

Ghidra

Ghidra (pronounced GEE-druh;^[3] /ˈɡiːdrə/^[4]) is a free and open source reverse engineering tool developed by the National Security Agency (NSA) of the United States. The binaries were released at RSA Conference in March 2019; the sources were published one month later on GitHub.^[5] Ghidra is seen by many security researchers as a competitor to IDA Pro.^[6] The software is written in Java using the Swing framework for the GUI. The decompiler component is written in C++, and is therefore usable in a stand-alone form.^[7]

Scripts to perform automated analysis with Ghidra can be written in Java or Python (via Jython),^[8]^[9] though this feature is extensible and support for other programming languages is available via community plugins.^[10] Plugins adding new features to Ghidra itself can be developed using a Java-based extension framework.^[11]

History

Ghidra's existence was originally revealed to the public via Vault 7 in March 2017,^[12] but the software itself remained unavailable until its declassification and official release two years later.^[5] Some comments in its source code indicates that it existed as early as 1999.^[13]

High-level changelog^[14]^[15]

Version	Year	Major features
1.0	2003	Proof of concept
2.0	2004	Database, docking windows
3.0	2006	SLEIGH, decompiler, version control
4.0	2007	Scripting, version tracking
5.0	2010	File system browser
6.0	2014	First unclassified version
9.0	2019	First public release
9.2	2020	Graph visualization, new <u>PDB</u> parser
10.0	2021	Debugger
11.0	2023	Rust and Go binaries support, BSim
11.1	2024	<u>Swift</u> and <u>DWARF 5</u> support, <u>Mach-O</u> improvements

Ghidra





Disassembly of a file in Ghidra

Original author(s)	NSA
Initial release	March 5, 2019
Stable release	11.1 ^[1] / June 7, 2024
Repository	github.com /NationalSecurityAgency/ghidra (https://github.com/NationalSecurityAgency/ghidra)
Written in	<u>Java</u> , <u>C++</u>
License	<u>Apache License 2.0</u> / <u>Public domain</u> ^[2]
Website	ghidra-sre.org (https://ghidra-sre.org)

In June 2019, coreboot began to use Ghidra for its reverse engineering efforts on firmware-specific problems following the open source release of the Ghidra software suite.^[16]

Ghidra can be used, officially,^{[17][18]} as a debugger since Ghidra 10.0. Ghidra's debugger supports debugging user-mode Windows programs via WinDbg, and Linux programs via GDB.^[19]

Supported architectures

The following architectures or binary formats are supported:^[20] ^[21]

- x86 16, 32 and 64 bit
- ARM and AARCH64
- PowerPC 32/64 and VLE
- MIPS 16/32/64
- MicroMIPS
- 68xxx
- Java and DEX bytecode
- PA-RISC
- RISC-V
- eBPF
- BPF
- Tricore
- PIC 12/16/17/18/24
- SPARC 32/64
- CR16C
- Z80
- 6502
- MC6805/6809, HC05/HC08/HC12
- 8048, 8051, 8085
- CP1600
- MSP430
- AVR8, AVR32
- SuperH
- V850
- LoongArch
- Xtensa

See also

- IDA Pro
- JEB decompiler
- radare2
- Binary Ninja


References

1. "Releases · NationalSecurityAgency/ghidra" (<https://github.com/NationalSecurityAgency/ghidra/releases>). *GitHub*. Archived (<https://web.archive.org/web/20240608085420/https://github.com/NationalSecurityAgency/ghidra/releases>) from the original on June 8, 2024. Retrieved June 8, 2024.
2. "ghidra/NOTICE" (<https://github.com/NationalSecurityAgency/ghidra/blob/79d8f164f8bb8b15cfb60c5d4faeb8e1c25d15ca/NOTICE>). *GitHub.com*. Archived (<https://web.archive.org/web/20221027123954/https://github.com/NationalSecurityAgency/ghidra/blob/79d8f164f8bb8b15cfb60c5d4faeb8e1c25d15ca/NOTICE>) from the original on October 27, 2022. Retrieved April 13, 2019.

