UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES:

Jonathan Andrés Corrales Yánez
Juan Fernando López Tito
Iván Galo Reyes Chacón
Livardi Paul Salgado Flores

TUTOR:

Ing. Jaime Ibarra

Desarrollo de un Marco de Trabajo de Análisis Forense y Localización de Información en Equipos Informáticos con Sistema Operativo Windows 10

APROBACIÓN DEL TUTOR

Yo**, Jaime Ibarra Jiménez,** certifico que conozco los autores del presente trabajo siendo ellos los responsables exclusivos tanto de su originalidad y autenticidad, como de su contenido.

Firmado electrónicamente por:
JAIME BLADIMIR
IBARRA JIMENEZ

Jaime Ibarra

DIRECTOR DE TESIS

CERTIFICACIÓN DE AUTORÍA

Yo, **Jonathan Andrés Corrales Yanez, Juan Fernando López Tito, Iván Galo Reyes Chacón, Livardi Paul Salgado Flores,** 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.

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

……..……

Jonathan Andrés Corrales Yánez

1722720784

……..……

Juan Fernando López Tito

1719664938

……..……

Iván Galo Reyes Chacón

1716633944

……..……

Livardi Paul Salgado Flores

1716690969

DEDICATORIA

Nada de esta meta alcanzada sería posible sin la ayuda de Dios, él es quien me ha provisto de mi amada esposa e hija, quienes me han brindado su apoyo incondicional en este reto, agradezco a mi madre, Raulito, mi hermana y mi cuñado, por estar siempre presentes y ayudarme con su consejo en todo momento.

Att. Jonathan Andrés Corrales Yánez

Quiero dedicar este logro a mi amada esposa, a mi hija, por estar siempre entregándome su amor incondicional y por la paciencia que han tendido durante todo este tiempo, también a cada una de las personas que me brindaron su apoyo a lo largo de mis jornadas de estudio. A todos ustedes, GRACIAS.

Att. Juan Fernando López Tito

Quiero dedicar este trabajo Dios por hacerlo todo posible, a mi hermosa Carlita, ella es la luz que guía mi camino, mi sincero empuje en momentos complicados, mi par, mi todo.. Gracias por tu compresión y todo tu apoyo incondicional.
Att. Iván Galo Reyes Chacón

Dedico este logro a mi madre, hermanos, abuelitos y amigos que siempre han estado en constante apoyo y atentos de mi bienestar, animándome a ser una mejor persona al igual que un excelente profesional. Muchas gracias a todos ustedes.
Att. Livardi Paul Salgado Flores

RESUMEN

Con la realización del proyecto denominado “Desarrollo de un Marco de Trabajo de Análisis Forense y Localización de Información en Equipos Informáticos con Sistema Operativo Windows 10” se han establecido una serie de pasos y puntos a considerar al momento de realizar un análisis forense de un equipo con sistema operativos Windows 10, los cuales fueron comprobados en diferentes laboratorios, realizando un análisis de los resultados obtenidos, esto nos permitió validar la funcionalidad del Marco de Trabajo planteado.

En el Estado del Arte se presenta una introducción a la seguridad de la información, y a los ciberataques y la importancia del análisis forense de un equipo ante un evento que genere una vulnerabilidad en la seguridad de la información. Después se detallan algunas herramientas utilizadas durante el desarrollo de este proyecto, también se describen las diferentes distribuciones que puede usar un investigador, con varias herramientas. Finalmente, se detallan las normativas para el análisis forense.

En el marco de trabajo se detallan las consideraciones a tomar en cada fase, en la etapa previa, durante y al finalizar un Análisis Forense, siendo este apartado la parte central del proyecto. En la prueba de concepto, se plantean dos laboratorios en los que se pone a prueba lo planteado en el apartado anterior, permitiendo crear una guía paso a paso de cómo aplicar cada idea propuesta en este trabajo.

En el Análisis de Resultados se detallan las ideas más relevantes que se obtuvieron al aplicar el Marco de Trabajo desarrollado, evidenciando su efectividad a la hora de ponerlo en práctica.

Palabras Claves: forense, volcado, memoria, disco, evidencias.

ABSTRACT

With the completion of the project called “Development of a Framework for Forensic Analysis and Information Location on Computer Equipment with Windows 10 Operating System” a series of steps and points have been established to consider when carrying out a forensic analysis of a computer. with Windows 10 operating system, which were tested in different laboratories, carrying out an analysis of the results obtained, this allowed us to validate the functionality of the proposed Framework.

The art status section presents an introduction to information security, cyber attacks and the importance of forensic analysis of a computer in the event of an event that generates a vulnerability in information security. Afterwards, some tools used during the development of this project are detailed, and the different distributions that a researcher can use, with various tools, are also described. Finally, the regulations for forensic analysis are detailed.

The framework details the considerations to be taken in each phase, in the previous stage, during and at the end of a Forensic Analysis, this section being the central part of the project.

In the proof of concept, two laboratories are proposed in which what was proposed in the previous section is tested, allowing the creation of a step-by-step guide on how to apply each idea proposed in this work.

The Analysis of Results details the most relevant ideas that were obtained when applying the developed Framework, evidencing its effectiveness when putting it into practice.

Keywords: forensic, dump, memory, disk, evidence

Contenido

Lista de Figuras.

Capítulo I

Introducción

El aumento exponencial de las amenazas cibernéticas que hoy en día se están presentando a nivel mundial, el análisis forense a dispositivos electrónicos, la investigación, análisis y recuperación de información contenida en ellos, ha tomado una gran importancia en los últimos años. Es por esta razón, que se ve necesario contar con un marco de trabajo y una metodología adecuada, para efectuar un análisis forense apropiado a cada situación.

De acuerdo con una publicación de Asobanca en su página web menciona que, en Ecuador, según cifras de la Policía Nacional, los ciberdelitos han aumentado a partir de la pandemia. En 2020 la institución policial reportó 682 pedidos de investigación. En 2021 se registraron 1851 pedidos. En 2022 1400, siendo el delito más reportado, el de la apropiación fraudulenta por dispositivos electrónicos a través del mecanismo de phishing. (Asobanca, 2023).

Así también el estudio publicado en febrero del 2023 por parte de la empresa StatCounter, los ordenadores con sistemas operativos Windows al 2022 se mantenían en un 75.44% sobre sistemas como MacOS y Linux, notándose claramente la preferencia de los usuarios y las empresas por este sistema, pero que visto desde la perspectiva de un profesional de seguridad de la información los desafíos al intentar recopilar y analizar las pruebas digitales en Windows, son cada vez más desafiantes debido a la rápida evolución de las tecnologías informáticas y la falta de un enfoque estandarizado. (Fernandez, 2023).

Esto lleva a que las empresas públicas y privadas usen estos sistemas, convirtiéndose en objetivo por una acelerada transformación digital que, acompañada por el desconocimiento de los colaboradores y falta de concientización dentro de las empresas, genera un sin número de posibles vulnerabilidades.

Con este proyecto se responderá a la siguiente problemática: Cómo analizar un equipo

vulnerado, con errores o averías, para preservarse, analizar, recuperar la información y determinar el impacto provocado en su integridad, que está o estaba contenida en el equipo analizado. Obteniendo resultados relevantes y que permitan prevenir y contrarrestar el impacto en caso de presentarse eventos futuros, y reducir el tiempo de resolución del evento.

Justificación del proyecto

En 2023 la empresa Kaspersky por medio de sus diferentes herramientas, detectaron aproximadamente 411000 eventos que involucraban virus y programas maliciosos, los mismos que intentaban hacer uso de diferentes exploits. La mayoría de estos eventos se los encontraba en productos de Microsoft Office. Adicionalmente se encontraron alrededor de 125 millones de archivos con contenido malicioso. Los ataques se dirigían a usuarios con equipos con Windows como sistema operativo. (Duran, 2024)

Actualmente, varios dispositivos se ven afectados por diferentes circunstancias relacionadas con la ciberseguridad, ya sea porque fueron vulnerados o porque sufrieron daños. Sin embargo, encontrar documentación que permita realizar un análisis del dispositivo afectado y encontrar causas y plantear soluciones, es muy limitado.

Así, este trabajo plantea detallar buenas prácticas de análisis forense a un dispositivo con sistemas operativo Windows, basadas en herramientas actualizadas para identificar y localizar información, para que sus resultados puedan ser replicables.

Alcance del Proyecto

Con la realización de este proyecto, se busca brindar una guía para el análisis, localización e identificación de información digital contenida en ordenadores, con sistemas operativos Windows 10.

El desarrollo de este trabajo se basará en un análisis bibliográfico, para poder determinar un procedimiento estándar para el análisis de ordenadores con sistema operativo Windows. Una

vez revisada la literatura, se realizará una investigación experimental, donde, se evaluarán los posibles escenarios en los que un equipo con sistema operativo Windows, requiere someterse a un proceso de análisis forense, para recolectar información suficiente y establecer los pasos a seguir. Por último, se realizará el análisis a un equipo virtual y físico con previa autorización de su propietario, para obtener resultados que nos permitan obtener conclusiones que refuercen a esta guía.

Objetivos del Proyecto

El principal objetivo del presente trabajo es Desarrollar un Marco de Trabajo de Análisis Forense y Localización de Información en Equipos Informáticos con Sistema Operativo Windows 10, con el fin de mejorar la eficiencia en la respuesta ante incidentes de seguridad a partir de las lecciones aprendidas en los diferentes análisis realizados.

Objetivos Específicos:

- Investigar y recopilar las mejores prácticas y métodos de análisis forense para equipos con sistema operativo Windows 10.
- Efectuar prácticas con equipos reales donde se emplearán las diferentes herramientas utilizadas.
- Desarrollar un procedimiento para la preservación de la evidencia digital.
- Proporcionar y recomendar un conjunto de herramientas para localización y extracción de evidencias apoyando al proceso de análisis forense.

Capítulo II - Revisión de Literatura

Estado del Arte

La seguridad de la información en un entorno digitalizado se ha convertido en un área relevante por el aumento de ataques y la sofisticación en el desarrollo de amenazas de los ciberdelincuentes y es aquí donde el análisis forense juega un papel fundamental en la identificación, mitigación y respuesta a estos incidentes de seguridad. Bajo este contexto la investigación forense implica la recolección de datos del equipo atacado, permitiendo al experto indagar en búsqueda de pruebas que indiquen la causa raíz de la vulnerabilidad explotada por el atacante para comprometer el equipo, a tiempo que se puedan desarrollar estrategias efectivas para evitar futuros eventos similares.

En el análisis forense, la identificación de amenazas persistentes tiene un papel crucial en el análisis de malware, ya que permite al investigador entrenarse en las técnicas que los atacantes usan para dar una respuesta rápida a los incidentes, como informa en su investigación Block (2023), las técnicas más utilizadas actualmente radican en la infección de los procesos de memoria de las victimas provocando accesos remotos no autorizados o instalación de software maliciosos, uno de los ejemplos remarcados es el uso de ganchos de API, que buscan alterar la funcionalidad de un API. En otra investigación de Choi, Park, & Lee, (2021) denotan acerca del crecimiento de los dispositivos de almacenamiento basados en memoria flash y la dificultad de la recuperación de los archivos de las áreas no asignadas, esto conlleva a los investigadores forenses utilizar técnicas avanzadas de búsqueda, recopilación de datos y reconstrucción de eventos.

Pero el análisis forense no solo esta como respuesta a incidentes, sino que permite optimizar medidas de seguridad proactiva mediante la evaluación de los sucesos pasados que permitirá entender cómo se llevó a cabo el ataque, qué métodos se utilizaron y cuales brechas fueron

explotadas, y con toda esta información alimentar los sistemas de detección de intrusiones para que se fortalezcan las capacidades de detección temprana y generar métricas eficaces que eviten futuros incidentes (Analuisa Muso & Solís Acosta, 2022).

Bajo todo este contexto se debe resaltar también el marco legal, la conservación de pruebas digitales se torna esencial para cualquier procedimiento judicial. El análisis forense realiza la recopilación y preservación precisa de datos, garantizando que la evidencia sea válida, íntegra y pueda presentarse eficazmente ante un tribunal.

La preservación rigurosa de evidencia digital emerge como un requisito fundamental en el contexto legal, proporcionando una base sólida para acciones judiciales. El análisis forense, al desempeñar un papel clave, se compromete a recopilar y conservar datos de manera meticulosa, asegurando que la evidencia mantenga su integridad y validez, fundamentales para una presentación exitosa en el entorno judicial.

En este análisis no debemos dejar de lado que un investigador forense se apoya en herramientas especializadas para realizar sus funciones de manera efectiva. Estas herramientas abarcan aspectos como la adquisición de imágenes de discos, análisis de memoria, análisis de registros, análisis de red, recuperación de datos, entre otros. Pero la elección de herramientas dependerá de la naturaleza del caso, los requisitos legales, las preferencias del investigador y la complejidad de la investigación (Block, 2023). Siempre es importante que los investigadores forenses se familiaricen con diversas herramientas y es primordial alinearse con estándares y pautas para garantizar la credibilidad y validez de sus procesos y resultados. La conformidad con estas normas no solo mejora la calidad del trabajo forense, sino que también contribuye a la aceptación de la evidencia en contextos legales.

Herramientas de Análisis Forense

Según el documento RFC 3227, existen recomendaciones que deben seguir al seleccionar las herramientas con las que se realizará un análisis forense de un sistema, las que se mencionan a continuación. (Martínez, 2014)

- Utilizar herramientas que no sean parte del sistema, para evitar comprometer la información extraída.
- Utilizar herramientas que generen el menor impacto posible en el escenario.
- Evitar el uso de herramientas con interfaz gráfica.
- Los programas que sean seleccionados deben estar contenidos en dispositivos con permisos de lectura.
- Es importante preparar un conjunto de herramientas para cada sistema a analizar.
- Utilizar programas que permitan detallar y examinar procesos, examinar el estado del sistema y realizar copias bit a bit.

A continuación, se detallan las herramientas que pueden seleccionarse en un análisis forense.

VMware:

VMware desarrolla un software de virtualización, que crea una capa de abstracción sobre el hardware de una computadora, permitiendo que todos sus recursos (memoria, procesamiento, almacenamiento) se dividan en computadoras u ordenadores, que ejecutan su sistema operativo y se comporta como una maquina independiente, y que se manejan con un hipervisor que separa el sistema operativo de cada máquina virtual para evitar interferencias entre sí. Posee varias herramientas dentro de la solución, como, por ejemplo: vSphere Client, para la gestión de archivos a través una línea de comandos (CLI), vSphere Web Services, un kit desarrollo de software para configurar máquinas virtuales con ayuda de otros programas, entre otras herramientas más.

Este tipo de soluciones ha generado muchos beneficios para las compañías hoy en día de los

cuales se puede destacar los siguientes:

- **ROI (Retorno de Inversión):** El contar con una misma infraestructura que permite levantar múltiples máquinas virtuales con su propio SO y adaptarlas a las necesidades de cualquier proyecto, permite a las organizaciones optimizar sus gastos y obtener un mayor retorno de inversión tanto a nivel de infraestructura (hardware, software) y soporte.
- **Eficiencia de espacio y energía:** Eficiencia de espacio y energía: La solución permite obtener una importante eficiencia tanto física como eléctrica, o sea, optimizar el espacio y la energía usadas en un centro de datos para mantener operativas múltiples máquinas en una misma infraestructura. (IBM, 2024).

Forensic Toolkit (FTK)

Es una herramienta desarrollada por una empresa de seguridad conocida como AccessData, la cual, permite crear, obtener y visualizar de manera digital, una copia de un determinado dispositivo de manera exacta, cuya imagen, se podrá utilizar para realizar un análisis forense y examinar la información obtenida en un entorno controlado y seguro, evitando así, comprometer la información y/o dispositivo original.

Funcionalidades de la herramienta FTK:

- **Creación de Imágenes forenses:** Se puede crear copias “exactas” de dispositivos de almacenamientos, tales como, discos duros, CD-ROMs, DVD-ROMs memorias USB, obteniendo toda la información contenida en los mismos (metadatos, imágenes, documentos, etc), para posteriormente, visualizarlos y analizarlos en entornos controlados y seguros sin afectar el dispositivo o información original.
- **Carga de Imágenes forenses:** Se puede cargar imágenes forenses obtenidas que hayan sido obtenidas por otro medio, y cargarlas para realizar el análisis respectivo.

- **Extracción de Archivos:** Se puede extraer archivos de una imagen forense cargada en la herramienta y exportarlos a algún lugar en específico para respaldarlo y analizarlo, de acuerdo con lo requerido.
- **Verificación de Integridad:** Se puede verificar la integridad de la imagen en MD5 hash y SHA1 hash, a fin de constatar que la copia obtenida, corresponde a una copia original del dispositivo que será analizado.
- **Búsqueda de Palabras Claves:** Se puede realizar búsquedas específicas dentro de la imagen forense, lo cual, permite optimizar el tiempo durante el análisis de una determinada información. (KeepCoding, 2023)

Volatility

Volatility basada en Phyton, se desarrolló como una herramienta forense de memoria, de Código abierto, la cual tiene una licencia GPL(General Public License). Es utilizada para analizar incidentes relacionados con malware, los cuales se almacenan en la memoria RAM de un computador. Actualmente es utilizada por investigadores, militares y como recurso educativo. (Daza, 2021) (Volatility Fundation, 2024)

Reg Ripper

La funcionalidad más importante que nos brinda esta herramienta es la de poder sintetizar todo el sistema de archivos de los registros de Windows y resumirlos en un solo documento que permite su entendimiento para posterior análisis. (Mohammed, 2023)

Utilizado para analizar los registros del sistema de archivos de Windows, permite evaluar los registros de cada árbol al crear un archivo .log con el mismo nombre. (Rai, 2023)

Autopsy

Autopsy es una herramienta de análisis forense digital utilizada para investigaciones permitiendo la extracción y examen de datos de dispositivos electrónicos. Funciona mediante la visualización, búsqueda y extracción de información de diversos dispositivos como

computadoras, teléfonos inteligentes y discos duros externos. La herramienta es distribuida bajo licencia de software libre, lo que la hace accesible para investigadores informáticos y profesionales en el campo de la informática forense.

Una característica destacada es su capacidad para analizar imágenes completas de discos duros, lo que evita daños al equipo original, manteniendo siempre la integridad de la evidencia forense. Además, cuenta con un sistema modular de plugins y extensiones que amplían sus funcionalidades, como detección de malware, extracción de contraseñas y análisis avanzados. Otra característica importante de Autopsy es su facilidad para permitir colocar comentarios, etiquetar archivos y generar informes detallados en cada análisis realizado. Facilita la búsqueda por palabras clave en todo el disco analizado y clasifica los archivos en categorías para una visualización más eficiente. Su poder de integración es muy destacable, puede trabajar con módulos de terceros desarrollados por organismos especializados en análisis forense (Rubio Alamillo, 2022).

Para realizar un análisis forense con esta herramienta, es necesario crear un caso que debe estar vinculado a una fuente de datos que comúnmente hace referencia a una imagen forense que puede ser un disco duro, pendrive o tarjeta de memoria. Iniciado el procesamiento como se ha mencionado el investigador se pueden ejecutar acciones como etiquetar archivos, añadir comentarios y generar informes detallados sobre el análisis realizado. Autopsy también destaca por su capacidad para analizar información del encabezado Exif en archivos de imagen JPEG, proporcionando metadatos importantes como fecha, hora y geolocalización (Autopsy Digital Forensics, 2024).

Distribuciones

CAINE Linux – Digital Forensics Project

Computer Aided Investigative Environment, se trata de una distribución Live CD basada en

GNU/Linux y basada en la filosofía de Open Source, la cual, posee una suite de herramientas existentes que permiten al usuario realizar análisis forenses informáticos que ha formado parte como una de las distribuciones más usadas hoy en día (Rashi Garg, 2020).

Dentro de esta suite, podemos encontrar herramientas adicionales a las ya mencionadas anteriormente (**Autopsy y Volatility**) y que servirían para nuestro estudio, como, por ejemplo:

- **Sleuth Kit:** Se trata de un abanico de herramientas que, bajo línea de comandos (CLI), permite generar una copia de información e imágenes de dispositivos de almacenamiento, es decir, discos duros, memorias USB, entre otros dispositivos, para posteriormente, efectuar análisis de dichos datos obtenidos (Brian Carrier, 2023).
- **Wireshark:** Se trata de una herramienta de bastante utilidad en especial en el campo de las telecomunicaciones, dado que, permite analizar paquetes cuyo tráfico pasa a nivel de red de datos, ya sean estos a nivel físico o inalámbrico (wifi). Con este análisis se puede determinar, puertos, protocolos, problemas, seguridad, es decir, información necesaria y muy útil para identificar alguna anomalía o suceso en la información obtenida (Rafael Altube, 2021).
- **QuickHash:** Es una herramienta de distribución open source, la cual, permite comprobar y verificar la integridad de los archivos que se han obtenido y entregados, para posteriormente efectuar un análisis de dicha información. También se utiliza para poder crear hashes dando seguridad a los documentos o archivos creados (Lorena Fernández, 2023).

DEFT - Digital Evidence & Forensic Toolkit

Distribución basada en GNU/Linux, es una suite herramientas que permiten al usuario realizar análisis forense, dichas herramientas incluyen el crear imágenes, validación de integridad, análisis de malware, recuperación de información, gestión de unidades de almacenamiento.

Dentro de sus herramientas más útiles encontramos las siguientes:

Dcfldd: Se dedica a la generación de Hashes, mostrando su avance en tiempo real

Guymager: Su variedad de formatos permite la generación de imágenes forenses rápidamente.

Esximager: Centra su función en trabajar con máquinas virtuales para generar imágenes forenses.

Esta distribución fue concebida para análisis forense en la Universidad Di Bologna, lo cual permite tener una documentación bastante robusta, hay que considerar que esta se encuentra totalmente escrita en idioma italiano. (BeHackerPro, 2021)

Actualmente está disponible la distribución DEFT Zero, la cual requiere de menos recursos y permite operar en sistemas de 32 y 64 bits, incluso con sistemas UEFI. (LORENZO, 2023)

Tsurugi

Tsurugi es una distribución de Linux especializada en informática forense y análisis de seguridad digital. Esta herramienta se utiliza en investigaciones forenses digitales para recolectar, preservar, analizar y presentar evidencia digital de manera eficiente y segura. Esta distribución ofrece un entorno especializado que integra una amplia gama de herramientas forenses en una sola plataforma, lo que facilita el análisis exhaustivo de sistemas, archivos y redes relevantes para una investigación. Algunos de los instrumentos disponibles dentro de Tsurugi incluyen Autopsy para análisis de datos de discos duros, Volatility para análisis de memoria ram, Wireshark para análisis de tráfico de red y Sleuth Kit para recuperación y análisis forense de sistemas informáticos. En conjunto todas estas herramientas permiten a los investigadores llevar a cabo análisis profundos, recuperar datos eliminados, examinar metadatos y reconstruir eventos digitales relevantes para una investigación forense (Somos Libres, 2024).

Al incluir instrumentos reconocidos en la exploración forense Tsurugi se ha ido convirtiendo

en una opción muy válida en la investigación de delitos informáticos, como fraudes en línea, robo de datos entre otros; recuperación de datos eliminados o dañados, crucial al momento de reconstruir eventos o recobrar información importante; análisis de malware, permitiendo comprender el comportamiento malintencionado de los diferentes malwares; análisis especializado de dispositivos móviles

En el contexto de la investigación forense digital, Tsurugi Linux se puede utilizar en modo Live-CD, pero su principal objetivo es instalarse y convertirse en un laboratorio forense completo. Esta distribución de Linux está respaldada por la empresa WetStone Technologies, lo que garantiza actualizaciones regulares y relevancia para las necesidades de los usuarios. Además, Tsurugi Linux es un proyecto de código abierto, lo que permite a la comunidad de usuarios acceder al código fuente, modificarlo y distribuirlo bajo los términos de la licencia (Tsurugi, 2024).

Kali

Conocido como BackTrack en sus inicios, es la distribución basada en DebianGNU/Linux más usada hoy en día. Sus fundadores y responsables de mantenimiento Offensive Security, han logrado llegar a contar con más de 600 aplicaciones de hacking y seguridad. Respaldados por una enorme comunidad en crecimiento, les permite el acreditarse como uno de los sistemas más respaldados en cuanto a soporte y mantenimiento.

El sin número de herramientas que posee esta suite ha centrado su funcionamiento en la seguridad de las redes y los sistemas, centrando su objetivo meramente educativo en fortalecer un internet seguro para los usuarios. (MEJÍAS, 2021)

Esta distribución posee un modo live diseñado específicamente para análisis forense, lo cual permite a sus usuarios el manipular la información sin la necesidad de escribir en sus discos duros. (LORENZO, 2023)

Dentro de la suite de Kali entre muchas otras que se pueden emplear, la que ocupará nuestra

mayor atención es Autopsy, la misma que detallaremos mas adelante su funcionamiento y fortaleza.

Pentoo- Penetration Testing and Security Assessment

Pentoo Linux está basado en Gentoo Linux y diseñado para realizar pruebas de penetración y evaluaciones de seguridad, siendo una alternativa a Kali Linux, ya que contiene varias herramientas de pentesting y de seguridad. Algunas de las herramientas que dispone, agrupadas por su categoría son: (Cyberpunk, 2024)

- **Analyzer Tools:** hidra, Metasploit, Nmap, TCPdum, etc
- **Wireless Tool:** Aircrack-ng, firmware bladerf, bully
- **Crypt Tools:** Hashcat, John the Ripper
- **Forensics Tools:** Autopsy, SleuthKit, Volatility, memdump, foremost, etc.

Encase Forensic

Es una herramienta de investigación bastante poderosa y permite recolectar, analizar y emitir informes digitales, manteniendo un formato válido para efectos legales y que normalmente, son aprobados y avalados por los tribunales respectivos.

Sus principales características radican en la cantidad de sistemas operativos que puede soportar, tales como: **Windows, Linux, Solaris, OSX y AIX**, y, por otro lado, sistemas de archivos, tales como: **FAT12, FAT32, NTFS, Macintosh HFS, HFS+, Linux EXT2/3, Sun Solaris UFS, Reiser, BSD FFS, DVD, AIX, CDFS, JFS, Joilet, UDF e ISO 9660**, entre otros. (Guidance Software, 2005)

Características principales:

- **Obtención válida para temas legales:**

  La duplicación de una imagen es un proceso binario donde cuyos bits son verificados continuamente y donde se asignan valores de CRC’s a los datos que son calculados de manera simultánea durante su adquisición. Una vez obtenida la imagen, se verificará

por segunda vez con un hash MD5, y cuya validación forma parte de la evidencia del dispositivo analizado.

- **Funciones avanzadas de productividad:**

  Los investigadores pueden evaluar y validar de manera simultánea, otras unidades o medios donde se han creado las imágenes previamente. Incluso, se puede obtener una vista previa de los datos obtenidos al acceder a los medios analizados.

- **Programación EnScript para personalizar Encase:**

  Encase Forensic también permite la creación de programas de forma personalizada por medio del lenguaje EnScript para todos sus usuarios, esto a fin de conseguir varias automatizaciones que son muy útiles para realizar ciertas tareas dentro de la investigación. La programación de EnScript está orientada a objetos de manera similar como lo es C++ o Java.

- **Gestionar datos e informes:**

  Permite elaborar y emitir informes relevantes de los datos obtenidos en la investigación, para la presentación de los resultados ante los tribunales correspondientes, gerencias o cualquier autoridad legal que sea el caso. La exportación se la puede realizar en diferentes formatos. (International, 2002)

Normativas de Análisis Forense

Usar normativas en el análisis forense es esencial para garantizar la integridad y eficacia de las investigaciones. En una investigación forense es de vital importancia precautelar el entorno de pruebas, recolectar y preservar las evidencias de manera adecuada, analizarlas minuciosamente y redactar informes claros y precisos (Cajo, Pucuna, Cajo, Coronado, & Orozco, 2018).

El utilizar normativas permite al investigador garantizar la legitimidad de sus análisis, evita errores y proporciona directrices profesionales, algo que se destaca es que existen varias, lo

que hasta el momento ha impedido el que se establezca una metodología única, a continuación, serán analizadas tres, de las cuales será seleccionada una para la generación de este marco de trabajo.

ISO 27037

La normativa ISO 27037 es una normativa internacional que establece directrices para la identificación, recopilación, adquisición y preservación de evidencia digital en entornos de ciberseguridad y análisis forense digital. Esta se enfoca en garantizar la integridad, autenticidad y confiabilidad de la evidencia digital recopilada durante investigaciones legales y forenses. La norma ISO 27037 se basa en tres principios fundamentales: relevancia, confiabilidad y suficiencia, los cuales definen la calidad de cualquier investigación basada en evidencia digital. Además, la norma proporciona pautas para el manejo de la evidencia digital, asegurando procesos diseñados para respetar la integridad de la evidencia y garantizar su validez en procedimientos legales (ciberseguridad.com, s.f.).

Entre los aspectos clave de la normativa ISO 27037 se encuentran las siguientes fases:

- Identificación: En esta fase se determina y se identifica la evidencia digital relevante para la investigación forense. Es crucial para establecer qué pruebas son necesarias y significativas para el caso en cuestión.
- Recolección: Durante esta etapa, se lleva a cabo la recolección de la evidencia digital identificada en la fase anterior. Es fundamental realizar esta tarea de manera cuidadosa y siguiendo procedimientos forenses para preservar la integridad y autenticidad de la evidencia.
- Adquisición: La fase de adquisición implica obtener la evidencia digital de manera forense, asegurando que se mantenga intacta y que se respeten los protocolos establecidos para garantizar su validez en procedimientos legales.
- Preservación: En la fase de preservación, se asegura que la evidencia digital recopilada

se mantenga íntegra y protegida de alteraciones. Es esencial para garantizar que la evidencia sea válida y confiable en futuras investigaciones o procedimientos judiciales.

Estas fases son fundamentales a lo largo del proceso de gestión de evidencia digital. Así mismo la normativa define dos roles especializados: los DEFR (Digital Evidence First Responders) y los DES (Digital Evidence Specialists), quienes son expertos en la primera intervención y gestión de evidencias electrónicas, respectivamente (ciberseguridad.com, s.f.).

Para aplicar la normativa ISO 27037 en la investigación forense, se deben considerar los dispositivos y circunstancias para los cuales proporciona orientación, como medios de almacenamiento digitales, teléfonos móviles, sistemas de navegación móvil, entre otros. Además, se destaca la importancia de contar con un kit de análisis que incluya herramientas como programas para listar y examinar procesos, examinar el estado del sistema y realizar copias bit a bit.

Uno de los principales beneficios que esta normativa brinda a los investigadores, es la confianza de que sus procesos de recolección y preservación de evidencia digital son sólidos y están alineados con estándares internacionales reconocidos. Esto no solo fortalece la postura de ciberseguridad, sino que también facilita la cooperación con autoridades legales en caso de incidentes.

UNE 71506

El estándar español UNE 71506 establece el proceso de análisis forense en el ciclo de gestión de evidencias informáticas. Para complementar la norma UNE 71505, esta norma establece una metodología para la preservación, adquisición, documentación, análisis y presentación de evidencias informáticas. Su objetivo principal es garantizar que las evidencias electrónicas sean confiables y válidas durante todo el proceso forense. La norma UNE 71506 se aplica a organizaciones de cualquier tamaño y sector, así como a profesionales competentes en el campo de la informática forense. No se ocupa de la validación de laboratorios forenses, la

homologación de software ni de la generación, gestión, seguridad, conservación o almacenamiento de pruebas antes de la adquisición (GlobátiKa SL, s.f.).

Las siguientes son las fases de la norma UNE 71506:

Preservación: Su principal objetivo es mantener la legitimidad e inviolabilidad de todas las evidencias, para lo cual el investigador debe almacenarlas de la manera más adecuada, permitiendo cumplir con el objetivo.

- Adquisición: En esta etapa, se obtienen las evidencias digitales de manera segura y con la integridad preservada.
- Documentación: Esta etapa prioriza, el registro detallado y preciso de todas las acciones realizadas durante el proceso de análisis forense.
- Análisis: En esta etapa, las pruebas digitales recopiladas se examinan e interpretan para encontrar patrones, anomalías o información relevante.
- Presentación: implica comunicar los hallazgos del análisis forense de manera clara y efectiva tanto en informes como en posibles testimonios judiciales.

Estas etapas son esenciales para garantizar una gestión adecuada de la evidencia electrónica.

RFC 3227

Directrices para la recolección de evidencias y su almacenamiento.

Uno de los referentes al momento de recolectar y archivar evidencias es el RFC3227, que detalla, desde una perspectiva teórica y completa, la manera de actuar y los pasos a seguir al realizar un análisis forense.

Esta es una guía que destaca las mejores prácticas para determinar la volatilidad de los datos, decidir qué recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos, además de abordar los problemas legales relacionados. Sirve como una ayuda a los administradores de sistemas a recopilar pruebas, lo que facilita la identificación del atacante y aumenta la probabilidad de que las pruebas sean aceptadas en los procesos judiciales

(Ciberforensic, 2020).

Además, en caso de un dilema entre la recolección y el análisis, el RFC 3227 establece que, para garantizar la preservación de la información original, se debe priorizar la recolección de evidencias antes que el análisis. Este método mantiene la integridad de los datos recolectados y evita cualquier manipulación que pueda dañar las pruebas en un proceso forense.

La Figura 1 ilustra los pasos que normalmente se deben seguir dentro del proceso de análisis forense:

Los puntos más relevantes detallados dentro del RFC 3227 son:

- Guía de recolección de evidencias.
- Procedimiento de recolección
- Procedimiento de almacenamiento
- Herramientas necesarias

Figura 1.

Principales procesos de análisis forense

Nota: Obtenido de (Martínez, 2014)

Capítulo III - Metodología de Investigación

En el presente trabajo se proponen las siguientes metodologías:

1. **Revisión Bibliográfica:** En Ecuador se han venido llevando a cabo varios ciberdelitos principalmente sobre equipos bajo sistemas operativos Windows, por este motivo, es importante establecer procesos de análisis (Analuisa Muso & Solís Acosta, 2022). Este método permite realizar una revisión exhaustiva de literatura especializada en análisis forense y las prácticas recomendadas para sistemas operativos Windows, considerando las siguientes etapas de análisis forense. (Olmo, 2020).
    - Evaluación Preliminar.
    - Recolección de evidencia.
    - Análisis de evidencias.
    - Elaboración de un Informe.
2. **Análisis Cuantitativo:** En este método se requiere recolectar información sobre los escenarios más comunes, para lo cual, se establecerán ambientes controlados para el análisis de los dispositivos seleccionados, ya sean equipos virtuales o físicos.
3. **Análisis Experimental:** Finalmente el análisis de los resultados nos permitirá establecer de manera general el proceso para analizar equipos con sistemas Windows 10.

Evaluación de la metodología para desarrollo del Framework

En la sección anterior se realizaron tres metodologías más utilizadas en la investigación forense, cada una con ventajas que garantizan la integridad, precisión y eficiencia de las investigaciones y con desventajas distintas. Luego compararemos para determinar cuál de estas tres metodologías se alinea de una mejor forma al enfoque de nuestro Framework.

La ISO 27037 es una norma internacional ampliamente utilizada que entrega una guía integral de todo el proceso de análisis forense digital, otra de las características importantes es su

adaptabilidad a los diferentes casos en distintas industrias lo que la hace una opción importante al momento de contar con escenarios complejos. Por su esencia detalla y exhaustivamente su uso puede incidir en la necesidad de mayor tiempo para la investigación tornándose en ciertas ocasiones un tanto compleja y con mucho trabajo para el especialista forense. También se debe tomar en cuenta que esta norma igualmente tiene un costo de adquisición e igualmente si el investigador o la institución desean certificarse puede implicar costos significativos, especialmente para las organizaciones más pequeñas o con recursos limitados.

La UNE 71506 es una normativa que se caracteriza debido a su diseño específicamente adaptado al ámbito español, así como también a sus normativas y legislaciones, tal y como lo resaltan Cajo. & et al, en su investigación en 2018. Una característica importante es su enfoque práctico que entrega directrices claras al momento de realizar una investigación forense, así mismo cuenta con una ampliar integración a marcos legales españoles garantizando una validez. Pero una desventaja es que al estar alineado netamente a España queda limitada internacionalmente debido a que no siempre las leyes son iguales entre países y es ahí donde el investigador debe evaluar que partes de la metodología debe utilizar y que no, lo que implicaría un mayor tiempo en la investigación. También el especialista forense debe tomar en cuenta que esta metodología tiene un costo tanto de adquisición como de certificación.

El RFC 3227 proporciona un conjunto de directrices sobre el análisis forense digital lo que entrega al investigador una mayor flexibilidad y adaptabilidad en diferentes contextos, esta es una metodología de fácil acceso debido ya que se encuentra disponible en línea de forma abierta lo que facilita su consulta, y también cuenta con una comunidad de profesionales que de manera colaborativa la mantienen actualizada. Si bien es cierto que no es una normativa formal como la ISO 27037 o la UNE71506, pero es ampliamente utilizada a nivel internacional lo que le da un gran alcance.

Una vez analizada detenidamente las características de cada metodología, podemos identificar

las fortalezas y limitaciones de cada una, lo que nos permite seleccionar al RFC 3227 como la metodología base para nuestro framework, debido principalmente a su flexibilidad y accesibilidad.

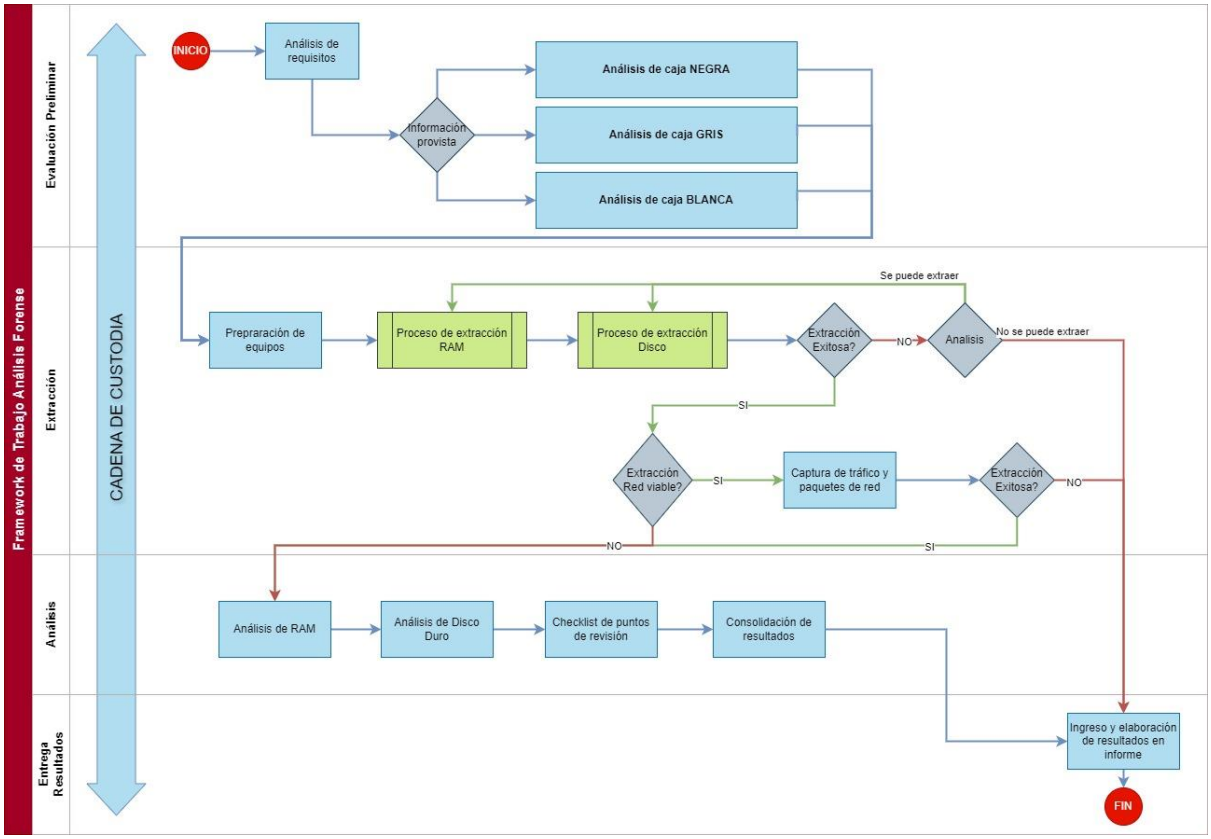
Desarrollo del Marco de Trabajo

Diagrama UML Framework

El siguiente Diagrama UML representa el Framework propuesto para el análisis forense Digital, diseñado para guiar y organizar el proceso de investigación en casos de delitos cibernéticos. Este framework se basa en las buenas prácticas del RFC 3227, abarca desde la evaluación preliminar del hecho, la recolección, el análisis de evidencia hasta la entrega de resultados. Cada elemento del diagrama ilustra una serie de fases clave del análisis, a través de las cuales, se busca proporcionar una guía clara y estructurada para los profesionales de la investigación digital en la gestión efectiva de casos forenses.

