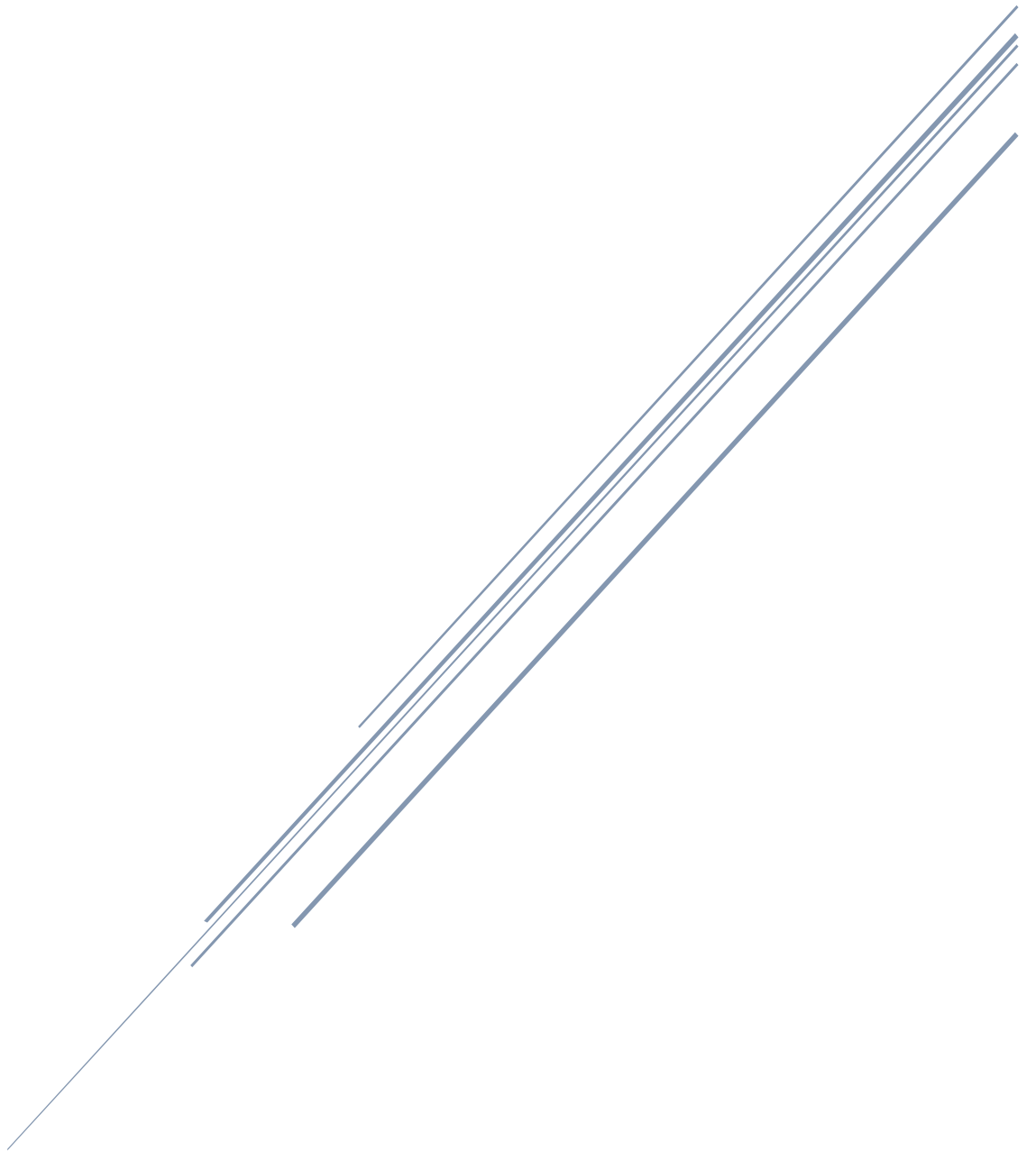


# ADQUISICIÓN FORENSE EN VIVO DE UNA MAQUINA WINDOWS

Memoria volátil y no volátil.



