# ESTUDIO

## Fingerprinting o Huella digital del dispositivo

# ÍNDICE

# 1. INTRODUCCIÓN

Actualmente, el modelo que subyace tras la mayoría de los servicios web se basa en prestar un servicio de forma totalmente gratuita, a cambio de la monetización de los datos recopilados de los usuarios. En la mayoría de los casos la información recogida de los usuarios se rentabiliza a través de servicios de marketing que dirigen campañas de publicidad personalizadas por quien desea publicitar un producto o servicio. Por lo tanto, además de identificar al usuario y realizar un seguimiento y recopilación de datos, necesitan perfilarlo con el objetivo de maximizar la eficacia de la publicidad que se les ofrece.

Para identificar a los usuarios se utilizan diferentes técnicas de seguimiento, las más conocidas son las cookies, es decir, ficheros almacenados en el ordenador del usuario que crea la propia página web del proveedor de servicios y que son utilizados posteriormente con diversas finalidades, como mejorar la experiencia de usuario con su navegador web o estudiar la estadística de uso del sitio web por los usuarios, pero también son utilizados con otras finalidades como es el perfilado de los usuarios.

La LSSI[1] regula en su artículo 22.2 que los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a la legislación vigente. En el caso que nos ocupa, de acuerdo a lo establecido en el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD) y el artículo 11 de la Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones, siempre que aquél deba proceder a su configuración durante su instalación o actualización mediante una acción expresa a tal efecto.

Hoy en día, los navegadores pueden ser configurados, entre otras opciones, para que no acepten cookies o para que acepten cookies temporales que son automáticamente borradas al cerrar el navegador. Por su parte, los sistemas antivirus han instalado protecciones consistentes en poder programar un borrado periódico de cookies y otros ficheros de rastreo instalados en el ordenador del usuario por las aplicaciones web además de los anonimizadores de los datos de los terminales.

Sin embargo, nos encontramos ante un mercado muy dinámico en el que que los navegadores y antivirus proveen de herramientas para permitir a los usuarios gestionar la exposición de su información personal, lo que implica una dificultad para perfilar con alta precisión a los potenciales

[1] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

clientes. Por ello, los diversos agentes implicados en el mercado de Internet no cesan de investigar nuevas formas de poder salvar esas protecciones para recopilar y explotar datos de los usuarios.

De los numerosos estudios existentes en relación con las técnicas de identificación en internet se deriva que se están utilizando otras técnicas de seguimiento más avanzadas y que han superado a las cookies, basadas en la recopilación de información específica del navegador web y/o dispositivo de navegación, cuya combinación permite construir un identificador para singularizar al usuario, y cuya legitimación no está clara. Este conjunto de técnicas se conoce en la terminología anglosajona como *device fingerprinting*, *browser fingerprinting* o simplemente *fingerprinting*, en español *huella digital del dispositivo* o *huella del dispositivo*. A lo largo del texto se utilizarán indistintamente todas estas denominaciones.

En el presente estudio se realiza una aproximación al concepto de huella digital del dispositivo; se describen las técnicas más utilizadas para obtenerla; cómo identifican el dispositivo utilizado por el usuario; algunas recomendaciones para que los usuarios puedan proteger su privacidad mediante el uso de medidas a su alcance y así evitar el uso de la huella con fines de seguimiento y perfilado, y finalmente las recomendaciones para la industria.

## 2. HUELLA DIGITAL DEL DISPOSITIVO

La huella digital del dispositivo es una recopilación sistemática de información sobre un determinado dispositivo remoto con el objetivo de identificarlo, singularizarlo y, de esa forma, poder hacer un seguimiento de la actividad del usuario del mismo con el propósito de perfilarlo.

El Comité Europeo de Protección de Datos, en su documento "Dictamen 9/2014 sobre la aplicación de la Directiva 2002/58/CE a la toma de *fingerprinting* de dispositivos" asume la definición de la RFC 6973[2] que define la huella como "*un conjunto de elementos de información que identifica un dispositivo o una instancia de aplicación*". [3]

Dicho en términos más comprensibles, la huella digital del dispositivo es un conjunto de datos extraídos del terminal del usuario que permiten individualizar de forma unívoca dicho terminal. Dado que lo habitual es que las personas no compartan sus equipos, ya sea este un teléfono móvil, tableta, portátil u ordenador de trabajo, individualizar el terminal supone individualizar a la persona que lo utiliza. Las entidades que utilizan los mecanismos de huella digital realizan una recopilación sistemática de información de todos los terminales que se conecten a sus servidores con el objetivo de singularizarlos y poder hacer un seguimiento de la navegación del usuario para construir un perfil.

[2] *RFC 6973 Privacy Considerations for Internet Protocols*. Documento que ofrece una guía con consideraciones sobre privacidad para incluir en el desarrollo de especificaciones de protocolos de internet. Su objetivo es que los diseñadores, implementadores y usuarios de protocolos de internet sean conscientes de las opciones de diseño relativas a la privacidad.

[3] Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting.

Contrariamente a lo que pueda pensar, el perfilado no se limita a recopilar y analizar los hábitos de navegación del usuario o las búsquedas que realiza en servidores. Las técnicas más avanzadas permiten registrar los movimientos que realiza el usuario a través de la página web con el ratón, examinando en que partes de la pantalla se detiene por más tiempo[4]. Por otro lado, los desarrollos de software para dispositivos, como por ejemplo JavaScript o Flash, facilitan la implementación de procedimientos para recoger información muy concreta del dispositivo, como por ejemplo el modelo de navegador, tipo y versión de sistema operativo, resolución de la pantalla, arquitectura de procesador, listas de fuentes de texto, plugins o dispositivos instalados, direcciones IP, etc.[5] La combinación apropiada de toda esta información permite confeccionar una suerte de huella digital única del dispositivo que lo singulariza y, por lo tanto, diferencia de forma univoca a cada usuario en internet.

Mediante estas técnicas de huella digital, al acceder a una página web, el navegador ejecuta en el dispositivo del usuario, y sin su conocimiento, una serie de tratamientos con el objetivo de realizar una recopilación de datos de éste suficiente detallada como para poder individualizarlo y la trasmiten al servidor que las almacena para su uso posterior. Esta información se une a otra que recibe el servidor desde el navegador del usuario, cuya finalidad puede ser inicialmente técnica (por ejemplo, adaptar los contenidos al tipo de pantalla del terminal), pero que es reutilizada con finalidades de identificación.

Es ampliamente conocido y aceptado que un determinado servicio web pueda hacer un seguimiento de la navegación de los usuarios mediante cookies, con la garantía de que un borrado de las cookies elimina el vínculo entre el dispositivo y la información personal recopilada. La realidad es que el uso de las técnicas de huella digital permiten volver a asignar al mismo usuario la información viculada al identificador de la cookie eliminada y no perder trazabilidad sobre los datos de navegación del usuario o simplemente realizar el seguimiento en base únicamente a la huella digital. En conclusión, si a la vez que se genera una cookie de identidad se detecta y almacena su huella digital, en el caso de que el usuario borre las cookies en su navegador éstas se pueden restituir utilizando la huella digital para reidentificar al usuario,por lo que el borrado de cookies no sería eficaz.

Las técnicas de identificación mediante huella digital del dispositivo se llegan a describir en la literatura especializada como “cookieless monsters”, pues no es necesario instalar ningún tipo de cookie en el dispositivo para recoger dicha información, y si esto sucede de forma totalmente transparente al usuario, éste no puede tomar medidas para evitarlo (N. Nikiforakis, 2013).

Entre las diferentes técnicas que se pueden utilizar para obtener la huella digital de un dispositivo, existen algunas especialmente avanzadas como canvas fingerprint, canvas font fingerprint, webRTC fingerprint o audio fingerprint que permiten obtener singularizaciones muy precisas.

[4] Véase, por ejemplo, la actividad de www.hotjar.com o de www.crazyegg.com, que permiten registrar recorridos del ratón, los clicks del usuario, la navegación de páginas, analizar la forma en que los usuarios utilizan los formularios web, etc.

[5] https://amiunique.org/faq

El uso de estas técnicas puede tener finalidades legítimas como, por ejemplo, formar parte de mecanismos de autenticación de factor múltiple. Sin embargo, también pueden utilizarse para hacer un seguimiento de los usuarios durante su navegación web y recopilar información sobre sus hábitos e intereses sin que el propio usuario sea consciente de ello.

En relación con la obligación de información, es habitual encontrar en los sitios web y aplicaciones cláusulas de privacidad específicas que permiten al usuario dar su consentimiento para el uso de cookies, pero no es tan común encontrar información para el usuario sobre el uso de técnicas de seguimiento basadas en huella digital para realizar un perfilado del usuario.

## 3. TÉCNICAS DE FINGERPRINTING

Existen numerosas propiedades que se pueden recopilar de un dispositivo a través del navegador web y que permiten recoger información suficiente para que, en determinadas situaciones, se pueda identificar unívocamente el terminal. Como se ha comentado anteriormente, algunas de estas características son ampliamente conocidas porque se vienen utilizando habitualmente para presentar las aplicaciones o páginas web adaptadas al dispositivo que accede a ellas. Sin embargo, otras son mucho menos conocidas y pueden llegar a sorprender por su grado de sofisticación.

En el anexo I se listan, sin ánimo de exhaustividad, algunas de las características del terminal que se pueden recoger mediante el navegador web y que pueden contribuir a la obtención de una huella digital de un dispositivo como son el tipo, versión y configuración personal del navegador, los conjuntos de caracteres instalados que dan información sobre las aplicaciones instaladas, el idioma, zona horaria, configuración de pantalla y de elementos técnicos del terminal, dirección IP, etc. También se incluye información sobre otras técnicas más avanzadas que en condiciones normales permiten una mayor particularización del dispositivo como son canvas fingerprinting, canvas font fingerprinting, webRTC fingerprinting y audiocontext fingerprinting.

Además de las técnicas citadas anteriormente existen muchas otras propiedades que se podrían recoger y en algunos casos se utilizan para formar parte de la huella digital del dispositivo, como son:

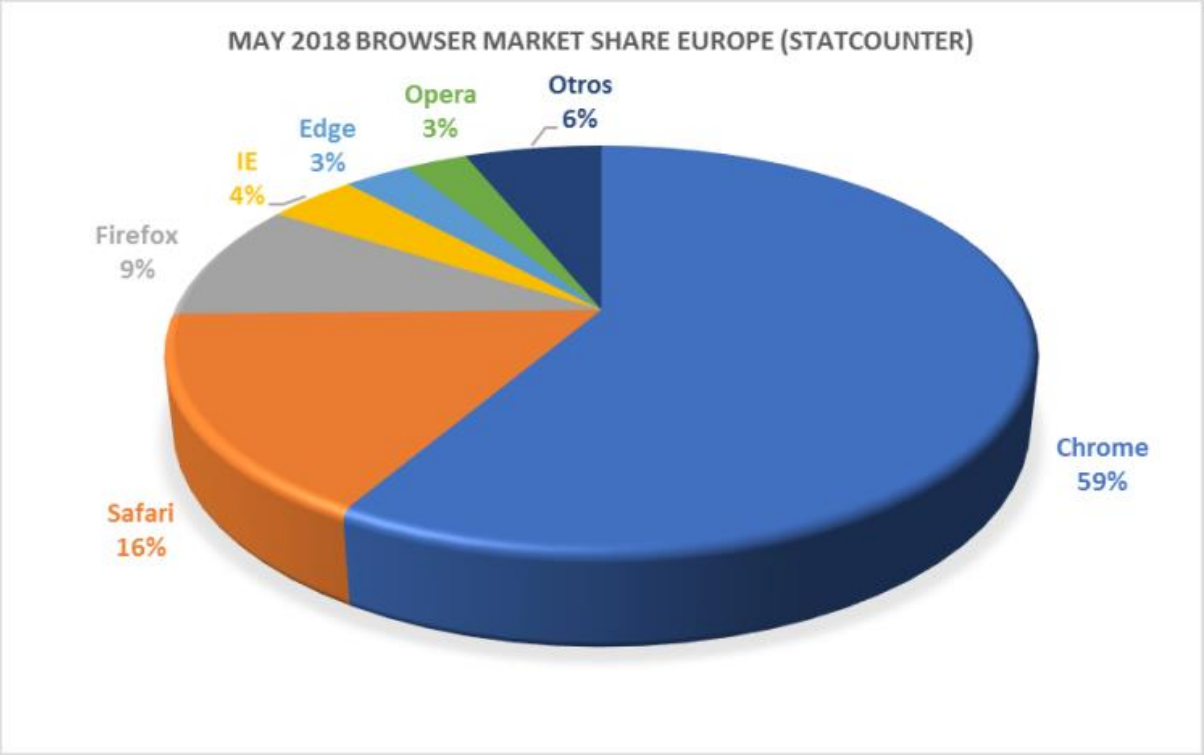
- Instalación de bloqueadores de publicidad en el navegador
- Memoria del dispositivo
- Número de monitores conectados al dispositivo
- Dispositivo con acelerómetro
- Presencia de teclados virtuales
- Lista de gestos soportados en el caso de dispositivos con pantalla multitáctil
- Codecs de audio y video disponibles
- Perfil de uso de la batería del terminal
- Listado de aplicaciones instaladas

# 4. NIVEL DE IDENTIFICACIÓN

Cada una de las técnicas de huella digital del dispositivo por separado no permitiría la particularización de un dispositivo o el individuo que lo utiliza. Sin embargo, cuando combinan un conjunto de estas técnicas con el objetivo de particularizar un dispositivo, la cantidad de información generada ofrece una alta probabilidad de que no existan colisiones entre los identificadores asignados a distintos terminales. Sin entrar en detalle, la cantidad de información será directamente proporcional al número de propiedades analizadas e inversamente proporcional a la probabilidad de que una de esas características se encuentre presente.

