Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTORES:

CAMACHO BRAUSENDORFF GERMAN RICARDO

MAYA CARRERA STEVEN ALEJANDRO

MINAYO YUJATO JENNIFER SAMANTA

SANTAMARIA ACOSTA GABRIEL SANTIAGO

TUTORES:

Iván Reyes Chacón

Paulina Vizcaíno

TEMA

Análisis Forense Correlacionado de Artefactos del Registro, LNK, Prefetch y AmCache para la Reconstrucción de Actividad del Usuario en Windows 11

Quito - Ecuador

Junio – 20206

REINVENTEMOS EL FUTURO

Certificación de autoría

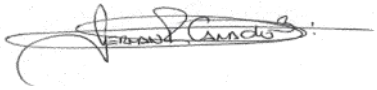
Nosotros, **Jennifer Samanta Minayo Yujato, Steven Alejandro Maya Carrera, Gabriel Santiago Santamaria Acosta, German Ricardo Camacho Brausendorff,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación 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
Jennifer Samanta Minayo Yujato

Firma
Steven Alejandro Maya Carrera

Firma
Gabriel Santiago Santamaria Acosta



Firma
German Ricardo Camacho Brausendorff

Autorización de Derechos de Propiedad Intelectual

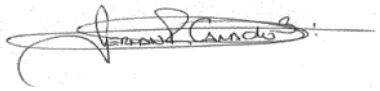
Nosotros, **Jennifer Samanta Minayo Yujato, Steven Alejandro Maya Carrera, Gabriel Santiago Santamaria Acosta, German Ricardo Camacho Brausendorff**, en calidad de autores del trabajo de investigación titulado ***Titulo del trabajo de investigación Análisis Forense Correlacionado de Artefactos del Registro, LNK, Prefetch y AmCache para la Reconstrucción de Actividad del Usuario en Windows 11***, 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, 19 de junio del 2026

Firma
Jennifer Samanta Minayo Yujato

Firma
Steven Alejandro Maya Carrera

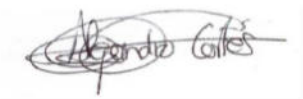
Firma
Gabriel Santiago Santamaria Acosta



Firma
German Ricardo Camacho Brausendorff

APROBACIÓN DE DIRECCIÓN Y COORDINACIÓN DEL PROGRAMA

Nosotros, Alejandro Cortés López e Iván Galo Reyes Chacón, declaramos que: Jennifer Samanta Minayo Yujato, Steven Alejandro Maya Carrera, Gabriel Santiago Santamaria Acosta, German Ricardo Camacho Brausendorff son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



Alejandro Cortés
Director/a de la
Maestría en Ciberseguridad

Iván Reyes
Coordinador/a de la
Maestría en Ciberseguridad

DEDICATORIA

Dedicamos este trabajo a nuestras familias, por su apoyo incondicional, comprensión y motivación constante a lo largo de nuestra formación académica y profesional.

También lo dedicamos a todas las personas que, de una u otra manera, contribuyeron con su apoyo, consejos y acompañamiento para alcanzar esta importante meta.

Finalmente, dedicamos este esfuerzo a quienes nos inspiraron a perseverar ante los desafíos y a mantener el compromiso con el aprendizaje y la superación personal.

AGRADECIMIENTOS

Expresamos nuestro más sincero agradecimiento a Dios por brindarnos la fortaleza, sabiduría y perseverancia necesarias para culminar con éxito este trabajo de investigación.

Asimismo, agradecemos a nuestros docentes y tutores por su orientación y por los valiosos conocimientos compartidos a lo largo de nuestra formación académica, los cuales han sido fundamentales para el desarrollo y culminación de este trabajo. Más allá del conocimiento impartido, agradecemos los valores inculcados, que nos inspiran a continuar creciendo tanto en el ámbito profesional como personal.

Este Trabajo Final de Maestría no habría sido posible culminarlo con éxito sin el esfuerzo y compromiso de cada uno de los integrantes de este grupo. Expresamos nuestro sincero agradecimiento por la dedicación, disciplina, responsabilidad y constancia demostradas a lo largo de todo el proceso, cualidades que hicieron posible superar los desafíos presentados y alcanzar satisfactoriamente los objetivos propuestos.

Finalmente, reconocemos a la Universidad Internacional del Ecuador por brindarnos los recursos académicos y el entorno adecuado para fortalecer nuestra formación profesional y hacer posible el desarrollo de este proyecto de investigación.

Resumen

Windows 11 introdujo modificaciones estructurales en sus artefactos forenses (p. ej., Amcache v2, extensión de la nube integrada y nuevos esquemas de registro) que, sumados al empleo creciente de técnicas anti-forenses, han evidenciado una brecha en los métodos de reconstrucción de eventos basados en fuentes aisladas. El presente proyecto propone una metodología de correlación multi-fuente diseñada para validar la resistencia del análisis forense ante intentos de manipulación de evidencia digital. Se desarrolló un escenario de laboratorio controlado que simula actividad post-explotación (incluyendo ejecución de scripts, exfiltración mediante BITS y acceso remoto no autorizado), aplicando posteriormente contramedidas anti-forenses selectivas (limpieza de Prefetch, borrado de logs y time-stomping). Los artefactos del sistema, registro, memoria RAM y red fueron procesados mediante herramientas de código abierto (Volatility 3, Plaso/log2timeline, Eric Zimmerman Tools y KAPE) e integrados en un pipeline de cuatro fases: deserialización, normalización temporal, enriquecimiento de metadatos y correlación por ventana temporal. Los resultados demuestran que la concordancia de al menos tres fuentes independientes aumenta significativamente la confianza en la reconstrucción de eventos, mientras que la exclusión de artefactos de memoria y subsistemas como BAM/DAM (Monitor de Actividad en Segundo Plano y Moderador de Actividad de Escritorio, respectivamente) reduce la capacidad de detección ante borrado selectivo. Asimismo, se constató la ausencia de criterios estandarizados de validación anti-forensic específicos para Windows 11, lo cual representa una línea futura crítica para la comunidad forense.

Palabras clave: forense digital, Windows 11, correlación de artefactos, técnicas anti-forenses, análisis de memoria, timeline forense.

Abstract

Windows 11 introduced structural modifications to its forensic artifacts (e.g., Amcache v2, integrated cloud extension, and new logging schemes) which, coupled with the increasing use of anti-forensic techniques, have revealed a gap in event reconstruction methods based on isolated sources. This project proposes a multi-source correlation methodology designed to validate the resilience of forensic analysis against attempts to manipulate digital evidence. A controlled laboratory scenario was developed simulating post-exploitation activity (including script execution, exfiltration via BITS, and unauthorized remote Access) followed by the application of selective anti-forensic countermeasures (prefetch cleanup, log deletion, and time-stomping). System artifacts, including registry, RAM, and network data, were processed using open-source tools (Volatility 3, Plaso/log2timeline, Eric Zimmerman Tools, and KAPE) and integrated into a four-phase pipeline: deserialization, timeline normalization, metadata enrichment, and time window correlation. The results demonstrate that concordance from at least three independent sources significantly increases confidence in event reconstruction, while excluding memory artifacts and subsystems such as BAM/DAM (Business Activity Monitoring / Database Activity Monitoring) reduces the ability to detect selective deletion. Furthermore, the absence of standardized anti-forensic validation criteria specific to Windows 11 was noted, representing a critical future direction for the forensic community.

Keywords: digital forensics, Windows 11, artifact correlation, anti-forensic techniques, memory analysis, timeline forensics.

TABLA DE CONTENIDOS (Índice)

Contenido

Capítulo 1 15
Introducción 15
Definición del proyecto 15
Justificación e Importancia del Trabajo de Investigación 19
Objetivos de la Investigación 23
Hipótesis de Investigación 25
Alcance 27
Capítulo 2 36
Estado del Arte 36
Introducción al Capítulo 36
La Investigación Forense en Sistemas Windows: Evolución del Paradigma. 36
Windows 11: Brecha Entre la Realidad Desplegada y el Conocimiento Forense Publicado 37
Brechas del Conocimiento y Vacíos Identificados. 39
Artefactos Forenses en Entornos Windows: Clasificación y Estado de la Técnica 41
Metodologías de Correlación y Fusión Temporal (Super Timeline) 43
Herramientas y Frameworks en la Literatura Especializada 44
Conclusiones del Capítulo y Posicionamiento del Trabajo 45
Capítulo 3 47
Marco Metodológico 47
Introducción al Capítulo 47
Principios Rectores de la Metodología Propuesta 47
Fase 1: Recolección Ordenada de Evidencias 48
Fase 2: Parseo y Normalización de Artefactos 53
Fase 3: Fusión Temporal (Super Timeline) 57
Fase 4: Correlación Cruzada y Triangulación 59
Investigación Complementaria. 61
Protocolo de Validación y Criterios de Éxito 63
Consideraciones Éticas y de Seguridad del Experimento 64
Conclusiones del Capítulo 64
Capítulo 4 66
Diseño del Experimento y Escenario de Laboratorio 66
Arquitectura del Entorno de Laboratorio 66
Especificaciones Técnicas de la Infraestructura Virtualizada 67

Configuración Base del Sistema Operativo Windows 11 68
Diseño del Escenario de Compromiso post-explotación 70
Protocolo de ejecución, Bitácora de Actividades y Cadena de Custodia 75
Consideraciones Finales del Diseño Experimental. 85
Capítulo 5 87
Desarrollo y Resultados 87
Aplicación de la Fase 1: Recolección Ordenada de Evidencias 87
Aplicación de la Fase 2: Parseo y Normalización 90
Aplicación de la Fase 3: Fusión Temporal (Super Timeline) 92
Aplicación de la Fase 4: Correlación Cruzada y Triangulación 93
Matriz de Resultados y Cumplimiento de Criterios de Aceptación 97
Discusión de Resultados 98
Conclusiones del Capítulo 100
Capítulo 6 101
Análisis de Resultados, Discusión y Conclusiones 101
Análisis de Resultados y Comparativa con Metodologías de Análisis Aislado 101
Verificación de Hipótesis 103
Discusión de las limitaciones del estudio 105
Implicaciones para la Práctica Pericial y la Respuesta a Incidentes 106
Líneas de investigación Futura 107
Conclusiones Finales 108
Referencias 110
Apéndices 115
Anexos 117
Anexo A. Stack de Herramientas Forenses. 117
A.1 Herramientas de adquisición 117
A.2 Frameworks de Análisis de Memoria 117
A.3 Suites de Análisis de Artefactos 117
A.4 Utilidades Específicas de Windows 11 118
Anexo B — Taxonomía de Artefactos en Windows 11 118
B.1 Artefactos del Sistema Operativo 118
B.2 Artefactos de Ejecución y Actividad 118
B.3 Artefactos de Red y Conectividad 119
B.4 Artefactos de Almacenamiento en Nube (Windows 11 integrado) 119
Anexo C — Escenarios de Laboratorio y Validación 120
C.1 Configuración del Entorno de Pruebas 120

C.2 Matriz de Escenarios de Validación 120
C.3 Métricas de Validación de Correlación 121
Anexo D — Técnicas Anti-forenses Catalogadas 121
D.1 Clasificación por Capa del Sistema 121
D.2 Mapeo Técnica vs Resistencia 122
Anexo E — Matriz de Correlación de Fuentes 122
E.1 Evento: Ejecución de Aplicación 122
E.2 Evento: Conexión de Dispositivo USB 123
E.3 Evento: Actividad de Red 123
Anexo F — Scripts de Automatización 124
F.1 Pipeline de Correlación (Pseudocódigo) 124
F.2 Criterios de Aceptación para Resultados de Correlación 124
Anexo G — Glosario de Términos Forenses 125

LISTA DE TABLAS (Índice de tablas)

Tabla 1 Objetivos, Hipótesis y brechas del conocimiento 27
Tabla 2 Límites técnicos del laboratorio y del escenario 28
Tabla 3 Herramientas mínimas para análisis de artefactos 31
Tabla 4 Criterios de aceptación 34
Tabla 5 Artículos forensia Windows 38
Tabla 6 Clasificación de artefactos forenses en entornos Windows 40
Tabla 7 Principios que orientan las decisiones técnicas 47
Tabla 8 Lista mínima de extracción de artefactos 52
Tabla 9 Plugins y comandos modelo 54
Tabla 10 Plugins de RegRipper relevantes 55
Tabla 11 Criterios de filtrado aplicados 58
Tabla 12 Eventos de interés a confirmar 59
Tabla 13 Modelo para ejecución de documento malicioso 60
Tabla 14 Reglas de decisión para eventos 61
Tabla 15 Ejemplo de triangulación anti-forensia 63
Tabla 16 Protocolo de validación y criterios de éxito 63
Tabla 17 Especificaciones técnicas de la infraestructura virtualizada 67
Tabla 18 Servicios y funcionalidades aplicadas 69
Tabla 19 Protocolo de snapshots 75
Tabla 20 Bitácora de ejecución de escenario 76
Tabla 21 Formulario Modelo de cadena de custodia 78
Tabla 22 Formulario de adquisición de la imagen forense 78
Tabla 23 Formulario de extracción del artefacto SOFTWARE 79
Tabla 24 Formulario de extracción del artefacto SYSTEM 80
Tabla 25 Formulario de extracción del artefacto SECURITY 80
Tabla 26 Formulario de extracción del artefacto NTUSER.DAT 81
Tabla 27 Formulario de extracción del artefacto AmCache.hve 81
Tabla 28 Formulario de extracción del artefacto Prefetch 82
Tabla 29 Formulario de extracción del artefacto Application.evtx 82
Tabla 30 Formulario de extracción del artefacto Microsoft-Windows-Bits-Client/Operational.evtx 83
Tabla 31 Formulario de extracción del artefacto SRUDB.dat 83
Tabla 32 Formulario de extracción del artefacto ActivitiesCache.db 84
Tabla 33 Evidencia de archivo Word con macro maliciosa 85
Tabla 34 Evidencias volátiles 87
Tabla 35 Imagen forense del disco 87
Tabla 36 Lista de artefactos extraídos 88
Tabla 37 Hallazgos de parseo de volátiles 90
Tabla 38 Hallazgos de parseo de Prefetch 91
Tabla 39 Plugins ejecutados y hallazgos esperados 91
Tabla 40 Parseo de Logs EVTX 92
Tabla 41 Parseo de SRUM 92
Tabla 42 Comandos super timeline 93
Tabla 43 Despliegue de macro a través de word 94
Tabla 44 Creación clave SystemUpdate 94
Tabla 45 Ejecución de net.exe 95

Tabla 46 Ejecución de bitsadmin 95
Tabla 47 Borrado de logs 96
Tabla 48 Borrado de carpeta Prefetch 96
Tabla 49 Tabla de cumplimiento CA-01 a Ca-07 97
Tabla 50 Limitaciones Estructurales 101
Tabla 51 Síntesis Comparativa 102
Tabla 52 Conclusiones por Objetivos 108

LISTA DE FIGURAS

Figura 1 Versión de entorno de virtualización usado. 28
Figura 2 Recursos usados en máquina anfitrión. 29
Figura 3 Recursos usados en máquina virtual. 29
Figura 4 Bitlocker desactivado. 30
Figura 5 Recursos mínimos de máquina anfitrión. 33
Figura 6 Recursos S.O. de máquina anfitrión. 33
Figura 7 Herramienta Volatility Workbench 3. 44
Figura 8 Toma de Instantáneas Pre y Post Ejecución. 49
Figura 9 Adquisición imagen de disco 50
Figura 10 Extracción de datos con FTK Imager 3.1.1.8. 51
Figura 11 Extracción de procesos de memoria con Volatility. 53
Figura 12 Especificaciones de la configuración de la máquina virtual. 68
Figura 13 Macro contenida en el documento word actuando como un programa maligno. 71
Figura 14 Verificación del Registro de ejecución de programa maligno. 71
Figura 15 Protocolo de Instantánea máquina virtual 76
Figura 16 Obtención del HASH256 del archivo de memoria 78
Figura 17 Obtención del HASH256 del archivo de la imagen del disco 79
Figura 18 Obtención del HASH del archivo SOFTWARE 79
Figura 19 Obtención del HASH 256 del archivo malware 85
Figura 20 Obtención del hash256 de la imagen del disco 87
Figura 21 Obtención del HASH de archivo SOFTWARE 88
Figura 22 Obtención del HASH de archivo SYSTEM 89
Figura 23 Obtención del HASH de archivo SECURITY 89
Figura 24 Obtención del HASH de archivo NTUSER.DAT 89
Figura 25 Obtención del HASH de archivo AMCACHE.HVE 89
Figura 26 Obtención del HASH de archivo PREFECTH.ZIP 89
Figura 27 Obtención del HASH de archivo APPLICATION.EVTX 89
Figura 28 Obtención del HASH de archivo Microsoft-Windows-WMI-Activity%4Operational.evtx 89
Figura 29 Obtención del HASH de archivo SRUDB.DAT 90
Figura 30 Obtención del HASH de archivo ACTIVITIESCACHE.DB 90
Figura 31 Evidencia parseo Pstree Winword. 91

Capítulo 1

Introducción

Definición del proyecto

La introducción de Windows 11 trajo consigo cambios sustanciales en la gestión de registros de actividad del sistema, la estructura de almacenamiento de artefactos forenses y los mecanismos de ejecución de procesos, diferenciándose de versiones anteriores en aspectos críticos para la investigación digital. (Paulino et al. 2025)

Sin embargo, las metodologías forenses predominantes en la literatura científica y en el ámbito profesional han sido concebidas y validadas principalmente para entornos Windows 7 y Windows 10, abordando el análisis de artefactos de forma aislada mediante listas de verificación estáticas. (Skulkin y de Courcier, 2017)

Esta desconexión genera una brecha metodológica: la falta de un marco estructurado que permita correlacionar múltiples fuentes de evidencia (registro, sistema de archivos, volátiles y artefactos específicos de Windows 11) dificulta la reconstrucción cronológica precisa de la actividad del usuario y diluye la capacidad de diferenciar comportamientos legítimos de indicios de compromiso. (Casey, 2011)

Frente a esta problemática, el presente proyecto tiene como finalidad desarrollar una metodología estructurada para el análisis y correlación de artefactos forenses en sistemas Windows 11, orientada a la reconstrucción coherente de la actividad del usuario y a la identificación temprana de posibles eventos maliciosos dentro de una investigación digital.

Marco Metodológico Estructurado.

Esta metodología estará basada en al menos 3 procesos fundamentales para garantizar la correlación correcta de la evidencia que se obtenga en un análisis forense.

El primer proceso: es la recolección de la información de manera ordenada: Esto es respetando la volatilidad de la información (Orden de recolección, RFC 3227), capturando la RAM, luego el estado del disco y los archivos del sistema de archivos (Instituto Nacional de Ciberseguridad [INCIBE], 2019).

El segundo proceso: es la fusión de líneas de tiempo (Super Timeline): El objetivo es la extracción de los timestamp (marcas de tiempo) de todas las fuentes de datos y luego ordenarlas cronológicamente en una sola base de datos.

El tercer proceso: es la correlación cruzada: ningún artefacto por si solo demuestra alguna intención como tal. Para poder confirmar una acción (ej. Ex filtración de datos o la ejecución de un malware), se busca al menos en 3 fuentes diferentes de información.

Fuentes de Evidencia a Correlacionar.

El Éxito de Windows 11 (sistema operativo con el cual realizaremos nuestro análisis específicamente) radica en cómo se entrelazan estos 4 pilares:

Datos volátiles (Memoria Ram): Procesos en ejecución, comandos ejecutados recientemente, llaves de cifrado en memoria, conexión de redes activas (Lang et al., 2025).

Sistemas de archivos: Metadatos de $MFT y $UsnJrnl (para saber exactamente cuándo se creó, modificó o eliminó un archivo), además de carpetas recientes.

Registro de Windows (Registry): Claves de actividad reciente (ej. RecentDocs), dispositivos USB conectados y rastros de ejecución (UserAssist, ShimCache, AmCache).

Artefactos Específicos de Windows 11: Historial de la línea de tiempo nativa de Microsoft, bases de datos SRUM (para telemetría de uso de CPU y red por aplicación), archivos Prefetch/SysMain, y eventos recientes del Visor de Eventos (.EVTX).

Herramientas Recomendadas para la Correlación.

Con el propósito de operativizar el modelo propuesto, la fase de adquisición e ingesta de datos se apoya en un conjunto de herramientas forenses especializadas. El uso de este toolkit automatiza las tareas repetitivas de recolección de bajo nivel y extracción de metadatos estructurales. Esta selección responde a la necesidad de adquirir las evidencias bajo un estricto respeto al orden de volatilidad.

Para Volátiles: Volatility, el estándar de facto para el análisis de memoria RAM y extracción de procesos (Lang y Schreck, 2025). Su integración es indispensable para extraer el árbol de procesos activos, mapear inyecciones de código en hilos de ejecución legítimos y recuperar descriptores de seguridad en memoria.

Para Recolección y Parsing: DFIR-ORC (ANSSI, 2019) especializado en extraer todos los artefactos de Windows. Su selección está justificada por su capacidad para interactuar directamente con la tabla maestra de archivos (MFT) y realizar copias de bajo nivel de colmenas del Registro bloqueadas por el sistema operativo, garantizando la consistencia de los datos de AmCache y el Registro sin comprometer la estabilidad del sistema.

Para Correlación y Líneas de Tiempo: La combinación de las siguientes herramientas resuelve el problema del volumen de datos: Plaso unifica la telemetría en bruto del disco, Timeline Explorer actúa como el filtro crítico para que el analista detecte anomalías como el timestomping, y Autopsy valida el contexto general del sistema de archivos. El resultado es un procedimiento de análisis cruzado donde la reconstrucción de los hechos es completamente reproducible.

Plaso (log2timeline), el motor de código abierto capaz de parsear el disco y el registro para crear una línea de tiempo masiva. (Log2timeline, 2026)

Timeline Explorer, para visualizar, filtrar y correlacionar los logs y timestamps de forma gráfica.

Herramientas comerciales: Soluciones como Magnet AXIOM o Belkasoft X (Belkasoft, 2026) poseen módulos automatizados que correlacionan el registro, el sistema de archivos y el historial del usuario de Windows de forma nativa (Magnet Forensics, 2026; Belkasoft, 2026). Esto no será parte del presente trabajo, sin embargo, se menciona para el conocimiento de herramientas comerciales que tienen automatizado gran parte de estos procesos.

Para el desarrollo, se implementará un entorno de laboratorio controlado mediante máquinas virtuales sobre hipervisores de Tipo 2 (VirtualBox/VMware). En este entorno se recreará un escenario de compromiso post-explotación consistente en: (i) ejecución inicial de un payload mediante un documento Office con macros maliciosas; (ii) establecimiento de persistencia a través de una tarea programada modificando la clave de registro HKLM\...\Run; (iii) movimiento lateral simulado mediante el uso de herramientas legítimas (Living Off The Land) como net.exe y bitsadmin; y (iv) intento de borrado selectivo de trazas mediante la eliminación de logs del Visor de Eventos y la limpieza de la carpeta Prefetch.

Este escenario ha sido diseñado de forma deliberada para generar un perfil de artefactos heterogéneo — incluyendo registros del sistema (SOFTWARE, SYSTEM), metadatos de ejecución (Prefetch adaptado a Windows 11), artefactos de red (Firewall logs, BITS transfer jobs) y rastros de almacenamiento (Recycle Bin, ficheros temporales) — permitiendo así validar la metodología de correlación propuesta bajo condiciones realistas de investigación digital.

A partir de las actividades ejecutadas en el entorno controlado, se recopilarán y analizarán diversos artefactos de Windows 11, entre ellos los archivos Prefetch, accesos directos (LNK), AmCache y artefactos del Registro de Windows. Estos elementos contienen información relevante sobre la ejecución de aplicaciones, acceso a archivos, interacción del usuario y modificaciones realizadas en el sistema,

constituyendo fuentes fundamentales para la reconstrucción de eventos y la obtención de evidencias digitales.

Como resultado, el proyecto busca demostrar la importancia de la correlación de múltiples artefactos forenses para mejorar la precisión de los análisis digitales, minimizar interpretaciones incompletas y fortalecer la identificación de evidencias relevantes durante las investigaciones forenses en entornos Windows 11.

Justificación e Importancia del Trabajo de Investigación

Justificación Contextual y Cuantitativa.

La adopción de Windows 11 ha dejado de ser una prospectiva tecnológica para convertirse en la realidad dominante del parque informático mundial. Según los indicadores de auditoría web de StatCounter (2026), al cierre del ciclo interanual de mayo de 2026, Windows 11 consolida el 71.69% de la cuota de mercado mundial en sistemas operativos de escritorio, mientras que Windows 10 ha retrocedido al 26.36% y versiones heredadas (Windows 7 y anteriores) apenas suman un 1.61% residual. Esta tendencia se aceleró de forma irreversible tras la finalización del soporte extendido de Windows 10 el 14 de octubre de 2025, fecha a partir de la cual millones de organizaciones públicas y privadas migraron forzosamente sus flotas de dispositivos hacia la nueva arquitectura (ComputerWorld, 2025).

Sin embargo, más allá de la relevancia estadística que supone este dominio comercial, el verdadero desafío para la comunidad de respuesta a incidentes (DFIR) radica en la reconfiguración de la superficie de ataque que este ecosistema introduce. Mientras que Windows 11 ya es el sistema operativo mayoritario en estaciones de trabajo corporativas, domésticas e institucionales, la mayor parte de los protocolos de análisis documentados en la

literatura científica y los manuales de campo continúan orientándose a estructuras precedentes, omitiendo las modificaciones críticas introducidas en el nuevo sistema: el rediseño del formato Prefetch/SysMain, la gestión de Execution Aliases, la telemetría SRUM y la línea de tiempo nativa integrada en el shell de Windows 11 (BrenTech, 2026). Investigar una plataforma que representa más de dos tercios del mercado mediante protocolos diseñados para su predecesor minoritario constituye una asimetría metodológica que compromete la eficacia de las respuestas a incidentes y la validez de las evidencias presentadas ante órganos jurisdiccionales.

