Maestría en

CIBERSEGURIDAD

Trabajo de investigación previo a la obtención del título de

Magíster en Ciberseguridad

AUTORES:

CHRISTIAN DANIEL MONTENEGRO CRUZ

JORGE RAMON PILATASIG OJEDA

JIMMY ALEXANDER PUENTE QUINGA

ERICK SEBASTIAN VEGA MUELA

TUTORES:

Iván Reyes

Alejandro Cortés

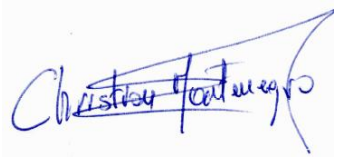
Desarrollo de una estrategia de trabajo para el análisis forense y la identificación de información en sistemas operativos Windows 11

Quito, Octubre 2024

Certificación de autoría

Nosotros, **Christian Daniel Montenegro Cruz, Jorge Ramon Pilatasig Ojeda, Jimmy Alexander Puente Quinga, Erick Sebastian Vega Muela,** 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.



Montenegro Cruz Christian Daniel
1711919074

Pilatasig Ojeda Jorge Ramon
1726605296

Puente Quinga Jimmy Alexander
1719201160

Vega Muela Erick Sebastian
1727604868

Autorización de Derechos de Propiedad Intelectual

Nosotros, **Christian Daniel Montenegro Cruz, Jorge Ramon Pilatasig Ojeda, Jimmy Alexander Puente Quinga, Erick Sebastian Vega Muela,** en calidad de autores del trabajo de investigación titulado ***Desarrollo de una Estrategia de Trabajo para el Análisis Forense y la Identificación de información con Sistema operativo 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, (Octubre 2024)

Montenegro Cruz Christian Daniel
1711919074

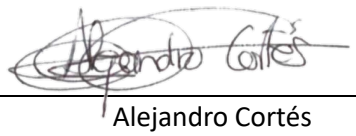
Pilatasig Ojeda Jorge Ramon
1726605296

Puente Quinga Jimmy Alexander
1719201160

Vega Muela Erick Sebastian
1727604868

Aprobación de dirección y coordinación del programa

Nosotros, **Alejandro Cortés e Iván Reyes ,** declaramos que: **Christian Daniel Montenegro Cruz, Jorge Ramon Pilatasig Ojeda, Jimmy Alexander Puente Quinga, Erick Sebastian Vega Muela** 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

El presente trabajo lo dedico a mi amada esposa Johanna, por ser mi compañera incondicional y mi mayor apoyo en esta etapa de mi vida. Gracias por tu paciencia, comprensión y por cada palabra de aliento en los momentos de dificultad. Tu amor y fortaleza han sido la luz que me ha guiado en este camino. Este logro no hubiera sido posible sin ti a mi lado.

A mis hijos Mathias e Isabella, quienes son mi mayor fuente de inspiración y alegría. Cada paso dado en este proyecto ha sido pensando en ustedes, para que vean en mí un ejemplo de esfuerzo y perseverancia. Ustedes son el motor que me impulsa a seguir adelante y la razón por la que aspiro a dar lo mejor de mí cada día.

Con todo mi amor y gratitud, dedico este trabajo a ustedes, mi familia, que hace que todo valga la pena.

Att. Montenegro Cruz Christian Daniel

A mis padres las personas que han sido quienes me han guiado, esforzado y me han brindado todo el apoyo en las variadas circunstacias de la vida, a mis Hermanos que han sido mi soporte en todos mis éxitos, finalmente quiero dedicar este trabajo a Vanessa quién ha sido y es mi compañera de vida.

Att. Pilatasig Ojeda Jorge Ramon

El presente trabajo lo dedico a mi familia ya que han sido quienes han apoyado cada paso en cuanto a la perseverancia y crecimiento personal. A ellos dedico la culminación de mis estudios por ser en todo momento fuente de inspiración y superación

Att. Puente Quinga Jimmy Alexander

Dedico este trabajo a mis padres, mi hermana, mis abuelos y amigos que han estado siempre a mi lado, brindándome su apoyo incondicional y sus valiosos consejos, los cuales me han permitido seguir adelante en cada paso de este camino.

Att. Vega Muela Erick Sebastian

AGRADECIMIENTOS

A Dios, por guiarme y darme fortaleza en cada paso de este camino.

A mis padres Guillermo y Rosita, por sus enseñanzas, amor y apoyo incondicional, que han sido el fundamento de mis logros.

A mi esposa Johanna, por su paciencia, comprensión y constante aliento; sin ti, este logro no habría sido posible.

A mis hijos Mathias Daniel e Isabella Kate, mi mayor inspiración y motivación para seguir adelante. Todo mi esfuerzo es para ustedes.

Att. Montenegro Cruz Christian Daniel

A mi madre que ha sido mi pilar, mi ejemplo a seguir y sobre todo una excelente persona que me ha motivado, me ha dado el empuje para seguir con mi carrera y cumpliendo todas las metas profesionales que me he trazado, todo lo realizado aquí y en mi vida no sería posible sin tan extraordinario ser.

Att. Pilatasig Ojeda Jorge Ramon

Mis agradecimientos y reconocimientos están dirigidos para todas las personas que han sido parte de este camino de crecimiento y aprendizaje y dirigido especialmente para todos quienes han aportado con guías y consejos y que han aportado al enriquecimiento y adquisición de conocimiento. Para todos aquellos que con su esfuerzo han logrado transmitir su conocimiento y han compartido enseñanzas, para todos aquellos mis más sinceros agradecimientos.

Att. Puente Quinga Jimmy Alexander

Quiero expresar mi más profundo agradecimiento a todas aquellas personas que han sido parte de este viaje. A mis padres y mi hermana, por su amor incondicional y por enseñarme el valor de la perseverancia. A mis abuelos, por su sabiduría y por ser un pilar en mi vida.

Att. Vega Muela Erick Sebastian

RESUMEN

Este trabajo propone una estrategia integral para el análisis forense de sistemas operativos Windows 11, centrada en metodologías y técnicas específicas para la recolección y análisis de evidencia digital. En el marco teórico se revisan conceptos clave, organizados en categorías que incluyen herramientas de análisis forense, distribuciones de software, normativas, y regulaciones de seguridad informática aplicables en Ecuador.

La metodología de investigación describe detalladamente el proceso aplicado, incluyendo la validación de la evidencia, análisis del entorno, y las limitaciones inherentes a este tipo de investigación. Como estudio de caso, se desarrolla un ejemplo práctico de análisis forense que abarca la recopilación de datos de la máquina del cliente y un proceso exhaustivo de análisis. Se detalla el flujo de la cadena de custodia y se examinan configuraciones específicas de la máquina del cliente que permiten identificar hallazgos clave. Estos hallazgos son acompañados de recomendaciones prácticas y soluciones personalizadas para el cliente, independientemente de su nivel técnico.

Finalmente, este trabajo concluye con una serie de reflexiones basadas en los puntos desarrollados, destacando tanto los resultados obtenidos como las posibles mejoras en el análisis forense de sistemas Windows 11.

Palabras claves: análisis forense digital, Windows 11, recolección de evidencia, cadena de custodia, seguridad informática, normativas, metodología de investigación, Ecuador, herramientas de análisis.

ABSTRACT

This project proposes a comprehensive strategy for the forensic analysis of Windows 11 operating systems, focusing on specific methodologies and techniques for the collection and analysis of digital evidence. The theoretical framework reviews key concepts, organized in categories that include forensic analysis tools, software distributions, norms, and computer security regulations applicable in Ecuador.

The research methodology describes in detail the applied process, including the validation of evidence, analysis of the environment, and the limitations inherent to this type of research. As a case study, a practical example of forensic analysis is developed, involving the collection of data from the client's machine and a comprehensive analysis process. The chain-of-custody flow is detailed, and specific configurations of the customer's machine are examined to identify key findings. These findings are accompanied by practical recommendations and customized solutions for the customer, regardless of their technical level.

Finally, this paper concludes with a series of reflections based on the points developed, highlighting both the results obtained and possible improvements in the forensic analysis of Windows 11 systems.

Keywords: digital forensic analysis, Windows 11, evidence collection, chain of custody, computer security, regulations, investigative methodology, Ecuador, analysis tools.

TABLA DE CONTENIDOS (Índice)

RESUMEN 9
ABSTRACT 10
CAPÍTULO I: 18
Introducción 18
Planteamiento del problema 19
Objetivos 21
Objetivo general 21
Objetivo especifico 21
Justificación del proyecto 22
CAPÍTULO II: 23
Marco Teórico 23
Herramientas de Análisis Forense 24
Oracle VM VirtualBox 24
Forensic Toolkit (FTK) imager 24
Volatility 26
Reg Ripper 3.0 26
Autopsy 27
Recuva 27
Distribuciones 28
CAINE Linux – Digital Forensics Project 28
DEFT - Digital Evidence & Forensic Toolkit 29
Parrot OS 30
BlackArch 30
BackBox 31
Deft linux ..... **¡Error! Marcador no definido.**
Normativas de Análisis Forense 31
ISO 27037 31
UNE 71506 32

RFC 3227 33
SANS 34
Regulación de la Seguridad Informática en Ecuador 35
Código Orgánico Integral Penal (COIP) 35
Ley Orgánica de Protección de Datos Personales (LOPDP) 36
Regulación por el sector público y sector privado. 37
CAPÍTULO III 38
Metodología de investigación 38
Diagrama UML Framework 38
Desarrollo del Framework Forense en Windows 11 40
Comparar las características de seguridad y los desafíos en Windows 11 frente a versiones anteriores de Windows. 41
Elección de la versión para el desarrollo del framework. 42
Cadena de Custodia 43
Evaluación Preliminar 45
Caja Blanca 45
Caja Gris 46
Caja Negra 46
Metodología de adquisición de evidencia 47
Validación de la evidencia forense 47
Entorno de laboratorio forense 47
Limitaciones del análisis forense en Windows 11 47
Capítulo IV - Desarrollo de Pruebas 49
Laboratorio 1 49
Antecedentes: 49
Recopilación de Datos y Documentación de Evidencias 50
Análisis Forense de la Máquina del Cliente: Captura de Memoria y Almacenamiento 50
Cadena de Custodia entre Dispositivos: Asegurando la Integridad Forense 55
Herramientas Forenses Utilizadas 56
Desarrollo del laboratorio: 57

Identificar configuraciones en la máquina de Windows 11, Smartscreen, Windows Security, Windows Update, Servicios del sistema. 57
Identificar porque se dan los reinicios en Windows 11. 63
Identificar aplicaciones instaladas y análisis del navegador para ver el inicio. 73
Revisión de los procesos de la memoria RAM y usando capturas desde CMD en Windows para identificar problemas. 83
Revisión de la integridad y recuperación de datos usando una captura del almacenamiento del sistema: 95
Identificar virus instalado 101
Identificar Conexiones de la Red. 108
Esquema de laboratorio realizado: 128
Soluciones y mejoras al cliente: 130
Solución reinicios en Windows. 130
Problemas de Hardware 130
Controladores de Dispositivo Mal Funcionando 131
Software o Aplicaciones Conflictivas 131
Errores en el Registro del Sistema 132
Configuración Incorrecta de Energía 132
Error de Pantalla Azul (BSOD) 132
Actualización de BIOS 132
Diagnóstico y Solución 133
Solución al Análisis de la máquina recursos, cambio de navegador, activar protecciones. 135
Solución y entendimiento de los procesos que están actualmente en la memoria ram. 136
Solución presencia del malware en el equipo 137
Cómo los virus causan reinicios inesperados 137
Solución del almacenamiento en el equipo 142
Solución Antivirus en el equipo 144
CAPÍTULO V 147
CONCLUSIONES 147
Referencias ..... **¡Error! Marcador no definido.**
Apéndice A Entrevista 156

Apéndice B Solicitud de Análisis Forense..... 159
Apéndice C Detalles del Equipo: 160
Apéndice D Formulario adquisión de datos:..... 164

LISTA DE TABLAS (Índice de tablas)

Tabla 1 52
Tabla 2 54
Tabla 3 56
Tabla 4 81
Tabla 5 82
Tabla 6 101
Tabla 7 105
Tabla 8 109
Tabla 9 120

LISTA DE FIGURAS (Índice de figuras)

Figura 1 39
Figura 2 53
Figura 3 54
Figura 4 58
Figura 5 59
Figura 6 59
Figura 7 60
Figura 8 61
Figura 9 62
Figura 10 63
Figura 11 66
Figura 12 67
Figura 13 69
Figura 14 70
Figura 15 74
Figura 16 74
Figura 17 76
Figura 18 77
Figura 19 78
Figura 20 79
Figura 21 80
Figura 22 81
Figura 23 83

Figura 24.....84
Figura 25.....85
Figura 26.....86
Figura 27.....86
Figura 28.....87
Figura 29.....88
Figura 30.....89
Figura 31.....90
Figura 32.....91
Figura 33.....91
Figura 34.....91
Figura 35.....92
Figura 36.....92
Figura 37.....93
Figura 38.....93
Figura 39.....94
Figura 40.....94
Figura 41.....95
Figura 42.....96
Figura 43.....96
Figura 44.....97
Figura 45.....98
Figura 46.....98
Figura 47.....99
Figura 48.....102
Figura 49.....103
Figura 50.....104
Figura 51.....104
Figura 52.....104
Figura 53.....105
Figura 54.....106
Figura 55.....106
Figura 56.....107
Figura 57.....107
Figura 58.....108
Figura 59.....108
Figura 60.....109
Figura 61.....111
Figura 62.....112
Figura 63.....113

Figura 64 115
Figura 65 116
Figura 66 117
Figura 67 118
Figura 68 119
Figura 69 120
Figura 70 123
Figura 71 123
Figura 72 124
Figura 73 125
Figura 74 125
Figura 75 126
Figura 76 127
Figura 77 128
Figura 78 128
Figura 79 143
Figura 80 145

CAPÍTULO I:

Introducción

En la era digital actual, la ciberseguridad se ha convertido en un pilar fundamental, dada la alarmante escalada de ciberataques en computadoras personales, tanto de escritorio como laptops. De acuerdo con un informe de Check Point Research (2024), durante el primer semestre de 2024, varias organizaciones en Latinoamérica experimentaron un promedio de 1.636 ciberataques por semana, lo que representa un incremento del 53% en comparación con el año anterior.

Considerando que los ciberataques suelen dirigirse a dispositivos específicos, es crucial analizar el sistema operativo más utilizado. Según datos de Vanguardia (2024), Windows 11 ha alcanzado los 400 millones de usuarios a nivel mundial. Aunque no ha sido tan popular como versiones anteriores, su adopción en Ecuador ha sido significativa. Windows 11 se ha consolidado como una solución preferida tanto por individuos como por empresas que buscan un sistema operativo práctico y accesible para sus actividades cotidianas. Sin embargo, estas mismas actividades pueden desencadenar incidentes de seguridad que, si no se gestionan adecuadamente, pueden resultar en la pérdida de información crítica. Entre los principales riesgos asociados se encuentran la presencia de virus, fallos de fábrica, cortes de energía y el uso indebido de los equipos.

En respuesta a esta realidad, el presente estudio tiene como objetivo identificar, localizar, recuperar y presentar información comprometida, empleando una metodología avanzada y herramientas tecnológicas de vanguardia. Este enfoque permitirá demostrar cómo las técnicas forenses pueden aplicarse eficazmente en la recuperación de datos tras incidentes de ciberseguridad.

Según Gartner de Unitrends (2024), se estima que el 25% de los usuarios de computadoras personales sufren pérdida de datos cada año.

Por tanto, el desarrollo de este marco de trabajo para el análisis forense digital en Windows 11 busca no solo ofrecer una actualización de las herramientas, sino también mejorar el conocimiento forense alineado con las mejores prácticas de seguridad, siguiendo las pautas específicas del contexto ecuatoriano.

Planteamiento del Problema

En un contexto donde la digitalización avanza a un ritmo vertiginoso, la seguridad de los sistemas operativos empleados por individuos y empresas se convierte en una preocupación crítica. Windows 11, a pesar de no haber alcanzado la popularidad esperada en comparación con sus predecesores, ha ganado una base considerable de usuarios en todo el mundo, incluyendo un crecimiento notable en Ecuador. Este sistema operativo es valorado por su practicidad y accesibilidad, características que lo han convertido en una elección predominante para una amplia gama de usuarios. Sin embargo, estas ventajas no lo eximen de ser un objetivo frecuente para los ciberataques, que continúan aumentando tanto en frecuencia como en sofisticación.

Los ciberataques en Windows 11 plantean serios desafíos, especialmente debido a la naturaleza crítica de las actividades que los usuarios realizan en este entorno operativo. La pérdida de datos ya sea por la acción de virus, fallos de fábrica, cortes de energía o un uso indebido, es un riesgo omnipresente.

Las consecuencias de tales incidentes no solo afectan la integridad de la información, sino que también pueden tener un impacto significativo en la continuidad de las operaciones tanto de usuarios individuales como corporativos.

El problema central que aborda este estudio radica en la necesidad de desarrollar un marco de trabajo robusto y adaptado a las particularidades de Windows 11, que permita a los usuarios identificar, localizar, recuperar y presentar información comprometida de manera efectiva. Este marco debe estar alineado con las mejores prácticas internacionales, pero también adaptado al contexto ecuatoriano, para ofrecer una solución integral que mejore la respuesta ante incidentes de ciberseguridad en este entorno operativo.

Objetivos

Objetivo General

Desarrollar y aplicar un marco de trabajo para el análisis forense digital y la identificación de información en equipos con el sistema operativo Windows 11, con el propósito de identificar, preservar y analizar evidencia digital en casos de incidentes de seguridad.

Objetivo Específico

• Analizar las principales vulnerabilidades de seguridad en Windows 11.

• Implementar técnicas de recuperación de datos en sistemas Windows 11 afectados por incidentes de seguridad.

• Utilizar herramientas forenses para la identificación y preservación de evidencias digitales.

• Documentar el proceso de análisis forense, desde la identificación del incidente hasta la recuperación de datos.

• Revisar y aplicar la normativa legal vigente en Ecuador relacionada con la informática forense y la protección de datos.

• Desarrollar un protocolo de mejores prácticas para la preservación de evidencias y la seguridad de los datos.

Justificación del Proyecto

El sistema operativo Windows, desarrollado por Microsoft, ha sido una solución esencial para una amplia variedad de usuarios, desde pequeñas y medianas empresas hasta grandes corporaciones. Con una amplia base de usuarios, Windows ha destacado por su capacidad para gestionar tareas a través de numerosas aplicaciones preinstaladas y de terceros. En los últimos años, se ha observado un notable crecimiento en la preferencia por Windows en comparación con otros sistemas operativos, en gran parte debido a sus mejoras continuas en seguridad, actualizaciones regulares y optimización general.

Sin embargo, esta popularidad también atrae la atención de actores maliciosos que buscan explotar vulnerabilidades dentro del sistema. Estos ataques pueden provocar la pérdida de información crítica o incluso dejar los equipos completamente inutilizables debido a infecciones por virus. Ante este panorama, se hace crucial el desarrollo de técnicas avanzadas en informática forense que permitan recuperar datos y analizar incidentes de seguridad en sistemas Windows.

La viabilidad de este proyecto radica en la identificación y aplicación de técnicas de informática forense, con un enfoque en la recuperación de datos y la seguridad de la información. Además, el proyecto considerará la normativa legal vigente en Ecuador, garantizando el cumplimiento de las leyes y regulaciones aplicables en el manejo de datos y preservación de evidencias.

Finalmente, se abordarán las mejores prácticas para la identificación y conservación de datos en dispositivos que operan con el sistema operativo Windows, asegurando una respuesta efectiva ante incidentes de seguridad.

CAPÍTULO II:

Marco Teórico

El marco teórico de este estudio se fundamenta en la necesidad de comprender los principios fundamentales que rigen la ciberseguridad, con un enfoque específico en el análisis forense digital aplicado al sistema operativo Windows 11. Este sistema operativo, pese a ser relativamente nuevo en comparación con sus predecesores, ha demostrado ser tanto una herramienta versátil para los usuarios como un objetivo atractivo para los cibercriminales.

Para abordar el problema central de este trabajo, es esencial explorar y definir los conceptos clave relacionados con la ciberseguridad, como la naturaleza y evolución de los ciberataques, las vulnerabilidades inherentes a los sistemas operativos, y las metodologías forenses aplicables en escenarios de incidentes. Además, se analizarán las características específicas de Windows 11, incluyendo sus innovaciones en seguridad y las posibles debilidades que lo hacen susceptible a amenazas.

Otro aspecto crucial es la revisión de las herramientas forenses disponibles y su efectividad en la recuperación de datos comprometidos en incidentes de ciberseguridad. Esto incluye una evaluación de cómo estas herramientas han sido adaptadas o podrían ser mejoradas para alinearse con las mejores prácticas internacionales, así como su aplicabilidad en el contexto ecuatoriano.

Asimismo, el marco teórico abordará las mejores prácticas y normativas en seguridad informática, con un enfoque en cómo estos estándares pueden ser implementados eficazmente en el análisis forense digital.

Esta revisión permitirá establecer una base sólida para el desarrollo de un marco de trabajo que no solo responda a las necesidades técnicas, sino que también incorpore un enfoque contextualizado y práctico para el manejo de incidentes de ciberseguridad en Windows 11.

Herramientas de Análisis Forense

Oracle VM VirtualBox

VirtualBox es un software de virtualización desarrollado por Oracle Corporation, es una herramienta gratuita la cual se puede descargar desde su sitio web, permite la ejecución de múltiples máquinas virtuales con diferentes características, como S.O, capacidad de disco duro o memoria RAM. De esta forma, es posible ejecutar programas y funciones en dichas máquinas sin afectar a la máquina anfitrión. Una de las desventajas de VirtualBox es que no tiene soporte para 32 bits, además que puede ser un programa pesado de ejecutar. (Dash, 2013)

En cuanto a la emulación de hardware, los discos duros de los sistemas invitados son almacenados en los sistemas del anfitrión como archivos individuales en un contenedor llamado Virtual Disk Image, el cual no es compatible con otros softwares.

Forensic Toolkit (FTK) imager

FTK Imager es una herramienta de análisis e imagen forense diseñada para adquirir, crear imágenes forenses y realizar análisis detallados de varios tipos de medios digitales. Proporciona a los investigadores una interfaz fácil de usar, amplias capacidades y compatibilidad con diferentes sistemas operativos, lo que la convierte en una herramienta esencial para los profesionales en el campo. (Carvey, 2009)

Características de FTK Imager:

1.Imagen Forense:

- Imagen de disco: FTK Imager permite la creación de imágenes forenses de discos duros, unidades de estado sólido y otros medios de almacenamiento. Admite múltiples formatos de imagen, incluido el formato EnCase® Evidence (E01) ampliamente utilizado.
- Adquisición de RAM en vivo: Permite la adquisición y análisis de datos de memoria volátil (RAM) de sistemas en vivo, proporcionando información valiosa que podría no estar disponible a través de imágenes de disco tradicionales. (Carbone, 2014)

2.Análisis y Examen:

- Análisis de archivos: FTK Imager facilita el examen de archivos y carpetas dentro de imágenes forenses. Permite a los investigadores ver y extraer archivos individuales, incluidos archivos eliminados u ocultos, para un análisis en profundidad.
- Soporte de Formato de Archivo: La herramienta admite una amplia gama de formatos de archivo, lo que permite el examen de varios artefactos digitales, como documentos, imágenes, videos, correos electrónicos y archivos del sistema.
- Extracción de metadatos: FTK Imager puede extraer metadatos asociados con archivos, proporcionando información valiosa sobre la creación de archivos, marcas de tiempo de modificación, detalles del usuario y más. (Thethi, 2014)
- Búsqueda de palabras clave: Los investigadores pueden realizar búsquedas de palabras clave a través de la imagen forense, ayudando en la identificación de evidencia relevante o información específica.

3.Verificación y Validación:

- Hash Calculation: FTK Imager permite el cálculo y la verificación de valores hash (por ejemplo, MD5, SHA-1, SHA-256) para imágenes forenses, asegurando la integridad de los datos y apoyando la documentación de la cadena de custodia.
- Análisis de firmas: La herramienta incluye una función de análisis de firmas que ayuda a identificar tipos de archivos conocidos e identificar archivos potencialmente maliciosos o contenido sospechoso. (Binus, 2023)

Volatility

Volatility es un framework de código abierto y gratuito para el análisis forense de memoria volátil, principalmente la memoria RAM. Se utiliza para extraer y analizar datos de la memoria volátil, que se pierde al apagar el equipo. Entre sus versiones encotramos Volatility 2, compatible con Windows, Linux y macOS. Volatility 3 que se encuentra en desarrollo, con nuevas funcionalidades y mejoras en el rendimiento. (Volatility, 2024)

Reg Ripper 3.0

RegRipper es una herramienta comúnmente utilizada en investigaciones forenses para analizar el registro de Windows y obtener pistas relevantes sobre posibles actividades sospechosas en un sistema. Dispone de una gran variedad de plugins que permiten examinar diferentes aspectos del registro, como configuraciones de red, información de usuarios o parámetros de seguridad, entre otros. (KeepCoding, 2024)

Autopsy

Autopsy, es un software que se utiliza para el análisis forense de imágenes de discos duros, es una herramienta que funciona en diferentes sistemas operativos, como:

Linux, Window, Mac OSx y Free BSD. (Guzmán J. , 2016)

Posee funcionalidades como:

- Análisis de la línea de tiempo - Interfaz de visualización de eventos gráficos avanzada (video tutorial incluido).
- Hash Filtering – Flag conocidos como archivos malos e ignorar el bien conocido.
- Keyword Search - Búsqueda clave indexada para encontrar archivos que mencionen los términos relevantes.
- Artificios Web - Extraer historia, marcadores y cookies de Firefox, Chrome e IE.
- Data Carving - Recuperar archivos borrados del espacio no asignado usando PhotoRec
- Multimedia - Extrae EXIF de imágenes y ver vídeos.
- Escaneo de malware (Carrier, 2024)

Recuva

Recuva es una herramienta de recuperación de archivos diseñada para sistemas operativos Windows. Esta aplicación se ha consolidado como una solución popular y accesible para la recuperación de archivos eliminados, tanto desde unidades internas como externas. La versión más reciente, 1.54.26, fue lanzada el 26 de junio de este año. (Al Sharif, 2014)

El funcionamiento de Recuva se basa en el análisis de la Tabla Maestro de Archivos (MFT, por sus siglas en inglés). Cuando Recuva detecta un registro marcado como "eliminado", puede localizar el espacio vacío en el disco donde se encontraba el archivo original y recuperar la información contenida en ese espacio. Sin embargo, es importante destacar que, aunque los datos pueden parecer eliminados, siguen presentes en el disco hasta que se sobrescriben con nuevos datos (Lazaridis, 2016)

Para maximizar la posibilidad de recuperación de archivos, es crucial utilizar Recuva lo antes posible después de la eliminación del archivo. En casos donde los archivos han sido eliminados hace un tiempo, se recomienda realizar un escaneo profundo. Este proceso implica examinar más exhaustivamente la MFT y otros sectores del disco para recuperar archivos que podrían haber sido fragmentados o que han estado expuestos a la escritura de nuevos datos. La eficacia de la recuperación puede verse afectada por factores como el tiempo transcurrido desde la eliminación, el tipo de sistema de archivos y el grado de fragmentación del archivo. (Kamble, 2015)

Distribuciones

CAINE Linux – Digital Forensics Project

Computer Aided Investigative Environment (CAINE) es una distribución de Linux basada en Ubuntu, especializada en el análisis forense digital. Diseñada para identificar y restaurar datos ocultos, dañados o eliminados de discos duros, CAINE está construida sobre una arquitectura x86_64 y tiene su origen en Italia. (Rueda-Rueda, 2019)

CAINE incluye una variedad de herramientas útiles para el proceso forense, organizadas en diferentes niveles:

- **Nivel de Red:**
    - **Wireshark:** Herramienta esencial para capturar y analizar paquetes de datos que circulan por la red configurada. (Chappell, 2012)
- **Nivel de Aplicación:**
    - **Autopsy:** Interfaz gráfica para realizar análisis forense digital.
    - **BitLocker:** Permite el acceso a particiones cifradas con el software de Microsoft.
- **Nivel de Disco/Archivo:**
    - **TestDisk y PhotoRec:** Herramientas para recuperar datos borrados o inaccesibles.

Además de estas herramientas preinstaladas, CAINE es altamente personalizable, permitiendo la adición de nuevas herramientas según las necesidades del usuario. Para prevenir operaciones accidentales de escritura en disco, CAINE está configurado para montar todos los dispositivos en modo de solo lectura. Si se necesita modificar esta configuración para permitir la escritura, se debe ajustar la configuración del sistema de CAINE adecuadamente. (Decusatis, 2015)

DEFT - Digital Evidence & Forensic Toolkit

Es una distribución personalizada de Linux basada en Lubuntu, diseñada específicamente para el análisis forense digital. La versión más reciente y estable de esta herramienta es la 8.2, lanzada en 2017, originaria de la Universidad de Bolonia en Italia, DEFT se basa en una arquitectura i686 y fue publicada por primera vez en 2005. A pesar de los años transcurridos desde su lanzamiento y múltiples actualizaciones, sigue siendo una solución relevante en la actualidad. (Parasram, 2020)

DEFT es mantenida activamente por la comunidad de usuarios y permite la incorporación de diversas herramientas adicionales. Entre las funcionalidades destacadas de DEFT se incluyen la

adquisición de imágenes forenses, la verificación de la integridad de archivos, el análisis de malware, la recuperación de información y la gestión de discos duros. (Grubor, 2013)

Parrot OS

Parrot es una distribución de GNU/Linux basada en Debian, diseñada para proporcionar soluciones de seguridad tanto para expertos en el área como para usuarios comunes que buscan mayor privacidad. Desde su lanzamiento en 2013, Parrot ha evolucionado significativamente, incorporando un amplio arsenal de herramientas para operaciones forenses digitales. (ul Hassan, 2021)

Parrot OS está optimizada para un uso eficiente de los recursos, enfocándose en la comodidad del usuario. Además, cuenta con comunidades activas en Facebook y Telegram que ofrecen soporte a los usuarios que enfrentan problemas o dudas. (Qureshi, 2022)

Parrot OS se distingue por su capacidad para equilibrar la seguridad, la privacidad y la facilidad de uso, ofreciendo soporte integral tanto para profesionales como para usuarios interesados en mejorar su privacidad en línea. (Reddy, 2019)

BlackArch

Es una distribución de Linux basada en Arch, orientada a profesionales interesados en pruebas de penetración, análisis forense digital y auditoría de seguridad. Lanzada por primera vez en 2012, su última actualización se realizó en 2023, con una versión Slim ISO que tiene un tamaño de 5.5 GB. (Dieguez Castro J. , 2016)

BlackArch se destaca por su extensa colección de herramientas, con un total de 2,597 herramientas disponibles que cubren una amplia gama de operaciones esenciales para identificar y recuperar datos en otros sistemas. (Cisar, 2019)

Algunas de las herramientas más utilizadas incluyen:

- **Nmap:** Permite escanear redes y descubrir información detallada sobre los dispositivos conectados.
- **Hydra:** Una herramienta de cracking de contraseñas que soporta varios protocolos y servicios, utilizada para ataques de diccionario y fuerza bruta.

BlackArch es una opción robusta tanto para profesionales experimentados como para aquellos que están comenzando en el campo de la seguridad informática. Su proceso de instalación es relativamente intuitivo, lo que facilita su implementación y uso en diversas operaciones de seguridad. (Dieguez Castro J. , 2016)

BackBox

Es una distribución de Linux basada en Ubuntu destinada a pruebas de penetración y evaluación de seguridad. Establece un conjunto de herramientas para analizar redes y sistemas informáticos, comprendiendo un conjunto completo de herramientas necesarias para la piratería ética y las pruebas de seguridad. Entre los detalles más importantes sobre BackBox se puede mencionar los siguientes: se centra en pruebas de penetración y evaluación de seguridad y entre sus principales herramientas incluye un conjunto completo de herramientas para piratería ética y pruebas de seguridad. (Uygur, 2014)

Normativas de Análisis Forense

ISO 27037

La normativa ISO 27037:2012 es ampliamente acogida y aplicada por peritos informáticos basando su utilidad en los lineamientos y preceptos que rigen el correcto proceso de obtención y

tratamiento de evidencias digitales. Sobre esta normativa se puede mencionar que constituye una revisión y mejoramiento sobre lineamientos anteriores como puede ser el RFC 3227, sin embargo, al ser una normativa que tiene como una de sus particularidades el estar fundamentada sobre normativas similares plantea un marco de trabajo optimizado y enfocado en el tratamiento de la evidencia en su forma de ser recolectada. (Didik, 2019)

Es necesario resaltar que el marco de trabajo de la normativa ISO 27037:2012 comprende principios sobre los cuales se hace énfasis en realizar un correcto procedimiento de obtención de evidencia y pruebas digitales primando la integridad de la información para preservarla tal como se presentó en el momento de la recolección. Se hace necesario resaltar énfasis también que los procesos de recolección de información están comprendidos en base a buenas prácticas profesionales, a fin de hacer que este proceso sea reproducible y que las utilidades o herramientas que sean empleadas deben ser parte de un conjunto de herramientas validadas y que permitan establecer un contraste sobres herramientas similares para procesos de obtención de información. (Ramadhan, 2022)

UNE 71506

La normativa UNE 71506/2013 menciona entre sus principios la definición de un proceso de análisis forense, conformada de fases hace que el enfoque se centre en resaltar la inviolabilidad de las muestras de recolección original. Este primer concepto hace que los peritos forenses manejen un estándar adecuado para la recolección de evidencias ya que toma en cuenta factores físicos al momento de la obtención de información. (Cajo, 2018)

Es importante mencionar también aspectos técnicos con respecto a la recolección de información como es la toma de muestra a bajo nivel para preservar la originalidad y completitud de la

muestra, tomando también en cuenta el estado del equipo o medio de información ya que un estado activo del equipo a analizar podría afectar la muestra.

La documentación bajo esta normativa es clave ya que nos permite establecer una secuencia temporal sobre los hechos que generaron el análisis forense, de esta manera se registraran todas las acciones llevadas a cabo durante el proceso de análisis, es así que se maneja la cadena de custodia sobre la información. (Coronel-Rojas, 2020)

El análisis es fundamental ya que da respuestas a partir del incidente reportado, esto quiere decir que durante esta fase el analista debe centrarse en: recuperación de evidencias borradas, estudio técnico del estado físico y lógico del medio de información. Finalmente se genera un documento de presentación de resultados o informe pericial sobre el análisis forense. (Cajo, 2018)

RFC 3227

Al igual que las anteriores normativas revisadas, RFC 3227 agrupa lineamientos que permitan establecer procedimiento y estándares que dirijan el análisis forense de tal manera que permitan evidenciar los incidentes de seguridad, sus causas y afectaciones. (Zhao, 2009)

Entre los principios fundamentales se encuentra la captura de imágenes o muestra forense base con la mayor precisión sobre el sistema afectado, evitar cambios sobre la información de la muestra. Existe dentro de la normativa consideraciones sobre el estado del software que interactué con la muestra considerando que se debe evitar fuentes que hayan sido comprometidos o información que sea proporcionado por software que pueda haberse visto comprometido durante las acciones que llevaron al análisis forense. (Forte, 2008)

SANS

El término SANS se refiere al **SysAdmin, Audit, Networking, and Security** Institute, una de las organizaciones más reconocidas a nivel mundial en la formación y certificación en ciberseguridad. Fundada en 1989, el SANS Institute se ha dedicado a desarrollar programas de capacitación y certificación que abordan las necesidades críticas de seguridad informática en una variedad de contextos (Institute, About SANS, 2021). A través de sus cursos y eventos, SANS busca proporcionar habilidades prácticas y conocimientos teóricos que son esenciales para la defensa contra amenazas cibernéticas.

SANS organiza diversas conferencias internacionales, donde se presentan nuevas investigaciones, técnicas y herramientas en el ámbito de la seguridad. Uno de los enfoques más destacados de la organización es la formación en respuesta a incidentes, análisis forense y gestión de vulnerabilidades. Esto permite a los profesionales de seguridad adaptarse rápidamente a un entorno que evoluciona constantemente en términos de amenazas y tecnologías.

Además, el SANS Institute también es responsable de la creación de la Community of Security Professionals (CSP), que promueve la colaboración y el intercambio de información entre los expertos en ciberseguridad. Sus certificaciones, como GIAC (Global Information Assurance Certification), son ampliamente reconocidas en la industria, proporcionando una validación confiable de las competencias de los profesionales (GIAC, 2021).

En resumen, el SANS Institute juega un papel crucial en el fortalecimiento de las capacidades de ciberseguridad a nivel mundial, ofreciendo educación de alta calidad y fomentando una comunidad profesional activa y comprometida con la protección de los sistemas informáticos.

