

# Sig • Mal

Meeting 5

# GHIDRA

The National Security Agency released the source code of Ghidra, its reverse engineering tool, April 4.

This source code repository includes instructions to build on all supported platforms (macOS, Linux, and Windows). With this release, developers will be able to collaborate by creating patches, and extending the tool to fit their cybersecurity needs.


The source code is available for download at [ghidra-sre.org](https://ghidra-sre.org) along with the 9.1.1 patch.

Ghidra is a software reverse engineering (SRE) framework developed by NSA's [Research](#) Directorate for NSA's [cybersecurity mission](#). It helps analyze malicious code and malware like viruses, and can give cybersecurity professionals a better understanding of potential vulnerabilities in their networks and systems.


We look forward to ideas and contributions from the community!

For more NSA releases, check out [CODE.NSA.GOV](#) for open source, and NSA's [Technology Transfer Program](#) for other technology.


## Key features of Ghidra:




includes a suite of software analysis tools for analyzing compiled code on a variety of platforms including Windows, Mac OS, and Linux



capabilities include disassembly, assembly, decompilation, graphing and scripting, and hundreds of other features



supports a wide variety of processor instruction sets and executable formats and can be run in both user-interactive and automated modes.



users may develop their own Ghidra plug-in components and/or scripts using the exposed API

# CFG -- Control Flow Graphs

src::

<https://www.geeksforgeeks.org/software-engineering-control-flow-graph-cfg/>

- Software Engineering → graphical representation of control flow or computations during the execution of a program.

**LIVE DEMO TIME**