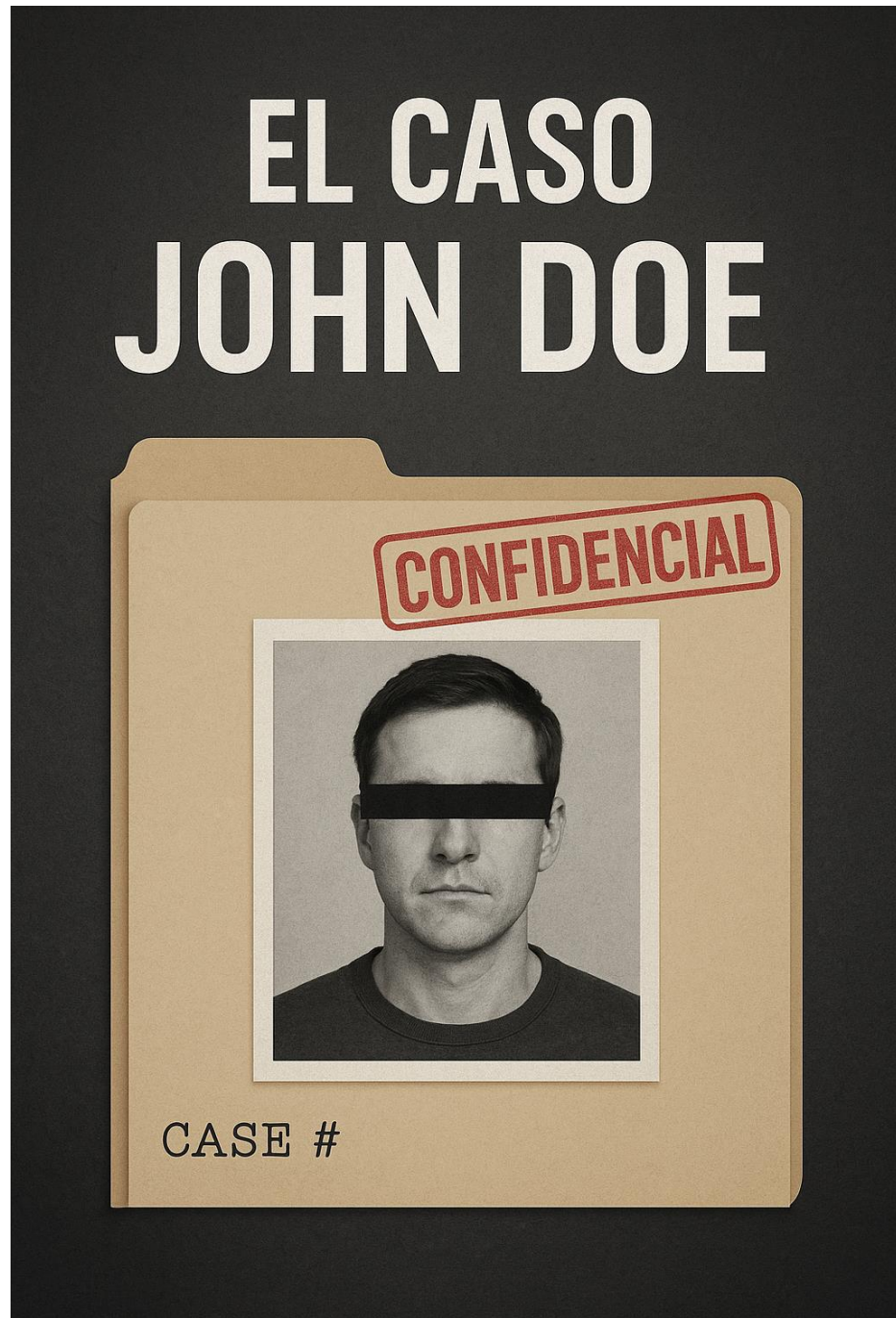


Informe de análisis forense.

“El caso John Doe”



Joel González

Herramientas Utilizadas.

