Maestría en

# Ciberseguridad

Trabajo previo a la obtención de título de

Magister en Ciberseguridad


**AUTORES:**

María Gabriela Gómez Yánez

Michael Jossue Rodríguez Rojas

Oscar Darwin Saavedra Paredes

Luis Fernando Sánchez Lincango

**TUTOR:**

Iván Reyes Chacón


## Herramientas y técnicas forenses para la adquisición y análisis de artefactos de Google Meet en navegadores web


QUITO - ECUADOR 2025


REINVENTEMOS EL FUTURO

Certificación de autoría

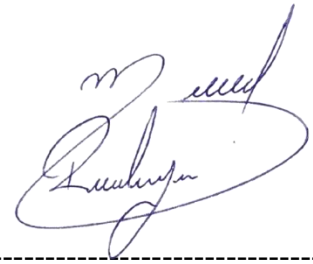
Nosotros, **María Gabriela Gómez Yánez, Michael Jossue Rodríguez Rojas, Oscar Darwin Saavedra Paredes, Luis Fernando Sánchez Lincango,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y 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 del graduando**

**María Gabriela Gómez Yánez**



---

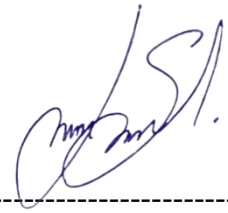
**Firma del graduando**

**Michael Jossue Rodríguez Rojas**

---

**Firma del graduando**

**Oscar Darwin Saavedra Paredes**



---

**Firma del graduando**

**Luis Fernando Sánchez Lincango**

**Autorización de Derechos de Propiedad Intelectual**

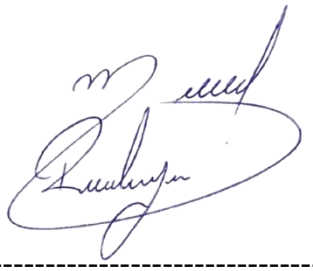
Nosotros, María Gabriela Gómez Yánez, Michael Jossue Rodríguez Rojas, Oscar Darwin Saavedra Paredes, Luis Fernando Sánchez Lincango, en calidad de autores del trabajo de investigación titulado *Herramientas y técnicas forenses para la adquisición y análisis de artefactos de Google Meet en navegadores web*, 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 2025

---

**Firma del graduando**

**María Gabriela Gómez Yánez**



---

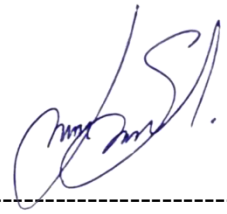
**Firma del graduando**

**Michael Jossue Rodríguez Rojas**

---

**Firma del graduando**

**Oscar Darwin Saavedra Paredes**



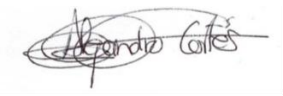
---

**Firma del graduando**

**Luis Fernando Sánchez Lincango**

**Aprobación de dirección y coordinación del programa**

Nosotros, **Alejandro Cortés e Iván Reyes**, declaramos que: María Gabriela Gómez Yánez, Michael Jossue Rodríguez Rojas, Oscar Darwin Saavedra Paredes, Luis Fernando Sánchez Lincango son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



Alejandro Cortés L.

Maestría en Ciberseguridad

Iván Reyes Ch.

Maestría en Ciberseguridad

DEDICATORIA

Dedicamos este trabajo, en primer lugar, a Dios, por la salud y la vida que nos ha concedido para poder culminar este proceso.

También lo dedicamos a nuestras familias, quienes han sido un pilar fundamental a lo largo de esta etapa académica, acompañándonos con paciencia y comprensión en cada momento. Nos brindaron su apoyo incondicional y palabras de aliento cuando más las necesitábamos.

Finalmente, queremos dedicar este logro a nosotros mismos, por la entrega, la perseverancia, el compromiso y, sobre todo, por la confianza que depositamos en este proyecto desde el inicio.

AGRADECIMIENTOS

Queremos expresar nuestros más sinceros agradecimientos a todas las personas que forman parte de la institución educativa. A los docentes, por compartir sus conocimientos y guiarnos en la comprensión de cada materia, y a las coordinadoras, por brindarnos su apoyo incondicional hasta el último día. Todo ese esfuerzo y compromiso se refleja ahora en la culminación de este proyecto.

Agradecemos profundamente a nuestras familias por el respaldo constante, tanto emocional como práctico, que nos permitió enfocarnos y afrontar este proceso académico con mayor solvencia.

Del mismo modo, valoramos el espíritu de compañerismo y colaboración que se fortaleció entre nosotros como equipo. El respeto, la comunicación y el compromiso fueron pilares esenciales para el desarrollo y la finalización de este trabajo.

Finalmente, extendemos nuestro agradecimiento a todas las personas que, con una palabra o un pequeño gesto de aliento, hicieron más llevadero este camino y contribuyeron de manera significativa a nuestro crecimiento académico.

RESUMEN

Este trabajo de titulación parte del análisis forense de una plataforma que se ha vuelto esencial en instituciones públicas, privadas y educativas, como lo es Google Meet. Actualmente, aún no existen metodologías claras ni herramientas estandarizadas que permitan realizar un análisis forense sobre las evidencias que esta herramienta puede dejar diferentes navegadores web.

El objetivo general de este trabajo de titulación es determinar las herramientas y técnicas forenses para la identificación y análisis de artefactos digitales creados por Google Meet en navegadores web, lo que permitirá desarrollar una metodología clara que asegure la integridad de la evidencia recolectada. Para lograr esto, se plantearon varios objetivos específicos como: identificar la información que genera y guarda distintos navegadores web, evaluar las herramientas forenses disponibles para adquirir y analizar artefactos digitales en entornos controlados, crear una metodología de análisis, validad esta metodología y emitir recomendaciones.

La metodología que se utilizó para el desarrollo del trabajo se basa en un entorno controlado con Windows 10 y dos distintos navegadores, en ellos se realizaron video llamadas de prueba en Google Meet para luego capturar y analizar la información local con distintas herramientas logrando recuperar información importante.

**Palabras Claves:** Google meet, informática forense, artefactos digitales, navegadores web, análisis forense, herramientas forenses, metodología forense.

ABSTRACT

This degree project is based on the forensic analysis of a platform that has become essential in public, private, and educational institutions: Google Meet. Currently, there are still no clear methodologies or standardized tools that allow a proper forensic analysis of the evidence this platform may leave behind in different web browsers.

The general objective of this project is to determine the forensic tools and techniques necessary to identify and analyze digital artifacts generated by Google Meet in web browsers. This will help develop a clear methodology that ensures the integrity of the collected evidence. To achieve this, several specific objectives were proposed: identifying the data generated and stored by different browsers, evaluating available forensic tools to acquire and analyze digital artifacts in controlled environments, creating an analysis methodology, validating that methodology, and issuing recommendations.

The methodology used for the development of this work is based on a controlled environment with Windows 10 and two different web browsers. Test video calls were carried out on Google Meet, and the local data was then captured and analyzed using various tools, successfully recovering important information.

**Keywords:** Google Meet, digital forensics, digital artifacts, web browsers, forensic analysis, forensic tools, forensic methodology.

**TABLA DE CONTENIDOS**

Capítulo 1 ..... 10

1.Introducción ..... 10

Definición Del Proyecto ..... 10

Justificación e importancia del trabajo de investigación ..... 13

Alcance ..... 16

Objetivos ..... 17

Capítulo 2: ..... 18

2.Revisión De Literatura ..... 19

Estado Del Arte ..... 19

Planteamiento del problema ..... 23

Marco Teórico ..... 25

Capítulo 3: ..... 53

3.Desarrollo ..... 53

Desarrollo del Trabajo ..... 53

Capítulo 4: ..... 66

4.Análisis De Resultados ..... 66

Pruebas de Concepto ..... 66

Análisis de Resultados ..... 67

Capítulo 5: ..... 68

5.Conclusiones Y Recomendaciones ..... 69

CONCLUSIONES ..... 69

RECOMENDACIONES ..... 71

6.Referencias Bibliográfica ..... 72

7Apéndices ..... 74

LISTA DE FIGURAS

Figura 1 ..... 57

Figura 2 ..... 58

Figura 3 ..... 59

Figura 4 ..... 61

Figura 5 ..... 61

Figura 6 ..... 62

Figura 7 ..... 63

Figura 8 ..... 64

Figura 9 ..... 65

Figura 10 ..... 66

Figura 11 ..... 67

# Capítulo 1

## 1. Introducción

### *Definición Del Proyecto*

En la situación actual, que al momento está marcada por el aumento de la digitalización y el requisito continuo para la comunicación remota, las videollamadas se han convertido en una herramienta crucial para la vida diaria y los entornos profesionales de hoy en día, estas plataformas no solo se utilizan por razones personales, como mantenerse en contacto con familiares o amigos, también juegan un papel fundamental en el funcionamiento de las instituciones públicas, empresas privadas, las escuelas, colegios y en general sitios de educación.

Gracias a la tecnología que respalda este servicio, es posible que los grupos o individuos enteros hablen en vivo, sin importar dónde se encuentren en el país o en todo el mundo. Este progreso ha eliminado muchas de las restricciones basadas en el área que solían estar allí y ha facilitado el trabajo en equipo más flexible, activo y productivo. En esta situación, dispositivos como Google Meet se han vuelto innegablemente importantes, particularmente por su simplicidad, su compatibilidad con otros programas y su flexibilidad para adaptarse a diversas situaciones y requisitos.

Google Meet ha demostrado ser una buena manera de realizar reuniones de trabajo, cursos en línea, entrevistas de trabajo y diferentes tareas administrativas Su aplicación ahora está muy extendida en escuelas, empresas y organismos gubernamentales, ayudando en operaciones

ininterrumpidas durante tiempos cruciales y alentando formas de comunicación más adaptables y accesibles

A pesar de la adopción generalizada de las herramientas de videoconferencia, también ha llevado a nuevas preocupaciones con respecto a la salvaguardia de la información, la privacidad de los detalles personales y el seguimiento de los mensajes en línea En situaciones en las que los eventos deben explicarse, realice controles internos o inicie sondas legales o administrativas, es crucial poseer métodos y reglas suficientes para el examen de evidencia digital que permitan un examen exhaustivo y legal de las actividades en estas plataformas

El escenario se vuelve más intrincado cuando se observa que numerosas organizaciones públicas han elegido el espacio de trabajo de Google como su entorno principal para las tareas institucionales. Este movimiento, a pesar de que significa una fase crucial en los métodos de actualización y un impulso importante en la productividad y la efectividad laboral, también plantea problemas importantes. Entre estos, un punto clave es asegurarse de que todos los datos creados e intercambiados por Google Meet puedan ser asegurados, verificados y examinados siguiendo las últimas reglas sobre seguridad y privacidad en línea.

Uno de los problemas clave que encontramos hoy en día en el examen forense digital es la ausencia de instrumentos particulares y métodos claros para manejar efectivamente la prueba digital creada a través de Google Meet, particularmente cuando ocurre en una configuración basada en la web Google Meet difiere de otras plataformas más privadas o de aquellas con

características combinadas para la grabación y el monitoreo centralizados, ya que utiliza el navegador web como el elemento principal de la experiencia del usuario, lo que lleva a los desafíos en la recopilación de confiables y

Esta ausencia de procedimientos directos plantea un desafío significativo para los expertos en investigación digital Estos expertos deben abordar la tarea de encontrar, eliminar y mantener una colección de elementos digitales importantes para cualquier estudio: desde registros de teléfonos, detalles sobre personas involucradas, datos sobre los archivos, el sonido y las transmisiones de video realizadas durante las reuniones No es suficiente adquirir estos componentes; También es crucial mostrar de dónde provienen, su importancia y su autenticidad, por lo que pueden ser aceptados como una prueba legítima en un procedimiento legal o administrativo

Cuando no se utiliza un enfoque estricto y uniforme, la prueba puede volverse menos importante En realidad, cualquier duda sobre su honestidad o el método de su reunión puede conducir a investigaciones sobre la precisión del examen forense, que socava la confiabilidad de las conclusiones y puede poner en peligro

En este estudio, nos concentramos en examinar este problema en profundidad, lo que sugiere y creando posibles correcciones técnicas para mejorar el método de recopilación de evidencia de Google Meet, siendo la configuración primaria el navegador web. El objetivo es crear un marco técnico sólido que actúe como una referencia inicial para los próximos estudios

forenses digitales, asegurando elementos básicos como la consistencia, la originalidad y la capacidad de registro de Data.

A largo plazo, el objetivo de estas sugerencias no es solo mejorar los métodos forenses, sino también para reforzar las habilidades institucionales en sectores cruciales como la seguridad cibernética, el examen digital y la investigación técnica de los eventos que tienen un sistema confiable para reunir pruebas en línea en lugares como Google se encuentran afectar significativamente cómo los problemas de seguridad se manejan en el mundo digital de hoy.

### *Justificación e importancia del trabajo de investigación*

En los últimos tiempos, el auge de las llamadas por video es innegable, tanto para temas personales como del trabajo. Esta moda surgió porque era necesario comunicarse bien a pesar de no estar cerca, algo que fue clave en eventos mundiales como la pandemia. Por esto, la opción de grabar videollamadas se ha vuelto muy popular, siendo una función que usan mucho los usuarios de distintos campos.

Plataformas como Google Meet se han vuelto muy importantes para facilitar la comunicación virtual cuando no estamos en el mismo lugar. Su uso se ha hecho fuerte en la educación, empresas y en el gobierno, permitiendo hablar de forma más ágil y eficiente. Pero, además de estas ventajas claras en cuanto a productividad, acceso fácil y flexibilidad, también han aparecido nuevos peligros relacionados con la seguridad de la información y el posible mal uso de estas plataformas.

Conforme nos apoyamos más en las aplicaciones de videoconferencia, también hay más chances de que se utilicen, a propósito, o sin querer, como medios para cosas ilegales o situaciones que pongan en riesgo a los usuarios. Ya hay muchos casos en los que delitos cibernéticos —como el acoso en línea, el robo de datos importantes, el fraude digital o el mostrar información sin permiso— empiezan o se hacen en una videollamada. Por eso, cada vez está más claro que estudiar las opciones de análisis forense en plataformas como Google Meet no solo es útil, sino muy necesario para mejorar la ciberseguridad y la protección digital.

Como pasa con cualquier herramienta digital, el uso de Google Meet crea ciertas cosas o "artefactos" en el sistema del usuario. Pueden ser archivos que duran poco, registros, historiales de lo que se busca en internet, configuraciones y otros datos que, aunque parezcan sin importancia, pueden tener información valiosa para un análisis forense. Sin embargo, las herramientas que hay hoy para encontrar, conseguir y analizar estos artefactos son pocas, lo que es un problema para los profesionales que deben hacer investigaciones serias en este campo.

