

Mein Browser – wie bringe ich die Plaudertasche zum Schweigen?

Ein Skript zum Vortrag der Gruppe



ITS Us.

Antje Hänzelmann (Stud. B.sc. Medieninformatik online)

Patrycja Magdalena Kupiec (Stud. B.sc. IT Sicherheit online)

Michael Georg Schmidt (Stud. B.sc. IT Sicherheit online)

der TH Lübeck



Inhaltsverzeichnis

Vorbemerkungen.....	3
1. Am I unique?.....	4
2. Cover your tracks.....	4
3. browserleaks.....	5
3.1 IP-Adresse.....	5
3.2 Canvas Fingerprint.....	6
3.3 Font Fingerprint.....	6
3.4 Social Media.....	7
4. Sicherheitseinstellungen im Browser.....	7
4.1 Datenschutz und Sicherheit.....	7
4.2 Do not track.....	7
4.3 Datenerhebung durch Firefox und deren Verwendung.....	8
4.4 Sicherheit → Schutz vor betrügerischen Inhalten und gefährlicher Software.....	8
4.5 Zertifikate.....	8
4.6 Updates.....	8
4.7 Standardsuchmaschine.....	8
4.8 Sicherer Abruf von Websites.....	8
Optional.....	8
4.9 Cookies und Website-Daten.....	8
4.10 Chronik.....	9
5. Add-ons die helfen die Privatsphäre zu schützen.....	9
5.1 uBlock Origin.....	9
5.2 I don't care about cookies.....	10
5.3 Firefox Multi Account Containers.....	12
5.4 Temporary Containers.....	12
5.5 NoScript.....	13
5.6 Referer Modifier.....	14
5.7 User Agent Switcher.....	14
5.8 Fake Filler.....	14
5.9 Tab Namen.....	15
5.9.1 Tab ReTitle.....	15
5.9.2 Custom Tab Title and Favicon.....	16
5.10 Privacy Badger.....	16
6. Einsatz von VPN.....	17
6.1 ProtonVPN.....	17
6.2 CyberGhost.....	17
6.3 CalyxVPN.....	18
6.4 Browser die VPN anbieten.....	18
6.4.1 Firefox.....	18
7. Bevorzugte Sprachen für die Darstellung von Websites wählen.....	19
8. Am I unique? - nach den Erweiterungen.....	20
9. Cover your tracks – nach den Erweiterungen.....	21
10. Browserleaks.....	22
10.1 IP-Adresse mit VPN.....	22
10.2 Canvas Fingerprint mit Add-on.....	24
10.3 Font Fingerprint mit Add-on.....	25
10.5 Social Media Login Detection mit Add-on.....	26
Quellen.....	27

Dieses Skript ergänzt den Vortrag *Mein Browser – wie bringe ich die Plaudertasche zum Schweigen?* Es zeigt auf, wie viele Daten Browser ausplaudern und was Sie dagegen machen können. Hauptsächlich geht es darum, die ausgeplauderten Daten zu verfälschen, so dass Sie möglichst nicht identifizierbar sind und Datensammler ein möglichst schlechtes, bestenfalls falsches Profil von Ihnen anlegen.

Ergänzend sind am Ende unter der Überschrift *Quellen* Links und Hinweise zu deutlich weiterführenden Informationen beigefügt. Sollten dennoch Fragen offen bleiben oder sich gar neue Fragen ergeben, stehen wir Ihnen gerne jederzeit per Threema

pkupiec@its-us.info

Z75KDBJJ

oder

mgschmidt@its-us.info

WYH86UFA

oder unter der E-Mailadresse

mail@its-us.info

zur Verfügung.

Wir hoffen, Ihnen hat der Vortrag gefallen und das Skript hilft Ihnen weiter.

Beste Grüße

ITS Us.

Bevor Sie beginnen, Ihre Identität zu schützen, sehen Sie sich an, welche Daten von Ihnen übertragen werden.

Vorbemerkungen

Die hier gegebenen Anleitungen sind *Empfehlungen*, denen Sie mit Bedacht folgen können. Alle Ausführungen beziehen sich auf den Browser *Firefox 90.0.2*. Es ist davon auszugehen, dass die hier gemachten Ausführungen noch lange Gültigkeit behalten. Für den Browser *Firefox ESR 78.12.0esr* gelten sie auch. Die ESR Version des Firefox steht für *Enhanced Service Release*. Dabei handelt es sich um eine besonders abgesicherte Version des Browsers. Das Menü sieht etwas anders aus als das „einfachen“ Firefox, aber es sollte kein Problem sein, die entsprechenden Einträge zu finden. Die gezeigten Beispiele lohnen sich nicht anzugreifen, weil sie durchweg von einer virtuellen Maschine stammen, die nur für diese Zwecke zum Einsatz kam. Dieser Rechner existiert also inzwischen gar nicht mehr.

1. Am I unique?

amiunique.org ist eine Website, welche die *EFF (Electronic Frontier Foundation)*, eine amerikanische Bürgerrechtsorganisation, zur Verfügung stellt. Sie finden Sie hier <https://amiunique.org>.



Abb. 1.1 Der Browser ist bereits hier sehr geschwätzig.

2. Cover your tracks

Auch die Website *coveryourtracks.eff.com* stellt die EFF zur Verfügung. Sie finden sie hier https://coveryourtracks.eff.org/results?&aat=1&fpi_whorls=%7B%22v2%22%3A%7B%22plugins%22%3A%22permission+denied%22%2C%22hardware_concurrency%22%3A8%2C%22audio%22%3A%2235.73833402246237%22%2C%22canvas_hash_v2%22%3A%22f139fb61b2b20249d81082f9012141dc%22%2C%22webgl_hash_v2%22%3A%2233dbdb28a8e5050332bc8f7473462c56%22%7D%7D.

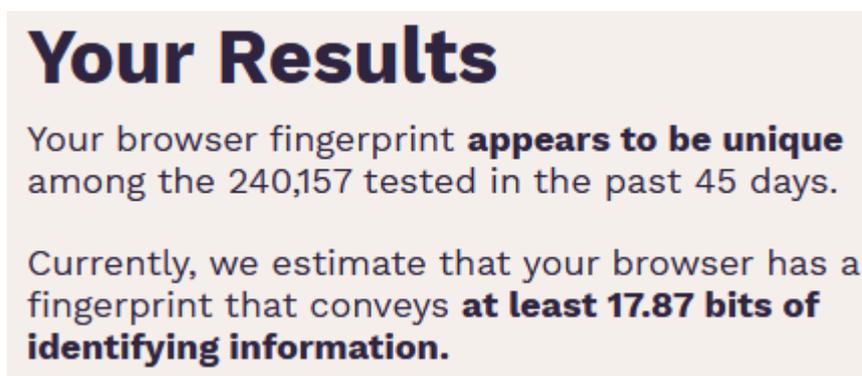


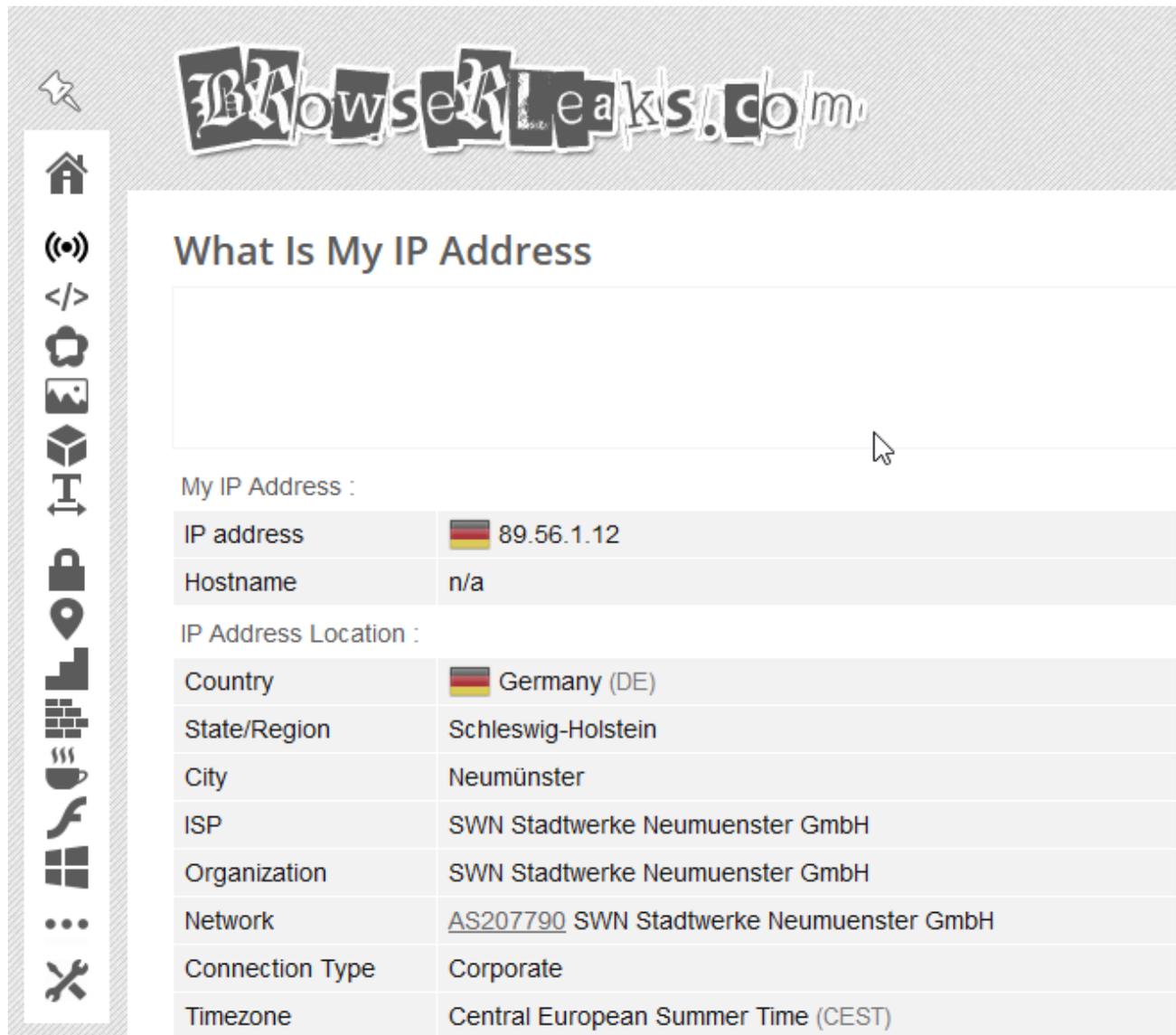
Abb. 2.1 Auch, wenn dieses Ergebnis Laien nicht viel sagt, so sind 17,87 Bit an identifizierenden Informationen sehr viel. Viel zu viel!