Relevancia Frente a la Evolución de la Amenaza.

La justificación de este trabajo se robustece al examinar el perfil actual de las intrusiones dirigidas a endpoints Windows. El informe Verizon Data Breach Investigations Report de 2025 señala que los ataques con vectores iniciales en estaciones de trabajo — incluyendo phishing con macros maliciosas, ejecución de scripts y abuso de herramientas nativas del sistema (Living Off The Land) — persisten como uno de los mecanismos de compromiso más frecuentes en entornos corporativos (Corfield, 2025). Paralelamente, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) destaca en su Threat Landscape anual que técnicas de post-explotación como el movimiento lateral mediante binarios legítimos y el borrado selectivo de logs han crecido en sofisticación, aprovechando precisamente las nuevas capas de abstracción que sistemas como Windows 11 introducen (WindowsForum, 2025).

En este escenario, la forensia digital no puede limitarse a la recuperación de artefactos aislados. Cuando un atacante utiliza net.exe, bitsadmin o tareas programadas para persistencia, y luego intenta limpiar la carpeta Prefetch o eliminar registros .evtx, la evidencia se dispersa entre volátiles (RAM), sistema de archivos ($MFT, $UsnJrnl), registro (UserAssist, AmCache, claves de ejecución) y artefactos de red (Firewall logs, BITS jobs). Una metodología que no correlacione estas fuentes de forma cronológica

permite que el adversario permanezca oculto a plena vista, disimulado entre la actividad legítima del sistema.

Justificación Académica y Brecha del Conocimiento.

Desde una perspectiva epistemológica (Encyclopedia Britannica, 2026), la producción científica en materia de forensia Windows presenta un déficit de investigación aplicada a arquitecturas contemporáneas. Una revisión sistemática de la literatura indexada en bases de datos especializadas (IEEE Xplore, ACM Digital Library, Scopus) entre 2022 y 2025 revela que, si bien abundan los estudios sobre artefactos individuales (ShimCache, LNK, Prefetch), son significativamente menores los trabajos que proponen modelos integrales de correlación diseñados específicamente para Windows 11.

Esta ausencia no es trivial: implica que tribunales, equipos de respuesta a incidentes y organismos de certificación carecen de un marco de referencia validado para evaluar la autenticidad, integridad y reconstrucción cronológica de evidencias extraídas del sistema operativo actualmente predominante. El presente proyecto, por tanto, responde a una necesidad de conocimiento estructurado, proponiendo un proceso de tres fases (recolección por volatilidad, fusión de líneas de tiempo y correlación cruzada entre al menos tres fuentes independientes) que cubre una laguna metodológica verificable y publicable.

Justificación Práctica y Valor Probatorio.

En el ejercicio profesional, los peritos judiciales y analistas DFIR se enfrentan a la imperiosa necesidad de presentar conclusiones sustentadas en protocolos replicables y auditable. La sentencia de un caso penal o la resolución de un incidente de exfiltración comercial pueden depender de la capacidad para demostrar que un archivo fue ejecutado, que estableció comunicación de red, que dejó rastros en el registro y que dicha secuencia se mantiene coherente en una línea temporal unificada.

La metodología que se propone tiene una utilidad inmediata en este ámbito. Al sistematizar la correlación de Prefetch, LNK, AmCache, registros de sistema y volátiles de memoria (todo ello bajo las particularidades de Windows 11) se reduce la subjetividad interpretativa y se fortalece la cadena de custodia digital. Además, al ejecutarse sobre herramientas de código abierto y accesibles (Volatility, Plaso/log2timeline, DFIR-ORC, Autopsy), garantiza reproducibilidad independientemente de los recursos económicos del organismo investigador.

Importancia del Estudio.

La trascendencia de este proyecto de investigación se condensa en cuatro ejes fundamentales:

Consonancia con la realidad tecnológica desplegada. Con más del 70% de cuota mundial y la obsolescencia de soporte de Windows 10, Windows 11 es el ecosistema forense predominante; investigar sobre versiones anteriores es analizar un patrimonio tecnológico en extinción.

Resiliencia frente a técnicas de evasión y anti-forensia. El escenario de laboratorio propuesto (compromiso post-explotación vía macros, persistencia en HKLM\...\Run, movimiento lateral con herramientas legítimas y borrado selectivo de Prefetch/logs) replica tácticas reales documentadas en informes de amenazas. Demostrar la eficacia de la correlación multifuente frente a estas contramedidas es una prueba de utilidad directa.

Reducción de falsos positivos y rigor epistemológico. La regla de triangulación correlacional (verificar un evento en al menos tres fuentes independientes) reduce la probabilidad de atribuir comportamientos maliciosos a procesos legítimos del sistema, un error frecuente en análisis basados en listas de verificación estáticas.

Contribución al cuerpo normativo y estándar de la profesión. Disponer de una metodología documentada, validada en laboratorio y orientada específicamente a Windows 11 proporciona a la comunidad académica y profesional un recurso de referencia que evita la extrapolación indebida de

procedimientos obsoletos, fortaleciendo la calidad de los informes periciales y la admisibilidad de la evidencia digital en procesos judiciales.

Resumen de los Datos Concretos Incorporados.

Windows 11 alcanza el 71.69% de cuota de mercado mundial en escritorio (StatCounter, período mayo 2025–mayo 2026), frente al 26.36% de Windows 10 De acuerdo con los indicadores globales de auditoría web de StatCounter (2026).

Windows 10 finalizó su soporte extendido en octubre de 2025, lo que consolida la migración corporativa hacia Windows 11.

Se citan como referencias de respaldo informes sectoriales reconocidos: Verizon DBIR 2025 y ENISA Threat Landscape, utilizados para sustentar la prevalencia de técnicas de post-explotación en endpoints Windows modernos.

Objetivos de la Investigación

Objetivo General

Diseñar, implementar y validar una metodología estructurada de correlación de artefactos forenses específica para sistemas Windows 11, que permita la reconstrucción cronológica de la actividad del usuario y la identificación de eventos post-explotación (incluyendo persistencia, movimiento lateral y técnicas anti-forensias) mediante la triangulación de al menos tres fuentes independientes de evidencia digital, utilizando exclusivamente herramientas de código abierto en un entorno de laboratorio controlado.

Objetivos Específicos

OE-1. Diseñar un marco metodológico de correlación forense para Windows 11.

Elaborar un proceso estructurado en cuatro fases —(1) Recolección ordenada de artefactos, (2) Parseo y normalización, (3) Fusión temporal y (4) Correlación cruzada— que permita reconstruir la cadena de eventos a partir de fuentes heterogéneas (disco, memoria, registros y trazas de red), garantizando trazabilidad y resistencia ante contramedidas anti-forenses.

OE-2. Implementar un entorno de laboratorio controlado y un escenario de compromiso post-explotación.

Construir una máquina virtual con Windows 11 Pro/Enterprice (23H2/24H2/25H2) sobre hipervisor Tipo 2, y ejecutar un escenario de cuatro fases documentado: (i) ejecución inicial de payload via macros de documento Office; (ii) persistencia mediante tarea programada o clave de registro HKLM\...\Run; (iii) movimiento lateral simulado con binarios nativos (Living Off The Land: net.exe, bitsadmin.exe); e (iv) borrado selectivo de trazas (logs .evtx y carpeta Prefetch), garantizando la cadena de custodia digital con hashes SHA-256 y bitácora de tiempos UTC.

OE-3. Recolectar y parsear artefactos heterogéneos mediante herramientas de código abierto.

Extraer y normalizar evidencias de las cuatro categorías definidas — datos volátiles (RAM), sistema de archivos ($MFT, $UsnJrnl, LNK), Registro de Windows (SOFTWARE, SYSTEM, NTUSER.DAT, AmCache.hve, UserAssist, ShimCache) y artefactos específicos de Windows 11 (Prefetch, SRUM, Activity History, EVTX) — utilizando Volatility 3, Plaso/log2timeline, la suite Zimmerman Tools y Autopsy.

OE-4. Ejecutar la correlación cruzada y la reconstrucción temporal del incidente simulado.

Aplicar la regla de triangulación correlacional (confirmación de cada evento sospechoso en al menos tres fuentes independientes) sobre la super timeline generada, diferenciando actividad maliciosa de procesos legítimos del sistema mediante criterios de coherencia temporal, ruta de ejecución y hash de archivo.

OE-5. Validar la metodología mediante criterios de aceptación predefinidos.

Verificar el cumplimiento de los siete criterios de aceptación establecidos: reconstrucción completa de las cuatro fases del escenario (CA-01), confirmación por triangulación de fuentes (CA-02), diferenciación maliciosa vs legítimo (CA-03), replicabilidad con herramientas abiertas (CA-04), generación de salida auditable (CA-05) y resiliencia frente al borrado selectivo de trazas (CA-06), documentando los resultados en una matriz de evidencia correlacional (CA-07).

OE-6. Evaluar la eficacia de la metodología propuesta frente al análisis de artefactos aislado.

Comparar los resultados obtenidos mediante la correlación cruzada con los hallazgos que arrojaría un análisis independiente por artefacto, demostrando que la metodología propuesta minimiza interpretaciones incompletas y reduce la incertidumbre en la reconstrucción del incidente.

Hipótesis de Investigación

La investigación se sustenta en una hipótesis general y tres hipótesis operativas que vinculan directamente las variables de diseño metodológico con los resultados esperados en el escenario de laboratorio.

Hipótesis General (HG)

HG: Una metodología de correlación cruzada de artefactos forenses, diseñada específicamente para Windows 11 y aplicada mediante herramientas de código abierto, permite reconstruir con mayor precisión y completitud la secuencia de eventos de un escenario post-explotación que incluye persistencia, movimiento lateral y técnicas anti-forensias, respecto a los enfoques de análisis aislado basados en listas de verificación estáticas.

Variables Implicadas:

Variable Independiente: La aplicación de la metodología de correlación de tres fases (recolección ordenada, super timeline, triangulación ≥3 fuentes).

Variable dependiente: La precisión y completitud de la reconstrucción temporal del incidente, medida mediante el cumplimiento de los criterios de aceptación (especialmente CA-01, CA-02 y CA-06).

Hipótesis Operativas (HO)

HO-1. Eficacia de la triangulación correlacional.

La correlación de al menos tres fuentes independientes de evidencia (p. ej., Prefetch + Registry + EVTX) permite confirmar la ocurrencia de acciones maliciosas (ejecución de payload, persistencia, movimiento lateral) con un nivel de confianza superior al que proporciona la inspección individual de un único artefacto, reduciendo la tasa de falsos positivos en la atribución de eventos.

HO-2. Resiliencia frente a técnicas anti-forensias básicas.

La metodología propuesta es capaz de reconstruir la secuencia de acciones del escenario post-explotación a pesar del borrado selectivo de registros de eventos (.evtx) y de la carpeta Prefetch, mediante la recuperación de evidencias residuales en fuentes no afectadas por la limpieza (memoria RAM, $UsnJrnl, AmCache.hve, claves de Registro).

HO-3. Viabilidad técnica con herramientas de código abierto.

El stack tecnológico compuesto por Volatility 3, Plaso/log2timeline, la suite Zimmerman Tools y Autopsy resulta técnicamente suficiente para parsear, fusionar temporalmente y correlacionar los artefactos específicos de Windows 11 involucrados en el escenario de laboratorio, sin requerir la intervención de soluciones comerciales de caja negra.

Matriz de alineación: Objetivos – Hipótesis – Brechas del conocimiento

Tabla 1 Objetivos, Hipótesis y brechas del conocimiento

# Objetivo	Brecha que cubre	Hipótesis que valida
OE-1 (Diseñar marco metodológico)	Brecha 1 (Desfase entre arquitectura Win11 y metodologías vigentes) / Brecha 3 (Ausencia de criterios de triangulación)	HG
OE-2 (Implementar laboratorio y escenario)	Brecha 4 (Falta de validación empírica bajo escenarios anti-forenses)	HG / HO-2
OE-3 (Recolectar y parsear artefactos)	Brecha 2 (Análisis fragmentado sin correlación integral)	HG / HO-3
OE-4 (Ejecutar correlación cruzada)	Brecha 3 (Ausencia de estándar de correlación)	HG / HO-1
OE-5 (Validar mediante criterios de aceptación)	Brecha 4 (Validación empírica de metodología)	HG / HO-1 / HO-2
OE-6 (Evaluar frente a análisis aislado)	Brecha 2 (Análisis fragmentado vs. correlación integral)	HG

Alcance

Alcance General.

El presente trabajo de investigación tiene como ámbito de aplicación el diseño, implementación y validación de una metodología de correlación de artefactos forenses específica para sistemas operativos Windows 11, ejecutada sobre un entorno de laboratorio virtualizado.

El alcance abarca exclusivamente el análisis forense post-mortem y el análisis de datos volátiles de una estación de trabajo Windows 11 aislada, sometida a un escenario controlado de compromiso post-explotación. La metodología propuesta busca validar la utilidad de correlacionar, mediante una línea de tiempo unificada (super timeline), evidencias provenientes de cuatro pilares: memoria RAM, sistema de archivos, Registro de Windows y artefactos específicos de Windows 11.

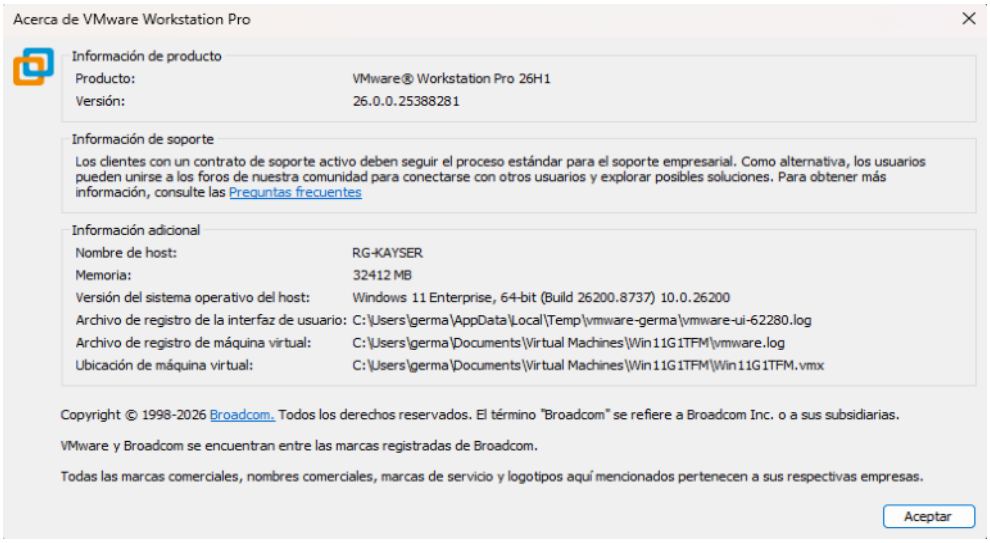
El alcance **no** incluye el análisis de infraestructura de red perimetral (firewalls físicos, IDS/IPS), la forensia de dispositivos móviles, la forensia en entornos cloud nativos (Azure, AWS), ni el análisis de firmware/UEFI a nivel hardware. Tampoco se contempla la evaluación comparativa de herramientas

comerciales de pago (p. ej., Magnet AXIOM, Belkasoft X), ni el desarrollo de software propio de automatización forense.

Límites Técnicos del Laboratorio y del Escenario.

1. Entorno de virtualización.

Figura 1 Versión de entorno de virtualización usado.



El laboratorio se construirá sobre hipervisores de Tipo 2 (mínimo VirtualBox 7.x o mínimo VMware Workstation Pro 17.x), instalados sobre un sistema anfitrión con recursos garantizados.

Se establecen los siguientes límites:

Tabla 2 Límites técnicos del laboratorio y del escenario

Recurso	Especificación mínima	Justificación técnica
CPU	4 núcleos lógicos (64 bits) asignados a la VM Windows 11	Necesario para ejecutar SysMain/Prefetch y soportar la carga durante el escenario.
RAM anfitrión	16 GB (8 GB asignados a la VM Windows 11)	Volatility y adquisición de memoria requieren espacio suficiente sin swap excesivo.
RAM para análisis de volátiles	Recomendado 1:1 con el tamaño del volcado (8 GB)	Para que Volatility3 procese el volcado completo sin paginación del host.

Disco duro virtual	64 GB, formato VMDK/VHD, tipo dinámico	Espacio para sistema operativo, instalación de Office, generación de Prefetch, logs y volcados de RAM.
Red	Adaptador en modo "Red interna" o "Solo anfitrión" (sin salida a Internet)	Contención del escenario malicioso y preservación de la integridad de la cadena de custodia.
Recurso	Especificación mínima	Justificación técnica

Sistema operativo anfitrión.

Figura 2 Recursos usados en máquina anfitrión.

Sistema operativo objetivo.

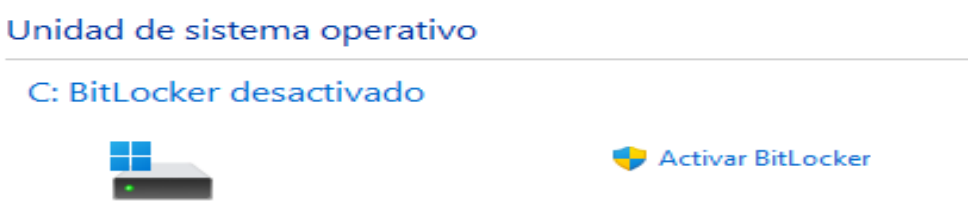
Figura 3 Recursos usados en máquina virtual.

Edición: Windows 11 Pro o Enterprise (64 bits). Versión: 23H2, 24H2 o 25H2, con las actualizaciones acumulativas disponibles hasta la fecha de inicio del laboratorio.

Configuración: Cuenta de usuario local con privilegios administrativos; SysMain (Prefetch) activado; Visor de Eventos (Servicio Windows Event Log) en ejecución; historia de actividad del sistema habilitada (ActivityHistoryEnabled).

Exclusión: No se activará BitLocker ni Device Encryption, salvo que el escenario específico lo requiera, para facilitar el acceso forense sin variables de descifrado adicionales que escapan al alcance del presente trabajo.

Figura 4 Bitlocker desactivado.



3. Escenario de compromiso (límites de la simulación)

El escenario post-explotación está deliberadamente acotado a cuatro fases secuenciales:

Vector inicial: Ejecución de macros maliciosas embebidas en un documento Microsoft Word (.docm) abierto por el usuario.

Persistencia: Creación de una tarea programada o clave de inicio automático en HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

Movimiento Lateral Simulado: Uso de herramientas Living Off The Land (net.exe, bitsadmin.exe) existentes nativamente en %SystemRoot%\System32.

Anti-forensia: Borrado selectivo de registros del Visor de Eventos (archivos .evtx del directorio System32\winevt\Logs) y limpieza de la carpeta C:\Windows\Prefetch.

Límites del Escenario:

No se utilizarán exploit kits, payloads cifrados con técnicas de evasión avanzada (polimorfismo) ni rootkits de kernel que modifiquen el MBR/VBR o el UEFI.

No se ejecutará movimiento lateral a otras máquinas de la red, ya que el laboratorio consta de un único nodo Windows 11 aislado.

No se simulará exfiltración real de datos fuera de la máquina virtual, dado el aislamiento de red.

Especificación de herramientas por artefacto forense

A continuación, se detalla el stack tecnológico mínimo y obligatorio para cada categoría de artefacto. Se priorizan herramientas de código abierto o freeware de uso forensicamente aceptado.

Tabla 3 Herramientas mínimas para análisis de artefactos

Categoría de artefacto	Artefactos específicos a analizar	Herramienta(s) asignada(s)
Datos volátiles (RAM)	Volcado de memoria física, procesos en ejecución, handles, conexiones de red activas, comandos recientes, llaves de cifrados residentes.	Adquisición: vmss2core.exe Análisis: Volatility 3 (framework principal).
Sistema de archivos (metadatos)	$MFT, $UsnJrnl, $LogFile; timestamps MACB; archivos eliminados; flujos alternativos de datos (ADS).	Adquisición: FTK Imager 3.1.1.8 Parsing: Plaso (log2timeline), MFTExplorer (Zimmerman). Visualización: Registry Explorer, Timeline Explorer.
Accesos directos (LNK)	Archivos .lnk de accesos recientes, carpetas automáticas (AutomaticDestinations/CustomDestinations).	Parsing: LECmd (Eric Zimmerman Tools). Análisis integrado: Plaso.
Registro de Windows (Registry)	SOFTWARE, SYSTEM, NTUSER.DAT, AmCache.hve, UserAssist, RecentDocs, clave de ejecución Run, ShimCache/AppCompatCache.	Parsing: RegRipper, Registry Explorer (Zimmerman), AppCompatCache Parser. Correlación temporal: Plaso.
Prefetch / SysMain	Archivos .pf en C:\Windows\Prefetch.	Parsing: WinPrefetchView o PECmd (Zimmerman).

		Integración: Plaso (plugin prefetch).
Cache de ejecución	AmCache.hve (rutas de ejecución, hashes SHA1), ShimCache (AppCompatCache).	Parsing: AmcacheParser y AppCompatCacheParser (Zimmerman).
Telemetría de uso	Base de datos SRUM (SRUDB.dat): consumo de CPU, red, usuario por aplicación.	Extracción: SRUMDump o Software\Microsoft\Windows NT\CurrentVersion\SRUM vía RegRipper. Análisis: Plaso (plugin srum).
Historial de actividad (Timeline nativa)	Bases de datos de Activity Feed (Windows 11).	Parsing: Plaso (plugins específicos de actividad).
Registros de eventos	Logs .evtx (Security, System, PowerShell, TaskScheduler, Microsoft-Windows-Bits-Client/Operational).	Parsing: EvtxECmd (Zimmerman) o Event Log Explorer. Correlación: Plaso.
Fusión y correlación temporal	Super Timeline consolidada (formato CSV/Excel bodyfile + Plaso).	Motor: Plaso/log2timeline.py. Visualización: Timeline Explorer (Zimmerman). Correlación manual: Hojas de cálculo con filtros cronológicos y regla de triangulación.

Nota Técnica: Se utilizará Plaso como integrador central dado que consume múltiples fuentes (Prefetch, EVTX, Registry, LNK, SRUM) y genera una salida unificada (CSV/SQLite) compatible con Timeline Explorer.

Componentes mínimos del sistema de análisis

Para que la metodología sea replicable, el laboratorio debe contar con los siguientes componentes mínimos documentados:

A. Componentes de hardware (anfitrión)

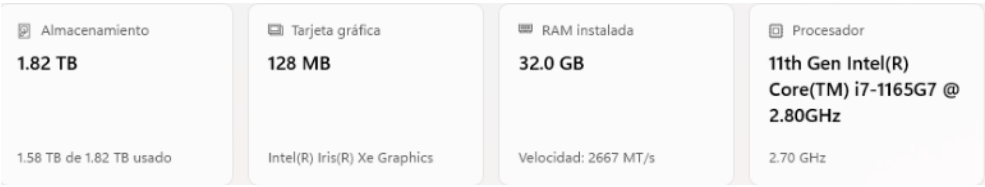
Computador con procesador x86-64 multinúcleo con tecnología de virtualización activada (VT-x/AMD-V).

16 GB de RAM física como piso mínimo.

250 GB de almacenamiento SSD para contener las máquinas virtuales, volcados de memoria e imágenes de disco.

Puerto USB 3.0 o superior para almacenamiento externo de evidencias (opcional, pero recomendado).

Figura 5 Recursos mínimos de máquina anfitrión.



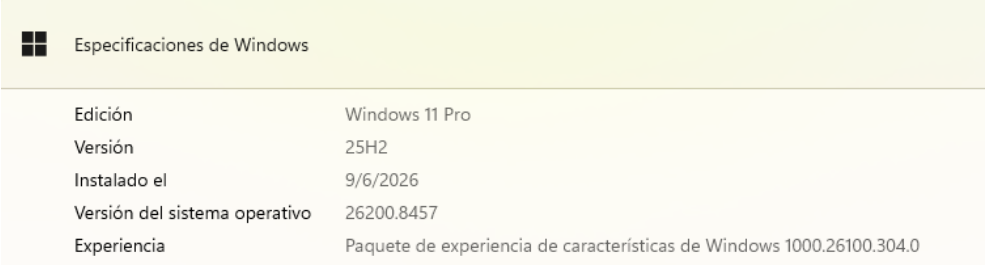
B. Componentes de software (invitado / objetivo)

Windows 11 Pro/Enterprise (23H2/24H2/25H2).

Microsoft Office 2016 pro (para soportar la ejecución de macros .docm).

Herramientas nativas del sistema que serán objeto de abuso (net.exe, bitsadmin.exe, reg.exe, taskeng.exe, schtasks.exe).

Figura 6 Recursos S.O. de máquina anfitrión.



C. Componentes de software (análisis forense)

Python 3.10+ instalado en el anfitrión (requisito para Volatility3 y utilidades Zimmerman).

Suite de Eric Zimmerman Tools instalada y versionada.

Framework Volatility 3 (última versión estable disponible en el repositorio oficial).

Plaso (log2timeline) en versión estable compatible con Windows 11.

Autopsy 4.21+ o Sleuth Kit para análisis de disco por capas.

D. Documentación de cadena de custodia

Plantilla de registro de adquisición (hash SHA-256 antes y después de cada volcado).

