hex-rays

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.

A disassembler


A debugger


interactive


Programmable

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

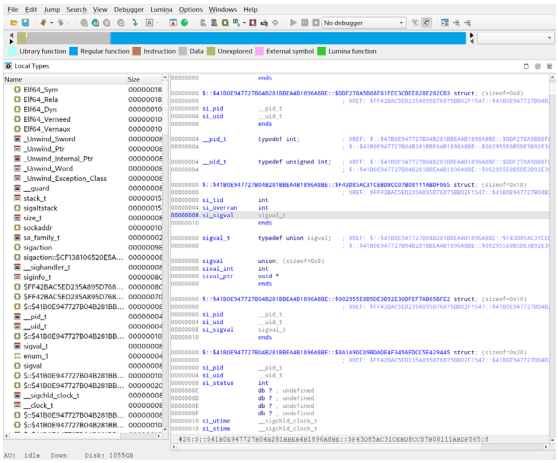
- The debugger adds the dynamic analysis of the information collected statically by the disassembler;
- Offers all the features expected from a debugger and more: "remote" function and tracking. Remote debugger: for Windows, Linux, Mac OS X, and other machines in any combination;

More features and upgrades are introduced along with new IDA version releases!

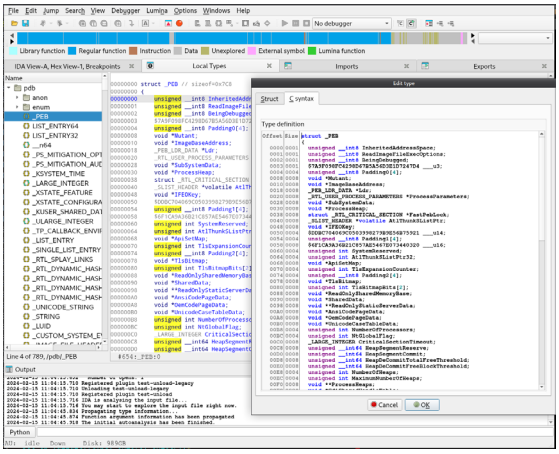
IDA 8.4 Highlights

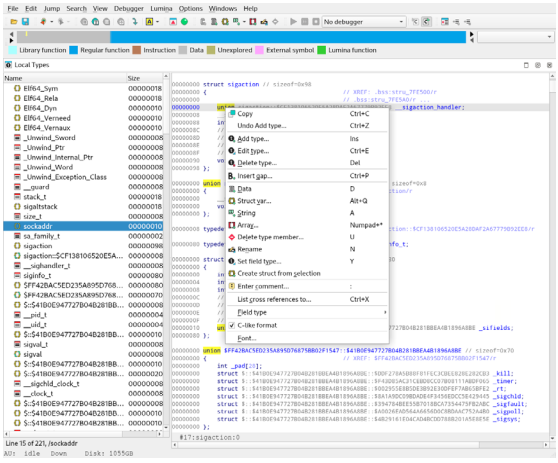
Unified type storage (ASMTIL)

- The presence of Structures, Enums and Local Types views and synchronization between them confused many users, especially those new to IDA. We have decided to add all missing features (such as structure field representation) to Local Types and now all type manipulations (still with familiar hotkeys!) can be done there. New databases will only have Local Types by default and Structures and Enums are deprecated.

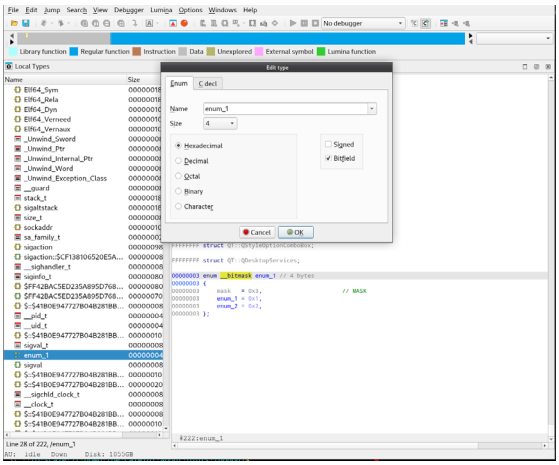


- The new Local Types Widget allows editing structures like the classic Structures widget, or via a free-text editor.