- Autopsy
- Visualizador de archivos zip
- Navegador web

Evidencias relevantes

1. Búsqueda Intencionada de Herramientas Portables

Prueba encontrada:

Historial de búsqueda en Google y Bing muestra términos como:

- “descarga 7-Zip portable”
- “wettransfer”

Interpretación:

El usuario no llegó accidentalmente a las herramientas utilizadas. Hubo intención clara de buscar y obtener 7-Zip Portable, lo que evita dejar rastros de instalación en el sistema. También buscó explícitamente servicios de transferencia de archivos, lo que sugiere intención de compartir información hacia el exterior.

2- Descarga de 7-Zip Portable.

Prueba encontrada:

Registro de descarga del archivo 7-ZipPortable_24.09.paf.exe desde:

- portableapps.com
- download2.portableapps.com

Ruta: C:\Users\johndoe\Downloads\

Interpretación:

Se descargó una versión portable del compresor 7-Zip, herramienta muy usada para empaquetar datos confidenciales antes de enviarlos o eliminarlos. Al ser portable, no requiere instalación ni genera registros en “Program Files” o en el Registro de Windows.

3. Acceso a Plataformas de Transferencia Cifradas

Prueba encontrada:

Cookies activas e historial web de:

- mega.nz
- wetransfer.com

Interpretación:

Estas plataformas permiten la transferencia de archivos cifrados a través de la nube, lo cual es altamente sospechoso en un análisis forense, especialmente si hay evidencia de compresión previa. Esto sugiere una posible exfiltración de información.

4. Presencia de Archivos Comprimidos Anómalos**Prueba encontrada:**

Archivo Revert.wmz en formato comprimido, con change time que indican:

- Created/Access/Modified: 03/03/2022
- Change Time: 10/05/2025

Interpretación:

Aunque el archivo parece antiguo, su Change Time (modificación de metadatos) es reciente, lo que indica que fue manipulado en 2025. Esto sugiere un posible intento de ocultamiento o preparación para transferencia.

5. Secuencia Temporal Coordinada**Prueba encontrada:**

Todas las acciones anteriores ocurrieron entre las 15:28 y 15:37 del 4 de junio de 2025:

- Búsqueda de 7-Zip
- Descarga de software
- Navegación a MEGA y WeTransfer
- Presencia de cookies e historial

Interpretación:

Esta secuencia estructurada sugiere una acción deliberada y rápida: descargar una herramienta, usarla, y transferir posibles datos en menos de 10 minutos. Este comportamiento no es casual ni accidental.

Archivos Comprimidos

Entre los archivos comprimidos que se encontraron en la imagen virtual del disco están:

Msedge.7z: Es un formato de compresión de archivos de alta eficiencia, es similar a ZIP o RAR, pero este cuenta con mejor compresión.

Posibles escenarios para la creación de este archivo.

1. Copia de seguridad: Alguien podría haber creado este archivo para hacer una copia de seguridad de la configuración, extensiones o archivos de Microsoft Edge.
2. Versión personalizada: Es posible que se trate de una versión de Edge personalizada para un propósito específico, como para ser usada en un entorno empresarial o para fines educativos.
3. Malware: También existe la posibilidad de que este archivo sea malicioso que se hace pasar por un archivo legítimo de Edge, es importante verificar su procedencia y si hay dudas escanearlo con un antivirus.

Dado que este es un archivo que se podría enmascarar y utilizar para fines delictivos podríamos estar ante un malware el cual podría causarnos una pérdida de archivos importante.

Windows10.0-KB5058385: También se encontró este archivo .cab que parece ser una actualización reciente lanzada el 13 de mayo del 2025, esta actualización aborda problemas de seguridad y mejora la estabilidad del sistema.

Dispositivos conectados al equipo.

Esto es evidencia de dispositivos USB conectados en el equipo original.

- ROOT_HUB30 es el controlador raíz USB 3.0 — indica puertos USB disponibles.
- VirtualBox USB Tablet aparece cuando la máquina analizada es una VM o se usó VirtualBox en algún momento.

EL de dispositivos que se han conectado recientemente al equipo nos indica que los puertos USB 3.0 están disponibles, si los puertos están disponibles para que cualquier usuario pueda conectar un

dispositivo USB propio fácilmente se puede extraer información confidencial o de importancia para la empresa.

