GHIDRA

**AIM:**

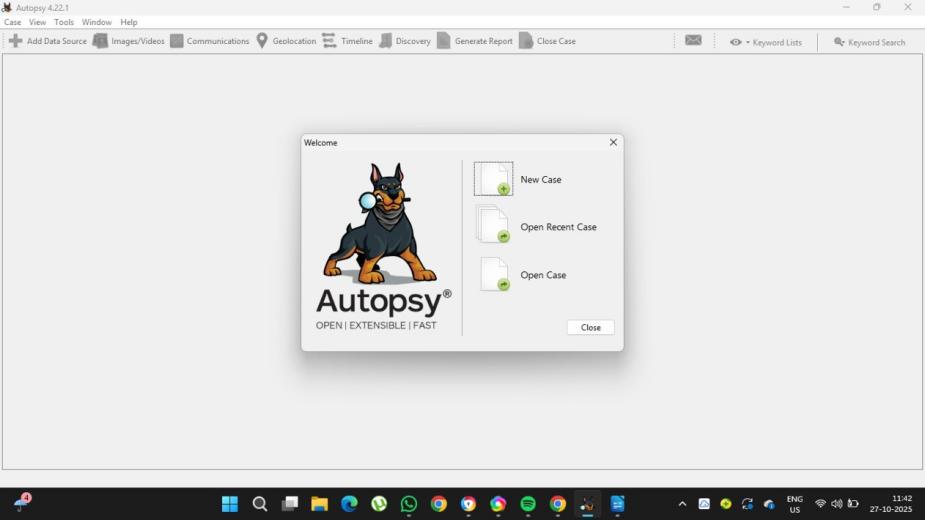
To perform static malware analysis using Ghidra by disassembling binary code,

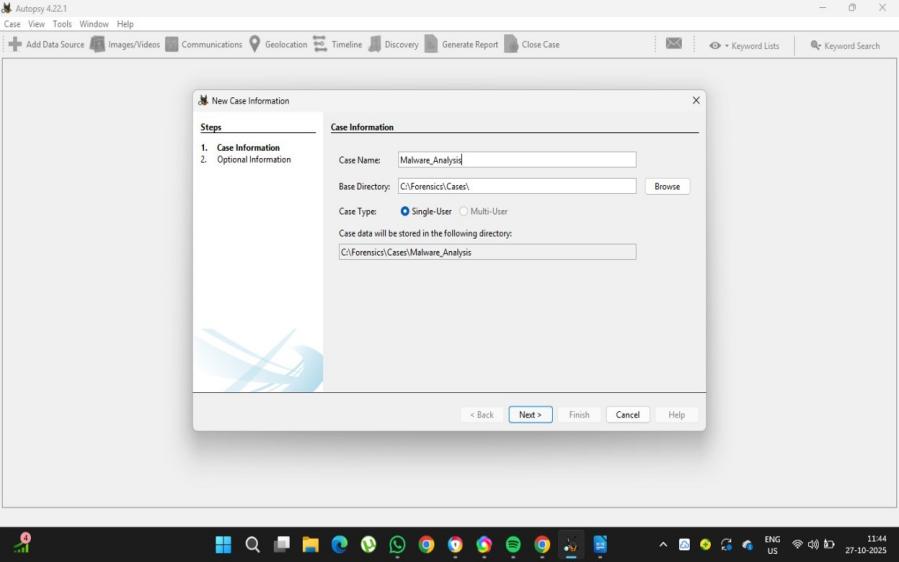
identifying malicious functions, and documenting the reverse engineering process.

