Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de Magister en Ciberseguridad

AUTORES:

ALAVA BOLAÑOS JENNY JULIZZA

MERINO TORRES ANGEL FABRIZIO

ORDOÑEZ VIVANCO MARIA FERNANDA

TOASA ARROBA FABRICIO ALEXANDER

TUTORES:

Iván Reyes Chacón

Paulina Vizcaíno

TEMA

Reconstrucción forense de actividad web mediante el análisis de artefactos persistentes del navegador Brave en Windows 11 orientada a la identificación de incidentes de seguridad.

Quito - Ecuador

Junio – 20206

REINVENTEMOS EL FUTURO

Certificación de autoría

Nosotros, **Fabricio Alexander Toasa Arroba, Ángel Fabrizio Merino Torres, María Fernanda Ordoñez Vivanco y Jenny Julizza Alava Bolaños** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Firma
Fabricio Alexander Toasa Arroba

Firma
Ángel Fabrizio Merino Torres

Firma
María Fernanda Ordoñez Vivanco

Firma
Jenny Julizza Alava Bolaños

Autorización de Derechos de Propiedad Intelectual

Nosotros, **Fabricio Alexander Toasa Arroba, Ángel Fabrizio Merino Torres, María Fernanda Ordoñez Vivanco y Jenny Julizza Alava Bolaños**, en calidad de autores del trabajo de investigación titulado ***"Reconstrucción forense de actividad web mediante el análisis de artefactos persistentes del navegador Brave en Windows 11 orientada a la identificación de incidentes de seguridad"***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, Junio 2026

Firma
Fabricio Alexander Toasa Arroba

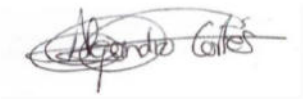
Firma
Ángel Fabrizio Merino Torres

Firma
María Fernanda Ordoñez Vivanco

Firma
Jenny Julizza Alava Bolaños

APROBACIÓN DE DIRECCIÓN Y COORDINACIÓN DEL PROGRAMA

Nosotros, Alejandro Cortés López e Iván Reyes Chacón, declaramos que: Fabricio Alexander Toasa Arroba, Ángel Fabrizio Merino Torres, María Fernanda Ordoñez Vivanco y Jenny Julizza Alava Bolaños son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



Alejandro Cortés
Director/a de la
Maestría en Ciberseguridad

Iván Reyes
Coordinador/a de la
Maestría en Ciberseguridad

DEDICATORIA

Dedicamos este Trabajo Fin de Maestría, en primer lugar, a nuestras familias, quienes han sido la fuente constante de inspiración, apoyo y motivación durante todo este proceso académico. Su amor incondicional, comprensión y sacrificio nos brindaron la fortaleza necesaria para enfrentar los desafíos y alcanzar esta importante meta profesional.

A nuestros padres, cónyuges, hijos y demás seres queridos, por acompañarnos en cada etapa de este camino, alentándonos a seguir adelante aun en los momentos más exigentes. Este logro también les pertenece, pues su respaldo fue fundamental para hacer posible la culminación de nuestros estudios de maestría.

Dedicamos igualmente este trabajo a todas aquellas personas que confiaron en nuestras capacidades, nos impulsaron a superarnos y compartieron con nosotros el valor del aprendizaje continuo, la disciplina y el compromiso profesional.

Que este logro represente no solo la culminación de una etapa académica, sino también el inicio de nuevos desafíos y oportunidades para contribuir al desarrollo de la sociedad mediante la aplicación ética y responsable de los conocimientos adquiridos.

Agradecimiento conjunto de los cuatro autores.

AGRADECIMIENTOS

Expresamos nuestro más profundo agradecimiento a Dios, por brindarnos la fortaleza, la sabiduría y la perseverancia necesarias para culminar satisfactoriamente esta importante etapa de formación académica. Su guía y bendición fueron fundamentales para superar cada desafío y alcanzar los objetivos planteados durante el desarrollo de este trabajo.

A nuestras familias, quienes con su amor, comprensión y apoyo incondicional nos acompañaron a lo largo de este proceso. Su paciencia, motivación y confianza constituyeron un pilar esencial para mantenernos firmes en el cumplimiento de nuestras metas personales y profesionales.

A la Universidad Internacional del Ecuador (UIDE), a sus autoridades, docentes y personal administrativo, por proporcionarnos los conocimientos, herramientas y espacios académicos que contribuyeron significativamente a nuestro crecimiento profesional y humano. De manera especial, agradecemos a nuestros tutores y profesores por compartir su experiencia, orientación y acompañamiento durante el desarrollo de este proyecto.

Finalmente, a cada uno de los integrantes de este grupo de trabajo, por el compromiso, la colaboración, el respeto y el esfuerzo conjunto demostrados durante toda la maestría y en la elaboración de este Trabajo Fin de Maestría. La suma de nuestras capacidades, experiencias y dedicación hizo posible la culminación exitosa de este proyecto.

Con gratitud compartida de parte de todo nuestro equipo.

RESUMEN

El presente trabajo desarrolla un análisis forense digital de los artefactos persistentes del navegador Brave — basado en el motor Chromium — en un entorno Windows 11, con el propósito de evaluar su utilidad y alcance probatorio en la identificación y documentación de incidentes de seguridad. El estudio aplica un escenario híbrido que combina el análisis del historial de navegación real del equipo investigador con eventos controlados documentados, incluyendo la descarga de muestras de malware desde repositorios especializados, archivos de prueba antimalware y un escenario de acceso a dominios fraudulentos.

La adquisición de los artefactos se realizó mediante FTK Imager sobre el equipo físico del investigador, con verificación de integridad mediante valores hash y documentación de la cadena de custodia. El análisis técnico se fundamentó en la explotación estructurada de los artefactos mediante consultas SQL con conversión de marcas temporales a UTC-5, validado mediante comparación cruzada con Hindsight, ChromeHistoryView, BrowsingHistoryView y Autopsy, adoptando el análisis SQL como fuente de verdad metodológica ante divergencias.

El análisis reconstruyó una línea de tiempo forense de 74 eventos de interés distribuidos en 79 días, identificando cuatro incidentes documentados, entre ellos la descarga de software de activación ilegal como hallazgo no planificado. La evaluación del alcance probatorio identificó evidencia directa e indiciaria, estableciendo como principales limitaciones el pre-fetching, las redirecciones automáticas y la imposibilidad de los artefactos del navegador para acreditar la ejecución de archivos descargados.

Las metodologías y procesos desarrollados pueden extenderse a otros navegadores basados en Chromium, debido a la similitud de su arquitectura y de los artefactos persistentes que generan. No obstante, su aplicación requiere considerar las particularidades técnicas propias de cada navegador, proporcionando un enfoque metodológico reproducible para el análisis forense de incidentes de seguridad basados en navegador.

Palabras clave: forense digital, navegadores basados en Chromium, artefactos persistentes, análisis forense web, línea de tiempo forense, alcance probatorio.

ABSTRACT

This work develops a digital forensic analysis of persistent artifacts from the Brave browser — based on the Chromium engine — in a Windows 11 environment, with the purpose of evaluating their utility and probative value in the identification and documentation of security incidents. The study applies a hybrid scenario combining the analysis of the research team's real browsing history with documented controlled events, including the download of malware samples from specialized repositories, antimalware test files, and a fraudulent domain access scenario.

Artifact acquisition was performed using FTK Imager on the investigator's physical device, with integrity verification through hash values and chain of custody documentation. The technical analysis was based on the structured examination of the artifacts using SQL queries with timestamp conversion to UTC-5, validated through cross-comparison with Hindsight, ChromeHistoryView, BrowsingHistoryView, and Autopsy, adopting SQL analysis as the methodological source of truth for discrepancy resolution.

The analysis reconstructed a forensic timeline of 74 events of interest distributed over 79 days, identifying four documented incidents, including the download of illegal activation software as an unplanned finding. The probative scope evaluation identified direct and circumstantial evidence, establishing as main limitations the pre-fetching mechanism, automatic redirections, and the inability of browser artifacts to certify the execution of downloaded files.

The methodologies and processes developed can be extended to other Chromium-based browsers, due to the similarity of their architecture and the persistent artifacts they generate. However, its application requires considering the technical particularities of each browser, providing a reproducible methodological approach for the forensic analysis of browser-based security incidents.

Keywords: digital forensics, Chromium-based browsers, persistent artifacts, web forensic analysis, forensic timeline, probative scope.

Tabla de contenido

Lista de Tablas

Lista de Figuras

1. Introducción

1.1. Definición del Proyecto

La proliferación de incidentes de seguridad vinculados a la navegación web — incluyendo la descarga de software malicioso, el acceso a dominios fraudulentos y la interacción con plataformas de distribución de amenazas — plantea una necesidad metodológica concreta en el ámbito del análisis forense digital: identificar qué información puede recuperarse de los artefactos persistentes de un navegador, con qué nivel de certeza puede atribuirse a acciones deliberadas del usuario y cuál es su valor probatorio en un proceso de investigación.

El presente proyecto consiste en la realización de un análisis forense digital orientado a la reconstrucción de la actividad de navegación web mediante el examen técnico de los artefactos persistentes del navegador Brave, basado en el motor Chromium, en un sistema operativo Windows 11. El estudio tomará como fuentes de evidencia la base de datos History, el archivo Preferences y la base de datos Web Data. El análisis se desarrollará en un escenario híbrido que combina el historial real del equipo investigador con eventos controlados generados deliberadamente, lo que permitirá contrastar los artefactos producidos por ambos tipos de actividad.

Los eventos controlados documentados comprenderán la descarga de muestras de malware desde repositorios especializados de análisis de amenazas, la descarga de archivos de prueba antimalware desde su servidor oficial, y el acceso a un dominio fraudulento configurado en un servidor local. El análisis se fundamentará en la explotación estructurada de las tablas urls, visits, downloads, downloads_url_chains y keyword_search_terms de la base de datos History, complementado con el examen del archivo Preferences y la base de

datos Web Data, con validación cruzada de los resultados mediante herramientas forenses especializadas.

1.2. Justificación e importancia del trabajo de investigación

La navegación web constituye una de las principales fuentes de evidencia digital en investigaciones forenses, ya que permite reconstruir comportamientos, establecer patrones de acceso y correlacionar eventos relevantes dentro de una línea de tiempo (Nelson et al., 2020; Quick & Choo, 2014). Los navegadores almacenan artefactos persistentes que aportan información valiosa sobre la actividad del usuario, convirtiéndose en elementos de interés central en procesos periciales y de respuesta a incidentes.

Los navegadores basados en el motor Chromium representan la plataforma dominante a nivel mundial. Google Chrome, Microsoft Edge, Brave y Opera acumulan conjuntamente más del 70% de la cuota de mercado global según (StatCounter, 2026), lo que incrementa significativamente la probabilidad de que sus artefactos digitales estén presentes en escenarios de análisis forense.

La relevancia metodológica de este trabajo reside precisamente en que las técnicas, consultas SQL y procesos documentados son aplicables a cualquier navegador que comparta el motor Chromium, dado que todos ellos presentan la misma estructura de bases de datos SQLite (Boucher et al., 2022a).

Entre los artefactos de estos navegadores, la base de datos **History** representa un repositorio estructurado de información que registra sitios visitados, cadenas de redirección, búsquedas realizadas y descargas efectuadas, datos que contribuyen a la reconstrucción cronológica de la actividad del usuario (Chand et al., 2025a). La elección del escenario de análisis forense de historial de navegación real con eventos controlados documentados responde a tres criterios metodológicos.

- **El primero es su representatividad:** los vectores de ataque vinculados a la navegación web se encuentran entre los más prevalentes en los informes de seguridad actuales (MITRE ATT&CK, 2024a)
- **El segundo es su trazabilidad:** la combinación de historial real con eventos controlados permite contrastar artefactos de distinta naturaleza y evaluar la consistencia de los registros forenses.
- **El tercero es su reproducibilidad:** la metodología desarrollada será documentada con criterios concretos que permitirán su replicación sobre cualquier perfil de navegador basado en Chromium.

El análisis permitirá evaluar la utilidad de estos artefactos como evidencia digital persistente y determinar su alcance probatorio, considerando limitaciones como la generación automática de registros por mecanismos internos del navegador (Breitinger et al., 2025). En síntesis, este trabajo aporta un enfoque metodológico claro y reproducible para la explotación forense de artefactos de navegadores Chromium, fortaleciendo los procedimientos de análisis digital tanto en entornos académicos como profesionales.

1.3. Alcance

El proyecto se limita al análisis de los artefactos persistentes generados por el navegador Brave en Windows 11 bajo un entorno de usuario único. Aunque Brave se basa en Chromium y comparte con otros navegadores derivados gran parte de su arquitectura de almacenamiento y de los principales artefactos persistentes descritos en la literatura (Boucher et al., 2022b); (Chand et al., 2025b)), la metodología propuesta fue desarrollada y validada exclusivamente en este navegador. Por ello, su aplicación a otros navegadores basados en Chromium requiere una validación previa que considere las particularidades de cada implementación.

El estudio comprende los siguientes artefactos principales:

- **Base de datos History (SQLite):** tablas urls, visits, downloads, downloads_url_chains y keyword_search_terms.
- **Archivo Preferences (JSON):** configuración del perfil, estado de protecciones del navegador y metadatos de actividad.
- **Base de datos Web Data (SQLite):** datos de autocompletado complementarios al historial de búsqueda, verificados como libres de información sensible de cualquier tipo.

El análisis seguirá un proceso estructurado que incluye: la adquisición y preservación de evidencia, junto con el cálculo de valores hash MD5, SHA-1 mediante FTK Imager y SHA-256; examen técnico mediante consultas SQL en DB Browser for SQLite; procesos ETL para conversión de marcas temporales y correlación de registros; y validación cruzada con herramientas como Hindsight, ChromeHistoryView, BrowsingHistoryView y Autopsy, contrastando sus salidas con el análisis manual en DB Browser for SQLite, adoptado como fuente de verdad metodológica ante divergencias entre herramientas.

Los resultados se integrarán en una línea de tiempo forense que reconstruirá cronológicamente la actividad de navegación, identificando cadenas de redirección y distinguiendo entre evidencia directa e indiciaria.

1.3.1. Marco de autorización y condiciones de acceso a la evidencia

El análisis se realizará sobre artefactos digitales obtenidos de un dispositivo personal propiedad de uno de los integrantes del equipo investigador, quien otorgará consentimiento expreso e informado para la realización del análisis forense con fines académicos, documentado mediante declaración formal incluida como apéndice al trabajo. Los artefactos no contendrán datos de naturaleza corporativa, institucional ni personal de terceras personas,

y la información personal identificable será anonimizada conforme a los criterios documentados en el presente trabajo. El acceso a la evidencia se realizará en condiciones controladas siguiendo los principios establecidos en la RFC 3227 (Brezinski, 2002) y las directrices (ACPO, 2015).

1.3.2. Exclusiones del alcance

Quedan explícitamente excluidos del alcance del proyecto los siguientes elementos:

- Análisis de navegación en modo incógnito, dado que Brave no persiste registros en la base de datos History para este modo.
- Adquisición o examen de memoria volátil (RAM).
- Descifrado de información protegida por mecanismos criptográficos.
- Análisis de Cookies, y tráfico de red.
- Análisis de otros navegadores o del motor Chromium en sistemas operativos distintos de Windows 11.
- Acreditación de la ejecución de los archivos descargados — los artefactos del navegador registran la descarga, pero no la ejecución posterior.

Si bien los artefactos excluidos pueden enriquecer un análisis forense completo, su inclusión superaría el alcance definido para este trabajo. Su existencia será reconocida en el documento como líneas de trabajo futuro.

1.4. Objetivos

1.4.1. Objetivo general

Realizar un análisis forense de la actividad de navegación web mediante el análisis de los artefactos persistentes del navegador Brave en un entorno Windows 11, con el propósito de evaluar la utilidad y el alcance probatorio de dichos artefactos en la identificación y documentación de incidentes de seguridad.

1.4.2. Objetivos específicos

- Diseñar el escenario forense y realizar la adquisición de los artefactos digitales garantizando su integridad mediante verificación hash y estableciendo la cadena de custodia del proceso de análisis.
- Analizar la estructura interna de los artefactos seleccionados (History, Preferences y Web Data), extrayendo y correlacionando sus registros mediante consultas SQL con conversión de marcas temporales a UTC-5 e interpretación de los indicadores técnicos de navegación.
- Reconstruir cronológicamente la actividad de navegación del equipo investigador mediante una línea de tiempo forense integrada, identificando las cadenas de eventos asociadas a los incidentes documentados.
- Validar los resultados del análisis manual mediante la comparación cruzada con herramientas forenses especializadas (ChromeHistoryView, BrowsingHistoryView, Hindsight y Autopsy), documentando coincidencias, divergencias y capacidades diferenciales entre métodos.
- Evaluar el alcance probatorio de la información recuperada, determinando qué hechos pueden acreditarse de manera directa y cuáles solo pueden inferirse de forma indiciaria, considerando las limitaciones técnicas de los artefactos analizados.

2. Revisión de Literatura

2.1. Estado del Arte

La investigación forense orientada al análisis de artefactos de navegadores web ha experimentado un crecimiento sostenido en la última década, impulsado por el incremento de la actividad delictiva en entornos digitales y la consolidación de los navegadores como fuente primaria de evidencia en investigaciones de seguridad. Los estudios recientes abordan este campo desde perspectivas complementarias que van desde el análisis comparativo de herramientas hasta la evaluación del alcance probatorio de los artefactos recuperados.

2.1.1. Análisis forense de navegadores web

El análisis forense de navegadores web constituye una de las áreas más activas dentro de la forense digital, dado que los navegadores almacenan de forma persistente registros detallados de la actividad del usuario que pueden resultar determinantes en la reconstrucción de incidentes de seguridad.

Chand et al. (2025a) presentan una evaluación crítica de herramientas y técnicas emergentes en forense de navegadores, analizando Google Chrome, Mozilla Firefox, Brave, Tor y Microsoft Edge bajo distintos escenarios de navegación. Su estudio examina los cambios en áreas clave de almacenamiento como caché, cookies, historial y almacenamiento local, concluyendo que artefactos como términos de búsqueda, URLs y detalles de sesión permanecen recuperables incluso tras el borrado del historial. Este hallazgo refuerza el valor forense de los artefactos persistentes del navegador como fuente de evidencia digital, particularmente en investigaciones donde el usuario puede haber intentado eliminar rastros de su actividad.

Boucher et al. (2022a) complementan este análisis con un estudio sobre los artefactos de navegadores basados en Chromium almacenados en SQLite y JSON, estableciendo que la

base de datos History constituye el repositorio más estructurado del perfil del navegador al integrar URLs visitadas, cadenas de redirección, términos de búsqueda y descargas en un esquema relacional que facilita la correlación forense de eventos. En esta línea, Brave y Chrome comparten estructuras de datos casi idénticas, con recuperación de artefactos exitosa incluso para datos eliminados (Reed et al., 2022).

En cuanto al modo privado, aunque Brave no deja rastros en el disco, las URLs, imágenes y búsquedas pueden recuperarse desde la memoria RAM, lo que evidencia sus límites de privacidad (Mahlous & Mahlous, 2020).

A pesar de estos avances, la literatura identifica como limitación la escasez de estudios que combinen el análisis manual mediante consultas SQL con la validación cruzada sistemática mediante múltiples herramientas forenses en un escenario de incidente específico. Esta brecha metodológica constituye uno de los aportes centrales del presente trabajo.

2.1.2. Reconstrucción cronológica web y líneas de tiempo forenses

La reconstrucción de líneas de tiempo forenses a partir de artefactos digitales constituye uno de los procesos más complejos y críticos en una investigación de seguridad, ya que permite establecer la secuencia de eventos que precedieron, acompañaron y siguieron a un incidente.

Breitinger et al. (2025) en su estudio de sistematización del conocimiento sobre reconstrucción de eventos basada en líneas de tiempo, identifican los principales desafíos metodológicos: la heterogeneidad de las fuentes de evidencia, la dificultad de correlacionar marcas temporales de distintos artefactos y la ausencia de terminología estandarizada. Su análisis revela que la mayoría de los estudios abordan la reconstrucción de la línea de tiempo (timestamps) de forma parcial, sin considerar todo el ciclo de vida del evento investigado.

Cantelli-Forti et al. (2025) complementan este marco proponiendo mediante WEFT una metodología de adquisición de evidencia web con verificación automática que garantiza la trazabilidad e integridad de cada artefacto desde su obtención. Ambos estudios convergen en una conclusión común: la reconstrucción cronológica de la actividad web requiere un proceso estructurado de normalización, correlación y verificación de los artefactos analizados, que va más allá del simple volcado del historial del navegador.

2.1.3. Distribución de malware desde el navegador como vector de ataque

El navegador web se ha consolidado como uno de los principales vectores de distribución de malware, a través de técnicas que aprovechan tanto vulnerabilidades técnicas del software como patrones de comportamiento del usuario.

Ibrahim et al. (2020) señalan que el *drive-by download* corresponde a una descarga automática, que ocurre sin acción consciente del usuario. Este tipo de ataque explota vulnerabilidades del navegador, sus extensiones o el sistema operativo, generando la descarga e instalación de archivos maliciosos en segundo plano. En el contexto forense, la tabla *downloads_url_chains* de Chrome constituye una evidencia clave para reconstruir las cadenas de redirección que conducen a estas descargas automáticas.

A este vector se suma el *typosquatting*, técnica que aprovecha errores tipográficos al ingresar direcciones en la barra del navegador (Agten et al., 2015; Kintis et al., 2017; Szurdi et al., 2014). Este patrón deja trazas en la tabla *urls* y en la tabla visits, particularmente cuando el campo transition type registra el valor TYPED, lo que permite diferenciar accesos directos de redirecciones automáticas. A estos vectores se suma el malvertising, técnica que distribuye malware a través de redes de publicidad legítimas. MITRE ATT&CK (2024a) clasifica esta técnica dentro de la táctica de acceso inicial mediante Drive-by Compromise

(T1189), destacando su prevalencia creciente y su capacidad para eludir controles basados en reputación de sitios web.

Chand et al. (2025) confirman que los artefactos del navegador — historial, descargas y URLs — constituyen evidencia crítica para reconstruir actividades basadas en estos vectores. No obstante, los artefactos generados dependen del tipo específico de vector y del escenario concreto analizado: mientras el drive-by download produce principalmente registros en downloads_url_chains, el typosquatting se refleja en visits y urls, y el malvertising combina trazas en visits y downloads.

2.1.4. Herramientas y metodologías de análisis forense digital

La validación de los resultados obtenidos en un análisis forense mediante el contraste entre diferentes herramientas especializadas constituye un requisito metodológico fundamental para garantizar la fiabilidad y reproducibilidad de los hallazgos.

Un análisis comparativo establece que ninguna solución individual ofrece cobertura completa de todos los dominios de análisis forense, haciendo necesaria la combinación de múltiples herramientas para garantizar la exhaustividad de la investigación (Javed et al., 2022; Sanghvi et al., 2023). En el contexto del presente trabajo, las diferencias concretas que pueden manifestarse entre herramientas incluyen divergencias en la interpretación de zonas horarias, diferencias en el conteo de registros según la fuente de datos accedida — tabla visits versus URLs únicas — y variaciones en la capacidad de acceso a fuentes no-SQLite del perfil del navegador. Estas divergencias serán documentadas mediante una tabla comparativa que registre para cada herramienta los registros identificados, las coincidencias con el análisis manual en DB Browser for SQLite y las capacidades diferenciales observadas, adoptando el análisis SQL como fuente de verdad metodológica ante cualquier discrepancia.

Chand et al. (2025a) complementan este planteamiento evidenciando diferencias significativas en la recuperación de artefactos según la herramienta utilizada, particularmente en escenarios con procesos automáticos del navegador. Entre las diferencias concretas que pueden manifestarse se encuentran divergencias en la interpretación de zonas horarias, diferencias en el conteo de registros según la fuente de datos accedida y variaciones en la capacidad de cada herramienta para acceder a fuentes no-SQLite del perfil del navegador. En conjunto, ambos estudios establecen que la robustez de un análisis forense depende de la consistencia de hallazgos obtenidos mediante múltiples métodos independientes y no de la sofisticación individual de una herramienta.

2.1.5. Alcance probatorio de la evidencia digital en navegadores

La determinación del valor técnico-probatorio de los artefactos digitales recuperados en un análisis forense constituye uno de los aspectos más delicados de la práctica pericial, requiriendo distinguir con precisión entre lo que la evidencia acredita directamente y lo que solo puede inferirse de forma indiciaria.

Ismail & Zainol Ariffin (2025) demuestran que la fiabilidad de la evidencia digital depende en mayor medida del proceso metodológico aplicado que de la naturaleza comercial o abierta de las herramientas utilizadas, concluyendo que herramientas de código abierto producen resultados con valor técnico-probatorio equivalente a soluciones comerciales cuando se aplica un proceso de validación riguroso y documentado. Estos principios fundamentan el enfoque comparativo del presente trabajo, donde la validación cruzada mediante múltiples herramientas constituye el mecanismo de verificación del valor técnico-probatorio de los hallazgos obtenidos.

Un factor crítico que condiciona el alcance probatorio en el análisis de artefactos de navegadores basados en Chromium es el pre-fetching, mecanismo automático del navegador

que puede generar registros indistinguibles de visitas reales. Chand et al. (2025a) identifican esta limitación como uno de los principales desafíos del análisis forense de navegadores, subrayando la necesidad de analizar indicadores complementarios para diferenciar visitas intencionales de procesos automáticos. En consecuencia, el valor técnico-probatorio de los artefactos no puede evaluarse de forma aislada, sino dentro de un proceso metodológico que integre múltiples fuentes de evidencia y análisis crítico de las limitaciones inherentes a cada artefacto (Breitinger et al., 2025).

2.2. Marco Teórico

El marco teórico establece los fundamentos conceptuales y técnicos. El propósito es delimitar el vocabulario empleado a lo largo del estudio y proporcionar el sustento conceptual necesario para comprender el alcance y la metodología del análisis forense realizado.

2.2.1. Forense digital y artefactos persistentes

La informática forense es la disciplina científica que se ocupa de la identificación, adquisición, preservación, análisis y presentación de evidencia digital con el propósito de reconstruir eventos ocurridos en sistemas informáticos y apoyar procesos de investigación en contextos judiciales, corporativos o académicos (Casey, 2011). Su práctica se rige por principios de integridad, reproducibilidad y trazabilidad que garantizan que los hallazgos obtenidos sean verificables de forma independiente.

La evidencia digital se clasifica en dos categorías según su persistencia. La evidencia volátil existe únicamente mientras el sistema permanece activo y se pierde de forma irreversible al apagar el equipo (Choi et al., 2023; Jeong, 2024). La evidencia persistente, por el contrario, se almacena en medios no volátiles y permanece disponible con independencia del estado del sistema, constituyendo la fuente primaria de evidencia en la mayoría de las investigaciones forenses (Javed et al., 2022).

Los artefactos de navegadores basados en Chromium objeto del presente estudio — la base de datos History, el archivo Preferences y la base de datos Web Data — pertenecen a esta segunda categoría, ya que se almacenan de forma permanente en el sistema de archivos y mantienen su integridad tras el cierre del navegador y el reinicio del sistema. Un artefacto digital persistente es cualquier registro generado automáticamente por una aplicación como resultado de la actividad del usuario, que permanece accesible en el sistema de archivos tras la finalización de la sesión que lo originó.

2.2.2. Arquitectura del navegador Chromium y sus artefactos

Los navegadores basados en el motor Chromium almacenan la información asociada a la actividad del usuario en un conjunto de archivos que conforman el perfil del navegador, ubicado en el sistema de archivos de Windows 11 bajo la ruta:

```
C:\Users\[usuario]\AppData\Local\[Navegador]\User Data\Default\
```

Esta carpeta contiene múltiples artefactos de distinta naturaleza y formato (Carrier, 2005). El presente estudio se centra en tres de ellos: la base de datos History, Web Data y el archivo Preferences, seleccionados por su relevancia directa para la reconstrucción de la actividad de navegación y la identificación de indicadores técnicos asociados al escenario de incidente analizado.

Base de datos History

La base de datos History es el artefacto central del análisis. Se trata de una base de datos relacional en formato SQLite que registra de forma estructurada la actividad de navegación del usuario. Su esquema incluye cinco tablas de interés forense directo:

La tabla **urls** almacena cada URL visitada junto con su título, el número de veces que ha sido visitada (visit_count), el número de veces que fue escrita directamente en la barra de direcciones (typed_count) y la marca temporal de la última visita (last_visit_time).

La tabla **visits** registra cada evento de visita de forma individualizada, vinculando cada registro con su URL correspondiente mediante el campo url, con la visita anterior que lo originó mediante el campo from_visit. Incluye además los campos visit_duration, que expresa la duración de la visita en microsegundos, y transition, que codifica el mecanismo por el que el navegador accedió a la URL.

La tabla **downloads** registra cada archivo descargado desde el navegador, incluyendo la URL de origen, la ruta local de almacenamiento, el tamaño del archivo, el estado de la descarga y las marcas temporales de inicio y finalización.

La tabla **downloads_url_chains** registra la cadena completa de URLs intermedias que precedieron a una descarga, vinculando cada eslabón con el identificador de la descarga correspondiente. Este artefacto es especialmente relevante en escenarios de descarga de malware, donde el archivo raramente se obtiene directamente desde la URL que el usuario visitó, sino a través de una cadena de redirecciones (Chand et al., 2025a).

La tabla **keyword_search_terms** registra los términos introducidos por el usuario en motores de búsqueda, vinculándolos con la URL del motor utilizado y con el identificador de la visita correspondiente.

Las marcas temporales almacenadas en estas tablas utilizan el formato interno de Chrome, expresado en microsegundos desde el 1 de enero de 1601. Su conversión al huso horario UTC-5 se detalla en el apartado metodológico del Capítulo 3.

Archivo Preferences

El archivo Preferences es un documento en formato JSON que almacena la configuración del perfil del navegador. Desde una perspectiva forense, sus campos de mayor interés son el directorio configurado para las descargas, las extensiones instaladas y activas durante el período analizado, y la última URL activa al cerrar el navegador. Su análisis

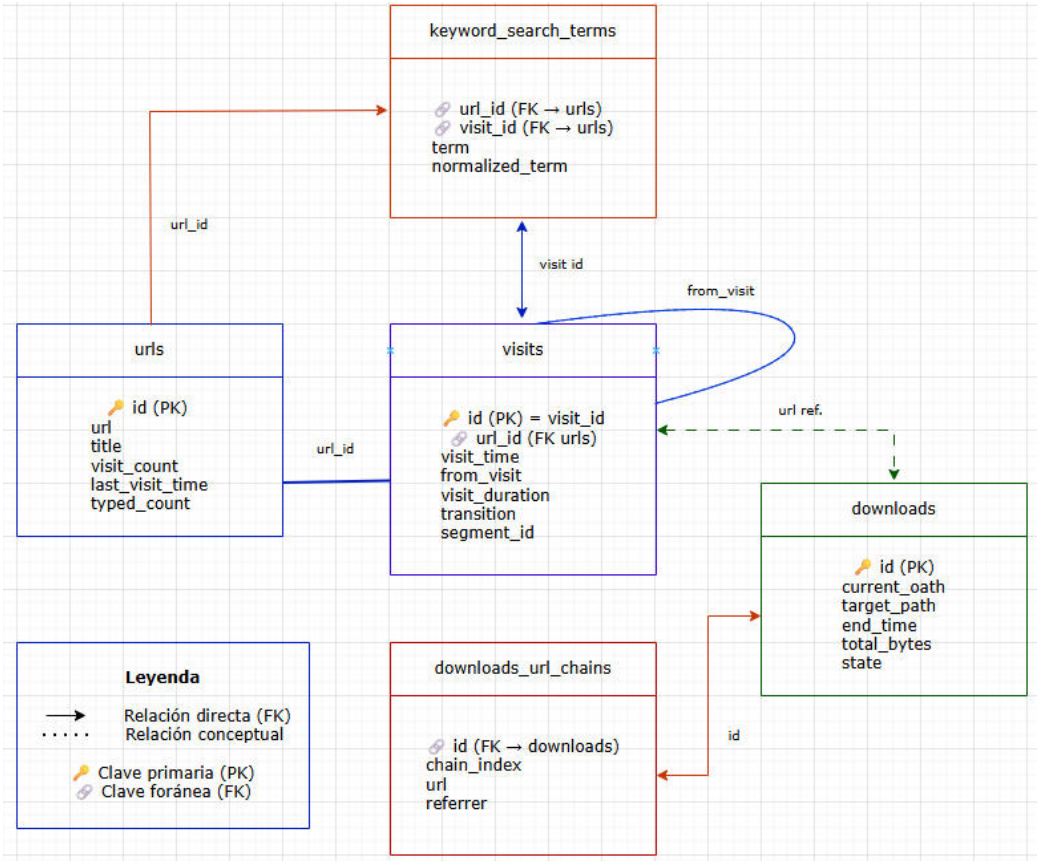
complementa los hallazgos de la base de datos History al proporcionar contexto sobre el entorno de navegación en el momento del incidente.

