How Your Browser Is Snitching on You and How You Can Take Control

JCON WORLD 2023 ONLINE

KARAKUN

www.karakun.com

François Martin

Senior Full Stack Software Engineer

✉ francois.martin@karakun.com

martinfrancois

/in/françoismartin

@fmartin_

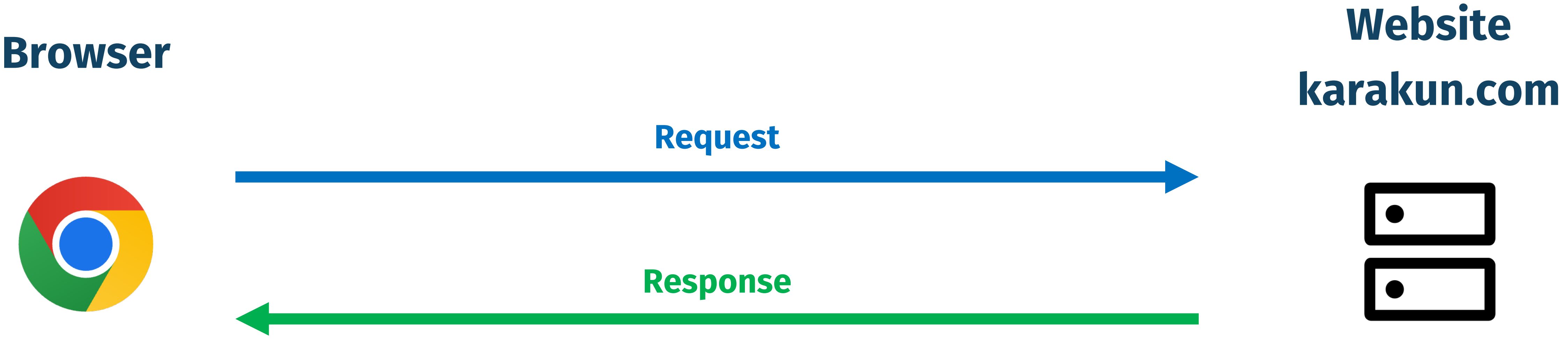
Who benefits from this?

- ”Normal” users assume they **cannot** be uniquely identified on the internet without login / account
- Advertising agencies and websites want to be able to uniquely identify users **at any point**
  - Ad agencies want to be able to place targeted ads
  - Websites want to tailor their offerings and recommendations to the user
- All identifiable collected data together forms a detailed behavioral profile of the online activity and includes
  - Political affiliation
  - Educational level
  - Income bracket

How do websites identify us?

1. “Tracking Cookies”
    - Upon first visit, website saves a cookie associated with that website in the browser
    - Upon following visits, the cookie is read by the website
    - Activity on the website is associated with the cookie
    - Analogy: Visitors at a conference wear lanyards with a sequential number on it
        - Companies at booths recognize visitors by the number
        - Booths can exchange information about visitors by referencing them by the number
        - Visitors can refuse to wear a lanyard or stop wearing it at some point
2. “Fingerprinting”
    - Users are recognized based on the data the browser transmits or is asked to transmit
    - Analogy: Even without a lanyard, visitors can be uniquely identified based on their hair color, language, accent, etc.

How do browsers communicate?



Browser

Website

karakun.com

Request

Response

- Request and response consist of two parts each:
  - Metadata in headers
  - Content in the body

Transmitted information

Automatically transmitted or retrievable by JavaScript without prompting for permission (excerpt)

- Browser and version
- Operating system (Windows, Mac, Linux) and version
- Installed plugins / extensions
- Screen resolution and color depth
- Installed fonts
- Processor architecture (f. e., Mac Intel, Mac M2)
- Available CPU core count
- Amount of RAM
- Video card hardware and drivers via Canvas Fingerprinting
- WebGL vendor, renderer and parameters

- Time zone
- Are cookies allowed?
- Language (f. e., en-US, de-CH)
- Touchscreen support
- Ad blocker active?
- IP address (rough geolocation)
- Gyroscope present
- Proximity sensor present
- Battery (exists, charge time, level)
- Accelerometer