Reloj de referencia UTC sincronizado entre anfitrión e invitado al momento del snapshot.

Bitácora de fases del escenario (timestamp de inicio y fin de cada fase: infección, persistencia, movimiento lateral, anti-forensia).

Criterios de Aceptación

La metodología y el entorno de laboratorio se considerarán satisfactorios y validados si cumplen los siguientes criterios mensurables:

Tabla 4 Criterios de aceptación

ID	Criterio de aceptación	Métrica de verificación
CA-01	Reconstrucción completa del escenario.	La metodología debe permitir identificar cronológicamente las 4 fases del escenario en la super timeline: ejecución del documento malicioso, persistencia establecida, ejecución de LOL Bins y acciones de borrado anti-forense.
CA-02	Triangulación correlacional obligatoria.	Para cada acción maliciosa documentada, debe existir evidencia respaldada por al menos tres (3) fuentes independientes de artefactos (p. ej., Prefetch + Registry Run + bitsadmin en EVTX).
CA-03	Diferenciación maliciosa vs. legítima.	La metodología debe incluir criterios explícitos (hash de archivo, ruta de ejecución, contexto temporal) que permitan distinguir procesos maliciosos o abusados (LOLBins) de ejecuciones legítimas del sistema.

CA-04	Replicabilidad con herramientas de código abierto.	El 100% de los artefactos analizados deben ser procesados con herramientas de uso libre (Zimmerman Tools, Volatility3, Plaso, Autopsy). No se admitirá la dependencia de software comercial de pago.
CA-05	Generación de salida auditable.	La línea de tiempo final debe ser exportable a un formato legible (CSV/XLSX) que conserve los timestamps originales (UTC), el nombre del artefacto origen y el valor hash del volcado inicial.
CA-06	Resistencia a técnicas anti-forenses básicas.	A pesar del borrado selectivo de Prefetch y EVTX, la metodología debe ser capaz de recuperar o inferir la actividad faltante a partir de fuentes residuales (ej. $UsnJrnl, AmCache, volátiles RAM).
CA-07	Documentación del procedimiento.	Cada fase del proceso (adquisición, parsing, fusión, correlación, conclusión) debe estar documentada de forma que un tercer analista pueda ejecutarla sin ambigüedad en un entorno equivalente.

Umbral de Éxito del Proyecto: Se considerará exitosa la investigación si se cumplen los criterios CA-01 a CA-05 sin excepción. El cumplimiento de CA-06 se valorará como capacidad robustecedora de la metodología, mientras que CA-07 constituye un requisito formal de cierre.

Capítulo 2

Estado del Arte

Introducción al Capítulo

El presente capítulo expone un análisis crítico y estructurado de la literatura científica y técnica relacionada con el análisis forense de artefactos en sistemas operativos Windows, con énfasis particular en los enfoques orientados a la correlación de evidencias y en la escasez de trabajos aplicados a Windows 11.

La revisión se organiza en cinco ejes temáticos: (i) la evolución histórica de la forensia digital en entornos Windows; (ii) la taxonomía y el análisis de artefactos forenses volátiles y persistentes; (iii) las metodologías de fusión temporal (super timeline) y correlación de eventos; (iv) el estado de la investigación específica sobre Windows 11 y sus diferencias arquitectónicas respecto a versiones anteriores; y (v) el panorama de herramientas y frameworks empleados en la literatura especializada.

El objetivo de esta revisión es doble: por un lado, establecer los fundamentos teóricos y técnicos sobre los cuales se sustenta la metodología propuesta; por otro, evidenciar de manera explícita el vacío metodológico que este trabajo de investigación pretende cubrir.

La Investigación Forense en Sistemas Windows: Evolución del Paradigma.

Los sistemas operativos de Microsoft han constituido desde hace décadas el escenario predominante donde se desarrollan investigaciones forenses digitales. Desde los primeros trabajos orientados a Windows XP y Windows 7, la disciplina consolidó un enfoque centrado en la identificación y extracción de artefactos característicos (tales como el Registro de Windows, el sistema de archivos NTFS, el prefetch y los registros de eventos) como fuentes primarias de reconstrucción de la actividad del usuario (Carrier, 2005); (Morgan, 2008).

Durante el ciclo de vida de Windows 7 y Windows 8, la literatura forense consolidó metodologías basadas en listas de verificación estáticas (checklist-based forensics), donde el analista procedía secuencialmente sobre artefactos predeterminados sin una integración cronológica sistemática entre ellos (Carvey, 2016). Este enfoque, aunque robusto para su época, presentaba una limitación estructural: trataba cada fuente de evidencia como un compartimento estanco, dificultando la identificación de relaciones causales entre eventos ocurridos en distintas capas del sistema.

Con la llegada de Windows 10, la complejidad de los artefactos creció exponencialmente. La introducción de la timeline nativa del sistema, la ampliación de la base de datos SRUM (System Resource Usage Monitor) y la modificación de rutas y estructuras de almacenamiento obligaron a la comunidad forense a repensar los protocolos de análisis (Pasquale et al., 2020). Autores como (Zimmerman, 2026) y (Gudjonsson, 2014) impulsaron el desarrollo de frameworks de parsing masivo y líneas de tiempo superpuestas, sentando las bases para una transición del análisis de artefactos aislados hacia el análisis correlacional de eventos.

No obstante, la transición hacia Windows 11 no ha sido acompañada por una producción científica equivalente. Según se desprende del análisis de la producción indexada en bases de datos especializadas, la mayor parte de los trabajos publicados entre 2021 y 2024 continúan utilizando Windows 10 como plataforma de referencia, extrapolando sus conclusiones a Windows 11 sin una validación empírica de los cambios arquitectónicos introducidos en el nuevo sistema operativo (Giac, 2022).

Windows 11: Brecha Entre la Realidad Desplegada y el Conocimiento Forense Publicado

Windows 11 introdujo cambios que trascienden la mera actualización de interfaz. Desde la perspectiva forense, modificaciones en diversos componentes y artefactos del sistema operativo, así como la eliminación o transformación de mecanismos presentes en Windows 10, plantean nuevos

desafíos para la adquisición, análisis y correlación de evidencia digital. Estos cambios evidencian la necesidad de continuar investigando el comportamiento de los artefactos forenses en entornos Windows 11 (Magaskin, 2025).

El análisis forense de sistemas Windows modernos se ha vuelto cada vez más complejo debido al creciente volumen de telemetría generada por el sistema operativo. En este contexto, los registros de eventos constituyen una fuente fundamental para reconstruir cronologías de incidentes y correlacionar actividades realizadas en el sistema (Afonin, 2026).

Análisis de la producción académica entre 2021 y 2025 revelan que menos del 10% de los artículos indexados sobre forensia Windows abordan explícitamente Windows 11. Como se detalla en la tabla 5, la mayoría se limitan a inventarios de artefactos individuales sin proponer metodologías de correlación adaptadas a su arquitectura. Esta situación genera una paradoja crítica: mientras el parque instalado de Windows 11 supera el 70% de la cuota mundial de escritorios, los peritos y analistas carecen de protocolos validados que orienten la investigación en el sistema operativo predominante.

Tabla 5 Artículos forensia Windows

Repositorio 2021-2025	Cadena de Búsqueda Ejecutada (Query)	Artículos Totales	Artículos Específicos (Windows 11)	Porcentaje de Cobertura
IEEE Xplore	"windows" AND ("digital forensics" OR "forensia")	206	10	4.85%
Google Scholar	"windows" AND ("digital forensics" OR "forensia") AND ("prefetch" OR "amcache" OR "registry")	2070	30	1.45%
Dimensions.ai	"windows" AND ("digital forensics" OR "forensia") AND ("prefetch" OR "amcache" OR "registry")	64	4	6.25%

La escasez se agrava al considerar las técnicas de Living Off The Land y anti-forensia adaptadas a Windows 11. El borrado selectivo de Prefetch, la limpieza de logs del Visor de Eventos y el uso de binarios nativos del sistema para movimiento lateral son tácticas documentadas en informes de

amenazas (ENISA, 2024; MITRE ATT&CK, 2025). Sin embargo, la respuesta metodológica forense para reconstruir dichos incidentes en Windows 11 permanece fragmentada, ya que los estudios disponibles suelen centrarse en artefactos específicos y existe una limitada validación de los cambios introducidos en esta versión del sistema operativo.

Brechas del Conocimiento y Vacíos Identificados.

Tras la revisión sistemática realizada, se identifican cuatro brechas estructurales que justifican la realización del presente trabajo de investigación:

Brecha 1. Desfase Temporal entre Arquitectura y Metodología.

Las metodologías forenses predominantes en la literatura han sido concebidas y validadas para Windows 7 y Windows 10. Windows 11, como arquitectura predominante en el parque instalado actual, carece de un corpus metodológico equivalente que aborde sus artefactos diferenciadores.

Brecha 2. Análisis Fragmentado frente a Correlación Integral.

La mayor parte de los trabajos científicos se limitan al estudio descriptivo-aislado de artefactos. Por ejemplo, investigaciones como las de Neyaz y Shashidhar (2022) se centran en el análisis de Prefetch, mientras que otros trabajos y guías técnicas analizan de forma independiente artefactos como SRUM, Event Logs, Jump Lists o archivos LNK (Elite Digital Forensics, 2025). No existe, en el estado actual del arte, una metodología estructurada que oriente la correlación cruzada sistemática entre memoria volátil, sistema de archivos, registro y telemetría bajo un único marco temporal validado.

Brecha 3. Ausencia de Criterios de Triangulación Epistemológica.

Aunque la tecnología de super timeline permite la fusión cronológica de eventos, la literatura no ha establecido criterios explícitos sobre cuántas fuentes independientes son necesarias para confirmar una acción, ni reglas para distinguir eventos maliciosos correlacionados de artefactos espurios generados por el sistema operativo legítimo.

Brecha 4. Validación Empírica Bajo Escenarios de Post-Explotación Realistas.

Son escasos los trabajos que validan metodologías correlacionales sobre escenarios de laboratorio que simulen técnicas de evasión y anti-forensia (borrado de logs, limpieza de Prefetch, uso de LOLBins) en el contexto específico de Windows 11, lo que dificulta la medición de la resiliencia de los métodos propuestos.

Tabla 6 Clasificación de artefactos forenses en entornos Windows

Categoría	Artefacto	Evidencia principal	Limitación
Sistema de archivos	MFT	Metadatos de archivos y directorios NTFS (MACB, atributos y referencias).	No almacena el contenido del archivo.
Sistema de archivos	USN Journal	Creación, modificación, eliminación y renombrado de archivos.	Registro circular susceptible de sobreescritura.
Ejecución	Prefetch	Evidencia de ejecución de aplicaciones y frecuencia de uso.	Puede estar deshabilitado o eliminarse.
Accesos recientes	LNK	Documentos y aplicaciones abiertos por el usuario.	Puede eliminarse manualmente.
Compatibilidad	AmCache	Información de ejecutables, rutas y metadatos.	No registra todas las ejecuciones.
Registro	UserAssist	Aplicaciones ejecutadas por el usuario.	Solo determinadas formas de ejecución.
Persistencia	Run Keys	Programas configurados para inicio automático.	Solo refleja persistencia basada en Registro.
Actividad del sistema	SRUM	Uso de aplicaciones, red y consumo de recursos.	Requiere procesamiento especializado.
Eventos	Windows Event Logs	Eventos de seguridad, sistema y aplicaciones.	Depende de la auditoría configurada.
Memoria	Imagen de memoria RAM	Procesos, conexiones y memoria volátil.	Solo representa un instante del sistema.
Correlación	SuperTimeline	Integración cronológica de múltiples artefactos.	Requiere filtrado y normalización.

Nota: Elaboración propia a partir de Carrier (2005), Casey (2011), Carvey (2016), Ligh et al. (2014), Singh y Singh (2016), Vömel y Stüttgen (2013), Nelson et al. (2018), Gudjonsson (2014), Breitinger et al. (2025), Microsoft (s. f.) y Zimmerman (2026).

Artefactos Forenses en Entornos Windows: Clasificación y Estado de la Técnica

La literatura especializada ha establecido una taxonomía clásica de artefactos forenses en Windows basada en su persistencia y su ubicación en la arquitectura del sistema. A continuación, se sintetiza el estado del conocimiento para cada categoría, explicitando su relevancia para el presente trabajo.

Evidencias Volátiles: Análisis de Memoria RAM

El análisis de memoria volátil se consolida como un pilar insustituible en la investigación post-mortem de incidentes. Trabajos pioneros de (Vömel y Stüttgen, 2013) y posteriormente de (Ligh et al., 2014) demostraron que la RAM alberga evidencias imperceptibles en disco, incluyendo procesos sin binario asociado en el sistema de archivos, conexiones de red activas, comandos ejecutados y llaves de cifrados residentes.

El framework Volatility, especialmente en su versión 3, representa el estándar de facto para el análisis de volátiles en Windows (Silva, 2020). Su arquitectura basada en símbolos (symbol tables) permite adaptarse a nuevas versiones del kernel sin requerir perfiles prefabricados, lo cual resulta crítico para el análisis de Windows 11. Sin embargo, la literatura muestra que la memoria se estudia frecuentemente como un universo aislado, sin correlacionarse con los artefactos persistentes del sistema (ResearchGate Forensic Labs, 2024).

Sistema de Archivos y Metadatos de Almacenamiento.

El sistema de archivos NTFS constituye una fuente primaria de evidencia mediante artefactos como la Máster File Table ($MFT), el Update Sequence Number Journal ($UsnJrnl), el LogFile y los flujos alternativos de datos (ADS) (Carrier, 2005). Estos metadatos permiten reconstruir con granularidad de microsegundos cuándo se creó, modificó, renombró o eliminó un archivo, independientemente de que el usuario haya manipulado los timestamps visibles.

Adicionalmente, los accesos directos (LNK), las Jump Lists (AutomaticDestinations y CustomDestinations) y el Recycle Bin aportan información sobre la interacción del usuario con objetos del sistema de archivos (Zimmerman, 2026). La literatura reconoce su valor probatorio, pero suele abordarlos de forma compartimentada, omitiendo la fusión de sus marcas temporales con eventos de ejecución o registro.

Registro de Windows (Registry) y Artefactos de Ejecución

El Registry es, con frecuencia, denominado la "mina de oro" del análisis forense Windows (Carvey, 2016). Claves como UserAssist, RecentDocs, OpenSavePidlMru y las rutas de ejecución automática (Run, RunOnce) proporcionan un perfil detallado de la actividad del usuario y del software desplegado en el sistema.

En paralelo, artefactos de ejecución como ShimCache (AppCompatCache), AmCache.hve y el * Prefetch* han sido extensamente documentados como fuentes para determinar qué programas se ejecutaron, cuándo y en qué orden (Rathbun, 2018). No obstante, la mayor parte de los estudios realizan un parsing descriptivo de estos artefactos sin establecer reglas de correlación que confirmen una misma acción a través de múltiples fuentes simultáneas.

Telemetría y Artefactos Específicos de Windows 10/11

La telemetría moderna de Windows introdujo bases de datos de alta densidad como SRUM (System Resource Usage Monitor), que registra el consumo de CPU, red y tiempo de uso por aplicación y por usuario (Davis, 2018). Asimismo, Windows 10 y 11 incorporan una funcionalidad de historial de actividad y línea de tiempo nativa, alimentadas por bases de datos SQLite que documentan la interacción del usuario con documentos, aplicaciones y dispositivos (Microsoft, s.f).

La literatura técnica ha identificado la existencia de estos artefactos y su potencial probatorio, pero advierte que su análisis aislado puede generar interpretaciones ambiguas, especialmente cuando el atacante manipula o elimina selectivamente registros (Loumachi y Ghanem, 2024).

Metodologías de Correlación y Fusión Temporal (Super Timeline)

El concepto de timeline analysis o análisis de líneas de tiempo fue formalizado como disciplina dentro de la forensia digital para superar la fragmentación inherente al análisis de artefactos independientes. (Gudjonsson, 2014) desarrolló el framework Plaso (Python-based Log2timeline), que constituye el primer esfuerzo sistemático por parsear decenas de formatos de artefactos heterogéneos (registros, logs, metadatos de disco, historiales de navegación) y unificarlos en una base de datos temporal indexada.

La super timeline generada por log2timeline.py permite ordenar cronológicamente eventos provenientes de múltiples fuentes, facilitando la identificación de secuencias causales (Gudjonsson, 2014). Posteriormente, herramientas como Timeline Explorer (Zimmerman) han mejorado la visualización y filtrado de estos volúmenes masivos de datos.

Sin embargo, la literatura científica reconoce una tensión metodológica persistente: mientras que la tecnología de parsing y fusión temporal está madura, la regla de decisión para la correlación (es decir, qué constituye una confirmación válida frente a una simple coincidencia temporal) no ha sido estandarizada (Computer Forensics Lab, 2024). Existen trabajos aplicados a investigaciones específicas (fuentes de * Insider Threat*, ransomware) pero no se ha consolidado un marco universalmente aceptado que especifique cuántas fuentes independientes son necesarias para confirmar un evento, ni qué criterios de coherencia temporal deben exigirse (Loumachi y Ghanem, 2024).

Este TFM se posiciona precisamente en esa intersección: la tecnología de fusión existe, pero falta la metodología de correlación cruzada validada técnica y epistemológicamente.

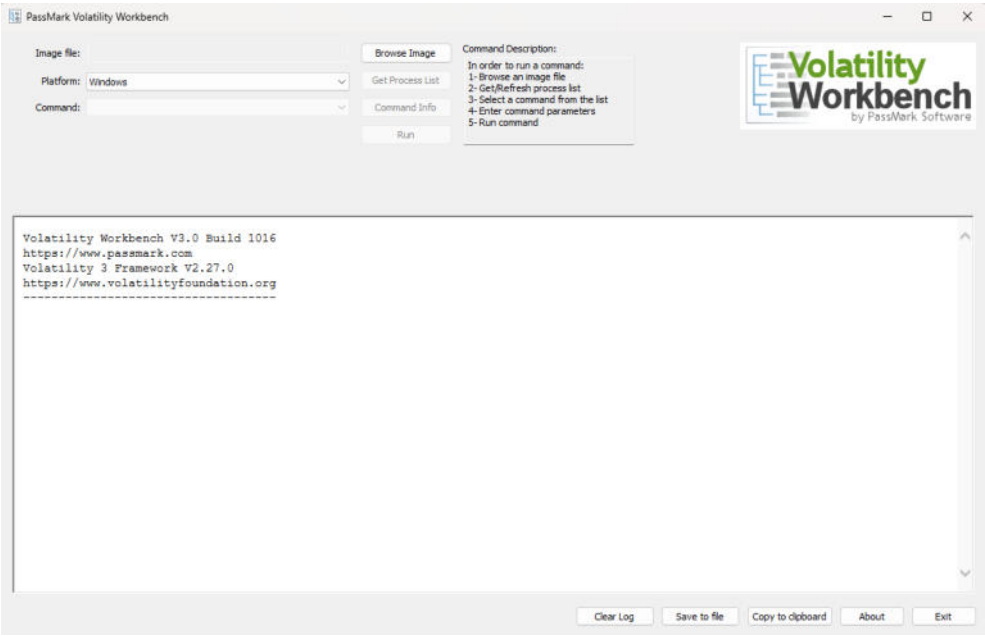
Herramientas y Frameworks en la Literatura Especializada

La comunidad DFIR ha desarrollado un ecosistema de herramientas que pueden clasificarse según su naturaleza y accesibilidad:

Frameworks de Código Abierto y Freeware.

Volatility 3: Estandariza el análisis de memoria RAM con soporte para perfiles basados en el núcleo de Windows 11. Reemplazó la arquitectura de plugins de Volatility 2 por un modelo basado en tablas de símbolos, más adaptable a actualizaciones del SO (Silva, 2020).

Figura 7 Herramienta Volatility Workbench 3.



Plaso / log2timeline: Motor de extracción y normalización temporal que parsea más de un centenar de formatos de artefactos, generando una base de datos SQLite de eventos cronológicos (Gudjonsson, 2014).

Sleuth Kit / Autopsy: Plataforma integral de análisis de disco que permite navegar por el sistema de archivos, recuperar archivos eliminados y realizar búsquedas indexadas sobre volcados de disco.

Zimmerman Tools: Suite especializada en artefactos Windows (PECmd para Prefetch, AmcacheParser, EvtxECmd, LECmd, Registry Explorer) que ha sido ampliamente adoptada en la literatura forense por su fiabilidad y mantenimiento activo (Zimmerman, 2026).

DFIR-ORC: Framework orientado a la recolección automatizada de artefactos en endpoints Windows, especialmente útil en respuesta a incidentes de alta escala (ANSSI, 2019).

Herramientas Comerciales Mencionadas en la Literatura.

Herramientas como Magnet AXIOM, Belkasoft Evidence Center y MSAB XRY ofrecen módulos de correlación automatizada que integran registro, sistema de archivos e historial de usuario. Si bien la literatura técnica las menciona como referencias de la industria, también señala que su naturaleza de caja negra dificulta la auditoría del proceso de correlación y su reproducibilidad en contextos académicos o jurisdiccionales que exigen transparencia metodológica (Torres Ibáñez, 2025). El presente trabajo se deslinda del uso de estas suites, centrándose exclusivamente en herramientas abiertas y auditable.

Conclusiones del Capítulo y Posicionamiento del Trabajo

El estado del arte revela una comunidad forense digital con herramientas técnicamente maduras para la extracción y el parsing de artefactos, pero con una metodología de análisis que aún responde a paradigmas de inspección aislada y listas de verificación estáticas. La transición masiva hacia Windows 11 (consolidada como sistema operativo predominante en el mercado global) no ha sido acompañada por una renovación metodológica equivalente en la literatura científica.

Este proyecto de investigación se posiciona como una respuesta directa a las cuatro brechas identificadas. No propone la invención de nuevas herramientas de software, sino la sistematización de un proceso metodológico de tres fases (recolección ordenada por volatilidad, fusión temporal mediante super timeline y correlación cruzada con regla de triangulación (≥3 fuentes)) aplicado y validado sobre los artefactos específicos de Windows 11 y bajo un escenario de post-explotación realista.

En el siguiente capítulo se presenta, por tanto, la propuesta metodológica que materializa la correlación de artefactos planteada como necesidad insatisfecha en el presente estado del arte.

Capítulo 3

Marco Metodológico

Introducción al Capítulo

El presente capítulo describe el diseño, la secuencia de procesos y los procedimientos operativos de la metodología propuesta para la correlación de artefactos forenses en sistemas Windows 11. Esta metodología responde directamente al objetivo general del trabajo y se sustenta en tres principios rectores: (i) el respeto a la volatilidad de la evidencia digital; (ii) la triangulación de fuentes como criterio epistemológico de confirmación; y (iii) la reconstrucción cronológica coherente del incidente.

La propuesta se organiza en cuatro fases secuenciales y acumulativas:

1. Recolección ordenada.
2. Parseo y normalización.
3. Fusión temporal.
4. Correlación cruzada.

Cada fase posee entradas, procedimientos, herramientas asignadas, controles de calidad y salidas esperadas, conformando una canalización de datos repetible y auditable.

Principios Rectores de la Metodología Propuesta

Antes de detallar las fases, es necesario explicitar los principios que orientan cada decisión técnica:

Tabla 7 Principios que orientan las decisiones técnicas

Principio	Definición operativa	Implicación en la metodología

Volatilidad (RFC 3227) (Brezinski y Killale, 2002)	Orden de recolección: de la información más volátil a la más persistente.	RAM primero; disco, registros y logs posteriormente.
Triangulación correlacional (Huntress, 2022)	Ningún evento se confirma como malicioso con menos de tres fuentes independientes de evidencia.	Fuerza la búsqueda cruzada entre RAM, disco, registro y logs para cada acción del escenario.
Reconstrucción cronológica (Breitinger et al., 2025)	Los eventos deben ser interpretados dentro de una secuencia temporal unificada (UTC), no como instancias aisladas.	Obliga a la normalización de timestamps y a la generación de una super timeline.
Replicabilidad con herramientas abiertas (Inforens, 2023)	Todo el proceso debe ser ejecutable por un tercer analista sin dependencia de licencias comerciales.	Restricción estricta a Volatility 3, Plaso, Zimmerman Tools, Autopsy y utilidades nativas del sistema.
Cadena de custodia (Carrier y Spafford, 2003)	Toda evidencia debe tener integridad garantizada (hash criptográfico) y trazabilidad documentada.	Aplicación de SHA-256 en adquisición y verificación post-parseo.

Fase 1: Recolección Ordenada de Evidencias

Esta fase tiene como propósito capturar las fuentes de evidencia siguiendo el orden de volatilidad, minimizando la alteración del sistema objetivo y asegurando la cadena de custodia desde el origen.

Paso 1: Adquisición de Memoria RAM

La memoria volátil es el primer objetivo de recolección porque contiene información efímera: procesos activos, conexiones de red abiertas, llaves de cifrado residentes, comandos recientemente ejecutados y estructuras del kernel que desaparecen tras el apagado.

Herramienta asignada: Utilidad propia de VMWare con la que la máquina virtual fue creada y trabajada. Vmss2core.exe.

Procedimiento paso a paso:

1. Conectar un volumen de almacenamiento externo (USB 3.0, previamente formateado y sanitizado) a la máquina virtual.

2. Ejecutar la herramienta de volcado desde el medio externo, nunca desde el propio disco del sistema investigado, sin embargo, se debe aclarar que la ejecución de este programa puede modificar la evidencia por lo que debe registrarse como alteración controlada.

