GHIDRA

NSA Reverse Engineering Software

Ghidra was built in support of NSA's Cybersecurity mission to streamline the process of complex software reverse engineering (SRE) efforts. NSA has applied Ghidra SRE capabilities to a variety of hard problems involving analyzing malicious code and generating deep insights for analysts who seek a better understanding of potential vulnerabilities in networks and systems.

This SRE framework developed by NSA's Research Directorate, includes a suite of full-featured, high-end software analysis tools that enable users to analyze compiled code on a variety of platforms including Windows, Mac OS, and Linux. Capabilities include disassembly, assembly, decompilation, graphing, and scripting, along with hundreds of other features. Ghidra supports a wide variety of processor instruction sets and executable formats and can be run in both user-interactive and automated modes. Users may also develop their own Ghidra plug-in components and/or scripts using the exposed application programing interface (API).

https://www.nsa.gov/ghidra

NOTICE: As a software reverse engineering (SRE) framework, Ghidra is designed solely to facilitate lawful SRE activities. You should always ensure that any SRE activities in which you engage are permissible as computer software may be protected under governing law (e.g., copyright) or under an applicable licensing agreement. In making Ghidra available for public use, the Agency does not condone or encourage any improper usage of Ghidra. Consistent with the Apache 2.0 license under which Ghidra has been made available, you are solely responsible for determining the appropriateness of using or redistributing Ghidra.

FEATURES AND BENEFITS

SLEIGH

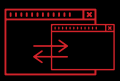
Ghidra uses a processor modeling language called Sleigh to specify how machine language instructions, unique to a given processor, are disassembled and then transformed to Ghidra's intermediate representation (IR) called p-code. Ghidra's full set of features, including decompilation, are enabled for a new processor simply by writing a Sleigh specification file. Existing Sleigh specifications can be changed by end users, supporting rapid updates, and adventurous users can write their own specifications.

UNDO/REDO

Instant undo/redo capability allows investigation without fear of making mistakes.

MULTI-USER COLLABORATION REPOSITORY

Using a multi-user server, teams can work together in order to cooperatively reverse engineer to a common understanding of a system.



DATA TYPE DEFINITIONS

As information is recovered or applied from additional sources such as header files or debug information, it can be shared by all programs within a system under evaluation.

SCRIPTING

Scripting environments for Java and Python are supported with an Eclipse integrated development environment to provide full debugging of scripts, and, in some cases, core Ghidra code.

CUSTOMIZABLE

Users may develop their own more complex features, such as loaders, analyzers, and visualizations using the robust program analysis API.

HEADLESS CAPABILITY

A command-line interface is available for automating mass binary analysis or for embedding Ghidra into alternative analysis pipelines.

HELP MENU

Extensive context-sensitive help is available for every action and feature.