3. browserleaks

Die Website browserleaks.com finden Sie hier <https://browserleaks.com/>.

Browserleaks verrät eindeutige und wichtige Informationen, die Sie identifizieren können. Einige Beispiele sind

3.1 IP-Adresse



The screenshot shows the website 'Browserleaks.com' with a navigation sidebar on the left. The main content area is titled 'What Is My IP Address' and displays the following information:

My IP Address :

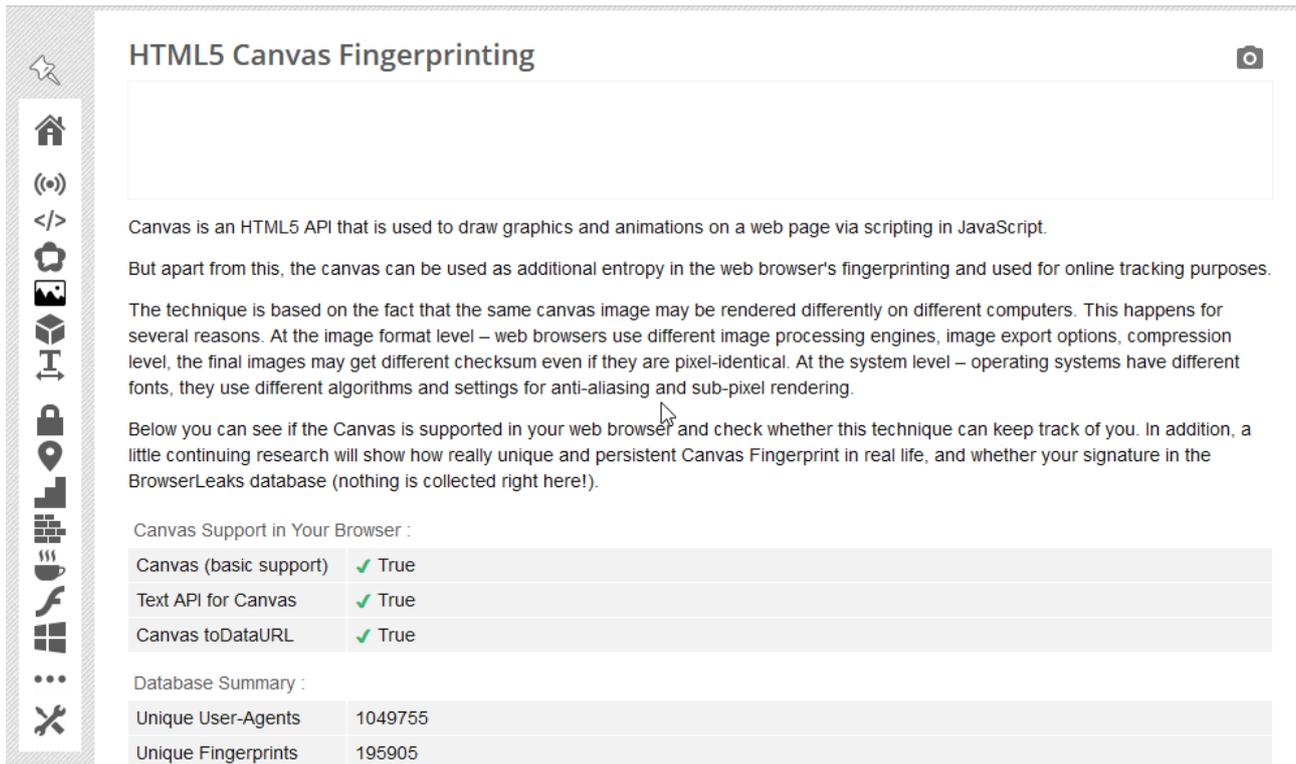
IP address	 89.56.1.12
Hostname	n/a

IP Address Location :

Country	 Germany (DE)
State/Region	Schleswig-Holstein
City	Neumünster
ISP	SWN Stadtwerke Neumuenster GmbH
Organization	SWN Stadtwerke Neumuenster GmbH
Network	AS207790 SWN Stadtwerke Neumuenster GmbH
Connection Type	Corporate
Timezone	Central European Summer Time (CEST)

Abb. 3.1.1 Die Site lässt keinen Zweifel daran, wo ich mich befinde

3.2 Canvas Fingerprint



The screenshot shows a web page with a sidebar on the left containing various icons. The main content area is titled "HTML5 Canvas Fingerprinting" and includes a large empty box at the top. Below this, there is explanatory text about the Canvas API and its use in fingerprinting. A table lists browser support for Canvas features, and a database summary shows the number of unique user-agents and fingerprints.

HTML5 Canvas Fingerprinting

Canvas is an HTML5 API that is used to draw graphics and animations on a web page via scripting in JavaScript.

But apart from this, the canvas can be used as additional entropy in the web browser's fingerprinting and used for online tracking purposes.

The technique is based on the fact that the same canvas image may be rendered differently on different computers. This happens for several reasons. At the image format level – web browsers use different image processing engines, image export options, compression level, the final images may get different checksum even if they are pixel-identical. At the system level – operating systems have different fonts, they use different algorithms and settings for anti-aliasing and sub-pixel rendering.

Below you can see if the Canvas is supported in your web browser and check whether this technique can keep track of you. In addition, a little continuing research will show how really unique and persistent Canvas Fingerprint in real life, and whether your signature in the BrowserLeaks database (nothing is collected right here!).

Canvas Support in Your Browser :

Canvas (basic support)	✓ True
Text API for Canvas	✓ True
Canvas toDataURL	✓ True

Database Summary :

Unique User-Agents	1049755
Unique Fingerprints	195905

Abb. 3.2.1 Mein Browser liefert viele Informationen in Bezug auf Canvas Fingerprinting

3.3 Font Fingerprint

Font fingerprinting techniques are based on measuring the onscreen dimensions of HTML elements filled with text pieces or single Unicode glyphs. Font rendering in web browsers is affected by many factors, and these measurements may vary slightly.

Fonts Enumeration attack is a brute-force method that tries different fonts from a sizeable font-family dictionary. If the rendered element's size differs from the default values, it means that the substituted font is present in the system. The Unicode Glyphs Measurement does almost the same job. Instead of a text line, it uses single, specifically selected Unicode characters with a large font-size, and uses only default letterforms as a font-family. Fingerprints are formed after hashing the obtained measurement results.

Fonts Enumeration :

Fingerprint	✓ 978756816352C0667E55E21B4E0BA692
Report	102 fonts and 88 unique metrics found
	<pre>4512,143 default, sans-serif, fantasy 4431,142 serif 4097,145 monospace 4562,178 cursive 5317,181 Arial Black 4581,128 Bahnschrift</pre>

Abb. 3.3.1 Auch die Schriften die mein Browser verwendet helfen, mich zu identifizieren

3.4 Social Media

Browser Security Test :

Third-Party Cookies ! Allowed – You can be vulnerable to this attack.

Tracking Protection ✓ Found – You may have protected against some templates of this attack.

You are logged in to:

✓ Nothing Found

You are not logged in to:

Twitter	Facebook	Reddit	Square	Khan Academy
VK	500px	Foursquare	Steam	Academia.edu
Twitch	Expedia	Paypal	IMDb	Hackernews
BitBucket	Github	Slack	Medium	EdX
Spotify	Indeed	Dropbox	Carbonmade	Battle.net
Meetup	Airbnb	Craigslist	Blogger	Youtube
Gmail	Disqus	Amazon.com	Tumblr	Skype
Pinterest				

Abb. 3.5.1 Auch *nicht* eingeloggte Social Media helfen Angreifern. Dort muss mich keiner suchen

4. Sicherheitseinstellungen im Browser

Alle Angaben beziehen sich auf das Einstellungsmenü, das Sie über **Extras → Einstellungen** erreichen. Unter Linux ist dieses Menü oft über **Bearbeiten → Einstellungen** erreichbar.

4.1 Datenschutz und Sicherheit

Gehen Sie dafür auf den Punkt

Extras → Einstellungen → Datenschutz & Sicherheit

Wählen Sie hier unter dem Punkt **Verbesserter Schutz vor Aktivitätsverfolgung** die Option *Strong* aus.

Anschließend klicken Sie auf den Button *Alle Tabs neu laden*.

Die Warnung die Firefox ausgibt können Sie ignorieren, da in den meisten Fällen keine Einschränkungen entstehen. Sollte dies doch einmal geschehen, wählen Sie an dieser Stelle den Button *Ausnahmen verwalten* und fügen die betreffende Website als Ausnahme hinzu.

4.2 Do not track

Bei *Do not track* handelt es sich um eine Aufforderung an die Betreiber:innen von Websites, deren Befolgung freiwillig ist. Dieses Projekt gilt als gescheitert.

4.3 Datenerhebung durch Firefox und deren Verwendung

Nehmen Sie unter der Überschrift *Datenerhebung durch Firefox und deren Verwendung* alle Häkchen heraus. Ihre Daten gehen nur Sie selbst etwas an.

4.4 Sicherheit → Schutz vor betrügerischen Inhalten und gefährlicher Software

Setzen Sie hier bei allen Punkten einen Haken.

4.5 Zertifikate

Setzen Sie den Punkt bei *Automatisch eins wählen* und einen Haken bei *Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen*.

4.6 Updates

Sie sollten dafür sorgen, dass Ihr Browser immer auf dem aktuellsten Stand ist. Deshalb setzen Sie bei *Allgemein → Firefox Updates → Firefox erlauben → Updates automatisch zu installieren (empfohlen)* ein Häkchen.

4.7 Standardsuchmaschine

Standardmäßig ist bei Firefox Google als Suchmaschine eingestellt. Das ist nicht empfehlenswert, da Google massiv Daten sammelt. Gehen Sie auf *Suche → Standardsuchmaschine* und ändern sie diese am besten auf *DuckDuckGo*.