Fingerprinting: simple but effective

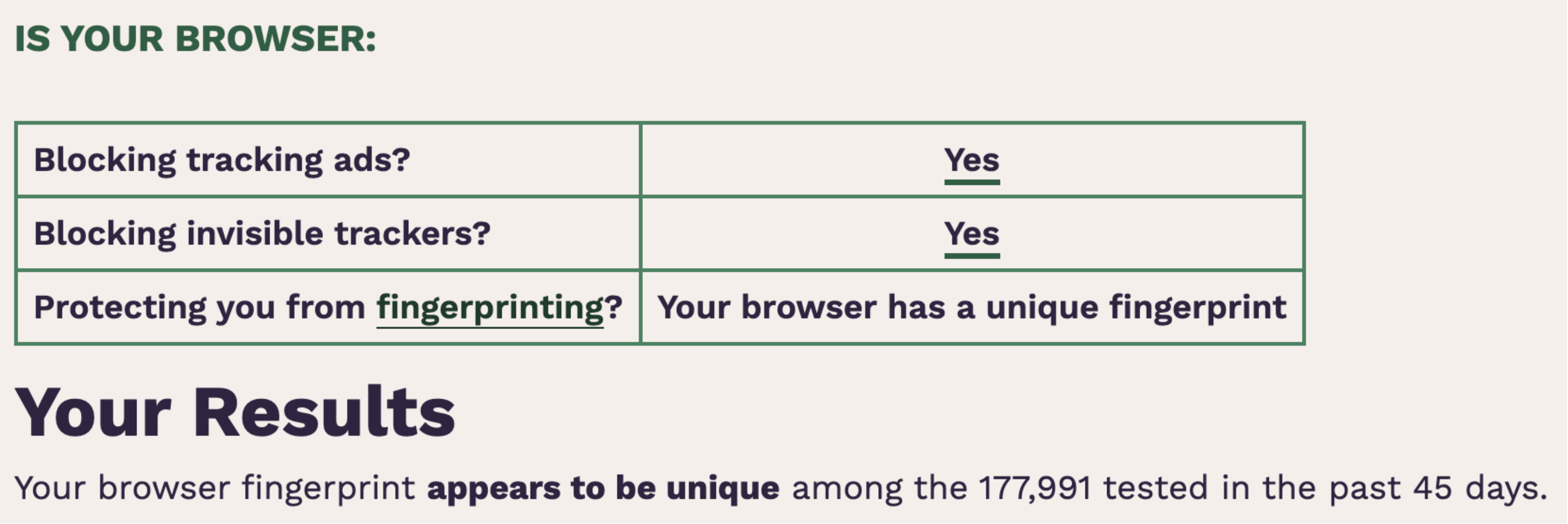
- Website saves all the information sent by the browser as ”fingerprint”
  - When visiting a website again, the website can recognize this “fingerprint” by comparison
- Information is in (almost) all cases a **unique** combination!
  - 99.5 % accuracy according to fingerprint.com
- Enables websites to **uniquely** identify users, even **without a login**!
  - Slightly different languages, time zones, screen resolutions, browser versions, installed plugins…
  - f. e., language “de-DE” is only used in Germany
  - Many use Windows, a resolution of 1920 x 1080 and have a certain graphics card, but only **very few** have the **exact same** combination

Testing for fingerprinting

- Commonly used test is “**Cover Your Tracks**” (earlier name: ”Panopticlick”)
- Provided by the Electronic Frontier Foundation (EFF) for free
  - https://coveryourtracks.eff.org/
  - Open Source
- Shows you how unique the ”fingerprint” of your browser is
  - Compared to other users that did the test in the last 45 days
  - Around 3954 tests per day on average
- Other tests:
  - https://amiunique.org/
  - https://browserleaks.com/canvas
  - https://fingerprint.com

Chrome

Oh oh...



