**HEADER METRICS**

Whenever you connect to a website (in our case, “**https://coveryourtracks.eff.org**”), your device sends a request that includes several HTTP headers. These headers contain information like your device’s language and security settings, cookies, and the referring URL (the link that you clicked on prior to arriving on the site). Header metrics are transmitted by your browser by default.

**BROWSER METRICS**

Unique attributes or modifications that you’ve made to your browser.

**FINGERPRINTING METRICS**

The end product of a tracker running a fingerprinting script and comparing how your device renders graphics in comparison to other users’ devices.

**HARDWARE METRICS**

The permanent hardware specs of your device.

Keep in mind: Each browser metric is highly connected to other metrics in complex ways.

This is why we don’t recommend:

* trying to change a single element of your fingerprint,
* striving to get the most common result for any individual metric.

Let’s look at an example of how these metrics are interconnected:

No matter what browser you’re using, you could pretend to be using a more common browser on the web: You could modify the user-agent string to be seen as Chrome. You may think this would increase your anonymity and hide your individualized fingerprint among the millions of other Chrome users–but you will actually become more identifiable. How could choosing a more common metric make one stick out more? Because when considered in combination with other metrics, your browser will be the only one that has a user-agent of Chrome on Windows with a hardware and software profile, fonts, screen size and color depth, and platform string indicative of an iOS device.

**USER AGENT**

##### WHAT IS THIS?

A web header which relays information to the web server about:

* your browser
* its version

##### HOW IS THIS USED IN YOUR FINGERPRINT?

This information can be very specific, and if customized can single-handedly identify a specific user’s browser.

#### HTTP\_ACCEPT HEADERS

##### WHAT IS THIS?

A web header that is used to let the server know:

* what types of content the browser is able to handle. For example, a server can choose to deliver a CSV file if it sees that a user’s browser does not support XML.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

This information can be fairly unique, and varies from browser to browser. However, this string doesn’t tend to change much over time, and can remain constant through many versions of the same browser.

#### BROWSER PLUGIN DETAILS

##### WHAT IS THIS?

A plugin is a small piece of software that helps a browser manage content it’s unable to process on its own.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

Browser plugins have been phased out over the past few years in favor of more regulated add-ons and extensions, but they persist in older browsers.

#### TIME ZONE OFFSET

##### WHAT IS THIS?

This metric is a number which indicates the current difference between your time and GMT, in minutes.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

Historically, time zones couldn’t be transmitted by browser headers, so time offset was used instead. It does not always change in step with the ‘time zone’ metric and thus can provide more insight particular in areas that are unique in the way they observe daylight savings time.

#### TIME ZONE

##### WHAT IS THIS?

This metric is a string which indicates your time zone, like ‘America/Los\_Angeles’.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

This metric can be used to figure out your general location, especially if you live in a time zone without many other users.

#### SCREEN SIZE AND COLOR DEPTH

##### WHAT IS THIS?

The dimensions of your current browser window, and its color depth (determined by your monitor).

##### HOW IS THIS USED IN YOUR FINGERPRINT?

While this metric can supplement other information, it’s often too ‘brittle’ to be usable by trackers because users can easily change their browser window dimensions.

#### SYSTEM FONTS

##### WHAT IS THIS?

To determine your system fonts, tracking sites commonly display some text in an [**HTML <span> tag**](https://developer.mozilla.org/en-US/docs/Web/HTML/Element/span). Trackers then rapidly change the style for that span, rendering it in hundreds or thousands of known fonts. For each of these fonts, the site determines whether the width of the span has changed from the default width when rendered in that particular font. If it has, the tracker knows that font is installed.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

The list of fonts you have installed on your machine is generally consistent and linked to a particular operating system. If you install just one font which is unusual for your particular browser, this can be a highly identifying metric.

#### ARE COOKIES ENABLED?

##### WHAT IS THIS?

Cookies are small chunks of information that websites store in your browser. They are primarily used to automatically remember things like your account login info, or what items were in your online shopping cart–in other words, they save your place. However, they can also be used to link all of your visits, searches, and other activities on a site together.

As a metric, “cookies enabled” is either ‘True’ or ‘False’, and means your browser allows cookies, rather than blocking them. Whether cookies are enabled can be determined with or without the use of JavaScript.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

Whether cookies are enabled or not provides a single bit of information: either ‘true’ or ‘false.’ However, this feature can be far more identifying when combined with other details.