Figura 2.

Diagrama UML del Framework propuesto



Desarrollo del Framework

Cadena de Custodia

Dentro de las consideraciones que debemos tomar en cuenta para mantener una correcta cadena de custodia, debemos considerar las siguientes pautas:

1. **Documentación:** Deberá ser detallada, minuciosa y amigable al usuario para mostrar gran cantidad de detalle al leerlo, deberá considerar el proceso desde el inicio del trabajo, acciones realizadas, personal e instituciones involucradas, y los datos de tiempo que permitan identificar las circunstancias y resultados.
2. **Etiquetado de la evidencia:** El manejo de un sistema de etiquetado único que permita verificar y ubicar los registros en una línea de tiempo nos permitirá incluso identificar en que etapa del proceso se ha generado el registro/evidencia.
3. **Control de acceso:** Se deben establecer medidas de seguridad perimetral y lógica para evitar el acceso no autorizado a las evidencias provistas. Incluso se debe definir espacios físicos limitados y supervisados que garanticen la confidencialidad.
4. **Conservación de evidencias:** La preservación de evidencias deberá controlarse con una verificación de hash que permita mantener la integridad de la información. Se deberá emplear técnicas de copia forense para extraer ya analizar la información sin realizar modificaciones a la evidencia original
5. **Registro de accesos:** Cualquier interacción que se realice con la evidencia provista, será necesario identificar en un registro, el mismo dictará las pautas necesarias para una identificación del acceso incluyendo la identificación de la persona que acceda, temporalidad y un detalle de la actividad realizada.
6. **Definición de funciones:** Las funciones y responsabilidades del equipo que analiza deberá mantenerse documentada para evidenciar la correcta manipulación de la evidencia por parte del equipo forense.

7. **Herramientas Oficiales:** Se deberá procurar el uso de herramientas y metodologías validadas por entes de control oficiales que garanticen la efectividad del análisis y validez en un eventual proceso judicial.
8. **Personal capacitado:** Debe considerarse un requisito fundamental contar con el personal altamente calificado, con las certificaciones que avalen la capacidad para realizar un trabajo efectivo.
9. **Materiales sugeridos:**
    - Equipo de Protección Personal (Mascarilla, guantes de latex, etc)
    - Computadora con procesador Core i5 o superior.
    - Herramientas para análisis forense (FTK, Caine, Kali Linux, Autopsy, RegRip,)
    - Discos Externos nuevos.
    - Implementos de registro fotográfico.

Documentos Para Considerar como Anexo

Según el caso, se debe considerar y contar con plantillas sobre los servicios o trabajos que se brindarán, documentos, por ejemplo, como el de la primera entrevista, donde se detalla la fecha, información del cliente, alcance del trabajo, fechas de reuniones, entre otros aspectos.

Otro documento importante y relevante, es el de secreto profesional, donde se detalla la relación de confidencialidad entre cliente e investigador. Por tanto, toda información que durante la investigación pueda solicitarse y/o dialogarse, será estrictamente confidencial.

También se considera necesario contar con documentos de consentimiento por parte del cliente, esto debido al acceso (casi siempre) a información sensible y/o delicada, y cuyo manejo de esa información, está amparada por la ley de datos personales.

Por último, ya establecido el alcance de los trabajos y tareas por realizar, es necesario firmar el documento por honorarios profesionales, donde se detallarán los valores y gastos que deberá incurrir el cliente, considerando un aporte inicial del 50% de su total.

Todos los documentos detallados anteriormente, se recomienda agregarse como anexo como parte de los informes que se deberán entregar.

Evaluación Preliminar

Se debe considerar que existen 3 tipos de análisis a realizar, caja blanca, caja gris y caja negra.

Caja Blanca

Este procedimiento se lo aplicará cuando, el cliente nos proporciona información relevante de los equipos y/o infraestructura a analizar, es decir, puede entregar información como, por ejemplo: la marca y/o modelo del equipo, tipo y versión del sistema operativo instalado, cantidad y capacidad de memorias RAM y almacenamiento, programas instalados, y adicional, información acerca del comportamiento y/o acontecimientos que suscitaron con el equipo en cuestión.

Estos casos podrían suscitarse generalmente, cuando, el cliente tiene conocimiento medio o avanzado en lo referente al campo tecnológico y/o directamente relacionado con lo suscitado en el equipo.

Caja Gris

Este procedimiento se lo aplicará cuando, el cliente nos proporciona información parcial o casi nula de los equipos y/o infraestructura a analizar, es decir, entregando información muy básica o limitada tanto a nivel de hardware como de software de la mencionada anteriormente en el análisis de caja blanca. Y de igual manera, información parcial o casi nula respecto al comportamiento y/o acontecimientos que suscitaron con el equipo en cuestión.

Estos casos podrían suscitarse generalmente, cuando, el cliente no tiene mayor conocimiento en lo referente al campo tecnológico y/o no estaba relacionado directamente con lo suscitado en el equipo.

Caja Negra

Este procedimiento se lo aplicará cuando, el cliente no nos proporciona información alguna de

los equipos y/o infraestructura a analizar, ni tampoco, acerca del comportamiento y/o acontecimientos que suscitaron con el equipo en cuestión. Por tanto, la revisión deberá ser más minuciosa y exhaustiva tanto a nivel de software y hardware del equipo a analizar.

Estos casos podrían suscitarse generalmente, cuando, el cliente no tiene información o conocimiento en lo referente al campo tecnológico y/o no estaba relacionado con lo suscitado en el equipo.

En cualquiera de los 3 casos expuestos, ya sea en el análisis de caja blanca, gris o negra, se deberá considerar todo lo necesario para la revisión del equipo, y bajo el mejor criterio profesional, efectuar el análisis según sea el caso propuesto.

Extracción de Evidencia.

Para la extracción de la evidencia y siguiendo las directrices de la guía RFC 3227, se debe iniciar con la extracción de información desde lo más volátil hacia lo menos volátil. Para lo cual, y bajo mejor criterio, se deberá analizar y determinar la información de mayor volatilidad a fin de proceder con la respectiva extracción. Esto debido a que, tras el apagado de cualquier equipo, la información desaparece o se elimina al cabo de un tiempo.

Figura 3.

Orden de volatilidad – RFC 3227

Por motivos expuestos, se procederá de la siguiente manera:

1. **Extracción de Memoria RAM:** Con ayuda de herramientas, tales como, **FTK Imager**, se obtendrá una imagen a través del volcado de la memoria RAM del equipo, donde, se creará una nomenclatura para la imagen, y cuya información, deberá detallarse explícitamente en el informe a elaborar.

   La información que se deberá considerar para etiquetar, nombrar y obtener la imagen de la memoria RAM a analizar, deberá ser similar a la siguiente:

   - **Path destino**
   - **Nombre del archivo**
   - **Número de evidencia**
   - **Descripción** (opcional)

2. **Extracción de Discos:** Con ayuda de las herramientas **Caine** para el montado de los discos y **Guymager** para la extracción de la imagen, se obtendrá una imagen a través del volcado del disco duro del equipo, donde, se creará igualmente una nomenclatura para la imagen, y cuya información, deberá detallarse explícitamente en el informe a elaborar.

   La información que se deberá considerar para etiquetar, nombrar y obtener la imagen

del disco dura a analizar, deberá ser similar a la siguiente:

- **Formato**
- **Nombre del archivo**
- **Número de evidencia**
- **Descripción** (opcional)
- **Path destino**

Cabe mencionar que, con la imagen obtenida del disco, también se ha obtenido los logs del sistema, los cuales, se procederán a revisar posteriormente.

Análisis de Evidencias

Creación de Hash

Al momento de tener identificados las distintas evidencias se iniciará por gestionar la creación de hash empleando la herramienta QuickHash, se debe tomar las siguientes consideraciones:

1. Identificar y definir el procedimiento y las herramientas necesarias para levantar el hash, estas pueden incluir desde verificar los periféricos necesarios para el levantamiento, capacidad de almacenamiento, suministro eléctrico y demás.
2. Acorde a la necesidad del análisis se deberá seleccionar un tipo de algoritmo de cifrado, siendo la recomendación de este Framework un algoritmo igual o superior a SHA-256.
3. Para terminar con la creación del hash, se deberá hacer una verificación de la integridad de este. Finalmente se ha de registrar en los informes de levantamiento de información los hashes obtenidos.

Análisis de RAM

Para iniciar el proceso de análisis de la RAM se deberá asegurar un entorno de trabajo que incluya una copia de la imagen a analizarse, continuando con el proceso de análisis, se debe realizar los siguientes pasos:

Empleando la herramienta **volatility**, realizamos el análisis de la captura de memoria, para lo

cual podremos usar los siguientes comandos:

1. Usar el comando **imageninfo** para obtener los perfiles con los que se puede trabajar en el análisis.
2. Emplear el comando **kdbgscan** con el cual se obtendrá más información de los perfiles obtenidos.
3. Revisar el listado de los procesos que se encontraban activos en el momento de la captura con el comando **pslist.**
4. A partir de este paso se deberá evaluar los procesos en busca de factores fuera de lo común, empleando el criterio de aquellos que son normales de una ejecución en Windows o programas oficiales.
   4.1. Una vez identificados los procesos que se consideren sospechosos, se deberá realizar el análisis exhaustivo de estos. Aplicando los siguientes parámetros a cada proceso identificado podremos evaluar de mejor manera:
      4.1.1. Se realizará un escaneo de las conexiones realizadas desde el dispositivo empleando el plugin **netscan**, en busca de IP's externas a la red, mismas que emplearemos en el siguiente paso.
      4.1.2. Usando la herramienta **Shodan**, se realizará un análisis de las direcciones encontradas en busca de más información que nos permita establecer criterios de conclusión.
      4.1.3. Si se da el caso de no encontrar información en la herramienta Shodan, podremos hacer uso de la herramienta **whois** con la ayuda de la consola de Kali-Linux.
      4.1.4. Con el fin de mantener información más clara, podemos aplicar el comando **dig -x <<IP>>**, con el cual podremos revisar los registros de DNS's para la IP en revisión.

4.1.5. Finalmente es necesario el establecer la relación entre las conexiones establecidas y los procesos identificados.

4.2. Si no ha sido clara la relación entre los procesos y conexiones establecidas, será necesario obtener el árbol de procesos a fin de identificar completamente el proceso, realizando los siguientes pasos:

4.2.1. Empleando el comando **pstree**, obtenemos el arbol de procesos en busca de procesos hijos que se relacionen con el proceso en revisión.

4.2.2. Usando el comando **dlllist**, se podrá revisar las librerías DLL, con el cual podremos analizar aquellas que estén ligadas al PID.

4.3. Para continuar con el análisis del proceso en revisión se ha de evaluar con el comando **filescan** en busca de los archivos, punteros o permisos relacionados.

4.4. Continuando con el análisis de la memoria RAM, se ha de emplear el comando **photorec** para extraer los archivos relacionados y posteriormente identificarlos como un disco duro a revisar, para esto, emplearemos los siguientes pasos:

4.4.1. Se deberá seleccionar el sistema de archivos al que pertenece la captura

4.4.2. Identificar la ubicación donde recibiremos los archivos a descargar

4.4.3. Se realizará un filtro en el directorio que contiene los archivos descargados, empleando el criterio del proceso identificado en los pasos anteriores.

4.4.4. Se debe realizar un análisis con la información obtenida, de darse el caso que no se encuentre información al respecto, se deberá emplear recursos como **Google Dorking, DeepWeb** que ayuden en el entendimiento del proceso en análisis.

4.5. Finalmente, es necesario definir el si el proceso identificado se relaciona con algún tipo de programa maligno, identificando su modo de operación y la ubicación de este para posteriormente realizar el análisis en el disco duro del equipo.

Análisis de Disco

Para el análisis del Disco Duro provisto, se ha emplear la herramienta Autopsy, estas deberán considerar el emplear las palabras claves del software malicioso detectado y seguir las directrices:

1. Configurar el software Autopsy en un nuevo caso, indicando los siguientes valores:
    a. Nombre del caso
    b. Ubicación del archivo base
    c. Información adicional del autor
    d. Exactitud de las palabras buscadas
    e. Ajustar los parámetros de ingesta de data a fin de optimizar los tiempos de extracción.
2. Cuando se ha finalizado el análisis del disco duro, se ha de empezar por buscar los resultados cuyos valores sean exactos a los parametrizados
3. Se deberá realizar una revisión a los eventos que coincidan con las palabras clave.
4. Se deberá buscar en los archivos descargados posibles conexiones con servidores.
5. Procedemos con el historial de navegación, verificando si han existido descargas adicionales que nos permita evaluar más aristas de los archivos con palabras clave.
6. Deberemos llegar a obtener un archivo de ejecución al cual poder hacerle un análisis exhaustivo.
7. Para examinar los archivos obtenidos se podría hacer uso de las siguientes herramientas **Virus Total, Meta defender**
8. Emplear la herramienta **RegRipper,** para realizamos un análisis de los registros
9. Concluyendo el análisis del disco, a partir de la información recolectada se ha de levantar alimentar el informe de resultados.

Entrega de Resultados

El informe pericial es un documento que detalla las conclusiones que el investigador forense

obtiene analizando las evidencias. Este documento puede ser utilizado tanto en ámbitos judiciales y empresariales, y para su redacción el investigador debe poseer conocimientos técnicos y legales.

Según Medrano, 2022 un informe debe contener los siguientes:

1. Portada
    1.1. Título del caso.
    1.2. Identificación del caso.
    1.3. Fecha del Informe.
    1.4. Dirigido a.
    1.5. Nombre del perito.
2. Índice
3. Declaración de tachas (si aplica).
4. Identificación del perito
5. Cuerpo del informe.
    5.1. Objeto.
    5.2. Alcance.
    5.3. Antecedentes.
    5.4. Consideraciones Preliminares.
    5.5. Documentos de Referencia.
    5.6. Terminología y Abreviaturas.
    5.7. Desarrollo del estudio.
        5.7.1. Elementos objeto del estudio.
        5.7.2. Procedimientos y métodos empleados.
        5.7.3. Resultados obtenidos, análisis e interpretación.
        5.7.4. Situación de los elementos del estudio.

6. Conclusiones.
7. Anexos (si aplica).

Es importante recalcar que un informe pericial informático debe caracterizarse por ser claro, conciso, objetivo, estar fundamentado y coherente.

Capítulo IV - Pruebas de Concepto y Análisis de Resultados

En el ámbito del análisis forense, las pruebas de concepto desempeñan un papel crucial en la validación y evaluación de herramientas y técnicas. Los laboratorios validadores son entornos diseñados específicamente para llevar a cabo estas pruebas, permitiendo al grupo comprobar la efectividad y fiabilidad tanto del framework como de las herramientas seleccionadas. Estos laboratorios no solo sirven como espacios para evaluar escenarios de delitos cibernéticos, sino también como bancos de pruebas para verificar la integridad y precisión de los procesos propuestos en nuestro framework para el tratamiento de evidencia digital. A continuación, se presentan dos laboratorios en condiciones totalmente distintas cómo pruebas de concepto para garantizar la rigurosidad y validez de las técnicas empleadas en el presente trabajo, brindando una guía a los profesionales del campo.

Laboratorio 1

Antecedentes:

El presente laboratorio surge como respuesta a la solicitud nuestro cliente, quien experimenta problemas de rendimiento en su computador. El cliente ha proporcionado una captura de la memoria RAM y una imagen del disco duro para su análisis exhaustivo.

Se ha reportado que su máquina experimenta periodos de lentitud significativos, lo que afecta negativamente su productividad y desempeño. Estos lapsos de baja velocidad en el sistema están generando preocupación en el cliente, quien busca identificar y remediar cualquier posible anomalía o compromiso en la integridad de su sistema.

El análisis forense digital se hará para identificar cualquier actividad sospechosa, malware, procesos no autorizados o cualquier otro factor que pueda contribuir a los problemas de rendimiento del sistema. Se empleará el framework de trabajo que hemos desarrollado para examinar tanto la memoria RAM como la imagen del disco duro, con el fin de detectar y documentar cualquier indicio de actividad maliciosa o inusual.

Características del equipo:

La evidencia entregada pertenece a un computador con:

RAM: 4 GB

Disco duro: 60Gb

Sistema Operativo: Windows 10 home

Análisis de las Evidencias

Análisis de la Memoria RAM

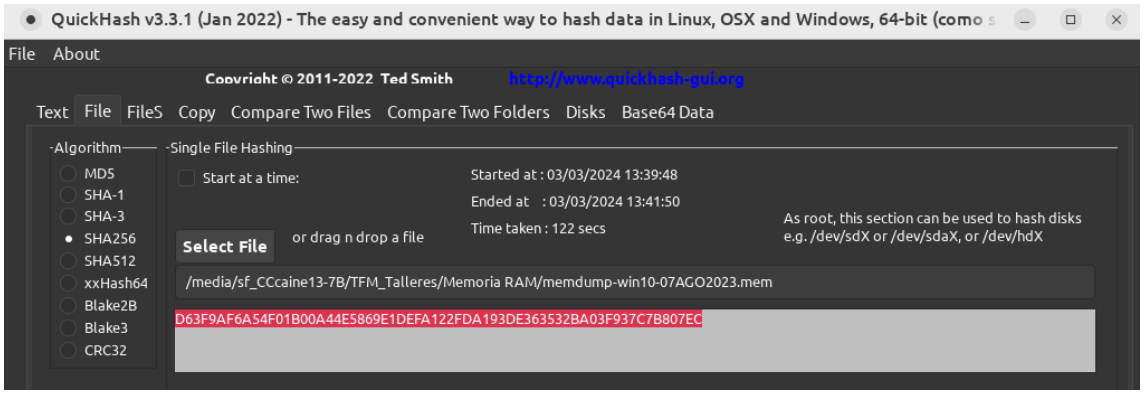
En función de las evidencias entregadas se inicia el proceso del análisis de memoria RAM obteniendo su hash mediante la herramienta QuickHash.

Como se observa en la Figura 4, el valor del hash con la utilización de un algoritmo SHA-256

es: D63F9AF6A54F01B00A44E5869E1DEFA122FDA193DE363532BA03F937C7B807EC

Figura 4.

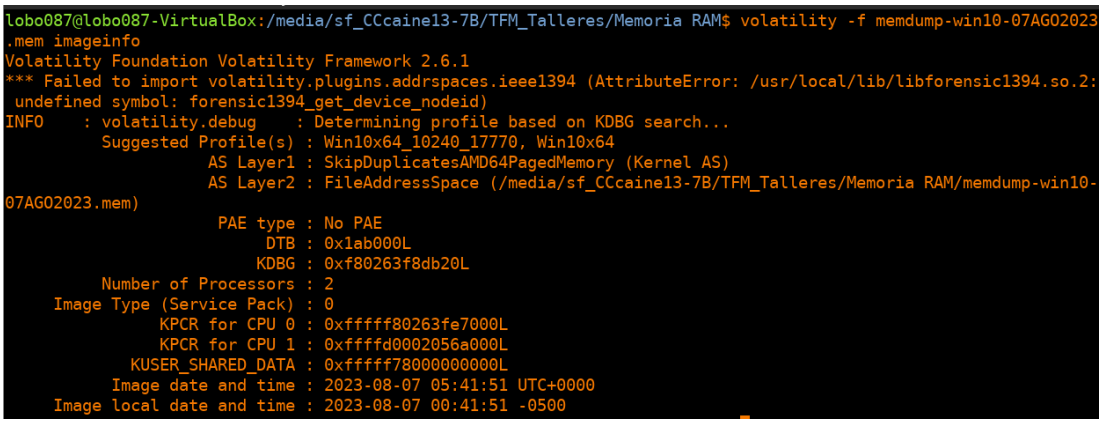
SHA-256 memoria RAM



Segundo, se procede el análisis de la captura abriendo la herramienta Volatility y el argumento/ la del plugin a utilizar **imageinfo**, para obtener los perfiles con los que se podrá trabajar.

Figura 5.

Plugin imageinfo



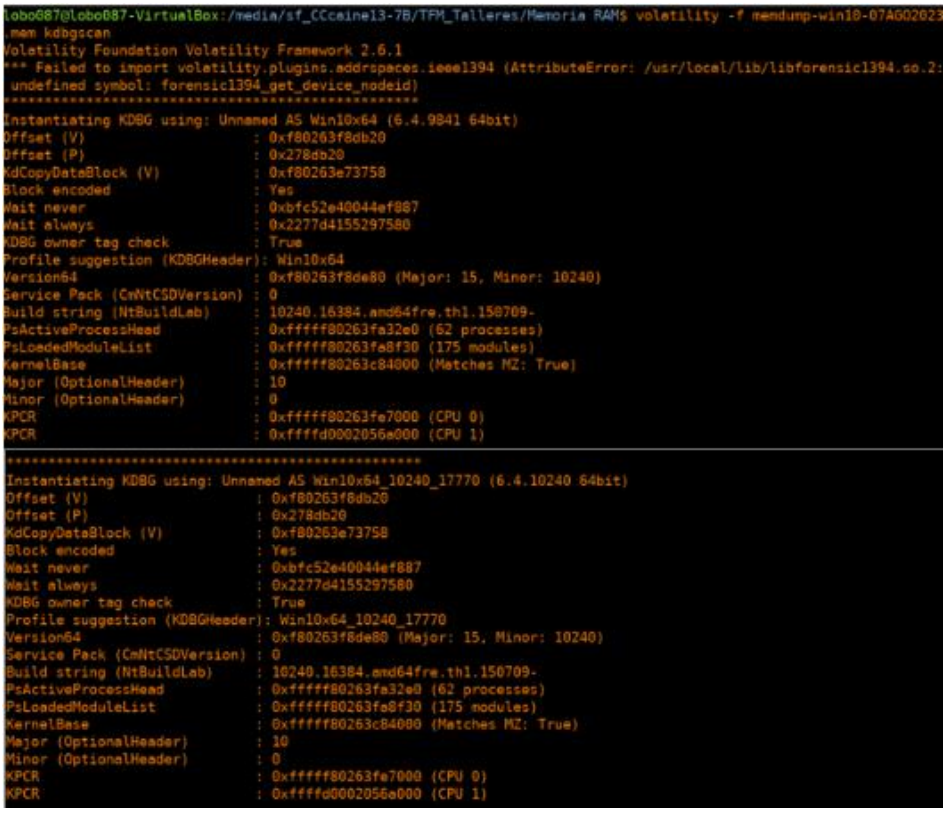
Los perfiles obtenidos fueron:

- Win10x64_10240_17770
- Win10x64

Para obtener un mayor detalle de los perfiles se utiliza el argumento/ el plugin **kdbgscan**

Figura 6.

Plugin kdbgscan



Tras evaluar detenidamente los perfiles se pueden ver claramente que los dos tienen las mismas características por lo que para continuar con el análisis se decidió trabajar con el perfil **Win10x64**

Continuamos el análisis con la búsqueda de los procesos que se encontraban activos en esa captura con el plugin **pslist**

Figura 7.

Plugin pslist

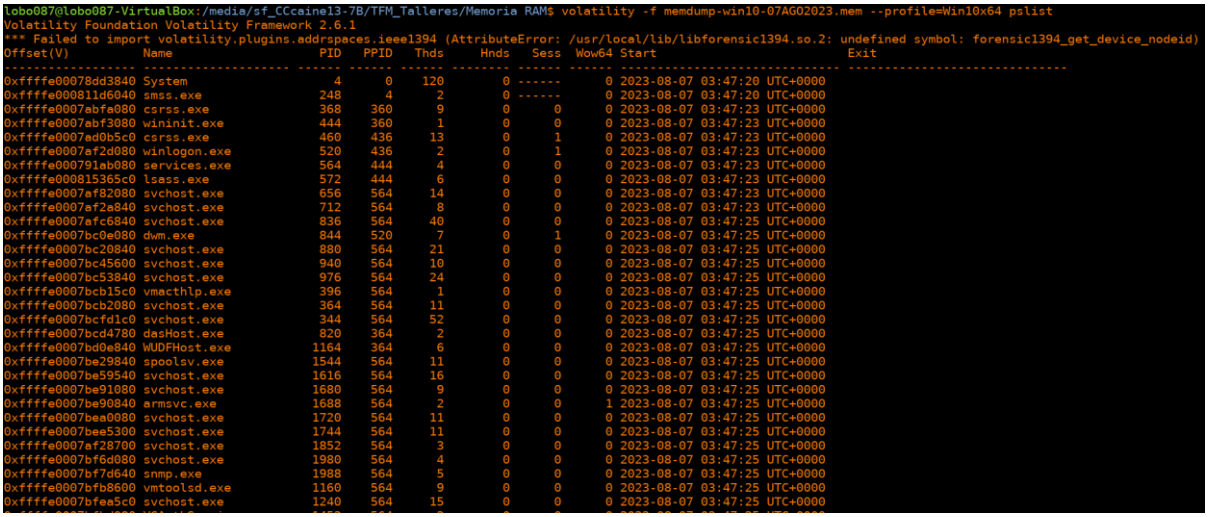
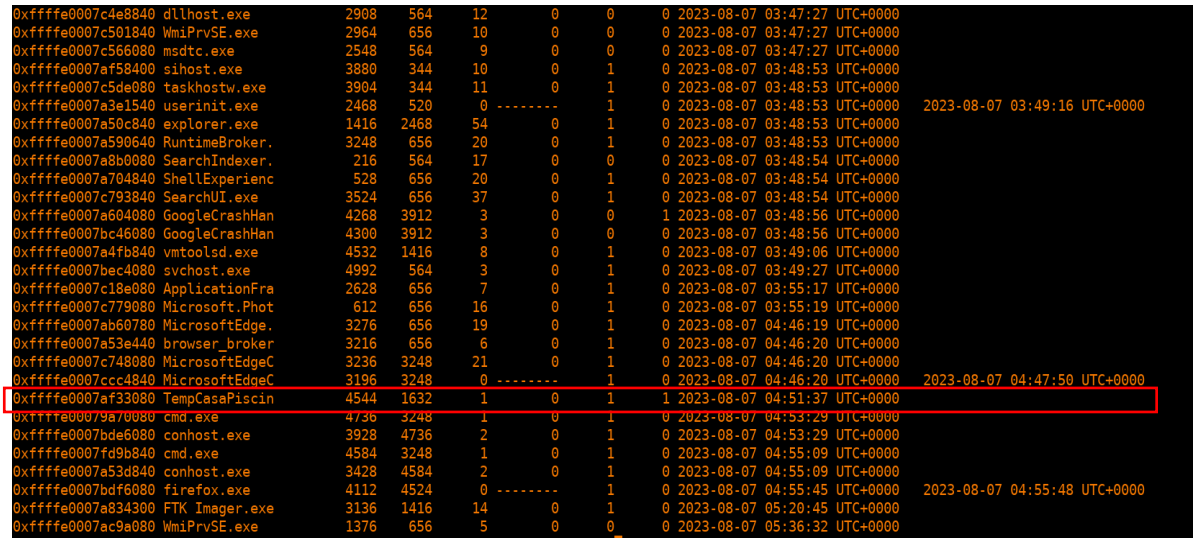


Figura 8.

Plugin Pslist continuación

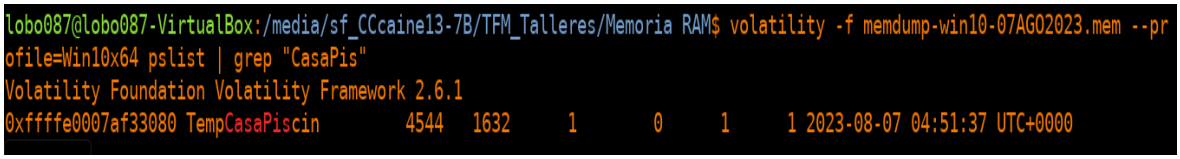


```
0xffffe0007c4e8840 dllhost.exe           2908    564     12        0      0      0 2023-08-07 03:47:27 UTC+0000
0xffffe0007c501840 WmiPrvSE.exe          2964    656     10        0      0      0 2023-08-07 03:47:27 UTC+0000
0xffffe0007c566080 msdtc.exe             2548    564      9        0      0      0 2023-08-07 03:47:27 UTC+0000
0xffffe0007af58400 sihost.exe            3880    344     10        0      1      0 2023-08-07 03:48:53 UTC+0000
0xffffe0007c5de080 taskhostw.exe         3904    344     11        0      1      0 2023-08-07 03:48:53 UTC+0000
0xffffe0007a3e1540 userinit.exe          2468    520      0 --------      1      0 2023-08-07 03:48:53 UTC+0000   2023-08-07 03:49:16 UTC+0000
0xffffe0007a50c840 explorer.exe          1416   2468     54        0      1      0 2023-08-07 03:48:53 UTC+0000
0xffffe0007a590640 RuntimeBroker.        3248    656     20        0      1      0 2023-08-07 03:48:53 UTC+0000
0xffffe0007a8b0080 SearchIndexer.         216    564     17        0      0      0 2023-08-07 03:48:54 UTC+0000
0xffffe0007a704840 ShellExperienc         528    656     20        0      1      0 2023-08-07 03:48:54 UTC+0000
0xffffe0007c793840 SearchUI.exe          3524    656     37        0      1      0 2023-08-07 03:48:54 UTC+0000
0xffffe0007a604080 GoogleCrashHan        4268   3912      3        0      0      1 2023-08-07 03:48:56 UTC+0000
0xffffe0007bc46080 GoogleCrashHan        4300   3912      3        0      0      0 2023-08-07 03:48:56 UTC+0000
0xffffe0007a4fb840 vmtoolsd.exe          4532   1416      8        0      1      0 2023-08-07 03:49:06 UTC+0000
0xffffe0007bec4080 svchost.exe           4992    564      3        0      1      0 2023-08-07 03:49:27 UTC+0000
0xffffe0007c18e080 ApplicationFra        2628    656      7        0      1      0 2023-08-07 03:55:17 UTC+0000
0xffffe0007c779080 Microsoft.Phot         612    656     16        0      1      0 2023-08-07 03:55:19 UTC+0000
0xffffe0007ab60780 MicrosoftEdge.        3276    656     19        0      1      0 2023-08-07 04:46:19 UTC+0000
0xffffe0007a53e440 browser_broker        3216    656      6        0      1      0 2023-08-07 04:46:20 UTC+0000
0xffffe0007c748080 MicrosoftEdgeC        3236   3248     21        0      1      0 2023-08-07 04:46:20 UTC+0000
0xffffe0007ccc4840 MicrosoftEdgeC        3196   3248      0 --------      1      0 2023-08-07 04:46:20 UTC+0000   2023-08-07 04:47:50 UTC+0000
0xffffe0007af33080 TempCasaPiscin        4544   1632      1        0      1      1 2023-08-07 04:51:37 UTC+0000
0xffffe0007a70080 cmd.exe                4736   3248      1        0      1      0 2023-08-07 04:53:29 UTC+0000
0xffffe0007bde6080 conhost.exe           3928   4736      2        0      1      0 2023-08-07 04:53:29 UTC+0000
0xffffe0007fd9b840 cmd.exe               4584   3248      1        0      1      0 2023-08-07 04:55:09 UTC+0000
0xffffe0007a53d840 conhost.exe           3428   4584      2        0      1      0 2023-08-07 04:55:09 UTC+0000
0xffffe0007bdf6080 firefox.exe           4112   4524      0 --------      1      0 2023-08-07 04:55:45 UTC+0000   2023-08-07 04:55:48 UTC+0000
0xffffe0007a834300 FTK Imager.exe        3136   1416     14        0      1      0 2023-08-07 05:20:45 UTC+0000
0xffffe0007ac9a080 WmiPrvSE.exe          1376    656      5        0      0      0 2023-08-07 05:36:32 UTC+0000
```

Aquí se encontró un proceso llamado **TempCasaPiscin**. Esto parece algo fuera de lo común, por lo tanto procedemos a realizar filtros de texto para una mejor visualización.

Figura 9.

Filtrado de proceso en sospecha

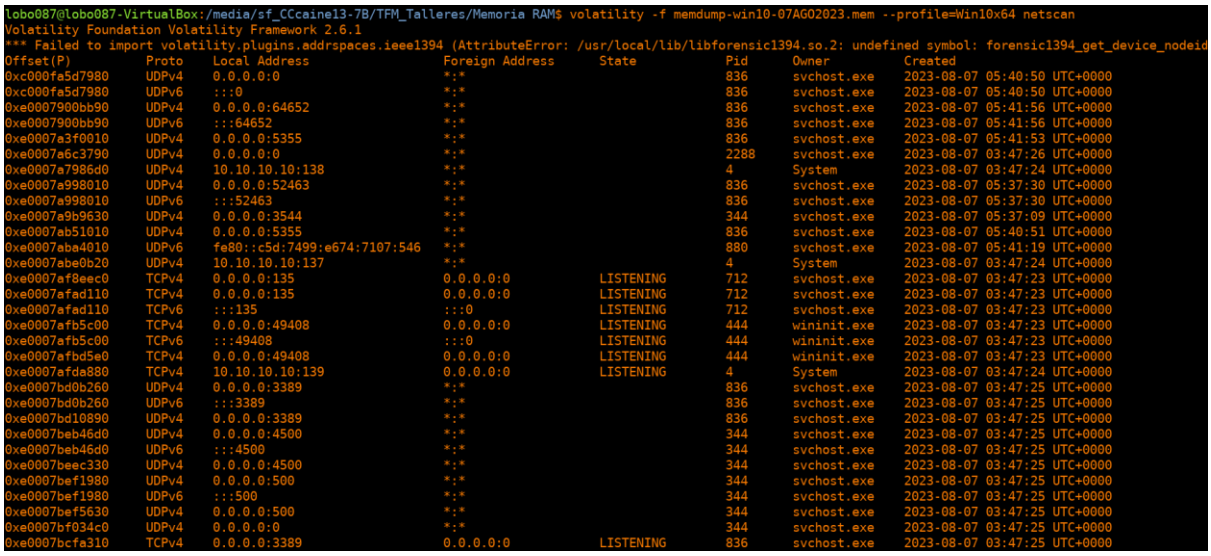


```
lobo087@lobo087-VirtualBox:/media/sf_CCcaine13-7B/TFM_Talleres/Memoria RAM$ volatility -f memdump-win10-07AGO2023.mem --pr
ofile=Win10x64 pslist | grep "CasaPis"
Volatility Foundation Volatility Framework 2.6.1
0xffffe0007af33080 TempCasaPiscin        4544   1632      1        0      1      1 2023-08-07 04:51:37 UTC+0000
```

El siguiente paso es realizar una revisión de las conexiones realizadas desde el dispositivo con el plugin **netscan**

Figura 10.

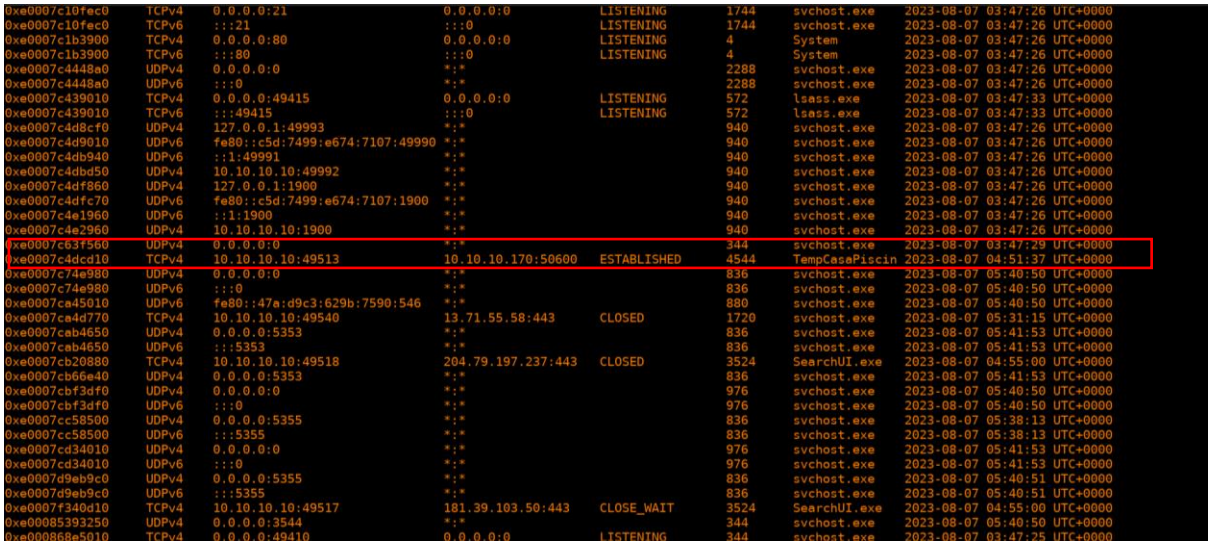
Plugin netscan



```
lobo087@lobo087-VirtualBox:/media/sf_CCcaine13-7B/TFM_Talleres/Memoria RAM$ volatility -f memdump-win10-07AGO2023.mem --profile=Win10x64 netscan
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_device_nodeid
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0xc000fa5d7980     UDPv4    0.0.0.0:0                      *:*                                   836      svchost.exe    2023-08-07 05:40:50 UTC+0000
0xc000fa5d7980     UDPv6    :::0                           *:*                                   836      svchost.exe    2023-08-07 05:40:50 UTC+0000
0xe0007900bb90     UDPv4    0.0.0.0:64652                  *:*                                   836      svchost.exe    2023-08-07 05:41:56 UTC+0000
0xe0007900bb90     UDPv6    :::64652                       *:*                                   836      svchost.exe    2023-08-07 05:41:56 UTC+0000
0xe0007a3f0010     UDPv4    0.0.0.0:5355                   *:*                                   836      svchost.exe    2023-08-07 05:41:53 UTC+0000
0xe0007a6c3790     UDPv4    0.0.0.0:0                      *:*                                   2288     svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007a7986d0     UDPv4    10.10.10.10:138                *:*                                   4        System         2023-08-07 03:47:24 UTC+0000
0xe0007a998010     UDPv4    0.0.0.0:52463                  *:*                                   836      svchost.exe    2023-08-07 05:37:30 UTC+0000
0xe0007a998010     UDPv6    :::52463                       *:*                                   836      svchost.exe    2023-08-07 05:37:30 UTC+0000
0xe0007a9b9630     UDPv4    0.0.0.0:3544                   *:*                                   344      svchost.exe    2023-08-07 05:37:09 UTC+0000
0xe0007ab51010     UDPv4    0.0.0.0:5355                   *:*                                   836      svchost.exe    2023-08-07 05:40:51 UTC+0000
0xe0007aba4010     UDPv6    fe80::c5d:7499:e674:7107:546   *:*                                   880      svchost.exe    2023-08-07 05:41:19 UTC+0000
0xe0007abe0b20     UDPv4    10.10.10.10:137                *:*                                   4        System         2023-08-07 03:47:24 UTC+0000
0xe0007af8eec0     TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        712      svchost.exe    2023-08-07 03:47:23 UTC+0000
0xe0007afad110     TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        712      svchost.exe    2023-08-07 03:47:23 UTC+0000
0xe0007afad110     TCPv6    :::135                         :::0                 LISTENING        712      svchost.exe    2023-08-07 03:47:23 UTC+0000
0xe0007afb5c00     TCPv4    0.0.0.0:49408                  0.0.0.0:0            LISTENING        444      wininit.exe    2023-08-07 03:47:23 UTC+0000
0xe0007afb5c00     TCPv6    :::49408                       :::0                 LISTENING        444      wininit.exe    2023-08-07 03:47:23 UTC+0000
0xe0007afbd5e0     TCPv4    0.0.0.0:49408                  0.0.0.0:0            LISTENING        444      wininit.exe    2023-08-07 03:47:23 UTC+0000
0xe0007afda880     TCPv4    10.10.10.10:139                0.0.0.0:0            LISTENING        4        System         2023-08-07 03:47:24 UTC+0000
0xe0007bd0b260     UDPv4    0.0.0.0:3389                   *:*                                   836      svchost.exe    2023-08-07 03:47:25 UTC+0000
0xe0007bd0b260     UDPv6    :::3389                        *:*                                   836      svchost.exe    2023-08-07 03:47:25 UTC+0000
0xe0007bd10890     UDPv4    0.0.0.0:3389                   *:*                                   836      svchost.exe    2023-08-07 03:47:25 UTC+0000
0xe0007beb46d0     UDPv4    0.0.0.0:4500                   *:*                                   344      svchost.exe    2023-08-07 03:47:25 UTC+0000
0xe0007beb46d0     UDPv6    :::4500                        *:*                                   344      svchost.exe    2023-08-07 03:47:25 UTC+0000
0xe0007beec330     UDPv4    0.0.0.0:4500                   *:*                                   344      svchost.exe    2023-08-07 03:47:25 UTC+0000
0xe0007bef1980     UDPv4    0.0.0.0:500                    *:*                                   344      svchost.exe    2023-08-07 03:47:25 UTC+0000
0xe0007bef1980     UDPv6    :::500                         *:*                                   344      svchost.exe    2023-08-07 03:47:25 UTC+0000
0xe0007bef5630     UDPv4    0.0.0.0:500                    *:*                                   344      svchost.exe    2023-08-07 03:47:25 UTC+0000
0xe0007bf034c0     UDPv4    0.0.0.0:0                      *:*                                   344      svchost.exe    2023-08-07 03:47:25 UTC+0000
0xe0007bcfa310     TCPv4    0.0.0.0:3389                   0.0.0.0:0            LISTENING        836      svchost.exe    2023-08-07 03:47:25 UTC+0000
```

Figura 11.