Estas limitaciones afectan lo bueno que es, lo fiable que es y el valor que tienen los datos que se pueden sacar de una sesión de Google Meet. Esto es muy importante en juicios o procesos internos, donde la información digital puede servir como prueba para ayudar a tomar decisiones legales.

La cosa se pone peor al ver que muchas entidades del gobierno usan Google Meet para hablar de temas importantes, hacer planes e incluso tomar decisiones grandes. Por esto, es

urgente tener herramientas que aseguren que los datos que se producen se guarden bien y se estudien después, siguiendo procesos que aseguren que son fiables, verdaderos y que se pueda saber de dónde salieron.

Por otro lado, el asunto se vuelve aún más crítico si notamos el auge de plataformas como Google Meet en el sector público para temas muy serios. A menudo, estas organizaciones emplean las videoconferencias no solo para el día a día, sino para debates clave y decisiones que impactan a la institución y a la sociedad. La agilidad de estas herramientas ha cambiado la comunicación interna, pero exige más seguridad, control y seguimiento de la información.

Ante esto, es clave tener buenos métodos para obtener datos forenses, así como estrategias que mejoren constantemente y se adapten al mundo digital. Esto haría posible grabar, guardar y analizar la información de una videollamada de forma seria, sobre todo si se necesita como prueba en juicios, investigaciones internas o auditorías.

Con esta necesidad en mente, este estudio busca analizar qué tan forense es Google Meet. La idea es crear una propuesta técnica completa que ofrezca herramientas para encontrar, recopilar y analizar evidencia digital válida. Esta solución busca ayudar no solo a peritos forenses o policías, sino también a profesionales como consultores de ciberseguridad, administradores de redes, técnicos y otros que gestionan entornos digitales seguros.

Se prevé que los hallazgos de esta investigación ayuden a mejorar las herramientas y el saber hacer para el análisis forense de videollamadas. Además, se busca impulsar el uso de buenas prácticas en el manejo de evidencias digitales, vital para mejorar la respuesta a incidentes de seguridad, apoyar juicios con pruebas fiables y, en general, fortalecer la informática forense en ciberseguridad.

### *Alcance*

Este estudio revisa a detalle qué rastros deja usar Google Meet, viéndolo desde cómo va en navegadores web de computadoras. Lo hacemos así porque en oficinas, universidades y empresas, casi siempre se usan navegadores para las videollamadas por lo fácil que es, porque funciona en casi todo y porque no hay que instalar nada.

Nos quedamos solo en esto, sin meternos en cosas técnicas o problemas con Google Meet en celulares o apps aparte. Es que esas plataformas son distintas y guardan datos diferentes, así que necesitaríamos otra forma de revisarlas y eso ya sería mucho para este trabajo.

Vamos a ver cómo funcionan dos navegadores conocidos: Mozilla Firefox y Microsoft Edge. Guardan datos de forma diferente, como los archivos temporales, los historiales y los datos de sesión, y eso cambia los rastros que dejan cuando usas Google Meet. Saber esto es clave para ver qué información se puede sacar para investigaciones, y qué tan fácil o difícil es encontrarla según el navegador.

La investigación mirará bien las herramientas y métodos que hay para rescatar, guardar y analizar los datos que quedan después de las videollamadas. Esto es ver archivos temporales, cookies, la memoria caché del navegador, historiales y otras cosas que se guardan en la computadora y que pueden tener información útil para una investigación digital. Las pruebas se harán como si fueran casos de verdad, para asegurarnos de que los resultados sirvan en situaciones reales.

También, veremos las mejores maneras de guardar la evidencia digital, asegurándonos de que esté completa, que se sepa quién la tuvo y que se presente bien en juicios. Esto es importante para que la información valga como prueba y nadie dude si es real o no.

Es importante aclarar que este estudio no hablará de cosas como revisar el tráfico de red en el momento, ver transmisiones de video en vivo o el cifrado que usa Google Meet para proteger las conversaciones. Tampoco vamos a comparar esta plataforma con otras para videollamadas, porque lo que queremos es revisar a fondo una herramienta para sacar información específica que sea útil y se pueda usar directamente.

## *Objetivos*

### .1..1 Objetivo general.

Determinar herramientas y técnicas forenses para la identificación y análisis de artefactos digitales creados por Google Meet en navegadores web. Esto permitirá desarrollar una metodología clara que asegure la integridad de la evidencia recolectada.

### .1..2 Objetivo específico.

Identificar la información que genera y guarda distintos navegadores como , Firefox y Edge durante y después de una video llamada.

Evaluar las herramientas forenses disponibles para adquirir y analizar artefactos digitales en entornos controlados.

Crear una metodología clara para extraer y analizar de gorma sistemátca los artefactos relacionados con Google Meet.

Validar la eficiencia de la metodología creada mediante un caso de estudios con pruebas experimentales.

Elaborar recomendaciones sobre las buenas prácticas para profesionales forenses que trabajen en entornos web que utilicen Google Meet.

# Capítulo 2:

## 2. Revisión De Literatura

### *Estado Del Arte*

En los últimos años, los servicios de videollamadas han avanzado enormemente y se han convertido en herramientas indispensables para la comunicación instantánea y la colaboración. Tanto que en las organizaciones públicas como privadas, utilizan herramientas digitales para hacer videollamadas como, por ejemplo: Zoom, Google Meet o incluso Microsoft Teams para realizar reuniones virtuales, capacitaciones en línea, entrevistas, clases virtuales y eventos corporativos se están llevando a cabo a través de estas plataformas.

Una de las herramientas más utilizadas y confiables es Google Meet, esta es una solución de video conferencias, que se destaca por ser segura, confiable y sencilla de utilizar, lo que permite que muchos estudiantes y profesionales la utilicen (Google, 2025). Se ha vuelto popular porque viene como una aplicación integrada en Google y por su interfaz de usuario simple; además, es completamente basada en la web y no requiere que descargues ningún software. Sin embargo, el crecimiento de los datos recuperables también ha traído nuevos desafíos para el área de seguridad cibernética, lo cual es el caso del escenario de la informática forense.

Google Meet se ha convertido en una herramienta comúnmente utilizada para videollamadas en línea, pero hay un estudio limitado que se centra en la investigación forense de

Google Meet. Los informes existentes en su mayoría se concentran en sistemas comparables como Zoom o Microsoft Teams, y todavía hay una escasez de análisis en profundidad de los artefactos producidos por Google Meet en el curso de su operación. Esta brecha es alarmante, ya que Google Meet ha sido ampliamente adoptado en entornos institucionales, y la seguridad de la información y la posibilidad de realizar investigaciones digitales efectivas son consideraciones importantes.

Realizar un análisis forense es de suma importancia debido a que ayuda a los informáticos a identificar, documentar e interpretar información en situaciones legales o judiciales. Es importante conocer, que este análisis no se centra en frustrar delitos cibernéticos, sino, en investigar y descubrir datos cruciales que sirvan en una investigación legal. Dentro de un análisis forense se busca identificar pistas de casos de delitos cibernéticos, en el seguimiento de chats, correos electrónicos, entre otros. En los últimos años, la informática forense evolucionó, al igual que los ataques de los ciberdelincuentes, por lo que ahora recuperar y analizar la información almacenada en los dispositivos no es suficiente, ahora, es necesario también analizar los dispositivos que tienen gran capacidad de almacenamiento y que se encuentran conectados a la red y a la nube, debido a que en ellos se pueden encontrar direccionamiento de IP, registros de seguridad, redes, entre otros que pueden ayudar a que el profesional que realice el análisis (Bermudez, 2025).

De toda la literatura existente en este dominio. Solo unos pocos estudios han abordado el problema de recuperar evidencia digital de delitos sociales hasta ahora, y muchos de los estudios

realizados se concentran en la recuperación de evidencia digital dejada por los navegadores web al visitar plataformas sociales en línea. Estos artefactos están compuestos por archivos de caché, cookies, historiales de navegación, almacenamiento local y otros archivos que contienen datos sensibles o relevantes en un contexto forense. Algunos de los datos que se pueden obtener a través de estos elementos son pruebas de que ciertas funciones en la plataforma fueron utilizadas, ya sea participación en videollamadas, autenticaciones de usuario, URL de acceso a la reunión, marcas de tiempo y configuraciones transitorias que podrían proporcionar información valiosa en el contexto de una investigación digital.

Esta es una tarea compleja en Google Meet debido a cómo se procesa y almacena la información en cada navegador web. Estudios anteriores también encontraron que navegadores web como Mozilla Firefox y Microsoft Edge manejaban los datos relacionados con sesiones web de diferentes maneras. Estas divergencias no solo tienen un impacto en la disponibilidad de cultura y artefactos materiales específicos, sino que también impactan y definen los enfoques correctos utilizados para su recuperación y estudio. El almacenamiento en caché, el modo en que se guarda la información en el almacenamiento local (localStorage o IndexedDB) y el nivel de acceso que puede ser asignado a un registro particular difieren significativamente entre navegadores; por lo tanto, se hace necesario adaptar la extracción y el análisis para ellos.

Hasta donde sabemos, con respecto a conjuntos de herramientas dedicadas a realizar este tipo de análisis, se han reconocido varias soluciones forenses comúnmente utilizadas por los profesionales. Autopsy, que es un programa que realiza búsquedas forenses en volúmenes de

almacenamiento informático de código abierto (Autopsy, 2025), Magnet AXIOM (que es una plataforma integral de investigación digital que permite a lso examinadores adquirir y analizar datos forenses de manera fluída (Magnet Forensics, 2025), Browser History Examiner, que es una herramienta de software forense para capturar, analizar e informar el historial de Internet de los principales navegadores web de escritorio (Foxton Forensics, 2025), entre otras soluciones comerciales y de código abierto, han sido utilizadas de manera efectiva para analizar la actividad del usuario en navegadores web. Aunque estos no han sido diseñados o implementados específicamente para Google Meet, algunos de ellos producen visualizaciones de datos relacionados al examinar artefactos generados por navegadores. La efectividad de estas soluciones varía dependiendo de factores como el sistema operativo que estás utilizando, la versión del navegador y si hay configuraciones de privacidad del usuario o mecanismos de eliminación/cifrado automático de datos en su lugar.

Por el contrario, se han desarrollado metodologías generales para adquirir y analizar evidencias digitales en relación con la web, de acuerdo con los estándares internacionales de usabilidad que definen las mejores prácticas disponibles en el campo. En particular, ISO/IEC 27037 ofrece mejores prácticas para la identificación, recopilación, adquisición y preservación de evidencia digital. Este principio aboga por un proceso metódico y profesional para mantener la integridad de los datos en el trabajo forense. Pero también son pasos genéricos, por lo que ni siquiera se corresponden directamente con una tarea determinada, como el análisis de sesiones de Google Meet en un navegador web.

Por lo tanto, se requiere investigación dedicada para tener en cuenta las especificaciones técnicas de cada plataforma y su rendimiento en escenarios prácticos. Con Google Meet, encontramos necesario examinar los artefactos creados cuando ciertos factores están presentes (por ejemplo, navegador web utilizado; sistema operativo; acciones realizadas en una videollamada) para avanzar el nivel de conocimiento hacia su valor forense. Este trabajo se propone exactamente como un paso en esa dirección; cubre un campo altamente descuidado y una perspectiva técnica sobre ese tema que puede ayudar aún más a guiar la investigación y/o el desarrollo de herramientas especializadas o mejores prácticas en el contexto de la informática forense.

### *Planteamiento del problema*

Google Meet se ha convertido en una de las principales plataformas de videoconferencia a nivel mundial, permitiendo conectar en tiempo real a millones de personas y organizaciones. Su simplicidad, su conexión con el ecosistema de Google, así como su acceso a través de navegadores web, lo han llevado a un uso masivo en la educación, en el trabajo remoto, en la gestión pública y en la coordinación interinstitucional.

A esta velocidad de desarrollo, la informática forense ha enfrentado nuevos desafíos, por ejemplo, las plataformas de comunicaciones electrónicas (e-comm) con la privacidad y la recuperabilidad de artefactos forenses relacionados con información probatoria importante en una investigación digital.

En la actualidad, la informática forense se encuentra a varios retos, debido a que se encuentra en una época con sistemas computacionales separados y complejos, esto se refiere a que lo que antes se necesitaba de una presencia física, ahora se ejecuta de manera remota, en una interacción continua y fluida, estas acciones tienen lugar en plataformas que operan en varios niveles de tecnología, lo que complica las investigaciones. Un gran ejemplo es la transformación en Google Meet, el uso extendido y su diseño esencialmente basado en la nube han revolucionado la manera en que se produce y se recopila la evidencia digital, cada reunión y acción que un usuario lleva a cabo en esta plataforma, genera una gran cantidad de datos y huellas. Es fundamental reconocer que esta evidencia no solo se almacena en la infraestructura en la nube, sino que también se expresa y se registra de manera significativa en el dispositivo del usuario, especialmente a través de la interacción con el navegador. Esto implica que, para los expertos en forense, tener un conocimiento sólido sobre estos flujos de información y la capacidad para recuperarlos de manera completa es más importante que nunca. El realizar este trabajo incluye aprender a interpretar cómo estas complicaciones tecnológicas afectan la obtención de pruebas y, en última instancia, la búsqueda de la verdad.

Desafortunadamente, dicha evidencia no es fácil de reconocer, recuperar o interpretar, lo que representa un verdadero desafío para los expertos responsables de la investigación. Esta falta de documentación general y técnica sobre qué tipo de datos se generan localmente en los dispositivos de los usuarios y dónde se almacenan, no se pueden recuperar de manera confiable como evidencia en un proceso forense.

Aun así, hay más de 300 millones de usuarios mensuales de Google Meet, lo que convierte a Google Meet en la segunda plataforma de videollamadas más utilizada en el mundo, con un 29.39% de penetración de mercado (D'Souza, 2025). Esta falta de transparencia técnica dificulta la labor de los investigadores si el trabajo de investigación requiere recolectar evidencia sólida y precisa para entender qué está sucediendo en incidentes de ciberdelitos, accesos no autorizados, filtraciones de datos, robos de identidad, entre otros.

El desafío es aún mayor si tenemos en cuenta que Google Meet se ejecuta en el navegador y que hay diferentes arquitecturas en cada navegador para manejar los datos de peer-to-peer. Por ejemplo, Mozilla Firefox y Microsoft Edge almacenan los datos del usuario de diferentes maneras, tanto en disco como en memoria. Lo cual significa que la forma antigua de obtener los objetos digitales puede no ser suficiente, o incluso ser contraproducente si no está personalizada de manera interactiva para cada entorno.

