

Ciberseguridad - Práctica 2

Auditoría e Informática forense

Alejandro Monterrubio Navarro

Esther Pérez Gil

Grupo 2462 - Pareja 2

Índice

Introducción y objetivos	2
Parte 1: Análisis de un equipo involucrado en un delito	3
Fase 1: Creación del documento de cadena de custodia	3
Fase 2: Clonado del disco duro	4
Preparación de la máquina virtual	4
Clonado del disco duro	4
Verificación de hashes	7
Fase 3: Estudio de artefactos forenses de actividad del usuario	9
Papelera de reciclaje	9
Navegador web	12
Informe de errores de Windows	15
Inicios de sesión con credenciales	16
Ficheros log de dispositivos USB	17
Fase 4: Conclusiones	19
Parte 2: InmoHouse	20
Objetivo	20
Análisis	20
Puesta en marcha	20
Descarga y ejecución de programas no permitidos	21
Conexiones remotas	25
Conclusiones	26
¿Se han utilizado programas no permitidos por las políticas de la empresa?	26
¿Se han realizado conexiones remotas fuera del horario laboral por parte de la empresa?	26
¿Ha incumplido el empleado las normas internas de la empresa?	26
Conclusiones personales	27



Introducción y objetivos

En esta segunda práctica, compuesta por dos partes, se va a desarrollar el trabajo de perito forense informático.

La primera parte tiene un objetivo preparatorio, donde se va a examinar un disco duro involucrado en un delito informático. Para ello primero se elaborará un documento de cadena de custodia. Más tarde, se hará un clonado del disco duro del ordenador, verificando los hashes del disco original y de la copia. Finalmente se procederá a hacer un estudio de cinco artefactos forenses.

La segunda parte busca aplicar los conocimientos aprendidos hasta el momento. Se dispone de la imagen del disco duro del ordenador de un empleado de la inmobiliaria InmoHouse, del cual se sospecha que ha incumplido las políticas de uso de los dispositivos TI. El objetivo es analizar la unidad y averiguar si se han descargado, instalado y ejecutado programas no permitidos, o si han realizado borrados de información, ejecuciones de comandos o conexiones al sistema fuera del horario laboral.

Parte 1: Análisis de un equipo involucrado en un delito

Fase 1: Creación del documento de cadena de custodia

A continuación se incluye la cadena de custodia¹ del equipo Windows involucrado en un delito informático.

Cadena de custodia				
Nombre	Fecha	Hora	Actividad de custodia sobre las muestras	Incidencias
Juan José Sánchez	13/03/24	16:00	Subida del sandbox a Moodle	Ninguna
Esther Pérez	14/03/24	16:00	Descarga del sandbox de Moodle a ordenador personal	Ninguna
Alejandro Monterrubio	14/03/24	17:25	Descarga del sandbox de Moodle a ordenador personal y ejecución	Ninguna
Esther Pérez	25/03/24	12:00	Ejecución del sandbox, eliminación del fichero malware y adición de artefactos forenses	Ninguna
Esther Pérez	25/03/24	12:10	Inicio del clonado del disco duro	Ninguna
Esther Pérez	25/03/24	15:00	Finalización del clonado del disco duro	Ninguna
Alejandro Monterrubio y Esther Pérez	25/03/24	16:00	Reparto de la carpeta del caso que contiene la imagen	Ninguna

Nota: Se va a considerar que el equipo Windows original es el generado tras eliminar el malware y añadir los artefactos forenses, para simular que ha sido utilizado previamente por una persona.

¹ <https://aeaof.com/media/revista/2/4.%20EL%20DOCUMENTO%20DE%20CADENA%20DE%20CUSTODIA.pdf>

Fase 2: Clonado del disco duro

Preparación de la máquina virtual

Para el clonado del disco duro se va a utilizar el sandbox de Windows 11 proporcionado para el laboratorio 5: análisis dinámico de malware. A su vez, para simular que la máquina virtual era un ordenador utilizado por alguien previamente y poder tener artefactos forenses que estudiar más adelante, se han hecho las siguientes acciones:

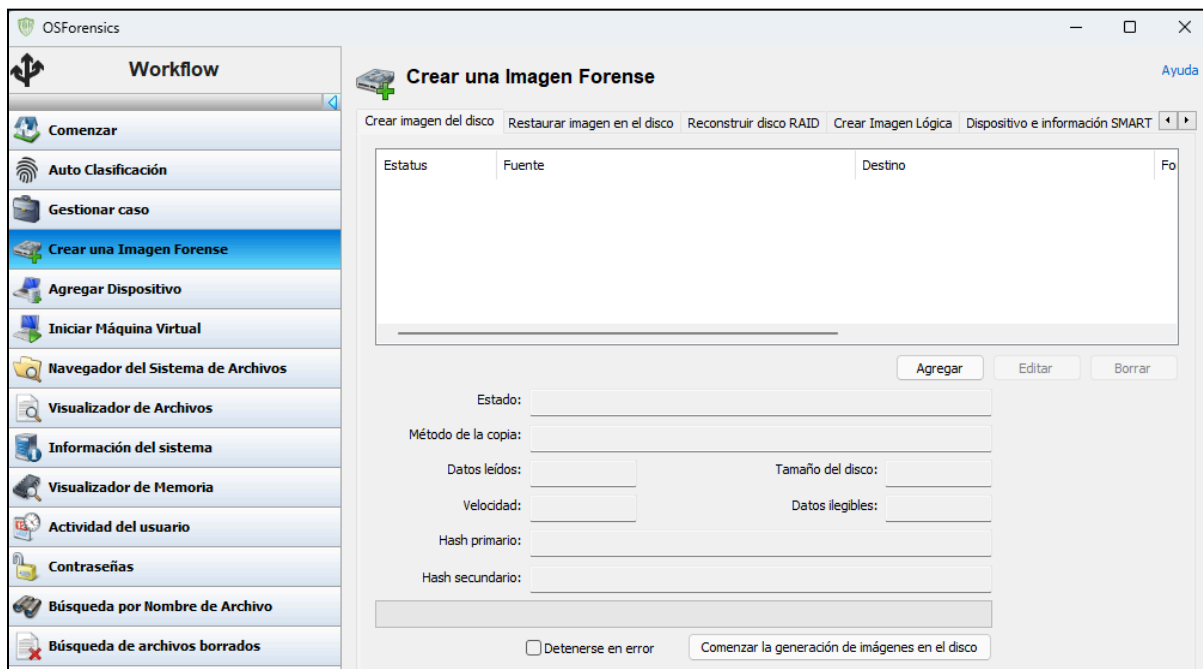
1. Eliminar el fichero “Malware”.
2. Buscar “perro salchicha” en Microsoft Edge.
3. Guardar una imagen en el escritorio con el nombre “perro”.
4. Guardar como favorito en el buscador la web de la imagen guardada.
5. Acceder a la página de extensiones de Microsoft Edge.
6. Añadir al buscador la extensión “Web paint online”.
7. Introducir un USB y guardar en el escritorio una imagen que contenía llamada “gato”.
8. Mandar a la basura las imágenes “perro” y “gato”.
9. Eliminar definitivamente la imagen “perro” (el malware y la imagen del gato se mantienen en la basura).
10. Expulsar el USB.

Clonado del disco duro

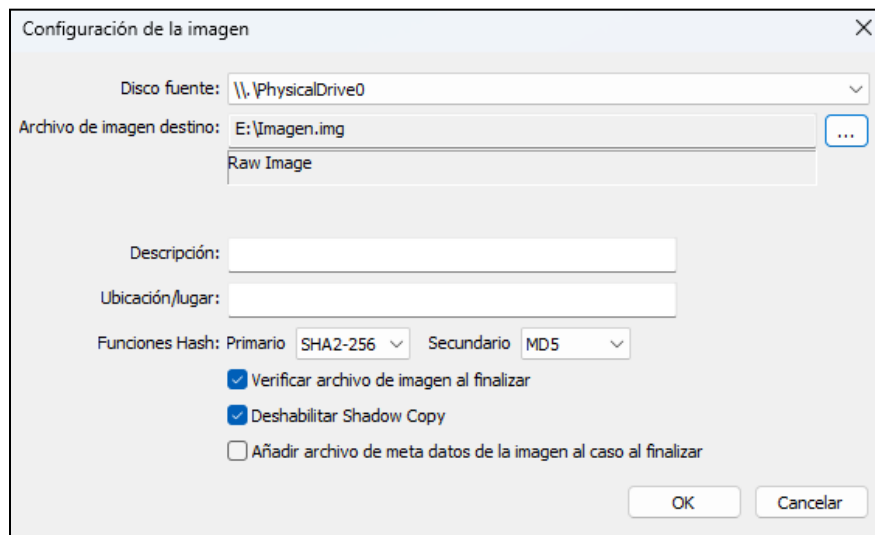
En primer lugar, se introduce en la máquina virtual con el disco a clonar un USB con el programa *OSForensics*², y se ejecuta.

Primero, en el menú de la izquierda se selecciona la opción “Crear una Imagen Forense”.

² <https://www.osforensics.com/>



Después, se selecciona la opción “Agregar”, y seleccionamos el disco duro a clonar, el lugar donde guardar la imagen (en este caso el USB) y el hash que queremos que se genere, en este caso SHA2-256 y MD5.



Una vez añadida la configuración del disco a clonar, se procede con el clonado.

