MEMORY DUMP EXERCISE

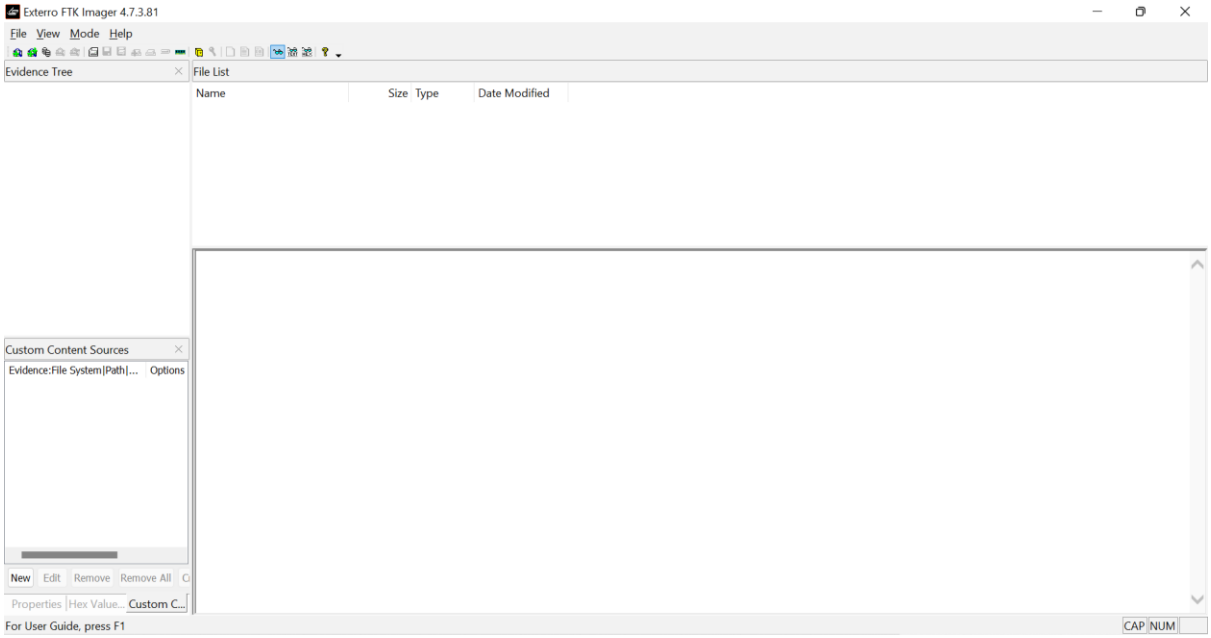
USING FTK IMAGER AND PHOTOREC

"ACQUIRE MEMORY DUMP OF A WINDOWS SYSTEM WITH FTK IMAGER"

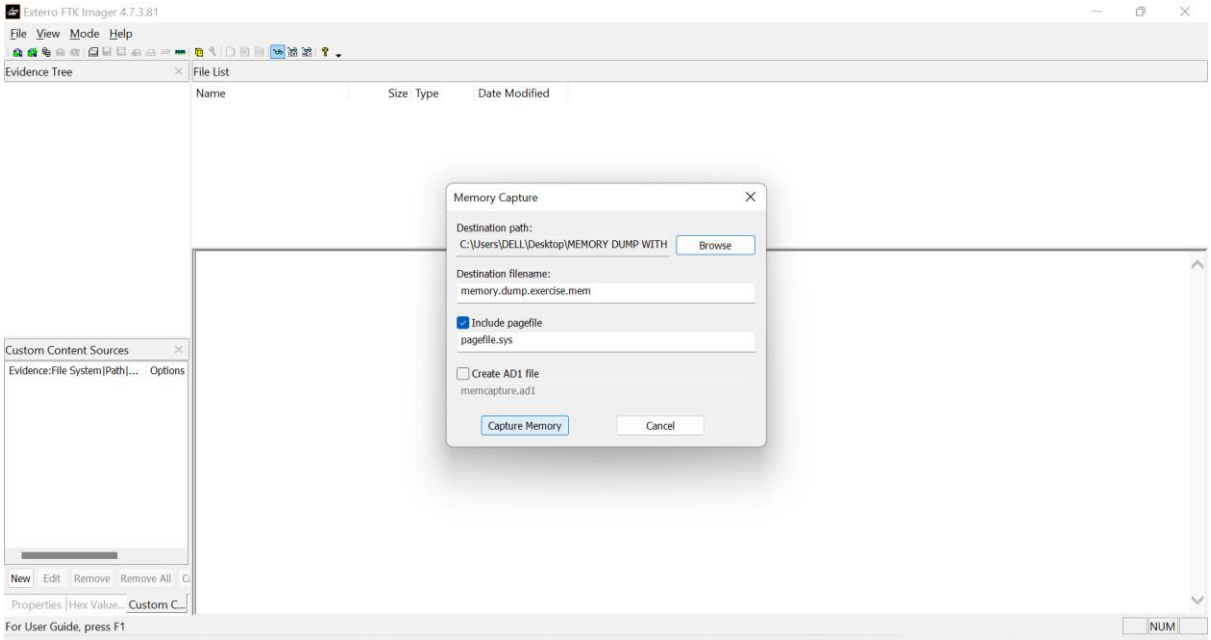
"CARVE THE MEMORY DUMP USING PHOTOREC"