Regulación de la Seguridad Informática en Ecuador

Código Orgánico Integral Penal (COIP)

El Código Orgánico Integral Penal (COIP) de Ecuador, en vigor desde 2014, marca un hito en la legislación penal del país, incluyendo disposiciones específicas relacionadas con la seguridad informática. En un contexto global donde la digitalización ha transformado la forma de interacción social y económica, el COIP se presenta como un instrumento clave para abordar los delitos cibernéticos, garantizando la protección de los derechos de los ciudadanos y la seguridad de la información.

El COIP establece diferentes tipos penales asociados a los delitos informáticos, como el acceso no autorizado a sistemas informáticos, la interceptación de datos y el uso indebido de dispositivos o tecnologías para el fraude. Estas normativas no solo tipifican las conductas delictivas, sino que también imponen sanciones severas, promoviendo así un entorno de mayor seguridad en el uso de tecnologías de la información (Ecuador A. N., Código Orgánico Integral Penal (COIP). Registro Oficial No. 180, 2014).

La normativa busca fomentar la responsabilidad penal de los infractores y utilizar herramientas legales que permitan a las autoridades perseguir y sancionar eficazmente los delitos cibernéticos. Este marco legal es fundamental, ya que refuerza la confianza de los usuarios en el uso de plataformas digitales y en la gestión de su información personal (Ambato, 2018).

Además, el COIP establece la cooperación entre entidades del Estado, como la Policía Nacional y la Fiscalía, para la prevención y combate del ciberdelito. Esta colaboración es crucial para la implementación de estrategias efectivas que fortalezcan la seguridad informática en el país (Estado, 2015).

En resumen, el COIP se erige como un fundamento pilar en la regulación de la seguridad informática en Ecuador, adaptándose a las exigencias de una sociedad cada vez más interconectada y digitalizada.

Ley Orgánica de Protección de Datos Personales (LOPDP)

La Ley Orgánica de Protección de Datos Personales (LOPDP), promulgada en 2021 en Ecuador, establece un marco normativo esencial para la protección de datos personales, enfocándose en la regulación de la seguridad informática. En un mundo digital donde la información circula de forma vertiginosa, la LOPDP no solo busca proteger los derechos de los titulares de datos, sino también garantizar la seguridad de la información ante amenazas cibernéticas (Ecuador A. N., Ley Orgánica de Protección de Datos Personales, 2021).

La ley se articula en torno a principios fundamentales como la legalidad, la seguridad y la responsabilidad proactiva, obligando a las entidades a implementar medidas de seguridad adecuadas para proteger los datos personales que manejan. Estas medidas deben abarcar tanto aspectos técnicos como organizativos, asegurando que se adopten prácticas de seguridad informática que minimicen el riesgo de accesos no autorizados, pérdida o divulgación de datos (Law, 2021).

Uno de los pilares de la LOPDP es el establecimiento de sanciones para aquellas instituciones que no cumplan con las normativas de seguridad, lo que subraya la seriedad con la que se aborda la protección de datos en el contexto digital. Adicionalmente, la creación de la Agencia de Protección de Datos permite supervisar a las entidades y asegurar que las buenas prácticas de seguridad se implementen de manera efectiva, promoviendo una cultura de respeto y cuidado hacia la información personal (Ecuador L. , 2023).

En conclusión, la LOPDP no solo contribuye a la protección de la privacidad de los ciudadanos, sino que también establece un robusto marco de regulación para la seguridad informática en Ecuador, combinando la protección de datos con la necesidad imperiosa de salvaguardar la integridad de la información en un entorno interconectado.

Regulación por el Sector público y Sector Privado.

La regulación de la seguridad informática en Ecuador se ha convertido en una prioridad tanto para el sector público como para el privado, dados los crecientes riesgos asociados a la digitalización y la proliferación de delitos cibernéticos. La Ley de Protección de Datos Personales, el Código Orgánico Integral Penal (COIP) y diversas normativas sectoriales constituyen el marco regulador que establece las directrices y principios que deben seguir las entidades tanto del sector público como privado.

El sector público, a través de entidades como la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y el Ministerio de Telecomunicaciones, ha implementado políticas y marcos normativos que buscan asegurar un manejo responsable de la información y la infraestructura tecnológica. Estas instituciones fomentan la adopción de estándares de seguridad y la capacitación del personal en materia de ciberseguridad, a fin de prevenir incidentes de seguridad que puedan comprometer datos sensibles (Telecomunicaciones, 2021).

Por otro lado, el sector privado también enfrenta la imperiosa necesidad de establecer medidas de seguridad robustas. La regulación exige que las empresas implementen estrategias de gestión de riesgos y planes de contingencia que garanticen la protección de la información que manejan. Las normativas aplicables, como la Ley Orgánica de Protección de Datos Personales, demandan a las

empresas adoptar buenas prácticas en el tratamiento de datos, incluyendo la notificación de brechas de seguridad y la implementación de controles técnicos y organizativos efectivos (González J. , 2022).

La colaboración entre ambos sectores es crucial para enfrentar las amenazas cibernéticas de manera efectiva. La creación de espacios de cooperación y el intercambio de información sobre amenazas emergentes y vulnerabilidades son esenciales para fortalecer la seguridad informática en el país (Sierra, 2022).

CAPÍTULO III

Metodología de Investigación

Diagrama UML Framework

Este framework se fundamenta en las buenas prácticas del RFC 3227. El diagrama muestra una estrategia de trabajo de análisis forense con cinco fases principales:

Evaluación Preliminar: Identifica requisitos y define el tipo de análisis (Caja Negra, Gris o Blanca).

Extracción de Evidencias: Realiza extracción de memoria RAM y disco, con análisis adicional si hay problemas.

Extracción de Tráfico de Red: Captura tráfico de red si es viable.

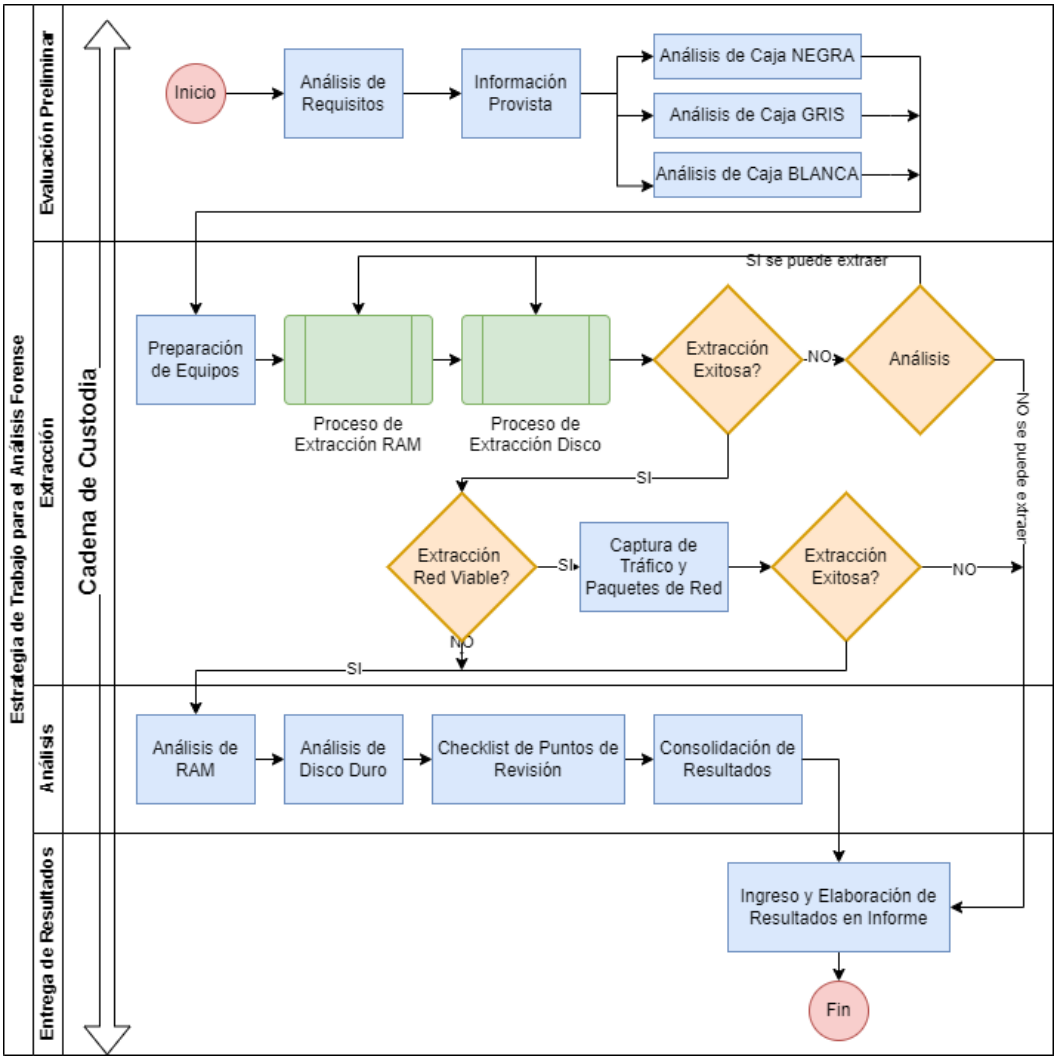
Análisis: Analiza RAM, disco duro y checklist revisión, consolidando los resultados.

Entrega de Resultados: Documenta los hallazgos en un informe.

Durante todo el proceso, se mantiene la cadena de custodia para asegurar la integridad de las evidencias.

Figura 1

Imagen de Diagrama UML Framework



Nota: El diagrama de flujo presenta una estrategia de trabajo para el análisis forense, estructurada en cuatro fases: *Evaluación Preliminar*, *Extracción*, *Análisis* y *Entrega de Resultados*. Detalla procesos clave como la preparación de equipos, extracción de datos (RAM, disco y red), análisis mediante métodos de Caja Negra, Caja Gris y Caja Blanca, así como la consolidación de resultados. Además, incluye puntos de decisión para manejar casos de extracción fallida y asegurar la rigurosidad metodológica en cada etapa.

Desarrollo del Framework Forense en Windows 11

El framework propuesto en este trabajo establece una estructura clara y comprensible que facilita el análisis forense digital en entornos Windows 11. Este enfoque permite desglosar de manera sistemática cada una de las etapas críticas del proceso forense, como la identificación, recuperación y análisis de evidencia digital, garantizando que cada paso se ejecute de forma organizada y coherente, conforme a los estándares establecidos.

Comparar las Características de Seguridad y los Desafíos en Windows 11 frente a Versiones Anteriores de Windows.

Windows 11 incorpora mejoras significativas en seguridad en comparación con versiones previas como Windows 10 y Windows 7, adaptándose a un entorno de ciberseguridad moderno que busca protegerse contra amenazas avanzadas. Algunas de las características clave que diferencian a Windows 11 de sus predecesores incluyen: (Arthur, 2015)

Requerimientos de hardware más estrictos: Windows 11 exige el uso de módulos de seguridad TPM 2.0 (Trusted Platform Module), lo que asegura un entorno más confiable para almacenar claves de cifrado y manejar operaciones criptográficas. Esto aumenta la protección de la información sensible y de los datos en el sistema. (Arthur, 2015)

Arranque seguro y UEFI: El arranque seguro, junto con la arquitectura UEFI (Unified Extensible Firmware Interface), protege el sistema contra malware que intenta modificar el proceso de inicio. Esta protección contra amenazas de bajo nivel proporciona una capa adicional de seguridad desde el arranque. (Jeong, 2019)

Virtualización basada en seguridad (VBS): Windows 11 emplea VBS para crear un entorno seguro y aislado en el que se ejecutan funciones críticas del sistema. Esto es especialmente útil para reducir el

impacto de ataques dirigidos a la memoria y evitar la manipulación de procesos fundamentales del sistema.

Control de aplicaciones de Windows Defender: Con Windows Defender Application Control (WDAC), Windows 11 refuerza la política de permitir solo aplicaciones de confianza, reduciendo la posibilidad de que software malicioso se ejecute en el sistema.

Protección contra vulnerabilidades: La función Windows Defender Exploit Guard se mejora en Windows 11 para ofrecer un mejor control sobre la protección frente a ataques de exploits. Esto permite monitorear y restringir los tipos de aplicaciones y scripts que pueden ejecutarse, previniendo amenazas comunes de ingeniería social y ataques de día cero. (Halsey, 2022)

Sin embargo, estos avances también presentan desafíos en el análisis forense. Windows 11 implementa sistemas de encriptación de datos y mecanismos de seguridad que dificultan la extracción de evidencia sin comprometer su integridad. Las características avanzadas de seguridad también implican que muchas actividades y procesos clave se ejecuten en entornos aislados, lo cual requiere herramientas específicas para acceder a áreas protegidas de la memoria y el disco.

Elección de la Versión Para el Desarrollo del Framework.

La elección de Windows 11 como plataforma para el desarrollo del framework forense responde a varias razones clave:

1. **Relevancia en entornos empresariales**: Windows 11 ha comenzado a ser adoptado rápidamente en entornos empresariales debido a su enfoque en la seguridad y compatibilidad con herramientas de productividad modernas. Esto hace que sea esencial desarrollar

metodologías que permitan realizar análisis forenses en este sistema operativo, ya que las empresas necesitan estar preparadas para responder a incidentes de seguridad en su infraestructura actualizada.

2. **Compatibilidad con herramientas modernas de análisis**: Windows 11 es compatible con las últimas versiones de herramientas de análisis forense, como Volatility, FTK Imager, y Autopsy, y con tecnologías avanzadas como el TPM. Esto permite que el framework se construya sobre tecnologías compatibles con el análisis forense de última generación, optimizando el proceso de identificación y recuperación de evidencia.
3. **Mejoras en seguridad y desafíos forenses**: Las características avanzadas de seguridad de Windows 11 presentan desafíos y oportunidades únicas en el análisis forense, permitiendo que el framework proponga técnicas específicas para superar obstáculos como el acceso a entornos protegidos. Windows 11 exige enfoques actualizados para gestionar datos encriptados y procesar información en entornos de virtualización segura, lo que enriquece el proceso de investigación y permite documentar soluciones avanzadas.
4. **Preparación para el futuro**: Al centrarse en Windows 11, el framework se prepara para una larga vigencia, dada la permanencia esperada de este sistema operativo en los entornos de trabajo. Windows 11 representa una evolución significativa en seguridad y manejo de procesos, lo cual hace que su elección asegure una metodología actualizada y adaptable para los próximos años. (Shaaban, 2016)

Cadena de Custodia

La cadena de custodia es un componente esencial en cualquier análisis forense, ya que garantiza la integridad y el control de la evidencia desde su descubrimiento hasta su presentación en instancias

legales. Es fundamental que este proceso cumpla con las normativas legales vigentes. En casos donde los dispositivos comprometidos provengan de diferentes jurisdicciones, se debe tener en cuenta la legislación aplicable de cada país. Para el contexto de este trabajo, la cadena de custodia se ajustará a las normativas legales de Ecuador. (Arellano, 2012)

- **Identificación y Recolección de la Evidencia**: El primer paso es identificar la evidencia clave, detallando la fecha, el lugar y los dispositivos comprometidos. Es necesario registrar los nombres de los profesionales responsables de la recolección inicial, así como describir el estado de los dispositivos y el método de recolección utilizado, prestando especial atención a evitar la pérdida de datos volátiles.

- **Etiquetado y Documentación**: El etiquetado adecuado de la evidencia es crucial para garantizar su trazabilidad. Se recomienda seguir un estándar, como "Evidencia A-001-2024_01_01", que refleje profesionalismo y organización. Además, es vital documentar cada paso del proceso de forma clara y precisa, facilitando la comprensión de lo realizado.

- **Transporte de la Evidencia**: El transporte de la evidencia debe cumplir con estrictos procedimientos de seguridad, utilizando contenedores sellados y bolsas de Faraday para proteger los dispositivos de cualquier fuente de energía que pueda alterar su contenido. También se debe registrar quién fue el responsable del transporte, la ruta seguida, así como la hora de entrega y recepción de la evidencia. (Bórquez, 2011)

- **Almacenamiento y Preservación**: La evidencia debe ser almacenada en un gabinete seguro, dentro de una infraestructura física controlada, con acceso limitado solo a personal autorizado.

El uso de controles biométricos para asegurar el acceso restringido garantiza la preservación de los datos.

- **Análisis Forense**: Es esencial planificar el análisis forense, detallando la fecha, el responsable del análisis y las herramientas utilizadas. Se debe trabajar siempre con copias de la evidencia, preservando intactos los originales.
- **Transferencia y Custodia Posterior**: Una vez finalizado el análisis forense, es crucial documentar detalladamente la transferencia de la evidencia a las autoridades correspondientes. Esto incluye la entrega del contenedor sellado y los informes del análisis realizado, asegurando la integridad y protección de la evidencia.

Evaluación Preliminar

Es fundamental tener presente que hay tres categorías de análisis que se deben llevar a cabo: caja blanca, caja gris y caja negra.

Caja Blanca

El análisis de caja blanca se utiliza cuando se tiene acceso completo y detallado al sistema investigado. Este enfoque es ideal en escenarios donde el objetivo es analizar el comportamiento interno del sistema, incluyendo el código fuente, configuraciones del sistema, y artefactos críticos como el registro de Windows, los procesos en ejecución, y los controladores.

Se aplica especialmente cuando se requiere identificar actividad sospechosa o maliciosa a nivel profundo, rastrear cambios en la integridad del sistema, detectar malware sofisticado, o realizar una auditoría completa de los logs y artefactos del sistema. Dado que Windows 11 incorpora nuevas capas de seguridad (TPM 2.0, arranque seguro, BitLocker), el análisis de caja blanca permite evaluar cómo

estos mecanismos impactan la evidencia forense y cómo los atacantes podrían haber interactuado con el sistema a nivel interno. (Bonetti, 2013)

Caja Gris

El análisis de Caja Gris se utiliza cuando el cliente proporciona información parcial o limitada sobre el equipo o sistema a analizar. Esta información suele ser insuficiente tanto a nivel de hardware como de software. En muchos casos, el cliente no es un experto en tecnología, por lo que solo puede ofrecer detalles básicos.

El equipo forense debe recolectar y consolidar toda la información disponible, incluso si es fragmentada, para aprovechar al máximo cada dato en el proceso de análisis, ya que cualquier detalle puede ser clave para la investigación forense. (Grispos, 2021)

Caja Negra

El enfoque de caja negra en análisis forense implica investigar un sistema o dispositivo sin acceso a su estructura interna o a detalles de implementación, limitándose a examinar su entrada y salida de datos, tal como lo haría un atacante externo. Este método es ideal cuando no se dispone del código fuente o cuando es fundamental preservar la integridad de las pruebas, ya que permite analizar el comportamiento y actividad del sistema sin modificaciones. En la práctica forense, se utilizan técnicas como el monitoreo de tráfico y registros, el análisis de comportamiento y la detección de actividad en la red, lo que permite identificar patrones anómalos o sospechosos. Asimismo, el análisis de archivos binarios y ejecutables puede revelar acciones maliciosas sin necesidad de revisar el código. Este enfoque, además de proteger el entorno investigado, ofrece una perspectiva objetiva y controlada del sistema,

simulando el acceso de un atacante y facilitando la identificación de posibles vulnerabilidades externas. (McDonald, 2008)

Metodología de Adquisición de Evidencia

Explicar diferentes métodos de adquisición, como adquisición en vivo o post-mortem (después de apagar el sistema).

Herramientas usadas en el proceso de adquisición y su justificación, como FTK Imager o dd.

Validación de la Evidencia Forense

Incluir cómo se asegura la integridad de la evidencia digital utilizando hashes (SHA-256, MD5, etc.).

Justificación del uso de múltiples hashes y su importancia en la cadena de custodia.

Entorno de Laboratorio Forense

Detallar la configuración del entorno de laboratorio, incluyendo hardware y software utilizados, como Parrot OS, Autopsy, y Volatility.

Medidas de seguridad implementadas en el laboratorio para garantizar la no alteración de la evidencia.

Limitaciones del Análisis Forense en Windows 11

Identificar las limitaciones que pueden surgir durante el análisis, como cifrado de disco o tecnologías de seguridad avanzadas (TPM, Secure Boot).

Capítulo IV - Desarrollo de Pruebas

En el ámbito del análisis forense digital, el desarrollo de un laboratorio en las pruebas juega un papel fundamental para validar la efectividad de herramientas y técnicas utilizadas en la investigación. Estos entornos controlados permiten simular diversos escenarios, desde fallos de rendimiento hasta incidentes de seguridad, garantizando la fiabilidad y precisión de los métodos propuestos en nuestro framework forense. Además de servir como espacios para replicar y analizar posibles delitos cibernéticos, estos laboratorios son esenciales para asegurar que los procedimientos empleados cumplen con los más altos estándares de integridad y exactitud en el manejo de la evidencia digital.

Laboratorio 1

Antecedentes:

Un cliente se comunica con profesionales forenses en busca de una solución a problemas críticos que ha detectado en su equipo. Nos informa que ha estado experimentando una degradación significativa en el rendimiento, acompañada de reinicios inesperados que interrumpen sus tareas diarias. El cliente, entusiasta de las inversiones digitales, menciona que ha instalado varias aplicaciones recientemente, las cuales parecen estar afectando el rendimiento del sistema, generando lentitud y afectando su productividad.

Su principal preocupación es la estabilidad del hardware, ya que también ha notado sobrecalentamientos frecuentes, lo que le hace temer por una posible falla catastrófica que podría resultar en la pérdida de datos almacenados en su disco duro. Además, está profundamente inquieto por la seguridad de su información, considerando el riesgo de que malware haya podido infiltrarse en su equipo.

Para abordar estos problemas, se propone realizar un análisis de análisis de caja blanca permite una inspección detallada del sistema, ya que se tiene acceso completo al código fuente, configuraciones, y arquitectura interna del equipo. También se podrían ejecutar escaneos de seguridad profundos en busca de malware que podría estar oculto en el sistema, verificando la integridad de archivos críticos y analizando el comportamiento de las aplicaciones en ejecución.

Recopilación de Datos y Documentación de Evidencias

Para llevar a cabo la recopilación de datos forenses en la máquina del cliente, se han seguido procedimientos estándares que incluyen la obtención de información clave mediante entrevistas, documentos proporcionados por el cliente, detalles técnicos de la máquina y una hoja de trabajo de adquisición de datos. Estos elementos se detallan a continuación y se incluyen en los anexos correspondientes para una mayor claridad y documentación adecuada.

a. "Se realizó una entrevista con el cliente para obtener información relevante sobre el sistema y su entorno (ver Anexo A)."

b. "El cliente proporcionó una solicitud del análisis forense, el cuales se detallan en el Anexo B."

c. "Se documentaron los detalles técnicos de la máquina del cliente, como se describe en el Anexo C."

d. "Se completó una hoja de trabajo para la adquisición de datos, la cual está disponible en el Anexo D."

Análisis Forense de la Máquina del Cliente: Captura de Memoria y Almacenamiento

Con el fin de realizar un análisis forense detallado, se llevará a cabo una investigación utilizando la máquina del cliente. Este proceso incluye tanto análisis estático como dinámico de los datos

extraídos. Como parte de la recolección de evidencias, se ha procedido a capturar la memoria RAM y realizar una copia de seguridad del almacenamiento interno del cliente. A continuación, se describen los detalles técnicos y las herramientas utilizadas para esta tarea, asegurando la integridad de los datos mediante la generación de los correspondientes hashes.

Análisis del detalle de la memoria RAM:

Tabla 1

Datos a detalle Memoria RAM

	RAM (Random Access Memory)
Tecnología	DDDR5
Fecha	2024-10-19
Peso	8GB
Extensión	.mem
MD5	B2E8CE0162FC91F8FBA805AA5B1D3329
SHA-1	76E898FD89B2C34BD517F0852191318A37222BF4
Herramienta	AccessData® FTK® Imager 4.7.1.2

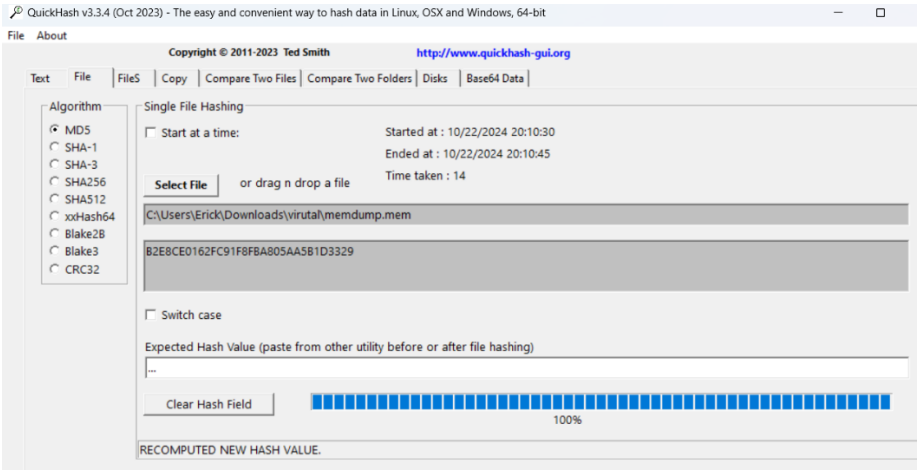
Nota: Esta tabla muestra el detalle de la extraccion de la memoria Ram.

Recolección de usando la herramienta de quickhash v3.3.4:

MD5:

Figura 2

Imagen de la revisión del Algoritmo MD5 de la memoria RAM en QuickHash

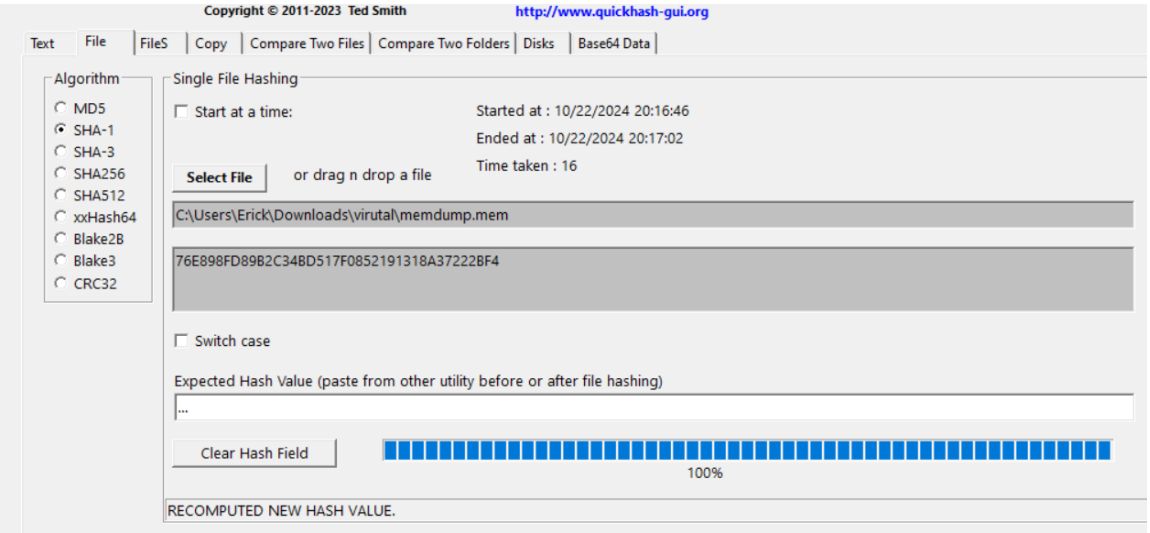


Nota: La imagen muestra el uso de la herramienta QuickHash v3.3.4 para el cálculo del hash MD5 de un archivo de memoria denominado "memdump.mem". Se empleó el algoritmo xxHash64 para generar el valor hash único, asegurando la integridad del archivo durante el análisis forense.

SHA-1:

Figura 3

Imagen de la revisión del Algoritmo SHA-1 de la memoria RAM en QuickHash



Nota: La imagen muestra el uso de la herramienta QuickHash v3.3.4 para el cálculo del hash sha-1 de un archivo de memoria denominado "memdump.mem".

Análisis del almacenamiento interno:

Tabla 2

Datos a detalle Almacenamiento Interno

	Almacenamiento Interno
Tecnología:	SSD
Fecha:	2024-10-19
Peso:	80 GB
Extensión:	.rar
MD5:	6b50f72e023b5b49f3fb016015cb88a8

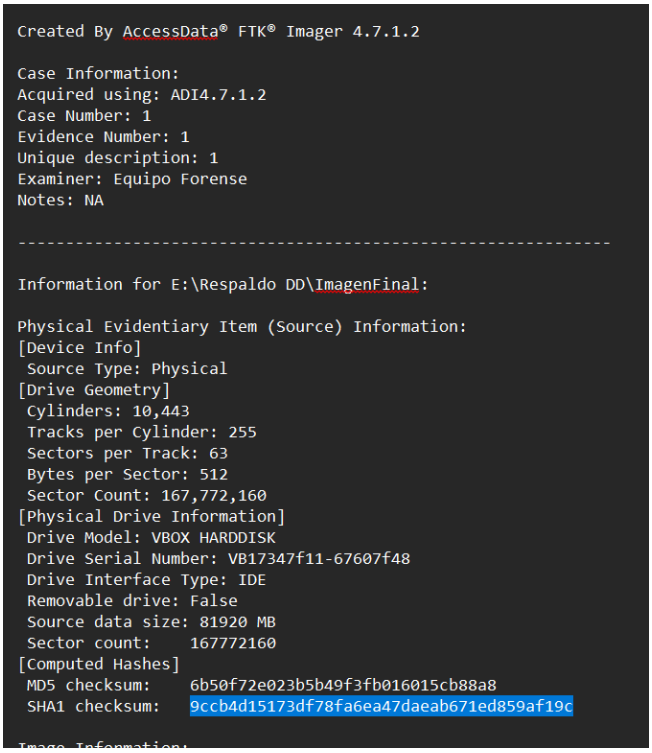
SHA-1:	9ccb4d15173df78fa6ea47daeab671ed859af19c
Herramienta:	AccessData® FTK® Imager 4.7.1.2

Nota: Esta tabla muestra el detalle de la extraccion Almacenamiento Interno.

Información sobre el archivo que se ha generado desde FTK Imager.

Figura 4

Archivo Generado sobre el disco clonado usando FTK Imager



Nota: La imagen muestra el uso de la herramienta FTK Imager. Una vez que se generó los datos respectivos.

Cadena de Custodia entre Dispositivos: Asegurando la Integridad Forense

En este apartado se detalla el proceso de transferencia de datos entre la computadora A, que podría estar comprometida o infectada, y la computadora B, destinada al análisis forense en un entorno

controlado. Para preservar la integridad de la evidencia, se sigue estrictamente la cadena de custodia, asegurando que toda la información transferida mantenga su autenticidad y trazabilidad.

Herramientas Forenses Utilizadas

Para el análisis forense de esta investigación, se ha seleccionado Parrot OS como sistema operativo base debido a su estabilidad y soporte continuo, a diferencia de CAINE Linux, cuyas actualizaciones y estabilidad presentan problemas. En cuanto al análisis de la memoria RAM, se utiliza Volatility versión 3, aunque su uso en Windows 11 es limitado por la falta de una build específica. Como solución provisional, se emplean herramientas nativas de Windows para capturar procesos. Autopsy se utiliza para el análisis detallado del caso, facilitando el seguimiento y la documentación de la investigación forense.

Tabla 3

Herramientas Forenses usadas en la investigación

Elemento	**Descripción**
Sistema Operativo	Parrot OS: Elegido por su estabilidad y soporte continuo
Análisis de Memoria	Volatility 3: Utilizado para el análisis de memoria RAM, aunque con limitaciones en Windows 11.
Análisis	Autopsy: Utilizada para un análisis detallado del caso.
Almacenamiento interno:	

Nota: Esta tabla muestra el detalle de las herramientas forenses usadas en la investigación.

Desarrollo del Laboratorio:

En este laboratorio, se investigan las configuraciones del sistema operativo Windows 11, con especial atención a características como Smartscreen, Windows Security, Windows Update y Cloud Services (OneDrive). También se identifican las causas detrás de los reinicios automáticos, el análisis de las aplicaciones instaladas y la revisión del navegador. Además, se examinan los procesos activos en la memoria RAM utilizando capturas desde el CMD en Windows para detectar posibles problemas de rendimiento o seguridad.

Identificar Configuraciones en la Máquina de Windows 11, Smartscreen, Windows Security, Windows Update, Servicios del Sistema.

Descripción Informativa Windows 11

La versión de compilación 26100.2033 de Windows 11 24H2, lanzada en octubre de 2024, incluye mejoras en usabilidad y rendimiento, entre las que podemos encontrar el rediseño del gestor de cuentas en el menú de Inicio, haciendo más accesible el botón de “Cerrar sesión” y añadiendo controles de medios en la pantalla de bloqueo para gestionar audio y video fácilmente. También se optimizó el uso compartido de archivos, permitiendo compartir resultados de búsqueda desde la barra de tareas. (Narayanaswamy, 2024)

Figura 4

Versión de Windows 11 - version 24H2 (OS Build 26100.2033)

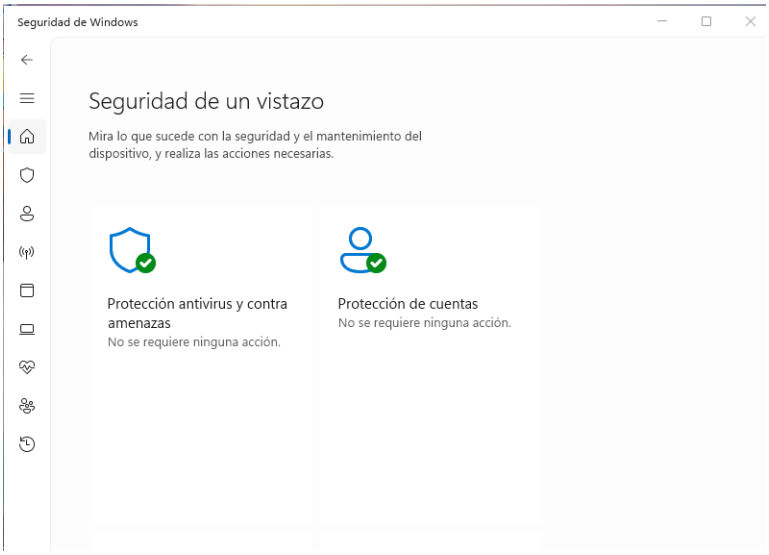
Nota: Versión de windows usando la herramienta de Acerca de Windows.

Windows Security:

Windows Security es el panel de control que centraliza todas las configuraciones y herramientas de seguridad de Windows, incluyendo Windows Defender, firewall, protección de red y dispositivos, control de aplicaciones y navegador, y la configuración de cuentas familiares. A través de este panel, los usuarios pueden revisar el estado de seguridad de su dispositivo y ajustar configuraciones de seguridad para mantener su sistema protegido. (Lipner, 2023)

Figura 5

Estado Windows Security

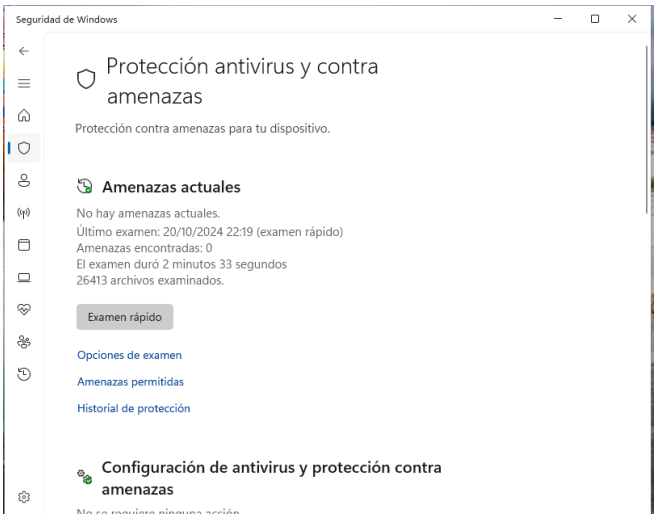


Nota: Estado de seguridad de Windows 11, usando la configuración de windows.

