

# idapython-cheatsheet



Cheatsheets and example scripts for IDAPython (7.x and 6.x).

It looks like this:

The cheatsheet is a detailed reference for IDAPython 7.x, covering various API functions and constants. It is organized into several sections:

- Some constants:** Defines constants like `BADADDR`, `BADSEL`, `MAXADDR`, and `SIZE_MAX`.
- Analysis:** Functions for analyzing code, such as `plan_and_wait`, `auto_mark_range`, and `delete_all_segments`.
- Entry points:** Functions for finding entry points, including `add_entry`, `rename_entry`, and `get_entry_qty`.
- Cross references (XRef):** Functions for finding cross references, such as `CodeRefsTo`, `DataRefsTo`, and `XRefsFrom`.
- Functions:** Functions for finding and managing functions, including `get_name`, `get_func_name`, and `add_func`.
- User interface:** Functions for interacting with the user interface, such as `get_screen_ea` and `ask_yn`.
- Search in database:** Functions for searching the database, including `find_binary`, `find_text`, and `find_func_end`.
- Items:** Functions for finding items, such as `next_addr`, `prev_addr`, and `get_item`.
- Segments:** Functions for finding and managing segments, including `get_seg_attr`, `set_seg_attr`, and `get_seg_name`.
- Read / Write in database:** Functions for reading and writing data to the database, such as `get_byte`, `get_word`, and `set_byte`.
- Colors (background):** Functions for setting colors, including `get_color` and `set_color`.
- Debugger Hooks:** Functions for setting debugger hooks, such as `add_bpt`, `enable_bpt`, and `del_bpt`.
- Enums:** Functions for finding and managing enums, including `get_enum_qty` and `get_enum_name`.
- Listing, comments, operands:** Functions for listing code, comments, and operands, such as `get_cmt`, `set_cmt`, and `get_operand`.
- Structures:** Functions for finding and managing structures, including `add_struct`, `del_struct`, and `get_struct_qty`.
- IDAPython 7.x:** Overview of IDAPython 7.x, including its features and compatibility.

## Printable versions

### PDF

- English (IDA 6.x and 7.x)
- Russian (IDA 6.x and 7.x)

### IDAPython 7.x (PNG)

- IDAPython 7.x cheatsheet (English)
- IDAPython 7.x cheatsheet (Russian)

---

## **IDAPython 6.x (PNG)**

- IDAPython 6.x cheatsheet (English)
- IDAPython 6.x cheatsheet (Russian)

## **Tips & tricks & examples**

### **Debugger Hooks**

- Work with breakpoints source code

### **Listing**

- Simple transformations in disassembler view source code
- Make comment to function, using it's argument source code

### **Types**

- Apply types to functions and data source code
- Work with enums source code

### **Xrefs**

- Add simple code and data cross-references source code

### **Miscellaneous**

- Parsing Global Descriptor Table (GDT, x86) source code
- Parsing Interrupt Descriptor Table (IDT, x86) source code

### **Links**

- “The Beginner’s Guide to IDAPython” by Alexander Hanel
- “Introduction to IDAPython” by Ero Carrera
- IDAPyHelper - script that helps writing IDAPython scripts and plugins