



Retargetable Decompiler's IDA Plugin

User Guide

Version 0.4

<https://github.com/avast-tl/retdec-idaplugin>

<https://retdec.com>

support@retdec.com

January 16, 2018

Contents

1	Introduction	2
2	Installation	3
2.1	IDA	3
2.2	Linux	3
2.3	Windows	4
2.4	Windows Plugin on Linux	4
3	Configuration	4
3.1	IDA's plugin.cfg	5
3.2	Decompilation Configuration	5
3.3	Configuration from IDA	6
4	Plugin Information	7
4.1	About Plugin	7
4.2	Output Window	7
4.3	GUI Windows	9
5	Decompilation	9
5.1	Selective Decompilation	9
5.2	Full Decompilation	9
6	User Interactions	9
6.1	Basic Interactions	10
6.2	Navigation	10
6.3	Code Refactoring	11
7	List of All User Actions	11
7.1	Function-Declaration/Definition Context	11
7.2	Function-Call Context	12
7.3	Global-Variable Context	12
7.4	Global Context	12
8	Support and Feedback	13

1 Introduction

This document describes the Retargetable Decompiler's plugin for IDA (RetDec plugin). Its goal is to integrate with IDA, give transparent access to the Retargetable Decompiler and provide user-interaction capabilities like navigation or code refactoring. An example of code decompiled by Retdec plugin is shown in Figure 1.

Retargetable Decompiler (RetDec) is a reverse-engineering tool independent of any particular target architecture, file format, operating system, or compiler. It was developed in cooperation of Faculty of Information Technology, Brno University of Technology and AVG Technologies. Since the acquisition of AVG Technologies by Avast in 2016, Avast has continued to develop the decompiler. It is using Capstone disassembler engine and a Capstone2LLvmlR library to translate machine code into a high-level-language representation. Currently, the decompiler supports the MIPS, ARM (including Thumb extension), x86, and PowerPC architectures using the Windows PE, COFF, Unix ELF, Intel HEX, and RAW binary file formats.

RetDec can be used in the following ways:

1. Online decompilation using [web interface](#).
2. Remote decompilation using [Application programming interface](#) (API).
3. Local build:
 - (a) Compiling [RetDec repository](#) on your own.
 - (b) Downloading and installing [RetDec binary release](#).
4. [RetDec IDA plugin](#) (this guide's topic):
 - (a) Remote decompilation using API.
 - (b) Local decompilation using local build.

