RELYZE

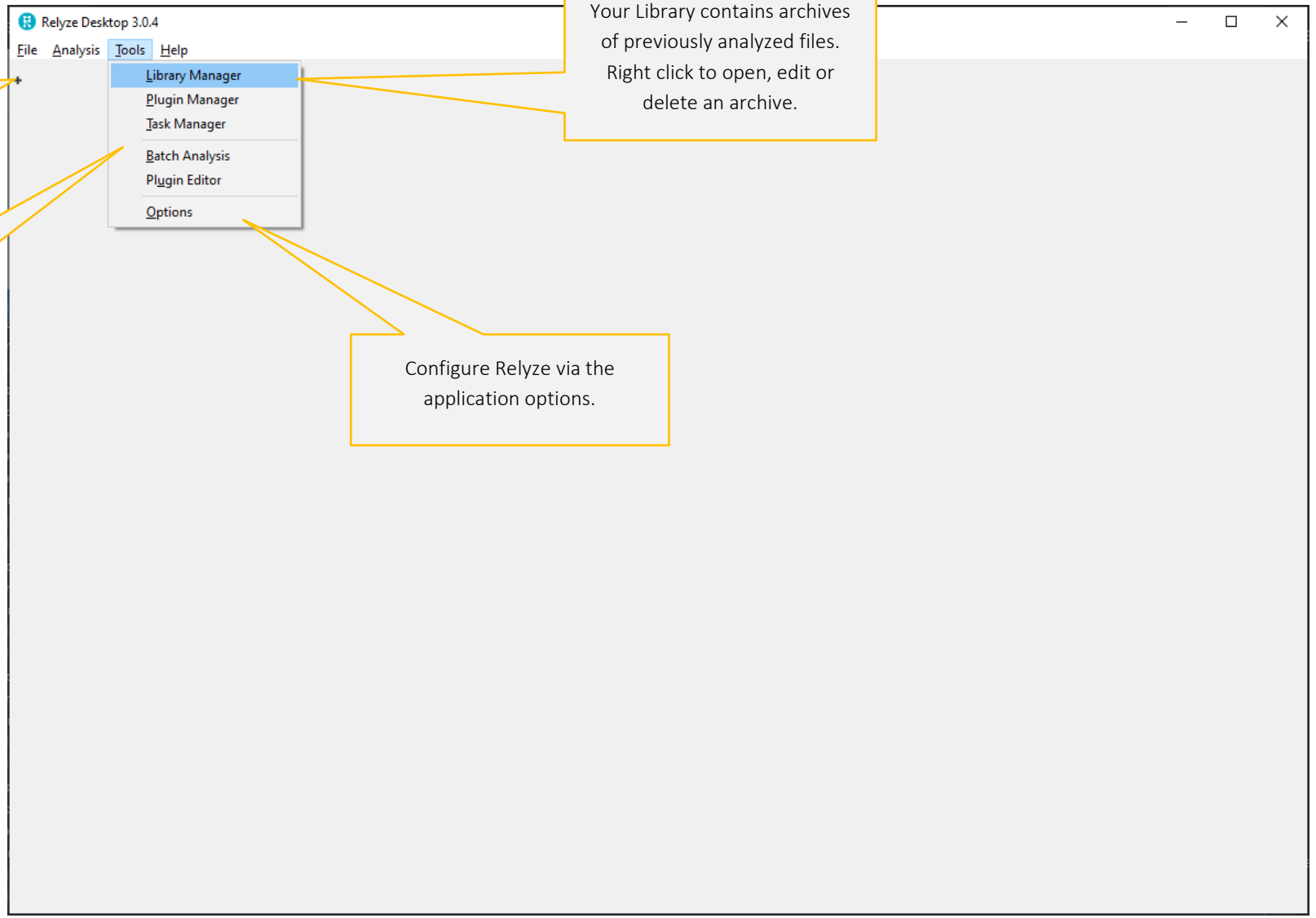
QUICK START GUIDE

28 November 2022

CONTENTS

GUI OVERVIEW

Analyze a file either by clicking the + button, dragging a file onto the application or select Open from the File menu.

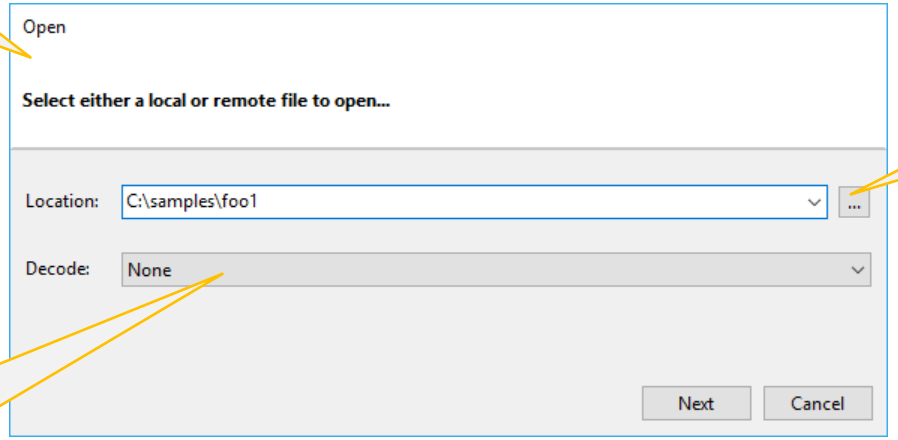


Your Library contains archives of previously analyzed files. Right click to open, edit or delete an archive.

You can access the applications task manager, batch analysis and the plugin editor here. Press F1 at any time to display the Plugin Editor.

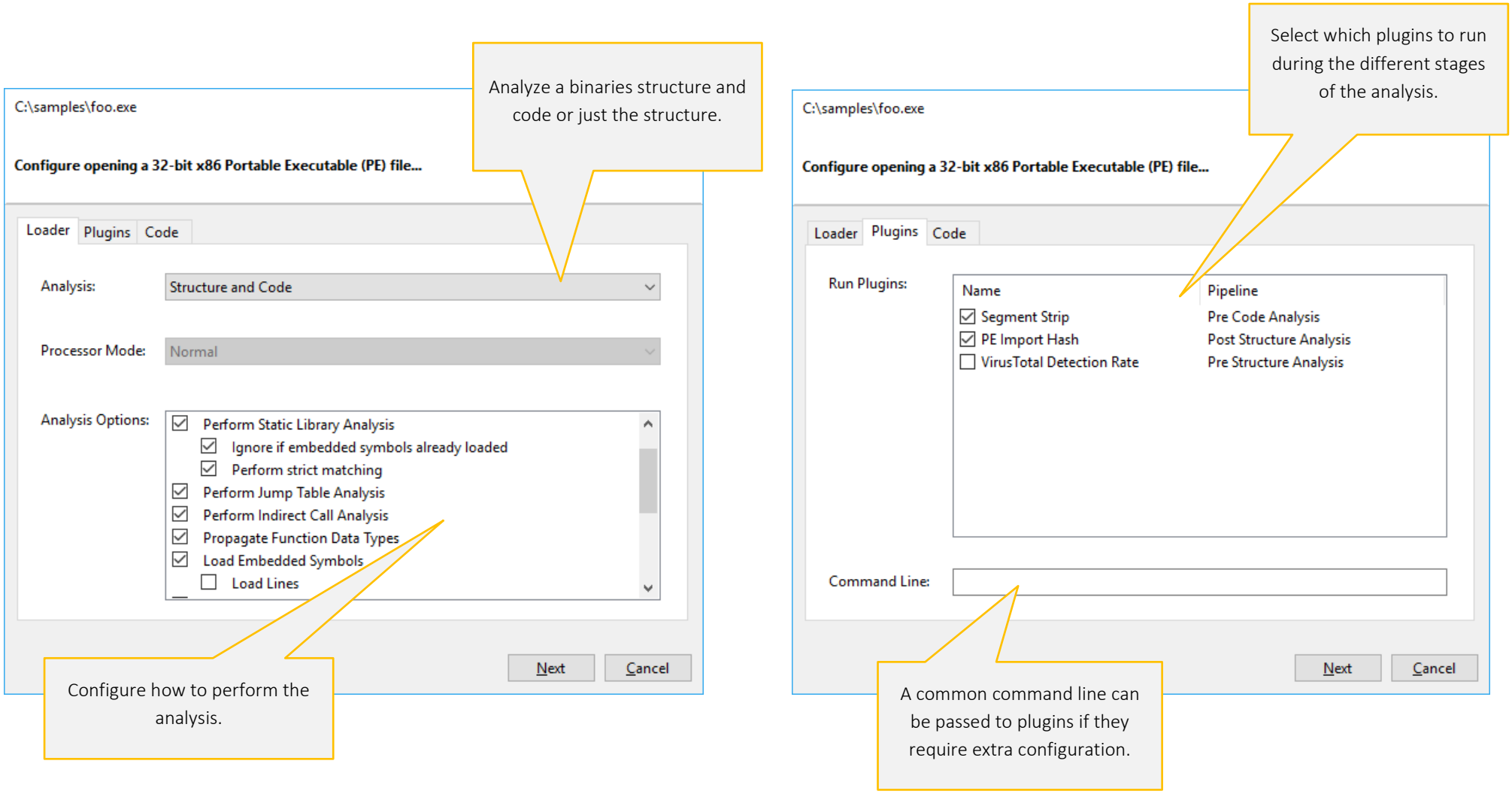
Configure Relyze via the application options.