Estado detalle de amenazas:

Figura 6

Estado protección antivirus y contra amenazas



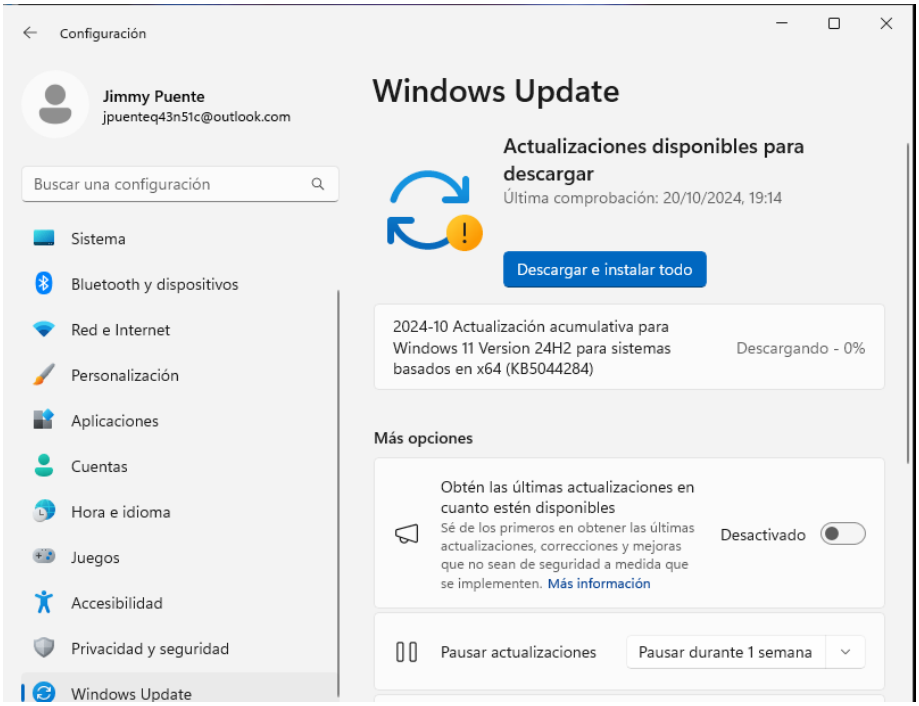
Nota: El gráfico presenta la revision de la proteccion antivirus y contra amenazas desde la configuracion de windows 11.

Windows Update:

Windows Update es el servicio de actualización de Windows que proporciona parches de seguridad, actualizaciones de características, controladores y otras mejoras. Mantiene el sistema operativo actualizado con los últimos parches, asegurando la corrección de vulnerabilidades de seguridad y la compatibilidad con aplicaciones y hardware. Los usuarios pueden configurar Windows Update para descargar e instalar actualizaciones automáticamente, programar reinicios y administrar el historial de actualizaciones. (Lipner, 2023)

Figura 7

Estado Windows Update



Nota: El gráfico representa la configuración de windows update en la configuracion de windows.

Estado Seguridad Windows:

Windows Defender es el software antivirus y antimalware integrado en Windows, diseñado para proteger el sistema en tiempo real contra virus, malware, spyware y otras amenazas. Ofrece escaneos automáticos y actualizaciones frecuentes de la base de datos de amenazas, así como funciones avanzadas como protección basada en la nube y análisis de comportamiento para detectar amenazas desconocidas.

Figura 8

Estado Seguridad de Windows

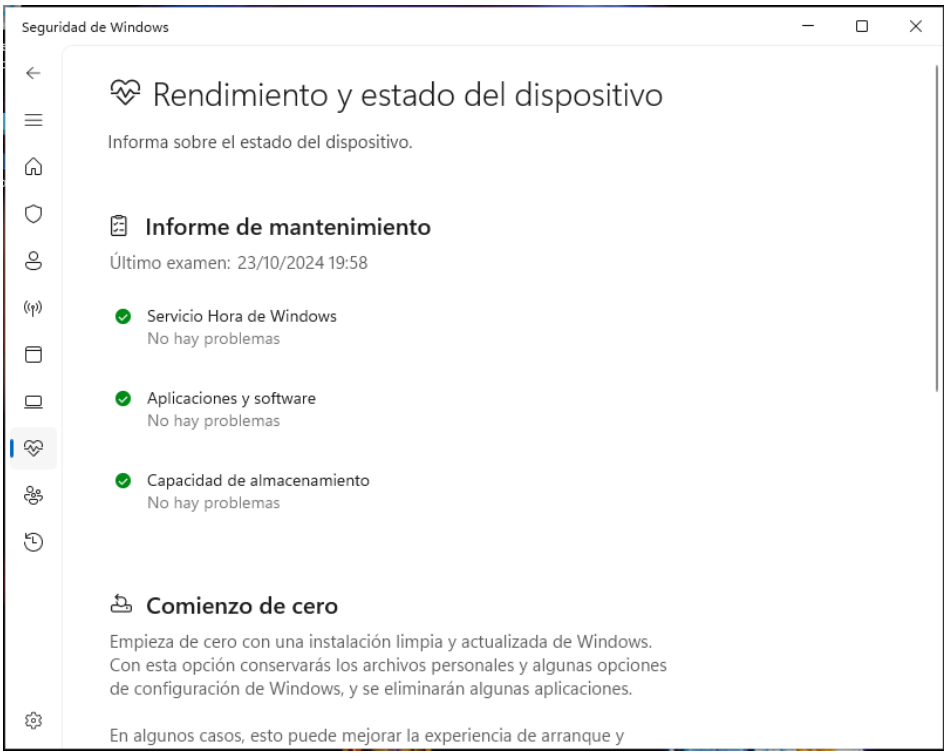
Nota: El Gráfico representa la configuracion en la pantalla de seguridad de windows.

Rendimiento del dispositivo:

El informe del estado del dispositivo en el Centro de Seguridad de Windows de Windows 11 ofrece una evaluación rápida y clara de cuatro áreas clave para el buen funcionamiento del equipo: el almacenamiento, revisando problemas en discos duros; la batería, evaluando el rendimiento y estado de vida útil (en laptops); las aplicaciones y el software, alertando de errores o programas que afectan al sistema; y el tiempo de inicio, identificando posibles demoras en el arranque del sistema y recomendando ajustes.

Figura 9

Seguridad de Windows - Rendimiento y estado del dispositivo



Nota: El gráfico representa la configuracion en la pantalla de seguridad de windows.

Identificar Porque se Dan los Reinicios en Windows 11

Los reinicios inesperados en Windows 11 pueden deberse a una variedad de causas, tanto relacionadas con el hardware como con el software. Identificar la raíz del problema es clave para mitigar el riesgo de daño al equipo o pérdida de datos

A continuación, se detalla las causas más comunes de los reinicios inesperados en Windows 11 y cómo diagnosticarlas:

Problemas de Hardware

- **Sobrecalentamiento**: El sobrecalentamiento de componentes clave como la CPU, GPU o placa madre puede desencadenar reinicios automáticos para proteger el sistema.

Figura 10

Análisis del Cpu Máquina cliente usando HWinfo 64

CPU [#0]: AMD Ryzen 5 7520U: Enhanced				
CPU (Tctl/Tdie)	54.2 °C	48.0 °C	60.6 °C	54.2 °C
Núcleo de CPU	53.2 °C	46.4 °C	61.4 °C	53.0 °C
CPU SOC	48.5 °C	43.1 °C	50.1 °C	47.6 °C
APU GFX	50.3 °C	44.1 °C	54.3 °C	49.6 °C
CPU Skin Temperatura	33.4 °C	32.1 °C	33.4 °C	32.9 °C
Temperaturas núcleo	49.3 °C	28.5 °C	58.0 °C	48.8 °C
L3 Cache	37.1 °C	6.3 °C	55.8 °C	39.4 °C
CPU VDDCR_VDD Voltaje (S...	1.168 V	0.786 V	1.325 V	1.205 V
CPU VDDCR_SOC Voltaje (S...	0.645 V	0.645 V	0.646 V	0.645 V
Corriente del núcleo de la C...	2.188 A	0.521 A	5.085 A	2.477 A
Corriente del SoC (SVI3 TFN)	0.803 A	0.740 A	1.019 A	0.850 A
CPU TDC	2.191 A	0.502 A	5.024 A	2.475 A
CPU EDC	34.626 A	9.907 A	44.857 A	35.248 A
Potencia total de CPU	2.212 W	0.447 W	7.419 W	2.550 W
Potencia los núcleos	0.331 W	0.000 W	2.200 W	0.404 W
CPU Potencia del núcleo (S...	2.958 W	0.420 W	6.973 W	3.390 W
Potencia de SoC CPU (SVI3 ...	0.518 W	0.478 W	0.657 W	0.548 W
Core+SoC Potencia (SVI2 T...	3.476 W	0.944 W	7.596 W	3.939 W
APU STAPM	4.201 W	2.292 W	7.906 W	4.836 W
Infinity Fabric Reloj (FCLK)	399.3 MHz	399.3 MHz	399.3 MHz	399.3 MHz
Reloj del controlador de me...	399.3 MHz	399.3 MHz	399.3 MHz	399.3 MHz
L3 Cache	2,921.6 MHz	1,447.8 MHz	3,889.1 MHz	2,817.6 MHz
Límite de frecuencia: Global	4,321.4 MHz	4,282.4 MHz	4,350.0 MHz	4,316.4 MHz
Límite de CPU TDC	7.8 %	1.8 %	17.9 %	8.8 %
Límite de CPU EDC	69.3 %	19.8 %	89.7 %	70.5 %
CPU PPT FAST Limit	18.0 %	7.4 %	35.6 %	20.0 %
CPU PPT SLOW Limit	24.7 %	20.8 %	26.8 %	24.5 %
APU STAPM Limit	17.5 %	9.5 %	32.9 %	20.2 %
Thermal Limit	55.4 %	48.3 %	64.0 %	55.2 %
Desaceleración térmica (HTC)	No	No	No	0 %
Desaceleración térmica (PR...	No	No	No	0 %
Desaceleración térmica (PR...	No	No	No	0 %
Ancho de banda de lectura ...	1.633 Gbps	1.078 Gbps	2.804 Gbps	1.732 Gbps
Ancho de banda de escritur...	0.341 Gbps	0.060 Gbps	1.122 Gbps	0.335 Gbps

Nota: Imagen obtenida desde la herramienta HWinfo 64 en la máquina del cliente para analizar los recursos.

En la Figura 10. se muestra una lectura detallada de los parámetros del CPU en un sistema con un procesador **AMD Ryzen 5 7520U**. Esta lectura parece haber sido obtenida a través de un software de monitoreo de hardware, mostrando diversos aspectos de rendimiento y estado del procesador. A continuación, algunos detalles clave que se observan:

Temperaturas:

- La temperatura general del CPU (Tctl/Tdie) se encuentra en 54.2°C, con un mínimo de 48.0°C y un máximo de 60.6°C.
- Temperaturas específicas de componentes internos, como el núcleo y el SOC, muestran valores entre los 43.1°C y 61.4°C.

Voltajes:

- Se observa el voltaje de varios componentes, incluyendo el VDDCR_VDD y el VDDCR_SOC, que rondan los 0.876 V y 0.645 V respectivamente.

Corrientes y Potencias:

- Las corrientes para el núcleo y el SOC también están registradas, con valores que oscilan entre 0.501 A y 5.088 A.

- La potencia total del CPU es de aproximadamente 2.212 W, con una potencia máxima en los núcleos de 0.404 W.

Frecuencias:

- La frecuencia global del CPU se encuentra alrededor de los 4.321 MHz, con variaciones que alcanzan un máximo de 4.350 MHz.
- Se listan límites de frecuencia y de varios parámetros, como el CPU TDC, CPU EDC, y el PPT Fast Limit, todos en porcentajes de uso actuales.

Límites Térmicos:

- El límite térmico del CPU está marcado a 55.4°C, indicando que el CPU está cercano a su límite máximo de temperatura operativa.

Desaceleraciones y Ancho de Banda:

- Los valores de ancho de banda de lectura y escritura están entre 1.078 Gbps y 2.804 Gbps para lectura, y entre 0.056 Gbps y 1.122 Gbps para escritura.

Esta información es útil para diagnosticar el estado de operación del procesador, particularmente en términos de rendimiento, eficiencia energética y temperaturas en diversas condiciones de carga.

- **Fallos en la Fuente de Alimentación (PSU)**:
    - Una fuente de alimentación defectuosa o inestable puede no suministrar la energía adecuada a los componentes del equipo, lo que genera reinicios.

Figura 11

Detalle de la batería del Cliente

Battery: innotek 1				
Voltaje de la batería	10.000 V	10.000 V	10.000 V	10.000 V
Capacidad restante	30.000 Wh	30.000 Wh	41.500 Wh	35.724 Wh
Nivel de carga	60.0 %	60.0 %	83.0 %	71.4 %
Nivel de desgaste	0.0 %	0.0 %	0.0 %	0.0 %

Nota: Imagen obtenida desde la herramienta HWinfo 64 Se muestra el detalle de la batería del Cliente Innotek1.

En la Figura 11. se muestra el estado de una batería identificada como **innotek 1** y presenta información sobre su voltaje, capacidad, nivel de carga y desgaste. A continuación, se detallan los datos:

Voltaje de la batería:

- El voltaje es constante en 10.000 V.

Capacidad restante:

- La capacidad de la batería varía, con un valor actual de 30.000 Wh, un mínimo de 30.000 Wh, y un máximo de 41.500 Wh. La capacidad media registrada es de 35.724 Wh.

Nivel de carga:

- La carga actual es del 60.0%, con un máximo registrado de 83.0% y un promedio de 71.4%.

Nivel de desgaste:

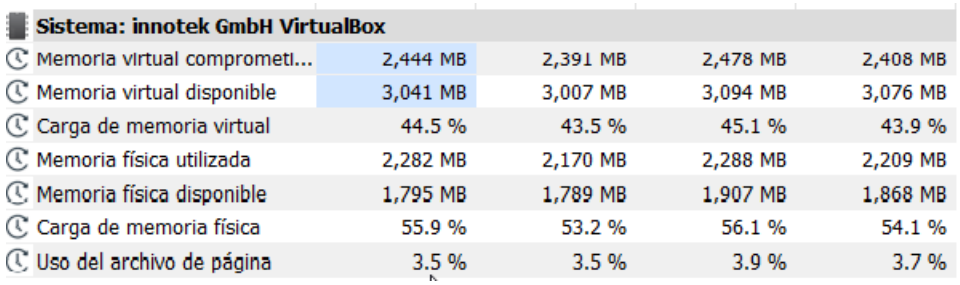
- No se registra desgaste en la batería; el nivel de desgaste es de 0.0%.

Estos valores sugieren que la batería se encuentra en buen estado sin signos de deterioro, con un nivel de carga adecuado y un voltaje estable.

- **Problemas con la Memoria RAM**:
    - Errores en la RAM pueden causar reinicios si el sistema intenta acceder a sectores defectuosos.

Figura 12

Imagen de la memoria virtual



Sistema: innotek GmbH VirtualBox				
Memoria virtual comprometi...	2,444 MB	2,391 MB	2,478 MB	2,408 MB
Memoria virtual disponible	3,041 MB	3,007 MB	3,094 MB	3,076 MB
Carga de memoria virtual	44.5 %	43.5 %	45.1 %	43.9 %
Memoria física utilizada	2,282 MB	2,170 MB	2,288 MB	2,209 MB
Memoria física disponible	1,795 MB	1,789 MB	1,907 MB	1,868 MB
Carga de memoria física	55.9 %	53.2 %	56.1 %	54.1 %
Uso del archivo de página	3.5 %	3.5 %	3.9 %	3.7 %

Nota: Imagen obtenida desde la herramienta HWinfo 64, para analizar la memoria virtual.

En la Figura 12. se muestra el uso de memoria de **innotek GmbH**, detallando tanto la memoria virtual como la memoria física y el archivo de página. A continuación, se desglosan los datos principales:

Memoria Virtual:

- Memoria virtual comprometida: Actualmente es de 2,444 MB, con variaciones entre 2,391 MB y 2,478 MB.

- Memoria virtual disponible: Actualmente hay 3,041 MB disponibles, con un mínimo de 3,007 MB y un máximo de 3,094 MB.
- Carga de memoria virtual: La carga oscila alrededor del 44.5%, con valores entre 43.5% y 45.1%.

Memoria Física:

- Memoria física utilizada: 2,282 MB en uso, con variaciones entre 2,170 MB y 2,288 MB.
- Memoria física disponible: Actualmente disponible 1,795 MB, con un rango de 1,789 MB a 1,907 MB.
- Carga de memoria física: La carga actual es del 55.9%, con fluctuaciones entre 53.2% y 56.1%.

Uso del Archivo de Página:

- Actualmente en un 3.5%, con valores registrados entre 3.5% y 3.9%.

Estos datos reflejan que el sistema utiliza una cantidad considerable de memoria física y virtual, pero aún tiene memoria disponible, tanto en virtual como en física, sin indicios de sobrecarga significativa. El archivo de página también se encuentra en un nivel bajo de uso.

- **Disco Duro o SSD Dañado**:
    - Sectores defectuosos o fallos en el disco pueden provocar reinicios, especialmente durante el acceso a archivos del sistema.

Figura 13

Muestra estadísticas de rendimiento de un disco duro virtual.

Drive: VBOX HARDDISK (VB16e53697-8ba1bd1c)				
Actividad de lectura	0.0 %	0.0 %	53.9 %	0.1 %
Actividad de escritura	0.0 %	0.0 %	27.1 %	0.1 %
Actividad total	0.0 %	0.0 %	54.0 %	0.1 %
Tasa de lecturas	0.000 MB/s	0.000 MB/s	32.524 MB/s	0.026 MB/s
Tasa de escrituras	0.048 MB/s	0.000 MB/s	9.605 MB/s	0.028 MB/s
Leer total	2,436 MB	2,286 MB	2,436 MB	
Escribe total	715 MB	548 MB	715 MB	

Nota: Imagen obtenida desde la herramienta HWinfo 64, muestras estadísticas de rendimiento de un disco duro virtual,

En la Figura 13, se muestra estadísticas de rendimiento de un disco duro virtual, identificado como "VBOX HARDDISK (VB16e53697-8ba1bd1c)". Las columnas presentan valores que cambian en tiempo real y abarcan las siguientes métricas:

- Actividad de lectura: Varía entre 0.0 % y 53.9 %.
- Actividad de escritura: Ronda entre 0.0 % y 27.1 %.
- Actividad total: Alcanza hasta un 54.0 %.
- Tasa de lecturas: Fluctúa de 0.000 MB/s hasta 32.524 MB/s.
- Tasa de escrituras: Oscila entre 0.000 MB/s y 9.605 MB/s.
- Leer total: Registra valores acumulados, como 2,436 MB en algunos casos.
- Escribe total: Tiene acumulados hasta 715 MB en algunos puntos.

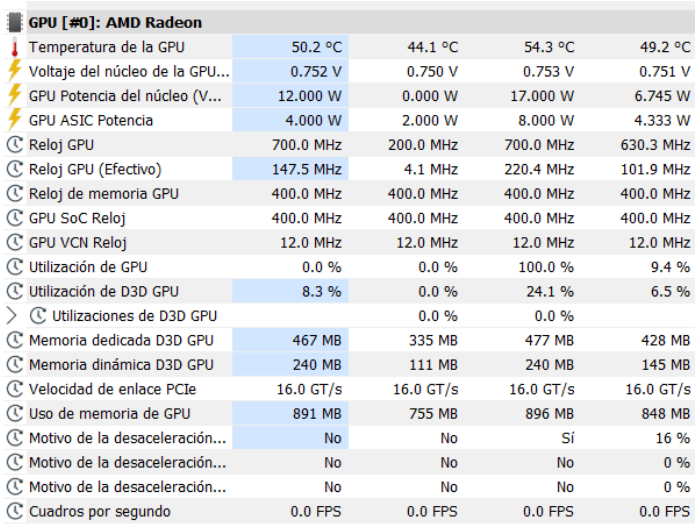
La información proporciona una visión general del uso y la carga actual en el disco, mostrando que ha habido picos de actividad de lectura y escritura, aunque en el momento de la captura, la actividad es baja o nula en varias columnas.

Controladores de Dispositivo Mal Funcionando

- **Controladores Incorrectos o Corruptos**:
    - Los controladores defectuosos, en particular los de gráficos, red o chipset, pueden causar inestabilidad en el sistema.
- **Drivers de GPU**:
    - Los problemas con controladores de la tarjeta gráfica suelen causar reinicios, especialmente durante tareas intensivas de gráficos (juegos, edición de video).

Figura 14

Monitor de hardware



GPU [#0]: AMD Radeon				
Temperatura de la GPU	50.2 °C	44.1 °C	54.3 °C	49.2 °C
Voltaje del núcleo de la GPU...	0.752 V	0.750 V	0.753 V	0.751 V
GPU Potencia del núcleo (V...	12.000 W	0.000 W	17.000 W	6.745 W
GPU ASIC Potencia	4.000 W	2.000 W	8.000 W	4.333 W
Reloj GPU	700.0 MHz	200.0 MHz	700.0 MHz	630.3 MHz
Reloj GPU (Efectivo)	147.5 MHz	4.1 MHz	220.4 MHz	101.9 MHz
Reloj de memoria GPU	400.0 MHz	400.0 MHz	400.0 MHz	400.0 MHz
GPU SoC Reloj	400.0 MHz	400.0 MHz	400.0 MHz	400.0 MHz
GPU VCN Reloj	12.0 MHz	12.0 MHz	12.0 MHz	12.0 MHz
Utilización de GPU	0.0 %	0.0 %	100.0 %	9.4 %
Utilización de D3D GPU	8.3 %	0.0 %	24.1 %	6.5 %
Utilizaciones de D3D GPU		0.0 %	0.0 %	
Memoria dedicada D3D GPU	467 MB	335 MB	477 MB	428 MB
Memoria dinámica D3D GPU	240 MB	111 MB	240 MB	145 MB
Velocidad de enlace PCIe	16.0 GT/s	16.0 GT/s	16.0 GT/s	16.0 GT/s
Uso de memoria de GPU	891 MB	755 MB	896 MB	848 MB
Motivo de la desaceleración...	No	No	Sí	16 %
Motivo de la desaceleración...	No	No	No	0 %
Motivo de la desaceleración...	No	No	No	0 %
Cuadros por segundo	0.0 FPS	0.0 FPS	0.0 FPS	0.0 FPS

Nota: Imagen obtenida desde la herramienta HWinfo 64, Monitor de Gpu usando la herramienta.

En la Figura 14, se muestra una captura de pantalla de un monitor de hardware, específicamente el estado de una GPU AMD Radeon. Los valores están distribuidos en cuatro columnas y muestran diferentes estadísticas en tiempo real.

Aquí se detallan los principales:

- **Temperatura de la GPU:** Varía entre 44.1 °C y 54.3 °C.
- **Voltaje del núcleo de la GPU:** Ronda entre 0.750 V y 0.753 V.
- **Potencia del núcleo de la GPU:** Oscila entre 4.000 W y 8.000 W.
- **Reloj de la GPU:** Frecuencias en MHz que van desde 4.1 MHz hasta 700.0 MHz.
- **Utilización de la GPU:** Baja, entre 0 % y 8.3 %.
- **Memoria de la GPU:** Uso de memoria entre 755 MB y 896 MB.

Algunas otras métricas como el motivo de la desaceleración muestran "No" o "Sí", indicando probablemente si hay limitaciones de rendimiento. En el apartado de "Cuadros por segundo (FPS)" todos los valores son 0, lo que sugiere que no se está ejecutando ninguna carga gráfica intensiva en el momento.

Este tipo de detalles ayudan a verificar el estado y rendimiento de la GPU.

Software o Aplicaciones Conflictivas

- **Actualizaciones del Sistema**:
    - Las actualizaciones de Windows mal instaladas o fallidas pueden provocar reinicios recurrentes.

- **Aplicaciones de Terceros**:
    - Las aplicaciones instaladas recientemente (como software de minería, antivirus mal configurados o herramientas de sistema) pueden provocar conflictos y reinicios.
- **Malware**:
    - El malware puede infiltrarse en el sistema y provocar inestabilidad, incluidos reinicios forzados.

Errores en el Registro del Sistema

- **Entradas de Registro Corruptas**:
    - Modificaciones incorrectas en el Registro de Windows pueden desestabilizar el sistema, provocando reinicios.

Configuración Incorrecta de Energía

- **Opciones de energía mal configuradas**:
    - Ajustes inadecuados de energía, como activación de hibernación o apagado automático, pueden provocar reinicios no deseados.

E**rror de Pantalla Azul (BSOD)**

- **Errores Críticos del Sistema (BSOD)**:
    - Los errores de pantalla azul (BSOD) por fallos en el sistema operativo pueden desencadenar reinicios. Estos errores suelen estar relacionados con drivers, hardware defectuoso o configuraciones de software.

Actualización de BIOS

- **BIOS Obsoleto o Mal Configurado**:
    - Una versión desactualizada del BIOS o configuraciones incorrectas pueden causar reinicios, especialmente si el hardware ha sido actualizado recientemente.

Si tras descartar problemas de hardware, controladores defectuosos, conflictos con aplicaciones, malware, errores en el registro, configuraciones de energía, pantallas azules (BSOD) y actualización de BIOS, no se detecta ninguna novedad en estos aspectos, el problema de reinicios podría estar relacionado con una **incorrecta actualización del sistema operativo Windows 11**.

Resumen del diagnóstico:

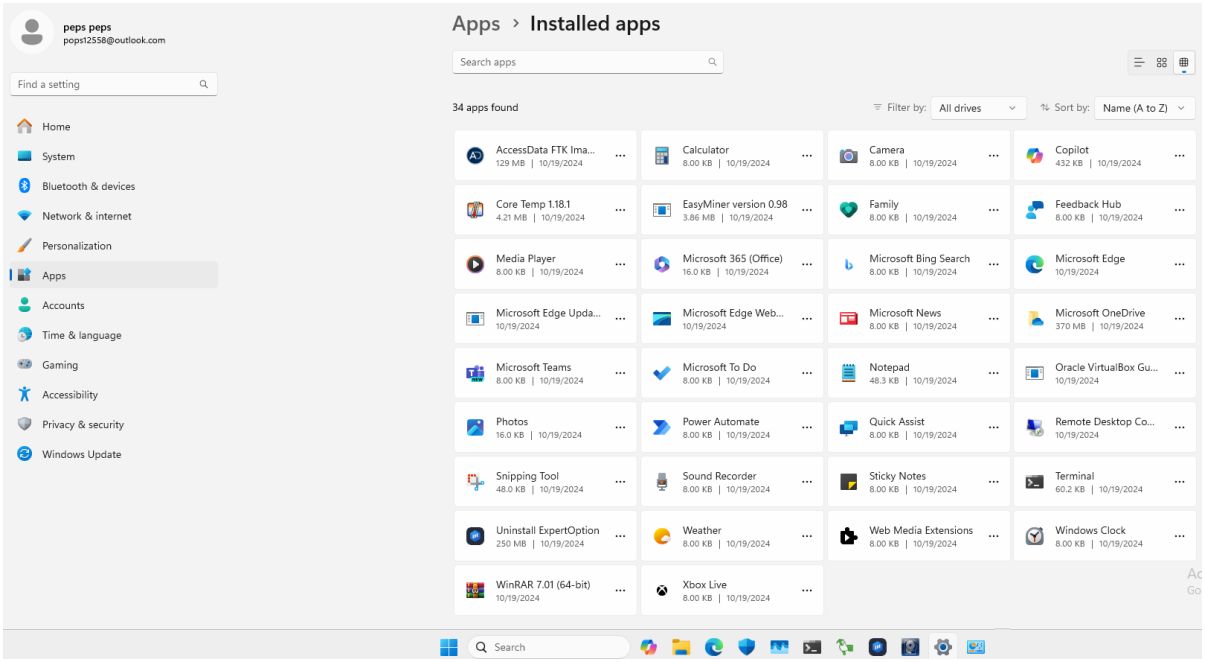
- **Causa probable**: Una actualización fallida o mal implementada de Windows 11 que afecta la estabilidad del sistema.
- **Síntomas observados**: Reinicios recurrentes y posibles problemas de rendimiento derivados de incompatibilidades o errores introducidos en la actualización.

Identificar Aplicaciones Instaladas y Análisis del Navegador para ver el Inicio

En esta sección, se detallará el proceso para identificar las aplicaciones instaladas en el sistema y analizar la actividad del navegador web con el fin de obtener datos que nos ayuden a analizar el ingreso de esta aplicación y el comportamiento del usuario. Aplicaciones instaladas revisión usando la herramienta de Windows 11 para ver las aplicaciones instaladas:

Figura 15

Aplicaciones desde la opción de aplicaciones Instaladas en Windows 11



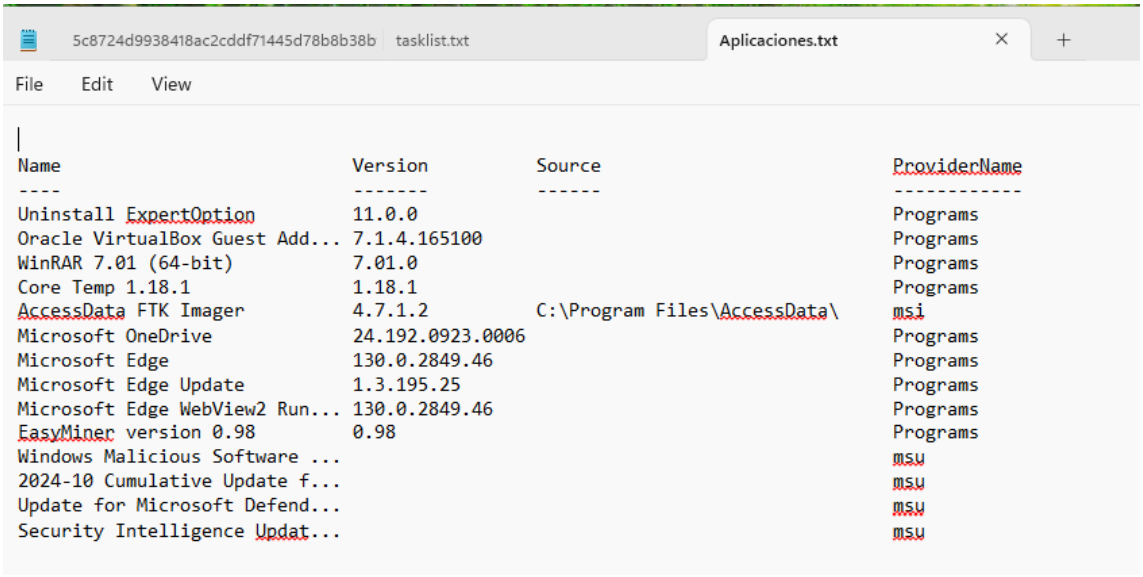
Nota: Imagen con las aplicaciones de configuracion de windows 11.

Para analizar las aplicaciones se puede usar PowerShell, para obtener una lista más detallada. Abre PowerShell y se ejecutó el siguiente comando:

Get-Package > text.txt

Figura 16

Revisión de las aplicaciones usando PowerShell



Nota: Gráfico Revision del detalle de aplicaciones.txt,

Durante este análisis se puede revisar algunas aplicaciones que vienen por default en el sistema operativo de Windows 11, tal como:

- Calculadora.
- Fotos.
- Microsoft 365.
- Microsoft To do.
- Windows Clock.

Entre algunas aplicaciones que se puede analizar y llaman la atención:

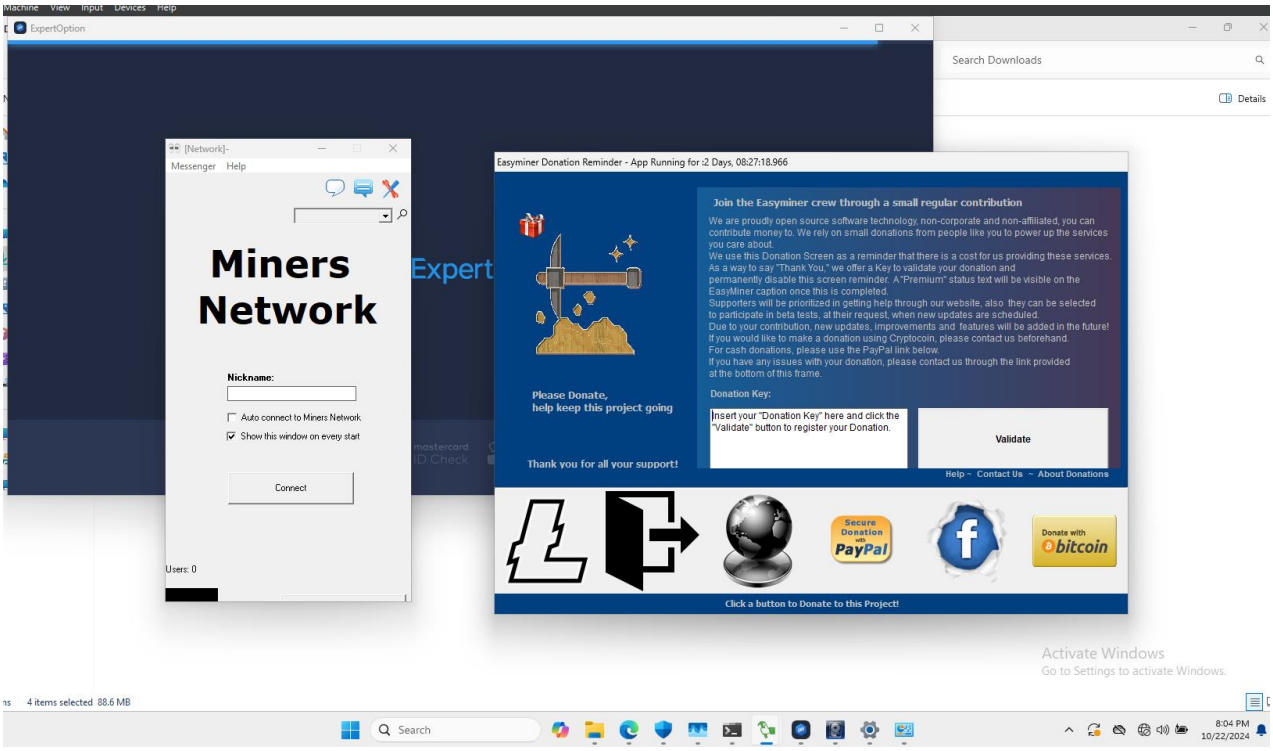
- Core Temp 1.18.1.
- Easy miner.

- Uninstall Expert option.

También se tiene actualmente algunas aplicaciones que quedaron activas y se están ejecutando en segundo plano:

Figura 17

Ventana Emergente de BitCoin Miner que aparece en Windows 11



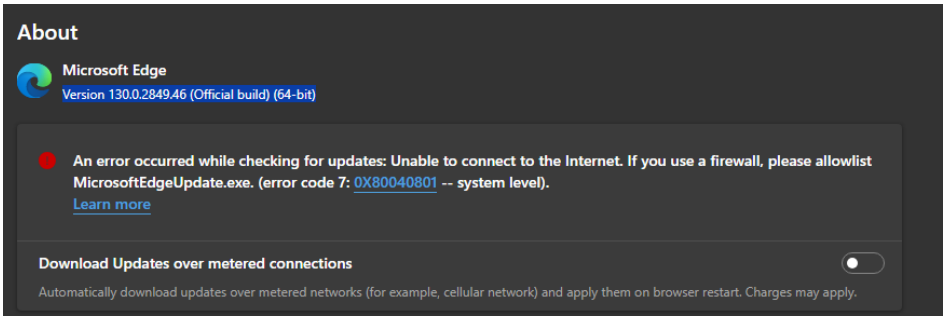
Nota: Captura de Pantalla del escritorio del cliente con algunas aplicaciones actualmente trabajando.

El navegador web del cliente representa una fuente valiosa de información, ya que el historial de navegación y las descargas reflejan el comportamiento del usuario y su interacción con el entorno digital. Examinar estos datos permite identificar patrones de búsqueda y hábitos de descarga, lo cual es fundamental para evaluar posibles riesgos de seguridad.

Revisando el navegador de la computadora de nuestro cliente se puede saber que se está trabajando con una versión de Microsoft Edge como navegador por defecto, con la versión 130.0.2849.46:

Figura 18

Versión del Navegador Microsoft Edge



Nota: Versión del navegador del uso del cliente.

