CIBERSEGURIDAD

PRÁCTICA 2: Análisis forense

AUTORES

CARLOS GARCÍA SANTA

GRUPO 14

INGENIERÍA INFORMÁTICA

ESCUELA POLITÉCNICA SUPERIOR

UNIVERSIDAD AUTÓNOMA DE MADRID

04/04/2025

Índice

1. Clonado de un disco duro

1.1. Crear un documento de cadena de custodia para la evidencia facilitada (disco duro). 1.2. Clonar el disco con la herramienta que estiméis oportuna.

Para realizar el clonado de un disco duro, primero creamos una máquina virtual en VirtualBox con Debian 12 como sistema operativo, una vez en la terminal del sistema, se ejecuta el comando “fdisk -l” con el objetivo de identificar las particiones y localizar el disco principal de la máquina virtual.

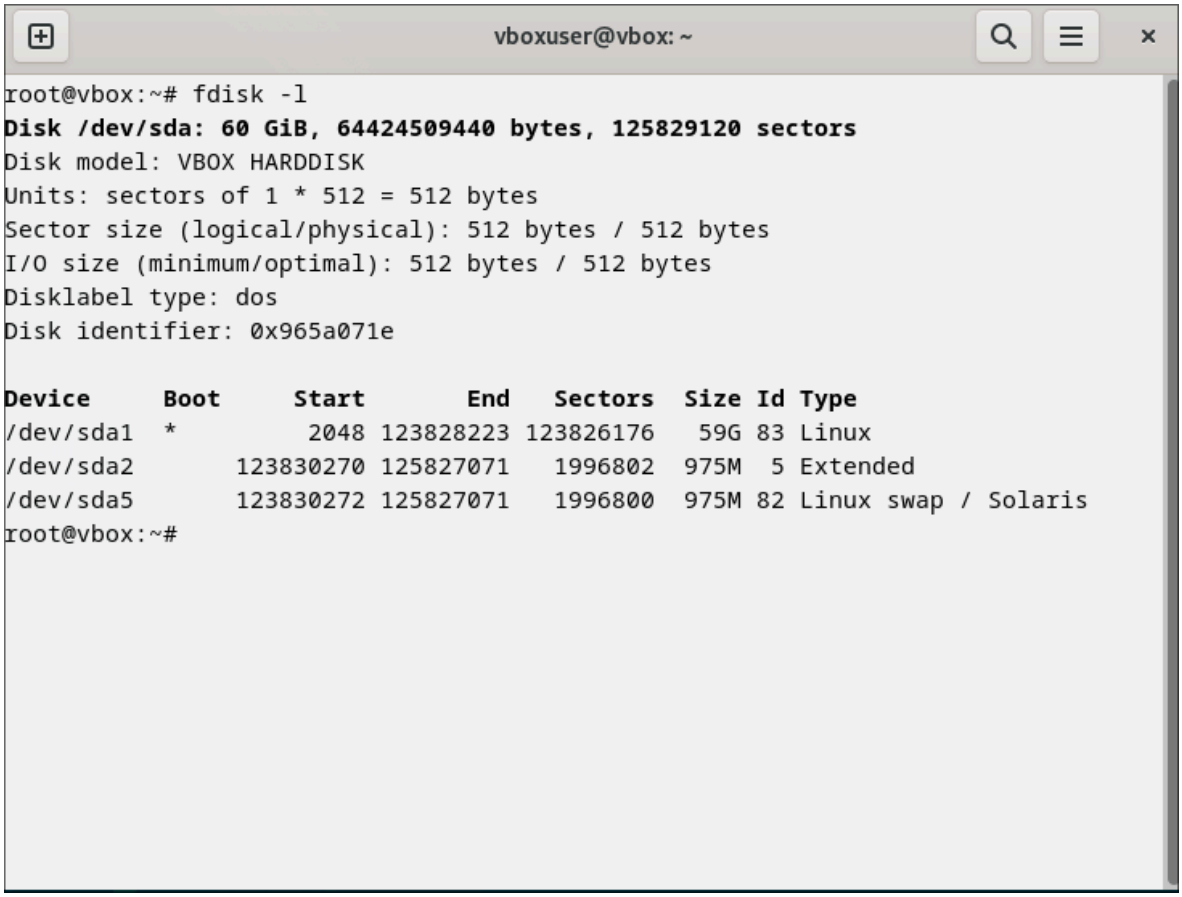


Figura 1: Captura del comando de “fdisk -l” en la máquina virtual.

En nuestro caso, el disco principal corresponde a /dev/sda, y procedemos a su clonación utilizando la herramienta dc3dd, que permite volcar los datos del disco a un archivo imagen. Este comando también calcula de forma simultánea la suma hash SHA256, lo cual es fundamental para garantizar la integridad de la copia forense.

```
vboxuser@vbox:/mnt$ sudo dc3dd if=/dev/sda hash=sha256 log=/mnt/shared/dc3dd_log.txt of=/mnt/shared/imagen_disco_dc3dd.img

dc3dd 7.2.646 started at 2025-04-04 20:45:58 +0200
compiled options:
command line: dc3dd if=/dev/sda hash=sha256 log=/mnt/shared/dc3dd_log.txt of=/mnt/shared/imagen_disco_dc3dd.img
device size: 42257612 sectors (probed),   21,635,897,344 bytes
sector size: 512 bytes (probed)
 21635897344 bytes ( 20 G ) copied ( 100% ),  127 s, 163 M/s

input results for device `/dev/sda':
   42257612 sectors in
   0 bad sectors replaced by zeros
   777798d760d29a97afc65822c405d875e6cb71074df153cb368e627a98689286 (sha256)

output results for file `/mnt/shared/imagen_disco_dc3dd.img':
   42257612 sectors out

dc3dd completed at 2025-04-04 20:48:05 +0200
```

Figura 2: Captura de ejecución del comando "dc3dd" en la máquina virtual.

Alternativamente y como opción más sencilla, podemos realizar un clonado de disco con OSForensics, dónde además tenemos la posibilidad de crear un caso y emplear el documento de cadena de custodia que ya incluye esta funcionalidad. Esta herramienta también permite el cálculo del hash del disco, pudiendo elegir entre distintos algoritmos (SHA256, MD5…), al igual que la herramienta de terminal dc3dd.