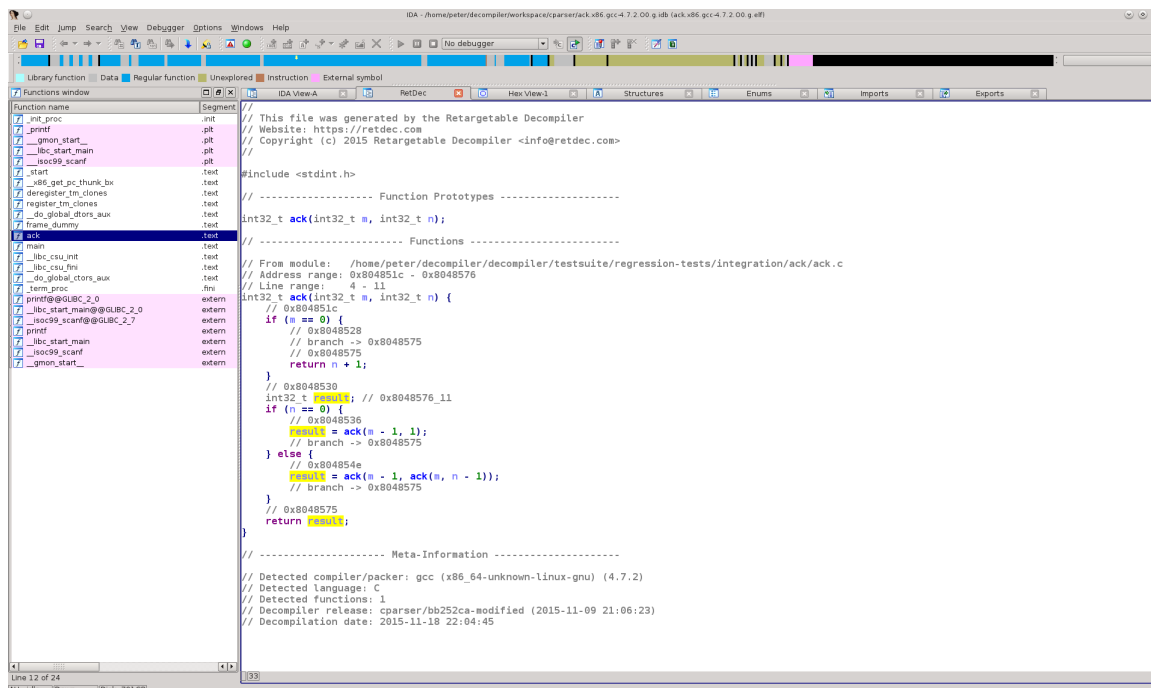


Figure 1: Example of code decompiled by RetDec plugin.

2 Installation

This section describes prerequisites and the installation process of RetDec IDA plugin binary release.

It is also possible to build and install the plugin directly from sources. To do so, follow the [Build and Installation](#) instructions instead of this section.

2.1 IDA

The plugin is created using IDA SDK version 6.6. The plugin is compatible with the following IDA versions: 6.6, 6.7, 6.8, 6.9, 6.95. The plugin does NOT work with IDA 7.x.

2.2 Linux

Follow the next steps to install RetDec plugin in a Linux environment:

1. Install 32-bit versions of the following shared-object dependencies:

```
libc.so.6 libgcc_s.so.1 libm.so.6 libpthread.so.0 libstdc++.so.6
```

2. If you plan to use local RetDec build, install Python 3 and [Pygments](#).
3. Download the Linux installation package (Table 1) from the [project's release page](#).
4. Copy `retdec.plx` to the IDA's plugin directory (`<IDA_ROOT>/plugins`).

Table 1: Linux installation package contents.

File	Description
license	Directory with licenses.
license/LICENSE	RetDec IDA plugin's license.
license/LICENSE-THIRD-PARTY	Licenses of libraries used by RetDec plugin.
retdec.plx	32-bit Linux RetDec plugin.
user_guide.pdf	RetDec plugin's user guide (this document).

2.3 Windows

The Windows version of the plugin requires Windows 7 or later, with the MSVC 2015 runtime¹ installed.

Follow the next steps to install RetDec plugin in a Windows environment:

1. If you plan to use local RetDec build, install Python 3 and [Pygments](#).
2. Download the Windows installation package (Table 2) from the [project's release page](#).
3. Copy `retdec.plw` to the IDA's plugin directory (`<IDA_ROOT>/plugins`).

Table 2: Windows installation package contents.

File	Description
license	Directory with licenses.
license/LICENSE	RetDec IDA plugin's license.
license/LICENSE-THIRD-PARTY	Licenses of libraries used by RetDec plugin.
retdec.plw	32-bit Windows RetDec plugin.
user_guide.pdf	RetDec plugin's user guide (this document).

2.4 Windows Plugin on Linux

It is also possible to run the Windows version of IDA with the Windows version of RetDec plugin on Linux using Wine². Install RetDec plugin as described in Section 2.3 and if it does not run out of the box, try a workaround³.

3 Configuration

This section describes how to configure RetDec plugin. After you follow these steps, you should have your plugin ready for work.

¹Visual C++ Redistributable for Visual Studio 2015: <https://www.microsoft.com/en-us/download/details.aspx?id=48145>

²<https://www.winehq.org/>

³https://bugs.winehq.org/show_bug.cgi?id=39437#c6

3.1 IDA's plugin.cfg

The plugin's default mode is set to selective decompilation (see Section 5). It tries to register hotkey `CTRL+D` for its invocation. If you already use this hotkey for another action or you just want to use a different hotkey, you need to modify IDA's plugin configuration file. Moreover, the plugin supports one more decompilation mode and a hotkey invocation for the plugin's configuration. If you want to use any of them, you also have to modify the config file.