Either drop a file onto the application or click the + button in the main window to bring up the Open dialog



Browse for a local file or enter a remote file location such as a UNC path, HTTP or FTP location.

If needed, a decoder plugin may be used to decode an input source into an expected format



Switch between the analysis overview, structure, code and diff views.

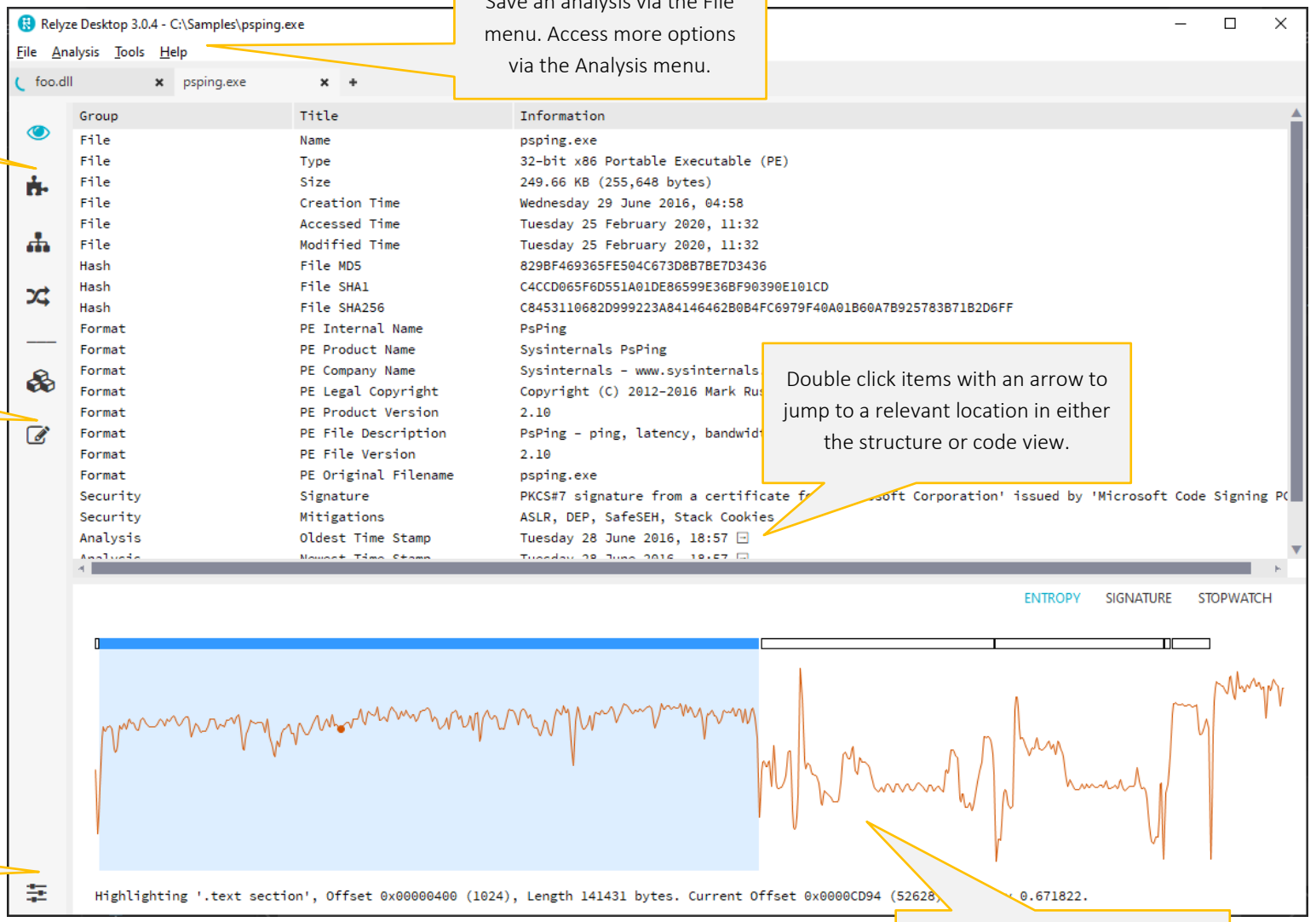
Save an analysis via the File menu. Access more options via the Analysis menu.

Access the Data Type Manager and Plugin Editor here.

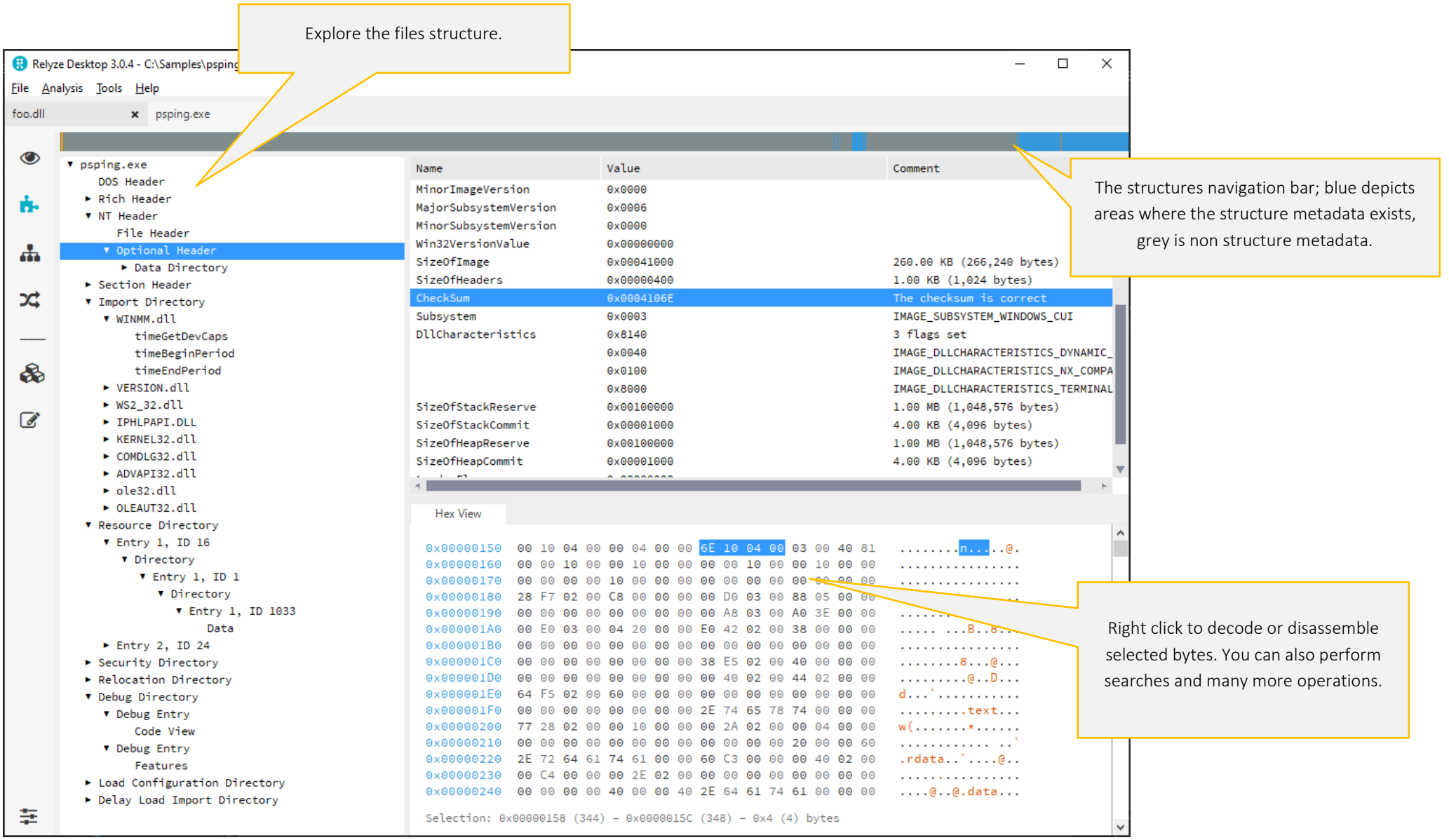
Double click items with an arrow to jump to a relevant location in either the structure or code view.

