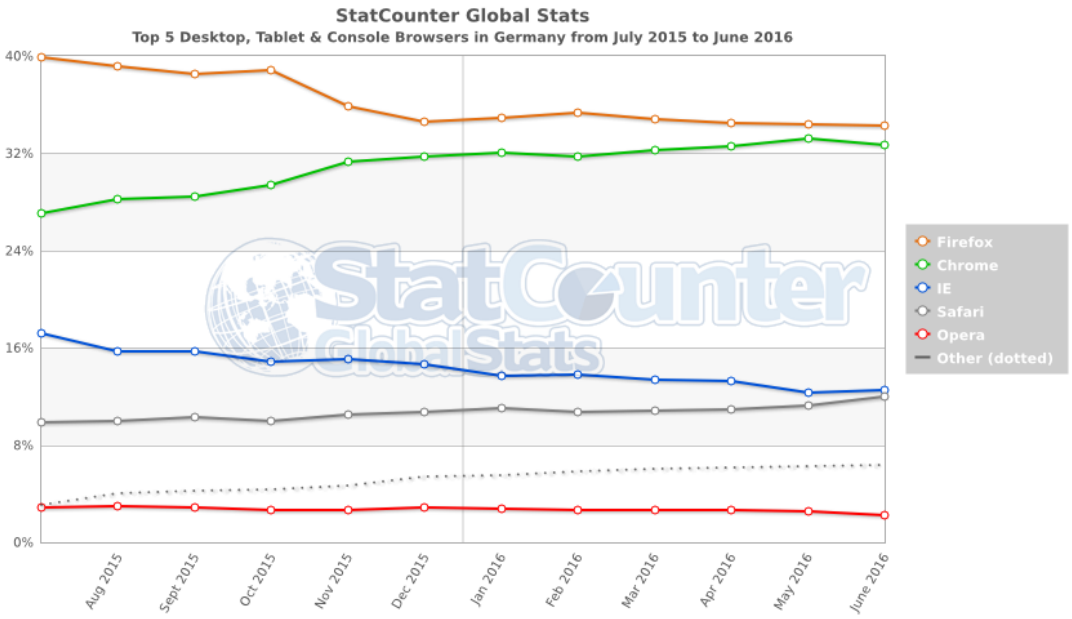


Abbildung 4.8: Einstellung: StatCounter[1]: Browser Statistik[2] - Deutschland

4.2.1 Übersicht

Einstellungen	Anonymität & Privatsphäre	Sicherheit & Schutz	Performanz	Nutzung	Einrichtung
Tracking Protection					
Datenschutz					
DNT					
WebRTC					
Optimierungen					

(a)

Symbol	Bedeutung
	neutral
	gut / einfach
	schlecht / schwer

(b) Legende

Tabelle 4.6: Einstellung: Übersicht

[1]Quelle: `http://gs.statcounter.com/#browser-DE-monthly-201507-201606` (Abruf: 31.07.2016)
[2]Über den Zeitraum von Jul 2015 bis Jun 2016.

4.2.2 Tracking Protection

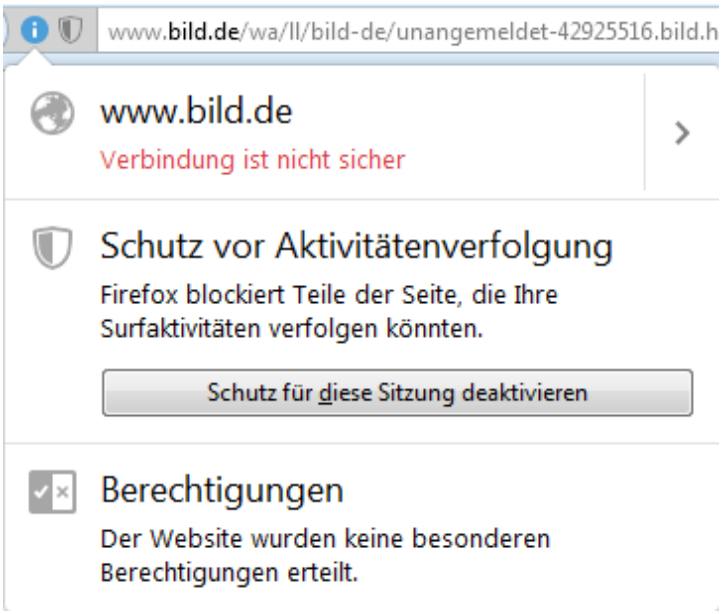


Abbildung 4.9: Einstellung: Tracking Protection

Die Tracking Protection Funktion (siehe Abbildung 4.9) ist der native Werbe- und Trackingblocker des Firefoxs. Das Paper "Tracking Protection in Firefox For Privacy and Performance" [KC15] beschreibt die Nutzung, die Funktionen und die Effizienz und vergleicht diese mit anderen Entwicklungen. Tracking Protection nutzt eine Blacklist, um Anfragen an Drittanbietern, wie beispielsweise Tracking Domains, zu verhindern. Außerdem wird das Application Programming Interface (API), die Programmierschnittstelle, von Google Safe Browsering sowie eine Teilliste von der Privatsphären orientierten Blacklist von Disconnect (siehe Kapitel 4.3.8) genutzt. Es ist möglich, noch weitere Einstellungen vorzunehmen. Die Hilfeseite von Mozilla wiki.mozilla.org/Security/Tracking_protection erklärt die weiteren Einstellungsmöglichkeiten.

Bewertungskriterien

Anonymität & Privatsphäre

Die Privatsphäre des Nutzers wird erhöht, da Cookies und weitere Tracking-Technologien unterbunden werden. Die Autoren des Papers [KC15] haben festgestellt, dass die Anzahl der HTTP-Cookies, die über die Webseiten der "Alexa top 200 news sites" verteilt werden, um 67,5% reduziert werden konnten. Außerdem bietet die Privatsphären orientierte Blacklist von Disconnect, die etwa 1500 Domains beinhaltet, zusätzlichen Schutz der

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Erw.	0.60	0.47	0.54	0.39	0.39	0.48
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Erw.	3.30	1.68	1.73	1.61	1.70	2.00

(a) Performanz[3]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit Erw.	2.00	8.00	17.80	11.00	0.00	1.00	1.20

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Erw.	3.00	2.00	0.00	1.00	1.00	0.00	0.00	7.00

(c) Tracker

Tabelle 4.7: Einstellung: Tracking Protection[1][2]

Privatsphäre.

Durch die Aktivierung dieser Funktion wurden lediglich 7 von den 78 Tracker (siehe Tabelle 4.7c) beim Besuch der Webseite geladen. Etwa 91 Prozent der Tracker wurden blockiert.

Performanz

In Tabelle 4.7a ist zu sehen, dass die Testseite mit Erweiterung um ein Vielfaches schneller lädt. Die Ladezeit mit aktiviertem Cache reduzierte sich um etwa 92 Prozent und ohne den Cache sind es immer noch 81 Prozent. Die kürzere Ladezeit kommt dadurch zustande, dass die Testseite wesentlich weniger Elemente enthält und Anfragen (siehe Tabelle 4.7b) und Tracker (siehe Tabelle 4.7c) blockiert werden.

Im Paper [KC15] wurde zusätzlich noch die Performanz bei den Webseiten der "Alexa top 200 news sites" getestet und die Autoren konnten feststellen, dass die durchschnittliche Ladezeit um 44% und das Datenvolumen um 39% reduziert wurde.

[1] Die graue Zeile bedeutet, dass die Webseite nur eingeschränkt nutzbar ist.
[2] Details zu den Messungen befinden sich im Anhang A.2 und A.7.
[3] Werte entsprechen der Ladezeit in Sekunden.

Nutzung

Die Nutzung ist sehr einfach gehalten. Der Nutzer kann lediglich die Funktion für eine Sitzung komplett deaktivieren (siehe Abbildung 4.9). Es ist dem Nutzer nicht möglich, die Funktion für einzelne Webseiten, sowie für ausgewählte Drittanbieter, zu deaktivieren oder die Einstellung dauerhaft zu speichern.

Leider gestattet die Testseite die Nutzung vom “Privaten Modus” bzw. der Tracking Protection von Firefox nicht. Daher ist sie nur sehr eingeschränkt nutzbar - der Nutzer erhält lediglich die Meldung und Informationen, weshalb die Webseite eingeschränkt nutzbar ist und wie er die normale Ansicht wiederherstellen kann.

Einrichtung

Die Tracking Protection des Firefoxs ist standardmäßig nur im Privaten Modus von Firefox aktiviert, aber die Funktion lässt sich auch dauerhaft im Browser über die `about:config` aktivieren:

Einstellungsname	Wert
privacy.trackingprotection.enabled	true

4.2.3 Datenschutz

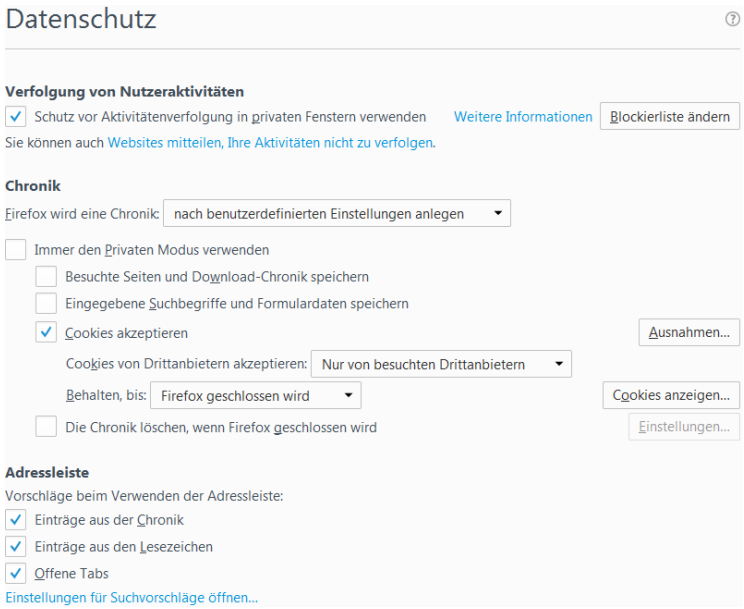


Abbildung 4.10: Einstellung: Datenschutzeinstellungen

Die in der Abbildung 4.10 unter Chronik befindlichen Datenschutzeinstellungen zeigen, wie der Browser mit Cookies umgehen soll. Der Nutzer sollte bei Cookies nach dem Minimalprinzip vorgehen. Es ist zu empfehlen, nur die wirklich notwendigen Cookies zuzulassen und die zugelassenen Cookies, sobald sie nicht mehr benötigt werden, zu entfernen.

Bewertungskriterien

Einstellung	Angepasst	Standard
Cookies	53	209

Tabelle 4.8: Einstellung: Datenschutz - Cookies[1]

Anonymität & Privatsphäre

Die Privatsphäre des Nutzers wird durch diese Einstellung erhöht, da weniger Webseiten-Betreiber den Nutzer mithilfe eines Cookies tracken können. Durch die in Abbildung 4.10 gezeigten Einstellungen werden nur noch Cookies von besuchten Drittanbietern akzeptiert und beim Schließen des Browsers werden diese gelöscht. Das reduziert die Anzahl der Cookies von 209 auf 53 Cookies (siehe Tabelle 4.8). Das entspricht einer Reduzierung von etwa 75 Prozent.

Sicherheit & Schutz

Die Einstellungen schützen vor Langzeit-Cookies und bewirken, dass Firefox die Cookies von nicht besuchten Webseiten ablehnt. Dies erschwert den Webseiten-Betreibern das Sammeln von wertvollen Informationen über die Nutzer und sie müssen andere Wege finden, den Nutzer zu identifizieren.

Nutzung

Die Nutzung der Einstellungen ist sehr einfach. Die Löschung der Cookies erfolgt automatisch beim Schließen des Browsers, ohne dass der Nutzer eingreifen muss.

Einrichtung

Die Einstellungen des Firefoxs lassen sich entweder über **Menü öffnen → Einstellungen → Datenschutz**, in der Menüleiste **Extras → Einstellungen → Datenschutz** oder über die URL `about:preferences#privacy` öffnen. Die Datenschutzeinstellungen sollten wie auf Abbildung 4.10 ersichtlich vorgenommen werden.

[1] Details zu den Cookies befinden sich im Anhang A.8.

Alternativ ist es möglich, diese Einstellungen über `about:config` zu konfigurieren:

Einstellungsname	Wert
network.cookie.cookieBehavior	3
network.cookie.lifetimePolicy	2

4.2.4 Do Not Track (DNT)

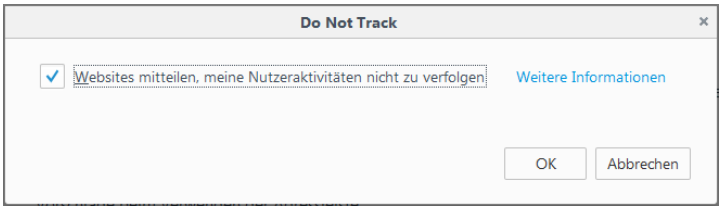


Abbildung 4.11: Einstellung: DNT-Einstellungen

DNT ist eine HTTP-Kopfzeilenerweiterung, die vom World Wide Web Consortium (W3C) in [W3CDNT] definiert wurde. Sie teilt einer Webseite mit, ob der Nutzer verhaltensbasierte Werbung von Dritten erhalten möchte. Die Unternehmen arbeiten daran, diese Funktion auf ihren Webseiten und Webservern umzusetzen.

Bewertungskriterien

Anonymität & Privatsphäre

Die Anonymität und Privatsphäre des Nutzers wird durch diese Einstellung erhöht, weil die Webseiten-Betreiber aufgefordert werden, den Nutzer nicht zu tracken.

Sicherheit & Schutz

Bietet Schutz vor Tracking, sofern der Webserver die DNT HTTP-Kopfzeilenerweiterung interpretiert und bearbeitet.

Performanz

Abhängig von der Umsetzung des Webseiten-Betreibers kann der Browser weniger Anfragen stellen und dadurch die Webseite schneller laden.

Nutzung

Die Nutzung ist sehr einfach, weil der Browser die HTTP-Kopfzeilenerweiterung automatisch an jede HTTP-Anfrage anfügt.

Einrichtung

Die DNT-Einstellungen sind in den Datenschutzeinstellungen (siehe Abbildung 4.11) des Firefoxs zu finden und sollten aktiviert werden.

Alternativ lässt sich DNT auch über `about:config` aktivieren:

Einstellungsname	Wert
privacy.donottrackheader.enabled	true

4.2.5 WebRTC

Real-Time Communication (RTC) ist ein Protokoll zur Übertragung von Multimedia-Daten in hoher Qualität wie sie beispielsweise bei Ton- und Video-Übertragungen benötigt wird. WebRTC [WebRTC] wird von den gängigen Browsern und Plattformen (Chrome, Firefox, Opera, Android und iOS) unterstützt. Außerdem ist WebRTC ein Open Source Projekt, das von Google, Mozilla und Opera unterstützt wird. Die API und das zugrunde liegende Protokoll wurden gemeinsam vom W3C und Internet Engineering Task Force (IETF) entwickelt.

Der WebRTC-Fingerprint bleibt bestehen, auch wenn der Nutzer den ISP wechselt, die IP-Adresse ändert, den Webbrowser oder den Rechner neu startet. Auch das Löschen der Cookies und des Zwischenspeichers hat keine Auswirkung auf den Fingerprint.

WebRTC sollte deaktiviert werden, wenn der Nutzer es nicht benötigt.

Bewertungskriterien

Anonymität & Privatsphäre
: Die Anonymität und Privatsphäre des Nutzers wird durch diese Einstellung erhöht, da die Webseiten-Betreiber einen Nutzer anhand des WebRTC-Fingerprints identifizieren können.

Sicherheit & Schutz
: Es nicht möglich, die lokalen und öffentlichen IP-Adressen des Rechners abzufragen. Die Nutzung eines VPNs oder eines Anonymous-Proxys wird von WebRTC nicht erkannt.

Nutzung
: Die Nutzung ist sehr einfach. Es ist nicht möglich die Deaktivierung für einzelne Webseiten vorzunehmen.

Einrichtung
: Die WebRTC-Einstellungen des Firefoxs lassen sich lediglich über `about:config` konfigurieren.

Die Werte sollten wie folgt gesetzt werden:

Einstellungsname	Wert
media.peerconnection.enabled	false

Eine noch sichere Konfiguration ist, wenn die Werte wie folgt eingestellt sind:

Einstellungsname	Wert
media.peerconnection.turn.disable	true
media.peerconnection.use_document_iceservers	false
media.peerconnection.video.enabled	false
media.peerconnection.identity.timeout	1

4.2.6 Optimierungen

Die Einstellungen von Firefox lassen sich trotz der zuvor beschriebenen Einstellungen weiter optimieren (siehe Tabelle 4.9).

Bewertungskriterien

Anonymität & Privatsphäre

Alle Einstellungen haben eine Auswirkung auf die Anonymität und Privatsphäre des Nutzers.

Nutzung

Bei den Einstellungen ist es möglich, dass besuchte Webseiten teilweise nicht mehr fehlerfrei funktionieren bzw. falsch dargestellt werden.

Einrichtung

Die in der Tabelle 4.9 aufgelisteten Einstellungen lassen sich lediglich über `about:config` konfigurieren.

Einstellungsname	Wert	Kurzbeschreibung
geo.enabled	false	Deaktiviert die Ortsbestimmung.
browser.safebrowsing.enabled	false	Deaktiviert Google Safe Browsing und Phishing Schutz. Dies ist ein Sicherheitsrisiko, aber es ist eine Verbesserung der Privatsphäre.
browser.safebrowsing.malware.enabled	false	Deaktiviert Google Safe Browsing Schadsoftware-Prüfungen. Dies ist ein Sicherheitsrisiko, aber es ist eine Verbesserung der Privatsphäre.
dom.event.clipboardevents.enabled	false	Deaktiviert die Meldung, das Webseiten benachrichtigt werden, wenn der Nutzer Inhalt der Webseite kopiert, einfügt oder ausgeschnitten hat - mit übermittelt wird, welcher Teil der Webseite markiert war.
network.cookie.cookieBehavior	1	Nur Cookies vom Ursprungs-Server akzeptieren (blockiert Drittanbieter Cookies). (Siehe Kapitel 4.2.3)
browser.cache.offline.enable	false	Deaktiviert den offline Cache.
browser.send_pings	false	Hilfreich beim Tracken der Klicks der Nutzer.
webgl.disabled	true	Dies ist ein mögliches Sicherheitsrisiko.
dom.battery.enabled	false	Webseiten-Betreiber können den Batteriestatus des Geräts tracken.
browser.sessionstore.max_tabs_undo	0	Deaktiviert die Chronik der kürzlich geschlossenen Tabs. Einsehbar über die Menü-Leiste → Chronik → Kürzlich geschlossene Tabs.

Tabelle 4.9: Einstellung: Optimierungen der Einstellungen

4.3 Erweiterungen für den Browser

Die Erweiterungen (*Add-ons*) des Browsers Firefox lassen sich entweder über **Menü öffnen → Add-ons**, in der Menüleiste **Extras → Add-ons** oder über die URL `about:addons` installieren.

4.3.1 Übersicht

Erweiterungen	Anonymität & Privatsphäre	Sicherheit & Schutz	Performanz	Nutzung	Einrichtung
Privacy Settings					
Random Agent Spoofer					
HTTPS Everywhere					
Decentraleyes					
Self-Destructing Cookies					
BetterPrivacy					
Disconnect					
Ghostery					
Privacy Badger					
Adblock Plus					
uBlock Origin					
uMatrix					
RequestPolicy					
NoScript					
Policeman					

(a)

Symbol	Bedeutung
	neutral
	gut / einfach
	schlecht / schwer

(b) Legende

Tabelle 4.10: Erweiterung: Übersicht

4.3.2 Privacy Settings

Diese Erweiterung [FFAPS] beinhaltet ähnliche und gleiche Einstellungen, die bereits in den Unterpunkten des Kapitels 4.2 erwähnt worden sind. Die Erweiterung beinhaltet intuitive Symbole für Sicherheit und Privatsphäre sowie kurze Erläuterungen zu den Funktionen (siehe

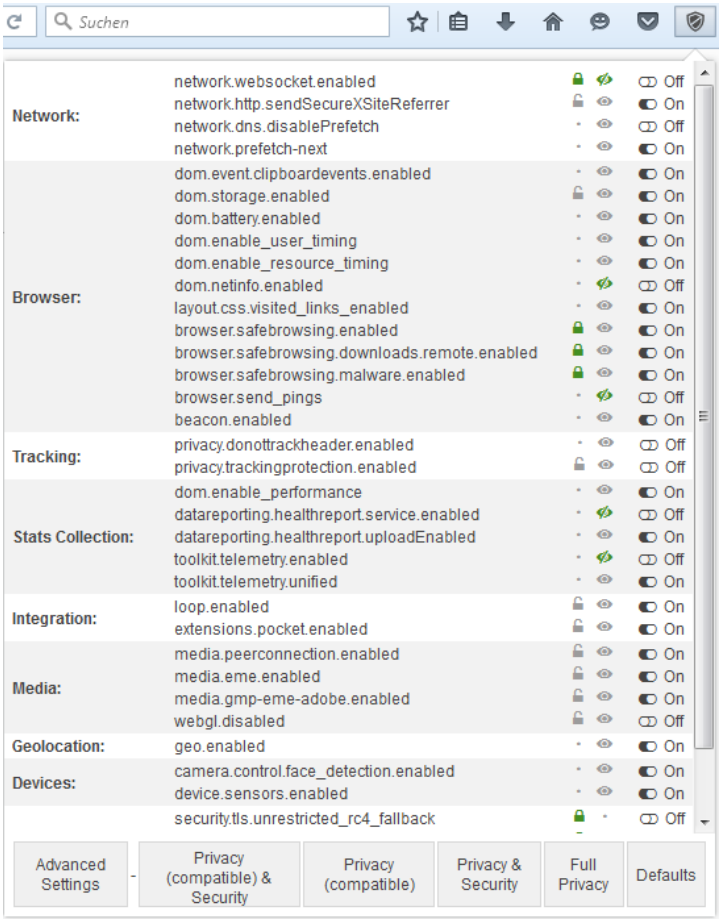


Abbildung 4.12: Erweiterung: Privacy Settings

Abbildung 4.12), die es dem Nutzer ermöglicht, die Einstellungen auf einen Blick zu verstehen. Diese Einstellungen lassen sich auch manuell über `about:config` konfigurieren. Der Quellcode der Erweiterung ist bei GitHub einsehbar und frei verfügbar.

Informationen

GitHub: `https://github.com/schomery/privacy-settings`
URL: `https://addons.mozilla.org/de/firefox/addon/privacy-settings/`

Bewertungskriterien

Anonymität & Privatsphäre

Die Erweiterung hat Auswirkungen auf die Anonymität und die Privatsphäre des Nutzers - insgesamt 43 Einstellungen haben diese Auswirkung. Diese Einstellungen sind durch ein Augen-Symbol in der Liste oder durch die Abkürzung “prvcy” in den erweiterten Einstellungen gekennzeichnet.

Nutzung

Die Nutzung der Erweiterung ist sehr einfach und intuitiv gestaltet. Der Nutzer erhält einen Überblick über viele wichtige Funktionen, die er häufig nur nach einer bestimmten Suche in `about:config` hätte einstellen können. Die Einstellungen können aber auch dazu führen, dass besuchte Webseiten nicht fehlerfrei funktionieren und dargestellt werden.

Einrichtung

Nach der Installation der Erweiterung kann der Nutzer sich eine eigene Einstellung zusammenklicken. Alternativ beinhaltet es fünf vorgefertigte Profile, die der Nutzer per Knopfdruck verwenden kann. Außerdem beinhaltet es noch zusätzliche Einstellungen, die bei der Erweiterung unter “Advanced Settings” (siehe unten links in der Abbildung 4.12) eingesehen und eingestellt werden können.

4.3.3 Random Agent Spoofer

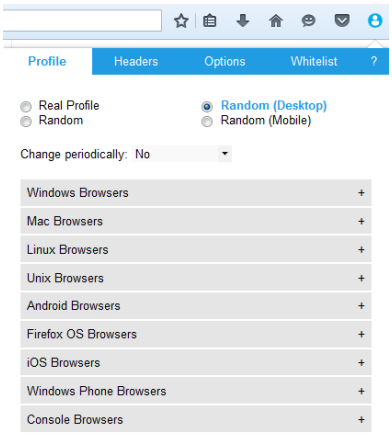


Abbildung 4.13: Erweiterung: Random Agent Spoofer

Die Erweiterung Random Agent Spoofer dient zur Verschleierung des Useragents - der vom Browser an den Webserver bei jedem Aufruf einer Webseite übermittelt wird. Des Weiteren bietet die Erweiterung noch sehr viele Funktionen zur Anonymisierung und zum Schutze der Privatsphäre wie bei der Erweiterung "Privacy Settings" in Kapitel 4.3.2. Es ist möglich, verschiedene HTTP-Steuerinformationen - wie sie bei der Nutzung eines Proxies (siehe Kapitel 4.1.3) hinzugefügt werden - zu aktivieren. Oder HTTP-Steuerinformationen Werte zu manipulieren, die Auskunft über die Herkunft eines Nutzers geben.

Informationen

GitHub: `https://github.com/dillbyrne/random-agent-spoofer`
URL: `https://addons.mozilla.org/de/firefox/addon/random-agent-spoofer/`

Bewertungskriterien

Anonymität & Privatsphäre

Die Anonymität des Nutzers erhöht sich, weil die Identifizierung über den HTTP-Agent durch die Erweiterung erschwert wird.

Performanz

Die Performanz bei der Standardeinstellung unterscheidet sich nicht zur normalen Nutzung. Sollte der Nutzer durch die weiteren Einstellungen beispielsweise Elemente blockieren, dann kann die Einstellung dazu führen, dass sich die Ladezeit der Webseite reduziert.

Nutzung

Die Nutzung der Erweiterung ist sehr einfach, da sie alle Einstellungen automatisch im Hintergrund vornimmt. Sollte der Nutzer nicht die Standardeinstellung nutzen - beispielsweise Einstellungen unter *Options* vornehmen - kann es vorkommen, dass die Webseiten nur eingeschränkt nutzbar sind und nicht mehr fehlerfrei funktionieren bzw. falsch dargestellt werden.

Einrichtung

Nach der Installation funktioniert die Erweiterung sofort. Der Nutzer sollte das Profil (siehe Abbildung 4.13) einstellen, sodass es sich periodisch ändert. Des Weiteren kann der Nutzer das verwendete Profil noch weiter ändern, die Steuerinformationen (*Headers*) anpassen und weitere Einstellungen (*Options*) konfigurieren.

4.3.4 HTTPS Everywhere

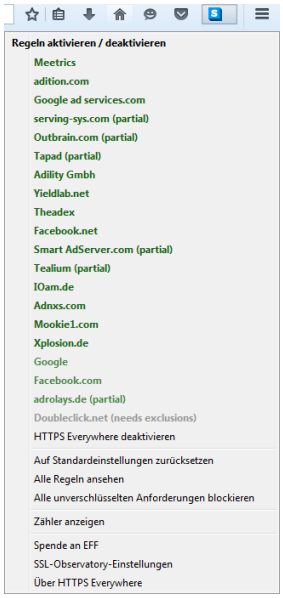


Abbildung 4.14: Erweiterung: HTTPS Everywhere

HTTPS Everywhere (siehe Abbildung 4.14) hat die einfache und schlichte Funktion zu prüfen ob die Webseite oder -seiten, die aber HTTP aufgerufen werden, auch über HTTPS erreichbar sind und diese dann per HTTPS aufzurufen. Die Erweiterung bietet auch noch die Funktion die Zertifikate der HTTPS Webseiten überprüfen zu lassen, um ein Man-in-the-Middle Angriff zu erkennen. Dazu werden die HTTPS-Zertifikate an das Electronic Frontier Foundations SSL-Observatory gesendet.

Informationen

GitHub:	`https://github.com/EFForg/https-everywhere`
URL:	`https://addons.mozilla.org/de/firefox/addon/https-everywhere/`
Entwickler:	`https://www.eff.org/https-everywhere`

Bewertungskriterien

Anonymität & Privatsphäre

Durch die Verschlüsselung des Datenverkehrs erhöht sich die Privatsphäre des Nutzers. Es wird verhindert den Datenverkehr bzw. den Dateninhalt mitzulesen und zu analysieren.

Performanz

Die Ladezeit der besuchten Webseite kann sich erhöhen. Die Studie [Nay+14] beschreibt, dass bei einer HTTPS-Verbindung die Latenz bei 40% der Webseiten von "Alexa Top 500 Sites" um mehr als 500 ms angestiegen ist.

Nutzung

Der Nutzer kann die verschiedenen Regeln (siehe Abbildung 4.14) per Knopfdruck aktivieren oder deaktivieren. Darüber hinaus kann er die Erweiterung auch für einzelne Webseiten deaktivieren und alle unverschlüsselten HTTP-Anfragen blockieren.

Einrichtung

Die Installation der Erweiterung benötigt einen Neustart des Browsers. Nachdem der Browser neu gestartet wurde erscheint ein Fenster von HTTPS Everywhere mit der Frage, ob das SSL-Observatory von EFF verwendet werden soll.

4.3.5 Decentraleyes

Decentraleyes verhindert, dass Fremdbibliotheken von Dritten geladen werden müssen. Dazu werden die Anfragen an Dritte blockiert und die Bibliothek lokal bereitgestellt.