3. "Frequently asked questions" (<https://github.com/NationalSecurityAgency/ghidra/wiki/Frequently-asked-questions#how-do-you-pronounce-ghidra>). *GitHub.com*. Archived (<https://web.archive.org/web/20190305235545/https://github.com/NationalSecurityAgency/ghidra/wiki/Frequently-asked-questions#how-do-you-pronounce-ghidra>) from the original on March 5, 2019. Retrieved March 7, 2019.
4. "Come Get Your Free NSA Reverse Engineering Tool!" (<https://www.youtube.com/watch?v=r3N13ig8H7s&t=4>). *YouTube.com*. May 16, 2019. Archived (<https://ghostarchive.org/varchive/youtube/20211215/r3N13ig8H7s>) from the original on December 15, 2021. Retrieved May 17, 2019.
5. Newman, Lily Hay. "The NSA Makes Ghidra, a Powerful Cybersecurity Tool, Open Source" (<https://www.wired.com/story/nsa-ghidra-open-source-tool/>). *Wired*. Archived (<https://web.archive.org/web/20190306095048/https://www.wired.com/story/nsa-ghidra-open-source-tool/>) from the original on March 6, 2019. Retrieved March 6, 2019.
6. Cimpanu, Catalin. "NSA releases Ghidra, a free software reverse engineering toolkit" (<https://www.zdnet.com/article/nsa-release-ghidra-a-free-software-reverse-engineering-toolkit/>). *ZDNet*. Archived (<https://web.archive.org/web/20190306041159/https://www.zdnet.com/article/nsa-release-ghidra-a-free-software-reverse-engineering-toolkit/>) from the original on March 6, 2019. Retrieved March 7, 2019.
7. e. g. as Plugin (<https://rada.re/n/radare2.html>) Archived (<https://web.archive.org/web/20221014223153/https://rada.re/n/radare2.html>) 2022-10-14 at the Wayback Machine for Radare2 oder Rizin.
8. "Ghidra Scripting Class" (<https://github.com/NationalSecurityAgency/ghidra/blob/master/GhidraDocs/GhidraClass/Intermediate/Scripting.html>). *GitHub*. Archived (<https://web.archive.org/web/20230220023138/https://github.com/NationalSecurityAgency/ghidra/blob/master/GhidraDocs/GhidraClass/Intermediate/Scripting.html>) from the original on February 20, 2023. Retrieved February 19, 2023.
9. "Three Heads are Better Than One: Mastering NSA's Ghidra Reverse Engineering Tool" (<https://github.com/0xAlexei/INFILTRATE2019/blob/master/INFILTRATE%20Ghidra%20Slides.pdf>) (PDF). *GitHub*. Archived (<https://web.archive.org/web/20200301211705/https://github.com/0xAlexei/INFILTRATE2019/blob/master/INFILTRATE%20Ghidra%20Slides.pdf>) (PDF) from the original on March 1, 2020. Retrieved September 30, 2019.
10. "Ghidraal" (<https://github.com/jpleasu/ghidraal>). *GitHub*. Archived (<https://web.archive.org/web/20230220023155/https://github.com/jpleasu/ghidraal>) from the original on February 20, 2023. Retrieved February 19, 2023.
11. "Ghidra Advanced Development Class" (<https://github.com/NationalSecurityAgency/ghidra/blob/master/GhidraDocs/GhidraClass/AdvancedDevelopment/GhidraAdvancedDevelopment.html>). *GitHub*. Archived (<https://web.archive.org/web/20230220023139/https://github.com/NationalSecurityAgency/ghidra/blob/master/GhidraDocs/GhidraClass/AdvancedDevelopment/GhidraAdvancedDevelopment.html>) from the original on February 20, 2023. Retrieved February 19, 2023.
12. "NSA to release a free reverse engineering tool" (<https://www.zdnet.com/article/nsa-to-release-a-free-reverse-engineering-tool/>). *ZDNET*. Archived (<https://web.archive.org/web/20240222203111/https://www.zdnet.com/article/nsa-to-release-a-free-reverse-engineering-tool/>) from the original on February 22, 2024. Retrieved February 22, 2024.
13. "Build software better, together" (<https://github.com/search?q=repo:NationalSecurityAgency/ghidra+1999+language:Java&type=code&l=Java>). *GitHub*. Archived (<https://web.archive.org/web/20240222203731/https://github.com/search?q=repo:NationalSecurityAgency/ghidra+1999+language:Java&type=code&l=Java>) from the original on February 22, 2024. Retrieved February 22, 2024.
14. "ghidra/Ghidra/Configurations/Public_Release/src/global/docs/ChangeHistory.html at master · NationalSecurityAgency/ghidra" (https://github.com/NationalSecurityAgency/ghidra/blob/master/Ghidra/Configurations/Public_Release/src/global/docs/ChangeHistory.html). *GitHub*. Archived (https://web.archive.org/web/20240508162105/https://github.com/NationalSecurityAgency/ghidra/blob/master/Ghidra/Configurations/Public_Release/src/global/docs/ChangeHistory.html) from the original on May 8, 2024. Retrieved May 8, 2024.
15. *Ghidra - Journey from Classified NSA Tool to Open Source* (<https://www.youtube.com/watch?v=kx2xp7IQNSc>). Archived (<https://web.archive.org/web/20240508162105/https://www.youtube.com/watch?v=kx2xp7IQNSc>) from the original on May 8, 2024. Retrieved May 8, 2024 – via www.youtube.com.
16. "Coreboot Project Is Leveraging NSA Software To Help With Firmware Reverse Engineering" (https://www.phoronix.com/scan.php?page=news_item&px=Ghidra-Coreboot-NSA-RE). Archived (https://web.archive.org/web/20190604134804/https://www.phoronix.com/scan.php?page=news_item&px=Ghidra-Coreboot-NSA-RE) from the original on June 4, 2019. Retrieved June 5, 2019.