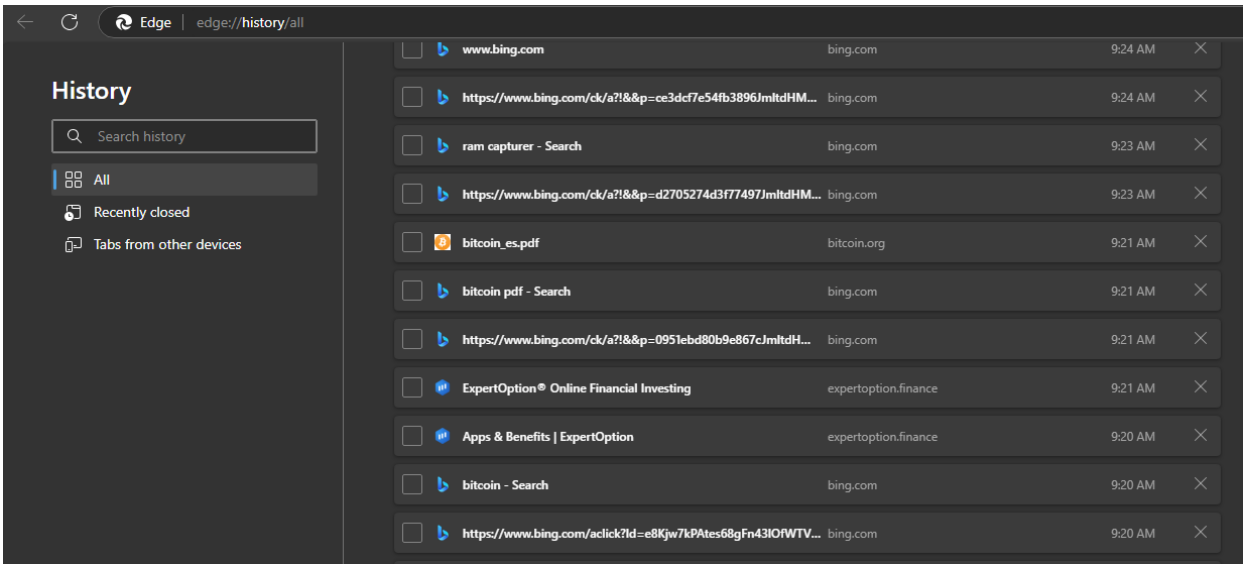
El análisis del historial de navegación y de los archivos descargados no solo permite reconstruir la actividad en línea del cliente, sino que también puede revelar intentos de acceso a sitios web potencialmente maliciosos o la instalación de aplicaciones que representan una amenaza para el sistema.

En este apartado, se presentan los resultados detallados del análisis de la actividad del navegador, segmentados en dos secciones Historial de Búsqueda y Descargas del cliente.

Muestra A:

Figura 19

Historial Microsoft Edge Búsquedas Importantes lapso A



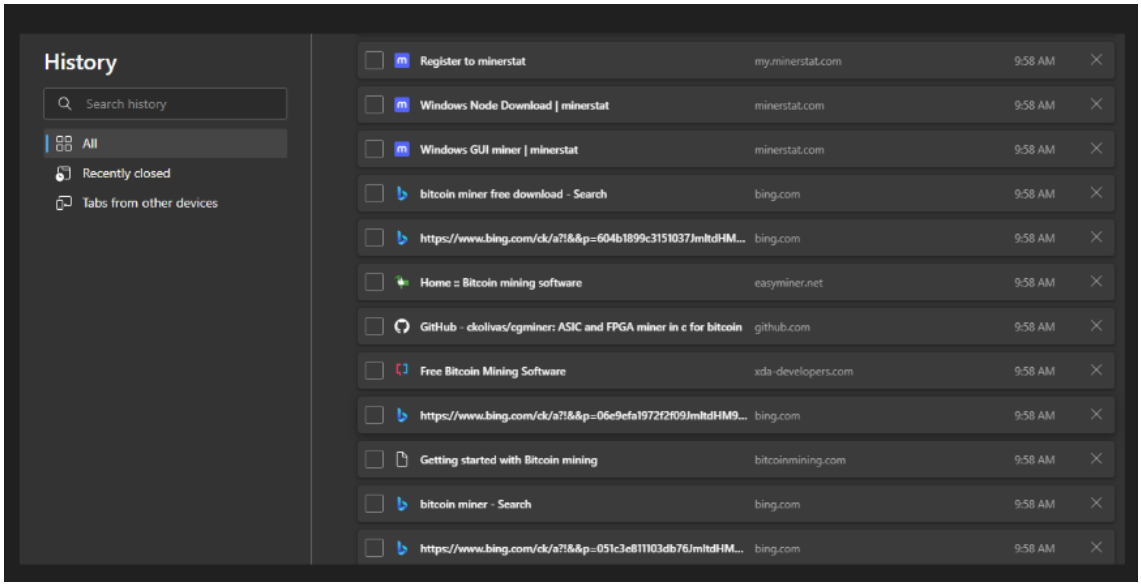
Nota: Captura de Pantalla del historial del navegador del cliente.

En la figura 19 se revisa varios datos de búsqueda se puede apreciar que el cliente ha ingresado ciertos criterios de búsqueda simples que le han llevado a descargar aplicaciones sin supervisión uno de los resultados que más llama la atención es: “bitcoin”, “bitcoin pdf”, “bitcoin miner”.

Muestra B:

Figura 20

Historial Microsoft Edge Búsquedas Importantes lapso B



Nota: Captura de Pantalla del historial del navegador del cliente lapso de tiempo mayor.

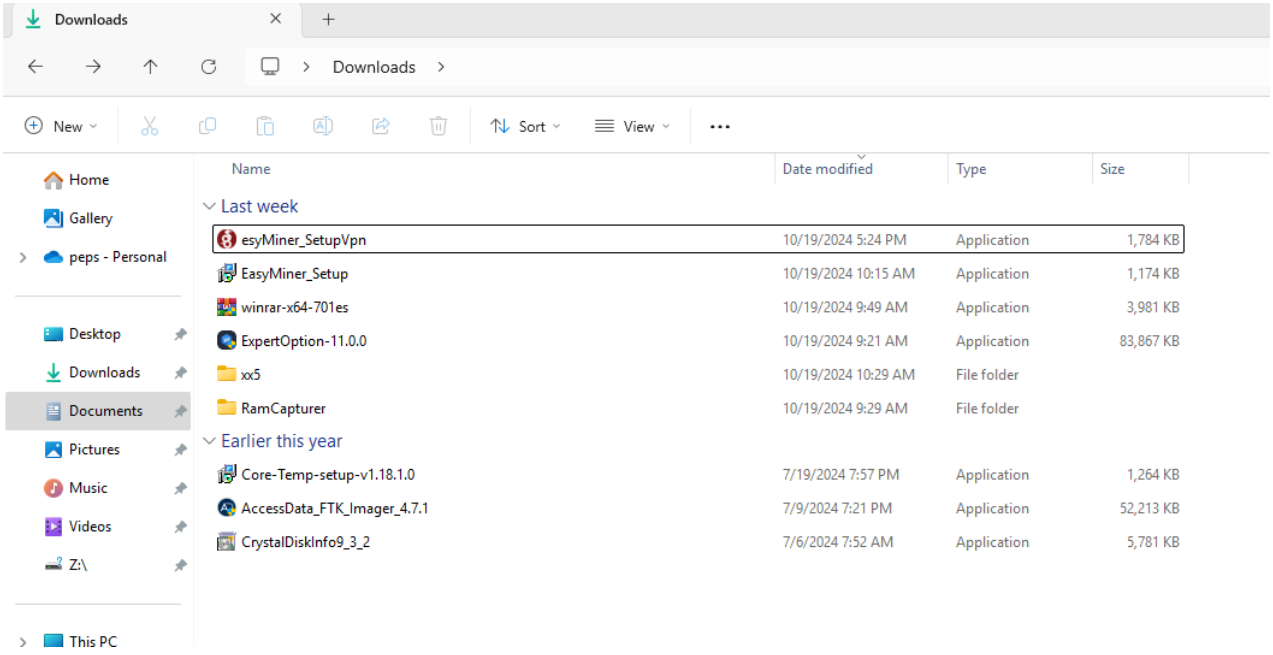
En la figura 20 se representa el historial de búsquedas del cliente, se puede observar una variedad de sitios web visitados en un período determinado. Este historial es crucial para identificar patrones de comportamiento y posibles riesgos.

Descargas del Cliente:

Además de las búsquedas, se revisaron las descargas realizadas por el cliente, observándose ciertos archivos que podrían considerarse de riesgo. Estos archivos, posiblemente descargados como resultado de las búsquedas mencionadas, pueden contener aplicaciones no supervisadas que exponen el sistema a vulnerabilidades.

Figura 21

Carpeta de Descargas de la Máquina del Cliente



Nota: Captura de Pantalla a la carpeta de descargas en el del navegador del cliente lapso de tiempo mayor.

En la figura 21 se tiene algunas aplicaciones en la carpeta de descargas que se va a detallar en este análisis se encuentran en el rango de tiempo de las búsquedas más importantes del cliente.

Detalle de las aplicaciones:

Tabla 4

Detalle de las aplicaciones encontradas en la carpeta de descargas

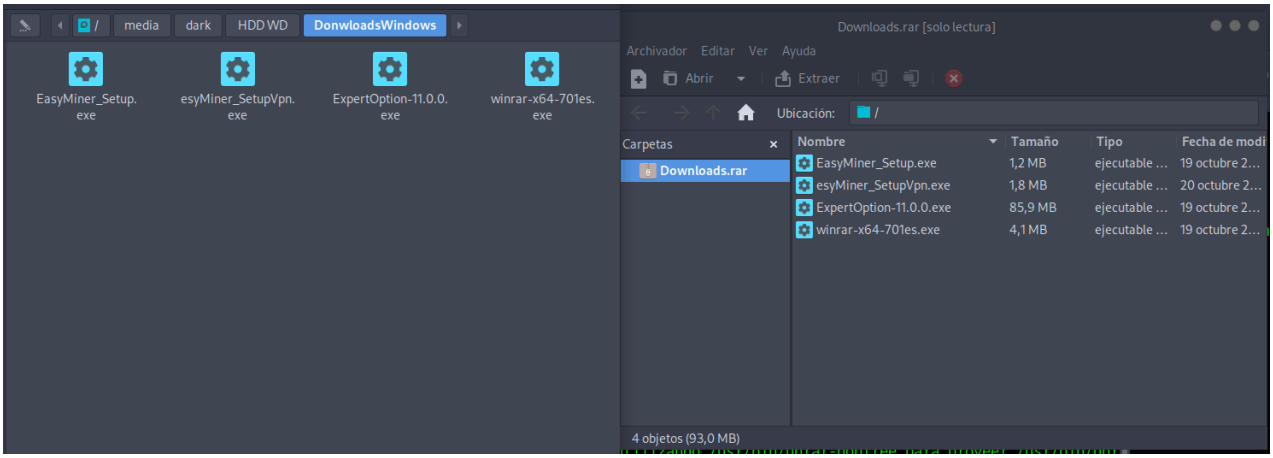
Nombre aplicación:	**Fecha de instalación**	**Localización**	**Tamaño:**
ExpertioOption-11.0.0	Octubre 19, 2024, 9:21:00	C:\Users\pops1\Downloads	81.9 MB
Winrar-x64-701es	Octubre 19, 2024, 9:49:08	C:\Users\pops1\Downloads	3.88 MB
EasyMiner_Setup	Octubre 19, 2024, 10:15:08	C:\Users\pops1\Downloads	1.14 MB
esyMiner_Setup	Octubre 19, 2024, 10:23:31	C:\Users\pops1\Downloads	1.74 MB

Nota: Esta tabla muestra las aplicaciones al detalle que se han instalado en la maquina del cliente.

Entre estas aplicaciones para identificar cual es el malware se debe hacer un análisis revisando los ejecutables en la maquina usando Linux, para la transferencia de esos archivos se utilizó un disco duro externo para copiar los ejecutables y analizarlos en el sistema operativo Parrot OS:

Figura 22

Transferencia de los archivos al sistema operativo Parrot OS



Nota: Transferencia de los archivos a una máquina un poco más segura.

En la figura 22 se aprecia la transferencia de los archivos y una vez revisados estos ejecutables en el sistema operativo de Linux se procedió a revisar todos los ejecutables:

Se reviso usando la herramienta web virus total analizando todos los ejecutables:

Tabla 5

Calificación de Aplicación usando virus total

Nombre aplicación:	Extensión	Calificación Virus Total	Popular threat label
ExpertioOption-11.0.0	.exe	0/79	NA
Winrar-x64-701es	.exe	0/70	NA
EasyMiner_Setup	.exe	7/73	miner.filerepmalware/misc
esyMiner_Setup	.exe	57/73	trojan.msil/injuke

Nota: Esta tabla muestra el detalle usando virus total, con el detalle y la calificación.

Como se puede apreciar en la tabla 5, se tiene 2 de 4 aplicaciones que son preocupantes, un easyminer que está actuando como un bitcoin miner en la máquina del cliente, y otro como un troyano con alrededor de 57 puntos en la escala de virus total.

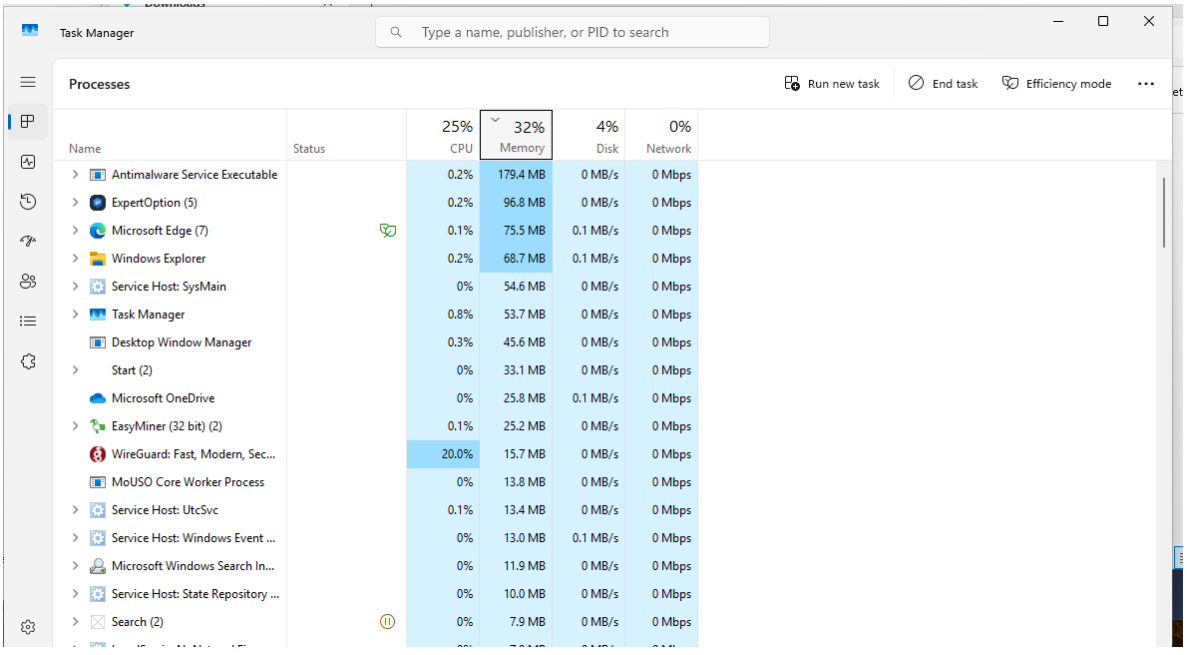
Revisión de los Procesos de la Memoria RAM y Usando Capturas desde CMD en Windows para Identificar Problemas

Para identificar los procesos en la máquina del cliente se ha usado 2 herramientas importantes, se tiene acceso a la máquina del cliente por lo tanto se ha tomado información de ciertos procesos que pueden ser beneficiosos:

Administrador de tareas en Windows:

Figura 23

Administrador de Tareas en Windows 11

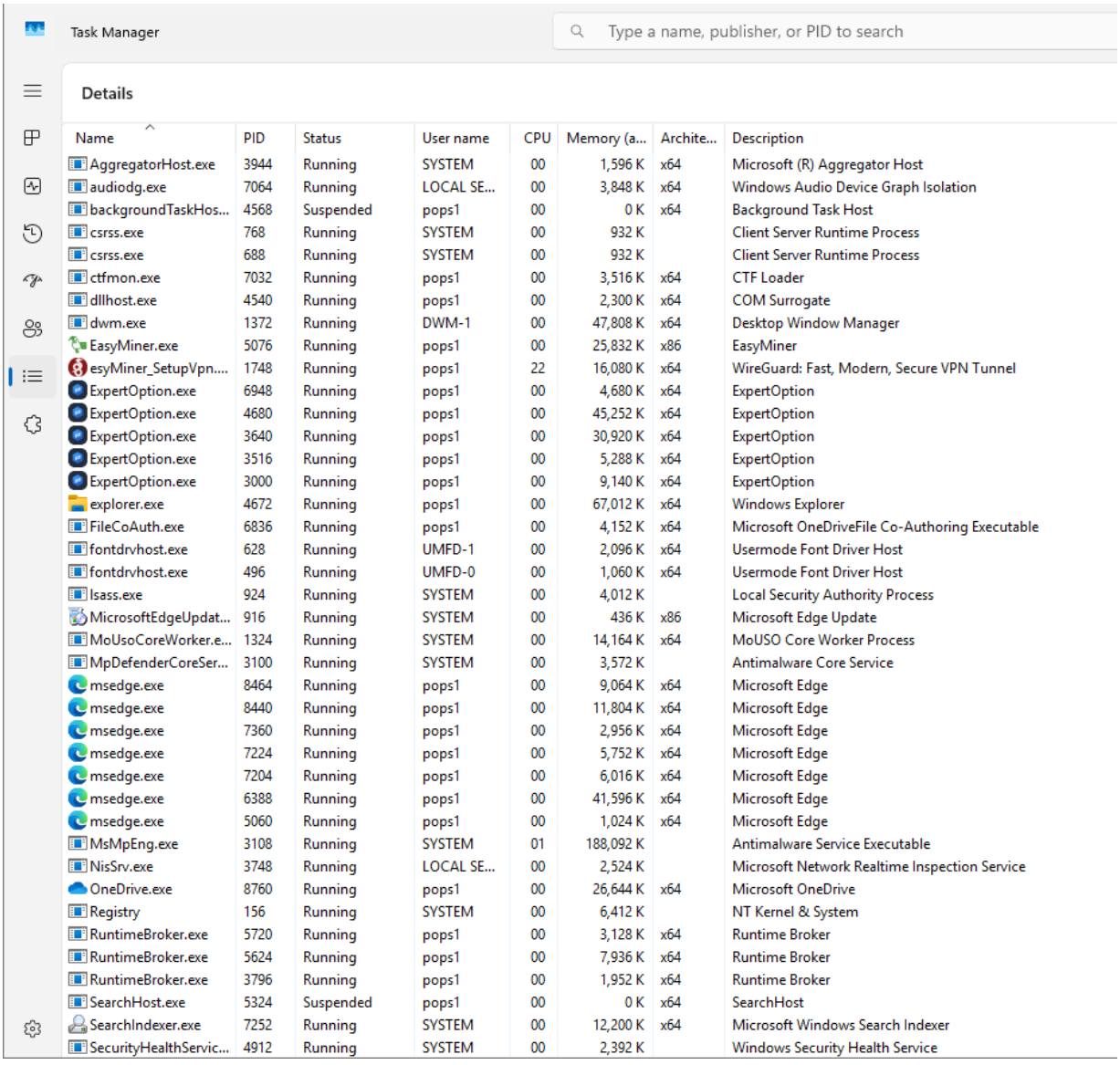


Nota: Captura de Pantalla del administrador de tareas de la máquina del cliente.

Detalles:

Figura 24

Detalle del Administrador de Tareas en Windows 11



Name	PID	Status	User name	CPU	Memory (a...	Archite...	Description
AggregatorHost.exe	3944	Running	SYSTEM	00	1,596 K	x64	Microsoft (R) Aggregator Host
audiodg.exe	7064	Running	LOCAL SE...	00	3,848 K	x64	Windows Audio Device Graph Isolation
backgroundTaskHos...	4568	Suspended	pops1	00	0 K	x64	Background Task Host
csrss.exe	768	Running	SYSTEM	00	932 K		Client Server Runtime Process
csrss.exe	688	Running	SYSTEM	00	932 K		Client Server Runtime Process
ctfmon.exe	7032	Running	pops1	00	3,516 K	x64	CTF Loader
dllhost.exe	4540	Running	pops1	00	2,300 K	x64	COM Surrogate
dwm.exe	1372	Running	DWM-1	00	47,808 K	x64	Desktop Window Manager
EasyMiner.exe	5076	Running	pops1	00	25,832 K	x86	EasyMiner
esyMiner_SetupVpn....	1748	Running	pops1	22	16,080 K	x64	WireGuard: Fast, Modern, Secure VPN Tunnel
ExpertOption.exe	6948	Running	pops1	00	4,680 K	x64	ExpertOption
ExpertOption.exe	4680	Running	pops1	00	45,252 K	x64	ExpertOption
ExpertOption.exe	3640	Running	pops1	00	30,920 K	x64	ExpertOption
ExpertOption.exe	3516	Running	pops1	00	5,288 K	x64	ExpertOption
ExpertOption.exe	3000	Running	pops1	00	9,140 K	x64	ExpertOption
explorer.exe	4672	Running	pops1	00	67,012 K	x64	Windows Explorer
FileCoAuth.exe	6836	Running	pops1	00	4,152 K	x64	Microsoft OneDriveFile Co-Authoring Executable
fontdrvhost.exe	628	Running	UMFD-1	00	2,096 K	x64	Usermode Font Driver Host
fontdrvhost.exe	496	Running	UMFD-0	00	1,060 K	x64	Usermode Font Driver Host
lsass.exe	924	Running	SYSTEM	00	4,012 K		Local Security Authority Process
MicrosoftEdgeUpdat...	916	Running	SYSTEM	00	436 K	x86	Microsoft Edge Update
MoUsoCoreWorker.e...	1324	Running	SYSTEM	00	14,164 K	x64	MoUSO Core Worker Process
MpDefenderCoreSer...	3100	Running	SYSTEM	00	3,572 K		Antimalware Core Service
msedge.exe	8464	Running	pops1	00	9,064 K	x64	Microsoft Edge
msedge.exe	8440	Running	pops1	00	11,804 K	x64	Microsoft Edge
msedge.exe	7360	Running	pops1	00	2,956 K	x64	Microsoft Edge
msedge.exe	7224	Running	pops1	00	5,752 K	x64	Microsoft Edge
msedge.exe	7204	Running	pops1	00	6,016 K	x64	Microsoft Edge
msedge.exe	6388	Running	pops1	00	41,596 K	x64	Microsoft Edge
msedge.exe	5060	Running	pops1	00	1,024 K	x64	Microsoft Edge
MsMpEng.exe	3108	Running	SYSTEM	01	188,092 K		Antimalware Service Executable
NisSrv.exe	3748	Running	LOCAL SE...	00	2,524 K		Microsoft Network Realtime Inspection Service
OneDrive.exe	8760	Running	pops1	00	26,644 K	x64	Microsoft OneDrive
Registry	156	Running	SYSTEM	00	6,412 K		NT Kernel & System
RuntimeBroker.exe	5720	Running	pops1	00	3,128 K	x64	Runtime Broker
RuntimeBroker.exe	5624	Running	pops1	00	7,936 K	x64	Runtime Broker
RuntimeBroker.exe	3796	Running	pops1	00	1,952 K	x64	Runtime Broker
SearchHost.exe	5324	Suspended	pops1	00	0 K	x64	SearchHost
SearchIndexer.exe	7252	Running	SYSTEM	00	12,200 K	x64	Microsoft Windows Search Indexer
SecurityHealthServic...	4912	Running	SYSTEM	00	2,392 K		Windows Security Health Service

Nota: Captura de Pantalla del administrador de tareas de la máquina del cliente, con más detalle.

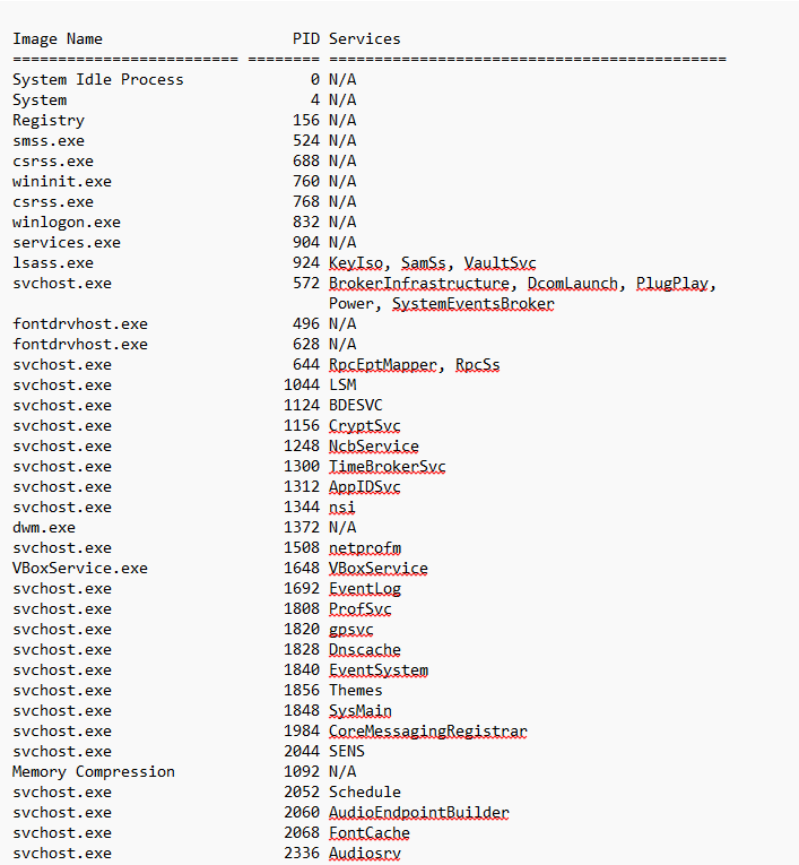
CMD:

Usando la línea de comandos nos permite realizar una copia a la lista de tareas que este disponible:

tasklist /svc >> taslist.txt

Figura 25

Comando para mirar todos los procesos y servicios



```
Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
Registry                       156 N/A
smss.exe                       524 N/A
csrss.exe                      688 N/A
wininit.exe                    760 N/A
csrss.exe                      768 N/A
winlogon.exe                   832 N/A
services.exe                   904 N/A
lsass.exe                      924 KeyIso, SamSs, VaultSvc
svchost.exe                    572 BrokerInfrastructure, DcomLaunch, PlugPlay,
                                   Power, SystemEventsBroker
fontdrvhost.exe                496 N/A
fontdrvhost.exe                628 N/A
svchost.exe                    644 RpcEptMapper, RpcSs
svchost.exe                   1044 LSM
svchost.exe                   1124 BDESVC
svchost.exe                   1156 CryptSvc
svchost.exe                   1248 NcbService
svchost.exe                   1300 TimeBrokerSvc
svchost.exe                   1312 AppIDSvc
svchost.exe                   1344 nsi
dwm.exe                       1372 N/A
svchost.exe                   1508 netprofm
VBoxService.exe               1648 VBoxService
svchost.exe                   1692 EventLog
svchost.exe                   1808 ProfSvc
svchost.exe                   1820 gpsvc
svchost.exe                   1828 Dnscache
svchost.exe                   1840 EventSystem
svchost.exe                   1856 Themes
svchost.exe                   1848 SysMain
svchost.exe                   1984 CoreMessagingRegistrar
svchost.exe                   2044 SENS
Memory Compression            1092 N/A
svchost.exe                   2052 Schedule
svchost.exe                   2060 AudioEndpointBuilder
svchost.exe                   2068 FontCache
svchost.exe                   2336 Audiosrv
```

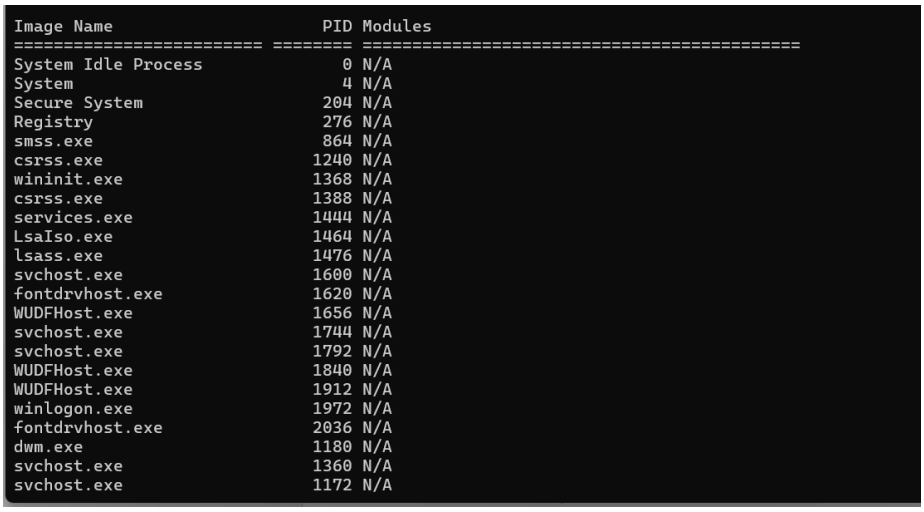
Nota: Imagen de los procesos y servicios con la línea de comandos.

Se muestran todos los procesos y DLLs, usando la linea de comandos.

tasklist /m >> taslist.txt

Figura 26

Comando para mirar todos los procesos y DLLs



```
Image Name                     PID Modules
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
Secure System                  204 N/A
Registry                       276 N/A
smss.exe                       864 N/A
csrss.exe                     1240 N/A
wininit.exe                   1368 N/A
csrss.exe                     1388 N/A
services.exe                  1444 N/A
LsaIso.exe                    1464 N/A
lsass.exe                     1476 N/A
svchost.exe                   1600 N/A
fontdrvhost.exe               1620 N/A
WUDFHost.exe                  1656 N/A
svchost.exe                   1744 N/A
svchost.exe                   1792 N/A
WUDFHost.exe                  1840 N/A
WUDFHost.exe                  1912 N/A
winlogon.exe                  1972 N/A
fontdrvhost.exe               2036 N/A
dwm.exe                       1180 N/A
svchost.exe                   1360 N/A
svchost.exe                   1172 N/A
```

Nota: Imagen de todos los procesos y dlls con la línea de comandos.

Proceso en revisión: Se identifica el proceso con el proceso esyMiner Setup Vpn.

Figura 27

Proceso identificado Administrador de Tareas

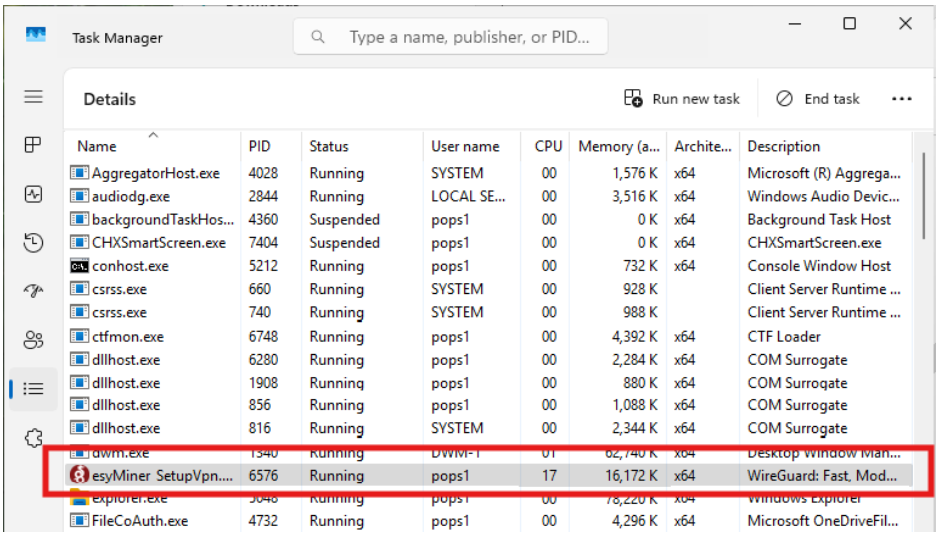
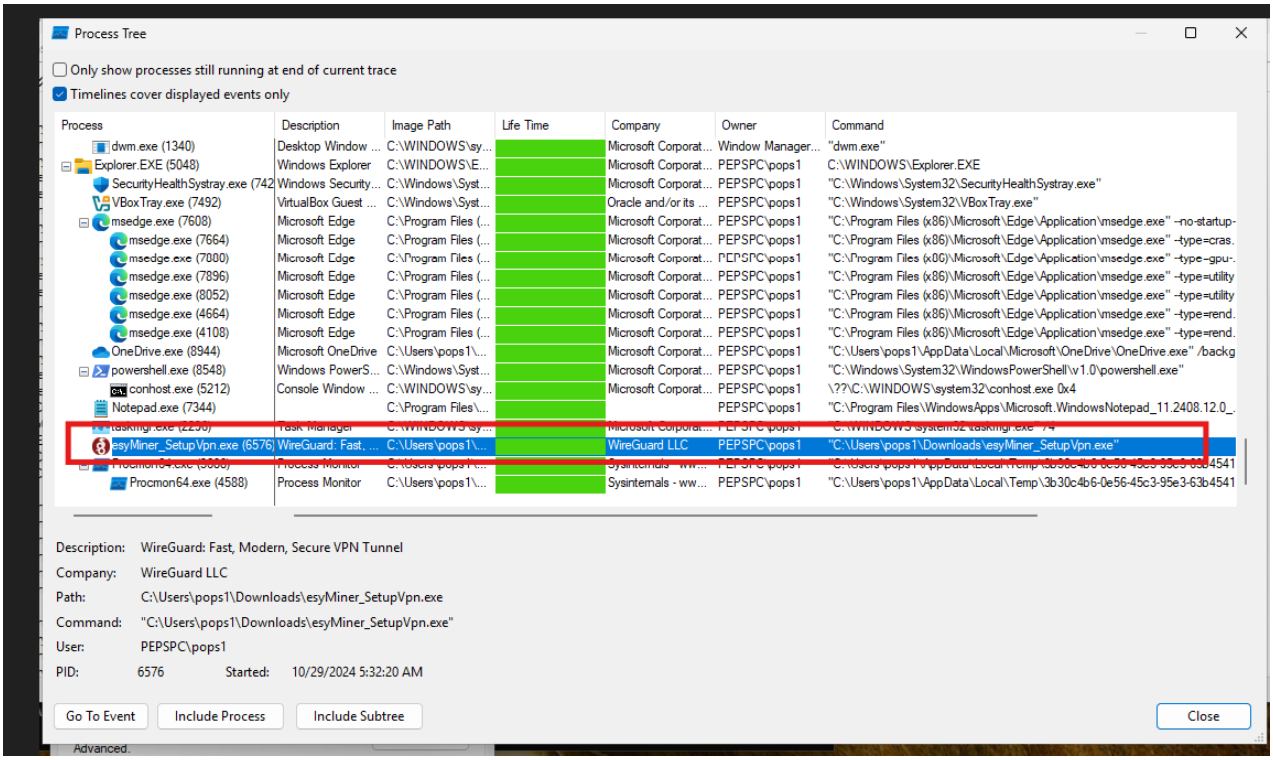


Figura 28

Process Tree Explorer



Nota: Captura de pantalla del proceso identificado como novedad en el árbol de procesos.

En la figura 28 se tiene el Process Explorer herramienta gratuita de Windows que nos ayuda a detectar anomalías, como procesos que se ejecutan sin razón aparente o programas que consumen más recursos de lo normal, revelando potenciales amenazas. Además, permite examinar cada proceso con detalle, obteniendo información sobre sus propiedades, identificador (PID), rutas de archivo y bibliotecas cargadas.

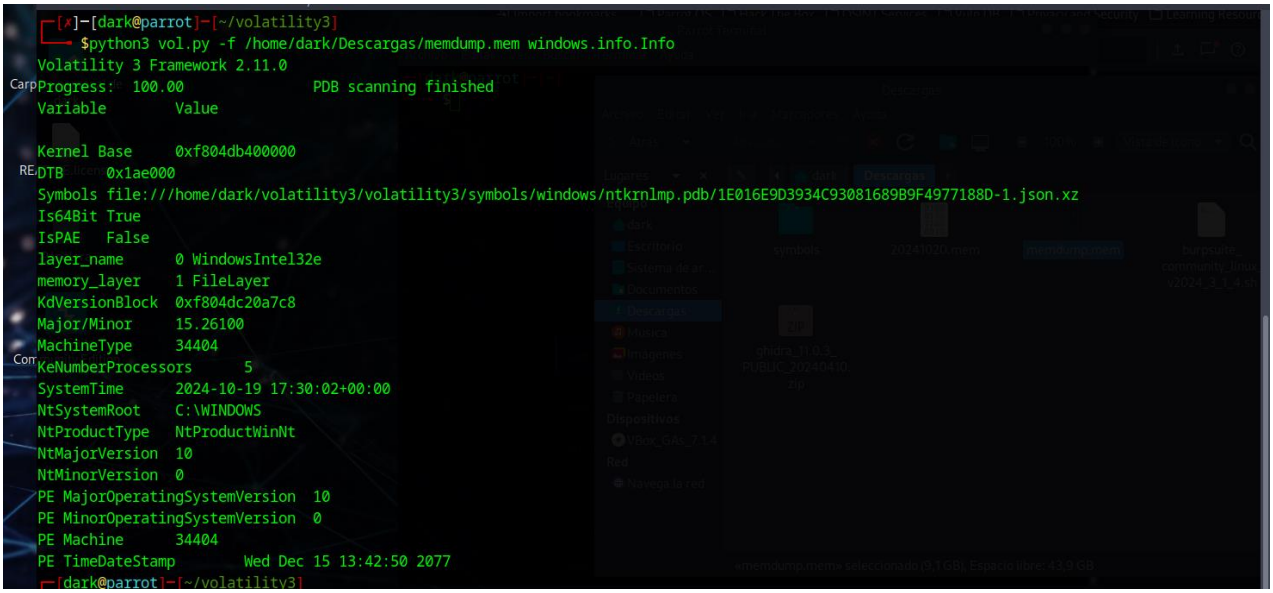
Revisión de la memoria RAM usando Volatitlity 3 Framework 2.11.0

Volatility, en su última versión ejecutada en Parrot OS, se ha convertido en una herramienta crucial para el análisis forense de memoria.

python3 vol.py -f /home/dark/Descargas/memdump.mem windows.info.Info

Figura 29

Captura del comando Info en volatility en Parrot OS



Nota: Captura de pantalla del comando info en el sistema operativo en Parrot OS.

