Surfen ohne Spuren zu hinterlassen

PC-Treff-BB Aidlingen

Günter Waller

12.04.2014

Agenda

- Einführung, Motivation
- Begriffe
- Welche Spuren kann man hinterlassen?
- IP-Adresse
- Cookies
- Browser-Fingerprinting
- Benutzerkennungen, Nicknames

Einführung, Motivation

- Ich möchte gerne selbst bestimmen, wem ich mich beim Bewegen im Internet zu erkennen gebe und welche Informationen ich dabei preisgebe.
- Es geht also um personenbezogene Daten, die geschützt werden sollen.
- Die Preisgabe dieser Daten kann **explizit** erfolgen (Login mit nachvollziehbarer, meiner Person zurechenbarer Kennung), oder unter Verwendung eines **Pseudonyms** (kann nicht unmittelbar, evtl. aber mittelbar) zugeordnet werden, oder **anonym** (kann nicht oder mit erheblichem Aufwand enttarnt werden.
- Wer nach Informationen sucht oder Dienste nutzt, gibt zwangsläufig etwas über sich preis. Dies kann sich nachteilig auswirken.
- Die Folgen können lästig (Spam), peinlich (Bekanntwerden von privaten Dingen), teuer (Betrug) bis hin zu existenzbedrohend (Identitätsdiebstahl) sein.

Begriffe

- **Anonymität** ist die Eigenschaft, dass eine Person, eine Gruppe, eine Institution oder eine agierenden Struktur nicht identifiziert werden kann. Von der Bedeutung her zum Teil synonym zu anonym ist inkognito, sonst spricht man deutsch von unbekannt.
- Das Internet ermöglicht unterschiedlich weitgehende Formen der Anonymität. Eingeschränkt wird diese beispielsweise dadurch, dass bei jeder Kommunikation im Internet eine **IP-Adresse** mitübertragen wird. Auch durch **sorgloses Verhalten** hinterlassen Internetbenutzer Spuren, und mit **technischen Tricks** können viele Informationen über diese gesammelt werden.
- Bei der **Pseudonymisierung** wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym (Nickname) ersetzt, um die Identifizierung des Betroffenen auszuschließen oder wesentlich zu erschweren. Es bleiben jedoch Bezüge verschiedener Datensätze, die auf dieselbe Art pseudonymisiert wurden, erhalten.
- Die Pseudonymisierung ermöglicht – unter Zuhilfenahme eines Schlüssels – die Zuordnung von Daten zu einer Person, was ohne diesen Schlüssel nicht oder nur schwer möglich ist, da Daten und Identifikationsmerkmale getrennt sind. Entscheidend ist also, dass eine Zusammenführung von Person und Daten noch möglich ist.

Quelle: Wikipedia

Welche Spuren kann man hinterlassen

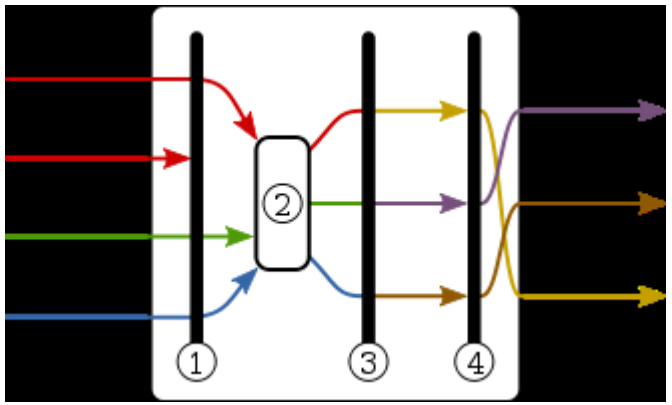
- IP-Adresse
  - Fest (direkt nachvollziehbar)
  - Dynamisch (Provider kann die Zuordnung nachvollziehen, Preisgabe bei Gerichtsbeschluß)
- Cookies
- Personalisierte Links
- In den Seiten enthaltene aktive Teile (z.B. Javascript)
- Browserprofil
  - HTTP-Header

IP-Adresse

- Ohne die IP-Adresse des Absenders kann die Antwort auf eine Anfrage nicht zugestellt werden. Daher wird sie zwangsläufig übertragen. Sie ist gleichzeitig – über den Internetanschluß, zu dem sie gehört - der Schlüssel zur Identität des Anfragenden.
  - Feste (statische) IP-Adresse – meist bei Firmen
  - Dynamische, über DHCP vom Provider zugeordnete IP-Adresse – Normalfall bei Privatnutzern. Unterschiedliche Vergabepraxis bei den Providern.
    - Speicherung und Preisgabe der Zuordnung juristisch strittiges Thema (Vorratsdatenspeicherung, Telekommunikationsgesetz)
    - Wer dem entgehen will, kann Anonymisierungsdienste wie Tor verwenden.

