

Was dein Browser über dich verrät



François Martin



François Martin

Full Stack Software Engineer

 francois.martin@karakun.com

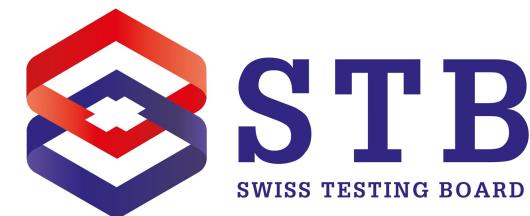
 [martinfrancois](https://github.com/martinfrancois)

 [/in/francoismartin](https://www.linkedin.com/in/francoismartin)

 [@fmartin_](https://twitter.com/fmartin_)



Fachhochschule Nordwestschweiz
Hochschule für Technik





karakun

Wir entwickeln Software.



Agil. Nutzerzentriert. Erfolgreich.

Karakun im Detail



Nachhaltige Individuallösungen

Kunden aus unterschiedlichen Bereichen, u.a. Versicherung, Finanz, Life Science, Logistik

Kompetenzen

State-of-the-Art Tech-Stack (Java, Web)
Text Analytics / KI / Big Data
Fokus auf Open-Source-Software

Community Engagement

Autoren, Referenten, Java Champions,
Universitätsdozenten, Kontributoren in
Open-Source-Projekten

Dienstleistungen

Software Engineering, UX-Design,
Consulting, Training, Wartung &
Support

Plattformen & Produkte

Effizienzsteigernde Software-
Plattformen, fertige Produkte für
ausgewählte Bereiche

Erfahrenes, eingespieltes Team

60+ Mitarbeitende an 4 Standorten in
CH (Hauptsitz), D und IN





Wer profitiert davon?

- "Normale" Nutzer im Internet gehen davon aus, dass sie ohne Login / Account **nicht** eindeutig identifiziert werden können
- Werbeagenturen und Webseiten möchten Nutzer **jederzeit** eindeutig identifizieren können
 - Werbeagenturen wollen gezielte Werbung schalten
 - Webseiten wollen Angebot und Empfehlungen auf Nutzer anpassen
- Alle erfassten, eindeutig zu einer Person zuweisbaren Daten **zusammen** bilden ein detailliertes Verhaltensprofil der Online-Aktivität
 - politische Einstellung
 - Ausbildungsstand
 - Einkommensklasse

Wie identifizieren Webseiten uns?

1. “Tracking Cookies”

- Bei erstem Besuch der Webseite wird mit Webseite assoziiertes Cookie im Browser gespeichert
- Bei erneutem Besuch wird Cookie von Webseite ausgelesen
- Aktivität auf der Webseite wird mit Cookie assoziiert
- Analogie: Jeder Besucher einer Konferenz trägt einen Lanyard mit einer fortlaufenden Nummer
 - Unternehmen an Ständen erkennen Besucher an der Nummer
 - Stände können sich untereinander zu Informationen anhand von Nummer austauschen
 - Besucher können sich weigern, einen Lanyard zu tragen oder ihn später weglegen

2. “Fingerprinting”

- Nutzer wird anhand von Daten, die vom Browser übermittelt werden erkannt
- Analogie: Auch ohne Lanyard können Stände Besucher anhand von Haarfarbe, Sprache, Akzent etc. eindeutig identifizieren





Wie kommuniziert der Browser?

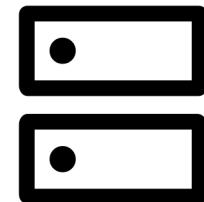
Browser



Anfrage (Request)



Website
karakun.com



- Anfrage und Antwort bestehen jeweils aus zwei Teilen:
 - Metadaten in “Header-Feldern” (vgl. Kopfzeile)
 - Inhalt der Nachricht im “Body” (vgl. Text)

Übermittelte Informationen



Automatisch mitgeschickt oder von Webseite anforderbar / ermittelbar (Auszug)

- Browser und Version
- Betriebssystem (Windows, Mac, Linux) und Version
- Installierte Plugins / Extensions
- Bildschirmauflösung und Farbtiefe
- Installierte Schriftarten auf dem System
- Prozessor Plattform (z. B. Mac Intel, oder Mac M1)
- Anzahl der Prozessorkerne
- Menge an Arbeitsspeicher (RAM)
- Verwendete Grafikkarte
- Zeitzone
- Sind Cookies aktiviert?
- Sprache (z. B. en-US, de-CH)
- Touchscreen unterstützt
- Werbeblocker aktiviert?



Das Heikle an Fingerprinting

- Beim Fingerprinting speichert Webseite speichert alle Informationen, die der Browser übermittelt als “Fingerabdruck”
 - Besucht man Webseite später erneut, kann Webseite den “Fingerabdruck” erkennen
- Informationen sind in (fast) allen Fällen eine **einzigartige** Kombination!
 - Analyse von fast einer halben Million von Browern ergaben zu 84 % einzigartige Kombinationen
- Ermöglicht Webseiten individuelle Nutzer eindeutig zu erkennen, **auch ohne Login!**
 - Nutzer haben leicht andere Sprache, Zeitzone, Bildschirmauflösung, installierte Plugins...
 - z. B. Sprache “de-DE” wird nur in Deutschland verwendet
 - Viele benutzen z. B. Windows, eine Auflösung von 1920 x 1080 und eine bestimmte Grafikkarte, aber nur wenige **genau diese** Kombination



Test auf Fingerprinting

- Standard-Test ist “**Cover Your Tracks**” (ehemaliger Name: “Panopticlick”)
- Von Electronic Frontier Foundation (EFF) kostenlos im Internet
 - <https://coveryourtracks.eff.org/>
 - Open Source, Quelltext (Code) kann von allen eingesehen werden
- Sagt aus, wie einzigartig der “Fingerabdruck” des Browsers ist
 - Im Vergleich zu anderen Nutzern, die den Test in den letzten 45 Tagen gemacht haben
 - Durchschnittlich ca. 3'810 Tests pro Tag
- Weitere Tests:
 - <https://audiofingerprint.openwpm.com/>
 - <https://browserleaks.com/canvas>

Chrome



Oh oh...

IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from <u>fingerprinting</u> ?	<u>Your browser has a unique fingerprint</u>

Your Results

Your browser fingerprint **appears to be unique** among the 171,478 tested in the past 45 days.

Firefox



Nicht besser...

IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from <u>fingerprinting</u> ?	Your browser has a unique fingerprint

Your Results

Your browser fingerprint **appears to be unique** among the 171,498 tested in the past 45 days.

Safari



Leicht besser, aber immer noch ziemlich einzigartig...

IS YOUR BROWSER:

Blocking tracking ads?	<u>Partial protection</u>
Blocking invisible trackers?	<u>Partial protection</u>
Protecting you from <u>fingerprinting</u> ?	<u>Your browser has a nearly-unique fingerprint</u>

Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 85752.0 browsers have the same fingerprint as yours.**

Brave



"Fingerabdruck" wird randomisiert (zufällig gemacht)

IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from <u>fingerprinting</u> ?	● <u>your browser has a randomized fingerprint</u>

Your Results

Your browser fingerprint **has been randomized** among the 171,509 tested in the past 45 days. Although sophisticated adversaries may still be able to track you to some extent, randomization provides a very strong protection against tracking companies trying to fingerprint your browser.



Das Dilemma

Mehr Schutz vor Tracking = weniger Schutz vor Tracking?

- Durch Installieren von Plugins, die Tracking blockieren, wird Browser einzigartiger
 - Schützt zwar vor Tracking Cookies, macht aber Fingerprinting effektiver
- Browser wie Brave mit Schutzmechanismen gegen Fingerprinting schützen nur bedingt
- Plugins wie NoScript verhindern die Ausführung von JavaScript, macht Fingerprinting unmöglich
 - Macht aber auch praktisch alle Webseiten unbenutzbar
 - Nicht alltagstauglich
- Einziger wirklicher Schutz vor Tracking Cookies und Fingerprinting
 - Tor Browser
 - Ziel, möglichst alle Nutzer gleich aussehen zu lassen
 - z. B. beim Start wird immer die **gleiche Fenstergrösse** eingestellt, bei **allen Nutzern**
 - Schränkt viele Features ein, damit Metadaten möglichst gleich bei allen Nutzern



Tor Browser

Standard

IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from fingerprinting?	Your browser has a non-unique fingerprint

Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 2810.24 browsers have the same fingerprint as yours.**

Nach Maximieren des Fensters

IS YOUR BROWSER:

Blocking tracking ads?	<u>Yes</u>
Blocking invisible trackers?	<u>Yes</u>
Protecting you from fingerprinting?	Partial protection

Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 8048.64 browsers have the same fingerprint as yours.**



Was soll ich nun tun?

- **Option 1:** Chrome, Firefox, Edge, Opera zusammen mit dem Privacy Badger Plugin vom EFF verwenden
- **Option 2:** Brave Browser verwenden
- Beide Optionen schützen gegen Tracking Cookies und Brave etwas besser gegen Fingerprinting
 - aber nur wenn man Browser häufig neu startet, sonst sind beide Optionen equivalent
- Schutz gegen Tracking Cookies ist immer noch wichtiger, als Schutz vor Fingerprinting
 - Person an Konferenz mit Lanyard mit einzigartiger Nummer ist immer noch einfacher eindeutig zu identifizieren als Person ohne Lanyard
- In sehr kritischen Fällen oder für Paranoide: Tor Browser
- Webseiten die GDPR einhalten, dürfen wenn man Tracking nicht zustimmt **weder** Tracking Cookies, **noch** Fingerprinting verwenden!
 - wird man in einem Popup nach Zustimmung gefragt, für maximale Privatsphäre alles ablehnen
 - Tracking ist aber **nicht immer** schlecht, kann Entwicklern helfen Webseite besser zu machen!



Stand und Links

Aktuellste Browerversisionen vom 17.09.2022, jeweils auf macOS Intel

- Chrome 105.0.5195.102
- Firefox 104.0.2
- Safari 15.6.1 (17613.3.9.1.16)
- Brave 1.43.93
- Tor Browser 11.5.2

Weiterführende Links:

- <https://themarkup.org/the-breakdown/2020/09/22/i-scanned-the-websites-i-visit-with-blacklight-and-its-horrifying-now-what>
- <https://www.practicalecommerce.com/as-cookies-crumble-fingerprinting-could-grow>
- <https://coveryourtracks.eff.org/learn>
- <https://www.eff.org/deeplinks/2010/05/every-browser-unique-results-fom-panopticlick>

Unsere #diwodo22 Beiträge



www.karakun.com/youtube



Karakun AG

Elisabethenanlage 25
4051 Basel
Switzerland

T. +41 61 551 36 00
E. info@karakun.com
W. www.karakun.com