En la figura 29 se aprecia la ejecución del comando `python3 vol.py -f /home/dark/Descargas/memdump.mem windows.info.Info` el cual nos permite extraer información detallada del sistema operativo Windows a partir de un volcado de memoria (memdump).

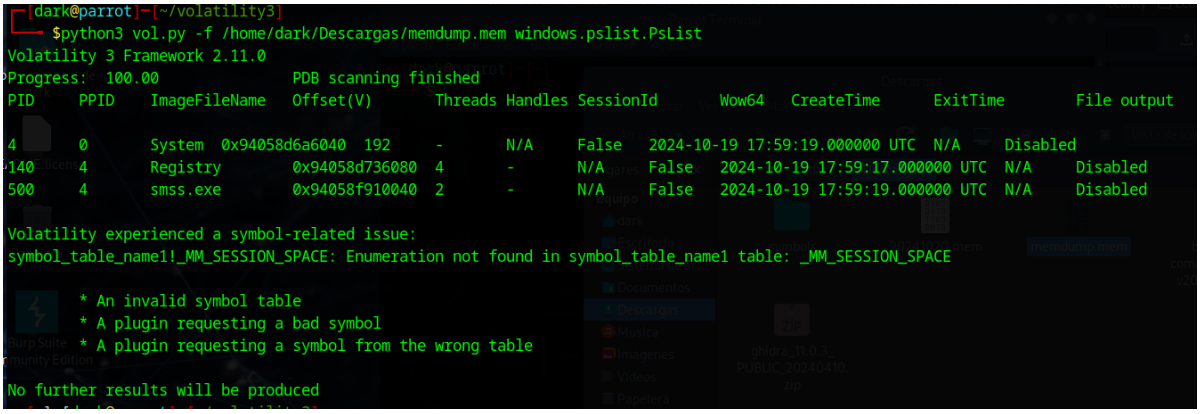
Este análisis ayuda a obtener datos relevantes sobre el entorno del sistema, como el perfil de la versión de Windows, procesos activos, sesiones de usuario, y otros detalles de configuración interna que pueden ser cruciales para la investigación.

La estructura del comando especifica el uso de la opción `-f` para indicar la ubicación del archivo de memoria, mientras que el plugin `windows.info.Info` facilita la recuperación de detalles críticos del sistema que permiten evaluar el estado del dispositivo en el momento del volcado. Esta versión de Volatility mejora el rendimiento y amplía la compatibilidad con versiones modernas de Windows, proporcionando resultados más completos y detallados en el análisis forense.

python3 vol.py -f /home/dark/Descargas/memdump.mem windows.pslist.Pslist

Figura 30

Captura del comando pslist en volatility en Parrot OS



Nota: Captura de pantalla del comando info en el sistema operativo en Parrot OS.

En la figura 30 se tiene el detalle de ejecutar la opción en volatility python3 vol.py -f /home/dark/Descargas/memdump.mem windows.pslist.Pslist, se inicia un análisis exhaustivo de la

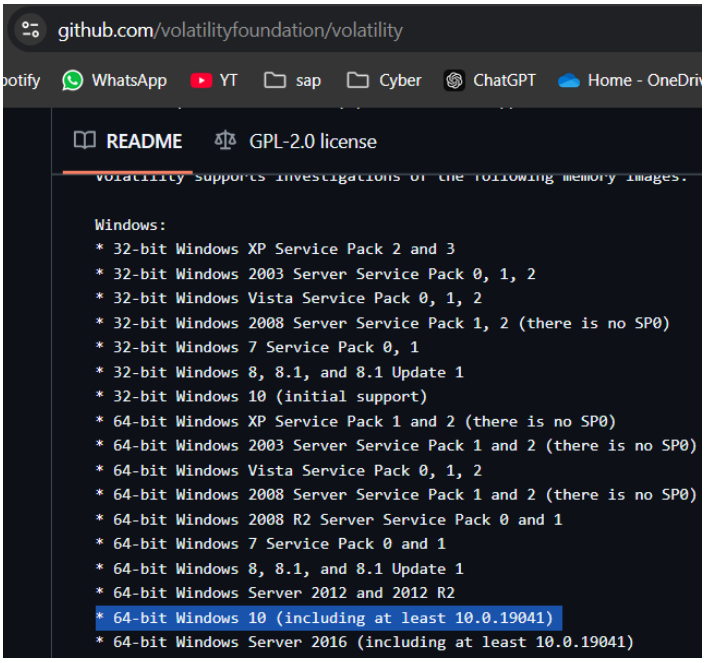
memoria orientado a identificar todos los procesos activos en el sistema Windows al momento de capturar el volcado.

El comando utiliza el plugin windows.pslist.Pslist, que permite listar todos los procesos ejecutados en la memoria, incluyendo su estructura jerárquica, PID, tiempo de inicio, y cualquier relación entre procesos (padre-hijo). Sin embargo, la versión de windowss 11 para ser ejecutada en volaitliy por el momento no tiene soporte y por lo tanto no está soportado comandos como pslist.

En la figura 31 se puede apreciar que la versión 64- bit Windows 11 no se encuentra la lista de imágenes que soporta volatility en la última versión de la aplicación. Se ha consultado sobre seste tema, pero las actualizaciones pueden demorarse.

Figura 31

Imágenes de memoria Volality Disponibles en la Página Oficial



Nota: Captura de pantalla de las imágenes de volatility en la página oficial de github.

Comandos que si están en funcionamiento en la versión volatility 3.0:

Lista de Dlllist en windows: windows.dlllist.DllList

Figura 32

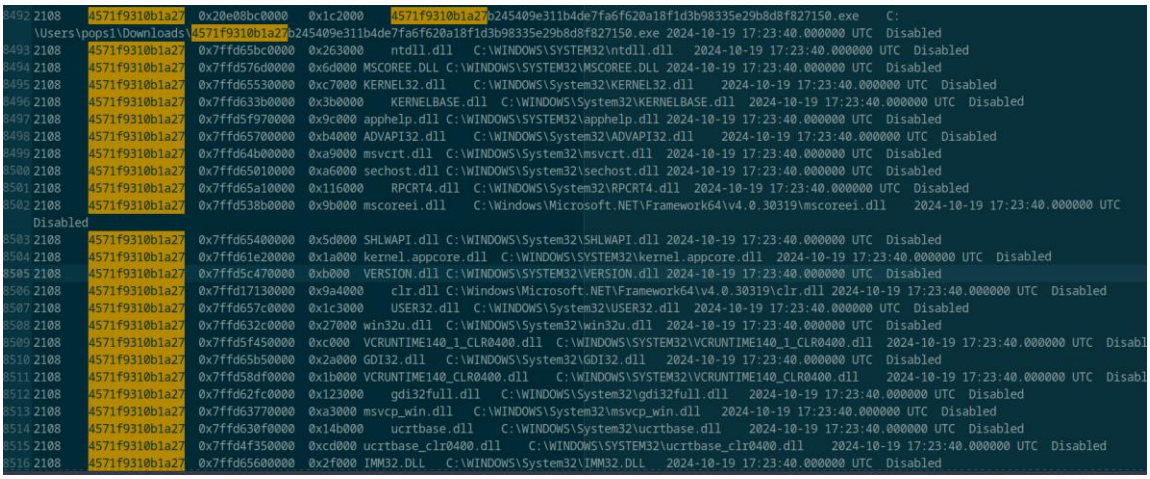
Listar llos dll en la captura de memoria RAM

Nota: Captura desde Parrot OS donde se genera los dlllist disponibles.

Revisando el proceso que tiene anexado el dll:

Figura 33

Procesos Dll que se encuentran relacionados al proceso con novedad



Nota: Captura de pantalla de los procesos relacionados con la novedad detectada.

Filescan en windows: windows.filescan.FileScan

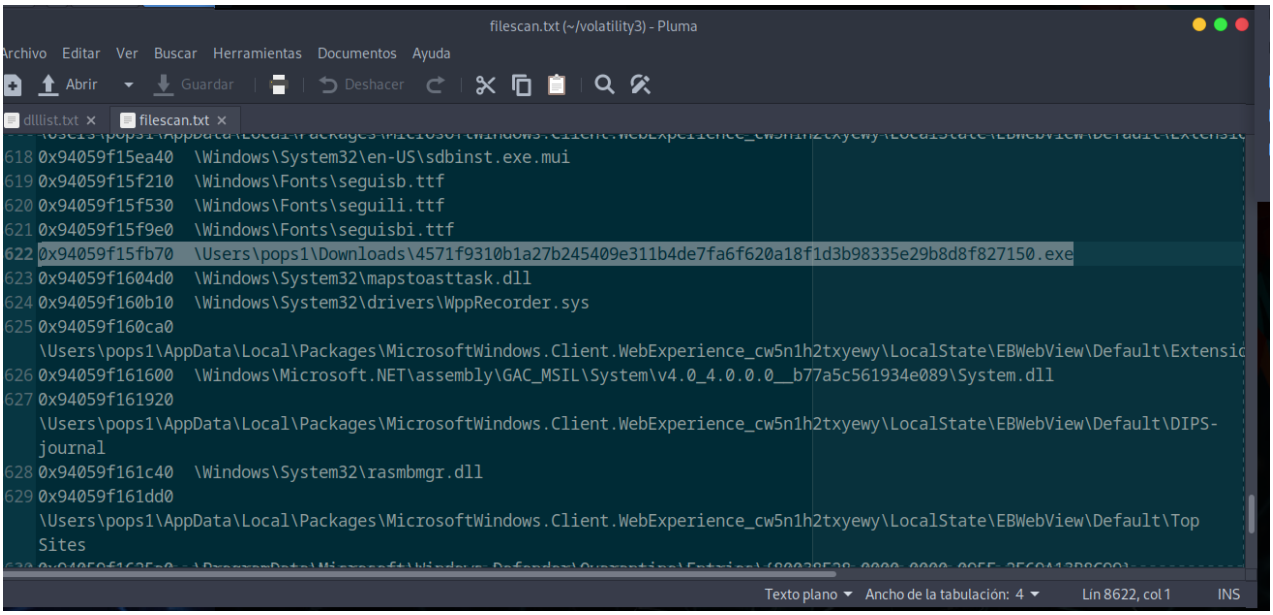
Figura 34

Referencias a archivos que fueron abiertos o manejados por el sistema operativo.

Nota: Captura desde Parrot OS donde se genera los archivos manejados.

Figura 35

Archivo que afecto al Sistema operativo Identificado



Nota: Informe usando la herramienta de volatility3 usando el comando windows.modules.Modules

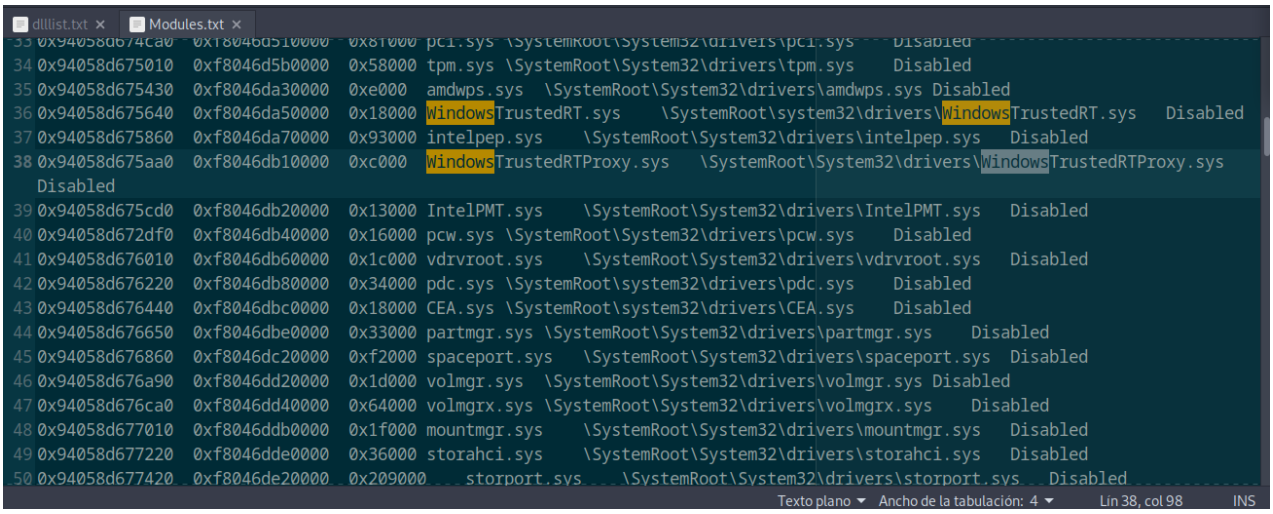
Figura 36

Se enumeran los módulos de kernel cargados en la memoria, lo cual ayuda a identificar controladores de dispositivos.

Nota: Captura desde Parrot OS donde se genera los módulos de kernel cargados.

Figura 37

Módulos del kernel que se encuentran cargados



Nota: Captura de pantalla del archivo con la respuesta de los módulos del kernel.

Hilos en windows: windows.threads.Threads

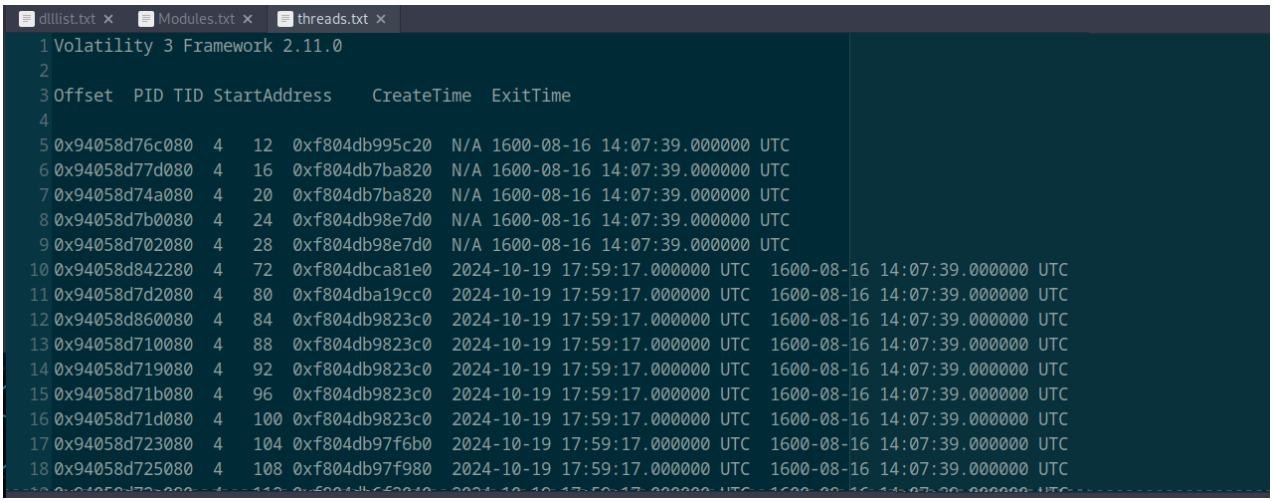
Figura 38

Se muestra los hilos activos en la memoria.

Nota: Captura desde Parrot OS donde se genera los hilos.

Figura *39*

Hilos activos en memoria



Nota: Captura de pantalla del archivo con la respuesta a el módulo del kernel.

Lista del mapa de memoria en windows: windows.memmap.Memmap

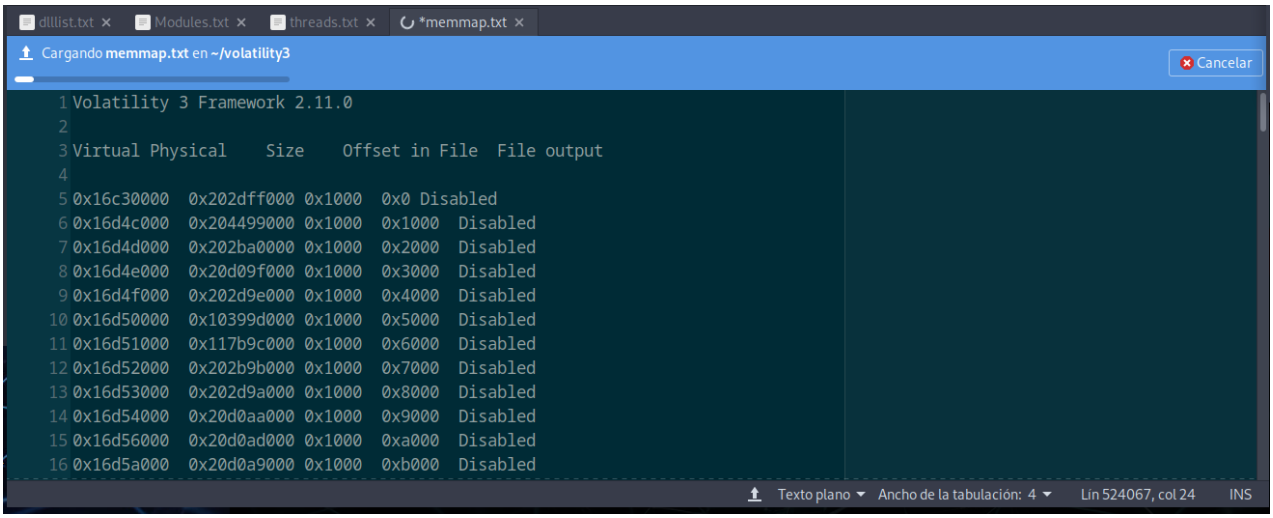
Figura 40

Muestra el mapeo de memoria, detallando qué partes de la memoria están asignadas a cada proceso.

Nota: Captura desde Parrot OS donde se genera el mapa de memoria del proceso.

Figura *41*

Muestra del mapeo de la memoria RAM



Nota: Captura de pantalla del archivo con la respuesta de la memoria RAM.

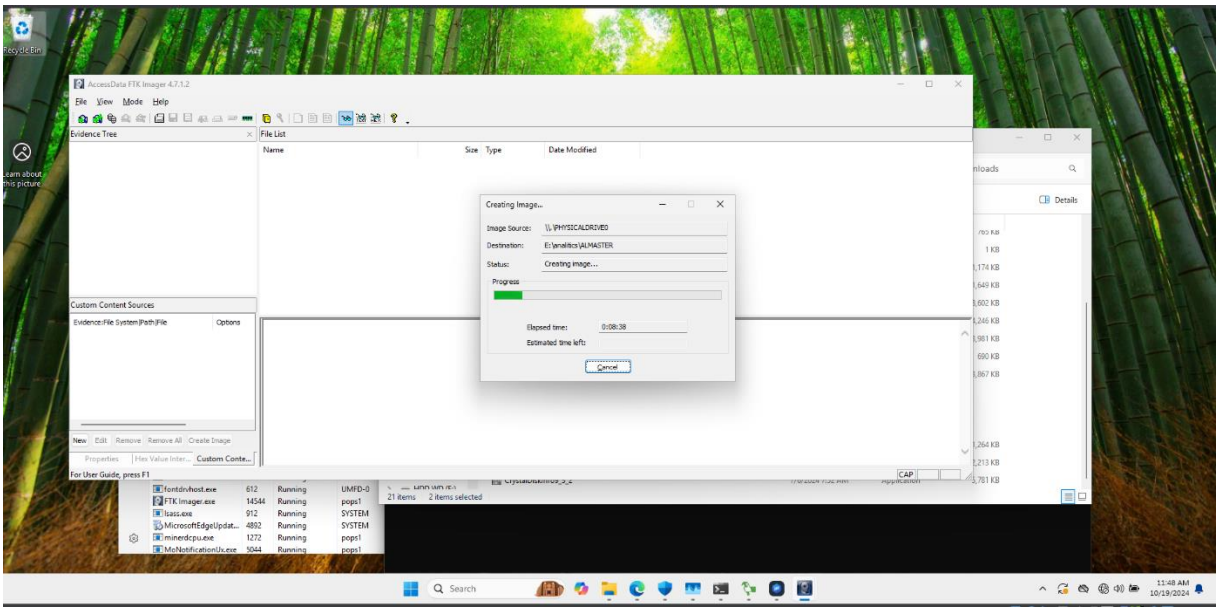
Revisión de la Integridad y Recuperación de Datos usando una Captura del Almacenamiento del Sistema

Se ha identificado la necesidad de realizar una revisión exhaustiva del disco del cliente mediante análisis de la memoria con la herramienta Volatility, complementada con un análisis detallado del disco utilizando Autopsy. Este análisis se enfoca en evaluar la integridad y recuperación de los archivos, abordando también la eliminación de datos de manera controlada y manual cuando es necesario. Autopsy está siendo utilizado como la herramienta principal para analizar los archivos, asegurando una revisión meticulosa y completa del sistema del cliente para detectar cualquier anomalía o evidencia forense relevante.

Generar Captura de la imagen usando FTK Imagener:

Figura 42

Captura de Disco del cliente con la herramienta FTK Imagener

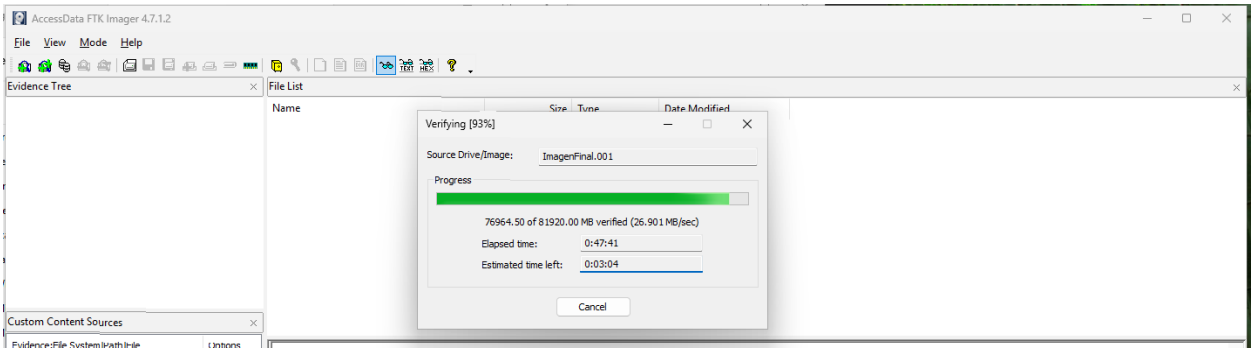


Nota: Captura de la pantalla del disco del cliente con la herramienta FTK imagener.

Tamaño del archivo 80 GB tiempo en ejecución 1:33:39.

Figura 43

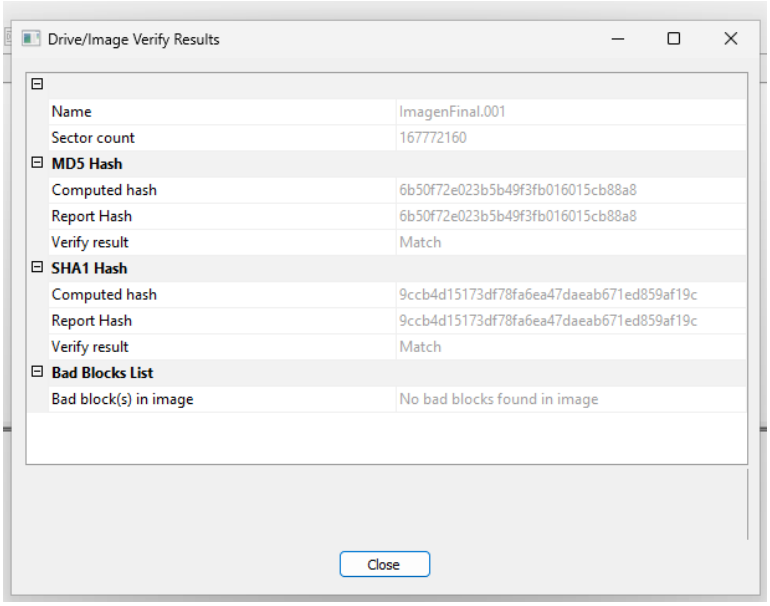
Captura exitosa del Disco del cliente con la herramienta FTK Imagener



Nota: Captura Exitosa del disco del cliente usando la herramienta FTK Imagener.

Figura *44*

Verificación de la imagen.



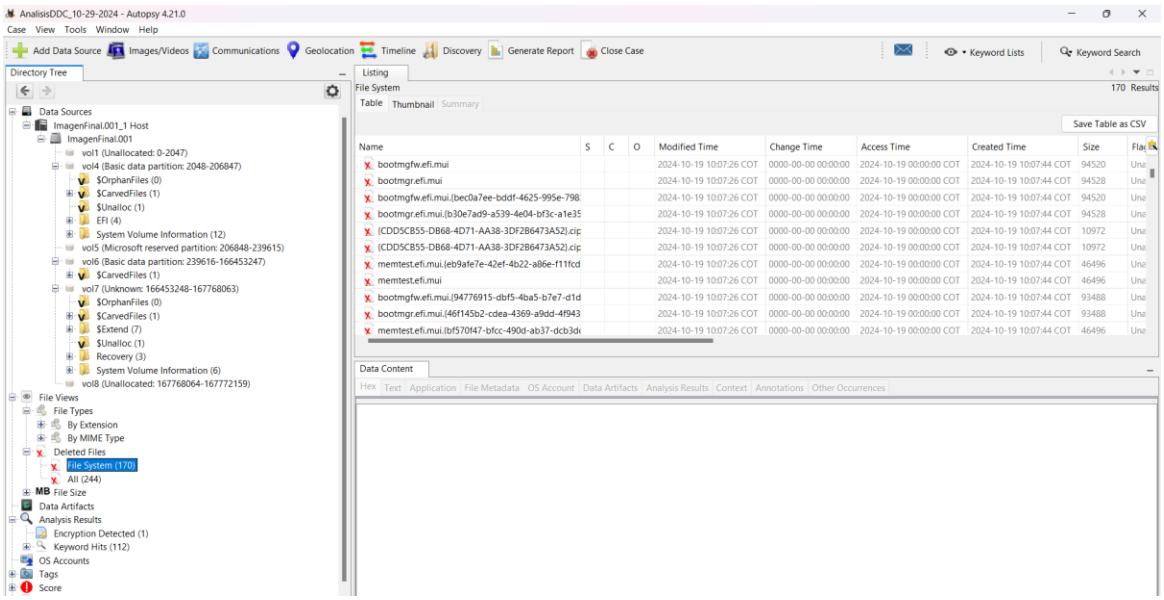
Nota: Detalle de la verificacion de la imagen una vez realiza su captura.

Análisis Usando la herramienta Autopsy 4.21.0

En el análisis forense llevado a cabo en el disco duro del cliente, se utilizó la versión 4.21.0 de Autopsy, una herramienta ampliamente reconocida en la comunidad de análisis forense digital. Este análisis permitió evaluar la integridad y el estado de múltiples volúmenes de datos, identificando tanto archivos activos como remanentes de archivos eliminados.

Figura 45

Autopsy análisis Disco Duro

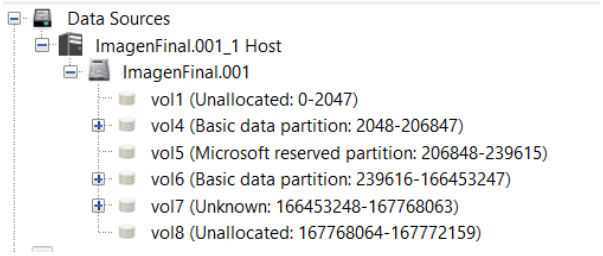


Nota: Captura de pantalla usando Autopsy para un analisis del disco del cliente.

La figura 45 proporciona una vista detallada del proceso de análisis de disco, mostrando los volúmenes en los cuales se detectaron elementos de interés forense, específicamente en ocho volúmenes correspondientes a datos del cliente.

Figura 46

Volúmenes disponibles

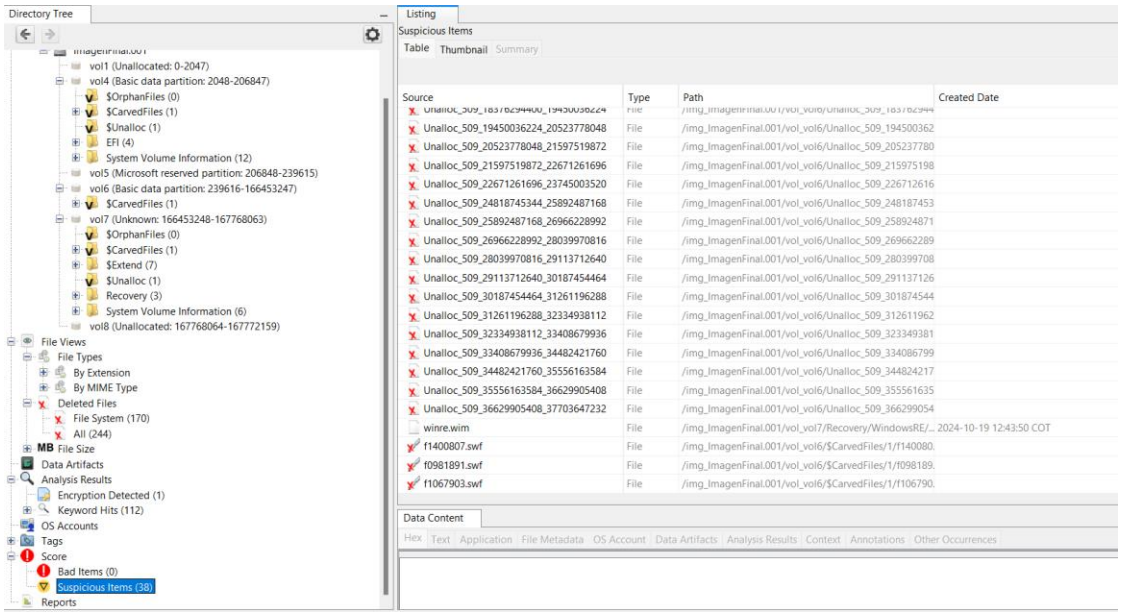


Nota: Volúmenes disponibles en la herramienta de autopsy

Siguiendo las especificaciones del cliente, se realizó un análisis exhaustivo del almacenamiento, tomando en cuenta todas las medidas forenses necesarias para preservar la integridad de los datos y asegurar la validez de los hallazgos. Durante el análisis, Autopsy generó directrices detalladas sobre el estado de cada archivo y alertas sobre posibles indicadores de infección en el sistema, resaltando archivos potencialmente alterados o infectados que representan riesgo para el cliente.

Figura *47*

Elementos Sospechosos en Autopsy



Nota: Captura de pantalla usando Autopsy para un analisis del disco del cliente.

En la Figura 47, se aprecia todos los elementos sospechosos que se encontraron usando la herramienta autopsy.

Hallazgos Relevantes:

Archivos .mui y .mui-slack: Se encuentran varias instancias de archivos relacionados con el arranque de Microsoft (bootmgfw.efi.mui y bootmgr.efi.mui), en su mayoría borrados. Los archivos "slack" indican fragmentos de datos sobrantes en el espacio no utilizado del archivo, posiblemente remanentes de archivos eliminados. Las fechas de creación y modificación están alineadas al 19 de octubre de 2024.

Archivos .dll y .cip: Archivos como "kd_02_1137.dll" (módulo de depuración) y archivos de políticas de integridad ({82443e1e-8a39...}.cip) se encontraron en la misma partición EFI. Algunos archivos .cip están duplicados en versiones "slack", sugiriendo una configuración de políticas de seguridad activa en el sistema.

Hash y permisos: Se registraron varios hashes MD5, aunque muchos archivos "slack" tienen valores hash nulos. Todos los archivos tienen permisos de lectura y escritura para el propietario y el grupo, lo que indica permisos permisivos en esta partición.

La recopilación y verificación forense de datos son altamente demandantes en términos de tiempo, almacenamiento y recursos de procesamiento. Este análisis depende directamente de la capacidad de almacenamiento disponible; si el espacio es insuficiente o si el equipo no está adecuadamente preparado para manejar grandes volúmenes de información, se pueden presentar retrasos o incluso pérdidas de datos críticos. La falta de almacenamiento adecuado y recursos de procesamiento impacta directamente en el tiempo de respuesta y en la precisión del análisis, lo que puede comprometer la integridad de la evidencia y la validez de los hallazgos forenses.

Estas limitaciones resaltan la importancia de contar con recursos técnicos suficientes y un plan de almacenamiento bien estructurado en los análisis forenses, especialmente cuando se manejan volúmenes grandes de datos o múltiples dispositivos.

Identificar Virus Instalado

Tabla 6

Análisis de archivo photo.scr

ID	CoinMiner; Trojan.BitCoinMiner
HASH 256	a17b0884e00bab93fa46a08043a5d972c3dd0cbc2331448e365b988dbc76843d
HASH MD5	02b62ba806003929e8fef1ec14471536
Nombre del archivo	• photo.scr • dttcodexgigas.dce5336d77e505f0e20dfb2e73fb99b0aa1779e2 • 64871489
Tipo de archivo	WIN32 EXE
Fecha de detección	2020 – 09 – 30
Hora de detección	21:44:00 UTC
Sistema Operativo	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Máquina Objetivo	Intel 386 or later processors and compatible processors
Tamaño del archivo	783101 bytes

Método de Infección	Método común de infección por un archivo de coin miner es a través de un programa aparentemente legítimo que se distribuye en sitios de descarga no oficiales. Un usuario puede descargar este software, creyendo que es útil o interesante. Sin embargo, al ejecutarlo, se instala un malware que utiliza los recursos del sistema para minar criptomonedas sin el conocimiento del usuario. Este tipo de infección a menudo se oculta en el proceso de instalación y puede deshabilitar o eludir medidas de seguridad, lo que permite que el miner funcione en segundo plano, consumiendo CPU y energía, y afectando el rendimiento general del equipo.

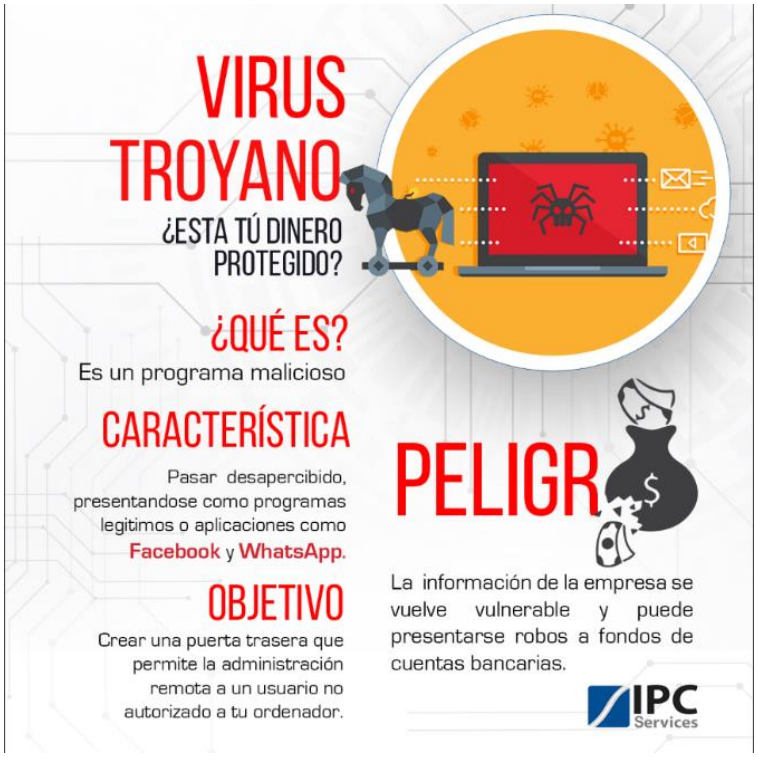
Nota: Esta tabla muestra el detalle de la aplicación que se ha instalado como tambien el detalle del sistema del metodo de infección.

Análisis del Malware Identificado

De acuerdo con la clasificación verificada por Any.run y las evidencias encontradas en el análisis del virus en bases de datos de malware como bazaar y CISCO TALOS este virus se clasifica como coin miner troyano en consecuencia (Kaspersky, 2024) la cual la destaca como: “El malware en esta familia usa secretamente la capacidad del procesador de una computadora infectada para generar criptomonedas (bitcoins).”