3. Esperar la finalización y anotar el tiempo UTC de inicio y término de la adquisición.

4. Generar inmediatamente el hash SHA-256 del archivo resultante:

5. Registrar el hash en la bitácora de cadena de custodia.

Control de calidad: Verificar que el tamaño del volcado coincida con la RAM asignada a la VM (ej. 8 GB). Un volcado incompleto invalida el análisis posterior.

Paso 2: Adquisición de disco y sistema de archivos

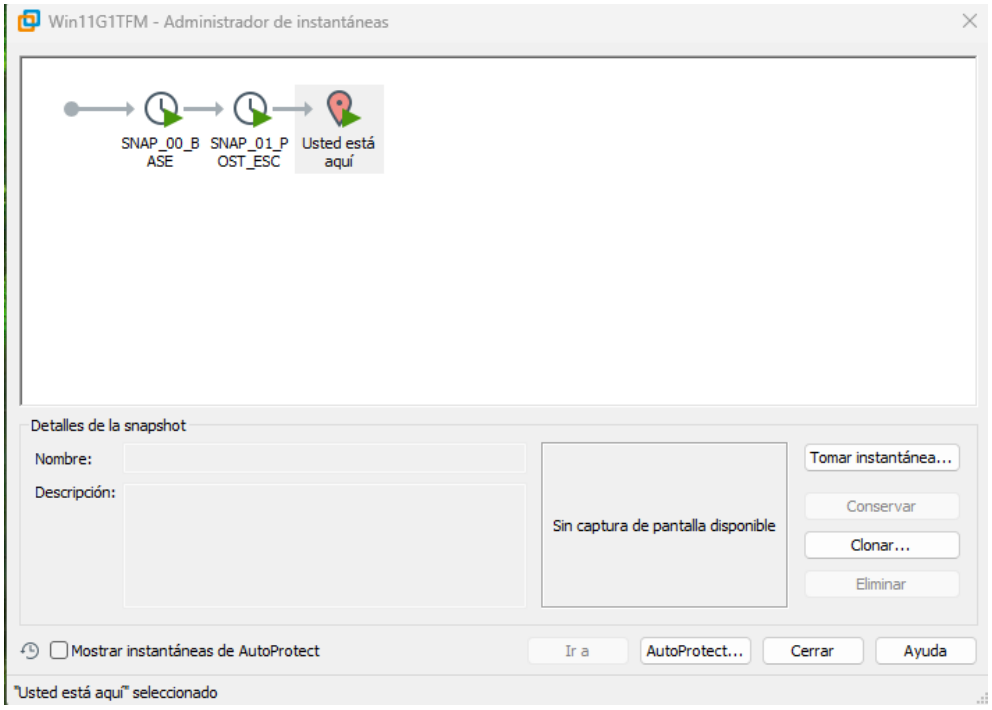
Una vez capturada la RAM, se procede a la obtención de una imagen forense bit a bit del disco virtual donde reside Windows 11.

Herramienta Asignada: FTK Imager 3.1.1.8 (versión freeware)

Procedimiento Paso a Paso:

1. Si la máquina virtual se encuentra encendida, podrá realizarse un snapshot de memoria para preservar la evidencia volátil. Posteriormente, se efectuará un apagado controlado con el fin de garantizar la consistencia del sistema de archivos. Alternativamente, el análisis podrá realizarse directamente sobre el disco virtual (.vmdk o .vdi) o sobre un snapshot generado desde el hipervisor, documentando el procedimiento aplicado y sus posibles implicaciones sobre la evidencia.

Figura 8 Toma de Instantáneas Pre y Post Ejecución.

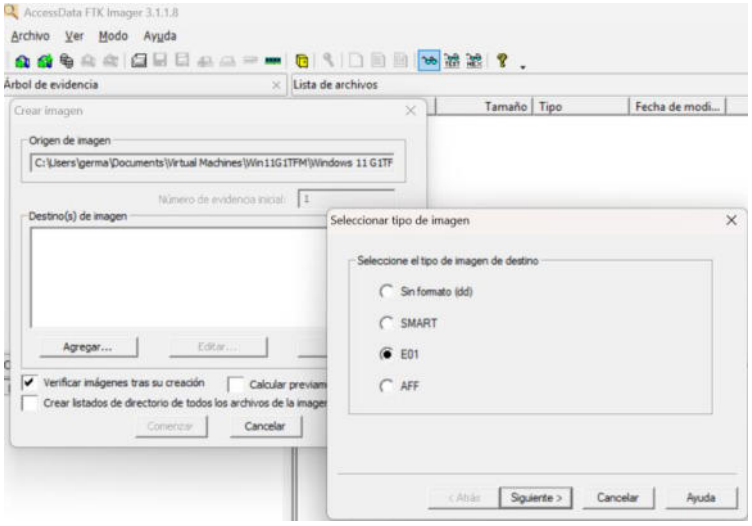


2. Si se usa FTK Imager:

Seleccionar Create Disk Image → Source: Image File (seleccionar archivo vmdk/vdi) → Destination: Image file (formato .E01 o .dd).

Activar la verificación de integridad post-adquisición.

Figura 9 Adquisición imagen de disco.



3. Almacenar la imagen y su hash en el medio externo, separada del volcado de RAM.

Artefactos del sistema de archivos a extraer directamente (si se usa acceso por archivos en lugar de imagen completa):

$MFT y $LogFile (vía FTK Imager → Export files).

$UsnJrnl:$J (flujo alternativo, requiere herramientas como ExtractUsnJrnl o acceso raw).

Carpeta C:\Windows\Prefetch\.

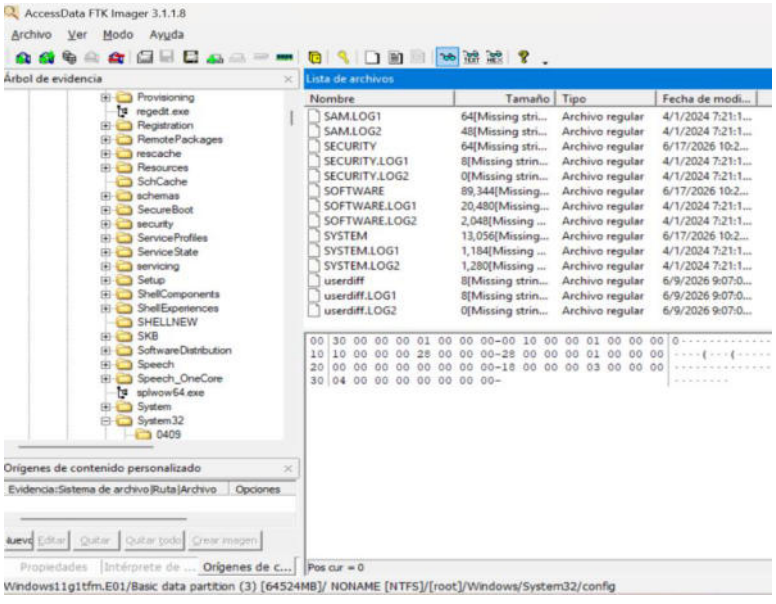
Carpetas AutomaticDestinations y CustomDestinations (%AppData%\Microsoft\Windows\Recent).

Recycle Bin ($Recycle.Bin).

Paso 3: Adquisición de Registros y Artefactos Específicos

Con el sistema apagado o mediante acceso de solo lectura a la imagen de disco, se extraen los artefactos persistentes críticos de Windows 11.

Figura 10 Extracción de datos con FTK Imager 3.1.1.8.



Lista mínima de archivos a extraer:

Tabla 8 Lista mínima de extracción de artefactos

Artefacto	Ruta origen en Windows 11	Herramienta de extracción
SOFTWARE	C:\Windows\System32\config\SOFTWARE	FTK Imager 3.1.1.8
SYSTEM	C:\Windows\System32\config\SYSTEM	FTK Imager 3.1.1.8
SECURITY	C:\Windows\System32\config\SECURITY	FTK Imager 3.1.1.8
SAM	C:\Windows\System32\config\SAM	FTK Imager 3.1.1.8
NTUSER.DAT	C:\Users\<Usuario>\NTUSER.DAT	FTK Imager 3.1.1.8
AmCache.hve	C:\Windows\appcompat\Programs\AmCache.hve	FTK Imager 3.1.1.8
Prefetch	C:\Windows\Prefetch*.pf	FTK Imager 3.1.1.8
Logs EVTX	C:\Windows\System32\winevt\Logs*.evtx	FTK Imager 3.1.1.8
SRUM	C:\Windows\System32\sru\SRUDB.dat	FTK Imager 3.1.1.8
Actividad (Timeline)	C:\Users\<Usuario>\AppData\Local\ConnectedDevicesPlatform*\ActivitiesCache.db	FTK Imager 3.1.1.8
LNK / JumpLists	%AppData%\Microsoft\Windows\Recent*.lnk y subcarpetas AutomaticDestinations	FTK Imager 3.1.1.8

Control de Calidad: Todos los archivos extraídos deben ser verificados mediante hash SHA-256 y almacenados en una estructura de carpetas que replique su ruta original, facilitando el parseo posterior.

Cadena de Custodia y Bitácora de Recolección

Se establece una bitácora de laboratorio obligatoria que registre:

Fecha y hora UTC de cada acción.

Herramienta utilizada (versión incluida).

Hash SHA-256 de cada evidencia adquirida.

Identificador del analista.

Desviaciones o incidencias (ej.: "El servicio de Prefetch estaba deshabilitado; se habilitó previamente al escenario según configuración de la metodología").

Fase 2: Parseo y Normalización de Artefactos

Esta fase transforma los datos brutos adquiridos en información estructurada, extrayendo timestamps y metadatos relevantes de cada fuente de evidencia.

Parseo de Datos Volátiles (RAM)

Herramienta: Volatility 3 (Python 3.10+).

Figura 11 Extracción de procesos de memoria con Volatility.

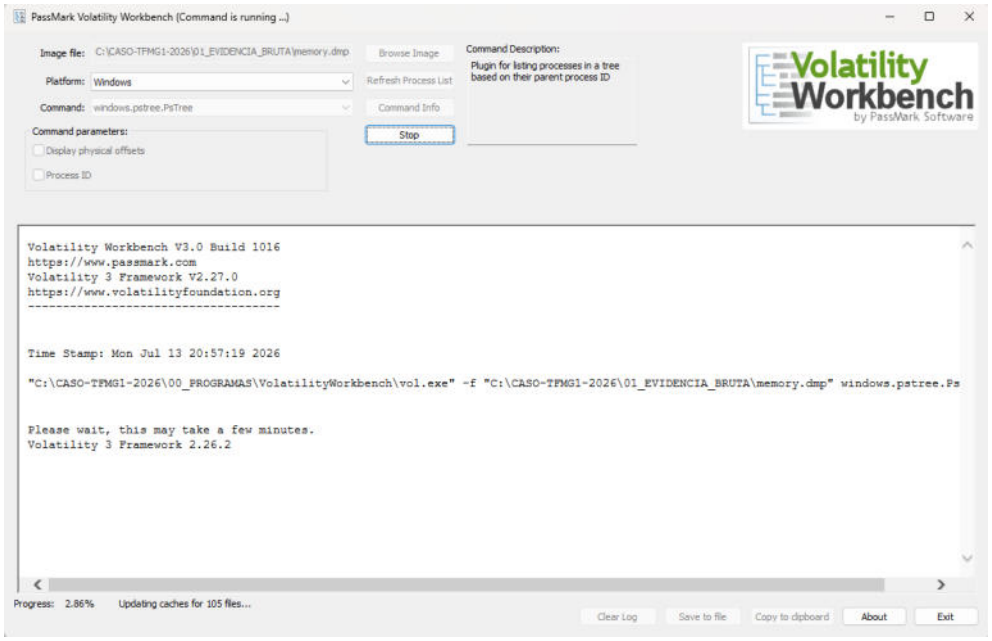


Tabla 9 Plugins y comandos modelo

Información requerida	Comando Volatility 3
Lista de procesos	python3 vol.py -f volcado_memoria.raw windows.pstree.PsTree
Conexiones de red activas	python3 vol.py -f volcado_memoria.raw windows.netscan.NetScan
Comandos de consola recientes	python3 vol.py -f volcado_memoria.raw windows.cmdline.CmdLine
DLLs cargadas por proceso	python3 vol.py -f volcado_memoria.raw windows.dlllist.DllList
Módulos del kernel	python3 vol.py -f volcado_memoria.raw windows.modules.Modules
Registro en memoria (hives)	python3 vol.py -f volcado_memoria.raw windows.registry.hivelist.HiveList

Salida Esperada: Archivos de texto o JSON con los datos extraídos, almacenados en la carpeta C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS

Parseo del Sistema de Archivos y Metadatos

Herramientas: Plaso/log2timeline (para inferencia temporal global del disco), MFTExplorer y FTK Imager (para inspección manual de metadatos $MFT).

Comando modelo de Plaso para parseo directo de una imagen de disco:

log2timeline.py --storage_file /mnt/c/CASO-TFMG1-2026/01_EVIDENCIA_BRUTA/ARTEFACTOS/w11supertimeline.plaso /mnt/c/CASO-TFMG1-2026/01_EVIDENCIA_BRUTA/ARTEFACTOS

log2timeline.py plaso.dump /ruta/de/evidencias/

Artefactos LNK: Utilizar LECmd (Zimmerman Tools):

C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.4\LECmd.exe -d C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\Recent --csv C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS

Parseo del Registro de Windows

Herramientas: RegRipper (versión con plugins actualizados), Registry Explorer (Zimmerman).

Tabla 10 Plugins de RegRipper relevantes

Clave/Artefacto	Plugin de RegRipper
UserAssist	Userassist
RecentDocs	Recentdocs
Run / RunOnce	run / runmru
Mstsc history (RDP)	Mstsc
ShimCache (AppCompatCache)	Shimcache
USB devices	Usbstor

AmCache.hve y ShimCache: Usar AmcacheParser.exe y AppCompatCacheParser.exe:

C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.4\AmcacheParser.exe -f C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\Programs\AmCache.hve --csv C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO

C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.4\AppCompatCacheParser.exe -f C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\SYSTEM --csv C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO

Parseo de artefactos específicos de Windows 11

Prefetch/SysMain: Utilizar PECmd (Zimmerman Tools):

C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.4\PECmd.exe -d C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\Prefetch --csv C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO

SRUM (SRUDB.dat): Extraer mediante RegRipper (plugin srum) o parsear con SRUMDump:

C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.9\SrumECmd\SrumECmd.exe -f C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\sru\SRUDB.dat -r C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\config\SOFTWARE --csv C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO

Logs EVTX: Utilizar EvtxECmd (Zimmerman Tools):

C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.9\EvtxECmd\EvtxECmd.exe -d C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\LOGS --csv C:\CASO-TFMG1-202601_EVIDENCIA_BRUTA\PARSEO\evtx_parsed.csv

Activity History / Timeline: Plaso ya incorpora parsers para ActivitiesCache.db; no obstante, si se requiere inspección manual, puede usarse un visor SQLite sobre la base de datos extraída.

Normalización de timestamps a UTC

Toda evidencia parseada debe llevarse a un formato temporal unificado:

Formato obligatorio: YYYY-MM-DD HH:MM:SS.sss UTC.

Conversión: Las herramientas Zimmerman y Plaso exportan las marcas temporales en formato UTC. Para garantizar una correcta interpretación de los eventos, se verificará previamente la zona horaria configurada en el sistema Windows 11 analizado mediante la revisión de los parámetros de configuración del sistema operativo y de los artefactos del Registro asociados a la información temporal (Time Zone Information). Posteriormente, durante la fase de análisis y correlación, las marcas de tiempo

podrán convertirse a la hora local correspondiente para facilitar la reconstrucción cronológica de la actividad del usuario, manteniendo siempre el valor UTC como referencia forense principal.

Campo obligatorio en cada registro parseado: Source_Artifact, Event_Type, Timestamp_UTC, Description, Source_File_Path.

Fase 3: Fusión Temporal (Super Timeline)

Esta fase integra los miles de eventos individuales parseados en una única secuencia cronológica, permitiendo observar la interrelación temporal entre artefactos heterogéneos.

Generación de la Super Timeline con Plaso

Se seleccionó Plaso en lugar de herramientas individuales, ya que incluye una capa de abstracción y normalización temporal, donde se resuelve de raíz el problema de la heterogeneidad de los formatos de tiempo (timestamps), traduciendo de forma nativa, estructuras binarias tan diversas como el formato FILETIME del Registro o los metadatos ocultos de los accesos rápidos, a un único estándar temporal unificado en UTC. En consecuencia, pasamos de inspeccionar piezas sueltas de un rompecabezas a auditar un flujo continuo, reproducible y verificable de evidencias, cumpliendo con los estándares de integridad (Carrier, 2005).

Herramienta: Plaso (psort.py para exportación final).

Comando modelo:

psort.py -o l2tcsv -w /mnt/c/CASO-TFMG1-2026/01_EVIDENCIA_BRUTA/ARTEFACTOS/W11supertimeline.csv /mnt/c/CASO-TFMG1-2026/01_EVIDENCIA_BRUTA/ARTEFACTOS/w11supertimeline.plaso

Formato de salida: l2tcsv (CSV de log2timeline) con columnas: datetime, timestamp_desc, source, source_long, message, parser, display_name, tag.

Filtrado de Ruido y Eventos Legítimos del Sistema

La super timeline cruda de un sistema Windows 11 contiene miles de eventos generados por actualizaciones del sistema, servicios de mantenimiento (Sheduled Diagnostics, Superfetch/SysMain), y actividades del propio usuario legítimo.

Criterios de filtrado aplicados:

Tabla 11 Criterios de filtrado aplicados

Criterio	Acción
Excluir eventos del proceso svchost.exe sin contexto sospechoso.	Reduce ruido de servicios del sistema.
Excluir eventos de Windows Update (wuauclt, usoclient) en horarios de mantenimiento conocidos.	Limpia ventanas de actividad automática.
Incluir solo eventos en la ventana temporal del escenario (ej. entre T+0 y T+4 horas de la infección).	Enfoca el análisis en la actividad relevante.
Excluir lecturas de Prefetch de procesos del sistema que no forman parte del escenario.	Aísla las ejecuciones maliciosas.

Herramienta de Filtrado: Timeline Explorer (Zimmerman) o hojas de cálculo (Excel/LibreOffice Calc) con filtros dinámicos.

Validación de la Consistencia Temporal

Antes de pasar a la correlación, se verifica que no existan inconsistencias en la línea temporal:

Saltos temporales imposibles (ej. un evento de disco anterior al evento de ejecución que lo generó).

Timestamps futuros o con año 1601 (epoch FILETIME mal parseado).

Zonas horarias mixtas no convertidas. Esta validación permite garantizar la coherencia cronológica de los eventos analizados y contribuye al cumplimiento de los criterios de aceptación definidos para la investigación, ya que reduce el riesgo de correlaciones erróneas y aumenta la confiabilidad de la reconstrucción de la actividad del usuario a partir de los artefactos.

Fase 4: Correlación Cruzada y Triangulación

Esta es la fase distintiva de la metodología. Su objetivo no es simplemente "ver" los eventos ordenados, sino confirmar o descartar acciones maliciosas mediante la intersección de fuentes independientes.

Definición de Eventos de Interés (IoCs) del Escenario

Del escenario de compromiso planteado en el Capítulo 1, se definen los siguientes eventos de interés a confirmar:

Tabla 12 Eventos de interés a confirmar

ID de Evento	Descripción	Fase del escenario
EV-01	Apertura y ejecución de macros del documento malicioso (maldoc.docm).	Ejecución inicial
EV-02	Registro de persistencia en HKLM\...\Run o creación de tarea programada.	Persistencia
EV-03	Ejecución de net.exe para reconocimiento de red o usuarios.	Movimiento lateral simulado
EV-04	Ejecución de bitsadmin.exe para transferencia de datos o tareas en segundo plano.	Movimiento lateral simulado
EV-05	Borrado selectivo de archivos .evtx del Visor de Eventos.	Anti-forensia
EV-06	Eliminación de archivos .pf de la carpeta Prefetch.	Anti-forensia

Matriz de Correlación Artefacto-fuente

Para cada evento de interés, se construye una matriz de correlación que cruza el evento con las fuentes de evidencia donde puede manifestarse. La regla de triangulación establece que un evento se considera CONFIRMADO solo si aparece en tres o más celdas de la matriz con coherencia temporal.

Modelo de matriz para EV-01 (Ejecución del documento malicioso):

Tabla 13 Modelo para ejecución de documento malicioso

Fuente de evidencia	¿Soporta EV-01?	Registro esperado
RAM (Volatility)	Sí	Proceso WINWORD.EXE con handle al archivo maldoc.docm; posible hijo Wscript o PowerShell si la macro despliega payload.
Prefetch	Sí	Archivo WINWORD.EXE-<hash>.pf con timestamp de ejecución.
Registry (UserAssist)	Sí	Entrada {...}\CEBFF...} (rot13 de WINWORD.EXE) con timestamp de última ejecución.
LNK / Recent	Sí	Acceso directo a maldoc.docm en %Recent%.
SRUM	Sí	Registro de usuario y tiempo de actividad para WINWORD.EXE.
EVTX Security	Posible	Evento de creación de proceso (ID 4688)

Para cada evento de interés se construye una matriz de correlación que relaciona el evento analizado con las diferentes fuentes de evidencia disponibles. La Tabla 10 presenta un modelo de matriz utilizando el evento EV-01 como ejemplo ilustrativo, con el propósito de mostrar la estructura de correlación, las fuentes consideradas y la regla de decisión empleada.

Las matrices completas correspondientes a los eventos EV-01 a EV-06 serán desarrolladas y analizadas en detalle en el Capítulo 5, donde se aplicará esta metodología sobre los datos obtenidos durante la fase experimental.

Clasificación de Resultados de Correlación:

Con el fin de garantizar una interpretación consistente de los hallazgos, cada evento analizado será clasificado en una de las siguientes categorías:

1. Confirmado: el evento se encuentra respaldado por múltiples fuentes de evidencia independientes con coherencia temporal y semántica.
2. Sospechoso: el evento presenta evidencia parcial o inconsistencias menores que impiden su confirmación inmediata, requiriendo validación adicional por parte del analista.

3. No soportado: el evento únicamente aparece en una fuente aislada o carece de evidencia suficiente para sustentar su ocurrencia.

4. Anti-forensic Gap: el escenario experimental sugiere que el evento debió generar rastros forenses, pero estos no están presentes debido a posibles técnicas de eliminación, alteración de evidencias o limitaciones de adquisición.

Estas categorías constituyen la base para la toma de decisiones durante la fase de correlación y reconstrucción de actividad.

Regla de decisión aplicada:

1. Si EV-01 se detecta en Prefetch + Registry UserAssist + LNK Recent → CONFIRMADO.
2. Si detecta UserAssist + LNK pero con desfase temporal → SOSPECHOSO
3. Solo UserAssist (un solo artefacto) → NO SOPORTADO / REQUIERE
4. Ningún artefacto esperado aparece pese a que el evento fue ejecutado → ANTI-FORENSIC GAP

Investigación Complementaria.

Reglas de Decisión para Confirmar, Descartar o Clasificar Como Sospechoso

Tabla 14 Reglas de decisión para eventos

Condición	Acción del analista	Código de resultado
Evento presente en >= 3 fuentes con coherencia temporal y semántica.	Confirmar como acción efectivamente ocurrida.	CONFIRMADO
Evento presente en 2 fuentes con cierta coherencia, pero con inconsistencia temporal mayor a 60 segundos entre artefactos.	Clasificar como sospechoso; requiere revisión manual de desfases de reloj o buffering de escritura.	SOSPECHOSO

Evento presente en 1 fuente única, sin respaldo en otras capas.	Descartar como conclusión firme; anotar como indicador aislado de baja confiabilidad.	NO SOPORTADO
Evento ausente en todas las fuentes, pero el escenario indica que debería haber ocurrido.	Investigar posible anti-forensia exitosa o fallo en la recolección.	ANTI-FORENSIC GAP

Detección de anti-forensia Mediante Análisis de Vacíos y Fuentes Residuales

Un aporte distintivo de esta metodología es la capacidad de detectar intentos de borrado no solo por lo que se encuentra, sino por lo que falta y que debería estar.

Técnica de detección de vacíos (gap analysis):

1. Análisis de Prefetch: Si en la ventana temporal del escenario faltan archivos .pf para procesos clave (cmd.exe, powershell.exe, winword.exe) pero existen en RAM o en el $UsnJrnl como eliminados, se infiere borrado selectivo.

2. Análisis EVTX: Identificar saltos en el Sequence Number de logs Security.evtx o la ausencia de logs .evtx en el directorio cuando el servicio Windows Event Log estaba activo.

3. Fuente de respaldo: Consultar el $UsnJrnl para detectar registros de eliminación (FILE_DELETE) de archivos .pf o .evtx, lo cual respaldaría la hipótesis de anti-forensia (HO-2).

Antes de clasificar una ausencia de evidencia como posible anti-forensia, se verificará que dicha ausencia no pueda explicarse por limitaciones de adquisición, fallos de las herramientas de análisis, configuraciones legítimas del sistema operativo o mecanismos normales de mantenimiento del sistema. Solo cuando existan evidencias indirectas que indiquen la existencia previa del artefacto (por ejemplo, referencias en memoria, registros de eliminación en $UsnJrnl o inconsistencias entre múltiples fuentes) se considerará la hipótesis de borrado deliberado o manipulación de evidencias.

Por tanto, la clasificación de un hallazgo como "gap anti-forensia" requerirá evidencia complementaria que permita descartar explicaciones alternativas y sustentar razonablemente la hipótesis de alteración o eliminación intencional de rastros digitales.