Base de datos Web Data

La base de datos Web Data es una base de datos SQLite que almacena, entre otros elementos, los datos introducidos por el usuario en formularios web mediante la función de autocompletado. Su tabla autofill puede contener términos de búsqueda y datos de formularios que complementan los registros de keyword_search_terms, especialmente en casos donde el usuario haya borrado parcialmente el historial de búsquedas.

Figura 1

Esquema relacional de la base de datos History



Nota. Elaboración propia basada en el esquema interno de la base de datos History analizada mediante DB Browser for SQLite (2026).

2.2.3. Cadena de custodia y preservación de la evidencia digital

La cadena de custodia es el registro documentado y cronológico de todos los accesos, transferencias y acciones realizadas sobre una evidencia digital desde su adquisición hasta su presentación final con el propósito de garantizar su integridad y autenticidad a lo largo de todo el proceso de análisis.

Los principios fundacionales de la preservación de evidencia digital fueron establecidos en la RFC 3227 (Brezinski, 2002), que enfatiza la minimización de la alteración de los datos originales, la documentación exhaustiva de cada acción realizada sobre la evidencia y la verificación de integridad mediante funciones hash criptográficas. Las directrices de la Association of Chief Police Officers (ACPO, 2015; ISO/IEC, 2012) complementan este marco estableciendo cuatro principios fundamentales: no alterar los datos del dispositivo original, documentar todo proceso que implique acceso a la evidencia, conservar un registro auditable de cada acción y garantizar que el responsable del análisis actúe dentro del marco legal aplicable.

El National Institute of Standards and Technology (NIST, 2015) refuerza estas directrices en su guía SP 800-86, subrayando la necesidad de trazabilidad y reproducibilidad en la preservación de evidencia digital. La literatura científica ha propuesto enfoques innovadores que incluyen el uso de algoritmos hash avanzados como SHA-3 y tecnologías de blockchain, orientadas a reforzar la trazabilidad y mitigar vulnerabilidades en la cadena de custodia (D'Anna et al., 2023; Yang, 2025).

Estos principios constituyen el fundamento metodológico del proceso de adquisición y preservación de evidencia implementado en el presente trabajo, detallado en el Capítulo 3.

2.2.4. Incidentes de seguridad basados en navegador

Los incidentes de seguridad basados en navegador constituyen una categoría de amenazas que utilizan este software como vector primario de ataque, explotando vulnerabilidades técnicas o patrones de comportamiento del usuario para comprometer sistemas y datos. (MITRE ATT&CK, 2024a) clasifica estos ataques dentro de la táctica de acceso inicial, identificando la descarga maliciosa desde el navegador como una de las técnicas más prevalentes.

El drive-by download corresponde a una **descarga automática**, que ocurre sin acción ni conocimiento del usuario, mediante la explotación de vulnerabilidades del navegador o sus complementos (Ibrahim et al., 2020). En contraste, las descargas inducidas — donde el usuario es dirigido mediante ingeniería social hacia un enlace de descarga— y las descargas manuales iniciadas voluntariamente por el usuario generan patrones diferenciados en los artefactos del navegador, reflejados principalmente en las tablas visits y downloads.

El typosquatting consiste en registrar dominios con variaciones tipográficas mínimas respecto a sitios legítimos, con el propósito de interceptar usuarios que cometen errores al escribir la dirección en la barra del navegador. Desde una perspectiva forense, este vector produce registros en la tabla *visits* con *transition type* igual a **TYPED**, lo que permite identificar accesos directos al dominio fraudulento.

El malvertising distribuye malware a través de redes de publicidad legítimas, comprometiendo al usuario incluso desde sitios confiables (MITRE ATT&CK, 2024b). Señala que este vector puede no generar registros en la tabla *downloads* si la descarga es bloqueada por mecanismos de protección del navegador, lo que limita la evidencia disponible para el análisis.

Los artefactos generados por estos vectores varían según el tipo de ataque y el escenario concreto analizado. No todos los vectores producen necesariamente registros en las mismas tablas ni con la misma completitud, por lo que su interpretación forense requiere el análisis conjunto de múltiples campos y tablas para reconstruir la cadena de eventos que condujo al incidente.

2.2.5. Alcance probatorio de la evidencia digital

El alcance probatorio de la evidencia digital hace referencia a la capacidad real de los artefactos recuperados en un análisis forense para acreditar hechos de forma directa o sustentarlos de forma indiciaria. Esta distinción es fundamental en la práctica forense, ya que determina el peso que puede asignarse a cada hallazgo en el contexto de una investigación.

La evidencia directa acredita un hecho sin necesidad de inferencias intermedias. En el contexto de navegadores basados en Chromium, un registro en la tabla downloads con URL de origen, ruta local de almacenamiento y marca temporal verificada constituye evidencia directa de que un archivo fue descargado desde esa dirección en un momento específico.

La evidencia indiciaria requiere una inferencia para conectar el artefacto con el hecho que se pretende acreditar. Por ejemplo, un registro en la tabla visits puede sugerir que el usuario accedió a un sitio de forma consciente, pero no lo confirma de manera absoluta, ya que el mismo registro podría generarse por procesos automáticos del navegador.

El principal mecanismo generador de ambigüedad forense en los artefactos de navegadores basados en Chromium es el **pre-fetching** — la carga anticipada de recursos que el navegador realiza sin intervención del usuario para acelerar la navegación. Este mecanismo puede generar registros en la tabla visits indistinguibles en apariencia de visitas reales, requiriendo el análisis de indicadores complementarios para su correcta interpretación.

3. Desarrollo

El capítulo describe el proceso metodológico aplicado en la investigación forense, estructurado en cuatro fases: diseño del escenario, adquisición de artefactos, análisis técnico y validación cruzada de resultados. Cada fase responde a los principios del análisis forense digital — planificación, adquisición, análisis y validación — asegurando integridad, trazabilidad y reproducibilidad en todo el proceso.

3.1. Diseño del escenario forense

El escenario corresponde a un modelo híbrido que combina artefactos de navegación reales con eventos controlados. Este enfoque permite analizar registros auténticos y, al mismo tiempo, asegurar la presencia de patrones técnicos verificables en las tablas. El escenario se organiza en tres categorías: hallazgos no planificados del historial de navegación, descargas controladas de archivos maliciosos y un entorno simulado de typosquatting que reproduce indicadores técnicos propios de este vector de ataque en los artefactos del navegador Brave.

3.1.1. Entorno de laboratorio

El análisis se realizó sobre los artefactos persistentes del perfil de Brave instalado en el equipo personal del investigador, con las siguientes características técnicas:

Tabla 1

Resumen general del dispositivo investigado

Componente	**Detalle**
Sistema Operativo	Windows 11 Home 25H2 - Compilación 26200.8457
Navegador	Brave versión 149.1.91.168
Perfil analizado	Perfil principal – sin sincronización con cuenta Google.
Periodo de análisis	14/03/2026 – 04/06/2026 (79 días)

Nota. Datos obtenidos del dispositivo personal miembro del equipo investigador.

3.1.2. Análisis forense sobre historial de navegación real

El análisis se realizó sobre el historial real de navegación del equipo del investigador, sin intervención previa ni selección anticipada de eventos, replicando las condiciones de un examen forense profesional.

El proceso siguió la metodología establecida en la literatura: adquisición íntegra de artefactos, consultas SQL sobre tablas relevantes, identificación de patrones y evaluación de su valor probatorio. Los hallazgos, incluidos eventos no planificados, serán documentados en el capítulo 4.3.1. conforme a los criterios de evidencia definidos en el marco teórico.

Esta aproximación aporta autenticidad y permite valorar el alcance real de los artefactos de Brave en condiciones equivalentes a un caso forense profesional.

3.1.3. Escenarios controlados – descarga de archivos maliciosos

Para generar artefactos forenses verificables y reproducibles, se diseñaron escenarios de descarga de archivos maliciosos desde fuentes reconocidas en el ámbito académico y profesional de la seguridad informática. Todos los escenarios siguieron la misma metodología: descargas deliberadas en sesiones distintas durante el período de análisis.

El escenario incluyó la descarga del archivo de prueba EICAR y de muestras obtenidas desde MalwareBazaar. En ambos casos, las muestras fueron empleadas únicamente para provocar la generación de artefactos forenses asociados al proceso de descarga. Ninguna de las muestras fue ejecutada; únicamente se verificó su descarga, almacenamiento y registro en los artefactos persistentes del navegador, preservando posteriormente su integridad mediante el cálculo de hashes SHA-256.

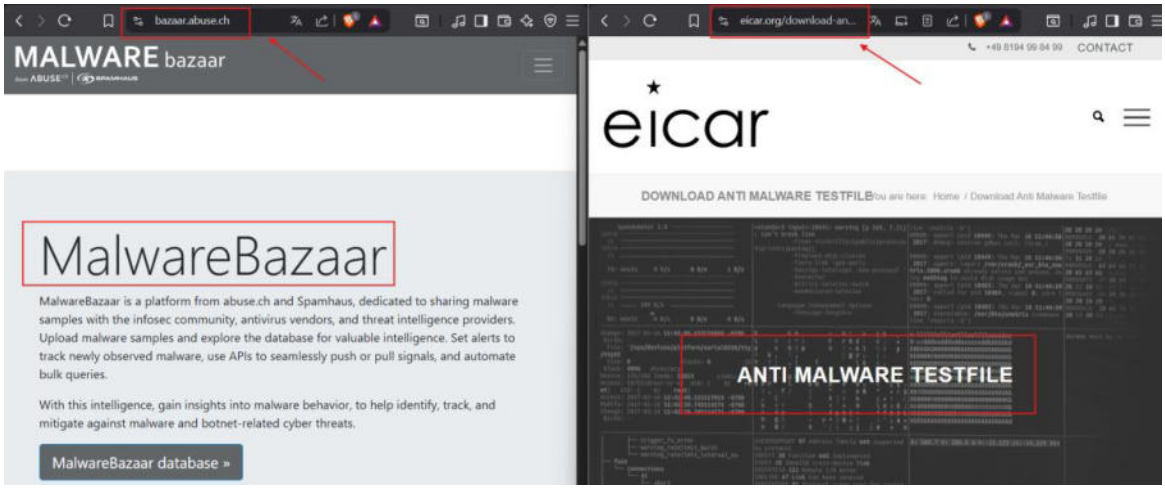
Malware Bazaar: repositorio mantenido por abuse.ch, ampliamente utilizado en investigación de seguridad. Se descargaron muestras comprimidas con contraseña, evitando

su ejecución accidental. La integridad de cada muestra es verificable mediante sus hashes SHA-256 públicos (abuse.ch, 2026).

EICAR: archivo estándar internacional de prueba antivirus, reconocido por todos los motores de detección como archivo de prueba no dañino (EICAR, 2026) . Su descarga permitió documentar el comportamiento del navegador y del sistema operativo frente a archivos identificados como maliciosos.

Figura 2

Repositorios para la descarga de malware.



Nota. Captura de pantalla obtenida en (abuse.ch, 2026; EICAR, 2026)

3.1.4. Escenario simulado – typosquatting

Para generar los patrones técnicos de un ataque de typosquatting, se implementó un entorno de simulación local compuesto por dos elementos:

1. La modificación del archivo hosts de Windows, ubicado en ***C:\Windows\System32\drivers\etc\hosts***, consistió en redirigir un dominio con variante tipográfica hacia la dirección de loopback, Esta acción simula la resolución DNS de un dominio de typosquatting real en un entorno de ataque.

Figura 3

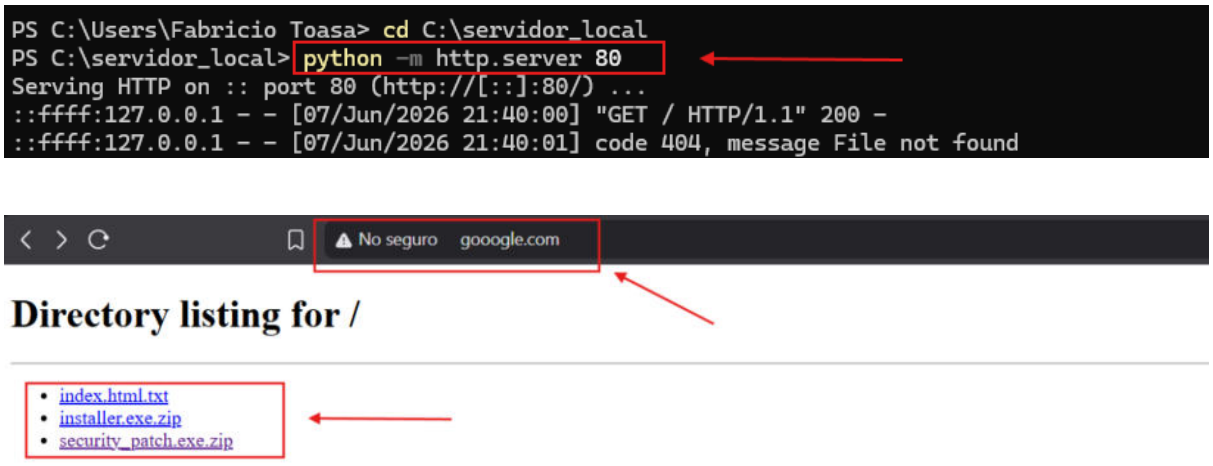
Modificación del archivo hosts en Windows 11

Nota. Se agregaron 3 dominios ilegítimos para simular el typosquatting.

2. Un servidor HTTP local levantado con Python, que sirvió una página de descarga accesible únicamente desde el propio equipo.

Figura 4

Server local para typosquatting con Python



Nota. Server HTTP local para typosquatting y ejecutado desde el navegador Brave.

El servidor alojó dos archivos de prueba con nombres diseñados para simular contenido legítimo: una supuesta actualización de seguridad y un instalador de software. Ambos se basaron en el estándar EICAR, pero fueron renombrados con extensiones y denominaciones propias de programas confiables. Esta estrategia reproduce la técnica habitual de camuflaje en la distribución de malware, donde los archivos maliciosos se presentan como descargas seguras para inducir al usuario a ejecutarlos.

Este método permitió replicar de forma controlada y segura el vector de entrada característico del typosquatting generando en los artefactos persistentes de Brave indicadores técnicos equivalentes a los que se producen durante la fase de navegación y descarga de un ataque real de typosquatting, sin depender de infraestructura externa ni exponer el equipo a amenazas genuinas.

3.2. Adquisición y preservación de la evidencia digital

La adquisición de los artefactos se realizó siguiendo los principios de la informática forense, garantizando la integridad de la evidencia desde el momento de su obtención. El proceso se estructuró en tres etapas: adquisición forense, verificación de integridad y establecimiento de la cadena de custodia.

3.2.1. Proceso de adquisición con FTK Imager

La obtención de los artefactos se efectuó mediante **FTK Imager 4.7.3.81**, herramienta forense ampliamente utilizada en investigaciones digitales que permite generar copias verificables sin alterar el sistema de origen. Para la adquisición se verificaron las siguientes condiciones:

- Se realizó sobre el equipo físico con Brave cerrado, asegurando la confirmación de registros en SQLite antes de la copia forense.
- El volumen correspondiente fue montado en modo lectura mediante FTK Imager, garantizando acceso completo sin modificar su contenido

Los artefactos adquiridos corresponden a los tres archivos definidos en el alcance del trabajo, ubicados en la ruta:

Tabla 2.

Lista y formatos de artefactos persistentes de Brave.

C:\Users\[USUARIO]\AppData\Local\BraveSoftware\Brave-Browser\User Data\Default\

Artefacto	Formato	Descripción
History	SQLite	Base de datos principal de navegación
Web Data	SQLite	Base de datos de autocompletado
Preferences	JSON	Archivo de configuración del perfil

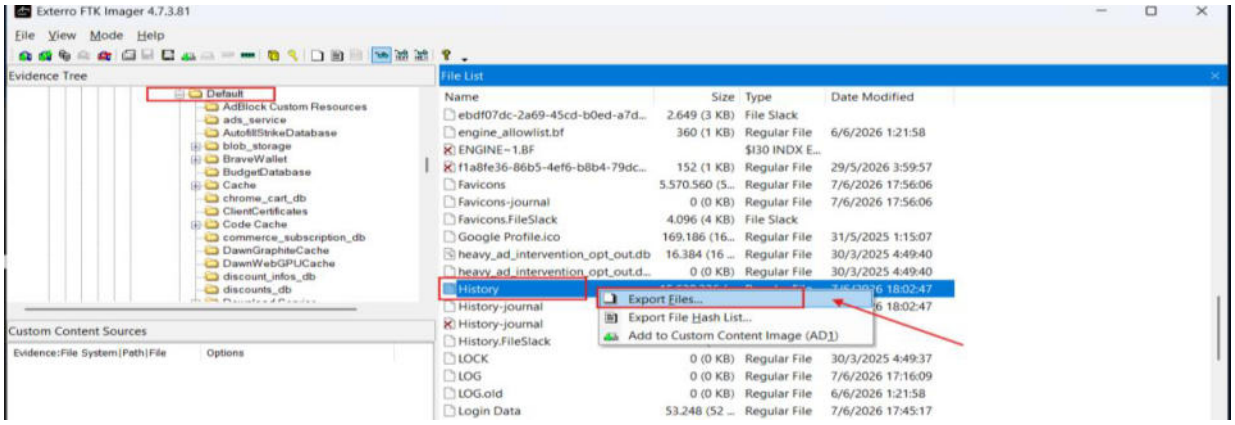
Nota. Autores.

El procedimiento de exportación se realizó mediante la función de ***Export Files*** de FTK Imager, seleccionando cada artefacto individualmente y exportándolo hacia la carpeta de destino designada para el análisis:

C:\Users\ [USUARIO]\Desktop\evidencias

Figura 5

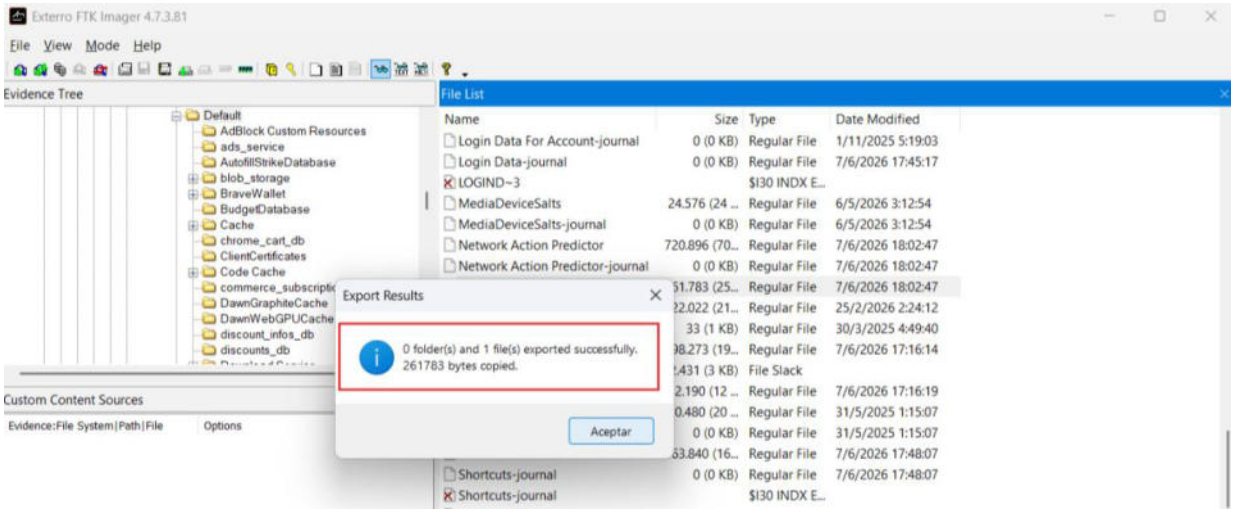
Exportación del artefacto History mediante FTK Imager



Nota. Se exporta mediante la opción Export Files el artefacto History.

Figura 6

Exportación completa de los 3 artefactos de Brave



Nota. Se exporta los tres artefactos definidos mediante FTK Imager en la ruta definida.

3.2.2. Verificación de integridad mediante hashes criptográficos

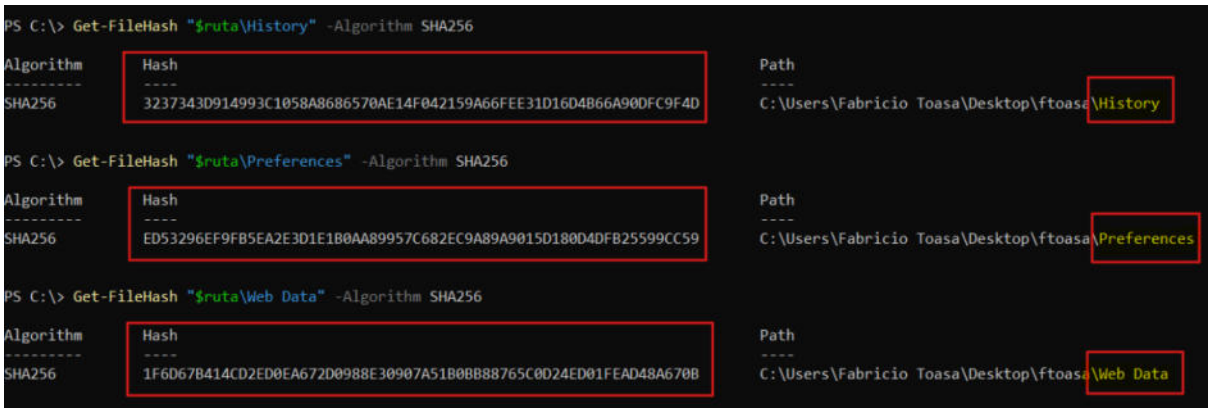
La integridad de cada artefacto fue verificada mediante el cálculo de valores hash criptográficos sobre el archivo original y su copia forense. La coincidencia entre ambos garantiza que el proceso de exportación no introdujo modificaciones y que la copia es idéntica a la original.

Los valores SHA-256 de las copias forenses se calcularon mediante PowerShell mediante el cmdlet ***`Get-FileHash`***, ejecutando sobre los archivos exportados:

```
Get-FileHash "ruta\History" -Algorithm SHA256
Get-FileHash "ruta\Web Data" -Algorithm SHA256
Get-FileHash "ruta\Preferences" -Algorithm SHA256
```

Figura 7

Cálculo de hash criptográficos SHA-256 con PowerShell

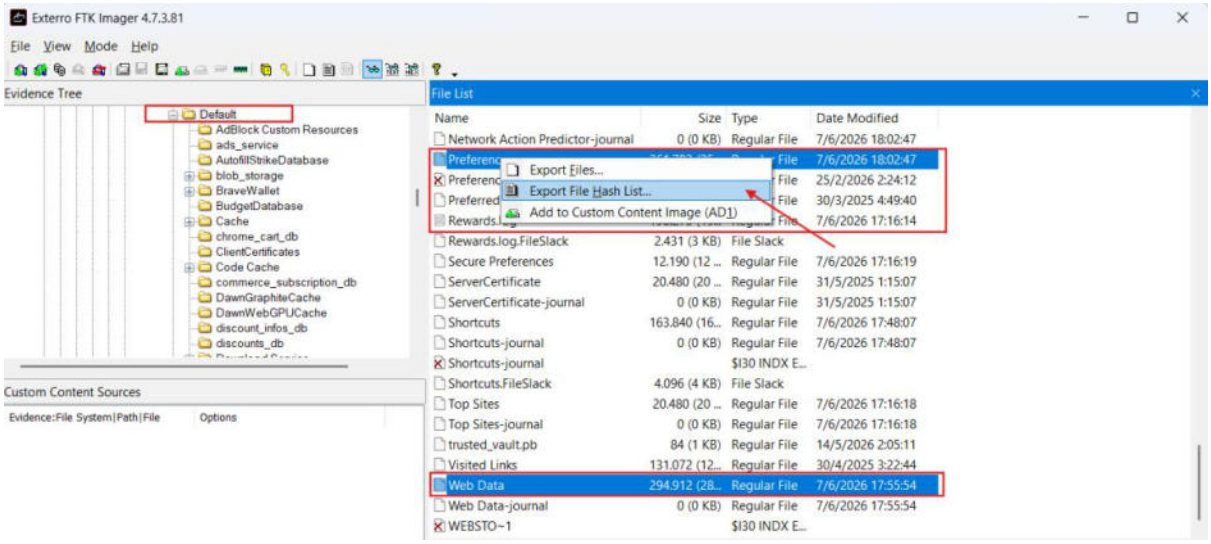


Nota. FTK Imager no exporta el hash SHA256.

FTK Imager generó los valores MD5 y SHA-1 de cada artefacto original mediante la función ***Export File Hash List***. Esta operación produce un archivo .CSV que contiene los hashes junto con la ruta de origen de los artefactos. Los resultados de la verificación se presentan en la Tabla 3, garantizando la trazabilidad y reproducibilidad del proceso.

Figura 8

Exportando los hashes MD5 y SHA-1 con FTK Imager



Nota. Para la exportación se utiliza la función Export File Hash List.

Los resultados de la verificación se documentan en la siguiente tabla:

Tabla 3.

Resumen de hashes criptográficos de los artefactos de Brave.

Artefacto	Algoritmo	Hash original / Hash copia
History	MD5	9bc7d7a4535c21264b13e61b63e0d4b7 / 9bc7d7a4535c21264b13e61b63e0d4b7
	SHA-1	58a20ecabf10b4c30a222c8ee34b99a14ddafa7b / 58a20ecabf10b4c30a222c8ee34b99a14ddafa7b
	SHA-256	3237343d914993c1058a8686570ae14f042159a66fee31d16d4b66a90dfc9f4d / 3237343d914993c1058a8686570ae14f042159a66fee31d16d4b66a90dfc9f4d
Preferences	MD5	f4a28a498725e69efc538379b4014d0f / f4a28a498725e69efc538379b4014d0f
	SHA-1	668a0c93143f6549a9bb37aac981921d71690af9 / 668a0c93143f6549a9bb37aac981921d71690af9
	SHA-256	ed53296ef9fb5ea2e3d1e1b0aa89957c682ec9a89a9015d180d4dfb25599cc59 / ed53296ef9fb5ea2e3d1e1b0aa89957c682ec9a89a9015d180d4dfb25599cc59
Web Data	MD5	a39fc4cd636e8f518ff28c0cbcf34fb9 / a39fc4cd636e8f518ff28c0cbcf34fb9
	SHA-1	776d32c76b192194d2e386d889ab439ffcbc1298 / 776d32c76b192194d2e386d889ab439ffcbc1298

	SHA-256	1f6d67b414cd2ed0ea672d0988e30907a51b0bb88765c0d24ed01fead48a670b / 1f6d67b414cd2ed0ea672d0988e30907a51b0bb88765c0d24ed01fead48a670b

Nota. Los valores criptográficos exportados coinciden con el valor original.

3.2.3. Cadena de custodia

La cadena de custodia documenta cronológicamente cada acción realizada sobre los artefactos desde su adquisición hasta el cierre del análisis, garantizando la trazabilidad completa de la evidencia. Los eventos principales de la cadena de custodia son los siguientes:

Tabla 4.

Resumen cadena de custodia de los artefactos persistentes.

N°	Fecha	Acción	Herramienta	Artefacto
1	7/6/2026 13:00	Adquisición forense	FTK Imager	History, Web Data, Preferences
2	7/6/2026 13:20	Verificación de hashes MD5 y SHA-1	FTK Imager	History, Web Data, Preferences
3	7/6/2026 13:30	Verificación de hashes SHA-256	PowerShell	History, Web Data, Preferences
4	7/6/2026 14:00	Apertura en modo solo lectura	DB Browser for SQLite	History, Web Data
6	8/6/2026 14:30	Análisis con herramienta automatizada	ChromeHistoryView	History
8	9/6/2026 15:00	Análisis con herramienta automatizada	BrowsingHistoryView	History
15	13/6/2026 21:20	Análisis con herramienta automatizada	Hindsight	Perfil Brave

22	17/6/2026 9:15	Análisis con plataforma forense	Autopsy	History
35	19/6/2026 16:00	Verificación final de hashes	PowerShell	History, Web Data, Preferences

Nota. Autores.

3.3. Análisis técnico de los artefactos con DB Browser

El análisis técnico se realizó sobre las copias forenses de los artefactos adquiridos, manteniendo en todo momento los archivos originales sin modificaciones. El proceso comprende el examen estructurado de las bases de datos History y Web Data mediante consultas SQL, el análisis del archivo Preferences, la aplicación del proceso ETL para la normalización de los datos extraídos y la reconstrucción de la línea de tiempo forense.

3.3.1. Preparación del entorno de análisis

Las bases de datos History y Web Data fueron abiertas en modo de solo lectura mediante DB Browser for SQLite versión 3.13.1, herramienta que permite el examen directo del contenido SQLite sin riesgo de modificación de los datos. La apertura en modo solo lectura constituye un requisito metodológico fundamental que garantiza la preservación de la integridad de la evidencia durante el análisis.

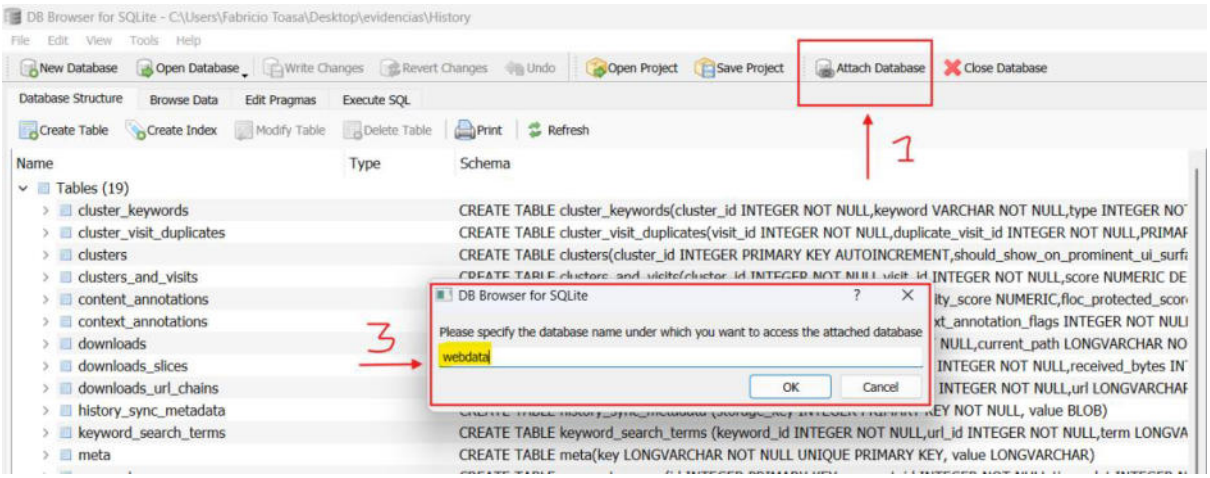
Para permitir la correlación entre ambas bases de datos en una única sesión de consulta, se adjuntó la base de datos **Web Data** a la sesión principal de **History** mediante el comando ATTACH de SQLite. Esta instrucción establece una referencia cruzada entre ambas bases, lo que posibilita la ejecución de consultas JOIN entre sus tablas sin alterar ni modificar los archivos originales, garantizando así la integridad de la evidencia.

```
ATTACH DATABASE 'ruta\Web Data' AS webdata;
```

Este procedimiento también puede realizarse directamente desde la interfaz de DB Browser, seleccionando la opción ***Attach Database***, indicando la ruta donde se encuentran los artefactos exportados y asignando un alias a la base de datos, en este caso `webdata`. De esta manera, se facilita la ejecución de consultas conjuntas que integran información de ambos artefactos, optimizando el proceso de correlación y análisis.