SUBMITTED BY ADENIKE OLUWABUSOLA ONI

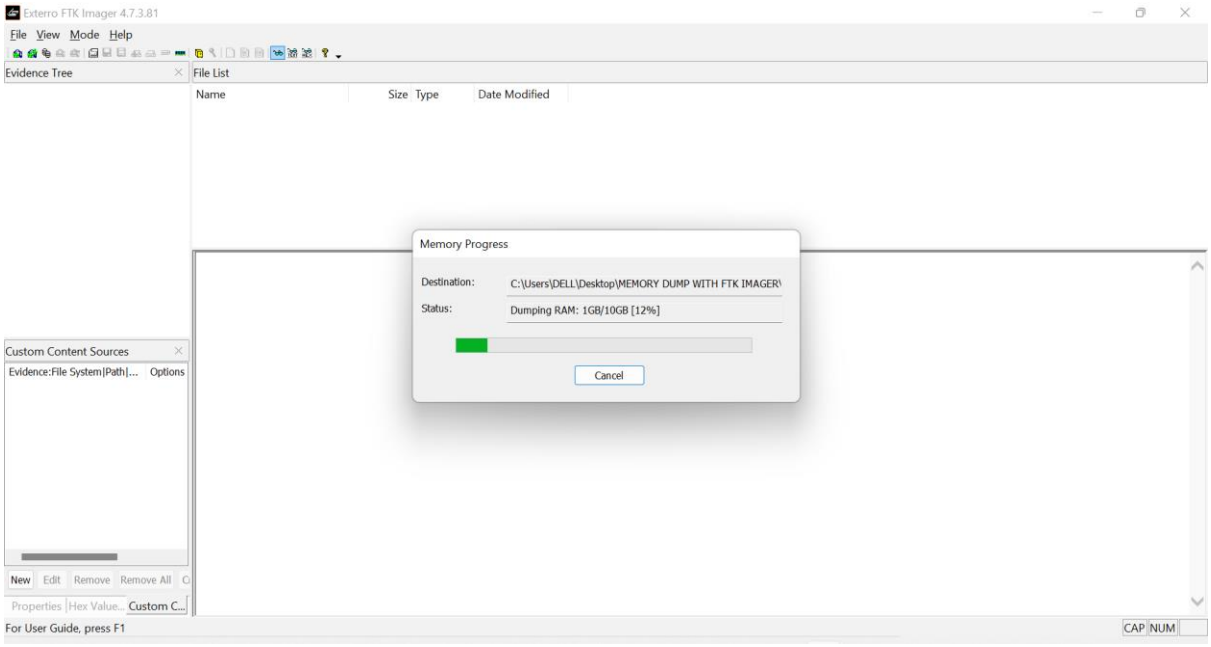
FTK Imager Software

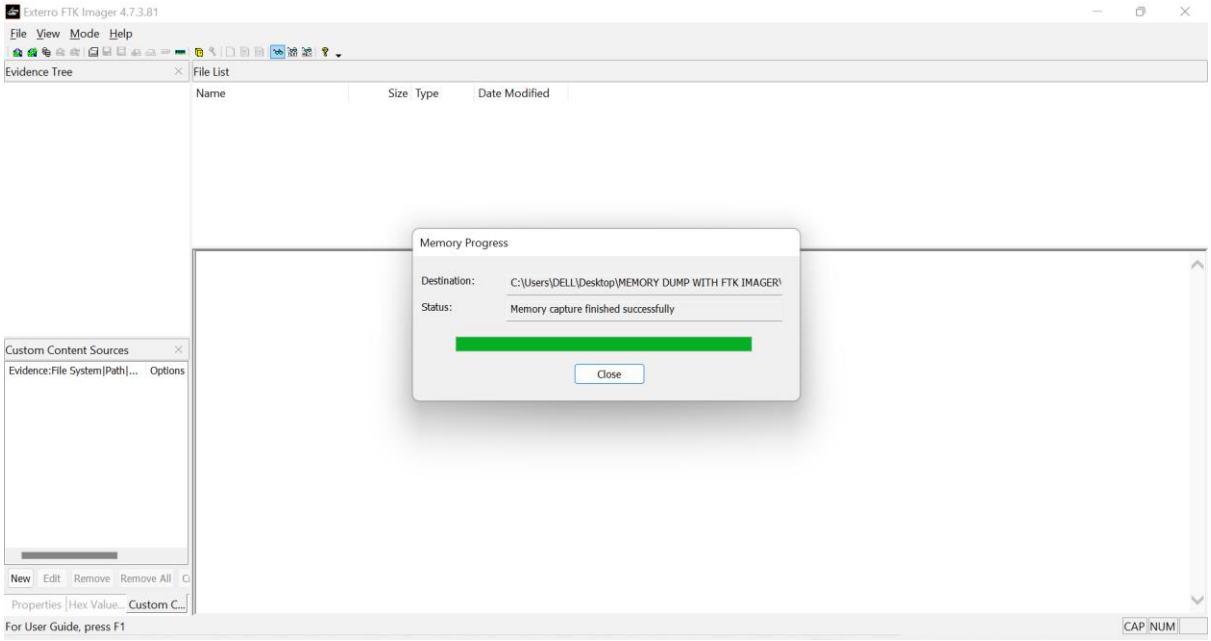


File - Capture memory - Browse destination path - Fill destination file name - Include page file - Capture memory