Access the analysis options.

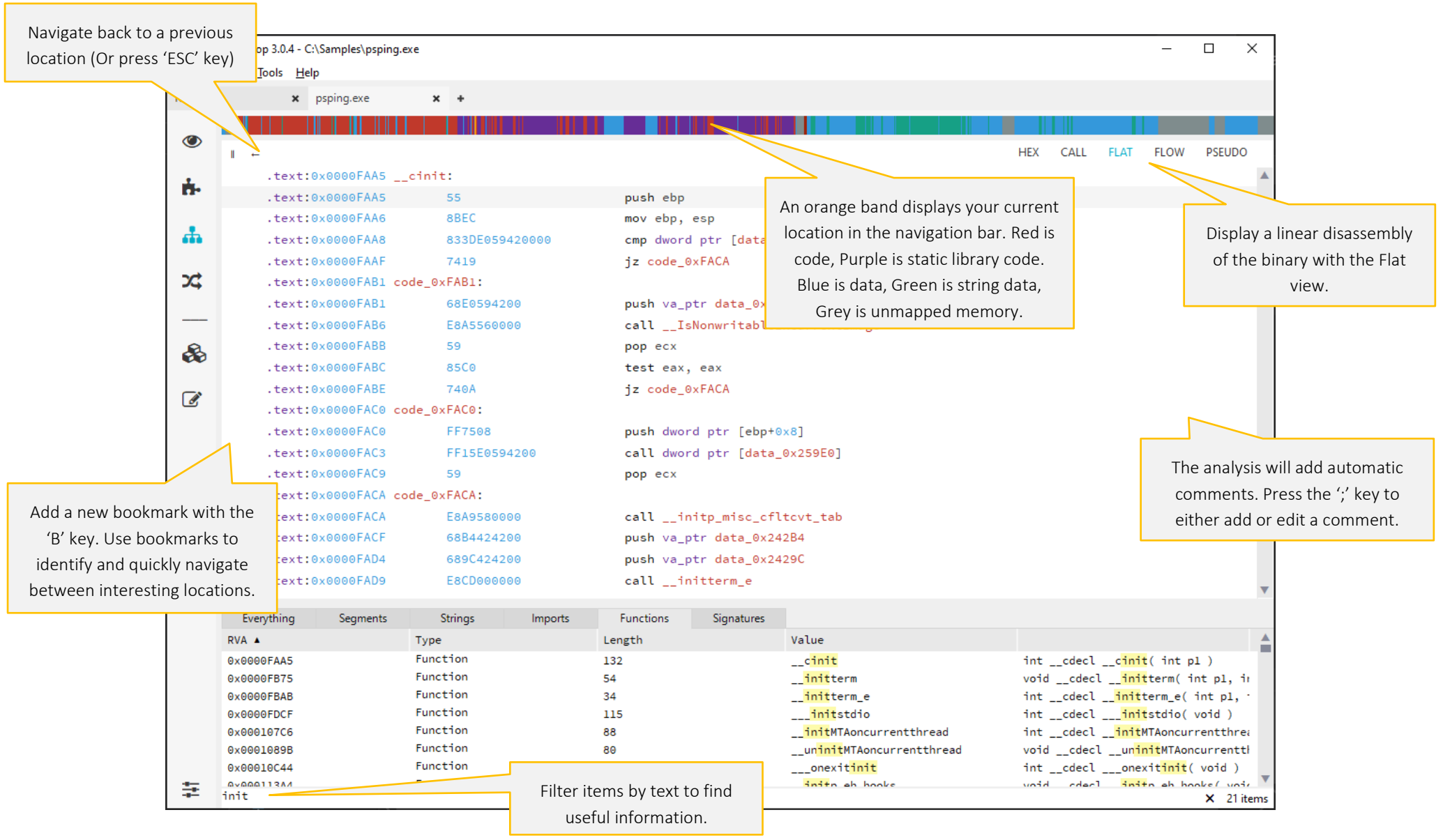
Right click the entropy graph to jump into the code or structure.