17. "Compiled/built Ghidra 9.3 for Windows with Debugger feature by Galician R&D Center in Advanced Telecommunications employees" (https://www.linkedin.com/posts/davidalvarezperez_ghidra-software-reverse-engineering-for-beginners-activity-6746028492950945792-F8BG). Archived (https://web.archive.org/web/20221125075600/https://www.linkedin.com/posts/davidalvarezperez_ghidra-software-reverse-engineering-for-beginners-activity-6746028492950945792-F8BG?utm_source=share&utm_medium=member_desktop) from the original on November 25, 2022. Retrieved November 25, 2022.
18. "Analizando el depurador de Ghidra" (<https://www.gradiant.org/blog/analizando-el-depurador-de-ghidra/>). March 11, 2021. Archived (<https://web.archive.org/web/20221214230458/https://www.gradiant.org/blog/analizando-el-depurador-de-ghidra/>) from the original on December 14, 2022. Retrieved December 14, 2022.
19. "What's new in Ghidra 10.0" (https://htmlpreview.github.io/?https://github.com/NationalSecurityAgency/ghidra/blob/Ghidra_10.0_build/Ghidra/Configurations/Public_Release/src/global/docs/WhatsNew.html). Archived (https://web.archive.org/web/20230619084429/https://htmlpreview.github.io/?https://github.com/NationalSecurityAgency/ghidra/blob/Ghidra_10.0_build/Ghidra/Configurations/Public_Release/src/global/docs/WhatsNew.html) from the original on June 19, 2023. Retrieved June 24, 2021.
20. Joyce, Rob [@RGB_Lights] (March 5, 2019). "Ghidra processor modules: X86 16/32/64, ARM/AARCH64, PowerPC 32/64, VLE, MIPS 16/32/64, micro, 68xxx, Java / DEX bytecode, PA-RISC, PIC 12/16/17/18/24, Sparc 32/64, CR16C, Z80, 6502, 8051, MSP430, AVR8, AVR32, Others+ variants as well. Power users can expand by defining new ones" (https://x.com/RGB_Lights/status/1103019876203978752) (Tweet). Archived (https://web.archive.org/web/20190307005026/https://twitter.com/RGB_Lights/status/1103019876203978752) from the original on March 7, 2019. Retrieved March 6, 2019 – via [Twitter](#).
21. "List of Processors Supported by Ghidra" (<https://github.com/NationalSecurityAgency/ghidra/tree/master/Ghidra/Processors>). *Github.com*. Archived (<https://web.archive.org/web/20231012032914/https://github.com/NationalSecurityAgency/ghidra/tree/master/Ghidra/Processors>) from the original on October 12, 2023. Retrieved September 29, 2023.

External links

- [Official website](https://www.ghidra-sre.org/) (<https://www.ghidra-sre.org/>) 
- [ghidra](https://github.com/NationalSecurityAgency/ghidra) (<https://github.com/NationalSecurityAgency/ghidra>) on [GitHub](#)

Retrieved from "<https://en.wikipedia.org/w/index.php?title=Ghidra&oldid=1238000131>"