Actualmente se estima que hay unos 4.000 millones de ordenadores, smartphones y otro tipo de terminales en el mundo. Con un conjunto suficiente de datos discriminantes se pueden llegar a individualizar todos ellos y es esto precisamente lo que hace la *huella*. Además, lo hace masivamente, pues todo terminal que se conecte a una página web que use estas técnicas quedará identificado para siempre en ese servidor y lo hace globalmente, pues el alcance de internet es planetario.

En el ámbito de la navegación web, se puede pensar en un servicio que intenta obtener una huella digital de un dispositivo simplemente detectando el modelo de navegador empleado. Parece obvio que no se va a conseguir una particularización muy eficaz, dado que atendiendo a las estadísticas[6] alrededor del 59% de los usuarios en Europa utilizan Chrome, aproximadamente un 16% utiliza Safari, un 9% Firefox, un 4% Internet Explorer y el 12% restante otros navegadores.




[6] http://gs.statcounter.com/browser-market-share/all/europe/#monthly-201805-201805-bar

Un servicio web que únicamente detecte el modelo de navegador probablemente lo haga con el objetivo de adaptar el contenido de la web al navegador del usuario. Sin embargo, si además de una simple detección del modelo de navegador se detectan otras características como el idioma configurado en el sistema, el sistema operativo utilizado, la versión del navegador, el huso horario, la lista de fuentes de texto del sistema, etc… y se utiliza una combinación de estas características para obtener una huella digital del dispositivo, el nivel de particularización podría ser mucho mayor y, en determinadas circunstancias, se podría llegar a particularizar un dispositivo concreto entre todas los usuarios del servicio web.

Resulta conveniente establecer una métrica que permita determinar el nivel de identificación que potencialmente se puede alcanzar con cada una de las técnicas de fingerprinting bajo estudio y por tanto cabe hacerse la siguiente pregunta: ¿existe alguna forma científica de cuantificar el nivel de particularización que se puede alcanzar?

La respuesta es afirmativa, y esta cuantificación se puede realizar tomando como referencia el concepto de *entropía* tal como se define en la 'Teoría de la Información'. La *entropía* mide en bits el grado de incertidumbre que existe en el resultado de cualquier experimento o suceso aleatorio o, intuitivamente, la cantidad de información que proporciona la ocurrencia de un suceso. Por ejemplo, si un suceso puede tomar dos posibles estados equiprobables hablaremos de un bit de entropía, si son cuatro hablaremos de dos bits de entropía, y así sucesivamente[7]. Un dado de seis caras equilibrado podrá dar seis resultados distintos con igual probabilidad, por lo que la entropía o cantidad de información que proporciona una tirada es igual a $log_2 6 = 2{,}58\ bits$. Si el dado está trucado, no todos los resultados tendrán la misma probabilidad y la cantidad de información de cada tirada se medirá como $-\sum_1^6 P_n . log_2 P_n$, siendo $P_n$ la probabilidad de uno resultado del dado.

Si consideramos que la población mundial es de 7.500 millones de habitantes, la identidad de una persona desconocida elegida arbitrariamente representaría una entropía de algo menos de 33 bits, dado que $2^{33}$ es más de 8.000 millones.

A medida que se conocen características sobre un individuo se acumula una reducción de bits de entropía, de forma que si se consigue reducir la entropía en 33 bits, se puede decir que se tiene perfectamente particularizado a ese individuo.

Por ejemplo, en el caso particular de que mediante una técnica de fingerprinting se detecte que se esté utilizando para navegar Internet Explorer, eso supondrá una reducción de entropía de cuatro bits, mientras que utilizando Chrome la reducción de entropía será únicamente de un bit[8].

En líneas generales, cuanto más se acerque el dispositivo a la generalidad o a la configuración por defecto, menos factores se están ofreciendo que posibiliten la identificación del mismo. Esta

[7] (Eckersley, A Primer on Information Theory and Privacy, 2010)

[8] Como se ha establecido anteriormente, la cantidad de información $\Delta S = -\log_2 P(X = x)$, donde $\Delta S$ representa la reducción de entropía medida en bits y $P(X = x)$ representa la probabilidad de que un caso particular se materialice. En términos mas profanos, diríamos cuanto mayor sea $\Delta S$ más precisa es la determinación del equipo del usuario.

afirmación es el principal mecanismo de defensa que el usuario puede explotar a la hora de minimizar las acciones de seguimiento que se puedan realizar en su contra.

Aunque en términos generales la acumulación de factores detectados permite reducir el número de bits de entropía hasta llegar a la particularización total, esta reducción no es absolutamente acumulativa, depende de si hay correlación o no entre las variables aleatorias. Por ejemplo, un individuo del que se conoce su fecha de nacimiento supone una reducción de entropía de 8,5 bits. Otro individuo del que se conoce su signo zodiacal supone una reducción de entropía de 3,6 bits. Sin embargo, el conocimiento de la fecha de nacimiento y signo zodiacal de un mismo individuo no supone más que una reducción de entropía de 8,5 bits, puesto que la información que proporciona el signo zodiacal está implícitamente contenida en la fecha de nacimiento.

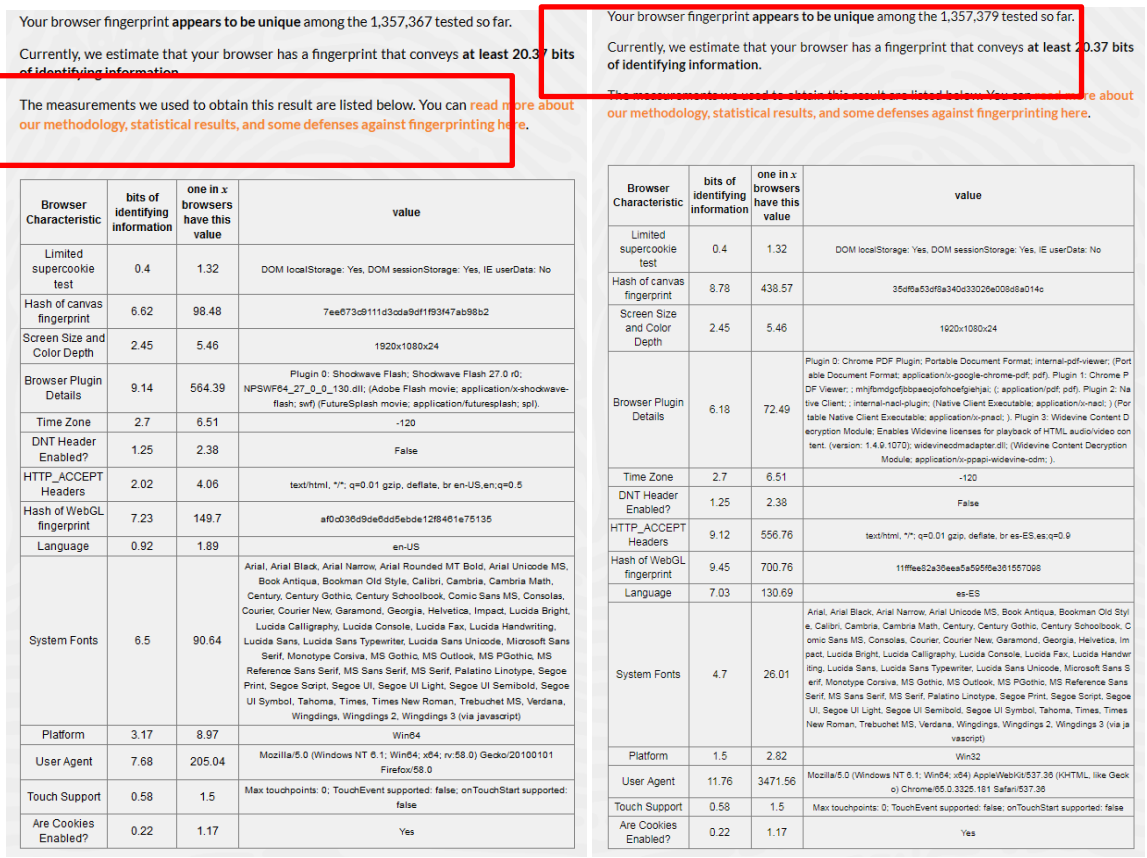
# 5. EVALUACIÓN DEL NIVEL DE IDENTIFICACIÓN

Existen diversos proyectos de investigación que permiten comprobar si un navegador/dispositivo es potencialmente identificable mediante técnicas de fingerprinting.

- PANOPTICLICK[9].

  Esta web permite realizar un rápido test con el que comprobar algunas de las técnicas anteriormente relacionadas. En la siguiente figura se muestra el resultado del test realizado por panoptipclick con dos navegadores diferentes. Como se puede leer en el recuadro destacado en rojo, con ambos navegadores sucede que la huella digital generada es única entre más de un millon de huellas digitales generadas en este proyecto. Esta huella digital supone al menos 20.37 bits de reducción de *entropía* en total. Adicionalmente, en cada línea se indican los bits de entropía estimados para cada una de las características detectadas.

[9] Proyecto de investigación de Electronic Frontier Foundation. La Electronic Frontier Foundation es una organización sin ánimo de lucro fundada en 1990 cuyo objetivo es la defensa de los derechos y libertades civiles en el mundo digital



Your browser fingerprint **appears to be unique** among the 1,357,367 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 20.37 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting here.

| Browser Characteristic | bits of identifying information | one in $x$ browsers have this value | value |
|---|---|---|---|
| Limited supercookie test | 0.4 | 1.32 | DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No |
| Hash of canvas fingerprint | 6.62 | 98.48 | 7ee673c9111d3cda9df1f93f47ab98b2 |
| Screen Size and Color Depth | 2.45 | 5.46 | 1920x1080x24 |
| Browser Plugin Details | 9.14 | 564.39 | Plugin 0: Shockwave Flash; Shockwave Flash 27.0 r0; NPSWF64_27_0_0_130.dll; (Adobe Flash movie; application/x-shockwave-flash; swf) (FutureSplash movie; application/futuresplash; spl). |
| Time Zone | 2.7 | 6.51 | -120 |
| DNT Header Enabled? | 1.25 | 2.38 | False |
| HTTP_ACCEPT Headers | 2.02 | 4.06 | text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5 |
| Hash of WebGL fingerprint | 7.23 | 149.7 | af0c036d9de6dd5ebde12f8461e75135 |
| Language | 0.92 | 1.89 | en-US |
| System Fonts | 6.5 | 90.64 | Arial, Arial Black, Arial Narrow, Arial Rounded MT Bold, Arial Unicode MS, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Garamond, Georgia, Helvetica, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS Outlook, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript) |
| Platform | 3.17 | 8.97 | Win64 |
| User Agent | 7.68 | 205.04 | Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0 |
| Touch Support | 0.58 | 1.5 | Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false |
| Are Cookies Enabled? | 0.22 | 1.17 | Yes |

Your browser fingerprint **appears to be unique** among the 1,357,379 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 20.37 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting here.