Figura 9

Attach Database Web Data



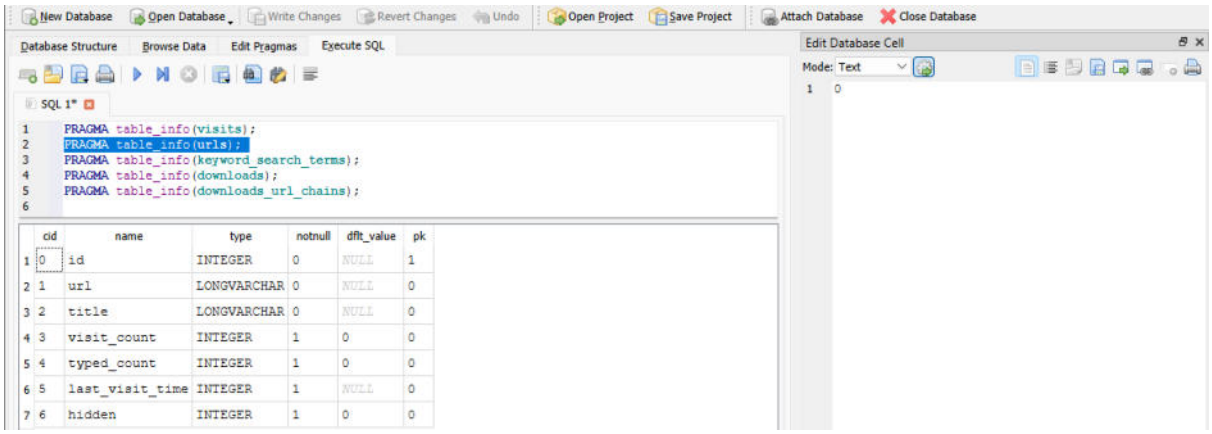
Nota. El artefacto Web Data se integra con el alias `webdata`

Previo al análisis del contenido, se verificó la estructura de las tablas mediante la instrucción ***PRAGMA*** para confirmar los nombres exactos de los campos en la versión de Brave analizada:

```
PRAGMA table_info(visits);
PRAGMA table_info(urls);
PRAGMA table_info(keyword_search_terms);
PRAGMA table_info(downloads);
PRAGMA table_info(downloads_url_chains);
```

Figura 10

Validación de tablas



Nota. Datos obtenidos con DB Browser a partir de la copia forense del archivo History.

Esta verificación es relevante dado que el esquema interno de las bases de datos SQLite de Brave puede variar entre versiones de Chromium. En la versión analizada se confirmó que el campo de relación entre las tablas visits y urls se denomina url en lugar de url_id, nomenclatura presente en versiones anteriores del navegador documentada en la literatura forense (Chand et al., 2025a)

3.3.2. Análisis de la base de datos History

El análisis de la base de datos History se estructuró en cinco consultas principales, cada una orientada a extraer y correlacionar información de las tablas definidas en el alcance del trabajo.

Conversión de marcas temporales

Brave almacena todas las marcas temporales en formato interno propio, expresado en microsegundos transcurridos desde el 1 de enero de 1601 — epoch de Windows. La conversión al formato Unix legible requiere la aplicación de la siguiente transformación en todas las consultas:

```
datetime((timestamp / 1000000) - 11644473600 - 18000, 'unixepoch')
```

El valor 11644473600 corresponde a la diferencia en segundos entre el epoch de Windows (1601) y el epoch Unix (1970). El valor 18000 aplica el ajuste de zona horaria UTC-5 correspondiente a Ecuador, donde se realizó el análisis. Este proceso constituye el paso de transformación del proceso ETL aplicado a los artefactos.

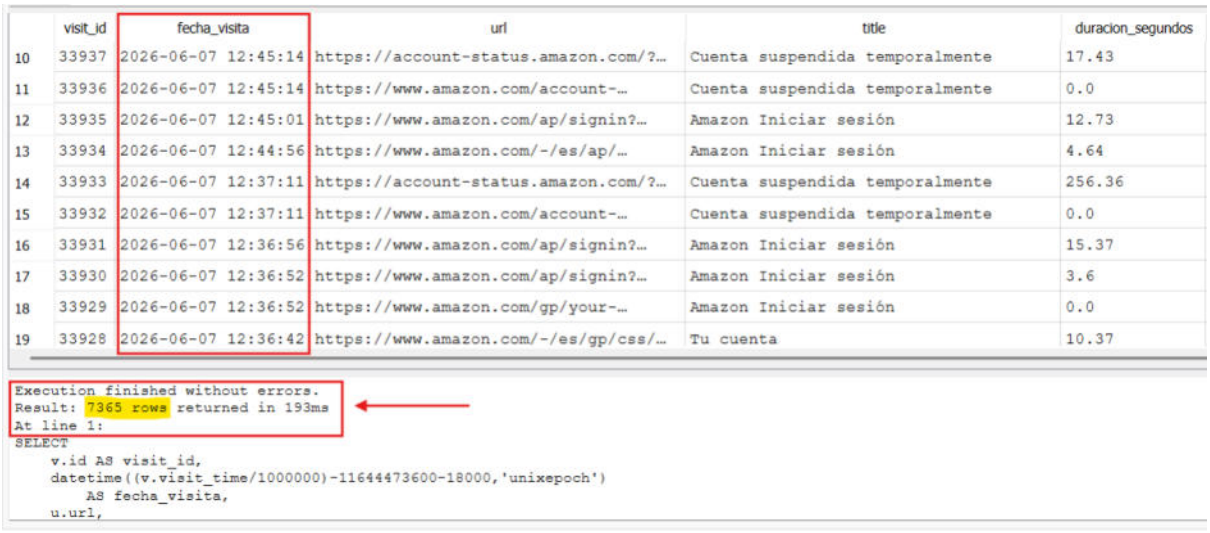
Consulta 1 — Reconstrucción de la cadena de navegación

La primera consulta extrae la secuencia completa de visitas correlacionando las tablas ***visits*** y ***urls***, incluyendo la conversión de timestamps, el cálculo de la duración en segundos y la decodificación del campo ***transition*** mediante una expresión CASE:

```
SELECT
    v.id AS visit_id,
    datetime((v.visit_time/1000000)-11644473600-18000,'unixepoch')
        AS fecha_visita,
    u.url,
    u.title,
    ROUND(v.visit_duration/1000000.0, 2) AS duracion_segundos,
    v.from_visit,
    CASE v.transition & 255
        WHEN 0 THEN 'LINK'
        WHEN 1 THEN 'TYPED'
        WHEN 5 THEN 'GENERATED'
        WHEN 7 THEN 'FORM_SUBMIT'
        WHEN 8 THEN 'RELOAD'
        ELSE 'REDIRECT'
    END AS tipo_transicion
FROM visits v
JOIN urls u ON v.url = u.id
ORDER BY v.visit_time DESC;
```

Figura 11

Reconstrucción de la cadena de navegación



	visit_id	fecha_visita	url	title	duracion_segundos
10	33937	2026-06-07 12:45:14	https://account-status.amazon.com/?…	Cuenta suspendida temporalmente	17.43
11	33936	2026-06-07 12:45:14	https://www.amazon.com/account-…	Cuenta suspendida temporalmente	0.0
12	33935	2026-06-07 12:45:01	https://www.amazon.com/ap/signin?…	Amazon Iniciar sesión	12.73
13	33934	2026-06-07 12:44:56	https://www.amazon.com/-/es/ap/…	Amazon Iniciar sesión	4.64
14	33933	2026-06-07 12:37:11	https://account-status.amazon.com/?…	Cuenta suspendida temporalmente	256.36
15	33932	2026-06-07 12:37:11	https://www.amazon.com/account-…	Cuenta suspendida temporalmente	0.0
16	33931	2026-06-07 12:36:56	https://www.amazon.com/ap/signin?…	Amazon Iniciar sesión	15.37
17	33930	2026-06-07 12:36:52	https://www.amazon.com/ap/signin?…	Amazon Iniciar sesión	3.6
18	33929	2026-06-07 12:36:52	https://www.amazon.com/gp/your-…	Amazon Iniciar sesión	0.0
19	33928	2026-06-07 12:36:42	https://www.amazon.com/-/es/gp/css/…	Tu cuenta	10.37

```
Execution finished without errors.
Result: 7365 rows returned in 193ms
At line 1:
SELECT
    v.id AS visit_id,
    datetime((v.visit_time/1000000)-11644473600-18000,'unixepoch')
        AS fecha_visita,
    u.url,
```

Nota. Correlación entre *visits* y *urls* para reconstruir la secuencia de navegación.

Consulta 2 — Identificación de la cadena de redirección

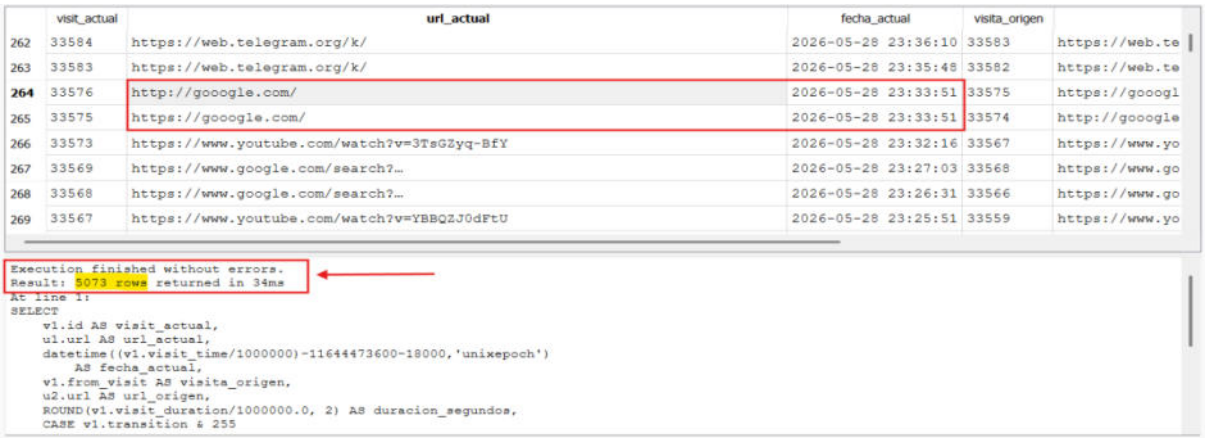
La segunda consulta reconstruye la cadena de redirección entre visitas mediante el campo ***from_visit***, que vincula cada visita con la visita precedente que la originó:

```
SELECT
    v1.id AS visit_actual,
    u1.url AS url_actual,
    datetime((v1.visit_time/1000000)-11644473600-18000,'unixepoch')
        AS fecha_actual,
    v1.from_visit AS visita_origen,
    u2.url AS url_origen,
    ROUND(v1.visit_duration/1000000.0, 2) AS duracion_segundos,
    CASE v1.transition & 255
        WHEN 0 THEN 'LINK'
        WHEN 1 THEN 'TYPED'
        WHEN 5 THEN 'GENERATED'
        WHEN 7 THEN 'FORM_SUBMIT'
        ELSE 'REDIRECT'
```

```
    END AS tipo_transicion
FROM visits v1
JOIN urls u1 ON v1.url = u1.id
LEFT JOIN visits v2 ON v1.from_visit = v2.id
LEFT JOIN urls u2 ON v2.url = u2.id
WHERE v1.from_visit != 0
ORDER BY v1.visit_time DESC;
```

Figura 12

Reconstrucción cadena de redirección



Nota. Cadena de redirección reconstruida con visits y urls mediante from_visit.

Consulta 3 — Análisis de descargas con cadena completa

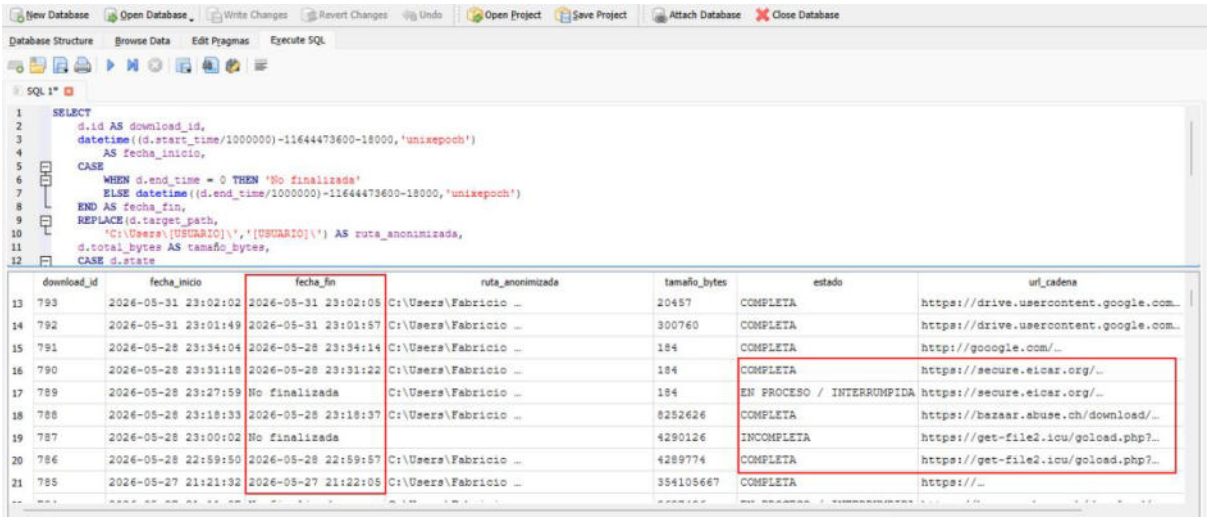
La tercera consulta correlaciona las tablas ***downloads*** y ***downloads_url_chains*** para obtener la cadena completa de URLs que precedieron a cada descarga, incluyendo la conversión de timestamps y el tratamiento del campo ***end_time*** para gestionar descargas no finalizadas:

```
SELECT
  d.id AS download_id,
  datetime((d.start_time/1000000)-11644473600-18000,'unixepoch')
    AS fecha_inicio,
  CASE
    WHEN d.end_time = 0 THEN 'No finalizada'
```

```
    ELSE datetime((d.end_time/1000000)-11644473600-18000,'unixepoch')
  END AS fecha_fin,
  REPLACE(d.target_path,
    'C:\Users\[USUARIO]\','[USUARIO]\') AS ruta_anonimizada,
  d.total_bytes AS tamaño_bytes,
  CASE d.state
    WHEN 1 THEN 'COMPLETA'
    WHEN 2 THEN 'INCOMPLETA'
    WHEN 3 THEN 'CANCELADA'
    ELSE 'EN PROCESO / INTERRUMPIDA'
  END AS estado,
  c.url AS url_cadena,
  c.chain_index AS posicion_cadena
FROM downloads d
LEFT JOIN downloads_url_chains c ON d.id = c.id
ORDER BY d.start_time DESC, c.chain_index ASC;
```

Figura 13

Cadena de redirección de descargas



	download_id	fecha_inicio	fecha_fin	ruta_anonimizada	tamaño_bytes	estado	url_cadena
13	793	2026-05-31 23:02:02	2026-05-31 23:02:05	C:\Users\Fabricio …	20457	COMPLETA	https://drive.usercontent.google.com…
14	792	2026-05-31 23:01:49	2026-05-31 23:01:57	C:\Users\Fabricio …	300760	COMPLETA	https://drive.usercontent.google.com…
15	791	2026-05-28 23:34:04	2026-05-28 23:34:14	C:\Users\Fabricio …	184	COMPLETA	http://gooogle.com/…
16	790	2026-05-28 23:31:18	2026-05-28 23:31:22	C:\Users\Fabricio …	184	COMPLETA	https://secure.eicar.org/…
17	789	2026-05-28 23:27:59	No finalizada	C:\Users\Fabricio …	184	EN PROCESO / INTERRUMPIDA	https://secure.eicar.org/…
18	788	2026-05-28 23:18:33	2026-05-28 23:18:37	C:\Users\Fabricio …	8252626	COMPLETA	https://bazaar.abuse.ch/download/…
19	787	2026-05-28 23:00:02	No finalizada		4290126	INCOMPLETA	https://get-file2.icu/goload.php?…
20	786	2026-05-28 22:59:50	2026-05-28 22:59:57	C:\Users\Fabricio …	4289774	COMPLETA	https://get-file2.icu/goload.php?…
21	785	2026-05-27 21:21:32	2026-05-27 21:22:05	C:\Users\Fabricio …	354105667	COMPLETA	https://…

Nota. Correlación entre *downloads* y *downloads_url_chains* para reconstruir la cadena de URLs asociadas a cada descarga.

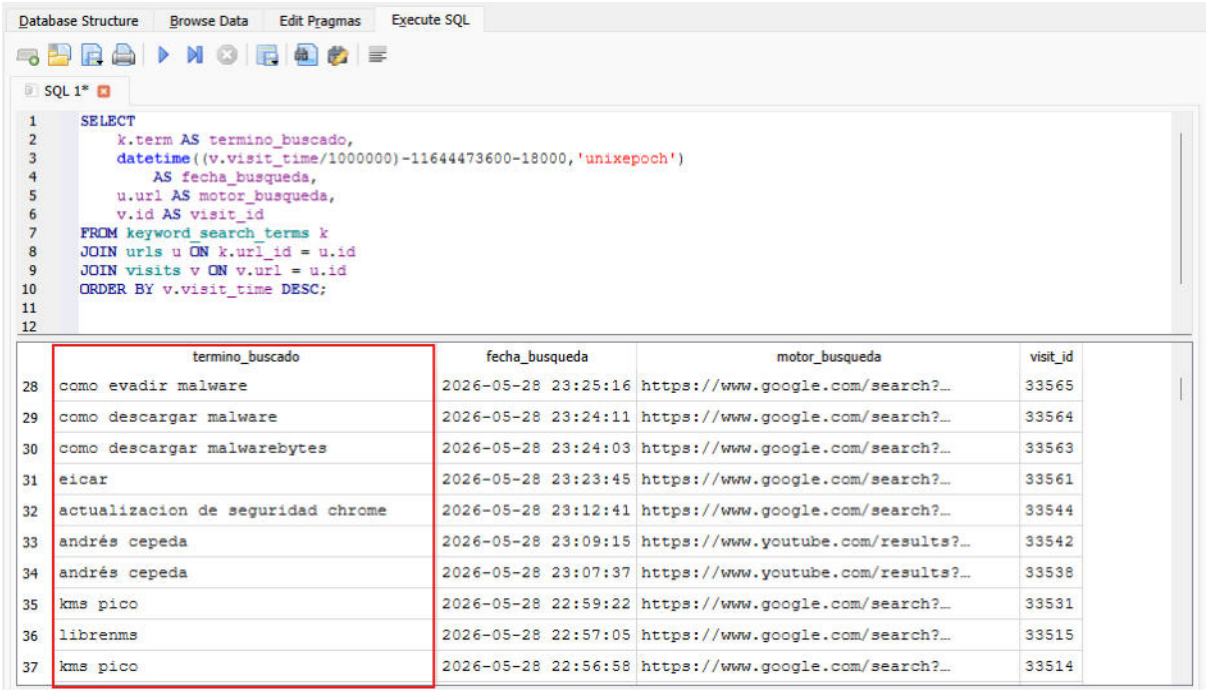
Consulta 4 — Extracción de términos de búsqueda

La cuarta consulta extrae los términos de búsqueda registrados en ***keyword_search_terms*** correlacionándolos con sus visitas correspondientes para obtener la marca temporal de cada búsqueda:

```
SELECT
    k.term AS termino_buscado,
    datetime((v.visit_time/1000000)-11644473600-18000,'unixepoch')
        AS fecha_busqueda,
    u.url AS motor_busqueda,
    v.id AS visit_id
FROM keyword_search_terms k
JOIN urls u ON k.url_id = u.id
JOIN visits v ON v.url = u.id
ORDER BY v.visit_time DESC;
```

Figura 14

Extracción de términos de búsqueda en keyword_search_terms



Nota. La correlación se realiza mediante visitas y sus marcas temporales.

Consulta 5 — Identificación de visitas con duration cero

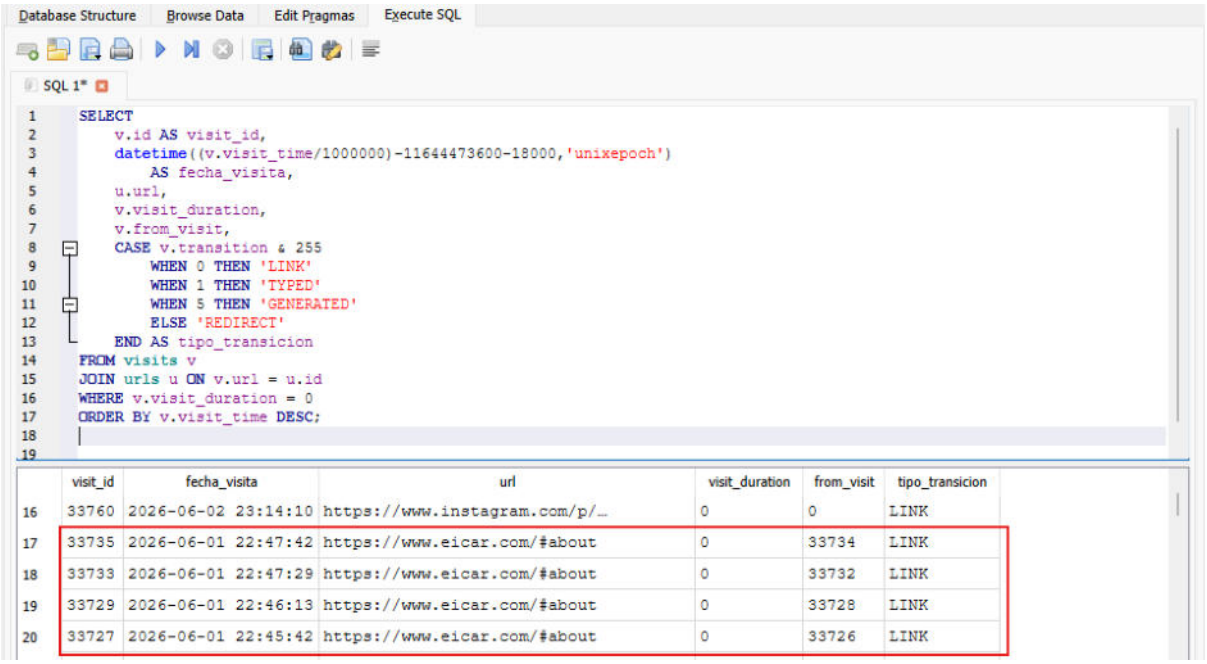
La quinta consulta identifica visitas con ***visit_duration*** igual a cero, indicador técnico que puede corresponder a procesos de ***pre-fetching*** del navegador o redirecciones automáticas no atribuibles a la acción consciente del usuario:

```
SELECT
    v.id AS visit_id,
    datetime((v.visit_time/1000000)-11644473600-18000,'unixepoch')
        AS fecha_visita,
    u.url,
    v.visit_duration,
    v.from_visit,
    CASE v.transition & 255
        WHEN 0 THEN 'LINK'
        WHEN 1 THEN 'TYPED'
        WHEN 5 THEN 'GENERATED'
        ELSE 'REDIRECT'
    END AS tipo_transicion
FROM visits v
```

```
JOIN urls u ON v.url = u.id
WHERE v.visit_duration = 0
ORDER BY v.visit_time DESC;
```

Figura 15

Consultas para identificar pre-fetching



Nota. visit_duration permite detectar eventos de pre-fetching o redirecciones automáticas.

3.3.3. Análisis de Web Data y Preferences

Web Data

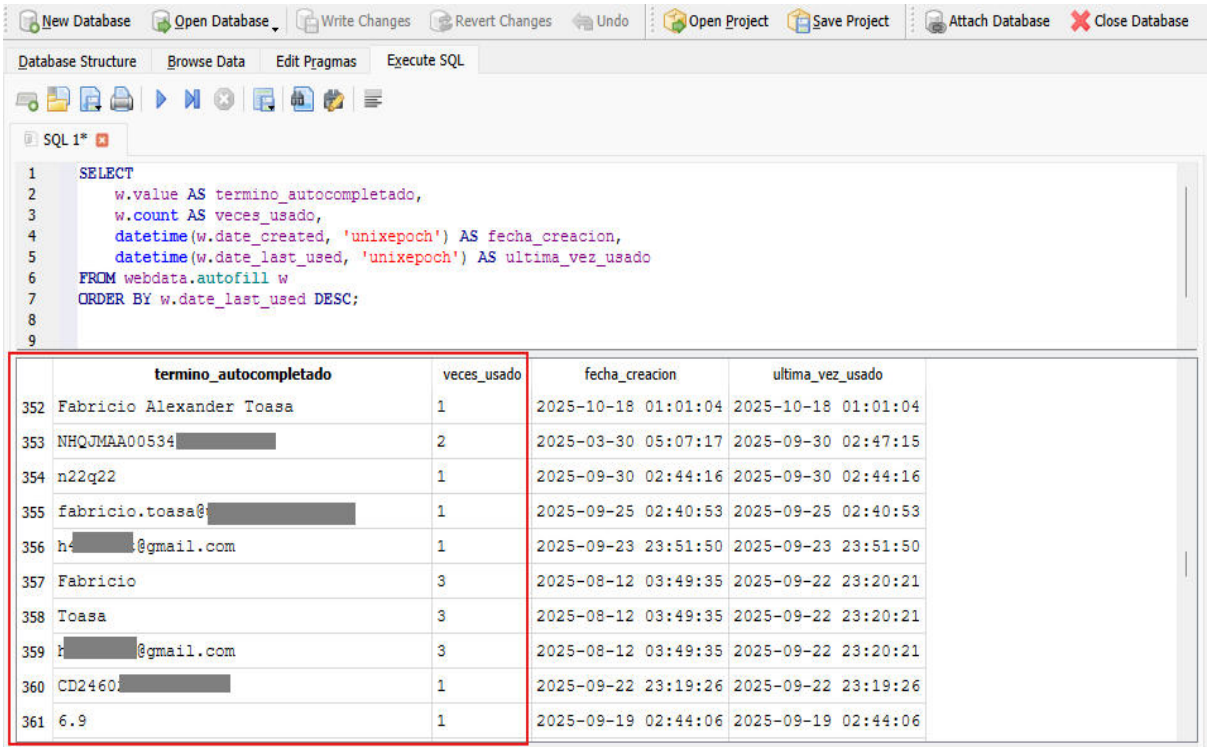
La base de datos Web Data fue analizada mediante consulta directa a la tabla ***autofill***, que almacena los términos introducidos por el usuario en formularios web mediante la función de autocompletado. La consulta empleada extrae los términos registrados con sus marcas temporales de creación y último uso:

```
SELECT
    w.value AS termino_autocompletado,
    w.count AS veces_usado,
    datetime(w.date_created, 'unixepoch') AS fecha_creacion,
    datetime(w.date_last_used, 'unixepoch') AS ultima_vez_usado
```

```
FROM webdata.autofill w
ORDER BY w.date_last_used DESC;
```

Figura 16

Análisis de Web Data para autocompletado



Nota. Se encontraron correos e información sensible, la cual fue anonimizada.

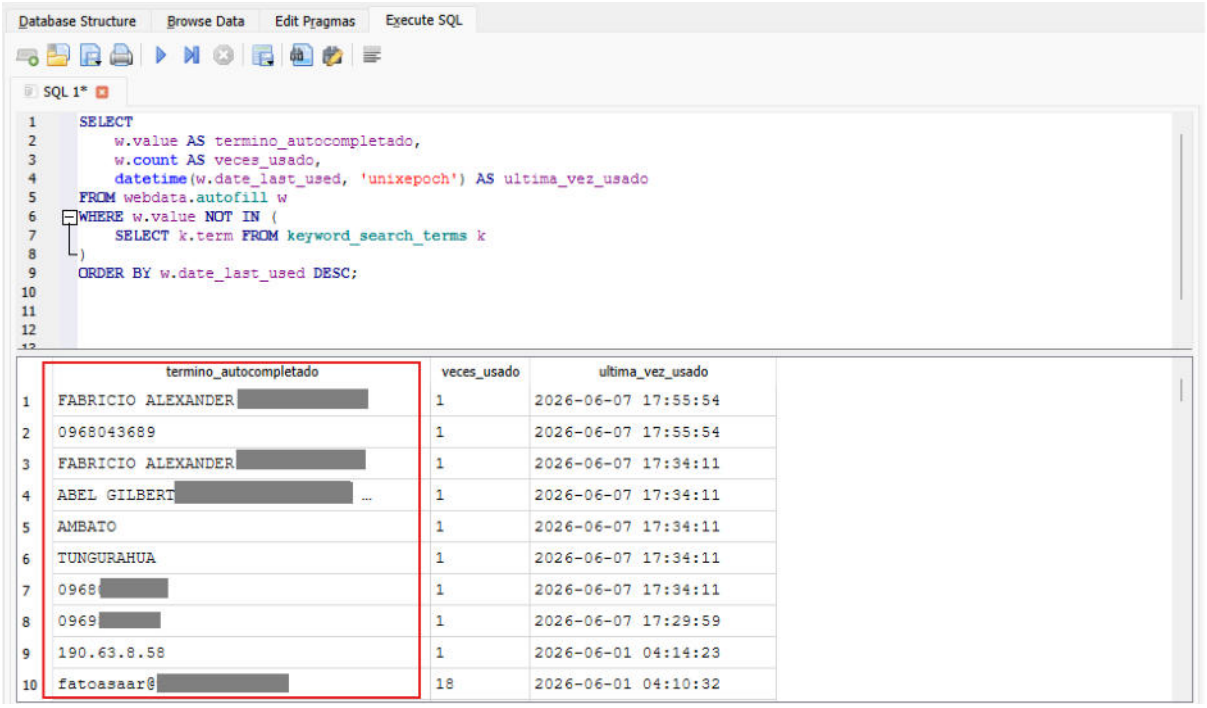
Adicionalmente se realizó una consulta de correlación entre ***keyword_search_terms*** de History y la tabla ***autofill*** de Web Data para identificar términos presentes en el autocompletado que no aparezcan en el historial de búsquedas, patrón que puede indicar borrado parcial del historial:

```
SELECT
    w.value AS termino_autocompletado,
    w.count AS veces_usado,
    datetime(w.date_last_used, 'unixepoch') AS ultima_vez_usado
FROM webdata.autofill w
WHERE w.value NOT IN (
```

```
   SELECT k.term FROM keyword_search_terms k
)
ORDER BY w.date_last_used DESC;
```

Figura 17

Correlación con la base de datos History y autocompletado



Nota. Correlación entre autofill y keyword_search_terms para detectar términos de búsqueda ausentes en el historial.

