

Master Universitario de Ciberseguridad y privacidad.

M1.881 - TFM - Análisis forense

Alumno:

José Enrique Rodríguez González.

Tutora de TFM:

Dña. Elena Botana de Castro.

Profesor responsable de la asignatura:

D. Jordi Serra Ruiz.

Fecha de Entrega:

Enero de 2024.

FICHA DEL TRABAJO FINAL DE MASTER

Titulo del trabajo:	Análisis forense de un ordenador.
Nombre del autor:	José Enrique Rodríguez González.
Nombre del Consultor:	Elena Botana de Castro.
Área de trabajo final:	Análisis Forense.
Título del Master:	Master Universitario de Ciberseguridad y Privacidad (MUCYP).
Universidad:	Universitat Oberta de Catalunya.

RESUMEN DEL TRABAJO

El objetivo del presente Trabajo de Fin de Máster es realizar un análisis forense de un ordenador del que se sospecha de que han accedido a los sistemas de forma ilícita. Se comprobará si realmente han accedido, así como el método que han utilizado. Por otro lado, se elaborará un informe con las consecuencias que se derivan del dicho acceso ademas se comprobará si ha habido extracción de información alguna. Por último, y no menos importante, para el presente trabajo se tendrán en cuenta los estándares que existen en la actualidad, como pueden ser la norma ISO 27037, la RFC 3227 o las normas de la Asociación Española de Normalización UNE 71505 y UNE 71506.

Índice General.

- Deuda técnica.
- 0. Agradecimientos.
- 1. Plan de trabajo.
 - Índice del capítulo 1. Plan de trabajo.
 - 1.0. Introducción al capítulo 1. Plan de trabajo.
 - 1.1. Problema a resolver.
 - 1.2. Objetivos.
 - 1.3 Metodologías.
 - 1.4. Descripción del entorno de trabajo.
 - 1.5. Listado de tareas.
 - 1.6. Planificación temporal de las tareas.
 - 1.7. Revisión del estado del arte de la informática forense.
- 2. Extremos del análisis y previsión de pruebas técnicas.
 - Índice del capítulo 2. Extremos del análisis y previsión de pruebas técnicas.
 - 2.0. Introducción al capítulo 2. Extremos del análisis y previsión de pruebas técnicas.
 - 2.1. Propuesta de extremos.
 - 2.2. Previsión de pruebas técnicas.
- 3. Análisis de la memoria RAM.
 - Índice del capítulo 3. Análisis de la memoria RAM.
 - 3.0. Introducción al capítulo 3. Análisis de la memoria RAM.
 - 3.1. Acciones previas al análisis de la memoria RAM.
 - 3.2. Sistema Operativo de la memoria RAM analizada.
 - 3.3. Creación de perfil para volatility.
 - 3.4. Datos de interés de la captura de la memoria RAM.
 - 3.5. Búsqueda de procesos en funcionamiento de interés para el análisis.
 - 3.6. Listado de conexiones de red y conexiones sospechosas.
- 4. Análisis del disco duro.
 - Índice del capítulo 4. Análisis del disco duro.
 - 4.0. Introducción al capítulo 4. Análisis del disco duro.
 - 4.1. Acciones previas al análisis del disco duro.
 - 4.2. Datos de interés del disco duro.
 - 4.3. Usuarios del sistema.
 - 4.4. Análisis de evidencias del disco duro.
- 5. Resumen ejecutivo.
 - Índice del capítulo 5. Resumen ejecutivo.
 - 5.0. Introducción al capítulo 5. Resumen ejecutivo.
 - 5.1. Resumen ejecutivo
- 6. Informe pericial.
 - Índice del capítulo 6. Informe pericial.
 - 6.0. Introducción al capítulo 6. Informe pericial.
 - 6.1. Informe pericial.
- 7. Conclusiones.
 - Índice del capítulo 7. Conclusiones.
 - 7.0. Introducción al capítulo 7. Conclusiones.

- 7.1 Conclusiones.
 - 8. Anexos.
 - Índice del capítulo 8. Anexos.
 - 8.0. Introducción al capítulo 8. Anexos.
 - 8.1. Glosario de términos y abreviaturas.
 - 8.2. Imágenes.
 - 8.3. Videos.
 - 8.4. Extracto de comandos utilizados.
 - 8.5. Referencias.
 - 8.6. Línea de tiempo de evidencias.
-

Deuda técnica.

Este no es un capítulo al uso del TFM, si no que tratará de llevar un control de las tareas pendientes (Deuda técnica) de todo el TFM.

PEC 1

DEUDA TÉCNICA: Listado de aplicaciones a utilizar en la descripción del entorno de trabajo

DEUDA TÉCNICA: plantear posible reducción del estado del arte

DEUDA TÉCNICA: Referencia a Wikipedia

PEC 2

DEUDA TÉCNICA: Indexar indice, indicar paginas

DEUDA TÉCNICA: ENLAZAR CON INDICE DEL CAPITULO

DEUDA TÉCNICA: MOVER COMANDOS UTILIZADOS Y LAS IMÁGENES A LOS ANEXOS DE IMÁGENES.

COMENTARIOS TUTORA TFM PEC 1.

- Has realizado un buen trabajo con la planificación temporal y actividades.
 - Sin embargo, deben mejorarse los siguientes puntos:
 - 2. Definición de Objetivos: Has definido claramente tus objetivos, lo cual es positivo. Sin embargo, es esencial que logres responder a todos ellos en la entrega final o justifiques cualquier impedimento que impida su cumplimiento.
 - 3. Entorno de Trabajo: Debes proporcionar más detalles sobre el equipo y las herramientas específicas que utilizarás en tu análisis forense. Esto garantizará una comprensión completa de tu enfoque.
 - 5. Comparativa de Herramientas: La comparativa de herramientas es exhaustiva, pero muchas de ellas pueden resultar irrelevantes. Sería más beneficioso seleccionar algunas, analizarlas en detalle y explicar por qué las has elegido y cómo se utilizarán en tu TFM.
 - 6. Glosario: Es positivo que incluyas un glosario de términos y abreviaturas, pero es necesario desarrollarlo, incluyendo el origen de abreviaturas como "CISO".
 - 7. Bibliografía: La ausencia de una bibliografía es una deficiencia significativa. Debes incluir una bibliografía que respalde tus afirmaciones y muestre la base teórica en la que se basa tu TFM.
 - 8. Impacto ético y social: No he podido ver nada relativo a este punto en la entrega realizada.

0. Agradecimientos.

A mi esposa e hija, acompañantes en todo momento de esta aventura académica.

A mis compañeros de trabajo, Juanma, Luisma y Borja, que saben de que estos tres años que llevo realizando este master y han conocido todos los derroteros que me ha llevado este camino.

[**Volver al Índice General.**](#)

1. Plan de trabajo.

Índice del capítulo 1. Plan de trabajo.

- 1.0. Introducción al capítulo 1. Plan de trabajo.
- 1.1. Problema a resolver.
- 1.2. Objetivos.
- 1.3. Metodologías.
 - 1.3.1. Introducción.
 - 1.3.2. Normas ISO 27037 e ISO 30121.
 - 1.3.3. Norma RFC 3227.
 - 1.3.4. Normas UNE 71505 y UNE 71506.
 - 1.3.5. Conclusiones relativo a las metodologías.
- 1.4. Descripción del entorno de trabajo.
- 1.5. Listado de tareas.
- 1.6. Planificación temporal de las tareas.
- 1.7. Revisión del estado del arte de la informática forense.
 - 1.7.1. Introducción del estado del arte de la informática forense.
 - 1.7.2. Definiciones.
 - 1.7.3. Objetivos de la informática forense.
 - 1.7.4. Evidencia digital.
 - 1.7.5. Perspectiva de tres roles.
 - 1.7.6. Retos y riesgos en el análisis forense.
 - 1.7.7. Herramientas del análisis forense.

[Volver al Índice General.](#)

1.0. Introducción al capítulo 1. Plan de trabajo.

La situación en la que nos encontramos es un caso práctico laboral, en el que realizamos el papel de **CISO**.

En este caso, la dirección de la empresa tiene serias sospechas, no probadas, de que han accedido a los sistemas de forma ilícita. Por lo que el gerente de la empresa me solicita, como **CISO**, que se compruebe si realmente han accedido, así como el método que han utilizado. Por otro lado, solicitan las consecuencias que se derivan del dicho acceso, si ha habido extracción de información alguna.

1.0. Referencia 001.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

[Volver al Índice General.](#)

1.1. Problema a resolver.

Por lo expuesto en la introducción del capítulo, se coliga que el problema a resolver es la resolución de las cuestiones solicitadas por el Gerente de la empresa.

Una definición idónea que se puede adoptar en el presente Trabajo de Final de Máster (en adelante TFM) es lo indicado en su momento en la propuesta del TFM:

Solventar las necesidades del gerente de la empresa mediante el análisis forense del disco duro y la captura de memoria de un ordenador personal, en un caso real con un sistema virtualizado, vinculado a una presunta conducta delictiva real. Para ello, se utilizarán herramientas específicas para la localización de las evidencias digitales sobre los discos duros y la memoria que puedan demostrar el presunto delito (EnCase, Autopsy, Volatility, o cualquier otra herramienta, o conjunto de herramientas con prestaciones equivalentes). Finalmente, las evidencias localizadas deberán recogerse en un informe ejecutivo o pericial, el cual, además de los aspectos técnicos, deberá tener en cuenta aquellos requisitos procesales necesarios para que el análisis pueda tener validez en un proceso judicial.

1.1. Referencia 002.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

[Volver al Índice General.](#)

1.2. Objetivos.

Se describe un el siguiente listado de objetivos que se obtienen al analizar el enunciado del TFM:

1. Elaboración del Análisis forense de Disco Duro y RAM.

- 1.1. realizar una recuperación parcial o total de la información borrada existente en los dispositivos susceptibles de ser analizados (**carving**).
- 1.2. Relativo al análisis de la memoria RAM.
 - 1.2.1. Comprobar la **integridad** de la memoria RAM.
 - 1.2.2. Comprobar fecha de la captura de la RAM.
 - 1.2.3. Determinar la edición y versión de Windows que tiene instalado el sistema operativo del ordenador sobre el cual se ha efectuado la captura de la memoria RAM.
 - 1.2.4. Buscar los procesos en funcionamiento y localiza aquellos que te parezcan de interés para el análisis forense del ordenador analizado.
 - 1.2.5. Extraer los procesos que consideres sospechosos y analizarlos.
 - 1.2.6. Listar las conexiones de red y analizarlas.
- 1.3. Relativo al análisis del Disco Duro.
 - 1.3.1. Comprobar la **integridad** del disco duro.
 - 1.3.2. Determinar la siguiente información del disco duro.
 - 1.3.2.1. Tamaño del disco duro analizado.
 - 1.3.2.2. Sistema y versión del sistema operativo instalado.
 - 1.3.2.3. Nombre del propietario y relación de software instalado.
 - 1.3.2.4. "**Product ID**" y "**Product Key**" asociadas al sistema.
 - 1.3.2.5. Fecha y hora de instalación del sistema operativo.
 - 1.3.2.6. Determinar marca y modelo (si es posible) del hardware siguiente: **CPU**, monitor, tarjeta gráfica, tarjeta **Ethernet** y **Wireless**.
 - 1.3.3. Determinar qué usuarios tiene definidos el sistema.
 - 1.3.4. Localizar los documentos (archivos PDF, de texto, hojas de cálculo, etc.) que puedan tener relación con alguna conducta presuntamente delictiva.
 - 1.3.5. Localizar los archivos eliminados y determina si hay alguno relevante para la causa investigada.
 - 1.3.6. Localizar los ficheros comprimidos relevantes analizarlos, reventar contraseña si es necesario y analizar su contenido.
 - 1.3.7. Localizar algún fichero ejecutable que pueda resultar de interés para la investigación, ademas, analizar la relación con alguna evidencia anterior.
 - 1.3.8. Determinar el contenido del fichero log de un conocido programa de comunicación si es necesario y relacionarlo con el caso investigado.
 - 1.3.9. Realizar un análisis de la navegación web.
 - 1.3.10. Estudio de los dispositivos físicos que en algún momento fueron conectados al sistema estudiado: móviles, **USB's**, impresoras, escáneres, cámaras, tarjetas de memoria.
 - 1.3.11. Estudio de la información contenida en los unallocated cluster o en el file slack.
 - 1.3.12. Información contenida en los archivos de hibernación, paginación, particiones y archivos de intercambio (**swap**).
 - 1.3.13. Análisis de la cola de impresión.
 - 1.3.14. Visualización de los links de los archivos y de los archivos accedidos recientemente.
 - 1.3.15. Estudio de los metadatos de los archivos, si se considera que pueden ser relevantes para el caso.

- 1.3.16. Estudio de las aplicaciones de virtualización.
- 1.3.17 Estudio de las bases de datos instaladas y las aplicaciones que permiten su gestión.
- 1.3.18. Estudio de los programas de cifrado, particiones cifradas.
- 1.3.19. Análisis de los clientes de correo electrónico y del webmail.
- 1.4. Realizar un estudio de la seguridad.
 - 1.4.1. Estudiar si las evidencias analizadas han sido comprometidas.
 - 1.4.2. Identificar cualquier aplicación vulnerable, software malicioso, evaluar el daño sufrido, identificar los archivos que han sido comprometidos, así como determinar la vía de acceso al sistema.

2. Relativo al resumen ejecutivo, elaborarlo teniendo en cuenta los siguientes apartados.

- 2.1. Claridad en la comunicación, proporcionando información de forma clara y concisa y, por otro lado, utilizar un lenguaje accesible para los no expertos en el área.
- 2.2. Presentar el contexto u antecedentes, describiendo el motivo y las circunstancias del análisis forense y Proporcionar una breve descripción del incidente o situación bajo investigación.
- 2.3. Redactar un resumen ejecutivo con los hallazgos clave y las recomendaciones.
- 2.4. Describir la metodología utilizada durante el análisis forense.
- 2.5. Explicar las herramientas y técnicas de análisis implementadas.
- 2.6. Proporcionar una línea de tiempo detallada de los eventos y acciones tomadas.
- 2.7. Detallar los hallazgos significativos del análisis.
- 2.8. Incluir evidencia técnica relevante, como registros de logs, archivos, etc
- 2.9. Evaluar y describir el impacto del incidente en la organización o individuos afectados.
- 2.10. Proveer conclusiones basadas en los hallazgos del análisis forense.
- 2.11. Proporcionar recomendaciones para la acción futura, basadas en los hallazgos y conclusiones.
- 2.12. Sugerir medidas preventivas y correctivas para evitar incidentes similares en el futuro.

3. Elaborar un informe pericial teniendo en cuenta los siguientes apartados.

- 3.1. Mantener una postura objetiva e imparcial en todo momento.
- 3.2. Garantizar que el análisis y las conclusiones estén fundamentados en evidencias tangibles y replicables.
- 3.3. Mantener la **cadena de custodia** y la **integridad** de las pruebas durante todo el proceso.
- 3.4. Redactar el informe de manera clara, precisa y entendible para personas sin conocimientos técnicos específicos.
- 3.5. Describir detalladamente el caso, partes involucradas, y el objeto del peritaje.
- 3.6. Detallar las herramientas, técnicas y procedimientos utilizados en el análisis forense.
- 3.7. Justificar la elección de la metodología y herramientas utilizadas.
- 3.8. Establecer una línea temporal clara de todas las acciones y procesos llevados a cabo durante la investigación
- 3.9. Presentar de forma clara y precisa los hallazgos resultantes del análisis forense. Los cuales será
- 3.10 Incluir elementos visuales como gráficos, imágenes o tablas para facilitar la comprensión de los datos.
- 3.11. Interpretar las evidencias de manera fundamentada y ligada a las normativas y principios de la ciencia forense digital.
- 3.12. Derivar conclusiones basadas exclusivamente en las evidencias y hallazgos del análisis.
- 3.13. Ofrecer una opinión pericial en base a los hallazgos, respetando los límites de la prueba pericial y los datos disponibles.

- 3.14. Garantizar que toda la información manejada se mantiene confidencial y segura.
- 3.15. Discutir las implicaciones legales de los hallazgos y su posible impacto en el caso.
- 3.16. Estar preparado para ratificar el informe en un tribunal y responder a preguntas relacionadas con el análisis y los hallazgos. Este supuesto, el defensor se intuye que se realizará en la defensa síncrona de la defensa de este TFM.

4. Realizar unas conclusiones acordes a todo el TFM realizado.

- 4.1. Basarse en ideas fuerza que han aparecido durante todo el TFM.
- 4.2. Tener en cuenta que este apartado es el que finalmente, el gerente de la empresa, como miembro directivo de la misma, usando el método del Presidente Reagan.

1.2. Referencia 001.

1.2. Referencia 003.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

[Volver al Índice General.](#)

1.3. Metodologías.

1.3.1. Introducción.

En esta sección se procederá a realizar un repaso general de algunas de las normativas y estándares.

Primero abordaremos un pequeño estudio relativo a las normas ISO 27037 e ISO 30131, posteriormente abordaremos la normativa **RFC** 3227 para finalmente comentar un resumen de las normas UNE 71505 y UNE 71506.

Por ultimo, pero no menos importante, trataré unas conclusiones sobre esta sección.

1.3.2. Normas ISO 27037 e ISO 30121.

Dentro de la seguridad informática cabe destacar una normativa ampliamente conocida, es la familia ISO 27000. Esta serie de normas son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Esta serie contiene diversas normas todas relacionadas con las mejores prácticas recomendadas en Seguridad de la Información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Concretamente, existe una norma dedicada en exclusiva al análisis forense, se trata de la ISO 27037 Directrices para la identificación, recolección, adquisición y preservación de la prueba digital.

Esta norma ofrece orientación para tratar situaciones frecuentes durante todo el proceso de tratamiento de las pruebas digitales. Además define dos roles especialistas:

- **DEFR (Digital Evidence First Responders)**: Expertos en primera intervención de evidencias electrónicas.
- **DES (Digital Evidence Specialists)**: Experto en gestión de evidencias electrónicas.

ISO 27037 proporciona orientación para los siguientes dispositivos y circunstancias:

- Medios de almacenamiento digitales utilizados en equipos varios como por ejemplo discos duros, disquetes, discos magneto-ópticos y ópticos y otros similares.
- Teléfonos móviles, **PDA's**, tarjetas de memoria.
- Sistemas de navegación móvil (**GPS**).
- Cámaras de video y cámaras digitales (incluyendo circuitos cerrados de televisión).
- Ordenadores estándares con conexiones a redes.
- Redes basadas en protocolos **TCP/IP** y otros protocolos digitales.
- Otros dispositivos con funcionalidades similares a las descritas anteriormente.

Resumiendo, se puede destacar que esta norma ofrece orientación sobre el manejo de las pruebas digitales. Siguiendo las directrices de esta norma se asegura que la evidencia digital potencial se recoge de manera válida a efectos legales para facilitar su aportación en juicios y procesos legales. Además cabe destacar que cubre una amplia gama de tipos de dispositivos y situaciones, por lo que la orientación dentro de la norma es ampliamente aplicable.

Se dispone de una copia de la ISO 27037 en inglés.

1.3.2. Referencia 004

La **ISO/IEC** 30121 es la norma internacional para el análisis forense digital. Define los requisitos mínimos que todas las organizaciones deben cumplir para estar preparados ante un análisis forense digital. La primera edición de la norma se publicó en 2015. Desde entonces, se han realizado varias actualizaciones importantes para reflejar las nuevas tecnologías y la evolución de los procedimientos de investigación criminal. Ha sido adoptada por muchas organizaciones de todo el mundo como base de las mejores prácticas para el manejo de las pruebas digitales, maximizando la disponibilidad y acceso a esta.

La **ISO/IEC** 30121 se creó para garantizar que las pruebas digitales se traten de forma coherente en las distintas organizaciones y para ayudar a garantizar que las pruebas digitales puedan utilizarse como prueba

en los procedimientos judiciales.

1.3.2. Referencia 005

[**Volver al Índice del capítulo 1. Plan de trabajo.**](#)

1.3.3. Norma RFC 3227.

Otra norma destacable para mencionar es la **RFC** 3227. Este documento publicado por la **Internet Engineering Task Force (IETF)** recoge directrices para recopilar y almacenar evidencias sin ponerlas en riesgo.

En cuanto a los principios para la recolección de evidencias destacan básicamente tres, el orden de volatilidad de los datos, las acciones que deben evitarse y las consideraciones sobre la privacidad.

Sobre el procedimiento de almacenamiento tiene en cuenta la **cadena de custodia** de las pruebas recogidas anteriormente y dónde y cómo se deben almacenar estas para que estén a buen recaudo.

Para acabar detalla qué tipo de herramientas son las más útiles y qué características deben tener para evitar conflictos, haciendo hincapié en que las herramientas deben alterar lo menos posible el escenario. Según este documento el kit de análisis debe incluir las siguientes herramientas:

- Programas para listar y examinar procesos.
- Programas para examinar el estado del sistema.
- Programas para realizar copias bit a bit.

Todas estas recomendaciones tienen como epicentro el principio de intercambio de Locard, que señala que: "siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto".

Se dispone de una copia de la **RFC** 3227 en español.

1.3.3. Referencia 006.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

1.3.4. Normas UNE 71505 y UNE 71506.

Las normas UNE son normas técnicas desarrolladas por el organismo español de normalización, la Asociación Española de Normalización (UNE). "UNE" es el acrónimo de "Una Norma Española". Estas normas establecen especificaciones técnicas, criterios y directrices que deben seguirse en la fabricación, diseño, instalación, uso o mantenimiento de productos, sistemas o servicios en España.

1.3.4. Referencia 007.

Estas normas que tratamos en el presente trabajo tienen como finalidad dar una metodología para la preservación, adquisición, documentación, análisis y presentación de pruebas digitales.

Según la asociación esta norma debe dar respuesta a las infracciones legales e incidentes informáticos en las distintas empresas y entidades. Con la obtención de dichas pruebas digitales, que serán más robustas y fiables siguiendo la normativa, se podrá discernir si su causa tiene como origen un carácter intencional o negligente.

Estas normativas son de aplicación a cualquier organización con independencia de su actividad o tamaño, así como a cualquier profesional competente en este ámbito. Se dirige especialmente a incidentes y seguridad, así como al personal técnico que trabaje en laboratorios o entornos de análisis forense de evidencias electrónicas.

Se dispone de una copia de la norma UNE 71505 en el siguiente repositorio de la referencia que a continuación se detalla.

1.3.4. Referencia 008.

[**Volver al Índice del capítulo 1. Plan de trabajo.**](#)

1.3.5. Conclusiones relativo a las metodologías.

Tras analizar los distintos apartados de esta sección y otras fuentes que se indicarán al final de la sección, se puede llegar a la conclusión de que el análisis forense informático recoge de la misma manera la metodología forense por sé, siguiendo la siguiente estructura.

Aunque no existe una metodología que sea única y universal en el análisis forense, a tenor de la documentación consultada y tomando en consideración la normativa legal y los estándares vigentes a nivel internacional, sí que se puede decir que existen una serie de fases o puntos importantes que se tienen que tomar en consideración para que el análisis forense sea adecuado y sirva como elemento probatorio ante un incidente.

Todas estas recomendaciones, recogidas en distintas documentaciones (ver bibliografía), establecen una estructura lógica que permiten garantizar el proceso y que, en el ámbito civil, se compone básicamente de las siguientes fases:

1.3.5. Imagen 001.

En cada una de las fases indicadas en la imagen anterior podemos destacar las siguientes tareas.

1.3.5. Imagen 002.

1.3.5. Imagen 003.

1.3.5. Imagen 004.

PLANTEAMIENTO DEL PROBLEMA.

En el caso de que nos trata el presente TFM, estas acciones de planteamiento del problema, nos viene dado en el enunciado, ya que el enunciado, se expresa claramente que el jefe de la empresa tiene serias sospechas, no probadas, de que se ha accedido de forma licita al sistema, y por tanto, en primera instancia se requieren nuestras acciones relativo al asunto.

Entrando en el trasfondo de la legalidad y posible contaminación de pruebas, ante un presunto delito que este tipificado en el código penal, suelen ser las Fuerzas y Cuerpos de Seguridad del estado los que, bajo la orden de un juzgado de instrucción, las competentes en realizar este análisis forense por un presunto hecho

IDENTIFICACIÓN.

En el caso del presente TFM, en el enunciado hemos recibido y el material didáctico que se adjunta, se han realizado previamente y satisfactoriamente todos los pasos de esta metodología.

Cabe destacar en uno de las tareas dedicadas a la identificación, nos encontramos con la tarea de asegurar la escena, es recomendable realizar las siguientes acciones:

1. Realizar fotografías del entorno del equipo para evidenciar el estado original de la escena, identificando así el perímetro de la escena a analizar y protegiéndolo de accesos de personal no autorizado.
2. Proteger las huellas dactilares que pueda haber en los equipos para que los demás cuerpos y unidades de policía e investigadores puedan realizar su tarea. Es por lo tanto recomendable el uso de guantes de látex o similar para esta finalidad. En este punto se recuerda el principio de intercambio de Locard ya citado en el [apartado 1.3.3](#).
3. Anotar la hora y fecha de los equipos implicados que no tiene por qué coincidir con la real, esto es importante para la investigación posterior y para la realización de una línea temporal con todos los

sucesos que han ocurrido. En caso de haber desfase entre la hora del equipo y la real, este desfase se tiene que documentar para tenerlo en cuenta posteriormente. La captura de la hora y fecha se puede realizar fotografiando la pantalla o grabando un vídeo de la misma, siempre y cuando no haya que manipular el equipo para ello.

4. Ver si en pantalla hay algún proceso que nos aporte información útil sobre lo que esté pasando en directo, en ese caso, grabar todo lo que ocurre. Es importante valorar las entradas y salidas de los equipos, pues nos pueden aportar pistas importantes. De igual modo con otros periféricos de entrada/salida, tales como impresoras, teléfonos IP, escáneres, etcétera.

ADQUISICIÓN.

Llegados a esta fase, la cual ya ha sido previamente realizada a la elaboración del TFM, cabe destacar la tarea de establecer el orden de prioridad de la recolección de las evidencias. Para ello, hay que tener en cuenta una serie de principios acerca de la identificación de las evidencias y más específicamente sobre la volatilidad de las mismas. Es vital conocer qué datos son más o menos volátiles, identificarlos correctamente y posteriormente proceder a su recolección.

Entendemos por volatilidad de los datos el período de tiempo en el que estarán accesibles en el equipo. Por lo tanto, se deberán recolectar previamente aquellas pruebas más volátiles. Según la [RFC 3227](#), el que se presenta a continuación, es un posible orden de volatilidad de mayor a menor:

1.3.5. Imagen 005.

Como ya se ha indicado previamente, si se quiere realizar una depuración de responsabilidades de manera penal, es necesario establecer una autoridad legal que presente la recogida de evidencias, ya sea un secretario judicial o un notario.

La ultima tarea de esta fase es la recogida de evidencias, para ello se realiza una copia bit a bit de los discos que se quieran analizar, es decir, se requiere una copia exacta del contenido de los discos incautados. Esto incluye todos los archivos del disco, por ejemplo los temporales, los ocultos, los de configuración, los eliminados y no sobrescritos y la información relativa a la parte del disco no asignada, es lo que se conoce como copia a bajo nivel.

Esta copia se llevará a cabo sobre un soporte limpio mediante un borrado seguro de los datos que pudiera contener anteriormente para evitar así contaminaciones con otros casos.

PRESERVACIÓN.

Esta acción, se ha realizado al igual que las anteriores, ha sido realizada de manera previa a la elaboración del TFM, para ello se tienen que tener en cuenta las siguientes consideraciones.

Una vez realizada la copia se debe verificar la [integridad](#) de la misma. Para ello se calcula el [hash](#) o [CRC](#) de la copia, normalmente los equipos destinados al clonado de discos ya incorporan esa característica. Así con el [hash](#) del disco original y el de la copia se puede certificar que ambos son idénticos a todos los niveles y ante un juez, por ejemplo, quedará probado que no se ha manipulado de ningún modo. Con este procedimiento también nos aseguraremos que no se han producido errores en la copia.

Con la primera copia realizada y comprobada procedemos a realizar una segunda copia sobre la primera. En este caso también se comprobará que el contenido es idéntico mediante el mismo proceso descrito

anteriormente. Teniendo ambas copias entregaremos la primera al secretario judicial o notario responsable del caso y nos quedaremos con la segunda para poder trabajar. La segunda copia será nuestra copia de respaldo en todo momento en el laboratorio y no será para trabajar directamente con ella en ningún caso. Para realizar el análisis se deberá realizar una tercera copia, comprobar su **integridad** y trabajar sobre ella, de tal modo que en caso de cualquier desastre o alteración de los datos siempre tengamos la segunda copia exacta al original de donde poder volver a realizar otra copia para analizar.

Una mala preservación de las evidencias, un mal uso o una mala manipulación pueden invalidar toda la investigación que se lleva a cabo delante de un tribunal, este es un factor muy importante que se va repitiendo a lo largo de toda la metodología.

La **cadena de custodia** es el procedimiento controlado aplicable a las evidencias relacionadas con el suceso, desde el momento en que se encuentran en la escena hasta su análisis en el laboratorio. La finalidad de la **cadena de custodia** es evitar cualquier tipo de manipulación y tener un control absoluto sobre todos los elementos incautados, quién los ha manipulado, cómo lo ha realizado, porqué los ha manipulado, para qué lo ha hecho y cuándo ha tenido lugar dicha manipulación.

Es importante realizar todas las anotaciones descritas en la fase de identificación de las evidencias para que esta fase sea aún más sólida. Con todos los elementos documentados será mucho más fácil tener un control de todas las evidencias que disponemos y poder realizar una traza de todas las pruebas adquiridas.

Además se tendrá en cuenta de proteger los bienes para el transporte desde el lugar de los hechos hasta el laboratorio con los medios necesarios para evitar golpes o proteger de caídas fortuitas.

La documentación de la **cadena de custodia** deberá contener también todos los lugares por donde ha pasado la evidencia y quién ha realizado su transporte y su acceso.

En nuestro caso, cabe destacar que una vez iniciado el análisis de la memoria, esta no debe de modificarse ni contaminarse, en caso de ello el **Hash** de las evidencias cambiaría, por lo que la evidencia ha quedado contaminada. Hay que hacer estas acciones teniendo presente al secretario judicial, para que esa copia quede registrada si es necesario y que no ha habido mas alteraciones al respecto, ese cambio de **hash** será notificado y adjuntado en el proceso de instrucción, haciéndose también nuevas copias de este nuevo "snapshot" de la prueba.

ANÁLISIS.

La fase de análisis, **en la cual iniciamos la elaboración del presente TFM**, no termina hasta que no se puede determinar qué o quién causó el incidente, cómo lo hizo, qué afectación ha tenido en el sistema, etc. Es decir, es el núcleo duro de la investigación y tiene que concluir con el máximo de información posible para poder proceder a elaborar unos informes con todo el suceso bien documentado.

Antes de empezar el análisis, es importante recordar unas premisas básicas que todo investigador debe tener presente en el momento de enfrentarse al incidente. Como ya se ha explicado nunca se debe trabajar con datos originales y se debe respetar cada una de las leyes vigentes en la jurisdicción donde se lleve a cabo la investigación. Los resultados que se obtengan de todo el proceso han de ser verificables y reproducibles, así que en cualquier momento debemos poder montar un entorno donde reproducir la investigación y mostrarlo a quién lo requiera. Es importante también disponer de una documentación adicional con información de diversa índole, por ejemplo:

- Sistema operativo del sistema.

- Programas instalados en el equipo.
- Hardware, accesorios y periféricos que forman parte del sistema.
- Datos relativos a la conectividad del equipo:
 - Si dispone de **firewall**, ya sea físico o lógico.
 - Si el equipo se encuentra en zonas de red especiales, por ejemplo, **DMZ**.
 - Si tiene conexión a Internet o utiliza **proxies**.
- Datos generales de configuración que puedan ser de interés para el investigador para ayudar en la tarea.

Para ayudar al desarrollo de esta fase del análisis forense podemos centrarnos en varias subfases o puntos importantes que generalmente siempre deben realizarse. Cabe recordar que no existe ningún proceso estándar que ayude a la investigación y habrá que estudiar cada caso por separado teniendo en cuenta las diversas particularidades que nos podamos encontrar. No será lo mismo analizar un equipo con sistema operativo Windows o con Linux. Tampoco será lo mismo un caso de intrusión en el correo electrónico de alguien o un ataque de denegación de servicio a una institución. De igual forma no actuaremos con los mismos pasos en un caso de instalación de un malware que destruya información de una ubicación de disco o un malware que envíe todo lo que se teclea en un equipo.

En todo caso, se pueden destacar varios pasos, que habrá que adaptar en cada caso:

- Preparar un entorno de trabajo adaptado a las necesidades del incidente.
- Reconstruir una línea temporal con los hechos sucedidos.
- Determinar qué procedimiento se llevó a cabo por parte del atacante.
- Identificar el autor o autores de los hechos.
- Evaluar el impacto causado y si es posible la recuperación del sistema.

Antes de empezar el análisis propiamente, se debe preparar un entorno para dicho análisis. Es el momento de decidir si se va a hacer un análisis en caliente o en frío.

En caso de un análisis en caliente se hará la investigación sobre los discos originales, lo que conlleva ciertos riesgos. Hay que tomar la precaución de poner el disco en modo sólo lectura, esta opción sólo está disponible en sistemas operativos Linux pero no en Windows. Si se opta por esta opción hay que operar con sumo cuidado pues cualquier error puede ser fatal y dar al traste con todo el proceso, invalidando las pruebas.

Si se opta por un análisis en frío, lo más sencillo es preparar una máquina virtual (en adelante VM) con el mismo sistema operativo del equipo afectado y montar una imagen del disco. Para ello, previamente habremos creado la imagen a partir de las copias que se hicieron para el análisis. En este caso podremos trabajar con la imagen, ejecutar archivos y realizar otras tareas sin tanto cuidado, pues siempre cabe la opción de volver a montar la imagen desde cero en caso de problemas.

La opción del análisis en frío, ***La cual será el caso que nos atañe el presente TFM, ya que de este modo es como se realizará el análisis***, resulta muy atractiva pues en caso de malwares se podrán ejecutar sin miedo, reproducir lo que ocurre y desmontar la imagen sin que la copia original resulte afectada. De este modo tal vez se pueda ir un poco más allá en la investigación y ser un poco más agresivo.

Existen varios programas gratuitos para crear y gestionar VM's por ejemplo, Oracle VM VirtualBox, que ofrecen muy buenas prestaciones.

Para la tarea de construir una cadena de acontecimientos y hacer una linea temporal cabe destacar lo siguiente.

Para crear la línea temporal, lo más sencillo es referirnos a los tiempos MACD de los archivos, es decir, las fechas de modificación, acceso, cambio y borrado, en los casos que aplique. Es importante, como ya se ha indicado en alguna ocasión tener en cuenta los husos horarios y que la fecha y hora del sistema no tienen por qué coincidir con los reales. Este dato es muy importante para poder dar crédito a las pruebas y a la investigación en general.

Para empezar, lo mejor es determinar la fecha de instalación del sistema operativo, para ello se puede buscar en los datos de registro. Además la mayoría de ficheros del sistema compartirán esa fecha. A partir de aquí puede ser interesante ver qué usuarios se crearon al principio, para ver si hay discrepancias o usuarios fuera de lo común en últimos instantes del equipo. Para ver esta información también es útil acudir al registro del sistema operativo.

Teniendo ya los datos iniciales del sistema, ahora se puede proceder a buscar más información en los ficheros que se ven "a simple vista". Lo importante es localizar que programas fueron los últimos en ser instalados y qué cambios repercutieron en el sistema. Lo más habitual es que estos programas no se instalen en los lugares habituales, sino que se localicen en rutas poco habituales, por ejemplo en archivos temporales o mezclados con los archivos y librerías del sistema operativo. Aquí se puede ir creando la línea temporal con esos datos.

Alternativamente es útil pensar que no todos los archivos están a la vista. Se puede encontrar información en archivos normales, pero también en temporales, ocultos, borrados o usando técnicas como la esteganografía, no se puede obviar ninguna posibilidad.

Habitualmente los sistemas operativos ofrecen la opción de visualizar los archivos ocultos y también las extensiones. Es útil activar estas opciones para detectar posibles elementos ocultos y extensiones poco habituales que nos resulten extrañas.

Para los archivos borrados se utilizarán programas especiales capaces de recuperar aquellos datos que se hayan eliminado del disco pero sobre los cuales aún no se haya sobrescrito nada. Es posible que el atacante elimine archivos o registros varios en afán de esconder lo que ha ocurrido, si estos no han sido sobrescritos se podrán recuperar y se podrán situar en la línea temporal relacionándolos con el conjunto de sucesos. Para recuperar información oculta mediante esteganografía también se deberán usar programas concretos. Es posible que el atacante ocultara información sobre otros archivos, tales como imágenes o audio para enviarlos posteriormente o tenerlos almacenados sin llamar la atención. Habitualmente hallaremos más información en ubicaciones ocultas que en los lugares más habituales.

Con todos estos datos se debería poder crear un esbozo de los puntos clave en el tiempo tales como la instalación del sistema, el borrado de determinados archivos, la instalación de los últimos programas, etcétera.

El siguiente paso del análisis es determinar el **como se actuó**. Para determinar cómo se actuó es importante llevar a cabo una investigación sobre la memoria del equipo. Es interesante realizar un volcado de memoria para la obtención de cierta información. Con programas destinados a tal fin podremos ver que procesos se están ejecutando en el momento concreto y también aquellos que hayan sido ocultados para no levantar sospechas. Con esta información podremos saber qué ejecutables inician los procesos en ejecución y qué librerías se ven involucradas. Llegados aquí se puede proceder a realizar volcados de los ejecutables y de dichas librerías para poder analizar si contienen cadenas sospechosas o si, por lo contrario, son archivos legítimos. Sabiendo los procesos que se ejecutan y su naturaleza podemos obtener pistas de cómo se actuó para comprometer el equipo.

A menudo nos deberemos fijar en procesos en ejecución aparentemente inofensivos, habituales y legítimos en los sistemas operativos. No es extraño que determinados procesos con fines malintencionados se camuflen con procesos legítimos. Para ello deberemos observar que muchas veces estos se encuentran sin un proceso padre, cuando lo más habitual es que dependan de otros. En otras ocasiones simplemente se camuflan con nombres muy parecidos a otros para pasar desapercibidos.

Ciertos programas también nos darán información sobre las cadenas del ejecutable en cuestión. Con ellas podremos ver si mutan su contenido cuando se ejecutan en memoria y cuál es su contenido. En ocasiones, cierta información de las cadenas nos puede dar pistas muy valiosas, como por ejemplo, cadenas dónde encontrar logs, o enlaces a direcciones de Internet. También nos puede dar pistas sobre el tipo de malware al que nos enfrentamos. Si por ejemplo encontramos cadenas con alfabetos o teclas concretas del teclado, es probable que nos encontremos ante un keylogger.

Finalmente, otra práctica interesante para determinar cómo se actuó es leer la secuencia de comandos escrita por consola. Para ello procederemos con el volcado de memoria y podremos obtener dicha información. De este modo podremos leer qué comandos se hicieron por consola y sabremos si se ejecutó algún proceso de este modo. Debemos excluir nuestras propias instrucciones pues seguramente aparecerán los comandos del volcado de memoria que se hicieron en su momento. Relativo a esta práctica, personalmente es la primera que se debería de realizar en un análisis forense, de ahí también poder corroborar qué es lo que pueda decir el usuario en una posible entrevista, que en este caso no va a ser posible.

Para la tarea de identificación de autores, cabe destacar que para poder realizar una identificación del autor o autores del incidente, otra información importante que nos puede dar el volcado de memoria son las conexiones de red abiertas y las que están preparadas para enviar o recibir datos. Con esto podremos relacionar el posible origen del ataque buscando datos como la dirección **IP** en Internet.

Hay que actuar con prudencia puesto que en ocasiones se utilizan técnicas para distribuir los ataques o falsear la dirección **IP**. Hay que ser crítico con la información que se obtiene y contrastarla correctamente. No siempre se obtendrá la respuesta al primer intento y posiblemente en ocasiones sea muy difícil averiguar el origen de un incidente.

Es interesante recapacitar en los distintos perfiles de atacantes que se pueden dar hoy día en este ámbito para intentar mimetizarse y entender quién pudo ser el autor.

Por un lado podemos encontrar organizaciones y criminales que actúan por motivaciones económicas. Su finalidad es robar cierta información, ya sea empresarial o personal, para una vez obtenida venderla o sacar un rendimiento oneroso de la información.

Por otro lado está quién sólo busca acceder a sistemas por mero prestigio y reconocimiento en su ambiente cibernético. Accediendo a sistemas mal configurados y publicando datos que prueben su fechoría incrementará su notoriedad y se dará a conocer más en las redes.

En este punto es importante analizar dos vertientes. En caso que se esté realizando un peritaje con fines inculpatorios, o sea, judiciales, se deberá intentar resolver quién es el autor o al menos aportar pistas fiables para que otros investigadores puedan llevar a cabo otras investigaciones de otros ámbitos.

En cambio, si es con fines correctivos lo más interesante seguramente será obviar esta fase y proceder con el estudio del impacto causado y estudiar las mejoras que se pueden implantar para evitar episodios similares.

Para establecer el impacto causado, cabe destacar que se puede calcular en base a distintos factores y no hay un método único para su cálculo, ni una fórmula que nos dé un importe económico. Aun así para estos cálculos puede servir ayudarse de métodos como BIA (Business Impact Analysis) que determinan el impacto de ciertos eventos ayudando a valorar los daños económicamente.

A la larga cualquier incidente ocurrido devengará en unos gastos económicos que habrá que cuantificar en función de los ítems afectados tras el suceso. En ocasiones el coste económico resultará de tener que reemplazar una máquina o dispositivo que ha quedado inservible tras un ataque o bien las horas de empleado de tener que reinstalar el sistema. En este caso, el cálculo no supone mayor dificultad y se resuelve fácilmente.

En otras ocasiones, por ejemplo, los daños pueden deberse al robo de una información de secreto industrial en el que habrá que cuantificar no sólo qué supone reponer el sistema sino, a la larga, en qué se verá afectada la empresa. Los datos robados pueden ser para publicar cierta información sobre la empresa y poner en la opinión pública datos con intenciones de crear mala imagen, lo cual supone un daño incalculable y muy elevado para la empresa.

El impacto no sólo se puede calcular en base económica. Como ya se ha comentado al inicio de esta sección también existen otros factores, es el caso del tiempo de inactividad. Si el incidente ha supuesto paralizar la producción de una planta automatizada de fabricación esto supone muchas horas en que la producción es nula, por lo tanto no se trabajará. Evidentemente, a la larga también supondrá un problema económico pues no se podrán servir los pedidos pendientes de los clientes. Si la paralización afecta a una oficina, tal vez no se pare la producción de bienes pero sí el trabajo de los empleados que verán retrasado todo su trabajo.

PRESENTACIÓN.

La última fase de un análisis forense queda para redactar los informes que documenten los antecedentes del evento, todo el trabajo realizado, el método seguido y las conclusiones e impacto que se ha derivado de todo el incidente.

Para ello se redactarán dos informes, a saber, el informe técnico y el ejecutivo. En esencia en ambos informes se explican los mismos hechos pero varía su enfoque y el grado de detalle con que se expone el asunto.

- En el informe ejecutivo se usará un lenguaje claro y sin tecnicismos, se debe evitar usar terminología propia de la ciencia e ingeniería y expresiones confusas para gente no ducha en el tema. Hay que pensar que el público lector de estos informes serán jueces y gerentes que seguramente estén poco relacionados con el tema y además tengan poco tiempo para dedicarle. Se les debe facilitar la tarea al máximo.
- En el informe técnico, por el contrario, el público final será técnico y con conocimientos de la materia que se expone. Aquí se detallarán todos los procesos, los programas utilizados, las técnicas, etcétera. Debemos crear un documento que pueda servir de guía para repetir todo el proceso que se ha realizado en caso necesario.

Relativo al informe ejecutivo, cabe destacar que será un resumen de toda la tarea que se ha llevado a cabo con las evidencias digitales. Aunque será un documento de poca extensión, al menos comparado con el informe técnico, éste deberá contener al menos los siguientes apartados:

- Motivos de la intrusión.
 - ¿Por qué se ha producido el incidente?

- ¿Qué finalidad tenía el atacante?
- Desarrollo de la intrusión.
 - ¿Cómo lo ha logrado?
 - ¿Qué ha realizado en los sistemas?
- Resultados del análisis.
 - ¿Qué ha pasado?
 - ¿Qué daños se han producido o se prevén que se producirán?
 - ¿Es denunciable?
 - ¿Quién es el autor o autores?
- Recomendaciones.
 - ¿Qué pasos dar a continuación?
 - ¿Cómo protegerse para no repetir los hechos?

El informe técnico será más largo que el anterior y contendrá mucho más detalle. Se hará una exposición muy detallada de todo el análisis con profundidad en la tecnología usada y los hallazgos. En este caso se deberá redactar, al menos:

- Antecedentes del incidente.
 - Puesta en situación de cómo se encontraba la situación anteriormente al incidente.
- Recolección de datos.
 - ¿Cómo se ha llevado a cabo el proceso?
 - ¿Qué se ha recolectado?
- Descripción de la evidencia.
 - Detalles técnicos de las evidencias recolectadas, su estado, su contenido, etc.
- Entorno de trabajo del análisis.
 - ¿Qué herramientas se han usado?
 - ¿Cómo se han usado?
- Análisis de las evidencias.
 - Se deberá informar del sistema analizado aportando datos como las características del sistema operativo, las aplicaciones instaladas en el equipo, los servicios en ejecución, las vulnerabilidades que se han detectado y la metodología usada.
- Descripción de los resultados.
 - ¿Qué herramientas ha usado el atacante?
 - ¿Qué alcance ha tenido el incidente?
 - Determinar el origen del mismo y como se ha encontrado.
- Dar la línea temporal de los hechos ocurridos con todo detalle.
- Redactar unas conclusiones con las valoraciones que se crean oportunas a la vista de todo el análisis realizado.
- Dar unas recomendaciones sobre cómo proteger los equipos para no repetir el incidente o sobre cómo actuar legalmente contra el autor.

1.3.5. Referencia 009.

1.3.5. Referencia 010.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

[Volver al Índice General.](#)

1.4. Descripción del entorno de trabajo.

El entorno de trabajo para un análisis forense enfocado en la exploración de memoria RAM y disco duro exige una meticulosa preparación y adecuación de las herramientas y espacios de trabajo. Las evidencias, provenientes tanto de la RAM como del almacenamiento persistente del ordenador en cuestión, se convierten en el pilar fundamental del análisis, permitiendo la evaluación de procesos en ejecución, archivos almacenados, registros de actividad y cualquier otro elemento que pueda arrojar luz sobre las acciones realizadas en la máquina.

En un segundo plano, pero no menos esencial, se encuentra el portátil personal, que se configura como la estación de trabajo principal para la realización del análisis forense. Este debe estar equipado con un sistema operativo que, comúnmente en el ámbito forense, suele ser alguna distribución de Linux, junto con una serie de herramientas específicas para el análisis forense (como Autopsy o Sleuth Kit). No obstante, la selección y configuración de estas herramientas incurren en una deuda técnica que debe ser minuciosamente administrada, asegurando la pertinencia, licencia y compatibilidad de las mismas.

Relativo al ordenador personal destacar las siguientes aplicaciones que se van a utilizar para la realización del análisis.

- VirtualBox
- Volatility

DEUDA TÉCNICA: Listado de aplicaciones a utilizar en la descripción del entorno de trabajo

Por otro lado, la documentación y redacción del TFM se consolida mediante el uso del repositorio en GitHub TFM-ANÁLISIS-FORENSE (<https://github.com/jrodg85/TFM-ANALYSIS-FORENSE>). Este repositorio no solo sirve como medio para documentar y presentar los hallazgos y metodologías empleadas, sino que también se erige como una herramienta para gestionar versiones y cambios a lo largo del desarrollo del trabajo, facilitando la trazabilidad y coherencia del mismo. Se deben establecer estrategias robustas para garantizar la **integridad** y confidencialidad de la información almacenada, considerando la naturaleza sensible de los datos manejados en la investigación forense.

Finalmente, Internet emerge como un recurso invaluable para la investigación, actualización y comunicación a lo largo del proyecto. Navegar por la red debe ser realizado de forma segura y consciente, protegiendo las comunicaciones y asegurando la **integridad** de las herramientas y datos descargados.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

[Volver al Índice General.](#)

1.5. Listado de tareas.

En esta sección se ha elaborado después de una planificación del trabajo, el cual se han designado el siguiente listado de tareas a realizar. Gracias a este listado, podemos organizar el cómo vamos a realizar el TFM

Destacar que durante el listado de las tareas, cabe mencionar que habrán tareas de grooming o refinamiento, ellas no son utilizadas para reducción de deuda técnica, el objetivo estas jornadas es reflexionar sobre el contenido del mismo y valorar posibilidad de mejorar la organización del mismo. Estas variaciones, gracias a que se está realizando un control de versiones con git, se podrán ver las evoluciones o cambios del TFM en el mismo.

Durante la elaboración del reto 1 (PEC 1), se realizarán las siguientes tareas:

1. Lectura enunciado actividad 1.
2. Decisión de formato de TFM.
3. Maquetación de TFM en LaTeX.
4. Elaboración de índice.
5. Refinamiento de TFM 1.
6. Diagrama de Gantt.
7. Problema a resolver.
8. Objetivos.
9. Revisión del estado del arte de la informática forense.
10. Refinamiento de TFM 2.

Durante la elaboración del reto 2 (PEC 2), se realizarán las siguientes tareas:

1. Lectura enunciado actividad 2.
2. Extremos de análisis y previsión de pruebas: Introducción.
3. Extremos de análisis.
4. Previsión de pruebas.
5. Análisis de la memoria RAM: Introducción.
6. Acciones previas al análisis de RAM.
7. Búsqueda de procesos en funcionamiento.
8. Análisis y extracción de procesos sospechosos.
9. Listado de conexiones de red y conexiones sospechosas.
10. Refinamiento TFM 3.
11. Feedback de la PEC 01.
12. Análisis de disco duro: Introducción.
13. Acciones previas al análisis de disco duro.
14. Datos de interés y usuarios del sistema del disco duro analizado.
15. Análisis de las evidencias del disco duro.
16. Planning relativo al resumen ejecutivo.
17. Planning relativo al informe pericial.
18. Adaptación al índice a los nuevos cambios en los capítulos 6 y 7.
19. Refinamiento TFM 4.

Durante la elaboración del reto 3 (PEC 3), se realizarán las siguientes tareas:

1. Lectura enunciado actividad 3.
2. Introducción Resumen ejecutivo.
3. Análisis Ejecutivo.
4. Conclusión de análisis ejecutivo.
5. Refinamiento TFM 5.
6. Feedback de la PEC 02.
7. Introducción del informe pericial.
8. Cuerpo del informe pericial.
9. Conclusiones del informe pericial.
10. Conclusiones TFM.
11. Revision de términos abreviaturas y acrónimos.
12. Revisión de imágenes.
13. Revision de referencias.
14. Refinamiento TFM 6.

Durante la elaboración del reto 4 (PEC 4), se realizarán las siguientes tareas.

1. Revisión de las anotaciones y consejos de la tutora de TFM 1.
2. Ultimas correcciones Feedback TFM 1.
3. Revisión de las anotaciones y consejos de la tutora de TFM 2.
4. Ultimas correcciones Feedback TFM 2.

La Entrega de videos, presentación y realización de la defensa del TFM, se consideran que están fuera de este TFM, ya que a partir de la fecha se considera entregado el presente documento.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

[Volver al Índice General.](#)

1.6. Planificación temporal de las tareas.

Para esta sección, se han elaborado los siguientes diagramas de Gantt relativos a cada uno de los retos a entregar.

Relativo al reto/PEC 1 se establece el siguiente diagrama:

1.6. Imagen 001.

Relativo al reto/PEC 2 se establece el siguiente diagrama.

1.6. Imagen 002.

Relativo al reto/PEC 3 se establece el siguiente diagrama.

1.6. Imagen 003.

Relativo al reto/PEC 4 se establece el siguiente diagrama.

1.6. Imagen 004.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

[Volver al Índice General.](#)

1.7. Revisión del estado del arte de la informática forense.

1.7.1. Introducción del estado del arte de la informática forense.

El análisis forense, también llamado informática forense, computación forense, análisis forense digital o examen forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal.

Dichas técnicas incluyen reconstruir elementos informáticos, examinar datos residuales, autenticar datos y explicar las características técnicas del uso de datos y bienes informáticos.

Esta disciplina no sólo hace uso de tecnologías de punta para mantener la **integridad** de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados de informática y sistemas para identificar lo que ha ocurrido dentro de cualquier dispositivo electrónico. La formación de un informático forense abarca no sólo el conocimiento del software, sino también de hardware, redes, seguridad, piratería, hackeo y recuperación de información.

La informática forense ayuda a detectar pistas sobre ataques informáticos, robos de información, conversaciones o para recolectar evidencias en correos electrónicos y chats.

La evidencia digital o electrónica es sumamente frágil, de ahí la importancia de mantener su integridad; por ejemplo, el simple hecho de pulsar dos veces en un archivo modificaría la última fecha de acceso del mismo.

Dentro del proceso del análisis forense, un examinador forense digital puede llegar a recuperar información que haya sido borrada desde el sistema operativo. El informático forense debe tener muy presente el principio de intercambio de Locard por su importancia en el análisis criminalístico, así como el estándar de Daubert para hacer admisibles en juicio las pruebas presentadas por el experto forense.

Es muy importante mencionar que la informática o el análisis forense no tiene como objetivo prevenir delitos, por lo que resulta imprescindible tener claros los distintos marcos de actuación de la informática forense, la seguridad informática y la auditoría informática.

[**Volver al Índice del capítulo 1. Plan de trabajo.**](#)

1.7.2. Definiciones.

Existen diferentes términos referentes a la ciencia forense en informática. Cada uno de estos términos trata de manera particular o general temas que son de interés para las ciencias forenses.

Computación forense (computer forensics).

1. Disciplina de la ciencia forense que considera los procedimientos en relación con las evidencias para descubrir e interpretar la información en los medios informáticos con el fin de establecer hipótesis o hechos relacionados con un caso. (Centrada en las consideraciones forenses).
2. Disciplina científica que ofrece un análisis de la información que contienen las tecnologías y de los equipos de computación a partir de su compresión.(Centrada en la tecnología).

Ciencia forense en las redes (network forensics).

1. Trata las operaciones de redes de computadores, estableciendo rastros e identificando movimientos y acciones. Es necesario entender los protocolos, configuraciones y la infraestructura de las comunicaciones. A diferencia de la computación forense, es necesario poder establecer relaciones entre eventos diferentes e incluso aleatorios.

Ciencia forense digital (digital forensics).

1. Es una forma de aplicar los conceptos y procedimientos de la criminalística a los medios informáticos o digitales. Su objetivo es apoyar al poder judicial en el contexto de la inseguridad informática es decir, la perpetración de posibles delitos aclarando temas relacionados con incidentes o fraudes.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

1.7.3. Objetivos de la informática forense.

La informática forense tiene tres objetivos:

1. La compensación de los daños causados por los intrusos o criminales.
2. La persecución y procesamiento judicial de los criminales.
3. La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos se alcanzan de varias formas, siendo la principal la recopilación de evidencias.

Es importante mencionar que quienes se dedican a la informática forense deben ser profesionales con altos niveles de ética, pues gracias a su trabajo se toman decisiones sobre los hechos y casos analizados.

[**Volver al Índice del capítulo 1. Plan de trabajo.**](#)

1.7.4. Evidencia digital.

Los discos duros, las memorias **USB** y las impresoras (entre otros elementos) se pueden considerar evidencias en un proceso legal, al igual que las huellas digitales o las armas. Las evidencias digitales son las que se extraen de un medio informático.

Características.

Estas evidencias comparten una serie de características que dificultan el ejercicio de la computación forense:

1. Volatilidad.
2. Anonimato.
3. Facilidad de duplicación.
4. Alterabilidad.
5. Facilidad de eliminación.

Categorías.

Estas evidencias se pueden dividir en tres categorías:

- Registros almacenados en el equipo de tecnología informática (ej. imágenes y correos).
- Registros generados por equipos de tecnología informática (ej. transacciones, registros en eventos).
- Registros parcialmente generados y almacenados en los equipos de tecnología informática (ej. consultas en bases de datos).

Dispositivos a analizar.

Cualquier infraestructura informática que tenga una memoria (almacenamiento) es susceptible a los análisis:

- Disco duro de una Computadora o Servidor.
- Documentación referente al caso.
- Tipo de sistema de telecomunicaciones.
- Dirección **MAC**.
- Inicios de sesiones.
- Información de los cortafuegos.
- **IP**, redes **Proxy**, **LMhost**, host, conexiones cruzadas, pasarelas.
- Software de supervisión y seguridad.
- Credenciales de autentificación.
- Rastreo de paquetes de red.
- Teléfonos móviles o celulares (telefonía móvil)
- Agendas electrónicas (**PDA**).
- Dispositivos de **GPS**.
- Impresoras.
- Memorias **USB**.
- **BIOS**.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

1.7.5. Perspectiva de tres roles.

En el análisis de un caso en el que sea necesario el cómputo forense, hay tres roles principales que son importantes y se deben tener en cuenta: el intruso, el administrador y la infraestructura de la seguridad informática, al igual que el investigador.

Intrusos.

El intruso es aquel que ataca un sistema, hace cambios no autorizados, manipula contraseñas o cambia configuraciones, entre otras actividades que ponen a prueba la seguridad de un sistema. La intención de los intrusos es un punto clave para poder analizar el caso, ya que no se puede comparar un intruso cuya motivación es el dinero con otro cuya motivación es la demostración de sus habilidades. Jeimy J. Cano hace una comparación entre las motivaciones de diferentes tipos de atacantes en la siguiente tabla, basada en el artículo de Steven Furnell Cybercrime.

Motivaciones	Ciberterroristas	Phreakers	Script kiddies	Crackers	Desarrollo de virus	Atacante interno
Reto	X				X	X
Ego	X	X			X	
Espionaje				X	X	X
Ideología	X					
Dinero		X		X	X	X
Venganza	X		X		X	X

En la primera fase (reconocimiento), se busca reconocer y recolectar información. De esta manera, el atacante puede saber cómo puede actuar y los riesgos posibles, para así poder avanzar. En la segunda fase (ataque) se compromete el sistema, avanzando hasta el nivel más alto, teniendo el control del sistema atacado. Esta etapa usualmente se maneja de manera discreta, lo que dificulta la identificación del intruso. Usualmente, la vanidad del intruso y la falta de discreción ayudan al investigador a resolver el caso con mayor facilidad. Finalmente, (en la fase de eliminación) se altera, elimina o desaparece toda la evidencia que pueda comprometer al intruso en algún caso judicial. Del cuidado con el que el atacante proceda en esta fase depende el proceso del informático forense y del caso.

Administradores y la infraestructura de la seguridad informática.

El administrador del sistema es el experto encargado de la configuración de este, de la infraestructura informática y de la seguridad del sistema. Estos administradores son los primeros en estar en contacto con la inseguridad de la información, ya sea por un atacante o por una falla interna de los equipos. Al ser los arquitectos de la infraestructura y de la seguridad de la información del sistema, son quienes primero deberían reaccionar ante un ataque. Además, ellos deben proporcionar su conocimiento de la infraestructura del sistema para apoyar el caso y poder resolverlo con mayor facilidad.

Las infraestructuras de seguridad informática (realizadas por el administrador) han avanzado a medida que avanzan las tecnologías. Inicialmente, se utilizaba una infraestructura centralizada en la cual la información se encontraba en un equipo. Por lo tanto, en este caso la seguridad informática se concentraba en el control del

acceso a los equipos con la información, al control del lugar en donde se encontraban y en el entrenamiento de quienes estaban encargados de manejar los equipos. Pero con la tecnología fueron cambiando las infraestructuras y las inseguridades cambiaron. Así es como se crearon los **proxies**, **firewall**, el sistema de detección de intrusos (**IDS**), el sistema de prevención de intrusos (**IPS**) entre muchas otras herramientas para proveer una mejor seguridad a los sistemas, ya que ahora el acceso no ocurría solo a través de la máquina, sino a través de otras y de la Web.

Por otro lado, es importante hablar de la auditabilidad y trazabilidad, que son propiedades del sistema, relacionados con la infraestructura que son útiles como evidencia para el investigador. La auditabilidad es la capacidad del sistema para registrar los eventos de una acción en particular con el fin de mantener la historia de estos y de realizar un control con mayor facilidad. En cambio, la trazabilidad es la propiedad que tiene un sistema para rastrear o reconstruir relaciones entre diferentes objetos monitorizados.

Es importante resaltar que el administrador debe conocer lo suficiente sobre la infraestructura del sistema para poder colaborar con el caso, ya que su análisis puede facilitar el proceso del investigador forense. Adicionalmente, contar con los rastros y registro de eventos (Auditoría informática) en los sistemas es crucial para el administrador y su infraestructura, no solo porque genera confianza en sus clientes, sino también porque es una buena práctica en términos de seguridad para toda la empresa.

Investigador.

Es un nuevo profesional que actúa como experto, criminalista digital, o informático. Comprende y conoce las nuevas tecnologías de la información. Además, el investigador analiza la inseguridad informática emergente en los sistemas. El perfil del investigador es nuevo y necesario en el contexto abierto informático en el que vivimos. Por lo tanto, es necesario formar personas que puedan trabajar como investigadores en la disciplina emergente de la criminalística digital y el cómputo forense. Estas prácticas emergentes buscan articular las prácticas generales de la criminalística con las evidencias digitales disponibles en una escena del crimen. El trabajo del informático es indagar en las evidencias, analizarlas y evaluarlas para poder decidir cómo estas evidencias pueden ayudar a resolver el caso. Por lo tanto, es ideal que un investigador tenga conocimientos (al menos) sobre las siguientes áreas: justicia criminal, auditoría, administración y operación de tecnologías de Información.

En una investigación informática forense, hay ocho roles principales en un caso: el líder del caso, el propietario del sistema, el asesor legal, el auditor/ingeniero especialista en seguridad de la información, el administrador del sistema, el especialista en informática forense, el analista en informática forense y el fiscal. Usualmente, entre todos estos roles, los informáticos forenses pueden tomar los siguientes cuatro roles:

1. Líder del caso.

Es aquel que planea y organiza todo el proceso de investigación digital. Debe identificar el lugar en donde se realizará la investigación, quienes serán los participantes y el tiempo necesario para esta.

2. Auditor/ingeniero especialista en seguridad de la información.

Conoce el escenario en donde se desarrolla la investigación. Tiene el conocimiento del modelo de seguridad, los usuarios y las acciones que pueden realizar en el respectivo sistema. A partir de sus conocimientos debe entregar información crítica a la investigación.

3. Especialista en informática forense:

Es un criminalista digital que debe identificar los diferentes elementos probatorios informáticos vinculados al caso, determinando la relación entre los elementos y los hechos para descubrir el autor del delito.

4. Analista en informática forense:

Examina en detalle los datos, los elementos informáticos recogidos en la escena del crimen con el fin de extraer toda la información posible y relevante para resolver el caso.

[**Volver al Índice del capítulo 1. Plan de trabajo.**](#)

1.7.6. Retos y riesgos en el análisis forense.

Al estar en un escenario que evoluciona constantemente, cada vez surgen más retos y riesgos en el área de la informática forense. Entre ellos la formación de informáticos forenses, la confiabilidad de las herramientas, la facilidad de la destrucción de las evidencias, las amenazas estratégicas y tácticas que plantea el ciberterrorismo; y las tecnologías emergentes como la nube, las tecnologías móviles, y las redes sociales. Algunos de estos temas se abordarán a continuación:

Formación de informáticos forenses.

Los criminales informáticos son una nueva generación de delincuentes, en este contexto, es necesario desarrollar un nuevo tipo de investigadores: los informáticos forenses. En este momento es un desafío encontrar personas que tengan este perfil, ya que no existen suficientes programas que realicen este tipo de formación. Adicionalmente, en este momento, la mayoría de las personas ignoran la importancia de los informáticos forenses porque no son conscientes de la dimensión del cibercrimen. Usualmente se cree que no es algo tan grave y se le da mayor importancia a otro tipo de crímenes.

Por lo tanto, se deben plantear programas e iniciativas para poder realizar esta formación. Según investigaciones e iniciativas ya realizadas, hay cuatro componentes principales que deben estar presentes en un programa de computación forense o forensia digital: contenido multidisciplinario, ejercicios prácticos, profesores de calidad y ejemplos del mundo real (investigación de Taylor Endicott-Popovsky y Phillips, 2007).

- **Contenido multidisciplinario.**
 - Técnico en informática, conocimiento de criminalística, seguridad y delitos informáticos, entre otros.
- **Ejercicios prácticos en el laboratorio.**
 - Con herramientas tecnológicas forenses, en diferentes niveles de dificultad y variedad de componentes a analizar.
- **Profesores calificados.**
 - Con alto conocimiento en el tema.
- **Ejemplos del mundo real.**
 - Con el fin de dar mayor profundidad al aprendizaje.

Confiabilidad de las herramientas.

Las herramientas existentes disponibles para el cómputo forense presentan otro reto. Las herramientas licenciadas exigen a los investigadores inversiones altas (tanto en hardware, como en software), al adquirirlas y para mantenerlas. Adicionalmente, como las herramientas están avanzando constantemente requieren técnicos y usuarios que estén constantemente aprendiendo las actualizaciones, las modificaciones y los posibles errores. Por otro lado, las herramientas de código abierto son cuestionadas en muchos tribunales por su confiabilidad. Por lo tanto, no se recomiendan a la hora de usarse en una audiencia.

Es por esto que el **NIST** (National Institute of Standards and Technology de Estados Unidos) ha planteado importantes investigaciones para probar y poner reglas para las herramientas del cómputo forense, en su proyecto **NIST** Computer Forensic Tool Testing Program. Las pruebas realizadas serán útiles para cumplir las exigencias del test de Daubert standard, prueba que establece la confiabilidad de las herramientas en computación forense.

[Volver al Índice del capítulo 1. Plan de trabajo.](#)

1.7.7. Herramientas de Análisis Forense.

La siguiente tabla compara cuatro herramientas reconocidas internacionalmente al ser muy completas. Luego, se encuentra una lista más completa de herramientas útiles para la labor del investigador.

Herramienta	Licencia	Imagen	Control de Integridad	Administración del caso
Encase	SI	SI	SI	SI
Forensic Toolkit	SI	SI	SI	SI
WInHex	SI	SI	SI	SI
Sleuth Kit	NO	SI	SI	SI

- Air (Forensics Imaging GUI).
- Autopsy (Forensics Browser for Sleuth Kit) Cryptcat (Command Line) Deep Freeze.
- Dcfldd (DD Imaging Tool command line tool and also works with AIR).
- Dumpzilla (Forensics Browser: Firefox, Iceweasel and Seamonkey).
- Encase: \url{https://www.guidancesoftware.com/encase-forensic?cmpid=nav_r}.
- Exif Viewer (Visor de metadatos en imágenes).
- Faces.
- Foremost (Data Carver command line tool).
- Forensik Toolkit: \url{https://accessdata.com/products-services/forensic-toolkit-ftk}.
- Helix.
- Hetman software (Recuperador de datos borrados por los criminales).
- Hiren's boot.
- Md5deep (MD5 Hashing Program).
- Metashield Analyser Online (Analizador de metadatos online).
- Mini XP.
- NTFS-Tools.
- Netcat (Command Line).
- Net resident.
- NetFlow.
- Py-Flag (Forensics Browser).
- Qtparted (GUI Partitioning Tool).
- R-Studio Emergency (Bootable Recovery media Maker).
- R-Studio Network Edition.
- R-Studio RS Agent.
- Regviewer (Windows Registry).
- Sleuth Kit (Forensics Kit. Command Line): \url{https://www.sleuthkit.org/}.
- Snort.
- Viewer.
- Volatility (Reconstrucción y análisis de memoria RAM).
- X-Ways Forensics.
- X-Ways WinHex \url{https://www.x-ways.net/winhex/}.
- X-Ways WinTrace.

Herramientas para el análisis de discos duros:

- AccessData Forensic ToolKit (FTK).
- Guidance Software EnCase.
- Kit Electrónico de Transferencia de datos.

Herramientas para el análisis de correos electrónicos:

- Paraben.
- AccessData Forensic ToolKit (FTK).

Herramientas para el análisis de dispositivos móviles:

- Cellebrite UFED Touch 2, Physical Analyzer.
- AccessData Mobile Phone Examiner Plus (MPE+).

Herramientas para el análisis de redes:

- E-Detective - Decision Computer Group.
- SilentRunner - AccessData.
- NetworkMiner.
- Nerviness Investigator.

Herramientas para filtrar y monitorear el tráfico de una red tanto interna como a internet:

- Tcpdump.
- USBDevview.
- SilentRunner - AccessData.
- Wireshark.

1.7. Referencia 011.[Volver al Índice del capítulo 1. Plan de trabajo.](#)[Volver al Índice General.](#)

2. Extremos del análisis y previsión de pruebas técnicas.

Índice del capítulo 2. Extremos del análisis y previsión de pruebas técnicas.

- [2.0. Introducción al capítulo 2. Extremos del análisis y previsión de pruebas técnicas.](#)
- [2.1. Propuesta de extremos.](#)
- [2.2. Previsión de pruebas técnicas.](#)

[Volver al Índice General.](#)

2.0. Introducción al capítulo 2. Extremos del análisis y previsión de pruebas técnicas.

En la era digital actual, la capacidad de llevar a cabo análisis forenses en ordenadores se ha convertido en una competencia crítica dentro del ámbito de la investigación criminal. El análisis forense informático permite a los investigadores descubrir, preservar y analizar datos en dispositivos electrónicos que pueden ser críticos para resolver delitos. Este capítulo se dedica al estudio meticuloso de los métodos y prácticas estándar en la computación forense, con un enfoque específico en la adquisición y análisis de datos de la memoria RAM y discos duros. Se expondrá la metodología utilizada para garantizar la **integridad** de la evidencia y se ilustrarán los desafíos asociados a la recolección y el análisis de datos digitales.

Con el avance de la tecnología, los investigadores forenses enfrentan la dualidad de oportunidades y desafíos. Por un lado, las herramientas modernas ofrecen capacidades sin precedentes para recuperar y analizar datos; por otro lado, la creciente sofisticación del software y hardware supone nuevos niveles de complejidad y la necesidad de constante actualización en conocimientos y técnicas. Este capítulo también contempla la noción de deuda técnica asociada a la utilización de herramientas y sistemas operativos en la investigación forense, reconociendo la importancia de mantener un enfoque crítico hacia las herramientas utilizadas.

La documentación y control de versiones son aspectos cruciales en cualquier proyecto de investigación y desarrollo, más aún en el ámbito forense digital, donde la transparencia y reproducibilidad son fundamentales. Se detallará el uso del repositorio de **Github** (<https://github.com/jrodg85/TFM-ANALISIS-FORENSE>) para la documentación del TFM y el control de versiones aplicado al proceso de análisis forense. Se discutirá la relevancia de la colaboración y el seguimiento preciso de cambios en el código y documentos relacionados con el proyecto.

Finalmente, no se puede ignorar el papel fundamental que juega el acceso a recursos online en la actualización constante y el acceso a información relevante y actualizada en el campo de la forense digital. La Internet es una fuente inagotable de conocimiento, pero también presenta riesgos que deben ser gestionados con prudencia. En resumen, este capítulo traza el panorama del análisis forense en ordenadores, describiendo las herramientas y metodologías utilizadas, así como las mejores prácticas en la documentación y gestión de la información digital en investigaciones forenses.

Esta introducción proporciona una vista general y establece las expectativas para el contenido que seguirá, preparando al lector para los detalles técnicos y metodológicos que se presentarán en el capítulo.

[Volver al Índice del capítulo 2. Extremos del análisis...](#)

[Volver al Índice General.](#)

2.1. Propuesta de extremos.

La presente investigación tiene como propósito fundamental el establecimiento de un marco metodológico para el análisis forense de ordenadores, específicamente orientado hacia la identificación, recolección y análisis de evidencias digitales que puedan ser presentadas en un entorno judicial. A continuación, se delinean los extremos de esta propuesta:

Objeto de Estudio:

- La investigación se centrará exclusivamente en el análisis forense del material facilitado para el desarrollo de la asignatura por parte del profesorado de la asignatura.
- Se realizará una breve indicación sobre la aplicación utilizada con cada uno de los objetivos del presente TFM.

Alcance metodológico:

- La validación de la **integridad** de la evidencia se hará mediante el uso de funciones **hash** estándar.
- Se examinarán las metodologías para el análisis de la memoria volátil y no volátil.

Limitaciones:

- La validación de la **integridad** de la evidencia se hará mediante el uso de funciones **hash** estándar.
- Se examinarán las metodologías para el análisis de la memoria volátil y no volátil.

Exclusiones:

- No se utilizará material de análisis que no sea el proporcionado por la asignatura.

[Volver al Índice del capítulo 2. Extremos del análisis...](#)

[Volver al Índice General.](#)

2.2. Previsión de pruebas técnicas.

Pruebas técnicas:

- El propósito de estas pruebas técnicas es lo indicado en el apartado de problema a resolver del presente Trabajo de fin de master
 - Solventar las necesidades del gerente de la empresa mediante el análisis forense del disco duro y la captura de memoria de un ordenador personal, en un caso real con un sistema virtualizado.
 - Posible vinculación con una presunta conducta delictiva real.
- Importancia de las pruebas para validar la hipótesis y objetivos de investigación.
 - La posible imputación de los hechos ocurridos y tomar posibles medidas legales contra el autor unívoco de la acción detectada.

Marco metodológico de las pruebas:

- Las pruebas que se realizarán serán una investigación y un estudio temporal de los hechos ocurridos dentro del servidor.
- Se emplearán herramientas de análisis forense en sus distintos sistemas operativos (Linux/Windows) para su detección.
- se tratará de arrancar el sistema virtualizado para posible **carving** de la información del disco duro por posible eliminación de pruebas por parte del posible infractor.
- La planificación de las pruebas ha quedado detallado en la sección "planificación temporal de las tareas".

Criterios de éxito de las pruebas:

- Análisis de los incidentes ocurridos con una justificación probatoria del mismo.
- Realización de un análisis de seguridad de las vulnerabilidades detectadas y una vía de mitigación de los mismos.

Cronograma de pruebas:

- El cronograma de las pruebas ha quedado detallado en la sección "planificación temporal de las tareas".
- Hitos importantes, fechas de entrega de las PEC.

[Volver al Índice del capítulo 2. Extremos del análisis...](#)

[Volver al Índice General.](#)

3. Análisis de la memoria RAM.

Índice del capítulo 3. Análisis de la memoria RAM.

[Volver al Índice General.](#)

3.0. Introducción al capítulo 3. Análisis de la memoria RAM.

El análisis forense de la memoria RAM es un componente crítico en la investigación digital, pues permite a los analistas extraer información valiosa que no persiste una vez que el dispositivo se apaga. Esta volatilidad hace que la memoria RAM sea una fuente de evidencia esencial, especialmente en casos donde los procesos activos y la información en tránsito son relevantes para el caso. El presente capítulo detalla un enfoque metodológico estructurado para examinar de manera exhaustiva el contenido de la memoria RAM capturada de un sistema informático, con el objetivo de identificar y analizar aspectos críticos que contribuyan a la investigación.

Las acciones específicas que se abordarán son las siguientes:

1. Comprobación del MD5:

- Iniciaremos con la verificación de la **integridad** del volcado de la memoria RAM mediante el cálculo de su suma de verificación MD5. Este paso es fundamental para asegurar que los datos analizados no han sido alterados desde el momento de su adquisición, garantizando así la **cadena de custodia** digital.

2. Identificación del Sistema Operativo:

- Aunque ya intuyamos, por el apartado anterior datos básicos del Sistema operativo, es vital determinar la versión y configuración del sistema operativo en uso, ya que esto influirá en la interpretación de los datos y en la selección de las herramientas de análisis adecuadas.

3. Búsqueda de Datos de Interés:

- Seguiremos con la inspección minuciosa del contenido de la memoria para identificar información potencialmente relevante para el caso. Esto incluye, pero no se limita a, datos residuales de aplicaciones, fragmentos de comunicaciones y elementos que puedan ser reconstruidos para obtener evidencia. Servirá para tener una previsión de por donde dirigir el estudio de todo el análisis forense.

4. Búsqueda de Procesos en Funcionamiento de Interés:

- Un punto focal de nuestra investigación será el examen de los procesos activos en el momento de la captura de la memoria. Esta inspección nos permitirá comprender mejor el estado del sistema antes del apagado o la hibernación.

5. Análisis y Extracción de Procesos Sospechosos:

- Finalmente, nos concentraremos en reconstruir y examinar las conexiones de red activas y pasivas. El objetivo es identificar patrones de tráfico inusuales o conexiones que puedan indicar comunicación con servidores de comando y control, exfiltración de datos o cualquier otra actividad que se considere sospechosa.

El resultado de este análisis exhaustivo proporcionará una comprensión detallada de lo que estaba ocurriendo en el sistema en el momento de la captura de la memoria. Esta información es invaluable para formar una imagen completa de los eventos bajo investigación y para establecer hechos concretos que puedan ser presentados como evidencia en un entorno judicial.

3.1. Acciones previas al análisis de la memoria RAM.

En el presente TFM, se nos ha proporcionado a los alumnos un archivo de captura de memoria RAM .mem. Por otro lado, se nos ha proporcionado los resúmenes o **hash** en MD5 y en SHA1 de los archivos tal y como se muestra en la siguiente imagen.