Ante este panorama, es evidente que se requieren más estudios para localizar y describir las huellas digitales que deja Google Meet en los navegadores, discutir el desempeño de las herramientas forenses existentes en el análisis de esas huellas y concebir una metodología sólida y repetible conforme a las mejores prácticas de análisis forense digital. Esto no solo tiene consecuencias técnicas, sino también legales y organizativas, dado que la evidencia de baja calidad y/o parcial puede afectar la legitimidad de toda una investigación.

En este contexto, este documento se presenta como una respuesta a esta falta de detalles técnicos en los métodos y tiene como objetivo generar las bases para estrategias forenses al analizar plataformas de videoconferencia en escenarios reales.

Al ofrecer una metodología estructurada y sistemática que se ajusta al mundo actual, esperamos que esto proporcione las herramientas prácticas necesarias para mejorar la seguridad cibernética y la respuesta a investigaciones, tanto en el ámbito público como privado.

## *Marco Teórico*

### .2..1 Informática Forense.

La informática forense o ciencia informática forense es una rama de la ciencia forense digital que se ocupa de las pruebas encontradas en computadoras y medios de almacenamiento digital.

La función principal de la forense digital es la identificación, preservación, examen y producción de pruebas digitales de tal manera que sean tanto precisas como admisibles para su consideración en un tribunal o en una forma aceptable dentro de un campo de investigación (IBM, 2025).

En las últimas décadas, este campo ha avanzado rápidamente debido al uso generalizado sin precedentes de las tecnologías digitales en todas las áreas de la vida contemporánea y ha

estado respondiendo a una demanda creciente para abordar las ocurrencias que involucran el uso indebido de sistemas informáticos, redes y servicios digitales.

A diferencia de algunas otras disciplinas de ciencias de la computación, como la informática pura o las redes, los problemas de la informática forense involucran muchos insumos externos. Aquí se hace hincapié en un registro meticuloso de datos que puedan ser utilizados como prueba en un entorno judicial.

Para ello, es necesario utilizar metodologías rigurosas, procedimientos consistentes y herramientas especializadas que garanticen que la evidencia digital no se modifique durante los procesos de adquisición y análisis. En este sentido, uno de los aspectos clave de esta disciplina es la integridad de la evidencia, es decir, la capacidad de probar de alguna forma que los datos adquiridos no han sido alterados, manipulados o afectados de ninguna manera desde que fueron obtenidos hasta su presentación.

Por un lado, la informática forense es uno de los componentes más importantes para la respuesta a incidentes porque, mediante esta técnica, somos capaces de restaurar lo que sucedió, de dónde se derivó un ataque, quién estuvo involucrado y mantener un registro exacto de lo acontecido. Por otro lado, los resultados de las investigaciones forenses digitales ofrecen la oportunidad de reaccionar, y pueden mejorar los sistemas de seguridad, políticas y procedimientos al actualizar los requisitos sobre sistemas del pasado y aumentar la capacidad organizacional para prevenir amenazas cibernéticas.

Esta conexión ha dado lugar al desarrollo de metodologías consolidadas que incorporaron tecnologías de informática forense en el proceso de gestión de incidentes y ampliaron las dimensiones operativas y estratégicas de los dos dominios. En práctica, esto significa equipos multifuncionales que no solo descubren qué salió mal, sino que también ayudan activamente a dar forma al diseño de controles, la detección temprana de vulnerabilidades y la implementación de medidas de remediación para reducir la probabilidad de repetir el mismo error en el futuro.

El auge de los servicios en la nube, dispositivos móviles o redes corporativas intrincadas, por no mencionar los sistemas de comunicación digital como Google Meet, ha hecho que el trabajo de los expertos en informática forense sea más complejo. Ya no se trata simplemente de archivos eliminados o direcciones IP, sino de cómo funcionan internamente múltiples tecnologías, la forma en que los conjuntos de datos se almacenan en entornos virtualizados y encontrar la pistola humeante en un sistema distribuido y de difícil acceso.

La informática forense no es solo el proceso de analizar información de sistemas y redes informáticos para eliminar la duda o aclarar cómo se ha usado, almacenado, creado y eliminado la información cuando ha tenido lugar una actividad ilegal, sino también la validación de derechos digitales y la verificación de reclamaciones de seguros, disputas contractuales, fraudes corporativos y cumplimiento normativo. Sus efectos son amplios y ha trascendido sus límites legales y se ha extendido a esferas técnicas, convirtiéndose así en un campo estratégico para cualquier entidad digital compleja.

Como se mencionó anteriormente la informática forense es de suma importancia debido a que ayuda a los informáticos a identificar, documentar e interpretar información en situaciones legales o judiciales, y se debe tomar en cuenta que debido a la evolución de la tecnología en la actualidad, , es necesario también analizar los dispositivos que tienen gran capacidad de almacenamiento y que se encuentran conectados a la red y a la nube, debido a que en ellos se pueden encontrar direccionamiento de IP, registros de seguridad, redes, entre otros.

Por todas las razones mencionadas anteriormente, es necesario que los expertos en informática forense estén bien informados sobre los estándares, herramientas y técnicas que regulan y guían esta práctica. También es importante que sean capaces de operar en diferentes plataformas y entornos, como videollamadas basadas en navegadores web, donde la identificación y análisis de artefactos digitales requieren un enfoque específico y técnicamente riguroso.

### .2..2 Artefactos Digitales.

Las huellas de interacción entre un usuario y el sistema informático son artefactos digitales. Las cuales se podrían considerar huellas digitales, y son una parte integral del campo de la Computación Forense, que intenta rastrear movimientos que se han realizado en un entorno digital basado en datos que finalmente podrían almacenarse directa o indirectamente en dispositivos digitales. Estos artefactos pueden incluir archivos de registro, archivos temporales, historial de navegación, datos de configuración, cookies, tokens de autenticación, datos en

almacenamiento local o en bases de datos del navegador, o metadatos sobre la actividad del usuario (Miner, 2021).

Desde el punto de vista forense, el análisis de artefactos digitales es importante para determinar qué ocurrió exactamente en un sistema en un momento preciso. Alguna forma de detectarlos y examinarlos puede permitir que se descubran pruebas sensibles al tiempo o que se rastreen o confirmen plazos para el acceso, modificaciones a, o quién modificó qué y cuándo. El estado y la naturaleza de los objetos recuperados, y la manera de recuperarlos, son importantes en el contexto de las pruebas en una investigación forense digital.

En el caso de los sistemas de videoconferencia, como Google Meet, la investigación sobre objetos digitales es aún más importante. Ahora hay diferentes planes para este servicio de almacenamiento en la nube proporcionado por Google que dependen de la cantidad de almacenamiento que se busque. Esto representa un desafío para el análisis forense tradicional que históricamente se deriva de la recuperación de datos almacenados en los dispositivos locales del usuario (D'Souza, 2025).

Al igual que ocurre con la mayoría de las aplicaciones web, existen artefactos que el sistema operativo y el navegador dejan atrás y que podrían ser aprovechados por alguien malintencionado (quizá en menor grado aquí). Sin embargo, la naturaleza y cantidad de estos artefactos varían significativamente con el software de navegación web, la configuración del sistema, la actividad del usuario y el comportamiento de las herramientas de navegación web.

Los artefactos recuperables pueden incluir, entre otros, registros de autenticación, cookies de sesión, archivos de caché que contienen fragmentos de código, imágenes en caché, URL visualizadas, datos de almacenamiento local (por ejemplo, localStorage o IndexedDB) y un historial de navegación que refleja un patrón de uso de la plataforma.

Sin embargo, como resultado de la arquitectura del servicio Google Meet y estar vinculado a funcionar solo en la nube, muchos de estos datos, es decir, contenido de videollamada, lista de participantes de la llamada y mensajes de chat no se almacenan en el dispositivo local del usuario y, por lo tanto, no pueden ser accesibles de forma independiente, incluso mediante una herramienta forense. Esta situación nos anima a investigar los subproductos indirectos que se pueden derivar del navegador y el sistema operativo utilizando herramientas dedicadas.

Una de las partes más difíciles es que el almacenamiento de datos no es uniforme entre los navegadores web modernos. Por ejemplo, Mozilla Firefox y Microsoft Edge se encuentran en dos lugares diferentes para sus archivos temporales, cookies y otros datos. Esta variabilidad afecta la manera en que se diseccionan los objetos que nos interesan y exige que el examinador tenga un buen conocimiento técnico de cómo opera cada navegador y las mejores herramientas para manejar sus paradigmas de almacenamiento.

En este entorno, la identificación y examen de evidencia digital derivada de Google Meet en el navegador web es de importancia para el campo de la computación forense digital. No se

trata tanto de encontrar lo que el ojo desnudo puede ver, sino de comprender dónde los datos pueden estar esparcidos por un sistema, cuidando la cadena de custodia y no alterando la evidencia.

Por lo tanto, analizar artefactos digitales no es solo un enfoque técnico en el análisis de plataformas digitales, sino también un enfoque en analizar el rápido surgimiento de incidentes virtuales en plataformas de comunicación remota. Dada la naturaleza limitada de los datos, la importancia de la correcta identificación y análisis de dichos archivos es primordial, particularmente al realizar investigaciones eficaces y legales a nivel internacional en el campo del ciberdelito y la ciencia forense digital.2021).

Desde una perspectiva forense, el análisis de artefactos digitales es crítico para saber qué sucedió en un sistema en un momento particular. Al revelarlos, extraerlos y analizarlos, se puede recuperar evidencia basada en el tiempo y rastrear o verificar accesos, cambios, o quién tomó qué decisiones o acciones. Tanto la condición y calidad de los artefactos recuperados, como el método de su recuperación, son críticos para la validez de la evidencia recopilada durante una investigación digital.

El estudio de artefactos digitales se vuelve aún más importante cuando se piensa en plataformas de videoconferencia como Google Meet. Google Meet es una herramienta SaaS (Software como Servicio), por lo que gran parte del procesamiento y almacenamiento ocurre en la nube, particularmente en los servidores de Google. Esta situación plantea un desafío para el

análisis forense clásico que tradicionalmente se ha concentrado en la recuperación de datos almacenados localmente en los dispositivos finales de un usuario (D'Souza, 2025).

Como otras herramientas basadas en la web, hay huellas que el sistema operativo y el navegador recogen que pueden ser explotadas por un atacante (aunque en menor medida). Sin embargo, la cantidad y calidad de estos artefactos dependen en gran medida del software de navegación web, la configuración del sistema, la actividad del usuario y el comportamiento de las herramientas utilizadas para navegar por la web. Ejemplos de artefactos recuperables pueden incluir, pero no se limitan a, registros de autenticación, cookies de sesión, archivos de caché que contienen fragmentos de código o imágenes, URLs vistas, datos de almacenamiento local (incluyendo localStorage e IndexedDB), y un historial de navegación que muestra el uso de la plataforma.

Sin embargo, debido a la arquitectura de Google Meet y la naturaleza basada en la nube de sus operaciones, muchos de estos datos, es decir, contenido de la videollamada, lista de participantes de la llamada y mensajes de chat no se guardan en el dispositivo local del usuario y no son fácilmente accesibles de manera independiente sin una herramienta forense. Este escenario nos motiva a estudiar los artefactos indirectos que podrían extraerse del navegador y el sistema operativo con herramientas especiales.

Uno de los desafíos más difíciles es que los navegadores web modernos manejan el almacenamiento de datos de manera diferente. Por ejemplo, Mozilla Firefox y Microsoft Edge

tienen diferentes lugares donde guardan sus archivos temporales, cookies y otros datos. Tal variabilidad impacta en la manera en que se extraen los artefactos de interés, lo que requiere un conocimiento técnico profundo de cómo se comporta cada navegador y las herramientas óptimas para tratar con sus arquitecturas de almacenamiento.

En este contexto, localizar y analizar la evidencia digital relacionada con Google Meet en navegadores web es una habilidad importante para los practicantes de la informática forense digital. No se trata solo de identificar los archivos visibles, sino también de comprender adecuadamente los datos dispersos que podrían existir en todo el sistema mientras se mantiene el enlace en la custodia y se preserva la integridad de la evidencia.

Como resultado, el examen de artefactos digitales no es simplemente un método técnico de análisis, sino un elemento estratégico en el análisis de eventos virtuales que se desarrollan rápidamente en el contexto de plataformas de comunicación remota. La importancia de la identificación y análisis adecuados de estos archivos difícilmente puede sobreestimarse en términos de la implementación de investigaciones sólidas y legales conformes con los estándares internacionales en el ámbito de la ciberseguridad y la ciencia forense digital.

### .2..3 Navegadores Web.

Los navegadores web son un software esencial en la aplicación diaria de Internet. Son la interfaz entre los usuarios y los recursos disponibles en la red, permitiendo el acceso a sitios web y plataformas digitales, utilizando contenido en la nube y multimedia. Según Bodnar (2021), tales aplicaciones ayudan a los usuarios a moverse entre diferentes lugares digitales y trabajar, siendo algo así como los guardianes del vasto dominio de información y servicios que constituyen la web contemporánea.

Además de ser meramente herramientas de visualización, como su propósito original, los navegadores modernos se han convertido en sistemas complejos que combinan múltiples tecnologías: motores de renderizado, gestión de sesiones, almacenamiento local, base de datos temporal, extensiones que los mejoran. Por ejemplo, tanto Mozilla Firefox como Microsoft Edge han añadido algunas de las características más sofisticadas para mejorar la experiencia de navegación del usuario, proporcionar mejoras de rendimiento y reforzar la privacidad y seguridad. Esto ha transformado al navegador de ser una mera interfaz para acceder a la web a ser un participante activo en el manejo de datos y la interacción directa con servicios web como Google Meet.

Existe un punto de vista de la informática forense en el que el navegador es particularmente importante. La interacción de cualquier usuario con cualquier aplicación web resulta en una multitud de huellas digitales que quedan en el dispositivo individual. Estas huellas

(también conocidas como "exhausto digital" en algunas literaturas previas), que pueden quedar dentro del entorno informático, pueden comprender, por ejemplo, archivos de caché, cookies, URLs, tokens de autenticación, entradas de almacenamiento local, bases de datos del navegador y metadatos. Estos elementos hacen posible la reconstrucción de la historia (atribución de eventos, patrones de uso, acceso no autorizado, etc.) o la presencia de un usuario en una o más plataformas.

Esta información no es manejada uniformemente por todos los navegadores. Cada uno tiene su propio método de guardar, tanto en dónde en su sistema operativo se almacenan los archivos como en cómo se formatea la información. Echa un vistazo a Mozilla Firefox que utiliza bases de datos SQLite para gestionar cosas como el historial de navegación (places.sqlite) o cookies (cookies.sqlite) y Microsoft Edge (construido sobre el motor Chromium) donde una nueva estructura, reuniendo las rutas de almacenamiento basadas en Windows que las políticas corporativas también pueden impactar cómo los datos se conservan o se eliminan. Estas idiosincrasias deben tenerse en cuenta al realizar análisis forenses ya que impactan la visibilidad de la evidencia y los métodos apropiados de adquisición de datos.