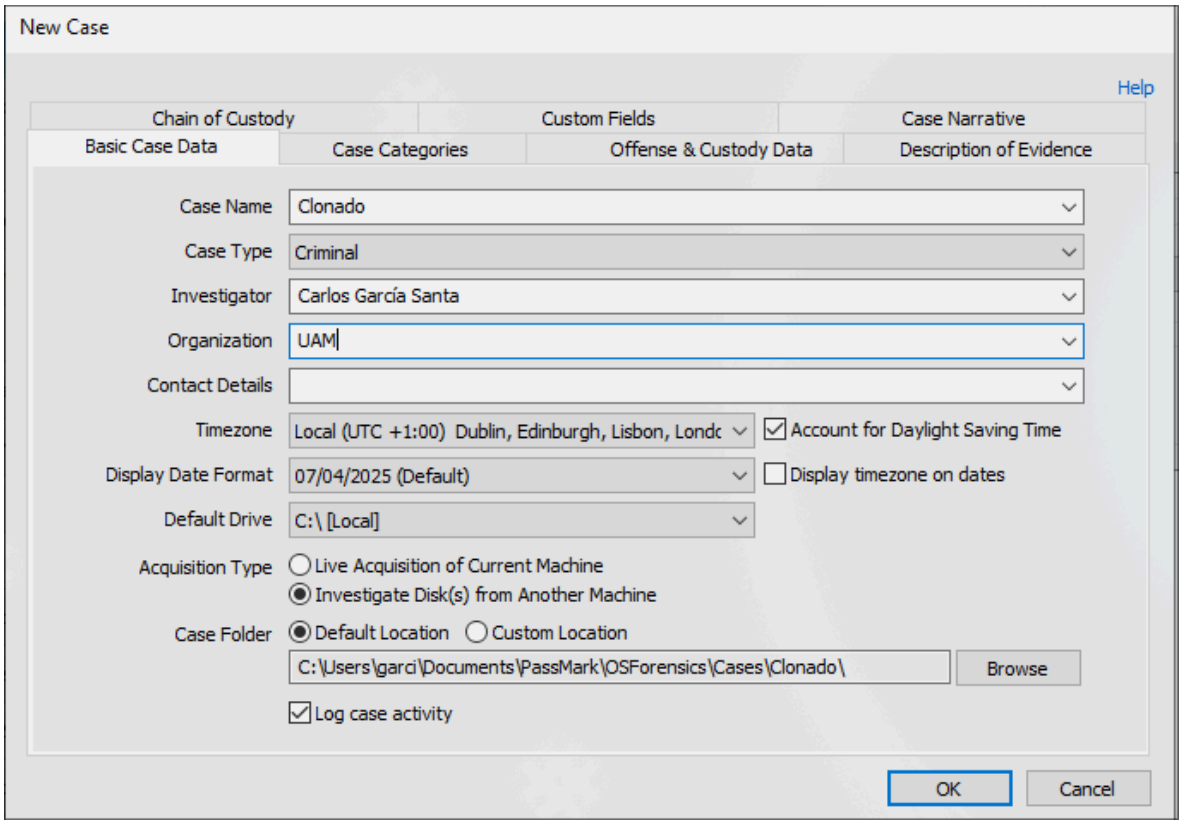


Figura 3: Captura de apertura de caso (se observa que una de las opciones es la de cadena de custodia).

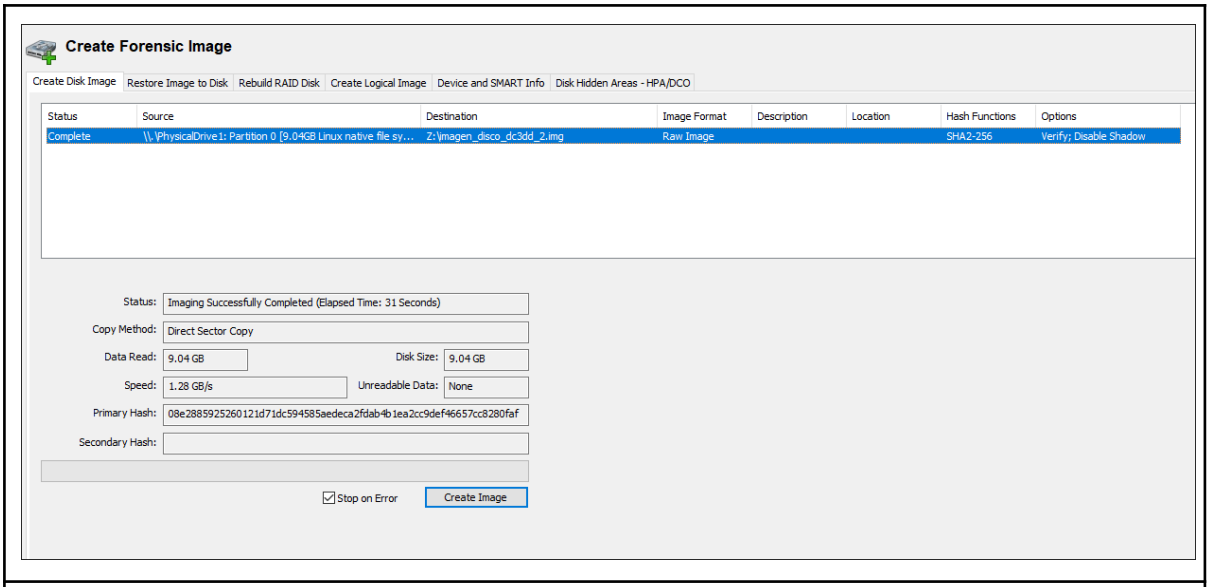


Figura 4: Captura de creación de imagen forense.

1.3. Verificar hashes del disco original y el clonado.

Una vez finalizada la clonación, se verifica la integridad de la imagen generada. Para ello, se calcula nuevamente la suma SHA256 de la imagen desde el sistema host (con una función del sistema operativo) y se compara con la generada previamente por dc3dd y por OSForensics. La coincidencia entre ambos valores confirma que la copia forense se ha realizado correctamente, sin alteraciones ni pérdida de datos.

```
[santacg@archlinux Shared]$ cat dc3dd_log.txt

dc3dd 7.2.646 started at 2025-04-04 20:45:58 +0200
compiled options:
command line: dc3dd if=/dev/sda hash=sha256 log=/mnt/shared/dc3dd_log.txt of=/mnt/shared/imagen_disco_dc3dd.img
device size: 42257612 sectors (probed),   21,635,897,344 bytes
sector size: 512 bytes (probed)
 21635897344 bytes ( 20 G ) copied ( 100% ), 126.66 s, 163 M/s

input results for device `/dev/sda':
   42257612 sectors in
   0 bad sectors replaced by zeros
   777798d760d29a97afc65822c405d875e6cb71074df153cb368e627a98689286 (sha256)

output results for file `/mnt/shared/imagen_disco_dc3dd.img':
   42257612 sectors out

dc3dd completed at 2025-04-04 20:48:05 +0200

[santacg@archlinux Shared]$ sha256sum imagen_disco.img
sha256sum: imagen_disco.img: No such file or directory
[santacg@archlinux Shared]$ sha256sum imagen_disco_dc3dd.img
777798d760d29a97afc65822c405d875e6cb71074df153cb368e627a98689286  imagen_disco_dc3dd.img
```

Figura 5: Captura de la comprobación del resultado de calcular la suma hash SHA256 de la imagen clonada con la suma calculada en el comando "dc3dd".

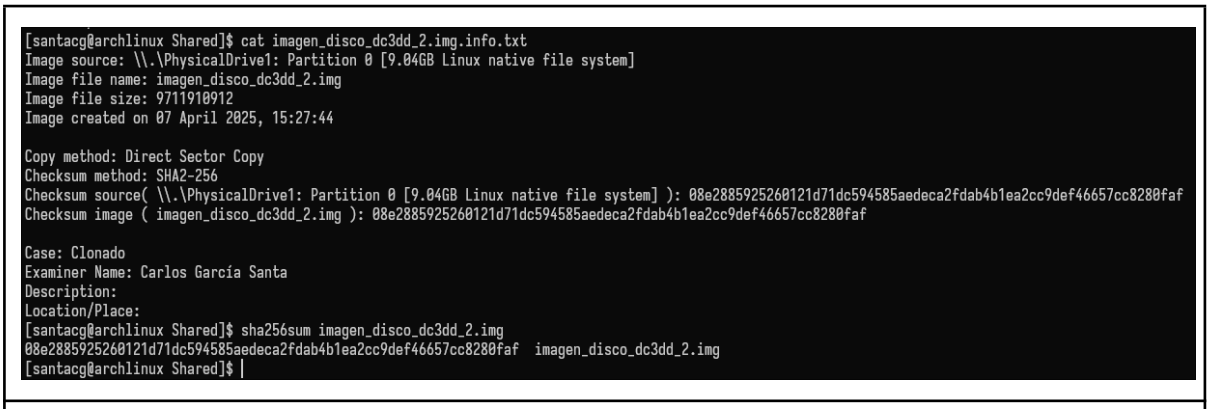


Figura 6: Captura de la comprobación del resultado de calcular la suma hash SHA256 de la imagen clonada con la suma calculada por OSForensics.