3.1 Imagen 001.

Como podemos ver, los **hash** resúmenes del archivo de la ram, tenemos los siguientes hashes en MD5 y en SHA1:

- **MD5:** 75a99b57032aa34ba19042ed85db273f
- **SHA1:** cc1fad2af321b8c2ddf0103986e3b344eb8f2cc8

El **hash** tal y como se indica en los apuntes de la asignatura, en el módulo de Fases y metodología del análisis forense, durante la adquisición de evidencias digitales dice lo siguiente:

Una vez generada la copia o clon del soporte original, el programa o el dispositivo hardware empleado en este proceso realiza el cálculo del **CRC** o del valor **hash** del soporte original y del destino, con la finalidad de garantizar que los dos son idénticos y que la copia se ha producido sin ningún error. Este cálculo puede realizarse sobre todo el conjunto de información contenida en el soporte original, o bien emplear solamente un conjunto de ficheros del total.

A su vez, en el glosario de términos la definición de **hash** es la siguiente:

Es una función matemática unidireccional que resume un mensaje de tamaño variable (por ejemplo, un archivo), en una representación de tamaño fijo. Es poco probable que dos ficheros distintos tengan la misma representación **hash**, lo cual significa que este valor puede utilizarse a efectos de comprobación de la **integridad** de un archivo (o de un sistema entero). Las funciones **hash** más conocidas son MD5 y SHA-1.

Una vez descargado el archivo de captura de la memoria RAM, procedemos a usar PowerShell para determinar el **hash** del archivo. Para ello usamos el comando "Get-FileHash [Argumento] -Algorithm MD5". En nuestro caso hemos usado los siguientes comandos:

4.1 Comando 001.

4.1 Comando 002.

Se puede observar en la siguiente imagen la respuesta de PowerShell de los hashes de MD5 y SHA1.

3.1. Imagen 002.

Como conclusión podemos verificar que la **integridad** de la copia facilitada para realizar el TFM no ha sido vulnerada.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

[Volver al Índice General.](#)

3.2. Sistema Operativo de la memoria RAM analizada.

Procedemos a preparar una VM con Ubuntu 22.04, el cual le instalamos el volatility según en el siguiente enlace. Haga click en la imagen para acceder al enlace:

3.2. Video 001

A continuación procedemos a buscar el perfil con volatility con el comando `imageinfo`.

3.2 Imagen 001

Como se puede observar en la imagen anterior, no hemos llegado a encontrar un perfil concreto con `imageinfo`, eso se debe a que el perfil creado no es el que se encuentra dentro de las conocidas en la base de datos de volatility. Por ello procedemos a buscar dentro de la memoria RAM un string que tenga la cadena de texto "linux version". para ello ejecutamos el comando `strings Server_{RAM}.mem \mid grep -Ei linux version \mid uniq`.

3.2 Imagen 002.

Podemos observar en la imagen anterior que el sistema operativo que utiliza en nuestro caso es un sistema operativo Linux para Amazon Web Service, concretamente el sistema operativo es el **4.15.0-1021.21-aws 4.15.18**. Esta versión de Linux, es muy usada para las instancias de Amazon Web Services.

Como no tenemos el perfil cargado dentro de volatility, nos va a tocar hacer la tarea de cargar un perfil de este Sistema operativo para poder seguir ejecutando la aplicación volatility.

Buscando en google **linux version 4.15.0-1021.21-aws volatility**, nos encontramos solo un enlace en internet, el cual es <https://lists.ubuntu.com/archives/bionic-changes/2018-August/016183.html>, con ello nos encontrábamos con algo que ya se intuía previamente, y es que la versión del server de **AWS**, es basada en un ubuntu 18.04, ya que la fecha que indica 4.15.18 es una fecha en tipo "d.mm.aa".

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

[Volver al Índice General.](#)

3.3. Creación de perfil para volatility.

3.3.0. Introducción de creación de perfil de volatility.

Crear un perfil de volatility es fundamental para poder extraer la información de los datos de la ram.

En el repositorio de github de volatility podemos observar perfiles relativos a windows, pero ninguno relativo al sistema operativo linux. Si ejecutamos el comando `sudo python2.7 vol.py --info` tenemos la siguiente respuesta relativo a perfiles:

3.3.0. Comando 001.

Como ya hemos observado en la sección anterior, el kernel del la memoria RAM a analizar es del tipo `linux version 4.15.0-1021.21-aws`, además, se puede en el comando citado que este perfil no aparece en volatility por defecto , basándome en las páginas web de referencias 12 y 13, procederé a crear un perfil adaptado para esta memoria RAM. Estas acciones, deben de ser una práctica común para capturas de memoria de sistemas operativos del tipo Linux, por lo que se ha considerado recomendable introducirlo en el cuerpo del TFM, además que ya forma parte del trabajo de investigación.

[3.3.0. Referencia 012.](#)

[3.3.0. Referencia 013.](#)

[3.3.0. Referencia 014.](#)

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.3.1. Creación de la máquina virtual, búsqueda en cache e instalación del kernel relativo al perfil a crear.

Vamos crear una VM para generar una base con el mismo kernel que el servidor auditado. Lo configuraremos según la siguiente imagen, finalmente procederemos a su arranque para su instalación.

3.3.1. Imagen 001.

Procedemos a ejecutar el comando `hostnamectl` para ver las características que ahora mismo tenemos instalada en la VM.

3.3.1. Imagen 002.

Como se observa en la imagen anterior, este servidor utiliza el kernel ***Linux 4.15.0-213-generic***, por lo que para obtener el perfil de la RAM, tendremos que instalar un kernel distinto.

Procedemos a arrancar la VM, una vez realizado el login, procedemos a ejecutar el comando `sudo apt-cache search linux-image | grep 4.15.0-1021`.

Este comando realiza dos acciones, por un lado `sudo apt-cache search linux-image`, y por otro `grep 4.15.0-1021`. Gracias al "pipe" o "|", pasaremos la respuesta del primera acción como entrada de la segunda acción.. Es una parte fundamental de la filosofía de Unix que permite a los usuarios combinar múltiples comandos sencillos para realizar tareas más complejas. En nuestro caso:

`sudo apt-cache search linux-image`.

- Esta parte del comando busca en la caché de APT (Advanced Package Tool) todos los paquetes cuyos nombres o descripciones contienen la cadena "linux-image". Los paquetes "linux-image" generalmente se refieren a imágenes del kernel de Linux para diferentes versiones y configuraciones.

| grep 4.15.0-1021.

- La salida del primer comando se canaliza () al comando grep, que filtra y muestra solo las líneas que contienen la cadena "4.15.0-1021". En este contexto, "4.15.0-1021" probablemente se refiere a una versión específica del kernel de Linux.

Al combinar estos dos comandos, `sudo apt-cache search linux-image | grep 4.15.0-1021-aws` efectivamente busca y lista todas las versiones de las imágenes del kernel de Linux disponibles en los repositorios que coincidan con la versión específica "4.15.0-1021". Este comando es útil para identificar si una versión específica del kernel está disponible para la instalación o actualización en el sistema.

Se adjunta pantallazo de la respuesta por parte de la consola.

3.3.1. Imagen 003.

Como podemos observar en la imagen observada, el primer kernel que buscamos exactamente aparece como `linux-image-4.15.0-1021-aws`, esto significa que es un kernel disponible para ser instalado en el sistema operativo, por lo que procederemos a su instalación.

A continuación, procedemos a instalarla en el sistema, para ello ejecutamos el comando `sudo apt-get install linux-image-4.15.0-1021-aws`.

3.3.1. Imagen 004.

El comando `sudo apt-get install linux-image-4.15.0-2021-aws` en Ubuntu o sistemas basados en Debian, se utiliza para instalar una versión específica del kernel de Linux, diseñada para ambientes Amazon Web Services (**AWS**). Al usar `sudo`, el comando se ejecuta con privilegios de superusuario, necesarios para instalar software a nivel de sistema. `apt-get install` es parte del sistema de gestión de paquetes APT, y se usa aquí para instalar el paquete `linux-image-4.15.0-2021-aws`. Este paquete contiene una imagen del kernel de Linux, la cual está optimizada para correr en servidores **AWS**, indicando que este kernel podría tener configuraciones o parches específicos para un rendimiento mejorado o características adicionales en esa plataforma. **Al instalar un nuevo kernel, es importante reiniciar el sistema para que empiece a usar esta nueva versión.** Para comprobar lo mencionado anteriormente, procederemos a realizar de nuevo el comando `hostnamectl`.

3.3.1. Imagen 005.

Como hemos indicado anteriormente, es necesario reiniciar el sistema para que el kernel instalado se utilice en el Sistema operativo, procederemos a ejecutar el comando `sudo reboot now` para realizar esta acción.

3.3.1. Imagen 006.

Una vez reiniciado el sistema, procedemos a ejecutar el comando `hostnamectl` o `uname - r` para comprobar que el comando se ha ejecutado correctamente.

3.3.1. Imagen 007.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.3.2. Instalación y creación del perfil de volatility.

Una vez comprobado, procederemos a la instalación de volatility en el servidor de ubuntu.

Primero de todo instalaremos los paquetes relativos a `dwarfdump` ya que el servidor no los tiene instalado por defecto.

3.3.2. Imagen 001.

Seguiremos los pasos ya indicados en el [Apartado 3.2](#):

3.3.2. Video 001.

3.3.2. Imagen 002.

Ahora, se procede a instalar dwarfdum, para poder hacer el `modules.dwarf` que mas adelante se explica. Una vez hemos realizado la instalación procedemos a crear el perfil de volatility.

Para ello entraremos en la carpeta `/home/jrodg85/volatility/tools/linux`, una vez allí dentro ejecutaremos el comando `make`. Con ello, generaremos el archivo `modules.dwarf`. Se puede ver en las siguientes imágenes como se ha generado tras ejecutar el comando make.

3.3.2. Imagen 003.

3.3.2. Imagen 004.

Ahora procederemos a nombrar el perfil de volatility para ello vamos a generar un archivo zip, este archivo, como norma general, usaremos los valores de `lsb_release -si` y `uname -r`. De esta manera nombraremos de manera correcta el perfil de volatility para después no tengamos problemas al importarlo dentro de la máquina donde estamos realizando la investigación.

3.3.2. Imagen 005.

Este archivo zip, debe de contener los dos archivos necesarios de perfil:

modules.dwarf

- Este archivo se genera a partir de los módulos del kernel de Linux y contiene información sobre las estructuras de datos del kernel. Es creado usando, en nuestro caso, la herramienta dwarfdump sobre módulos del kernel compilados con símbolos de depuración (debugging symbols). El archivo `module.dwarf` es crucial porque contiene los offsets y las definiciones de las estructuras de datos internas del kernel, lo que permite a Volatility entender cómo están organizados los datos en el volcado de memoria.

/boot/System.map-4.15.0-1021-aws

- Este archivo es un mapa de símbolos del kernel. Proporciona una lista de todas las funciones y variables en el kernel, junto con sus direcciones de memoria. Cada versión del kernel de Linux tiene su propio archivo `System.map`, y el archivo específico para una versión dada del kernel (en tu caso, `4.15.0-1021-aws`) es necesario para analizar un volcado de memoria tomado de un sistema que ejecuta esa versión del kernel. Este archivo es esencial para que Volatility pueda mapear las direcciones de memoria en el volcado a nombres de funciones y variables específicas en el kernel.

Para la generación del perfil, procederemos, desde `/home/jrodg85` a ejecutar el comando para crear un archivo .zip `sudo zip linux$(lsb_release -si)_$(uname -r)_profile.zip /home/jrodg85/volatility/tools/linux/module.dwarf /boot/System.map-4.15.0-1021-aws`

3.3.2. Imagen 006.

3.3.2. Imagen 007.

Para una aclaración de cualquier duda relativo a la elaboración de la elaboración de este servidor y las acciones realizadas en ella, se ha extraído el history al completo para que cualquier persona pueda realizar los mismos pasos que he realizado para la creación del perfil.

3.3.2. comando 001

Una vez creado el perfil, tenemos que sacar el perfil del servidor para después pegarlo dentro de la máquina una donde realizaremos el análisis. para ello procederemos a montar un usb dentro del servidor del ubuntu, posteriormente copiamos el archivo,

`/home/jrodg85/volatility/volatility/plugins/overlays/linuxUbuntu_4.15.0-1021-aws_profile.zip`, y lo pegamos en el **USB**. En nuestro caso, hemos el **USB** lo hemos montado en `/home/jrodg85/usb/`

3.3.2. Imagen 008.

Posteriormente, procedemos a insertar en la VM de Ubuntu con Volatility en la carpeta en la carpeta `/home/jrodg85/volatility/volatility/plugins/overlays/linux` tal y como se muestra en la siguiente imagen.

3.3.2. Imagen 009.

para comprobar que esta correctamente creado el perfil procedemos a ejecutar el comando `sudo python2.7 vol.py --info`, donde se podrá observar que se ha creado correctamente el perfil.

3.3.2. Imagen 010.

Para probar el correcto funcionamiento del perfil, procederemos a hacer la captura de la cpu con el siguiente comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_cpuinfo`. Esta información la usaremos mas adelante, en este caso es solo para prueba.

3.3.2. Imagen 011.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

[Volver al Índice General.](#)

3.4. Datos de interés de la captura de la memoria RAM.

3.4.0. Introducción de datos de interés de la captura de la memoria RAM.

En el anexo Creación perfil ubuntu **AWS**, hemos realizado una guía para crear el perfil de Linux **AWS** que detectado durante el análisis del sistema operativo.

Una vez creado el perfil de linuxUbuntu_4.15.0-1021-aws procederemos a hacer un pslist para listar todas las aplicaciones que estaban ejecutándose en el momento de la captura.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.4.1. Linux_cpuinfo.

Para comprobar que el perfil funciona, vamos a comenzar a comprobar cual es el **CPU** que usa el sistema.

Para ello, situados en `/home/jrodg85/volatility$` ejecutaremos `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_cpuinfo.`

3.4.1. Imagen 001.

Al comprobar que el perfil funciona, obtenemos que solo hay un procesador de marca GenuineIntel modelo Intel(R) Xeon(R) **CPU** E5-2676 v3 que tiene una frecuencia de 2.4Ghz.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.4.2. Linux_banner.

Otro dato de interés es la versión del kernel y la información de distribución de Linux. Esto es útil para identificar la versión específica del sistema operativo que se estaba ejecutando. Para ello se ejecuta el comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_banner`, dando la siguiente imagen como respuesta

3.4.2. Imagen 001.

Un análisis de Información del Kernel de Linux es la siguiente:

- Versión del Kernel.
 - La captura de memoria analizada corresponde a un sistema que ejecuta la versión 4.15.0-1021-aws del kernel de Linux. Este dato era ya conocido en el TFM.
- Ambiente **AWS**.
 - El sufijo **aws** sugiere que esta versión del kernel está optimizada o diseñada para ejecutarse en Amazon Web Services, una plataforma de cloud computing.
- Construcción y Compilador.
 - La captura incluye detalles de la compilación del kernel, como el compilador utilizado (gcc version 7.3.0) y la configuración específica de Ubuntu (Ubuntu 7.3.0-16ubuntu3).
- Número de Compilación y Fecha.
 - Se muestra el número de compilación (#21-Ubuntu SMP) y la fecha (Tue Aug 28 10:23:07 UTC 2018), que proporcionan un contexto sobre cuándo y cómo se construyó esta versión del kernel.

Esta respuesta básicamente te indica la versión exacta del sistema operativo Linux que estaba corriendo en la máquina de la cual se tomó la captura de memoria. Es un paso esencial en el análisis forense, ya que te permite seleccionar o validar el perfil correcto en Volatility para un análisis más detallado y preciso de la captura de memoria.

Aunque este dato ya lo sabíamos anteriormente, la salida muestra que la versión del kernel es 4.15.0-1021-aws. Esta es una versión específica para las instancias de Ubuntu en **AWS**. **La fecha de compilación (Tue Aug 28 10:23:07 UTC 2018)**.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.4.3. Linux_mount.

A continuación, se va a proceder a enumerar los sistemas de archivos montados en el momento del volcado de memoria. Esto puede proporcionar información sobre las particiones y los sistemas de archivos utilizados. Para ello, ejecutaremos el comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_mount`. Se procede a adjuntar una captura de pantalla del comando y del comando utilizado en este caso. Además se ha elaborado una tabla detallada en el comando para su comprensión.

3.4.3. Imagen 001.

3.4.3. Comando 001.

Teniendo en cuenta que es un servidor con un kernel de Amazon Web Services. Se puede realizar el siguiente análisis.

- cgroup (/sys/fs/cgroup/rdma):
 - Usado para control de recursos y aislamiento de grupos de procesos. Las opciones indican un enfoque en seguridad y rendimiento.
- tmpfs (/sys/fs/cgroup):
 - Sistema de archivos temporal en memoria, utilizado para almacenamiento de corta duración y rápido acceso.
- /dev/xvda1 (/):
 - Sistema de archivos principal, ext4 proporciona robustez y mejor manejo de grandes archivos.
- proc (/bus):
 - Usado para acceder a información del sistema y procesos en ejecución.
- pstore (/sys/fs/pstore):
 - Almacenamiento persistente para registros del núcleo y datos de diagnóstico.
- fusectl (/sys/fs/fuse/connections):
 - Interfaz para sistemas de archivos FUSE, permite a usuarios no privilegiados crear sus propios sistemas de archivos.
- lxcfs (/var/lib/lxcfs):
 - Proporciona un sistema de archivos virtual para contenedores LXC.
- /dev/loop0 (/snap/core/5328):
 - Usado para montar imágenes de Snap, squashfs es eficiente en espacio y de solo lectura.
- udev (/dev):
 - Sistema de archivos para dispositivos, gestionado dinámicamente.
- cgroup (/sys/fs/cgroup/unified):
 - Nueva versión de cgroup para mejor gestión de recursos.

Los restantes puntos de montaje siguen patrones similares en cuanto a tipos y opciones, enfocándose en la seguridad (nosuid, nodev, noexec), rendimiento (relatime), y tipo de acceso (ro, rw). Los sistemas de archivos como tmpfs, squashfs, y cgroup son comunes en entornos Linux y son utilizados para propósitos específicos como almacenamiento temporal, montaje de paquetes de software, y gestión de recursos del sistema.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.4.4. Linux_memmap.

Se procede ahora a realizar un mapa de memoria del sistema, para así, entender cómo está organizada la memoria en el servidor. Para ello ejecutaremos el comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_memmap > /home/jrodg85/informe-memmap.txt`. Lo hemos pasado la salida a un archivo .txt debido a la gran cantidad de datos que maneja este comando (375 Mb).

3.4.4. Imagen 001.

Tras un trabajo de limpieza de datos, de un archivo de 4519734 líneas a solo 200 líneas, y posteriormente a 109 líneas, ya que las direcciones de memoria última de cada aplicación era la misma, por lo que también ha sido desecharido, podemos así obtener de esta manera todos los procesos que estaban ocurriendo dentro del servidor.

3.4.4. Comando 001.

3.3.4. Referencia 015.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.4.5. Linux_iomem.

A continuación, se procede a obtener información relativa a la memoria de entrada/salida (I/O) en un sistema Linux. para ello usaremos el comando `linux_iomem` Este comando es similar a la herramienta iomem en Linux, la cual proporciona información sobre el mapeo de la memoria de entrada/salida del kernel. El comando `linux_iomem` en Volatility analiza un volcado de memoria de un sistema Linux y extrae información sobre cómo el kernel ha mapeado la memoria física para dispositivos de entrada/salida. Por lo anteriormente expuesto y ya realizado en las anteriores secciones, se colige que el comando a utilizar es `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem'` `linux_iomem`. Se adjunta en el TFM pantallazo del mismo y captura del comando, localizados en los siguientes enlaces.

3.4.5. Imagen 001.

3.4.5. Comando 001.

Un pequeño análisis explicativo de la respuesta del comando iomem es la siguiente:

System RAM (0x1000 - 0x9DFF y 0x100000 - 0x3FFFFFF).

Estas áreas representan la memoria RAM del sistema. La primera sección es una pequeña porción al inicio de la memoria, y la segunda es la parte principal de la memoria RAM.

Reserved (0x9E000 - 0x9FFFF y 0xE0000 - 0xFFFFF).

Estas son áreas de memoria reservadas, posiblemente por el BIOS o por el sistema operativo para funciones específicas.

PCI Bus 0000:00 (0xA0000 - 0xBFFFF y 0xF0000000 - 0xFBFFFFFF).

Estas áreas están asignadas a los buses PCI del sistema, utilizadas para la comunicación con dispositivos de hardware conectados a través de estos buses.

Video ROM (0xC0000 - 0xC8BFF).

Esta es la memoria reservada para el ROM de la tarjeta de video, que contiene el firmware básico para la tarjeta gráfica.

System ROM (0xF0000 - 0xFFFFF).

Esta sección es para el ROM del sistema, donde reside el BIOS o firmware básico de la máquina.

Kernel code, data, and bss (0x31C00000 - 0x33516FFF).

Estas áreas son específicas para el núcleo del sistema operativo, incluyendo el código del kernel, los datos y el segmento 'bss' (bloque de inicio sin asignar), que se utiliza para las variables globales no inicializadas.

IOAPIC, HPET, Local APIC (0xFEC00000 - 0xFEE00FFF).

Estos son componentes de hardware relacionados con la gestión de interrupciones y temporizadores de alta precisión.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.4.6. Linux_dmesg.

Se procede a recabar una información mas completa de la memoria RAM, hablamos del comando **linux_dmesg**, este comando puede sernos de gran utilidad por las siguientes razones:

1. Extracción de Mensajes del Kernel.

Linux_dmesg se utiliza para extraer los mensajes del buffer de registro del kernel, conocido como dmesg, de un volcado de memoria de Linux. Este buffer contiene mensajes de diagnóstico y de depuración que son emitidos por el kernel de Linux.

Los mensajes extraídos pueden proporcionar información valiosa durante un análisis forense. Pueden incluir detalles sobre el hardware del sistema, errores del kernel, información de carga de módulos del kernel y otros mensajes de diagnóstico que son útiles para entender el estado y las acciones del sistema en el momento del volcado de la memoria.

2. Investigación de Incidentes de Seguridad.

linux_dmesg puede ayudar a identificar actividades sospechosas o maliciosas, como la carga de módulos del kernel no autorizados o errores relacionados con intentos de explotación.

3. Uso en Conjunto con Otros Comandos.

A menudo, **linux_dmesg** se utiliza en combinación con otros comandos de Volatility diseñados para el análisis de sistemas Linux, como **linux_pslist** para listar procesos, **linux_netstat** para ver conexiones de red, entre otros, proporcionando una vista más completa del estado del sistema. En los próximos apartados del TFM, realizaremos estos comandos para obtener una visión global de lo ocurrido.

Por tanto en este caso, como muy presumiblemente va a resultar un comando bastante extenso, ejecutaremos el comando el cual la salida se extraerá a un documento de texto para ser integrado en el anexo de [Extracto de comandos utilizados..](#) El comando a utilizar es **sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_dmesg > /home/jrodg85/informe-linux_dmesg.txt**. Se adjunta imagen y comando del mismo

3.4.6. Imagen 001.

3.4.6. Comando 001.

3.4.6. Referencia 016.

Un resumen de interés para el análisis forense de estos datos es la siguiente:

3.4.6. Comando 002.

3.4.6. Referencia 017.

Los puntos destacables son los siguientes, algunos de estos datos se pueden encontrar con mayor detalle en el comando citado anteriormente.

1. Establecimiento del tiempo origen de tiempos donde el 28 de Agosto de 2018 a las 10:23:07 UTC el cual arranca el servidor. Se considera que el tiempo [0.0] es el origen de tiempos del sistema marcado en microsegundos.
 - o Linux version 4.15.0-1021-aws (buildd@lcy01-amd64-001) (gcc version 7.3.0 (Ubuntu 7.3.0-16ubuntu3)) #21-Ubuntu SMP Tue Aug 28 10:23:07 UTC 2018 (Ubuntu 4.15.0-1021.21-aws 4.15.18)
2. Se descarta información relativo al arranque del servidor. Se mantiene la relevante la cual se explica a continuación.
 - o El Servidor es una Máquina virtual.
 - Hypervisor detected: Xen HVM.
 - o Memoria disponible y su distribución.
 - Memory: 983488K/1048180K available (12300K kernel code, 2391K rwdta, 3908K rodata, 2372K init, 2376K bss, 64692K reserved, 0K cma-reserved).
 - o Seguridad, ver referencia 17.
 - selinux.
 - SMACK64.
 - SMACK64EXEC.
 - SMACK64TRANSMUTE.
 - SMACK64MMAP.
 - apparmor.
 - ima.
 - capability.
3. EL RCT no coincide con el timestamp!!!, puede ser una coordinación de tiempos. el 28 de agosto de 2018 a las 10:27:31 UTC.
 - o RTC time: 12:04:38, date: 12/21/18
4. Reinicio del Servidor. 1 de septiembre de 2018 a las 09:53:22 UTC.
5. Reinicio del servicio Journal 1 de septiembre de 2018 a las 09:59:10 UTC.
6. Inicio de denegación de servicio SQL 3 de mayo de 2019 a las 20:10:29 UTC.
7. Denegación de servicio SQL, 7 de mayo de 2019 a las 05:53:01 UTC.
8. Denegación de servicio SQL, 10 de mayo de 2019 a las 06:39:15.104327 UTC.
9. Denegación de servicio SQL, 12 de mayo de 2019 a las 12:02:32.671468 UTC.
10. 13 de mayo de 2019 a las 05:27:58 UTC, posible brecha y entrada no deseada en el sistema a través de un ataque SQL. Se reemplaza un perfil en el sistema.
11. Posible ataque al servidor el 13 de mayo de 2019 a las 07:20:17 UTC por SQL.
12. Posible ataque al servidor el 14 de mayo de 2019 a las 21:55:10 UTC por SQL.
13. 19 de junio de 2019 a las 20:51:55.627714 UTC. Posible parcheo de la vulnerabilidad.

3.4.6. Linux_bash.

Por último y no menos importante, ya que considero que es un comando fundamental para saber qué acciones se han realizado a través de la terminal, es el comando `linux_bash`, ya que permite ver qué se ha realizado exactamente dentro del sistema, no obtendremos sus respuestas, pero se sabe qué comandos se han ejecutado, y por tanto sus consecuencias. El comando a utilizar en este caso es `sudo python2.7 vol.py --profile=LinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_bash`. En este caso se adjunta una captura completa de los comandos ejecutados.

3.4.7. Comando 001.

Relativo al código mostrado, cabe destacar que las fechas que marca la maquina como las calculadas en el apartado anterior, son totalmente erróneas entre sí, ya que por `linux_dsmeg` calculamos fechas de mayo de 2019, sin embargo este comando data de 3 de enero de 2019, por otro lado, no creo que una persona humana, bot o proceso automatizado, escriba tan de seguido con esas fechas que marca el comando. Por lo que en principio parece descartable las fechas que indica este comando. Cabe destacar que posiblemente haya comandos del administrador relativos a la configuración y del atacante. A continuación se detallan comando importantes de las acciones realizadas que pueden afectar a la seguridad.

3.4.7. Referencia 018.

- Intenta una conexión con el usuario root al servidor [MySQL](#).
- Se sitúa dentro del directorio de [Apache](#).
- Edita el fichero debian.cnf del servidor [MySQL](#).
- Muestra todos los procesos referentes a [MySQL](#).
- Muestra las últimas líneas del archivo Access.log.1.
- se mueve de directorio situándose en /var/html/www, este directorio suele ser por defecto donde se alojan las páginas web.
- Intenta matar el proceso 4539, digo intenta porque enlazando con el anterior estudio detectamos un denied en la linea `[22074531220184.22074] audit: type=1400 audit(1545415953.092:83): apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld" name="/sys/devices/system/node/" pid=4539 comm="mysqld" requested_mask="r" denied_mask="r" fsuid=0 ouid=0`, la cual se encuentra dentro del estudio del comando del apartado 3.4.5, donde indico lo siguiente `# Denegación de servicio SQL 10 de mayo de 2019 a las 06:39:15.104327 UTC.`
- se posiciona en `/`.
- Muestra de nuevo todos los procesos relativos a [MySQL](#).
- Hace un `ls` (en adelante lista) los ficheros de /var/run/mysqld.
- lista una primera vez /run y después con paginación por fecha de modificación, claramente busca algo.
- Edita de nuevo Access.log.1
- Arranca mysql_secure_intallation.
- Lista el contenido de la carpeta actual, recordemos que su ultimo posicionamiento es `/`.
- Muestra el contenido del archivo /var/log/mysql/error.log, esta buscando si hay pistas de lo que esta realizando.
- busca ficheros php en la carpeta y subcarpetas donde está situado.
- Instala el paquete python cerbot [Apache](#).
 - Destacar lo siguiente:
 - Es un complemento de [Apache](#) para Certbot.
 - El objetivo de Certbot, Let's Encrypt y ACME (Automated Certificate Management Environment) es para hacer posible para configurar un servidor HTTPS y hacer que obtenga automáticamente un Certificado de confianza del navegador, sin ninguna intervención humana. Esto es logrado ejecutando un agente de gestión de certificados en la web servidor.
 - Este agente se utiliza para:
 - Demostrar automáticamente a Let's Encrypt CA que usted controla el sitio web
 - Obtenga un certificado de confianza del navegador y configúrelo en su servidor web
 - Lleve un registro de cuándo caducará su certificado y reneúvelo

- Ayudarle a revocar el certificado si alguna vez fuera necesario.

- Reinicia el servicio de **Apache**.
- Lista los procesos de **MySQL**.
- Reinstala el servidor **Apache**.
- Busca paquete del servidor **MySQL** y con php.
- Intenta conectarse como root a **MySQL**. Cabe destacar que esto no es una práctica normal de un administrador entrar como root directamente.
- Introduce los caracteres #1546501785.
 - Relativo a esto, cabe destacar que las líneas de registro de apparmor, marcan números muy parecidos a este código.
- Realiza varias consultas, edita functions.php.
- Vuelve a ejecutar mySQL.
- Edita con **sudo /etc/mysql/debian**.
- Instala **MySQL**.
- Busca paquetes de **MySQL** que contengan la palabra php.
- se trae un archivo de wordpress 4.9.8.
 - **CVE-2018-1000773**.
- Busca paquetes relacionados con **MySQL**.
- Muestra el directorio actual donde está posicionado.
 - Si ejecuto este comando, es que estoy fuera de la consola, pudiendo ser un path transversal o entrar en la consola de metasploitable.
- Copia los ficheros de la ubicación actual al nivel superior.
- realiza una serie de acciones y extrae wordpress, lo instala.
- Instala de nuevo **Apache**.
- Vuelve a ejecutar **MySQL** com root.
- Se mueve a la ubicación donde se publican webs y es accesible por el puerto 80 /var/html/www.
- Cambia permisos a /var/run/mysqld a drwxrwxrwx (777).
 - Poner que todos los usuario puedan hacer lo que quieran con el servicio de mysql es dar "barra libre".
- Busca ficheros multimedia.
- Conecta mySQL con root.
- Inicia **MySQL** en modo seguro sin tener que autenticar.
- Reinicia **Apache** y arranca **MySQL**.
- Revisa Access.log y las 100 últimas de syslog.
- Se coloca en /var/log/apache2/
- Lista el contenido de la carpeta.
- Vuelve a mirar en que carpeta esta situado.
- Crea la carpeta **/var/run/mysqld**
- Inicia el servidor **MySQL** en modo seguro sin autenticación ejecutándose en segundo plano.
- Mata el proceso 3181, sale de **MySQL** y reinicia **Apache**.
- Instala php-mysql.
 - Este paquete proporciona un módulo **MySQL** para PHP.
 - PHP (acrónimo recursivo de PHP: preprocesador de hipertexto) es un lenguaje de programación de código abierto de propósito general que es especialmente adecuado para desarrollo web y puede integrarse en HTML.
- Muestra la hora del sistema.

- muestra archivos y carpetas de ap.
- Edita access.log.
- Verifica los ficheros de configuración de **Apache**.
- Arranca el servicio de **MySQL**.
- Edita php.ini de /etc/php/7.2/apache2/.
- Mata el proceso 4178.
- Consulta los últimos 100 registros de access.log.
- Vuelve a mostrar ficheros relativos a **MySQL** y lista las 100 ultimas líneas de sys.log
- Repite este paso 3 veces.
- Borrar el wordpress 4.9.8.
- Los siguientes procesos son claramente para realizar la captura de la memoria RAM, empezando a buscar evidencias.

Conclusiones.

1. Ha realizado acciones que vulneran el servicio **MySQL** y Apache.
 - Abre la puerta a poder acceder a las tablas sin necesidad de autenticación.
 - Concede todos los permisos a todos los usuarios a /run/nysqld
 - Elimina archivos de configuración de **MySQL**.
 - Numerosos reinicio de servicios web.
 - Modificación de Access.log
 - Modifica el fichero de configuración de WordPress.
2. Realiza búsquedas de archivos multimedia, como buscando información.
3. Añade un correo electrónico, test12312321@mailinator.com. un correo de un portal de Pruebas de flujo de trabajo de correo electrónico y SMS.
4. Acciones relativas a configuraciones.
 - Modificaciones de ficheros de configuración de php **Apache** y **MySQL**.
 - Buscar palabra POST en ficheros .php.
 - Utiliza una versión de WordPress que se descubrió su vulnerabilidad el 6 de septiembre de 2018.

Considero que, por el momento, es casualidad de que una semana después de la instalación del servidor, sin realizarse una actualización posterior. Quizás debe de estar atento a este tipo de posibles vulnerabilidades. Hoy día para el desarrollo web, Snyk revisa si las librerías que utilizas tienen vulnerabilidades. Tener alertas de este tipo siempre vienen bien para andar protegidos.

5. La hora que marca **linux_bash** no parece en cierta manera ser falsa, ya que marca la misma hora.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

[Volver al Índice General.](#)

3.5. Búsqueda de procesos en funcionamiento de interés para el análisis.

3.5.1. Linux_pslist.

A continuación vamos a proceder a enumerar los procesos en ejecución de la memoria capturada. Para ello ejecutaremos el comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_pslist`. Al ejecutar `linux_pslist`, se obtiene una lista detallada de todos los procesos activos en el momento en que se tomó la imagen de la memoria. Esta lista incluye información valiosa como el PID (identificador de proceso), el nombre del proceso, el usuario que lo ejecuta, y los tiempos de inicio y finalización del proceso. Esta información es fundamental para entender el estado del sistema en un momento específico y es especialmente útil para identificar actividades sospechosas o maliciosas, como procesos desconocidos o inusuales en ejecución, que podrían indicar la presencia de malware o la intervención de un atacante. A continuación se adjunta el comando la salida de la terminal.

3.5.1. Comando 001.

Una conclusión muy clara es que estos datos corroboran dos cosas, las fechas de `linux_bash` y los datos proporcionados por `memmap` con lo mismos.

1. Ya en `memmap` teníamos conocimiento de 11 procesos **Apache**. Se puede declarar que el primer síntoma de anomalía en el sistema es en la ejecución de `kworker/0:0` con Pid 19056 siento la hora el **1 de marzo de 2019 a las 4:24:46 UTC**.
2. Se procede a empezar a pintar la linea del tiempo. uniendo cronológicamente tanto `linux_bash` como `linux_pslist`.
3. Se llega a la conclusión de que el ataque verdaderamente ha venido por el servidor **Apache** y no por un servidor SQL ya que las aplicación de **MySQL** estuvo sin ser modificada. Eso no descarta que al tener el acceso a las tablas sin necesidad de privilegios, provoque un error en el sistema y una vulnerabilidad en la entrada no deseada.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.5.2. Linux_pstree.

En la sección anterior, hemos procedido a buscar todos los procesos activos, ahora procederemos a ver si hay relación entre ellos. Para ello ejecutaremos `linux_pstree`. Con este comando, se obtiene una estructura jerárquica que ilustra cómo los procesos están interconectados, incluyendo detalles como el identificador del proceso (PID), el nombre del proceso y los procesos hijos asociados. Esta visión jerárquica es esencial para entender la organización y la dinámica de los procesos en el sistema en el momento de la captura de la memoria. Es especialmente útil para identificar patrones anómalos o sospechosos, como procesos maliciosos que pueden estar ocultos o disfrazados bajo procesos legítimos. El comando a utilizar es `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_pstree`. Una vez obtenido el comando se procederá a adjuntarse a modo de captura del comando ejecutado.

3.5.2. Comando 001.

Analizando los datos obtenidos, encontramos un UserID 33, sabemos por defecto, las acciones por usuarios registrados en el sistema es a partir de l UserID 1000, en este caso nos encontramos con 33. Posteriormente, en la captura de la memoria cache o en la captura de la memoria, investigaremos quien es el usuario 33. Buscando por internet, he realizado un `sudo nano /etc/passwd` para ver cual es el UserID predefinido para el ID 33 siendo este `www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin`, por lo que se puede reafirmar que el ataque ha sido a través del servidor **Apache**. De todas maneras, se recomienda probar a hacer un `linux_recover_filesystem` para ver que tenemos en el archivo original.

3.5.2. Imagen 001.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.5.3. Linux_recover_filesystem.

Aunque no sea un proceso de interés procesos en funcionamiento de interés para el análisis propiamente dicho, ya que considero a procesos como archivos en ejecución por parte del sistema operativo, la sección anterior, recomienda hacer esta acción en este momento, así que procederé a ello.

El comando `linux_recover_filesystem` permite a los analistas forenses recuperar archivos de una imagen de memoria del sistema. Al ejecutar `linux_recover_filesystem`, puedo extraer archivos y directorios que estaban presentes en el sistema de archivos en el momento en que se tomó la imagen de memoria. Esto incluye archivos que pueden haber sido eliminados o no estar inmediatamente visibles en un análisis superficial. La capacidad de recuperar archivos de este modo es crucial en investigaciones forenses, ya que permite a los analistas acceder a evidencia potencial que podría haber sido ocultada, eliminada o manipulada por un usuario o por un software malicioso. Esta herramienta es particularmente útil en casos de análisis de malware, investigaciones de intrusiones y recuperación de datos. En este caso el comando a usar en la consola es `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_recover_filesystem --dump-dir /home/jrodg85/volcado-datos/`, donde con `--dump-dir /home/jrodg85/volcado-datos/` vamos a dirigir el volcado de datos a la carpeta que hemos creado en `/home/jrodg85/`.

3.5.3. Imagen 001.

3.5.3. Imagen 002.

Como podemos ver, esta es la distribución de las carpetas que se han descargado cuando se ha ejecutado el comando, en vez de verlo de esta manera, considero realizar a `/home/jrodg85/volcado-datos/` un tree, de modo que podremos ver de manera ordenada. El comando a ejecutar desde `/home/jrodg85/volcado-datos/`, será `sudo tree . > /home/jrodg85/informe-tree.txt` ya que de este modo obtendremos un informe del comando para poder analizarlo paralelamente. Debido a que la salida del comando es de 16390 líneas, se procederá a realizar una referencia dentro al archivo para que pueda ser analizado.

3.5.3. Imagen 003.

3.5.3. Imagen 004.

3.5.3. Referencia 019.

Se pueden llegar a las siguientes conclusiones:

1. Los servicios que por defecto arrancan el ser servidor, los alojados en `/etc/init.d/` son los siguientes:

- acpid
- apache2
- apache-htcacheclean
- apparmor
- apport
- atd
- console-setup.sh
- cron
- cryptdisks
- cryptdisks-early
- dbus
- ebttables
- grub-common
- hibagent
- hwclock.sh
- irqbalance
- iscsid
- keyboard-setup.sh
- kmod
- lvm2
- lvm2-lvmetad
- lvm2-lvmpolld
- lxcfs
- lxd
- mdadm
- mdadm-waitidle
- mysql
- open-iscsi
- open-vm-tools
- plymouth
- plymouth-log
- postfix
- procps
- rsync
- rsyslog
- screen-cleanup
- ssh
- udev
- ufw
- unattended-upgrades
- uuidd

2. Se confirma en [/etc/passwd](#) que:

- El usuario UserID 33 es www-data [www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin](#).

- No hay mas usuarios después de creados en el servidor que aparte de Ubuntu `ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash`.

3. En `/home/jrodg85/volcado-datos/etc/sudoers.d/` encontramos el archivo `90-cloud-init-users` el cual indica `ubuntu ALL=(ALL) NOPASSWD:ALL`.

- Esta acción viene por defecto en las instancias EC2, pero no viene normalmente dentro de los servidores independientes de Ubuntu. Esto lo que hace es no requerir contraseña cuando usas sudo con ese usuario, personalmente, no permitiría un NOPASSWD en un cloud server.

4. En `/home/` solo encontramos una carpeta llamada Ubuntu, la cual solo tiene 2 archivos:

- `accelerated-mobile-pages.0.9.97.19.zip`
- `wordpress-4.9.8.tar.gz`

Por último voy a proceder a pasar por VirusTotal los archivos extraídos, para ello los comprimo en un .zip y ese archivo zip, lo pasare por [virustotal.com](#).

Primero de todo vamos a hacer un sha256sum para corroborar posteriormente que el archivo subido en cuestión tiene el mismo hash. Para ello ejecutaremos en ubuntu el comando `sha256sum /home/jrodg85/volcado-datos.zip`, de este modo obtenemos que el hash en sha256 del archivo es `5d842006ca8551f683e78c2b5474eb79145f64eb2167683151b6fadb0bce0062`

3.5.3. Imagen 005.

Procedemos a subir el archivo a [virustotal.com](#) obteniendo el siguiente resultado:

3.5.3. Imagen 006.

Encontramos al menos que dentro de él hay un virus detectado, por ello, para detectar exactamente procedemos a dividir cada una de las carpetas en ZIP para así ir buscando nivel por nivel donde está el archivo infectado. Los zip que están limpios procederán a descartarlos y eliminarlos, los positivos, les haré un pantallazo.

Haciendo el proceso en primer nivel, se detecta que la carpeta `var` contiene, al menos un virus, se adjunta pantallazo de corroboración.

3.5.3. Imagen 007.

Esta ha sido la única notificación de primer nivel encontrada, por lo que a continuación, se procederá a hacer la misma acción de segundo nivel, pero esta vez dentro de `/var`, de modo que las siguientes detecciones serán dentro de `/var`. Los análisis que resulten negativo se ignorarán y solo se marcarán lo que resulten con posible virus dentro del archivo.

Se detecta virus dentro de `/var/lib/`.

3.5.3. Imagen 008.

Se detecta virus dentro de `/var/www/`.

3.5.3. Imagen 009.

Se procede a realizar análisis dentro de `/var/lib/`.

Se detecta virus en `/var/lib/snapd/`.

3.5.3. Imagen 010.

Se procede a realizar análisis dentro de `/var/lib/snapd/`.

Se detecta virus en `/var/lib/snapd/snaps/`.

3.5.3. Imagen 011.

Se procede a realizar análisis dentro de `/var/lib/snapd/snaps/`.

Virus total no detecta virus alguno, se puede entender como falsa alarma. Se ha procesado tanto comprimidos como sin comprimir todos los archivos independientes para corroborar con doble confirmación.

Se procede a realizar análisis dentro de `/var/www/`, como solo tenemos la carpeta html, procedemos entonces a realizar el análisis directamente en `/var/www/html/`. Para los archivos ocultos procedemos a quitar el punto

Se detecta virus en `/var/www/html/.htaccess`. Este archivo fue modificado por ultima vez el 21 de diciembre de 2018 a las 18:24:40 UTC.

3.5.3. Imagen 012.

3.5.3. Imagen 013.

En este caso hemos encontrado con un archivo dentro del sistema que puede resultar dañino para el cloud server.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

[Volver al Índice General.](#)

3.6. Listado de conexiones de red y conexiones sospechosas.

3.6.0. Introducción al listado de conexiones de red y conexiones sospechosas.

La investigación relativa a las conexiones del servidor analizado, nos permitirá tratar de descubrir cuales son las conexiones que tenia el servidor en el momento de realizar la captura de la RAM, de lo que se puede aportar información valiosa a la hora de la realización de los informes.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.6.1 Linux_arp.

En este apartado, nos vamos a enfocar en descubrir la tabla ARP del servidor, para ello ejecutaremos `linux_arp`, gracias a este comando obtendremos una lista detallada de las entradas de ARP, que incluye información vital como las direcciones IP y las direcciones MAC asociadas. Esta tabla es esencial para entender

cómo el sistema infectado o comprometido estaba comunicándose con otros dispositivos en la red. La información de la tabla ARP puede revelar conexiones de red previas, identificar dispositivos dentro de la red local con los que el sistema interactuó, y puede ser particularmente útil para rastrear la actividad de red sospechosa o maliciosa. El comando usado en este caso es `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_arp`. Se adjunta imagen de pantallazo del mismo.

3.6.1. Imagen 001.

Se observa que la VM ha enviado paquetes a las direcciones 172.31.32.1 y 172.31.33.128. Tenemos 0.0.0.0 por lo que hay conexión a una red externa.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.6.2 Linux_ifconfig.

En este apartado lo que se va a realizar es ver cual es la dirección IP del cloud server dentro de su red. Para ello usare el comando `linux_ifconfig`. Con este comando se va a obtener cuatro datos. El primero de ello es la interfaz de conexión. El segundo es la dirección IP. El tercero es la dirección MAC. El cuarto consulta si ese interfaz está en modo promiscuo, es decir, comprobará si dentro de la red, puede ver todos los paquetes del dominio de difusión. El comando que utilizaremos en este caso es `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_ifconfig`, viene a recordar el comando `ifconfig` el cual revela toda la información de red. Se adjunta imagen de pantallazo del mismo.

3.6.2. Imagen 001.

Un breve análisis de este comando es el siguiente:

1. Solo tiene una interfaz de conexión de red conectada, `eth0`.
 - o `lo` es una dirección IP lógica y es la de localhost, como en el apartado anterior hemos encontrado también la etiqueta `lo`, podemos intuir que quene de loopback o similar. Se puede considerar un dato desecharable en ese sentido.
2. La dirección IP de la VM es 172.31.38.110.
3. La dirección MAC de la VM es 06:4c f6:51:2c. Se podría estudiar la interfaz de red de esta máquina y hacer un MAC lookup, pero directamente voy a considerar que, al tener constancia de que es una VM, puedo acreditar directamente que es una MAC virtual. Ya que las máquinas virtuales suelen comunicarse a través de una red interna virtual a la red exterior, usando todos ellos la misma MAC física, y siendo esta red interna virtual como un Switch que distribuye a necesidad dentro de la red.
4. La interfaz de red `eth0` no está en modo promiscuo o monitor.

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

3.6.3 Linux_netstat.

En este apartado procederemos a tratar de tener una visión detallada de las conexiones de red, para ello ejecutaremos el comando `linux_netstat`. Con este comando, obtendremos información de todas las

conexiones TCP y UDP activas, incluyendo direcciones IP y puertos locales y remotos, así como el estado de estas conexiones. Esta información es crucial para comprender con qué otros sistemas y servicios estaba interactuando el sistema en cuestión. Es especialmente valioso para identificar comunicaciones sospechosas o no autorizadas, como conexiones a direcciones IP desconocidas o el uso de puertos inusuales, que podrían indicar actividad maliciosa, como exfiltración de datos, comando y control de malware, o accesos no autorizados. El comando a utilizar es `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_netstat`. Se hace captura del comando.

3.6.3. Comando 001.

Se procede a realizar una limpieza de datos del comando anterior, quedando de la siguiente manera.

3.6.3. Comando 002.

Analizando las conexiones se detecta lo siguiente:

A parte de la gran cantidad de conexiones a través de los puertos principales de HTTP (80) y HTTPS (443). Se observan dos conexiones realizadas a través del servicio de apache2 con id del proceso 19952.

```
TCP      ::ffff:172.31.38.110:    80  ::ffff:18.195.165.56:41529 CLOSE_WAIT  
apache2/19952  
TCP      172.31.38.110     :46384  172.31.33.128     : 8080 ESTABLISHED  
apache2/19952
```

1. Podemos ver una primera conexión que la dirección IP de destino es 18.195.165.56, cerrada y esperando. El cloud server usa en este caso el puerto 80, el puerto por defecto para HTTP y remite al puerto 45219 de destino. La aplicación que está conectada es apache2 con id 19952.
2. Podemos ver una segunda conexión que en el cloud server cuyo destino es 172.31.33.128. Esta conexión está establecida, por lo que hay comunicación. Esta asociada al puerto 46384, el cual es un puerto que no tiene una asignación determinada, sin embargo, en destino tiene establecido el puerto 8080, el cual es el puerto de reserva de HTTP. La aplicación que está conectada es la misma que la anterior, apache2 con id 19952.
 - Personalmente me resulta extraño esta conexión a un puerto de origen excesivamente alto.

```
TCP      172.31.38.110     : 22  83.247.136.74     :16666 ESTABLISHED  
sshd/20483  
TCP      172.31.38.110     : 22  83.247.136.74     :16666 ESTABLISHED  
sshd/20576
```

3. Me parece bastante extraño que hayan 2 conexiones establecidas al mismo puerto pero a distintas aplicaciones, aunque reciban el mismo nombre.
 - Son dos conexiones al puerto 22 (SSH) a la ip 83.247.136.74 y puerto 16666. Sin embargo la aplicación de conexión es la misma (sshd) pero con dos Id distintas (20483 y 20576).

[Volver al Índice del capítulo 3. Análisis de la memoria RAM.](#)

[Volver al Índice General.](#)

4. Análisis del disco duro.

Índice del capítulo 4. Análisis del disco duro.

[Volver al Índice General.](#)

4.0. Introducción al capítulo 4. Análisis del disco duro.

[Volver al Índice del capítulo 4. Análisis del disco duro.](#)

[Volver al Índice General.](#)

4.1. Acciones previas al análisis del disco duro.

En el presente TFM, se nos ha proporcionado a los alumnos un archivo de captura de disco duro en formato **.E01**. Por otro lado, se nos ha proporcionado los resúmenes o **hash** en MD5 y en SHA1 de los archivos tal y como se muestra en la siguiente imagen.

4.1 Imagen 001.

Como podemos ver, los **hash** resúmenes del archivo del HDD, tememos los siguientes hashes en MD5 y en SHA1:

- **MD5:** 324ed7db769620e3fb55c027480d0ef3
- **SHA1:** 3398f90d2438230aaaf7b5e8ce0a01e456d9ca10

El **hash** tal y como se indica en los apuntes de la asignatura, en el módulo de Fases y metodología del análisis forense, durante la adquisición de evidencias digitales dice lo siguiente:

Una vez generada la copia o clon del soporte original, el programa o el dispositivo hardware empleado en este proceso realiza el cálculo del **CRC** o del valor **hash** del soporte original y del destino, con la finalidad de garantizar que los dos son idénticos y que la copia se ha producido sin ningún error. Este cálculo puede realizarse sobre todo el conjunto de información contenida en el soporte original, o bien emplear solamente un conjunto de ficheros del total.

A su vez, en el glosario de términos la definición de **hash** es la siguiente:

Es una función matemática unidireccional que resume un mensaje de tamaño variable (por ejemplo, un archivo), en una representación de tamaño fijo. Es poco probable que dos ficheros distintos tengan la misma representación **hash**, lo cual significa que este valor puede utilizarse a efectos de comprobación de la **integridad** de un archivo (o de un sistema entero). Las funciones **hash** más conocidas son MD5 y SHA-1.

Una vez descargado el archivo de captura de la memoria RAM, procedemos a usar PowerShell para determinar el **hash** del archivo. Para ello usamos el comando "Get-FileHash [Argumento] -Algorithm MD5". En nuestro caso hemos usado los siguientes comandos:

4.1 Comando 001.

4.1 Comando 002.

Se puede observar en la siguiente imagen la respuesta de PowerShell de los hashes de MD5 y SHA1.

4.1. Imagen 002.

Como conclusión podemos verificar que la **integridad** de la copia facilitada para realizar el TFM no ha sido vulnerada.

[Volver al Índice del capítulo 4. Análisis del disco duro.](#)

[Volver al Índice General.](#)

4.2. Datos de interés del disco duro.

La herramienta para utilizar en este caso será Autopsy 4.21.0 para Windows. Arrancaremos la aplicación y generaremos un nuevo caso.

4.2. Imagen 001.

Procedemos a la carga de datos y de la imagen de disco duro.

4.2. Imagen 002.

Procedemos a hacer una visualización general. En el TFM, la autoridad, nos da fe de que esta es la imagen extraída del servidor y en la sección anterior hemos corroborado el hash del archivo. Se puede dar fe de que ambos datos provienen del mismo servidor. Por otro lado se ha comprobado los datos de la extracción de la RAM así como de la extracción del HDD que el archivo `/home/jrodg85/volvado-datos/home/ubuntu/.bash_history`, son exactamente el mismo. Se adjunta imagen donde se puede comprobar al acción.

4.2. Imagen 003.

A continuación, procederemos a extraer los archivos en adelante en `C:\TFM-estudio\` y, mediante WSL, procederemos a hacer las acciones necesarias para su análisis.

[Volver al Índice del capítulo 4. Análisis del disco duro.](#)

[Volver al Índice General.](#)

4.3. Usuarios del sistema.

A continuación vamos a proceder a investigar los usuarios que hay en el cloud server, para ello vamos a proceder a investigar el contenido del archivo `/etc/passwd`, en el comprobaremos los usuarios del sistema.

4.3. Imagen 001.

Analizando los usuarios del sistema, el único usuario que realmente es el ya encontrado en la RAM es el usuario Ubuntu.

```
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
```

No contentos con este análisis puesto que no sacamos nada nuevo, vamos a observar en los registros del sistema que autenticaciones han ocurrido en el cloud server, para ello procederemos a extraer `/var/log/auth.log`, con ello veremos un registro completo de las acciones llevadas a cabo dentro del cloud server. Procedemos con WSL a realizar un primer análisis haciendo un `grep "user" auth.log`, el cual nos da muchísima información. Se adjunta pantallazo del mismo.

4.3. Imagen 002.

Al ver tal cantidad ingente de información procedemos a ver un patrón de usuarios invalidos en auth.log. Por lo que buscamos los invalid user con el comando `grep "Invalid user" auth.log`

4.2 Comando 001.

[Volver al Índice del capítulo 4. Análisis del disco duro.](#)

[Volver al Índice General.](#)

4.4. Análisis de evidencias del disco duro.

[Volver al Índice del capítulo 4. Análisis del disco duro.](#)

[Volver al Índice General.](#)

5. Resumen ejecutivo.

Índice del capítulo 5. Resumen ejecutivo.

[Volver al Índice General.](#)

5.0. Introducción al capítulo 5. Resumen ejecutivo.

[Volver al Índice del capítulo 5. Resumen ejecutivo.](#)

[Volver al Índice General.](#)

5.1. Resumen ejecutivo.

[Volver al Índice del capítulo 5. Resumen ejecutivo.](#)

[Volver al Índice General.](#)

6. Informe pericial.

Índice del capítulo 6. Informe pericial.

[Volver al Índice General.](#)

6.0. Introducción al capítulo 6. Informe pericial.

[Volver al Índice del capítulo 6. Informe pericial.](#)

[Volver al Índice General.](#)

6.1. Informe pericial.

[Volver al Índice del capítulo 6. Informe pericial.](#)

[Volver al Índice General.](#)

7. Conclusiones.

Índice del capítulo 7. Conclusiones.

[Volver al Índice General.](#)

7.0. Introducción al capítulo 7. Conclusiones.

[Volver al Índice del capítulo 7. Conclusiones.](#)

[Volver al Índice General.](#)

7.1. Conclusiones.

[Volver al Índice del capítulo 7. Conclusiones.](#)

[Volver al Índice General.](#)

8. Anexos.

Índice del capítulo 8. Anexos.

[Volver al Índice General.](#)

8.0. Introducción al capítulo 8. Anexos.

[Volver al Índice del capítulo 8. Anexos.](#)

[Volver al Índice General.](#)

8.1. Glosario de términos y abreviaturas.

8.1.001.000.001. CISO.

1. La persona responsable de velar por la ciberseguridad de una empresa, es el acrónimo de (Chief Information Security Officer). También podemos conocerlo como director de seguridad de la información. Esta persona es la que se encarga de proteger la información ante posibles ciberataques y fugas de datos. De esta manera, garantiza la seguridad dentro de las posibilidades tanto humanas, técnicas como económicas que tenga cada empresa.

[Volver al texto del término en la Sección 1.0.](#)

[Volver al Índice del capítulo 8. Anexos.](#)

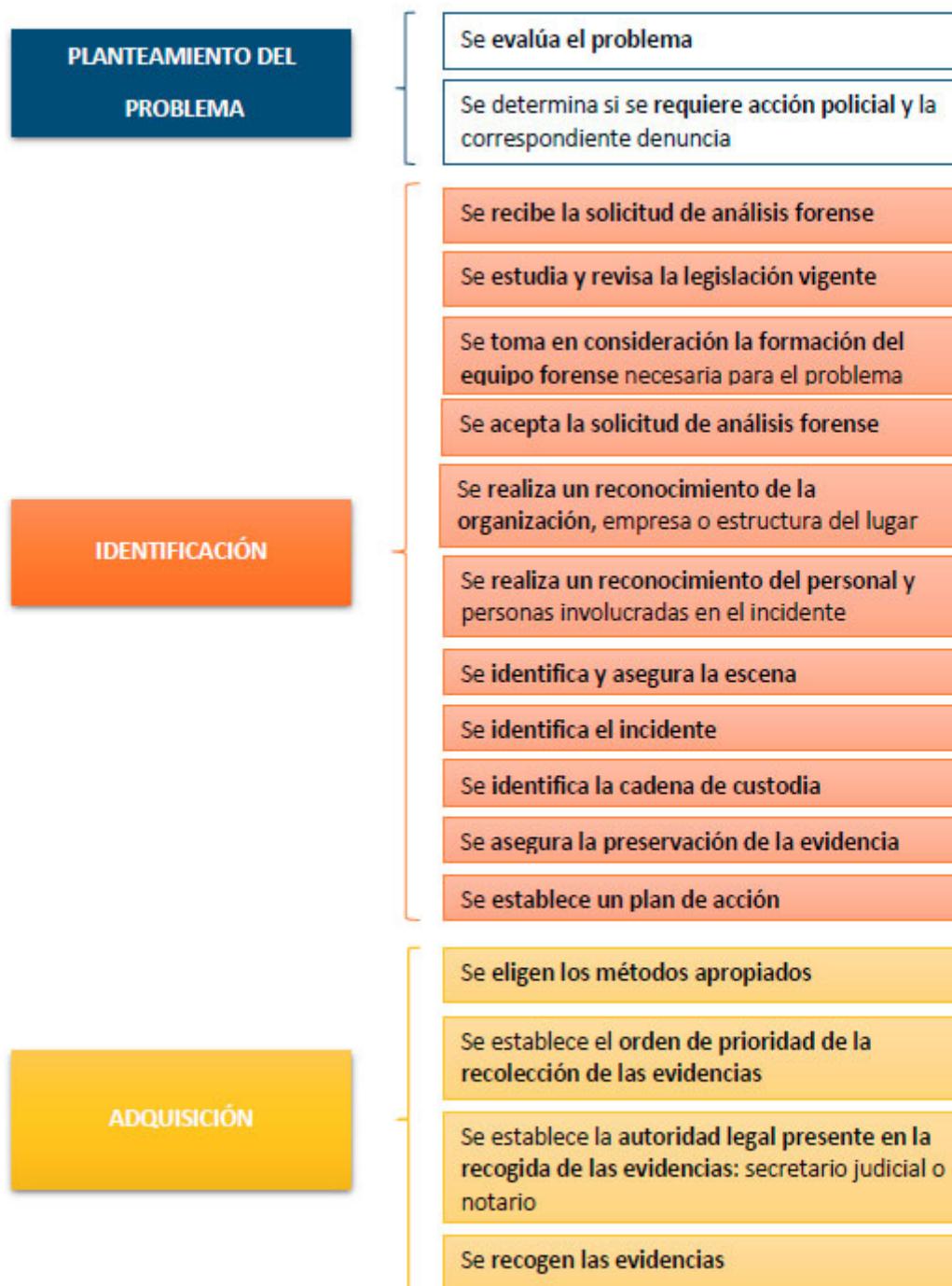
[Volver al Índice General.](#)

8.2. Imágenes.

8.2.001.003.005.001. Diagrama de metodología del análisis forense.

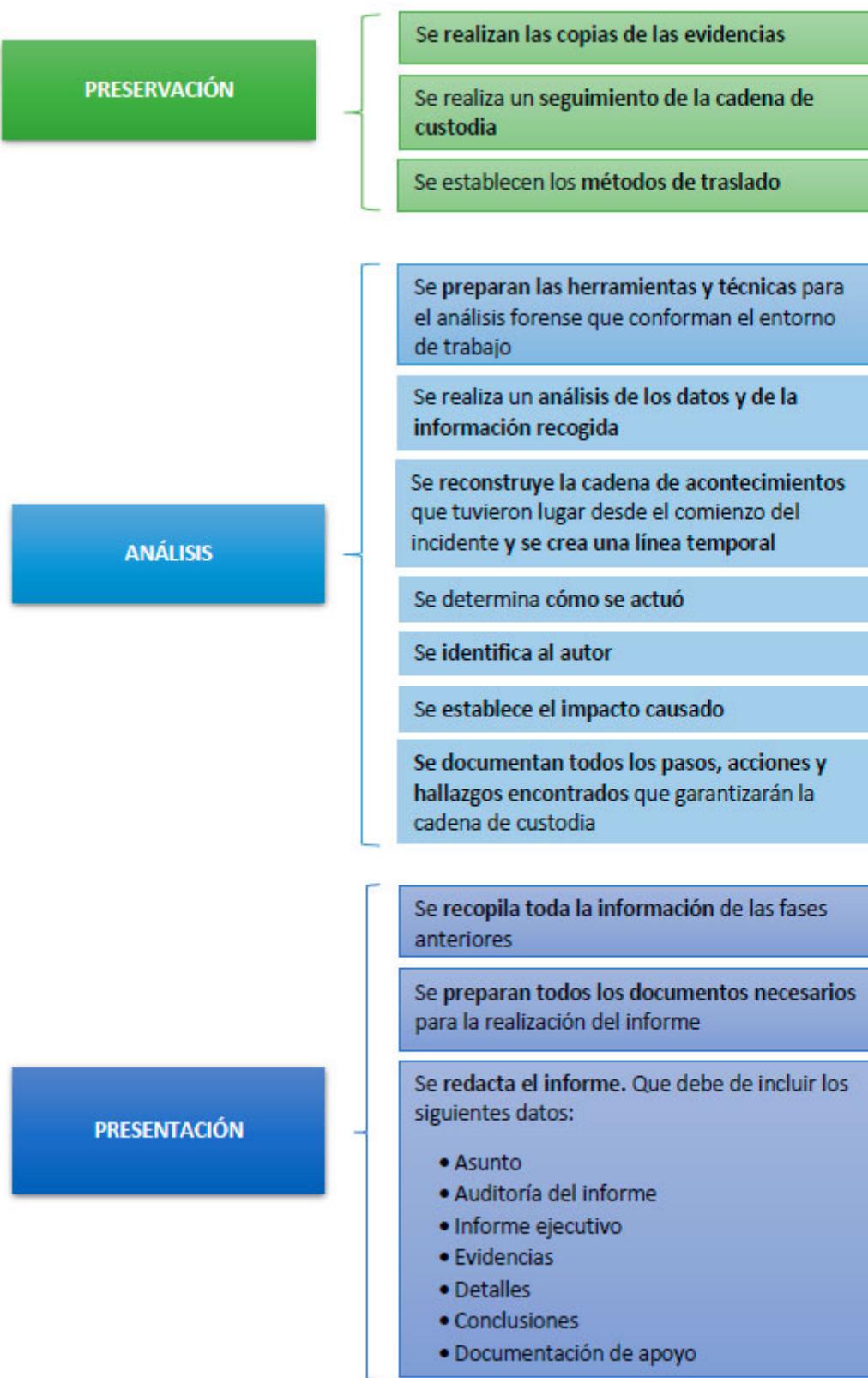


[Volver al texto de la imagen en la Sección 1.3.5.](#)

8.2.001.003.005.002. Fases 1 2 y 3 de la metodología del análisis forense.

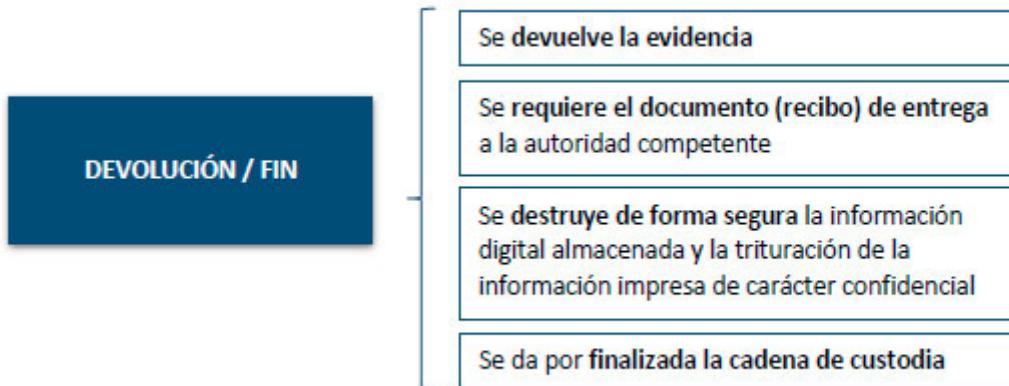
[Volver al texto de la imagen en la Sección 1.3.5.](#)

8.2.001.003.005.003. Fases 4 5 y 6 de la metodología del análisis forense.



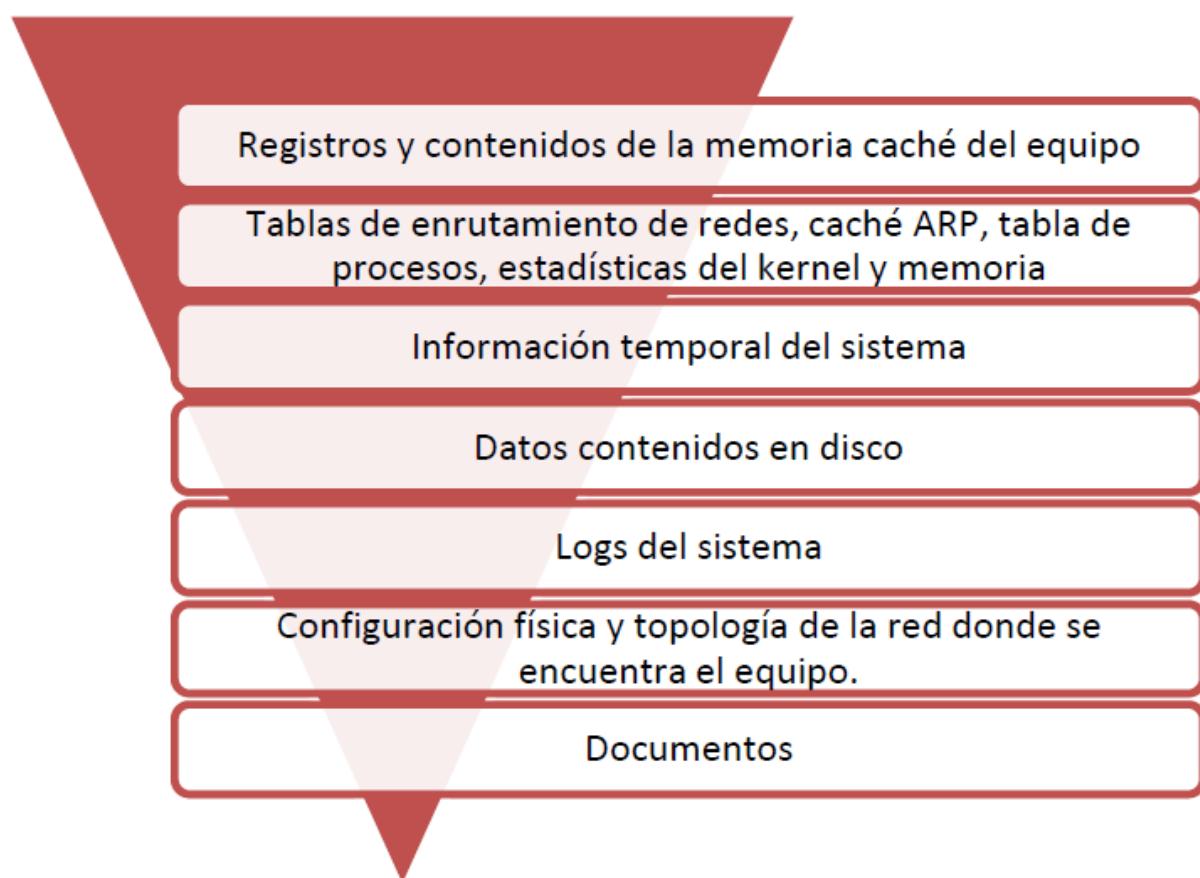
[Volver al texto de la imagen en la Sección 1.3.5.](#)

8.2.001.003.005.004. Fase 7 de la metodología del análisis forense.



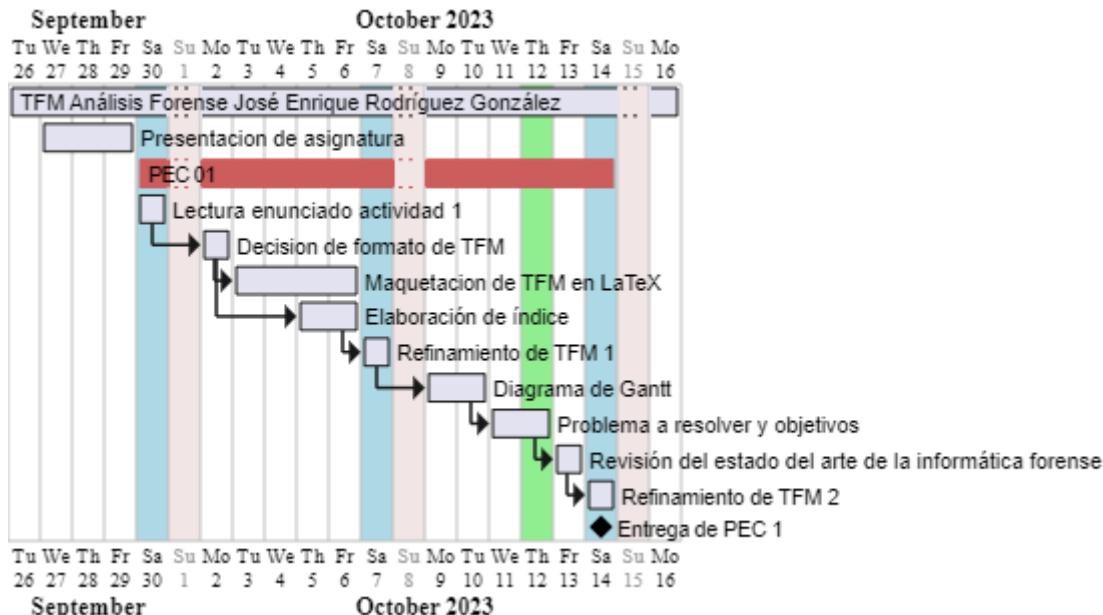
[Volver al texto de la imagen en la Sección 1.3.5.](#)

8.2.001.003.005.005. Orden de volatilidad análisis forense.



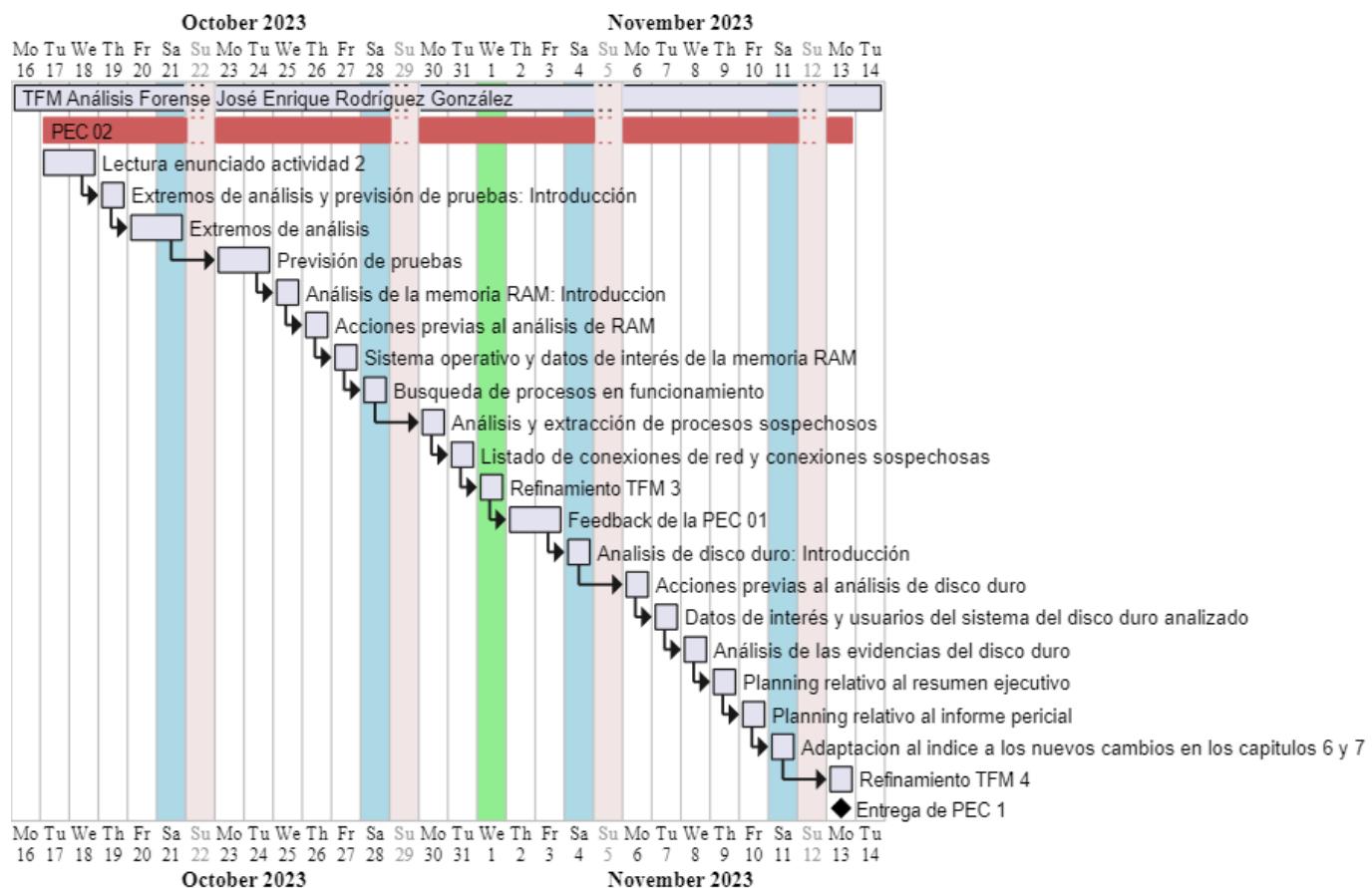
[Volver al texto de la imagen en la Sección 1.3.5.](#)

8.2.001.006.001. Diagrama de Gantt reto/PEC 1.



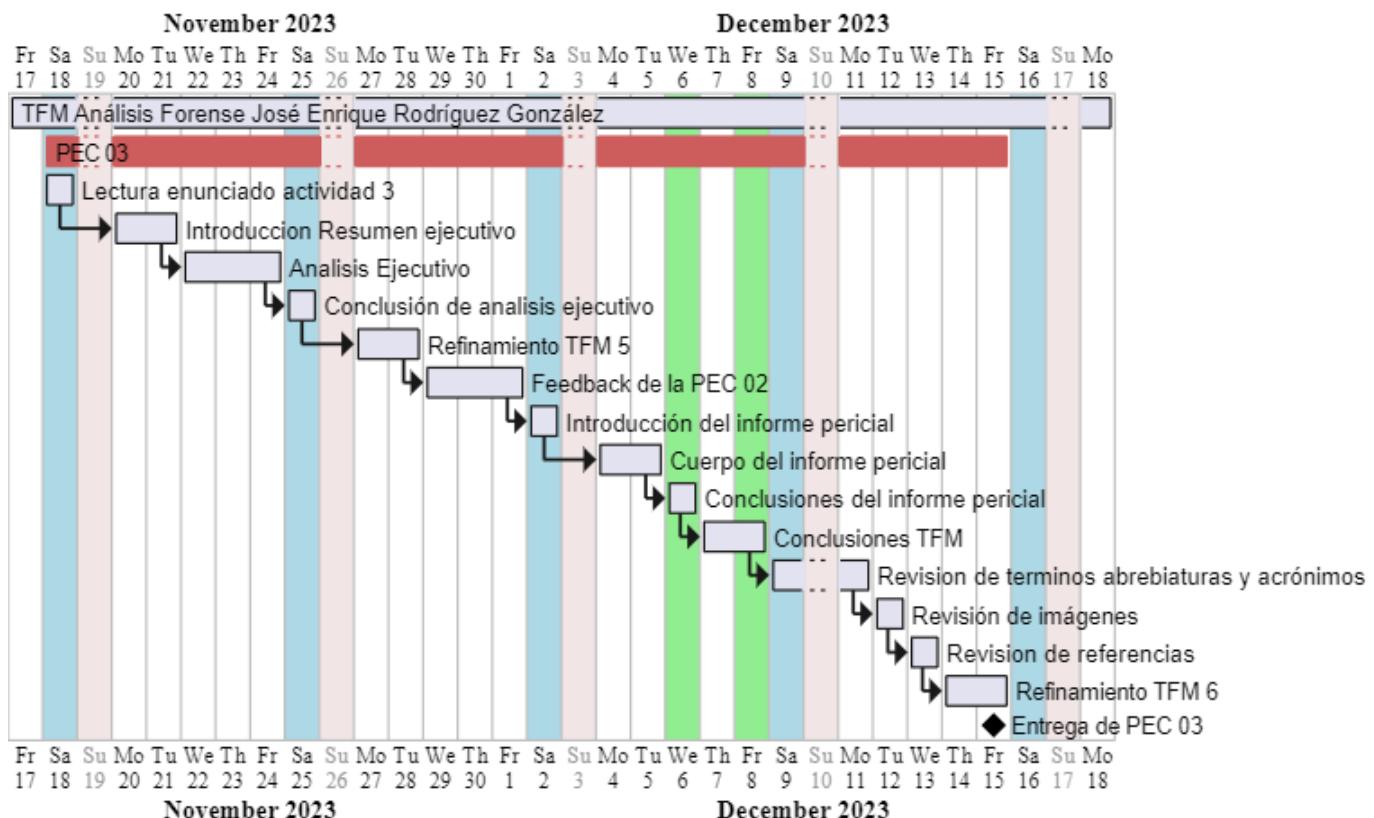
[Volver al texto de la imagen en la Sección 1.6.](#)

8.2.001.006.002. Diagrama de Gantt reto/PEC 2.



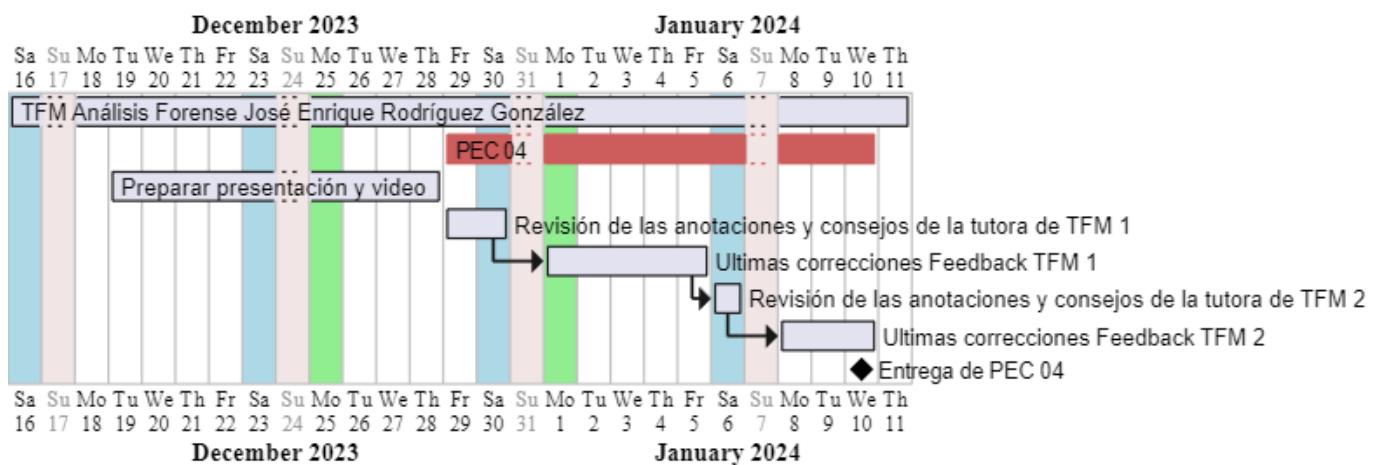
[Volver al texto de la imagen en la Sección 1.6.](#)

8.2.001.006.003. Diagrama de Gantt reto/PEC 3.



[Volver al texto de la imagen en la Sección 1.6.](#)

8.2.001.006.004. Diagrama de Gantt reto/PEC 4.



[Volver al texto de la imagen en la Sección 1.6.](#)

8.2.003.001.001. Imagen Hash archivos.

```

Server_HDD.E01
*****
Acquisition hash MD5: 72d2cd59ff2167c501c67cc918d60d39

MD5: 324ed7db769620e3fb55c027480d0ef3
SHA1: 3398f90d2438230aaaf7b5e8ce0a01e456d9ca10

Server_RAM.mem
*****
MD5: 75a99b57032aa34ba19042ed85db273f
SHA1: cc1fad2af321b8c2ddf0103986e3b344eb8f2cc8

```

[Volver al texto de la imagen en la Sección 3.1.](#)

8.2.003.001.002. Imagen Hash PowerShell.

```

Windows PowerShell

PS D:\TFM\RAM> Get-FileHash .\Server_RAM.mem -Algorithm MD5
Algorithm      Hash                                         Path
----          ----                                         ---
MD5           75A99B57032AA34BA19042ED85DB273F             D:\TFM\RAM\...

PS D:\TFM\RAM> Get-FileHash .\Server_RAM.mem -Algorithm SHA1
Algorithm      Hash                                         Path
----          ----                                         ---
SHA1          CC1FAD2AF321B8C2DDF0103986E3B344EB8F2CC8             D:\TFM\RAM\...