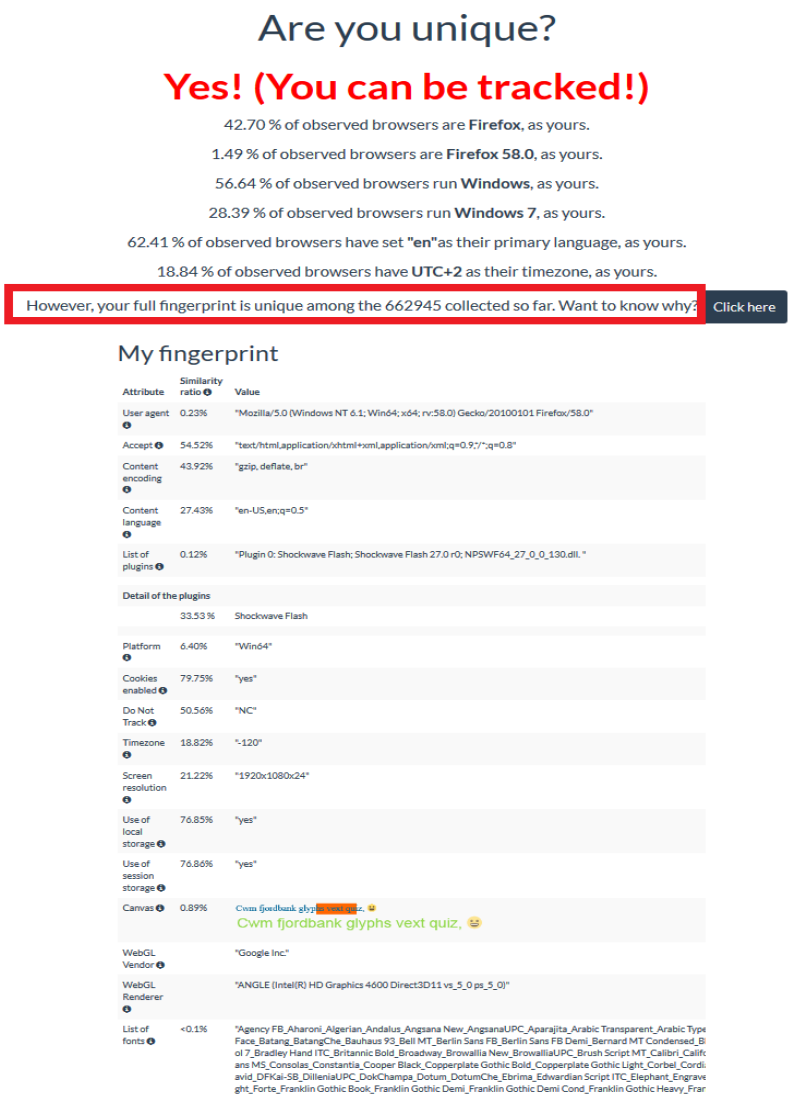
| Browser Characteristic | bits of identifying information | one in $x$ browsers have this value | value |
|---|---|---|---|
| Limited supercookie test | 0.4 | 1.32 | DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No |
| Hash of canvas fingerprint | 8.78 | 438.57 | 35df6a53df8a340d33026e008d8a014c |
| Screen Size and Color Depth | 2.45 | 5.46 | 1920x1080x24 |
| Browser Plugin Details | 6.18 | 72.49 | Plugin 0: Chrome PDF Plugin; Portable Document Format; internal-pdf-viewer; (Portable Document Format; application/x-google-chrome-pdf; pdf). Plugin 1: Chrome PDF Viewer; ; mhjfbmdgcfjbbpaeojofohoefgiehjai; (; application/pdf; pdf). Plugin 2: Native Client; ; internal-nacl-plugin; (Native Client Executable; application/x-nacl; ) (Portable Native Client Executable; application/x-pnacl; ). Plugin 3: Widevine Content Decryption Module; Enables Widevine licenses for playback of HTML audio/video content. (version: 1.4.9.1070); widevinecdmadapter.dll; (Widevine Content Decryption Module; application/x-ppapi-widevine-cdm; ). |
| Time Zone | 2.7 | 6.51 | -120 |
| DNT Header Enabled? | 1.25 | 2.38 | False |
| HTTP_ACCEPT Headers | 9.12 | 556.76 | text/html, */*; q=0.01 gzip, deflate, br es-ES,es;q=0.9 |
| Hash of WebGL fingerprint | 9.45 | 700.76 | 11fffee82a36eea5a595f6e361557098 |
| Language | 7.03 | 130.69 | es-ES |
| System Fonts | 4.7 | 26.01 | Arial, Arial Black, Arial Narrow, Arial Unicode MS, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Garamond, Georgia, Helvetica, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monotype Corsiva, MS Gothic, MS Outlook, MS PGothic, MS Reference Sans Serif, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript) |
| Platform | 1.5 | 2.82 | Win32 |
| User Agent | 11.76 | 3471.56 | Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.181 Safari/537.36 |
| Touch Support | 0.58 | 1.5 | Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false |
| Are Cookies Enabled? | 0.22 | 1.17 | Yes |

- AmIUnique.org[10].

El objetivo de esta página es la investigación sobre el uso de huellas digitales en navegación web, que permite informar al usuario sobre determinados detalles de su configuración de navegación y en qué medida permiten el seguimiento de los mismos. Asímismo, pretende aprovechar la información sobre huellas digitales recogida para aconsejar al usuario configuraciones de navegación que le permitan ser más similar al resto de usuarios y, por lo tanto, minimicen las opciones de seguimiento real de navegación.

En la siguiente figura se muestra el resultado del test realizado en amiunique.org con un navegador web. Como se puede apreciar en la parte resaltada en rojo, la huella digital completa obtenida es única sobre algo más de medio millón de huellas digitales recopiladas en el proyecto.

[10] (Laperdrix, Rudametkin, & Baudry, 2016). Se trata de una web creada y mantenida por un grupo de investigación financiado por el proyecto europeo DIVERSIFY y el Instituto Nacional de Ciencias Aplicadas de Rennes.




# 6. ESTUDIO REALIZADO

En 2018 la Agencia se planteó realizar un estudio sobre el uso de estas técnicas en webs dirigidas al público español y en español. Para ello se ha utilizado la herramienta OpenWPM[11], que es un entorno de trabajo con múltiples herramientas que permite automatizar parcialmente el estudio y recopilar datos de navegación en páginas web a gran escala y una versión de Firefox modificada para registrar información sobre las visitas realizadas de forma automática, en particular las llamadas a funciones

[11] OpenWPM (Web Privacy Measurement). Es la plataforma desarrollada por la Universidad de Princeton para realizar estudios sobre la privacidad en la Web. Usada en más de 20 estudios realizados por diferentes instituciones, OpenWPM es de uso libre bajo la licencia GPLv3. Basada en Python, OpenWPM permite utilizar Firefox para automatizar y simular el acceso a distintas páginas web recopilando información como el uso de cookies, fingerprinting, tracking, etc.

que se ejecutan en el dispositivo/navegador del usuario y pueden considerarse indicadores del empleo de técnicas de fingerprinting.

Una llamada a funciones que recogen características del terminal no significa obligatoriamente que una web esté utilizando técnicas de fingerprinting, pero si dicha llamada sigue ciertos patrones determinados o cumple algunas condiciones concretas, sí se podría deducir que en dicho servicio web potencialmente se están utilizando estas técnicas.

También hay que tener en cuenta que son dos procesos distintos. Por un lado, utilizar este tipo de funciones en el lado de usuario para extraer información y, por otro, el uso o procesamiento de esa información que se pueda realizar en el lado del proveedor del servicio web (servidor).

Además de OpenWPM, se han utilizado otras herramientas en forma de plugins específicos en navegadores y otros navegadores especialmente desarrollados para potenciar la privacidad de los usuarios con el objetivo de validar las detecciones realizadas automáticamente con OpenWPM.

Por otra parte, actualmente, la mayoría de navegadores permiten establecer las preferencias de seguimiento del usuario, especialmente los de uso más extendido. Concretamente W3C[12] ha propuesto un mecanismo para que el usuario pueda expresar sus preferencias de privacidad, de forma que un servicio web pueda deshabilitar sus técnicas de seguimiento ante la petición del usuario, Do Not Track (DNT).

El campo de cabecera DNT puede aceptar dos valores: uno en el caso de que el usuario no quiera que se le haga un seguimiento de navegación y cero en caso de que el usuario consienta el seguimiento. También existe la posibilidad de no enviar este campo de cabecera en las peticiones HTTP, por lo que DNT tomará el valor Null y significará que el usuario no ha establecido una preferencia. El estándar establece que por defecto no se envíe este campo de cabecera a menos que el usuario lo habilite desde el navegador.

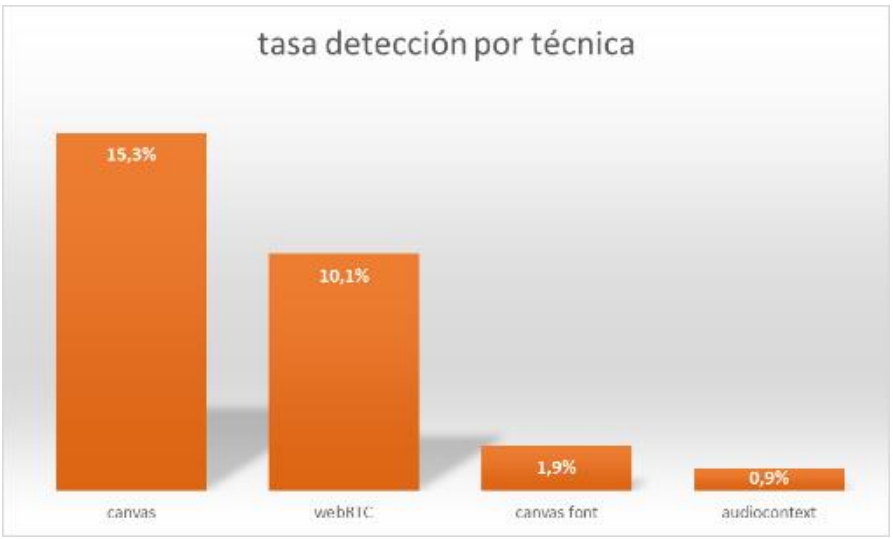
A continuación, se describen las comprobaciones realizadas durante el estudio y los resultados obtenidos en cada caso.

#### DETECCIÓN DE TÉCNICAS DE FINGERPRINTING WEB

En una primera fase del estudio se ha realizado un análisis para la detección del uso potencial de algunas técnicas avanzadas de fingerprinting web, en concreto canvas, webRTC, canvas font y audiocontext fingerprinting. Con este objetivo se han analizado 5.006 urls[13] correspondientes a 2.503 dominios, detectándose el uso potencial de estas técnicas en el **28.19%** de las peticiones a estas urls, con los siguientes resultados detallados:

[12] *World Wide Web Consortium* (W3C), es un consorcio internacional que genera recomendaciones y estándares para asegurar el crecimiento de la *World Wide Web* a largo plazo.

[13] Direcciones web.



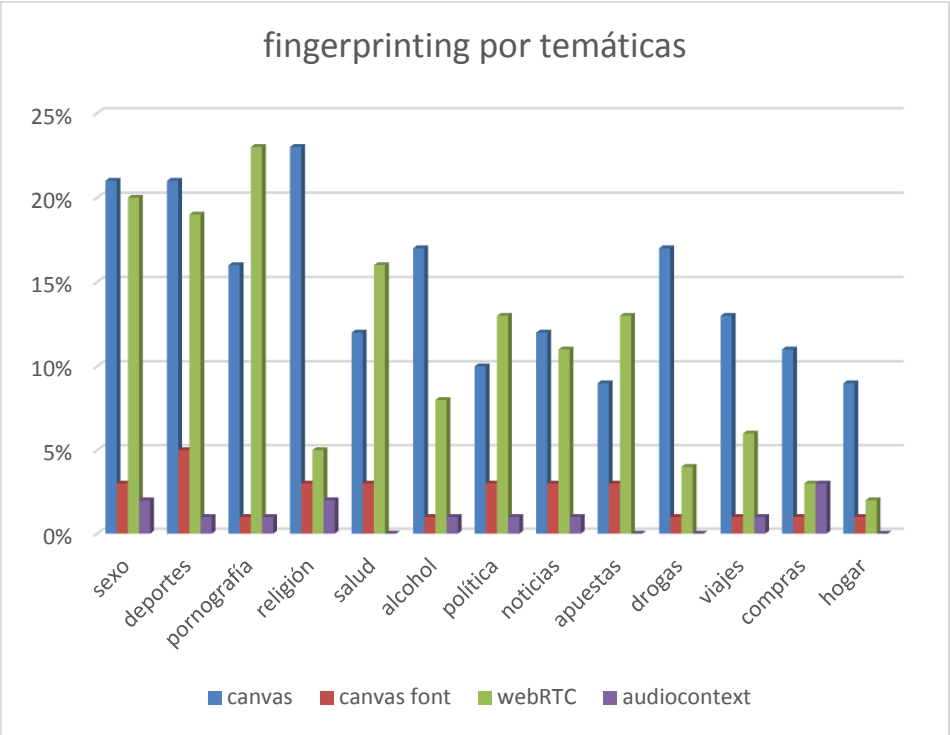

Durante el estudio se han detectado situaciones en las que en varias peticiones sucesivas a una misma URL se encuentran variaciones en el uso de técnicas de detección de huella, observando los siguientes comportamientos:

- Webs que únicamente utilizan técnicas de detección de huella cuando el dispositivo no tiene determinadas cookies instaladas.
- Webs en las que inicialmente se detectaba el uso de técnicas de detección de huella y, después de un conjunto de accesos, estás técnicas dejan de utilizarse.

Se incluye información más detallada sobre las técnicas de detección utilizadas en el Anexo II.