Plugin netscan continuación



```
0xe0007c10fec0     TCPv4    0.0.0.0:21                     0.0.0.0:0            LISTENING        1744     svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c10fec0     TCPv6    :::21                          :::0                 LISTENING        1744     svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c1b3900     TCPv4    0.0.0.0:80                     0.0.0.0:0            LISTENING        4        System         2023-08-07 03:47:26 UTC+0000
0xe0007c1b3900     TCPv6    :::80                          :::0                 LISTENING        4        System         2023-08-07 03:47:26 UTC+0000
0xe0007c4448a0     UDPv4    0.0.0.0:0                      *:*                                   2288     svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c4448a0     UDPv6    :::0                           *:*                                   2288     svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c439010     TCPv4    0.0.0.0:49415                  0.0.0.0:0            LISTENING        572      lsass.exe      2023-08-07 03:47:33 UTC+0000
0xe0007c439010     TCPv6    :::49415                       :::0                 LISTENING        572      lsass.exe      2023-08-07 03:47:33 UTC+0000
0xe0007c4d8cf0     UDPv4    127.0.0.1:49993                *:*                                   940      svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c4d9010     UDPv6    fe80::c5d:7499:e674:7107:49990 *:*                                   940      svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c4db940     UDPv6    ::1:49991                      *:*                                   940      svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c4dbd50     UDPv4    10.10.10.10:49992              *:*                                   940      svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c4df860     UDPv4    127.0.0.1:1900                 *:*                                   940      svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c4dfc70     UDPv6    fe80::c5d:7499:e674:7107:1900  *:*                                   940      svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c4e1960     UDPv6    ::1:1900                       *:*                                   940      svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c4e2960     UDPv4    10.10.10.10:1900               *:*                                   940      svchost.exe    2023-08-07 03:47:26 UTC+0000
0xe0007c63f560     UDPv4    0.0.0.0:0                      *:*                                   344      svchost.exe    2023-08-07 03:47:29 UTC+0000
0xe0007c4dcd10     TCPv4    10.10.10.10:49513              10.10.10.170:50600   ESTABLISHED      4544     TempCasaPiscin 2023-08-07 04:51:37 UTC+0000
0xe0007c74e980     UDPv4    0.0.0.0:0                      *:*                                   836      svchost.exe    2023-08-07 05:40:50 UTC+0000
0xe0007c74e980     UDPv6    :::0                           *:*                                   836      svchost.exe    2023-08-07 05:40:50 UTC+0000
0xe0007ca45010     UDPv6    fe80::47a:d9c3:629b:7590:546   *:*                                   880      svchost.exe    2023-08-07 05:40:50 UTC+0000
0xe0007ca4d770     TCPv4    10.10.10.10:49540              13.71.55.58:443      CLOSED           1720     svchost.exe    2023-08-07 05:31:15 UTC+0000
0xe0007cab4650     UDPv4    0.0.0.0:5353                   *:*                                   836      svchost.exe    2023-08-07 05:41:53 UTC+0000
0xe0007cab4650     UDPv6    :::5353                        *:*                                   836      svchost.exe    2023-08-07 05:41:53 UTC+0000
0xe0007cb20880     TCPv4    10.10.10.10:49518              204.79.197.237:443   CLOSED           3524     SearchUI.exe   2023-08-07 04:55:00 UTC+0000
0xe0007cb66e40     UDPv4    0.0.0.0:5353                   *:*                                   836      svchost.exe    2023-08-07 05:41:53 UTC+0000
0xe0007cbf3df0     UDPv4    0.0.0.0:0                      *:*                                   976      svchost.exe    2023-08-07 05:40:50 UTC+0000
0xe0007cbf3df0     UDPv6    :::0                           *:*                                   976      svchost.exe    2023-08-07 05:40:50 UTC+0000
0xe0007cc58500     UDPv4    0.0.0.0:5355                   *:*                                   836      svchost.exe    2023-08-07 05:38:13 UTC+0000
0xe0007cc58500     UDPv6    :::5355                        *:*                                   836      svchost.exe    2023-08-07 05:38:13 UTC+0000
0xe0007cd34010     UDPv4    0.0.0.0:0                      *:*                                   976      svchost.exe    2023-08-07 05:41:53 UTC+0000
0xe0007cd34010     UDPv6    :::0                           *:*                                   976      svchost.exe    2023-08-07 05:41:53 UTC+0000
0xe0007d9eb9c0     UDPv4    0.0.0.0:5355                   *:*                                   836      svchost.exe    2023-08-07 05:40:51 UTC+0000
0xe0007d9eb9c0     UDPv6    :::5355                        *:*                                   836      svchost.exe    2023-08-07 05:40:51 UTC+0000
0xe0007f340d10     TCPv4    10.10.10.10:49517              181.39.103.50:443    CLOSE_WAIT       3524     SearchUI.exe   2023-08-07 04:55:00 UTC+0000
0xe00085393250     UDPv4    0.0.0.0:3544                   *:*                                   344      svchost.exe    2023-08-07 05:40:50 UTC+0000
0xe000868e5010     TCPv4    0.0.0.0:49410                  0.0.0.0:0            LISTENING        344      svchost.exe    2023-08-07 03:47:25 UTC+0000
```

Aquí se pueden ver varias conexiones de navegación web realizadas por el puerto 443 a las direcciones externas de la red 13.71.55.58, 204.79.197.237 y 181.39.103.50. Por lo tanto, es necesario llevar a cabo la investigación correspondiente, para lo cual se utilizará la herramienta Shodan para obtener más información sobre dichas direcciones.

La dirección 13.71.55.58 pertenece a un servicio de Microsoft llamado settings.data.microsoft.com, que permite la conexión de aplicaciones de Windows para

actualizar sus configuraciones de manera dinámica.

Figura 12.

Resultado de búsqueda con shodan de ip 13.71.55.58

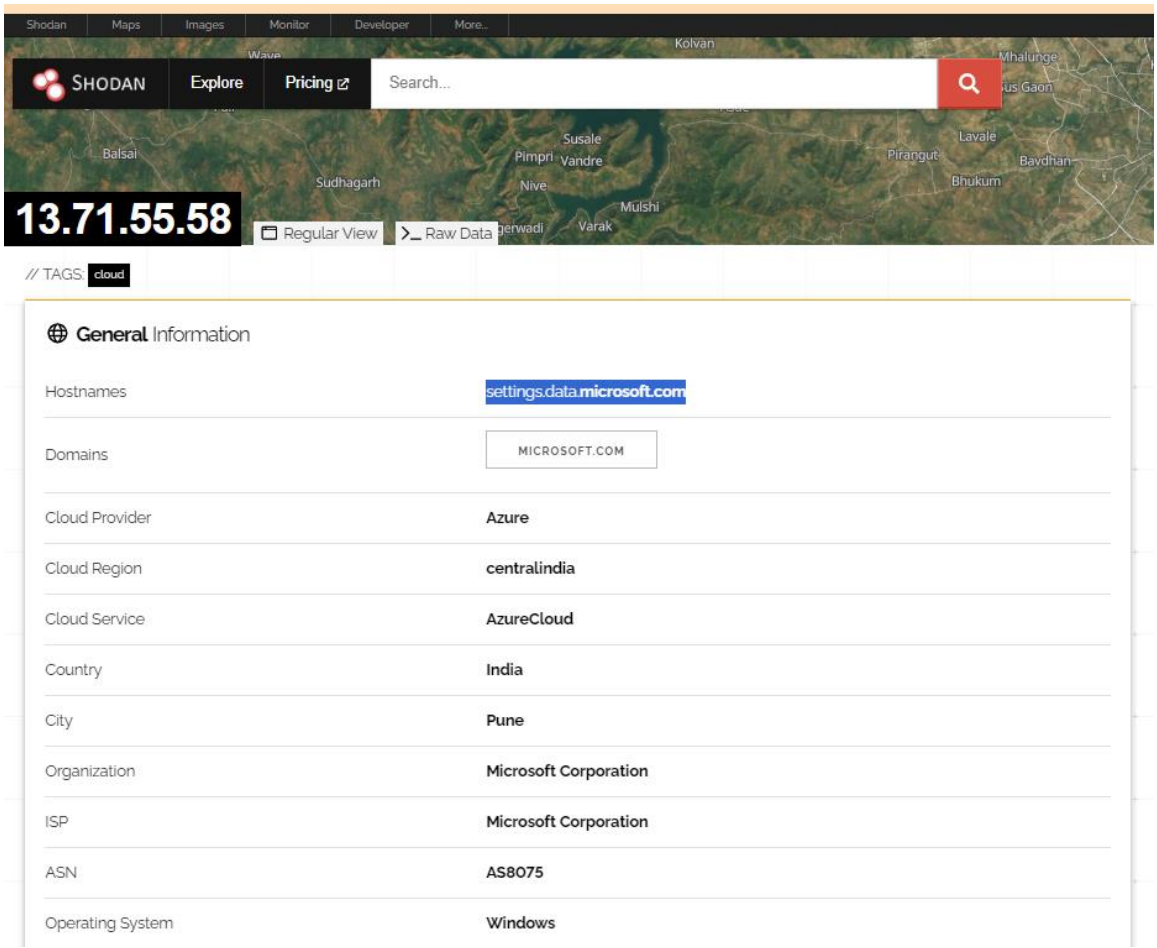
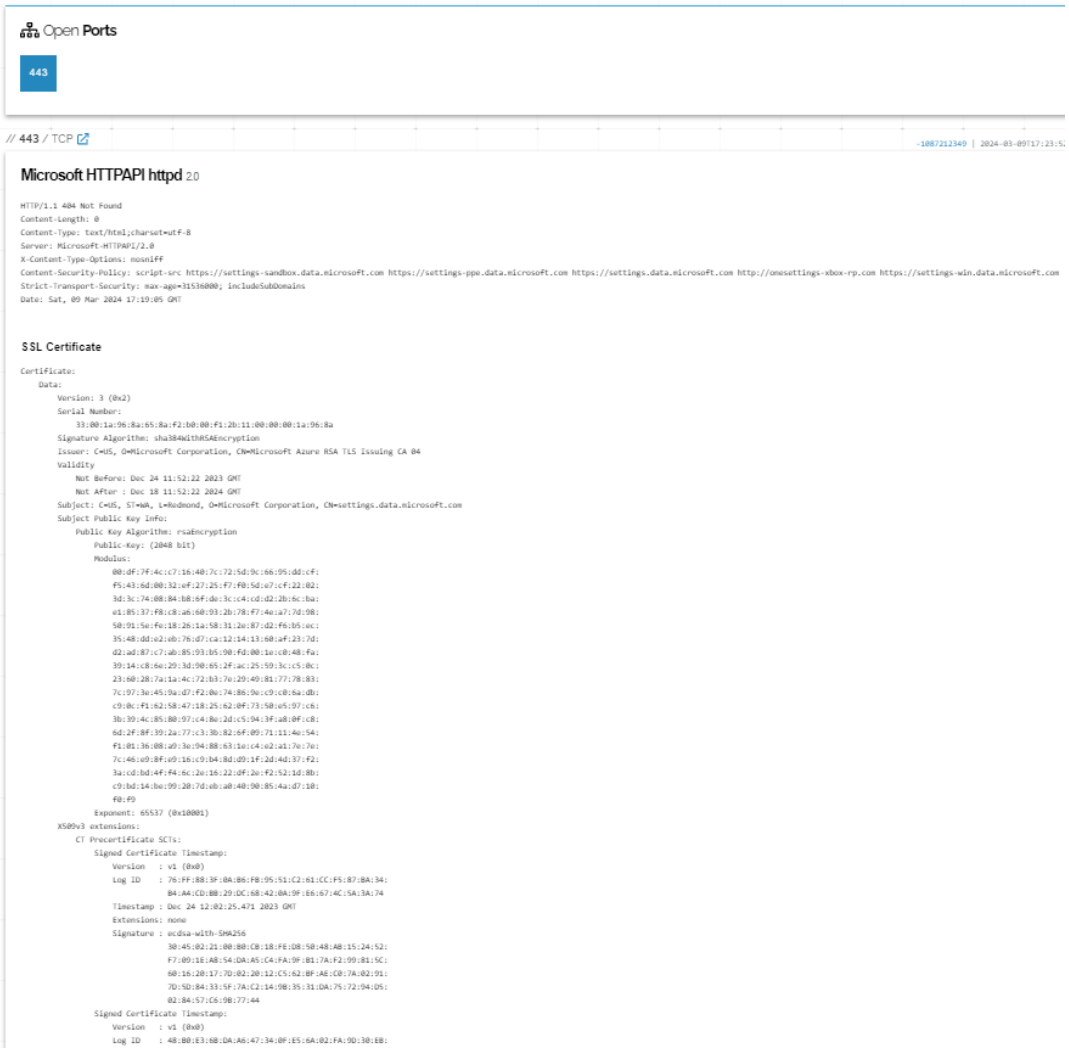


Figura 13.

Resultado de búsqueda con shodan de ip 13.71.55.58- Certificados SSL



La dirección 204.79.197.237 pertenece a un servicio de Bing que es el motor de busquedas de Microsoft.

Figura 14.

Servicio Bing Microsoft

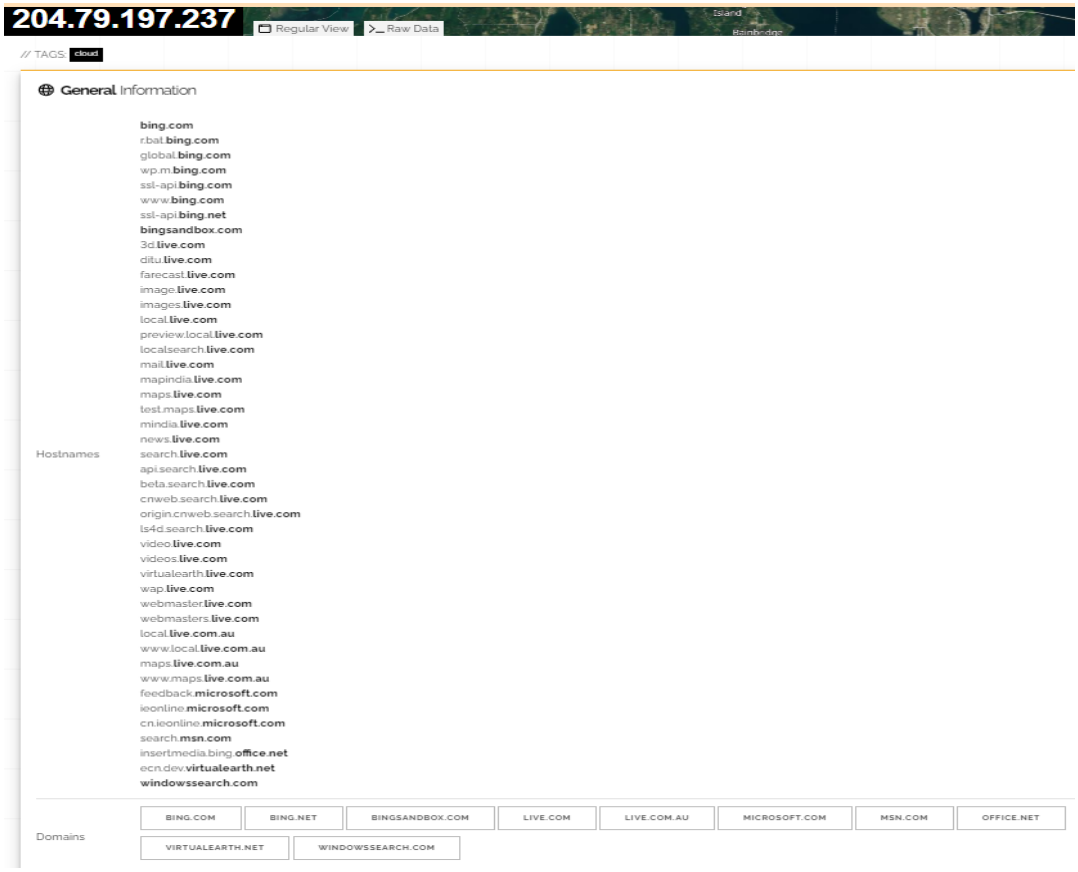


Figura 15.

Puerto 80 TCP del servicio

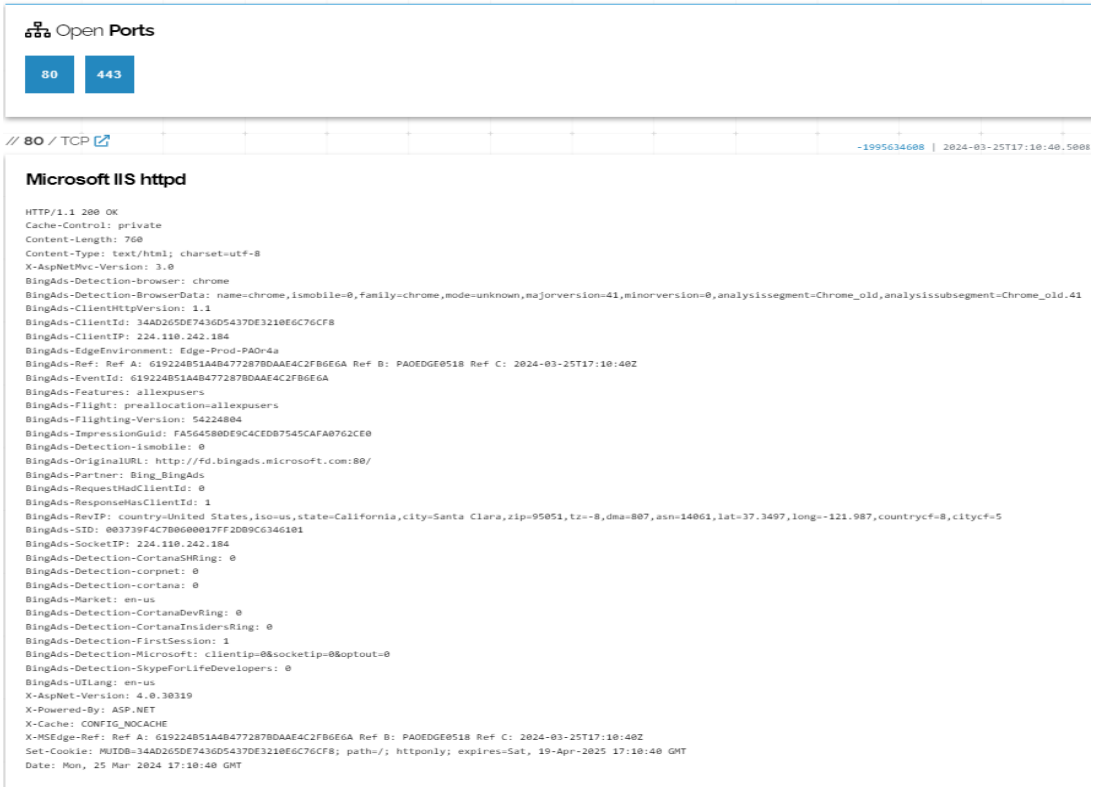
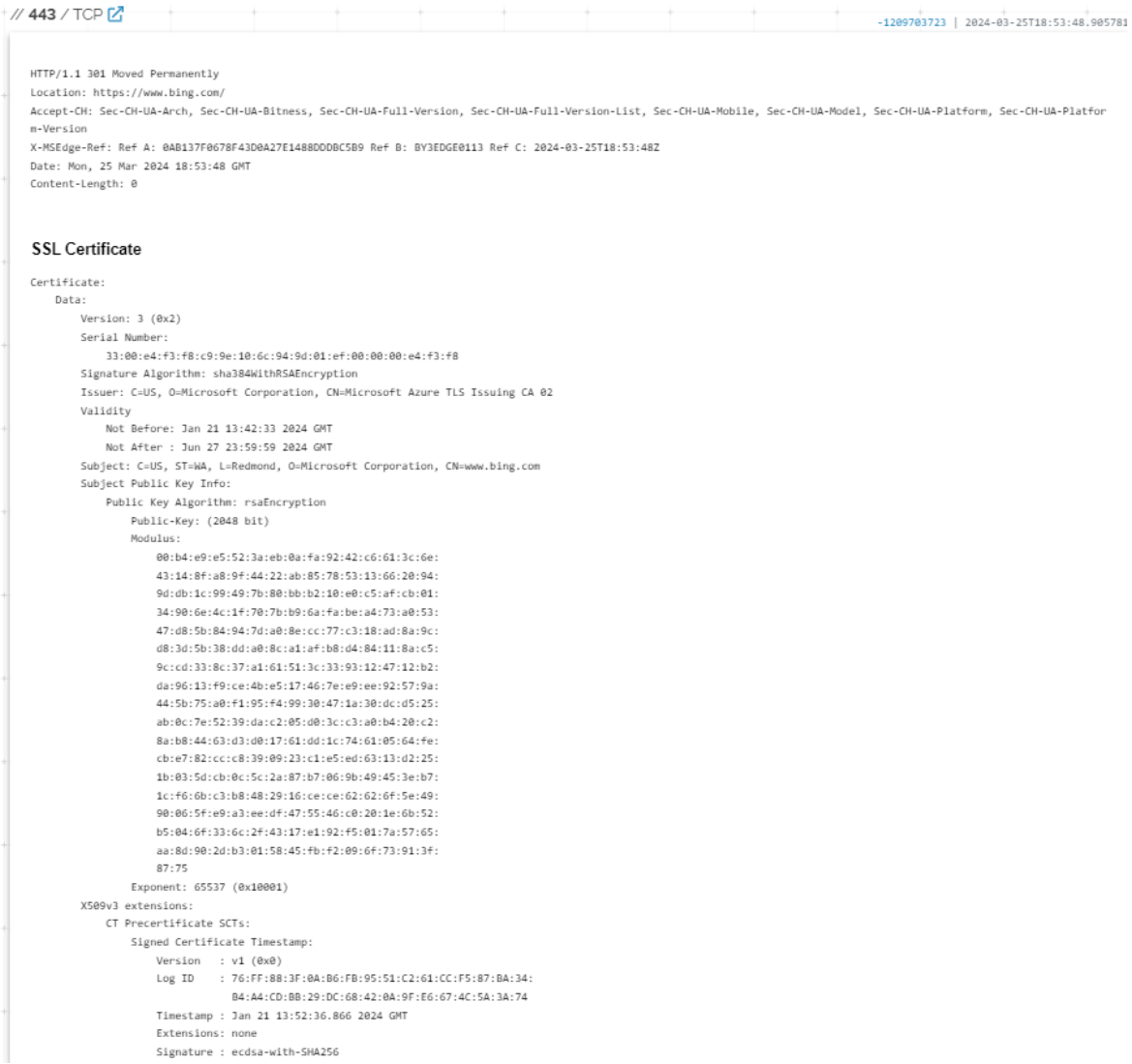


Figura 16.

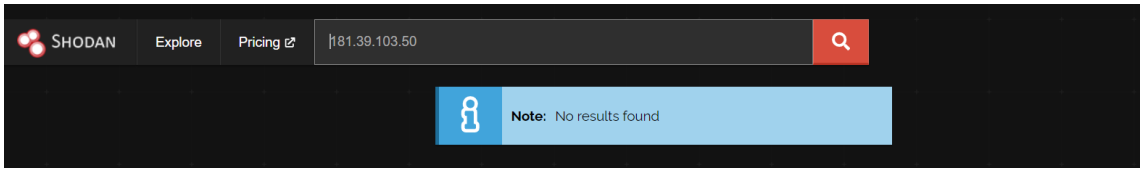
Puerto 443 TCP del servicio



La dirección 181.39.103.50 no muestra resultados en Shodan

Figura 17.

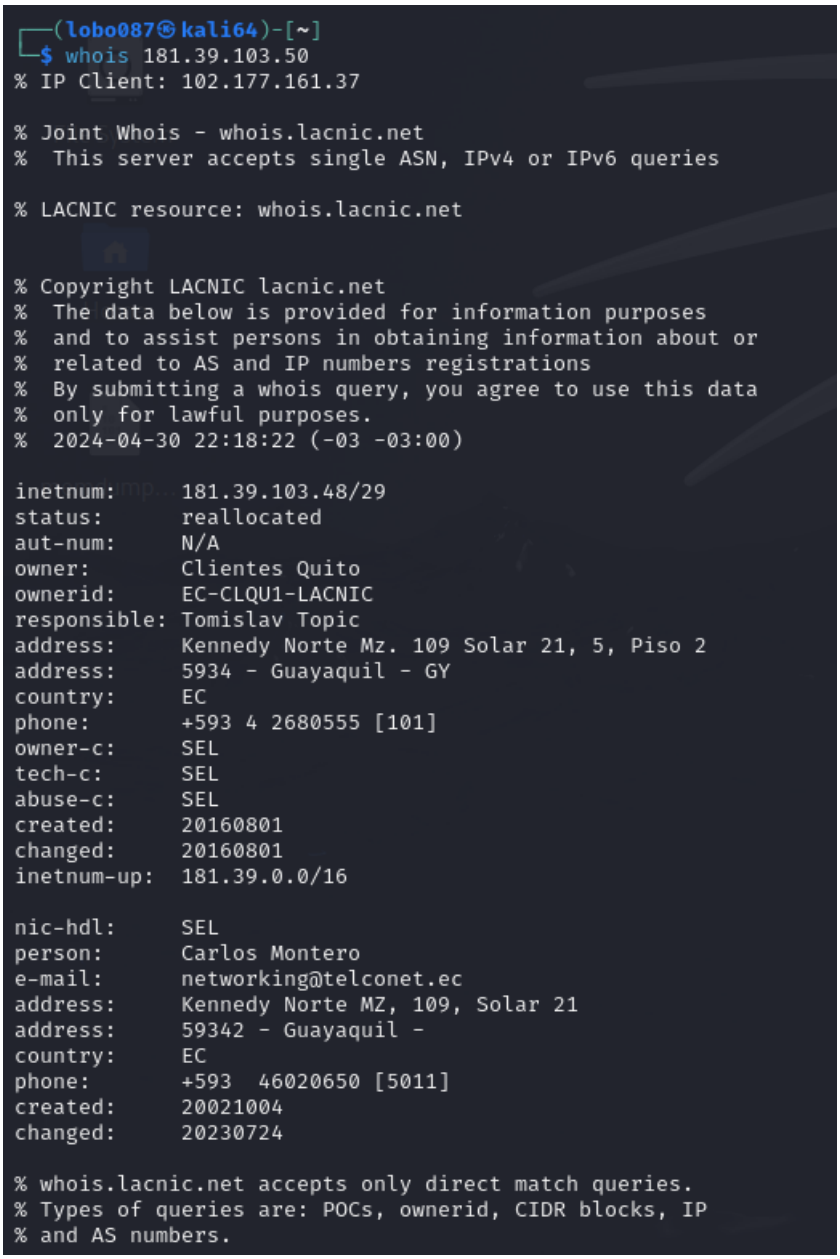
Resultado shodan 181.39.103.50



Por lo que se utiliza otra herramineta whois en la que se obtiene la información que se muestra a continuación.

Figura 18.

Información whois de ip 181.39.103.50



Con la finalidad de obtener mayor información de esta ip se utiliza el comando dig-x que ayuda a buscar en los registros DNS, así se obtuvo la siguiente información

Figura 19.

Comando dig ip 181.39.103.50

La con la información proporcionada de las figuras 18 y 19 se puede llegar a determinar que este es un nodo de comunicación.

Finalmente se realiza un filtro para buscar si entre las conexiones existe alguna relación con el PID 4544 de “TempCasaPiscin”

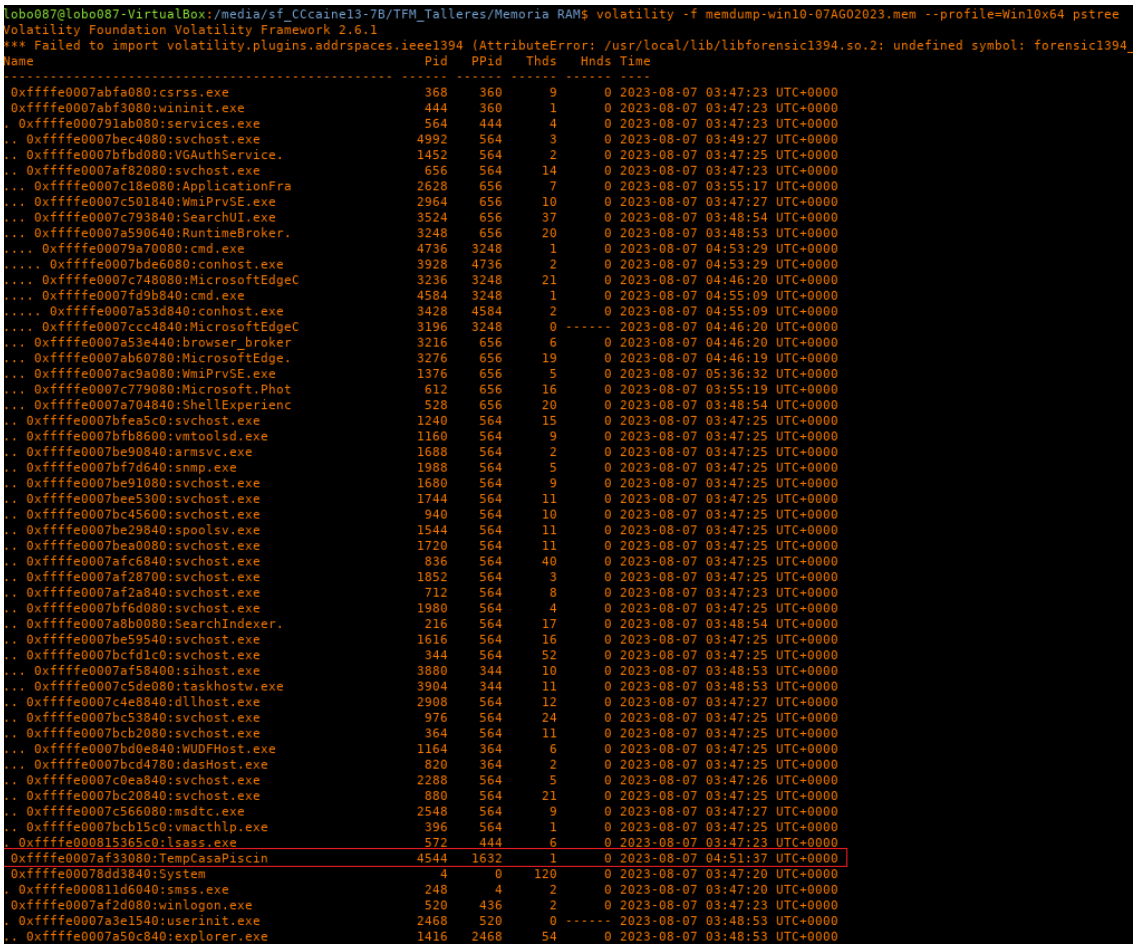
Figura 20.

Filtrado del proceso sospechoso a partir de netscan

Encontrando que se ha establecido una conexión desde la ip 10.10.10.10 por el puesto 49513 a la ip 10.10.10.170 por el puerto 50600 pero el servicio dueño de esta conexión aún no está claro, no se muestra más detalle que el nombre ya encontrado, por lo que se procede a obtener el árbol de procesos de toda la RAM con la finalidad de poder llegar a determinar el nombre completo del proceso.

Figura 21.

Árbol de procesos



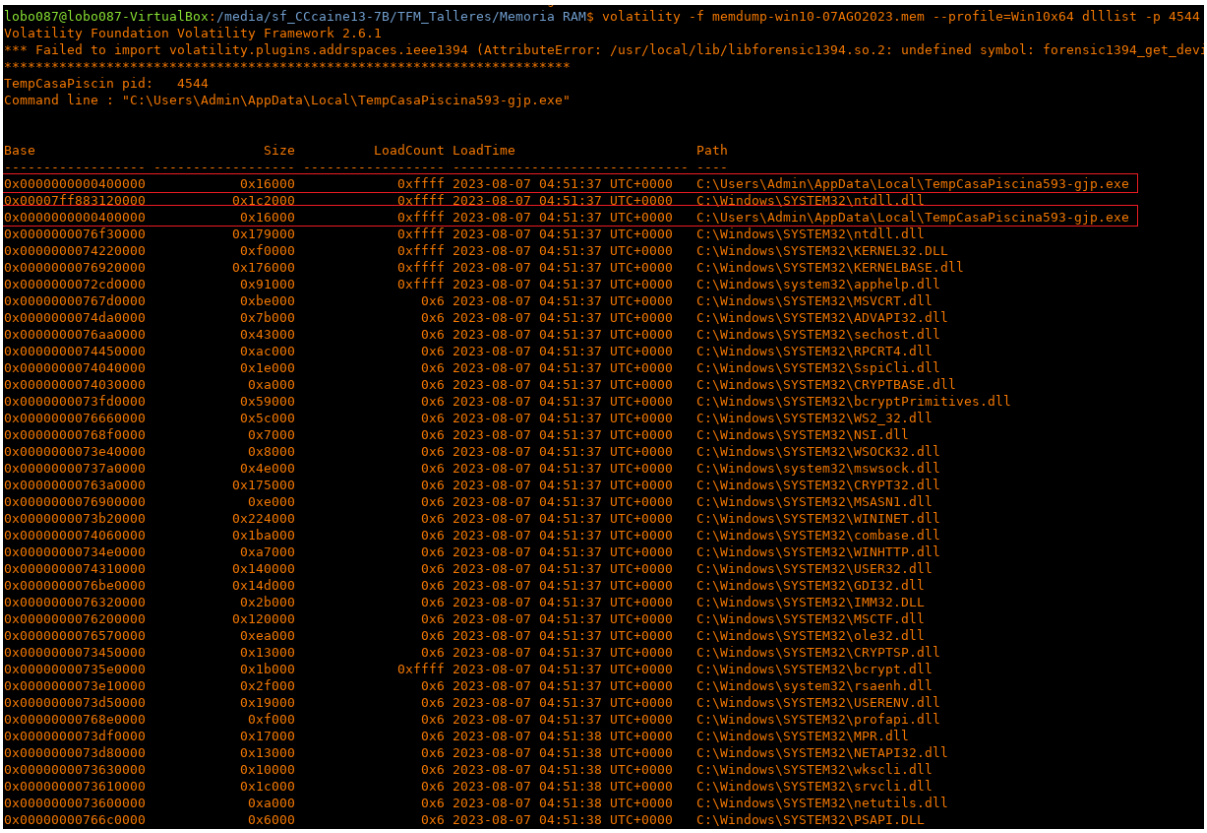
```
lobo087@lobo087-VirtualBox:/media/sf_CCcaine13-7B/TFM_Talleres/Memoria RAM$ volatility -f memdump-win10-07AGO2023.mem --profile=Win10x64 pstree
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xffffe0007abfa080:csrss.exe                         368    360      9      0 2023-08-07 03:47:23 UTC+0000
 0xffffe0007abf3080:wininit.exe                       444    360      1      0 2023-08-07 03:47:23 UTC+0000
. 0xffffe00079lab080:services.exe                     564    444      4      0 2023-08-07 03:47:23 UTC+0000
.. 0xffffe0007bec4080:svchost.exe                    4992    564      3      0 2023-08-07 03:49:27 UTC+0000
.. 0xffffe0007bfbd080:VGAuthService.                 1452    564      2      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007af82080:svchost.exe                     656    564     14      0 2023-08-07 03:47:23 UTC+0000
... 0xffffe0007c18e080:ApplicationFra                2628    656      7      0 2023-08-07 03:55:17 UTC+0000
... 0xffffe0007c501840:WmiPrvSE.exe                  2964    656     10      0 2023-08-07 03:47:27 UTC+0000
... 0xffffe0007c793840:SearchUI.exe                  3524    656     37      0 2023-08-07 03:48:54 UTC+0000
... 0xffffe0007a590640:RuntimeBroker.                3248    656     20      0 2023-08-07 03:48:53 UTC+0000
.... 0xffffe00079a70080:cmd.exe                      4736   3248      1      0 2023-08-07 04:53:29 UTC+0000
..... 0xffffe0007bde6080:conhost.exe                 3928   4736      2      0 2023-08-07 04:53:29 UTC+0000
.... 0xffffe0007c748080:MicrosoftEdgeC               3236   3248     21      0 2023-08-07 04:46:20 UTC+0000
.... 0xffffe0007fd9b840:cmd.exe                      4584   3248      1      0 2023-08-07 04:55:09 UTC+0000
..... 0xffffe0007a53d840:conhost.exe                 3428   4584      2      0 2023-08-07 04:55:09 UTC+0000
.... 0xffffe0007ccc4840:MicrosoftEdgeC               3196   3248      0 ------ 2023-08-07 04:46:20 UTC+0000
... 0xffffe0007a53e440:browser_broker                3216    656      6      0 2023-08-07 04:46:20 UTC+0000
... 0xffffe0007ab60780:MicrosoftEdge.                3276    656     19      0 2023-08-07 04:46:19 UTC+0000
... 0xffffe0007ac9a080:WmiPrvSE.exe                  1376    656      5      0 2023-08-07 05:36:32 UTC+0000
... 0xffffe0007c779080:Microsoft.Phot                 612    656     16      0 2023-08-07 03:55:19 UTC+0000
... 0xffffe0007a704840:ShellExperienc                 528    656     20      0 2023-08-07 03:48:54 UTC+0000
.. 0xffffe0007bfea5c0:svchost.exe                    1240    564     15      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007bfb8600:vmtoolsd.exe                   1160    564      9      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007be90840:armsvc.exe                     1688    564      2      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007bf7d640:snmp.exe                       1988    564      5      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007be91080:svchost.exe                    1680    564      9      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007bee5300:svchost.exe                    1744    564     11      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007bc45600:svchost.exe                     940    564     10      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007be29840:spoolsv.exe                    1544    564     11      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007bea0080:svchost.exe                    1720    564     11      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007afc6840:svchost.exe                     836    564     40      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007af28700:svchost.exe                    1852    564      3      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007af2a840:svchost.exe                     712    564      8      0 2023-08-07 03:47:23 UTC+0000
.. 0xffffe0007bf6d080:svchost.exe                    1980    564      4      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007a8b0080:SearchIndexer.                  216    564     17      0 2023-08-07 03:48:54 UTC+0000
.. 0xffffe0007be59540:svchost.exe                    1616    564     16      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007bcfd1c0:svchost.exe                     344    564     52      0 2023-08-07 03:47:25 UTC+0000
... 0xffffe0007af58400:sihost.exe                    3880    344     10      0 2023-08-07 03:48:53 UTC+0000
... 0xffffe0007c5de080:taskhostw.exe                 3904    344     11      0 2023-08-07 03:48:53 UTC+0000
.. 0xffffe0007c4e8840:dllhost.exe                    2908    564     12      0 2023-08-07 03:47:27 UTC+0000
.. 0xffffe0007bc53840:svchost.exe                     976    564     24      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007bcb2080:svchost.exe                     364    564     11      0 2023-08-07 03:47:25 UTC+0000
... 0xffffe0007bd0e840:WUDFHost.exe                  1164    364      6      0 2023-08-07 03:47:25 UTC+0000
... 0xffffe0007bcd4780:dasHost.exe                    820    364      2      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007c0ea840:svchost.exe                    2288    564      5      0 2023-08-07 03:47:26 UTC+0000
.. 0xffffe0007bc20840:svchost.exe                     880    564     21      0 2023-08-07 03:47:25 UTC+0000
.. 0xffffe0007c566080:msdtc.exe                      2548    564      9      0 2023-08-07 03:47:27 UTC+0000
.. 0xffffe0007bcb15c0:vmacthlp.exe                    396    564      1      0 2023-08-07 03:47:25 UTC+0000
. 0xffffe000815365c0:lsass.exe                        572    444      6      0 2023-08-07 03:47:23 UTC+0000
 0xffffe0007af33080:TempCasaPiscin                   4544   1632      1      0 2023-08-07 04:51:37 UTC+0000
 0xffffe00078dd3840:System                              4      0    120      0 2023-08-07 03:47:20 UTC+0000
. 0xffffe000811d6040:smss.exe                         248      4      2      0 2023-08-07 03:47:20 UTC+0000
 0xffffe0007af2d080:winlogon.exe                      520    436      2      0 2023-08-07 03:47:23 UTC+0000
. 0xffffe0007a3e1540:userinit.exe                    2468    520      0 ------ 2023-08-07 03:48:53 UTC+0000
.. 0xffffe0007a50c840:explorer.exe                   1416   2468     54      0 2023-08-07 03:48:53 UTC+0000
```

El resultado de este comando nos muestra que el proceso TempCasaPiscin no tiene hijos que dependan de él debido a que no hay ninguna indentación ni otro proceso que su PPID sea el 4544.