Álvaro Pérez Rey  
Análisis Forense Informático

## Realiza una adquisición forense en vivo usando las herramientas que estimes.

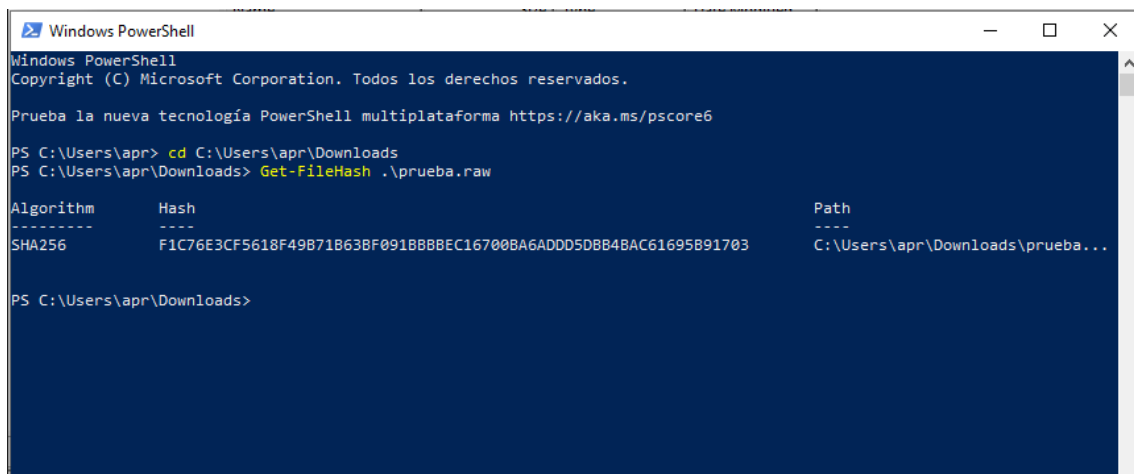
En esta práctica realizaremos una adquisición forense de una máquina que tiene instalado un SO Windows. La adquisición se realizará de la memoria volátil (Memoria RAM) y de la memoria no volátil (Disco) por lo que tendremos que establecer un orden de prioridad a la hora de determinar cuál de las dos debemos clonar primero.

Por lo que estableceremos el siguiente orden:

- Memoria volátil.
- Triage
- Memoria no volátil

### Memoria volátil

Por lo que comenzaremos con la clonación de la memoria volátil con la herramienta Magnet Ram Capture, y tras un breve periodo de clonado obtendremos nuestra copia. Una vez tengamos nuestra copia ejecutaremos en la Powershell de Windows el siguiente comando que se muestra en la imagen.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

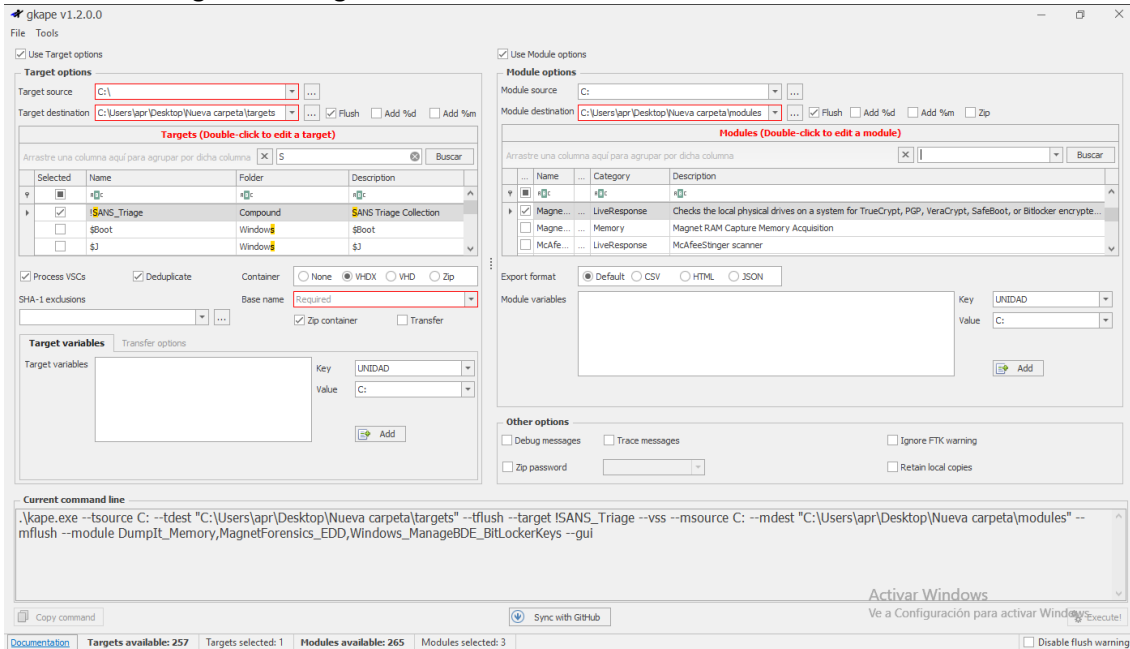
PS C:\Users\apr> cd C:\Users\apr\Downloads
PS C:\Users\apr\Downloads> Get-FileHash .\prueba.raw

