VALIDACIÓN DE PROCESO PARA LA CREACIÓN DE PERFILES EN VOLATILITY2.6 PARA EL ANÁLISIS DE MEMORIA VOLÁTIL EN SISTEMAS OPERATIVOS LINUX DEBIAN Y UBUNTU QUE PUEDAN APOYAR EN UNA INVESTIGACIÓN FORENSE O EN UNA RESPUESTA A INCIDENTES.

HECTOR ALBERTO DUSSAN MONTOYA

MIGUEL ANGEL PACHECO ALFONSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2025

VALIDACIÓN DE PROCESO PARA LA CREACIÓN DE PERFILES EN VOLATILITY2.6 PARA EL ANÁLISIS DE MEMORIA VOLÁTIL EN SISTEMAS OPERATIVOS LINUX DEBIAN Y UBUNTU QUE PUEDAN APOYAR EN UNA INVESTIGACIÓN FORENSE O EN UNA RESPUESTA A INCIDENTES.

HECTOR ALBERTO DUSSAN MONTOYA

MIGUEL ANGEL PACHECO ALFONSO

Proyecto de Grado – Monografía presentado para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMATICA

ALEXANDER LARRAHONDO

DOCENTE MEDIO TIEMP - CEAD JOSE ACEVEDO Y GOMEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2025

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., 2025

DEDICATORIA

Dedicado primero a Dios y a mi pareja Sandra Piña, que ha sido mi motor y mi apoyo teniendo paciencia en las largas jornadas de aprendizaje, a mi mama María Alfonso, a mi papa Jeremías Pacheco, a mis hermanos Carlos Pacheco, Jorge Pacheco, y Jaison Pacheco, así como a toda mi familia y mis acompañamientos permanentes tanto perruna (minis) como gatuna (Hydra, Eve, Pochita, Ryu, Valiente y Queen) y el apoyo directo en la presente carrera y trabajo de grado mi estimado amigo Hector Alberto Dussan Montoya.

Primero que nada, quiero agradecer a Dios por darme la oportunidad de cursar esta Especialización y la salud para llevarla a cabo. A mi madre, Alba Montoya, por soportar mi ausencia durante este proceso. A mis hermanos, por apoyarme y ayudarme en cada momento de zozobra e incertidumbre en la realización de mis actividades estudiantiles. A mi amigo, Miguel Ángel Pacheco Alonso, por estar siempre dispuesto a explicarme de la mejor manera y cuantas veces fuera necesario las actividades que nos asignaron día a día. A mi hermano, Nelson Fernando Arévalo Suárez, por brindar consejos, apoyo y palabras de ánimo cuando sentía pereza de realizar mis actividades. A mi perro, Ozymandias, por acompañarme en los momentos de soledad mientras trabajaba. Y finalmente, a mis compañeros de trabajo, por ayudarme a entender y fortalecer los conceptos que no comprendía.

AGRADECIMIENTOS

Agradecimientos primero a Dios y a mi pareja Sandra Piña, que ha sido mi motor y mi apoyo teniendo paciencia en las largas jornadas de aprendizaje, a mi mama María Alfonso, a mi papa Jeremías Pacheco, a mis hermanos Carlos Pacheco, Jorge Pacheco, y Jaison Pacheco, así como a toda mi familia y mis acompañamientos permanentes tanto perruna (minis) como gatuna (Hydra, Eve, Pochita, Ryu, Valiente y Queen) y el apoyo directo en la presente carrera y trabajo de grado mi estimado amigo Hector Dussan.

Primero que nada, quiero agradecer a Dios por darme la oportunidad de cursar esta Especialización y la salud para llevarla a cabo. A mi madre, Alba Montoya, por soportar mi ausencia durante este proceso. A mis hermanos, por apoyarme y ayudarme en cada momento de zozobra e incertidumbre en la realización de mis actividades estudiantiles. A mi amigo, Miguel Ángel Pacheco Alonso, por estar siempre dispuesto a explicarme de la mejor manera y cuantas veces fuera necesario las actividades que nos asignaron día a día. A mi hermano, Nelson Fernando Arévalo Suárez, por brindar consejos, apoyo y palabras de ánimo cuando sentía pereza de realizar mis actividades. A mi perro, Ozymandias, por acompañarme en los momentos de soledad mientras trabajaba. Y finalmente, a mis compañeros de trabajo, por ayudarme a entender y fortalecer los conceptos que no comprendía.

CONTENIDO

TABLA DE FIGURAS

pág

GLOSARIO

ANÁLISIS DE MALWARE: Aplicación y ejecución de métodos y procesos especializados o probados científicamente para la conservación, recolección, validación, identificación, análisis, interpretación, documentación y presentación de evidencia obtenida a partir de un software malicioso, con el objetivo de identificar la naturaleza y actuar de la amenaza.

ARTEFACTO: RELACIONADO a un archivo u objeto involucrado en un incidente de Ciberseguridad en una red o sistema, o que el mismo fuese utilizado para evadir los controles y medidas de seguridad, por lo que cuando se identifica un artefacto malicioso requiere ser informado, tratado y eliminado de los sistemas afectados.

CIBER INCIDENTE: Aquellas acciones o eventos a través del uso de redes o infraestructura que resulta en afectaciones adversas, no deseadas o que indispongan los sistemas o la información allí administrada.

INTEGRIDAD: Principio de la seguridad que garantiza que los datos solo puedan ser alterados por el personal autorizado, asegurando que estos sean íntegros en todo momento desde su inicio hasta su fin.

MALICIOSO: Programas o aplicaciones de software los cuales están diseñados para alterar o indisponer un sistema de información, estos pueden ser utilizados por actores cibercriminales para realizar sus actividades delictivas.

PERFIL VOLATILITY: Para que la aplicación pueda reconocer un volcado de memoria debe tener de manera previa un mapeo de la configuración a bajo nivel con la que cuenta determinado sistema operativo, de lo contrario las búsquedas avanzadas en un volcado de memoria no podrá ser efectivo.

PROCESO: Conjunto de actividades diseñadas para lograr un objetivo especificó, un proceso puede contener múltiples entradas y tener una salida definida dependiendo del resultado esperado en lo indicado en el proceso en cuestión.

RIESGO: Posibilidad o probabilidad de que ocurra un evento o situación que pueda tener cierto impacto no esperado o malicioso para la organización o infraestructura, causando posibles afectaciones a la operación normal.

TRIAGE: De un universo de información se extrae únicamente la información requerida o relevante para el proceso a realizar, enfocado las actividades únicamente en un sector de información especifico.

VOLCADO DE MEMORIA: Proceso mediante el cual se toma una copia de la memoria volátil o memoria RAM del estado actual en ese momento de la máquina para su posterior análisis.

RESUMEN

De acuerdo con el entorno actual de la Ciberseguridad, se deben tener claros mecanismos que permitan afrontar de una manera adecuada las nuevas amenazas y el cibercrimen, mediante mecanismos investigativos que permitan dar una respuesta rápida a los incidentes durante las investigaciones forenses o de respuesta a incidentes. Es por esto que se debe tener claro la importancia de realizar el análisis de la memoria volátil de manera efectiva, utilizando herramientas confiables y especializadas que permitan extraer la mayor cantidad de información relevante asociada al incidente, siendo para este caso la mejor Volatility, sin embargo, esta herramienta funciona mediante el uso de perfiles que para el caso de Linux deben ser generados manualmente en su mayoría, por lo cual, el presente documento se enfoca en dar respuesta de manera detallada a como se deben generar dichos perfiles que permitan el uso de Volatility para el análisis de memoria volátil.

PALABRAS CLAVÉ: VOLATILITY, CIBERSEGURIDAD. FORENSE, RESPUESTA A INCIDENTES.

ABSTRACT

In accordance with the current Cybersecurity environment, there must be clear mechanisms that allow us to adequately address new threats and cybercrime, through investigative mechanisms that allow for a rapid response to incidents during forensic investigations or incident response. This is why the importance of carrying out the analysis of volatile memory effectively, using reliable and specialized tools that allow extracting the greatest amount of relevant information associated with the incident, being in this case the best Volatility, however, must be clear. , this tool works through the use of profiles that, in the case of Linux, must be generated manually for the most part, therefore, this document focuses on providing a detailed answer to how these profiles that allow the use of Volatility for volatile memory analysis.

KEYWORDS: VOLATILITY, CYBERSECURITY. FORENSIC, INCIDENT RESPONSE.

1 INTRODUCCIÓN

La era digital actual ha desencadenado una creciente sofisticación de ciber amenazas y esto de la mano con el aumento del uso de sistemas operativos basados en Linux en los entornos empresariales, transformo a la ciberseguridad en un pilar fundamental para la protección de organizaciones y sus activos. La distribución de malware y la constante evolución de la cibercriminalidad exigen un enfoque más amplio de la ciberseguridad, que no se limite a aspectos técnicos, sino que aborde cada faceta de una organización y como esta puede responder a estas amenazas de una manera más eficaz mediante las investigaciones de datos volátiles.

En el año 2022, se registraron 121,6 millones de nuevas muestras de malware asociadas a sistemas Linux, subrayando la necesidad imperante de fortalecer las estrategias de ciberseguridad, Monzón[1]. La ciberseguridad ya no se trata solo de prevenir ataques, sino de estar preparado para responder eficazmente a incidentes y llevar a cabo investigaciones forenses exhaustivas que permitan identificar, contener y mitigar las amenazas. Esta capacidad de respuesta es esencial para reducir el impacto de los incidentes y prevenir futuros ataques, Sánchez, F[2].

La respuesta a incidentes y la informática forense, si bien son diferentes en sus enfoques, comparten un elemento fundamental: la investigación. Ambos procesos se basan en la recolección y análisis de evidencia digital para asegurar la protección

[1] Monzón, T. (2021). CYBER SECURITY MAGAZINE. [En línea]. Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internet https://csecmagazine.com/2020/12/31/convercienciaguatemala/

[2] Sánchez F. (2021). La importancia de la informática forense como un eslabón en el proceso de ciberseguridad. [En línea]. INCIBE Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internethttps://incibe.gt/wp-content/uploads/2021/09/Revista-Digital-Cybersecurity-Vol5.pdf#page=12

de los activos de la organización Sánchez, F[3]. Esta evidencia se puede encontrar en diversas fuentes, desde sistemas de seguridad perimetral hasta registros de aplicaciones y sistemas.

La información recopilada se divide en dos categorías: información no volátil y memoria volátil. La información no volátil se almacena de forma permanente, mientras que la memoria volátil es transitoria y se pierde cuando el dispositivo se apaga o se sobrescribe. Sin embargo, la memoria volátil puede contener información crítica, como procesos en ejecución, registros de aplicaciones, conexiones y actividad del atacante Villinger, S.[4]; Gómez M[5].

Para recolectar y analizar la memoria RAM, existen varias herramientas, como FTK Imager, DumpIt, Axiom Magnet Forensic y comandos en Linux. Sin embargo, el análisis de memoria volátil en sistemas basados en Linux presenta desafíos específicos. A diferencia de los sistemas Windows, que son más homogéneos, Linux tiene una amplia variedad de distribuciones y versiones, lo que dificulta la creación de perfiles de análisis.

En este contexto, la investigación se centra en responder a la pregunta: ¿Cómo se pueden crear perfiles de sistemas operativos basados en Linux, como DEBIAN y Ubuntu, para llevar a cabo análisis de memoria volátil (Memoria RAM) con la herramienta "Volatility" en el contexto de investigaciones forenses o respuestas a incidentes?

---

[3] Sánchez F. (2021). La importancia de la informática forense como un eslabón en el proceso de ciberseguridad. [En línea]. INCIBE Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internethttps://incibe.gt/wp-content/uploads/2021/09/Revista-Digital-Cybersecurity-Vol5.pdf#page=12

[4] Villinger, S. (2019). ¿Qué es la memoria RAM en un ordenador? AVAST. [En línea]. AVAST. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.avast.com/es-es/c-what-is-ram-memory.

[5] Gómez M. (2020). La importancia de la memoria RAM en un análisis forense. [En línea]. Red Seguridad. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.redseguridad.com/especialidades-tic/activos-de-informacion/la-importancia-de-la-memoria-ram-en-un-analisis-forense_20201030.html

La importancia de esta investigación radica en la creciente necesidad de profesionales de ciberseguridad altamente capacitados y en la creciente amenaza de ciberataques en sistemas Linux, que representan una parte significativa del mercado. La falta de candidatos calificados y la creciente incidencia de ataques subrayan la necesidad de contar con herramientas y metodologías efectivas para abordar incidentes cibernéticos en sistemas Linux.

2 DEFINICIÓN DEL PROBLEMA.

2.1 ANTECEDENTES DEL PROBLEMA.

Teniendo en cuenta que para el 2022 se identificaron 121,6 millones de muestras de malware; nuevas asociadas a sistemas operativos basados en Linux y a nuevas amenazas que se afrontan gracias a la Cibercriminalidad se hace necesario pensar en la Ciberseguridad, no solo como el aseguramiento técnico, si no que este tiene que ser pensado de manera general en cada ámbito de la organización, Monzón[6], bajo estrategias y marcos que apliquen capas de seguridad que permitan a su vez hacer frente a cualquier amenaza, lograr tener las herramientas necesarias en caso de un incidente y poder realizar identificar y contener a un atacante, realizando un proceso efectivo de una respuesta a incidentes o de informática forense logrando disminuir impactos y la probabilidad incidentes futuros Sánchez, F[7].

Ahora bien, si la respuesta a incidentes es diferente a la informática forense, ya que una se basa en la respuesta integral del incidente Sánchez F[8], y la otra en investigar a profundidad mediante procesos técnicos para identificar, preservar, recolectar, y analizar la información con resultados aceptables en un procedimiento o litigio legal (Alamillo, 2022), ambos comparten una similitud considerable y tienen su factor

[6] Monzón, T. (2021). CYBER SECURITY MAGAZINE. [En línea]. Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internet https://csecmagazine.com/2020/12/31/convercienciaguatemala/

[7] Sánchez F. (2021). La importancia de la informática forense como un eslabón en el proceso de ciberseguridad. [En línea]. INCIBE Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internethttps://incibe.gt/wp-content/uploads/2021/09/Revista-Digital-Cybersecurity-Vol5.pdf#page=12

[8] Sánchez F. (2021). La importancia de la informática forense como un eslabón en el proceso de ciberseguridad. [En línea]. INCIBE Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internethttps://incibe.gt/wp-content/uploads/2021/09/Revista-Digital-Cybersecurity-Vol5.pdf#page=12

investigativo, vital para que la Ciberseguridad pueda cumplir el trabajo de proteger, responder y mitigar los activos de la organización Sánchez F[9].

Continuando, ese factor investigativo presente en la informática forense y en la respuesta a incidentes, tiene actividades que podrían segmentarse en fases en las que podemos encontrar las fuentes de evidencia que quieren analizarse, que para efectos prácticos puede ser cualquier sistema con información como sistemas de seguridad perimetral que van desde firewall hasta las bitácoras de los sistemas López M[10], entre esta información encontramos la información no volátil, la que se almacena permanentemente y la memoria volátil, que es la que se almacena en el espacio Ordoñez J[11].

En este sentido, la información no volátil es aquella que permite almacenar registros al interior del sistema de forma secuencial y permanente, a diferencia de la memoria volátil, que almacena datos temporales en una sesión actual del usuario, esta última puede alojar información altamente relevante, como procesos en ejecución, registros de aplicaciones legítimas o maliciosas, puertos abiertos, conexiones activas, ejecutables, archivos temporales recientemente abiertos o eliminados, e incluso, dependiendo del caso, rastros de actividad del atacante, a ejecución de procesos, scripts o sentencias, entre otros, que únicamente registran en la memoria volátil, esta información contenida en dicha memoria volátil puede resultar crucial al

[9] Sánchez F. (2021). La importancia de la informática forense como un eslabón en el proceso de ciberseguridad. [En línea]. INCIBE Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internethttps://incibe.gt/wp-content/uploads/2021/09/Revista-Digital-Cybersecurity-Vol5.pdf#page=12

[10] López, M. (2007). Análisis forense digital. Hackers & Seguridad. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

[11] Ordoñez J. (2019). Entorno de análisis de memoria volátil para estudiantes. [En línea]. Universidad de Málaga. [Citado 24-Noviembre-2024]. Disponible en Internet https://riuma.uma.es/xmlui/handle/10630/18711

momento de identificar indicadores de compromiso con los cuales es posible contener y/o bloquear a un atacante Villinger, S.[12]; Gómez M[13].

Así mismo, para poder recolectar esta memoria RAM se cuenta con múltiples herramientas que pueden ser utilizadas tales como FTK Imager, Dumplt Gómez, H.[14], Axiom Magnet Forensic, comandos en Linux, así como también, herramientas OPENSOURCE como AVML (Adquirir memoria volátil para Linux) o Linpmem, entre otros.

Pero, si hablamos del análisis a estas memorias volátiles se evidencia que no existen muchas opciones reales para realizar este tipo de análisis tan especializados, y la aplicación más conocida y con mayor trayectoria en este campo en “Volatility” la cual, es un proyecto que se diseñó para ejecutarse en sistemas basados en Linux desde el 2007, siendo este pionero en la materia para el análisis de memoria volátil que hasta ese momento solo estaba enfocada en los datos no volátiles por no contar con herramientas específicas para facilitar esta labor de análisis en la data volátil Gómez M[15].

Para realizar procesos de análisis forense es necesario generar un “Profile”. Este cuenta con una estructura que permite al sistema almacenar sus sectores de

---

[12] Villinger, S. (2019). ¿Qué es la memoria RAM en un ordenador? AVAST. [En línea]. AVAST. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.avast.com/es-es/c-what-is-ram-memory.

[13] Gómez M. (2020). La importancia de la memoria RAM en un análisis forense. [En línea]. Red Seguridad. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.redseguridad.com/especialidades-tic/activos-de-informacion/la-importancia-de-la-memoria-ram-en-un-analisis-forense_20201030.html

[14] Gómez M. (2020). La importancia de la memoria RAM en un análisis forense. [En línea]. Red Seguridad. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.redseguridad.com/especialidades-tic/activos-de-informacion/la-importancia-de-la-memoria-ram-en-un-analisis-forense_20201030.html

[15] Gómez M. (2020). La importancia de la memoria RAM en un análisis forense. [En línea]. Red Seguridad. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.redseguridad.com/especialidades-tic/activos-de-informacion/la-importancia-de-la-memoria-ram-en-un-analisis-forense_20201030.html

memoria en la información volátil Gómez M[16]. Dicho “Profile” varían de acuerdo con las diferentes versiones de cada sistema operativo. Por ello realizar análisis en sistemas operativos basados en Windows representan una tarea mucho más sencilla. Esto se debe a que Windows es el sistema operativo más comercial, y cuenta con el mayor porcentaje de cuota en el mercado. Es más estable y tiene un número más reducido de versiones en comparación con otros sistemas.

Así mismo, podemos observar que, los sistemas basados en Linux, en su mayoría cuenta con cientos de versiones de cada una de sus distribuciones. Además, al ser libre o de código abierto puede tener más versiones desarrolladas por la comunidad, lo que hace realmente difícil que se pueden encontrar “Profiles”, diseñados para los sistemas operativos basados en Linux y por el contrario, la facilidad de encontrar “Profiles”, para cada una de las versiones de Windows.

2.2 FORMULACIÓN DEL PROBLEMA

Por último, la generación de estos “Profiles”, cuentan con un procedimiento que puede no ser efectivo a la hora de ejecutarlo en ambientes Linux reales lo que nos lleva a la pregunta que trata de resolver la presente investigación, ¿Cómo se pueden crear perfiles de sistemas operativos basados en Linux, como DEBIAN y Ubuntu, para llevar a cabo análisis de memoria volátil (Memoria RAM) con la herramienta "Volatility" en el contexto de investigaciones forenses o respuestas a incidentes?

[16] Gómez M. (2020). La importancia de la memoria RAM en un análisis forense. [En línea]. Red Seguridad. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.redseguridad.com/especialidades-tic/activos-de-informacion/la-importancia-de-la-memoria-ram-en-un-analisis-forense_20201030.html

3 JUSTIFICACIÓN

Los Ciberataques se han vuelto cada vez más comunes en nuestro día a día y tomaron una relevancia y notoriedad sin precedentes a razón principalmente de la pandemia y la virtualidad, lo que dio visibilidad a la necesidad de contar con una ciberseguridad fuerte y dejo en evidencia las muchas falencias, entre ellas la falta de profesionales que existen con dichos conocimientos y habilidades específicos, estos últimos están aumentando el déficit día tras día, tanto es así que según lo indicado por la OEA (Organización de los estados americanos)[17] en su reporte "Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades", la falta de candidatos para cubrir vacantes de ciberseguridad para el año 2021 fue de 8% mientras que para el 2022 fue de más del 25% . Así mismo, en lo mencionado por dicho artículo según ISACA ("Information Systems Audit and Control Association") se evidencio que las empresas presentaron un comportamiento de aumento de ciberataques de hasta un 62% del 2018 al 2022.

De la misma manera según datos extraídos de Kaspersky, mencionan que al menos el 80% de las empresas han experimentado algún ataque de Ransomware Kaspersky[18], y según SOPHOS[19] en al menos 76% de todos los casos se logró cifrar

[17] OEA. (2023). Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades. [En línea]. OAS. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf

[18] Kaspersky. (2023). Principales amenazas de ciberseguridad para empresas: cómo protegerse de ellas. Kaspersky. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://latam.kaspersky.com/resource-center/preemptive-safety/website-security-is-your-business-at-risk

[19] Sophos Iberia. (2023). El 76% de los ataques de ransomware en 2022 implicaron cifrado de datos, el nivel más alto de los últimos cuatro años. [En línea]. Sophos News. [Citado 24-Noviembre-2024]. Disponible en Internet https://news.sophos.com/es-es/2023/05/12/el-76-de-los-ataques-de-

con éxito los datos, siendo las razones más comunes de ataques una explotación de vulnerabilidades (36%), seguida de credenciales comprometidas (29%).

Así mismo, gracias a la importancia que ha tomado la tecnología y el uso de medios digitales se evidenció que en el 2022 de todos los correos enviados a nivel mundial el 48,63% de los correos electrónicos fueron de spam, y el 29,82% de estos tienen como origen Rusia, según datos analizados por Kaspersky Kulikova, Tatyana; Dedenok, Roman; Svistunova, Olga; Kovtun, Andrey; Shimko, Irina[20].

Por otra parte, el sistema operativo más dominante es Windows con un 75,44% de la cuota del mercado mundial y Linux solo cuenta con aproximadamente el 2,55% de este Stadista[21], este último es ampliamente reconocido y utilizado en las Compañías y entidades gubernamentales como Google, la NASA, el CERN, la bolsa de valores de los Estados Unidos, y de manera local en Colombia según Jorge Peláez, Diario la república, indicó en su publicación que de las 1.000 empresas más grandes que hay registradas en Colombia para el 2018, 995 de ellas usan el sistema operativo Red Hat Peláez, J[22]. Esto concuerda con la estadística compartida por w3

---

ransomware-en-2022-implicaron-cifrado-de-datos-el-nivel-mas-alto-de-los-ultimos-cuatro-anos/#:~:text=a%C3%B1os%20%E2%80%93%20Sophos%20News-,El%2076%25%20de%20los%20ataques%20de%20ransomware%20en%202022%20implicaron,los%20costes%20de%20recuperaci%C3%B3n%20totales.

[20] Kulikova, T; Dedenok, R; Svistunova, O; Kovtun, A; Shimko, I. (2023). El spam y el phishing en 2022. [En línea]. Secure List By Kaspersky. [Citado 24-Noviembre-2024]. Disponible en Internet https://securelist.lat/spam-phishing-scam-report-2022/97582/#:~:text=En%202022%2C%20nuestras%20soluciones%20frustraron,robar%20cuentas%20de%20Telegram%20messenger.

[21] Stadista. (2023). Cuota de mercado mundial de los sistemas operativos para ordenadores de sobremesa de 2010 a 2022. [En línea]. Stadista. [Citado 24-Noviembre-2024]. Disponible en Internethttps://es.statista.com/estadisticas/634540/sistemas-operativos-para-pc-cuota-de-mercado-mundial/

[22] Peláez, H. (2018). “De las 1.000 grandes empresas que hay en el país, 995 usa la tecnología de Red Hat”. [En línea]. La república. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.larepublica.co/empresas/de-las-1-000-grandes-empresas-que-hay-en-el-pais-995-usa-la-tecnologia-de-red-hat-2808854#:~:text=Tecnolog%C3%ADa-,%E2%80%9CDe%20las%201.000%20grandes%20empresas%20que%20hay%20en%20el%20pa%C3%ADs,la%20tecnolog%C3%ADa%20de%20Red%20Hat%E2%80%9D&text=Blockchain%20es%20el%20proyecto%20m%C3%A1s,en%20d%C3%ADa%20en%20Open%20Source.&text=Uno%20de%20los%20mayores%20avances,mayores%20jugadores%20es%20Red%20Hat.

“ransomware techs.com” donde se evidenció que cerca del 75% de los servicios web utilizan un sistema operativo basado en Linux DataScientest[23].

Lo anterior, es importante porque si bien el sistema operativo Windows tiene la mayor cuota del mercado y cantidad de detecciones de malware nuevo identificado año tras año, Linux ocupa el segundo lugar como el sistema operativo que más detecciones de malware nuevo a registrado ya que para el año 2022 alcanzó una cifra histórica, identificando 121,6 millones de muestras de malware nuevas, lo que representó un aumento del 117% en comparación a los años anteriores, siendo esta la identificación de malware más grande que se ha registrado desde el 2008 (Jack Germain[24], por lo que se deja en claro que Linux es un sistema operativo que también es vulnerable al malware y puede verse involucrado en incidentes de ciberseguridad al interior de las organizaciones.

Así mismo, la adopción de Linux en servidores, especialmente en entornos de nube, ha superado significativamente a Windows, consolidándose como la plataforma preferida para servicios web, contenedores Docker y virtualización bare-metal. De igual manera, según un informe de Mordor Intelligence, el mercado global de sistemas operativos para servidores alcanzó un valor de 19,07 mil millones de dólares, con una proyección de crecimiento a 30,69 mil millones, lo que representa cerca del 62,7% de la cuota de servidores, impulsado en gran medida por la preferencia hacia soluciones basadas en Linux debido a su flexibilidad, seguridad y rentabilidad Mordor Intelligence[25]. Además, la naturaleza de código abierto de Linux

---

[23] DataScientest. (2022). ¿Por qué Linux es el sistema operativo preferido de los desarrolladores? DataScientest. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://datascientest.com/es/por-que-linux-es-preferido-de-los-desarrolladores

[24] Germain, J. (2023). Linux Malware Rates Rise to Record Levels Amid Hacker Inconsistency. [En línea]. Technewsworld. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.technewsworld.com/story/linux-malware-rates-rise-to-record-levels-amid-hacker-inconsistency-176834.html

[25] Mordor Intelligence. (2023). Análisis de mercado de sistemas operativos para servidores. [En línea]. Mordor. [Citado 24-Noviembre-2024]. Disponible en Internet

facilita su integración en tecnologías emergentes como Docker y Kubernetes, permitiendo una gestión eficiente de contenedores y aplicaciones en la nube Red Hat[26]. Esta tendencia refuerza la justificación para proyectos que se basan en Linux, ya que las proyecciones indican un crecimiento del 19.2% en cuota de mercado de Linux en servidores Darkcrizt[27], dado su dominio en infraestructuras de servidores y su capacidad para soportar tecnologías clave en la computación moderna.

Por tanto, la obtención y análisis de la memoria volátil (RAM) es fundamental en procesos de computación forense ya sea en Windows o Linux, debido a la naturaleza efímera de los datos que almacena, la RAM contiene información crítica sobre procesos en ejecución, conexiones de red activas, claves de cifrado, artefactos del sistema, archivos de paginación, líneas de tiempo de los artefactos almacenados en memoria, extracción de MFT (Master File Table), registros de Windows, Librerías DLL, claves de registro, ficheros abiertos o en ejecución, extracción de objetos, drivers o ficheros creados en el sistema, y búsquedas avanzadas en espacios de memoria específicos Monedero, M[28];. Según un estudio publicado en la revista "Digital Investigation", la memoria RAM alberga datos temporales que, de no ser preservados adecuadamente, pueden desaparecer al apagar o reiniciar el sistema, impidiendo la recuperación de información vital para

https://www.mordorintelligence.com/es/industry-reports/server-operating-system-market/market-size

[26] RedHat. (2020). Contenedores versus máquinas virtuales. [En línea]. REDHAT. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.redhat.com/es/topics/containers/containers-vs-vms

[27] Darkcrizt. (2024). La cuota de mercado de Linux podría crecer un 19,2% para el 2027. [En línea]. Linuxadictos. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.linuxadictos.com/la-cuota-de-mercado-de-linux-podria-crecer-un-192-para-el-2027.html

[28] Monedero, M. (2020). La importancia de la memoria RAM en un análisis forense. [En línea]. Redseguridad.[Citado 24-Noviembre-2024]. Disponible en Internet https://www.redseguridad.com/especialidades-tic/activos-de-informacion/la-importancia-de-la-memoria-ram-en-un-analisis-forense_20201030.html

el análisis forense Rosales, G[29]. Por ejemplo, herramientas como Volatility permiten extraer y analizar estos datos, facilitando la identificación de malware en memoria y la reconstrucción de actividades sospechosas Portillo, I; Rodríguez, A[30]; por lo que ignorar la captura de la memoria volátil puede resultar en la pérdida de evidencia e información clave, dificultando la respuesta efectiva a incidentes de ciberseguridad, comprometiendo la integridad de la investigación forense y entorpeciendo las actividades de una recuperación efectiva.

[29] Rosales, G. (2022). VOLATILITY: ANÁLISIS FORENSE DE MEMORIA. [En línea]. yanapti. [Citado 24-Noviembre-2024]. Disponible en Internet https://yanapti.com/2022/volatility-analisis-forense-de-memoria/

[30] Portillo, I; Rodríguez, A. (2022). Informática Forense: Las herramientas y técnicas que debes dominar. [En línea]. Campusciberseguridad.[Citado 24-Noviembre-2024]. Disponible en Internet https://www.campusciberseguridad.com/blog/item/189-informatica-forense-herramientas-tecnicas-deber-dominar

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Definir un procedimiento para la creación de perfiles de los sistemas operativos Linux DEBIAN (Ver. 18.04.6 y 12.4.0) y Ubuntu (Ver. 18.04.6 y 22.04.3) con el propósito de analizar la memoria volátil a través del uso de la herramienta “Volatility2.6”.

4.2 OBJETIVOS ESPECÍFICOS

- Examinar el panorama actual de los ciberataques relacionados con sistemas operativos basados en Linux, por medio del análisis documental, para evidenciar su nivel de riesgo.
- Establecer los tipos de análisis que se pueden realizar a la memoria volátil utilizando las funcionalidades disponibles en Volatility 2.6, a partir de la revisión documental en fuentes especializadas, para realizar los análisis de memoria volátil en sistemas operativos Linux.
- Recomendar un procedimiento optimizado para la creación de perfiles en Volatility 2.6, basado en la documentación oficial de la Volatility Foundation y de la comunidad que facilite y apoye el análisis de memoria volátil en contextos de análisis forense o respuesta a incidentes.
- Usar los perfiles creados mediante el procedimiento optimizado de Volatility 2.6, a través de la ejecución de comandos de Volatility Linux sobre volcados de memoria RAM obtenidos de sistemas operativos Linux Debian (Ver. 18.04.6 y 12.4.0) y Ubuntu (Ver. 18.04.6 y 22.04.3), para verificar su funcionalidad.

5 MARCO REFERENCIAL

5.1 MARCO TEÓRICO

Memoria Principal: Unidad de almacenamiento de acceso rápido, con capacidad limitada y central, que se encarga de almacenar información clave de los programas y datos para la operación del computador. Esta tecnología se basa en los circuitos integrados semiconductores, estos solo pueden tener dos estados posibles, estáticos y dinámicos, o lo que sería la RAM y la ROM Morris, M[31].

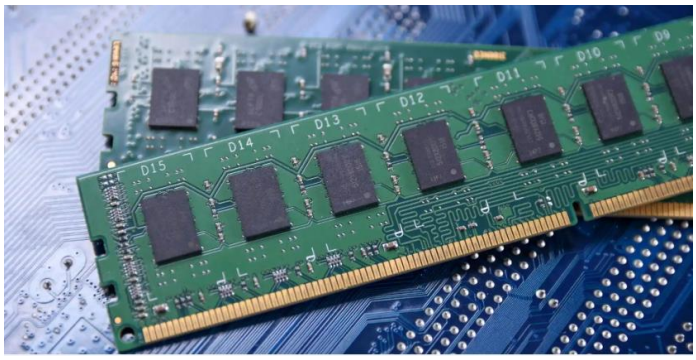


Figura 1 Memoria RAM.

Fuente: Fortinet (2021). ABC de la memoria RAM. Recuperado de https://frontier.com.co/blog/sabias_que/abc-de-la-memoria-ram

Memoria Auxiliar o Almacenamiento Secundario: La memoria auxiliar o el también llamado almacenamiento secundario son aquellos dispositivos que están creados para guardar datos e información a largo plazo que no va a requerir un

[31] Morris Mano M. (1994). Arquitectura de Computadoras. [En línea]. Pearson Prentice Hall. Pag. 480. [Citado 24-Noviembre-2024]. Disponible en Internet https://books.google.com.co/books?hl=es&lr=&id=2wWZyKu60cAC&oi=fnd&pg=PR10&dq=memoria+principal+de+una+computadora&ots=DTMKg_8uvt&sig=2YKd8sEB9WswlPcW0l3_hTm_JSo&redir_esc=y#v=onepage&q=memoria%20principal%20de%20una%20computadora&f=false

acceso frecuente y es generalmente datos persistentes. Adicionalmente, una parte de esta memoria auxiliar puede llegar a ser utilizada por la memoria principal en un tipo de memoria principal virtual, teniendo en cuenta que esta memoria no tiene la misma rapidez ni características que si tiene la memoria principal, de igual manera en esta categoría encontramos los discos duros mecánicos (HDD) y los discos duros de estado sólido (SSD) Sánchez, L[32].

Memoria RAM: Memoria de acceso aleatorio (Random Access Memory), esta memoria almacena de manera temporal datos de las aplicaciones que están en uso, optimizando el uso del equipo ya que la CPU puede apuntar a un espacio en memoria donde este alojado temporalmente la aplicación lo que permite que esta pueda ser ejecutada más rápidamente, esto también aplica con las aplicaciones propias del sistema para que este función, de igual manera, esta memoria RAM almacena la información mientras mantenga energía, una vez esta es apagada o pierde energía deja de almacenar la información que contenía y se “reinicia” Sánchez, L.

Memoria ROM: Memoria de Solo Lectura (Read-Only Memory), también llamados chips no volátiles es aquella memoria que almacena datos de forma permanente que no pueden ser alterados o modificados directamente por el usuario, estos se mantienen incluso cuando el computador pierde energía o se apaga, este contiene un conjunto de instrucciones y configuraciones para incorporar de forma adecuada todos los componentes físicos del equipo como la CPU, para que el computador pueda funcionar y ponerse en marcha, aquí tenemos por ejemplo las BIOS, la

[32] Sánchez J. (2016). Arquitectura de Computadoras Modernas. [En línea]. Universidad Autónoma del Estado de México. [Citado 24-Noviembre-2024]. Disponible en Internet http://ri.uaemex.mx/bitstream/handle/20.500.11799/63958/secme-25335.pdf?sequence=1

memoria de lectura de consolas NES o calculadoras científicas, entre otras Santos J[33].

Volatility: Software de código abierto lanzado en el 2007 en la conferencia de Black Hat DC de ese año, este software está especializado y enfocado en el análisis de memoria volátil de manera forense o de análisis de memoria avanzado Volatility Foundation[34]. Esta herramienta sirve para apoyar en las investigaciones de incidentes puesto que la memoria almacena de manera temporal datos y procesos en ejecución, por lo que es posible extraer información crítica del sistema y las amenazas cibernéticas. Entre las funcionalidades y capacidades podemos encontrar: Análisis de Volcados de memoria; extracción de data (p. ej. Procesos, actividades de red, conexiones, eventos, contraseñas, recuperar archivos y demás artefactos que puedan resultar relevantes); Soporte de múltiples plataformas desde computadores hasta dispositivos móviles; Personalizable y con mejoras continuas oficiales o de la comunidad; Soporte oficial por parte de la comunidad y de manera oficial; Puede ser soportado legalmente en procesos y litigios legales Macht, H[35].

Computo Forense / Informática Forense: La informática forense es la ciencia enfocada en realizar el análisis de los incidentes, eventos o situaciones judiciales que así lo requieren y que involucran cualquier tipo de fuente de información en cualquiera de sus estados y medios tanto físicos como digitales, en el cual, se incluyen, pero no se limita a las etapas de identificación (identificar las fuentes de

---

[33] Santos, J. (2020). Sistemas de Información Geográfica. Universidad Nacional de Educación a Distancia – UNED. [En línea]. Cap. 3.1.2. El componente físico (Hardware) [Citado 24-Noviembre-2024]. Disponible en Internet https://books.google.com.co/books?hl=es&lr=&id=xjbeDwAAQBAJ&oi=fnd&pg=PP1&dq=memoria+ROM&ots=wru4kzxGbh&sig=xQ7PA-fn9gCdfXAkggEAHkLGwqE&redir_esc=y#v=onepage&q=memoria%20ROM&f=false

[34] The Volatility Foundation (2020). [En línea]. About The Volatility Foundation. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.volatilityfoundation.org/about

[35] Macht, H. (2013). Live Memory Forensics on Android with Volatility. [En línea]. FAU – Friedrich – Alexander Universität. [Citado 24-Noviembre-2024]. Disponible en Internet https://homac.github.io/publications/Live_Memory_Forensics_on_Android_with_Volatility.pdf

información involucradas), preservación (Salvaguardar la integralidad de las evidencias hasta que se realice el proceso), recolección (Recolectar las fuentes de información involucradas), procesamiento (Procesar la información en herramientas forenses), revisión, análisis, producción y presentación, López O; Amaya H[36]. Para que el resultado pueda ser utilizado para procesos internos de una compañía o para algún proceso jurídico o de ley Dominguez, F[37].

CSIRT: Es un equipo interdisciplinario de diferentes áreas de TI especializados en Ciberseguridad y dedicados a realizar las respuestas a incidentes, esto incluyen las fases de preparación (activadas previo a un incidente), detección (Identificación de un posible evento que puede volverse un incidente o un incidente), respuesta (Durante el incidente se realizan actividades de contención, erradicación y recuperación) y lecciones aprendidas (Todas las actividades de aprendizaje post Incidente) Luna, H. E. R., & Miranda, J. M[38]. Así mismo, el termino CSIRT es un acrónimo (Computer Security Incident Response Team), pero también puede ser conocido como:

- CERT o CERT/CC (Equipo de respuesta a incidentes / Centro de Coordinación).
- CSIRT (Equipo de respuesta a incidentes de seguridad informática).
- IRT (Equipo de respuesta a incidentes).
- CIRT (Equipo de respuesta a incidentes informáticos).

---

[36] López, Ó., Amaya, H., León, R., & Acosta, B. (2001). Informática forense: generalidades, aspectos técnicos y herramientas. [En línea]. Universidad de los Andes. Colombia. [Citado 24-Noviembre-2024]. Disponible en Internet https://urru.org/papers/RRfraude/InformaticaForense_OL_HA_RL.pdf

[37] Dominguez, F. L. (2013). Introducción a la informática forense.[En línea]. Ra-Ma Editorial. [Citado 24-Noviembre-2024]. Disponible en Internet https://books.google.com.co/books?hl=es&lr=&id=Yaa6EAAAQBAJ&oi=fnd&pg=PP1&dq=inform%C3%A1tica+forense&ots=_qg997SwLd&sig=3FZLoRgRQ1v6amQjkHz2oHJCQhk&redir_esc=y#v=onepage&q=inform%C3%A1tica%20forense&f=false

[38] Luna, H. E. R., & Miranda, J. M. (2015). Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). [En línea]. ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, (1). [Citado 24-Noviembre-2024]. Disponible en Internet https://www.redalyc.org/pdf/5122/512251501006.pdf

- SERT (Equipo de respuesta a emergencias de seguridad).

Respuesta a Incidentes: Según el NIST en su guía 200-61 v2, indica que la respuesta a incidentes es un proceso integral que se lleva a cabo para gestionar y mitigar los impactos que un incidente de Ciberseguridad puede ocasionar en una organización, teniendo definidos algunos pasos para realizar este proceso los cuales son NIST[39]:

- Preparación: Actividades preventivas que permiten disminuir las probabilidades de un incidente.
- Detección y análisis: Monitorear, análisis y reportar cualquier actividad sospechosa o posibles incidentes, para determinar su alcance.
- Contención, erradicación y recuperación: Cuando se confirma el incidente se debe realizar una investigación y realizar procesos de Contención de la amenaza para evitar su propagación en toda la red, los procesos de erradicación profunda de la amenaza y la recuperación de la operatividad de los sistemas.
- Lecciones aprendidas: Actividades post incidente, que permiten mejorar los procesos y fortalecer los sistemas de acuerdo con lo identificado en el incidente.

Linux: Linux es un sistema operativo de código abierto bajo términos de licencia GPL (Licencia publica generar o GNU) que fue desarrollado en Unix, en 1991 por un estudiante de la universidad de Helsinki, actualmente basado en Kernel de Linux, lo que hace que el núcleo del sistema se encargue de las operaciones de bajo nivel y de traducir las instrucciones a el hardware de la computadora, es ampliamente

[39] Instituto Nacional de Estándares y Tecnología (NIST). (2020). Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2). [En línea]. NIST. [Citado 24-Noviembre-2024]. Disponible en Internet https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

conocido por su estabilidad, seguridad y flexibilidad, utilizado ampliamente por organizaciones para algunos de sus servicios Pons; N[40].

5.2 MARCO CONCEPTUAL.

Se realiza la revisión de fuentes de información ampliando el soporte de los procesos planteados en el desarrollo del presente documento.

Por lo que contrario al mito de que Linux es invulnerable al malware, la realidad muestra un aumento significativo en la cantidad de amenazas que afectan al sistema operativo de código abierto. Según un informe de Crowdstrike, la presencia de malware en Linux ha experimentado un aumento del 35% en 2021 en comparación con el año anterior Medina, E[41]. De igual manera Eduardo Medina, en su publicación “Malware en Linux, una tendencia al alza”, indica que entre las amenazas más destacadas se encuentran las familias de malware Mirai, Mozi y XorDDoS, que representaron el 22% de todos los ataques dirigidos contra Linux en 2021. Estas amenazas, en su mayoría, siguen centradas en dispositivos IoT, aunque los usuarios de escritorio no deben subestimar la importancia de mantener la seguridad, ya que se están diseñando variantes de estas que por ejemplo están enfocadas en atacar protocolos como él y realizar ataques de fuerza bruta para vulnerar credenciales débiles.

---

[40] Pons, N. (2016). Linux: principios básicos de uso del sistema. [En línea]. Ediciones ENI. [Citado 24-Noviembre-2024]. Disponible en Internet https://books.google.com.co/books?hl=es&lr=&id=U9e6CLWQEaoC&oi=fnd&pg=PA11&dq=que+es+linux&ots=n5PEsH8OpH&sig=fv7Ojmzd5sBEwlTSYBgbCO3l1Fc&redir_esc=y#v=onepage&q=que%20es%20linux&f=false

[41] Medina, E. (2022). Malware en Linux, una tendencia al alza. [En línea]. Muy Linux. [Página web]. Recuperado el 15 de enero de 2024. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.muylinux.com/2022/01/20/malware-linux-2021/

En consecuencia, si vemos el panorama local de los cibercrímenes en Colombia se evidencia que según el Observatorio de Cibercrimen de la Policía nacional que el uso de software malicioso fue el delito informático que más presento un incremento del 58% en el periodo de enero de 2022 a mayo de 2023, así mismo teniendo que las dos ciudades con más reportes de incidentes informáticos son Bogotá con más de 7.359 casos, seguido de Medellín con 1.910 casos Policía Nacional; Centro Cibernético Policial[42].

Adicionalmente, según lo reportado por Cendales, M. A[43]. Gerente de ciberseguridad producto B2B de Claro Colombia, en su artículo "Ciberseguridad a la medida" publicado por la revista Portafolio, la actualidad de la ciberseguridad en la región y específicamente en Colombia presenta desafíos significativos, ya que según estadísticas globales se generan alrededor de un millón de ataques informáticos por segundo, así mismo, Colombia se destaca como el segundo con menos cultura en ciberseguridad en la región, ya que durante el tercer trimestre, el CSIRT reportó cerca de 29,000 ataques a infraestructuras empresariales, generando interrupciones operativas, suplantaciones de identidad y fraudes financieros. Además, se registraron más de 31,000 incidentes de ransomware, y las pérdidas promedio por estos eventos aumentaron de 175,000 millones dólares en 2022 a sorprendentes 400,000 millones de dólares en 2023 Cendales[44].

---

[42] Escobar, J. (2023). Los delitos cibernéticos se han reducido en el 2023: Policía Nacional. [En línea]. Radio Nacional de Colombia. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.radionacional.co/actualidad/delitos-ciberneticos-en-colombia-estadisticas-actuales

[43] Cendales, M. A. (2023, 2 de noviembre). 'Ciberseguridad a la medida' para todas las empresas de Colombia. [En línea]. Portafolio.co. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.portafolio.co/contenido-patrocinado/ciberseguridad-a-la-medida-para-las-empresas-colombianas-592267

[44] Cendales, M. A. (2023, 2 de noviembre). 'Ciberseguridad a la medida' para todas las empresas de Colombia. [En línea]. Portafolio.co. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.portafolio.co/contenido-patrocinado/ciberseguridad-a-la-medida-para-las-empresas-colombianas-592267

Germain J.M.[45], en su artículo para ECT News Network titulado 'Las tasas de malware de Linux aumentan a niveles récord en medio de la inconsistencia de los piratas informáticos', destaca un aumento preocupante en la frecuencia del malware en sistemas operativos Linux, esto basado en el análisis de datos de las investigaciones realizadas por Atlas VPN, enfatizando que la amenaza de malware en Linux está en constante evolución, tal como lo indican en el artículo. Específicamente, se registró un incremento del 50% en nuevas amenazas de malware, alcanzando 1,9 millones el 18 de enero de 2022, frente a los 121,6 millones de muestras detectadas el año anterior. Sin embargo, el articulo también señala una disminución del 39% en el número total de nuevos malware, situándose en 73,7 millones, como se muestra en la siguiente imagen:"

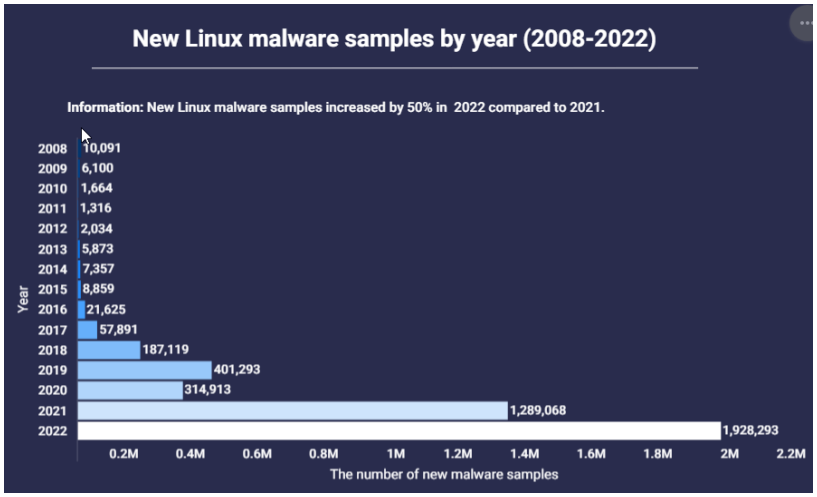


Figura 2 Muestras de malware Linux para el periodo de 2008 – 2022.

Fuente: Germain, J. M. (2023, 23 de enero). Linux Malware Rates Rise to Record Levels Amid Hacker Inconsistency. LinuxInsider. https://www.linuxinsider.com/story/linux-malware-rates-rise-to-record-levels-amid-hacker-inconsistency-176834.html.

[45] Germain, J. (2023). Linux Malware Rates Rise to Record Levels Amid Hacker Inconsistency. [En línea]. Technewsworld. [Citado 24-Noviembre-2024]. [Citado 24-Noviembre-2024]. Disponible en Internet Disponible en Internet https://www.technewsworld.com/story/linux-malware-rates-rise-to-record-levels-amid-hacker-inconsistency-176834.html

De igual manera, estos datos son contrastados con lo indicado por la firma de Ciberseguridad Fortinet donde indican que en Colombia para el 2021 se registraron 7 billones de intentos de Ciberataques de 41 billones que se registraron en todo el mundo en cualquiera de sus modalidades FortiGuard Labs; Fortinet[46]. Así mismo, Fortinet resalta que:

> "De acuerdo con la firma, se detectaron numerosas campañas con troyanos durante este período, y generalmente incluían el establecimiento de conexiones de acceso remoto, la captura de entrada de teclado, la recopilación de información del sistema descarga y carga de archivos y colocación de otros 'malware' en el sistema" Fortinet[47].

Adicional, según el informe compartido por Dmitry Bestuzhev, director del Equipo Global de Investigación y Análisis en Latinoamérica Kaspersky, en Colombia se bloquean cada minuto al menos 87 intentos de infección de los malware que son más reconocidos Diaz Hernán[48] y también reconoció que los ataques para el 2020 se incrementaron en un 316% posicionando a Colombia como la tercera más

[46] Fortinet. (2022). América Latina empieza el año con más de 7 mil millones de intentos de ciberataques. [En línea]. FORTINET. [Citado 24-Noviembre-2024]. Disponible en Internet Disponible en Internet https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/america-latina-empieza-el-ano-con-mas-de-7-mil-intentos-ciberataques

[47] Fortinet. (2022). América Latina empieza el año con más de 7 mil millones de intentos de ciberataques. [En línea]. FORTINET. [Citado 24-Noviembre-2024]. Disponible en Internet Disponible en Internet https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/america-latina-empieza-el-ano-con-mas-de-7-mil-intentos-ciberataques

[48] Diaz, H. (2021). Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. [En línea]. Kaspersky. [Citado 24-Noviembre-2024]. Disponible en Internet https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

atacada de sur América seguida de Brasil y Argentina TicTac[49], así mismo, Diaz Hernán, asevero que:

> Este tipo de ataque explota vulnerabilidades presentes en las tecnologías de acceso remoto o intenta adivinar las contraseñas para acceder a una máquina o servidor conectado a Internet e ingresar a la red corporativa para robar datos o extorsionar a su víctima. Al comparar los primeros ocho meses de 2021 con el mismo periodo del año anterior, vemos un aumento del 78% de este tipo de ataques. Diaz Hernán.

Por lo que, teniendo esta visión global y local, Marcos Merino, en su publicación "Cuanto más popular es Linux, más vulnerable: vemos dos ejemplos de malware destacados en el último mes", asevera que a medida que Linux se vuelve más popular, también se vuelve más vulnerable, tomando como referencia que el uso generalizado de componentes de código abierto, ya sea en forma de bibliotecas o servidores, ha planteado desafíos de seguridad significativos, puesto que los hackers han aumentado su interés en atacar aplicaciones de código abierto, y vulnerar las diferentes distribuciones de Linux. Por lo que contrariamente a la percepción anterior de que Linux era sinónimo de seguridad y no necesitaba antivirus, la realidad actual muestra una creciente exposición a nuevas ciber amenazas, ya que, en la primera mitad de 2023, se registraron 260,000 muestras únicas de malware dirigidas específicamente a Linux, según datos de telemetría revelados por Secure List.

Así mismo, Marcos Merino, indicó que el malware en Linux puede estar presente sin que se haya detectado y reportado o sencillamente pueden existir malware que aprovechen vulnerabilidades del propio sistema operativo para lo cual, detalló dos aplicaciones de malware que se descubrieron en septiembre de 2023, demostrando

[49] TicTac CCIT. 2020. Tendencias del Cibercrimen en Colombia 2019-2020. [En línea]. CCIT Camara Colombiana de Informática y Telecomunicaciones. [Citado 24-Noviembre-2024]. Disponible en Internet ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

que este sistema se ha vuelto más vulnerable, el primer ejemplo es vulnerabilidad en la biblioteca libcue, integrada en el Tracker Miners utilizado por GNOME, el entorno de escritorio más popular en sistemas Linux, esta vulnerabilidad, identificada como CVE-2023-43641, permite a los atacantes ejecutar código malicioso aprovechando que Tracker Miners indexa automáticamente todos los archivos descargados con ciertas extensiones lo que permite que se descargue un archivo infectando con cierta extensión y características para que lo indexe automáticamente INCIBE-CERT[50]. Así mismo, el segundo ejemplo fue la campaña de malware activa que operaba durante varios años, que fue descubierta por Kaspersky identificando que desde el 2013 afecta a usuarios que instalaban un gestor de descargas llamado 'Free Download Manager' desde un repositorio oficial de la aplicación, por lo que podría tratarse de un caso de un ataque a la cadena de suministros hacia el fabricante de la aplicación, este paquete infectado instalaba una puerta trasera y un "Bash stealer" que recopilaba información confidencial, como datos del sistema, historial de navegación, credenciales almacenadas, billeteras de criptomonedas, credenciales de servicios WEB y en la nube, entre otros Kaspersky[51].

Continuando con lo indicado por Marcos Merino, encontramos otros autores como Roberto Cantero en su publicación “Un malware que robaba contraseñas en Linux ha funcionado durante 3 años y nadie se ha dado cuenta hasta ahora”, donde sugiere que, a pesar de la reputación de estabilidad y robustez de Linux, no es inmune a amenazas de malware, como se evidencia en el caso específico del gestor de descargas Free Download Manager, destacando la necesidad actual de que las

[50] INCIBE-CERT. (2023). Vulnerabilidades CVE-2023-43641. [En línea]. INCIBE. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2023-43641

[51] Kaspersky. (2023). Principales amenazas de ciberseguridad para empresas: cómo protegerse de ellas. Kaspersky. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://latam.kaspersky.com/resource-center/preemptive-safety/website-security-is-your-business-at-risk

personas dedicadas a la ciberseguridad intensifiquen sus esfuerzos en la investigación y atención de amenazas, tanto emergentes como ya existentes, dirigidas a afectar las diversas distribuciones de Linux, ya que este no está exento de riesgos, y se debe prestar atención a la seguridad incluso en entornos menos frecuentemente afectados Cantero, R[52].

