Ghidra is a debugging program and reverse engineering tool, used for malware analysis and program dissection without danger to the user’s device

Firstly, it’s most commonly used for reverse engineering malware, general software and firmware.  
Its wide array of tools and interfaces allow intermediate programmers to understand what they’re dealing with very easily, thanks to how it maps out functions

The graph function allows you to lay out the program into a graph, where you can see what the program is doing as interconnected boxes, like a family tree showing which functions are called by their parent function.

The emulator allows you to run the program in customizable environments, you can use the emulator to create a virtual machine on which to run your application, so as to not endanger your own computer.

The debugger lets you manually progress through the program. While it isn’t specific to Ghidra, it allows you to look at what the program does to better understand its inner workings, Ghidra has a large set of powerful debuggers to accommodate different workflows

Ghidra supports the creation of different tools written in python

### **Conclusion**

The current suite of tools provided by Ghidra can perform a large variety of tasks with ease