```

[Volver al texto de la imagen en la Sección 3.1.](#)

8.2.003.002.001. Imagen de imageinfo.

```

jrodg85@jrodg85-VirtualBox:~/volatility$ sudo python2.7 vol.py -f '/home/jrodg85/Server_RAM.mem' imageinfo
[sudo] contraseña para jrodg85:
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
         Suggested Profile(s) : No suggestion (Instantiated with no profile)
                  AS Layer1 : LimeAddressSpace (Unnamed AS)
                  AS Layer2 : FileAddressSpace (/home/jrodg85/Server_RAM.mem)
                 PAE type : No PAE

```

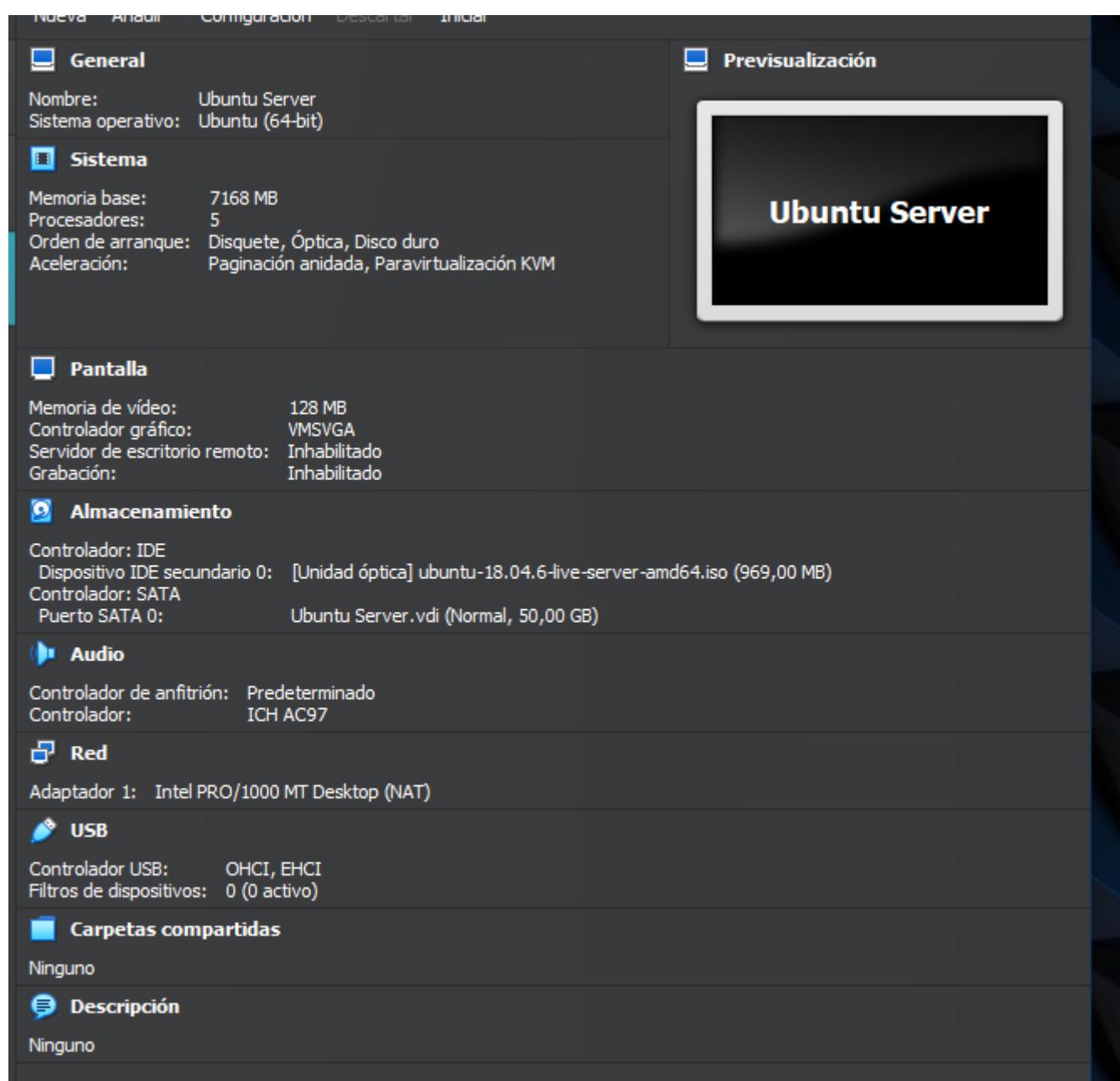
[Volver al texto de la imagen en la Sección 3.2.](#)

8.2.003.002.002. Imagen de búsqueda de string linux version.

```
jrodg85@jrodg85-VirtualBox:~/volatility$ strings '/home/jrodg85/Server_RAM.mem' | grep -Ei "linux version" | uniq
 Packages build for Linux versions have support to btrfs filesystem.
MESSAGE=Linux version 4.15.0-1021-aws (buildd@lcy01-amd64-001) (gcc version 7.3.0 (Ubuntu 7.3.0-16ubuntu3)) #21-Ubuntu SMP Tue Aug 28 10:23:07 UTC 2018 (Ubuntu 4.15.0-1021.21-aws 4.15.18)
Also included is a Linux version of the VMS "Phone" utility and a VMSMail
This is the GNU/Linux version of the popular PasswordSafe password
file systems, NFS, top processes, resources (Linux version & processors) and
This package provides the Linux version
file systems, NFS, top processes, resources (Linux version & processors) and
On some Linux version, write-only pipe are detected as readable. This
o The intent is to make the tool independent of Linux version dependencies,
Linux version 4.15.0-1021-aws (buildd@lcy01-amd64-001) (gcc version 7.3.0 (Ubuntu 7.3.0-16ubuntu3)) #21-Ubuntu SMP Tue Aug 28 10:23:07 UTC 2018 (Ubuntu 4.15.0-1021.21-aws 4.15.18)
On some Linux version, write-only pipe are detected as readable. This
```

[Volver al texto de la imagen en la Sección 3.2.](#)

8.2.003.003.001.001. Características VM perfil Volatility.



[Volver al texto de la imagen en la Sección 3.3.1.](#)

8.2.003.003.001.002. Características VM kernel.

```
jrodg85@jrodg85:~$ hostnamectl
  Static hostname: jrodg85
    Icon name: computer-vm
    Chassis: vm
  Machine ID: 2030803e359c4fed8f380dbcdb3ef21f
    Boot ID: c05d0aab9e214c26bed0f2388222e900
  Virtualization: oracle
Operating System: Ubuntu 18.04.6 LTS
          Kernel: Linux 4.15.0-213-generic
        Architecture: x86-64
jrodg85@jrodg85:~$
```

[Volver al texto de la imagen en la Sección 3.3.1.](#)

8.2.003.003.001.003. Búsqueda Kernel 4.15.0-1021-aws.

```
jrodg85@jrodg85:~$ sudo apt-cache search linux-image | grep 4.15.0-1021-aws
linux-image-4.15.0-1021-aws - Linux kernel image for version 4.15.0 on 64 bit x86 SMP
jrodg85@jrodg85:~$
```

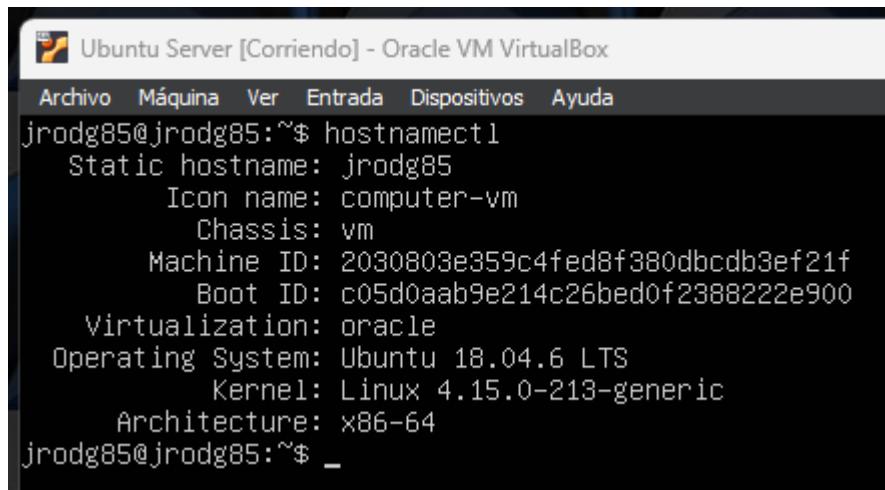
[Volver al texto de la imagen en la Sección 3.3.1.](#)

8.2.003.003.001.004. Instalación Kernel 4.15.0-1021-aws.

```
jrodg85@jrodg85:~$ sudo apt-get install linux-image-4.15.0-1021-aws
[sudo] password for jrodg85:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  linux-modules-4.15.0-1021-aws
Paquetes sugeridos:
  fdutils linux-aws-doc-4.15.0 | linux-aws-source-4.15.0 linux-aws-tools
  linux-headers-4.15.0-1021-aws
Se instalarán los siguientes paquetes NUEVOS:
  linux-image-4.15.0-1021-aws linux-modules-4.15.0-1021-aws
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 43 no actualizados.
Se necesita descargar 20,1 MB de archivos.
Se utilizarán 70,9 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

[Volver al texto de la imagen en la Sección 3.3.1.](#)

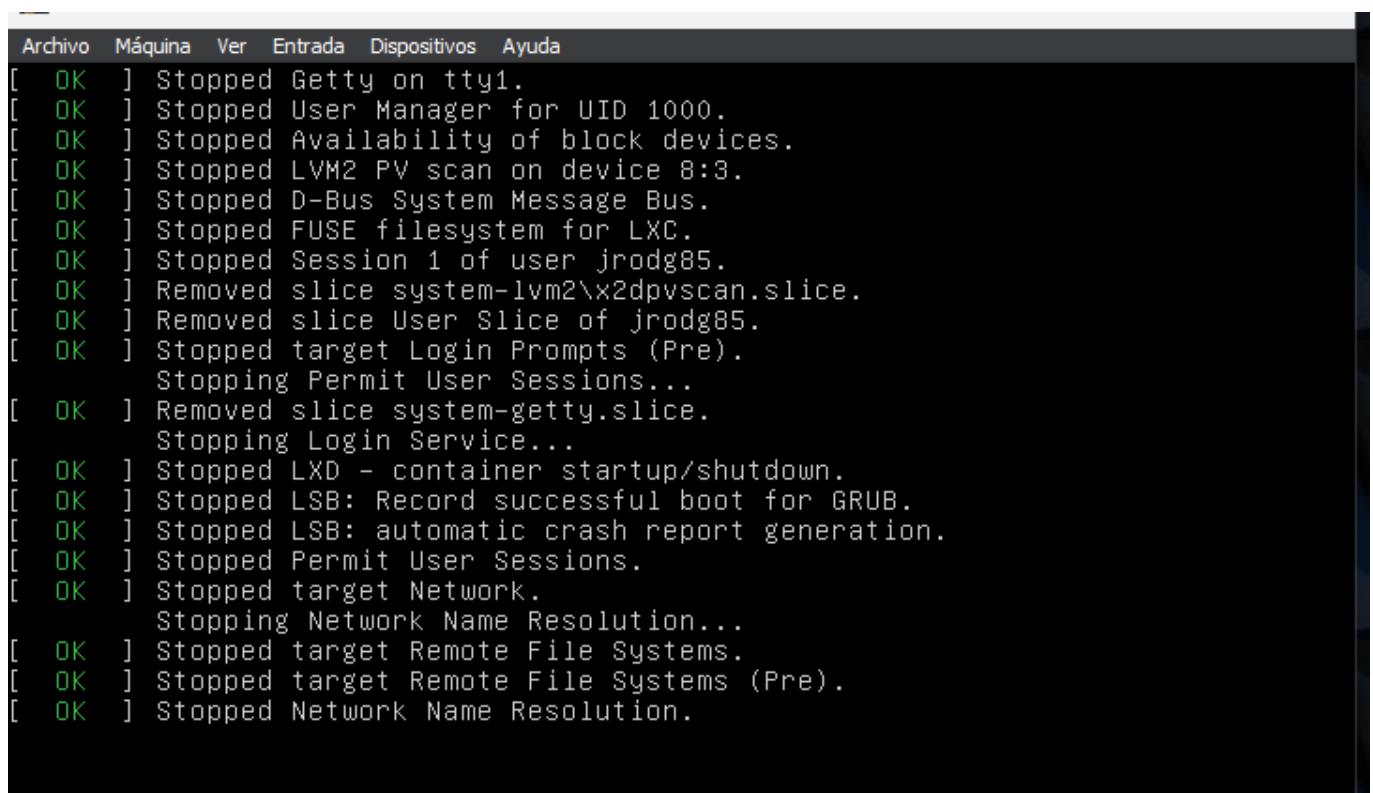
8.2.003.003.001.005. Probando de nuevo hostnamectl.



```
Ubuntu Server [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
jrodg85@jrodg85:~$ hostnamectl
Static hostname: jrodg85
  Icon name: computer-vm
  Chassis: vm
Machine ID: 2030803e359c4fed8f380dbcdb3ef21f
  Boot ID: c05d0aab9e214c26bed0f2388222e900
Virtualization: oracle
Operating System: Ubuntu 18.04.6 LTS
  Kernel: Linux 4.15.0-213-generic
Architecture: x86-64
jrodg85@jrodg85:~$ _
```

[Volver al texto de la imagen en la Sección 3.3.1.](#)

8.2.003.003.001.006. Reiniciando server.



```
Archivo Máquina Ver Entrada Dispositivos Ayuda
[ OK ] Stopped Getty on tty1.
[ OK ] Stopped User Manager for UID 1000.
[ OK ] Stopped Availability of block devices.
[ OK ] Stopped LVM2 PV scan on device 8:3.
[ OK ] Stopped D-Bus System Message Bus.
[ OK ] Stopped FUSE filesystem for LXC.
[ OK ] Stopped Session 1 of user jrodg85.
[ OK ] Removed slice system-lvm2\x2dpvscan.slice.
[ OK ] Removed slice User Slice of jrodg85.
[ OK ] Stopped target Login Prompts (Pre).
  Stopping Permit User Sessions...
[ OK ] Removed slice system-getty.slice.
  Stopping Login Service...
[ OK ] Stopped LXD - container startup/shutdown.
[ OK ] Stopped LSB: Record successful boot for GRUB.
[ OK ] Stopped LSB: automatic crash report generation.
[ OK ] Stopped Permit User Sessions.
[ OK ] Stopped target Network.
  Stopping Network Name Resolution...
[ OK ] Stopped target Remote File Systems.
[ OK ] Stopped target Remote File Systems (Pre).
[ OK ] Stopped Network Name Resolution.
```

[Volver al texto de la imagen en la Sección 3.3.1.](#)

8.2.003.003.001.007. Comprobando kernel.

```
Archivo Máquina Ver Entrada Dispositivos Ayuda
jrodg85@jrodg85:~$ hostnamectl
  Static hostname: jrodg85
    Icon name: computer-vm
    Chassis: vm
    Machine ID: 2030803e359c4fed8f380dbcdb3ef21f
      Boot ID: 3b275702afea4b3c9bb134454284b369
  Virtualization: oracle
Operating System: Ubuntu 18.04.6 LTS
  Kernel: Linux 4.15.0-1021-aws
  Architecture: x86-64
jrodg85@jrodg85:~$ uname -r
4.15.0-1021-aws
jrodg85@jrodg85:~$
```

[Volver al texto de la imagen en la Sección 3.3.1.](#)

8.2.003.003.002.001. Instalación de dwarfdump.

```
jrodg85@jrodg85:~/volatility$ sudo apt install dwarfdump
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 0 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://es.archive.ubuntu.com/ubuntu bionic/universe amd64 dwarfdump amd64
20180129-1 [249 kB]
Descargados 249 kB en 2s (139 kB/s)
Seleccionando el paquete dwarfdump previamente no seleccionado.
(Leyendo la base de datos ... 72451 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) ...
jrodg85@jrodg85:~/volatility$ _
```

[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.003.002.002. Volatility instalado.

```
jrodg85@jrodg85:~/volatility$ 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 is no longer maintained. pip 21.0 will drop s
upport for Python 2.7 in January 2021. More details about Python 2 support in pi
p can be found at https://pip.pypa.io/en/latest/development/release-process/#pyt
hon-2-support pip 21.0 will remove support for this functionality.
WARNING: The directory '/home/jrodg85/.cache/pip' or its parent directory is not
owned or is not writable by the current user. The cache has been disabled. Chec
k the permissions and owner of that directory. If executing pip with sudo, you m
ay 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
volatility   2.6.1
wheel         0.37.1
yara-python   3.8.1
jrodg85@jrodg85:~/volatility$ _
```

[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.003.002.003. ls /home/jrodg85/volatility/tools/linux.

```
jrodg85@jrodg85:~/volatility/tools/linux$ ls
kcore  Makefile  Makefile.enterprise  module.c
jrodg85@jrodg85:~/volatility/tools/linux$ _
```

[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.003.002.004. make /home/jrodg85/volatility/tools/linux.

```

Ubuntu Server [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
jrodg85@jrodg85:~/volatility/tools/linux$ make
make -C /lib/modules/4.15.0-1021-aws/build CONFIG_DEBUG_INFO=y M="/home/jrodg85/volatility/tools/linux" modules
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-1021-aws'
^[[3~Makefile:976: "Cannot use CONFIG_STACK_VALIDATION=y, please install libelf-dev, libelf-devel or elfutils-libelf-devel"
  CC [M]  /home/jrodg85/volatility/tools/linux/module.o
  Building modules, stage 2.
  MODPOST 1 modules
WARNING: modpost: missing MODULE_LICENSE() in /home/jrodg85/volatility/tools/linux/module.o
see include/linux/module.h for more information
  CC      /home/jrodg85/volatility/tools/linux/module.mod.o
  LD [M]  /home/jrodg85/volatility/tools/linux/module.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-1021-aws'
dwarfdump -di module.ko > module.dwarf
make -C /lib/modules/4.15.0-1021-aws/build M="/home/jrodg85/volatility/tools/linux" clean
make[1]: Entering directory '/usr/src/linux-headers-4.15.0-1021-aws'
  CLEAN  /home/jrodg85/volatility/tools/linux/.tmp_versions
  CLEAN  /home/jrodg85/volatility/tools/linux/Module.symvers
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-1021-aws'
jrodg85@jrodg85:~/volatility/tools/linux$ ls
kcore Makefile Makefile.enterprise module.c module.dwarf
jrodg85@jrodg85:~/volatility/tools/linux$
```

[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.003.002.005. Comandos comprobación kernel.

```

Ubuntu Server [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
jrodg85@jrodg85:~/volatility/tools/linux$ lsb_release -si
Ubuntu
jrodg85@jrodg85:~/volatility/tools/linux$ uname -r
4.15.0-1021-aws
jrodg85@jrodg85:~/volatility/tools/linux$ _
```

[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.003.002.006. Perfil creado.

```

Archivo Máquina Ver Entrada Dispositivos Ayuda
jrodg85@jrodg85:~$ sudo zip linux$(lsb_release -si)_$(uname -r)_profile.zip /home/jrodg85/volatility/tools/linux/module.dwarf /boot/System.map-4.15.0-1021-aws
  adding: home/jrodg85/volatility/tools/linux/module.dwarf (deflated 91%)
  adding: boot/System.map-4.15.0-1021-aws (deflated 79%)
jrodg85@jrodg85:~$ _
```

[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.003.002.007. ls a la carpeta del perfil.

```
Ubuntu Server [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
jrodg85@jrodg85:~$ ls
get-pip.py  linuxUbuntu_4.15.0-1021-aws_profile.zip  usb  volatility
jrodg85@jrodg85:~$ _
```

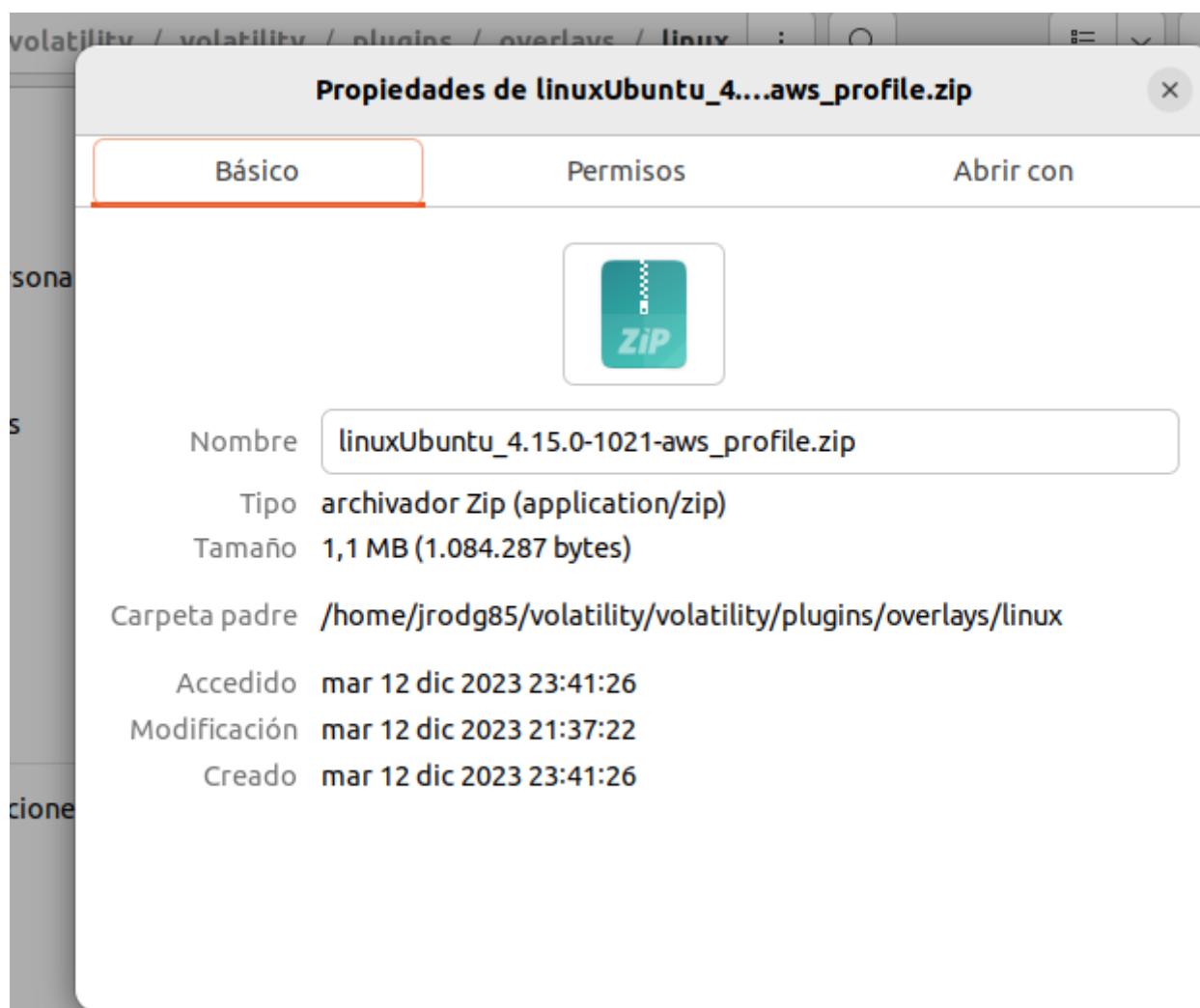
[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.003.002.008. Perfil copiado a usb.

```
Archivo Máquina Ver Entrada Dispositivos Ayuda
jrodg85@jrodg85:~$ ls usb/
historial.txt
linuxUbuntu_4.15.0-1021-aws_profile.zip
jrodg85@jrodg85:~$ _
```

[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.003.002.009. Perfil copiado entorno volatility.



[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.003.002.010. Perfil creado en entorno volatility.

The screenshot shows the 'Ubuntu volatility [Corriendo] - Oracle VM VirtualBox' interface. In the terminal window, the command `sudo python2.7 vol.py --info` is run, displaying the Volatility Foundation Volatility Framework version 2.6.1. The terminal also lists various profiles available, including LinuxUbuntu_4_15_0-1021-awsx64 and several Windows Vista profiles (SP0x64, SP0x86, SP1x64, SP1x86, SP2x64, SP2x86, Win10x64).

```
jrodg85@jrodg85-VirtualBox:~/volatility$ sudo python2.7 vol.py --info
Volatility Foundation Volatility Framework 2.6.1

jrodg85@jrodg85-VirtualBox:~/volatility$
```

LinuxUbuntu_4_15_0-1021-awsx64 - A Profile for Linux linuxUbuntu_4.15.0-1021-aws x64
VistaSP0x64 - A Profile for Windows Vista SP0 x64
VistaSP0x86 - A Profile for Windows Vista SP0 x86
VistaSP1x64 - A Profile for Windows Vista SP1 x64
VistaSP1x86 - A Profile for Windows Vista SP1 x86
VistaSP2x64 - A Profile for Windows Vista SP2 x64
VistaSP2x86 - A Profile for Windows Vista SP2 x86
Win10x64 - A Profile for Windows 10 x64

[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.003.002.011. Prueba funcionamiento perfil.

The screenshot shows the 'Ubuntu volatility [Corriendo] - Oracle VM VirtualBox' interface. In the terminal window, the command `sudo python2.7 vol.py --profile=LinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_cpu info` is run, displaying the Volatility Foundation Volatility Framework version 2.6.1. The terminal then lists processor information, showing one Intel Xeon E5-2676 v3 @ 2.40GHz.

```
jrodg85@jrodg85-VirtualBox:~/volatility$ sudo python2.7 vol.py --profile=LinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_cpu info
Volatility Foundation Volatility Framework 2.6.1
Processor Vendor Model
0 GenuineIntel Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz
jrodg85@jrodg85-VirtualBox:~/volatility$
```

[Volver al texto de la imagen en la Sección 3.3.2.](#)

8.2.003.004.001.001. Linux cpuinfo.

The screenshot shows the 'Ubuntu volatility [Corriendo] - Oracle VM VirtualBox' interface. In the terminal window, the command `sudo python2.7 vol.py --profile=LinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_cpuinfo` is run, displaying the Volatility Foundation Volatility Framework version 2.6.1. The terminal then lists processor information, showing one Intel Xeon E5-2676 v3 @ 2.40GHz.

```
jrodg85@jrodg85-VirtualBox:~/volatility$ sudo python2.7 vol.py --profile=LinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_cpuinfo
Volatility Foundation Volatility Framework 2.6.1
Processor Vendor Model
0 GenuineIntel Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz
jrodg85@jrodg85-VirtualBox:~/volatility$
```

[Volver al texto de la imagen en la Sección 3.4.1.](#)

8.2.003.004.002.001. linux banner.

```
jrodg85@jrodg85-VirtualBox:~/volatility$ sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_banner
Volatility Foundation Volatility Framework 2.6.1
Linux version 4.15.0-1021-aws (buildd@lcy01-amd64-001) (gcc version 7.3.0 (Ubuntu 7.3.0-16ubuntu3)) #21-Ubuntu SMP Tue Aug 28 10:23:07 UTC 2018 (Ubuntu 4.15.0-1021.21-aws 4.15.18)
jrodg85@jrodg85-VirtualBox:~/volatility$
```

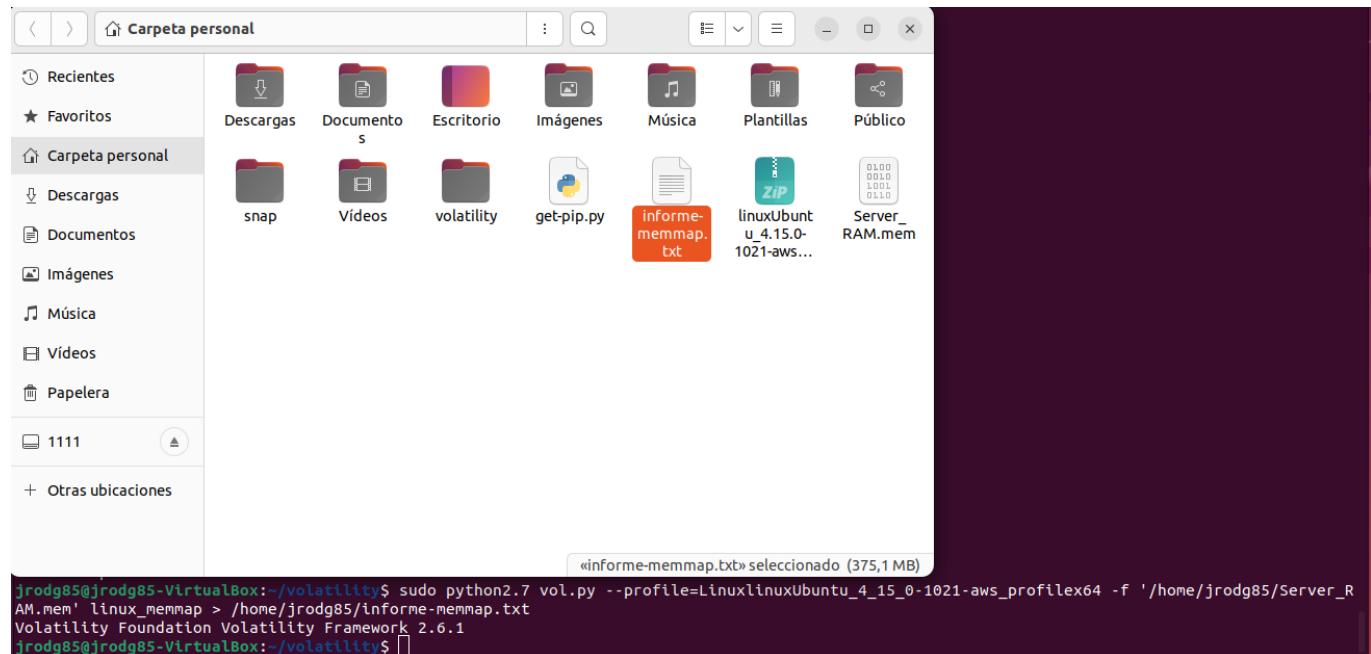
[Volver al texto de la imagen en la Sección 3.4.2.](#)

8.2.003.004.003.001. linux mount.

```
jrodg85@jrodg85-VirtualBox:~/volatility$ sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_mount
Volatility Foundation Volatility Framework 2.6.1
cgroup          /sys/fs/cgroup/rdma      cgroup      rw,relatime,nosuid,nodev,noexec
tmpfs           /sys/fs/cgroup         tmpfs       ro,nosuid,nodev,noexec
/dev/xvda1      /                      ext4       ro,relatime
proc            /bus                   proc       ro,relatime,nosuid,nodev,noexec
pstore          /sys/fs/pstore        pstore     rw,relatime,nosuid,nodev,noexec
fusectl         /sys/fs/fuse/connections fusectl    rw,relatime
lxcfs           /var/lib/lxcfs        fuse      ro,relatime,nosuid,nodev
/dev/loop0       /snap/core/5328       squashfs   ro,relatime,nodev
udev            /dev                   devtmpfs   rw,relatime,nosuid
cgroup          /sys/fs/cgroup/unified cgroup2    rw,relatime,nosuid,nodev,noexec
sysfs           /sys                  sysfs     rw,relatime,nosuid,nodev,noexec
tmpfs           /run/user/1000        tmpfs     rw,relatime,nosuid,nodev
/dev/loop1       /snap/amazon-ssm-agent/495 squashfs   ro,relatime,nodev
tmpfs           /run                  tmpfs     rw,relatime,nosuid,noexec
devpts          /dev/pts              devpts    rw,relatime,nosuid,noexec
systemd-1       /proc/sys/fs/binfmt_misc   autosys   rw,relatime
tmpfs           /dev/shm              tmpfs     rw,nosuid,nodev
cgroup          /sys/fs/cgroup/net_cls,net_prio cgroup    rw,relatime,nosuid,nodev,noexec
cgroup          /sys/fs/cgroup/hugetlb   cgroup    ro,relatime,nosuid,nodev,noexec
hugetlbfs       /dev/hugepages       hugetlbfs rw,relatime
tmpfs           /dev                  tmpfs     ro,nosuid,noexec
/dev/loop2       /snap/core/6130        squashfs  ro,relatime,nodev
tmpfs           /run/lock             tmpfs     rw,relatime,nosuid,nodev,noexec
/dev/loop3       /snap/amazon-ssm-agent/930  squashfs  ro,relatime,nodev
cgroup          /sys/fs/cgroup/cpuset    cgroup    rw,relatime,nosuid,nodev,noexec
tmpfs           /dev                  tmpfs     ro,nosuid,noexec
mqueue          /dev/mqueue            mqueue   rw,relatime
cgroup          /sys/fs/cgroup/devices  cgroup    rw,relatime,nosuid,nodev,noexec
cgroup          /sys/fs/cgroup/freezer   cgroup    rw,relatime,nosuid,nodev,noexec
securityfs     /sys/kernel/security   securityfs rw,relatime,nosuid,nodev,noexec
cgroup          /sys/fs/cgroup/blkio    cgroup    rw,relatime,nosuid,nodev,noexec
cgroup          /sys/fs/cgroup/cpu,cpuacct cgroup    ro,relatime,nosuid,nodev,noexec
cgroup          /sys/fs/cgroup/systemd  cgroup    ro,relatime,nosuid,nodev,noexec
cgroup          /sys/fs/cgroup/perf_event cgroup    rw,relatime,nosuid,nodev,noexec
debugfs         /sys/kernel/debug      debugfs   rw,relatime
configfs        /sys/kernel/config     configfs  rw,relatime
cgroup          /sys/fs/cgroup/memory   cgroup    rw,relatime,nosuid,nodev,noexec
cgroup          /sys/fs/cgroup/pids    cgroup    ro,relatime,nosuid,nodev,noexec
tmpfs           /var/lib/private      tmpfs     ro,nosuid,nodev,noexec
jrodg85@jrodg85-VirtualBox:~/volatility$
```

[Volver al texto de la imagen en la Sección 3.4.3.](#)

8.2.003.004.004.001. linux memmap.



[Volver al texto de la imagen en la Sección 3.4.4.](#)

8.2.003.004.005.001. linux iomem.

```
jrodg85@jrodg85-VirtualBox:~/volatility$ sudo python2.7 vol.py --profile=LinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_iomem
Volatility Foundation Volatility Framework 2.6.1
Reserved 0x0 0xFFFF
System RAM 0x1000 0x9DFFF
Reserved 0x9E000 0x9FFFF
PCI Bus 0000:00 0xA0000 0xBFFFF
Video ROM 0xC0000 0xC8BFF
Reserved 0xE0000 0xFFFFF
System ROM 0xF0000 0xFFFFF
System RAM 0x100000 0x3FFFFFFF
Kernel code 0x31C00000 0x328031D0
Kernel data 0x328031D1 0x33055EBF
Kernel bss 0x332C5000 0x33516FFF
PCI Bus 0000:00 0x00000000 0xFBFFFFFF
    0000:00:02.0 0xF0000000 0xF1FFFFFF
    0000:00:03.0 0xF2000000 0xF2FFFFFF
        xen-platform-pci 0xF2000000 0xF2FFFFFF
    0000:00:02.0 0xF3000000 0xF3000FFF
Reserved 0xFC000000 0xFFFFFFF
    IOAPIC 0 0xFEC00000 0xFEC003FF
    HPET 0 0xFED00000 0xFED003FF
    PNP0103:00 0xFED00000 0xFED003FF
    Local APIC 0x00000000 0x00000000
jrodg85@jrodg85-VirtualBox:~/volatility$
```

[Volver al texto de la imagen en la Sección 3.4.5.](#)

8.2.003.004.006.001. linux dmesg.

The screenshot shows a terminal window titled "jrodg85@jrodg85-VirtualBox: ~/volatility" with the following command and output:

```
jrodg85@jrodg85-VirtualBox:~/volatility$ sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_dmesg > /home/jrodg85/informe-linux_dmesg.txt
Volatility Foundation Volatility Framework 2.6.1
jrodg85@jrodg85-VirtualBox:~/volatility$
```

Below the terminal is a file properties dialog for "informe-linux_dmesg.txt". The "Básico" tab is selected, showing the following details:

	informe-linux_dmesg.txt
Tipo	documento de texto sencillo (text/plain)
Tamaño	45,2 kB (45.199 bytes)
Carpeta padre	/home/jrodg85
Accedido	jue 14 dic 2023 01:07:41
Modificación	jue 14 dic 2023 01:07:33
Creado	jue 14 dic 2023 01:07:27

[Volver al texto de la imagen en la Sección 3.4.5.](#)

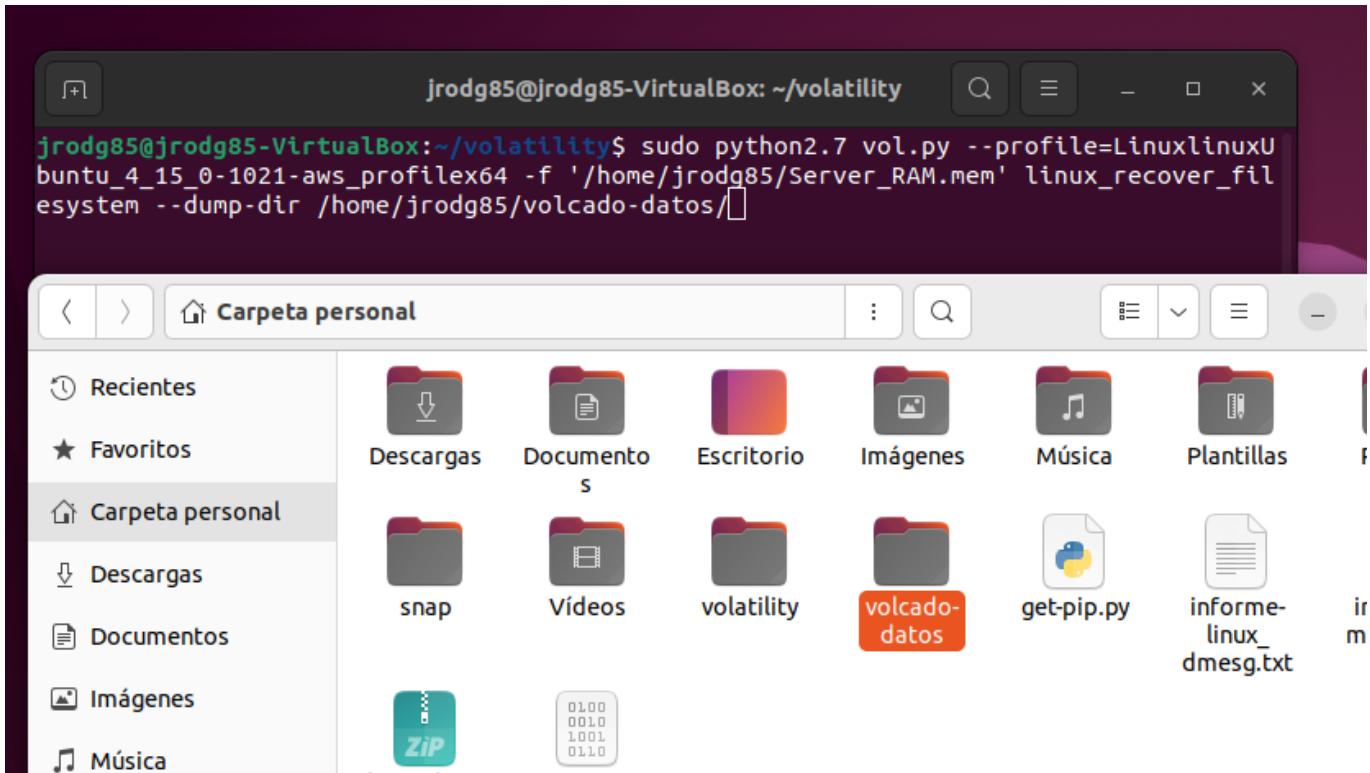
8.2.003.005.002.001. sudo nano etc passwd.

The screenshot shows a terminal window titled "jrodg85@jrodg85-VirtualBox: ~/volatility" displaying the contents of the "/etc/passwd" file using the "GNU nano 6.2" editor. The file contains the following entries:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

[Volver al texto de la imagen en la Sección 3.5.2.](#)

8.2.003.005.003.001. Volcado de datos.



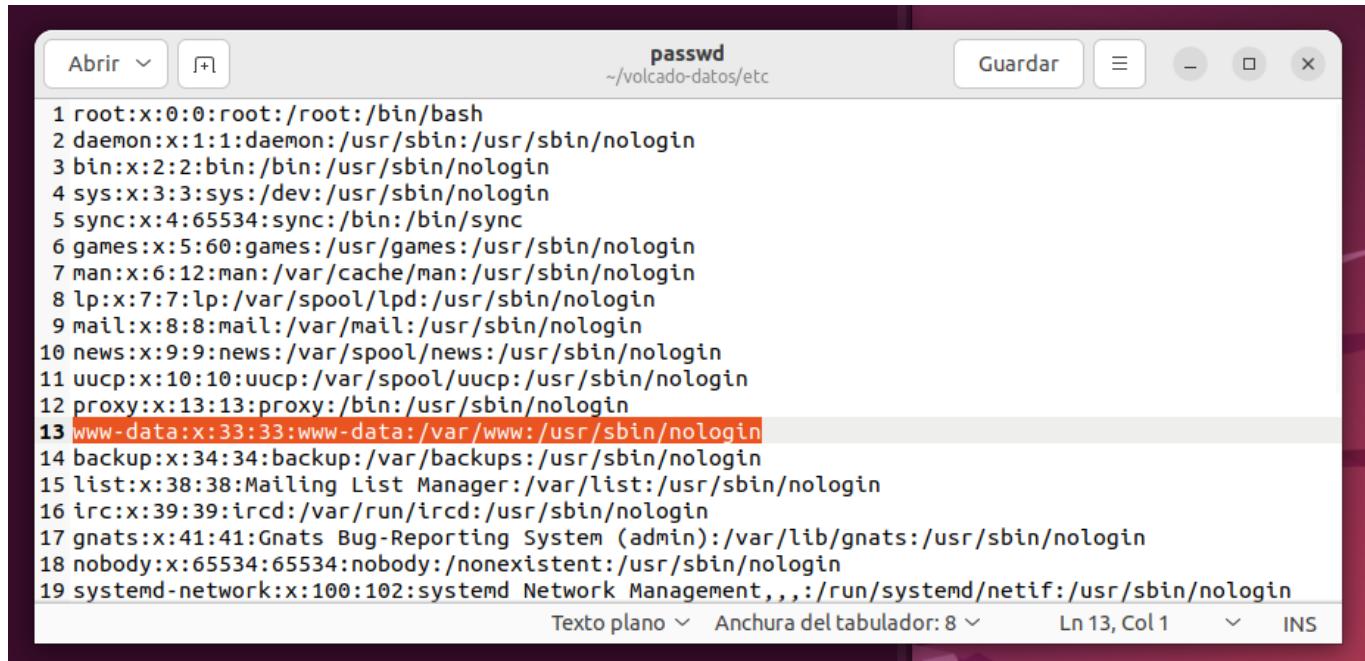
[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.002. cantidad de archivos recuperados.

```
multi internal
multi internal
Recovered 19117 files
jrodg85@jrodg85-VirtualBox:~/volatility$
```

[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.003. passwd de volcado.



```

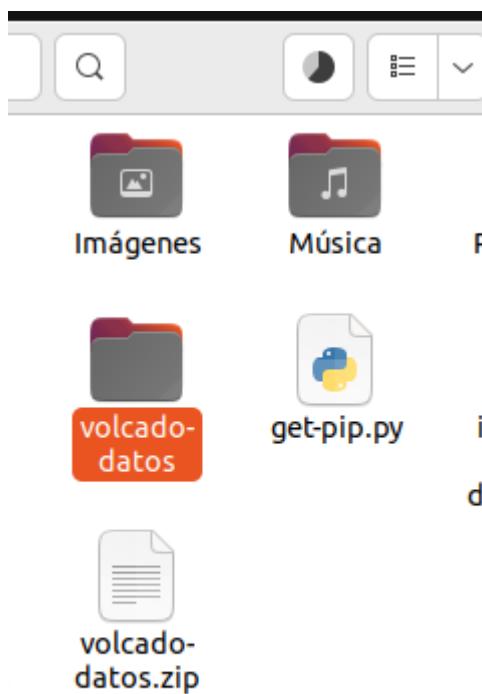
1 root:x:0:0:root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin

```

Texto plano ▾ Anchura del tabulador: 8 ▾ Ln 13, Col 1 ▾ INS

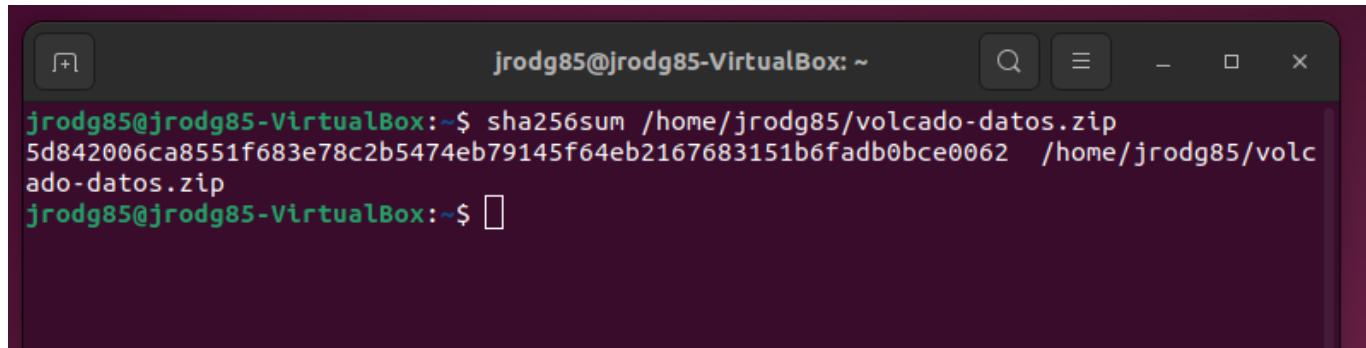
[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.004. Comprimiendo datos.



[Volver al texto de la imagen en la Sección 3.5.3.](#)

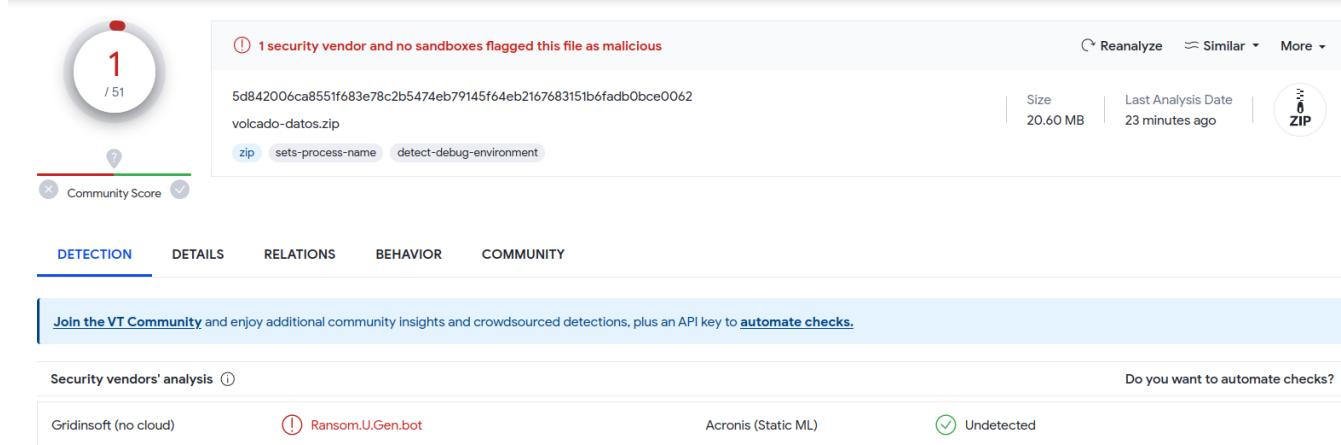
8.2.003.005.003.005. hash archivo zip.



```
jrodg85@jrodg85-VirtualBox:~$ sha256sum /home/jrodg85/volcado-datos.zip
5d842006ca8551f683e78c2b5474eb79145f64eb2167683151b6fadb0bce0062  /home/jrodg85/volcado-datos.zip
jrodg85@jrodg85-VirtualBox:~$
```

[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.006. Pantallazo Virustotal 1.



1 / 51

① 1 security vendor and no sandboxes flagged this file as malicious

5d842006ca8551f683e78c2b5474eb79145f64eb2167683151b6fadb0bce0062
volcado-datos.zip

zip sets-process-name detect-debug-environment

Size 20.60 MB | Last Analysis Date 23 minutes ago | ZIP

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ①

Gridinsoft (no cloud)	① Ransom.U.Gen.bot	Acronis (Static ML)	Undetected

Do you want to automate checks?

[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.007. Pantallazo Virustotal 2.

1 / 59

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

Security vendors' analysis

Gridinsoft (no cloud) Ransom.U.Gen.bot Acronis (Static ML) Undetected

```
jrodg85@jrodg85-VirtualBox:~$ sha256sum /home/jrodg85/zip/var.zip  
d2348d8ad77423705681bf4afaf28a18e6e2a12f400f948ac90f64b203a29e78 /home/jrodg85/zip/  
var.zip  
jrodg85@jrodg85-VirtualBox:~$
```

[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.008. Pantallazo Virustotal 3.

1 / 59

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

Security vendors' analysis

MAX Malware (ai Score=63) Acronis (Static ML) Undetected

```
jrodg85@jrodg85-VirtualBox:~/zip$ sha256sum /home/jrodg85/zip/lib.zip  
0a307ba2d022373fc539b6f76df4b17ca5d7e0c77420802ce3a72bb6ca4ead3 /home/jrodg85/  
zip/lib.zip  
jrodg85@jrodg85-VirtualBox:~/zip$
```

[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.009. Pantallazo Virustotal 4.

The screenshot shows the Virustotal analysis interface. At the top left, there's a circular progress bar with the number '1' and '/ 61'. To its right, a message says '1 security vendor and no sandboxes flagged this file as malicious'. Below this, the file details are listed: SHA256 hash (0192dba0ea584aa45de55e763554a020df475da4c2dbf084ba5ac43364029cbb), filename (www.zip), size (4.30), and type (zip). Below the file details, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. The DETECTION tab is selected. Under the DETECTION tab, it says 'Security vendors' analysis' and lists three vendors: Gridinsoft (no cloud) with a warning icon and 'Ransom.U.Gen.bot' detection, Acronis (Static ML) with a checkmark and 'Undetected', and another vendor with a checkmark and 'Undetected'. Below this, a terminal window shows the command 'sha256sum /home/jrodg85/zip/www.zip' being run, followed by the output: '0192dba0ea584aa45de55e763554a020df475da4c2dbf084ba5ac43364029cbb /home/jrodg85/zip/www.zip'. The terminal prompt 'jrodg85@jrodg85-VirtualBox:~/zip\$' is at the bottom.

[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.010. Pantallazo Virustotal 5.

1 / 60

Community Score

1 security vendor and no sandboxes flagged this file as malicious

850e3884f37b8e038f5452660077f65f73f4d0792384fbc4cbdeb2de97a5a98c
snapd.zip

zip

Size 224.15 K

DETECTION DETAILS RELATIONS COMMUNITY

Security vendors' analysis ⓘ

Antiy-AVL ⚠️ Trojan[ArcBomb]/Win32.Agent

Acronis (Static ML)

Undetected

Undetected

```
jrodg85@jrodg85-VirtualBox: ~/zip$ sha256sum /home/jrodg85/zip/nivel\ 2\ var\ lib/snapd.zip
850e3884f37b8e038f5452660077f65f73f4d0792384fbc4cbdeb2de97a5a98c  /home/jrodg85/
zip/nivel 2 var lib/snapd.zip
jrodg85@jrodg85-VirtualBox: ~/zip$
```

[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.011. Pantallazo Virustotal 6.

1 / 60

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

Security vendors' analysis ⓘ

Antiy-AVL ⚠️ Trojan[ArcBomb]/Win32.Agent Acronis (Static ML) Undete

```
jrodg85@jrodg85-VirtualBox: ~/zip$ sha256sum /home/jrodg85/zip/nivel\ 2\ var\ lib\nivel\ 3\ snapd/snaps.zip
94b364356cdc8201e4bfd9a015bf9b9fb62c5f5b1866713f1e6f0bb4c3443c40 /home/jrodg85/zip/nivel 2 var lib/nivel 3 snapd/snaps.zip
jrodg85@jrodg85-VirtualBox:~/zip$
```

[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.012. Pantallazo Virustotal 7.

1 / 60

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

Security vendors' analysis ⓘ

Gridinsoft (no cloud) ⚠️ Ransom.U.Gen.bot Acronis (Static ML) Undete

```
jrodg85@jrodg85-VirtualBox:~$ sha256sum /home/jrodg85/html/.htaccess
22b94c6893bfc091be2a9f454a045184df6c0398cffa2b4e90c0065dd6eeb1b0 /home/jrodg85/html/.htaccess
jrodg85@jrodg85-VirtualBox:~$
```

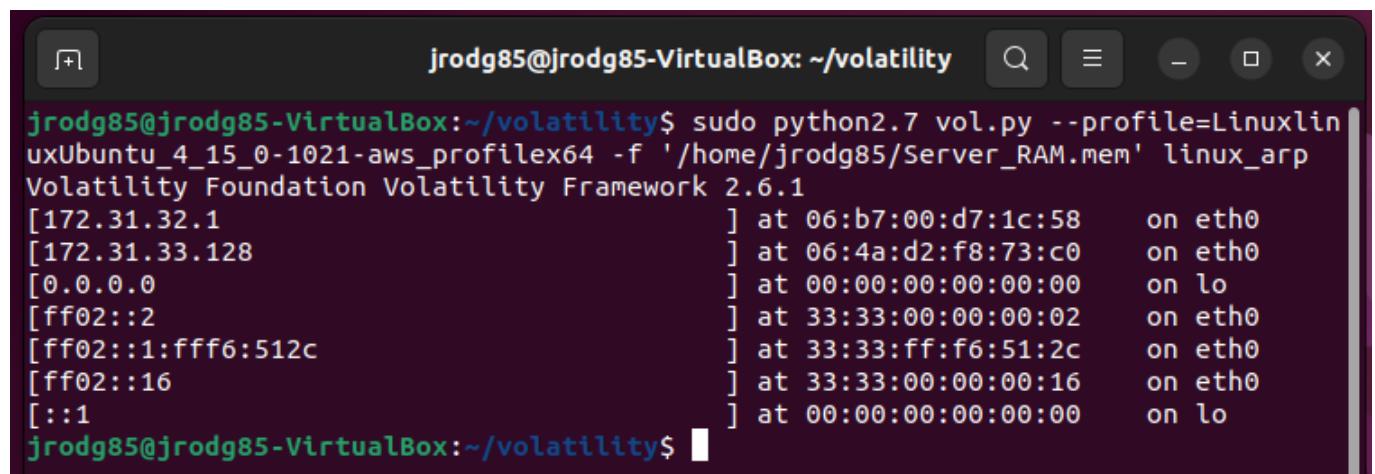
[Volver al texto de la imagen en la Sección 3.5.3.](#)

8.2.003.005.003.013. Archivo htaccess.

```
jrodg85@jrodg85-VirtualBox:~$ exiftool '/home/jrodg85/volcado-datos/var/www/html/.htaccess'
ExifTool Version Number      : 12.40
File Name                   : .htaccess
Directory                  : /home/jrodg85/volcado-datos/var/www/html
File Size                   : 235 bytes
File Modification Date/Time : 2018:12:21 19:24:40+01:00
File Access Date/Time       : 2023:12:16 22:00:09+01:00
File Inode Change Date/Time: 2023:12:16 21:10:46+01:00
File Permissions            : -rwxrwxrwx
Error                      : Entire file is binary zeros
jrodg85@jrodg85-VirtualBox:~$
```

[Volver al texto de la imagen en la Sección 3.5.3.](#)

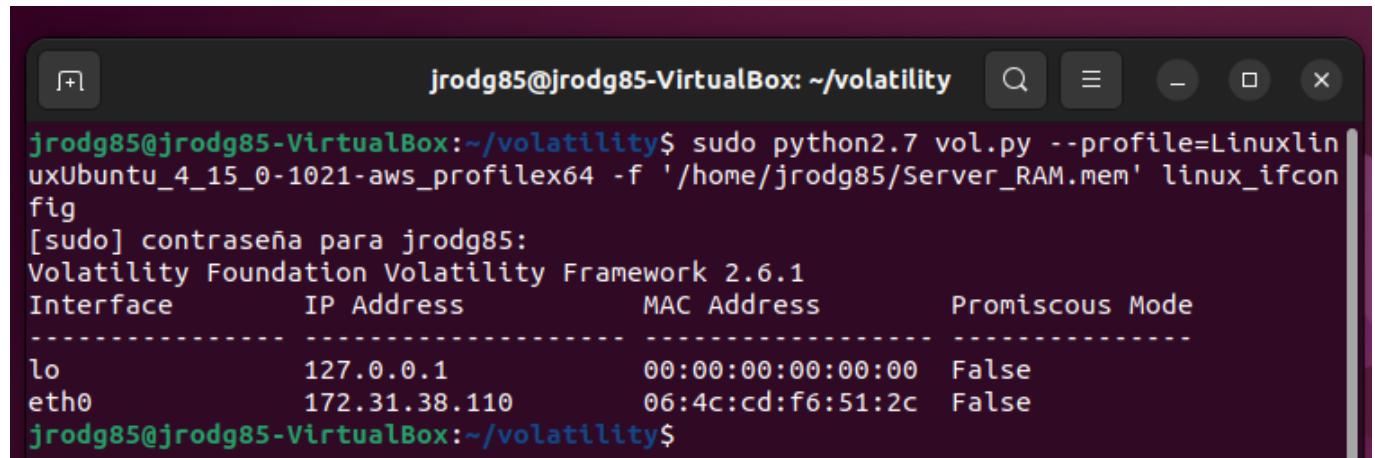
8.2.003.006.001.001. linux arp.



```
jrodg85@jrodg85-VirtualBox:~/volatility$ sudo python2.7 vol.py --profile=Linuxlin
uxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_arp
Volatility Foundation Volatility Framework 2.6.1
[172.31.32.1] at 06:b7:00:d7:1c:58 on eth0
[172.31.33.128] at 06:4a:d2:f8:73:c0 on eth0
[0.0.0.0] at 00:00:00:00:00:00 on lo
[ff02::2] at 33:33:00:00:00:02 on eth0
[ff02::1:ffff6:512c] at 33:33:ff:f6:51:2c on eth0
[ff02::16] at 33:33:00:00:00:16 on eth0
[::1] at 00:00:00:00:00:00 on lo
jrodg85@jrodg85-VirtualBox:~/volatility$
```

[Volver al texto de la imagen en la Sección 3.6.1.](#)

8.2.003.006.002.001. linux ifconfig.



```
jrodg85@jrodg85-VirtualBox:~/volatility$ sudo python2.7 vol.py --profile=Linuxlin
uxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_ifcon
fig
[sudo] contraseña para jrodg85:
Volatility Foundation Volatility Framework 2.6.1
Interface      IP Address        MAC Address        Promiscous Mode
-----
lo            127.0.0.1          00:00:00:00:00:00  False
eth0           172.31.38.110     06:4c:cd:f6:51:2c  False
jrodg85@jrodg85-VirtualBox:~/volatility$
```

[Volver al texto de la imagen en la Sección 3.6.2.](#)

8.2.004.001.001. Imagen Hash archivos.

The screenshot shows a Google Drive file titled 'Cálculo HASH.txt'. The content of the file is as follows:

```
Server_HDD.E01
*****
Acquisition hash MD5: 72d2cd59ff2167c501c67cc918d60d39

MD5: 324ed7db769620e3fb55c027480d0ef3
SHA1: 3398f90d2438230aaaf7b5e8ce0a01e456d9ca10

Server_RAM.mem
*****
MD5: 75a99b57032aa34ba19042ed85db273f
SHA1: cc1fad2af321b8c2ddf0103986e3b344eb8f2cc8
```

[Volver al texto de la imagen en la Sección 4.1.](#)

8.2.004.001.002. Imagen Hash PowerShell.

The screenshot shows a Windows PowerShell window. The command run is `Get-FileHash .\Server_HDD.E01 -Algorithm MD5`. The output is:

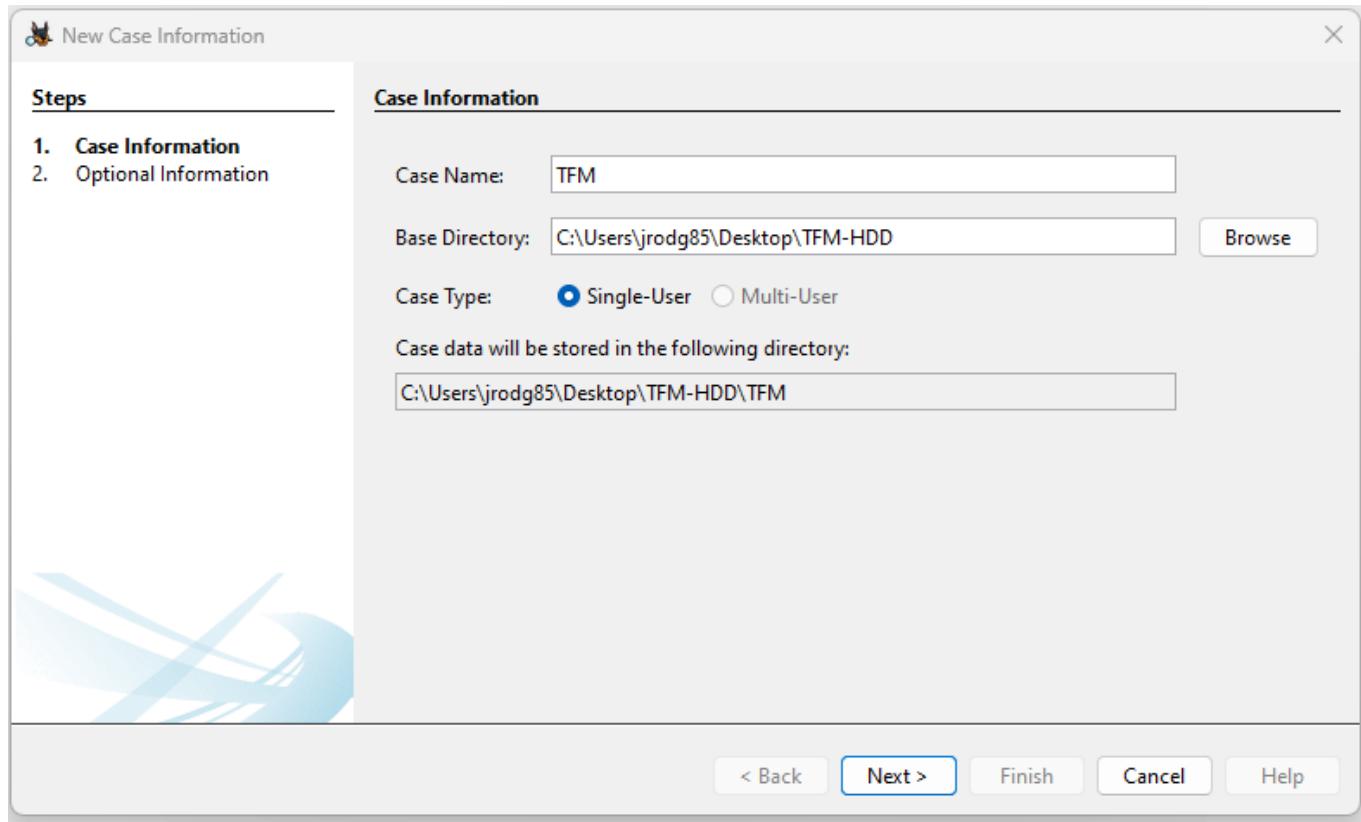
Algorithm	Hash	Path
MD5	324ED7DB769620E3FB55C027480D0EF3	C:\Users\jrodg85\Desktop\Nueva carpeta (2)\Server_HDD.E01

Then, the command `Get-FileHash .\Server_HDD.E01 -Algorithm SHA1` is run, and the output is:

Algorithm	Hash	Path
SHA1	3398F90D2438230AAAF7B5E8CE0A01E456D9CA10	C:\Users\jrodg85\Desktop\Nueva carpeta (2)\Server_HDD.E01

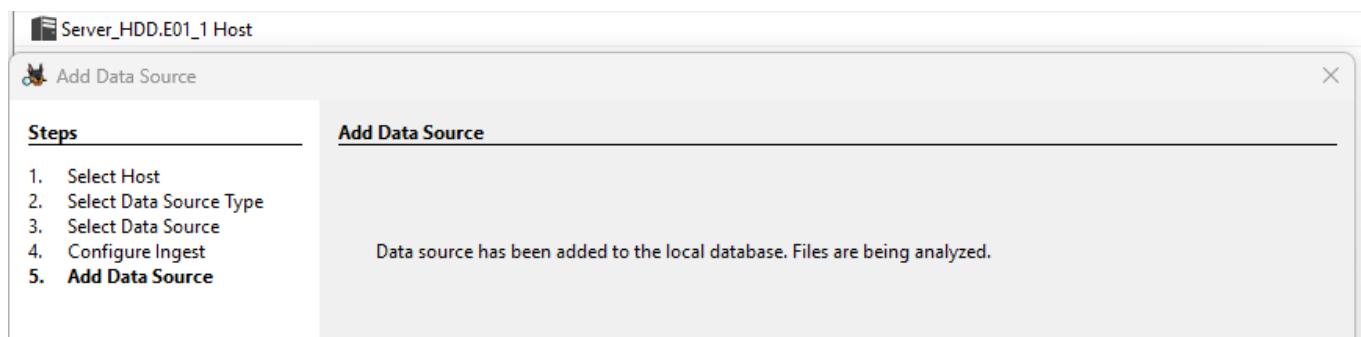
[Volver al texto de la imagen en la Sección 4.1.](#)

8.2.004.002.001. Nuevo caso Autopsy.



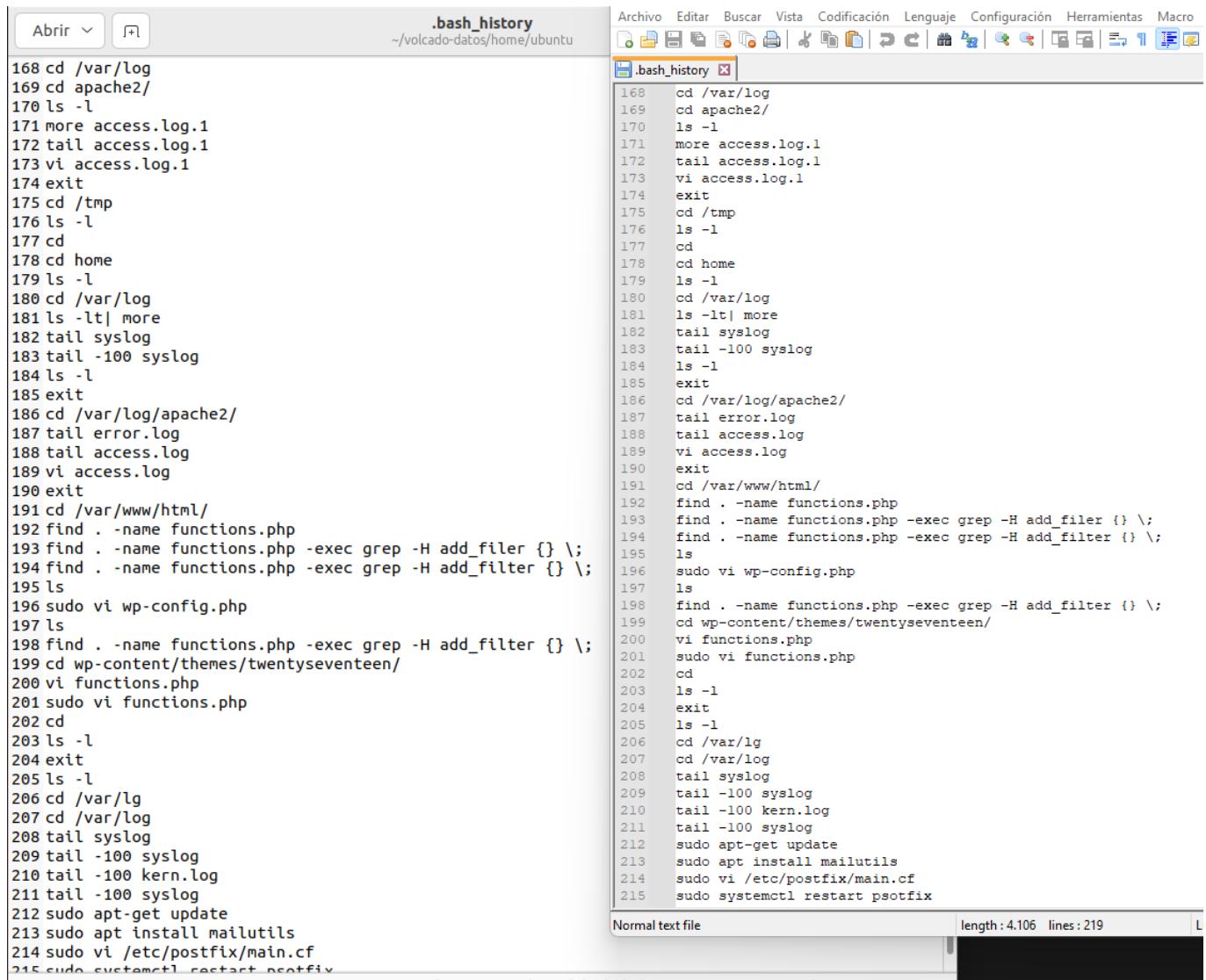
[Volver al texto de la imagen en la Sección 4.2.](#)

8.2.004.002.002. Caso Autopsy generado correctamente.



[Volver al texto de la imagen en la Sección 4.2.](#)

8.2.004.002.003. Comprobación bash history.



```

.bash_history
~/volcado-datos/home/ubuntu

168 cd /var/log
169 cd apache2/
170 ls -l
171 more access.log.1
172 tail access.log.1
173 vi access.log.1
174 exit
175 cd /tmp
176 ls -l
177 cd
178 cd home
179 ls -l
180 cd /var/log
181 ls -lt| more
182 tail syslog
183 tail -100 syslog
184 ls -l
185 exit
186 cd /var/log/apache2/
187 tail error.log
188 tail access.log
189 vi access.log
190 exit
191 cd /var/www/html/
192 find . -name functions.php
193 find . -name functions.php -exec grep -H add_filter {} \;
194 find . -name functions.php -exec grep -H add_filter {} \;
195 ls
196 sudo vi wp-config.php
197 ls
198 find . -name functions.php -exec grep -H add_filter {} \;
199 cd wp-content/themes/twentyseventeen/
200 vi functions.php
201 sudo vi functions.php
202 cd
203 ls -l
204 exit
205 ls -l
206 cd /var/lg
207 cd /var/log
208 tail syslog
209 tail -100 syslog
210 tail -100 kern.log
211 tail -100 syslog
212 sudo apt-get update
213 sudo apt install mailutils
214 sudo vi /etc/postfix/main.cf
215 sudo systemctl restart postfix

```

Normal text file length : 4.106 lines : 219

[Volver al texto de la imagen en la Sección 4.2.](#)

8.2.004.003.001. Usuarios del sistema.

/img_Server_HDD.E01/etc

Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access T
overlayroot.local.conf			0	2018-09-12 17:59:32 CEST	2018-09-12 18:10:08 CEST	2018-09-
pam.conf			0	2018-04-04 23:56:02 CEST	2018-09-12 18:10:08 CEST	2018-09-
passwd			1	2018-12-30 11:44:23 CET	2018-12-30 11:44:23 CET	2019-01-1
passwd-			1	2018-12-30 11:44:23 CET	2018-12-30 11:44:23 CET	2018-12-
popularity-contest.conf				2018-09-12 17:59:28 CEST	2018-09-12 18:10:08 CEST	2019-01-1
profile			1	2018-04-09 13:10:28 CEST	2018-09-12 18:10:08 CEST	2019-01-1
protocols			0	2016-12-26 02:56:39 CET	2018-09-12 18:10:08 CEST	2018-09-
rmt			0	2017-07-21 16:35:22 CEST	2018-09-12 18:10:08 CEST	2018-09-
rnc			0	2016-12-26 02:56:29 CET	2018-09-12 18:10:08 CEST	2018-09-

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations C

Strings Extracted Text Translation

Page: 1 of 1 Page ← → Go to Page:

```

root:x:0:0:root:/root/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:112:117::/var/spool/postfix:/usr/sbin/nologin

```

[Volver al texto de la imagen en la Sección 4.3.](#)

8.2.004.003.002. Análisis auth log 1.