Informationen

GitHub: `https://github.com/Synzvato/decentraleyes`
URL: `https://addons.mozilla.org/de/firefox/addon/decentraleyes/`

Bewertungskriterien

Anonymität & Privatsphäre

Die Anonymität und Privatsphäre des Nutzers wird erhöht, weil die Erweiterung verhindert, dass Anfragen an Anbieter von Fremdbibliotheken weitergeleitet werden und diese dadurch Informationen über den Nutzer sammeln könnten.

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	0	0	0	0	0	0.00
	mit Erw.	0	0.05	0	0	0	0.01
ohne Cache	ohne Erw.	0.17	0.15	0.15	0.15	0.14	0.15
	mit Erw.	0.10	0.10	0.09	0.09	0.09	0.09

(a) Performanz[2]

Typ		html	js
Ø	ohne Erw.	1.00	3.00
	mit Erw.	1.00	1.00

(b) Anfragen

Tabelle 4.11: Erweiterung: Decentraleyes[1]

Performanz

Die Ladezeit der Webseite ist abhängig von der genutzten Anzahl von Fremdbibliotheken sowie von der Anzahl der unterstützen Netzwerke bzw. der lokal zur Verfügung stehenden Bibliotheken der Erweiterung. Die Ladezeit (siehe Tabelle 4.11a) der Testseite und aktiviertem Cache bietet keinen guten Vergleich. Ohne Cache jedoch reduziert sich die Ladezeit von 0.15 auf 0.09 Sekunden (≈ 40 Prozent). Die Testseite lädt schneller, weil 2 von den 3 js-Dateien (siehe Tabelle 4.11b) lokal abgerufen werden konnten.

Nutzung

Die Erweiterung leitet automatisch die Anfragen im Hintergrund um, sodass keine Anfragen an die Dritten gestellt werden - sofern die Bibliothek lokal vorhanden ist.

Einrichtung

Nach der Installation kann der Nutzer in den Erweiterungseinstellungen noch konfigurieren, dass fehlende Inhalte nicht nachgeladen werden dürfen und das ausgewählte Domains von der Erweiterung ausgelassen werden.

4.3.6 Self-Destructing Cookies

Self-Destructing Cookies (siehe Abbildung 4.15) entfernt standardmäßig die Daten, die eine Webseite abspeichert, sobald die Webseite verlassen wird. Die Erweiterung überwacht dazu die Cookies und den lokalen Speicher des Firefoxs.

[1] Details zu den Messungen befinden sich im Anhang A.7.
[2] Werte entsprechen der Ladezeit in Sekunden.

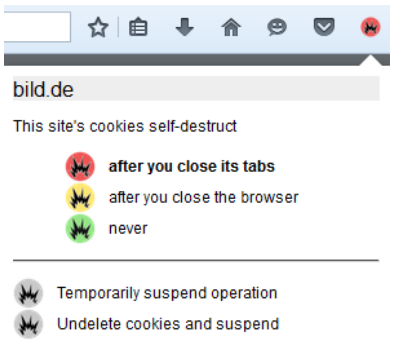


Abbildung 4.15: Erweiterung: Self-Destructing Cookies

Informationen

URL: `https://addons.mozilla.org/de/firefox/addon/self-destructing-cookies`

Bewertungskriterien

Anonymität & Privatsphäre

Die Anonymität und Privatsphäre erhöht sich durch die Erweiterung, weil die Webseiten-Betreiber die - durch die Erweiterung erkannten und gelöschten - zustandsbehafteten Tracker nicht verwenden können.

Nutzung

Der Nutzer kann Webseiten-spezifische Einstellungen vornehmen, sodass die angelegten Daten erst beim Schließen des Firefoxs oder nicht durch die Erweiterung gelöscht werden - die Erweiterung speichert die Einstellung. Die Standardeinstellung löscht die Daten nachdem der Tab geschlossen wurde. Anschließend erhält der Nutzer darüber eine Benachrichtigung.

Einrichtung

Nach der Installation der Erweiterung öffnet sich ein neues Fenster bzw. Tab in die Funktionen von Self-Destructing Cookies erklärt werden. Die Standardeinstellung der Erweiterung löscht die Cookies nachdem der Tab geschlossen wurde. Der Nutzer kann noch weitere Einstellungen bei der Erweiterung konfigurieren, wie beispielsweise die Benachrichtigung, dass der lokale Speicher des Firefoxs eingebunden ist, eine Wiederherstellungsfunktion für einen gelöschten Cookie und noch einige mehr.

4.3.7 BetterPrivacy

BetterPrivacy durchsucht standardmäßig beim Beenden des Firefoxs den Flash-Speicher nach Cookies - sofern der Flash Player auf dem Rechner installiert ist. Diese Cookies können sehr lange unbemerkt bleiben, da sie werden nicht automatisch gelöscht und sie somit wesentlich mehr Informationen über den Nutzer sammeln können. Es ist auch möglich, die Cookies manuell über den Flash Player zu löschen oder die Speicherung der Flash-Cookies einzuschränken bzw. zu deaktivieren. Standardmäßig werden die Cookies jedoch zugelassen.

Informationen

URL: `https://addons.mozilla.org/de/firefox/addon/betterprivacy/`

Bewertungskriterien

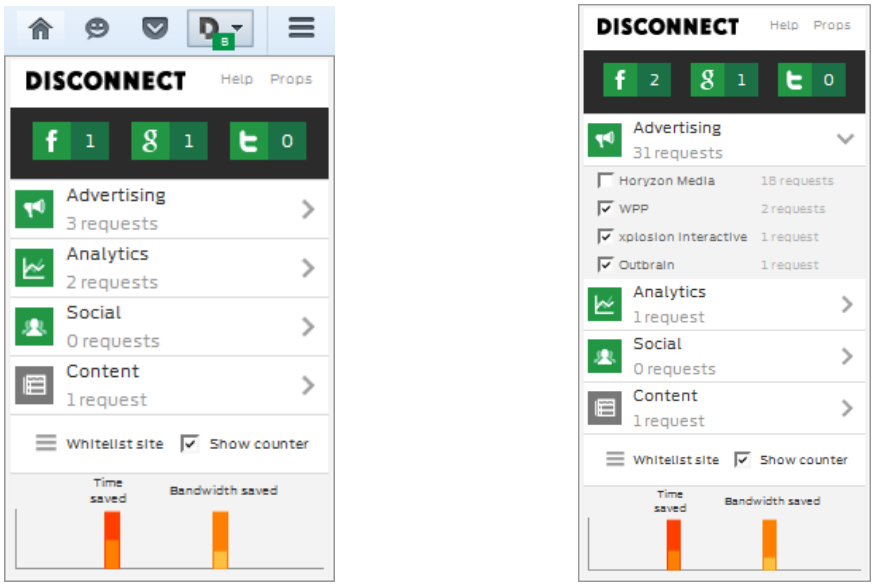
Anonymität & Privatsphäre
: Die Erweiterung erhöht die Anonymität und Privatsphäre, weil die gespeicherten Langzeit Flash-Cookies nicht mehr lange unbemerkt bleiben und gelöscht werden. Wodurch die Identifizierung der Nutzer für die Webseiten-Betreiber erschwert wird.

Nutzung
: Beim Schließen des Browsers wird BetterPrivacy ausgeführt und kontrolliert, ob sich Flash-Cookies im Speicher von Flash befinden. Befindet sich ein Cookie im Speicher, so wird der Nutzer befragt, ob er diesen löschen oder behalten möchte. Alternativ ist es möglich, die Nachfrage zu deaktivieren, sodass die Cookies automatisch gelöscht werden.

Einrichtung
: Die Installation der Erweiterung benötigt einen Neustart des Browsers. Unter Umständen muss der Nutzer in den Einstellungen der Erweiterungen den Ordner, in dem sich die Flash-Daten befinden, suchen oder wählen. Bei Nutzung von Windows 7 befinden sich die Flash-Daten beispielsweise unter *%APPDATA%\Macromedia*.

4.3.8 Disconnect

Disconnect (siehe Abbildung 4.16a) dient zum Schutz der Privatsphäre der Nutzer. Sie beinhaltet die Funktion Werbe-, Analyse-, Soziale Medien- und Content-Anbieter zu blockieren. Dies erfolgt durch das Blacklist-Prinzip. Es existiert eine Blacklist von Drittanbietern, die von dem Anbieter Disconnect zur Verfügung gestellt wird. Durch das Blockieren dieser Drittanbieter



(a) (b) Anpassung[1]

Abbildung 4.16: Erweiterung: Disconnect

können Webseiten schneller geladen werden. Der Anbieter der Erweiterung hat hierzu eine Statistik [FFADS] veröffentlicht, die zeigt, dass durchschnittlich 21% weniger Anfragen und 17% weniger Bandbreite erzeugt wurden. Dadurch konnte die Ladezeit um 27% reduziert werden. Der Quellcode der Erweiterung ist bei GitHub einsehbar und frei verfügbar.

Informationen

GitHub:	`https://github.com/disconnectme/disconnect`
URL:	`https://addons.mozilla.org/de/firefox/addon/disconnect/`
Entwickler:	`https://disconnect.me/`

Bewertungskriterien

Anonymität & Privatsphäre

In der Tabelle 4.12c ist ersichtlich, dass bei der Standard Installation von Disconnect neun Tracker aktiv sind. Leider ist die Testseite in diesem Zustand nicht nutzbar. Falls der Nutzer die Webseite ohne Einschränkungen verwenden möchte, muss er den Werbe-Anbieter

[1] Unter Advertising den Anbieter “Horyzon Media” zulassen.

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Erw.	4.48	3.41	2.98	3.67	3.32	3.57
	mit Erw.	8.43	9.87	8.84	3.50	9.08	7.94
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Erw.	19.54	10.19	10.68	11.25	11.34	12.60
	mit Erw.	10.80	11.03	9.96	4.72	10.39	9.38

(a) Performanz[3]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit Erw.	4.00	11.00	67.00	54.00	0.00	5.00	1.00
	mit Erw.	2.00	8.00	19.80	20.00	0.00	2.00	2.00

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Erw.	31.00	1.00	0.00	1.00	2.00	1.00	0.00	36.00
	mit Erw.	3.00	2.00	0.00	1.00	2.00	1.00	0.00	9.00

(c) Tracker

Tabelle 4.12: Erweiterung: Disconnect[1][2]

"Horyzon Media" zulassen (siehe Abbildung 4.16b). Nachdem der Werbe-Anbieter zugelassen ist, erhöht sich die Anzahl der erkannten Tracker auf insgesamt 36. Von den 36 Trackern sind etwa 18 Werbe-Anbieter und ein Inhalt-Anbieter zugelassen und die restlichen blockiert. Also ist die Anzahl der Tracker insgesamt von 78 auf etwa 19 Tracker ($\approx$ 76 Prozent) gesunken.

Performanz

Die Tabelle 4.12a zeigt die Ladezeiten der Testseite. Sie zeigt, dass die Ladezeit mit der Erweiterung ohne die Anpassung der zugelassenen Tracker mit aktiviertem Cache sogar von 6.16 auf 7.96 Sekunden ($\approx$ 29 Prozent) steigt. Ohne Cache ist die Ladezeit etwas geringer, dort sinkt sie von 10.61 auf 9.38 Sekunden ($\approx$ 12 Prozent).

Nachdem der Werbe-Anbieter zugelassen worden ist, sinkt die Ladezeit mit aktiviertem Cache von 6.16 auf 3.57 Sekunden ($\approx$ 42 Prozent). Ohne aktivierten Cache steigt sie jedoch von 10.61 auf 12.60 Sekunden ($\approx$ 19 Prozent).

[1] Die graue Zeile bedeutet, dass die Webseite nur eingeschränkt nutzbar ist.
[2] Details zu den Messungen befinden sich im Anhang A.2 und A.10.
[3] Werte entsprechen der Ladezeit in Sekunden.

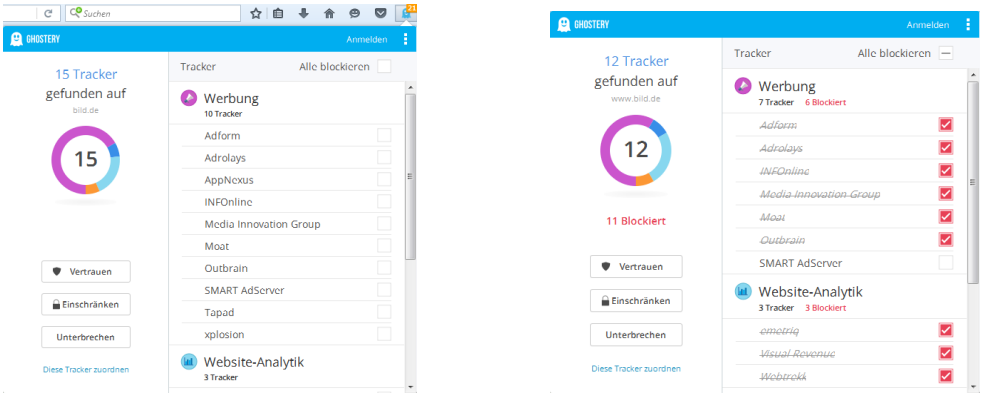
Nutzung

Es werden standardmäßig alle gefundenen Tracker blockiert. Durch die Blockierung der Tracker kann es passieren, dass die Webseite nicht mehr fehlerfrei funktioniert oder dargestellt wird. Der Nutzer hat aber die Möglichkeit, gefundene Tracker wieder zuzulassen - die Einstellung wird von der Erweiterung gespeichert und wird erst gelöscht, wenn der Nutzer den Tracker wieder blockiert - um beispielsweise die Webseite wieder in vollem Umfang nutzen zu können.

Einrichtung

Die Einrichtung der Erweiterung ist sehr einfach, der Nutzer muss das Plugin lediglich installieren und den Browser neu starten. Nach dem Neustart des Browsers blockiert die Erweiterung automatisch die erkannten Tracking-Anbieter.

4.3.9 Ghostery



(a) (b) Anpassung[1]

Abbildung 4.17: Erweiterung: Ghostery

Ghostery (siehe Abbildung 4.17a) erkennt Tracker, Web Bugs, Pixel und Beacons. Es ist möglich, die erkannten Anbieter auf der besuchten Webseite zu blockieren. Die Erweiterung arbeitet mit verschiedenen Blacklisten - für Werbung, Analyse-Webseiten, Kundenkontakt, Soziale Medien und weitere.

[1] Unter Werbung den Anbieter "SMART AdServer" zulassen.

Informationen

URL: `https://addons.mozilla.org/de/firefox/addon/ghostery/`

Entwickler: `https://www.ghostery.com/`

Bewertungskriterien

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Erw.	1.66	2.16	19.60	1.55	18.39	8.67
	mit Erw.	0.31	0.19	0.34	0.22	0.26	0.26
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Erw.	11.36	5.53	23.27	4.60	22.76	13.50
	mit Erw.	1.27	1.12	1.21	1.14	1.20	1.19

(a) Performanz[3]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit Erw.	4.20	11.00	63.60	38.00	0.00	4.20	2.20
	mit Erw.	2.00	8.00	14.00	9.00	0.00	1.00	1.00

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Erw.	29.00	1.00	0.00	1.00	1.00	0.00	0.00	32.00
	mit Erw.	3.00	2.00	0.00	1.00	1.00	0.00	0.00	7.00

(c) Tracker

Tabelle 4.13: Erweiterung: Ghostery[1][2]

Anonymität & Privatsphäre

Während Ghostery alle erkannten Tracker blockiert hatte, hat Disconnect[2] weiterhin 7 Tracker (siehe Tabelle 4.13c) auf der Webseite erkannt. Nachdem der Nutzer den Tracker "SMART AdServer" zugelassen hat, erhöht sich die Anzahl auf insgesamt 32 Tracker. Ghostery hat mit den Einstellungen die Anzahl der aktiven Tracker von 78 auf 32 (≈ 59 Prozent) reduziert.

[1] Die graue Zeile bedeutet, dass die Webseite nur eingeschränkt nutzbar ist.
[2] Details zu den Messungen befinden sich im Anhang A.2 und A.11.
[3] Werte entsprechen der Ladezeit in Sekunden.

Performanz

Die Ladezeit (siehe Tabelle 4.13a) - während Ghostery alle Tracker blockiert hat - betrug 0.26 statt 6.16 Sekunden (≈ 96 Prozent) mit genutztem Cache. Ohne Cache reduziert sich die Ladezeit von 10.61 auf 1.19 Sekunden (≈ 89 Prozent).

Nachdem der Tracker "SMART AdServer" zugelassen wurde, stieg die durchschnittliche Ladezeit mit Cache von 6.16 auf 8.67 Sekunden (≈ 41 Prozent) und ohne Cache von 10.61 auf 13.50 Sekunden (≈ 27 Prozent). Die durchschnittliche Ladezeit ist angestiegen, weil zwei Messungen - der 3. und 5. Abruf - eine verhältnismäßig sehr hohe Ladezeit hatten und dies trotz der niedrigen Anzahl an Anfragen (siehe Tabelle 4.13b). Die anderen drei Messungen waren wesentlich geringer als die normale Ladezeit der Testseite.

Nutzung

Die Standardeinstellung der Erweiterung lässt alle Tracker zu. Sobald der Nutzer ein Tracking-Anbieter blockiert, speichert die Erweiterung die Einstellung und übernimmt sie für alle besuchten Webseiten. Daher sollte der Nutzer als erstes alle erkannten Tracker blockieren und - sollte die Webseite irgendwelche Einschränkungen haben - dann Tracker für Tracker durchprobieren. Damit der Nutzer die Testseite uneingeschränkt wieder nutzen kann, muss er den Werbe-Anbieter "SMART AdServer" bei Ghostery zulassen (siehe Abbildung 4.17b).

Einrichtung

Nach der Installation der Erweiterung öffnet sich ein Fenster bzw. Tab mit zwei Schritten - bei neueren Versionen erscheinen die Schritte sobald der Nutzer das Ghostery Symbol anklickt. Der erste Schritt beinhaltet die Abfrage, ob die Webseiten- und Tracking-Daten des Nutzers erfasst werden dürfen. Beim zweiten Schritt wird der Nutzer gefragt, ob er sich einen GhostRank Benutzer erstellen möchte. Bei der Erweiterung unter **Settings → Support Ghostery** ist außerdem standardmäßig die Option **Sharing extension usage analytics** (siehe Abbildung 4.18) aktiviert.

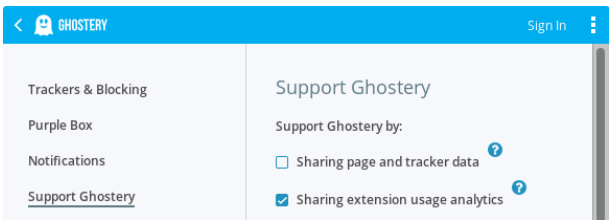
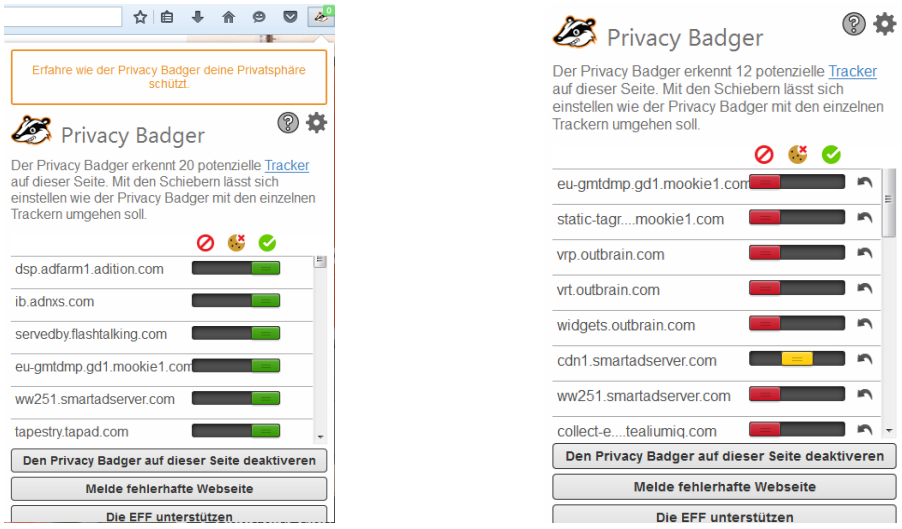


Abbildung 4.18: Erweiterung: Ghostery - Standardeinstellung

4.3.10 Privacy Badger



(a) (b) Anpassung[1]

Abbildung 4.19: Erweiterung: Privacy Badger

Privacy Badger (siehe Abbildung 4.19a) verhindert, dass eingebundene Drittanbieter einer Webseite einen Nutzer mithilfe von Cookies, "Supercookies" oder Canvas-Fingerprinting identifizieren und mit anderen Daten verknüpfen können [FFAPB]. Der Quellcode der Erweiterung ist bei GitHub einsehbar, frei verfügbar und basiert auf dem Code von Adblock Plus (ABP).

Informationen

GitHub:	`https://github.com/EFForg/privacybadgerfirefox`
URL:	`https://addons.mozilla.org/de/firefox/addon/privacy-badger-firefox/`
Entwickler:	`https://www.eff.org/privacybadger`

Bewertungskriterien

Anonymität & Privatsphäre

Sperrt der Nutzer alle potenziellen Tracker, dann ist die Testseite nur noch eingeschränkt nutzbar und die Anzahl der Tracker (siehe Tabelle 4.14c) reduziert sich von 78 auf 11 Tracker (≈ 86 Prozent).

[1] Den potenziellen Tracker "cdn1.smartadserver.com" erlauben - Cookies können weiterhin blockiert werden.

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Erw.	2.22	1.97	2.04	1.87	4.16	2.45
	mit Erw.	8.55	3.74	8.58	8.27	3.88	6.60
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Erw.	5.84	11.94	5.08	4.86	11.49	7.84
	mit Erw.	10.06	5.27	10.11	10.08	5.20	8.14

(a) Performanz[3]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit Erw.	3.00	11.00	62.00	34.00	0.00	4.00	1.00
	mit Erw.	2.00	8.00	22.00	20.00	0.00	1.00	3.00

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Erw.	10.00	0.00	0.00	1.00	6.00	1.00	0.00	18.00
	mit Erw.	2.00	1.00	0.00	1.00	6.00	1.00	0.00	11.00

(c) Tracker

Tabelle 4.14: Erweiterung: Privacy Badger[1][2]

Damit der Nutzer die Testseite wieder nutzen kann, muss er den potenzielle Tracker "cdn1.smartadserver.com" zulassen (siehe Abbildung 4.19b) - die Cookies dieser Webseite können weiterhin blockiert bleiben. Durch das Zulassen dieser beiden Webseiten kommen 7 weitere Tracker hinzu. Insgesamt reduziert sich jedoch die Anzahl von 78 auf 18 Tracker (≈ 77 Prozent).

Performanz

Die Ladezeit (siehe Tabelle 4.14a) der Testseite hat sich nicht stark verändert, aber alle potenziellen Tracker wurden blockiert. Mit Cache hat die Testseite 6.60 statt 6.16 Sekunden geladen (ein Anstieg von etwa 7 Prozent). Ohne Cache reduzierte sich die Ladezeit auf 7.84 statt 10.61 Sekunden (≈ 26 Prozent).

Nachdem der potenzielle Tracker "cdn1.smartadserver.com" (Abbildung 4.19b) zugelassen wurde, hat sich die Ladezeit der Testseite grundsätzlich verringert. Mit Cache

[1] Die graue Zeile bedeutet, dass die Erweiterung die Standardeinstellung verwendet.
[2] Details zu den Messungen befinden sich im Anhang A.2 und A.12.
[3] Werte entsprechen der Ladezeit in Sekunden.

reduzierte sich die Ladezeit von 6.16 auf 2.45 Sekunden (≈ 60 Prozent) und ohne Cache von 10.61 auf 7.84 Sekunden (≈ 26 Prozent).

Nutzung

Standardmäßig werden alle potenziellen Tracker zugelassen. Die potenziellen Tracker einer Webseite lassen sich über das Privacy Badger Symbol anzeigen. Außerdem erscheint die Anzahl der Tracker beim Symbol. Der Nutzer kann entscheiden, ob er die Webseite komplett oder nur die Cookies blockieren möchte - alternativ kann er auch Privacy Badger für die besuchte Webseite deaktivieren. Die vorgenommen Einstellungen werden durch die Erweiterung gespeichert und auf andere Webseiten übertragen.

Einrichtung

Nach der Installation von Privacy Badger öffnet sich ein neues Fenster bzw. ein neuer Tab, in dem die Funktion der Erweiterung erklärt wird. Der Nutzer muss keine weiteren Einstellungen vornehmen um die Erweiterung zu verwenden.

4.3.11 Adblock Edge

Adblock Edge blockiert Anfragen an Werbe-Anbieter und blockiert dadurch die Darstellung von Werbung. Die Erweiterung basiert auf den Quellcode von Adblock Plus (Version 2.1.2) (siehe Kapitel 4.3.12). Sie war eine sehr lange Zeit die unabhängige Alternative zu Adblock Plus - nachdem Adblock Plus die Funktion der akzeptablen Werbung eingebaut hatte. Der Entwickler hat die Weiterentwicklung der Erweiterung eingestellt und verweist auf die Erweiterung "uBlock Origin" (siehe Kapitel 4.3.13). Der Quellcode der Erweiterung ist noch bei Bitbucket und GitHub einsehbar und frei verfügbar.

Informationen

Bitbucket:	`https://bitbucket.org/adstomper/adblockedge/`
GitHub:	`https://github.com/adstomper/adblockedge`
URL:	`https://addons.mozilla.org/de/firefox/addon/adblock-edge/`

4.3.12 Adblock Plus

Adblock Plus (ABP) [FFABP] (siehe Abbildung 4.20) ist einer der ersten Werbeblocker, die es als Erweiterung für den Firefox gab. 2006 wurde er maßgeblich von Wladimir Palant als ein Open-Source Gemeinschaftsprojekt entwickelt. 2011 haben Wladimir Palant und Till Faida die Eyeo GmbH gegründet, die das Projekt von ABP nachhaltig gestalten sollte. Dies führte

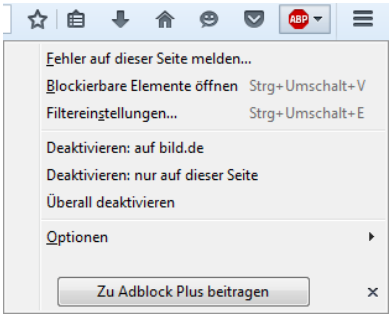


Abbildung 4.20: Erweiterung: Adblock Plus

beispielsweise zu der Funktion, dass eine Liste mit akzeptabler Werbung eingeführt wurde, die durch die Eyeo GmbH verwaltet wird.

Informationen

GitHub:	`https://github.com/adblockplus`
URL:	`https://addons.mozilla.org/de/firefox/addon/adblock-plus/`
Entwickler:	`https://adblockplus.org/`

Bewertungskriterien

Anonymität & Privatsphäre

Ohne die Abonnierung von der Filterliste von "Reek" (siehe Webseite github.com/reek/anti-adblock-killer) reduziert sich die Anzahl der Tracker (siehe Tabelle 4.15c) von 78 auf 14 (≈ 82 Prozent) - die Testseite ist nur eingeschränkt nutzbar. Nachdem der Nutzer die zusätzliche Filterliste abonniert hat - wodurch er die Testseite ohne Einschränkungen nutzen kann - erhöht sich die Anzahl von 14 auf 52 Tracker (≈ 271 Prozent). Insgesamt reduziert sich die Anzahl der Tracker von 78 auf 52 (≈ 33 Prozent).

Performanz

Ohne die zusätzliche Filterliste steigt die Ladezeit (siehe Tabelle 4.15a) der Testseite mit Cache von 6.16 auf 8.12 Sekunden (≈ 32 Prozent) an. Ohne Cache reduziert sich die Ladezeit geringfügig von 10.61 auf 9.38 Sekunden (≈ 12 Prozent).

Bei der Nutzung der zusätzlichen Filterliste mit Cache erhöhte sich die durchschnittliche Ladezeit von 6.16 auf 8.47 Sekunden (≈ 38 Prozent). Der 2. Abruf ist wahrscheinlich ein Ausreißer, da der Wert dieses Abrufes fast das Fünffache des normalen Abrufs (ohne die

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Erw.	4.42	26.19	3.77	3.85	4.12	8.47
	mit Erw.	8.78	9.28	9.38	4.12	9.04	8.12
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Erw.	10.33	33.51	8.98	7.34	9.97	14.03
	mit Erw.	10.06	10.52	10.61	5.38	10.33	9.38

(a) Performanz[3]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit Erw.	3.00	10.00	68.20	60.20	0.00	5.40	4.00
	mit Erw.	2.00	8.00	25.00	21.00	0.00	2.00	2.00

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Erw.	39.40	4.00	0.00	1.00	6.00	2.00	0.00	52.40
	mit Erw.	2.00	3.00	0.00	1.00	6.00	2.00	0.00	14.00

(c) Tracker

Tabelle 4.15: Erweiterung: Adblock Plus[1][2]

Erweiterung) beträgt. Bei den anderen Abrufen war die Ladezeit mindestens um 1.15 Sekunden geringer. Ohne Cache stieg die durchschnittliche Ladezeit von 10.61 auf 14.03 Sekunden (≈ 32 Prozent). Auch hier war es der 2. Abruf, der für diesen Durchschnittswert gesorgt hat. Die Ladezeit der anderen Abrufe sind grundsätzlich etwas schneller als beim normalen Abruf.