Wenn Sie mit DuckDuckGo nicht so ganz glücklich sind, können Sie unter dem Punkt *Startseite* auch jede beliebige andere Suchmaschine, wie vielleicht *startpage.com* eintragen.

4.8 Sicherer Abruf von Websites

Damit niemand mitlesen kann, welche Site Sie gerade anfragen, sollten Sie auf den Punkt *Allgemein* → *Verbindungseinstellungen (Einstellungen)* gehen und hier einen Haken bei *DNS über HTTPS* setzen. Dann sendet Firefox Ihre Anfragen ausschließlich über Leitungen, die mit *TLS (Transport Layer Security)* verschlüsselt sind.

Optional

4.9 Cookies und Website-Daten

Wenn Sie die folgende Funktion wählen, löschen Sie sämtliche Daten, die Ihr Browser gespeichert hat. Auch Cookies, die dafür sorgen, dass Sie sich bei einigen Websites nicht mehr manuell anmelden müssen. Daher überlegen Sie, ob Sie das wollen.

Datenschutz & Sicherheit → Cookies und Websitedaten → Daten entfernen

4.10 Chronik

Wenn Sie die Chronik auf *niemals anlegen* stellen, entspricht das dem Aufruf des *privaten Modus*. In diesem Modus zeigt Firefox die *Icons* der hier erwähnten Add-ons nicht an. Sie können diese anzeigen lassen, indem Sie unter *Extras* → *Add-ons* alle Add-ons einzeln anklicken und unter dem Reiter *Details* bis nach unten scrollen und dort den Button *Im privaten Fenster ausführen – erlauben* anklicken. Diesen Vorgang müssen Sie für alle Add-ons einzeln durchführen. Um die *Container Add-ons Firefox Multi Container* und *Temporary Container* nutzen zu können, müssen Sie unter *Extras* → *Optionen* → *Datenschutz & Sicherheit* → *Chronik* das Häkchen bei *Immer den privaten Modus verwenden* entfernen. Nehmen Sie auch beim Menüpunkt *Adressleiste* alle Häkchen heraus.

Datenschutz & Sicherheit → *Chronik*

Hier gibt es zwei wichtige Funktionen. Die erste betrifft das Anlegen einer Chronik. Standardmäßig geschieht dies. Um zu vermeiden, dass Unbefugte sehen, wo Sie gesurft haben, sollten Sie bei

Firefox wird eine Chronik anlegen **niemals**

auswählen.

Wenn Sie diese Funktion wählen, löschen Sie Ihre gesamte Browser / Surf-Historie.

Datenschutz & Sicherheit → *Chronik löschen*

5. Add-ons die helfen die Privatsphäre zu schützen

5.1 uBlock Origin

Ublock Origin ist eine Browser Erweiterung, die es seit 2015 als uBlock Origin für mehrere Browser



gibt. Ihre Geschichte hat 2014 als uBlock begonnen und startete mit den Browsern Chrome und Opera. Das Add-on verwaltet *Blocklisten* mit Informationen über Seiten, Skripte, Anbieter und ähnliches, welche die Privatsphäre der Internetnutzer bedrohen. Es ist eine Open Source Software, die der Gründer und Entwickler Raymond Hill von Anfang an betreut.



Abb. 5.1.1 Das uBlock Origin Logo

Abb. 5.1.2 Das uBlock Origin Bedienfeld

5.2 I don't care about cookies

I don't care about cookies ist ein Add-on, das sich um so genannte *Consent Banner* kümmert. Consent Banner sind die Pop-up Fenster die beim Aufruf vieler Webseiten erscheinen, um einen aufzufordern doch alle Cookies anzunehmen. Alternativ kann man auch oft die Einstellungen selber anpassen. Das lohnt sich in der Regel, da man so auf viele Schnüffler verzichten kann. Lästig ist es dennoch. *I don't care about cookies* wählt die nutzerfreundlichsten Einstellungen automatisch und verhindert so, dass das Consent Banner überhaupt erst erscheint.

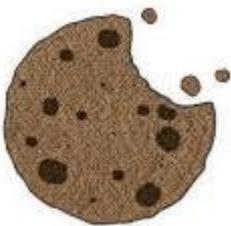


Abb. 5.2.1 I don't care about cookies

Im Vergleich

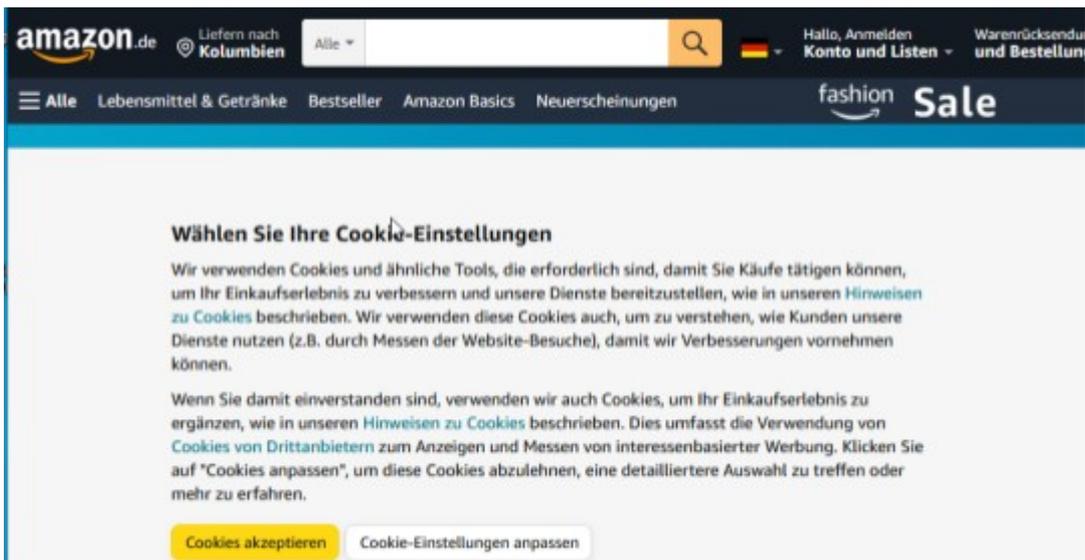


Abb. 5.2.1 Aufruf der Site ohne das Add-on *I don't care about cookies*

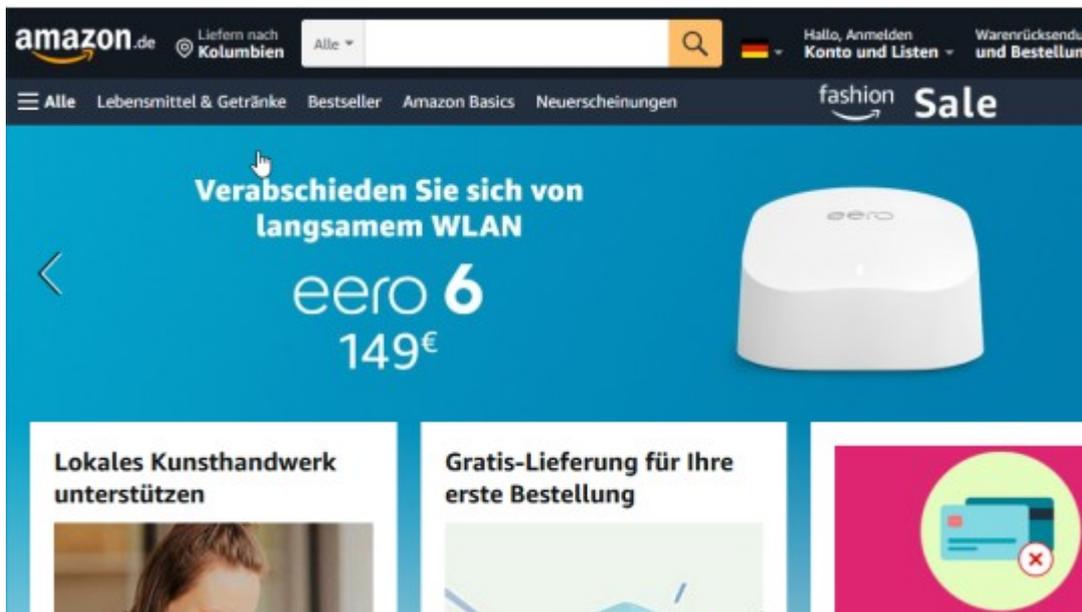


Abb. 5.2.2 Mit dem Add-on *I don't care about cookies* kommt man gleich ans Ziel

5.3 Firefox Multi Account Containers

Firefox Multi Account Containers ist ein Add-on, das *Mozilla* selbst entwickelt. Es stellt *Firefox* so genannte *Container* zur Verfügung, in denen die Nutzer:innen Websites zusammenfassen können, um sie in den entsprechenden Containern zu öffnen. Das Add-on bringt von sich aus einige Container wie *Arbeit*, *Banking*, *Shopping* und *Freizeit* mit. Jedoch kann man beliebig viele eigene Container erstellen, um häufig genutzte Sites darin zusammenzufassen. Dafür gibt es den Button *Manage Containers*.

Das hat den Vorteil, dass die Websites die man für die Arbeit braucht, nicht „sehen können“ welche Websites man in der Freizeit aufruft und welche Cookies diese speichern. Oder, dass der Sportverein nicht weiß, nach welchen Krankheiten man gesucht hat.



Abb. 5.3.1 Firefox Multi Account Containers

Es könnte sinnvoll sein, alle Sites zum Thema IT Security in einen Container zu packen.



Abb. 5.3.2 Eine IT Security Site im *IT Security* Container – zu erkennen in der URL-Zeile oben rechts, links des blauen Punkts

5.4 Temporary Containers

Temporary Containers ist ein Add-on, das alle aufgerufenen Websites in Container packt, sofern sie nicht von *Firefox Multi Account Containers* bereits kategorisiert wurden. Das hat den Vorteil, dass die aufgerufenen Websites den geringstmöglichen Zugriff auf Ihre Daten erlangen. 15 Minuten nachdem die Nutzer:innen eine Site verlassen haben, löscht *Temporary Containers* alle Daten, die damit in Zusammenhang stehen von sich aus.



Abb. 5.4.1 Temporary Containers

Es geht niemanden etwas an, wann ich wohin mit der Bahn fahren will. Daher ist *Temporary Containers* für den Aufruf von *bahn.de* eine gute Idee.