**ANÁLISIS POR TEMÁTICAS**

En esta fase se ha realizado el análisis de los cien primeros resultados de búsqueda en Google de los siguientes términos: sexo, drogas, alcohol, pornografía, salud, política, noticias, deportes, compras, hogar, apuestas, viajes y religión. Para cada resultado de búsqueda se ha analizado también la página principal (homepage).




Al igual que en la fase anterior, se pretende cuantificar el porcentaje de webs que potencialmente utilizan técnicas avanzadas de detección como canvas, webRTC, canvas font y audiocontext, al ser las que permiten una mayor singularización del dispositivo. El resultado se muestra en la gráfica anterior.

Se puede observar que para algunas temáticas se alcanzan porcentajes de detección superiores al 20% en las técnicas canvas y webRTC. Llama la atención los porcentajes particularmente altos para los resultados de búsqueda correspondientes a los términos sexo, pornografía, religión, salud y política. En el Anexo III se incluye la tabla completa con los porcentajes detallados.

**USO DE LA PETICIÓN DO NOT TRACK**

El 5 de abril de 2018 se inició desde la Agencia una prueba sobre 14.442 sitios webs dirigidos a usuarios españoles. La lista de sitios web se ha obtenido uniendo todas las listas de URL's utilizadas en pruebas anteriores y eliminando las repeticiones que pudieran producirse. El contenido de la lista de urls es muy heterogéneo, comprendiendo webs de toda índole: medios de comunicación, entidades bancarias, apuestas online, etc. Para cada uno de los sitios web de la lista se ha realizado una única visita a la página principal, registrando las llamadas que realizan a funciones susceptibles de ser utilizadas para la aplicación de técnicas de fingerprinting.

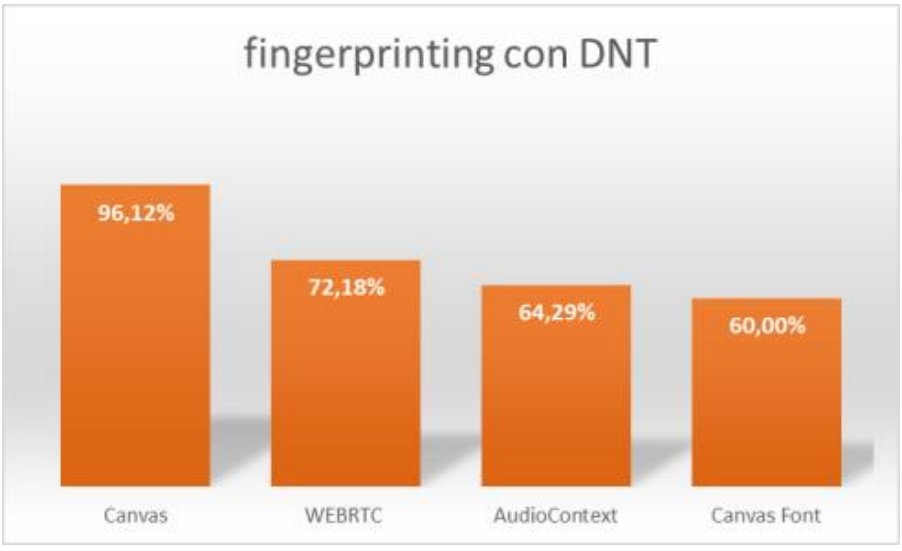
Como en todas las pruebas llevadas a cabo, se ha descartado la llamada a funciones de tecnología Flash, ya que se trata de una tecnología en desuso debido a los problemas de seguridad y la mayoría de los navegadores actuales o no incluyen esta tecnología o la tienen desactivada por defecto.

En esta ocasión el foco del análisis se centra en verificar el uso de la petición Do Not Track (DNT) por parte de las webs visitadas. Se ha detectado que el 16,72% de los sitios comprueban este parámetro mediante llamadas a funciones javascript en el dispositivo del usuario, que sería sustancial para que el responsable del tratamiento detectase el no consentimiento del interesado. Cabe destacar que en el 92% de las ocasiones en las que se comprueba el parámetro DNT, esta comprobación es realizada por terceras partes. Esas conexiones a tercera parte son trozos de código incluidos en la página web visitada pero que se enlazan a otra página web. Por ejemplo, al visitar una página web, en un lateral aparece un marco conteniendo anuncios. La información que aparece en ese marco no tiene su origen en la propia página web visitada sino en una tercera página alojada en otro servidor web distinto.

El Anexo III incluye información sobre las detecciones de técnicas de huella digital en las webs analizadas, así como representaciones gráficas con información sobre las principales funciones utilizadas.

Sobre esa misma muestra se ha realizado un análisis para verificar el nivel de cumplimiento del deseo del usuario, expresado utilizando DNT, mediante una exploración de sitios web simulando un navegador con el DNT activado, comprobándose que los programas de extracción de la huella hacen un uso muy diverso de esta posibilidad.

A continuación, se muestra el porcentaje de visitas web en las que a pesar de haberse comprobado mediante funciones javascript que la petición DNT está activada por el usuario, se siguen haciendo llamadas a funciones sospechosas de ser utilizadas para la confección de la huella de usuario mediante alguna de las técnicas avanzadas estudiadas:




Como se puede ver, en el mejor de los casos (Canvas Font), el 60% de las ocasiones en que se chequea la variable DNT, se continúa confeccionando la huella e ignorando el deseo del usuario.

En el peor de los casos (Canvas), el 96,12% de las ocasiones en que se chequea la variable DNT, se continúa confeccionando la huella e ignorando el deseo del usuario.

Examinado con mayor detalle, se ha podido comprobar que, no es que el programa que confecciona la huella vulnere la solicitud del usuario expresada a través del valor de la variable DNT, sino que estos programas pueden incluso utilizar la variable DNT para confeccionar la huella como un factor de singularización adicional.

**EFICACIA DE MEDIDAS DE MITIGACIÓN**

Todos los navegadores web de uso general permiten instalar extensiones (también conocidas como plugins o add-ons) que amplían o modifican la funcionalidad del navegador. Entre éstas existen algunas cuya funcionalidad es la mejora de la privacidad del usuario en forma de bloqueadores de publicidad y, en definitiva, bloqueadores de herramientas de seguimiento de usuario. Entre las más conocidas están uBlock Origin, Ghostery, Disconnect, Adguard, Adsafe y Adblock.

En esta fase final del estudio se pretende valorar si la instalación de alguna de las extensiones que promete mejorar la privacidad puede ser de ayuda y realmente cumplen eficazmente con esa funcionalidad. Se estudiarán únicamente opciones de código abierto como Disconnect, Ghostery y uBlock Origin, por ser además los más extendidos entre los usuarios.

La herramienta OpenWPM permite realizar un estudio de este tipo, realizando visitas automáticas con diferentes extensiones y configuraciones de opciones de privacidad en el navegador. Pensando en minimizar los tiempos de estudio se ha generado una lista conteniendo únicamente urls en las que se han detectado técnicas de fingerprinting. El resultado es una lista con aproximadamente 1.400 webs sobre las que analizar las diferentes extensiones.

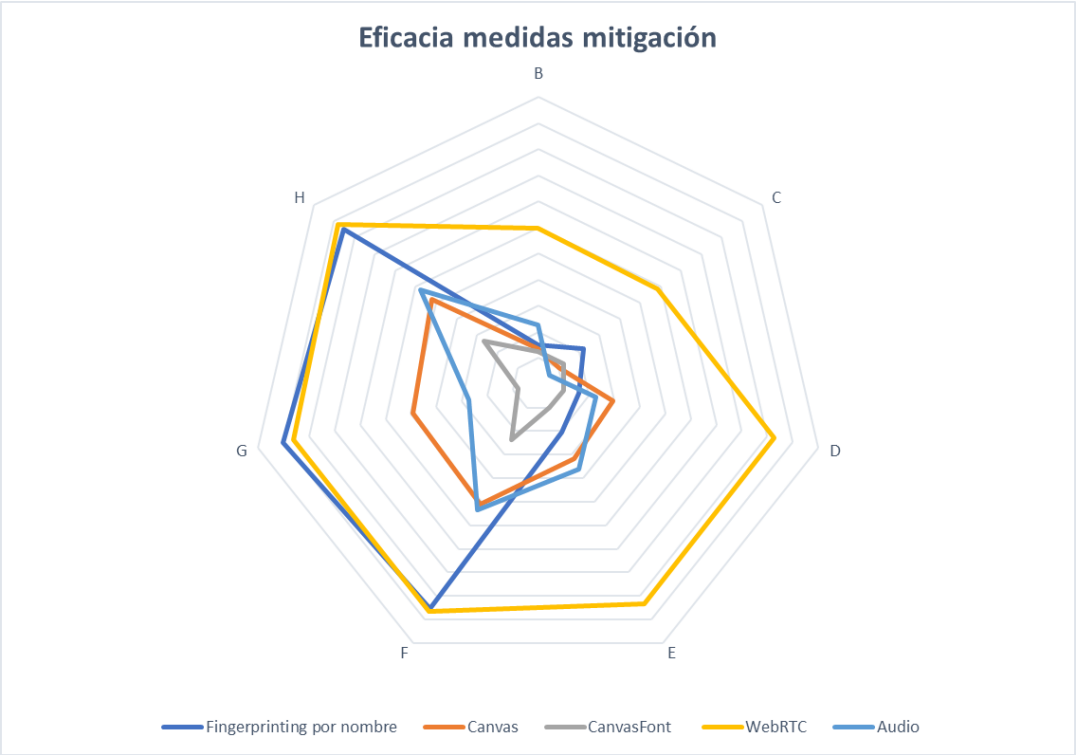
En la siguiente tabla se muestran las diferentes pruebas que se han realizado y la configuración de las opciones de privacidad y extensiones del navegador en cada una de ellas.

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| Aceptar cookies de 3ª partes | Siempre | Siempre | Nunca | Siempre | Siempre | Siempre | Siempre | Nunca |
| Flash deshabilitado | No | Si | Si | No | Si | Si | Si | Si |
| Petición “DoNotTrack” | No | Si | Si | Si | Si | Si | Si | Si |
| Ghostery | No | No | No | No | No | No | Si | No |
| Disconnect | No | No | No | Si | Si | No | No | No |
| ublock Origin | No | No | No | No | No | Si | No | Si |

Se toma prueba A como referencia inicial para medir la eficacia de las diferentes opciones de configuración y para el resto de pruebas se cuantifica la reducción de llamadas a funciones características de figerprinting. En la siguiente tabla se muestran los resultados obtenidos durante las diferentes pruebas y a continuación una representación gráfica de estos datos.

| **Técnica detectada** | **B** | **C** | **D** | **E** | **F** | **G** | **H** |
|---|---|---|---|---|---|---|---|
| fingerprinting por nombre función | -5,0% | -12,0% | -5,9% | -10,5% | -85,3% | -90,1% | -85,3% |
| canvas | -3,6% | 0,0% | -19,2% | -21,7% | -40,9% | -39,4% | -41,9% |
| canvas font | -2,5% | -2,5% | 0,0% | 0,0% | -13,8% | 2,1% | -16,7% |
| webRTC | -49,7% | -48,5% | -82,8% | -83,4% | -86,6% | -86,0% | -87,9% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| audiocontext | -12,7% | 4,5% | -12,7% | -26,1% | -43,3% | -17,2% | -47,8% |




Como se puede comprobar, la activación de las opciones de privacidad que incluyen los navegadores (pruebas B, C) como deshabilitar la tecnología Flash, enviar la petición de no seguimiento y bloquear las cookies de terceros no produce una reducción significativa de las detecciones de técnicas fingerprinting, excepto para el caso de webRTC. Sin embargo, la activación de bloqueadores de publicidad sí parece ofrecer una mejora en la protección contra el seguimiento de terceras partes mediante fingerprinting, en tanto que se produce una reducción significativa en las detecciones.

En el Anexo III se puede encontrar información ampliada sobre los resultados obtenidos durante esta fase del estudio.

# 7. MEDIDAS AL ALCANCE DEL USUARIO

El usuario puede proteger su privacidad implantando medidas a su alcance y así evitar el uso de la huella con fines de seguimiento y perfilado. A ucontinuación, se sugieren algunas medidas que, lamentablemente, son complejas para un usuario común, dificultan la navegación en internet y tienen una efectividad limitada:

- Utilización de la opción Do Not Track del navegador

La opción Do Not Track (DNT) es el mecanismo propuesto por W3C[14] para que el usuario pueda expresar sus preferencias sobre seguimiento, de forma que un servicio web pueda deshabilitar sus técnicas de seguimiento ante la petición del usuario. Éste debe acceder al menú de opciones de su navegador e indicar si quiere tener activa esta opción, actualmente disponible por la práctica totalidad de los navegadores.