Figura 48

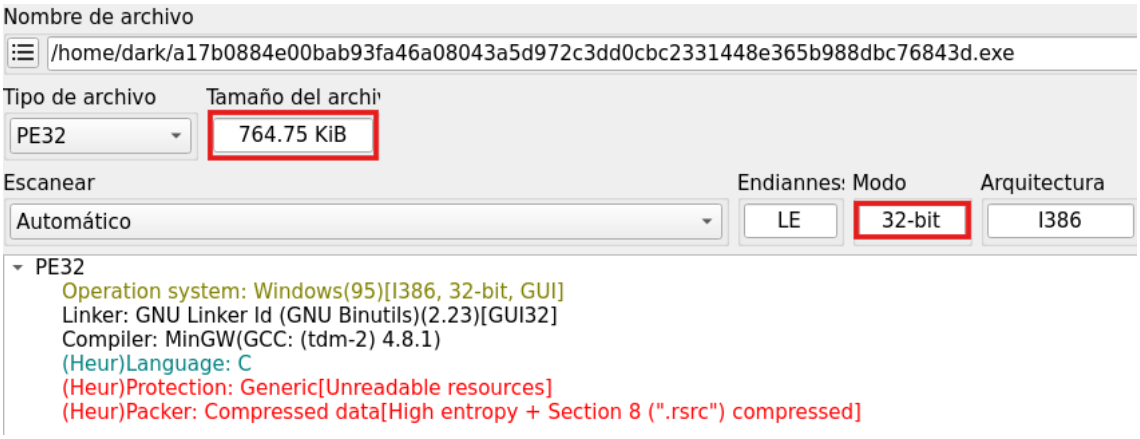
Gráfico ¿Qué es un virus Troyano? , por IPC Services.



Nota: Captura de virus troyano obtenida del navegador web.

Figura *49*

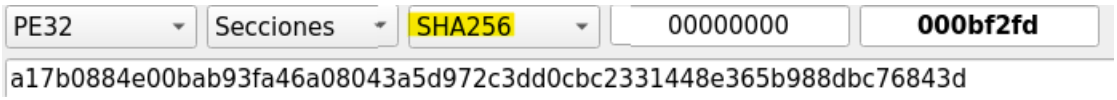
Tamaño y Tipo de archivo photo.scr



Nota: Captura de pantalla con la herramienta detect it easy pestaña general.

Figura *50*

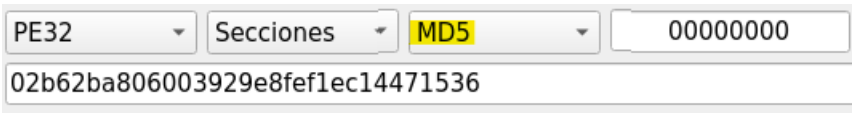
Hash 256 photo.scr



Nota: Captura de pantalla en la herramienta detect it easy seccón HASH.

Figura *51*

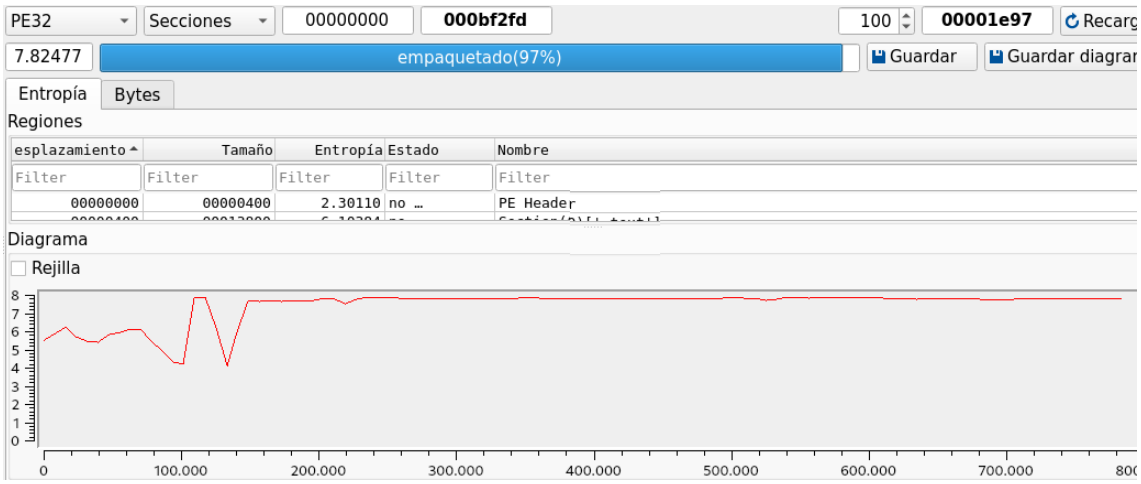
Hash MD5 archivo photo.scr



Nota: Captura de pantalla en la herramienta detect it easy seccón HASH.

Figura 52

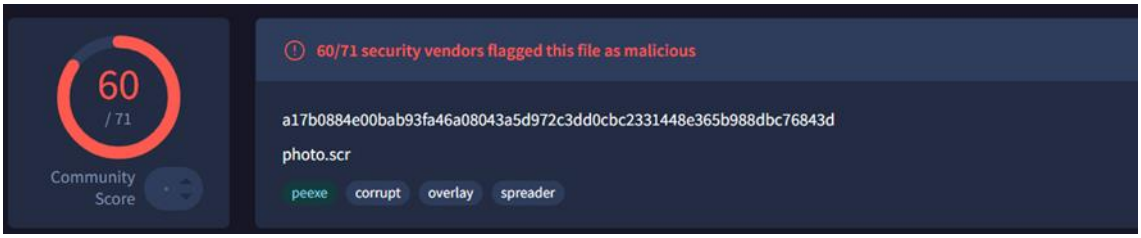
Entropía photo.scr



Nota: Captura de pantalla en la herramienta detect it easy sección entropía.

Figura 53

Ranking Virus Total photo.scr



Nota: Captura de pantalla usando la herramienta de virus total.

Tabla 7

Análisis archivo good.exe

ID	CoinMiner
HASH 256	4571f9310b1a27b245409e311b4de7fa6f620a18f1d3b98335e29b8d8f827150
HASH MD5	b353eef73cf06a89bf3d199050783f77
Nombre del archivo	• esyMiner_SetupVpn.exe • good.exe • 4571f9310b1a27b245409e311b4de7fa6f620a18f1d3b98335e29b8d8f827150.exe • payload_1.exe
Tipo de archivo	WIN64 EXE
Fecha de detección	2024 – 10 – 08
Hora de detección	01:01:35 UTC
Sistema Operativo	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Desarrollador	WireGuard LLC
Máquina Objetivo	AMD AMD64
Tamaño del archivo	1826816bytes
Método de Infección	Método común de infección por un archivo de coin miner es a través de un programa aparentemente legítimo que se distribuye en sitios de descarga no oficiales. Un usuario puede descargar este software, creyendo que es útil o interesante. Sin embargo, al ejecutarlo, se instala un malware que utiliza los recursos del sistema para minar criptomonedas sin el conocimiento del usuario. Este tipo de infección a menudo se oculta

> en el proceso de instalación y puede deshabilitar o eludir medidas de seguridad, lo que permite que el miner funcione en segundo plano, consumiendo CPU y energía, y afectando el rendimiento general del equipo.

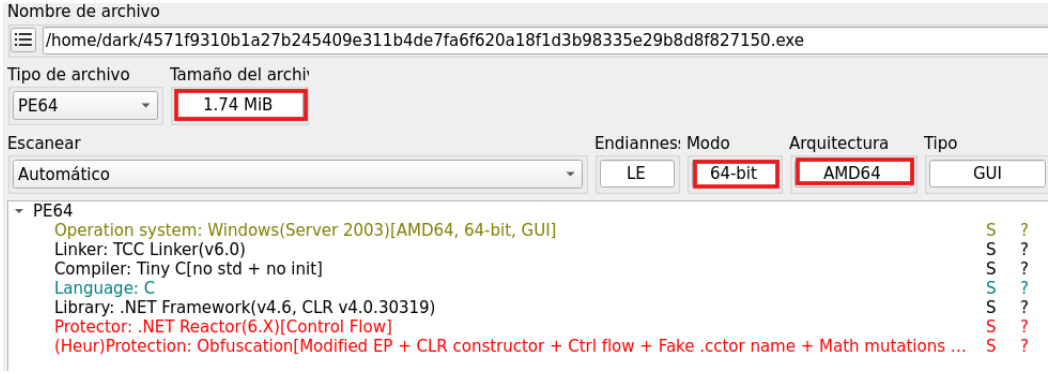
Nota: Esta tabla muestra el detalle de la aplicación que se ha instalado como tambien el detalle del sistema del metodo de infección.

- ✓ **Análisis del Malware Identificado**

Como se pudo analizar con el anterior malware, en este se puede clasificar de la misma forma como trojan coin miner debido a que pertenecen a la misma familia y causan los mismos efectos por lo que se clasifica dentro de un malware Coin Miner Troyano.

Figura 54

Tamaño y tipo de archivo good.exe

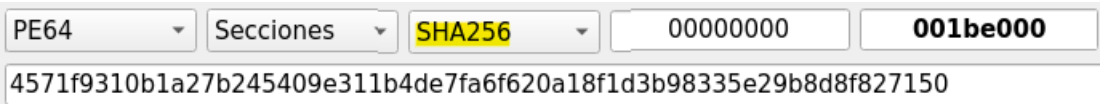


Nota: Captura de pantalla con la herramienta detect it easy pestaña general.

- ✓ Hash 256

Figura 55

HASH 256 good.exe

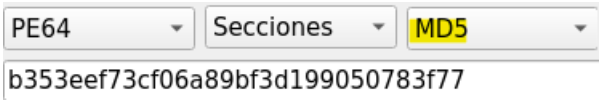


Nota: Captura de pantalla en la herramienta detect it easy sección HASH.

- ✓ Hash MD5

Figura 56

HASH MD5 good.exe

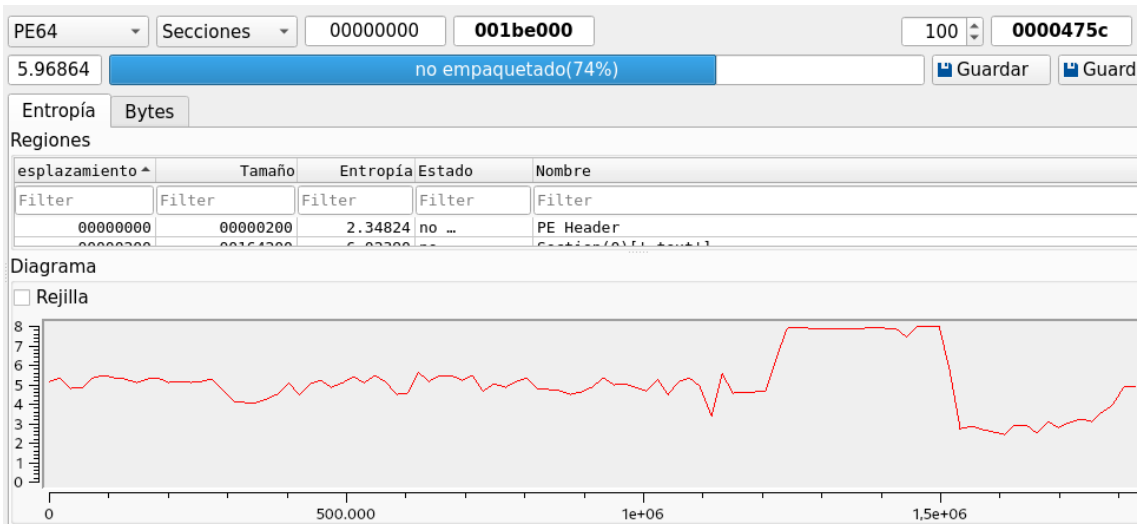


Nota: Captura de pantalla en la herramienta detect it easy sección HASH.

- ✓ Entropía

Figura 57

Entropía good.exe

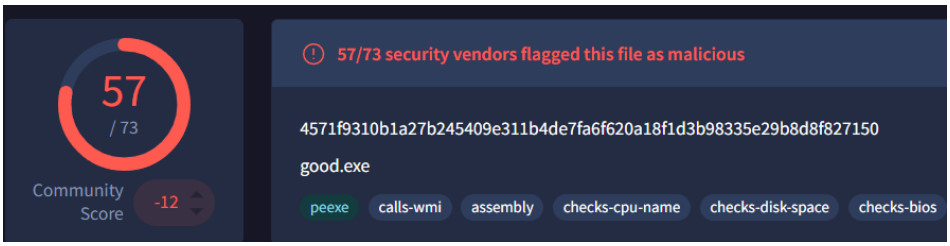


Nota: Captura de pantalla en la herramienta detect it easy sección entropía.

- ✓ Rating en Virus Total

Figura 58

Ranking en virus total good.exe



Nota: Captura de pantalla usando la herramienta de virus total.

Identificar Conexiones de la Red

Netstat (Network Statistics) es una utilidad de línea de comandos en Windows (y en otros sistemas operativos) que permite al usuario ver conexiones de red activas, puertos de escucha y estadísticas de red. Es útil para monitorear la actividad de red del sistema y verificar conexiones sospechosas. Los usuarios pueden ver detalles de las conexiones TCP, UDP y el estado de las mismas, ayudando en la detección de posibles intrusiones o anomalías de red.

Figura 59

Conexiones de red equipo Windows 11

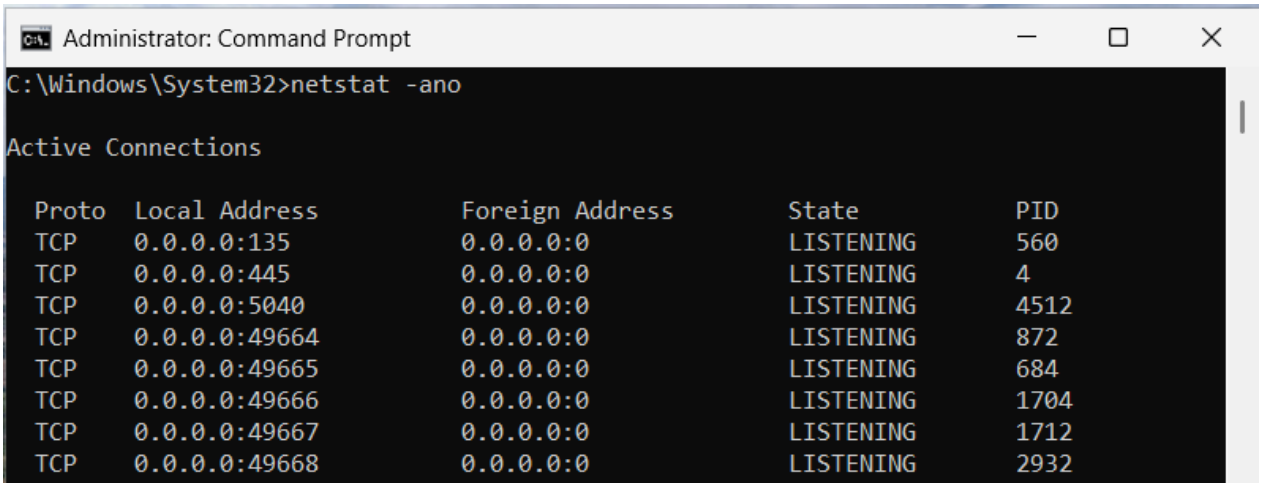
```
C:\Users\win11>netstat -v

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.0.2.15:49698        172.172.255.217:https  ESTABLISHED
  TCP    10.0.2.15:50035        a23-223-28-196:https   ESTABLISHED
  TCP    10.0.2.15:50064        192.16.49.85:http      CLOSE_WAIT
  TCP    [fd00::c1da:2085:9da8:8d40]:49996  [2620:1ec:bdf::41]:https  FIN_WAIT_2
```

Nota: Captura de pantalla usando el CMD del equipo para obtener información detallada y extensa sobre estadísticas de red y conexiones

Para realizar esta revisión nos vamos a servir del comando '*netstat -ano*', el cual nos proporciona información con respecto las conexiones de red actuales del sistema, las interfaces de red activas y los puertos abiertos. Este comando proporciona cinco columnas clave:

Figura 60

Conexiones de red de sistema Windows 11



Nota: Captura de pantalla usando el CMD del equipo para obtener información detallada sobre las conexiones de red y los puertos en uso.

Esto muestra todas las conexiones activas, las direcciones IP remotas y los PID de los procesos relacionados.

Conexiones de red antes de infección:

Tabla 8

Conexiones de red de sistema Windows antes de infección

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	560
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	4512

TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	872
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	684
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1704
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1712
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	2932
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	828
TCP	10.0.2.15:139	0.0.0.0:0	LISTENING	4
TCP	10.0.2.15:49707	172.172.255.217:443	ESTABLISHED	3236
TCP	10.0.2.15:49718	52.109.108.109:443	ESTABLISHED	1620
TCP	10.0.2.15:50026	23.212.150.29:443	ESTABLISHED	8612
TCP	10.0.2.15:50030	23.212.150.29:443	ESTABLISHED	8612
TCP	10.0.2.15:50065	181.112.12.16:80	ESTABLISHED	5124
TCP	10.0.2.15:50071	20.190.151.9:443	TIME_WAIT	0
TCP	10.0.2.15:50075	150.171.84.254:443	ESTABLISHED	1572
TCP	10.0.2.15:50076	192.16.49.85:80	ESTABLISHED	1572
TCP	10.0.2.15:50082	20.190.151.70:443	ESTABLISHED	3244
TCP	10.0.2.15:50083	23.223.28.206:443	ESTABLISHED	1572
TCP	10.0.2.15:50084	13.107.136.254:443	ESTABLISHED	1572
TCP	10.0.2.15:50085	13.107.213.254:443	ESTABLISHED	1572
TCP	10.0.2.15:50086	13.107.246.41:443	ESTABLISHED	1572
TCP	10.0.2.15:50087	204.79.197.222:443	ESTABLISHED	1572
TCP	[::]:135	[::]:0	LISTENING	560
TCP	[::]:445	[::]:0	LISTENING	4
TCP	[::]:49664	[::]:0	LISTENING	872
TCP	[::]:49665	[::]:0	LISTENING	684
TCP	[::]:49666	[::]:0	LISTENING	1704
TCP	[::]:49667	[::]:0	LISTENING	1712
TCP	[::]:49668	[::]:0	LISTENING	2932
TCP	[::]:49669	[::]:0	LISTENING	828
TCP	[fd00::5059:b492:4405:830d]:49778	[2600:1419:5600:7::5c7a:9d86]:443	FIN_WAIT_2	8832
TCP	[fd00::5059:b492:4405:830d]:49799	[2620:1ec:bdf::41]:443	FIN_WAIT_2	8832
TCP	[fd00::5059:b492:4405:830d]:50066	[2620:1ec:12::239]:443	ESTABLISHED	8832
TCP	[fd00::5059:b492:4405:830d]:50080	[2620:1ec:c11::239]:443	ESTABLISHED	8832
TCP	[fd00::5059:b492:4405:830d]:50081	[2620:1ec:bdf::41]:443	ESTABLISHED	8832
UDP	0.0.0.0:5050	*:*	4512	

UDP	0.0.0.0:5353	*:*	1928
UDP	0.0.0.0:5355	*:*	1928
UDP	0.0.0.0:51055	*:*	1928
UDP	10.0.2.15:137	*:*	4
UDP	10.0.2.15:138	*:*	4
UDP	10.0.2.15:1900	*:*	6024
UDP	10.0.2.15:49492	*:*	6024
UDP	127.0.0.1:1900	*:*	6024
UDP	127.0.0.1:49493	*:*	6024
UDP	127.0.0.1:51056	127.0.0.1:51056	3112
UDP	[::]:5353	*:*	1928
UDP	[::]:5355	*:*	1928
UDP	[::]:51055	*:*	1928
UDP	[::1]:1900	*:*	6024
UDP	[::1]:49491	*:*	6024
UDP	[fe80::f9a4:dd78:d78:fdeb%6]:1900	*:*	6024
UDP	[fe80::f9a4:dd78:d78:fdeb%6]:49490	*:*	6024

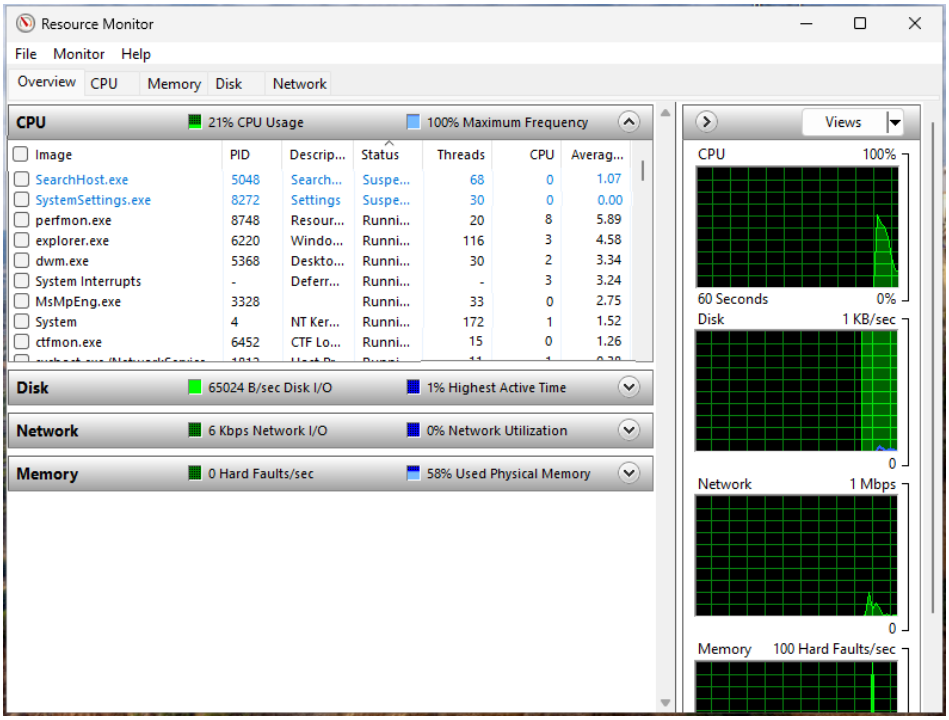
Nota: Esta tabla muestra el detalle de la red, cuando se ejecutan las conexiones de red de sistema Windows antes de infección.

Monitor de Recursos

En la pestaña de Red muestra actividad de red en tiempo real, con procesos y conexiones asociadas.

Figura 61

Monitor de recursos



Nota: Captura de pantalla usando el monitor de recursos en el sistema operativo windows.

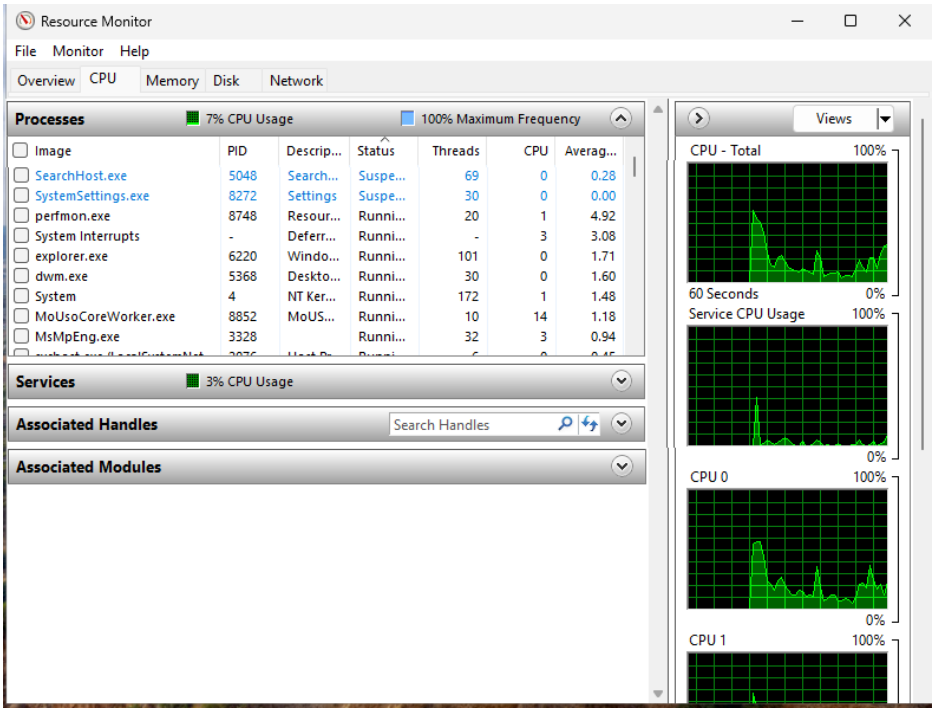
CPU

La pestaña CPU en el Resource Monitor de Windows 11 ofrece una visión detallada del uso del procesador y permite analizar el impacto de los procesos en la capacidad de procesamiento en tiempo real.

Es especialmente útil para identificar qué aplicaciones o procesos consumen más recursos y pueden estar afectando el rendimiento del sistema.

Figura 62

Sección CPU - Resource Monitoring



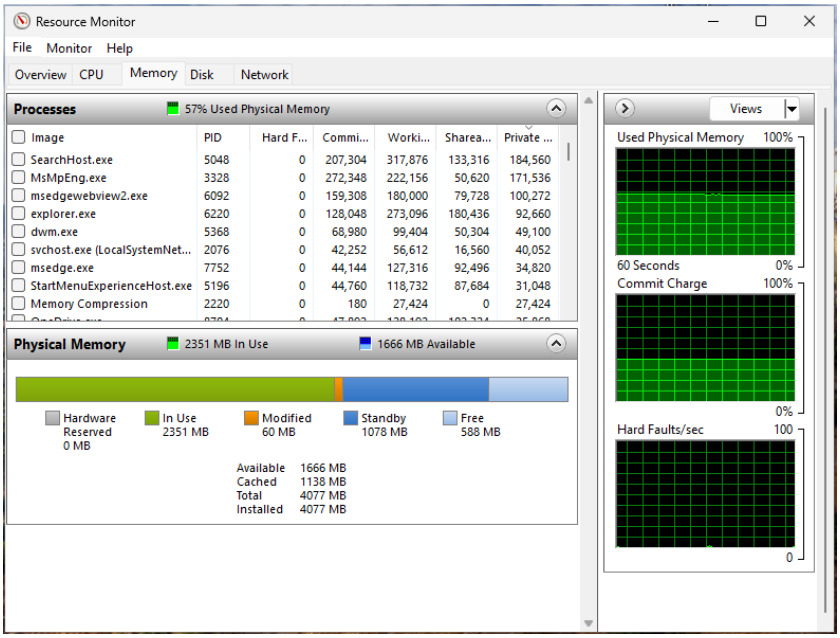
Nota: Captura de pantalla usando el monitor de recursos pestaña CPU en el sistema operativo windows.

Memory

Memory en el Resource Monitor de Windows 11 proporciona información detallada sobre el uso de la memoria física (RAM) en tiempo real. Esta pestaña es útil para entender cómo los procesos y aplicaciones en ejecución están utilizando la memoria, permitiendo identificar aquellos que podrían estar consumiendo demasiados recursos y afectando el rendimiento del sistema. (Khatri, 2015)

Figura 63

Sección Memory - Resource Monitoring



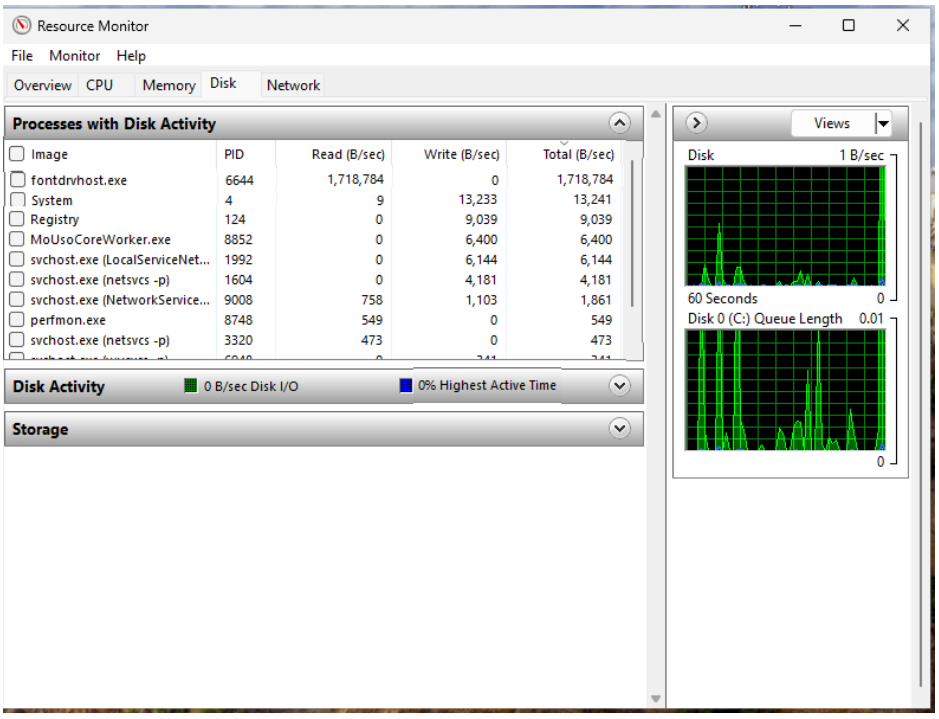
Nota: Captura de pantalla usando el monitor de recursos pestaña Memoria en el sistema operativo windows.

Disco

Disco en el Resource Monitor de Windows 11 ofrece una visión detallada del uso de los discos duros y SSD, permitiendo analizar cómo los procesos y aplicaciones están leyendo y escribiendo datos en el disco en tiempo real. Esta herramienta es muy útil para identificar procesos que podrían estar ralentizando el sistema debido a un uso intensivo de disco y para diagnosticar problemas de rendimiento relacionados con el almacenamiento. (Khatri, 2015)

Figura 64

Sección disco - Resource Monitoring



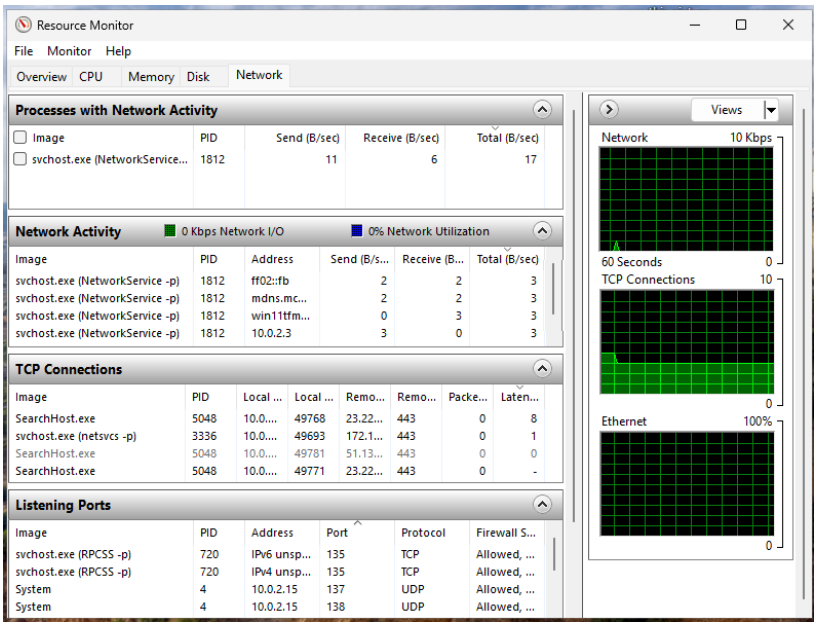
Nota: Captura de pantalla usando el monitor de recursos pestaña Disco en el sistema operativo windows.

Red

Red en el Resource Monitor de Windows 11 permite monitorear en tiempo real la actividad de red en el sistema, mostrando qué aplicaciones y procesos están utilizando la red, cuánto ancho de banda consumen y a qué direcciones remotas están conectadas. Esta información es esencial para diagnosticar problemas de conectividad, identificar aplicaciones que utilizan excesivamente la red, y detectar actividades de red sospechosas que podrían indicar presencia de malware o accesos no autorizados.

Figura 65

Sección Red - Resource Monitoring



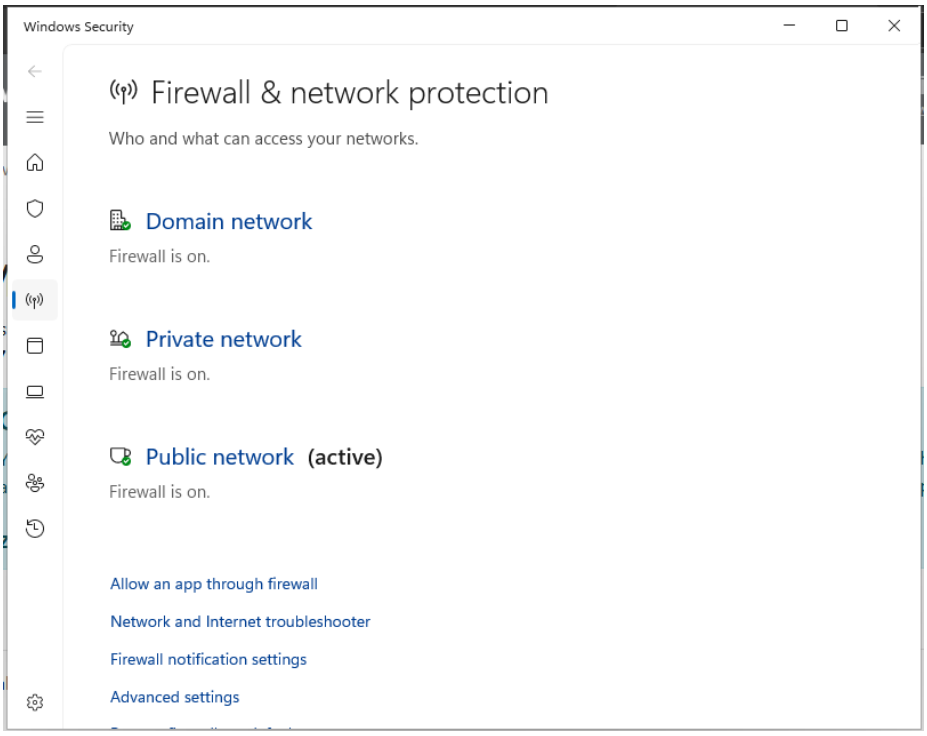
Nota: Captura de pantalla usando el monitor de recursos pestaña Red en el sistema operativo windows.

Configuración del Firewall

El Firewall de Windows 11 es una parte fundamental de la seguridad del sistema, encargada de monitorear y filtrar las conexiones de red para proteger el dispositivo contra accesos no autorizados y amenazas externas. Tener una configuración de firewall correcta es esencial para garantizar que el sistema esté seguro y solo permita conexiones confiables. (Naik, 2016)

Figura 66

Estado de Firewall & network protection



Nota: Captura de pantalla, de la configuración del firewall y protecciones de red.

