PROCESS EXPLORER

**AIM:**

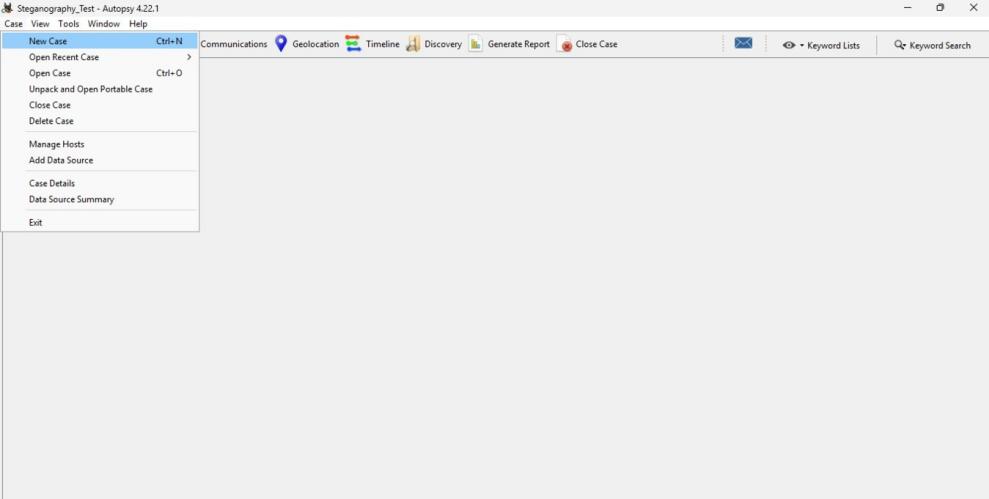
**AIM:**

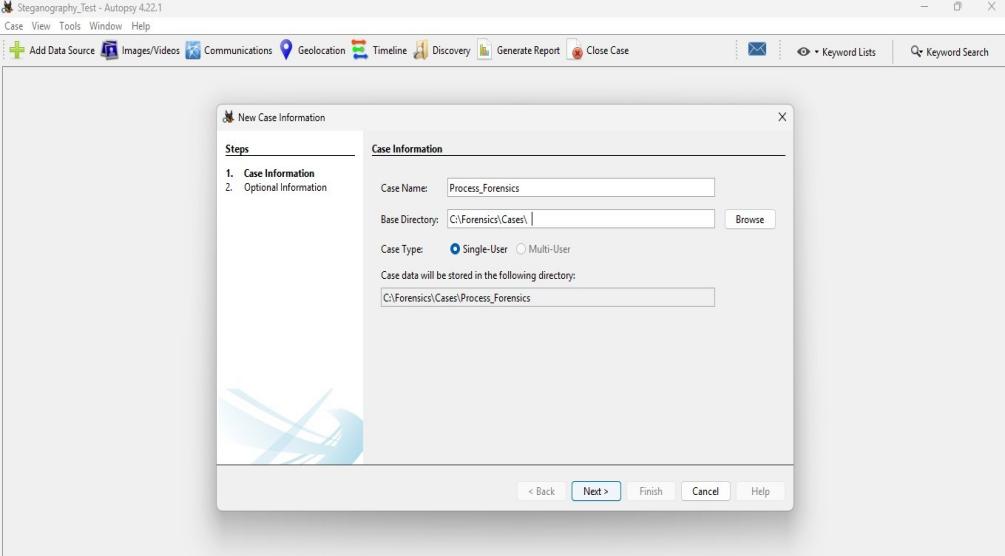
To monitor and analyze system processes using Process Explorer and to identify suspicious or unauthorized activities from running tasks.