Por otra parte, según indica Rahul Varshney ,Nitesh Kumar ,Anand Handa y Sandeep Kumar Shukla, en su trabajo “Perfiles personalizados de volatilidad para la detección automatizada de malware ELF híbrido”, resaltan como la creciente prevalencia del malware en sistemas Linux representa una grave amenaza para las organizaciones y sus datos privados, así como también, los costos que conlleva que una amenaza se materialice en dichos entornos. Por lo tanto, existe una necesidad urgente de aprender a utilizar herramientas como lo es Volatility para poder realizar análisis que permitan automatizar las extracciones entorno al malware en Linux y lograr comprender sus capacidades y comportamiento de la manera más rápida posible Varshney, R., Kumar, N., Handa, A., & Shukla, S. K.[53].

En términos de un análisis forense digital la memoria RAM o memoria volátil según Guillermo Jaramillo[54] en su artículo “Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles”, indica que tiene un papel relevante cuando se requiere analizar el malware utilizado por el atacante, además de resaltar que estos análisis generalmente se realizan en vivo, adicionalmente, enfatiza que los investigadores deben tener clara su labor y el juicio para poder determinar cuándo

---

[52] Cantero, R. (2023). Un malware que robaba contraseñas en Linux ha funcionado durante 3 años y nadie se ha dado cuenta hasta ahora. [En línea]. UrbanTecno. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.mundodeportivo.com/urbantecno/linux/un-malware-que-robaba-contrasenas-en-linux-ha-funcionado-durante-3-anos-y-nadie-se-ha-dado-cuenta-hasta-ahora

[53] Varshney, R., Kumar, N., Handa, A., & Shukla, S. K. (2022, November). Volatility Custom Profiling for Automated Hybrid ELF Malware Detection. [En línea]. In International Conference on Digital Forensics and Cyber Crime (pp. 274-291). Cham: Springer Nature Switzerland.

[54] Guillermo, J. (2011). Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles. [En línea]. Universidad Continental. [Citado 24-Noviembre-2024]. Disponible en Internet https://dialnet.unirioja.es/servlet/articulo?codigo=5042969

es posible o no analizar un dispositivo o sistema móvil, así como la manera en que lo va a realizar siempre soportando y justificando las acciones y decisiones tomadas.

Adicionalmente, Juan Castilla, y Jonhattan Romero[55], en su documento "Importancia de la recolección de datos volátiles dentro de una investigación forense", indican que el orden de recolección en cualquier incidente o investigación debe darse por el orden de volatilidad de los datos, es decir que debe priorizarse lo que tenga más posibilidad de perderse como la memoria principal o también conocida como memoria RAM que almacena gran cantidad de información pero esta es constantemente sobre escrita y puede perderse en caso de que el dispositivo pierda corriente o se sobrescriban muchos datos sobre la misma, además de enfatizar como actualmente es más común que los diferentes tipos de malware (p. ej. Troyanos, gusanos, fileless, entre otros), o ciberdelincuentes utilicen la memoria RAM para ejecutar sus herramientas, procesos y tareas; ya que esto, entre otras cosas, permite disminuir y dificultar la tarea de encontrar los rastros del atacante en el sistema víctima, resaltando finalmente que en los datos volátiles podemos encontrar información útil como por ejemplo: Contenido de portapapeles, puertos abiertos, información de red, procesos, servicios y aplicaciones, datos temporales, información almacenada en cache, o artefactos, entre otros.

En cuanto al tiempo necesario para realizar una captura de memoria RAM en comparación con el tiempo que toma capturar todas las particiones del disco duro en un servidor Linux, diversos estudios y experiencias en el campo forense resaltan que la captura de la memoria RAM suele ser significativamente más rápida, esto se debe principalmente a que la memoria RAM, aunque volátil, tiene un tamaño mucho menor en comparación con el almacenamiento de disco duro, que puede abarcar

[55] Castilla, J; Romero, J. (2018). Importancia de la recolección de datos volátiles dentro de una investigación forense. [En línea]. Universidad Piloto de Colombia. [Citado 24-Noviembre-2024]. Disponible en Internet http://repository.unipiloto.edu.co/handle/20.500.12277/3088?show=full

cientos de gigabytes o incluso terabytes. Según Casey, E[56], en su obra Handbook of Digital Forensics and Investigation, la extracción de memoria RAM en un sistema operativo Linux puede tomar entre unos pocos segundos a varios minutos dependiendo de la capacidad total de la memoria y las herramientas utilizadas, como dd, LiME (Linux Memory Extractor) o fmem. Por otro lado, según Carrier, B.[57], en su libro File System Forensic Analysis, capturar todas las particiones de un disco duro completo puede extenderse por varias horas hasta más de un día, especialmente en sistemas con discos de gran capacidad o cuando se utiliza un método de adquisición forense que garantiza la integridad y evita la corrupción de datos, como imágenes completas con herramientas como dcfldd o FTK Imager. Este contraste subraya la importancia de priorizar la captura de memoria RAM durante una investigación, no solo por su volatilidad, sino también por la rapidez con la que puede realizarse en comparación con la adquisición del disco duro.

Por otra parte, en cuanto a los procesos de recolección, se ha señalado que la captura y análisis de memoria RAM presenta mayores desafíos comparado con el disco duro, debido a su naturaleza volátil y a la susceptibilidad de errores durante su adquisición. Según Mandia, k; Prosise, C; y Pepe, M[58]; la memoria RAM almacena datos que están en uso activo por el sistema operativo y las aplicaciones, lo que la convierte en una fuente valiosa de información para investigaciones forenses, sin embargo, esta misma volatilidad implica que los datos pueden alterarse o perderse fácilmente si no se utilizan herramientas adecuadas y

---

[56] Casey, E. (2011). Handbook of Digital Forensics and Investigation. [En línea]. Academic Press. Sciencedirect. [Citado 24-Noviembre-2024]. Disponible en Internethttps://www.sciencedirect.com/book/9780123742674/handbook-of-digital-forensics-and-investigation

[57] Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional. [En línea]. 1er edición.[Citado 24-Noviembre-2024]. Disponible en Internet https://repo.zenk-security.com/Forensic/File%20System%20Forensic%20Analysis.pdf

[58] Mandia, k; Prosise, C; y Pepe, M. Incident response & computer forensics. [En línea]. McGraw-Hill, Inc.. Disponible en Internet https://dl.acm.org/doi/abs/10.5555/1207603

procedimientos estrictos en la recolección; además, Cromwell, T; Smith, J; y Vance, L; destacan que los errores más comunes en la adquisición de memoria RAM incluyen la sobreescritura de datos por procesos del sistema, fallos durante la extracción y la posible corrupción del volcado si no se maneja correctamente. Por el contrario, la recolección de un disco duro es menos propensa a errores críticos siempre que no presente fallos físicos o lógicos, ya que los datos se encuentran almacenados de manera más persistente y estructurada, lo que facilita incluso su análisis posterior.

Para apoyar los procesos de recolección y análisis de información que se encuentra alojada al interior de la memoria RAM, existen diversas herramientas, algunas mencionadas por Pedro Arnedo[59], en el trabajo “Herramientas de análisis forense y su aplicabilidad en los delitos informáticos”, entre estas herramientas podemos identificar RedLine, que se utiliza para adquirir y analizar la memoria RAM; FTK Imager, que, además de permitir la recolección de memoria no volátil, también facilita la adquisición de la memoria RAM; Process Dumper (PD), una herramienta que, aunque no permite obtener toda la memoria RAM, es útil para extraer procesos específicos que están siendo ejecutados en el equipo; DumpIt, que permite realizar un volcado completo de la memoria RAM; AVML (Adquirir memoria volátil para Linux) que permite adquirir memoria sin conocer la distribución del sistema operativo de destino; Linpmem utilizada para realizar volcado de memoria en sistemas Linux de una manera no tradicional, ofreciendo un API para realizar la lectura de información desde cualquier dirección física, incluida la memoria reservada y los agujeros de memoria, además, existe una herramienta especializada para analizar los volcados de memoria RAM llamada “Volatility”, por medio de la cual, una vez obtenida la memoria RAM, es posible realizar consultas para obtener evidencia de

[59] Arnedo, P. Herramientas de análisis forense y su aplicabilidad en investigación de delitos informáticos, 2014. [En línea] Universidad Internacional de la Rioja. [Citado 24-Noviembre-2024]. Disponible en Internet https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

una conversación de chat y artefactos WEB relevantes para la investigación, entre otras.

5.3 MARCO LEGAL.

Debido al incremento de los ciberdelitos (ej. acceso sin autorización a sistemas de información, fraude financiero, pornografía infantil, entre otros), en Colombia y América Latina en los últimos años y el rápido avance tecnológico y de la conectividad, existió la necesidad de que se actualizarán el alcance de tipificación de delitos cibernéticos, por lo que en 2009, un grupo de países de la región incluido Colombia, actualizó su sistema judicial para lograr procesar correctamente a los Ciberdelincuentes.

Por lo cual, se promulgo la Ley 1273 del 5 de enero de 2009, la bien conocida ley de “Delitos informáticos” o “de la protección de la información y de los datos”, esta ley complementa el Código Penal bajo un concepto de la protección de la información de datos, esto fue relevante ya que las empresas públicas y privadas pueden defender sus sistemas de información de los actores cibercriminales, y teniendo argumentos sólidos para incurrir en acciones legales que respalden la mundialización de dichos delitos.

Dentro de la Ley 1273 de 2009 [60] (Protección de la información y de los datos) REPÚBLICA DE COLOMBIA GOBIERNO NACIONAL. (5 de enero de 2009), publicada en el diario oficinal No. 47.223 del 5 de enero de 2009, encontramos 7 artículos los cuales tipifican los delitos cibernéticos en Colombia, resaltando que las multas por incurrir en cualquiera de estos van de los 100 a los 1.000 salarios

[60] REPÚBLICA DE COLOMBIA GOBIERNO NACIONAL. (5 de enero de 2009). [En línea]. LEY 1273 DE 2009 - Delitos informaticos. Bogotá. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

mínimos legales vigentes (SMLV). De acuerdo con los alcances del proyecto, se resaltan los siguientes artículos que tienen relación directa o indirecta con el mismo:

- Articulo 269 A. Acceso abusivo a un sistema informático: Este concepto se pone en práctica cuando se aprovecha una vulnerabilidad o debilidad en el acceso a un sistema informático, este tiene una condena de 48 a 96 meses de privación de la libertad.
- Articulo 259B. Obstaculización ilegitima de sistema informático o red de telecomunicación: Comete un delito quien bloquea o restringe el acceso a un sistema de información sin el consentimiento apropiado, este tiene una condena de 48 a 96 meses de privación de la libertad.
- Articulo 269C. Interceptación ilícita de datos informativos: El que sin una autorización u orden previa capte de manera ilícita datos durante su proceso de transmisión entre su origen y su destino cualquiera que sea el medio en que se transporta el mismo, este tiene una condena de privación de la libertad de 36 a 73 meses.
- Articulo 269D. Daños informáticos: Cuando alguien, sin tener la debida autorización, efectúa cambios, causa daños o altera datos en un programa o documentos, y esto ocurre en los recursos de los sistemas de información este tiene una condena de cárcel de 48 a 96 meses.
- Articulo 269E. Uso de software malicioso: Cualquier tipo de software o programa malicioso diseñado y ejecutado específicamente para alterar el correcto funcionamiento de un sistema de información, este tiene una condena de cárcel de 48 a 96 meses.
- Articulo 269F. Violación de datos personales: Es cuando sin estar autorizado, capta, obtiene, vende, envía, divulga, datos personales almacenados cualquier medio físico o digital, este tiene una condena de privación de la libertad de 48 a 96 meses.

  Articulo 269G. Suplantación de sitios web para capturar datos personales: Cualquier tipo de suplantación de una entidad en el Ciberespacio que pueda

tener la finalidad de engañar a los usuarios para que ingresen su información confidencial o para enviar correos phishing, este tiene una condena de prisión de 48 a 96.

Asimismo, se resalta la Ley 1581 de 2012, conocida como la 'Ley de Protección de Datos Personales' MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE (13 DE NOVIEMBRE DE 2015)[61], junto con el Decreto 1377 de 2013[62], que reglamenta dicha normativa, esta legislación establece las definiciones, responsabilidades y sanciones legales, tanto económicas como penales, aplicables a quienes accedan o utilicen datos personales sin la debida autorización; en el contexto del análisis forense y la respuesta a incidentes, resulta particularmente relevante debido a que en la memoria volátil es posible recuperar información sensible del usuario, como sesiones activas o datos personales, por ello, es fundamental contar con actas o soportes que autoricen expresamente el acceso y tratamiento de los datos recolectados, independientemente del tipo de investigación o incidente en curso..

[61] MINISTERIOR DE AMBIENTE Y DESARROLLO SOSTENIBLE (13 DE NOVIEMBRE DE 2015). [En línea]. Ley de Protección de Datos Personales o Ley 1581 de 2012. Bogotá. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protecci%C3%B3n%20de%20Datos,de%20naturaleza%20p%C3%BAblica%20o%20privada.

[62] PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. (27 de junio de 2013). [En línea]. DECRETO 1377 DE 2013 - Reglamentación de la ley 1581. Bogotá. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

6 DISEÑO METODOLÓGICO.

Para realizar el desarrollo de esta actividad, como se mencionó anteriormente el análisis de memoria volátil o memoria RAM es una temática que no ha sido abordada con tanta profundidad, sin embargo, hoy día representa un artefacto esencial en las investigaciones relacionadas con incidentes ya que permite determinar algunas características del malware o los TTP's de algunos actores Cibercriminales, como por ejemplo podemos encontrar algunos malware que únicamente se ejecutan en memoria como los conocidos "Fileless Malware PowerGhost", este tipo de malware actúan como troyanos ejecutando todas sus acciones en memoria únicamente por lo que en el dispositivo es posible que no exista información o artefactos asociados a la ejecución del mismo, este malware se aprovecha de la vulnerabilidad de "EternalBlue" para realizar movimiento lateral, tiene funcionalidad de troyano y cripto minero Trend Micro[63].

Por lo que, al ser un proyecto de tipo exploratorio lo que permitirá comprender el problema descrito en el presente documento, por lo que se tomó como referencia las normas ISO 27037 y la ISO 27042, se puede establecer lo siguiente:

6.1 ISO 27037:2012 "GUIDELINES FOR IDENTIFICATION, COLLECTION, ACQUISITION AND PRESERVATION OF DIGITAL EVIDENCE"

[63] Trend Micro. (2018). Fileless Malware PowerGhost Targets Corporate Systems. [En línea]. trendmicro. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/fileless-malware-powerghost-targets-corporate-systems

La ISO 27037[64] tiene las directrices que deben aplicarse hoy día, y se enfoca en el manejo de evidencia digital, lo que incluyen las etapas (ISO27037, 2012):

- Identificación: Localizar las fuentes de información asociadas a un evento o incidente, que sean relevantes para el objetivo de la investigación.
- Recolección: Definición de la estrategia de recolección que será utilizada dependiendo las diferentes fuentes de información y teniendo en cuenta si esta es volátil o no volátil.
- Adquisición: Realizar el proceso de las copias forenses y de trabajo.
- Preservación: Los resultados de las copias forenses deben ser almacenados en lugares controlados y seguros durante todo el tiempo de la investigación o hasta que se determine.

[64] Organización Internacional de Normalización. (2012). Tecnología de la información - Técnicas de seguridad - Directrices para la identificación, recolección, adquisición y preservación de pruebas electrónicas (ISO 27037:2012).

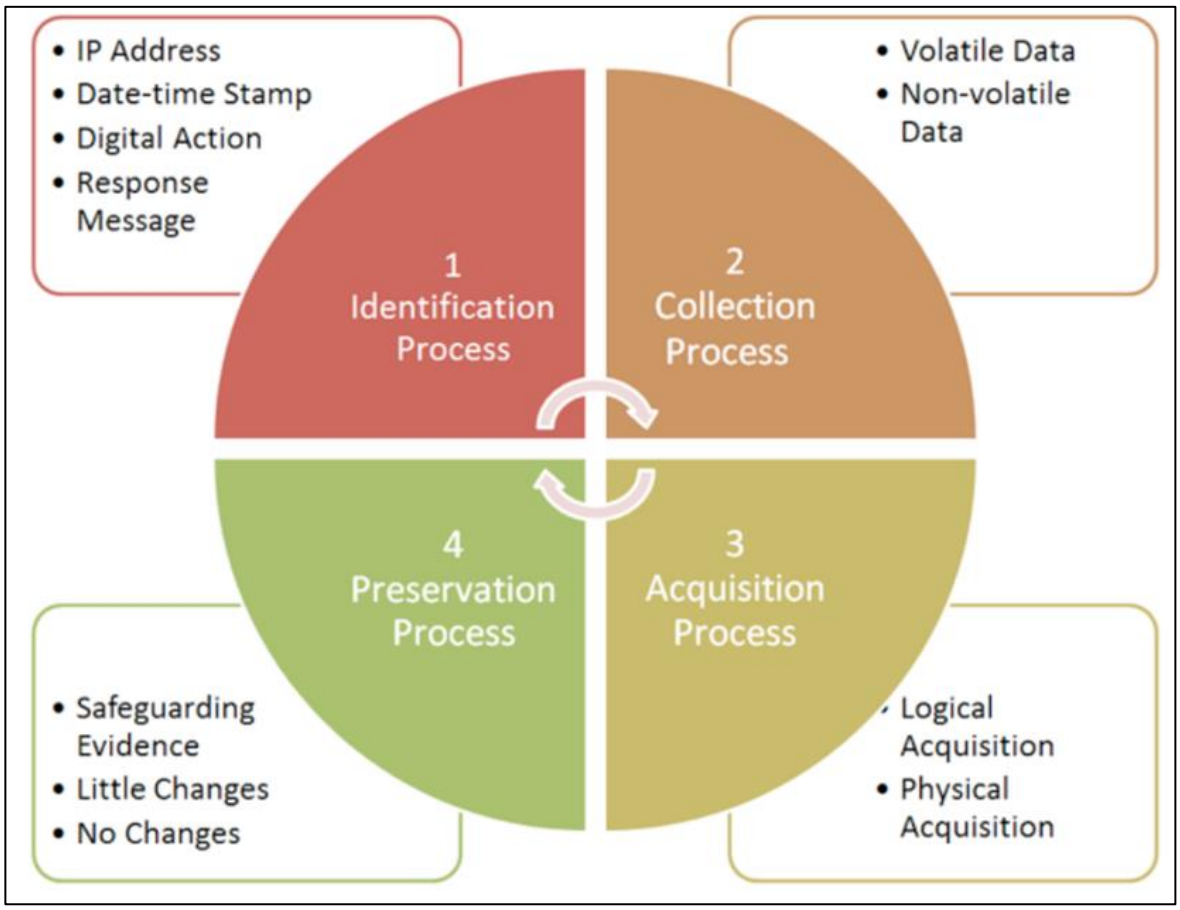


Figura 3 ISO 27037:2012.

Fuente: semanticscholer.org, A Novel Process Framework for Digital Forensics Tools: Based on ISO/IEC 27037:2012. Recuperado de: https://www.semanticscholar.org/paper/A-Novel-Process-Framework-for-Digital-Forensics-on-Kao-Wu/3bc102a301f7e521eee2cd6fb0c5da2f53af424d

Así mismo la norma incluye los principios básicos que corresponden principalmente a tres:

- ✓ Relevancia: Importancia de tener en cuenta todas las fuentes de información.
- ✓ Confiabilidad: Todos los procesos y la información recolectaba debe ser auditable y repetible por cualquier persona.

- ✓ Suficiencia: Las fuentes de información y los procesos deben ser lo suficientes y concretos para sustentar los hallazgos y resultados de la investigación.

Aunque el presente trabajo sigue las directrices de la norma ISO 27037:2012 y reconoce la importancia de sus cuatro etapas (identificación, recolección, adquisición y preservación), su alcance está delimitado específicamente al diseño y validación de perfiles para los sistemas operativos Linux Debian (Ver. 18.04.6 y 12.4.0) y Ubuntu (Ver. 18.04.6 y 22.04.3) con el uso de Volatility 2.6. Por lo tanto, se prioriza documentar las etapas relacionadas con la identificación y recolección, ya que estas son fundamentales para establecer las fuentes de información (en este caso, la memoria volátil) y definir las estrategias para su obtención.

Si bien las etapas de adquisición y preservación son inherentes al proceso general y se cumplen al generar y proteger los volcados de memoria que alimentan el análisis, su documentación no se aborda explícitamente en este trabajo, esto se debe a que el objetivo del documento no incluye la creación del volcado de memoria, la especificación de formatos o las técnicas para preservar la evidencia, sino que se enfoca en el desarrollo de perfiles y su posterior validación.

En este sentido, el documento adopta un enfoque metodológico basado en la ISO 27037, pero lo adapta al propósito específico de analizar la memoria volátil mediante la herramienta Volatility 2.6, así, se proporciona un marco útil para investigadores y analistas forenses o de respuesta a incidentes sin abarcar aspectos que, aunque importantes, están fuera del alcance definido por los objetivos del proyecto.

7 DESARROLLO DE LOS OBJETIVOS.

7.1 PANORAMA ACTUAL DE CIBERATAQUES EN LINUX

Basado en el análisis documental sobre el panorama actual de los ciberataques relacionados con los sistemas operativos Linux, dando cuenta que este sistema operativo a pesar de no tener una cuota en el mercado tan amplia como si lo tienen Windows, se ha convertido en una en un sistema operativo apetecido por los Cibercriminales ya que sobre este reposan múltiples servicios empresariales que pueden tener un beneficio económico muy grande para ellos si llegan a comprometer o vulnerar dichos sistemas operativos, por lo cual, se encontró que:

Durante las últimas dos décadas, la comunidad de seguridad ha centrado sus esfuerzos en combatir el malware, especialmente en sistemas operativos Windows por su vasta cuota de casi el 85% del mercado de sistemas operativos. Sin embargo, el crecimiento exponencial de dispositivos integrados, impulsado por la revolución del Internet de las cosas (IoT), está cambiando el escenario del malware.

A diferencia de las computadoras personales que tradicionalmente ejecutan Windows, los dispositivos integrados adoptan sistemas operativos similares a Unix, con versiones de Linux ganando popularidad, lo que es resaltado por Emanuele Cozzi; Mariano Graziano; Yanick Fratantonio y Davide Balzarotti[65]; en su investigación “Understanding Linux Malware”, señalando que este cambio ha llevado al surgimiento del "malware para Linux", pero también enfatizan que la atención de la industria de Ciberseguridad hacia este tipo de amenazas fue limitada hasta finales de 2014 donde Virus Total llamo la atención por el aumento exponencial y complejidad de amenazas para dicho sistema operativo, sin embargo,

[65] Cozzi, E., Graziano, M., Fratantonio, Y., & Balzarotti, D. (2018, May). Understanding linux malware. [En línea]. In 2018 IEEE symposium on security and privacy (SP) (pp. 161-175). IEEE.

no se ha tenido grandes avances y hallazgos por lo que la información disponible a menudo se limita a publicaciones de blogs.

Así mismo, el documento “Understanding Linux Malware”, menciona que tras realizar el análisis empírico de más de 10 mil muestras de diferentes tipos de malware para Linux, se evidencia como éstos han avanzado en complejidad y cantidad; lo que es realmente preocupante, puesto que éstos incluso pueden modificar los archivos ELF (Executable and Linkeable Format), con el objetivo de modificar cabeceras y contenido almacenar su ejecución, únicamente en memoria o utilizarla para dejar sus artefactos haciendo especial énfasis en los desafíos específicos al analizar muestras de Linux, como la diversidad de arquitecturas y el uso de técnicas como trucos anti análisis, empaquetado y polimorfismo. Los resultados revelan que el malware para Linux ya presenta complejidades, con muestras capaces de ejecutarse en varios sistemas operativos, almacenarse en memoria volátil únicamente y utilizar exploits de escalada de privilegios. Además, de abordar la interacción con utilidades de shell y enfoques de detección de máquinas virtuales.

En un informe publicado por la empresa Trend Micro se observó que el aumento en las vulnerabilidades asociadas a los sistemas operativos Linux, especialmente en entornos de nube y dispositivos IoT son provocados en gran medida por la obsolescencia y la falta de actualizaciones de seguridad en sus parches. Por ello, a medida que los sistemas operativos Linux se integra más en la infraestructura de la nube, su popularidad se convierte en un blanco atractivo para los ciberdelincuentes logrando de esta forma que, en un período de seis meses, se identificarán 200 vulnerabilidades distintas Byte[66].

En 2023 la empresa Kaspersky detectó 125 millones de archivos maliciosos evidenciando que Windows fue el sistema más atacado, con un 88% de archivos

[66] Byte. (2021). La seguridad en Linux, en entredicho. Revista Byte TI. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://revistabyte.es/ciberseguridad/seguridad-en-linux/

malintencionados detectados diariamente, y un notable aumento en documentos de varios formatos. Además, los archivos maliciosos en ofimática subieron un 53%, alcanzando unos 24,000 infectados. Kaspersky señala que los troyanos, aumentando de 15,000 a 40,000 entre 2022 y 2023, son el malware predominante. Las puertas traseras son consideradas como los troyanos más peligrosos, permitiendo obtener control remoto de los dispositivos, son los más peligrosos, facilitando enviar, recibir, ejecutar y eliminar archivos, recopilar datos confidenciales y registrar actividad de las acciones realizadas a través de la computadora Alberto, M[67].

Por lo que para el año 2022, se registraron un alarmante total de 121,6 millones de nuevas muestras de malware específicamente dirigidas a sistemas Linux. Este dato resalta la creciente importancia de fortalecer de manera urgente las estrategias de ciberseguridad en estos sistemas operativos Monzón[68]. La ciberseguridad ya no se limita únicamente a la prevención de ataques, sino que se ha convertido en una necesidad imperante estar preparado para responder eficazmente a incidentes de seguridad. Esto incluye la capacidad de llevar a cabo investigaciones forenses exhaustivas con el objetivo de identificar, contener y mitigar las amenazas.

De igual manera, la capacidad de respuesta en ciberseguridad es esencial para reducir el impacto de los incidentes en curso y, al mismo tiempo, prevenir futuros ataques Sánchez, F[69]. En un panorama de amenazas en constante evolución, las organizaciones y los profesionales de seguridad informática deben estar equipados

---

[67] Alberto, M. CIBERAMENAZAS AL ALZA: 411,000 ARCHIVOS MALICIOSOS CIRCULARON DIARIAMENTE EN 2023. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.estamosenlinea.com/2023/12/29/ciberamenazas-al-alza-411000-archivos-maliciosos-circularon-diariamente-en-2023/

[68] Monzón, T. (2021). CYBER SECURITY MAGAZINE. [En línea]. Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internet https://csecmagazine.com/2020/12/31/convercienciaguatemala/

[69] Sánchez F. (2021). La importancia de la informática forense como un eslabón en el proceso de ciberseguridad. [En línea]. INCIBE Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internethttps://incibe.gt/wp-content/uploads/2021/09/Revista-Digital-Cybersecurity-Vol5.pdf#page=12

con las herramientas y los conocimientos necesarios para detectar, analizar y responder de manera efectiva a las amenazas cibernéticas en sistemas Linux. Esto implica no solo la implementación de medidas preventivas sólidas, sino también la capacidad de llevar a cabo una respuesta rápida y eficiente cuando se producen incidentes de seguridad. La ciberseguridad se ha convertido en una prioridad crítica en la protección de la información y la infraestructura de las organizaciones en el entorno digital actual.

Así mismo, según Giovanni Vigna, director senior de inteligencia de amenazas de VMware, indicó que Linux, es un sistema operativo ampliamente utilizado en servidores, dispositivos IoT y entornos de nube, por lo que se ha convertido en un objetivo deseado por los ciberdelincuentes en los últimos años debido a que vulnerar o afectar uno de estos sistemas puede ser muy benéfico en materia económica puesto que generalmente se está apuntando a afectar a grandes empresas con un fuerte poder económico que tiene sus servicios más críticos en servicios basados en sistemas operativos Linux. A menudo, la seguridad de las máquinas que ejecutan Linux se pasa por alto, lo que ha dado lugar a un aumento significativo en ataques de malware dirigidos a esta plataforma. Los atacantes explotan debilidades como la autenticación débil, vulnerabilidades sin parchear y la desconfiguración o mala parametrización de los servidores. Además, el malware para Linux se ha vuelto más diverso y sofisticado, incluyendo ransomware, troyanos bancarios y botnets. Este crecimiento en la focalización de Linux puede estar relacionado con la creciente adopción de entornos en la nube que dependen de Linux. Por lo tanto, es esencial que las organizaciones refuercen la seguridad de los sistemas Linux y tomen medidas proactivas para protegerse contra las amenazas

en constante evolución Fiscutean, A[70]. De igual manera se resalta que los seis ataques que más crecimiento ha tenido es:

- Ransomware En los últimos años, ha habido una incursión de bandas de ransomware en los entornos Linux, y aunque la calidad de las muestras de malware varía, grupos como Conti, DarkSide, REvil y Hive están actualizando rápidamente sus habilidades. Los ataques de ransomware en entornos de nube suelen ser meticulosamente planeados, según VMware, con ciberdelincuentes buscando comprometer completamente a la víctima antes de cifrar los archivos. Recientemente, se ha observado que grupos como RansomExx/Defray777 y Cçlzonti se centran en las imágenes de host de Linux utilizadas en entornos virtualizados, indicando una nueva y preocupante tendencia donde los atacantes buscan afectar los activos más valiosos en entornos de nube para causar el máximo daño. Estos grupos muestran un interés particular en cifrar imágenes de máquinas virtuales alojadas en hipervisores ESXi, ya que son conscientes de que esto puede tener un impacto significativo en las operaciones. La creación de nuevos binarios específicos para cifrar máquinas virtuales y sus entornos de gestión es una práctica común en el panorama del ransomware, según un informe de la empresa de seguridad Trellix.
- El criptojacking, se destaca como uno de los tipos más comunes de malware dirigido a sistemas Linux, ya que ofrece la posibilidad de generar ingresos de manera rápida. Este tipo de software tiene como objetivo principal utilizar los recursos informáticos para la minería de criptomonedas en beneficio del atacante, generalmente optando por Monero, según Tokazowski. Un ejemplo notable de este tipo de ataque se remonta a 2018, cuando la nube pública de

[70] Fiscutean, A. (2022, June 3). El ‘malware’ para Linux va en aumento: seis tipos de ataques a tener en cuenta. [En línea]. CSO España. [Citado 24-Noviembre-2024]. Disponible en Internet https://cso.computerworld.es/cibercrimen/el-malware-para-linux-va-en-aumento-seis-tipos-de-ataques-a-tener-en-cuenta

Tesla fue comprometida. En este caso, los ciberdelincuentes lograron infiltrarse en la consola de Kubernetes de Tesla, que carecía de protección mediante contraseña, exponiendo así las credenciales de acceso dentro de un pod de Kubernetes. Estas credenciales proporcionaron acceso al entorno AWS de Tesla, que albergaba un cubo de Amazon S3 con datos sensibles, incluyendo información de telemetría.

La frecuencia del criptojacking ha ido en aumento, destacando XMRig y Sysrv como familias prominentes de criptomineros. Un informe de SonicWall reveló un aumento del 19% en los intentos de criptojacking en 2021 en comparación con 2020. En entornos gubernamentales y de salud, este incremento fue aún más pronunciado, con un crecimiento del 709% y 218%, respectivamente, según el informe. Para llevar a cabo estos ataques, muchas bandas recurren a contraseñas por defecto, exploits bash o exploits diseñados específicamente para sistemas mal configurados con débiles medidas de seguridad, como desconfiguraciones que involucran ataques de cruce de directorios, inclusión remota de archivos, o aprovechamiento de procesos mal configurados con instalaciones predeterminadas.

- Tres familias de malware, XorDDoS, Mirai y Mozi, están dirigidas al Internet de las cosas (IoT) basado en Linux. El Internet de las Cosas (IoT), en su gran mayoría, opera en entornos basados en Linux, y la naturaleza sencilla de estos dispositivos los vuelve susceptibles a amenazas. Según CrowdStrike, el volumen de malware dirigido a dispositivos IoT con sistema Linux aumentó significativamente, registrando un crecimiento del 35% en 2021 en comparación con 2020. Dentro de este panorama, tres familias de malware, XorDDoS, Mirai y Mozi, representan el 22% del total. Estos malwares siguen un patrón común al infectar dispositivos, integrarlos en una red de bots y utilizarlos para llevar a cabo ataques de denegación de servicio (DDoS).

  Mirai, considerado el ancestro común de muchos malwares DDoS de Linux, utiliza tácticas de fuerza bruta en Telnet y Secure Shell (SSH) para

comprometer dispositivos. Tras la publicación de su código fuente en 2016, surgieron múltiples variantes que los desarrolladores de malware incorporaron en sus propios troyanos. Según CrowdStrike, el número de variantes de malware Mirai para sistemas Linux con tecnología Intel se duplicó considerablemente en el primer trimestre de 2022 en comparación con el mismo período de 2021, especialmente dirigido a procesadores x86 de 32 bits. XorDDoS, otro troyano destacado, experimentó un aumento del 254% en los últimos seis meses, utilizando tácticas similares de fuerza bruta y escaneo en busca de servidores Docker para obtener acceso remoto al host. Mozi, por su parte, bloquea puertos SSH y Telnet, establece redes de botnets peer-to-peer y emplea sistemas de tabla de hash distribuida (DHT) para ocultar su comunicación, asegurando la persistencia de la infección a lo largo del tiempo, según el informe de Fortinet.

- Los ataques patrocinados por estados, Los expertos en seguridad han detectado un aumento en la orientación de grupos de estados nacionales hacia entornos Linux. Según Ryan Robinson, investigador de seguridad de Intezer, se ha desplegado considerablemente malware para Linux durante el conflicto entre Rusia y Ucrania, con la participación del grupo ruso APT Sandworm, que habría atacado sistemas Linux de agencias británicas y estadounidenses justo antes del inicio del conflicto.

  ESET, una empresa de ciberseguridad, observó de cerca las implicaciones del conflicto y siguió el ataque denominado Industroyer2, dirigido a un proveedor de energía ucraniano. Marc-Étienne Léveillé, investigador senior de malware en ESET describe este ataque como altamente dirigido, utilizando gusanos de Linux y Solaris que se propagaban mediante SSH y posiblemente credenciales robadas. El malware de limpieza utilizado por Sandstorm APT, asociado a este ataque, destruye el contenido de los discos conectados al sistema, utilizando shred o dd, acelerando el proceso si hay varios discos conectados.

En el ámbito de los actores de estados-nación, Microsoft y Mandiant señalaron que diversos grupos respaldados por China, Irán, Corea del Norte y otros, han estado aprovechando la famosa vulnerabilidad Log4j en sistemas Windows y Linux para obtener acceso a las redes objetivo. Este aumento de actividades respaldadas por estados en entornos Linux destaca la creciente importancia de la ciberseguridad en este ámbito.

- Ataques sin archivos, Los expertos en seguridad de Alien Labs de AT&T observaron que varios actores, incluido TeamTNT, han adoptado Ezuri, una herramienta de código abierto desarrollada en Golang. Estos atacantes emplean Ezuri para cifrar el código malicioso, y al descifrarlo, la carga útil se ejecuta directamente desde la memoria, evitando dejar rastros en el disco y dificultando su detección por parte del software antivirus. TeamTNT, el grupo principal vinculado a esta táctica concentra sus esfuerzos en sistemas Docker mal configurados, buscando instalar bots, DDoS y cripto mineros.
- El malware de Linux puede dirigirse a máquinas Windows El malware de Linux tiene la capacidad de aprovechar las máquinas con sistema operativo Windows mediante el Subsistema de Windows para Linux (WSL), una función que permite ejecutar binarios de Linux de manera nativa en Windows. Para llevar a cabo ataques o asegurar persistencia en máquinas Windows mediante WSL, los atacantes pueden instalar manualmente WSL o unirse al programa Windows Insider. Qualys, una empresa de seguridad en la nube evaluó la viabilidad de dos técnicas: ejecución por proxy e instalación de utilidades, concluyendo que ambas son altamente factibles. Se sugiere a las organizaciones desactivar la virtualización y la capacidad de instalar WSL para protegerse contra este tipo de ataques, y realizar auditorías continuas de los procesos en ejecución.

  Además, los atacantes están trasladando la funcionalidad de las herramientas de Windows a Linux para ampliar sus objetivos. Vermilion Strike, un ejemplo de esta tendencia, se basa en CobaltStrike, una popular

herramienta de pruebas de penetración para Windows. Vermilion Strike puede utilizarse tanto en Windows como en Linux, ofreciendo a los atacantes muchas capacidades de acceso remoto, manipulación de archivos y ejecución de comandos de shell. Esta herramienta ha sido utilizada para realizar espionaje contra empresas de telecomunicaciones, agencias gubernamentales e instituciones financieras. Los investigadores de Intezer señalan que "Vermilion Strike podría no ser la última implementación en Linux" de CobaltStrike Beacon.

Según Mario Micucci[71], de ESET y basado en los datos históricos de los registros de vulnerabilidades en la base de datos CVE, resaltando que, en relación con Debian Linux, se registra un historial de 7489 vulnerabilidades documentadas desde 1999 hasta 2022. En el año 2022, se reportaron 720 vulnerabilidades, siendo 2018 el año con el mayor número, llegando a 1407. En cuanto a la gravedad, de las 720 incidencias de 2022, solo 14 fueron consideradas críticas, y 109 posibilitaron la ejecución de código.

Así mismo, el ransomware en Linux representa una amenaza significativa para la infraestructura crítica, y las organizaciones que dependen de distribuciones de Linux deben ser proactivas en la defensa de sus sistemas contra estos ataques, así como lo mencionó Jon Miller[72], en su artículo “Linux Ransomware Poses Significant Threat to Critical Infrastructure”, que si bien Linux es menos visible en equipos personales en comparación con Windows, este desempeña un papel crucial tras bastidores, ejecutando la mayoría de los servidores web, dispositivos IoT en energía y

[71] Micucci, M. (2023). Vulnerabilidades reportadas en 2022 aumentaron 26% y alcanzaron nuevo récord histórico. [En línea]. WeLiveSecurity. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.welivesecurity.com/la-es/2023/01/12/vulnerabilidades-reportadas-2022-aumentaron-record-historico/

[72] Miller, J. (2023). Linux Ransomware Poses Significant Threat to Critical Infrastructure. [En línea]. Dark Reading. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.darkreading.com/vulnerabilities-threats/linux-ransomware-poses-significant-threat-to-critical-infrastructure

manufactura, redes gubernamentales y militares de EE. UU., sistemas financieros y la columna vertebral de Internet.

Además, Jon Miller, asevera que a pesar de su prevalencia en operaciones críticas, Linux a menudo pasa desapercibido en términos de seguridad, ya que la mayoría de las soluciones de seguridad para puntos finales lo descuidan, reflejo de esto es que para el 2022, los ataques de ransomware en sistemas Linux aumentaron en un 75%, con grupos notorios como Conti, LockBit, RansomEXX, REvil y Hive dirigiéndose cada vez más a Linux, así como también, actores de amenazas menos conocidos, como Black Basta, IceFire, HelloKitty, BlackMatter y AvosLocker, también están mejorando sus capacidades para afectar sistemas operativos Linux, un ejemplo de esta situación se registró con el grupo cibercriminal llamado "RansomEXX", quien diseña malware tipo Ransomware con el mismo nombre de la organización, específicamente para atacar sistemas Linux, y ha sido utilizado en ataques dirigidos a organizaciones de alto perfil, como el gobierno brasileño en 2021 y el Departamento de Transporte de Texas en 2022; este malware se presenta en forma de un binario ELF de 64 bits programado en C y compilado con GCC Cynet[73].

En el ámbito de Android, se alcanzó un récord histórico en 2022 con 899 vulnerabilidades notificadas, superando el registro de 2020, que hasta ese momento ostentaba el mayor número con 859. De las vulnerabilidades comunicadas en 2022, 43 fueron catalogadas como de alta criticidad, y 102 permitieron la ejecución de código. En el periodo acumulado desde 2009 hasta 2022, se contabilizaron 4902 vulnerabilidades en Android Micucci; M[74].

---

[73] Cynet. (2023). Linux Ransomware Attack: Anatomy, Examples and Protection. [En línea]. Cynet. Estados Unidos. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.cynet.com/ransomware/linux-ransomware-attack-anatomy-examples-and-protection/

[74] Micucci, M. (2023). Vulnerabilidades reportadas en 2022 aumentaron 26% y alcanzaron nuevo récord histórico. [En línea]. WeLiveSecurity. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.welivesecurity.com/la-es/2023/01/12/vulnerabilidades-reportadas-2022-aumentaron-record-historico/

En lo que respecta a Fedora, figura como el tercer sistema operativo con más vulnerabilidades documentadas desde 2007 hasta 2022, sumando un total de 4108. Durante 2022, se informaron 906 vulnerabilidades, de las cuales 84 posibilitaron la ejecución de código, Semana[75].

Lo anteriormente mencionado se evidenció en la siguiente grafica del Top de la cantidad de vulnerabilidades identificadas en el año 2023 para cada uno de los sistemas operativos, en la base de datos de vulnerabilidades CVE[76].

[75] eSemana. (2023). Durante 2022 se incrementaron en 26% las vulnerabilidades informáticas. [En línea]. ESET. [Citado 24-Noviembre-2024]. Disponible en Internet https://esemanal.mx/2023/01/eset-durante-2022-se-incrementaron-en-26-las-vulnerabilidades-informaticas/

[76] CVE (2023). Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2023. [En línea]. Common Vulnerabilities and Exposures. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.cvedetails.com/top-50-products.php?year=2022

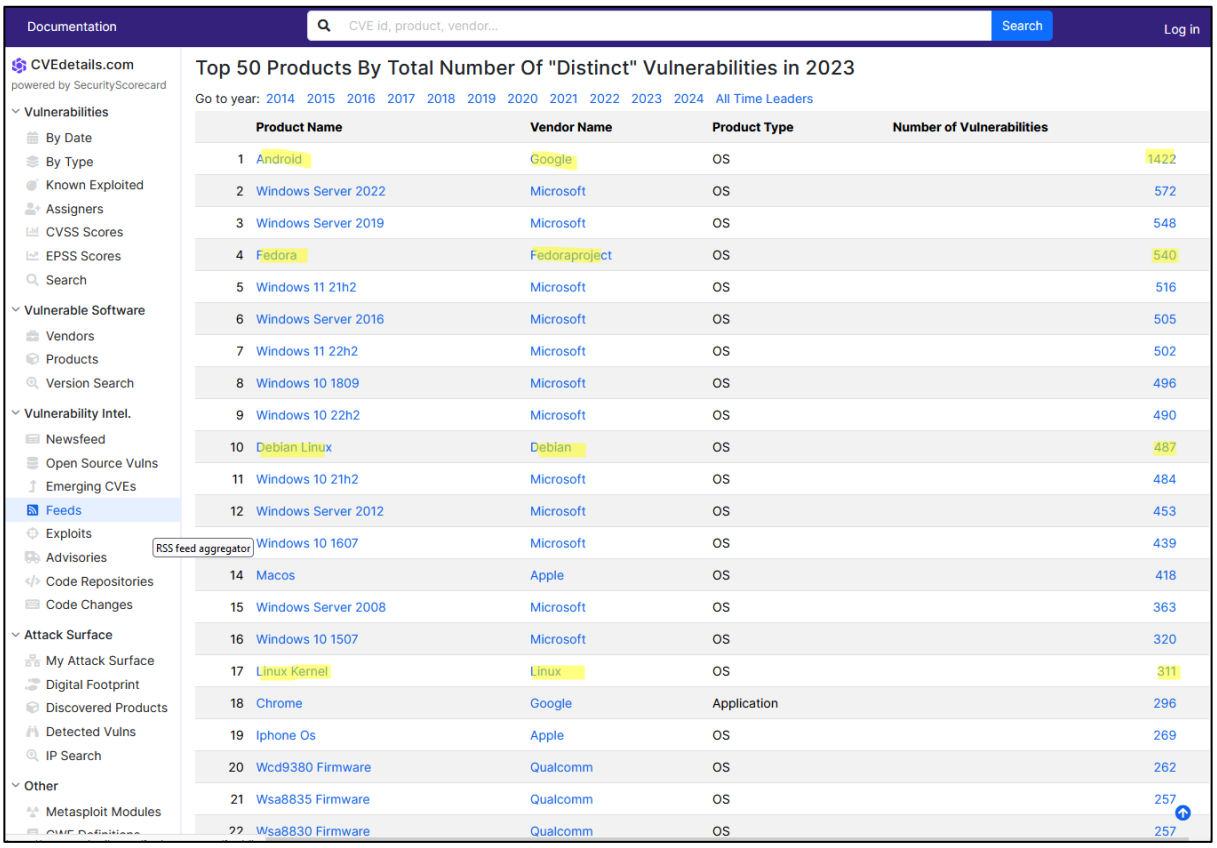


Figura 4 Cantidad de vulnerabilidades detectadas en el 2023 por sistemas operativos.

Fuente: CVE (2023). Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2023. Common Vulnerabilities and Exposures. Recuperado de https://www.cvedetails.com/top-50-products.php?year=2023

Según IT DIGITAL SECURITY[77], en su publicación “Aumentan los ciberataques dirigidos contra dispositivos basados en Linux”, indicaron que, con el fin de salvaguardar sus sistemas, los departamentos de Tecnologías de la Información (TI) optan cada vez más por el uso de Linux. No obstante, grupos de amenazas como Barium, Sofacy o Turla están respondiendo a esta tendencia mediante la creación de herramientas avanzadas que pueden vulnerar dichos sistemas. A pesar

[77] IT DIGITAL SECURITY. 2020. Aumentan los ciberataques dirigidos contra dispositivos basados en Linux. [En línea]. IT DIGITAL SECURITY. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.itdigitalsecurity.es/endpoint/2020/09/aumentan-los-ciberataques-dirigidos-contra-dispositivos-basados-en-linux

de que muchas organizaciones prefieren Linux para servidores y sistemas críticos, considerándolo más seguro que el sistema operativo Windows, los investigadores de Kaspersky han identificado un aumento en los ataques dirigidos a dispositivos basados en Linux.

Además, según la firma ITRESELLER[78], en su publicación "Los actores de amenazas diversifican su arsenal con herramientas Linux", se destaca que, en los últimos ocho años, más de una docena de Actores de Amenazas Persistentes Avanzadas (APT) han integrado malware específico para Linux o módulos basados en este sistema en sus operaciones, entre estos actores se encuentran grupos notorios como Barium, Sofacy, Lamberts y Equation, así como campañas más recientes como LightSpy de TwoSail Junk y WellMess. Ya que a medida que la seguridad en entornos Windows ha mejorado, los actores de amenazas han ampliado su enfoque hacia plataformas menos monitoreadas, como Linux, buscando eludir detecciones y persistir a largo plazo en sistemas comprometidos, demostrando además la capacidad de los atacantes para llevar a cabo operaciones de manera más complejas, efectivas y con un alcance más amplio, mediante la creciente sofisticación y diversificación de las amenazas cibernéticas diseñadas específicamente para dicho sistema operativo.

Para cambiar la citación a una citación basada en autor, el autor se convierte en el foco de la oración y se menciona explícitamente al principio, sin paréntesis. Aquí está el texto ajustado:

De igual manera, Özeren S.[79], en su artículo publicado en octubre, destaca que los actores de amenazas Kinsing están realizando explotación de una vulnerabilidad

---

[78] IT RESELLER. (2020). Los actores de amenazas diversifican su arsenal con herramientas Linux. [En línea]. IT RESELLER TECH & CONSULTING. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.itreseller.es/seguridad/2020/09/los-actores-de-amenazas-diversifican-su-arsenal-con-herramientas-linux

[79] Özeren, S. (2023, 13 de noviembre). October 2023: Key Threat Actors, Malware and Exploited Vulnerabilities. [En línea]. THE COMPLETE SECURITY VALIDATION PLATFORM. [Citado 24-

reciente en Linux, identificada como CVE-2023-4911 o "Looney Tunables". Esta vulnerabilidad, originada en el cargador dinámico de la biblioteca GNU C, permite realizar un escalamiento de privilegios local permitiendo a los atacantes manipular la variable 'GLIBC_TUNABLES', alterando el comportamiento en tiempo de ejecución de la biblioteca y provocando un desbordamiento de búfer. Esto les permite redirigir la ruta de búsqueda de la biblioteca y cargar una versión maliciosa de 'libc.so', obteniendo acceso raíz en sistemas Linux.

Además, Özeren señala la aparición del malware Wiper BiBi-Linux, una herramienta cibernética destructiva dirigida contra organizaciones israelíes. Este malware, al obtener acceso raíz, puede borrar directorios especificados o, en ausencia de una ruta concreta, eliminar todos los archivos del directorio raíz. Este enfoque enfatiza la importancia de proteger los sistemas operativos Linux ante amenazas emergentes y la capacidad de ciertos malwares de explotar vulnerabilidades críticas para ganar control total sobre los sistemas afectados.

De igual manera, la Asolación de Informáticos del Uruguay (AsIAP)[80], resaltaron en su publicación “Los servidores y equipos Linux, en el punto de mira de los ciber atacantes”, que, si bien los ataques dirigidos a sistemas Linux son aún poco comunes, existen malware diseñados para ellos, como webshells, puertas traseras, rootkits y exploits personalizados. A pesar de la baja frecuencia de estos ataques, el compromiso exitoso de un servidor que ejecuta Linux puede tener consecuencias significativas. Los atacantes pueden no solo acceder al dispositivo infectado, sino también a los endpoints que ejecutan sistemas operativos como Windows o macOS, lo que brinda un acceso más extenso y potencialmente inadvertido. Ejemplos notables incluyen el cambio en las tácticas de Turla, que ha incorporado puertas

---

Noviembre-2024]. Disponible en Internet https://www.picussecurity.com/resource/blog/october-2023-key-threat-actors-malware-and-exploited-vulnerabilities

[80] AsIAP. (s.f.). (2020). Los servidores y equipos Linux en el punto de mira de los ciberatacantes. [En línea]. AsIAP.org. [Página web]. Recuperado el 15 de enero de 2024. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.asiap.org/AsIAP/index.php/noticias-de-tecnologia/8525-los-servidores-y-equipos-linux-en-el-punto-de-mira-de-los-ciberatacantes

traseras de Linux en su conjunto de herramientas. Además, Lazarus sigue diversificando su arsenal y desarrollando malware no específico para Windows. Por ejemplo, el marco multiplataforma llamado MATA, asociado a Lazarus, fue reportado por Kaspersky. Estos desarrollos indican una creciente sofisticación de los ataques dirigidos a sistemas basados en Linux, resaltando la importancia de la seguridad en esta plataforma.

Esto se puede corroborar si analizamos el total de vulnerabilidades reportadas en la base de datos del CVE, en donde se evidencia que Debian basado en Linux, es el cuarto fabricante que tiene más vulnerabilidades reportadas para ese año, y si tenemos en cuenta que este sistema operativo está enfocado especialmente en el ámbito empresarial, es un panorama muy preocupante en términos de Ciberseguridad.

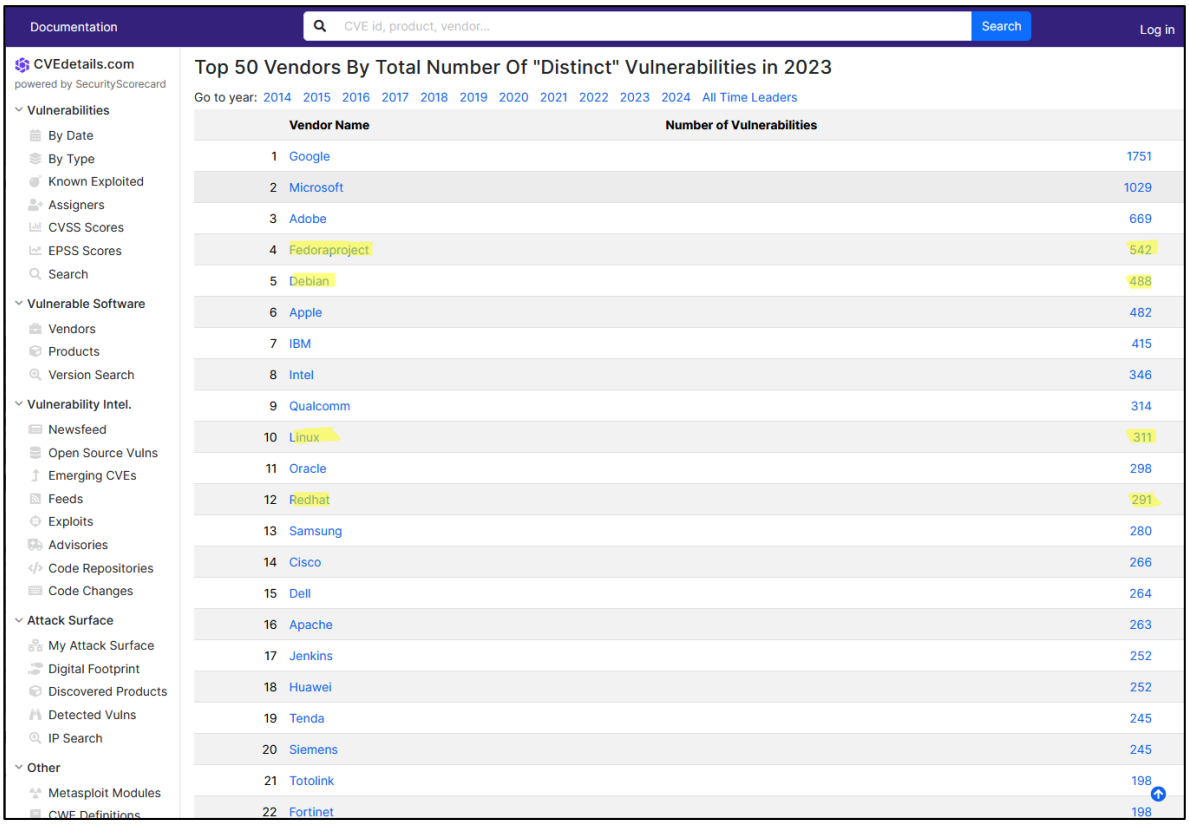


Figura 5 Cantidad de Vulnerabilidades por Fabricante reportadas para el 2023.

Fuente: CVE (2023). Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities in 2023. Common Vulnerabilities and Exposures. Recuperado de https://www.cvedetails.com/top-50-vendors.php?year=2023

En Conclusión, el análisis documental evidencia el aumento en ciberataques dirigidos a sistemas operativos Linux, lo que pone de manifiesto la creciente vulnerabilidad de esta plataforma, a pesar de su percepción histórica de seguridad. Con más de 121 millones de nuevas muestras de malware específico para Linux en 2022, se subraya la urgente necesidad de fortalecer las estrategias de ciberseguridad en este entorno, especialmente dado su papel crítico en servicios empresariales. La diversificación de tácticas, desde ransomware hasta ataques sin archivos, resalta la complejidad de las amenazas a las que se enfrenta Linux.