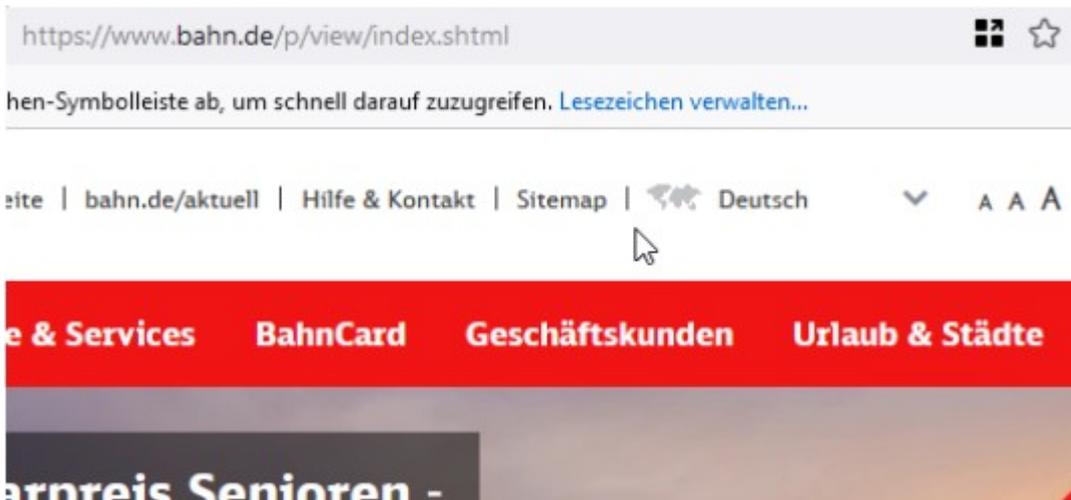


Abb. 5.4.2 Die Site der Bahn in *Temporary Containers* aufgerufen

5.5 NoScript

NoScript ist ein Klassiker. Das Programm verhindert die Ausführung von Skripten auf Websites. Das erhöht die Sicherheit beim Surfen erheblich, ist jedoch zunächst äußerst lästig, denn ständig laden Inhalte oder ganze Seiten nicht. Dann ist die Nutzer:in gefragt, von Hand Skripte freizugeben. Das kann einmalig aber auch dauerhaft geschehen. So lernt *No Script* mit der Zeit, was „gut“ ist und verhindert irgendwann nur noch Skripte, die für die Nutzer:innen nicht von Vorteil sind.



Abb. 5.5.1 *NoScript*



Abb. 5.5.2 *NoScript* hindert amazon daran einige Skripte auszuführen

5.6 Referer Modifier

Referer Modifier ist ein Add-on, das dafür sorgt, dass die aktuell aufgerufene Website nicht erfährt, auf welcher Website die Nutzer:in vorher war. Standardmäßig überträgt der Browser diese Information an die aktuell aufgerufene Website. Referer Modifier fälscht diese Informationen.



Abb. 5.6.1 Referer Modifier

5.7 User Agent Switcher

User Agent Switcher ist ein Add-on, das die Möglichkeit bietet, sowohl die Angaben über das Betriebssystem – Windows, Mac, Linux oder andere – als auch den verwendeten Browser zu fälschen. Es steht jeweils eine Vielzahl von Alternativen zur Verfügung.



Abb. 5.7.1 User Agent Switcher

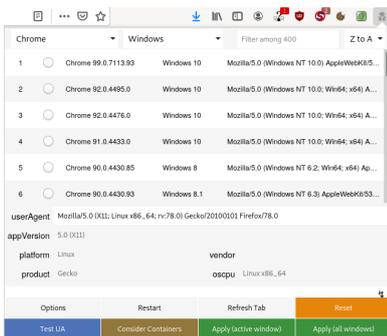


Abb. 5.7.2 Das Menü des *User Agent Switchers*

5.8 Fake Filler

Fake Filler ist ein Add-on, das den Nutzern hilft Formulare auszufüllen. Einige Websites verlangen das, bevor man an die eigentlichen Informationen gelangt. Fake Filler sorgt dafür, dass diese Angaben garantiert falsch sind.



Abb. 5.8.1 Fake Filler

SWN
Städtische Wasserwerke

Kontakt

Frau Herr

Vorname*
Tallulah Booker

Nachname
Kim Kim

Straße/Nr.
Et deserunt in archi

PLZ
In sed dolor ipsam q

Ort
Magni praesentium nu

E-Mail*
diho@mailinator.com

Telefon*
+1 (515) 964-3844

Abb. 5.8.2
Fakefiller füllt

das Formular perfekt falsch aus

5.9 Tab Namen

Es gibt Situationen in denen es unangenehm sein könnte, wenn jemand bei einem Blick über die Schulter sieht, welche Tabs im Browser geöffnet sind. Die vorgestellten Add-ons helfen dabei, die Namen zu fälschen, jedoch gibt es entscheidende Unterschiede.

5.9.1 Tab ReTitle

Tab ReTitle ist ein Add-on, das den Namen eines aufgerufenen Tabs einfach ändern lässt. So steht dann auf dem Tab, der Amazon aufgerufen hat Wikipedia. Das schützt die Privatsphäre auf einfache und schnelle Art. Die Nutzer:innen können die Namen der Tabs frei wählen.

Ein Manko bei diesem Add-on ist jedoch, dass es die Favicons – die kleinen Bildchen, die eine Website identifizieren – nicht mit ändert. So hätte Wikipedia das Favicon von Amazon – das ist wenig hilfreich.



Abb. 5.9.1.1 Tab ReTitle

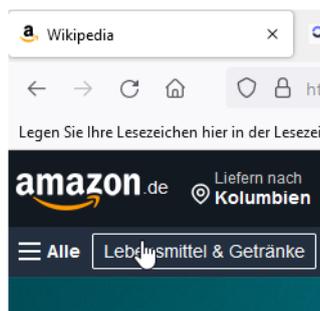


Abb. 5.9.2.2 Der Tab heißt *Wikipedia*, das Favicon ist jedoch noch immer *amazon*

5.9.2 Custom Tab Title and Favicon

Custom Tab Title and Favicon ist ein Add-on, das etwas mehr Aufwand erfordert, aber dafür feste Regeln zur Verfügung stellt. Mit Custom Tab Title and Favicon können Sie auch das Favicon ändern, so dass nach einer selbst definierten Regel bei Amazon nicht nur Wikipedia steht, sondern auch das Favicon von Wikipedia zu sehen ist. Das ist schließlich das, was eine dritte Person als erstes in den Blick bekommt.



Abb. 5.9.2.1 Custom Tab Title and Favicon

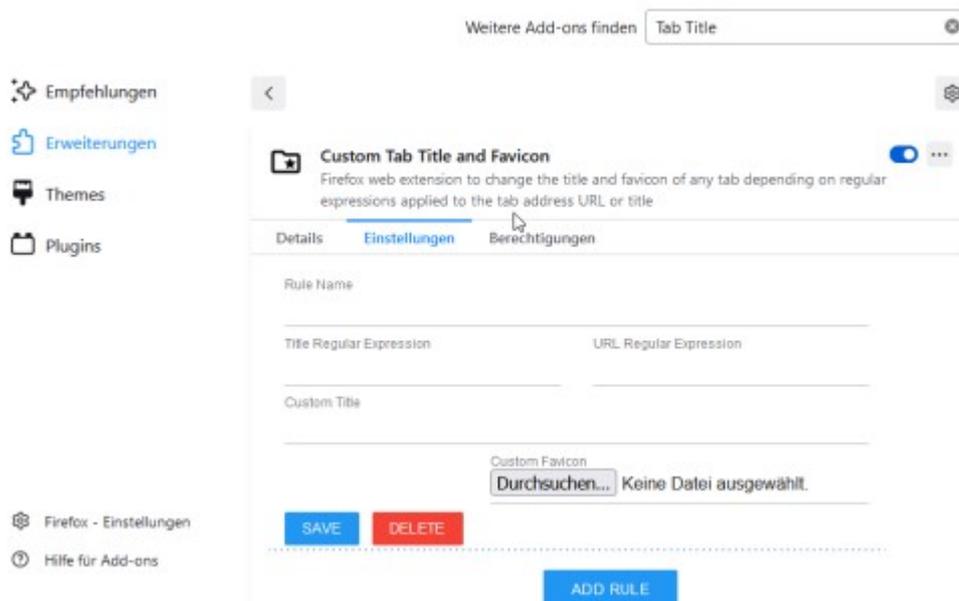


Abb. 9.2.2
Dieses Add-on

macht es möglich, auch das Favicon anzupassen

5.10 Privacy Badger

Privacy Badger ist ein Add-on, das sich ausgeklügelt um die Privatsphäre der Nutzer:innen kümmert. Privacy Badger blockiert keine Websites an Hand von Listen, sondern lernt selbstständig. Taucht ein Tracker zum dritten mal beim Einsatz des Privacy Badgers auf, blockiert er automatisch Websites, die diesen Tracker einbinden. Zusätzlich teilt das Add-on allen Websites von sich aus mit, dass die Nutzer:innen nicht – in keiner Form – getrackt werden wollen.

Es ist ein Klassiker der EFF (Electronic Frontier Foundation – eine amerikanische Bürgerrechtsorganisation), die bekannt für ihre wirksamen und ausgeklügelten Tools ist.



Abb. 5.10.1 Privacy Badger

6. Einsatz von VPN

VPN steht für *Virtual Private Network*. Dabei handelt es sich um eine Technik, die es möglich macht, sichere, verschlüsselte *Ende zu Ende (E2EE - End-to-End-Encryption)* Verbindungen über unsichere Netzwerke wie das Internet herzustellen. Wenn Sie im Internet surfen, können bis zu 40 *Hops (Zwischenstationen)* zwischen Ihnen und dem aufgerufenen Ziel liegen. Das sind alles potentielle Angreifer. Ein VPN schließt das aus, indem es Direktverbindungen herstellt, die besonders gut gesichert sind.

Der Schwachpunkt eines VPN ist immer der Anbieter, denn dem muss die Nutzer:in vertrauen. Der Anbieter könnte nämlich sämtlichen Datenverkehr mitschneiden.