El uso del navegador también conlleva inconvenientes y limitaciones relacionadas con la persistencia de la información. Se supone que características como la navegación privada o el modo incógnito eliminan todas las huellas locales de la actividad del usuario. Además, en muchas configuraciones hoy en día se eliminan automáticamente las cookies y los archivos temporales cuando cierras el navegador, e incluso usan cifrado y aislamiento de sesiones. Estos

factores pueden dificultar la identificación y recuperación de artefactos relevantes para una investigación forense, particularmente cuando la adquisición del entorno se retrasa.

Por otro lado, los navegadores web contemporáneos también sirven como repositorios temporales de datos para aplicaciones alojadas en plataformas basadas en SaaS (Software como Servicio) (por ejemplo, Google Meet). Como son basadas en navegador y no requieren ninguna instalación, estas plataformas dejan pocos artefactos en la máquina local, pero podría accederse a datos ulteriores (por ejemplo, prueba de autenticación, URLs visitados para la reunión, huellas de participación, o datos temporales almacenados durante la sesión). La identificación y el análisis adecuados de estas huellas dependen del conocimiento interno sobre cómo cada navegador interactúa con la plataforma dada.

El comportamiento de los navegadores también puede ser influenciado por sus versiones, complementos instalados o los sistemas operativos en los que están instalados. Las modificaciones a la privacidad, la actualización automática o los servicios externos pueden cambiar la ruta de almacenamiento, los privilegios de acceso y la información conservada en la memoria. Los analistas forenses deben estar actualizados sobre esto y ser capaces de ajustar sus habilidades al entorno específico en el que se analiza el repositorio.

Así, en el contexto de un examen forense de plataformas, como Google Meet, el navegador emerge como un elemento técnico crucial. No solo se utiliza para obtener acceso a la plataforma, sino que también puede ser una fuente potencial de evidencia digital. Conocer cómo

opera, cómo almacena y las limitaciones que impone es esencial para proporcionar hallazgos verdaderos y confiables en una investigación digital.

### .2..4 Google Meet.

Google Meet es un servicio de videoconferencia desarrollado por Google que, anteriormente, era parte de G Suite de Google (rebautizado como Google Workspace en diciembre de 2020). Su objetivo principal es proporcionar una forma fácil, eficiente y confiable para reuniones virtuales y se integra bien en el entorno de Google: Correo, Calendario, Drive. Esta inclusión ha contribuido a su adopción global en sectores públicos y privados, convirtiéndolo en uno de los sistemas de videoconferencia más comunes a nivel mundial (GCF Global, 2021).

Una de las características destacadas es la capacidad de transmitir audio y video en alta definición, lo cual es crucial para asegurar que la calidad no se vea comprometida cuando se comunica en espacios virtuales. En cuanto a accesibilidad, la plataforma integra una herramienta de transcripción que genera subtítulos en tiempo real a través del reconocimiento de voz, transcribiendo las contribuciones de los participantes de la sesión. Esta característica también es útil en entornos escolares o educativos o en cualquier reunión donde los asistentes puedan tener discapacidad auditiva.

En cuanto a características, Google Meet tiene varias basadas en el tipo de cuenta utilizada. Las cuentas personales gratuitas, que generalmente se acceden a través de una

dirección de Gmail, están limitadas en cuanto a la duración de las reuniones y los participantes. Por otro lado, las cuentas con licencia de Google Workspace se benefician de más de un mero límite de 1 hora en las reuniones (con capacidad para grabar reuniones completas, así como salas de espera, herramientas de moderador en sesión, grabación avanzada de sesiones, controles administrativos para el creador de la reunión, y más).

Una de las características más significativas de Google Meet para la informática forense digital es que es completamente una aplicación web. Es lo que se conoce como un software de texto a voz basado en navegador. Mientras que, por un lado, ofrece los beneficios de portabilidad y usabilidad, por otro lado, crea un punto de preocupación técnica para reconocer y extraer evidencias digitales. Como servicio basado en la nube, la mayor parte de los datos creados durante las sesiones video, audio, asistentes o mensajes de chat se procesan y mantienen directamente en los servidores ubicados en las instalaciones de Google, fuera de la jurisdicción local del investigador forense.

Pero, al usarlo, Google Meet puede producir rastros en el dispositivo del usuario de forma indirecta, particularmente a través del navegador web. Los artefactos pueden consistir en archivos de caché relacionados con la transmisión de audio y video, cookies de sesión y autenticación que se utilizan para controlar el acceso del usuario a la plataforma, rastros o registros que pueden verse en la consola del navegador, especialmente cuando alguien había iniciado sesión en sus herramientas de desarrollador, y entradas en el historial de navegación que indican las fechas y horas en que alguien accedió a una reunión segura o la URL a la que

accedieron (GCF Global, 2021). Aunque estos no revelan directamente datos sobre el contenido de las videollamadas, pueden ser útiles para reconstruir los eventos, probar que un usuario participó en una sesión o vincular actividades a una línea de tiempo forense.

Además, el diseño de Google Meet también tiene una cadena de procesos en el navegador que puede generar artefactos efímeros. Estos pueden almacenarse en archivos temporales, en almacenamiento local, como localStorage o IndexedDB, o incluso simplemente en la RAM del sistema, dependiendo del navegador que estés usando. La longevidad y accesibilidad de tales artefactos, debido a varios problemas, como configuraciones del navegador, políticas de privacidad aplicadas o el comportamiento del usuario, requieren una técnica detallada adaptada al entorno específico.

Debido a su creciente utilización, principalmente en áreas críticas como la administración pública, la educación, o las empresas que trabajan con datos sensibles, resulta crucial conocer cómo funciona Google Meet desde un punto de vista tecnológico, qué tipo de datos se pueden recuperar localmente y qué herramientas y metodologías son viables para la investigación en escenarios de informática forense digital.

### .2..5 Almacenamiento Local.

El almacenamiento local es una piedra angular del navegador contemporáneo, almacenando una variedad de datos generados localmente durante el uso del usuario con varias páginas y servicios web. Estos datos pueden incluir elementos como cookies, archivos de caché e historial de navegación de esa máquina, así como configuraciones de sitios web y otros elementos para mejorar la usabilidad. Un ejemplo de para qué se utiliza este tipo de almacenamiento es que navegadores como Mozilla Firefox y Microsoft Edge pueden usarlo para

mejorar el rendimiento recordando las preferencias de usuario y permitiendo acceder a contenido previamente visitado (Cookie Script, 2025).

Técnicamente, el almacenamiento local puede tener diversas formas y dimensiones. Los navegadores web no solo almacenan archivos de texto simples, sino también aspectos complejos como bases de datos, incluyendo SQLite, que permite potentes consultas tipo chance. Y, por supuesto, utilizan localStorage, sessionStorage e IndexedDB, permitiendo que los datos sean escritos y leídos de forma persistente o temporal en su navegador sin una conexión activa a un servidor. Estos mecanismos fueron introducidos inicialmente para aumentar la funcionalidad y usabilidad de los sitios web, pero pueden ser un elemento informativo/evidencia importante durante las investigaciones forenses digitales.

Los datos almacenados localmente pueden estar ubicados en lugares que difieren según cada sistema operativo (SO) y contenedor de navegador. Por ejemplo, en Windows, Firefox guarda los archivos en carpetas de perfil de usuario, mientras que Edge utiliza rutas del entorno de Microsoft que tienen ciertos nombres y representaciones. Esta dispersión y heterogeneidad de formatos demanda una profunda especialización por parte del analista forense para reconocer correctamente los artefactos pertinentes y extraerlos sin dañar su validez.

Uno de los aspectos más importantes del almacenamiento local es que una cantidad significativa de evidencia digital vinculada a la interacción con plataformas como Google Meet puede capturarse en estos tipos de archivos. Aunque la mayoría de los datos que procesa Google

Meet se mantienen en la nube, al ser una aplicación web, pueden existir trazas de uso, tales como cookies de sesión y video y audio en caché en el navegador, URLs web y otros metadatos. Estos elementos, retenidos localmente, pueden servir para confirmar la presencia de un usuario en una sesión, la fecha y hora de la conexión o incluso la actividad realizada durante una reunión virtual.

Además de esto, la información almacenada localmente permanece intacta incluso después de cerrar el navegador o la sesión (a menos que tenga el sistema configurado para limpiarlo). Esto presenta una amplia ventana forense para el examen, suponiendo que el examen se realice de manera oportuna y se utilice la tecnología adecuada para adquirir los datos. También debemos señalar que la extracción de estos datos debe seguir los principios de preservación de evidencia (el proceso no debe escribir sobre los datos originales y debe mantenerse la cadena de custodia).

Involucrando escenarios de investigación digital, el almacenamiento local desempeña un papel importante al potencialmente contener información importante no disponible de otra manera. Es por eso por lo que los profesionales en informática forense necesitan comprender cómo funcionan los diferentes navegadores, dónde se almacenan los archivos que se utilizan internamente, cómo están estructurados y qué utilidades o dispositivos son más útiles para examinarlos sin afectar la integridad y admisibilidad de la evidencia.

### .2..6 Herramientas forenses.

En el ámbito de la informática forense, las herramientas se convierten en un apoyo básico para adquirir, preservar, analizar y presentar pruebas digitales forenses. Estas soluciones operan bajo los principios de integridad, trazabilidad y fiabilidad, asegurando que los investigadores puedan reunir pruebas sin modificar los datos originales, lo cual es necesario en los procesos legales o administrativos para que la evidencia sea admisible.

Para la investigación en actividades web mediadas por computadora, existen varias herramientas de auditoría que apoyan el análisis de rastros digitales de actividad de navegación. Estas herramientas pueden recuperar el historial de navegación, cookies, archivos de caché, registros de sesiones grabados, etc., elementos que pueden aplicarse para reprocesar las acciones del usuario. Hay algunas soluciones profesionales destacadas en esta industria, como Autopsy, Magnet AXIOM, Browser History Examiner, X-Ways Forensics y FTK Imager, que proporcionan operaciones específicas para diferentes casos de análisis.

La que se utilizará en el actual proyecto de graduación es el FTK Imager, desarrollado por Exterro, que se emplea ampliamente en investigaciones forenses por la posibilidad de adquirir imágenes forenses de discos duros, particiones, volúmenes o archivos aislados, por supuesto, sin cambiar el contenido original. Esta es una característica crucial para garantizar que la evidencia recolectada se mantenga en su estado probatorio original y pueda ser auditada por terceros. FTK Imager permite visualizar datos antes de la adquisición, crear copias bit a bit de discos, analizar el contenido de volúmenes físicos o lógicos y produce archivos hash para asegurar que los datos extraídos sean sólidos (Exterro, 2023).

Uno de los principales beneficios de FTK Imager es el hecho de que puede realizar una imagen (crear una copia bit a bit) del dispositivo de almacenamiento fuente, asegurando así que los datos originales no han sido alterados, eliminados ni comprometidos. Esto también permite que la evidencia auténtica se mantenga en su forma verdadera, así como el hecho de que cada parte de la investigación forense pueda ser documentada. En el contexto de una investigación, una cadena de custodia adecuada y la capacidad de testificar sobre los resultados en un tribunal de justicia dependen de tales técnicas.

FTK Imager también es compatible con muchos sistemas de archivos, lo que lo hace útil para las condiciones del sistema operativo del usuario. En el presente estudio, utilizaremos esta herramienta como un método adicional para capturar y analizar artefactos digitales que se hayan guardado en navegadores web locales, específicamente durante el uso de la plataforma Google Meet. Este instrumento nos permitirá examinar los lugares exactos donde los navegadores almacenan los datos sobre las sesiones activas, cookies de autenticación, cachés de contenido multimedia y otros tipos de datos que pueden constituir la evidencia digital crítica en un análisis forense.

Gratis y con una Guía de Usuario Sólida. Como un producto gratuito con documentación técnica bastante extensa, el FTK Imager proporciona una herramienta forense fácil de usar para quien hacer una inversión con un presupuesto ajustado no debería ser un problema. Sus

características, precisión y adherencia a los principios de recolección de pruebas forenses lo convierten en un miembro crítico del repertorio de utilidades de investigación digital.

La implementación de software como FTK Imager en este contexto no solo añade credibilidad a la metodología utilizada, sino que asegura que los resultados obtenidos puedan ser replicados, verificados y también respaldados técnica y legalmente.

### .2..7 Metodología Forense.

La base de la metodología forense es una investigación sistemática y estructurada de fallos, errores y problemas de sistemas tecnológicos, con la intención de identificar sus raíces y reconstruir eventos. Este método combina los conceptos de ingeniería con la solidez del método científico para analizar elementos o sistemas que no funcionan como se pretende y permite un estudio profundo e imparcial de los percances.

En el entorno digital, la práctica forense atiende a las diversas características de los entornos de hardware y de red y a la preservación/recolección de información, sin la cual la evidencia se compromete y se invalida (Sedgwick, 2023).

Su uso al planificar un estudio en la web implica una serie de pasos bien pensados para conducir la investigación empírica de manera sólida y replicable. Dado que los servicios web, como Google Meet, producen objetos digitales distribuidos por varias partes de la infraestructura, es importante que el análisis se realice de una manera que permita un proceso

controlado y documentado de identificación, adquisición, preservación, análisis y reporte de la información.

Preservar la evidencia digital es una de las técnicas más importantes de la informática forense y debe hacerse de manera que se mantenga la integridad de los datos originales sin ninguna modificación o destrucción de estos. Esto es posible mediante el uso de procedimientos particulares de adquisición forense para generar imágenes o copias exactas de los sistemas involucrados, que garantizan no interferir en la evidencia mientras se realiza una credibilidad de los resultados del examen, utilizando algoritmos de hash y registros de cadena de custodia.

A continuación, el proceso presenta una etapa de análisis que emplea técnicas específicas para investigar evidencias digitales, interpretar el contenido de los mensajes y correlacionar eventos. Dicho análisis debe realizarse de acuerdo con criterios técnicos específicos y estándares internacionales, permitiendo un resultado reproducible y susceptible de su validación en prácticas legales o institucionales.

En el contexto de estudios en plataformas web, encontramos particularmente relevante tener en cuenta las idiosincrasias del entorno, incluyendo la diversidad de navegadores, políticas de privacidad, almacenamiento local y la arquitectura de aplicaciones SaaS. La metodología forense debe responder a estas variables mediante la recolección de evidencia a través de un riguroso proceso de laboratorio profundamente arraigado en los casos técnicos en cuestión.

Además, el registro meticuloso de cada fase del proceso es esencial para preservar la transparencia y la trazabilidad en el análisis. Esto implica la especificación exacta de las fuentes de datos, el método de adquisición, las herramientas de análisis y/o los resultados obtenidos. Todo esto ayuda a construir la cadena de custodia y a que la evidencia pueda ser utilizada de manera confiable en juicio o administrativamente.