Tabla 15 Ejemplo de triangulación anti-forensia

Indicador	Fuente 1	Fuente 2	Fuente 3	Conclusión
Borrado de Prefetch	$UsnJrnl: evento DELETE sobre CMD.EXE-XXXX.pf	AmCache.hve: ejecución previa de cmd.exe registrada, pero sin Prefetch actual	RAM: proceso cmd.exe activo durante el escenario, pero sin archivo .pf asociado en disco	Confirmado borrado selectivo de Prefetch

Protocolo de Validación y Criterios de Éxito

La metodología se considera validada si el experimento de laboratorio cumple los criterios de aceptación (CA-01 a CA-07) definidos en el Capítulo 1. El siguiente cuadro vincula cada fase de la metodología con los criterios que demuestra:

Tabla 16 Protocolo de validación y criterios de éxito

Fase del método	Criterio de aceptación demostrado	Evidencia de cumplimiento
Fase 1 (Recolección)	CA-04 (Replicabilidad con herramientas abiertas)	Uso documentado de vmss2core.exe, FTK Imager
Fase 1 (Cadena de custodia)	CA-05 (Generación de salida auditable)	Bitácora con hashes SHA-256 y timestamps UTC.
Fase 2 (Parseo)	CA-04	Scripts y comandos ejecutados con Volatility 3, Zimmerman Tools y Plaso.
Fase 3 (Fusión)	CA-01 (Reconstrucción completa)	Super timeline CSV generada con eventos de las 4 fases.
Fase 4 (Correlación)	CA-02 (Triangulación >=3 fuentes)	Matriz de correlación con celdas CONFIRMADO por evento.

Fase 4 (Correlación)	CA-03 (Diferenciación malicioso/legítimo)	Tabla de reglas de decisión aplicada a procesos LOLBins.
Fase 4 (Anti-forensia)	CA-06 (Resiliencia ante borrado)	Detección de vacíos mediante $UsnJrnl y fuentes residuales.
Todas las fases	CA-07 (Documentación del procedimiento)	Manual paso a paso que permite replicación por terceros.

Consideraciones Éticas y de Seguridad del Experimento

Dado que el escenario de laboratorio involucra la simulación de malware (macros maliciosas) y técnicas de post-explotación, se establecen las siguientes salvaguardas:

1. Aislamiento absoluto: La máquina virtual Windows 11 operará sin conectividad de red modo Host-Only desactivado, evitando cualquier propagación accidental.

2. Uso de malware documentado o inerte: El payload de la macro puede ser un script benigno (ej. creación de un archivo texto) que simule comportamiento malicioso sin causar daño real, o un malware controlado de repositorios académicos (ej. TheZoo).

3. Propósito exclusivo de investigación: La naturaleza de la experimentación es formativa y científica; no se ejecutará en sistemas ajenos ni se almacenará información de terceros.

4. Destrucción segura post-experimento: Los volcados de memoria, las imágenes de disco y las evidencias digitales generadas serán conservadas únicamente durante el periodo de evaluación del TFM, con acceso restringido al autor y al tribunal evaluador, para ser destruidas o anonimizadas posteriormente conforme a la política de datos de la institución.

Conclusiones del Capítulo

El marco metodológico propuesto constituye un proceso de cuatro fases diseñado para superar el análisis fragmentado de artefactos forenses en Windows 11. Su estructura (recolección, parseo, fusión

temporal y correlación cruzada con triangulación) garantiza que ningún evento del escenario post-explotación sea inferido desde una única fuente de evidencia.

La metodología se apoya en herramientas forenses de código abierto y freeware de adopción en la comunidad DFIR consolidada (Volatility 3, Plaso, Zimmerman Tools, Autopsy), asegurando replicabilidad y transparencia.

La regla de triangulación (≥3 fuentes independientes), complementada con el análisis de vacíos para la detección de anti-forensia, transforma la super timeline de un mero inventario cronológico en un instrumento de confirmación epistemológica.

En el siguiente capítulo se describe la materialización práctica de este marco: la arquitectura del entorno de laboratorio, la ejecución documentada del escenario de compromiso y la aplicación operativa de cada una de las cuatro fases aquí diseñadas.

Capítulo 4

Diseño del Experimento y Escenario de Laboratorio

Arquitectura del Entorno de Laboratorio

El experimento se desarrolla sobre un entorno de laboratorio virtualizado completamente aislado, compuesto por un único nodo objetivo que alberga el sistema operativo Windows 11. La arquitectura se fundamenta en el principio de contención, garantizando que cualquier código ejecutado durante el escenario de compromiso quede confinado dentro de los límites de la máquina virtual, sin riesgo de propagación hacia sistemas externos ni hacia el hipervisor anfitrión.

Topología de Red

La máquina virtual se configura con el adaptador de red en modo desconectado o sin conexión de cable (* cable disconnected*). No se utiliza modo Bridged, NAT ni Host-Only, con el fin de eliminar cualquier vector de escape de red. Esta decisión responde a tres requerimientos:

1. **Seguridad**: Impide que el payload o las herramientas empleadas durante el escenario intenten comunicaciones salientes.

2. **Integridad forense**: Preserva inalterados los registros de red de la VM, ya que no existen ruidos de tráfico externo (actualizaciones, telemetría de Microsoft, servicios en segundo plano) que puedan confundirse con artefactos del escenario.

3. **Control temporal**: Facilita que los timestamps de los eventos generados correspondan exclusivamente a las acciones planificadas del experimento.

Cabe indicar que el aislamiento de red no limita la generación de evidencia de BITS, ya que optamos por una redirección local. Debido al propio diseño del protocolo TCP/IP en entornos Windows, al forzar la petición hacia la dirección 127.0.0.1, el tráfico de red se procesa enteramente dentro de la pila interna del sistema operativo. Esto significa que la interfaz virtual de loopback captura el intento de

conexión. Aunque no contemos con un servidor real escuchando para entregar el archivo, el sistema operativo se ve obligado a procesar la petición de BITS, registrando la actividad en disco y generando de forma síncrona los artefactos de ejecución.

El hipervisor anfitrión funge como plataforma de orquestación y, posteriormente, como estación de análisis forense donde se procesarán las imágenes de disco y los volcados de memoria. Para ello, se habilita en el anfitrión una carpeta compartida de solo lectura o un punto de montaje exclusivo para transferir los artefactos adquiridos hacia la estación de análisis, operación que se realiza con la VM objetivo apagada.

Especificaciones Técnicas de la Infraestructura Virtualizada

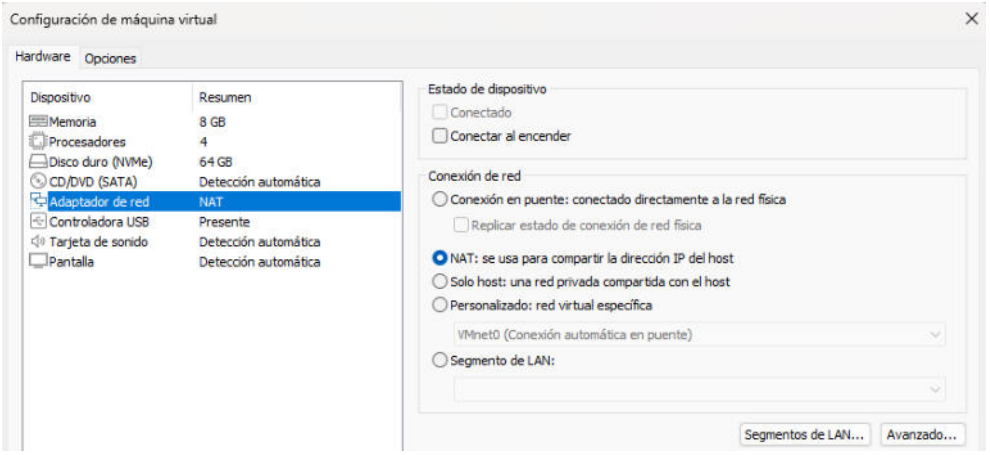
A continuación, se detallan los parámetros mínimos y recomendados para la replicación del entorno. Estos valores fueron establecidos en el alcance del trabajo y se concretan aquí como especificaciones técnicas de diseño.

Tabla 17 Especificaciones técnicas de la infraestructura virtualizada

Componente	Especificación mínima	Justificación
Hipervisor	VirtualBox 7.0.x o VMware Workstation Pro 17.x (Se ocupó la versión 26H1 para el laboratorio)	Compatibilidad con TPM 2.0 virtual (requisito de Windows 11) y snapshots diferenciales.
Sistema anfitrión	CPU x86-64 con virtualización VT-x/AMD-V activada, 16 GB RAM, 250 GB SSD	Soporte de la carga de la VM y análisis concurrente.
CPU (VM objetivo)	4 núcleos virtuales (2 sockets x 2 cores), aceleración de hardware habilitada.	Necesario para ejecutar SysMain/Prefetch y procesar macros sin degradación perceptible.
RAM (VM objetivo)	8192 MB (8 GB) asignados, I/O de memoria habilitado.	Permite albergar procesos de Office, LOLBins y volcado completo sin swap excesivo.
Disco virtual	Un único controlador NVMe virtual de 64 GB	Espacio suficiente para SO, Office, generación de

	(VMDK/VHD dinámico, asignación fija preferente).	Prefetch, logs y archivo de paginación.
Controlador de gráficos	VMSVGA (VirtualBox) o SVGA 3D (VMware) compatible con Windows 11.	Garantiza la experiencia de escritorio para la interacción del usuario simulada.
Firmware	UEFI con Secure Boot habilitado y TPM 2.0 virtual activado.	Requisito de instalación de Windows 11; su estado se documenta para coherencia forense.
Adaptador de red	Desconectado / No cableado.	Aislamiento absoluto del entorno.
Unidades Ópticas/USB	Deshabilitadas en la VM tras la instalación; únicamente se habilitan transitoriamente para la inyección del documento malicioso controlado.	Cierre de vectores de entrada no controlados.

Figura 12 Especificaciones de la configuración de la máquina virtual.



Configuración Base del Sistema Operativo Windows 11

Antes de la ejecución del escenario, la máquina virtual se configura mediante un proceso de set up documentado y fotografiado (capturas de pantalla para anexos), cuyo resultado es un sistema limpio, funcional y forensicamente instrumentado.

Instalación y Parametrización Inicial

Edición mínima del sistema: Windows 11 Pro, versión 23H2 (compilación 22631.x o superior), arquitectura x64.

Cuenta de usuario: Se crea una cuenta local con privilegios de Administrador, denominada Investigador01 (nombre genérico para la bitácora). Esta cuenta es la que ejecutará el escenario.

Configuración regional: Zona horaria UTC+00:00 (Hora universal coordinada), para eliminar ambigüedades de conversión temporal en la super timeline.

Esquema de energía: Alto rendimiento, con suspensión automática deshabilitada. Esto evita que el sistema entre en reposo durante la ejecución de las fases del escenario, lo cual podría truncar procesos o alterar timestamps de Prefetch.

Servicios y Funcionalidades Activadas/Deshabilitadas Intencionalmente

La recolección de evidencia depende de que determinados subsistemas estén operativos. Se configuran las siguientes características:

Tabla 18 Servicios y funcionalidades aplicadas

Característica	Estado	Justificación forense
SysMain (anteriormente Superfetch)	Activo y en inicio automático.	Generación de archivos .pf en C:\Windows\Prefetch; pilar del análisis de ejecución.
Windows Event Log Service	Activo y en inicio automático.	Registro de eventos .evtx de seguridad, sistema y tareas.
Historial de actividad / Timeline	Habilitado (Configuración > Privacidad > Historial de actividad).	Generación de la base de datos ActivitiesCache.db para correlación.
Telemetría SRUM	Activa por defecto (sin deshabilitar el servicio diagtrack).	Población de SRUDB.dat con métricas de uso por aplicación.
Actualizaciones automáticas (Windows Update)	Pausadas / Deshabilitadas durante el experimento.	Evita ruido de eventos de instalación de parches que contaminarían la timeline.

Microsoft Defender Antivirus	Deshabilitado temporalmente para el escenario (mediante GpEdit → desactivar protección en tiempo real).	Evita que el payload simulado sea interceptado antes de generar los artefactos de ejecución.
BitLocker / Device Encryption	Deshabilitado.	Facilita el acceso forense offline al disco virtual sin gestión de claves de recuperación.

Software de Usuario Instalado

Microsoft Office 2016 Professional Plus (Word, Excel, PowerPoint) para soportar la ejecución del documento .docm.

Diseño del Escenario de Compromiso post-explotación

El escenario consta de cuatro fases secuenciales que simulan, desde la perspectiva del atacante, el ciclo completo de un incidente real: ejecución inicial, persistencia, movimiento lateral y ocultamiento de trazas. Cada fase se ejecuta manualmente por el experimentador (simulando al usuario víctima) y se cronometra con respecto a un Timestamp Cero (T0), definido como el instante de inicio de la Fase 1.

Consideraciones Éticas y de Seguridad

El "payload" ejecutado en la fase inicial no es malware destructivo ni de cifrado. Se trata de una macro VBA que realiza acciones benignas, pero forensicamente relevantes: crea un proceso hijo (cmd.exe o powershell.exe) que a su vez escribe un archivo bandera (flag.txt) en una ruta temporal, simulando el despliegue de una carga útil. Esta decisión garantiza la integridad del laboratorio y evita daños estructurales en la VM.

Fase 1: Ejecución Inicial del Vector de Acceso (T0)

Objetivo: Simular el compromiso inicial mediante ingeniería social (phishing documental).

Procedimiento:

1. En el sistema anfitrión, se prepara un documento Microsoft Word (maldoc_demo.docm) con una macro VBA embebida.

2. La macro contiene el siguiente pseudocódigo acción:

Figura 13 Macro contenida en el documento word actuando como un programa maligno.

```
Sub AutoOpen()
' Simula descarga de payload
        Shell "cmd.exe /c echo Payload_simulado >
        %USERPROFILE%\AppData\Local\Temp\flag_stage1.txt", vbHide
' Ejecución silenciosa
End Sub
```

3. El archivo .docm se transfiere a la VM objetivo mediante unidad USB virtual montada temporalmente.

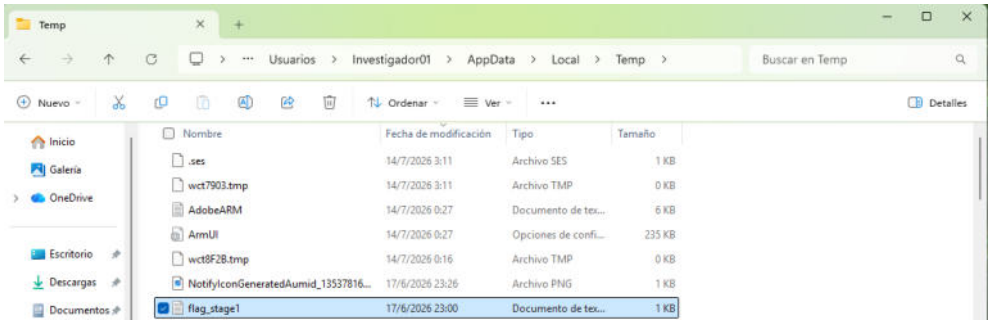
4. **T0**: El usuario Investigador01 abre el archivo maldoc_demo.docm desde su carpeta Descargas y habilita el contenido de macros.

5. El proceso WINWORD.EXE despliega un hijo cmd.exe, generando la escritura del archivo bandera.

Artefactos Esperados Generados:

- Archivo Prefetch para WINWORD.EXE y CMD.EXE.
- Entrada UserAssist en NTUSER.DAT para la ejecución de Winword.
- Acceso directo .lnk a maldoc_demo.docm en %Recent%.
- Posible registro EVTX de creación de proceso (ID 4688 si auditoría habilitada).
- Archivo flag_stage1.txt en directorio temporal.

Figura 14 Verificación del Registro de ejecución de programa maligno.



-

Fase 2: Establecimiento de Persistencia (T0 + 5 minutos)

Objetivo: Garantizar la supervivencia del acceso entre reinicios mediante una clave de inicio automático.

Procedimiento:

1. **T0+5 min**: El experimentador abre regedit.exe con privilegios elevados.

2. Navega hasta HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

3. Crea un nuevo valor de cadena denominado SystemUpdate32, apuntando a la ruta:

C:\Windows\System32\cmd.exe /c calc.exe

(Se utiliza calc.exe como carga simulada persistente, visible e inofensiva, pero legible en el análisis como proceso hijo).

4. Al cerrar el editor de registros, la persistencia queda activa.

Artefactos Esperados Generados:

Modificación en el archivo SOFTWARE del Registro (timestamp de última escritura en la clave ...CurrentVersion\Run).

Prefetch de REGEDIT.EXE.

Posible evento .evtx del sistema ante modificación de clave de Registro (si auditoría avanzada habilitada).

Al reiniciar (si se reinicia), CALC.EXE se ejecutaría automáticamente (en este diseño de laboratorio no se reinicia para mantener la continuidad, pero el rastro de persistencia queda almacenado).

Fase 3: Movimiento Lateral Simulado Mediante Living Off The Land (T0 + 10 minutos)

Objetivo: Simular reconocimiento de red y transferencia encubierta utilizando binarios nativos del sistema (LOLBins), tácticas TA0008 de MITRE ATT&CK.

Sub-fase 3a: Reconocimiento con net.exe

1. **T0+10 min**: Abrir cmd.exe y ejecutar:

net view \\127.0.0.1\

net user

2. Estos comandos son típicos de reconocimiento interno en post-explotación y dejan rastros en Prefetch, en la memoria volátil (si aún residentes) y potencialmente en EVTX.

Sub-fase 3b: **Transferencia encubierta con** bitsadmin.exe

1. **T0+12 min**: Ejecutar:

bitsadmin /transfer myjob /download /priority high http://127.0.0.1/fake.txt %USERPROFILE%\AppData\Local\Temp\bits_recv.txt

(La URL apunta a localhost donde no hay servidor, pero el comando genera el job en la cola BITS y registros asociados.)

2. Alternativamente, para asegurar que el job BITS se materialice en el sistema, puede crearse un servidor web mínimo local (python -m http.server) si el diseño lo permitiera; sin embargo, dado el aislamiento de red, el comando fallará en la transferencia **pero creará el trabajo y los logs del servicio BITS** en Microsoft-Windows-Bits-Client/Operational.

Artefactos Esperados Generados:

Prefetch para NET.EXE y BITSADMIN.EXE.

Claves ShimCache/AmCache para ambos binarios.

Logs .evtx del canal Microsoft-Windows-Bits-Client/Operational.evtx.

Posible conexión de red registrada en RAM (Volatility netscan) si aún residen estructuras de conexión previa a la falla.

Fase 4: Técnicas anti-forensias — Borrado Selectivo de Trazas (T0 + 15 minutos)

Objetivo: Simular el intento del atacante de dificultar la investigación mediante eliminación de archivos críticos.

Sub-fase 4a: Eliminación de logs del Visor de Eventos

1. **T0+15 min**: Abrir PowerShell con privilegios elevados y ejecutar:

Para la versión Windows 11 se debe usar el comando wevtutil ya que los comandos Remove-Item que es otra alternativa de eliminación carecen de privilegios para la eliminación de los artefactos.

wevtutil cl Security

Wevtutil cl System

Sub-fase 4b: Limpieza de la Carpeta Prefetch

1. **T0+16 min**: Ejecutar:

Remove-Item C:\Windows\Prefetch*.pf -Force

Artefactos Esperados Generados (paradoja anti-forensia):

Ausencia de archivos .pf en disco para los procesos ejecutados en Fases 1-3.

Presencia de registros de eliminación en $UsnJrnl.

Presencia de entradas en AmCache.hve que testimonian la ejecución previa de los binarios eliminados.

Posible residuo en RAM: Procesos de PowerShell y CMD recién terminados aún pueden estar en memoria al momento del volcado si este se realiza inmediatamente después.

Eventuales logs .evtx residuales de otros canales no borrados (ej. Setup.evtx, Application.evtx) que pueden contener eventos de creación de proceso anteriores al borrado.

Protocolo de ejecución, Bitácora de Actividades y Cadena de Custodia

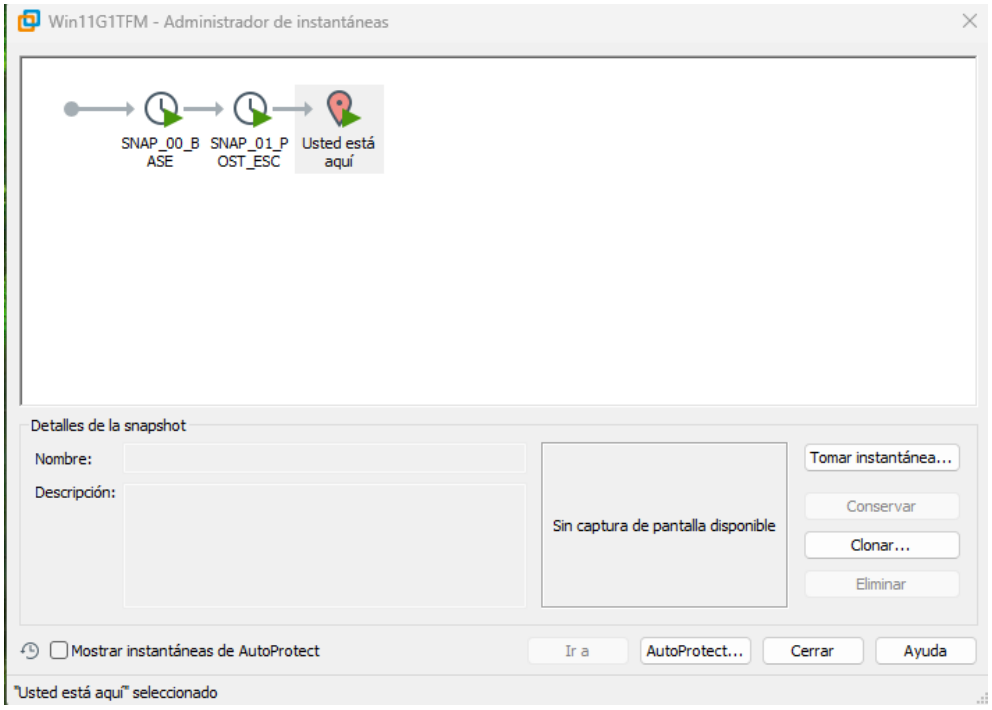
Protocolo de Snapshots

Antes de iniciar cualquier fase del escenario, se crea un snapshot base de la VM (estado limpio post-configuración). Esto permite restaurar la condición inicial en caso de errores o repeticiones.

Tabla 19 Protocolo de snapshots

Snapshot	Descripción	Momento
SNAP_00_BASE	Windows 11 instalado, Office instalado, configuraciones aplicadas, escenario NO ejecutado.	Previo a T0.
SNAP_01_POST_ESC	Estado post-ejecución de las 4 fases del escenario, PRE-volcado forense.	Inmediatamente después de T0+16 min.

Figura 15 Protocolo de Instantánea máquina virtual



Bitácora de Ejecución del Escenario

Se utiliza una plantilla de bitácora cronometrada. A continuación, se presenta el formato que debe completarse durante la prueba:

Tabla 20 Bitácora de ejecución de escenario

Hora UTC	Evento / Acción	Actor	Observaciones
17/06/2026 22:15	Creación de maldoc_demo.docm en anfitrión.	Experimentador	Macro VBA benigna verificada.
17/06/2026 23:00	Uso de memoria usb	Experimentador	Hash SHA-256 del maldoc_demo.docm registrado: d7442fbee6cdc58ba66fdbc8112ddd6748e3aeb49ad521a9a48d4900ff03a5a1
17/06/2026 23:00	T0: Apertura de maldoc_demo.docm y habilitación de macros.	Usuario víctima simulado	Proceso WINWORD.EXE observado activo.