IS YOUR BROWSER:

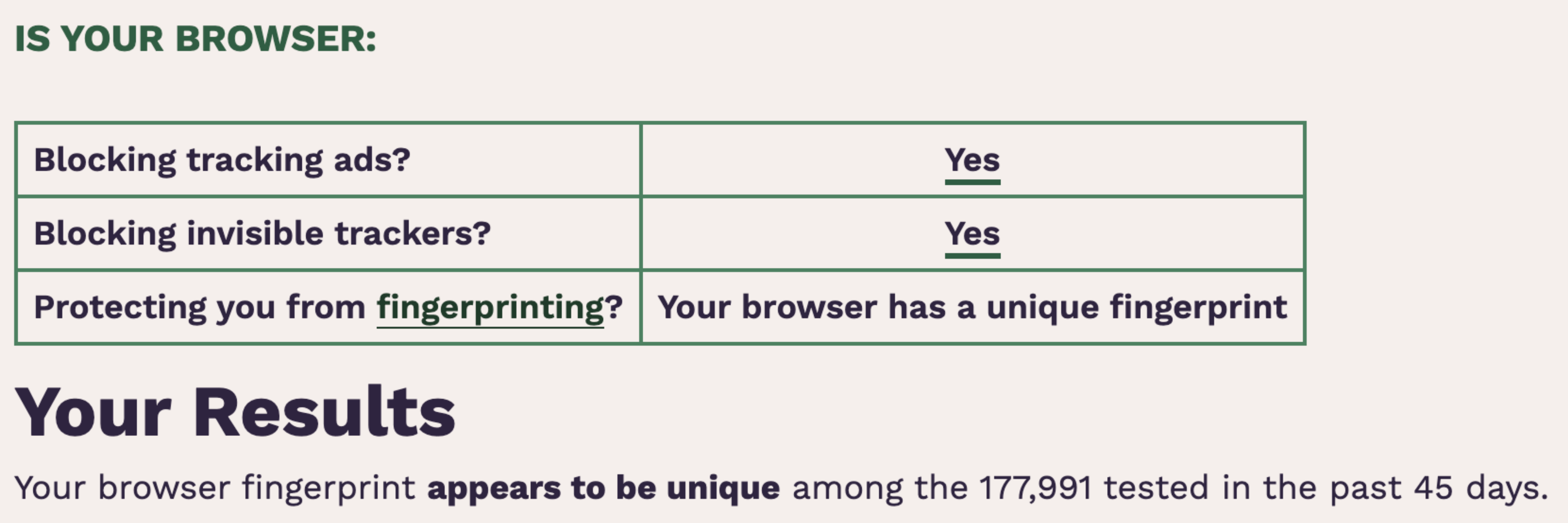
Blocking tracking ads?	**Yes**
Blocking invisible trackers?	**Yes**
Protecting you from fingerprinting?	**Your browser has a unique fingerprint**

Your Results

Your browser fingerprint **appears to be unique** among the 177,991 tested in the past 45 days.

Firefox

Same…



IS YOUR BROWSER:

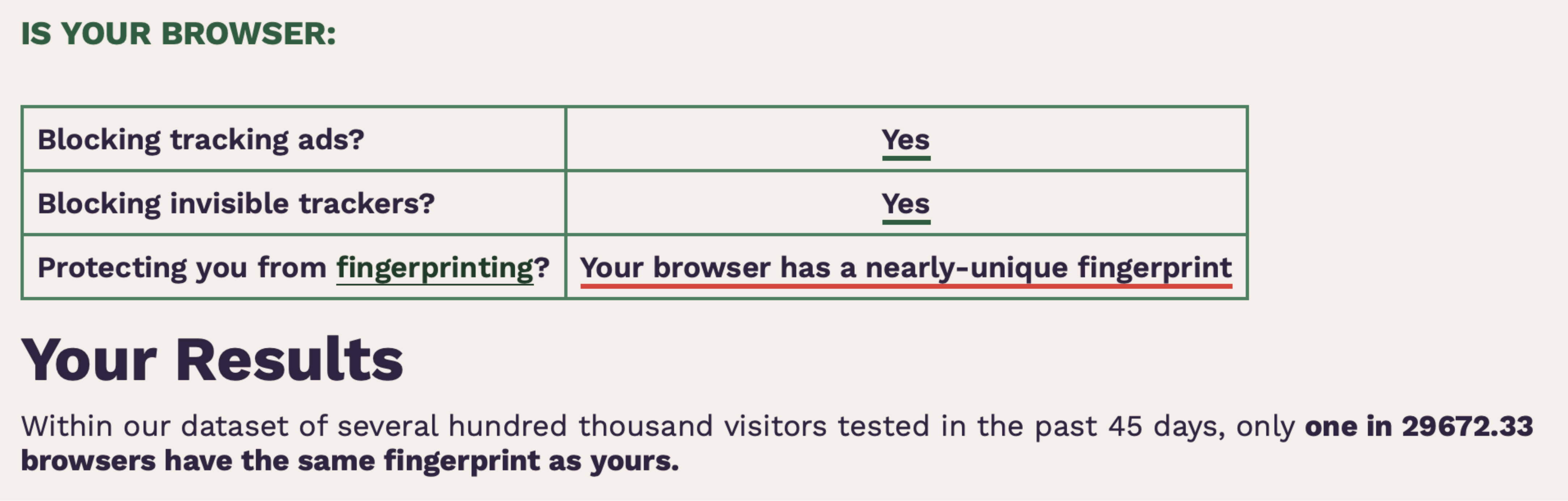
Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Your browser has a unique fingerprint