```
jrodrig85@LAPTOP-688R5QV7: ~ % grep "user" auth.log
Dec 31 06:25:04 ip-172-31-38-110 CRON[31257]: pam_unix(cron:session): session closed for user root
Dec 31 06:26:19 ip-172-31-38-110 sshd[31531]: Disconnected from authenticating user root 113.228.245.4 port 35721 [preauth]
Dec 31 06:29:18 ip-172-31-38-110 sshd[31534]: Invalid user celery from 113.22.4.10 port 47532 [preauth]
Dec 31 06:29:41 ip-172-31-38-110 sshd[31536]: Disconnected from invalid user celery 113.22.4.10 port 47532 [preauth]
Dec 31 06:29:59 ip-172-31-38-110 sshd[31539]: Disconnected from authenticating user root 122.226.181.166 port 46726 [preauth]
Dec 31 06:32:08 ip-172-31-38-110 sshd[31542]: Disconnected from authenticating user root 36.156.24.96 port 34474 [preauth]
Dec 31 06:33:59 ip-172-31-38-110 sshd[31544]: Invalid user pi from 42.224.39.125 port 53156 [preauth]
Dec 31 06:34:01 ip-172-31-38-110 sshd[31544]: error: maximum authentication attempts exceeded for invalid user pi from 42.224.39.125 port 53156 ssh2 [preauth]
Dec 31 06:34:01 ip-172-31-38-110 sshd[31544]: Disconnecting invalid user pi 42.224.39.125 port 53158: Too many authentication failures [preauth]
Dec 31 06:34:39 ip-172-31-38-110 sshd[31547]: Disconnected from authenticating user root 122.226.181.167 port 57386 [preauth]
Dec 31 06:39:40 ip-172-31-38-110 sshd[31548]: Disconnected from authenticating user root 36.156.24.94 port 45294 [preauth]
Dec 31 06:39:50 ip-172-31-38-110 sshd[31551]: Disconnected from authenticating user root 122.226.181.167 port 44792 [preauth]
Dec 31 06:39:50 ip-172-31-38-110 CRON[31550]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 31 06:39:51 ip-172-31-38-110 CRON[31554]: pam_unix(cron:session): session closed for user root
Dec 31 06:41:01 ip-172-31-38-110 sshd[31625]: pam_unix(cron:session): session opened for user root 118.238.245.8 port 42688 [preauth]
Dec 31 06:41:01 ip-172-31-38-110 sshd[31629]: Disconnected from authenticating user root 118.238.245.8 port 42688 [preauth]
Dec 31 06:46:38 ip-172-31-38-110 sshd[31629]: Invalid user BasisK from 115.159.218.200 port 64920 [preauth]Dec 31 06:46:57 ip-172-31-38-110 sshd[31631]: Disconnected from authenticating user root 223.111.139.247 port 50652 [preauth]
Dec 31 06:48:37 ip-172-31-38-110 sshd[31729]: Disconnected from authenticating user root 58.242.83.7 port 40236 [preauth]
Dec 31 06:58:01 ip-172-31-38-110 sshd[31731]: Disconnected from authenticating user root 36.156.24.97 port 47589 [preauth]
Dec 31 06:51:21 ip-172-31-38-110 sshd[31733]: Disconnected from authenticating user root 36.156.24.95 port 45241 [preauth]
Dec 31 06:52:19 ip-172-31-38-110 sshd[31736]: Invalid user test from 159.95.146.154 port 59118 [preauth]
Dec 31 06:52:19 ip-172-31-38-110 sshd[31738]: Disconnected from authenticating user root 36.156.24.97 port 37967 [preauth]
Dec 31 06:53:19 ip-172-31-38-110 sshd[31740]: Disconnected from authenticating user root 122.226.181.167 port 37398 [preauth]
Dec 31 06:55:04 ip-172-31-38-110 sshd[31742]: Disconnected from authenticating user root 36.156.24.97 port 58571 [preauth]
Dec 31 06:55:40 ip-172-31-38-110 sshd[31744]: Invalid user asteriskuser from 201.76.162.152 port 35365
Dec 31 06:55:40 ip-172-31-38-110 sshd[31749]: Disconnected from invalid user asteriskuser 201.76.162.152 port 35365 [preauth]
Dec 31 07:00:57 ip-172-31-38-110 sshd[31749]: Disconnected from authenticating user root 122.226.181.167 port 35958 [preauth]
Dec 31 07:02:35 ip-172-31-38-110 sshd[31751]: Disconnected from authenticating user root 118.123.15.142 port 38372 [preauth]
Dec 31 07:05:44 ip-172-31-38-110 sshd[31754]: Disconnected from authenticating user root 115.238.245.4 port 46353 [preauth]
Dec 31 07:07:17 ip-172-31-38-110 sshd[31756]: Disconnected from authenticating user root 223.111.139.211 port 48602 [preauth]
Dec 31 07:07:35 ip-172-31-38-110 sshd[31758]: Disconnected from authenticating user root 36.156.24.93 port 33488 [preauth]
Dec 31 07:08:13 ip-172-31-38-110 sshd[31760]: Disconnected from authenticating user root 223.111.139.244 port 60184 [preauth]
Dec 31 07:08:38 ip-172-31-38-110 sshd[31762]: Disconnected from authenticating user root 61.184.247.6 port 41238 [preauth]
Dec 31 07:09:01 ip-172-31-38-110 CRON[31764]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 31 07:09:01 ip-172-31-38-110 CRON[31764]: pam_unix(cron:session): session closed for user root
Dec 31 07:18:15 ip-172-31-38-110 sshd[31834]: Disconnected from authenticating user root 36.156.24.97 port 43438 [preauth]
Dec 31 07:18:08 ip-172-31-38-110 sshd[31836]: Disconnected from authenticating user root 122.226.181.167 port 56278 [preauth]
Dec 31 07:18:32 ip-172-31-38-110 sshd[31838]: Disconnected from authenticating user root 61.184.247.4 port 57158 [preauth]
Dec 31 07:19:53 ip-172-31-38-110 sshd[31841]: Invalid user ur from 193.193.67.82 port 48226 [preauth]
Dec 31 07:19:53 ip-172-31-38-110 sshd[31841]: Disconnected from invalid user ur 193.193.67.82 port 48226 [preauth]
Dec 31 07:19:53 ip-172-31-38-110 sshd[31843]: Disconnected from authenticating user root 223.111.139.211 port 57588 [preauth]
Dec 31 07:19:53 ip-172-31-38-110 sshd[31845]: Disconnected from authenticating user root 36.156.24.95 port 43536 [preauth]
Dec 31 07:19:58 ip-172-31-38-110 sshd[31847]: Invalid user deploy from 181.188.268.46 port 43114 [preauth]
Dec 31 07:19:58 ip-172-31-38-110 sshd[31847]: Disconnected from invalid user deploy 181.188.268.46 port 43114 [preauth]
Dec 31 07:17:01 ip-172-31-38-110 CRON[31849]: pam_unix(cron:session): session opened for user root by (uid=0)
Dec 31 07:17:01 ip-172-31-38-110 CRON[31849]: pam_unix(cron:session): session closed for user root
Dec 31 07:18:16 ip-172-31-38-110 sshd[31852]: Disconnected from authenticating user root 36.156.24.97 port 54583 [preauth]
```

[Volver al texto de la imagen en la Sección 4.3.](#)

[Volver al Índice del capítulo 8. Anexos.](#)

[Volver al Índice General.](#)

8.3. Videos.

8.3.003.002.001. Video de instalación de Volatility en Ubuntu.



https://www.youtube.com/watch?v=dCU6klh0qSI&ab_channel=TFM-ANALISIS-FORENSE

[Volver al texto del video en la Sección 3.2.](#)

[Volver al texto del video en la Sección 3.3.2.](#)

[Volver al Índice del capítulo 8. Anexos.](#)

[Volver al Índice General.](#)

8.4. Extracto de comandos utilizados.

8.4.003.001.001. Comando Hash MD5.

```
Get-FileHash .\Server_RAM.mem -Algorithm MD5
```

La respuesta de PowerShell es el siguiente:

Algorithm	Hash
Path	-----
-----	-----
MD5	75A99B57032AA34BA19042ED85DB273F
D:\TFM\RAM\...	

[Volver al texto del comando en la Sección 3.1](#)

8.4.003.001.002. Comando Hash SHA1.

```
Get-FileHash .\Server_RAM.mem -Algorithm SHA1
```

La respuesta de PowerShell es el siguiente:

Algorithm	Hash
Path	-----
-----	-----
SHA1	CC1FAD2AF321B8C2DDF0103986E3B344EB8F2CC8
D:\TFM\RAM\...	

[Volver al texto del comando en la Sección 3.1.](#)

8.4.003.003.000.001. Comando sudo python2.7 vol.py --info.

```
sudo python2.7 vol.py --info
```

La respuesta de la shell es la siguiente:

Profiles

VistaSP0x64

- A Profile for Windows Vista SP0 x64

VistaSP0x86

- A Profile for Windows Vista SP0 x86

VistaSP1x64

- A Profile for Windows Vista SP1 x64

VistaSP1x86

- A Profile for Windows Vista SP1 x86

VistaSP2x64

- A Profile for Windows Vista SP2 x64

VistaSP2x86

- A Profile for Windows Vista SP2 x86

Win10x64

- A Profile for Windows 10 x64

Win10x64_10240_17770

(10.0.10240.17770 / 2018-02-10)

- A Profile for Windows 10 x64 (10.0.10586.306

/ 2016-04-23)

- A Profile for Windows 10 x64 (10.0.14393.0 /

2016-07-16)

- A Profile for Windows 10 x64 (10.0.15063.0 /

2017-04-04)

- A Profile for Windows 10 x64 (10.0.16299.0 /

2017-09-22)

- A Profile for Windows 10 x64 (10.0.17134.1 /

2018-04-11)

- A Profile for Windows 10 x64 (10.0.17763.0 /

2018-10-12)

- A Profile for Windows 10 x64 (10.0.18362.0 /

2019-04-23)

- A Profile for Windows 10 x64 (10.0.19041.0 /

2020-04-17)

- A Profile for Windows 10 x86

Win10x86_10240_17770

(10.0.10240.17770 / 2018-02-10)

- A Profile for Windows 10 x86 (10.0.10586.420

/ 2016-05-28)

- A Profile for Windows 10 x86 (10.0.14393.0 /

2016-07-16)

- A Profile for Windows 10 x86 (10.0.15063.0 /

2017-04-04)

- A Profile for Windows 10 x86 (10.0.16299.15

/ 2017-09-29)

- A Profile for Windows 10 x86 (10.0.17134.1 /

2018-04-11)

- A Profile for Windows 10 x86 (10.0.17763.0 /

2018-10-12)

- A Profile for Windows 10 x86 (10.0.18362.0 /

2019-04-23)

- A Profile for Windows 10 x86 (10.0.19041.0 /

2020-04-17)

- A Profile for Windows 2003 SP0 x86

Win2003SP1x64

- A Profile for Windows 2003 SP1 x64

Win2003SP1x86

- A Profile for Windows 2003 SP1 x86

Win2003SP2x64

- A Profile for Windows 2003 SP2 x64

Win2003SP2x86

- A Profile for Windows 2003 SP2 x86

Win2008R2SP0x64

- A Profile for Windows 2008 R2 SP0 x64

Win2008R2SP1x64

- A Profile for Windows 2008 R2 SP1 x64

Win2008R2SP1x64_23418 (6.1.7601.23418 / 2016-04-09)	- A Profile for Windows 2008 R2 SP1 x64
Win2008R2SP1x64_24000 (6.1.7601.24000 / 2016-04-09)	- A Profile for Windows 2008 R2 SP1 x64
Win2008SP1x64	- A Profile for Windows 2008 SP1 x64
Win2008SP1x86	- A Profile for Windows 2008 SP1 x86
Win2008SP2x64	- A Profile for Windows 2008 SP2 x64
Win2008SP2x86	- A Profile for Windows 2008 SP2 x86
Win2012R2x64	- A Profile for Windows Server 2012 R2 x64
Win2012R2x64_18340 (6.3.9600.18340 / 2016-05-13)	- A Profile for Windows Server 2012 R2 x64
Win2012x64	- A Profile for Windows Server 2012 x64
Win2016x64_14393 (10.0.14393.0 / 2016-07-16)	- A Profile for Windows Server 2016 x64
Win7SP0x64	- A Profile for Windows 7 SP0 x64
Win7SP0x86	- A Profile for Windows 7 SP0 x86
Win7SP1x64	- A Profile for Windows 7 SP1 x64
Win7SP1x64_23418 (6.1.7601.23418 / 2016-04-09)	- A Profile for Windows 7 SP1 x64
Win7SP1x64_24000 (6.1.7601.24000 / 2018-01-09)	- A Profile for Windows 7 SP1 x64
Win7SP1x86	- A Profile for Windows 7 SP1 x86
Win7SP1x86_23418 (6.1.7601.23418 / 2016-04-09)	- A Profile for Windows 7 SP1 x86
Win7SP1x86_24000 (6.1.7601.24000 / 2018-01-09)	- A Profile for Windows 7 SP1 x86
Win81U1x64	- A Profile for Windows 8.1 Update 1 x64
Win81U1x86	- A Profile for Windows 8.1 Update 1 x86
Win8SP0x64	- A Profile for Windows 8 x64
Win8SP0x86	- A Profile for Windows 8 x86
Win8SP1x64	- A Profile for Windows 8.1 x64
Win8SP1x64_18340 (6.3.9600.18340 / 2016-05-13)	- A Profile for Windows 8.1 x64
Win8SP1x86	- A Profile for Windows 8.1 x86
WinXPSP1x64	- A Profile for Windows XP SP1 x64
WinXPSP2x64	- A Profile for Windows XP SP2 x64
WinXPSP2x86	- A Profile for Windows XP SP2 x86
WinXPSP3x86	- A Profile for Windows XP SP3 x86

[Volver al texto del comando en la Sección 3.3.0.](#)

8.4.003.003.002.001. Comando sudo history > usb/historial.txt.

```
history > usb/historial.txt
```

Se ha guardado en el archivo `/home/jrodg85/usb/historial.txt` el siguiente historial de acciones de la consola:

```
1 sudo apt update
2 sudo apt upgrade
3 sudo apt install zip
4 sudo apt install git
5 sudo apt install make
6 sudo apt install dwarfdump
7 sudo apt-cache search linux-image | grep 4.15.0-1021-aws
8 sudo apt install linux-image-4.15.0-1021-aws
9 sudo reboot now
10 uname -r
11 hostnamectl
12 sudo apt install build-essential
13 sudo apt update
14 sudo apt install linux-headers-$(uname -r)
15 sudo apt install python2.7 python2.7-dev
16 sudo snap install curl
17 dpkg -l python2.7
18 curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
19 sudo python2.7 get-pip.py
20 sudo pip2.7 --version
21 git clone https://github.com/volatilityfoundation/volatility.git
22 sudo pip2.7 install distorm3
23 sudo pip2.7 list
24 sudo pip2.7 install yara-python==3.8.1
25 sudo pip2.7 list
26 sudo pip2.7 install pycrypto
27 sudo pip2.7 list
28 sudo pip2.7 install Pillow
29 sudo pip2.7 list
30 sudo pip2.7 install openpyxl==2.6.4
31 sudo pip2.7 list
32 sudo pip2.7 install ujson
33 sudo pip2.7 list
34 cd volatility/
35 sudo python2.7 setup.py install
36 sudo python2.7 vol.py --info
37 cd tools/linux/
38 make
39 cd ..
40 cd ../..
41 lsb_release -si
42 uname -r
43 clear
44 sudo zip linux$(lsb_release -si)_$(uname -r)_profile.zip
/home/jrodg85/volatility/tools/linux/module.dwarf /boot/System.map-4.15.0-1021-aws
45 mkdir usb
46 ls
47 sudo mount /dev/sdb usb/
48 cp linuxUbuntu_4.15.0-1021-aws_profile.zip usb/
49 touch usb/historial.txt
50 history > usb/historial.txt
```

[Volver al texto del comando en la Sección 3.3.2](#)

8.4.003.004.003.001. Comando sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_mount.

```
sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f  
'/home/jrodg85/Server_RAM.mem' linux_mount
```

La respuesta de volatility ha sido la siguiente

```
Volatility Foundation Volatility Framework 2.6.1

cgroup           /sys/fs/cgroup/rdma           cgroup
rw,relatime,nosuid,nodev,noexec

tmpfs            /sys/fs/cgroup               tmpfs
ro,nosuid,nodev,noexec

/dev/xvda1        /                         ext4
ro,relatime

proc              /bus                      proc
ro,relatime,nosuid,nodev,noexec

pstore            /sys/fs/pstore             pstore
rw,relatime,nosuid,nodev,noexec

fusectl          /sys/fs/fuse/connections   fusectl
rw,relatime

lxcfs             /var/lib/lxcfs            fuse
ro,relatime,nosuid,nodev

/dev/loop0         /snap/core/5328          squashfs
ro,relatime,nodev

udev              /dev                      devtmpfs
rw,relatime,nosuid

cgroup            /sys/fs/cgroup/unified    cgroup2
rw,relatime,nosuid,nodev,noexec

sysfs             /sys                      sysfs
rw,relatime,nosuid,nodev,noexec

tmpfs              /run/user/1000          tmpfs
rw,relatime,nosuid,nodev

/dev/loop1         /snap/amazon-ssm-agent/495 squashfs
```

ro,relatime,nodev		
tmpfs	/run	tmpfs
rw,relatime,nosuid,noexec		
devpts	/dev/pts	devpts
rw,relatime,nosuid,noexec		
systemd-1	/proc/sys/fs/binfmt_misc	autofs
rw,relatime		
tmpfs	/dev/shm	tmpfs
rw,nosuid,nodev		
cgroup	/sys/fs/cgroup/net_cls,net_prio	cgroup
rw,relatime,nosuid,nodev,noexec		
cgroup	/sys/fs/cgroup/hugetlb	cgroup
ro,relatime,nosuid,nodev,noexec		
hugetlbfs	/dev/hugepages	hugetlbfs
rw,relatime		
tmpfs	/dev	tmpfs
ro,nosuid,noexec		
/dev/loop2	/snap/core/6130	squashfs
ro,relatime,nodev		
tmpfs	/run/lock	tmpfs
rw,relatime,nosuid,nodev,noexec		
/dev/loop3	/snap/amazon-ssm-agent/930	squashfs
ro,relatime,nodev		
cgroup	/sys/fs/cgroup/cpuset	cgroup
rw,relatime,nosuid,nodev,noexec		
tmpfs	/dev	tmpfs
ro,nosuid,noexec		
mqueue	/dev/mqueue	mqueue
rw,relatime		
cgroup	/sys/fs/cgroup/devices	cgroup
rw,relatime,nosuid,nodev,noexec		
cgroup	/sys/fs/cgroup/freezer	cgroup
rw,relatime,nosuid,nodev,noexec		
securityfs	/sys/kernel/security	securityfs
rw,relatime,nosuid,nodev,noexec		
cgroup	/sys/fs/cgroup/blkio	cgroup

```

rw,relatime,nosuid,nodev,noexec

cgroup           /sys/fs/cgroup/cpu,cpuacct      cgroup
ro,relatime,nosuid,nodev,noexec

cgroup           /sys/fs/cgroup/systemd        cgroup
ro,relatime,nosuid,nodev,noexec

cgroup           /sys/fs/cgroup/perf_event    cgroup
rw,relatime,nosuid,nodev,noexec

debugfs          /sys/kernel/debug            debugfs
rw,relatime

configfs         /sys/kernel/config          configfs
rw,relatime

cgroup           /sys/fs/cgroup/memory       cgroup
rw,relatime,nosuid,nodev,noexec

cgroup           /sys/fs/cgroup/pids        cgroup
ro,relatime,nosuid,nodev,noexec

tmpfs            /var/lib/private           tmpfs
ro,nosuid,nodev,noexec

```

Procesado el comando, se puede obtener esta tabla resumen:

Punto de Montaje	Dispositivo o Sistema de Archivos	Tipo	Opciones de Montaje
cgroup	/sys/fs/cgroup/rdma	cgroup	rw,relatime,nosuid,nodev,noexec
tmpfs	/sys/fs/cgroup	tmpfs	ro,nosuid,nodev,noexec
/dev/xvda1	/	ext4	ro,relatime
proc	/bus	proc	ro,relatime,nosuid,nodev,noexec
pstore	/sys/fs/pstore	pstore	rw,relatime,nosuid,nodev,noexec
fusectl	/sys/fs/fuse/connections	fusectl	rw,relatime
lxcfs	/var/lib/lxcfs	fuse	ro,relatime,nosuid,nodev
/dev/loop0	/snap/core/5328	squashfs	ro,relatime,nodev
udev	/dev	devtmpfs	rw,relatime,nosuid
cgroup	/sys/fs/cgroup/unified	cgroup2	rw,relatime,nosuid,nodev,noexec
sysfs	/sys	sysfs	rw,relatime,nosuid,nodev,noexec
tmpfs	/run/user/1000	tmpfs	rw,relatime,nosuid,nodev

Punto de Montaje	Dispositivo o Sistema de Archivos	Tipo	Opciones de Montaje
/dev/loop1	/snap/amazon-ssm-agent/495	squashfs	ro,relatime,nodev
tmpfs	/run	tmpfs	rw,relatime,nosuid,noexec
devpts	/dev/pts	devpts	rw,relatime,nosuid,noexec
systemd-1	/proc/sys/fs/binfmt_misc	autofs	rw,relatime
tmpfs	/dev/shm	tmpfs	rw,nosuid,nodev
cgroup	/sys/fs/cgroup/net_cls,net_prio	cgroup	rw,relatime,nosuid,nodev,noexec
cgroup	/sys/fs/cgroup/hugetlb	cgroup	ro,relatime,nosuid,nodev,noexec
hugetlbfs	/dev/hugepages	hugetlbfs	rw,relatime
tmpfs	/dev	tmpfs	ro,nosuid,noexec
/dev/loop2	/snap/core/6130	squashfs	ro,relatime,nodev
tmpfs	/run/lock	tmpfs	rw,relatime,nosuid,nodev,noexec
/dev/loop3	/snap/amazon-ssm-agent/930	squashfs	ro,relatime,nodev
cgroup	/sys/fs/cgroup/cpuset	cgroup	rw,relatime,nosuid,nodev,noexec
tmpfs	/dev	tmpfs	ro,nosuid,noexec
mqueue	/dev/mqueue	mqueue	rw,relatime
cgroup	/sys/fs/cgroup/devices	cgroup	rw,relatime,nosuid,nodev,noexec
cgroup	/sys/fs/cgroup/freezer	cgroup	rw,relatime,nosuid,nodev,noexec
securityfs	/sys/kernel/security	securityfs	rw,relatime,nosuid,nodev,noexec
cgroup	/sys/fs/cgroup/blkio	cgroup	rw,relatime,nosuid,nodev,noexec
cgroup	/sys/fs/cgroup/cpu,cpuacct	cgroup	ro,relatime,nosuid,nodev,noexec
cgroup	/sys/fs/cgroup/systemd	cgroup	ro,relatime,nosuid,nodev,noexec
cgroup	/sys/fs/cgroup/perf_event	cgroup	rw,relatime,nosuid,nodev,noexec
debugfs	/sys/kernel/debug	debugfs	rw,relatime
configfs	/sys/kernel/config	configfs	rw,relatime
cgroup	/sys/fs/cgroup/memory	cgroup	rw,relatime,nosuid,nodev,noexec
cgroup	/sys/fs/cgroup/pids	cgroup	ro,relatime,nosuid,nodev,noexec
tmpfs	/var/lib/private	tmpfs	ro,nosuid,nodev,noexec

[Volver al texto del comando en la Sección 3.4.3.](#)

8.4.003.004.004.001. Comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_memmap > /home/jrodg85/informe-memmap.txt`.

```
sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f
'/home/jrodg85/Server_RAM.mem' linux_memmap > /home/jrodg85/informe-memmap.txt
```

Tras una limpieza de datos se obtiene la siguiente información.

Task	Pid	Virtual
systemd	1	0x000056198f210000
Unable to read pages for kthreadd pid 2.		
Unable to read pages for kworker/0:0H pid 4.		
Unable to read pages for mm_percpu_wq pid 6.		
Unable to read pages for ksoftirqd/0 pid 7.		
Unable to read pages for rcu_sched pid 8.		
Unable to read pages for rcu_bh pid 9.		
Unable to read pages for migration/0 pid 10.		
Unable to read pages for watchdog/0 pid 11.		
Unable to read pages for cpuhp/0 pid 12.		
Unable to read pages for kdevtmpfs pid 13.		
Unable to read pages for netns pid 14.		
Unable to read pages for rcu_tasks_kthre pid 15.		
Unable to read pages for kauditfd pid 16.		
Unable to read pages for xenbus pid 17.		
Unable to read pages for xenwatch pid 18.		
Unable to read pages for khungtaskd pid 20.		
Unable to read pages for oom_reaper pid 21.		
Unable to read pages for writeback pid 22.		
Unable to read pages for kcompactd0 pid 23.		
Unable to read pages for ksmd pid 24.		
Unable to read pages for khugepaged pid 25.		
Unable to read pages for crypto pid 26.		
Unable to read pages for kintegrityd pid 27.		
Unable to read pages for kblockd pid 28.		
Unable to read pages for ata_sff pid 29.		
Unable to read pages for md pid 30.		
Unable to read pages for edac-poller pid 31.		
Unable to read pages for devfreq_wq pid 32.		
Unable to read pages for watchdog pid 33.		
Unable to read pages for kswapd0 pid 36.		
Unable to read pages for ecryptfs-kthrea pid 37.		
Unable to read pages for kthrotld pid 79.		
Unable to read pages for nvme-wq pid 80.		
Unable to read pages for scsi_eh_0 pid 81.		
Unable to read pages for scsi_tmf_0 pid 82.		
Unable to read pages for scsi_eh_1 pid 83.		
Unable to read pages for scsi_tmf_1 pid 84.		
Unable to read pages for ipv6_addrconf pid 89.		

```
Unable to read pages for kstrp pid 99.
Unable to read pages for kworker/0:1H pid 100.
Unable to read pages for raid5wq pid 280.
Unable to read pages for jbd2/xvda1-8 pid 330.
Unable to read pages for ext4-rsv-conver pid 331.
Unable to read pages for iscsi_eh pid 395.
Unable to read pages for ib-comp-wq pid 408.
Unable to read pages for ib_mcast pid 409.
Unable to read pages for ib_nl_sa_wq pid 410.
lvmtdad 414 0x000055c919805000
Unable to read pages for rdma_cm pid 415.
systemd-logind 712 0x0000555feb5b1000
dbus-daemon 720 0x000055e82c96e000
cron 733 0x000055da6b87f000
accounts-daemon 734 0x00005622d937a000
lxcfs 737 0x0000559f4b3c0000
atd 749 0x00005617c519f000
polkitd 771 0x000055e2bdf70000
agetty 785 0x0000561ce77d2000
Unable to read pages for loop0 pid 951.
Unable to read pages for loop1 pid 1103.
systemd-network 2788 0x000056528aefc000
systemd-resolve 2804 0x0000556117890000
systemd-timesyn 2818 0x000055ec03062000
systemd-journal 2825 0x000055788deea000
uuidd 5077 0x00005626dc1f7000
systemd-udevd 5160 0x000055db9d680000
Unable to read pages for xfsalloc pid 10374.
Unable to read pages for xfs_mru_cache pid 10375.
iscsid 10988 0x0000556f3766c000
networkd-dispat 11199 0x000000000040b000
sshd 12159 0x000055ced2c2b000
mysqld 5127 0x0000000000758000
apache2 5469 0x0000555836828000
Unable to read pages for loop2 pid 6189.
snapd 6219 0x000000c000000000
Unable to read pages for loop3 pid 6349.
amazon-ssm-agen 6445 0x0000000000401000
rsyslogd 26254 0x000055a525c04000
master 26489 0x0000560cfcc179000
qmgr 26500 0x00005561e4c3e000
Unable to read pages for kworker/0:0 pid 19056.
Unable to read pages for kworker/u30:2 pid 19454.
apache2 19704 0x0000555836828000
apache2 19705 0x0000555836828000
apache2 19706 0x0000555836828000
apache2 19707 0x0000555836828000
apache2 19708 0x0000555836828000
Unable to read pages for kworker/0:1 pid 19709.
apache2 19952 0x0000555836828000
apache2 19953 0x0000555836828000
apache2 20230 0x0000555836828000
apache2 20231 0x0000555836828000
apache2 20232 0x0000555836828000
```

```

apache2          20233 0x0000555836828000
Unable to read pages for sh pid 20381.
sshd            20483 0x0000556d21d8b000
systemd          20485 0x000055cc54c92000
(sd-pam)         20486 0x000056198f210000
sshd            20576 0x0000556d21d90000
bash             20577 0x000055931a312000
pickup           20703 0x00005566d1a50000
Unable to read pages for kworker/u30:1 pid 20781.
Unable to read pages for kworker/u30:0 pid 20886.
sudo             20893 0x000055c043a14000
insmod          20894 0x00005620e496f000
Unable to read pages for kworker/0:2 pid 20898.

```

[Volver al texto del comando en la Sección 3.4.4.](#)

8.4.003.004.005.001. Comando sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_iomem.

```

sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f
'/home/jrodg85/Server_RAM.mem' linux_iomem

```

La respuesta de la consola ha sido la siguiente:

```

Volatility Foundation Volatility Framework 2.6.1
Reserved          0x0          0xFFFF
System RAM        0x1000      0x9DFFF
Reserved          0x9E000     0x9FFFF
PCI Bus 0000:00   0xA0000     0xBFFFF
Video ROM         0xC0000     0xC8BFF
Reserved          0xE0000     0xFFFFFFF
    System ROM    0xF0000     0xFFFFFFF
System RAM        0x100000    0x3FFFFFFF
    Kernel code   0x31C00000  0x328031D0
    Kernel data   0x328031D1  0x33055EBF
    Kernel bss    0x332C5000  0x33516FFF
PCI Bus 0000:00   0xF0000000  0xFBFFFFFF
    0000:00:02.0   0xF0000000  0xF1FFFFFF
    0000:00:03.0   0xF2000000  0xF2FFFFFF
    xen-platform-pci 0xF2000000  0xF2FFFFFF
    0000:00:02.0   0xF3000000  0xF3000FFF
Reserved          0xFC000000  0xFFFFFFFF
    IOAPIC 0       0xFEC00000  0xFEC003FF
    HPET 0         0xFED00000  0xFED003FF
    PNP0103:00    0xFED00000  0xFED003FF
    Local APIC    0xFEE00000  0xFEE00FFF

```

[Volver al texto del comando en la Sección 3.4.5.](#)

8.4.003.004.006.001. Comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_dmesg > /home/jrodg85/informe-linux_dmesg.txt`.

```
sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f  
'/home/jrodg85/Server_RAM.mem' linux_dmesg > /home/jrodg85/informe-linux_dmesg.txt
```

La respuesta del comando en el archivo de texto fue el siguiente:

```
[0.0] Linux version 4.15.0-1021-aws (buildd@lcy01-amd64-001) (gcc version 7.3.0  
(Ubuntu 7.3.0-16ubuntu3)) #21-Ubuntu SMP Tue Aug 28 10:23:07 UTC 2018 (Ubuntu  
4.15.0-1021.21-aws 4.15.18)  
[0.0] Command line: BOOT_IMAGE=/boot/vmlinuz-4.15.0-1021-aws root=LABEL=cloudimg-  
rootfs ro console=tty1 console=ttyS0 nvme.io_timeout=4294967295  
[0.0] KERNEL supported cpus:  
[0.0]   Intel GenuineIntel  
[0.0]   AMD AuthenticAMD  
[0.0]   Centaur CentaurHauls  
[0.0] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'  
[0.0] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'  
[0.0] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'  
[0.0] x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256  
[0.0] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using  
'standard' format.  
[0.0] e820: BIOS-provided physical RAM map:  
[0.0] BIOS-e820: [mem 0x0000000000000000-0x000000000009ffff] usable  
[0.0] BIOS-e820: [mem 0x000000000009e000-0x000000000009ffff] reserved  
[0.0] BIOS-e820: [mem 0x0000000000e0000-0x0000000000ffff] reserved  
[0.0] BIOS-e820: [mem 0x0000000000100000-0x0000000003ffffffff] usable  
[0.0] BIOS-e820: [mem 0x00000000fc000000-0x00000000ffffffff] reserved  
[0.0] NX (Execute Disable) protection: active  
[0.0] SMBIOS 2.7 present.  
[0.0] DMI: Xen HVM domU, BIOS 4.2.amazon 08/24/2006  
[0.0] Hypervisor detected: Xen HVM  
[0.0] Xen version 4.2.  
[0.0] Xen Platform PCI: I/O protocol version 1  
[0.0] Netfront and the Xen platform PCI driver have been compiled for this kernel:  
unplug emulated NICs.  
[0.0] Blkfront and the Xen platform PCI driver have been compiled for this kernel:  
unplug emulated disks.  
You might have to change the root device  
from /dev/hd[a-d] to /dev/xvd[a-d]  
in your root= kernel command line option  
[0.0] HVMOP_pagetable_dying not supported  
[0.0] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved  
[0.0] e820: remove [mem 0x000a0000-0x000fffff] usable  
[0.0] e820: last_pfn = 0x40000 max_arch_pfn = 0x400000000
```

```
[0.0] MTRR default type: write-back
[0.0] MTRR fixed ranges enabled:
[0.0]   00000-9FFFF write-back
[0.0]   A0000-BFFFF write-combining
[0.0]   C0000-FFFFF write-back
[0.0] MTRR variable ranges enabled:
[0.0]   0 base 0000F0000000 mask 3FFFF8000000 uncachable
[0.0]   1 base 0000F8000000 mask 3FFFC000000 uncachable
[0.0]   2 disabled
[0.0]   3 disabled
[0.0]   4 disabled
[0.0]   5 disabled
[0.0]   6 disabled
[0.0]   7 disabled
[0.0] x86/PAT: Configuration [0-7]: WB WC UC- UC WB WP UC- WT
[0.0] found SMP MP-table at [mem 0x000fbcc50-0x000fbcc5f] mapped at [
(ptrval)]
[0.0] Scanning 1 areas for low memory corruption
[0.0] Base memory trampoline at [           (ptrval)] 98000 size 24576
[0.0] BRK [0x33518000, 0x33518fff] PGTABLE
[0.0] BRK [0x33519000, 0x33519fff] PGTABLE
[0.0] BRK [0x3351a000, 0x3351afff] PGTABLE
[0.0] BRK [0x3351b000, 0x3351bfff] PGTABLE
[0.0] RAMDISK: [mem 0x359e1000-0x36ce7fff]
[0.0] ACPI: Early table checksum verification disabled
[0.0] ACPI: RSDP 0x00000000000EA020 000024 (v02 Xen    )
[0.0] ACPI: XSDT 0x00000000FC00E2A0 000054 (v01 Xen    HVM      00000000 HVML
00000000)
[0.0] ACPI: FACP 0x00000000FC00DF60 0000F4 (v04 Xen    HVM      00000000 HVML
00000000)
[0.0] ACPI: DSDT 0x00000000FC0021C0 00BD19 (v02 Xen    HVM      00000000 INTL
20090123)
[0.0] ACPI: FACS 0x00000000FC002180 000040
[0.0] ACPI: FACS 0x00000000FC002180 000040
[0.0] ACPI: APIC 0x00000000FC00E060 0000D8 (v02 Xen    HVM      00000000 HVML
00000000)
[0.0] ACPI: HPET 0x00000000FC00E1B0 000038 (v01 Xen    HVM      00000000 HVML
00000000)
[0.0] ACPI: WAET 0x00000000FC00E1F0 000028 (v01 Xen    HVM      00000000 HVML
00000000)
[0.0] ACPI: SSDT 0x00000000FC00E220 000031 (v02 Xen    HVM      00000000 INTL
20090123)
[0.0] ACPI: SSDT 0x00000000FC00E260 000031 (v02 Xen    HVM      00000000 INTL
20090123)
[0.0] ACPI: Local APIC address 0xfeee0000
[0.0] No NUMA configuration found
[0.0] Faking a node at [mem 0x0000000000000000-0x000000003fffff]
[0.0] NODE_DATA(0) allocated [mem 0x3ffd5000-0x3fffffff]
[0.0] tsc: Fast TSC calibration using PIT
[0.0] Zone ranges:
[0.0]   DMA      [mem 0x0000000000001000-0x0000000000ffff]
[0.0]   DMA32     [mem 0x0000000001000000-0x0000000003fffff]
[0.0]   Normal    empty
[0.0]   Device    empty
```

```
[0.0] Movable zone start for each node
[0.0] Early memory node ranges
[0.0]   node  0: [mem 0x0000000000001000-0x000000000009ffff]
[0.0]   node  0: [mem 0x0000000000100000-0x000000003fffffff]
[0.0] Initmem setup node 0 [mem 0x0000000000001000-0x000000003fffffff]
[0.0] On node 0 totalpages: 262045
[0.0]   DMA zone: 64 pages used for memmap
[0.0]   DMA zone: 21 pages reserved
[0.0]   DMA zone: 3997 pages, LIFO batch:0
[0.0]   DMA32 zone: 4032 pages used for memmap
[0.0]   DMA32 zone: 258048 pages, LIFO batch:31
[0.0] Reserved but unavailable: 99 pages
[0.0] ACPI: PM-Timer IO Port: 0xb008
[0.0] ACPI: Local APIC address 0xfeee0000
[0.0] IOAPIC[0]: apic_id 1, version 17, address 0xfec00000, GSI 0-47
[0.0] ACPI: INT_SRC_OVR (bus 0 bus_irq 0 global_irq 2 dfl dfl)
[0.0] ACPI: INT_SRC_OVR (bus 0 bus_irq 5 global_irq 5 low level)
[0.0] ACPI: INT_SRC_OVR (bus 0 bus_irq 10 global_irq 10 low level)
[0.0] ACPI: INT_SRC_OVR (bus 0 bus_irq 11 global_irq 11 low level)
[0.0] ACPI: IRQ0 used by override.
[0.0] ACPI: IRQ5 used by override.
[0.0] ACPI: IRQ9 used by override.
[0.0] ACPI: IRQ10 used by override.
[0.0] ACPI: IRQ11 used by override.
[0.0] Using ACPI (MADT) for SMP configuration information
[0.0] ACPI: HPET id: 0x8086a201 base: 0xfed00000
[0.0] smpboot: Allowing 15 CPUs, 14 hotplug CPUs
[0.0] PM: Registered nosave memory: [mem 0x00000000-0x00000fff]
[0.0] PM: Registered nosave memory: [mem 0x0009e000-0x0009ffff]
[0.0] PM: Registered nosave memory: [mem 0x000a0000-0x000dffff]
[0.0] PM: Registered nosave memory: [mem 0x000e0000-0x000fffff]
[0.0] e820: [mem 0x40000000-0xfbfffff] available for PCI devices
[0.0] Booting paravirtualized kernel on Xen HVM
[0.0] clocksource: refined-jiffies: mask: 0xffffffff max_cycles: 0xffffffff,
max_idle_ns: 7645519600211568 ns
[0.0] random: get_random_bytes called from start_kernel+0x99/0x4fd with
crng_init=0
[0.0] setup_percpu: NR_CPUS:8192 nr_cpumask_bits:15 nr_cpu_ids:15 nr_node_ids:1
[0.0] percpu: Embedded 46 pages/cpu @           (ptrval) s151552 r8192 d28672 u262144
[0.0] pcpu-alloc: s151552 r8192 d28672 u262144 alloc=1*2097152
[0.0] pcpu-alloc: [0] 00 01 02 03 04 05 06 07 [0] 08 09 10 11 12 13 14 --
[0.0] xen: PV spinlocks enabled
[0.0] PV qspinlock hash table entries: 256 (order: 0, 4096 bytes)
[0.0] Built 1 zonelists, mobility grouping on. Total pages: 257928
[0.0] Policy zone: DMA32
[0.0] Kernel command line: BOOT_IMAGE=/boot/vmlinuz-4.15.0-1021-aws
root=LABEL=cloudimg-rootfs ro console=tty1 console=ttyS0
nvme.io_timeout=4294967295
[0.0] Calgary: detecting Calgary via BIOS EBDA area
[0.0] Calgary: Unable to locate Rio Grande table in EBDA - bailing!
[0.0] Memory: 983488K/1048180K available (12300K kernel code, 2391K rwdta, 3908K
rodata, 2372K init, 2376K bss, 64692K reserved, 0K cma-reserved)
[0.0] SLUB: Hwalign=64, Order=0-3, MinObjects=0, CPUs=15, Nodes=1
[0.0] Kernel/User page tables isolation: enabled
```

```
[0.0] ftrace: allocating 37478 entries in 147 pages
[4000000.0] Hierarchical RCU implementation.
[4000000.0]     RCU restricting CPUs from NR_CPUS=8192 to nr_cpu_ids=15.
[4000000.0]     Tasks RCU enabled.
[4000000.0] RCU: Adjusting geometry for rcu_fanout_leaf=16, nr_cpu_ids=15
[4000000.0] NR_IRQS: 524544, nr_irqs: 952, preallocated irqs: 16
[4000000.0] xen:events: Using 2-level ABI
[4000000.0] xen:events: Xen HVM callback vector for event delivery is enabled
[4000000.0] Console: colour VGA+ 80x25
[4000000.0] console [tty1] enabled
[4000000.0] Cannot get hvm parameter CONSOLE_EVTCHN (18): -22!
[4000000.0] console [ttyS0] enabled
[4000000.0] ACPI: Core revision 20170831
[4000000.0] ACPI: 3 ACPI AML tables successfully acquired and loaded
[4000000.0] clocksource: hpet: mask: 0xffffffff max_cycles: 0xffffffff,
max_idle_ns: 30580167144 ns
[4000000.0] hpet clockevent registered
[4012590.0] APIC: Switch to symmetric I/O mode setup
[8797214.0] x2apic: IRQ remapping doesn't support X2APIC mode
[12004299.0] Switched APIC routing to physical flat.
[22666924.0] ..TIMER: vector=0x30 apic1=0 pin1=2 apic2=0 pin2=0
[32000000.0] tsc: Fast TSC calibration using PIT
[48004887.0] tsc: Detected 2399.970 MHz processor
[52004528.0] tsc: Detected 2400.054 MHz TSC
[52016727.0] Calibrating delay loop (skipped), value calculated using timer
frequency.. 4800.10 BogoMIPS (lpj=9600216)
[68005949.0] pid_max: default: 32768 minimum: 301
[72070014.0] Security Framework initialized
[80004040.0] Yama: becoming mindful.
[84055921.0] AppArmor: AppArmor initialized
[88241470.0] Dentry cache hash table entries: 131072 (order: 8, 1048576 bytes)
[96117080.0] Inode-cache hash table entries: 65536 (order: 7, 524288 bytes)
[104030958.0] Mount-cache hash table entries: 2048 (order: 2, 16384 bytes)
[112014881.0] Mountpoint-cache hash table entries: 2048 (order: 2, 16384 bytes)
[120351090.0] mce: CPU supports 2 MCE banks
[124036266.0] Last level iTLB entries: 4KB 1024, 2MB 1024, 4MB 1024
[128003783.0] Last level dTLB entries: 4KB 1024, 2MB 1024, 4MB 1024, 1GB 4
[136003494.0] Spectre V2 : Mitigation: Full generic retpoline
[140001652.0] Speculative Store Bypass: Vulnerable
[165828900.0] clocksource: xen: mask: 0xffffffffffffffff max_cycles:
0x1cd42e4dfffb, max_idle_ns: 881590591483 ns
[176023475.0] Xen: using vcpuop timer interface
[176032015.0] installing Xen timer for CPU 0
[180111677.0] smpboot: CPU0: Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz (family:
0x6, model: 0x3f, stepping: 0x2)
[184057450.0] cpu 0 spinlock event irq 53
[188120120.0] Performance Events: unsupported p6 CPU model 63 no PMU driver,
software events only.
[192062597.0] Hierarchical SRCU implementation.
[196661290.0] NMI watchdog: Perf event create on CPU 0 failed with -2
[200009797.0] NMI watchdog: Perf NMI watchdog permanently disabled
[204213544.0] smp: Bringing up secondary CPUs ...
[208008649.0] smp: Brought up 1 node, 1 CPU
[212007617.0] smpboot: Max logical packages: 15
```

```
[216008120.0] smpboot: Total of 1 processors activated (4800.10 BogoMIPS)
[220324515.0] devtmpfs: initialized
[224092426.0] x86/mm: Memory block size: 128MB
[228243285.0] evm: security.selinux
[232011134.0] evm: security.SMACK64
[236008501.0] evm: security.SMACK64EXEC
[240007990.0] evm: security.SMACK64TRANSMUTE
[244004736.0] evm: security.SMACK64MMAP
[248007490.0] evm: security.apparmor
[252007875.0] evm: security.ima
[255626852.0] evm: security.capability
[256213945.0] clocksource: jiffies: mask: 0xffffffff max_cycles: 0xffffffff,
max_idle_ns: 7645041785100000 ns
[260030763.0] futex hash table entries: 4096 (order: 6, 262144 bytes)
[264281367.0] RTC time: 12:04:38, date: 12/21/18
[268155981.0] NET: Registered protocol family 16
[272130796.0] audit: initializing netlink subsys (disabled)
[276162251.0] audit: type=2000 audit(1545393878.626:1): state=initialized
audit_enabled=0 res=1
[280121685.0] cpuidle: using governor ladder
[284009008.0] cpuidle: using governor menu
[288078749.0] ACPI: bus type PCI registered
[292010193.0] acpiphp: ACPI Hot Plug PCI Controller Driver version: 0.5
[296639948.0] PCI: Using configuration type 1 for base access
[301191889.0] HugeTLB registered 2.00 MiB page size, pre-allocated 0 pages
[304312441.0] ACPI: Added _OSI(Module Device)
[308012050.0] ACPI: Added _OSI(Processor Device)
[312006482.0] ACPI: Added _OSI(3.0 _SCP Extensions)
[316008134.0] ACPI: Added _OSI(Processor Aggregator Device)
[320029821.0] ACPI: Added _OSI(Linux-Dell-Video)
[324034589.0] ACPI: Added _OSI(Linux-Lenovo-NV-HDMI-Audio)
[328323227.0] xen: --> pirq=16 -> irq=9 (gsi=9)
[331823202.0] ACPI: Interpreter enabled
[332019685.0] ACPI: (supports S0 S4 S5)
[336005805.0] ACPI: Using IOAPIC for interrupt routing
[340043356.0] PCI: Using host bridge windows from ACPI; if necessary, use
"pci=nocrs" and report a bug
[344569571.0] ACPI: Enabled 2 GPEs in block 00 to 0F
[420316390.0] ACPI: PCI Root Bridge [PCI0] (domain 0000 [bus 00-ff])
[424019107.0] acpi PNP0A03:00: _OSC: OS supports [ASPM ClockPM Segments MSI]
[428017458.0] acpi PNP0A03:00: _OSC failed (AE_NOT_FOUND); disabling ASPM
[432040471.0] acpi PNP0A03:00: fail to add MMCONFIG information, can't access
extended PCI configuration space under this bridge.
[437327815.0] acpiphp: Slot [0] registered
[441458080.0] acpiphp: Slot [3] registered
[444572762.0] acpiphp: Slot [4] registered
[448589162.0] acpiphp: Slot [5] registered
[452589562.0] acpiphp: Slot [6] registered
[456907838.0] acpiphp: Slot [7] registered
[460588788.0] acpiphp: Slot [8] registered
[464529668.0] acpiphp: Slot [9] registered
[468526877.0] acpiphp: Slot [10] registered
[472538820.0] acpiphp: Slot [11] registered
[476582467.0] acpiphp: Slot [12] registered
```

```
[480513845.0] acpiphp: Slot [13] registered
[484492750.0] acpiphp: Slot [14] registered
[488534618.0] acpiphp: Slot [15] registered
[492522623.0] acpiphp: Slot [16] registered
[496554151.0] acpiphp: Slot [17] registered
[500536805.0] acpiphp: Slot [18] registered
[504599294.0] acpiphp: Slot [19] registered
[508613655.0] acpiphp: Slot [20] registered
[512605089.0] acpiphp: Slot [21] registered
[516671137.0] acpiphp: Slot [22] registered
[520667249.0] acpiphp: Slot [23] registered
[524611994.0] acpiphp: Slot [24] registered
[528642191.0] acpiphp: Slot [25] registered
[532521958.0] acpiphp: Slot [26] registered
[536623890.0] acpiphp: Slot [27] registered
[540617055.0] acpiphp: Slot [28] registered
[544765646.0] acpiphp: Slot [29] registered
[548612800.0] acpiphp: Slot [30] registered
[552714668.0] acpiphp: Slot [31] registered
[556552139.0] PCI host bridge to bus 0000:00
[560012424.0] pci_bus 0000:00: root bus resource [io 0x0000-0x0cf7 window]
[564007160.0] pci_bus 0000:00: root bus resource [io 0xd00-0xffff window]
[568011420.0] pci_bus 0000:00: root bus resource [mem 0x000a0000-0x000bffff
window]
[572013069.0] pci_bus 0000:00: root bus resource [mem 0xf0000000-0xfbffff
window]
[576012283.0] pci_bus 0000:00: root bus resource [bus 00-ff]
[580286295.0] pci 0000:00:00.0: [8086:1237] type 00 class 0x060000
[583621159.0] pci 0000:00:01.0: [8086:7000] type 00 class 0x060100
[587551883.0] pci 0000:00:01.1: [8086:7010] type 00 class 0x010180
[589618211.0] pci 0000:00:01.1: reg 0x20: [io 0xc100-0xc10f]
[590522231.0] pci 0000:00:01.1: legacy IDE quirk: reg 0x10: [io 0x01f0-0x01f7]
[592014892.0] pci 0000:00:01.1: legacy IDE quirk: reg 0x14: [io 0x03f6]
[596014153.0] pci 0000:00:01.1: legacy IDE quirk: reg 0x18: [io 0x0170-0x0177]
[600017938.0] pci 0000:00:01.1: legacy IDE quirk: reg 0x1c: [io 0x0376]
[605093715.0] pci 0000:00:01.3: [8086:7113] type 00 class 0x068000
[605155743.0] * Found PM-Timer Bug on the chipset. Due to workarounds for a bug,
* this clock source is slow. Consider trying other clock sources
[611143923.0] pci 0000:00:01.3: quirk: [io 0xb000-0xb03f] claimed by PII4 ACPI
[613820403.0] pci 0000:00:02.0: [1013:00b8] type 00 class 0x030000
[614700428.0] pci 0000:00:02.0: reg 0x10: [mem 0xf0000000-0xf1ffff pref]
[615180233.0] pci 0000:00:02.0: reg 0x14: [mem 0xf3000000-0xf3000fff]
[618557606.0] pci 0000:00:03.0: [5853:0001] type 00 class 0xff8000
[619685245.0] pci 0000:00:03.0: reg 0x10: [io 0xc000-0xc0ff]
[620182481.0] pci 0000:00:03.0: reg 0x14: [mem 0xf2000000-0xf2ffff pref]
[626047486.0] ACPI: PCI Interrupt Link [LNKA] (IRQs *5 10 11)
[628420777.0] ACPI: PCI Interrupt Link [LNKB] (IRQs 5 *10 11)
[632391633.0] ACPI: PCI Interrupt Link [LNKC] (IRQs 5 10 *11)
[636428660.0] ACPI: PCI Interrupt Link [LNKD] (IRQs *5 10 11)
[669110123.0] xen:balloon: Initialising balloon driver
[676188633.0] SCSI subsystem initialized
[680076192.0] libata version 3.00 loaded.
[680190616.0] pci 0000:00:02.0: vgaarb: setting as boot VGA device
[684000000.0] pci 0000:00:02.0: vgaarb: VGA device added:
```

```
decodes=io+mem,owns=io+mem,locks=none
[684010921.0] pci 0000:00:02.0: vgaarb: bridge control possible
[688009773.0] vgaarb: loaded
[691574079.0] ACPI: bus type USB registered
[692042107.0] usbcore: registered new interface driver usbf
[696026458.0] usbcore: registered new interface driver hub
[700037279.0] usbcore: registered new device driver usb
[704117108.0] EDAC MC: Ver: 3.0.0
[709010892.0] PCI: Using ACPI for IRQ routing
[712012630.0] PCI: pci_cache_line_size set to 64 bytes
[712730583.0] e820: reserve RAM buffer [mem 0x0009e000-0x0009ffff]
[712885309.0] NetLabel: Initializing
[716006891.0] NetLabel: domain hash size = 128
[720007284.0] NetLabel: protocols = UNLABLED CIPSOv4 CALIPSO
[724034694.0] NetLabel: unlabeled traffic allowed by default
[728217434.0] HPET: 3 timers in total, 0 timers will be used for per-cpu timer
[732028320.0] hpet0: at MMIO 0xfed00000, IRQs 2, 8, 0
[736009287.0] hpet0: 3 comparators, 64-bit 62.500000 MHz counter
[744040291.0] clocksource: Switched to clocksource xen
[762129275.0] VFS: Disk quotas dquot_6.6.0
[767211362.0] VFS: Dquot-cache hash table entries: 512 (order 0, 4096 bytes)
[774865282.0] random: fast init done
[779219045.0] AppArmor: AppArmor Filesystem Enabled
[784713979.0] pnp: PnP ACPI init
[789365523.0] system 00:00: [mem 0x00000000-0x0009ffff] could not be reserved
[796449347.0] system 00:00: Plug and Play ACPI device, IDs PNP0c02 (active)
[796557833.0] system 00:01: [io 0x08a0-0x08a3] has been reserved
[803273905.0] system 00:01: [io 0xcc0-0x0ccf] has been reserved
[809828198.0] system 00:01: [io 0x04d0-0x04d1] has been reserved
[816484507.0] system 00:01: Plug and Play ACPI device, IDs PNP0c02 (active)
[816527928.0] xen: --> pirq=17 -> irq=8 (gsi=8)
[816566112.0] pnp 00:02: Plug and Play ACPI device, IDs PNP0b00 (active)
[816600184.0] xen: --> pirq=18 -> irq=12 (gsi=12)
[816617483.0] pnp 00:03: Plug and Play ACPI device, IDs PNP0f13 (active)
[816637273.0] xen: --> pirq=19 -> irq=1 (gsi=1)
[816654278.0] pnp 00:04: Plug and Play ACPI device, IDs PNP0303 PNP030b (active)
[816673114.0] xen: --> pirq=20 -> irq=6 (gsi=6)
[816675024.0] pnp 00:05: [dma 2]
[816690852.0] pnp 00:05: Plug and Play ACPI device, IDs PNP0700 (active)
[816726798.0] xen: --> pirq=21 -> irq=4 (gsi=4)
[816738678.0] pnp 00:06: Plug and Play ACPI device, IDs PNP0501 (active)
[816792399.0] system 00:07: [io 0x10c0-0x1141] has been reserved
[823694822.0] system 00:07: [io 0xb044-0xb047] has been reserved
[830123664.0] system 00:07: Plug and Play ACPI device, IDs PNP0c02 (active)
[859627027.0] pnp: PnP ACPI: found 8 devices
[870896669.0] clocksource: acpi_pm: mask: 0xffffffff max_cycles: 0xffffffff,
max_idle_ns: 2085701024 ns
[881068904.0] pci_bus 0000:00: resource 4 [io 0x0000-0x0cf7 window]
[881070659.0] pci_bus 0000:00: resource 5 [io 0xd00-0xffff window]
[881072084.0] pci_bus 0000:00: resource 6 [mem 0x000a0000-0x000bffff window]
[881073629.0] pci_bus 0000:00: resource 7 [mem 0xf0000000-0xfbffff window]
[881304275.0] NET: Registered protocol family 2
[887469737.0] TCP established hash table entries: 8192 (order: 4, 65536 bytes)
[894636662.0] TCP bind hash table entries: 8192 (order: 5, 131072 bytes)
```

```
[901469128.0] TCP: Hash tables configured (established 8192 bind 8192)
[910384231.0] UDP hash table entries: 512 (order: 2, 16384 bytes)
[918017947.0] UDP-Lite hash table entries: 512 (order: 2, 16384 bytes)
[926287637.0] NET: Registered protocol family 1
[932154252.0] pci 0000:00:00.0: Limiting direct PCI/PCI transfers
[939972751.0] pci 0000:00:01.0: PIIX3: Enabling Passive Release
[947484564.0] pci 0000:00:01.0: Activating ISA DMA hang workarounds
[955698287.0] pci 0000:00:02.0: Video device with shadowed ROM at [mem 0x000c0000-
0x000dffff]
[965760966.0] PCI: CLS 0 bytes, default 64
[965826364.0] Unpacking initramfs...
[1251931051.1] Freeing initrd memory: 19484K
[1256370252.1] Scanning for low memory corruption every 60 seconds
[1261529945.1] Initialise system trusted keyrings
[1265242812.1] Key type blacklist registered
[1270703630.1] workingset: timestamp_bits=36 max_order=18 bucket_order=0
[1278759071.1] zbud: loaded
[1282878516.1] squashfs: version 4.0 (2009/01/31) Phillip Louher
[1289539736.1] fuse init (API version 7.26)
[1295108453.1] Key type asymmetric registered
[1298571769.1] Asymmetric key parser 'x509' registered
[1302435161.1] Block layer SCSI generic (bsg) driver version 0.4 loaded (major
247)
[1308347952.1] io scheduler noop registered
[1311560798.1] io scheduler deadline registered
[1314961112.1] io scheduler cfq registered (default)
[1318964495.1] intel_idle: Please enable MWAIT in BIOS SETUP
[1319064795.1] input: Power Button as
/devices/LNXSYSYM:00/LNXPWRBN:00/input/input0
[1324979857.1] ACPI: Power Button [PWRF]
[1328381431.1] input: Sleep Button as
/devices/LNXSYSYM:00/LNXSLPBN:00/input/input1
[1334783883.1] ACPI: Sleep Button [SLPF]
[1338657919.1] xen: --> pirq=22 -> irq=28 (gsi=28)
[1338772212.1] xen:grant_table: Grant tables using version 1 layout
[1343758938.1] Grant table initialized
[1347166831.1] Cannot get hvm parameter CONSOLE_EVTCHN (18): -22!
[1351528333.1] Serial: 8250/16550 driver, 4 ports, IRQ sharing enabled
[1388458801.1] 00:06: ttyS0 at I/O 0x3f8 (irq = 4, base_baud = 115200) is a 16550A
[1396306426.1] Linux agpgart interface v0.103
[1402652628.1] loop: module loaded
[1406942041.1] Invalid max_queues (4), will use default max: 1.
[1413146002.1] ata_piix 0000:00:01.1: version 2.13
[1414367912.1] scsi host0: ata_piix
[1417942126.1] scsi host1: ata_piix
[1421407329.1] ata1: PATA max MWDMA2 cmd 0x1f0 ctl 0x3f6 bmdma 0xc100 irq 14
[1427375516.1] ata2: PATA max MWDMA2 cmd 0x170 ctl 0x376 bmdma 0xc108 irq 15
[1435175394.1] libphy: Fixed MDIO Bus: probed
[1439163785.1] tun: Universal TUN/TAP device driver, 1.6
[1443671722.1] PPP generic driver version 2.4.2
[1449954098.1] xen_netfront: Initialising Xen virtual ethernet driver
[1457572685.1] ehci_hcd: USB 2.0 'Enhanced' Host Controller (EHCI) Driver
[1473237021.1] ehci-pci: EHCI PCI platform driver
[1477331938.1] ehci-platform: EHCI generic platform driver
```

```
[1481865344.1] ohci_hcd: USB 1.1 'Open' Host Controller (OHCI) Driver
[1487124516.1] ohci-pci: OHCI PCI platform driver
[1491288855.1] ohci-platform: OHCI generic platform driver
[1496019580.1] uhci_hcd: USB Universal Host Controller Interface driver
[1501787328.1] i8042: PNP: PS/2 Controller [PNP0303:PS2K,PNP0f13:PS2M] at
0x60,0x64 irq 1,12
[1512138293.1] serio: i8042 KBD port at 0x60,0x64 irq 1
[1517061669.1] serio: i8042 AUX port at 0x60,0x64 irq 12
[1521867400.1] mousedev: PS/2 mouse device common for all mice
[1528305597.1] input: AT Translated Set 2 keyboard as
/devices/platform/i8042/serio0/input/input2
[1536216041.1] rtc_cmos 00:02: rtc core: registered rtc_cmos as rtc0
[1541608368.1] rtc_cmos 00:02: alarms up to one day, 114 bytes nvram, hpet irqs
[1549307710.1] device-mapper: uevent: version 1.0.3
[1558880159.1] device-mapper: ioctl: 4.37.0-ioctl (2017-09-20) initialised: dm-
devel@redhat.com
[1565660037.1] NET: Registered protocol family 10
[1573786413.1] blkfront: xvda: barrier or flush: disabled; persistent grants:
disabled; indirect descriptors: enabled;
[1582735856.1] Segment Routing with IPv6
[1586085339.1] NET: Registered protocol family 17
[1589697824.1] Key type dns_resolver registered
[1595366946.1] intel_rdt: Intel RDT L3 allocation detected
[1601257953.1] RAS: Correctable Errors collector initialized.
[1606481120.1] sched_clock: Marking stable (1606281847, 0)->(10112567157,
-8506285310)
[1612342540.1] registered taskstats version 1
[1615606009.1] xvda: xvda1
[1618389864.1] Loading compiled-in X.509 certificates
[1624882494.1] Loaded X.509 cert 'Build time autogenerated kernel key:
1472665054521b238871beb9554d15504325c156'
[1632653831.1] zswap: loaded using pool lzo/zbud
[1639087595.1] Key type big_key registered
[1642294522.1] Key type trusted registered
[1647154794.1] Key type encrypted registered
[1650919509.1] AppArmor: AppArmor sha1 policy hashing enabled
[1655497188.1] ima: No TPM chip found, activating TPM-bypass! (rc=-19)
[1660714633.1] ima: Allocated hash algorithm: sha1
[1664278207.1] evm: HMAC attrs: 0x1
[1667608602.1] Magic number: 14:400:77
[1671075735.1] rtc_cmos 00:02: setting system clock to 2018-12-21 12:04:40 UTC
(1545393880)
[1677355139.1] BIOS EDD facility v0.16 2004-Jun-25, 0 devices found
[1681780336.1] EDD information not available.
[1687733151.1] Freeing unused kernel memory: 2372K
[1696070973.1] Write protecting the kernel read-only data: 18432k
[1701254154.1] Freeing unused kernel memory: 2008K
[1705743711.1] Freeing unused kernel memory: 188K
[1715477224.1] x86/mm: Checked W+X mappings: passed, no W+X pages found.
[1721193335.1] x86/mm: Checking user space page tables
[1731102653.1] x86/mm: Checked W+X mappings: passed, no W+X pages found.
[1751868658.1] random: udevadm: uninitialized urandom read (16 bytes read)
[1757302492.1] random: systemd-udevd: uninitialized urandom read (16 bytes read)
[1762931607.1] random: systemd-udevd: uninitialized urandom read (16 bytes read)
```

```
[1945727269.1] AVX2 version of gcm_enc/dec engaged.
[1949613014.1] AES CTR mode by8 optimization enabled
[2272165675.2] tsc: Refined TSC clocksource calibration: 2400.001 MHz
[2277150119.2] clocksource: tsc: mask: 0xfffffffffffffff max_cycles:
0x22983858435, max_idle_ns: 440795258295 ns
[3660065068.3] raid6: sse2x1 gen() 9113 MB/s
[3708065561.3] raid6: sse2x1 xor() 6397 MB/s
[3756067802.3] raid6: sse2x2 gen() 10919 MB/s
[3808061488.3] raid6: sse2x2 xor() 7010 MB/s
[3860065926.3] raid6: sse2x4 gen() 12602 MB/s
[3912063347.3] raid6: sse2x4 xor() 8000 MB/s
[3964064174.3] raid6: avx2x1 gen() 15380 MB/s
[4016062541.4] raid6: avx2x1 xor() 12087 MB/s
[4068062848.4] raid6: avx2x2 gen() 20769 MB/s
[4120063141.4] raid6: avx2x2 xor() 12674 MB/s
[4172062033.4] raid6: avx2x4 gen() 23766 MB/s
[4220061121.4] raid6: avx2x4 xor() 14645 MB/s
[4224268335.4] raid6: using algorithm avx2x4 gen() 23766 MB/s
[4229047220.4] raid6: .... xor() 14645 MB/s, rmw enabled
[4233500421.4] raid6: using avx2x2 recovery algorithm
[4239865431.4] xor: automatically using best checksumming function avx
[4247550014.4] async_tx: api initialized (async)
[4318120055.4] Btrfs loaded, crc32c=crc32c-intel
[4353096368.4] EXT4-fs (xvda1): mounted filesystem with ordered data mode. Opts:
(null)
[4517023086.4] ip_tables: (C) 2000-2006 Netfilter Core Team
[4528241306.4] systemd[1]: systemd 237 running in system mode. (+PAM +AUDIT
+SELINUX +IMA +APPARMOR +SMACK +SYSVINIT +UTMP +LIBCRYPTSETUP +GCRYPT +GNUTLS +ACL
+XZ +LZ4 +SECCOMP +BLKID +ELFUTILS +KMOD -IDN2 +IDN -PCRE2 default-
hierarchy=hybrid)
[4552411301.4] systemd[1]: Detected virtualization xen.
[4559563819.4] systemd[1]: Detected architecture x86-64.
[4574473157.4] systemd[1]: Set hostname to <ubuntu>.
[4583794096.4] systemd[1]: Initializing machine ID from random generator.
[4590444341.4] systemd[1]: Installed transient /etc/machine-id file.
[4750864284.4] systemd[1]: Created slice User and Session Slice.
[4760750738.4] systemd[1]: Created slice System Slice.
[4769034200.4] systemd[1]: Listening on Journal Audit Socket.
[4778512441.4] systemd[1]: Created slice system-serial\x2dgetty.slice.
[4874400462.4] Loading iSCSI transport class v2.0-870.
[4904053086.4] iscsi: registered transport (tcp)
[4940496394.4] EXT4-fs (xvda1): re-mounted. Opts: discard
[5106934367.5] systemd-journald[393]: Received request to flush runtime journal
from PID 1
[5121476059.5] iscsi: registered transport (iser)
[6501940919.6] audit: type=1400 audit(1545393885.328:2): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="lxc-container-default" pid=464
comm="apparmor_parser"
[6502505558.6] audit: type=1400 audit(1545393885.328:3): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="lxc-container-default-cgns"
pid=464 comm="apparmor_parser"
[6504509960.6] audit: type=1400 audit(1545393885.332:4): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="lxc-container-default-with-
mounting" pid=464 comm="apparmor_parser"
```

```
[6505058227.6] audit: type=1400 audit(1545393885.332:5): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="lxc-container-default-with-
nesting" pid=464 comm="apparmor_parser"
[7032124407.7] audit: type=1400 audit(1545393885.860:6): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="/sbin/dhclient" pid=482
comm="apparmor_parser"
[7032718031.7] audit: type=1400 audit(1545393885.860:7): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="/usr/lib/NetworkManager/nm-
dhcp-client.action" pid=482 comm="apparmor_parser"
[7033191452.7] audit: type=1400 audit(1545393885.860:8): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="/usr/lib/NetworkManager/nm-
dhcp-helper" pid=482 comm="apparmor_parser"
[7034851907.7] audit: type=1400 audit(1545393885.860:9): apparmor="STATUS"
operation="profile_load" profile="unconfined"
name="/usr/lib/conman/scripts/dhclient-script" pid=482 comm="apparmor_parser"
[7051552932.7] audit: type=1400 audit(1545393885.876:10): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="/usr/bin/lxc-start" pid=517
comm="apparmor_parser"
[7199498724.7] audit: type=1400 audit(1545393886.024:11): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="/usr/bin/man" pid=519
comm="apparmor_parser"
[11161377278.11] new mount options do not match the existing superblock, will be
ignored
[12363474839.12] random: crng init done
[12363476830.12] random: 7 urandom warning(s) missed due to ratelimiting
[16900680066.16] kauditd_printk_skb: 5 callbacks suppressed
[16900681473.16] audit: type=1400 audit(1545393895.728:17): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="snap-update-ns.core" pid=961
comm="apparmor_parser"
[16971224711.16] audit: type=1400 audit(1545393895.796:18): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="snap.core.hook.configure"
pid=963 comm="apparmor_parser"
[19172179813.19] audit: type=1400 audit(1545393898.000:19): apparmor="STATUS"
operation="profile_load" profile="unconfined"
name="/snap/core/5328/usr/lib/snapd/snap-confine" pid=1033 comm="apparmor_parser"
[19172634993.19] audit: type=1400 audit(1545393898.000:20): apparmor="STATUS"
operation="profile_load" profile="unconfined"
name="/snap/core/5328/usr/lib/snapd/snap-confine//mount-namespace-capture-helper"
pid=1033 comm="apparmor_parser"
[19190877440.19] audit: type=1400 audit(1545393898.016:21): apparmor="STATUS"
operation="profile_replace" profile="unconfined" name="snap-update-ns.core"
pid=1038 comm="apparmor_parser"
[19255303345.19] audit: type=1400 audit(1545393898.080:22): apparmor="STATUS"
operation="profile_replace" profile="unconfined" name="snap.core.hook.configure"
pid=1040 comm="apparmor_parser"
[20044096523.20] audit: type=1400 audit(1545393898.868:23): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="snap-update-ns.amazon-ssm-
agent" pid=1115 comm="apparmor_parser"
[20048992141.20] audit: type=1400 audit(1545393898.876:24): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="snap.amazon-ssm-agent.amazon-
ssm-agent" pid=1117 comm="apparmor_parser"
[20053640745.20] audit: type=1400 audit(1545393898.880:25): apparmor="STATUS"
operation="profile_load" profile="unconfined" name="snap.amazon-ssm-agent.ssm-cli"
pid=1119 comm="apparmor_parser"
```

```
[343815640354.343] systemd: 36 output lines suppressed due to ratelimiting
[343819811212.343] systemd[1]: systemd 237 running in system mode. (+PAM +AUDIT
+SELINUX +IMA +APPARMOR +SMACK +SYSVINIT +UTMP +LIBCRYPTSETUP +GCRYPT +GNUTLS +ACL
+XZ +LZ4 +SECCOMP +BLKID +ELFUTILS +KMOD -IDN2 +IDN -PCRE2 default-
hierarchy=hybrid)
[343819860527.343] systemd[1]: Detected virtualization xen.
[343819868348.343] systemd[1]: Detected architecture x86-64.
[344163440924.344] systemd[1]: Stopping Journal Service...
[344166748005.344] systemd-journald[393]: Received SIGTERM from PID 1 (systemd).
[344191632037.344] systemd[1]: Stopped Journal Service.
[344193359863.344] systemd[1]: Starting Journal Service...
[344209913346.344] systemd[1]: Started Journal Service.
[388149683405.388] audit: type=1400 audit(1545394267.287:26): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/usr/bin/man" pid=9951 comm="apparmor_parser"
[388150220347.388] audit: type=1400 audit(1545394267.287:27): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="man_filter" pid=9951 comm="apparmor_parser"
[388150640322.388] audit: type=1400 audit(1545394267.287:28): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="man_groff" pid=9951 comm="apparmor_parser"
[388935289550.388] SGI XFS with ACLs, security attributes, realtime, no debug
enabled
[394016817570.394] audit: type=1400 audit(1545394273.155:29): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="lxc-container-default" pid=10795 comm="apparmor_parser"
[394017449828.394] audit: type=1400 audit(1545394273.155:30): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="lxc-container-default-cgns" pid=10795
comm="apparmor_parser"
[394017954690.394] audit: type=1400 audit(1545394273.155:31): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="lxc-container-default-with-mounting" pid=10795
comm="apparmor_parser"
[394018487638.394] audit: type=1400 audit(1545394273.155:32): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="lxc-container-default-with-nesting" pid=10795
comm="apparmor_parser"
[394184258557.394] audit: type=1400 audit(1545394273.323:33): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/sbin/dhclient" pid=10797 comm="apparmor_parser"
[394184852626.394] audit: type=1400 audit(1545394273.323:34): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-client.action"
pid=10797 comm="apparmor_parser"
[394185330873.394] audit: type=1400 audit(1545394273.323:35): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-helper" pid=10797
comm="apparmor_parser"
[394185765851.394] audit: type=1400 audit(1545394273.323:36): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/usr/lib/connman/scripts/dhclient-script" pid=10797
comm="apparmor_parser"
[394196588105.394] audit: type=1400 audit(1545394273.335:37): apparmor="STATUS"
```

```
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/usr/bin/lxc-start" pid=10799 comm="apparmor_parser"
[394269978275.394] audit: type=1400 audit(1545394273.407:38): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/usr/bin/man" pid=10801 comm="apparmor_parser"
[432983200194.432] kauditd_printk_skb: 12 callbacks suppressed
[432983201820.432] audit: type=1400 audit(1545394312.118:51): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="lxc-container-default" pid=12672 comm="apparmor_parser"
[432985982514.432] audit: type=1400 audit(1545394312.122:52): apparmor="STATUS"
operation="profile_replace" profile="unconfined" name="lxc-container-default-cgns"
pid=12672 comm="apparmor_parser"
[432986465264.432] audit: type=1400 audit(1545394312.122:53): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="lxc-container-default-with-mounting" pid=12672
comm="apparmor_parser"
[432986978760.432] audit: type=1400 audit(1545394312.122:54): apparmor="STATUS"
operation="profile_replace" profile="unconfined" name="lxc-container-default-with-
nesting" pid=12672 comm="apparmor_parser"
[433153679997.433] audit: type=1400 audit(1545394312.286:55): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/sbin/dhclient" pid=12675 comm="apparmor_parser"
[433154323395.433] audit: type=1400 audit(1545394312.290:56): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-client.action"
pid=12675 comm="apparmor_parser"
[433154810248.433] audit: type=1400 audit(1545394312.290:57): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-helper" pid=12675
comm="apparmor_parser"
[433155243731.433] audit: type=1400 audit(1545394312.290:58): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/usr/lib/connman/scripts/dhclient-script" pid=12675
comm="apparmor_parser"
[433167590815.433] audit: type=1400 audit(1545394312.302:59): apparmor="STATUS"
operation="profile_replace" profile="unconfined" name="/usr/bin/lxc-start"
pid=12677 comm="apparmor_parser"
[433240662059.433] audit: type=1400 audit(1545394312.374:60): apparmor="STATUS"
operation="profile_replace" info="same as current profile, skipping"
profile="unconfined" name="/usr/bin/man" pid=12679 comm="apparmor_parser"
[21462442803498.21462] kauditd_printk_skb: 13 callbacks suppressed
[21462442805151.21462] audit: type=1400 audit(1545415341.020:74):
apparmor="STATUS" operation="profile_load" profile="unconfined"
name="/usr/sbin/mysqld" pid=773 comm="apparmor_parser"
[21463206148453.21463] audit: type=1400 audit(1545415341.784:75):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=867 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[21463221380545.21463] audit: type=1400 audit(1545415341.800:76):
apparmor="DENIED" operation="capable" profile="/usr/sbin/mysqld" pid=867
comm="mysqld" capability=2 capname="dac_read_search"
[21463255863431.21463] audit: type=1400 audit(1545415341.836:77):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=879 comm="mysqld" requested_mask="r"
```

```
denied_mask="r" fsuid=111 ouid=0
[21756594961731.21756] audit: type=1400 audit(1545415635.164:78):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=2652 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[21833553902942.21833] audit: type=1400 audit(1545415712.122:79):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=3061 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[21875757992232.21875] audit: type=1400 audit(1545415754.321:80):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=3542 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22018568104327.22018] audit: type=1400 audit(1545415897.129:81):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=3758 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22018607698200.22018] audit: type=1400 audit(1545415897.169:82):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=3763 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=111 ouid=0
[22074531220184.22074] audit: type=1400 audit(1545415953.092:83):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4539 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22210765671468.22210] audit: type=1400 audit(1545416089.324:84):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4632 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22210807976537.22210] audit: type=1400 audit(1545416089.368:85):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4640 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=111 ouid=0
[22273491157183.22273] audit: type=1400 audit(1545416152.047:86):
apparmor="STATUS" operation="profile_replace" info="same as current profile,
skipping" profile="unconfined" name="/usr/sbin/mysqld" pid=4768
comm="apparmor_parser"
[22273549967523.22273] audit: type=1400 audit(1545416152.107:87):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4786 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22273604163691.22273] audit: type=1400 audit(1545416152.159:88):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4801 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22277537601294.22277] audit: type=1400 audit(1545416156.095:89):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4860 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22280230105408.22280] audit: type=1400 audit(1545416158.786:90):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4912 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22282295921818.22282] audit: type=1400 audit(1545416160.850:91):
```

```
apparmor="STATUS" operation="profile_replace" info="same as current profile,
skipping" profile="unconfined" name="/usr/sbin/mysqld" pid=4947
comm="apparmor_parser"
[22282854213630.22282] audit: type=1400 audit(1545416161.410:92):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=5019 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22282898519612.22282] audit: type=1400 audit(1545416161.454:93):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=5027 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=111 ouid=0
[22419123420018.22419] audit: type=1400 audit(1545416297.675:94):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=5121 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22419167903891.22419] audit: type=1400 audit(1545416297.719:95):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=5125 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=111 ouid=0
[25524580731645.25524] audit: type=1400 audit(1545419403.049:96):
apparmor="STATUS" operation="profile_load" profile="unconfined"
name="/snap/core/6130/usr/lib/snapd/snap-confine" pid=6200 comm="apparmor_parser"
[25524581172130.25524] audit: type=1400 audit(1545419403.049:97):
apparmor="STATUS" operation="profile_load" profile="unconfined"
name="/snap/core/6130/usr/lib/snapd/snap-confine//mount-namespace-capture-helper"
pid=6200 comm="apparmor_parser"
[25524661228460.25524] audit: type=1400 audit(1545419403.129:98):
apparmor="STATUS" operation="profile_replace" profile="unconfined"
name="snap.core.hook.configure" pid=6203 comm="apparmor_parser"
[25524667927860.25524] audit: type=1400 audit(1545419403.137:99):
apparmor="STATUS" operation="profile_replace" info="same as current profile,
skipping" profile="unconfined" name="snap-update-ns.core" pid=6205
comm="apparmor_parser"
[25525728627714.25525] audit: type=1400 audit(1545419404.197:100):
apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap-
update-ns.amazon-ssm-agent" pid=6264 comm="apparmor_parser"
[25525731681561.25525] audit: type=1400 audit(1545419404.201:101):
apparmor="STATUS" operation="profile_replace" profile="unconfined"
name="snap.amazon-ssm-agent.amazon-ssm-agent" pid=6265 comm="apparmor_parser"
[25525734393872.25525] audit: type=1400 audit(1545419404.201:102):
apparmor="STATUS" operation="profile_replace" profile="unconfined"
name="snap.amazon-ssm-agent.ssm-cli" pid=6266 comm="apparmor_parser"
[25525776327926.25525] audit: type=1400 audit(1545419404.245:103):
apparmor="STATUS" operation="profile_replace" profile="unconfined"
name="/snap/core/6130/usr/lib/snapd/snap-confine" pid=6271 comm="apparmor_parser"
[25525776541774.25525] audit: type=1400 audit(1545419404.245:104):
apparmor="STATUS" operation="profile_replace" profile="unconfined"
name="/snap/core/6130/usr/lib/snapd/snap-confine//mount-namespace-capture-helper"
pid=6271 comm="apparmor_parser"
[25525795866859.25525] audit: type=1400 audit(1545419404.265:105):
apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap-
update-ns.core" pid=6273 comm="apparmor_parser"
[66030429896299.66030] new mount options do not match the existing superblock,
will be ignored
```

```
[1108227154620838.1108227] lime: version magic '4.15.0-42-generic SMP mod_unload'
should be '4.15.0-1021-aws SMP mod_unload'
[1109556640120032.1109556] lime: loading out-of-tree module taints kernel.
[1109556640155159.1109556] lime: module verification failed: signature and/or
required key missing - tainting kernel
```

[Volver al texto del comando en la Sección 3.4.6.](#)

8.4.003.004.006.002. Resumen del comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_dmesg > /home/jrodg85/informe-linux_dmesg.txt.`

Para los cálculos de tiempos se ha usado el siguiente script de Python.