2. OSForensics

Una vez clonado el disco, se procede al análisis forense de la imagen obtenida de la máquina virtual con Debian 12, para ello, utilizamos la herramienta OSForensics instalada en una máquina virtual con sistema operativo Windows. Previo a esta parte se han realizado algunas acciones con el fin de dejar rastro para el análisis, simulando actividad del usuario en el sistema que posteriormente pueda ser detectada mediante el estudio de los distintos artefactos elegidos.

2.1. Artefacto 1 - Historial de bash

El historial de Bash recoge los comandos introducidos por el usuario en la terminal en los sistemas operativos Linux, este archivo se encuentra normalmente en la ruta /home/"usuario"/.bash_history.

Se monta la imagen desde OSForensics y se accede al directorio del usuario para localizar el archivo. Al abrirlo, se observan los comandos ejecutados previamente, lo que permite identificar acciones relevantes realizadas desde la línea de comandos, como instalaciones, accesos remotos o comandos del sistema.

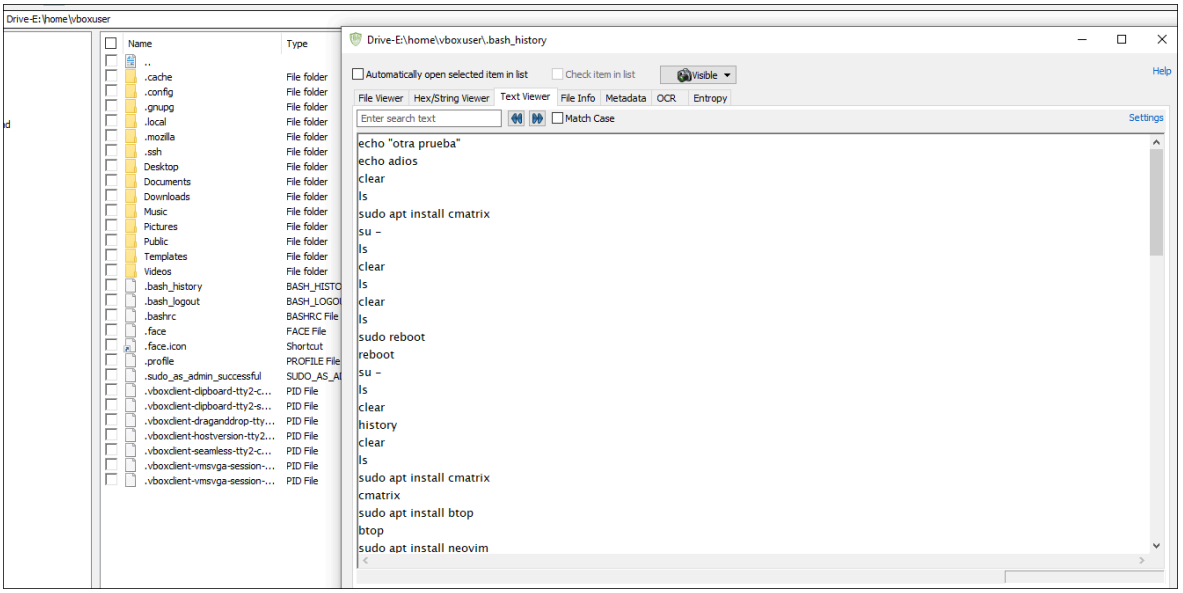


Figura 7: Visualización del historial de Bash.

2.2. Artefacto 2 - Historial de búsqueda

Este artefacto refleja la actividad del usuario en el navegador web, concretamente en Mozilla Firefox. OSForensics permite acceder al historial almacenado en el perfil del navegador, donde queda registrada información relevante sobre las búsquedas realizadas y los sitios visitados. Para su análisis se utiliza la funcionalidad User Activity Scan, que detecta automáticamente los perfiles configurados en el navegador y extrae los registros asociados. A partir de ahí, se puede consultar el historial de búsquedas junto con datos como la hora de la última visita, el número de veces que se ha accedido a una URL concreta, el tiempo aproximado de permanencia en cada página, el nombre del usuario del sistema operativo que realizó la actividad y el perfil exacto del navegador desde el que se llevó a cabo.

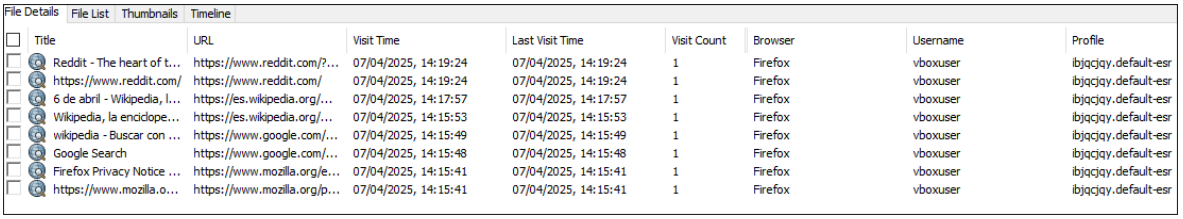


Figura 8: Visualización del historial de búsqueda extraído con la herramienta System Information.

2.3. Artefacto 3 - Elementos borrados

El análisis de archivos eliminados permite recuperar información que el usuario ha intentado borrar, para ello utilizamos la opción Deleted Files

Search de OSForensics, que examina los sectores del disco en busca de archivos que hayan sido marcados como eliminados. Al ejecutar esta funcionalidad se nos muestra información como el nombre del archivo, la fecha de acceso y de modificación, la ruta original y, además, permite ver el texto que contenía el archivo eliminado, así como los metadatos o la entropía del archivo, como se muestra en la siguiente figura. De esta forma podemos ver que este tipo de artefacto resulta muy útil para detectar intentos de ocultación o eliminación de evidencias.

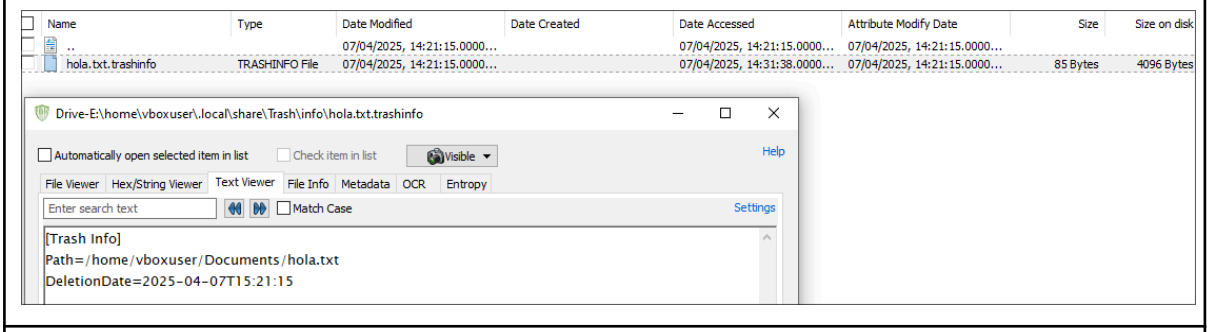


Figura 9. Archivos eliminados detectados con Deleted Files Search.

2.4. Artefacto 4 - Logs del sistema

Los registros del sistema nos permiten reconstruir eventos que pueden aportar información relacionada con el funcionamiento del equipo, como instalaciones de paquetes, actualizaciones, inicios o apagados. En sistemas Linux, esta información la podemos encontrar en distintos archivos dentro del directorio “/var/log”.