Your Results

Your browser fingerprint **appears to be unique** among the 177,991 tested in the past 45 days.

Safari

A little better, but still pretty unique...



IS YOUR BROWSER:

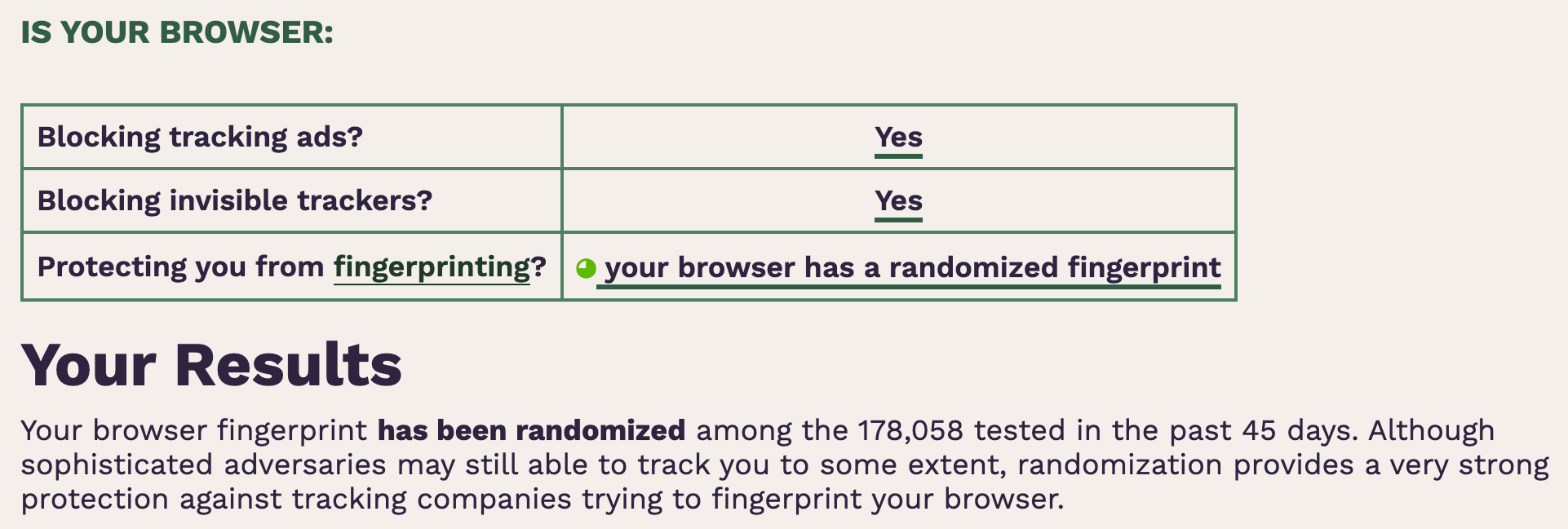
Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Your browser has a nearly-unique fingerprint

Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 29672.33 browsers have the same fingerprint as yours.**

Brave

”Fingerprint” is randomized



IS YOUR BROWSER:

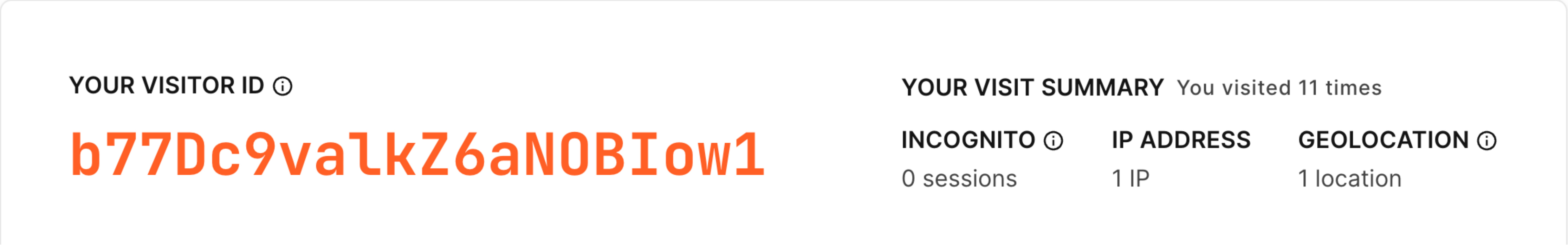
Blocking tracking ads?	**Yes**
Blocking invisible trackers?	**Yes**
Protecting you from fingerprinting?	● **your browser has a randomized fingerprint**

Your Results

Your browser fingerprint **has been randomized** among the 178,058 tested in the past 45 days. Although sophisticated adversaries may still able to track you to some extent, randomization provides a very strong protection against tracking companies trying to fingerprint your browser.

Brave

Even with a randomized fingerprint, fingerprint.com recognizes the browser across restarts



YOUR VISITOR ID ⓘ

b77Dc9valkZ6aNOBIow1

YOUR VISIT SUMMARY You visited 11 times

INCOGNITO ⓘ	IP ADDRESS	GEOLOCATION ⓘ
0 sessions	1 IP	1 location

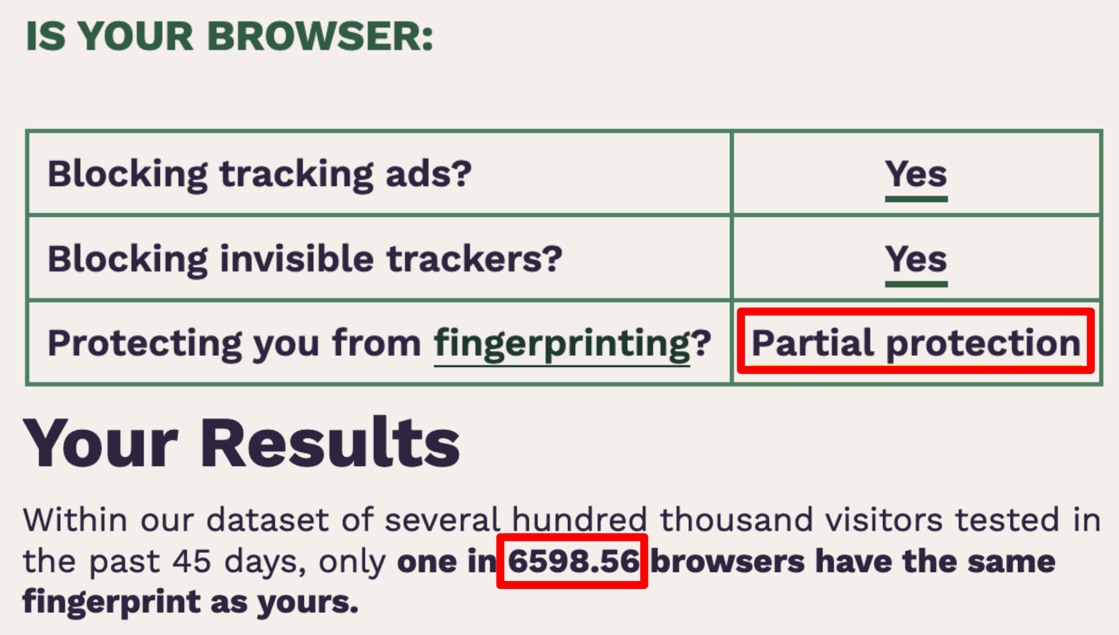
The dilemma

More protection against tracking = less protection against tracking?