USB Device Attached

Table

Thumbnail

Summary

Sav

Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM		3		2025-06-04 18:21:54 CEST		ROOT_HUB30	48:24054718&0&0	windows-machine:evidence.E01
SYSTEM		3		2025-06-04 18:21:54 CEST	VirtualBox	USB Tablet	5812c8f4c0&0&1	windows-machine:evidence.E01

Hex

Text

Application

Source File Metadata

OS Account

Data Artifacts

Analysis Results

Content

Annotations

Other Occurrences

Result: 1 of 2

Result

←























→

USB

Type	Value	Source(s)
Date/Time	2025-06-04 18:21:54 CEST	Recent Activity
Device Make		Recent Activity
Device Model	ROOT_HUB30	Recent Activity
Device ID	48:24054718&0&0	Recent Activity
Source File Path	/img_windows-machine-evidence.E01/vol.vol9/Windows/System32/config/SYSTEM	Recent Activity
Artifact ID	-922337203685477573	

Historial de archivos abiertos o modificados.

Se detectaron múltiples archivos con estado "Unallocated", lo que indica que fueron eliminados tras su uso. Entre ellos hay registros de usuario, bases de datos del sistema, archivos temporales y configuraciones. Todo esto ocurrió en el mismo rango horario que la actividad maliciosa detectada. Este comportamiento apunta a una posible intención de ocultar rastros, borrar evidencia de actividad o preparar el sistema para no dejar huella tras la exfiltración de datos.





System												
Table	Thumbnail	Summary										
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	
 EventStore.db-shm				2025-06-04 18:22:13 CEST	2025-06-04 18:22:13 CEST	2025-06-04 18:22:13 CEST	2025-06-04 18:09:36 CEST	32768	Unallocated	Unallocated	unknown	
 EventStore.db-wal				2025-06-04 15:42:28 CEST	2025-06-04 15:42:28 CEST	2025-06-04 15:42:28 CEST	2025-06-04 18:09:36 CEST	65952	Unallocated	Unallocated	unknown	
 EventStore.db-shm				2025-06-04 18:22:13 CEST	2025-06-04 18:22:13 CEST	2025-06-04 18:22:13 CEST	2025-06-04 18:09:36 CEST	32768	Unallocated	Unallocated	unknown	
 EventStore.db-wal				2025-06-04 15:52:17 CEST	2025-06-04 15:52:17 CEST	2025-06-04 15:52:17 CEST	2025-06-04 18:09:36 CEST	1048576	Unallocated	Unallocated	unknown	
 EventStore.db-shm				2025-06-04 18:22:13 CEST	2025-06-04 18:22:13 CEST	2025-06-04 18:22:13 CEST	2025-06-04 18:09:36 CEST	32768	Unallocated	Unallocated	unknown	
 mpengine.db-wal				2025-06-04 15:53:15 CEST	2025-06-04 15:53:15 CEST	2025-06-04 15:53:15 CEST	2025-06-04 15:34:49 CEST	498552	Unallocated	Unallocated	unknown	
 mpengine.db-shm				2025-06-04 15:34:49 CEST	2025-06-04 15:34:49 CEST	2025-06-04 15:34:49 CEST	2025-06-04 15:34:49 CEST	32768	Unallocated	Unallocated	unknown	
 IMpService7BDaF73-B396-481F-9042-AD358843EC				2025-06-04 15:34:49 CEST	2025-06-04 15:34:49 CEST	2025-06-04 15:34:49 CEST	2025-06-04 15:34:49 CEST	0	Unallocated	Unallocated	unknown	
 hlncc2e.tmp				2025-06-04 15:52:15 CEST	2025-06-04 15:52:15 CEST	2025-06-04 15:52:15 CEST	2025-06-04 15:52:15 CEST	0	Unallocated	Unallocated	unknown	
 user.config				2025-06-04 15:52:14 CEST	2025-06-04 15:52:14 CEST	2025-06-04 15:52:14 CEST	2025-05-10 00:22:17 CEST	6041	Unallocated	Unallocated	unknown	
 ServerList.xml				2025-05-10 18:42:16 CEST	2025-05-10 18:42:16 CEST	2025-05-10 18:42:16 CEST	2025-05-10 00:25:16 CEST	327	Unallocated	Unallocated	unknown	
 NTUSER.DAT[c76cbcd4-afc9-11eb-8234-000d3aa6d				2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	65536	Unallocated	Unallocated	unknown	
 NTUSER.DAT[c76cbcd4-afc9-11eb-8234-000d3aa6d				2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	1048576	Unallocated	Unallocated	unknown	
 NTUSER.DAT[c76cbcd4-afc9-11eb-8234-000d3aa6d				2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	1048576	Unallocated	Unallocated	unknown	
 NTUSER.DAT[c76cbcd4-afc9-11eb-8234-000d3aa6d				2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	2025-06-04 18:22:03 CEST	1048576	Unallocated	Unallocated	unknown	
 NTUSER.DAT[c76cbcd4-afc9-11eb-8234-000d3aa6d				2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	65536	Unallocated	Unallocated	unknown	
 NTUSER.DAT[c76cbcd4-afc9-11eb-8234-000d3aa6d				2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	1048576	Unallocated	Unallocated	unknown	
 NTUSER.DAT[c76cbcd4-afc9-11eb-8234-000d3aa6d				2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	1048576	Unallocated	Unallocated	unknown	
 NTUSER.DAT[c76cbcd4-afc9-11eb-8234-000d3aa6d				2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	2025-06-04 18:22:01 CEST	1048576	Unallocated	Unallocated	unknown	
 lastalive0.dat				2025-06-04 15:52:09 CEST	2025-06-04 15:52:09 CEST	2025-06-04 15:52:09 CEST	2025-06-04 18:09:30 CEST	2048	Unallocated	Unallocated	unknown	
 lastalive1.dat				2025-06-04 15:53:09 CEST	2025-06-04 15:53:09 CEST	2025-06-04 15:53:09 CEST	2025-06-04 15:10:06 CEST	2048	Unallocated	Unallocated	unknown	
 tmp.edb				2025-06-04 15:32:35 CEST	2025-06-04 15:32:35 CEST	2025-06-04 15:32:35 CEST	2025-06-04 15:10:06 CEST	262144	Unallocated	Unallocated	unknown	