Lamentablemente, no todos los servicios web cumplen o respetan la solicitud DNT del usuario, fundamentalmente porque todavía no constituye una recomendación firme por parte del W3C y porque los requisitos de cumplimiento[15] están todavía en versión borrador. De hecho, algunos servicios web utilizan esta información como un factor más de la huella digital del usuario.

- Instalación de bloqueadores

  Actualmente se han popularizado las extensiones de navegador (también conocidas como plugins o add-ons) que amplían o modifican su funcionalidad. Uno de los tipos de extensiones son los bloqueadores, que permiten al usuario eludir la publicidad y el seguimiento del usuario.

  Se ha procedido a probar un navegador, con diferentes configuraciones, sobre webs en las que se había detectado previamente actividad de *fingerprinting*. Dichas pruebas se han comparado con el uso de las opciones de privacidad del navegador. Del resultado de dichos análisis se ha llegado a las siguientes conclusiones:

  - ✓ La activación de las opciones de privacidad que incluyen los navegadores, como deshabilitar la tecnología Flash, enviar la petición de no seguimiento y bloquear las cookies de terceros son medidas pueden ser eficaces ante otras técnicas pero no producen una reducción significativa de las detecciones de técnicas fingerprinting.
  - ✓ Sin embargo, la activación de bloqueadores de publicidad sí ha mostrado una protección efectiva contra el seguimiento de terceras partes, en tanto que se produce una reducción significativa en las detecciones.

  De las observaciones realizadas, se ha destacado como los bloqueadores más eficaces *Ghostery* y *uBlock Origin*.

- Deshabilitar el uso de Javascript

  La deshabilitación del uso de Javascript evita la captura de parte de los datos del terminal, aunque no en todos los casos, y puede impedir la navegación efectiva en muchas de las páginas web.

- Alternar el uso de navegadores

  Utilizar distintos navegadores en un mismo terminal no elimina el uso de la huella, pero permitirá que no toda la información sobre la actividad del usuario se consolide asociada a un mismo identificador.

[14] *World Wide Web Consortium* (W3C), es un consorcio internacional que genera recomendaciones y estándares para asegurar el crecimiento de la *World Wide Web* a largo plazo.
[15] https://www.w3.org/2011/tracking-protection/drafts/tracking-compliance.html

Por otro lado, el uso del navegador TOR enmascará la huella del terminal cuando se accede a internet.

- Ejecución del acceso a internet en máquinas virtuales

  Esta es una opción al alcance de usuarios más avanzados y consiste en la ejecución de aplicaciones que simulan dispositivos que utilizan distintos sistemas operativos y configuraciones de navegadores. De esta forma, se puede acceder a internet en un entorno controlado sin que se proporcione acceso a todo el terminal, aunque no se puede evitar que se filtre cierta información como la dirección IP.

Respecto a las medidas para prevenir el seguimiento, vamos a proporcionar un apunte sobre dos de ellas que no resultan efectivas:

- Navegación privada. Muchos navegadores tienen la opción de navegación privada o de incognito. Con esta opción los usuarios tienen la sensación de que su navegación es segura y no será rastreable. En esta opción el navegador no guarda información sobre páginas web, ni historial de navegación, caché web, contraseñas, información de formularios, cookies u otros datos de sitios web, y al cerrar la ventana borra del equipo del usuario toda esta información. Puede dar la sensación de que la navegación permite que el usuario esté protegido frente al uso de la huella, pero es una sensación de falsa seguridad, pues a las técnicas usadas en la confección de la huella les resulta transparente la navegación privada, ya que las características que chequea la huella son las mismas, con navegación privada o sin ella, y el equipo del usuario quedará igualmente individualizado. Así pues, en este sentido, la navegación privada no es efectiva.
- Utilización de redes de anonimización o VPN's. Aunque evitan la revelación de las direcciones IP al servidor de destino, no filtran la recogida de datos sobre las características de los terminales. Además, es necesario ser conscientes de que detrás de un servicio gratuito ha de existir una estrategia de monetización.

Para finalizar este apartado de conclusiones cabe añadir que una de las principales recomendaciones para incrementar la privacidad de un navegador es, en la medida de lo posible, reducir la instalación de otro tipo de extensiones en el navegador, por dos motivos fundamentales:

1. Uno de los factores de identificación mediante huella digital consiste en obtener una lista de extensiones o plugins del navegador, cuantas más extensiones se tengan instaladas y más alejado se encuentre el navegador de su configuración por defecto más capacidad para singularizarnos tendrá la lista de extensiones.
2. Instalar una extensión supone añadir una pieza de software en nuestro navegador desarrollado por un tercero ajeno al desarrollador del navegador, con todas las implicaciones que ello conlleva.

# 8. RECOMENDACIONES A LA INDUSTRIA

Del estudio realizado se derivan las siguientes recomendaciones tanto para los desarrolladores de productos y servicios para acceso a internet, como para aquellas entidades que explotan los datos obtenidos a partir de la huella del dispositivo:

**RECOMENDACIONES PARA FABRICANTES Y/O DESARROLLADORES**

Así como hay navegadores que incluyen la opción DNT y diversas opciones de aceptación de cookies, los fabricantes y desarrolladores de equipos susceptibles de ser objeto de las tecnologías de huella deberían incluir en sus productos las opciones necesarias para que el usuario de los mismos disponga de capacidades para denegar o aceptar, de forma total o parcial, el uso de estas tecnologías.

Además, se debería proporcionar al consumidor dichos equipos con las máximas opciones de privacidad activadas de forma predeterminada, y que sea el propio usuario quien reduzca esas opciones, si fuese su voluntad. Como buena práctica, los navegadores podrían tener la opción DNT activada por defecto.

**RECOMENDACIONES PARA ENTIDADES QUE QUIERAN UTILIZAR LA HUELLA**

El procedimiento de la huella deberá seguir, en los términos previstos del artículo 22.2 de la LSSI que traspone el artículo 5.3 de la Directiva 2002/58/CE, los requisitos de información al usuario y obtención del consentimiento. Requisitos sobre cuya aplicación se detallan criterios en la 'Guía del Uso de Cookies' de la AEPD.

En tanto el usuario no haya dado el consentimiento al tratamiento, el responsable del tratamiento debe abstenerse de recabar y tratar la huella y cualquier otro dato asociado a la misma. Además, toda aplicación de huella debería chequear el estado de la opción DNT. Si el usuario tiene habilitada dicha opción, debería ser interpretado como una negativa clara, y actuar en consecuencia. Como buena práctica, los proveedores de servicio deberían considerar tener activada la opción DNT en los casos en los que no se haya establecido una preferencia clara por parte del usuario.

Aun cuanto la opción DNT esté inactiva, debe, igualmente, darse la oportunidad de otorgar su consentimiento previo al tratamiento de huella para finalidades más allá de la estricta para proporcionar el servicio, así como la posibilidad de retirarlo posteriormente.

En todo caso, en la medida que las técnicas de huella del dispositivo recojan datos personales conforme a lo establecido en el artículo 4.1 y considerando 26 del RGPD, el régimen de tratamiento está sometido a lo previsto en el mismo, en particular en cuanto al ejercicio de derechos.

La entidad ha de confeccionar un registro de actividades de tratamiento, en el que se incluyan los tratamientos que utilicen la *huella*.

Deberá igualmente evaluar si cumple los criterios para contar con los servicios de un Delegado de Protección de Datos y contratarlo siguiendo los criterios que fija el RGPD. Su asesoramiento será muy importante para poder adaptarse al RGPD.

Igualmente, deberán realizar un análisis de riesgos de protección de datos relativos a los derechos y libertades de los afectados. Si de dicho análisis se deriva que el nivel de riesgo es elevado, será entonces obligada la realización de una Evaluación de Impacto para la Protección de Datos (EIPD) para establecer las medidas necesarias que garanticen la protección de los derechos de los usuarios.

Esta evaluación de impacto deberá contemplar, al menos, los siguientes riesgos:

- El impacto del filtración de la información de perfilado contenidas en las bases de datos.
- En relación con la anterior, el acceso a dicha información por organizaciones gubernamentales o políticas.
- La utilización de sesgos sociales, culturales, raciales, etc, que conlleven decisiones automáticas.
- El acceso por empleados o terceros a datos de usuarios concretos.
- La utilización de los datos para la realización de acoso social, político o de género.
- La recogida excesiva de datos y su conservación por un tiempo excesivo.
- El impacto sobre la percepción de la libertad de actuación del uso de la información de perfilado.
- La manipulación de los deseos, creencias y estado emocional de los usuarios.
- En relación con los anteriores, el riesgo de una reidentificación.

Como resultado de la EIPD deberán establecerse los requisitos de Privacidad por Defecto, aplicar las medidas de Privacidad desde el Diseño, y definir los requisitos concretos de confidencialidad, disponibilidad, integridad, autenticación y trazabilidad que, desde la perspectiva de protección de datos, se utilicen en la gestión de riesgos de la seguridad del sistema de información que trata dichos datos.

# 9. CONCLUSIONES

Del análisis de la información expuesta en los apartados anteriores, los problemas que presenta la huella serían los siguientes:

- Las técnicas de fingerprinting recogen datos del equipo del usuario, de forma general, sin su conocimiento ni consentimiento, tratando información sobre las características del terminal, en algunos casos con una finalidad distinta del propósito técnico inicialmente previsto, mediante la ejecución en el terminal de aplicaciones que captan y transmiten datos hacia los servidores del responsable del tratamiento.
- El conjunto de datos recabados puede ser tan extenso, o enriquecerse de tal forma, que identifique unívocamente al usuario, y entre los mismos se pueden encontar algunos definidos como de categoría especial según el RGPD. Este conjunto es, a priori, desconocido, se plantean serias dudas sobre la aplicación del principio de minimización de datos, así como del periodo durante el cual son almacenados.

- No se proporcionan herramientas para poder evitar la recogida de datos, ya que una vez iniciado el acceso la página en internet, y antes de que el usuario haya podido visualizarlo, el servidor ya tiene toda la información de su fingerprint.
- Incluso se han detectado casos en los que, de forma general, no se atiende a la configuración DNT (Do Not Track) establecida por el usuario para desactivar la recogida de la huella digital en los servicios de Internet.
- No se cumple con la obligación de obtener el consentimiento informado y, en particular, respecto a la finalidad para la que se recaban los datos, ya que dichas técnicas se utilizan generalmente para realizar perfilado del usuario (entre las cuales cabe la toma de decisiones con consecuencias sobre el servicio) y analizar su actividad en internet.
- El usuario no dispone de medios para ejercer los derechos establecidos en el RGPD cuando se recogen o asocian a datos personales.

El impacto que tiene el uso de estas técnicas sobre los derechos y libertades de los usuarios no ha sido analizado por los responsables del el modelo de huella del dispositivo, ni se ha informado de las medidas establecidas para minimizar el riesgo así como para evitar los efectos potenciales de una brecha de seguridad.

El tratamiento de datos mediante técnicas de huella del dispositivo ha de seguir los criterios recogidos en la 'Guía del Uso de Cookies' de la AEPD y lo establecido en el Reglamento General de Protección de Datos en los tratamiento de datos de carácter personal.

## Trabajos citados

Eckersley, P. (2010). *A Primer on Information Theory and Privacy*. Retrieved from Electronic Frontier Foundation: https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy

Eckersley, P. (2010). ow Unique Is Your Web Browser? *Privacy Enhancing Technologies*.

Englehardt, S., & Narayanan, A. (2016). Online Tracking: A 1-million-site Measurement and Analysis. *Proceedings of ACM CCS 2016*.

Laperdrix, P., Rudametkin, W., & Baudry, B. (2016). Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints. *37th IEEE Symposium on Security and Privacy*.

Mowery, K., & Shacham, H. (2012). Pixel Perfect: Fingerprinting Canvas in HTML5.

N. Nikiforakis, A. K. (2013). Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting,. *2013 IEEE Symposium on Security and Privacy*, 541-555.