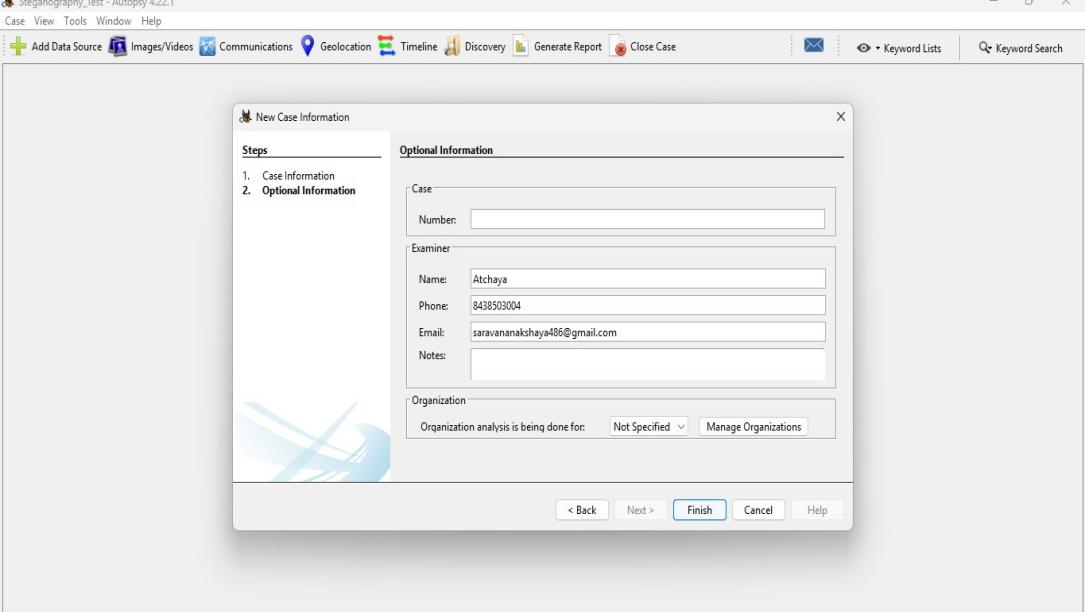
**DESCRIPTION OF THE TOOL USED:m**

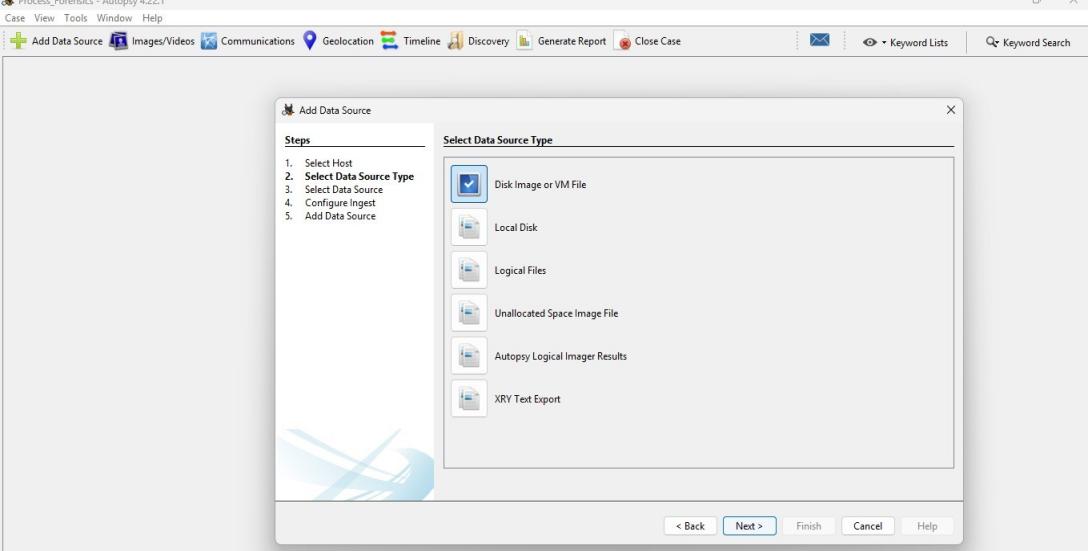
Process Explorer is a system utility developed by Microsoft for viewing running processes, their resource usage, and associated files. It provides detailed information about process trees, DLLs, and handles. In this experiment, the data gathered was examined in Autopsy for forensic evidence. Process Explorer helps detect malware, rootkits, or unauthorized software. It is an essential forensic tool for system monitoring and live analysis. The experiment demonstrated how process inspection aids in digital investigations.artifacts, and system compromise indicators through memory and disk analysis.

**STEPS INVOLVED:**

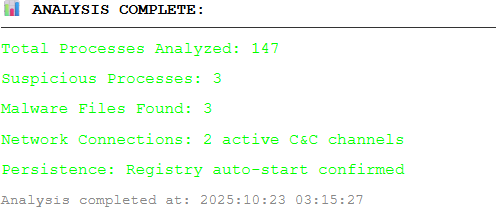
****

****



****

**OUTPUT:**

****