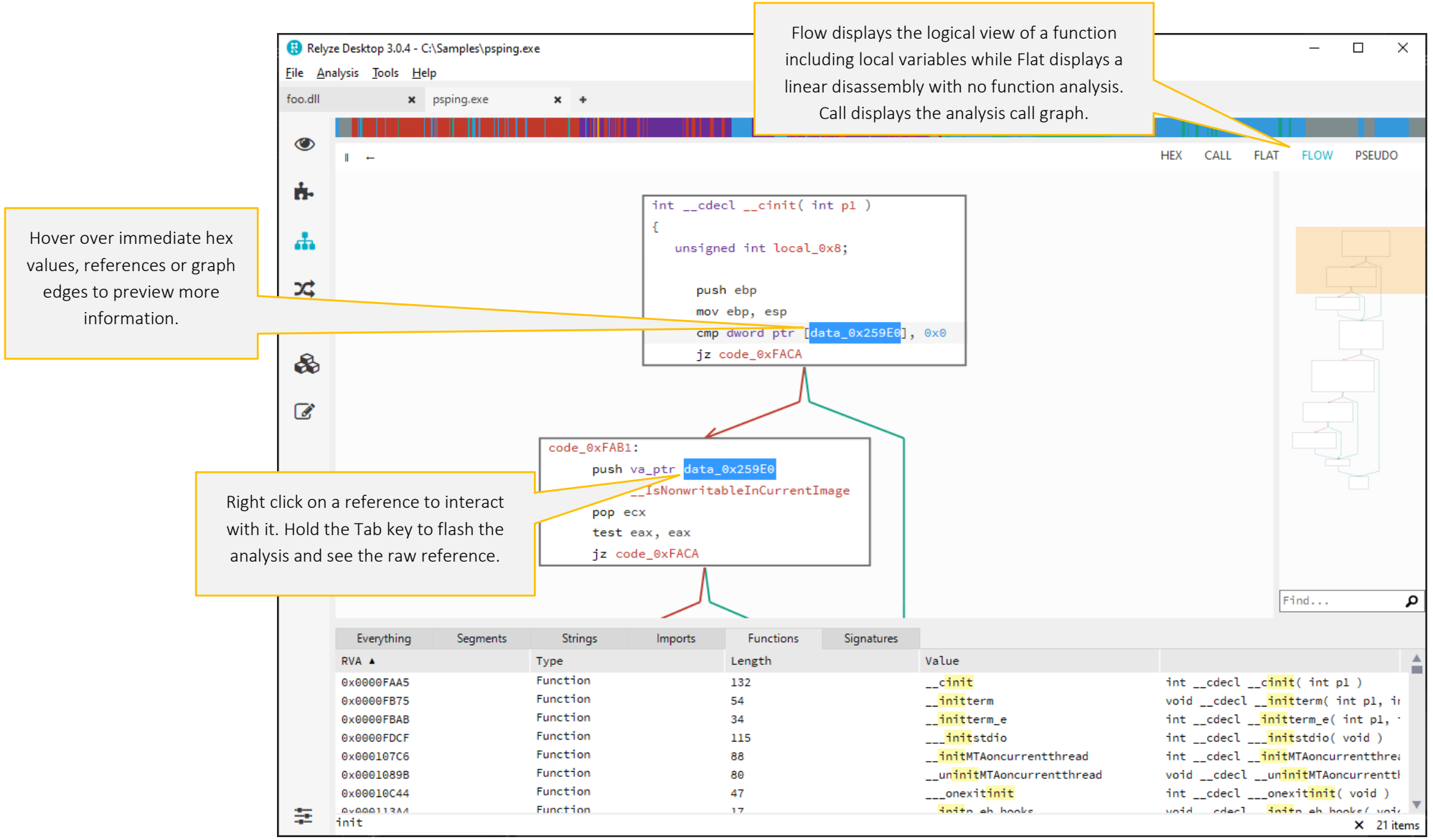


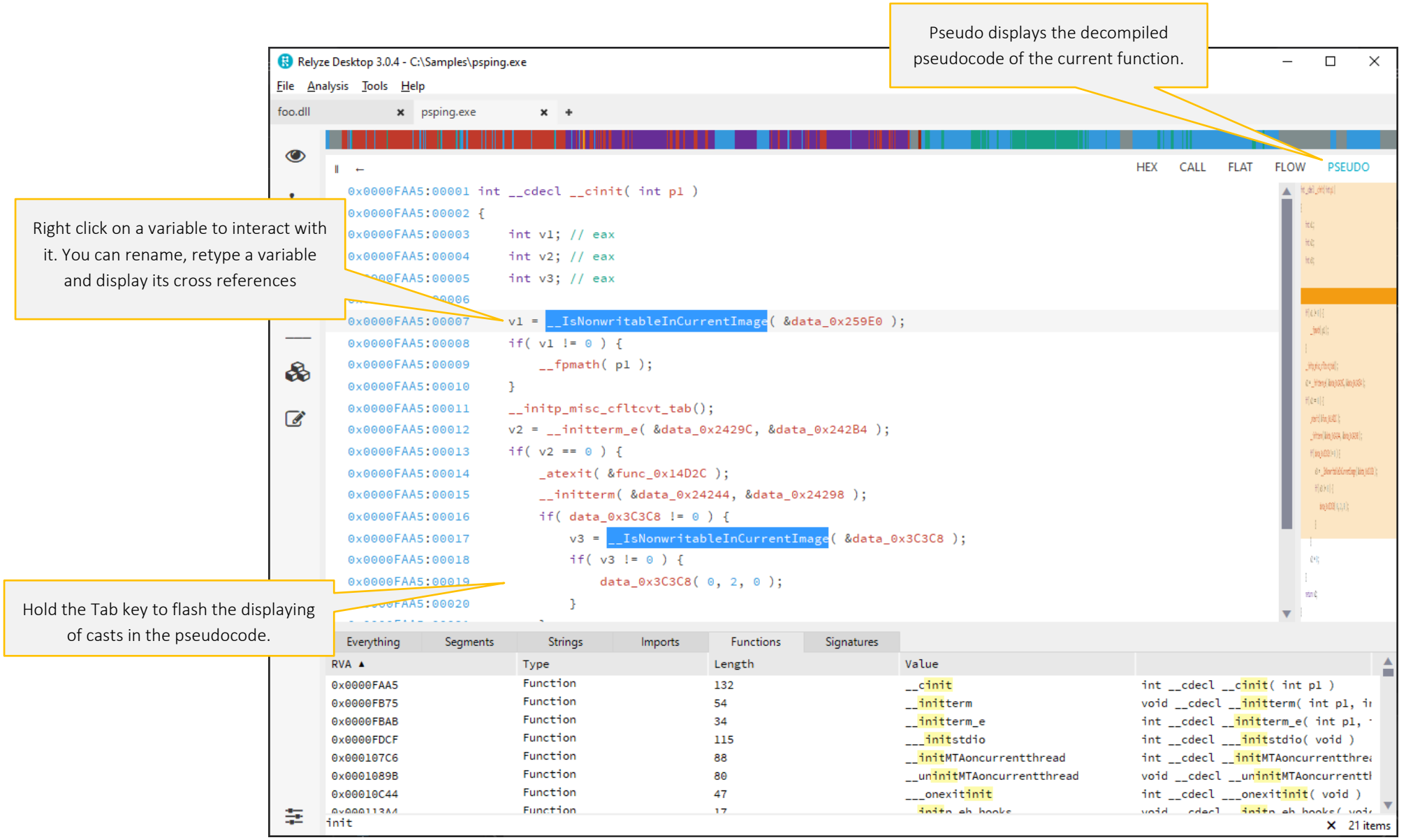
STRUCTURE VIEW

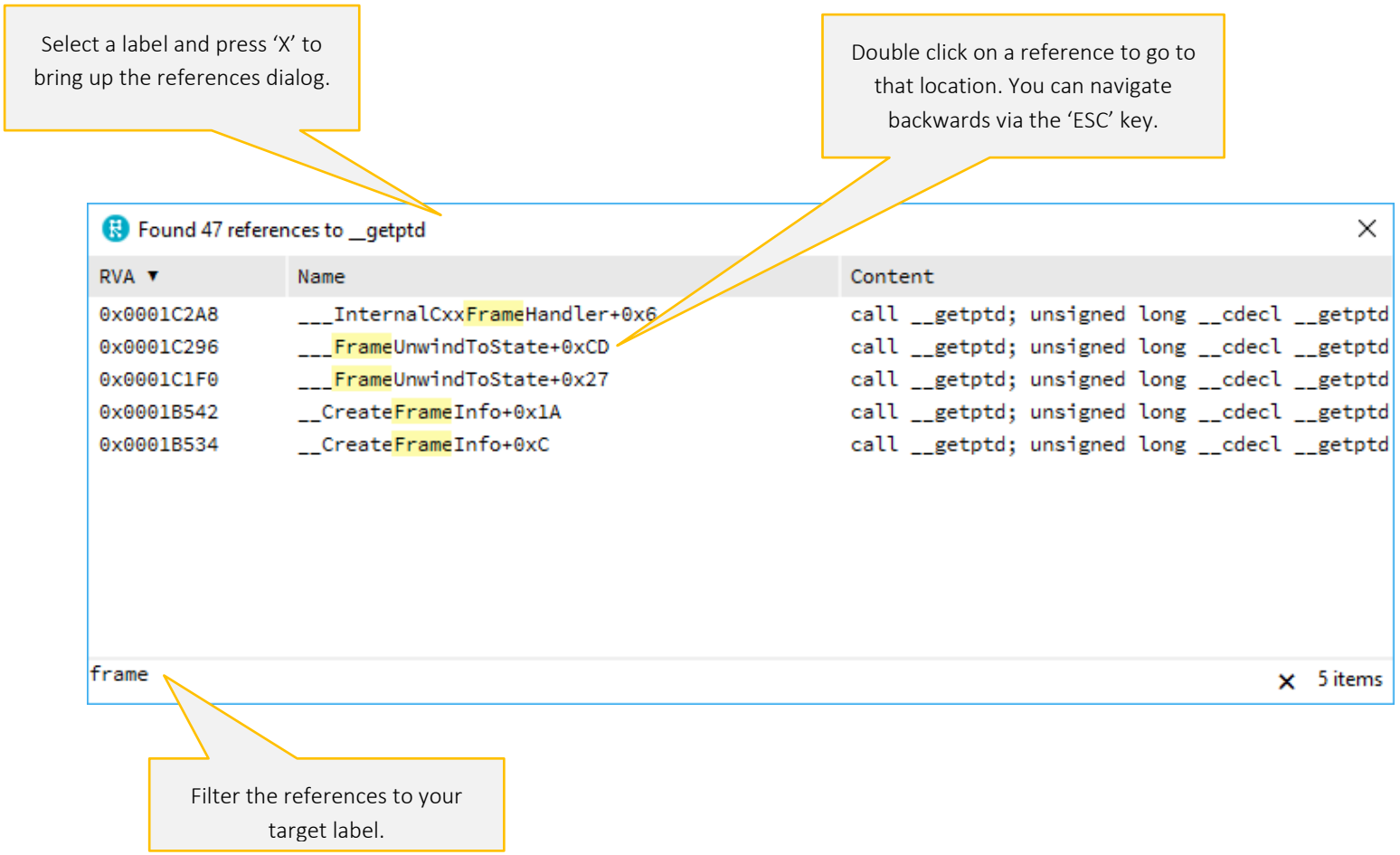


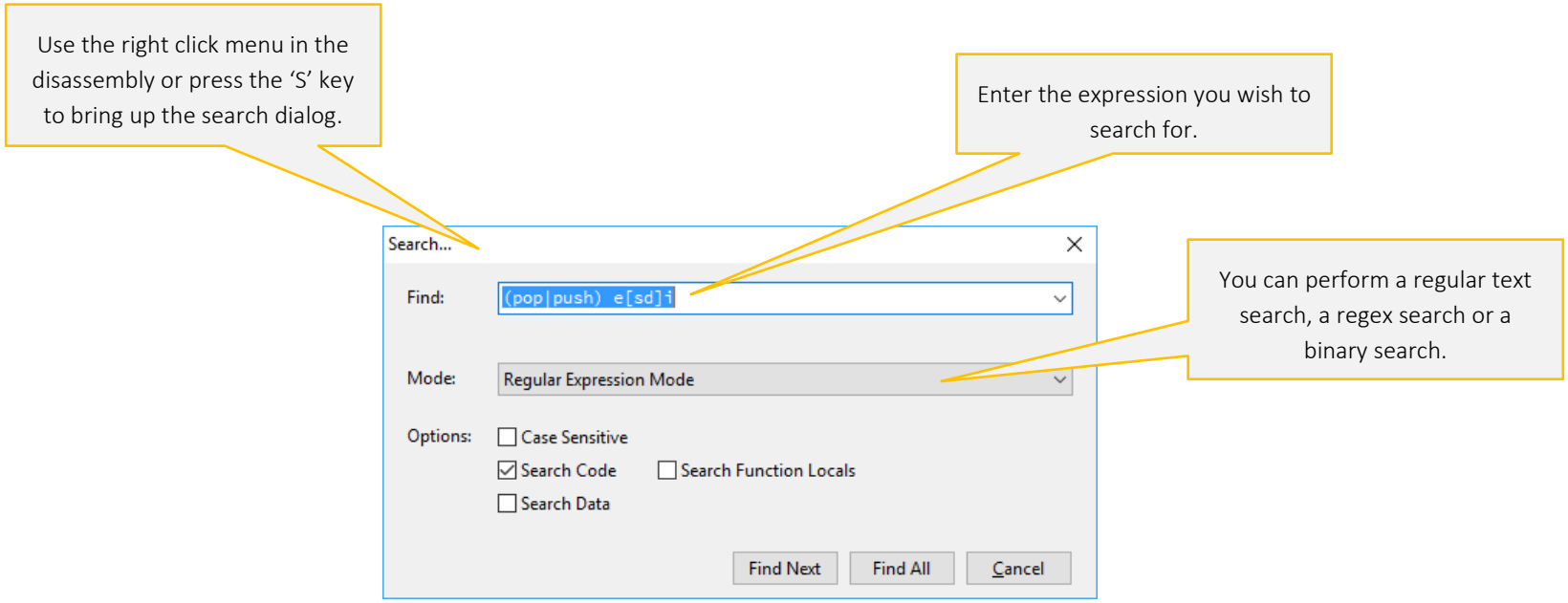
CODE FLAT VIEW





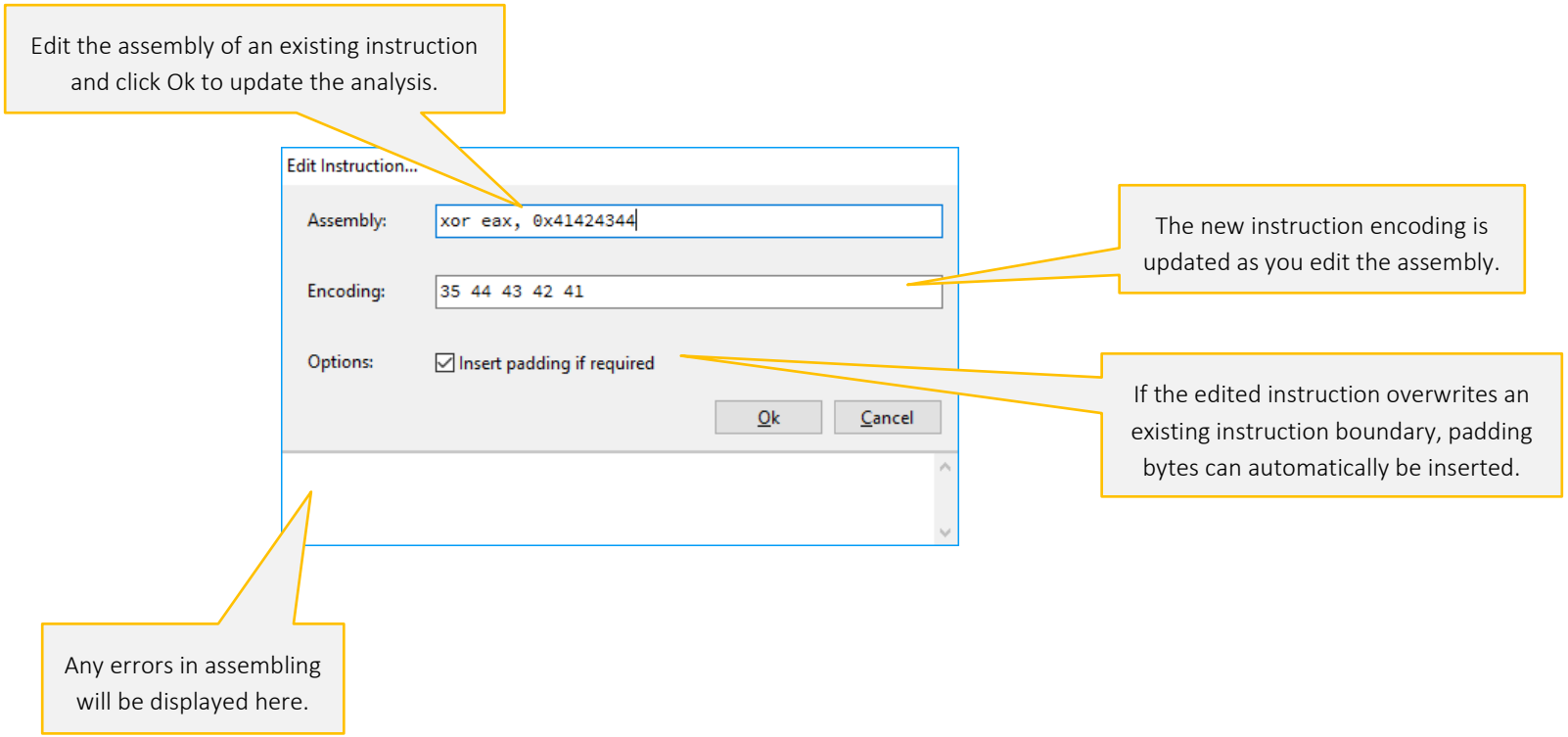






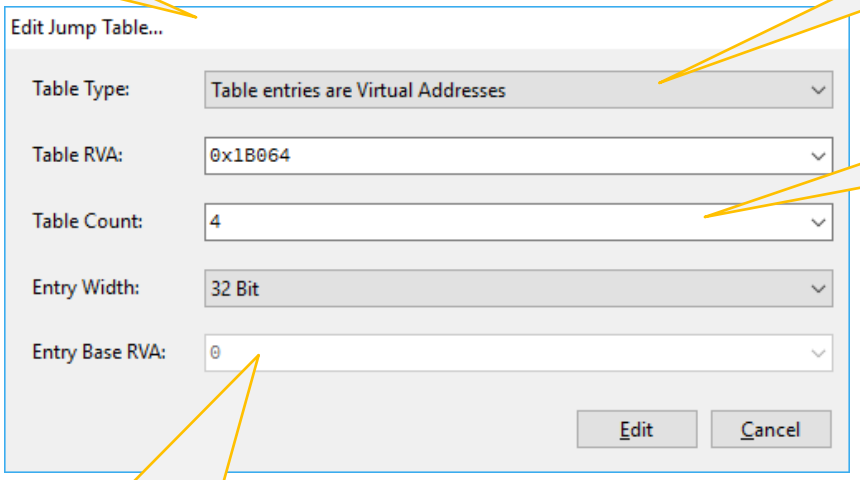
EDIT AN INSTRUCTION

To edit an existing instruction, select the line containing the instruction in either the flat or flow view. You can then either use the right click menu and select Block -> Edit Instruction, or you can use the default keyboard shortcut ‘e’. The following dialog is then displayed allowing you to edit the selected instruction.



EDIT A JUMP TABLE

If a jump table was analysed incorrectly you can manually edit it. Select the jump instruction and right click to edit it (Or press the 'J' key).