Tor und Vorläufer

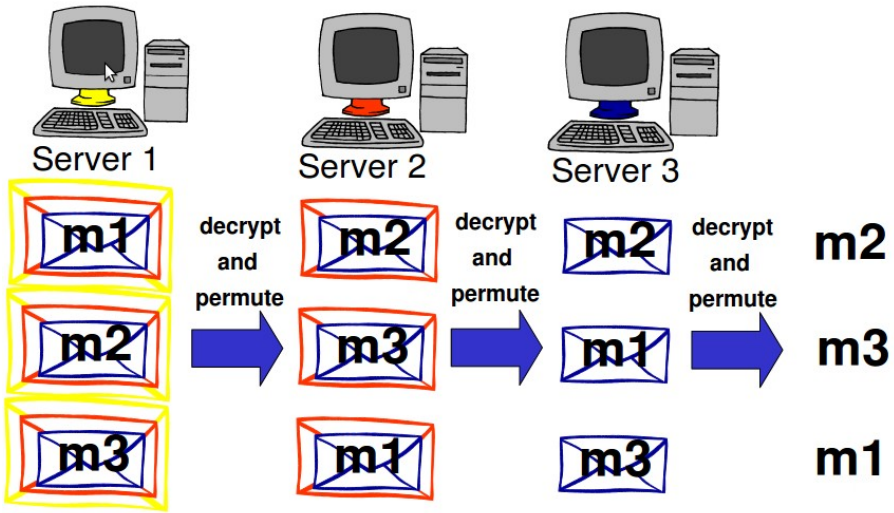
- Anonymität durch Verstecken in der Menge.
- 2 Ansätze:
  - Mixes
  - Proxies
- Grundfunktionen eines Mixes:
  1. Filtern
  2. Sammeln
  3. Umkodieren
  4. Umsortieren der Nachrichten

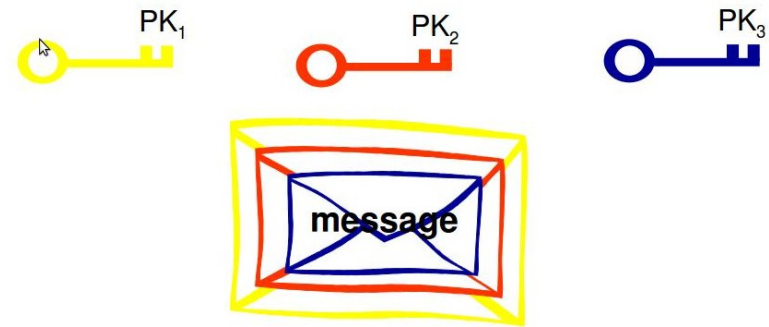


Quelle: Wikipedia

Mix

- Das 1981 von David Chaum eingeführte Konzept der (umkodierenden) Mixe dient der anonymen Kommunikation innerhalb eines Netzwerkes. Dabei werden Nachrichten nicht direkt vom Sender zum Empfänger übertragen, sondern über mehrere Zwischenstationen (Mixe genannt) geleitet. Das Ziel ist die Anonymisierung der Kommunikationsbeziehung, was abhängig vom zugrunde liegenden Konzept zu einer der folgenden drei Ausprägungen führt:
  - der Empfänger bleibt vor dem Sender anonym
  - der Sender bleibt vor dem Empfänger anonym
  - Sender und Empfänger bleiben voreinander anonym
- Die wichtigste Eigenschaft, der Schutz von Verkehrsinformationen gegenüber außenstehenden Dritten, wird durch alle drei Konzepte realisiert.