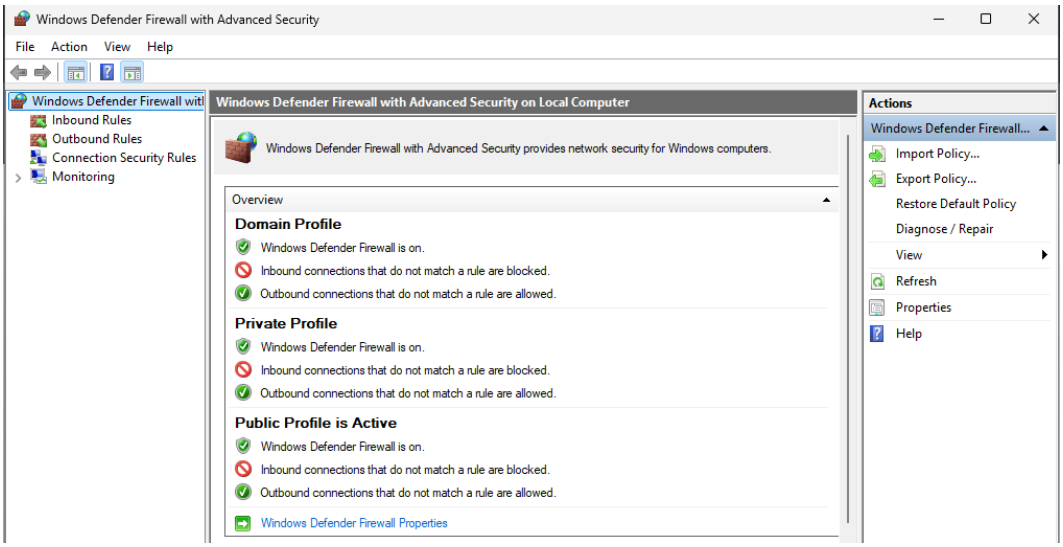
Windows Defender Firewall with Advanced Security

Windows Defender Firewall with Advanced Security en Windows 11 es una versión avanzada del firewall que permite configuraciones de seguridad y control de tráfico de red más detalladas que el Firewall básico. A través de esta herramienta, los administradores pueden crear reglas personalizadas para regular el tráfico de red entrante y saliente, controlar accesos de aplicaciones, servicios y usuarios, y definir configuraciones específicas para diferentes tipos de redes (públicas, privadas, y de dominio). Una

configuración correcta del Windows Defender Firewall Advanced Security garantiza la protección efectiva del sistema en varios niveles de la red. (Emmanuel, 2021)

Figura 67

Windows Defender Firewall with Advanced Security



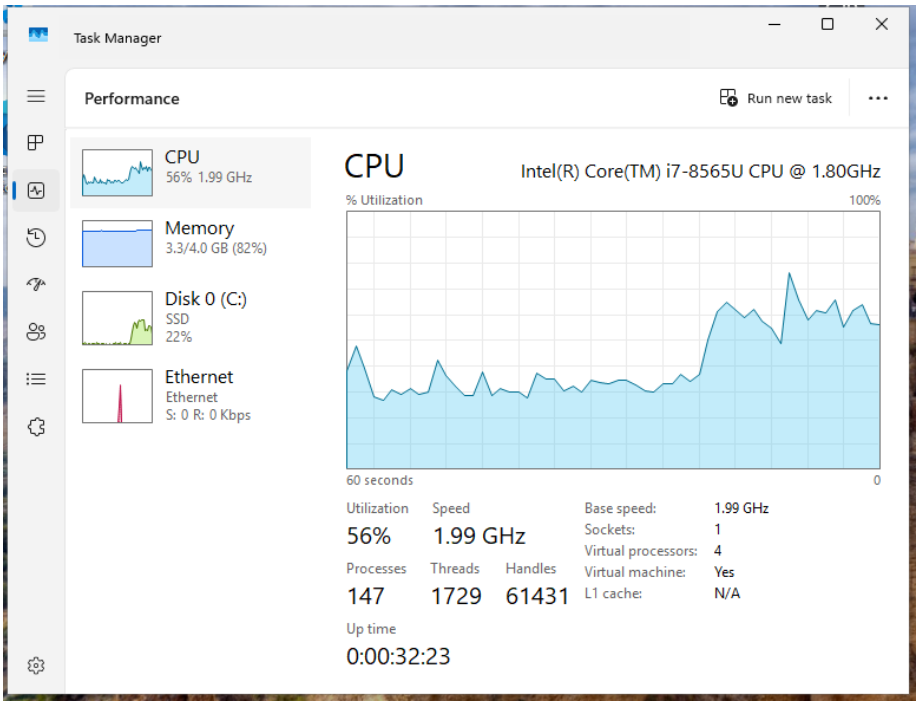
Nota**:** Captura de pantalla de la configuración de windows defender.

Administrador de Tareas

El Administrador de tareas de Windows 11 es una herramienta esencial para monitorear y gestionar el consumo de CPU en el sistema, proporcionando una visión en tiempo real de cómo los procesos y aplicaciones afectan el rendimiento. Ofrece una interfaz accesible para identificar qué programas están usando más recursos y ayuda a diagnosticar y solucionar problemas de rendimiento relacionados con el uso excesivo de CPU. En el Administrador de Tareas vamos a revisar la pestaña Procesos y Rendimiento para capturar información sobre procesos activos, su consumo de CPU y memoria. (Margosis, 2011)

Figura 68

Resumen de rendimiento - Administrador de tareas



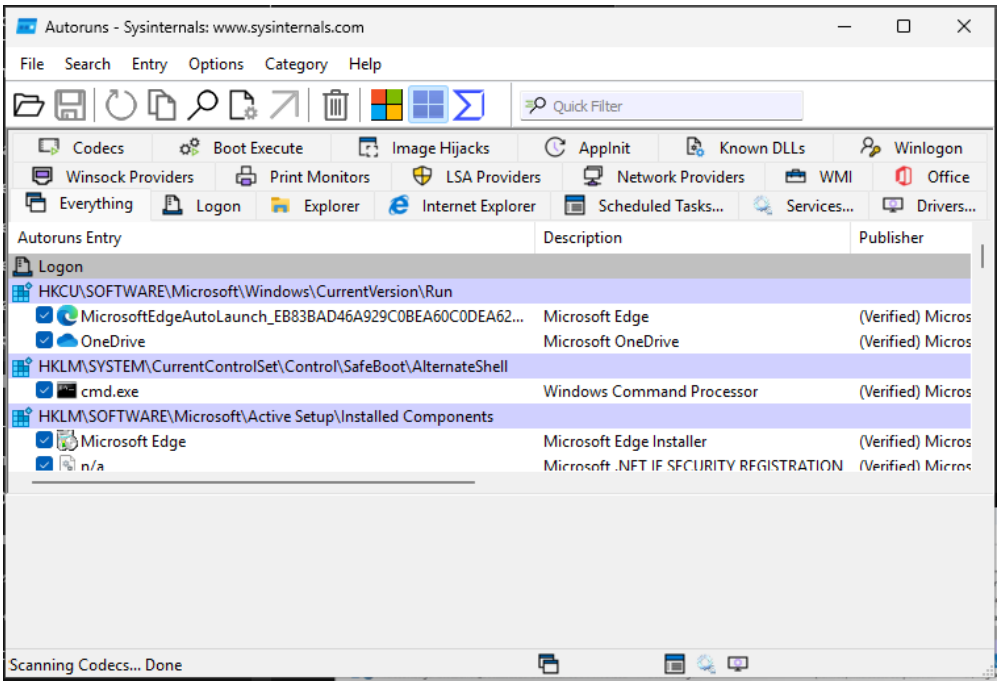
Nota: Captura de pantalla del administrador de tareas en widows 11.

Autoruns de Sysinternals

Autoruns es una herramienta avanzada de la suite Sysinternals de Microsoft, diseñada para proporcionar un control exhaustivo sobre todos los programas y servicios que se inician automáticamente en Windows. Esta herramienta permite a los usuarios y administradores ver y gestionar elementos de inicio en profundidad, identificando cualquier programa, servicio, controlador, o componente de sistema que se cargue automáticamente, lo que es fundamental para optimizar el rendimiento y la seguridad de un equipo. (Russinovich, 2012)

Figura 69

Resumen de información Autoruns de Sysinternals



Nota: Captura de pantalla usando la aplicación autoruns en windows.

Conexiones de red después de infección:

Tabla 9

Conexiones de red después de infección

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	720
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	4572
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	864
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	696
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1604
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1992
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	2936
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	840
TCP	10.0.2.15:139	0.0.0.0:0	LISTENING	4
TCP	10.0.2.15:49693	172.172.255.216:443	ESTABLISHED	3336

TCP	10.0.2.15:49791	23.39.223.11:443	FIN_WAIT_2	4616
TCP	10.0.2.15:49807	143.204.23.85:443	FIN_WAIT_2	4616
TCP	10.0.2.15:49836	35.245.40.102:443	FIN_WAIT_2	4616
TCP	10.0.2.15:49840	68.67.179.155:443	FIN_WAIT_2	4616
TCP	10.0.2.15:49866	20.201.52.37:443	FIN_WAIT_2	4616
TCP	10.0.2.15:49882	192.16.48.200:443	FIN_WAIT_2	4616
TCP	10.0.2.15:49885	191.237.206.80:443	FIN_WAIT_2	4616
TCP	10.0.2.15:50111	192.168.231.128:9876	FIN_WAIT_2	4616
TCP	10.0.2.15:50112	192.168.231.128:9876	FIN_WAIT_2	4616
TCP	10.0.2.15:50506	23.223.28.213:443	ESTABLISHED	5048
TCP	10.0.2.15:50507	204.79.197.222:443	ESTABLISHED	5048
TCP	10.0.2.15:50523	23.223.28.202:443	ESTABLISHED	5048
TCP	10.0.2.15:50524	23.223.28.202:443	ESTABLISHED	5048
TCP	10.0.2.15:50525	23.223.28.202:443	ESTABLISHED	5048
TCP	10.0.2.15:50526	23.223.28.202:443	ESTABLISHED	5048
TCP	10.0.2.15:50527	23.223.28.202:443	ESTABLISHED	5048
TCP	10.0.2.15:50528	23.223.28.202:443	ESTABLISHED	5048
TCP	10.0.2.15:50533	31.13.224.51:80	SYN_SENT	5344
TCP	[::]:135	[::]:0	LISTENING	720
TCP	[::]:445	[::]:0	LISTENING	4
TCP	[::]:49664	[::]:0	LISTENING	864
TCP	[::]:49665	[::]:0	LISTENING	696
TCP	[::]:49666	[::]:0	LISTENING	1604
TCP	[::]:49667	[::]:0	LISTENING	1992
TCP	[::]:49668	[::]:0	LISTENING	2936
TCP	[::]:49669	[::]:0	LISTENING	840
TCP	[fd00::2987:5e0f:4933:22d9]:49808	[2800:370:0:50::b570:c10]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:49809	[2620:1ec:bdf::41]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:49821	[2600:1419:5600:18c::356e]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:49827	[2600:1419:5600:7::5c7a:9d9d]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:49832	[2a04:4e42:49::300]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:49833	[2600:1f18:4e9:5a02:8e76:58ea:e2c:7d59]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:49864	[2600:1419:5600:192::3544]:443	FIN_WAIT_2	4616

TCP	[fd00::2987:5e0f:4933:22d9]:49868	[2600:1419:5600:184::356e]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:49871	[2800:370:0:50::b570:c0b]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:49948	[2800:370:0:50::b570:c10]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:49958	[2600:1419:5600:7::5c7a:9d9c]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:49975	[2a03:2880:f32f:121:face:b00c:0:167]:443	FIN_WAIT_2	4616
TCP	[fd00::2987:5e0f:4933:22d9]:50066	[2a03:2880:f202:d0:face:b00c:0:167]:443	FIN_WAIT_2	4616
UDP	0.0.0.0:5050	*:*	4572	
UDP	0.0.0.0:5353	*:*	1812	
UDP	0.0.0.0:5355	*:*	1812	
UDP	0.0.0.0:57626	*:*	1812	
UDP	0.0.0.0:62581	*:*	1812	
UDP	0.0.0.0:62667	*:*	1812	
UDP	10.0.2.15:137	*:*	4	
UDP	10.0.2.15:138	*:*	4	
UDP	10.0.2.15:1900	*:*	8964	
UDP	10.0.2.15:62829	*:*	8964	
UDP	127.0.0.1:1900	*:*	8964	
UDP	127.0.0.1:57627	127.0.0.1:57627	3248	
UDP	127.0.0.1:62830	*:*	8964	
UDP	[::]:5353	*:*	1812	
UDP	[::]:5355	*:*	1812	
UDP	[::]:57626	*:*	1812	
UDP	[::]:62581	*:*	1812	
UDP	[::]:62667	*:*	1812	
UDP	[::1]:1900	*:*	8964	
UDP	[::1]:62828	*:*	8964	
UDP	[fe80::f9a4:dd78:d78:fdeb%6]:1900	*:*	8964	
UDP	[fe80::f9a4:dd78:d78:fdeb%6]:62827	*:*	8964	

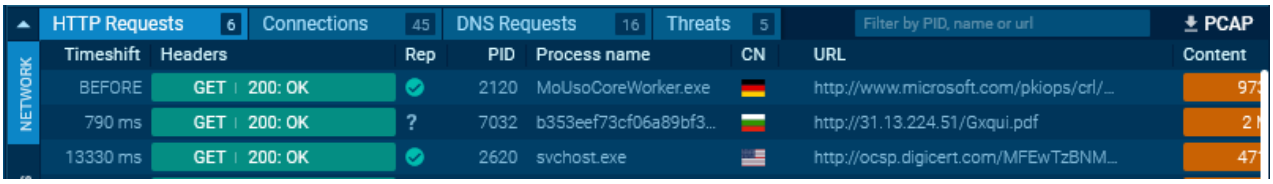
Nota: Esta tabla muestra, las conexiones de red después de infección.

Tras comparar las dos tablas de conexiones de red se puede observar una dirección IP relacionada a actividades maliciosas y que no se encontraba antes de la infección, de esta manera se

evidencia que hay comunicación hacia un servidor externo que tiene relación con el malware con el que fue infectado el equipo objetivo.

Figura 70

Conexiones de red identificado con malware desde sandbox



Nota: Captura de pantalla identificado las conexiones con el malware ejecutandose.

También se puede observar que la dirección IP (31[.]13[.]224[.]51) se encuentra reportada en bases de datos públicas de direcciones IP maliciosas (abuseipdb).

Figura 71

Dirección IP reportada en sitio abuseipdb

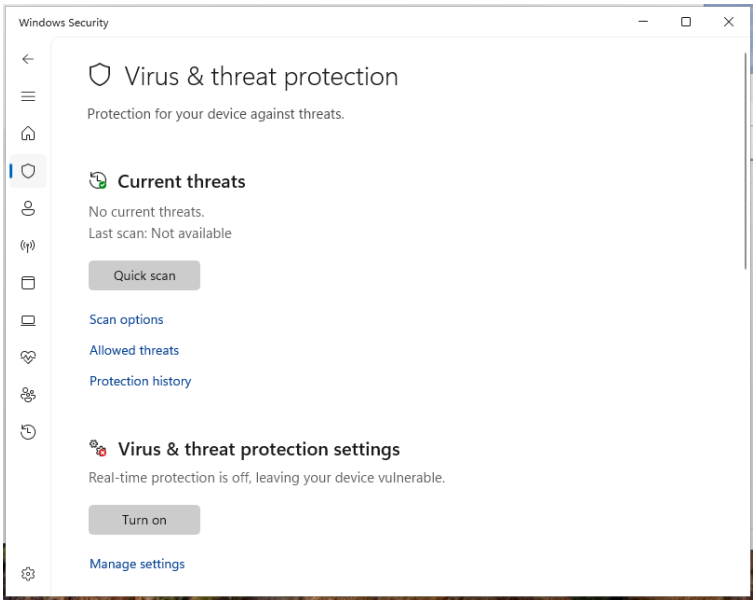
Nota: Captura de pantalla, de la IP reportada en abuseipdb.

Windows Defender

Tras la infección se puede evidenciar que la protección antivirus nativa de Windows sigue activa y no ha detectado la muestra de malware.

Figura 72

Configuración Windows Defender tras infección



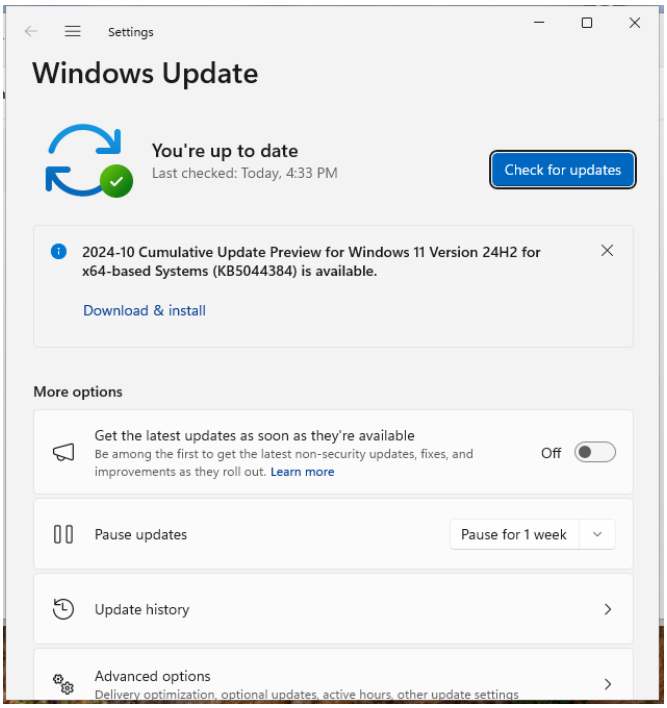
Nota: Captura de pantalla de la configuración de Virus y protecciones en windows security.

Windows Update

En la configuración de actualizaciones de Windows también podemos notar como el sistema infectado se encuentra con las actualizaciones al día.

Figura 73

Configuración Windows Update tras infección



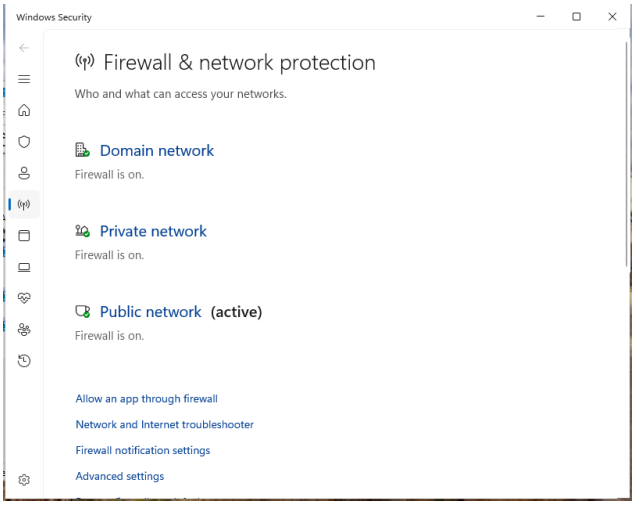
Nota: Captura de pantalla de la configuración de windows update posterior a la infección.

Configuración del Firewall

Las configuraciones de firewall nativo de Windows se pueden observar con todos sus componente activos por lo que podemos afirmar que le sistema cuenta con la protección de firewall.

Figura 74

Configuración firewall nativo de Windows 11 tras infección



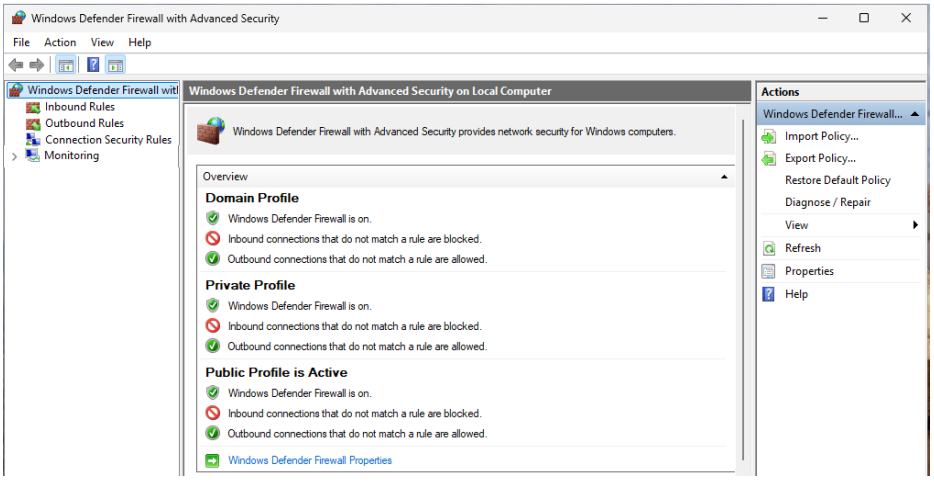
Nota: Captura de la Configuración del firewall y protecciones de red en windows.

Windows Defender Firewall con seguridad avanzada

De la misma manera se puede observar que la configuración de Windows Defender Firewall se encuentra activa y con las configuraciones por defecto habilitadas.

Figura 75

Configuración Windows Defender Firewall con seguridad avanzada



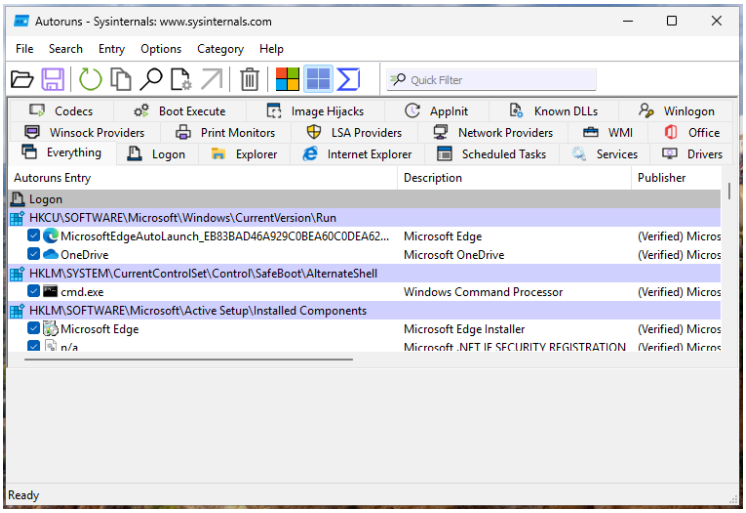
Nota: Captura de pantalla de la configuracion de windows defender Firewall.

Autoruns de Sysinternals

En análisis de la herramienta Autoruns de Sysinternals no se evidencian comportamientos maliciosos como actividades sospechosas de login o llaves de registro para aplicaciones externas al sistema operativo.

Figura 76

Información de Autoruns sysinternals después de la infección



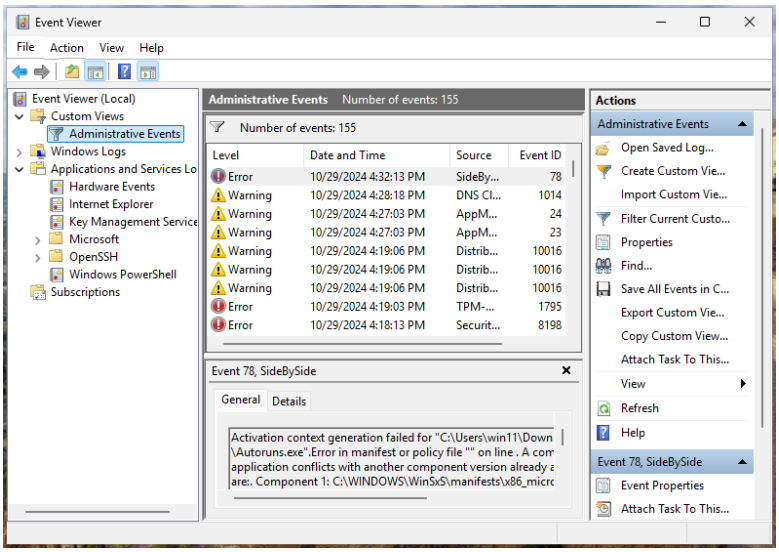
Nota: Captura de pantalla con Autoruns

Visor de eventos

Revisando la información que proporciona el visor de eventos de la máquina infectada inicialmente no se puede identificar cambios o eventos sospechosos que puedan estar relacionados al malware recientemente ejecutado en la máquina objetivo.

Figura 77

Información de visor de eventos tras la ejecución de la infección

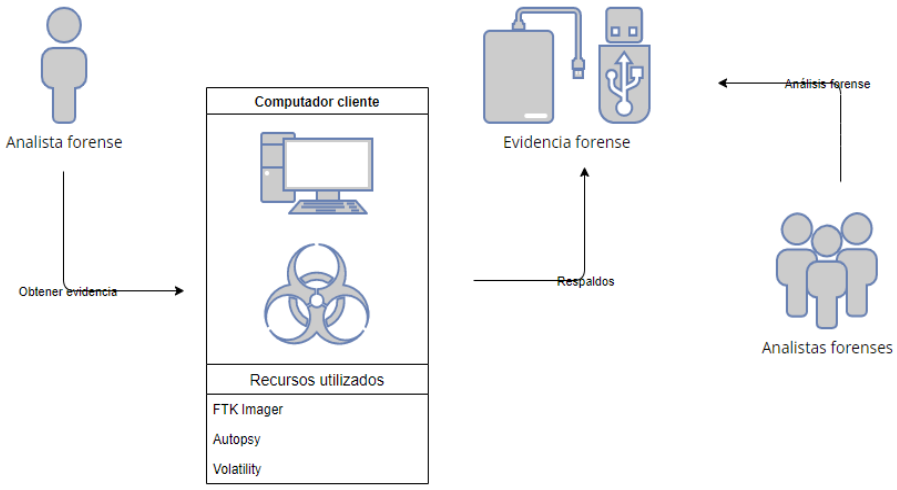


Nota: Captura de pantalla de la Información del visor de eventos en windows.

Esquema de Laboratorio Realizado

Figura 78

Proceso de recolección y análisis de evidencia forense



Nota: Gráfico creado sobre el proceso de recolección de análisis de evidencia forense.

Relacionado a hablar del laboratorio realizado en el presente TFM debemos mencionar el rol que cumple la cadena de custodia con respecto a la investigación como un proceso esencial para asegurar la preservación, manejo y documentación de la evidencia digital de manera adecuada y segura, esto siempre considerando el inicio de la cadena de custodia a partir del momento en que se obtiene la evidencia digital hasta que es presentada en un tribunal o durante una investigación. Por la naturaleza del proceso sea vital garantizar una correcta cadena de custodia para lograr de esta manera que la evidencia digital sea admisible y confiable.

Entre los elementos clave que podemos mencionar con respecto a aspectos clave de la cadena de custodia tenemos los siguientes:

- Identificación de la evidencia: Añadir todos los detalles e información relevante con respecto a la evidencia digital.
- Adquisición: Se debe garantizar que no se altere el estado original de los datos. Es importante verificar hashes de las muestras obtenidas.
- Documentación: Se hace necesario registrar y documentar a todas las personas que interactúen con las evidencias digitales. Se debe incluir datos de la persona o analista forense, fechas, horas, lugares, tipo de almacenamiento, etc.
- Almacenamiento seguro: La evidencia debe ser almacenada en un lugar seguro y protegido contra accesos no autorizados para garantizar que no se altere ni se dañe.
- Transferencia de evidencia: Cada vez que la evidencia cambie de manos, debe ser documentado en un registro de cadena de custodia. Esto puede incluir múltiples personas (peritos forenses,

personal de seguridad, investigadores, etc.), pero cada transferencia debe seguirse de cerca y documentarse con el propósito de mantener la integridad del proceso.

- Presentación en juicio o proceso legal: La documentación completa y clara de la cadena de custodia es vital para que un tribunal acepte la evidencia como válida. Si se rompe la cadena de custodia o hay lagunas en su documentación, la evidencia podría ser inadmisible o ser puesta en duda.

Soluciones y Mejoras al Cliente

Solución Reinicios en Windows

A continuación, se detalla las posibles soluciones y mejoras:

Problemas de Hardware

- **Sobrecalentamiento**:
    - **Solución**: Usar herramientas de monitoreo como HWMonitor o AIDA64 para controlar las temperaturas en tiempo real. Si las temperaturas son elevadas (por ejemplo, >90°C para la CPU), limpia los ventiladores o mejora la refrigeración.
- **Fallos en la Fuente de Alimentación (PSU)**:
    - **Solución**: Probar otra fuente de alimentación o utilizar una herramienta de diagnóstico de hardware.
- **Problemas con la Memoria RAM**:
    - **Solución**: Ejecutar **Windows Memory Diagnostic** (mdsched.exe) o **MemTest86** para detectar fallos en los módulos de RAM.

- **Disco Duro o SSD Dañado**:
    - **Solución**: Verificar el estado del disco con herramientas como **CrystalDiskInfo** o ejecutar chkdsk para corregir errores en el disco.

Controladores de Dispositivo Mal Funcionando

- **Controladores Incorrectos o Corruptos**:
    - **Solución**: Usar el **Administrador de dispositivos** para identificar controladores con problemas (iconos de advertencia) y actualízalos o reinstálalos desde el sitio web del fabricante.
- **Drivers de GPU**:
    - **Solución**: Instalar la versión más reciente del controlador de la GPU (NVIDIA, AMD, Intel) o retrocede a una versión anterior si los problemas comenzaron después de una actualización.

Software o Aplicaciones Conflictivas

- **Actualizaciones del Sistema**:
    - **Solución**: Verificar en **Configuración > Actualización y seguridad** si hay actualizaciones pendientes o fallidas y realizar una instalación limpia.
- **Aplicaciones de Terceros**:
    - **Solución**: Revisar el **Visor de Eventos** y el **Administrador de tareas** para identificar qué aplicaciones estaban activas antes de los reinicios. Prueba desinstalar o reinstalar esas aplicaciones.

- **Malware**:
    - **Solución**: Realizar un escaneo profundo con **Windows Defender Offline** o una herramienta antivirus especializada como **Malwarebytes**.

Errores en el Registro del Sistema

- **Entradas de Registro Corruptas**:
    - **Solución**: Usar una herramienta como **CCleaner** (con cuidado) o restaurar una copia del Registro desde el **Punto de Restauración**.

Configuración Incorrecta de Energía

- **Opciones de energía mal configuradas**:
    - **Solución**: Revisar la configuración de energía en **Configuración > Sistema > Energía y suspensión** y ajustar los valores.

Error de Pantalla Azul (BSOD)

- **Errores Críticos del Sistema (BSOD)**:
    - **Solución**: Revisar los códigos de error del BSOD en el **Visor de Eventos** o usa herramientas como **BlueScreenView** para analizar los minivolcados y determinar la causa exacta.

Actualización de BIOS

- **BIOS Obsoleto o Mal Configurado**:

- **Solución**: Consultar el fabricante de la placa base para actualizar el BIOS a la última versión.

Diagnóstico y Solución

Para determinar la causa de los reinicios, se recomienda seguir el siguiente flujo de trabajo:

Revisar los Registros de Eventos:

- Usar el **Visor de Eventos** de Windows (eventvwr.msc) para identificar cualquier evento crítico o advertencias justo antes del reinicio.

Monitorear la Temperatura del Sistema:

- Ejecutar una herramienta de monitoreo de hardware y verificar las temperaturas mientras el equipo está bajo carga.

Revisar Controladores:

- Utilizar el Administrador de Dispositivos para verificar controladores defectuosos o desactualizados.

Realizar Escaneos de Malware:

- Ejecutar un análisis completo de malware y utiliza software forense para detectar actividades sospechosas.

Test de Memoria RAM y Disco Duro:

- Usa **MemTest86** y herramientas de diagnóstico de disco para detectar fallos de hardware.

Pruebas de Estrés del Sistema:

- Ejecutar pruebas de estrés en CPU, GPU y RAM para detectar problemas de estabilidad bajo cargas intensas.

Acciones para corregir problemas causados por una incorrecta actualización del Sistema Operativo Windows 11:

Restauración del sistema: Utilizar la opción de "Restaurar sistema" para regresar a un punto anterior a la actualización problemática. Esto puede revertir los cambios que generaron la inestabilidad.

Desinstalar actualizaciones recientes: Ir a Configuración > Actualización y seguridad > Historial de actualizaciones y desinstalar la actualización más reciente si el problema comenzó tras una actualización específica.

Reparar archivos del sistema: Ejecutar los comandos sfc /scannow y DISM /Online /Cleanup-Image /RestoreHealth en el Símbolo del sistema (CMD) con privilegios de administrador para detectar y reparar archivos corruptos del sistema.

Actualizar controladores: Revisar y actualizar los controladores, especialmente los de gráficos, red y chipset, desde el sitio web del fabricante o mediante el Administrador de dispositivos para evitar conflictos con la actualización de Windows.

Realizar una reinstalación limpia de Windows 11: Si los problemas persisten, considerar una reinstalación limpia del sistema. Asegurarse de respaldar tus datos antes de proceder.

Desactivar actualizaciones automáticas: Temporalmente, desactivar las actualizaciones automáticas para evitar que se reinstale la actualización problemática hasta que Microsoft publique una solución.

Solución al Análisis de la Máquina Recursos, Cambio de Navegador, Activar Protecciones

Escaneo Completo del Sistema: Utilizar un antivirus actualizado para ejecutar un análisis completo del sistema y eliminar cualquier amenaza detectada. Se recomienda considerar soluciones de seguridad avanzadas que incluyan protección en tiempo real y funciones de eliminación de malware.

Optimización de Recursos: Revisar y ajustar el uso de recursos del sistema deshabilitando aplicaciones innecesarias en segundo plano, lo que mejorará el rendimiento general y reducirá la carga en la memoria y el CPU, permitiendo que las herramientas de seguridad funcionen de manera óptima.

Cambio de Navegador y Configuración Segura: Si el virus afecta el navegador actual, instalar uno diferente y asegurar su configuración de privacidad y seguridad. Esto incluye activar bloqueadores de anuncios y extensiones de seguridad para minimizar el riesgo de futuros ataques a través de sitios web maliciosos.

Activación de Protección Avanzada de Windows: Habilitar las características de seguridad de Windows 11, como Windows Defender, el control de aplicaciones y el acceso controlado a carpetas para proteger archivos críticos de posibles amenazas. Además, verificar que el firewall esté activado y configurado correctamente.

Actualización del Sistema y Software: Asegurarse de que Windows y todos los programas estén actualizados a la última versión para corregir vulnerabilidades de seguridad.

Estimado cliente, tras el análisis de su equipo con Windows 11, hemos detectado un virus que requiere atención inmediata. La solución incluye realizar un escaneo completo con un antivirus actualizado, optimizar el uso de recursos del sistema, cambiar a un navegador seguro, activar todas las protecciones avanzadas de Windows y actualizar el sistema y el software. Estas acciones no solo eliminarán la amenaza actual, sino que fortalecerán la seguridad de su equipo para prevenir futuras infecciones.

Solución y Entendimiento de los Procesos que están Actualmente en la Memoria Ram.
Identificación y Análisis de Procesos

Use el Administrador de Tareas para identificar procesos que consumen un 19.5% de CPU y 14.0 MB de RAM, verificando sus detalles (nombre, ubicación y función). Esto permite determinar si se trata de aplicaciones necesarias o si pueden ser optimizadas o cerradas.

Evaluación de Procesos Críticos y No Críticos: Clasifique los procesos según su importancia en el sistema. Algunos procesos esenciales pueden requerir altos recursos, pero si detecta aplicaciones desconocidas o innecesarias con un consumo elevado, podrían indicar un problema.

Control de Aplicaciones en Segundo Plano: Limite aplicaciones que se ejecutan automáticamente en segundo plano y no son esenciales, deshabilitándolas desde la Configuración de Inicio. Esto puede reducir la carga tanto en CPU como en RAM.

Optimización y Seguridad del Sistema: Asegúrese de que el sistema esté actualizado y cuente con una solución antivirus activa para evitar que procesos maliciosos se ejecuten en segundo plano, ya que estos pueden consumir recursos innecesariamente.

Estimado cliente, hemos identificado procesos que están consumiendo un alto porcentaje de CPU y RAM en su equipo, lo cual puede afectar su rendimiento. La solución incluye analizar y clasificar estos procesos para determinar su importancia, deshabilitar aplicaciones en segundo plano no esenciales, y optimizar el sistema mediante actualizaciones y un antivirus actualizado. Esto permitirá liberar recursos y mejorar significativamente el rendimiento de su equipo.

Solución Presencia del Malware en el Equipo

Si los reinicios inesperados en un sistema operativo Windows 11 son causados por un virus o malware**,** esto suele deberse a que el software malicioso está afectando procesos críticos del sistema operativo, modificando configuraciones o consumiendo excesivamente recursos, lo que genera inestabilidad y fallos. El malware puede inyectarse en archivos del sistema, corromper registros, o incluso intentar deshabilitar funciones de seguridad.

Cómo los virus causan reinicios inesperados

- Consumo excesivo de recursos**:** Algunos virus, especialmente los asociados a minería de criptomonedas **o** botnets, consumen altos niveles de CPU, memoria o energía, lo que puede llevar al sobrecalentamiento y a reinicios automáticos como medida de protección del hardware.
- Modificación de archivos del sistema**:** Los virus pueden alterar archivos críticos de Windows, como ntoskrnl.exe, winlogon.exe, o configuraciones del Registro, que son esenciales para el

correcto funcionamiento del sistema.

- Sobrecarga en el inicio o servicios de fondo: Algunos virus se ejecutan como servicios ocultos o entradas de inicio, provocando fallos al intentar cargar procesos dañados o maliciosos.
- Deshabilitación de servicios críticos**:** El malware puede deshabilitar servicios importantes como Windows Defender, el Firewall, o incluso funciones del núcleo de Windows, lo que provoca inestabilidad y reinicios.

Pasos para eliminar un virus en Windows 11 y restaurar la estabilidad

Desconectar de Internet y evitar la propagación

- **Desconectar de la red**: Desconectar el equipo de Internet para evitar que el virus se comunique con servidores remotos o se propague a otros dispositivos de la red.
- **Evitar el uso de dispositivos externos**: No conectar unidades USB ni discos externos para evitar que el virus se replique.

Entrar en modo seguro (Safe Mode)

- Ejecutar el sistema con solo los procesos mínimos necesarios, impidiendo que la mayoría de virus se inicien automáticamente.
- **Pasos para entrar en Modo Seguro**:
    1. Presionar Shift y reiniciar el equipo.
    2. Seleccionar Solucionar problemas > Opciones avanzadas > Configuración de inicio**.**
    3. Elegir Modo Seguro con funciones de red si se necesita acceder a Internet para descargar herramientas de eliminación de malware.