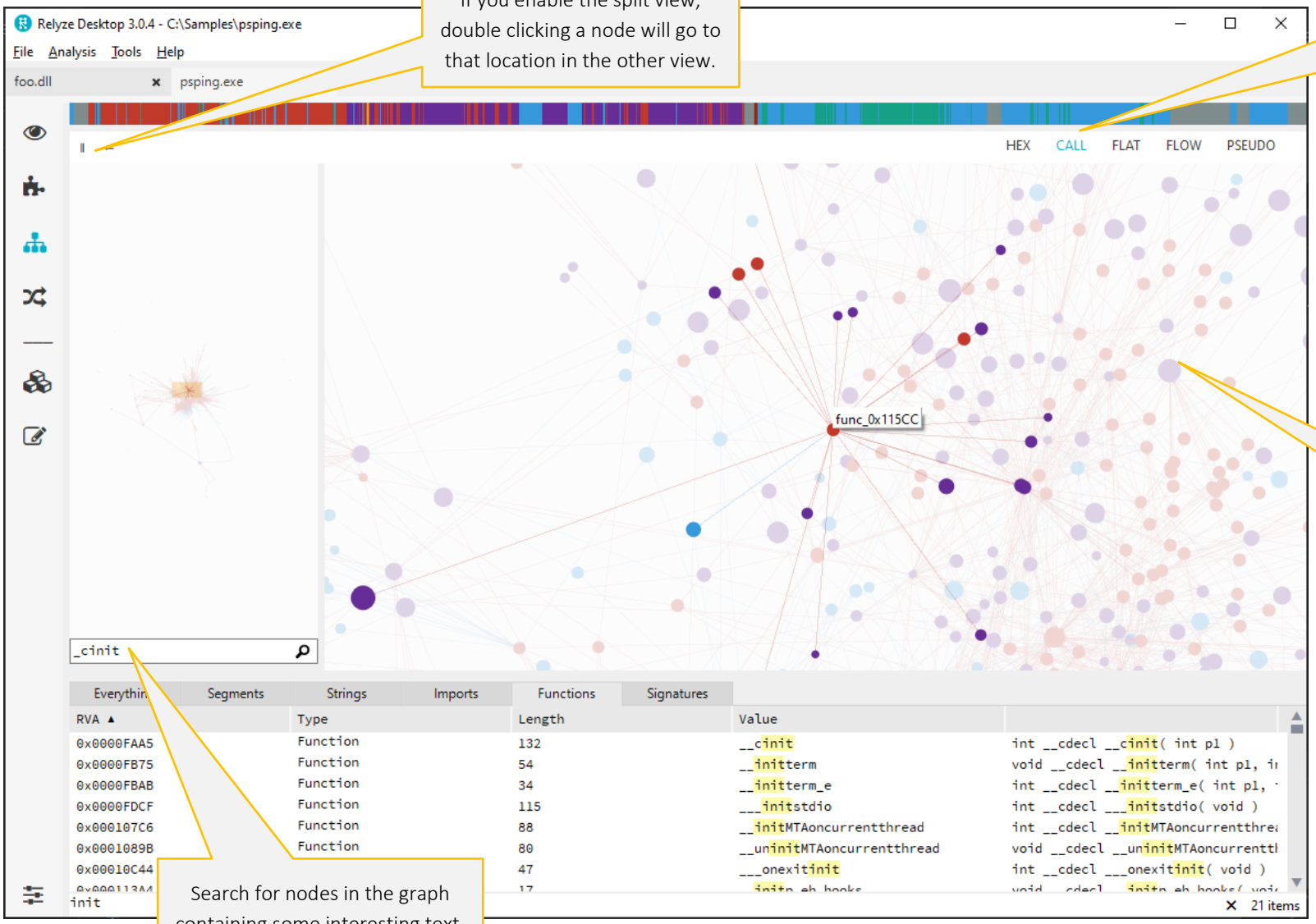


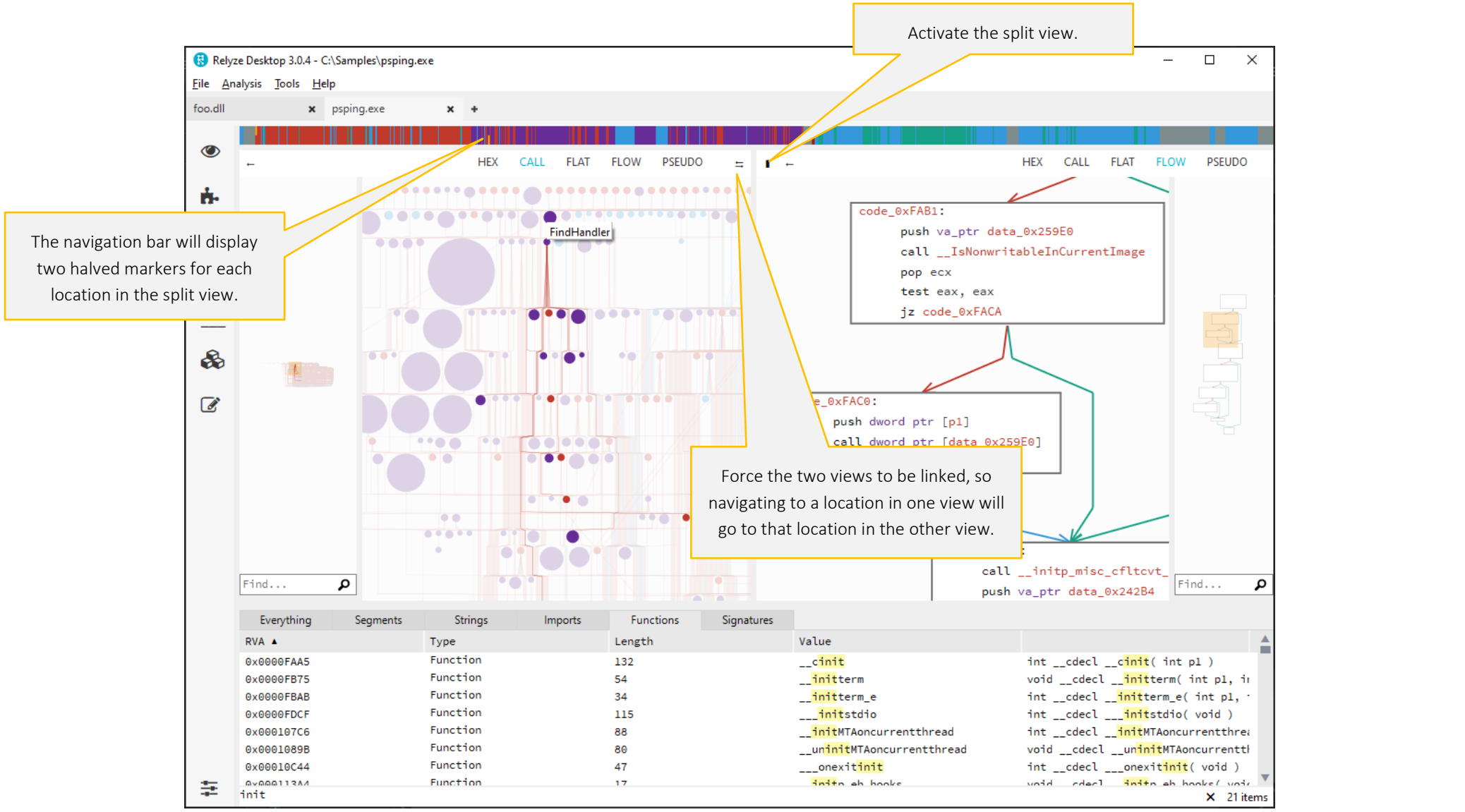
Select the type of jump table you are editing.

Configure the location of the table and the number of entries held there.

You can optionally specify a custom base address to add to a table entry.