Crear una Imagen Forense Ayuda

Crear imagen del disco Restaurar imagen en el disco Reconstruir disco RAID Crear Imagen Lógica Dispositivo e información SMART

Estatus	Fuente	Destino	Fo
Imaging...	\\.\PhysicalDrive0	E:\Imagen.img	Ra

Agregar Editar Borrar

Estado: Copying (48 Minutes Remaining)

Método de la copia: Direct Sector Copy (no lock)

Datos leídos: 128.0 MB Tamaño del disco: 64.00 GB

Velocidad: 22.69 MB/s Datos ilegibles: None

Hash primario: 9c613bc98e2b6c5346fe0dec99e10381758b34c50bf95cd49359086364d0bf5d

Hash secundario: af6de762abd1610967c36d512453e21f

☐ Detenerse en error Cancel

Una vez se ha creado la imagen del disco duro, se puede extraer el USB y apagar la máquina virtual, para así evitar manipular accidentalmente el disco original. En el ordenador donde realizaremos el análisis forense procedemos a crear un nuevo caso.

Nuevo caso Ayuda

Descripción de la evidencia Cadena de custodia Campos personalizados Relato del caso

Datos básicos del caso Categorías del caso Datos sobre Delitos & Custodia

Nombre del caso: CiberParte1

Case Type: Criminal

Investigador:

Organización:

Detalles de contacto:

Zona horaria: Local (UTC +1:00) Brussels, Copenhagen, Madrid, I ☒ Account for Daylight Saving Time

Formato de fecha: 25/03/2024 (Default) ☐ Display timezone on dates

Unidad por defecto: C:\ [Local]

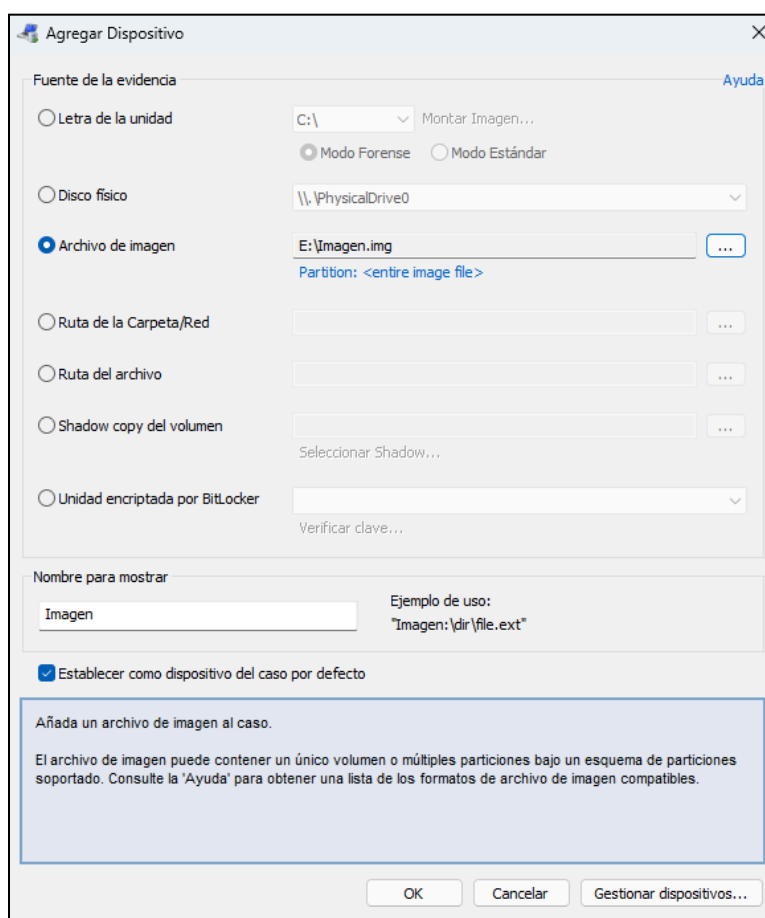
Tipo de obtención:
☐ Obtención en vivo de la máquina actual
☒ Registrar disco(s) de otra máquina

Carpeta del caso:
☐ Ubicación por defecto ☒ Ubicación personalizada
E:\Caso\ Buscar

☒ Registrar actividad del caso ☐ Permitir dispositivo USB Wr

OK Cancelar

Más adelante se añade la imagen que acabamos de generar al caso.



Ya disponemos de un caso forense con la imagen del disco correspondiente. A continuación se compararán los hashes, para verificar que el disco original y el clonado contienen lo mismo y no han sido manipulados.

Verificación de hashes

Para verificar³ que la copia del disco y el original son idénticos en contenido y que no han sido modificados, se comparan sus hashes. Para ello, desde *OSForensics* se accede a “Hashing de archivos -> Verificar/Crear Hash”. Se selecciona la imagen del disco creada anteriormente y se espera a que finalice de crear el hash para el disco y sus contenidos.

³ <https://www.osforensics.com/faqs-and-tutorials/how-to-check-md5-hash-checksum-volume-disk-image.html>

Hashing de archivos

Hash sets: Verificar/Crear Hash

☐ Archivo ☒ Volumen ☐ Texto

Volumen

Imagen: [Image File (Entire image)] ... **Detener**

Función Hash: SHA2-256 Función Hash secundaria: MD5

☐ Volumen de salida de mayúsculas

Progreso

Datos pasados por el proceso de hash: 18.70 GB

Hash calculado

Primario: 84058ea835877cd99ab0364e857bf2693674c36542853fe1096175c13388f6a0 (SHA2-256)

Secundario: 87727892abe8df9a0219347b41624c43 (MD5)

Hash de comparación:
Hash de comparación es un campo opcional

Una vez generado el hash, se copia y pega en el campo “Hash de comparación”. Si los hash coinciden y, efectivamente, los contenidos del disco y la imagen generada son los mismos y ésta no ha sido manipulada, aparece un símbolo de confirmación.

Hashing de archivos

Hash sets: Verificar/Crear Hash

☐ Archivo ☒ Volumen ☐ Texto

Volumen

Imagen: [Image File (Entire image)] ... **Calcular**

Función Hash: SHA2-256 Función Hash secundaria: SHA3-256

☐ Volumen de salida de mayúsculas

Progreso

Datos pasados por el proceso de hash: 64.00 GB

Hash calculado

Primario: 61357a6fc308e100b7b8d9b6ff7ebce92dd38170b234960c96f752c1b0995809 (SHA2-256)

Secundario: 4f3551e4fb38a7daaf94b5497f466417 (MD5)

Hash de comparación: 61357a6fc308e100b7b8d9b6ff7ebce92dd38170b234960c96f752c1b0995809

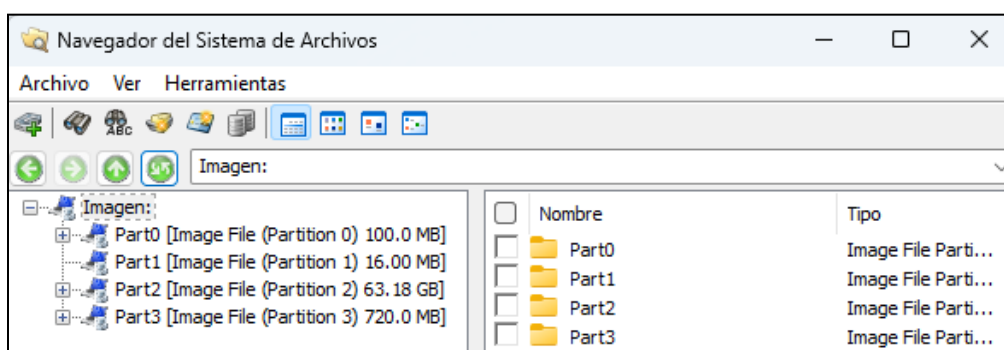
Los hashes (primarios) son iguales

Ya se pueden analizar los cinco artefactos forenses elegidos.

Fase 3: Estudio de artefactos forenses de actividad del usuario

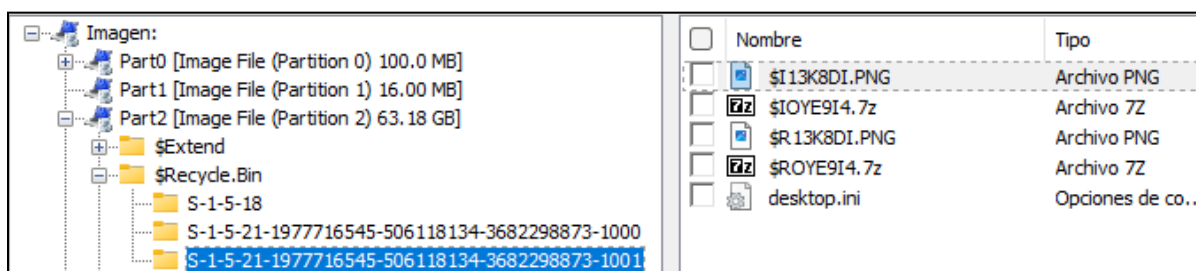
Tras investigar ^{4 5 6} sobre los distintos artefactos forenses hemos elegido los siguientes: papelera de reciclaje, navegador web, informe de errores de Windows, inicios de sesión con credenciales y ficheros log de dispositivos USB. Previamente habíamos colocado artefactos forenses adrede para poder buscarlos ahora; estos artefactos están relacionados con la papelera, navegador web y ficheros log de dispositivos USB.

Para estudiar estos artefactos, desde *OSForensics* se accede a la imagen del disco con sus distintas particiones (en este caso 4). Accediendo a las distintas carpetas de las particiones podremos buscar información en relación a los distintos artefactos.



Papelera de reciclaje

Para acceder a la papelera de reciclaje entramos en la partición 2 y en la carpeta “\$Recycle.Bin”. Aquí encontramos cinco archivos: dos imágenes, dos archivos comprimidos y el fichero “desktop.ini”, que aparece en la mayoría de carpetas.