Algorithm      Hash                                                    Path
-----
SHA256         F1C76E3CF5618F49B71B63BF091B8BBEC16700BA6ADD5DBB4BAC61695B91703  C:\Users\apr\Downloads\prueba...
```

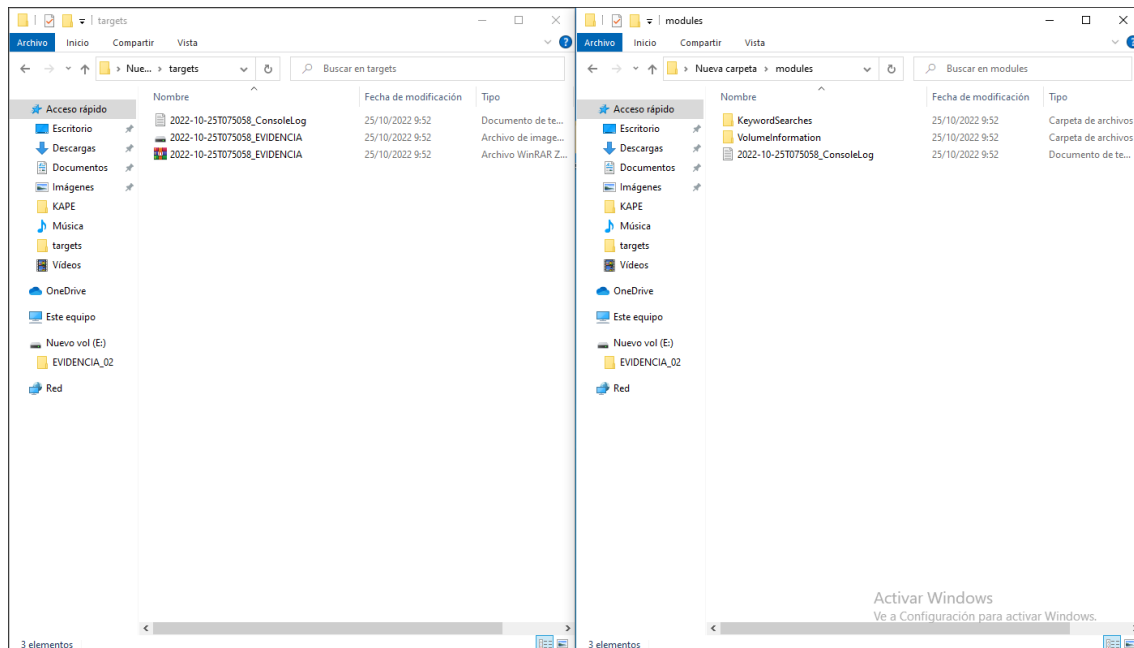
De la siguiente manera habremos calculado el hash de nuestro fichero con el algoritmo SHA256, sin embargo, nosotros no disponemos de otro hash de la memoria RAM para comparar, ya que esta va continuamente cambiando y sobrescribiéndose por lo que esto servirá para cuando otro analista forense decida realizar una clonación a nuestra evidencia los hashes coincidan y así se siga cumpliendo el principio de integridad de nuestras adquisiciones.

## Triaje

A continuación, realizaremos nuestro triaje con la herramienta KAPE (Kroll Artefact Parser & Extractor). El triaje consiste en la preadquisición de datos a través de una librería, por ejemplo, nosotros vamos a utilizar la librería Sans y los modules de BitLocker, DumpIt y EDD como se muestra en la siguiente imagen.