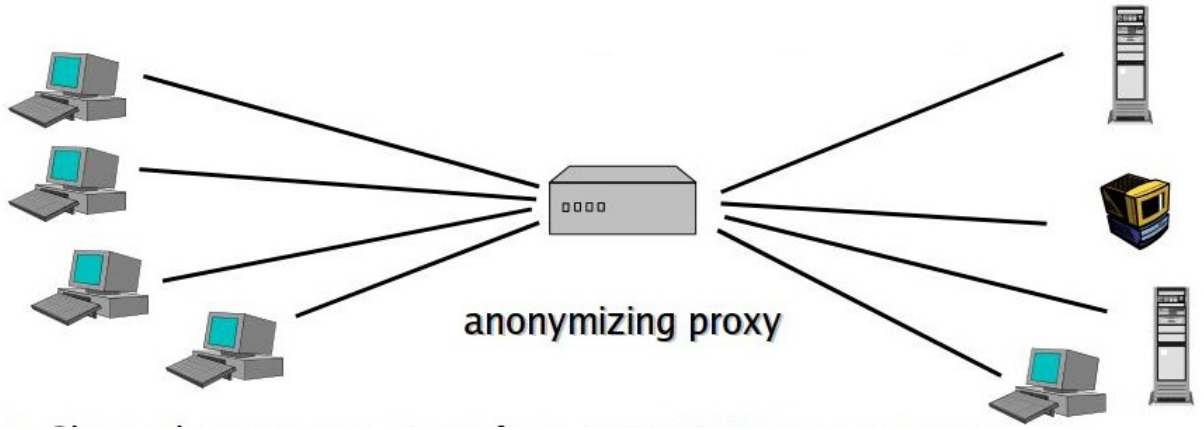




Quellen: Wikipedia
www.torproject.org

Proxy

- Ein Anonymisierer wird als ein so genannter Proxy bzw. ein Virtual Private Network (VPN) zwischen Benutzer und Zielrechner geschaltet. Da nun der Proxy/VPN anstelle des Benutzers mit dem Zielrechner kommuniziert, kann die Verbindung zum ursprünglichen Nutzer nicht ohne weiteres zurückverfolgt werden. Dazu ist es allerdings nötig, dass der Proxy wirklich anonym ist und nicht wie ein regulärer Proxy per Kopfdaten mitteilt, dass die Anfrage von einem Proxy kommt und welcher Client anfragt.
- Üblicherweise wird der Datenstrom zwischen Nutzer und Anonymisierer verschlüsselt, um ein Abhören der Verbindung zwischen Nutzer und Proxy zu verhindern. Dabei wird vorausgesetzt, dass möglichst viele Nutzer denselben Proxy gleichzeitig nutzen, damit einzelne Verbindungen nicht bestimmten Nutzern zugeordnet werden können.
- Viele bekannte Anonymisierer setzen auf das SSL- oder SOCKS-Protokoll und können daher mit einer Vielzahl von Anwendungen genutzt werden.



Quellen: Wikipedia
www.torproject.org

Onion Routing verbindet die beiden Ansätze

- Die Webinhalte werden über **ständig wechselnde Routen** von mehreren Mixen geleitet, welche in diesem Zusammenhang auch Knoten genannt werden. Diese stellen jeweils eine Art verschlüsselnder Proxyserver dar.
- Verwendung von Public-Key Verschlüsselung nur für Verbindungsaufbau
- Verwendung von (weniger aufwendiger) symmetrischer Verschlüsselung für die Daten – ähnlich wie bei SSL/TLS
- Im Gegensatz zu Diensten, die auf festen Mix-Kaskaden basieren, d. h. die stets eine für alle Nutzer gleiche Route zwischen den Mixen verwenden, wird beim Onion-Routing die Auswahl und Reihenfolge der benutzten Knoten immer wieder individuell durch jeden Nutzer geändert. Somit scheint auch ein späterer erneuter Zugriff auf einen Server aus Sicht dieses Servers von einem neuen Benutzer zu kommen, da sich die IP-Adresse zwischenzeitlich ebenso geändert hat. Dies gilt allerdings nur, falls nicht auf Grund der übertragenen Inhaltsdaten eine weitere Identifikation möglich ist, z. B. wegen Cookies oder personalisierten Links.
- Weiterführende Lektüre: http://www.onion-router.net/Publications.html

Quelle: Wikipedia

TOR – The Onion Router

1 Der Nutzer installiert auf seinem Computer einen Client, den sogenannten **Onion-Proxy.** Dieses Programm verbindet sich mit dem Tor-Netzwerk. In der Startphase lädt sich das Programm eine Liste aller vorhandenen und nutzbaren Tor-Server herunter. Diese mit einer digitalen Signatur versehene Liste wird von Verzeichnisservern aufbewahrt. Deren öffentliche Schlüssel werden mit dem Tor-Quellcode geliefert. Das soll sicherstellen, dass der Onion-Proxy ein authentisches Verzeichnis erhält.

2 Wenn die Liste empfangen wurde, wählt der Onion-Proxy eine zufällige Route über die Tor-Server.

3 Der Client verhandelt mit dem ersten Tor-Server eine verschlüsselte Verbindung. Wenn diese aufgebaut ist, wird sie um einen weiteren Server verlängert. Diese Prozedur wiederholt sich noch einmal, so dass eine Verbindungskette immer drei Tor-Server enthält. Jeder Server kennt seinen Vorgänger und seinen Nachfolger. Die Entwickler des Projektes wählten drei Server, um möglichst große Anonymität bei noch akzeptabler Verzögerungszeit zu erreichen. **Der Erfolg hängt dabei davon ab, dass mindestens einer der Server vertrauenswürdig ist und ein Angreifer nicht schon den Anfangs- und Endpunkt der Kommunikation überwacht.**

4 Nachdem eine Verbindung aufgebaut wurde, werden über diese Server die Daten versandt. Der letzte Server tritt dabei als Endpunkt der Kommunikation auf. Er wird als Exit- oder Austritts-Server oder -Knoten (englisch exit node) bezeichnet.

Quelle: Wikipedia

TOR – Hilfsprogramme

- **Vidalia** ist eine grafische Benutzeroberfläche zur Konfiguration und Steuerung des eigenen Tor-Clients. Das Programm hilft bei der Überwachung der Netzwerkaktivität und ermöglicht das einfache Verwalten von Logdateien. Vidalia kann die geographische Lage der Tor-Server und den Weg des eigenen Tor-Verkehrs auf einer Karte darstellen.

- Das **Tor Browser Bundle** (stellenweise auch nur „Tor Browser“) ist eine vorkonfigurierte Kombination aus dem Browser Mozilla Firefox, Tor Launcher und dem Tor-Client. Das Paket ist portabel und kann somit auch von einem Wechseldatenträger gestartet werden, wodurch es relativ unabhängig vom laufenden Betriebssystem ist. Dank der auf Kompatibilität ausgelegten Konfiguration der Komponenten ist auch Laien ein schneller Einstieg in das Tor-Netzwerk möglich.