El siguiente paso del análisis es la evaluación de las dll que están ligadas a este proceso para lo cual se utiliza el plugin **dlllist** en el que aparece en la siguiente ubicación: C:\Users\Admin\AppData\Local\TempCasaPiscina593-gjp.exe tenemos un ejecutable con el nombre **TempCasaPiscina593-gjp.exe**

Figura 22.

Plugin Dlllist



```
lobo087@lobo087-VirtualBox:/media/sf_CCcaine13-7B/TFM_Talleres/Memoria RAM$ volatility -f memdump-win10-07AGO2023.mem --profile=Win10x64 dlllist -p 4544
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.addrspaces.ieee1394 (AttributeError: /usr/local/lib/libforensic1394.so.2: undefined symbol: forensic1394_get_dev
**********************************************************************
TempCasaPiscin pid:   4544
Command line : "C:\Users\Admin\AppData\Local\TempCasaPiscina593-gjp.exe"


Base                             Size          LoadCount LoadTime                       Path
-------------------- ---------- ---------- -------------------------- ----
0x0000000000400000           0x16000             0xffff 2023-08-07 04:51:37 UTC+0000   C:\Users\Admin\AppData\Local\TempCasaPiscina593-gjp.exe
0x00007ff883120000           0x1c2000            0xffff 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
0x0000000000400000           0x16000             0xffff 2023-08-07 04:51:37 UTC+0000   C:\Users\Admin\AppData\Local\TempCasaPiscina593-gjp.exe
0x0000000076f30000          0x179000             0xffff 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\ntdll.dll
0x0000000074220000           0xf0000             0xffff 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\KERNEL32.DLL
0x0000000076920000          0x176000             0xffff 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\KERNELBASE.dll
0x0000000072cd0000           0x91000             0xffff 2023-08-07 04:51:37 UTC+0000   C:\Windows\system32\apphelp.dll
0x000000000767d0000           0xbe000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\MSVCRT.dll
0x0000000074da0000           0x7b000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\ADVAPI32.dll
0x0000000076aa0000           0x43000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\sechost.dll
0x0000000074450000           0xac000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\RPCRT4.dll
0x0000000074040000           0x1e000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\SspiCli.dll
0x0000000074030000            0xa000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\CRYPTBASE.dll
0x0000000073fd0000           0x59000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\bcryptPrimitives.dll
0x0000000076660000           0x5c000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\WS2_32.dll
0x00000000768f0000            0x7000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\NSI.dll
0x0000000073e40000            0x8000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\WSOCK32.dll
0x00000000737a0000           0x4e000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\system32\mswsock.dll
0x0000000076 3a0000          0x175000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\CRYPT32.dll
0x0000000076900000            0xe000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\MSASN1.dll
0x0000000073b20000          0x224000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\WININET.dll
0x0000000074060000           0x1ba000               0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\combase.dll
0x000000000734e0000           0xa7000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\WINHTTP.dll
0x0000000074310000          0x140000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\USER32.dll
0x0000000076be0000           0x14d000               0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\GDI32.dll
0x0000000076320000           0x2b000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\IMM32.DLL
0x0000000076200000          0x120000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\MSCTF.dll
0x0000000076570000           0xea000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\ole32.dll
0x0000000073450000           0x13000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\CRYPTSP.dll
0x000000000735e0000           0x1b000             0xffff 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\bcrypt.dll
0x0000000073e10000           0x2f000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\system32\rsaenh.dll
0x0000000073d50000           0x19000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\USERENV.dll
0x000000000768e0000            0xf000                0x6 2023-08-07 04:51:37 UTC+0000   C:\Windows\SYSTEM32\profapi.dll
0x0000000073df0000           0x17000                0x6 2023-08-07 04:51:38 UTC+0000   C:\Windows\SYSTEM32\MPR.dll
0x0000000073d80000           0x13000                0x6 2023-08-07 04:51:38 UTC+0000   C:\Windows\SYSTEM32\NETAPI32.dll
0x0000000073630000           0x10000                0x6 2023-08-07 04:51:38 UTC+0000   C:\Windows\SYSTEM32\wkscli.dll
0x0000000073610000           0x1c000                0x6 2023-08-07 04:51:38 UTC+0000   C:\Windows\SYSTEM32\srvcli.dll
0x0000000073600000            0xa000                0x6 2023-08-07 04:51:38 UTC+0000   C:\Windows\SYSTEM32\netutils.dll
0x000000000766c0000            0x6000                0x6 2023-08-07 04:51:38 UTC+0000   C:\Windows\SYSTEM32\PSAPI.DLL
```

Ahora se procede a utilizar el plugin **filescan** con la finalidad de encontrar los archivos, el numero de punteros a cada objeto y los permisos concedidos este resultado se encuentra filtrado en función del nombre del proceso que se ha estado buscando “CasaPiscina”

Figura 23.

Plugin filescan

```
lobo087@lobo087-VirtualBox:/media/sf_CCcaine13-7B/TFM_Talleres/Memoria RAM$ volatility -f memdump-win10-07AGO2023.mem --pr
ofile=Win10x64 filescan | grep "CasaP"
Volatility Foundation Volatility Framework 2.6.1
0x0000e0007a411c50      8      0 R--r-d \Device\HarddiskVolume4\Users\Admin\AppData\Local\TempCasaPiscina593-gjp.exe
0x0000e0007a4435c0     16      0 RW---- \Device\HarddiskVolume4第廊鬾 [illegible]名 《鬾 [illegible]min\Desktop\CasaPiscina-593-r7e0eh.exexe.jpg
laitrap.u
0x0000e0007a59da40     16      0 R--r-d \Device\HarddiskVolume4ぢ勞鬾 [illegible]賺ｺ鬾 [illegible]min\Documents\CasaPiscina-593-exe.jpg
0x0000e0007a735350     11      0 R--r-d \Device\HarddiskVolume4櫺福鬾 [illegible]酸殺鬾 [illegible]min\Documents\CasaPiscina-593-e.jpg
lobo087@lobo087-VirtualBox:/media/sf_CCcaine13-7B/TFM_Talleres/Memoria RAM$
```

Finalmente, mediante el uso de la herramienta photorec se va a tratar de extraer archivos que se tenga en esta captura de memoria

Figura 24.

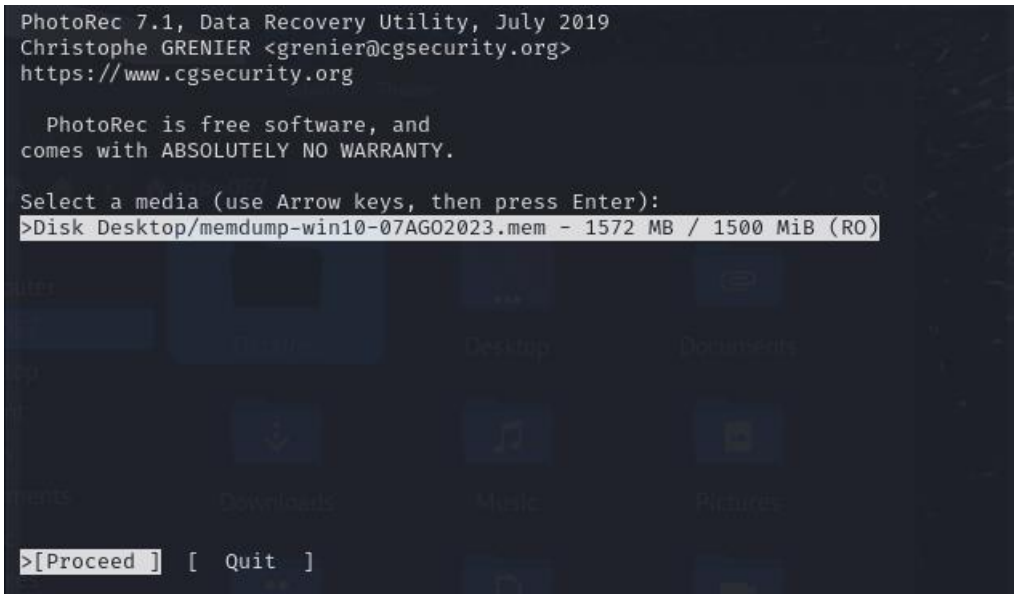
Plugin photorec

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
lobo087@lobo087-VirtualBox:~$ sudo photorec /media/sf_CCcaine13-7B/TFM_Talleres/
Memoria RAM/memdump-win10-07AGO2023.mem
```

Tras reconocer como disco la captura de memoria RAM de la que se extraerán los archivos, se continúa.

Figura 25.

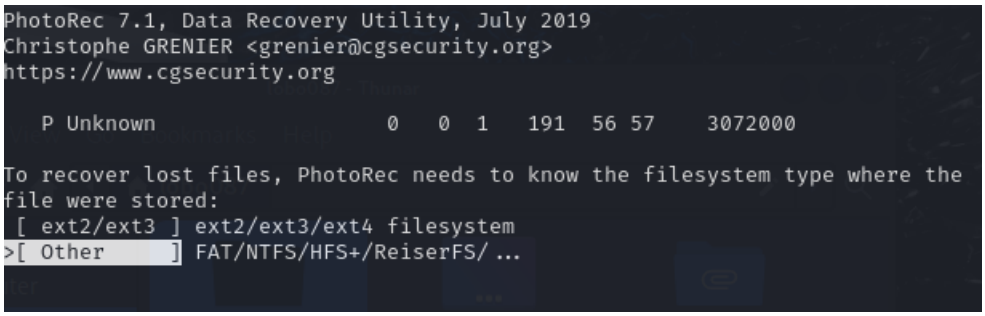
Reconocimiento de la RAM como disco



Se selecciona el sistema de archivos que pertenece la captura

Figura 26.

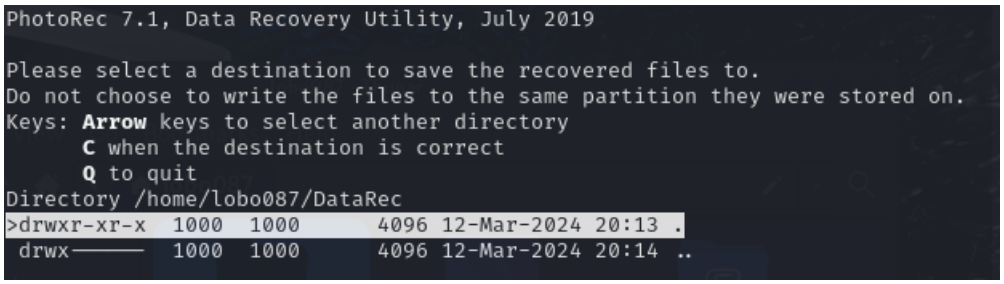
Selección de sistema de archivos



Y se selecciona donde se va a realizar la descarga de la información extraída para este efecto se ha creado una carpeta llamada DataRec

Figura 27.

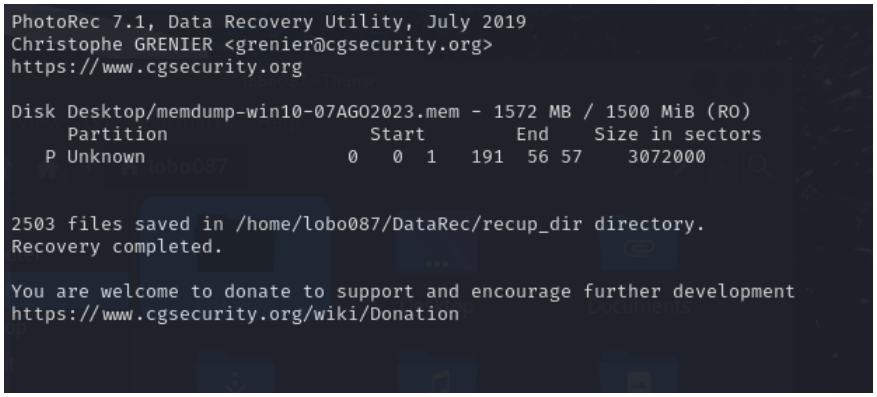
Ubicación extracción



Culminado el proceso de extracción se muestra que fueron obtenidos **2503** archivos desde la memoria RAM

Figura 28.

Resultado de la extracción



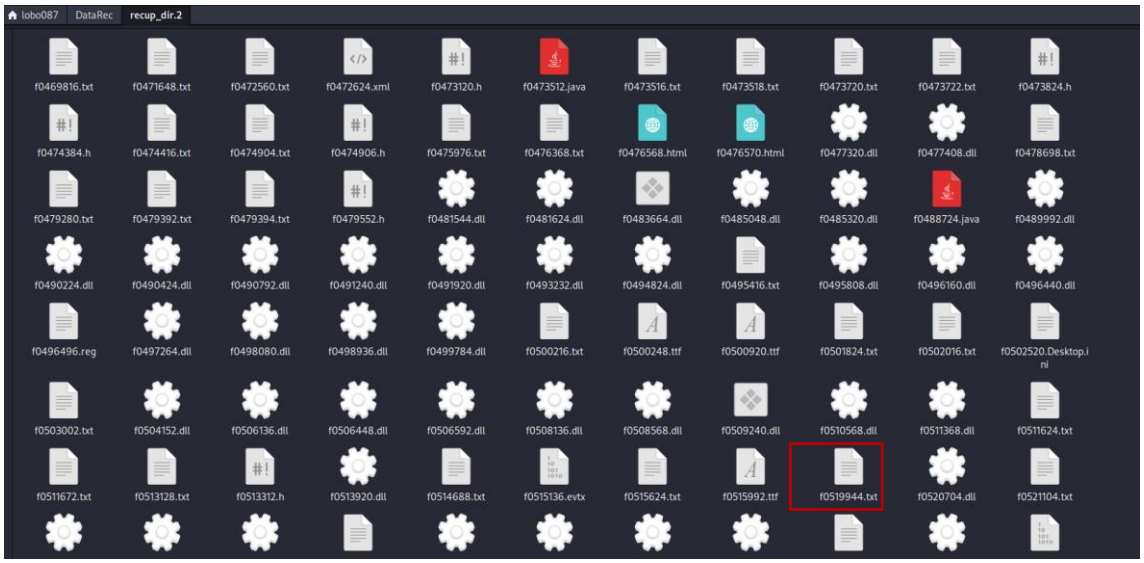
Continuando con la investigación se intenta buscar información de este proceso sospechoso dentro de la información extraida para lo cual se realiza un filtro en el directorio que contienen los documentos extraidos de la ram

Figura 29.

Filtro de búsqueda de archivos

Figura 30.

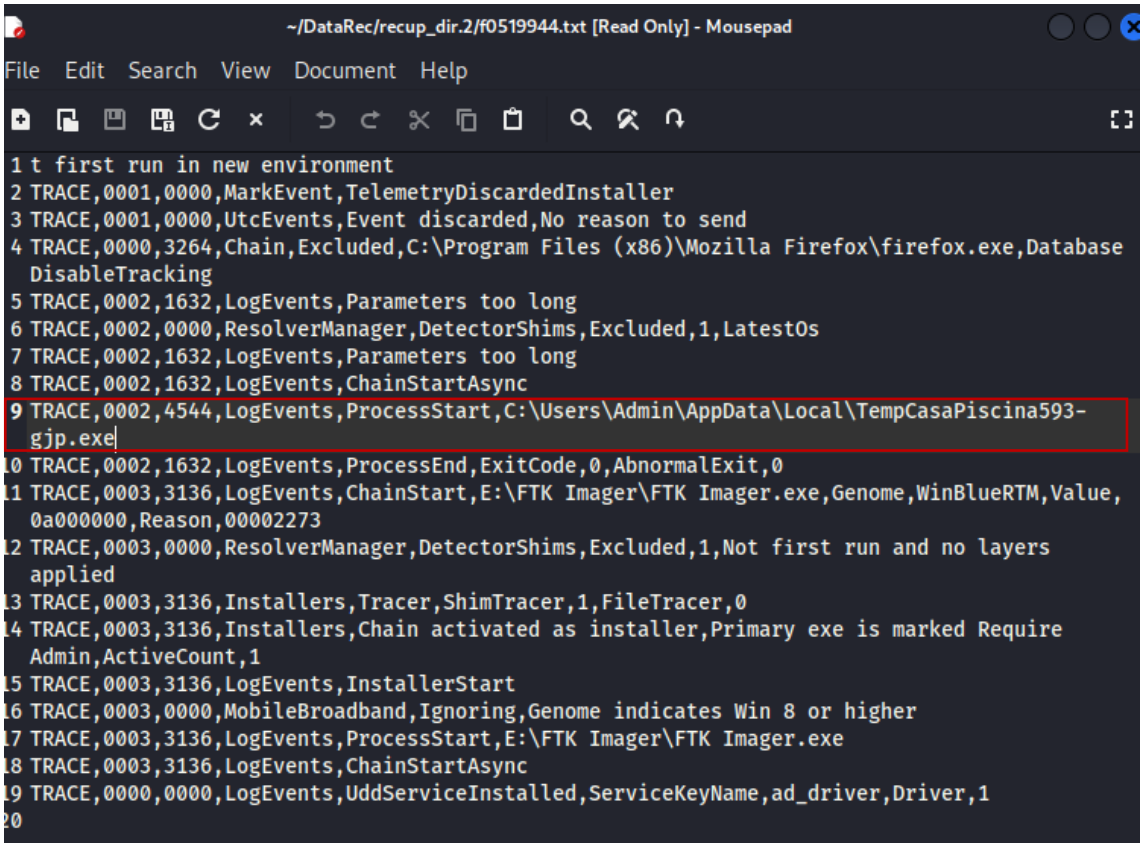
Archivo f0519944



Según la respuesta obtenida, el archivo f0519944.txt en su línea 9 contiene información del proceso, por lo que se busca y abre dicho documento.

Figura 31.

Path archivo sospechoso en EventLog



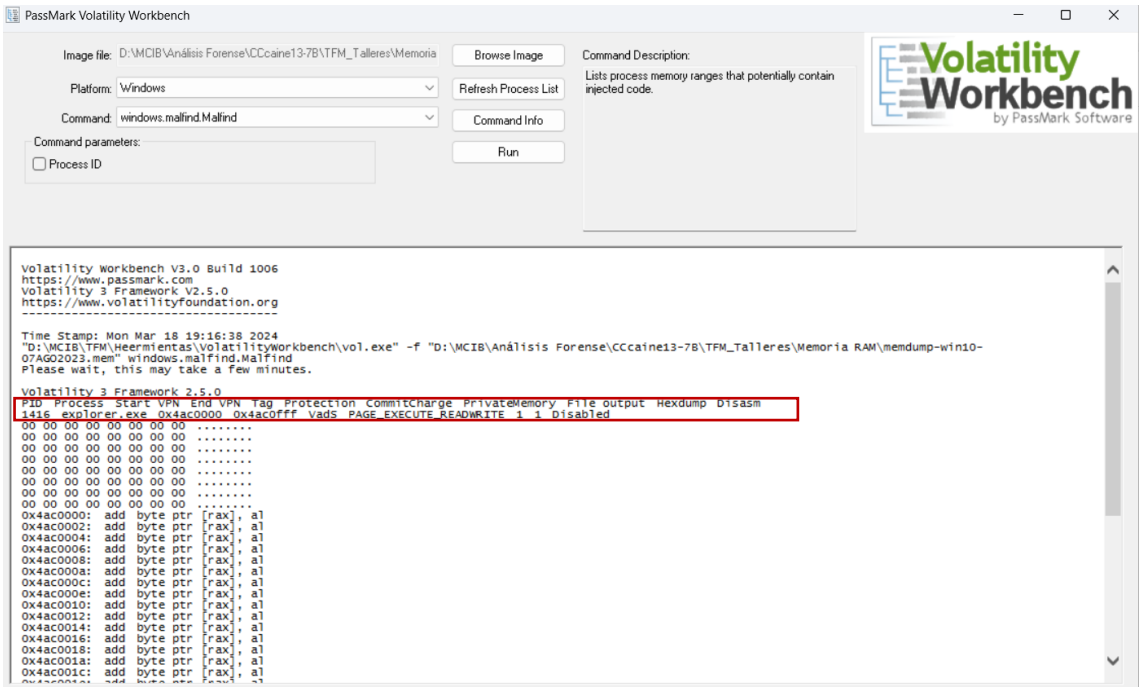
En dicho archivo únicamente se encuentra información del “EventLog” de Windows en el cual indica el inicio del proceso y el path en el que se encuentra

Al no encontrar más información en la evidencia volátil se procedió a utilizar Google dorking, al igual que búsquedas en la Deep web que lleven a entender cómo funciona este proceso malicioso, sin mayor éxito, pues no se encontró información que coincida con TempCasaPiscina593-gjp.exe.

Finalmente, con el uso de la herramienta VolatilityWorkbench se procedió a realizar el ultimo análisis que fue mediante el comando malfind que nos entregó información adicional.

Figura 32.

Plugin malfind Volatility Workbench



En donde se confirma que esta evidencia cuenta con un malware, que en este caso está identificado dentro del proceso de Pid 1416 que corresponde al proceso explorer.exe, lo que da a notar que se trata de un tipo de malware que trabaja con punteros de memora para ocultar su rastro y que se encuentra ubicado en la dirección: C:\Users\Admin\AppData\Local\TempCasaPiscina593-gjp.exe

EL siguiente paso de la investigación nos lleva investigar dentro del disco para tratar de extraer

el malware de la ubicación ya identificada.

Análisis de Disco.

En función a la imagen entregada se procede a agregar la evidencia a Autopsy, y a configurar cada uno de los pasos para realizar el análisis adecuado, también fueron agregados las palabras identificadas del malware para que también agregue esas palabras claves a la búsqueda a realizar

Figura 33.

Análisis de Disco - Información del caso

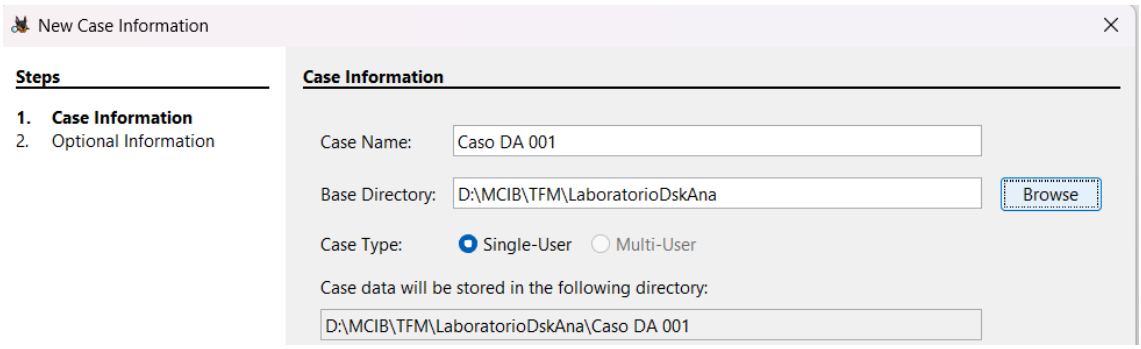


Figura 34.

Análisis de Disco -Información adicional

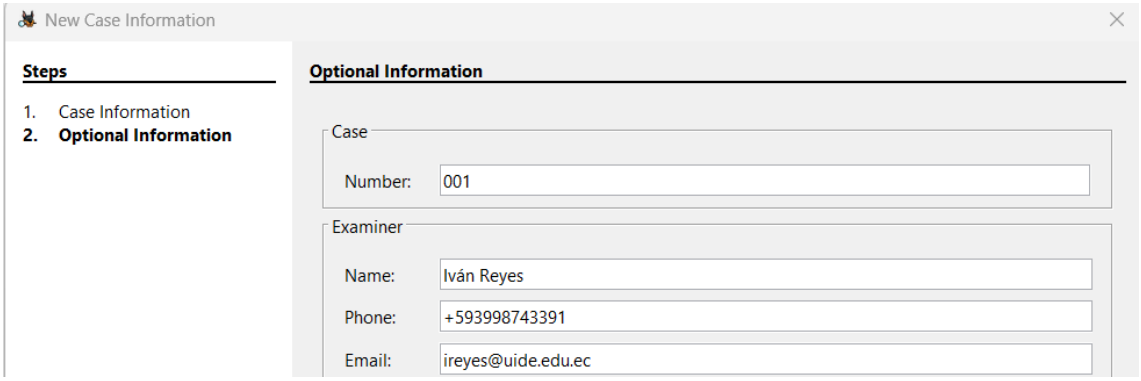


Figura 35.

Análisis de Disco – Filtrado de Keywords

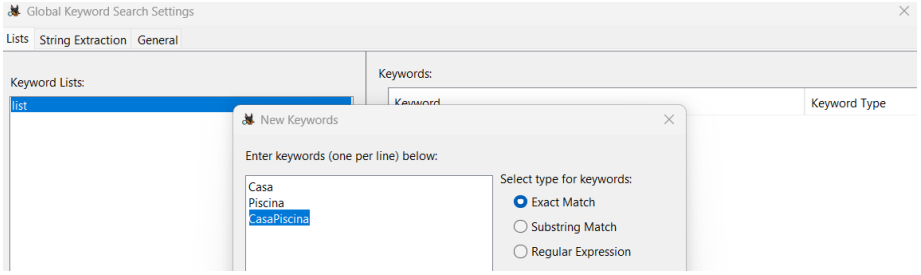
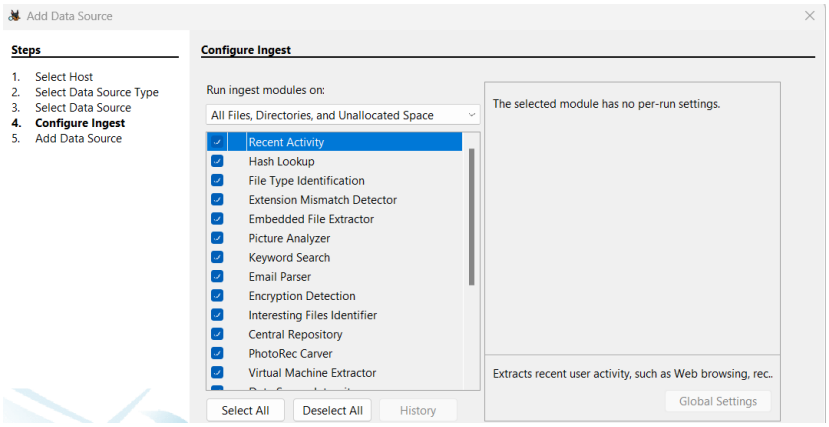


Figura 36.

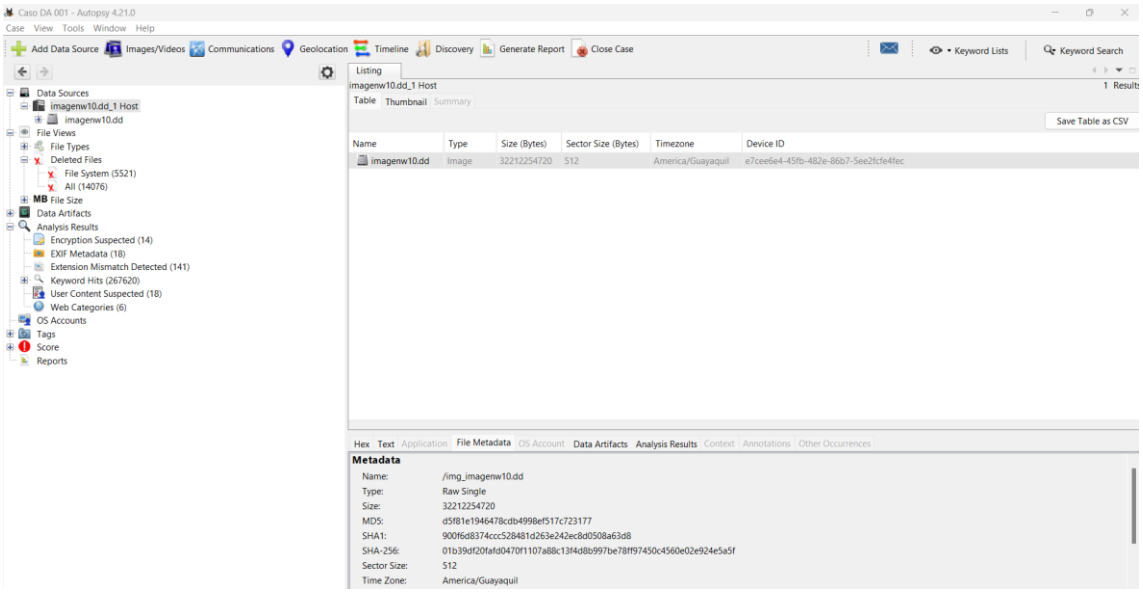
Análisis de Disco -Configuración de módulos



Al finalizar la configuración de la herramienta el análisis del disco duró más de 10 horas debido a la extensión del disco, que tenía un tamaño de 32Gb.

Figura 37.

Análisis de Disco -Resultados del análisis



Una vez finalizado el análisis completo del disco lo primero que se busca son las coincidencias con las palabras claves colocadas

Figura 38.

Análisis de Disco -Evaluación de keywords

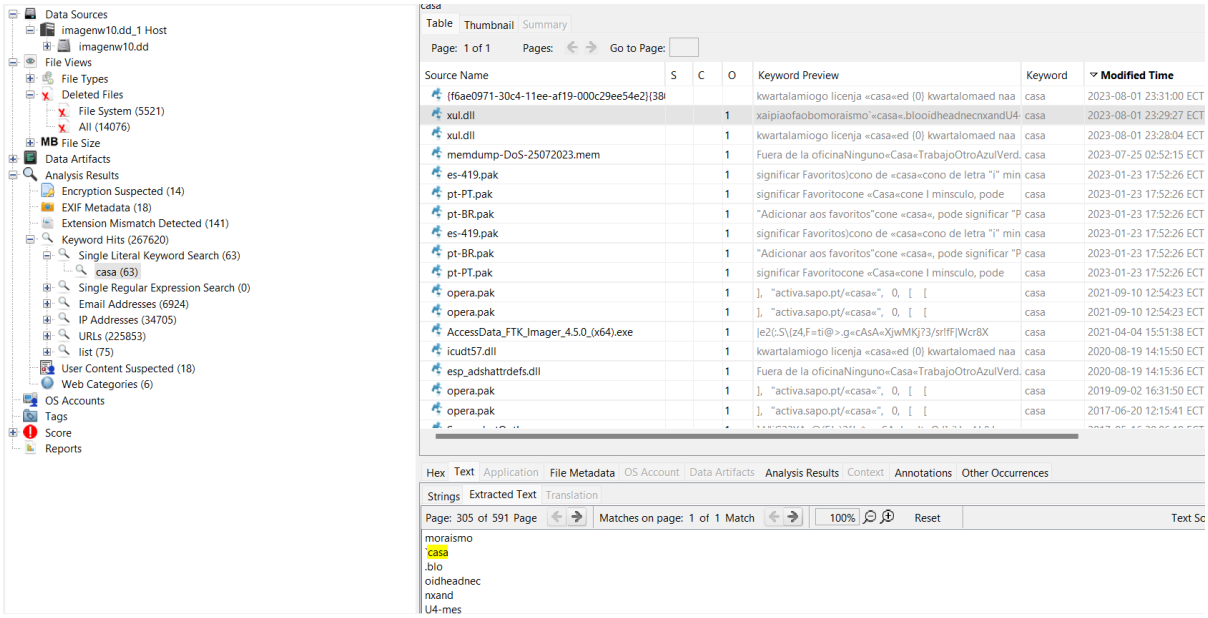


Figura 39.

Análisis de Disco - Evaluación de keywords continuación

Source Name	S	C	O	Keyword Preview	Keyword	Modified Time
amd64_microsoft-windows-comdlg32.resources_31			0	reloazulcsiaazul-«piscina«brancopersonalizad	piscina	2009-07-13 21:58:55 ECT
x86_microsoft-windows-comdlg32.resources_31bf3			0	reloazulcsiaazul-«piscina«brancopersonalizad	piscina	2009-07-13 21:57:17 ECT
LXKXLUI.DLL			0	brancolaranjaazul-«piscina«castanhoo que is	piscina	2009-07-13 20:41:49 ECT
lxkpsui.dll			0	eadolimacsiaazul-«piscina«erro de dadosbranc	piscina	2009-07-13 20:41:49 ECT
lxkpsui.dll			0	eadolimacsiaazul-«piscina«erro de dadosbranc	piscina	2009-07-13 20:41:49 ECT
LXKXLUI.DLL			0	brancolaranjaazul-«piscina«castanhoo que is	piscina	2009-07-13 20:41:49 ECT
lxkpclui.dll			0	brancolaranjaazul-«piscina«castanhoo que is	piscina	2009-07-13 20:41:48 ECT
lxkpclui.dll			0	brancolaranjaazul-«piscina«castanhoo que is	piscina	2009-07-13 20:41:48 ECT
comdlg32.dll.mui			0	reloazulcsiaazul-«piscina«brancopersonalizad	piscina	2009-07-13 20:17:43 ECT
comdlg32.dll.mui			0	reloazulcsiaazul-«piscina«brancopersonalizad	piscina	2009-07-13 20:17:43 ECT
comdlg32.dll.mui			0	reloazulcsiaazul-«piscina«brancopersonalizad	piscina	2009-07-13 19:55:31 ECT
comdlg32.dll.mui			0	reloazulcsiaazul-«piscina«brancopersonalizad	piscina	2009-07-13 19:55:31 ECT

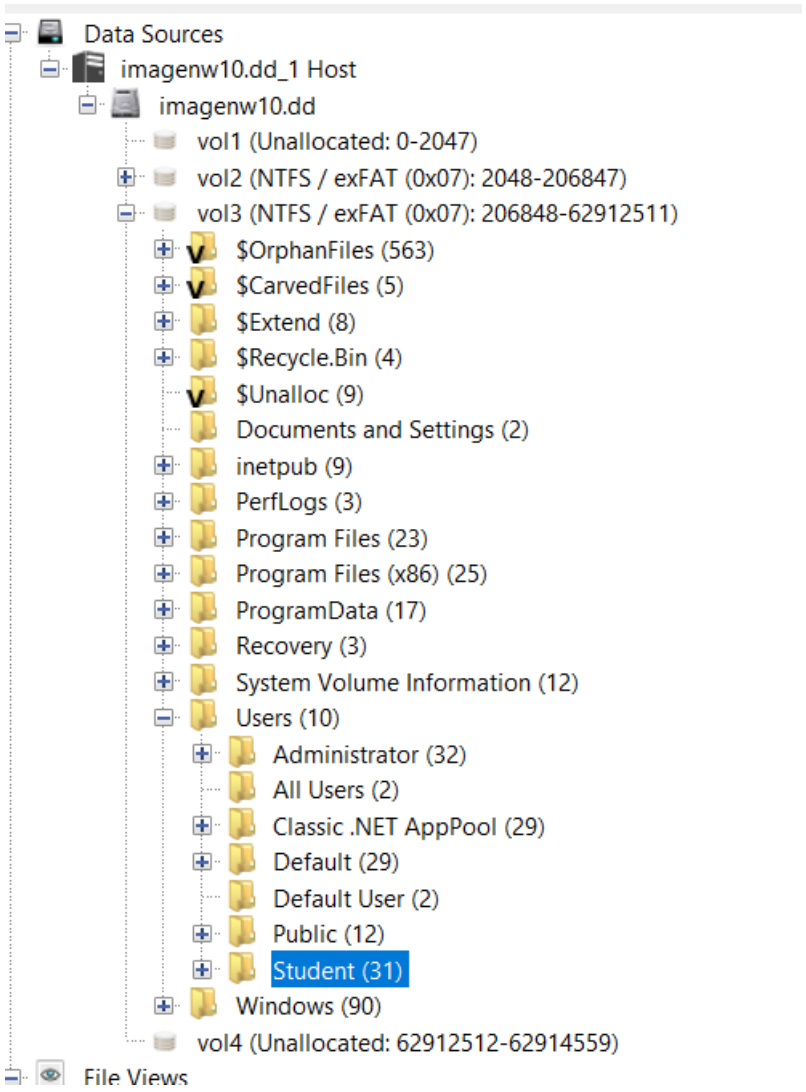
Dentro de la lista de coincidencias a ser buscadas se colocaron las palabras “casa”, “Piscina” y “CasaPis”, pero dentro del análisis se encontró coincidencia en “casa”, y “piscina” por separado algo que parece extraño, pues al buscar dentro de las coincidencias no se encuentra nada que tenga que ver con el malware buscado.

Al tratar de buscar el path C:\Users\Admin\AppData\Local\TempCasaPiscina593-gjp.exe

dentro del disco analizado no se puede acceder a esa ubicación

Figura 40.

Análisis de Disco – Análisis de usuarios



Dentro del árbol de usuario no se encuentra un usuario Admin, este disco tiene los directorios para los usuarios admisnistrator, Student, default, y default user.

Se intenta ingresar a la ubicación Temp pero del usuario administrator que es el que se encuentra en este disco, pero no hay ningún rastro del malware. Tras realizar varias búsquedas adicionales se puede identificar que esta imagen de disco analizada no corresponde a la captura de RAM, por lo que no se puede avanzar más en la búsqueda del software malicioso encontrado en la captura de RAM inicial.

Laboratorio 2

Antecedentes:

El Cliente solicita que se analice una máquina, la misma que presenta lo siguiente:

Características del equipo:

- **Marca:** Dell
- **Procesador:** AMD Ryzen 5 3450U
- **RAM:** 2 GB
- **Disco:** 60 GB

Recopilación de Evidencias

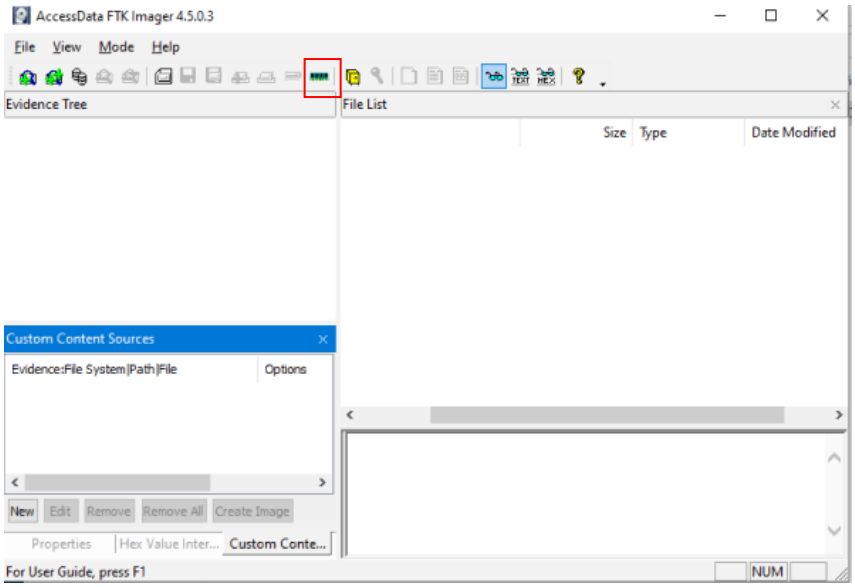
Volcado de la memoria RAM

Ya que no se tiene mucha información del equipo se solicita al cliente que no apague el dispositivo para poder hacer la captura de la memoria RAM ya que es la más volátil.

1. Abrimos FTK Imager y seleccionamos Capture Memory

Figura 41.

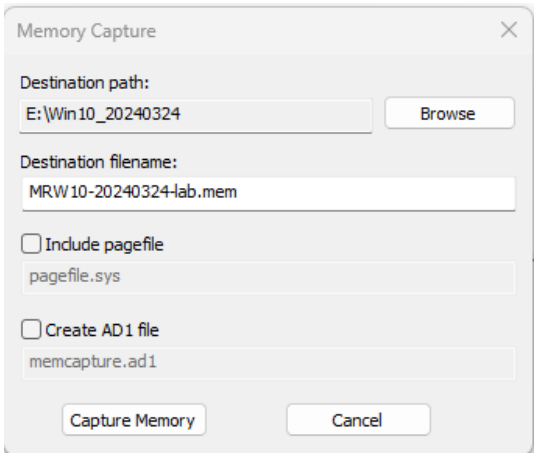
Volcado de Ram



2. Iniciamos la captura

Figura 42.

Inicio de Captura

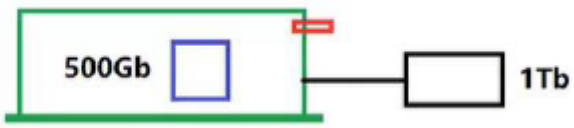


Extracción de la imagen del disco duro.

Parala extracción de la imagen del disco nos basamos en el siguiente diagrama. Donde se va a utilizar la versión Live de Caine contenida en un USB booteable. Para la extraer la imagen del disco se requiere un disco externo con capacidad de almacenamiento de al menos el doble del tamaño del disco del cual se va a extraer la imagen forense.

Figura 43.

Diagrama de extracción de imagen

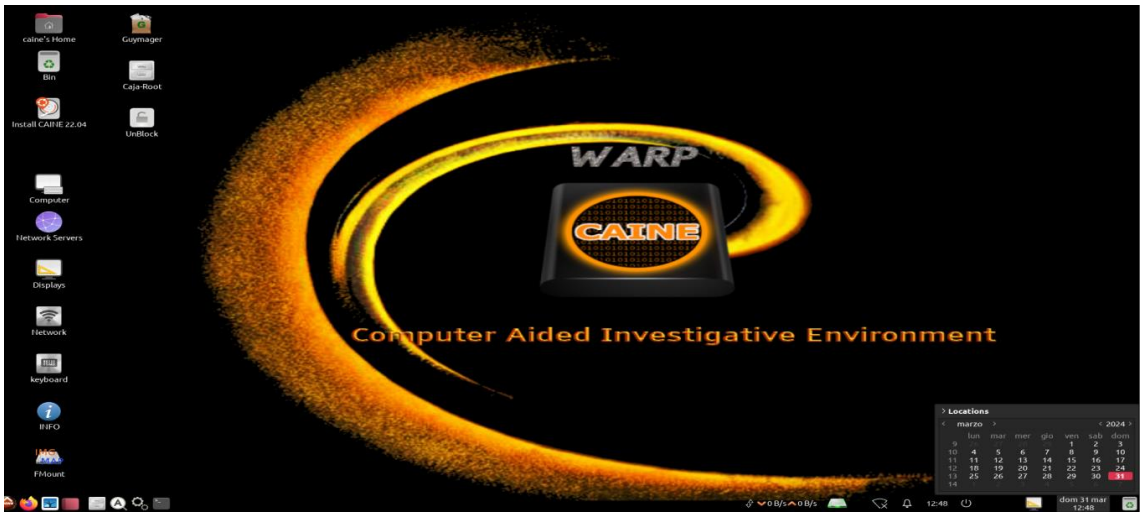


Ejecutamos en la maquina a analizar Caine con un usb botteable para que se pueda extraer la imagen del disco, con las siguientes características:

- Read only
- No eject
- No dev
- No atime

Figura 44.

Configuración de zona horaria



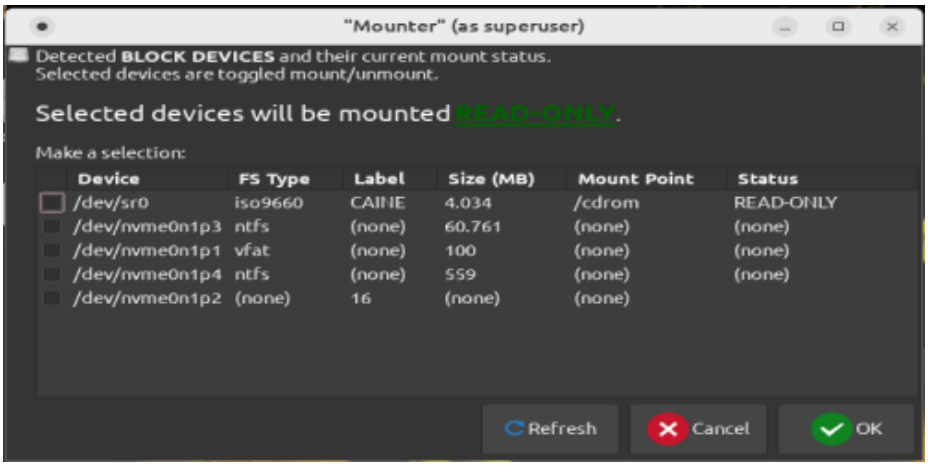
1. Una vez ejecutado se debe configurar la zona horaria correcta para actualizar la hora de lugar donde se está haciendo el análisis.
2. Se selecciona los discos que van a establecer como **read only**.

Figura 45.

Análisis de hora

Figura 46.

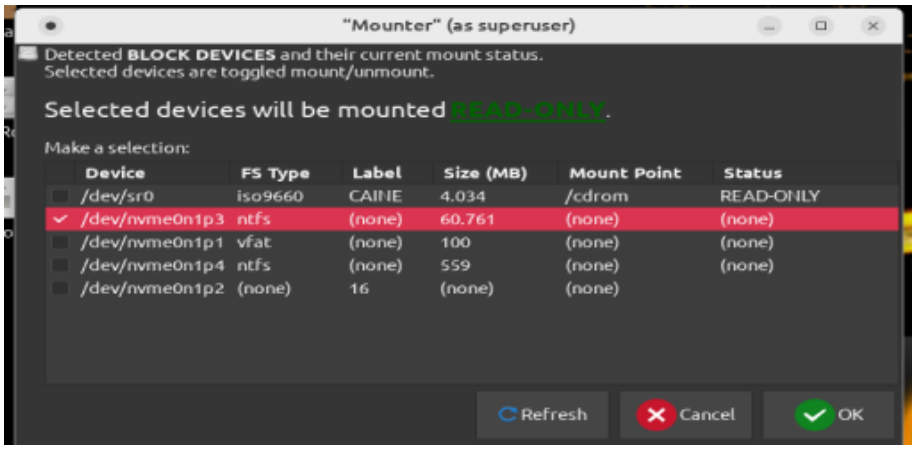
Evaluación de discos en estado read only



3. Seleccionar el disco del sistema operativo que se analizará.

Figura 47.

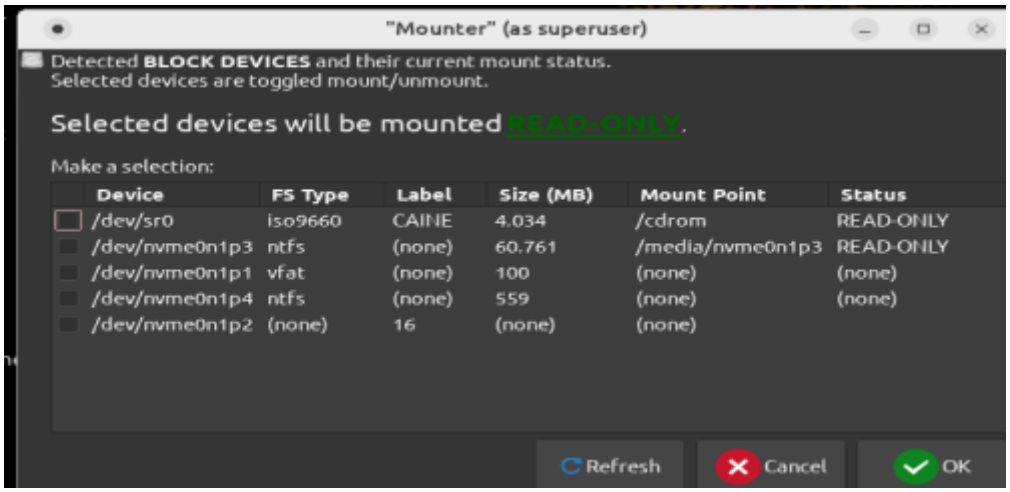
Selección del disco de evaluación



4. Se observa que se tiene asegurado el disco interno del equipo que se está analizando.

Figura 48.

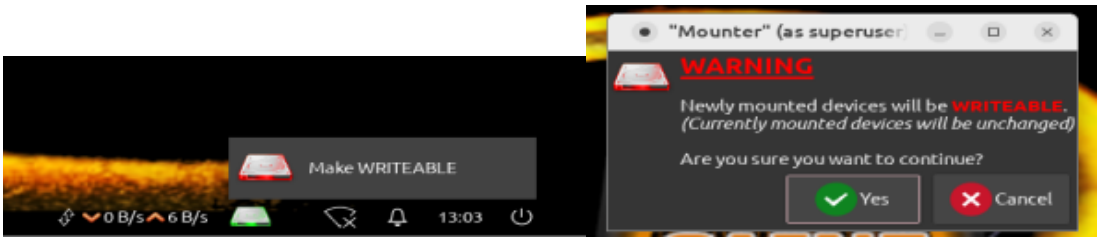
Verificación del estado del disco



5. Ahora se establece los discos que no van a tener protección contra escritura, en este caso el disco en donde va a copiar la imagen, el cual deberá ser de al menos del doble de la capacidad. Con clic derecho sobre el icono de discos seleccionamos **MAKE WRITEABLE** y aceptamos

Figura 49.

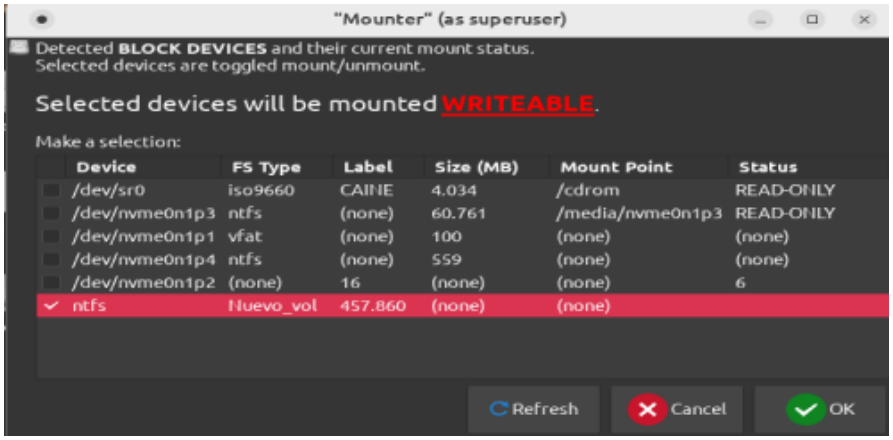
Cambiando el estado a "writeable" al disco target



6. Se conecta el disco en el cual se va a colocar la imagen forense de la maquina analizada y se la monta en Caine.

Figura 50.

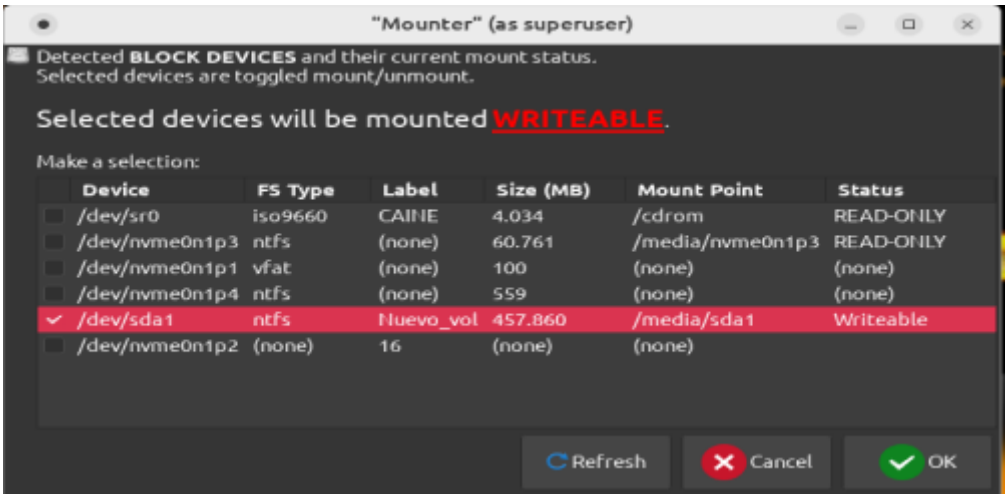
Veridfcación de permisos de escritura



7. Una vez montado se verifica que tenga permisos de escritura.

Figura 51.

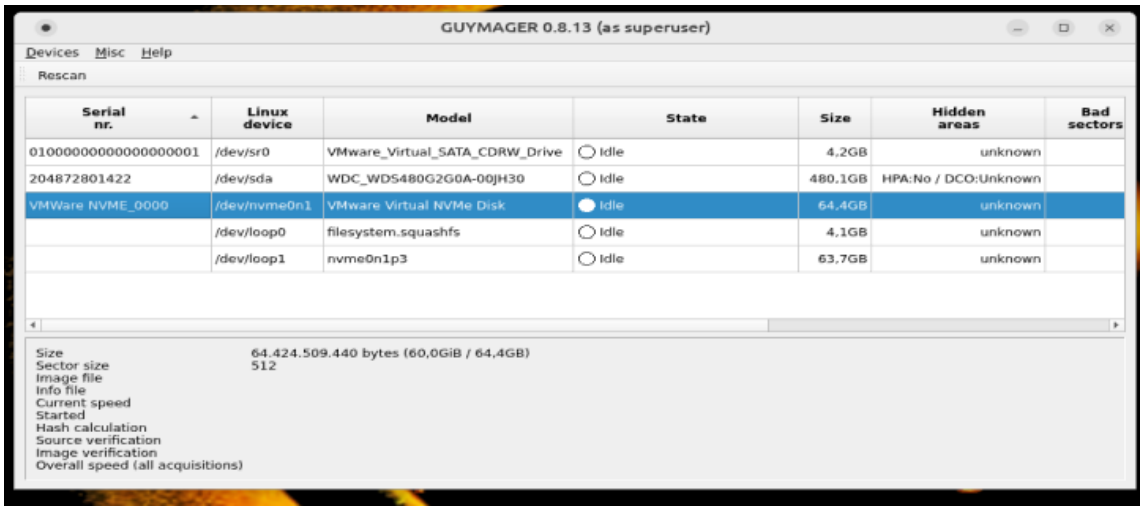
Veridfcación de permisos de escritura continuación



8. Se ejecuta Guymager y se selecciona el disco del cual se va a extraer la imagen.

Figura 52.

Selección del disco objetivo



9. Empezar la extracción de la imagen.

Figura 53.

Inicio de extracción

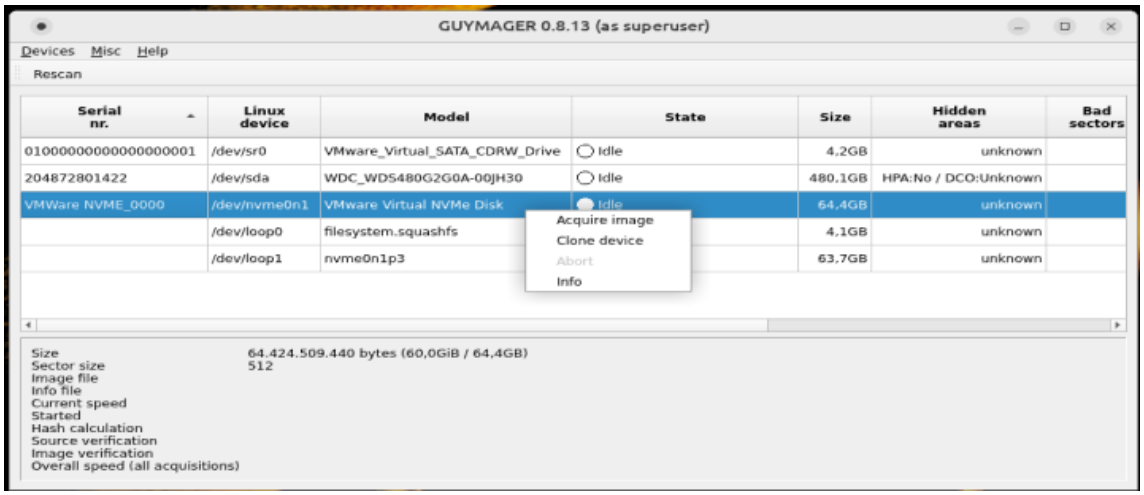
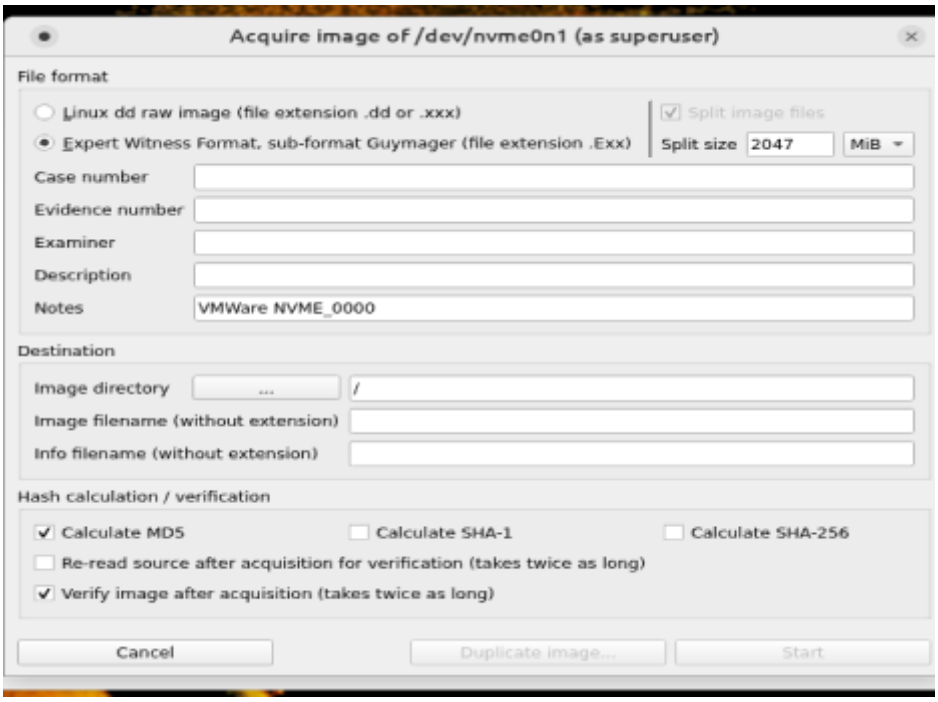


Figura 54.

Configuración de la extracción



10. En la ventana que se abre se selecciona las opciones de extracción:

- Seleccionar el formato de **Linux**
- Seleccionar que extraiga un solo archivo sin marcar **Split image file**
- Seleccionar la ruta donde se enviará la imagen en el disco duro, para lo cual se verifica cual es el disco correcto, con el comando **mount** en el terminal.

Figura 55.

Evaluación de disco y target

En la imagen se observa que se encuentran los dos discos, al que se va a extraer la imagen y en

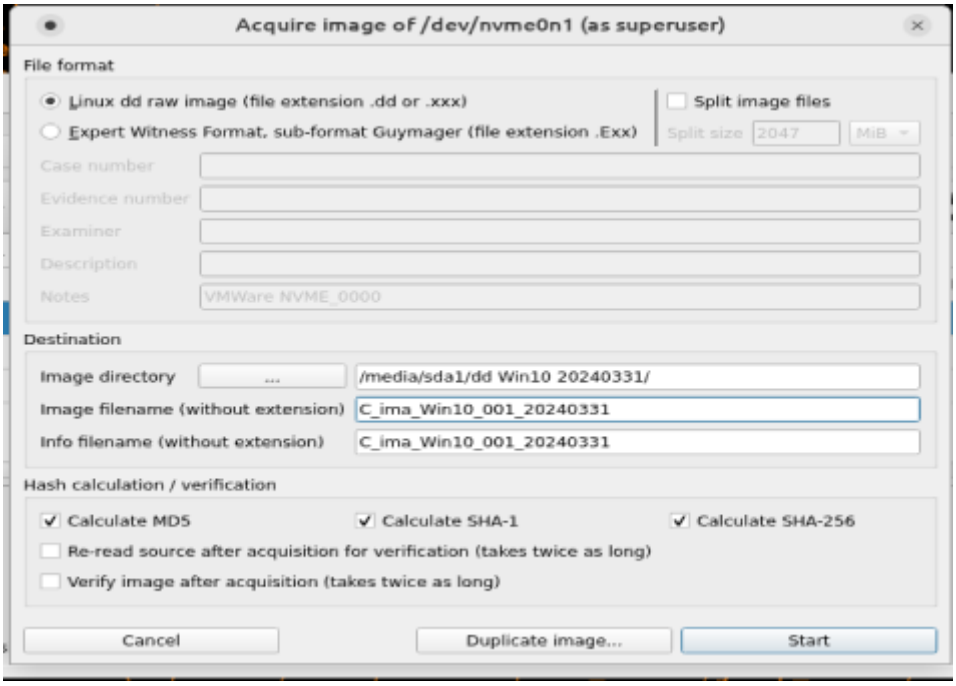
el que vamos a colocar la imagen, se los puede identificar ya que el disco de la maquina tiene **(ro, nodev, no exec, noatime).**

11. Colocar el nombre que le asignará a la imagen.

12. Seleccionar el hash que se va a calcular, e iniciar la extracción.

Figura 56.

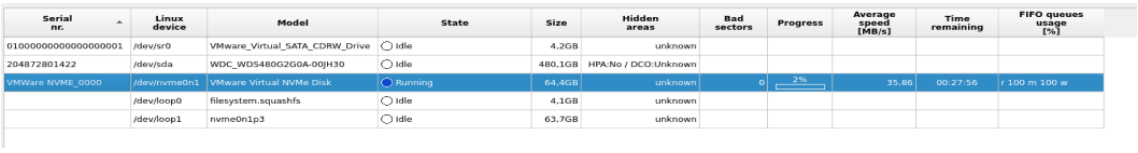
Extración de disco duro



13. Esperar a que se termine la extracción.

Figura 57.

Extracción de disco duro



Análisis de las Evidencias

Análisis de la Memoria RAM

1. Extracción del hash de la imagen

Para nuestro análisis se va a usar la Suite de CAINE, en donde se tienen varias Herramientas de Análisis Forense. Con el uso de QuickHash se va a obtener el hash del archivo que contiene la imagen de la memoria RAM obtenida anteriormente.

Figura 58.

Hash MD5

Figura 59.

Hash SHA1

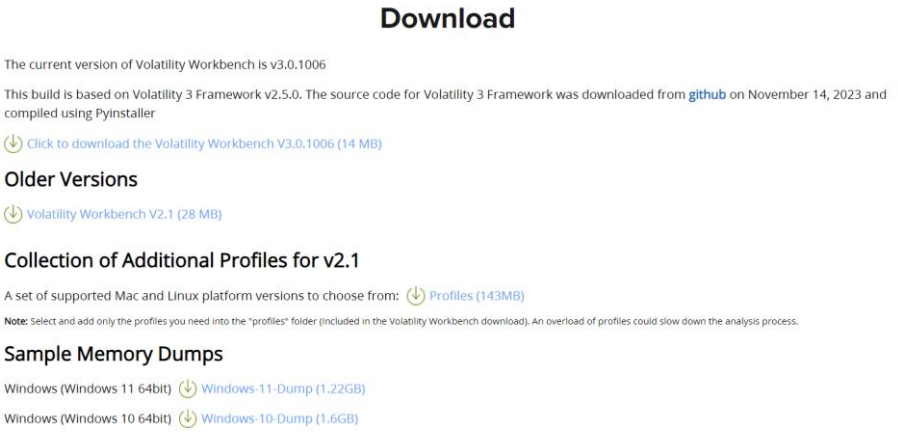
Figura 60.

Hash SHA256

2. Para iniciar con el análisis de la memoria RAM, se debe descargar la aplicación volatility workbrench desde https://www.osforensics.com/tools/volatility-workbench.html.

Figura 61.

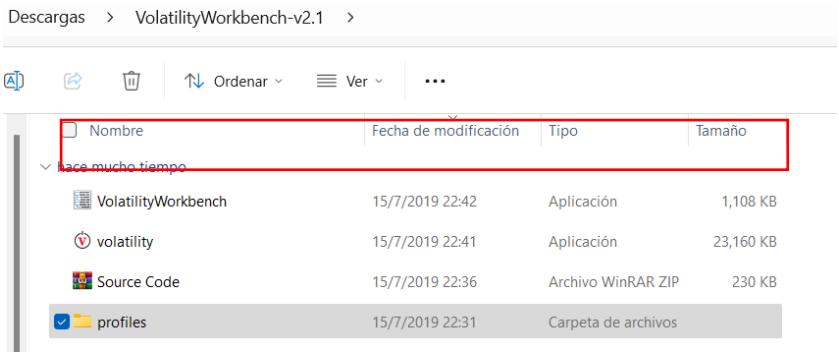
Descarga de volatility workbrench



3. Una vez descargado, se debe descomprimir el archivo zip y se ejecuta la aplicación.

Figura 62.

Descarga de volatility workbrench



4. Cuando se ejecuta la aplicación se busca la imagen de la memoria RAM que se extrajo anteriormente.

Figura 63.

Carga de Imagen

5. Seleccionar la plataforma con la que se va a analizar y presionar **Get proccess List.**

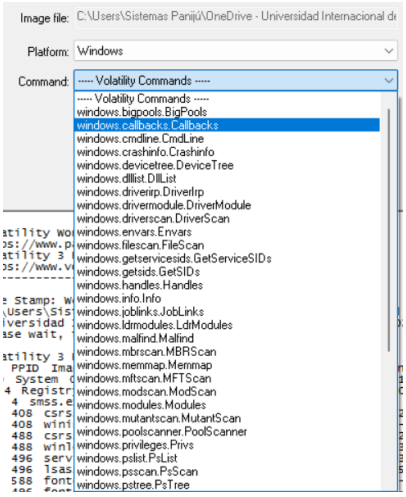
Figura 64.

Carga de plugins

6. Una vez que se haya cargado toda la información se podrá elegir los diferentes plugin con los que se puede trabajar para analizar la imagen.

Figura 65.

Carga de plugins continuación



Para iniciar nuestro análisis se va a revisar la información de la captura.

Figura 66.

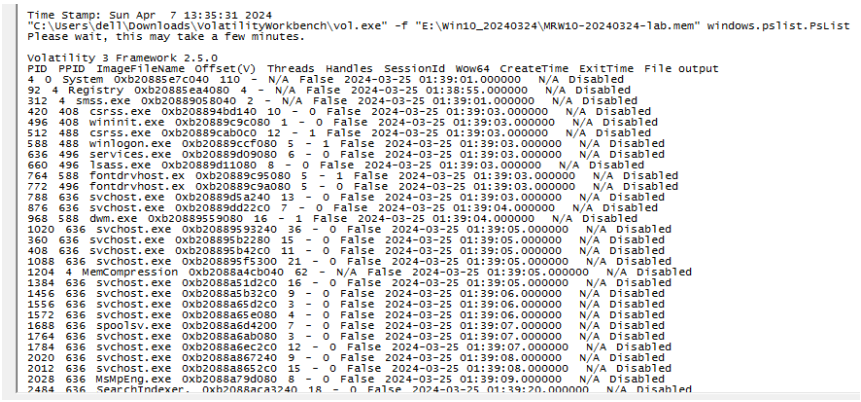
Inicio del análisis