Por último, el proceso forense está dirigido tanto a la determinación de causas y responsabilidades como a proporcionar recomendaciones que mejoren la seguridad y prevengan incidentes futuros. Es en esto en lo que constituye el componente táctico importante de la gestión de ciberseguridad más amplia y en reforzar los requisitos para la protección de la información en un mundo digital (Sedgwick, 2023).

### .2..8 FTK Imager.

FTK Imager es una herramienta forense ampliamente utilizada en la informática forense. Se sabe que AccessData es su desarrollador. Este programa se utiliza para capturar imágenes y leer de vuelta los medios desde el hardware forense.

La característica más atractiva es la capacidad de replicar estas imágenes sin alterar ni modificar la evidencia existente, apoyando la integridad y admisibilidad legal de la evidencia

digital y utilizada en un entorno judicial o de investigación, tanto para el análisis como para la visualización (AccessData Group, 2025).

Una de las características más agradables de FTK Imager es que te permite ver una vista completa del contenido de un disco (no solamente lo que es visible y está en uso en este momento), incluso si alguien intentó ocultar el archivo o borrarlo de manera forense.

La escalabilidad de una investigación permite a los investigadores interrogar datos que de otro modo serían considerados como inactivos o perdidos, aumentando la cantidad de datos disponibles con los cuales reconstruir e identificar actividades. Debería quedar claro que el potencial de recrear eventos se ha expandido enormemente desde la rutina analítica forense tradicional.

FTK Imager también te permite informar tus hallazgos, asegurando que toda la evidencia que has descubierto en tu investigación forense sea fácil de reportar también. Estos informes contienen metadatos tales como fechas y horas, tamaño de archivo, ruta de acceso, hash para incluir cierto nivel de integridad y autenticación de datos. Estos registros son críticos para mantener la cadena de custodia y la integridad del proceso forense.

La herramienta funciona con una amplia gama de sistemas de archivos e interfaces de medios de almacenamiento y puede usarse en todos los sistemas operativos populares, incluidos

los de la última generación de dispositivos. Es una herramienta poderosa, aún más en la práctica forense donde existe una gran diversidad tecnológica que permite estandarizar un procedimiento y aplicar la misma solución a muchos casos.

En un entorno forense que trata con evidencia producida por aplicaciones web como Google Meet, es crucial para los investigadores capturar datos del navegador local de manera persuasiva con FTK Imager.

Facilita al analista forense desarrollar imágenes de flujo de bits de dispositivos de almacenamiento y volúmenes en cualquier herramienta de Windows, lo que a su vez retiene los datos disponibles para el sistema operativo Windows que pueden analizarse sin realizar ninguna modificación.

Además, la interfaz amigable para el usuario y lo que ves es lo que obtienes de FTK Imager hacen que la herramienta sea adaptable para profesionales en forense desde principiantes hasta expertos, de modo que ellos, en lugar de la herramienta, lleven a cabo la mayoría de las tareas relacionadas con la adquisición de evidencia, lo que hace que el proceso de adquisición sea más rápido y reduce el potencial de error humano al procesar la evidencia.

Por último, pero no menos importante, el uso de FTK Imager otorga integridad al proceso forense y validez profesional, ya que la tecnología, y la metodología por extensión, cumplen con

los criterios internacionalmente aceptados empleados para la preservación y examen de la evidencia digital. Esto es tranquilizador con respecto a los resultados y la robustez de esta herramienta ante problemas desafiantes en ciberseguridad e informática forense.

### .2..9 DB Browser for SQLite.

DB Browser para SQLite (DB4S) es una herramienta visual de alta calidad, de código abierto, para crear, diseñar y editar archivos de bases de datos compatibles con SQLite. Esta utilidad permite a los especialistas forenses leer directamente los archivos de bases de datos que contienen estas piezas de información restringida (por ejemplo, el historial de navegación), así como una variedad de otros restos digitales que son creados por múltiples programas y navegadores web. Entre los archivos más vistos utilizando esta utilidad están el historial y los archivos `places.sqlite`, que se centran en la información y a menudo contienen datos de actividad en internet del usuario (SQLite, 2025).

La contribución de DB Browser para SQLite a la investigación forense se proporciona mediante su método eficaz de ejecutar scripts SQL más complejos y personalizados, lo que a su vez agiliza la selección y clasificación de bases de datos complejas de piezas individuales de evidencia. Exactamente, lo necesitamos para un análisis preciso de eventos digitales, análisis de uso y recopilación de evidencias de calidad judicial. Además, como una herramienta de código abierto, los investigadores pueden personalizar el software y añadir nuevas características para adaptarlo a cada caso.

Desde su irrupción en el mundo de la informática forense, Belkasoft ha desarrollado software forense informático original y potente que permite adquirir y analizar evidencia digital, además de desarrollar y analizar productos forenses. Una de sus aplicaciones más famosas es el Belkasoft Live RAM Capturer, una herramienta especializada desarrollada para extraer datos de la RAM de un sistema vivo. Otra captura que necesita realizarse es la captura volátil (información recuperable no guardada en el disco), como: sesión válida; contraseña en uso; y procesos activos (Belkasoft, 2025).

El análisis e imagen de RAM utilizando herramientas como el Belkasoft Live RAM Capturer permite obtener una "instantánea" de un sistema en funcionamiento que mostrará claramente cómo se estaba utilizando el sistema en el momento de la adquisición, y podría potencialmente devolver evidencia relevante de actividades que de otra manera serían imposibles de obtener si tales actividades se realizaron y la imagen inicial fue infructuosa. Esta información basada en volátiles sirve para reforzar (no sobrescribir) el análisis de artefactos almacenados (en bases de datos SQLite, véase abajo) y el examen de otros medios localizados en el dispositivo (señalado abajo) para crear una imagen holística de lo que el sistema ha estado haciendo y cómo el usuario ha estado interactuando con el sistema, para formar la imagen completa.

Herramientas como DB Browser para SQLite y Belkasoft Live RAM Capturer son, de hecho, herramientas vitales para el examinador forense informático, capaces de examinar tanto datos estáticos como volátiles y cruciales para un examen forense completo de la evidencia.

### .2..10 Volatility3.

La RAM, siendo la memoria volátil del ordenador, contiene evidencia vital que puede adquirirse utilizando diversas herramientas forenses como Volatility. Volatility3 es una herramienta muy popular que se utiliza en el análisis forense observado en RAM. Esta herramienta ayuda a extraer información vital que descansa exclusivamente en la memoria volátil del sistema. A diferencia de otros tipos de análisis enfocados en discos duros o archivos persistentes, esta herramienta te permite explorar el contenido de la memoria activa del sistema operativo en el momento en que se capturó la memoria, lo cual se dice que es muy importante en algunas investigaciones, donde el tiempo juega un papel crucial (Volatility Foundation, 2025).

Esta utilidad hace uso de módulos o plugins específicos para explorar muchos elementos del sistema. Los casos de uso común son el listado de procesos en ejecución, conexiones de red abiertas, archivos abiertos, contenidos de claves de registro y la recuperación de artefactos sensibles como credenciales temporales o cargas útiles de malware en ejecución sin escribir nunca en el disco. Toda esta información puede ser vital para desentrañar qué exactamente estaba ocurriendo en un sistema antes, durante o después de un incidente.

Volatility3 es la siguiente iteración de este grupo de herramientas, desarrollada para tener mayor compatibilidad con sistemas contemporáneos y un análisis más detallado en entornos actuales, por ejemplo, sistemas Windows 10, Windows 11 y versiones recientes de Linux y macOS. En contraste con las diversas series de código de Volatility2, Volatility3 fue reimplementado en Python 3, aumentando la facilidad de mantenibilidad, extensibilidad, y ciertamente, eficiencia en casos de análisis complejos.

En la informática forense, herramientas como estas son otro componente importante del rompecabezas para un análisis más intensivo, ya que la memoria es uno de los medios más poderosos para identificar la presencia de amenazas avanzadas que operan en segundo plano o desaparecen durante un reinicio. Un número de técnicas utilizadas por adversarios avanzados, como malware en memoria o manipulación de procesos en memoria, son detectables solo basándose en este tipo de análisis, de ahí que herramientas como Volatility3 sean casi obligatorias en investigaciones de alto nivel.

Aunque se necesita un nivel de experiencia técnica, SIFT tiene buena documentación y una comunidad entusiasta de usuarios en el campo de la seguridad y la forense que ayuda a las personas a usarla diariamente para realizar sus trabajos. Y al ser una herramienta de código abierto, puede adaptarse y ajustarse para responder al entorno digital a lo largo del tiempo.

Volatility3 no solo ayuda a determinar qué ocurrió en un sistema, sino también cómo y cuándo ocurrió, una pieza crítica para ensamblar los eventos y luego identificar debilidades para el futuro. La capacidad de trabajar estrechamente con volcados de memoria permite al investigador recuperar datos transitorios, con frecuencia la evidencia más incriminadora en un examen forense.

**Capítulo 3:**

## 3. Desarrollo

## *Desarrollo del Trabajo*

### Metodología

Este trabajo de titulación se va a desarrollar de forma práctica, haciendo pruebas en un entorno controlado que simula el uso real de Google Meet desde navegadores web. El objetivo es identificar y analizar los archivos o artefactos que se generan en el equipo después de realizar una video llamada, y que pueden servir como evidencia digital.

### Entorno de trabajo controlado

Para desarrollar el trabajo de titulación se utilizó lo siguiente:

- Sistema operativo: Windows 10, 64bits
- Navegadores web: , Mozilla Firefox y Microsoft Edge
- Herramientas Forenses: FTK Imager, DB Browser for SQLite, Belkasoft Live RAM Capturer
- Volatility3

### Procedimiento

1. Utilizar Google Meet

Se debe abrir cada navegador y conectarse a una videollamada de prueba en Google Meet, aquí se deben realizar varias acciones como: encender la cámara, encender el micrófono, escribir en el chat, compartir pantalla, utilizar los subtítulos, participar en la llamada durante algunos minutos.

2. Adquisición de datos con la herramienta forense

Una vez realizadas las acciones del paso anterior, abrir la herramienta forense FKT Imager para hacer copias forenses de las carpetas donde cada navegador guarda la información localmente. Normalmente las ubicaciones suelen guardarse en la siguiente ruta: C:\Users\(Usuario)\AppData\Local\(Nombre del Navegador) \User Data\Default.

3. Análisis de los artefactos

Con los datos adquiridos por la herramienta forense FKT Imager, se deben revisar los archivos que quedaron en almacenados en el equipo e iniciar a analizarlos, se debería poder encontrar información como el historial de navegación con acceso a Google Meet, los archivos temporales o de caché, cookies y archivos de almacenamiento. Es importante destacar que esta práctica es realizada con fines académicos, no se afectan a terceros y tampoco se utiliza información confidencial de ningún miembro del equipo o externo.

## Desarrollo

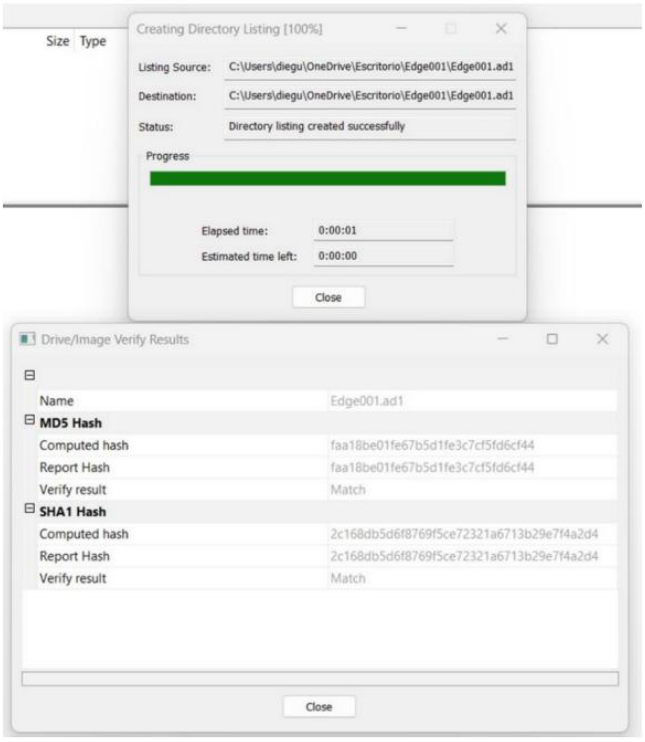
Para llevar a cabo la adquisición y el análisis forense de los artefactos generados por Google Meet cuando se utiliza en diferentes navegadores web en un sistema operativo Windows 10, primero se mostrará el proceso práctico, el objetivo principal es demostrar cómo se pueden obtener evidencias digitales de las acciones realizadas durante una video conferencia.

Para ello primero se configuró un entorno controlado donde se pudieron realizar videoconferencias reales utilizando tres diferentes navegadores: , Mozilla Firefox y Microsoft Edge.

A continuación, se crea imagen utilizando FTK Imager, se genera un informe del contenido de la imagen forense con extensión .ad1, como se muestra en la Figura 1.