Para este análisis volvemos a emplear el File Viewer de OSForensics. En el archivo history.log ubicado en “/var/log/apt/”, observamos el historial de las instalaciones y actualizaciones de paquetes realizadas a través del gestor de paquetes APT.

Este archivo permite verificar qué software se ha instalado, cuándo se hizo y desde qué usuario, así, se podría establecer una cronología precisa de cambios en el sistema y asociarlos a la actividad registrada en otros artefactos.

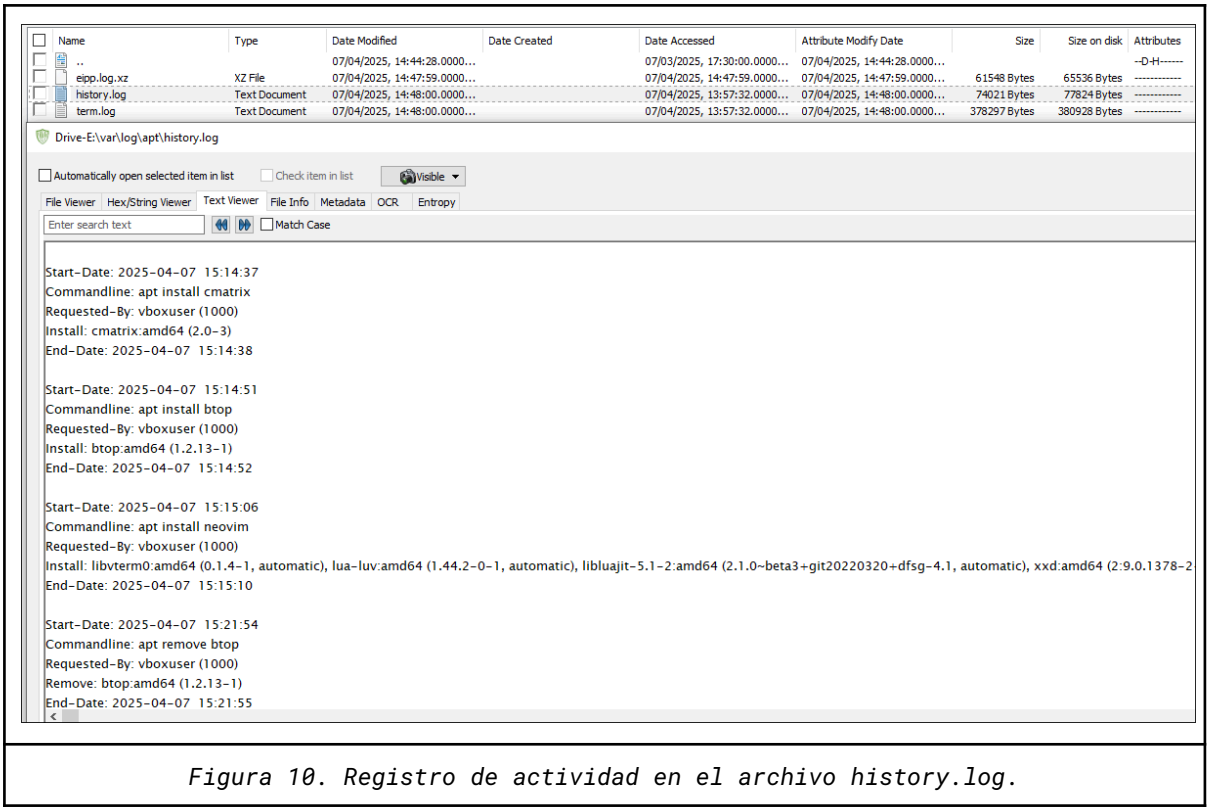


Figura 10. Registro de actividad en el archivo history.log.

2.5. Artefacto 5 - Detalles del sistema

Este artefacto nos da información sobre los componentes hardware del sistema operativo, se accede a estos datos a través del archivo hardware-summary, ubicado en la ruta “/var/log/installer/”. En este archivo se encuentran registros generados durante la instalación del sistema, como la salida de los comandos uname -a y lspci, a través de esta información se identifican detalles sobre el kernel y la arquitectura del sistema, el tipo de CPU, los adaptadores de red, los dispositivos USB, la tarjeta de sonido, etc.

Estos nos puede ser útil para analizar el entorno de ejecución del sistema, detectar si por ejemplo se ha utilizado una máquina virtual y entender las capacidades físicas del equipo desde el que se generaron otros artefactos.

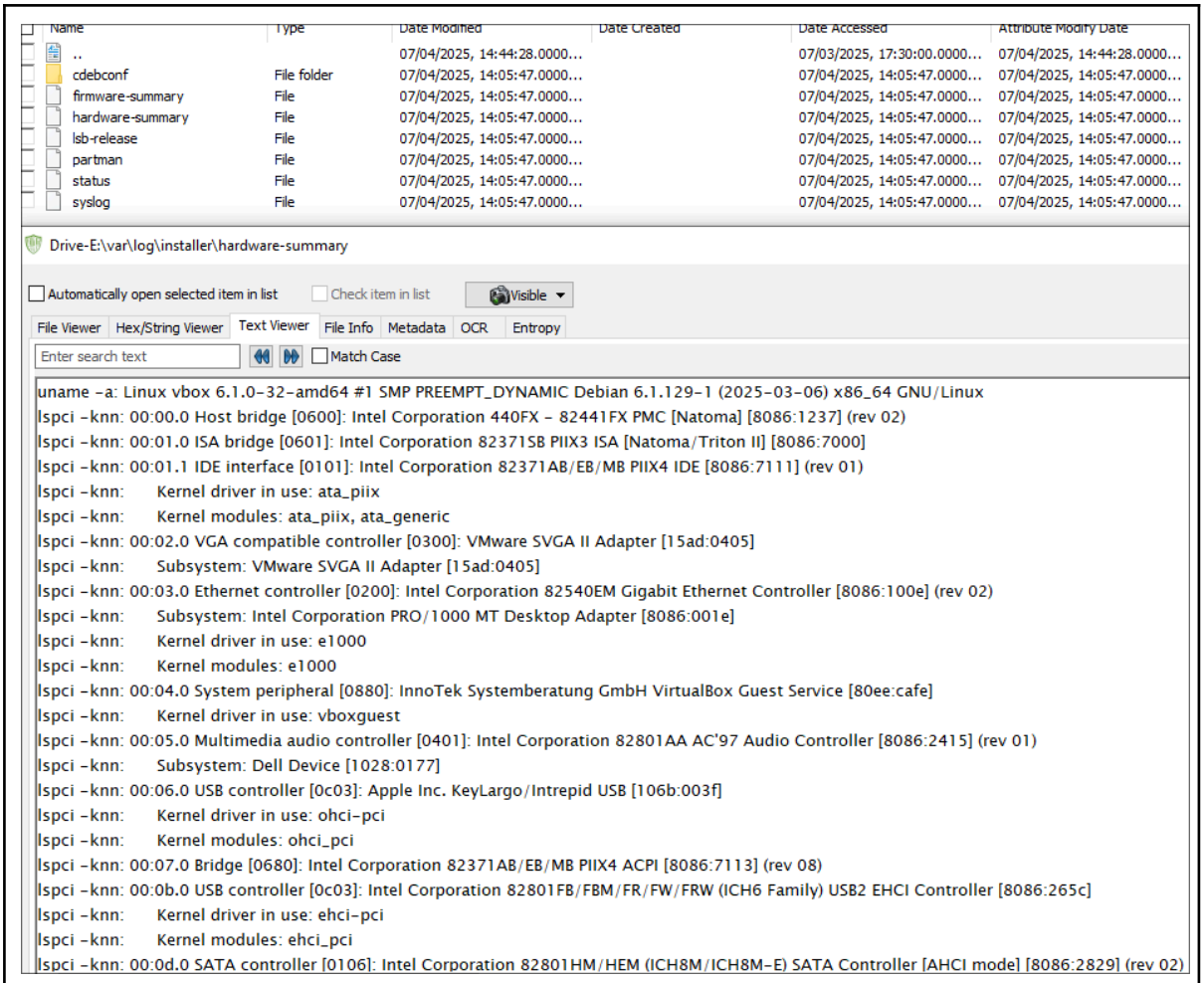


Figura 11: Detalles del sistema extraídos desde el archivo hardware-summary.