Sowohl ProtonVPN als auch CyberGhost bieten ihre kostenpflichtigen Pakete für mehrere Geräte an. Damit können Sie sowohl Ihren Rechner, das Smartphone, den Fernseher, die Telefonanlage ... absichern. ProtonVPN hat jedoch auch ein kostenloses Angebot im Portfolio (Stand 12.11.2021 - <https://account.protonvpn.com/signup/account>)

6.1 ProtonVPN

ProtonVPN ist ein Anbieter von VPN der in der Schweiz ansässig ist. Das ist für die Nutzer:innen von Vorteil, weil die Schweiz sehr strikte Datenschutzbestimmungen hat. Es ist aus einem Projekt des Forschungszentrums CERN – hier geht es um Atomforschung – entstanden. Die dortigen Forscher hatten das Bedürfnis ihre Erkenntnisse mit höchster Sicherheit transportieren zu können.

ProtonVPN gibt es in einer kostenlosen und in kostenpflichtigen Versionen.



Abb. 6.1.1 ProtonVPN

6.2 CyberGhost

CyberGhost ist eine deutsche Firma, die vor einigen Jahren nach Rumänien übersiedelt ist.

CyberGhost bietet ein ganzes Paket an Schutzfunktionen an. Neben dem VPN buchen Sie mit einem Account auch weitere sinnvolle Tools, die Ihre Privatsphäre im Internet schützen.

CyberGhost bietet immer wieder Rabatte von bis zu 83% an. Es lohnt sich also möglicherweise ein wenig zu warten, bis der Preis günstig ist.



Abb. 6.2.1 CyberGhost

6.3 CalyxVPN

CalyxVPN ist ein Angebot des *Calyx Institute*, das ein amerikanischer ISP (Internet Service Provider) gegründet hat, nachdem er einen *NSA Letter* erhalten hatte. Er sollte Daten eines Kunden herausgeben und durfte darüber nicht reden. Das hat ihn dazu bewogen, den Betrieb einzustellen und ein Institut zu gründen, das sich für die Privatsphäre von Menschen einsetzt.

Soweit die bekannte Geschichte. Calyx ist in den USA ansässig, wo es faktisch keinen Datenschutz für Ausländer gibt. Daher muss jede:r für sich selbst entscheiden, ob es ein kostenloses VPN wert ist, sich diesem Risiko auszusetzen. Dies ist **keine** Bewertung von CalyxVPN, was durchaus sehr gut sein kann.



Abb. 6.3.1 CalyxVPN

6.4 Browser die VPN anbieten

6.4.1 Firefox

Mozilla bietet die kostenlose Möglichkeit ein *VPN* zu nutzen. Natürlich ist auch *Mozilla* in den USA beheimatet, jedoch deutlich bekannter als *Calyx*. Auch hier gilt, dass jede:r für sich selbst entscheiden muss, was das Richtige ist. Sie finden den Zugang hier

<https://www.mozilla.org/de/products/vpn/>.



Sicher, schnell und zuverlässig – auf jedem Gerät, egal wo du bist.

Ein Virtuelles Privates Netzwerk von den Machern von Firefox.

Jetzt Mozilla VPN nutzen

30 Tage Geld-zurück-Garantie



Abb. 6.4.1.1 Das Mozilla VPN

Mozilla bietet auch kostenpflichtige VPN-Optionen an. Dahinter soll sich der schwedische Anbieter *Mullvad* verbergen, der einen guten Ruf genießt – <https://mullvad.net/de/>. Es könnte sich lohnen, die Preise von *Firefox* und *Mullvad* zu vergleichen.

7. Bevorzugte Sprachen für die Darstellung von Websites wählen

Wie Sie bereits gesehen haben, werten Skripte auch aus, welche Sprache Sie für Ihren Browser bevorzugen. Dies ist eine wichtige Information, weil damit in den meisten Fällen ein Rückschluss auf das Herkunftsland der Nutzer:innen möglich ist.

Deshalb empfiehlt es sich, auch diese Information zu verfälschen.

Gehen Sie dafür auf *Extras* → *Einstellungen* → *Allgemein* → *Sprache* → *Bevorzugte Sprache für die Darstellung von Websites wählen*

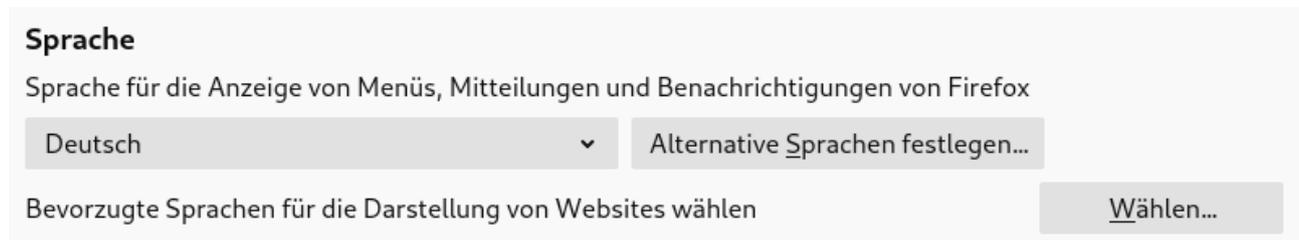


Abb. 7.1 Bevorzugte Sprache wählen

Klicken Sie auf den Button *wählen* und suchen Sie sich eine Sprache aus, die **nicht** der Sprache des Landes entspricht in dem Sie sich hauptsächlich aufhalten. Achten Sie jedoch darauf, dass Sie eine Sprache wählen, deren Buchstaben Sie kennen, nicht dass Sie, wenn etwas schief geht, nicht einmal die Zeichen lesen können.

In der Regel dürfte diese Einstellung für Sie keine Rolle spielen, da Sie vermutlich vor allem Websites aufrufen, die originär die von Ihnen bevorzugte Sprache verwenden.

8. Am I unique? - nach den Erweiterungen

Nachdem wir einige Add-ons installiert und Einstellungen vorgenommen haben, ist der Browser zwar immer noch „einzigartig“, aber er erzählt ganz andere Dinge als vorher.

Im Vergleich

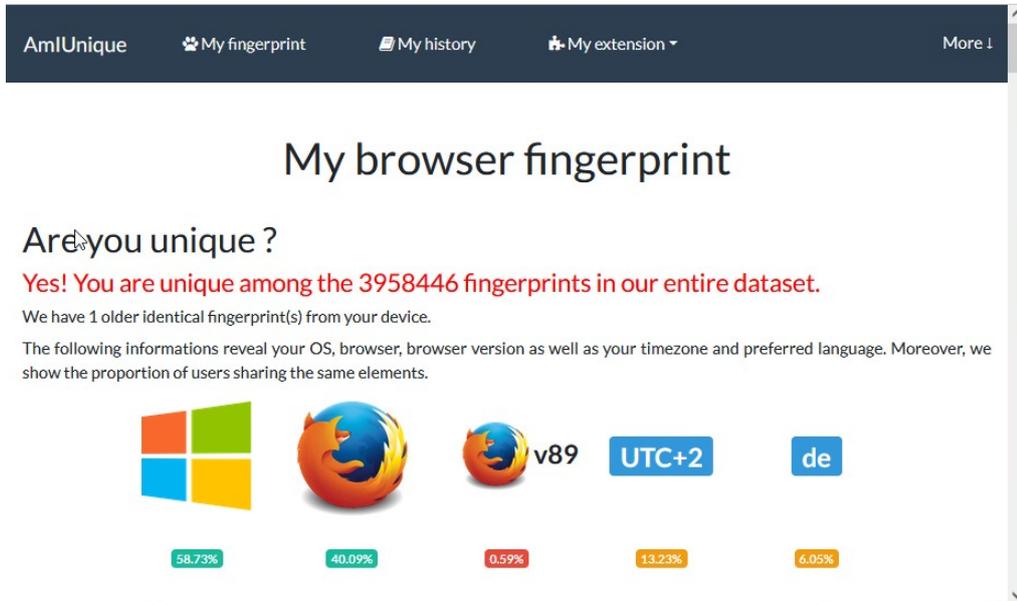


Abb. 8.1 Am I unique mit realen

Angaben

My browser fingerprint

Are you unique ?

Yes! You are unique among the 3960187 fingerprints in our entire dataset.

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users sharing the same elements.

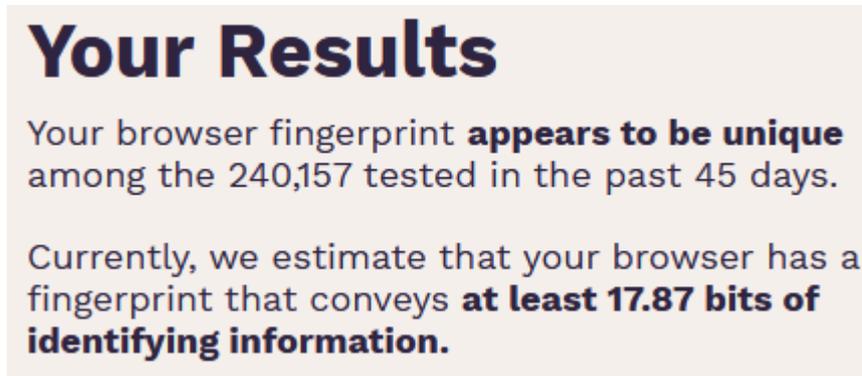


Abb. 8.2 Am I unique nach den Veränderungen – achten Sie auf die Sprache „da“. Nur noch No JS stimmt überein. Es steht für kein Java Script

9. Cover your tracks - nach den Erweiterungen

Auch *Cover your tracks* kommt zu einem ganz anderen Ergebnis.