```
from datetime import datetime, timedelta

# Initial timestamp in UTC
initial_timestamp = datetime(2018, 8, 28, 10, 23, 7)

# Additional microseconds
additional_microseconds = 0.0 #insertar aquí el timestamp

# Convert microseconds to seconds for timedelta
additional_seconds = additional_microseconds / 1_000_000

# Calculate new datetime
new_datetime = initial_timestamp + timedelta(seconds=additional_seconds)
print("new_datetime: ", new_datetime.isoformat())
```

Explicado el script anterior, un resumen de los datos de interés para este análisis forense de este servidor es el siguiente:

```
# Establecimiento del tiempo origen de tiempos donde el 28 de Agosto de 2018 a las
10:23:07 UTC el cual arranca el servidor. Se considera que el tiempo [0.0] es el
origen de tiempos del sistema marcado en microsegundos.

[0.0] Linux version 4.15.0-1021-aws (buildd@lcy01-amd64-001) (gcc version 7.3.0
(Ubuntu 7.3.0-16ubuntu3)) #21-Ubuntu SMP Tue Aug 28 10:23:07 UTC 2018 (Ubuntu
4.15.0-1021.21-aws 4.15.18)

# Se descarta información relativa al arranque del servidor, la cual tiene marcada
el tiempo [0.0], ya que sería el 1 de enero de 1979. Se mantiene la relevante la
cual se explica a continuación.

# El Servidor es una Máquina virtual

[0.0] Hypervisor detected: Xen HVM
```

Memoria disponible y su distribución.

```
[0.0] Memory: 983488K/1048180K available (12300K kernel code, 2391K rwdta
```

Seguridad, ver referencia 17.

```
[228243285.0] evm: security.selinux  
[232011134.0] evm: security.SMACK64  
[236008501.0] evm: security.SMACK64EXEC  
[240007990.0] evm: security.SMACK64TRANSMUTE  
[244004736.0] evm: security.SMACK64MMAP  
[248007490.0] evm: security.apparmor  
[252007875.0] evm: security.ima  
[255626852.0] evm: security.capability
```

EL RCT no coincide con el timestamp!!!, puede ser una coordinación de tiempos.
el 28 de agosto de 2018 a las 10:27:31 UTC..

```
[264281367.0] RTC time: 12:04:38, date: 12/21/18
```

Reinicio del Servidor. 1 de septiembre de 2018 a las 09:53:22 UTC

```
[343815640354.343] systemd: 36 output lines suppressed due to ratelimiting  
[343819811212.343] systemd[1]: systemd 237 running in system mode. (+PAM +AUDIT  
+SELINUX +IMA +APPARMOR +SMACK +SYSVINIT +UTMP +LIBCRYPTSETUP +GCRYPT +GNUTLS +ACL  
+XZ +LZ4 +SECCOMP +BLKID +ELFUTILS +KMOD -IDN2 +IDN -PCRE2 default-  
hierarchy=hybrid)  
[343819860527.343] systemd[1]: Detected virtualization xen.  
[343819868348.343] systemd[1]: Detected architecture x86-64.
```

Reinicio del servicio Journal 1 de septiembre de 2018 a las 09:59:10 UTC

```
[344163440924.344] systemd[1]: Stopping Journal Service...  
[344166748005.344] systemd-journald[393]: Received SIGTERM from PID 1 (systemd).  
[344191632037.344] systemd[1]: Stopped Journal Service.  
[344193359863.344] systemd[1]: Starting Journal Service...  
[344209913346.344] systemd[1]: Started Journal Service.
```

Inicio de denegación de servicio SQL 3 de mayo de 2019 a las 20:10:29 UTC.

```
[21462442803498.21462] kauditd_printk_skb: 13 callbacks suppressed  
[21462442805151.21462] audit: type=1400 audit(1545415341.020:74):  
apparmor="STATUS" operation="profile_load" profile="unconfined"  
name="/usr/sbin/mysqld" pid=773 comm="apparmor_parser"  
[21463206148453.21463] audit: type=1400 audit(1545415341.784:75):  
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"  
name="/sys/devices/system/node/" pid=867 comm="mysqld" requested_mask="r"  
denied_mask="r" fsuid=0 ouid=0  
[21463221380545.21463] audit: type=1400 audit(1545415341.800:76):  
apparmor="DENIED" operation="capable" profile="/usr/sbin/mysqld" pid=867  
comm="mysqld" capability=2 capname="dac_read_search"  
[21463255863431.21463] audit: type=1400 audit(1545415341.836:77):
```

```
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=879 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=111 ouid=0
```

Denegación de servicio SQL 7 de mayo de 2019 a las 05:53:01 UTC

```
[21756594961731.21756] audit: type=1400 audit(1545415635.164:78):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=2652 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[21833553902942.21833] audit: type=1400 audit(1545415712.122:79):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=3061 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[21875757992232.21875] audit: type=1400 audit(1545415754.321:80):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=3542 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
```

Denegación de servicio SQL 10 de mayo de 2019 a las 06:39:15.104327 UTC

```
[22018568104327.22018] audit: type=1400 audit(1545415897.129:81):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=3758 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22018607698200.22018] audit: type=1400 audit(1545415897.169:82):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=3763 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=111 ouid=0
[22074531220184.22074] audit: type=1400 audit(1545415953.092:83):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4539 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
```

12 de mayo de 2019 a las 12:02:32.671468 UTC

```
[22210765671468.22210] audit: type=1400 audit(1545416089.324:84):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4632 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22210807976537.22210] audit: type=1400 audit(1545416089.368:85):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4640 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=111 ouid=0
```

13 de mayo de 2019 a las 05:27:58 UTC, posible brecha y entrada no deseada en el sistema a traves de un ataque SQL. Se reemplaza un perfil en el sistema.

```
[22273491157183.22273] audit: type=1400 audit(1545416152.047:86):
apparmor="STATUS" operation="profile_replace" info="same as current profile,
skipping" profile="unconfined" name="/usr/sbin/mysqld" pid=4768
comm="apparmor_parser"
[22273549967523.22273] audit: type=1400 audit(1545416152.107:87):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
```

```
name="/sys/devices/system/node/" pid=4786 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22273604163691.22273] audit: type=1400 audit(1545416152.159:88):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4801 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22277537601294.22277] audit: type=1400 audit(1545416156.095:89):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4860 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0

# 13 de mayo de 2019 a las 07:20:17 UTC

[22280230105408.22280] audit: type=1400 audit(1545416158.786:90):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=4912 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22282295921818.22282] audit: type=1400 audit(1545416160.850:91):
apparmor="STATUS" operation="profile_replace" info="same as current profile,
skipping" profile="unconfined" name="/usr/sbin/mysqld" pid=4947
comm="apparmor_parser"
[22282854213630.22282] audit: type=1400 audit(1545416161.410:92):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=5019 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22282898519612.22282] audit: type=1400 audit(1545416161.454:93):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=5027 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=111 ouid=0

# 14 de mayo de 2019 a las 21:55:10 UTC

[22419123420018.22419] audit: type=1400 audit(1545416297.675:94):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=5121 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=0 ouid=0
[22419167903891.22419] audit: type=1400 audit(1545416297.719:95):
apparmor="DENIED" operation="open" profile="/usr/sbin/mysqld"
name="/sys/devices/system/node/" pid=5125 comm="mysqld" requested_mask="r"
denied_mask="r" fsuid=111 ouid=0
[25524580731645.25524] audit: type=1400 audit(1545419403.049:96):
apparmor="STATUS" operation="profile_load" profile="unconfined"
name="/snap/core/6130/usr/lib/snapd/snap-confine" pid=6200 comm="apparmor_parser"
[25524581172130.25524] audit: type=1400 audit(1545419403.049:97):
apparmor="STATUS" operation="profile_load" profile="unconfined"
name="/snap/core/6130/usr/lib/snapd/snap-confine//mount-namespace-capture-helper"
pid=6200 comm="apparmor_parser"
[25524661228460.25524] audit: type=1400 audit(1545419403.129:98):
apparmor="STATUS" operation="profile_replace" profile="unconfined"
name="snap.core.hook.configure" pid=6203 comm="apparmor_parser"
[25524667927860.25524] audit: type=1400 audit(1545419403.137:99):
apparmor="STATUS" operation="profile_replace" info="same as current profile,
skipping" profile="unconfined" name="snap-update-ns.core" pid=6205
comm="apparmor_parser"
```

```
# 19 de junio de 2019 a las 20:51:55.627714 UTC. Posible parcheo de la
vulnerabilidad.

[25525728627714.25525] audit: type=1400 audit(1545419404.197:100):
apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap-
update-ns.amazon-ssm-agent" pid=6264 comm="apparmor_parser"
[25525731681561.25525] audit: type=1400 audit(1545419404.201:101):
apparmor="STATUS" operation="profile_replace" profile="unconfined"
name="snap.amazon-ssm-agent.amazon-ssm-agent" pid=6265 comm="apparmor_parser"
[25525734393872.25525] audit: type=1400 audit(1545419404.201:102):
apparmor="STATUS" operation="profile_replace" profile="unconfined"
name="snap.amazon-ssm-agent.ssm-cli" pid=6266 comm="apparmor_parser"
[25525776327926.25525] audit: type=1400 audit(1545419404.245:103):
apparmor="STATUS" operation="profile_replace" profile="unconfined"
name="/snap/core/6130/usr/lib/snapd/snap-confine" pid=6271 comm="apparmor_parser"
[25525776541774.25525] audit: type=1400 audit(1545419404.245:104):
apparmor="STATUS" operation="profile_replace" profile="unconfined"
name="/snap/core/6130/usr/lib/snapd/snap-confine//mount-namespace-capture-helper"
pid=6271 comm="apparmor_parser"
[25525795866859.25525] audit: type=1400 audit(1545419404.265:105):
apparmor="STATUS" operation="profile_replace" profile="unconfined" name="snap-
update-ns.core" pid=6273 comm="apparmor_parser"
[66030429896299.66030] new mount options do not match the existing superblock,
will be ignored
[1108227154620838.1108227] lime: version magic '4.15.0-42-generic SMP mod_unload '
should be '4.15.0-1021-aws SMP mod_unload '
[1109556640120032.1109556] lime: loading out-of-tree module taints kernel.
[1109556640155159.1109556] lime: module verification failed: signature and/or
required key missing - tainting kernel
```

[Volver al texto del comando en la Sección 3.4.6.](#)

8.4.003.004.007.001. Comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021- aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_bash`.

```
sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f
'/home/jrodg85/Server_RAM.mem' linux_bash
```

La respuesta de la consola es la siguiente:

```
Volatility Foundation Volatility Framework 2.6.1
```

Pid	Name	Command	Time
<hr/>			
20577	bash	exit	2019-01-03 07:49:45 UTC+0000

20577	bash	2019-01-03 07:49:45 UTC+0000	sudo apt update
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo systemctl
restart	postfix		
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -uroot -p
20577	bash	2019-01-03 07:49:45 UTC+0000	cd apache2/
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo vi
/etc/mysql/debian.cnf			
20577	bash	2019-01-03 07:49:45 UTC+0000	ps -ef grep mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	tail access.log.1
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /var/www/html
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo kill -9 4539
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -als
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /
20577	bash	2019-01-03 07:49:45 UTC+0000	ps -ef grep mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo mysqld_safe --
skip-grant-tables			
20577	bash	2019-01-03 07:49:45 UTC+0000	H=? &
20577	bash	2019-01-03 07:49:45 UTC+0000	qls -l tmp
20577	bash	2019-01-03 07:49:45 UTC+0000	qls -l tmp
20577	bash	2019-01-03 07:49:45 UTC+0000	cd
20577	bash	2019-01-03 07:49:45 UTC+0000	exit
20577	bash	2019-01-03 07:49:45 UTC+0000	vi functions.php
20577	bash	2019-01-03 07:49:45 UTC+0000	ps -ef grep mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l /var/run/mysqld
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l /run
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -lt
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -lt more
20577	bash	2019-01-03 07:49:45 UTC+0000	vi access.log.1
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo
mysql_secure_installation			
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	p?JU
20577	bash	2019-01-03 07:49:45 UTC+0000	su mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	tail access.log
20577	bash	2019-01-03 07:49:45 UTC+0000	cat
/var/log/mysql/error.log			
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /var/log
20577	bash	2019-01-03 07:49:45 UTC+0000	find . -name
functions.php			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo apt install
python-certbot-apache			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo service apache2
restart			
20577	bash	2019-01-03 07:49:45 UTC+0000	ps -ef grep mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -uroot -p
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo apt-get install
apache2			
20577	bash	2019-01-03 07:49:45 UTC+0000	apt-cache search
mysql-server			
20577	bash	2019-01-03 07:49:45 UTC+0000	apt-cache search php
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -u root -p
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l

20577	bash	2019-01-03 07:49:45 UTC+0000	#1546501785
20577	bash	2019-01-03 07:49:45 UTC+0000	tail error.log
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo vi functions.php
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l /var/run
20577	bash	2019-01-03 07:49:45 UTC+0000	exit
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	apt-cache search php
	grep apache		
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo vi
	/etc/mysql/debian		
20577	bash	2019-01-03 07:49:45 UTC+0000	tail syslog
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo apt-get install
	mysql-server		
20577	bash	2019-01-03 07:49:45 UTC+0000	_service
20577	bash	2019-01-03 07:49:45 UTC+0000	apt-cache search
	mysql grep php		
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo cp
	/home/ubuntu/wordpress-4.9.8.tar.gz .		
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /var/log
20577	bash	2019-01-03 07:49:45 UTC+0000	cd
20577	bash	2019-01-03 07:49:45 UTC+0000	U
20577	bash	2019-01-03 07:49:45 UTC+0000	H???Nt??nu??6
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo mysqld_safe --
	skip-grant-tables &		
20577	bash	2019-01-03 07:49:45 UTC+0000	apt-cache search
	mysql		
20577	bash	2019-01-03 07:49:45 UTC+0000	pwd
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	`uSU
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo mv * ..
20577	bash	2019-01-03 07:49:45 UTC+0000	? ,YU
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo mysqld_safe --
	skip-grant-tables		
20577	bash	2019-01-03 07:49:45 UTC+0000	r="\$c_clear\$r"
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l /run
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	COMPREPLY=\$(\$(compgen
	-W "--help --local" -- \$cur_word))		
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo tar xzf
	wordpress-4.9.8.tar.gz		
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo apt-get install
	aapche2		
20577	bash	2019-01-03 07:49:45 UTC+0000	tail -100 kern.log
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -u root -p
20577	bash	2019-01-03 07:49:45 UTC+0000	cd ..
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /var/www/html/
20577	bash	2019-01-03 07:49:45 UTC+0000	ps -ef grep mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	apt-cache search php
20577	bash	2019-01-03 07:49:45 UTC+0000	cd wordpress/
20577	bash	2019-01-03 07:49:45 UTC+0000	cd hhtml
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo rm -r wordpress/

20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo chmod 777
/var/run/mysqld			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo apt upgrade
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo vi
/etc/apache2/sites-enabled/000-default.conf			
20577	bash	2019-01-03 07:49:45 UTC+0000	cd htmls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -uroot -p
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo chown -R www-
data:www-data html			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo mysqld_safe --
skip-grant-tables			
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /var/www/html
20577	bash	2019-01-03 07:49:45 UTC+0000	find . -name
functions.php -exec grep -H add_filer {} \;			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo apt install
libapache2-mod-php			
20577	bash	2019-01-03 07:49:45 UTC+0000	exit
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /var/lg
20577	bash	2019-01-03 07:49:45 UTC+0000	suudo mysqld_safe --
skip-grant-tables &			
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	cd
/var/log/apache2/sites-e			
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -u root -p
20577	bash	2019-01-03 07:49:45 UTC+0000	cd
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo service mysql
restart			
20577	bash	2019-01-03 07:49:45 UTC+0000	find . -name
functions.php -exec grep -H add_filter {} \;			
20577	bash	2019-01-03 07:49:45 UTC+0000	apt-cache search
apache2			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo apt-get update
20577	bash	2019-01-03 07:49:45 UTC+0000	cat debian
20577	bash	2019-01-03 07:49:45 UTC+0000	?2JU
20577	bash	2019-01-03 07:49:45 UTC+0000	echo "Test 1" mail
-s "Test 1" test12312321@mailinator.com			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo chmod 777
/run/mysqld/			
20577	bash	2019-01-03 07:49:45 UTC+0000	dpkg -l grep mysql-
server			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo certbot --apache
-d ganga.site -d www.ganga.site			
20577	bash	2019-01-03 07:49:45 UTC+0000	ps -ef grep mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /var/log/apache2/
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo mkdir
/run/mysqld			
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /etc/mysql/
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo grep root *

20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -u root -p
20577	bash	2019-01-03 07:49:45 UTC+0000	ps -ef grep mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo mysqld_safe --skip-grant-tables
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -u root
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l /run
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /var/log
20577	bash	2019-01-03 07:49:45 UTC+0000	cd
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo dpkg-reconfigure mysql-server-5.7
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo service mysql stop
20577	bash	2019-01-03 07:49:45 UTC+0000	cd apache2/
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo service mysql stop
20577	bash	2019-01-03 07:49:45 UTC+0000	cat /var/log/mysql/error.log
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo kill -9 3181
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -u root
20577	bash	2019-01-03 07:49:45 UTC+0000	more access.log.1
20577	bash	2019-01-03 07:49:45 UTC+0000	dpkg -l grep mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	chmod 777 /run/mysqld/
20577	bash	2019-01-03 07:49:45 UTC+0000	g MP?
(E)G wm[av] WM[AV] avi AVI ASF vob VOB bin dat divx DIVX vcd ps pes fli flv FLV fx m FXM viv rmp ram yuv mov MOV qt QT web[am] WEB[AM] mp[234] MP[234] m?(p)4[av] M? P)4[AV] mkv MKV og[agmvx] OG[AGMVX] t[ps] T[PS] m2t?(s) M2T?			
(S) mts MTS wav WAV flac FLAC asx ASX mng MNG srt m[eo]d M[EO]D s[3t]m S[3T]M it IT xm XM) +([0-9]).@(vdr VDR))?(.part)'			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo kill -9 3182
3542			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo kill -9 4179
20577	bash	2019-01-03 07:49:45 UTC+0000	ls
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo service mysql stop
20577	bash	2019-01-03 07:49:45 UTC+0000	?
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo service apache2 restart
20577	bash	2019-01-03 07:49:45 UTC+0000	ls
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo apt install mailutils
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -lt more
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo cat debian.cnf
20577	bash	2019-01-03 07:49:45 UTC+0000	exit
20577	bash	2019-01-03 07:49:45 UTC+0000	pwd
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -u root -p
20577	bash	2019-01-03 07:49:45 UTC+0000	cat /etc/issue
20577	bash	2019-01-03 07:49:45 UTC+0000	cd wordpress/
20577	bash	2019-01-03 07:49:45 UTC+0000	tail error.log
20577	bash	2019-01-03 07:49:45 UTC+0000	tail error.log
20577	bash	2019-01-03 07:49:45 UTC+0000	vi access.log

20577	bash	2019-01-03 07:49:45 UTC+0000	cd ..
20577	bash	2019-01-03 07:49:45 UTC+0000	cd wp-
content/themes/twentyseventeen/			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo systemctl
restart psotfix			
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	exit
20577	bash	2019-01-03 07:49:45 UTC+0000	
mysql_secure_installation			
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -uroot -p
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo cat
/etc/mysql/debian			
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l tmp
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -u root -p
20577	bash	2019-01-03 07:49:45 UTC+0000	tail syslog
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /tmp
20577	bash	2019-01-03 07:49:45 UTC+0000	exit
20577	bash	2019-01-03 07:49:45 UTC+0000	cd html
20577	bash	2019-01-03 07:49:45 UTC+0000	find . -name
functions.php -exec grep -H add_filter {} \;			
20577	bash	2019-01-03 07:49:45 UTC+0000	cat debian.cnf
20577	bash	2019-01-03 07:49:45 UTC+0000	mysql -u root
20577	bash	2019-01-03 07:49:45 UTC+0000	suudo
mysql_secure_installation			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo cat
/etc/mysql/debian.cnf			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo service apache2
restart			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo rm index.html
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo rm -r
/run/mysqld			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo vi wp-config.php
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo systemctl reload
apache2			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo service mysql
start			
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo vi
/etc/postfix/main.cf			
20577	bash	2019-01-03 07:49:45 UTC+0000	tail access.log
20577	bash	2019-01-03 07:49:45 UTC+0000	tail -100 syslog
20577	bash	2019-01-03 07:49:45 UTC+0000	ps -ef grep mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	cd /var/log/apache2/
20577	bash	2019-01-03 07:49:45 UTC+0000	ls -l
20577	bash	2019-01-03 07:49:45 UTC+0000	pwd
20577	bash	2019-01-03 07:49:45 UTC+0000	vi index.html
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo apachectl
configtest			
20577	bash	2019-01-03 07:49:45 UTC+0000	ps -ef grep mysql
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo mkdir
/var/run/mysqld			
20577	bash	2019-01-03 07:49:45 UTC+0000	tail access.log
20577	bash	2019-01-03 07:49:45 UTC+0000	exit
20577	bash	2019-01-03 07:49:45 UTC+0000	sudo add-apt-
repository ppa:certbot/certbot			

```

20577 bash 2019-01-03 07:49:45 UTC+0000 tail access.log
20577 bash 2019-01-03 07:49:45 UTC+0000 ls -l
20577 bash 2019-01-03 07:49:45 UTC+0000 tail -100 access.log
20577 bash 2019-01-03 07:49:45 UTC+0000 tail -100 access.log
20577 bash 2019-01-03 07:49:45 UTC+0000 execute-command
20577 bash 2019-01-03 07:49:45 UTC+0000 sudo mysqld_safe --
skip-grant-tables &
20577 bash 2019-01-03 07:49:45 UTC+0000 sudo kill 3181
20577 bash 2019-01-03 07:49:45 UTC+0000 exit
20577 bash 2019-01-03 07:49:45 UTC+0000 !
20577 bash 2019-01-03 07:49:45 UTC+0000 sudo service apache2
restart
20577 bash 2019-01-03 07:49:45 UTC+0000 sudo apt install php-
mysql
20577 bash 2019-01-03 07:49:45 UTC+0000 date
20577 bash 2019-01-03 07:49:45 UTC+0000 cd ap
20577 bash 2019-01-03 07:49:45 UTC+0000 ls -l
20577 bash 2019-01-03 07:49:45 UTC+0000 grep POST access.log
20577 bash 2019-01-03 07:49:45 UTC+0000 ls -l
20577 bash 2019-01-03 07:49:45 UTC+0000 vi access.log
20577 bash 2019-01-03 07:49:45 UTC+0000 ls -l
20577 bash 2019-01-03 07:49:45 UTC+0000 cd home
20577 bash 2019-01-03 07:49:45 UTC+0000 cd /var/log
20577 bash 2019-01-03 07:49:45 UTC+0000 sudo apchectl
configtest
20577 bash 2019-01-03 07:49:45 UTC+0000 sudo service mysql
start
20577 bash 2019-01-03 07:49:45 UTC+0000 sudo vi
/etc/php/7.2/apache2/php.ini
20577 bash 2019-01-03 07:49:45 UTC+0000 sudo kill -9 4178
20577 bash 2019-01-03 07:49:45 UTC+0000 tail -100 syslog
20577 bash 2019-01-03 07:49:45 UTC+0000 ps -ef| grep mysql
20577 bash 2019-01-03 07:49:45 UTC+0000 tail -100 syslog
20577 bash 2019-01-03 07:49:45 UTC+0000 sudo rm wordpress-
4.9.8.tar.gz
20577 bash 2019-01-03 07:49:45 UTC+0000 ls -l /run
20577 bash 2019-01-03 07:49:45 UTC+0000 ??OU
20577 bash 2019-01-03 07:49:45 UTC+0000 ls -l /etc/cron.d
20577 bash 2019-01-03 07:54:14 UTC+0000 ls -l
20577 bash 2019-01-03 07:54:14 UTC+0000 cd /tmp
20577 bash 2019-01-03 07:54:36 UTC+0000 sudo insmod lime-
4.15.0-42-generic.ko "path=captura.mem format=lime"
20577 bash 2019-01-03 07:54:50 UTC+0000 cat /etc/issue
20577 bash 2019-01-03 07:55:13 UTC+0000 uname -a
20577 bash 2019-01-03 08:16:13 UTC+0000 ls -l
20577 bash 2019-01-03 08:16:23 UTC+0000 rm lime-4.15.0-42-
generic.ko
20577 bash 2019-01-03 08:16:24 UTC+0000 ls -l
20577 bash 2019-01-03 08:16:46 UTC+0000 sudo insmod lime-
4.15.0-1021-aws.ko "path=captura.mem format=lime"

```

[Volver al texto del comando en la Sección 3.4.7.](#)

8.4.003.005.001.001. Comando sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_pslist.

```
sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f
'/home/jrodg85/Server_RAM.mem' linux_pslist
```

La respuesta de la consola ha sido la siguiente:

Offset	Name	Pid	PPid	Uid	Gid	DTB
Start Time						
-----	-----	-----	-----	-----	-----	-----
0xfffff90057df50000	systemd	1	0	0	0	-----
0x000000003b7ba000	2018-12-21 12:04:59 UTC+0000					
0xfffff90057df55b00	kthreadd	2	0	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057df52d80	kworker/0:0H	4	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057df916c0	mm_percpu_wq	6	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057df90000	ksoftirqd/0	7	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057df95b00	rcu_sched	8	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057df94440	rcu_bh	9	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057df92d80	migration/0	10	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057df9db00	watchdog/0	11	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057dff8000	cpuhp/0	12	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057dffdb00	kdevtmpfs	13	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057dffc440	netns	14	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057dffad80	rcu_tasks_kthre	15	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057dff96c0	kauditd	16	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057d49db00	xenbus	17	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057d49c440	xenwatch	18	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057d4996c0	khungtaskd	20	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057d498000	oom_reaper	21	2	0	0	-----
---	2018-12-21 12:04:59 UTC+0000					
0xfffff90057d510000	writeback	22	2	0	0	-----

--- 2018-12-21 12:04:59 UTC+0000						
0xfffff90057d515b00 kcompactd0	23	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d5144400 ksmd	24	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d512d80 khugepaged	25	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d5116c0 crypto	26	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d53db00 kintegrityd	27	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d53c440 kblockd	28	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d53ad80 ata_sff	29	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d5396c0 md	30	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d538000 edac-poller	31	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d7216c0 devfreq_wq	32	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d720000 watchdogd	33	2	0	0		-----
--- 2018-12-21 12:04:59 UTC+0000						-----
0xfffff90057d722d80 kswapd0	36	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff90057d724440 ecryptfs-kthrea	37	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff900579725b00 kthrotld	79	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff900579724440 nvme-wq	80	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff900579722d80 scsi_eh_0	81	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff9005797216c0 scsi_tmf_0	82	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff900579720000 scsi_eh_1	83	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff900579718000 scsi_tmf_1	84	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff900579710000 ipv6_addrconf	89	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff9005796e8000 kstrp	99	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff9005796ead80 kworker/0:1H	100	2	0	0		-----
--- 2018-12-21 12:05:00 UTC+0000						-----
0xfffff900576f896c0 raid5wq	280	2	0	0		-----
--- 2018-12-21 12:05:03 UTC+0000						-----
0xfffff900576f7db00 jbd2/xvda1-8	330	2	0	0		-----
--- 2018-12-21 12:05:03 UTC+0000						-----
0xfffff900576f7c440 ext4-rsv-conver	331	2	0	0		-----
--- 2018-12-21 12:05:03 UTC+0000						-----
0xfffff900576f796c0 iscsi_eh	395	2	0	0		-----
--- 2018-12-21 12:05:03 UTC+0000						-----
0xfffff9005797016c0 ib-comp-wq	408	2	0	0		-----

---	2018-12-21 12:05:04 UTC+0000						
0xfffff9005796c16c0	ib_mcast	409	2	0	0		-----
---	2018-12-21 12:05:04 UTC+0000						-----
0xfffff9005796c5b00	ib_nl_sa_wq	410	2	0	0		-----
---	2018-12-21 12:05:04 UTC+0000						-----
0xfffff900576f7ad80	lvmetad	414	1	0	0		
0x0000000039cf6000	2018-12-21 12:05:04 UTC+0000						
0xfffff9005796e96c0	rdma_cm	415	2	0	0		-----
---	2018-12-21 12:05:04 UTC+0000						-----
0xfffff90057971ad80	systemd-logind	712	1	0	0		
0x000000003b2b6000	2018-12-21 12:05:09 UTC+0000						
0xfffff900576f88000	dbus-daemon	720	1	103	107		
0x000000003bccaa000	2018-12-21 12:05:09 UTC+0000						
0xfffff900576f8ad80	cron	733	1	0	0		
0x000000003baaac000	2018-12-21 12:05:10 UTC+0000						
0xfffff9005796c0000	accounts-daemon	734	1	0	0		
0x000000003bb3c000	2018-12-21 12:05:10 UTC+0000						
0xfffff9005796ec440	lxcfs	737	1	0	0		
0x000000003b00e000	2018-12-21 12:05:10 UTC+0000						
0xfffff90057b014440	atd	749	1	0	0		
0x000000003b1a4000	2018-12-21 12:05:10 UTC+0000						
0xfffff90057ae28000	polkitd	771	1	0	0		
0x000000003af6e000	2018-12-21 12:05:10 UTC+0000						
0xfffff90057ae2ad80	agetty	785	1	0	0		
0x000000003bcc2000	2018-12-21 12:05:10 UTC+0000						
0xfffff90057ae2db00	agetty	791	1	0	0		
0x0000000039ff8000	2018-12-21 12:05:10 UTC+0000						
0xfffff90057bd196c0	loop0	951	2	0	0		-----
---	2018-12-21 12:05:15 UTC+0000						
0xfffff90057bd18000	loop1	1103	2	0	0		-----
---	2018-12-21 12:05:18 UTC+0000						
0xfffff90057a73c440	systemd-network	2788	1	100	102		
0x000000003a536000	2018-12-21 12:10:43 UTC+0000						
0xfffff90057a73db00	systemd-resolve	2804	1	101	103		
0x0000000039ea6000	2018-12-21 12:10:43 UTC+0000						
0xfffff900579712d80	systemd-timesyn	2818	1	-	62583		
0x000000003a75a000	2018-12-21 12:10:43 UTC+0000						
0xfffff90057a7396c0	systemd-journal	2825	1	0	0		
0x0000000004406000	2018-12-21 12:10:43 UTC+0000						
0xfffff9005445a0000	uuidd	5077	1	106	110		
0x0000000039ec8000	2018-12-21 12:11:11 UTC+0000						
0xfffff90057bd1ad80	systemd-udevd	5160	1	0	0		
0x000000003a790000	2018-12-21 12:11:12 UTC+0000						
0xfffff90057bd1db00	xfsalloc	10374	2	0	0		-----
---	2018-12-21 12:11:28 UTC+0000						
0xfffff90057bd1c440	xfs_mru_cache	10375	2	0	0		-----
---	2018-12-21 12:11:28 UTC+0000						
0xfffff90054466ad80	iscsid	10988	1	0	0		
0x0000000036d48000	2018-12-21 12:11:35 UTC+0000						
0xfffff90054466db00	iscsid	10989	1	0	0		
0x0000000039d76000	2018-12-21 12:11:35 UTC+0000						
0xfffff90057d49ad80	networkd-dispat	11199	1	0	0		
0x0000000039e26000	2018-12-21 12:11:37 UTC+0000						
0xfffff90057940c440	sshd	12159	1	0	0		

0x000000000472c000	2018-12-21 12:12:06 UTC+0000				
0xfffff90054f4cdb00	mysqld	5127	1	111	116
0x000000003af40000	2018-12-21 18:18:37 UTC+0000				
0xfffff90057b4cdb00	apache2	5469	1	0	0
0x00000000044da000	2018-12-21 18:29:25 UTC+0000				
0xfffff9005445a2d80	loop2	6189	2	0	0
--- 2018-12-21 19:10:22 UTC+0000					
0xfffff9005445a16c0	snapd	6219	1	0	0
0x0000000039eb2000	2018-12-21 19:10:23 UTC+0000				
0xfffff90054da68000	loop3	6349	2	0	0
--- 2018-12-21 19:10:26 UTC+0000					
0xfffff9005797196c0	amazon-ssm-agen	6445	1	0	0
0x0000000039e12000	2018-12-21 19:10:27 UTC+0000				
0xfffff9005796edb00	rsyslogd	26254	1	102	106
0x0000000017b26000	2018-12-30 10:44:51 UTC+0000				
0xfffff900557adad80	master	26489	1	0	0
0x0000000036a42000	2018-12-30 10:46:13 UTC+0000				
0xfffff900557ad8000	qmgr	26500	26489	112	117
0x0000000017baa000	2018-12-30 10:46:13 UTC+0000				
0xfffff90057940ad80	kworker/0:0	19056	2	0	0
--- 2019-01-03 04:24:46 UTC+0000					
0xfffff90057b010000	kworker/u30:2	19454	2	0	0
--- 2019-01-03 05:50:42 UTC+0000					
0xfffff9005448adb00	apache2	19704	5469	33	33
0x000000003a7ec000	2019-01-03 06:25:21 UTC+0000				
0xfffff9005448ac440	apache2	19705	5469	33	33
0x000000003ce4a000	2019-01-03 06:25:21 UTC+0000				
0xfffff9005448aad80	apache2	19706	5469	33	33
0x000000003cf7e000	2019-01-03 06:25:21 UTC+0000				
0xfffff900557b6ad80	apache2	19707	5469	33	33
0x000000002c6d8000	2019-01-03 06:25:21 UTC+0000				
0xfffff900579f34440	apache2	19708	5469	33	33
0x000000003ae1a000	2019-01-03 06:25:21 UTC+0000				
0xfffff900579715b00	kworker/0:1	19709	2	0	0
--- 2019-01-03 06:25:21 UTC+0000					
0xfffff900579f32d80	apache2	19952	5469	33	33
0x000000002c644000	2019-01-03 06:33:15 UTC+0000				
0xfffff900579f316c0	apache2	19953	5469	33	33
0x0000000036fcf000	2019-01-03 06:33:16 UTC+0000				
0xfffff900579f30000	apache2	20230	5469	33	33
0x000000000453c000	2019-01-03 07:26:31 UTC+0000				
0xfffff900557b6db00	apache2	20231	5469	33	33
0x000000003ad62000	2019-01-03 07:26:32 UTC+0000				
0xfffff900557b6c440	apache2	20232	5469	33	33
0x0000000036ccc000	2019-01-03 07:26:33 UTC+0000				
0xfffff900557b696c0	apache2	20233	5469	33	33
0x000000003b35e000	2019-01-03 07:26:34 UTC+0000				
0xfffff900557b68000	sh	20381	19952	33	33
--- 2019-01-03 07:32:10 UTC+0000					
0xfffff90054f620000	sshd	20483	12159	0	0
0x0000000016244000	2019-01-03 07:50:04 UTC+0000				
0xfffff9005797116c0	systemd	20485	1	1000	1000
0x000000003b608000	2019-01-03 07:50:05 UTC+0000				
0xfffff9005445c0000	(sd-pam)	20486	20485	1000	1000

```

0x0000000036902000 2019-01-03 07:50:05 UTC+0000
0xfffff90057b6bdb00 sshd                  20576   20483   1000   1000
0x0000000019760000 2019-01-03 07:50:05 UTC+0000
0xfffff90057b6bc440 bash                  20577   20576   1000   1000
0x000000001624c000 2019-01-03 07:50:05 UTC+0000
0xfffff900542fadb00 pickup                20703   26489   112    117
0x000000002c792000 2019-01-03 08:01:34 UTC+0000
0xfffff90057df516c0 kworker/u30:1        20781   2          0      0      -----
--- 2019-01-03 08:09:21 UTC+0000
0xfffff90057df54440 kworker/u30:0        20886   2          0      0      -----
--- 2019-01-03 08:16:28 UTC+0000
0xfffff90057b4396c0 sudo                 20893   20577   0      0
0x000000003b602000 2019-01-03 08:17:06 UTC+0000
0xfffff90057b43c440 insmod               20894   20893   0      0
0x00000000002f26000 2019-01-03 08:17:06 UTC+0000
0xfffff90057b015b00 kworker/0:2         20898   2          0      0      -----
--- 2019-01-03 08:17:06 UTC+0000

```

[Volver al texto del comando en la Sección 3.5.1.](#)

8.4.003.005.002.001. Comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_pstree`.

```

sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f
'/home/jrodg85/Server_RAM.mem' linux_pstree

```

La respuesta de la consola ha sido la siguiente:

```
Volatility Foundation Volatility Framework 2.6.1
```

Name	Pid	Uid
systemd	1	
.lvmtrad	414	
.systemd-logind	712	
.dbus-daemon	720	103
.cron	733	
.accounts-daemon	734	
.lxvfs	737	
.atd	749	
.polkitd	771	
.agetty	785	
.agetty	791	
.systemd-network	2788	100
.systemd-resolve	2804	101
.systemd-timesyn	2818	62583
.systemd-journal	2825	
.uuidd	5077	106

.systemd-udevd	5160
.iscsid	10988
.iscsid	10989
.networkd-dispat	11199
.sshd	12159
..sshd	20483
...sshd	20576 1000
....bash	20577 1000
.....sudo	20893
.....insmod	20894
.mysqld	5127 111
.apache2	5469
..apache2	19704 33
..apache2	19705 33
..apache2	19706 33
..apache2	19707 33
..apache2	19708 33
..apache2	19952 33
...[sh]	20381 33
..apache2	19953 33
..apache2	20230 33
..apache2	20231 33
..apache2	20232 33
..apache2	20233 33
.snapd	6219
.amazon-ssm-agen	6445
.rsyslogd	26254 102
.master	26489
..qmgr	26500 112
..pickup	20703 112
.systemd	20485 1000
..(sd-pam)	20486 1000
[kthreadd]	2
.[kworker/0:0H]	4
.[mm_percpu_wq]	6
.[ksoftirqd/0]	7
.[rcu_sched]	8
.[rcu_bh]	9
.[migration/0]	10
.[watchdog/0]	11
.[cpuhp/0]	12
.[kdevtmpfs]	13
.[netns]	14
.[rcu_tasks_kthre]	15
.[kauditfd]	16
.[xenbus]	17
.[xenwatch]	18
.[khungtaskd]	20
.[oom_reaper]	21
.[writeback]	22
.[kcompactd0]	23
.[ksmd]	24
.[khugepaged]	25
.[crypto]	26

.[kintegrityd]	27
.[kblockd]	28
.[ata_sff]	29
.[md]	30
.[edac-poller]	31
.[devfreq_wq]	32
.[watchdogd]	33
.[kswapd0]	36
.[ecryptfs-kthrea]	37
.[kthrotld]	79
.[nvme-wq]	80
.[scsi_eh_0]	81
.[scsi_tmf_0]	82
.[scsi_eh_1]	83
.[scsi_tmf_1]	84
.[ipv6_addrconf]	89
.[kstrp]	99
.[kworker/0:1H]	100
.[raid5wq]	280
.[jbd2/xvda1-8]	330
.[ext4-rsv-conver]	331
.[iscsi_eh]	395
.[ib-comp-wq]	408
.[ib_mcast]	409
.[ib_nl_sa_wq]	410
.[rdma_cm]	415
.[loop0]	951
.[loop1]	1103
.[xfsalloc]	10374
.[xfs_mru_cache]	10375
.[loop2]	6189
.[loop3]	6349
.[kworker/0:0]	19056
.[kworker/u30:2]	19454
.[kworker/0:1]	19709
.[kworker/u30:1]	20781
.[kworker/u30:0]	20886
.[kworker/0:2]	20898

[Volver al texto del comando en la Sección 3.5.2.](#)

8.4.003.006.003.001. Comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem' linux_netstat`.

```
sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f  
'/home/jrodg85/Server_RAM.mem' linux_netstat
```

La respuesta de la consola ha sido la siguiente:

```
Volatility Foundation Volatility Framework 2.6.1
UNIX 26653          systemd/1
UNIX 26655          systemd/1    /run/systemd/private
UNIX 439014         systemd/1
UNIX 12401          systemd/1    /run/systemd/notify
UNIX 12402          systemd/1
UNIX 12403          systemd/1
UNIX 674406         systemd/1    /run/systemd/journal/stdout
UNIX 27271          systemd/1
UNIX 27272          systemd/1
UNIX 12487          systemd/1    /run/lvm/lvmpolld.socket
UNIX 16183          systemd/1    /run/uuid/request
UNIX 16173          systemd/1    /run/acpid.socket
UNIX 12489          systemd/1    /run/systemd/journal/dev-log
UNIX 96496          systemd/1    /run/systemd/journal/stdout
UNIX 45081          systemd/1    /run/systemd/journal/stdout
UNIX 43741          systemd/1    /run/systemd/journal/stdout
UNIX 32383          systemd/1    /run/systemd/journal/stdout
UNIX 32104          systemd/1    /run/systemd/journal/stdout
UNIX 27373          systemd/1    /run/systemd/journal/stdout
UNIX 27010          systemd/1    /run/systemd/journal/stdout
UNIX 26769          systemd/1    /run/systemd/journal/stdout
UNIX 13606          systemd/1    /run/systemd/journal/stdout
UNIX 18718          systemd/1    /run/systemd/journal/stdout
UNIX 18729          systemd/1    /run/systemd/journal/stdout
UNIX 18730          systemd/1    /run/systemd/journal/stdout
UNIX 18731          systemd/1    /run/systemd/journal/stdout
UNIX 18756          systemd/1    /run/systemd/journal/stdout
UNIX 97213          systemd/1    /run/systemd/journal/stdout
UNIX 16178          systemd/1    /run/snapd.socket
UNIX 16180          systemd/1    /run/snapd-snap.socket
UNIX 12732          systemd/1    /run/udev/control
UNIX 12878          systemd/1    /run/lvm/lvmetad.socket
UNIX 16171          systemd/1    /var/run/dbus/system_bus_socket
UNIX 12417          systemd/1    /run/systemd/journal/stdout
UNIX 12419          systemd/1    /run/systemd/journal/socket
UNIX 12532          systemd/1    /run/systemd/journal/syslog
UNIX 16191          systemd/1    /var/lib/lxd/unix.socket
UNIX 13181          lvmetad/414
UNIX 13181          lvmetad/414
UNIX 12878          lvmetad/414    /run/lvm/lvmetad.socket
UNIX 16470          systemd-logind/712
UNIX 16470          systemd-logind/712
UNIX 16548          systemd-logind/712
UNIX 16630          systemd-logind/712
UNIX 16785          dbus-daemon/720
UNIX 16785          dbus-daemon/720
UNIX 16171          dbus-daemon/720    /var/run/dbus/system_bus_socket
UNIX 16822          dbus-daemon/720
UNIX 16823          dbus-daemon/720
UNIX 16824          dbus-daemon/720
UNIX 26801          dbus-daemon/720    /var/run/dbus/system_bus_socket
```

UNIX 43825	dbus-daemon/720	/var/run/dbus/system_bus_socket	
UNIX 16827	dbus-daemon/720	/var/run/dbus/system_bus_socket	
UNIX 27245	dbus-daemon/720	/var/run/dbus/system_bus_socket	
UNIX 17410	dbus-daemon/720	/var/run/dbus/system_bus_socket	
UNIX 18201	dbus-daemon/720	/var/run/dbus/system_bus_socket	
UNIX 26654	dbus-daemon/720	/var/run/dbus/system_bus_socket	
UNIX 16917	cron/733		
UNIX 16917	cron/733		
UNIX 16999	accounts-daemon/734		
UNIX 16999	accounts-daemon/734		
UNIX 17409	accounts-daemon/734		
UNIX 17231	lxcfs/737		
UNIX 17231	lxcfs/737		
UNIX 18200	polkitd/771		
UNIX 26767	systemd-network/2788		
UNIX 26767	systemd-network/2788		
UNIX 26789	systemd-network/2788		
UNIX 26796	systemd-network/2788		
UNIX 26797	systemd-network/2788		
UNIX 26798	systemd-network/2788		
UNIX 26799	systemd-network/2788		
UNIX 26800	systemd-network/2788		
UDP 172.31.38.110 : 68 0.0.0.0	:	0	systemd-network/2788
UNIX 27007	systemd-resolve/2804		
UNIX 27007	systemd-resolve/2804		
UNIX 27228	systemd-resolve/2804		
UNIX 27244	systemd-resolve/2804		
UDP 127.0.0.53 : 53 0.0.0.0	:	0	systemd-resolve/2804
TCP 127.0.0.53 : 53 0.0.0.0	:	0 LISTEN	systemd-resolve/2804
UNIX 27371	systemd-timesyn/2818		
UNIX 27371	systemd-timesyn/2818		
UNIX 27393	systemd-timesyn/2818		
UNIX 27396	systemd-timesyn/2818		
UNIX 27397	systemd-timesyn/2818		
UNIX 27398	systemd-timesyn/2818		
UNIX 27399	systemd-timesyn/2818		
UNIX 12417	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 12419	systemd-journal/2825	/run/systemd/journal/socket	
UNIX 12489	systemd-journal/2825	/run/systemd/journal/dev-log	
UNIX 27373	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 43741	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 27010	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 26769	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 96496	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 97213	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 674406	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 13606	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 32383	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 18718	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 18729	systemd-journal/2825	/run/systemd/journal/stdout	
UNIX 18730	systemd-journal/2825	/run/systemd/journal/stdout	

```

UNIX 18731      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 45081      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 18756      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 27521      systemd-journal/2825
UNIX 32104      systemd-journal/2825  /run/systemd/journal/stdout
UNIX 32103          uidd/5077
UNIX 32103          uidd/5077
UNIX 16183          uidd/5077  /run/uidd/request
UNIX 32381      systemd-udevd/5160
UNIX 32381      systemd-udevd/5160
UNIX 12732      systemd-udevd/5160  /run/udev/control
UNIX 32384      systemd-udevd/5160
UNIX 32388      systemd-udevd/5160
UNIX 32389      systemd-udevd/5160
UNIX 43155          iscsid/10988
UNIX 43143          iscsid/10989
UNIX 43153          iscsid/10989
UNIX 43740      networkd-dispat/11199
UNIX 43740      networkd-dispat/11199
UNIX 43824      networkd-dispat/11199
UNIX 45080          sshd/12159
UNIX 45080          sshd/12159
TCP    0.0.0.0      :  22 0.0.0.0      :  0 LISTEN
sshd/12159
TCP    ::          :  22 ::          :  0 LISTEN
sshd/12159
TCP    127.0.0.1    :  3306 0.0.0.0      :  0 LISTEN
mysqld/5127
UNIX 90469      mysqld/5127  /var/run/mysqld/mysqld.sock
TCP    0.0.0.0      :  0 0.0.0.0      :  0 CLOSE
apache2/5469
TCP    ::          :  80 ::          :  0 LISTEN
apache2/5469
TCP    0.0.0.0      :  0 0.0.0.0      :  0 CLOSE
apache2/5469
TCP    ::          :  443 ::          :  0 LISTEN
apache2/5469
UNIX 96495      snapd/6219
UNIX 96495      snapd/6219
UNIX 16178      snapd/6219  /run/snapd.socket
UNIX 16180      snapd/6219  /run/snapd-snap.socket
UNIX 97212      amazon-ssm-agen/6445
UNIX 97212      amazon-ssm-agen/6445
UNIX 12532      rsyslogd/26254 /run/systemd/journal/syslog
UNIX 439139      rsyslogd/26254 /var/spool/postfix/dev/log
UNIX 439143      rsyslogd/26254
UNIX 440157      master/26489
TCP    127.0.0.1    :  25 0.0.0.0      :  0 LISTEN
master/26489
TCP    ::1          :  25 ::          :  0 LISTEN
master/26489
UNIX 440176      master/26489
UNIX 440177      master/26489
UNIX 440178      master/26489  public/pickup

```

UNIX 440179	master/26489
UNIX 440180	master/26489
UNIX 440182	master/26489 public/cleanup
UNIX 440183	master/26489
UNIX 440184	master/26489
UNIX 440185	master/26489 public/qmgr
UNIX 440186	master/26489
UNIX 440187	master/26489
UNIX 440189	master/26489 private/tlsmgr
UNIX 440190	master/26489
UNIX 440191	master/26489
UNIX 440192	master/26489 private/rewrite
UNIX 440193	master/26489
UNIX 440194	master/26489
UNIX 440195	master/26489 private/bounce
UNIX 440196	master/26489
UNIX 440197	master/26489
UNIX 440198	master/26489 private/defer
UNIX 440199	master/26489
UNIX 440200	master/26489
UNIX 440201	master/26489 private/trace
UNIX 440202	master/26489
UNIX 440203	master/26489
UNIX 440204	master/26489 private/verify
UNIX 440205	master/26489
UNIX 440206	master/26489
UNIX 440207	master/26489 public/flush
UNIX 440208	master/26489
UNIX 440209	master/26489
UNIX 440210	master/26489 private/proxymap
UNIX 440211	master/26489
UNIX 440212	master/26489
UNIX 440213	master/26489 private/proxywrite
UNIX 440214	master/26489
UNIX 440215	master/26489
UNIX 440216	master/26489 private/smtp
UNIX 440217	master/26489
UNIX 440218	master/26489
UNIX 440219	master/26489 private/relay
UNIX 440220	master/26489
UNIX 440221	master/26489
UNIX 440222	master/26489 public/showq
UNIX 440223	master/26489
UNIX 440224	master/26489
UNIX 440225	master/26489 private/error
UNIX 440226	master/26489
UNIX 440227	master/26489
UNIX 440228	master/26489 private/retry
UNIX 440229	master/26489
UNIX 440230	master/26489
UNIX 440231	master/26489 private/discard
UNIX 440232	master/26489
UNIX 440233	master/26489
UNIX 440234	master/26489 private/local

UNIX 440235	master/26489			
UNIX 440236	master/26489			
UNIX 440237	master/26489 private/virtual			
UNIX 440238	master/26489			
UNIX 440239	master/26489			
UNIX 440240	master/26489 private/lmtp			
UNIX 440241	master/26489			
UNIX 440242	master/26489			
UNIX 440243	master/26489 private/anvil			
UNIX 440244	master/26489			
UNIX 440245	master/26489			
UNIX 440246	master/26489 private/scache			
UNIX 440247	master/26489			
UNIX 440248	master/26489			
UNIX 440249	master/26489 private/maildrop			
UNIX 440250	master/26489			
UNIX 440251	master/26489			
UNIX 440252	master/26489 private/uucp			
UNIX 440253	master/26489			
UNIX 440254	master/26489			
UNIX 440255	master/26489 private/ifmail			
UNIX 440256	master/26489			
UNIX 440257	master/26489			
UNIX 440258	master/26489 private/bsmtp			
UNIX 440259	master/26489			
UNIX 440260	master/26489			
UNIX 440261	master/26489 private/scalemail-backend			
UNIX 440262	master/26489			
UNIX 440263	master/26489			
UNIX 440264	master/26489 private/mailman			
UNIX 440265	master/26489			
UNIX 440266	master/26489			
UNIX 440187	qmgr/26500			
UNIX 440185	qmgr/26500 public/qmgr			
UNIX 440388	qmgr/26500			
TCP 0.0.0.0	:	0.0.0.0	:	0 CLOSE
apache2/19704				
TCP ::	:	80 ::	:	0 LISTEN
apache2/19704				
TCP 0.0.0.0	:	0.0.0.0	:	0 CLOSE
apache2/19704				
TCP ::	:	443 ::	:	0 LISTEN
apache2/19704				
TCP 0.0.0.0	:	0.0.0.0	:	0 CLOSE
apache2/19705				
TCP ::	:	80 ::	:	0 LISTEN
apache2/19705				
TCP 0.0.0.0	:	0.0.0.0	:	0 CLOSE
apache2/19705				
TCP ::	:	443 ::	:	0 LISTEN
apache2/19705				
TCP 0.0.0.0	:	0.0.0.0	:	0 CLOSE
apache2/19706				
TCP ::	:	80 ::	:	0 LISTEN

```

apache2/19706
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/19706
TCP      ::          :      443 ::          :      0 LISTEN
apache2/19706
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/19707
TCP      ::          :      80 ::          :      0 LISTEN
apache2/19707
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/19707
TCP      ::          :      443 ::          :      0 LISTEN
apache2/19707
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/19708
TCP      ::          :      80 ::          :      0 LISTEN
apache2/19708
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/19708
TCP      ::          :      443 ::          :      0 LISTEN
apache2/19708
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/19952
TCP      ::          :      80 ::          :      0 LISTEN
apache2/19952
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/19952
TCP      ::          :      443 ::          :      0 LISTEN
apache2/19952
TCP      ::fffff172.31.38.110: 80 ::fffff18.195.165.56:41529 CLOSE_WAIT
apache2/19952
TCP      172.31.38.110 :46384 172.31.33.128 : 8080 ESTABLISHED
apache2/19952
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/19953
TCP      ::          :      80 ::          :      0 LISTEN
apache2/19953
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/19953
TCP      ::          :      443 ::          :      0 LISTEN
apache2/19953
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/20230
TCP      ::          :      80 ::          :      0 LISTEN
apache2/20230
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/20230
TCP      ::          :      443 ::          :      0 LISTEN
apache2/20230
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE
apache2/20231
TCP      ::          :      80 ::          :      0 LISTEN
apache2/20231
TCP      0.0.0.0      :      0 0.0.0.0      :      0 CLOSE

```

```

apache2/20231
TCP      ::          :  443  ::          :  0  LISTEN
apache2/20231
TCP      0.0.0.0      :  0  0.0.0.0      :  0  CLOSE
apache2/20232
TCP      ::          :  80  ::          :  0  LISTEN
apache2/20232
TCP      0.0.0.0      :  0  0.0.0.0      :  0  CLOSE
apache2/20232
TCP      ::          :  443  ::          :  0  LISTEN
apache2/20232
TCP      0.0.0.0      :  0  0.0.0.0      :  0  CLOSE
apache2/20233
TCP      ::          :  80  ::          :  0  LISTEN
apache2/20233
TCP      0.0.0.0      :  0  0.0.0.0      :  0  CLOSE
apache2/20233
TCP      ::          :  443  ::          :  0  LISTEN
apache2/20233
TCP      172.31.38.110  :  22  83.247.136.74  :16666 ESTABLISHED
sshd/20483
UNIX 674291          sshd/20483
UNIX 674626          sshd/20483
UNIX 674389          systemd/20485
UNIX 674389          systemd/20485
UNIX 674408          systemd/20485
UNIX 674432          systemd/20485 /run/user/1000/systemd/notify
UNIX 674433          systemd/20485
UNIX 674434          systemd/20485
UNIX 674435          systemd/20485 /run/user/1000/systemd/private
UNIX 674439          systemd/20485 /run/user/1000/gnupg/S.dirmngr
UNIX 674440          systemd/20485 /run/user/1000/gnupg/S.gpg-agent.ssh
UNIX 674441          systemd/20485 /run/user/1000/gnupg/S.gpg-agent.extra
UNIX 674442          systemd/20485 /run/user/1000/gnupg/S.gpg-agent
UNIX 674443          systemd/20485 /run/user/1000/gnupg/S.gpg-agent.browser
UNIX 674389          (sd-pam)/20486
UNIX 674389          (sd-pam)/20486
UNIX 674395          (sd-pam)/20486
TCP      172.31.38.110  :  22  83.247.136.74  :16666 ESTABLISHED
sshd/20576
UNIX 674291          sshd/20576
UNIX 674625          sshd/20576
UNIX 440180          pickup/20703
UNIX 440178          pickup/20703 public/pickup
UNIX 675208          pickup/20703
UNIX 676234          sudo/20893

```

[Volver al texto del comando en la Sección 3.5.2.](#)

8.4.003.006.003.002. Resumen del comando `sudo python2.7 vol.py --profile=LinuxlinuxUbuntu_4_15_0-1021-aws_profilex64 -f '/home/jrodg85/Server_RAM.mem'`

linux_netstat.

Un análisis del comando anterior es el siguiente

```
Volatility Foundation Volatility Framework 2.6.1
UDP      172.31.38.110    :  68 0.0.0.0          :  0           systemd-
network/2788
UDP      127.0.0.53       :  53 0.0.0.0          :  0           systemd-
resolve/2804
TCP      127.0.0.53       :  53 0.0.0.0          :  0 LISTEN   systemd-
resolve/2804
TCP      0.0.0.0          :  22 0.0.0.0          :  0 LISTEN   sshd/12159
TCP      ::                :  22 ::              :  0 LISTEN   sshd/12159
TCP      127.0.0.1         :  3306 0.0.0.0        :  0 LISTEN   mysqld/5127
TCP      0.0.0.0          :  0 0.0.0.0          :  0 CLOSE    apache2/5469
TCP      ::                :  80 ::              :  0 LISTEN   apache2/5469
TCP      0.0.0.0          :  0 0.0.0.0          :  0 CLOSE    apache2/5469
TCP      ::                :  443 ::             :  0 LISTEN   apache2/5469
TCP      127.0.0.1         :  25 0.0.0.0          :  0 LISTEN   master/26489
TCP      ::1               :  25 ::              :  0 LISTEN   master/26489
TCP      0.0.0.0          :  0 0.0.0.0          :  0 CLOSE    apache2/19704
TCP      ::                :  80 ::              :  0 LISTEN   apache2/19704
TCP      0.0.0.0          :  0 0.0.0.0          :  0 CLOSE    apache2/19704
TCP      ::                :  443 ::             :  0 LISTEN   apache2/19704
TCP      0.0.0.0          :  0 0.0.0.0          :  0 CLOSE    apache2/19705
TCP      ::                :  80 ::              :  0 LISTEN   apache2/19705
TCP      0.0.0.0          :  0 0.0.0.0          :  0 CLOSE    apache2/19705
TCP      ::                :  443 ::             :  0 LISTEN   apache2/19705
TCP      0.0.0.0          :  0 0.0.0.0          :  0 CLOSE    apache2/19706
TCP      ::                :  80 ::              :  0 LISTEN   apache2/19706
TCP      0.0.0.0          :  0 0.0.0.0          :  0 CLOSE    apache2/19706
TCP      ::                :  443 ::             :  0 LISTEN   
```

apache2/19706
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/19707
TCP :: : 80 :: : 0 LISTEN
apache2/19707
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/19707
TCP :: : 443 :: : 0 LISTEN
apache2/19707
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/19708
TCP :: : 80 :: : 0 LISTEN
apache2/19708
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/19708
TCP :: : 443 :: : 0 LISTEN
apache2/19708
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/19952
TCP :: : 80 :: : 0 LISTEN
apache2/19952
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/19952
TCP :: : 443 :: : 0 LISTEN
apache2/19952
TCP ::fffff172.31.38.110: 80 ::fffff18.195.165.56:41529 CLOSE_WAIT
apache2/19952
TCP 172.31.38.110 :46384 172.31.33.128 : 8080 ESTABLISHED
apache2/19953
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/19953
TCP :: : 80 :: : 0 LISTEN
apache2/19953
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/19953
TCP :: : 443 :: : 0 LISTEN
apache2/19953
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/20230
TCP :: : 80 :: : 0 LISTEN
apache2/20230
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/20230
TCP :: : 443 :: : 0 LISTEN
apache2/20230
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/20231
TCP :: : 80 :: : 0 LISTEN
apache2/20231
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE
apache2/20231
TCP :: : 443 :: : 0 LISTEN
apache2/20231
TCP 0.0.0.0 : 0 0.0.0.0 : 0 CLOSE

```
apache2/20232
TCP      ::          :     80  ::          :     0  LISTEN
apache2/20232
TCP      0.0.0.0      :     0  0.0.0.0      :     0  CLOSE
apache2/20232
TCP      ::          :     443 ::          :     0  LISTEN
apache2/20232
TCP      0.0.0.0      :     0  0.0.0.0      :     0  CLOSE
apache2/20233
TCP      ::          :     80  ::          :     0  LISTEN
apache2/20233
TCP      0.0.0.0      :     0  0.0.0.0      :     0  CLOSE
apache2/20233
TCP      ::          :     443 ::          :     0  LISTEN
apache2/20233
TCP      172.31.38.110  :     22  83.247.136.74  :16666 ESTABLISHED
sshd/20483
TCP      172.31.38.110  :     22  83.247.136.74  :16666 ESTABLISHED
sshd/20576
```

[Volver al texto del comando en la Sección 3.5.2.](#)

8.4.004.001.001. Comando Hash MD5.

```
Get-FileHash .\Server_HDD.E01 -Algorithm MD5
```

~~

La respuesta de PowerShell es el siguiente:

```
~~~PowerShell
Algorithm      Hash
Path
-----
MD5           324ED7DB769620E3FB55C027480D0EF3
C:\Users\jrodg85\Desktop\Nuev...
```

[Volver al texto del comando en la Sección 3.1](#)

8.4.004.001.002. Comando Hash SHA1.

```
Get-FileHash .\Server_HDD.E01 -Algorithm SHA1
```

La respuesta de PowerShell es el siguiente:

Algorithm	Hash
Path	-----
-----	-----
SHA1	3398F90D2438230AAAF7B5E8CE0A01E456D9CA10
C:\Users\jrodg85\Desktop\Nuev...	

[Volver al texto del comando en la Sección 3.1.](#)