3. Análisis forense InmoHouse

Para esta parte de la práctica, se nos proporciona una imagen de un disco duro clonado de un servidor perteneciente a la empresa ficticia InmoHouse, donde se sospecha que un empleado ha incumplido las políticas de uso de los sistemas informáticos. La normativa interna de la empresa establece que no está permitida la instalación ni ejecución de programas no relacionados con lo laboral, así como tampoco se permiten conexiones o ejecuciones de comandos fuera del horario de trabajo establecido entre las 9:00 y las 19:00.

Para poder analizar el disco clonado, primero montamos el disco en OSForensics, tratándolo como un disco duro virtual con emulación física y asegurando que no se modifiquen los datos marcando la propiedad de solo lectura.

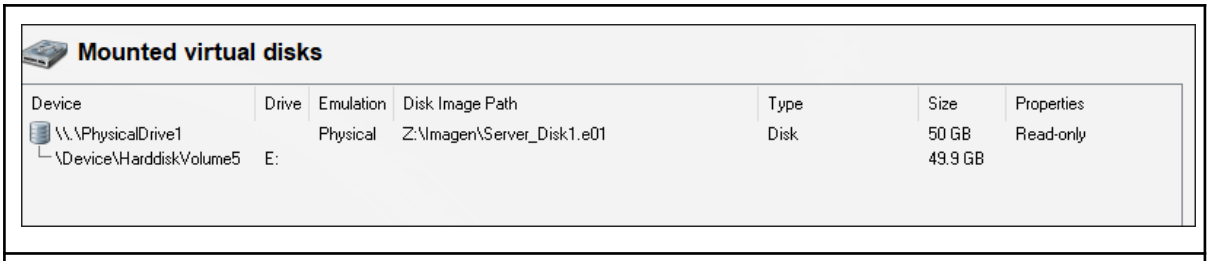


Figura 12: Montado del disco clonado.

3.1. ¿Qué usuario (o usuarios) se han utilizado?

Para poder responder a esta pregunta analizamos los logs del sistema con el Registry Viewer y el System Information de OSForensics, con ambos métodos podemos ver la existencia de tres usuarios: Guest, Administrador y powers; estos dos primeros usuarios son los creados por defecto por Windows. En el Registry Viewer podemos ver esta información en el path "\Windows\System32\Config\SAM" que es el Security Account Manager donde se observan datos como los nombres de usuario y los Relative Identifier (RID) de los usuarios.

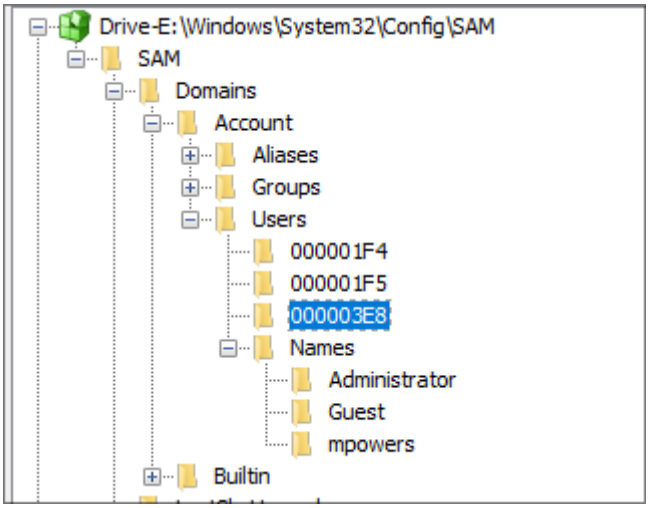
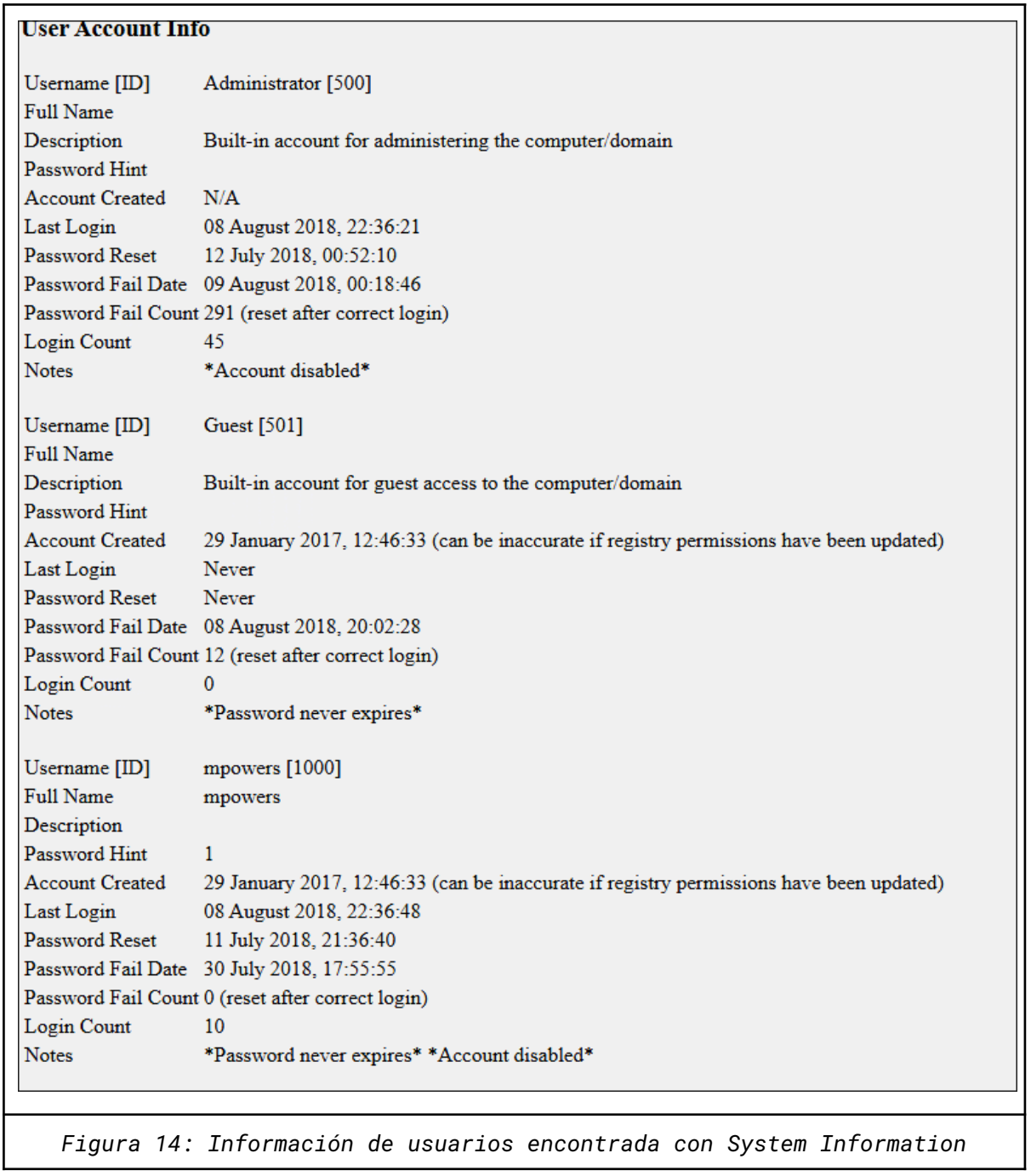


Figura 13: Información de usuarios encontrada con Registry Viewer.