- By installing plugins that block tracking, the browser becomes more unique
  - Protects from tracking cookies, but makes fingerprinting more effective
- Fingerprinting protections from browsers like Brave only offer limited protection at best
- Plugins like NoScript prevent execution of JavaScript, which makes Fingerprinting (almost) impossible
  - At the same time also renders almost all websites unusable
  - Not suitable for everyday use
- Only real protection against tracking cookies and fingerprinting
  - Tor Browser
  - Goal, to make all users seem as similar as possible
    - f. e., after start, the **same window size** is set for **all users**
  - Limits many features, so metadata is as indistinguishable as possible between users
  - (very) slow

Tor Browser

Default



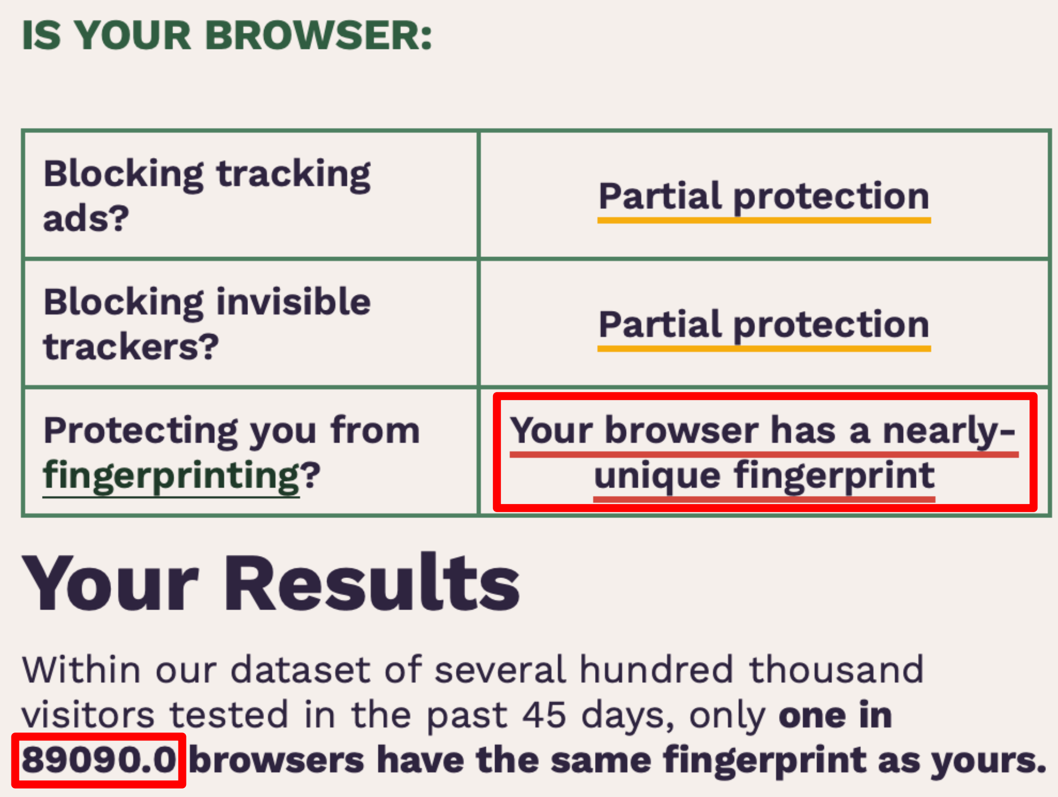
IS YOUR BROWSER:

Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
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 6598.56 browsers have the same fingerprint as yours.**

After maximizing the window



IS YOUR BROWSER:

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

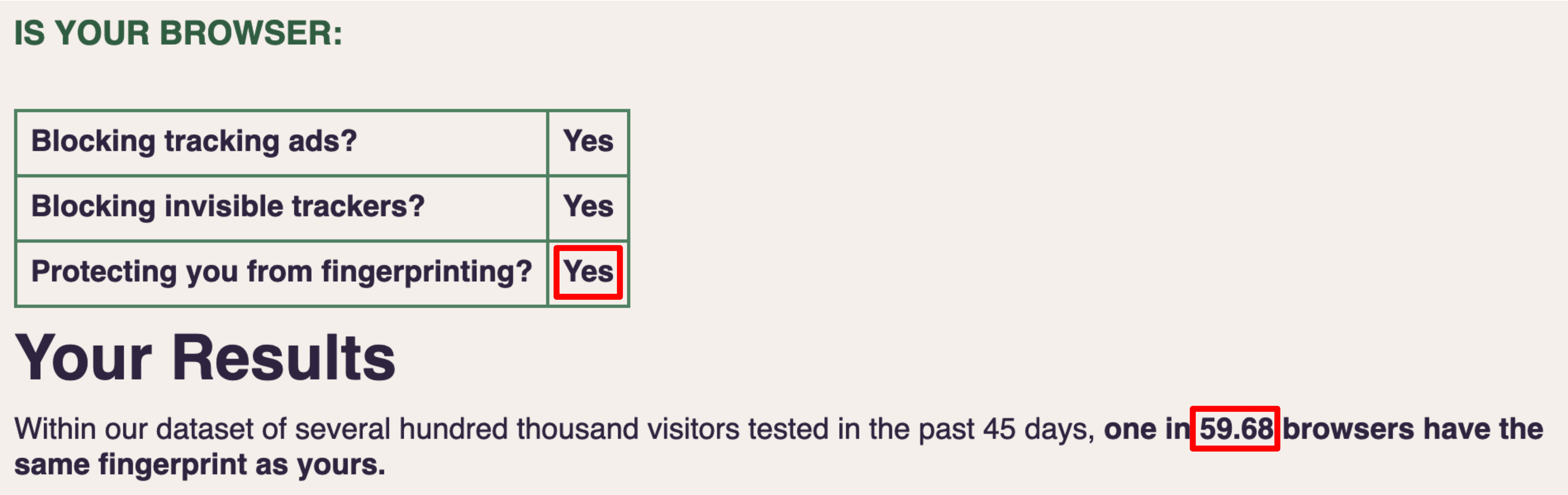
Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, only **one in 89090.0 browsers have the same fingerprint as yours.**

13.5x less unique!

Tor Browser

Security set to ”Safest” (JavaScript blocked)



IS YOUR BROWSER:

Blocking tracking ads?	Yes
Blocking invisible trackers?	Yes
Protecting you from fingerprinting?	Yes

Your Results

Within our dataset of several hundred thousand visitors tested in the past 45 days, **one in 59.68 browsers have the same fingerprint as yours.**

What should I do?

- **Option 1:** Chrome, Firefox, Edge, Opera, with the Privacy Badger Plugin from the EFF installed
- **Option 2:** Brave Browser
- Both options protect against tracking cookies, Brave a little better against fingerprinting
  - But only if you restart your browser frequently, otherwise the options are equivalent
- Protection against tracking cookies is still more important, than protection against fingerprinting
  - Visitor at a conference with lanyard and unique number is still easier to identify than a person without a lanyard
- In privacy-critical cases: Tor Browser
- Websites following GDPR are **not allowed** to use **tracking cookies** or perform **fingerprinting**, if you do **not consent**!
  - For maximum privacy: decline as much as possible when asked in a popup
  - Tracking is **not always** bad, can help developers make a website better

Versions and links

Most recent browser versions as of the 23rd of September 2023, on macOS with Apple Silicon

- Chrome 117.0.5938.92
- Firefox 117.0.1
- Safari 16.6 (18615.3.12.11.2)
- Brave 1.58.131
- Tor Browser 12.5.4

Further reading:

- 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

Slides:

https://bit.ly/jconworld2023