8.4.004.003.001. Comando buscar usuarios inválidos en auth.log.

```
grep "Invalid user" auth.log
```

La respuesta de WSL es la siguiente:

```
Dec 31 06:29:18 ip-172-31-38-110 sshd[31534]: Invalid user celery from 113.22.4.10
port 47532
Dec 31 06:33:59 ip-172-31-38-110 sshd[31544]: Invalid user pi from 42.224.39.125
port 53150
Dec 31 06:46:38 ip-172-31-38-110 sshd[31629]: Invalid user Basisk from
115.159.218.200 port 64920
Dec 31 06:52:19 ip-172-31-38-110 sshd[31736]: Invalid user test from
150.95.146.154 port 59110
Dec 31 06:55:49 ip-172-31-38-110 sshd[31744]: Invalid user asteriskuser from
201.76.162.152 port 35365
Dec 31 07:14:53 ip-172-31-38-110 sshd[31841]: Invalid user ur from 193.193.67.82
port 48226
Dec 31 07:16:58 ip-172-31-38-110 sshd[31847]: Invalid user deploy from
181.188.208.46 port 43114
Dec 31 07:28:51 ip-172-31-38-110 sshd[31873]: Invalid user data from 198.98.60.234
port 52544
Dec 31 08:06:39 ip-172-31-38-110 sshd[32010]: Invalid user admin from 5.101.40.37
port 54776
Dec 31 08:06:43 ip-172-31-38-110 sshd[32012]: Invalid user ubnt from 5.101.40.38
port 60048
Dec 31 08:06:43 ip-172-31-38-110 sshd[32016]: Invalid user admin from 5.101.40.37
port 54501
Dec 31 08:08:13 ip-172-31-38-110 sshd[32025]: Invalid user angus from
101.89.114.94 port 59408
Dec 31 08:08:28 ip-172-31-38-110 sshd[32027]: Invalid user ansible from
190.96.54.68 port 59118
Dec 31 08:11:04 ip-172-31-38-110 sshd[32104]: Invalid user user2 from
178.128.98.90 port 36714
Dec 31 08:14:19 ip-172-31-38-110 sshd[32109]: Invalid user gary from 24.232.46.141
port 35192
Dec 31 08:15:24 ip-172-31-38-110 sshd[32113]: Invalid user muhammad from
132.148.152.53 port 56118
```

```
Dec 31 08:31:21 ip-172-31-38-110 sshd[32128]: Invalid user dario from
54.37.155.215 port 41238
Dec 31 08:42:47 ip-172-31-38-110 sshd[32209]: Invalid user gary from 93.39.196.245
port 43726
Dec 31 08:42:53 ip-172-31-38-110 sshd[32211]: Invalid user admin from
51.255.166.189 port 46619
Dec 31 08:46:09 ip-172-31-38-110 sshd[32215]: Invalid user user9 from
187.39.201.19 port 34959
Dec 31 08:47:33 ip-172-31-38-110 sshd[32222]: Invalid user qp from 200.35.109.138
port 53893
Dec 31 08:47:47 ip-172-31-38-110 sshd[32219]: Invalid user stream from
109.190.153.178 port 39292
Dec 31 08:48:02 ip-172-31-38-110 sshd[32225]: Invalid user prueba from
159.65.94.135 port 45316
Dec 31 08:49:30 ip-172-31-38-110 sshd[32227]: Invalid user unreal from
106.12.37.232 port 60964
Dec 31 08:49:37 ip-172-31-38-110 sshd[32229]: Invalid user weblogic from
106.51.70.251 port 47408
Dec 31 08:49:38 ip-172-31-38-110 sshd[32231]: Invalid user unreal from
219.246.78.18 port 54326
Dec 31 08:51:48 ip-172-31-38-110 sshd[32235]: Invalid user atlbitbucket from
213.234.26.179 port 43327
Dec 31 09:06:35 ip-172-31-38-110 sshd[32245]: Invalid user www from 61.147.181.27
port 24748
Dec 31 09:06:42 ip-172-31-38-110 sshd[32247]: Invalid user SYSTEM from
211.157.146.102 port 50144
Dec 31 09:20:16 ip-172-31-38-110 sshd[32329]: Invalid user zabbix from
104.248.124.163 port 36952
Dec 31 09:28:53 ip-172-31-38-110 sshd[32332]: Invalid user jira from
59.167.123.249 port 50092
Dec 31 09:29:51 ip-172-31-38-110 sshd[32337]: Invalid user tester from
79.127.55.189 port 58419
Dec 31 09:33:02 ip-172-31-38-110 sshd[32342]: Invalid user test from 106.12.212.39
port 52300
Dec 31 09:33:52 ip-172-31-38-110 sshd[32344]: Invalid user msda from
123.207.231.63 port 35416
Dec 31 09:40:24 ip-172-31-38-110 sshd[32421]: Invalid user mongodb2 from
37.187.54.45 port 44698
Dec 31 09:42:33 ip-172-31-38-110 sshd[32425]: Invalid user friend from
106.12.205.168 port 44786
Dec 31 10:01:46 ip-172-31-38-110 sshd[32441]: Invalid user ftp_user from
170.79.120.4 port 51350
Dec 31 10:04:45 ip-172-31-38-110 sshd[32444]: Invalid user administrador from
27.50.25.250 port 64736
Dec 31 10:08:25 ip-172-31-38-110 sshd[32447]: Invalid user user from 65.210.106.73
port 39120
Dec 31 10:12:48 ip-172-31-38-110 sshd[32524]: Invalid user tomcat from
62.234.208.99 port 46057
Dec 31 10:21:29 ip-172-31-38-110 sshd[32534]: Invalid user jake from
209.97.143.239 port 39281
Dec 31 10:30:37 ip-172-31-38-110 sshd[32540]: Invalid user squid from 79.8.94.58
port 58997
Dec 31 10:49:55 ip-172-31-38-110 sshd[32623]: Invalid user luis from 95.130.8.206
port 40214
```

```
Dec 31 11:02:47 ip-172-31-38-110 sshd[32639]: Invalid user ts3server from
132.232.108.143 port 47324
Dec 31 11:05:45 ip-172-31-38-110 sshd[32642]: Invalid user u1 from 68.188.68.18
port 36378
Dec 31 11:09:57 ip-172-31-38-110 sshd[32721]: Invalid user admin from 2.177.22.85
port 55076
Dec 31 11:17:36 ip-172-31-38-110 sshd[32733]: Invalid user admin from
114.223.167.124 port 55966
Dec 31 11:19:22 ip-172-31-38-110 sshd[32737]: Invalid user admin from 51.75.26.106
port 38278
Dec 31 11:21:00 ip-172-31-38-110 sshd[32741]: Invalid user gabi from
192.144.137.95 port 41616
Dec 31 11:23:17 ip-172-31-38-110 sshd[32744]: Invalid user user from 116.196.90.63
port 38532
Dec 31 11:30:46 ip-172-31-38-110 sshd[32751]: Invalid user user from 116.196.90.63
port 41936
Dec 31 11:35:25 ip-172-31-38-110 sshd[32755]: Invalid user write from 200.73.6.198
port 49326
Dec 31 11:42:34 ip-172-31-38-110 sshd[375]: Invalid user admin from 51.15.213.235
port 42026
Dec 31 11:52:34 ip-172-31-38-110 sshd[381]: Invalid user anastacia from
23.224.135.202 port 47806
Dec 31 12:15:15 ip-172-31-38-110 sshd[474]: Invalid user user from 191.17.188.119
port 59415
Dec 31 12:29:37 ip-172-31-38-110 sshd[500]: Invalid user admin from 80.14.3.159
port 37165
Dec 31 12:59:14 ip-172-31-38-110 sshd[587]: Invalid user gabriel from
175.117.145.239 port 21909
Dec 31 13:12:03 ip-172-31-38-110 sshd[670]: Invalid user pi from 178.14.21.238
port 34926
Dec 31 13:12:03 ip-172-31-38-110 sshd[672]: Invalid user pi from 178.14.21.238
port 34930
Dec 31 13:24:47 ip-172-31-38-110 sshd[693]: Invalid user admin from 168.253.72.209
port 36900
Dec 31 13:31:18 ip-172-31-38-110 sshd[704]: Invalid user temp from 114.80.118.185
port 47270
Dec 31 13:56:19 ip-172-31-38-110 sshd[804]: Invalid user jonathan from
206.189.167.33 port 36374
Dec 31 14:06:13 ip-172-31-38-110 sshd[814]: Invalid user test from 81.149.211.134
port 54414
Dec 31 14:09:23 ip-172-31-38-110 sshd[893]: Invalid user hduser from 61.19.254.65
port 40030
Dec 31 14:22:05 ip-172-31-38-110 sshd[907]: Invalid user mj from 178.128.116.162
port 45224
Dec 31 14:22:16 ip-172-31-38-110 sshd[909]: Invalid user camera from 73.53.95.248
port 44158
Dec 31 14:23:52 ip-172-31-38-110 sshd[911]: Invalid user loop from 91.121.154.100
port 56936
Dec 31 14:32:45 ip-172-31-38-110 sshd[918]: Invalid user lg from 125.71.211.10
port 47148
Dec 31 14:34:03 ip-172-31-38-110 sshd[920]: Invalid user glassfish from
106.12.109.250 port 47988
Dec 31 14:36:15 ip-172-31-38-110 sshd[923]: Invalid user nagios from 89.70.140.24
port 19583
```

```
Dec 31 14:36:34 ip-172-31-38-110 sshd[925]: Invalid user git from 50.21.180.85
port 51286
Dec 31 14:37:26 ip-172-31-38-110 sshd[927]: Invalid user git from 142.44.242.254
port 48328
Dec 31 14:38:48 ip-172-31-38-110 sshd[931]: Invalid user ms from 118.201.134.43
port 55155
Dec 31 14:54:54 ip-172-31-38-110 sshd[1013]: Invalid user ntp from 85.38.164.51
port 37162
Dec 31 14:55:02 ip-172-31-38-110 sshd[1015]: Invalid user ircbot from 200.33.10.14
port 32799
Dec 31 14:55:20 ip-172-31-38-110 sshd[1017]: Invalid user admin from
71.161.213.253 port 53573
Dec 31 15:05:51 ip-172-31-38-110 sshd[1026]: Invalid user ftptest from
217.92.99.172 port 60244
Dec 31 15:06:31 ip-172-31-38-110 sshd[1028]: Invalid user account from
110.227.189.6 port 57448
Dec 31 15:07:03 ip-172-31-38-110 sshd[1030]: Invalid user account from
104.248.148.60 port 37660
Dec 31 15:09:16 ip-172-31-38-110 sshd[1111]: Invalid user debian from
114.67.239.17 port 59368
Dec 31 15:12:18 ip-172-31-38-110 sshd[1114]: Invalid user gitolite from
202.166.206.166 port 37496
Dec 31 15:25:47 ip-172-31-38-110 sshd[1123]: Invalid user joel from 144.217.79.237
port 51520
Dec 31 15:26:48 ip-172-31-38-110 sshd[1125]: Invalid user pi from 159.203.123.25
port 45082
Dec 31 15:35:06 ip-172-31-38-110 sshd[1130]: Invalid user yan from 142.44.184.156
port 60124
Dec 31 15:35:44 ip-172-31-38-110 sshd[1132]: Invalid user yan from 201.68.138.187
port 5757
Dec 31 15:37:48 ip-172-31-38-110 sshd[1135]: Invalid user sftp from 118.24.54.178
port 42430
Dec 31 15:42:57 ip-172-31-38-110 sshd[1216]: Invalid user yang from 79.137.82.213
port 52526
Dec 31 15:43:16 ip-172-31-38-110 sshd[1218]: Invalid user super from 45.55.145.31
port 58007
Dec 31 15:55:58 ip-172-31-38-110 sshd[1283]: Invalid user student from
132.148.152.53 port 57128
Dec 31 15:59:32 ip-172-31-38-110 sshd[1289]: Invalid user wwwdata from
116.196.125.172 port 42638
Dec 31 15:59:47 ip-172-31-38-110 sshd[1291]: Invalid user saned from 37.59.6.106
port 52382
Dec 31 16:00:16 ip-172-31-38-110 sshd[1293]: Invalid user aris from 103.37.160.252
port 38528
Dec 31 16:05:45 ip-172-31-38-110 sshd[1299]: Invalid user christian from
120.131.9.177 port 10581
Dec 31 16:07:54 ip-172-31-38-110 sshd[1302]: Invalid user bnc from 27.122.250.248
port 43405
Dec 31 16:08:03 ip-172-31-38-110 sshd[1304]: Invalid user test from 178.128.217.40
port 36176
Dec 31 16:15:11 ip-172-31-38-110 sshd[1386]: Invalid user service from
45.55.156.159 port 49430
Dec 31 16:15:26 ip-172-31-38-110 sshd[1388]: Invalid user eg from 52.72.201.38
port 38515
```

```
Dec 31 16:26:13 ip-172-31-38-110 sshd[1397]: Invalid user test from 206.189.83.245
port 52614
Dec 31 16:30:27 ip-172-31-38-110 sshd[1401]: Invalid user admin from 78.186.8.194
port 40279
Dec 31 16:35:31 ip-172-31-38-110 sshd[1404]: Invalid user hadoop from
104.233.73.213 port 40465
Dec 31 16:41:37 ip-172-31-38-110 sshd[1483]: Invalid user sftp from 80.11.236.191
port 36551
Dec 31 17:22:16 ip-172-31-38-110 sshd[2019]: Invalid user music from 213.21.0.62
port 45314
Dec 31 17:23:15 ip-172-31-38-110 sshd[2022]: Invalid user tom from 128.199.189.192
port 50084
Dec 31 17:33:20 ip-172-31-38-110 sshd[2028]: Invalid user admin from 139.255.83.52
port 60894
Dec 31 17:33:27 ip-172-31-38-110 sshd[2030]: Invalid user oracle from
181.228.135.175 port 59410
Dec 31 17:33:32 ip-172-31-38-110 sshd[2032]: Invalid user cic from 183.6.176.182
port 49908
Dec 31 17:37:47 ip-172-31-38-110 sshd[2039]: Invalid user robin from
149.202.152.219 port 29170
Dec 31 17:42:13 ip-172-31-38-110 sshd[2119]: Invalid user ftpuser from
183.63.87.235 port 41320
Dec 31 17:52:27 ip-172-31-38-110 sshd[2125]: Invalid user nexus from
161.10.238.114 port 39956
Dec 31 17:52:56 ip-172-31-38-110 sshd[2127]: Invalid user git from 159.203.139.128
port 60304
Dec 31 17:54:38 ip-172-31-38-110 sshd[2130]: Invalid user trevor from
121.201.34.100 port 35206
Dec 31 17:55:52 ip-172-31-38-110 sshd[2132]: Invalid user friends from
52.169.27.152 port 39636
Dec 31 17:58:01 ip-172-31-38-110 sshd[2137]: Invalid user monitor from
185.62.129.91 port 52792
Dec 31 18:01:55 ip-172-31-38-110 sshd[2141]: Invalid user chris from 52.169.27.152
port 55424
Dec 31 18:11:24 ip-172-31-38-110 sshd[2222]: Invalid user svn from 91.112.90.6
port 45108
Dec 31 18:21:32 ip-172-31-38-110 sshd[2229]: Invalid user osboxes from
122.225.60.26 port 10545
Dec 31 18:28:08 ip-172-31-38-110 sshd[2235]: Invalid user sandeep from
129.211.104.184 port 36316
Dec 31 18:29:22 ip-172-31-38-110 sshd[2240]: Invalid user jaqueline from
151.80.155.98 port 34558
Dec 31 18:29:23 ip-172-31-38-110 sshd[2238]: Invalid user rancid from
129.191.22.195 port 27953
Dec 31 18:30:32 ip-172-31-38-110 sshd[2243]: Invalid user jaqueline from
91.46.13.104 port 21071
Dec 31 18:32:14 ip-172-31-38-110 sshd[2245]: Invalid user user from 37.139.121.129
port 34212
Dec 31 18:32:30 ip-172-31-38-110 sshd[2247]: Invalid user mysftp from
101.89.109.35 port 56986
Dec 31 18:41:54 ip-172-31-38-110 sshd[2324]: Invalid user kumar from 197.5.144.78
port 60093
Dec 31 18:42:09 ip-172-31-38-110 sshd[2326]: Invalid user kumar from 188.166.17.82
port 39120
```

```
Dec 31 18:53:52 ip-172-31-38-110 sshd[2335]: Invalid user mailserver from
161.132.195.76 port 46546
Dec 31 18:54:41 ip-172-31-38-110 sshd[2337]: Invalid user sampless from
187.72.141.129 port 54269
Dec 31 18:54:42 ip-172-31-38-110 sshd[2339]: Invalid user student09 from
178.254.13.216 port 36112
Dec 31 19:08:26 ip-172-31-38-110 sshd[2344]: Invalid user michal from
192.144.155.63 port 56152
Dec 31 19:08:31 ip-172-31-38-110 sshd[2346]: Invalid user varnish from
139.59.135.84 port 38294
Dec 31 19:12:04 ip-172-31-38-110 sshd[2426]: Invalid user csgoserver from
45.55.176.173 port 38632
Dec 31 19:13:01 ip-172-31-38-110 sshd[2428]: Invalid user ftpusr from
177.103.179.92 port 40058
Dec 31 19:15:18 ip-172-31-38-110 sshd[2433]: Invalid user email from 189.7.129.60
port 35993
Dec 31 19:20:54 ip-172-31-38-110 sshd[2441]: Invalid user nasa from 81.134.44.190
port 35305
Dec 31 19:23:07 ip-172-31-38-110 sshd[2445]: Invalid user git from 54.36.181.173
port 47280
Dec 31 19:23:12 ip-172-31-38-110 sshd[2447]: Invalid user confluence from
111.230.247.243 port 49360
Dec 31 19:26:17 ip-172-31-38-110 sshd[2450]: Invalid user toto from 36.110.217.176
port 51138
Dec 31 19:29:41 ip-172-31-38-110 sshd[2453]: Invalid user alan from
107.175.246.204 port 51586
Dec 31 19:40:02 ip-172-31-38-110 sshd[2538]: Invalid user admin from
150.109.101.46 port 38930
Dec 31 19:49:02 ip-172-31-38-110 sshd[2545]: Invalid user tommy from 64.71.131.98
port 43208
Dec 31 19:49:39 ip-172-31-38-110 sshd[2548]: Invalid user tommy from 46.101.22.87
port 37210
Dec 31 19:49:44 ip-172-31-38-110 sshd[2550]: Invalid user tommy from 51.68.230.28
port 35258
Dec 31 19:49:54 ip-172-31-38-110 sshd[2552]: Invalid user tommy from 169.239.13.41
port 42220
Dec 31 19:50:10 ip-172-31-38-110 sshd[2554]: Invalid user tommy from
67.167.203.131 port 52454
Dec 31 19:51:08 ip-172-31-38-110 sshd[2557]: Invalid user mailtest from
47.180.162.186 port 55642
Dec 31 19:52:19 ip-172-31-38-110 sshd[2559]: Invalid user tracy from 106.51.72.37
port 17681
Dec 31 19:53:04 ip-172-31-38-110 sshd[2561]: Invalid user gogs from 107.170.63.221
port 59542
Dec 31 19:53:41 ip-172-31-38-110 sshd[2563]: Invalid user or from 118.89.240.78
port 49662
Dec 31 19:56:15 ip-172-31-38-110 sshd[2568]: Invalid user rack from 101.236.5.253
port 54820
Dec 31 20:01:00 ip-172-31-38-110 sshd[2574]: Invalid user sa from 101.236.42.219
port 57624
Dec 31 20:03:30 ip-172-31-38-110 sshd[2579]: Invalid user edition from
106.12.13.26 port 58214
Dec 31 20:05:39 ip-172-31-38-110 sshd[2582]: Invalid user admin from 119.28.50.163
port 36828
```

```
Dec 31 20:09:01 ip-172-31-38-110 sshd[2585]: Invalid user black from 120.92.15.82
port 5282
Dec 31 20:10:53 ip-172-31-38-110 sshd[2662]: Invalid user otrs from 104.198.154.16
port 35004
Dec 31 20:11:11 ip-172-31-38-110 sshd[2664]: Invalid user glen from 51.68.230.28
port 43492
Dec 31 20:11:20 ip-172-31-38-110 sshd[2666]: Invalid user jeff from 217.182.71.54
port 58670
Dec 31 20:16:29 ip-172-31-38-110 sshd[2671]: Invalid user pieter from 78.131.56.62
port 58422
Dec 31 20:21:22 ip-172-31-38-110 sshd[2680]: Invalid user luis from 45.55.156.159
port 60964
Dec 31 20:33:12 ip-172-31-38-110 sshd[2687]: Invalid user web3 from
149.202.152.219 port 31327
Dec 31 20:33:25 ip-172-31-38-110 sshd[2689]: Invalid user build from
110.45.190.197 port 35134
Dec 31 20:35:25 ip-172-31-38-110 sshd[2692]: Invalid user jeff from 142.44.242.155
port 55821
Dec 31 20:35:30 ip-172-31-38-110 sshd[2694]: Invalid user octsr from 59.152.223.62
port 52428
Dec 31 20:44:43 ip-172-31-38-110 sshd[2773]: Invalid user jboss from 138.68.12.43
port 56770
Dec 31 20:45:01 ip-172-31-38-110 sshd[2775]: Invalid user aman from 61.147.181.27
port 25924
Dec 31 20:52:45 ip-172-31-38-110 sshd[2781]: Invalid user j from 24.156.128.7 port
42672
Dec 31 20:54:23 ip-172-31-38-110 sshd[2784]: Invalid user ventas from
37.187.118.14 port 36734
Dec 31 20:57:18 ip-172-31-38-110 sshd[2786]: Invalid user bruno from
125.124.26.178 port 44318
Dec 31 21:07:34 ip-172-31-38-110 sshd[2795]: Invalid user ts3server from
180.250.115.98 port 39433
Dec 31 21:09:22 ip-172-31-38-110 sshd[2872]: Invalid user splash from
49.248.167.102 port 56896
Dec 31 21:09:28 ip-172-31-38-110 sshd[2874]: Invalid user utente from
159.89.141.163 port 35010
Dec 31 21:17:51 ip-172-31-38-110 sshd[2882]: Invalid user sybase from
51.38.231.249 port 44856
Dec 31 21:17:58 ip-172-31-38-110 sshd[2884]: Invalid user jboss from
195.101.202.16 port 59519
Dec 31 21:24:08 ip-172-31-38-110 sshd[2887]: Invalid user sentry from
177.131.27.26 port 51517
Dec 31 21:26:03 ip-172-31-38-110 sshd[2889]: Invalid user operador from
219.239.47.66 port 49432
Dec 31 21:41:47 ip-172-31-38-110 sshd[2984]: Invalid user ftpuser from
103.241.183.235 port 54549
Dec 31 21:43:32 ip-172-31-38-110 sshd[2986]: Invalid user admin from 14.161.36.71
port 51206
Dec 31 22:01:11 ip-172-31-38-110 sshd[3011]: Invalid user admin from 5.150.236.109
port 44482
Dec 31 22:04:53 ip-172-31-38-110 sshd[3016]: Invalid user tester from
18.223.108.173 port 47410
Dec 31 22:07:34 ip-172-31-38-110 sshd[3018]: Invalid user vyos from 5.150.236.109
port 46304
```

```
Dec 31 22:09:56 ip-172-31-38-110 sshd[3097]: Invalid user mailer from 51.38.239.50
port 47320
Dec 31 22:10:31 ip-172-31-38-110 sshd[3099]: Invalid user vyatta from
5.150.236.109 port 47302
Dec 31 22:13:43 ip-172-31-38-110 sshd[3103]: Invalid user pi from 5.150.236.109
port 48272
Dec 31 22:14:05 ip-172-31-38-110 sshd[3105]: Invalid user ttadmin from
95.85.23.154 port 34100
Dec 31 22:14:13 ip-172-31-38-110 sshd[3107]: Invalid user admin from 91.134.140.32
port 43546
Dec 31 22:14:39 ip-172-31-38-110 sshd[3109]: Invalid user system from 167.99.76.63
port 54678
Dec 31 22:16:05 ip-172-31-38-110 sshd[3112]: Invalid user pppp from 157.230.24.38
port 48234
Dec 31 22:16:55 ip-172-31-38-110 sshd[3114]: Invalid user debian from
5.150.236.109 port 49222
Dec 31 22:20:21 ip-172-31-38-110 sshd[3129]: Invalid user osmc from 5.150.236.109
port 50152
Dec 31 22:23:48 ip-172-31-38-110 sshd[3133]: Invalid user xbian from 5.150.236.109
port 51080
Dec 31 22:27:00 ip-172-31-38-110 sshd[3137]: Invalid user ubnt from 5.150.236.109
port 52042
Dec 31 22:30:27 ip-172-31-38-110 sshd[3141]: Invalid user pi from 5.150.236.109
port 53072
Dec 31 22:33:53 ip-172-31-38-110 sshd[3144]: Invalid user bananapi from
5.150.236.109 port 53928
Dec 31 22:34:17 ip-172-31-38-110 sshd[3148]: Invalid user zhouh from 119.78.243.7
port 52076
Dec 31 22:34:32 ip-172-31-38-110 sshd[3151]: Invalid user pul from 119.78.243.4
port 40914
Dec 31 22:34:46 ip-172-31-38-110 sshd[3153]: Invalid user yuanwd from 119.78.243.7
port 57966
Dec 31 22:35:31 ip-172-31-38-110 sshd[3160]: Invalid user packer from 119.78.243.6
port 52616
Dec 31 22:35:46 ip-172-31-38-110 sshd[3162]: Invalid user packer from 119.78.243.7
port 41454
Dec 31 22:36:01 ip-172-31-38-110 sshd[3164]: Invalid user test1 from 119.78.243.7
port 58496
Dec 31 22:36:16 ip-172-31-38-110 sshd[3166]: Invalid user test2 from 119.78.243.4
port 47298
Dec 31 22:36:31 ip-172-31-38-110 sshd[3168]: Invalid user test3 from 119.78.243.7
port 36124
Dec 31 22:36:46 ip-172-31-38-110 sshd[3172]: Invalid user test4 from 119.78.243.9
port 53166
Dec 31 22:37:01 ip-172-31-38-110 sshd[3174]: Invalid user test5 from 119.78.243.7
port 41974
Dec 31 22:37:10 ip-172-31-38-110 sshd[3176]: Invalid user buildbot from
142.93.245.81 port 54084
Dec 31 22:37:15 ip-172-31-38-110 sshd[3178]: Invalid user user1 from 119.78.243.7
port 59014
Dec 31 22:37:31 ip-172-31-38-110 sshd[3180]: Invalid user user2 from 119.78.243.9
port 47826
Dec 31 22:37:38 ip-172-31-38-110 sshd[3182]: Invalid user buildbot from
23.30.117.166 port 35222
```

```
Dec 31 22:37:47 ip-172-31-38-110 sshd[3184]: Invalid user user3 from 119.78.243.7
port 36670
Dec 31 22:37:53 ip-172-31-38-110 sshd[3186]: Invalid user michael from
210.240.163.64 port 54972
Dec 31 22:38:02 ip-172-31-38-110 sshd[3188]: Invalid user user4 from 119.78.243.7
port 53728
Dec 31 22:38:19 ip-172-31-38-110 sshd[3190]: Invalid user user5 from 119.78.243.9
port 42562
Dec 31 22:38:41 ip-172-31-38-110 sshd[3194]: Invalid user michael from
128.199.162.14 port 41350
Dec 31 22:40:06 ip-172-31-38-110 sshd[3284]: Invalid user wh from 206.81.2.60 port
45432
Dec 31 22:40:10 ip-172-31-38-110 sshd[3286]: Invalid user vitaly from 51.38.48.127
port 58844
Dec 31 22:44:10 ip-172-31-38-110 sshd[3320]: Invalid user gabriel from
186.215.204.5 port 35440
Dec 31 22:47:19 ip-172-31-38-110 sshd[3347]: Invalid user jupiter from
51.75.198.127 port 37426
Dec 31 22:48:52 ip-172-31-38-110 sshd[3361]: Invalid user sadler from 61.183.9.191
port 36320
Dec 31 22:49:17 ip-172-31-38-110 sshd[3365]: Invalid user arnold from
202.201.242.182 port 52642
Dec 31 22:52:48 ip-172-31-38-110 sshd[3396]: Invalid user noreply from
120.92.210.64 port 22478
Dec 31 22:59:25 ip-172-31-38-110 sshd[3451]: Invalid user llama from
202.120.62.138 port 44856
Dec 31 23:00:43 ip-172-31-38-110 sshd[3464]: Invalid user michael from
159.203.179.230 port 59438
Dec 31 23:07:05 ip-172-31-38-110 sshd[3519]: Invalid user ts3srv from
164.132.225.151 port 58393
Dec 31 23:08:49 ip-172-31-38-110 sshd[3534]: Invalid user elasticsearch from
119.78.243.3 port 44626
Dec 31 23:09:06 ip-172-31-38-110 sshd[3611]: Invalid user elasticsearch from
119.78.243.7 port 33452
Dec 31 23:09:22 ip-172-31-38-110 sshd[3613]: Invalid user elasticsearch from
119.78.243.7 port 50512
Dec 31 23:09:38 ip-172-31-38-110 sshd[3615]: Invalid user elsearch from
119.78.243.5 port 39330
Dec 31 23:09:55 ip-172-31-38-110 sshd[3617]: Invalid user elsearch from
119.78.243.7 port 56372
Dec 31 23:10:11 ip-172-31-38-110 sshd[3620]: Invalid user elsearch from
119.78.243.3 port 45178
Dec 31 23:11:28 ip-172-31-38-110 sshd[3630]: Invalid user contabilidad from
178.48.181.9 port 34023
Dec 31 23:13:24 ip-172-31-38-110 sshd[3646]: Invalid user oracle from 119.78.243.7
port 52206
Dec 31 23:13:40 ip-172-31-38-110 sshd[3648]: Invalid user nagios from 119.78.243.7
port 41038
Dec 31 23:13:56 ip-172-31-38-110 sshd[3650]: Invalid user git from 119.78.243.9
port 58062
Dec 31 23:14:12 ip-172-31-38-110 sshd[3656]: Invalid user arkserver from
142.44.247.87 port 33226
Dec 31 23:14:12 ip-172-31-38-110 sshd[3654]: Invalid user hadoop from 119.78.243.7
port 46880
```

```
Dec 31 23:14:28 ip-172-31-38-110 sshd[3658]: Invalid user vnc from 119.78.243.7
port 35704
Dec 31 23:14:45 ip-172-31-38-110 sshd[3660]: Invalid user wang from 119.78.243.4
port 52762
Dec 31 23:15:01 ip-172-31-38-110 sshd[3662]: Invalid user postgres from
119.78.243.7 port 41594
Dec 31 23:15:17 ip-172-31-38-110 sshd[3667]: Invalid user deploy from 119.78.243.8
port 58654
Dec 31 23:17:10 ip-172-31-38-110 sshd[3687]: Invalid user brandon from
200.35.109.138 port 50533
Dec 31 23:24:45 ip-172-31-38-110 sshd[3751]: Invalid user terminfo from
106.12.127.25 port 48042
Dec 31 23:37:38 ip-172-31-38-110 sshd[3848]: Invalid user db2fenc1 from
119.78.243.5 port 39340
Dec 31 23:37:55 ip-172-31-38-110 sshd[3850]: Invalid user db2fenc1 from
119.78.243.7 port 56392
Dec 31 23:38:12 ip-172-31-38-110 sshd[3852]: Invalid user db2fenc1 from
119.78.243.5 port 45204
Dec 31 23:38:29 ip-172-31-38-110 sshd[3854]: Invalid user db2fenc1 from
119.78.243.7 port 34030
Dec 31 23:38:47 ip-172-31-38-110 sshd[3856]: Invalid user db2fenc1 from
119.78.243.7 port 51114
Dec 31 23:39:04 ip-172-31-38-110 sshd[3933]: Invalid user db2fenc1 from
119.78.243.7 port 39912
Dec 31 23:39:22 ip-172-31-38-110 sshd[3935]: Invalid user db2fenc1 from
119.78.243.6 port 56970
Dec 31 23:39:39 ip-172-31-38-110 sshd[3937]: Invalid user postgres from
119.78.243.7 port 45802
Dec 31 23:39:56 ip-172-31-38-110 sshd[3939]: Invalid user postgres from
119.78.243.7 port 34644
Dec 31 23:40:14 ip-172-31-38-110 sshd[3941]: Invalid user postgres from
119.78.243.7 port 51700
Dec 31 23:40:31 ip-172-31-38-110 sshd[3943]: Invalid user postgres from
119.78.243.7 port 40510
Dec 31 23:40:48 ip-172-31-38-110 sshd[3946]: Invalid user postgres from
119.78.243.6 port 57554
Dec 31 23:41:05 ip-172-31-38-110 sshd[3948]: Invalid user postgres from
119.78.243.7 port 46396
Dec 31 23:41:17 ip-172-31-38-110 sshd[3950]: Invalid user gate from 119.29.131.79
port 43682
Dec 31 23:41:22 ip-172-31-38-110 sshd[3952]: Invalid user postgres from
119.78.243.7 port 35218
Dec 31 23:41:39 ip-172-31-38-110 sshd[3954]: Invalid user oracle from 119.78.243.7
port 52278
Dec 31 23:41:57 ip-172-31-38-110 sshd[3956]: Invalid user oracle from 119.78.243.7
port 41116
Dec 31 23:42:14 ip-172-31-38-110 sshd[3958]: Invalid user oracle from 119.78.243.4
port 58170
Dec 31 23:42:32 ip-172-31-38-110 sshd[3960]: Invalid user oracle from 119.78.243.9
port 47000
Dec 31 23:42:49 ip-172-31-38-110 sshd[3962]: Invalid user oracle from 119.78.243.7
port 35824
Dec 31 23:43:07 ip-172-31-38-110 sshd[3964]: Invalid user oracle from 119.78.243.7
port 52878
```

```
Dec 31 23:43:24 ip-172-31-38-110 sshd[3966]: Invalid user oracle from 119.78.243.7
port 41720
Dec 31 23:43:41 ip-172-31-38-110 sshd[3968]: Invalid user user from 119.78.243.9
port 58778
Dec 31 23:43:59 ip-172-31-38-110 sshd[3970]: Invalid user user from 119.78.243.7
port 47616
Dec 31 23:44:17 ip-172-31-38-110 sshd[3972]: Invalid user user from 119.78.243.5
port 36454
Dec 31 23:44:34 ip-172-31-38-110 sshd[3974]: Invalid user user from 119.78.243.4
port 53506
Dec 31 23:44:52 ip-172-31-38-110 sshd[3976]: Invalid user user from 119.78.243.7
port 42334
Dec 31 23:45:10 ip-172-31-38-110 sshd[3978]: Invalid user user from 119.78.243.7
port 59396
Dec 31 23:45:27 ip-172-31-38-110 sshd[3980]: Invalid user test from 119.78.243.3
port 48182
Dec 31 23:45:44 ip-172-31-38-110 sshd[3982]: Invalid user test from 119.78.243.8
port 36982
Dec 31 23:46:01 ip-172-31-38-110 sshd[3985]: Invalid user test from 119.78.243.7
port 54034
Dec 31 23:46:19 ip-172-31-38-110 sshd[3987]: Invalid user test from 119.78.243.3
port 42846
Dec 31 23:46:36 ip-172-31-38-110 sshd[3989]: Invalid user test from 119.78.243.7
port 59908
Dec 31 23:46:53 ip-172-31-38-110 sshd[3991]: Invalid user test from 119.78.243.6
port 48704
Dec 31 23:49:13 ip-172-31-38-110 sshd[4007]: Invalid user tom from 119.78.243.7
port 43952
Dec 31 23:49:31 ip-172-31-38-110 sshd[4009]: Invalid user tom from 119.78.243.7
port 32774
Dec 31 23:49:48 ip-172-31-38-110 sshd[4011]: Invalid user tom from 119.78.243.9
port 49836
Dec 31 23:50:06 ip-172-31-38-110 sshd[4013]: Invalid user tom from 119.78.243.7
port 38632
Dec 31 23:50:23 ip-172-31-38-110 sshd[4015]: Invalid user tom from 119.78.243.9
port 55676
Dec 31 23:50:42 ip-172-31-38-110 sshd[4017]: Invalid user tom from 119.78.243.7
port 44488
Dec 31 23:51:00 ip-172-31-38-110 sshd[4019]: Invalid user tom from 119.78.243.4
port 33312
Dec 31 23:51:17 ip-172-31-38-110 sshd[4022]: Invalid user tomcat from 119.78.243.7
port 50386
Dec 31 23:51:35 ip-172-31-38-110 sshd[4024]: Invalid user tomcat from 119.78.243.7
port 39250
Dec 31 23:51:53 ip-172-31-38-110 sshd[4026]: Invalid user tomcat from 119.78.243.7
port 56318
Dec 31 23:52:10 ip-172-31-38-110 sshd[4030]: Invalid user tomcat from 119.78.243.8
port 45162
Dec 31 23:52:28 ip-172-31-38-110 sshd[4032]: Invalid user tomcat from 119.78.243.9
port 33972
Dec 31 23:52:46 ip-172-31-38-110 sshd[4034]: Invalid user tomcat from 119.78.243.4
port 51004
Dec 31 23:53:03 ip-172-31-38-110 sshd[4037]: Invalid user tomcat from 119.78.243.9
port 39810
```

```
Dec 31 23:53:22 ip-172-31-38-110 sshd[4039]: Invalid user cacti from 119.78.243.7
port 56872
Dec 31 23:53:39 ip-172-31-38-110 sshd[4041]: Invalid user cacti from 119.78.243.9
port 45674
Dec 31 23:53:57 ip-172-31-38-110 sshd[4043]: Invalid user cacti from 119.78.243.7
port 34486
Dec 31 23:54:16 ip-172-31-38-110 sshd[4045]: Invalid user cacti from 119.78.243.7
port 51504
Dec 31 23:54:33 ip-172-31-38-110 sshd[4047]: Invalid user cacti from 119.78.243.6
port 40324
Dec 31 23:54:51 ip-172-31-38-110 sshd[4049]: Invalid user cacti from 119.78.243.7
port 57382
Dec 31 23:55:08 ip-172-31-38-110 sshd[4051]: Invalid user cacti from 119.78.243.6
port 46204
Dec 31 23:55:27 ip-172-31-38-110 sshd[4053]: Invalid user ohh from 119.78.243.7
port 35040
Dec 31 23:55:45 ip-172-31-38-110 sshd[4057]: Invalid user ohh from 119.78.243.7
port 52072
Dec 31 23:55:46 ip-172-31-38-110 sshd[4059]: Invalid user administrator from
104.52.24.81 port 37726
Dec 31 23:56:03 ip-172-31-38-110 sshd[4061]: Invalid user ohh from 119.78.243.7
port 40914
Dec 31 23:56:21 ip-172-31-38-110 sshd[4064]: Invalid user ohh from 119.78.243.7
port 57976
Dec 31 23:56:38 ip-172-31-38-110 sshd[4066]: Invalid user ohh from 119.78.243.7
port 46804
Dec 31 23:56:50 ip-172-31-38-110 sshd[4068]: Invalid user millers from
62.234.131.188 port 37522
Dec 31 23:56:56 ip-172-31-38-110 sshd[4070]: Invalid user ohh from 119.78.243.7
port 35660
Dec 31 23:57:14 ip-172-31-38-110 sshd[4072]: Invalid user ohh from 119.78.243.5
port 52710
Dec 31 23:57:15 ip-172-31-38-110 sshd[4074]: Invalid user millers from
122.228.253.94 port 39554
Dec 31 23:57:32 ip-172-31-38-110 sshd[4076]: Invalid user solr from 119.78.243.9
port 41522
Dec 31 23:57:50 ip-172-31-38-110 sshd[4078]: Invalid user solr from 119.78.243.7
port 58600
Dec 31 23:58:09 ip-172-31-38-110 sshd[4080]: Invalid user solr from 119.78.243.7
port 47420
Dec 31 23:58:28 ip-172-31-38-110 sshd[4082]: Invalid user solr from 119.78.243.7
port 36244
Dec 31 23:58:46 ip-172-31-38-110 sshd[4084]: Invalid user solr from 119.78.243.8
port 53298
Dec 31 23:59:04 ip-172-31-38-110 sshd[4086]: Invalid user solr from 119.78.243.7
port 42114
Dec 31 23:59:24 ip-172-31-38-110 sshd[4088]: Invalid user solr from 119.78.243.7
port 59158
Dec 31 23:59:41 ip-172-31-38-110 sshd[4091]: Invalid user ec2-user from
119.78.243.7 port 47944
Dec 31 23:59:59 ip-172-31-38-110 sshd[4093]: Invalid user ec2-user from
119.78.243.9 port 36768
Jan 1 00:00:17 ip-172-31-38-110 sshd[4097]: Invalid user ec2-user from
119.78.243.7 port 53810
```

```
Jan  1 00:00:35 ip-172-31-38-110 sshd[4099]: Invalid user ec2-user from
119.78.243.7 port 42626
Jan  1 00:00:53 ip-172-31-38-110 sshd[4101]: Invalid user ec2-user from
119.78.243.7 port 59686
Jan  1 00:01:11 ip-172-31-38-110 sshd[4103]: Invalid user ec2-user from
119.78.243.7 port 48510
Jan  1 00:01:30 ip-172-31-38-110 sshd[4106]: Invalid user ec2-user from
119.78.243.7 port 37336
Jan  1 00:01:42 ip-172-31-38-110 sshd[4108]: Invalid userigor from 37.139.20.56
port 57408
Jan  1 00:04:00 ip-172-31-38-110 sshd[4124]: Invalid user dev from 119.78.243.9
port 60884
Jan  1 00:04:20 ip-172-31-38-110 sshd[4126]: Invalid user dev from 119.78.243.7
port 49714
Jan  1 00:04:38 ip-172-31-38-110 sshd[4129]: Invalid user dev from 119.78.243.7
port 38530
Jan  1 00:04:57 ip-172-31-38-110 sshd[4131]: Invalid user dev from 119.78.243.8
port 55586
Jan  1 00:05:15 ip-172-31-38-110 sshd[4133]: Invalid user dev from 119.78.243.7
port 44422
Jan  1 00:05:34 ip-172-31-38-110 sshd[4135]: Invalid user dev from 119.78.243.7
port 33232
Jan  1 00:05:53 ip-172-31-38-110 sshd[4137]: Invalid user dev from 119.78.243.9
port 50264
Jan  1 00:06:11 ip-172-31-38-110 sshd[4139]: Invalid user dev from 119.78.243.7
port 39104
Jan  1 00:06:30 ip-172-31-38-110 sshd[4141]: Invalid user jenkins from
119.78.243.7 port 56154
Jan  1 00:06:49 ip-172-31-38-110 sshd[4144]: Invalid user jenkins from
119.78.243.7 port 44986
Jan  1 00:07:08 ip-172-31-38-110 sshd[4146]: Invalid user jenkins from
119.78.243.7 port 33808
Jan  1 00:07:26 ip-172-31-38-110 sshd[4148]: Invalid user jenkins from
119.78.243.7 port 50858
Jan  1 00:07:44 ip-172-31-38-110 sshd[4150]: Invalid user jenkins from
119.78.243.7 port 39686
Jan  1 00:08:04 ip-172-31-38-110 sshd[4152]: Invalid user jenkins from
119.78.243.6 port 56744
Jan  1 00:08:19 ip-172-31-38-110 sshd[4154]: Invalid user brandon from
14.116.254.127 port 34974
Jan  1 00:08:24 ip-172-31-38-110 sshd[4156]: Invalid user jenkins from
119.78.243.7 port 45574
Jan  1 00:08:41 ip-172-31-38-110 sshd[4158]: Invalid user zabbix from 119.78.243.4
port 34424
Jan  1 00:08:42 ip-172-31-38-110 sshd[4160]: Invalid user loyd from 201.134.231.33
port 40651
Jan  1 00:08:47 ip-172-31-38-110 sshd[4162]: Invalid user brandon from
115.84.112.98 port 44256
Jan  1 00:09:00 ip-172-31-38-110 sshd[4164]: Invalid user zabbix from 119.78.243.7
port 51490
Jan  1 00:09:19 ip-172-31-38-110 sshd[4241]: Invalid user zabbix from 119.78.243.7
port 40298
Jan  1 00:09:37 ip-172-31-38-110 sshd[4243]: Invalid user zabbix from 119.78.243.7
port 57360
```

```
Jan  1 00:09:57 ip-172-31-38-110 sshd[4245]: Invalid user zabbix from 119.78.243.7
port 46198
Jan  1 00:10:17 ip-172-31-38-110 sshd[4247]: Invalid user zabbix from 119.78.243.3
port 35016
Jan  1 00:10:35 ip-172-31-38-110 sshd[4249]: Invalid user zabbix from 119.78.243.7
port 52098
Jan  1 00:10:54 ip-172-31-38-110 sshd[4251]: Invalid user weblogic from
119.78.243.4 port 40930
Jan  1 00:11:13 ip-172-31-38-110 sshd[4253]: Invalid user weblogic from
119.78.243.7 port 58000
Jan  1 00:11:32 ip-172-31-38-110 sshd[4256]: Invalid user weblogic from
119.78.243.7 port 46810
Jan  1 00:11:51 ip-172-31-38-110 sshd[4258]: Invalid user weblogic from
119.78.243.9 port 35618
Jan  1 00:12:10 ip-172-31-38-110 sshd[4260]: Invalid user weblogic from
119.78.243.4 port 52704
Jan  1 00:12:29 ip-172-31-38-110 sshd[4262]: Invalid user weblogic from
119.78.243.7 port 41530
Jan  1 00:12:48 ip-172-31-38-110 sshd[4264]: Invalid user weblogic from
119.78.243.9 port 58570
Jan  1 00:13:07 ip-172-31-38-110 sshd[4266]: Invalid user weblogic from
119.78.243.7 port 47374
Jan  1 00:13:26 ip-172-31-38-110 sshd[4268]: Invalid user content from
119.78.243.7 port 36196
Jan  1 00:13:45 ip-172-31-38-110 sshd[4270]: Invalid user content from
119.78.243.5 port 53276
Jan  1 00:14:04 ip-172-31-38-110 sshd[4272]: Invalid user content from
119.78.243.7 port 42116
Jan  1 00:14:23 ip-172-31-38-110 sshd[4274]: Invalid user content from
119.78.243.7 port 59164
Jan  1 00:14:42 ip-172-31-38-110 sshd[4276]: Invalid user content from
119.78.243.7 port 48002
Jan  1 00:15:02 ip-172-31-38-110 sshd[4278]: Invalid user content from
119.78.243.7 port 36862
Jan  1 00:15:20 ip-172-31-38-110 sshd[4280]: Invalid user content from
119.78.243.7 port 53938
Jan  1 00:15:40 ip-172-31-38-110 sshd[4282]: Invalid user jira from 119.78.243.6
port 42768
Jan  1 00:15:59 ip-172-31-38-110 sshd[4284]: Invalid user jira from 119.78.243.4
port 59834
Jan  1 00:16:18 ip-172-31-38-110 sshd[4286]: Invalid user jira from 119.78.243.9
port 48656
Jan  1 00:16:37 ip-172-31-38-110 sshd[4289]: Invalid user jira from 119.78.243.7
port 37464
Jan  1 00:16:57 ip-172-31-38-110 sshd[4291]: Invalid user jira from 119.78.243.7
port 54530
Jan  1 00:17:16 ip-172-31-38-110 sshd[4296]: Invalid user jira from 119.78.243.7
port 43344
Jan  1 00:17:35 ip-172-31-38-110 sshd[4298]: Invalid user jira from 119.78.243.7
port 60398
Jan  1 00:17:55 ip-172-31-38-110 sshd[4300]: Invalid user chef from 119.78.243.7
port 49236
Jan  1 00:18:14 ip-172-31-38-110 sshd[4302]: Invalid user chef from 119.78.243.9
port 38078
```

```
Jan  1 00:18:33 ip-172-31-38-110 sshd[4304]: Invalid user chef from 119.78.243.7
port 55132
Jan  1 00:18:52 ip-172-31-38-110 sshd[4306]: Invalid user chef from 119.78.243.7
port 43960
Jan  1 00:19:11 ip-172-31-38-110 sshd[4308]: Invalid user admin from 5.101.40.81
port 34053
Jan  1 00:19:11 ip-172-31-38-110 sshd[4310]: Invalid user chef from 119.78.243.7
port 32796
Jan  1 00:19:31 ip-172-31-38-110 sshd[4312]: Invalid user chef from 119.78.243.7
port 49858
Jan  1 00:19:50 ip-172-31-38-110 sshd[4314]: Invalid user chef from 119.78.243.7
port 38686
Jan  1 00:19:59 ip-172-31-38-110 sshd[4316]: Invalid user test from 118.179.136.26
port 41028
Jan  1 00:20:09 ip-172-31-38-110 sshd[4318]: Invalid user testuser from
119.78.243.7 port 55724
Jan  1 00:20:28 ip-172-31-38-110 sshd[4320]: Invalid user testuser from
119.78.243.3 port 44556
Jan  1 00:20:48 ip-172-31-38-110 sshd[4324]: Invalid user testuser from
119.78.243.7 port 33392
Jan  1 00:21:09 ip-172-31-38-110 sshd[4326]: Invalid user testuser from
119.78.243.5 port 50440
Jan  1 00:21:29 ip-172-31-38-110 sshd[4328]: Invalid user testuser from
119.78.243.7 port 39262
Jan  1 00:21:48 ip-172-31-38-110 sshd[4331]: Invalid user testuser from
119.78.243.7 port 56334
Jan  1 00:22:08 ip-172-31-38-110 sshd[4333]: Invalid user testuser from
119.78.243.7 port 45166
Jan  1 00:22:27 ip-172-31-38-110 sshd[4337]: Invalid user vagrant from
119.78.243.7 port 33988
Jan  1 00:22:46 ip-172-31-38-110 sshd[4339]: Invalid user vagrant from
119.78.243.7 port 51052
Jan  1 00:23:06 ip-172-31-38-110 sshd[4341]: Invalid user vagrant from
119.78.243.7 port 39894
Jan  1 00:23:26 ip-172-31-38-110 sshd[4343]: Invalid user vagrant from
119.78.243.6 port 56970
Jan  1 00:23:46 ip-172-31-38-110 sshd[4345]: Invalid user vagrant from
119.78.243.7 port 45818
Jan  1 00:24:06 ip-172-31-38-110 sshd[4347]: Invalid user vagrant from
119.78.243.9 port 34652
Jan  1 00:24:26 ip-172-31-38-110 sshd[4349]: Invalid user vagrant from
119.78.243.7 port 51722
Jan  1 00:24:48 ip-172-31-38-110 sshd[4351]: Invalid user vps from 119.78.243.8
port 40546
Jan  1 00:25:08 ip-172-31-38-110 sshd[4353]: Invalid user vps from 119.78.243.3
port 57634
Jan  1 00:25:30 ip-172-31-38-110 sshd[4355]: Invalid user vps from 119.78.243.6
port 46468
Jan  1 00:25:49 ip-172-31-38-110 sshd[4357]: Invalid user vps from 119.78.243.8
port 35308
Jan  1 00:26:08 ip-172-31-38-110 sshd[4359]: Invalid user vps from 119.78.243.5
port 52390
Jan  1 00:26:28 ip-172-31-38-110 sshd[4361]: Invalid user vps from 119.78.243.4
port 41212
```

```
Jan  1 00:26:48 ip-172-31-38-110 sshd[4363]: Invalid user vps from 119.78.243.7
port 58306
Jan  1 00:27:07 ip-172-31-38-110 sshd[4366]: Invalid user nagios from 119.78.243.7
port 47130
Jan  1 00:27:27 ip-172-31-38-110 sshd[4370]: Invalid user nagios from 119.78.243.7
port 35960
Jan  1 00:27:47 ip-172-31-38-110 sshd[4372]: Invalid user nagios from 119.78.243.5
port 53040
Jan  1 00:27:58 ip-172-31-38-110 sshd[4374]: Invalid user system from 92.222.84.34
port 39174
Jan  1 00:28:07 ip-172-31-38-110 sshd[4376]: Invalid user nagios from 119.78.243.3
port 41874
Jan  1 00:28:27 ip-172-31-38-110 sshd[4378]: Invalid user nagios from 119.78.243.9
port 58946
Jan  1 00:28:47 ip-172-31-38-110 sshd[4380]: Invalid user nagios from 119.78.243.3
port 47776
Jan  1 00:29:08 ip-172-31-38-110 sshd[4382]: Invalid user nagios from 119.78.243.9
port 36618
Jan  1 00:29:29 ip-172-31-38-110 sshd[4385]: Invalid user nagios from 119.78.243.5
port 53698
Jan  1 00:29:48 ip-172-31-38-110 sshd[4387]: Invalid user mongo from 119.78.243.7
port 42554
Jan  1 00:30:10 ip-172-31-38-110 sshd[4389]: Invalid user mongo from 119.78.243.9
port 59632
Jan  1 00:30:30 ip-172-31-38-110 sshd[4391]: Invalid user mongo from 119.78.243.7
port 48492
Jan  1 00:30:51 ip-172-31-38-110 sshd[4395]: Invalid user mongo from 119.78.243.5
port 37356
Jan  1 00:31:10 ip-172-31-38-110 sshd[4397]: Invalid user mongo from 119.78.243.7
port 54418
Jan  1 00:31:31 ip-172-31-38-110 sshd[4399]: Invalid user mongo from 119.78.243.7
port 43262
Jan  1 00:31:51 ip-172-31-38-110 sshd[4402]: Invalid user mongo from 119.78.243.7
port 60328
Jan  1 00:32:11 ip-172-31-38-110 sshd[4404]: Invalid user nexus from 119.78.243.7
port 49160
Jan  1 00:32:30 ip-172-31-38-110 sshd[4406]: Invalid user nexus from 119.78.243.7
port 38002
Jan  1 00:32:51 ip-172-31-38-110 sshd[4408]: Invalid user nexus from 119.78.243.7
port 55076
Jan  1 00:32:57 ip-172-31-38-110 sshd[4410]: Invalid user viper from
185.120.221.10 port 51252
Jan  1 00:33:11 ip-172-31-38-110 sshd[4412]: Invalid user nexus from 119.78.243.4
port 43926
Jan  1 00:33:32 ip-172-31-38-110 sshd[4414]: Invalid user nexus from 119.78.243.6
port 32784
Jan  1 00:33:52 ip-172-31-38-110 sshd[4416]: Invalid user nexus from 119.78.243.7
port 49854
Jan  1 00:34:12 ip-172-31-38-110 sshd[4418]: Invalid user nexus from 119.78.243.5
port 38696
Jan  1 00:34:33 ip-172-31-38-110 sshd[4424]: Invalid user nginx from 119.78.243.6
port 55776
Jan  1 00:34:53 ip-172-31-38-110 sshd[4426]: Invalid user nginx from 119.78.243.7
port 44640
```

```
Jan  1 00:35:13 ip-172-31-38-110 sshd[4428]: Invalid user nginx from 119.78.243.5
port 33502
Jan  1 00:35:34 ip-172-31-38-110 sshd[4430]: Invalid user nginx from 119.78.243.8
port 50574
Jan  1 00:35:54 ip-172-31-38-110 sshd[4432]: Invalid user nginx from 119.78.243.8
port 39420
Jan  1 00:36:15 ip-172-31-38-110 sshd[4434]: Invalid user nginx from 119.78.243.7
port 56490
Jan  1 00:36:35 ip-172-31-38-110 sshd[4436]: Invalid user nginx from 119.78.243.7
port 45318
Jan  1 00:36:55 ip-172-31-38-110 sshd[4439]: Invalid user vnc from 119.78.243.7
port 34158
Jan  1 00:37:15 ip-172-31-38-110 sshd[4441]: Invalid user vnc from 119.78.243.8
port 51194
Jan  1 00:37:36 ip-172-31-38-110 sshd[4443]: Invalid user vnc from 119.78.243.7
port 40022
Jan  1 00:37:56 ip-172-31-38-110 sshd[4445]: Invalid user vnc from 119.78.243.7
port 57076
Jan  1 00:38:16 ip-172-31-38-110 sshd[4447]: Invalid user vnc from 119.78.243.7
port 45908
Jan  1 00:38:37 ip-172-31-38-110 sshd[4449]: Invalid user vnc from 119.78.243.4
port 34730
Jan  1 00:38:58 ip-172-31-38-110 sshd[4453]: Invalid user vnc from 119.78.243.4
port 51802
Jan  1 00:39:19 ip-172-31-38-110 sshd[4457]: Invalid user azureuser from
119.78.243.7 port 40656
Jan  1 00:39:40 ip-172-31-38-110 sshd[4533]: Invalid user azureuser from
119.78.243.7 port 57752
Jan  1 00:40:00 ip-172-31-38-110 sshd[4535]: Invalid user azureuser from
119.78.243.4 port 46600
Jan  1 00:40:21 ip-172-31-38-110 sshd[4537]: Invalid user azureuser from
119.78.243.8 port 35402
Jan  1 00:40:41 ip-172-31-38-110 sshd[4539]: Invalid user azureuser from
119.78.243.7 port 52476
Jan  1 00:41:02 ip-172-31-38-110 sshd[4541]: Invalid user azureuser from
119.78.243.7 port 41312
Jan  1 00:41:22 ip-172-31-38-110 sshd[4543]: Invalid user azureuser from
119.78.243.7 port 58372
Jan  1 00:41:43 ip-172-31-38-110 sshd[4545]: Invalid user odoo from 119.78.243.9
port 47182
Jan  1 00:42:04 ip-172-31-38-110 sshd[4548]: Invalid user odoo from 119.78.243.7
port 36010
Jan  1 00:42:25 ip-172-31-38-110 sshd[4550]: Invalid user odoo from 119.78.243.7
port 53072
Jan  1 00:42:45 ip-172-31-38-110 sshd[4552]: Invalid user odoo from 119.78.243.3
port 41924
Jan  1 00:43:06 ip-172-31-38-110 sshd[4554]: Invalid user odoo from 119.78.243.8
port 58998
Jan  1 00:43:27 ip-172-31-38-110 sshd[4556]: Invalid user odoo from 119.78.243.7
port 47852
Jan  1 00:43:48 ip-172-31-38-110 sshd[4558]: Invalid user odoo from 119.78.243.6
port 36682
Jan  1 00:44:09 ip-172-31-38-110 sshd[4560]: Invalid user data from 119.78.243.7
port 53732
```

```
Jan  1 00:44:30 ip-172-31-38-110 sshd[4562]: Invalid user data from 119.78.243.4
port 42568
Jan  1 00:44:51 ip-172-31-38-110 sshd[4564]: Invalid user data from 119.78.243.5
port 59632
Jan  1 00:45:11 ip-172-31-38-110 sshd[4566]: Invalid user data from 119.78.243.7
port 48482
Jan  1 00:45:32 ip-172-31-38-110 sshd[4568]: Invalid user data from 119.78.243.6
port 37328
Jan  1 00:45:53 ip-172-31-38-110 sshd[4570]: Invalid user data from 119.78.243.4
port 54406
Jan  1 00:46:14 ip-172-31-38-110 sshd[4572]: Invalid user data from 119.78.243.3
port 43254
Jan  1 00:46:35 ip-172-31-38-110 sshd[4574]: Invalid user linuxacademy from
119.78.243.4 port 60308
Jan  1 00:46:56 ip-172-31-38-110 sshd[4576]: Invalid user linuxacademy from
119.78.243.7 port 49136
Jan  1 00:47:16 ip-172-31-38-110 sshd[4579]: Invalid user linuxacademy from
119.78.243.7 port 37960
Jan  1 00:47:40 ip-172-31-38-110 sshd[4583]: Invalid user linuxacademy from
119.78.243.7 port 55030
Jan  1 00:47:59 ip-172-31-38-110 sshd[4585]: Invalid user linuxacademy from
119.78.243.5 port 43874
Jan  1 00:48:20 ip-172-31-38-110 sshd[4588]: Invalid user linuxacademy from
119.78.243.7 port 60948
Jan  1 00:48:41 ip-172-31-38-110 sshd[4590]: Invalid user linuxacademy from
119.78.243.7 port 49802
Jan  1 00:49:02 ip-172-31-38-110 sshd[4592]: Invalid user deploy from 119.78.243.6
port 38640
Jan  1 00:49:24 ip-172-31-38-110 sshd[4594]: Invalid user deploy from 119.78.243.7
port 55712
Jan  1 00:49:45 ip-172-31-38-110 sshd[4596]: Invalid user deploy from 119.78.243.7
port 44540
Jan  1 00:50:06 ip-172-31-38-110 sshd[4598]: Invalid user deploy from 119.78.243.9
port 33388
Jan  1 00:50:28 ip-172-31-38-110 sshd[4600]: Invalid user deploy from 119.78.243.9
port 50462
Jan  1 00:50:49 ip-172-31-38-110 sshd[4602]: Invalid user deploy from 119.78.243.4
port 39312
Jan  1 00:51:10 ip-172-31-38-110 sshd[4604]: Invalid user deploy from 119.78.243.7
port 56374
Jan  1 00:51:31 ip-172-31-38-110 sshd[4608]: Invalid user redis from 119.78.243.6
port 45202
Jan  1 00:51:53 ip-172-31-38-110 sshd[4610]: Invalid user redis from 119.78.243.9
port 34030
Jan  1 00:52:14 ip-172-31-38-110 sshd[4612]: Invalid user redis from 119.78.243.7
port 51074
Jan  1 00:52:35 ip-172-31-38-110 sshd[4615]: Invalid user redis from 119.78.243.7
port 39892
Jan  1 00:52:57 ip-172-31-38-110 sshd[4617]: Invalid user redis from 119.78.243.7
port 56962
Jan  1 00:53:18 ip-172-31-38-110 sshd[4619]: Invalid user redis from 119.78.243.7
port 45804
Jan  1 00:53:39 ip-172-31-38-110 sshd[4621]: Invalid user redis from 119.78.243.7
port 34648
```

```
Jan  1 00:54:02 ip-172-31-38-110 sshd[4623]: Invalid user bpadmin from
119.78.243.6 port 51716
Jan  1 00:54:23 ip-172-31-38-110 sshd[4625]: Invalid user bpadmin from
119.78.243.7 port 40548
Jan  1 00:54:45 ip-172-31-38-110 sshd[4627]: Invalid user bpadmin from
119.78.243.3 port 57610
Jan  1 00:55:07 ip-172-31-38-110 sshd[4629]: Invalid user bpadmin from
119.78.243.7 port 46458
Jan  1 00:55:29 ip-172-31-38-110 sshd[4631]: Invalid user bpadmin from
119.78.243.4 port 35312
Jan  1 00:55:51 ip-172-31-38-110 sshd[4633]: Invalid user bpadmin from
119.78.243.4 port 52388
Jan  1 00:56:13 ip-172-31-38-110 sshd[4635]: Invalid user bpadmin from
119.78.243.7 port 41246
Jan  1 00:56:34 ip-172-31-38-110 sshd[4637]: Invalid user gpadmin from
119.78.243.9 port 58318
Jan  1 00:56:57 ip-172-31-38-110 sshd[4639]: Invalid user gpadmin from
119.78.243.7 port 47170
Jan  1 00:57:18 ip-172-31-38-110 sshd[4641]: Invalid user gpadmin from
119.78.243.3 port 36010
Jan  1 00:57:41 ip-172-31-38-110 sshd[4644]: Invalid user gpadmin from
119.78.243.7 port 53078
Jan  1 00:58:00 ip-172-31-38-110 sshd[4646]: Invalid user tamaki from
121.253.254.155 port 45249
Jan  1 00:58:01 ip-172-31-38-110 sshd[4648]: Invalid user gpadmin from
119.78.243.7 port 41930
Jan  1 00:58:23 ip-172-31-38-110 sshd[4652]: Invalid user gpadmin from
119.78.243.7 port 59030
Jan  1 00:58:45 ip-172-31-38-110 sshd[4654]: Invalid user spark from 119.78.243.8
port 47890
Jan  1 00:59:07 ip-172-31-38-110 sshd[4656]: Invalid user spark from 119.78.243.5
port 36746
Jan  1 00:59:29 ip-172-31-38-110 sshd[4659]: Invalid user spark from 119.78.243.5
port 53792
Jan  1 00:59:51 ip-172-31-38-110 sshd[4661]: Invalid user spark from 119.78.243.6
port 42626
Jan  1 01:00:12 ip-172-31-38-110 sshd[4666]: Invalid user spark from 119.78.243.7
port 59716
Jan  1 01:00:35 ip-172-31-38-110 sshd[4670]: Invalid user spark from 119.78.243.6
port 48542
Jan  1 01:00:57 ip-172-31-38-110 sshd[4672]: Invalid user spark from 119.78.243.7
port 37378
Jan  1 01:01:19 ip-172-31-38-110 sshd[4674]: Invalid user docker from 119.78.243.7
port 54456
Jan  1 01:01:41 ip-172-31-38-110 sshd[4676]: Invalid user docker from 119.78.243.5
port 43312
Jan  1 01:02:04 ip-172-31-38-110 sshd[4678]: Invalid user docker from 119.78.243.4
port 60390
Jan  1 01:02:25 ip-172-31-38-110 sshd[4680]: Invalid user docker from 119.78.243.7
port 49236
Jan  1 01:02:47 ip-172-31-38-110 sshd[4683]: Invalid user docker from 119.78.243.4
port 38084
Jan  1 01:03:09 ip-172-31-38-110 sshd[4685]: Invalid user docker from 119.78.243.7
port 55142
```

```
Jan  1 01:03:31 ip-172-31-38-110 sshd[4689]: Invalid user docker from 119.78.243.7
port 43988
Jan  1 01:03:53 ip-172-31-38-110 sshd[4691]: Invalid user mongodb from
119.78.243.7 port 32840
Jan  1 01:04:16 ip-172-31-38-110 sshd[4693]: Invalid user mongodb from
119.78.243.7 port 49912
Jan  1 01:04:37 ip-172-31-38-110 sshd[4695]: Invalid user mongodb from
119.78.243.8 port 38732
Jan  1 01:05:00 ip-172-31-38-110 sshd[4697]: Invalid user mongodb from
119.78.243.7 port 55802
Jan  1 01:05:22 ip-172-31-38-110 sshd[4699]: Invalid user mongodb from
119.78.243.5 port 44674
Jan  1 01:05:44 ip-172-31-38-110 sshd[4701]: Invalid user mongodb from
119.78.243.7 port 33538
Jan  1 01:06:06 ip-172-31-38-110 sshd[4703]: Invalid user mongodb from
119.78.243.7 port 50628
Jan  1 01:06:28 ip-172-31-38-110 sshd[4705]: Invalid user git from 119.78.243.7
port 39468
Jan  1 01:06:50 ip-172-31-38-110 sshd[4707]: Invalid user git from 119.78.243.7
port 56534
Jan  1 01:07:13 ip-172-31-38-110 sshd[4709]: Invalid user git from 119.78.243.7
port 45372
Jan  1 01:07:36 ip-172-31-38-110 sshd[4711]: Invalid user git from 119.78.243.7
port 34218
Jan  1 01:07:58 ip-172-31-38-110 sshd[4716]: Invalid user git from 119.78.243.8
port 51302
Jan  1 01:08:20 ip-172-31-38-110 sshd[4718]: Invalid user git from 119.78.243.7
port 40134
Jan  1 01:08:42 ip-172-31-38-110 sshd[4720]: Invalid user git from 119.78.243.7
port 57194
Jan  1 01:09:04 ip-172-31-38-110 sshd[4797]: Invalid user kafka from 119.78.243.7
port 46042
Jan  1 01:09:27 ip-172-31-38-110 sshd[4799]: Invalid user kafka from 119.78.243.7
port 34894
Jan  1 01:09:49 ip-172-31-38-110 sshd[4801]: Invalid user kafka from 119.78.243.5
port 51994
Jan  1 01:10:11 ip-172-31-38-110 sshd[4803]: Invalid user kafka from 119.78.243.7
port 40858
Jan  1 01:10:27 ip-172-31-38-110 sshd[4807]: Invalid user admin from 5.101.40.37
port 45082
Jan  1 01:10:29 ip-172-31-38-110 sshd[4809]: Invalid user ubnt from 5.101.40.37
port 56304
Jan  1 01:10:30 ip-172-31-38-110 sshd[4813]: Invalid user admin from 5.101.40.38
port 44719
Jan  1 01:10:33 ip-172-31-38-110 sshd[4815]: Invalid user kafka from 119.78.243.4
port 57958
Jan  1 01:10:56 ip-172-31-38-110 sshd[4817]: Invalid user kafka from 119.78.243.7
port 46816
Jan  1 01:11:18 ip-172-31-38-110 sshd[4819]: Invalid user kafka from 119.78.243.6
port 35660
Jan  1 01:11:41 ip-172-31-38-110 sshd[4821]: Invalid user hadoop from 119.78.243.5
port 52752
Jan  1 01:12:03 ip-172-31-38-110 sshd[4823]: Invalid user hadoop from 119.78.243.7
port 41606
```

```
Jan  1 01:12:16 ip-172-31-38-110 sshd[4825]: Invalid user pieter from
167.114.109.167 port 37942
Jan  1 01:12:26 ip-172-31-38-110 sshd[4827]: Invalid user hadoop from 119.78.243.7
port 58684
Jan  1 01:12:38 ip-172-31-38-110 sshd[4829]: Invalid user stefan from
121.134.159.21 port 48428
Jan  1 01:12:48 ip-172-31-38-110 sshd[4831]: Invalid user hadoop from 119.78.243.7
port 47536
Jan  1 01:13:11 ip-172-31-38-110 sshd[4834]: Invalid user hadoop from 119.78.243.7
port 36384
Jan  1 01:13:35 ip-172-31-38-110 sshd[4836]: Invalid user hadoop from 119.78.243.7
port 53462
Jan  1 01:13:58 ip-172-31-38-110 sshd[4838]: Invalid user hadoop from 119.78.243.7
port 42306
Jan  1 01:14:22 ip-172-31-38-110 sshd[4842]: Invalid user apache from 119.78.243.7
port 59356
Jan  1 01:14:46 ip-172-31-38-110 sshd[4844]: Invalid user apache from 119.78.243.5
port 48212
Jan  1 01:15:10 ip-172-31-38-110 sshd[4846]: Invalid user apache from 119.78.243.6
port 37052
Jan  1 01:15:34 ip-172-31-38-110 sshd[4849]: Invalid user apache from 119.78.243.5
port 54146
Jan  1 01:15:56 ip-172-31-38-110 sshd[4851]: Invalid user apache from 119.78.243.7
port 42980
Jan  1 01:16:19 ip-172-31-38-110 sshd[4853]: Invalid user apache from 119.78.243.7
port 60058
Jan  1 01:16:42 ip-172-31-38-110 sshd[4855]: Invalid user apache from 119.78.243.7
port 48904
Jan  1 01:17:04 ip-172-31-38-110 sshd[4860]: Invalid user centos from 119.78.243.7
port 37744
Jan  1 01:17:27 ip-172-31-38-110 sshd[4862]: Invalid user centos from 119.78.243.7
port 54828
Jan  1 01:17:52 ip-172-31-38-110 sshd[4864]: Invalid user centos from 119.78.243.7
port 43682
Jan  1 01:18:14 ip-172-31-38-110 sshd[4867]: Invalid user centos from 119.78.243.4
port 60760
Jan  1 01:18:38 ip-172-31-38-110 sshd[4869]: Invalid user centos from 119.78.243.7
port 49628
Jan  1 01:19:02 ip-172-31-38-110 sshd[4871]: Invalid user centos from 119.78.243.7
port 38480
Jan  1 01:19:25 ip-172-31-38-110 sshd[4873]: Invalid user centos from 119.78.243.7
port 55558
Jan  1 01:22:30 ip-172-31-38-110 sshd[4889]: Invalid user backups from
119.78.243.7 port 51014
Jan  1 01:22:54 ip-172-31-38-110 sshd[4891]: Invalid user backups from
119.78.243.7 port 39868
Jan  1 01:23:19 ip-172-31-38-110 sshd[4894]: Invalid user backups from
119.78.243.7 port 56966
Jan  1 01:23:42 ip-172-31-38-110 sshd[4896]: Invalid user backups from
119.78.243.4 port 45818
Jan  1 01:24:05 ip-172-31-38-110 sshd[4898]: Invalid user backups from
119.78.243.7 port 34660
Jan  1 01:24:08 ip-172-31-38-110 sshd[4900]: Invalid user ji from 157.230.15.57
port 55450
```

```
Jan  1 01:24:31 ip-172-31-38-110 sshd[4903]: Invalid user backups from
119.78.243.5 port 51758
Jan  1 01:24:53 ip-172-31-38-110 sshd[4906]: Invalid user backups from
119.78.243.7 port 40626
Jan  1 01:25:18 ip-172-31-38-110 sshd[4908]: Invalid user azureadmin from
119.78.243.5 port 57708
Jan  1 01:25:43 ip-172-31-38-110 sshd[4910]: Invalid user azureadmin from
119.78.243.7 port 46578
Jan  1 01:25:54 ip-172-31-38-110 sshd[4912]: Invalid user gitlab from
60.250.243.186 port 35138
Jan  1 01:26:08 ip-172-31-38-110 sshd[4914]: Invalid user azureadmin from
119.78.243.7 port 35434
Jan  1 01:26:32 ip-172-31-38-110 sshd[4916]: Invalid user azureadmin from
119.78.243.7 port 52534
Jan  1 01:26:56 ip-172-31-38-110 sshd[4918]: Invalid user azureadmin from
119.78.243.7 port 41396
Jan  1 01:27:20 ip-172-31-38-110 sshd[4922]: Invalid user azureadmin from
119.78.243.7 port 58482
Jan  1 01:27:45 ip-172-31-38-110 sshd[4924]: Invalid user azureadmin from
119.78.243.7 port 47336
Jan  1 01:28:09 ip-172-31-38-110 sshd[4926]: Invalid user azure from 119.78.243.7
port 36174
Jan  1 01:28:33 ip-172-31-38-110 sshd[4929]: Invalid user azure from 119.78.243.7
port 53244
Jan  1 01:28:56 ip-172-31-38-110 sshd[4931]: Invalid user azure from 119.78.243.7
port 42100
Jan  1 01:29:21 ip-172-31-38-110 sshd[4933]: Invalid user azure from 119.78.243.5
port 59174
Jan  1 01:29:44 ip-172-31-38-110 sshd[4936]: Invalid user azure from 119.78.243.7
port 48026
Jan  1 01:30:08 ip-172-31-38-110 sshd[4941]: Invalid user azure from 119.78.243.7
port 36888
Jan  1 01:30:32 ip-172-31-38-110 sshd[4943]: Invalid user azure from 119.78.243.7
port 53976
Jan  1 01:30:56 ip-172-31-38-110 sshd[4945]: Invalid user www from 119.78.243.7
port 42838
Jan  1 01:31:20 ip-172-31-38-110 sshd[4947]: Invalid user www from 119.78.243.7
port 59918
Jan  1 01:31:44 ip-172-31-38-110 sshd[4949]: Invalid user www from 119.78.243.7
port 48782
Jan  1 01:32:08 ip-172-31-38-110 sshd[4951]: Invalid user www from 119.78.243.7
port 37634
Jan  1 01:32:32 ip-172-31-38-110 sshd[4953]: Invalid user www from 119.78.243.4
port 54714
Jan  1 01:32:57 ip-172-31-38-110 sshd[4955]: Invalid user www from 119.78.243.7
port 43560
Jan  1 01:33:21 ip-172-31-38-110 sshd[4957]: Invalid user www from 119.78.243.6
port 60636
Jan  1 01:33:45 ip-172-31-38-110 sshd[4960]: Invalid user app from 119.78.243.7
port 49498
Jan  1 01:34:11 ip-172-31-38-110 sshd[4965]: Invalid user app from 119.78.243.7
port 38342
Jan  1 01:34:36 ip-172-31-38-110 sshd[4967]: Invalid user app from 119.78.243.7
port 55416
```

```
Jan  1 01:35:00 ip-172-31-38-110 sshd[4969]: Invalid user app from 119.78.243.7
port 44268
Jan  1 01:35:24 ip-172-31-38-110 sshd[4971]: Invalid user app from 119.78.243.7
port 33114
Jan  1 01:35:48 ip-172-31-38-110 sshd[5447]: Invalid user app from 119.78.243.7
port 50204
Jan  1 01:36:13 ip-172-31-38-110 sshd[5449]: Invalid user app from 119.78.243.7
port 39058
Jan  1 01:36:37 ip-172-31-38-110 sshd[5451]: Invalid user a from 119.78.243.6 port
56128
Jan  1 01:37:02 ip-172-31-38-110 sshd[5453]: Invalid user b from 119.78.243.7 port
44974
Jan  1 01:37:28 ip-172-31-38-110 sshd[5455]: Invalid user c from 119.78.243.9 port
33816
Jan  1 01:37:52 ip-172-31-38-110 sshd[5457]: Invalid user trainee from
119.78.243.3 port 50884
Jan  1 01:38:17 ip-172-31-38-110 sshd[5459]: Invalid user trainer from
119.78.243.7 port 39736
Jan  1 01:38:42 ip-172-31-38-110 sshd[5461]: Invalid user perry from 119.78.243.7
port 56814
Jan  1 01:39:07 ip-172-31-38-110 sshd[5542]: Invalid user developer from
119.78.243.7 port 45662
Jan  1 01:39:32 ip-172-31-38-110 sshd[5544]: Invalid user default from
119.78.243.9 port 34510
Jan  1 01:39:56 ip-172-31-38-110 sshd[5546]: Invalid user cloud-user from
119.78.243.9 port 51584
Jan  1 01:40:21 ip-172-31-38-110 sshd[5548]: Invalid user cpnelsolr from
119.78.243.7 port 40428
Jan  1 01:40:22 ip-172-31-38-110 sshd[5550]: Invalid user mickey from
159.65.145.175 port 33000
Jan  1 01:40:45 ip-172-31-38-110 sshd[5552]: Invalid user cistest from
119.78.243.7 port 57516
Jan  1 01:41:03 ip-172-31-38-110 sshd[5554]: Invalid user jojo from 178.32.137.119
port 59054
Jan  1 01:41:10 ip-172-31-38-110 sshd[5556]: Invalid user bistel from 119.78.243.7
port 46352
Jan  1 01:41:35 ip-172-31-38-110 sshd[5558]: Invalid user lextend from
119.78.243.6 port 35190
Jan  1 01:41:59 ip-172-31-38-110 sshd[5560]: Invalid user ubuntu12 from
119.78.243.7 port 52288
Jan  1 01:42:11 ip-172-31-38-110 sshd[5562]: Invalid user dis from 111.231.76.101
port 45020
Jan  1 01:42:24 ip-172-31-38-110 sshd[5564]: Invalid user pi from 119.78.243.7
port 41156
Jan  1 01:42:49 ip-172-31-38-110 sshd[5566]: Invalid user clouadmin from
119.78.243.4 port 58234
Jan  1 01:43:14 ip-172-31-38-110 sshd[5568]: Invalid user clouduser from
119.78.243.7 port 47084
Jan  1 01:43:39 ip-172-31-38-110 sshd[5570]: Invalid user deployer from
119.78.243.6 port 35934
Jan  1 01:44:04 ip-172-31-38-110 sshd[5573]: Invalid user ntp from 119.78.243.7
port 53006
Jan  1 01:59:06 ip-172-31-38-110 sshd[5580]: Invalid user vi from 192.99.68.130
port 52560
```

```
Jan  1 01:59:32 ip-172-31-38-110 sshd[5585]: Invalid user csgo from 51.75.201.55
port 58662
Jan  1 02:18:55 ip-172-31-38-110 sshd[5666]: Invalid user admin from 14.186.37.57
port 57786
Jan  1 02:19:51 ip-172-31-38-110 sshd[5669]: Invalid user dev from 112.186.72.190
port 36360
Jan  1 02:24:37 ip-172-31-38-110 sshd[5672]: Invalid user logan from 85.38.164.51
port 51812
Jan  1 02:27:22 ip-172-31-38-110 sshd[5675]: Invalid user webuser from
189.194.130.251 port 53750
Jan  1 02:31:12 ip-172-31-38-110 sshd[5679]: Invalid user mf from 93.104.208.151
port 53814
Jan  1 02:31:18 ip-172-31-38-110 sshd[5681]: Invalid user test from 46.101.9.250
port 45375
Jan  1 02:31:51 ip-172-31-38-110 sshd[5683]: Invalid user test from 91.229.106.49
port 38426
Jan  1 02:44:41 ip-172-31-38-110 sshd[5767]: Invalid user new from 104.131.178.223
port 60971
Jan  1 02:48:45 ip-172-31-38-110 sshd[5769]: Invalid user ben from 178.128.61.166
port 48689
Jan  1 02:56:12 ip-172-31-38-110 sshd[5774]: Invalid user test from 150.95.146.154
port 57788
Jan  1 03:16:43 ip-172-31-38-110 sshd[5876]: Invalid user prios from
188.166.245.70 port 50770
Jan  1 03:21:34 ip-172-31-38-110 sshd[5889]: Invalid user demo from 88.198.72.129
port 39156
Jan  1 03:21:47 ip-172-31-38-110 sshd[5891]: Invalid user demo from 195.181.209.71
port 39024
Jan  1 03:23:10 ip-172-31-38-110 sshd[5893]: Invalid user demo from
115.186.147.235 port 38171
Jan  1 03:25:09 ip-172-31-38-110 sshd[5897]: Invalid user fc from 139.199.119.97
port 54044
Jan  1 03:30:43 ip-172-31-38-110 sshd[5903]: Invalid user amax from 180.76.51.114
port 60196
Jan  1 03:40:12 ip-172-31-38-110 sshd[5991]: Invalid user sybase from
123.207.244.13 port 40526
Jan  1 03:46:32 ip-172-31-38-110 sshd[5996]: Invalid user frappe from 154.8.139.43
port 36698
Jan  1 03:53:35 ip-172-31-38-110 sshd[6003]: Invalid user admin from 5.101.40.37
port 35391
Jan  1 03:53:35 ip-172-31-38-110 sshd[6005]: Invalid user ubnt from 5.101.40.37
port 33704
Jan  1 03:53:35 ip-172-31-38-110 sshd[6009]: Invalid user admin from 5.101.40.37
port 39456
Jan  1 03:56:08 ip-172-31-38-110 sshd[6012]: Invalid user jboss from
172.76.228.184 port 33026
Jan  1 03:57:19 ip-172-31-38-110 sshd[6015]: Invalid user admin from
107.175.246.204 port 34666
Jan  1 04:07:08 ip-172-31-38-110 sshd[6025]: Invalid user rds from 104.131.254.205
port 51031
Jan  1 04:08:04 ip-172-31-38-110 sshd[6027]: Invalid user deployer from
201.134.231.33 port 43006
Jan  1 04:09:01 ip-172-31-38-110 sshd[6029]: Invalid user cooper from 14.161.36.71
port 44512
```

```
Jan  1 04:29:58 ip-172-31-38-110 sshd[6122]: Invalid user sebastian from
83.222.220.58 port 33891
Jan  1 04:34:06 ip-172-31-38-110 sshd[6126]: Invalid user admin from 190.82.73.92
port 53702
Jan  1 04:34:17 ip-172-31-38-110 sshd[6128]: Invalid user ftp from 51.38.112.218
port 48450
Jan  1 04:35:58 ip-172-31-38-110 sshd[6131]: Invalid user unreal from
187.167.73.69 port 55688
Jan  1 04:37:16 ip-172-31-38-110 sshd[6133]: Invalid user oracle from
159.89.180.93 port 32866
Jan  1 04:42:12 ip-172-31-38-110 sshd[6213]: Invalid user monsegur from
91.121.174.88 port 34174
Jan  1 04:54:37 ip-172-31-38-110 sshd[6227]: Invalid user brett from 101.236.5.253
port 60181
Jan  1 04:55:34 ip-172-31-38-110 sshd[6229]: Invalid user sa from 178.128.98.90
port 43531
Jan  1 05:10:36 ip-172-31-38-110 sshd[6319]: Invalid user tunnel from
96.114.71.146 port 50892
Jan  1 05:10:46 ip-172-31-38-110 sshd[6322]: Invalid user ashok from 217.40.104.61
port 61350
Jan  1 05:11:13 ip-172-31-38-110 sshd[6324]: Invalid user wii from 123.124.156.253
port 48860
Jan  1 05:13:21 ip-172-31-38-110 sshd[6326]: Invalid user deluge from
37.187.181.182 port 33058
Jan  1 05:15:51 ip-172-31-38-110 sshd[6329]: Invalid user butter from
202.28.33.166 port 57998
Jan  1 05:16:40 ip-172-31-38-110 sshd[6331]: Invalid user wagner from
140.143.100.89 port 54042
Jan  1 05:17:30 ip-172-31-38-110 sshd[6336]: Invalid user rajesh from
183.238.229.250 port 17665
Jan  1 05:17:47 ip-172-31-38-110 sshd[6338]: Invalid user csgoserver from
82.200.65.218 port 55756
Jan  1 05:21:34 ip-172-31-38-110 sshd[6378]: Invalid user ns2 from 118.163.107.56
port 34378
Jan  1 05:23:48 ip-172-31-38-110 sshd[6382]: Invalid user operator from
37.252.185.53 port 33906
Jan  1 05:28:57 ip-172-31-38-110 sshd[6394]: Invalid user transfer from
81.174.39.219 port 44367
Jan  1 05:30:32 ip-172-31-38-110 sshd[6398]: Invalid user test from 37.59.119.237
port 33834
Jan  1 05:32:15 ip-172-31-38-110 sshd[6401]: Invalid user cactiuser from
140.143.230.156 port 44362
Jan  1 05:37:44 ip-172-31-38-110 sshd[6409]: Invalid user deploy from 41.214.20.60
port 44028
Jan  1 05:39:35 ip-172-31-38-110 sshd[6494]: Invalid user sentry from
181.115.248.51 port 52386
Jan  1 05:50:50 ip-172-31-38-110 sshd[6499]: Invalid user factorio from
159.65.111.89 port 54988
Jan  1 05:53:40 ip-172-31-38-110 sshd[6501]: Invalid user omega from 94.191.87.180
port 38684
Jan  1 06:19:54 ip-172-31-38-110 sshd[6595]: Invalid user zeus from 42.116.82.122
port 47588
Jan  1 06:22:30 ip-172-31-38-110 sshd[6600]: Invalid user multimedia from
37.187.195.209 port 41987
```

```
Jan  1 06:25:36 ip-172-31-38-110 sshd[6775]: Invalid user sai from 160.124.155.165
port 49389
Jan  1 06:27:27 ip-172-31-38-110 sshd[6778]: Invalid user redmine from
51.38.239.50 port 56794
Jan  1 06:28:45 ip-172-31-38-110 sshd[6781]: Invalid user jens from 181.112.228.90
port 10991
Jan  1 06:35:26 ip-172-31-38-110 sshd[6884]: Invalid user sujat from
210.129.184.15 port 60368
Jan  1 06:35:44 ip-172-31-38-110 sshd[6886]: Invalid user usuario from
103.51.48.212 port 56586
Jan  1 06:38:01 ip-172-31-38-110 sshd[6888]: Invalid user nadya from 170.79.120.4
port 45704
Jan  1 06:38:35 ip-172-31-38-110 sshd[6890]: Invalid user amaina from
111.246.94.154 port 15156
Jan  1 06:40:36 ip-172-31-38-110 sshd[6965]: Invalid user www from 89.151.134.78
port 59092
Jan  1 06:44:35 ip-172-31-38-110 sshd[6967]: Invalid user sybase from
46.243.253.57 port 45556
Jan  1 06:59:59 ip-172-31-38-110 sshd[6979]: Invalid user dialer from
196.196.192.49 port 60674
Jan  1 07:00:58 ip-172-31-38-110 sshd[6981]: Invalid user dialer from
193.252.59.41 port 57632
Jan  1 07:01:41 ip-172-31-38-110 sshd[6983]: Invalid user aloko from 121.8.210.59
port 10429
Jan  1 07:04:03 ip-172-31-38-110 sshd[6985]: Invalid user matt from 106.13.46.243
port 37086
Jan  1 07:04:17 ip-172-31-38-110 sshd[6987]: Invalid user admin from 5.101.40.81
port 55015
Jan  1 07:17:25 ip-172-31-38-110 sshd[7066]: Invalid user kevin from 203.67.127.83
port 45085
Jan  1 07:27:21 ip-172-31-38-110 sshd[7072]: Invalid user tc from 210.73.195.244
port 40422
Jan  1 07:28:23 ip-172-31-38-110 sshd[7075]: Invalid user nginx from 60.29.254.252
port 30588
Jan  1 07:30:35 ip-172-31-38-110 sshd[7078]: Invalid user box from 118.24.33.65
port 46556
Jan  1 07:37:06 ip-172-31-38-110 sshd[7081]: Invalid user william from
89.36.221.229 port 57879
Jan  1 07:54:26 ip-172-31-38-110 sshd[7160]: Invalid user openstack from
124.248.237.142 port 36242
Jan  1 07:58:10 ip-172-31-38-110 sshd[7163]: Invalid user wp-user from
93.88.196.34 port 46902
Jan  1 07:58:27 ip-172-31-38-110 sshd[7165]: Invalid user wp-user from
177.103.179.92 port 36696
Jan  1 08:00:25 ip-172-31-38-110 sshd[7171]: Invalid user postgres from
200.35.109.138 port 34944
Jan  1 08:03:02 ip-172-31-38-110 sshd[7173]: Invalid user artifactory from
45.119.82.174 port 47430
Jan  1 08:03:40 ip-172-31-38-110 sshd[7176]: Invalid user pc from 41.203.216.86
port 55908
Jan  1 08:22:42 ip-172-31-38-110 sshd[7261]: Invalid user nagios from
159.65.235.37 port 55098
Jan  1 08:31:56 ip-172-31-38-110 sshd[7272]: Invalid user admon from
49.206.196.254 port 43204
```

```
Jan  1 08:38:36 ip-172-31-38-110 sshd[7294]: Invalid user deployer from
51.68.44.126 port 48902
Jan  1 08:45:54 ip-172-31-38-110 sshd[7375]: Invalid user student from
89.219.21.252 port 43740
Jan  1 08:48:53 ip-172-31-38-110 sshd[7377]: Invalid user koen from 186.15.24.34
port 35594
Jan  1 08:49:18 ip-172-31-38-110 sshd[7379]: Invalid user melanie from
106.51.73.204 port 15478
Jan  1 08:57:44 ip-172-31-38-110 sshd[7383]: Invalid user testuser from
103.28.23.57 port 37542
Jan  1 08:58:03 ip-172-31-38-110 sshd[7385]: Invalid user jenkins from
188.166.213.254 port 35368
Jan  1 09:17:56 ip-172-31-38-110 sshd[7469]: Invalid user tracie from
180.76.175.102 port 54528
Jan  1 09:26:00 ip-172-31-38-110 sshd[7475]: Invalid user worker from 41.196.0.189
port 46242
Jan  1 09:27:10 ip-172-31-38-110 sshd[7479]: Invalid user ts from 210.212.215.165
port 50324
Jan  1 09:31:27 ip-172-31-38-110 sshd[7484]: Invalid user monitor from
217.61.107.185 port 38628
Jan  1 09:32:30 ip-172-31-38-110 sshd[7487]: Invalid user iv from 201.145.163.178
port 34044
Jan  1 09:37:51 ip-172-31-38-110 sshd[7490]: Invalid user technical from
138.197.5.191 port 57280
Jan  1 09:41:20 ip-172-31-38-110 sshd[7570]: Invalid user chen from 180.250.115.93
port 44228
Jan  1 09:45:17 ip-172-31-38-110 sshd[7573]: Invalid user buildbot from
167.99.66.83 port 57096
Jan  1 09:48:18 ip-172-31-38-110 sshd[7576]: Invalid user last from
192.144.156.133 port 58744
Jan  1 09:50:00 ip-172-31-38-110 sshd[7578]: Invalid user compta from 36.81.58.5
port 43758
Jan  1 09:50:25 ip-172-31-38-110 sshd[7581]: Invalid user last from 78.8.9.196
port 40052
Jan  1 10:12:16 ip-172-31-38-110 sshd[7663]: Invalid user editor from 94.25.38.70
port 35576
Jan  1 10:21:46 ip-172-31-38-110 sshd[7671]: Invalid user vbox from 185.96.53.111
port 43446
Jan  1 10:25:04 ip-172-31-38-110 sshd[7673]: Invalid user sammy from 194.42.75.228
port 46886
Jan  1 10:26:32 ip-172-31-38-110 sshd[7675]: Invalid user pankaj from
178.128.119.190 port 34210
Jan  1 10:27:14 ip-172-31-38-110 sshd[7678]: Invalid user fff from 89.133.108.28
port 41384
Jan  1 11:05:39 ip-172-31-38-110 sshd[7776]: Invalid user eddy from 89.36.220.145
port 47122
Jan  1 11:05:47 ip-172-31-38-110 sshd[7778]: Invalid user counterstrike from
40.70.12.248 port 55972
Jan  1 11:27:38 ip-172-31-38-110 sshd[7875]: Invalid user training from
191.54.175.66 port 50292
Jan  1 11:54:49 ip-172-31-38-110 sshd[7959]: Invalid user pyimagesearch from
106.12.14.189 port 33220
Jan  1 12:11:39 ip-172-31-38-110 sshd[8044]: Invalid user ron from 189.254.33.157
port 34091
```

```
Jan  1 12:16:13 ip-172-31-38-110 sshd[8049]: Invalid user sensu from 82.64.8.34
port 47938
Jan  1 12:16:58 ip-172-31-38-110 sshd[8051]: Invalid user sensu from
52.213.179.131 port 46238
Jan  1 12:17:17 ip-172-31-38-110 sshd[8056]: Invalid user sandeep from
131.100.219.3 port 49928
Jan  1 12:20:21 ip-172-31-38-110 sshd[8062]: Invalid user oracle from
177.103.179.92 port 47700
Jan  1 12:28:52 ip-172-31-38-110 sshd[8085]: Invalid user java from 51.38.54.87
port 52174
Jan  1 12:29:19 ip-172-31-38-110 sshd[8088]: Invalid user tim from 180.243.220.254
port 51301
Jan  1 12:29:35 ip-172-31-38-110 sshd[8090]: Invalid user test from 202.131.152.2
port 60835
Jan  1 12:29:45 ip-172-31-38-110 sshd[8092]: Invalid user java from 46.101.192.45
port 58426
Jan  1 12:30:50 ip-172-31-38-110 sshd[8094]: Invalid user administrator from
190.64.68.178 port 43041
Jan  1 12:33:32 ip-172-31-38-110 sshd[8097]: Invalid user desadm from 73.129.11.75
port 42304
Jan  1 12:34:14 ip-172-31-38-110 sshd[8099]: Invalid user sameer from
118.193.191.18 port 40090
Jan  1 12:34:51 ip-172-31-38-110 sshd[8101]: Invalid user desadm from
139.199.207.31 port 38216
Jan  1 12:40:16 ip-172-31-38-110 sshd[8182]: Invalid user bouncer from
80.15.161.135 port 38777
Jan  1 12:41:25 ip-172-31-38-110 sshd[8184]: Invalid user ftpusr from
181.188.208.46 port 35952
Jan  1 12:43:41 ip-172-31-38-110 sshd[8186]: Invalid user willy from
164.132.225.151 port 38245
Jan  1 12:48:14 ip-172-31-38-110 sshd[8189]: Invalid user pi from 121.238.15.190
port 45838
Jan  1 12:48:14 ip-172-31-38-110 sshd[8191]: Invalid user pi from 121.238.15.190
port 45840
Jan  1 12:54:06 ip-172-31-38-110 sshd[8194]: Invalid user minecraft from
161.132.195.76 port 33573
Jan  1 12:54:10 ip-172-31-38-110 sshd[8196]: Invalid user odoo from 197.156.88.195
port 42142
Jan  1 12:56:16 ip-172-31-38-110 sshd[8201]: Invalid user jesus from 107.0.156.82
port 45986
Jan  1 12:56:38 ip-172-31-38-110 sshd[8203]: Invalid user dicky from
201.16.247.150 port 41726
Jan  1 13:01:00 ip-172-31-38-110 sshd[8207]: Invalid user zeus from 125.75.47.97
port 53463
Jan  1 13:02:06 ip-172-31-38-110 sshd[8209]: Invalid user test from 114.34.53.178
port 33910
Jan  1 13:05:21 ip-172-31-38-110 sshd[8215]: Invalid user aaron from
117.48.224.130 port 57281
Jan  1 13:21:07 ip-172-31-38-110 sshd[8302]: Invalid user apidoc from
119.254.209.115 port 47918
Jan  1 13:21:13 ip-172-31-38-110 sshd[8304]: Invalid user jboss from
193.112.68.149 port 55808
Jan  1 13:35:57 ip-172-31-38-110 sshd[8312]: Invalid user pascal from
185.189.115.37 port 43736
```

```
Jan  1 13:36:57 ip-172-31-38-110 sshd[8314]: Invalid user pg from 51.254.108.67
port 45024
Jan  1 13:39:45 ip-172-31-38-110 sshd[8393]: Invalid user sqoop from
140.143.134.86 port 42286
Jan  1 13:40:29 ip-172-31-38-110 sshd[8395]: Invalid user staffc from
186.42.165.11 port 52620
Jan  1 13:46:05 ip-172-31-38-110 sshd[8398]: Invalid user malcom from
176.182.189.29 port 37156
Jan  1 14:13:44 ip-172-31-38-110 sshd[8486]: Invalid user element from
103.57.210.21 port 33172
Jan  1 14:18:07 ip-172-31-38-110 sshd[8530]: Invalid user avahi-autoipd from
94.76.179.235 port 49968
Jan  1 14:19:48 ip-172-31-38-110 sshd[8535]: Invalid user ftpproc from 210.59.78.1
port 53757
Jan  1 14:28:19 ip-172-31-38-110 sshd[8541]: Invalid user yarn from 209.49.237.35
port 58759
Jan  1 14:28:48 ip-172-31-38-110 sshd[8545]: Invalid user ts3server from
217.128.2.139 port 44782
Jan  1 14:29:34 ip-172-31-38-110 sshd[8548]: Invalid user desop from
211.23.139.122 port 36748
Jan  1 14:33:08 ip-172-31-38-110 sshd[8557]: Invalid user git from 83.144.92.94
port 57042
Jan  1 14:33:46 ip-172-31-38-110 sshd[8560]: Invalid user super from
68.183.233.146 port 35078
Jan  1 14:42:35 ip-172-31-38-110 sshd[8647]: Invalid user creadur from
64.34.202.161 port 45342
Jan  1 14:43:26 ip-172-31-38-110 sshd[8649]: Invalid user ts3bot from
212.85.79.102 port 34292
Jan  1 14:43:59 ip-172-31-38-110 sshd[8653]: Invalid user ts3bot from
89.90.209.252 port 41652
Jan  1 14:44:12 ip-172-31-38-110 sshd[8655]: Invalid user server from 51.77.151.46
port 40537
Jan  1 14:45:14 ip-172-31-38-110 sshd[8657]: Invalid user skaner from
181.49.150.45 port 42546
Jan  1 14:45:23 ip-172-31-38-110 sshd[8659]: Invalid user configure from
139.199.228.133 port 53639
Jan  1 14:46:24 ip-172-31-38-110 sshd[8661]: Invalid user dicky from 113.176.195.4
port 50770
Jan  1 14:47:17 ip-172-31-38-110 sshd[8663]: Invalid user ts3bot from 42.159.8.20
port 22976
Jan  1 14:51:42 ip-172-31-38-110 sshd[8668]: Invalid user pamela from
202.69.73.114 port 37480
Jan  1 14:56:33 ip-172-31-38-110 sshd[8672]: Invalid user tanja from 185.139.21.20
port 36122
Jan  1 14:58:15 ip-172-31-38-110 sshd[8674]: Invalid user field from
213.167.35.214 port 40916
Jan  1 15:01:25 ip-172-31-38-110 sshd[8679]: Invalid user tomcat from 190.82.73.92
port 42238
Jan  1 15:06:09 ip-172-31-38-110 sshd[8690]: Invalid user apache from 54.37.210.25
port 44668
Jan  1 15:07:04 ip-172-31-38-110 sshd[8702]: Invalid user apache from
93.104.208.151 port 50244
Jan  1 15:07:06 ip-172-31-38-110 sshd[8704]: Invalid user apache from
85.214.154.197 port 47718
```

```
Jan  1 15:08:22 ip-172-31-38-110 sshd[8720]: Invalid user old from 101.89.114.213
port 39896
Jan  1 15:08:29 ip-172-31-38-110 sshd[8724]: Invalid user wo from 114.80.87.245
port 45666
Jan  1 15:10:28 ip-172-31-38-110 sshd[8822]: Invalid user mcadmin from
27.128.169.31 port 18946
Jan  1 15:10:42 ip-172-31-38-110 sshd[8824]: Invalid user oracle from
109.197.85.35 port 54178
Jan  1 15:10:52 ip-172-31-38-110 sshd[8827]: Invalid user oracle from
109.197.85.35 port 55560
Jan  1 15:11:05 ip-172-31-38-110 sshd[8829]: Invalid user oracle from
109.197.85.35 port 56794
Jan  1 15:11:30 ip-172-31-38-110 sshd[8833]: Invalid user darvin from
109.197.85.35 port 60044
Jan  1 15:11:40 ip-172-31-38-110 sshd[8835]: Invalid user daniel from
109.197.85.35 port 33184
Jan  1 15:11:51 ip-172-31-38-110 sshd[8837]: Invalid user john from 109.197.85.35
port 34302
Jan  1 15:12:02 ip-172-31-38-110 sshd[8839]: Invalid user john from 109.197.85.35
port 35428
Jan  1 15:12:12 ip-172-31-38-110 sshd[8841]: Invalid user jon from 109.197.85.35
port 36670
Jan  1 15:12:23 ip-172-31-38-110 sshd[8843]: Invalid user jon from 109.197.85.35
port 37812
Jan  1 15:12:34 ip-172-31-38-110 sshd[8845]: Invalid user test from 109.197.85.35
port 39016
Jan  1 15:12:45 ip-172-31-38-110 sshd[8847]: Invalid user test from 109.197.85.35
port 40210
Jan  1 15:12:55 ip-172-31-38-110 sshd[8849]: Invalid user test1 from 109.197.85.35
port 41502
Jan  1 15:13:05 ip-172-31-38-110 sshd[8851]: Invalid user test from 109.197.85.35
port 42796
Jan  1 15:13:15 ip-172-31-38-110 sshd[8853]: Invalid user testuser from
109.197.85.35 port 44222
Jan  1 15:13:26 ip-172-31-38-110 sshd[8855]: Invalid user tmp from 109.197.85.35
port 45610
Jan  1 15:13:36 ip-172-31-38-110 sshd[8857]: Invalid user git from 109.197.85.35
port 47234
Jan  1 15:13:48 ip-172-31-38-110 sshd[8859]: Invalid user git from 109.197.85.35
port 48654
Jan  1 15:14:00 ip-172-31-38-110 sshd[8861]: Invalid user git from 109.197.85.35
port 50522
Jan  1 15:14:11 ip-172-31-38-110 sshd[8863]: Invalid user postgres from
109.197.85.35 port 52392
Jan  1 15:14:22 ip-172-31-38-110 sshd[8865]: Invalid user postgres from
109.197.85.35 port 53956
Jan  1 15:14:34 ip-172-31-38-110 sshd[8867]: Invalid user postgres from
109.197.85.35 port 55596
Jan  1 15:14:45 ip-172-31-38-110 sshd[8869]: Invalid user postgres from
109.197.85.35 port 57224
Jan  1 15:14:58 ip-172-31-38-110 sshd[8871]: Invalid user postgres from
109.197.85.35 port 58844
Jan  1 15:15:08 ip-172-31-38-110 sshd[8873]: Invalid user prueba from
109.197.85.35 port 60574
```

```
Jan  1 15:15:21 ip-172-31-38-110 sshd[8875]: Invalid user user from 109.197.85.35
port 33704
Jan  1 15:15:33 ip-172-31-38-110 sshd[8877]: Invalid user user1 from 109.197.85.35
port 35630
Jan  1 15:16:29 ip-172-31-38-110 sshd[8888]: Invalid user cyrus from 109.197.85.35
port 43548
Jan  1 15:16:40 ip-172-31-38-110 sshd[8890]: Invalid user zabbix from
109.197.85.35 port 45062
Jan  1 15:16:52 ip-172-31-38-110 sshd[8892]: Invalid user deploy from
109.197.85.35 port 46590
Jan  1 15:17:04 ip-172-31-38-110 sshd[8894]: Invalid user deploy from
109.197.85.35 port 48198
Jan  1 15:17:15 ip-172-31-38-110 sshd[8899]: Invalid user nagios from
109.197.85.35 port 49844
Jan  1 15:17:25 ip-172-31-38-110 sshd[8901]: Invalid user nagios from
109.197.85.35 port 51358
Jan  1 15:17:34 ip-172-31-38-110 sshd[8905]: Invalid user koen from 120.92.137.144
port 10421
Jan  1 15:17:37 ip-172-31-38-110 sshd[8903]: Invalid user media from 109.197.85.35
port 52784
Jan  1 15:17:48 ip-172-31-38-110 sshd[8907]: Invalid user maria from 109.197.85.35
port 54400
Jan  1 15:17:59 ip-172-31-38-110 sshd[8909]: Invalid user michael from
109.197.85.35 port 55874
Jan  1 15:18:11 ip-172-31-38-110 sshd[8911]: Invalid user jboss from 109.197.85.35
port 57250
Jan  1 15:18:22 ip-172-31-38-110 sshd[8913]: Invalid user vincent from
109.197.85.35 port 58870
Jan  1 15:18:32 ip-172-31-38-110 sshd[8915]: Invalid user hadoop from
109.197.85.35 port 60228
Jan  1 15:18:42 ip-172-31-38-110 sshd[8917]: Invalid user hadoop from
109.197.85.35 port 33270
Jan  1 15:18:54 ip-172-31-38-110 sshd[8919]: Invalid user system from
109.197.85.35 port 34656
Jan  1 15:19:05 ip-172-31-38-110 sshd[8921]: Invalid user school from
109.197.85.35 port 36202
Jan  1 15:35:47 ip-172-31-38-110 sshd[8931]: Invalid user saeed from 130.212.72.39
port 55086
Jan  1 15:48:23 ip-172-31-38-110 sshd[9010]: Invalid user xxx from 209.97.140.142
port 35946
Jan  1 16:04:13 ip-172-31-38-110 sshd[9018]: Invalid user ts3 from 178.128.98.90
port 33744
Jan  1 16:09:32 ip-172-31-38-110 sshd[9097]: Invalid user mcftp from
149.56.166.241 port 46168
Jan  1 16:09:33 ip-172-31-38-110 sshd[9095]: Invalid user admin from
171.255.242.147 port 37054
Jan  1 16:15:45 ip-172-31-38-110 sshd[9102]: Invalid user vn from 202.86.167.74
port 53830
Jan  1 16:17:13 ip-172-31-38-110 sshd[9109]: Invalid user vn from 81.137.199.19
port 38913
Jan  1 16:18:58 ip-172-31-38-110 sshd[9111]: Invalid user samuel from 58.20.30.55
port 31284
Jan  1 16:24:52 ip-172-31-38-110 sshd[9114]: Invalid user bx from 103.5.112.128
port 40832
```

```
Jan  1 16:26:19 ip-172-31-38-110 sshd[9117]: Invalid user cvsuser from
54.36.189.240 port 59476
Jan  1 16:48:14 ip-172-31-38-110 sshd[9198]: Invalid user minecraft from
73.108.52.30 port 50622
Jan  1 17:02:27 ip-172-31-38-110 sshd[9206]: Invalid user stack from
164.132.51.216 port 57490
Jan  1 17:06:44 ip-172-31-38-110 sshd[9209]: Invalid user admin from 51.255.35.58
port 59758
Jan  1 17:22:00 ip-172-31-38-110 sshd[9366]: Invalid user sam from 142.44.188.51
port 40631
Jan  1 17:22:09 ip-172-31-38-110 sshd[9368]: Invalid user usuario from
175.175.151.36 port 42934
Jan  1 17:41:25 ip-172-31-38-110 sshd[9456]: Invalid user aogola from 118.192.9.10
port 59355
Jan  1 17:46:57 ip-172-31-38-110 sshd[9459]: Invalid user anderson from
91.229.106.49 port 45234
Jan  1 17:56:12 ip-172-31-38-110 sshd[9467]: Invalid user git from 47.205.245.164
port 49090
Jan  1 17:57:08 ip-172-31-38-110 sshd[9469]: Invalid user admin from
112.238.124.121 port 42521
Jan  1 17:59:29 ip-172-31-38-110 sshd[9472]: Invalid user ftpuser from
118.25.45.24 port 36712
Jan  1 18:01:51 ip-172-31-38-110 sshd[9475]: Invalid user frappe from
161.10.238.114 port 57257
Jan  1 18:04:29 ip-172-31-38-110 sshd[9477]: Invalid user test from 5.39.89.70
port 36636
Jan  1 18:09:42 ip-172-31-38-110 sshd[9555]: Invalid user tester from
124.43.13.199 port 11489
Jan  1 18:10:03 ip-172-31-38-110 sshd[9557]: Invalid user zimbra from
200.69.250.253 port 39962
Jan  1 18:15:07 ip-172-31-38-110 sshd[9562]: Invalid user centos from 81.2.249.224
port 33844
Jan  1 18:18:36 ip-172-31-38-110 sshd[9567]: Invalid user admin from 131.72.141.34
port 60094
Jan  1 18:21:27 ip-172-31-38-110 sshd[9571]: Invalid user master from 58.87.120.53
port 35242
Jan  1 18:53:02 ip-172-31-38-110 sshd[9659]: Invalid user deploy from
109.115.54.245 port 51939
Jan  1 18:56:42 ip-172-31-38-110 sshd[9664]: Invalid user deploy2 from
124.194.44.219 port 51964
Jan  1 19:13:51 ip-172-31-38-110 sshd[9746]: Invalid user fletcher from
209.97.143.239 port 40644
Jan  1 19:18:03 ip-172-31-38-110 sshd[9751]: Invalid user testbed from
110.18.61.66 port 46029
Jan  1 19:19:03 ip-172-31-38-110 sshd[9754]: Invalid user testbed from
221.131.28.146 port 47482
Jan  1 19:19:07 ip-172-31-38-110 sshd[9756]: Invalid user admin from
201.238.215.168 port 55412
Jan  1 20:08:42 ip-172-31-38-110 sshd[9858]: Invalid user kai from 118.25.190.181
port 33168
Jan  1 20:14:28 ip-172-31-38-110 sshd[9938]: Invalid user testuser from
139.199.101.72 port 51452
Jan  1 20:34:20 ip-172-31-38-110 sshd[9950]: Invalid user admin from 5.101.40.37
port 39026
```

```
Jan  1 20:34:21 ip-172-31-38-110 sshd[9952]: Invalid user ubnt from 5.101.40.37
port 35396
Jan  1 20:34:21 ip-172-31-38-110 sshd[9956]: Invalid user admin from 5.101.40.38
port 56593
Jan  1 20:35:35 ip-172-31-38-110 sshd[9958]: Invalid user kernoops from
206.248.229.4 port 37312
Jan  1 20:40:16 ip-172-31-38-110 sshd[10061]: Invalid user suse from
209.97.140.142 port 45028
Jan  1 20:43:26 ip-172-31-38-110 sshd[10063]: Invalid user kiwi from 78.36.7.170
port 59642
Jan  1 20:47:42 ip-172-31-38-110 sshd[10066]: Invalid user user from 51.75.122.16
port 48626
Jan  1 20:52:54 ip-172-31-38-110 sshd[10069]: Invalid user macintosh from
190.144.161.11 port 53916
Jan  1 20:58:11 ip-172-31-38-110 sshd[10073]: Invalid user student from
220.133.198.188 port 32838
Jan  1 20:58:39 ip-172-31-38-110 sshd[10075]: Invalid user debian from
178.32.141.39 port 57358
Jan  1 20:59:44 ip-172-31-38-110 sshd[10078]: Invalid user changem from
193.112.7.36 port 54684
Jan  1 21:00:01 ip-172-31-38-110 sshd[10080]: Invalid user changem from
190.153.249.99 port 39592
Jan  1 21:04:55 ip-172-31-38-110 sshd[10093]: Invalid user software from
195.208.30.140 port 52536
Jan  1 21:15:06 ip-172-31-38-110 sshd[10190]: Invalid user charles from
183.195.134.90 port 40137
Jan  1 21:16:54 ip-172-31-38-110 sshd[10194]: Invalid user web3 from 5.135.152.97
port 38182
Jan  1 21:20:09 ip-172-31-38-110 sshd[10202]: Invalid user both from
211.159.242.143 port 57174
Jan  1 21:21:42 ip-172-31-38-110 sshd[10210]: Invalid user system from
122.160.137.37 port 51702
Jan  1 21:22:43 ip-172-31-38-110 sshd[10218]: Invalid user alfred from
190.82.73.92 port 58182
Jan  1 21:26:08 ip-172-31-38-110 sshd[10223]: Invalid user internal from
120.92.137.144 port 4923
Jan  1 21:32:23 ip-172-31-38-110 sshd[10245]: Invalid user arasaac from
118.182.118.248 port 46052
Jan  1 21:35:31 ip-172-31-38-110 sshd[10250]: Invalid user demo3 from
103.235.228.131 port 59879
Jan  1 21:38:02 ip-172-31-38-110 sshd[10259]: Invalid user demo3 from
122.152.210.200 port 35240
Jan  1 21:52:14 ip-172-31-38-110 sshd[10385]: Invalid user rdp from 103.82.101.44
port 46913
Jan  1 22:09:02 ip-172-31-38-110 sshd[10417]: Invalid user provider from
152.32.140.158 port 53792
Jan  1 22:09:13 ip-172-31-38-110 sshd[10495]: Invalid user admin from
182.162.96.185 port 36026
Jan  1 22:09:38 ip-172-31-38-110 sshd[10497]: Invalid user xxx from 201.47.91.199
port 16295
Jan  1 22:34:04 ip-172-31-38-110 sshd[10597]: Invalid user I2b2workdata2 from
47.22.135.70 port 62756
Jan  1 22:36:27 ip-172-31-38-110 sshd[10599]: Invalid user www-upload from
51.38.176.147 port 58807
```

```
Jan  1 22:36:42 ip-172-31-38-110 sshd[10601]: Invalid user sftp from
138.197.202.144 port 57870
Jan  1 22:37:16 ip-172-31-38-110 sshd[10603]: Invalid user cron from 111.230.34.82
port 33008
Jan  1 22:46:25 ip-172-31-38-110 sshd[10683]: Invalid user biz from 87.98.182.87
port 41961
Jan  1 22:47:39 ip-172-31-38-110 sshd[10686]: Invalid user javier from
186.120.93.42 port 51248
Jan  1 22:47:41 ip-172-31-38-110 sshd[10688]: Invalid user debbie from
222.252.30.117 port 60754
Jan  1 22:47:58 ip-172-31-38-110 sshd[10690]: Invalid user xys from 59.167.123.249
port 51836
Jan  1 22:50:11 ip-172-31-38-110 sshd[10692]: Invalid user teamspeak3 from
176.31.252.148 port 39889
Jan  1 22:51:41 ip-172-31-38-110 sshd[10695]: Invalid user jonah from
104.131.90.193 port 59365
Jan  1 22:58:12 ip-172-31-38-110 sshd[10700]: Invalid user test from 106.12.127.25
port 58328
Jan  1 23:00:26 ip-172-31-38-110 sshd[10705]: Invalid user czarek from
89.90.209.252 port 59590
Jan  1 23:01:39 ip-172-31-38-110 sshd[10708]: Invalid user sales from
149.202.214.11 port 49442
Jan  1 23:01:52 ip-172-31-38-110 sshd[10710]: Invalid user stream from
101.231.101.140 port 58207
Jan  1 23:01:54 ip-172-31-38-110 sshd[10712]: Invalid user stream from
220.134.8.244 port 36176
Jan  1 23:02:28 ip-172-31-38-110 sshd[10714]: Invalid user chad from 31.172.80.88
port 48830
Jan  1 23:02:40 ip-172-31-38-110 sshd[10716]: Invalid user sales from
185.251.32.170 port 52638
Jan  1 23:19:10 ip-172-31-38-110 sshd[10809]: Invalid user neutron from
178.22.122.234 port 47926
Jan  1 23:22:11 ip-172-31-38-110 sshd[10814]: Invalid user bwadmin from
190.149.238.2 port 42351
Jan  1 23:22:34 ip-172-31-38-110 sshd[10818]: Invalid user jeus from
14.116.254.127 port 37532
Jan  1 23:23:14 ip-172-31-38-110 sshd[10822]: Invalid user jesse from
91.121.101.159 port 57602
Jan  1 23:23:15 ip-172-31-38-110 sshd[10820]: Invalid user ecqusers from
181.123.9.130 port 33116
Jan  1 23:23:22 ip-172-31-38-110 sshd[10824]: Invalid user jeus from 49.255.44.154
port 54164
Jan  1 23:25:08 ip-172-31-38-110 sshd[10828]: Invalid user demo from
223.223.186.114 port 60327
Jan  1 23:28:35 ip-172-31-38-110 sshd[10832]: Invalid user testuser from
51.75.26.106 port 33066
Jan  1 23:34:18 ip-172-31-38-110 sshd[10838]: Invalid user saphir from
75.139.51.215 port 49574
Jan  1 23:46:52 ip-172-31-38-110 sshd[10916]: Invalid user logan from 51.38.128.30
port 35332
Jan  1 23:48:49 ip-172-31-38-110 sshd[10918]: Invalid user internet from
62.24.102.106 port 11395
Jan  1 23:59:21 ip-172-31-38-110 sshd[10925]: Invalid user fcoperador from
67.41.195.160 port 38436
```

```
Jan  2 00:00:03 ip-172-31-38-110 sshd[10930]: Invalid user admin from 95.85.23.154
port 53222
Jan  2 00:00:13 ip-172-31-38-110 sshd[10932]: Invalid user admin from 80.211.7.198
port 47434
Jan  2 00:00:25 ip-172-31-38-110 sshd[10934]: Invalid user team from 173.210.1.162
port 46425
Jan  2 00:00:31 ip-172-31-38-110 sshd[10936]: Invalid user saned from 96.56.82.194
port 53958
Jan  2 00:00:33 ip-172-31-38-110 sshd[10938]: Invalid user fletcher from
167.99.43.65 port 34993
Jan  2 00:01:02 ip-172-31-38-110 sshd[10942]: Invalid user vps from 68.183.233.146
port 34397