Nutzung

Der Nutzer kann bei der Erweiterung einstellen, dass sie auf der Domain, nur auf der besuchten Webseite oder überall deaktiviert ist. Außerdem hat er die Möglichkeit noch weiter Elemente über die Einstellung *Blockierbare Elemente* hinzuzufügen. Die Einstellung zeigt jedes geladene sowie zugelassene oder blockierte Element der besuchten Webseite an. Es ist möglich, die Position des gewünschten Elements aufzeigen zu lassen - das Fenster springt zum Element und es erscheint ein rot gepunkteter Rahmen.

Einrichtung

Die Einrichtung von Adblock Plus ist sehr einfach. Nach der Installation ist der Werbeblocker mit einer Filterliste standardmäßig aktiviert. Der Nutzer kann über die Fil-

[1] Die graue Zeile bedeutet, dass die Webseite nur eingeschränkt nutzbar ist.
[2] Details zu den Messungen befinden sich im Anhang A.2 und A.13.
[3] Werte entsprechen der Ladezeit in Sekunden.

tereinstellungen noch weitere Filterlisten hinzufügen. Sollte der Nutzer viele englische Webseiten besuchen, dann sollte er zusätzlich noch die Filterliste “EasyList (English)” abonnieren. Außerdem ist noch die Filterliste “EasyList (privacy protection)” vorhanden, die Tracker beinhaltet und vor diesen schützt. Wenn der Nutzer die Testseite besucht und keine Einschränkungen haben möchte, kann er die Filterliste von “Reek” (siehe Webseite github.com/reek/anti-adblock-killer) abonnieren.

Die Option *Einige nicht aufdringliche Werbung zulassen* (siehe Abbildung 4.21) ist standardmäßig in den Einstellungen aktiviert. Die Liste[1] der akzeptablen Werbung beinhaltet 9.852 Zeilen.

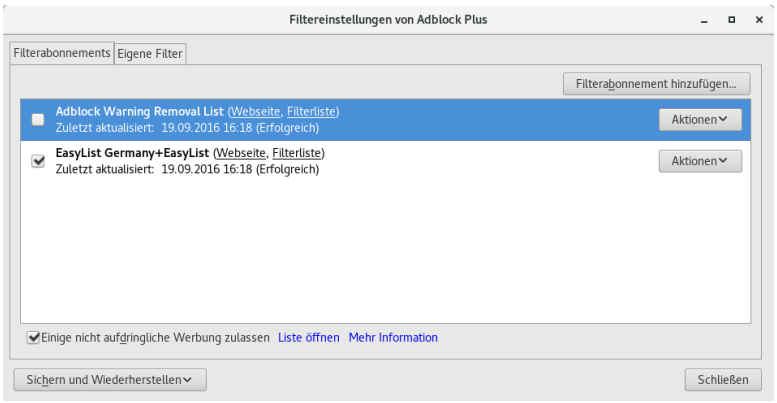


Abbildung 4.21: Erweiterung: Adblock Plus - Standardeinstellung

4.3.13 uBlock Origin

uBlock Origin (siehe Abbildung 4.22) kann mithilfe von Filterlisten Werbung aus verschiedene Bereichen blockieren. Zu diesen Bereichen gehören Listen zu Werbung, Privatsphäre, Schadsoftware, Soziale Netzwerke und anderen Themen. Außerdem existiert die Möglichkeit, einen Regionen - bzw. Sprachen - bezogenen Filter zu abonnieren. Der Quellcode der Erweiterung ist bei GitHub einsehbar und Open Source mit einer Public License (GPLv3).

[1] Quelle: `https://easylist-downloads.adblockplus.org/exceptionrules.txt` (Abruf am 19.09.16)

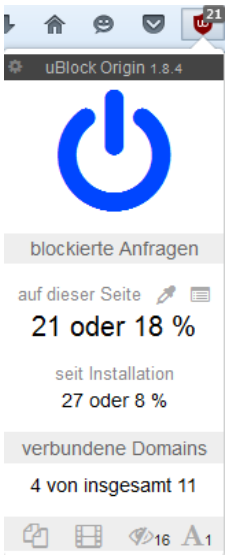


Abbildung 4.22: Erweiterung: uBlock Origin

Informationen

GitHub: `https://github.com/gorhill/uBlock`
URL: `https://addons.mozilla.org/de/firefox/addon/ublock-origin/`

Bewertungskriterien

Anonymität & Privatsphäre

Die Anzahl der Tracker (siehe Tabelle 4.16c) wird von 78 auf 9 ($\approx$ 88 Prozent) reduziert.

Performanz

Die Ladezeit (siehe Tabelle 4.16a) reduzierte sich mit Cache von 6.16 auf 0.94 Sekunden ($\approx$ 85 Prozent). Ohne Cache betrug die Ladezeit weniger als die Hälfte der normalen Ladezeit - sie reduzierte sich von 10.61 auf 4.79 Sekunden ($\approx$ 55 Prozent).

Nutzung

Der Nutzer kann die Erweiterung für die besuchte Webseite oder die gesamte Domain deaktivieren. Außerdem kann er weitere Elemente der Webseite mithilfe der Pipette (*Element-Picker-Modus*) oder der Netzwerkanfragen blockieren. Darüber hinaus kann der Nutzer für jede Webseite noch weitere Filter (*Blockieren von Popups* und *Blockieren großer Medienelemente*) aktivieren und die standardmäßig aktivierten Filter (*Kosmetische Filter* und *Remote-Schriftarten*) deaktivieren.

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Erw.	1.10	0.84	1.10	0.77	0.88	0.94
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Erw.	3.96	4.59	5.23	4.71	5.48	4.79

(a) Performanz[3]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit Erw.	2.00	9.00	57.00	19.00	0.00	4.00	1.00

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Erw.	2.00	2.00	0.00	1.00	3.00	1.00	0.00	9.00

(c) Tracker

Tabelle 4.16: Erweiterung: uBlock Origin[1][2]

Einrichtung

Nach der Installation ist uBlock Origin direkt einsatzbereit. Der Nutzer kann in den Einstellungen der Erweiterung im Reiter *Vorgegebene Filter* weitere Filterlisten abonnieren. Standardmäßig sind nur 10 von den 62 Filterlisten aktiv.

4.3.14 uMatrix

uMatrix (siehe Abbildung 4.23a) ist eine sehr komplexe Erweiterung. Die Erweiterung besitzt eine Matrix-basierte Darstellung. Damit ist es möglich, verschiedene Einstellungen per Maus-Klick zu erlauben oder zu verbieten. Die Standardeinstellung der Erweiterung ist der "blockiere alles/erlaube ausnahmsweise"-Modus, wodurch unkontrollierte Anfragen an Dritte vermieden werden.

Informationen

GitHub: `https://github.com/gorhill/uMatrix`
URL: `https://addons.mozilla.org/de/firefox/addon/umatrix/`

[1] Die graue Zeile bedeutet, dass die Webseite nur eingeschränkt nutzbar ist.
[2] Details zu den Messungen befinden sich im Anhang A.2 und A.14.
[3] Werte entsprechen der Ladezeit in Sekunden.

(a) (b) Anpassung[1]

Abbildung 4.23: Erweiterung: uMatrix

Bewertungskriterien

Anonymität & Privatsphäre

Während die Erweiterung die Standardeinstellungen verwendet hat, reduzierte sich die Anzahl der Tracker von 78 auf 4 (≈ 95 Prozent). In diesem Zustand ist aber die Testseite leider nicht nutzbar und der Nutzer muss die in Abbildung 4.23b gezeigten Elemente zulassen.

Nachdem er dies ausgeführt hat, erhöht sich die Anzahl der Tracker von 4 auf 27 (≈ 575 Prozent). Insgesamt hat sich jedoch die Anzahl der Tracker von 78 auf 27 (≈ 65 Prozent) reduziert.

Performanz

Die Ladezeit mit Standardeinstellungen und Cache reduzierte sich von 6.16 auf 0.21 Sekunden (≈ 97 Prozent). Ohne Cache reduzierte sich die Ladezeit von 10.61 auf 3.90 Sekunden (≈ 63 Prozent).

Nachdem der Nutzer die Erweiterung angepasst hat - wie in Abbildung 4.23b gezeigt - reduzierte sich die Ladezeit noch einmal mit aktiviertem Cache von 6.16 auf 0.12 Sekunden (≈ 98 Prozent) und ohne Cache von 10.61 auf 3.04 Sekunden (≈ 71 Prozent).

[1] Skripte zulassen von: `code.bildstatic.de`, `ec-ns.sascdn.com` und `cdn1.smartadserver.com`.

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Erw.	0.18	0.10	0.11	0.15	0.04	0.12
	mit Erw.	0.32	0.14	0.42	0.04	0.11	0.21
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Erw.	3.41	3.09	2.64	3.27	2.81	3.04
	mit Erw.	3.99	2.88	5.52	2.73	4.38	3.90

(a) Performanz[3]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit Erw.	2.00	10.00	54.00	19.00	0.00	4.00	1.00
	mit Erw.	2.00	8.00	43.00	2.00	0.00	1.00	1.00

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Erw.	24.00	1.00	0.00	1.00	1.00	0.00	0.00	27.00
	mit Erw.	2.00	1.00	0.00	1.00	0.00	0.00	0.00	4.00

(c) Tracker

Tabelle 4.17: Erweiterung: uMatrix[1][2]

Nutzung

Die Erweiterung blockiert standardmäßig alle Anfragen bis auf die, die zur Domain der besuchten Webseite gehen. Es kann vorkommen, dass durch die Blockierung die besuchte Webseite nicht mehr richtig funktioniert - wie bei der Testseite. Dann muss der Nutzer probieren, welche Elemente die besuchte Webseite benötigt. Bei der Testseite sind es die in Abbildung 4.23b gezeigten Elemente.

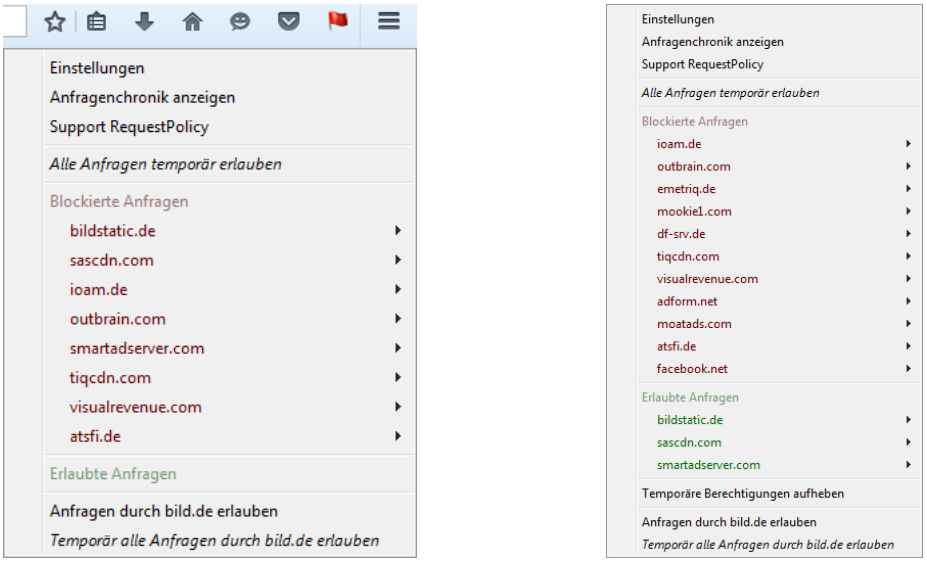
Der Nutzer kann in der Matrix (siehe Abbildung 4.23a) jedes Feld auswählen. Der obere Teil des Feldes lässt das Element zu und der untere Teil des Feldes blockiert das Element. Die vorgenommenen Einstellungen sind jedoch nur temporär und nur für die aktuell besuchte Webseite, aber der Nutzer hat die Möglichkeit, die Einstellungen explizit für die Webseite zu speichern oder zu löschen. Außerdem kann der Nutzer den User-Agent verschleiern (siehe Kapitel 4.3.3), den Referrer verschleiern und HTTPS erzwingen (siehe Kapitel 4.3.4).

[1] Die graue Zeile bedeutet, dass die Webseite nicht nutzbar ist.
[2] Details zu den Messungen befinden sich im Anhang A.2 und A.15.
[3] Werte entsprechen der Ladezeit in Sekunden.

Einrichtung

Der Nutzer muss keine speziellen Einstellungen vornehmen. Er kann aber die Einstellungen der Erweiterung (im *Dashboard*) dauerhaft anpassen und darunter sind Einstellungen der Privatsphäre, die Möglichkeit eigene Regeln zu erstellen oder zu importieren und weitere Hosts-Dateien hinzufügen oder die bereits abonnierten Hosts-Dateien zu entfernen.

4.3.15 RequestPolicy



(a) (b) Anpassung[1]

Abbildung 4.24: Erweiterung: RequestPolicy

RequestPolicy (siehe Abbildung 4.24a) überprüft Cross-Site Anfragen der besuchten Webseite. Es existiert eine neue Version dieser Erweiterung, die unter dem Namen "RequestPolicy Continued" weiterentwickelt wird. Aktuell ist die Weiterentwicklung jedoch nur als Beta Version verfügbar.

[1] Anfragen erlauben durch `bild.de` nach: `bildstatic.de`, `sascdn.com` und `smartadserver.com`.

Informationen

GitHub:	`https://github.com/RequestPolicy/requestpolicy`
URL:	`https://addons.mozilla.org/de/firefox/addon/requestpolicy/`
Entwickler:	`https://www.requestpolicy.com/`

Bewertungskriterien

Anonymität & Privatsphäre

Während die Erweiterung alle Cross-Site Anfragen blockiert, reduziert sich die Anzahl der Tracker (siehe Tabelle 4.18c) von 78 auf 4 (≈ 95 Prozent). In diesem Zustand ist die Testseite jedoch nicht nutzbar und der Nutzer muss die in Abbildung 4.24b gezeigten Regeln übernehmen. Nachdem die Regeln übernommen wurden, steigt die Anzahl der Tracker von 4 auf 32 (≈ 700 Prozent). Insgesamt reduzierte sich die Anzahl der Tracker jedoch von 78 auf 32 (≈ 59 Prozent).

Performanz

Die Ladezeit (siehe Tabelle 4.18a) - während alle Cross-Site Anfragen blockiert wurden - mit Cache reduzierte sich von 6.16 auf 0.17 Sekunden (≈ 97 Prozent). Ohne Cache erhöhte sich die Ladezeit von 10.61 auf 13.98 Sekunden (≈ 32 Prozent). Die erhöhte Ladezeit kam durch den 1. Abruf zustande, der wahrscheinlich ein Ausreißer war. Die Ladezeit bei den anderen vier Abrufen war mindestens 5 Sekunden geringer.

Mit den Anpassungen der Regeln (siehe Abbildung 4.24b) verschlechterten sich die Ladezeiten mit Cache von 6.16 auf 11.80 Sekunden ≈ 92 Prozent und ohne Cache von 10.61 auf 18.78 Sekunden ≈ 77 Prozent.

Nutzung

Der Nutzer kann die Erweiterung deaktivieren indem er die Einstellung *Alle Anfragen temporär erlaubt* (siehe Abbildung 4.24a) verwendet. Des Weiteren kann der Nutzer bei einem Besuch einer Webseite jede erkannte Cross-Site Anfrage auswählen, ob er diese dauerhaft oder lediglich temporär erlauben möchte, ob nur die direkte Verbindung erlaubt sein soll oder ob die gesamte Zieldomain in die Whitelist übernommen werden soll.

Die Testseite ist nicht nutzbar, wenn alle Cross-Site Anfragen blockiert werden. Der Nutzer muss die in der Abbildung 4.24b gezeigten Anfragen erlauben.

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Erw.	10.31	10.29	25.15	1.94	11.33	11.80
	mit Erw.	0.20	0.12	0.17	0.22	0.12	0.17
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Erw.	18.27	18.70	31.31	10.26	15.34	18.78
	mit Erw.	53.98	3.36	4.96	3.32	4.26	13.98

(a) Performanz[3]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit Erw.	3.80	11.00	63.80	39.00	0.20	4.00	1.00
	mit Erw.	2.00	5.00	36.00	4.00	0.00	0.20	1.00

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Erw.	29.00	1.00	0.00	1.00	1.00	0.00	0.00	32.00
	mit Erw.	2.00	1.00	0.00	1.00	0.00	0.00	0.00	4.00

(c) Tracker

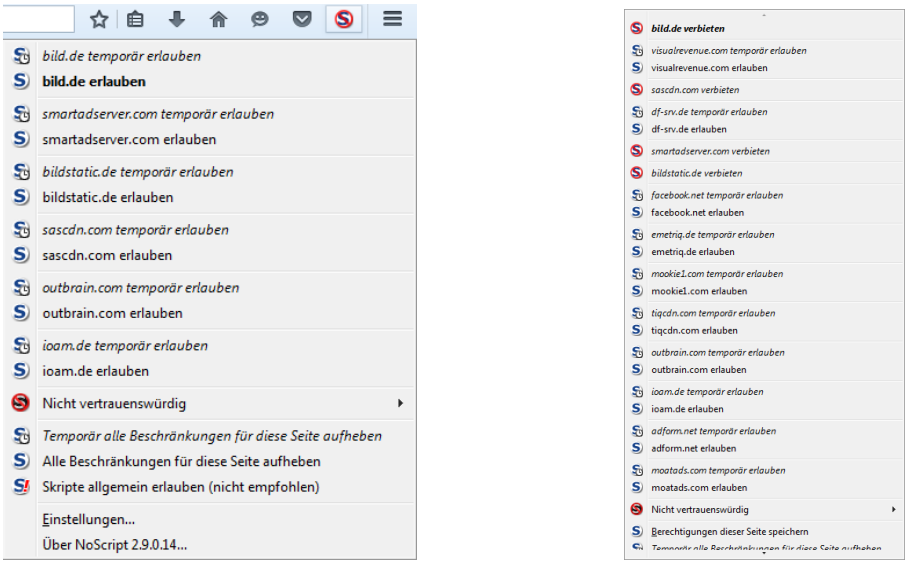
Tabelle 4.18: Erweiterung: RequestPolicy[1][2]

Einrichtung

Die Installation der Erweiterung benötigt einen Neustart des Browsers. Nachdem der Browser neu gestartet wurde, kann der Nutzer eine Region aus der Liste - International, Amerika, Asien, USA und Kanada, Europa und Russland, Ozeanien - auswählen, welche für die Region vorgefertigte Regeln enthält. Ansonsten ist die Whitelist leer und es werden alle Cross-Site Anfragen blockiert. Außerdem hat der Nutzer noch die Möglichkeit, die Einstellungen zu exportieren oder zu importieren und Regeln manuell anzulegen. Unter der Einstellung *Allgemein* kann der Nutzer die Option *Host* (oder sogar *Vollständige Adresse*) verwenden. Damit lassen sich die Regeln noch wesentlich genauer und nicht nur auf Domain-Ebene definieren. Alternativ kann der Nutzer die Regeln auch während des Besuchs einer Webseite konfigurieren (siehe Abbildung 4.24a).

[1] Die graue Zeile bedeutet, dass die Webseite nicht nutzbar ist.
[2] Details zu den Messungen befinden sich im Anhang A.2 und A.16.
[3] Werte entsprechen der Ladezeit in Sekunden.

4.3.16 NoScript



(a) (b) Anpassung[1]

Abbildung 4.25: Erweiterung: NoScript

NoScript (siehe Abbildung 4.25a) unterbindet standardmäßig die Ausführung von Skripten, wie beispielsweise JavaScript und Flash. NoScript arbeitet mit einer Black- und Whitelist. Sollte der Nutzer die Skripte einer Webseite erlauben, so landet diese in der Whitelist - alternativ kann der Nutzer die Skripte einer Webseite auch nur temporär erlauben. Die Erweiterung beinhaltet außerdem noch einen Schutz vor Cross-Site Skripting und fügt den HTTP-Anfragen die DNT HTTP-Steuerinformation (siehe Kapitel 4.2.4) an.

Informationen

URL: `https://addons.mozilla.org/de/firefox/addon/noscript/`

Entwickler: `https://noscript.net/`

[1] Folgende Domains erlauben: `bild.de`, `bildstatic.de`, `sascdn.com` und `smartadserver.com`.

Bewertungskriterien

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Erw.	2.18	1.75	15.46	12.58	10.53	8.50
	mit Erw.	0.66	0.63	0.14	1.03	0.27	0.55
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Erw.	10.18	8.26	19.68	18.49	15.99	14.52
	mit Erw.	4.34	2.98	3.17	3.97	4.81	3.85

(a) Performanz[3]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit Erw.	4.00	11.00	63.00	39.00	0.00	4.00	1.00
	mit Erw.	2.00	8.00	44.40	0.00	0.00	0.00	0.00

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Erw.	29.00	1.00	0.00	1.00	1.00	0.00	0.00	32.00
	mit Erw.	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

(c) Tracker

Tabelle 4.19: Erweiterung: NoScript[1][2]

Anonymität & Privatsphäre

Die Erweiterung schafft es als eine von zwei der vorgestellten Erweiterungen die Anzahl der Tracker (siehe Tabelle 4.19c) mit Standardeinstellungen der Testseite von 78 auf 0 (≈ 100 Prozent) zu reduzieren. Leider ist die Testseite in diesem Zustand nicht nutzbar, daher muss der Nutzer die in Abbildung 4.25b gezeigten Einstellungen übernehmen. Durch diese Einstellungen reduziert sich die Anzahl der Tracker lediglich von 78 auf 32 (≈ 59 Prozent).

Performanz

Mit den Standardeinstellungen reduzieren sich die Ladezeiten (siehe Tabelle 4.19a) mit Cache von 6.16 auf 0.55 Sekunden (≈ 91 Prozent) und ohne Cache von 10.61 auf 3.85 Sekunden (≈ 64 Prozent). Nachdem der Nutzer die Einstellungen (Abbildung 4.25b)

[1] Die graue Zeile bedeutet, dass die Webseite nicht nutzbar ist.
[2] Details zu den Messungen befinden sich im Anhang A.2 und A.17.
[3] Werte entsprechen der Ladezeit in Sekunden.

übernommen hat, steigen die Ladezeiten mit Cache von 6.16 auf 8.50 Sekunden (≈ 38 Prozent) und ohne Cache von 10.61 auf 14.52 Sekunden (≈ 37 Prozent).

Nutzung

Der Nutzer kann die Erweiterung deaktivieren indem er die Einstellung *Skripte allgemein erlauben* verwendet. Zusätzlich kann er die Einstellung *Temporär alle Beschränkungen für diese Seite aufheben* (siehe Abbildung 4.25a) verwenden. Nachdem die Webseite neu geladen wurde kann es vorkommen, dass zusätzliche Webseiten erkannt worden sind. Des Weiteren kann der Nutzer bei einem Besuch einer Webseite jede erkannte Webseite auswählen, ob er diese lediglich temporär oder dauerhaft erlauben möchte - er kann die Webseite auch als nicht vertrauenswürdig einstufen, wodurch alle Anfragen blockiert werden. Die temporären Einstellungen kann der Nutzer speichern lassen.

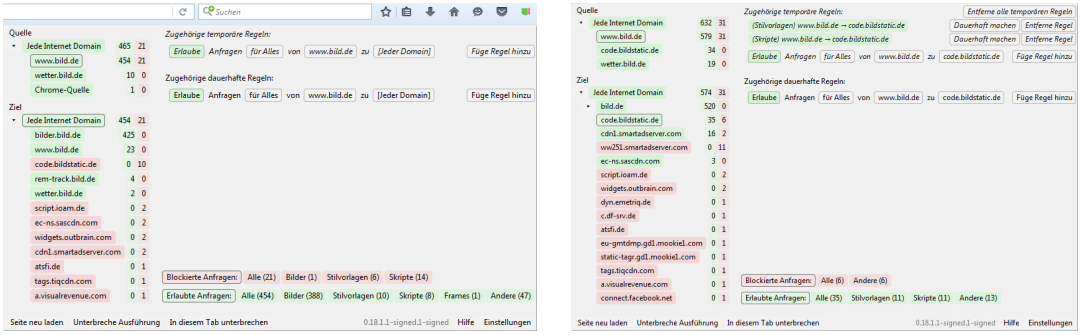
Die Erweiterung blockiert standardmäßig alle Anfragen. Durch die Blockierung kann es vorkommen, dass die besuchte Webseite nicht mehr richtig funktioniert - wie bei der Testseite. Dann muss der Nutzer probieren, welche Elemente die besuchte Webseite benötigt. Bei der Testseite sind es die in Abbildung 4.25b gezeigten und genannten Elemente.

Einrichtung

Die Installation der Erweiterung benötigt einen Neustart des Browsers. Nachdem der Browser neu gestartet worden ist öffnet sich die Webseite des Entwicklers `https://noscript.net/` mit dem Parameter `?ver=2.9.0.14`. Dieser Parameter gibt die installierte Version an.

Der Nutzer kann noch einige Einstellungen in der Erweiterung vornehmen, wie beispielsweise die *Positivliste*, die gesperrten *Eingebettete Objekte* und das *Aussehen*. Unter der Einstellung *Aussehen* kann der Nutzer unter anderem die Option *Vollständige Domains* (oder sogar *Vollständige Adressen*) aktivieren. Damit lassen sich die Regeln noch wesentlich genauer und nicht nur auf Domain-Ebene definieren.

4.3.17 Policeman



(a) (b) Anpassung[1]

Abbildung 4.26: Erweiterung: Policeman

Policeman (siehe Abbildung 4.26a) blockiert das Laden von Inhalten, die auf Servern von Drittanbietern liegen. Dabei geht die Erweiterung ähnlich vor wie ein Skriptblocker, jedoch erfolgt die Erlaubnis nach Inhaltstypen wie beispielsweise Bilder, Stilvorlagen und Skripte.

Informationen

GitHub: `https://github.com/futpib/policeman/wiki`
URL: `https://addons.mozilla.org/de/firefox/addon/policeman/`

Bewertungskriterien

Anonymität & Privatsphäre

Die Erweiterung schafft es mit Standardeinstellungen - als eine von den zwei der vorgestellten Erweiterungen - die Anzahl der Tracker (siehe Tabelle 4.20c) von 78 auf 0 ($\approx$ 100 Prozent) zu reduzieren. Mit den Standardeinstellungen ist die Testseite jedoch nicht nutzbar und der Nutzer muss die Einstellungen (siehe Abbildung 4.26b) anpassen. Nachdem die Einstellung angepasst wurde, ist die Anzahl der Tracker immer noch stark reduziert. Insgesamt wurde die Anzahl der Tracker von 78 auf 7 ($\approx$ 91 Prozent) reduziert.

[1] Skripte erlauben von `www.bild.de` zu: `code.bildstatic.de`, `ec-ns.sascdn.com` und `cdn1.smartadserver.com`
Stilvorlagen erlauben von `www.bild.de` zu: `code.bildstatic.de`.

Abruf		1.	2.	3.	4.	5.	Ø
mit Cache	ohne Erw.	9.44	5.25	5.65	5.19	5.27	6.16
	mit Erw.	0.54	0.24	0.28	0.22	0.33	0.32
	mit Erw.	0.46	0.26	0.22	0.18	0.13	0.25
ohne Cache	ohne Erw.	13.51	9.72	9.99	9.82	10.02	10.61
	mit Erw.	4.03	3.57	5.71	4.59	4.32	4.44
	mit Erw.	2.28	4.27	3.30	2.50	2.86	3.04

(a) Performanz[3]

Typ		html	css	images	js	flash	xhr	other
Ø	ohne Erw.	5.00	11.00	87.60	75.20	1.00	6.20	6.00
	mit Erw.	2.00	10.00	54.80	22.00	0.00	4.00	1.00
	mit Erw.	2.00	5.00	34.20	4.00	0.00	0.00	1.00

(b) Anfragen

Typ		Werbung	Analyse	Sozial	Inhalt	F	G	T	Gesamt
Ø	ohne Erw.	64.20	4.00	0.00	2.00	6.00	2.00	0.00	78.20
	mit Erw.	7.00	0.00	0.00	0.00	0.00	0.00	0.00	7.00
	mit Erw.	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

(c) Tracker

Tabelle 4.20: Erweiterung: Policeman[1][2]

Performanz

Die Ladezeiten (siehe Tabelle 4.20a) konnten mit den Standardeinstellungen mit Cache von 6.16 auf 0.25 Sekunden ($\approx$ 96 Prozent) und ohne Cache von 10.61 auf 3.04 Sekunden ($\approx$ 71 Prozent) reduziert werden.

Nachdem die Einstellungen (siehe Abbildung 4.26b) angepasst wurden sind, erhöhte sich diese Ladezeit leicht aber ist im Vergleich zu der normalen Ladezeit noch stark reduziert. Die Ladezeiten sanken mit Cache von 6.16 auf 0.32 Sekunden ($\approx$ 95 Prozent) und ohne Cache von 10.61 auf 4.44 Sekunden ($\approx$ 58 Prozent).

Nutzung

Die Nutzung ist ähnlich wie bei den bereits vorgestellten Erweiterungen, aber im Vergleich zu diesen etwas komplexer. Der Nutzer erhält eine Übersicht (siehe Abbildung 4.26a), welche Anfragen blockiert und zugelassen werden. Die Standardeinstellung der Erweiterung lässt alle Anfragen von der besuchten Webseite (Domain) sowie von den

[1] Die graue Zeile bedeutet, dass die Webseite nicht nutzbar ist.
[2] Details zu den Messungen befinden sich im Anhang A.2 und A.18.
[3] Werte entsprechen der Ladezeit in Sekunden.

