

## 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

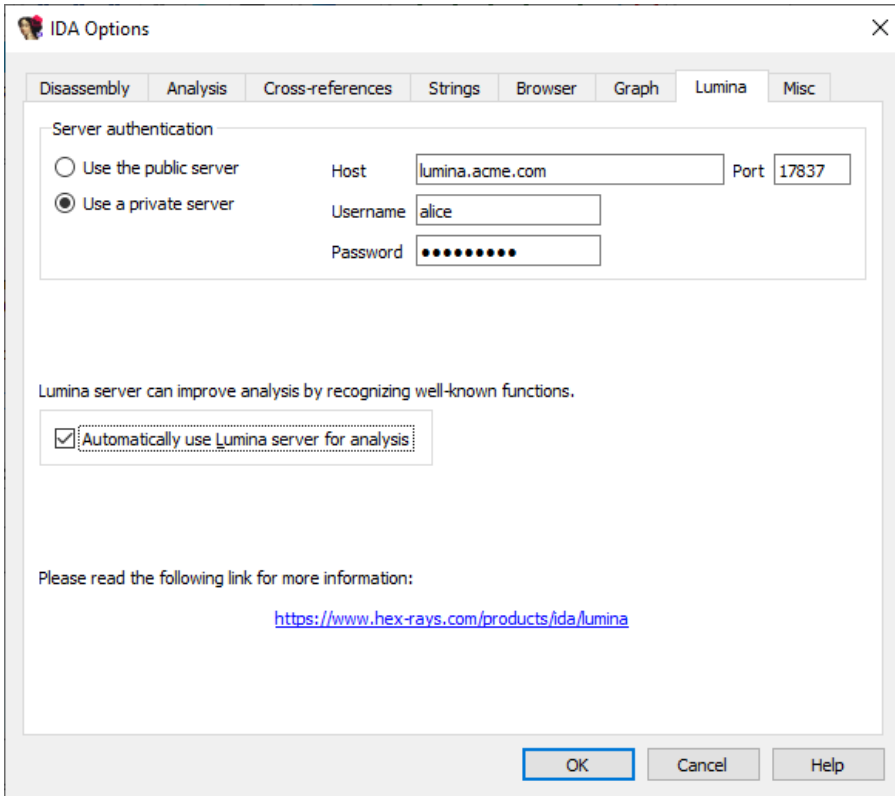
- The debugger adds the dynamic analysis of the information collected statically by the disassembler;
- Offers all the features expected from a debugger and more: "remote" function and tracking. Remote debugger: for Windows, Linux, Mac OS X, and other machines in any combination;

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

# IDA 8.1 Highlights Release date: October 2022

## Private Lumina server

Our public Lumina database has been available for several years now and is full of useful information. However, not all organizations can use it due to confidentiality requirements, so now we offer an option of a private server which can be used to share functions metadata inside the organization.



IDA Teams will include a free Lumina license while IDA Pro users can purchase it separately.

## New icons

We have designed a brand new icon set for IDA. The icon used will be specific to the IDA edition:



## Sunsetting IDA for 32-bit binaries (IDA32)

The world is moving to 64 bits (in fact, IDA itself is a 64-bit executable since 7.0), so the 32-bit IDA gets used less and less. Due to implementation details, it was still necessary to use it for decompiling 32-bit executables, but now we are gradually lifting this limitation, so that in the future 32-bit files will be analyzed and decompiled in IDA64. Eventually we plan to completely deprecate 32-bit IDA and only keep it around for working with legacy .idb files.

## Golang regabi support

Recent Go versions have enabled register-based calling convention (ABIInternal) instead of the original stack-based one for several architectures. While it was possible to describe it manually using `__usercall` in IDA, now it automatically allocates registers for the standard `__golang` convention based on the detected Go version and architecture of the binary.