- **Polipo** und **Privoxy**: Lange Zeit war es nötig, einen lokalen Proxy zwischen den Tor-Client und den empfohlenen Browser Firefox zu schalten, da letzterer bis zur Version 6 einen Fehler aufwies, der die direkte Kommunikation beider Programme unmöglich machte. Empfohlen wurde hier zunächst Privoxy, später der einfacher gestaltete Polipo. Seitdem der Fehler in Firefox behoben ist, raten die Entwickler dazu, nach Möglichkeit keinen Proxy mehr zu verwenden, da der Tor-Client dadurch bessere Kontrolle über den Browser hat.

- **Orbot** (Google Android ab Version 2.0) ist ein quelloffener Tor-Proxy für Android, welcher bei gerooteten Android-Geräten in der Lage ist, den gesamten Internetverkehr durch das Tor-Netzwerk zu leiten. Bei Geräten ohne Root-Berechtigungen funktioniert Orbot nur im Zusammenspiel mit dem ebenfalls quelloffenen Browser Orweb; das Durchleiten des Netzverkehrs von anderen Apps ist nicht möglich.

- **Orweb** (Google Android) ist ein speziell für das Tor-Netzwerk optimierter quelloffener Browser für Android, welcher auch sonst sehr großen Wert auf den Schutz der Privatsphäre legt. Er kommt auf ungerooteten Geräten zum Einsatz, um zusammen mit Orbot anonym mit einem Tor-Proxy zu surfen. Für die Nutzung von Orweb muss Orbot gestartet und eine Verbindung zum Tor-Netzwerk hergestellt sein.

- **Onion Browser** (Apple IOS ab Version 5.1): kostenpflichtiger IOS Browser, welcher die Seitenaufrufe über das Tor-Netzwerk durchführt. Obwohl der Onion Browser im AppStore nur kostenpflichtig zu erhalten ist, sind die Quelldateien kostenlos auf GitHub verfügbar.

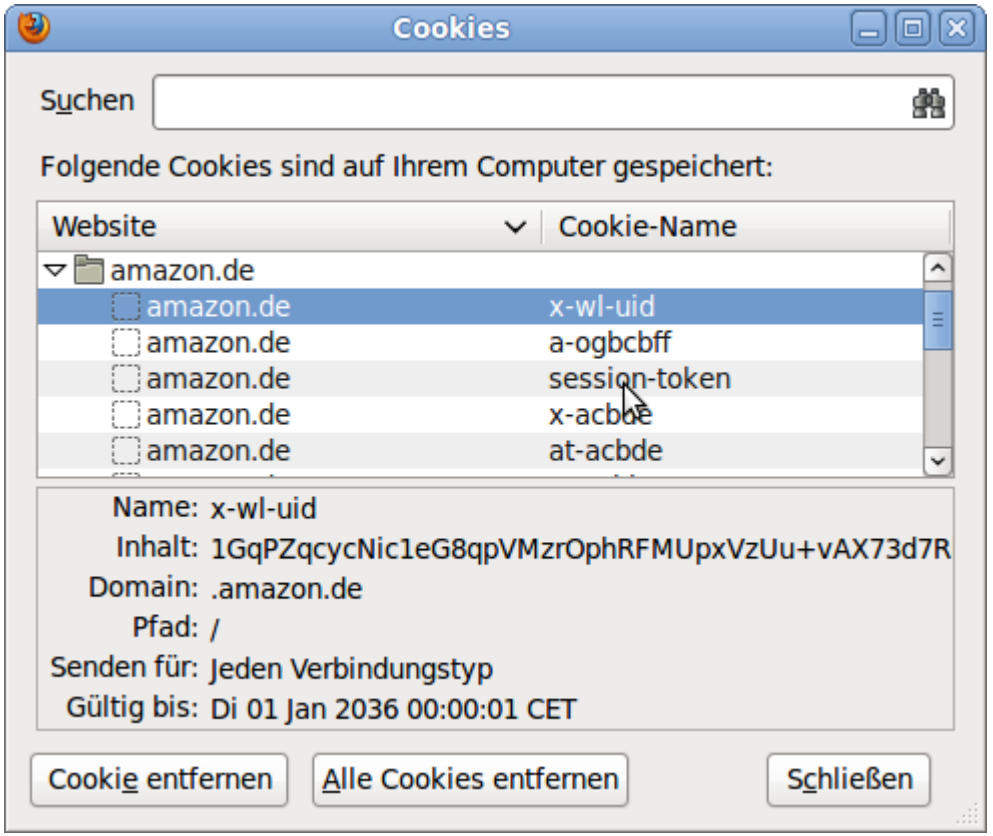
Quelle: Wikipedia

Vergleich von Anonymisierern

- Überblicksartikel, gefunden hier (allerdings von interessierter Seite):
- artikel.softonic.de/anonym-surfen-tor-jondo-vpn-und-web-proxies-im-vergleich
- Fazit des Artikels:
  - Für sicheres anonymes Surfen kommt nur JonDo wirklich in Betracht. Tor ist etwas schneller und theoretisch auch anonym. Die Wahrscheinlichkeit einer großangelegten Überwachung von Tor durch Geheimdienste sollte nach den PRISM-Enthüllungen aber nicht unterschätzt werden. VPN-Dienste sichern nur die Privatsphäre zuverlässig, für anonymes Surfen sind die Anbieter kaum empfehlenswert. Web-Proxies sollte man schlicht meiden!
- Mein Fazit:
  - Wer bietet das favorisierte JonDo an? Die gleiche Firma, die den Artikel geschrieben hat. Ein Schelm, wer schlechtes dabei denkt.
  - Aber trotzdem interessant für einen ersten Überblick.

