Infographics

Browser fingerprinting infographic

Everyone has a digital fingerprint relating to their browser software and hardware activities and this data can be used to detect suspicious connections i.e. an imposter.

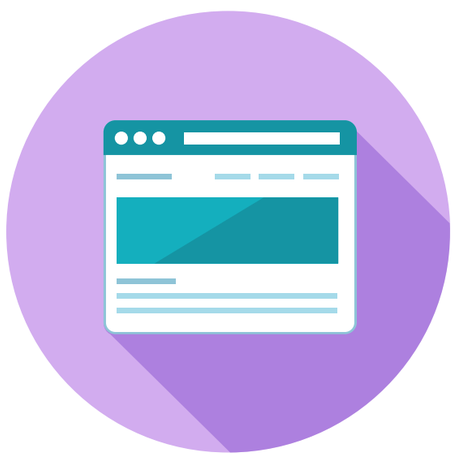
Words Inside Fingerprint

It can tell you parameters such as:

- System fonts
- If cookies are enabled
- Language
- Platform
- Keyboard layout
- Sensors such as accelerator, proximity and gyroscope
- Browser local databases
- Navigator properties
- HTTP header attributes
- Extensions used
- Audio context analysis
- CPU Class
- HTML5 canvas fingerprinting (looking at canvas size)
- Touch support

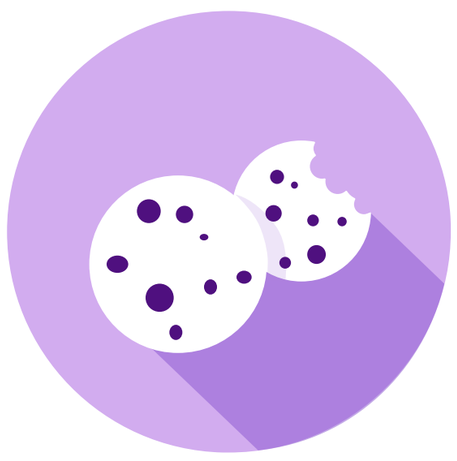
And more...

In order to help create unique IDs we stitch the data in the right sets:



Browser

- \+ Hash doesn't change
- – Multiple browsers will generate different hashes

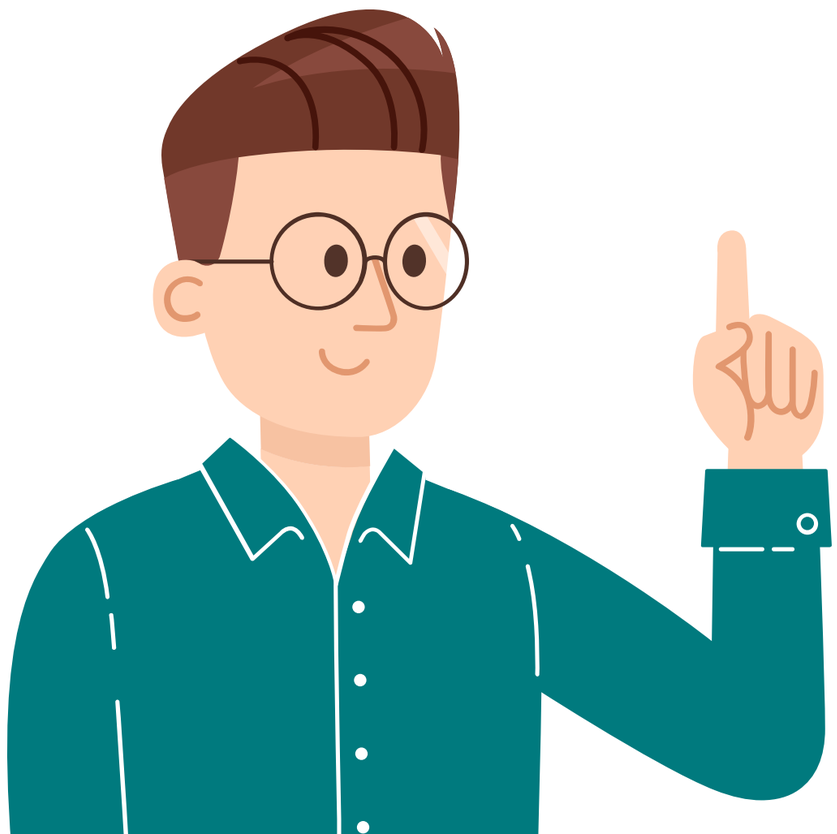


Cookie

- \+ Easy to prove multiple users are the same person
- – Common practise to clear the browser cookies and cache

Device

- \+ Tools generate same Hash despite misleading plugins
- – Fewer unique IDs due to same phone / laptop / browser version



Online browser fingerprinting is a fantastic method for identifying suspicious users but it's by no means sufficient by itself.