El resumen del sistema nos aporta más información sobre estos usuarios, pudiendo ver datos relevantes para el caso como la última fecha de Login, la fecha de reseteo de contraseña, la fecha de fallo de contraseña, el conteo de fallos de contraseña o el número de Login correctos.



User Account Info

Username [ID]	Administrator [500]
Full Name	
Description	Built-in account for administering the computer/domain
Password Hint	
Account Created	N/A
Last Login	08 August 2018, 22:36:21
Password Reset	12 July 2018, 00:52:10
Password Fail Date	09 August 2018, 00:18:46
Password Fail Count	291 (reset after correct login)
Login Count	45
Notes	*Account disabled*
Username [ID]	Guest [501]
Full Name	
Description	Built-in account for guest access to the computer/domain
Password Hint	
Account Created	29 January 2017, 12:46:33 (can be inaccurate if registry permissions have been updated)
Last Login	Never
Password Reset	Never
Password Fail Date	08 August 2018, 20:02:28
Password Fail Count	12 (reset after correct login)
Login Count	0
Notes	*Password never expires*
Username [ID]	mpowers [1000]
Full Name	mpowers
Description	
Password Hint	1
Account Created	29 January 2017, 12:46:33 (can be inaccurate if registry permissions have been updated)
Last Login	08 August 2018, 22:36:48
Password Reset	11 July 2018, 21:36:40
Password Fail Date	30 July 2018, 17:55:55
Password Fail Count	0 (reset after correct login)
Login Count	10
Notes	*Password never expires* *Account disabled*

Figura 14: Información de usuarios encontrada con System Information

Analizando toda esta información podemos llegar a la conclusión de que el usuario del empleado corresponde a mpowers, siendo los otros dos creados por defecto por el sistema como ya se ha mencionado.

3.2. ¿Se han utilizado programas no permitidos por las políticas de la empresa? Lista los programas utilizados.

Podemos ver de forma sencilla los programas instalados utilizando la herramienta User Activity clicando en Installed Programs; aplicando esto podemos ver el software F-response instalado en el sistema la madrugada del día que se produjo el último Login de mpowers, buscando en Google vemos que

este programa es una herramienta forense avanzada, esto claramente si asumimos que ha sido instalado por el empleado sería una violación de las políticas de uso.

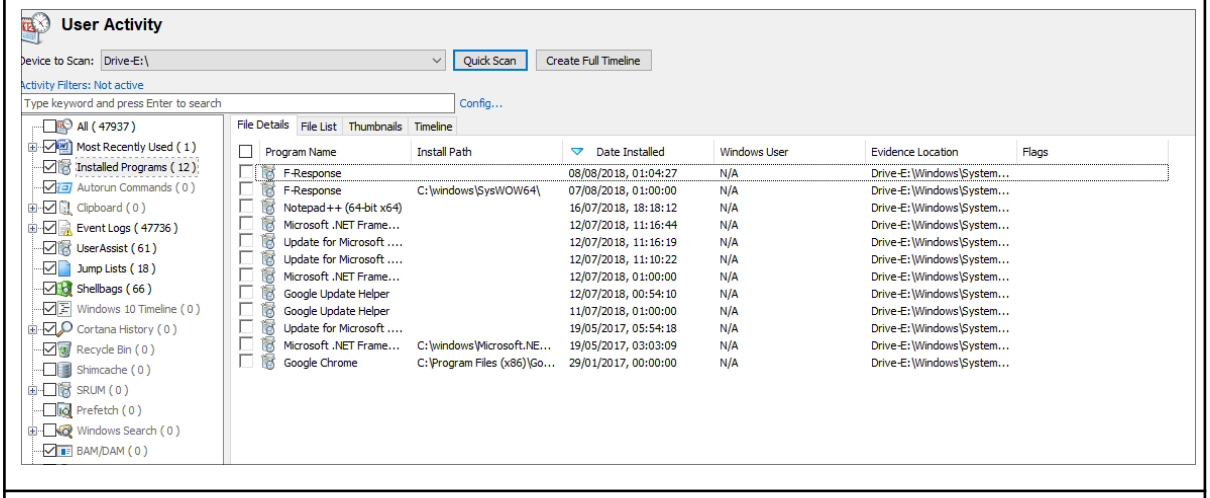


Figura 15: Captura que muestra como OSForensics detecta F-response como un programa instalado.

Para intentar buscar más programas no permitidos se usa el buscador de archivos, y encontramos en el escritorio un ejecutable de la aplicación PrivaZer que es una herramienta de borrado de información, este tipo de aplicación está explícitamente prohibida por las políticas de la empresa.

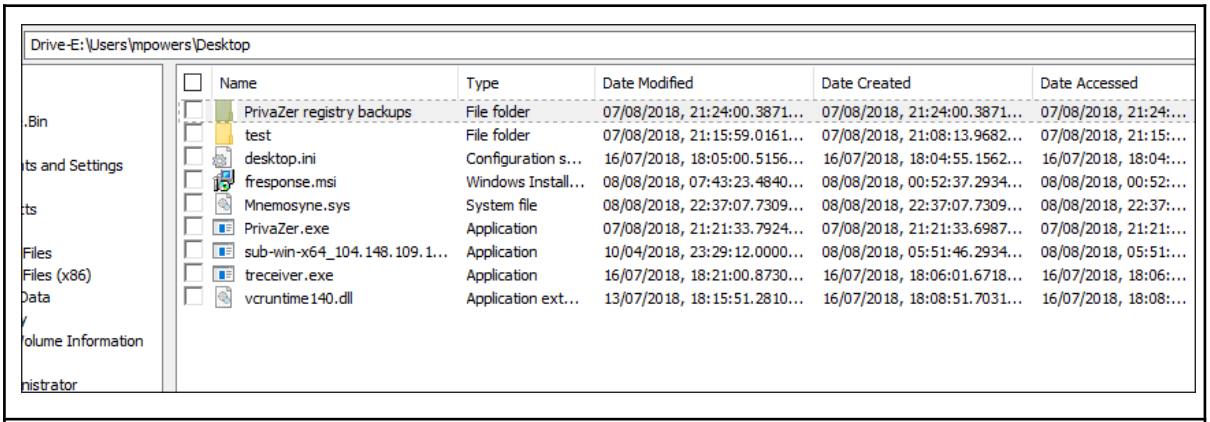


Figura 16: Presencia de la herramienta de borrado de información PrivaZer en el escritorio.

3.3. ¿Se han realizado conexiones remotas fuera del horario laboral de la empresa? Indica los días y las horas.

Viendo los datos encontrados en el apartado 3.1 se encuentra que se han hecho múltiples intentos fallidos de inicio de sesión en la cuenta de Administrador, usando el Event Log Viewer y filtrando eventos de tipo “Failed Logon Attempts” observamos más de 30000 intentos de inicio de

sesión fallidos en un solo día empleando distintos nombres de usuario, lo que parece indicar intentos de acceso maliciosos no autorizados. A continuación se muestran dos ejemplos de intento de inicio sesión con diferentes nombres fuera del horario laboral, además del gráfico de intentos fallidos de inicio de sesión.