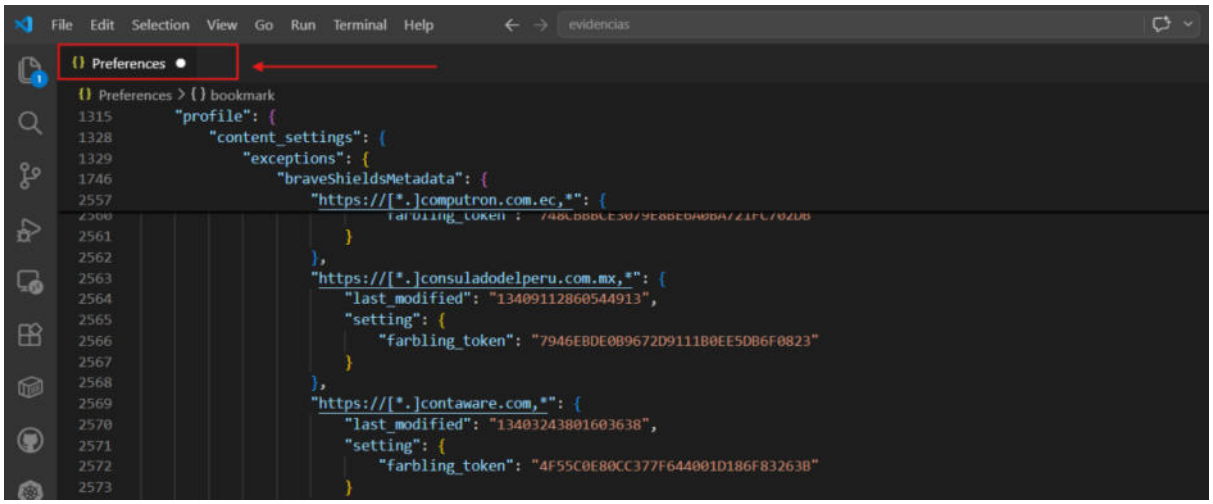
Preferences

El archivo Preferences es un documento en formato JSON ubicado en la carpeta del perfil del navegador. A diferencia de las bases de datos SQLite, su análisis no requiere consultas SQL sino la inspección directa de su estructura mediante un editor de texto con soporte para formato JSON.

Para su análisis se utilizó Visual Studio Code, que permite formatear el archivo desde una única línea compacta — formato en que Brave lo almacena — hacia una estructura legible con indentación jerárquica mediante ***Format Document (Shift + Alt + F).***

Figura 18

Análisis del artefacto Preferences con Visual Studio Code



Nota. Visual Studio Code, versión 1.105.1.

Una vez formateado, el análisis se realizó mediante búsqueda directa de campos de interés forense con el comando (Ctrl + F), orientada a siete categorías de información: configuración del directorio de descargas, estado de los mecanismos de protección del navegador (SafeBrowsing y SafeSearch), estado de sincronización con cuenta externa, vinculación de cuenta de usuario, configuración de restauración de sesión, permisos concedidos a sitios web y extensiones instaladas.

Tabla 5.

Resumen del artefacto Preferences.

Campo	Descripción	Relevancia forense

savefile.default_directory	Directorio de descargas configurado	Confirma la ruta de almacenamiento de archivos descargados durante el análisis
selectfile.last_directory	Último directorio de descarga utilizado	Detecta posibles cambios en la ruta de descarga durante el período analizado
safebrowsing.isCurrentlyActive	Estado activo de la navegación segura	Indica si el mecanismo de protección estaba activo durante la navegación analizada
safebrowsing.safeBrowsingStatus	Estado del filtrado de búsqueda segura	Indica si el filtrado de contenido estaba habilitado durante las búsquedas realizadas
sync.data_type_status	Estado de sincronización por tipo de dato	Determina si los artefactos analizados son exclusivamente locales o pueden haber sido alterados por sincronización remota
account_info	Información de cuenta vinculada al perfil	Confirma si el perfil estuvo asociado a una cuenta externa durante el período analizado
session_last_active_time	Marca temporal de la última sesión activa	Establece el límite temporal del período de actividad registrado en el perfil
session_number	Número total de sesiones registradas	Contextualiza el uso del perfil a lo largo del tiempo
sessions.restore_browser	Configuración de restauración de sesión	Identifica si visitas automáticas pudieron generarse al restaurar la sesión anterior

notifications (content_settings)	Permisos de notificaciones concedidos a sitios	Identifica dominios que recibieron permisos especiales del navegador
extensions.last_chrome_version	Versión del motor Chromium del navegador	Documenta la versión exacta del navegador al momento de la adquisición

Nota. Datos obtenidos mediante Visual Studio Code sobre la copia forense del artefacto Preferences.

Los valores obtenidos en cada campo, junto con su interpretación forense, se documentan en la Tabla 9 del Capítulo 4.

3.3.4. Proceso ETL y línea de tiempo forense integrada

El proceso de extracción, transformación y normalización (ETL) aplicado a los artefactos comprende tres operaciones fundamentales. La extracción se realizó mediante consultas SQL sobre las bases de datos History y Web Data. La transformación incluyó la conversión de marcas temporales al formato Unix con ajuste de zona horaria (UTC-5), la decodificación del campo transition mediante expresiones CASE, la normalización del campo state de la tabla downloads y la anonimización de rutas de usuario en target_path. La carga consistió en la integración de los registros extraídos de las distintas tablas en una línea de tiempo forense unificada, ordenada cronológicamente y clasificada por tipo de evento.

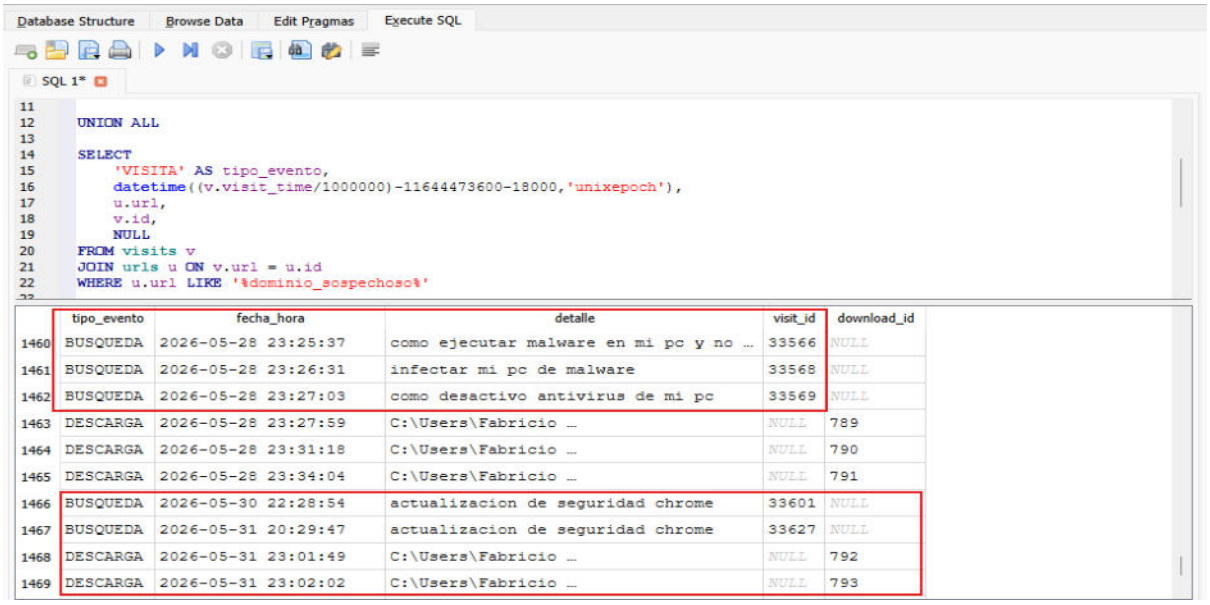
La línea de tiempo forense integrada se construyó mediante una consulta UNION ALL consolidando en una única vista los tres eventos de interés forense — búsquedas, visitas sospechosas y descargas — en orden cronológico.

```
SELECT
  'BUSQUEDA' AS tipo_evento,
  datetime((v.visit_time/1000000)-11644473600-18000,'unixepoch')
    AS fecha_hora,
```

```
    k.term AS detalle,
    v.id AS visit_id,
    NULL AS download_id
FROM keyword_search_terms k
JOIN urls u ON k.url_id = u.id
JOIN visits v ON v.url = u.id

UNION ALL

SELECT
    'VISITA' AS tipo_evento,
    datetime((v.visit_time/1000000)-11644473600-18000,'unixepoch'),
    u.url,
    v.id,
    NULL
FROM visits v
JOIN urls u ON v.url = u.id
WHERE u.url LIKE '%dominio_sospechoso%'

UNION ALL

SELECT
    'DESCARGA' AS tipo_evento,
    datetime((d.start_time/1000000)-11644473600-18000,'unixepoch'),
    REPLACE(d.target_path,'C:\Users\[USUARIO]\','[USUARIO]\')
        || ' — ' || c.url,
    NULL,
    d.id
FROM downloads d
JOIN downloads_url_chains c ON d.id = c.id

ORDER BY fecha_hora ASC;
```

Figura 19

Reconstrucción línea de tiempo forense mediante UNION ALL



Nota. La línea de tiempo forense integra búsquedas, visitas sospechosas y descargas en orden cronológico.

Los resultados de esta consulta constituyen la fuente de datos principal del análisis presentado en el Capítulo 4.

3.4. Validación Cruzada

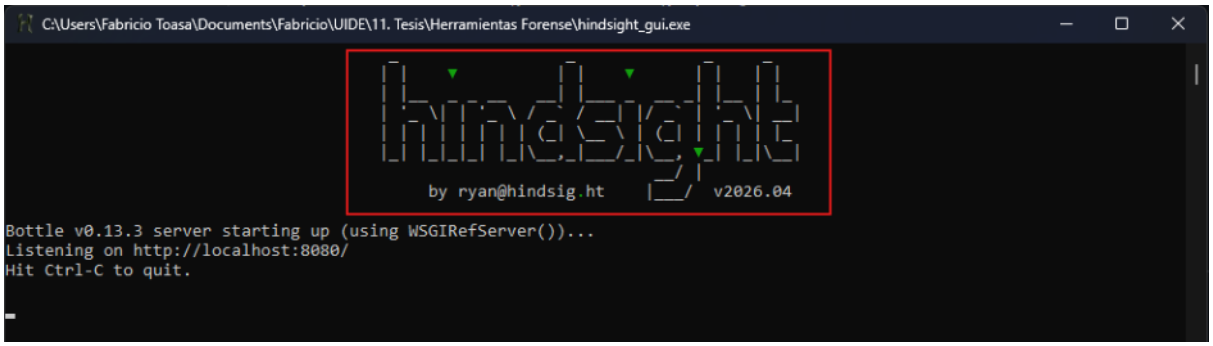
La validación cruzada se realizó aplicando diferentes herramientas forenses sobre los mismos artefactos del navegador, con el objetivo de corroborar la consistencia de los resultados obtenidos y detectar posibles variaciones en la interpretación de los datos. Las herramientas utilizadas fueron Hindsight, ChromeHistoryView, BrowsingHistoryView y Autopsy.

3.4.1. Hindsight

Para la validación cruzada se utilizó la herramienta **Hindsight**, desarrollada por Ryan Benson y distribuida en su repositorio oficial de GitHub. Se empleó la versión portable **hindsight_gui.exe (2026.04)**, la cual permite su ejecución directa sin necesidad de instalación. Al iniciar el programa se despliega una consola que habilita el uso de la interfaz gráfica a través de la dirección local http://localhost:8080/.

Figura 20

Ejecución de Hindsight portable



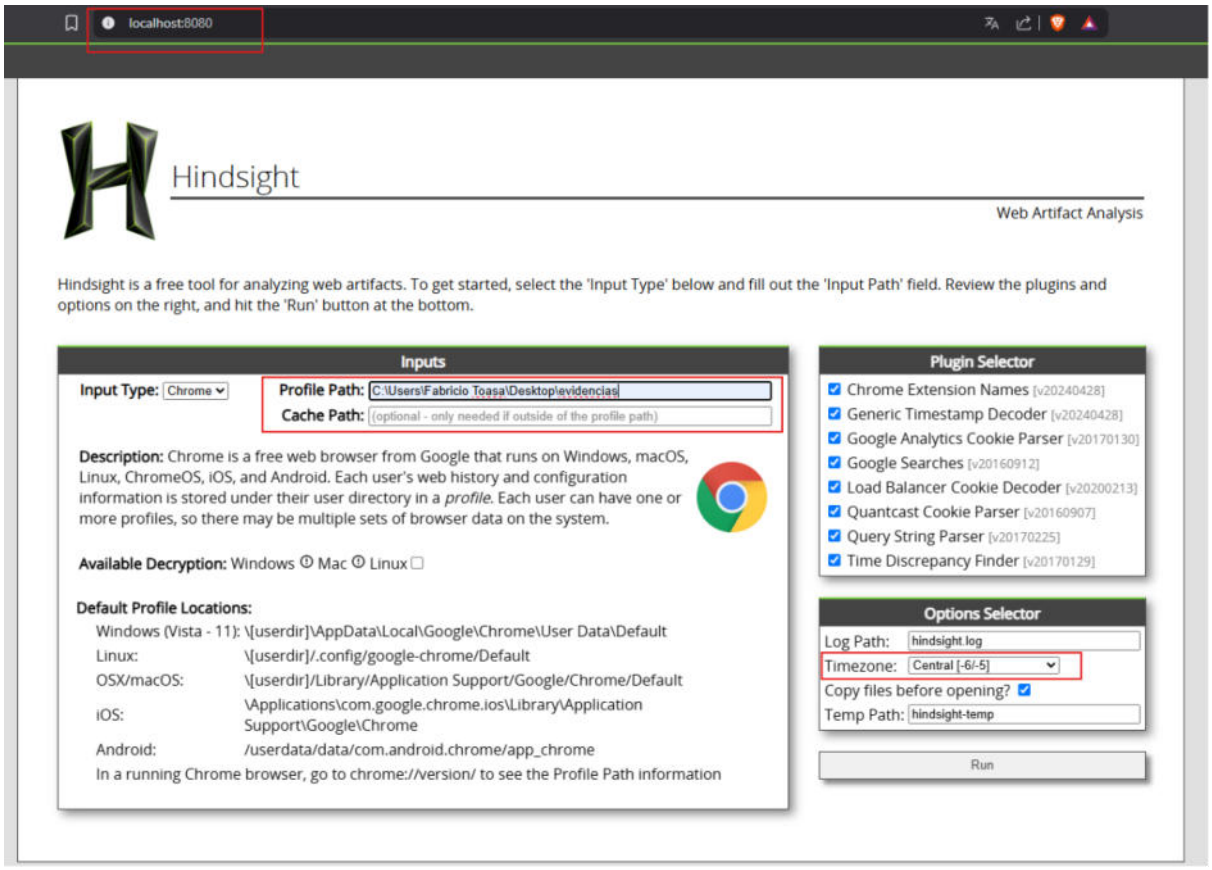
Nota. Hindsight ejecuta un server local en localhost.

En la configuración inicial se definió el **Profile Path**, especificando la ruta donde se encontraban los artefactos del navegador Brave (bases de datos SQLite y archivos JSON). Posteriormente se ajustaron los parámetros de análisis:

- **Plugin Selector**: para determinar los módulos de extracción aplicados.
- **Zona horaria:** la metodología admite la parametrización de cualquier zona horaria de acuerdo con el contexto de la investigación. En este trabajo se configuró la zona horaria oficial de Ecuador (UTC-05:00) como Timezone: Central [-6/-5], con el fin de normalizar las marcas temporales registradas en los artefactos analizados y asegurar la reconstrucción cronológica consistente de los eventos.

Figura 21

Configuración de Hindsight para el análisis

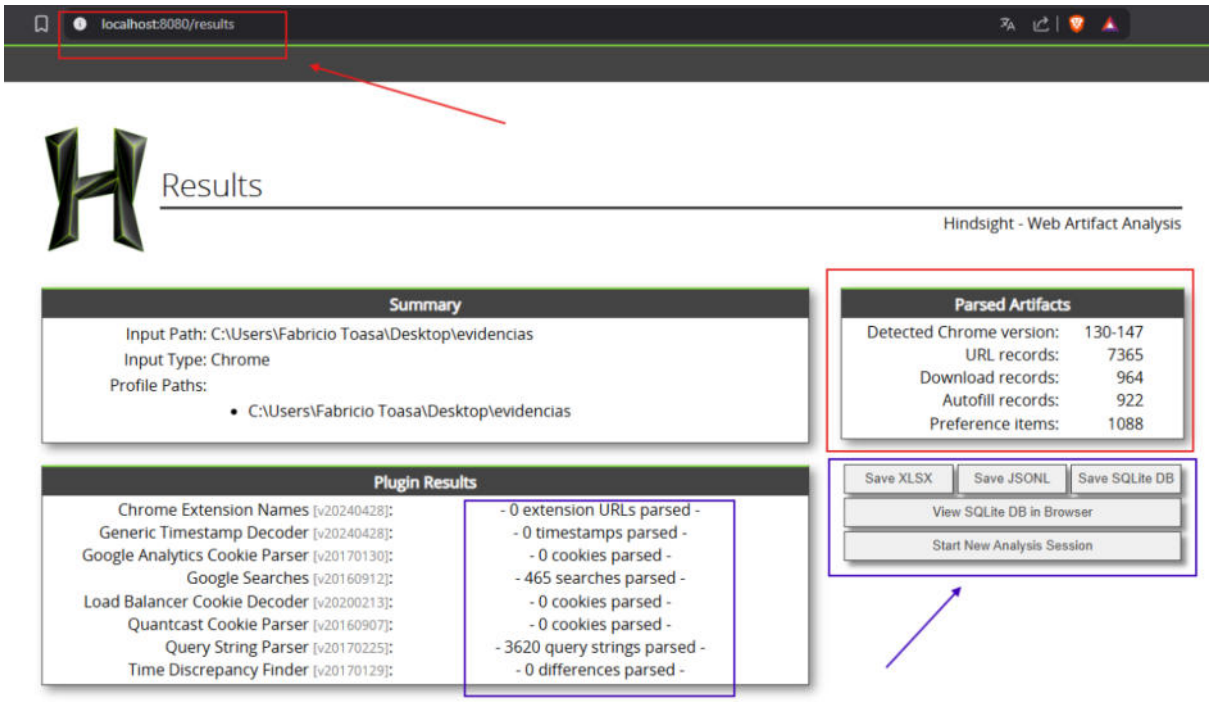


Nota. Hindsight: soporte exclusivo para Chrome/Chromium.

Una vez configurados estos parámetros, Hindsight ejecutó el **parseo automático de los artefactos SQLite y JSON**, interpretando campos internos como *transition*, *state* y *danger_type*. El proceso concluyó con la generación de tres archivos: un archivo en formato **XLSX**, un archivo **JSON** y una base de datos **SQLite**, que contienen la información consolidada de visitas, búsquedas, descargas y configuraciones del navegador.

Figura 22

Exportación de resultados mediante Hindsight



Nota. Hindsight procesa tres tipos de documentos para su análisis: **XLSX, JSON y SQLite**.

Para verificar la consistencia de los resultados, se realizaron consultas SQL directamente sobre la base de datos generada por Hindsight. Entre las más relevantes se incluye:

Consulta 1 – Visitas (History)

Esta consulta permitió extraer las URLs visitadas, sus títulos, la marca temporal y el tipo de transición asociado.

```
SELECT url, title, timestamp, visit_id, transition
FROM timeline
WHERE type='url'
ORDER BY timestamp DESC;
```

Figura 23

Registros de urls consultadas desde Hindsight

	url	title	timestamp
10	https://www.amazon.com/account-…	Cuenta suspendida temporalmente	2026-06-07 12:45:14.115
11	https://account-status.amazon.com/?…	Cuenta suspendida temporalmente	2026-06-07 12:45:14.115
12	https://www.amazon.com/ap/signin?…	Amazon Iniciar sesión	2026-06-07 12:45:01.385
13	https://www.amazon.com/-/es/ap/…	Amazon Iniciar sesión	2026-06-07 12:44:56.750
14	https://www.amazon.com/account-…	Cuenta suspendida temporalmente	2026-06-07 12:37:11.953
15	https://account-status.amazon.com/?…	Cuenta suspendida temporalmente	2026-06-07 12:37:11.953
16	https://www.amazon.com/ap/signin?…	Amazon Iniciar sesión	2026-06-07 12:36:56.589
17	https://www.amazon.com/gp/your-…	Amazon Iniciar sesión	2026-06-07 12:36:52.994
18	https://www.amazon.com/ap/signin?…	Amazon Iniciar sesión	2026-06-07 12:36:52.994
19	https://www.amazon.com/-/es/gp/css/…	Tu cuenta	2026-06-07 12:36:42.631

```
Execution finished without errors.
Result: 7365 rows returned in 40ms
At line 1:
```

Nota. Extracción de 7.365 registros de URLs desde timeline.

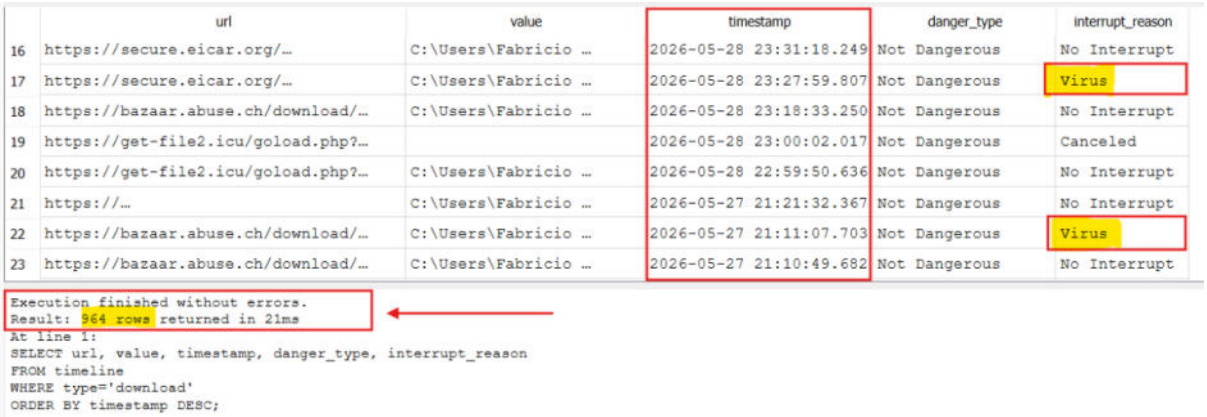
Consulta 2 – Descargas (Downloads)

Con esta instrucción se obtuvieron los registros de descargas, incluyendo la URL de origen, el archivo descargado, la clasificación de riesgo (*danger_type*) y posibles interrupciones.

```
SELECT url, value, timestamp, danger_type, interrupt_reason
FROM timeline
WHERE type='download'
ORDER BY timestamp DESC;
```

Figura 24

Registros de descargas con Hindsight



	url	value	timestamp	danger_type	interrupt_reason
16	https://secure.eicar.org/…	C:\Users\Fabricio …	2026-05-28 23:31:18.249	Not Dangerous	No Interrupt
17	https://secure.eicar.org/…	C:\Users\Fabricio …	2026-05-28 23:27:59.807	Not Dangerous	Virus
18	https://bazaar.abuse.ch/download/…	C:\Users\Fabricio …	2026-05-28 23:18:33.250	Not Dangerous	No Interrupt
19	https://get-file2.icu/goload.php?…		2026-05-28 23:00:02.017	Not Dangerous	Canceled
20	https://get-file2.icu/goload.php?…	C:\Users\Fabricio …	2026-05-28 22:59:50.636	Not Dangerous	No Interrupt
21	https://…	C:\Users\Fabricio …	2026-05-27 21:21:32.367	Not Dangerous	No Interrupt
22	https://bazaar.abuse.ch/download/…	C:\Users\Fabricio …	2026-05-27 21:11:07.703	Not Dangerous	Virus
23	https://bazaar.abuse.ch/download/…	C:\Users\Fabricio …	2026-05-27 21:10:49.682	Not Dangerous	No Interrupt

```
Execution finished without errors.
Result: 964 rows returned in 21ms
At line 1:
SELECT url, value, timestamp, danger_type, interrupt_reason
FROM timeline
WHERE type='download'
ORDER BY timestamp DESC;
```

Nota. Extracción de 964 registros de descargas con Hindsight

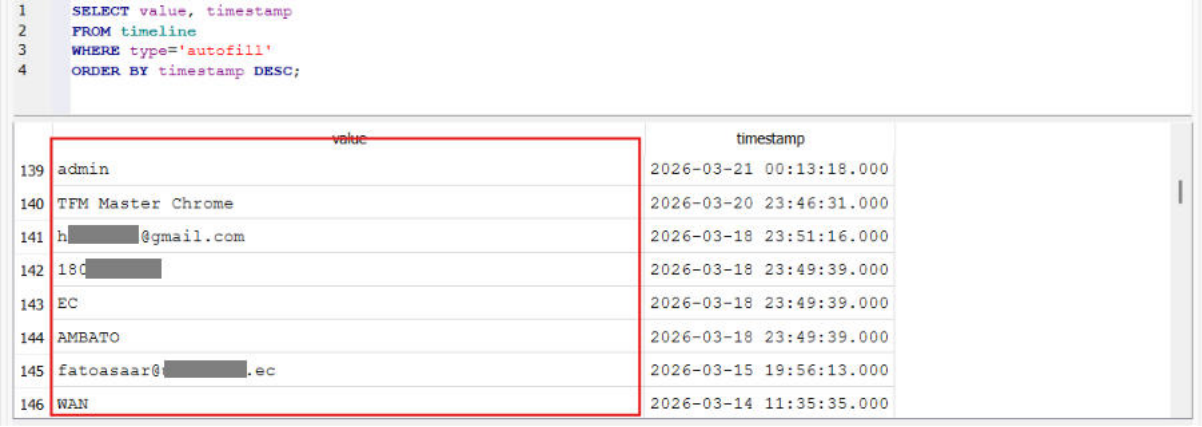
Consulta 3 – Autocompletado (Web Data)

Esta consulta permitió identificar valores de autocompletado registrados en formularios, junto con su marca temporal.

```
SELECT value, timestamp
FROM timeline
WHERE type='autofill'
ORDER BY timestamp DESC;
```

Figura 25

Resultados autocompletado mediante Hindsight

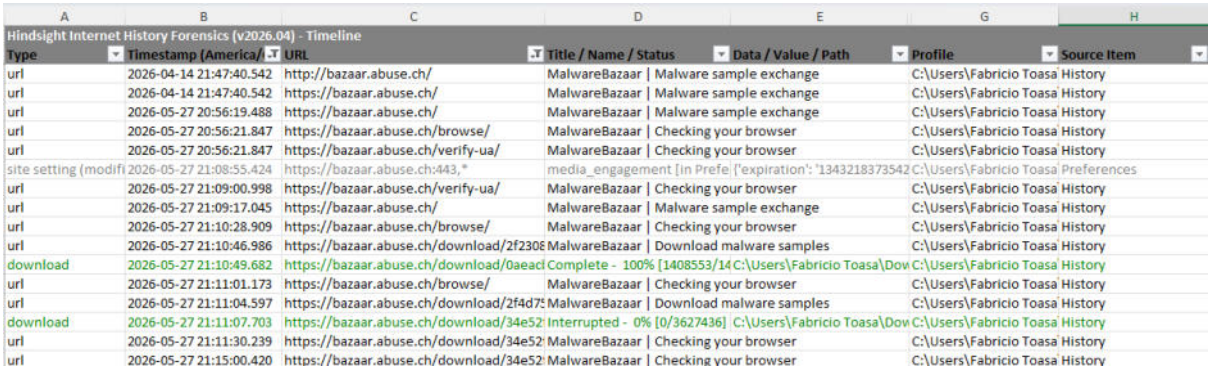


Nota. Se extrajeron 922 resultados del campo autofill utilizando Hindsight.

El archivo **CSV** generado por Hindsight constituye un insumo central para el análisis forense, ya que consolida en una única estructura cronológica los distintos eventos extraídos de los artefactos del navegador. Su formato tabular permite examinar de manera integrada las visitas, descargas y valores de autocompletado, facilitando la correlación entre registros y la identificación de patrones técnicos asociados a los tres escenarios planteados: historial de navegación real, descargas controladas de archivos maliciosos y simulación de typosquatting.

Figura 26

Análisis del archivo CSV generado por Hindsight



A	B	C	D	E	G	H
Hindsight Internet History Forensics (v2026.04) - Timeline						
Type	Timestamp (America/	URL	Title / Name / Status	Data / Value / Path	Profile	Source Item
url	2026-04-14 21:47:40.542	http://bazaar.abuse.ch/	MalwareBazaar | Malware sample exchange		C:\Users\Fabricio Toasa	History
url	2026-04-14 21:47:40.542	https://bazaar.abuse.ch/	MalwareBazaar | Malware sample exchange		C:\Users\Fabricio Toasa	History
url	2026-05-27 20:56:19.488	https://bazaar.abuse.ch/	MalwareBazaar | Malware sample exchange		C:\Users\Fabricio Toasa	History
url	2026-05-27 20:56:21.847	https://bazaar.abuse.ch/browse/	MalwareBazaar | Checking your browser		C:\Users\Fabricio Toasa	History
url	2026-05-27 20:56:21.847	https://bazaar.abuse.ch/verify-ua/	MalwareBazaar | Checking your browser		C:\Users\Fabricio Toasa	History
site setting (modifi	2026-05-27 21:08:55.424	https://bazaar.abuse.ch:443,*	media_engagement [in Prefe	{'expiration': '1343218373542	C:\Users\Fabricio Toasa	Preferences
url	2026-05-27 21:09:00.998	https://bazaar.abuse.ch/verify-ua/	MalwareBazaar | Checking your browser		C:\Users\Fabricio Toasa	History
url	2026-05-27 21:09:17.045	https://bazaar.abuse.ch/	MalwareBazaar | Malware sample exchange		C:\Users\Fabricio Toasa	History
url	2026-05-27 21:10:28.909	https://bazaar.abuse.ch/browse/	MalwareBazaar | Checking your browser		C:\Users\Fabricio Toasa	History
url	2026-05-27 21:10:46.986	https://bazaar.abuse.ch/download/2f2308	MalwareBazaar | Download malware samples		C:\Users\Fabricio Toasa	History
download	2026-05-27 21:10:49.682	https://bazaar.abuse.ch/download/0aeacl	Complete - 100% [1408553/14	C:\Users\Fabricio Toasa\Dow	C:\Users\Fabricio Toasa	History
url	2026-05-27 21:11:01.173	https://bazaar.abuse.ch/browse/	MalwareBazaar | Checking your browser		C:\Users\Fabricio Toasa	History
url	2026-05-27 21:11:04.597	https://bazaar.abuse.ch/download/2f4d7	MalwareBazaar | Download malware samples		C:\Users\Fabricio Toasa	History
download	2026-05-27 21:11:07.703	https://bazaar.abuse.ch/download/34e52	Interrupted - 0% [0/3627436]	C:\Users\Fabricio Toasa\Dow	C:\Users\Fabricio Toasa	History
url	2026-05-27 21:11:30.239	https://bazaar.abuse.ch/download/34e52	MalwareBazaar | Checking your browser		C:\Users\Fabricio Toasa	History
url	2026-05-27 21:15:00.420	https://bazaar.abuse.ch/download/34e52	MalwareBazaar | Checking your browser		C:\Users\Fabricio Toasa	History

Nota. CSV de Hindsight revisado manualmente.

El examen de este archivo posibilitó verificar la correcta normalización de las marcas temporales, la clasificación de los tipos de evento y la preservación de campos relevantes como *transition*, *danger_type* e *interrupt_reason*. Para reforzar la transparencia metodológica, se incorporaron capturas del CSV en el desarrollo, ilustrando cómo Hindsight organiza los datos en una línea de tiempo forense integrada que será objeto de interpretación detallada en el capítulo 4.