The IDA's plugin configuration file is in `<IDA_ROOT>/plugins/plugins.cfg`. Its format is documented inside the file itself. To configure RetDec plugin, add the following lines at the beginning⁴ of the file:

```
; Plugin_name          File_name Hotkey      Arg
; -----
Retargetable_Decompiler retdec    Ctrl-d    0
Retargetable_Decompiler retdec    Ctrl-Shift-d 1
Retargetable_Decompiler retdec    Ctrl-Shift-c 2
```

These lines tell IDA which hotkeys invoke the plugin and what argument is passed to it. The plugin's behavior after invocation is determined by the passed argument. Possible argument values are summarized in Table 3. In the provided example, we mapped selective decompilation to hotkey `CTRL+D` (plugin's default), full decompilation to `CTRL+SHIFT+D`, and plugin configuration to `CTRL+SHIFT+C`. However, you may choose whichever hotkeys you like, provided they do not clash with other plugins or IDA.

Table 3: Description of RetDec plugin's invocation arguments.

Argument value	Description
0	Invokes selective decompilation. See Section 5.
1	Invokes full decompilation. See Section 5.
2	Invokes plugin configuration inside IDA. See Section 3.3.

3.2 Decompilation Configuration

Each time a decompilation is triggered, plugin checks that it is properly configured. If it is not, warning shown in Figure 2 is displayed. After you hit `OK`, the configuration dialog (Figure 3) appears. Here, you can choose the decompilation mode to use:

1. Remote API decompilation (plugin's default) – you have to provide your API key. To access it, register to <https://retdec.com>, login, and click on `Account`.
2. Local decompilation – you have to install `RetDec` local build and make sure plugin finds the `retdec-decompiler.sh` script. Either add the decompiler's `bin` directory to the system `PATH`, or set path to `retdec-decompiler.sh` in the form as shown in Figure 4.

⁴Newer versions of IDA behave strangely when the lines are appended at the end, so just put them at the start.

The settings will be saved and if you want to change them later, you need to manually invoke the plugin's configuration from IDA (see Section 3.3).

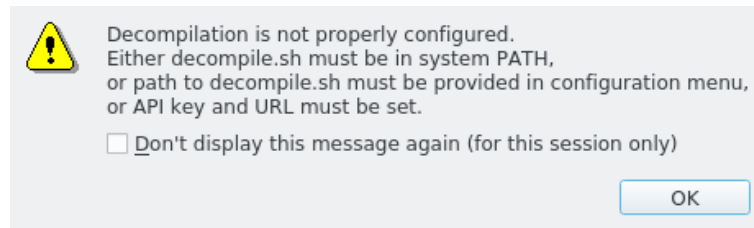


Figure 2: RetDec plugin's configuration warning.

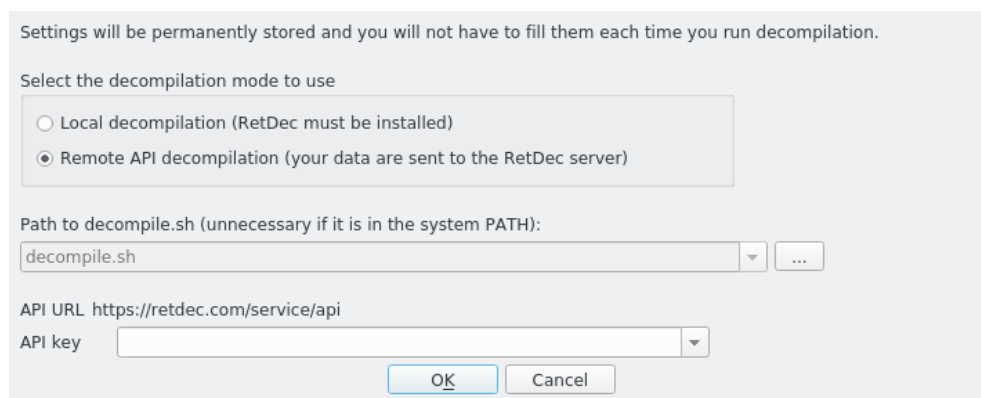


Figure 3: RetDec plugin's configuration dialog.