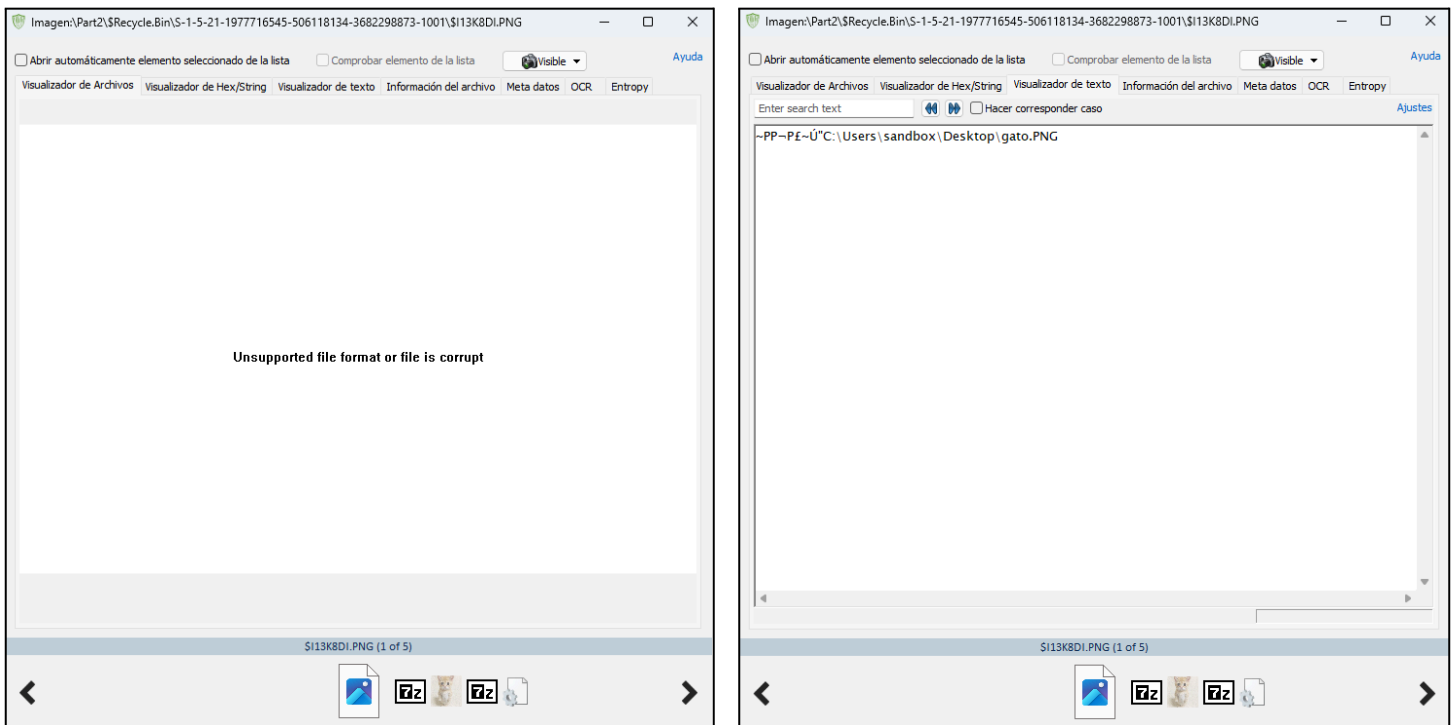


⁴ <https://www.geeksforgeeks.org/windows-forensic-analysis/>

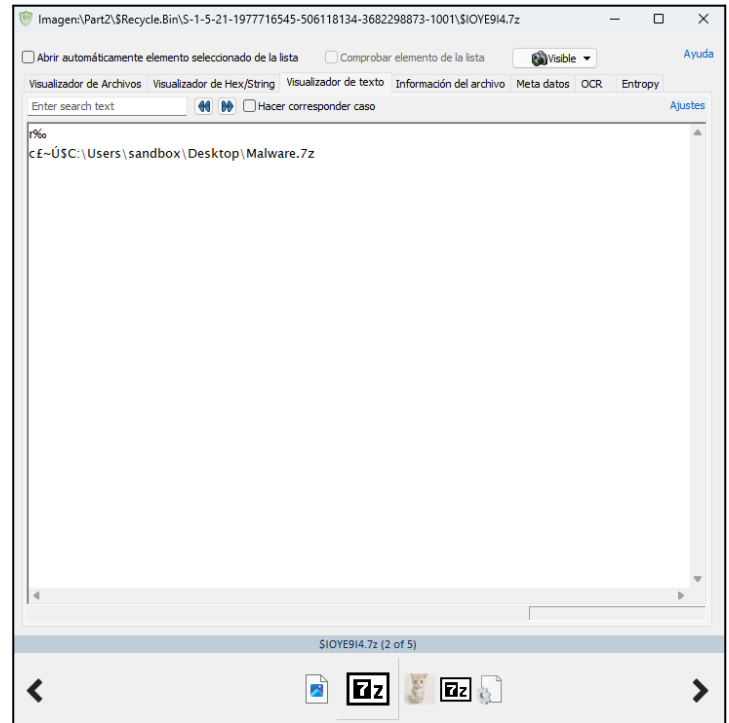
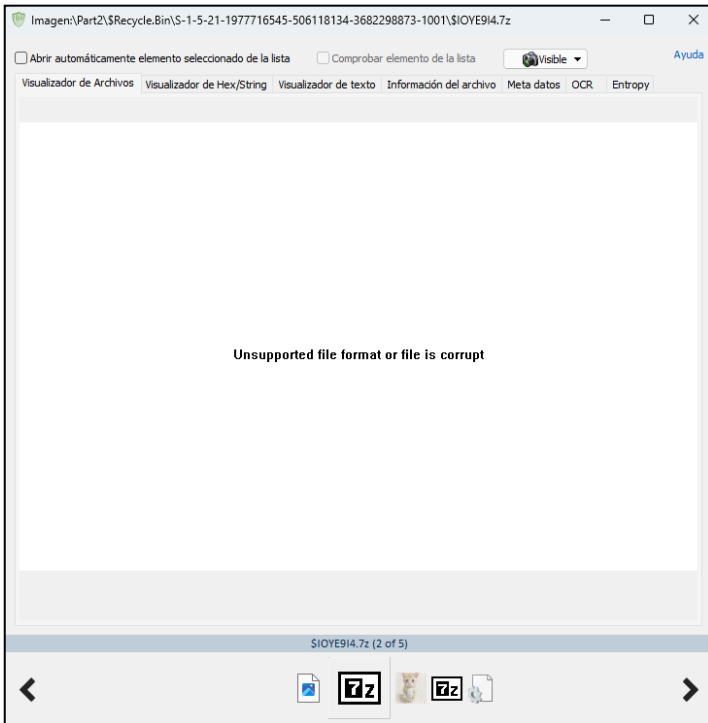
⁵ <https://gist.github.com/richaarya/d336fec34c600cc8ab8a51195289c99a>

⁶ <https://www.linkedin.com/pulse/windows-forensic-analysis-uncovering-digital-yugal-pathak-cyberyuvi--3tovf>

Si analizamos la primera imagen se abre una ventana donde poder ver en detalle los contenidos. El primer archivo no permite una visualización, sin embargo, si se visualiza el texto se puede ver que se corresponde a la imagen “gato.PNG”, que habíamos guardado desde el USB. A su vez, se puede apreciar en la parte inferior de las imágenes que el tercer archivo se corresponde con la visualización de la imagen “gato.PNG”, de modo que sí se ha podido recuperar pese a estar en la papelera de reciclaje. El primer fichero tiene un tamaño de 96B, mientras que el tercero son 261,1kB, de modo que podemos asumir que el primero es la previsualización que se vería en la papelera de reciclaje, y el tercero es la imagen en sí.



Si se analiza el segundo archivo, tampoco se permite una visualización, pero analizándolo como texto vemos que se trata del archivo “Malware.7z”, el que venía instalado con la máquina virtual. Podemos apreciar que el cuarto archivo tiene la misma extensión. El segundo tiene un tamaño de 100B y el cuarto de 34,4kB, de modo que se trata de nuevo de la previsualización de la papelera (especialmente considerando que en la imagen anterior también ocupaba 100B) y el archivo en sí, respectivamente.

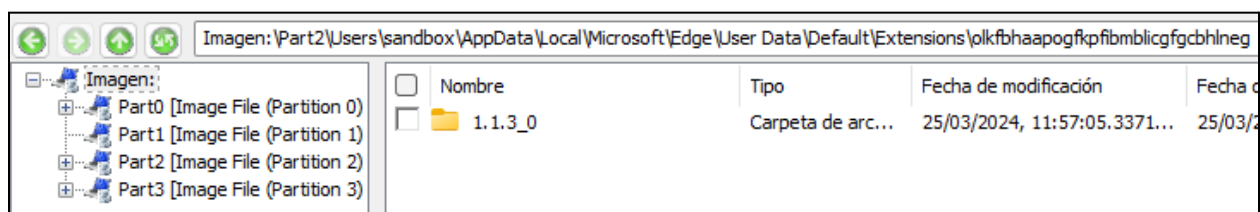


Desde la papelera de reciclaje no hemos podido encontrar la imagen “perro” que habíamos borrado definitivamente desde la papelera. Sin embargo, desde la opción “Búsqueda de archivos borrados” de *OSForensics* sí hemos podido encontrarla haciendo una búsqueda de ficheros jpg.