Cookies

- Cookies sind eine nützliche Erfindung. Da HTTP zustandslos ist, gibt es keine Session, unter der man etwas speichern kann. Stattdessen verwendet man kleine Textdateien, die Cookies, die der Browser speichert und bei jedem Request wieder mitschickt.
- Es sind entweder Host- oder Domaincookies.
- Sie haben einen Namen, Inhalt (hier: verschlüsselt), sowie einige Metadaten.
- Verwaltung im Browser.
- Anwendung: Session-Id, Warenkorb, Speicherung von Dialogfeld-Eingaben.
- Problem: Mißbrauch.



Cookies - Funktionsweise

- Es gibt 2 Varianten:
  - Übertragung im HTTP-Header:

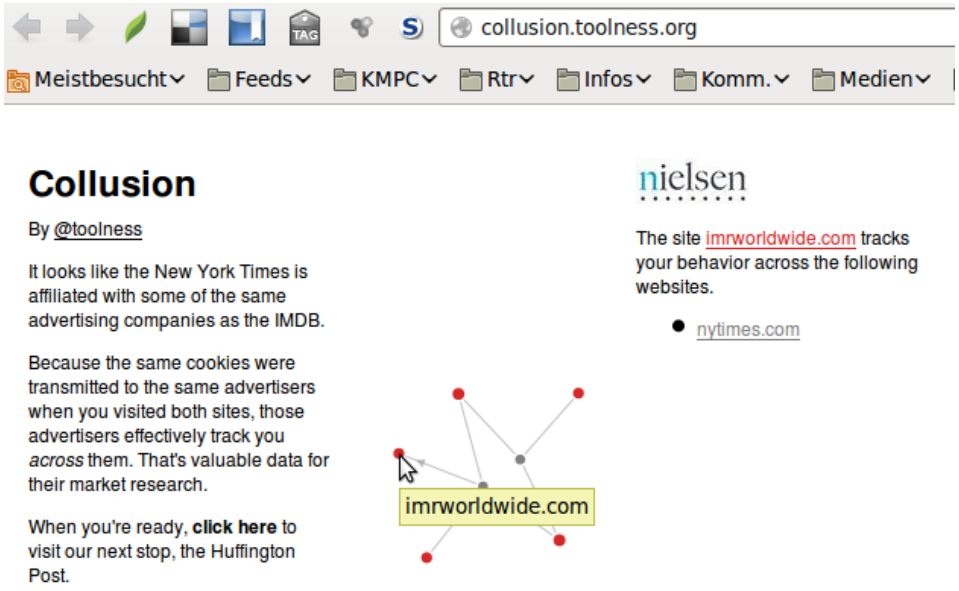
```
Set-Cookie: letzteSuche="cookie aufbau";
            expires=Tue, 29-Mar-2005 19:30:42 GMT;
            Max-Age=2592000; Path=/cgi/suche.py; Version="1"
```

  - Erzeugen im Browser durch JavaScript o.ä.
- Bei nachfolgenden Zugriffen auf den Webserver sucht der Client-Browser alle Cookies dieser Domain heraus, die zum Webserver und dem Verzeichnispfad des aktuellen Aufrufs passen. Diese Cookie-Daten werden im Header des HTTP-Zugriffs mit übertragen, sodass die Cookies nur an jenen Webserver zurückgehen dürfen, von dem sie einst auch stammten.
  - Syntax entsprechend:

```
Set-Cookie: . . .
```

Cookies - Gefahren

- Der ausstellende Server kann ggf. eine Zuordnung zur Person herstellen (z.B. bei Webshops) → Nutzerprofil, gezielte Werbung
- Durch versteckte Seiteninhalte (z.B. 1-Pixel-Bilder) können Cookies von anderen Servern (Third Party-Cookies, Tracking Cookies) eingeschleust werden. Dadurch kann das Surfverhalten beobachtet werden.
  - Beispiel: Facebook „Like“ Button auf einer Seite
  - Mit dem Browser-Plugin Collusion kann diese Nachverfolgung grafisch dargestellt werden.
  - Demo
- Gegenmaßnahmen:
  - Cookies öfter löschen
  - JavaScript einschränken



Browser-Fingerprinting

- Aus Informationen, die der Browser preisgibt, läßt sich ein digitaler Fingerabdruck der Systemkonfiguration erstellen.
- Einige Informationen werden vom Browser automatisch an den Webserver geschickt (passives Fingerprinting), andere lassen sich durch JavaScript oder Flash auslesen (aktives Fingerprinting). Dieser Code wird vom Server empfangen, im Browser ausgeführt und schickt dann seine Ergebnisse zurück an den Server.
- Anwendungen:
  - Positiv: Wiedererkennen des Gerätes, Schutz vor Identitätsbetrug, Risikobewertung eines Zugriffes
  - Negativ: Tracking für Werbezwecke, statt Cookies, falls diese unterdrückt sind.
- Quelle und mehr Infos:
  - Diplomarbeit Henning Tillmann
  - Selbstversuch (siehe nächste 2 Seiten, dauert u.U. Minuten): https://panopticlick.eff.org/index.php?action=log&js=yes
  - Browserspy.dk
  - Heise-Ticker vom 21.10.2013

Panopticlick

How Unique — and Trackable — Is Your Browser?

