Interactive Disassembler

The **Interactive Disassembler (IDA)** is a disassembler for computer software which generates assembly language source code from machine-executable code. It supports a variety of executable formats for different processors and operating systems. It can also be used as a debugger for Windows PE, Mac OS X Mach-O, and Linux ELF executables. A decompiler plug-in, which generates a high level, C source code-like representation of the analysed program, is available at extra cost.[4][5]

IDA is used widely in software reverse engineering, including for malware analysis[6][7] and software vulnerability research.[8] IDA has been referred to as the "de-facto industry standard disassembler".[9][10][11][12]

History

Ilfak Guilfanov began working on IDA in 1990,[13][14][15][16] and initially distributed it as a shareware application. In 1996, the Belgian company DataRescue took over the development of IDA and began to sell it as a commercial product, under the name IDA Pro.[17][18]

Initial versions of IDA did not have a graphical user interface (GUI), and ran as an extended DOS, OS/2, or Windows console application.[19] In 1999, DataRescue released the first version of IDA Pro with a GUI, IDA Pro 4.0.[20]

In 2005, Guilfanov founded Hex-Rays to pursue the development of the Hex-Rays Decompiler IDA extension.[21][22] In January 2008, Hex-Rays assumed the development and support of DataRescue's IDA Pro.[23][24]

In 2022, Hex-Rays was acquired by Smartfin, a European venture capital and private equity investor.[25][26]

Features

IDA disassembles a compiled program back into an assembly language representation. In addition to performing basic disassembly, IDA also automatically annotates disassembled programs with information about:[27]

- cross-references between code and data in the program
- function locations, function stack frames, and function calling conventions
- reconstructed data types

Interactive Disassembler

Portrait of Françoise d'Aubigné, whose image is used as the IDA logo

Original author(s)	Ilfak Guilfanov
Developer(s)	Hex-Rays
Initial release	May 21, 1991[1]
Stable release	8.4 SP2[2] / May 27, 2024
Written in	C++[3]
Operating system	Microsoft Windows, Mac OS X, and Linux
Available in	English, Russian
Type	Disassembler, Decompiler
License	Proprietary
Website	hex-rays.com /ida-pro/ (http s://hex-rays.co m/ida-pro/)

However, the nature of disassembly precludes total accuracy, and a great deal of human intervention is necessarily required; IDA has interactive functionality to aid in improving the disassembly. A typical IDA user will begin with an automatically generated disassembly listing and then convert sections from code to data and vice versa, rename, annotate, and otherwise add information to the listing, until its functionality becomes clear.

Scripting

"IDC scripts" make it possible to extend the operation of the disassembler. Some helpful scripts are provided, which can serve as the basis for user written scripts. Most frequently scripts are used for extra modification of the generated code. For example, external symbol tables can be loaded thereby using the function names of the original source code.

Users have created plugins that allow other common scripting languages to be used instead of, or in addition to, IDC. IdaRUB[28] supports Ruby and IDAPython[29] adds support for Python. As of version 5.4, IDAPython (dependent on Python 2.5) comes preinstalled with IDA Pro.

Debugging

IDA Pro supports a number of debuggers,[30] including:

- Remote Windows, Linux, and Mac applications (provided by Hex-Rays) allow running an executable in its native environment (presumably using a virtual machine for malware)
- GNU Debugger (gdb) is supported on Linux and OS X, as well as the native Windows debugger
- A Bochs plugin is provided for debugging simple applications (i.e., damaged UPX or mpress compacted executables)
- An Intel PIN-based debugger
- A trace replayer

Versions

The latest full version of IDA Pro is commercial (version 8.4 as of June 2024), while a less capable version, named IDA Free, is available for download free of cost.[31]

Supported systems/processors/compilers

- System hosts

  - Windows x86 and ARM
  - Linux x86
  - Mac OS X x86
- Recognized executable file formats