Im Vergleich



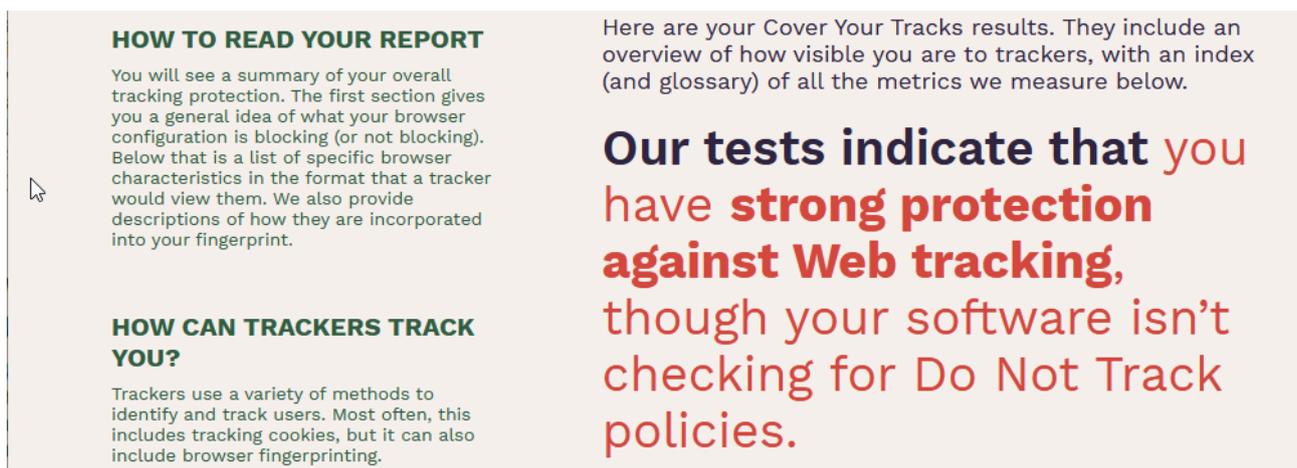
Your Results

Your browser fingerprint **appears to be unique** among the 240,157 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.87 bits of identifying information.**

Abb. 9.1 *Cover your tracks* im

Auslieferungszustand des Browsers



HOW TO READ YOUR REPORT

You will see a summary of your overall tracking protection. The first section gives you a general idea of what your browser configuration is blocking (or not blocking). Below that is a list of specific browser characteristics in the format that a tracker would view them. We also provide descriptions of how they are incorporated into your fingerprint.

HOW CAN TRACKERS TRACK YOU?

Trackers use a variety of methods to identify and track users. Most often, this includes tracking cookies, but it can also include browser fingerprinting.

Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

Our tests indicate that you have strong protection against Web tracking, though your software isn't checking for Do Not Track policies.

Abb. 9.2 *Cover your tracks* nach den Veränderungen

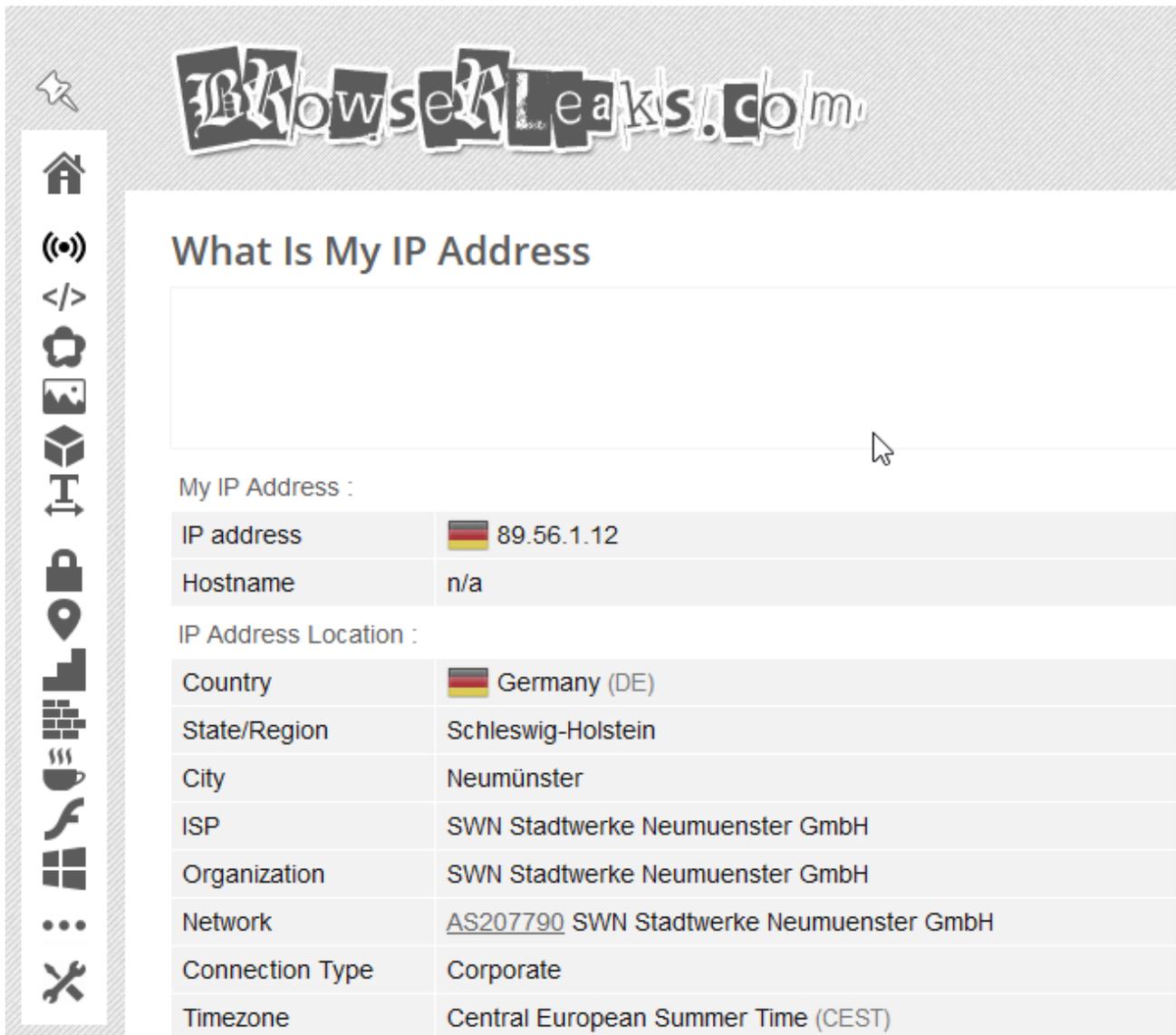
10. Browserleaks

Browser Leaks verrät wesentlich weniger an Informationen, nach den Umstellungen

10.1 IP-Adresse mit VPN

Ursprünglich war ich ohne VPN im Internet unterwegs. Der Test gab den genauen Standort preis.

Im Vergleich



The screenshot shows the website 'Browserleaks.com' with a navigation sidebar on the left containing icons for home, signal strength, code editor, chat, image, 3D, I/O, lock, location, keyboard, coffee, mouse, window, and tools. The main content area is titled 'What Is My IP Address' and displays the following information:

My IP Address :

IP address	 89.56.1.12
Hostname	n/a

IP Address Location :

Country	 Germany (DE)
State/Region	Schleswig-Holstein
City	Neumünster
ISP	SWN Stadtwerke Neumuenster GmbH
Organization	SWN Stadtwerke Neumuenster GmbH
Network	AS207790 SWN Stadtwerke Neumuenster GmbH
Connection Type	Corporate
Timezone	Central European Summer Time (CEST)

Abb. 10.1.1 Der Browser verrät viel zu viele Details



What Is My IP Address

My IP Address :

IP address	 45.144.227.9
Hostname	n/a

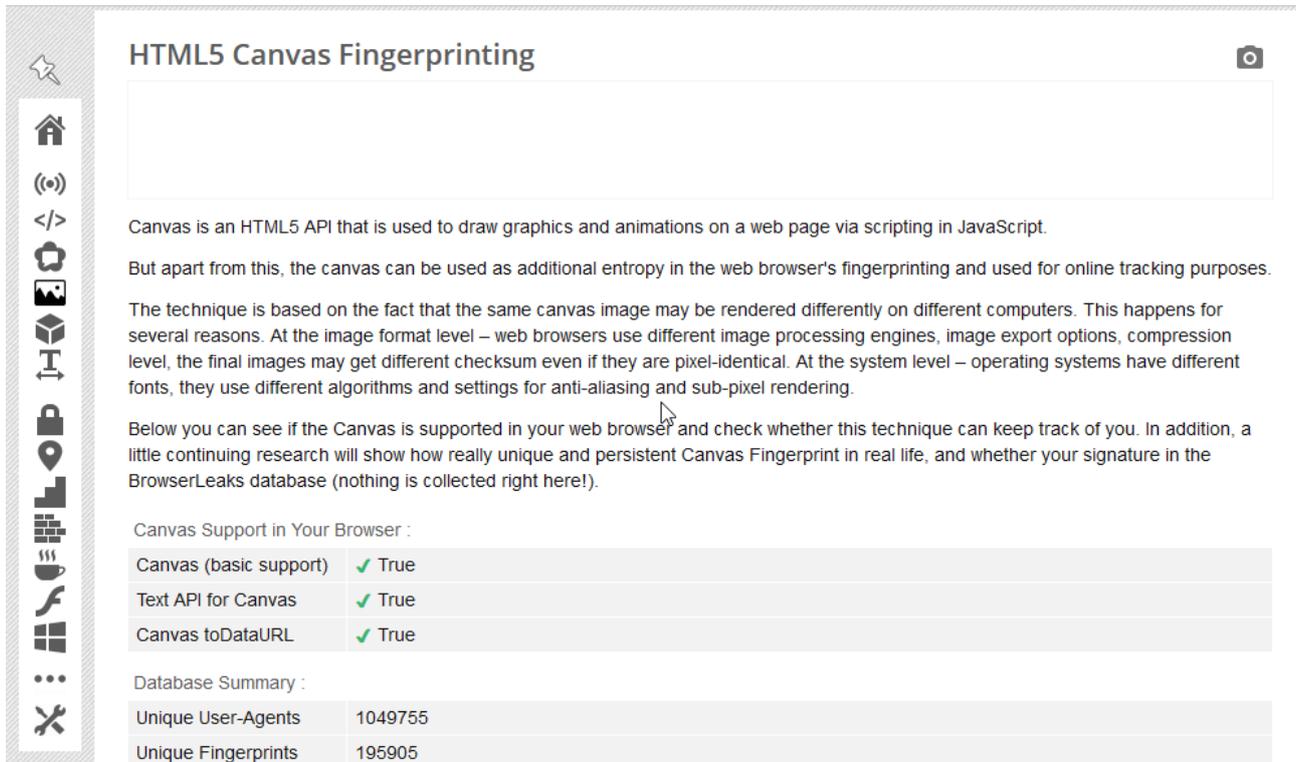
IP Address Location :

Country	 Colombia (CO)
State/Region	Bogota D.C.
City	Bogotá
ISP	Des Capital B.V.
Network	AS213035 Des Capital B.V.
Connection Type	Corporate
Timezone	Colombia Time (COT)
Local Time	Tue, 03 Aug 2021 05:44:20 -0500
Coordinates	4.7110,-74.0721

Abb. 10.1.2 Das VPN versetzt mich nach Kolumbien - Bogota

10.2 Canvas Fingerprint mit Add-on

Im Vergleich



The screenshot shows the 'HTML5 Canvas Fingerprinting' tool interface. On the left is a vertical toolbar with various icons. The main content area has the title 'HTML5 Canvas Fingerprinting' and a camera icon in the top right. Below the title is a large empty white box. The text explains that Canvas is an HTML5 API used for drawing graphics and animations, and that it can be used as additional entropy in web browser fingerprinting. It details how the technique works based on differences in image processing engines, compression levels, and system-level settings like fonts and anti-aliasing. Below this, it offers to check browser support and track the user's signature in the BrowserLeaks database. Two tables are displayed: 'Canvas Support in Your Browser' and 'Database Summary'.