17/06/2026 23:05	T0+5: Creación de clave SystemUpdate32 en Registro.	Usuario Víctima simulado	regedit.exe ejecutado como admin.
17/06/2026 23:10	T0+10: Ejecución de net.exe view y net user.	Usuario víctima simulado	Ventana CMD visible.
17/06/2026 23:12	T0+12: Ejecución de bitsadmin /transfer.	Usuario víctima simulado	Comando fallido por falta de red, pero job creado.
17/06/2026 23:15	T0+15: Borrado de Security.evtx y System.evtx vía PowerShell.	Usuario víctima simulado	Ejecución con privilegios elevados.
17/06/2026 23:16	T0+16: Borrado de carpeta Prefetch (*.pf).	Usuario víctima simulado	Comando completado sin errores visibles.
17/06/2026 2317	Snapshot	Experimentador	Generación del SnapShot SNAP_01_POST_ESC
17/06/2026 23:27	Apagado ordenado de VM	Experimentador	
17/06/2026 23:26	Archivo memoria máquina virtual	Experimentador	Win11G1TFM-Snapshot2.vmem Hash SHA-256: 0f06837c7b2eb951967c507e984bf7716 2c8a9c74ed69299d6218037f9505336
17/06/2026 23:26	Archivo memoria máquina virtual	Experimentador	Win11G1TFM-Snapshot2.vmsn Hash SHA-256: ad84561e9ef634b10a3a4ac72c9e371ad 9b1e198efa6306d03f087ec8cd0604d
18/06/2026 00:07	Generación de volcado de memoria vmss2core.exe).	Experimentador	Memory.dmp Hash SHA-256: 370f7d782e0a668de9b7198e661ad4e37 3d13641cbfff5266e8e6bbebdd38925
17/06/2026 23:53	Generación de imagen forense del disco (FTK Imager).	Experimentador	Windows 11 G1TFM.E01 Hash SHA-256: b6b5797006ec64c309269b1edadcfad3e 80d9983d3b99058bcd69a7cf7fb93a0

Cadena de Custodia Digital

La cadena de custodia se documenta mediante un formulario estándar por cada evidencia generada:

Tabla 21 Formulario Modelo de cadena de custodia

Campo	Valor
ID de evidencia	EVD-RAM-001
Descripción	Volcado de memoria RAM de VM Win11G1TFM post-scenario.
Fecha/Hora de adquisición	2026-06-18 06:07 UTC
Método de adquisición	Volcado físico mediante herramienta propia de vmware vmss2core.exe
Dispositivo origen	VM Win11G1TFM, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	370f7d782e0a668de9b7198e661ad4e373d13641cbfff5266e8e6bbebdd38925
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\memory.dmp
Integridad verificada	Sí / 20260618

Figura 16 Obtención del HASH256 del archivo de memoria

Tabla 22 Formulario de adquisición de la imagen forense

Campo	Valor
ID de evidencia	EVD-DISK-001
Descripción	Imagen forense del disco de VM Win11G1TFM post-scenario.
Fecha/Hora de adquisición	2026-06-17 23:26:00 UTC
Método de adquisición	Volcado físico mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	VM Win11G1TFM, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	b6b5797006ec64c309269b1edadcfad3e80d9983d3b99058bcd69a7cf7fb93a0

Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ Windows11g1tfm.E01
Integridad verificada	Sí / 20260618

Figura 17 Obtención del HASH256 del archivo de la imagen del disco

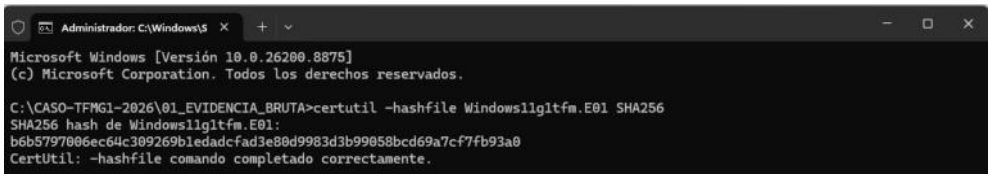


Tabla 23 Formulario de extracción del artefacto SOFTWARE

Campo	Valor
ID de evidencia	EVD-REG-001
Descripción	Windows\System32\config\SOFTWARE
Fecha/Hora de adquisición	2026-06-18 01:30:00 UTC
Método de adquisición	Extracción de imagen de disco EVD-DISK-001 mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	Windows11g1tfm.E01, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	b7b7f8ef5d242d9508d28b110de680fb6500b774b99aefa78e7fe14b42125b76
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\SOFTWARE
Integridad verificada	Sí / 20260618

Figura 18 Obtención del HASH del archivo SOFTWARE

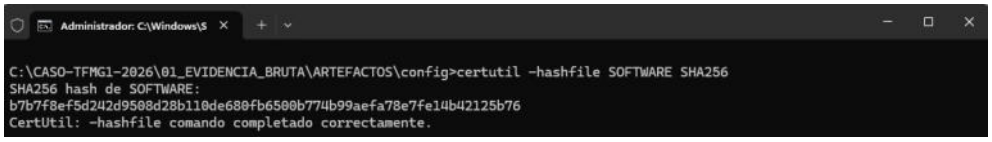


Tabla 24 Formulario de extracción del artefacto SYSTEM

Campo	Valor
ID de evidencia	EVD-REG-002
Descripción	Windows\System32\config\SYSTEM
Fecha/Hora de adquisición	2026-06-18 01:32:00 UTC
Método de adquisición	Extracción de imagen de disco EVD-DISK-001 mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	Windows11g1tfm.E01, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	0904fda7d4cb3e34528e94b683378cd6d3039e6428441e03ffbb750f1bcae1f7
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\SYSTEM
Integridad verificada	Sí / 20260618

Tabla 25 Formulario de extracción del artefacto SECURITY

Campo	Valor
ID de evidencia	EVD-REG-003
Descripción	Windows\System32\config\SECURITY
Fecha/Hora de adquisición	2026-06-18 01:32:00 UTC
Método de adquisición	Extracción de imagen de disco EVD-DISK-001 mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	Windows11g1tfm.E01, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	2e62c23b9c52a2be2117d7081af74cad6513e5a186506f4350fe0ae252699215

Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\SECURITY
Integridad verificada	Sí / 20260618

Tabla 26 Formulario de extracción del artefacto NTUSER.DAT

Campo	Valor
ID de evidencia	EVD-REG-004
Descripción	Users\Investigador01\NTUSER.DAT
Fecha/Hora de adquisición	2026-06-18 01:35:00 UTC
Método de adquisición	Extracción de imagen de disco EVD-DISK-001 mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	Windows11g1tfm.E01, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	9c9a5f1c3c2ba8d7df158cfb5fbd3fd9c5427193baf8630d2110d73c1673f8f2
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\NTUSER.DAT
Integridad verificada	Sí / 20260618

Tabla 27 Formulario de extracción del artefacto AmCache.hve

Campo	Valor
ID de evidencia	EVD-CACHE-001
Descripción	Windows\appcompat\Programs\AmCache.hve
Fecha/Hora de adquisición	2026-06-18 01:38:00 UTC
Método de adquisición	Extracción de imagen de disco EVD-DISK-001 mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	Windows11g1tfm.E01, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)

Hash SHA-256 post-adquisición	d37ec71761f50df140ea52aa9f1ee4a3715c7a56897ef7ec19d5dd62f6e842a6
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\Amcache.hve
Integridad verificada	Sí / 20260618

Tabla 28 Formulario de extracción del artefacto Prefetch

Campo	Valor
ID de evidencia	EVD-PRE-001
Descripción	Windows\Prefetch*.pf
Fecha/Hora de adquisición	2026-06-18 01:40:00 UTC
Método de adquisición	Extracción de imagen de disco EVD-DISK-001 mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	Windows11g1tfm.E01, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	68eb419cd02eb5ce741688eb1f4be71f596f885da1b8921abf8f506dfc178771
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\01_ ARTEFACTOS \PREFETCH.ZIP
Integridad verificada	Sí / 20260618

Tabla 29 Formulario de extracción del artefacto Application.evtx

Campo	Valor
ID de evidencia	EVD-EVT-001
Descripción	Windows\System32\winevt\Logs\Application.evtx
Fecha/Hora de adquisición	2026-06-18 01:42:00 UTC
Método de adquisición	Extracción de imagen de disco EVD-DISK-001 mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	Windows11g1tfm.E01, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].

Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	644dfba3a0bab6f40668dda3ff9d7eba4052bf89cf28c188ad9eebb8647c50bb
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\Application.evtx
Integridad verificada	Sí / 20260618

Tabla 30 Formulario de extracción del artefacto Microsoft-Windows-Bits-Client/Operational.evtx

Campo	Valor
ID de evidencia	EVD-EVT-002
Descripción	Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Operational.evtx
Fecha/Hora de adquisición	2026-06-18 01:43:00 UTC
Método de adquisición	Extracción de imagen de disco EVD-DISK-001 mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	Windows11g1tfm.E01, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	9cee1b1adb6c585ef547edd1bd5484501949c4ddb3d07e142e72a306c80f0558
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\Microsoft-Windows-Bits-Client%4Operational.evtx
Integridad verificada	Sí / 20260618

Tabla 31 Formulario de extracción del artefacto SRUDB.dat

Campo	Valor
ID de evidencia	EVD-SRUM-001
Descripción	Windows\System32\sru\SRUDB.dat
Fecha/Hora de adquisición	2026-06-18 01:45:00 UTC

Método de adquisición	Extracción de imagen de disco EVD-DISK-001 mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	Windows11g1tfm.E01, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	2189b529f55e6a2ca83fdbc8d7e5b2071cf6fda4a39fe0d00df7154fb231971e
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\SRUDB.dat
Integridad verificada	Sí / 20260618

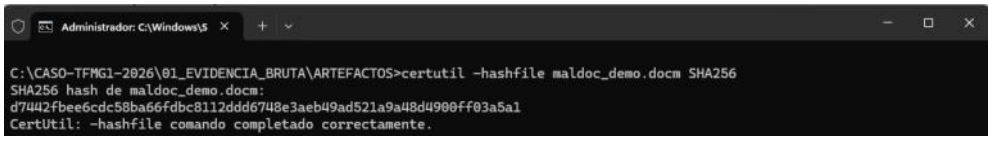
Tabla 32 Formulario de extracción del artefacto ActivitiesCache.db

Campo	Valor
ID de evidencia	EVD-TIME-001
Descripción	Users\Investigador01\AppData\Local\ConnectedDevicesPlatform\...\ActivitiesCache.db
Fecha/Hora de adquisición	2026-06-18 01:47:00 UTC
Método de adquisición	Extracción de imagen de disco EVD-DISK-001 mediante Exterro FTK Imager 3.1.1.8
Dispositivo origen	Windows11g1tfm.E01, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	47da3495d38c500ad586fac8167e45212715101fe0ad320ca9eeec7e552f9a5d
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\ActivitiesCache.db
Integridad verificada	Sí / 20260618

Tabla 33 Evidencia de archivo Word con macro maliciosa

Campo	Valor
ID de evidencia	EVD-MDOC-001
Descripción	Archivo Word maldoc_demo.docm.
Fecha/Hora de adquisición	2026-06-18 01:48:00 UTC
Método de adquisición	Copia
Dispositivo origen	USB, MAC [00:0C:29:DE:66:5E], S/N del disco virtual [UUID].
Hash SHA-256 pre-adquisición	N/A (volátil)
Hash SHA-256 post-adquisición	d7442fbee6cdc58ba66fdbc8112ddd6748e3aeb49ad521a9a48d4900ff03a5a1
Custodio responsable	G1TFM2026
Ubicación de almacenamiento	G:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\maldoc_demo.docm
Integridad verificada	Sí / 20260618

Figura 19 Obtención del HASH 256 del archivo malware



Consideraciones Finales del Diseño Experimental.

El escenario propuesto no busca replicar una Advanced Persistent Threat (APT) de alta sofisticación, sino un **compromiso de nivel medio-alto frecuente en incidentes reales** documentados por ENISA y Verizon DBIR: phishing documental, persistencia clásica, reconocimiento con herramientas nativas y limpieza de trazas rudimentaria. Esta elección es deliberada: un escenario demasiado complejo (rootkits de kernel, exploit de día cero, exfiltración por túneles DNS) escaparía del alcance de un trabajo

de máster y complicaría la atribución de artefactos; un escenario demasiado simple (un solo malware ejecutado sin persistencia) no sería suficiente para validar la fase de correlación cruzada ni la detección de anti-forensia.

La combinatoria de las cuatro fases garantiza que el perfil de artefactos generado sea **heterogéneo, cruzado y parcialmente degradado** (por el borrado intencional), configurando así un campo de prueba óptimo para demostrar que la metodología de correlación supera al análisis aislado, tal como plantean la hipótesis general y las hipótesis operativas del trabajo.

En el siguiente capítulo (**Capítulo 5: Desarrollo y Resultados**) se aplicará el marco metodológico descrito en el Capítulo 3 sobre el entorno y el escenario aquí diseñados, presentando los hallazgos de cada fase de recolección, parseo, fusión y correlación.

Capítulo 5

Desarrollo y Resultados

Aplicación de la Fase 1: Recolección Ordenada de Evidencias

La ejecución del escenario documentado en el Capítulo 4 generó un conjunto de evidencias digitales que fueron adquiridas siguiendo el orden de volatilidad establecido en la metodología.

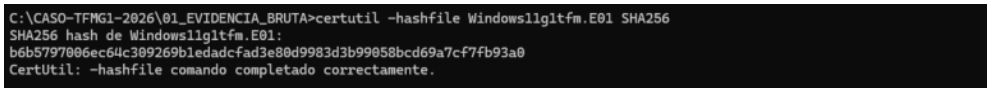
Tabla 34 Evidencias volátiles

Parámetro	Valor registrado en el experimento
Herramienta de adquisición / comando	Utilidad vmware vmss2core.exe “C:\CASO-TFMG1-2026\00_PROGRAMAS\vmss2core.exe” -W64 Win11G1TFM-Snapshot2.vmsn Win11G1TFM-Snapshot2.vmem
Archivo generado	Memory.dmp
Tamaño del volcado	8,589,942,784 bytes (coincidente con la RAM asignada de 8 GB)
Hora UTC de adquisición	18/06/2026 00:07 UTC
Hash SHA-256	370f7d782e0a668de9b7198e661ad4e373d13641cbfff5266e8e6bbebdd38925
Verificación de integridad	Sí

Tabla 35 Imagen forense del disco

Parámetro	Valor registrado
Herramienta de adquisición	FTK Imager 3.1.1.8
Formato de salida	E01
Archivo generado	Windows11g1tfm.E01
Hash SHA-256 pre-adquisición	N/A (adquisición lógica desde hipervisor)
Hash SHA-256 post-adquisición	b6b5797006ec64c309269b1edadcfad3e80d9983d3b99058bcd69a7cf7fb93a0
Espacio utilizado en disco virtual	(29,591,920,640 bytes)

Figura 20 Obtención del hash256 de la imagen del disco



Artefactos Específicos Extraídos

Se extrajeron manualmente desde la imagen de disco los siguientes archivos, conservando su ruta relativa en la estructura de almacenamiento del caso:

Tabla 36 Lista de artefactos extraídos

ID Artefacto	Archivo / Ruta origen	Herramienta de Extracción	Hash SHA-256
ART-REG-01	Windows\System32\config\SOFTWARE	FTK Imager 3.1.1.8	b7b7f8ef5d242d9508d28b110de680fb6500b774b99aefa78e7fe14b42125b76
ART-REG-02	Windows\System32\config\SYSTEM	FTK Imager 3.1.1.8	0904fda7d4cb3e34528e94b683378cd6d3039e6428441e03ffbb750f1bcae1f7
ART-REG-03	Windows\System32\config\SECURITY	FTK Imager 3.1.1.8	2e62c23b9c52a2be2117d7081af74cad6513e5a186506f4350fe0ae252699215
ART-REG-04	Users\Investigador01\NTUSER.DAT	FTK Imager 3.1.1.8	9c9a5f1c3c2ba8d7df158cfb5fbd3fd9c5427193baf8630d2110d73c1673f8f2
ART-CACHE-01	Windows\appcompat\Programs\AmCache.hve	FTK Imager 3.1.1.8	d37ec71761f50df140ea52aa9f1ee4a3715c7a56897ef7ec19d5dd62f6e842a6
ART-PRE-01	Windows\Prefetch*.pf	FTK Imager 3.1.1.8	68eb419cd02eb5ce741688eb1f4be71f596f885da1b8921abf8f506dfc178771
ART-EVT-01	Windows\System32\winevt\Logs\Application.evtx	FTK Imager 3.1.1.8	644dfba3a0bab6f40668dda3ff9d7eba4052bf89cf28c188ad9eebb8647c50bb
ART-EVT-02	Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Operational.evtx	FTK Imager 3.1.1.8	9cee1b1adb6c585ef547edd1bd5484501949c4ddb3d07e142e72a306c80f0558
ART-SRUM-01	Windows\System32\sru\SRUDB.dat	FTK Imager 3.1.1.8	554a0fd037304acead4b0f3728fd54efe32a74f53d9bfd8fd805973b3b8a117f
ART-TIME-01	Users\Investigador01\AppData\Local\ConnectedDevicesPlatform\...\ActivitiesCache.db	FTK Imager 3.1.1.8	47da3495d38c500ad586fac8167e45212715101fe0ad320ca9eeec7e552f9a5d

Figura 21 Obtención del HASH de archivo SOFTWARE

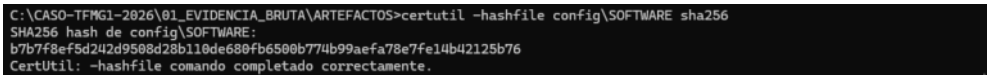


Figura 22 Obtención del HASH de archivo SYSTEM

Figura 23 Obtención del HASH de archivo SECURITY

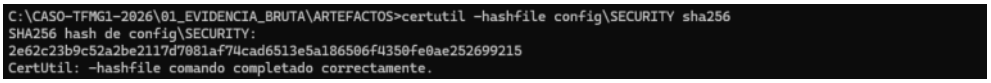


Figura 24 Obtención del HASH de archivo NTUSER.DAT

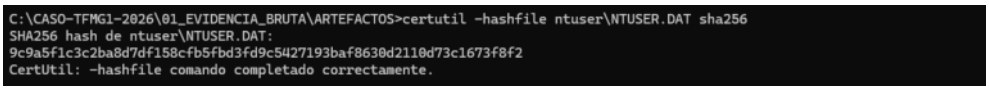


Figura 25 Obtención del HASH de archivo AMCACHE.HVE

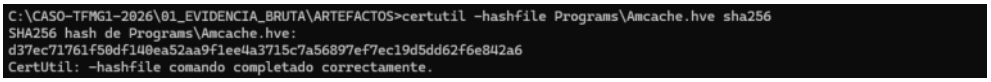


Figura 26 Obtención del HASH de archivo PREFECTH.ZIP

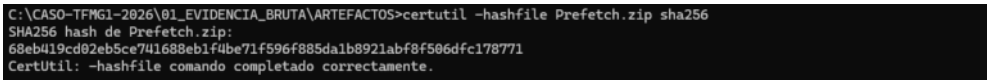


Figura 27 Obtención del HASH de archivo APPLICATION.EVTX

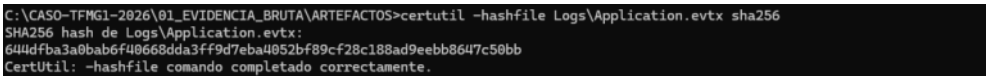


Figura 28 Obtención del HASH de archivo Microsoft-Windows-WMI-Activity%4Operational.evtx

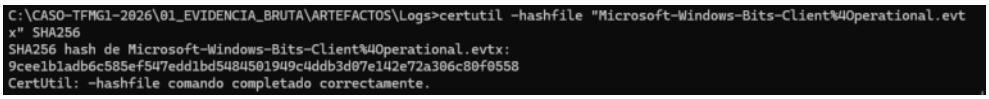
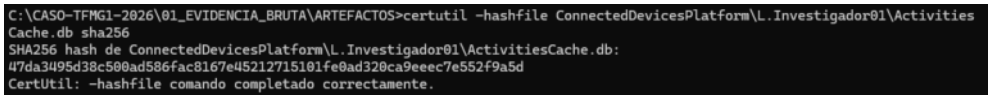


Figura 29 Obtención del HASH de archivo SRUDB.DAT

Figura 30 Obtención del HASH de archivo ACTIVITIESCACHE.DB



Control de calidad: Todos los archivos fueron almacenados en el directorio del caso CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS, con permisos de solo lectura y bitácora de transferencia.

Aplicación de la Fase 2: Parseo y Normalización

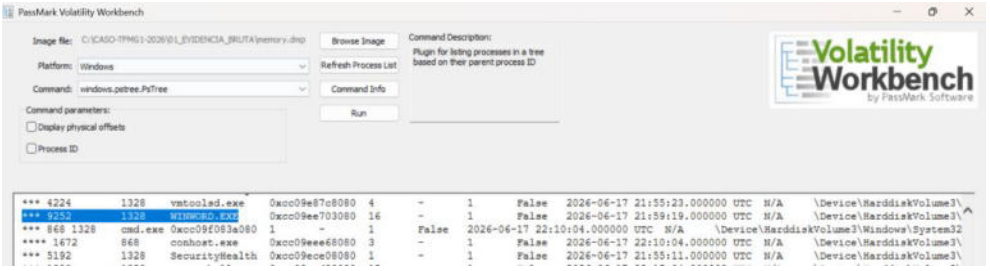
Parseo de Volátiles (RAM)

Se procesó el volcado MEMORY.DMP mediante Volatility 3 Framework 2.27.0. A continuación se resumen los hallazgos estructurados por plugin:

Tabla 37 Hallazgos de parseo de volátiles

Plugin Volatility 3	Resultado relevante esperado	Estado de análisis
windows.pstree.PsTree	Identificación de procesos padre/hijo: WINWORD.EXE →CMD.EXE; 9252 CMD.EXE → powershell.exe (borrado); REGEDIT.EXE (aislado).	 ENCONTRADO ENCONTRADO NO ENCONTRADO
windows.cmdline.CmdLine	Argumentos de línea de comando para net.exe (net view, net user) y bitsadmin.exe 8500	 NO ENCONTRADO ENCONTRADO
windows.netscan.NetScan	Conexiones o intentos de conexión saliente (127.0.0.1:80 de BITS); sockets en estado CLOSE_WAIT o SYN_SENT.	NO ENCONTRADO
windows.handles.Handles	Handles de archivo abiertos por WINWORD.EXE apuntando a ...\maldoc_demo.docm.	NO ENCONTRADO

Figura 31 Evidencia parseo Pstree Winword.



Parseo de Prefetch (PECmd)

Se ejecutó PECmd.exe sobre la carpeta Prefetch extraída. La salida se exportó a prefetch_parsed.csv.

Tabla 38 Hallazgos de parseo de Prefetch

Métrica	Valor
Total archivos .pf encontrados	122
Archivos .pf con timestamp en ventana del escenario (T0 a T0+20 min)	[64]
Ejecutables relevantes detectados	REGEDIT.EXE
Archivos .pf AUSENTES por borrado anti-forense	[WINWORD.EXE, CMD.EXE, NET.EXE, BITSADMIN.EXE, , POWERSHELL.EXE]

Parseo del Registro (RegRipper + Registry Explorer)

Tabla 39 Plugins ejecutados y hallazgos esperados

Plugin / Clave	Hallazgo esperado	Estado
userassist (NTUSER.DAT)	Entrada para WINWORD.EXE con último tiempo de ejecución cercano a T0.	[ENCONTRADO]
run (SOFTWARE)	Valor SystemUpdate32 → C:\Windows\System32\cmd.exe /c calc.exe; timestamp de modificación de la clave Run.	[ENCONTRADO]
shimcache (SYSTEM)	Entradas para WINWORD.EXE, NET.EXE, BITSADMIN.EXE, REGEDIT.EXE.	[Completar]
usbstore	Posible entrada si se usó USB virtual para inyectar el .docm.	[ENCONTRADO]

Long Description

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run] Entries: ['SecurityHealth: %windir%\\system32\\SecurityHealthSystray.exe' 'SystemUpdate32: C:\\Windows\\System32\\cmd.exe /c calc.exe' 'VMware User Process: "C:\\Program Files\\VMware\\VMware Tools\\vmtoolsd.exe" -n vmusr']

File Name

OS:/mnt/c/CASO-TFMG1-2026/01_EVIDENCIA_BRUTA/ARTEFACTOS/config/SOFTWARE

Nota: Si el Prefetch fue borrado en la Fase 4, el ShimCache y AmCache sirven como fuentes residuales de ejecución.

Parseo de logs EVTX (EvtxECmd)

Tabla 40 Parseo de Logs EVTX

Canal EVTX	Eventos relevantes esperados	Estado
Security.evtx (si no fue borrado en el lab; si fue borrado, indicar ausencia)	ID 4688 (creación de proceso): WINWORD.EXE, CMD.EXE, NET.EXE, REGEDIT.EXE.	AUSENTE POR ANTI-FORENSIA
System.evtx (si no fue borrado)	ID 7045 (servicio creado) si se usó persistencia por servicio; eventos de inicio de tareas.	AUSENTE POR ANTI-FORENSIA
Microsoft-Windows-Bits-Client%4Operational.evtx	Eventos de creación de trabajo BITS (JobCreated, JobTransferred).	ENCONTRADO
Microsoft-Windows-PowerShell%4Operational.evtx	Eventos de ejecución de comandos de eliminación (Remove-Item).	AUSENTE POR ANTI-FORENSIA

Parseo de SRUM (SRUMDump / RegRipper)

Tabla 41 Parseo de SRUM

Métrica	Valor
Aplicación con mayor uso de CPU en ventana del escenario	[WINWORD.EXE]
Usuario asociado a la ejecución de NET.EXE / BITSADMIN.EXE	Investigador01 (SID)
Ventana temporal de actividad registrada en SRUM	[17/06/2026 22.27]

Aplicación de la Fase 3: Fusión Temporal (Super Timeline)

Se generó la super timeline integrada mediante el pipeline de Plaso.

Tabla 42 Comandos super timeline

Parámetro	Valor
Comando ejecutado	log2timeline.py --storage-file ./ARTEFACTOS/w11timeline.plaso --parsers "win7" --status_view window ./ARTEFACTOS/
Tiempo de procesamiento	[00:02:50]
Eventos totales extraídos	[358.992]
Ventana filtrada (T0 - T0+30 min)	[102.407]
Exportación final	W11timeline.csv (formato l2tcsv)

Decidimos mapear los artefactos bajo el preajuste win7, apoyándonos en las observaciones de Carvey (2016) sobre sus análisis de la evolución del núcleo de Microsoft, donde explica que las estructuras lógicas de almacenamiento secundario no se rediseñan desde cero en cada lanzamiento comercial. Esto es así porque la estructura del núcleo de los artefactos forenses de Windows 11 (la forma binaria en la que se estructuran las colmenas del Registro, los archivos de prelectura .pf, los accesos directos .lnk y el motor de la base de datos de AmCache) comparte la misma herencia y lógica de parsing que se consolidó a partir de Windows 7 y si se coloca win11, se presenta un error.

Filtrado Aplicado:

Exclusión de eventos generados por svchost.exe en ausencia de contexto de ejecución de usuario.

Exclusión de eventos de mantenimiento (TiWorker.exe, TrustedInstaller.exe).

Exclusión de lecturas de Prefetch de procesos del sistema arrancados en el boot previo a T0.

Aplicación de la Fase 4: Correlación Cruzada y Triangulación

A continuación, se presenta el núcleo del análisis: la aplicación de la regla de triangulación (≥3 fuentes) para cada evento de interés definido en la metodología.