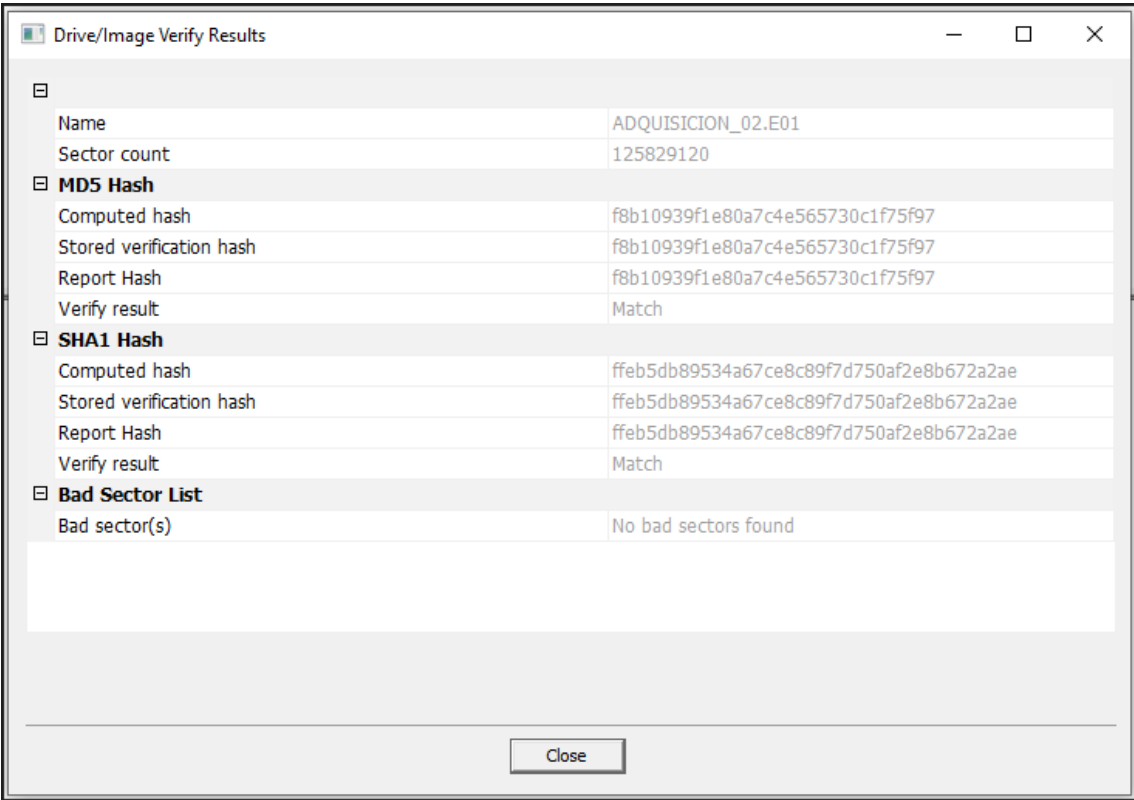


Y una vez realizado este proceso con las configuraciones adecuadas iremos a nuestras carpetas de destino preseleccionadas para encontrarnos con el resultado de dicho triaje, donde, en nuestro caso, podremos montar nuestra imagen en FTK Imager para continuar con nuestro análisis forense.



## Memoria no volátil

Para la clonación del disco C: hemos optado por utilizar la herramienta FTK Imager y tras un periodo de espera nos ha informado de que la clonación se ha ejecutado de manera correcta mostrándonos el siguiente mensaje.



Como se puede apreciar, se están comparando dos tipos de algoritmos de hashes, MD5 y SHA 1, para así verificar que el principio de integridad de la adquisición se cumple en todo momento.