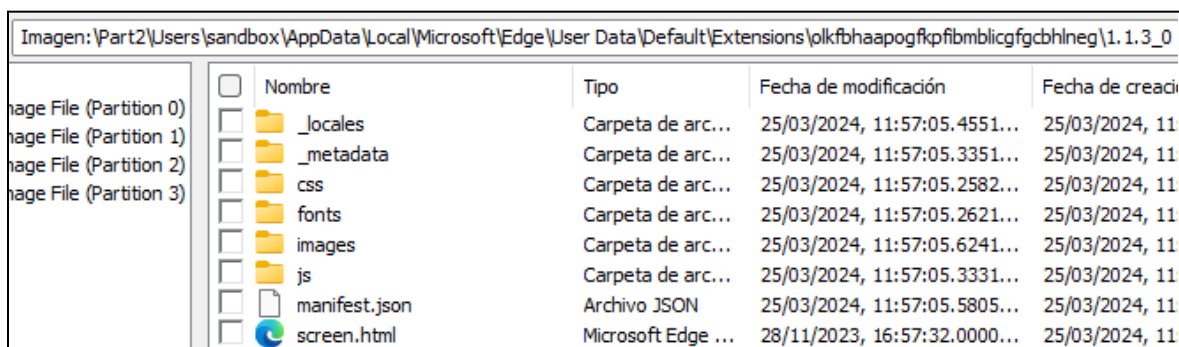


Navegador web

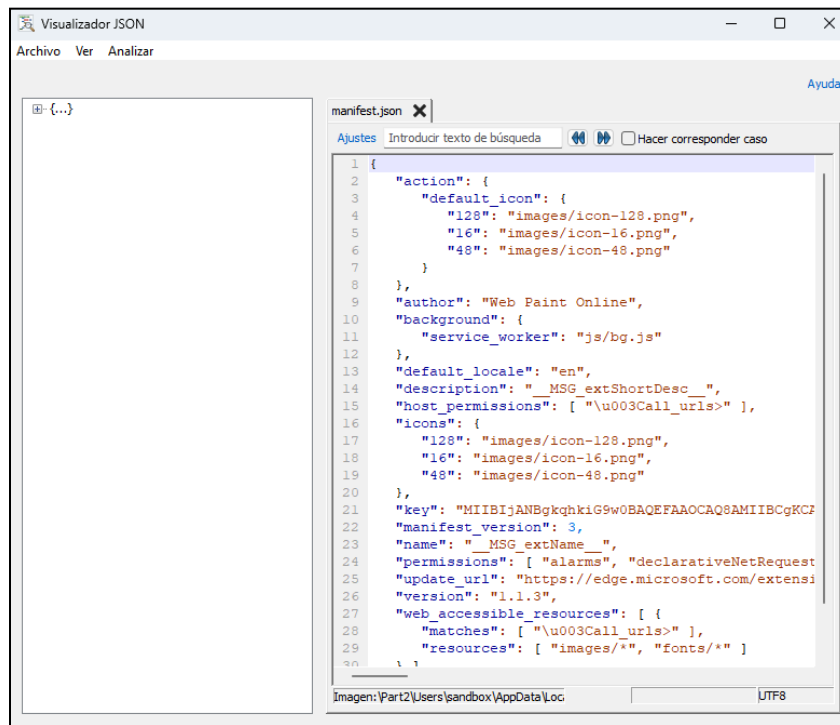
Al preparar la máquina virtual nos descargamos la extensión *Web Paint Online*. Para visualizar a las extensiones de *Microsoft Edge* se accede a la partición 2 y a la ruta Users->sandbox->AppData->Local->Microsoft->Edge->User Data->Default->Extensions. Dentro de la ruta encontramos una carpeta con un nombre muy complicado, y dentro de ella otra carpeta con lo que parece ser la versión de un programa.



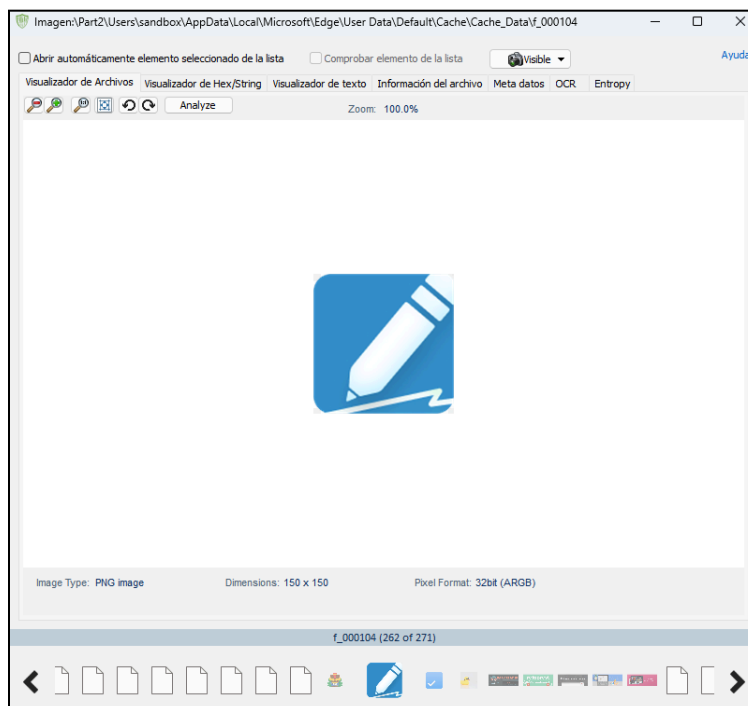
Al acceder a la carpeta “1.1.3_0” encontramos otras subcarpetas con información que a primera vista no aporta información de la extensión que es, si es que realmente es una.



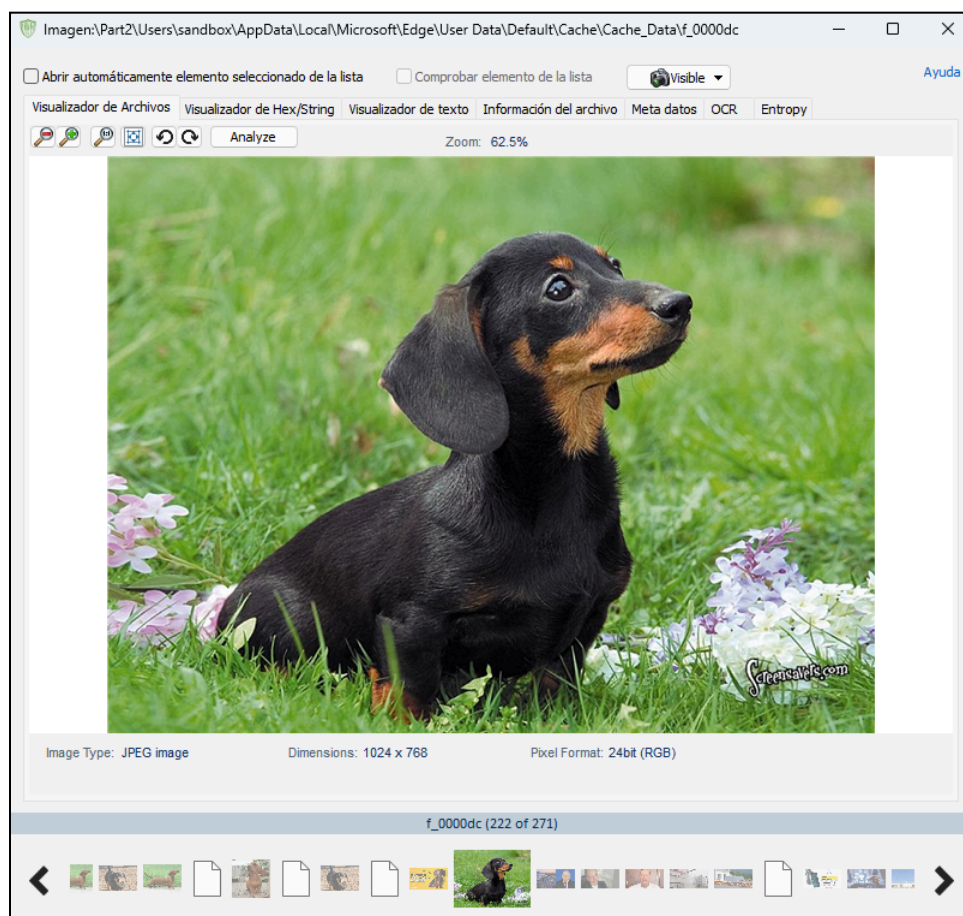
Al acceder al fichero “manifest.json” podemos ver que el autor es “Web Paint Online”, confirmando que se trata de la extensión añadida.