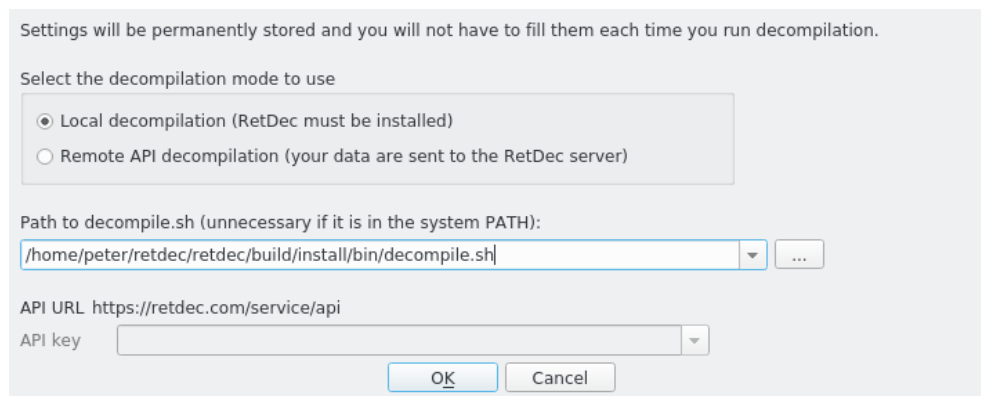


Figure 4: RetDec plugin's configuration dialog – path to `retdec-decompiler.sh` set.

3.3 Configuration from IDA

The same dialog (Figure 3) that is displayed if the plugin is misconfigured can be opened from IDA anytime later. There are the following two ways to do it:

- If you configured a hotkey for the plugin's configuration argument value according to Section 3.1, you can use it to invoke the configuration dialog.
- You can also open the configuration dialog from the Options/RetDec plugin options menu (Figure 5).

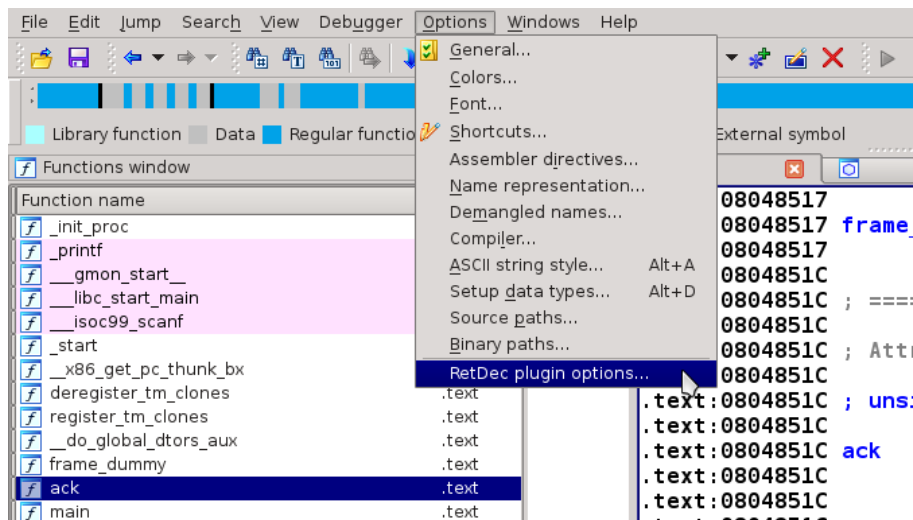


Figure 5: Opening the plugin's configuration dialog from the menu.

4 Plugin Information

This section describes how to find information about RetDec plugin you are currently using and how the plugin communicates information to you.

4.1 About Plugin

Information about RetDec plugin can be found among IDA's information on the registered plugins at Help/About program (Figure 6), where you need to click on the Addons button (Figure 7). Then, find the Retargetable Decompiler entry in the presented list (Figure 8).