Your browser fingerprint **appears to be unique** among the 3,984,387 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 21.93 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in **this article**.

Help us increase our sample size:

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	10.78	1754.46	Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:20.0) Gecko/20100101 Firefox/20.0
HTTP_ACCEPT Headers	5.26	38.23	text/html, */* gzip, deflate de-de,de;q=0.8,en-us;q=0.5,en;q=0.3
			Plugin 0: Adobe Reader 9.5; The Adobe Reader plugin is used to enable viewing of PDF and FDF files from within the browser. ; nppdf.so; (Portable Document Format; application/pdf; pdf) (Acrobat Forms Data Format; application/vnd.fdf; fdf) (XML Version of Acrobat Forms Data Format; application/vnd.adobe.xfdf; xfdf) (Acrobat XML Data Package; application/vnd.adobe.xdp+xml; xdp) (Adobe FormFlow99 Data File; application/vnd.adobe.xfd+xml; xfd). Plugin 1: Adobe Reader 9.5; The Adobe Reader plugin is used to enable viewing of PDF and FDF files from within the browser. ; nppdf.so; (Portable Document Format; application/pdf; pdf) (Acrobat Forms Data Format; application/vnd.fdf; fdf) (XML Version of Acrobat Forms Data Format; application/vnd.adobe.xfdf; xfdf) (Acrobat XML Data Package; application/vnd.adobe.xdp+xml; xdp) (Adobe FormFlow99 Data File; application/vnd.adobe.xfd+xml; xfd). Plugin 2: DivX® Web Player; DivX Web Player version 1.4.0.233; libtotem-mully-plugin.so; (AVI-Video; video/divx; divx). Plugin 3: IcedTea-Web Plugin (using IcedTea-Web 1.2.3 (1.2.3-0ubuntu0.10.04.1)); The IcedTea-Web Plugin executes Java applets.; IcedTeaPlugin.so; (IcedTea; application/x-java-vm; class,jar) (IcedTea; application/x-java-applet; class,jar) (IcedTea; application/x-java-applet;version=1.1; class,jar) (IcedTea; application/x-java-applet;version=1.1.1; class,jar) (IcedTea; application/x-java-applet;version=1.1.2; class,jar) (IcedTea; application/x-java-applet;version=1.1.3; class,jar) (IcedTea; application/x-java-applet;version=1.2; class,jar) (IcedTea; application/x-java-applet;version=1.2.1; class,jar) (IcedTea; application/x-java-applet;version=1.2.2; class,jar) (IcedTea; application/x-java-applet;version=1.3; class,jar)