For example, a function taking a slice and two integers had to be described manually in 8.0 as follows:

```
__int16 __usercall main_crc16@<ax>(_slice_uint8 buffer@<0:rax, 8:rbx, 16:rcx>, __int64 start@<r-di>, __int64 length@<rsi>)
```

```
// main_crc16
__int16 __usercall main_crc16@<ax>(
    _slice_uint8 buffer@<0:rax, 8:rbx, 16:rcx>,
    __int64 start@<rdi>,
    __int64 length@<rsi> _slice_uint8 buffer; // 0:rax.8,8:rbx.8,16:rcx.8 ISARG
)
{
    unsigned __int64 v3; // rdx
    int v4; // ecx
    unsigned int v6; // esi
    __int64 i; // r8
    int v8; // r9d

    if ( !length )
        return 0;
    v3 = length + start;
    v4 = -1;
    while ( start < v3 )
    {
        if ( buffer.len <= start )
            runtime_panicIndexU();
        v6 = buffer.ptr[start];
        for ( i = 0LL; i < 8; ++i )
        {
            HIWORD(v8) = HIWORD(v4);
            LOWORD(v8) = (unsigned __int16)v4 >> 1;
            if ( (v6 & 1) != (v4 & 1) )
                v8 ^= 0xFFFF8408;
            v4 = v8;
            v6 >>= 1;
        }
        ++start;
    }
    return (unsigned __int8)((unsigned __int16)-(WORD)v4 >> 8) | (unsigned __int16)-(WORD)v4 << 8);
}
```

ida 8.0

While in 8.1 the following works fine:

```
__int16 __golang main_crc16(_slice_uint8 buffer, __int64 start, __int64 length);
```

```
// main_crc16
__int16 __golang main_crc16(_slice_uint8 buffer, __int64 start, __int64 length)
{
    unsigned __int64 v3; // rdx
    int v4; // ecx
    unsigned int v6; // esi
    __int64 i; // r8
    int v8; // r9d

    if ( !length )
        return 0;
    v3 = length + start;
    v4 = -1;
    while ( start < v3 )
    {
        if ( buffer.len <= start )
            runtime_panicIndexU(start, buffer.len, buffer.len);
        v6 = buffer.ptr[start];
        for ( i = 0LL; i < 8; ++i )
        {
            HIWORD(v8) = HIWORD(v4);
            LOWORD(v8) = (unsigned __int16)v4 >> 1;
            if ( (v6 & 1) != (v4 & 1) )
                v8 ^= 0xFFFF8408;
            v4 = v8;
            v6 >>= 1;
        }
        ++start;
    }
    return (unsigned __int8)((unsigned __int16)-(WORD)v4 >> 8) | (unsigned __int16)-(WORD)v4 << 8);
}
```

ida 8.1

## Previous releases

**IDA Version 8.0 – Service Pack 1** - Release date: 19th 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/](https://www.hex-rays.com/products/ida/news/8_0sp1/)

---

**IDA Version 8.0** - Release date: 29th July 2022

Highlights: introduced DA Teams, iOS 16 dyld shared cache support, Outlined functions Golang 1.18, New decompiler: ARC, Better firmware analysis thanks to the function finder plugin (patfind), FLAIR pattern generator (makepat) And much more!

**Full changelist:** [https://www.hex-rays.com/products/ida/news/8\\_0/](https://www.hex-rays.com/products/ida/news/8_0/)

---

**IDA Version 7.7 – Service Pack 1** - Release date: 18th January 2022

Highlights: The Service Pack 1 of IDA 7.7 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\\_7sp1/](https://www.hex-rays.com/products/ida/news/7_7sp1/)

---

**IDA Version 7.7** – Release date: 24th December 2020

Highlights: IDA 7.6 introduced DA Teams, iOS 16 dyld shared cache support, Outlined functions Golang 1.18, New decompiler: ARC, Better firmware analysis thanks to the function finder plugin (patfind), FLAIR pattern generator (makepat) And much more!

**Full changelist:** [https://www.hex-rays.com/products/ida/news/7\\_7/](https://www.hex-rays.com/products/ida/news/7_7/)

---