Subdomains zu. Anfragen an Webseiten der Subdomains werden nur ausgeführt, wenn sie durch die besuchte Webseite initiiert wurden. Durch diese Einstellung ist die Testseite nicht nutzbar. Der Nutzer muss die in der Abbildung 4.26b gezeigten Einstellungen übernehmen oder selbst probieren, welche Elemente zugelassen werden müssen, damit die Webseite fehlerfrei funktioniert.

Einrichtung

Der Nutzer kann noch verschiedene Einstellungen - *Allgemeine Einstellungen*, *Popup*, *Verwaltete Regelsätze* und *Bearbeite eigene Regeln* - an der Erweiterung vornehmen. Unter der Einstellung *Verwaltete Regelsätze* lassen sich beispielsweise noch weitere vordefinierte Regeln aktivieren wie z.B. die Blockierung von Tor und I2P (ein Anonymes Netzwerk - ähnlich wie Tor). Außerdem lässt sich hier auch die Reihenfolge der Anwendung durch Regeln bestimmen. Unter der Einstellung *Verwaltete Regelsätze* kann der Nutzer manuell Regeln erstellen oder vorhandene Regeln exportieren oder importieren.

5 Schlussbetrachtung

In diesem Kapitel werden die vorherigen Kapitel der Arbeit zusammengefasst. Es folgen das Fazit und ein Ausblick auf die Zukunft der vorgestellten Technologien und Mechanismen.

5.1 Zusammenfassung

Das Kapitel der Grundlagen erklärt die verschiedenen Tracking-Definitionen. Es werden die bisherige und künftige Zunahme der Geräte im Internet sowie des Datenaufkommens und der dazugehörigen Bandbreite beschrieben. Des Weiteren wird der "Big Brother Award" erwähnt, um exemplarisch zu zeigen, wie Unternehmen teilweise mit den persönlichen Daten der Nutzer umgehen.

Im darauf folgenden Kapitel werden die verschiedenen Tracking-Technologien und die dazu verwendeten Verfahren kompakt vorgestellt. In der Arbeit wird zwischen allgemeinen Verfahren und konkreten Implementierungen der Technologien unterschieden.

Danach werden die verschiedenen Tracking-Schutzmechanismen vorgestellt. Mithilfe des praktischen Teils der Arbeit werden diese bewertet und miteinander verglichen. Die Tracking-Schutzmechanismen werden in drei Unterkapitel aufgegliedert. Das erste Unterkapitel befasst sich mit der Verschleierung der Steuerinformationen. Das nächste Unterkapitel zeigt, die Möglichkeiten der Nutzer hat, sich mit den nativen Funktionen und Einstellungen des Browsers vor Tracking zu schützen. Das letzte Unterkapitel befasst sich mit möglichen Erweiterungen, die der Nutzer verwenden kann, um das Tracking einzuschränken. Die Einstellungen und Erweiterungen fokussieren sich im Vergleich zu dem ersten Unterkapitel auf die Nutzlast bzw. den Dateninhalt.

Jedes dieser drei Unterkapitel beginnt mit einer tabellarischen Übersicht und einer Bewertung der beschriebenen Werkzeuge, Einstellungen und Erweiterungen. Die fünf Kriterien zur Bewertung setzen sich zusammen aus "Anonymität & Privatsphäre", "Sicherheit & Schutz", "Per-

formanz", "Nutzung" und "Einrichtung". Zu den zuvor genannten Bereichen wurden praktische Messungen durchgeführt, deren Ergebnisse zur Bewertung herangezogen werden.

5.2 Fazit

Bei der Verwendung der Tracking-Schutzmechanismen muss der Nutzer den Aufwand gegenüber dem Nutzen für sich abwägen und meistens einen Kompromiss eingehen:

Die Einrichtung und Benutzung der Werkzeuge zur Verschleierung VPN, Proxy und Tor sind nicht ganz einfach. Des Weiteren leidet die Performanz stark darunter, da die Pakete umgeleitet werden müssen, um die Anonymität und Privatsphäre des Nutzers zu erhöhen. Zusätzlich muss bei der Nutzung von VPN und Proxy auf die Vertrauenswürdigkeit des Anbieters geachtet werden.

Mithilfe der Browser Einstellungen kann der Nutzer seine Anonymität, Privatsphäre und Performanz verbessern. Die Einstellungen haben zur Folge, dass die Einrichtung teilweise kompliziert ist und die Nutzung nicht einfach ist. Sollte der Nutzer beispielsweise nur die Einstellungen verwenden, die über die normale Oberfläche (Datenschutz und DNT) einstellbar sind, wird die Nutzung des Browsers kaum beeinflusst. Alle anderen Einstellungen können aber größere Folgen für die Nutzung haben, da dann besuchte Webseiten unter Umständen falsch dargestellt werden oder nur eingeschränkt funktionieren.

Die Auswahl der Erweiterungen ist nicht einfach: Zum einen existieren sehr viele verschiedene Erweiterungen und zum anderen haben diese Erweiterungen auch häufig ähnliche oder gleiche Funktionen. Die vorgestellten Erweiterungen lassen sich in fünf Gruppen unterteilen. Die ersten vier Erweiterungen (Privacy Settings, Random Agent Spoofer, HTTPS Everywhere und Decentraleyes) sind allgemeine Erweiterungen. Danach folgen zwei Erweiterungen (Self-Destructing Cookies und BetterPrivacy), die speziell dem Schutz vor Cookies dienen. Darauf folgen drei Erweiterungen (Disconnect, Ghostery und Privacy Badger), die sich generell auf Tracker konzentrieren. Die nächsten zwei Erweiterungen (Adblock Plus und uBlock Origin) dienen hauptsächlich der Blockierung von Werbe-Anbietern. Die letzten vier Erweiterungen (uMatrix, RequestPolicy, NoScript und Policeman) blockieren HTTP-Anfragen für verschiedene Webseiten-Elemente.

Es ist nicht sinnvoll, alle Erweiterungen gleichzeitig einzusetzen, da sie sich teilweise gegenseitig "blockieren" und die Performanz des Browsers darunter leidet. Ferner hängt es sehr von den Ansprüchen des Nutzers - hinsichtlich Anonymität & Privatsphäre usw. - ab, welche Erweiterung eingesetzt werden sollte. In den ersten beiden Gruppen hebt sich keine Erweiterung ab, da sie unterschiedliche Ziele verfolgen. In den drei weiteren Gruppen zeichnen sich Privacy Badger, uBlock Origin und Policeman durch die Untersuchungsergebnisse aus und werden zur Nutzung empfohlen.

Der Nutzer kann sich nicht vor allen Tracking-Technologien schützen, er kann lediglich Tracking-Daten reduzieren. Bei der Auswahl der Schutzmechanismen muss er Prioritäten setzen und ggf. Defizite in Kauf nehmen.

5.3 Ausblick

Die vorgestellten Tracking-Technologien sind wahrscheinlich nur ein kleiner Ausschnitt von den derzeit eingesetzten Tracking-Methoden. Tracking-Technologien zeichnen sich dadurch aus, dass sie lange unbemerkt bleiben und dadurch möglichst viele Informationen über Nutzer sammeln können. Die vorgestellten Verfahren sind daher lediglich die, die bereits "enttarnt" worden sind bzw. zu denen öffentliche Informationen existieren.

"Daten sind das neue Öl" ist ein Zitat aus dem Jahr 2009 von Meglena Kuneva (EU-Politikerin). Dieses Zitat scheint auch die Einschätzung großer Konzerne zu sein. Diese suchen immer weitere Wege, den Nutzer bzw. den Kunden für sich transparenter zu machen und weitere Informationen über ihn zu erhalten. Der Nutzer wird die Dienste künftig nur ohne Einschränkungen verwenden können, wenn er die Einbindung der Tracking-Verfahren vom Anbieter akzeptiert.

Es zeichnet sich bereits jetzt schon ab, dass Informationen aus verschiedenen Bereichen des täglichen Lebens (Medien, Finanzen, Gesundheit, usw.) miteinander verknüpft werden, um daraus einen Mehrwert der Daten zu erzeugen. Diese Entwicklung befindet sich im Anfangsstadium, und die möglichen Folgen für die Nutzer lassen sich noch nicht abschätzen. Es ist aber zu befürchten, dass sensible, personenbezogene Daten gesammelt, verwendet und sogar gehandelt werden. Die Privatsphäre wird verloren gehen.

A Anhang

A.1 Allgemeines zu den Messungen

A.1.1 Testsystems

Die Ergebnisse wurden mithilfe einer virtuellen Maschine erzeugt.

Details der virtuellen Maschine:

Prozessor	1 CPU
Arbeitsspeicher	2 GiB
Betriebssystem	Windows 7
Browser	Mozilla Firefox - x86
Internet	100.000 MBit/s

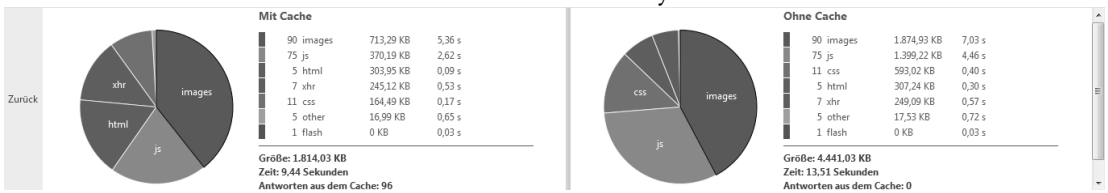
A.1.2 Testseite

Die Messungen wurden am 19.09.2016 mit der Webseite `http://www.bild.de/` erzeugt, sofern nichts anderes direkt bei der Messung angegeben worden ist.

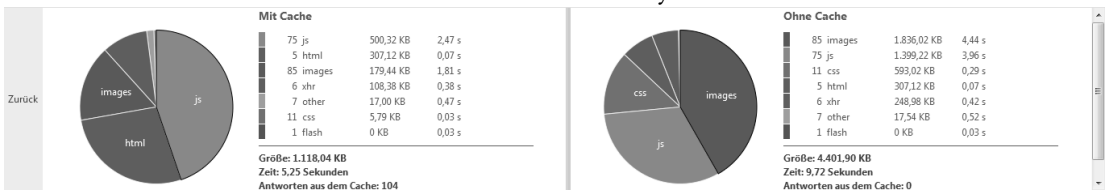
A.2 Standardinstallation von Firefox

Es wurde eine Standardinstallation von Firefox verwendet. Firefox bietet mit seinen Entwickler-Werkzeugen eine Möglichkeit einen Performanz-Test auszuführen. Dazu wurde das Entwickler-Werkzeug *Netzwerkanalyse* verwendet, das die Ladezeit und Anfragen misst. Die Installation wurde zusätzlich mit den Plugin Disconnect (siehe Kapitel 4.3.8) erweitert. Die Filterung von Disconnect wurde deaktiviert, um feststellen zu können, wie viele und aus welcher Kategorie die Tracker auf der Seite aktiv sind.

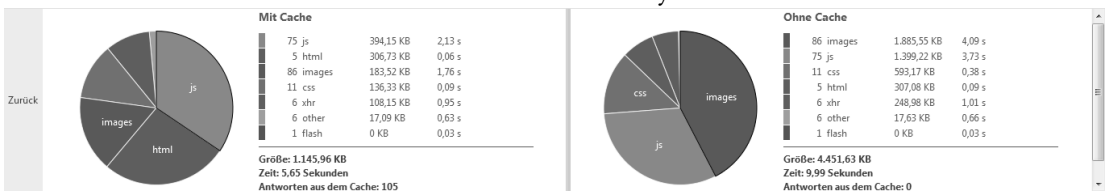
Firefox - Netzwerkanalyse: 1.



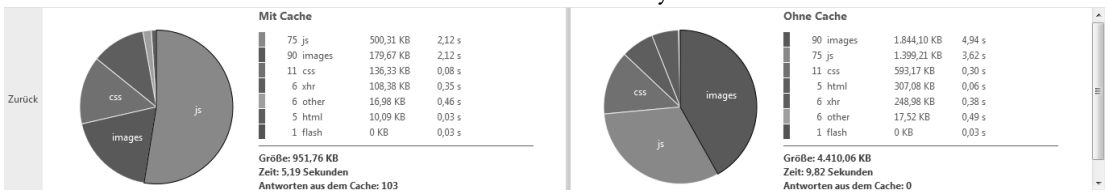
Firefox - Netzwerkanalyse: 2.



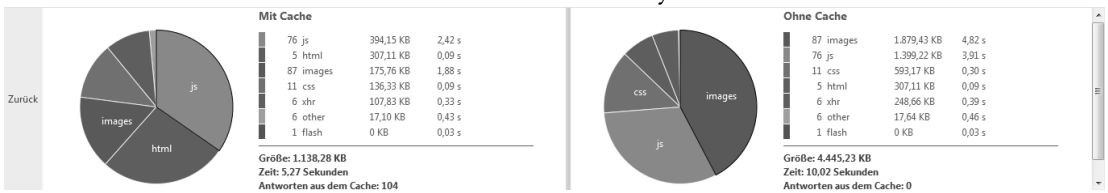
Firefox - Netzwerkanalyse: 3.



Firefox - Netzwerkanalyse: 4.



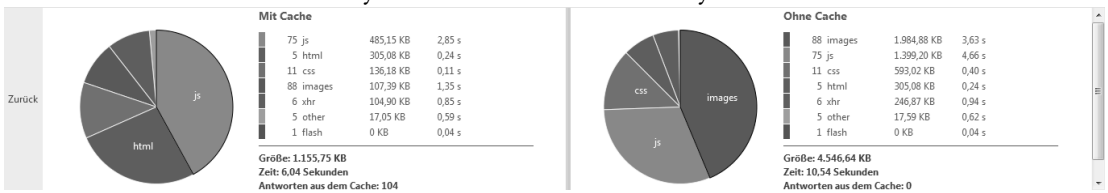
Firefox - Netzwerkanalyse: 5.



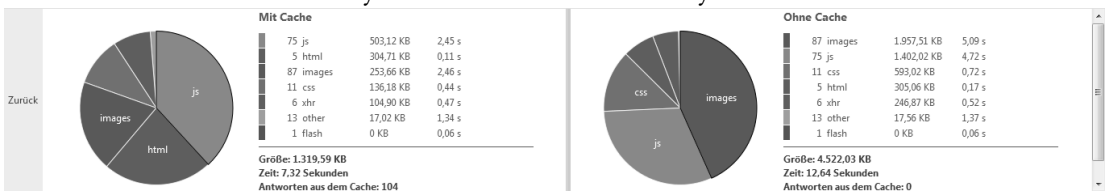
Firefox - Tracker: 1 - 5

A.3 Werkzeug: VPN - Messungen

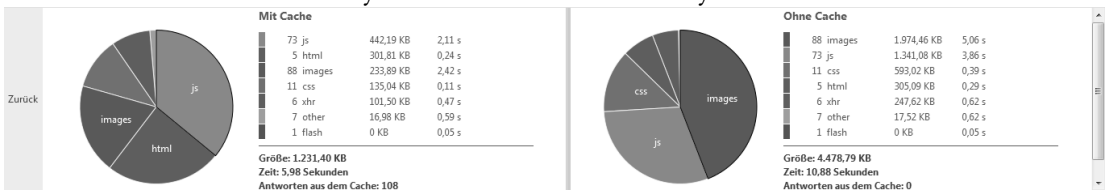
CyberGhost 6 - Netzwerkanalyse: 1.



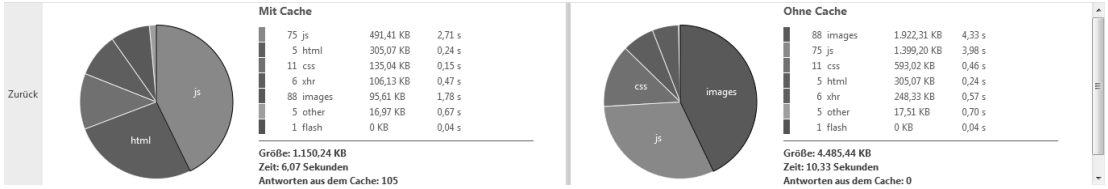
CyberGhost 6 - Netzwerkanalyse: 2.



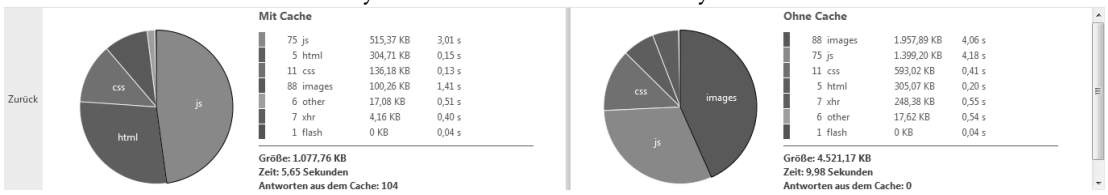
CyberGhost 6 - Netzwerkanalyse: 3.



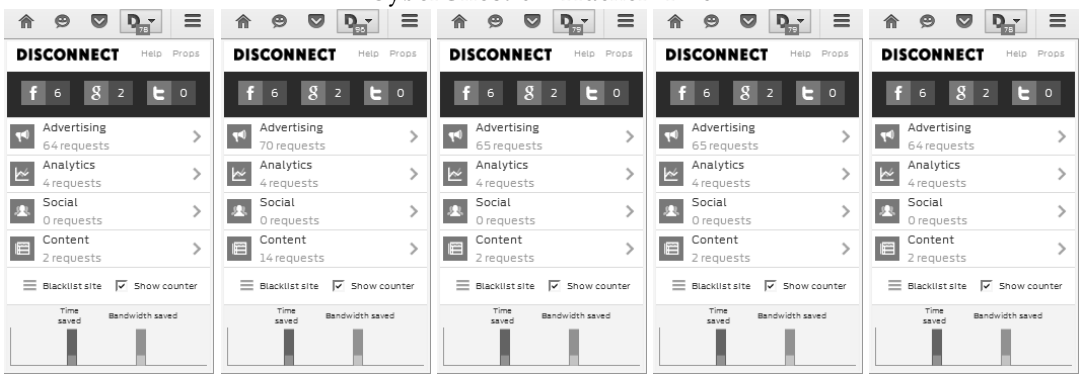
CyberGhost 6 - Netzwerkanalyse: 4.



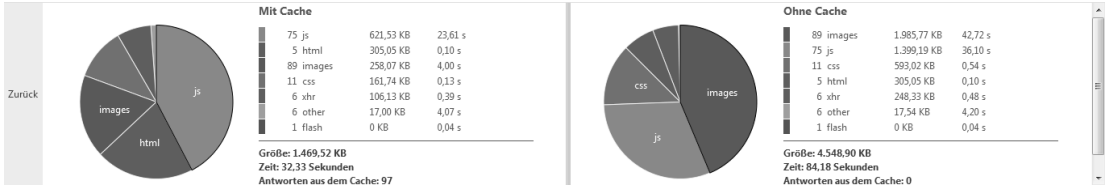
CyberGhost 6 - Netzwerkanalyse: 5.



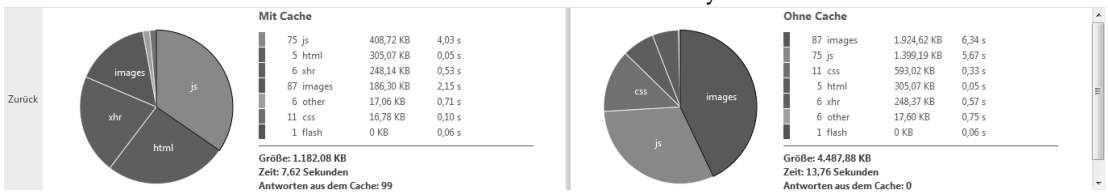
CyberGhost 6 - Tracker: 1 - 5



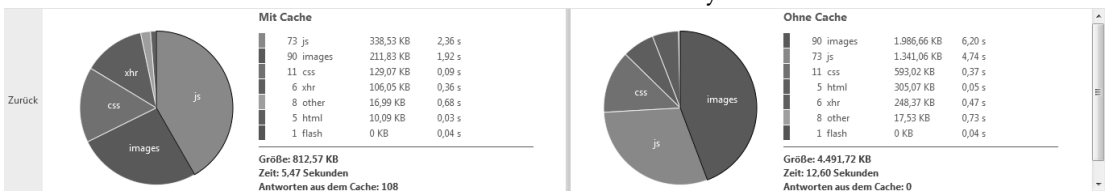
VPN Unlimited - Netzwerkanalyse: 1.



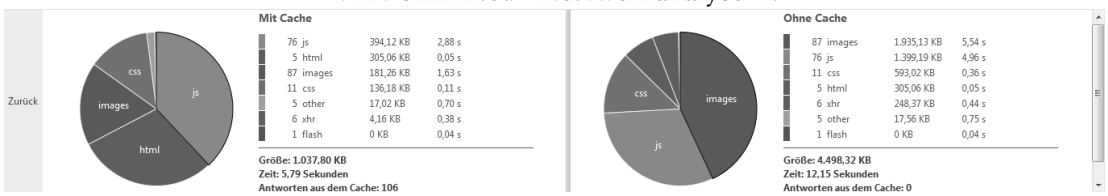
VPN Unlimited - Netzwerkanalyse: 2.



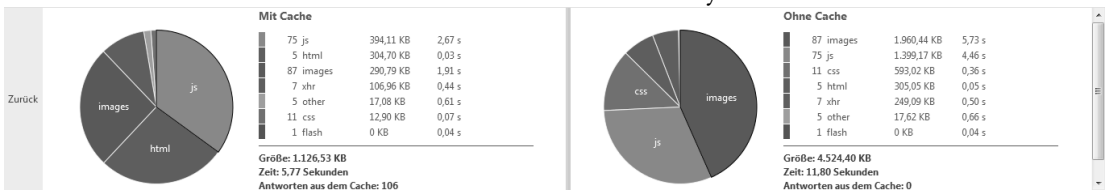
VPN Unlimited - Netzwerkanalyse: 3.



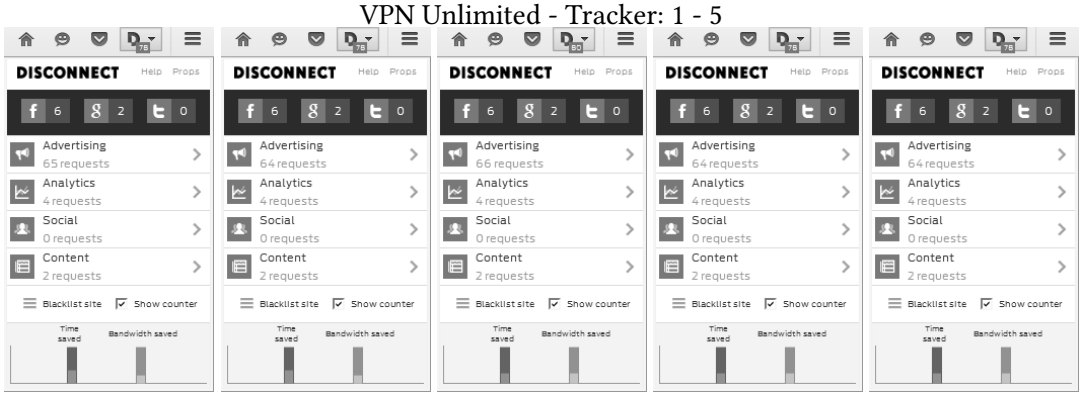
VPN Unlimited - Netzwerkanalyse: 4.



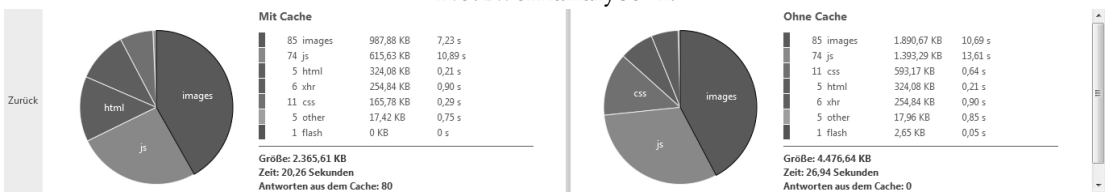
VPN Unlimited - Netzwerkanalyse: 5.



VPN Unlimited - Tracker: 1 - 5



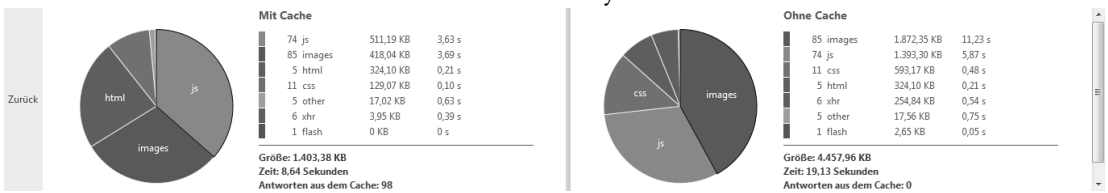
Netzwerkanalyse: 1.



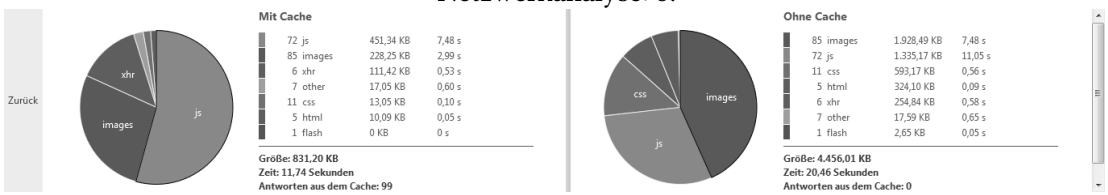
Netzwerkanalyse: 2.

Netzwerkanalyse: 3.

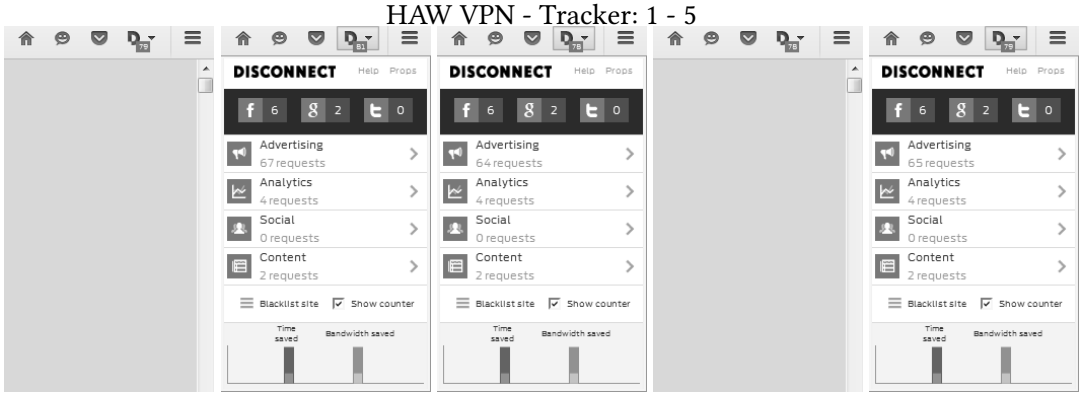
Netzwerkanalyse: 4.



Netzwerkanalyse: 5.