```
Time Stamp: Wed Apr  3 17:43:10 2024
"C:\Users\Sistemas Panijú\Downloads\VolatilityWorkbench\vol.exe" windows.info.Info -h
Please wait, this may take a few minutes.

Volatility 3 Framework 2.5.0
usage: volatility windows.info.Info [-h]
options:
  -h, --help  show this help message and exit

Time Stamp: Wed Apr  3 17:43:11 2024

******* End of command output ******

Time Stamp: Wed Apr  3 17:43:22 2024
"C:\Users\Sistemas Panijú\Downloads\VolatilityWorkbench\vol.exe" -f "C:\Users\Sistemas Panijú\OneDrive - Universidad Internacional del Ecuador\Laboratorio\Win10_20240324\MRW10-20240324-
lab.mem" windows.info.Info
Please wait, this may take a few minutes.

Volatility 3 Framework 2.5.0
Variable  Value
Kernel Base  0xf80144419000
DTB  0x1ad000
Symbols  file:///C:/Users/Sistemas%20Panij%C3%BA/Downloads/VolatilityWorkbench/symbols/windows/ntkrnlmp.pdb/3A3DF78E73ED8201D671C995F240BCDC-1.json.xz
IS64Bit  True
ISPAE  False
layer_name  0 WindowsIntel32e
memory_layer  1 FileLayer
KdVersionBlock  0xf80145028408
Major/Minor  15.19041
MachineType  34404
KeNumberProcessors  2
SystemTime  2024-03-25 03:16:10
NtSystemRoot  C:\Windows
NtProductType  NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine  34404
PE TimeDateStamp  Sun Feb 16 02:05:08 2003

Time Stamp: Wed Apr  3 17:43:26 2024

******* End of command output ******
```

7. Se continúa revisando la lista de todos los procesos que se están ejecutando al momento de extraer la imagen con el comando **pslist.**

Figura 67.

Plugin pslist



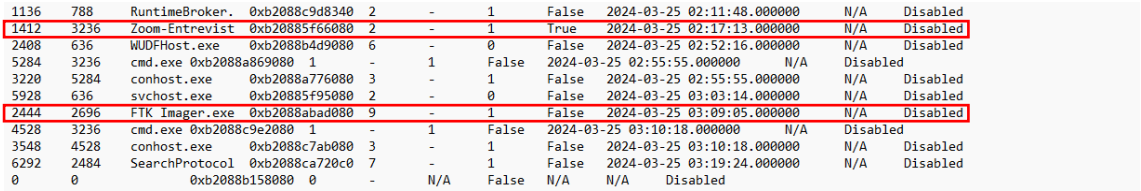
```
Time Stamp: Sun Apr  7 13:35:31 2024
"C:\Users\dell\Downloads\VolatilityWorkbench\vol.exe" -f "E:\Win10_20240324\MRW10-20240324-lab.mem" windows.pslist.PsList
Please wait, this may take a few minutes.

Volatility 3 Framework 2.5.0
PID  PPID  ImageFileName  Offset(V)  Threads  Handles  SessionId  Wow64  CreateTime  ExitTime  File output
4  0  System  0xb20885e7c040  110  -  N/A  False  2024-03-25 01:39:01.000000  N/A  Disabled
92  4  Registry  0xb20885ea4080  4  -  N/A  False  2024-03-25 01:38:55.000000  N/A  Disabled
312  4  smss.exe  0xb20889058040  2  -  N/A  False  2024-03-25 01:39:01.000000  N/A  Disabled
420  408  csrss.exe  0xb208894bd140  10  -  0  False  2024-03-25 01:39:03.000000  N/A  Disabled
496  408  wininit.exe  0xb20889c9c080  1  -  0  False  2024-03-25 01:39:03.000000  N/A  Disabled
512  488  csrss.exe  0xb20889cab0c0  12  -  1  False  2024-03-25 01:39:03.000000  N/A  Disabled
588  488  winlogon.exe  0xb20889ccf080  5  -  1  False  2024-03-25 01:39:03.000000  N/A  Disabled
636  496  services.exe  0xb20889d09080  6  -  0  False  2024-03-25 01:39:03.000000  N/A  Disabled
660  496  lsass.exe  0xb20889d11080  8  -  0  False  2024-03-25 01:39:03.000000  N/A  Disabled
764  588  fontdrvhost.ex  0xb20889c95080  5  -  1  False  2024-03-25 01:39:03.000000  N/A  Disabled
772  496  fontdrvhost.ex  0xb20889c9a080  5  -  0  False  2024-03-25 01:39:03.000000  N/A  Disabled
788  636  svchost.exe  0xb20889d5a240  13  -  0  False  2024-03-25 01:39:03.000000  N/A  Disabled
876  636  svchost.exe  0xb20889dd22c0  7  -  0  False  2024-03-25 01:39:04.000000  N/A  Disabled
968  588  dwm.exe  0xb20889559080  16  -  1  False  2024-03-25 01:39:04.000000  N/A  Disabled
1020  636  svchost.exe  0xb20889593240  36  -  0  False  2024-03-25 01:39:05.000000  N/A  Disabled
360  636  svchost.exe  0xb208895b2280  15  -  0  False  2024-03-25 01:39:05.000000  N/A  Disabled
408  636  svchost.exe  0xb208895b42c0  11  -  0  False  2024-03-25 01:39:05.000000  N/A  Disabled
1088  636  svchost.exe  0xb208895f5300  21  -  0  False  2024-03-25 01:39:05.000000  N/A  Disabled
1204  4  MemCompression  0xb2088a4cb040  62  -  N/A  False  2024-03-25 01:39:05.000000  N/A  Disabled
1384  636  svchost.exe  0xb2088a51d2c0  16  -  0  False  2024-03-25 01:39:05.000000  N/A  Disabled
1456  636  svchost.exe  0xb2088a5b32c0  9  -  0  False  2024-03-25 01:39:06.000000  N/A  Disabled
1556  636  svchost.exe  0xb2088a65d2c0  3  -  0  False  2024-03-25 01:39:06.000000  N/A  Disabled
1572  636  svchost.exe  0xb2088a65e080  4  -  0  False  2024-03-25 01:39:06.000000  N/A  Disabled
1688  636  spoolsv.exe  0xb2088a6d4200  7  -  0  False  2024-03-25 01:39:07.000000  N/A  Disabled
1764  636  svchost.exe  0xb2088a6ab080  3  -  0  False  2024-03-25 01:39:07.000000  N/A  Disabled
1784  636  svchost.exe  0xb2088a6ec2c0  12  -  0  False  2024-03-25 01:39:07.000000  N/A  Disabled
2020  636  svchost.exe  0xb2088a867240  9  -  0  False  2024-03-25 01:39:08.000000  N/A  Disabled
2012  636  svchost.exe  0xb2088a8652c0  15  -  0  False  2024-03-25 01:39:08.000000  N/A  Disabled
2028  636  MsMpEng.exe  0xb2088a79d080  8  -  0  False  2024-03-25 01:39:09.000000  N/A  Disabled
2484  636  SearchIndexer.  0xb2088aca3240  18  -  0  False  2024-03-25 01:39:20.000000  N/A  Disabled
```

8. Para mayor facilidad del análisis se extrae la información en un archivo **txt**.

9. Al analizar los procesos nos llama la atención los procesos con PID 1412, 2444,

Figura 68.

Análisis de resultados



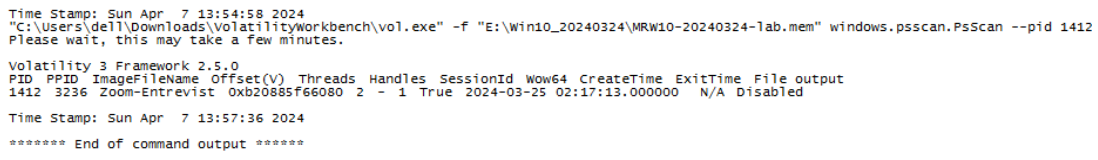
```
1136  788  RuntimeBroker.  0xb2088c9d8340  2  -  1  False  2024-03-25 02:11:48.000000  N/A  Disabled
1412  3236  Zoom-Entrevist  0xb20885f66080  2  -  1  True  2024-03-25 02:17:13.000000  N/A  Disabled
2408  636  WUDFHost.exe  0xb2088b4d9080  6  -  0  False  2024-03-25 02:52:16.000000  N/A  Disabled
5284  3236  cmd.exe 0xb2088a869080  1  -  1  False  2024-03-25 02:55:55.000000  N/A  Disabled
3220  5284  conhost.exe  0xb2088a776080  3  -  1  False  2024-03-25 02:55:55.000000  N/A  Disabled
5928  636  svchost.exe  0xb20885f95080  2  -  0  False  2024-03-25 03:03:14.000000  N/A  Disabled
2444  2696  FTK Imager.exe  0xb2088abad080  9  -  1  False  2024-03-25 03:09:05.000000  N/A  Disabled
4528  3236  cmd.exe 0xb2088c9e2080  1  -  1  False  2024-03-25 03:10:18.000000  N/A  Disabled
3548  4528  conhost.exe  0xb2088c7ab080  3  -  1  False  2024-03-25 03:10:18.000000  N/A  Disabled
6292  2484  SearchProtocol  0xb2088ca720c0  7  -  1  False  2024-03-25 03:19:24.000000  N/A  Disabled
0  0  0xb2088b158080  0  -  N/A  False  N/A  N/A  Disabled
```

- El proceso 1412 corresponde a una aplicación llamada Zoom-Entrevist, la cual fue iniciada 25-03-2024 a las 02:17:13, por lo que se procede a ampliar su análisis.
- El proceso 2444 corresponde al volcado de la imagen de la memoria ram al momento que se la extrajo.

10. Se analiza si el proceso 1412 tiene subprocesos con el comando **psscan.**

Figura 69.

Plugin psscan

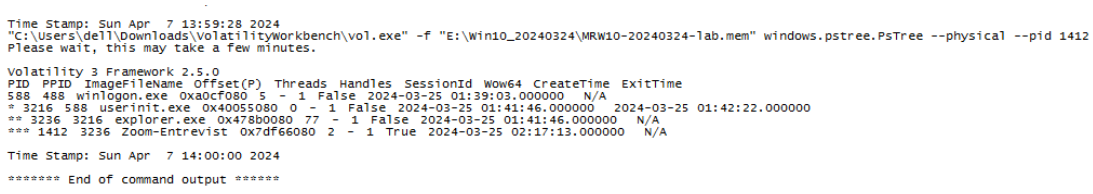


```
Time Stamp: Sun Apr  7 13:54:58 2024
"C:\Users\dell\Downloads\VolatilityWorkbench\vol.exe" -f "E:\Win10_20240324\MRW10-20240324-lab.mem" windows.psscan.PsScan --pid 1412
Please wait, this may take a few minutes.

Volatility 3 Framework 2.5.0
PID  PPID  ImageFileName  Offset(V)  Threads  Handles  SessionId  Wow64  CreateTime  ExitTime  File output
1412  3236  Zoom-Entrevist  0xb20885f66080  2  -  1  True  2024-03-25 02:17:13.000000  N/A  Disabled

Time Stamp: Sun Apr  7 13:57:36 2024

******* End of command output ******
```

11. Revisar el árbol de procesos correspondiente al proceso 1412 con el comando **pstree.**

Figura 70.

Plugin pstree

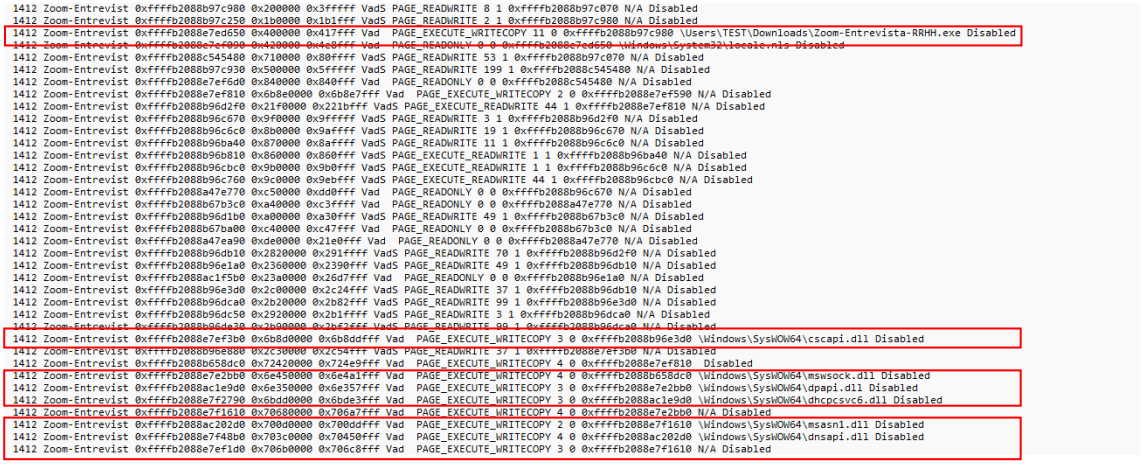


```
Time Stamp: Sun Apr  7 13:59:28 2024
"C:\Users\dell\Downloads\VolatilityWorkbench\vol.exe" -f "E:\Win10_20240324\MRW10-20240324-lab.mem" windows.pstree.PsTree --physical --pid 1412
Please wait, this may take a few minutes.