Jan  2 00:01:04 ip-172-31-38-110 sshd[10944]: Invalid user vps from 197.50.49.37
port 41718
Jan  2 00:01:29 ip-172-31-38-110 sshd[10946]: Invalid user team from 202.83.56.48
port 10019
Jan  2 00:01:42 ip-172-31-38-110 sshd[10948]: Invalid user vps from 103.24.118.28
port 42696
Jan  2 00:02:03 ip-172-31-38-110 sshd[10952]: Invalid user saned from
188.165.34.30 port 56662
Jan  2 00:02:14 ip-172-31-38-110 sshd[10954]: Invalid user tomcat from
116.212.237.226 port 32935
Jan  2 00:02:42 ip-172-31-38-110 sshd[10956]: Invalid user student from
195.239.204.94 port 50470
Jan  2 00:02:58 ip-172-31-38-110 sshd[10958]: Invalid user kumar from
31.179.137.38 port 60612
Jan  2 00:04:42 ip-172-31-38-110 sshd[10961]: Invalid user sybase from
107.191.56.63 port 45451
Jan  2 00:12:39 ip-172-31-38-110 sshd[11045]: Invalid user admin from 80.88.90.108
port 49532
Jan  2 00:16:50 ip-172-31-38-110 sshd[11049]: Invalid user pub from 142.44.247.87
port 48588
Jan  2 00:18:05 ip-172-31-38-110 sshd[11055]: Invalid user oracle from
140.143.208.176 port 37948
Jan  2 00:18:42 ip-172-31-38-110 sshd[11057]: Invalid user tapestry from
51.15.221.51 port 53640
Jan  2 00:18:44 ip-172-31-38-110 sshd[11059]: Invalid user tapestry from
92.222.84.34 port 35014
Jan  2 00:19:58 ip-172-31-38-110 sshd[11063]: Invalid user admin from
129.211.104.114 port 36180
Jan  2 00:20:10 ip-172-31-38-110 sshd[11065]: Invalid user test from 139.255.83.52
port 35216
Jan  2 00:21:41 ip-172-31-38-110 sshd[11105]: Invalid user jira from 106.13.38.158
port 49240
Jan  2 00:21:48 ip-172-31-38-110 sshd[11107]: Invalid user tomcat from
68.183.52.89 port 36242
Jan  2 00:22:40 ip-172-31-38-110 sshd[11111]: Invalid user default from
107.175.24.212 port 43806
Jan  2 00:22:58 ip-172-31-38-110 sshd[11113]: Invalid user default from
125.131.140.234 port 39998
Jan  2 00:24:27 ip-172-31-38-110 sshd[11118]: Invalid user ada from
140.143.137.188 port 51704
Jan  2 00:31:56 ip-172-31-38-110 sshd[11122]: Invalid user minecraftserver from
51.255.83.44 port 6802
```

```
Jan  2 00:48:14 ip-172-31-38-110 sshd[11209]: Invalid user bruno from
113.134.211.228 port 60061
Jan  2 00:53:46 ip-172-31-38-110 sshd[11212]: Invalid user teamspeak3 from
159.65.239.104 port 44036
Jan  2 00:54:15 ip-172-31-38-110 sshd[11214]: Invalid user teamspeak3 from
138.197.5.191 port 38132
Jan  2 00:55:36 ip-172-31-38-110 sshd[11218]: Invalid user factorio from
119.29.251.152 port 60302
Jan  2 01:03:02 ip-172-31-38-110 sshd[11228]: Invalid user testing from
84.254.0.120 port 38846
Jan  2 01:03:26 ip-172-31-38-110 sshd[11232]: Invalid user info from
51.145.137.251 port 41994
Jan  2 01:10:08 ip-172-31-38-110 sshd[11313]: Invalid user fdrusers from
178.128.53.145 port 48892
Jan  2 01:18:45 ip-172-31-38-110 sshd[11323]: Invalid user user from 54.38.240.250
port 46438
Jan  2 01:19:22 ip-172-31-38-110 sshd[11325]: Invalid user millers from
190.16.254.111 port 51186
Jan  2 01:19:59 ip-172-31-38-110 sshd[11328]: Invalid user demo from
121.201.110.60 port 52912
Jan  2 01:20:51 ip-172-31-38-110 sshd[11330]: Invalid user ejabberd from
128.71.106.51 port 39696
Jan  2 01:21:07 ip-172-31-38-110 sshd[11332]: Invalid user vyatta from
111.231.71.177 port 42916
Jan  2 01:21:46 ip-172-31-38-110 sshd[11336]: Invalid user radio from
114.67.88.116 port 57883
Jan  2 01:22:04 ip-172-31-38-110 sshd[11338]: Invalid user bobby from 51.75.142.40
port 43342
Jan  2 01:22:23 ip-172-31-38-110 sshd[11340]: Invalid user bobby from
91.229.106.49 port 35426
Jan  2 01:27:01 ip-172-31-38-110 sshd[11347]: Invalid user xavier from 81.86.212.0
port 47889
Jan  2 01:36:54 ip-172-31-38-110 sshd[11357]: Invalid user zachary from
190.55.238.31 port 52623
Jan  2 01:40:13 ip-172-31-38-110 sshd[11436]: Invalid user ftp from 200.90.11.218
port 11317
Jan  2 01:48:35 ip-172-31-38-110 sshd[11439]: Invalid user bx from 35.200.174.79
port 40212
Jan  2 01:53:56 ip-172-31-38-110 sshd[11442]: Invalid user git from 180.76.52.25
port 40208
Jan  2 01:56:05 ip-172-31-38-110 sshd[11444]: Invalid user amuiruri from
190.85.63.50 port 56570
Jan  2 01:56:19 ip-172-31-38-110 sshd[11446]: Invalid user user from 187.16.96.35
port 33146
Jan  2 01:56:20 ip-172-31-38-110 sshd[11447]: Invalid user jose from 111.230.34.82
port 49356
Jan  2 02:09:17 ip-172-31-38-110 sshd[11535]: Invalid user oracle from
190.128.137.10 port 27756
Jan  2 02:09:28 ip-172-31-38-110 sshd[11537]: Invalid user puppet from
148.70.55.214 port 37262
Jan  2 02:10:57 ip-172-31-38-110 sshd[11539]: Invalid user debian from
142.44.184.156 port 43472
Jan  2 02:11:39 ip-172-31-38-110 sshd[11541]: Invalid user alexander from
58.210.42.4 port 45898
```

```
Jan  2 02:12:16 ip-172-31-38-110 sshd[11543]: Invalid user oracle from
190.128.137.10 port 60998
Jan  2 02:12:17 ip-172-31-38-110 sshd[11545]: Invalid user puppet from
41.75.113.170 port 41332
Jan  2 02:12:27 ip-172-31-38-110 sshd[11547]: Invalid user oracle from
190.128.137.10 port 4888
Jan  2 02:16:01 ip-172-31-38-110 sshd[11552]: Invalid user admin1 from
149.56.10.119 port 44822
Jan  2 02:16:42 ip-172-31-38-110 sshd[11555]: Invalid user kiwi from
103.75.209.154 port 49414
Jan  2 02:18:36 ip-172-31-38-110 sshd[11562]: Invalid user kiwi from 201.245.1.107
port 33048
Jan  2 02:19:17 ip-172-31-38-110 sshd[11564]: Invalid user carter from
190.64.68.178 port 56449
Jan  2 02:21:49 ip-172-31-38-110 sshd[11567]: Invalid user zule from
140.143.246.199 port 52514
Jan  2 02:31:25 ip-172-31-38-110 sshd[11574]: Invalid user gadmin from
118.97.111.210 port 38464
Jan  2 02:31:50 ip-172-31-38-110 sshd[11576]: Invalid user downloader from
222.110.45.23 port 33092
Jan  2 02:45:06 ip-172-31-38-110 sshd[11654]: Invalid user dice from
167.99.162.138 port 40536
Jan  2 02:45:38 ip-172-31-38-110 sshd[11656]: Invalid user dice from 187.16.96.35
port 35622
Jan  2 02:45:41 ip-172-31-38-110 sshd[11658]: Invalid user wii from
186.103.179.158 port 36322
Jan  2 02:47:02 ip-172-31-38-110 sshd[11660]: Invalid user bouncer from
142.44.242.155 port 59967
Jan  2 02:49:05 ip-172-31-38-110 sshd[11662]: Invalid user bouncer from
218.10.228.90 port 45606
Jan  2 02:49:28 ip-172-31-38-110 sshd[11664]: Invalid user riley from
118.71.224.186 port 61457
Jan  2 02:56:18 ip-172-31-38-110 sshd[11672]: Invalid user or from 51.38.37.69
port 39273
Jan  2 02:56:48 ip-172-31-38-110 sshd[11675]: Invalid user myftp from
202.149.193.118 port 17417
Jan  2 02:57:29 ip-172-31-38-110 sshd[11677]: Invalid user bouncer from
71.246.234.139 port 52678
Jan  2 03:00:41 ip-172-31-38-110 sshd[11680]: Invalid user simone from
217.182.93.140 port 50468
Jan  2 03:01:12 ip-172-31-38-110 sshd[11682]: Invalid user angela from
170.79.120.4 port 51310
Jan  2 03:02:09 ip-172-31-38-110 sshd[11686]: Invalid user informix from
111.231.102.179 port 36764
Jan  2 03:13:04 ip-172-31-38-110 sshd[11777]: Invalid user qf from 189.45.13.3
port 42420
Jan  2 03:13:12 ip-172-31-38-110 sshd[11779]: Invalid user pub from 179.97.130.153
port 40883
Jan  2 03:15:45 ip-172-31-38-110 sshd[11789]: Invalid user copy from 83.94.206.4
port 59569
Jan  2 03:20:58 ip-172-31-38-110 sshd[11800]: Invalid user graham from
82.62.117.253 port 54840
Jan  2 03:32:44 ip-172-31-38-110 sshd[11805]: Invalid user student from
122.160.48.64 port 39540
```

```
Jan  2 03:32:51 ip-172-31-38-110 sshd[11807]: Invalid user wogan from
37.187.25.138 port 59876
Jan  2 03:33:17 ip-172-31-38-110 sshd[11809]: Invalid user test from 218.28.76.138
port 58812
Jan  2 03:33:23 ip-172-31-38-110 sshd[11811]: Invalid user wogan from 51.75.26.236
port 36260
Jan  2 03:33:28 ip-172-31-38-110 sshd[11813]: Invalid user mrtg from 80.211.14.153
port 47618
Jan  2 03:33:38 ip-172-31-38-110 sshd[11815]: Invalid user chloe from
52.38.158.201 port 50030
Jan  2 03:34:11 ip-172-31-38-110 sshd[11820]: Invalid user juanda from
117.218.78.97 port 39404
Jan  2 03:37:33 ip-172-31-38-110 sshd[11825]: Invalid user kubuntu from
217.182.93.140 port 43228
Jan  2 03:43:12 ip-172-31-38-110 sshd[11910]: Invalid user matthew from
106.75.146.213 port 52000
Jan  2 03:45:12 ip-172-31-38-110 sshd[11912]: Invalid user ftptest from
145.239.92.73 port 38032
Jan  2 03:48:00 ip-172-31-38-110 sshd[11915]: Invalid user sorin from
212.237.38.213 port 40908
Jan  2 03:51:09 ip-172-31-38-110 sshd[11920]: Invalid user tapas from
139.199.183.185 port 45572
Jan  2 03:52:49 ip-172-31-38-110 sshd[11924]: Invalid user thanks from
119.28.50.163 port 32782
Jan  2 04:01:39 ip-172-31-38-110 sshd[11935]: Invalid user qf from 46.182.109.140
port 6866
Jan  2 04:14:27 ip-172-31-38-110 sshd[12017]: Invalid user osboxes from
217.182.93.140 port 35971
Jan  2 04:20:09 ip-172-31-38-110 sshd[12024]: Invalid user operator from
182.61.13.138 port 40616
Jan  2 04:25:51 ip-172-31-38-110 sshd[12027]: Invalid user angus from
91.121.110.50 port 49884
Jan  2 04:25:57 ip-172-31-38-110 sshd[12029]: Invalid user angus from
74.208.43.208 port 55832
Jan  2 04:28:33 ip-172-31-38-110 sshd[12034]: Invalid user mac from 136.159.169.6
port 1303
Jan  2 04:31:00 ip-172-31-38-110 sshd[12038]: Invalid user olingo from
158.69.221.102 port 46661
Jan  2 04:32:43 ip-172-31-38-110 sshd[12040]: Invalid user angus from
80.20.125.243 port 53255
Jan  2 04:32:43 ip-172-31-38-110 sshd[12042]: Invalid user utente from
118.24.112.191 port 39014
Jan  2 04:40:07 ip-172-31-38-110 sshd[12124]: Invalid user hue from
140.143.208.176 port 35102
Jan  2 04:40:07 ip-172-31-38-110 sshd[12123]: Invalid user sam from 117.48.206.48
port 50346
Jan  2 04:42:00 ip-172-31-38-110 sshd[12127]: Invalid user sk from 103.27.238.202
port 34624
Jan  2 04:42:56 ip-172-31-38-110 sshd[12130]: Invalid user minecraft from
107.191.56.63 port 40588
Jan  2 04:47:26 ip-172-31-38-110 sshd[12132]: Invalid user sa from 41.82.254.90
port 50739
Jan  2 04:51:29 ip-172-31-38-110 sshd[12135]: Invalid user admin from
217.182.93.140 port 56949
```

```
Jan  2 04:56:36 ip-172-31-38-110 sshd[12138]: Invalid user ts3 from 112.64.34.171
port 39741
Jan  2 05:15:48 ip-172-31-38-110 sshd[12225]: Invalid user cos from 88.99.227.252
port 57992
Jan  2 05:17:54 ip-172-31-38-110 sshd[12231]: Invalid user inn from 158.132.80.111
port 44346
Jan  2 05:19:43 ip-172-31-38-110 sshd[12235]: Invalid user inn from 46.105.123.11
port 42157
Jan  2 05:28:29 ip-172-31-38-110 sshd[12242]: Invalid user xrdp from
217.182.93.140 port 49693
Jan  2 05:30:43 ip-172-31-38-110 sshd[12250]: Invalid user stef from
35.196.116.239 port 52374
Jan  2 05:31:17 ip-172-31-38-110 sshd[12255]: Invalid user steam from
185.6.172.152 port 46422
Jan  2 05:31:49 ip-172-31-38-110 sshd[12257]: Invalid user admin from 120.227.4.77
port 36319
Jan  2 05:33:34 ip-172-31-38-110 sshd[12259]: Invalid user puppet from
128.199.118.81 port 58814
Jan  2 05:33:41 ip-172-31-38-110 sshd[12261]: Invalid user services from
182.162.96.184 port 18286
Jan  2 05:38:53 ip-172-31-38-110 sshd[12266]: Invalid user reiner from
107.170.246.89 port 47192
Jan  2 05:39:53 ip-172-31-38-110 sshd[12344]: Invalid user test from 195.70.44.3
port 33193
Jan  2 05:41:01 ip-172-31-38-110 sshd[12346]: Invalid user hue from 183.136.239.37
port 42606
Jan  2 05:57:42 ip-172-31-38-110 sshd[12351]: Invalid user jack from 78.139.9.6
port 50058
Jan  2 06:00:22 ip-172-31-38-110 sshd[12355]: Invalid user bouncer from
202.71.176.113 port 43204
Jan  2 06:06:59 ip-172-31-38-110 sshd[12358]: Invalid user test from
107.175.246.204 port 55538
Jan  2 06:07:06 ip-172-31-38-110 sshd[12360]: Invalid user net from
183.107.101.252 port 33268
Jan  2 06:09:30 ip-172-31-38-110 sshd[12438]: Invalid user pgadmin from
116.7.245.184 port 61715
Jan  2 06:10:18 ip-172-31-38-110 sshd[12440]: Invalid user admin from 171.7.78.95
port 54921
Jan  2 06:16:35 ip-172-31-38-110 sshd[12445]: Invalid user dorin from
18.223.108.173 port 58501
Jan  2 06:44:07 ip-172-31-38-110 sshd[12787]: Invalid user vagrant from
206.189.155.156 port 60648
Jan  2 06:53:54 ip-172-31-38-110 sshd[12790]: Invalid user indiana from
62.218.23.242 port 5377
Jan  2 06:54:08 ip-172-31-38-110 sshd[12792]: Invalid user indiana from
206.189.3.162 port 59362
Jan  2 06:54:18 ip-172-31-38-110 sshd[12794]: Invalid user indiana from
77.199.87.64 port 39697
Jan  2 06:54:56 ip-172-31-38-110 sshd[12798]: Invalid user student from
98.209.70.36 port 34204
Jan  2 06:56:16 ip-172-31-38-110 sshd[12800]: Invalid user test from 78.137.5.38
port 55340
Jan  2 06:56:28 ip-172-31-38-110 sshd[12802]: Invalid user mongodb from
142.93.120.94 port 41121
```

```
Jan  2 06:57:55 ip-172-31-38-110 sshd[12804]: Invalid user pri from 79.2.22.244
port 39492
Jan  2 06:59:29 ip-172-31-38-110 sshd[12808]: Invalid user army from 118.24.84.203
port 31010
Jan  2 07:05:45 ip-172-31-38-110 sshd[12813]: Invalid user admin from
116.126.53.112 port 35566
Jan  2 07:07:37 ip-172-31-38-110 sshd[12815]: Invalid user myftp from
35.188.27.107 port 59816
Jan  2 07:07:42 ip-172-31-38-110 sshd[12817]: Invalid user matt from
110.141.243.23 port 54514
Jan  2 07:11:16 ip-172-31-38-110 sshd[12892]: Invalid user kai from 103.100.209.44
port 51221
Jan  2 07:26:07 ip-172-31-38-110 sshd[12900]: Invalid user adela from
109.61.74.245 port 34702
Jan  2 07:26:54 ip-172-31-38-110 sshd[12902]: Invalid user minecraft from
165.227.34.164 port 58726
Jan  2 07:27:08 ip-172-31-38-110 sshd[12904]: Invalid user adela from 190.85.63.50
port 37676
Jan  2 07:27:45 ip-172-31-38-110 sshd[12906]: Invalid user redmine from
206.189.130.251 port 54506
Jan  2 07:31:58 ip-172-31-38-110 sshd[12911]: Invalid user yq from 188.230.79.30
port 46892
Jan  2 07:34:37 ip-172-31-38-110 sshd[12913]: Invalid user sentry from
51.255.162.65 port 43728
Jan  2 07:37:00 ip-172-31-38-110 sshd[12923]: Invalid user carter from
83.248.216.236 port 36552
Jan  2 07:37:18 ip-172-31-38-110 sshd[12925]: Invalid user sammy from
101.89.109.35 port 22572
Jan  2 07:39:22 ip-172-31-38-110 sshd[12999]: Invalid user test from 36.67.59.193
port 55844
Jan  2 07:40:52 ip-172-31-38-110 sshd[13001]: Invalid user sshvpn from
189.153.232.233 port 43284
Jan  2 07:41:41 ip-172-31-38-110 sshd[13003]: Invalid user helena from
119.90.39.158 port 17356
Jan  2 07:53:36 ip-172-31-38-110 sshd[13006]: Invalid user InTouchWebsite.sock
from 111.207.49.185 port 53689
Jan  2 07:58:44 ip-172-31-38-110 sshd[13009]: Invalid user france from 5.39.77.167
port 53068
Jan  2 08:10:20 ip-172-31-38-110 sshd[13089]: Invalid user centos from
222.127.99.45 port 44137
Jan  2 08:16:35 ip-172-31-38-110 sshd[13097]: Invalid user ci from 159.65.239.104
port 33154
Jan  2 08:26:18 ip-172-31-38-110 sshd[13112]: Invalid user ubnt from 178.128.98.90
port 38792
Jan  2 08:28:28 ip-172-31-38-110 sshd[13114]: Invalid user connor from
94.155.97.95 port 41300
Jan  2 08:29:06 ip-172-31-38-110 sshd[13119]: Invalid user admin from
84.193.181.150 port 44802
Jan  2 08:32:11 ip-172-31-38-110 sshd[13122]: Invalid user emma from 51.38.58.42
port 39884
Jan  2 08:32:42 ip-172-31-38-110 sshd[13126]: Invalid user marko from
192.99.244.105 port 45340
Jan  2 08:36:15 ip-172-31-38-110 sshd[13129]: Invalid user postgres from
69.195.148.15 port 49331
```

```
Jan  2 08:39:31 ip-172-31-38-110 sshd[13206]: Invalid user tajo from 118.24.44.129
port 38470
Jan  2 08:44:44 ip-172-31-38-110 sshd[13218]: Invalid user pokemon from
169.239.13.41 port 49034
Jan  2 08:45:11 ip-172-31-38-110 sshd[13220]: Invalid user sinusbot from
103.56.189.134 port 53232
Jan  2 08:53:28 ip-172-31-38-110 sshd[13232]: Invalid user contato from
192.144.155.63 port 51928
Jan  2 08:56:05 ip-172-31-38-110 sshd[13234]: Invalid user git from 106.12.42.98
port 45538
Jan  2 08:56:57 ip-172-31-38-110 sshd[13236]: Invalid user phion from
109.73.46.142 port 59210
Jan  2 09:01:34 ip-172-31-38-110 sshd[13240]: Invalid user fwupgrade from
179.184.0.138 port 40329
Jan  2 09:03:54 ip-172-31-38-110 sshd[13247]: Invalid user miller from
73.207.34.185 port 41864
Jan  2 09:09:28 ip-172-31-38-110 sshd[13253]: Invalid user joyce from 51.255.83.44
port 31692
Jan  2 09:11:16 ip-172-31-38-110 sshd[13328]: Invalid user system from
178.128.107.61 port 57321
Jan  2 09:17:49 ip-172-31-38-110 sshd[13336]: Invalid user control from
118.192.66.79 port 57078
Jan  2 09:18:05 ip-172-31-38-110 sshd[13338]: Invalid user deluge from
103.241.146.65 port 43179
Jan  2 09:29:55 ip-172-31-38-110 sshd[13344]: Invalid user uploader from
51.254.125.33 port 55912
Jan  2 09:31:20 ip-172-31-38-110 sshd[13346]: Invalid user system from
203.75.29.213 port 47375
Jan  2 09:31:58 ip-172-31-38-110 sshd[13350]: Invalid user fff from 5.39.77.117
port 40431
Jan  2 09:32:12 ip-172-31-38-110 sshd[13352]: Invalid user git from 51.38.37.69
port 55609
Jan  2 09:32:12 ip-172-31-38-110 sshd[13354]: Invalid user git from 54.36.181.173
port 46878
Jan  2 09:40:01 ip-172-31-38-110 sshd[13430]: Invalid user sybase from
84.254.0.120 port 33488
Jan  2 09:44:17 ip-172-31-38-110 sshd[13437]: Invalid user carter from
46.101.230.131 port 34808
Jan  2 09:44:20 ip-172-31-38-110 sshd[13439]: Invalid user pascal from
69.90.223.232 port 48712
Jan  2 09:48:52 ip-172-31-38-110 sshd[13444]: Invalid user git from 61.91.14.170
port 34530
Jan  2 09:48:57 ip-172-31-38-110 sshd[13446]: Invalid user test from 96.85.229.50
port 45092
Jan  2 09:49:13 ip-172-31-38-110 sshd[13448]: Invalid user www from 78.231.186.151
port 50180
Jan  2 09:49:43 ip-172-31-38-110 sshd[13451]: Invalid user stas from 218.19.141.70
port 50940
Jan  2 09:50:05 ip-172-31-38-110 sshd[13453]: Invalid user www from
163.172.174.112 port 41286
Jan  2 10:01:29 ip-172-31-38-110 sshd[13460]: Invalid user uj from 31.131.88.66
port 42900
Jan  2 10:03:18 ip-172-31-38-110 sshd[13462]: Invalid user mid from 95.130.8.206
port 36920
```

```
Jan  2 10:03:44 ip-172-31-38-110 sshd[13464]: Invalid user jquery from
47.185.142.141 port 46001
Jan  2 10:05:27 ip-172-31-38-110 sshd[13467]: Invalid user oracle from
183.240.157.3 port 50090
Jan  2 10:06:03 ip-172-31-38-110 sshd[13469]: Invalid user user from 68.183.120.30
port 33156
Jan  2 10:06:09 ip-172-31-38-110 sshd[13471]: Invalid user win from 37.59.99.243
port 52144
Jan  2 10:06:38 ip-172-31-38-110 sshd[13473]: Invalid user win from 201.238.150.58
port 58846
Jan  2 10:09:22 ip-172-31-38-110 sshd[13551]: Invalid user stefan from
190.145.241.122 port 23004
Jan  2 10:11:38 ip-172-31-38-110 sshd[13554]: Invalid user db2fenc1 from
58.210.42.4 port 37900
Jan  2 10:12:05 ip-172-31-38-110 sshd[13556]: Invalid user pgsql from 95.227.7.106
port 65449
Jan  2 10:16:24 ip-172-31-38-110 sshd[13558]: Invalid user fahmed from
85.214.228.9 port 36274
Jan  2 10:18:07 ip-172-31-38-110 sshd[13564]: Invalid user zabbix from
103.21.176.33 port 55051
Jan  2 10:18:45 ip-172-31-38-110 sshd[13566]: Invalid user fahmed from
118.25.222.203 port 58134
Jan  2 10:29:41 ip-172-31-38-110 sshd[13572]: Invalid user sajid from
104.194.250.10 port 41872
Jan  2 10:31:45 ip-172-31-38-110 sshd[13574]: Invalid user admin from
94.191.87.180 port 45124
Jan  2 10:33:21 ip-172-31-38-110 sshd[13576]: Invalid user postgresql from
203.86.8.44 port 35414
Jan  2 10:35:12 ip-172-31-38-110 sshd[13579]: Invalid user corentin from
45.55.67.128 port 59609
Jan  2 10:35:58 ip-172-31-38-110 sshd[13581]: Invalid user corentin from
14.116.217.18 port 43855
Jan  2 10:37:11 ip-172-31-38-110 sshd[13587]: Invalid user localadmin from
188.11.67.165 port 43705
Jan  2 10:46:53 ip-172-31-38-110 sshd[13665]: Invalid user anita from 139.59.78.70
port 34240
Jan  2 10:49:01 ip-172-31-38-110 sshd[13667]: Invalid user admin from
121.13.107.114 port 41219
Jan  2 10:50:45 ip-172-31-38-110 sshd[13672]: Invalid user lazaro from 27.82.0.143
port 48028
Jan  2 11:08:41 ip-172-31-38-110 sshd[13681]: Invalid user foo from 65.182.171.122
port 50931
Jan  2 11:09:14 ip-172-31-38-110 sshd[13759]: Invalid user foo from 144.217.83.109
port 59118
Jan  2 11:09:32 ip-172-31-38-110 sshd[13761]: Invalid user oracle from
186.146.1.37 port 45888
Jan  2 11:09:51 ip-172-31-38-110 sshd[13763]: Invalid user oracle from
14.18.118.232 port 52764
Jan  2 11:10:43 ip-172-31-38-110 sshd[13765]: Invalid user oracle from
121.201.78.33 port 29392
Jan  2 11:17:18 ip-172-31-38-110 sshd[13773]: Invalid user test from 51.15.51.54
port 39202
Jan  2 11:17:59 ip-172-31-38-110 sshd[13776]: Invalid user test from
212.237.38.213 port 57558
```

```
Jan  2 11:18:37 ip-172-31-38-110 sshd[13778]: Invalid user ben from 95.58.194.141
port 35394
Jan  2 11:18:56 ip-172-31-38-110 sshd[13780]: Invalid user fcoperador from
113.137.41.56 port 57148
Jan  2 11:19:26 ip-172-31-38-110 sshd[13782]: Invalid user fcoperador from
132.232.18.128 port 59426
Jan  2 11:20:30 ip-172-31-38-110 sshd[13784]: Invalid user ben from
111.231.220.138 port 56682
Jan  2 11:21:51 ip-172-31-38-110 sshd[13788]: Invalid user technical from
119.27.170.189 port 59108
Jan  2 11:27:33 ip-172-31-38-110 sshd[13793]: Invalid user server from
132.232.39.15 port 49390
Jan  2 11:29:21 ip-172-31-38-110 sshd[13797]: Invalid user bot from 5.249.145.73
port 56206
Jan  2 11:29:49 ip-172-31-38-110 sshd[13799]: Invalid user mongo from
210.29.36.183 port 50992
Jan  2 11:30:03 ip-172-31-38-110 sshd[13801]: Invalid user alpha from
128.199.189.192 port 36714
Jan  2 11:36:23 ip-172-31-38-110 sshd[13809]: Invalid user admin from
145.239.76.62 port 43946
Jan  2 11:40:30 ip-172-31-38-110 sshd[13887]: Invalid user DBSNMP from
37.187.23.116 port 41832
Jan  2 11:41:12 ip-172-31-38-110 sshd[13889]: Invalid user DBSNMP from 188.2.61.41
port 44989
Jan  2 11:54:24 ip-172-31-38-110 sshd[13897]: Invalid user student09 from
170.210.60.25 port 55822
Jan  2 11:58:07 ip-172-31-38-110 sshd[13899]: Invalid user cpanel from
217.61.107.185 port 58416
Jan  2 11:59:54 ip-172-31-38-110 sshd[13905]: Invalid user user from
177.103.179.92 port 52360
Jan  2 12:07:48 ip-172-31-38-110 sshd[13912]: Invalid user oracle from
221.231.11.243 port 53783
Jan  2 12:10:48 ip-172-31-38-110 sshd[13993]: Invalid user applvis from
178.48.177.251 port 43766
Jan  2 12:12:47 ip-172-31-38-110 sshd[13995]: Invalid user pi from 88.190.183.18
port 46968
Jan  2 12:12:47 ip-172-31-38-110 sshd[13997]: Invalid user pi from 88.190.183.18
port 46970
Jan  2 12:29:03 ip-172-31-38-110 sshd[14026]: Invalid user odoo from 5.196.66.30
port 35754
Jan  2 12:30:16 ip-172-31-38-110 sshd[14028]: Invalid user odoo from
94.135.173.134 port 47191
Jan  2 12:30:56 ip-172-31-38-110 sshd[14030]: Invalid user vbox from 217.91.87.131
port 37654
Jan  2 12:31:25 ip-172-31-38-110 sshd[14032]: Invalid user desadm from 45.55.158.8
port 40988
Jan  2 12:31:35 ip-172-31-38-110 sshd[14034]: Invalid user cali from
218.77.105.251 port 53798
Jan  2 12:31:46 ip-172-31-38-110 sshd[14036]: Invalid user uj from 194.182.86.133
port 50748
Jan  2 12:31:54 ip-172-31-38-110 sshd[14038]: Invalid user admin from 129.144.9.88
port 16394
Jan  2 12:32:10 ip-172-31-38-110 sshd[14040]: Invalid user mq from 188.166.233.64
port 59343
```

```
Jan  2 12:32:29 ip-172-31-38-110 sshd[14042]: Invalid user desadm from
178.128.107.147 port 58704
Jan  2 12:32:31 ip-172-31-38-110 sshd[14044]: Invalid user titan from
217.182.74.125 port 45350
Jan  2 12:32:36 ip-172-31-38-110 sshd[14046]: Invalid user uj from 190.116.41.227
port 50060
Jan  2 12:33:26 ip-172-31-38-110 sshd[14050]: Invalid user desadm from
118.24.221.190 port 25070
Jan  2 12:33:30 ip-172-31-38-110 sshd[14052]: Invalid user Administrator from
178.128.22.66 port 36911
Jan  2 12:34:27 ip-172-31-38-110 sshd[14055]: Invalid user dev from 106.12.197.85
port 52814
Jan  2 12:41:50 ip-172-31-38-110 sshd[14130]: Invalid user noc from 176.31.182.158
port 43067
Jan  2 12:43:42 ip-172-31-38-110 sshd[14132]: Invalid user uftp from
207.154.232.160 port 55832
Jan  2 12:43:59 ip-172-31-38-110 sshd[14134]: Invalid user server from
87.140.14.142 port 32640
Jan  2 12:54:42 ip-172-31-38-110 sshd[14141]: Invalid user boris from 159.89.13.0
port 56392
Jan  2 12:54:55 ip-172-31-38-110 sshd[14143]: Invalid user pankaj from
193.70.79.213 port 46226
Jan  2 12:58:22 ip-172-31-38-110 sshd[14145]: Invalid user pythia from
172.254.107.118 port 37851
Jan  2 13:03:37 ip-172-31-38-110 sshd[14149]: Invalid user media from 94.23.0.13
port 38479
Jan  2 13:07:06 ip-172-31-38-110 sshd[14151]: Invalid user owen from 119.28.50.163
port 57198
Jan  2 13:08:07 ip-172-31-38-110 sshd[14153]: Invalid user sammy from
138.197.153.30 port 47586
Jan  2 13:09:51 ip-172-31-38-110 sshd[14231]: Invalid user hayden from
14.63.221.108 port 33697
Jan  2 13:11:27 ip-172-31-38-110 sshd[14233]: Invalid user ethos from
114.67.72.212 port 51174
Jan  2 13:12:26 ip-172-31-38-110 sshd[14235]: Invalid user florian from
159.65.12.204 port 37970
Jan  2 13:23:55 ip-172-31-38-110 sshd[14242]: Invalid user vi from 207.154.206.212
port 34534
Jan  2 13:23:56 ip-172-31-38-110 sshd[14244]: Invalid user vi from 159.203.94.6
port 60196
Jan  2 13:29:12 ip-172-31-38-110 sshd[14248]: Invalid user test from 118.25.52.98
port 56346
Jan  2 13:30:25 ip-172-31-38-110 sshd[14253]: Invalid user bryan from
140.143.93.31 port 36816
Jan  2 13:45:01 ip-172-31-38-110 sshd[14339]: Invalid user ivan from 165.227.69.39
port 45383
Jan  2 13:45:05 ip-172-31-38-110 sshd[14341]: Invalid user ivan from
107.170.95.116 port 36352
Jan  2 13:45:12 ip-172-31-38-110 sshd[14343]: Invalid user psimiyu from
121.44.63.241 port 57426
Jan  2 13:48:11 ip-172-31-38-110 sshd[14346]: Invalid user cpanel from
122.55.90.45 port 60230
Jan  2 13:48:24 ip-172-31-38-110 sshd[14348]: Invalid user old from
192.241.227.172 port 44780
```

```
Jan  2 13:56:12 ip-172-31-38-110 sshd[14351]: Invalid user soporte from
81.217.11.47 port 54881
Jan  2 14:09:47 ip-172-31-38-110 sshd[14434]: Invalid user admin from 5.101.40.37
port 48876
Jan  2 14:09:48 ip-172-31-38-110 sshd[14436]: Invalid user ubnt from 5.101.40.37
port 60266
Jan  2 14:09:48 ip-172-31-38-110 sshd[14440]: Invalid user admin from 5.101.40.38
port 53687
Jan  2 14:39:33 ip-172-31-38-110 sshd[14450]: Invalid user edi from 61.178.93.167
port 43143
Jan  2 15:01:04 ip-172-31-38-110 sshd[14536]: Invalid user vbox from
211.159.219.105 port 59232
Jan  2 15:35:27 ip-172-31-38-110 sshd[14626]: Invalid user admin from 5.101.40.38
port 34604
Jan  2 15:35:27 ip-172-31-38-110 sshd[14628]: Invalid user ubnt from 5.101.40.37
port 33360
Jan  2 15:35:28 ip-172-31-38-110 sshd[14632]: Invalid user admin from 5.101.40.37
port 38354
Jan  2 16:06:56 ip-172-31-38-110 sshd[14717]: Invalid user ftp1 from 106.12.92.88
port 42420
Jan  2 16:09:34 ip-172-31-38-110 sshd[14796]: Invalid user byu from 148.235.57.179
port 43208
Jan  2 16:09:44 ip-172-31-38-110 sshd[14798]: Invalid user byu from 152.249.246.65
port 39692
Jan  2 16:12:09 ip-172-31-38-110 sshd[14801]: Invalid user Administrator from
35.196.174.223 port 51020
Jan  2 16:14:59 ip-172-31-38-110 sshd[14808]: Invalid user admin from 27.72.24.93
port 54382
Jan  2 16:15:32 ip-172-31-38-110 sshd[14810]: Invalid user ghost from
104.248.65.180 port 41734
Jan  2 16:15:33 ip-172-31-38-110 sshd[14814]: Invalid user sienna from
46.41.149.32 port 48478
Jan  2 16:15:34 ip-172-31-38-110 sshd[14812]: Invalid user king from
159.89.199.224 port 53152
Jan  2 16:15:52 ip-172-31-38-110 sshd[14816]: Invalid user sienna from
71.239.149.126 port 59241
Jan  2 16:17:41 ip-172-31-38-110 sshd[14822]: Invalid user wms from 104.248.29.180
port 41090
Jan  2 16:17:43 ip-172-31-38-110 sshd[14824]: Invalid user wms from 178.33.45.156
port 37602
Jan  2 16:17:44 ip-172-31-38-110 sshd[14826]: Invalid user squid from
178.128.227.38 port 48972
Jan  2 16:19:52 ip-172-31-38-110 sshd[14828]: Invalid user www-ssl from
85.192.171.23 port 36162
Jan  2 16:38:58 ip-172-31-38-110 sshd[15275]: Invalid user wh from 169.50.36.140
port 44606
Jan  2 16:41:00 ip-172-31-38-110 sshd[15355]: Invalid user zv from 41.216.228.158
port 34625
Jan  2 16:44:25 ip-172-31-38-110 sshd[15357]: Invalid user rachel from
50.73.95.203 port 42276
Jan  2 16:44:27 ip-172-31-38-110 sshd[15359]: Invalid user rachel from
178.128.150.79 port 41984
Jan  2 16:44:44 ip-172-31-38-110 sshd[15361]: Invalid user steam from
170.210.88.50 port 36308
```

```
Jan  2 16:44:59 ip-172-31-38-110 sshd[15364]: Invalid user ftp_id from
62.12.115.116 port 51786
Jan  2 16:49:30 ip-172-31-38-110 sshd[15366]: Invalid user oracle from
195.154.82.158 port 50552
Jan  2 16:49:35 ip-172-31-38-110 sshd[15372]: Invalid user ork from 139.59.133.18
port 52712
Jan  2 16:49:35 ip-172-31-38-110 sshd[15370]: Invalid user oracle from
67.205.135.65 port 51540
Jan  2 16:49:35 ip-172-31-38-110 sshd[15374]: Invalid user oracle from
79.106.191.5 port 56802
Jan  2 16:49:36 ip-172-31-38-110 sshd[15378]: Invalid user oracle from
35.204.13.102 port 52462
Jan  2 16:49:37 ip-172-31-38-110 sshd[15380]: Invalid user minecraft from
141.85.241.166 port 34310
Jan  2 16:49:38 ip-172-31-38-110 sshd[15382]: Invalid user minecraft from
35.239.133.223 port 47460
Jan  2 16:49:38 ip-172-31-38-110 sshd[15384]: Invalid user minecraft from
158.69.221.102 port 37801
Jan  2 16:49:42 ip-172-31-38-110 sshd[15386]: Invalid user minecraft from
82.27.152.254 port 36324
Jan  2 16:49:51 ip-172-31-38-110 sshd[15388]: Invalid user postmaster from
91.216.178.210 port 54684
Jan  2 16:50:09 ip-172-31-38-110 sshd[15391]: Invalid user postmaster from
116.196.112.25 port 52122
Jan  2 16:56:10 ip-172-31-38-110 sshd[15394]: Invalid user monsegur from
35.227.34.247 port 41212
Jan  2 16:56:12 ip-172-31-38-110 sshd[15396]: Invalid user hw from 142.93.160.229
port 41704
Jan  2 16:56:25 ip-172-31-38-110 sshd[15398]: Invalid user hw from 118.45.190.133
port 35922
Jan  2 17:01:22 ip-172-31-38-110 sshd[15403]: Invalid user shoping from
178.62.193.128 port 45082
Jan  2 17:01:23 ip-172-31-38-110 sshd[15405]: Invalid user annmarie from
104.236.246.127 port 41932
Jan  2 17:01:26 ip-172-31-38-110 sshd[15407]: Invalid user annmarie from
188.20.26.110 port 49348
Jan  2 17:01:27 ip-172-31-38-110 sshd[15409]: Invalid user slu from 117.3.69.194
port 50064
Jan  2 17:01:27 ip-172-31-38-110 sshd[15411]: Invalid user avahi-autoipd from
128.199.106.169 port 59262
Jan  2 17:01:31 ip-172-31-38-110 sshd[15413]: Invalid user mrtg from 211.216.79.93
port 48052
Jan  2 17:01:37 ip-172-31-38-110 sshd[15415]: Invalid user avahi-autoipd from
106.12.197.253 port 46152
Jan  2 17:01:37 ip-172-31-38-110 sshd[15417]: Invalid user annmarie from
159.89.170.154 port 33864
Jan  2 17:01:39 ip-172-31-38-110 sshd[15419]: Invalid user thanks from
37.59.183.21 port 52872
Jan  2 17:01:43 ip-172-31-38-110 sshd[15421]: Invalid user thanks from
150.214.140.117 port 59582
Jan  2 17:01:49 ip-172-31-38-110 sshd[15424]: Invalid user qy from 128.199.232.32
port 44926
Jan  2 17:01:49 ip-172-31-38-110 sshd[15423]: Invalid user qy from 120.92.19.174
port 2590
```

```
Jan  2 17:01:53 ip-172-31-38-110 sshd[15427]: Invalid user louis from
106.12.201.226 port 46578
Jan  2 17:02:03 ip-172-31-38-110 sshd[15429]: Invalid user iptv from 180.76.233.55
port 59142
Jan  2 17:02:19 ip-172-31-38-110 sshd[15431]: Invalid user thanks from
41.249.251.226 port 42550
Jan  2 17:04:29 ip-172-31-38-110 sshd[15433]: Invalid user element from
203.142.65.188 port 39978
Jan  2 17:04:31 ip-172-31-38-110 sshd[15435]: Invalid user codeunbug from
116.93.119.13 port 39688
Jan  2 17:11:01 ip-172-31-38-110 sshd[15515]: Invalid user medias from
195.68.29.234 port 53646
Jan  2 17:11:02 ip-172-31-38-110 sshd[15517]: Invalid user medias from
69.195.148.15 port 48503
Jan  2 17:11:05 ip-172-31-38-110 sshd[15519]: Invalid user medias from
209.97.178.123 port 40252
Jan  2 17:11:07 ip-172-31-38-110 sshd[15521]: Invalid user mailadmin from
68.183.113.232 port 33404
Jan  2 17:11:15 ip-172-31-38-110 sshd[15523]: Invalid user mailadmin from
185.193.235.42 port 45796
Jan  2 17:11:17 ip-172-31-38-110 sshd[15525]: Invalid user max from
122.160.152.107 port 54680
Jan  2 17:11:33 ip-172-31-38-110 sshd[15527]: Invalid user medias from
223.171.32.66 port 54442
Jan  2 17:18:31 ip-172-31-38-110 sshd[15534]: Invalid user fdrusers from
185.207.232.232 port 53560
Jan  2 17:18:37 ip-172-31-38-110 sshd[15536]: Invalid user admin from
43.225.117.245 port 46040
Jan  2 17:18:38 ip-172-31-38-110 sshd[15538]: Invalid user fdrusers from
124.194.44.219 port 41290
Jan  2 17:18:41 ip-172-31-38-110 sshd[15540]: Invalid user fdrusers from
172.81.248.131 port 33096
Jan  2 17:18:42 ip-172-31-38-110 sshd[15542]: Invalid user admin from
178.128.119.59 port 56260
Jan  2 17:18:45 ip-172-31-38-110 sshd[15544]: Invalid user admin from
114.143.109.126 port 50372
Jan  2 17:18:47 ip-172-31-38-110 sshd[15546]: Invalid user fdrusers from
125.70.230.211 port 35476
Jan  2 17:18:58 ip-172-31-38-110 sshd[15548]: Invalid user fdrusers from
118.24.101.182 port 49466
Jan  2 17:24:34 ip-172-31-38-110 sshd[15553]: Invalid user newgit from
104.131.178.223 port 56488
Jan  2 17:24:45 ip-172-31-38-110 sshd[15555]: Invalid user stefan from
67.198.104.73 port 56028
Jan  2 17:24:53 ip-172-31-38-110 sshd[15557]: Invalid user stefan from
31.19.254.144 port 58687
Jan  2 17:26:09 ip-172-31-38-110 sshd[15559]: Invalid user pentaho from
189.204.229.30 port 52202
Jan  2 17:27:14 ip-172-31-38-110 sshd[15561]: Invalid user jenny from
197.245.235.170 port 15890
Jan  2 17:28:22 ip-172-31-38-110 sshd[15564]: Invalid user sa from 89.134.42.194
port 42171
Jan  2 17:34:33 ip-172-31-38-110 sshd[15570]: Invalid user sysadmin from
207.154.192.36 port 37072
```

```
Jan  2 17:34:33 ip-172-31-38-110 sshd[15573]: Invalid user sysadmin from
51.75.198.127 port 41208
Jan  2 17:34:33 ip-172-31-38-110 sshd[15568]: Invalid user roland from 71.198.1.69
port 39410
Jan  2 17:34:33 ip-172-31-38-110 sshd[15572]: Invalid user roland from
108.235.160.215 port 44772
Jan  2 17:34:43 ip-172-31-38-110 sshd[15576]: Invalid user user1 from
222.255.46.225 port 60028
Jan  2 17:34:44 ip-172-31-38-110 sshd[15578]: Invalid user sysadmin from
95.90.131.203 port 32890
Jan  2 17:34:48 ip-172-31-38-110 sshd[15580]: Invalid user roland from
79.175.151.153 port 53572
Jan  2 17:34:51 ip-172-31-38-110 sshd[15582]: Invalid user http from
222.223.121.114 port 54624
Jan  2 17:34:54 ip-172-31-38-110 sshd[15584]: Invalid user sysadmin from
83.244.80.102 port 43676
Jan  2 17:38:20 ip-172-31-38-110 sshd[15587]: Invalid user bserver from
106.12.10.194 port 59042
Jan  2 17:38:44 ip-172-31-38-110 sshd[15589]: Invalid user svn from
114.255.153.237 port 58842
Jan  2 17:44:28 ip-172-31-38-110 sshd[15669]: Invalid user gogs from 5.135.152.97
port 50302
Jan  2 17:44:41 ip-172-31-38-110 sshd[15671]: Invalid user online from 79.9.33.138
port 52400
Jan  2 17:45:43 ip-172-31-38-110 sshd[15673]: Invalid user online from
128.199.189.192 port 52350
Jan  2 17:50:41 ip-172-31-38-110 sshd[15676]: Invalid user johnny from
125.75.47.88 port 40948
Jan  2 18:05:01 ip-172-31-38-110 sshd[15684]: Invalid user guest from 139.59.13.63
port 60744
Jan  2 18:07:10 ip-172-31-38-110 sshd[15687]: Invalid user wangtao from
188.219.40.66 port 50946
Jan  2 18:07:13 ip-172-31-38-110 sshd[15689]: Invalid user amarco from
116.235.212.124 port 58402
Jan  2 18:07:52 ip-172-31-38-110 sshd[15691]: Invalid user ut2k4server from
123.207.142.31 port 58222
Jan  2 18:10:51 ip-172-31-38-110 sshd[15768]: Invalid user it from 137.135.73.152
port 48764
Jan  2 18:10:52 ip-172-31-38-110 sshd[15770]: Invalid user it from 31.168.73.2
port 48160
Jan  2 18:10:58 ip-172-31-38-110 sshd[15772]: Invalid user it from 194.182.66.70
port 42848
Jan  2 18:11:33 ip-172-31-38-110 sshd[15774]: Invalid user ser from 218.2.234.6
port 11740
Jan  2 18:13:12 ip-172-31-38-110 sshd[15776]: Invalid user lab from 115.159.46.47
port 46309
Jan  2 18:15:25 ip-172-31-38-110 sshd[15778]: Invalid user vnc from 165.227.17.252
port 36602
Jan  2 18:15:25 ip-172-31-38-110 sshd[15781]: Invalid user amit from 145.239.91.65
port 43318
Jan  2 18:15:26 ip-172-31-38-110 sshd[15780]: Invalid user amit from
209.217.192.148 port 45052
Jan  2 18:15:27 ip-172-31-38-110 sshd[15784]: Invalid user amit from 186.146.1.37
port 59278
```

```
Jan  2 18:15:35 ip-172-31-38-110 sshd[15786]: Invalid user vnc from 219.246.78.18
port 49950
Jan  2 18:16:00 ip-172-31-38-110 sshd[15789]: Invalid user prova from 37.59.6.106
port 48492
Jan  2 18:16:14 ip-172-31-38-110 sshd[15791]: Invalid user user from
222.122.50.237 port 54112
Jan  2 18:16:16 ip-172-31-38-110 sshd[15793]: Invalid user user from
195.189.68.170 port 39486
Jan  2 18:16:23 ip-172-31-38-110 sshd[15795]: Invalid user deploy3 from
118.89.111.229 port 34561
Jan  2 18:16:25 ip-172-31-38-110 sshd[15797]: Invalid user wp from 150.107.148.155
port 56292
Jan  2 18:20:15 ip-172-31-38-110 sshd[15804]: Invalid user wyf from 24.49.175.75
port 37762
Jan  2 18:20:17 ip-172-31-38-110 sshd[15806]: Invalid user wyf from 13.67.34.145
port 49028
Jan  2 18:20:23 ip-172-31-38-110 sshd[15808]: Invalid user wyf from 14.116.251.29
port 55654
Jan  2 18:20:26 ip-172-31-38-110 sshd[15810]: Invalid user bridge from
178.128.217.40 port 60908
Jan  2 18:22:16 ip-172-31-38-110 sshd[15813]: Invalid user isa from 210.154.29.140
port 45028
Jan  2 18:24:07 ip-172-31-38-110 sshd[15816]: Invalid user kr from 52.14.117.0
port 63926
Jan  2 18:24:08 ip-172-31-38-110 sshd[15818]: Invalid user kr from 158.69.121.144
port 40062
Jan  2 18:24:08 ip-172-31-38-110 sshd[15820]: Invalid user kadmin from
194.182.76.190 port 55110
Jan  2 18:24:09 ip-172-31-38-110 sshd[15822]: Invalid user kr from 129.144.180.57
port 60429
Jan  2 18:24:11 ip-172-31-38-110 sshd[15824]: Invalid user kr from 68.183.62.109
port 47754
Jan  2 18:24:25 ip-172-31-38-110 sshd[15826]: Invalid user stack from
68.183.182.103 port 59910
Jan  2 18:24:33 ip-172-31-38-110 sshd[15828]: Invalid user tommy from
132.232.105.220 port 40630
Jan  2 18:24:37 ip-172-31-38-110 sshd[15830]: Invalid user annmarie from
191.17.185.28 port 49421
Jan  2 18:24:46 ip-172-31-38-110 sshd[15832]: Invalid user annmarie from
107.191.56.63 port 53713
Jan  2 18:31:14 ip-172-31-38-110 sshd[15838]: Invalid user mozilla from
51.38.185.231 port 32918
Jan  2 18:31:14 ip-172-31-38-110 sshd[15839]: Invalid user beau from
104.248.121.89 port 47812
Jan  2 18:32:19 ip-172-31-38-110 sshd[15843]: Invalid user git from 104.248.188.44
port 57636
Jan  2 18:32:30 ip-172-31-38-110 sshd[15845]: Invalid user test from 106.37.111.34
port 47505
Jan  2 18:36:50 ip-172-31-38-110 sshd[15848]: Invalid user hadoop from
119.29.204.217 port 60184
Jan  2 18:40:06 ip-172-31-38-110 sshd[15936]: Invalid user sun from 81.217.11.47
port 44518
Jan  2 18:41:09 ip-172-31-38-110 sshd[15939]: Invalid user support from
186.116.221.161 port 55356
```

```
Jan  2 18:45:35 ip-172-31-38-110 sshd[15944]: Invalid user master from 5.39.3.235
port 49442
Jan  2 18:46:00 ip-172-31-38-110 sshd[15946]: Invalid user informix from
106.12.92.88 port 52246
Jan  2 18:48:57 ip-172-31-38-110 sshd[15948]: Invalid user ts3bot from
182.71.188.10 port 38182
Jan  2 18:51:49 ip-172-31-38-110 sshd[15954]: Invalid user user from 108.36.241.40
port 17646
Jan  2 18:52:02 ip-172-31-38-110 sshd[15956]: Invalid user user from 41.138.88.3
port 56935
Jan  2 18:52:04 ip-172-31-38-110 sshd[15958]: Invalid user postgres from
103.110.89.148 port 41068
Jan  2 18:52:09 ip-172-31-38-110 sshd[15960]: Invalid user user from 63.143.98.38
port 43291
Jan  2 18:54:59 ip-172-31-38-110 sshd[15963]: Invalid user databse from
110.35.173.102 port 27508
Jan  2 18:55:02 ip-172-31-38-110 sshd[15965]: Invalid user field from
190.153.219.50 port 50334
Jan  2 18:55:06 ip-172-31-38-110 sshd[15967]: Invalid user teamspeak3 from
120.92.173.154 port 2660
Jan  2 18:55:24 ip-172-31-38-110 sshd[15969]: Invalid user oradev from
223.171.32.55 port 3986
Jan  2 18:56:49 ip-172-31-38-110 sshd[15971]: Invalid user solo from 72.38.90.230
port 5313
Jan  2 18:56:52 ip-172-31-38-110 sshd[15973]: Invalid user student from
190.85.234.215 port 49992
Jan  2 18:56:57 ip-172-31-38-110 sshd[15975]: Invalid user solo from 181.55.95.52
port 40497
Jan  2 18:57:07 ip-172-31-38-110 sshd[15977]: Invalid user qf from 119.28.71.103
port 54812
Jan  2 18:57:07 ip-172-31-38-110 sshd[15979]: Invalid user bot from 90.65.67.16
port 39020
Jan  2 18:57:11 ip-172-31-38-110 sshd[15981]: Invalid user openerp from
89.22.255.160 port 38882
Jan  2 18:58:28 ip-172-31-38-110 sshd[15988]: Invalid user test from
206.189.198.64 port 58012
Jan  2 18:58:40 ip-172-31-38-110 sshd[15990]: Invalid user openerp from
188.131.139.105 port 60184
Jan  2 19:01:04 ip-172-31-38-110 sshd[15998]: Invalid user test from
89.154.183.131 port 56934
Jan  2 19:03:44 ip-172-31-38-110 sshd[16002]: Invalid user ftp from 168.62.59.195
port 55674
Jan  2 19:03:46 ip-172-31-38-110 sshd[16004]: Invalid user ftp from
188.213.165.189 port 59668
Jan  2 19:03:46 ip-172-31-38-110 sshd[16006]: Invalid user ftp from 109.248.149.82
port 49544
Jan  2 19:03:54 ip-172-31-38-110 sshd[16010]: Invalid user ec2-user from
122.228.253.94 port 58741
Jan  2 19:07:15 ip-172-31-38-110 sshd[16017]: Invalid user et from 91.121.142.225
port 56290
Jan  2 19:07:55 ip-172-31-38-110 sshd[16022]: Invalid user taiga from
91.121.134.80 port 48142
Jan  2 19:08:30 ip-172-31-38-110 sshd[16024]: Invalid user xguest from
80.11.44.112 port 40346
```

```
Jan  2 19:08:33 ip-172-31-38-110 sshd[16026]: Invalid user xguest from
79.11.169.178 port 59548
Jan  2 19:08:37 ip-172-31-38-110 sshd[16028]: Invalid user build from
104.236.181.90 port 42326
Jan  2 19:08:40 ip-172-31-38-110 sshd[16030]: Invalid user build from
141.136.44.81 port 57356
Jan  2 19:08:52 ip-172-31-38-110 sshd[16032]: Invalid user tanja from
189.125.2.234 port 34843
Jan  2 19:10:50 ip-172-31-38-110 sshd[16109]: Invalid user xerox from
52.246.254.177 port 46472
Jan  2 19:10:58 ip-172-31-38-110 sshd[16111]: Invalid user xerox from 125.63.78.18
port 42534
Jan  2 19:11:53 ip-172-31-38-110 sshd[16113]: Invalid user admin from 209.97.164.5
port 59210
Jan  2 19:14:15 ip-172-31-38-110 sshd[16120]: Invalid user forums from
83.211.93.54 port 26106
Jan  2 19:14:17 ip-172-31-38-110 sshd[16122]: Invalid user forums from
94.23.204.136 port 60524
Jan  2 19:14:30 ip-172-31-38-110 sshd[16124]: Invalid user jc2server from
206.189.155.156 port 35078
Jan  2 19:18:11 ip-172-31-38-110 sshd[16131]: Invalid user jason from 54.36.151.64
port 60122
Jan  2 19:18:19 ip-172-31-38-110 sshd[16133]: Invalid user stefan from
209.97.178.123 port 33110
Jan  2 19:18:19 ip-172-31-38-110 sshd[16135]: Invalid user stefan from
217.182.206.141 port 49024
Jan  2 19:18:19 ip-172-31-38-110 sshd[16137]: Invalid user wii from
104.248.128.101 port 51732
Jan  2 19:18:35 ip-172-31-38-110 sshd[16139]: Invalid user testxp from
129.204.46.170 port 41150
Jan  2 19:19:34 ip-172-31-38-110 sshd[16141]: Invalid user bobbi from 51.254.125.33
port 58076
Jan  2 19:20:02 ip-172-31-38-110 sshd[16143]: Invalid user chimistry from
125.134.251.45 port 37884
Jan  2 19:20:04 ip-172-31-38-110 sshd[16145]: Invalid user weblogic from
118.45.190.133 port 45706
Jan  2 19:21:57 ip-172-31-38-110 sshd[16147]: Invalid user chimistry from
111.230.151.185 port 54270
Jan  2 19:26:53 ip-172-31-38-110 sshd[16154]: Invalid user ryder from
213.108.216.19 port 51836
Jan  2 19:27:00 ip-172-31-38-110 sshd[16156]: Invalid user giga from 124.43.17.169
port 41192
Jan  2 19:27:02 ip-172-31-38-110 sshd[16158]: Invalid user od from 204.197.182.51
port 22107
Jan  2 19:28:37 ip-172-31-38-110 sshd[16162]: Invalid user melinda from
91.121.211.34 port 41998
Jan  2 19:28:40 ip-172-31-38-110 sshd[16164]: Invalid user team from 178.62.60.225
port 51430
Jan  2 19:28:41 ip-172-31-38-110 sshd[16166]: Invalid user team from 142.93.109.33
port 52288
Jan  2 19:28:42 ip-172-31-38-110 sshd[16168]: Invalid user gitlab from
136.159.169.8 port 3247
Jan  2 19:28:42 ip-172-31-38-110 sshd[16170]: Invalid user nexthink from
31.19.254.144 port 37640
```

```
Jan  2 19:28:49 ip-172-31-38-110 sshd[16175]: Invalid user team from 193.24.222.66
port 50088
Jan  2 19:28:53 ip-172-31-38-110 sshd[16177]: Invalid user melinda from
122.228.253.96 port 46105
Jan  2 19:28:56 ip-172-31-38-110 sshd[16179]: Invalid user melinda from
186.223.130.160 port 39262
Jan  2 19:29:03 ip-172-31-38-110 sshd[16181]: Invalid user tracy from
106.12.30.122 port 46047
Jan  2 19:29:23 ip-172-31-38-110 sshd[16184]: Invalid user vftp from 223.171.32.55
port 3986
Jan  2 19:29:31 ip-172-31-38-110 sshd[16188]: Invalid user user2 from
140.143.206.82 port 36980
Jan  2 19:35:01 ip-172-31-38-110 sshd[16205]: Invalid user bc from 138.197.150.166
port 54054
Jan  2 19:35:19 ip-172-31-38-110 sshd[16207]: Invalid user czarek from
210.154.29.140 port 43162
Jan  2 19:35:35 ip-172-31-38-110 sshd[16209]: Invalid user ph from 18.205.233.192
port 60276
Jan  2 19:35:39 ip-172-31-38-110 sshd[16211]: Invalid user ph from 129.150.169.32
port 39102
Jan  2 19:35:45 ip-172-31-38-110 sshd[16213]: Invalid user bc from 178.151.69.163
port 34632
Jan  2 19:35:47 ip-172-31-38-110 sshd[16215]: Invalid user sinusbot from
41.138.88.3 port 52496
Jan  2 19:35:49 ip-172-31-38-110 sshd[16217]: Invalid user portal from
40.73.119.16 port 39678
Jan  2 19:42:31 ip-172-31-38-110 sshd[16297]: Invalid user webmaster from
116.196.80.82 port 56302
Jan  2 19:43:27 ip-172-31-38-110 sshd[16301]: Invalid user wwwadm from
84.91.128.47 port 36722
Jan  2 19:43:58 ip-172-31-38-110 sshd[16303]: Invalid user nagios from
51.68.127.28 port 38642
Jan  2 19:44:00 ip-172-31-38-110 sshd[16305]: Invalid user nagios from
45.55.67.128 port 51743
Jan  2 19:44:34 ip-172-31-38-110 sshd[16307]: Invalid user test from
178.151.69.163 port 32934
Jan  2 19:45:08 ip-172-31-38-110 sshd[16311]: Invalid user lab from 54.36.47.248
port 45274
Jan  2 19:45:09 ip-172-31-38-110 sshd[16310]: Invalid user spark from
133.130.121.140 port 37430
Jan  2 19:45:25 ip-172-31-38-110 sshd[16314]: Invalid user automak from
193.112.10.59 port 46538
Jan  2 19:45:29 ip-172-31-38-110 sshd[16316]: Invalid user user from 148.70.11.98
port 60336
Jan  2 19:50:21 ip-172-31-38-110 sshd[16320]: Invalid user student06 from
190.85.247.157 port 55362
Jan  2 19:50:27 ip-172-31-38-110 sshd[16322]: Invalid user bob from 217.36.223.29
port 51677
Jan  2 19:50:39 ip-172-31-38-110 sshd[16324]: Invalid user dg from 106.12.10.194
port 43754
Jan  2 20:02:41 ip-172-31-38-110 sshd[16336]: Invalid user mrtg from 106.12.37.232
port 50652
Jan  2 20:03:21 ip-172-31-38-110 sshd[16339]: Invalid user kevin from
158.69.161.90 port 46725
```

```
Jan  2 20:03:54 ip-172-31-38-110 sshd[16341]: Invalid user oracle from
188.131.142.28 port 42574
Jan  2 20:04:16 ip-172-31-38-110 sshd[16343]: Invalid user sam from 178.128.150.79
port 54134
Jan  2 20:05:28 ip-172-31-38-110 sshd[16347]: Invalid user site from 73.207.34.185
port 59572
Jan  2 20:05:33 ip-172-31-38-110 sshd[16350]: Invalid user site from
190.145.237.254 port 44994
Jan  2 20:05:37 ip-172-31-38-110 sshd[16352]: Invalid user site from 61.12.38.162
port 38192
Jan  2 20:05:41 ip-172-31-38-110 sshd[16354]: Invalid user hadoop from
139.199.166.104 port 40210
Jan  2 20:06:00 ip-172-31-38-110 sshd[16356]: Invalid user mf from 137.116.207.14
port 1464
Jan  2 20:09:52 ip-172-31-38-110 sshd[16436]: Invalid user admin from
14.186.253.189 port 59784
Jan  2 20:10:16 ip-172-31-38-110 sshd[16438]: Invalid user florian from
37.139.9.20 port 59884
Jan  2 20:10:19 ip-172-31-38-110 sshd[16440]: Invalid user florian from
212.156.115.58 port 56558
Jan  2 20:10:20 ip-172-31-38-110 sshd[16442]: Invalid user db2 from
104.236.148.206 port 50296
Jan  2 20:10:27 ip-172-31-38-110 sshd[16446]: Invalid user db2 from 125.63.78.18
port 33038
Jan  2 20:11:10 ip-172-31-38-110 sshd[16448]: Invalid user uno8 from 217.61.97.168
port 47108
Jan  2 20:11:22 ip-172-31-38-110 sshd[16450]: Invalid user sienna from
67.188.137.57 port 38972
Jan  2 20:12:17 ip-172-31-38-110 sshd[16452]: Invalid user surf from 98.143.158.42
port 62442
Jan  2 20:12:33 ip-172-31-38-110 sshd[16454]: Invalid user admin4 from
193.112.7.36 port 42236
Jan  2 20:12:41 ip-172-31-38-110 sshd[16458]: Invalid user desop from
35.240.151.20 port 51264
Jan  2 20:12:44 ip-172-31-38-110 sshd[16460]: Invalid user craig from
132.232.76.213 port 38954
Jan  2 20:15:09 ip-172-31-38-110 sshd[16465]: Invalid user logan from
190.27.135.113 port 36134
Jan  2 20:15:11 ip-172-31-38-110 sshd[16467]: Invalid user cron from
153.232.22.202 port 41584
Jan  2 20:15:16 ip-172-31-38-110 sshd[16469]: Invalid user cron from 178.128.98.86
port 40730
Jan  2 20:22:12 ip-172-31-38-110 sshd[16483]: Invalid user don from 5.51.234.155
port 38866
Jan  2 20:22:24 ip-172-31-38-110 sshd[16485]: Invalid user don from 2.31.102.106
port 57678
Jan  2 20:22:36 ip-172-31-38-110 sshd[16489]: Invalid user vmuser from
223.223.186.114 port 43919
Jan  2 20:22:46 ip-172-31-38-110 sshd[16491]: Invalid user test from
211.159.242.143 port 41664
Jan  2 20:24:24 ip-172-31-38-110 sshd[16497]: Invalid user rails from 51.75.142.40
port 35826
Jan  2 20:24:26 ip-172-31-38-110 sshd[16499]: Invalid user rails from
192.99.145.77 port 53146
```

```
Jan  2 20:24:28 ip-172-31-38-110 sshd[16501]: Invalid user bernd from
148.216.54.69 port 34868
Jan  2 20:24:46 ip-172-31-38-110 sshd[16503]: Invalid user pokemon from
106.12.30.122 port 47737
Jan  2 20:24:47 ip-172-31-38-110 sshd[16505]: Invalid user server from
132.232.2.184 port 45720
Jan  2 20:26:56 ip-172-31-38-110 sshd[16510]: Invalid user hadoop from
91.121.211.34 port 48458
Jan  2 20:27:01 ip-172-31-38-110 sshd[16512]: Invalid user ee from 12.133.183.250
port 15008
Jan  2 20:27:02 ip-172-31-38-110 sshd[16514]: Invalid user hadoop from
40.89.157.49 port 55448
Jan  2 20:27:11 ip-172-31-38-110 sshd[16517]: Invalid user gnuworld from
61.91.126.151 port 32834
Jan  2 20:27:12 ip-172-31-38-110 sshd[16516]: Invalid user gnuworld from
119.92.174.170 port 34608
Jan  2 20:27:53 ip-172-31-38-110 sshd[16521]: Invalid user admin from
50.197.60.170 port 48780
Jan  2 20:37:09 ip-172-31-38-110 sshd[16535]: Invalid user caleb from
107.170.231.130 port 40453
Jan  2 20:37:32 ip-172-31-38-110 sshd[16538]: Invalid user wx from 111.230.225.158
port 59376
Jan  2 20:37:44 ip-172-31-38-110 sshd[16540]: Invalid user lhy from 40.122.70.21
port 50642
Jan  2 20:42:49 ip-172-31-38-110 sshd[16628]: Invalid user ale from 80.11.44.112
port 50398
Jan  2 20:42:49 ip-172-31-38-110 sshd[16626]: Invalid user ale from 51.143.88.126
port 35268
Jan  2 20:42:51 ip-172-31-38-110 sshd[16630]: Invalid user gk from 91.234.241.55
port 57676
Jan  2 20:43:03 ip-172-31-38-110 sshd[16632]: Invalid user teamspeak from
211.170.59.148 port 47714
Jan  2 20:43:05 ip-172-31-38-110 sshd[16634]: Invalid user teamspeak from
123.207.142.31 port 35616
Jan  2 20:44:12 ip-172-31-38-110 sshd[16638]: Invalid user upload from 5.39.3.235
port 59364
Jan  2 20:44:16 ip-172-31-38-110 sshd[16640]: Invalid user upload from
40.115.23.233 port 55114
Jan  2 20:44:18 ip-172-31-38-110 sshd[16642]: Invalid user dspace from
176.111.72.225 port 53699
Jan  2 20:53:16 ip-172-31-38-110 sshd[16648]: Invalid user opc from 43.243.128.213
port 52060
Jan  2 20:53:27 ip-172-31-38-110 sshd[16654]: Invalid user opc from
178.128.219.126 port 40778
Jan  2 20:53:30 ip-172-31-38-110 sshd[16656]: Invalid user dell from
175.145.93.174 port 53074
Jan  2 20:53:31 ip-172-31-38-110 sshd[16658]: Invalid user ecommerce from
132.232.47.139 port 56858
Jan  2 21:03:11 ip-172-31-38-110 sshd[16673]: Invalid user mlh from 186.42.165.11
port 44928
Jan  2 21:04:52 ip-172-31-38-110 sshd[16685]: Invalid user bodega from
133.130.127.188 port 55798
Jan  2 21:07:59 ip-172-31-38-110 sshd[16693]: Invalid user rdp from 95.156.31.74
port 59656
```

```
Jan  2 21:08:02 ip-172-31-38-110 sshd[16695]: Invalid user rdp from 206.81.2.60
port 57888
Jan  2 21:08:05 ip-172-31-38-110 sshd[16697]: Invalid user ftpuser from
175.140.248.94 port 33353
Jan  2 21:08:10 ip-172-31-38-110 sshd[16699]: Invalid user opc from 181.48.71.58
port 48740
Jan  2 21:08:11 ip-172-31-38-110 sshd[16701]: Invalid user ftpuser from
193.112.71.80 port 37242
Jan  2 21:12:58 ip-172-31-38-110 sshd[16785]: Invalid user db_shv from 51.75.29.64
port 51860
Jan  2 21:13:08 ip-172-31-38-110 sshd[16787]: Invalid user daniel from
103.249.100.12 port 33626
Jan  2 21:13:16 ip-172-31-38-110 sshd[16789]: Invalid user chase from
188.131.142.88 port 54928
Jan  2 21:14:16 ip-172-31-38-110 sshd[16796]: Invalid user db_shv from
217.128.200.240 port 53535
Jan  2 21:17:21 ip-172-31-38-110 sshd[16809]: Invalid user pc from 94.25.38.210
port 60970
Jan  2 21:17:23 ip-172-31-38-110 sshd[16811]: Invalid user jira from 120.88.46.226
port 37512
Jan  2 21:17:27 ip-172-31-38-110 sshd[16813]: Invalid user jira from
122.228.253.96 port 43424
Jan  2 21:17:30 ip-172-31-38-110 sshd[16815]: Invalid user jira from 118.25.102.61
port 36300
Jan  2 21:17:37 ip-172-31-38-110 sshd[16817]: Invalid user shashi from
68.183.103.253 port 37912
Jan  2 21:17:39 ip-172-31-38-110 sshd[16819]: Invalid user ez from 182.61.61.185
port 44000
Jan  2 21:18:25 ip-172-31-38-110 sshd[16821]: Invalid user sftpuser from
220.133.198.188 port 37748
Jan  2 21:19:27 ip-172-31-38-110 sshd[16826]: Invalid user mailtest from
209.97.185.16 port 35554
Jan  2 21:19:28 ip-172-31-38-110 sshd[16828]: Invalid user mailtest from
46.105.98.93 port 42112
Jan  2 21:19:32 ip-172-31-38-110 sshd[16830]: Invalid user mailtest from
165.227.171.60 port 50736
Jan  2 21:19:32 ip-172-31-38-110 sshd[16832]: Invalid user mailtest from
142.93.109.33 port 52098
Jan  2 21:19:33 ip-172-31-38-110 sshd[16834]: Invalid user tommy from
167.114.109.167 port 37280
Jan  2 21:19:45 ip-172-31-38-110 sshd[16840]: Invalid user tommy from
61.246.140.80 port 50746
Jan  2 21:19:50 ip-172-31-38-110 sshd[16842]: Invalid user murad from
24.232.114.219 port 43054
Jan  2 21:19:50 ip-172-31-38-110 sshd[16844]: Invalid user rdp from 122.152.199.11
port 36974
Jan  2 21:30:53 ip-172-31-38-110 sshd[16876]: Invalid user musikbot from
190.144.161.11 port 45378
Jan  2 21:34:11 ip-172-31-38-110 sshd[16884]: Invalid user steam from
81.174.227.27 port 49750
Jan  2 21:34:12 ip-172-31-38-110 sshd[16886]: Invalid user steam from
129.173.67.230 port 45024
Jan  2 21:34:16 ip-172-31-38-110 sshd[16888]: Invalid user web_admin from
178.62.61.192 port 42860
```

```
Jan  2 21:34:18 ip-172-31-38-110 sshd[16890]: Invalid user steam from
142.93.31.198 port 60626
Jan  2 21:34:19 ip-172-31-38-110 sshd[16892]: Invalid user aaron from
104.248.188.192 port 59014
Jan  2 21:34:20 ip-172-31-38-110 sshd[16894]: Invalid user steam from
106.51.72.240 port 42878
Jan  2 21:34:26 ip-172-31-38-110 sshd[16896]: Invalid user web_admin from
196.1.99.10 port 50000
Jan  2 21:34:27 ip-172-31-38-110 sshd[16898]: Invalid user steam from
139.59.225.138 port 46536
Jan  2 21:34:29 ip-172-31-38-110 sshd[16900]: Invalid user manager from
159.65.135.64 port 55980
Jan  2 21:34:31 ip-172-31-38-110 sshd[16902]: Invalid user web_admin from
35.200.239.160 port 36876
Jan  2 21:35:03 ip-172-31-38-110 sshd[16906]: Invalid user finance from
216.126.239.70 port 58822
Jan  2 21:35:25 ip-172-31-38-110 sshd[16909]: Invalid user luan from 94.191.81.131
port 43502
Jan  2 21:35:39 ip-172-31-38-110 sshd[16911]: Invalid user test from 5.39.3.235
port 50674
Jan  2 21:50:07 ip-172-31-38-110 sshd[17005]: Invalid user lazaro from
178.128.37.180 port 54352
Jan  2 21:50:08 ip-172-31-38-110 sshd[17007]: Invalid user hbase from
137.116.126.169 port 50674
Jan  2 21:50:08 ip-172-31-38-110 sshd[17009]: Invalid user lazaro from
54.38.181.69 port 44262
Jan  2 21:50:14 ip-172-31-38-110 sshd[17011]: Invalid user hbase from
139.59.132.28 port 53178
Jan  2 21:50:21 ip-172-31-38-110 sshd[17013]: Invalid user user from
190.210.223.247 port 52756
Jan  2 21:50:22 ip-172-31-38-110 sshd[17015]: Invalid user nagios from
107.170.11.31 port 58794
Jan  2 21:50:23 ip-172-31-38-110 sshd[17017]: Invalid user default from
172.247.194.58 port 52738
Jan  2 21:50:52 ip-172-31-38-110 sshd[17021]: Invalid user bart from
117.156.119.39 port 40432
Jan  2 21:52:38 ip-172-31-38-110 sshd[17026]: Invalid user forrest from
136.61.99.34 port 43846
Jan  2 21:52:41 ip-172-31-38-110 sshd[17028]: Invalid user forrest from
190.217.17.52 port 56257
Jan  2 21:52:43 ip-172-31-38-110 sshd[17030]: Invalid user avahi from
77.158.223.83 port 51644
Jan  2 21:52:43 ip-172-31-38-110 sshd[17032]: Invalid user csserver from
46.101.35.132 port 57194
Jan  2 21:52:44 ip-172-31-38-110 sshd[17034]: Invalid user avahi from
178.62.60.225 port 59036
Jan  2 21:52:46 ip-172-31-38-110 sshd[17036]: Invalid user avahi from
213.108.216.19 port 59978
Jan  2 21:52:47 ip-172-31-38-110 sshd[17038]: Invalid user csserver from
80.211.99.165 port 35458
Jan  2 21:52:48 ip-172-31-38-110 sshd[17040]: Invalid user csserver from
178.20.159.232 port 52242
Jan  2 21:52:50 ip-172-31-38-110 sshd[17042]: Invalid user avahi from
173.249.31.76 port 40756
```

```
Jan  2 21:52:55 ip-172-31-38-110 sshd[17044]: Invalid user deb from 222.255.46.225
port 54078
Jan  2 21:52:57 ip-172-31-38-110 sshd[17046]: Invalid user avahi from
178.128.55.52 port 49036
Jan  2 21:52:58 ip-172-31-38-110 sshd[17048]: Invalid user bgr from 132.232.76.213
port 56078
Jan  2 21:53:00 ip-172-31-38-110 sshd[17050]: Invalid user oracle from
154.8.167.48 port 49002
Jan  2 21:55:45 ip-172-31-38-110 sshd[17052]: Invalid user qhsupport from
165.227.25.195 port 57452
Jan  2 21:55:46 ip-172-31-38-110 sshd[17054]: Invalid user daniel from
105.235.201.251 port 44934
Jan  2 21:55:51 ip-172-31-38-110 sshd[17056]: Invalid user daniel from
128.199.106.169 port 34380
Jan  2 21:55:53 ip-172-31-38-110 sshd[17058]: Invalid user weixinapp from
211.21.129.4 port 54154
Jan  2 21:56:01 ip-172-31-38-110 sshd[17060]: Invalid user vagrant from
106.12.88.182 port 60444
Jan  2 21:56:16 ip-172-31-38-110 sshd[17062]: Invalid user daniel from
177.183.75.23 port 54337
Jan  2 21:57:54 ip-172-31-38-110 sshd[17065]: Invalid user db2fenc1 from
198.46.182.139 port 52636
Jan  2 21:58:00 ip-172-31-38-110 sshd[17067]: Invalid user db2fenc1 from
80.211.38.77 port 35190
Jan  2 21:58:02 ip-172-31-38-110 sshd[17069]: Invalid user wk from 79.172.212.243
port 49686
Jan  2 21:58:03 ip-172-31-38-110 sshd[17071]: Invalid user db2fenc1 from
105.235.201.251 port 57216
Jan  2 21:58:16 ip-172-31-38-110 sshd[17075]: Invalid user lukasz from
196.25.239.10 port 56154
Jan  2 22:07:50 ip-172-31-38-110 sshd[17090]: Invalid user biology from
78.193.8.166 port 48008
Jan  2 22:07:51 ip-172-31-38-110 sshd[17092]: Invalid user biology from
159.65.183.47 port 39212
Jan  2 22:08:11 ip-172-31-38-110 sshd[17094]: Invalid user admin1 from 155.0.32.9
port 50162
Jan  2 22:10:40 ip-172-31-38-110 sshd[17172]: Invalid user antonio from
219.117.238.181 port 54624
Jan  2 22:16:45 ip-172-31-38-110 sshd[17175]: Invalid user chef from
49.248.167.102 port 49842
Jan  2 22:18:21 ip-172-31-38-110 sshd[17182]: Invalid user sftp from 188.68.55.246
port 46538
Jan  2 22:25:10 ip-172-31-38-110 sshd[17187]: Invalid user arthur from
91.134.140.32 port 38084
Jan  2 22:28:29 ip-172-31-38-110 sshd[17192]: Invalid user fengjian from
43.225.117.245 port 55250
Jan  2 22:39:50 ip-172-31-38-110 sshd[17276]: Invalid user yq from 104.248.46.187
port 34546
Jan  2 22:40:16 ip-172-31-38-110 sshd[17278]: Invalid user omega from
178.128.221.237 port 46788
Jan  2 22:48:45 ip-172-31-38-110 sshd[17285]: Invalid user SuperUser from
116.212.237.226 port 38070
Jan  2 22:52:01 ip-172-31-38-110 sshd[17330]: Invalid user clamav1 from
159.89.13.0 port 44656
```

```
Jan  2 22:53:29 ip-172-31-38-110 sshd[17332]: Invalid user demo from
178.62.210.221 port 34206
Jan  2 22:53:53 ip-172-31-38-110 sshd[17337]: Invalid user usuario from
1.190.188.43 port 54964
Jan  2 22:53:56 ip-172-31-38-110 sshd[17339]: Invalid user gaurav from
111.198.66.172 port 52924
Jan  2 22:54:10 ip-172-31-38-110 sshd[17341]: Invalid user usuario from
202.126.46.39 port 50857
Jan  2 22:59:08 ip-172-31-38-110 sshd[17347]: Invalid user rds from 104.236.214.8
port 55663
Jan  2 23:00:51 ip-172-31-38-110 sshd[17349]: Invalid user louis from
188.166.243.150 port 50072
Jan  2 23:03:26 ip-172-31-38-110 sshd[17352]: Invalid user antonio from
108.235.160.215 port 34684
Jan  2 23:03:34 ip-172-31-38-110 sshd[17354]: Invalid user antonio from
183.61.126.200 port 49018
Jan  2 23:03:36 ip-172-31-38-110 sshd[17356]: Invalid user vmware from
71.90.181.64 port 58774
Jan  2 23:03:42 ip-172-31-38-110 sshd[17358]: Invalid user vmware from
188.131.142.88 port 58292
Jan  2 23:11:34 ip-172-31-38-110 sshd[17439]: Invalid user klaus from
54.39.144.129 port 32936
Jan  2 23:11:40 ip-172-31-38-110 sshd[17441]: Invalid user control from
182.23.104.211 port 43594
Jan  2 23:11:48 ip-172-31-38-110 sshd[17443]: Invalid user activemq from
183.61.126.200 port 43110
Jan  2 23:11:53 ip-172-31-38-110 sshd[17445]: Invalid user activemq from
183.61.126.200 port 44548
Jan  2 23:13:23 ip-172-31-38-110 sshd[17447]: Invalid user pt from 145.239.6.160
port 47654
Jan  2 23:13:30 ip-172-31-38-110 sshd[17449]: Invalid user arod from
159.203.175.144 port 36748
Jan  2 23:13:31 ip-172-31-38-110 sshd[17451]: Invalid user pt from 51.15.173.30
port 34402
Jan  2 23:13:38 ip-172-31-38-110 sshd[17453]: Invalid user frappe from
204.197.182.51 port 23810
Jan  2 23:13:40 ip-172-31-38-110 sshd[17455]: Invalid user arod from 117.66.243.77
port 57230
Jan  2 23:13:41 ip-172-31-38-110 sshd[17458]: Invalid user arod from 142.93.210.90
port 51832
Jan  2 23:13:42 ip-172-31-38-110 sshd[17457]: Invalid user frappe from
103.27.200.205 port 43582
Jan  2 23:17:00 ip-172-31-38-110 sshd[17464]: Invalid user gio from 5.135.162.113
port 38226
Jan  2 23:17:08 ip-172-31-38-110 sshd[17469]: Invalid user xu from 125.134.251.45
port 41872
Jan  2 23:17:31 ip-172-31-38-110 sshd[17471]: Invalid user admin from
111.230.225.158 port 52046
Jan  2 23:17:48 ip-172-31-38-110 sshd[17473]: Invalid user testuser from
147.135.134.53 port 52223
Jan  2 23:17:48 ip-172-31-38-110 sshd[17475]: Invalid user et from 82.165.64.64
port 35822
Jan  2 23:18:03 ip-172-31-38-110 sshd[17477]: Invalid user pg from 119.29.251.152
port 56908
```

```
Jan  2 23:22:02 ip-172-31-38-110 sshd[17482]: Invalid user devuser from
35.204.13.102 port 44020
Jan  2 23:22:18 ip-172-31-38-110 sshd[17484]: Invalid user bsd02 from 154.8.214.14
port 50092
Jan  2 23:26:04 ip-172-31-38-110 sshd[17487]: Invalid user info from 91.234.241.55
port 37152
Jan  2 23:26:08 ip-172-31-38-110 sshd[17489]: Invalid user slut from 168.62.59.195
port 37548
Jan  2 23:26:16 ip-172-31-38-110 sshd[17491]: Invalid user pankaj from
106.51.39.163 port 49592
Jan  2 23:30:00 ip-172-31-38-110 sshd[17495]: Invalid user daniel from
178.62.252.89 port 48766
Jan  2 23:30:03 ip-172-31-38-110 sshd[17497]: Invalid user daniel from
159.89.139.228 port 41082
Jan  2 23:38:03 ip-172-31-38-110 sshd[17583]: Invalid user ejabberd from
129.213.88.199 port 52304
Jan  2 23:38:14 ip-172-31-38-110 sshd[17585]: Invalid user qbtuser from
104.209.158.39 port 51578
Jan  2 23:38:21 ip-172-31-38-110 sshd[17587]: Invalid user money from
222.255.46.225 port 35732
Jan  2 23:38:28 ip-172-31-38-110 sshd[17589]: Invalid user ejabberd from
211.159.176.185 port 58912
Jan  2 23:38:29 ip-172-31-38-110 sshd[17591]: Invalid user foo from 106.12.88.182
port 47352
Jan  2 23:38:45 ip-172-31-38-110 sshd[17593]: Invalid user super from
106.12.24.108 port 41608
Jan  2 23:53:56 ip-172-31-38-110 sshd[17676]: Invalid user orange from
206.189.239.156 port 35398
Jan  2 23:53:57 ip-172-31-38-110 sshd[17678]: Invalid user orange from
178.128.201.224 port 53248
Jan  2 23:54:00 ip-172-31-38-110 sshd[17680]: Invalid user orange from
80.211.240.158 port 44966
Jan  2 23:54:06 ip-172-31-38-110 sshd[17684]: Invalid user orange from
94.233.30.122 port 47776
Jan  2 23:58:47 ip-172-31-38-110 sshd[17688]: Invalid user sebastian from
106.37.75.74 port 60696
Jan  2 23:58:47 ip-172-31-38-110 sshd[17689]: Invalid user sebastian from
106.37.75.74 port 60722
Jan  3 00:00:34 ip-172-31-38-110 sshd[17696]: Invalid user william from
104.248.117.234 port 34504
Jan  3 00:00:37 ip-172-31-38-110 sshd[17698]: Invalid user william from
54.38.55.182 port 48472
Jan  3 00:00:45 ip-172-31-38-110 sshd[17700]: Invalid user pgsql from
177.53.223.30 port 38590
Jan  3 00:00:47 ip-172-31-38-110 sshd[17702]: Invalid user tina from
113.108.79.182 port 58930
Jan  3 00:00:49 ip-172-31-38-110 sshd[17704]: Invalid user server from
50.192.195.225 port 46259
Jan  3 00:01:05 ip-172-31-38-110 sshd[17706]: Invalid user deploy from
124.131.8.170 port 60160
Jan  3 00:08:37 ip-172-31-38-110 sshd[17714]: Invalid user testxp from
94.23.204.136 port 50310
Jan  3 00:08:40 ip-172-31-38-110 sshd[17716]: Invalid user sammy from
178.128.71.114 port 58112
```

```
Jan  3 00:08:46 ip-172-31-38-110 sshd[17718]: Invalid user sammy from 41.138.88.3
port 48617
Jan  3 00:08:50 ip-172-31-38-110 sshd[17720]: Invalid user sammy from
35.221.234.66 port 55054
Jan  3 00:15:52 ip-172-31-38-110 sshd[17803]: Invalid user vh from 104.248.17.137
port 57324
Jan  3 00:15:52 ip-172-31-38-110 sshd[17801]: Invalid user james from
159.89.115.126 port 43418
Jan  3 00:15:55 ip-172-31-38-110 sshd[17805]: Invalid user foo from 159.65.103.189
port 39510
Jan  3 00:15:55 ip-172-31-38-110 sshd[17807]: Invalid user foo from 187.217.199.20
port 48414
Jan  3 00:15:59 ip-172-31-38-110 sshd[17809]: Invalid user james from
27.109.19.158 port 35854
Jan  3 00:16:06 ip-172-31-38-110 sshd[17813]: Invalid user user5 from
104.248.158.83 port 35958
Jan  3 00:17:13 ip-172-31-38-110 sshd[17820]: Invalid user prakash from
104.248.55.166 port 38364
Jan  3 00:17:37 ip-172-31-38-110 sshd[17822]: Invalid user gabriel from
177.131.27.26 port 45427
Jan  3 00:17:52 ip-172-31-38-110 sshd[17824]: Invalid user bob from 102.164.60.160
port 44126
Jan  3 00:18:05 ip-172-31-38-110 sshd[17826]: Invalid user viktor from
181.215.89.98 port 41828
Jan  3 00:18:22 ip-172-31-38-110 sshd[17828]: Invalid user web_admin from
14.29.157.19 port 54570
Jan  3 00:23:31 ip-172-31-38-110 sshd[17832]: Invalid user alvin from
51.68.198.119 port 37190
Jan  3 00:23:42 ip-172-31-38-110 sshd[17834]: Invalid user nexus from
128.199.145.242 port 60155
Jan  3 00:23:55 ip-172-31-38-110 sshd[17836]: Invalid user celery from
118.24.31.37 port 50916
Jan  3 00:32:15 ip-172-31-38-110 sshd[17849]: Invalid user mongouser from
199.192.27.143 port 40196
Jan  3 00:32:15 ip-172-31-38-110 sshd[17851]: Invalid user mongouser from
212.114.63.44 port 53004
Jan  3 00:32:16 ip-172-31-38-110 sshd[17853]: Invalid user test from
186.151.197.178 port 45509
Jan  3 00:32:18 ip-172-31-38-110 sshd[17855]: Invalid user mongouser from
77.199.87.64 port 38596
Jan  3 00:32:24 ip-172-31-38-110 sshd[17857]: Invalid user test from
78.231.186.151 port 40803
Jan  3 00:32:29 ip-172-31-38-110 sshd[17859]: Invalid user mongouser from
188.131.207.158 port 35028
Jan  3 00:33:44 ip-172-31-38-110 sshd[17862]: Invalid user svt from 27.254.208.35
port 50140
Jan  3 00:33:44 ip-172-31-38-110 sshd[17864]: Invalid user svt from 118.24.19.185
port 37078
Jan  3 00:34:28 ip-172-31-38-110 sshd[17866]: Invalid user zabbix from
159.65.7.200 port 47946
Jan  3 00:34:31 ip-172-31-38-110 sshd[17868]: Invalid user eagle from 92.222.75.72
port 47154
Jan  3 00:34:32 ip-172-31-38-110 sshd[17870]: Invalid user john from
201.163.111.42 port 59410
```

```
Jan  3 00:34:40 ip-172-31-38-110 sshd[17872]: Invalid user zabbix from
14.41.77.225 port 37518
Jan  3 00:34:40 ip-172-31-38-110 sshd[17874]: Invalid user halt from
139.199.166.104 port 40014
Jan  3 00:35:20 ip-172-31-38-110 sshd[17876]: Invalid user deploy from
206.189.219.253 port 53624
Jan  3 00:35:21 ip-172-31-38-110 sshd[17878]: Invalid user odoo from 93.43.119.9
port 37688
Jan  3 00:35:22 ip-172-31-38-110 sshd[17880]: Invalid user odoo from 54.37.232.108
port 34514
Jan  3 00:35:30 ip-172-31-38-110 sshd[17882]: Invalid user deploy from
139.99.40.27 port 55956
Jan  3 00:35:35 ip-172-31-38-110 sshd[17884]: Invalid user ethos from
139.199.221.21 port 58388
Jan  3 00:35:40 ip-172-31-38-110 sshd[17886]: Invalid user deploy from
200.196.240.60 port 43022
Jan  3 00:37:09 ip-172-31-38-110 sshd[17888]: Invalid user databse from
212.237.33.240 port 39350
Jan  3 00:56:28 ip-172-31-38-110 sshd[17972]: Invalid user design from
145.239.6.160 port 56424
Jan  3 00:56:30 ip-172-31-38-110 sshd[17974]: Invalid user share from
195.22.141.33 port 43740
Jan  3 00:56:30 ip-172-31-38-110 sshd[17976]: Invalid user share from
129.144.3.230 port 51382
Jan  3 00:56:34 ip-172-31-38-110 sshd[17978]: Invalid user design from
50.226.108.234 port 35658
Jan  3 00:56:38 ip-172-31-38-110 sshd[17980]: Invalid user share from
110.36.181.44 port 51294
Jan  3 00:56:49 ip-172-31-38-110 sshd[17982]: Invalid user apache2 from
182.61.31.103 port 53328
Jan  3 00:56:51 ip-172-31-38-110 sshd[17984]: Invalid user design from
94.191.81.131 port 48402
Jan  3 00:57:09 ip-172-31-38-110 sshd[17986]: Invalid user share from 89.165.3.46
port 41187
Jan  3 00:59:12 ip-172-31-38-110 sshd[17994]: Invalid user test101 from
104.248.254.51 port 49276
Jan  3 00:59:19 ip-172-31-38-110 sshd[17996]: Invalid user aoyule from
183.82.121.65 port 34346
Jan  3 01:06:00 ip-172-31-38-110 sshd[18000]: Invalid user dice from 83.14.199.51
port 38466
Jan  3 01:06:03 ip-172-31-38-110 sshd[18002]: Invalid user italy from
159.89.174.228 port 45410
Jan  3 01:06:04 ip-172-31-38-110 sshd[18003]: Invalid user italy from 49.206.30.37
port 48260
Jan  3 01:06:04 ip-172-31-38-110 sshd[18005]: Invalid user italy from
220.128.119.251 port 46912
Jan  3 01:07:17 ip-172-31-38-110 sshd[18008]: Invalid user iQ from 45.55.35.40
port 42004
Jan  3 01:07:18 ip-172-31-38-110 sshd[18010]: Invalid user iQ from 151.106.28.235
port 44722
Jan  3 01:07:37 ip-172-31-38-110 sshd[18012]: Invalid user giter from
27.254.206.238 port 59084
Jan  3 01:09:03 ip-172-31-38-110 sshd[18089]: Invalid user named from
123.136.161.146 port 37868
```

```
Jan  3 01:09:15 ip-172-31-38-110 sshd[18091]: Invalid user named from
132.232.112.25 port 51214
Jan  3 01:16:05 ip-172-31-38-110 sshd[18094]: Invalid user zhou from
189.206.130.170 port 42894
Jan  3 01:18:32 ip-172-31-38-110 sshd[18100]: Invalid user matilda from
84.254.0.120 port 39770
Jan  3 01:22:27 ip-172-31-38-110 sshd[18111]: Invalid user wwwroot from
150.109.196.143 port 58744
Jan  3 01:24:11 ip-172-31-38-110 sshd[18114]: Invalid user ckobia from
187.19.49.74 port 44968
Jan  3 01:30:24 ip-172-31-38-110 sshd[18120]: Invalid user connor from 80.67.252.7
port 44944
Jan  3 01:30:26 ip-172-31-38-110 sshd[18122]: Invalid user connor from
40.114.25.203 port 40560
Jan  3 01:30:27 ip-172-31-38-110 sshd[18124]: Invalid user admin from
5.196.137.213 port 45337
Jan  3 01:30:27 ip-172-31-38-110 sshd[18126]: Invalid user connor from
51.77.148.203 port 42220
Jan  3 01:30:30 ip-172-31-38-110 sshd[18128]: Invalid user connor from
52.246.254.177 port 47624
Jan  3 01:30:34 ip-172-31-38-110 sshd[18130]: Invalid user uj from 119.29.197.54
port 45854
Jan  3 01:30:41 ip-172-31-38-110 sshd[18132]: Invalid user connor from
119.94.176.235 port 52346
Jan  3 01:33:55 ip-172-31-38-110 sshd[18135]: Invalid user antoine from
123.206.37.155 port 45988
Jan  3 01:36:48 ip-172-31-38-110 sshd[18138]: Invalid user myftp from
158.69.121.144 port 47436
Jan  3 01:36:49 ip-172-31-38-110 sshd[18140]: Invalid user ts3bot from 80.13.46.54
port 50470
Jan  3 01:36:51 ip-172-31-38-110 sshd[18142]: Invalid user myftp from
167.99.84.229 port 56152
Jan  3 01:36:52 ip-172-31-38-110 sshd[18144]: Invalid user ts3bot from
40.114.25.203 port 46164
Jan  3 01:36:57 ip-172-31-38-110 sshd[18146]: Invalid user myftp from
159.89.139.228 port 43004
Jan  3 01:37:03 ip-172-31-38-110 sshd[18150]: Invalid user bernard from
209.97.161.46 port 58236
Jan  3 01:37:03 ip-172-31-38-110 sshd[18148]: Invalid user ts3bot from 5.196.75.47
port 32920
Jan  3 01:37:07 ip-172-31-38-110 sshd[18152]: Invalid user bernard from
134.175.103.114 port 60426
Jan  3 01:42:31 ip-172-31-38-110 sshd[18234]: Invalid user foo from 186.84.172.25
port 41900
Jan  3 01:42:34 ip-172-31-38-110 sshd[18236]: Invalid user train5 from
120.197.130.114 port 57948
Jan  3 01:42:41 ip-172-31-38-110 sshd[18238]: Invalid user starbound from
222.122.202.176 port 39892
Jan  3 01:42:42 ip-172-31-38-110 sshd[18240]: Invalid user train5 from
58.210.96.156 port 45238
Jan  3 01:42:55 ip-172-31-38-110 sshd[18242]: Invalid user foo from 35.210.1.76
port 56954
Jan  3 01:43:06 ip-172-31-38-110 sshd[18244]: Invalid user foo from 179.234.96.93
port 33446
```

```
Jan  3 01:45:17 ip-172-31-38-110 sshd[18247]: Invalid user protocol from
216.169.152.133 port 46031
Jan  3 01:49:52 ip-172-31-38-110 sshd[18253]: Invalid user amy from 27.122.250.248
port 50729
Jan  3 01:52:58 ip-172-31-38-110 sshd[18261]: Invalid user train5 from
51.75.122.16 port 35734
Jan  3 01:53:33 ip-172-31-38-110 sshd[18264]: Invalid user maundy from
89.218.14.61 port 55732
Jan  3 01:55:22 ip-172-31-38-110 sshd[18266]: Invalid user cx sdk from
77.40.127.254 port 42010
Jan  3 01:56:54 ip-172-31-38-110 sshd[18268]: Invalid user cpanel from
189.155.206.113 port 39826
Jan  3 02:08:15 ip-172-31-38-110 sshd[18275]: Invalid user public from 51.75.29.64
port 35574
Jan  3 02:08:16 ip-172-31-38-110 sshd[18277]: Invalid user public from
51.77.148.203 port 40084
Jan  3 02:08:25 ip-172-31-38-110 sshd[18281]: Invalid user nexus from
188.166.228.28 port 38664
Jan  3 02:08:27 ip-172-31-38-110 sshd[18283]: Invalid user admin from
217.128.2.139 port 60246
Jan  3 02:08:41 ip-172-31-38-110 sshd[18285]: Invalid user vlad from
106.12.216.170 port 51344
Jan  3 02:08:51 ip-172-31-38-110 sshd[18288]: Invalid user public from
187.146.157.52 port 58641
Jan  3 02:09:31 ip-172-31-38-110 sshd[18364]: Invalid user staffc from
139.159.3.218 port 63437
Jan  3 02:09:37 ip-172-31-38-110 sshd[18366]: Invalid user codeunbug from
134.175.103.114 port 35926
Jan  3 02:10:38 ip-172-31-38-110 sshd[18368]: Invalid user tamaki from 71.198.1.69
port 40418
Jan  3 02:10:45 ip-172-31-38-110 sshd[18370]: Invalid user raja from 1.179.185.50
port 40336
Jan  3 02:10:58 ip-172-31-38-110 sshd[18372]: Invalid user tamaki from
118.24.19.185 port 51404
Jan  3 02:18:21 ip-172-31-38-110 sshd[18381]: Invalid user mitchell from
167.114.109.167 port 38474
Jan  3 02:25:16 ip-172-31-38-110 sshd[18384]: Invalid user personal from
13.67.34.145 port 56176
Jan  3 02:25:24 ip-172-31-38-110 sshd[18386]: Invalid user stefan from
193.112.27.92 port 40180
Jan  3 02:25:26 ip-172-31-38-110 sshd[18388]: Invalid user simone from 103.28.2.60
port 45162
Jan  3 02:33:10 ip-172-31-38-110 sshd[18396]: Invalid user guest from
35.236.15.241 port 48616
Jan  3 02:37:07 ip-172-31-38-110 sshd[18399]: Invalid user sienna from
104.238.92.100 port 50216
Jan  3 02:37:08 ip-172-31-38-110 sshd[18401]: Invalid user ej from 178.128.242.233
port 44254
Jan  3 02:37:09 ip-172-31-38-110 sshd[18403]: Invalid user ej from 142.93.109.33
port 57756
Jan  3 02:37:11 ip-172-31-38-110 sshd[18405]: Invalid user sienna from
216.126.238.100 port 59740
Jan  3 02:37:12 ip-172-31-38-110 sshd[18407]: Invalid user sienna from
159.89.139.228 port 48828
```

```
Jan  3 02:37:12 ip-172-31-38-110 sshd[18409]: Invalid user ej from 134.0.106.152
port 57254
Jan  3 02:37:27 ip-172-31-38-110 sshd[18411]: Invalid user camera from
62.234.136.76 port 48186
Jan  3 02:42:41 ip-172-31-38-110 sshd[18490]: Invalid user beau from 1.234.79.66
port 59509
Jan  3 02:49:17 ip-172-31-38-110 sshd[18499]: Invalid user kumar from 46.105.98.93
port 36518
Jan  3 02:49:17 ip-172-31-38-110 sshd[18497]: Invalid user postgres from
192.99.212.244 port 58170
Jan  3 02:49:25 ip-172-31-38-110 sshd[18501]: Invalid user yw from 112.175.106.53
port 57798
Jan  3 02:52:49 ip-172-31-38-110 sshd[18503]: Invalid user test from
194.182.76.190 port 46772
Jan  3 02:52:52 ip-172-31-38-110 sshd[18505]: Invalid user software from
104.248.121.89 port 45290
Jan  3 02:52:53 ip-172-31-38-110 sshd[18507]: Invalid user software from
159.203.185.59 port 52176
Jan  3 02:52:53 ip-172-31-38-110 sshd[18511]: Invalid user test from 54.37.68.191
port 52646
Jan  3 02:52:53 ip-172-31-38-110 sshd[18509]: Invalid user software from
35.239.133.223 port 44206
Jan  3 02:52:57 ip-172-31-38-110 sshd[18513]: Invalid user houx from 118.24.31.37
port 57436
Jan  3 02:53:06 ip-172-31-38-110 sshd[18515]: Invalid user software from
177.137.205.150 port 48200
Jan  3 02:53:07 ip-172-31-38-110 sshd[18517]: Invalid user postmaster from
150.161.8.120 port 47640
Jan  3 02:57:43 ip-172-31-38-110 sshd[18522]: Invalid user is from 67.188.137.57
port 40202
Jan  3 02:57:44 ip-172-31-38-110 sshd[18524]: Invalid user admin from
134.175.12.105 port 41236
Jan  3 02:57:46 ip-172-31-38-110 sshd[18526]: Invalid user admin from
120.197.130.114 port 42972
Jan  3 02:57:53 ip-172-31-38-110 sshd[18528]: Invalid user is from 106.12.216.170
port 51652
Jan  3 02:59:35 ip-172-31-38-110 sshd[18531]: Invalid user test from 178.62.214.85
port 59782
Jan  3 02:59:47 ip-172-31-38-110 sshd[18533]: Invalid user devserver from
113.193.127.138 port 49978
Jan  3 03:01:34 ip-172-31-38-110 sshd[18539]: Invalid user pub from 163.13.112.220
port 40178
Jan  3 03:01:43 ip-172-31-38-110 sshd[18541]: Invalid user pub from
132.232.230.211 port 39020
Jan  3 03:05:01 ip-172-31-38-110 sshd[18544]: Invalid user cos from 91.217.34.129
port 33932
Jan  3 03:05:06 ip-172-31-38-110 sshd[18546]: Invalid user student from
222.124.12.57 port 29301
Jan  3 03:05:20 ip-172-31-38-110 sshd[18548]: Invalid user wcc from 106.51.76.165
port 46722
Jan  3 03:05:37 ip-172-31-38-110 sshd[18551]: Invalid user pppp from
123.207.239.90 port 46856
Jan  3 03:06:01 ip-172-31-38-110 sshd[18553]: Invalid user student from
41.21.195.197 port 47211
```

```
Jan  3 03:09:58 ip-172-31-38-110 sshd[18630]: Invalid user celery from
40.67.196.191 port 56666
Jan  3 03:11:11 ip-172-31-38-110 sshd[18633]: Invalid user oravis from
212.10.74.113 port 58040
Jan  3 03:11:15 ip-172-31-38-110 sshd[18635]: Invalid user oravis from
92.222.70.130 port 40900
Jan  3 03:11:15 ip-172-31-38-110 sshd[18637]: Invalid user weblogic from
82.165.64.64 port 58438
Jan  3 03:11:16 ip-172-31-38-110 sshd[18639]: Invalid user guest from
68.183.21.151 port 49470
Jan  3 03:11:18 ip-172-31-38-110 sshd[18641]: Invalid user weblogic from
202.131.227.60 port 53072
Jan  3 03:11:23 ip-172-31-38-110 sshd[18643]: Invalid user myftp from
80.211.99.165 port 46018
Jan  3 03:11:23 ip-172-31-38-110 sshd[18644]: Invalid user lhy from 68.183.62.109
port 39394
Jan  3 03:11:26 ip-172-31-38-110 sshd[18647]: Invalid user weblogic from
103.94.121.242 port 36144
Jan  3 03:11:37 ip-172-31-38-110 sshd[18649]: Invalid user ts3server1 from
159.65.5.209 port 37096
Jan  3 03:14:15 ip-172-31-38-110 sshd[18653]: Invalid user vyatta from 46.97.5.249
port 34464
Jan  3 03:14:18 ip-172-31-38-110 sshd[18655]: Invalid user user2 from
222.110.45.23 port 35330
Jan  3 03:14:38 ip-172-31-38-110 sshd[18657]: Invalid user debian from
132.232.112.25 port 35512
Jan  3 03:14:42 ip-172-31-38-110 sshd[18659]: Invalid user test2 from
119.29.251.152 port 46068
Jan  3 03:20:02 ip-172-31-38-110 sshd[18665]: Invalid user taiga from
79.137.76.126 port 41725
Jan  3 03:20:15 ip-172-31-38-110 sshd[18667]: Invalid user facturacion from
140.143.164.213 port 42492
Jan  3 03:22:12 ip-172-31-38-110 sshd[18670]: Invalid user test from
107.170.95.116 port 45337
Jan  3 03:22:25 ip-172-31-38-110 sshd[18672]: Invalid user logger from
134.175.8.27 port 38604
Jan  3 03:22:47 ip-172-31-38-110 sshd[18674]: Invalid user share from 80.13.46.54
port 55344
Jan  3 03:22:52 ip-172-31-38-110 sshd[18676]: Invalid user share from 80.6.162.204
port 50340
Jan  3 03:22:58 ip-172-31-38-110 sshd[18680]: Invalid user elastic from
92.42.46.219 port 48962
Jan  3 03:22:58 ip-172-31-38-110 sshd[18678]: Invalid user pc from 203.229.196.132
port 34787
Jan  3 03:23:58 ip-172-31-38-110 sshd[18682]: Invalid user odoo from
104.248.158.83 port 52748
Jan  3 03:23:59 ip-172-31-38-110 sshd[18684]: Invalid user michelle from
122.228.253.95 port 43131
Jan  3 03:24:38 ip-172-31-38-110 sshd[18686]: Invalid user iQ from 123.206.16.61
port 40628
Jan  3 03:26:32 ip-172-31-38-110 sshd[18688]: Invalid user server from
36.67.135.42 port 55813
Jan  3 03:26:41 ip-172-31-38-110 sshd[18690]: Invalid user appuser from
106.12.125.27 port 39858
```

```
Jan  3 03:27:01 ip-172-31-38-110 sshd[18692]: Invalid user fahmed from
134.175.103.114 port 53772
Jan  3 03:27:01 ip-172-31-38-110 sshd[18694]: Invalid user lenin from
165.227.150.158 port 16745
Jan  3 03:27:05 ip-172-31-38-110 sshd[18696]: Invalid user ts3 from
104.248.182.124 port 59352
Jan  3 03:27:06 ip-172-31-38-110 sshd[18698]: Invalid user lenin from
82.27.152.254 port 47772
Jan  3 03:31:31 ip-172-31-38-110 sshd[18706]: Invalid user admin1 from
178.128.97.110 port 44448
Jan  3 03:31:34 ip-172-31-38-110 sshd[18710]: Invalid user info from 94.184.89.134
port 58406
Jan  3 03:31:34 ip-172-31-38-110 sshd[18708]: Invalid user mailadmin from
52.83.110.58 port 47154
Jan  3 03:33:20 ip-172-31-38-110 sshd[18712]: Invalid user rack from 103.21.176.33
port 35948
Jan  3 03:33:44 ip-172-31-38-110 sshd[18715]: Invalid user salman from
81.174.227.27 port 46994
Jan  3 03:33:49 ip-172-31-38-110 sshd[18717]: Invalid user salman from
85.238.104.197 port 46134
Jan  3 03:36:57 ip-172-31-38-110 sshd[18719]: Invalid user julien from
89.3.236.207 port 46768
Jan  3 03:37:08 ip-172-31-38-110 sshd[18721]: Invalid user julien from
79.109.239.49 port 44726
Jan  3 03:40:59 ip-172-31-38-110 sshd[18801]: Invalid user aris from 159.65.183.47
port 43866
Jan  3 03:41:06 ip-172-31-38-110 sshd[18803]: Invalid user webadmin from
35.198.233.210 port 34380
Jan  3 03:41:31 ip-172-31-38-110 sshd[18805]: Invalid user teamspeak3 from
159.203.179.230 port 45534
Jan  3 03:42:59 ip-172-31-38-110 sshd[18809]: Invalid user postgres from
129.213.147.93 port 57022
Jan  3 03:43:00 ip-172-31-38-110 sshd[18811]: Invalid user selena from
142.93.160.229 port 58712
Jan  3 03:43:03 ip-172-31-38-110 sshd[18813]: Invalid user admin from
181.143.146.42 port 38854
Jan  3 03:43:06 ip-172-31-38-110 sshd[18815]: Invalid user admin from
115.112.176.202 port 59980
Jan  3 03:43:06 ip-172-31-38-110 sshd[18817]: Invalid user admin from
105.235.193.251 port 46204
Jan  3 03:43:07 ip-172-31-38-110 sshd[18819]: Invalid user test from 67.198.104.73
port 40310
Jan  3 03:43:07 ip-172-31-38-110 sshd[18823]: Invalid user selena from
164.132.107.245 port 40598
Jan  3 03:43:07 ip-172-31-38-110 sshd[18821]: Invalid user test from
137.135.73.152 port 59400
Jan  3 03:43:10 ip-172-31-38-110 sshd[18825]: Invalid user aoyule from
142.93.87.125 port 53966
Jan  3 03:43:11 ip-172-31-38-110 sshd[18827]: Invalid user aoyule from
150.95.153.7 port 53458
Jan  3 03:43:16 ip-172-31-38-110 sshd[18829]: Invalid user aoyule from
170.84.208.251 port 57008
Jan  3 03:45:27 ip-172-31-38-110 sshd[18834]: Invalid user win from 194.208.135.39
port 54988
```

```
Jan  3 03:45:56 ip-172-31-38-110 sshd[18836]: Invalid user admin from
118.89.145.197 port 39432
Jan  3 03:46:45 ip-172-31-38-110 sshd[18838]: Invalid user cheryl from
187.172.20.43 port 52689
Jan  3 03:46:46 ip-172-31-38-110 sshd[18840]: Invalid user cheryl from
188.131.154.248 port 42900
Jan  3 03:49:17 ip-172-31-38-110 sshd[18842]: Invalid user lottis from
103.99.63.65 port 50542
Jan  3 03:49:52 ip-172-31-38-110 sshd[18844]: Invalid user admin from 5.101.40.81
port 41818
Jan  3 03:52:59 ip-172-31-38-110 sshd[18882]: Invalid user odc from 104.236.60.180
port 46416
Jan  3 03:54:47 ip-172-31-38-110 sshd[18884]: Invalid user cynthia from
217.61.97.168 port 44310
Jan  3 03:54:47 ip-172-31-38-110 sshd[18886]: Invalid user sergey from
142.93.109.33 port 51530
Jan  3 03:55:28 ip-172-31-38-110 sshd[18889]: Invalid user admin from
104.236.246.127 port 46252
Jan  3 03:55:33 ip-172-31-38-110 sshd[18891]: Invalid user admin from 84.91.128.47
port 50392
Jan  3 03:55:33 ip-172-31-38-110 sshd[18893]: Invalid user cb from 89.218.14.61
port 36510
Jan  3 03:56:59 ip-172-31-38-110 sshd[18895]: Invalid user oracle from
206.189.149.126 port 48740
Jan  3 04:02:21 ip-172-31-38-110 sshd[18899]: Invalid user ejabberd from
204.48.21.183 port 60586
Jan  3 04:02:22 ip-172-31-38-110 sshd[18901]: Invalid user ejabberd from
217.61.105.236 port 41418
Jan  3 04:02:34 ip-172-31-38-110 sshd[18903]: Invalid user user4 from
61.14.208.253 port 40917
Jan  3 04:02:49 ip-172-31-38-110 sshd[18905]: Invalid user radius from
122.193.57.50 port 33174
Jan  3 04:06:52 ip-172-31-38-110 sshd[18909]: Invalid user ts3server from
88.99.112.212 port 34960
Jan  3 04:06:56 ip-172-31-38-110 sshd[18911]: Invalid user ts3server from
51.38.37.69 port 45814
Jan  3 04:06:59 ip-172-31-38-110 sshd[18913]: Invalid user k1 from 50.226.108.234
port 43010
Jan  3 04:06:59 ip-172-31-38-110 sshd[18915]: Invalid user k1 from 178.128.13.21
port 55536
Jan  3 04:07:00 ip-172-31-38-110 sshd[18917]: Invalid user k1 from 165.227.63.250
port 60154
Jan  3 04:07:06 ip-172-31-38-110 sshd[18919]: Invalid user test from 121.184.64.15
port 2757
Jan  3 04:07:07 ip-172-31-38-110 sshd[18921]: Invalid user minecraft from
213.41.102.5 port 15571
Jan  3 04:07:14 ip-172-31-38-110 sshd[18923]: Invalid user k1 from 193.112.156.59
port 48516
Jan  3 04:07:18 ip-172-31-38-110 sshd[18925]: Invalid user sebastian from
190.27.135.113 port 48078
Jan  3 04:07:22 ip-172-31-38-110 sshd[18927]: Invalid user test from 148.70.11.98
port 41258
Jan  3 04:07:30 ip-172-31-38-110 sshd[18930]: Invalid user test from 36.112.130.77
port 64016
```

```
Jan  3 04:07:33 ip-172-31-38-110 sshd[18932]: Invalid user deploy from
118.89.145.197 port 45600
Jan  3 04:07:33 ip-172-31-38-110 sshd[18934]: Invalid user deploy from
123.207.137.176 port 50579
Jan  3 04:08:21 ip-172-31-38-110 sshd[18938]: Invalid user fz from 208.92.218.66
port 44932
Jan  3 04:08:25 ip-172-31-38-110 sshd[18940]: Invalid user fz from 144.217.83.109
port 49374
Jan  3 04:08:46 ip-172-31-38-110 sshd[18942]: Invalid user pt from 132.232.47.139
port 34532
Jan  3 04:08:48 ip-172-31-38-110 sshd[18944]: Invalid user admin from
27.155.99.161 port 52088
Jan  3 04:12:47 ip-172-31-38-110 sshd[19025]: Invalid user vps from
129.213.145.222 port 36750
Jan  3 04:12:50 ip-172-31-38-110 sshd[19027]: Invalid user testserver from
63.135.16.12 port 56298
Jan  3 04:12:51 ip-172-31-38-110 sshd[19031]: Invalid user python from
217.61.97.168 port 44882
Jan  3 04:12:51 ip-172-31-38-110 sshd[19029]: Invalid user testserver from
85.238.104.197 port 37434
Jan  3 04:12:51 ip-172-31-38-110 sshd[19032]: Invalid user python from
195.98.73.196 port 33168
Jan  3 04:14:47 ip-172-31-38-110 sshd[19035]: Invalid user shaun from
134.175.62.14 port 39112
Jan  3 04:16:00 ip-172-31-38-110 sshd[19039]: Invalid user jeff from
164.132.43.198 port 60779
Jan  3 04:17:14 ip-172-31-38-110 sshd[19046]: Invalid user deluge from
186.230.34.233 port 29505
Jan  3 04:18:41 ip-172-31-38-110 sshd[19049]: Invalid user test from
154.120.242.70 port 42730
Jan  3 04:20:43 ip-172-31-38-110 sshd[19051]: Invalid user test from
154.120.242.70 port 52760
Jan  3 04:24:20 ip-172-31-38-110 sshd[19054]: Invalid user ir from 115.68.181.222
port 49354
grep: auth.log: binary file matches
```