HAW VPN - Tracker: 1 - 5



A.4 Werkzeug: VPN - Privatsphäre

Generell ist es den Webseiten-Betreibern möglich die Browser Informationen des Nutzers auszuwerten, da diese von der genutzten Anwendung übermittelt werden.

```
Refered From: Direct Visit
User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:48.0) Gecko
   /20100101 Firefox/48.0
Screen Resolution: 1366 x 768 (pixels)
Browser Dimensions: 1366 x 657 (pixels)
Cookie Status: Enabled
Cookies (Only Cookies Visible to WhatsMyIP.org): none
Browser Plugins: No Plugins Installed
```

Abbildung A.5: VPN: Privatsphäre mit VPN - Browser Information[1]

ohne VPN: Browser-Infromationen

```
Hostname: ip92342caa.dynamic.kabel-deutschland.de
Proxy: No Proxy or Invisible Proxy Used
SCRIPT_URL: /more-info-about-you/
SCRIPT_URI: http://www.whatsmyip.org/more-info-about-you/
HTTP_HOST: www.whatsmyip.org
HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:48.0) Gecko
   /20100101 Firefox/48.0
HTTP_ACCEPT: text/html, application/xhtml+xml, application/xml;q
   =0.9, */*;q=0.8
HTTP_ACCEPT_LANGUAGE: de, en-US;q=0.7, en;q=0.3
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_CONNECTION: keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS: 1
...
```

Abbildung A.6: VPN: Privatsphäre ohne VPN - Server & Network Information[2]

[1] Quelle: http://www.whatsmyip.org/more-info-about-you/ (Abruf: 06.07.2016)
[2] Quelle: http://www.whatsmyip.org/more-info-about-you/ (Abruf: 21.09.2016)

mit VPN: Browser-Infromationen

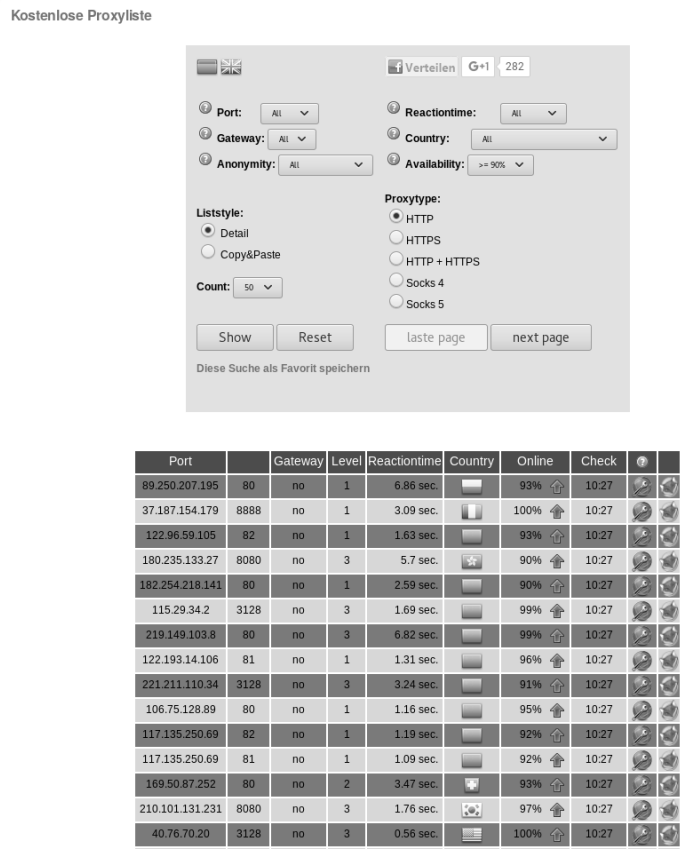
```
Hostname: ws197180.vpn.haw-hamburg.de
Proxy: No Proxy or Invisible Proxy Used
SCRIPT_URL: /more-info-about-you/
SCRIPT_URI: http://www.whatsmyip.org/more-info-about-you/
HTTP_HOST: www.whatsmyip.org
HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:48.0) Gecko
   /20100101 Firefox/48.0
HTTP_ACCEPT: text/html, application/xhtml+xml, application/xml;q
   =0.9, */*;q=0.8
HTTP_ACCEPT_LANGUAGE: de, en-US;q=0.7, en;q=0.3
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_CONNECTION: keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS: 1
...
```

Abbildung A.7: VPN: Privatsphäre mit VPN - Server & Network Information[1]

[1] Quelle: `http://www.whatsmyip.org/more-info-about-you/` (Abruf: 21.09.2016)

A.5 Werkzeug: Proxy - Privatsphäre

Es existieren Seiten die Listen von Proxy-Servern zur Verfügung stellen, die in regelmäßigen Abständen überprüft werden. Beispielsweise ist proxy-listen.de eine solcher Seiten (siehe unterer Abschnitt der Abbildung A.8), die solch eine Liste zur Verfügung stellt. Nun verwendet diese Seite eine andere Bezeichnungen für die Klassifizierung der Privatsphäre. Diese Bezeichnungen können jedoch zurück geführt werden auf die vom Autor definierten.



Port		Gateway	Level	Reactiontime	Country	Online	Check
89.250.207.195	80	no	1	6.86 sec.		93%	10:27
37.187.154.179	8888	no	1	3.09 sec.		100%	10:27
122.96.59.105	82	no	1	1.63 sec.		93%	10:27
180.235.133.27	8080	no	3	5.7 sec.		90%	10:27
182.254.218.141	80	no	1	2.59 sec.		90%	10:27
115.29.34.2	3128	no	3	1.69 sec.		99%	10:27
219.149.103.8	80	no	3	6.82 sec.		99%	10:27
122.193.14.106	81	no	1	1.31 sec.		96%	10:27
221.211.110.34	3128	no	3	3.24 sec.		91%	10:27
106.75.128.89	80	no	1	1.16 sec.		95%	10:27
117.135.250.69	82	no	1	1.19 sec.		92%	10:27
117.135.250.69	81	no	1	1.09 sec.		92%	10:27
169.50.87.252	80	no	2	3.47 sec.		93%	10:27
210.101.131.231	8080	no	3	1.76 sec.		97%	10:27
40.76.70.20	3128	no	3	0.56 sec.		100%	10:27

Abbildung A.8: Proxy: Ausschnitt einer Webseite mit einer Proxyliste[1]

Bezeichnungstabelle:

Transparent (L3)	Transparent
Anonym (L2)	Distorting
Elite (L1)	Anonymous

[1] Quelle: `http://www.proxy-listen.de/Proxy/Proxyliste.html` (Abruf: 14.07.2016)

Transparent-Proxy: Browser-Infromationen

Details:

Server 180.235.133.27

Port 8080

```
Hostname: promail.vpshosting.com.hk
Proxy: 180.235.133.27
Proxy Type: 1.1 VPS12 (squid/3.1.23)
SCRIPT_URL: /more-info-about-you/
SCRIPT_URI: http://www.whatsmyip.org/more-info-about-you/
HTTP_HOST: www.whatsmyip.org
HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:48.0) Gecko
   /20100101 Firefox/48.0
HTTP_ACCEPT: text/html, application/xhtml+xml, application/xml;q
   =0.9, */*;q=0.8
HTTP_ACCEPT_LANGUAGE: de, en-US;q=0.7, en;q=0.3
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_VIA: 1.1 VPS12 (squid/3.1.23)
HTTP_X_FORWARDED_FOR: 146.52.44.170
HTTP_CACHE_CONTROL: max-age=259200
HTTP_CONNECTION: keep-alive
...
```

Abbildung A.9: VPN: Privatsphäre mit Transparent-Proxy - Server & Network Information[1]

[1] Quelle: http://www.whatsmyip.org/more-info-about-you/ (Abruf: 21.09.2016)

Distorting-Proxy: Browser-Infromationen

Details:

Server 169.50.87.252

Port 80

```
Hostname: fc.57.32a9.ip4.static.sl-reverse.com
Proxy: No Proxy or Invisible Proxy Used
Proxy Type: 1.1 www.dev1.beautifulyou.boots.co.uk
SCRIPT_URL: /more-info-about-you/
SCRIPT_URI: http://www.whatsmyip.org/more-info-about-you/
HTTP_HOST: www.whatsmyip.org
HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:48.0) Gecko
   /20100101 Firefox/48.0
HTTP_ACCEPT: text/html, application/xhtml+xml, application/xml;q
   =0.9, */*;q=0.8
HTTP_ACCEPT_LANGUAGE: de, en-US;q=0.7, en;q=0.3
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_PRAGMA: no-cache
HTTP_CACHE_CONTROL: no-cache
HTTP_VIA: 1.1 www.dev1.beautifulyou.boots.co.uk
HTTP_CONNECTION: Keep-Alive
...
```

Abbildung A.10: VPN: Privatsphäre mit Distorting-Proxy - Server & Network Information[1]

Anonymous-Proxy: Browser-Infromationen

Details:

Server 89.250.207.195

Port 80

[1] Quelle: `http://www.whatsmyip.org/more-info-about-you/` (Abruf: 21.09.2016)

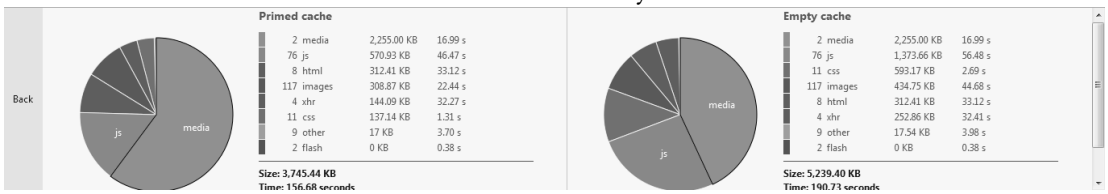
```
Hostname: ip-89-250-207-195.rev.snt.net.pl
Proxy: No Proxy or Invisible Proxy Used
SCRIPT_URL: /more-info-about-you/
SCRIPT_URI: http://www.whatsmyip.org/more-info-about-you/
HTTP_HOST: www.whatsmyip.org
HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:48.0) Gecko
   /20100101 Firefox/48.0
HTTP_ACCEPT: text/html, application/xhtml+xml, application/xml;q
   =0.9, */*;q=0.8
HTTP_ACCEPT_LANGUAGE: de, en-US;q=0.7, en;q=0.3
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_PRAGMA: no-cache
HTTP_CACHE_CONTROL: no-cache
HTTP_CONNECTION: Keep-Alive
...
```

Abbildung A.11: VPN: Privatsphäre mit Anonymous-Proxy - Server & Network Information[1]

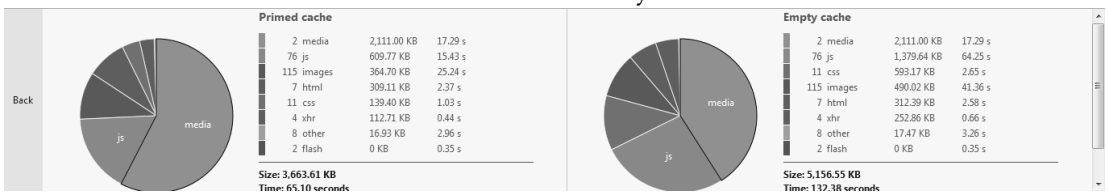
[1] Quelle: `http://www.whatsmyip.org/more-info-about-you/` (Abruf: 21.09.2016)

A.6 Werkzeug: Tor - Messungen

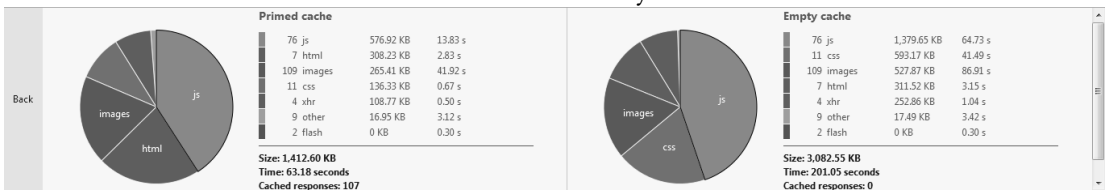
Tor - Netzwerkanalyse: 1.



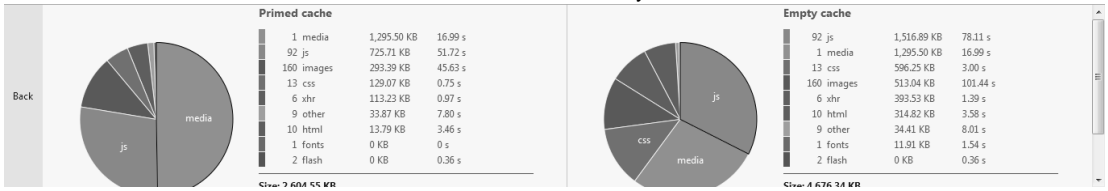
Tor - Netzwerkanalyse: 2.



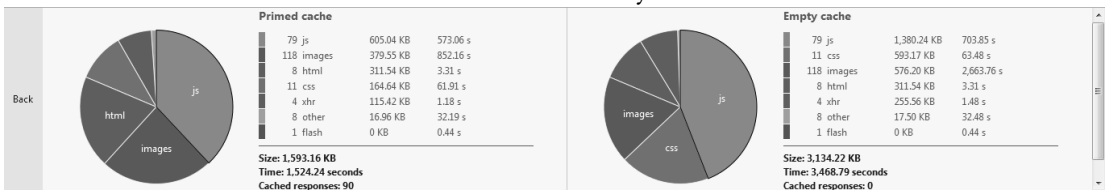
Tor - Netzwerkanalyse: 3.



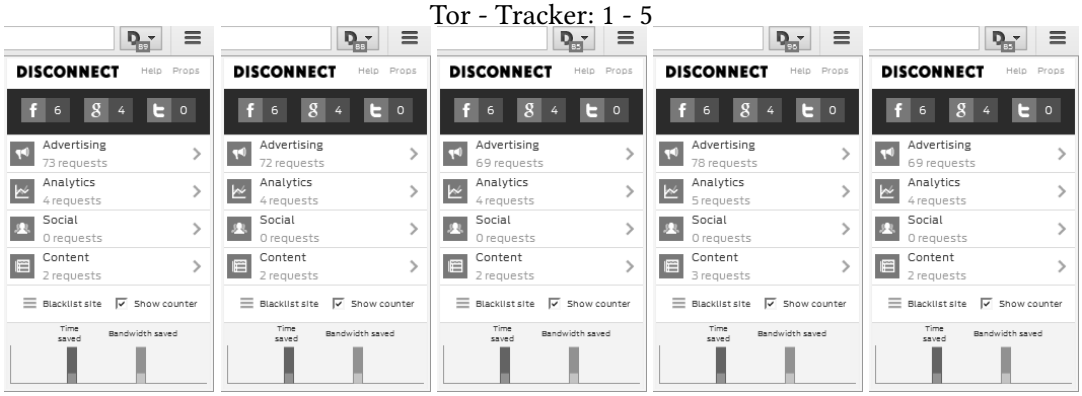
Tor - Netzwerkanalyse: 4.



Tor - Netzwerkanalyse: 5.

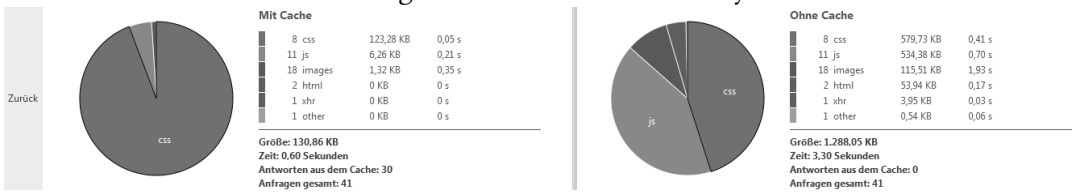


Tor - Tracker: 1 - 5

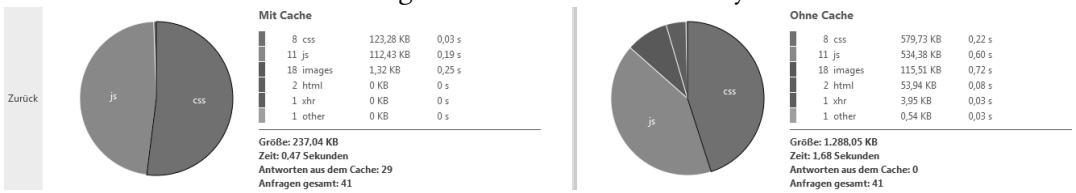


A.7 Einstellung: Tracking Protection - Messungen

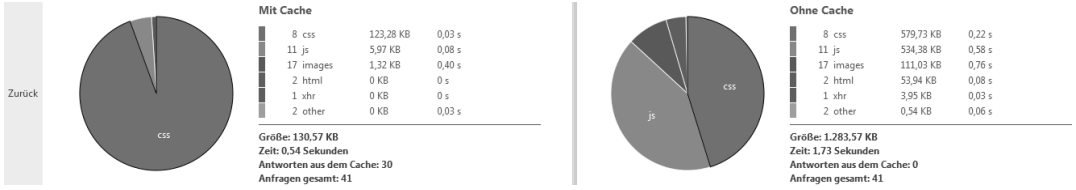
Tracking Protection - Netzwerkanalyse: 1.



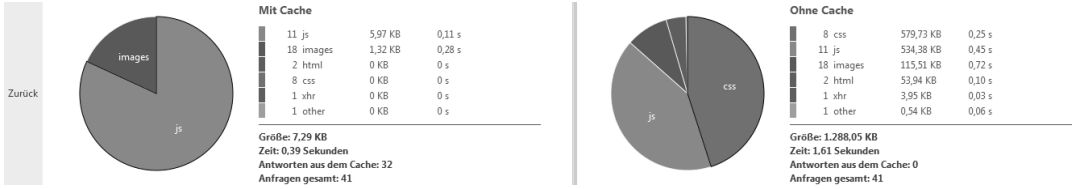
Tracking Protection - Netzwerkanalyse: 2.



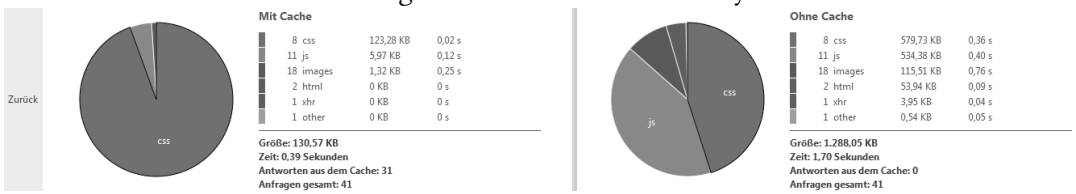
Tracking Protection - Netzwerkanalyse: 3.



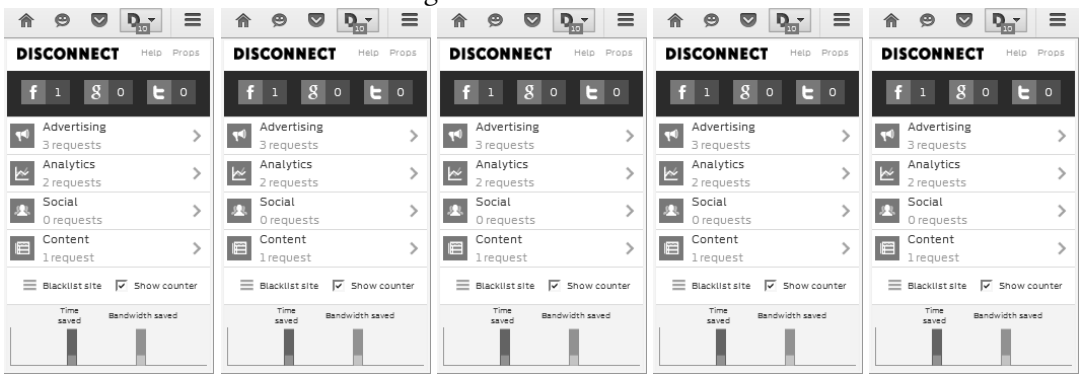
Tracking Protection - Netzwerkanalyse: 4.



Tracking Protection - Netzwerkanalyse: 5.



Tracking Protection - Tracker: 1 - 5



A.8 Einstellung: Datenschutz - Cookies

Für diesen Vergleich wurden zwei HTTP-Archive miteinander verglichen. Die HTTP-Archive wurden mit dem Entwickler-Werkzeug *Netzwerkanalyse* erzeugt. Es beinhaltet alle Ergebnisse einer Netzwerkanalyse.

Ausschnitt des Vergleichs (links Standardeinstellung und rechts angepasste Einstellungen)

HAR parser

What is this?

"HAR": ".har is a common filename extension denoting an HTTP Archive file. It is a JSON-formatted file that contain a trace of a Web browsers interaction with a given site." — Source: Wikipedia: .har

This tool allows you to find out what your blocker is **NOT** blocking. There are two panes, which allows you to easily compare two result sets – useful to compare two blockers, or same blocker with different settings, or a web page with and without a blocker, etc.

Important: be sure you factor out your browser cache by forcing a full reload of the page which you want to analyze. Usually a full reload can be forced by `Shift`-clicking on your browser's *Reload* button.

Note that HAR content can be quite large sometimes, and when pasting this content into a `textarea`, your browser may end up "seizing" -- this is not caused by the parser itself.

Results

	Paste here clipboard content after clicking "Copy All as HAR" in Network pane			Paste here clipboard content after clicking "Copy All as HAR" in Network pane		
URL:	http://www.bild.de/			http://www.bild.de/		
Load:	0 ms			0 ms		
Distinct hostnames:	110			56		
Hostnames	**cookies s...**	**javascript**	**bandwidth**	**cookies s...**	**javascript**	**bandwidth**
	208	81	1.554.576	53	86	2.459.444

Erzeugt mit: `http://raymondhill.net/httpsb/har-parser.html`

A.9 Erweiterung: Decentraleyes - Messungen

Die Testseite, mit der die Messungen erzeugt wurden, für Decentraleyes war: `https://decentraleyes.org/test/`

ohne Decentraleyes - Netzwerkanalyse: 1.

ohne Decentraleyes - Netzwerkanalyse: 2.

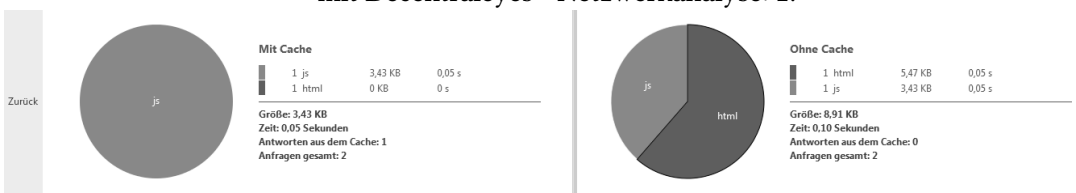
ohne Decentraleyes - Netzwerkanalyse: 3.

ohne Decentraleyes - Netzwerkanalyse: 4.

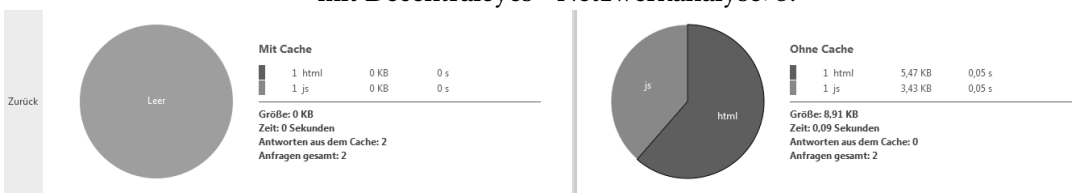
ohne Decentraleyes - Netzwerkanalyse: 5.

mit Decentraleyes - Netzwerkanalyse: 1.

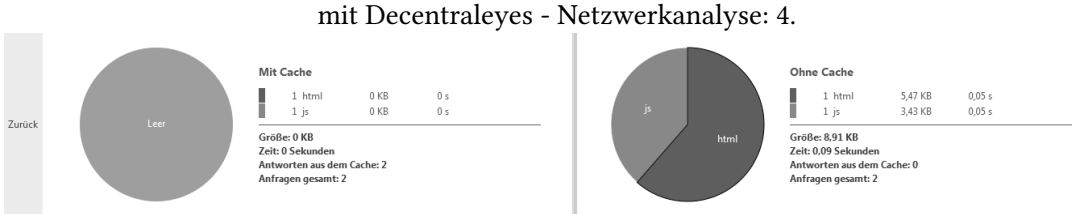
mit Decentraleyes - Netzwerkanalyse: 2.



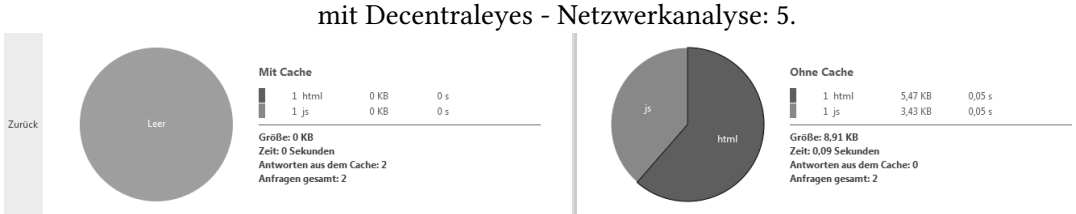
mit Decentraleyes - Netzwerkanalyse: 3.



mit Decentraleyes - Netzwerkanalyse: 4.



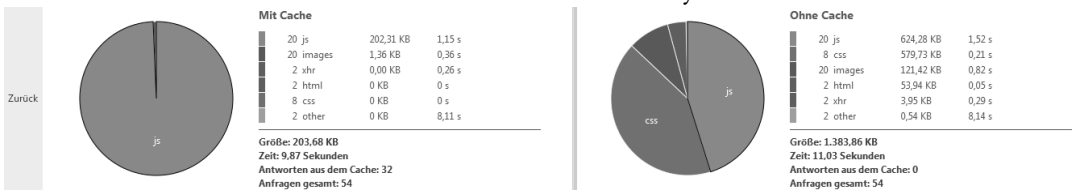
mit Decentraleyes - Netzwerkanalyse: 5.



A.10 Erweiterung: Disconnect - Messungen

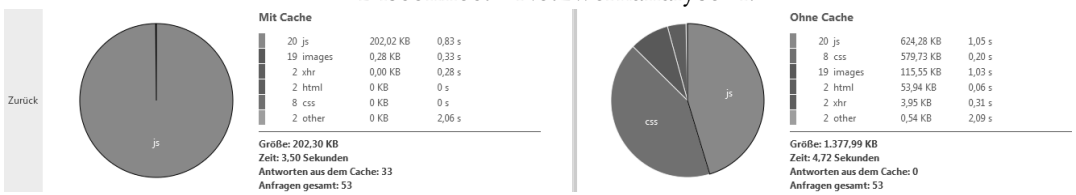
Disconnect - Netzwerkanalyse: 1.

Disconnect - Netzwerkanalyse: 2.

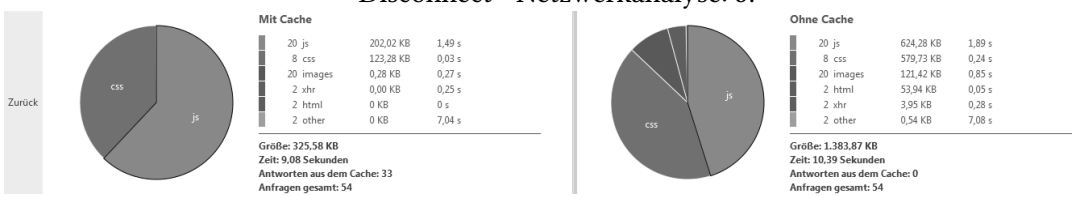


Disconnect - Netzwerkanalyse: 3.

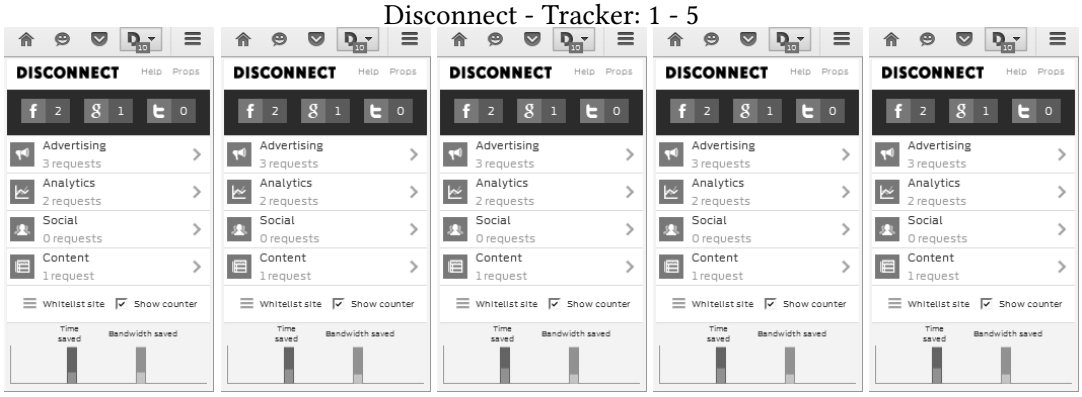
Disconnect - Netzwerkanalyse: 4.



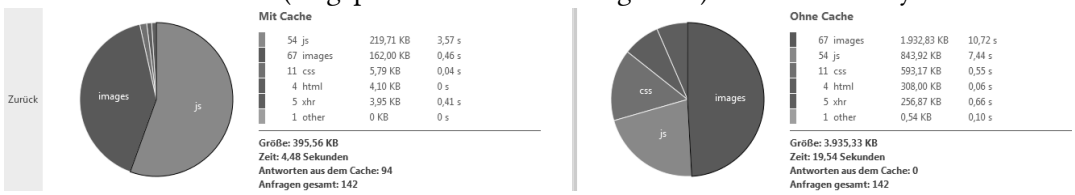
Disconnect - Netzwerkanalyse: 5.



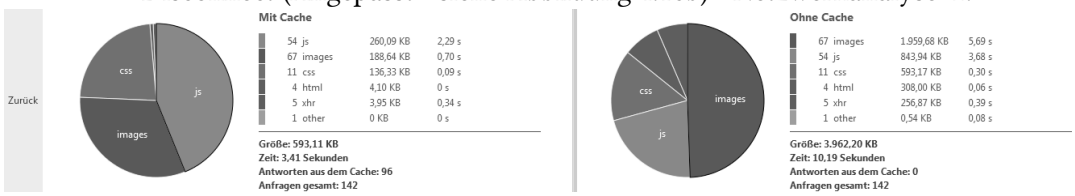
Disconnect - Tracker: 1 - 5



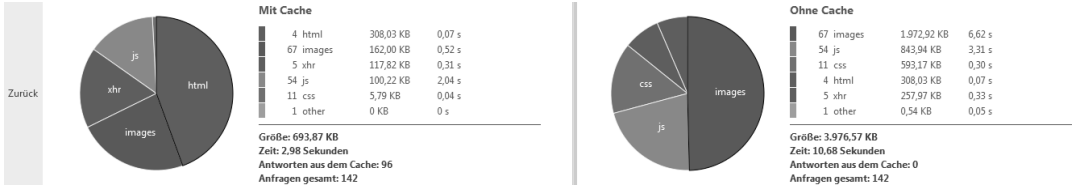
Disconnect (Angepasst - siehe Abbildung 4.16b) - Netzwerkanalyse: 1.



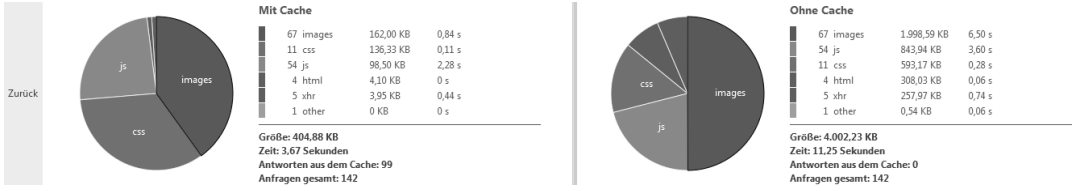
Disconnect (Angepasst - siehe Abbildung 4.16b) - Netzwerkanalyse: 2.