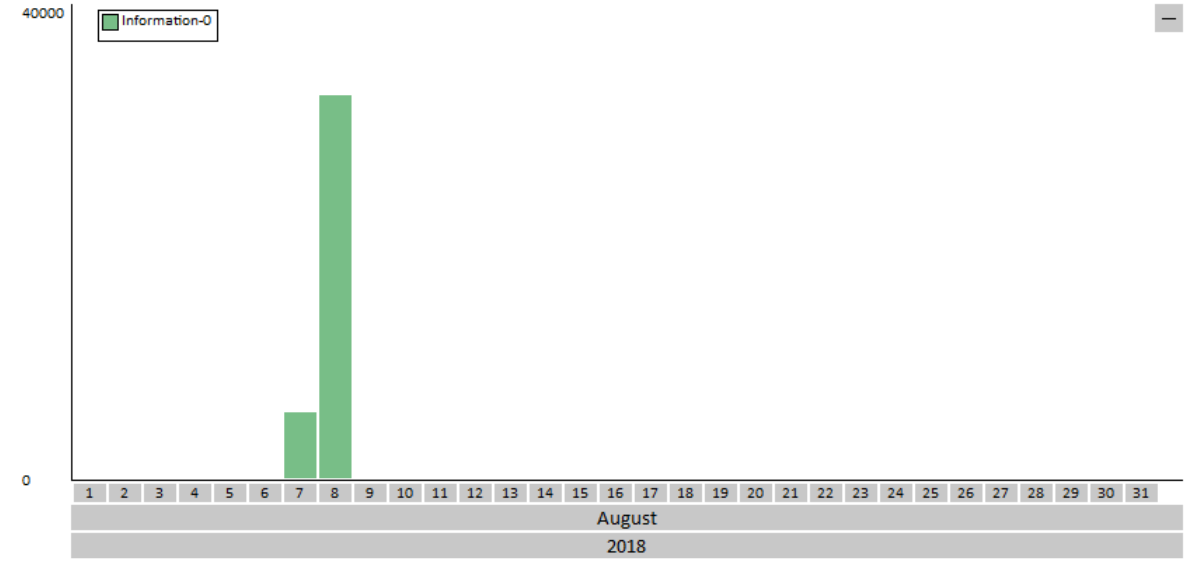


Figura 17: representación gráfica de intentos de acceso fallidos por día.

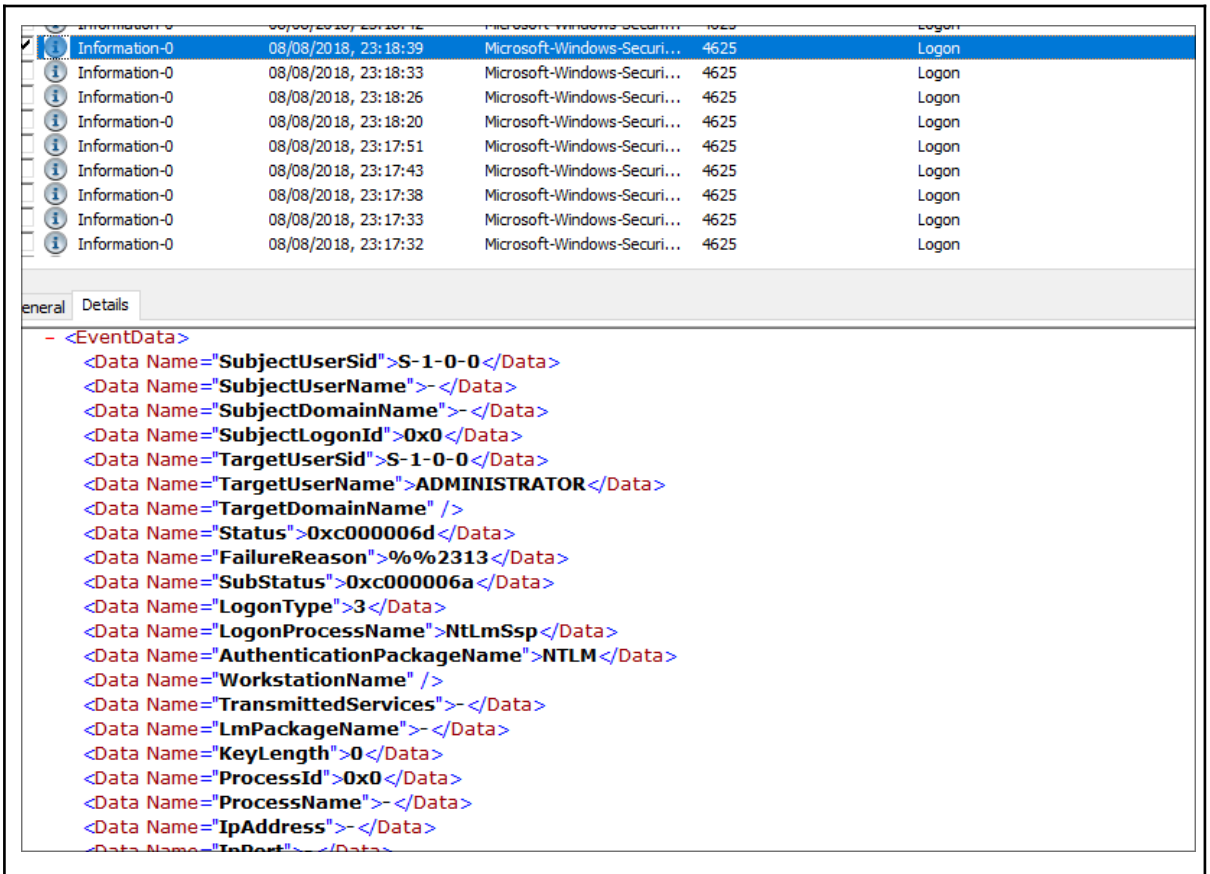


Figura 18: Captura de uno de los múltiples accesos fallidos observados.

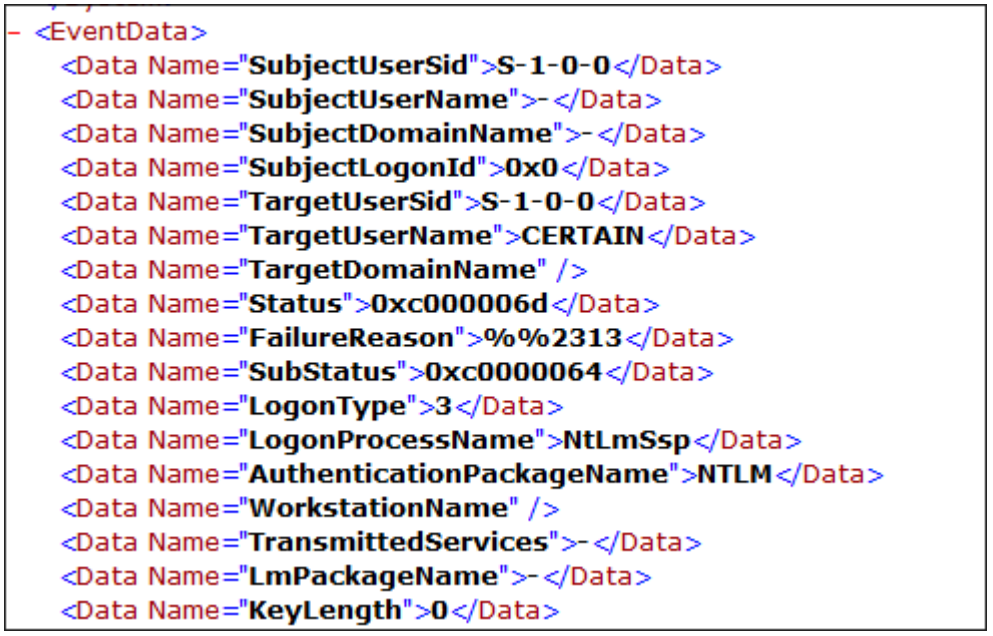


Figura 19: Captura de otro de los múltiples accesos fallidos observados.