[Volver al Índice del capítulo 8. Anexos.](#)

[Volver al Índice General.](#)

8.5. Referencias.

8.5.001. Enunciado TFM:

- Autor: Universitat Oberta de Catalunya.
- Título del trabajo: Enunciado TFM - Análisis forense.
- Título del Contenedor: Descripción del caso.
- URL: https://drive.google.com/file/d/1TOKWOF_akO6IKVvXJ9ovPxMMhd9kafy1/view

- URL repositorio Github: [ENUNCIADO-M1.881-TFM-ANÁLISIS-FORENSE-SISTEMAS-INFORMÁTICOS.pdf](#)

[Volver al texto de la referencia en la Sección 1.0.](#)

[Volver al texto de la referencia en la Sección 1.2.](#)

8.5.002. Propuestas de TFM:

- Autor: Universitat Oberta de Catalunya.
- Título del trabajo: M1.881 - Análisis forense.
- Título del Contenedor: Descripción.
- URL:
https://docs.google.com/spreadsheets/d/16JGkkrY4fiPN32RAfdpVuLJBZrnewscpmuTelbe3X_o/edit#gid=0
- URL repositorio Github: [002-PROUESTA-TFM-EXCEL.pdf](#)

[Volver al texto de la referencia en la Sección 1.1.](#)

8.5.003. El método Reagan:

- Autor: GEFIRA.
- Título del trabajo: El método Reagan.
- URL: <https://www.xn--elespaoldigital-3qb.com/el-metodo-reagan/>

[Volver al texto de la referencia en la Sección 1.2.](#)

8.5.004. Norma ISO 27037:

- Autor: International Organization for Standardization.
- Título del trabajo: Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence.
- URL: <https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027037-2012.pdf>
- URL repositorio Github: [003-ISOIEC-27037-2012.pdf](#)

[Volver al texto de la referencia en la Sección 1.3.2.](#)

8.5.005. IMPLEMENTACIÓN DE HERRAMIENTAS PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL:

- Autor: ANTHONY ALEXANDER GUZMÁN MOLINA.
- Título del trabajo: IMPLEMENTACIÓN DE HERRAMIENTAS PARA LA EXTRACCIÓN DE EVIDENCIA DIGITAL .
- Título del Contenedor: ISO/IEC 30121.
- URL: <https://bibdigital.epn.edu.ec/bitstream/15000/23797/1/CD%202013084.pdf>
- URL repositorio Github: [004-IMPLEMENTACIÓN-HERRAMIENTAS-PARA-LA-EXTRACCIÓN-DE-EVIDENCIA-DIGITAL.pdf](#)

[Volver al texto de la referencia en la Sección 1.3.2.](#)

8.5.006. Norma RFC 3227:

- Autores: Dominique Brezinski & Tom Killalea.
- Título del trabajo: RFC 3227.
- URL Español: <https://www.rfc-es.org/pendientes/rfc3227-es.nroff>
- URL Inglés: <https://datatracker.ietf.org/doc/html/rfc3227>
- URL repositorio Github: [005-RFC-3227-ESP.pdf](https://github.com/005-RFC-3227-ESP.pdf)

[Volver al texto de la referencia en la Sección 1.3.3.](#)

8.5.007. Que son las normas UNE:

- Autor: Grupo ACMS Consultores.
- Título del trabajo: Norma UNE: Significado y Estructura.
- URL Español: <https://www.grupoacms.com/consultora/norma-une-significado>

[Volver al texto de la referencia en la Sección 1.3.4.](#)

8.5.008. Norma UNE 71505:

- Autor: AENOR, Asociación Española de Normalización y Certificación.
- Título del trabajo: Norma UNE 71505.
- URL repositorio Github: [006-UNE-71505-2013.pdf](https://github.com/006-UNE-71505-2013.pdf)

[Volver al texto de la referencia en la Sección 1.3.4.](#)

8.5.009. Metodología para un análisis forense:

- Autores: Carles Gervilla Rivas.
- Título del trabajo: Metodología para un Análisis Forense.
- Título del Contenedor: DESARROLLO DE UNA METODOLOGÍA PARA EL ANÁLISIS FORENSE.
- URL: <https://openaccess.uoc.edu/bitstream/10609/39681/6/cgervillarTFM1214memoria.pdf>
- URL repositorio Github: [007-METODOLOGÍA-PARA-UN-ANÁLISIS-FORENSE.pdf](https://github.com/007-METODOLOGÍA-PARA-UN-ANÁLISIS-FORENSE.pdf)

[Volver al texto de la referencia en la Sección 1.3.5.](#)

8.5.010. Ninjas de la web. Metodología para un análisis forense:

- Autor: Miguel Angel Olivares.
- Título del trabajo: Metodología de Análisis Forense (Ninjas de la Web).
- URL: <https://ninjasdelaweb.com/metodologia-de-analisis-forense/>

[Volver al texto de la referencia en la Sección 1.3.5.](#)

8.5.011. Cómputo Forense de Wikipedia:

- Autor: Avelaz
- Último editor: Sabbut
- Título visualizado: Cómputo forense
- Criterio de ordenación predeterminado: Cómputo forense
- URL: https://es.wikipedia.org/wiki/C%C3%B3mputo_forense

[Volver al texto de la referencia en la Sección 1.7.](#)

8.5.012. Creación de perfil en Volatility (hotfixed42):

- Autor: hotfixed42.
- Título del trabajo: Creación de perfiles linux para Volatility.
- URL: <https://hotfixed42.rssing.com/chan-32986353/article3.html>

[Volver al texto de la referencia en la Sección 3.3.0.](#)

8.5.013. Creación de perfil en Volatility (bytelearning):

- Autor: bytelearning.
- Título del trabajo: Memoria RAM en Linux; una valiosa fuente de información.
- URL: <https://bytelearning.blogspot.com/2017/02/memoria-ram-linux-fuente-informacion.html>

[Volver al texto de la referencia en la Sección 3.3.0.](#)

8.5.014. Creación de perfil en Volatility (andreafortuna):

- Autor: andreafortuna.
- Título del trabajo: How to generate a Volatility profile for a Linux system.
- URL: <https://andreafortuna.org/2019/08/22/how-to-generate-a-volatility-profile-for-a-linux-system/>

[Volver al texto de la referencia en la Sección 3.3.0.](#)

8.5.015. Informe memmap:

- Autor: José Enrique Rodríguez González.
- Título del trabajo: 008-informe-memmap.
- ◦ URL repositorio Github: [008-informe-memmap.txt](#)

[Volver al texto de la referencia en la Sección 3.3.4.](#)

8.5.016. Informe dmesg:

- Autor: José Enrique Rodríguez González.
- Título del trabajo: 009-informe-dmesg.

- URL repositorio Github: [009-informe-dmesg.txt](#)

[Volver al texto de la referencia en la Sección 3.4.6.](#)

8.5.017. Security elinux.org:

- Autor: Wmat
- Último editor: Tim Bird
- Título visualizado: Security
- Criterio de ordenación predeterminado: Security
- URL: <https://elinux.org/Security>

[Volver al texto de la referencia en la Sección 3.4.6.](#)

8.5.018. Package: python3-certbot-apache (2.1.0-2):

- Autor: Debian.org
- Título visualizado: Package: python3-certbot-apache (2.1.0-2)
- URL: <https://packages.debian.org/sid/python3-certbot-apache>

[Volver al texto de la referencia en la Sección 3.4.7.](#)

8.5.019. Informe tree:

- Autor: José Enrique Rodríguez González.
- Título del trabajo: 011-informe-tree.
- URL repositorio Github: [009-informe-dmesg.txt](#)

[Volver al texto de la referencia en la Sección 3.4.6.](#)

[Volver al Índice del capítulo 8. Anexos.](#)

[Volver al Índice General.](#)

8.6. Línea de tiempo de evidencias.

- 2019-01-03 04:24:46 UTC+0000
 - Arranque del proceso kworker/0:0
 - Pid: 19056
- 2019-01-03 05:50:42 UTC+0000
 - Arranque del proceso kworker/u30:2
 - Pid: 19454
- 2019-01-03 06:25:21 UTC+0000

- Arranque del proceso apache2
 - Pid: 19704
- 2019-01-03 06:25:21 UTC+0000
 - Arranque del proceso apache2
 - Pid: 19705
- 2019-01-03 06:25:21 UTC+0000
 - Arranque del proceso apache2
 - Pid: 19706
- 2019-01-03 06:25:21 UTC+0000
 - Arranque del proceso apache2
 - Pid: 19707
- 2019-01-03 06:25:21 UTC+0000
 - Arranque del proceso apache2
 - Pid: 19708
- 2019-01-03 06:25:21 UTC+0000
 - Arranque del proceso kworker/0:1
 - Pid: 19709
- 2019-01-03 06:33:15 UTC+0000
 - Arranque del proceso apache2
 - Pid: 19952
- 2019-01-03 06:33:16 UTC+0000
 - Arranque del proceso apache2
 - Pid: 19953
- 2019-01-03 07:26:31 UTC+0000
 - Arranque del proceso apache2
 - Pid: 20230
- 2019-01-03 07:26:32 UTC+0000
 - Arranque del proceso apache2
 - Pid: 20231
- 2019-01-03 07:26:33 UTC+0000
 - Arranque del proceso apache2
 - Pid: 20232
- 2019-01-03 07:26:34 UTC+0000
 - Arranque del proceso apache2
 - Pid: 20233

- Arranque del proceso apache2
 - Pid: 20233
- 2019-01-03 07:32:10 UTC+0000
 - Arranque del proceso sh
 - Pid: 20381
- 2019-01-03 07:49:45 UTC+0000
 - Ver Comandos [Linux bash](#).
- 2019-01-03 07:50:04 UTC+0000
 - Arranque del proceso sshd
 - Pid: 20483
- 2019-01-03 07:50:05 UTC+0000
 - Arranque del proceso systemd
 - Pid: 20485
- 2019-01-03 07:50:05 UTC+0000
 - Arranque del proceso (sd-pam)
 - Pid: 20486
- 2019-01-03 07:50:05 UTC+0000
 - Arranque del proceso sshd
 - Pid: 20576
- 2019-01-03 07:50:05 UTC+0000
 - Arranque del proceso bash
 - Pid: 20577
- 2019-01-03 08:01:34 UTC+0000
 - Arranque del proceso pickup
 - Pid: 20703
- 2019-01-03 08:09:21 UTC+0000
 - Arranque del proceso kworker/u30:1
 - Pid: 20781
- 2019-01-03 08:16:28 UTC+0000
 - Arranque del proceso kworker/u30:0
 - Pid: 20886
- 2019-01-03 08:17:06 UTC+0000

- Arranque del proceso sudo
 - Pid: 20893
- 2019-01-03 08:17:06 UTC+0000
 - Arranque del proceso insmod
 - Pid: 20894
 - 2019-01-03 08:17:06 UTC+0000
 - Arranque del proceso kworker/0:2
 - Pid: 20898

[Volver al Índice del capítulo 8. Anexos.](#)

[Volver al Índice General.](#)