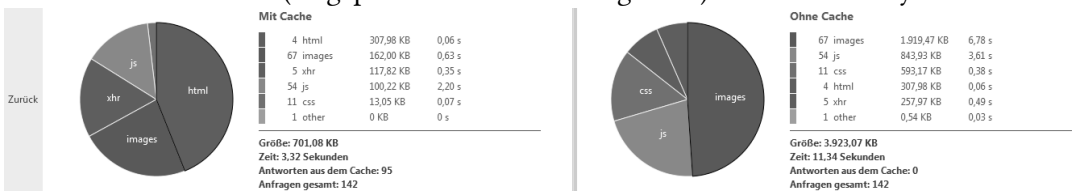
Disconnect (Angepasst - siehe Abbildung 4.16b) - Netzwerkanalyse: 3.



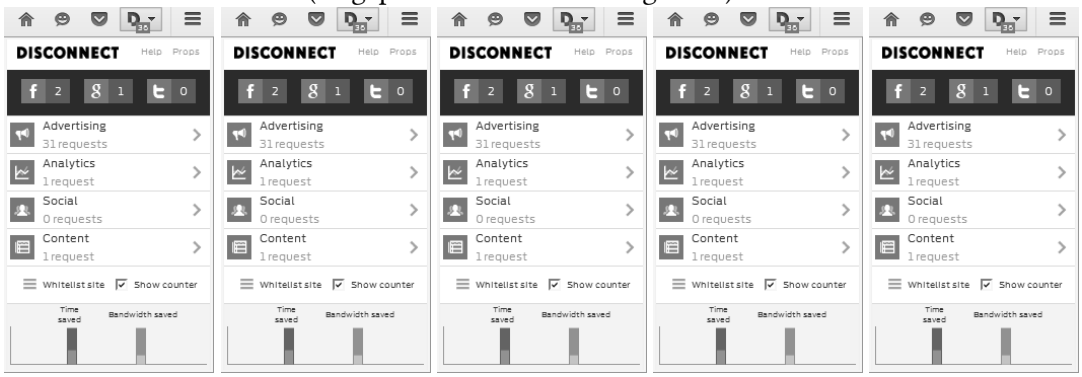
Disconnect (Angepasst - siehe Abbildung 4.16b) - Netzwerkanalyse: 4.



Disconnect (Angepasst - siehe Abbildung 4.16b) - Netzwerkanalyse: 5.



Disconnect (Angepasst - siehe Abbildung 4.16b) - Tracker: 1 - 5



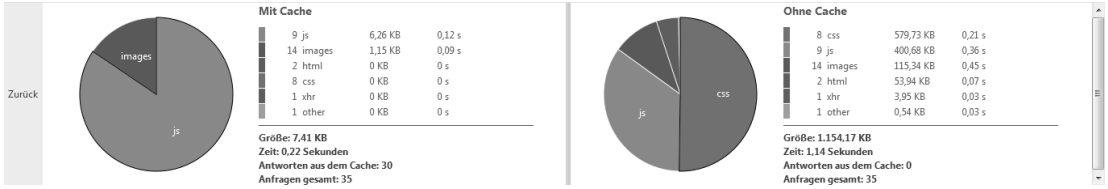
A.11 Erweiterung: Ghostery - Messungen

Ghostery - Netzwerkanalyse: 1.

Ghostery - Netzwerkanalyse: 2.

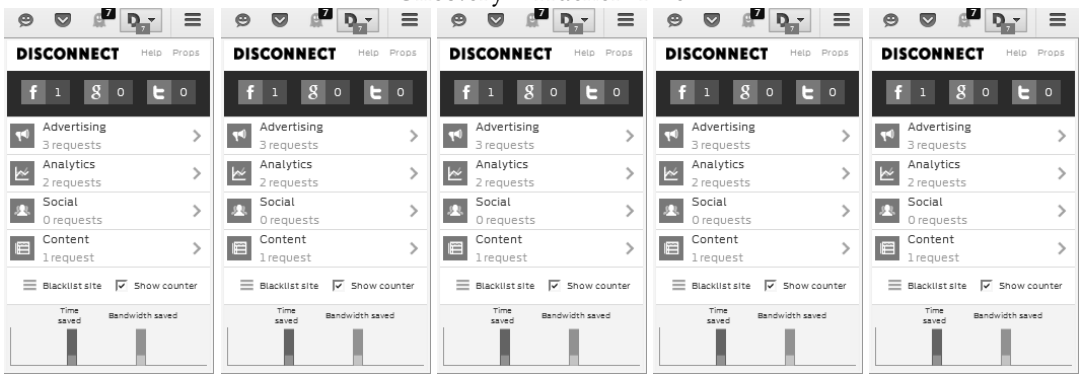
Ghostery - Netzwerkanalyse: 3.

Ghostery - Netzwerkanalyse: 4.



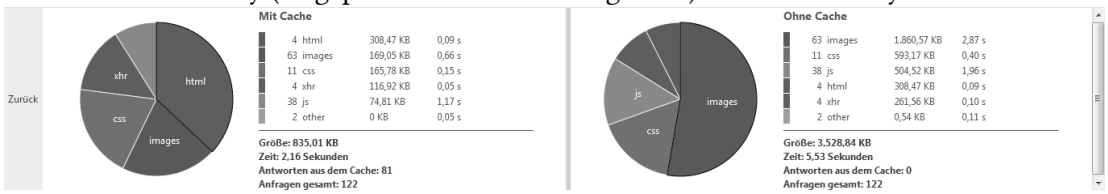
Ghostery - Netzwerkanalyse: 5.

Ghostery - Tracker: 1 - 5



Ghostery (Angepasst - siehe Abbildung 4.17b) - Netzwerkanalyse: 1.

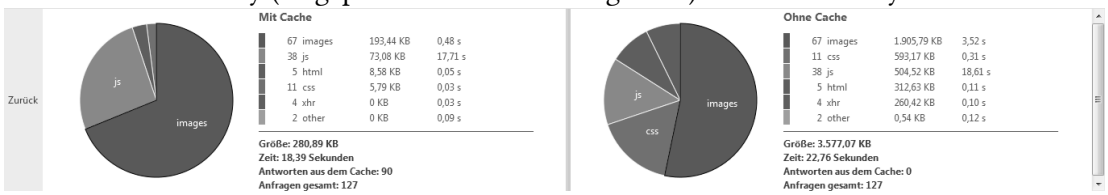
Ghostery (Angepasst - siehe Abbildung 4.17b) - Netzwerkanalyse: 2.



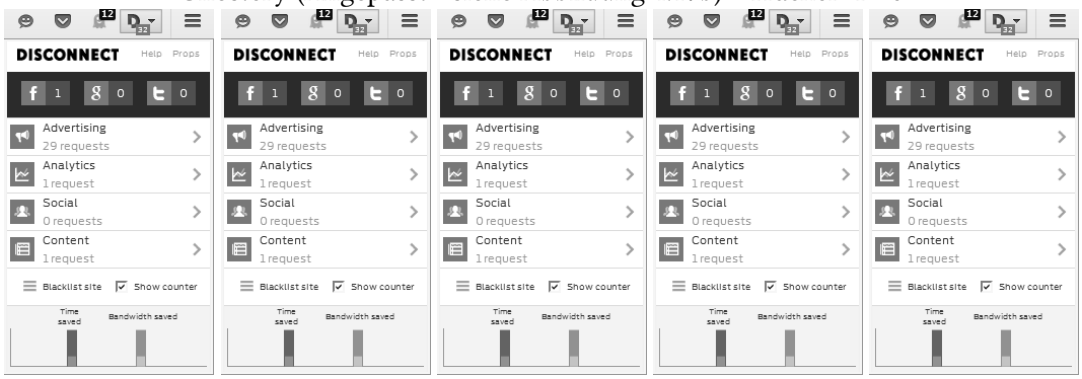
Ghostery (Angepasst - siehe Abbildung 4.17b) - Netzwerkanalyse: 3.

Ghostery (Angepasst - siehe Abbildung 4.17b) - Netzwerkanalyse: 4.

Ghostery (Angepasst - siehe Abbildung 4.17b) - Netzwerkanalyse: 5.



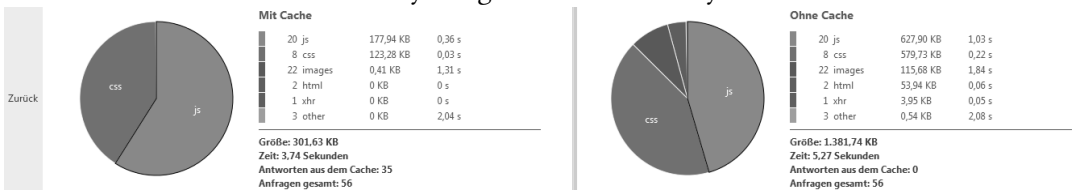
Ghostery (Angepasst - siehe Abbildung 4.17b) - Tracker: 1 - 5



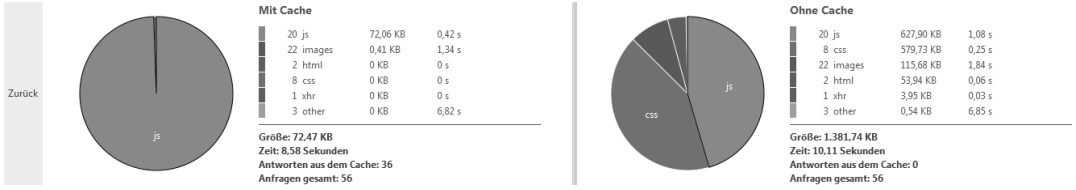
A.12 Erweiterung: Privacy Badger - Messungen

Privacy Badger - Netzwerkanalyse: 1.

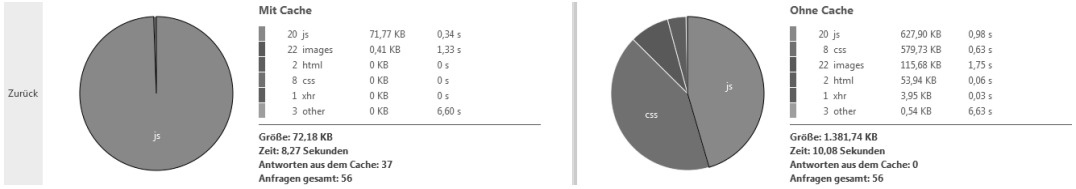
Privacy Badger - Netzwerkanalyse: 2.



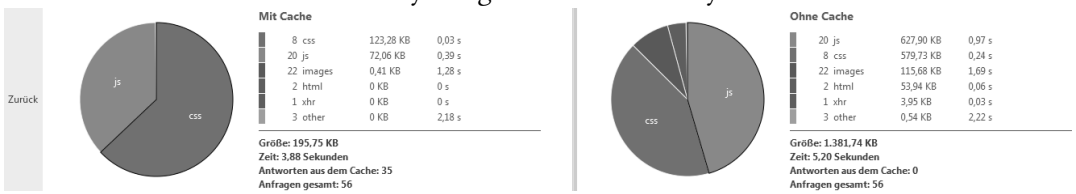
Privacy Badger - Netzwerkanalyse: 3.



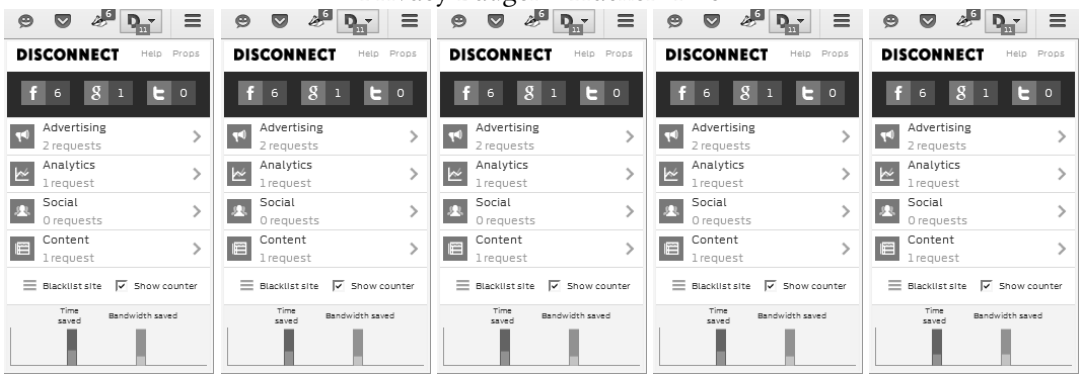
Privacy Badger - Netzwerkanalyse: 4.



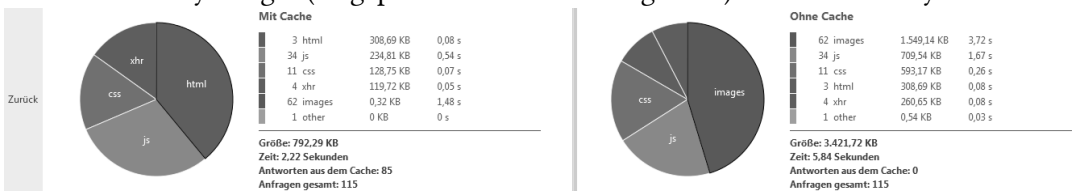
Privacy Badger - Netzwerkanalyse: 5.



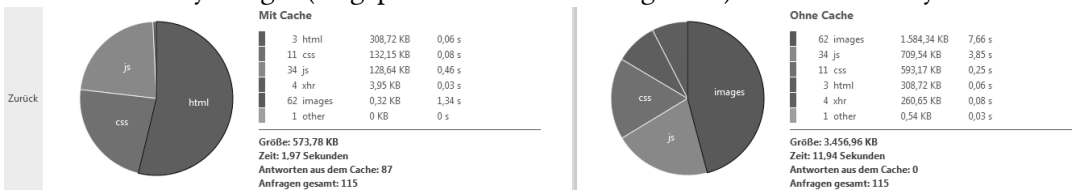
Privacy Badger - Tracker: 1 - 5



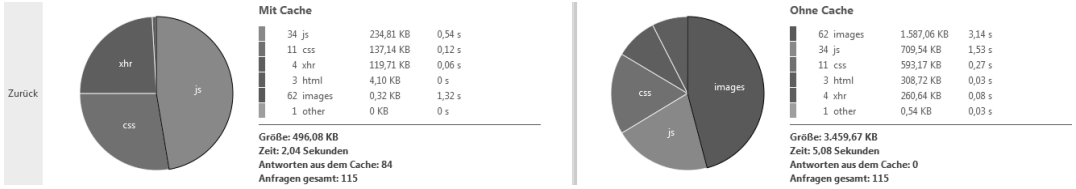
Privacy Badger (Angepasst - siehe Abbildung 4.19b) - Netzwerkanalyse: 1.



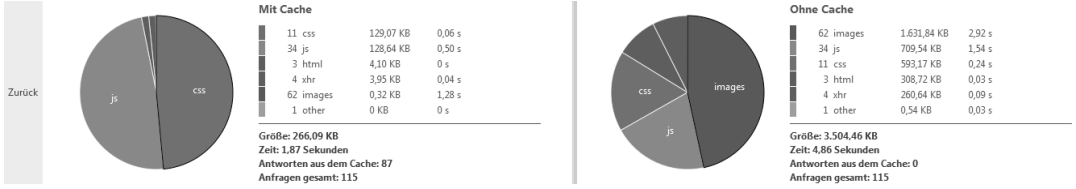
Privacy Badger (Angepasst - siehe Abbildung 4.19b) - Netzwerkanalyse: 2.



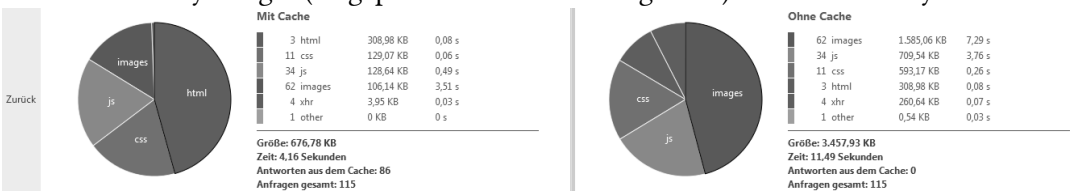
Privacy Badger (Angepasst - siehe Abbildung 4.19b) - Netzwerkanalyse: 3.



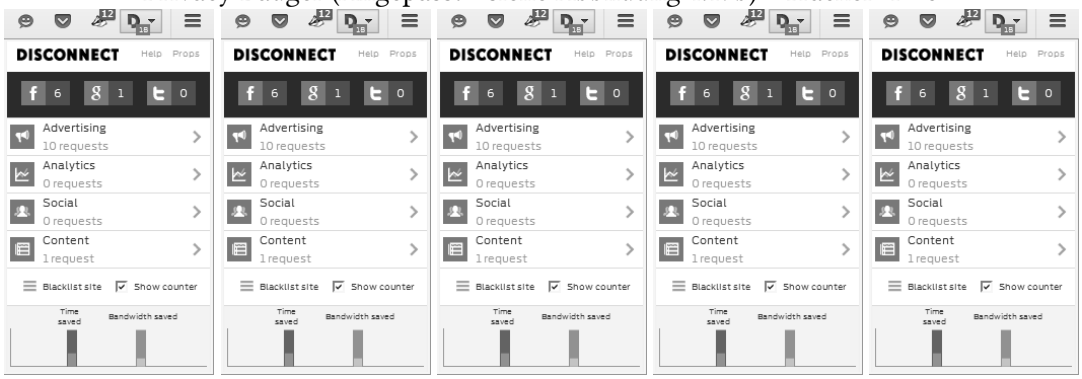
Privacy Badger (Angepasst - siehe Abbildung 4.19b) - Netzwerkanalyse: 4.



Privacy Badger (Angepasst - siehe Abbildung 4.19b) - Netzwerkanalyse: 5.



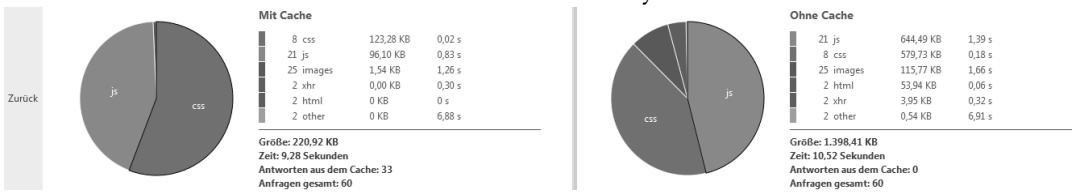
Privacy Badger (Angepasst - siehe Abbildung 4.19b) - Tracker: 1 - 5



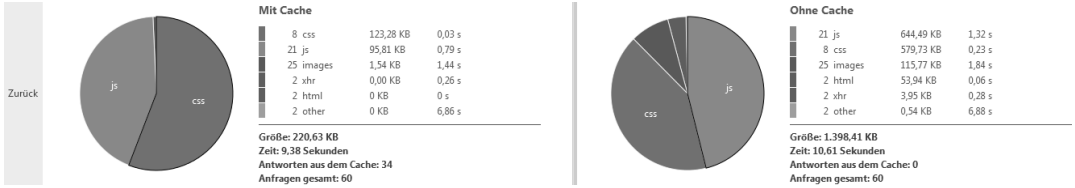
A.13 Erweiterung: ABP - Messungen

ABP - Netzwerkanalyse: 1.

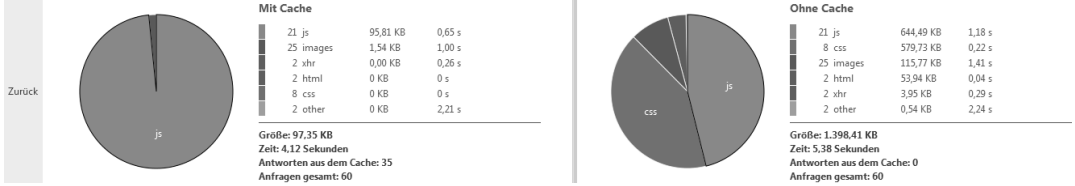
ABP - Netzwerkanalyse: 2.



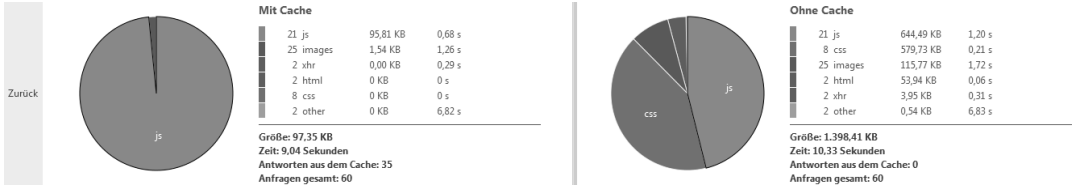
ABP - Netzwerkanalyse: 3.



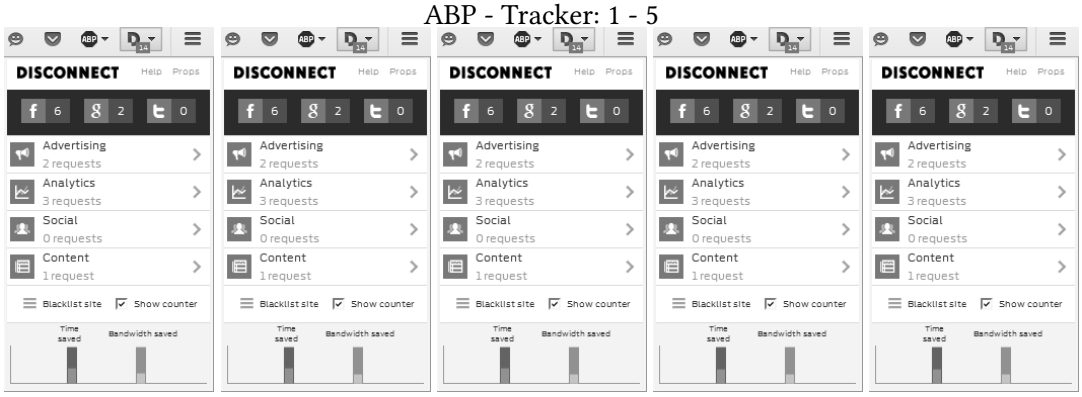
ABP - Netzwerkanalyse: 4.



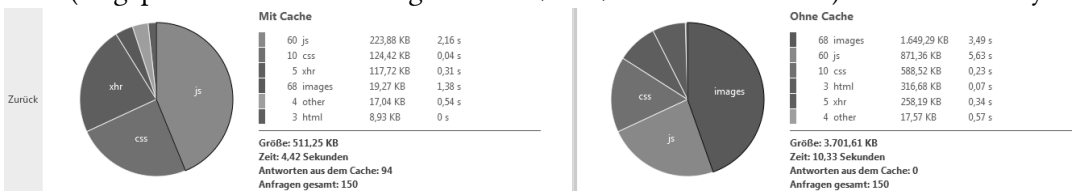
ABP - Netzwerkanalyse: 5.



ABP - Tracker: 1 - 5

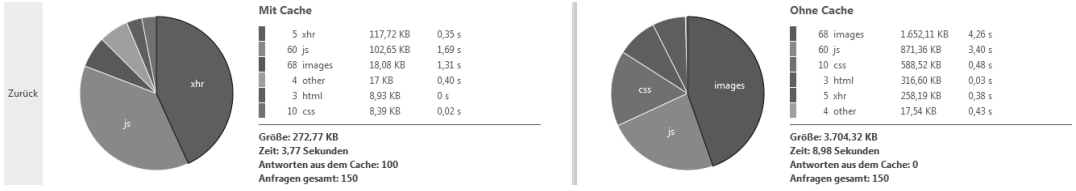


ABP (Angepasst - siehe Webseite github.com/reek/anti-adblock-killer) - Netzwerkanalyse: 1.

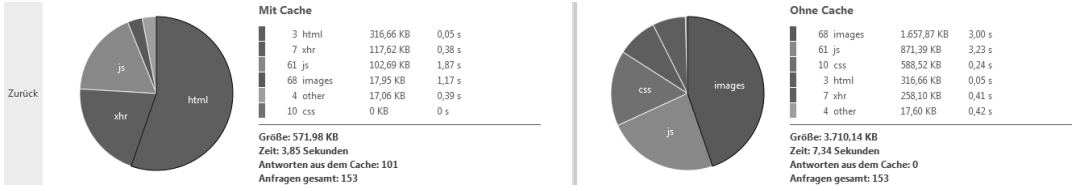


ABP (Angepasst - siehe Webseite github.com/reek/anti-adblock-killer) - Netzwerkanalyse: 2.

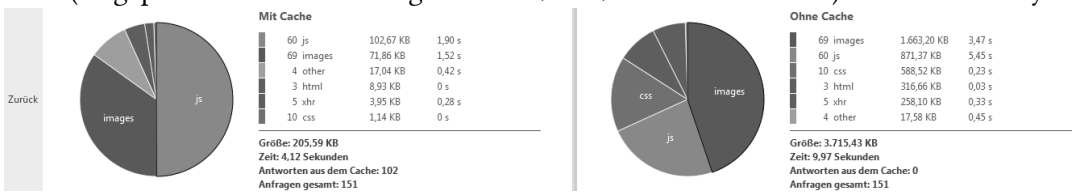
ABP (Angepasst - siehe Webseite github.com/reek/anti-adblock-killer) - Netzwerkanalyse: 3.



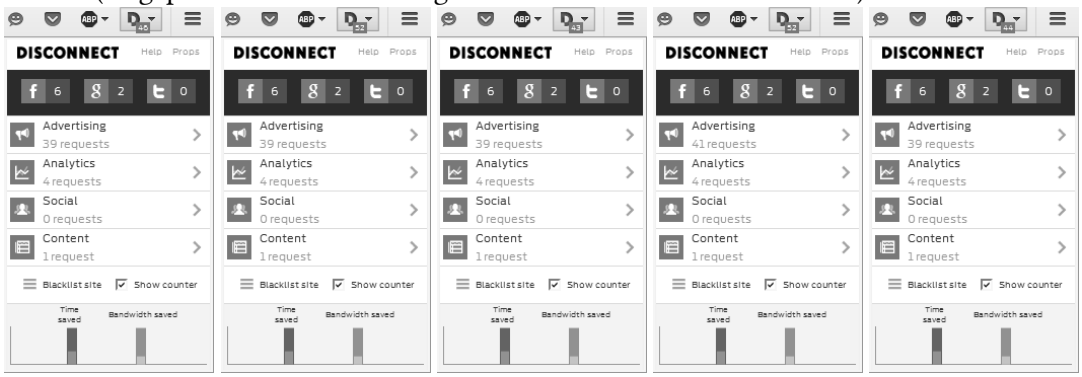
ABP (Angepasst - siehe Webseite github.com/reek/anti-adblock-killer) - Netzwerkanalyse: 4.



ABP (Angepasst - siehe Webseite github.com/reek/anti-adblock-killer) - Netzwerkanalyse: 5.

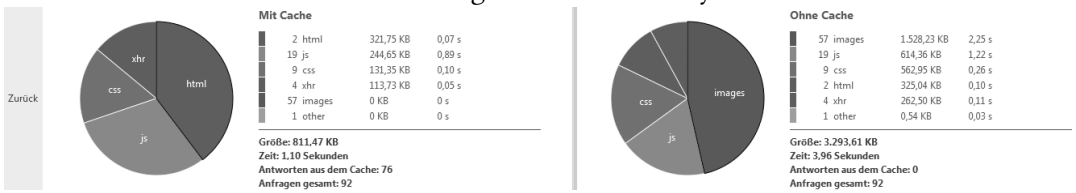


ABP (Angepasst - siehe Webseite github.com/reek/anti-adblock-killer) - Tracker: 1 - 5

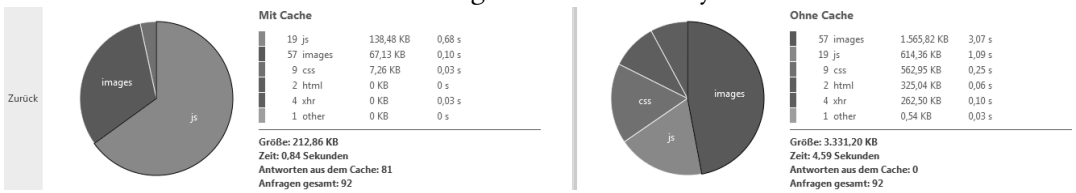


A.14 Erweiterung: uBlock Origin - Messungen

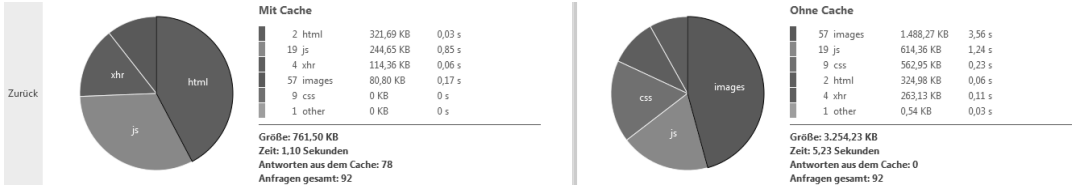
uBlock Origin - Netzwerkanalyse: 1.