Además, la elevada cantidad de vulnerabilidades documentadas, especialmente en Debian, resalta la imperante importancia de contar con procesos eficaces para investigar incidentes en entornos Linux. Esta conclusión refuerza la necesidad de no solo implementar medidas preventivas sólidas, sino también de desarrollar capacidades de respuesta ágiles y exhaustivas que permitan a dar respuestas en las investigaciones forenses o de respuesta a incidentes para identificar las actividades del Ciberdelincuente. Además, en un panorama de amenazas en constante evolución, la ciberseguridad en sistemas Linux ha pasado de ser una simple consideración para convertirse en una prioridad crítica para la protección de la **información y la continuidad operativa de las organizaciones.**

CAPITULO 2: ANÁLISIS A MEMORIA VOLATIL APROVECHANDO FUNCIONALIDADES DE VOLATILITY2.6 CON BASE EN LA CREACIÓN DEL RESPECTIVO PERFIL DEL SISTEMA OPERATIVO

Basado en los tipos de análisis que se pueden realizar a la memoria volátil utilizando las funcionalidades disponibles en Volatility 2.6, se pudo evidenciar como esta herramienta tiene funcionalidades útiles que permiten realizar un análisis de un volcado de memoria de manera ágil, ordenando la información contenida en dicha memoria, como por ejemplo evidenciar los procesos que estaban corriendo en el sistema, servicios en ejecución, registros de auditoría, e inclusive se puede reconstruir un artefacto y extraerlo de un volcado de memoria, por tanto en la revisión documental se encuentra que:

El uso de Volatility en el análisis de malware en entornos Linux se destaca como una herramienta crucial para entender y contrarrestar las amenazas de manera eficiente debido a la automatización de consultas avanzadas, dado que muchos dispositivos utilizan Linux debido a su flexibilidad y naturaleza de código abierto, por lo que se ha convertido en un objetivo para ataques de malware, por lo que Monnappa[81], en su trabajo “Automating Linux Malware Analysis Using Limon Sandbox”, expone los tres tipos de análisis que se realizan con la herramienta Limon Sandbox, las cuales son análisis estático, análisis dinámico y análisis de memoria, resaltando en este último que lo que le permite al Sandbox realizar el análisis de la memoria es la integración de Volatility, además de especifica que si bien en la mayoría de los casos, el análisis estático y dinámico produce resultados suficientes, la memoria es la que ayuda a determinar todo el comportamiento especifico de la ejecución de un archivo malicioso, logrando identificar procesos, cambios en el

[81] Monnappa, K. (2015). Automating linux malware analysis using limon sandbox. [En línea]. Black Hat Europe, 2015, IV-A. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.blackhat.com/docs/asia-16/materials/arsenal/asia-16-KA-Limon-wp.pdf

sistema específicos, artefactos ocultos, rootkits y capacidades de ocultamiento de algunos malware como los malware Fileless utilizando la técnica “Living off the Land”, se ocultan y ejecutan específicamente en la memoria, por lo que no hay otra forma de analizarlos e identificarlos si no se realiza el respectivo análisis de la memoria volátil o RAM Warburton, A[82].

Según Sergio Álvarez[83], en su trabajo de grado “Análisis forense de una infección por malware”, resalta la utilización de herramientas para el análisis de la memoria volátil (RAM), reconociendo que la mejor herramienta para el análisis de memoria RAM es Volatility, ya que este permite analizar volcados sin procesar tanto de equipos como de máquinas virtuales. Así mismo se resalta que la fase más crítica para la investigación de una infección de malware es la extracción y análisis de la memoria volátil, ya que de hacerse incorrectamente se estaría perdiendo pistas que pueden resultar claves para identificar el ataque. Una vez se obtiene la información volátil utilizando “DumpIt”, se realizó el respectivo análisis con “Volatility”, detallando que las actividades de análisis se enfocaron en:

- Procesos en ejecución: Para validar los procesos en ejecución en Volatility se debe hacer uso del comando “PSList”, este genera el listado de todos los procesos que estaba ejecutando el sistema.
- Servicios en ejecución: Este genera el listado de todos los servicios que estaba ejecutando el sistema, para la investigación se usó “PSService”.
- Listado de usuarios: Para el caso de volatility se puede realizar ejecutando el comando “hashdump”, para el caso del trabajo se usó “PSloggedon.exe”.

---

[82] Warburton, A. (2019). Fileless malware: qué es y cómo funciona el malware sin archivos. [En línea]. WeLiveSecurity. [Citado 24-Noviembre-2024]. Disponible en Internethttps://www.welivesecurity.com/la-es/2019/12/05/fileless-malware-que-es-como-funciona-malware-sin-archivos/

[83] Álvarez, S. Análisis forense de una infección por malware. [En línea]. Universidad de Barcelona , 2021. [Citado 24-Noviembre-2024]. Disponible en Internet https://diposit.ub.edu/dspace/bitstream/2445/182840/2/tfg_sergio_agru%c3%b1a_alvarez.pdf

- Actividad en RED: Se usaron los comandos para analizar la actividad en red registrada esto incluye, la información general de red asignada al dispositivo, las conexiones establecidas, cerradas, en espera, los puertos activos y demás relacionado.
- Contenido del cache DNS: Nos trae la información de los dominios que estaba respondiendo el equipo en un momento determinado.
- ARP: Almacena toda la información del MAC y direcciones IP de todos los dispositivos que se han comunicado con el equipo.
- Cabe resaltar que Volatility tiene un amplio espectro de comandos, los cuales deben aplicarse en consideración del investigador dependiendo del escenario y el objetivo de la investigación.

De igual manera, para Ana Haydée Di Iorio, Gonzalo Ruiz de Angeli, Juan Ignacio Alberdi, Hugo Curti, Fernando Greco, Ariel Podestá, Martin Castellote, Bruno Constanzo, Juan Iturriaga y Santiago Trigo[84], en su proyecto de grado "Análisis Forense de Memoria: Malware y Evidencia Oculta", indican que la memoria principal es la memoria que se conecta al procesador directamente a través de un bus interno lo que se conoce como memoria RAM, en el documento detallan un procedimiento para el análisis de memoria RAM, el cual consiste en la realización de las siguientes actividades:

- Generación del Volcado de memoria.
- Reconocimiento de estructuras en la memoria.
- Reconocimiento de relación.
- Análisis automático.
- Análisis forense.

[84] Ana Di Lorio, Gonzalo Angeli, Juan Alberdi, Hugo Curti, Fernando Greco, Ariel Podestá, Martin Castellote, Bruno Constanzo, Juan Iturriaga y Santiago Trigo. (2016). Análisis forense de memoria: malware y evidencia oculta. [En línea]. Universidad FASTA. [Citado 24-Noviembre-2024]. Disponible en Internet http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1547

- Elaboración de conclusiones.

Así mismo, en el mismo proyecto de grado se establece que la estructura de memoria donde se tienen los artefactos ocultos y el malware, en esta estructura resaltan lo siguiente: Procesos, servicios, Hilos (Threads), DLLs, conexiones, hives, artefactos de usuarios, entradas de registro, entre otros. Adicionalmente, en el documento puntualizan que cada proceso en el sistema tiene un proceso padre que desencadena todos los procesos hijos y de manera sucesiva con los procesos que los hijos generen, sin embargo, un malware rompe este ciclo y se convierte generalmente en un proceso huérfano al cual, no se le puede asociar un proceso padre y generalmente los procesos hijos son sospechosos.

Igualmente, según Paula Mejías[85], en su proyecto de grado "Estudio Comparativo De Distribuciones Linux Para Análisis Forense", se establece que la memoria volátil resulta de vital importancia para las investigaciones forenses y las investigaciones de respuesta a incidentes, por lo que se debe hacer uso de VOLATILITY, explicando que este tiene soporte para diversos sistemas operativos mientras siempre y cuando tenga el perfil correspondiente, soportando Windows de 32 y 64 bits, formatos raw, archivos de hibernación, instantáneas de máquinas virtuales, Mac OSX, Android con procesadores ARM. Por otro lado, especifica que Volatility está diseñado para funcionar con Python y algunas librerías específicas, resaltando que Volatility cuenta con dos funcionalidades esenciales incluidos en los complementos, el primero llamado "list", el cual, navega a través del Kernel del sistema operativo lo que permite recuperar información de manera más rápida pero estos tienden a ser muy vulnerables a la manipulación frente a amenazas, y el segundo llamado "scan", que permite realizar actividades de "data carving", en la memoria y buscar estructuras específicas, lo que permite a su vez recuperar la mayor cantidad de

[85] Mejías, P. (2021). ESTUDIO COMPARATIVO DE DISTRIBUCIONES LINUX PARA ANÁLISIS FORENSE. ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y SISTEMAS DE TELECOMUNICACIÓN. [En línea]. Madrid. [Citado 24-Noviembre-2024]. Disponible en Internet https://oa.upm.es/70654/1/TFG_PAULA_CARBONE_MEJIAS.pdf

información disponible en la memoria volátil, así como la extracción de artefactos, pero también es propenso a traer falsos positivos.

Así mismo, según indica Rahul Varshney ,Nitesh Kumar ,Anand Handa y Sandeep Kumar Shukla[86], en su trabajo "Perfiles personalizados de Volatility para la detección automatizada de malware ELF híbrido", para realizar análisis efectivos de archivos binarios maliciosos de tipo ELF (Executable and Linkable Format) en entornos basados en Linux, se requiere conocer Volatility y su proceso para lograr crear un perfil personalizado de acuerdo con el sistema operativo Linux exacto sobre el cual se va a realizar el volcado de memoria RAM y su posterior análisis, para que Volatility pueda mapearlo, ejecutar los comandos y extraer la información de manera efectiva de dicho volcado, puesto que los ELF se almacena información en la memoria RAM cuando se ejecuta, así como también, el sistema operativo asigna espacio en la memoria RAM para almacenar el código ejecutable, datos y otras secciones necesarias y relevantes para comprender el comportamiento del ELF malicioso. Por tanto, ellos profundizan e indican que se hace indispensable utilizar Volatility para apoyar en la tarea de automatizar procesos y optimizar esfuerzos cuando se presenta una infección por malware con ejecutables de Linux en formato ELF y se requiere una respuesta a incidentes o una investigación forense.

De la misma manera, según Richard Carbone[87], investigador del área de investigación y desarrollo de defensa de Canadá, en sus resultados presentados en el documento "Malware memory analysis of the IVYL Linux rootkit", lo primero que resalta es la diferencia entre analizar la memoria volátil o RAM usando Volatility en

[86] Varshney, R., Kumar, N., Handa, A., & Shukla, S. K. (2022, November). Volatility Custom Profiling for Automated Hybrid ELF Malware Detection. [En línea]. In International Conference on Digital Forensics and Cyber Crime (pp. 274-291). Cham: Springer Nature Switzerland.

[8787] Carbone, R., & Defence Research and Development Canada-Valcartier Research Centre Quebec, Quebec Canada. (2015). Malware Memory Analysis of the IVYL Linux Rootkit: Investigating a Publicly Available Linux Rootkit Using the Volatility Memory Analysis Framework. [En línea]. Defence Research and Development Canada-Valcartier Research Centre Quebec, Quebec Canada. [Citado 24-Noviembre-2024]. Disponible en Internethttps://apps.dtic.mil/sti/citations/AD1004349

un ambiente Windows y Linux, explicando que la primera diferencia radica en que para poder utilizar correctamente Volatility y analizar un volcado de memoria en un ambiente Linux se requiere crear el perfil exacto del sistema operativo Linux asociado a ese volcado de memoria, mientras que en Windows se pueden correr varios comandos o incluso utilizar algunos comandos generales o utilizar algún perfil de un sistema operativo Windows genérico según la versión ejecutada, y la segunda diferencia radica en que algunos comandos o funcionalidades de Volatility pueden no estar compatibles aun cuando se tenga el perfil correcto, sin embargo, la creación del perfil si bien es resalta de vital importancia para realizar un correcto análisis del volcado de memoria en Linux, no detalla el procedimiento para realizar dicha creación del perfil. De igual manera, en el trabajo es un proceso para realizar el análisis de los volcados de la memoria enfocados en la identificación de un Rootkit, siendo lo más relevante para la presente investigación la ejecución de algunos comandos o “complementos” como los siguientes:

- Linux_banner: Utilizado para determinar información del kernel, información de la versión y arquitectura del sistema operativo Linux.
- Linux_cpuinfo: Utilizado para identificar el tipo y la cantidad de CPU que está en uso en el equipo en el momento de la realización del volcado de memoria.
- Linux_dmesg: Utilizada para extraer y analizar el buffer del kernel de mensajes (dmesg) de un sistema Linux volátil. El buffer de mensajes del kernel almacena mensajes generados por el kernel del sistema operativo, que pueden ser útiles para el análisis forense y la investigación de incidentes.
- Linux_iomem: Utilizada para analizar y presentar información sobre el espacio de entrada/salida de memoria (I/O memory) en sistemas Linux volátiles. El espacio de I/O memory es una región de la memoria que se utiliza para mapear registros de hardware y facilitar la comunicación entre el sistema operativo y los dispositivos periféricos.

- Linux_slabinfo: Utilizada para analizar y presentar información sobre el caché de objetos SLAB en sistemas Linux volátiles. Este comando solo funcionará con imágenes de memoria que utilicen el kernel 2.6.22 y versiones anteriores. Los kernels 2.6.23 y posteriores, de forma predeterminada, utilizan la gestión de memoria basada en SLUB.
- Linux_mount: Utilizado para analizar y presentar información sobre los puntos de montaje y los sistemas de archivos montados en un sistema Linux.
- Linux_psaux: Utilizado para generar el listado completo de todos los procesos del sistema, es lo mismo que ejecutar en una termina el comando ps -aux.
- Linux_pslist: Muestra una lista simple de procesos que estaban en ejecución en el sistema en el momento de la captura de memoria. Incluye información básica como el PID y el nombre del proceso.
- Linux_pslist_cache: Similar a linux_pslist, pero utiliza información en caché para acelerar el análisis. Puede ser útil para sistemas con un gran número de procesos.
- Linux_pstree: Genera un árbol de procesos que representa las relaciones padre-hijo entre los procesos en el sistema.
- Linux_pidhashtable: Proporciona acceso a la tabla de hash de PID, lo que permite buscar información sobre un proceso específico más rápidamente.
- Linux_psxview: Muestra información sobre procesos ocultos o alterados. Puede ser útil para detectar rootkits u otras técnicas de ocultamiento de procesos.

También, según lo indicado por Gaurav Kamathe[88] en su publicación “Realice análisis forenses de memoria de Linux con esta herramienta de código abierto”, Volatility debe conocer el sistema y la arquitectura de donde se adquirió el volcado de memoria antes de extraer la información. Es por esta razón que existen una serie de comandos por medio de los cuales es posible identificar esta información y para ello es necesaria la creación de los perfiles personalizados. Así mismo, se presenta identifican algunos complementos asociados a las búsquedas de información a través de la herramienta Volatility para los cuales se presentarán algunos a continuación:

- linux_psaux: Es utilizado para verificar algunos procesos que se estaban ejecutando al interior del sistema operativo al momento de realizar el volcado de memoria.
- linux_netstat: Permite identificar el estado de las conexiones de red cuando se realiza el proceso de volcado de memoria y sockets en escucha en un sistema Linux al momento del volcado de memoria.
- linux_lsmod: Es utilizado para identificar los módulos del kernel que se cargaron al interior del sistema.
- linux_bash: permite encontrar los comandos ejecutados por el usuario almacenados en el historial del bash, busca en la memoria volcada para encontrar instancias del shell de bash y extrae los comandos que se han ejecutado en cada sesión de bash.
- linux_lsof: Es utilizado para listar los archivos que fueron abiertos y los procesos asociados a esos archivos, Es útil para investigar qué archivos estaban siendo accedidos o manipulados por procesos específicos.

[88] Kamathe, G. (2021) Realice análisis forenses de la memoria de Linux con esta herramienta de código abierto, Descubra qué sucede con las aplicaciones, las conexiones de red, los módulos del kernel, los archivos y mucho más con Volatility. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://opensource.com/article/21/4/linux-memory-forensics

El software Volatility 2.6 se destaca como una herramienta esencial en el campo del análisis forense y las investigaciones de respuesta a incidente para realizar el respectivo análisis de la memoria volátil, especialmente en la detección y análisis de malware. Su capacidad para manejar volcados de memoria de manera eficiente ya sea de sistemas físicos o máquinas virtuales, lo convierte en una opción indispensable para los investigadores, esta permite un análisis detallado y organizado de diversos aspectos como procesos en ejecución, servicios activos, actividad de red, y contenido de caché DNS. Además, su amplia gama de comandos ofrece flexibilidad para adaptarse a diferentes escenarios investigativos.

Así mismo, se resalta la importancia de un correcto análisis de la memoria volátil en investigaciones forenses e investigaciones de respuesta a incidentes, haciendo énfasis en que una extracción y análisis inadecuados pueden resultar en la pérdida de información crucial. También destacan la relevancia de entender los perfiles que permiten que volatility reconozca un sistema operativo determinado y pueda realizar su correcto análisis, así como la estructura de la memoria y la relación entre los diferentes elementos, como procesos y servicios, para identificar actividades sospechosas, procesos huérfanos típicos de un malware, entre otros.

En conclusión, Volatility se consolida como una herramienta imprescindible en el análisis forense y las investigaciones de respuesta a incidentes relacionados a los análisis de la memoria volátil, por lo que se debe conocer cómo crear y utilizar los “profiles”, que permite que la herramienta pueda reconocer y analizar determinado sistema operativo, lo que brinda al investigador las capacidades de análisis profundo y adaptabilidad, cruciales para la investigación eficaz de infecciones por malware, incidentes de ciberseguridad, investigaciones forenses, identificar técnicas, tácticas o procedimientos o artefactos utilizados por el atacante u otras amenazas cibernéticas.

7.2 PROCEDIMIENTO PARA LA CREACIÓN DE PERFILES EN VOLATILITY 2.6 PARA EL ANÁLISIS DE MEMORIA VOLATIL.

Para la creación de perfiles tenemos autores como Luis Guillén Civera[89], en su artículo “Análisis forense con Volatility en Virtualbox y Ubuntu”, en donde describe cómo realizar la creación de un perfil de un sistema operativo basado en Linux para el posterior análisis de la memoria volátil, indicando que el primer paso es la descarga de la herramienta Volatility2.6, la cual puede obtenerse desde el siguiente repositorio:

- wget http://downloads.volatilityfoundation.org/releases/2.6/volatility_2.6_lin64_standalone.zip

Posteriormente, es posible visualizar si el programa está funcionando, utilizando la sentencia “volatility –help” con la cual, se despliegan las opciones de ayuda de la herramienta, al igual que los diferentes plugins que se pueden utilizar para analizar archivos de volcado de memoria, otro comando relevante es “volatility –info | grep “profile””, el cual lista los perfiles con los que cuenta en ese momento la herramienta y por ende los sistemas operativos soportados. Además, otro dato relevante de Volatility para tener en cuenta para el análisis de Linux, está relacionado con la ruta “Address spaces” donde se encuentra:

- LinuxAMD64PagedMemory El cual es utilizado para identificar un tipo de perfil o implementación de manejo de memoria específicamente diseñado para analizar volcados de memoria de sistemas Linux de 64 bits.
- VirtualBoxCoreDumpElf64 El cual está relacionado a un perfil específico utilizado para analizar volcados de memoria de máquinas virtuales que se

[89] Guillen, L. (2018, 1 de febrero). AnÃ¡lisis forense con Volatility en Virtualbox y Ubuntu. [En línea]. Luis GuillÃ©n Civera. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.luisguillen.com/posts/2018/01/analisis-forense-volatility-virtualbox-ubuntu/

ejecutan en VirtualBox y que posteriormente nos permitirá analizar este volcado de memoria.

Así mismo, en el artículo el autor registro cuatro recomendaciones generales para la creación del perfil en un equipo objetivo, la cual consta de:

- Crear un snapshot.
- Instalar las herramientas requeridas (por ejemplo, Python 2.6, Python 2.7).
- Crear el perfil, y exportar el resultado.
- Restaura el snapshot.

De igual manera asevera que Volatility usa diferentes tipos de datos para trabajar con los diferentes sistemas operativos, y puesto que las estructuras del kernel de Linux cambia con respecto a cada versión y compilación, lo que genera la necesidad de crear un perfil nuevo por cada compilación para poder realizar el respectivo análisis Volátil, puesto que el repositorio oficial carece de actualizaciones constantes Guillen; L[90], como se evidencia en la imagen a continuación.

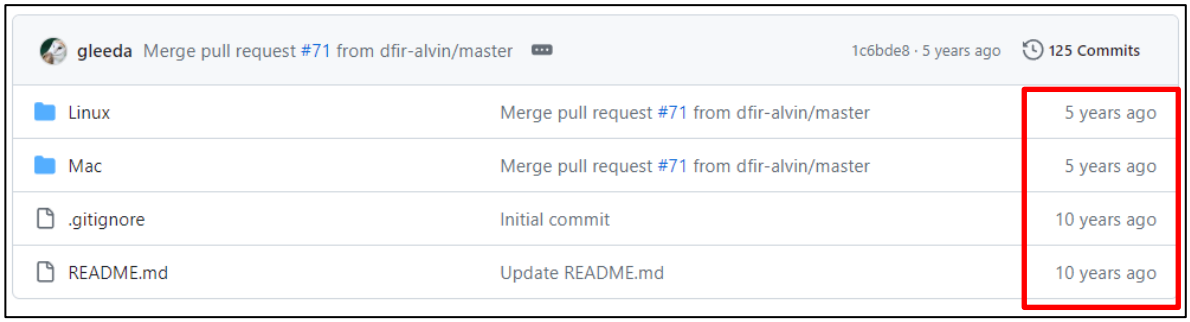


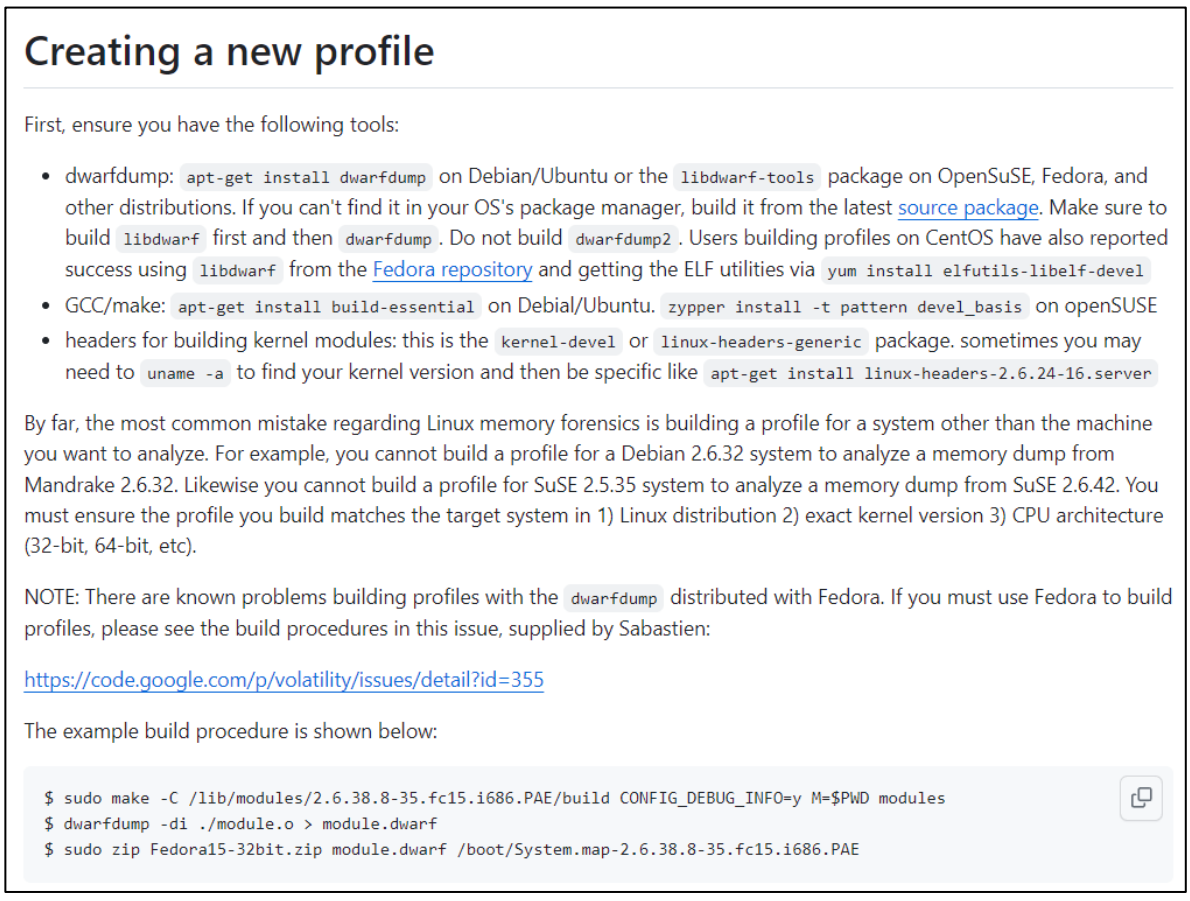
Figura 6 Repositorio Oficial Volatility sección Profiles.

Fuente: Volatility Foundation (2019). GitHub/VolatilityFoundation/profiles. Recuperado de https://github.com/volatilityfoundation/profiles

[90] Guillen, L. (2018, 1 de febrero). AnÃ¡lisis forense con Volatility en Virtualbox y Ubuntu. [En línea]. Luis GuillÃ©n Civera. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.luisguillen.com/posts/2018/01/analisis-forense-volatility-virtualbox-ubuntu/

Por lo tanto, en un escenario real, el primer paso que se debe realizar es descartar que el perfil del sistema operativo Linux al cual se le va a realizar el análisis del volcado de memoria no exista en el repositorio antes mencionado.

Luego, se debe realizar el paso a paso que indica Volatility en su repositorio de Github para la creación del respectivo perfil, pero como se evidenció en las respectivas pruebas documentadas posteriormente, este procedimiento supone que el sistema operativo objetivo ya cuenta con algunas aplicaciones y librearías, lo cual en un escenario real puede generar diversos errores o incompatibilidades. A continuación, la sección donde indican como crear el perfil en Volatility2.6.



Creating a new profile

First, ensure you have the following tools:

- dwarfdump: `apt-get install dwarfdump` on Debian/Ubuntu or the `libdwarf-tools` package on OpenSuSE, Fedora, and other distributions. If you can't find it in your OS's package manager, build it from the latest source package. Make sure to build `libdwarf` first and then `dwarfdump`. Do not build `dwarfdump2`. Users building profiles on CentOS have also reported success using `libdwarf` from the Fedora repository and getting the ELF utilities via `yum install elfutils-libelf-devel`
- GCC/make: `apt-get install build-essential` on Debial/Ubuntu. `zypper install -t pattern devel_basis` on openSUSE
- headers for building kernel modules: this is the `kernel-devel` or `linux-headers-generic` package. sometimes you may need to `uname -a` to find your kernel version and then be specific like `apt-get install linux-headers-2.6.24-16.server`

By far, the most common mistake regarding Linux memory forensics is building a profile for a system other than the machine you want to analyze. For example, you cannot build a profile for a Debian 2.6.32 system to analyze a memory dump from Mandrake 2.6.32. Likewise you cannot build a profile for SuSE 2.5.35 system to analyze a memory dump from SuSE 2.6.42. You must ensure the profile you build matches the target system in 1) Linux distribution 2) exact kernel version 3) CPU architecture (32-bit, 64-bit, etc).

NOTE: There are known problems building profiles with the `dwarfdump` distributed with Fedora. If you must use Fedora to build profiles, please see the build procedures in this issue, supplied by Sabastien:

https://code.google.com/p/volatility/issues/detail?id=355

The example build procedure is shown below:

```
$ sudo make -C /lib/modules/2.6.38.8-35.fc15.i686.PAE/build CONFIG_DEBUG_INFO=y M=$PWD modules
$ dwarfdump -di ./module.o > module.dwarf
$ sudo zip Fedora15-32bit.zip module.dwarf /boot/System.map-2.6.38.8-35.fc15.i686.PAE
```

Figura 7 Sección de Volatility para la creación del Perfil.

Fuente: Volatility Foundation (2019). Linux. Recuperado de https://github.com/volatilityfoundation/volatility/wiki/Linux.

Teniendo en cuenta la información mencionada anteriormente, se realizará una recomendación para la creación del perfil aplicando la guía oficial, esta recomendación se aplica en un ambiente virtualizado, donde se tiene un sistema operativo que estaría instalado en cualquier organización, el cual, no tiene por defecto la herramienta Volatility instalada, puesto que esta es utilizada para procesos forenses específicos, por tanto, es poco común que la tengan instalada en los equipos.

Para la realización de dicho proceso se realizan las siguientes aseveraciones:

1. Se realizará el proceso aplicando la guía oficial, por tanto, si la documentación presenta deficiencias o falta de información de algún complemento se continuará con dicho proceso hasta que se genere un error que impida continuar con el procedimiento el cual quedará documentado.
2. Si bien el enfoque del documento no está enfocado en la instalación de la herramienta Volatility, si se aclara que la documentación de instalación es demasiado general, por lo que para la correcta instalación puede generar algunos errores diferentes, por tanto, para el presente procedimiento se instala todas las herramientas necesarias asegurando que Volatility funcione correctamente, sin embargo, esto no asegura que la creación del perfil se realice de manera correcta puesto que puede necesitar herramientas o complementos diferentes que no a aparecen ni siquiera listados en la guía oficial de Volatility.

Adicionalmente, se indicarán los pasos que se van a realizar, existiendo pasos adicionales que se dejaran plasmados más no documentados puesto que son muy genéricos y no aportan al proceso (p. ej. como lo es la instalación del sistema operativo o la creación de los SnapShot), los cuales son:

1. Acceso al sistema operativo al cual se le va a realizar el procedimiento.
2. Creación de snapshot o instantáneas.

3. Revisión de la existencia de un perfil ya creado para la versión exacta del sistema operativo.
4. Verificación del funcionamiento de Volatility
5. Verificación de la instalación de las herramientas necesarias para la creación del perfil de acuerdo con la documentación oficial.
6. Generación del perfil de acuerdo con la guía oficial.
7. Documentación del error.

NOTA: El procedimiento será ejecutado hasta que se identifiquen errores que impidan realizar correctamente el procedimiento de la creación del perfil.

7.2.1 Escenario 1: Ubuntu-18.04.6.

7.2.1.1 Revisión de la existencia de un perfil para la versión exacta del sistema operativo

Como primer paso se debe revisar la versión exacta del sistema operativo, que para este caso se realizó ejecutando el comando “uname -a” y “lsb_release -a”, con lo cual se obtiene que la versión es un Ubuntu 18.04.6 LTS.

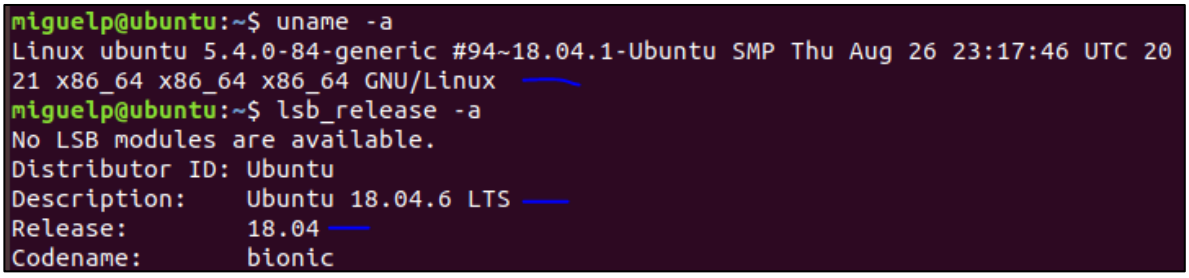


Figura 8 Información Ubuntu 18 procedimiento 1.

Fuente: Elaboración propia (2024).

Seguidamente con la versión del sistema operativo se verificó en el repositorio de GitHub si ya existe un perfil creado para esa versión en especificó, identificando que para el caso en cuestión la versión del sistema operativo aún no cuenta con un perfil creado.

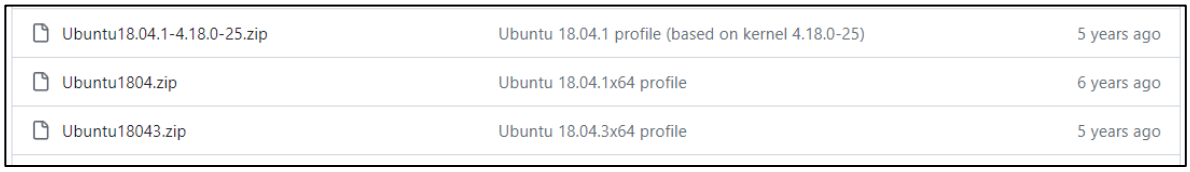


Figura 9 Versiones de perfiles disponibles para Ubuntu 18.

Fuente: Elaboración propia (2024).

7.2.1.2 Verificación de funcionamiento de Volatility

Se resalta que para el funcionamiento de Volatility es necesario realizar la descarga de Python y PIP, así como una serie de complementos para este último. Estas aplicaciones, herramientas y complementos si bien se mencionan en la página oficial de Volatility, en su sección de instalación, no indican su proceso de instalación, por tanto, puede ser confuso y generar errores al momento de intentar generar el perfil correctamente.

Continuando, suponiendo que todo ya se encuentra instalado y configurado en el sistema se realiza la verificación de que las aplicaciones Python, PIP y las dependencias de este último, se encuentren instaladas correctamente en el sistema.

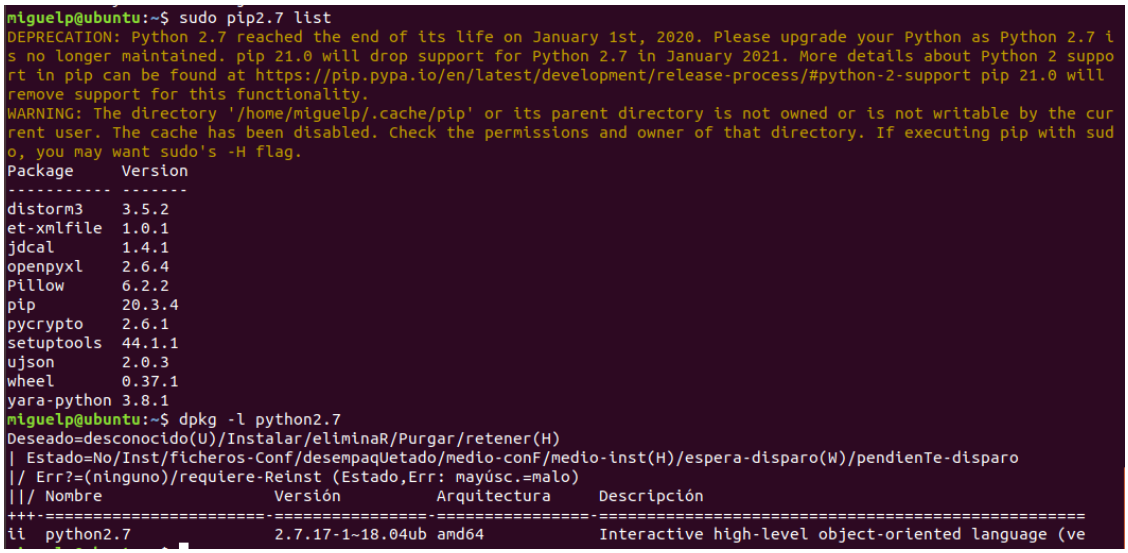


Figura 10 Verificación de instalación de Python, Pip y dependencias.

Fuente: Elaboración propia (2024).

7.2.1.3 Verificación de las herramientas necesarias para la creación del perfil de acuerdo con la documentación oficial

Se realizó la verificación de la instalación del paquete “build-essential”, el cual, es un paquete recomendado en la guía oficial de Volatility para la creación del Perfil, identificando que para este caso ya se encontraba instalado en el sistema.

```
miguelp@ubuntu:~/Downloads/volatility_2.6_lin64_standalone$ sudo apt update
[sudo] contraseña para miguelp:
Obj:1 http://co.archive.ubuntu.com/ubuntu bionic InRelease
Obj:2 http://co.archive.ubuntu.com/ubuntu bionic-updates InRelease
Obj:3 http://co.archive.ubuntu.com/ubuntu bionic-backports InRelease
Obj:4 http://security.ubuntu.com/ubuntu bionic-security InRelease
Des:5 http://co.archive.ubuntu.com/ubuntu bionic/main Translation-es [364 kB]
Des:6 http://co.archive.ubuntu.com/ubuntu bionic/main Translation-en_GB [432 kB]
Des:7 http://co.archive.ubuntu.com/ubuntu bionic/restricted Translation-en_GB [2.072 B]
Des:8 http://co.archive.ubuntu.com/ubuntu bionic/restricted Translation-es [1.960 B]
Des:9 http://co.archive.ubuntu.com/ubuntu bionic/universe Translation-en_GB [4.118 kB]
Des:10 http://co.archive.ubuntu.com/ubuntu bionic/universe Translation-es [1.259 kB]
Des:11 http://co.archive.ubuntu.com/ubuntu bionic/multiverse Translation-en_GB [82,1 kB]
Des:12 http://co.archive.ubuntu.com/ubuntu bionic/multiverse Translation-es [74,9 kB]
Descargados 6.334 kB en 2s (2.552 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se pueden actualizar 317 paquetes. Ejecute «apt list --upgradable» para verlos.
miguelp@ubuntu:~/Downloads/volatility_2.6_lin64_standalone$ sudo apt-get install build-essential
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
build-essential ya está en su versión más reciente (12.4ubuntu1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 317 no actualizados.
```

Figura 11 Verificación de paquete build-essential.

Fuente: Elaboración propia (2024).

Se realizó la instalación de “dwarfdump”, según la indicación de la guía oficial.

```
miguelp@ubuntu:~$ sudo apt install dwarfdump
[sudo] contraseña para miguelp:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  dwarfdump
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 313 no actualizados.
Se necesita descargar 249 kB de archivos.
Se utilizarán 643 kB de espacio de disco adicional después de esta operación.
Des:1 http://co.archive.ubuntu.com/ubuntu bionic/universe amd64 dwarfdump amd64 20180129-1 [249 kB]
Descargados 249 kB en 1s (284 kB/s)
Seleccionando el paquete dwarfdump previamente no seleccionado.
(Leyendo la base de datos ... 135604 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../dwarfdump_20180129-1_amd64.deb ...
Desempaquetando dwarfdump (20180129-1) ...
Configurando dwarfdump (20180129-1) ...
Procesando disparadores para man-db (2.8.3-2ubuntu0.1) ...
```

Figura 12 instalación de “dwarfdump".

Fuente: Elaboración propia (2024).

7.2.1.4 Generación del perfil de acuerdo con la guía oficial

Se verificó la guía a detalle encontrando que la misma no cuenta con un procedimiento específico para la realización del proceso de creación del perfil, si

bien ejemplifica el comando que debe realizarse, no especifica las rutas exactas y el detalle de las instrucciones escritas en el comando de ejemplo, por lo cual, para un usuario que no tiene el conocimiento encontraría una barrera en cuanto a la correcta realización del proceso de creación del perfil.

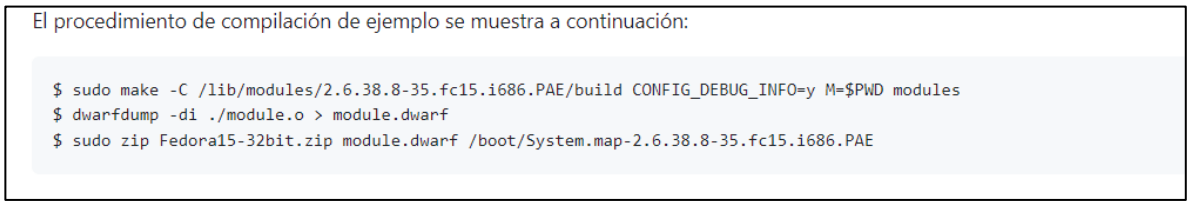


Figura 13 Ejemplo de referencia para la creación del perfil.

Fuente: Elaboración propia (2024).

Sin embargo, para poder dar continuidad a la prueba, la ruta desde la cual se deben ejecutar los comandos en cuestión es la ruta “Volatility/tools/linux”, desde la cual se encuentran los archivos “Makefile”, y “Module.C”, los cuales son los scripts necesarios para la realización del perfil del sistema operativo, datos que no se aclaran de manera específica en dicha guía.

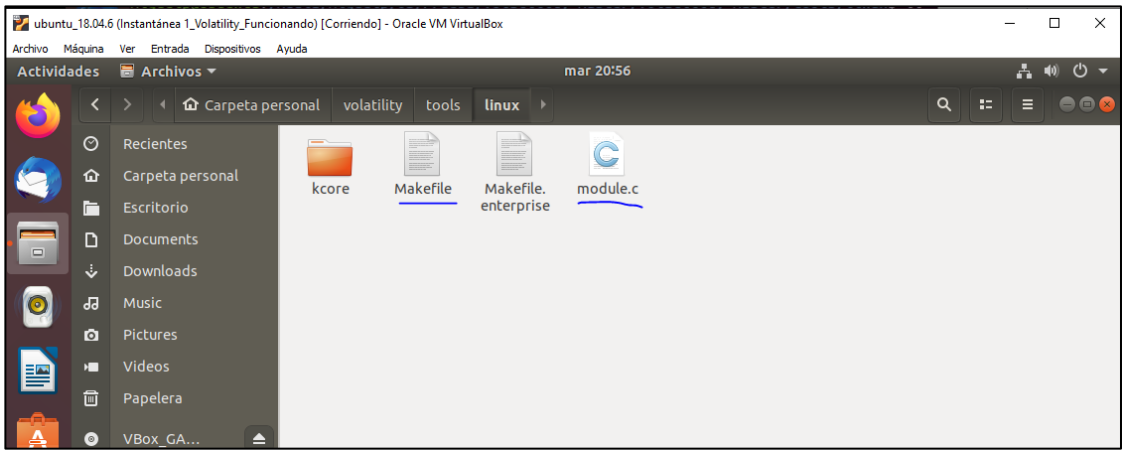


Figura 14 Archivos para la creación del perfil.

Fuente: Elaboración propia (2024).

7.2.1.5 Error en la generación del perfil

En el momento de realizar la ejecución del comando MAKE, tal y como indica la documentación encontramos un mensaje de error “make: *** [dwarf] Error 2”, el cual no permite continuar con el proceso, por tanto, se evidencia que en la guía faltan complementos y herramientas que Volatility supone ya se encuentran previamente parametrizados para su correcto funcionamiento, en este caso el error está relacionado con un error de licencia “MODULE_LICENSE()” y la librería “flex”, la cual, no se encuentra instalada.

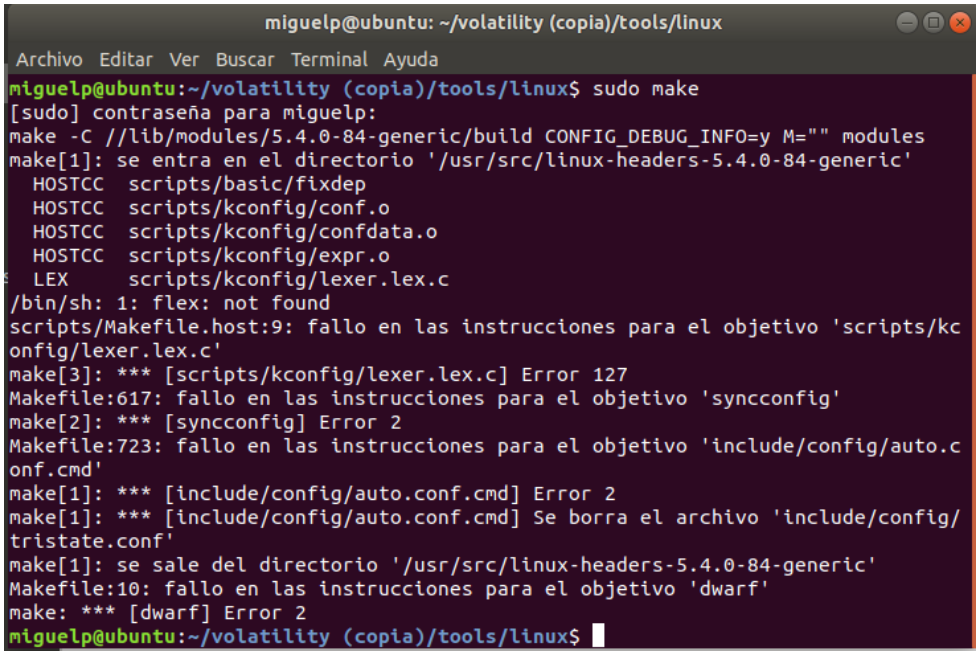


Figura 15 Error en la generación del perfil.

Fuente: Elaboración propia (2024).

7.2.2 Escenario 2: Ubuntu-22.04.3

Se realiza el procedimiento de igual manera al escenario anterior.

7.2.2.1 Revisión de la existencia de un perfil para la versión exacta del sistema operativo.

Como primer paso se debe revisar la versión exacta del sistema operativo, que para este caso se realizó ejecutando el comando “uname -a” y “lsb_release -a”, con lo cual se obtiene que la versión es un Ubuntu 22.04.3 LTS.

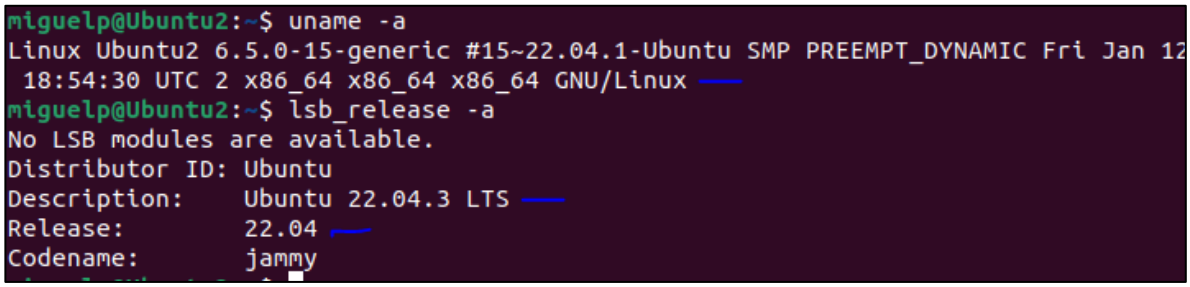


Figura 16 Información Ubuntu 22 procedimiento 2.

Fuente: Elaboración propia (2024).

Seguidamente con la versión del sistema operativo se verificó en el repositorio de GitHub si ya existe un perfil creado para esa versión en especificó, identificando que para el caso en cuestión la versión del sistema operativo aún no cuenta con un perfil creado ya que la versión más reciente con perfil es la 18.04.3.

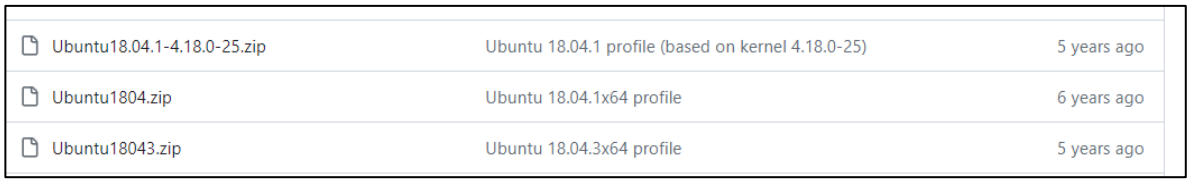


Figura 17 Versiones de perfiles disponibles para Ubuntu 22.

Fuente: Elaboración propia (2024).

7.2.2.2 Verificación de funcionamiento de Volatility.

Se resalta que para el funcionamiento de Volatility es necesario realizar la descarga de Python y PIP, así como una serie de complementos para este último. Estas

aplicaciones, herramientas y complementos si bien se mencionan en la página oficial de Volatility, en su sección de instalación, no indican su proceso de instalación, por tanto, puede ser confuso y generar errores al momento de intentar generar el perfil correctamente.

Continuando, suponiendo que todo ya se encuentra instalado y configurado en el sistema se realiza la verificación de que las aplicaciones Python, PIP y las dependencias de este último, se encuentren instaladas correctamente en el sistema.

Figura 18 Verificación de instalación de Python, Pip y dependencias.

Fuente: Elaboración propia (2024).

7.2.2.3 Verificación de las herramientas necesarias para la creación del perfil de acuerdo con la documentación oficial.

Se realizó la verificación de la instalación del paquete “build-essential”, el cual, es un paquete recomendado en la guía oficial de Volatility para la creación del Perfil, identificando que para este caso ya se encontraba instalado en el sistema.

```
miguelp@Ubuntu2:~$ sudo apt update
Obj:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Obj:2 http://co.archive.ubuntu.com/ubuntu jammy InRelease
Obj:3 http://co.archive.ubuntu.com/ubuntu jammy-updates InRelease
Obj:4 http://co.archive.ubuntu.com/ubuntu jammy-backports InRelease
Des:5 http://co.archive.ubuntu.com/ubuntu jammy/main Translation-es [332 kB]
Des:6 http://co.archive.ubuntu.com/ubuntu jammy/restricted Translation-es [964 B]
Des:7 http://co.archive.ubuntu.com/ubuntu jammy/universe Translation-es [1.356 kB]
Des:8 http://co.archive.ubuntu.com/ubuntu jammy/multiverse Translation-es [68,2 kB]
Descargados 1.758 kB en 1s (1.436 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 189 paquetes. Ejecute «apt list --upgradable» para verlos.
miguelp@Ubuntu2:~$ sudo apt-get install build-essential
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
build-essential ya está en su versión más reciente (12.9ubuntu3).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 189 no actualizados.
```

Figura 19 Verificación de paquete build-essential.

Fuente: Elaboración propia (2024).

Se realizó la instalación de “dwarfdump”, según la indicación de la guía oficial.

```
miguelp@Ubuntu2:~$ sudo apt install dwarfdump
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libdwarf1
Se instalarán los siguientes paquetes NUEVOS:
  dwarfdump libdwarf1
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 188 no actualizados.
Se necesita descargar 555 kB de archivos.
Se utilizarán 1.370 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://co.archive.ubuntu.com/ubuntu jammy/universe amd64 libdwarf1 amd64 20210528-1 [307 kB]
Des:2 http://co.archive.ubuntu.com/ubuntu jammy/universe amd64 dwarfdump amd64 20210528-1 [248 kB]
Descargados 555 kB en 1s (850 kB/s)
Seleccionando el paquete libdwarf1:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 211904 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../libdwarf1_20210528-1_amd64.deb ...
```

Figura 20 Instalación de dwarfdump.

Fuente: Elaboración propia (2024).

7.2.2.4 Generación del perfil de acuerdo con la guía oficial.

Se verificó la guía a detalle encontrando que la misma no cuenta con un procedimiento específico para la realización del proceso de creación del perfil, si bien ejemplifica el comando que debe realizarse, no especifica las rutas exactas y el detalle de las instrucciones escritas en el comando de ejemplo, por lo cual, para un usuario que no tiene el conocimiento encontraría una barrera en cuanto a la correcta realización del proceso de creación del perfil.

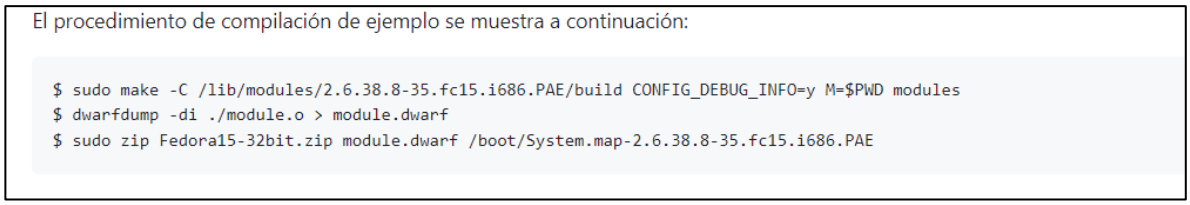


Figura 21 Ejemplo de referencia para la creación del perfil.

Fuente: Elaboración propia (2024).

Sin embargo, para poder dar continuidad a la prueba, la ruta desde la cual se deben ejecutar los comandos en cuestión es la ruta “Volatility/tools/linux”, desde la cual se encuentran los archivos “Makefile”, y “Module.C”, los cuales son los scripts necesarios para la realización del perfil del sistema operativo, datos que no se aclaran de manera específica en dicha guía.

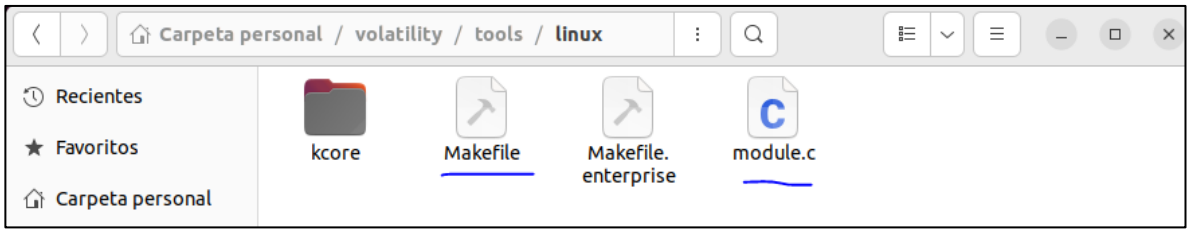


Figura 22 Archivos para la creación del perfil.

Fuente: Elaboración propia (2024).

7.2.2.5 Error en la generación del perfil.

En el momento de realizar la ejecución del comando MAKE, tal y como indica la documentación encontramos un mensaje de error “x86_64-linux-gnu-gcc-12”, el cual no permite continuar con el proceso, por tanto, se evidencia que en la guía faltan complementos y herramientas que Volatility supone ya se encuentran previamente parametrizados para su correcto funcionamiento, en este caso el error está relacionado con el kernel y la compilación.