  - COFF and derivatives, including Win32/64/generic PE
  - ELF and derivatives (generic)
  - Mach-O (Mach)
  - NLM (NetWare)
  - LC/LE/LX (OS/2 2.x+ and various DOS extenders)
  - NE (OS/2 1.x, Win16, and various DOS extenders)
  - MZ (MS-DOS)
  - OMF and derivatives (generic)
  - AIM (generic)

- raw binary, such as a ROM image or a COM file
- Instruction sets
  - Intel 80x86 family
  - ARM architecture
  - Motorola 68k and H8
  - Zilog Z80
  - MOS 6502
  - Intel i860
  - DEC Alpha
  - Analog Devices ADSP218x
  - Angstrem KR1878
  - Atmel AVR series
  - DEC series PDP11
  - Fujitsu F2MC16L/F2MC16LX
  - Fujitsu FR 32-bit Family
  - Hitachi SH3/SH3B/SH4/SH4B
  - Hitachi H8: h8300/h8300a/h8s300/h8500
  - Intel 196 series: 80196/80196NP
  - Intel 51 series: 8051/80251b/80251s/80930b/80930s
  - Intel i960 series
  - Intel Itanium (ia64) series
  - Java virtual machine
  - MIPS: mipsb/mipsl/mipsr/mipsrl/r5900b/r5900l
  - Microchip PIC: PIC12Cxx/PIC16Cxx/PIC18Cxx
  - MSIL
  - Mitsubishi 7700 Family: m7700/m7750
  - Mitsubishi m32/m32rx
  - Mitsubishi m740
  - Mitsubishi m7900
  - Motorola DSP 5600x Family: dsp561xx/dsp5663xx/dsp566xx/dsp56k
  - Motorola ColdFire
  - Motorola HCS12
  - NEC 78K0/78K0S
  - PA-RISC
  - PowerPC
  - Xenon PowerPC Family
  - SGS-Thomson ST20/ST20c4/ST7
  - SPARC Family
  - Samsung SAM8
  - Siemens C166
  - TMS320Cxxx series
- Compiler/libraries (for automatic library function recognition)[32]
  - Borland C++ 5.x for DOS/Windows
  - Borland C++ 3.1
  - Borland C Builder v4 for DOS/Windows
  - GNU C++ for Cygwin
  - Microsoft C
  - Microsoft QuickC
  - Microsoft Visual C++

- - Watcom C/C++ (16/32 bit) for DOS/OS2
  - ARM C v1.2
  - GNU C++ for Unix/common

Logo

IDA Pro's logo is a cropped image of Françoise d'Aubigné, Marquise de Maintenon. The logo image is similar to a miniature painting of Françoise d'Aubigné attested to a painter in the circle of Pierre Mignard.[33]

The original greyscale version of the logo was introduced in September 1999, with the release of IDA 4.0.[15] Ilfak Guilfanov has stated that the logo is not a depiction of Saint Ida of Louvain.[34]