# ANEXO I

**Características de identificación:**

Algunas de las características que se pueden detectar mediante el navegador web y que pueden contribuir a la obtención de una huella digital de un dispositivo son:

- User Agent: Se trata de una cadena de texto que el navegador envía en las cabeceras de las peticiones HTTP al servidor. Esta cadena de texto contiene información sobre el navegador que se está utilizando y el sistema operativo del dispositivo. Contiene también información sobre las versiones de navegador y sistema operativo.
- HTTP Accept Header: Cabecera HTTP Accept que se envía en las peticiones HTTP al servidor para indicar el tipo de contenido que el navegador aceptará en las respuestas del servidor.
- HTTP Accept-Charset: Cabecera HTTP Accept-Charset que se envía al servidor en las peticiones HTTP para indicarle el conjunto de caracteres que se acepta en las respuestas HTTP, por ejemplo 'utf-8'.
- HTTP Accept-Encoding: Cabecera HTTP Accept-Encoding que se envía al servidor en las peticiones HTTP para indicarle el tipo de codificación que se acepta en las respuestas, por ejemplo 'gzip, deflate'.
- HTTP Accept-Language: Cabecera HTTP Accept-Encoding que se envía al servidor en las peticiones HTTP para indicarle el idioma que se acepta en las respuestas, por ejemplo 'en-US'.
- Lista de plugins activados en el navegador: Mediante javascript se puede obtener la lista de plugins activados en el navegador web.
- Plataforma sobre la que se ejecuta el navegador: Mediante javascript se puede obtener la plataforma sobre la cual se está ejecutando la instancia del navegador, por ejemplo 'Win32'.
- Cookies habilitadas: Se detecta mediante javascript si el navegador tiene habilitadas las cookies o no.
- HTTP Do not track Header: La mayoría de navegadores actuales permiten informar a las páginas web que se visitan, sus anunciantes y sus proveedores de contenidos que el usuario no desea que se realice el seguimiento de su navegación. Esto se hace mediante una cabecera en las peticiones HTTP. Con javascript se puede detectar si esta característica ha sido activada o no.
- Zona horaria del navegador: Se puede obtener mediante javascript.
- Resolución de la pantalla: Se puede obtener mediante javascript.
- Uso de local storage: Se utiliza javascript para comprobar si se puede hacer uso de local storage proporcionado por HTML5.
- Uso de sesion storage: Se utiliza javascript para comprobar si se puede hacer uso del sesion storage proporcionado por HTML5.
- WebGL Vendor: Algunos navegadores proporcionan la identificación completa de la tarjeta gráfica instalada en el sistema.

- WebGL Renderer: Algunos navegadores proporcionan el nombre completo del driver gráfico instalado en el sistema.
- Lista de fuentes de texto: Mediante javascript se puede detectar.
- Uso de bloqueadores de publicidad: Se realizan diversas comprobaciones para determinar el empleo de bloqueadores de publicidad en el navegador.
- Dispositivo táctil: Se detecta si el dispositivo dispone de pantalla táctil.
- IP pública con la que el dispositivo se conecta a internet.

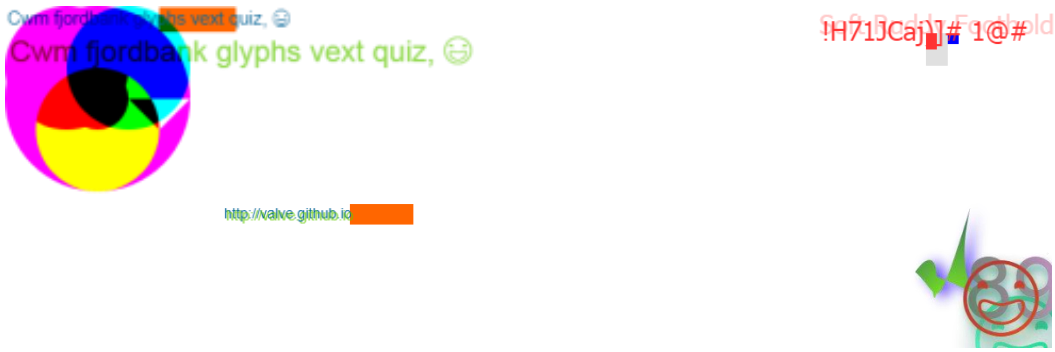
## Técnicas avanzadas de huella digital sobre las que se centra este estudio:

a) **CANVAS:**

Se hace uso del elemento canvas de HTML5 para renderizar una determinada imagen mediante javascript. Esta imagen será renderizada de forma sutilmente diferente por las diferencias de hardware/software de cada dispositivo. Estas sutiles diferencias pueden detectarse al objeto de identificar los dispositivos.

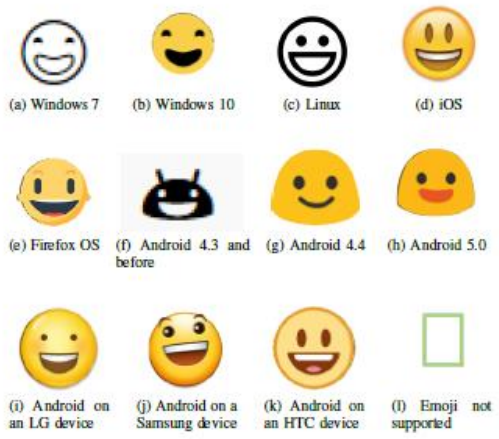
HTML Canvas es un elemento que se utiliza para dibujar en tiempo real en páginas web utilizando código JavaScript que se ejecuta en el navegador del usuario. El elemento Canvas es únicamente un contenedor para gráficos, se necesita hacer uso de lenguajes como JavaScript para dibujar en el contenedor. HTML Canvas tiene diferentes métodos que permiten dibujar líneas, rectángulos, arcos, texto y añadir imágenes. Este elemento, HTML Canvas, se puede utilizar para hacer *fingerprinting* de usuarios (Mowery & Shacham, 2012). Diferencias en la renderización de fuentes, suavizados, anti-aliasing y otras características hacen que cada dispositivo dibuje la imagen de forma sutilmente diferente, lo que permite obtener una huella digital del usuario. El factor que forma parte de la huella digital del dispositivo es un hash de la imagen particular renderizada por el dispositivo.

Algunos ejemplos de imágenes generadas mediante JavaScript en webs para identificar usuarios se muestran en la Figura 1. Estas imágenes se renderizan en el navegador pero no se muestran al usuario.




- **Figura 1: Ejemplos de imágenes utilizadas en Canvas Fingerprinting.**

La mayoría de las cadenas de texto incluyen caracteres especiales Unicode, en los que las diferencias de renderización se hacen si cabe más evidentes. Este es el caso por ejemplo del carácter UNICODE U+1F603, que representa el emoji 'cara sonriente'. En la figura 2 se muestran las diferencias de renderización de este carácter en diferentes dispositivos (Laperdrix, Rudametkin, & Baudry, 2016).




➢ **Figura 2: Diferente renderización de un mismo carácter UNICODE.**

**CANVAS FONT:**

La lista de fuentes de texto de un dispositivo o navegador web es una característica que unida a otras puede utilizarse para obtener un identificador único para cada usuario (Eckersley, How Unique Is Your Web Browser?, 2010).

Canvas Font Fingerprinting se considera una variante de Canvas Fingerprinting, en la que se utiliza una lista de fuentes de texto para generar múltiples veces (generalmente varias decenas) imágenes de una misma cadena de texto. La variedad de fuentes unida a las sutiles diferencias de renderización permite extraer métricas sobre el texto generado en las imágenes que sirven para generar un identificador único del navegador.

Cuando el navegador no facilita la lista de fuentes mediante Flash o Javascript, se puede utilizar esta misma técnica para detectar la presencia de determinadas fuentes en el sistema. Se realiza una primera renderización con una fuente inexistente que provoca que el navegador renderice con la fuente por defecto. La obtención de métricas de la fuente por defecto permite por comparación ir elaborando una lista de fuentes presentes en el sistema a base de renderizar la misma cadena de texto con una lista de fuentes predeterminada.

**WEBRTC:**

Esta técnica consiste en el uso de la API WebRTC de HTML5 para obtener la IP local (IP detrás de un NAT) de un dispositivo. La IP local en combinación con la IP pública constituye un factor de identificación del dispositivo muy consistente.

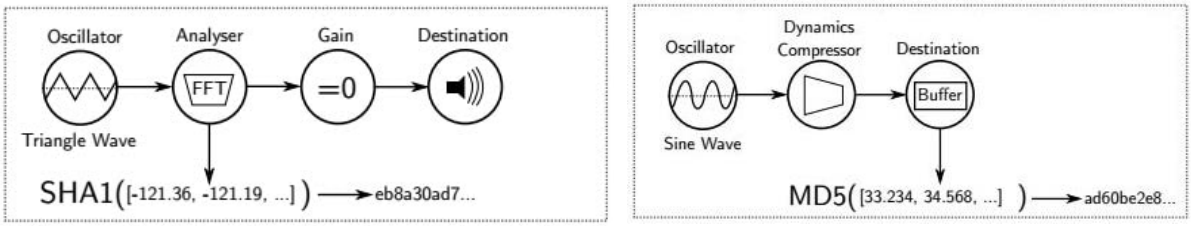
WebRTC es un framework libre y de código abierto que proporciona a navegadores y aplicaciones móviles capacidades de comunicación en tiempo real (Real-Time Communications RTC) p2p (peer to peer) entre dispositivos. Para determinar el mejor camino en la red entre los dispositivos, cada uno de ellos recoge información sobre las direcciones del otro, incluido direcciones IP de redes locales (Ethernet o WiFi) y direcciones del lado público del NAT, haciéndolas disponibles a la aplicación web sin el consentimiento explícito del usuario [Apartado 6.3 de (Englehardt & Narayanan, 2016)]. Las aplicaciones web pueden acceder a las direcciones IP locales de los usuarios detrás de un NAT (Network Address Translation), y esta información es muy útil con fines de seguimiento. Pongamos el ejemplo de una red local con 20 dispositivos conectados a la red y a internet a través de un router. Una aplicación web podría acceder a la IP pública de la red/router y a la IP privada de cada uno de los dispositivos, pudiendo singularizar perfectamente cada dispositivo a pesar de estar detrás de un router.

**AUDIOCONTEXT:**

Se utiliza la API AudioContext de HTML5 para realizar una serie de procesamientos sobre una señal de audio fija. Las ligeras diferencias en el resultado del procesamiento según el hardware/software del sistema concreto permiten particularizar el dispositivo.

Este tipo de técnica funciona de forma muy similar al Canvas Fingerprinting, pero utilizando audio en lugar de imágenes. Mediante la utilización de la librería AudioContext disponible en la mayoría de navegadores más recientes se pueden utilizar las sutiles diferencias de renderización de una señal de audio determinada, por ejemplo una señal sinusoidal o triangular, para generar una huella digital. Cabe reseñar que el uso de esta técnica no implica recoger señales de audio reproducidas o grabadas en el dispositivo, sino que se trata de una propiedad de la pila de proceso de audio del dispositivo.

Los dos métodos más utilizados para AudioContext fingerprinting se muestran en la Figura 2 (Englehardt & Narayanan, 2016). Ambos métodos procesan una señal generada mediante un *OscillatorNode* para luego leer la señal resultante y generar un hash que constituye la huella digital generada. La misma señal de audio procesada por distintos dispositivos o navegadores tendrá sutiles diferencias debido a las diferencias de hardware/software entre dispositivos.




➢ **Figura 3: Métodos AudioContext Fingerprinting.**

# ANEXO II

## Patrones de detección de fingerprinting

La detección de técnicas de fingerprinting se ha realizado mediante la identificación de determinados patrones en los datos registrados durante las navegaciones automáticas con la herramienta OpenWPM. Estos patrones están basados en los descritos en (Englehardt & Narayanan, 2016).

### a) DETECCIÓN DE TÉCNICAS FINGERPRINTING EN GENERAL

Este patrón de detección es el más sencillo de todos, pues se trata de identificar en el código de las webs analizadas las llamadas a funciones javascript con nombres alusivos a este tipo de técnicas. Es decir, se identifican llamadas a funciones con nombres como '*getCanvasFingerprint*', '*getFP*', '*getFingerprint*'. Este patrón de detección tiene la ventaja de permitir la detección de todo tipo de técnica de huella digital y la desventaja de no detectar el uso de técnicas de huella digital cuando los nombres de funciones no son alusivos al uso de este tipo de técnicas.