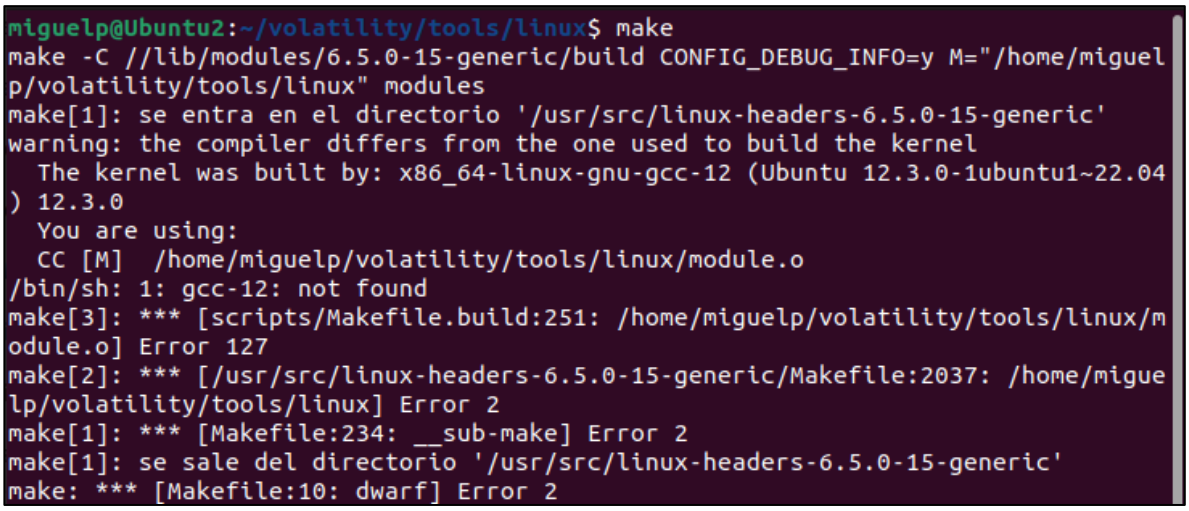


Figura 23 Error en la generación del perfil.

Fuente: Elaboración propia (2024).

7.2.3 Escenario 3: Debian-11.0.8.

Al igual que en los casos anteriores, se realiza el siguiente procedimiento.

7.2.3.1 Revisión de la existencia de un perfil para la versión exacta del sistema operativo

Como primer paso se debe revisar la versión exacta del sistema operativo, que para este caso se realizó ejecutando el comando “uname -a” y “lsb_release -a”, con lo cual se obtiene que la versión es Debian GNU/Linux 11 (bullseye).

```
hector@debian:~$ uname -a
Linux debian 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64 GNU/Li
nux
hector@debian:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 11 (bullseye)
Release:        11
Codename:       bullseye
hector@debian:~$
```

Figura 24 Información procedimiento 3.

Fuente: Elaboración propia (2024).

Seguidamente, con la versión del sistema operativo se verificó en el repositorio de GitHub si ya existe un perfil creado para esa versión en especificó, identificando que para el caso en cuestión la versión del sistema operativo aún no cuenta con un perfil creado ya que la versión más reciente con perfil es la Debian 9.4.0.

Name	Last commit message	Last commit date
..		
Debian40r9.zip	adding linux profiles	10 years ago
Debian5010.zip	adding linux profiles	10 years ago
Debian608.zip	adding linux profiles	10 years ago
Debian73.zip	adding linux profiles	10 years ago
Debian74.zip	adding linux profiles	10 years ago
Debian8.zip	added profile for Debian 8 and Fedora 21 Workstation	9 years ago
Debian82.zip	Debian 8.2 profile	9 years ago
Debian83.zip	Debian83 profile	8 years ago
Debian84.zip	Debian84	8 years ago
Debian86.zip	Add files via upload	8 years ago
Debian94.zip	Add Debian 9.4.0 x64	6 years ago

Figura 25 Versiones de perfiles disponibles para Debian.

Fuente: Elaboración propia (2024).

7.2.3.2 Verificación de funcionamiento de Volatility

Se resalta que para el funcionamiento de Volatility es necesario realizar la descarga de Python y PIP, así como una serie de complementos para este último. Estas aplicaciones, herramientas y complementos si bien se mencionan en la página oficial de Volatility, en su sección de instalación, no indican su proceso de instalación, por tanto, puede ser confuso y generar errores al momento de intentar generar el perfil de manera satisfactoria.

Continuando, suponiendo que todo ya se encuentra instalado y configurado en el sistema se realiza la verificación de que las aplicaciones Python, PIP y las dependencias de este último, se encuentren instaladas correctamente en el sistema operativo Debian GNU/Linux 11 (bullseye).

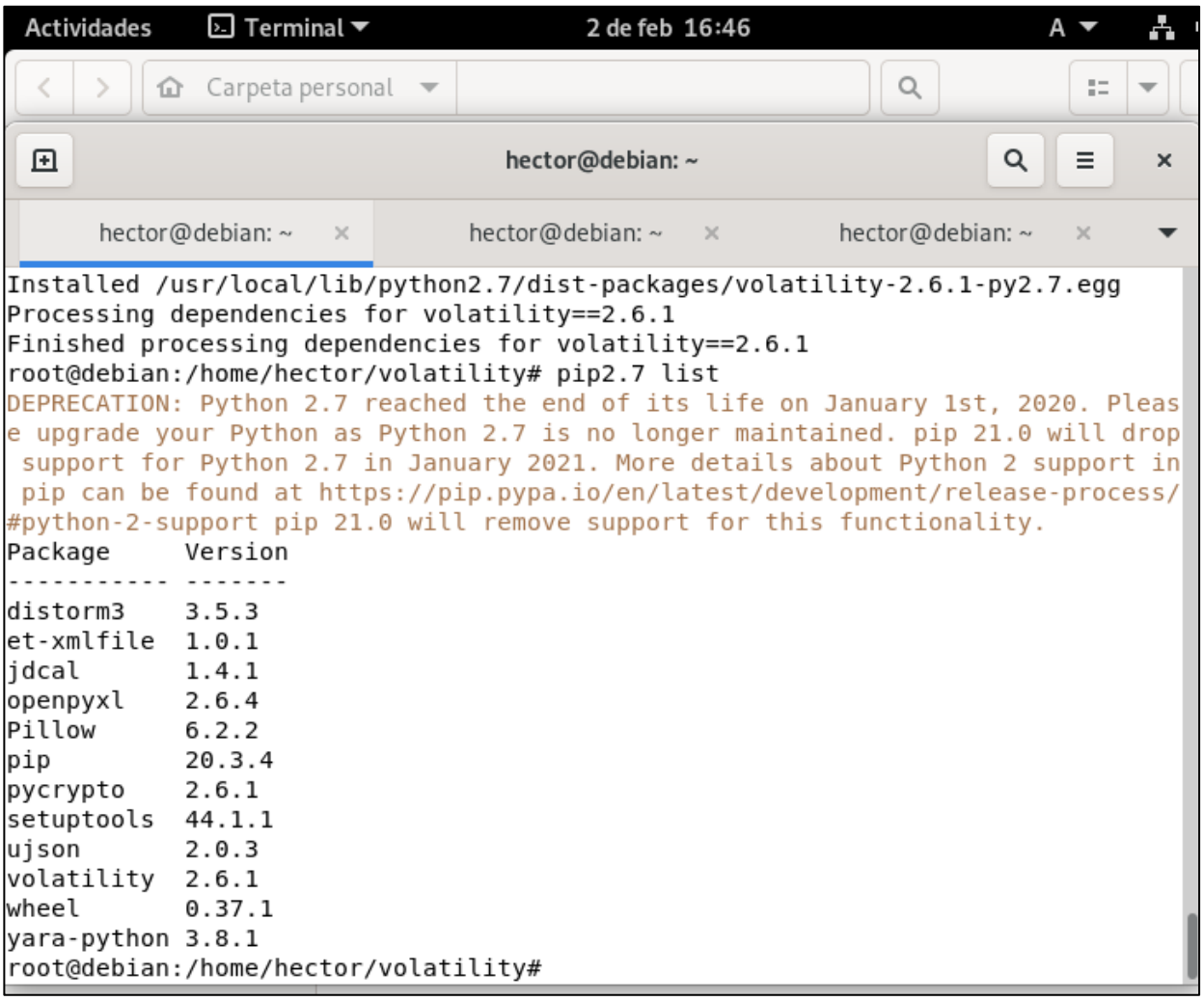


Figura 26 Verificación de instalación de Python, Pip y dependencias.

Fuente: Elaboración propia (2024).

7.2.3.3 Verificación de las herramientas necesarias para la creación del perfil de acuerdo con la documentación oficial

Se realizó la verificación de la instalación del paquete “build-essential”, el cual, es un paquete recomendado en la guía oficial de Volatility para la creación del Perfil, identificando que para este caso ya se encontraba instalado en el sistema.

```
hector@debian:~$ su
Contraseña:
root@debian:/home/hector# apt update
Obj:1 http://deb.debian.org/debian bullseye InRelease
Obj:2 http://security.debian.org/debian-security bullseye-security InRelease
Obj:3 http://deb.debian.org/debian bullseye-updates InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 239 paquetes. Ejecute «apt list --upgradable» para verlos.
root@debian:/home/hector# sudo apt-get install build-essential
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
build-essential ya está en su versión más reciente (12.9).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 239 no actualizados.
root@debian:/home/hector#
```

Figura 27 Verificación de paquete build-essential.

Fuente: Elaboración propia (2024).

Se realizó la instalación de “dwarfdump”, según la indicación de la guía oficial.

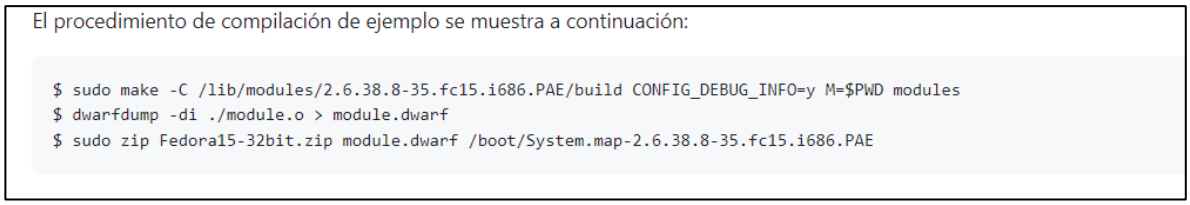
```
root@debian:/home/hector# sudo apt install dwarfdump
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libdwarf1
Se instalarán los siguientes paquetes NUEVOS:
  dwarfdump libdwarf1
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 239 no actualizados.
Se necesita descargar 544 kB de archivos.
Se utilizarán 1.348 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Figura 28 Instalación de dwarfdump en Debian 1.

Fuente: Elaboración propia (2024).

7.2.3.4 Generación del perfil de acuerdo con la guía oficial.

Se verificó la guía a detalle encontrando que la misma no cuenta con un procedimiento específico para la realización del proceso de creación del perfil, si bien ejemplifica el comando que debe realizarse, no especifica las rutas exactas y el detalle de las instrucciones escritas en el comando de ejemplo, por lo cual, para un usuario que no tiene el conocimiento encontraría una barrera en cuanto a la correcta realización del proceso de creación del perfil.


El procedimiento de compilación de ejemplo se muestra a continuación:

```
$ sudo make -C /lib/modules/2.6.38.8-35.fc15.i686.PAE/build CONFIG_DEBUG_INFO=y M=$PWD modules
$ dwarfdump -di ./module.o > module.dwarf
$ sudo zip Fedora15-32bit.zip module.dwarf /boot/System.map-2.6.38.8-35.fc15.i686.PAE
```

Figura 29 Ejemplo de referencia para la creación del perfil.

Fuente: Elaboración propia (2024).

Sin embargo, para poder dar continuidad a la prueba, la ruta desde la cual se deben ejecutar los comandos en cuestión se encuentra en la ubicación del sistema operativo Debian GNU/Linux 11 (bullseye). “Volatility/tools/linux”, dentro de la cual se encuentran los ubicados los archivos “Makefile”, y “Module.C”, los cuales son los scripts necesarios para la realización del perfil del sistema operativo, datos que no se aclaran de manera específica en dicha guía.

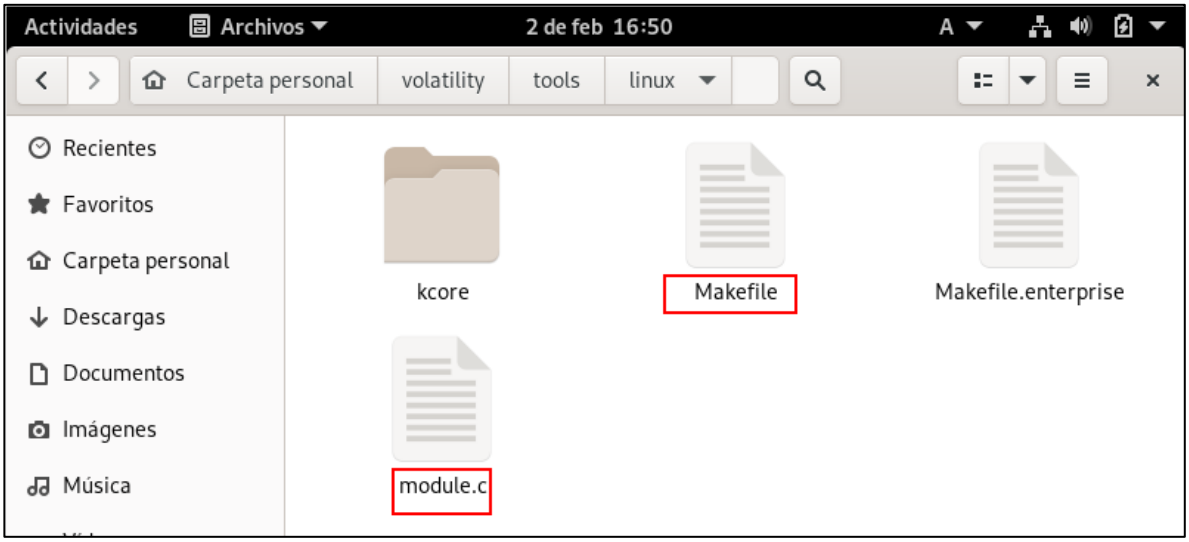


Figura 30 Archivos para la creación del perfil.

Fuente: Elaboración propia (2024).

7.2.3.5 Error en la generación del perfil.

En el momento de realizar la ejecución del comando MAKE, tal y como indica la documentación encontramos un mensaje error asociado a la ausencia de un módulo de licencia “MODULE_LICENSE ()”, el cual no se encuentra.

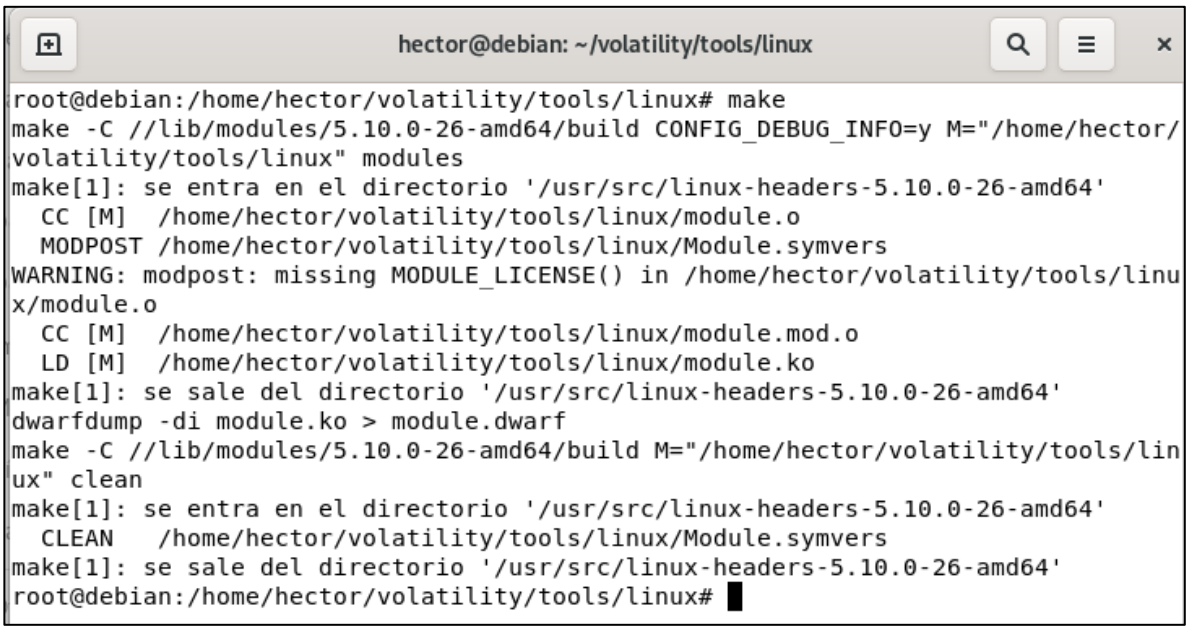


Figura 31 Error en la generación del perfil.

Fuente: Elaboración propia (2024).

7.2.4 Escenario 4: Debian-12.4.0.

Al igual que en los casos anteriores, se realiza el siguiente procedimiento.

7.2.4.1 Revisión de la existencia de un perfil para la versión exacta del sistema operativo.

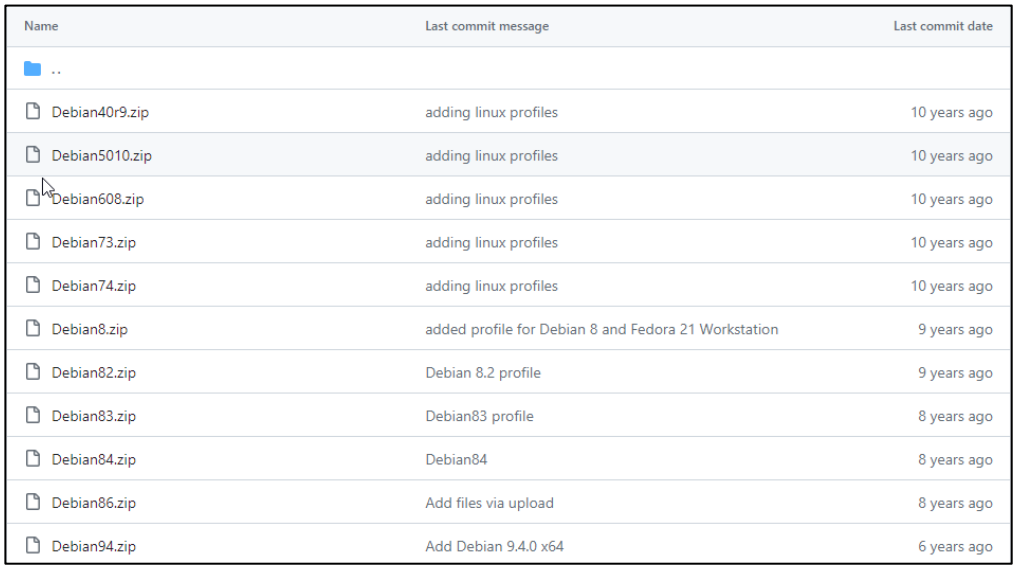
Como primer paso se debe revisar la versión exacta del sistema operativo, que para este caso se realizó ejecutando el comando “uname -a” y “lsb_release -a”, con lo cual se obtiene que la versión es un Debian GNU/Linux 12 (bookworn).

```
hector@debian:~$ uname -a
Linux debian 6.1.0-17-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.69-1 (2023-12-30) x86_64
GNU/Linux
hector@debian:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 12 (bookworm)
Release:        12
Codename:       bookworm
```

Figura 32 Información Debian GNU/Linux 12 (bookworn)procedimiento 4.

Fuente: Elaboración propia (2024).

Seguidamente, con la versión del sistema operativo se verificó en el repositorio de GitHub si ya existe un perfil creado para esa versión en especificó, identificando que para el caso en cuestión la versión del sistema operativo aún no cuenta con un perfil creado ya que la versión más reciente con perfil es la Debian 9.4.0.



Name	Last commit message	Last commit date
..		
Debian40r9.zip	adding linux profiles	10 years ago
Debian5010.zip	adding linux profiles	10 years ago
Debian608.zip	adding linux profiles	10 years ago
Debian73.zip	adding linux profiles	10 years ago
Debian74.zip	adding linux profiles	10 years ago
Debian8.zip	added profile for Debian 8 and Fedora 21 Workstation	9 years ago
Debian82.zip	Debian 8.2 profile	9 years ago
Debian83.zip	Debian83 profile	8 years ago
Debian84.zip	Debian84	8 years ago
Debian86.zip	Add files via upload	8 years ago
Debian94.zip	Add Debian 9.4.0 x64	6 years ago

Figura 33 Versiones de perfiles disponibles para Debian.

Fuente: Elaboración propia (2024).

7.2.4.2 Verificación de funcionamiento de Volatility.

Se resalta que para el funcionamiento de Volatility es necesario realizar la descarga de Python y PIP, así como una serie de complementos para este último. Estas aplicaciones, herramientas y complementos si bien se mencionan en la página oficial de Volatility, en su sección de instalación, no indican su proceso de instalación, por tanto, puede ser confuso y generar errores al momento de intentar generar el perfil correctamente.

Continuando, suponiendo que todo ya se encuentra instalado y configurado en el sistema se realizan las verificaciones en las aplicaciones Python, PIP y las dependencias de este último, para validar que se encuentren instaladas correctamente al interior del sistema operativo Debian GNU/Linux 12 (bookworm).

```
root@debian:/home/hector# sudo pip2.7 list
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Package     Version
----------- -------
distorm3    3.5.2
et-xmlfile  1.0.1
jdcal       1.4.1
openpyxl    2.6.4
Pillow      6.2.2
pip         20.3.4
pycrypto    2.6.1
setuptools  44.1.1
ujson       2.0.3
volatility  2.6.1
wheel       0.37.1
yara-python 3.8.1
```

Figura 34 Verificación de instalación de Python, Pip y dependencias.

Fuente: Elaboración propia (2024).

7.2.4.3 Verificación de las herramientas necesarias para la creación del perfil de acuerdo con la documentación oficial

Se realizó la verificación de la instalación del paquete “build-essential”, el cual, es un paquete recomendado en la guía oficial de Volatility para la creación del Perfil, identificando que para este caso ya se encontraba instalado en el sistema.

```
root@debian:/home/hector# sudo apt update
Obj:1 http://security.debian.org/debian-security bookworm-security InRelease
Obj:2 http://deb.debian.org/debian bookworm InRelease
Obj:3 http://deb.debian.org/debian bookworm-updates InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Todos los paquetes están actualizados.
root@debian:/home/hector# sudo apt-get install build-essential
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
```

Figura 35 Verificación de paquete build-essential.

Fuente: Elaboración propia (2024).

Se realizó la instalación de “dwarfdump”, según la indicación de la guía oficial.

```
root@debian:/home/hector# sudo apt install dwarfdump
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
```

Figura 36 Instalar dwarfdump Debian 2.

Fuente: Elaboración propia (2024).

7.2.4.4 Generación del perfil de acuerdo con la guía oficial

Se verificó la guía a detalle encontrando que la misma no cuenta con un procedimiento específico para la realización del proceso de creación del perfil, si bien ejemplifica el comando que debe realizarse, no especifica las rutas exactas y el detalle de las instrucciones escritas en el comando de ejemplo, por lo cual, para

un usuario que no tiene el conocimiento encontraría una barrera en cuanto a la correcta realización del proceso de creación del perfil.

El procedimiento de compilación de ejemplo se muestra a continuación:

```
$ sudo make -C /lib/modules/2.6.38.8-35.fc15.i686.PAE/build CONFIG_DEBUG_INFO=y M=$PWD modules
$ dwarfdump -di ./module.o > module.dwarf
$ sudo zip Fedora15-32bit.zip module.dwarf /boot/System.map-2.6.38.8-35.fc15.i686.PAE
```

Figura 37 Ejemplo de referencia para la creación del perfil.

Fuente: Elaboración propia (2024).

Sin embargo, para poder dar continuidad a la prueba, la ruta desde la cual se deben ejecutar los comandos en cuestión se encuentra en la ubicación del sistema operativo Debian GNU/Linux 12 (bookworm) “Volatility/tools/linux”, dentro de la cual se encuentran los ubicados los archivos “Makefile”, y “Module.C”, los cuales son los scripts necesarios para la realización del perfil del sistema operativo, datos que no se aclaran de manera específica en dicha guía.

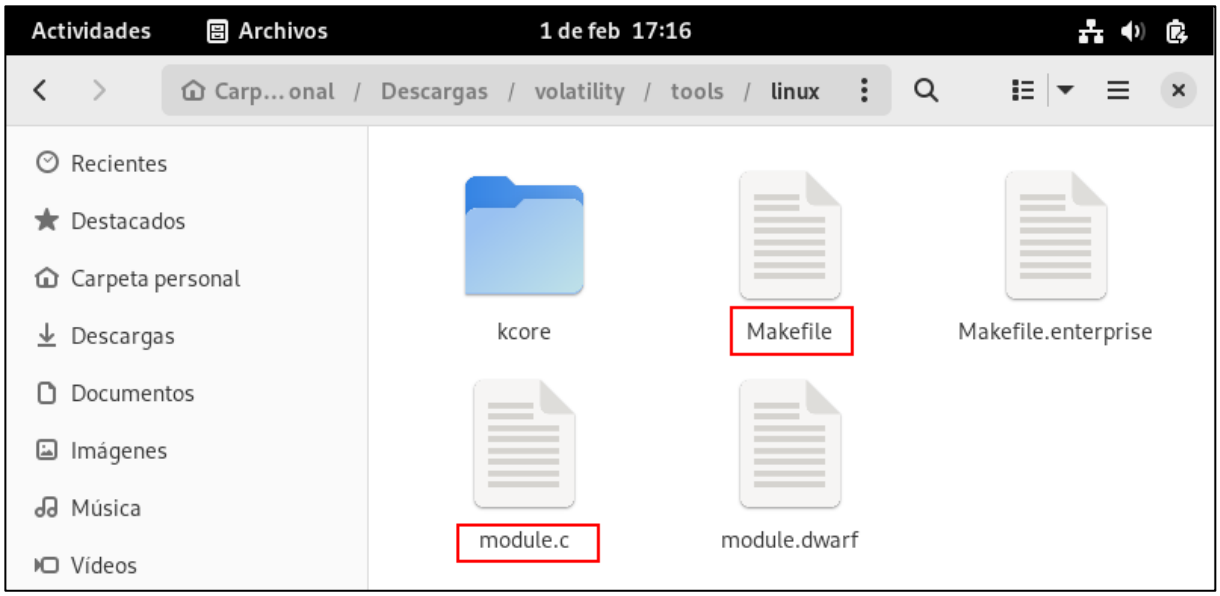


Figura 38 Archivos para la creación del perfil.

Fuente: Elaboración propia (2024).

7.2.4.5 Error en la generación del perfil.

En el momento de realizar la ejecución del comando MAKE, tal y como indica la documentación encontramos un mensaje error asociado a la ausencia de un módulo de licencia “MODULE_LICENSE ()”, el cual no se encuentra.

```
root@debian:/home/hector/volatility/tools/linux# make
make -C //lib/modules/6.1.0-17-amd64/build CONFIG_DEBUG_INFO=y M="/home/hector/volatili
ty/tools/linux" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-6.1.0-17-amd64'
  CC [M]  /home/hector/volatility/tools/linux/module.o
  MODPOST /home/hector/volatility/tools/linux/Module.symvers
ERROR: modpost: missing MODULE_LICENSE() in /home/hector/volatility/tools/linux/module.
o
make[2]: *** [/usr/src/linux-headers-6.1.0-17-common/scripts/Makefile.modpost:126: /hom
e/hector/volatility/tools/linux/Module.symvers] Error 1
make[1]: *** [/usr/src/linux-headers-6.1.0-17-common/Makefile:1991: modpost] Error 2
make[1]: se sale del directorio '/usr/src/linux-headers-6.1.0-17-amd64'
make: *** [Makefile:10: dwarf] Error 2
root@debian:/home/hector/volatility/tools/linux#
```

Figura 39 Error en la generación del perfil.

Fuente: Elaboración propia (2024).

En resumen, al realizar las diferentes pruebas de creación de los respectivos perfiles de Volatility con el procedimiento oficial se evidencio que el procedimiento supone que ya se cuentan con aplicaciones y librerías ya instaladas anteriormente como python2.6 y librerías del mismo, además, de errores por falta de instalación de librerías que utiliza Volatility pero no se encuentran relacionadas directamente en la guía oficial, o errores propios del sistema operativo por ejemplo los errores de configuración invalida de Kernel, o la falta de licencia en el “module” para poder compilar y crear el perfil del sistema operativo respectivo, por lo que si bien las

indicaciones dadas en el foro oficial no están alejadas de la realidad, si requieren que el usuario tenga conocimientos medios o avanzados para poder ejecutar las acciones y dar solución a los problemas que surjan al momento de crear el respectivo perfil, por lo tanto no es un procedimiento enfocado a cualquier tipo de usuario.

En conclusión, si bien se proporciona una guía detallada sobre la creación de perfiles en Volatility para el análisis forense de sistemas Linux y aunque se destaca la importancia de perfiles específicos y brinda recomendaciones prácticas, las pruebas realizadas revelan que el procedimiento oficial presupone la existencia previa de ciertas aplicaciones y bibliotecas, lo que podría generar dificultades en entornos operativos reales, además de evidenciar la necesidad de conocimientos avanzados para abordar posibles problemas, lo que sugiere que el proceso no es accesible para usuarios sin experiencia técnica significativa en Volatility, por lo que en consecuencia, la implementación efectiva de este procedimiento podría ser desafiante para aquellos con habilidades limitadas en el ámbito forense y tecnológico.

7.3 PROCEDIMIENTO OPTIMIZADO PARA LA CREACIÓN DE PERFILES EN VOLATILITY2.6.

Con los resultados obtenidos en la sección “6.3 PROCEDIMIENTO PARA LA CREACIÓN DE PERFILES EN VOLATILITY 2.6 PARA EL ANÁLISIS DE MEMORIA VOLATIL”, se desarrolló un procedimiento optimizado para la creación de perfiles en Volatility 2.6, el cual, está diseñado a partir de la guías oficiales, foros oficiales de errores, recomendaciones de diversas páginas y autores, resultando un procedimiento que disminuye la posibilidad de que se genere un error al momento de realizar la creación del perfil, cabe resaltar que esto puede variar para cada distribución de Linux, por tanto, puede que lo que funcione para Ubuntu, no funcione en Fedora o DEBIAN y viceversa.

Este procedimiento se detallará a continuación de acuerdo con la distribución de Linux revisada, dando las recomendaciones generales y específicas abarca desde la instalación de Volatility como la creación del perfil puesto que de esto depende que la creación del perfil se realice correctamente, así como la solución de dos errores comunes y como solucionarlo, puesto que es indispensable para lograr generar correctamente el perfil.

7.3.1 Procedimiento optimizado para la creación de perfiles en Linux con demostración en 4 escenarios Ubuntu y Debian.

Para la creación de perfiles en Volatility en sistemas operativos Linux se deben realizar los siguientes pasos:

Nota: Los pasos que se catalogan como “No se documenta”, son pasos que no hacen parte ni son relevantes para el objetivo de la investigación actual.

1. Se debe generar un clon del sistema operativo en el cual se va a realizar el procedimiento, ya que la generación del perfil requiere el Sistema Operativo

donde se generó el volcado de memoria. Este clon permitirá mantener la integralidad del sistema de información disminuyendo el riesgo de contaminar la evidencia original. (No se documenta).

2. Acceso al sistema operativo al cual se le va a realizar el procedimiento (No se documenta).
3. Creación de snapshot o instantáneas (No se documenta).
4. Revisión de la existencia de un perfil ya creado para la versión exacta del sistema operativo.
5. Instalar herramientas y dependencias
    a. build-essential (Obligatorio)
    b. dwarfdump (Obligatorio)
    c. Python2.6
    d. Curl
    e. GIT
    f. Flex
    g. bison
    h. PIP
        i. Distorm3
        ii. Yara-python
        iii. Pycrypto
        iv. Pillow
        v. Openpyxl==2.6.4
        vi. Ujson
6. Clonar github Volatility (Instalar opcional)
7. Creación del perfil
8. Validación del funcionamiento del perfil
9. Solucionar errores comunes Ubuntu
    a. Error de Kernel (Opcional solo si aparece)

b. Error de licencia perdida “ERROR: modpost: missing MODULE_LICENSE ()” (Opcional solo si aparece)

7.3.1.1 Recomendación separación de ambiente vulnerado generación del Clon

De acuerdo con lo indicado en la ISO 27037, se debe mantener la integridad de las evidencias, por tanto, se hace necesario que antes de realizar los procedimientos descritos a continuación se genere un clon del sistema en el cual se van a ejecutar los procedimientos. Si los ambientes son virtualizados se pueden generar clones directamente en las consolas de administración de las máquinas virtuales. Por tanto, se recomienda revisar la documentación de cada fabricante para poder realizar dicho proceso, en caso de Virtual Box que es el entorno utilizado en este proyecto, la generación de un clon se realiza siguiendo los siguientes pasos:

1. Se debe seleccionar la máquina que se requiere clonar.
2. En la cinta opciones seleccionar “Máquina”
3. En la opción de “Máquina”, se debe seleccionar la opción “Clonar” y seguir las instrucciones.

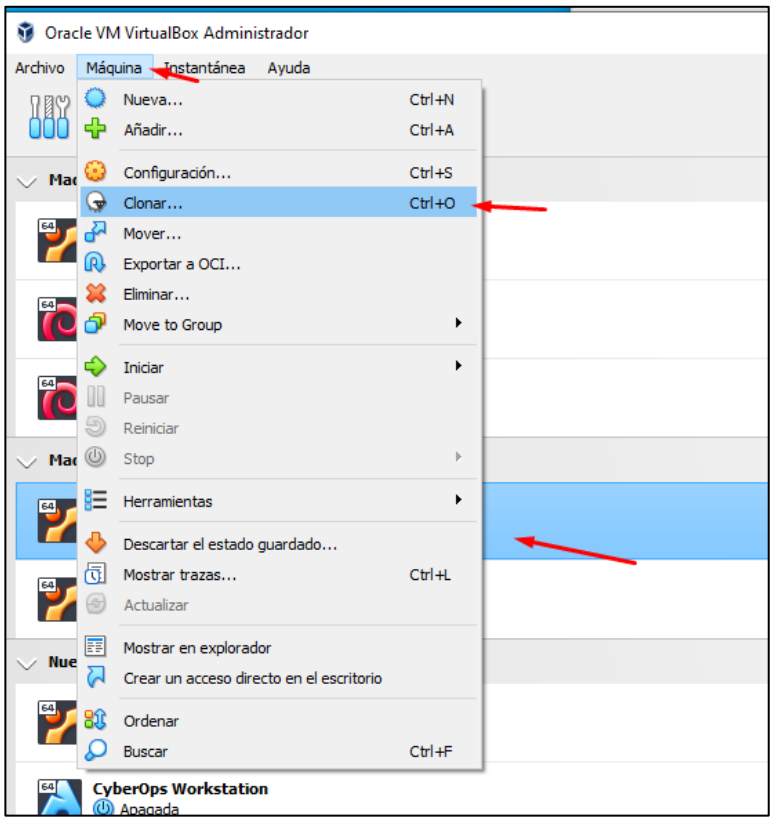


Figura 40 Ejemplo Clonación de máquina virtual VirtualBox.

Fuente: Elaboración propia (2024).

7.3.1.2 Escenario 1: Ubuntu-18.04.6.

7.3.1.2.1 Revisión de la existencia de un perfil para la versión exacta del sistema operativo

Como primer paso se debe revisar la versión exacta del sistema operativo, que para este caso se realizó ejecutando el comando “uname -a” y “lsb_release -a”, con lo cual se obtiene que la versión es un Ubuntu 18.04.6 LTS.

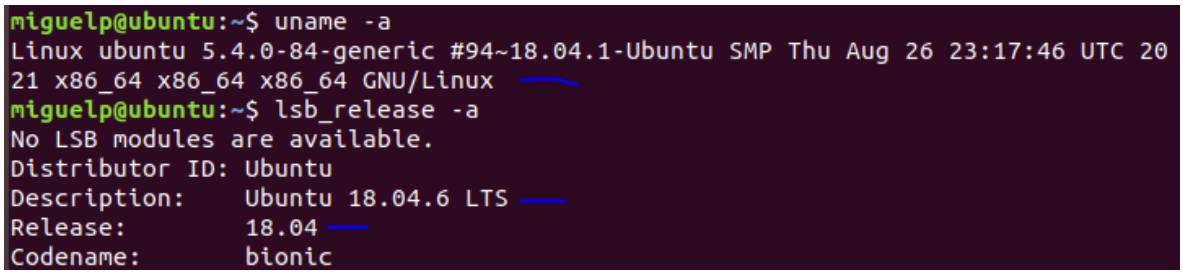


Figura 41 Información Ubuntu 18 procedimiento 1.

Fuente: Elaboración propia (2024).

Seguidamente con la versión del sistema operativo se verificó en el repositorio de GitHub si ya existe un perfil creado para esa versión en especificó, identificando que para el caso en cuestión la versión del sistema operativo aún no cuenta con un perfil creado.

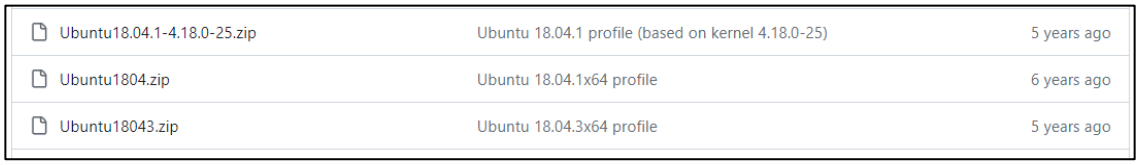


Figura 42 Versiones de perfiles disponibles para Ubuntu 18.

Fuente: Elaboración propia (2024).

7.3.1.2.2 Instalar herramientas y dependencias

Este representa el paso a paso sugerido para realizar la correcta instalación de todos los complementos necesarios para la instalación de Volatility, y asegurar la menor cantidad de errores por incompatibilidades, el cual consta de la instalación de:

Como primer paso la instalación de “build-essential”, para lo cual, se realizó la actualización de la biblioteca “apt update” y la posterior instalación “apt-get install build-essential”, como se muestra a continuación.

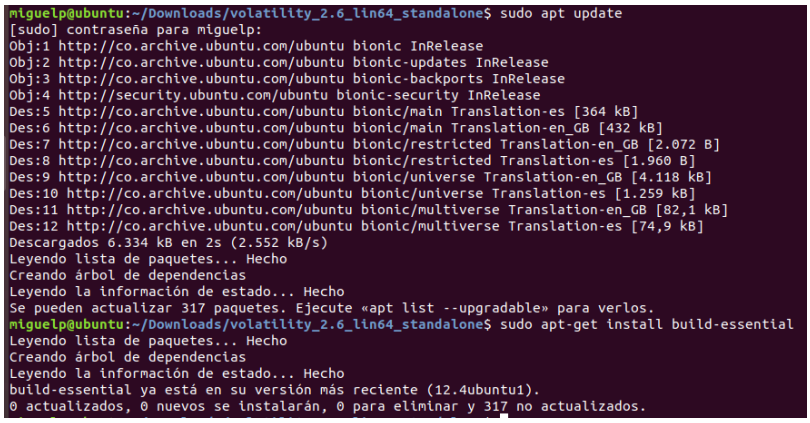


Figura 43 Verificación de paquete build-essential escenario 1.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación de “flex”, como se muestra a continuación.

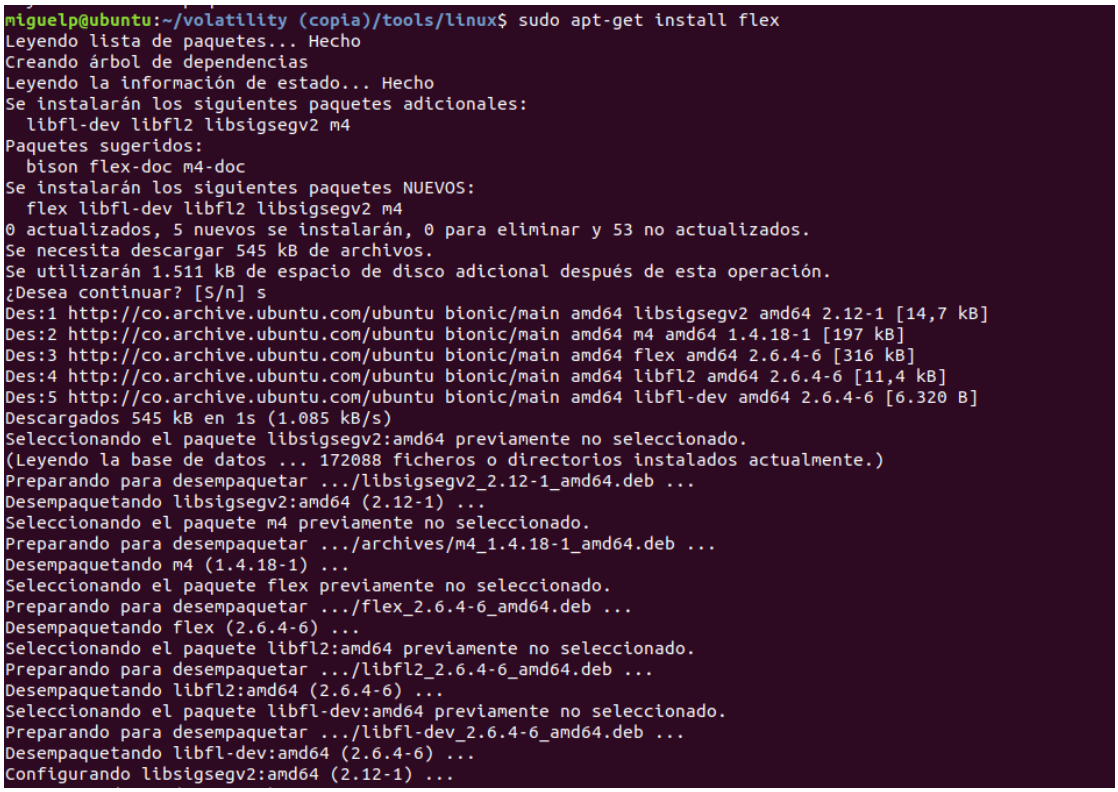


Figura 44 Instalación de Flex escenario 1.

Fuente: Elaboración propia (2024).

Seguidamente se realiza la instalación de Python2.7, indispensable para el funcionamiento de Volatilita, como se muestra a continuación.

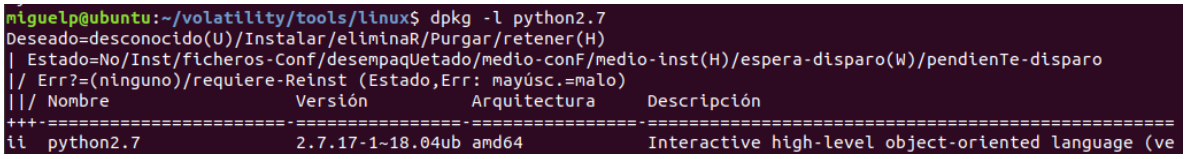


Figura 45 Instalación de Python2.7 escenario 1.

Fuente: Elaboración propia (2024).

Posteriormente se debe realizar la instalación de “curl”, como se muestra a continuación.

Figura 46 Instalación de Curl escenario 1.

Fuente: Elaboración propia (2024).

Continuando se debe realizar la instalación de “PIP”, ejecutando el comando “curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py” como se muestra a continuación.

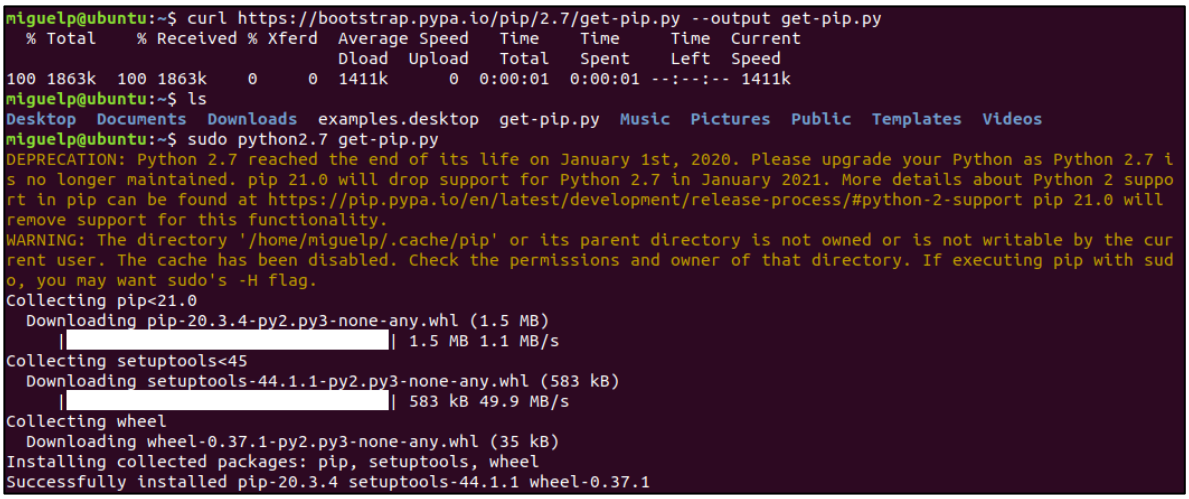


Figura 47 Instalación de PIP escenario 1.

Fuente: Elaboración propia (2024).

Seguidamente se debe realizar la instalación de “GIT”, como se muestra a continuación.

Figura 48 Instalación de GIT escenario 1

Fuente: Elaboración propia (2024).

Seguidamente, se debe realizar la instalación de “bison”, el cual, permite la compilación de aplicaciones relacionadas con Kernel, ejecutando el comando como se muestra a continuación.

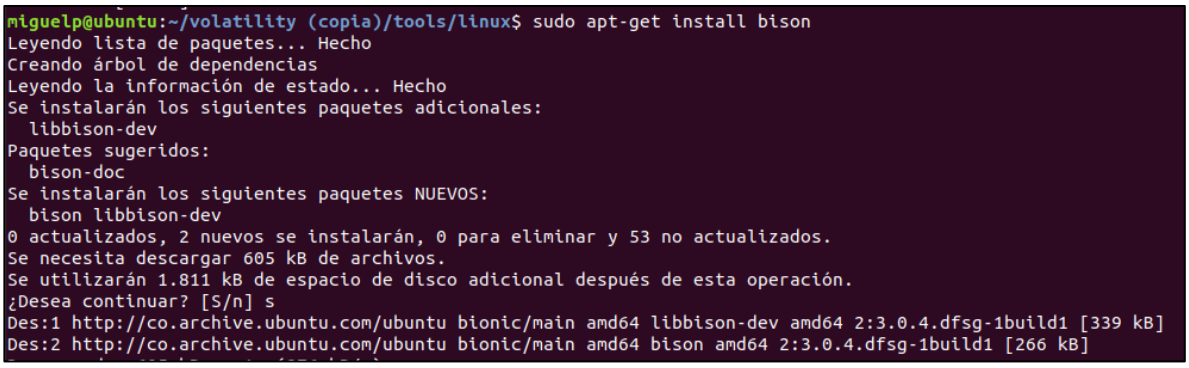


Figura 49 Instalación Bison escenario 1.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “Distorm3”, como se muestra a continuación.

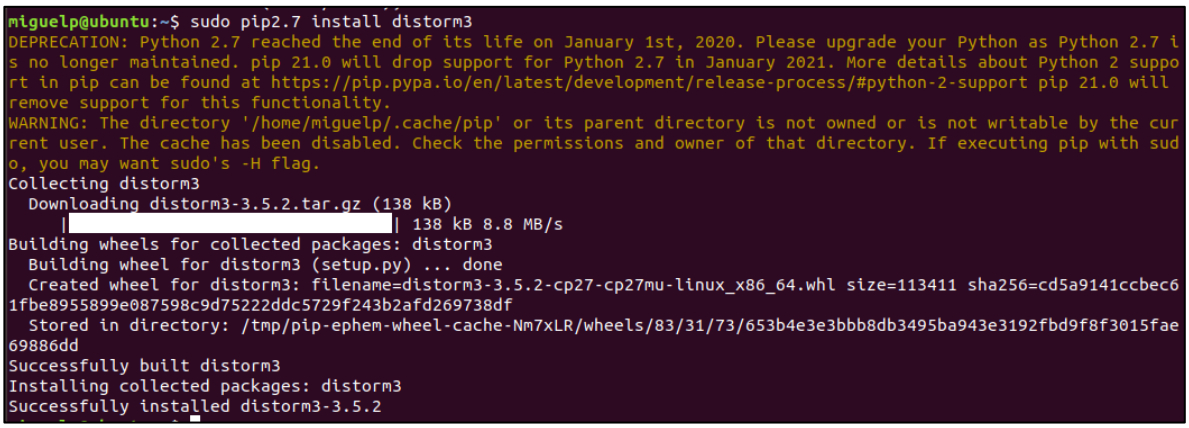


Figura 50 Instalación de dependencia distorm3 escenario 1.

Fuente: Elaboración propia (2024).

De igual manera, se debe realizar la instalación dependencia de PIP “yara-python”, como se muestra a continuación.

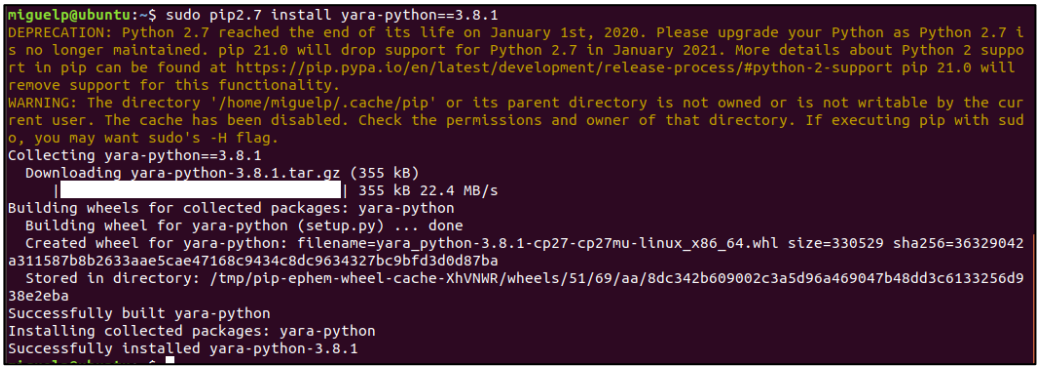


Figura 51 Instalación de dependencia yara-python escenario 1.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “Pycrypto”, como se muestra a continuación.

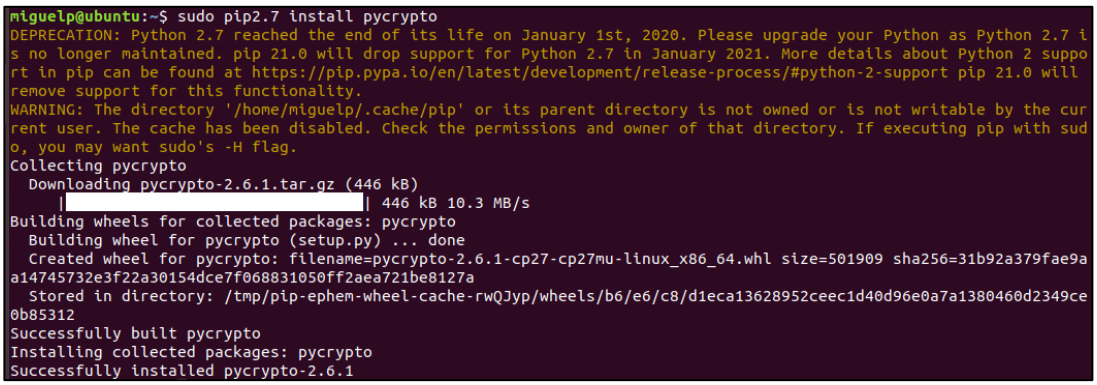


Figura 52 Instalación de dependencia pycrypto escenario 1.

Fuente: Elaboración propia (2024).

Así mismo, se debe realizar la instalación dependencia de PIP “pillow”, como se muestra a continuación.

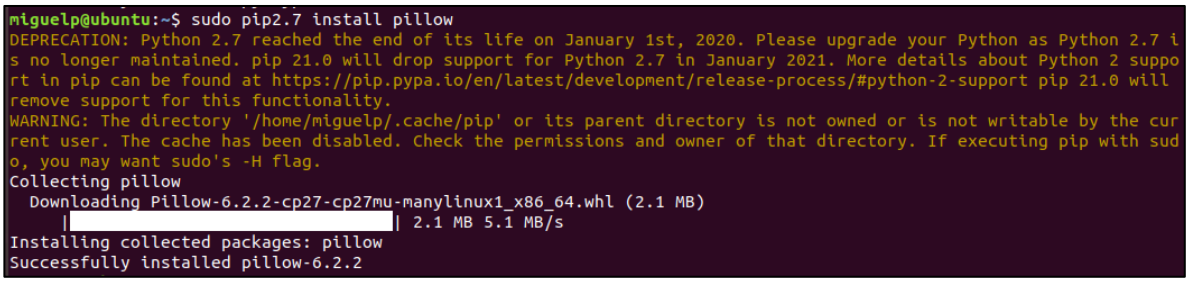


Figura 53 Instalación de dependencia pillow escenario 1.

Fuente: Elaboración propia (2024).

Posteriormente, se debe realizar la instalación dependencia de PIP “openpyxl==2.6.4”, como se muestra a continuación.

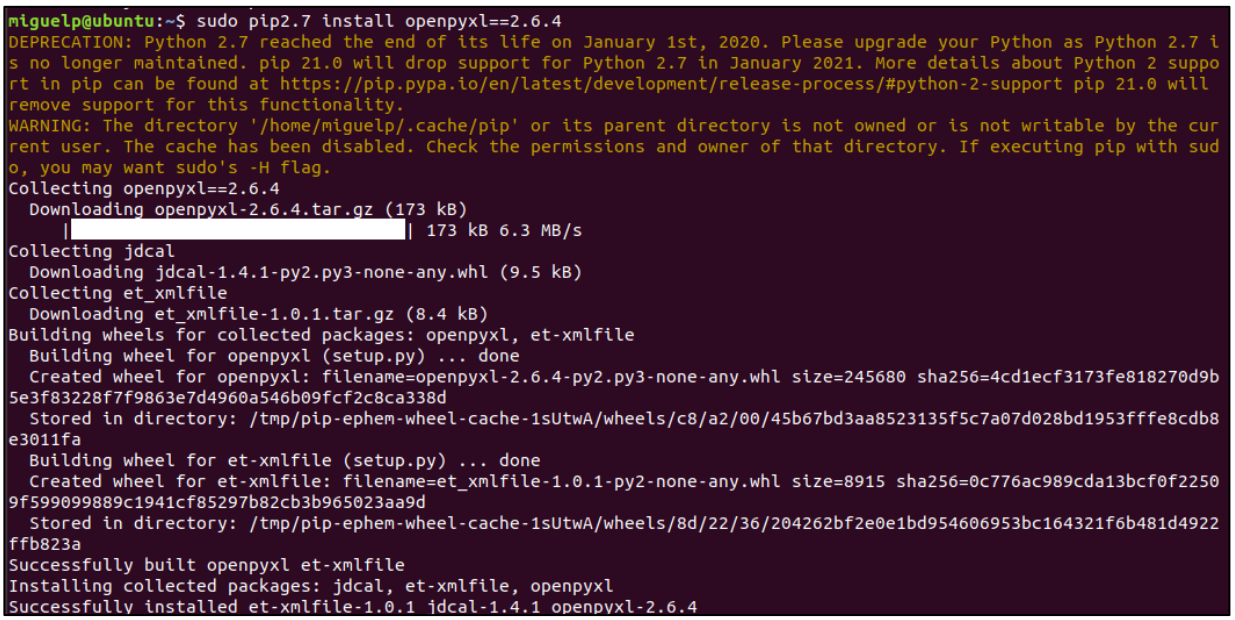


Figura 54 Instalación de dependencia openpyxl==2.6.4 escenario 1.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “ujson”, como se muestra a continuación.

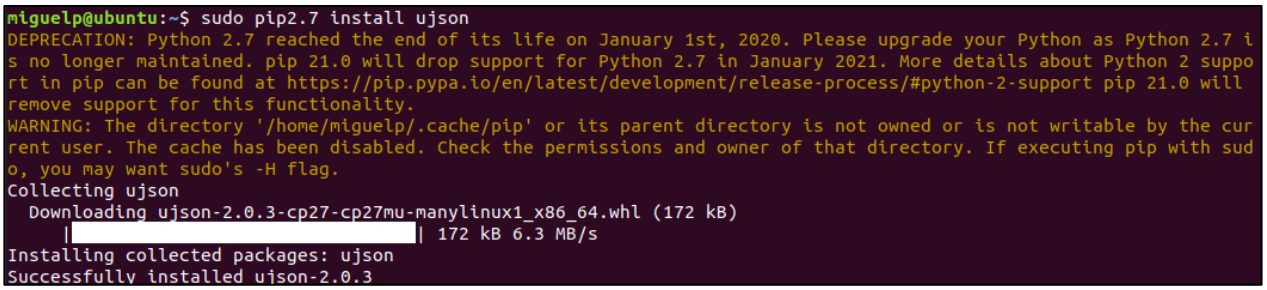


Figura 55 Instalación de ujson escenario 1.

Fuente: Elaboración propia (2024).

Una vez instalados todos los complementos se realiza la verificación de la correcta instalación de estos ejecutando el comando “sudo pip2.7 list”, dando como resultado las 11 dependencias que se muestran a continuación.