Archivo comprimido, usado habitualmente para temas visuales de Windows, pero también puede ser renombrado para ocultar contenido como por ejemplo un zip camuflado

El archivo fue creado y se accedió a el originalmente en el 2022, sin embargo, ha sido modificado en el 2025, esto nos puede indicar lo siguiente:

- Movido a otra ubicación.
- Accedido por una herramienta como, por ejemplo .zip
- Preparado para compresión o extracción.
- Renombrarlo para disfrazarlo.

Esto podría coincidir con el periodo del 4 de junio, donde se detecto actividad con 7-Zip y navegación a mega.

Listing							
application/zip							
Table Thumbnail Summary							
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
 Revert.wmz			3	2022-03-03 04:54:51 CET	2025-05-10 10:13:51 CEST	2022-03-03 04:54:51 CET	2022-03-03 04:54:51
 Revert.wmz			3	2022-03-03 04:54:53 CET	2025-05-10 10:13:55 CEST	2022-03-03 04:54:53 CET	2022-03-03 04:54:53
 Revert.wmz			3	2022-03-03 04:54:51 CET	2025-05-10 10:13:51 CEST	2022-03-03 04:54:51 CET	2022-03-03 04:54:51
 Revert.wmz			3	2022-03-03 04:54:53 CET	2025-05-10 10:13:55 CEST	2022-03-03 04:54:53 CET	2022-03-03 04:54:53



Navegación sospechosa

Uso de Internet Explorer Analyzer: El día 10/052025 se utilizó esta herramienta específicamente la función modo IE que permite ejecutar sitios web que requieren compatibilidad con internet explorer 11 o herramientas de diagnóstico como iediagcmd.exe.

Peligros de utilizar Internet Explorer 11: Internet Explorer es reconocido por tener numerosas vulnerabilidades de seguridad que los atacantes pueden explotar para comprometer la seguridad.



















Internet Explorer es un software obsoleto que ya no recibe actualizaciones no soporte técnico por parte de Microsoft, lo que nos dice que cualquier vulnerabilidad detectada ya no será parcheada.