**Figura 1**

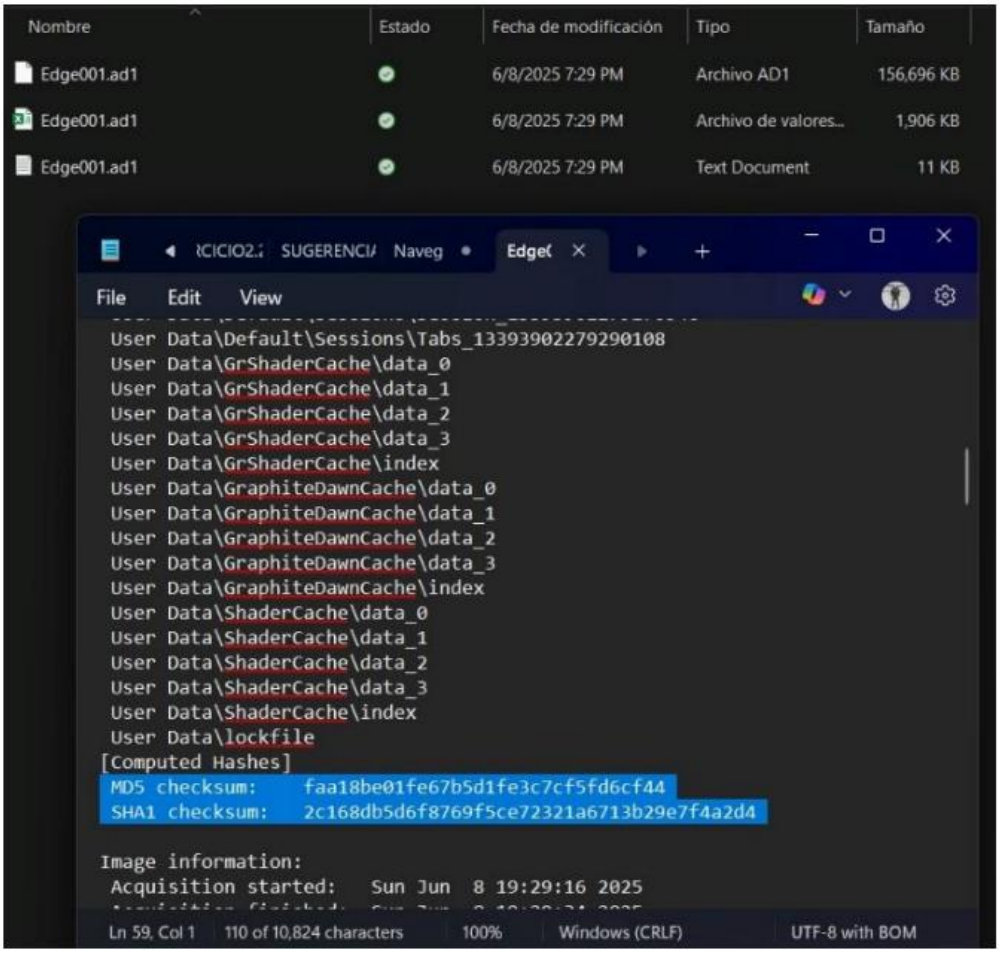
Creación de Imagen con FTK Imager




Se elabora un informe mediante la herramienta FTK Imager, el cual presenta un resumen detallado de los archivos identificados dentro de la imagen forense, incluyendo información relevante sobre sus metadatos. Esta información se visualiza de manera clara y estructurada, como se ilustra en la Figura 2.

**Figura 2**

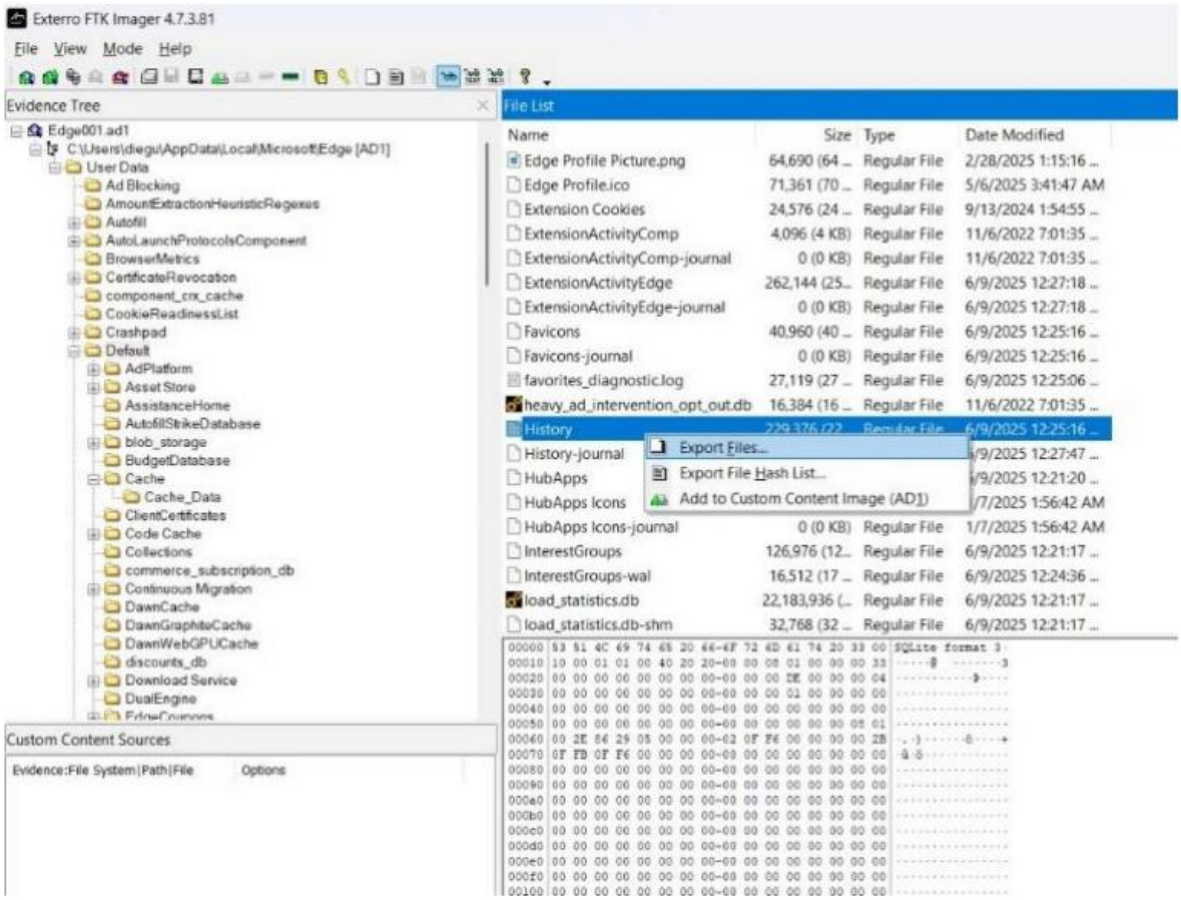
Generación de Reporte con FTK Imager




Se lleva a cabo un análisis forense del navegador Microsoft Edge con el objetivo de identificar posibles evidencias relacionadas con el uso de la plataforma Google Meet. Para ello, se procede a la extracción del archivo History, el cual almacena el historial de navegación del usuario. Este archivo resulta fundamental para rastrear accesos al dominio meet.google.com y permite la reconstrucción de una línea temporal de eventos vinculados a su uso, como se ejemplifica en la Figura 3.

**Figura 3**

Análisis Forense en el Navegador

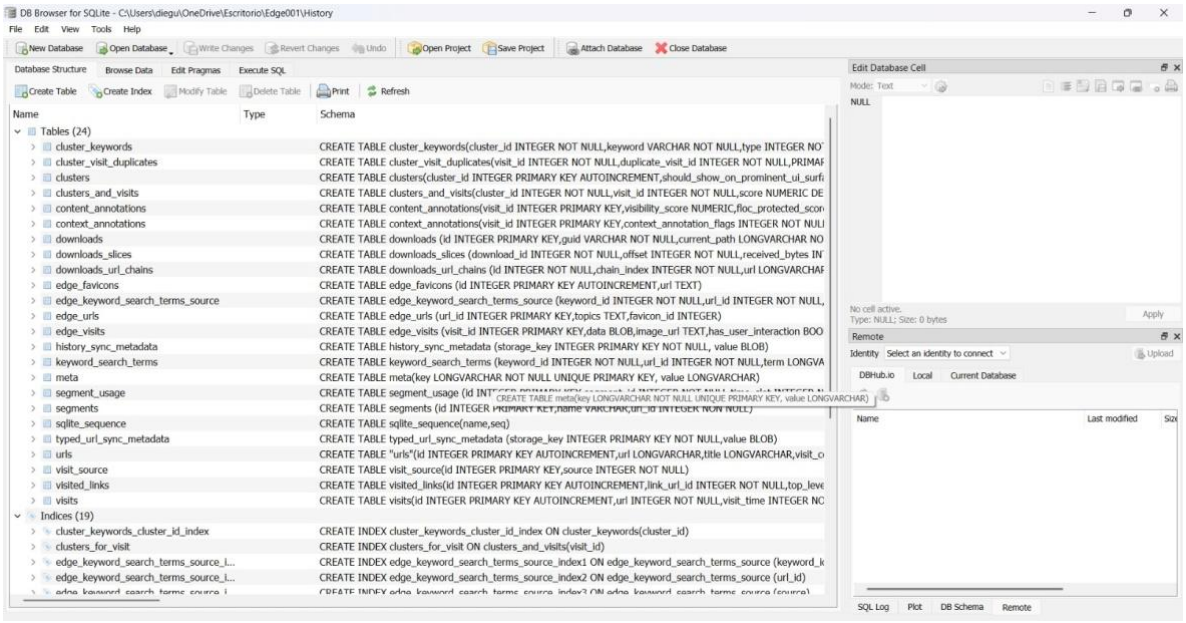



Como parte del análisis de artefactos forenses vinculados al uso de Google Meet, se utiliza la herramienta DB Browser for SQLite para examinar minuciosamente el archivo History del navegador Microsoft Edge. Este archivo, estructurado en formato de base de datos SQLite, contiene registros detallados de la actividad de navegación del usuario. A través de esta herramienta es posible acceder a dicha información de forma clara y organizada, como se ilustra en la Figura 4. El objetivo principal de esta fase del análisis es identificar accesos a meet.google.com, obteniendo con precisión las fechas y horas correspondientes, lo que permite

construir una línea de tiempo precisa de las sesiones realizadas mediante esta plataforma de videoconferencias.

**Figura 4**

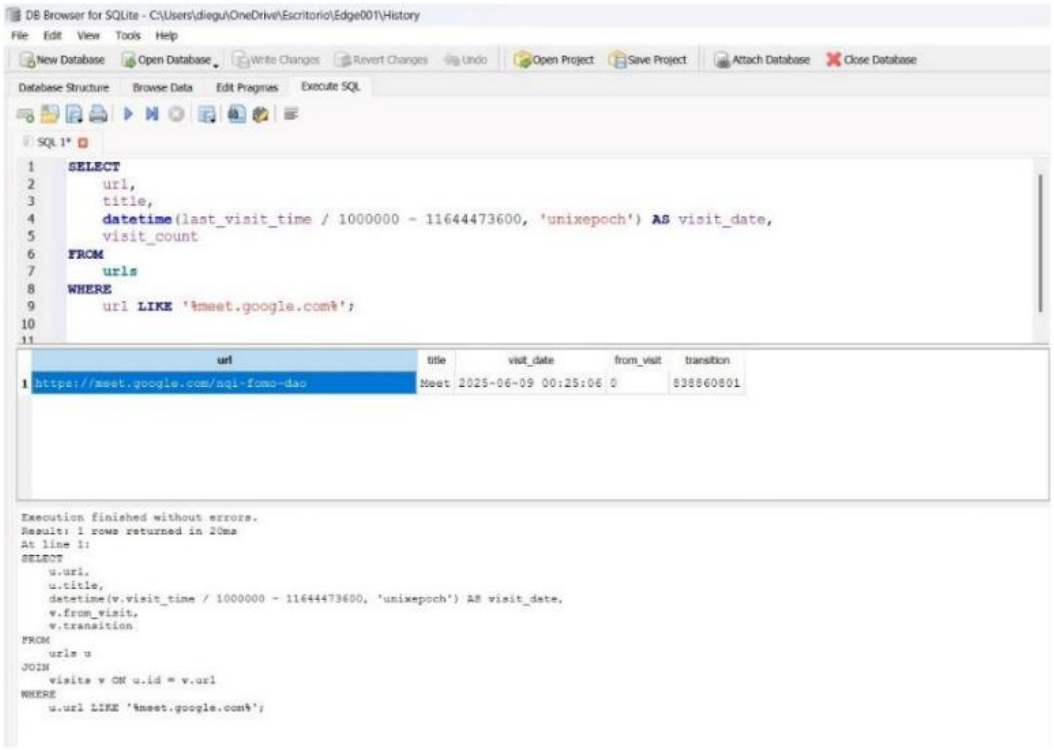
Examinar Archivo History




Se realiza una consulta SQL dentro de DB Browser for SQLite con el propósito de extraer información específica relacionada con el uso de Google Meet. Esta consulta permite recuperar las URLs visitadas, los títulos de las páginas, las marcas temporales y el número de accesos asociados al dominio meet.google.com. Los resultados obtenidos constituyen evidencia clave en la identificación de patrones de uso y frecuencia de acceso a la plataforma, tal como se visualiza en la Figura 5.

**Figura 5**

Obtención de Información

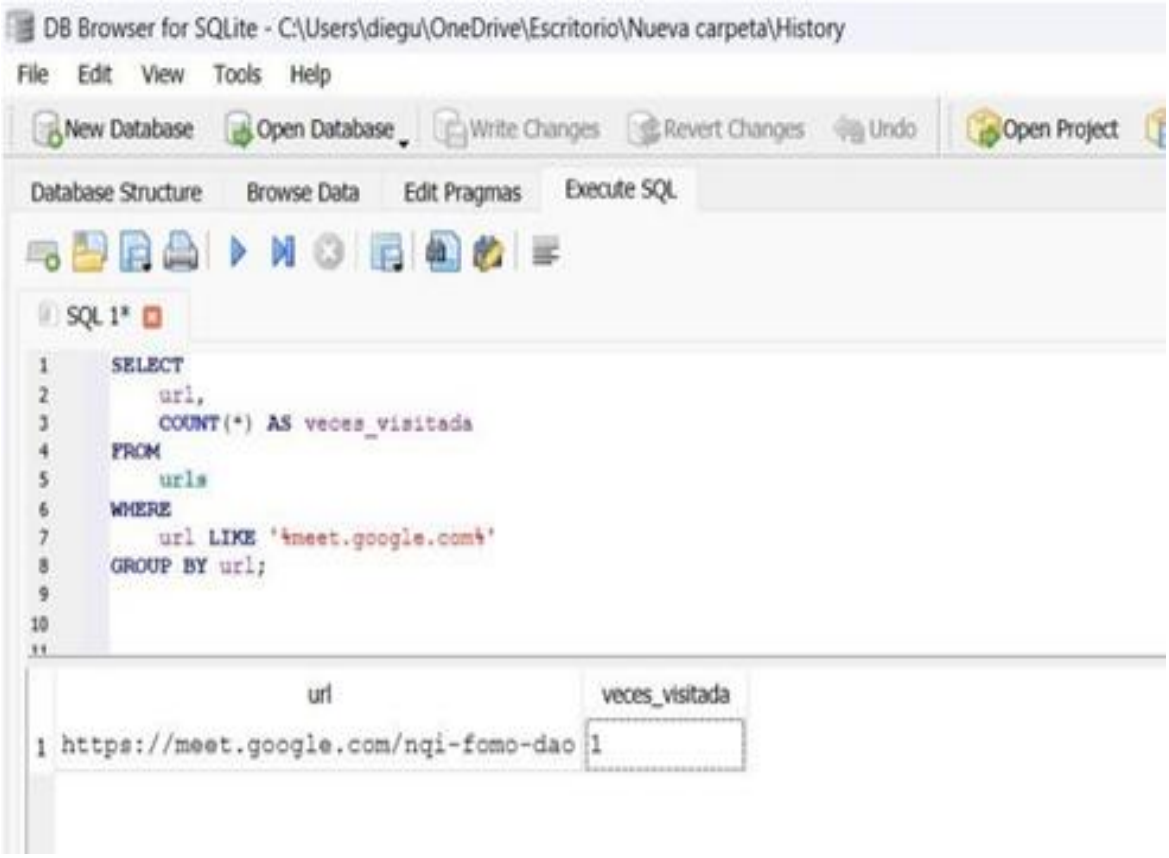



Se ejecuta una consulta SQL avanzada con el objetivo de extraer la totalidad de las visitas web realizadas en el intervalo comprendido entre el primer y el último acceso a Google Meet.