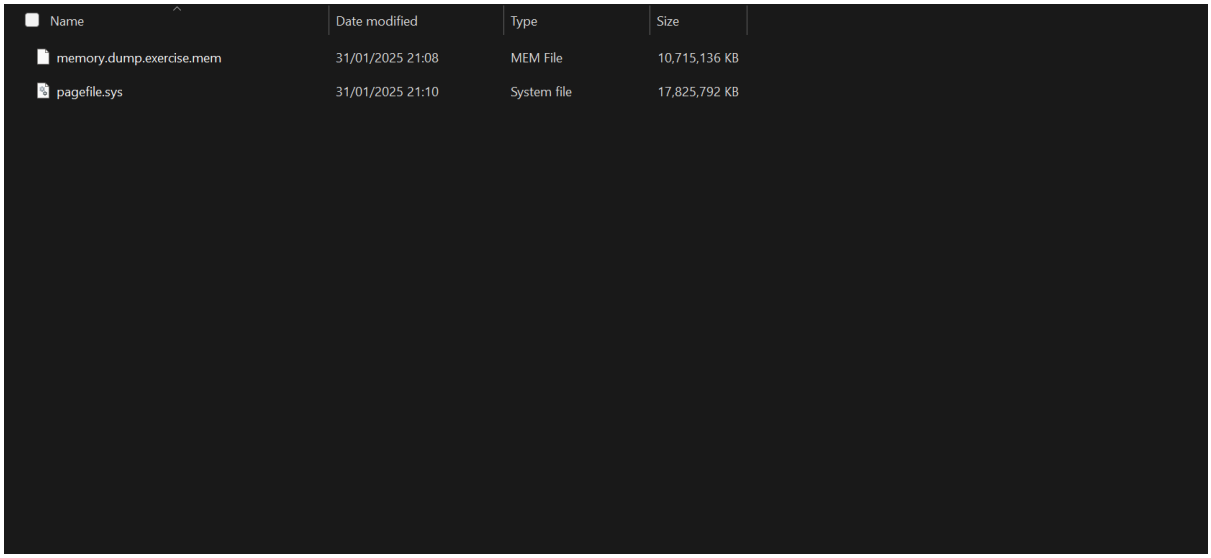


In progress - Completed

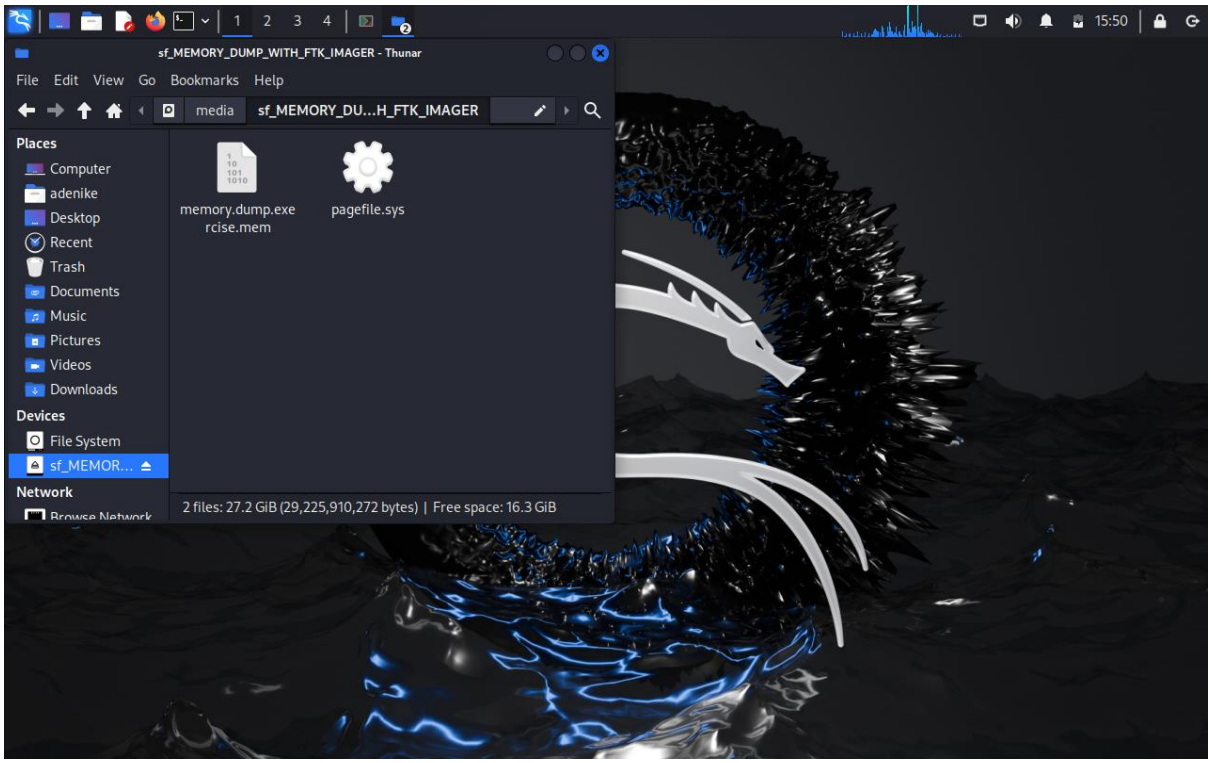




Memory dump file folder