```
miguelp@ubuntu:~$ sudo pip2.7 list
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 i
s no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 suppo
rt in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
WARNING: The directory '/home/miguelp/.cache/pip' or its parent directory is not owned or is not writable by the cur
rent user. The cache has been disabled. Check the permissions and owner of that directory. If executing pip with sud
o, you may want sudo's -H flag.
Package     Version
----------- -------
distorm3    3.5.2
et-xmlfile  1.0.1
jdcal       1.4.1
openpyxl    2.6.4
Pillow      6.2.2
pip         20.3.4
pycrypto    2.6.1
setuptools  44.1.1
ujson       2.0.3
wheel       0.37.1
yara-python 3.8.1
```

Figura 56 Verificación de instalación de dependencias escenario 1

Fuente: Elaboración propia (2024).

7.3.1.2.3 Clonar repositorio de Volatility e instalación opcional.

Se debe verificar una ruta donde se quiera clonar el repositorio de Volatility, para este caso será “USER\home\”, ejecutando el comando “git clone https://github.com/volatilityfoundation/volatility.git” como se muestra a continuación.

```
miguelp@ubuntu:~$ git clone https://github.com/volatilityfoundation/volatility.git
Clonando en 'volatility'...
remote: Enumerating objects: 27411, done.
remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411
Recibiendo objetos: 100% (27411/27411), 21.10 MiB | 16.34 MiB/s, listo.
Resolviendo deltas: 100% (19758/19758), listo.
```

Figura 57 Clonación de repositorio Volatility Escenario 1.

Fuente: Elaboración propia (2024).

Por otra parte, la instalación opcional de Volatility se realiza ingresando en el repositorio clonado y ejecutando el comando “sudo python2.7 setup.py install”.

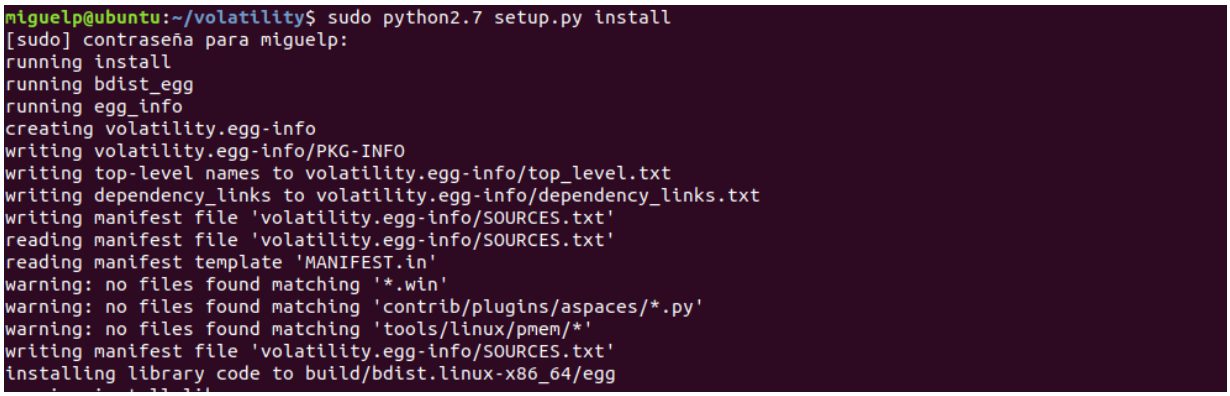


Figura 58 Instalación opcional de Volatility escenario 1.

Fuente: Elaboración propia (2024).

7.3.1.2.4 Creación del perfil.

Una vez realizados los pasos anteriores se debe realizar la creación del perfil, para lo cual se accede a la carpeta de Volatility en donde se haya realizado la Clonación o instalación de este e ingresar a la siguiente ruta "…/volatility/tools/linux/", donde se encuentran los siguientes archivos "Makefile", "Makefile.enterprise", "module.c", y la carpeta "kcore", como se evidencia a continuación.

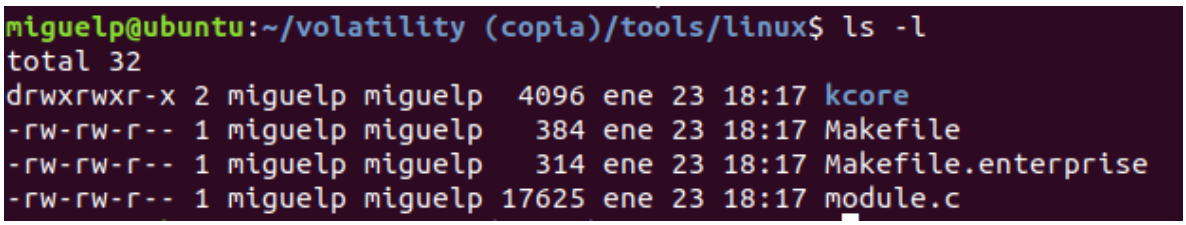


Figura 59 Contenido de la ruta "…/volatility/tools/linux/" escenario 1.

Fuente: Elaboración propia (2024).

En dicha ruta se encuentran los archivos necesarios para la generación del perfil, para lo cual se ejecuta el comando "make", para este caso se generó un error que

indica “ERROR: modpost: missing MODULE_LICENSE ()”, como se evidencia a continuación.

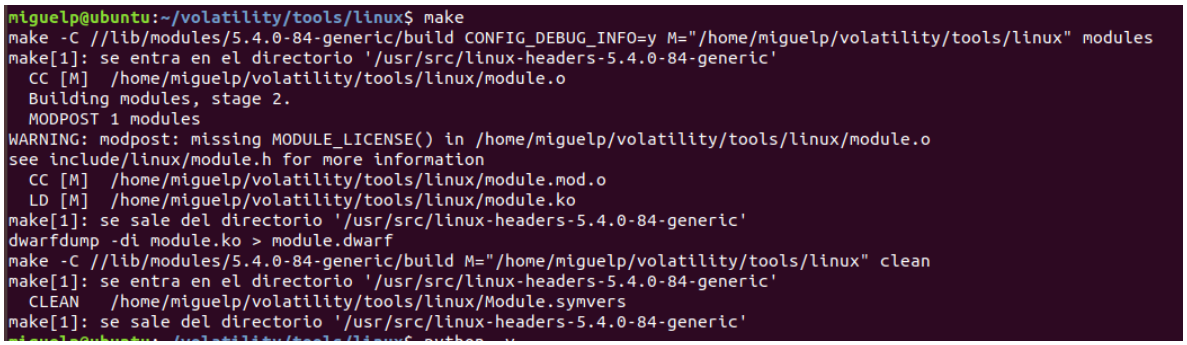


Figura 60 Error al ejecutar el comando MAKE escenario 1.

Fuente: Elaboración propia (2024).

Este error es común en la generación del perfil, para dar solución se debe realizar modificación del archivo “module.c”, agregando dos líneas con la misma sentencia como se evidencia a continuación (Para mayor detalle de la solución de este error ver la sección 6.4.4.2).

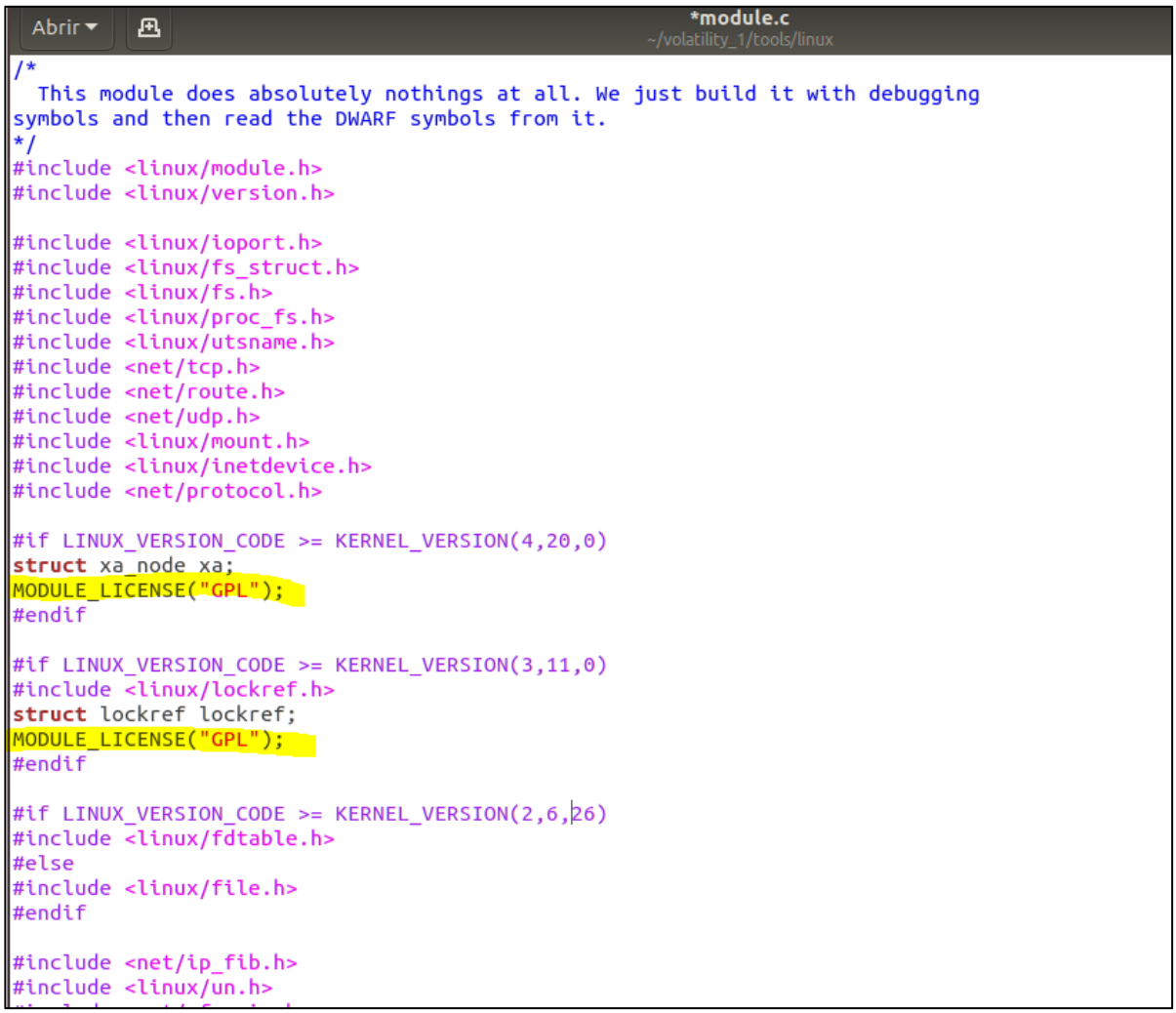


Figura 61 Solución de “ERROR: modpost: missing MODULE_LICENSE ()” escenario 1

Fuente: Elaboración propia (2024).

Seguidamente, se vuelve a ejecutar el comando make, en esta ocasión obteniendo un resultado positivo, el cual de manera genera indica:

- Se ingresó al directorio del kernel con éxito.
- Se compiló el módulo del kernel (module.o) sin errores aparentes.
- Se ejecutó la fase 2 de la construcción de módulos con éxito.

- Se realizó la fase de post procesamiento del módulo (MODPOST) sin errores.
- Se creó el archivo del módulo (module.ko) sin errores aparentes.
- Se ejecutó el comando dwarfdump para extraer información de depuración del módulo.
- Se limpiaron los archivos temporales de la compilación sin errores.

La línea que indica make[1]: se sale del directorio '/usr/src/linux-headers-5.4.0-84-generic' indica que el proceso de construcción del módulo del kernel ha finalizado, como se evidencia a continuación.

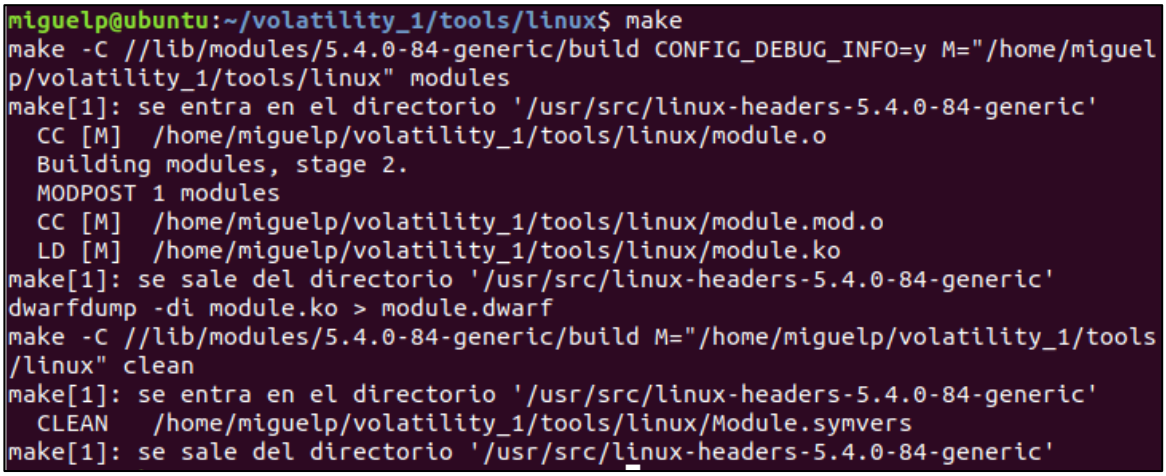


Figura 62 Generación exitosa de perfil escenario 1.

Fuente: Elaboración propia (2024).

Continuando con el proceso se debe generar el zip que se nombrar con el nombre del Kernel, para obtener este nombre se debe ejecutar el comando “uname -a”, tal como se muestra a continuación.

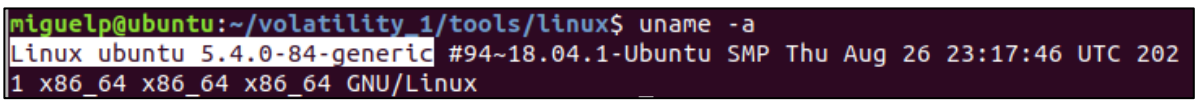


Figura 63 Nombre del kernel escenario 1.

Fuente: Elaboración propia (2024).

Este zip debe contener el archivo “module.dwarf” resultado de la ejecución del comando “make” y la ruta “/boot/System.map…”, esta información es necesaria para que Volatility reconozca correctamente el perfil del sistema operativo, se debe tener en cuenta que el archivo zip resultante no quede vacío y que contenga las dos rutas en cuestión para lo que es importante ejecutar el comando con permisos administrador.

```
miguelp@ubuntu:~$ sudo zip ubuntu18P_5.4.0-84-generic.zip ./volatility/tools/linux/module.dwarf /boot/System.map-5.4
.0-84-generic
  adding: volatility/tools/linux/module.dwarf (deflated 91%)
  adding: boot/System.map-5.4.0-84-generic (deflated 79%)
```

Figura 64 archivo ZIP con los archivos del perfil del sistema operativo escenario 1.

Fuente: Elaboración propia (2024).

El archivo zip resultando debe tener la estructura que se muestra a continuación.

```
Archive:  ubuntu18P_5.4.0-84-generic.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
  3337343  2024-01-25 11:11   volatility/tools/linux/module.dwarf
  4588571  2021-08-26 17:48   boot/System.map-5.4.0-84-generic
---------                     -------
  7925914                     2 files
```

Figura 65 Estructura del contenido del archivo escenario 1.

Fuente: Elaboración propia (2024).

El archivo Zip resultante debe guardarse en la siguiente ruta “/volatility/volatility/puglins/overlays/Linux/”, una vez verificado que este almacenado allí se finalizaría con la creación del perfil del sistema operativo.

```
miguelp@ubuntu:~/volatility/volatility/plugins/linux$ mv ubuntu18P_5.4.0-84-generic.zip /home/miguelp/volatility/vol
atility/plugins/overlays/linux/
miguelp@ubuntu:~/volatility/volatility/plugins/linux$ ls /home/miguelp/volatility/volatility/plugins/overlays/linux/
elf.py  __init__.py  linux.py  ubuntu18P_5.4.0-84-generic.zip
```

Figura 66 Mover perfil a la ruta especifica escenario 1.

Fuente: Elaboración propia (2024).

7.3.1.2.5 Verificación de perfil

Una vez finalizado los procedimientos anteriores, se debe ejecutar la herramienta volatility con el comando “vol.py –info | more”, para que liste todos los profiles que están disponibles, para este caso se debe verificar que el creado se encuentre en la lista corroborando que el proceso se realizó correctamente.

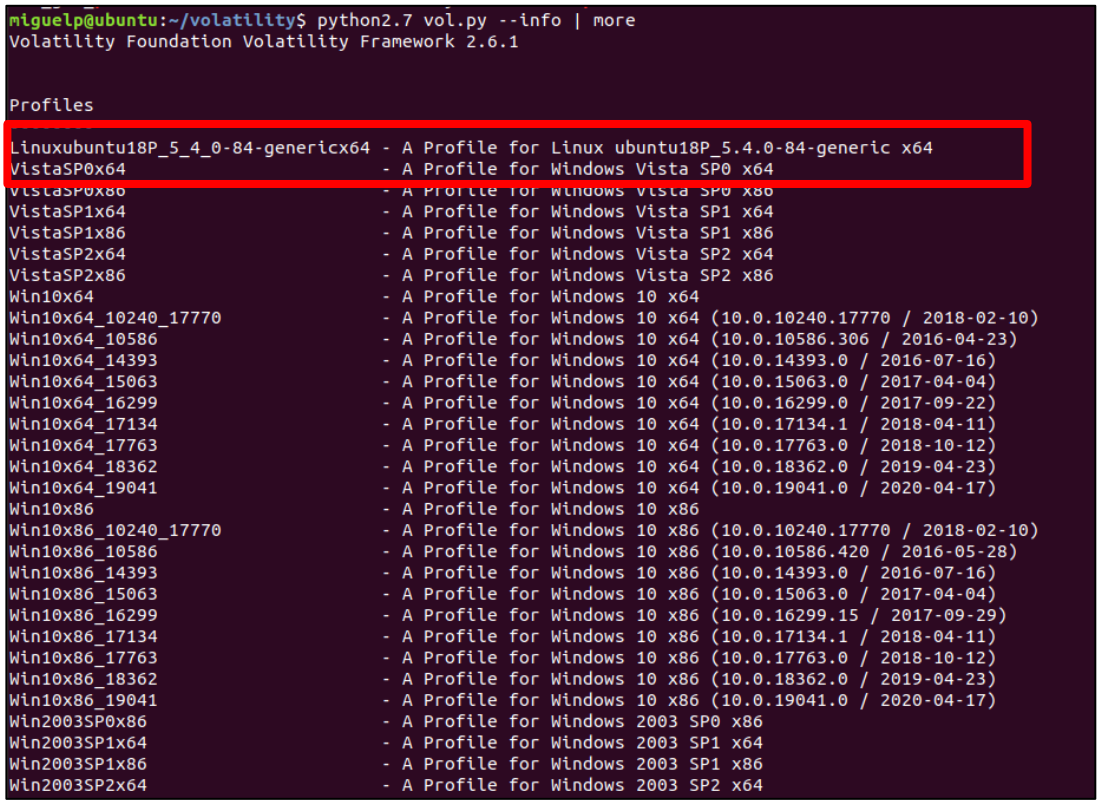


Figura 67 Validación de perfil funcionando en Volatility2.6

Fuente: Elaboración propia (2024).

Así mismo, se vuelve a aseverar que el este perfil solo funciona con esta versión exacta de sistema operativo.

Por otra parte, se pueden ejecutar algunos comandos relevantes para comprobar su funcionamiento, como los siguientes que serán ejecutados con el perfil obtenido

únicamente a manera de ejemplo, teniendo como volcado de memoria RAM al mismo sistema al cual se le realizó el perfil antes mencionado:

- Comando linux_pslist: Lista los procesos en ejecución en el sistema operativo.

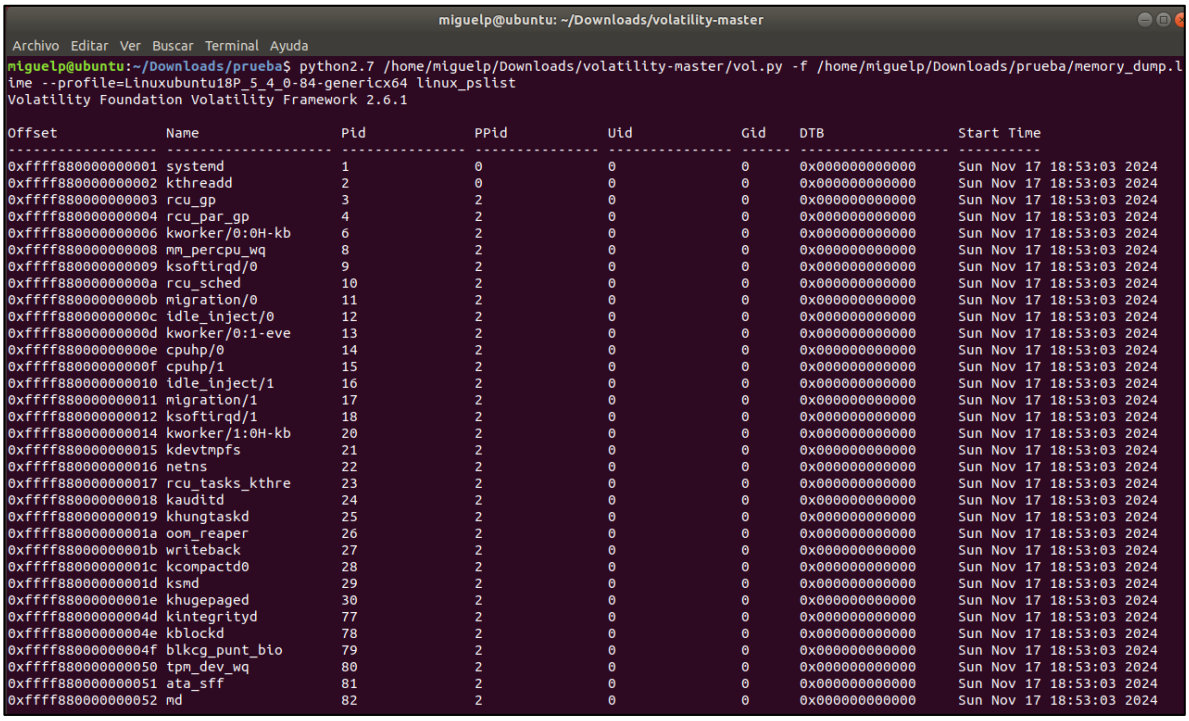


Figura 68 Resultado ejecución de comando linux_pslist escenario 1.

Fuente: Elaboración propia (2024).

- Comando linux_lsof: Muestra los archivos abiertos por los procesos en el sistema.

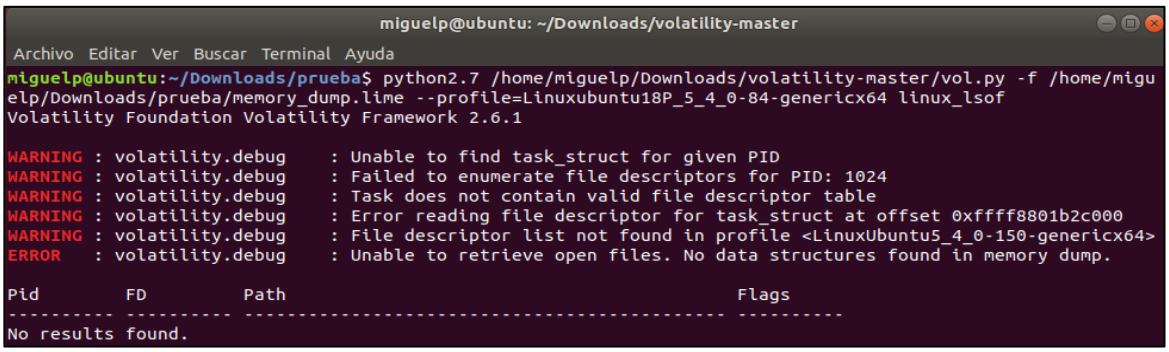


Figura 69 Ejecución Comando linux_lsof escenario 1.

Fuente: Elaboración propia (2024).

- Comando linux_netstat: Detalla las conexiones de red activas y los puertos en escucha.

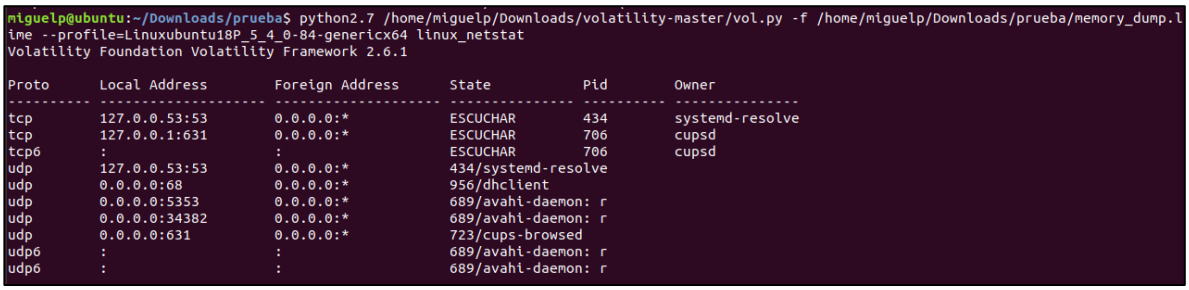


Figura 70 Ejecución de comando linux_netstat escenario 1.

Fuente: Elaboración propia (2024).

- Comando linux_sockets: Enumera los sockets TCP y UDP activos.

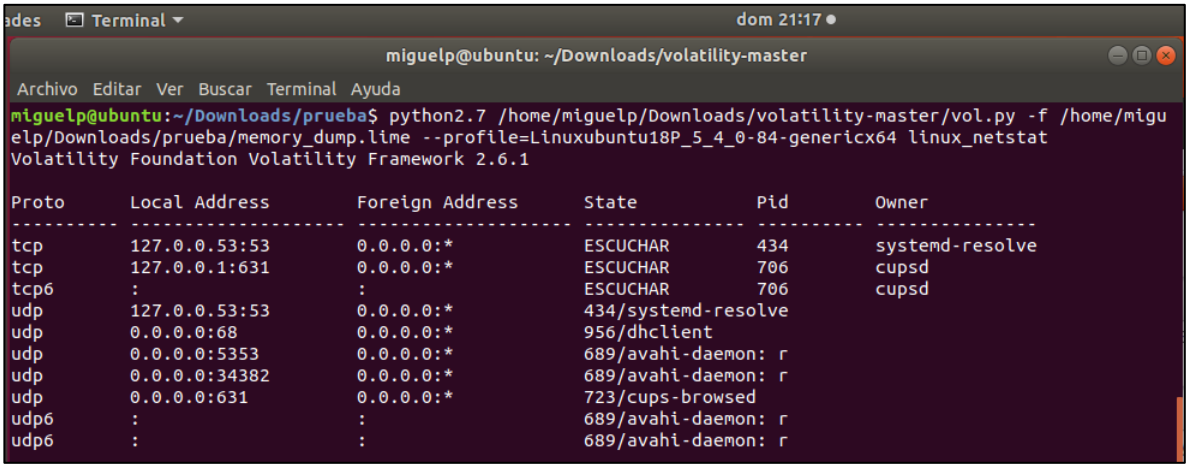


Figura 71 Ejecución de comnado Linux_sockets escenario 1.

Fuente: Elaboración propia (2024).

7.3.1.3 Escenario 2: Ubuntu-22.04.3

7.3.1.3.1 Revisión de la existencia de un perfil para la versión exacta del sistema operativo

Como primer paso se debe revisar la versión exacta del sistema operativo, que para este caso se realizó ejecutando el comando “uname -a” y “lsb_release -a”, con lo cual se obtiene que la versión es un Ubuntu 22.04.3 LTS.

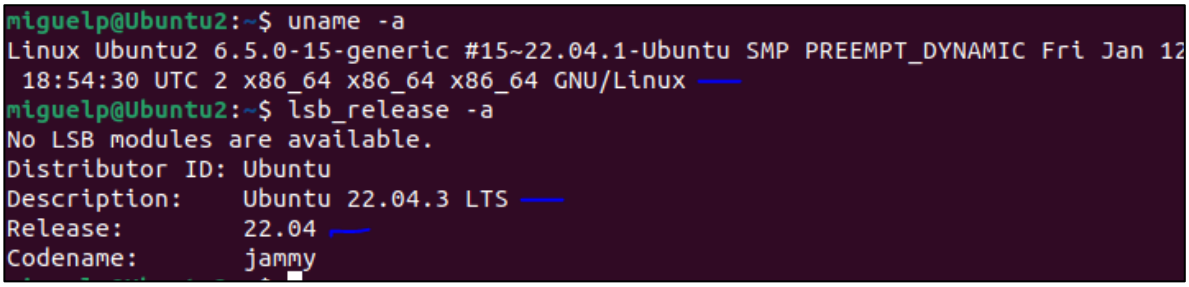


Figura 72 Información Ubuntu 22 procedimiento 2.

Fuente: Elaboración propia (2024).

Seguidamente con la versión del sistema operativo se verificó en el repositorio de GitHub si ya existe un perfil creado para esa versión en especificó, identificando que para el caso en cuestión la versión del sistema operativo aún no cuenta con un perfil creado ya que la versión más reciente con perfil es la 18.04.3.

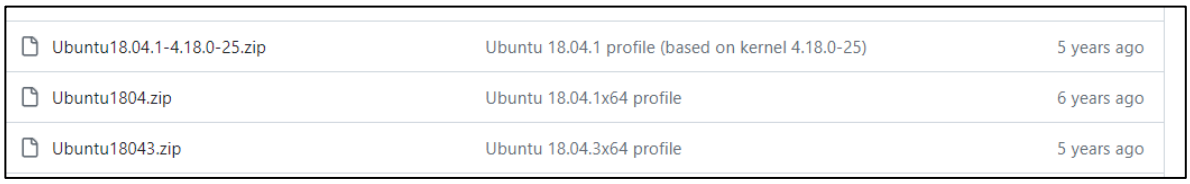


Figura 73 Versiones de perfiles disponibles para Ubuntu 22.

Fuente: Elaboración propia (2024).

7.3.1.3.2 Instalar herramientas y dependencias.

Este representa el paso a paso sugerido para realizar la correcta instalación de todos los complementos necesarios para la instalación de Volatility, y asegurar la menor cantidad de errores por incompatibilidades, el cual consta de la instalación de:

Como primer paso la instalación de “build-essential”, para lo cual, se realizó la actualización de la biblioteca “apt update” y la posterior instalación “apt-get install build-essential”, como se muestra a continuación.

```
miguelp@Ubuntu2:~$ sudo apt update
Obj:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Obj:2 http://co.archive.ubuntu.com/ubuntu jammy InRelease
Obj:3 http://co.archive.ubuntu.com/ubuntu jammy-updates InRelease
Obj:4 http://co.archive.ubuntu.com/ubuntu jammy-backports InRelease
Des:5 http://co.archive.ubuntu.com/ubuntu jammy/main Translation-es [332 kB]
Des:6 http://co.archive.ubuntu.com/ubuntu jammy/restricted Translation-es [964 B]
Des:7 http://co.archive.ubuntu.com/ubuntu jammy/universe Translation-es [1.356 kB]
Des:8 http://co.archive.ubuntu.com/ubuntu jammy/multiverse Translation-es [68,2 kB]
Descargados 1.758 kB en 1s (1.436 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 189 paquetes. Ejecute «apt list --upgradable» para verlos.
miguelp@Ubuntu2:~$ sudo apt-get install build-essential
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
build-essential ya está en su versión más reciente (12.9ubuntu3).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 189 no actualizados.
```

Figura 74 Verificación de paquete build-essential escenario 2.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación de “flex”, como se muestra a continuación.