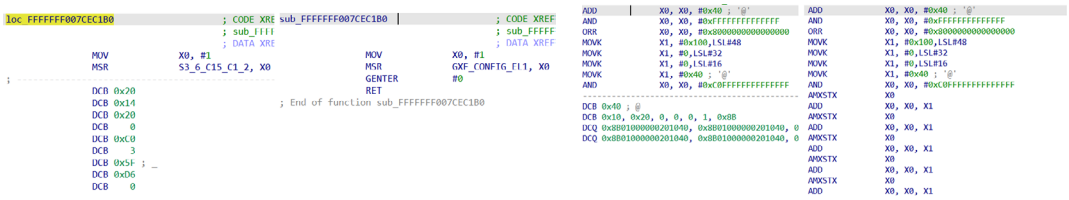


- The same goes for enum types:

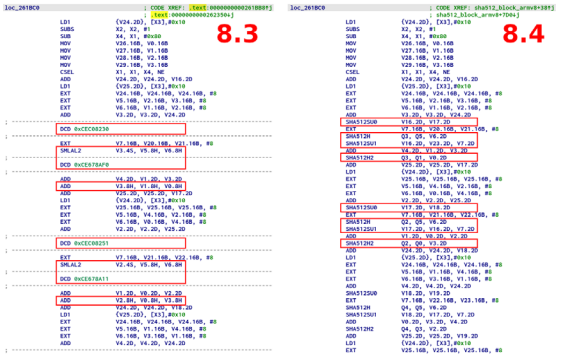


ARM/iOS improvements

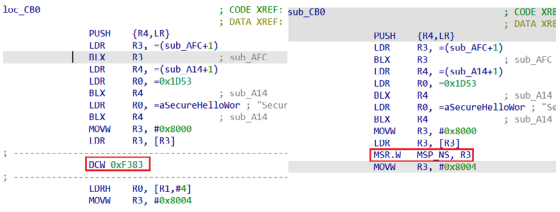
- We added support for common Apple-specific instructions and system registers commonly encountered in iOS and macOS software. This means you should see fewer instances of undefined bytes breaking disassembly and more understandable code when working with these files.



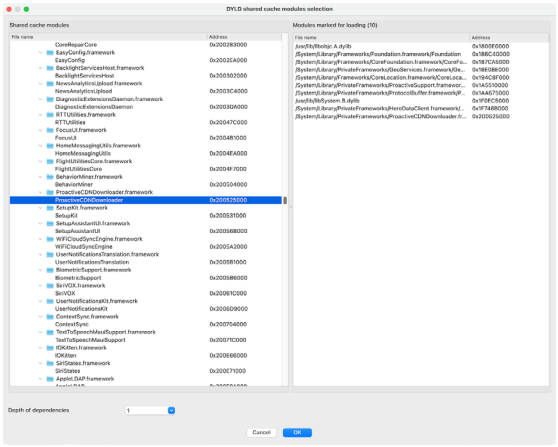
- ARMv8.6-A support. We've added most of mandatory and optional instructions from ARMv8.6-A (with notable exception of SVE). In particular, we added the following instruction set extensions:
  - FEAT_SHA3: (4) Advanced SIMD SHA3 instructions
  - FEAT_SHA512: (4) Advanced SIMD SHA512 instructions
  - FEAT_DotProd: (2) Advanced SIMD dot product instructions
  - FEAT_BF16: (8) BFloat16 (Brain Floating Point) instructions
  - FEAT_FHM: (2) Floating-point half-precision multiplication instructions
  - FEAT_I8MM: (5) Int8 matrix multiplication instructions



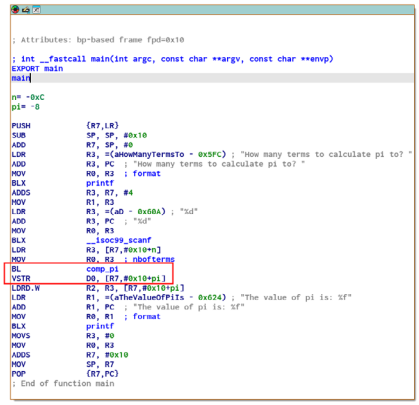
- ARMv8-M support: we now properly disassemble accesses to the new system registers introduced since ARMv7-M (for example, NS variants of some registers)

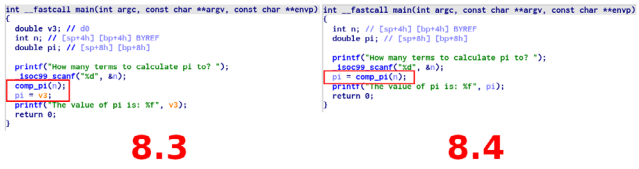


- The Mach-O loader now offers fine-grained control over the selection of dyld shared cache modules and their dependencies:



- The ARM32 decompiler supports hard-float ABI (floating point values passed and returned in FPU registers):