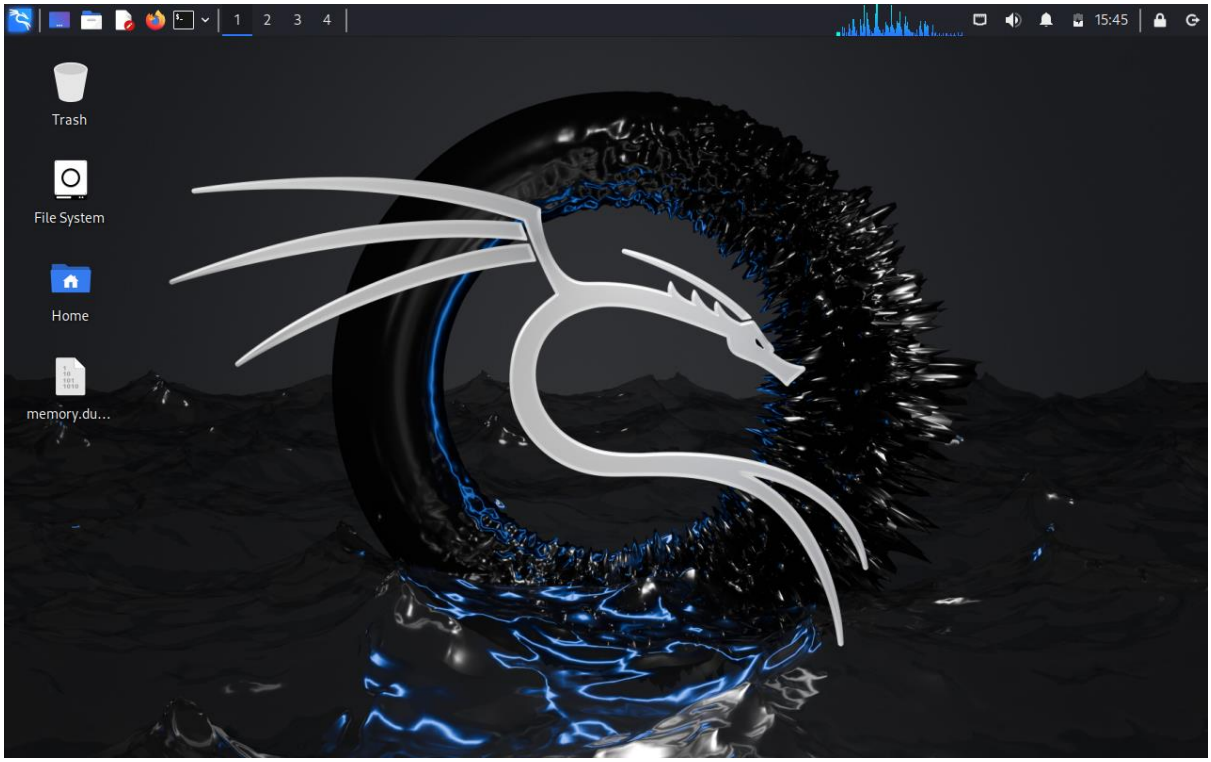


Share folder to access the memory dump in Kali Linux

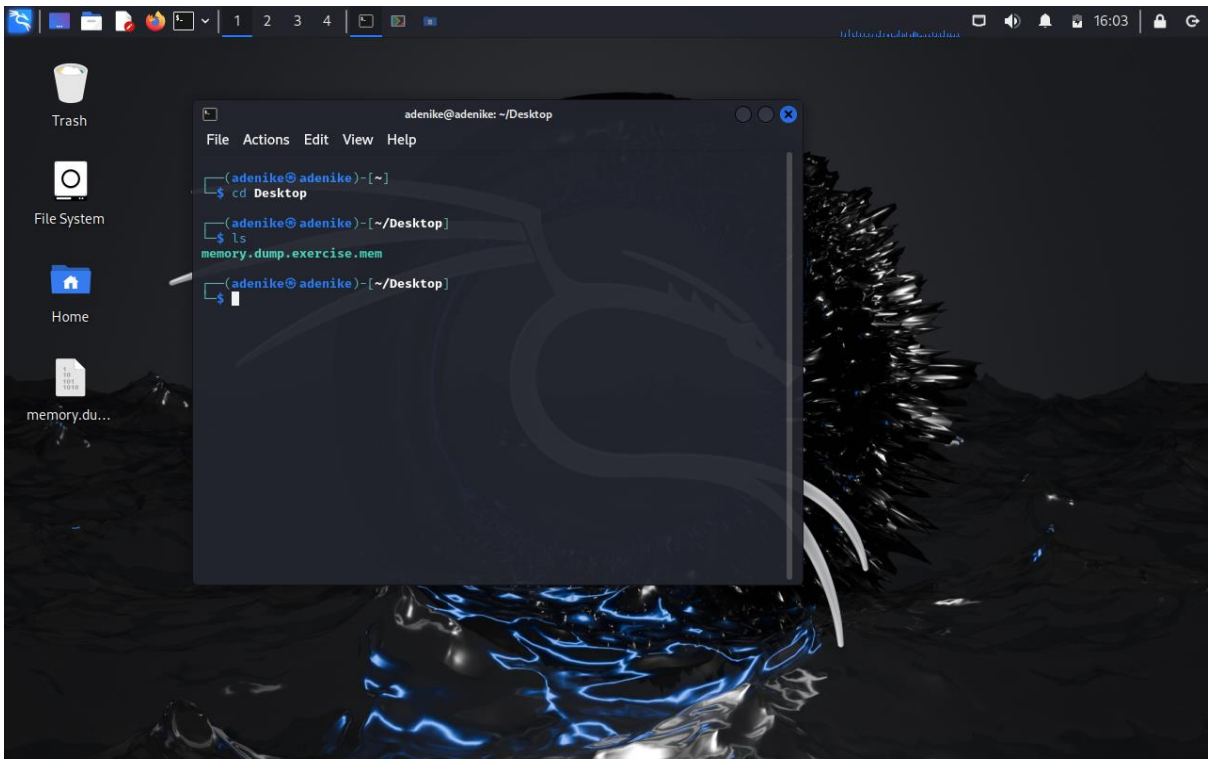