3.4.2. ChromeHistoryView

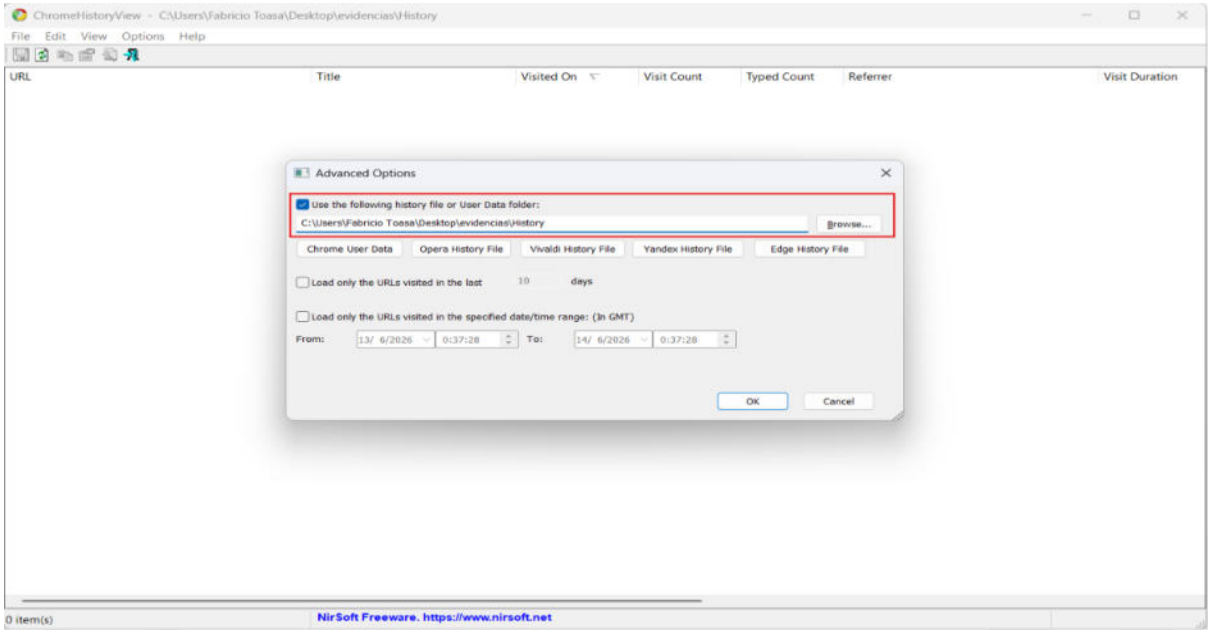
ChromeHistoryView es una utilidad portable desarrollada por NirSoft, diseñada específicamente para la lectura e interpretación del historial de navegación de navegadores basados en Chromium. Opera directamente sobre el archivo History en formato SQLite y presenta sus resultados en una interfaz tabular con capacidad de exportación en múltiples formatos.

El procedimiento consistió en cargar el archivo History correspondiente al perfil analizado del navegador Brave. Una vez abierto, la herramienta desplegó en formato tabular

los principales campos de interés: URL visitada, título de la página, fecha y hora de acceso, número de visitas y perfil de usuario asociado. Esta representación permitió revisar de manera directa los registros de navegación y contrastarlos con los datos previamente extraídos mediante consultas SQL en DB Browser y con el archivo CSV generado por Hindsight.

Figura 27

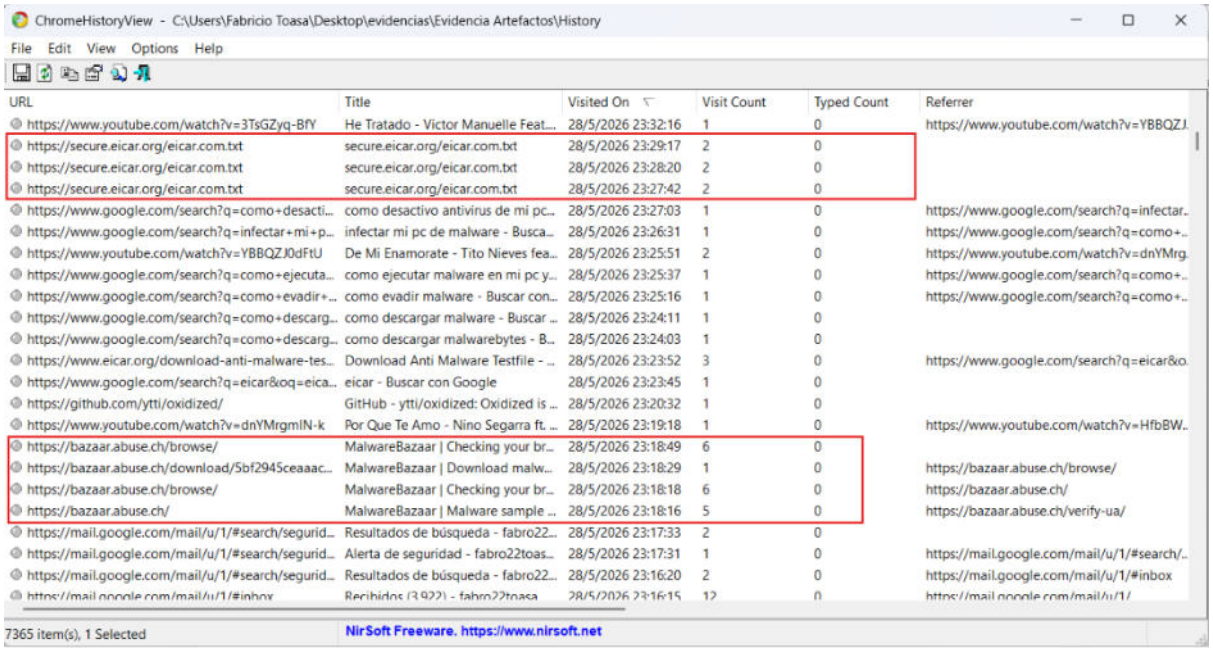
Ejecución de ChromeHistoryView



Nota. ChromeHistoryView es un archivo ejecutable compatible con Windows 11.

Figura 28

Análisis de resultados con ChromeHistoryView



Nota. Análisis manual de los registros generados por ChromeHistoryView.

El análisis con **ChromeHistoryView** se orientó a verificar la consistencia de las visitas registradas en los tres escenarios planteados. Para garantizar la transparencia del procedimiento, se incorporaron capturas de la interfaz que muestran cómo la herramienta organiza los registros y permiten evidenciar su correlación con los artefactos analizados en las demás plataformas.

Figura 29

Análisis historial real con ChromeHistoryView

	A	B	C	D	E	F	G	H	I	J	K
1	URL	Title	Visited On	Visit Coun	Typed Cou	Referrer	Visit Durat	Visit ID	Profile	URL Length	Transition
414	https://winload1.fin-tech.c	File is ready t	28/5/2026 22:59	1	0		00:00:45.183	33534	evidencias	45	Link
415	https://oficial-kmspico.io/d	42%20MB&e1	Descargar Archi	##########	1	0		00:02:12.392	33533	evidencias	89
416	https://oficial-kmspico.io/	?? Descargar	28/5/2026 22:59	1	0	https://www.	00:02:16.079	33532	evidencias	27	Link
7367											

Nota. Exportación de registros de ChromeHistoryView a CSV.

Figura 30

Análisis de descarga de malware con ChromeHistoryView

	A	B	C	D	E	F	G	H	I	J	K
1	URL	Title	Visited On	Visit Coun	Typed Cou	Referrer	Visit Durat	Visit ID	Profile	URL Length	Transition
108	https://www.eicar.org/dowi	Download Ar	4/6/2026 21:34	3	0		00:52:22.217	33840	evidencias	53	Reload
145	https://www.eicar.org/dowi	Download Ar	3/6/2026 22:11	3	0		01:23:25.921	33803	evidencias	53	Reload
177	https://www.eicar.org/dowi	Download Ar	3/6/2026 19:51	3	0		02:19:02.320	33771	evidencias	53	Reload
211	https://www.eicar.org/dowi	Download Ar	1/6/2026 22:47	3	0	https://www.	24:28:29.133	33737	evidencias	53	Link
212	https://www.eicar.com/#ab	Eicar e.V. - Eu	1/6/2026 22:47	4	0	https://www.	eicar.org/#ab	33735	evidencias	28	Link
213	https://www.eicar.org/#abc	Eicar e.V. - Eu	1/6/2026 22:47	4	0	https://www.	00:00:05.221	33736	evidencias	28	Link
214	https://www.eicar.org/#abc	Eicar e.V. - Eu	1/6/2026 22:47	4	0	https://www.	00:00:12.602	33734	evidencias	28	Link
215	https://www.eicar.com/#ab	Eicar e.V. - Eu	1/6/2026 22:47	4	0	https://www.	eicar.org/proj	33733	evidencias	28	Link
216	https://www.eicar.org/proj	Projects - EIC	1/6/2026 22:47	2	0	https://www.	00:00:05.932	33732	evidencias	31	Link
217	https://www.eicar.org/tean	Our Team of	1/6/2026 22:47	3	0	https://www.	00:00:05.745	33731	evidencias	27	Link
218	https://www.eicar.com/#ab	Eicar e.V. - Eu	1/6/2026 22:46	4	0	https://www.	eicar.org/#ab	33729	evidencias	28	Link
219	https://www.eicar.org/#abc	Eicar e.V. - Eu	1/6/2026 22:46	4	0	https://www.	00:01:04.304	33730	evidencias	28	Link

Nota. Búsqueda de incidentes de seguridad mediante ChromeHistoryView.

Figura 31

Análisis de typosquatting con ChromeHistoryView

	A	B	C	D	E	F	G	H	I	J	K
1	URL	Title	Visited On	Visit Coun	Typed Cou	Referrer	Visit Durat	Visit ID	Profile	URL Length	Transition
372	http://gooogle.com/	Directory listi	28/5/2026 23:33	2	0	https://gooo	00:01:24.628	33576	evidencias	19	Typed
373	https://gooogle.com/	Directory listi	28/5/2026 23:33	1	1	http://gooogle.com/		33575	evidencias	20	Typed
374	http://gooogle.com/	Directory listi	28/5/2026 23:33	2	0			33574	evidencias	19	Typed
7367											

Nota. Se analiza registros del sitio fraudulento implementado mediante el server local.

De este modo, ChromeHistoryView aportó una verificación independiente y ágil de los eventos, fortaleciendo la validez del análisis forense.

3.4.3. BrowsingHistoryView

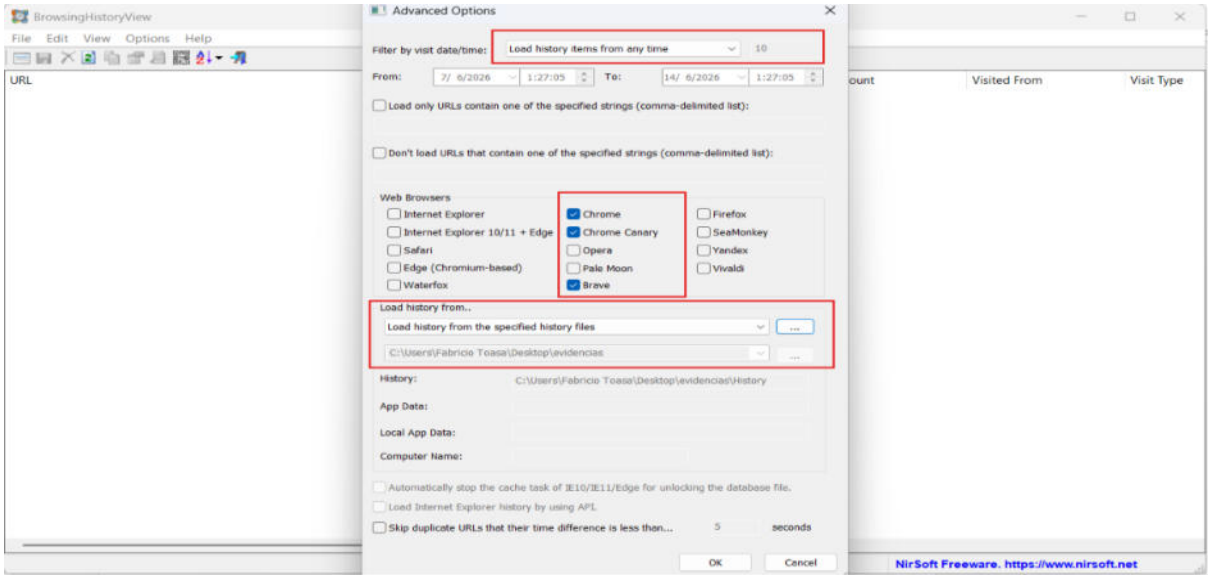
La herramienta **BrowsingHistoryView**, también desarrollada por NirSoft, se utilizó como parte del proceso de validación cruzada. A diferencia de ChromeHistoryView, esta utilidad permite consolidar en una sola vista los historiales de distintos navegadores instalados en el sistema, incluyendo Brave, lo que facilita la comparación y verificación de registros en entornos híbridos.

El procedimiento consistió en cargar el archivo History del perfil analizado de Brave, configurando la herramienta para que reconociera específicamente este navegador. Una vez

ejecutada, BrowsingHistoryView presentó un listado cronológico de las páginas visitadas, con campos relevantes como **URL, título, fecha y hora de acceso, número de visitas y navegador asociado**. Esta representación permitió revisar de manera integrada los registros y contrastarlos con los datos obtenidos mediante DB Browser y Hindsight.

Figura 32

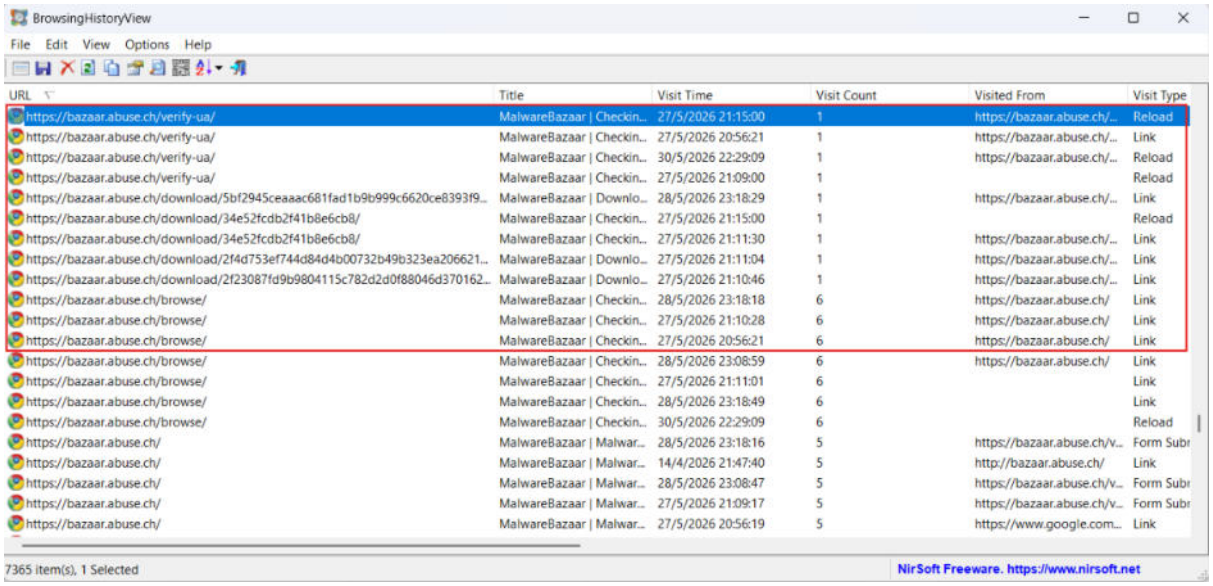
Ejecución de BrowsingHistoryView



Nota. BrowsingHistoryView es un archivo ejecutable compatible con Windows 11.

Figura 33

Análisis de resultados con BrowsingHistoryView

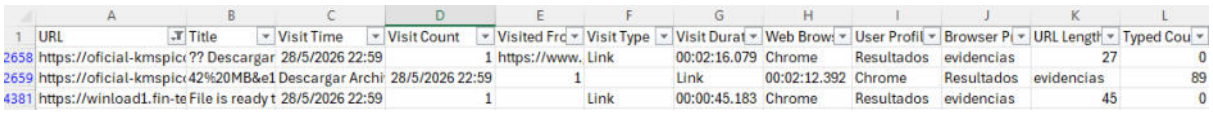


Nota. Análisis manual de los registros generados por BrowsingHistoryView.

El análisis con **BrowsingHistoryView** se orientó a comprobar la consistencia de los eventos de navegación en los tres escenarios definidos. Para garantizar la transparencia del procedimiento, se añadieron capturas de la interfaz que muestran cómo la herramienta organiza los registros y permiten evidenciar su correlación con los artefactos examinados en las demás plataformas.

Figura 34

Análisis historial real con BrowsingHistoryView



	A	B	C	D	E	F	G	H	I	J	K	L
1	URL	Title	Visit Time	Visit Count	Visited Frc	Visit Type	Visit Durat	Web Brow	User Profil	Browser P	URL Length	Typed Cou
2658	https://oficial-kmspic	?? Descargar	28/5/2026 22:59	1	https://www.	Link	00:02:16.079	Chrome	Resultados	evidencias	27	0
2659	https://oficial-kmspic	42%20MB&e1	Descargar Archi	28/5/2026 22:59	1		Link	00:02:12.392	Chrome	Resultados	evidencias	89
4381	https://winload1.fin-te	File is ready t	28/5/2026 22:59	1		Link	00:00:45.183	Chrome	Resultados	evidencias	45	0

Nota. Búsqueda de incidentes de seguridad mediante BrowsingHistoryView.

Figura 35

Análisis de descarga de malware con BrowsingHistoryView

	A	B	C	D	E	F	G	H	I	J	K	L
1	URL	Title	Visit Time	Visit Coun	Visited Frc	Visit Type	Visit Durat	Web Brow	User Profil	Browser P	URL Length	Typed Cou
630	http://bazaar.abuse.cl	MalwareBaza	14/4/2026 21:47	1		Link		Chrome	Resultados	evidencias	23	0
1600	https://bazaar.abuse.(	MalwareBaza	14/4/2026 21:47	5	http://bazaar	Link	00:00:08.107	Chrome	Resultados	evidencias	24	0
1601	https://bazaar.abuse.(	MalwareBaza	27/5/2026 21:09	5	https://bazaa	Form Submit	00:01:11.871	Chrome	Resultados	evidencias	24	0
1602	https://bazaar.abuse.(	MalwareBaza	28/5/2026 23:18	5	https://bazaa	Form Submit	00:00:01.486	Chrome	Resultados	evidencias	24	0
1603	https://bazaar.abuse.(	MalwareBaza	27/5/2026 20:56	5	https://www.	Link	00:00:02.362	Chrome	Resultados	evidencias	24	0
1604	https://bazaar.abuse.(	MalwareBaza	28/5/2026 23:08	5	https://bazaa	Form Submit	00:00:12.093	Chrome	Resultados	evidencias	24	0
1605	https://bazaar.abuse.(	MalwareBaza	28/5/2026 23:08	6	https://bazaa	Link	00:09:17.731	Chrome	Resultados	evidencias	31	0
1606	https://bazaar.abuse.(	MalwareBaza	28/5/2026 23:18	6	https://bazaa	Link	00:00:11.285	Chrome	Resultados	evidencias	31	0
1607	https://bazaar.abuse.(	MalwareBaza	27/5/2026 21:10	6	https://bazaa	Link	00:00:18.080	Chrome	Resultados	evidencias	31	0
1608	https://bazaar.abuse.(	MalwareBaza	28/5/2026 23:18	6		Link	00:23:32.540	Chrome	Resultados	evidencias	31	0
1609	https://bazaar.abuse.(	MalwareBaza	30/5/2026 22:29	6		Reload		Chrome	Resultados	evidencias	31	0

Nota. Búsqueda de incidentes de malware mediante BrowsingHistoryView.

Figura 36

Análisis de typosquatting con BrowsingHistoryView

	A	B	C	D	E	F	G	H	I	J	K
1	URL	Title	Visit Time	Visit Count	Visited Frc	Visit Type	Visit Durat	Web Brow	User Profil	Browser P	URL Length
641	http://gooogle.com/	Directory listi	28/5/2026 23:33	2	https://goooş	Typed URL	00:01:24.628	Chrome	Resultados	evidencias	19
642	http://gooogle.com/	Directory listi	28/5/2026 23:33	2		Typed URL		Chrome	Resultados	evidencias	19
1960	https://gooogle.com/	Directory listi	28/5/2026 23:33	1	http://gooogl	Typed URL		Chrome	Resultados	evidencias	20

Nota. Se analiza registros del sitio fraudulento implementado mediante el servidor local.

De este modo, BrowsingHistoryView ofreció una verificación independiente y complementaria, fortaleciendo la validez del proceso forense.

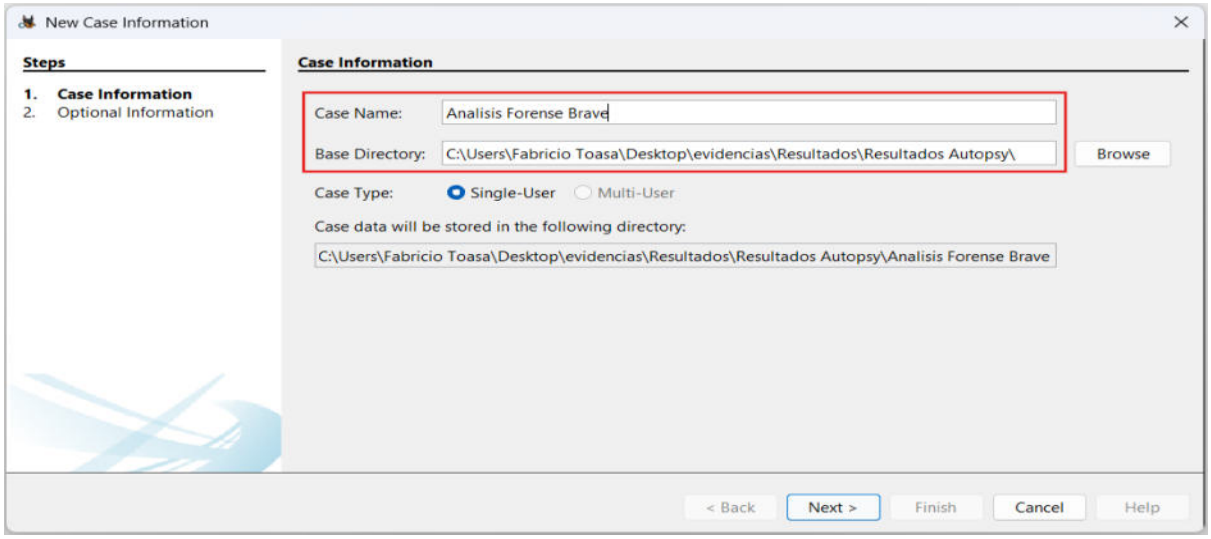
3.4.4. Autopsy

Autopsy es una plataforma de análisis forense digital de código abierto desarrollada por Basis Technology, utilizada en entornos profesionales y académicos como plataforma de investigación forense integral. A diferencia de las herramientas anteriores, Autopsy no está diseñada específicamente para el análisis de artefactos de navegador sino para el análisis forense completo de sistemas de archivos, lo que la convierte en la herramienta de mayor alcance, aunque con requerimientos de configuración más complejos.

Se creó un caso forense denominado Análisis Forense Brave con configuración Single-user.

Figura 37

Creación de caso en Autopsy

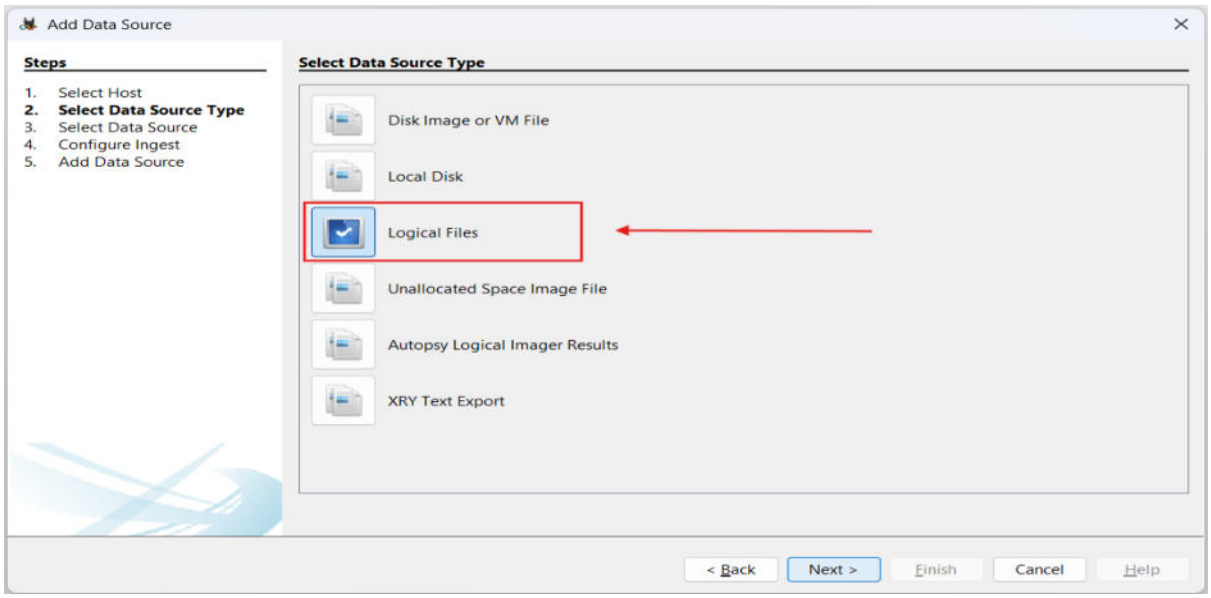


Nota. Autopsy versión 4.23.1.

La fuente de datos fue cargada como Logical Files apuntando a la estructura de directorios del perfil de Brave replicada localmente bajo la siguiente jerarquía de carpetas: Users\[USUARIO]\`AppData\Local\BraveSoftware\Brave-Browser\User` Data\Default\

Figura 38

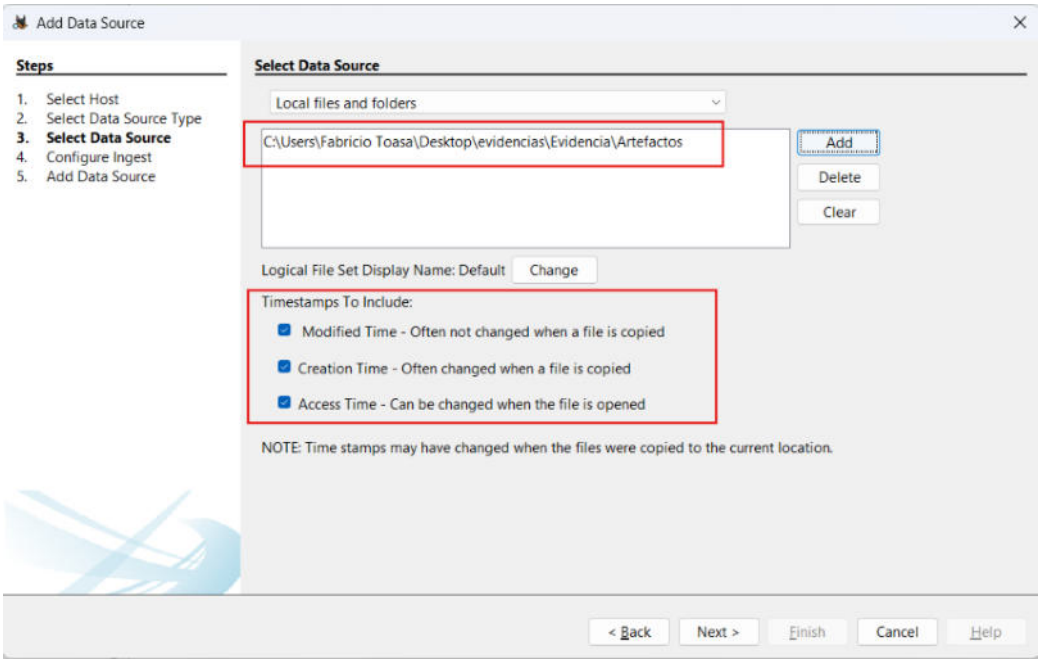
Selección de artefactos con Logical Files en Autopsy



Nota. Logical Files se usa cuando se cargan archivos o carpetas individuales.

Figura 39

Selección de archivos a analizar con Autopsy



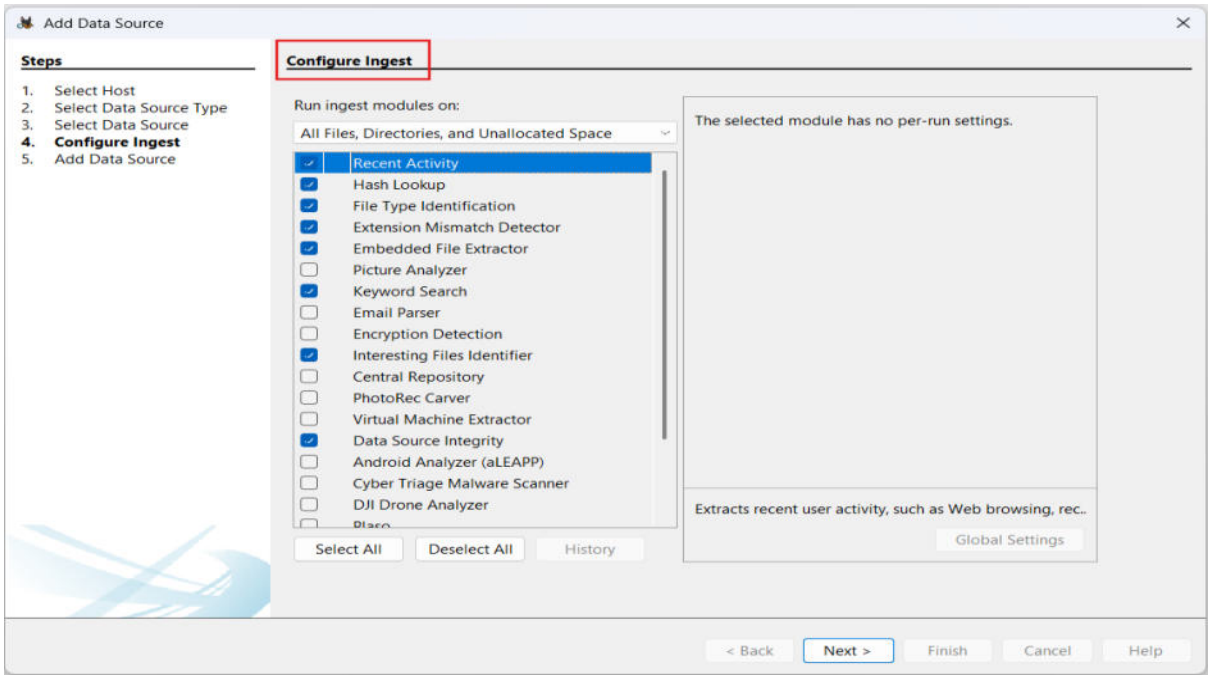
Nota. Se habilita los MAC Times en Autopsy.

Esta estructura replica la ruta original del perfil en el sistema operativo Windows 11, condición necesaria para que el módulo ***Recent Activity*** reconozca los artefactos como pertenecientes a un perfil de navegador. La fuente de datos incluyó los artefactos: History, Web Data y Preferences.

Se activaron los siguientes módulos de ingestión: ***Recent Activity, File Type Identification, Extension Mismatch Detector, Keyword Search, Hash Lookup e Interesting*** Files. En el módulo ***Keyword Search*** se configuró una lista personalizada denominada ***analisis_brave*** con los términos de búsqueda correspondientes a los escenarios del análisis: kmspico, eicar, get-file2, bazaar, gooogle, malware, utilizando el tipo de coincidencia Substring para detectar ocurrencias parciales en cualquier archivo del perfil.

