

# Introduction to Browser Fingerprinting

Fabio Fontana

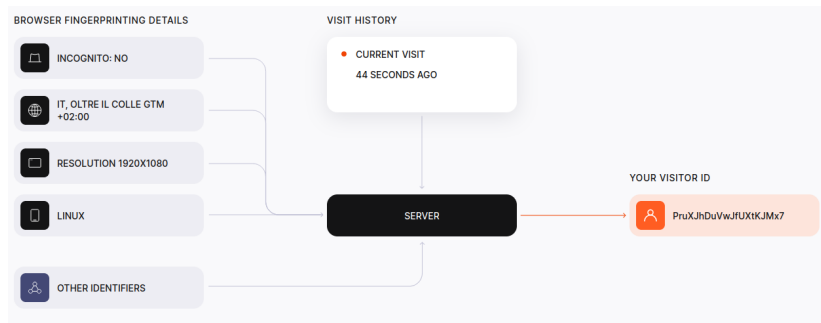
Supervisor: Prof. Marina Ribaudó

University of Genoa

2023

# What is Browser Fingerprinting

Browser Fingerprinting is a method that allows websites and online services to collect and analyze specific data about a user's device resulting in a unique fingerprint of it.



# Which data is collected

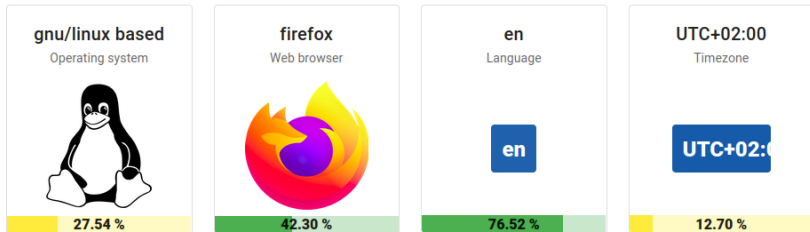
- ▶ **Browser info:** type, version, language, plugins, settings, ...
- ▶ **Device info:** os, gpu, screen size, fonts, battery info, ...
- ▶ **Network and Session info:** public ip, local ip, timezone, supported protocols and ciphers, ...

# Browser Fingerprinting properties: uniqueness

It is highly improbable for two users to have identical fingerprints. In fact, studies have suggested the uniqueness can be so specific that only one in several hundred thousand users might share the same fingerprint.

**Yes! You are unique among the 2118922 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.



# Browser Fingerprinting properties: stateless

Even if users disable cookies, change IP or use privacy-focused browsing modes, fingerprinting can still function, making it both challenging to detect and thwart. This method is stateless, not relying on stored data in the browser, and hence, it leaves no obvious trace.

YOUR ID

**PruXJhDuVwJfUXtKJMx7**

IP	INCOGNITO	BROWSER
146.241.144.46	No	Firefox on Linux

YOUR ID

**PruXJhDuVwJfUXtKJMx7**

IP	INCOGNITO	BROWSER
109.54.221.114	Yes	Firefox on Linux

## Why it is used: the constructive way

- ▶ combat fraud or credential hijacking
- ▶ suggest updates for out of date devices
- ▶ bot detection

# Why it is used: the questionable way

- ▶ track users across websites and collect information about their habits and their tastes without the users knowing about it:
  - ▶ **Fingerprints as Global Identifiers:** if a device has a unique fingerprint, it is akin to a cookie that cannot be deleted
  - ▶ **Fingerprint + IP address**
    - ▶ **as Cookie Regenerators:** deleted cookies can be restored by matching the IP and the fingerprint
    - ▶ **in the absence of Cookies:** unmask different machines behind the same IP

## Why it is used: advertising and customizing the online experience







- ▶ data collected allows advertising businesses to create a custom profile for targeted advertising which indirectly means higher revenue for the company
- ▶ adapt content and prices due to users habits, status and location















## Why it is used: the destructive way

Deliver exploits that are tailored for a specific user configuration

# How data is collected: HTTP request

1 - User agent 	0.03 %	Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/118.0
2 - Accept 	29.08 %	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
3 - Content encoding 	96.49 %	gzip, deflate, br
4 - Content language 	34.82 %	en-US,en;q=0.5
5 - Upgrade Insecure Requests 	91.25 %	1
6 - Referer 	2.33 %	https://www.google.com/

# How data is collected: JavaScript attributes

3 - Cookies enabled		88.22 %	
4 - Timezone		12.70 %	UTC+02:00
5 - Content language		43.08 %	en-US,en
7 - List of fonts (JS)		0.00 %	Courier And 22 others
8 - Use of Adblock		21.89 %	
9 - Do Not Track		65.20 %	
10 - Navigator properties		2.37 %	42 properties detected
20 - Screen width		20.60 %	1920
21 - Screen height		19.18 %	1080

# How data is collected: Canvas fingerprinting

The way an image or text is rendered on a canvas can vary based on the browser, os, gpu, font rendering settings and anti-aliasing algorithms, resulting in a unique image that can be used to create a fingerprint.

## How data is collected: Canvas fingerprinting example

```
// text with lowercase/uppercase/punctuation symbols
var txt = "BrowserLeaks.com <canvas> 1.0";
ctx.textBaseline = "top";
// the most common type
ctx.font = "14px 'Arial'";
ctx.textBaseline = "alphabetic";
ctx.fillStyle = "#f60";
ctx.fillRect(125,1,62,20);
// color mixing to increase the difference in rendering
ctx.fillStyle = "#069";
ctx.fillText(txt, 2, 15);
ctx.fillStyle = "rgba(102, 204, 0, 0.7)";
ctx.fillText(txt, 4, 17);
```

BrowserLeaks.com <canvas> 1.0

# How data is collected: WebGL fingerprinting

# How data is collected: TLS fingerprinting

# What about privacy: GDPR and ePrivacy Directive

Since browser fingerprinting relies on the collection of personal data, companies using this technique must comply with the strict requirements of the GDPR and the ePrivacy Directive:

- ▶ the data collection process must be transparent to users
- ▶ companies must ask for consent when personal data is involved

Otherwise, companies often have proprietary methods to perform browser fingerprinting and those often are hard to be detected and don't use personal data.



# What about privacy: prevention and mitigation

- ▶ use privacy-focused browsers like Tor and anti-fingerprinting extensions like Privacy-Badger and uBlock Origin
- ▶ disable unnecessary plugins, disable useless extensions and consider using default settings to blend in with a larger crowd
- ▶ keep the software updated
- ▶ if you are a developer, build your own anti-fingerprinting countermeasure

*Any questions?*

# References

## ▶ Bibliography

- ▶ Browser Fingerprinting: A survey
- ▶ How Unique Is Your Web Browser?
- ▶ A Survey of Browser Fingerprint Research and Application

## ▶ External sources

- ▶ <https://amiunique.org>
- ▶ <https://coveryourtracks.eff.org>
- ▶ <https://pixelprivacy.com/resources/browser-fingerprinting>