En la tabla 1 se muestran ejemplos de detecciones reales identificadas mediante la herramienta OpenWPM.

| visit_id | func_name | short_script_url |
|---|---|---|
| 3087 | e.prototype.**getCanvasFp** | crm.clubenvero.es/mtc.js |
| 3857 | window.SN</</**FingerPrint**</t</e.prototype.getHasLied Browser | d1af033869koo7.cloudfront.net/psp/platform/247px.js |
| 441 | q.**getFingerPrint** | mc.yandex.ru/metrika/watch.js |
| 215 | a.prototype.**getCanvasFingerprint** | prod-js.aws.y-track.com/v5/profile-hub.min.js |
| 216 | a.prototype.**getCanvasFingerprint** | prod-js.aws.y-track.com/v5/profile-hub.min.js |
| 3035 | Fingerprint.prototype.**getCanvasFingerprint** | s3.amazonaws.com/dmp-pr-production/JScript/fingerprintjs/fingerprint.js |
| 1371 | hj.**fingerprinter**.prototype.getHasLiedBrowser | script.hotjar.com/modules-b4b50aa474eaa7a39e3ccc9eed6884eb.js |
| 3155 | b.prototype.**getCanvasFp** | static.brandcrumb.com/bbva.js |
| 3155 | b.prototype.**getCanvasFp** | static.brandcrumb.com/bc.js |
| 2053 | [1]</a.prototype.**getCanvasFp** | www.edreams.es/drmsdstl.js |
| 2221 | e.**Fingerprint**2</t.prototype.getHasLiedBrowser | www.thehotelsnetwork.com/js/hotel_price_widget.js |
| 4075 | **Fingerprint**2.prototype.getHasLiedBrowser | www.thehotelsnetwork.com/js/hotel_price_widget.js |

**Tabla 1: Funciones javascript con nombres alusivos al empleo de técnicas fingerprinting.**

**DETECCIÓN DE CANVAS FINGERPRINTING:**

Para la detección de esta técnica se han utilizado dos patrones de identificación:

- Patrón C1: Llamadas desde una misma función JavaScript a canvas.toDataURL para obtener un hash de una imagen y canvas.fillText para escribir cadenas de texto en una imagen. En concreto serán particularmente sospechosas aquellas funciones que llamen 2 veces a canvas.fillText y una única vez a canvas.toDataURL, aunque no se pueden descartar otras combinaciones. Este patrón de identificación es típico del uso de canvas fingerprint, y se muestran algunos ejemplos de detección en la tabla 2.

| visit_id | func_name | toDataURL Count | fillText Count | short_script_url |
|---|---|---|---|---|
| 215 | a.prototype.getCanvasFingerprint | 1 | 2 | prod-js.aws.y-track.com/v5/profile-hub.min.js |
| 216 | a.prototype.getCanvasFingerprint | 1 | 2 | prod-js.aws.y-track.com/v5/profile-hub.min.js |
| 683 | cv/</</dF</N[112]</d | 1 | 2 | mmesbkildq-a.akamaihd.net/FLE5J21L2U.js |
| 861 | p.prototype.getCanvasPrint | 1 | 2 | cdn3.streamlike.com/secure/player/js/clientjs.js |
| 917 | l | 1 | 2 | www.logistics.dhl/akam/10/4731bef2 |
| 1023 | p.prototype.getCanvasPrint | 1 | 2 | cdn3.streamlike.com/secure/player/js/clientjs.js |
| 1285 | p.prototype.getCanvasPrint | 1 | 2 | cdn3.streamlike.com/secure/player/js/clientjs.js |
| 2221 | e.Fingerprint2</t.prototype.getCanvasFp | 1 | 2 | www.thehotelsnetwork.com/js/hotel_price_widget.js |
| 3035 | Fingerprint.prototype.getCanvasFingerprint | 1 | 2 | s3.amazonaws.com/dmp-pr-production/JScript/fingerprintjs/fingerprint.js |
| 3155 | b.prototype.getCanvasFp | 1 | 2 | static.brandcrumb.com/bc.js |
| 3723 | f | 1 | 2 | cdn.doubleverify.com/dvtp_src_internal121.js |
| 3857 | window.SN</</FingerPrint</t</e.prototype.getCanvasFp | 1 | 2 | d1af033869koo7.cloudfront.net/psp/platform/247px.js |
| 4075 | Fingerprint2.prototype.getCanvasFp | 1 | 2 | www.thehotelsnetwork.com/js/hotel_price_widget.js |
| 4443 | StripeM</t.default< | 1 | 2 | m.stripe.network/inner.html |

**Tabla 2: Detecciones mediante patrón C1: funciones javascript con 2 llamadas a fillText y 1 a toDataURL.**

- Patrón C2: Llamadas desde una misma función javascript a canvas.fillText para renderizar cadenas de texto concretas que han sido identificadas anteriormente como firmas típicas del empleo de técnicas canvas fingerprint. En muchos casos se trata de funciones de código abierto muy accesibles para cualquier desarrollador. Este indicador arroja resultados sin prácticamente falsos positivos, pero a cambio puede acarrear un número alto de falsos negativos por el empleo de cadenas de texto no identificadas.
  Ejemplos de detecciones mediante este patrón se pueden ver en la tabla 3, en la que se destacan en negrita las firmas identificadas.

| visit_id | arguments | KnowText Count | short_script_url |
|---|---|---|---|
| 92 | {"0":"**Hel$&?6%){mZ+#@**","1":2,"2":2} | 1 | www.iberia.com/ibcomv3/rbrand/scripts/libs/iberialib.js |
| 175 | {"0":"**!H71JCaj)]# 1@#**","1":4,"2":8} | 2 | www.vueling.com/akam/10/392f2669 |
| 215 | {"0":"**http://valve.github.io**","1":4,"2":17} | 2 | prod-js.aws.y-track.com/v5/profile-hub.min.js |
| 683 | {"0":"**al;kscja;lkdfjkAKJKJX😂**","1":4,"2":45} | 2 | mmesbkildq-a.akamaihd.net/FLE5J21L2U.js |
| 861 | {"0":"**ClientJS,org <canvas> 1.0**","1":4,"2":17} | 2 | cdn3.streamlike.com/secure/player/js/clientjs.js |
| 917 | {"0":"**!H71JCaj)]# 1@#**","1":4,"2":8} | 2 | www.logistics.dhl/akam/10/4731bef2 |
| 927 | {"0":"**<@nv45. F1n63r,Pr1n71n6!**","1":10,"2":40} | 1 | www.adidas.es/_bm/async.js |
| 1897 | {"0":"**Cwm fjordbank glyphs vext quiz, 😂**","1":2,"2":15} | 1 | fba.omniretailgroup.net/main-bru-built.js |
| 1897 | {"0":"**<@nv45. F1n63r,Pr1n71n6!**","1":10,"2":40} | 1 | www.toysrus.com/_bm/async.js |
| 3723 | {"0":"**!image!**","1":4,"2":17} | 2 | cdn.doubleverify.com/dvtp_src_internal121.js |
| 3857 | {"0":"**Cwm fjordbank glyphs vext quiz, 😂**","1":4,"2":45} | 2 | d1af033869koo7.cloudfront.net/psp/platform/247px.js |

**Tabla 3: Scripts que utilizan cadenas de texto típicas de librerías para canvas fingerprinting.**

**DETECCIÓN DE CANVAS FONT FINGERPRINTING:**

Para la detección de esta técnica se han utilizado dos patrones de identificación:

- Patrón CF1: Llamadas a canvas.measureText desde una misma función javascript en múltiples ocasiones (más de 30 ocasiones, por ejemplo). Esta vía de detección se puede afinar si todas las llamadas utilizan la misma cadena de texto y cambiando la fuente de texto a utilizar en cada ocasión.
  En la tabla 4 se muestran ejemplos de detecciones de este tipo, ya que en la columna "measureTextCount" se muestra el número de llamadas a measureText.

| visit_id | func_name | measureText Count | short_script_url |
|---|---|---|---|
| 211 | nds.common.bi.getFontMetrics | 68 | api-ob.nd.nudatasecurity.com/2.2/w/w-766580/sync/js/ |
| 212 | nds.common.bi.getFontMetrics | 68 | api-ob.nd.nudatasecurity.com/2.2/w/w-766580/sync/js/ |
| 395 | td_2C | 174 | regstat.betfair.com/fp/check.js |
| 1213 | td_0s | 174 | cdn1.f-cdn.com/fp/check.js |
| 1227 | cp< | 82 | www.iberia.com/ibcomv3/rbrand/scripts/libs/iberialib.js |
| 1605 | td_1T | 174 | datawi.pokerstars.com/fp/check.js |
| 2599 | cp< | 82 | www.westernunion.com/etc/clientlibs/westernunion/wu_common.js |
| 3023 | d | 497 | mathid.mathtag.com/d/i.js |
| 3481 | r | 58 | m.stripe.network/inner.html |

**Tabla 4: Scrips con funciones que llaman en más de 30 ocasiones a la función measureText.**

- Patrón CF2: Llamadas de canvas.measureText con cadenas de texto típicas de funciones desarrolladas para hacer Canvas Font Fingerprint.
  En la tabla 5 se muestran ejemplos de detecciones reales que cumplen estos patrones. Al igual que en el caso anterior, este método no proporciona prácticamente ningún falso positivo a cambio de posiblemente muchos falsos negativos por la utilización de cadenas de texto no identificadas.

| visit_id | arguments | KnowFontText Count | short_script_url |
|---|---|---|---|
| 211 | {"0":"**mmmmmmmmmlli**"} | 68 | api-ob.nd.nudatasecurity.com/2.2/w/w-766580/sync/js/ |
| 212 | {"0":"**mmmmmmmmmlli**"} | 68 | api-ob.nd.nudatasecurity.com/2.2/w/w-766580/sync/js/ |
| 395 | {"0":"**gMcdefghijklmnopqrstuvwxyz012345 6789**"} | 174 | regstat.betfair.com/fp/check.js |
| 1213 | {"0":"**gMcdefghijklmnopqrstuvwxyz012345 6789**"} | 174 | cdn1.f-cdn.com/fp/check.js |
| 1227 | {"0":"**0-_{w.**"} | 82 | www.iberia.com/ibcomv3/rbrand/scripts/libs/iberialib.js |
| 1415 | {"0":"**mmmmmmmmmlli**"} | 58 | m.stripe.network/inner.html |
| 1435 | {"0":"**mmmmmmmmmlli**"} | 58 | m.stripe.network/inner.html |
| 1605 | {"0":"**gMcdefghijklmnopqrstuvwxyz012345 6789**"} | 174 | datawi.pokerstars.com/fp/check.js |
| 2599 | {"0":"**0-_{w.**"} | 82 | www.westernunion.com/etc/clientlibs/westernunion/wu_com mon.js |

**Tabla 5: Scripts que utilizan cadenas de texto típicas de canvas font fingerprinting.**

### DETECCIÓN DE WEBRTC Y AUDIOCONTEXT FINGERPRINTING:

La detección de WebRTC y AudioContext fingerprinting se basa en la identificación de funciones javascript que hacen uso de determinadas funciones típicas de estas técnicas de identificación.

# ANEXO III

a) **TABLA RESULTADOS ANÁLISIS POR TEMÁTICA:**

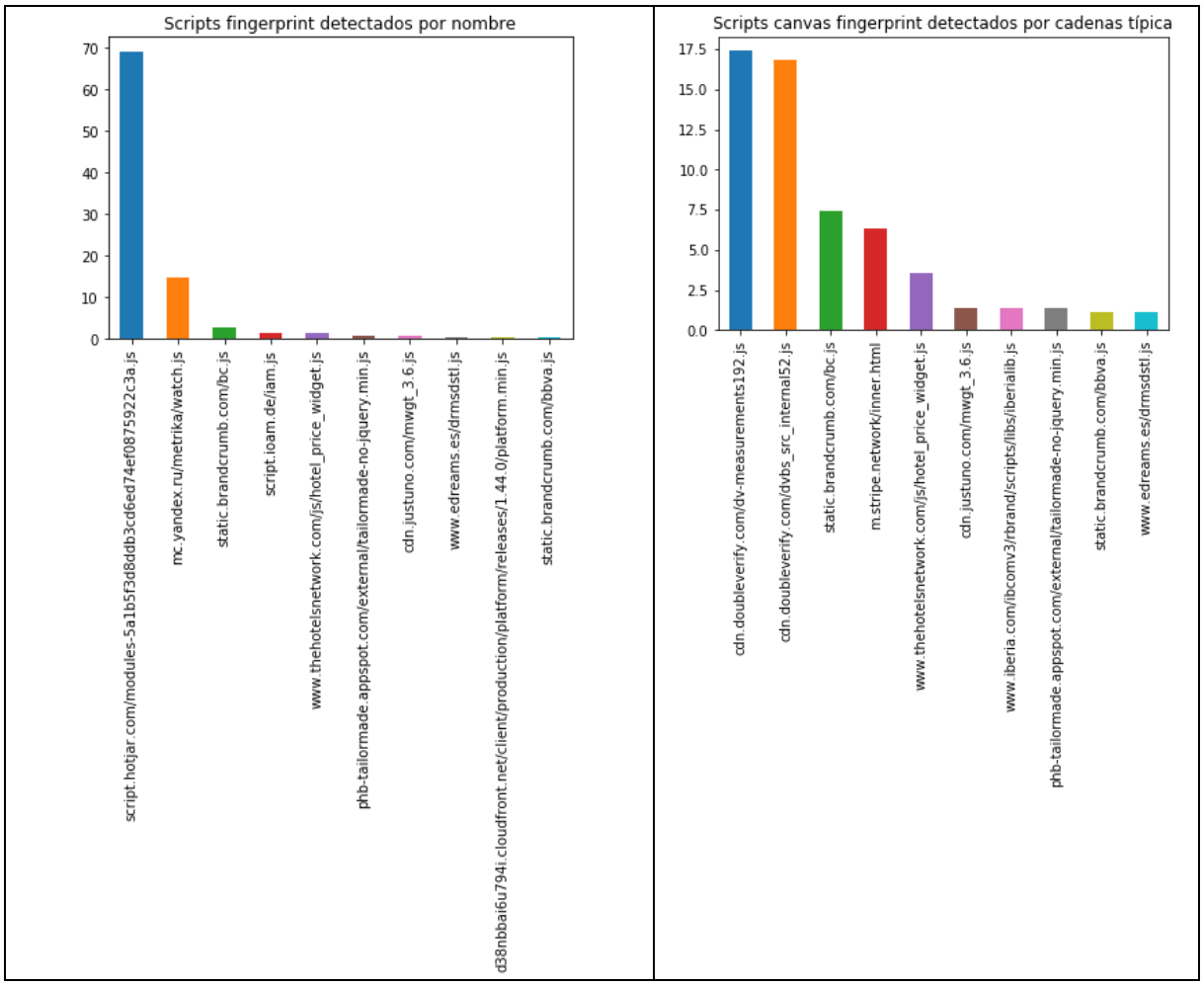
| | canvas | canvas font | webRTC | audiocontext | Total |
|---|---|---|---|---|---|
| sexo | 21% | 3% | 20% | 2% | 46% |
| deportes | 21% | 5% | 19% | 1% | 46% |
| pornografía | 16% | 1% | 23% | 1% | 41% |
| religión | 23% | 3% | 5% | 2% | 33% |
| salud | 12% | 3% | 16% | 0% | 31% |
| alcohol | 17% | 1% | 8% | 1% | 27% |
| política | 10% | 3% | 13% | 1% | 27% |
| noticias | 12% | 3% | 11% | 1% | 27% |
| apuestas | 9% | 3% | 13% | 0% | 25% |
| drogas | 17% | 1% | 4% | 0% | 22% |
| viajes | 13% | 1% | 6% | 1% | 21% |
| compras | 11% | 1% | 3% | 3% | 18% |
| hogar | 9% | 1% | 2% | 0% | 12% |