Figura 40

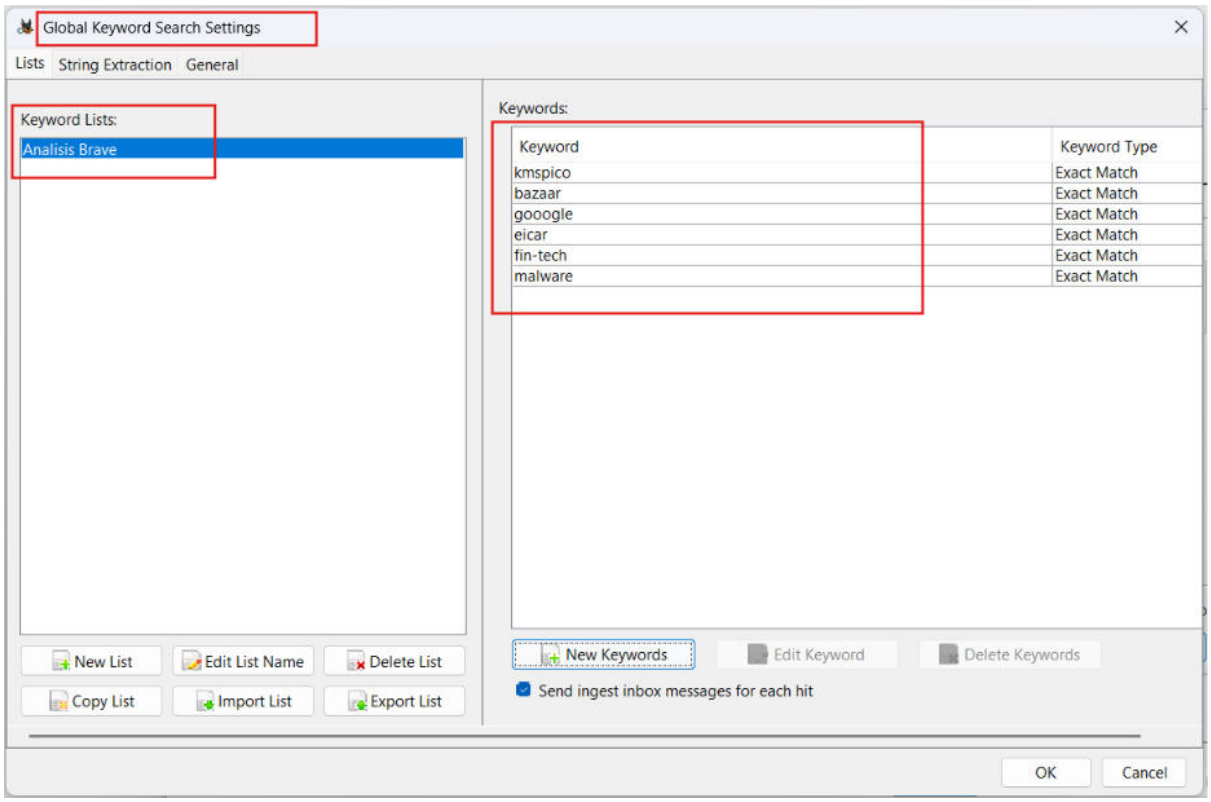
Configuración de módulos Ingest en Autopsy



Nota. Se habilitan solo los módulos necesarios para el análisis forense con Autopsy.

Figura 41

Configuración de Keywords Lists en el módulo Ingest



Nota. La lista se crea en base a los eventos detectados con las herramientas anteriores.

Una vez completada la ingestión se generó un informe forense en formato HTML mediante la función Generate Report, seleccionando todos los artefactos identificados durante el análisis. Este informe constituye el formato de documentación estándar en procesos periciales formales y se incluye en el Apéndice C de evidencias del presente trabajo.

4. Resultados

Este capítulo presenta el análisis forense de los artefactos persistentes del perfil del navegador Brave — basado en Chromium — en un entorno Windows 11. La información se organiza en cuatro apartados: el análisis manual con DB Browser for SQLite como método principal, la validación cruzada mediante cuatro herramientas especializadas, el examen detallado de los escenarios forenses planteados y la valoración del alcance probatorio de la evidencia recuperada. Todo dato personal identificable fue anonimizado conforme a los criterios establecidos en el marco de autorización del trabajo.

4.1. Resultados del análisis manual – DB Browser for SQLite

4.1.1. Estructura y esquema relacional de los artefactos

El análisis de la base de datos **History** mediante la instrucción `PRAGMA table_info` permitió confirmar que el esquema relacional de la versión de Chromium estudiada presenta una variación respecto a versiones anteriores documentadas: el campo de relación entre las tablas *visits* y *urls* se denomina **url** en lugar de **url_id**. Esta verificación previa fue clave para formular correctamente las consultas SQL de correlación entre tablas. La base de datos **History** mostró el siguiente volumen de registros en sus principales tablas:

Tabla 6.

Resultados principales tablas de la base de datos History.

Tabla	Total de registros	Descripción
Urls	3886	URLs únicas visitadas
Visits	7365	Eventos individuales de visita
downloads	606	Registros de descarga
downloads_url_chains	964	Eslabones de cadenas de descarga
keyword_search_terms	394	Términos de búsqueda registrados

Nota. Resultados generales del artefacto History.

La base de datos Web Data presento 922 registros en la tabla autofill, todos correspondientes a términos de autocompletado generados durante la navegación del periodo analizado. La verificación previa de las tablas *credit_cards, addresses y masked_credit_cards* confirmo que no contienen registros — garantía de ausencia de datos financieros sensibles en los artefactos analizados.

4.1.2. Hallazgos en la base de datos History

El análisis de la base de datos History permitió identificar 74 registros de interés forense distribuidos en el periodo comprendido entre el 14 de marzo y el 4 de junio de 2026, clasificados en tres categorías de eventos:

Tabla 7.

Hallazgos en la base de datos History.

Tipo de evento	Total de registros	Período
Búsquedas relacionadas con los escenarios	15	**14/03/2026** — 01/06/2026
Visitas a dominios de interés forense	53	14/04/2026 — **04/06/2026**
Descarga de los escenarios analizados	8	27/05/2026 — 01/06/2026
Total	74	82 días

Nota. Resumen de los 74 eventos identificadas.

El análisis de la tabla *downloads* identifico seis descargas de interés forense con los siguientes atributos:

Tabla 8.

Resultados tabla downloads en la base de datos History.

ID	Fecha y Hora	Archivo Descargado	Tamaño	Estado	URL de descarga
783	27/5/2026 21:10	2f23087f[...].zip	1.34 MB	Completa	bazaar.abuse.ch/download/0aeacbe9[...]

784	27/5/2026 21:11	2f4d753e[...].zip	3.45 MB	Interrumpida	bazaar.abuse.ch/download/34e52fcd[...]
786	28/5/2026 22:59	KMSpico-ENFT.rar	4.09 MB	Completa	get-file2.icu/goload.php?b1=KMSpico.zip
788	28/5/2026 23:18	5bf2945c[...].zip	7.87 MB	Completa	bazaar.abuse.ch/download/14a563a9[...]
791	2026-05-28 23:34:04	security_patch.exe.zip	184 bytes	Completa	gooogle.com/security_patch.exe.zip
800	28/5/2026 22:48	eicar_com.zip	184 bytes	Interrumpida	secure.eicar.org/eicar_com.zip
801	1/6/2026 22:48	eicar_com.zip	184 bytes	Completa	secure.eicar.org/eicar_com.zip
802	28/5/2026 22:48	eicar_com2.zip	308 bytes	Completa	secure.eicar.org/eicar_com[2].zip

Nota. Resultados obtenidos con DB Browser for SQL

El análisis del campo **end_time** en los registros con estado *INTERRUMPIDA* reveló que en todos los casos su valor era **0**, lo que indica que Brave no registró una marca temporal de finalización. Esto ocurre porque la descarga fue interrumpida por el sistema de protección del navegador antes de completarse.

4.1.3. Hallazgos en la base de datos Web Data

El análisis de la tabla autofill de la base de datos Web Data mediante la consulta de correlación con *keyword_search_terms* no identificó términos presentes en el autocompletado que estuvieran ausentes del historial de búsquedas — resultado que descarta la hipótesis de borrado parcial del historial durante el período analizado. Los 922 registros de autocompletado son consistentes con la actividad de navegación documentada en History, sin evidencia de manipulación de registros.

4.1.4. Hallazgos en el archivo Preferences

El análisis del archivo Preferences mediante inspección directa del documento JSON con Visual Studio Code permitió extraer los siguientes campos de interés forense:

Tabla 9.

Resultados del análisis del archivo Preferences.

Campo	**Valor encontrado**	**Relevancia forense**
Navegador	Brave — motor Chromium v149.1.91.168	Estructura SQLite idéntica a Chrome — análisis directamente aplicable
savefile.default_directory	[USUARIO]\Downloads	Directorio estándar sin modificación — descarta ocultamiento de descargas
selectfile.last_directory	[USUARIO]\Downloads	Coincide con directorio por defecto — consistencia verificada
safebrowsing.isCurrentlyActive	False	Navegación segura desactivada durante el período analizado
safebrowsing.safeBrowsingStatus	1	Actividad detectada con protección inactiva
settings.force_google_safesearch	False	SafeSearch desactivado — sin filtrado de contenido activo
sync (todos los tipos)	False	Perfil local sin sincronización — artefactos exclusivamente locales
account_info	No vinculada	Sin cuenta externa — descarta alteración por sincronización remota

default_private_search_provider	Brave Search (inactivo)	Motor de búsqueda privada configurado, pero no activo
session_last_active_time	7/6/2026 13:02	Última sesión activa registrada en el perfil
session_number	281	Total, de sesiones registradas — perfil con uso prolongado
sessions.restore_browser	true (type 5)	Restauración automática de sesión activa
notifications content_settings	YouTube (ignore_count: 1)	Sin permisos concedidos a dominios sospechosos
pinned_tabs	No configurado	Sin pestañas fijadas al momento de la adquisición
urls_to_restore_on_startup	No configurado	Sin URLs de inicio predefinidas
web_app_ids	lawinsider.com	Aplicación web instalada sin relevancia forense directa
extensions.last_chrome_version	149.1.91.168	Versión del motor Chromium al momento de la adquisición

Nota. Datos obtenidos mediante el análisis con Visual Studio Code.

El hallazgo más relevante de Preferences en el contexto del análisis forense es la combinación de tres campos: *safebrowsing.isCurrentlyActive: false, force_google_safesearch: false y sessions.restore_browser:* true. La desactivación simultánea de ambos mecanismos de protección del navegador, correlacionada con las búsquedas de "como desactivo antivirus de mi pc" identificadas en *keyword_search_terms*, constituye un patrón de comportamiento coherente con la preparación deliberada del entorno para la descarga y ejecución de contenido potencialmente malicioso.

4.1.5. Línea de tiempo forense integrada

La consulta *UNION ALL* ejecutada sobre la base de datos History permitió construir la línea de tiempo forense integrada que consolida los 74 eventos de interés forense en orden cronológico. La tabla siguiente presenta los eventos más relevantes del período analizado, clasificados por tipo y escenario:

Tabla 10.

Cronología web de incidentes de seguridad.

Fecha y hora	Tipo	Detalle	Escenario
14/3/2026 9:07	Búsqueda	protección contra malware	Contexto previo
14/3/2026 9:07	Búsqueda	protección contra malware Microsoft	Contexto previo
14/4/2026 21:47	Visita	bazaar.abuse.ch	Preparación
17/4/2026 20:00	Búsqueda	Crackmapexec	Contexto técnico
27/5/2026 20:56	Búsqueda	MALWARE BAZZAR	Malware Bazaar
27/5/2026 20:56	Visita	bazaar.abuse.ch	Malware Bazaar
27/5/2026 21:10	Descarga	2f23087f[...].zip — 1,34 MB	Malware Bazaar
27/5/2026 21:11	Descarga	2f4d753e[...].zip — INTERRUMPIDA	Malware Bazaar
28/5/2026 22:56	Búsqueda	kms pico	KMSpico
28/5/2026 22:59	Visita	oficial-kmspico.io	KMSpico
28/5/2026 22:59	Visita	oficial-kmspico.io/download-file	KMSpico
28/5/2026 22:59	Visita	winload1.fin-tech.com	KMSpico
28/5/2026 22:59	Descarga	KMSpico-ENFT.rar — 4,09 MB	KMSpico
28/5/2026 23:08	Visita	bazaar.abuse.ch	Malware Bazaar
28/5/2026 23:18	Visita	bazaar.abuse.ch/download/5bf2945c	Malware Bazaar
28/5/2026 23:18	Descarga	5bf2945c[...].zip — 7,87 MB	Malware Bazaar
28/5/2026 23:23	Búsqueda	Eicar	EICAR

28/5/2026 23:24	Búsqueda	como descargar malwarebytes	Comportamiento
28/5/2026 23:24	Búsqueda	como descargar malware	Comportamiento
28/5/2026 23:25	Búsqueda	como evadir malware	Comportamiento
28/5/2026 23:25	Búsqueda	como ejecutar malware en mi pc y no ser detectado	Comportamiento
28/5/2026 23:26	Búsqueda	infectar mi pc de malware	Comportamiento
28/5/2026 23:27	Búsqueda	como desactivo antivirus de mi pc	Comportamiento
28/5/2026 23:31	Descarga	eicar_com.zip — 184 bytes	EICAR
28/5/2026 23:33	Visita	gooogle.com (TYPED)	Typosquatting
28/5/2026 23:34	Descarga	security_patch.exe.zip — 184 bytes	Typosquatting
1/6/2026 22:48	Descarga	eicar_com.zip — 184 bytes	EICAR
1/6/2026 22:48	Descarga	eicar_com2.zip — 308 bytes	EICAR

Nota. Eventos relevantes de la línea de tiempo forense: 79 días analizados.

Resultados de la validación cruzada

Los resultados obtenidos mediante las cuatro herramientas de validación fueron contrastados sistemáticamente con los del análisis manual en DB Browser for SQLite, adoptado como fuente de verdad metodológica por ser el método que accede directamente a los datos sin capas de interpretación intermedia. La comparativa permitió identificar tanto coincidencias que refuerzan la fiabilidad de los hallazgos como divergencias que aportan información complementaria no disponible mediante análisis SQL directo.

4.1.6. Hindsight

Hindsight procesó correctamente los tres artefactos del alcance e identifico los siguientes tipos y volúmenes de registros:

Tabla 11.

Resultados del análisis con Hindsight.

Tipo de registro	**Total**	**Nota.**
url	7.365	History SQLite + LevelDB
Download	964	History SQLite
site setting (modified)	941	Preferences
Autofill	922	Web Data SQLite
site setting (engagement)	63	Preferences
preference	20	Preferences
Sesión	19	Preferences
permission action	19	Preferences
site setting (zoom level)	8	Preferences

Nota. Resultados del análisis de los tres artefactos con Hindsight.

El registro de tipo profile creation confirmó que el perfil de Brave fue creado el **2025-03-29 23:49:37**, estableciendo el límite temporal mínimo del historial analizado.

Hindsight identificó correctamente los cuatro escenarios del análisis. Los hallazgos adicionales respecto al análisis manual se detallan a continuación:

Tabla 12.

Incidentes de seguridad mediante Hindsight.

Descarga	**Estado**	**Danger Type**	**Interrupt Reason**
eicar_com.zip	INTERRUMPIDA	Not Dangerous	Virus

eicar_com.zip	INTERRUMPIDA	Not Dangerous	Virus
2f4d753e[...].zip	INTERRUMPIDA	Not Dangerous	Virus
KMSpico-ENFT.rar	COMPLETA	Not Dangerous	No Interrupt
5bf2945c[...].zip	COMPLETA	Not Dangerous	No Interrupt
security_patch.exe.zip	COMPLETA	Not Dangerous	No Interrupt

Nota. Resumen de descargas maliciosas detectadas por Hindsight.

El campo Interrupt Reason con valor Virus en las descargas interrumpidas confirma que fueron el sistema de protección del equipo — y no el navegador directamente — el que interceptó las descargas. El valor Not Dangerous en Danger Type indica que el navegador no clasificó los archivos como peligrosos per se, sino que la interrupción fue producida por el antivirus del sistema operativo de forma externa al navegador.

Segunda descarga cancelada de KMSpico:

Hindsight identificó un registro no detectado en el análisis manual:

Tabla 13.

Descarga de KMS pico no identificada por DB Browser SQLite.

Fecha y Hora	URL	Estado	Bytes
2026-05-28 23:00:02	get-file2.icu/goload.php?b1=KMSpico.zip	Cancelada	0 bytes

Nota. Descarga no identificada por el análisis manual pero identificada por Hindsight.

Este registro indica que inmediatamente después de completarse la descarga de *KMSpico-ENFT.rar* se inició una segunda descarga desde el mismo dominio que fue cancelada con 0 bytes transferidos — comportamiento consistente con mecanismos de descarga automática secundaria propios de sitios de distribución de software no oficial.

braveShieldsMetadata extraído de Preferences:

Hindsight extrajo automáticamente los tokens de protección de fingerprinting generados por Brave para cada dominio sospechoso visitado, corroborando las visitas documentadas en History:

Tabla 14.

Tokens de BraveshieldsMetadata con Hindsight.

Dominio	Timestamp (UTC-5)	Farbling Token
oficial-kmspico.io	28/5/2026 22:59	E8CA95DB852F367A...
fin-tech.com	28/5/2026 22:59	D3C2C93A22FD886D...
get-file2.icu	28/5/2026 22:59	2D3DD587FBA47D17...
eicar.org	28/5/2026 23:23	5E4B686503DAA578...
gooogle.com	28/5/2026 23:33	3A77819CEA25A734...

Nota. El farbling token es generado automáticamente por Brave Shields

Site engagement scores:

Tabla 15.

Calificación de sitio mediante site_engagement.

Dominio	rawScore	Interpretación
eicar.org	10,25	Mayor frecuencia de interacción
bazaar.abuse.ch	9,26	Alta frecuencia de interacción
gooogle.com	3,6	Interacción puntual — una sesión

Nota. Los site engagement scores son calculados automáticamente por el motor Chromium para cada dominio visitado en función de la frecuencia e intensidad de interacción del usuario, almacenados en el archivo Preferences.

Divergencia de zona horaria:

Hindsight aplicó la zona horaria Central [-6/-5] — la más próxima disponible a Ecuador UTC-5 — pudiendo existir una diferencia de hasta una hora en los timestamps respecto al análisis manual durante períodos de horario de verano estadounidense. Los timestamps del análisis manual aplican UTC-5 fijo y son más precisos para el contexto geográfico del análisis.

4.1.7. ChromeHistoryView

ChromeHistoryView cargó 7.365 registros — coincidencia exacta con el total de visitas identificado en DB Browser. Los Visit IDs, timestamps y URLs coincidieron en su totalidad con los resultados del análisis manual, confirmando la consistencia de los datos entre métodos.

La herramienta identificó correctamente los cuatro escenarios del análisis. Su principal aporte diferencial respecto al análisis manual es la columna Referrer visible directamente sin necesidad de consultas JOIN, permitiendo verificar de forma inmediata la cadena de navegación desde Google hasta cada descarga.

Tabla 16.

Resultados de ChromeHistoryView.

Record ID	URL	Referrer	Visit Type
33432	google.com/search?q=MALWARE+BAZZAR	—	Generated
33433	bazaar.abuse.ch/	google.com/search?q=MALWARE+BAZZAR	Link
33557	bazaar.abuse.ch/download/5bf2945c[...]	bazaar.abuse.ch/browse/	Link
33514	google.com/search?q=kms+pico	—	Generated
33532	oficial-kmspico.io/	google.com/search?q=kms+pico	Link
33533	oficial-kmspico.io/download-file/[...]	—	Link
33534	winload1.fin-tech.com/?b1=KMSpico.zip	—	Link
33561	google.com/search?q=eicar	—	Generated
33562	eicar.org/download-anti-malware-testfile/	google.com/search?q=eicar	Link

33574	http://gooogle.com/	—	Typed
33575	https://gooogle.com/	http://gooogle.com/	Typed
33576	http://gooogle.com/	https://gooogle.com/	Typed

Nota. El campo Referrer identifica la URL de origen desde la cual se accedió a cada sitio.

La tabla confirma visualmente la cadena de navegación completa desde la búsqueda en Google hasta el dominio de descarga en cada escenario — verificación que en el análisis manual requirió consultas JOIN entre las tablas visits y urls.

Adicionalmente la herramienta decodifica el campo transition en formato legible — Link, Form Submit, Typed, Reload, Generated — sin requerir la expresión CASE del análisis manual, y permitió detectar visualmente dos duraciones anómalas: el registro 33466 de MalwareBazaar (25:53:46) y el registro 33737 de EICAR (24:28:29), confirmando la limitación interpretativa del campo visit_duration documentada en la sección 4.4.3.

ChromeHistoryView no accede a las tablas downloads ni downloads_url_chains — limitación que impidió identificar el dominio de entrega final get-file2.icu del escenario KMSpico, visible únicamente mediante el análisis manual en DB Browser. El navegador fue identificado como Chrome en lugar de Brave, confirmando que las herramientas basadas en lectura directa del SQLite de Chromium no distinguen entre navegadores que comparten el mismo motor.

4.1.8. BrowsingHistoryView

BrowsingHistoryView extrajo 7.365 registros — coincidencia exacta con DB Browser y ChromeHistoryView. Los Visit IDs, timestamps, URLs, referrers y duraciones coincidieron en su totalidad con los resultados de ChromeHistoryView, confirmando la consistencia total entre ambas herramientas sobre la misma fuente de datos SQLite.

La herramienta identificó correctamente los cuatro escenarios del análisis con resultados idénticos a ChromeHistoryView. Su elemento diferenciador más relevante es la columna Typed Count, que confirma de forma explícita y cuantificada qué dominios fueron introducidos manualmente en la barra de direcciones:

Tabla 17.

Resultados Typed Count mediante BrowsingHistoryView

Record ID	URL	Visit Type	Typed Count	Interpretación forense
33433	bazaar.abuse.ch/	Link	0	Acceso mediante clic desde búsqueda en Google
33454	bazaar.abuse.ch/	Form Submit	0	Acceso mediante envío de formulario anti-bot
33455	bazaar.abuse.ch/browse/	Link	0	Navegación interna mediante clic
33456	bazaar.abuse.ch/download/2f23087f[...]	Link	0	Acceso a página de sample mediante clic
33557	bazaar.abuse.ch/download/5bf2945c[...]	Link	0	Acceso a página de sample mediante clic
33561	google.com/search?q=eicar	Generated	0	Búsqueda desde omnibox — no escritura directa del dominio

33562	eicar.org/download-anti-malware-testfile/	Link	0	Acceso mediante clic desde búsqueda en Google
33570	secure.eicar.org/eicar.com.txt	Link	0	Acceso mediante clic en enlace
33574	http://gooogle.com/	Typed URL	0	Acceso por redirección — no escrito directamente
33575	https://gooogle.com/	Typed URL	**1**	**Dominio escrito manualmente una vez**
33576	http://gooogle.com/	Typed URL	0	Redirección de servidor HTTP→HTTPS
33532	oficial-kmspico.io/	Link	0	Acceso mediante clic en resultado de búsqueda
33533	oficial-kmspico.io/download-file/[...]	Link	0	Acceso mediante clic en enlace
33534	winload1.fin-tech.com/?b1=KMSpico.zip	Link	0	Redirección automática

Nota. Visit Type indica el mecanismo de acceso a la URL.

El Typed Count = 1 en el registro 33575 confirma de forma independiente y cuantificada que gooogle.com fue introducido manualmente en la barra de direcciones exactamente una vez — corroborando el indicador técnico de typosquatting identificado en el análisis manual mediante el campo transition type TYPED. Los valores Typed Count = 0 en

los registros 33574 y 33576 confirman que las redirecciones posteriores no fueron iniciadas por el usuario.

La nomenclatura "Typed URL" en lugar de "Typed" para el tipo de transición es más descriptiva e inmediatamente interpretable que la de ChromeHistoryView, facilitando la identificación del mecanismo de acceso directo al dominio sin necesidad de interpretación adicional.

Al igual que ChromeHistoryView, BrowsingHistoryView no accede a las tablas downloads ni downloads_url_chains, y el navegador fue identificado como Chrome en lugar de Brave. Su ventaja diferencial en escenarios reales es su capacidad multi-navegador — en un caso con múltiples navegadores instalados permitiría consolidar el historial completo en una única vista sin analizar cada perfil por separado.

4.1.9. Autopsy

Autopsy no extrajo Web History, Web Downloads ni Web Search mediante el módulo Recent Activity al operar sobre artefactos individuales extraídos en lugar de una imagen forense completa del disco. Esta limitación determinó que los resultados de Autopsy sean complementarios y no directamente comparables con los de las herramientas anteriores en términos de reconstrucción cronológica de la actividad web.

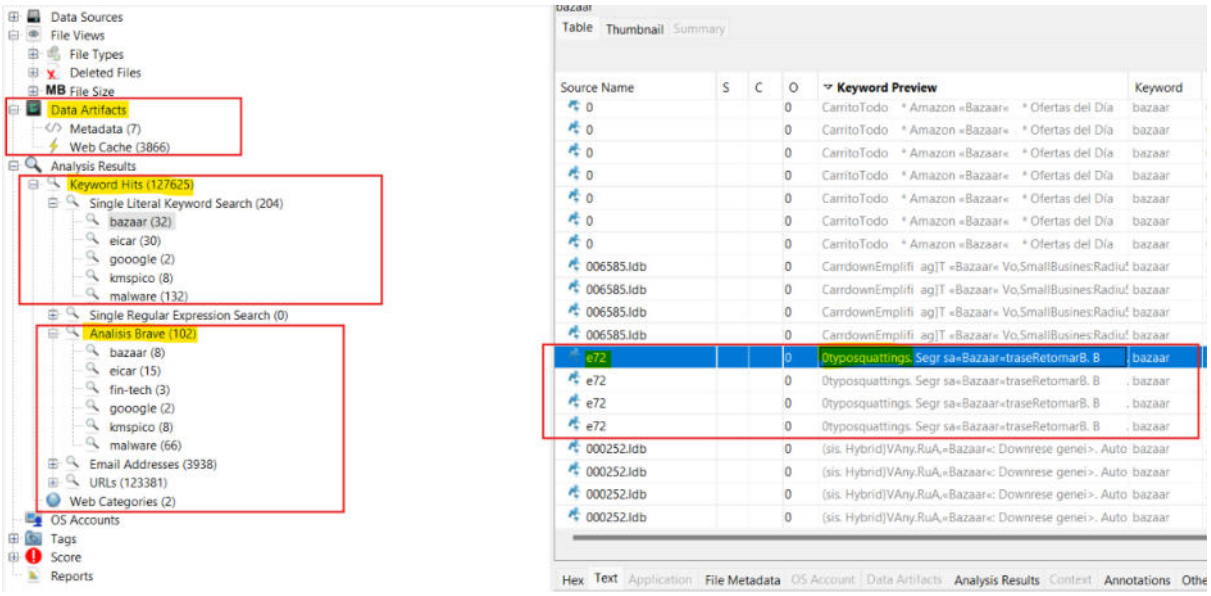
Autopsy aportó tres elementos no disponibles en las herramientas anteriores:

Web Cache (3.866 registros):

Autopsy extrajo el caché del navegador como artefacto complementario no analizado por ninguna otra herramienta. La presencia de recursos en caché de los dominios de los escenarios corrobora de forma independiente las visitas documentadas en History, constituyendo evidencia indirecta de la navegación hacia esos dominios.

Figura 42

Resultados con la herramienta forense Autopsy



Nota. Resultados de los Keyword Lists configurados.

Keyword Hits (127.625 coincidencias):

La búsqueda de palabras clave en el conjunto completo de artefactos del perfil identificó coincidencias en archivos binarios y de configuración no analizables mediante SQL. Los resultados por lista configurada fueron:

Tabla 18.

Resultados con Autopsy.

Lista	Total hits	Términos relevantes
Single Literal Search	204	bazaar (32), eicar (30), malware (132), kmspico (8), gooogle (2)
analisis_brave	102	malware (66), eicar (15), bazaar (8), kmspico (8), fin-tech (3), gooogle (2)

Email Addresses	3.938	h4xxxxxt@gmail.com, kxxxx.sxxxxxxa@u-----a.com.ec, prxxxxgroup.in
URLs	123.381	URLs identificadas en todos los artefactos del perfil

Nota. Resultados de la configuración de Keyword Lists en el módulo Ingest.

El hallazgo más significativo de la búsqueda de palabras clave fue el archivo **e72**, identificado con score **Likely Notable**, que contiene referencias simultáneas a los términos bazaar, gooogle, kmspico, eicar, fin-tech y malware en un único archivo binario del perfil — confirmando que los cinco escenarios dejaron rastros en fuentes no-SQLite del navegador más allá del archivo History.

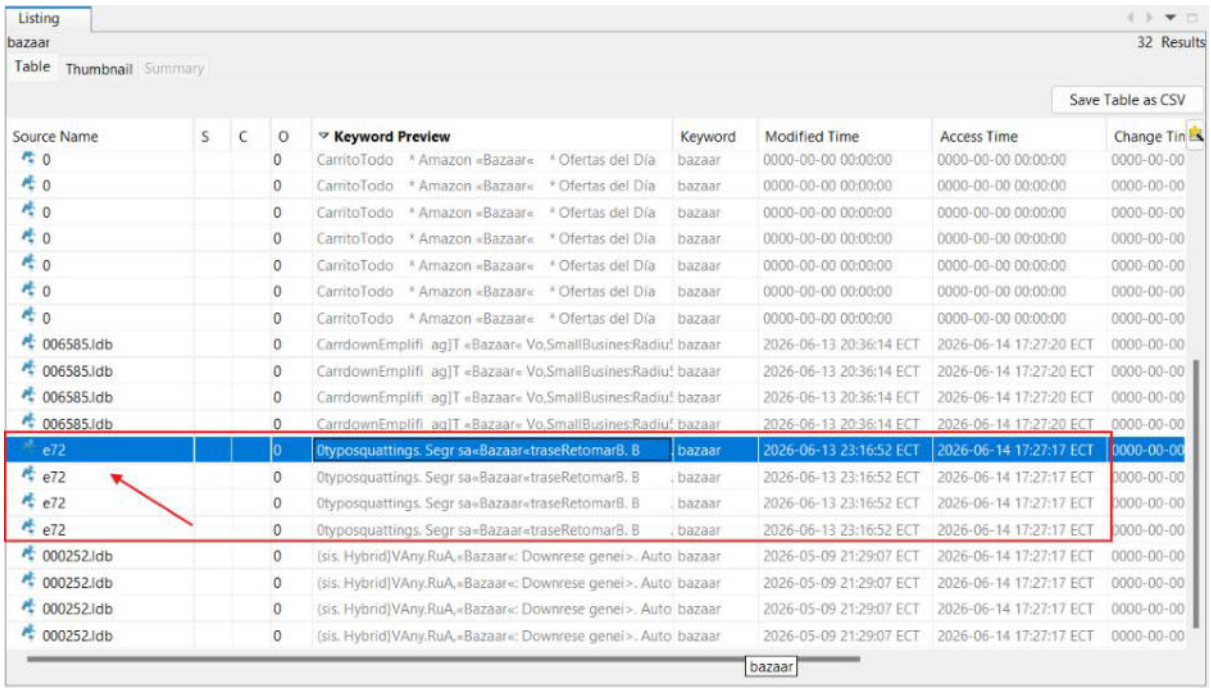
Los Email Addresses identificados incluyen tres direcciones que requieren anonimización antes de cualquier presentación pública del análisis: la cuenta personal del investigador, un correo corporativo y el dominio del remitente del correo de phishing analizado durante el período de investigación.

Informe forense estructurado:

Autopsy generó un informe forense en formato HTML con todos los hallazgos numerados, marcas temporales de ingestión y estructura de caso forense — formato estándar en procesos periciales formales que ninguna de las herramientas anteriores produce de forma nativa. Este informe se incluye como Apéndice C del presente trabajo.

Figura 43

Resultados de los incidentes de seguridad mediante Autopsy



Nota. Autopsy confirma los 5 incidentes detectados por otras herramientas.

4.1.10. Comparativa de herramientas

La siguiente tabla sintetiza los resultados y capacidades de los cinco métodos de análisis aplicados:

Tabla 19.

Comparativa de resultados mediante herramientas forenses.

Elemento	DB Browser SQL	Hindsight	Chrome History View	Browsing History View	Autopsy
Total visitas	7.365	7.365	7.365	7.365	N/A
Total URLs únicas	3.886	—	—	—	—
Total descargas	606	964	—	—	—

Búsquedas identificadas	394	465	—	—	—
Web Cache	—	—	—	—	3.866
Visit IDs coincidentes	✓	✓	✓	✓	N/A
Cadena KMSpico	Completa	Completa	Parcial	Parcial	—
Danger Type descargas	—	✓	—	—	—
Interrupt Reason	—	✓	—	—	—
braveShieldsMetadata	—	✓	—	—	—
Referrer directo	Requiere JOIN	—	✓	✓	—
Typed URL gooogle.com	✓	✓	✓	✓	—
Keyword Search	SQL	—	✓	✓	✓
Informe forense	—	—	—	—	✓
Acceso a Preferences	Manual	✓ Automático	—	—	Parcial
Zona horaria	UTC-5 exacto	Central [-6/-5]	Sistema local	Sistema local	Sistema local
Navegador identificado	N/A	Chromium	Chrome	Chrome	Chrome
Fuentes adicionales	Solo SQLite	SQLite+LevelDB	Solo SQLite	Solo SQLite	SQLite+Caché

Nota. Todas las herramientas coinciden en 7.365 visitas.