#### LIMITED SUPERCOOKIE TEST

DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No, openDatabase: true, indexed db: true

##### WHAT IS THIS?

Despite the name, “super cookies” are not technically cookies. While they also store and retrieve unique identifiers, they are much harder to detect and delete in comparison.

Super cookies can monitor what websites you visit and how long you spend on them. Super cookies can also access information collected by traditional tracking cookies–such as login information, cached images and files– and reference it after the traditional cookie has been deleted.

#### HASH OF CANVAS FINGERPRINT

##### WHAT IS THIS?

This metric is the unique identification assigned to your browser after a tracking site performs a specific test on the HTML5 <canvas> element in your browser.

[**Canvas fingerprinting.**](https://developer.mozilla.org/en-US/docs/Web/API/Canvas_API) is invisible to the user: a tracker can create a “canvas” in your browser, and generate a complicated collage of shapes, colors and text using JavaScript. Then, with the resulting collage, the tracker extracts data about exactly how each pixel on the canvas is rendered. The operating system, browser version, graphics card, firmware version, graphics driver version, and fonts installed on your computer all affect the final result.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

This is a complex and highly reliable fingerprinting metric. Canvas fingerprinting uses JavaScript, where a tracker renders a complex sequence of shapes, colors, and UTF characters to the HTML5 <canvas> element in your browser. This canvas is then serialized and hashed to provide the canvas fingerprint metric.

Small changes in video card hardware, operating system-level video drivers, and fonts installed will result in slightly different images being rendered to the canvas. Although different from one computer to the next, these settings are consistent enough on a single machine to clearly identify a user.

#### HASH OF WEBGL FINGERPRINT

##### WHAT IS THIS?

The 'hash of WebGL fingerprint' is very similar to the 'hash of canvas fingerprint' in its method of using your browser to generate graphics, extracting data from how each pixel is rendered, serializing the result and hashing it. However, it uses WebGL instead. WebGL is a JavaScript API for rendering interactive 2D and 3D graphics.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

The WebGL and Canvas fingerprinting results are highly linked, as they both examine browser-rendered graphics for tiny differences between users.

#### WEBGL VENDOR & RENDERER

##### WHAT IS THIS?

WebGL is a library that allows browsers to render 3D graphics. As with other graphics-based tracking methods, trackers look for any tiny differences between how your device displays 3D on the web compared to other users.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

This metric provides some level of granularity, depending on how unique your video card is. The WebGL Vendor and renderer is directly searchable using JavaScript, so trackers can access it without issue.

#### DNT HEADER ENABLED?

True

##### WHAT IS THIS?

A web header that is used to let the server know:

* if you prefer not to be tracked. This is usually either not delivered at all, or set to ‘1’. A setting of “1” indicates that your browser would prefer not to be tracked, but right now, most sites ignore this request.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

Browsers which set the DNT header to ‘1’ are fairly rare, and this can be an identifying metric. However, this should be left as the default for your browser.

#### LANGUAGE

#### PLATFORM

##### WHAT IS THIS?

This metric includes your operating system and CPU (central processing unit) architecture and is directly searchable by trackers using JavaScript.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

This can either be very unique or very commonplace, depending on your particular machine.

#### TOUCH SUPPORT

##### WHAT IS THIS?

This metric refers to the number of touch points on a device, such a tablet or phone.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

If you are using a mobile device, this may be very identifying depending on the hardware particularities. Your result will be 0 if your device has no touch points.

#### AD BLOCKER USED

#### AUDIOCONTEXT FINGERPRINT

##### WHAT IS THIS?

Rather than rendering graphics like with canvas fingerprinting or WebGL fingerprinting, an audio sample is generated;That audio sample is then serialized and measured to provide this fingerprint.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

Like Canvas Fingerprinting, this can be unique depending on your audio card and drivers, and usually will not change over time. In modern handheld devices and laptops, graphics cards and audio cards will vary depending on the model, but not between devices of the same model. For desktop machines, especially ones with customized hardware, the audio card will provide new information useful for fingerprinting.

#### CPU CLASS

#### HARDWARE CONCURRENCY

6

##### WHAT IS THIS?

This metric notes the number of CPU cores in your current machine.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

This can provide some additional information when combined with other fingerprinting metrics, but is not identifying on its own.

#### DEVICE MEMORY (GB)

8

##### WHAT IS THIS?

This metric notes the amount of memory on your current machine, rounded to the nearest gigabyte.

##### HOW IS THIS USED IN YOUR FINGERPRINT?

Like hardware concurrency, this is useful when combined with other metrics, but is not identifying on its own.