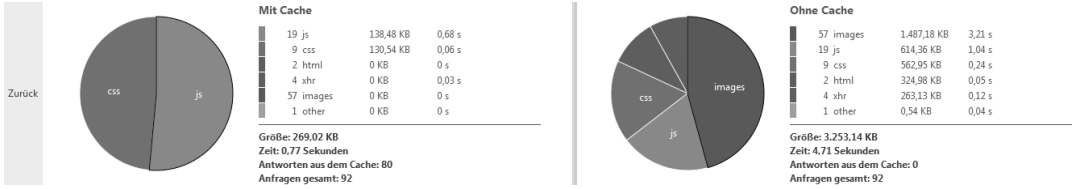
uBlock Origin - Netzwerkanalyse: 2.



uBlock Origin - Netzwerkanalyse: 3.

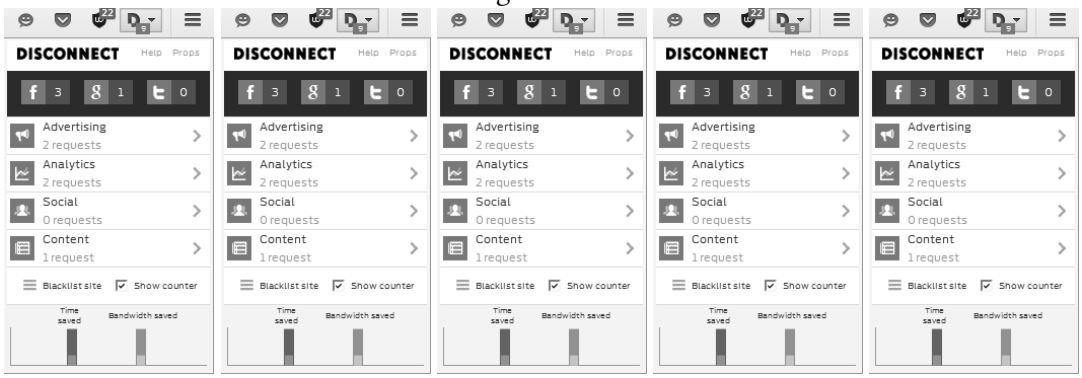


uBlock Origin - Netzwerkanalyse: 4.



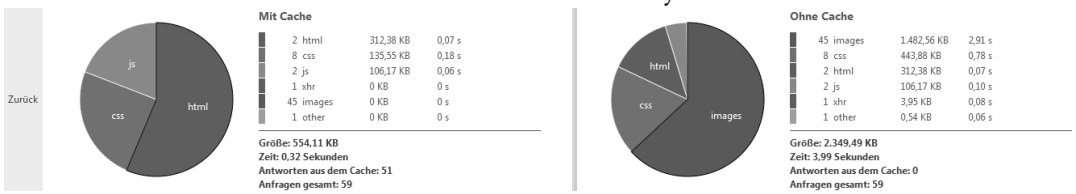
uBlock Origin - Netzwerkanalyse: 5.

uBlock Origin - Tracker: 1 - 5

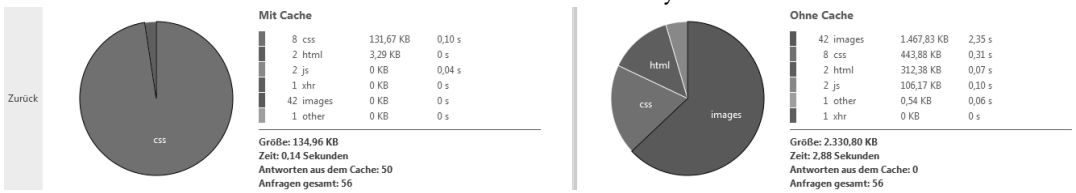


A.15 Erweiterung: uMatrix - Messungen

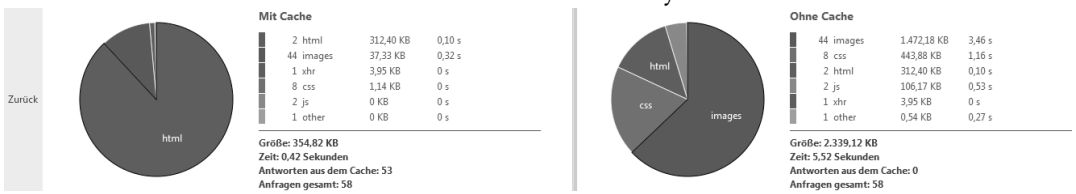
uMatrix - Netzwerkanalyse: 1.



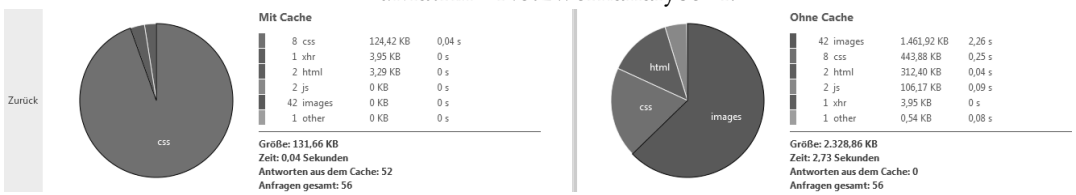
uMatrix - Netzwerkanalyse: 2.



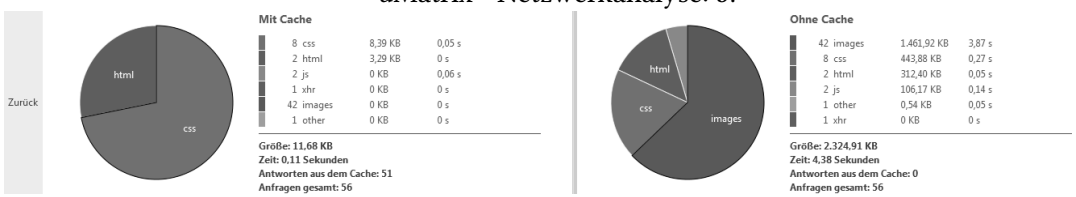
uMatrix - Netzwerkanalyse: 3.



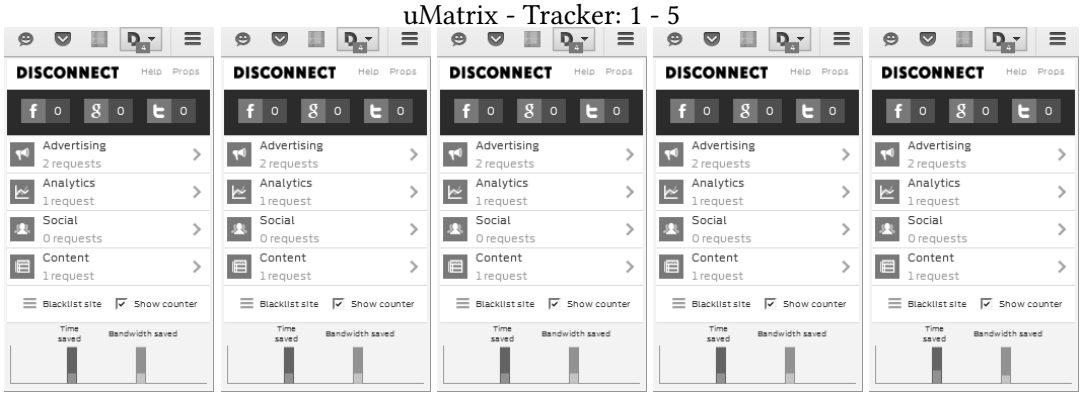
uMatrix - Netzwerkanalyse: 4.



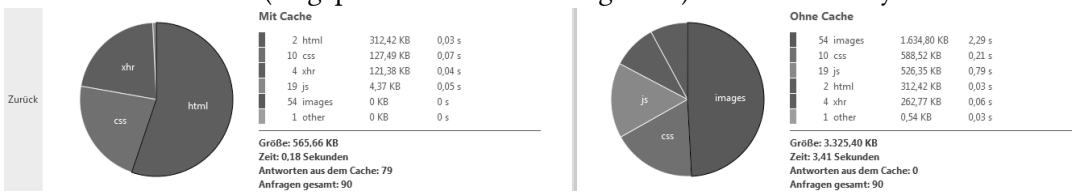
uMatrix - Netzwerkanalyse: 5.



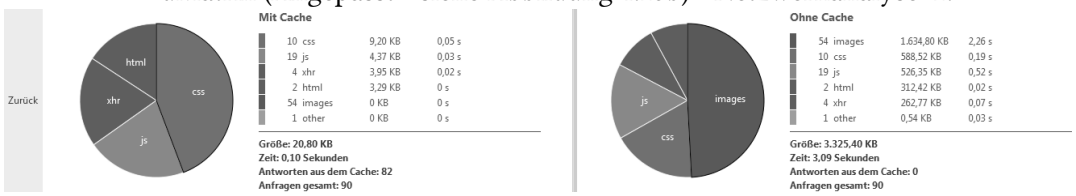
uMatrix - Tracker: 1 - 5



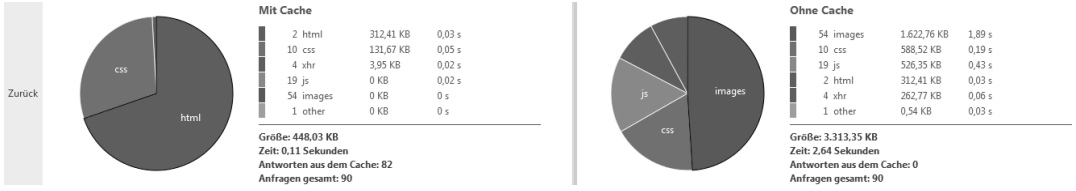
uMatrix (Angepasst - siehe Abbildung 4.23b) - Netzwerkanalyse: 1.



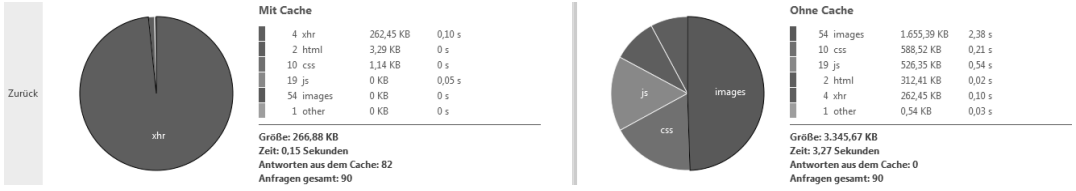
uMatrix (Angepasst - siehe Abbildung 4.23b) - Netzwerkanalyse: 2.



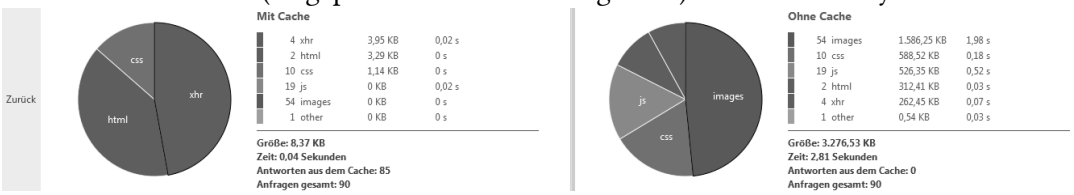
uMatrix (Angepasst - siehe Abbildung 4.23b) - Netzwerkanalyse: 3.



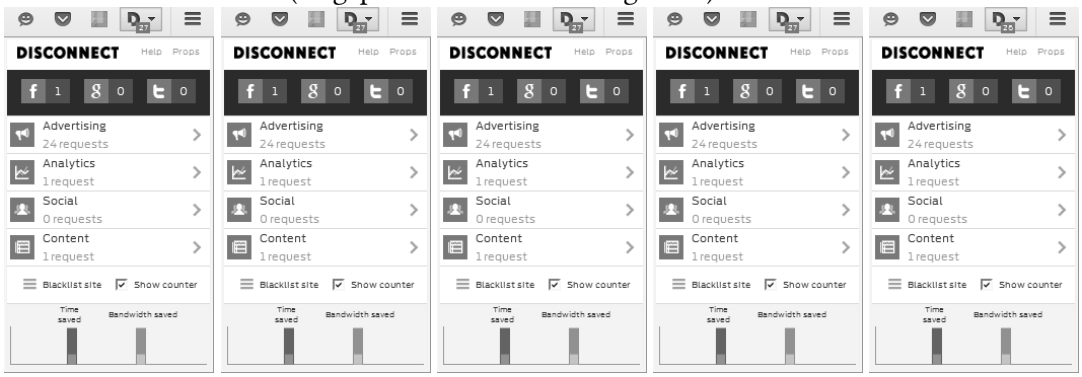
uMatrix (Angepasst - siehe Abbildung 4.23b) - Netzwerkanalyse: 4.



uMatrix (Angepasst - siehe Abbildung 4.23b) - Netzwerkanalyse: 5.

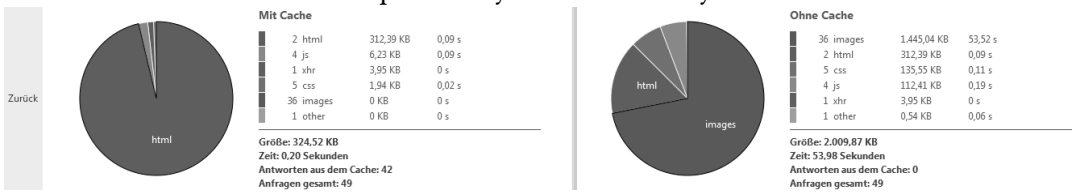


uMatrix (Angepasst - siehe Abbildung 4.23b) - Tracker: 1 - 5

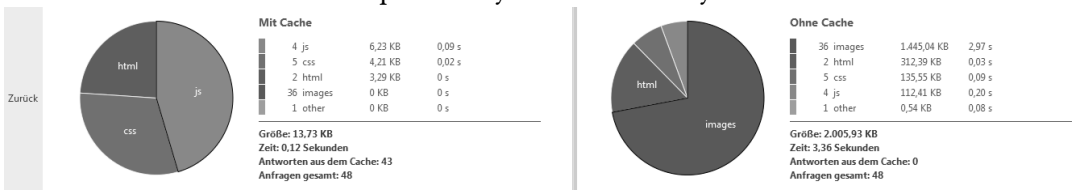


A.16 Erweiterung: RequestPolicy - Messungen

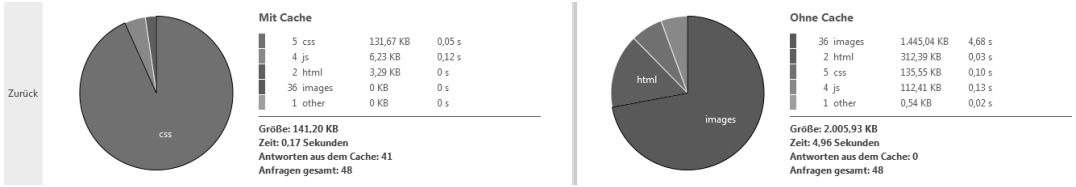
RequestPolicy - Netzwerkanalyse: 1.



RequestPolicy - Netzwerkanalyse: 2.

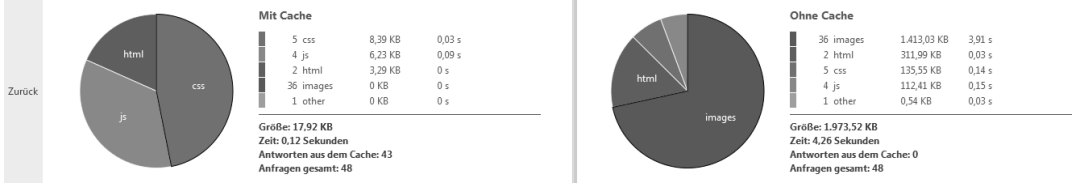


RequestPolicy - Netzwerkanalyse: 3.

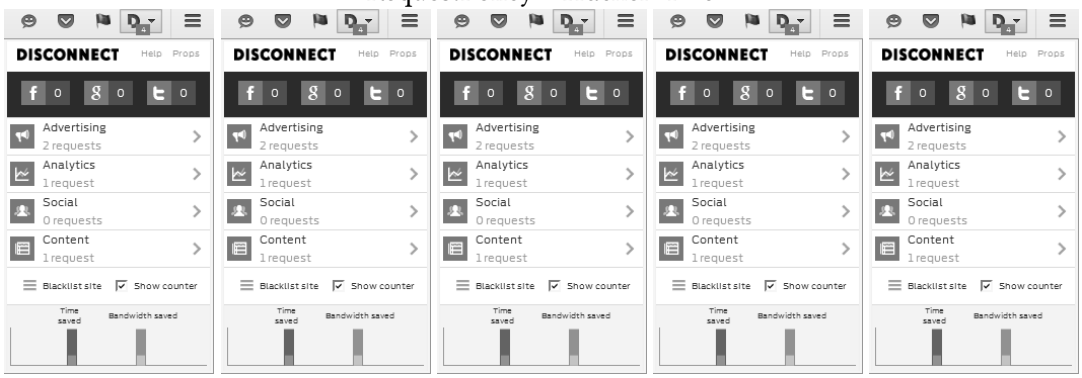


RequestPolicy - Netzwerkanalyse: 4.

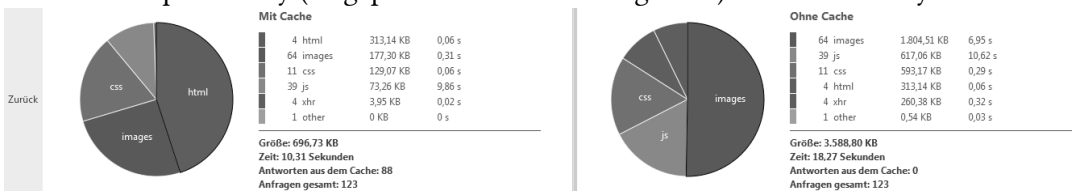
RequestPolicy - Netzwerkanalyse: 5.



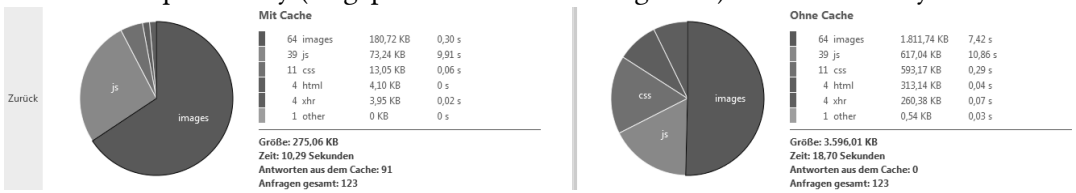
RequestPolicy - Tracker: 1 - 5



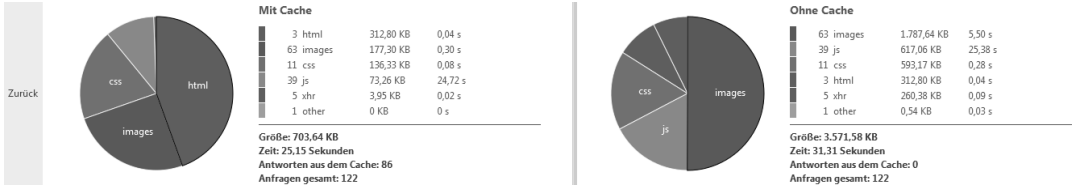
RequestPolicy (Angepasst - siehe Abbildung 4.24b) - Netzwerkanalyse: 1.



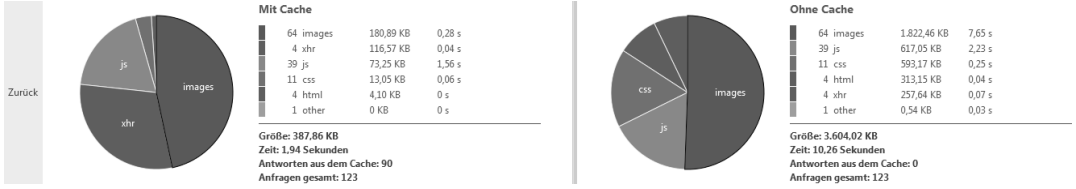
RequestPolicy (Angepasst - siehe Abbildung 4.24b) - Netzwerkanalyse: 2.



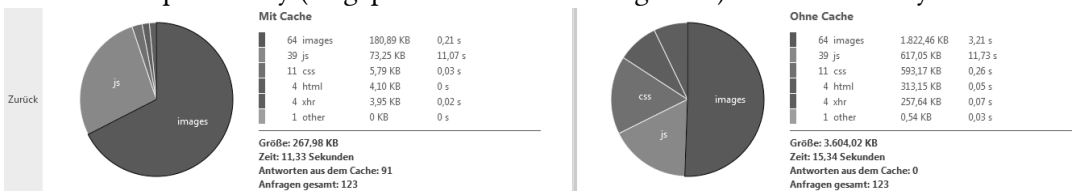
RequestPolicy (Angepasst - siehe Abbildung 4.24b) - Netzwerkanalyse: 3.



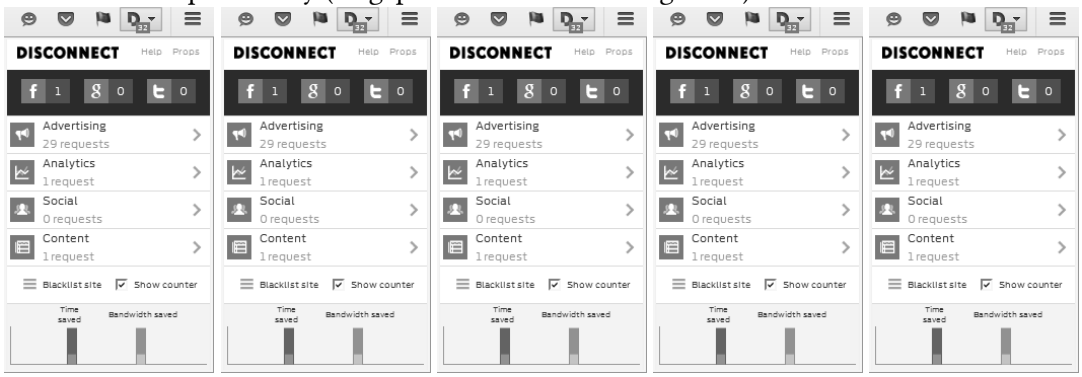
RequestPolicy (Angepasst - siehe Abbildung 4.24b) - Netzwerkanalyse: 4.



RequestPolicy (Angepasst - siehe Abbildung 4.24b) - Netzwerkanalyse: 5.

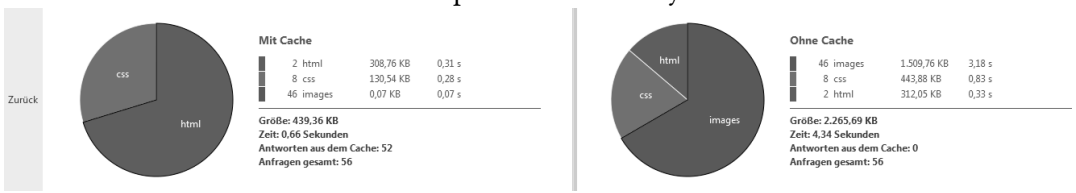


RequestPolicy (Angepasst - siehe Abbildung 4.24b) - Tracker: 1 - 5

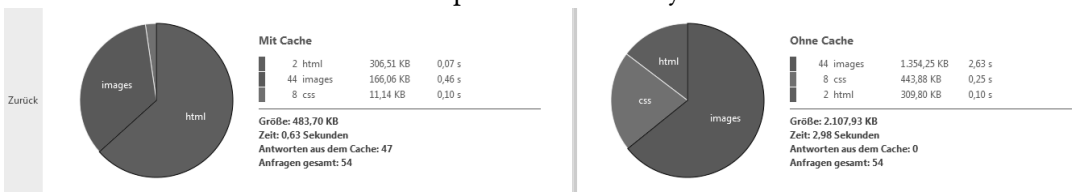


A.17 Erweiterung: NoScript - Messungen

NoScript - Netzwerkanalyse: 1.

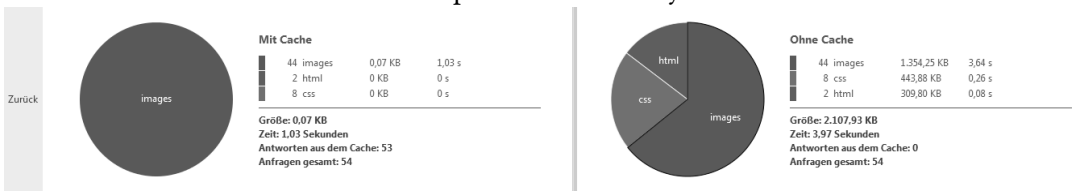


NoScript - Netzwerkanalyse: 2.

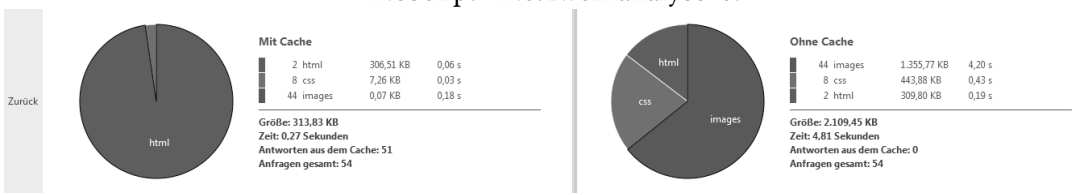


NoScript - Netzwerkanalyse: 3.

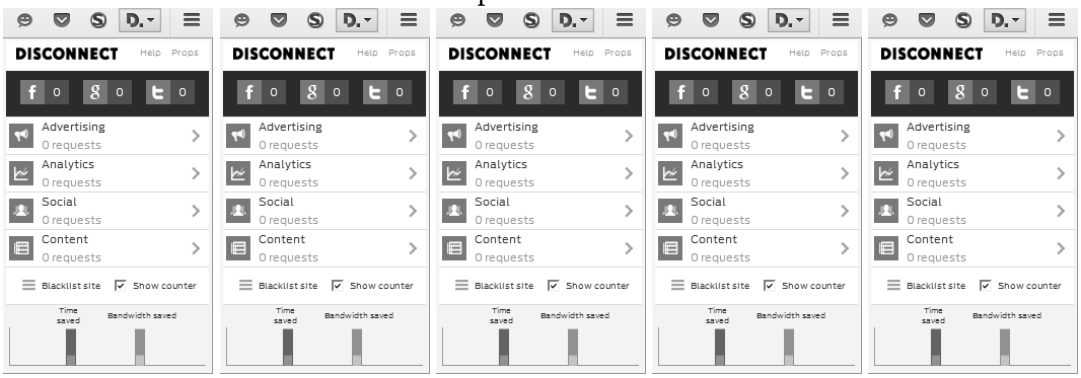
NoScript - Netzwerkanalyse: 4.



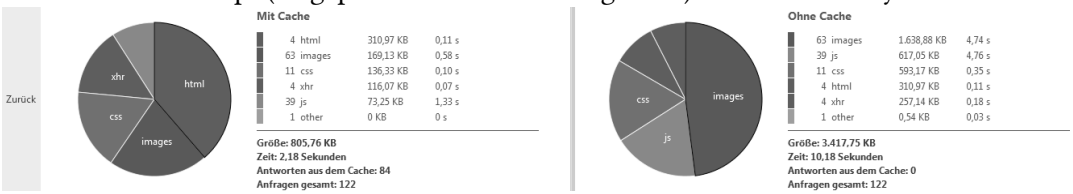
NoScript - Netzwerkanalyse: 5.



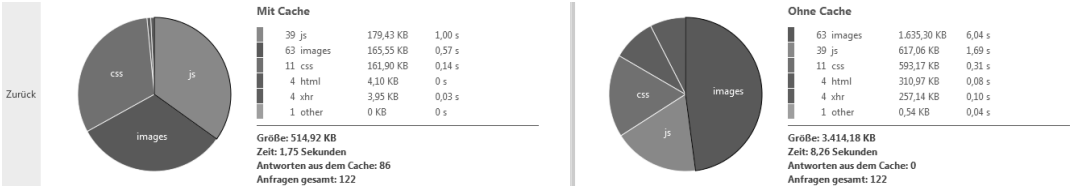
NoScript - Tracker: 1 - 5



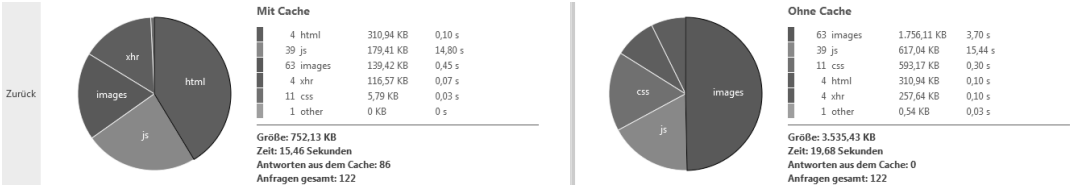
NoScript (Angepasst - siehe Abbildung 4.25b) - Netzwerkanalyse: 1.



NoScript (Angepasst - siehe Abbildung 4.25b) - Netzwerkanalyse: 2.

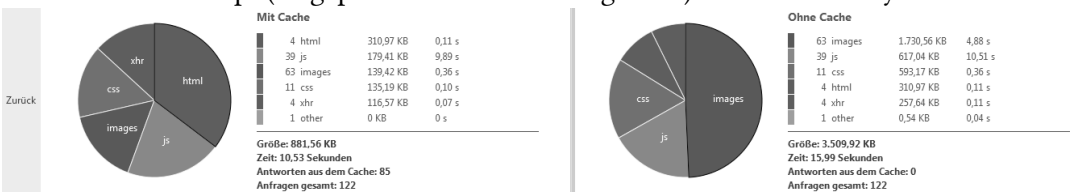


NoScript (Angepasst - siehe Abbildung 4.25b) - Netzwerkanalyse: 3.