Volatility 3 Framework 2.5.0
PID  PPID  ImageFileName  Offset(P)  Threads  Handles  SessionId  Wow64  CreateTime  ExitTime
588  488  winlogon.exe  0xa0cf080  5  -  1  False  2024-03-25 01:39:03.000000  N/A
* 3216  588  userinit.exe  0x40055080  0  -  1  False  2024-03-25 01:41:46.000000  2024-03-25 01:42:22.000000
** 3236  3216  explorer.exe  0x478b0080  77  -  1  False  2024-03-25 01:41:46.000000  N/A
*** 1412  3236  Zoom-Entrevist  0x7df66080  2  -  1  True  2024-03-25 02:17:13.000000  N/A

Time Stamp: Sun Apr  7 14:00:00 2024

******* End of command output ******
```

12. Para obtener información ampliada se ejecuta el comando **Vadinfo**, donde se puede observar que el proceso 1412 se ejecuta desde una descarga llamada **Zoom-Entrevista-RRHH.exe** y hace modificaciones en archivos dentro de la ruta **\Windows\SysWOW64.**

Figura 71.

Plugin Vadinfo



```
1412 Zoom-Entrevist 0xffffb2088b97c980 0x200000 0x3fffff VadS PAGE_READWRITE 8 1 0xffffb2088b97c070 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b97c250 0x1b0000 0x1b1fff VadS PAGE_READWRITE 2 1 0xffffb2088b97c980 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088e7ed650 0x400000 0x417fff Vad  PAGE_EXECUTE_WRITECOPY 11 0 0xffffb2088b97c980 \Users\TEST\Downloads\Zoom-Entrevista-RRHH.exe Disabled
1412 Zoom-Entrevist 0xffffb2088e7cf090 0x420000 0x4c8fff Vad  PAGE_READONLY 0 0 0xffffb2088e7ed650 \Windows\System32\locale.nls Disabled
1412 Zoom-Entrevist 0xffffb2088c545480 0x710000 0x80ffff VadS PAGE_READWRITE 53 1 0xffffb2088b97c070 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b97c930 0x500000 0x5fffff VadS PAGE_READWRITE 199 1 0xffffb2088c545480 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088e7ef6d0 0x840000 0x840fff Vad  PAGE_READONLY 0 0 0xffffb2088c545480 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088e7ef810 0x6b8e0000 0x6b8e7fff Vad  PAGE_EXECUTE_WRITECOPY 2 0 0xffffb2088e7ef590 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96d2f0 0x21f0000 0x221bfff VadS PAGE_EXECUTE_READWRITE 44 1 0xffffb2088e7ef810 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96c670 0x9f0000 0x9fffff VadS PAGE_READWRITE 3 1 0xffffb2088b96d2f0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96c6c0 0x8b0000 0x9affff VadS PAGE_READWRITE 19 1 0xffffb2088b96c670 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96ba40 0x870000 0x8affff VadS PAGE_READWRITE 11 1 0xffffb2088b96c6c0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96b810 0x860000 0x860fff VadS PAGE_EXECUTE_READWRITE 1 1 0xffffb2088b96ba40 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96cbc0 0x9b0000 0x9b0fff VadS PAGE_EXECUTE_READWRITE 1 1 0xffffb2088b96c6c0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96c760 0x9c0000 0x9ebfff VadS PAGE_EXECUTE_READWRITE 44 1 0xffffb2088b96cbc0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088a47e770 0xc50000 0xdd0fff Vad  PAGE_READONLY 0 0 0xffffb2088b96c670 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b67b3c0 0xa40000 0xc3ffff Vad  PAGE_READONLY 0 0 0xffffb2088a47e770 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96d1b0 0xa00000 0xa30fff VadS PAGE_READWRITE 49 1 0xffffb2088b67b3c0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b67ba00 0xc40000 0xc47fff Vad  PAGE_READONLY 0 0 0xffffb2088b67b3c0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088a47ea90 0xde0000 0x21e0fff Vad  PAGE_READONLY 0 0 0xffffb2088a47e770 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96db10 0x2820000 0x291ffff VadS PAGE_READWRITE 70 1 0xffffb2088b96d2f0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96e1a0 0x2360000 0x2390fff VadS PAGE_READWRITE 49 1 0xffffb2088b96db10 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088ac1f5b0 0x23a0000 0x26d7fff Vad  PAGE_READONLY 0 0 0xffffb2088b96e1a0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96e3d0 0x2c00000 0x2c24fff VadS PAGE_READWRITE 37 1 0xffffb2088b96db10 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96dca0 0x2b20000 0x2b82fff VadS PAGE_READWRITE 99 1 0xffffb2088b96e3d0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96dc50 0x2920000 0x2b1ffff VadS PAGE_READWRITE 3 1 0xffffb2088b96dca0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b96de30 0x2b90000 0x2bf2fff VadS PAGE_READWRITE 99 1 0xffffb2088b96dca0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088e7ef3b0 0x6b8d0000 0x6b8ddfff Vad  PAGE_EXECUTE_WRITECOPY 3 0 0xffffb2088b96e3d0 \Windows\SysWOW64\cscapi.dll Disabled
1412 Zoom-Entrevist 0xffffb2088b96e880 0x2c30000 0x2c54fff VadS PAGE_READWRITE 37 1 0xffffb2088e7ef3b0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088b658dc0 0x72420000 0x724e9fff Vad  PAGE_EXECUTE_WRITECOPY 4 0 0xffffb2088e7ef810  Disabled
1412 Zoom-Entrevist 0xffffb2088e7e2bb0 0x6e450000 0x6e4a1fff Vad  PAGE_EXECUTE_WRITECOPY 4 0 0xffffb2088b658dc0 \Windows\SysWOW64\mswsock.dll Disabled
1412 Zoom-Entrevist 0xffffb2088ac1e9d0 0x6e350000 0x6e357fff Vad  PAGE_EXECUTE_WRITECOPY 3 0 0xffffb2088e7e2bb0 \Windows\SysWOW64\dpapi.dll Disabled
1412 Zoom-Entrevist 0xffffb2088e7f2790 0x6bdd0000 0x6bde3fff Vad  PAGE_EXECUTE_WRITECOPY 3 0 0xffffb2088ac1e9d0 \Windows\SysWOW64\dhcpcsvc6.dll Disabled
1412 Zoom-Entrevist 0xffffb2088e7f1610 0x70680000 0x706a7fff Vad  PAGE_EXECUTE_WRITECOPY 4 0 0xffffb2088e7e2bb0 N/A Disabled
1412 Zoom-Entrevist 0xffffb2088ac202d0 0x700d0000 0x700ddfff Vad  PAGE_EXECUTE_WRITECOPY 2 0 0xffffb2088e7f1610 \Windows\SysWOW64\msasn1.dll Disabled
1412 Zoom-Entrevist 0xffffb2088e7f48b0 0x703c0000 0x70450fff Vad  PAGE_EXECUTE_WRITECOPY 4 0 0xffffb2088ac202d0 \Windows\SysWOW64\dnsapi.dll Disabled
1412 Zoom-Entrevist 0xffffb2088e7ef1d0 0x706b0000 0x706c8fff Vad  PAGE_EXECUTE_WRITECOPY 3 0 0xffffb2088e7f1610 N/A Disabled
```

13. Con el comando **privileges**, se verifica que tipo de privilegios tiene el proceso 142, donde observamos que realiza varias modificaciones internas al equipo.

Figura 72.

Plugin privileges

```
Please wait, this may take a few minutes.

Volatility 3 Framework 2.5.0
PID  Process  Value  Privilege  Attributes  Description
1412  Zoom-Entrevist  2  SeCreateTokenPrivilege   Create a token object
1412  Zoom-Entrevist  3  SeAssignPrimaryTokenPrivilege   Replace a process-level token
1412  Zoom-Entrevist  4  SeLockMemoryPrivilege   Lock pages in memory
1412  Zoom-Entrevist  5  SeIncreaseQuotaPrivilege   Increase quotas
1412  Zoom-Entrevist  6  SeMachineAccountPrivilege   Add workstations to the domain
1412  Zoom-Entrevist  7  SeTcbPrivilege   Act as part of the operating system
1412  Zoom-Entrevist  8  SeSecurityPrivilege   Manage auditing and security log
1412  Zoom-Entrevist  9  SeTakeOwnershipPrivilege   Take ownership of files/objects
1412  Zoom-Entrevist  10  SeLoadDriverPrivilege   Load and unload device drivers
1412  Zoom-Entrevist  11  SeSystemProfilePrivilege   Profile system performance
1412  Zoom-Entrevist  12  SeSystemtimePrivilege   Change the system time
1412  Zoom-Entrevist  13  SeProfileSingleProcessPrivilege   Profile a single process
1412  Zoom-Entrevist  14  SeIncreaseBasePriorityPrivilege   Increase scheduling priority
1412  Zoom-Entrevist  15  SeCreatePagefilePrivilege   Create a pagefile
1412  Zoom-Entrevist  16  SeCreatePermanentPrivilege   Create permanent shared objects
1412  Zoom-Entrevist  17  SeBackupPrivilege   Backup files and directories
1412  Zoom-Entrevist  18  SeRestorePrivilege   Restore files and directories
1412  Zoom-Entrevist  19  SeShutdownPrivilege  Present  Shut down the system
1412  Zoom-Entrevist  20  SeDebugPrivilege   Debug programs
1412  Zoom-Entrevist  21  SeAuditPrivilege   Generate security audits
1412  Zoom-Entrevist  22  SeSystemEnvironmentPrivilege   Edit firmware environment values
1412  Zoom-Entrevist  23  SeChangeNotifyPrivilege  Present,Enabled,Default  Receive notifications of changes to files or directories
1412  Zoom-Entrevist  24  SeRemoteShutdownPrivilege   Force shutdown from a remote system
1412  Zoom-Entrevist  25  SeUndockPrivilege  Present  Remove computer from docking station
1412  Zoom-Entrevist  26  SeSyncAgentPrivilege   Synch directory service data
1412  Zoom-Entrevist  27  SeEnableDelegationPrivilege   Enable user accounts to be trusted for delegation
1412  Zoom-Entrevist  28  SeManageVolumePrivilege   Manage the files on a volume
1412  Zoom-Entrevist  29  SeImpersonatePrivilege   Impersonate a client after authentication
1412  Zoom-Entrevist  30  SeCreateGlobalPrivilege  Default  Create global objects
1412  Zoom-Entrevist  31  SeTrustedCredManAccessPrivilege   Access Credential Manager as a trusted caller
1412  Zoom-Entrevist  32  SeRelabelPrivilege   Modify the mandatory integrity level of an object
1412  Zoom-Entrevist  33  SeIncreaseWorkingSetPrivilege  Present  Allocate more memory for user applications
1412  Zoom-Entrevist  34  SeTimeZonePrivilege  Present  Adjust the time zone of the computer's internal clock
1412  Zoom-Entrevist  35  SeCreateSymbolicLinkPrivilege   Required to create a symbolic link
1412  Zoom-Entrevist  36  SeDelegateSessionUserImpersonatePrivilege   Obtain an impersonation token for another user in the same session.

Time Stamp: Sun Apr  7 15:00:39 2024

******* End of command output ******
```

14. Ya que esta versión de Volatility Workbrendh no permite visualizar las conexiones de red, se hace uso de la versión por CMD en una distribución de Linux para lo cual agregamos volatility 3 desde la página oficial.

Figura 73.

Volatility 3