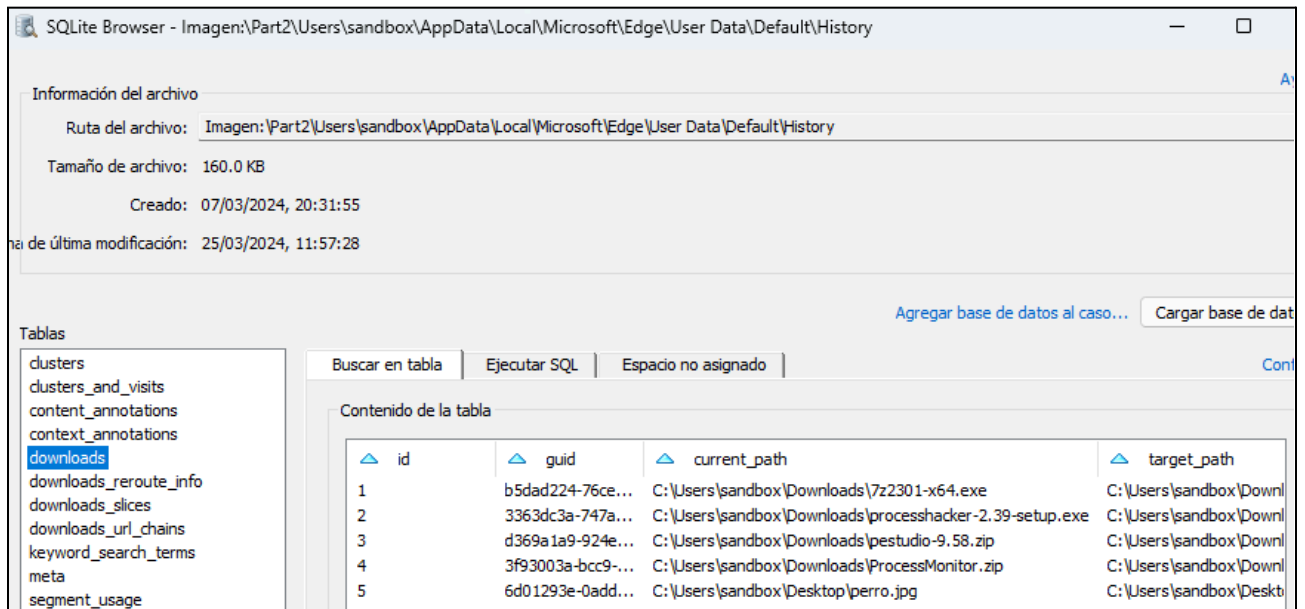
A su vez, accediendo Users->sandbox->AppData->Local->Microsoft->Edge->User Data->Default->Cache->Cache_Data podemos ver la caché de *Microsoft Edge*, siendo uno de los ficheros la imagen del logo de la extensión anterior.



En esta misma ruta de la caché de *Microsoft Edge*, si seguimos analizando los archivos podemos encontrar la imagen “perro” que habíamos descargado previamente, junto con el resto de imágenes que aparecieron en la búsqueda (algunas de ellas se pueden ver en la parte inferior de la imagen).

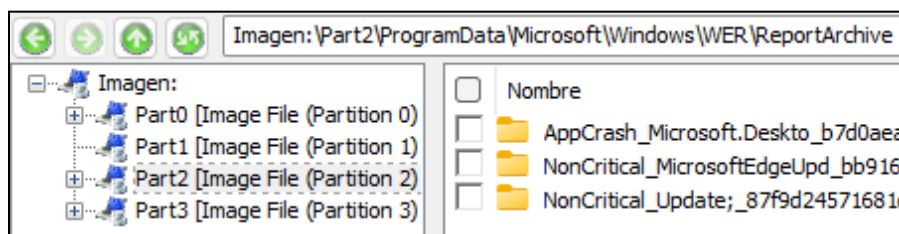


Si accedemos a la ruta del historial de *Microsoft Edge*, Users->sandbox->AppData->Local->Microsoft->Edge->User Data->Default->History encontramos un fichero SQL, pero analizando el apartado “Downloads” podemos ver que la última línea se refiere a la descarga de la imagen “perro.jpg”.

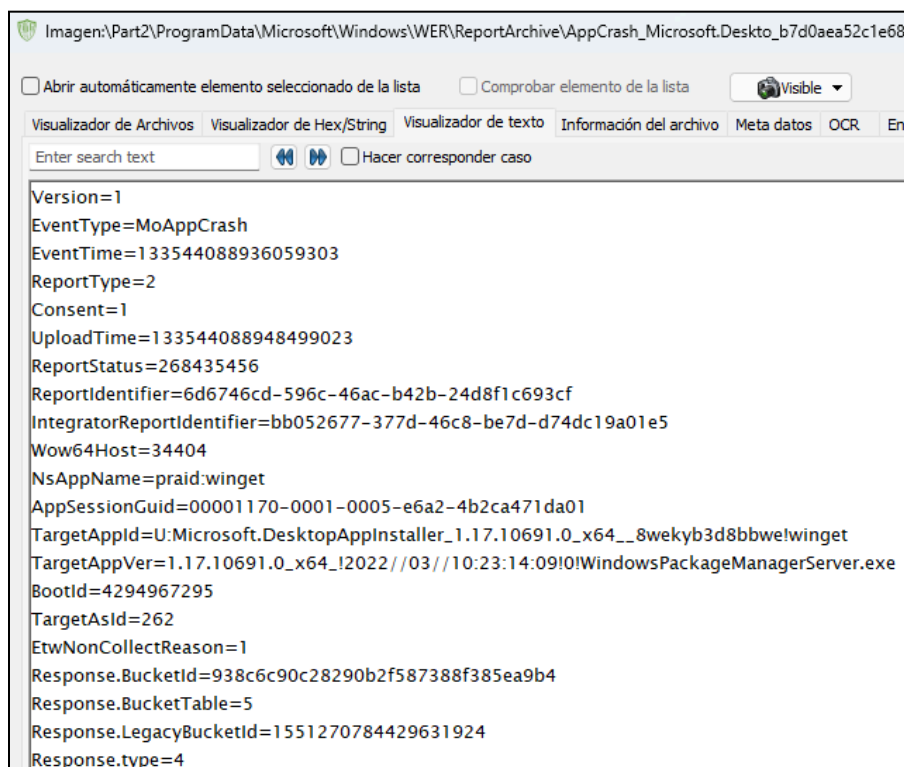


Informe de errores de Windows

El informe de errores de Windows proporciona información de fallos que se producen en las aplicaciones, fallos del núcleo o fallos en programas maliciosos. Para acceder a este registro se hace en la partición 2 desde la ruta ProgramData->Microsoft->Windows->WER->ReportArchive donde hay tres carpetas relativas a fallos de aplicaciones, y fallos no críticos de *Microsoft Edge* y actualizaciones, respectivamente.



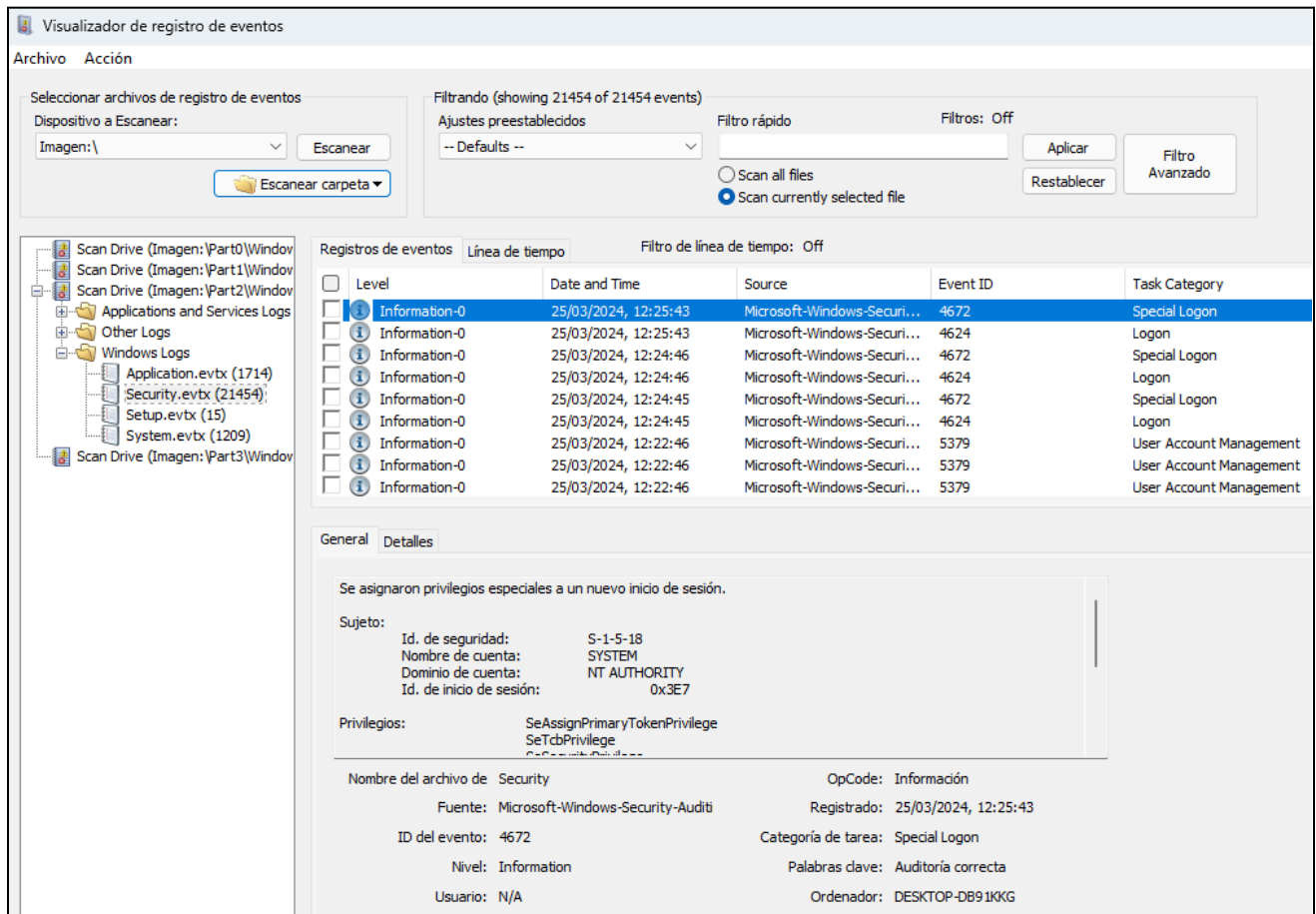
Dentro de cada carpeta hay un fichero "Report.wer" con la información. Por ejemplo del fichero de la primera carpeta informa de un fallo de tipo "MoAppCrash".