Al ser un navegador obsoleto es un objeto atractivo para malware, ya que se puede aprovechar su vulnerabilidad para infectar el sistema.

Web Bookmarks										
Table		Thumbnail		Summary						
Source Name	S	C	O	URL	Title	Date Created	Program Name	Domain	Data Source	
 Bing.url			4	http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url	2025-05-10 00:21:26 CEST	Internet Explorer Analyzer	microsoft.com	windows-machine-evidence.E01	
 Bing.url			4	http://go.microsoft.com/fwlink/p/?LinkId=255142	Bing.url	2025-06-04 15:23:51 CEST	Internet Explorer Analyzer	microsoft.com	windows-machine-evidence.E01	

Interacción con el sitio WeTransfer, alguien visito este sitio ya que las cookies indican navegación en él , esto podría implicar transferencia de archivos sospechosos o fuga de datos.

Las cookies snowplow, dd_s y otros similares son de seguimiento e indican que hay una interacción con el sitio y no solo una visita rápida.

 Cookies			4	.wetransfer.com	2025-06-04 15:30:27 CEST	wl_idmg			
 Cookies			4	www.bing.com	2025-06-04 15:41:52 CEST	MUIDB			
 Cookies			4	.bing.com	2025-06-04 15:41:52 CEST	SRCHHPGUSR			
 Cookies			4	.bing.com	2025-06-04 15:41:52 CEST	USRLOC			
 Cookies			4	.msn.com	2025-06-04 15:37:25 CEST	USRLOC			
 Cookies			4	accounts.google.com	2025-06-04 15:50:27 CEST	_Host-GAPS			
 Cookies			4	auth.wetransfer.com	2025-06-04 15:37:40 CEST	did			
 Cookies			4	.wetransfer.com	2025-06-04 15:50:27 CEST	AMP_874b771639			
 Cookies			4	.wetransfer.com	2025-06-04 15:50:27 CEST	AMP_MKTG_874b771639			
 Cookies			4	accounts.google.com	2025-06-04 15:50:27 CEST	OTZ			
 Cookies			4	apps.rokt.com	2025-06-04 15:38:00 CEST	akaalb_Instance-1			
 Cookies			4	.wetransfer.com	2025-06-04 15:37:55 CEST	amp_874b77			
 Cookies			4	wetransfer.com	2025-06-04 15:50:27 CEST	is_ivt			
 Cookies			4	.wetransfer.com	2025-06-04 15:50:27 CEST	_wt_snowplowid.0497			
 Cookies			4	.wetransfer.com	2025-06-04 15:50:27 CEST	_wt_snowplowses.0497			
 Cookies			4	.wetransfer.com	2025-06-04 15:50:27 CEST	sp			
 Cookies			4	wetransfer.com	2025-06-04 15:50:27 CEST	_dd_s			
 WebCacheV01.dat			3	windows.search	2025-06-04 13:13:44 CEST	SRCHHPGUSR			HV=174904282

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

PortableApps.com es un sitio que permite descargar software portable, ejecutable sin instalación. Esta característica puede utilizarse para ejecutar herramientas sin dejar rastros tradicionales.

MEGA.nz: es un servicio de almacenamiento cifrado y frecuentemente utilizado para la transferencia de archivos fuera del control institucional. Su uso en contextos forenses suele levantar alertas por posible exfiltración de datos o descarga de herramientas maliciosas.

Se observa un corto intervalo entre las visitas a estos sitios lo que nos hace sospechar que se han descargado y utilizado herramientas externas.

Esta evidencia nos podría revelar una secuencia de navegación web que indica una posible manipulación del sistema con fines de

evasión o actividad no autorizada el uso combinado de PortableApps y MEGA.nz sugiere descarga i transferencia de archivos

PortableApps y MEGA.nz.

