**Análisis Forense**

# Análisis de dos distribuciones Linux

### 

### 

| ÍNDICE |
| --- |
| [**Análisis de dos distribuciones Linux 1**](#_n6arwwmay01c)  [1. Contexto 2](#_hl79aikr2mgz)  [2. Herramientas 3](#_wrhbljp9e47w)  [3. Preguntas 3](#_s593ln4wjma3)  [3.1 Caso MATE 3](#_waho84hjm6fc)  [Verificación 3](#_a0n9899pxvfg)  [¿Cuál es el ID del último arranque? 3](#_cnxledj4r015)  [¿Cómo instaló el usuario Google Chrome en MATE? 4](#_rw7odf7i46qp)  [¿En qué fecha y hora lo instaló el usuario? 4](#_8k1gpu3owrhq)  [¿El nombre de un repositorio desde el cual se instaló más de una aplicación adicional? 5](#_ipqbxh57tpe9)  [¿Cuál es el nombre de la sesión de escritorio? 5](#_h1lcixr0ls1u)  [¿Cuál era el nombre del dominio sospechoso que visitó el usuario desde MATE? 5](#_ppw7k3ymvixb)  [**3.2 Caso kubuntu 6**](#_4w0k02m6fxkq)  [Verificación de la imagen 6](#_l7jq4zp6ma66)  [¿Cuál es el ID del último arranque? 6](#_l7jq4zp6ma66)  [¿Cómo usuario instaló Google Chrome? Fecha y hora. 7](#_jlrahs3vdfjo)  [¿Cuando se puso en modo de suspensión el dispositivo? 7](#_i9uxtl6iyvls)  [¿Cuántos comandos privilegiados ejecutó el usuario? 8](#_5k8nobo2ui06)  [¿Qué aplicación se utilizó para abrir el archivo de dispositivos principales? 8](#_1368kcv12cu6)  [/home/user/.config/ 8](#_6qbkfnm7srz6)  [/home/user/.local/share/ 8](#_j2qpzweukcux)  [¿Cuál era el UUID del volumen raíz principal? 9](#_449tmstqsogb)  [3.3 Ficheros 9](#_ju4sj0nc06i)  [Configuración Inicial 9](#_6jjomfbf3bo3)  [Verificar Imagen de disco forense E01 9](#_yf78s1h0uzal)  [Montaje físico 10](#_ox6s3lddkpr8)  [Verificar la información 11](#_bkipj8gnxajb)  [Montado de la partición lógica 12](#_ayjbvnm5klt5)  [Ejecución de comandos del sistema investigado 13](#_g7gdy9lepwkv)  [Desmontado 13](#_pcfyzb8f267b)  [Bibliografía 13](#_n8d2h5hidi9f) |
| Análisis de dos distribuciones Linux |
| Contexto |
| Ha sido llamado para analizar la máquina de un empleado; se sospecha que el empleado hace un mal  uso de la máquina de la empresa al violar las políticas de la empresa. Se le solicita que investigue la  máquina del empleado para encontrar artefactos de mal uso. Ejemplos de tales artefactos son navegar  por sitios web ilegales, descargar imágenes ilegales y archivos de música ilegales |
| Herramientas |
| * ewf-tools (ewfverify, ewfmount) * The Sleuth Kit (mmls) |
| Preguntas |

| 3.1 Caso MATE |
| --- |
| Verificación |
|  |
| Bits → 538968064 |
| ¿Cuál es el ID del último arranque? |
| **journalctl --list-boot** |
| 2a83e81d41694410928dd3c539a17f7d |
|  |
| ¿Cómo instaló el usuario Google Chrome en MATE? |
| A través de una instalación con apt. |
| **cat /var/log/apt/history.log | grep chrome** |
|  |
| ¿En qué fecha y hora lo instaló el usuario? |
| Una línea antes del comando se puede ver la fecha. |
| Con “grep -B1” vemos una linea antes,BEFORE, al texto filtrado |
| **cat /var/log/apt/history.log | grep -i -B1 chrome** |
|  |
| Fecha y horas de la instalación**: 2022-04-06 02:39:17** |
| ¿El nombre de un repositorio desde el cual se instaló más de una aplicación adicional? |
| **ls /etc/apt/sources.list.d/** |
|  |
| Podemos ver que se encuentran aplicaciones instaladas por el usuario como google chrome, brave o vlc. |
| ¿Cuál es el nombre de la sesión de escritorio? |
| **grep "session opened" /var/log/auth.log** |
|  |
| ¿Cuál era el nombre del dominio sospechoso que visitó el usuario desde MATE? |
| Probablemente haya tenido suerte, buscar más evidencia. |
| **cat /etc/hosts** |
|  |