File operation progress - Copy from the shared folder to Kali Linux desktop

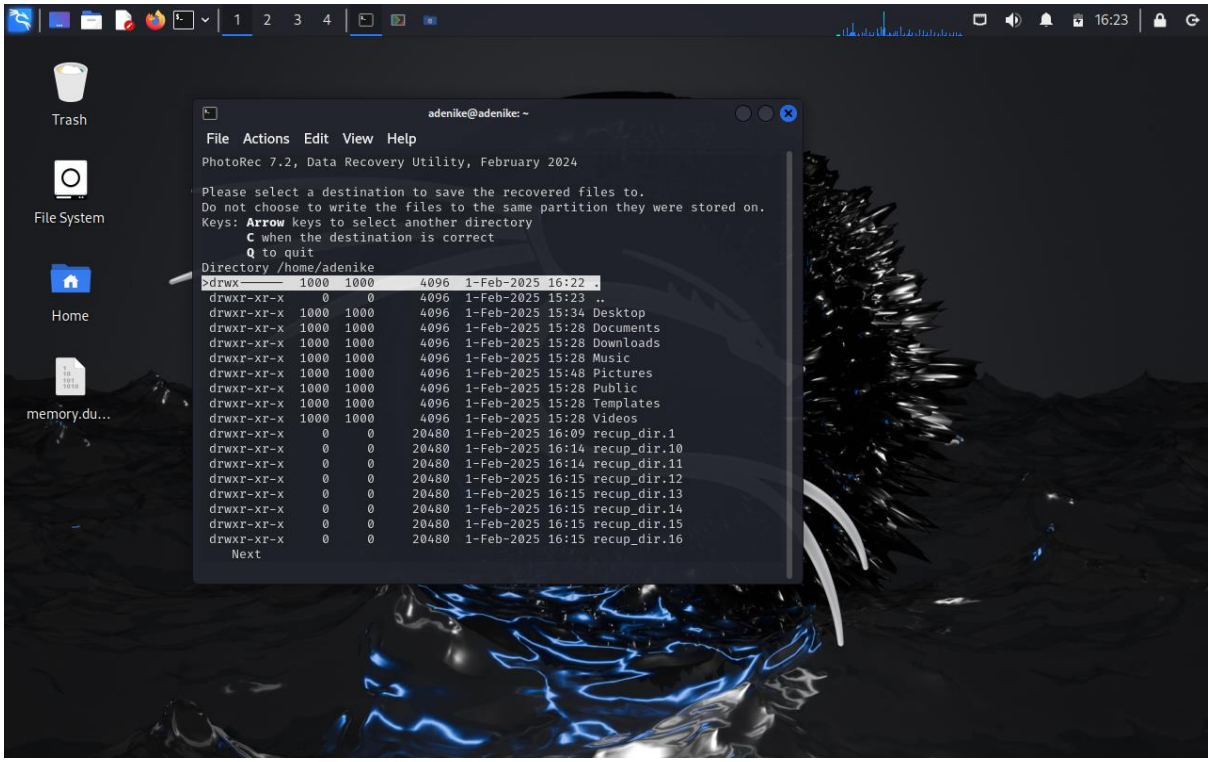
File copied to Kali Linux desktop