Browser Plugin Details	21.93+	3984387	java-applet;version=1.2.2; class,jar) (IcedTea; application/x-java-applet;version=1.3; class,jar) (IcedTea; application/x-java-applet;version=1.3.1; class,jar) (IcedTea; application/x-java-applet;version=1.4; class,jar) (IcedTea; application/x-java-applet;version=1.4.1; class,jar) (IcedTea; application/x-java-applet;version=1.4.2; class,jar) (IcedTea; application/x-java-applet;version=1.5; class,jar) (IcedTea; application/x-java-applet;version=1.6; class,jar) (IcedTea; application/x-java-applet;jpi-version=1.6.0_50; class,jar) (IcedTea; application/x-java-bean; class,jar) (IcedTea; application/x-java-bean;version=1.1; class,jar) (IcedTea; application/x-java-bean;version=1.1.1; class,jar) (IcedTea; application/x-java-bean;version=1.1.2; class,jar) (IcedTea; application/x-java-bean;version=1.1.3; class,jar) (IcedTea; application/x-java-bean;version=1.2; class,jar) (IcedTea; application/x-java-bean;version=1.2.1; class,jar) (IcedTea; application/x-java-bean;version=1.2.2; class,jar) (IcedTea; application/x-java-bean;version=1.3; class,jar) (IcedTea; application/x-java-bean;version=1.3.1; class,jar) (IcedTea; application/x-java-bean;version=1.4; class,jar) (IcedTea; application/x-java-bean;version=1.4.1; class,jar) (IcedTea; application/x-java-bean;version=1.4.2; class,jar) (IcedTea; application/x-java-bean;version=1.5; class,jar) (IcedTea; application/x-java-bean;version=1.6; class,jar) (IcedTea; application/x-java-bean;jpi-version=1.6.0_50; class,jar) (IcedTea; application/x-java-vm-npruntime;). Plugin 4: QuickTime Plug-in 7.6.6; The Totem 2.30.2 plugin handles video and audio streams.; libtotem-narrowspace-plugin.so; (QuickTime-Video; video/quicktime; mov) (MPEG-4-Video; video/mp4; mp4) (MacPaint-Bitmap-Datei; image/x-macpaint; pntg) (Macintosh-Quickdraw/PICT-Zeichnung; image/x-quicktime; pict, pict1, pict2) (MPEG-4-Video; video/x-m4v; m4v). Plugin 5: Shockwave Flash; Shockwave Flash 11.2 r202; libflashplayer.so; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 6: VLC Multimedia Plugin (compatible Totem 2.30.2); The Totem 2.30.2 plugin handles video and audio streams.; libtotem-cone-plugin.so; (VLC Multimedia Plugin; application/x-vlc-plugin;) (VLC Multimedia Plugin; application/vlc;) (VLC Multimedia Plugin; video/x-google-vlc-plugin;) (Ogg-Multimediadatei; application/x-ogg; ogg) (Ogg-Multimediadatei; application/ogg; ogg) (Ogg-Audio; audio/ogg; oga) (Ogg-Audio; audio/x-ogg; ogg) (Ogg-Video; video/ogg; ogv) (Ogg-Video; video/x-ogg; ogg) (Annodex-Wechselformat; application/annodex; anx) (Annodex-Audio; audio/annodex; axa) (Annodex-Video; video/annodex; axv) (MPEG-Video; video/mpeg; mpg, mpeg, mpe) (WAV-Audio; audio/wav; wav) (WAV-Audio; audio/x-wav; wav) (MP3-Audio; audio/mpeg; mp3) (NullSoft-Video; application/x-nsv-vp3-mp3; nsv) (Flash-Video; video/flv; flv) (Totem Multimedia plugin; application/x-totem-plugin;). Plugin 7: Windows Media Player Plug-in 10 (compatible; Totem); The Totem 2.30.2 plugin handles video and audio streams.; libtotem-gmp-plugin.so; (AVI-Video; application/x-mplayer2; avi, wma, wmv) (ASF-Video; video/x-ms-asf-plugin; asf, wmv) (AVI-Video; video/x-msvideo; asf, wmv) (ASF-Video; video/x-ms-asf; asf) (Windows-Media-Video; video/x-ms-wmv; wmv) (Windows-Media-Video; video/x-wmv; wmv) (Windows-Media-Video; video/x-ms-wvx; wmv) (Windows-Media-Video; video/x-ms-wm; wmv) (Windows-Media-Video; video/x-ms-wmp; wmv) (Windows-Media-Video; application/x-ms-wms; wms) (Windows-Media-Video; application/x-ms-wmp; wmp) (Microsoft-ASX-Wiedergabeliste; application/asx; asx) (Windows-Media-Audio; audio/x-ms-wma; wma). Plugin 8: iTunes Application Detector; This plug-in detects the presence of iTunes when opening iTunes Store URLs in a web page with Firefox.; librhythmbox-itms-detection-plugin.so; (; application/itunes-plugin;).
Time Zone	2.55	5.85	-60

Time Zone	2.55	5.85	-60
Screen Size and Color Depth	7.29	156.98	1600x1200x24
System Fonts	15.52	46875.14	Meera, FreeMono, UnDotum, Loma, Droid Sans, Century Schoolbook L, Garuda, Arial Black, Rekha, Purisa, Ume Mincho S3, DejaVu Sans Mono, Ume UI Gothic, Trebuchet MS, Impact, Ume P Gothic C4, Ume P Gothic C5, Ume P Gothic O5, Ume P Gothic S4, Ume P Gothic S5, Droid Sans Mono, Vemana2000, Umpush, OpenSymbol, Sawasdee, URW Palladio L, FreeSerif, Ume P Mincho S3, Symbol, Comic Sans MS, URW Gothic L, Webdings, Dingbats, URW Chancery L, Phetsarath OT, Droid Sans Japanese, Ume Gothic, Ume P Mincho, Tlwg Typist, utkal, DejaVu Sans Light, Times New Roman, Norasi, Verdana, Ume Mincho, Droid Sans Fallback, DejaVu Serif Condensed, KacstOne, Symbol, Lohit Gujarati, Liberation Mono, Mallige, Bitstream Charter, Liberation Serif, DejaVu Sans Condensed, Courier 10 Pitch, Nimbus Sans L, TakaoPGothic, 文泉驛等寬微米黑, DejaVu Sans, Kedage, Kinnari, TlwgMono, Standard Symbols L, Ume UI Gothic O5, Lohit Punjabi, Nimbus Mono L, Rachana, Waree, Khmer OS, FreeSans, gargi, Nimbus Roman No9 L, DejaVu Serif, 文泉驛微米黑, TlwgTypewriter, Tlwg Typo, Arial, Droid Serif, Mukti Narrow, Lohit Bengali, Liberation Sans, Courier New, UnBatang, Khmer OS System, Saab, Andale Mono, Mukti Narrow Bold, Lohit Hindi, Ume P Gothic, URW Bookman L, Pothana2000, Ume Gothic C4, Ume Gothic C5, Ume Gothic O5, Ume Gothic S4, Ume Gothic S5, Lohit Tamil, Georgia (via Flash)
Are Cookies Enabled?	0.43	1.35	Yes
Limited supercookie test	0.93	1.9	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No

Thanks to **browserspy.dk** for the font detection code, and to **breadcrumbs** for supercookie help.

Frequently asked questions.

Send other questions or comments to **panopticlick@eff.org**.