Inicios de sesión con credenciales

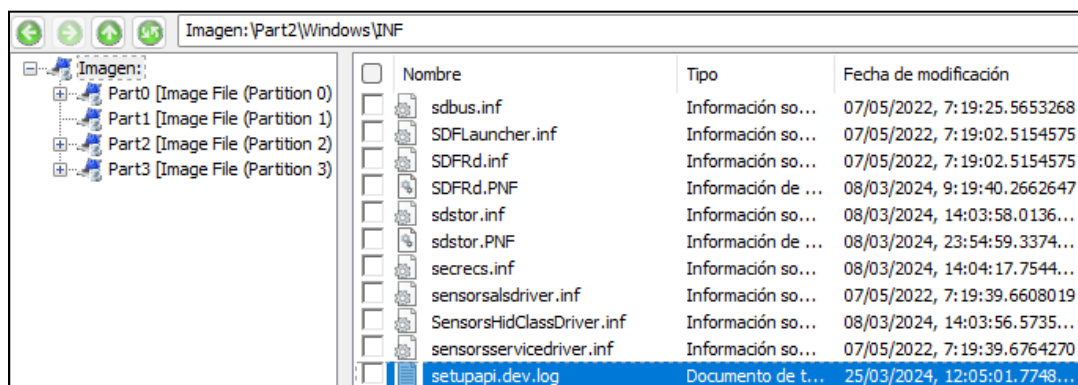
Es posible acceder a los inicios de sesión⁷ donde se han utilizado credenciales explícitas (aquellas que no están activas y han sido seleccionadas para determinadas acciones). Para ello se accede desde la partición 2 a la ruta Windows->System32->winevt->Logs->Security.evtx. Ya que no se ha iniciado sesión en ningún programa o sitio web, la mayoría de la información hace referencia a credenciales utilizadas para iniciar sesión en la propia máquina virtual, o para ejecutar programas.

⁷ <https://github.com/Psmths/windows-forensic-artifacts/tree/main>



Ficheros log de dispositivos USB

Para acceder al log con toda la información de los USB introducidos se accede nuevamente a la partición 2, a la ruta Windows->INF->setupapi.dev.log.



El fichero viene ordenado por fechas, de modo que hay que irse al final para ver las acciones más recientes. La última acción se corresponde con un USB de la marca SanDisk a las 12:03. Esta entrada se corresponde con el momento en el que se introdujo el USB para guardar la imagen “gato” y posteriormente para ejecutar *OSForensics* para realizar el clonado del disco.

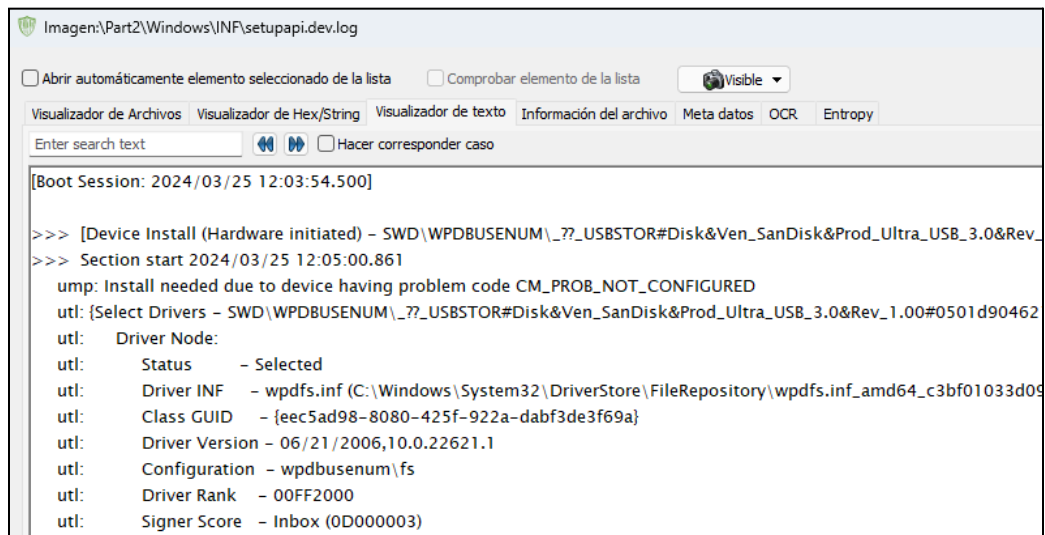


Imagen:\Part2\Windows\INF\setupapi.dev.log

☐ Abrir automáticamente elemento seleccionado de la lista ☐ Comprobar elemento de la lista Visible

Visualizador de Archivos Visualizador de Hex/String Visualizador de texto Información del archivo Meta datos OCR Entropy

Enter search text ⏮ ⏭ ☐ Hacer corresponder caso

```
[Boot Session: 2024/03/25 12:03:54.500]

>>> [Device Install (Hardware initiated) - SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_SanDisk&Prod_Ultra_USB_3.0&Rev_1.00#0501d90462]
>>> Section start 2024/03/25 12:05:00.861
ump: Install needed due to device having problem code CM_PROB_NOT_CONFIGURED
utl: {Select Drivers - SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_SanDisk&Prod_Ultra_USB_3.0&Rev_1.00#0501d90462}
utl:   Driver Node:
utl:     Status      - Selected
utl:     Driver INF   - wpdfs.inf (C:\Windows\System32\DriverStore\FileRepository\wpdfs.inf_amd64_c3bf01033d09
utl:     Class GUID    - {eec5ad98-8080-425f-922a-dabf3de3f69a}
utl:     Driver Version - 06/21/2006,10.0.22621.1
utl:     Configuration - wpdfbusenum\fs
utl:     Driver Rank   - 00FF2000
utl:     Signer Score   - Inbox (0D000003)
```

Fase 4: Conclusiones

La herramienta *OSForensics* ha sido muy cómoda y fácil de utilizar y nos ha permitido crear una imagen del disco duro, comprobar los hashes y analizar los artefactos forenses elegidos. A continuación se exponen las conclusiones del estudio de artefactos forenses.

En relación a la papelera de reciclaje, hemos sido capaces de recuperar la información que había accediendo desde las carpetas disponibles en la imagen del disco duro. Para acceder a la imagen que habíamos borrado definitivamente desde la papelera hemos tenido que recurrir a la funcionalidad de *OSForensics* para recuperar archivos borrados.

Sobre el navegador web, hemos encontrado la extensión instalada. También en la caché estaba la imagen que habíamos descargado, y en el historial constaba una descarga de un archivo “perro.jpg”.

Acerca del informe de errores de Windows, hemos encontrado tres carpetas distintas, relativas a fallos no críticos de *Microsoft Edge*, actualizaciones y fallos de aplicaciones, encontrando en esta última un fallo del tipo “MoAppCrash”.

Relativo a los inicios de sesión con credenciales únicamente hemos encontrado aquellas relativas al sistema, como el propio inicio de sesión a la máquina virtual. De haber iniciado sesión en programas o webs, aparecería esa información también.

Respecto al registro de USBs introducidos, hemos encontrado la marca del USB y hora en la que se introdujo para guardar la imagen “perro” y ejecutar *OSForensics*.

Parte 2: InmoHouse

Objetivo

El objetivo de esta parte de la práctica es poder determinar si un empleado de InmoHouse ha hecho un uso indebido del ordenador de la empresa. Para ello habrá que analizar la imagen del disco duro que proporciona la empresa en busca de uso de programas no permitidos o conexiones remotas en horario no laboral (9h - 19h).

Análisis

Puesta en marcha

Nuevamente utilizamos *OSForensics* para crear un caso y añadimos la imagen que nos proporciona la empresa.

Nuevo caso

Ayuda

Descripción de la evidencia	Cadena de custodia	Campos personalizados	Relato del caso
Datos básicos del caso	Categorías del caso	Datos sobre Delitos & Custodia	

Nombre del caso: InmoHouse

Case Type: Criminal

Investigador:

Organización:

Detalles de contacto:

Zona horaria: Local (UTC +1:00) Brussels, Copenhagen, Madrid, I ☒ Account for Daylight Saving Time

Formato de fecha: 27/03/2024 (Default) ☐ Display timezone on dates

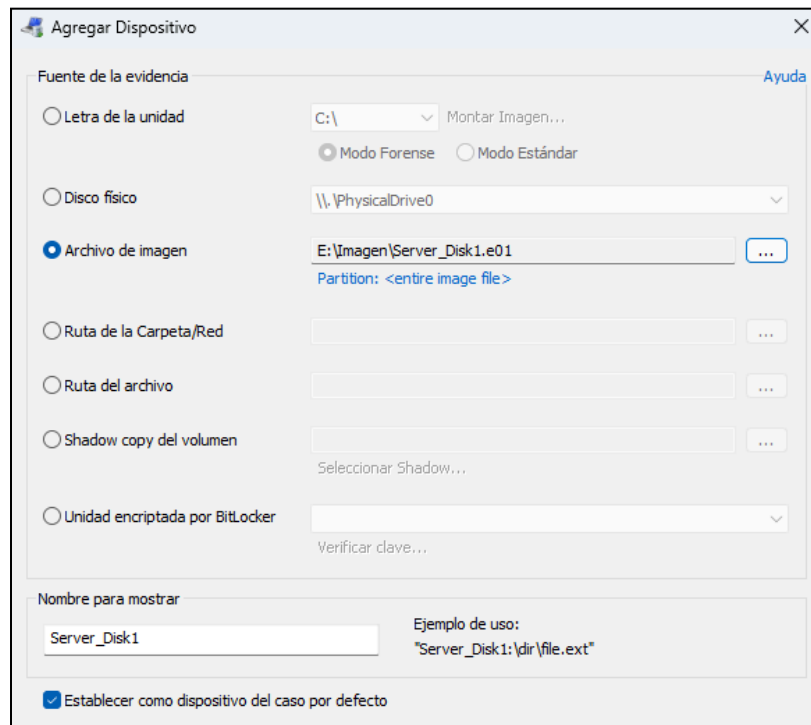
Unidad por defecto: C:\ [Local]