Escaneo profundo con software antimalware

- **Windows Defender Offline**:
    1. Ejecutar Windows Defender Offline desde el modo seguro. Esto escanea el sistema antes de que el virus se active.
    2. Ir a Configuración > Actualización y Seguridad > Seguridad de Windows > Protección contra virus y amenazas**.**
    3. Dar clic en **Escaneo sin conexión** y sigue las instrucciones.
- **Herramientas adicionales**:
    1. **Malwarebytes Anti-Malware**: Este software puede identificar y eliminar amenazas que el antivirus integrado de Windows no detecta. Descargar e instalar Malwarebytes, realizar un escaneo completo**,** y eliminar las amenazas detectadas.
    2. **ESET Online Scanner** o **Kaspersky Virus Removal Tool**: Se pueden utilizar estos escáneres online para detectar virus difíciles de eliminar.

Revisar aplicaciones y procesos sospechosos

- Utilizar Autoruns de Sysinternals para revisar entradas sospechosas en el inicio de Windows. Si se identifica programas o procesos que no se reconocen, o parecen maliciosos (por ejemplo, nombres aleatorios o asociados con malware conocido), desactivarlos.
- Usa Process Explorer para monitorear procesos en tiempo real y buscar comportamientos anómalos, como consumo excesivo de recursos o nombres de procesos sospechosos.

Analizar la integridad del sistema

- Después de eliminar el malware, es crucial verificar si los archivos del sistema han sido dañados o modificados:
    - **System File Checker (SFC)**: Ejecutar sfc /scannow en el símbolo del sistema con privilegios de administrador para reparar archivos del sistema corruptos.
    - **Herramienta DISM**: Usar DISM /Online /Cleanup-Image /RestoreHealth para reparar la imagen de Windows.

Limpiar el Registro de Windows

- A veces, el malware deja rastros en el **Registro de Windows**. Usar una herramienta confiable como **CCleaner** para limpiar entradas del registro dañadas, **tener cuidado** de hacerlo manualmente, ya que la edición incorrecta del registro puede dañar aún más el sistema.

Actualizar Windows y el antivirus

- Actualizar el sistema**:** Asegurarse de que Windows 11 y todos los controladores estén actualizados. Las actualizaciones de seguridad pueden corregir vulnerabilidades que el malware podría haber aprovechado.
- **Actualizar el software antivirus**: Mantener tu antivirus actualizado para estar protegido contra nuevas amenazas. Windows Defender en su configuración completa ofrece una buena protección, pero se puede considerar un antivirus adicional si es necesario.

Revisar controladores y servicios

- Algunos virus pueden instalar **drivers maliciosos** que siguen afectando el sistema incluso después de la eliminación del malware. Usar el **Administrador de dispositivos** para revisar si hay controladores sospechosos, y reinstalar los controladores necesarios desde fuentes confiables.

Restaura archivos críticos o reinstala Windows

- Si los daños causados por el malware son graves y el sistema sigue siendo inestable, es posible que se deba considerar una **restauración del sistema** a un punto anterior donde el equipo funcionaba correctamente.
- Si todo lo anterior falla, considerar una **reinstalación limpia** de Windows 11 para asegurarse de que no quedan rastros del malware.

Consejos para evitar infecciones futuras

1. **Mantener el antivirus actualizado** y activo en tiempo real.
2. **Evitar descargar software de fuentes no confiables** o abrir archivos adjuntos sospechosos en correos electrónicos.
3. **Realizar escaneos periódicos** y usar una solución antimalware secundaria para detectar posibles amenazas que el antivirus principal pueda omitir.
4. Configurar copias de seguridad automáticas en una unidad externa o en la nube para proteger tus datos.

Solución del almacenamiento en el equipo

Las copias de seguridad son importantes ya que de estas dependen el resguardo de la pérdida de datos. Ante cualquier evento de fallo técnico, sea por hardware como un disco duro con fallas o si ha sido atacado por un virus informático, la copia de seguridad nos garantiza la recuperación de los archivos, de esta manera podemos minimizar el impacto de la pérdida de archivos.

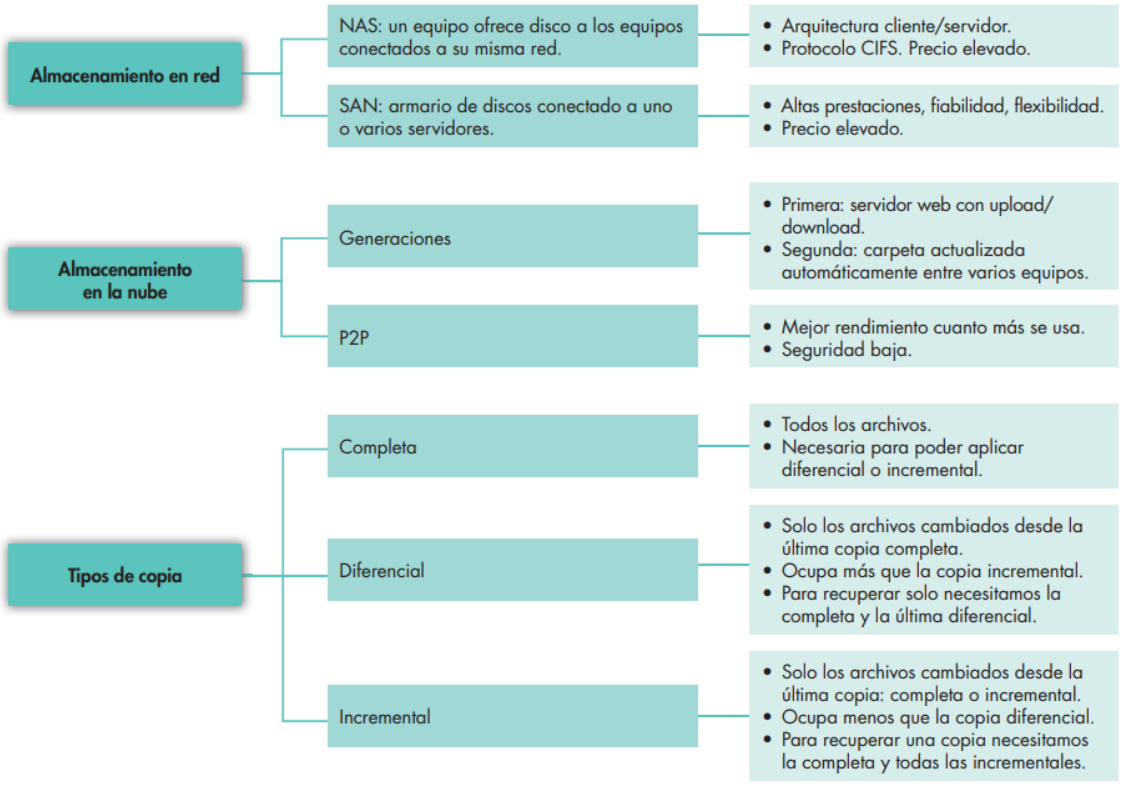
Tipos de copia de seguridad:

- Copias de seguridad en la nube: En este método se vale de realizar una copia de seguridad en servidores remotos de internet. Existen varios como lo son Drive de Google, Dropbox o iCloud.
- Copias de seguridad de almacenamientos externos: Consiste en realizar una copia en un dispositivo externo. En este sentido se puede entender como discos duros externos, memoria USB. Previo a la realización de la copia de seguridad en estos dispositivos es importante validar que los mismos se encuentren en óptimas condiciones.
- Copias de seguridad en red: En este método consiste en realizar copias de seguridad de los datos almacenados en un servidor local que se encuentre en la misma red.

Por lo que los tipos de almacenamiento también se pueden catalogar de acuerdo con la siguiente ilustración.

Figura 79

Seguridad Informática



Nota: El gráfico presenta un esquema organizado sobre almacenamiento en red, almacenamiento en la nube y tipos de copias de seguridad.

Para prevenir la pérdida de datos totales es importante realizar copias de seguridad de al menos una vez al mes y asegurarse que estas se encuentren en un lugar seguro y separado del dispositivo original.

El respaldo hace referencia a una copia representativa de los datos e incluye elementos esenciales de una base de datos, como archivos de datos y archivos de control. Como los errores inesperados en la base de datos no se pueden evitar, se requiere un respaldo de toda la base de datos. Existen dos tipos principales de respaldos:

1. Respaldo físico: Es una copia de los archivos de la base de datos física, como datos, archivos de control, archivos de registro y registros de rehacer archivados. Es una copia de los archivos que almacenan información de la base de datos en otra ubicación y forma la base del mecanismo de recuperación de la base de datos.

2. Respaldo lógico: Contiene los datos lógicos que se extraen de una base de datos, y consta de tablas, procedimientos, vistas, funciones, etc. Sin embargo, no se recomienda ni es útil mantener un respaldo lógico por sí solo, ya que solo proporciona información estructural. (Veritas, 2024)

Solución Antivirus en el equipo

Para elegir un antivirus que proporcione una solución confiable y utilizable que brinde un nivel de protección adecuado contra malware. Se deben tener ciertos criterios a la hora de obtener la mejor protección de antivirus.

En este apartado se enumeran los criterios recomendados, esto lo podemos encontrar dentro de las recomendaciones que se pueden encontrar en los blogs de (Kaspersky, 2024) a continuación:

Figura 80

Mejores Criterios Seguridad

Nota: El gráfico presenta cuatro aspectos clave a evaluar en una solución antivirus: Confiabilidad, Capacidad de uso, Protección integral, y Calidad de la protección.

En vista de que a diario se realizan descargas de sitios web, se debe realizar un vistazo a cuáles serían los consejos para evitar descargar archivos maliciosos de sitios no confiables y como detectarlos a tiempo, en este sentido tenemos unas buenas prácticas tomadas del sitio (González G. , 2024)

- Una de las bases de datos más grande de análisis de virus informáticos que se tiene a disposición es VirusTotal, al ingresar a este sitio web se puede incrustar el link del sitio de

descarga del archivo y enseguida se comprobará el archivo y se cotejará los datos con diferentes motores de antivirus diferentes. Cabe recalcar que existe la versión de la página web y también que se dispone de una extensión para navegadores tanto Chrome como Firefox.

- Otra solución a la hora de comprobar si esta descarga que se ha realizado es confiable, se puede determinar y poniéndolo a prueba en un entorno experimental como es una máquina virtual aislada, dentro de este entorno virtual se pueden realizar las pruebas respectivas y de esta forma encontrar si un archivo es dañino o por el contrario es confiable, antes de realizar la instalación en la máquina de uso diario.

CAPÍTULO V

CONCLUSIONES

A lo largo de este trabajo, se desarrolló un marco forense integral para la identificación, preservación y análisis de evidencia digital en entornos Windows 11, con un enfoque en la respuesta a incidentes de seguridad. Este marco permitió no solo abordar desafíos específicos como configuraciones críticas, reinicios inesperados y análisis de procesos en memoria, sino también mejorar la seguridad, estabilidad y eficiencia del sistema operativo en entornos corporativos.

Identificación de configuraciones críticas

Se analizaron configuraciones clave de Windows 11, como Smartscreen, Windows Security, Windows Update y servicios en la nube como OneDrive, identificando parámetros esenciales que impactan la seguridad del sistema. Este análisis incluyó detalles específicos sobre versiones y builds del sistema, contribuyendo a un entendimiento más completo y permitiendo implementar mejoras adaptadas a las necesidades del entorno.

Causas y resolución de reinicios inesperados

El estudio de los reinicios no programados reveló problemas en controladores y configuraciones inadecuadas. La incorporación de detalles técnicos sobre el hardware y la configuración del sistema permitió desarrollar soluciones personalizadas que mejoraron la estabilidad y minimizaron interrupciones operativas.

Análisis de procesos en memoria y aplicaciones instaladas

El análisis detallado de las aplicaciones y los procesos en ejecución en memoria permitió

detectar software potencialmente intrusivo y optimizar la eficiencia del sistema. El uso de herramientas estandarizadas y comandos avanzados de Volatility facilitó un monitoreo efectivo de los procesos, identificando y mitigando amenazas antes de que comprometieran la estabilidad del sistema.

Detección y análisis de amenazas

- Virus y malware**:** Se investigó un virus identificado durante el proceso, documentando su método de entrada, propagación y condiciones favorables. Esto permitió desarrollar estrategias preventivas y correctivas basadas en estándares y referencias confiables.
- Conexiones de red inseguras: Una auditoría exhaustiva de las conexiones de red activas permitió identificar vulnerabilidades en los servicios y proponer mejoras prácticas para fortalecer la seguridad de la infraestructura de red.

Optimización y recomendaciones

- Recursos del sistema: Se implementaron estrategias para proteger datos y optimizar recursos mediante navegadores seguros y medidas adicionales de seguridad, logrando un entorno más robusto.
- Gestión de almacenamiento y copias de seguridad: Se destacó la importancia de políticas de respaldo periódico para garantizar la integridad y disponibilidad de los datos críticos.
- Uso de antivirus y buenas prácticas: Se propusieron recomendaciones prácticas para maximizar la efectividad de los antivirus y se enfatizó la importancia de un enfoque preventivo basado en el "sentido común" al gestionar descargas y programas.

Contribuciones y resultados

Este trabajo demuestra que la implementación de estrategias forenses especializadas no solo facilita la identificación y mitigación de amenazas, sino que también optimiza el rendimiento operativo y los recursos del sistema. Las soluciones propuestas, desarrolladas con un enfoque práctico y basado en estándares, fortalecen las capacidades de prevención y respuesta en entornos corporativos, asegurando una gestión más eficiente y segura de los sistemas Windows 11.

Con el apoyo de contribuciones de expertos y un enfoque riguroso en cada etapa del proceso, este marco forense representa una herramienta valiosa para la seguridad digital, ofreciendo lineamientos claros y efectivos para la resolución de incidentes futuros.

Referencias

Al Sharif, S. A. (2014). An approach for the validation of file recovery functions in digital forensics' software tools. *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)*, 1-6.

Ambato, U. T. (2018). *La protección de datos y los delitos informáticos en el Código Orgánico Integral Penal de Ecuador*. Retrieved from La protección de datos y los delitos informáticos en el Código Orgánico Integral Penal de Ecuador: https://repositorio.uta.edu.ec

Arellano, L. E. (2012). La cadena de custodia informático-forense. *Cuaderno activa*, 67-81.

Arthur, W. C. (2015). *A practical guide to TPM 2.0: Using the new trusted platform module in the new age of security.* Springer Nature.

B., C. (2024, 9 5). *SleuthKit. Autopsy.* Retrieved from Autopsy: https://www.sleuthkit.org/autopsy/

Binus. (2023, Septiembre 20). *FTK IMAGER IN DIGITAL FORENSIC*. Retrieved from https://sis.binus.ac.id/2023/09/20/ftk-imager-in-digital-forensic/

Bonetti, G. V. (2013). A comprehensive black-box methodology for testing the forensic characteristics of solid-state drives. *Proceedings of the 29th Annual Computer Security Applications Conference*, 269-278.

Bórquez, P. (2011). Importancia de la cadena de custodia de evidencias . *Revista médica de Chile*, 820-821.

Buendía, J. F. (2013). *Seguridad Informática.* Madrid: Mc Graw Hill.

Cajo, I. M. (2018). Estudio comparativo de las metodologías de análisis forense informático para la examinación de datos en medios digitales. *European Scientific Journal*, 40-45.

Carbone, F. (2014). *Computer forensics with FTK.* Packt Publishing.

Carrier, B. (2024, 09 05). *SleuthKit*. Retrieved from Autopsy: https://www.sleuthkit.org/autopsy/

Carvey, H. (2009). *Windows forensic analysis DVD toolkit.* Syngress.

Chappell, L. (2012). *Wireshark network analysis.* Podbooks.

Check Point Research. (2024, 07 22). *Threat intelligence report*. Retrieved from 22nd July – Threat Intelligence Report: https://research.checkpoint.com/2024/22nd-july-threat-intelligence-report/

Cisar, P. &. (2019). Some ethical hacking possibilities in Kali Linux environment. *Journal of Applied Technical and Educational Sciences*, 129-149.

Cisco Talos Intelligence Group. (2024, 10 26). *CISCO TALOS*. Retrieved from https://talosintelligence.com/: https://talosintelligence.com/sha_searches

Cisco Talos Intelligence Group. (2024, 10 26). *CISCO TALOS*. Retrieved from https://talosintelligence.com/sha_searches

Coronel-Rojas, L. A.-A.-Q.-B. (2020). Definición de una metodología de adquisición de evidencias digitales basada en estándares internacionales. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 266-282.

Darkcrizt. (4 de 12 de 2019). *UbuntuBlog*. Obtenido de CAINE 11.0 ya liberada, la distro basada en Ubuntu para el análisis forense: https://ubunlog.com/caine-11-0-ya-liberada-la-distro-basada-en-ubuntu-para-el-analisis-forense/

Dash, P. (2013). *Getting started with oracle vm virtualbox.* Birmingham: Packt Publishing.

Daza, S. (03 de 12 de 2021). *BeHackerPro*. Obtenido de ¿Qué es DEFT y para qué sirve?: https://behacker.pro/que-es-deft-y-para-qe-sirve/

Decusatis, C. C. (2015). Methodology for an open digital forensics model based on CAINE. *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 935-940.

Didik, S. Y. (2019). Analysis and evaluation digital forensic investigation framework using iso 27037: 2012. *International Journal of Cyber-Security and Digital Forensics*, 1-14.

Dieguez Castro, J. (2016). *Introducing Linux Distros.* Berkeley: Apress.

Dieguez Castro, J. (2016). *Introducing Linux Distros.* Berkeley: Apress.

DistroWatch.com. (2024, 02 02). *DistroWatch.com: CAINE*. Retrieved from CAINE: https://distrowatch.com/table.php?distribution=caine

DistroWatch.com. (2024, 2 2). *DistroWatch.com*. Retrieved from DEFT Linux: https://distrowatch.com/table.php?distribution=deft

DragoN. (2017, 2 15). *DragonJar*. Retrieved from DEFT (Digital Evidence & Forensic Toolkit): https://www.dragonjar.org/deft-digital-evidence-forensic-toolkit.xhtml

Dragora. (2 de 4 de 2021). *https://underc0de.org/*. Obtenido de CAINE, el Linux forense auto-arrancable: https://underc0de.org/foro/gnulinux/caine-el-linux-forense-auto-arrancable/

Ecuador, A. N. (2014). *Código Orgánico Integral Penal (COIP). Registro Oficial No. 180*. Retrieved from Código Orgánico Integral Penal (COIP). Registro Oficial No. 180: https://www.asambleanacional.gob.ec

Ecuador, A. N. (2021). *Ley Orgánica de Protección de Datos Personales*. Retrieved from Ley Orgánica de Protección de Datos Personales: https://www.gob.ec

Ecuador, L. (2023). *Sobre la Ley de Protección de Datos Personales*. Retrieved from Sobre la Ley de Protección de Datos Personales: https://www.lexis.com.ec

Emmanuel, O. I. (2021). Windows Firewall Bypassing Techniques: An Overview of HTTP Tunneling and Nmap Evasion. *International Conference on Computational Science and Its Applications*, Springer International Publishing.

Estado, F. G. (2015). *Los delitos informáticos van desde el fraude hasta el espionaje*. Retrieved from Los delitos informáticos van desde el fraude hasta el espionaje: https://www.fiscalia.gob.ec

Forte, D. V. (2008). Volatile data vs. data at rest: the requirements of digital forensics. *Network Security*, 13-15.

García, D. (8 de 12 de 2023). *Andro4all*. Obtenido de Windows 11 no convence: solo un 26% de usuarios lo utilizan en 2023.: https://www.lavanguardia.com/andro4all/windows/windows-11-no-logra-acercarse-a-windows-10-solo-acumula-un-26-de-usuarios-tras-mas-de-dos-anos

GIAC. (2021). *Certifications*. Retrieved from Certifications: https://www.sans.org

González, G. (2024, 10 27). *Genbeta*. Retrieved from https://www.genbeta.com/paso-a-paso/como-asegurarte-que-una-descarga-en-internet-es-segura-antes-de-bajar-el-archivo

González, G. (27 de 10 de 2024). *Genbeta.* Obtenido de Cómo asegurarte que una descarga en internet es segura antes de bajar el archivo: https://www.genbeta.com/paso-a-paso/como-asegurarte-que-una-descarga-en-internet-es-segura-antes-de-bajar-el-archivo

González, J. (2022). *La importancia de la ciberseguridad en el sector privado de Ecuador.* Seguridad Informática.

Grispos, G. T. (2021). A digital forensics investigation of a smart scale iot ecosystem. *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications*, 710-717.

Grubor, G. R. (2013). Integrated forensic accounting investigative process model in digital environment. *International Journal of Scientific and Research Publications*, 1-9.

Guzmán, J. (2016, 09 07). *BlackTrack Academy*. Retrieved from Plataforma de análisis forense para imágenes de discos duros (Autopsy): https://backtrackacademy.com/articulo/plataforma-de-analisis-forense-para-imagenes-de-discos-duros-autopsy

Guzmán, J. (7 de 09 de 2024). *BackTrack Academy.* Obtenido de Plataforma de análisis forense para imágenes de discos duros (Autopsy): https://backtrackacademy.com/articulo/plataforma-de-analisis-forense-para-imagenes-de-discos-duros-autopsy

Halsey, M. (2022). Managing Your Privacy and Security. In *Windows 11 Made Easy: Getting Started and Making It Work for You* (pp. 163-185). Berkeley: Apress.

Institute, S. (2021). *About SANS*. Retrieved from About SANS: https://www.sans.org

Institute, S. (2021). *SANS Instiute*. Retrieved from About SANS: https://www.sans.org

Jeong, D. &. (2019). Forensic signature for tracking storage devices: Analysis of UEFI firmware image, disk signature and windows artifacts. *Digital Investigation*, 21-27.

Kamble, D. R. (2015). Cybercrimes solutions using digital forensic tools. *International Journal of Wireless and Microwave Technologies*, 11-18.

Kaspersky. (2024, 10 27). *Latam Kaspersky*. Retrieved from https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-choices

KeepCoding. (2024, 09 05). *KeepCoding*. Retrieved from Como funciona el RegRipper: https://keepcoding.io/blog/como-funciona-el-regripper/

keepcoding.io. (5 de 9 de 2024). *Cómo funciona el RegRipper*. Obtenido de KeepCoding: https://keepcoding.io/blog/como-funciona-el-regripper/

Khatri, Y. (2015). Forensic implications of system resource usage monitor (SRUM) data in windows 8. *Digital Investigation, 12*, 53-65.

Latam Kaspersky. (2024, 10 27). *Latam Kaspersky*. Retrieved from Antivirus Choices: https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-choices

Law, N. (2021). *Entra en vigencia la Ley Orgánica de Protección de Datos Personales*. Retrieved from Entra en vigencia la Ley Orgánica de Protección de Datos Personales: https://nmslaw.com.ec

Lazaridis, I. A. (2016). Evaluation of digital forensics tools on data recovery and analysis. *The third international conference on computer science, computer engineering, and social media*, 67.

Lipner, S. &. (2023). Inside the Windows Security Push: A Twenty-Year Retrospective. *IEEE Security & Privacy, 21(2)*, 24-31.

LLC, W. (2024, 10 09). *Any.run*. Retrieved from https://any.run/report/4571f9310b1a27b245409e311b4de7fa6f620a18f1d3b98335e29b8d8f827150/e3f10247-ca71-4618-87a4-735f4fa71331

M., C. (2024, 05 25). *Unitrends*. Retrieved from What are the consequences of data loss? Unitrends.: https://www.unitrends.com/blog/what-are-the-consequences-of-data-loss

Margosis, A. &. (2011). *Windows Sysinternals administrator's reference.* Pearson Education.

McDonald, J. T. (2008). Software issues in digital forensics. *ACM SIGOPS Operating Systems Review*, 29-40.

Naik, N. &. (2016). Enhancing windows firewall security using fuzzy reasoning. *n 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and*

Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, 263-269.

Narayanaswamy, A. (2024). Working with Copilot in Windows 11 – Part 2. In *Microsoft Copilot for Windows 11* (pp. 47-72). Berkeley: Apress.

Parasram, S. V. (2020). *Digital Forensics with Kali Linux: Perform data acquisition, data recovery, network forensics, and malware analysis with Kali Linux 2019.* Packt Publishing Ltd.

Qureshi, S. H. (2022). Browser Forensics: Extracting Evidence from Browser Using Kali Linux and Parrot OS Forensics Tools. *International Journal of Network Security*, 557-572.

Ramadhan, R. A. (2022). Digital forensic investigation for non-volatile memory architecture by hybrid evaluation based on ISO/IEC 27037: 2012 and NIST SP800-86 framework. *IT Journal Research and Development*, 162-168.

Reddy, N. (2019). *Linux Forensics. In: Practical Cyber Forensics.* Berkeley: Apress.

Rueda-Rueda, J. S.-B.-S. (2019). Guía práctica abierta para el análisis forense digital en dispositivos Android. *RISTI (Revista Ibérica de Sistemas y Tecnologías de La Información)*, 442-457.

Russinovich, M. E. (2012). *Windows internals, part 2.* Pearson Education.

Shaaban, A. &. (2016). *Practical windows forensics.* Packt Publishing Ltd.

Sierra, M. (2022). *Revista de Estudios Tecnológicos.*

srcr. (2024, 10 01). *Malware Bazaar*. Retrieved from https://bazaar.abuse.ch/sample/a17b0884e00bab93fa46a08043a5d972c3dd0cbc2331448e365b988dbc76843d/#comments

support.ccleaner.com. (5 de 08 de 2024). *How does Recuva work?* Obtenido de CCleaner Support: https://support.ccleaner.com/s/article/how-does-recuva-works

Telecomunicaciones, M. d. (2021). *Políticas y normativas de ciberseguridad en Ecuador*. Retrieved from Políticas y normativas de ciberseguridad en Ecuador: https://www.telecomunicaciones.gob.ec/

Thethi, N. &. (2014). Digital forensics investigations in the cloud. *2014 IEEE international advance computing conference (IACC)*, 1475-1480.

ul Hassan, S. Z. (2021). Operating Systems for Ethical Hackers-A Platform Comparison of Kali Linux and Parrot OS. *International Journal*.

Uygur, S. U. (2014). *Penetration Testing with BackBox.* Packt Publishing Ltd.

Veritas, C. d. (2024, 10 26). *Veritas.com*. Retrieved from https://www.veritas.com/es/es/information-center/data-backup-and-recovery

Volatility. (2024, 09 05). *Volatility Foundation*. Retrieved from https://volatilityfoundation.org/

zbetcheckin. (2024, 10 08). *Malware Bazaar*. Retrieved from https://bazaar.abuse.ch/sample/4571f9310b1a27b245409e311b4de7fa6f620a18f1d3b98335e29b8d8f827150#comments

Zhao, Q. &. (2009). Zhao, Q., & Cao, T. (2009). Collecting Sensitive Information from Windows Physical Memory. *J. Comput.*, 3-10.

Apéndices

Apéndice A Entrevista

Entrevista de Recolección de Información: Problemas de Rendimiento y Aplicación de Minería de Bitcoin

Recomendaciones para el entrevistador:

- Explicar la confidencialidad de la información y mostrar empatía para que el cliente se sienta cómodo compartiendo detalles.
- Usar lenguaje sencillo y evitar términos técnicos para facilitar la comprensión del cliente, adaptando las preguntas a su nivel de conocimiento.
- Organizar las preguntas en un orden secuencial, comenzar con los síntomas y luego pasar a detalles técnicos y recientes cambios en el sistema.
- Dividir las preguntas complejas y evita suposiciones, hacer que cada pregunta sea directa y fácil de responder.
- Dar tiempo al cliente para responder, escuchar sin interrumpir y permitir que brinde detalles adicionales espontáneamente.
- Registrar respuestas detalladas, utilizar listas de verificación para cubrir todos los puntos y estructurar la información obtenida.
- Reacciones no verbales pueden indicar dudas o inseguridades, lo cual puede guiar para aclarar temas o reformular preguntas.

- Indagar sobre otros síntomas para detectar comportamientos adicionales del sistema.
- Resumir los puntos clave al final de la entrevista para confirmar la precisión de las respuestas y evitar malentendidos.
- Informar al cliente sobre el uso de la información obtenida y los pasos iniciales del análisis para que conozca cómo se procederá.

Preguntas:

Síntomas y Problemas del Sistema

- ¿Desde cuándo ha comenzado a notar los problemas de rendimiento y los reinicios inesperados?
- ¿Con qué frecuencia se producen los reinicios del sistema?
- ¿Ocurre algo específico justo antes de que el equipo se reinicie? (Por ejemplo, al abrir aplicaciones, al ejecutar la aplicación de minería, etc.)
- ¿El equipo muestra otros síntomas como sobrecalentamiento, bloqueos o lentitud extrema?
- ¿Ha experimentado alguna pérdida de datos o archivos después de los reinicios?

Cambios Recientes en el Sistema

- ¿Ha realizado alguna actualización o cambio en el sistema operativo o en los controladores de hardware recientemente?
- ¿Qué otras aplicaciones han instalado en el sistema alrededor del tiempo en que comenzaron los problemas?
- ¿Ha conectado algún nuevo dispositivo de hardware (USB, discos externos, etc.) a su computadora?

Detalles de la Aplicación de Minería de Bitcoin

- ¿Cuál es el nombre de la aplicación de minería de bitcoin que instaló?
- ¿Dónde descargó la aplicación? (Sitio web oficial, foro, repositorio, etc.)
- ¿Recuerda la fecha exacta o aproximada en que instaló la aplicación?
- ¿La aplicación ha solicitado permisos específicos o configuraciones especiales para funcionar?
- ¿Ha notado un incremento en el uso de recursos (CPU, memoria, disco) desde que instaló la aplicación?
- ¿Está la aplicación configurada para ejecutarse automáticamente al iniciar el sistema?

Seguridad y Preocupaciones Adicionales

- ¿Está preocupado por posibles problemas de seguridad o privacidad relacionados con la aplicación de minería?
- ¿Ha recibido algún mensaje de advertencia del sistema o del antivirus sobre posibles riesgos o malware desde que instaló la aplicación?
- ¿Ha intentado desinstalar la aplicación o tomar alguna medida para solucionar los problemas?

Otros Detalles Relevantes

- ¿Tiene algún otro comentario o detalle que considere relevante para la investigación del problema?

Apéndice B Solicitud de Análisis Forense

Cliente: [Nombre del Cliente]

RUC: [Número de RUC]

Dirección: [Dirección del Cliente]

Teléfono: [Número de Teléfono]

Correo Electrónico: [Correo Electrónico]

Fecha: [Fecha de Solicitud]

A: [Nombre de la Empresa o Profesional que realizará el análisis]

Dirección: [Dirección de la Empresa o Profesional]

Asunto: Solicitud de Análisis Forense de Equipo Electrónico

Estimados señores,

Por medio de la presente, solicito formalmente la realización de un análisis forense del siguiente equipo electrónico, en virtud de la legislación ecuatoriana vigente que regula la recolección y análisis de evidencias digitales, específicamente en el contexto de la Ley de Protección de Datos Personales y las normas relacionadas con la informática forense.

Documentación Adjunta:

1. **Informe de incidente:** [Descripción del incidente que motivó la solicitud, si aplica]
2. **Autorización:** [Firma del cliente, si es necesario, para proceder con el análisis]

3. **Copia de identificación:** [Copia de la cédula de identidad o documento de identificación del solicitante]

Agradezco de antemano su pronta atención a esta solicitud y quedo atento a su confirmación sobre la recepción de esta carta y el inicio del proceso de análisis forense.

Atentamente,

[Firma]

[Nombre del Cliente]

[Cargo]

[Fecha]

Apéndice C Detalles del Equipo:

Registro de Configuración del Sistema

Información del Hardware

- **Nombre del equipo**: Windows1124H2
- **Fabricante**: VirtualBox 7.1.4
- **Modelo**: Máquina Virtual genérica
- **Procesador (CPU)**:
    - **Nombre**: AMD Ryzen 5 7520U with Radeon Graphics (Simulado)
    - **Velocidad**: 2.79 GHz (Simulado)
    - **Núcleos**: 2 núcleos virtuales
- **Memoria RAM**: 4 GB

- **Disco Duro**:
    - **Capacidad total**: 80 GB (dinámico)
    - **Tipo**: Virtual VDI
    - **Espacio usado**: 21 GB
- **Adaptador de Red**:
    - **Tipo**: Adaptador Puente
    - **MAC Address**: 08:00:27:82:E3:3F (Simulado)
    - **Dirección IP**: Asignada dinámicamente por DHCP
- **Controlador de gráficos**:
    - **Tipo**: Adaptador gráfico virtualizado
    - **Memoria de video asignada**: 128 MB

Información del Software

- **Sistema Operativo**:
    - **Edición**: Microsoft Windows 11 Home
    - **Versión**: 24H2
    - **Arquitectura**: x64 (64 bits)
    - **Fecha de instalación**: 01 de octubre de 2024
    - **Licencia activada**: No
- **Actualizaciones de Windows**:
    - **Actualización más reciente instalada**: 20 de octubre de 2024 (KB5044030)
    - **Estado de actualizaciones**: Todas las actualizaciones críticas y de seguridad están al día.

- **Antivirus**:
    - **Software**: Microsoft Defender Antivirus
    - **Versión**: 4.18.24080.9
    - **Estado**: Activado y actualizado
- **Firewall**:
    - **Software**: Firewall de Windows Defender
    - **Estado**: Activado con reglas predeterminadas
- **Otros Programas en segundo plano**:
    - **Administrador de Tareas de Windows**: Activo
    - **Explorador de Procesos (Process Explorer)**: Instalado para monitoreo de recursos.

Configuración del Sistema

- **Disco Duro Virtual**:
    - **Tipo**: Estático.
    - **Particiones**:
        - **Partición 1**: Disco principal (50 GB)
- **Uso de CPU**:
    - **Porcentaje de uso promedio**: 72-90% (cuando la aplicación de minería está activa)
- **Uso de Memoria RAM**:
    - **Porcentaje de uso promedio**: 70-85% (con la aplicación de minería ejecutándose)
- **Estado de la batería (si aplica)**:
    - **N/A** (la máquina virtual no tiene batería)

- **Velocidad del ventilador (si aplica)**:
    - **N/A** (la máquina virtual no refleja hardware físico)

Configuración de Red

- **Adaptador de red**: Adaptador Puente
    - **IP asignada**: 192.168.100.147 (por DHCP)
    - **Puerta de enlace**: 192.168.1.1
    - **DNS**: 8.8.8.8, 8.8.4.4 (Google DNS)
- **Firewall de Windows**:
    - **Reglas**:
        - Aplicación de minería permitida para conexiones de salida a puertos específicos (minado en pool de criptomonedas)
        - Bloqueo de puertos no esenciales para minimizar riesgos de seguridad.

Logs y Eventos del Sistema

- **Visor de Eventos (Event Viewer)**:
    - **Errores críticos**:
        - **ID de Evento 41**: Kernel-Power – Se detectaron reinicios inesperados relacionados con el uso intensivo de recursos.
    - **Advertencias**:
        - **ID de Evento 10016**: DistributedCOM – Advertencias recurrentes sin impacto directo en el rendimiento.

Información Adicional del Sistema

- **Política de Energía**:
    - **Configuración actual**: Máximo rendimiento, sin modo de suspensión para permitir que la aplicación de minería funcione continuamente.
- **Temperatura promedio del CPU**: 70-85°C bajo carga con la aplicación de minería activa (simulado).
- **Análisis de discos**: No se detectan sectores defectuosos ni fallos aparentes en la integridad del disco virtual.

Apéndice D Formulario Adquisición de datos:

Figura 81

Formulario Adquisición de datos

Formulario adquisición de datos	
Identificación de la evidencia (ID):	
Fecha y hora de la adquisición:	
Descripción de la evidencia:	
Número de serie del dispositivo:	
Lugar de adquisición	
Ubicación de la evidencia al momento de la recolección:	

Persona que realizó la recolección	
Nombre:	
Cargo:	
Firma:	
Fecha y hora de recolección:	
Organización/Institución:	
Métodos de adquisición de la evidencia	
Herramienta forense utilizada para la adquisición	
Método de adquisición	
Algoritmo de hash usado:	
Valor del hash evidencia original:	
Valor del hash copia forense:	

Transferencia de la Evidencia					
Fecha y hora	**Origen**	**Destino**	**Motivo de transferencia**	**Firma**	**Observaciones**

Almacenamiento de la Evidencia	
Ubicación de almacenamiento:	
Responsable del almacenamiento:	
Fecha y hora de almacenamiento:	
Condiciones de almacenamiento:	
Acceso a la Evidencia	

Fecha y hora de acceso	Nombre del solicitante	Motivo de acceso	Firma
Comentarios adicionales (si es necesario):			

Nota: Tabla creada para recolectar el Formulario de adquisición de datos.