4.2 Output Window

Right after the start, as well as during the work with RetDec plugin, it communicates with you mainly through the IDA's output window (Figure 9). Here, you are shown several kinds of important messages:

```
[RetDec info]    :    some important piece of information
[RetDec warning]:    something went a little bit wrong
[RetDec error]   :    something went very wrong
```

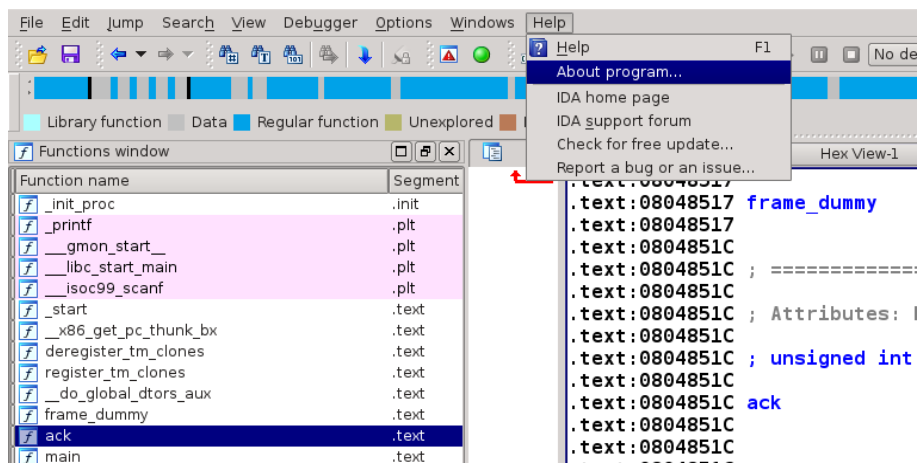



Figure 6: Opening the About IDA dialog from the menu.

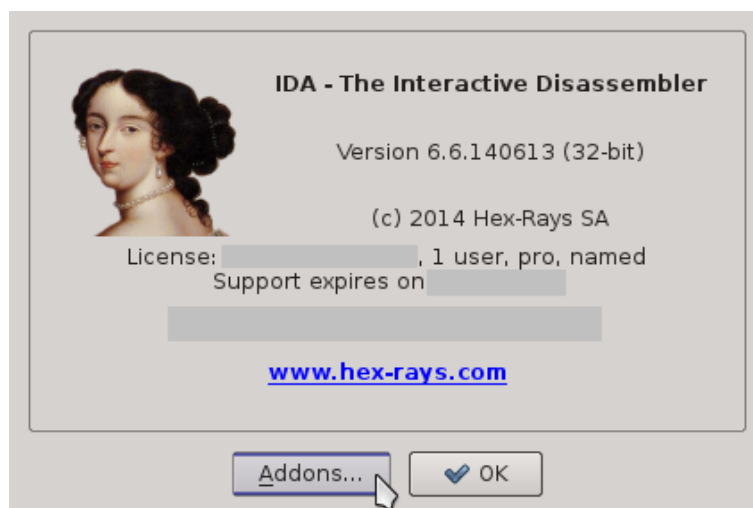


Figure 7: Information window about IDA.

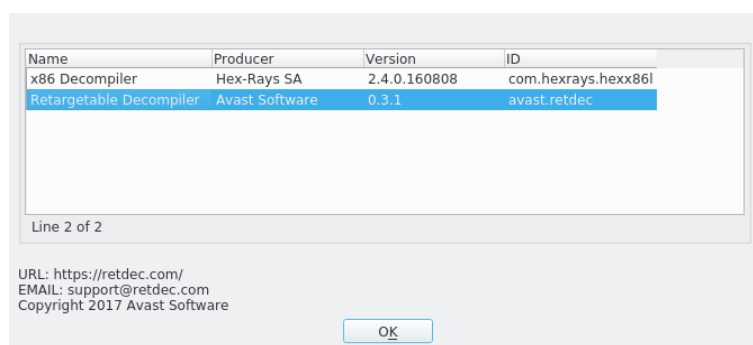


Figure 8: Information window about RetDec plugin.