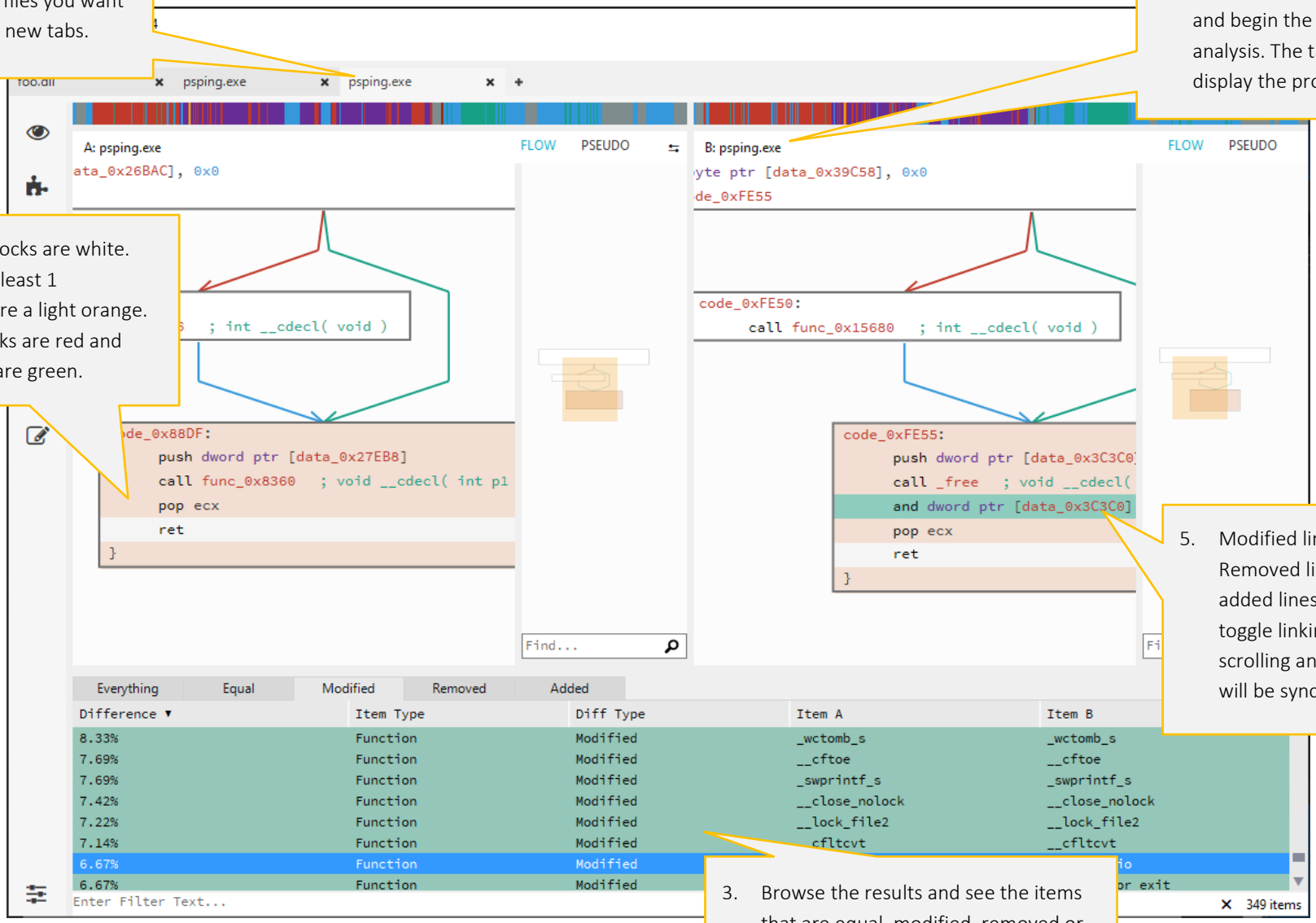
CALL GRAPH VIEW





1. Open the two files you want to compare in new tabs.

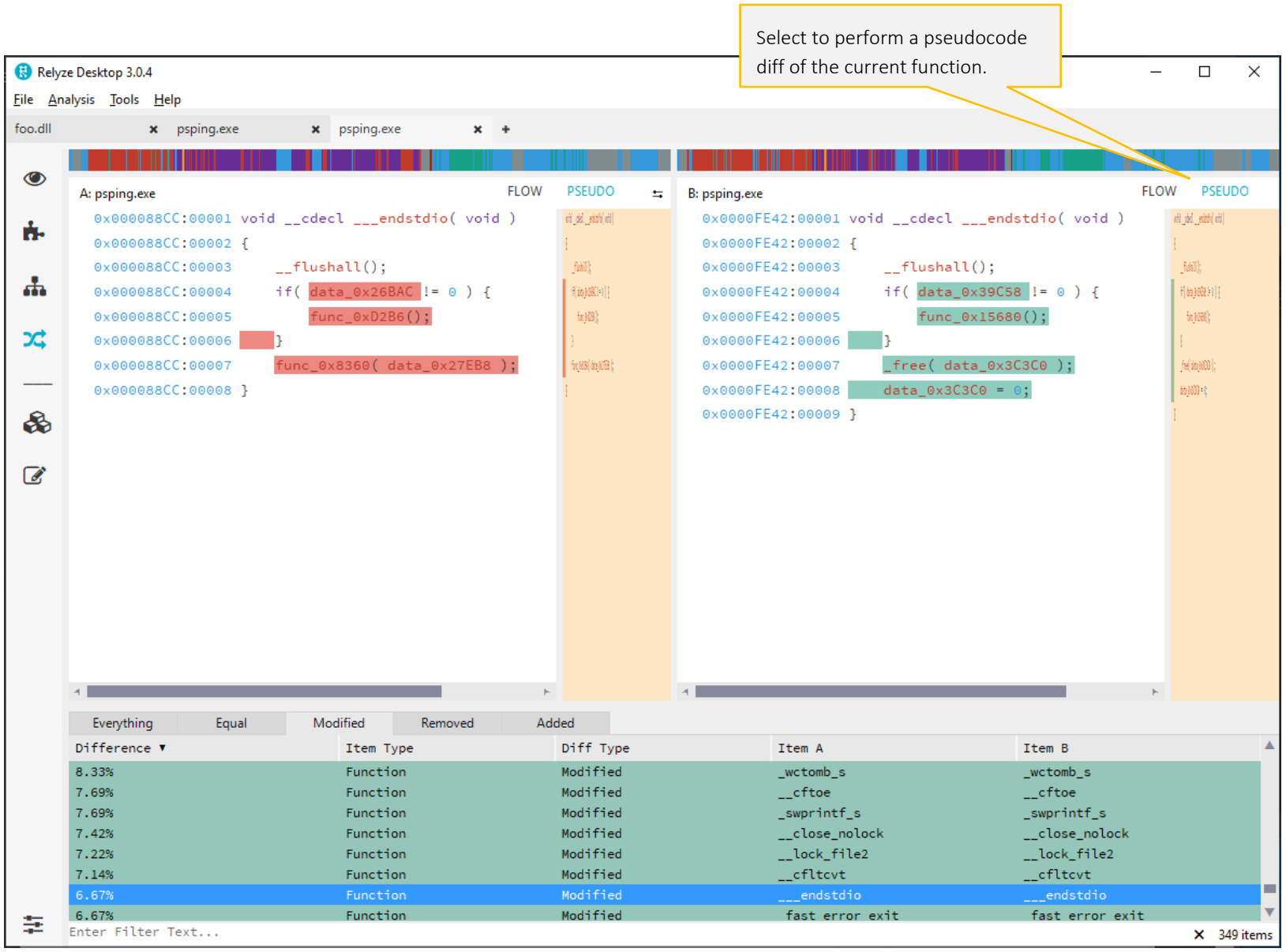
2. Click to select the second file and begin the differential analysis. The task manager will display the progress.