```
caine@caine:~$ git clone https://github.com/volatilityfoundation/volatility3.git
Cloning into 'volatility3'...
remote: Enumerating objects: 33181, done.
remote: Counting objects: 100% (4105/4105), done.
remote: Compressing objects: 100% (1010/1010), done.
remote: Total 33181 (delta 3624), reused 3319 (delta 3090), pack-reused 29076
Receiving objects: 100% (33181/33181), 6.50 MiB | 351.00 KiB/s, done.
Resolving deltas: 100% (25314/25314), done.
caine@caine:~$ ls -lh
total 0
drwxr-xr-x 2 caine caine 100 apr  7 15:38 debs
drwxr-xr-x 2 caine caine 220 apr  7 15:39 Desktop
drwxr-xr-x 2 caine caine  40 apr  7 15:38 Documents
drwxr-xr-x 2 caine caine  40 apr  7 15:38 Downloads
drwxr-xr-x 2 caine caine  40 apr  7 15:38 Music
drwxr-xr-x 2 caine caine  40 apr  7 15:38 Pictures
drwxr-xr-x 2 caine caine  40 apr  7 15:38 Public
drwxr-xr-x 2 caine caine  40 apr  7 15:38 Templates
drwxr-xr-x 2 caine caine  40 apr  7 15:38 Videos
drwxrwxr-x 8 caine caine 500 apr  7 15:49 volatility3
caine@caine:~$ cd volatility3/
```

15. Al ejecutar el comando **python3 vol.py -h** se verifica que se tienen los plugin que requerimos para completar el análisis.

Figura 74.

Veridicación de plugins

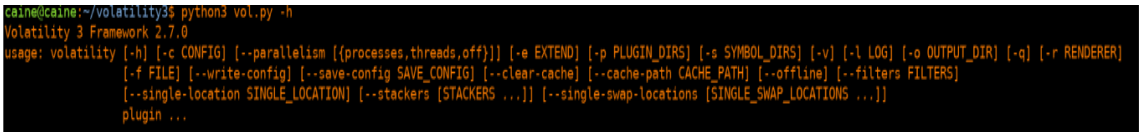
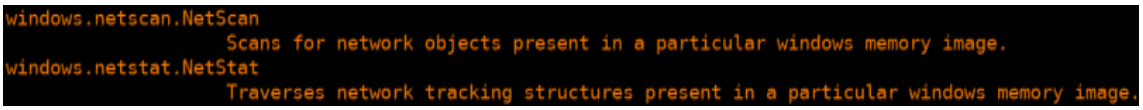


Figura 75.

Plugin netscan



16. Desde la carpeta que contiene volatility3 se analiza la imagen con el comando **python3 vol.py -f /home/kali/Desktop/Win10_20240324/MRW10-20240324-lab.mem windows.netscan.**

Figura 76.

Plugin netscan continuación

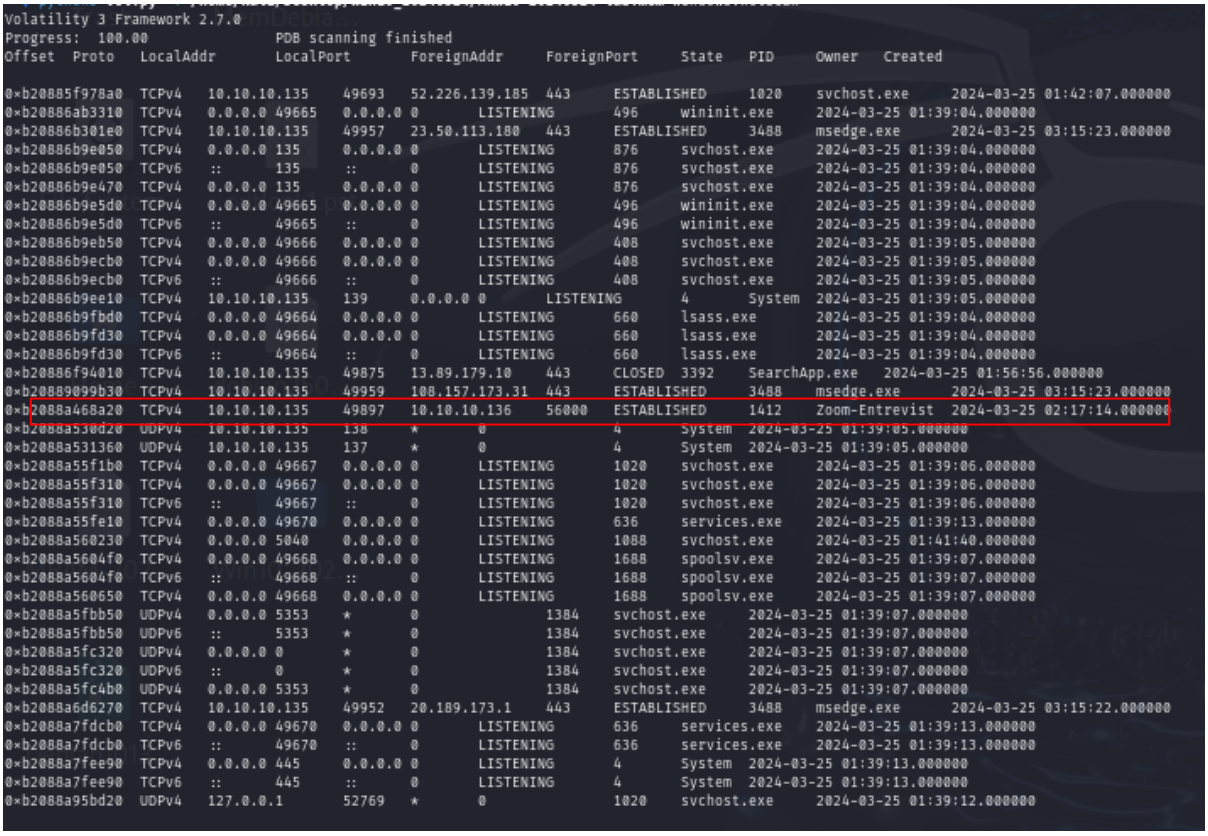
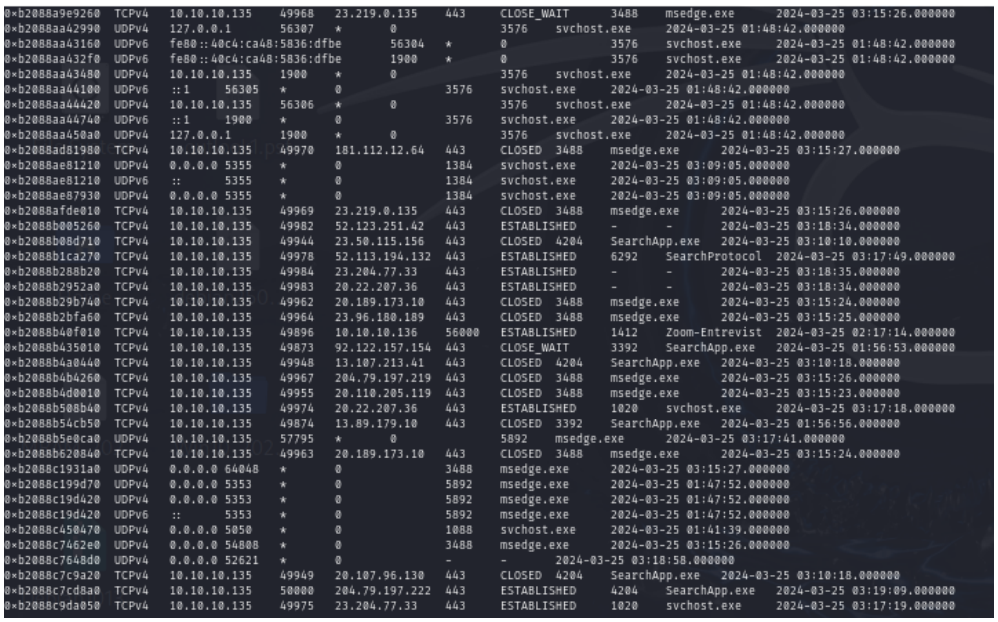


Figura 77.

Plugin netscan continuación

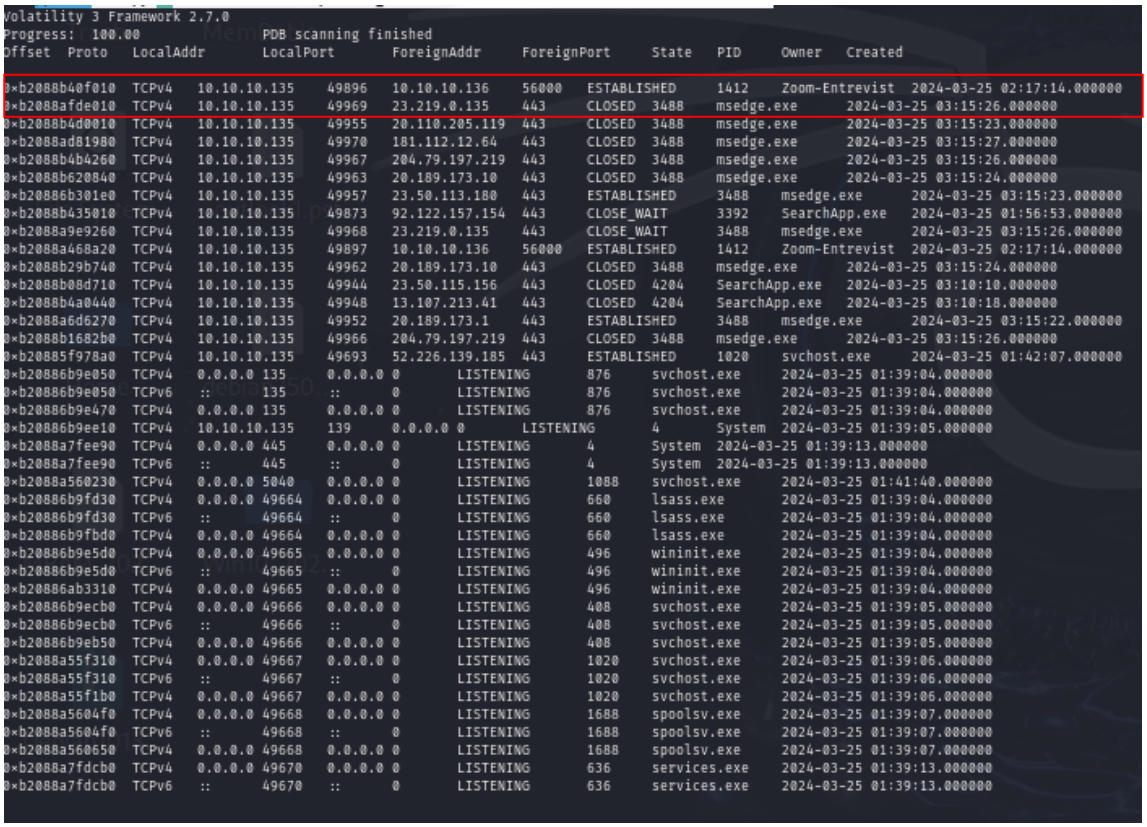


0×b2088a9e9260	TCPv4	10.10.10.135	49968	23.219.0.135	443	CLOSE_WAIT	3488	msedge.exe	2024-03-25 03:15:26.000000
0×b2088aa42990	UDPv4	127.0.0.1	56307	*	0		3576	svchost.exe	2024-03-25 01:48:42.000000
0×b2088aa43160	UDPv6	fe80::40c4:ca48:5836:dfbe	56304	*	0		3576	svchost.exe	2024-03-25 01:48:42.000000
0×b2088aa432f0	UDPv6	fe80::40c4:ca48:5836:dfbe	1900	*	0		3576	svchost.exe	2024-03-25 01:48:42.000000
0×b2088aa43480	UDPv4	10.10.10.135	1900	*	0		3576	svchost.exe	2024-03-25 01:48:42.000000
0×b2088aa44100	UDPv6	::1	56305	*	0		3576	svchost.exe	2024-03-25 01:48:42.000000
0×b2088aa44420	UDPv4	10.10.10.135	56306	*	0		3576	svchost.exe	2024-03-25 01:48:42.000000
0×b2088aa44740	UDPv6	::1	1900	*	0		3576	svchost.exe	2024-03-25 01:48:42.000000
0×b2088aa450a0	UDPv4	127.0.0.1	1900	*	0		3576	svchost.exe	2024-03-25 01:48:42.000000
0×b2088ad81980	TCPv4	10.10.10.135	49970	181.112.12.64	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:27.000000
0×b2088ae81210	UDPv4	0.0.0.0	5355	*	0		1384	svchost.exe	2024-03-25 03:09:05.000000
0×b2088ae81210	UDPv6	::	5355	*	0		1384	svchost.exe	2024-03-25 03:09:05.000000
0×b2088ae87930	UDPv4	0.0.0.0	5355	*	0		1384	svchost.exe	2024-03-25 03:09:05.000000
0×b2088afde010	TCPv4	10.10.10.135	49969	23.219.0.135	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:26.000000
0×b2088b005260	TCPv4	10.10.10.135	49982	52.123.251.42	443	ESTABLISHED	-	-	2024-03-25 03:18:34.000000
0×b2088b08d710	TCPv4	10.10.10.135	49944	23.50.115.156	443	CLOSED	4204	SearchApp.exe	2024-03-25 03:10:10.000000
0×b2088b1ca270	TCPv4	10.10.10.135	49978	52.113.194.132	443	ESTABLISHED	6292	SearchProtocol	2024-03-25 03:17:49.000000
0×b2088b288b20	TCPv4	10.10.10.135	49984	23.204.77.33	443	ESTABLISHED	-	-	2024-03-25 03:18:35.000000
0×b2088b2952a0	TCPv4	10.10.10.135	49983	20.22.207.36	443	ESTABLISHED	-	-	2024-03-25 03:18:34.000000
0×b2088b29b740	TCPv4	10.10.10.135	49962	20.189.173.10	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:24.000000
0×b2088b2bfa60	TCPv4	10.10.10.135	49964	23.96.180.189	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:25.000000
0×b2088b40f010	TCPv4	10.10.10.135	49896	10.10.10.136	56000	ESTABLISHED	1412	Zoom-Entrevist	2024-03-25 02:17:14.000000
0×b2088b435010	TCPv4	10.10.10.135	49873	92.122.157.154	443	CLOSE_WAIT	3392	SearchApp.exe	2024-03-25 01:56:53.000000
0×b2088b4a0440	TCPv4	10.10.10.135	49948	13.107.213.41	443	CLOSED	4204	SearchApp.exe	2024-03-25 03:10:18.000000
0×b2088b4b4260	TCPv4	10.10.10.135	49967	204.79.197.219	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:26.000000
0×b2088b4d0010	TCPv4	10.10.10.135	49955	20.110.205.119	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:23.000000
0×b2088b508b40	TCPv4	10.10.10.135	49974	20.22.207.36	443	ESTABLISHED	1020	svchost.exe	2024-03-25 03:17:18.000000
0×b2088b54cb50	TCPv4	10.10.10.135	49874	13.89.179.10	443	CLOSED	3392	SearchApp.exe	2024-03-25 01:56:56.000000
0×b2088b5e0ca0	UDPv4	10.10.10.135	57795	*	0		5892	msedge.exe	2024-03-25 03:17:41.000000
0×b2088b620840	TCPv4	10.10.10.135	49963	20.189.173.10	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:24.000000
0×b2088c1931a0	UDPv4	0.0.0.0	64048	*	0		3488	msedge.exe	2024-03-25 03:15:27.000000
0×b2088c199d70	UDPv4	0.0.0.0	5353	*	0		5892	msedge.exe	2024-03-25 01:47:52.000000
0×b2088c19d420	UDPv4	0.0.0.0	5353	*	0		5892	msedge.exe	2024-03-25 01:47:52.000000
0×b2088c19d420	UDPv6	::	5353	*	0		5892	msedge.exe	2024-03-25 01:47:52.000000
0×b2088c450470	UDPv4	0.0.0.0	5050	*	0		1088	svchost.exe	2024-03-25 01:41:39.000000
0×b2088c7462e0	UDPv4	0.0.0.0	54808	*	0		3488	msedge.exe	2024-03-25 03:15:26.000000
0×b2088c7648d0	UDPv4	0.0.0.0	52621	*	0		-	-	2024-03-25 03:18:58.000000
0×b2088c7c9a20	TCPv4	10.10.10.135	49949	20.107.96.130	443	CLOSED	4204	SearchApp.exe	2024-03-25 03:10:18.000000
0×b2088c7cd8a0	TCPv4	10.10.10.135	50000	204.79.197.222	443	ESTABLISHED	4204	SearchApp.exe	2024-03-25 03:19:09.000000
0×b2088c9da050	TCPv4	10.10.10.135	49975	23.204.77.33	443	ESTABLISHED	1020	svchost.exe	2024-03-25 03:17:19.000000

Con el siguiente comando se pueden observar las conexiones TCP: **python3 vol.py -f /home/kali/Desktop/Win10_20240324/MRW10-20240324-lab.mem windows.netstat..**

Figura 78.

Plugin netstat conexiones



Volatility 3 Framework 2.7.0
Progress: 100.00 PDB scanning finished

Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created
0×b2088b40f010	TCPv4	10.10.10.135	49896	10.10.10.136	56000	ESTABLISHED	1412	Zoom-Entrevist	2024-03-25 02:17:14.000000
0×b2088afde010	TCPv4	10.10.10.135	49969	23.219.0.135	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:26.000000
0×b2088b4d0010	TCPv4	10.10.10.135	49955	20.110.205.119	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:23.000000
0×b2088ad81980	TCPv4	10.10.10.135	49970	181.112.12.64	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:27.000000
0×b2088b4b4260	TCPv4	10.10.10.135	49967	204.79.197.219	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:26.000000
0×b2088b620840	TCPv4	10.10.10.135	49963	20.189.173.10	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:24.000000
0×b20886b301e0	TCPv4	10.10.10.135	49957	23.50.113.180	443	ESTABLISHED	3488	msedge.exe	2024-03-25 03:15:23.000000
0×b2088b435010	TCPv4	10.10.10.135	49873	92.122.157.154	443	CLOSE_WAIT	3392	SearchApp.exe	2024-03-25 01:56:53.000000
0×b2088a9e9260	TCPv4	10.10.10.135	49968	23.219.0.135	443	CLOSE_WAIT	3488	msedge.exe	2024-03-25 03:15:26.000000
0×b2088a468a20	TCPv4	10.10.10.135	49897	10.10.10.136	56000	ESTABLISHED	1412	Zoom-Entrevist	2024-03-25 02:17:14.000000
0×b2088b29b740	TCPv4	10.10.10.135	49962	20.189.173.10	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:24.000000
0×b2088b08d710	TCPv4	10.10.10.135	49944	23.50.115.156	443	CLOSED	4204	SearchApp.exe	2024-03-25 03:10:10.000000
0×b2088b4a0440	TCPv4	10.10.10.135	49948	13.107.213.41	443	CLOSED	4204	SearchApp.exe	2024-03-25 03:10:18.000000
0×b2088a6d6270	TCPv4	10.10.10.135	49952	20.189.173.1	443	ESTABLISHED	3488	msedge.exe	2024-03-25 03:15:22.000000
0×b2088b1682b0	TCPv4	10.10.10.135	49966	204.79.197.219	443	CLOSED	3488	msedge.exe	2024-03-25 03:15:26.000000
0×b2085f978a0	TCPv4	10.10.10.135	49693	52.226.139.185	443	ESTABLISHED	1020	svchost.exe	2024-03-25 01:42:07.000000
0×b20886b9e050	TCPv4	0.0.0.0	135	0.0.0.0	0	LISTENING	876	svchost.exe	2024-03-25 01:39:04.000000
0×b20886b9e050	TCPv6	::	135	::	0	LISTENING	876	svchost.exe	2024-03-25 01:39:04.000000
0×b20886b9e470	TCPv4	0.0.0.0	135	0.0.0.0	0	LISTENING	876	svchost.exe	2024-03-25 01:39:04.000000
0×b20886b9ee10	TCPv4	10.10.10.135	139	0.0.0.0	0	LISTENING	4	System	2024-03-25 01:39:05.000000
0×b2088a7fee90	TCPv4	0.0.0.0	445	0.0.0.0	0	LISTENING	4	System	2024-03-25 01:39:13.000000
0×b2088a7fee90	TCPv6	::	445	::	0	LISTENING	4	System	2024-03-25 01:39:13.000000
0×b2088a560230	TCPv4	0.0.0.0	5040	0.0.0.0	0	LISTENING	1088	svchost.exe	2024-03-25 01:41:40.000000
0×b20886b9fd30	TCPv4	0.0.0.0	49664	0.0.0.0	0	LISTENING	660	lsass.exe	2024-03-25 01:39:04.000000
0×b20886b9fd30	TCPv6	::	49664	::	0	LISTENING	660	lsass.exe	2024-03-25 01:39:04.000000
0×b20886b9fbd0	TCPv4	0.0.0.0	49664	0.0.0.0	0	LISTENING	660	lsass.exe	2024-03-25 01:39:04.000000
0×b20886b9e5d0	TCPv4	0.0.0.0	49665	0.0.0.0	0	LISTENING	496	wininit.exe	2024-03-25 01:39:04.000000
0×b20886b9e5d0	TCPv6	::	49665	::	0	LISTENING	496	wininit.exe	2024-03-25 01:39:04.000000
0×b20886ab3310	TCPv4	0.0.0.0	49665	0.0.0.0	0	LISTENING	496	wininit.exe	2024-03-25 01:39:04.000000
0×b20886b9ecb0	TCPv4	0.0.0.0	49666	0.0.0.0	0	LISTENING	408	svchost.exe	2024-03-25 01:39:05.000000
0×b20886b9ecb0	TCPv6	::	49666	::	0	LISTENING	408	svchost.exe	2024-03-25 01:39:05.000000
0×b20886b9eb50	TCPv4	0.0.0.0	49666	0.0.0.0	0	LISTENING	408	svchost.exe	2024-03-25 01:39:05.000000
0×b2088a55f310	TCPv4	0.0.0.0	49667	0.0.0.0	0	LISTENING	1020	svchost.exe	2024-03-25 01:39:06.000000
0×b2088a55f310	TCPv6	::	49667	::	0	LISTENING	1020	svchost.exe	2024-03-25 01:39:06.000000
0×b2088a55f1b0	TCPv4	0.0.0.0	49667	0.0.0.0	0	LISTENING	1020	svchost.exe	2024-03-25 01:39:06.000000
0×b2088a5604f0	TCPv4	0.0.0.0	49668	0.0.0.0	0	LISTENING	1688	spoolsv.exe	2024-03-25 01:39:07.000000
0×b2088a5604f0	TCPv6	::	49668	::	0	LISTENING	1688	spoolsv.exe	2024-03-25 01:39:07.000000
0×b2088a560650	TCPv4	0.0.0.0	49668	0.0.0.0	0	LISTENING	1688	spoolsv.exe	2024-03-25 01:39:07.000000
0×b2088a7fdcb0	TCPv4	0.0.0.0	49670	0.0.0.0	0	LISTENING	636	services.exe	2024-03-25 01:39:13.000000
0×b2088a7fdcb0	TCPv6	::	49670	::	0	LISTENING	636	services.exe	2024-03-25 01:39:13.000000

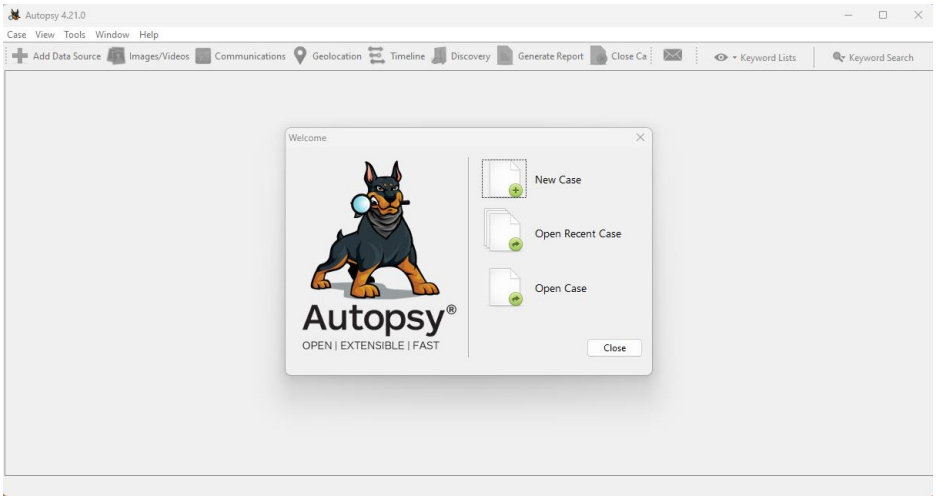
Con ambos comandos se puede determinar que esta máquina está teniendo una conexión a la IP 10.10.10.136 a través del puerto 56000, por medio del proceso 1412

Análisis de la imagen del Disco duro.

17. Abrir Autopsy y seleccionar **New Case.**

Figura 79.

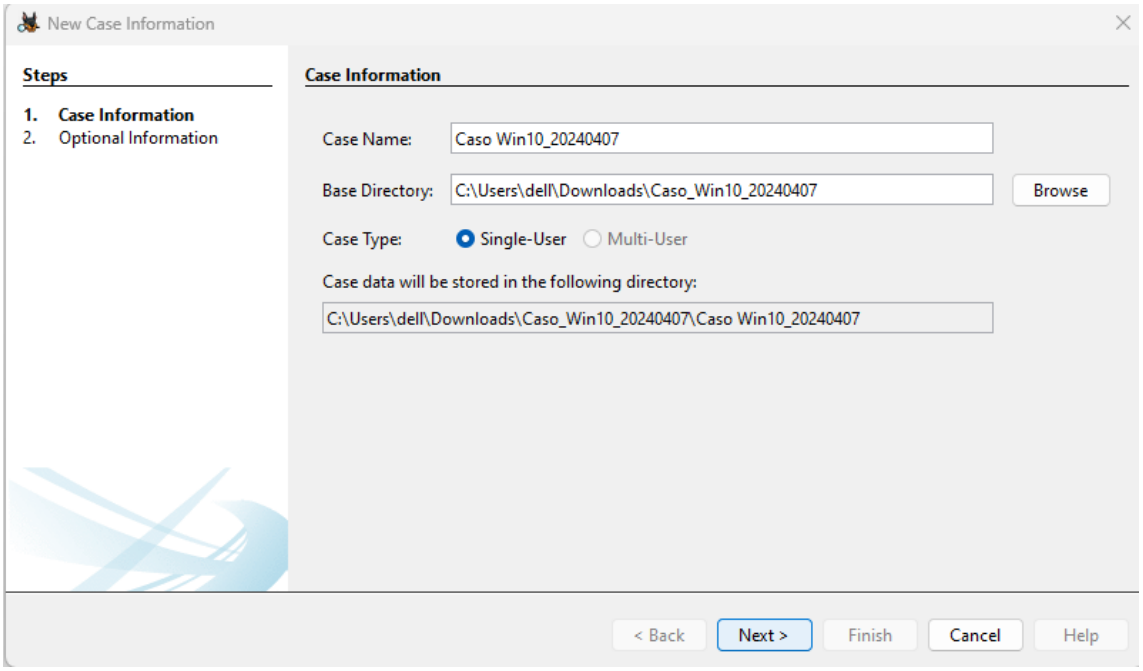
Autopsy



18. Ingresar los datos del caso.

Figura 80.

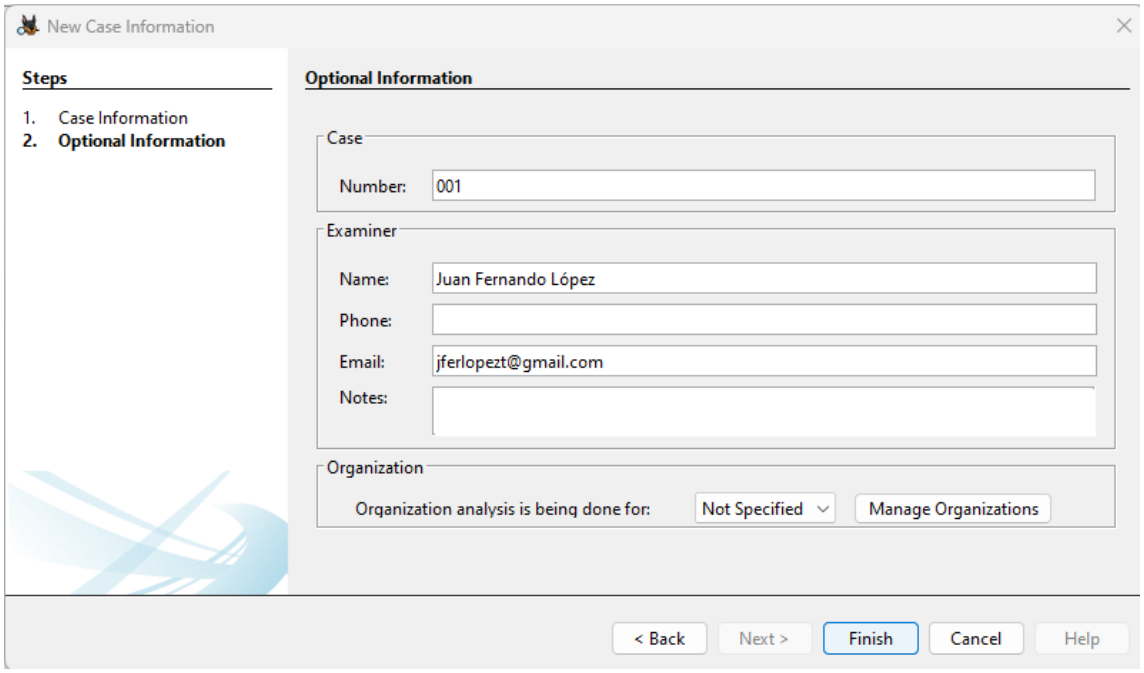
Información del caso



19. Ingresar la información del investigador y finalizar.

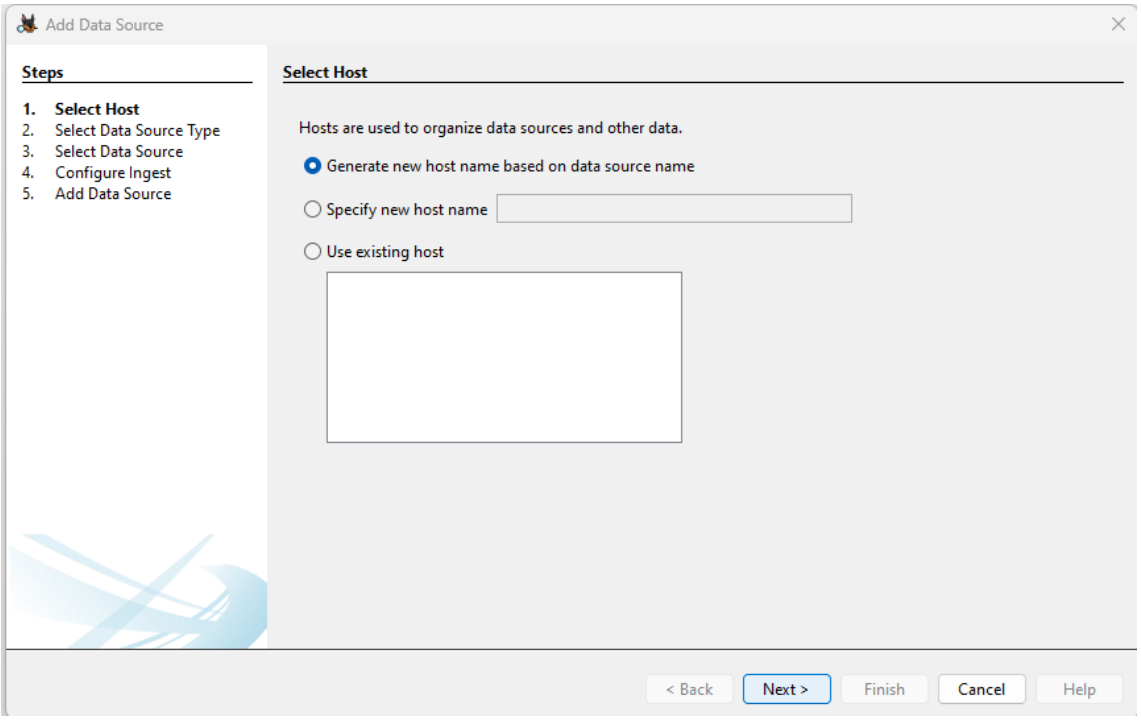
Figura 81.

Información adicional



20. Generar un nombre de host.

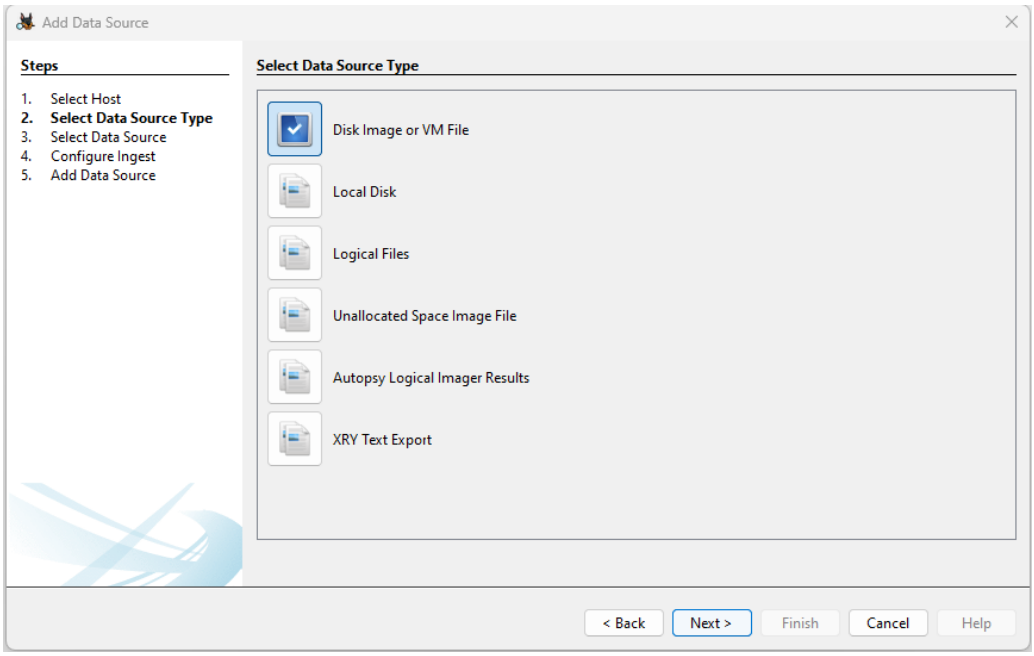
Selección del host



21. Seleccionar el tipo de origen.

Figura 82.

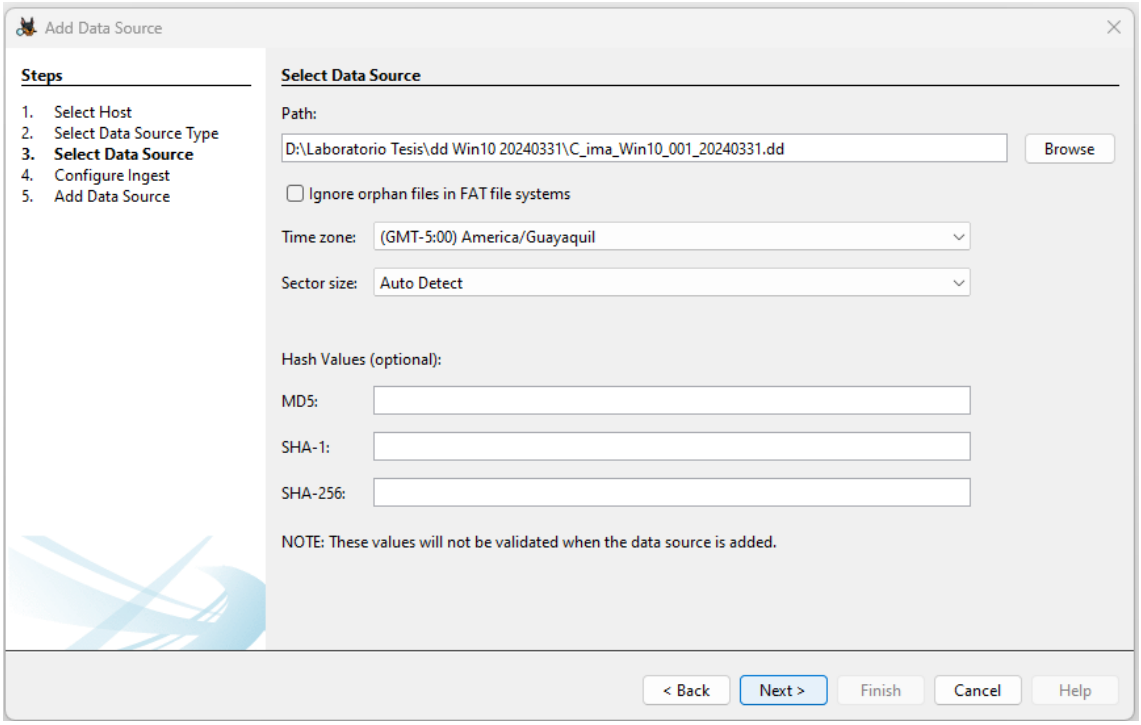
Tipo de origen



22. Seleccionar el origen.

Figura 83.

Selección del origen



23. Seleccionar los módulos de ingesta para lo cual se sugiere marcar:

- Recent Activity
- Hash Lookup
- File Type Identification
- Extension Mismatch Detector
- Picture Analizer
- Keywords Search
- Photorec Carver
- Data Spurce Integrity

24. Al momento de establecer las palabras clave , es importante usar palabras encontradas al analizar la imagen de la memoria RAM.

Figura 84.

Colocación de palabras clave

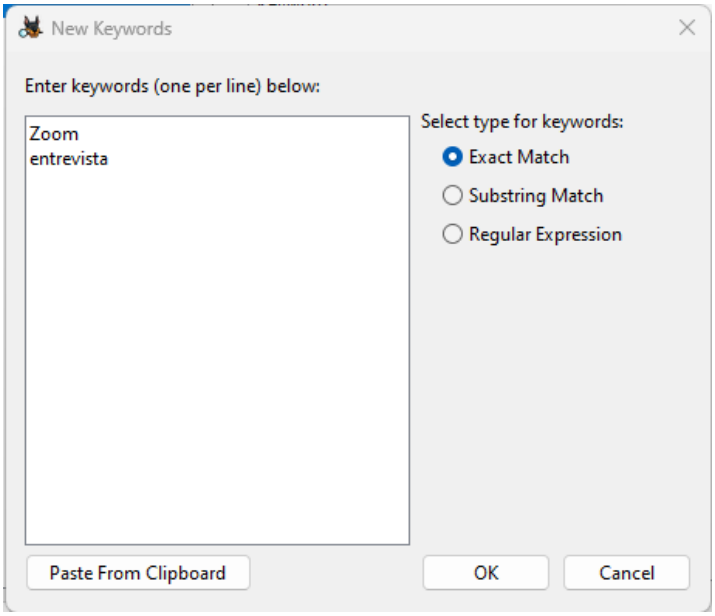
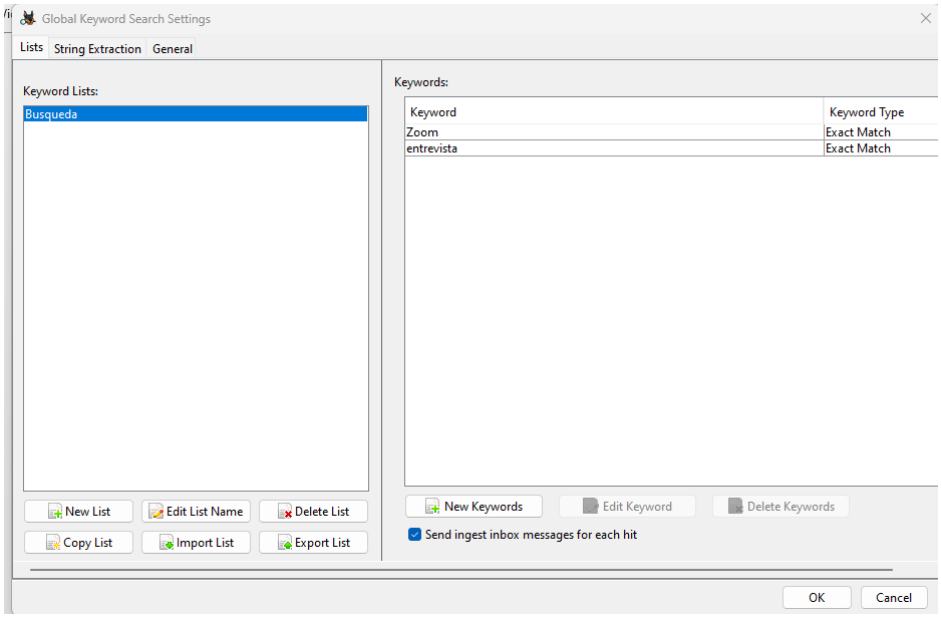


Figura 85.

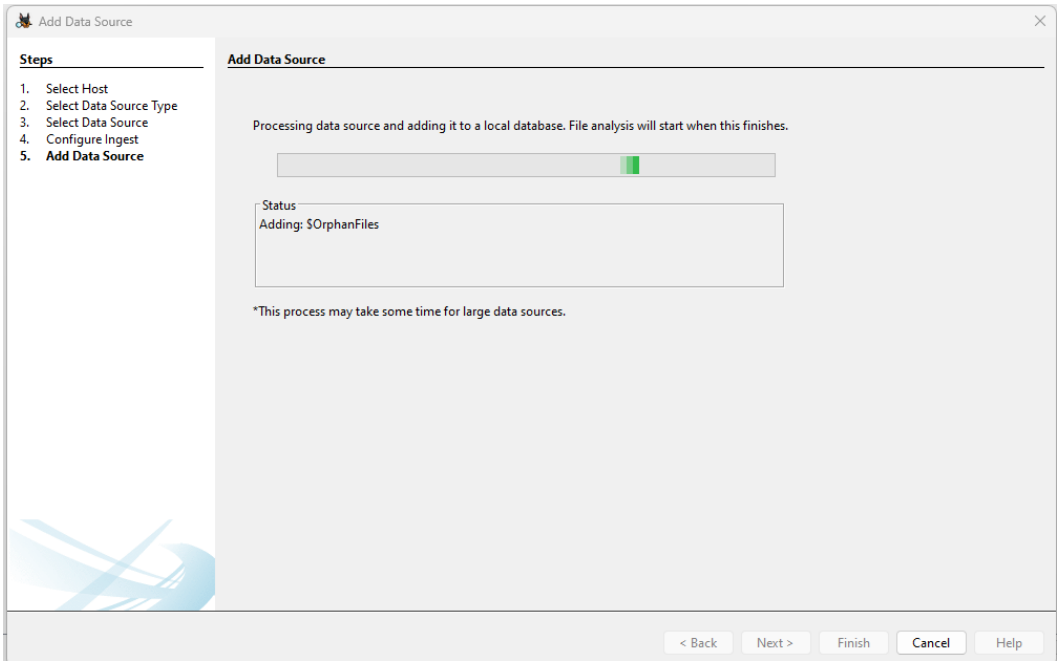
Colocación de palabras clave



25. Iniciar el análisis.

Figura 86.

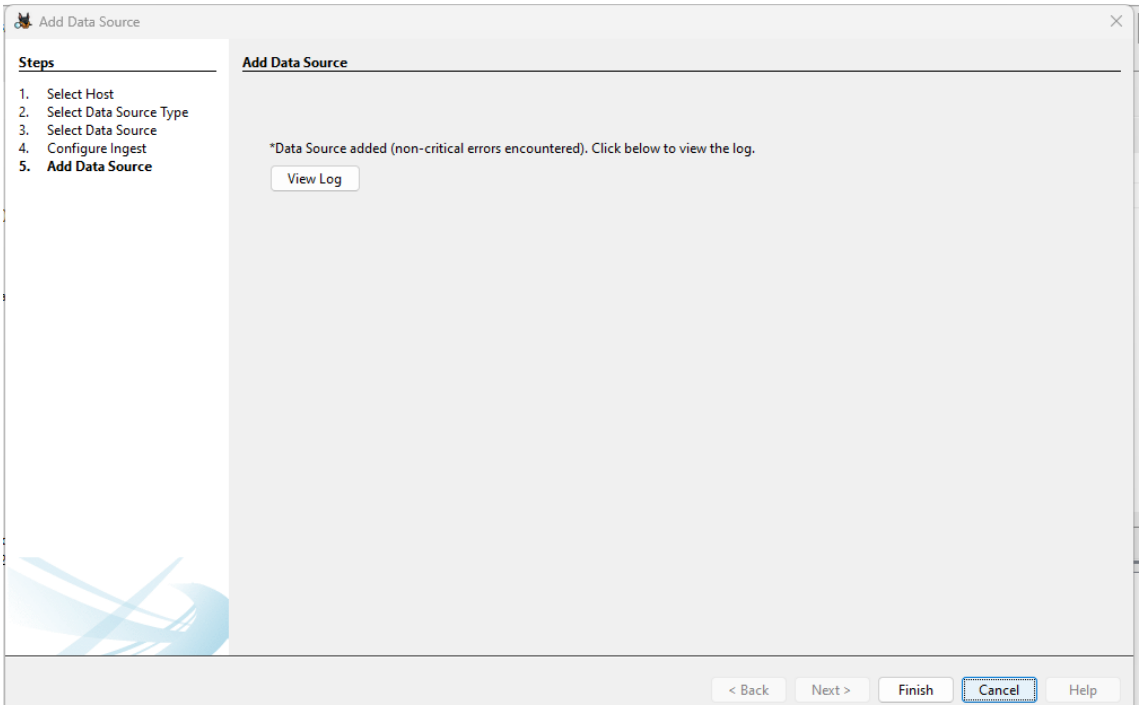
Inicio del analisis



26. Finalizar la carga y esperar a que termine el análisis.

Figura 87.

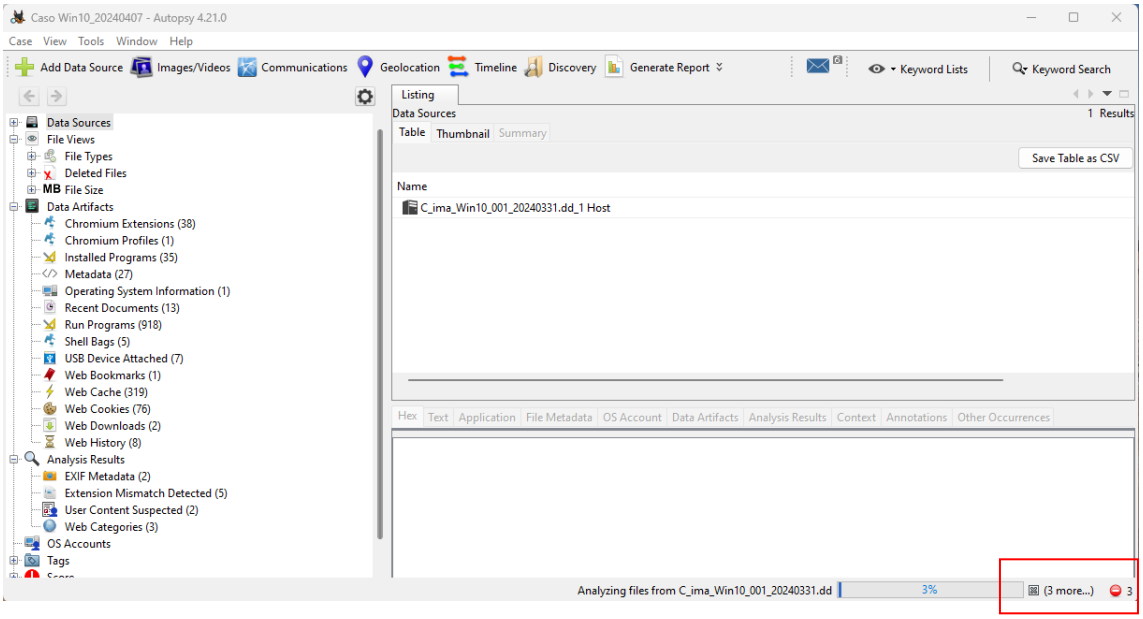
Finalización de la carga



27. Se debe prestar mucha atención a las alertas que aparecen, para poder dar continuidad al análisis.

Figura 88.

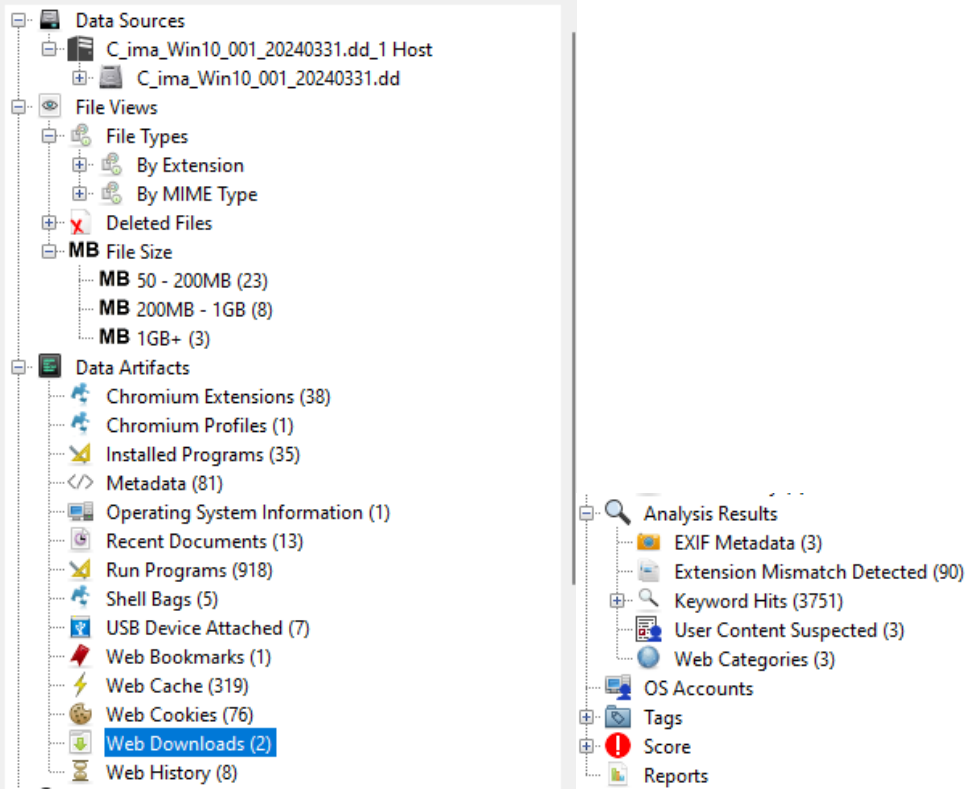
Revisión de alertas



Tras finalizar la carga se pueden revisar todos los archivos, organizados por diferentes categorías.

Figura 89.

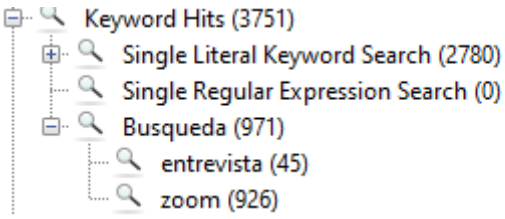
Análisis finalizado organizado por categorias



Cuando se hizo la carga se establecieron las palabras clave “Zoom” “Entrevista”, por lo que se pude iniciar el análisis por separado.

Figura 90.

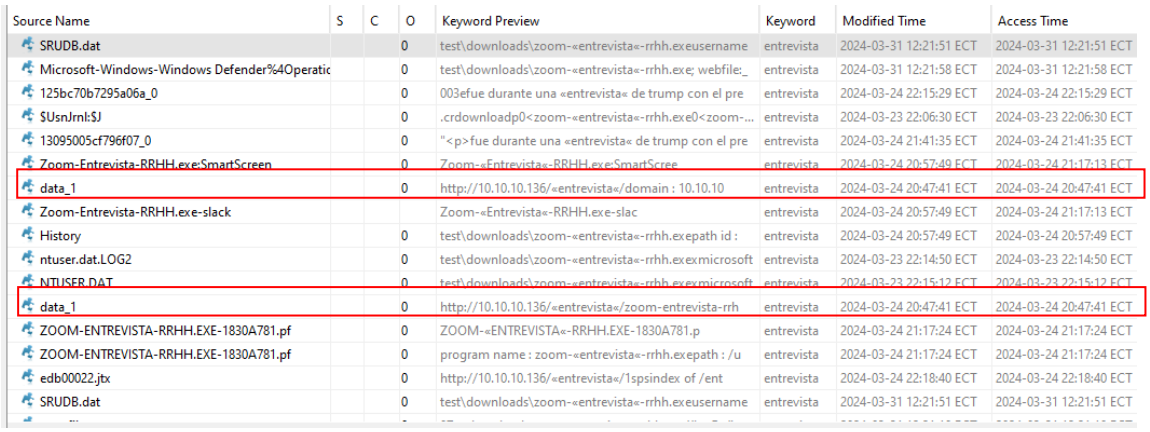
Resultados de las palabras clave



Al elegir los resultados de entrevista se encuentra la ubicación del archivo ejecutado, la IP a la que se conecta.

Figura 91.

Ip de conexion

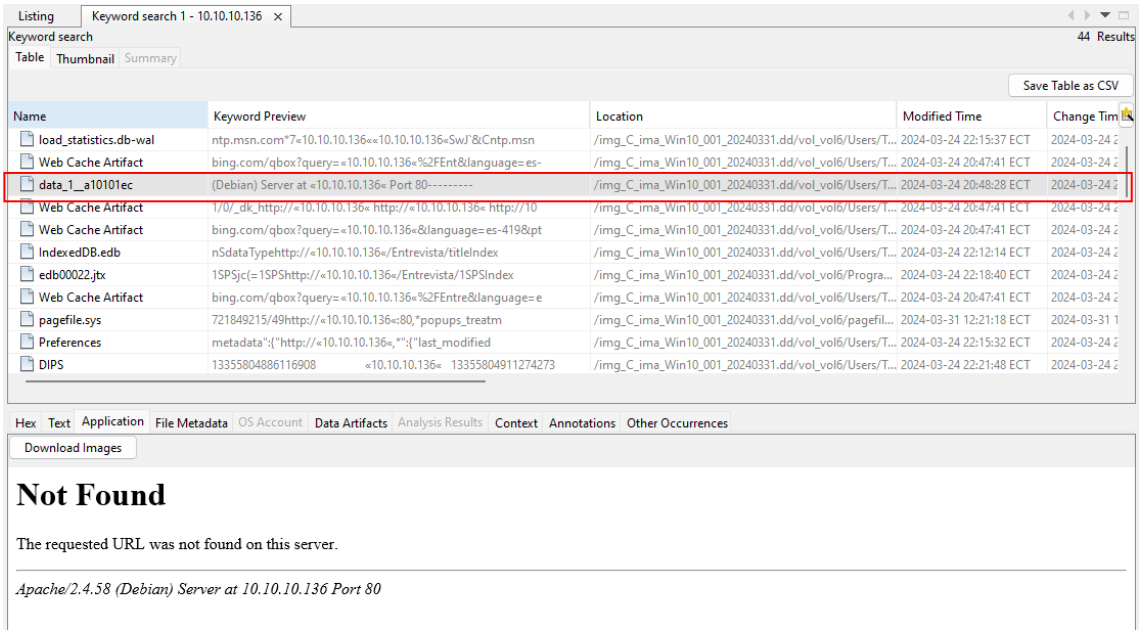


Source Name	S	C	O	Keyword Preview	Keyword	Modified Time	Access Time
SRUDB.dat			0	test\downloads\zoom-«entrevista«-rrhh.exeusername	entrevista	2024-03-31 12:21:51 ECT	2024-03-31 12:21:51 ECT
Microsoft-Windows-Windows Defender%4Operatic			0	test\downloads\zoom-«entrevista«-rrhh.exe; webfile:_	entrevista	2024-03-31 12:21:58 ECT	2024-03-31 12:21:58 ECT
125bc70b7295a06a_0			0	003efue durante una «entrevista« de trump con el pre	entrevista	2024-03-24 22:15:29 ECT	2024-03-24 22:15:29 ECT
$UsnJrnl:$J			0	.crdownloadp0<zoom-«entrevista«-rrhh.exe0<zoom-...	entrevista	2024-03-23 22:06:30 ECT	2024-03-23 22:06:30 ECT
13095005cf796f07_0			0	"<p>fue durante una «entrevista« de trump con el pre	entrevista	2024-03-24 21:41:35 ECT	2024-03-24 21:41:35 ECT
Zoom-Entrevista-RRHH.exe:SmartScreen			0	Zoom-«Entrevista«-RRHH.exe:SmartScree	entrevista	2024-03-24 20:57:49 ECT	2024-03-24 21:17:13 ECT
data_1			0	http://10.10.10.136/«entrevista«/domain : 10.10.10	entrevista	2024-03-24 20:47:41 ECT	2024-03-24 20:47:41 ECT
Zoom-Entrevista-RRHH.exe-slack				Zoom-«Entrevista«-RRHH.exe-slac	entrevista	2024-03-24 20:57:49 ECT	2024-03-24 21:17:13 ECT
History			0	test\downloads\zoom-«entrevista«-rrhh.exepath id :	entrevista	2024-03-24 20:57:49 ECT	2024-03-24 20:57:49 ECT
ntuser.dat.LOG2			0	test\downloads\zoom-«entrevista«-rrhh.exemicrosoft	entrevista	2024-03-23 22:14:50 ECT	2024-03-23 22:14:50 ECT
NTUSER.DAT			0	test\downloads\zoom-«entrevista«-rrhh.exemicrosoft	entrevista	2024-03-23 22:15:12 ECT	2024-03-23 22:15:12 ECT
data_1			0	http://10.10.10.136/«entrevista«/zoom-entrevista-rrh	entrevista	2024-03-24 20:47:41 ECT	2024-03-24 20:47:41 ECT
ZOOM-ENTREVISTA-RRHH.EXE-1830A781.pf			0	ZOOM-«ENTREVISTA«-RRHH.EXE-1830A781.p	entrevista	2024-03-24 21:17:24 ECT	2024-03-24 21:17:24 ECT
ZOOM-ENTREVISTA-RRHH.EXE-1830A781.pf			0	program name : zoom-«entrevista«-rrhh.exepath : /u	entrevista	2024-03-24 21:17:24 ECT	2024-03-24 21:17:24 ECT
edb00022.jtx			0	http://10.10.10.136/«entrevista«/1spsindex of /ent	entrevista	2024-03-24 22:18:40 ECT	2024-03-24 22:18:40 ECT
SRUDB.dat			0	test\downloads\zoom-«entrevista«-rrhh.exeusername	entrevista	2024-03-31 12:21:51 ECT	2024-03-31 12:21:51 ECT

Se realiza un filtrado por la IP encontrada y se tiene los diferentes eventos en los que interviene, en donde se tiene un registro en el que se muestra que la IP pertenecía a un servidor Debian.

Figura 92.

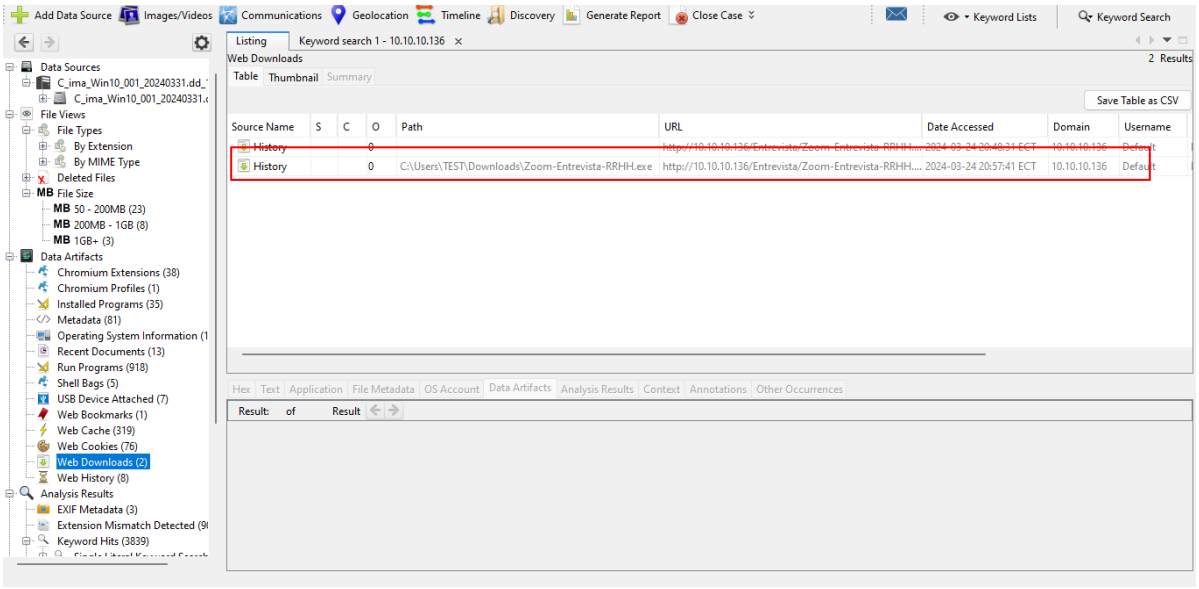
Ip servidor Debian



Al realizar una revisión de las descargas web, se encuentra el archivo que realiza la conexión al servidor Debian 10.10.10.136.

Figura 93.

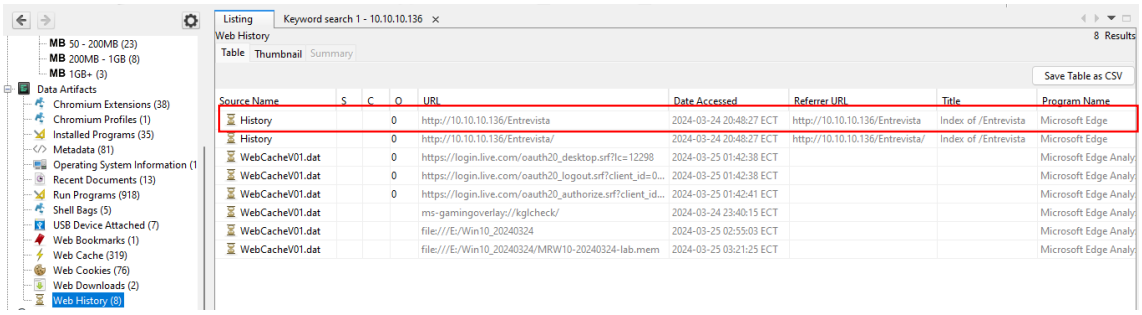
Archivo descargado



Al revisar el historial de navegación se observa que se ha navegado a través de la página 10.10.10.136/Entrevista, de donde se descargó el archivo.

Figura 94.

Historial de navegación



Se encuentra la ruta de la descarga y se accede al archivo descargado, se procede a la extracción.

Figura 95.

Extracción de archivo descargado

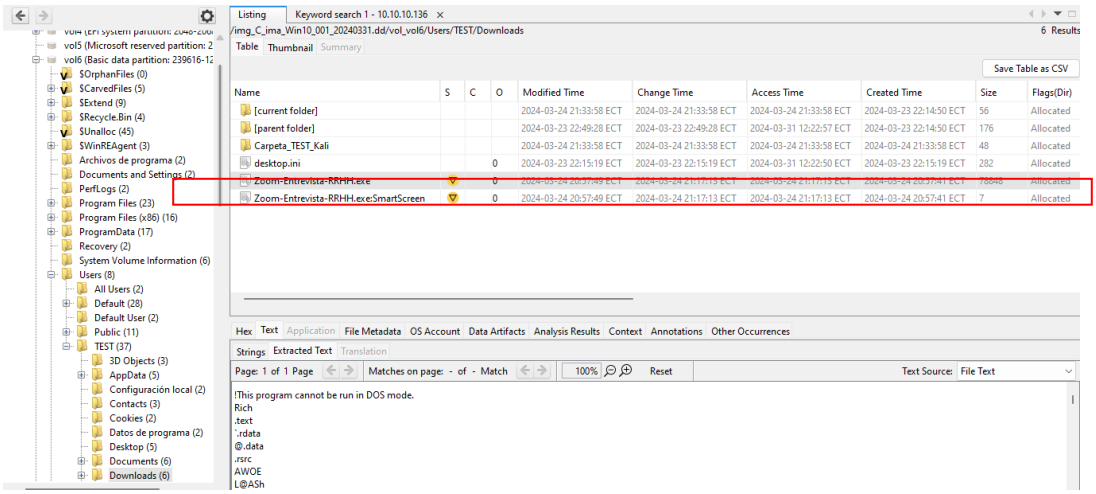
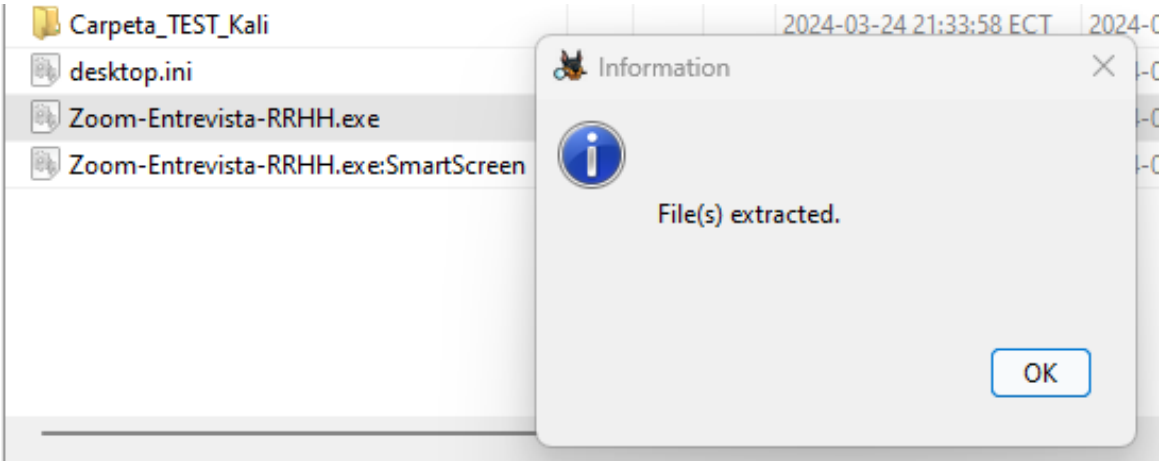


Figura 96.

Archivo extraido



Con el archivo descargado, se realiza un análisis de dicho archivo.

Usando Virus total

Figura 97.

Análisis en VirusTotal

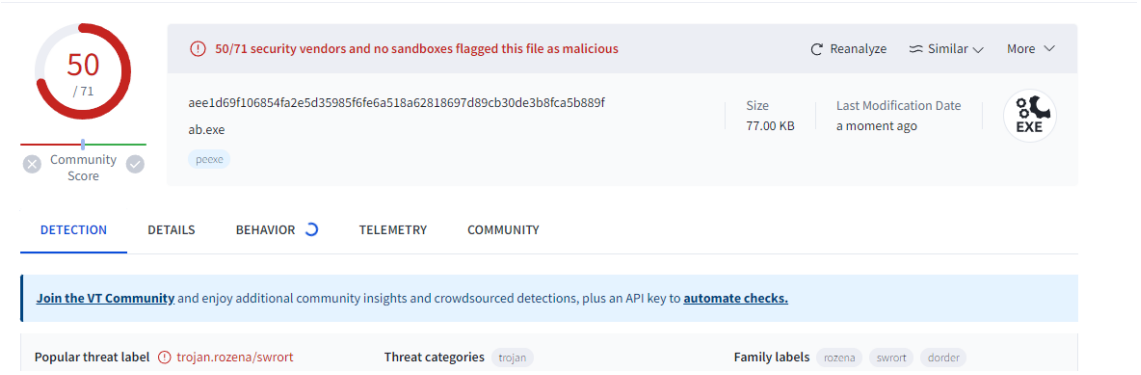
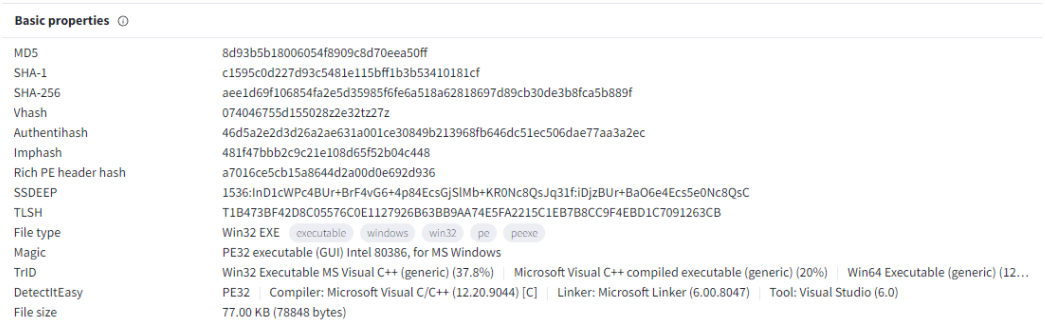


Figura 98.

Información del análisis

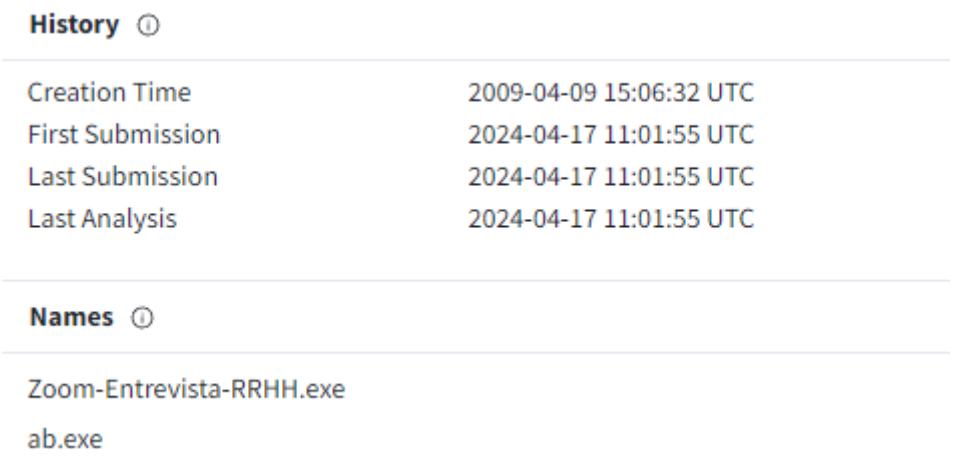


Basic properties

MD5	8d93b5b18006054f8909c8d70eea50ff
SHA-1	c1595c0d227d93c5481e115bff1b3b53410181cf
SHA-256	aee1d69f106854fa2e5d35985f6fe6a518a62818697d89cb30de3b8fca5b889f
Vhash	074046755d155028z2e32tz27z
Authentihash	46d5a2e2d3d26a2ae631a001ce30849b213968fb646dc51ec506dae77aa3a2ec
Imphash	481f47bbb2c9c21e108d65f52b04c448
Rich PE header hash	a7016ce5cb15a8644d2a00d0e692d936
SSDEEP	1536:InD1cWPc4BUr+BrF4vG6+4p84EcsGjSlMb+KR0Nc8QsJq31f:iDjzBUr+BaO6e4Ecs5e0Nc8QsC
TLSH	T1B473BF42D8C05576C0E1127926B63BB9AA74E5FA2215C1EB7B8CC9F4EBD1C7091263CB
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (37.8%) | Microsoft Visual C++ compiled executable (generic) (20%) | Win64 Executable (generic) (12…
DetectItEasy	PE32 | Compiler: Microsoft Visual C/C++ (12.20.9044) [C] | Linker: Microsoft Linker (6.00.8047) | Tool: Visual Studio (6.0)
File size	77.00 KB (78848 bytes)

Figura 99.

Detalles del analisis



History

Creation Time	2009-04-09 15:06:32 UTC
First Submission	2024-04-17 11:01:55 UTC
Last Submission	2024-04-17 11:01:55 UTC
Last Analysis	2024-04-17 11:01:55 UTC

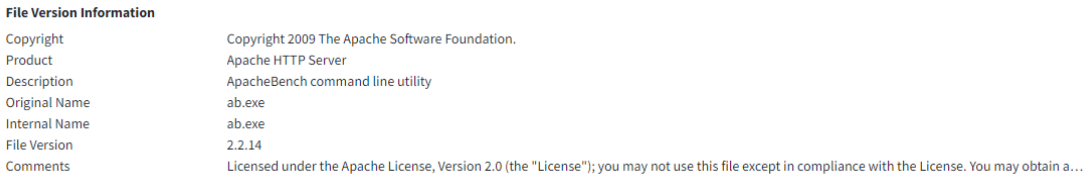
Names

Zoom-Entrevista-RRHH.exe

ab.exe

Figura 100.

Detalles del análisis

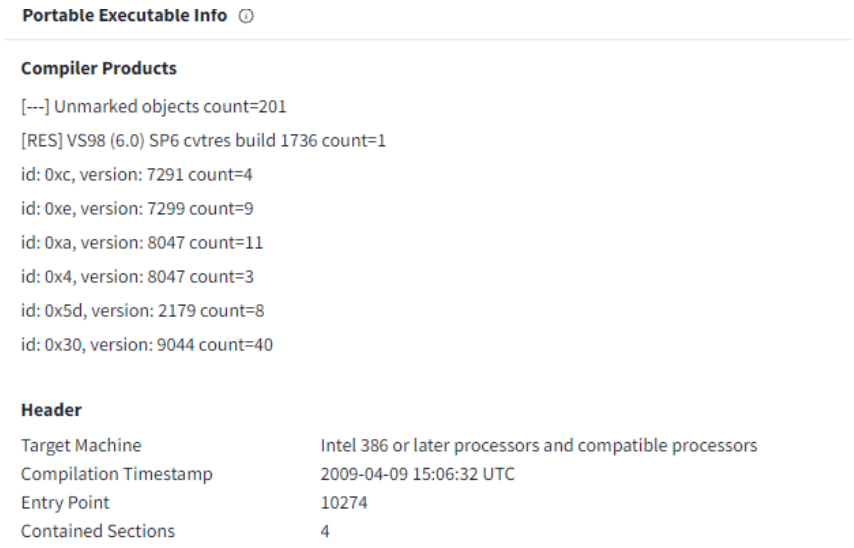


File Version Information

Copyright	Copyright 2009 The Apache Software Foundation.
Product	Apache HTTP Server
Description	ApacheBench command line utility
Original Name	ab.exe
Internal Name	ab.exe
File Version	2.2.14
Comments	Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a…

Figura 101.

Detalles del analisis



Portable Executable Info ⓘ

Compiler Products

[---] Unmarked objects count=201

[RES] VS98 (6.0) SP6 cvtres build 1736 count=1

id: 0xc, version: 7291 count=4

id: 0xe, version: 7299 count=9

id: 0xa, version: 8047 count=11

id: 0x4, version: 8047 count=3

id: 0x5d, version: 2179 count=8

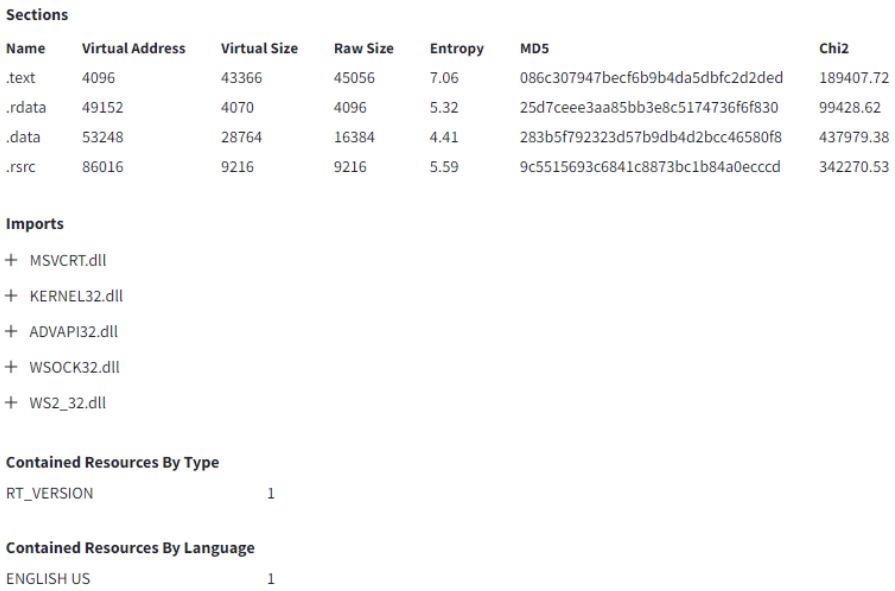
id: 0x30, version: 9044 count=40

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2009-04-09 15:06:32 UTC
Entry Point	10274
Contained Sections	4

Figura 102.

Detalles del analisis



Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	43366	45056	7.06	086c307947becf6b9b4da5dbfc2d2ded	189407.72
.rdata	49152	4070	4096	5.32	25d7ceee3aa85bb3e8c5174736f6f830	99428.62
.data	53248	28764	16384	4.41	283b5f792323d57b9db4d2bcc46580f8	437979.38
.rsrc	86016	9216	9216	5.59	9c5515693c6841c8873bc1b84a0ecccd	342270.53

Imports

+ MSVCRT.dll
+ KERNEL32.dll
+ ADVAPI32.dll
+ WSOCK32.dll
+ WS2_32.dll

Contained Resources By Type

RT_VERSION	1

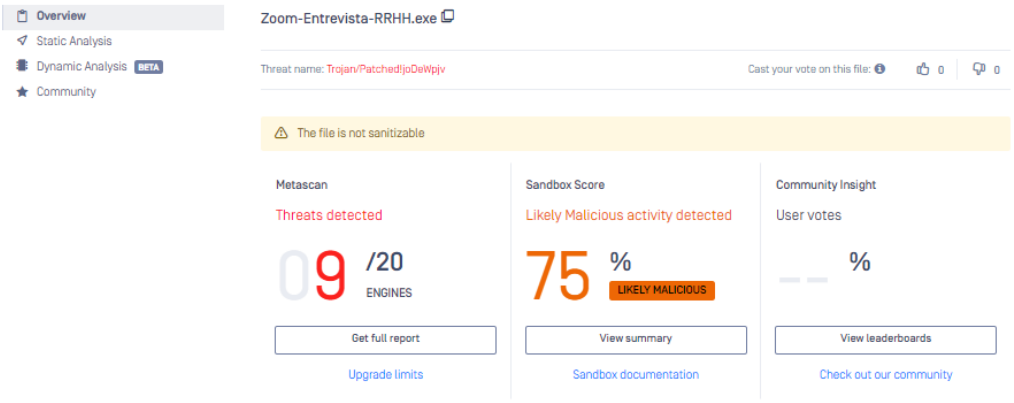
Contained Resources By Language

ENGLISH US	1

Usando Metadefender

Figura 103.

Análisis con Metadefender

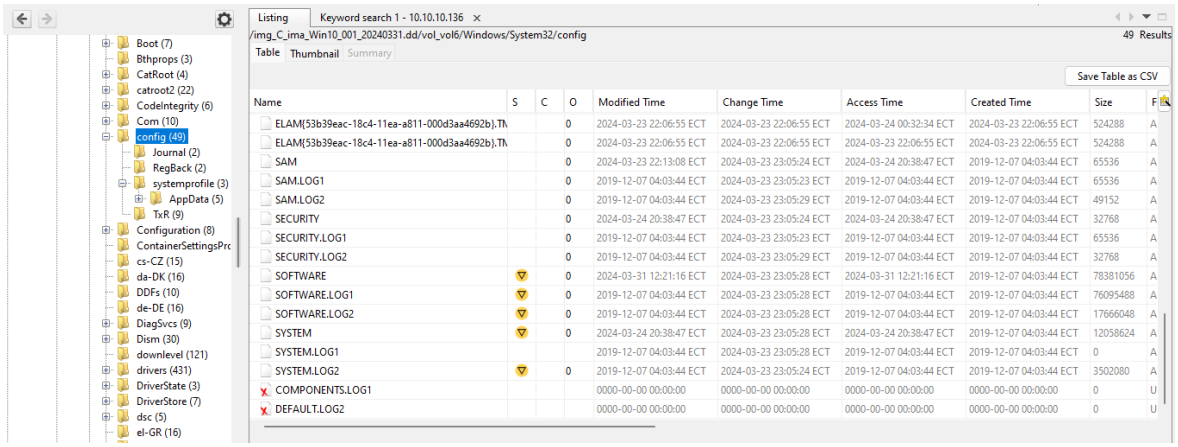


Análisis de Registros

Se procede a la extracción de los registros para el análisis en RegRipper en la ruta **C:\Windows\System32\config –**

Figura 104.

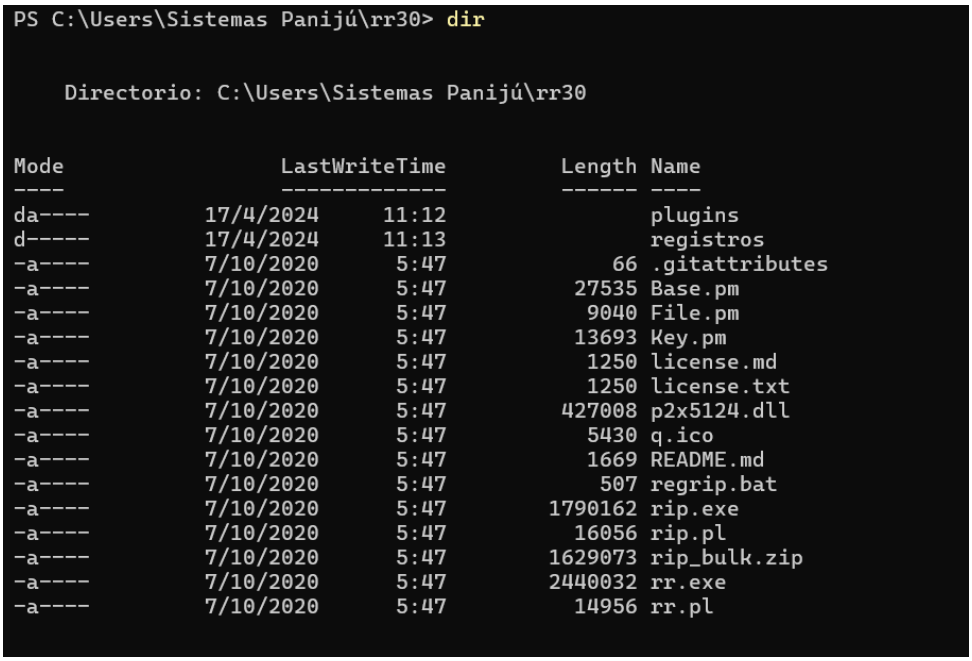
Localización de registros de Windows



Se ubica los registros extraídos desde el PowerShell del equipo con el que estamos trabajando.

Figura 105.

RegRipper