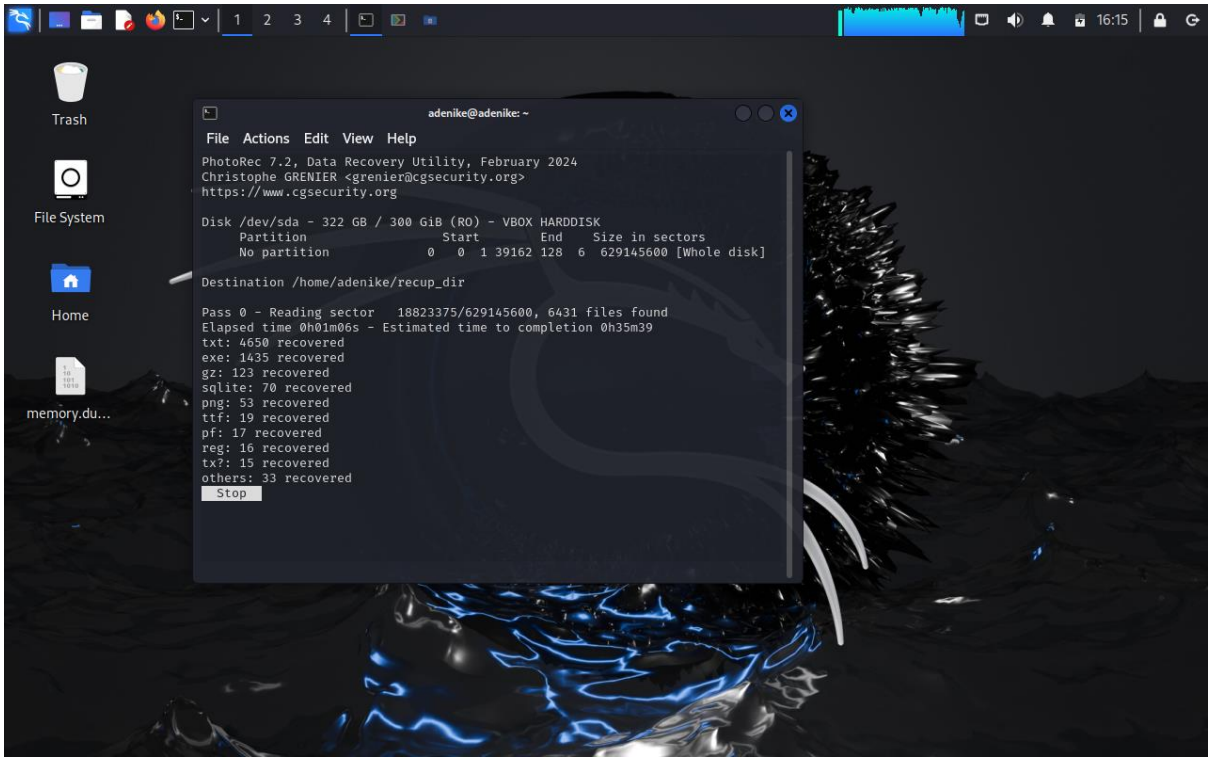
Run terminal to confirm memory dump has been successfully copied to the Desktop



Select destination to carve the memory dump using PhotoRec



Recovery in progress



Content of recovered information from memory dump