Tipo de obtención: ☐ Obtención en vivo de la máquina actual ☒ Registrar disco(s) de otra máquina

Carpeta del caso: ☐ Ubicación por defecto ☒ Ubicación personalizada

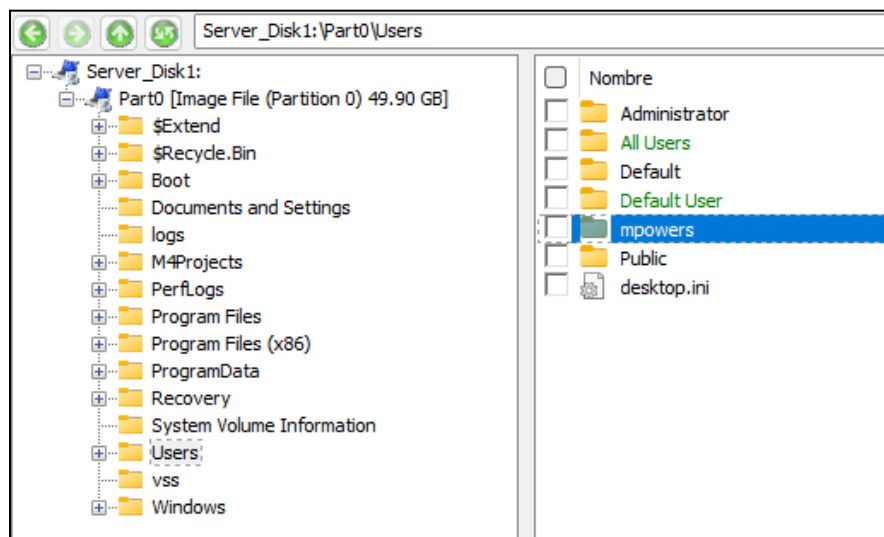
E:\InmoHouse\

☒ Registrar actividad del caso ☐ Permitir dispositivo USB Wri



Descarga y ejecución de programas no permitidos

Comenzamos mirando los usuarios registrados en el ordenador, donde nos llama la atención “mpowers”, que no es un usuario que aparezca por defecto, por lo que podemos dar por hecho que se trata del usuario del trabajador.



Dentro del usuario, en la ruta correspondiente al historial de búsquedas de *Google Chrome* “Users\mpowers\AppData\Local\Google\Chrome\User Data\Default\History” encontramos que ha buscado dos programas que limpian datos del ordenador: “CCleaner” y “Privazer”, siendo este último enfocado a la limpieza de trazas de actividades pasadas. Esto nos da a entender que el empleado realizó alguna acción no permitida por las políticas de la empresa y tenía intenciones de ocultarlo. Sin embargo, hasta ahora hay muestras de haber buscado esos programas, pero no de haberlos descargado.

SQLite Browser - Server_Disk1:\Part0\Users\mpowers\AppData\Local\Google\Chrome\User Data\Default\History

Información del archivo

Ruta del archivo: Server_Disk1:\Part0\Users\mpowers\AppData\Local\Google\Chrome\User Data\Default\History

Tamaño de archivo: 116.0 KB

Creado: 16/07/2018, 19:16:30

Fecha de última modificación: 07/08/2018, 22:24:07

Tablas

- downloads
- downloads_slices
- downloads_url_chains
- keyword_search_terms
- meta
- segment_usage
- segments
- sqlite_sequence
- typed_url_sync_metadata
- urls
- visit_source
- visits

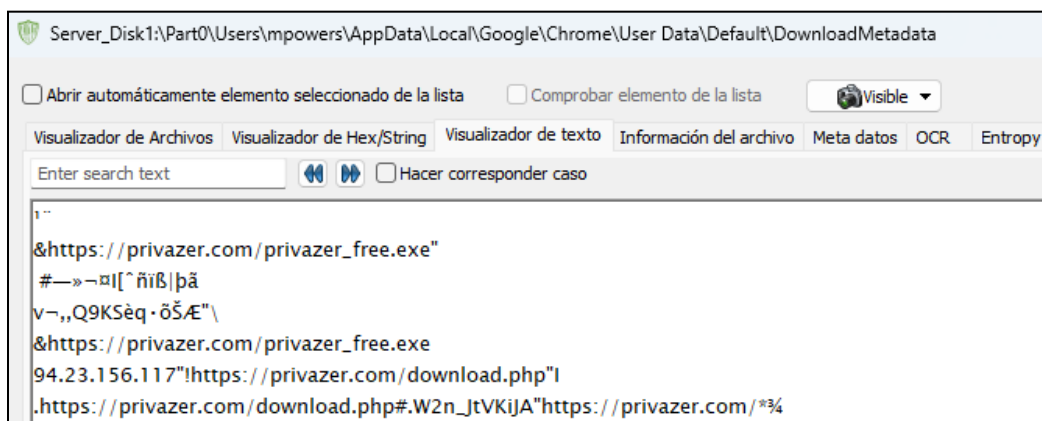
Buscar en tabla | Ejecutar SQL | Espacio no asignado

Contenido de la tabla

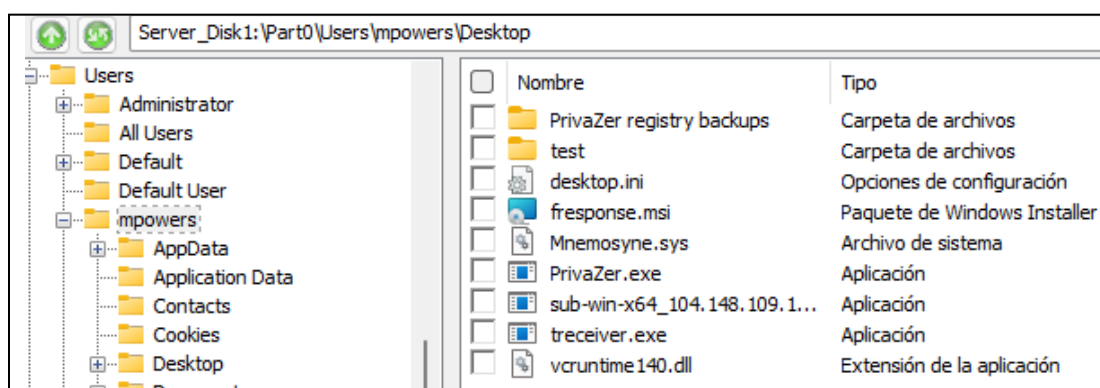
keyword_id	url_id	lower_term	term
2	1	notepad++	notepad++
2	6	ccleaner	ccleaner
2	10	privazy	privazy
2	11	privazer	privazer

Buscar en la tabla | Limpiar búsqueda

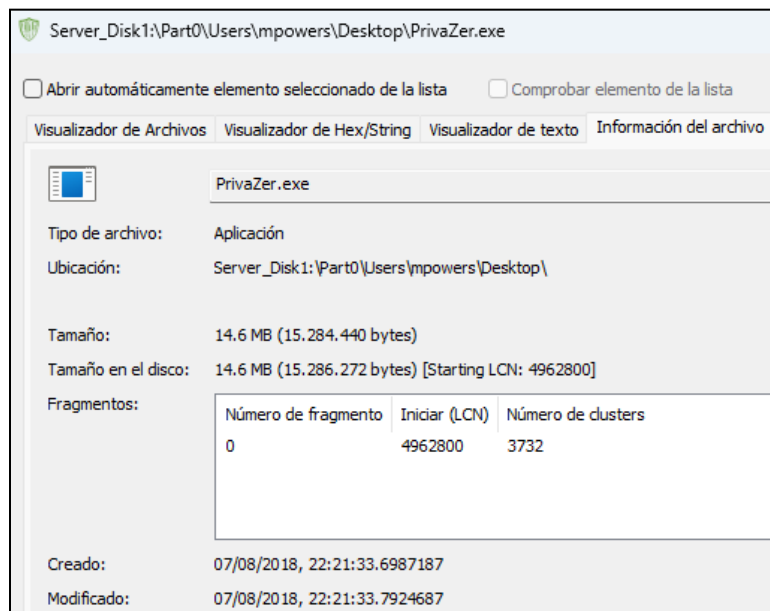
Comprobando el fichero de metadatos de descargas en *Google Chrome* desde la ruta “Users\mpowers\AppData\Local\Google\Chrome\User Data\Default\DownloadMetadata” se puede ver que hay registro de haber descargado el ejecutable de *Privazer* “privazer_free.exe”, confirmando que el empleado descargó programas no permitidos. A su vez, al tratarse de un programa pensado para borrar el rastro de ciertas actividades del ordenador, podemos pensar que ha estado haciendo alguna otra actividad no permitida. De haber ejecutado este programa, se habría borrado información, lo que también incumple las políticas de la empresa.