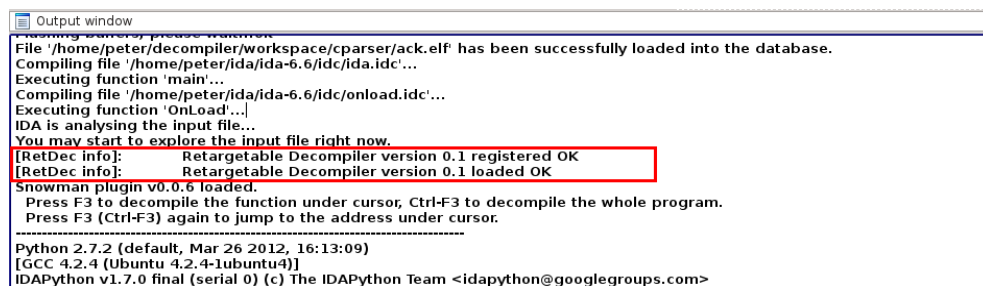
The image shows a screenshot of the 'Output window' in IDA Pro. The window contains several lines of text. The first line is a warning: 'Warning: RetDec plugin: please wait...'. The next line states: 'File "/home/peter/decompiler/workspace/cparser/jack.elf" has been successfully loaded into the database.' This is followed by 'Compiling file "/home/peter/ida/ida-6.6/idc/ida.idc"...', 'Executing function "main"...', 'Compiling file "/home/peter/ida/ida-6.6/idc/onload.idc"...', and 'Executing function "OnLoad"...'. Then it says 'IDA is analysing the input file...' and 'You may start to explore the input file right now.'. A red rectangular box highlights two lines: '[RetDec info]: Retargetable Decompiler version 0.1 registered OK' and '[RetDec info]: Retargetable Decompiler version 0.1 loaded OK'. Below this, it says 'Snowman plugin v0.0.6 loaded.' and provides instructions: 'Press F3 to decompile the function under cursor, Ctrl-F3 to decompile the whole program.' and 'Press F3 (Ctrl-F3) again to jump to the address under cursor.'. At the bottom, it shows the Python version 'Python 2.7.2 (default, Mar 26 2012, 16:13:09)', the GCC version '[GCC 4.2.4 (Ubuntu 4.2.4-1ubuntu4)]', and the IDAPython version 'IDAPython v1.7.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>'.

Figure 9: IDA's output window.

4.3 GUI Windows

Sometimes, RetDec plugin wants to be sure you noticed an important message or event. In such a case, it shows you a pop-up window, which forces you to acknowledge it by pressing OK or a similar button.

5 Decompilation

This section describes how to invoke a decompilation. After reading it, you should be able to decompile a selected function, as well as an entire binary that is being analyzed.

5.1 Selective Decompilation

RetDec plugin's primary decompilation mode is selective decompilation. It decompiles the function that is currently under the cursor. It is invoked from the IDA's disassembly window, where you need to bring focus to the desired function and use either the default hotkey CTRL+D, or a hotkey you configured according to Section 3.1.

Once the decompilation is finished, the decompiled source code is displayed in a new IDA viewer window. Here, you can invoke new decompilations by double-clicking on function calls.

5.2 Full Decompilation

If you configured a hotkey for full decompilation in Section 3.1, you can use it to decompile an entire binary that is being analyzed. The result of this decompilation is stored into an output file, whose location is communicated to you through IDA's output window. The result cannot be displayed in the IDA's viewer window.

6 User Interactions

This section describes various kinds of user interactions that are currently supported by RetDec plugin. As was stated in Section 5, these interactions are applicable only on results from selective decompilations because full decompilations cannot be displayed in IDA's viewer window.

6.1 Basic Interactions

We use the IDA's native custom viewer window to display the decompiled source codes. Therefore, the plugin feels like part of IDA and we get a word occurrences highlighting (Figure 10) out of the box.

```
int32_t ack(int32_t m, int32_t n) {  
    // 0x804851c  
    if (m == 0) {  
        // 0x8048528  
        // branch -> 0x8048575  
        // 0x8048575  
        return n + 1;  
    }  
    // 0x8048530  
    int32_t result; // 0x8048576_11  
    if (n == 0) {  
        // 0x8048536  
        result = ack(m - 1, 1);  
        // branch -> 0x8048575  
    } else {  
        // 0x804854e  
        result = ack(m - 1, ack(m, n - 1));  
        // branch -> 0x8048575  
    }  
    // 0x8048575  
    return result;  
}
```

Figure 10: Native word occurrence highlighting.