```
miguelp@Ubuntu2:~/volatility/tools/linux$ sudo apt install flex
[sudo] contraseña para miguelp:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libfl-dev libfl2 libsigsegv2 m4
Paquetes sugeridos:
  bison flex-doc m4-doc
Se instalarán los siguientes paquetes NUEVOS:
  flex libfl-dev libfl2 libsigsegv2 m4
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 188 no actualizados.
Se necesita descargar 537 kB de archivos.
Se utilizarán 1.552 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://co.archive.ubuntu.com/ubuntu jammy/main amd64 libsigsegv2 amd64 2.13-1ubuntu3 [14,6 kB]
Des:2 http://co.archive.ubuntu.com/ubuntu jammy/main amd64 m4 amd64 1.4.18-5ubuntu2 [199 kB]
Des:3 http://co.archive.ubuntu.com/ubuntu jammy/main amd64 flex amd64 2.6.4-8build2 [307 kB]
Des:4 http://co.archive.ubuntu.com/ubuntu jammy/main amd64 libfl2 amd64 2.6.4-8build2 [10,7 kB]
Des:5 http://co.archive.ubuntu.com/ubuntu jammy/main amd64 libfl-dev amd64 2.6.4-8build2 [6.236 B]
Descargados 537 kB en 2s (354 kB/s)
Seleccionando el paquete libsigsegv2:amd64 previamente no seleccionado.
(Leyendo la base de datos ... 211944 ficheros o directorios instalados actualmen
te.)
Preparando para desempaquetar .../libsigsegv2_2.13-1ubuntu3_amd64.deb ...
Desempaquetando libsigsegv2:amd64 (2.13-1ubuntu3) ...
```

Figura 75 Instalación de Flex escenario 2

Fuente: Elaboración propia (2024).

Seguidamente se realiza la instalación de Python2.7, indispensable para el funcionamiento de Volatility, como se muestra a continuación.

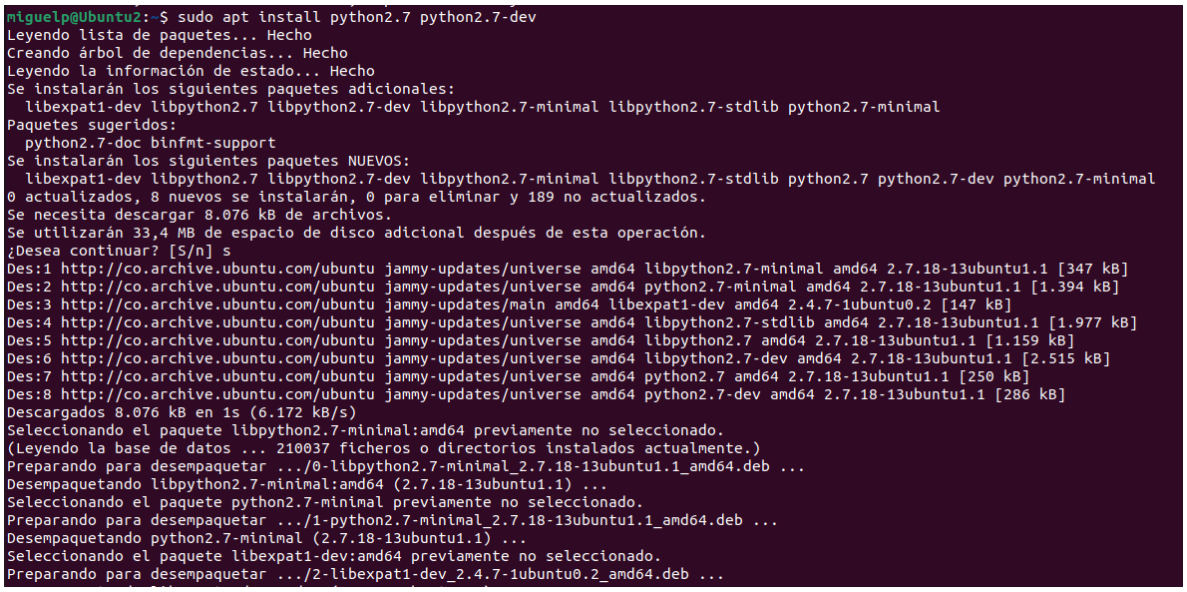


Figura 76 Instalación de Python2.7 escenario 2.

Fuente: Elaboración propia (2024).

Posteriormente se debe realizar la instalación de “curl”, como se muestra a continuación.

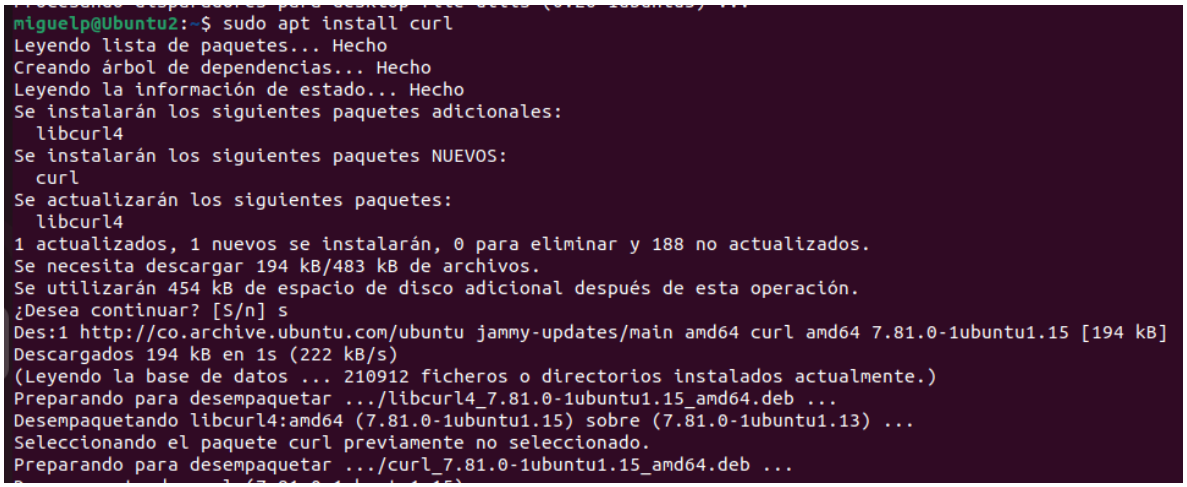


Figura 77 Instalación de Curl escenario 2.

Fuente: Elaboración propia (2024).

Continuando se debe realizar la instalación de “PIP”, ejecutando el comando “curl https://bootstrap.pypa.io/get-pip.py --output get-pip.py” como se muestra a continuación.

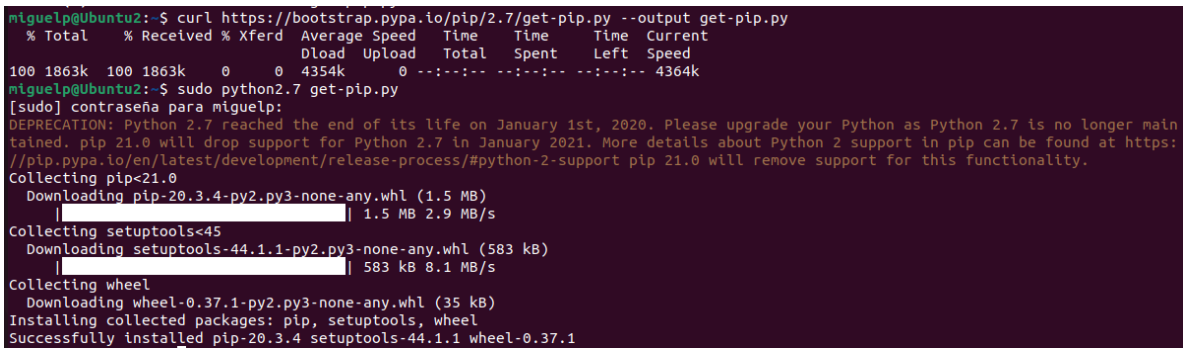


Figura 78 Instalación de PIP escenario 2.

Fuente: Elaboración propia (2024).

Seguidamente se debe realizar la instalación de “GIT”, como se muestra a continuación.

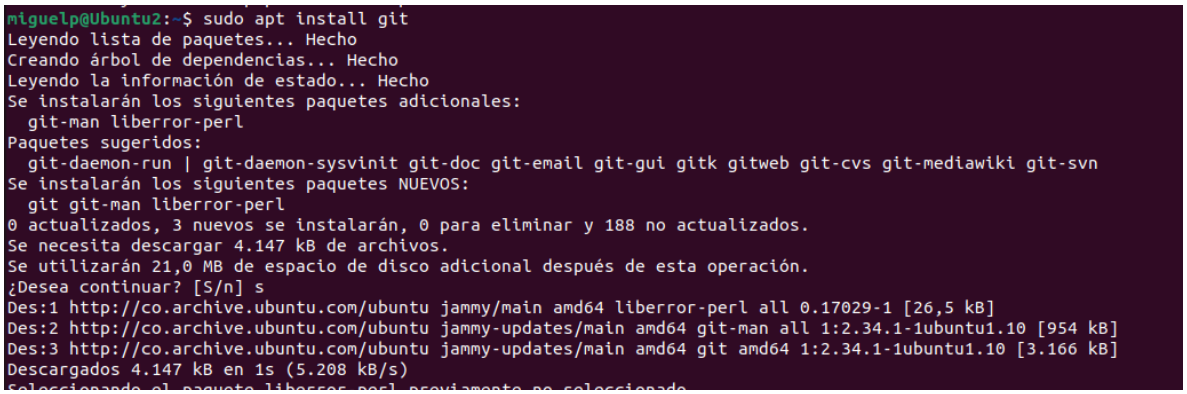


Figura 79 Instalación de GIT escenario 2.

Fuente: Elaboración propia (2024).

Seguidamente, se debe realizar la instalación de “bison”, el cual, permite la compilación de aplicaciones relacionadas con Kernel, ejecutando el comando como se muestra a continuación.

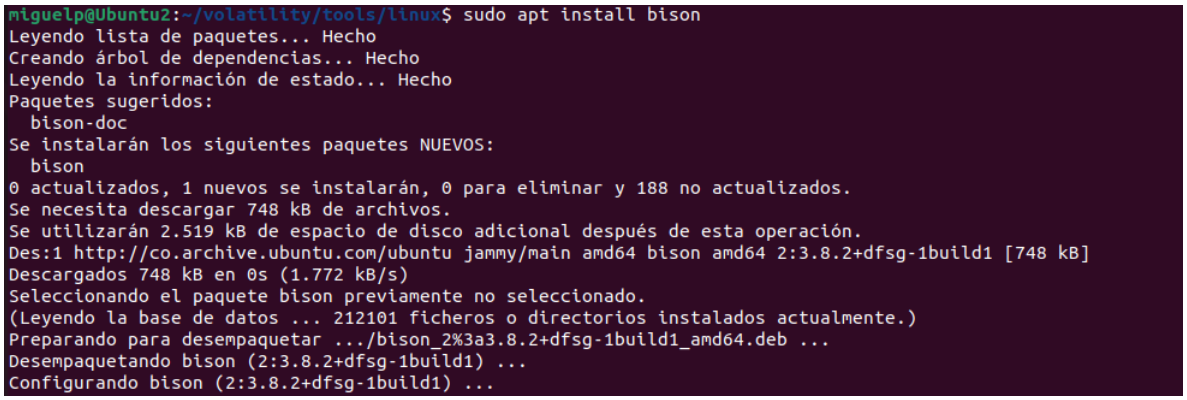


Figura 80 Instalación Bison escenario 2.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “Distorm3”, como se muestra a continuación.

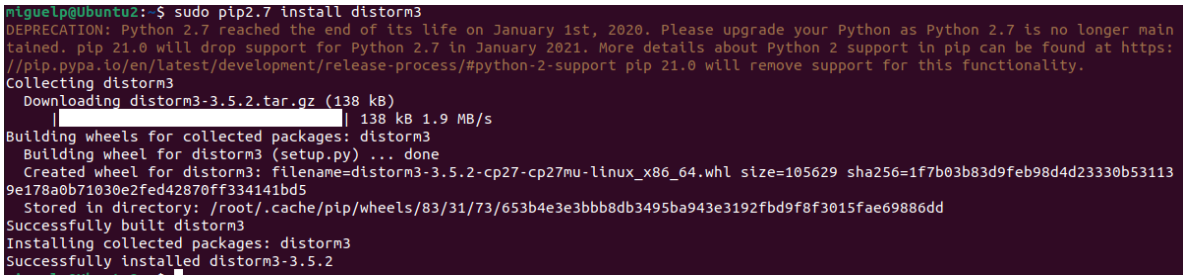


Figura 81 Instalación de dependencia distorm3 escenario 2.

Fuente: Elaboración propia (2024).

De igual manera, se debe realizar la instalación dependencia de PIP “yara-python”, como se muestra a continuación.

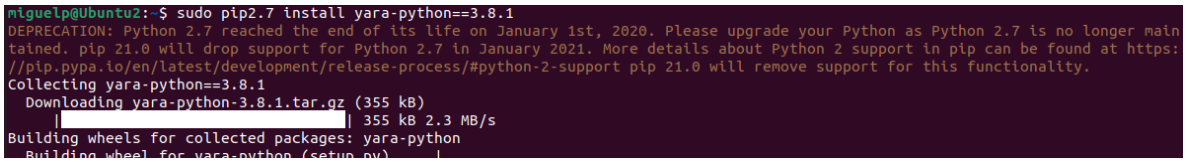


Figura 82 Instalación de dependencia yara-python escenario 2

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “Pycrypto”, como se muestra a continuación.

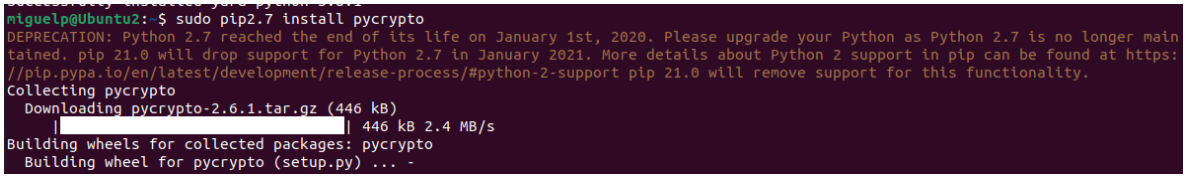


Figura 83 Instalación de dependencia pycrypto escenario 2.

Fuente: Elaboración propia (2024).

Así mismo, se debe realizar la instalación dependencia de PIP “pillow”, como se muestra a continuación.

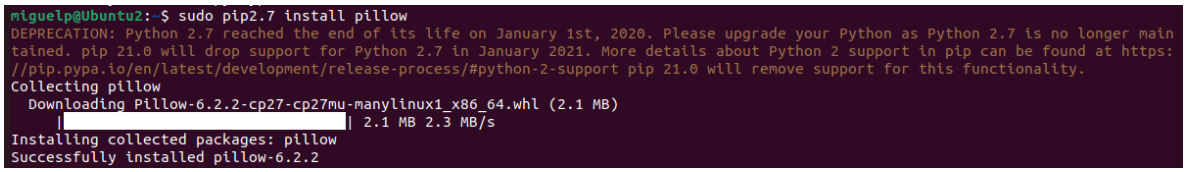


Figura 84 Instalación de dependencia pillow escenario 2.

Fuente: Elaboración propia (2024).

Posteriormente, se debe realizar la instalación dependencia de PIP “openpyxl==2.6.4”, como se muestra a continuación.

Figura 85 Instalación de dependencia openpyxl==2.6.4 escenario 2.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “ujson”, como se muestra a continuación.

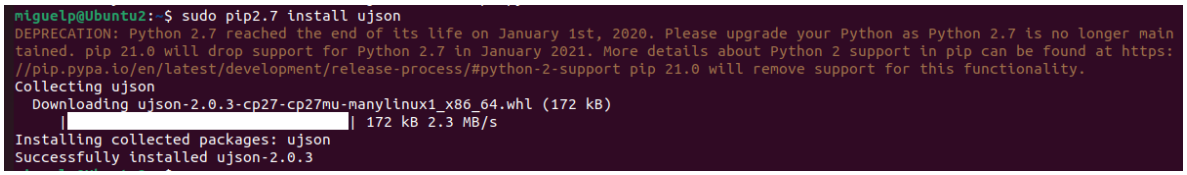


Figura 86 Instalación de ujson escenario 2

Fuente: Elaboración propia (2024).

Una vez instalados todos los complementos se realiza la verificación de la correcta instalación de estos ejecutando el comando “sudo pip2.7 list”, dando como resultado las 11 dependencias que se muestran a continuación.

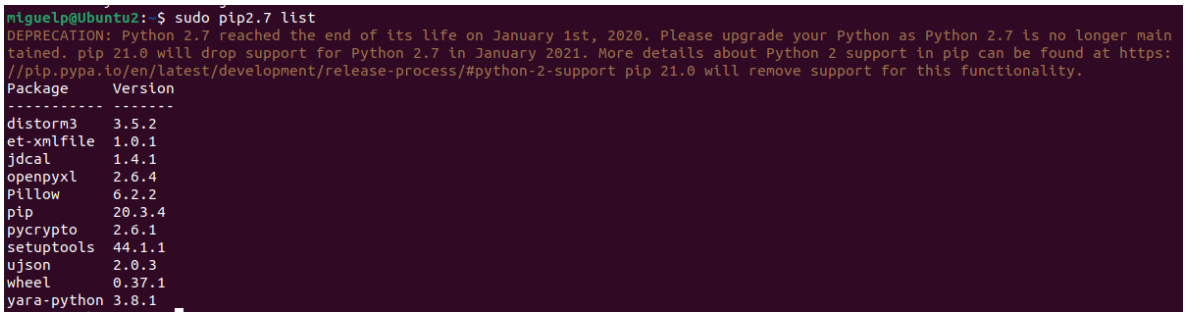


Figura 87 Verificación de instalación de dependencias escenario 2.

Fuente: Elaboración propia (2024).

7.3.1.3.3 Clonar repositorio de Volatility e instalación opcional

Se debe verificar una ruta donde se quiera clonar el repositorio de Volatility, para este caso será “USER\home\”, ejecutando el comando “https://github.com/volatilityfoundation/volatility.git” como se muestra a continuación.

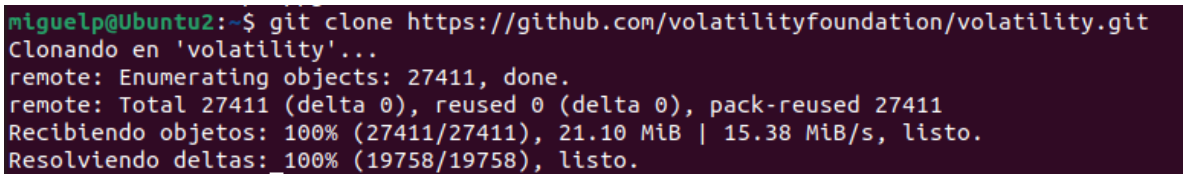


Figura 88 Clonación de repositorio Volatility Escenario 2.

Fuente: Elaboración propia (2024).

Por otra parte, la instalación opcional de Volatility, para este escenario 2 no se realizó dicha instalación.

7.3.1.3.4 Creación del perfil.

Una vez realizados los pasos anteriores se debe realizar la creación del perfil, para lo cual se accede a la carpeta de Volatility en donde se haya realizado la Clonación o instalación de este e ingresar a la siguiente ruta "…/volatility/tools/linux/", donde se encuentran los siguientes archivos "Makefile", "Makefile.enterprise", "module.c", y la carpeta "kcore", como se evidencia a continuación.

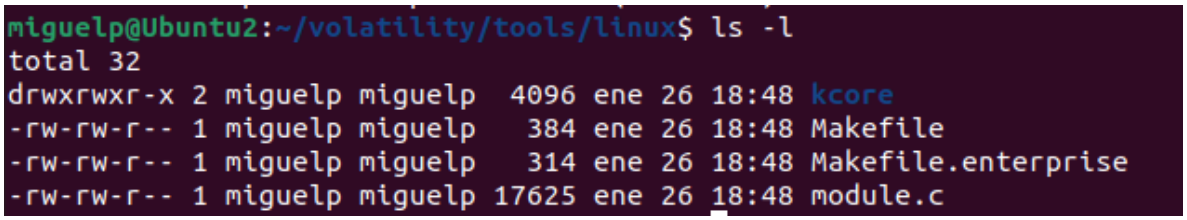


Figura 89 Contenido de la ruta "…/volatility/tools/linux/" escenario 2.

Fuente: Elaboración propia (2024).

En dicha ruta se encuentran los archivos necesarios para la generación del perfil, para lo cual se ejecuta el comando "make", para este caso se generó un error que

indica “ERROR: modpost: missing MODULE_LICENSE ()”, como se evidencia a continuación.

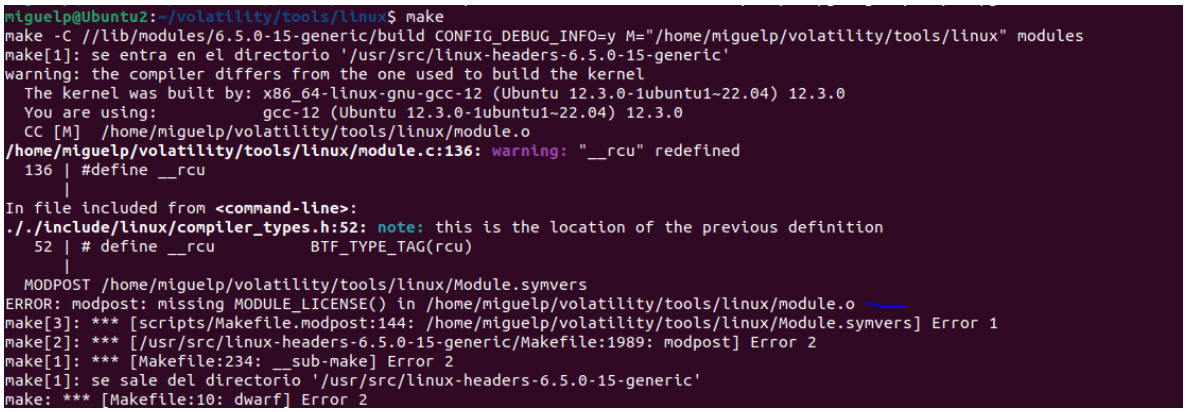


Figura 90 Error al ejecutar el comando MAKE escenario 2

Fuente: Elaboración propia (2024).

Este error es común en la generación del perfil, para dar solución se debe realizar modificación del archivo “module.c”, agregando dos líneas con la misma sentencia como se evidencia a continuación (Para mayor detalle de la solución de este error ver la sección 6.4.4.2).

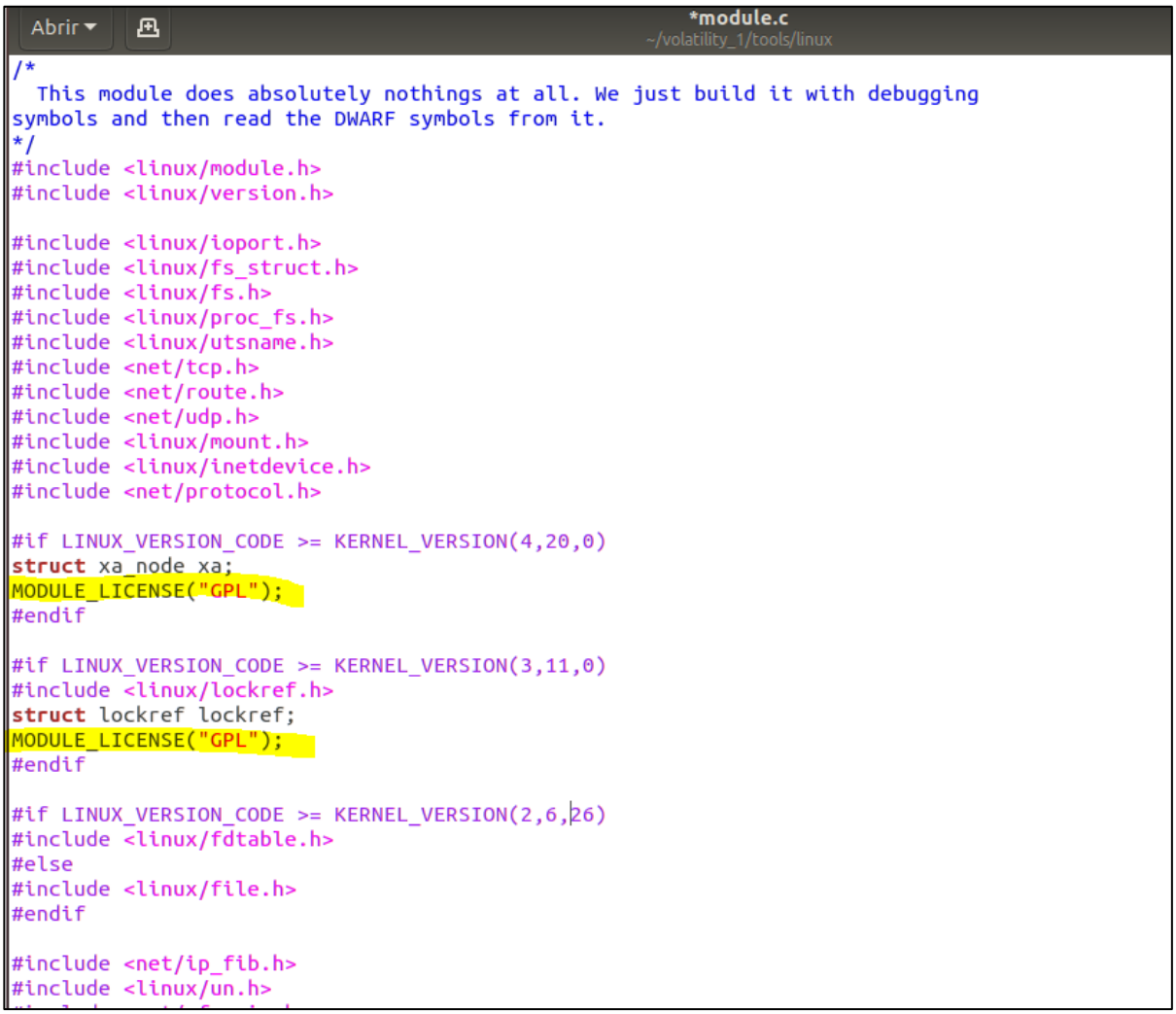


Figura 91 Solución de “ERROR: modpost: missing MODULE_LICENSE ()” escenario 2.

Fuente: Elaboración propia (2024).

Seguidamente, se vuelve a ejecutar el proceso, para lo cual se ejecuta el comando “make”, para este caso se generó un error que indica “gcc-12: not found”, como se evidencia a continuación.

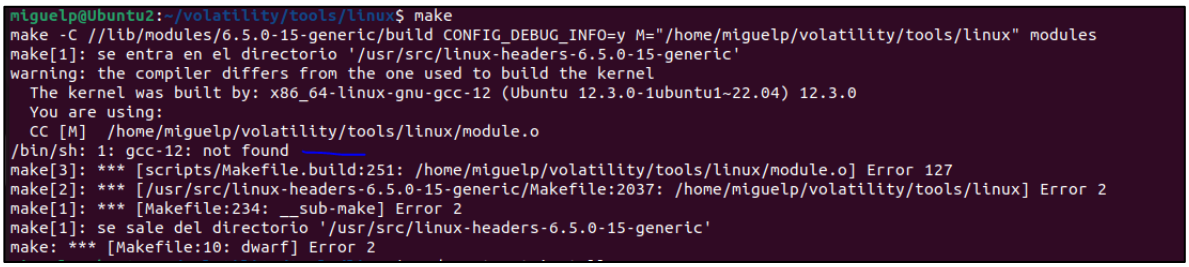


Figura 92 Error 2 al ejecutar el comando MAKE escenario 2.

Fuente: Elaboración propia (2024).

Este error es común en la generación del perfil en las últimas versiones de Ubuntu, para dar solución se debe realizar la instalación y configuración automática del compilador gcc-12, como se evidencia a continuación (Para mayor detalle de la solución de este error ver la sección 6.4.2.3).

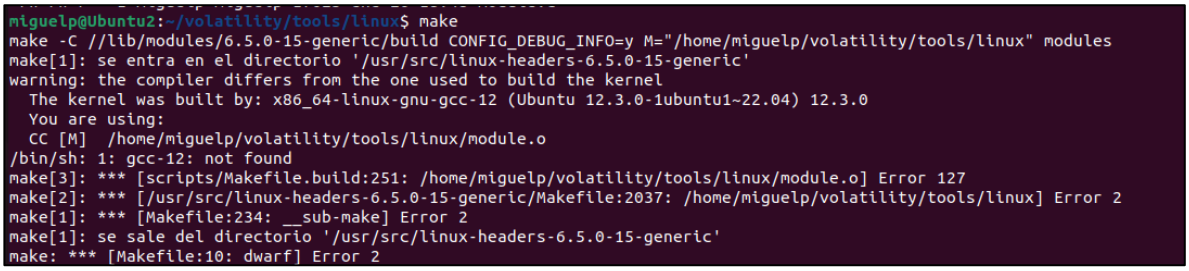


Figura 93 Solución de “gcc-12: not found” escenario 2.

Fuente: Elaboración propia (2024).

Seguidamente, se vuelve a ejecutar el comando make, en esta ocasión obteniendo un resultado positivo, el cual de manera genera indica:

- Se ingresó al directorio del kernel con éxito.
- Se compiló el módulo del kernel (module.o) sin errores aparentes.
- Se ejecutó la fase 2 de la construcción de módulos con éxito.
- Se realizó la fase de post procesamiento del módulo (MODPOST) sin errores.

- Se creó el archivo del módulo (module.ko) sin errores aparentes.
- Se ejecutó el comando dwarfdump para extraer información de depuración del módulo.
- Se limpiaron los archivos temporales de la compilación sin errores.

La línea que indica make[1]: se sale del directorio '/usr/src/linux-headers-5.4.0-84-generic' indica que el proceso de construcción del módulo del kernel ha finalizado, como se evidencia a continuación.

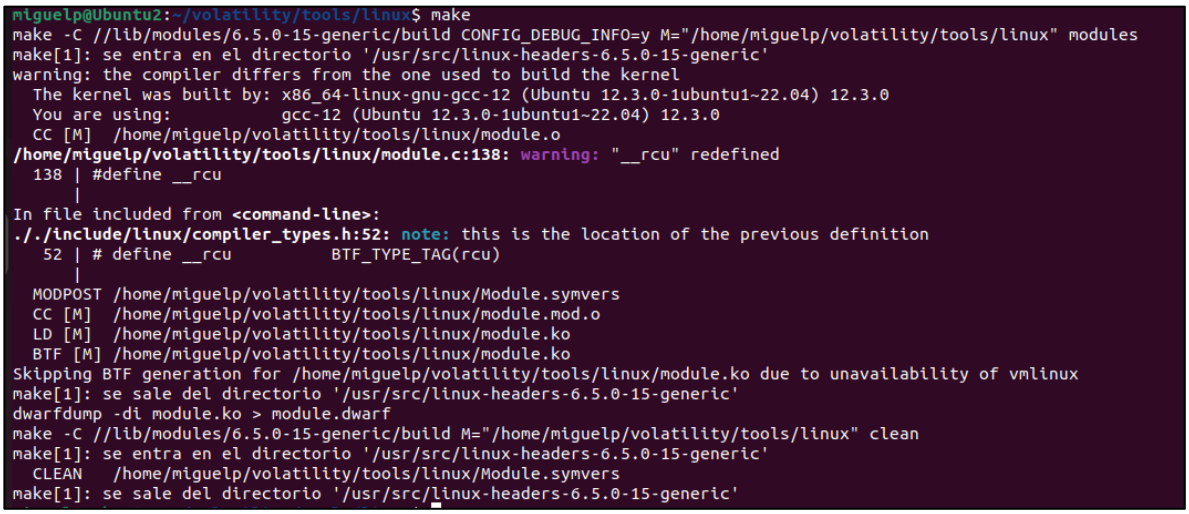


Figura 94 Generación exitosa de perfil escenario 2.

Fuente: Elaboración propia (2024).

Continuando con el proceso se debe generar el zip que se nombrar con el nombre del Kernel, para obtener este nombre se debe ejecutar el comando “uname -a”, tal como se muestra a continuación.

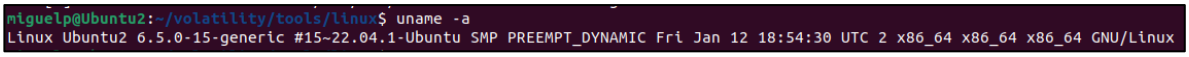


Figura 95 Nombre del kernel escenario 2.

Fuente: Elaboración propia (2024).

Este zip debe contener el archivo “module.dwarf” resultado de la ejecución del comando “make” y la ruta “/boot/System.map…”, esta información es necesaria para que Volatility reconozca correctamente el perfil del sistema operativo, se debe tener en cuenta que el archivo zip resultante no quede vacío y que contenga las dos rutas en cuestión para lo que es importante ejecutar el comando con permisos administrador.

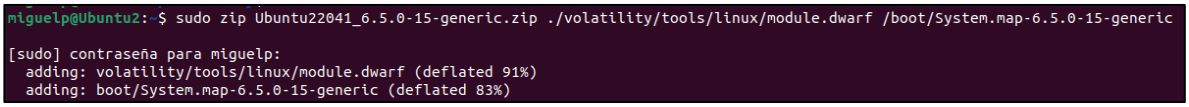


Figura 96 Archivo ZIP con los archivos del perfil del sistema operativo escenario 2.

Fuente: Elaboración propia (2024).

El archivo zip resultando debe tener la estructura que se muestra a continuación.

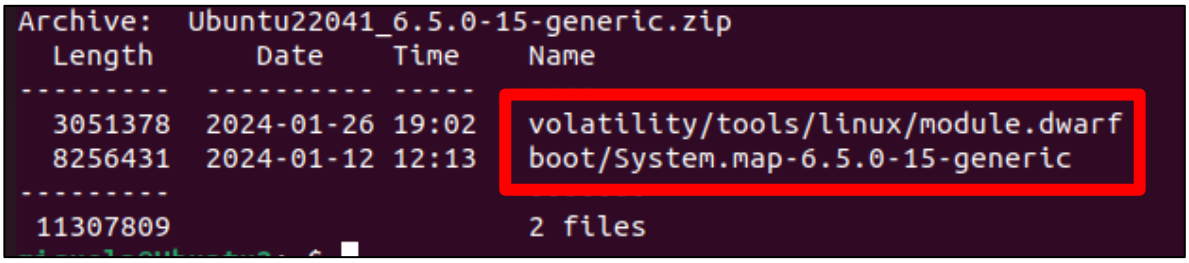


Figura 97 Estructura del contenido del archivo escenario 2.

Fuente: Elaboración propia (2024).

El archivo Zip resultante debe guardarse en la siguiente ruta “/volatility/volatility/plugins/overlays/Linux/”, una vez verificado que este almacenado allí se finalizaría con la creación del perfil del sistema operativo.

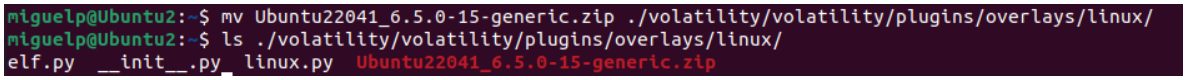


Figura 98 Mover perfil a la ruta especifica escenario 2.

Fuente: Elaboración propia (2024).

7.3.1.3.5 Verificación de perfil

Una vez finalizado los procedimientos anteriores, se debe ejecutar la herramienta volatility con el comando “vol.py –info | more”, para que liste todos los profiles que están disponibles, para este caso se debe verificar que el creado se encuentre en la lista corroborando que el proceso se realizó correctamente.

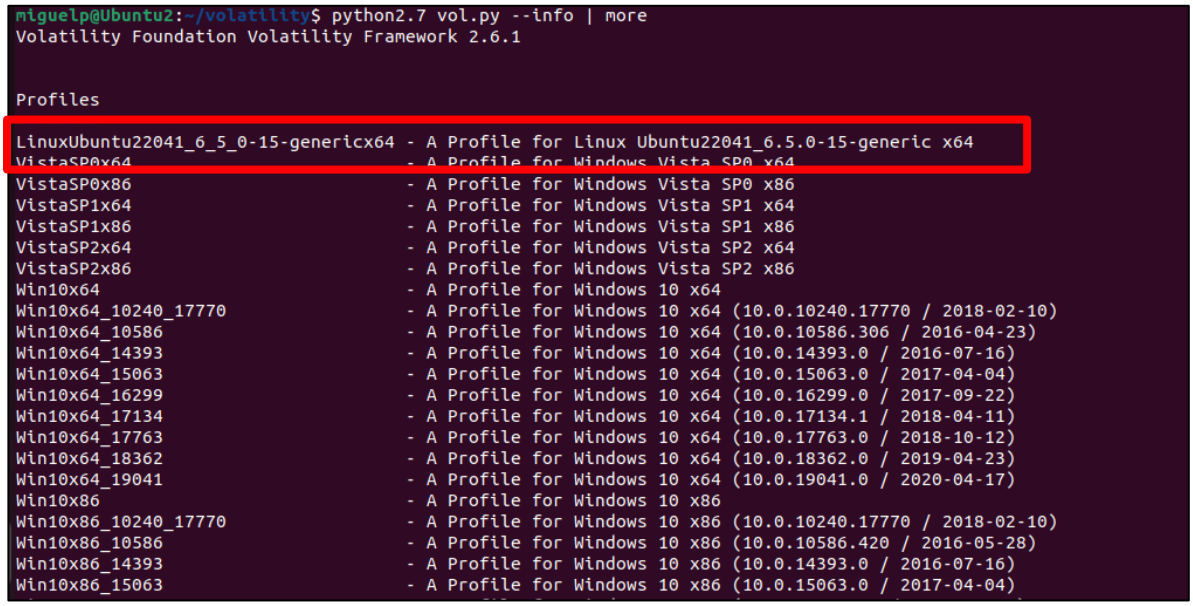


Figura 99 Validación de perfil funcionando en Volatility2.6.

Fuente: Elaboración propia (2024).

Así mismo, se vuelve a aseverar que el este perfil solo funciona con esta versión exacta de sistema operativo.

Por otra parte, se pueden ejecutar algunos comandos relevantes para comprobar su funcionamiento, como los siguientes que serán ejecutados con el perfil obtenido únicamente a manera de ejemplo, teniendo como volcado de memoria RAM al mismo sistema al cual se le realizó el perfil antes mencionado:

- Comando linux_pslist: Lista los procesos en ejecución en el sistema operativo.

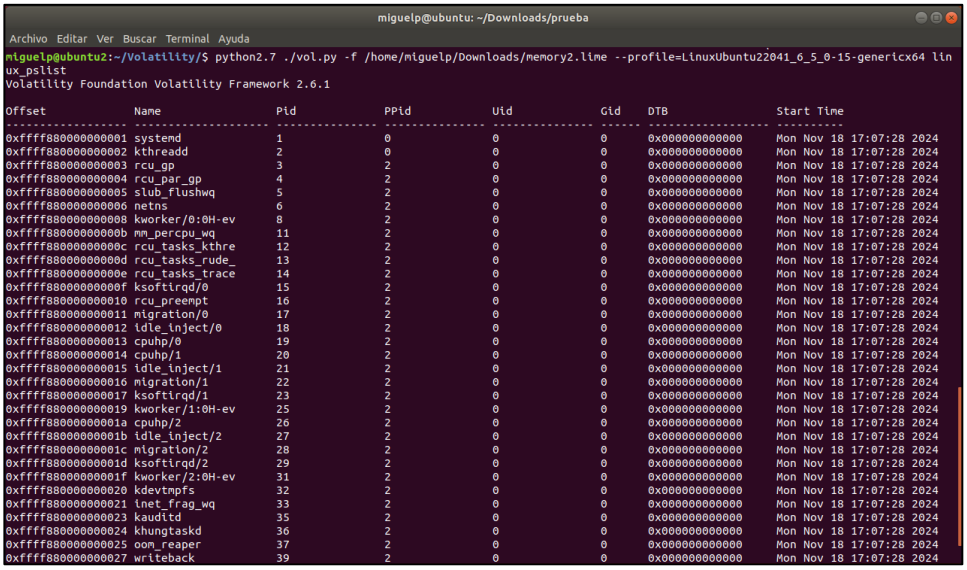


Figura 100 Resultado ejecución de comando linux_pslist escenario 2.

Fuente: Elaboración propia (2024).

- Comando linux_bash: Recupera el historial de comandos de las sesiones de Bash.

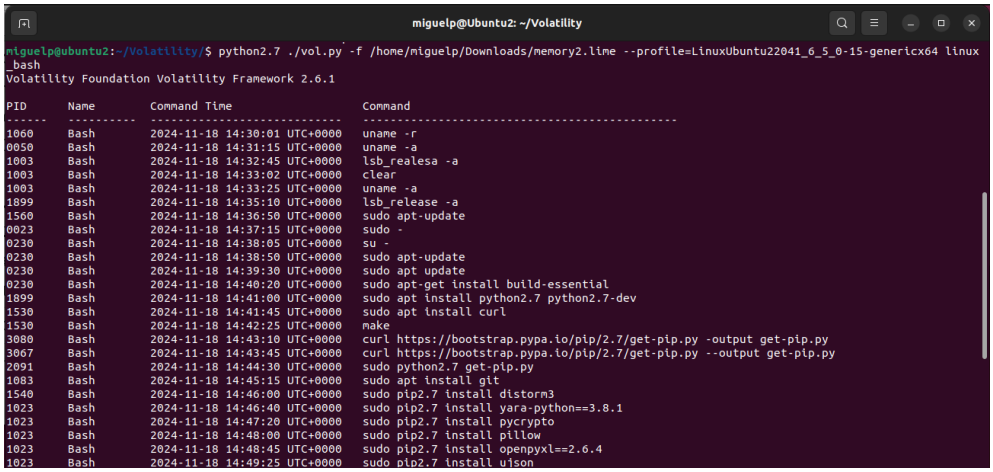


Figura 101 Ejecución Comando linux_bash escenario 2.

Fuente: Elaboración propia (2024).

- Comando linux_netstat: Detalla las conexiones de red activas y los puertos en escucha.

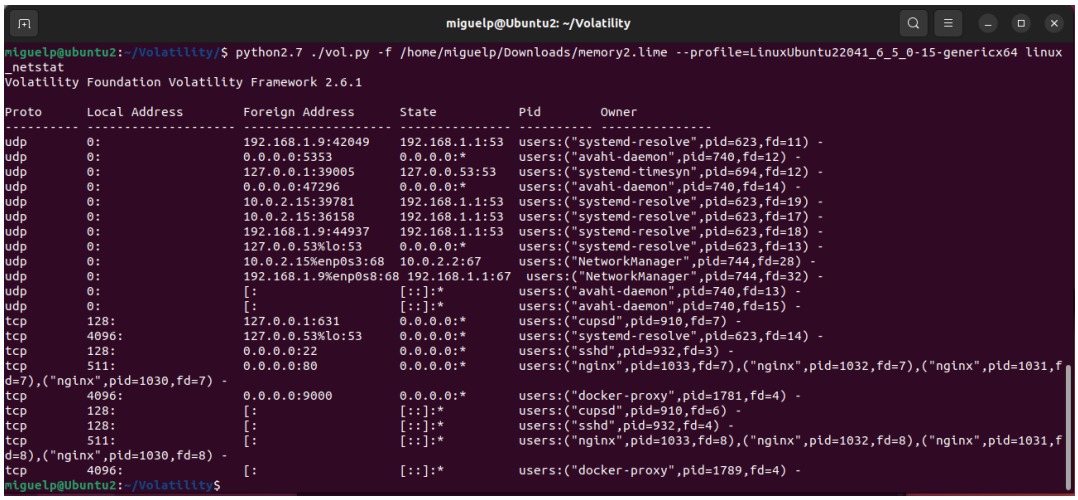


Figura 102 Ejecución de comando linux_netstat escenario 2.

Fuente: Elaboración propia (2024).

- Comando linux_sockets: Enumera los sockets TCP y UDP activos.

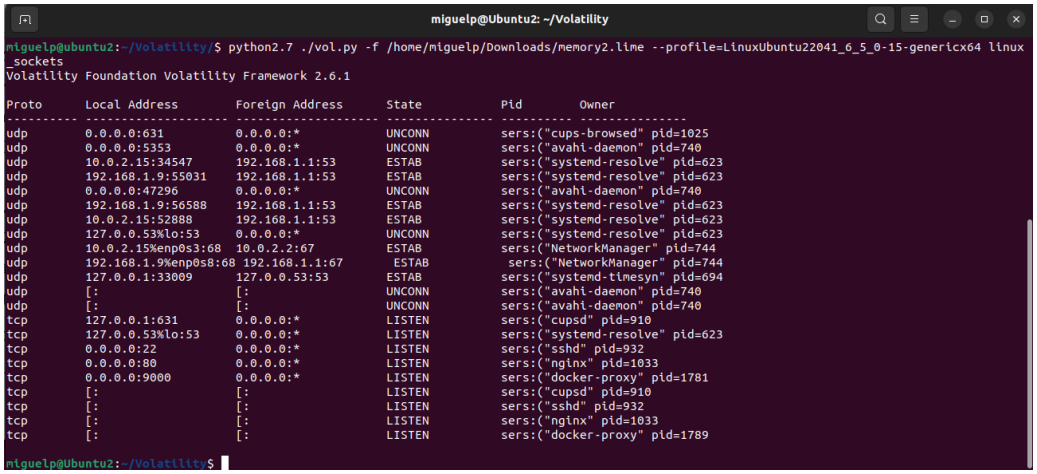


Figura 103 Ejecución de comnado Linux_sockets escenario 2.

Fuente: Elaboración propia (2024).

7.3.1.4 Escenario 3 Debian GNU/Linux 11.8.0(bullseye).:

7.3.1.4.1 Revisión de la existencia de un perfil para la versión exacta del sistema operativo.

Como primer paso se debe revisar la versión exacta del sistema operativo, que para este caso se realizó ejecutando el comando “uname -a” y “lsb_release -a”, con lo cual se obtiene que la versión es un Debian GNU/Linux 11.8.0 (bullseye).

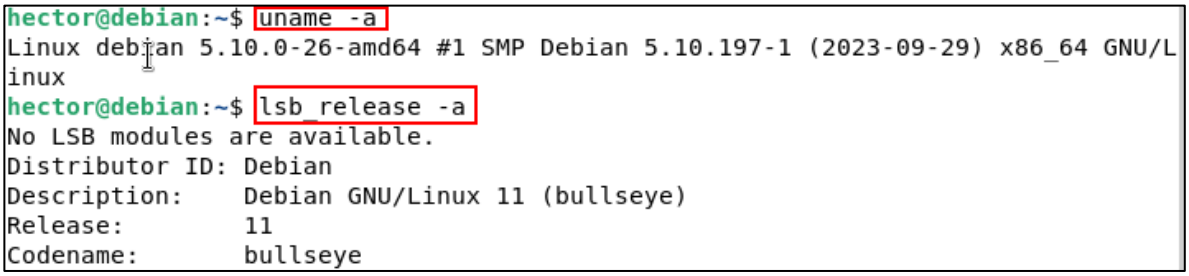
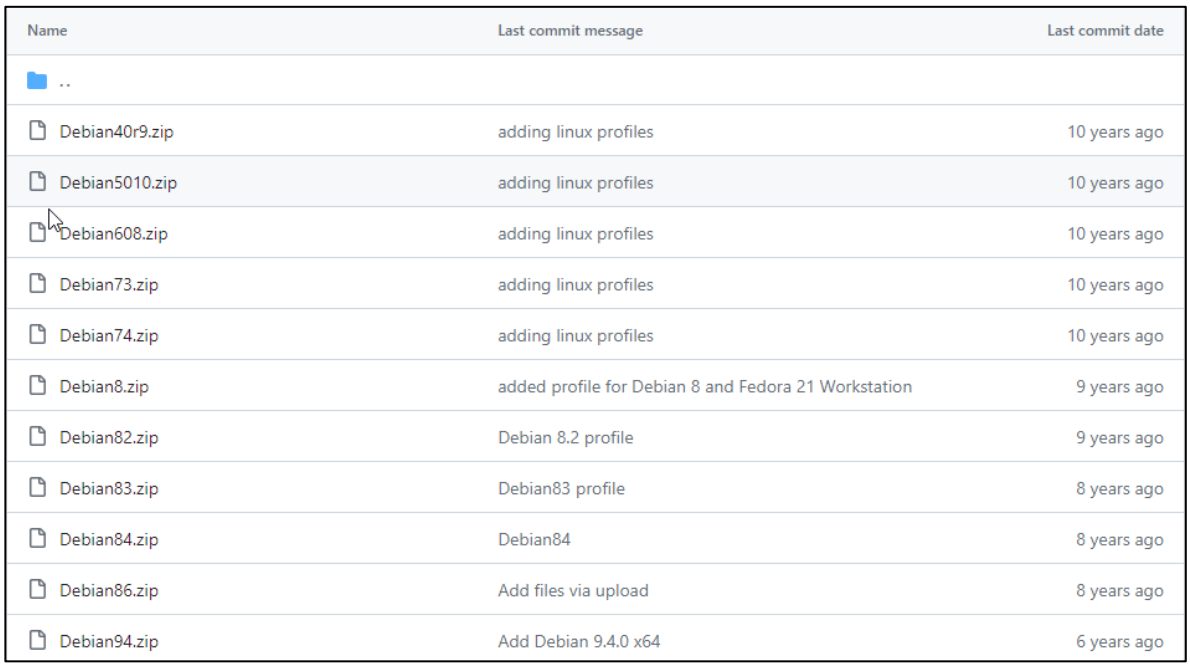


Figura 104 Información procedimiento 3.

Fuente: Elaboración propia (2024).

Seguidamente con la versión del sistema operativo se verificó en el repositorio de GitHub si ya existe un perfil creado para esa versión en especificó, identificando que para el caso en cuestión la versión del sistema operativo aún no cuenta con un perfil creado ya que la versión más reciente con perfil es la Debian 9.4.0.



Name	Last commit message	Last commit date
..		
Debian40r9.zip	adding linux profiles	10 years ago
Debian5010.zip	adding linux profiles	10 years ago
Debian608.zip	adding linux profiles	10 years ago
Debian73.zip	adding linux profiles	10 years ago
Debian74.zip	adding linux profiles	10 years ago
Debian8.zip	added profile for Debian 8 and Fedora 21 Workstation	9 years ago
Debian82.zip	Debian 8.2 profile	9 years ago
Debian83.zip	Debian83 profile	8 years ago
Debian84.zip	Debian84	8 years ago
Debian86.zip	Add files via upload	8 years ago
Debian94.zip	Add Debian 9.4.0 x64	6 years ago

Figura 105 Versiones de perfiles disponibles para Debian.

Fuente: Elaboración propia (2024).

7.3.1.4.2 Instalar herramientas y dependencias.

Este representa el paso a paso sugerido para realizar la correcta instalación de todos los complementos necesarios para la instalación de Volatility, y asegurar la menor cantidad de errores por incompatibilidades, el cual consta de la instalación de:

Como primer paso la instalación de “build-essential”, para lo cual, se realizó la actualización de la biblioteca “apt update” y la posterior instalación “apt-get install build-essential”, como se muestra a continuación.

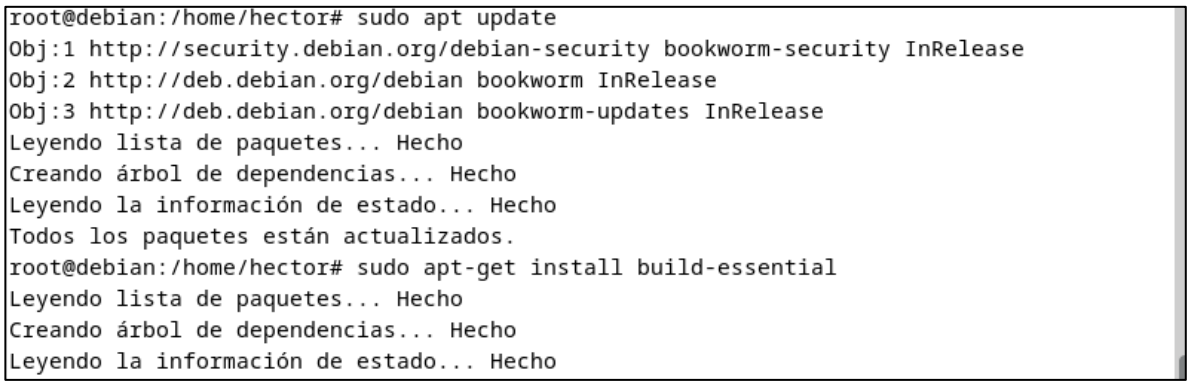


Figura 106 Verificación de paquete build-essential escenario 3.

Fuente: Elaboración propia (2024).

Seguidamente se realiza la instalación de Python2.7, indispensable para el funcionamiento de Volatility utilizando las siguientes líneas de código, como se presenta a continuación:

- Descarga el código fuente de Python 2.7 “sudo apt update”
- Descarga el código fuente de Python 2.7: “sudo apt install wget build-essential libreadline-dev libncursesw5-dev libssl-dev libsqlite3-dev tk-dev libgdbm-dev libc6-dev libbz2-dev -y”
- Descarga el código fuente de Python 2.7 “tar -xf Python-2.7.18.tar.xz”
- Navega al directorio del código fuente de Python 2.7: “cd Python-2.7.18”
- Configura la compilación de python2.7: “ ./configure --enable-optimizations --prefix=/usr/local” (La opción --prefix=/usr/local asegura que Python se instalará en /usr/local. Esto es útil para evitar sobrescribir cualquier versión del sistema de Python 3.)
- Compila la herramienta python2.7: “make -j 8” (ajusta "8" al número de núcleos de tu CPU).
- Instala Python 2.7 en tu sistema: “sudo make altinstall”

```
root@debian:/home/hector/Python-2.7.18# sudo make altinstall
/usr/bin/install -c python /usr/local/bin/python2.7
if test -f libpython2.7.a; then \
        if test -n "" ; then \
                /usr/bin/install -c -m 555  /usr/local/bin; \
        else \
                /usr/bin/install -c -m 555 libpython2.7.a /usr/local/lib/libpython2.7.a
; \
                if test libpython2.7.a != libpython2.7.a; then \
                        (cd /usr/local/lib; ln -sf libpython2.7.a libpython2.7.a) \
                fi \
        fi; \
else    true; \
fi
running build
running build_ext
warning: openssl 0x00000000 is too old for _hashlib

Python build finished, but the necessary bits to build these modules were not found:
_bsddb             _hashlib           bsddb185
```

Figura 107 Instalación de complemento en Debian.

Fuente: Elaboración propia (2024).

- Verifica de nuevo ejecutando: python2.7 –versión

```
root@debian:/home/hector# python2.7
Python 2.7.18 (default, Feb  1 2024, 15:46:53)
```

Figura 108 Verificar versión de python 2.7 en Debian.

Fuente: Elaboración propia (2024).

Posteriormente se debe realizar la instalación de “curl”, como se muestra a continuación.

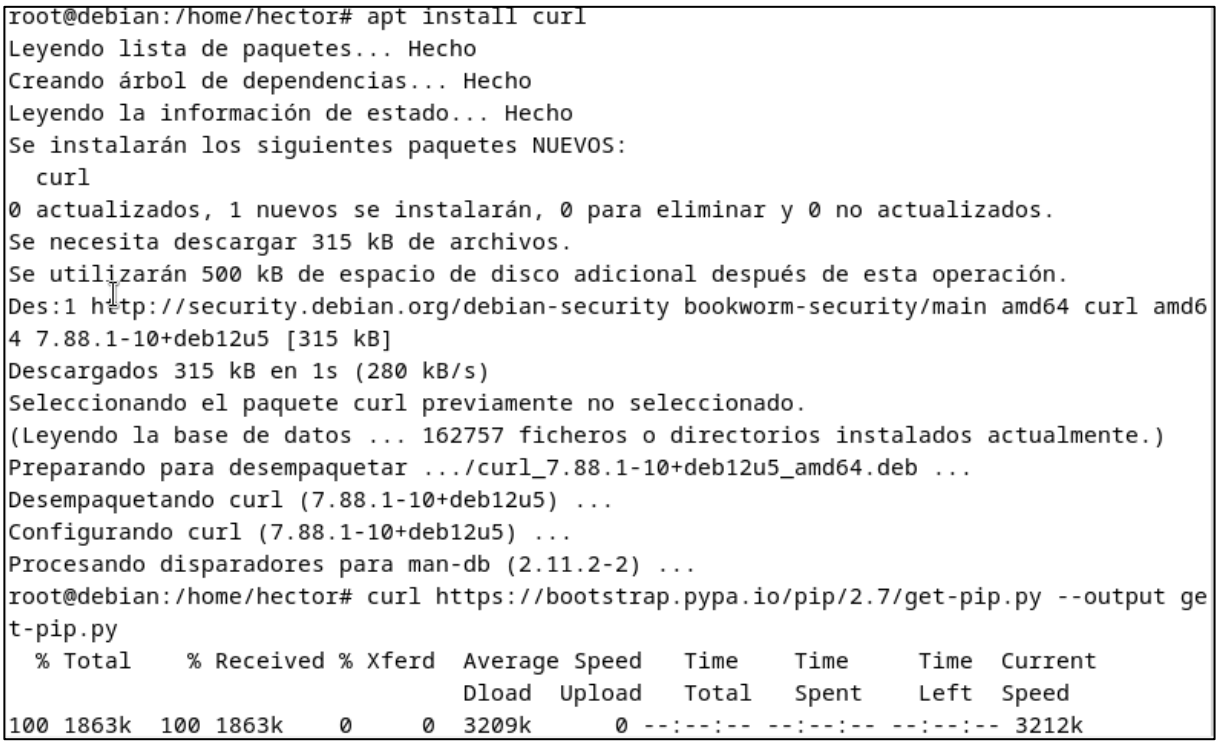


Figura 109 Instalación de Curl escenario 3.

Fuente: Elaboración propia (2024).

Continuando se debe realizar la instalación de “PIP”, ejecutando el comando “curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py” como se muestra a continuación.

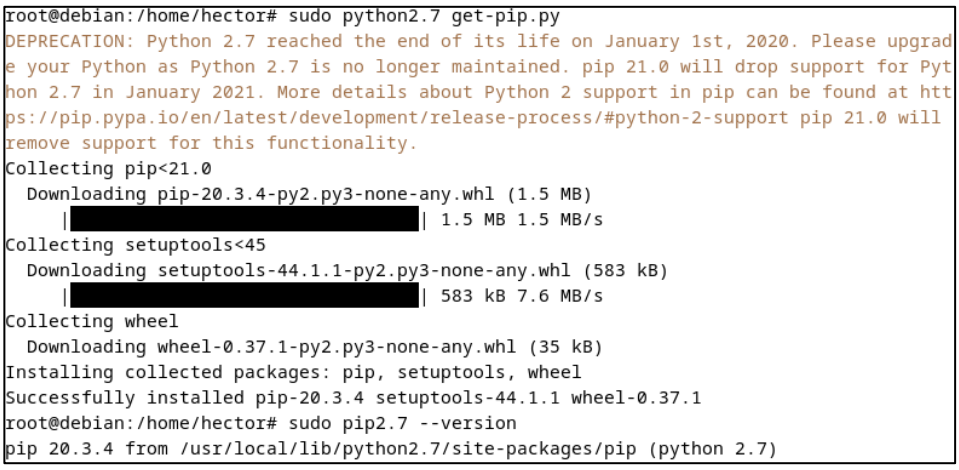


Figura 110 Instalación de PIP escenario 3.

Fuente: Elaboración propia (2024).

Seguidamente se debe realizar la instalación de “GIT”, como se muestra a continuación.

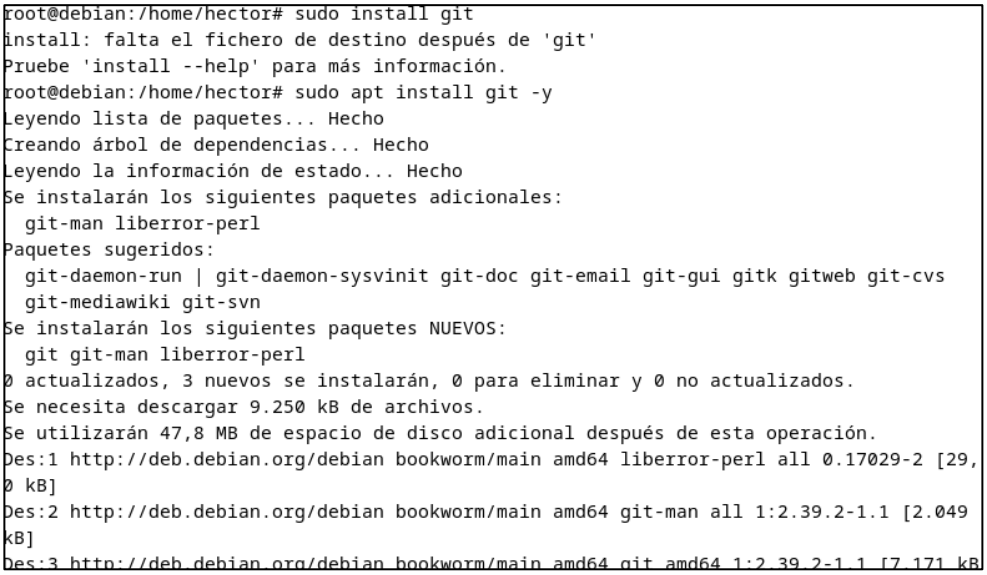


Figura 111 Instalación de GIT escenario 2.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “Distorm3”, como se muestra a continuación.

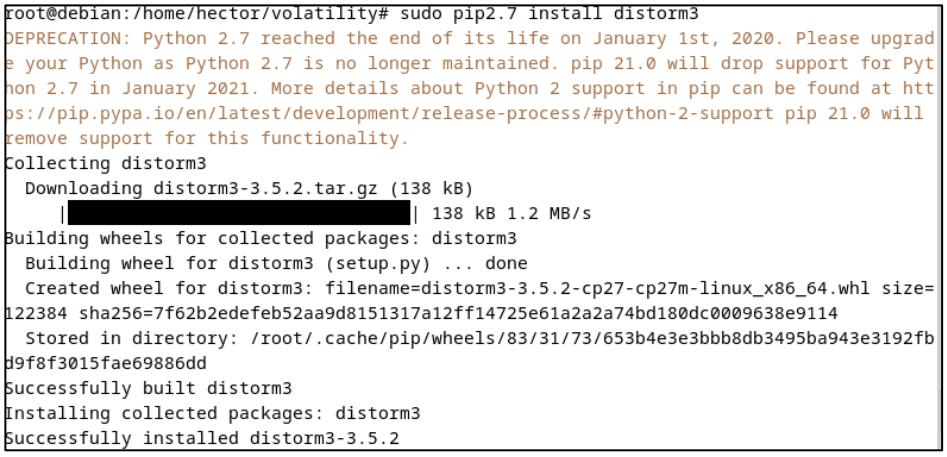


Figura 112 Instalación de dependencia distorm3 escenario 3.

Fuente: Elaboración propia (2024).

De igual manera, se debe realizar la instalación dependencia de PIP “yara-python”, como se muestra a continuación.

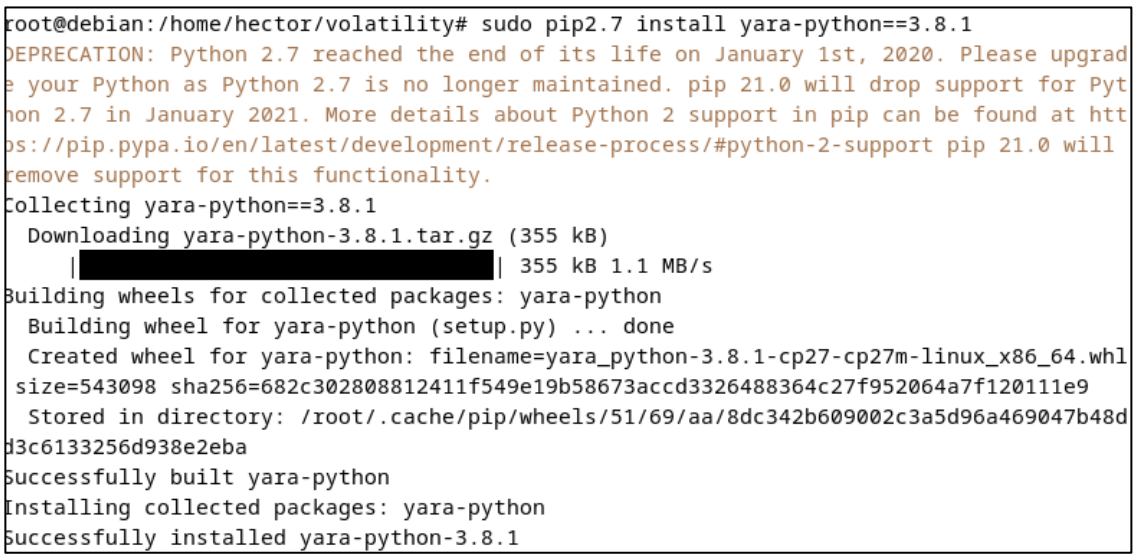


Figura 113 Instalación de dependencia yara-python escenario 3.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “Pycrypto”, como se muestra a continuación.

```
root@debian:/home/hector/volatility# sudo pip2.7 install pycrypto
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Collecting pycrypto
  Downloading pycrypto-2.6.1.tar.gz (446 kB)
     |[redacted]| 446 kB 1.1 MB/s
Building wheels for collected packages: pycrypto
  Building wheel for pycrypto (setup.py) ... done
  Created wheel for pycrypto: filename=pycrypto-2.6.1-cp27-cp27m-linux_x86_64.whl size=
490567 sha256=0ec06497c10443d3935e4874c312d26dc1a4071bcce85d6030a2a95ef66587b0
  Stored in directory: /root/.cache/pip/wheels/b6/e6/c8/d1eca13628952ceec1d40d96e0a7a13
80460d2349ce0b85312
Successfully built pycrypto
Installing collected packages: pycrypto
Successfully installed pycrypto-2.6.1
```

Figura 114 Instalación de dependencia pycrypto escenario 3.

Fuente: Elaboración propia (2024).

Así mismo, se debe realizar la instalación dependencia de PIP “pillow”, como se muestra a continuación.

```
root@debian:/home/hector/volatility# sudo pip2.7 install pillow
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Collecting pillow
  Downloading Pillow-6.2.2-cp27-cp27m-manylinux1_x86_64.whl (2.1 MB)
     |[redacted]| 2.1 MB 1.2 MB/s
Installing collected packages: pillow
Successfully installed pillow-6.2.2
```

Figura 115 Instalación de dependencia pillow escenario 3

Fuente: Elaboración propia (2024).

Posteriormente, se debe realizar la instalación dependencia de PIP “openpyxl==2.6.4”, como se muestra a continuación.

```
root@debian:/home/hector/volatility# sudo pip2.7 install openpyxl==2.6.4
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Requirement already satisfied: openpyxl==2.6.4 in /usr/local/lib/python2.7/site-package
s (2.6.4)
Requirement already satisfied: et-xmlfile in /usr/local/lib/python2.7/site-packages (fr
om openpyxl==2.6.4) (1.0.1)
Requirement already satisfied: jdcal in /usr/local/lib/python2.7/site-packages (from op
enpyxl==2.6.4) (1.4.1)
```

Figura 116 Instalación de dependencia openpyxl==2.6.4 escenario 3.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “ujson”, como se muestra a continuación.

```
root@debian:/home/hector/volatility# sudo pip2.7 install ujson
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Collecting ujson
  Downloading ujson-2.0.3-cp27-cp27m-manylinux1_x86_64.whl (172 kB)
     |████████████████████████████████| 172 kB 1.3 MB/s
Installing collected packages: ujson
Successfully installed ujson-2.0.3
```

Figura 117 Instalación de ujson escenario 3.

Fuente: Elaboración propia (2024).

Una vez instalados todos los complementos se realiza la verificación de la correcta instalación de estos ejecutando el comando “sudo pip2.7 list”, dando como resultado las 11 dependencias que se muestran a continuación.

```
root@debian:/home/hector/volatility# sudo pip2.7 list
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Package     Version
----------- -------
distorm3    3.5.2
et-xmlfile  1.0.1
jdcal       1.4.1
openpyxl    2.6.4
Pillow      6.2.2
pip         20.3.4
pycrypto    2.6.1
setuptools  44.1.1
ujson       2.0.3
wheel       0.37.1
yara-python 3.8.1
```

Figura 118 Verificación de instalación de dependencias escenario 3.

Fuente: Elaboración propia (2024).

7.3.1.4.3 Clonar repositorio de Volatility e instalación opcional.

Se debe verificar una ruta donde se quiera clonar el repositorio de Volatility, para este caso será “USER\home\”, ejecutando el comando “https://github.com/volatilityfoundation/volatility.git” como se muestra a continuación

.

```
hector@debian:~$ git clone https://github.com/volatilityfoundation/volatility.git
```

Figura 119 Clonación de repositorio Volatility Escenario 3.

Fuente: Elaboración propia (2024).

Por otra parte, la instalación opcional de Volatility, para este escenario 3 no se realizó.

7.3.1.4.4 Creación del perfil.

Una vez realizados los pasos anteriores se debe realizar la creación del perfil, para lo cual se accede a la carpeta de Volatility en donde se haya realizado la Clonación o instalación de este e ingresar a la siguiente ruta "…/volatility/tools/linux/", dentro de la cual se encuentran alojados los siguientes archivos "Makefile", "Makefile.enterprise", "module.c", y la carpeta "kcore", como se evidencia a continuación.

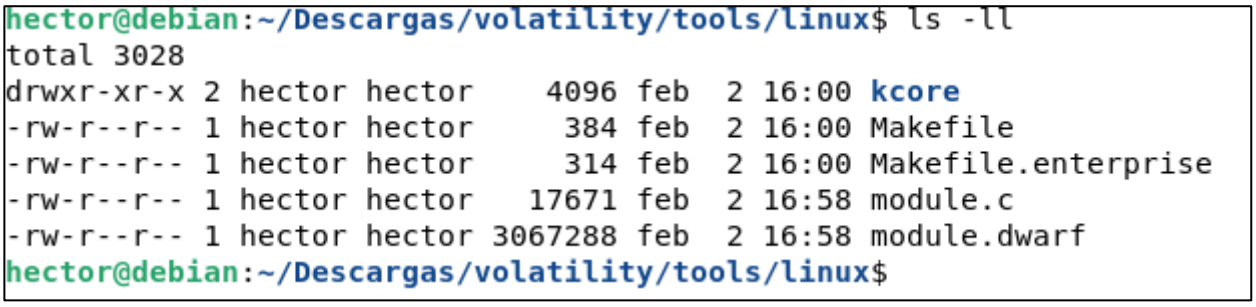


Figura 120 Contenido de la ruta "…/volatility/tools/linux/" escenario 3.

Fuente: Elaboración propia (2024).

En dicha ruta se encuentran los archivos necesarios para la generación del perfil, para lo cual se ejecuta el comando "make", en este caso se generó un error que indica "ERROR: modpost: missing MODULE_LICENSE ()", como se evidencia a continuación.

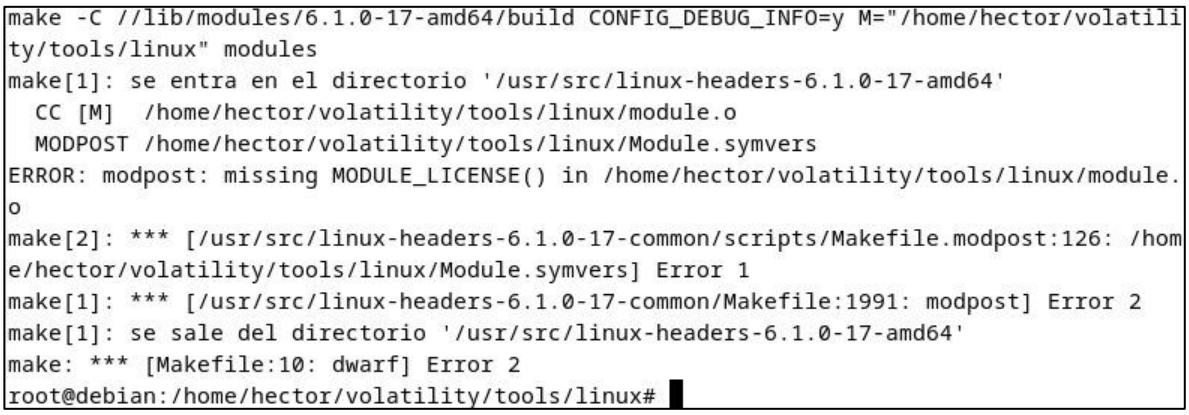


Figura 121 Error al ejecutar el comando MAKE escenario 3.

Fuente: Elaboración propia (2024).

Este error es común en la generación del perfil, para dar solución se debe realizar modificación del archivo “module.c”, agregando dos líneas con la misma sentencia como se evidencia a continuación (Para mayor detalle de la solución de este error ver la sección 6.4.4.2).

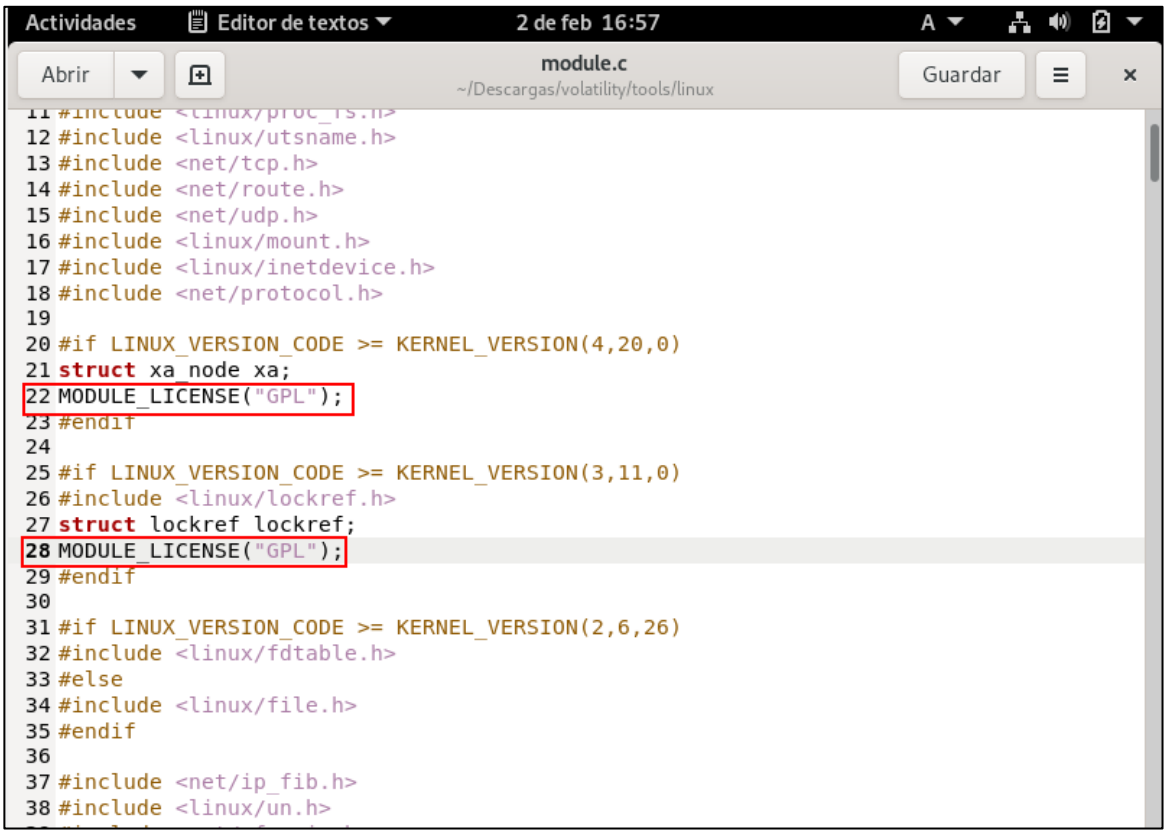


Figura 122 Solución de "ERROR: modpost: missing MODULE_LICENSE ()" escenario 3.

Fuente: Elaboración propia (2024).

Seguidamente, se vuelve a ejecutar el proceso, para lo cual se ejecuta el comando "make" observando lo siguiente:

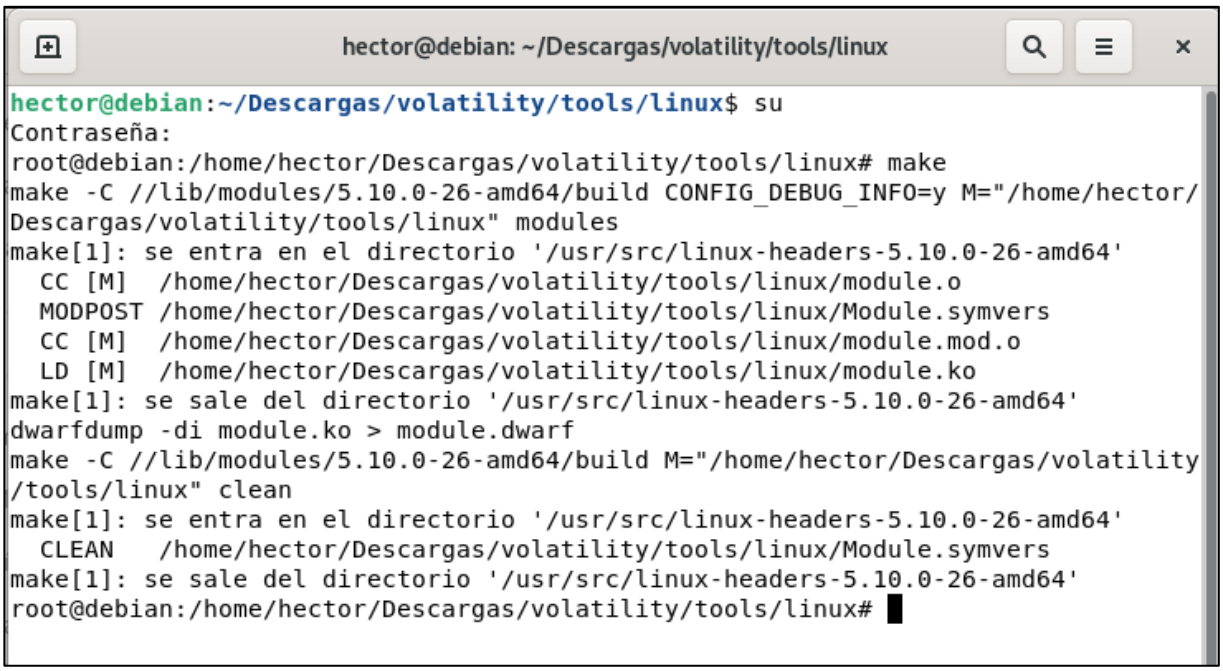


Figura 123 Generación exitosa de perfil escenario 3

Fuente: Elaboración propia (2024).

Continuando con el proceso se debe generar el zip que se nombrar con el nombre del Kernel, para obtener este nombre se debe ejecutar el comando “uname -a”, tal como se muestra a continuación.