| 3.2 Caso kubuntu |
| --- |
| Verificación de la imagen |
|  |
| ¿Cuál es el ID del último arranque? |
| **journalctl --list-boots** |
|  |
| Id → c541703922fd4f47851624e929f9821c |
| ¿Cómo usuario instaló Google Chrome? Fecha y hora. |
| **cat ~/.bash\_history** |
| Dos formas de instalación |
|  |
|  |
|  |
| ¿Cuando se puso en modo de suspensión el dispositivo? |
| **cat /var/log/auth.log\* | grep \'sleep\'** |
|  |
| O **journalctl | grep "systemd-sleep"** |
|  |
| ¿Cuántos comandos privilegiados ejecutó el usuario? |
| **cat /var/log/auth.log\* | grep sudo** |
|  |
| **cat /var/log/auth.log\* | grep -i sudo | wc -l** |
|  |
| ¿Qué aplicación se utilizó para abrir el archivo de dispositivos principales? |
| **grep -ri “top devices” \*** |
| */home/user/.config/* |
|  |
| */home/user/.local/share/* |
|  |
| ¿Cuál era el UUID del volumen raíz principal? |
| **cat /var/log/dmesg\* | grep -i uuid** |
|  |

| 3.3 Ficheros |
| --- |
| * kubuntu.E01 2a575d461d041e941bd4707afe9e8bb5e75548e2 * mate.E01 1167890df7d0acdae1efe97ae352035fa4ed1eeb |
|  |
|  |

| Configuración Inicial |
| --- |
| Verificar Imagen de disco forense E01 |
| E01 son imágenes en formato de EWF (Expert Witness). Este formato comprime los metadatos con el valor hash  que almacena dentro del pie de página de la imagen. Eso significa que si aplicamos hash al archivo E01 directamente, obtenemos el valor hash incorrecto. |
| **sudo ewfverify -d sha1 kubuntu.E01** |
|  |
| Acceder a los datos de una imagen de disco forense E01 |
| Montaje físico |
| **sudo mkdir /mnt/phy1 /mnt/log1** |
|  |
| **sudo ewfmount kubuntu.E01 /mnt/phy1**  **sudo file /mtn/phy1/ewf1** |
|  |
| Verificar la información |
| **mmls** muestra el diseño de los sistemas de administración de medios, que incluyen tablas de  particiones y etiquetas de discos. |
| **sudo mmls ewf1** |
|  |
| Inicio del sector a investigar → **0001052672** |
| Lo pasamos a bits con |
| **echo 1052672 \\* 512 | bc** |
|  |
| **538968064** |
|  |
| Montado de la partición lógica |
| **sudo mount -o ro,noload,offset=538968064 /mnt/phy1/ewf1 /mnt/log1** |
| * **mount:** Es el comando utilizado para montar sistemas de archivos en el árbol de directorios del sistema. * **-o ro,loop,offset=538968064:** Estas son opciones que se pasan al comando mount. Significan:   + **ro:** Monta el sistema de archivos en modo de solo lectura (read-only). Esto asegura que el sistema de archivos no pueda ser modificado.   + **loop:** Indica que el archivo de imagen de disco se debe montar como un dispositivo de bucle. Un dispositivo de bucle permite que un archivo actúe como un dispositivo de bloque, lo que facilita el montaje de sistemas de archivos que residen en archivos regulares. Da errores, usar Noload.   + **offset=538968064**: Esto indica el desplazamiento dentro del archivo de imagen de disco donde comienza el sistema de archivos que deseas montar. Este número (538968064) es el desplazamiento en bytes dentro del archivo de imagen donde se encuentra el inicio del sistema de archivos que quieres montar. Esta opción es útil cuando el sistema de archivos no comienza al principio del archivo de imagen de disco. Sin el desplazamiento correcto, el montaje puede fallar o mostrar datos incorrectos. * **/mnt/phy1/ewf1**: Es el archivo de imagen de disco que se está montando. En este caso, /mnt/phy1/ewf1 es la ruta del archivo de imagen de disco. * **/mnt/log1:** Es el directorio en el que se va a montar el sistema de archivos contenido en el archivo de imagen de disco. El contenido del sistema de archivos del archivo de imagen de disco será accesible en este directorio después del montaje. |
|  |
|  |
| Ejecución de comandos del sistema investigado |
| Podemos usar **chroot** para cambiar "al" sistema sospechoso y ejecutar comandos tal como lo harían ellos. |
| **sudo chroot ./log1 /usr/bin/bash** |
|  |
|  |
| Desmontado |
| **sudo umount /mnt/log1**  **sudo umount /mnt/phy1** |
| Si reiniciamos la máquina también se pierden los puntos de montaje. |

| Bibliografía |
| --- |
| <https://www.sqlitetutorial.net/sqlite-show-tables/> |
| <https://www.loc.gov/preservation/digital/formats/fdd/fdd000406.shtml> |
|  |