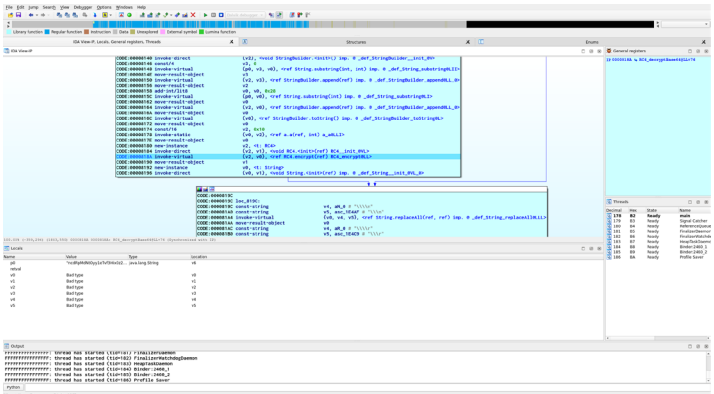




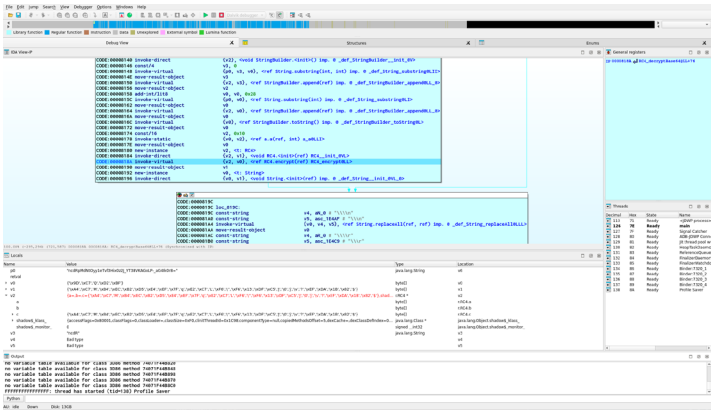
Debugger improvements

- We added support for recent Android versions and made it more robust when working with apps without debug information. If running on a recent (API28+) Android, IDA will try to guess the variable type automatically. Since in the Dalvik VM the value of a variable cannot be displayed without knowing its type, this boosts the debugging experience significantly.

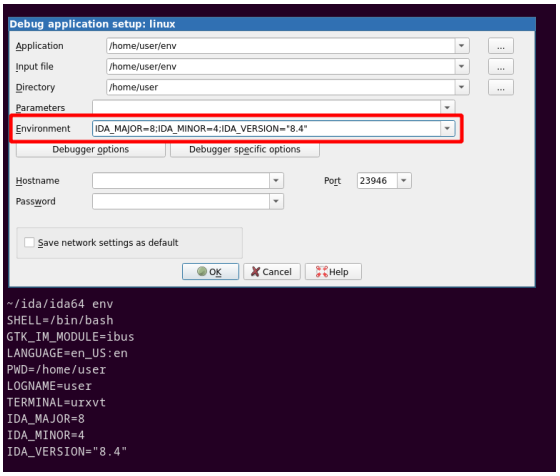
Dalvik debugger without type information:



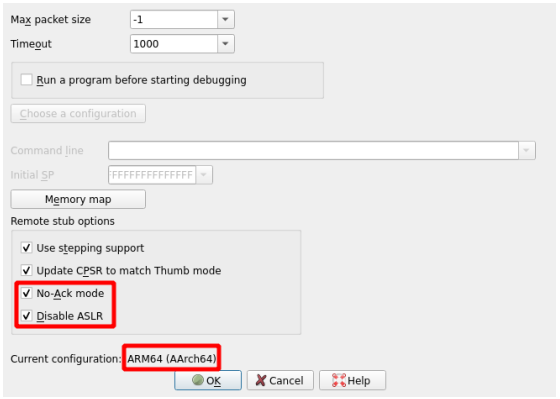
The same app, but with successfully guessed types for all local variable slots that are in scope:



- Environment variables can now be specified for Windows/Linux/Mac debuggers in process options:

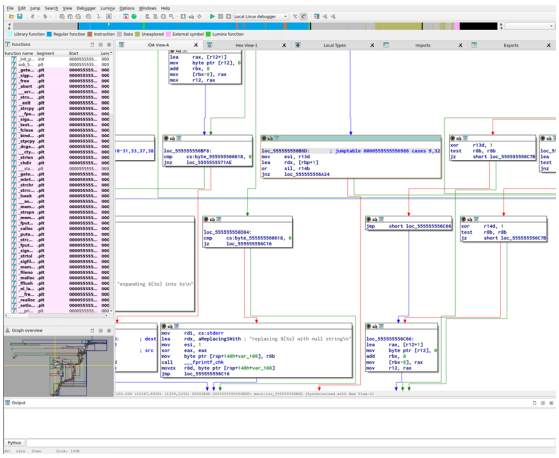


- We made various improvements to the debugging backends:
  - Address Space Layout Randomization (ASLR) can now be disabled for most platforms that support it (local debuggers and remote gdbstub). This simplifies debugging in cases where deterministic addresses are desired.
  - We enabled NoAck mode on iOS, saving one round trip time. This is beneficial for anybody debugging remote devices over high-latency connections (typically cloud-based emulators).
  - Finally, our remote debugging server now is available for ARM64 Linux.



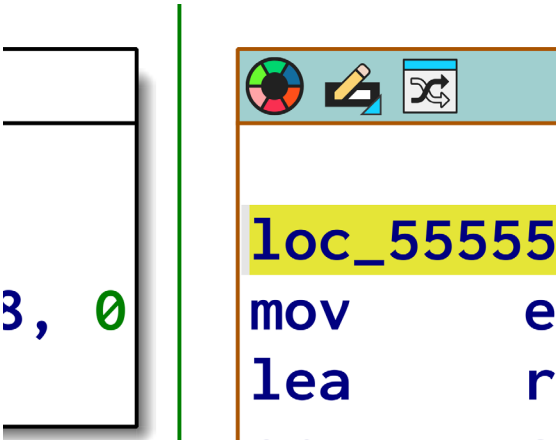
Modernized Look'n'Feel

- We replaced all icons with brushed-up, vectorized versions and added a crosshair effect to the minigraph view for orientation in large graphs.



IDA with new icons and crosshair effect in the minigraph view

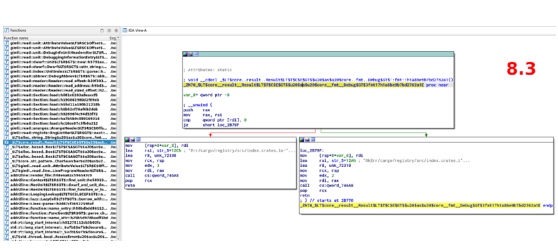
Moreover, pixelated fonts are a thing of the past. Texts in graph mode now render crisp at any zoom level.

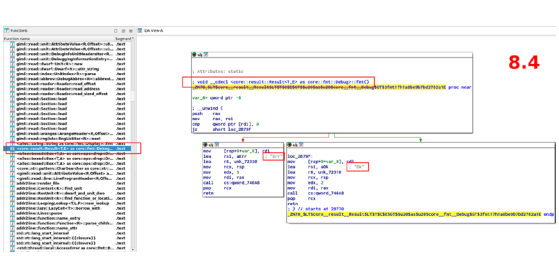


- Scrolling and zooming via the trackpad now works smoothly (especially, but not limited to, macOS)
- better graph layouts with fewer(none?) edge intersections, even on big functions

Improved Parsing of Rust metadata

- We added a plugin for parsing Rust-specific data and constructs. As a consequence, the huge string pools typically observed in Rust binaries are now split up properly. Moreover, the plugin adds demangling of both legacy and the v0 Rust name mangling format.





Full changelist: https://www.hex-rays.com/products/ida/news/8_4/

Previous releases

IDA Version 8.3 - Release date: 8th June 2023

Highlights: IDA64 support for (32-bit) .idb files, UX improvements, DWARF speedup, ARM64 system registers, Golang and much more!

Full changelist: https://www.hex-rays.com/products/ida/news/8_3/

IDA Version 8.2 – Service Pack 1 - Release date: 24th January 2023

Highlights: This Service Pack of IDA 8.2 is primarily a bugfix release.

Full changelist: https://www.hex-rays.com/products/ida/news/8_2sp1/

IDA Version 8.2 - Release date: 15th December 2022

Highlights: 32-bit support in IDA64, Processor modules improvements, Swift, picture_search plugin, UI candy and much more!

Full changelist: https://www.hex-rays.com/products/ida/news/8_2/

IDA Version 8.1 - Release date: 6th October 2022

Highlights: Private Lumina server, New icons, Golang regabi support, Sunsetting IDA for 32-bit binaries and much more!

Full changelist: https://www.hex-rays.com/products/ida/news/8_1/

IDA Version 8.0 – Service Pack 1 - Release date: 29th August 2022

Highlights: The Service Pack 1 of IDA 8.0 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/8_0sp1/