Para ello, se lleva a cabo la unión de las tablas visits y urls, lo que permite correlacionar las URLs con sus respectivos registros de acceso. Adicionalmente, se realiza la conversión de las marcas temporales a un formato de fecha y hora legible, facilitando así la interpretación cronológica de los eventos. Este procedimiento permite contextualizar la actividad del usuario alrededor del uso de la plataforma, tal como se ilustra en la Figura 6.

**Figura 6**

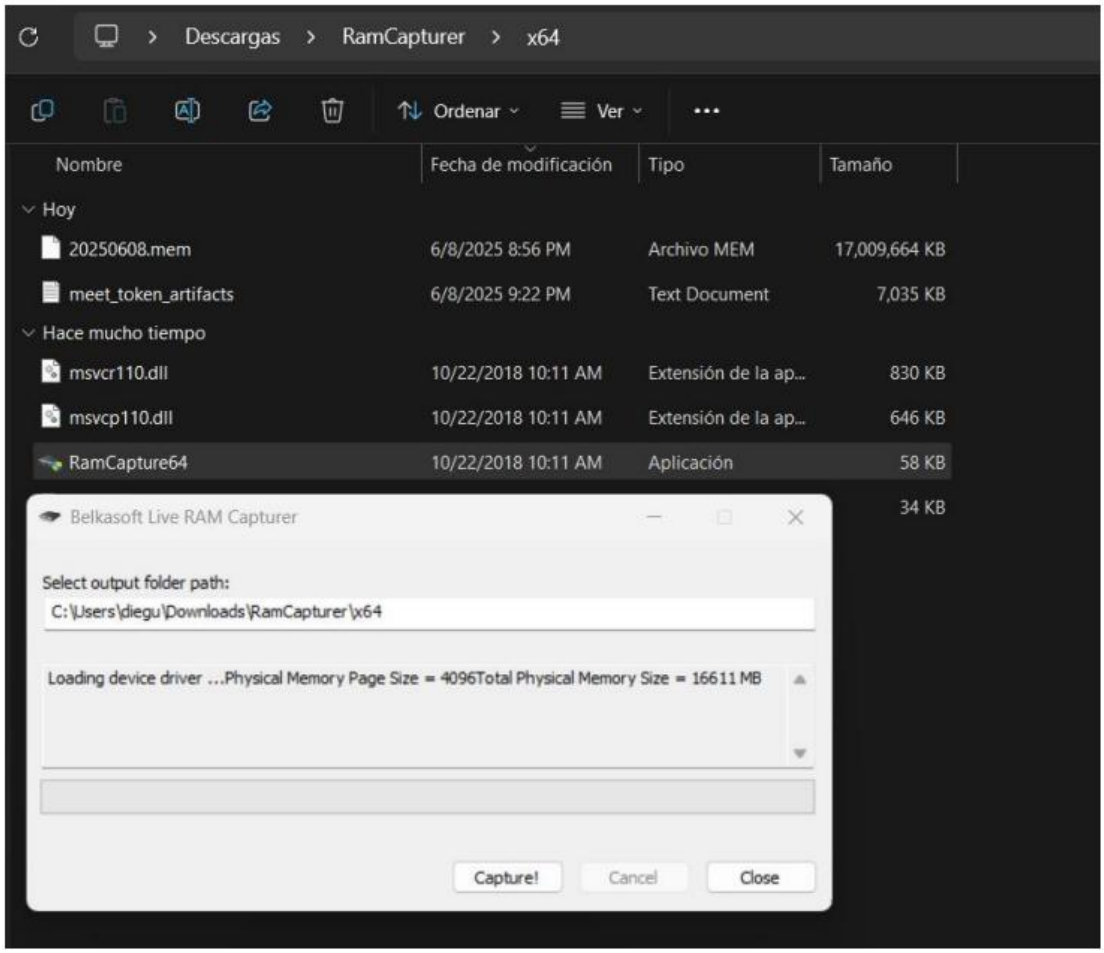
Consulta en el SQL




Se procedió a la captura de la memoria RAM del sistema empleando la herramienta especializada Belkasoft Live RAM Capture, con el fin de obtener información volátil de alto valor forense. Este procedimiento permite acceder a datos transitorios que residen únicamente en la memoria durante la ejecución del sistema, tales como procesos en curso, posibles credenciales en texto claro, sesiones activas y otros artefactos críticos para la investigación. Los resultados de esta operación se evidencian en la Figura 7.

**Figura 7**

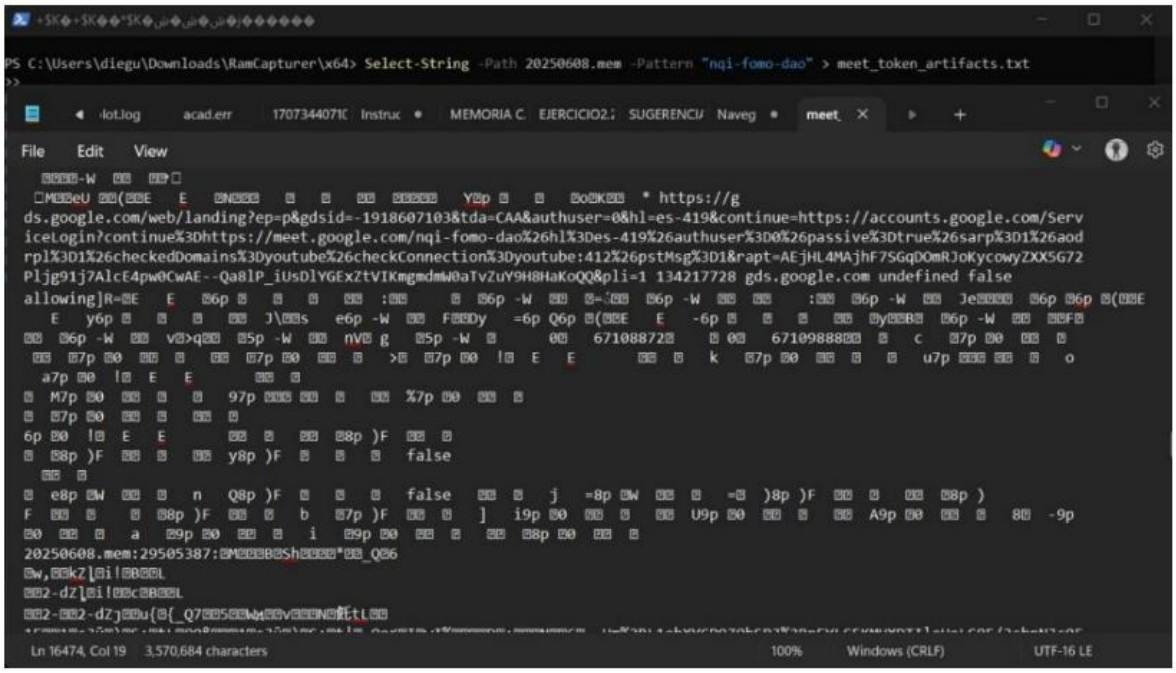
Captura de la Memoria RAM




En el caso del navegador Firefox, se efectuó un análisis del volcado de memoria utilizando la herramienta Volatility3, enfocando la búsqueda en cadenas de texto que incluyeran referencias al dominio de Google Meet, con el objetivo de identificar posibles artefactos relevantes. Si bien se realizaron múltiples intentos por recuperar información útil, la mayoría de los datos presentes en la memoria se encontraban cifrados, lo que limitó su explotación directa. No obstante, se logró identificar una referencia parcial a la URL de una reunión, la cual representa un indicio significativo dentro del contexto investigativo, como se muestra en la Figura 8.

**Figura 8**

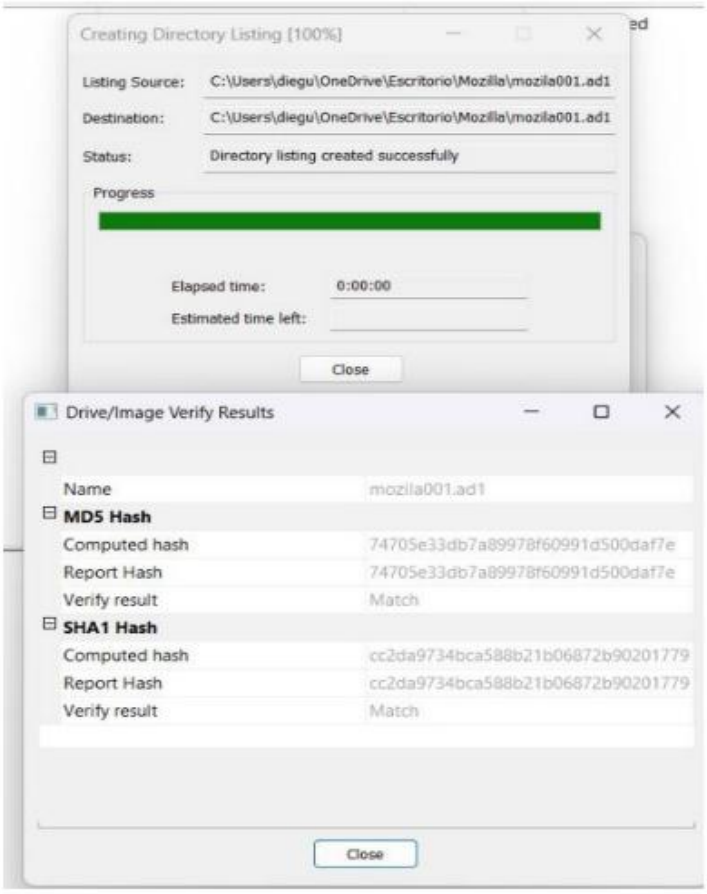
Análisis del archivo




En esta fase del análisis, se examina a través de FTK Imager la ruta C:\Users\diegu\AppData\Roaming\Mozilla\Firefox\Profiles, correspondiente al perfil de usuario del navegador Firefox. A diferencia de Microsoft Edge, Firefox emplea una estructura particular para la organización y almacenamiento de los datos de navegación, lo que implica un enfoque distinto en la localización y extracción de artefactos relevantes. Esta jerarquía de carpetas permite acceder a archivos esenciales como el historial de navegación, cookies y elementos de caché, constituyendo fuentes valiosas de evidencia digital, tal como se visualiza en la Figura 9.

**Figura 9**

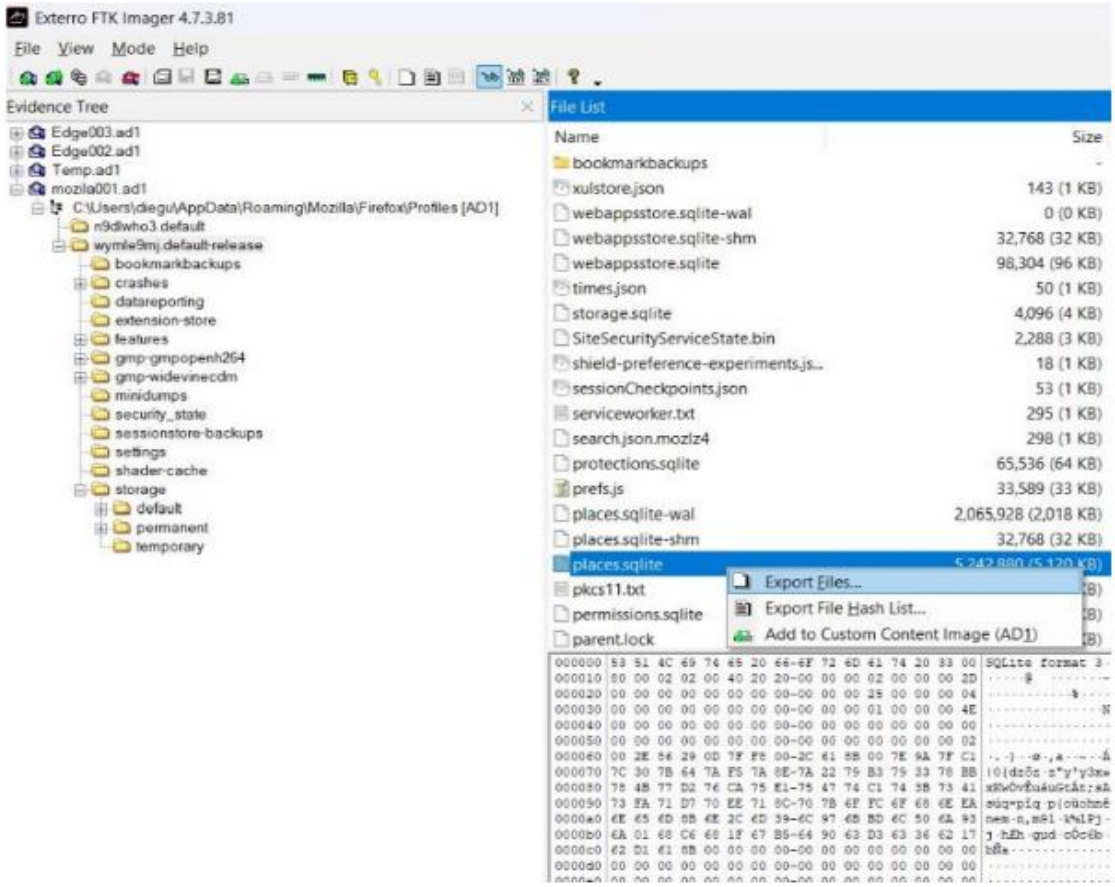
Examinación de ruta




En el navegador Firefox, el historial de navegación se encuentra almacenado en el archivo places.sqlite, ubicado dentro del directorio correspondiente al perfil del usuario. Este archivo, estructurado como una base de datos SQLite, consolida tanto las URLs visitadas como los marcadores que han sido guardados por el usuario. Su análisis permite obtener una visión detallada de la actividad en línea y de los sitios considerados de interés, constituyéndose como una fuente clave de artefactos forenses, tal como se ilustra en la Figura 10.

