THE BRIDGE

Herramienta Volatility

Volatility

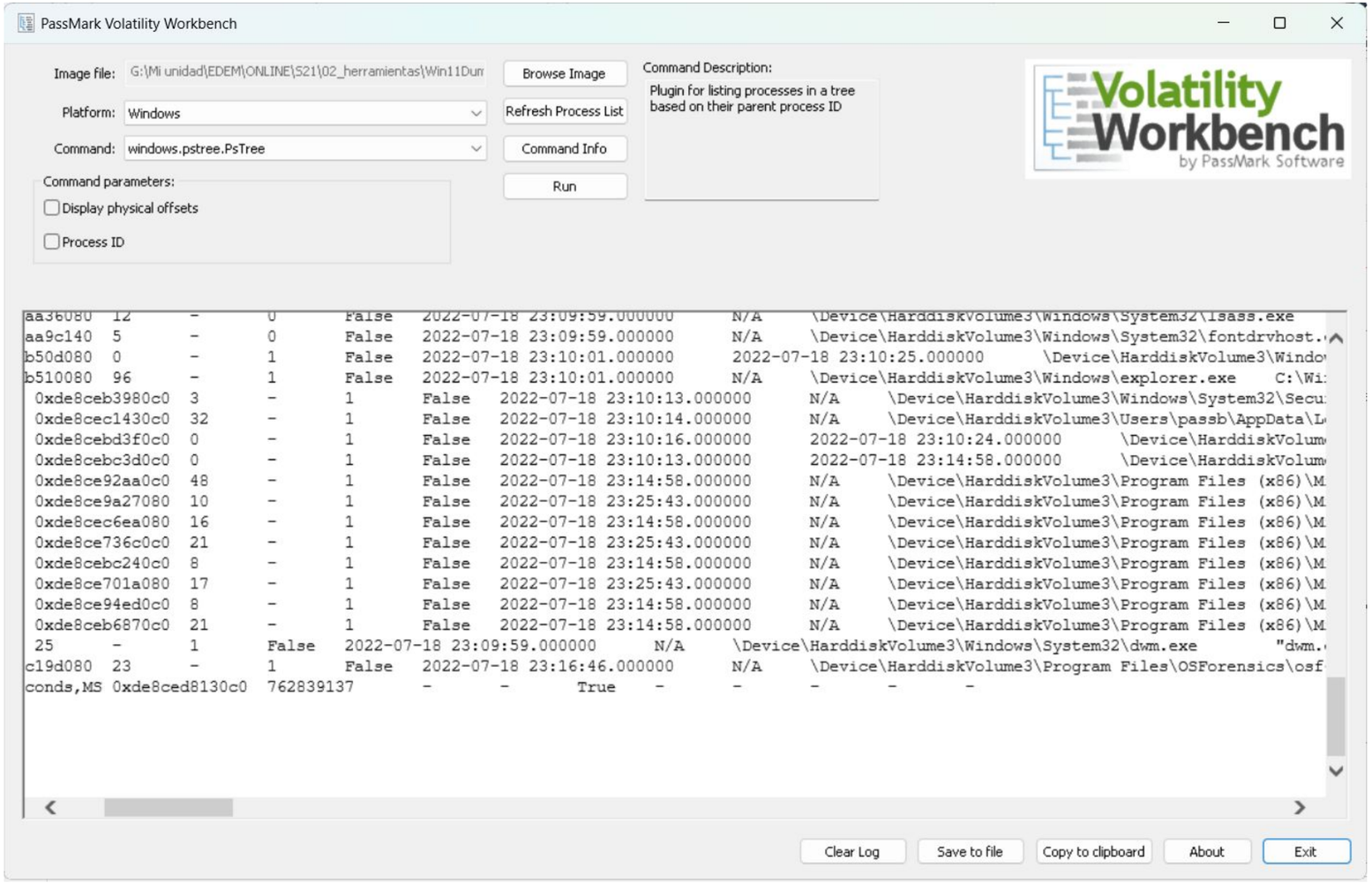
- Herramienta de análisis forense de memoria (RAM) para extraer información volátil del sistema comprometido.

- Se destaca por permitir a los analistas recuperar y analizar una amplia variedad de artefactos, como:

  - **Procesos activos y terminados.**
  - **Conexiones de red.**
  - **Archivos abiertos.**
  - **Módulos cargados del kernel.**
  - **Contraseñas en texto claro (si están en memoria).**
  - **Fragmentos de memoria relacionados con malware o exploits**.

- Funciona con sistemas operativos como Windows, Linux, MacOS, entre otros.

- Su funcionalidad es extendida a través de plugins,.



Volatility

- Descargar el software desde la página https://volatilityfoundation.org/
- Ir al repositorio de Github
- Descargar archivo .zip con la imagen de Windows.
- Descomprir el archivo
- Ejecutar **VolatilityWorkbench.exe**


THE
BRIDGE