Esto no corresponde estrictamente a conexiones remotas fuera del horario laboral, pero son indicios de actividad sospechosa y prohibida.

Para comprobar si existe el suceso pedido utilizamos la misma herramienta pero filtrando por “Succesfull Logon” y observamos lo siguiente.

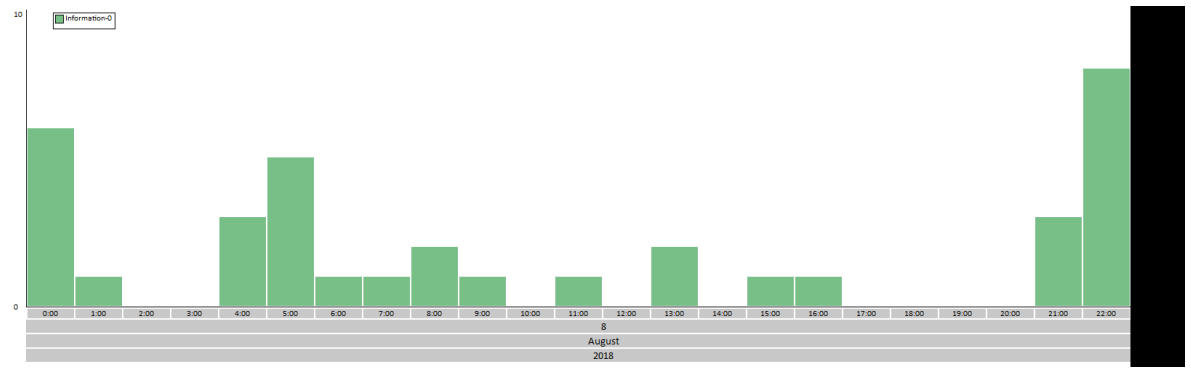


Figura 20: Gráfica de sesiones iniciadas correctamente por horario.

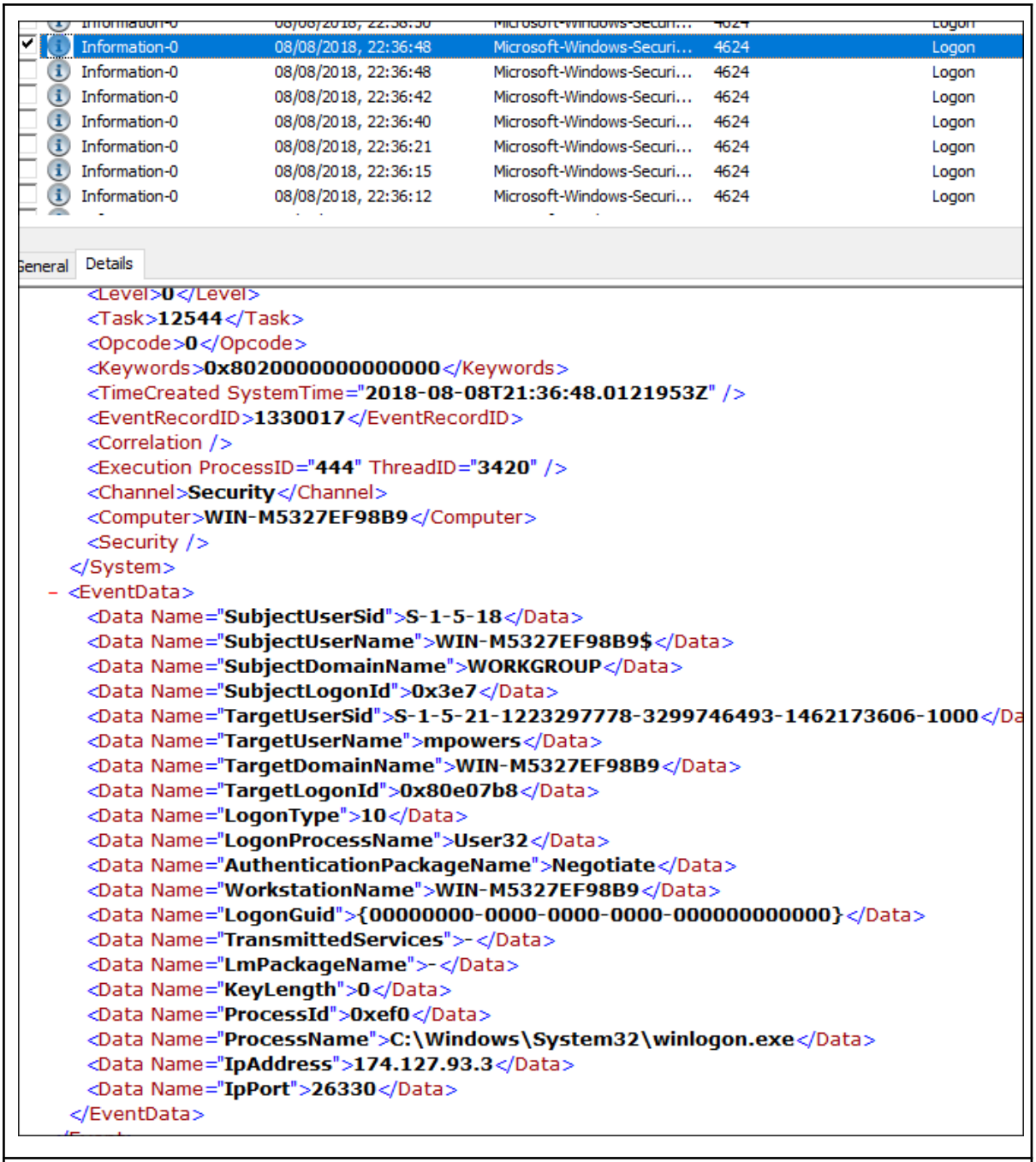


Figura 21: Ejemplo de nicios de sesión remoto.

Aquí podemos ver entre los múltiples inicios de sesión como muchos de ellos se han realizado fuera del horario laboral (esto también ocurre en Julio), y si vemos algunos de los ejemplos comprobamos que efectivamente muchos de los intentos de inicio de sesión se han hecho de forma remota, esto lo podemos saber con el campo “LogonType: 10” y la existencia de una dirección y puerto IP.

3.4. Llegados hasta aquí, ¿podemos afirmar que el empleado ha incumplido las normas internas de la empresa? Justifica razonadamente tu respuesta.

Sí, podemos afirmar razonadamente que el empleado ha incumplido las normas internas de la empresa. A lo largo del análisis hemos identificado que el usuario principal del sistema es mpowers, y asociado a este se han detectado tanto la instalación de programas no permitidos como F-response y PrivaZer, como múltiples inicios de sesión fuera del horario laboral establecido. Además, se han observado conexiones remotas (logon type 10) con IP y puerto, lo cual refuerza la sospecha de uso indebido. A esto se suma un volumen elevado de intentos fallidos de inicio de sesión, lo que indica actividad anómala por el empleado u otro actor externo malicioso. Todo ello supone una vulneración clara de las políticas de uso aceptable impuestas por la empresa.