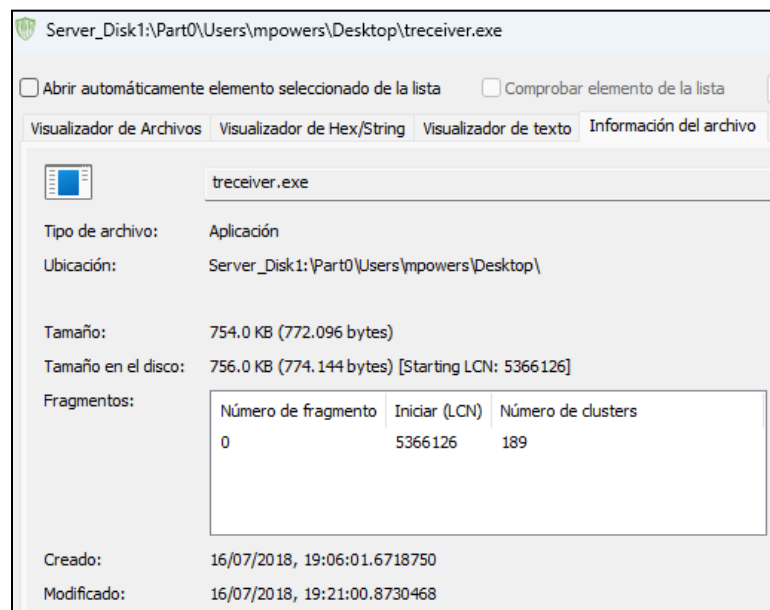
Comprobando ahora el escritorio (Users\mpowers\Desktop) vemos que están los backups del programa mencionado anteriormente, *PrivaZer*. Al haber backups podemos asumir que el empleado ejecutó el programa y eliminó datos, incumpliendo con la política de la empresa.



Además, entrando en los detalles del ejecutable “PrivaZer.exe”, vemos que se creó y modificó a las 22h, fuera del horario laboral.



También en el escritorio encontramos otro ejecutable llamado “treceiver.exe”, que fue creado y modificado más tarde de las 19h, nuevamente fuera del horario laboral.



No hemos encontrado información en internet sobre este programa, pero en el directorio “logs” encontramos un fichero “treceiver.log” con lo que parece ser una lista de pedidos a una empresa de reparto de comida a domicilio. Estas entradas en el log se producen durante julio y agosto del año 2018 en horario tanto laboral como no laboral.

Server_Disk1\Part0\logs\treceiver.log

☐ Abrir automáticamente elemento seleccionado de la lista ☐ Comprobar elemento de la lista

Visualizador de Archivos Visualizador de Hex/String Visualizador de texto Información del archivo Meta datos OCR Entropy

Enter search text

2018-07-23 14:37:55.262875 UTC	74.118.138.195:61500	4	["chicharron","chorizo","chorizo","chorizo"]
2018-07-23 14:38:18.184750 UTC	74.118.138.195:61501	5	["shrimp","al pastor","adobado","shrimp","barbacoa"]
2018-07-23 15:57:42.637875 UTC	74.118.138.195:61894	2	["al pastor","asado"]
2018-07-23 17:37:13.059750 UTC	74.118.139.108:53745	7	["fish","chorizo","barbacoa","chicharron","adobado","al pastor","chorizo"]
2018-07-23 17:38:05.512875 UTC	74.118.139.108:53747	7	["chicharron","beef tongue","barbacoa","adobado","carnitas","beef tongue","chorizo"]
2018-07-23 17:39:35.622250 UTC	74.118.139.108:53748	5	["barbacoa","chicharron","chorizo","chicharron","chorizo"]
2018-07-23 17:43:44.841 UTC	74.118.139.108:53749	6	["chicharron","chicharron","carnitas","shrimp","barbacoa","al pastor"]
2018-07-23 17:48:43.934750 UTC	74.118.139.108:53752	6	["beef tongue","carnitas","carnitas","adobado","chorizo","asado"]
2018-07-23 17:53:43.841 UTC	74.118.139.108:53753	5	["chicharron","barbacoa","adobado","chorizo","adobado"]
2018-07-23 18:07:16.544125 UTC	74.118.139.108:53791	3	["fish","chorizo","beef tongue"]
2018-07-23 18:12:43.559750 UTC	74.118.139.108:53792	8	["barbacoa","adobado","barbacoa","shrimp","adobado","chicharron","shrimp","adobado"]
2018-07-23 18:42:43.653500 UTC	74.118.139.108:53796	8	["shrimp","shrimp","barbacoa","al pastor","shrimp","carnitas","carnitas","beef tongue"]
2018-07-23 19:12:43.575375 UTC	74.118.139.108:53809	7	["chicharron","barbacoa","fish","barbacoa","al pastor","barbacoa","chorizo"]
2018-07-23 19:42:43.653500 UTC	74.118.139.108:53824	6	["carnitas","adobado","beef tongue","adobado","shrimp","al pastor"]
2018-07-23 20:12:43.637875 UTC	74.118.139.108:53828	7	["adobado","fish","adobado","asado","chorizo","shrimp","fish"]
2018-07-23 20:42:43.637875 UTC	74.118.139.108:53832	2	["asado","carnitas"]
2018-07-23 21:12:43.575375 UTC	74.118.139.108:53836	7	["carnitas","chorizo","al pastor","barbacoa","shrimp","al pastor","chicharron"]
2018-07-23 21:42:43.591 UTC	74.118.139.108:53841	6	["adobado","chorizo","barbacoa","chorizo","al pastor","fish"]
2018-07-23 22:12:43.669125 UTC	74.118.139.108:53844	5	["fish","beef tongue","carnitas","carnitas","al pastor"]
2018-07-23 22:42:43.747250 UTC	74.118.139.108:53848	8	["shrimp","barbacoa","asado","carnitas","asado","beef tongue","carnitas","asado"]
2018-07-23 23:12:43.622250 UTC	74.118.139.108:53853	3	["chorizo","adobado","carnitas"]
2018-07-23 23:42:45.731625 UTC	74.118.139.108:53856	5	["barbacoa","carnitas","adobado","fish","asado"]
2018-07-24 00:12:43.637875 UTC	74.118.139.108:53860	5	["barbacoa","adobado","chicharron","carnitas","barbacoa"]

Conexiones remotas

Para detectar posibles accesos remotos al ordenador fuera del horario laboral se accede a la ruta “Windows\System32\winevt\Logs” y al fichero “Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx”.

Podemos ver conexiones remotas del usuario “mpowers” fuera del horario laboral, empezando el día 16/07/18 y siendo las más recientes del día 08/08/18.

Registros de eventos Línea de tiempo Filtro de línea de tiempo: Off

<input type="checkbox"/> Level	Date and Time	Source
<input type="checkbox"/> Information-4	08/08/2018, 23:37:41	Microsoft-Windows-Termi...
<input type="checkbox"/> Information-4	08/08/2018, 23:36:49	Microsoft-Windows-Termi...
<input type="checkbox"/> Information-4	08/08/2018, 23:36:27	Microsoft-Windows-Termi...
<input type="checkbox"/> Information-4	08/08/2018, 23:36:22	Microsoft-Windows-Termi...
<input type="checkbox"/> Information-4	08/08/2018, 22:28:36	Microsoft-Windows-Termi...
<input type="checkbox"/> Information-4	08/08/2018, 22:25:37	Microsoft-Windows-Termi...
<input type="checkbox"/> Information-4	08/08/2018, 22:25:37	Microsoft-Windows-Termi...
<input type="checkbox"/> Error-2	08/08/2018, 10:05:57	Microsoft-Windows-Termi...

General Detalles

Servicios de Escritorio remoto: reconexión de sesión correcta:

Usuario: WIN-M5327EF98B9\mpowers
 Identificador de sesión: 2
 Dirección de red de origen: 174.127.93.3

Conclusiones

¿Se han utilizado programas no permitidos por las políticas de la empresa?

Sí, se han descargado y utilizado los siguientes programas:

- “PrivaZer”, ideado para eliminar el rastro de determinadas actividades del ordenador.
- “Treceiver”, aparentemente un programa para pedir comida a domicilio.

¿Se han realizado conexiones remotas fuera del horario laboral por parte de la empresa?

Hay evidencias de que el empleado realizó conexiones remotas al ordenador en horario no laboral, algunas de ellas para ejecutar los programas mencionados anteriormente.

¿Ha incumplido el empleado las normas internas de la empresa?

Sí, se han descargado y ejecutado programas no permitidos tanto dentro como fuera del horario laboral, se ha utilizado uno de esos programas para eliminar datos y se han realizado conexiones remotas fuera del horario laboral.



Conclusiones personales

Esta práctica nos ha parecido muy interesante y útil, ya que hemos podido aprender el trabajo de perito forense de manera práctica.

Al principio hemos tenido dificultades con la primera herramienta de clonado de disco que habíamos elegido, *Autopsy* ⁸, ya que no conseguimos generar los hash del disco original y clonado, pese a estar ejecutando el *ingest module* encargado de hacer el hash de los ficheros y el propio disco (*hash lookup*). Intentar solucionarlo nos retrasó muchos días. Finalmente, decidimos utilizar la herramienta *OSForensics* tanto para el clonado del disco como para el análisis de sus contenidos. No tuvimos ningún problema para clonar el disco, verificar su hash o examinar su contenido, y además, hay mucha información en la web para consultar el funcionamiento de este programa.

Respecto al estudio de los artefactos forenses, encontramos también en la web mucha información al respecto muy útil indicando para qué se utilizaba cada artefacto, en qué directorio se encontraba la información, y cómo interpretarla. Esto nos ha sido de gran ayuda especialmente en la segunda parte de la práctica, para poder revisar si se habían producido accesos remotos al ordenador.

■ ■ ■

⁸ <https://www.autopsy.com/>