La coincidencia exacta en el número de visitas entre DB Browser, Hindsight, ChromeHistoryView y BrowsingHistoryView confirma la integridad de los artefactos y la consistencia de los resultados entre métodos independientes. Las diferencias identificadas son de capacidad y no de precisión — el análisis manual mediante SQL es el método más preciso para el control de zona horaria y para consultas de correlación entre tablas, mientras que Hindsight supera a todos los demás métodos en profundidad de análisis al acceder a fuentes no-SQLite y extraer automáticamente información de Preferences estructurada como eventos en la línea de tiempo.

4.2. Análisis por escenario forense

Los cuatro escenarios identificados durante el análisis forense se presentan a continuación de forma individualizada, integrando los hallazgos obtenidos mediante el análisis manual en DB Browser for SQLite y los resultados de las herramientas de validación cruzada. Para cada escenario se reconstruye la cadena completa de eventos desde la búsqueda inicial hasta la descarga, mediante la correlación de los campos *visit_id, from_visit, transition type, visit_duration y referrer.*

4.2.1. Escenario 1 — Hallazgo no planificado: descarga de KMSpico

KMSpico es una herramienta de activación ilegal de licencias de Windows frecuentemente distribuida por actores maliciosos como vector de entrega de malware. El escenario fue identificado durante el análisis del historial de navegación real sin haber sido planificado previamente, constituyendo el hallazgo forense de mayor valor del análisis por documentar una cadena de navegación completa desde la búsqueda inicial hasta la descarga final a través de múltiples redirecciones.

Línea de tiempo forense — desde búsqueda hasta descarga (28/05/2026):

Tabla 20.

Resultado cadena de navegación descarga de KMSpico.

Paso	Hora	Tipo	URL	Referrer	Transition	Visit ID	Duración
1	22:56:58	BÚSQUEDA	google.com/search?q=kms+pico	—	Generated	33514	109,23 s
2	22:58:48	VISITA	learn.microsoft.com/[...]/kms-pico	google.com/search?q=kms+pico	Link	33530	33,91 s
3	22:59:22	BÚSQUEDA	google.com/search?q=kms+pico	google.com/search?q=kms+pico	Generated	33531	1,54 s
4	22:59:23	VISITA	oficial-kmspico.io	google.com/search?q=kms+pico	Link	33532	136,08 s
5	22:59:28	VISITA	oficial-kmspico.io/download-file/[...]	—	Link	33533	132,39 s
6	22:59:34	REDIRECCIÓN	winload1.fin-tech.com/?b1=KMSpico.zip	—	Link	33534	45,18 s

7	22:59:50	DESCARGA	get-file2.icu/golo ad.php?b1=K MSpico.zip	—	—	Downl oad 786	—
8	23:00:02	DESCARGA CANCELAD A	get-file2.icu/golo ad.php?b1=K MSpico.zip	—	—	—	—

Nota. KMSpico fue un hallazgo no planeado del análisis forense.

Análisis de la cadena:

La cadena reconstruida documenta ocho eventos en 3 minutos y 4 segundos. El Paso 2 — visita a Microsoft Q&A consultando sobre KMSpico — es un indicador de comportamiento relevante: el usuario investigó la legitimidad del software antes de proceder a su descarga, permaneciendo 33 segundos en la página. El Paso 3 muestra el retorno a los resultados de búsqueda con una duración de apenas 1,54 segundos — tiempo consistente con un usuario que revisó brevemente los resultados y seleccionó directamente el enlace de descarga.

Los registros 33533 y 33534 presentan from_visit = 0 pese a pertenecer a la cadena activa — comportamiento producido por redirecciones automáticas del servidor que Brave no pudo encadenar explícitamente. La correlación temporal y el referrer visible en ChromeHistoryView confirman su pertenencia a la cadena.

El dominio de entrega final get-file2.icu aparece exclusivamente en la tabla downloads_url_chains — no en visits — demostrando que el usuario nunca visitó ese dominio de forma explícita, sino que fue el servidor de winload1.fin-tech.com quien realizó la redirección HTTP hacia la descarga de forma automática. Hindsight identificó

adicionalmente una segunda descarga cancelada (Paso 8) desde el mismo dominio get-file2.icu con 0 bytes transferidos inmediatamente después de la descarga completada, comportamiento consistente con mecanismos de descarga automática secundaria propios de sitios de distribución de software no oficial.

4.2.2. Escenario 2 — Descarga de muestras desde Malware Bazaar y EICAR

Malware Bazaar — Sesión 1 (27/05/2026):

Tabla 21.

Cadena de navegación primera descarga Malware Bazaar.

Paso	Hora	Tipo	URL	Referrer	Transition	Visit ID	Duración
1	20:56:16	BÚSQUEDA	google.com/search?q=MALWARE+BAZZAR	—	Generated	33432	2,65 s
2	20:56:19	VISITA	bazaar.abuse.ch	google.com/search?q=MALWARE+BAZZAR	Link	33433	2,36 s
3	20:56:21	VERIFICACIÓN	bazaar.abuse.ch/browse	bazaar.abuse.ch	Link	33434	—
4	20:56:21	VERIFICACIÓN	bazaar.abuse.ch/verify-ua	bazaar.abuse.ch/browse	Link	33435	753,58 s
5	21:09:00	RELOAD	bazaar.abuse.ch/verify-ua	—	Reload	33438	16,05 s
6	21:09:17	ACCESO	bazaar.abuse.ch	bazaar.abuse.ch/verify-ua	Form Submit	33454	71,87 s
7	21:10:28	NAVEGACIÓN	bazaar.abuse.ch/browse	bazaar.abuse.ch	Link	33455	18,08 s

8	21:10:46	PÁGINA SAMPLE	bazaar.abuse.ch /download/2f23 087f[...]	bazaar.abuse.ch/ browse	Link	3345 6	14,19 s
9	21:10:49	**DESCARGA**	bazaar.abuse.ch /download/0aea cbe9[...]	—	—	Dow nload 783	—
10	21:11:04	PÁGINA SAMPLE	bazaar.abuse.ch /download/2f4d 753e[...]	bazaar.abuse.ch/ browse	Link	3345 8	25,65 s
11	21:11:07	**DESCARGA INTERRUMPI DA**	bazaar.abuse.ch /download/34e5 2fcd[...]	—	—	Dow nload 784	—

Nota. Línea de tiempo completa para la primera descarga de Malware.

Análisis de la cadena Malware Bazaar:

El sistema anti-bot de Malware Bazaar implementa una verificación de browser mediante la URL /verify-ua que genera un patrón técnico característico en los artefactos de Brave — la secuencia /browse → /verify-ua → Form Submit → /browse es reproducible en ambas sesiones y constituye un indicador forense identificable del acceso al repositorio. La duración de 753,58 segundos en el registro 33435 (Paso 4, Sesión 1) refleja el tiempo de espera durante la verificación anti-bot, no el tiempo efectivo de interacción del usuario con el contenido.

En la Sesión 1 se identificaron dos descargas: la primera completada (Download 783, 1,34 MB) y la segunda interrumpida por el antivirus del sistema (Download 784, Interrupt Reason: Virus según Hindsight). En la Sesión 2 se completó exitosamente la descarga de la muestra principal (Download 788, 7,87 MB) con hash SHA-256 5bf2945ceaaac681fad1b9b999c6620ce8393f919179ce6ca0fef5b411e984e5 verificable públicamente en la base de datos de MalwareBazaar.

La URL de entrega final de Download 788 (bazaar.abuse.ch/download/14a563a9[...]) es diferente a la URL de la página del sample visitada en el Paso 5 (bazaar.abuse.ch/download/5bf2945c[...]) — distinción solo observable mediante la correlación entre la tabla visits y la tabla downloads_url_chains, confirmando el valor metodológico del análisis conjunto de ambas tablas.

EICAR — Sesión 1 (28/05/2026) y Sesión 2 (01/06/2026):

Tabla 22.

Registro segunda descarga desde EICAR.

Paso	Hora	Tipo	URL	Referrer	Transition	Visit ID / Download ID	Estado
1	23:23:45	BÚSQUEDA	google.com/search?q=eicar	—	Generated	33561	—
2	23:23:52	VISITA	eicar.org/download/download-anti-malware-testfile	google.com/search?q=eicar	Link	33562	—
3	23:27:42	VISITA	secure.eicar.org/eicar.com.txt	—	Link	33570	—
4	23:27:59	**DESCARGA INTERRUMPIDA**	secure.eicar.org/eicar_com.zip	—	—	Download 789	Virus
5	23:28:20	VISITA	secure.eicar.org/eicar.com.txt	—	Link	33571	—
6	23:31:18	**DESCARGA COMPLETA**	secure.eicar.org/eicar_com.zip	—	—	Download 790	No Interrupt
7	22:44:27	BÚSQUEDA	google.com/search?q=eicar+tes	—	Generated	33722	—

			t+file+downloa d				
8	22:44: 34	VISITA	eicar.org/downl oad-anti- malware- testfile	google.com/searc h?q=eicar+test+fi le+download	Link	33723	—
9	22:47: 47	VISITA	eicar.org/downl oad-anti- malware- testfile	eicar.org/#about	Link	33737	—
10	22:48: 12	**DESCARGA INTERRUM PIDA**	secure.eicar.org /eicar_com.zip	—	—	Download 800	Virus
11	22:48: 49	**DESCARGA COMPLETA**	secure.eicar.org /eicar_com.zip	—	—	Download 801	No Interru pt
12	22:48: 56	**DESCARGA COMPLETA**	secure.eicar.org /eicar_com2.zip	—	—	Download 802	No Interru pt

Nota. Línea de tiempo forense para la descarga del archivo EICAR

Análisis de la cadena EICAR:

El patrón INTERRUMPIDA → COMPLETA se repite en ambas sesiones con una consistencia que constituye en sí misma un hallazgo forense. En la Sesión 1 el primer intento (Download 789) fue bloqueado por el antivirus (Interrupt Reason: Virus). Tras visitar nuevamente la página de descarga (Paso 5, visita 33571) el usuario completó la descarga exitosamente (Download 790). La Sesión 2 replica exactamente el mismo patrón (Pasos 10 y 11), añadiendo una tercera descarga del archivo eicar_com2.zip (Download 802).

El campo Danger Type identificado por Hindsight en ambas descargas interrumpidas muestra el valor Not Dangerous — indicando que el navegador no clasificó el archivo como

peligroso, sino que fue el antivirus del sistema operativo quien interceptó la descarga de forma externa al navegador. Esta distinción es forense¬mente relevante porque demuestra que los campos state e interrupt_reason de la tabla downloads registran el resultado de la intervención del antivirus del sistema, no la evaluación de seguridad del propio navegador.

4.2.3. Escenario 3 — Typosquatting simulado: gooogle.com

El escenario de typosquatting fue diseñado para generar en los artefactos de Brave los indicadores técnicos característicos de un ataque de typosquatting mediante un entorno de servidor local controlado.

Línea de tiempo forense — desde acceso al dominio hasta descarga:

Tabla 23.

Cadena de navegación descarga de security_patch.exe.zip.

Paso	Hora	Tipo	URL	Referrer	Transition	Visit ID	Typed Count	Duración
1	23:33:51	ACCESO DIRECTO	http://gooogle.com/	—	Typed	33574	0	0,00 s
2	23:33:51	REDIRECCIÓN HTTP→HTTPS	https://gooogle.com/	http://gooogle.com/	Typed	33575	1	0,00 s
3	23:33:51	REDIRECCIÓN SERVER	http://gooogle.com/	https://gooogle.com/	Typed	33576	0	84,63 s

4	23:34:04	**DESCARGA**	gooogle.com/security_patch.exe.zip	—	—	Download 791	—	—

Nota. Línea de tiempo forense para el escenario Typosquatting.

Análisis de la cadena:

Los tres registros de visita presentan timestamp idéntico (23:33:51) generado por el mecanismo de redirección automática HTTP→HTTPS del servidor local configurado en el entorno de simulación. Los valores de visit_duration iguales a 0 en los registros 33574 y 33575 reflejan la velocidad de la redirección automática del servidor — no un mecanismo de pre-fetching del navegador — distinción determinada por la correlación con el transition type TYPED y el Typed Count = 1 en el registro 33575.

La combinación de transition type TYPED con Typed Count = 1 en el registro 33575 constituye el indicador técnico forense más significativo del escenario: confirma que el dominio gooogle.com fue introducido manualmente en la barra de direcciones — patrón característico del typosquatting donde el usuario accede al dominio fraudulento por error tipográfico sin pasar por ningún referrer previo (from_visit = 0 en el registro 33574).

Hindsight aportó un registro adicional de Preferences no visible en el análisis manual: el campo http_allowed generado para gooogle.com:443 a las 23:34:04, indicando que Brave solicitó confirmación al usuario para continuar la conexión al dominio sin certificado HTTPS válido. Este registro en Preferences corrobora de forma independiente la visita al dominio y la interacción consciente del usuario con la advertencia de seguridad del navegador, constituyendo evidencia corroborante del acceso manual al dominio typosquatting.

4.2.4. Indicadores de comportamiento sospechoso

Durante el análisis de la tabla keyword_search_terms se identificó una secuencia de búsquedas que documenta la progresión de comportamiento del usuario a lo largo del período analizado, con especial relevancia en la sesión del 28 de mayo de 2026:

Contexto previo al incidente principal:

Tabla 24.

Indicadores de comportamiento sospechoso previo al incidente.

Fecha y hora (UTC-5)	Término buscado	Transition	Visit ID
14/3/2026 9:07	protección contra malware	Form Submit	26887
14/3/2026 9:07	protección contra malware Microsoft	Form Submit	26888
17/4/2026 20:00	Crackmapexec	Generated	29653
18/4/2026 8:27	Crackmapexec	Generated	29670
27/5/2026 20:56	MALWARE BAZZAR	Generated	33432

Nota. Análisis mediante DB Browser for SQL y validación cruzada.

Sesión del incidente — 28/05/2026:

Tabla 25.

Indicadores de comportamiento sospechoso día del incidente.

Hora (UTC-5)	Término buscado	Transition	Visit ID
22:56:58	kms pico	Generated	33514
22:59:22	kms pico	Generated	33531
23:23:45	eicar	Generated	33561
23:24:03	como descargar malwarebytes	Generated	33563
23:24:11	como descargar malware	Generated	33564

23:25:16	como evadir malware	Form Submit	33565
23:25:37	como ejecutar malware en mi pc y no ser detectado	Form Submit	33566
23:26:31	infectar mi pc de malware	Form Submit	33567

Nota. Análisis mediante DB Browser for SQL y validación cruzada.

Sesión posterior — 28/05/2026:

Tabla 26.

Indicadores de comportamiento sospechoso posterior al incidente

Fecha y hora (UTC-5)	Término buscado	Transition	Visit ID
1/6/2026 22:44	eicar test file download	Generated	33722

Nota. Análisis mediante DB Browser for SQL y validación cruzada.

Análisis de los indicadores:

La progresión de los términos de búsqueda entre las 23:24:03 y las 23:27:03 del 28 de mayo — un intervalo de 3 minutos — documenta una escalada desde la búsqueda de herramientas defensivas (malwarebytes) hasta la búsqueda de técnicas de evasión y desactivación de protecciones. El cambio en el transition type — de Generated (búsquedas desde la omnibox) a Form Submit (búsquedas realizadas directamente desde el campo de búsqueda de Google) — indica una interacción más deliberada con el motor de búsqueda en los términos más comprometedores.

Las búsquedas del contexto previo (marzo-abril 2026) establecen que el usuario tenía conocimiento técnico de herramientas de seguridad ofensiva como CrackMapExec semanas antes del incidente principal. Esta cronología completa de 79 días, desde las primeras

búsquedas defensivas en marzo hasta las descargas del 28 de mayo, constituye el marco temporal del análisis y aporta contexto comportamental que enriquece la interpretación forense de los hallazgos.

Es importante señalar que las búsquedas de la sesión del 28 de mayo relacionadas con técnicas de evasión ocurrieron después de las descargas documentadas — no antes — por lo que constituyen evidencia indiciaria de comportamiento posterior al incidente y no indicadores de intención previa.

4.3. Evaluación del alcance probatorio

La evaluación del alcance probatorio constituye el elemento diferenciador del presente análisis respecto a un volcado descriptivo de registros, y representa la contribución metodológica central del trabajo. Su propósito es determinar con precisión qué hechos pueden acreditarse de forma directa a partir de los artefactos analizados, cuáles solo pueden inferirse de forma indiciaria, y qué limitaciones técnicas condicionan la interpretación de los registros recuperados.

4.3.1. Evidencia directa identificada

La evidencia directa comprende los artefactos que acreditan hechos sin necesidad de inferencias intermedias. Los siguientes elementos fueron identificados como evidencia directa en el presente análisis:

Tabla 27.

Resultados evidencias directas identificadas.

Artefacto	Tabla / Fuente	Hecho acreditado directamente
Download ID 786	downloads + downloads_url_chains	Descarga completada del archivo KMSpico-ENFT.rar desde get-file2.icu el 28/05/2026 a las 22:59:50 UTC-5 — 4,09 MB transferidos íntegramente

Download ID 788	Downloads	Descarga completada de muestra de malware con hash SHA-256 5bf2945c[...] desde bazaar.abuse.ch el 28/05/2026 a las 23:18:33 UTC-5 — verificable públicamente
Download ID 791	Downloads	Descarga completada del archivo security_patch.exe.zip desde gooogle.com el 28/05/2026 a las 23:34:04 UTC-5
Downloads 790, 801, 802	Downloads	Descargas completadas de archivos EICAR desde secure.eicar.org en dos sesiones
Visit ID 33575	visits + urls	Acceso con Typed Count = 1 al dominio gooogle.com — introducción manual del dominio confirmada por las tres herramientas de validación
Visits 33514 y 33531	keyword_search_terms	Búsqueda del término "kms pico" en dos ocasiones el 28/05/2026 antes de la descarga de KMSpico
braveShieldsMetadata	Preferences	Visita confirmada de forma independiente a oficial-kmspico.io, fin-tech.com, get-file2.icu, eicar.org y gooogle.com mediante tokens de protección generados automáticamente por el navegador en el momento de cada visita
http_allowed gooogle.com	Preferences	Concesión explícita de permiso por parte del usuario para continuar la conexión al dominio gooogle.com sin certificado HTTPS válido el 28/05/2026 a las 23:34:04
Hashes SHA-256	FTK Imager	Integridad de los artefactos adquiridos verificada — las copias forenses son idénticas a los originales

Nota. Los artefactos del navegador acreditan la descarga de archivos, pero no su ejecución posterior, constituyendo esta su principal limitación como evidencia directa.

4.3.2. Evidencia indiciaria identificada

La evidencia indiciaria comprende los artefactos que requieren una inferencia para conectar el registro con el hecho que se pretende acreditar.

Para seleccionar un artefacto se consideró evidencia indiciaria cuando:

- El artefacto no acreditaba por sí solo que el usuario hubiera realizado una acción específica (por ejemplo, descargar deliberadamente malware).
- Era necesario analizar el contexto para relacionarlo con el caso.
- Debía ser confirmado con otras evidencias digitales. Su valor probatorio dependía de la correlación con otras evidencias (History, Downloads, Preferences, Cookies, Web Cache, etc.).
- Los registros analizados podían tener más de una interpretación técnicamente válida, por lo que no era concluyente de forma aislada.
- El artefacto mostraba consistencia con la hipótesis investigada, pero no permitía demostrar por sí mismo la causa o la intención del usuario.

En el presente análisis se identificaron los siguientes elementos de evidencia indiciaria:

Tabla 28.

Resultados de evidencias indiciarias identificadas.

Artefacto	Tabla / Fuente	Inferencia	Limitación
Visits 33532-33534	visits	La cadena de navegación sugiere intención deliberada de descarga de KMSpico	El from_visit = 0 en 33533 y 33534 impide verificar el encadenamiento explícito mediante el campo from_visit — requiere correlación temporal
Visit 33530	visits	La consulta a Microsoft Q&A sobre KMSpico sugiere que el usuario investigó la legitimidad	No acredita directamente la intención de descarga posterior

		del software antes de descargarlo	
Búsquedas 23:24-23:27	keyword_search_terms	La secuencia de búsquedas sobre evasión de malware y desactivación del antivirus sugiere exploración deliberada de técnicas de evasión de controles de seguridad	Ocurrieron después de las descargas — no acreditan intención previa al incidente
Búsquedas crackmapexec (abril 2026)	keyword_search_terms	Las búsquedas de herramientas de pentesting un mes antes del incidente sugieren conocimiento técnico previo en seguridad ofensiva	No existe relación causal verificable entre esas búsquedas y los eventos del 28 de mayo
safebrowsing.isCurrentlyActive: false	Preferences	La desactivación de SafeBrowsing es coherente con la preparación del entorno para descargas de contenido potencialmente malicioso	No acredita directamente que la desactivación fuera deliberada para facilitar las descargas — puede corresponder a una configuración previa no relacionada
Site engagement scores	Preferences	Los scores de bazaar.abuse.ch (9,26) y eicar.org (10,25) indican interacción frecuente y sostenida con esos dominios	El score se acumula en el tiempo y no permite determinar intención en visitas individuales
Downloads 789 y 800 interrumpidos	downloads	El Interrupt Reason Virus sugiere que los archivos descargados contenían código	La interrupción fue producida por el antivirus del sistema operativo — no por el

		detectado como malicioso	navegador — y el Danger Type registrado fue Not Dangerous
Web Cache (3.866 registros)	Autopsy	La presencia de recursos en caché de eicar.org y oficial-kmspico.io corrobora indirectamente las visitas documentadas en History	El caché almacena recursos con timestamps de creación en el servidor, no de visita del usuario — no permite establecer una cronología de acceso precisa

Nota. La evidencia indiciaria requiere inferencias adicionales para conectar el artefacto con el hecho investigado, por lo que su interpretación debe contextualizarse con otras fuentes de evidencia.

4.3.3. Limitaciones interpretativas

El análisis identificó cinco categorías de limitaciones interpretativas que condicionan el alcance probatorio de los artefactos analizados y que deben ser consideradas en cualquier proceso pericial basado en artefactos de navegadores Chromium:

Pre-fetching y visit_duration igual a cero:

El navegador Brave — al igual que Chrome — implementa mecanismos de carga anticipada de recursos (pre-fetching) que pueden generar registros en la tabla visits con visit_duration igual a cero, indistinguibles en apariencia de visitas reales de muy corta duración o de redirecciones automáticas del servidor. En el presente análisis los registros 33574 y 33575 del escenario de typosquatting presentan visit_duration = 0, determinándose mediante la correlación con el transition type TYPED y el Typed Count = 1 que corresponden a redirecciones HTTP→HTTPS y no a pre-fetching. Sin embargo, en escenarios donde esa correlación adicional no sea posible, los registros con visit_duration = 0 no pueden atribuirse directamente a una acción consciente del usuario sin evidencia corroborante adicional.

From_visit con valor cero en redirecciones automáticas

El registro 33466 (bazaar.abuse.ch/verify-ua) presenta una visit_duration de 25 horas 53 minutos — valor técnicamente imposible como visita real que corresponde a una sesión de verificación de browser activa en segundo plano durante un período prolongado. Este tipo de artefacto, si no es identificado y contextualizado correctamente, puede inducir interpretaciones erróneas sobre el tiempo efectivo de interacción del usuario con el sitio.

Navegador identificado incorrectamente:

Los registros 33533 y 33534 del escenario KMSpico presentan from_visit = 0 pese a pertenecer a una cadena de redirección activa. Este comportamiento — producido cuando el navegador no puede registrar explícitamente el origen de la navegación en redirecciones automáticas del servidor — limita la capacidad de reconstruir cadenas de redirección complejas mediante el campo from_visit de forma exclusiva. La reconstrucción completa requiere el uso complementario de la correlación temporal, el referrer visible en ChromeHistoryView y BrowsingHistoryView, y la tabla downloads_url_chains para los eslabones de descarga.

Duración anómala por sesión en segundo plano

El registro 33466 (bazaar.abuse.ch/verify-ua) presenta una visit_duration de 25 horas 53 minutos — valor técnicamente imposible como visita real. Este artefacto corresponde a una sesión de verificación de browser de Malware Bazaar que permaneció activa en segundo plano durante un período prolongado sin interacción del usuario, acumulando tiempo de duración de forma pasiva. Este tipo de registro, si no es identificado y contextualizado correctamente, puede inducir interpretaciones erróneas sobre el tiempo efectivo de interacción del usuario con el sitio.

Identificación del navegador en herramientas automatizadas

Las herramientas ChromeHistoryView, BrowsingHistoryView y Autopsy identificaron el navegador como Chrome en lugar de Brave. Esta limitación, derivada de que ambos navegadores comparten el mismo motor Chromium y la misma estructura de bases de datos SQLite, no afecta la integridad ni la interpretación de los datos analizados. Sin embargo, debe documentarse en cualquier proceso pericial que requiera la identificación específica del navegador utilizado, ya que ninguna de estas herramientas puede distinguir entre navegadores basados en Chromium a partir de los artefactos SQLite analizados.

Alcance de las herramientas automatizadas sobre artefactos individuales

Autopsy no pudo extraer Web History, Web Downloads ni Web Search al operar sobre artefactos individuales extraídos en lugar de una imagen forense completa del disco. ChromeHistoryView y BrowsingHistoryView no acceden a las tablas downloads ni downloads_url_chains, limitando su capacidad de reconstruir cadenas de descarga completas. Estas limitaciones evidencian que ninguna herramienta individual ofrece cobertura completa de todos los artefactos de un perfil de navegador Chromium, confirmando la conclusión metodológica de Javed et al. (2022) de que la combinación de múltiples herramientas y métodos es indispensable para garantizar la exhaustividad del análisis forense.

5. Conclusiones y Recomendaciones

5.1. Conclusiones

El presente trabajo demostró que los artefactos persistentes del navegador Brave — basado en el motor Chromium — constituyen una fuente de evidencia digital estructurada y recuperable que permite reconstruir con precisión la actividad de navegación web y documentar incidentes de seguridad en un entorno Windows 11. Las conclusiones se presentan en correspondencia con los objetivos específicos planteados.

- **Metodología y adquisición de evidencia:** El escenario híbrido, que combinó historial real con eventos controlados, permitió contrastar artefactos espontáneos y deliberados, enriqueciendo el análisis. La adquisición mediante FTK Imager y la verificación de integridad con hash MD5, SHA-1 y SHA-256 garantizaron la preservación de la evidencia y la cadena de custodia.

- **Extracción y análisis técnico:** El examen de la base de datos *History* mediante consultas SQL permitió identificar 3.886 URLs, 7.365 visitas, 606 descargas y 394 términos de búsqueda. La verificación del esquema reveló variaciones en campos de relación, subrayando la necesidad de validar estructuras antes de correlacionar datos. El proceso ETL aseguró la conversión precisa de marcas temporales y la construcción de una línea de tiempo verificable.

- **Reconstrucción de incidentes:** La línea de tiempo forense integró 74 eventos relevantes en 79 días, incluyendo cuatro incidentes principales: la descarga no planificada de KMSpico, descargas desde Malware Bazaar, el archivo de prueba EICAR y el escenario de *typosquatting* sobre gooogle.com. La correlación entre *visits*, *downloads* y *downloads_url_chains* permitió reconstruir cadenas completas de navegación y redirección.

- **Validación cruzada de herramientas:** El contraste con Hindsight, ChromeHistoryView, BrowsingHistoryView y Autopsy confirmó la consistencia de los hallazgos, aunque ninguna herramienta ofreció cobertura total. Hindsight aportó metadatos adicionales, mientras que Autopsy destacó por el análisis de caché y la generación de informes estructurados. Estos resultados respaldan la conclusión de (Javed et al., 2022) sobre la necesidad de combinar múltiples herramientas para un análisis exhaustivo.

- **Valor probatorio y limitaciones:** Se identificaron nueve elementos de evidencia directa (ej. descargas verificadas con hash, accesos tipográficos) y ocho de evidencia indiciaria (ej. búsquedas post-incidente, desactivación de SafeBrowsing). Las principales limitaciones fueron el pre-fetching, los valores *from_visit* iguales a cero en redirecciones automáticas y la imposibilidad de acreditar la ejecución de archivos descargados. Esto confirma que el valor técnico-probatorio de los artefactos debe evaluarse dentro de un proceso metodológico integral y crítico.

En síntesis, la metodología desarrollada, basada en análisis manual mediante consultas SQL y validación cruzada con herramientas especializadas, fue validada sobre el navegador Brave en Windows 11. Considerando que Brave utiliza la arquitectura Chromium y conserva la estructura de almacenamiento de artefactos persistentes definida por este proyecto, la metodología podría adaptarse a otros navegadores basados en Chromium que mantengan estructuras equivalentes. El hallazgo no planificado de KMSpico evidenció que el análisis de historial real puede revelar incidentes no previstos inicialmente, reforzando la utilidad del enfoque híbrido para la reconstrucción forense de la actividad web.

5.2. Recomendaciones

Metodológicas:

Verificar siempre el esquema de la base de datos *History* mediante `PRAGMA table_info` como primer paso del análisis, ya que la nomenclatura de campos puede variar entre versiones de Chromium. Omitir este paso puede invalidar consultas de correlación sin generar errores explícitos.

Adoptar el análisis manual mediante SQL como **fuente de verdad metodológica** ante divergencias entre herramientas automatizadas, dado que permite controlar la zona horaria y personalizar consultas de correlación. Las herramientas deben emplearse como mecanismos de verificación complementaria.

La tabla downloads_url_chains debe incluirse sistemáticamente en cualquier análisis forense de incidentes de descarga de malware, dado que es la única fuente que registra los dominios intermedios de redirección no visibles en la tabla visits ni en las herramientas que solo acceden al historial de navegación.

La combinación de historial real con eventos controlados permitió obtener resultados más confiables que los escenarios completamente simulados. Este enfoque facilitó la comparación de distintos tipos de artefactos y permitió verificar cómo se comportan los registros forenses en situaciones reales de uso del navegador. Por ello, se recomienda utilizar este tipo de escenarios en futuras investigaciones, ya que reflejan mejor las condiciones reales y ayudan a respaldar con mayor solidez los hallazgos obtenidos durante el análisis forense.

Para profesionales de ciberseguridad:

La desactivación de SafeBrowsing en el navegador — identificada en el archivo Preferences — debe considerarse un indicador de riesgo en análisis de respuesta a incidentes, dado que su desactivación elimina una capa de protección activa ante descargas maliciosas y acceso a dominios fraudulentos.

El campo Typed Count igual a 1 en la tabla visits, combinado con transition type TYPED, constituye un indicador técnico forense de acceso directo al dominio por escritura manual en la barra de direcciones, relevante para la identificación de incidentes de typosquatting en investigaciones de respuesta a incidentes.

La secuencia de búsquedas en keyword_search_terms debe analizarse en su contexto temporal respecto a los eventos de descarga documentados en la tabla downloads, dado que su posición anterior o posterior a la descarga determina si constituyen evidencia de intención previa o de comportamiento posterior al incidente — distinción crítica para la evaluación del alcance probatorio de los hallazgos.

Autopsy requiere la estructura de directorios completa del perfil del navegador desde la raíz del usuario para activar el módulo de análisis de actividad web. Su uso sobre artefactos extraídos individualmente limita sus capacidades de análisis de historial, siendo más efectivo cuando opera sobre imágenes forenses completas del disco.

Referencias Bibliográficas

abuse.ch. (2026, June 8). *MalwareBazaar*. https://bazaar.abuse.ch/

ACPO. (2015). Good Practice Guide for Digital Evidence. In *National Policing Improvement Agency.* (Vol. 5).