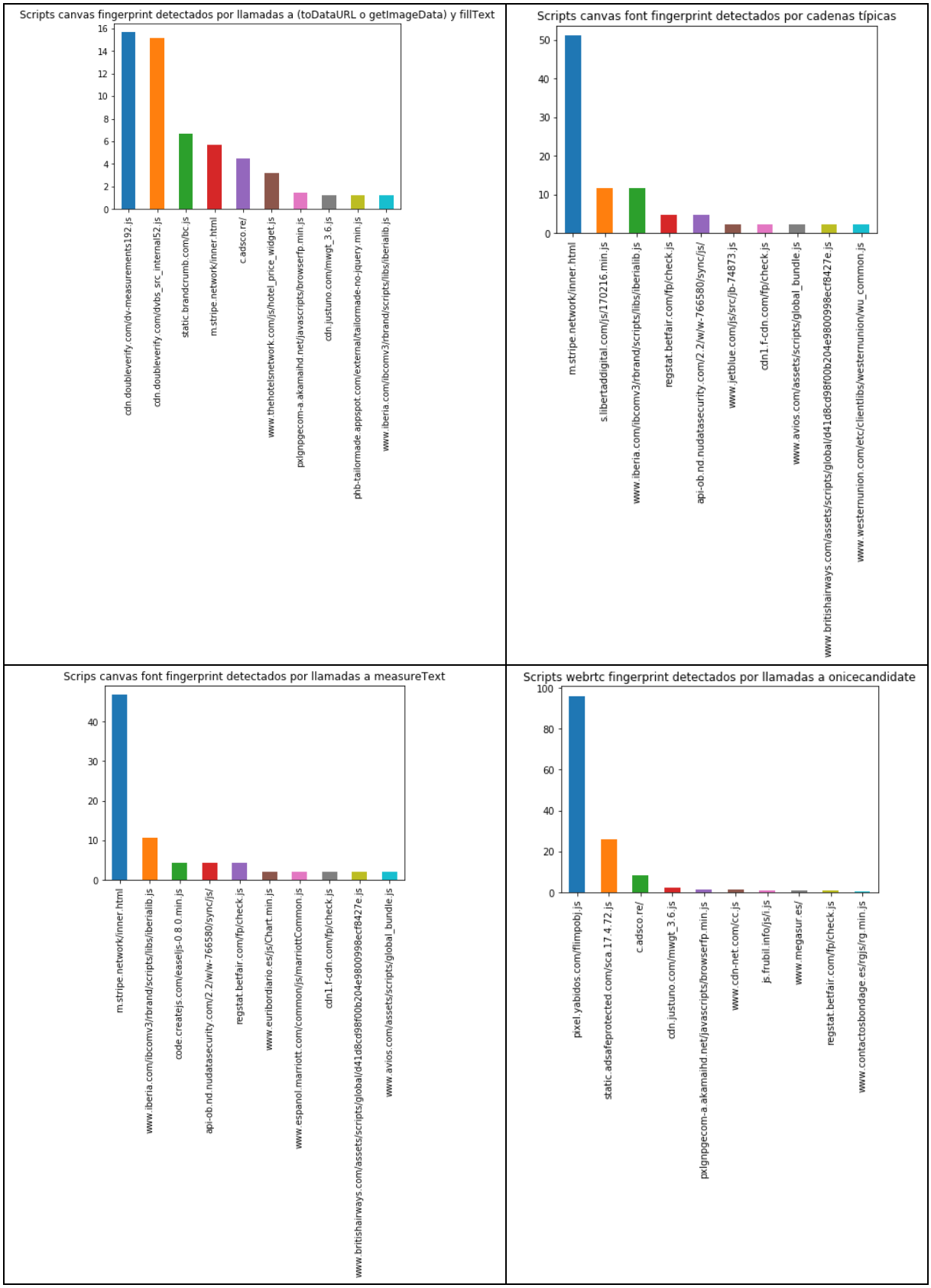
**TÉCNICAS FINGERPRINTING DETECTADAS EN PRUEBA SOBRE 14.442 SITIOS WEB**

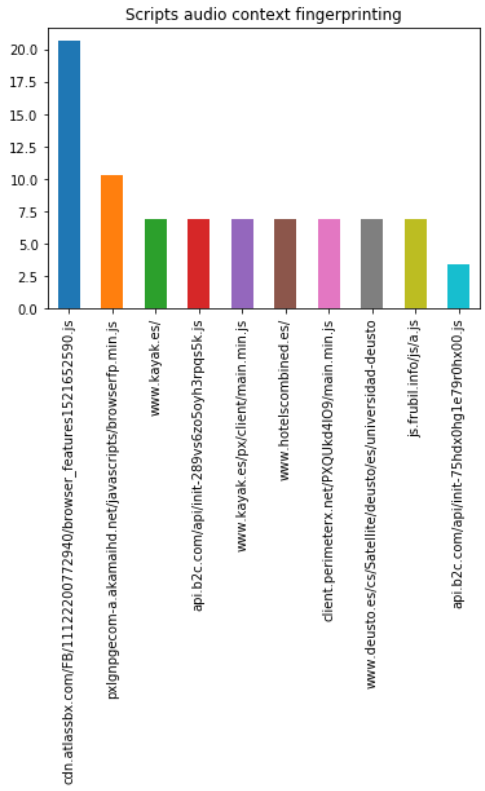
- Sitios web que llaman a funciones con nombres alusivos a fingerprinting en 1.107 visitas, esto supone un 7.7% del total de webs visitadas.
- Sitios web con funciones que utilizan llamadas a toDataURL y fillText (patrón de identificación C1), típicamente utilizadas para Canvas Fingerprint, en 402 visitas, lo que supone un 2.8% del total de webs visitadas.
- Sitios web con funciones que utilizan cadenas de texto típicas de Canvas Fingerprint (patrón de identificación C2) en 369 visitas, lo que supone un 2.6% del total de webs visitadas.
- Sitios web con funciones que realizan más de 30 llamadas a la función measureText (Patrón de identificación CF1), típico en las técnicas de Canvas Font Fingerprinting, en 38 visitas, lo que supone apenas un 0.26% de las visitas realizadas.
- Sitios web con funciones que utilizan cadenas de texto típicas de Canvas Font Fingerprinting (patrón de identificación CF2) en 43 visitas, lo que supone apenas un 0.3% de las visitas realizadas.
- Sitios web con llamadas a función onicecandidate, típicamente utilizado por técnicas WebRTC fingerprinting para obtener la IP privada del dispositivo en 221 visitas, lo que supone un 1.5% del total de visitas realizadas.
- Sitios web con llamadas a funciones típicas de AudioContext Fingerprinting en 29 visitas, lo que supone apenas un 0.2% del total de visitas realizadas.

**ANÁLISIS DE LOS SCRIPTS MÁS UTILIZADOS**

Porcentaje de utilización de algunos scripts en los que se han detectado técnicas de fingerprinting.




Scripts canvas fingerprint detectados por llamadas a (toDataURL o getImageData) y fillText
cdn.doubleverify.com/dv-measurements192.js
cdn.doubleverify.com/dvbs_src_internal52.js
static.brandcrumb.com/bc.js
m.stripe.network/inner.html
c.adsco.re/
www.thehotelsnetwork.com/js/hotel_price_widget.js
pxlgnpgecom-a.akamaihd.net/javascripts/browserfp.min.js
cdn.justuno.com/mwgt_3.6.js
phb-tailormade.appspot.com/external/tailormade-no-jquery.min.js
www.iberia.com/ibcomv3/rbrand/scripts/libs/iberialib.js
Scripts canvas font fingerprint detectados por cadenas típicas
m.stripe.network/inner.html
s.libertaddigital.com/js/170216.min.js
www.iberia.com/ibcomv3/rbrand/scripts/libs/iberialib.js
regstat.betfair.com/fp/check.js
api-ob.nd.nudatasecurity.com/2.2/w/w-766580/sync/js/
www.jetblue.com/js/src/jb-74873.js
cdn1.f-cdn.com/fp/check.js
www.avios.com/assets/scripts/global_bundle.js
www.britishairways.com/assets/scripts/global/d41d8cd98f00b204e9800998ecf8427e.js
www.westernunion.com/etc/clientlibs/westernunion/wu_common.js
Scrips canvas font fingerprint detectados por llamadas a measureText
m.stripe.network/inner.html
www.iberia.com/ibcomv3/rbrand/scripts/libs/iberialib.js
code.createjs.com/easeljs-0.8.0.min.js
api-ob.nd.nudatasecurity.com/2.2/w/w-766580/sync/js/
regstat.betfair.com/fp/check.js
www.euribordiario.es/js/Chart.min.js
www.espanol.marriott.com/common/js/marriottCommon.js
cdn1.f-cdn.com/fp/check.js
www.britishairways.com/assets/scripts/global/d41d8cd98f00b204e9800998ecf8427e.js
www.avios.com/assets/scripts/global_bundle.js
Scripts webrtc fingerprint detectados por llamadas a onicecandidate
pixel.yabidos.com/flimpobj.js
static.adsafeprotected.com/sca.17.4.72.js
c.adsco.re/
cdn.justuno.com/mwgt_3.6.js
pxlgnpgecom-a.akamaihd.net/javascripts/browserfp.min.js
www.cdn-net.com/cc.js
js.frubil.info/js/i.js
www.megasur.es/
regstat.betfair.com/fp/check.js
www.contactosbondage.es/rgjs/rg.min.js




### USO DE LA PETICIÓN DO NOT TRACK

| Técnica fingerprinting | % fingerprinting + DNT[16] |
|---|---|
| canvas: patrón detección C2[17] | 96,12% |
| canvas: patrón detección C1 | 93,97% |
| WebRTC: funciones sospechosas de FP | 72,18% |
| audiocontext: funciones sospechosas de FP | 64,29% |
| canvas font: patrón detección CF2 | 60,00% |
| canvas font: patrón detección CF1 | 58,14% |

### EFICACIA DE MEDIDAS DE MITIGACIÓN

| Técnica fingerprinting | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|
| fingerprinting por nombre de función | **-5,0%** | **-12,0%** | **-5,9%** | **-10,5%** | **-85,3%** | **-90,1%** | **-85,3%** |
| canvas: patrón C2 | **-3,6%** | **0,0%** | -13,5% | -15,1% | -35,4% | -34,4% | -36,5% |
| canvas: patrón C1 | -2,5% | 1,0% | **-19,2%** | **-21,7%** | **-40,9%** | **-39,4%** | **-41,9%** |
| canvas font: patrón CF2 | **-2,5%** | **-2,5%** | **0,0%** | **0,0%** | -12,5% | 2,1% | -14,6% |
| canvasfont: patrón CF1 | -2,4% | -2,4% | 0,0% | 0,0% | **-13,8%** | **2,8%** | **-16,7%** |
| webRTC | **-49,7%** | **-48,5%** | **-82,8%** | **-83,4%** | **-86,6%** | **-86,0%** | **-87,9%** |

[16] % de webs en las que se sigue detectando técnicas de fingerprinting a pesar de haber comprobado previamente que el usuario tiene activada la petición DNT.
[17] Información sobre patrones de detección Anexo II.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| audiocontext | **-12,7%** | **4,5%** | **-12,7%** | **-26,1%** | **-43,3%** | **-17,2%** | **-47,8%** |