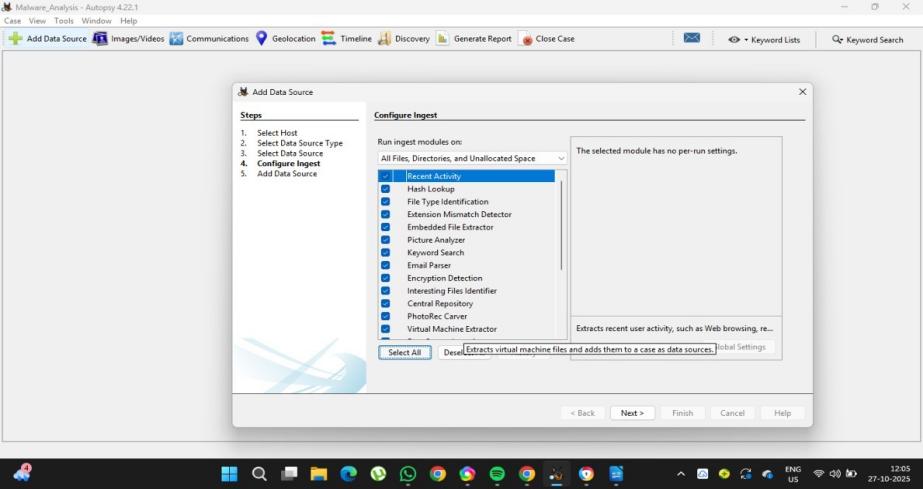
**DESCRIPTION OF THE TOOL USED:**

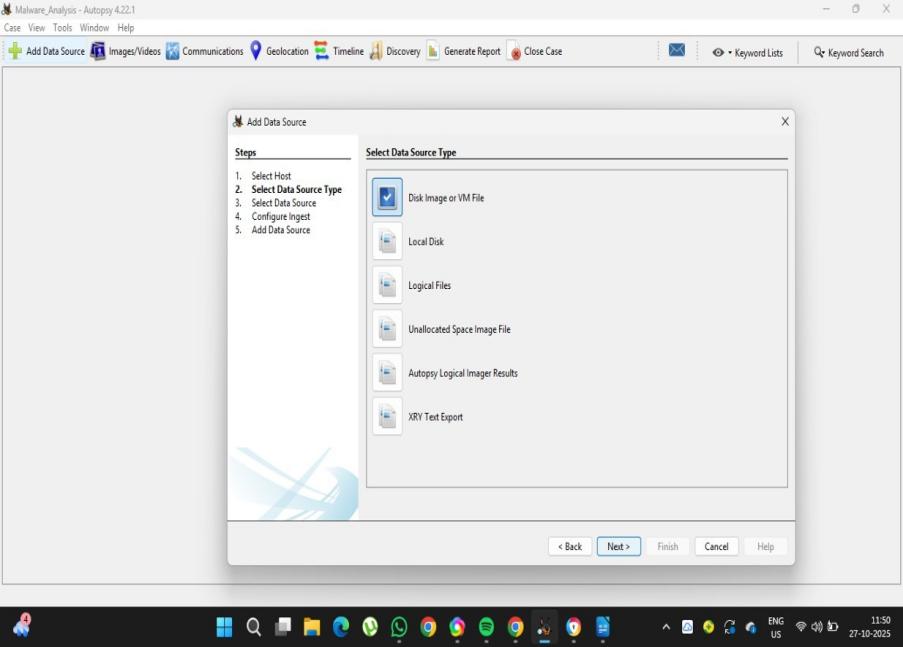
Ghidra is an open-source reverse engineering tool developed by the NSA. It disassembles and decompiles executable files for malware and security analysis. In this experiment, Autopsy was used alongside Ghidra to examine suspicious binary files. Ghidra helps forensic investigators understand code structure and identify embedded threats. It supports multiple architectures and detailed control-flow analysis. The experiment showed how reverse engineering complements forensic investigations in detecting malicious activity.