6.2 Navigation

RetDec plugin supports function navigation—jumping forward and backward between already decompiled functions, or invoke an entirely new decompilation. When you double-click on a function call, the plugin presents the requested function. If it was already decompiled in the past, the cached result is shown to perform the action faster. You have to either explicitly request a re-decompilation of the previously processed functions, or perform an action that triggers the re-decompilation automatically (see Section 6.3). Re-decompilation can be forced by using the selective decompilation hotkey in IDA's disassembly (re-decompilation of any function), or in the RetDec plugin's viewer window (re-decompilation of currently shown function). If the double-clicked function was not decompiled yet, it is selectively reversed and displayed. In either case, only one function is shown at a time. A navigation entry for the newly presented function is added into a doubly linked navigation list, right after the entry for function from which the invocation was made. The list is then used for forward and backward navigation between the stored functions. An example of such navigation is depicted in Figure 11.

Unfortunately, we were not able to integrate navigation with IDA's graphical control elements, so it can be done only through keyboard hotkeys:

- ESC to move back.
- CTRL+F to move forward.

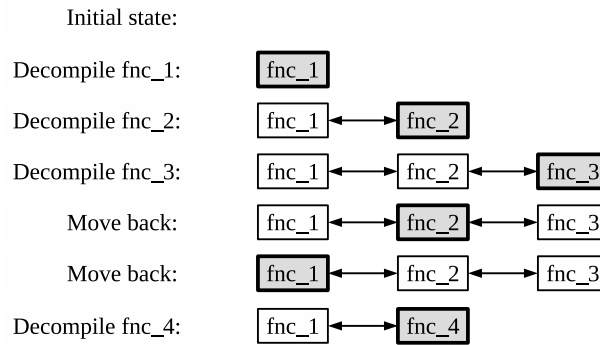


Figure 11: Decompiled function navigation example.

6.3 Code Refactoring

The RetDec plugin's viewer windows also allows you to refactor displayed source code. We can divide the source-code modifications into two basic categories:

- Those which do not require immediate re-decompilation, like object-identifier re-naming or function-comment insertion.
- Those which automatically trigger re-decompilation of the modified function. These are typically changes that can be used or propagated by reversing analyses. For example, a user-specified object data type can be spread by the data-flow type recovery analysis among other objects.

Refactoring actions are triggered either by hotkeys associated with them, or by pop-up menus shown on right-click. Actions are sensitive to the current context (current word under the cursor). As is shown in Figure 12 and Figure 13, actions available for functions differ from actions for global variables. Available actions at any given position are composed of two sets of actions:

- Actions available for the current context, i.e. for functions, global variables, function calls, etc. This set may be empty.
- Global actions available at all positions, i.e. navigation, current function comment modification, etc.

The complete catalog of available user actions is listed in Section 7.

7 List of All User Actions

This section provides a complete catalog of available user actions for all possible contexts.

7.1 Function-Declaration/Definition Context

Function actions are available on function declarations or definitions. They are listed in Table 4.

Table 5: Global-variable context user actions.

Action description	Hotkey	Triggers re-decompilation
Jump to IDA's ASM	A	X
Rename global variable	N	X

Table 6: Global context user actions.

Action description	Hotkey	Triggers re-decompilation
Edit current function's comment	;	X
Move backward (navigation)	ESC	X
Move forward (navigation)	CTRL+F	X

8 Support and Feedback

RetDec plugin is still in an experimental beta version. If you have any feedback, suggestions, or bug reports, please open an issue in the GitHub project (preferred), or send them to us either through our website, or through email.

<https://github.com/avast-tl/retdec-idaplugin>

<https://retdec.com>

support@retdec.com