**Figura 10**

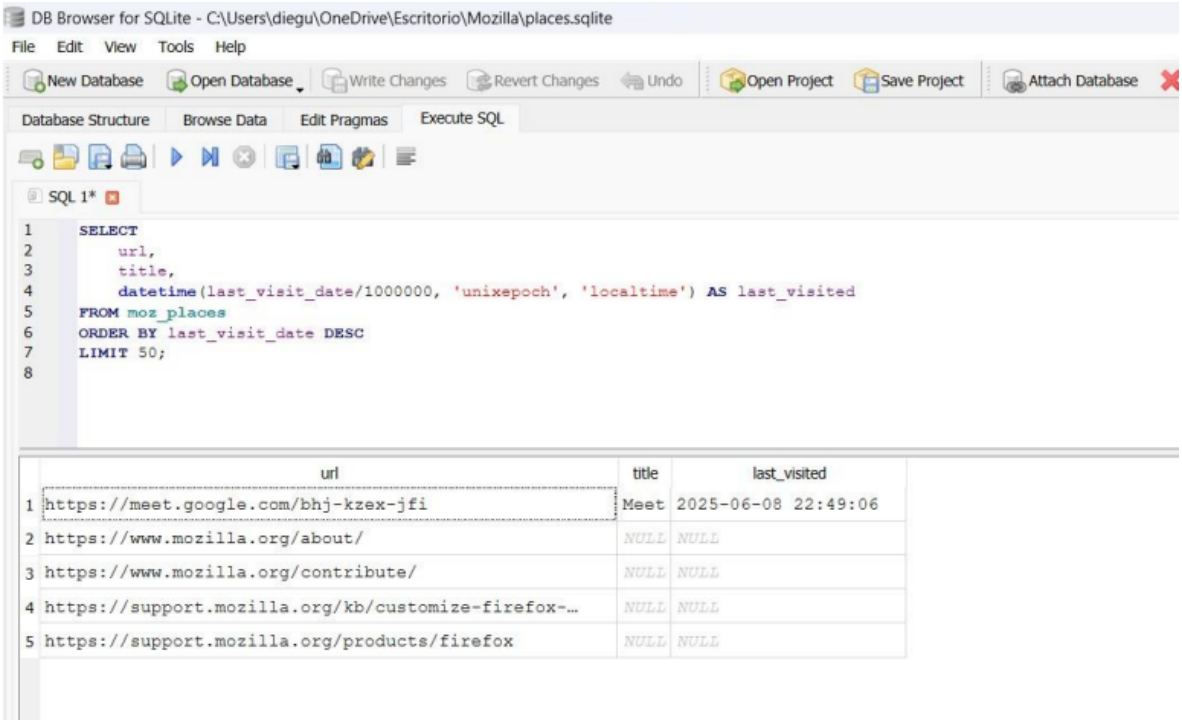
Historial de navegación




Se llevó a cabo la ejecución de una consulta SQL sobre el archivo places.sqlite de Firefox con el propósito de extraer las últimas 50 URLs visitadas por el usuario. La consulta recuperó información detallada que incluyó la dirección web, el título asociado a cada página y la fecha de la última visita, presentada en un formato legible para facilitar su interpretación. Este procedimiento fue fundamental para identificar y analizar la actividad reciente del usuario dentro del navegador, tal como se evidenció en la Figura 11.

**igura 11**

Extracción de URL




**Capítulo 4:**

## 4. Análisis De Resultados

### *Pruebas de Concepto*

Para evaluar la metodología propuesta, se realizaron pruebas en un entorno controlado con Windows 10 de 64 bits y tres navegadores web diferentes como: , Mozilla Firefox y Microsoft Edge, en cada navegador se realizó una videollamada de prueba en Google Meet y se realizaron diferentes acciones, como, por ejemplo: activar la cámara, activar el micrófono, enviar mensajes en el chat, compartir pantalla y activar subtítulos. Cada vez que se finalizaba la sesión, se utilizó la herramienta FTK Imager para generar imágenes forenses de las carpetas donde los

navegadores almacenan información local, estas imágenes incluyeron algunos artefactos digitales como son el historial de navegación, cookies, archivos temporales y caché.

En el navegador de Microsoft Edge, se pudo extraer el archivo History, para luego poder ser evaluado y analizado con DB Browser for SQLite, por medio de consultas SQL se logró identificar accesos a meet.google.com, y se obtuvieron marcas temporales que se utilizaron para reconstruir una línea de tiempo de las sesiones.

En el caso del navegador Mozilla Firefox, se pudo extraer el archivo places.sqlite y se logró obtener las últimas 50 URLs visitadas por el usuario, esto hizo que se logre identificar accesos relevantes hacia Google Meet, títulos de las páginas y fechas de acceso.

Se logró realizar un volcado de la memoria RAM con la herramienta Belkasoft Live RAM Capturer, para luego ser analizada por Volatility3, que permitió identificar varias cadenas de texto que contenían referencias a URLs de reuniones a pesar de que gran parte de la información se encontraba cifrada.

### *Análisis de Resultados*

Este proyecto de titulación demostró que sí es posible recuperar artefactos generados por Google Meet en distintos navegadores web que sean relevantes, aunque presenten algunas limitaciones dependiendo del tipo del navegador y el almacenamiento que utiliza.

En el caso de Microsoft Edge, el archivo de History permitió obtener las URL visitadas, fechas de acceso, entre otros metadatos, lo que hizo sencilla la reconstrucción de la actividad del usuario que estaba utilizando Google Meet, de igual forma en Mozilla Firefox, a pesar de tener una estrucutra de almacenamiento distinta, se logró obtener información desde places.sqlite.

El volcado de la memoria extrajo resultados más limitados, debido a que estaban cifrados, lo que dificultó extraer evidencia completa, sin embargo, se pudieron identificar algunos fragmentos útiles como referencias a reuniones.

El análisis de este proyecto y los resultados obtenidos validan que algunas herramientas como FTK Imager, DB Browser for SQLite, Belkasoft y Volatility3 permiten obtener evidencia digital sobre el uso de Google Meet y la metodología propuesta para realizar el análisis fue efectiva, debido a que, si se logró identificar artefactos de Google Meet en navegadores web, lo que respalda su utilidad en investigaciones forenses reales, pero únicamente cuando el analista forense actúe de manera oportuna para que logre conservar la evidencia necesaria.

**Capítulo 5:**

## 5. Conclusiones Y Recomendaciones

### *CONCLUSIONES*

Entrar en el análisis forense es mucho más difícil en plataformas de videollamada como Google Meet y requiere un sólido entendimiento de cómo operan los navegadores web, que son las puertas de entrada al servicio. Cada navegador en este caso Microsoft Edge y Mozilla Firefox utiliza una forma diferente de almacenar sus datos y, como resultado, qué opciones tenemos para recuperar y analizar las evidencias digitales. Estas variaciones impactan no solo la ubicación física donde se crean los archivos, sino también cómo se almacenan, los datos incluidos y qué datos también se retienen localmente. Es por eso por lo que el conocimiento técnico detallado de los internos del navegador es crucial para una captura efectiva y confiable de evidencias digitales.

En el curso de escribir este análisis, también mostramos que a través de marcas como el Historial en Edge y places.sqlite en Firefox, uno puede identificar accesos a Google Meet, reconstruir cuándo se utilizó y mapear URLs específicas a entidades basadas en la actividad. Dichos artefactos ayudan a establecer relaciones transparentes entre eventos digitales y actividades de los usuarios, haciendo posible comprender los hechos estudiados. La capacidad de extraer estos datos fue útil para confirmar la asistencia a sesiones remotas, lo cual podría ser crucial para temas relacionados con la ciberseguridad, cumplimiento normativo o investigaciones internas.

Por el contrario, el análisis de memoria con aplicaciones forenses como Volatility3 permitió enriquecer el análisis con datos volátiles que normalmente no se guardan en el disco. Pero la información estaba algo limitada en parte debido al hecho de que tanto Google Meet como los navegadores modernos ya cifran archivos en tiempo real. Esta limitación tecnológica no permite acceder a datos sensibles como credenciales o contenido de sesiones, evidenciando que esta es la limitación que enfrentan los investigadores al examinar plataformas profundamente comprometidas con la protección de la privacidad y seguridad del usuario. Aunque se utilizaron varias técnicas de recuperación de cadenas y análisis del diseño interno de la memoria, no se pudo reconstruir información útil que pudiera ayudar con las pistas investigativas.

Las lecciones aprendidas enfatizan la necesidad de integrar diversos conjuntos de evidencias digitales para aumentar el valor de los hallazgos. Aunque el análisis de memoria proporciona beneficios cuando se realiza en el momento adecuado, no se considera, sin embargo, la última opción para llegar a una conclusión. Este enfoque debe ser complementado con el examen de archivos locales almacenados, historiales de navegación y otros artefactos retenidos que puedan proporcionar más contexto. Además, esta investigación refuerza la importancia de la extracción y adquisición rápida, ya que la memoria volátil solo está disponible durante e inmediatamente después del uso de la plataforma, ya que la información puede ser purgada cuando una sesión ha terminado o el sistema ha sido reiniciado.

Por último, es obvio que el panorama forense digital sigue siendo muy dinámico, y las herramientas y técnicas deberían seguir el ritmo del avanzado tecnológico de los proveedores de software, navegadores y soluciones de comunicación por internet.

## *RECOMENDACIONES*

Vale la pena señalar que se aconseja un enfoque integrado, combinando el examen de la memoria volátil y la evidencia residente en disco. Deben emplearse herramientas como FTK Imager, DB Browser for SQLite y Volatility3 en combinación para aumentar con mayor éxito las posibilidades de encontrar y recuperar evidencia útil. Este enfoque híbrido amplía el alcance de la investigación y permite verificar la información mediante diversas fuentes, lo que incrementa la credibilidad de los hallazgos del estudio.

Al investigar con Google Meet, es esencial adquirir la RAM durante la sesión en vivo o inmediatamente después. "Este proceso incrementa considerablemente el potencial para la recuperación de rastros de datos en texto plano antes de que el sistema sobrescriba partes de esos rastros o se autodestruya la información." Además de lo anterior, deben conservarse los registros de cada movimiento, lo cual se mantiene como el principio de la cadena de custodia en la evidencia recogida.

Los sistemas de Google Meet y los navegadores web se actualizan frecuentemente, por lo tanto, para los investigadores, es esencial mantenerse al día con las actualizaciones relacionadas con el manejo del almacenamiento local, la política de privacidad o los nuevos mecanismos de

protección del navegador web y los métodos internos de los navegadores web. Eso incluye probar nuevas herramientas forenses, ajustar las maneras en que se analizan los materiales y actualizar la investigación que se realiza para desarrollar nueva tecnología.

La formación continua con ejercicios prácticos en un entorno real garantizará que los profesionales forenses se mantengan al día con el mundo digital en constante cambio, de modo que puedan contrarrestar las demandas y complejidades de la investigación.

## 6. Referencias Bibliográfica

AccessData Group. (2025). FTK Imager user guide. https://accessdata.com/product-download/ftk-imager-version-4-3-0

AccessData Group. (2025). FTK Imager user guide. https://accessdata.com/product-download/ftk-imager-version-4-3-0

Autopsy. (2025). Autopsy – Digital Forensics Platform. https://www.sleuthkit.org/autopsy/

Belkasoft. (2025). Belkasoft Live RAM Capturer. https://belkasoft.com/ram-capturer

Belkasoft. (2025). Belkasoft Live RAM Capturer. https://belkasoft.com/ram-capturer

Bermudez, A. M. (2025). *La importancia del análisis forense digital en la era tecnológica*. Obtenido de https://www.pwc.com/co/es/pwc-insights/importancia-analisis-forense.html

Bodnar, J. (2021). ¿Qué es un navegador web? https://www.avast.com/es-es/c-what-is-a-web-browser

Browser History Examiner. (2025). Browser History Examiner – Digital Forensics Tool.https://www.browserhistoryexaminer.com/

Carvey, H. (2018). *Windows Forensic Analysis Toolkit (4th ed.)*. Elsevier.

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

Cookie Script. (2025). ¿El almacenamiento local y el almacenamiento de sesiones cumplen con las leyes de privacidad? https://cookie-script.com/blog/local-storage-and-session-storage

D'Souza, J. (2025). Google Meet statistics and facts (2025). ElectroIQ. https://electroiq.com/stats/google-meet-statistics/

Exterro. (2025). Create Forensic Images with Exterro FTK Imager. https://www.exterro.com/digital-forensics-software/ftk-imager

Exterro. (2025). Create forensic images with Exterro FTK Imager. https://www.exterro.com/digital-forensics-software/ftk-imager

Foxton Forensics. (2025). Professional tool to investigate web browser history. Obtenido de https://www.foxtonforensics.com/browser-history-examiner/

GCF Global. (2021). Google Meet: ¿Qué es Google Meet? https://edu.gcfglobal.org/es/google-meet/que-es-google-meet/1/

Google. (2025). Descubre Google Meet, una solución de videoconferencias confiable, segura y fácil de usar. Obtenido de https://edu.google.com/intl/es-419_ALL/workspace-for-education/products/meet/

Google. (2025). browser. https://www.google.com//

IBM. (2025). ¿Qué es la informática forense? https://www.ibm.com/topics/forensic-computing

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

Jones, K. J., Bejtlich, R., & Rose, C. W. (2005). *Real Digital Forensics: Computer Security and Incident Response*. Addison-Wesley.

Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*. Wiley.

Magnet Forensics. (2025). Magnet AXIOM. https://www.magnetforensics.com/products/magnet-axiom/

Mandia, K., Prosise, C., & Pepe, M. (2003). *Incident Response and Computer Forensics (2nd ed.)*. McGraw-Hill/Osborne.

Microsoft. (2023). Windows 10 specifications. https://www.microsoft.com/windows/windows-10-specifications

Microsoft. (2025). Microsoft Edge browser. https://www.microsoft.com/edge

Miner, M. (2021). ¿Qué es un artefacto en ciberseguridad? SSI Insider. https://insider.ssi-

net.com/insights/what-is-an-artifact-in-cyber-security

Mozilla Foundation. (2025). Mozilla Firefox browser. https://www.mozilla.org/firefox/

Sedgwick. (2023). 8 pasos para una investigación forense exitosa. https://www.sedgwick.com/blog/8-steps-to-a-successful-forensic-investigation/?loc=lam

SQLite.org. (2025). DB Browser for SQLite. https://sqlitebrowser.org/

SQLite.org. (2025). DB Browser for SQLite. https://sqlitebrowser.org/

Volatility Foundation. (2025). Volatility3 framework. https://www.volatilityfoundation.org/volatility3

Volatility Foundation. (2025). Volatility3 framework. https://www.volatilityfoundation.org/volatility3

## 7. Apéndices

Debido al volumen de información desarrollado a lo largo del proyecto de titulación (16.5 GB), las evidencias que incluyen los volcados de memoria y las pruebas realizadas, se encuentran disponibles en el siguiente enlace: https://mailinternacionaledu-my.sharepoint.com/:f:/g/personal/lusanchezli_uide_edu_ec/EnR2XejfZMJBm1MdRdBvKdEBG03Zf2u9BHKyr-schMZm2A?e=uyVBTd