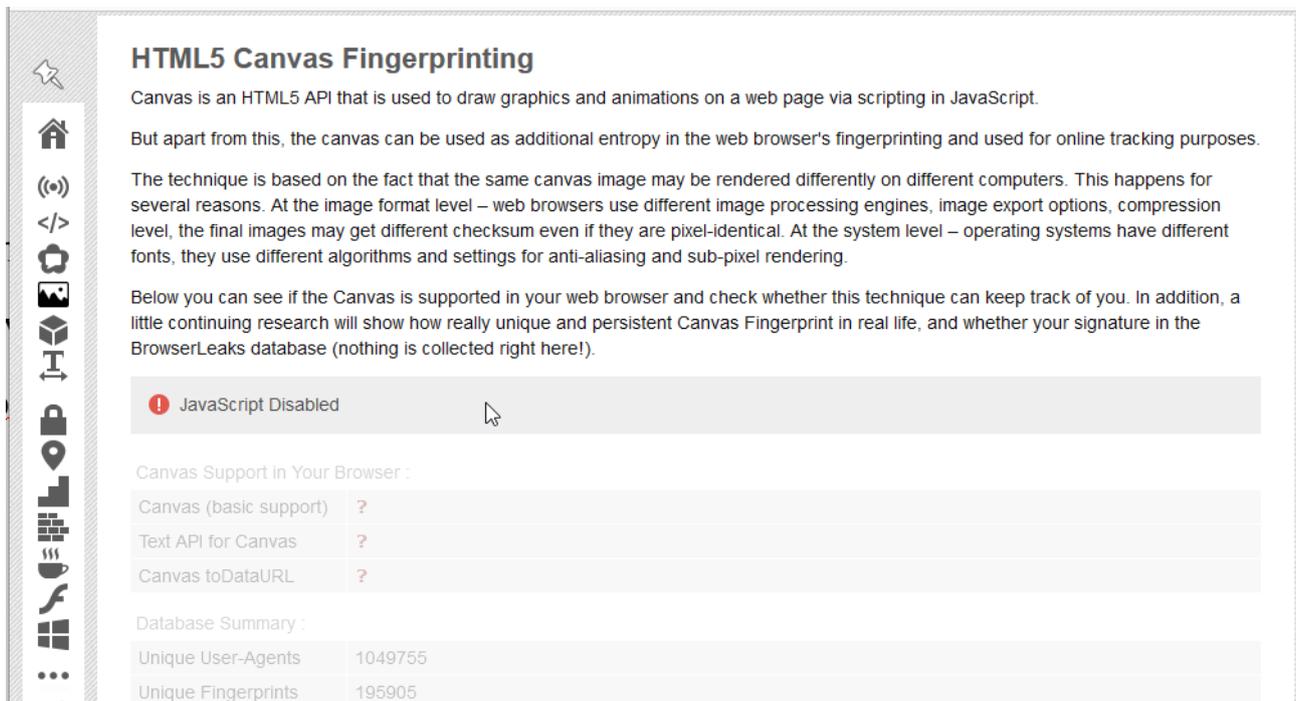
Canvas Support in Your Browser :

Canvas (basic support)	✓ True
Text API for Canvas	✓ True
Canvas toDataURL	✓ True

Database Summary :

Unique User-Agents	1049755
Unique Fingerprints	195905

Abb. 10.2.1 Canvas Fingerprinting im Auslieferungszustand



This screenshot shows the same 'HTML5 Canvas Fingerprinting' tool interface, but with JavaScript disabled. A prominent grey notification bar at the top of the content area reads 'JavaScript Disabled' with a red exclamation mark icon. The text and tables are identical to the previous screenshot, but the 'Canvas Support in Your Browser' table now shows question marks instead of checkmarks, indicating that the tool cannot determine support without JavaScript.

JavaScript Disabled

Canvas Support in Your Browser :

Canvas (basic support)	?
Text API for Canvas	?
Canvas toDataURL	?

Database Summary :

Unique User-Agents	1049755
Unique Fingerprints	195905

Abb. 10.2.2 Das Canvas Fingerprinting ist sehr schweigsam

10.3 Font Fingerprint mit Add-on

Auch installierte Schriften können eine Nutzer:in identifizieren. Das ist dann das *Font Fingerprinting*.