```
root@debian:/home/hector/Descargas/volatility/tools/linux# uname -a
Linux debian 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64 GNU/Li
nux
root@debian:/home/hector/Descargas/volatility/tools/linux#
```

Figura 124 Nombre del kernel escenario 3

Fuente: Elaboración propia (2024).

Este zip debe contener el archivo “module.dwarf” resultado de la ejecución del comando “make” y la ruta “/boot/System.map…”, esta información es necesaria para que Volatility reconozca correctamente el perfil del sistema operativo, se debe tener en cuenta que el archivo zip resultante no quede vacío y que contenga las dos rutas

en cuestión para lo que es importante ejecutar el comando con permisos administrador.

```
root@debian:/home/hector# sudo zip Debian11.0.8P_5.10.0.27-generic.zip ./Descarg
as/volatility/tools/linux/module.dwarf /boot/System.map-5.10.0-26-amd64
  adding: Descargas/volatility/tools/linux/module.dwarf (deflated 91%)
  adding: boot/System.map-5.10.0-26-amd64 (deflated 16%)
```

Figura 125 archivo ZIP con los archivos del perfil del sistema operativo escenario 3

Fuente: Elaboración propia (2024).

El archivo zip resultando debe tener la estructura que se muestra a continuación.

```
root@debian:/home/hector# unzip -l  Debian11.0.8P_5.10.0.27-generic.zip
Archive:  Debian11.0.8P_5.10.0.27-generic.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
  3067288  2024-02-02 16:58   Descargas/volatility/tools/linux/module.dwarf
       83  2023-09-28 23:25   boot/System.map-5.10.0-26-amd64
---------                     -------
  3067371                     2 files
```

Figura 126 Estructura del contenido del archivo escenario 3.

Fuente: Elaboración propia (2024).

El archivo Zip resultante debe guardarse en la siguiente ruta “/volatility/volatility/plugins/overlays/Linux/”, una vez verificado que este almacenado allí se finalizaría con la creación del perfil del sistema operativo.

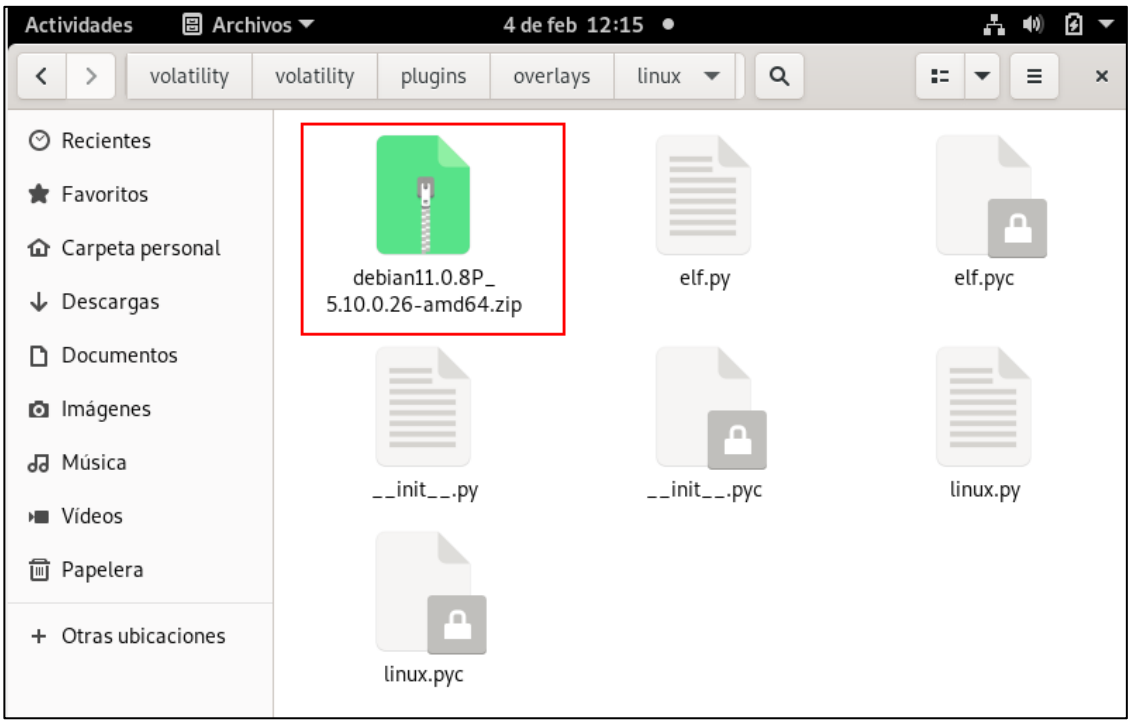


Figura 127 Mover perfil a la ruta especifica escenario 3.

Fuente: Elaboración propia (2024).

7.3.1.4.5 Verificación de perfil

Una vez finalizado los procedimientos anteriores, se debe ejecutar la herramienta volatility con el comando “vol.py –info | more”, para que liste todos los profiles que están disponibles, para este caso se debe verificar que el creado se encuentre en la lista corroborando que el proceso se realizó correctamente.

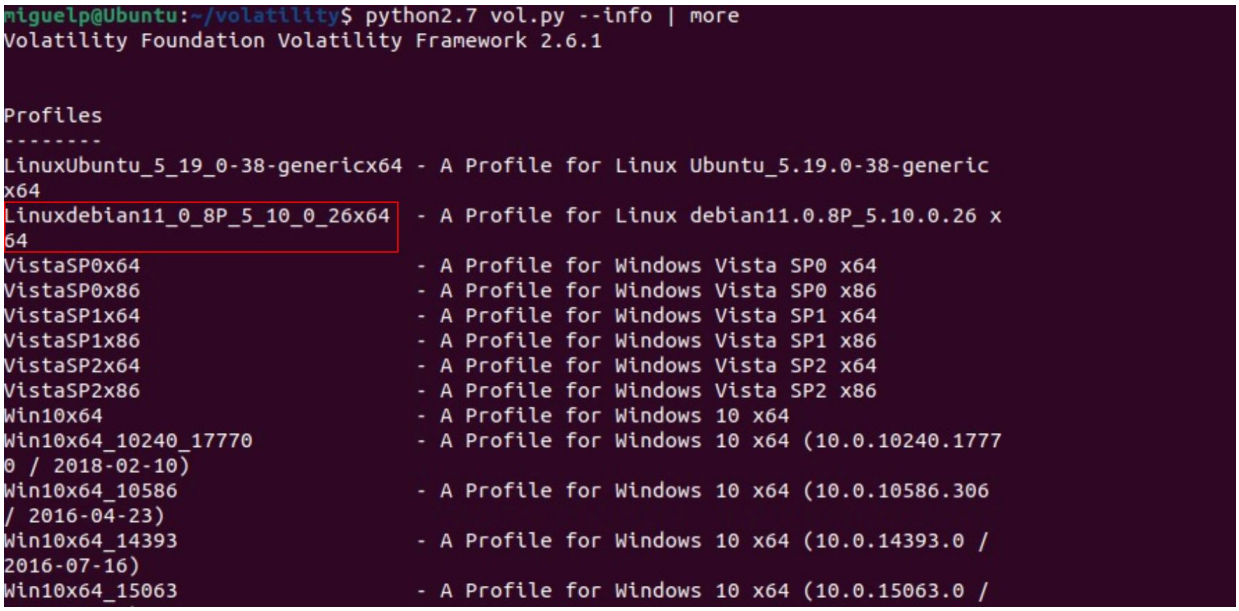


Figura 128 Verificación perfil escenario 3.

Fuente: Elaboración propia (2024).

Por otra parte, se pueden ejecutar algunos comandos relevantes para comprobar su funcionamiento, como los siguientes que serán ejecutados con el perfil obtenido únicamente a manera de ejemplo, teniendo como volcado de memoria RAM al mismo sistema al cual se le realizó el perfil antes mencionado:

- Comando linux_pslist: Lista los procesos en ejecución en el sistema operativo.

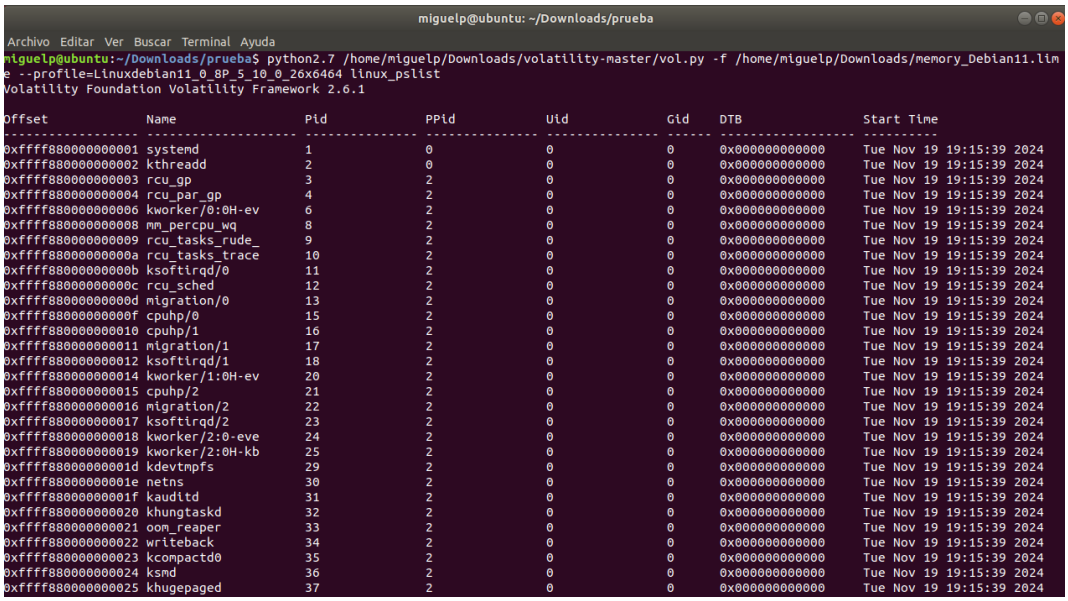


Figura 129 Resultado ejecución de comando linux_pslist escenario 3.

Fuente: Elaboración propia (2024).

- Comando linux_netstat: Detalla las conexiones de red activas y los puertos en escucha.

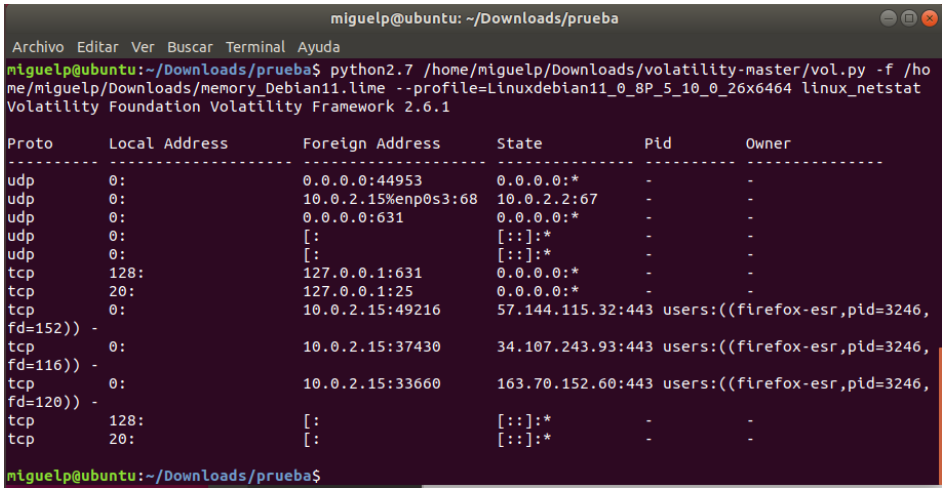


Figura 130 Ejecución de comando linux_netstat escenario 3.

Fuente: Elaboración propia (2024).

- Comando linux_sockets: Enumera los sockets TCP y UDP activos.

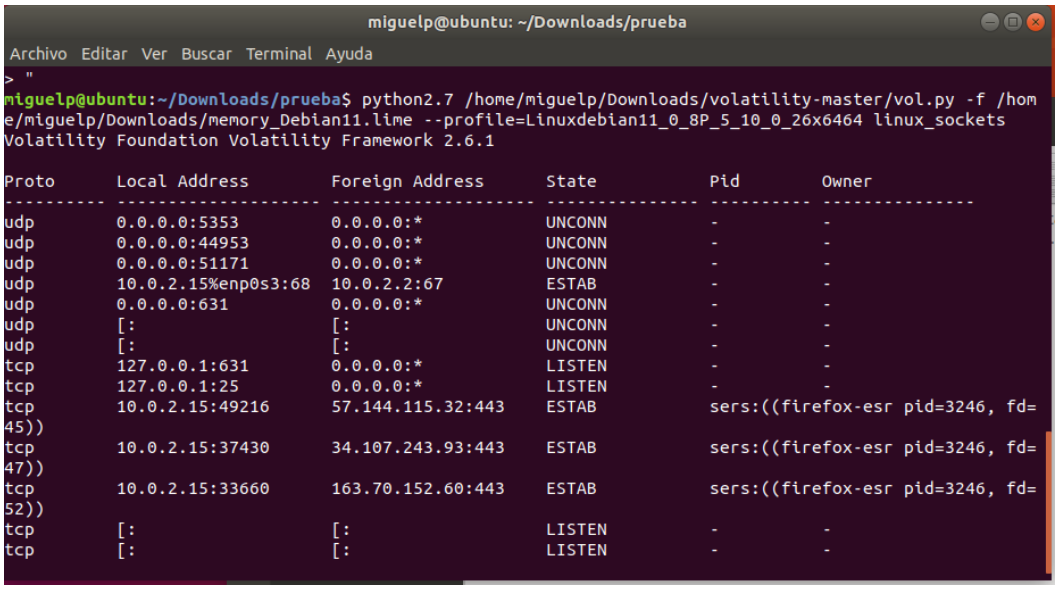


Figura 131 Ejecución de comnado Linux_sockets escenario 3.

Fuente: Elaboración propia (2024).

7.3.1.5 Escenario 4 Debian GNU/Linux 12.0.4 (bookworn):

7.3.1.5.1 Revisión de la existencia de un perfil para la versión exacta del sistema operativo

Como primer paso se debe revisar la versión exacta del sistema operativo, que para este caso se realizó ejecutando el comando “uname -a” y “lsb_release -a”, con lo cual se obtiene que la versión es un Debian GNU/Linux 12.0.4 (bookworn).

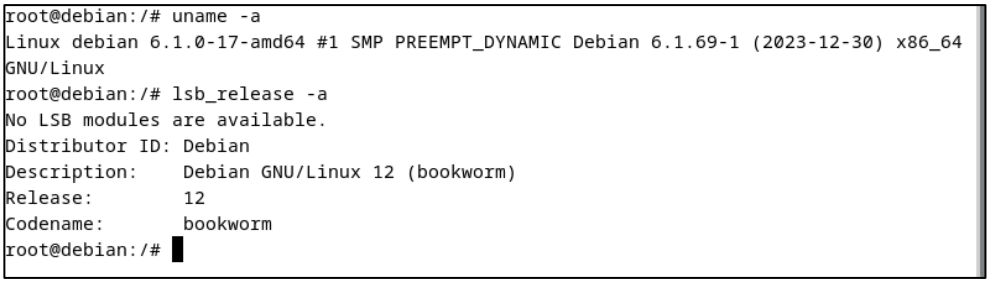
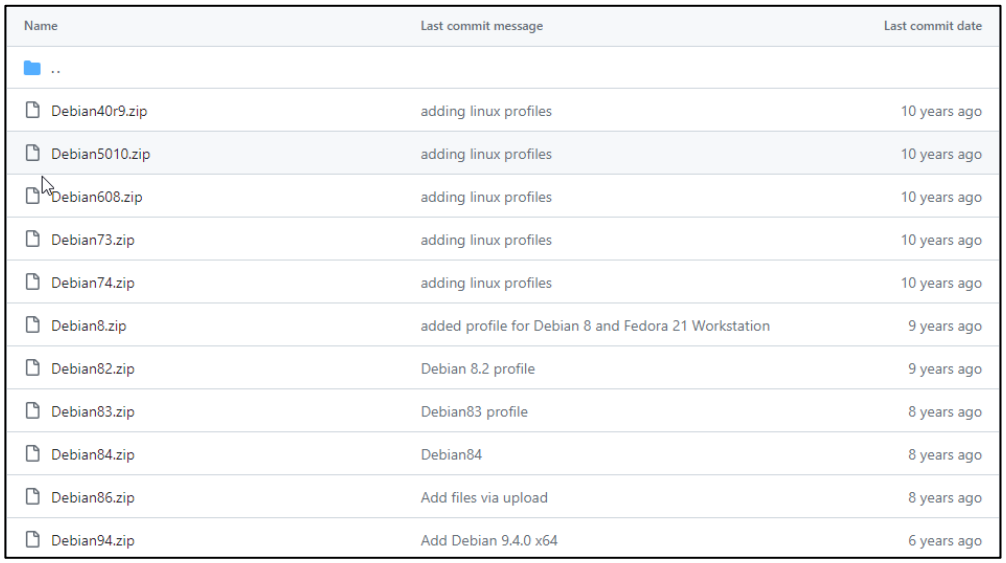


Figura 132 Información Debian 12.0.4 procedimiento 4.

Fuente: Elaboración propia (2024).

Seguidamente con la versión del sistema operativo se verificó en el repositorio de GitHub si ya existe un perfil creado para esa versión en especificó, identificando que para el caso en cuestión la versión del sistema operativo aún no cuenta con un perfil creado.



Name	Last commit message	Last commit date
..		
Debian40r9.zip	adding linux profiles	10 years ago
Debian5010.zip	adding linux profiles	10 years ago
Debian608.zip	adding linux profiles	10 years ago
Debian73.zip	adding linux profiles	10 years ago
Debian74.zip	adding linux profiles	10 years ago
Debian8.zip	added profile for Debian 8 and Fedora 21 Workstation	9 years ago
Debian82.zip	Debian 8.2 profile	9 years ago
Debian83.zip	Debian83 profile	8 years ago
Debian84.zip	Debian84	8 years ago
Debian86.zip	Add files via upload	8 years ago
Debian94.zip	Add Debian 9.4.0 x64	6 years ago

Figura 133 Versiones de perfiles disponibles para Debian.

Fuente: Elaboración propia (2024).

7.3.1.5.2 Instalar herramientas y dependencias.

Este representa el paso a paso sugerido para realizar la correcta instalación de todos los complementos necesarios para la instalación de Volatility, y asegurar la menor cantidad de errores por incompatibilidades, el cual consta de la instalación de:

Como primer paso la instalación de “build-essential”, para lo cual, se realizó la actualización de la biblioteca “apt update” y la posterior instalación “apt-get install build-essential”, como se muestra a continuación.

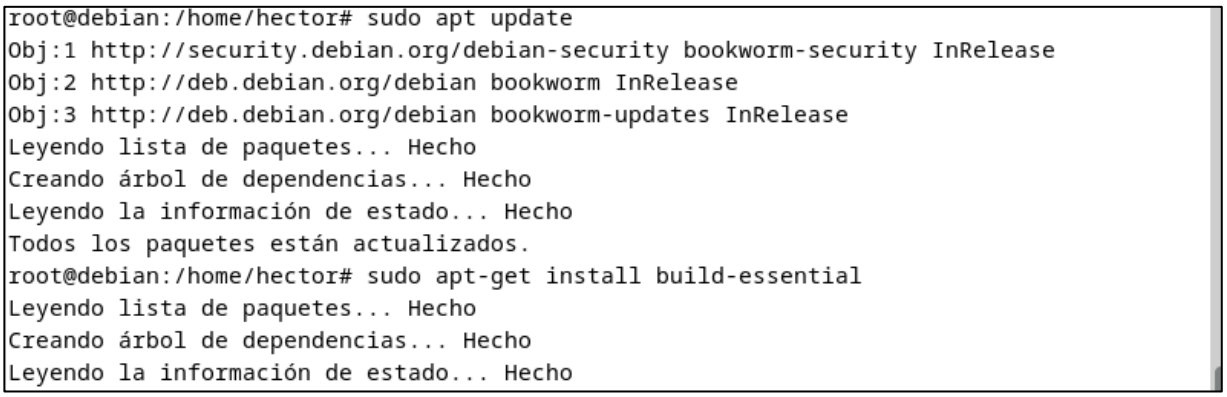


Figura 134 Verificación de paquete build-essential escenario 4.

Fuente: Elaboración propia (2024).

Seguidamente se realiza la instalación de Python2.7, indispensable para el funcionamiento de Volatility utilizando las siguientes líneas de código, como se muestra a continuación:

- Descarga el código fuente de Python 2.7 “sudo apt update”
- Descarga el código fuente de Python 2.7: “sudo apt install wget build-essential libreadline-dev libncursesw5-dev libssl-dev libsqlite3-dev tk-dev libgdbm-dev libc6-dev libbz2-dev -y”
- Descarga el código fuente de Python 2.7 “tar -xf Python-2.7.18.tar.xz”
- Navega al directorio del código fuente de Python 2.7: “cd Python-2.7.18”
- Configura la compilación de python2.7: “ ./configure --enable-optimizations --prefix=/usr/local” (La opción --prefix=/usr/local asegura que Python se instalará en /usr/local. Esto es útil para evitar sobrescribir cualquier versión del sistema de Python 3.)
- Compila la herramienta python2.7: “make -j 8” (ajusta "8" al número de núcleos de tu CPU).
- Instala Python 2.7 en tu sistema: “sudo make altinstall”

```
root@debian:/home/hector/Python-2.7.18# sudo make altinstall
/usr/bin/install -c python /usr/local/bin/python2.7
if test -f libpython2.7.a; then \
        if test -n "" ; then \
                /usr/bin/install -c -m 555  /usr/local/bin; \
        else \
                /usr/bin/install -c -m 555 libpython2.7.a /usr/local/lib/libpython2.7.a
; \
                if test libpython2.7.a != libpython2.7.a; then \
                        (cd /usr/local/lib; ln -sf libpython2.7.a libpython2.7.a) \
                fi \
        fi; \
else    true; \
fi
running build
running build_ext
warning: openssl 0x00000000 is too old for _hashlib

Python build finished, but the necessary bits to build these modules were not found:
_bsddb             _hashlib           bsddb185
```

Figura 135 Instalar altinstall Debian 2

Fuente: Elaboración propia (2024).

- Verifica de nuevo ejecutando: python2.7 –versión

```
root@debian:/home/hector# python2.7
Python 2.7.18 (default, Feb  1 2024, 15:46:53)
```

Figura 136 107 Verificación de python2.7

Fuente: Elaboración propia (2024).

Posteriormente se debe realizar la instalación de “curl”, como se muestra a continuación.

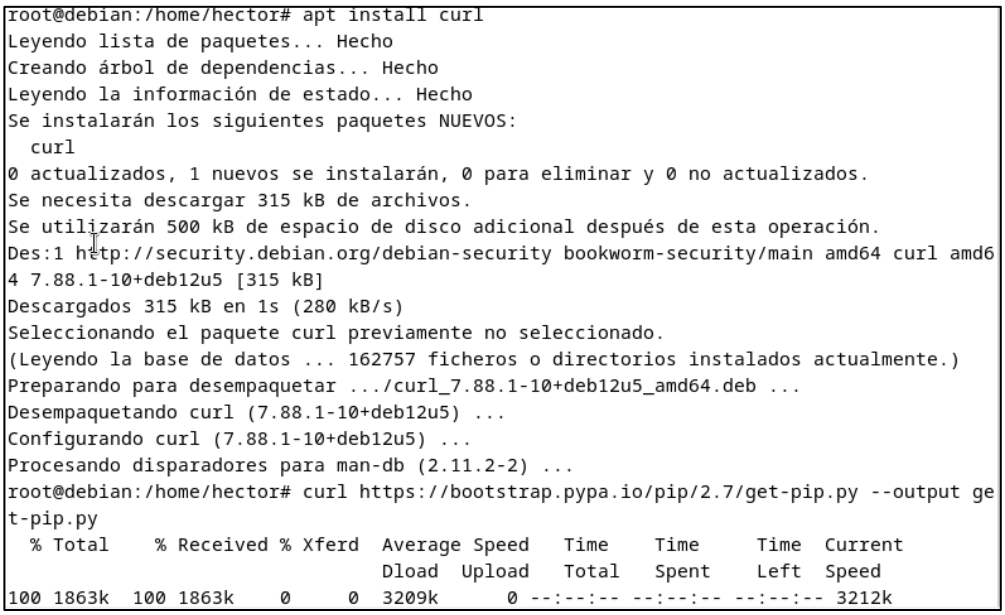


Figura 137 Instalación de Curl escenario 4.

Fuente: Elaboración propia (2024).

Continuando se debe realizar la instalación de “PIP”, ejecutando el comando “curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py” como se muestra a continuación.

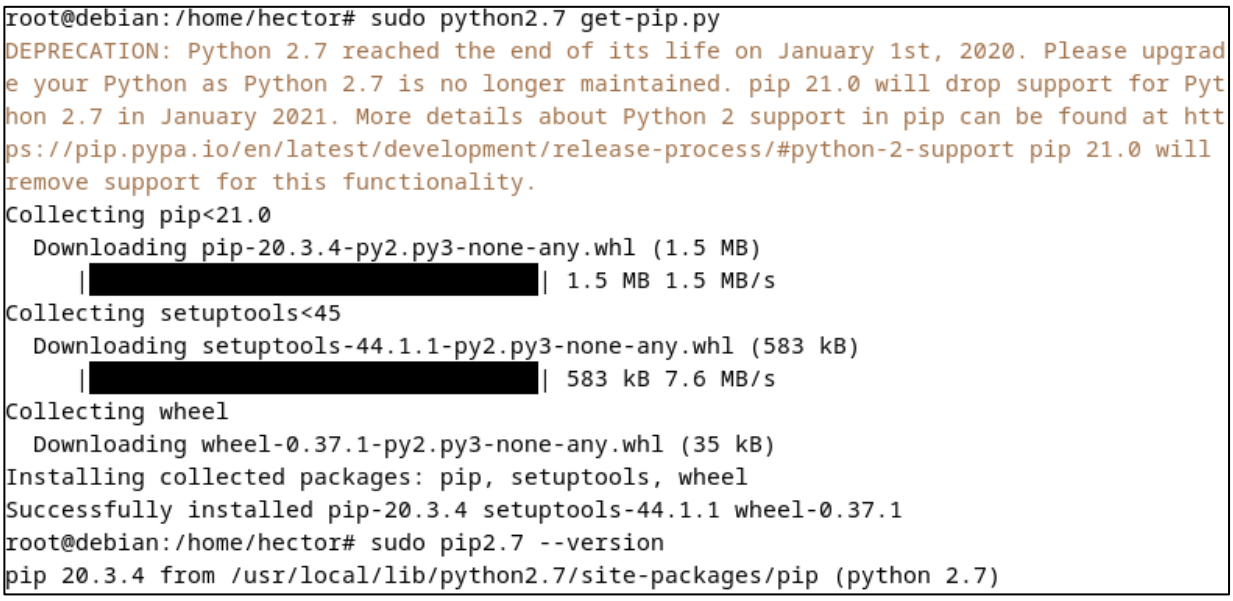


Figura 138 Instalación de PIP escenario 4.

Fuente: Elaboración propia (2024).

Seguidamente se debe realizar la instalación de “GIT”, como se muestra a continuación.

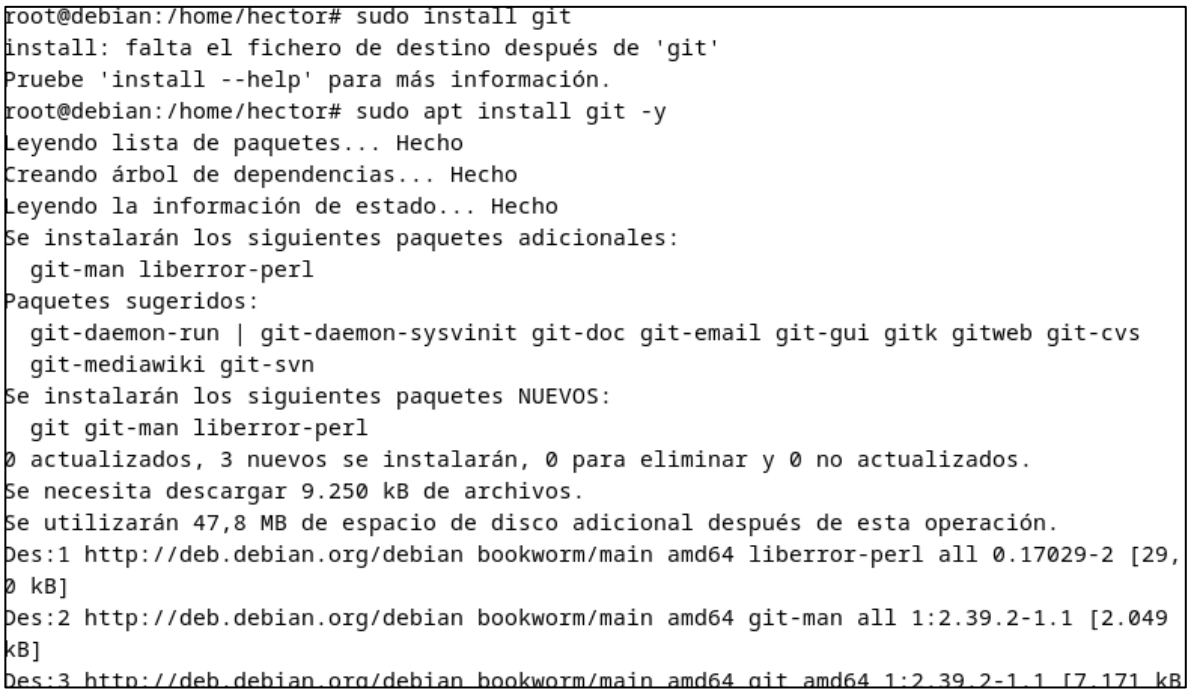


Figura 139 Instalación de GIT escenario 4.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “Distorm3”, como se muestra a continuación.

```
root@debian:/home/hector/volatility# sudo pip2.7 install distorm3
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Collecting distorm3
  Downloading distorm3-3.5.2.tar.gz (138 kB)
     |████████████████████████████████| 138 kB 1.2 MB/s
Building wheels for collected packages: distorm3
  Building wheel for distorm3 (setup.py) ... done
  Created wheel for distorm3: filename=distorm3-3.5.2-cp27-cp27m-linux_x86_64.whl size=
122384 sha256=7f62b2edefeb52aa9d8151317a12ff14725e61a2a2a74bd180dc0009638e9114
  Stored in directory: /root/.cache/pip/wheels/83/31/73/653b4e3e3bbb8db3495ba943e3192fb
d9f8f3015fae69886dd
Successfully built distorm3
Installing collected packages: distorm3
Successfully installed distorm3-3.5.2
```

Figura 140 Instalación de dependencia distorm3 escenario 4.

Fuente: Elaboración propia (2024).

De igual manera, se debe realizar la instalación dependencia de PIP “yara-python”, como se muestra a continuación.

```
root@debian:/home/hector/volatility# sudo pip2.7 install yara-python==3.8.1
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Collecting yara-python==3.8.1
  Downloading yara-python-3.8.1.tar.gz (355 kB)
     |████████████████████████████████| 355 kB 1.1 MB/s
Building wheels for collected packages: yara-python
  Building wheel for yara-python (setup.py) ... done
  Created wheel for yara-python: filename=yara_python-3.8.1-cp27-cp27m-linux_x86_64.whl
 size=543098 sha256=682c302808812411f549e19b58673accd3326488364c27f952064a7f120111e9
  Stored in directory: /root/.cache/pip/wheels/51/69/aa/8dc342b609002c3a5d96a469047b48d
d3c6133256d938e2eba
Successfully built yara-python
Installing collected packages: yara-python
Successfully installed yara-python-3.8.1
```

Figura 141 Instalación de dependencia yara-python escenario 4.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “Pycrypto”, como se muestra a continuación.

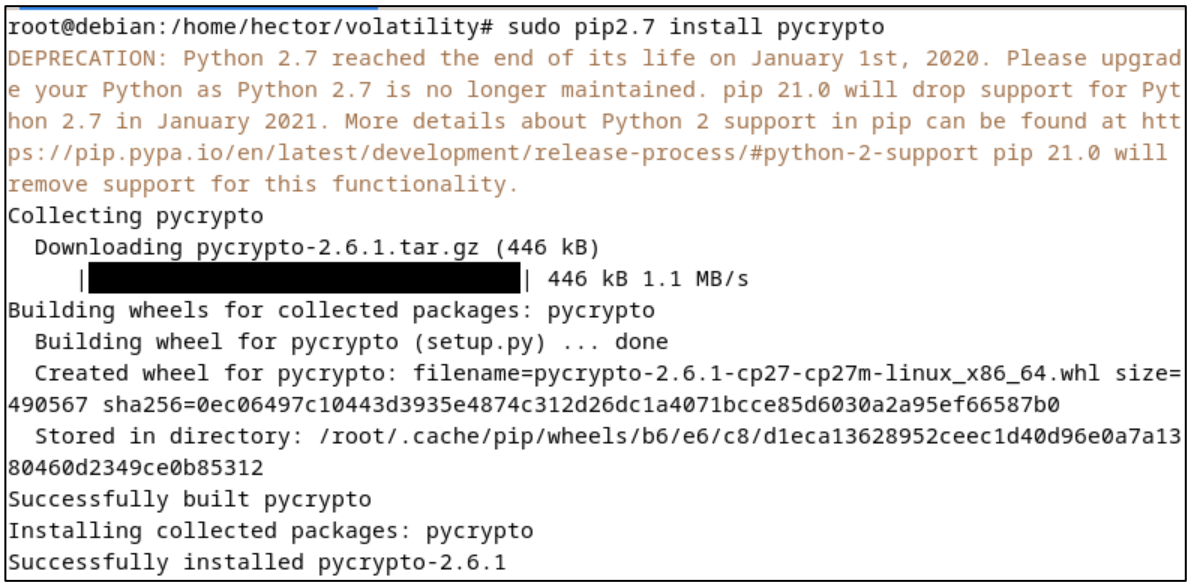


Figura 142 Instalación de dependencia pycrypto escenario 4.

Fuente: Elaboración propia (2024).

Así mismo, se debe realizar la instalación dependencia de PIP “pillow”, como se muestra a continuación.

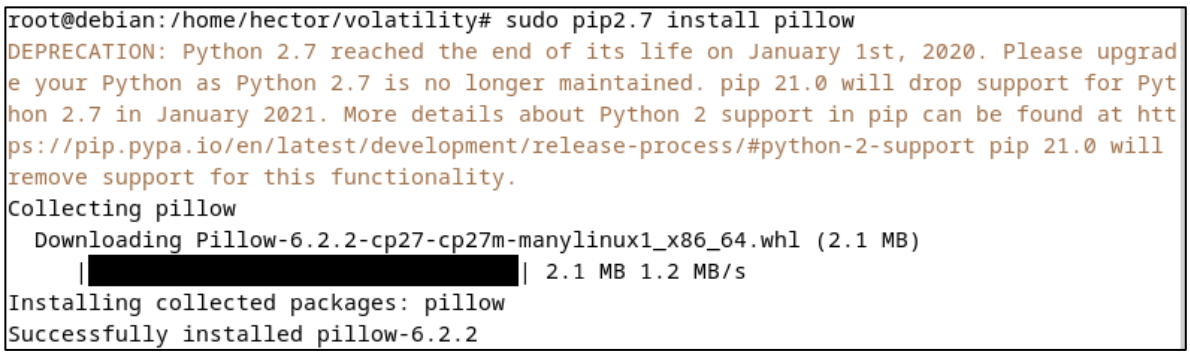


Figura 143 Instalación de dependencia pillow escenario 4.

Fuente: Elaboración propia (2024).

Posteriormente, se debe realizar la instalación dependencia de PIP “openpyxl==2.6.4”, como se muestra a continuación.

```
root@debian:/home/hector/volatility# sudo pip2.7 install openpyxl==2.6.4
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Requirement already satisfied: openpyxl==2.6.4 in /usr/local/lib/python2.7/site-package
s (2.6.4)
Requirement already satisfied: et-xmlfile in /usr/local/lib/python2.7/site-packages (fr
om openpyxl==2.6.4) (1.0.1)
Requirement already satisfied: jdcal in /usr/local/lib/python2.7/site-packages (from op
enpyxl==2.6.4) (1.4.1)
```

Figura 144 Instalación de dependencia openpyxl==2.6.4 escenario 4.

Fuente: Elaboración propia (2024).

Luego se debe realizar la instalación dependencia de PIP “ujson”, como se muestra a continuación.

```
root@debian:/home/hector/volatility# sudo pip2.7 install ujson
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Collecting ujson
  Downloading ujson-2.0.3-cp27-cp27m-manylinux1_x86_64.whl (172 kB)
     |                                | 172 kB 1.3 MB/s
Installing collected packages: ujson
Successfully installed ujson-2.0.3
```

Figura 145 Instalación de ujson escenario 4.

Fuente: Elaboración propia (2024).

Una vez instalados todos los complementos se realiza la verificación de la correcta instalación de estos ejecutando el comando “sudo pip2.7 list”, dando como resultado las 11 dependencias que se muestran a continuación.

```
root@debian:/home/hector/volatility# sudo pip2.7 list
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrad
e your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Pyt
hon 2.7 in January 2021. More details about Python 2 support in pip can be found at htt
ps://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Package     Version
----------- -------
distorm3    3.5.2
et-xmlfile  1.0.1
jdcal       1.4.1
openpyxl    2.6.4
Pillow      6.2.2
pip         20.3.4
pycrypto    2.6.1
setuptools  44.1.1
ujson       2.0.3
wheel       0.37.1
yara-python 3.8.1
```

Figura 146 Verificación de instalación de dependencias escenario 4.

Fuente: Elaboración propia (2024).

7.3.1.5.3 Clonar repositorio de Volatility e instalación opcional

Se debe verificar una ruta donde se quiera clonar el repositorio de Volatility, para este caso será “USER\home\”, ejecutando el comando “https://github.com/volatilityfoundation/volatility.git” como se muestra a continuación.

```
hector@debian:~$ git clone https://github.com/volatilityfoundation/volatility.git
```

Figura 147 Clonación de repositorio Volatility Escenario 4

Fuente: Elaboración propia (2024).

Por otra parte, la instalación opcional de Volatility, para este escenario 3 no se realizó.

7.3.1.5.4 Creación del perfil

Una vez realizados los pasos anteriores se debe realizar la creación del perfil, para lo cual se accede a la carpeta de Volatility en donde se haya realizado la Clonación o instalación de este e ingresar a la siguiente ruta "…/volatility/tools/linux/", donde se encuentran los siguientes archivos "Makefile", "Makefile.enterprise", "module.c", y la carpeta "kcore", como se evidencia a continuación.

```
hector@debian:~/volatility/tools/linux$ ls -l
total 468
drwxr-xr-x 2 root root   4096 feb  1 16:10 kcore
-rw-r--r-- 1 root root    384 feb  1 16:10 Makefile
-rw-r--r-- 1 root root    314 feb  1 16:10 Makefile.enterprise
-rw-r--r-- 1 root root  17625 feb  1 16:10 module.c
```

Figura 148 Contenido de la ruta "…/volatility/tools/linux/" escenario 4.

Fuente: Elaboración propia (2024).

En dicha ruta se encuentran los archivos necesarios para la generación del perfil, para lo cual se ejecuta el comando "make", para este caso se generó un error que indica "ERROR: modpost: missing MODULE_LICENSE ()", como se evidencia a continuación.

```
make -C //lib/modules/6.1.0-17-amd64/build CONFIG_DEBUG_INFO=y M="/home/hector/volatili
ty/tools/linux" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-6.1.0-17-amd64'
  CC [M]  /home/hector/volatility/tools/linux/module.o
  MODPOST /home/hector/volatility/tools/linux/Module.symvers
ERROR: modpost: missing MODULE_LICENSE() in /home/hector/volatility/tools/linux/module.
o
make[2]: *** [/usr/src/linux-headers-6.1.0-17-common/scripts/Makefile.modpost:126: /hom
e/hector/volatility/tools/linux/Module.symvers] Error 1
make[1]: *** [/usr/src/linux-headers-6.1.0-17-common/Makefile:1991: modpost] Error 2
make[1]: se sale del directorio '/usr/src/linux-headers-6.1.0-17-amd64'
make: *** [Makefile:10: dwarf] Error 2
root@debian:/home/hector/volatility/tools/linux#
```

Figura 149 Error al ejecutar el comando MAKE escenario 4.

Fuente: Elaboración propia (2024).

Este error es común en la generación del perfil, para dar solución se debe realizar modificación del archivo “module.c”, agregando dos líneas con la misma sentencia como se evidencia a continuación (Para mayor detalle de la solución de este error ver la sección 6.4.4.2).

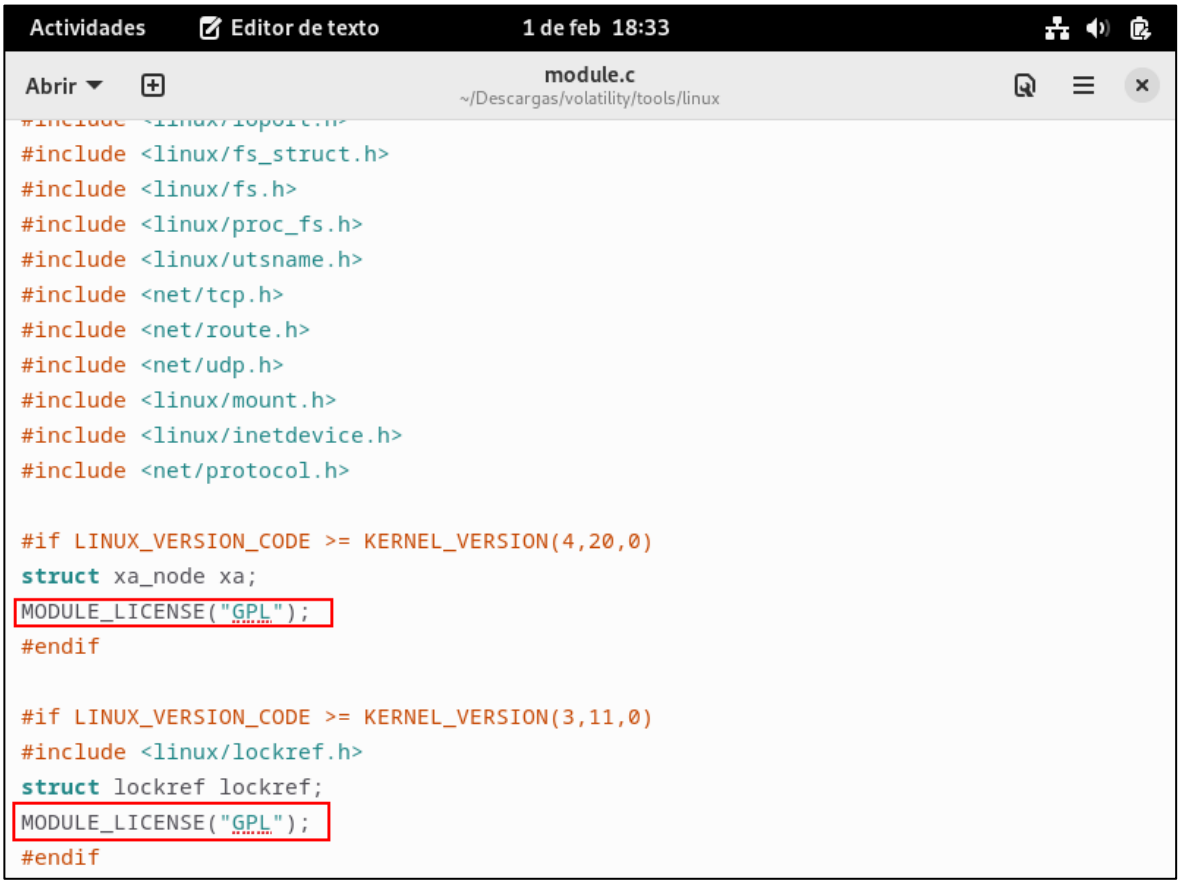


Figura 150 Solución de “ERROR: modpost: missing MODULE_LICENSE()” escenario 4.

Fuente: Elaboración propia (2024).

Seguidamente, se vuelve a ejecutar el proceso, para lo cual se ejecuta el comando “make”.

```
hector@debian:~/Descargas/volatility/tools/linux$ make
make -C //lib/modules/6.1.0-17-amd64/build CONFIG_DEBUG_INFO=y M="/home/hector/Descarga
s/volatility/tools/linux" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-6.1.0-17-amd64'
  CC [M]  /home/hector/Descargas/volatility/tools/linux/module.o
  MODPOST /home/hector/Descargas/volatility/tools/linux/Module.symvers
  CC [M]  /home/hector/Descargas/volatility/tools/linux/module.mod.o
  LD [M]  /home/hector/Descargas/volatility/tools/linux/module.ko
  BTF [M] /home/hector/Descargas/volatility/tools/linux/module.ko
Skipping BTF generation for /home/hector/Descargas/volatility/tools/linux/module.ko due
 to unavailability of vmlinux
make[1]: se sale del directorio '/usr/src/linux-headers-6.1.0-17-amd64'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/6.1.0-17-amd64/build M="/home/hector/Descargas/volatility/tools/l
inux" clean
make[1]: se entra en el directorio '/usr/src/linux-headers-6.1.0-17-amd64'
  CLEAN   /home/hector/Descargas/volatility/tools/linux/Module.symvers
make[1]: se sale del directorio '/usr/src/linux-headers-6.1.0-17-amd64'
hector@debian:~/Descargas/volatility/tools/linux$
```

Figura 151 Generación exitosa de perfil escenario 4.

Fuente: Elaboración propia (2024).

Continuando con el proceso se debe generar el zip que se nombrar con el nombre del Kernel, para obtener este nombre se debe ejecutar el comando “uname -a”, tal como se muestra a continuación.

```
hector@debian:~/Descargas/volatility/tools/linux$ uname -a
Linux debian 6.1.0-17-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.69-1 (2023-12-30) x86_64
GNU/Linux
```

Figura 152 Nombre del kernel escenario 4.

Fuente: Elaboración propia (2024).

Este zip debe contener el archivo “module.dwarf” resultado de la ejecución del comando “make” y la ruta “/boot/System.map…”, esta información es necesaria para que Volatility reconozca correctamente el perfil del sistema operativo, se debe tener en cuenta que el archivo zip resultante no quede vacío y que contenga las dos rutas

en cuestión para lo que es importante ejecutar el comando con permisos administrador.

```
root@debian:/home/hector# sudo zip Debian12P_6.1.0-17-generic.zip ./Descargas/volatilit
y/tools/linux/module.dwarf /boot/System.map-6.1.0-1-generic
        zip warning: name not matched: /boot/System.map-6.1.0-1-generic
  adding: Descargas/volatility/tools/linux/module.dwarf (deflated 91%)
```

Figura 153 Archivo ZIP con los archivos del perfil del sistema operativo escenario 4.

Fuente: Elaboración propia (2024).

El archivo zip resultando debe tener la estructura que se muestra a continuación.