```
PS C:\Users\Sistemas Panijú\rr30> dir


    Directorio: C:\Users\Sistemas Panijú\rr30


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
da----         17/4/2024     11:12                plugins
d-----         17/4/2024     11:13                registros
-a----         7/10/2020      5:47             66 .gitattributes
-a----         7/10/2020      5:47          27535 Base.pm
-a----         7/10/2020      5:47           9040 File.pm
-a----         7/10/2020      5:47          13693 Key.pm
-a----         7/10/2020      5:47           1250 license.md
-a----         7/10/2020      5:47           1250 license.txt
-a----         7/10/2020      5:47         427008 p2x5124.dll
-a----         7/10/2020      5:47           5430 q.ico
-a----         7/10/2020      5:47           1669 README.md
-a----         7/10/2020      5:47            507 regrip.bat
-a----         7/10/2020      5:47        1790162 rip.exe
-a----         7/10/2020      5:47          16056 rip.pl
-a----         7/10/2020      5:47        1629073 rip_bulk.zip
-a----         7/10/2020      5:47        2440032 rr.exe
-a----         7/10/2020      5:47          14956 rr.pl
```

Se verifican los registros extraídos.

Figura 106.

Revisión de registros

```
PS C:\Users\Sistemas Panijú\rr30> dir .\comp\
```

Figura 107.

Registros extraidos

```
    Directorio: C:\Users\Sistemas Panijú\rr30\comp


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         17/4/2024     12:24         524288 BBI
-a----         17/4/2024     12:25          28672 BCD-Template
-a----         17/4/2024     12:25       43253760 COMPONENTS
-a----         17/4/2024     12:25         524288 DEFAULT
-a----         17/4/2024     12:25        4194304 DRIVERS
-a----         17/4/2024     12:25          32768 ELAM
-a----         17/4/2024     12:26          65536 SAM
-a----         17/4/2024     12:26          32768 SECURITY
-a----         17/4/2024     12:26       78381056 SOFTWARE
-a----         17/4/2024     12:26       12058624 SYSTEM
```

Se ejecuta Regripper.

Figura 108.

Ejecución de RegRipper

```
PS C:\Users\Sistemas Panijú\rr30> .\rip.exe --help
Unknown option: -help
Rip v.3.0 - CLI RegRipper tool
Rip [-r Reg hive file] [-f profile] [-p plugin] [options]
Parse Windows Registry files, using either a single module, or a profile.

  -r [hive] .........Registry hive file to parse
  -d ................Check to see if the hive is dirty
  -g ................Guess the hive file type
  -a ................Automatically run hive-specific plugins
  -aT ...............Automatically run hive-specific TLN plugins
  -f [profile].......use the profile
  -p [plugin]........use the plugin
  -l ................list all plugins
  -c ................Output plugin list in CSV format (use with -l)
  -s systemname......system name (TLN support)
  -u username........User name (TLN support)
  -uP ...............Update default profiles
  -h.................Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
    C:\>rip -r c:\case\ntuser.dat -p userassist
    C:\>rip -r c:\case\ntuser.dat -a
    C:\>rip -l -c

All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.

copyright 2020 Quantum Analytics Research, LLC
```

Figura 109.

Pluggins de RegRipper

```
PS C:\Users\Sistemas Panijú\rr30> dir .\plugins\


    Directorio: C:\Users\Sistemas Panijú\rr30\plugins


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         7/10/2020      5:47           3795 adobe.pl
-a----         7/10/2020      5:47             57 all
-a----         7/10/2020      5:47           2451 allowedenum.pl
-a----         7/10/2020      5:47              8 amcache
-a----         7/10/2020      5:47           5920 amcache.pl
-a----         7/10/2020      5:47           5483 amcache_tln.pl
-a----         7/10/2020      5:47           1674 appassoc.pl
-a----         7/10/2020      5:47           2099 appcertdlls.pl
-a----         7/10/2020      5:47          14352 appcompatcache.pl
-a----         7/10/2020      5:47          14166 appcompatcache_tln.pl
-a----         7/10/2020      5:47           6873 appcompatflags.pl
-a----         7/10/2020      5:47           2722 appinitdlls.pl
-a----         7/10/2020      5:47           2225 appkeys.pl
-a----         7/10/2020      5:47           2242 appkeys_tln.pl
-a----         7/10/2020      5:47           2975 applets.pl
-a----         7/10/2020      5:47           2462 applets_tln.pl
-a----         7/10/2020      5:47           2833 apppaths.pl
-a----         7/10/2020      5:47           2477 apppaths_tln.pl
-a----         7/10/2020      5:47           1727 appspecific.pl
-a----         7/10/2020      5:47           2823 appx.pl
-a----         7/10/2020      5:47           2711 appx_tln.pl
-a----         7/10/2020      5:47           3580 arpcache.pl
-a----         7/10/2020      5:47           1666 at.pl
-a----         7/10/2020      5:47           2346 attachmgr.pl
-a----         7/10/2020      5:47           2683 attachmgr_tln.pl
-a----         7/10/2020      5:47           1351 at_tln.pl
-a----         7/10/2020      5:47           2441 audiodev.pl
-a----         7/10/2020      5:47          18964 auditpol.pl
-a----         7/10/2020      5:47           5230 backuprestore.pl
-a----         7/10/2020      5:47           2658 bam.pl
```

Se empieza con el análisis de los registros, en primer lugar, se verifica la versión, con el comando **.\rip.exe -r .\registros\NTUSER.DAT -p winver**; sin embargo, si usamos un plugin que no corresponde al registro, Regripper indicara donde buscar.

Figura 110.

Sugerencias de RegRipper

```
PS C:\Users\dell\rr30> .\rip.exe -r .\registros\NTUSER.DAT -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

Microsoft\Windows NT\CurrentVersion not found.
PS C:\Users\dell\rr30>
```

Al ingresar el comando **.\rip.exe -r .\registros\SOFTWARE -p winver**, se muestra la información.

Figura 111.

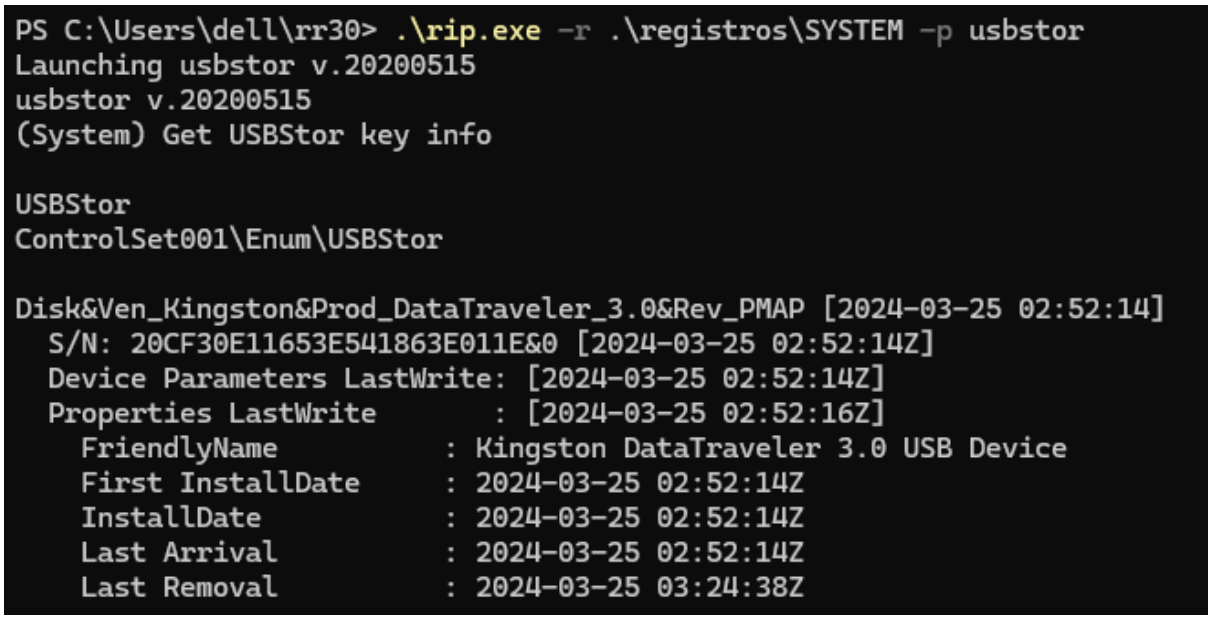
Revisión de versión

```
PS C:\Users\dell\rr30> .\rip.exe -r .\registros\SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName              Windows 10 Pro
ReleaseID                2009
BuildLab                 19041.vb_release.191206-1406
BuildLabEx               19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID     Enterprise
RegisteredOrganization
RegisteredOwner          TEST
InstallDate              2024-03-24 03:08:56Z
InstallTime              2024-03-24 03:08:56Z
PS C:\Users\dell\rr30>
```

Con el comando **.\rip.exe -r .\registros\SYSTEM -p usbstor**, podemos identificar los usb que se han conectado

Figura 112.

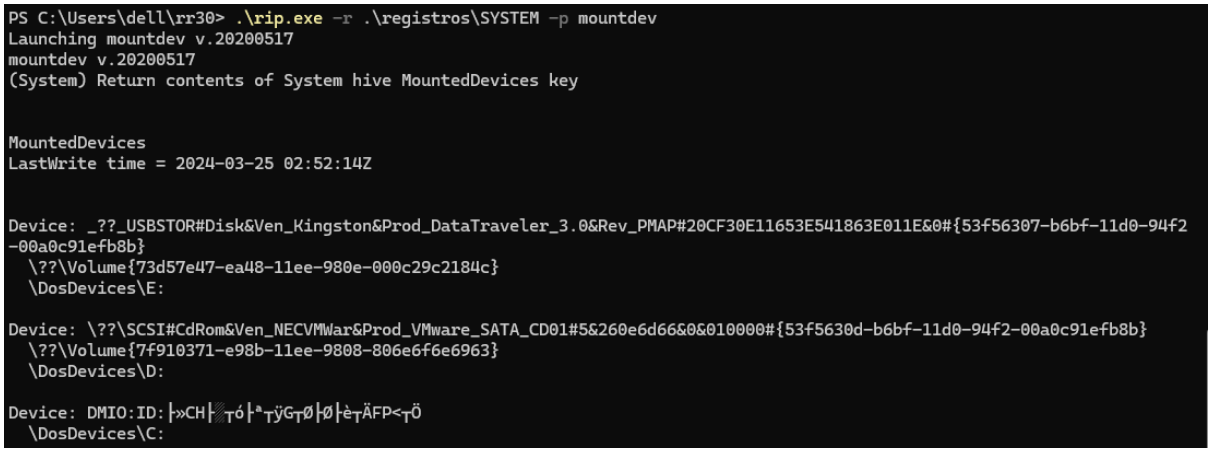
Revisión de USB's conectados



Con el comando **.\rip.exe -r .\registros\SYSTEM -p mountdev**, se pude observar la información de los dispositivos montados y la letra asignada

Figura 113.

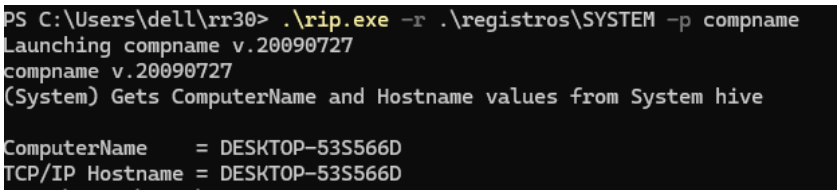
Dispositivos montados



Con el comando **.\rip.exe -r .\registros\SYSTEM -p compname,** averiguamos el nombre del dispositivo.

Figura 114.

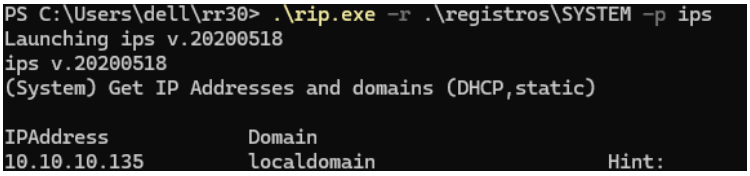
Nombre del dispositivo



Con el comando **.\rip.exe -r .\registros\SYSTEM -p ips**, se verifica que la IP del equipo es la 10.10.10.135.

Figura 115.

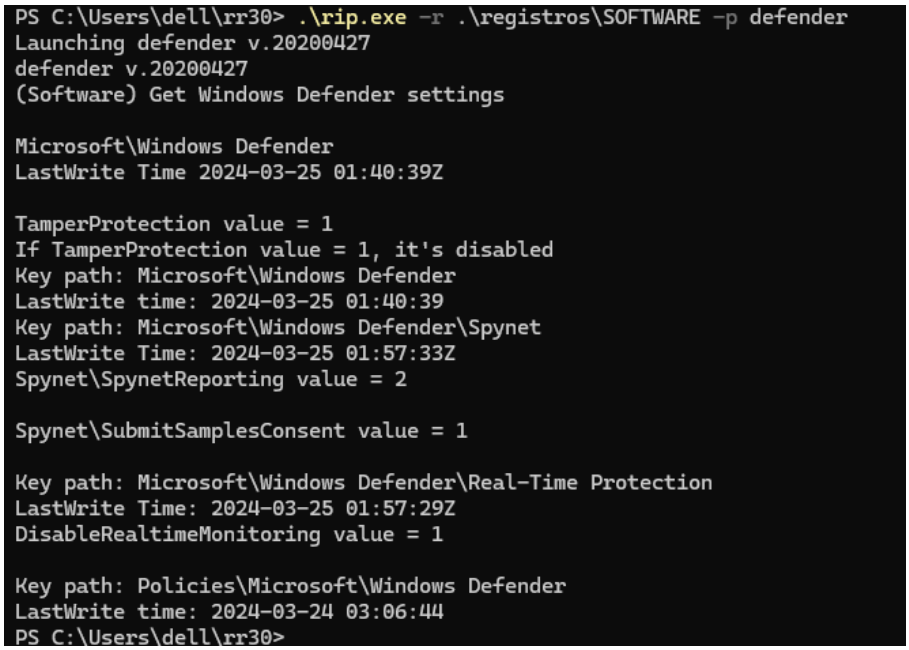
IP del dispositivo



Con el comando .**\rip.exe -r .\registros\SOFTWARE -p defender**, se pude verificar si el antivirus tuvo alguna modificación.

Figura 116.

Modificación de antivirus



Análisis de Resultados

El análisis de los resultados está enfocado en describir los hallazgos obtenidos a lo largo de las etapas de extracción y análisis de las evidencias, utilizando el Framework planteado en el presente proyecto y a través de un enfoque metódico y riguroso, hemos identificado patrones, anomalías y relaciones cruciales que arrojan luz sobre los eventos investigados.

Luego se detallarán las etapas y el análisis de cada caso de uso planteado.

Laboratorio 1

Etapa de Evaluación Preliminar

Esta etapa se caracteriza al tener un escenario de caja gris debido a que si bien es cierto el cliente proporcionó información de lo que sucedía en su computador, pero no tenía un conocimiento técnico motivo por el cual no hubo un mayor detalle desde esa perspectiva, pero una información importante proporcionada de su parte fue que la maquina se encendía y procesaba mucha información hasta iniciar el sistema operativo y se calentaba en este proceso. Previamente a la entrega de las evidencias la computadora fue llevada a un técnico que trató de darle una solución sin éxito.

Etapa de Extracción de Evidencias

En el caso del primer laboratorio la etapa de extracción no fue necesaria porque el cliente proporcionó las imágenes de la memora RAM y del disco, ya que ya no contaba con el equipo físico. La extracción fue realizada por un técnico de soporte técnico al cual llevó el cliente su máquina previamente, esto con la finalidad de poder tener una solución a su situación; ese es el motivo por el cual no se pudo solicitar la fuente de datos.

Etapa de Análisis de Evidencias

El uso del Framework ha permitido llevara cabo una investigación exhaustiva de las evidencias entregadas, en el caso de la memoria RAM se encontró un proceso sospechoso llamado

TempCasaPiscina593-gjp.exe, que tras utilizar todas las herramientas de análisis forense se pudo llegar a determinar que este tenía conexiones con otro equipo de red por el cual se estaba comunicando y probablemente sea el medio de acceso que tenía el atacante para provocar que la maquina tenga comportamientos de sobre procesamiento y lentitud.

Por otro lado, el principal resultado alarmante era la cantidad de permisos que tenía este ejecutable dentro de la máquina del cliente pues podía leer y escribir y modificar sin problema.

Otro hallazgo importante es que este malware no estaba alojado en una sola ubicación tenía punteros que apuntaban a varias ubicaciones de memoria dentro de las carpetas del sistema y del usuario administrador.

Por su comportamiento se puede determinar que era un archivo malicioso tipo mutante que se movía contantemente gracias a sus punteros que eran los que apoyaban en esta labor.

Así mismo la investigación llevó al "EventLog" de Windows el cual permite determinar que era un ejecutable que alojaba entre los procesos de inicio del computador, también se llegó a determinar la principal ubicación: C:\Users\Admin\AppData\Local\TempCasaPiscina593-gjp.exe.

Con esta importante información se procedió a realizar el análisis del disco con la finalidad de tener acceso a las ubicaciones encontradas en el EventLog, pero la evidencia de la disco entregada no correspondía a la memoria, por lo que no se pudo llegar a un resultado concluyente con el malware encontrado.

Laboratorio 2

Etapa de Evaluación Preliminar

En esta etapa, como investigadores debemos obtener la mayor cantidad de información posible sobre los eventos por los que nos solicitaron un análisis forense de un dispositivo.

En el laboratorio 2 las personas que solicitaron el análisis del equipo tenían conocimientos relacionados con informática, por lo que al momento de acceder al equipo nos encontramos

con un equipo que había sido desconectado de la red, sin embargo, lo habían mantenido encendido para poder recabar la mayor cantidad de evidencias.

Por otro lado, es importante mantener un adecuado manejo de la cadena de custodia y documentar que elementos recibimos por parte de los solicitantes para evitar cambios o adulteraciones de los elementos del equipo, y así poder realizar una extracción y un análisis de evidencias con la certeza que corresponden al equipo a analizar.

Etapa de Extracción de Evidencias

Para la extracción de las evidencias es importante tener un dispositivo de almacenamiento de preferencia nuevo y entregado por el cliente, de no tener esta opción, se sugiere hacer una sanitización de un disco con la suficiente capacidad de almacenamiento para la recolección de las evidencias. También es importante hacer uso de guantes de latex para evitar descargas de eléctricas originadas por estática, que puedan causar daños a los elementos del equipo que se va a analizar.

Al saber que no se apagó el equipo, se pudo extraer la información de la memoria RAM, cuya volatibilidad es muy alta, por lo que en este caso la extracción de la imagen de la memoria RAM se la realizó in situ, por eso se explicó la razón de ser de este procedimiento y se brindaron los detalles del desarrollo del mismo.

Haciendo uso de herramientas que nos permiten extraer una imagen forense de la memoria RAM se inició la extracción y almacenamiento de las evidencias.

No se realizó un análisis de tráfico y captura de paquetes de red porque el equipo estaba aislado de la red interna del establecimiento, pero si se puede obtener esta información, reforzaría la información encontrada en la memoria RAM.

En cuanto a la extracción de la imagen forense del disco del equipo, se optó por realizarlo usando los recursos lógicos propios del equipo entregado, sin embargo, hay que tener mucha precaución al realizar las configuraciones de booteo del equipo, de tal manera que nos

aseguremos que va a iniciar con el Sistema Operativo Caine, que contiene la herramienta Guymeyer. En este punto es importante identificar los discos que están involucrados, ya que debemos proteger contra escritura al disco del cual vamos a obtener la información, para que la imagen sea completamente integra.

Etapa de Análisis de Evidencias

Dado que la maquina analizada no fue apagada se pudo extraer una imagen de la memoria RAM que contenían los eventos que hicieron que la maquina sea aislada, la información obtenida fue de vital importancia dentro del análisis ya que se pudo detectar el archivo que desencadeno una vulneración del equipo, el tipo de conexión que mantuvo y los hosts con los cuales se comunicaba, los procesos que mantenida al momento de ser aislado y las rutas desde donde se ejecutaron descargas y conexiones.

Con esta información obtenida, el análisis del disco se facilitó, ya que, en este caso, el análisis se enfocó en reforzar la información antes encontrada. Al encontrar el archivo que genero la conexión, se pudo validar que reputación mantenía tanto en Virus Total como en MetaDefender, los cuales nos detallan que el archivo descargado es un Troyano, creado para establecer una conexión hacia un servidor.

Con la obtención de la imagen forense, se pueden extraer los archivos de los registros de Windows, a través de los cuales se complementa la información ya encontrada anteriormente.

Capítulo V – Conclusiones y Recomendaciones

- La investigación forense tiene como principal propósito identificar, extraer, analizar y presentar la evidencia digital dentro de un contexto de crímenes cibernéticos, el presente Framework permite al investigador contar con un guía estandarizada y probada, que asegure que los procedimientos y herramientas utilizados respetan las normativas para que la evidencia sea aceptada.

- Como investigadores debemos tener un amplio dominio de las herramientas que disponemos para realizar nuestro análisis, ya que dependiendo de la versión del Windows que tenga el equipo a analizar, es posible que debamos utilizar herramientas con diferentes versiones o con interfaz gráfica o por líneas de comando.
- Mantener la cadena de custodia es importante ya que de eso depende el resultado de nuestro análisis, y la correlación de los datos obtenidos al momento de analizar la imagen de la memoria RAM y el disco.
- Durante la extracción de las evidencias, hay que considerar que nuestras acciones no deben alterar el status del equipo, ya que podría anular la investigación, sobre todo si es una investigación dentro de un proceso judicial.

Referencias Bibliográficas

Analuisa Muso, J. D., & Solís Acosta, E. F. (2022). *ANÁLISIS FORENSE INFORMÁTICO DE UN SERVIDOR DE ARCHIVOS INSTITUCIONAL*. Ambato.

Asobanca. (Enero de 2023). *Asobanca*. Obtenido de asobanca.org.ec

Autopsy Digital Forensics. (2024). *Autopsy* . Obtenido de Autopsy User Documentation: https://sleuthkit.org/autopsy/docs/user-docs/4.21.0/

BeHackerPro. (19 de noviembre de 2021). *behacker*. Obtenido de https://behacker.pro: https://behacker.pro/que-es-deft-y-para-qe-sirve/#Que_es_DEFT_Desempolvando_mi_DEFT_Linux_Sistema_Operativo_para_Analisis_Forense_Digital

Block, F. (2023). Windows memory forensics: Identification of (malicious) modifications in memory-mapped image files. *Forensic Science International: Digital Investigation*. doi:https://doi.org/10.1016/j.fsidi.2023.301561.

Cajo, I., Pucuna, S., Cajo, B., Coronado, V., & Orozco, F. (2018). Estudio Comparativo De Las Metodologías De Análisis Forense Informático Para La Examinación De Datos En Medios Digitales. *ESJ*. doi:https://doi.org/10.19044/esj.2018.v14n18p40

Choi, J., Park, J., & Lee, S. (2021). Forensic exploration on windows File History. *Forensic Science International*. doi:https://doi.org/10.1016/j.fsidi.2021.301134

Ciberforensic. (2020). Directrices RFC 3227. *Ciberforensic*. Obtenido de https://www.ciberforensic.com/directrices-rfc-3227

ciberseguridad.com. (s.f.). *ISO/IEC 27037 DIRECTRICES PARA LA IDENTIFICACIÓN, RECOPILACIÓN, ADQUISICIÓN Y PRESERVACIÓN DE EVIDENCIA DIGITAL*. Obtenido de ciberseguridad.com: https://ciberseguridad.com/normativa/espana/iso-iec-27037-evidencia-digital

Cyberpunk. (2024). *pentoo*. Obtenido de https://www.cyberpunk.rs/pentoo-penetration-testing-distro

Daza, S. (Octubre de 2021). *Qué es Volatility y cómo instalarlo. Instalación "No standalone" en Windows 10*. Obtenido de https://behacker.pro/que-es-volatility-y-como-instalarloinstalacion-no-standalone-en-windows-10/#Que_es_Volatility

Duran, I. (03 de 01 de 2024). *Infobae*. Obtenido de Sistema operativo Windows fue el más vulnerable a ataques de malware en 2023: https://www.infobae.com/tecno/2024/01/03/diariamente-circulan-mas-de-400000-archivos-maliciosos-en-computadores-windows-sigue-en-la-mira/

Fernandez, R. (20 de Febrero de 2023). *Statista*. Obtenido de https://es.statista.com/estadisticas/634540/sistemas-operativos-para-pc-cuota-de-mercado-mundial/

GlobátiKa SL. (s.f.). *71506/2013. Metodología para el análisis forense de las evidencias electrónicas*. Obtenido de peritosinformaticos.es: https://peritosinformaticos.es/iso-71506-2013-perito-informatico/

Guidance Software, I. (2005). *La Norma en Análisis Forense Informático.* Obtenido de La Norma en Análisis Forense Informático: https://helling.wordpress.com/wp-content/uploads/2008/01/encaseforensicv6spanish.pdf

IBM. (2024). *¿Qué es VMware?* Obtenido de https://www.ibm.com/mx-es/topics/vmware

International, O. (2002). *ENCASE FORENSIC SOFTWARE: CARACTERÍSTICAS Y FUNCIONES.* Obtenido de ENCASE FORENSIC SOFTWARE: CARACTERÍSTICAS Y FUNCIONES: https://www.ondata.es/recuperar/encase_forensic.htm

KeepCoding, R. (12 de 12 de 2023). *¿Qué es FTK Imager?* Obtenido de ¿Qué es FTK Imager?: https://keepcoding.io/blog/que-es-ftk-imager-y-para-que-sirve/

LORENZO, J. A. (14 de noviembre de 2023). *Redeszone*. Obtenido de https://www.redeszone.net: https://www.redeszone.net/tutoriales/seguridad/mejores-herramientas-gratuitas-informatica-forense/

Martínez, A. (2014). RFC 3227 - Directrices para la recopilación de evidencias y su almacenamiento. *INCIBE- CERT*. Obtenido de https://www.incibe.es/incibe-cert/blog/rfc3227

Medrano, J. L. (09 de 2022). *https://www.bketl.es/.* Obtenido de Despachos BK ETL GLOBAL: https://www.bketl.es/wp-content/uploads/2022/09/Ejemplo-Informe-Pericial.pdf

MEJÍAS, P. C. (2021). ESTUDIO COMPARATIVO DE DISTRIBUCIONES LINUX PARA ANÁLISIS. *ESTUDIO COMPARATIVO DE DISTRIBUCIONES LINUX PARA ANÁLISIS*, 61.

Melian Angel, J. (2023). *Análisis forense de la huella digital de un usuario en sistemas informáticos.* Universitat Politècnica de València.

Mohammed, M. (2023). *Windows Forensics Analyst Field Guide.* Birmingham: Packt Publishing Ltd.

Olmo, F. J. (2020). *Crimen, cibercrimen y analisis forense.*

Ordóñez Bello, B. (2022). Análisis de delitos forenses con AutoPsy. *Universidad de Alcalá. Escuela Politécnica Superior*. Obtenido de http://hdl.handle.net/10017/52510

Rai, S. (2023). *Computer Forensic and digital crime investigation.* Tamil Nadu.

Rubio Alamillo, J. (27 de 11 de 2022). Peritaje Informático forense con Autopsy. Obtenido de https://peritoinformaticocolegiado.es/blog/peritaje-informatico-forense-con-autopsy/

Somos Libres. (18 de 01 de 2024). Tsurugi Linux: Adaptación de la experiencia del usuario a las investigaciones forenses digitales y OSINT. *somoslibres.org*. Obtenido de https://www.somoslibres.org/index.php/16-nieuws/seguridad/12539-tsurugi-linux-adaptacion-de-la-experiencia-del-usuario-a-las-investigaciones-forenses-digitales-y-osint

Tsurugi. (2024). documentation_tsurugi_linux. *tsurugi-linux.org*. Obtenido de https://tsurugi-linux.org/documentation_tsurugi_linux_1.php#

Volatility Fundation. (2024). *Volatility*. Obtenido de https://volatilityfoundation.org/