See also

- Binary Ninja
- Cheat engine
- Ghidra
- JEB
- Radare2

References

1. Czokow, Geoffrey (2021-05-20). "IDA: celebrating 30 years of binary analysis innovation" (https://hex-rays.com/blog/ida-celebrating-30-years-of-binary-analysis-innovation/). *Hex-Rays*. Retrieved 2023-03-19.
2. "IDA 8.4.240527 (8.4sp2)" (https://hex-rays.com/products/ida/news/8_4sp2/). Archived (https://web.archive.org/web/20240602042117/https://hex-rays.com/products/ida/news/8_4sp2/) from the original on June 2, 2024. Retrieved June 28, 2024.
3. "Hex-rays Home" (http://www.hex-rays.com/). Archived (https://web.archive.org/web/20240526003338/https://hex-rays.com/) from the original on 2024-05-26. Retrieved 2008-03-31.
4. Eagle, Chris (2011). "Chapter 23: Real-World IDA Plug-ins". *The IDA Pro Book : the Unoffical Guide to the World's Most Popular Disassembler* (https://www.worldcat.org/oclc/830164382) (2nd ed.). San Francisco: No Starch Press. pp. 500–502. ISBN 978-1-59327-395-8. OCLC 830164382 (https://www.worldcat.org/oclc/830164382).
5. "Hex-Rays Decompiler" (https://hex-rays.com/decompiler/). *hex-rays.com*. Retrieved 2023-03-18.
6. Staff, S. C. (2017-09-11). "Hex-Rays IDA Pro" (https://www.scmagazine.com/product-test/content/hex-rays-ida-pro). *SC Media*. Retrieved 2023-03-13.
7. Sikorski, Michael (2012). "Chapter 5. IDA Pro". *Practical Malware Analysis : a Hands-On Guide to Dissecting Malicious Software* (https://www.worldcat.org/oclc/830164262). Andrew Honig. San Francisco: No Starch Press. ISBN 978-1-59327-430-6. OCLC 830164262 (https://www.worldcat.org/oclc/830164262).
8. Shoshitaishvili, Yan; Wang, Ruoyu; Salls, Christopher; Stephens, Nick; Polino, Mario; Dutcher, Andrew; Grosen, John; Feng, Siji; Hauser, Christophe; Kruegel, Christopher; Vigna, Giovanni (2016-05-22). "SOK: (State of) the Art of War: Offensive Techniques in Binary Analysis" (https://ieeexplore.ieee.org/document/7546500). *2016 IEEE Symposium on Security and Privacy (SP)*. pp. 138–157. doi:10.1109/SP.2016.17 (https://doi.org/10.1109%2FSP.2016.17). hdl:11311/1161277 (https://hdl.handle.net/11311%2F1161277). ISBN 978-1-5090-0824-7. S2CID 3337994 (https://api.semanticscholar.org/CorpusID:3337994). Archived (https://web.archive.org/web/20221208155740/https://ieeexplore.ieee.org/document/7546500/) from the original on 2022-12-08. Retrieved 2023-03-17.

9. Ben Khadra, M. Ammar; Stoffel, Dominik; Kunz, Wolfgang (2016-10-01). "Speculative disassembly of binary code" (https://doi.org/10.1145/2968455.2968505). *Proceedings of the International Conference on Compilers, Architectures and Synthesis for Embedded Systems*. CASES '16. New York, NY, USA: Association for Computing Machinery. pp. 1–10. doi:10.1145/2968455.2968505 (https://doi.org/10.1145%2F2968455.2968505). ISBN 978-1-4503-4482-1. S2CID 16206393 (https://api.semanticscholar.org/CorpusID:16206393). "It outperforms IDA Pro, the de-facto industry standard disassembler, in terms of disassembly correctness."

10. Di Federico, Alessandro; Payer, Mathias; Agosta, Giovanni (2017-02-05). "Rev.ng: A unified binary analysis framework to recover CFGS and function boundaries" (https://doi.org/10.1145/3033019.3033028). *Proceedings of the 26th International Conference on Compiler Construction*. CC 2017. New York, NY, USA: Association for Computing Machinery. pp. 131–141. doi:10.1145/3033019.3033028 (https://doi.org/10.1145%2F3033019.3033028). ISBN 978-1-4503-5233-8. S2CID 15830760 (https://api.semanticscholar.org/CorpusID:15830760). "We evaluate our prototype implementation against the de-facto industry standard for static binary analysis, IDA Pro,"

11. Garcia Prado, Carlos; Erickson, Jon (April 10, 2018). "Solving Ad-hoc Problems with Hex-Rays API" (https://web.archive.org/web/20220602140613/https://www.fireeye.com/blog/threat-research/2018/04/solving-ad-hoc-problems-with-hex-rays-api.html). *FireEye Threat Research Blog*. Archived from the original (https://www.fireeye.com/blog/threat-research/2018/04/solving-ad-hoc-problems-with-hex-rays-api.html) on 2022-06-02. Retrieved March 12, 2023. "IDA Pro is the de facto standard when it comes to binary reverse engineering."