```
root@debian:/home/hector# unzip -l Debian12P_6.1.0-17-generic.zip
Archive:  Debian12P_6.1.0-17-generic.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
  2961394  2024-02-01 16:37   Descargas/volatility/tools/linux/module.dwarf
       83  2023-12-30 04:31   boot/System.map-6.1.0-17-amd64
---------                     -------
  2961477                     2 files
```

Figura 154 Estructura del contenido del archivo escenario 4.

Fuente: Elaboración propia (2024).

El archivo Zip resultante debe guardarse en la siguiente ruta “Descargas/volatility/volatility/plugins/overlays/Linux/”, una vez verificado que este almacenado allí se finalizaría con la creación del perfil del sistema operativo.

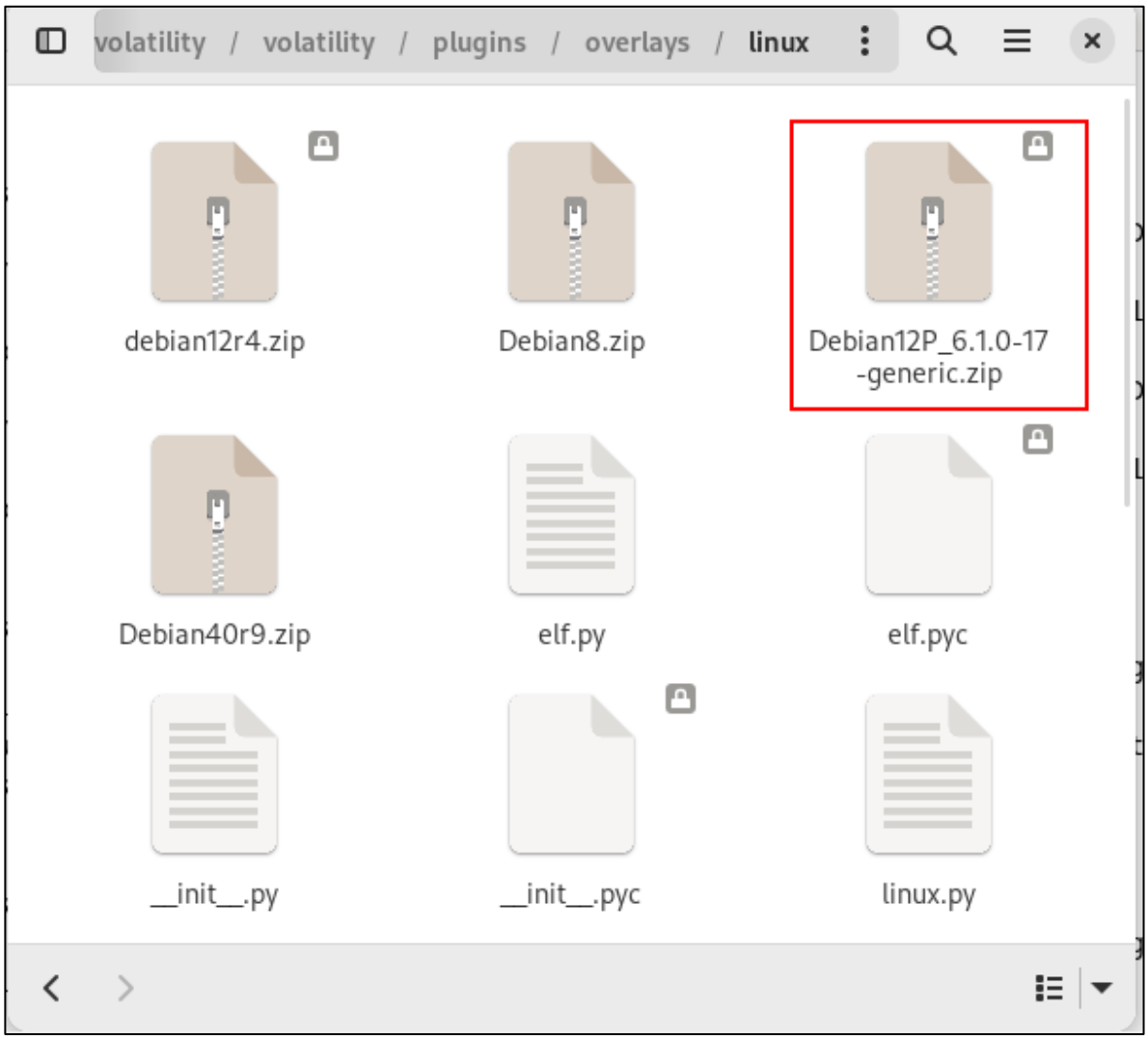


Figura 155 Mover perfil a la ruta especifica escenario 4.

Fuente: Elaboración propia (2024).

7.3.1.5.5 Verificación de perfil.

Una vez finalizado los procedimientos anteriores, se debe ejecutar la herramienta volatility con el comando “vol.py –info | more”, para que liste todos los profiles que están disponibles, para este caso se debe verificar que el creado se encuentre en la lista corroborando que el proceso se realizó correctamente.

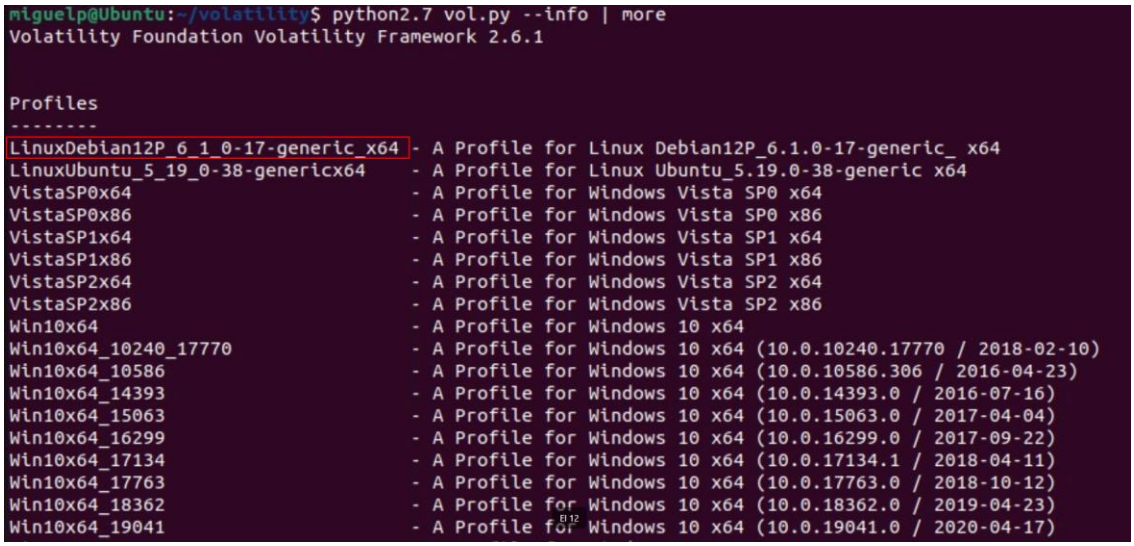


Figura 156 Verificación perfil escenario 4.

Fuente: Elaboración propia (2024).

Por otra parte, se pueden ejecutar algunos comandos relevantes para comprobar su funcionamiento, como los siguientes que serán ejecutados con el perfil obtenido únicamente a manera de ejemplo, teniendo como volcado de memoria RAM al mismo sistema al cual se le realizó el perfil antes mencionado:

- Comando linux_pslist: Lista los procesos en ejecución en el sistema operativo.

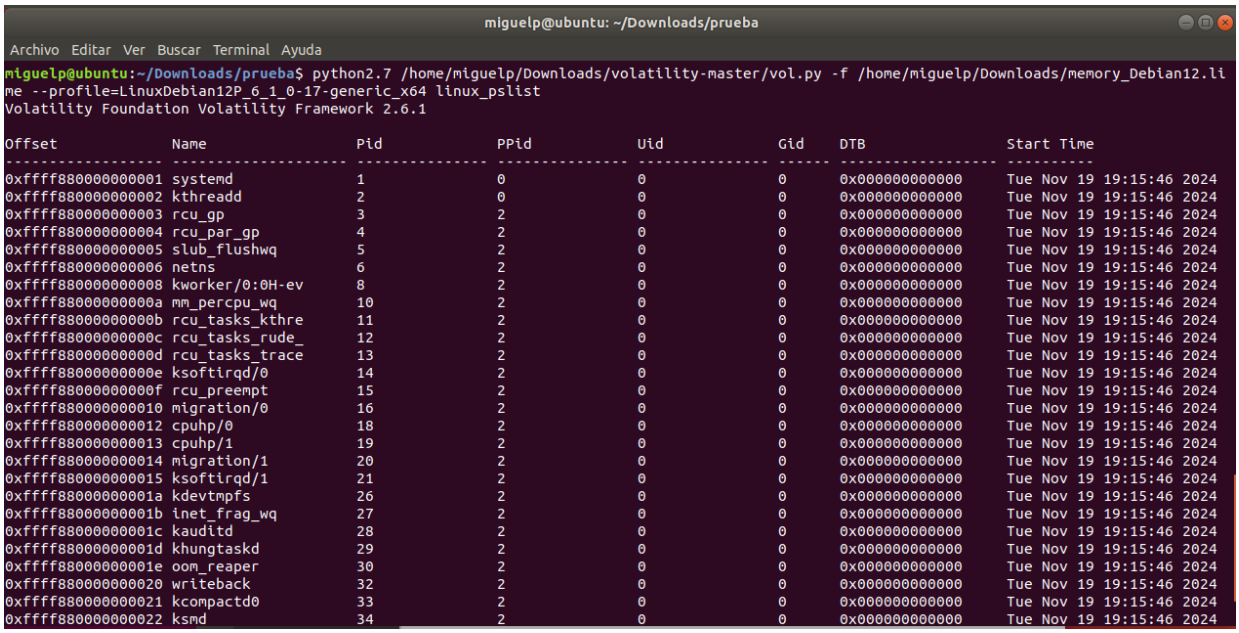


Figura 157 Resultado ejecución de comando linux_pslist escenario 4.

Fuente: Elaboración propia (2024).

- Comando linux_lsof: Muestra los archivos abiertos por los procesos en el sistema.

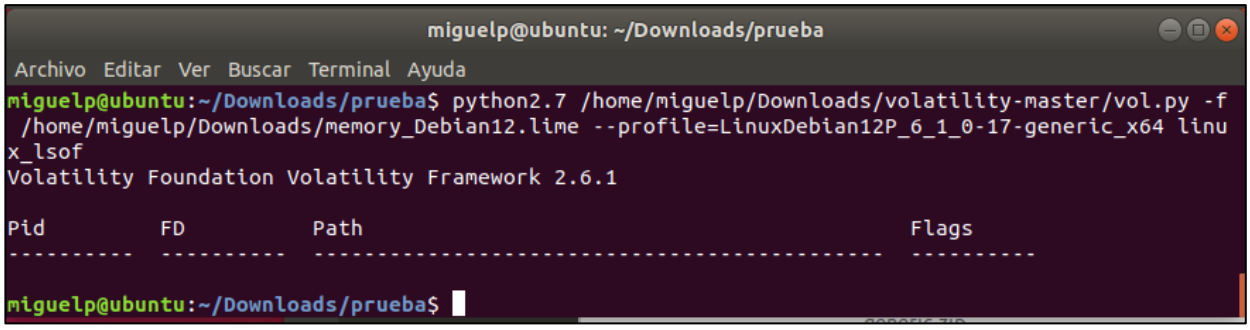


Figura 158 Ejecución Comando linux_lsof escenario 4

Fuente: Elaboración propia (2024).

- Comando linux_netstat: Detalla las conexiones de red activas y los puertos en escucha.

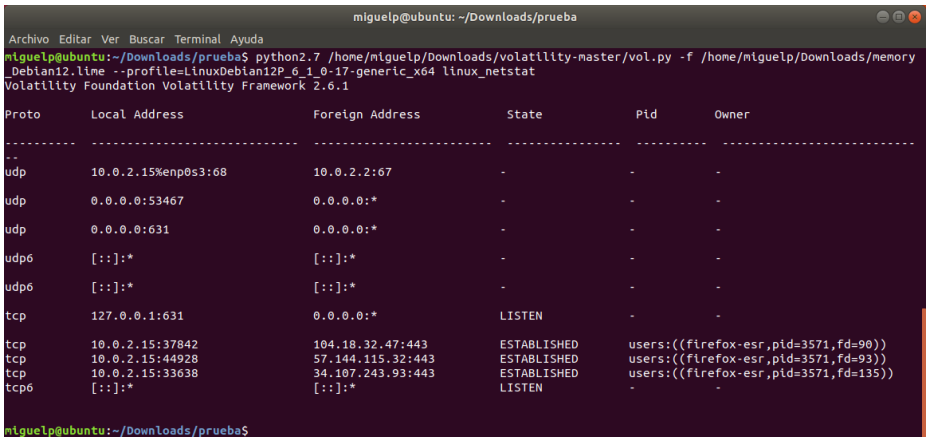


Figura 159 Ejecución de comando linux_netstat escenario 4.

Fuente: Elaboración propia (2024).

- Comando linux_sockets: Enumera los sockets TCP y UDP activos.

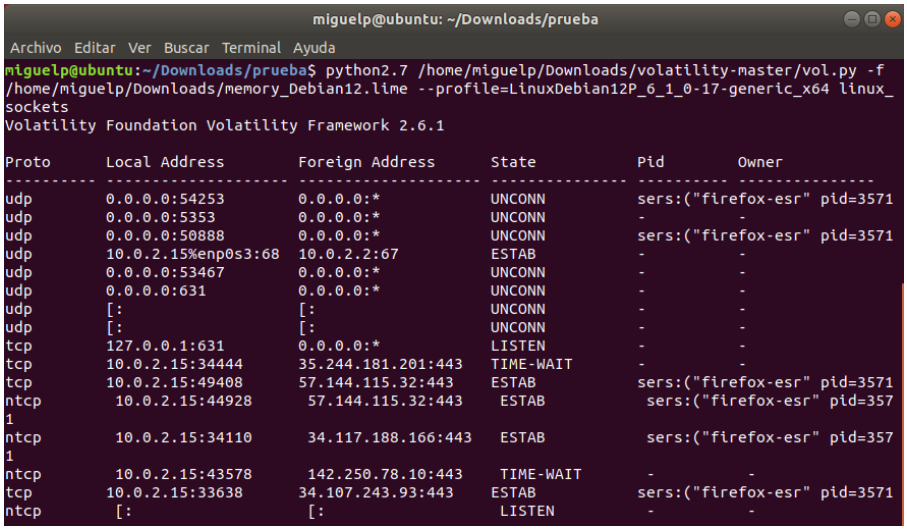


Figura 160 Ejecución de comando Linux_sockets escenario 4.

Fuente: Elaboración propia (2024).

Para superar estas limitaciones de la creación del perfil con las guías oficiales, se ha desarrollado un procedimiento optimizado que aborda las deficiencias encontradas en el procedimiento oficial, este procedimiento se basa en guías oficiales, foros, recomendaciones de diversas fuentes y autores, en busca de

minimizar la posibilidad de errores durante la creación del perfil en Volatility 2.6, sin embargo, se debe tener claro que es necesario adaptar el procedimiento a otras distribuciones de Linux diferentes a Ubuntu y Debian, puesto que algunos comandos o funcionalidades no están disponibles o funcionan de manera diferente, teniendo claro que lo que funciona para una distribución puede no ser aplicable directamente a otra.

El procedimiento optimizado está diseñado y ajustado específicamente para la distribución Ubuntu y Debian, abarcando desde la instalación de Volatility hasta la creación y validación del perfil, resaltando pasos clave, como la instalación de herramientas y dependencias necesarias, la clonación del repositorio de Volatility y la resolución de errores comunes durante la creación del perfil.

En conclusión, con las pruebas realizadas en los cuatro escenarios con sistemas operativos Ubuntu y Debian a el procedimiento ajustado, se validó la efectividad al facilitar la creación de perfiles y reducir los errores generados en Volatility 2.6, puesto que el procedimiento abarca desde la instalación de Volatility hasta la creación del perfil, lo que permite ser utilizado en investigaciones forenses o de respuesta a incidentes, lo que permitirá que no se pierda tanto tiempo realizando búsquedas y reprocesos que pueda generar la solución de errores, optimizando procesos y haciendo más efectiva la investigación en cuestión, de igual manera, si bien el procedimiento optimizado se elaboró para minimizar la complejidad, se reconoce que la adaptación a otras distribuciones de Linux puede ser necesaria, y finalmente la validación exitosa del perfil en Volatility después de seguir este procedimiento refuerza su utilidad y eficacia.

7.3.2 Solucionar errores comunes Linux

En esta sección de documentaron los errores más comunes presentados en la generación del perfil basado en experiencia realizando este procedimiento.

7.3.2.1 Solución error de Kernel

En el momento de la generación del perfil, si se identifica un mensaje de error relacionado con la configuración invalidad de kernel, tal y como se evidencia el mensaje de error a continuación:

> “ERROR: Kernel configuration is invalid.
>
> include/generated/autoconf.h or include/config/auto.conf are missing.
>
> Run 'make oldconfig && make prepare' on kernel src to fix it.”

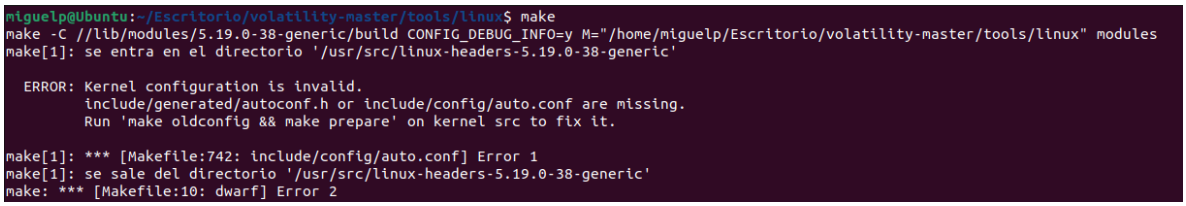


Figura 161 Imagen de referencia mensaje de error de Kernel.

Fuente: Elaboración propia (2024).

Para solucionar el error se debe realizar la reinstalación del header y el Kernel, para que estos sean reconstruidos ejecutando los siguientes comandos:

- sudo apt install --reinstall linux-headers-$(uname -r)
- sudo cp /usr/src/linux-headers-X.X.X-XX-generic/include/generated/autoconf.h /usr/src/linux-headers-X.X.X-XX-generic/include/generated/ (NOTA: Se debe verificar la versión del header correspondiente al sistema operativo en cuestión y reemplazar las XX)
- sudo apt install --reinstall build-essential
- sudo apt install --reinstall dkms
- sudo apt install --reinstall linux-generic
- sudo apt install --reinstall linux-signed-generic
- sudo apt-get install build-essential
- sudo apt-get install dwarfdump
- sudo apt autoremove

Para más información ver el foro https://askubuntu.com/questions/890712/kernel-configuration-is-invalid-error-while-trying-to-install-paragon-ufsd-profe.

7.3.2.2 Solución error de licencia perdida ERROR: modpost: missing MODULE_LICENSE ()

En el momento de la generación del perfil, si se identifica un mensaje de error relacionado con la configuración invalidad de la licencia “missing MODULE_LICENSE ()”, tal y como se evidencia el mensaje de error a continuación:

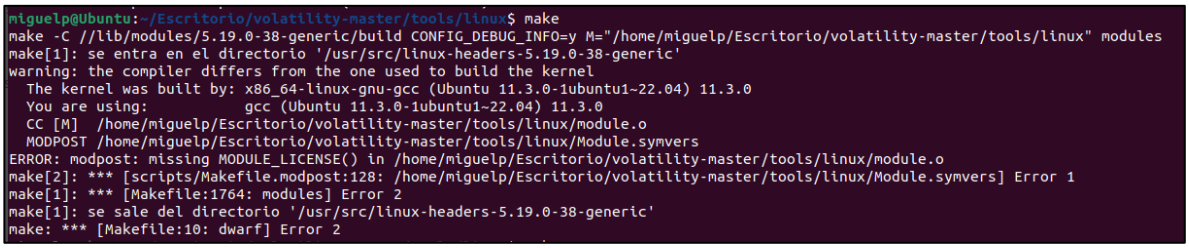


Figura 162 Imagen de referencia error de licencia perdida “ERROR: modpost: missing MODULE_LICENSE ()”.

Fuente: Elaboración propia (2024).

Para solucionar el error se debe modificar el “module.c” y agregar la línea “MODULE_LICENSE("GPL");”, como se muestra a continuación:

```
1 /*
2   This module does absolutely nothings at all. We just build it with debugging
3 symbols and then read the DWARF symbols from it.
4 */
5 #include <linux/module.h>
6 #include <linux/version.h>
7
8 #include <linux/ioport.h>
9 #include <linux/fs_struct.h>
10 #include <linux/fs.h>
11 #include <linux/proc_fs.h>
12 #include <linux/utsname.h>
13 #include <net/tcp.h>
14 #include <net/route.h>
15 #include <net/udp.h>
16 #include <linux/mount.h>
17 #include <linux/inetdevice.h>
18 #include <net/protocol.h>
19
20 #if LINUX_VERSION_CODE >= KERNEL_VERSION(4,20,0)
21 struct xa_node xa;
22 MODULE_LICENSE("GPL");
23 #endif
24
25 #if LINUX_VERSION_CODE >= KERNEL_VERSION(3,11,0)
26 #include <linux/lockref.h>
27 struct lockref lockref;
28 MODULE_LICENSE("GPL");
29 #endif
30
31 #if LINUX_VERSION_CODE >= KERNEL_VERSION(2,6,26)
32 #include <linux/fdtable.h>
33 #else
34 #include <linux/file.h>
35 #endif
36
37 #include <net/ip_fib.h>
38 #include <linux/un.h>
39 #include <net/af_unix.h>
40 #include <linux/pid.h>
41
42 #if LINUX_VERSION_CODE >= KERNEL_VERSION(2,6,20)
43 #include <linux/pid_namespace.h>
44 struct pid_namespace pid_namespace;
45 #endif
46
```

Figura 163 Agregar línea de licencia en el código fuente de module.c

Fuente: Elaboración propia (2024).

Para más información ver el foro https://stackoverflow.com/questions/56662176/linux-kernel-driver-modpost-missing-module-license.

7.3.2.3 Solución error de falta de compilador gcc-12

En el momento de la generación del perfil, si se identifica un mensaje de error relacionado con la configuración invalidad de la licencia “gcc-12: not found”, tal y como se evidencia el mensaje de error a continuación:

```
miguelp@Ubuntu2:~/volatility/tools/linux$ make
make -C //lib/modules/6.5.0-15-generic/build CONFIG_DEBUG_INFO=y M="/home/miguelp/volatility/tools/linux" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-6.5.0-15-generic'
warning: the compiler differs from the one used to build the kernel
  The kernel was built by: x86_64-linux-gnu-gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0
  You are using:
  CC [M]  /home/miguelp/volatility/tools/linux/module.o
/bin/sh: 1: gcc-12: not found
make[3]: *** [scripts/Makefile.build:251: /home/miguelp/volatility/tools/linux/module.o] Error 127
make[2]: *** [/usr/src/linux-headers-6.5.0-15-generic/Makefile:2037: /home/miguelp/volatility/tools/linux] Error 2
make[1]: *** [Makefile:234: __sub-make] Error 2
make[1]: se sale del directorio '/usr/src/linux-headers-6.5.0-15-generic'
make: *** [Makefile:10: dwarf] Error 2
```

Figura 164 Imagen de referencia error de licencia perdida “ERROR: gcc-12: not found”.

Fuente: Elaboración propia (2024).

Para solucionar el error se debe realizar la instalación del compilador gcc-12 y su configuración ejecutando los siguientes comandos:

- sudo apt-get install gcc-12
- sudo update-alternatives –install /usr/bin/gcc gcc /usr/bin/gcc-12 100

```
miguelp@Ubuntu2:~/volatility/tools/linux$ make
make -C //lib/modules/6.5.0-15-generic/build CONFIG_DEBUG_INFO=y M="/home/miguelp/volatility/tools/linux" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-6.5.0-15-generic'
warning: the compiler differs from the one used to build the kernel
  The kernel was built by: x86_64-linux-gnu-gcc-12 (Ubuntu 12.3.0-1ubuntu1~22.04) 12.3.0
  You are using:
  CC [M]  /home/miguelp/volatility/tools/linux/module.o
/bin/sh: 1: gcc-12: not found
make[3]: *** [scripts/Makefile.build:251: /home/miguelp/volatility/tools/linux/module.o] Error 127
make[2]: *** [/usr/src/linux-headers-6.5.0-15-generic/Makefile:2037: /home/miguelp/volatility/tools/linux] Error 2
make[1]: *** [Makefile:234: __sub-make] Error 2
make[1]: se sale del directorio '/usr/src/linux-headers-6.5.0-15-generic'
make: *** [Makefile:10: dwarf] Error 2
```

Figura 165 Imagen de referencia solución de error de licencia perdida “ERROR: gcc-12: not found”.

Fuente: Elaboración propia (2024).

Realizado este proceso vuelva a ejecutar nuevamente el proceso de creación de perfil.

8 CONCLUSIONES

En resumen, en cuanto al panorama actual de los ciberataques relacionados al sistema operativo Linux basado en el análisis documental revela un preocupante aumento en los ciberataques dirigidos a sistemas operativos Linux, desafiando la percepción histórica de seguridad de esta plataforma, así como también se enfatiza en la diversificación de tácticas, desde Ransomware hasta ataques sin archivos, destacando la complejidad de las amenazas que enfrenta Linux, sumado a la elevada cantidad de vulnerabilidades documentadas, especialmente en Debian, se genera una necesidad de crear y mantener procesos eficaces para investigar incidentes en entornos Linux, esta realidad en cifras refuerza la importancia de implementar medidas preventivas sólidas y desarrollar capacidades de respuesta ágiles para investigaciones forenses o de respuesta a incidentes.

En cuanto al objetivo de establecer tipos de análisis de memoria volátil utilizando Volatility 2.6, la herramienta se destaca como una herramienta esencial en el campo del análisis forense y las investigaciones de respuesta a incidentes por su eficiencia en el manejo de volcados de memoria, proporcionando un análisis detallado de procesos, servicios, actividad de red y contenido de caché DNS, así como también la relevancia de entender los perfiles puesto que de estos depende que sea posible realizar el análisis detallado antes mencionado. De igual manera, es importante resaltar que un análisis inadecuado podría resultar en la pérdida de información crucial, fomentando la necesidad de entender perfiles, la estructura de la memoria y las relaciones entre elementos para identificar actividades sospechosas, procesos huérfanos típicos de un malware, entre otros, siendo que Volatility se consolida como esencial en investigaciones forenses y de respuesta a incidentes ya que le brinda al investigador las capacidades de análisis profundo y adaptabilidad, cruciales para las investigaciones de infecciones por malware, incidentes de ciberseguridad, investigaciones forenses, así como la capacidad de identificar

técnicas, tácticas, procedimientos o artefactos utilizados por el atacante u otras amenazas cibernéticas.

En relación con el tercer objetivo, se evidencia que el procedimiento oficial para la creación de perfiles en Volatility presupone ciertas instalaciones previas y puede generar dificultades en entornos reales, además, de requerir conocimientos avanzados para abordar posibles problemas, limitando su accesibilidad, puesto que este no incluye un paso a paso de cómo se debe realizar correctamente el procedimiento si no que, brinda una serie de consejos muy generales y requisitos que son indispensables para que el proceso se lleve a cabo, sin embargo no se tienen en cuenta las condiciones específicas de cada distribución de Linux, encontrando errores por falta de instalación de librerías, dependencias o complementos que utiliza Volatility pero que no se encuentran relacionadas directamente en la guía oficial, o errores propios del sistema operativo, por ejemplo los errores de configuración invalida de Kernel, o la falta de licencia “GPL” para poder compilar y crear el perfil del sistema operativo respectivo, por lo que requiere que el usuario tenga conocimientos medios o avanzados para poder ejecutar las acciones indicadas y dar solución a los problemas que surjan al momento de ejecutar el proceso descrito, por lo tanto no es un procedimiento enfocado a cualquier tipo de usuario.

Finalmente, en el cuarto objetivo aborda las limitaciones de la guía oficial mediante un procedimiento optimizado diseñado a partir de guías oficiales y recomendaciones diversas fuentes, experiencias personales y autores, en busca de minimizar la posibilidad de errores durante la creación del perfil en Volatility 2.6. Este procedimiento optimizado para el sistema operativo Linux consta ocho pasos para la respectiva creación del perfil, los cuales son:

1. Acceso al sistema operativo al cual se le va a realizar el procedimiento (No se documenta).
2. Creación de snapshot o instantáneas (No se documenta).

3. Revisión de la existencia de un perfil ya creado para la versión exacta del sistema operativo.
4. Instalar herramientas y dependencias
    a. build-essential
    b. Python2.6
    c. Curl
    d. GIT
    e. Flex
    f. bison
    g. PIP
        i. Distorm3
        ii. Yara-python
        iii. Pycrypto
        iv. Pillow
        v. Openpyxl==2.6.4
        vi. Ujson
5. Clonar github Volatility (Instalar opcional)
6. Creación del perfil
7. Validación del funcionamiento del perfil
8. Solucionar errores comunes Ubuntu
    a. Error de Kernel (Opcional solo si aparece)
    b. Error de licencia perdida “ERROR: modpost: missing MODULE_LICENSE()” (Opcional solo si aparece).

Se comprobó la efectiva de estos procedimientos optimizados mediante su aplicación en cuatro escenarios dos utilizando la distribución de Linux Ubuntu y los otros dos utilizando la distribución DEBIAN, abarcando desde la instalación de Volatility hasta la creación y validación del perfil, resaltando pasos clave, como la instalación de herramientas y dependencias necesarias, la clonación del repositorio de Volatility y la resolución de errores comunes durante la creación del perfil.

El resultando en los cuatro escenarios fue la validación exitosa del perfil en Volatility después de seguir el procedimiento optimizado, lo que refuerza su utilidad y eficacia, reduciendo errores y optimizando procesos en investigaciones forenses o de respuesta a incidentes, puesto que puede facilitar la creación de perfiles y mejorar la efectividad de las investigaciones, siendo que el procedimiento detalla específicamente el paso a paso, por lo que es accesible a casi cualquier tipo de usuario, sin embargo, se reconoce la necesidad de adaptar el procedimiento a otras distribuciones de Linux, puesto que algunos comandos o funcionalidades no están disponibles o funcionan de manera diferente, teniendo claro que lo que funciona para una distribución puede no ser aplicable directamente a otra.

En conclusión, los sistemas operativos Linux y sus diferentes distribuciones tienen un nicho de mercado que ha venido en constante crecimiento al ser de código abierto es versátil y ajustable a las diferentes necesidades del mercado y las organizaciones, lo que ha a su vez ha atraído especial atención de los ciber atacantes que desde el 2014 han intensificado su actividad criminal evidenciado en cómo han crecido las amenazas a estos sistemas operativos desde el 2014, por lo que es imperativo contar con herramientas que tengan una robustes suficiente para realizar investigaciones y que estas se hagan en el menor tiempo posible, siendo la memoria RAM de vital importancia en Ciberataques con complejidades mayores como por ejemplo ataques de tipo APT, por lo que Volatility es una herramienta crucial siendo una de las pocas con la robustes necesaria para realizar dichos análisis compatibles con casi todos los diferentes sistemas operativos diseñados, y siendo la efectividad de las búsquedas avanzadas lo que resulta relevante, sin embargo, para que esta herramienta despliegue toda su capacidad es necesaria la creación del respectivo perfil del sistema que se quiere investigar, por lo que si bien existe un procedimiento oficial para Linux este cubre lo ideal necesario para que la

herramienta funcione, pero en la práctica se generan diversos errores o fallas, puesto que los sistemas operativos basados en Linux inclusive en sus propias distribuciones son diferentes unas de las otras, por lo que si bien en este documento se incluyeron procedimientos optimizados estos tampoco garantizan que realizándolos de la manera indicada no se vayan a generar errores por la diversidad en cada versión de los sistemas operativos, siendo que este procedimientos optimizados están enfocados en simplificar el procedimiento de creación del perfil en las distribuciones de Linux “Ubuntu” y “Debian”, y a su vez disminuir la cantidad de errores que este proceso pueda generar.

9 BIBLIOGRAFÍA

Álvarez, S. Análisis forense de una infección por malware. [En línea]. Universidad de Barcelona , 2021. [Citado 24-Noviembre-2024]. Disponible en Internet https://diposit.ub.edu/dspace/bitstream/2445/182840/2/tfg_sergio_agru%c3%b1a_alvarez.pdf

Alamillo, J. PERITAJE INFORMÁTICO, ANÁLISIS FORENSE DIGITAL Y RESPUESTA A INCIDENTES. [En línea]. Universidad de Castilla, 2022. [Citado 24-Noviembre-2024]. Disponible en Internet https://revista.uclm.es/index.php/ruiderae/article/view/3087

Alberto, M. CIBERAMENAZAS AL ALZA: 411,000 ARCHIVOS MALICIOSOS CIRCULARON DIARIAMENTE EN 2023. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.estamosenlinea.com/2023/12/29/ciberamenazas-al-alza-411000-archivos-maliciosos-circularon-diariamente-en-2023/

Almagro, L. Ciberseguridad marco NIST, 2019. [En línea] OEA. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Ana Di Lorio, Gonzalo Angeli, Juan Alberdi, Hugo Curti, Fernando Greco, Ariel Podestá, Martin Castellote, Bruno Constanzo, Juan Iturriaga y Santiago Trigo. (2016). Análisis forense de memoria: malware y evidencia oculta. [En línea]. Universidad FASTA. [Citado 24-Noviembre-2024]. Disponible en Internet http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1547

Ana Di Lorio, Gonzalo Angeli, Juan Alberdi, Hugo Curti, Fernando Greco, Ariel Podestá, Martin Castellote, Bruno Constanzo, Juan Iturriaga y Santiago Trigo. Análisis forense de memoria: malware y evidencia oculta, 2016. [En línea].

Universidad FASTA. [Citado 24-Noviembre-2024]. Disponible en Internet http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1547

Arnedo, P. Herramientas de análisis forense y su aplicabilidad en investigación de delitos informáticos, 2014. [En línea] Universidad Internacional de la Rioja. [Citado 24-Noviembre-2024]. Disponible en Internet https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y

AsIAP. (s.f.). (2020). Los servidores y equipos Linux en el punto de mira de los ciberatacantes. [En línea]. AsIAP.org. [Página web]. Recuperado el 15 de enero de 2024. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.asiap.org/AsIAP/index.php/noticias-de-tecnologia/8525-los-servidores-y-equipos-linux-en-el-punto-de-mira-de-los-ciberatacantes

Barrios, L. (2023). Bogotá es la ciudad de Colombia donde más ciberdelitos se cometen: cuál es la razón. Infoabe. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.infobae.com/colombia/2023/06/22/bogota-es-la-ciudad-de-colombia-donde-mas-ciberdelitos-se-cometen-cual-es-la-razon/

Byte. (2021). La seguridad en Linux, en entredicho. Revista Byte TI. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://revistabyte.es/ciberseguridad/seguridad-en-linux/

Cantero, R. (2023). Un malware que robaba contraseñas en Linux ha funcionado durante 3 años y nadie se ha dado cuenta hasta ahora. [En línea]. UrbanTecno. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.mundodeportivo.com/urbantecno/linux/un-malware-que-robaba-contrasenas-en-linux-ha-funcionado-durante-3-anos-y-nadie-se-ha-dado-cuenta-hasta-ahora

Carbone, R., & Defence Research and Development Canada-Valcartier Research Centre Quebec, Quebec Canada. (2015). Malware Memory Analysis of the IVYL Linux Rootkit: Investigating a Publicly Available Linux Rootkit Using the Volatility

Memory Analysis Framework. [En línea]. Defence Research and Development Canada-Valcartier Research Centre Quebec, Quebec Canada. [Citado 24-Noviembre-2024]. Disponible en Internethttps://apps.dtic.mil/sti/citations/AD1004349

Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional. [En línea]. 1er edición.[Citado 24-Noviembre-2024]. Disponible en Internet https://repo.zenk-security.com/Forensic/File%20System%20Forensic%20Analysis.pdf

Casey, E. (2011). Handbook of Digital Forensics and Investigation. [En línea]. Academic Press. Sciencedirect. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.sciencedirect.com/book/9780123742674/handbook-of-digital-forensics-and-investigation

Castañeda, M. (2022). Panorama de Ciberataques Más Recurrentes en Colombia 2021 y 2022. [En línea]. Universidad Piloto de Colombia. [Citado 24-Noviembre-2024]. Disponible en Internet http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/12279/Art%C3%ADculo_IEEE_Coterminal.pdf?sequence=1&isAllowed=n

Castilla, J; Romero, J. (2018). Importancia de la recolección de datos volátiles dentro de una investigación forense. [En línea]. Universidad Piloto de Colombia. [Citado 24-Noviembre-2024]. Disponible en Internet http://repository.unipiloto.edu.co/handle/20.500.12277/3088?show=full

Cendales, M. A. (2023, 2 de noviembre). 'Ciberseguridad a la medida' para todas las empresas de Colombia. [En línea]. Portafolio.co. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.portafolio.co/contenido-patrocinado/ciberseguridad-a-la-medida-para-las-empresas-colombianas-592267

Cozzi, E., Graziano, M., Fratantonio, Y., & Balzarotti, D. (2018, May). Understanding linux malware. [En línea]. In 2018 IEEE symposium on security and privacy (SP) (pp. 161-175). IEEE.

CVE (2023). Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2023. [En línea]. Common Vulnerabilities and Exposures. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.cvedetails.com/top-50-products.php?year=2022

Cynet. (2023). Linux Ransomware Attack: Anatomy, Examples and Protection. [En línea]. Cynet. Estados Unidos. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.cynet.com/ransomware/linux-ransomware-attack-anatomy-examples-and-protection/

Darkcrizt. (2024). La cuota de mercado de Linux podría crecer un 19,2% para el 2027. [En línea]. Linuxadictos. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.linuxadictos.com/la-cuota-de-mercado-de-linux-podria-crecer-un-192-para-el-2027.html

DataScientest. (2022). ¿Por qué Linux es el sistema operativo preferido de los desarrolladores? DataScientest. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://datascientest.com/es/por-que-linux-es-preferido-de-los-desarrolladores

Debian.org. (2023). debian-11.8.0-amd64-DVD. [En línea]. bullseye. [Citado 24-Noviembre-2024]. Disponible en Internet https://cdimage.debian.org/cdimage/archive/11.8.0/amd64/iso-dvd/

Debian.org. (2023). debian-12.4.0-amd64-DVD. [En línea]. Bookworn. [Citado 24-Noviembre-2024]. Disponible en Internet https://cdimage.debian.org/debian-cd/current/amd64/iso-dvd/

Diaz, H. (2021). Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. [En línea]. Kaspersky. [Citado 24-Noviembre-2024]. Disponible en Internet https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Dominguez, F. L. (2013). Introducción a la informática forense.[En línea]. Ra-Ma Editorial. [Citado 24-Noviembre-2024]. Disponible en Internet

https://books.google.com.co/books?hl=es&lr=&id=Yaa6EAAAQBAJ&oi=fnd&pg=PP1&dq=inform%C3%A1tica+forense&ots=_qg997SwLd&sig=3FZLoRgRQ1v6amQjkHz2oHJCQhk&redir_esc=y#v=onepage&q=inform%C3%A1tica%20forense&f=false

Escobar, J. (2023). Los delitos cibernéticos se han reducido en el 2023: Policía Nacional. [En línea]. Radio Nacional de Colombia. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.radionacional.co/actualidad/delitos-ciberneticos-en-colombia-estadisticas-actuales

eSemana. (2023). Durante 2022 se incrementaron en 26% las vulnerabilidades informáticas. [En línea]. ESET. [Citado 24-Noviembre-2024]. Disponible en Internet https://esemanal.mx/2023/01/eset-durante-2022-se-incrementaron-en-26-las-vulnerabilidades-informaticas/

Fiscutean, A. (2022, June 3). El 'malware' para Linux va en aumento: seis tipos de ataques a tener en cuenta. [En línea]. CSO España. [Citado 24-Noviembre-2024]. Disponible en Internet https://cso.computerworld.es/cibercrimen/el-malware-para-linux-va-en-aumento-seis-tipos-de-ataques-a-tener-en-cuenta

Fortinet. (2022). América Latina empieza el año con más de 7 mil millones de intentos de ciberataques. [En línea]. FORTINET. [Citado 24-Noviembre-2024]. Disponible en Internet Disponible en Internet https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/america-latina-empieza-el-ano-con-mas-de-7-mil-intentos-ciberataques

Germain, J. (2023). Linux Malware Rates Rise to Record Levels Amid Hacker Inconsistency. [En línea]. Technewsworld. [Citado 24-Noviembre-2024]. [Citado 24-Noviembre-2024]. Disponible en Internet Disponible en Internet https://www.technewsworld.com/story/linux-malware-rates-rise-to-record-levels-amid-hacker-inconsistency-176834.html

Germain, J. M. (2023, 23 de enero). Linux Malware Rates Rise to Record Levels Amid Hacker Inconsistency. [En línea]. LinuxInsider. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.linuxinsider.com/story/linux-malware-rates-rise-to-record-levels-amid-hacker-inconsistency-176834.html

Gómez M. (2020). La importancia de la memoria RAM en un análisis forense. [En línea]. Red Seguridad. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.redseguridad.com/especialidades-tic/activos-de-informacion/la-importancia-de-la-memoria-ram-en-un-analisis-forense_20201030.html

Guillen, L. (2018, 1 de febrero). AnÃ¡lisis forense con Volatility en Virtualbox y Ubuntu. [En línea]. Luis GuillÃ©n Civera. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.luisguillen.com/posts/2018/01/analisis-forense-volatility-virtualbox-ubuntu/

Guillermo, J. (2011). Técnicas de análisis forense digital aplicadas a dispositivos y sistemas móviles. [En línea]. Universidad Continental. [Citado 24-Noviembre-2024]. Disponible en Internet https://dialnet.unirioja.es/servlet/articulo?codigo=5042969

Gutiérrez H. (2022). Evaluación de herramientas de software libre, para el sistema operativo windows, en la adquisición de evidencias de la memoria ram. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/5567/5532

INCIBE-CERT. (2023). Vulnerabilidades CVE-2023-43641. [En línea]. INCIBE. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2023-43641

Instituto Nacional de Estándares y Tecnología (NIST). (2020). Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2). [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Instituto Nacional de Estándares y Tecnología (NIST). (2020). Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2). [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

IT DIGITAL SECURITY. 2020. Aumentan los ciberataques dirigidos contra dispositivos basados en Linux. [En línea]. IT DIGITAL SECURITY. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.itdigitalsecurity.es/endpoint/2020/09/aumentan-los-ciberataques-dirigidos-contra-dispositivos-basados-en-linux

IT RESELLER. (2020). Los actores de amenazas diversifican su arsenal con herramientas Linux. [En línea]. IT RESELLER TECH & CONSULTING. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.itreseller.es/seguridad/2020/09/los-actores-de-amenazas-diversifican-su-arsenal-con-herramientas-linux

Kamathe, G. (2021) Realice análisis forenses de la memoria de Linux con esta herramienta de código abierto, Descubra qué sucede con las aplicaciones, las conexiones de red, los módulos del kernel, los archivos y mucho más con Volatility. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://opensource.com/article/21/4/linux-memory-forensics

Kaspersky. (2023). Oculto a plena vista: Kaspersky descubre un presunto ataque a la cadena de suministro dirigido a Linux. Kaspersky Lab. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://latam.kaspersky.com/about/press-releases/2023_oculto-a-plena-vista-kaspersky-descubre-un-presunto-ataque-a-la-cadena-de-suministro-dirigido-a-linux

Kaspersky. (2023). Principales amenazas de ciberseguridad para empresas: cómo protegerse de ellas. Kaspersky. [En línea]. [Citado 24-Noviembre-2024]. Disponible en Internet https://latam.kaspersky.com/resource-center/preemptive-safety/website-security-is-your-business-at-risk

Kulikova, T; Dedenok, R; Svistunova, O; Kovtun, A; Shimko, I. (2023). El spam y el phishing en 2022. [En línea]. Secure List By Kaspersky. [Citado 24-Noviembre-2024]. Disponible en Internet https://securelist.lat/spam-phishing-scam-report-2022/97582/#:~:text=En%202022%2C%20nuestras%20soluciones%20frustraron,robar%20cuentas%20de%20Telegram%20messenger.

López, M. (2007). Análisis forense digital. Hackers & Seguridad. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

López, Ó., Amaya, H., León, R., & Acosta, B. (2001). Informática forense: generalidades, aspectos técnicos y herramientas. [En línea]. Universidad de los Andes. Colombia. [Citado 24-Noviembre-2024]. Disponible en Internet https://urru.org/papers/RRfraude/InformaticaForense_OL_HA_RL.pdf

Luna, H. E. R., & Miranda, J. M. (2015). Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). [En línea]. ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica, (1). [Citado 24-Noviembre-2024]. Disponible en Internet https://www.redalyc.org/pdf/5122/512251501006.pdf

Macht, H. (2013). Live Memory Forensics on Android with Volatility. [En línea]. FAU – Friedrich – Alexander Universität. [Citado 24-Noviembre-2024]. Disponible en Internet https://homac.github.io/publications/Live_Memory_Forensics_on_Android_with_Volatility.pdf

Mandia, k; Prosise, C; y Pepe, M. Incident response & computer forensics. [En línea]. McGraw-Hill, Inc.. Disponible en Internet https://dl.acm.org/doi/abs/10.5555/1207603

Medina, E. (2022). Malware en Linux, una tendencia al alza. [En línea]. Muy Linux. [Página web]. Recuperado el 15 de enero de 2024. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.muylinux.com/2022/01/20/malware-linux-2021/

Mejías, P. (2021). ESTUDIO COMPARATIVO DE DISTRIBUCIONES LINUX PARA ANÁLISIS FORENSE. ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y SISTEMAS DE TELECOMUNICACIÓN. [En línea]. Madrid. [Citado 24-Noviembre-2024]. Disponible en Internet https://oa.upm.es/70654/1/TFG_PAULA_CARBONE_MEJIAS.pdf

Mejías, P. (2021). ESTUDIO COMPARATIVO DE DISTRIBUCIONES LINUX PARA ANÁLISIS FORENSE. ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y SISTEMAS DE TELECOMUNICACIÓN. [En línea]. Madrid. [Citado 24-Noviembre-2024]. Disponible en Internet https://oa.upm.es/70654/1/TFG_PAULA_CARBONE_MEJIAS.pdf

Merino, M. (2023). Cuanto más popular es Linux, más vulnerable: vemos dos ejemplos de malware desvelados en el último mes. [En línea]. GENBETA. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.genbeta.com/linux/cuanto-popular-linux-vulnerable-vemos-dos-ejemplos-malware-desvelados-ultimo-mes

Micucci, M. (2023). Vulnerabilidades reportadas en 2022 aumentaron 26% y alcanzaron nuevo récord histórico. [En línea]. WeLiveSecurity. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.welivesecurity.com/la-es/2023/01/12/vulnerabilidades-reportadas-2022-aumentaron-record-historico/

Miller, J. (2023). Linux Ransomware Poses Significant Threat to Critical Infrastructure. [En línea]. Dark Reading. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.darkreading.com/vulnerabilities-threats/linux-ransomware-poses-significant-threat-to-critical-infrastructure

MINISTERIOR DE AMBIENTE Y DESARROLLO SOSTENIBLE (13 DE NOVIEMBRE DE 2015). [En línea]. Ley de Protección de Datos Personales o Ley 1581 de 2012. Bogotá. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/#:~:text=Ley%20de%20Protecci%C3%B3n%20de%20Datos,de%20naturaleza%20p%C3%BAblica%20o%20privada.

Monedero, M. (2020). La importancia de la memoria RAM en un análisis forense. [En línea]. Redseguridad.[Citado 24-Noviembre-2024]. Disponible en Internet https://www.redseguridad.com/especialidades-tic/activos-de-informacion/la-importancia-de-la-memoria-ram-en-un-analisis-forense_20201030.html

Monnappa, K. (2015). Automating linux malware analysis using limon sandbox. [En línea]. Black Hat Europe, 2015, IV-A. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.blackhat.com/docs/asia-16/materials/arsenal/asia-16-KA-Limon-wp.pdf

Monzón, T. (2021). CYBER SECURITY MAGAZINE. [En línea]. Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internet https://csecmagazine.com/2020/12/31/convercienciaguatemala/

Mordor Intelligence. (2023). Análisis de mercado de sistemas operativos para servidores. [En línea]. Mordor. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.mordorintelligence.com/es/industry-reports/server-operating-system-market/market-size

Morris Mano M. (1994). Arquitectura de Computadoras. [En línea]. Pearson Prentice Hall. Pag. 480. [Citado 24-Noviembre-2024]. Disponible en Internet https://books.google.com.co/books?hl=es&lr=&id=2wWZyKu60cAC&oi=fnd&pg=PR10&dq=memoria+principal+de+una+computadora&ots=DTMKg_8uvt&sig=2YKd8sEB9WswlPcW0l3_hTm_JSo&redir_esc=y#v=onepage&q=memoria%20principal%20de%20una%20computadora&f=false

OEA. (2023). Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades. [En línea]. OAS. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf

Ordoñez J. (2019). Entorno de análisis de memoria volátil para estudiantes. [En línea]. Universidad de Málaga. [Citado 24-Noviembre-2024]. Disponible en Internet https://riuma.uma.es/xmlui/handle/10630/18711

Organización Internacional de Normalización. (2012). Tecnología de la información - Técnicas de seguridad - Directrices para la identificación, recolección, adquisición y preservación de pruebas electrónicas (ISO 27037:2012).

Organización Internacional de Normalización. (2015). Normativa para el análisis e interpretación de evidencias digitales (ISO 27042:2015)

Özeren, S. (2023, 13 de noviembre). October 2023: Key Threat Actors, Malware and Exploited Vulnerabilities. [En línea]. THE COMPLETE SECURITY VALIDATION PLATFORM. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.picussecurity.com/resource/blog/october-2023-key-threat-actors-malware-and-exploited-vulnerabilities

Peláez, H. (2018). “De las 1.000 grandes empresas que hay en el país, 995 usa la tecnología de Red Hat”. [En línea]. La república. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.larepublica.co/empresas/de-las-1-000-grandes-empresas-que-hay-en-el-pais-995-usa-la-tecnologia-de-red-hat-2808854#:~:text=Tecnolog%C3%ADa-,%E2%80%9CDe%20las%201.000%20grandes%20empresas%20que%20hay%20en%20el%20pa%C3%ADs,la%20tecnolog%C3%ADa%20de%20Red%20Hat%E2%80%9D&text=Blockchain%20es%20el%20proyecto%20m%C3%A1s,en%20d%C3%ADa%20en%20Open%20Source.&text=Uno%20de%20los%20mayores%20avances,mayores%20jugadores%20es%20Red%20Hat.

Pons, N. (2016). Linux: principios básicos de uso del sistema. [En línea]. Ediciones ENI. [Citado 24-Noviembre-2024]. Disponible en Internet https://books.google.com.co/books?hl=es&lr=&id=U9e6CLWQEaoC&oi=fnd&pg=PA11&dq=que+es+linux&ots=n5PEsH8OpH&sig=fv7Ojmzd5sBEwlTSYBgbCO3l1Fc&redir_esc=y#v=onepage&q=que%20es%20linux&f=false

Portillo, I; Rodríguez, A. (2022). Informática Forense: Las herramientas y técnicas que debes dominar. [En línea]. Campusciberseguridad.[Citado 24-Noviembre-2024]. Disponible en Internet https://www.campusciberseguridad.com/blog/item/189-informatica-forense-herramientas-tecnicas-deber-dominar

PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. (27 de junio de 2013). [En línea]. DECRETO 1377 DE 2013 - Reglamentación de la ley 1581. Bogotá. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Quintero, G. E. (2015). Importancia de la Informática Forense. [En línea]. Bogotá: Universidad Piloto. [Citado 24-Noviembre-2024]. Disponible en Internet http://repository.unipiloto.edu.co/handle/20.500.12277/2889.

Redacción tecnología. (2021). Colombia fue objeto de 7 billones de intentos de ciberataques en 2020. [En línea]. El Espectador. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.elespectador.com/tecnologia/colombia-fue-objeto-de-7-billones-de-intentos-de-ciberataques-en-2020-article/

RedHat. (2020). Contenedores versus máquinas virtuales. [En línea]. REDHAT. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.redhat.com/es/topics/containers/containers-vs-vms

REPÚBLICA DE COLOMBIA GOBIERNO NACIONAL. (5 de enero de 2009). [En línea]. LEY 1273 DE 2009 - Delitos informaticos. Bogotá. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Rosales, G. (2022). VOLATILITY: ANÁLISIS FORENSE DE MEMORIA. [En línea]. yanapti. [Citado 24-Noviembre-2024]. Disponible en Internet https://yanapti.com/2022/volatility-analisis-forense-de-memoria/

Sánchez F. (2021). La importancia de la informática forense como un eslabón en el proceso de ciberseguridad. [En línea]. INCIBE Guatemala. [Citado 24-Noviembre-2024]. Disponible en Internethttps://incibe.gt/wp-content/uploads/2021/09/Revista-Digital-Cybersecurity-Vol5.pdf#page=12

Sánchez J. (2016). Arquitectura de Computadoras Modernas. [En línea]. Universidad Autónoma del Estado de México. [Citado 24-Noviembre-2024]. Disponible en Internet http://ri.uaemex.mx/bitstream/handle/20.500.11799/63958/secme-25335.pdf?sequence=1

Santos, J. (2020). Sistemas de Información Geográfica. Universidad Nacional de Educación a Distancia – UNED. [En línea]. Cap. 3.1.2. El componente físico (Hardware) [Citado 24-Noviembre-2024]. Disponible en Internet https://books.google.com.co/books?hl=es&lr=&id=xjbeDwAAQBAJ&oi=fnd&pg=PP1&dq=memoria+ROM&ots=wru4kzxGbh&sig=xQ7PA-fn9gCdfXAkggEAHkLGwqE&redir_esc=y#v=onepage&q=memoria%20ROM&f=false

Sophos Iberia. (2023). El 76% de los ataques de ransomware en 2022 implicaron cifrado de datos, el nivel más alto de los últimos cuatro años. [En línea]. Sophos News. [Citado 24-Noviembre-2024]. Disponible en Internet https://news.sophos.com/es-es/2023/05/12/el-76-de-los-ataques-de-ransomware-en-2022-implicaron-cifrado-de-datos-el-nivel-mas-alto-de-los-ultimos-cuatro-anos/#:~:text=a%C3%B1os%20%E2%80%93%20Sophos%20News-,El%2076%25%20de%20los%20ataques%20de%20ransomware%20en%202022%20implicaron,los%20costes%20de%20recuperaci%C3%B3n%20totales.

Stadista. (2023). Cuota de mercado mundial de los sistemas operativos para ordenadores de sobremesa de 2010 a 2022. [En línea]. Stadista. [Citado 24-Noviembre-2024]. Disponible en

Internethttps://es.statista.com/estadisticas/634540/sistemas-operativos-para-pc-cuota-de-mercado-mundial/

The Volatility Foundation (2020). [En línea]. About The Volatility Foundation. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.volatilityfoundation.org/about

TicTac CCIT. (10 de 2019). CCIT Camara Colombiana de Informática y Telecomunicaciones. [En línea]. CCIT. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/#:~:text=Frente%20a%20este%20escenario%2C%20Colombia,despu%C3%A9s%20de%20Brasil%20y%20Argentina.

TicTac CCIT. (2022). Informe safe tendencias del cibercrimen 2021-2022.pdf. [En línea]. Camara Informatica de informática y telecomunicaciones. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

TicTac CCIT. 2020. Tendencias del Cibercrimen en Colombia 2019-2020. [En línea]. CCIT Camara Colombiana de Informática y Telecomunicaciones. [Citado 24-Noviembre-2024]. Disponible en Internet ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Trend Micro. (2018). Fileless Malware PowerGhost Targets Corporate Systems. [En línea]. trendmicro. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/fileless-malware-powerghost-targets-corporate-systems

Ubuntu and Canonical . (2023). [En línea]. Ubuntu 22.04.3 LTS (Jammy Jellyfish). (22.04.3). [Citado 24-Noviembre-2024]. Disponible en Internet Recuperado de: https://releases.ubuntu.com/22.04.3/

Ubuntu and Canonical . (2023). Ubuntu 18.04.6 LTS (Bionic Beaver). [En línea]. Bionic. [Citado 24-Noviembre-2024]. Disponible en Internet: https://releases.ubuntu.com/bionic/

Valbuena, S. (2023, 24 de agosto). Panorama cibernético 2023: América Latina bajo asedio de los criminales por aumento de ataques. [En línea]. infobae. [Citado 24-Noviembre-2024]. Disponible en Internethttps://www.infobae.com/tecno/2023/08/24/panorama-cibernetico-2023-america-latina-bajo-asedio-de-los-criminales-por-aumento-de-ataques/

Varshney, R., Kumar, N., Handa, A., & Shukla, S. K. (2022, November). Volatility Custom Profiling for Automated Hybrid ELF Malware Detection. [En línea]. In International Conference on Digital Forensics and Cyber Crime (pp. 274-291). Cham: Springer Nature Switzerland.

Villinger, S. (2019). ¿Qué es la memoria RAM en un ordenador? AVAST. [En línea]. AVAST. [Citado 24-Noviembre-2024]. Disponible en Internet https://www.avast.com/es-es/c-what-is-ram-memory.

Warburton, A. (2019). Fileless malware: qué es y cómo funciona el malware sin archivos. [En línea]. WeLiveSecurity. [Citado 24-Noviembre-2024]. Disponible en Internethttps://www.welivesecurity.com/la-es/2019/12/05/fileless-malware-que-es-como-funciona-malware-sin-archivos/