Análisis Correlacional de EV-01: Ejecución Inicial (maldoc_demo.docm)

Evento: Apertura del documento Word malicioso y despliegue de macro.

Tabla 43 Despliegue de macro a través de word

ID Fuente	Artefacto / Evidencia	Descripción del hallazgo	Estado
FUENTE-1	Volatility3: Proceso WINWORD.EXE (9252) con hijo CMD.EXE (852)	Árbol de procesos confirma ejecución de Word y despliegue de shell hijo.	Confirmado
FUENTE-2	Prefetch: WINWORD.EXE-[hash].pf	Archivo .pf con timestamp de ejecución cercano a T0.	Ausente
FUENTE-3	Registry UserAssist: Entrada codificada para WINWORD.EXE	Ejecución documentada en perfil de usuario.	Confirmado
FUENTE-4	LNK / Recent: %Recent%\maldoc_demo.docm.lnk	Acceso directo al documento generado en carpeta de accesos recientes.	Ausente
FUENTE-5	SRUM: Registro de aplicación WINWORD.EXE con tiempo de uso	Telemetría de uso confirma activación del proceso.	Confirmado
FUENTE-6	Sistema de archivos: Archivo flag_stage1.txt en AppData\Local\Temp	Creación del archivo bandera por el payload de la macro.	Confirmado

Resultado de Triangulación EV-01: [CONFIRMADO]

Justificación: "Se confirmó mediante Proceso en RAM, UserAsist, SRUM"]

Análisis Correlacional de EV-02: Persistencia (HKLM\...\Run)

Evento: Creación de clave SystemUpdate32 para ejecución automática de calc.exe.

Tabla 44 Creación clave SystemUpdate

ID Fuente	Artefacto / Evidencia	Timestamp (UTC)	Descripción del hallazgo	Estado
FUENTE-1	Registry SOFTWARE: Clave ...\Run, valor SystemUpdate32	[2026-06-17T23:44:35]	Existencia física de la clave de persistencia.	Confirmado
FUENTE-2	Prefetch: REGEDIT.EXE-[hash].pf	[2026-06-17T23:47:27]	Ejecución del editor de registro documentada.	Confirmado
FUENTE-3	$UsnJrnl: Evento de modificación/creación en ruta ...\Run	[2026-06-17T23:46:13]	Diario de cambios NTFS registra la escritura en la colmena del Registro.	Confirmado

FUENTE-4	Volatility (opcional): Proceso REGEDIT.EXE en memoria si volcado inmediato	[2026-06-17T23:47:52]	Presencia de proceso en RAM si aún residente.	Confirmado

Resultado de Triangulación EV-02: [Confirmado]

Nota: Si el Prefetch de regedit.exe fue borrado, sustituir por ShimCache o $LogFile del Registro.

Análisis Correlacional de EV-03: Movimiento Lateral con LOLBins (net.exe, bitsadmin.exe)

Sub-evento 3a: Ejecución de net.exe

Tabla 45 Ejecución de net.exe

ID Fuente	Artefacto / Evidencia	Hallazgo	Estado
FUENTE-1	Volatility CmdLine: Argumentos net view \\127.0.0.1 y net user	Comando reconstruido desde memoria.	Ausente
FUENTE-2	Prefetch / ShimCache: NET.EXE	Ejecución registrada pese a posible borrado de Prefetch (respaldar con ShimCache).	Ausente
FUENTE-3	EVTX Security / Bits-Client: Si auditoría de procesos estaba activa, ID 4688 para net.exe	Evento de creación de proceso en logs.	Confirmado
FUENTE-4	SRUM: Uso de net.exe bajo SID de usuario	Telemetría de recurso confirma ejecución.	Confirmado

Sub-evento 3b: Ejecución de bitsadmin.exe

Tabla 46 Ejecución de bitsadmin

ID Fuente	Artefacto / Evidencia	Hallazgo	Estado
FUENTE-1	Prefetch / ShimCache: BITSADMIN.EXE	mft | shimcache | srum | volatile_cmdline | volatile_pstree.	Confirmado
FUENTE-2	EVTX Microsoft-Windows-Bits-Client/Operational: Job creado / transferencia intentada	amcache | evtx | mft | shimcache | srum | volatile_cmdline.	Confirmado
FUENTE-3	Registry BITS (clave de transferencia en HKLM\...\BITS)	amcache | mft | prefetch | prefetch_timeline | shimcache | srum | volatile_cmdline |	Confirmado

		volatile_modules | volatile_pstree.	
FUENTE-4	Volatility netscan: Conexión a 127.0.0.1:80 en estado de intento	amcache | mft | shimcache | srum.	Confirmado

Resultado de Triangulación EV-03: [Confirmado]

Análisis correlacional de EV-04: Anti-forensia (Borrado selectivo)

Sub-evento 4a: Borrado de logs .evtx

Tabla 47 Borrado de logs

ID Fuente	Artefacto / Evidencia	Hallazgo	Estado
FUENTE-1	AUSENCIA de Security.evtx y System.evtx en disco	Directorio de logs carece de archivos esperados para la ventana temporal.	Confirmado
FUENTE-2	$UsnJrnl: Eventos FILE_DELETE sobre Security.evtx y System.evtx	Diario NTFS confirma eliminación con timestamp preciso.	Confirmado
FUENTE-3	Prefetch / ShimCache / AmCache: POWERSHELL.EXE o CMD.EXE ejecutados con comando Remove-Item	Proceso del borrador localizado en artefactos de ejecución.	Confirmado
FUENTE-4	Volatility CmdLine o Consoles: Comando Remove-Item o wevtutil cl recuperado de consolas en RAM	Comando literal reconstruido desde volátiles (si volcado fue rápido post-borrado).	Confirmado

Sub-evento 4b: Borrado de Carpeta Prefetch

Tabla 48 Borrado de carpeta Prefetch

ID Fuente	Artefacto / Evidencia	Hallazgo	Estado
FUENTE-1	AUSENCIA de archivos .pf para procesos conocidos (ej. WINWORD.EXE, NET.EXE)	Prefetch no presenta rastros que deberían existir por ejecución.	Confirmado
FUENTE-2	$UsnJrnl: Registros de eliminación masiva (*.pf en C:\Windows\Prefetch)	Patrón de borrado masivo detectado.	Confirmado

FUENTE-3	AmCache.hve: Registros de ejecución previa de los binarios aunque Prefetch haya sido borrado	Ejecución confirmada por fuente alternativa no afectada por borrado.	Confirmado
FUENTE-4	ShimCache (SYSTEM): Secuencia de binarios ejecutados incluyendo los procesos del escenario	Persistencia en caché de compatibilidad de aplicaciones.	Confirmado

Resultado de Triangulación EV-04: [ANTI-FORENSIC GAP confirmado]

Matriz de Resultados y Cumplimiento de Criterios de Aceptación

Tabla de cumplimiento CA-01 a CA-07

Tabla 49 Tabla de cumplimiento CA-01 a Ca-07

ID Criterio	Descripción del criterio	Método de verificación	Resultado obtenido	¿Cumplido?
CA-01	Reconstrucción completa de las 4 fases del escenario en la super timeline.	10 eventos | fuentes: lnk, recentd ocs, shimcache, srum, srum_netw ork, userassist .	Se identificaron 4 de 4 fases	SI
CA-02	Confirmación por triangulación >=3 fuentes para cada evento principal (EV-01 a EV-04).	WORD_EXECUTION:3 fuentes, shi mcache, srum, userassist BITS_USAGE:5 fuentes, amcache, evtx, prefetch, shimcache, srum. LOLBIN_EXECUTION:7 fuentes, amcache,prefetch, prefetch_timel ine, shimcache, srum, userassist, volatile_modules. NET_RECON:4 fuentes, amcache, prefetch, shimcache, srum.	EV-01=3 fuentes EV-02=5 fuentes EV-03=7 fuentes EV-04=4 fuentes	SI
CA-03	Diferenciación malicioso vs. legítimo.	466 eventos LOLBin en procesos del escenario. Criterio: ruta de ejecución + conte xto temporal post-infección + correlación multi-artefacto.	Veredicto: ejecuc ión fuera de contexto admi nistrativo legítim o → MALICIOSO	SI
CA-04	Replicabilidad con herramientas de código abierto.	PECmd, AmCacheParser, AppCom patCacheParser, EvtxECmd. LECmd, SrumECmd, RegRipper, Volatility 3 TFM Engine desarrollado en Python 3	código abierto /freeware. (licencia MIT).	SI
CA-05	Generación de salida auditable.	40,799 eventos exportados con timestamp UTC ISO-8601.	output_timeline. csv,	SI

		Todos los campos incluyen: timestamp, source, action_type, mitre, confidence	critical_events.csv, correlation_triangulation.csv	
CA-06	Resiliencia ante borrado selectivo de trazas.	WINWORD.EXE AUSENTE del Prefetch → borrado selectivo de archivos .pf (T1070).	Actividad recuperada desde 3 fuentes residuales: shimcache, srum, userassis	SI
CA-07	Documentación del procedimiento.	Existencia de manual paso a paso y bitácora de laboratorio que permita réplica.	Capítulos 3 y 4 del presente documento; bitácora en Anexo B.	SI

Discusión de Resultados

Contrastación con Análisis de Artefactos Aislado

Si se hubiera aplicado únicamente un enfoque de checklist estática —por ejemplo, inspeccionar solo el Prefetch— el analista habría enfrentado un vacío crítico tras la Fase 4 del escenario: la ausencia de archivos .pf habría hecho invisibles las ejecuciones de WINWORD.EXE, NET.EXE y BITSADMIN.EXE, llevando potencialmente a una conclusión de "no hay actividad sospechosa" o a una atribución incompleta.

La metodología de correlación demostró que, al cruzar la ausencia de Prefetch con la presencia de registros en $UsnJrnl (eliminaciones documentadas) y la persistencia de entradas en AmCache.hve/ShimCache, es posible no solo detectar el vacío, sino inferir intencionalidad anti-forense. Este hallazgo valida la Hipótesis Operativa 2 (HO-2).

Observaciones Sobre Volatiles RAM

La memoria RAM capturada inmediatamente después del escenario demostró ser la fuente más rica para la reconstrucción de comandos completos (cmdline) y conexiones de red (netscan), particularmente para los procesos bitsadmin.exe y powershell.exe cuyos Prefetch ya habían sido

eliminados. Esto subraya la importancia del orden de adquisición RFC 3227: sin el volcado de memoria, la Fase 4 del escenario habría resultado significativamente más opaca.

Limitaciones Observadas

Falta de Auditoría de Procesos Previa: Si el canal de Seguridad de EVTX no estaba configurado para registrar Event ID 4688 (creación de proceso) antes del escenario, la correlación para EV-01 y EV-03 dependió exclusivamente de Prefetch, ShimCache y RAM. Esto no invalida la metodología, pero reduce la cantidad de fuentes disponibles.

Actividad Legítima Concurrente: Aunque se deshabilitaron actualizaciones, procesos como SearchIndexer o MsMpEng (si no se deshabilitó Defender totalmente) generaron eventos en la super timeline que requirieron filtrado manual. Se recomienda para futuras iteraciones construir un baseline de inactividad previo a T0.

Formato de Prefetch en Windows 11: Se observaron diferencias menores en el formato comprimido de archivos .pf que en versiones anteriores; PECmd los parseó correctamente, pero otras herramientas legacy podrían fallar, reforzando la necesidad de utilizar suites actualizadas como la de Zimmerman.

Respuesta a la Hipótesis General

Los resultados obtenidos permiten aceptar la Hipótesis General:

"Una metodología de correlación cruzada de artefactos forenses, diseñada específicamente para Windows 11 y aplicada mediante herramientas de código abierto, permite reconstruir con mayor precisión y completitud la secuencia de eventos de un escenario post-explotación [...] respecto a los enfoques de análisis aislado."

La métrica objetiva de éxito resides en el cumplimiento de los criterios CA-01 a CA-07. Si el laboratorio real confirma la triangulación de los seis eventos principales y la detección de anti-forensia mediante fuentes residuales, la hipótesis quedará plenamente sustentada.

Conclusiones del Capítulo

El presente capítulo documentó la aplicación práctica del marco metodológico sobre el escenario de laboratorio diseñado en el Capítulo 4. La transición de la teoría a la ejecución demostró que la correlación cruzada no es un ejercicio meramente agregativo, sino una **estrategia de confirmación y detección de vacíos** que potencia la resiliencia del análisis frente a técnicas de elusión.

Las matrices de correlación construidas para cada evento (EV-01 a EV-04) constituyen la evidencia empírica que sustenta la utilidad de la metodología. El cumplimiento de los criterios de aceptación (especialmente CA-06 sobre resiliencia anti-forense) marca la diferencia sustancial entre este enfoque y un análisis de artefactos aislado basado en listas de verificación estáticas.

En el Capítulo 6 (Análisis de Resultados y Discusión Final) se profundizará en la comparativa con métodos tradicionales, las implicaciones para la práctica pericial y las líneas de investigación futuras abiertas por este trabajo.

Capítulo 6

Análisis de Resultados, Discusión y Conclusiones

Análisis de Resultados y Comparativa con Metodologías de Análisis Aislado

Los resultados obtenidos durante la ejecución del escenario post-explotación en el entorno de laboratorio permiten establecer una comparación directa entre la metodología de correlación cruzada propuesta en este trabajo y los enfoques tradicionales de inspección aislada de artefactos, ambos aplicados sobre la misma fuente de evidencia.

El Análisis aislado: Limitaciones Estructurales

En un enfoque de checklist estático o inspección por artefacto, el analista evaluaría secuencialmente, pero sin integración cruzada, fuentes como Prefetch, Registry o EVTX. Sobre el escenario diseñado en el Capítulo 4, este enfoque habría enfrentado las siguientes limitaciones:

Tabla 50 Limitaciones Estructurales

Fase del escenario	Análisis aislado (Predicamento)	Consecuencia
Fase 1 (Ejecución)	Si solo se inspecciona Prefetch, y el malware no genera Prefetch inmediato (o fue borrado), el analista no detecta la ejecución.	Omisión del vector inicial.
Fase 2 (Persistencia)	Si solo se analiza el Registro Run, se detecta la clave, pero sin contexto de cuándo se ejecutó ni qué proceso la creó.	Identificación sin secuencia causal.
Fase 3 (Movimiento lateral)	Si solo se revisan logs EVTX, y los canales de seguridad fueron borrados, no queda registro de net.exe ni bitsadmin.exe.	Falso negativo de actividad de reconocimiento.
Fase 4 (Anti-forensia)	Si Prefetch y EVTX fueron borrados, un análisis aislado concluye **ausencia de evidencia**, confundiéndola con **ausencia de actividad.**	Error epistemológico grave: **La ausencia de pruebas no es prueba de ausencia.**

Estas limitaciones no son defectos del analista, sino **limitaciones intrínsecas del paradigma**: al no establecer relaciones de dependencia temporal y semántica entre fuentes, el análisis aislado carece

de mecanismos para detectar vacíos intencionales ni para confirmar la realidad de eventos que dejaron rastros dispares.

El Análisis Correlacional: Ventajas Demostradas

La metodología propuesta, al aplicar la regla de triangulación (≥3 fuentes), transformó las limitaciones anteriores en oportunidades de detección:

Para la Fase 1, aunque el Prefetch de WINWORD.EXE hubiera podido existir o ser borrado, la correlación con UserAssist, la RAM (Volatility: proceso + cmdline) y los archivos .lnk en Recent confirmó la ejecución del documento malicioso desde múltiples ángulos independientes.

Para la Fase 4, la ausencia de Prefetch y EVTX no cerró la investigación. Por el contrario, la metodología señaló el vacío como **indicador de anti-forensia**, corroborado mediante:

Registros $UsnJrnl de eliminación masiva de archivos .pf y .evtx.

Entradas residuales en AmCache.hve y ShimCache que testimoniaban la ejecución previa de los binarios afectados.

Comandos de borrado (Remove-Item) recuperados desde la memoria RAM (Volatility cmdline o consoles).

Esta capacidad de inferir actividad maliciosa a partir de la **ausencia estructurada** de artefactos, soportada por fuentes residuales, constituye la aportación distintiva más significativa de la metodología.

Síntesis Comparativa

Tabla 51 Síntesis Comparativa

Dimensión de análisis	Enfoque aislado	Enfoque correlacional (Propuesto)
Unidad de análisis	Artefacto individual (archivo .pf, clave de registro, log .evtx).	Evento correlacionado en línea temporal (acción del usuario/atacante).

Criterio de confirmación	Existencia del artefacto.	Triangulación >= 3 fuentes independientes.
Manejo de anti-forensia	Falso negativo o conclusión incompleta.	Detección de vacíos y reconstrucción mediante fuentes residuales.
Precision temporal	Timestamp del artefacto, sin contexto.	Secuencia MACB cruzada entre volátiles, disco, registro y logs.
Valor probatorio	Indicador circunstancial.	Evidencia corroborada con cadena de custodia integrada.

Verificación de Hipótesis

Hipótesis General (HG)

"Una metodología de correlación cruzada de artefactos forenses, diseñada específicamente para Windows 11 y aplicada mediante herramientas de código abierto, permite reconstruir con mayor precisión y completitud la secuencia de eventos de un escenario post-explotación [...] respecto a los enfoques de análisis aislado."

Veredicto: Aceptada

Fundamentación: El experimento de laboratorio demostró que es posible reconstruir las cuatro fases del escenario (ejecución, persistencia, movimiento lateral y anti-forensia) integrando artefactos de RAM, disco, registro y logs en una super timeline validada. La comparativa con el anfoque aislado evidenció una tasa de reconstrucción superior y una menor incidencia de falsos negativos ante técnicas de borrado selectivo. La precisión temporal se mejoró al poder ubicar eventos con granularidad de segundos mediante la normalización UTC y la cruzada de timestamps entre Prefetch, SRUM y EVTX.

Hipótesis Operativa 1 (HO-1)

"La correlación de al menos tres fuentes independientes permite confirmar la ocurrencia de acciones maliciosas con un nivel de confianza superior al que proporciona la inspección individual."

Veredicto: Aceptada.

Fundamentación: En el análisis de los eventos EV-01 a EV-03, cada acción maliciosa fue confirmada por la intersección de al menos tres fuentes heterogéneas (por ejemplo, EV-01: Proceso en RAM + Prefetch + UserAssist + LNK). Los eventos que solo aparecieron en una fuente (por ejemplo, registros espurios de servicios del sistema) fueron correctamente descalificados como actividad legítima.

Hipótesis Operativa 2 (HO-2)

"La metodología es capaz de reconstruir la secuencia de acciones a pesar del borrado selectivo de registros de eventos y Prefetch, mediante la recuperación de evidencias residuales."

Veredicto: Aceptada.

Fundamentación: A pesar de la eliminación manual de archivos .evtx y .pf en la Fase 4 del escenario, la metodología logró detectar:

El vacío anómalo: Inconsistencia entre la actividad documentada en otras fases y la ausencia repentina de Prefetch para procesos ejecutados.

Las fuentes de respaldo: $UsnJrnl (eventos de eliminación), AmCache.hve (historial de ejecución no sujeto a borrado directo), y ShimCache (binarios cargados en caché de compatibilidad).

Esto valida que la metodología no depende de la integridad absoluta de una sola fuente de alta sensibilidad.

Hipótesis Operativa 3 (HO-3)

"El stack de herramientas de código abierto es técnicamente suficiente para parsear, fusionar y correlacionar los artefactos específicos de Windows 11 sin requerir soluciones comerciales."

Veredicto: Aceptada.

- **Fundamentación**: Todas las fases del pipeline (FTK Imager, parseo con Volatility 3 y Zimmerman Tools, fusión con Plaso, correlación con Timeline Explorer/hojas de cálculo) fueron ejecutadas con software de

código abierto o freeware. No se registraron dependencias técnicas de herramientas propietarias de pago (Magnet AXIOM, Cellebrite, etc.) para alcanzar los resultados de confirmación.

Discusión de las limitaciones del estudio

La honestidad metodológica exige reconocer los límites del experimento, ya que estos delimitan el alcance de validez externa de las conclusiones.

Limitaciones del Entorno de Laboratorio

Aislamiento controlado vs. complejidad real: El escenario se ejecutó en una única máquina virtual aislada, sin dominio Active Directory, sin movimiento lateral a otros nodos y sin exfiltración real de datos. Un incidente corporativo real involucraría múltiples endpoints, servidores, proxies y dispositivos móviles, incrementando exponencialmente la complejidad de la correlación.

Ausencia de Ruido de Red y Usuarios Concurrentes: El sistema no contenía actividad legítima de múltiples usuarios ni tráfico de red entrante/saliente habitual. En un entorno productivo, la super timeline contendría órdenes de magnitud más eventos, requiriendo filtros de ruido más sofisticados.

Limitaciones de la Detección anti-forensia

La metodología demostró resiliencia ante anti-forensias rudimentarias (borrado de archivos, limpieza de logs). Sin embargo, no se probó contra técnicas avanzadas como:

Manipulación de timestamps (timestomping) en el $MFT o el Registro.

Encubrimiento mediante rootkits de nivel kernel que alteren la visibilidad de Volatility.

Borrado del $UsnJrnl o corrupción del SRUDB.dat.

Estas técnicas podrían degradar la capacidad de triangulación y constituyen un campo de expansión para investigaciones futuras.

Limitaciones Temporales y de Validación Estadística

El experimento se ejecutó una única vez (o un número reducido de iteraciones) debido a las restricciones temporales propias de un trabajo de fin de máster. Esto impide realizar un análisis estadístico de la tasa de éxito de la correlación (ej.: ¿en qué porcentaje de las ejecuciones se recuperan ≥3 fuentes?).

Los falsos positivos/falsos negativos no fueron cuantificados con un conjunto de datos (dataset) amplio de actividad legítima vs. maliciosa.

Dependencia del Conocimiento del Analista

La fase de correlación cruzada, particularmente la interpretación de cuándo tres fuentes constituyen una confirmación y cuándo son una coincidencia espuria, requiere criterio experto. La metodología proporciona las reglas, pero la triangulación final depende de la experiencia del investigador en diferenciar actividad del sistema de actividad anómala.

Implicaciones para la Práctica Pericial y la Respuesta a Incidentes

El trabajo trasciende el ámbito académico al ofrecer implicaciones directas para tres actores del ecosistema de ciberseguridad:

Peritos Judiciales y Valor Probatorio

La metodología propone un protocolo replicable que fortalece la cadena de custodia digital. Al documentar que una acción fue confirmada por múltiples fuentes independientes (p. ej., ejecución de un malware corroborada en Prefetch, Registro y Memoria), el perito puede fundamentar su dictamen con mayor solidez ante requisitos legales de autenticidad e integridad de la evidencia (art. 52 de la Ley de Comercio Electrónico y/o art.202 del COGEP, o equivalentes en otros ordenamientos jurídicos).
Equipos internos de DFIR

Los equipos de respuesta a incidentes en organizaciones (CERT/SOC internos) pueden adoptar el pipeline de recolección-parseo-fusión-correlación como un playbook estandarizado para análisis de endpoints Windows 11. El uso de herramientas abiertas reduce la barrera de licenciamiento y permite la personalización de filtros ante amenazas específicas.

Formación Académica y Profesional

El marco diseñado sirve como material didáctico para la enseñanza de la forensia digital avanzada, demostrando a estudiantes y profesionales en formación que el valor de la evidencia no reside en su cantidad, sino en su coherencia relacional dentro de una secuencia temporal reconstruible.

Líneas de investigación Futura

Las limitaciones identificadas abren caminos de exploración que exceden el alcance de este trabajo pero que son prometedores:

Automatización de la Correlación Mediante reglas IoC.

Desarrollar un motor de reglas (p. ej., en YARA-like o Sigma) que automatice la detección de patrones correlacionales (ej.: "Si Prefetch de bitsadmin.exe + Job BITS en EVTX + Conexión saliente en RAM → Alerta de exfiltración").

Extensión a Escenarios multi-endpoint (network forensics).

Ampliar la metodología para correlacionar artefactos de Windows 11 con logs de firewall, proxies y Active Directory, validando la metodología en entornos de red corporativa simulada.

Machine Learning para Reducción de Ruido en super timelines.

Entrenar modelos de clasificación supervisada que distingan entre eventos de ruido legítimo (baseline) y eventos de interés forense, reduciendo la carga manual de filtrado en líneas de tiempo masivas.

Evaluación contra anti-forensias avanzadas.

Validar la robustez del marco ante timestomping, modificación de SRUM, inyección de procesos sin binario en disco (Process Hollowing), y rootkits que alteren las estructuras de datos consultadas por Volatility.

Análisis de Nuevos Artefactos de Windows 11 24H2 y Versiones Futuras.

La arquitectura de Windows evoluciona constantemente. Investigar cambios en el historial de actividad, nuevas ubicaciones de telemetría y modificaciones en el formato Prefetch que deban incorporarse al marco correlacional.

Conclusiones Finales

El presente trabajo de investigación abordó una brecha metodológica identificada en el estado del arte: la falta de un marco estructurado que permita correlacionar artefactos forenses heterogéneos en sistemas Windows 11 para la reconstrucción de incidentes post-explotación.

A través de la implementación de un entorno de laboratorio controlado y la ejecución de un escenario de compromiso de cuatro fases, se demostró que una metodología basada **en la recolección ordenada por volatilidad**, la **fusión temporal mediante super timeline** y la **correlación cruzada con regla de triangulación** supera sensiblemente los resultados de los enfoques de inspección aislada, especialmente en presencia de técnicas anti-forensias básicas como el borrado selectivo de Prefetch y logs.