12. Andriesse, Dennis (2019). "Appendix C: List of Binary Analysis Tools". *Practical binary analysis : build your own Linux tools for binary instrumentation, analysis, and disassembly* (https://www.worldcat.org/oclc/1050453850). San Francisco, CA. ISBN 978-1-59327-913-4. OCLC 1050453850 (https://www.worldcat.org/oclc/1050453850). "This [IDA Pro] is the de facto industry-standard recursive disassembler."

13. Гильфанов, Ильфак (22 May 2003). "IDA Pro - samyj moshhnyj dizassembler v mire" IDA Pro - самый мощный дизассемблер в мире (https://web.archive.org/web/20210515200735/https://fcenter.ru/online/softarticles/interview/6704) [IDA Pro - the most powerful disassembler in the world] (Interview) (in Russian). Interviewed by Доля, Алексей. Компания "Ф-Центр". sec. 2.30. Archived from the original (https://fcenter.ru/online/softarticles/interview/6704) on May 15, 2021. Retrieved 14 March 2023. "Он начался как хобби в далеком 1991 году, просто увлечением для себя и для друзей."

14. "IDA Pro - Часто задаваемые вопросы" (https://web.archive.org/web/20031219030300/http://www.idapro.ru/faq.html#053). Archived from the original (http://www.idapro.ru/faq.html#053) on December 19, 2003. "Первые строки для IDA были написаны в декабре 1990."

15. Czokow, Geoffrey (2021-05-20). "IDA: celebrating 30 years of binary analysis innovation" (https://hex-rays.com/blog/ida-celebrating-30-years-of-binary-analysis-innovation/). *Hex-Rays*. Retrieved 2023-03-19.

16. "Hex Rays - State-of-the-art binary code analysis solutions" (https://hex-rays.com/about-us/our-journey/). *hex-rays.com*. Archived (https://web.archive.org/web/20230531100330/https://hex-rays.com/about-us/our-journey/) from the original on 2023-05-31. Retrieved 2023-07-21.

17. Guilfanov, Ilfak, *CODE BLUE 2014 : Ilfak Guilfanov - Keynote : The story of IDA Pro* (https://www.youtube.com/watch?v=hLBlck1ITUs), retrieved 2023-03-16, "Datarescue converted my hobby project into a commercial program in 1996."

18. "DataRescue IDA Pro Page" (https://web.archive.org/web/19970214111312/http://www.datarescue.com/ida.htm). *DataRescue*. Archived from the original (http://www.datarescue.com/ida.htm) on 1997-02-14.

19. "DataRescue IDA Page : download an evaluation version" (https://web.archive.org/web/19970214112722/http://www.datarescue.com/idadown.htm). *DataRescue*. Archived from the original (http://www.datarescue.com/idadown.htm) on 1997-02-14.

20. "DataRescue IDA Pro What's new Page" (https://web.archive.org/web/19991010010636/http://datarescue.com:80/idanew.htm). *DataRescue*. Archived from the original (http://datarescue.com:80/idanew.htm) on 1999-10-10.

21. "Gegevens van de geregistreerde entiteit | KBO Public Search" (https://kbopub.economie.fgov.be/kbopub/toonondernemingps.html?ondernemingsnummer=873473914). *kbopub.economie.fgov.be*. Retrieved 2023-03-13.

22. "Hex-Rays Decompiler" (https://web.archive.org/web/20071011044755/http://www.hex-rays.com/products.shtml). *Hex-Rays*. Archived from the original (http://www.hex-rays.com/products.shtml) on 2007-10-11.

23. "DataRescue Home Page : home of the IDA Pro Disassembler and of PhotoRescue" (https://web.archive.org/web/20080221202137/http://www.datarescue.com:80/). *DataRescue*. Archived from the original (http://www.datarescue.com/) on 2008-02-21. "News 07/01/2008: IDA Pro moves to Hex-Rays."