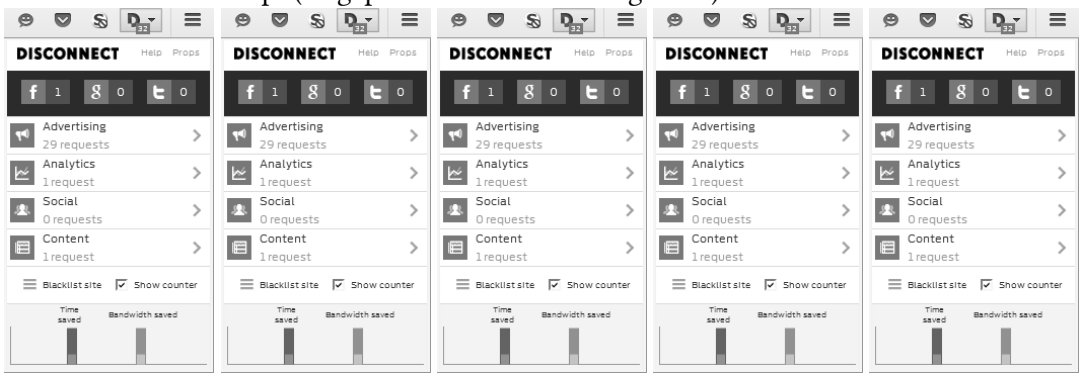


NoScript (Angepasst - siehe Abbildung 4.25b) - Netzwerkanalyse: 4.

NoScript (Angepasst - siehe Abbildung 4.25b) - Netzwerkanalyse: 5.

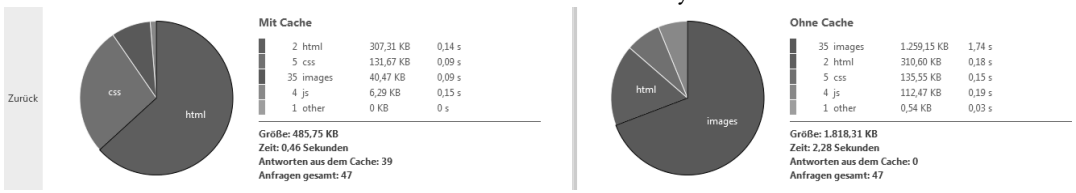


NoScript (Angepasst - siehe Abbildung 4.25b) - Tracker: 1 - 5

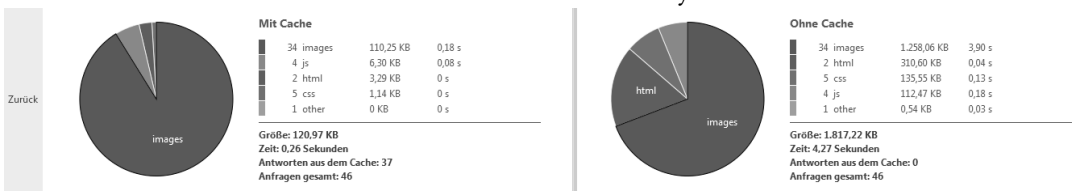


A.18 Erweiterung: Policeman - Messungen

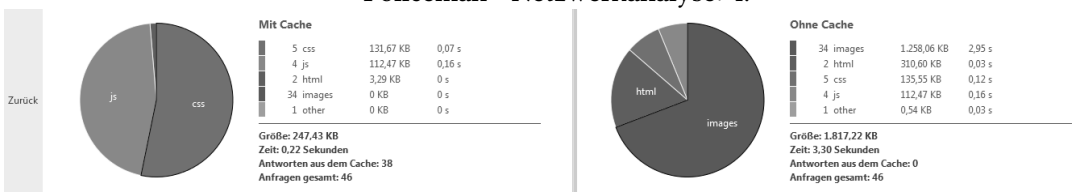
Policeman - Netzwerkanalyse: 2.



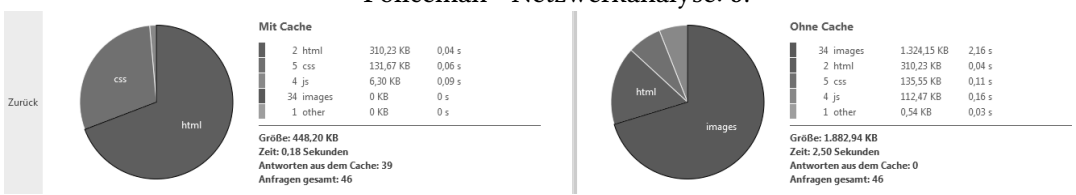
Policeman - Netzwerkanalyse: 3.



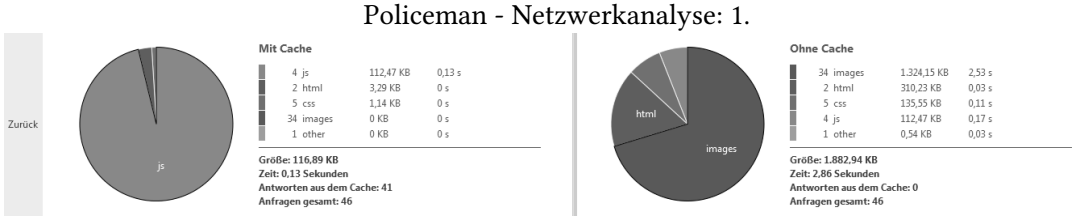
Policeman - Netzwerkanalyse: 4.



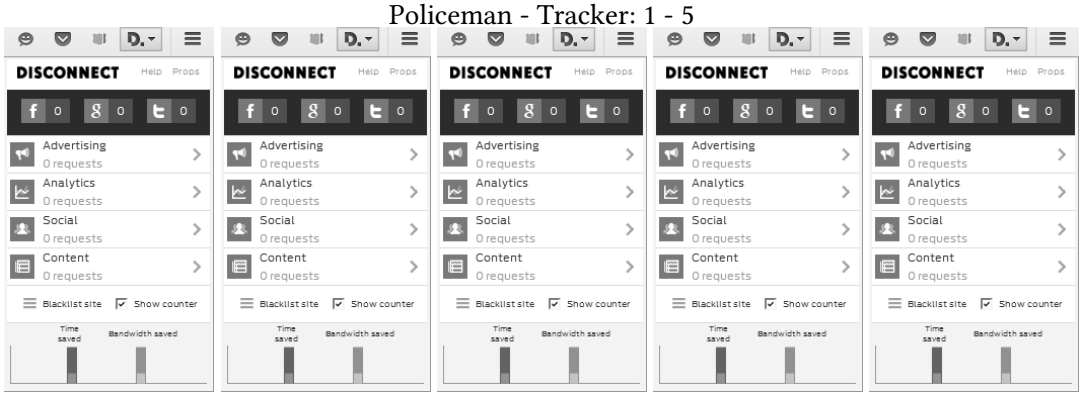
Policeman - Netzwerkanalyse: 5.



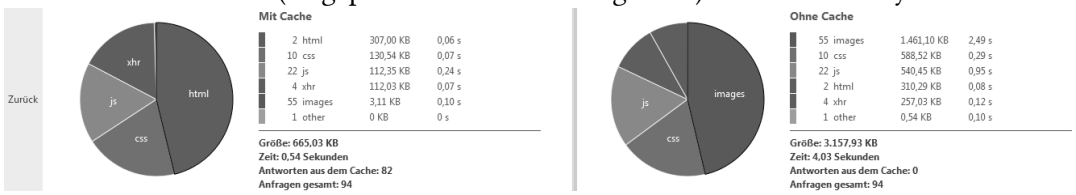
Policeman - Netzwerkanalyse: 1.



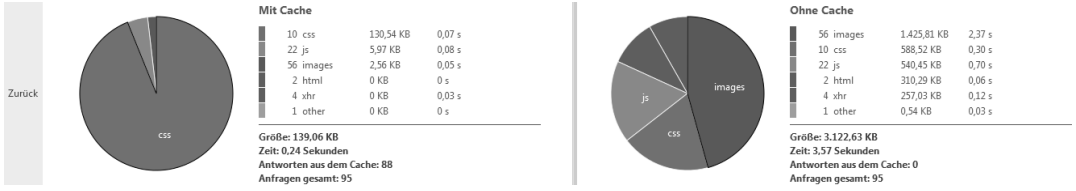
Policeman - Tracker: 1 - 5



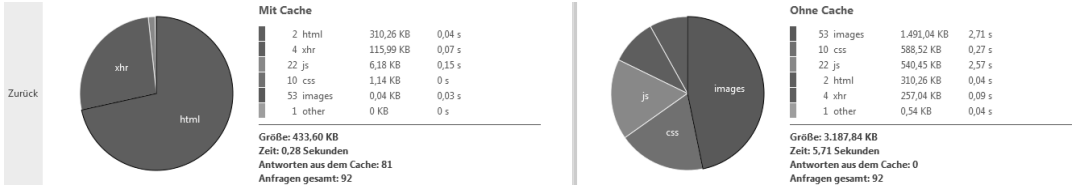
Policeman (Angepasst - siehe Abbildung 4.26b) - Netzwerkanalyse: 1.



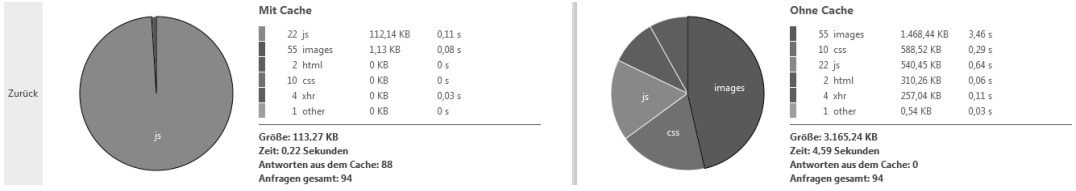
Policeman (Angepasst - siehe Abbildung 4.26b) - Netzwerkanalyse: 2.



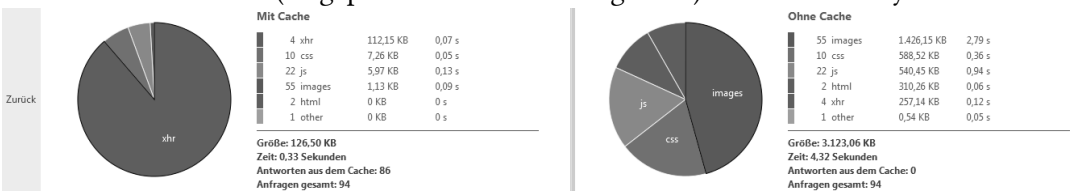
Policeman (Angepasst - siehe Abbildung 4.26b) - Netzwerkanalyse: 3.



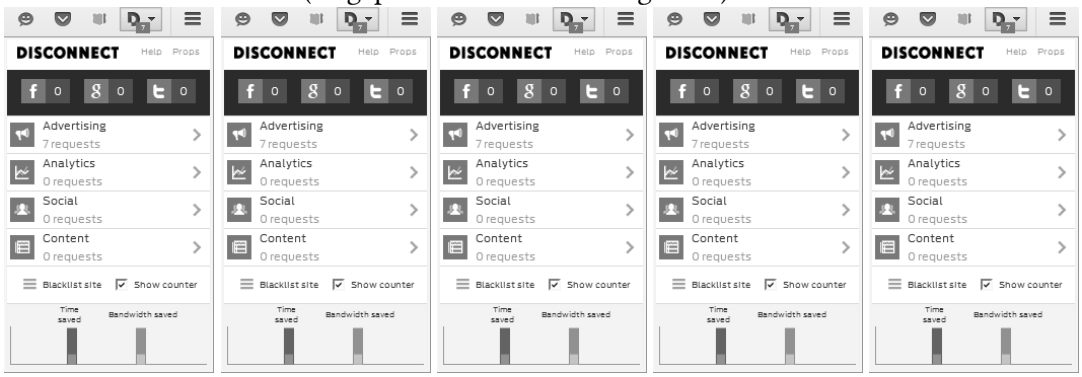
Policeman (Angepasst - siehe Abbildung 4.26b) - Netzwerkanalyse: 4.



Policeman (Angepasst - siehe Abbildung 4.26b) - Netzwerkanalyse: 5.



Policeman (Angepasst - siehe Abbildung 4.26b) - Tracker: 1 - 5



Literaturverzeichnis

[Akk16] Istemi Ekin Akkus. “Towards A Non-tracking Web”. Online erhältlich unter https://kluedo.ub.uni-kl.de/frontdoor/index/index/docId/4358 abgerufen am 11.05.2016. Diss. 2016, S. XIV, 182.

[BBDI13] Berliner Beauftragter für Datenschutz und Informationsfreiheit. *Webtracking und Privatsphäre: Die Beachtung von Kontext, Transparenz und Kontrolle bleibt unverzichtbar*. Techn. Ber. Online erhältlich unter https://datenschutz-berlin.de/attachments/951/675.46.18.pdf abgerufen am 13.04.2016. 2014.

[BITKOM14] BITKOM. *Jung und vernetzt - Kinder und Jugendliche in der digitalen Gesellschaft*. Techn. Ber. Online erhältlich unter https://www.bitkom.org/Publikationen/2014/Studien/Jung-und-vernetzt-Kinder-und-Jugendliche-in-der-digitalen-Gesellschaft/BITKOM-Studie-Jung-und-vernetzt-2014.pdf abgerufen am 24.03.2016. 2014.

[BSIDB] *BSIFB - Der Browser*. Online erhältlich unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/EinrichtungBrowser/derbrowser_node.html abgerufen am 03.08.2016.

[Bö02] Wolfgang Böhmer. “VPN-Virtual Private Networks”. In: *Die reale Welt der* (2002). Online erhältlich unter https://www.terrashop.de/pdfs/leseprobe/3446229302.pdf abgerufen am 01.07.2016.

[Bü13] René Büst. “Daten sind das neue öl”. In: *Wirtschaftsinformatik & Management* 5.2 (2013). Online erhältlich unter http://link.springer.com/article/10.1365/s35764-013-0277-4 abgerufen am 04.05.2016., S. 40 –46. ISSN: 1867-5905. DOI: 10.1365/s35764-013-0277-4.

[Cal+15] Chris Calabrese u. a. *Re: Comments for November 2015 Workshop on Cross-Device Tracking*. Online erhältlich unter https://cdt.org/files/

2015/10/10.16.15-CDT-Cross-Device-Comments.pdf abgerufen am 02.06.2016. Center for Democracy & Technology, Okt. 2015.

[Cha15] Hitesh Chawla. *Method and System for cross-device targeting of users*. Online erhältlich unter http://www.freepatentsonline.com/20150215668.pdf abgerufen am 02.06.2016. Juli 2015.

[Dig] Digitalcourage e.V. *BigBrotherAwards*. Online erhältlich unter https://bigbrotherawards.de/ abgerufen am 08.05.2016.

[Eck10] Peter Eckersley. "How Unique Is Your Web Browser?" In: *Privacy Enhancing Technologies: 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings*. Hrsg. von Mikhail J. Atallah und Nicholas J. Hopper. Online erhältlich unter http://link.springer.com/chapter/10.1007/978-3-642-14527-8_1 abgerufen am 15.09.2016. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, S. 1–18. ISBN: 978-3-642-14527-8. DOI: 10.1007/978-3-642-14527-8_1.

[FFABP] *Über Adblock Plus*. Online erhältlich unter https://adblockplus.org/de/about abgerufen am 07.09.2016.

[FFADS] *Disconnect: faster - Benchmark*. Online erhältlich unter https://disconnect.me/faster abgerufen am 17.08.2016.

[FFAPB] *Privacy Badger | Electronic Frontier Foundation*. Online erhältlich unter https://www.eff.org/de/node/73969 abgerufen am 24.08.2016.

[FFAPS] *Privacy Settings :: add0n.com*. Online erhältlich unter http://firefox.add0n.com/privacy-settings.html abgerufen am 12.08.2016.

[FM98] Hannes Federrath und Kai Martius. "Anonymität und Authentizität im World Wide Web". In: (1998). Online erhältlich unter http://epub.uni-regensburg.de/7396/1/FeMa1_98ITG.pdf abgerufen am 01.07.2016.

[FTC2015] Federal Trade Commission. "Internet of Things: Privacy and Security in a Connected". In: (Jan. 2015). Online erhältlich unter https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf abgerufen am 25.04.2016.

[Fin15] Kevin Finisterre. *SilverPushUnmasked*. Online erhältlich unter https://github.com/MAVProxyUser/SilverPushUnmasked abgerufen am 02.06.2016. Nov. 2015.

[Gartner15] Gartner. "Gartner Says 6.4 Billion Connected "Things"Will Be in Use in 2016, Up 30 Percent From 2015". In: (Nov. 2015). Online erhältlich unter http://www.gartner.com/newsroom/id/3165317 abgerufen am 25.04.2016.

[HA14] Jacob Hoffman-Andrews. *Verizon Injecting Perma-Cookies to Track Mobile Customers, Bypassing Privacy Controls*. Online erhältlich unter https://www.eff.org/de/deeplinks/2014/11/verizon-x-uidh abgerufen am 10.06.2016. Electronic Frontier Fundation, Nov. 2014.

[HBF13] Dominik Herrmann, Christian Banse und Hannes Federrath. "Behavior-based tracking: Exploiting characteristic patterns in DNS traffic". In: *Computers & Security* 39, Part A (2013). Online erhältlich unter http://www.sciencedirect.com/science/article/pii/S0167404813000576 abgerufen am 19.05.2016., S. 17 –33. ISSN: 0167-4048. DOI: http://dx.doi.org/10.1016/j.cose.2013.03.012.

[Hil14] Kashmir Hill. *AT&T Says It's 'Testing' Unique Tracker On Customers' Smartphones*. Online erhältlich unter http://www.forbes.com/sites/kashmirhill/2014/10/28/att-says-its-testing-unkillable-tracker-on-customers-smartphones/ abgerufen am 10.06.2016. Okt. 2014.

[KC15] Georgios Kontaxis und Monica Chew. *Tracking Protection in Firefox For Privacy and Performance*. Online erhältlich unter http://ieee-security.org/TC/SPW2015/W2SP/papers/W2SP_2015_submission_32.pdf abgerufen am 05.09.2016. 2015.

[Kep13] Ben Kepes. *Google Users - You're The Product, Not The Customer*. Online erhältlich unter http://www.forbes.com/sites/benkepes/2013/12/04/google-users-youre-the-product-not-the-customer/ abgerufen am 05.05.2016. 2013.

[LP14] Brian Libonate und Paul H. Prehn. *Obtaining targeted services using a unique identification header (UIDH)*. Online erhältlich unter https://www.google.com/patents/US8832436 abgerufen am 10.06.2016. Sep. 2014.

[Lee09] Waiki Lee. *Referral platform*. Online erhältlich unter https://www.google.com/patents/US20090234730 abgerufen am 30.05.2016. Sep. 2009. URL: https://www.google.com/patents/US20090234730.

[Lut+15] Timm Lutter u. a. *Zukunft der Consumer Electronics – 2015*. Techn. Ber. Online erhältlich unter https://www.bitkom.org/Publikationen/2015/Studien/CE-Studie-2015/150901-CE-Studie-2015-online.pdf abgerufen am 18.03.2016. 2015.

[MDK14] Bodo Möller, Thai Duong und Krzysztof Kotowicz. *This POODLE Bites: Exploiting The SSL 3.0 Fallback*. Online erhältlich unter https://www.openssl.org/~bodo/ssl-poodle.pdf abgerufen am 25.05.2016. Sep. 2014.

[MM12] J. R. Mayer und J. C. Mitchell. "Third-Party Web Tracking: Policy and Technology". In: *2012 IEEE Symposium on Security and Privacy*. Online erhältlich unter http://ieeexplore.ieee.org/document/6234427/ abgerufen am 15.09.2016. Mai 2012, S. 413–427. DOI: 10.1109/SP.2012.47.

[MS12] Keaton Mowery und Hovav Shacham. "Pixel perfect: Fingerprinting canvas in HTML5". In: *Proceedings of W2SP* (2012).

[Mor14] Jacob Morgan. "A Simple Explanation Of 'The Internet Of Things'". Online erhältlich unter http://ssrn.com/abstract=2715799 abgerufen am 25.04.2016. Magisterarb. Mai 2014. DOI: 10.2139/ssrn.2715799.

[Moz15] *Firefox Now Offers a More Private Browsing Experience*. Online erhältlich unter https://blog.mozilla.org/blog/2015/11/03/firefox-now-offers-a-more-private-browsing-experience/ abgerufen am 02.08.2016. Nov. 2015.

[Mue+16] Jonathan Muehlstein u. a. "Analyzing HTTPS Encrypted Traffic to Identify User Operating System, Browser and Application". In: *CoRR* abs/1603.04865 (2016). Online erhältlich unter https://arxiv.org/abs/1603.04865 abgerufen am 25.05.2016.

[NBV09] Shaneel Narayan, Kris Brooking und Simon de Vere. "Network performance analysis of vpn protocols: An empirical comparison on different operating systems". In: *Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC'09. International Conference on*. Bd. 1. Online erhältlich unter http://ieeexplore.ieee.org/document/4908347/ abgerufen am 16.09.2016. IEEE. 2009, S. 645–648.

[Nay+14] David Naylor u. a. “The cost of the s in https”. In: *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*. Online erhältlich unter http://dl.acm.org/citation.cfm?id=2674991 abgerufen am 26.09.2016. ACM. 2014, S. 133–140.

[Op15D] *Built-in ad blocker in Opera Mini and Opera for computers*. Online erhältlich unter http://www.opera.com/blogs/news/2016/05/ad-blocker-integrated-opera-for-android-windows-mac-opera-mini/ abgerufen am 02.08.2016. Mai 2016.

[Op15M] *Built-in ad blocker for Android, iOS and Windows Phone*. Online erhältlich unter http://www.opera.com/blogs/news/2016/06/ad-blocker-android-ios-windows-phone-download-free/ abgerufen am 2.08.2016. 2016.

[OpenVPN] *HOWTO*. Online erhältlich unter https://openvpn.net/index.php/open-source/documentation/howto.html abgerufen am 17.09.2016.

[PI] Privacy International. *Big Brother Awards International*. Online erhältlich unter http://www.bigbrotherawards.org/ abgerufen am 08.05.2016.

[QUIC] R. Hamilton u. a. *QUIC: A UDP-Based Secure and Reliable Transport for HTTP/2*. Internet-Draft. Online erhältlich unter https://tools.ietf.org/html/draft-hamilton-early-deployment-quic-00 abgerufen am 17.09.2016. Internet Engineering Task Force, Juli 2016.

[RBE03] Abdelmounaam Rezgui, Athman Bouguettaya und Mohamed Y Eltoweissy. “Privacy on the Web: Facts, challenges, and solutions”. In: *IEEE Security & Privacy* 6 (2003). Online erhältlich unter https://www.computer.org/csdl/mags/sp/2003/06/j6040.pdf abgerufen am 30.05.2016., S. 40–49.

[RFC1122] Robert Braden. *Requirements for Internet Hosts - Communication Layers*. RFC 1122 (INTERNET STANDARD). Online erhältlich unter https://tools.ietf.org/html/rfc1122 abgerufen am 21.05.2016. Internet Engineering Task Force, Okt. 1989.

[RFC1631] Kjeld Borch Egevang und Paul Francis. *The IP Network Address Translator (NAT)*. RFC 1631 (Informational). Online erhältlich unter https://tools.ietf.

org/html/rfc1631 abgerufen am 12.05.2016. Internet Engineering Task Force, Mai 1994.

[RFC1883] Stephen Deering und Robert M. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*. RFC 1883 (Proposed Standard). Online erhältlich unter https://tools.ietf.org/html/rfc1883 abgerufen am 17.06.2016. Internet Engineering Task Force, Dez. 1995.

[RFC1928] M. Leech u. a. *SOCKS Protocol Version 5*. RFC 1928 (Proposed Standard). Online erhältlich unter https://tools.ietf.org/html/rfc1928 abgerufen am 29.05.2016. Internet Engineering Task Force, März 1996.

[RFC2637] K. Hamzeh u. a. *Point-to-Point Tunneling Protocol (PPTP)*. RFC 2637 (Informational). Online erhältlich unter https://tools.ietf.org/html/rfc2637 abgerufen am 17.09.2016. Internet Engineering Task Force, Juli 1999.

[RFC2661] W. Townsley u. a. *Layer Two Tunneling Protocol "L2TP"*. RFC 2661 (Proposed Standard). Online erhältlich unter https://tools.ietf.org/html/rfc2661 abgerufen am 17.09.2016. Internet Engineering Task Force, Aug. 1999.

[RFC2818] Eric Rescorla. *HTTP Over TLS*. RFC 2818 (Informational). Online erhältlich unter https://tools.ietf.org/html/rfc2818 abgerufen am 25.05.2016. Internet Engineering Task Force, Mai 2000.

[RFC3193] B. Patel u. a. *Securing L2TP using IPsec*. RFC 3193 (Proposed Standard). Online erhältlich unter https://tools.ietf.org/html/rfc3193 abgerufen am 17.09.2016. Internet Engineering Task Force, Nov. 2001.

[RFC3798] Tony Hansen und Gregory Vaudreuil. *Message Disposition Notification*. RFC 3798 (Draft Standard). Online erhältlich unter https://tools.ietf.org/html/rfc3798 abgerufen am 29.05.2016. Internet Engineering Task Force, Mai 2004.

[RFC4301] S. Kent und K. Seo. *Security Architecture for the Internet Protocol*. RFC 4301 (Proposed Standard). Online erhältlich unter https://tools.ietf.org/html/rfc4301 abgerufen am 17.09.2016. Internet Engineering Task Force, Dez. 2005.

[RFC4302] S. Kent. *IP Authentication Header*. RFC 4302 (Proposed Standard). Online erhältlich unter https://tools.ietf.org/html/rfc4301 abgerufen am 17.09.2016. Internet Engineering Task Force, Dez. 2005.

[RFC4303] S. Kent. *IP Encapsulating Security Payload (ESP)*. RFC 4303 (Proposed Standard). Online erhältlich unter `https://tools.ietf.org/html/rfc4301` abgerufen am 17.09.2016. Internet Engineering Task Force, Dez. 2005.

[RFC4862] Susan Thomson, Thomas Narten und Tatuya Jinmei. *IPv6 Stateless Address Autoconfiguration*. RFC 4862 (Draft Standard). Online erhältlich unter `https://tools.ietf.org/html/rfc4862` abgerufen am 13.05.2016. Internet Engineering Task Force, Sep. 2007.

[RFC5322] Peter W. Resnick. *Internet Message Format*. RFC 5322 (Draft Standard). Online erhältlich unter `https://tools.ietf.org/html/rfc3798` abgerufen am 29.05.2016. Internet Engineering Task Force, Okt. 2008.

[RFC6347] E. Rescorla und N. Modadugu. *Datagram Transport Layer Security Version 1.2*. RFC 6347 (Proposed Standard). Online erhältlich unter `https://tools.ietf.org/html/rfc6347` abgerufen am 17.09.2016. Internet Engineering Task Force, Jan. 2012.

[RFC760] Jon Postel. *DoD standard Internet Protocol*. RFC 760. Online erhältlich unter `https://tools.ietf.org/html/rfc760` abgerufen am 17.06.2016. Internet Engineering Task Force, Jan. 1980.

[RIPE12] RIPE NCC. *IPv4 Exhaustion*. Online erhältlich unter `https://www.ripe.net/publications/ipv6-info-centre/about-ipv6/ipv4-exhaustion` abgerufen am 12.05.2016. Sep. 2012.

[Sch12] Jürgen Schmidt. *Der Todesstoß für PPTP | heise Security*. Online erhältlich unter `http://www.heise.de/security/artikel/Der-Todesstoss-fuer-PPTP-1701365.html` abgerufen am 17.09.2016. Sep. 2012.

[Sha+16] Scott Shackelford u. a. "When Toasters Attack: A Polycentric Approach to Enhancing the 'Security of Things'". Online erhältlich unter `http://ssrn.com/abstract=2715799` abgerufen am 25.04.2016. Magisterarb. Jan. 2016. DOI: `10.2139/ssrn.2715799`.

[Sol11] Olivia Solon. *You are Facebook's product, not customer*. Online erhältlich unter `http://www.wired.co.uk/news/archive/2011-09/21/doug-rushkoff-hello-etsy` abgerufen am 05.05.2016. 2011.

[Tor] *Tor Project: Anonymity Online*. Online erhältlich unter `https://www.torproject.org/index.html.en` abgerufen am 08.07.2016.

[W3CDNT] *Tracking Preference Expression (DNT).* Online erhältlich unter `https://www.w3.org/TR/tracking-dnt/` abgerufen am 04.08.2016.

[W3CETag] *CachingWithETag - Shared Techniques wiki for the W3C Mobile Web Initative Best Practices.* Online erhältlich unter `https://www.w3.org/2005/MWI/BPWG/techs/CachingWithETag.html` abgerufen am 15.09.2016.

[WebRTC] *Frequent Questions | WebRTC.* Online erhältlich unter `https://webrtc.org/faq/` abgerufen am 13.09.2016.

[XROXY] *What does "Anonymous", "Distorting" and "Transparent" actually mean?* Online erhältlich unter `https://www.xroxy.com/faq/proxy_classification.htm` abgerufen am 08.07.2016.

[abu14] abullrd. *fast_tim_conf/id_set.lua.* Online erhältlich unter `https://web.archive.org/web/20141027194059/https://github.com/Funnerator/fast_tim_conf/blob/master/lua/id_set.lua` abgerufen am 10.06.2016. Mai 2014.

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 13.10.2016 Kai Henken