Cookies		4	.youtube.com	2025-06-04 15:29:49 CEST	VISITOR_PRIVACY_METADATA	
Cookies		4	.youtube.com	2025-06-04 15:29:48 CEST	YSC	
Cookies		4	.youtube.com	2025-06-04 15:29:49 CEST	__Secure-ROLLOUT_TOKEN	
Cookies		4	.cdn2.portableapps.com	2025-06-04 15:30:31 CEST	__cf_bm	
Cookies		4	.portableapps.com	2025-06-04 15:30:40 CEST	_ga	
Cookies		4	.portableapps.com	2025-06-04 15:30:40 CEST	_ga_WHB3ZZ535L	
Cookies		4	assets.msn.com	2025-06-04 15:36:43 CEST	_C_Auth	
Cookies		4	ntp.msn.com	2025-06-04 15:36:42 CEST	ai_session	
Cookies		4	mega.nz	2025-06-04 15:37:39 CEST	geoip	
Cookies		4	.msn.com	2025-06-04 15:36:41 CEST	pglt-edgeChromium-ntp	

La siguiente imagen nos indica que efectivamente se han realizado descargas de la web PortableApps.

Web Downloads						
Table Thumbnail Summary						
Source Name	S	C	O	Path	URL	
History			4	C:\Users\johndoe\Downloads\7-ZipPortable_24.09.paf.exe	https://portableapps.com/redir2/?a=7-ZipPortable&s...	
History			4	C:\Users\johndoe\Downloads\7-ZipPortable_24.09.paf.exe	https://download2.portableapps.com/portableapps/7...	

El usuario descargo una versión portable de 7-Zip, específicamente la versión 24.09, este ejecutable es un instalador autoextraíble usado por la plataforma PortableApps, al ser portable, este software puede ejecutarse sin instalación y no deja registros en el sistema.

Las anteriores características lo convierten en una herramienta ideal para evadir controles administrativos o actuar sin dejar rastro, esto podría tener usos en:

- 1. Exfiltración de datos.
- 2. Acceso temporal a sistemas.
- 3. Compresión y borrado de evidencia.

Relación de hallazgos previos:

- 15:30- Navegación a PortableApps.
- 15:37- Navegación a MEGA.nz
- Entre medias se descargó 7-ZipPortable_2409.paf.exe

Esto nos hace sospechar que posiblemente se uso para comprimir archivos que luego se subieron a Mega.

Servicios externos con actividad.

akamaized.net es un dominio utilizado por Akamai Technologies, una empresa global que ofrece servicios de computación en la nube, seguridad y distribución de contenido. Este dominio forma parte de la infraestructura de Akamai y se utiliza para distribuir contenido web y aplicaciones de manera eficiente y segura a través de su red global de servidores. En esencia, cuando ves una URL que termina en akamaized.net, significa que el contenido que estás accediendo está siendo servido a través de la plataforma de Akamai.

Conclusión.

Tras el análisis detallado de la evidencia digital con la herramienta Autopsy, se identificó una serie clara de actividades que indican comportamiento sospechoso por parte del usuario investigado.

A través de la búsqueda en historial de navegación, búsquedas web, descargas, archivos comprimidos, cookies, y archivos eliminados, se logró reconstruir una línea de tiempo que demuestra lo siguiente:

- **Búsqueda intencionada** de herramientas portables para la compresión de archivos, específicamente 7-Zip Portable, con el objetivo de evitar dejar huella en el sistema.
- **Descarga directa** de dicho software desde sitios especializados como PortableApps.com.
- **Acceso inmediato** a plataformas de transferencia cifrada como MEGA.nz y WeTransfer, altamente utilizadas para el intercambio de archivos fuera del entorno controlado.
- Evidencia de archivos comprimidos manipulados, como Revert.wmz, cuyos metadatos revelan actividad reciente, pese a su aparente antigüedad.

- **Eliminación de múltiples archivos del sistema** (estado “Unallocated”), entre ellos registros de usuario (NTUSER.DAT), configuraciones y bases de datos temporales, lo cual sugiere un intento deliberado de borrar rastros de actividad.

Este comportamiento fue rápido, coordinado y orientado a la evasión, con todas las acciones sucediendo en una ventana crítica de menos de 10 minutos, el día 4 de junio de 2025.

Por tanto, se concluye que el usuario llevó a cabo acciones que podrían estar relacionadas con la compresión y exfiltración de información, utilizando herramientas diseñadas para no dejar trazabilidad evidente. Autopsy permitió no solo recuperar artefactos clave, sino también correlacionar cada evento y reconstruir el posible flujo de la actividad sospechosa.