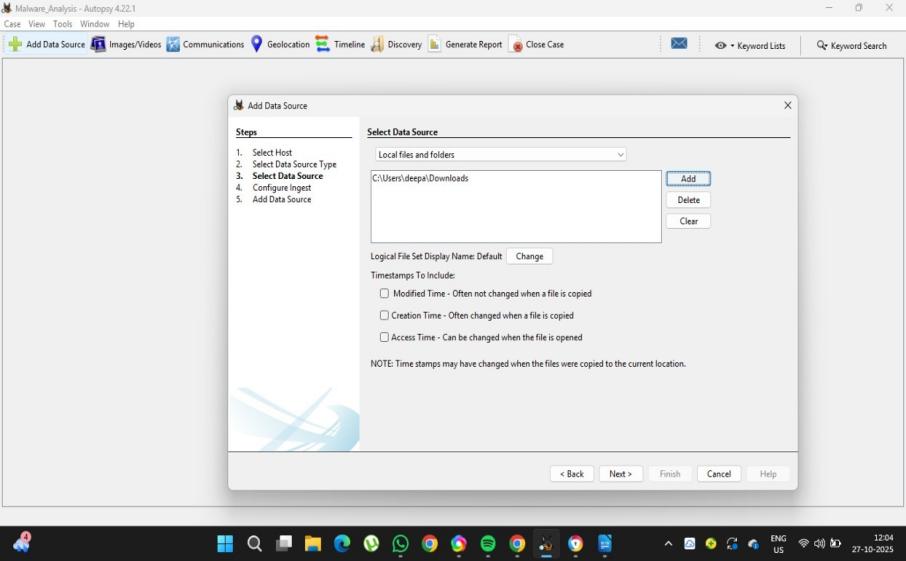
**STEPS INVOLVED IN GHIDRA:**

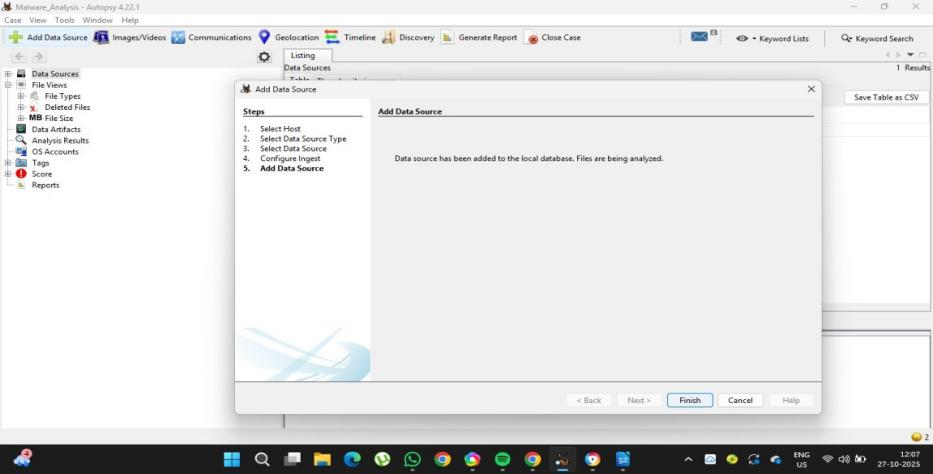




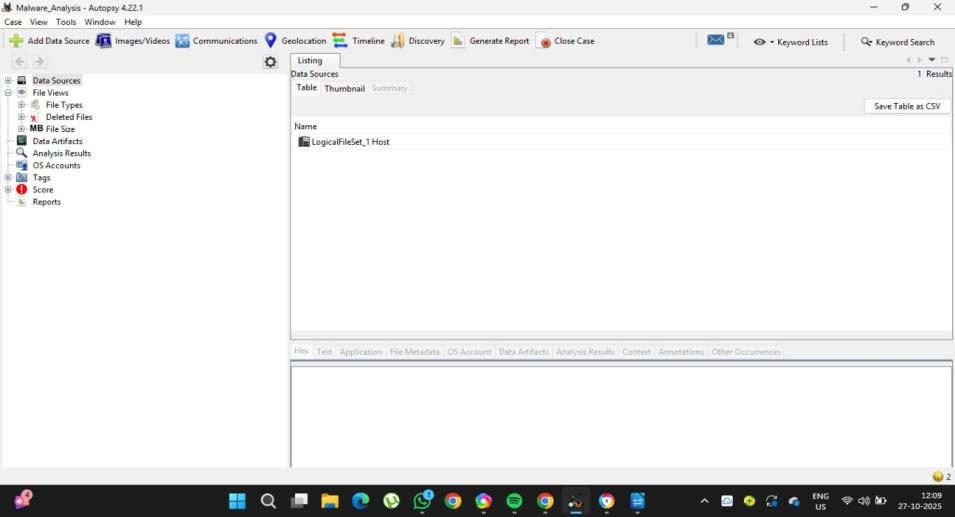








**OUTPUT:**

****