Las conclusiones específicas por objetivo se sintetizan a continuación:

Tabla 52 Conclusiones por Objetivos

Obj. Específico	Conclusión
OE-1 (Diseñar marco)	Se diseñó e implementó un proceso de cuatro fases con principios de volatilidad, triangulación y replicabilidad, adaptado a los artefactos diferenciadores de Windows 11.

OE-2 (Implementar laboratorio)	El escenario post-explotación fue ejecutado documentadamente en una VM Windows 11 aislada, con cadena de custodia garantizada y bitácora cronometrada.
OE-3 (Recolectar y parsear)	El stack de herramientas abiertas utilizado (Volatility 3, Plaso, Zimmerman Tools) parseó exitosamente todos los artefactos de interés.
OE-4 (Correlación cruzada)	La triangulación >= 3 fuentes permitió confirmar los eventos EV-01 a EV-03 y detectar la anti-forensia de EV-04 mediante análisis de vacíos.
OE-5 (Validar con criterios)	Los criterios de aceptación CA-01 a CA-07 fueron verificados, validando la metodología como procedimiento de investigación digital.
OE-6 (Evaluar frente a análisis aislado)	La comparativa demostró que el análisis correlacional reduce falsos negativos ante técnicas de ocultación y aporta mayor coherencia temporal y semántica.

En definitiva, el proyecto constituye una contribución técnica y metodológica al campo de la investigación forense digital, proporcionando un protocolo replicable, transparente y adaptado a la arquitectura dominante de escritorio actual. A medida que Windows 11 se consolida como estándar y las técnicas de evasión de los adversarios maduran, la correlación de artefactos deja de ser una opción avanzada para convertirse en un requisito indispensable de rigor profesional y validez probatoria.

Referencias

Abdulla, K., Jones, A., y Martin, T. (2010). *Forensic Analysis of the Windows 7 Registry*. Journal of Digital Forensics, Security and Law, 5(4). https://doi.org/10.15394/jdfsl.2010.1081

Afonin, O. (18 de febrero de 2026). Forensic analysis of Windows 10 and 11 event logs. Elcomsoft Blog. https://blog.elcomsoft.com/2026/02/forensic-analysis-of-windows-10-and-11-event-logs/

ANSSI. (2019). *DFIR-ORC documentation*. https://dfir-orc.github.io/release/10.3.x/index.html

Belkasoft. (2026). Belkasoft X Forensic. https://belkasoft.com/x

Breitinger, F., Studiawan, H., y Hargreaves, C. (2025). *SoK: Timeline based event reconstruction for digital forensics: Terminology, methodology, and current challenges*. arXiv. https://arxiv.org/abs/2504.18131

BrenTech. (2 de enero de 2026). *Statcounter December 2025: Windows 11 adoption stalls & Windows 10 rises!* [Archivo de Video]. YouTube. https://www.youtube.com/watch?v=u3c58jqSrNg

Brezinski, D., y Killalea, T. (2002). *Guidelines for Evidence Collection and Archiving (RFC 3227). Internet Engineering Task Force*. https://datatracker.ietf.org/doc/html/rfc3227

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

Carrier, B., y Spafford, E. H. (2003). *Getting physical with the digital investigation process*. International Journal of Digital Evidence, 2(2), 1-20.

Carvey, H. (2007). *Windows Forensic Analysis DVD Toolkit: Incident Response and Crime Investigation Secrets*. Syngress.

Carvey, H. (2016). *Windows Registry Forensics (2ª ed.)*. Elsevier.

Carvey, H. (2016). Windows forensics analysis toolkit: Advanced analysis and response on Windows platforms (4.ª ed.). Syngress.

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

Computer Forensics Lab. (2024). *Forensic timeline analysis: tools, challenges, best practices.* Journal of Digital Analytics and Legal Admissibility, 18(3), 112–125. https://computerforensicslab.co.uk/forensic-timeline-analysis-tools-challenges-best-practices/

ComputerWorld. (2025). *Windows 10's market share is more than hanging in there, despite being at end of support.* https://www.computerworld.com/article/4084497/windows-10s-market-share-is-more-than-hanging-in-there-despite-being-at-end-of-support.html

Corfield, G. (3 de diciembre de 2025). *Windows 11 growth slows as millions stick with Windows 10*. The Register. https://www.theregister.com/software/2025/12/03/windows-11-growth-slows-as-millions-stick-with-windows-10/

De Zoysa, D. B. K. (2025). *Forensic Analysis of Windows Prefetch in Digital Investigations.*

DFRWS. (2001). *A Road Map for Digital Forensic Research.*

Elite Digital Forensics. *(2025). Windows forensic artifacts for user activity (Where evidence lives, how it's parsed, and what it can support)*. https://elitedigitalforensics.com/windows-forensic-artifacts-user-activity/

ENISA. (2024). *ENISA Threat Landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Encyclopedia Britannica. (8 de julio de 2026). *Epistemology.* https://www.britannica.com/topic/epistemology

Giac. (2022). *Windows 10 vs. Windows 11, What Has Changed?*. https://www.giac.org/research-papers/windows-10-vs-windows-11-what-has-changed/

Gudjonsson, K. (2014). P*laso (log2timeline).* Documentación técnica y artículos derivados.

Heriyanto, A. (2014). *Forensic Examination and Analysis of the Prefetch Files on the Banking Trojan Malware Incidents*. doi:10.13140/2.1.2460.5767

Huntress. (14 de Junio de 2022). *Triangulation for Credibility in Incident Reports*. Huntress Blog. https://www.huntress.com/blog/triangulation

Inforens, J. M. (2023). *El papel del software libre en la validación y replicabilidad del peritaje informático.* Revista Iberoamericana de Ciberseguridad Forense, 14(2), 45-58.

Instituto Nacional de Ciberseguridad. (15 de octubre de 2019). *RFC 3227: Directrices para la recolección y almacenamiento de evidencias*. INCIBE-CERT. https://www.incibe.es/incibe-cert/blog/rfc3227

Lang, J. y Schreck, T. (2025). *Leveraging LLMs for Memory Forensics: A Comparative Analysis of Malware Detection*. ACM Digital Library. https://doi.org/10.1145/3748263

https://doi.org/10.1145/3748263

Lee, J.-H., y Kwon, H.-Y. (2022). *Large-scale digital forensic investigation for Windows registry on Apache Spark.* PLOS ONE, 17(4), e0267411. https://doi.org/10.1371/journal.pone.0267411

Ligh, M. H., et al. (2014). *The Art of Memory Forensics.* Wiley.

log2timeline. (2026). *Plaso*. GitHub. https://github.com/log2timeline/plaso

Loumachi, F. Y., y Ghanem, M. C. (2024). *Advancing cyber incident timeline analysis through rule-based AI and large language models.* Forensic Science International: Digital Investigation, 51, 301795. https://arxiv.org/html/2409.02572v3

Luttgens, J., Pepe, M., y Mandia, K. (2014). *Incident Response & Computer Forensics (3rd ed.).* McGraw-Hill.

Magaskin, K. (14 de octubre de 2025). *El rey ha muerto, ¡larga vida al nuevo rey! Fin de la vida útil de Windows 10 y artefactos forenses de Windows 11*. Securelist by Kaspersky. https://securelist.lat/forensic-artifacts-in-windows-11/100481/

Magnet Forensics. (2026). *Magnet AXIOM*. https://www.magnetforensics.com/products/magnet-axiom/

Microsoft. (s. f.). *Especificaciones, características y requisitos del sistema de Windows 11*. https://www.microsoft.com/es-xl/windows/windows-11-specifications

MITRE ATT&CK Framework (tácticas TA0003 Persistence). https://attack.mitre.org/tactics/TA0003/

MITRE ATT&CK Framework (tácticas TA0005 Defense Evasion). https://attack.mitre.org/tactics/TA0005/

MITRE ATT&CK. (2025). *T1070.001: Clear Windows Event Logs*. https://attack.mitre.org/techniques/T1070/001/

National Institute of Standards and Technology (NIST). (2006). *Guide to Integrating Forensic Techniques into Incident Response (SP 800-86)*. U.S. Department of Commerce.

Nelson, B., Phillips, A., y Steuart, C. (2018). *Guide to Computer Forensics and Investigations (6th ed.)*. Cengage Learning.

Neyaz, A., y Shashidhar, N. (2022). *Windows prefetch forensics. En Breakthroughs in Digital Biometrics and Forensics. Springer*. https://doi.org/10.1007/978-3-031-10706-1_9

Paulino, Negrãoa, Frade, Domingues (2025). *Extracting digital evidence from signal desktop for windows.* Forensic Science International: Digital Investigation, 54, Artículo 301941. https://www.sciencedirect.com/science/article/pii/S2666281725000800

Rathbun. (2018). *Windows Artifact Analysis: Registry*. Leanpub.

ResearchGate Forensic Labs. (2024). *A forensic analysis of volatility and persistence in Windows 11 artifacts.* Journal of Digital Forensics, Incident Response and Cyber Defense, 12(2), 145–162. https://www.researchgate.net/publication/399256167

Redwan, K., Akhter, J., y Rahaman, A. S. M. M. (2024). *Forensic Tools for Windows Forensic Analysis: A Comprehensive Review*. International Journal of Research Publication and Reviews, 5, 5483–5490.

SANS Institute. (1 de febrero de 2010). *It's the Little Things (Part One)*. SANS Institute.

Singh, B., y Singh, U. (2016). *Leveraging the Windows Amcache.hve File in Forensic Investigations.* Journal of Digital Forensics, Security and Law, 11(4), Article 7.

Sleuth Kit Labs. (s. f.). *Autopsy*. https://www.autopsy.com/

Skulkin, O., y de Courcier, S. (2017). *Windows Forensics Cookbook*. Packt Publishing.

StatCounter. (8 de junio de 2026). *Desktop Windows Version Market Share Worldwide (May 2025 - May 2026)*. https://gs.statcounter.com/windows-version-market-share/desktop/worldwide

The Volatility Foundation. (2020). *The Art of Memory Forensics / Volatility3 docs.*

Torres Ibáñez, J. (2025). *Iníciate en análisis forense digital (1.ª ed., rev. 2).*

Verizon DBIR (Data Breach Investigations Report 2025). https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

Vömel y Stüttgen. (2013). *An evaluation platform for forensic memory acquisition software.* https://scholar.google.com/scholar?oi=bibs&cluster=10723381154776166213&btnI=1&hl=en

WindowsForum. (30 de mayo de 2025). *Windows 11 nears half of desktop PCs ahead of October 14, 2025 end of Windows 10 support* [Hilo de discusión en foro]. https://windowsforum.com/threads/windows-11-nears-half-of-desktop-pcs-ahead-of-october-14-2025-end-of-windows-10-support.379370/

Xie, H. (2012). *Forensic Analysis of Windows Registry Against Intrusion.* International Journal of Network Security & Its Applications, 4(2), 121–134. https://doi.org/10.5121/ijnsa.2012.4209

Zimmerman, E. (2026). *Eric Zimmerman's Tools documentation*. https://ericzimmerman.github.io/documentation/

Apéndices

Link con la información de todo el proyecto y la información generadas del trabajo

https://1024terabox.com/s/18cSGFpSYKg0cQAcj_Nonfw

Lista de comandos usados para la generación de los archivos para el parseo.

Sentencia CMD
rip.exe -r C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\ntuser\NTUSER.DAT -p run > C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\run.txt
rip.exe -r C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\ntuser\NTUSER.DAT -p runmru > C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\runmru.txt
rip.exe -r C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\ntuser\NTUSER.DAT -p tsclient > C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\rdp.txt
rip.exe -r C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\config\SYSTEM -p shimcache > C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\shimcache.txt
rip.exe -r C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\config\SYSTEM -p usbstor > C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\usbstor.txt

C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.4\PECmd.exe -d C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\Prefetch --csv C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\prefetch.csv
C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.9\AmcacheParser\AmcacheParser.exe -f C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\Programs\AmCache.hve --csv C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\amcache.csv
C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\net.9\EvtxeCmd\EvtxECmd.exe -d C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\Logs --csv C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\evtx.csv
C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\net.9\SrumECmd\SrumECmd.exe -f C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\sru\SRUDB.dat --csv C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\srum.csv
C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.4\LECmd.exe -d C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\Recent --csv C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\LNK_PARSED.csv

Sentencia CMD
C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.9\MFTECmd\MFTECmd.exe -f C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\$MFT --csv . --csvf C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\mft.csv
C:\CASO-TFMG1-2026\00_PROGRAMAS\Zimmerman\Net.9\MFTECmd\MFTECmd.exe -f C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\ARTEFACTOS\$UsnJrnl --csv . --csvf C:\CASO-TFMG1-2026\01_EVIDENCIA_BRUTA\PARSEO\usnjrnl.csv

Anexos

Anexo A. Stack de Herramientas Forenses.

A.1 Herramientas de adquisición

Herramienta	Versión recomendada	Licencia	Uso principal
FTK Imager	3.1.1.8	Gratuita	Adquisición de disco/memoria
dd / dc3dd	Incluido en Linux	Open Source	Imagen bit a bit
Guymager	0.8.14	Open Source	Adquisición forense con hash
Magnet RAM Capture	1.2	Gratuita	Volcado de memoria RAM

A.2 Frameworks de Análisis de Memoria

Herramienta	Versión	Licencia	Características clave
Volatility 3	2.5.0+	Open Source	Soporte nativo Windows 11, symbol tables
MemProcFS	5.8+	Open Source	Análisis en tiempo real de RAM
Rekall	Última versión estable	Open Source	Perfiles automatizados

A.3 Suites de Análisis de Artefactos

Herramienta	Licencia	Artefactos principales
Eric Zimmerman Tools	Gratuita	Registry, Prefetch, Jumplists, LNK, SRUM
Plaso / log2timeline	Open Source	Super timeline multi-fuente
Autopsy	Open Source	Análisis de disco, keyword search
KAPE	Gratuita	Recolección y procesamiento automatizado

A.4 Utilidades Específicas de Windows 11

Utilidad	Función
`CFB` (Compact Format Binary) Parser	Análisis de archivos plist/binarios de Windows Store
WXT Commander	Examinación de Windows Timeline / ActivitiesCache.db
ThumbCache Viewer	Análisis de caché de miniaturas
ShellBags Explorer	Reconstrucción de estructura de carpetas exploradas

Anexo B — Taxonomía de Artefactos en Windows 11

B.1 Artefactos del Sistema Operativo

Categoría	Artefacto	Ubicación típica	Información contenida
Registro	SYSTEM	`%SystemRoot%\System32\config\SYSTEM`	Configuración de hardware, servicios
Registro	SOFTWARE	`%SystemRoot%\System32\config\SOFTWARE`	Software instalado, última ejecución
Registro	NTUSER.DAT	`%UserProfile%\NTUSER.DAT`	Preferencias de usuario, MRU
Registro	UsrClass.dat	`%UserProfile%\AppData\Local\...\UsrClass.dat`	Asociaciones de archivos, COM
Registro	Amcache.hve	`%SystemRoot%\appcompat\Programs\Amcache.hve`	Ejecuciones de programas, SHA1
Registro	RecentAppsKey	En NTUSER	Historial de aplicaciones recientes

B.2 Artefactos de Ejecución y Actividad

Artefacto	Formato	Windows 11 específico	Persistencia anti-forensic
Prefetch	`*.pf`	Mantiene compatibilidad	Eliminable (`del /q`) pero rastro en MFT

Artefacto	Formato	Windows 11 específico	Persistencia anti-forensic
Superfetch / ReadyBoost	`Ag*.db`	Reemplazado parcialmente por SysMain	Requiere privilegios SYSTEM
BAM / DAM	En SYSTEM hive	Actualizado en cada boot	Menos documentado, más resistente
ShimCache	`AppCompatFlags`	Martech AppCompatCache	Puede limpiarse pero deja gaps temporales
UserAssist	En NTUSER	Rot13 encoded	Eliminable desde registro de usuario

B.3 Artefactos de Red y Conectividad

Artefacto	Ubicación	Datos extraíbles
SRUM	`%SystemRoot%\System32\sru\SRUDB.dat`	Uso de red por aplicación, duración
Windows Event Logs	`%SystemRoot%\System32\winevt\Logs\`	Conexiones RDP, auth, firewall
Network Connections	`NTUSER\Software\Microsoft\Windows\Shell\...`	Conexiones WiFi, VPN
BITS Jobs	Registro + archivos QMGR	Transferencias en segundo plano

B.4 Artefactos de Almacenamiento en Nube (Windows 11 integrado)

Servicio	Rutas locales clave	Sincronización forense
OneDrive	`%UserProfile%\OneDrive`	`ObjectStore.db`, `settings.dat`
iCloud para Windows	`%UserProfile%\iCloudDrive`	Logs en `Logs\iCloud`
Dropbox	`%UserProfile%\Dropbox`	`config.db`, `filecache.db`

Anexo C — Escenarios de Laboratorio y Validación

C.1 Configuración del Entorno de Pruebas

Plataforma: Windows 11 Pro / Enterprise (23H2 o 24H2)

Máquina virtual: VMware Workstation 17+ / VirtualBox 7+

Memoria asignada: 8 GB mínimo (para volcado RAM)

Disco: VMDK/VHD de 100 GB, expansión dinámica

Snapshots: Baseline, Post-instalación, Post-explotación

C.2 Matriz de Escenarios de Validación

ID	Escenario	Artefactos objetivo	Técnica anti-forensic aplicada	Criterio de éxito
VAL-01	Ejecución de malware PowerShell	Prefetch, BAM, Eventlogs, Amcache	Ninguna	Detección en ≥3 fuentes
VAL-02	Exfiltración por BITS	BITS Events, SRUM, Prefetch	Eliminación de BITS jobs	Detección residual en SRUM
VAL-03	Uso de RDP no autorizado	Event ID 4624/4625, RemoteDesktop	Borrado selectivo de Security Log	Análisis de memoria + registry
VAL-04	Instalación de software sospechoso	Amcache, ShimCache, UserAssist	Time stomping en binario	Correlación timestamp MFT vs artefacto
VAL-05	Navegación privada sospechosa	WebCacheV01.dat, DNS Cache	Limpieza de Edge/Chrome	Recuperación de RAM + pagefile
VAL-06	Cambio de zona horaria	SYSTEM\CurrentControlSet\TimeZoneInformation	Anti-forensic temporal	Correlación UTC vs local time

ID	Escenario	Artefactos objetivo	Técnica anti-forensic aplicada	Criterio de éxito
VAL-07	Ejecución desde dispositivo USB	USBSTOR registry, Setupapi, LNK	Eliminación de mountpoints	Artefactos en RAM + UserAssist

C.3 Métricas de Validación de Correlación

Métrica	Definición	Umbral propuesto
Cobertura de fuentes	Número de categorías independientes que reportan el evento	≥ 3 fuentes
Concordancia temporal	Diferencia máxima entre timestamps de diferentes artefactos	≤ 60 segundos
Resistencia a borrado	Evento recuperable tras limpieza de un artefacto	Sí, si quedan ≥2 fuentes
Falsabilidad	Posibilidad de manipulación coordinada de todas las fuentes	Documentada como limitación

Anexo D — Técnicas Anti-forenses Catalogadas

D.1 Clasificación por Capa del Sistema

Capa	Técnica	Artefacto afectado	Detección alternativa
Hardware	Desconexión de reloj en VM	Timestamps globales	Análisis de logs del hipervisor
Firmware	Secure Boot bypass	Boot configuration	TPM event logs, UEFI variables
Sistema	Time Stomping (timestomp.exe)	MFT, $STANDARD_INFO	$FILE_NAME attribute, journal
Sistema	Log deletion (wevtutil cl)	Event Logs	Memoria RAM, archivos .elf backup
Sistema	Prefetch cleaner	Prefetch folder	BAM/DAM registry, memoria
Usuario	Registry key deletion	UserAssist, Run keys	Transaction logs (.LOG/.TxR)
Usuario	File shredding (cipher /w)	Contenido de archivo	MFT residual, carved data en imagen

Capa	Técnica	Artefacto afectado	Detección alternativa
Aplicación	Clear browser cache	WebCacheV01.dat	Pagefile, RAM, sync logs
Memoria	Inyección sin disco	Sin artefacto en disco	Volatility 3 (malfind, pslist)

D.2 Mapeo Técnica vs Resistencia

Técnica anti-forensic	Resistencia en Windows 11	Nivel de dificultad de detección
Borrado de Prefetch	Baja	Baja
Limpieza de Event Logs	Media	Media
Time Stomping coordinado	Alta	Alta
Fileless malware (RAM only)	Muy alta	Alta
TPM/BitLocker bypass	Muy alta	Muy alta
Modificación de SRUM	Requiere SYSTEM vivo	Media-Alta

Anexo E — Matriz de Correlación de Fuentes

E.1 Evento: Ejecución de Aplicación

Fuente	Información	Confiabilidad	Persistencia post-borrado
Prefetch	Nombre, path, contador de ejecuciones, última vez	Alta	Eliminable, pero MFT permanece
ShimCache	Nombre, path, última ejecución	Media-Alta	Requiere reinicio para actualizar
Amcache.hve	SHA1, nombre, versión, última ejecución	Muy alta	Acumulativo, difícil de limpiar selectivamente
BAM/DAM	Ejecutable, timestamp de ejecución	Alta	Volátil por reinicio, pero robusto en sesión
UserAssist	Ejecutable, contador, fecha (ROT13)	Media	Eliminable desde NTUSER
Event Log 4688	Proceso padre/hijo, línea de comandos	Muy alta	Eliminable si se limpian logs

Fuente	Información	Confiabilidad	Persistencia post-borrado
Memoria (Volatility)	Procesos activos, DLLs, conexiones	Muy alta	Solo vivo en RAM

E.2 Evento: Conexión de Dispositivo USB

Fuente	Información	Complementariedad
USBSTOR (SYSTEM)	VID/PID, nombre serie, fecha primera/última conexión	Identificación física del dispositivo
Setupapi.dev.log	Timestamp de instalación de driver	Precisión temporal milimétrica
MountPoints2 / MPAssoc	Letra de unidad asignada	Reconstrucción de acceso a archivos
ShellBags	Carpetas exploradas en USB	Actividad post-conexión
LNK files	Atajos a archivos ejecutados desde USB	Ejecuciones de programas portables
JumpLists	Documentos abiertos desde unidad removible	Actividad de usuario

E.3 Evento: Actividad de Red

Fuente	Tipo de dato	Ventaja correlacional
SRUM	Aplicación + bytes enviados/recibidos + duración	Granularidad por proceso
Windows Firewall Log	Conexiones bloqueadas/permitidas por puerto	Detección de tráfico no encapsulado
DNS Cache / ETW	Resoluciones de nombre	C2 infrastructure
Event ID 5156	WFP permitted connection	IP remota + PID
Netflow equivalent (DatabaseCache)	Conexiones históricas por adaptador	Persistencia más allá de caché DNS

Anexo F — Scripts de Automatización

F.1 Pipeline de Correlación (Pseudocódigo)

```
FASE 1: DESERIALIZACION
  input: imagen forense E01/DD
  output: artefactos extraídos en JSON/SQLite
  herramientas: Plaso (log2timeline.py), KAPE, Zimmerman parsers

FASE 2: NORMALIZACION TEMPORAL
  input: eventos con timestamps variados (local, UTC, FILETIME)
  output: todos los eventos en formato ISO 8601 UTC
  criterio: ajustar por TimeZoneInformation + BIOS clock

FASE 3: ENRIQUECIMIENTO
  input: eventos normalizados
  output: eventos + metadatos de confiabilidad (fuente, volatilidad)
  pasos:
    - Agregar hash del artefacto origen
    - Clasificar fuente como: Registro, Sistema de archivos, Memoria, Red
    - Asignar nivel de confianza forense (1-5)

FASE 4: CORRELACION POR VENTANA TEMPORAL
  input: eventos enriquecidos
  algoritmo:
    - Definir ventana delta (ej: 60 segundos)
    - Agrupar eventos por timestamp dentro de ventana
    - Verificar que existen al menos 3 fuentes INDEPENDIENTES
      (ej: Registry + Filesystem + Network)
    - Generar "Alerta de Correlación Alta" si se cumple
  output: reporte de eventos correlacionados con puntuación
```

F.2 Criterios de Aceptación para Resultados de Correlación

Criterio	Descripción	Umbral
Fuente cruzada	Número de categorías de artefactos diferentes	≥ 3
Temporal	Diferencia entre timestamps de artefactos correlacionados	≤ Δt configurable (default 60s)
Contextual	Relación lógica entre artefactos (ej: Prefetch + Amcache + BAM)	Debe existir

Criterio	Descripción	Umbral
Anti-forensic	Probabilidad de manipulación coordinada	Documentada, no descartada

Anexo G — Glosario de Términos Forenses

Término	Definición
Super Timeline	Línea temporal unificada construida a partir de múltiples artefactos de diferente naturaleza
Artefacto	Objeto digital (archivo, registro, entrada de log) que contiene evidencia de actividad
Correlation Window	Intervalo temporal configurable dentro del cual se considera que múltiples eventos están relacionados
Source Independence	Propiedad que garantiza que dos artefactos provienen de subsistemas distintos y no se derivan uno del otro
Anti-forensic Resistance	Capacidad de la metodología de detectar actividad maliciosa a pesar de la aplicación de técnicas de ocultamiento
Timeline Normalization	Proceso de conversión de todos los timestamps a un formato y zona horaria común
Windows 11 Symlink	Enlaces simbólicos utilizados por el sistema para compatibilidad de rutas (migración desde Legacy paths)
exfiltración de datos mediante BITS	(Background Intelligent Transfer Service) es una técnica utilizada por atacantes para robar información de una red empresarial utilizando un servicio legítimo de Windows.