Learn about **Panopticlick** and **web tracking.** The Panopticlick **Privacy Policy.** Learn about the **Electronic Frontier Foundation.**

A research project of the **Electronic Frontier Foundation**

So arbeitet Panopticlick

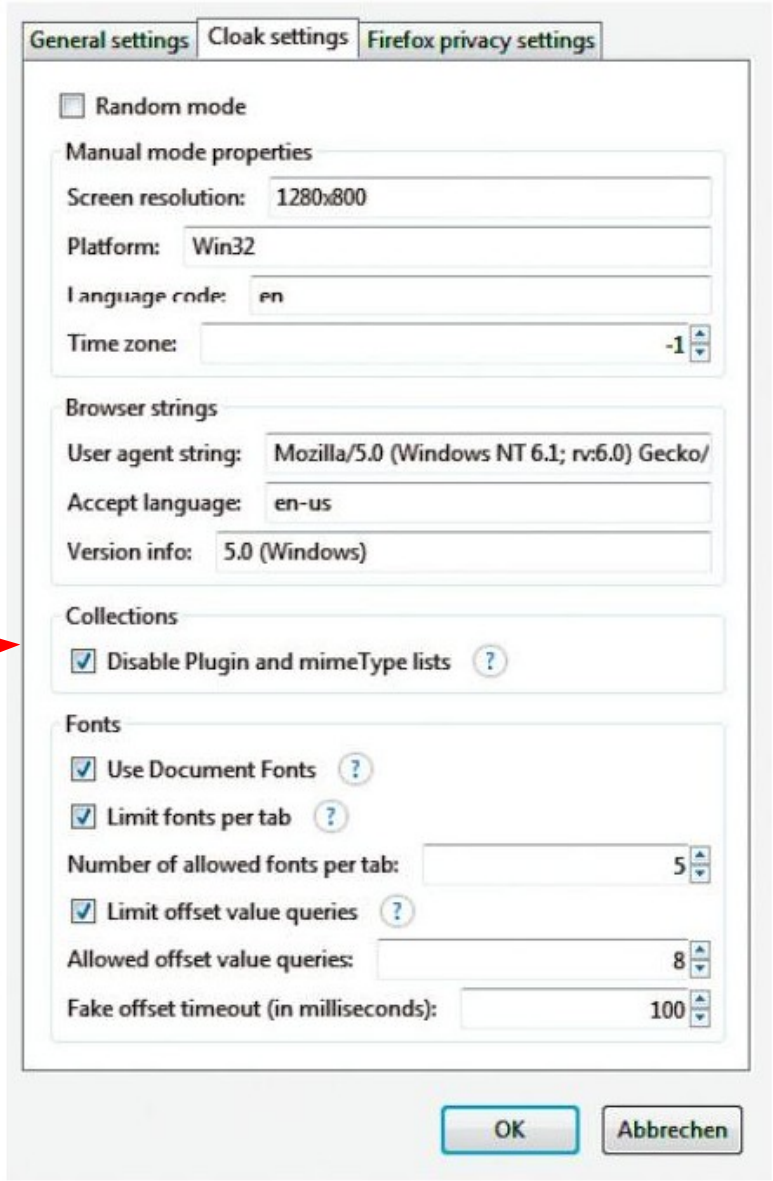
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html><head>
   <title>Panopticlick</title>
      <meta http-equiv="content-type" content="text/html; charset=UTF-8">
      <link rel="stylesheet" href="Panopticlick-Dateien/style.css" type="text/css">


         <script src="Panopticlick-Dateien/jquery-1.js" type="text/javascript"></script>
            <script src="Panopticlick-Dateien/plugin-detect-0.js" type="text/javascript"></script>
            <script src="Panopticlick-Dateien/deployJava.js" type="text/javascript"></script>
            <script src="Panopticlick-Dateien/jquery.js" type="text/javascript"></script>

 </head>
```

Übersichtsartikel „Mythos Anonymität“

- Quelle. c't 20/2013
- Neue Aspekte darin:
  - Flash Cookies (Supercookies)
  - Weitere FF-Plugins:
    - Cookie Monster (erweitertes Cookie Management)
    - FireGloves (manipuliert die Umgebungsparameter um Fingerprinting zu erschweren)
    - BetterPrivacy (deaktiviert Zugriff auf Local Storage)
  - Link auf Tor-Diskussion



Registrieren von Benutzerkennungen

- 3 Arten von E-Mail-Adressen
  - Primär: von seriösen Anbietern, die u.U. die Identität prüfen
  - Sekundär: seltener genutzt, anonym
  - Tertiär: Wegwerfadresse
- Oft sind Benutzerkennungen an die E-Mail-Adresse gebunden (oder gar identisch) → primär
  - Foren: Benachrichtigung bei Antworten
- Oder man braucht sie nur selten (z.B. bei vergessenem Passwort) → sekundär
- Oder man braucht sie nur zur Bestätigung der Registrierung → tertiär

Wegwerfadressen

- Gelten in der Regel 1 Stunde
- In dieser Zeit kann man auf der Anbieterseite Mails empfangen
- Beispiele (die ersten 4 bei Google)
  - Wegwerfemail.de
  - Byom.de
  - Wegwerfemailadresse.com
  - Squizzy.de