Im Vergleich

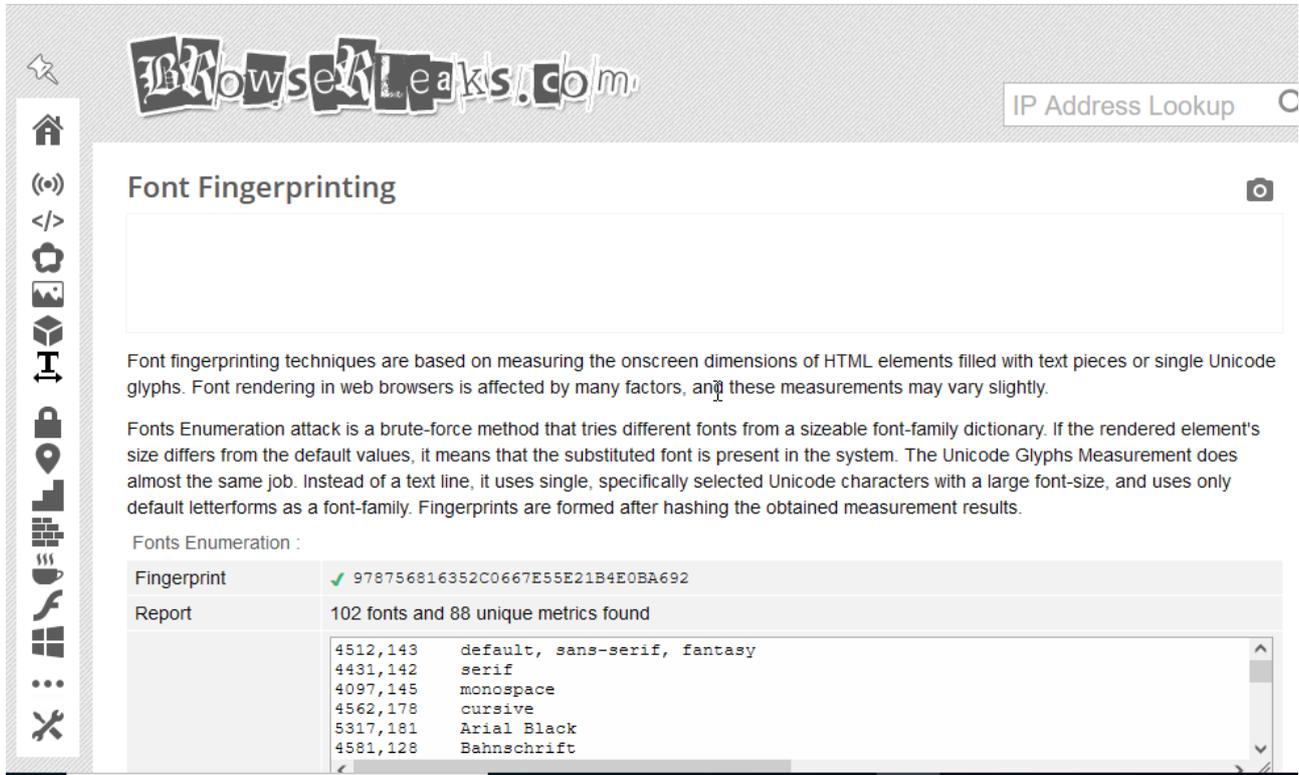


Abb. 10.3.1 browserleaks erkennt viele installierte Schriften

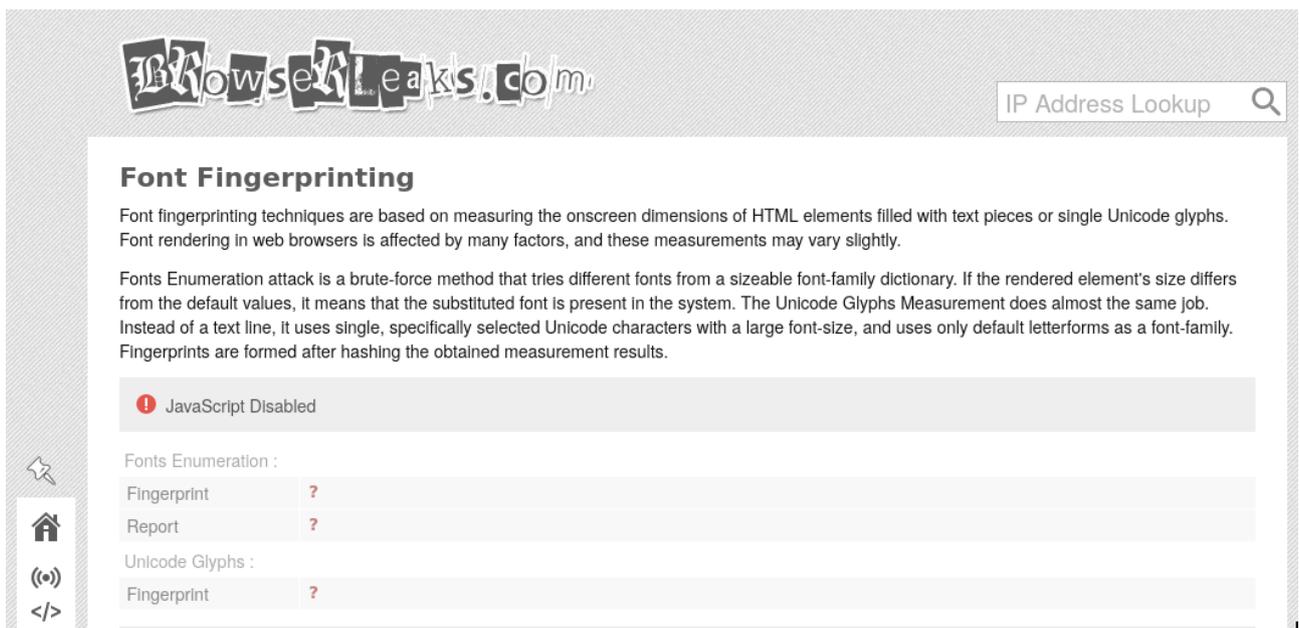
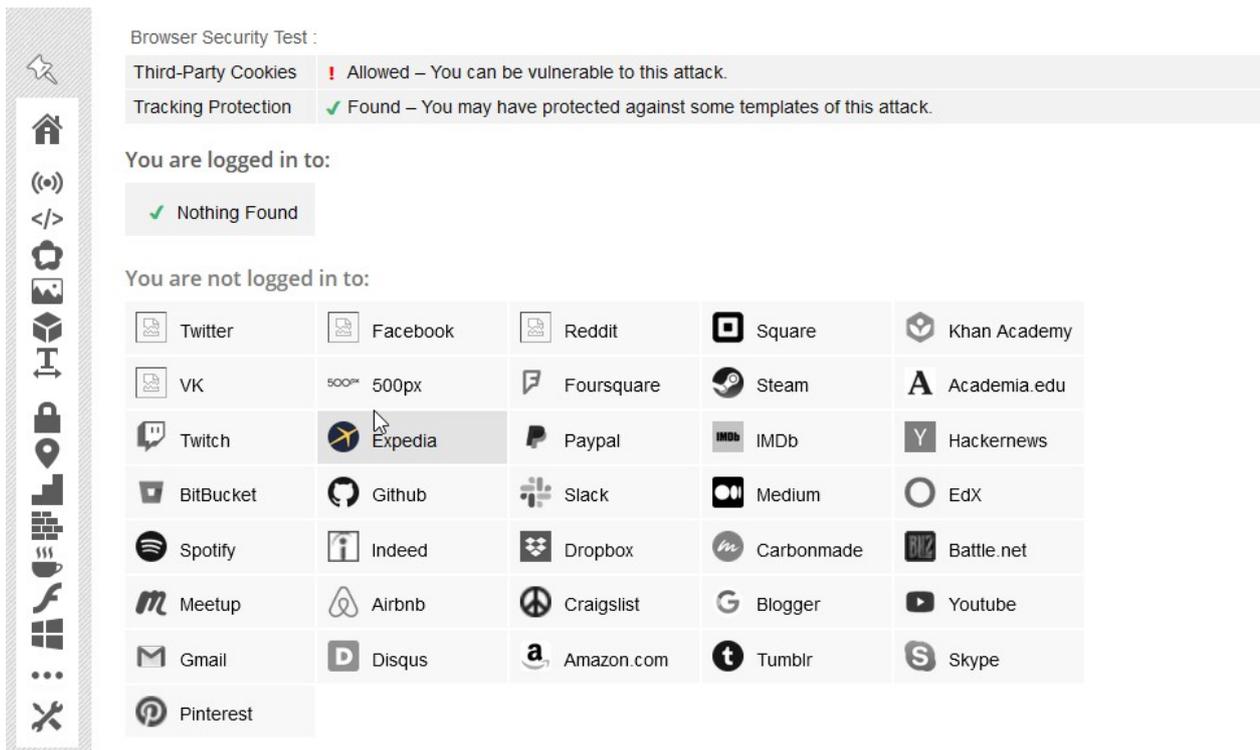


Abb. 10.3.2 browserleaks findet keine installierten Schriften seit NoScript aktiv ist

10.5 Social Media Login Detection mit Add-on

Bei den *Social Media* Logins ist kein Unterschied zu erkennen, da dieser Rechner nie in ein Social Media Tool eingeloggt war. Wäre er das gewesen, würde ein Angreifer dies nach der Aktivierung des Tools nicht mehr sehen.

Interessant für Angreifer ist hier der Umkehrschluss, denn das Tool zeigt an, in welchen Social Media die Nutzer:in **nicht** eingeloggt ist. Dort muss er Angriffe also gar nicht erst nach ihr suchen. Da die meisten Menschen in Social Media aktiv sind, lässt sich so schnell klären, wer welches Medium nutzt.



The screenshot displays a browser security tool interface. On the left is a vertical toolbar with various icons. The main content area shows a 'Browser Security Test' section with two items: 'Third-Party Cookies' (Allowed) and 'Tracking Protection' (Found). Below this, it states 'You are logged in to:' followed by a 'Nothing Found' message. The 'You are not logged in to:' section contains a grid of social media and service icons, including Twitter, Facebook, Reddit, Square, Khan Academy, VK, 500px, Foursquare, Steam, Academia.edu, Twitch, Expedia, Paypal, IMDb, Hackernews, BitBucket, Github, Slack, Medium, EdX, Spotify, Indeed, Dropbox, Carbonmade, Battle.net, Meetup, Airbnb, Craigslist, Blogger, Youtube, Gmail, Disqus, Amazon.com, Tumblr, Skype, and Pinterest.

You are not logged in to:				
Twitter	Facebook	Reddit	Square	Khan Academy
VK	500px	Foursquare	Steam	Academia.edu
Twitch	Expedia	Paypal	IMDb	Hackernews
BitBucket	Github	Slack	Medium	EdX
Spotify	Indeed	Dropbox	Carbonmade	Battle.net
Meetup	Airbnb	Craigslist	Blogger	Youtube
Gmail	Disqus	Amazon.com	Tumblr	Skype
Pinterest				

Abb. 10.5.1 Social Media Login

Quellen

1. Add-on Custom Tab Title and Favicon – ein Add-on, das den Namen geöffneter Tabs und das dazugehörige Favicon ändert
https://addons.mozilla.org/de/firefox/addon/custom-tab-title-and-favicon/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search
2. Add-on Fake Filler – ein Add-on, das in Formularen automatisch frei erfundene Daten einträgt
https://addons.mozilla.org/de/firefox/addon/fake-filler/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search
3. Add-on Firefox Multi Account Container – ein Add-on, direkt von Mozilla, das unterschiedliche Container zur Verfügung stellt, um die Inhalte von Websites gegeneinander abzuschirmen
https://addons.mozilla.org/de/firefox/addon/multi-account-containers/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search
4. Add-on I don't care about Cookies – ein Add-on, das die Einstellungen für Consent Banner (Pop Ups die einen auffordern alle Cookies anzunehmen) automatisch am benutzerfreundlichsten einstellt
https://addons.mozilla.org/de/firefox/addon/i-dont-care-about-cookies/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search
5. Add-on NoScript – ein Add-on, das die Ausführung von Skripten auf Websites verhindert
https://addons.mozilla.org/de/firefox/addon/noscript/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search
6. Add-on Privacy Badger – ein Add-on der EFF (Electronic Frontier Foundation – eine amerikanische Bürgerrechtsorganisation) zum Schutz der Privatsphäre
https://addons.mozilla.org/de/firefox/addon/privacy-badger17/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search
7. Add-on Referer Modifier – ein Add-on, das die Webadresse, die man vor der aktuellen aufgerufen hat, fälscht
https://addons.mozilla.org/de/firefox/addon/referer-modifier/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

8. Add-on Tab ReTitle – ein Add-on, das geöffneten Tabs andere Namen gibt. Aus Amazon wird Wikipedia oder ähnliches. Dieses Add-on verändert jedoch nicht das *Favicon*
https://addons.mozilla.org/de/firefox/addon/tab-retitle/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search
9. Add-on Temporary Containers – ein Add-on, das nicht kategorisierte Websites in einen Container legt, der nur 15 Minuten von Bestand ist
<https://addons.mozilla.org/de/firefox/addon/temporary-containers/>
10. Add-on User-Agent Switcher – ein Add-on, das dafür sorgt, dass die Angaben sowohl für das Betriebssystem, als auch den benutzten Browser gefälscht werden
https://addons.mozilla.org/de/firefox/addon/user-agent-string-switcher/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search
11. Am I unique – wie leicht ist Ihr Browser identifizierbar?
<https://amiunique.org>
12. browserleaks – eine Website, die aufzeigt, welche Daten der Browser verrät - <https://browserleaks.com/>
13. CalyxVPN – ein kostenloses amerikanisches VPN
<https://calyxinstitute.org/projects/digital-services/vpn>
14. coveryourtracks.eff.org – womit und wie verfolgt man Sie?
https://coveryourtracks.eff.org/results?&aat=1&fp_i_whorls=%7B%22v2%22%3A%7B%22plugins%22%3A%22permission+denied%22%2C%22hardware_concurrency%22%3A8%2C%22audio%22%3A%2235.73833402246237%22%2C%22canvas_hash_v2%22%3A%22f139fb61b2b20249d81082f9012141dc%22%2C%22webgl_hash_v2%22%3A%2233dbdb28a8e5050332bc8f7473462c56%22%7D%7D
15. CyberGhost – ein deutscher VPN Anbieter mit Sitz in Rumänien
https://www.cyberghostvpn.com/de_DE/
16. Mozilla VPN – kostenloses VPN, das Mozilla anbietet
<https://www.mozilla.org/de/products/vpn/>
17. ProtonVPN – ein schweizer VPN Anbieter mit kostenlosen und kostenpflichtigen Angeboten
<https://protonvpn.com/>
18. TLS (Transport Layer Security) – Verschlüsselung auf Transportwegen
<https://de.wikipedia.org/wiki/TLS>
19. VPN (Virtual Private Network) – Virtuelles privates Netzwerk, bietet mehr Sicherheit durch Punkt-zu-Punkt Verbindungen und

Transportverschlüsselung

https://de.wikipedia.org/wiki/Virtual_Private_Network