IDA PRO – the state-of-the-art binary code analysis tool

IDA Pro is the flagship product of Hex-Rays, the software provider in reverse engineering. Being an interactive and programmable disassembler and debugger, IDA Pro provides excellent quality performance on different platforms and is compatible with many processors. IDA Pro has become the de-facto standard for the analysis of hostile code, vulnerability research and commercial off-the-shelf validation.

IDA Pro comes with different types of licenses: Named, Computer, Floating and Educational license to meet different business’ scales and demands of usage.

Key features

Multi-processor Disassembler

• Disassembler modules for a large number of processors. The free SDK even allows you to run your custom disassembler;
• Full and extensible interactivity;
• Programmable: IDA can be extended in line with user’s own requirement with IDC or IDAPython
• Open plugin architecture: external plugins enable extension of IDA’s capability
• FLIRT technology (Fast library identification and recognition technology);
• Code graphing
• Lumina server holds metadata with a large number of well-known functions

Multi-target Debugger

• The debugger adds the dynamic analysis of the information collected statically by the disassembler;
• Offers all the features expected from a debugger and more: “remote” function and tracking. Remote debugger: for Windows, Linux, Mac OS X, and other machines in any combination;

More features and upgrades are introduced along with new IDA version releases!
IDA 7.7 Highlights Release date: December 2021

iOS15 and macOS 12 support

Apple has made major changes to the internal format of core OS files. In particular, the DYLD Shared Cache (DSC) has been split into multiple parts. Our Mach-O loader and the helper DSCU plugin have been updated to handle this seamlessly. We have also updated our iOS and Mac debuggers to handle peculiarities of debugging in the new OS versions.

Clang-based C++ parser

In addition to the built-in C parser, IDA now supports an additional parser based on libclang. It allows IDA to handle complex, real-life C, C++, and Objective-C syntax found in STL, MFC, Apple's XNU and iOS SDK, and Linux kernel headers. We will also soon provide a command-line version to build your own type libraries – stay tuned!

Thanks to Clang-based parser, now the types from the Boost library can be parsed:

Configuring it is very easy:
Golang improvements

We took our golang analysis to another level. Detection of golang binaries is more robust thanks to the standard startup code detection, and standard library signatures allow you to ignore unimportant functions. We also use more of the rich metadata present in Go binaries:

- Functions are automatically grouped into folders by modules. Once you enable folders, these groups will be visible:

![Golang function grouping](image)

- Reflection metadata is parsed to recover types used by the program:

![Reflection metadata](image)

UI candy

- The Lock Highlight button now allows you to have multiple permanent highlights in the database, so you can see the important things at a glance.
- New icons to easily hide or unhide the listing elements, like functions, segments, etc.
- Output window gained an option to enable timestamps making it easier to keep track of the various messages printed there.
- Qt libraries have been upgraded to version 5.15.2, offering improved support for HiDPI (4K+) screens, as well as native support for macOS’s “dark mode”.
• Switching between IDA's windows using a keyboard just got easier: hold down Alt to reveal the corresponding digit you need to press to switch to that window.

• Breakpoints list now uses the standard folder view for grouping. You can enable or disable all breakpoints in a folder with one click.

Multiple highlights:
Breakpoint groups:

New processors

Two new processor modules were added in this release: Cadence Tensilica Xtensa and the Renesas RX series.

RX processor:

XTensa processor:
Type system

Basic type system support has been enabled for all processors. This means that now you can use C syntax declarations for structures and enums via the Local Types editor or by parsing C headers. DWARF types are also imported, when available. FYI, DWARF5, the new version of the debug format, which is the default since GCC 11, is now supported.

RISC-V types imported from DWARF:

Decompilers

We have ported our decompiler to MIPS64. We have also added support for some of the custom instructions of Cavium OCTEON MIPS processors used in advanced network equipment. Currently only n64 ABI is supported for MIPS64. Of course, the existing decompilers also received numerous improvements and fixes. For example, the new extended flow guard (XFG) calls are handled in x64 and ARM64 Windows binaries.

Full changelist: https://www.hex-rays.com/products/ida/news/7_7/
Previous releases

IDA Version 7.6 - Release date: 28th April 2021

Highlights: The Service Pack 1 of IDA 7.6 is primarily a bug fixes release that provides fixes for a few errors that might affect many users.

Full changelist: https://www.hex-rays.com/products/ida/news/7_6sp1/

IDA Version 7.6 - Release date: 22nd March 2021

Highlights: IDA 7.5 introduced Apple Silicon's full support, Golang analysis, thorough improvements for Hex-Rays Decompiler, two new processor: RISC-V and RL78, further supports for compressed macOS and iOS kernelcache and for Python 3.9

Full changelist: https://www.hex-rays.com/products/ida/news/7_6/

IDA Version 7.5 - Release date: May 2020

Highlights: IDA 7.5 introduced the tree-like folder view that helped with information organization and hence incredibly increase efficiency when it comes to large binaries analysis. MIPS decompiler was added to the lineup, with Lumina now available for both MIPS and PPC binaries. IDA 7.5 comprised many iOS/macOS improvements such as the just-added type libraries with the most major APIs and additional frameworks from macOS and iPhone SDKs.

Full changelist: https://www.hex-rays.com/products/ida/news/7_5/

IDA Version 7.5 – Service Pack 1 - Release date: 19th June 2020

Highlights: This Service Pack was released to improve user experience especially for newly released features such as the tree-like folder view function and the MIPS Decompiler.

Full changelist: https://www.hex-rays.com/products/ida/news/7_5sp1/

IDA Version 7.5 – Service Pack 2 - Release date: 28th July 2020

Highlights: This release fixes some immediate issues with the new macOS11/iOS14 binaries and focuses principally on enhancing the static analysis for new file formats. MH_FILESET kernelcache format is fully supported, Objective-C metadata is improved and type libraries for MacOSX11.0.sdk and iPhoneOS14.0.sdk was added.

Full changelist: https://www.hex-rays.com/products/ida/news/7_5sp2/

IDA Version 7.5 – Service Pack 3 - Release date: 28th October 2020

Highlights: This service pack introduces a handful of new and interesting features specific to the soon-to-be-released macOS 11 (Big Sur) and provides fixes for numerous minor issues. macOS11 kernel debugging with VMware Fusion 12 and symbolication of MH_FILESET kernelcaches were both improved.

Full changelist: https://www.hex-rays.com/products/ida/news/7_5sp3/