24. "Hex-Rays Home Page" (https://web.archive.org/web/20080212081246/http://www.hex-rays.com/index.shtml). *Hex-Rays*. Archived from the original (http://www.hex-rays.com/index.shtml) on 2008-02-12.

25. "A consortium of investors acquires Hex-Rays – Hex Rays" (https://hex-rays.com/blog/hex-rays-acquisition/). Archived (https://web.archive.org/web/20230721143654/https://hex-rays.com/blog/hex-rays-acquisition/) from the original on 2023-07-21. Retrieved 2023-07-21.

26. "News Industry | Smartfin led consortium acquires Hex-Rays to accelerate product innovation efforts" (https://www.helpnetsecurity.com/2022/10/21/hex-rays-smartfin/). *Help Net Security*. 2022-10-20. Archived (https://web.archive.org/web/20230721143654/https://www.helpnetsecurity.com/2022/10/21/hex-rays-smartfin/) from the original on 2023-07-21. Retrieved 2023-07-21.

27. Eagle, Chris (2011). "Part II. Basic IDA Usage". *The IDA Pro Book : the Unoffical Guide to the World's Most Popular Disassembler* (https://www.worldcat.org/oclc/830164382) (2nd ed.). San Francisco: No Starch Press. ISBN 978-1-59327-395-8. OCLC 830164382 (https://www.worldcat.org/oclc/830164382).

28. "Archived copy" (https://github.com/spoonm/idarub). Archived (https://web.archive.org/web/20160108085820/https://github.com/spoonm/idarub) from the original on 2016-01-08. Retrieved 2011-12-05.

29. "Idapython [d-dome.net]" (https://web.archive.org/web/20060116123556/http://d-dome.net/idapython/). Archived from the original (http://d-dome.net/idapython/) on 2006-01-16.

30. Eagle, Chris (2008). *The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler*. No Starch Press. ISBN 978-1-59327-178-7.

31. "IDA Pro Freeware version download" (http://www.hex-rays.com/idapro/idadownfreeware.htm). Archived (https://web.archive.org/web/20080808195925/http://www.hex-rays.com/idapro/idadownfreeware.htm) from the original on 2008-08-08. Retrieved 2008-03-31.

32. "FLIRT Compiler Support" (http://www.hex-rays.com/idapro/idaflirtcomp.htm). Hex-Rays. Archived (https://web.archive.org/web/20111003155049/http://www.hex-rays.com/idapro/idaflirtcomp.htm) from the original on 2011-10-03. Retrieved 2010-04-13.

33. "Französische Schule, Nachfolge Pierre Mignard - Osterauktion 17.04.2019 - Schätzwert: EUR 1.500 bis EUR 2.600 - Dorotheum" (https://www.dorotheum.com/de/l/6130641/,%20https://www.dorotheum.com/de/l/6130641/). *www.dorotheum.com* (in Austrian German). Archived (https://web.archive.org/web/20230814052857/https://www.dorotheum.com/de/l/6130641/,%20https://www.dorotheum.com/de/l/6130641/) from the original on 2023-08-14. Retrieved 2024-07-08.

34. Guilfanov, Ilfak (2006-04-13). "Sainte Ida | Hex Blog" (http://www.hexblog.com/?p=38). *Hex Blog*. Archived (https://web.archive.org/web/20110617113702/http://www.hexblog.com/?p=38) from the original on 2011-06-17. Retrieved 2024-07-08.

Further reading

- Eilam, Eldad (2005). *Reversing: Secrets of Reverse Engineering*. Wiley Publishing. p. 595. ISBN 0-7645-7481-7.

External links

- Official website (https://www.hex-rays.com/products/ida/index.shtml)
- "IDA Pro on Internet Archive" (https://web.archive.org/web/20150116040613/http://www.idapro.ru/) (in Russian). Archived from the original (http://www.idapro.ru/) on 2015-01-16.
- "IDA plug-ins and scripts" (http://www.openrce.org). *Open Reverse Code Engineering (OpenRCE)*.