Agten, P., Joosen, W., Piessens, F., & Nikiforakis, N. (2015). Seven Months' Worth of Mistakes: A Longitudinal Study of Typosquatting Abuse. In *Network and Distributed System Security Symposium (NDSS)*. https://doi.org/10.14722/ndss.2015.23058

Boucher, J., Choo, K. K. R., & Le-Khac, N. A. (2022a). Web Browser Forensics—A Case Study with Chrome Browser. In *Studies in Big Data* (Vol. 116, pp. 251–291). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-16127-8_8

Boucher, J., Choo, K. K. R., & Le-Khac, N. A. (2022b). Web Browser Forensics—A Case Study with Chrome Browser. In *Studies in Big Data* (Vol. 116, pp. 251–291). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-16127-8_8

Breitinger, F., Studiawan, H., & Hargreaves, C. (2025). SoK: Timeline based event reconstruction for digital forensics: Terminology, methodology, and current challenges. *Forensic Science International: Digital Investigation*, *53*. https://doi.org/10.1016/j.fsidi.2025.301932

Brezinski, D. , & K. T. (2002). *RFC 3227: Guidelines for evidence collection and archiving. Internet Engineering Task Force*.

Cantelli-Forti, A., Longo, G., Lupia, F., & Russo, E. (2025). WEFT: a consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence.

International Journal of Information Security, *24*(2). https://doi.org/10.1007/s10207-025-00991-8

Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press.

Chand, R. R., Sharma, N. A., & Kabir, M. A. (2025a). Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques. *SN Computer Science*, *6*(4). https://doi.org/10.1007/s42979-025-03921-6

Chand, R. R., Sharma, N. A., & Kabir, M. A. (2025b). Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques. *SN Computer Science*, *6*(4). https://doi.org/10.1007/s42979-025-03921-6

Choi, G., Bang, J., Lee, S., & Park, J. (2023). Chracer: Memory analysis of Chromium-based browsers. *Forensic Science International: Digital Investigation*, *46*. https://dfrws.org/wp-content/uploads/2024/04/Chracer-Memory-analysis-of-Chromiu_2023_Forensic-Science-International-Dig.pdf

D'Anna, T., Puntarello, M., Cannella, G., Scalzo, G., Buscemi, R., Zerbo, S., & Argo, A. (2023). The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data. *Healthcare (Switzerland)*, *11*(5). https://doi.org/10.3390/healthcare11050634

EICAR. (2026, June 8). *Anti Malware Testfile*. https://www.eicar.org/download-anti-malware-testfile/

Ibrahim, S., Herami, N. Al, Naqbi, E. Al, & Aldwairi, M. (2020). *Detection and Analysis of Drive-by Downloads and Malicious Websites*. http://arxiv.org/abs/2002.08007

Ismail, I., & Zainol Ariffin, K. A. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLOS ONE*, *20*(9 September). https://doi.org/10.1371/journal.pone.0331683

ISO/IEC. (2012). *ISO/IEC 27037:2012 - Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence*. ISO. https://www.iso.org/standard/44381.html

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. *IEEE Access*, *10*, 11065–11089. https://doi.org/10.1109/ACCESS.2022.3142508

Jeong, D. (2024). MIC: Memory analysis of IndexedDB data on Chromium-based applications. *Forensic Science International: Digital Investigation*. https://www.sciencedirect.com/science/article/pii/S2666281724001331

Kintis, P., Miramirkhani, N., Lever, C., Chen, Y., Romero-Gomez, R., Pitropakis, N., Nikiforakis, N., & Antonakakis, M. (2017). Hiding in Plain Sight: A Longitudinal Study of Combosquatting Abuse. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)* (pp. 569–586). ACM. https://doi.org/10.1145/3133956.3134002

Mahlous, A., & Mahlous, H. (2020). Private Browsing Forensic Analysis: A Case Study of Privacy Preservation in the Brave Browser. *International Journal of Intelligent Engineering and Systems*, *13*(6), 294–306. https://doi.org/10.22266/ijies2020.1231.26

MITRE ATT&CK. (2024a). *Drive-by compromise (T1189).* . MITRE Corporation. https://attack.mitre.org/techniques/T1189/

MITRE ATT&CK. (2024b). *User execution: Malicious file (T1204.002)*. MITRE Corporation. https://attack.mitre.org/techniques/T1204/002/

Nelson, R., Shukla, A., & Smith, C. (2020). Web Browser Forensics in Google Chrome, Mozilla Firefox, and the Tor Browser Bundle. In *Studies in Big Data* (Vol. 61, pp. 219–241). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-23547-5_12

NIST. (2015). *SHA-3 STANDARD: PERMUTATION-BASED HASH AND EXTENDABLE OUTPUT FUNCTIONS*. https://doi.org/10.6028/NIST.FIPS.202

Quick, D., & Choo, K.-K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, *11*(4), 273–294. https://doi.org/10.1016/j.diin.2014.09.002

Reed, A., Scanlon, M., & Le-Khac, N.-A. (2022). A Critical Comparison of Brave Browser and Google Chrome Forensic Artefacts. *Journal of Digital Forensics, Security and Law*, *17*(1). https://commons.erau.edu/jdfsl/vol17/iss1/4

Sanghvi, H., Patel, V. J., Shah, R., Shukla, P., & Rathod, D. (2023). Web Browser Forensics: A Comparative Integrated Approach on Artefacts Acquisition, Evidence Collections and Analysis of Google Chrome, Firefox and Brave Browser. In *Computing Science, Communication and Security (COMS2 2023), CCIS Vol. 1861*. Springer, Cham. https://doi.org/10.1007/978-3-031-40564-8_15

StatCounter. (2026, June 15). *Browser Market Share Worldwide*. https://gs.statcounter.com/browser-market-share

Szurdi, J., Kocso, B., Cseh, G., Spring, J., Felegyhazi, M., & Kanich, C. (2014). The Long "Taile" of Typosquatting Domain Names. In *23rd USENIX Security Symposium*

(USENIX Security 14) (pp. 191–206). USENIX Association. https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/szurdi

Yang, W.-C. (2025). Decrypting Digital Secrets: Browser Password Recovery from RAM Dumps in Compliance with ISO/IEC 27037. In *Advances in Digital Forensics*. Springer. https://doi.org/10.1007/978-3-031-95017-9_6

Apéndices

Apéndice A

CARTA DE AUTORIZACIÓN Y CONSENTIMIENTO PARA EL USO DE MEDIOS TECNOLÓGICOS CON FINES DE INVESTIGACIÓN ACADÉMICA

D. M. Quito, 19 de junio de 2026

Yo, **Fabricio Alexander Toasa Arroba**, portador de la cédula de ciudadanía No. [redacted], por medio de la presente manifiesto mi consentimiento libre, previo, expreso e informado para autorizar el uso de mis medios tecnológicos y la información contenida en ellos exclusivamente con fines académicos y de investigación, en el marco del trabajo de titulación denominado:

"Reconstrucción forense de actividad web mediante el análisis de artefactos persistentes del navegador Brave en Windows 11 orientada a la identificación de incidentes de seguridad"

Desarrollo por los estudiantes:

- Ángel Fabrizio Merino Torres
- María Fernanda Ordoñez Vivanco
- Jenny Julizza Alava Bolaños
- Fabricio Alexander Toasa Arroba

de la **Maestría en Ciberseguridad de la Universidad Internacional del Ecuador (UIDE)**.

PRIMERA. OBJETO DE LA AUTORIZACIÓN

Autorizo a los investigadores antes mencionados a acceder, recopilar, analizar y documentar información contenida en los equipos y medios tecnológicos de mi propiedad que resulten necesarios para el desarrollo de la investigación académica.

La autorización comprende exclusivamente el análisis de artefactos digitales asociados a navegadores basados en Chromium instalados sobre sistemas operativos Windows 11, incluyendo bases de datos, archivos de configuración, registros de navegación, caché, historial, descargas, cookies, sesiones y demás artefactos persistentes requeridos por la metodología de investigación.

SEGUNDA. FINALIDAD DEL TRATAMIENTO DE LA INFORMACIÓN

La información obtenida será utilizada únicamente para:

- El desarrollo del trabajo de investigación.
- La validación de la metodología propuesta.
- La obtención de resultados académicos y científicos.
- La elaboración del documento final de titulación.
- La generación de evidencias técnicas necesarias para sustentar las conclusiones del estudio.

En ningún caso la información será utilizada con fines comerciales, publicitarios o distintos a los expresamente señalados en esta autorización.

TERCERA. CONFIDENCIALIDAD Y PROTECCIÓN DE LA INFORMACIÓN

Los investigadores se comprometen a mantener absoluta reserva respecto de toda información a la que tengan acceso durante el desarrollo del proyecto.

Asimismo, cualquier dato personal, sensible o confidencial que pudiera identificarse durante el análisis será anonimizado, seudonimizado o excluido de las publicaciones, informes y documentos académicos resultantes, salvo autorización expresa del titular.

CUARTA. ALCANCE DE LA AUTORIZACIÓN

La presente autorización comprende únicamente el acceso a la información estrictamente necesaria para cumplir los objetivos de la investigación y no implica transferencia de propiedad sobre los equipos, sistemas o información analizada.

El titular podrá solicitar en cualquier momento información sobre el tratamiento de los datos utilizados dentro del proyecto.

QUINTA. NORMATIVA APLICABLE

La presente autorización se emite de conformidad con los principios de buena fe, confidencialidad, finalidad, minimización y responsabilidad aplicables al tratamiento de información en el ámbito académico y científico, observando la normativa vigente de la República del Ecuador, incluyendo el **Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación (COESCCI)** y demás disposiciones legales aplicables.

SEXTA. DECLARACIÓN FINAL

Declaro que otorgo esta autorización de manera libre y voluntaria, habiendo comprendido el alcance, finalidad y limitaciones del tratamiento de la información que será utilizada en el desarrollo del proyecto de investigación antes referido.

Para constancia de lo expuesto, suscribo la presente autorización.

Fabricio Alexander Toasa Arroba
Titular de los Medios Tecnológicos

C.C. No. [redacted]

Correo electrónico: fatoasaar@uide.edu.ec

Firmado electrónicamente por:
FABRICIO ALEXANDER TOASA ARROBA

Apéndice B

Cadena de custodia completa de los artefactos del navegador Brave.

N°	Fecha y Hora	Acción	Herramienta	Artefacto
1	7/6/2026 13:00	Adquisición forense	FTK Imager	History, Web Data, Preferences
2	7/6/2026 13:20	Verificación de hashes MD5 y SHA-1	FTK Imager	History, Web Data, Preferences
3	7/6/2026 13:30	Verificación de hashes SHA-256	PowerShell	History, Web Data, Preferences
4	7/6/2026 14:00	Apertura en modo solo lectura	DB Browser for SQLite	History, Web Data
5	8/6/2026 9:00	Extracción de URLs visitadas	DB Browser for SQLite	History
6	8/6/2026 14:30	Análisis con herramienta automatizada	ChromeHistoryView	History
7	9/6/2026 9:15	Identificación de dominios visitados frecuentemente	ChromeHistoryView	History
8	9/6/2026 15:00	Análisis con herramienta automatizada	BrowsingHistoryView	History
9	10/6/2026 9:45	Correlación de visitas con palabras clave de riesgo	DB Browser for SQLite	History, Web Data

10	10/6/2026 16:20	Análisis de formularios autocompletados	DB Browser for SQLite	Web Data
11	11/6/2026 9:00	Revisión de configuraciones persistentes del navegador	Notepad++	Preferences
12	11/6/2026 14:10	Identificación de extensiones instaladas	Análisis Manual JSON	Preferences
13	12/6/2026 8:50	Identificación de búsquedas relacionadas con malware	BrowsingHistoryView	History
14	12/6/2026 15:30	Identificación de descargas asociadas a incidentes	DB Browser for SQLite	History
15	13/6/2026 9:20	Análisis con herramienta automatizada	Hindsight	Perfil Brave
16	13/6/2026 16:45	Generación de línea temporal preliminar	Hindsight	History, Web Data, Preferences
17	14/6/2026 15:00	Análisis de redirecciones encadenadas	Hindsight	History
18	15/6/2026 9:30	Correlación de dominios sospechosos con eventos de navegación	Hindsight	Perfil Brave

19	16/6/2026 14:30	Correlación de eventos sospechosos con dominios maliciosos	Autopsy	History
20	17/6/2026 9:15	Análisis con plataforma forense	Autopsy	History
21	17/6/2026 14:40	Identificación de patrones de navegación anómalos	Autopsy	History
22	18/6/2026 8:45	Revisión de cambios en configuraciones del navegador	DB Browser for SQLite	Preferences
23	18/6/2026 11:30	Análisis de persistencia mediante extensiones	Hindsight	Preferences
24	18/6/2026 15:30	Consolidación de evidencias digitales	Autopsy	History, Web Data, Preferences
25	18/6/2026 17:00	Elaboración de línea temporal definitiva	Hindsight	Perfil Brave
26	19/6/2026 9:00	Validación cruzada de hallazgos	ChromeHistoryView, BrowsingHistoryView	History
27	19/6/2026 10:30	Documentación de incidentes identificados	Microsoft Word	History, Web Data, Preferences
28	19/6/2026 12:00	Revisión final de artefactos analizados	DB Browser for SQLite	History, Web Data, Preferences

29	19/6/2026 13:00	Verificación intermedia de integridad SHA-256	PowerShell	History, Web Data, Preferences
30	19/6/2026 14:00	Consolidación de evidencias para informe pericial	Autopsy	History, Web Data, Preferences
31	19/6/2026 15:00	Validación final de resultados obtenidos	Hindsight	Perfil Brave
32	19/6/2026 16:00	Verificación final de hashes	PowerShell	History, Web Data, Preferences
33	19/6/2026 16:30	Cierre formal de la cadena de custodia	Registro documental	History, Web Data, Preferences

Apéndice C

Parte del Informe generado por Autopsy

Analisis Forense Artefactos Navegador Brave

Autopsy Forensic Report

HTML Report Generated on 2026/06/14 20:51:46

Case:	Analisis Forense Artefactos Brave
Number of data sources in case:	1

Image Information:

LogicalFileSet1

Software Information:

Autopsy Version:	4.23.1
Central Repository Module:	4.23.1
Data Source Integrity Module:	4.23.1
Email Parser Module:	4.23.1
Embedded File Extractor Module:	4.23.1
Encryption Detection Module:	4.23.1
Extension Mismatch Detector Module:	4.23.1
File Type Identification Module:	4.23.1
Hash Lookup Module:	4.23.1
Interesting Files Identifier Module:	4.23.1
Keyword Search Module:	4.23.1
Recent Activity Module:	4.23.1

Report Navigation

- Case Summary
- Keyword Hits (127625)
- Metadata (7)
- Tagged Files (0)
- Tagged Images (0)
- Tagged Results (0)
- Web Cache (3866)
- Web Categories (2)

Ingest History:

Job 1:

Data Source:	LogicalFileSet1
Status:	COMPLETED
Enabled Modules:	Recent Activity Hash Lookup File Type Identification Extension Mismatch Detector Embedded File Extractor Email Parser Encryption Detection Interesting Files Identifier Central Repository Data Source Integrity

Job 2:

Data Source:	LogicalFileSet1
Status:	COMPLETED
Enabled Modules:	Keyword Search

Powered by Autopsy Open Source Digital Forensics Platform - www.sleuthkit.org

Analisis Forense Artefactos Navegador Brave

Keyword Hits

- User Searches
- Analisis Brave
- Email Addresses
- URLs

User Searches

bazaar

Preview	Source File	Tags
Carrito Todo " Amazon «Bazaar« " Ofertas del Dia	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028b9b/f_028b9b/0	
Carrito Todo " Amazon «Bazaar« " Ofertas del Dia	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028b9b/f_028b9b/0	
Carrito Todo " Amazon «Bazaar« " Ofertas del Dia	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028b9b/f_028b9b/0	
Carrito Todo " Amazon «Bazaar« " Ofertas del Dia	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028b9b/f_028b9b/0	
Carrito Todo " Amazon «Bazaar« " Ofertas del Dia	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028bab/f_028bab/0	
Carrito Todo " Amazon «Bazaar« " Ofertas del Dia	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028bab/f_028bab/0	
Carrito Todo " Amazon «Bazaar« " Ofertas del Dia	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028bab/f_028bab/0	
Carrito Todo " Amazon «Bazaar« " Zona de envio gratis	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028bd6/f_028bd6/0	
Carrito Todo " Amazon «Bazaar« " Zona de envio gratis	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028bd6/f_028bd6/0	
Carrito Todo " Amazon «Bazaar« " Zona de envio gratis	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028bd6/f_028bd6/0	
Carrito Todo " Amazon «Bazaar« " Zona de envio gratis	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028bd6/f_028bd6/0	
Ld n d Uq /cart/carts/«bazaar« p /gp p default 22569	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Code Cache/js/962f82d217ecf29ff_0	
Ld n d Uq /cart/carts/«bazaar« p /gp p default 22569	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Code Cache/js/962f82d217ecf29ff_0	
Ld n d Uq /cart/carts/«bazaar« p /gp p default 22569	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Code Cache/js/962f82d217ecf29ff_0	
Ld n d Uq /cart/carts/«bazaar« p /gp p default 22569	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Code Cache/js/962f82d217ecf29ff_0	
(sis. Hybrid][V Any.RuA .«Bazaar«. Down rese genel> Auto	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000252.ldb	
(sis. Hybrid][V Any.RuA .«Bazaar«. Down rese genel> Auto	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000252.ldb	
(sis. Hybrid][V Any.RuA .«Bazaar«. Down rese genel> Auto	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000252.ldb	
(sis. Hybrid][V Any.RuA .«Bazaar«. Down rese genel> Auto	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000252.ldb	
0typosquatting s. Seg r sa «Bazaar« trase RetomarB . B o s	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72	
0typosquatting s. Seg r sa «Bazaar« trase RetomarB . B o s	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72	
0typosquatting s. Seg r sa «Bazaar« trase RetomarB . B o s	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72	
0typosquatting s. Seg r sa «Bazaar« trase RetomarB . B o s	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72	

eicar

Preview	Source File
google.com/search?q=«eicar«&oq=«eicar«&sourceid=chrome&ie=UTF-8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Favicons
google.com/search?q=«eicar«&oq=«eicar«&sourceid=chrome&ie=UTF-8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Favicons
google.com/search?q=«eicar«&oq=«eicar«&sourceid=chrome&ie=UTF-8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/History
google.com/search?q=«eicar«&oq=«eicar«&sourceid=chrome&ie=UTF-8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/History
com/search?q=«eicar«+test+file+download&oq=«eicar«+test+fil	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Network Action Predictor
com/search?q=«eicar«+test+file+download&oq=«eicar«+test+fil	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Network Action Predictor
663-883a-4ae8fbbac8ac «eicar« https://www.eicar.org/	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Shortcuts
663-883a-4ae8fbbac8ac «eicar« https://www.eicar.org/	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Shortcuts
mages/uploads/2022/06/«eicar«-news-013.jpg.webp 1/0/	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/data_1
mages/uploads/2022/06/«eicar«-news-013.jpg.webp 1/0/	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/data_1
google.com/search?q=«eicar«&oq=«eicar«&sourceid=chrome&ie=UTF-8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029203
google.com/search?q=«eicar«&oq=«eicar«&sourceid=chrome&ie=UTF-8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029203
google.com/search?q=«eicar«&oq=«eicar«&sourceid=chrome&ie=UTF-8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029204
google.com/search?q=«eicar«&oq=«eicar«&sourceid=chrome&ie=UTF-8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029204
google.com/search?q=«eicar«&oq=«eicar«&sourceid=chrome&ie=UTF-8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_02920c
google.com/search?q=«eicar«&oq=«eicar«&sourceid=chrome&ie=UTF-8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_02920c
data_1__a3014840 {"name":"«EICAR«","start_url":"https:\/\/www	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/data_1/data_1__a3014840
data_1__a3014840 {"name":"«EICAR«","start_url":"https:\/\/www	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/data_1/data_1__a3014840
8c;p 1 RNEn &/"aRu d"b «EICAR«=)r`:> *I.A pl<aD 0..$	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72
8c;p 1 RNEn &/"aRu d"b «EICAR«=)r`:> *I.A pl<aD 0..$	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72
kmspico bazaar gooogle «eicar« fin-tech get-file"]]]]	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.leveldb/000042.log
kmspico bazaar gooogle «eicar« fin-tech get-file"]]]]	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.leveldb/000042.log
whatsapp ww.amazon .br/ «eicar« google)B<# hornetsecurit	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Service Worker/Database/000035.ldb
whatsapp ww.amazon .br/ «eicar« google)B<# hornetsecurit	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Service Worker/Database/000035.ldb
9f1_acfc_19f681e063bb «eicar« ;cee644_29f8 GH2_87d2_	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Session Storage/001662.ldb
9f1_acfc_19f681e063bb «eicar« ;cee644_29f8 GH2_87d2_	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Session Storage/001662.ldb
https://www.eicar.org/#about@ «Eicar« e.V. - European Institute	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Sessions/Tabs_13425335190796400
https://www.eicar.org/#about@ «Eicar« e.V. - European Institute	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Sessions/Tabs_13425335190796400
Anti Malware Testfile - «EICAR«| https://www.eicar.org	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Sessions/Tabs_13425885269042086
Anti Malware Testfile - «EICAR«| https://www.eicar.org	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Sessions/Tabs_13425885269042086

gooogle

Preview	Source File
0MALWAREBAZAAR^n IP86j «gooogle« 0TYPOSQUATTING ORDER BY*	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72
busque por kmspico bazaar «gooogle« eicar fin-tech get-file"]]]]	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.leveldb/000042.log

kmspico

Preview	Source File	Tags
oads/2020/05/cropped-«kmspico«-logo-150x150-1-32x32.jpg	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Favicons	
ico.lo/ Descargar «KMSpico« Activador	Sitio Web	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/History	
ico.lo/ Descargar «KMSpico« Activador	Sitio Web	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029203	
"\ud83e\udd47 Descargar «KMSpico« Activador	Sitio Web	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029204	
ico.lo/ Descargar «KMSpico« Activador	Sitio Web	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_02920c	
5df53"E>" 50.412082 «KMSPICO« 33514 2026-05-28 22:56	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72	
timeline, ya busque por «kmspico« bazaar gooogle eicar fin-tech	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.leveldb/000042.log	
icio Toasa\Downloads\«KMSpico«-ENFT.rarx 021_download	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/shared_proto_db/000067.log	

malware

Preview	Source File
org/insights/blog/top-10-«malware«-q4-2024 4333 0 16670	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Favicons
org/insights/blog/top-10-«malware«-q4-2024 4333 0 16670	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Favicons
Windows 11 comprometido por «malware« fileless en un ataque	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/History
Windows 11 comprometido por «malware« fileless en un ataque	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/History
58de8 como descargar «malware« https://www.google.com/search	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Network Action Predictor
58de8 como descargar «malware« https://www.google.com/search	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Network Action Predictor
ti-«malware«-testfile/ 0,1 Download Anti «Malware« Testfile	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Shortcuts
ti-«malware«-testfile/ 0,1 Download Anti «Malware« Testfile	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Shortcuts
phishing y 32.520 son de «malware«. para la deteccion de	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Web Data
phishing y 32.520 son de «malware«. para la deteccion de	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Web Data
com/search?q=«MALWARE«+BAZZAR&oq=«malware«+ba&sourceid=	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/data_1
com/search?q=«MALWARE«+BAZZAR&oq=«malware«+ba&sourceid=	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/data_1
Lista de muestras de «malware« disponibles a descargar	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028e59
Lista de muestras de «malware« disponibles a descargar	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028e59
phishing y 32.520 son de «malware«. C:\Users\Fabricio T	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029203
phishing y 32.520 son de «malware«. C:\Users\Fabricio T	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029203
phishing y 32.520 son de «malware«.", "source_item": "Web	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029204
phishing y 32.520 son de «malware«.", "source_item": "Web	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029204
phishing y 32.520 son de «malware«. C:\Users\Fabricio T	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_02920c
phishing y 32.520 son de «malware«. C:\Users\Fabricio T	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_02920c
ones associated with «malware« or phishing). Users can	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_0291b1/hindsight-2026.04/documentation/hi
ones associated with «malware« or phishing). Users can	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_0291b1/hindsight-2026.04/documentation/hi
- Vulnerabilities and «malware«\n - Supply chain risks\n	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029305/f_029305/0
- Vulnerabilities and «malware«\n - Supply chain risks\n	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029305/f_029305/0
R/FETCH_REQUEST DMCA «MALWARE« ILLEGAL SPAM TERROR CSAI	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Code Cache/js/bb2da3a5c1f9cf96_0
R/FETCH_REQUEST DMCA «MALWARE« ILLEGAL SPAM TERROR CSAI	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Code Cache/js/bb2da3a5c1f9cf96_0
25PI 8%t4E (IPi `],"«malware«":[% D0e4 <lx aT |	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.blob/1/00/3
25PI 8%t4E (IPi `],"«malware«":[% D0e4 <lx aT |	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.blob/1/00/3
n ,40,113(4.2292 1],"«malware«":[118 < 4 @83243,330	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.blob/1/00/4
n ,40,113(4.2292 1],"«malware«":[118 < 4 @83243,330	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.blob/1/00/4
)Q %4ing".[1 96,1815],"«malware«":[19 "02425.99 .V0conduct	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.blob/2/00/4

Analisis Brave

bazaar

Preview	Source File	Tags
o todo " amazon «bazaar« " ofertas del d	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028b9b/f_028b9b/0	
o todo " amazon «bazaar« " ofertas del d	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028bab/f_028bab/0	
o todo " amazon «bazaar« " zona de envio	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028bd6/f_028bd6/0	
n d.uq /cart/carts/«bazaar« p./gp p default 225	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Code Cache/js/96282d217ecf29ff_0	
. hybrid}v any rua .«bazaar«: down rese genel>	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000252.ldb	
uatting s. seg r sa «bazaar« trase retomarb . b	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72	
busque por kmspico «bazaar« gooogle eicar fin-t	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.leveldb/000042.log	
own emplifi ag] t «bazaar« vo ,smallbusines: r	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Local Storage/leveldb/006585.ldb	

eicar

Preview	Source File	Tags
google.com/search?q=«eicar«&oq=eicar&sourceid=c	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Favicons	
google.com/search?q=«eicar«&oq=eicar&sourceid=c	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/History	
0-ad9f-9c117e1e9769 «eicar« test file download	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Network Action Predictor	
3-883a-4ae8fbbac8ac «eicar« https://www.eicar.o	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Shortcuts	
ges/uploads/2022/06/«eicar«-news-013.jpg.webp 1	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/data_1	
google.com/search?q=«eicar«&oq=eicar&sourceid=c	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029203	
google.com/search?q=«eicar«&oq=eicar&sourceid=c	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029204	
google.com/search?q=«eicar«&oq=eicar&sourceid=c	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_02920c	
{"name":"«eicar«","start_url":"https	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/data_1/data_1__a3014840	
1 men &\"aru d"b «eicar«=)r`> *l.a pl<ad	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72	
pico bazaar gooogle «eicar« fin-tech get-file"}	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.leveldb/000042.log	
app ww.amazon .br/ «eicar« google)b<# hornets	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Service Worker/Database/000035.ldb	
1_acfc_19f681e063bb «eicar« :cee644_298 gh2_87	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Session Storage/001662.ldb	
w.eicar.org/#about@ «eicar« e.v. - european ins	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Sessions/Tabs_13425335190796400	
malware testfile - «eicar«\ https://www.eicar.	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Sessions/Tabs_13425885269042086	

fin-tech

Preview	Source File	Tags
rous filtr .pdo por «fin-tech« dsigh cs (v2026.04	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72	
azaar gooogle eicar «fin-tech« get-file"}]}],"att	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.leveldb/000042.log	
bc69ad0f- @winload1 «fin-tech« m h352e1_d414_41c7_	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Session Storage/001662.ldb	

gooogle

Preview	Source File	Tags
warebazaar^n ip86j «gooogle« 0typosquatting orde	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72	
por kmspico bazaar «gooogle« eicar fin-tech get-	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.leveldb/000042.log	

kmspico

Preview	Source File	Tags
ads/2020/05/cropped-«kmspico«-logo-150x150-1-32x3	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Favicons	
co.io/ descargar «kmspico« activador | sitio w	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/History	
co.io/ descargar «kmspico« activador | sitio w	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029203	
83e\udd47 descargar «kmspico« activador | sitio w	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029204	
co.io/ descargar «kmspico« activador | sitio w	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_02920c	
df53"e>" 50.412082 «kmspico« 33514 2026-05-28 22	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.blob/1/0e/e72	
line, ya busque por «kmspico« bazaar gooogle eica	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_claude.ai_0.indexeddb.leveldb/000042.log	
cio toasa\downloads\«kmspico«-enft.rarx 021_downl	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/shared_proto_db/000067.log	

malware

Preview	Source File
nsights/blog/top-10-«malware«-q4-2024 4333 0 166	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Favicons
11 comprometido por «malware« fileless en un ataq	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/History
8de8 como descargar «malware« https://www.google.	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Network Action Predictor
r.org/download-anti-«malware«-testfile/ https://w	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Shortcuts
ing y 32.520 son de «malware«. para la deteccion	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Web Data
google.com/search?q=«malware«+bazzar&oq=malware+b	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/data_1
ista de muestras de «malware« disponibles a desca	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_028e59
ing y 32.520 son de «malware«. c:\users\fabricio	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029203
ing y 32.520 son de «malware«.", "source_item": "	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029204
ing y 32.520 son de «malware«. c:\users\fabricio	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_02920c
nes associated with «malware« or phishing). user	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_0291b1/hindsight-2026.04/documentation/Hindsight User Guid
vulnerabilities and «malware«\n - supply chain ri	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/Cache_Data/f_029305/f_029305/0
/fetch_request dmca «malware« illegal spam terror	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Code Cache/js/bb2da3a5c1f9cf96_0
25pl 8%t4e (tpi`:'],"«malware«":[% d0e4 <!x at |	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.blob/1/00/3
,40,113(4,2292 1],"«malware«":[118 < 4 @83243,3	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.blob/1/00/4
%4ing":[1 96,1815],"«malware«":[19 *02425,99 .v0c	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.blob/2/00/4
on rBiscovery%bf t8 «malware« iha"ana>ym@ j!v68 l	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.blob/2/00/8
evilbunnyz is a c++ «malware« sampl 8observed h20	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000229.ldb
.[1] id: s1211 $ @: «malware« l 1.0 c% (mod6 .8	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000230.ldb
intrusion activity. «malware«, tools, or other no	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000237.ldb
btain capabilities: «malware« adversaries may buy	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000238.ldb
velop capabilities: «malware« adversaries may dev	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000239.ldb
executly flow: dll `«malware« variant, terratv.lg	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000240.ldb
s tlike 'phish', '«malware« user xt scope5 moni	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000241.ldb
tentc $ h1n1. his a «malware« v 8iant tha 6(been	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000242.ldb
ly d port pecied1n «malware« often 1i$ors within	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000243.ldb
utolt backdoor his «malware« tha "@been used h8s	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000244.ldb
id: s0243 $ type: «malware« $ phms: window "(1.	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000245.ldb
evilbunnyz is a c++ «malware« sampl 8observed h20	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000246.ldb
[1] 0d: s038 type @«malware« v sion 1.1 % 25 ap	/LogicalFileSet1/Artefactos/Users/Fabricio Toasa/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/IndexedDB/https_attack.mitre.org_0.indexeddb.leveldb/000247.ldb

Apéndice D

Link espacio compartido

Se ha creado una carpeta compartida dentro de One Drive mediante la cuenta institucional por favor acceder por el siguiente enlace:

https://mailinternacionaledu-my.sharepoint.com/:f:/g/personal/fatoasaar_uide_edu_ec/IgB1xIXBYg8TQYWmGJaeRrbcATw45KKfjLjvKicSO8_9z-4?e=XgdHdC

Se ha configurado que los usuarios puedan editar, pero con la restricción que solo miembros del dominio Universidad Internacional del Ecuador puedan acceder.