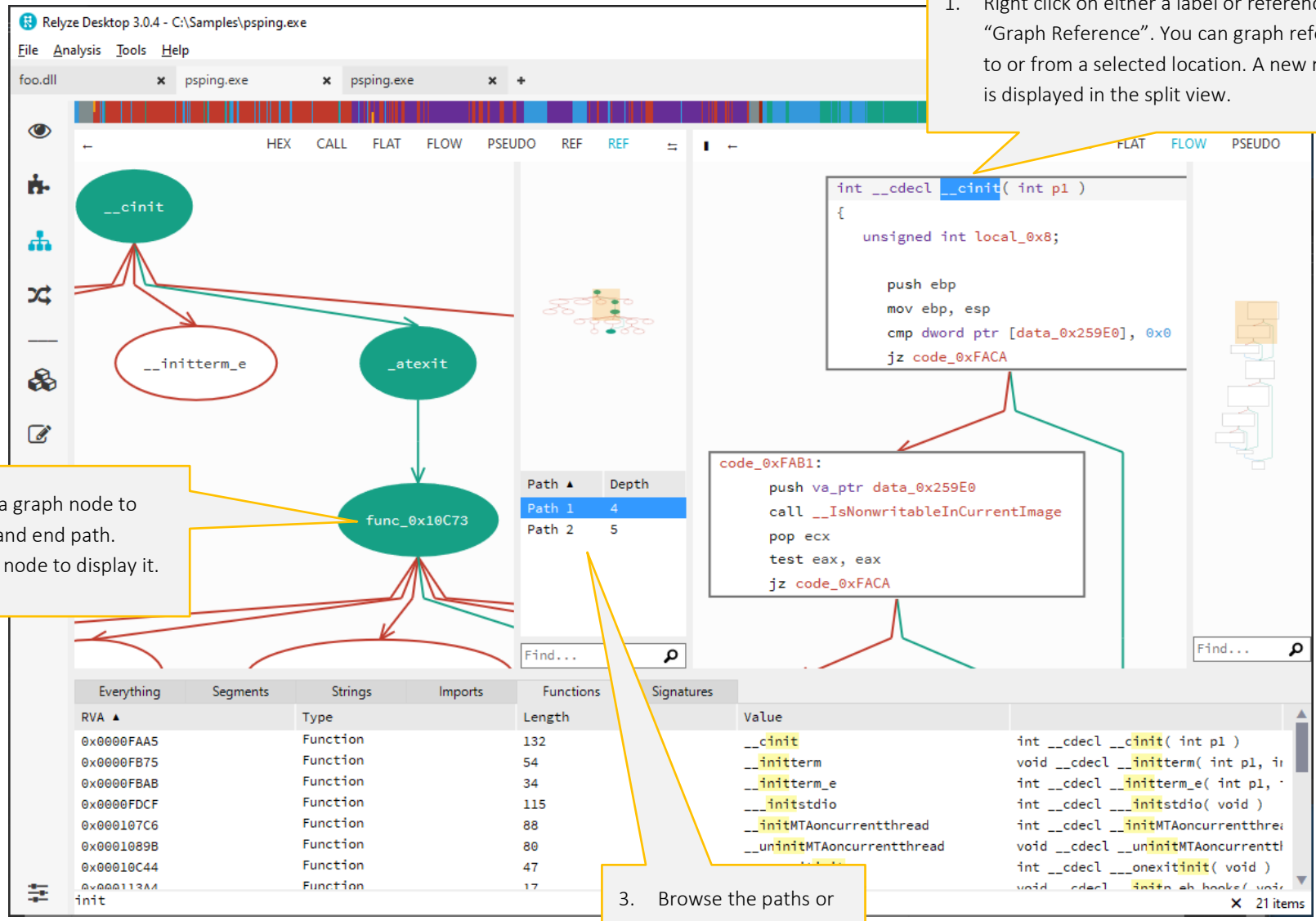


4. Unmodified blocks are white. Blocks with at least 1 modification are a light orange. Removed blocks are red and added blocks are green.

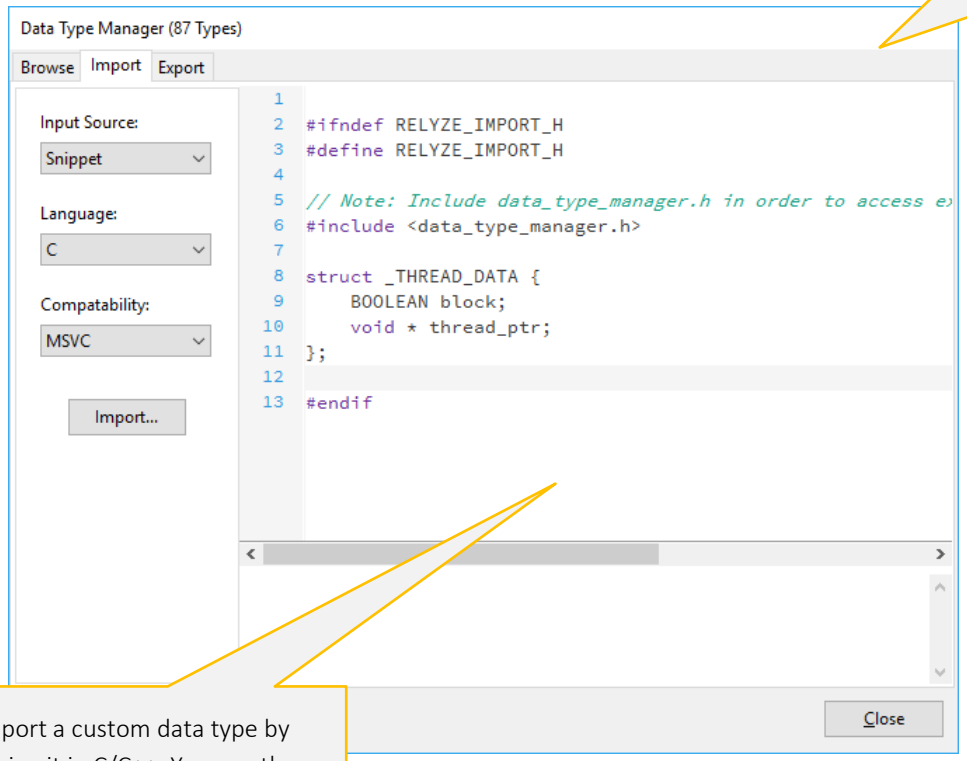
5. Modified lines are orange. Removed lines are red and added lines are green. If you toggle linking the split view, scrolling and selecting a line will be synced in both views.

3. Browse the results and see the items that are equal, modified, removed or added. Right click for more options.

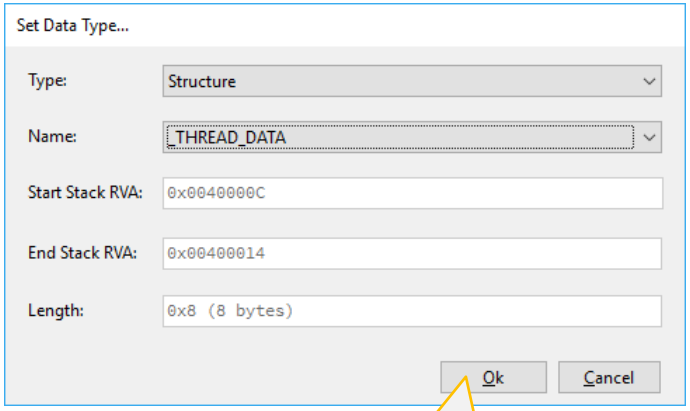




Open the Data Type Manager via either the analysis menu or the default keyboard shortcut ‘F3’.



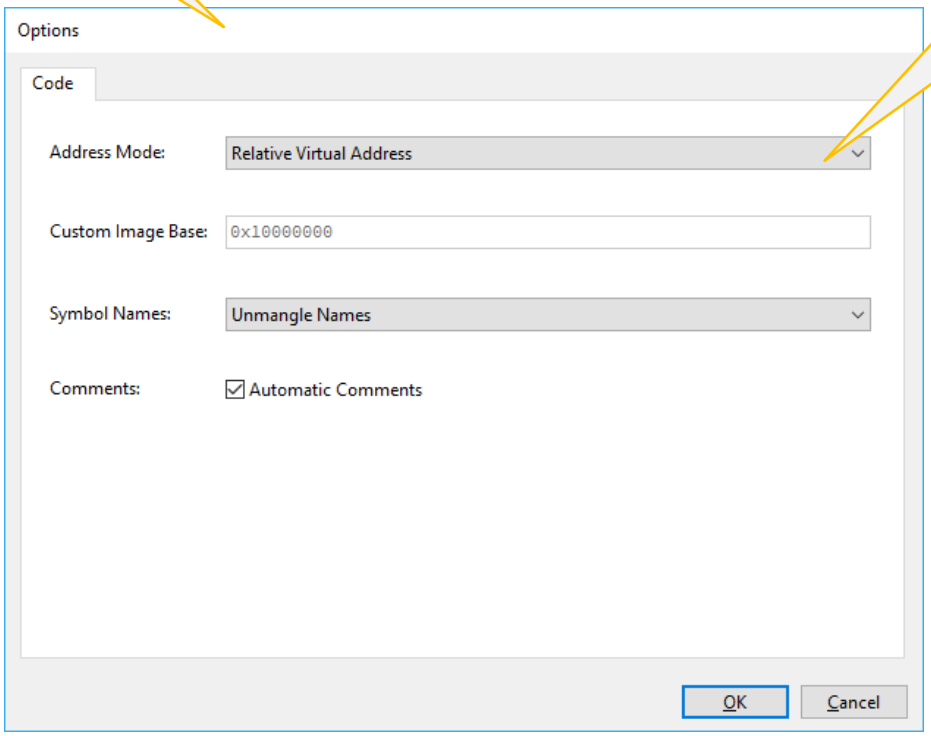
Import a custom data type by defining it in C/C++. You can then set a data block to this new type.

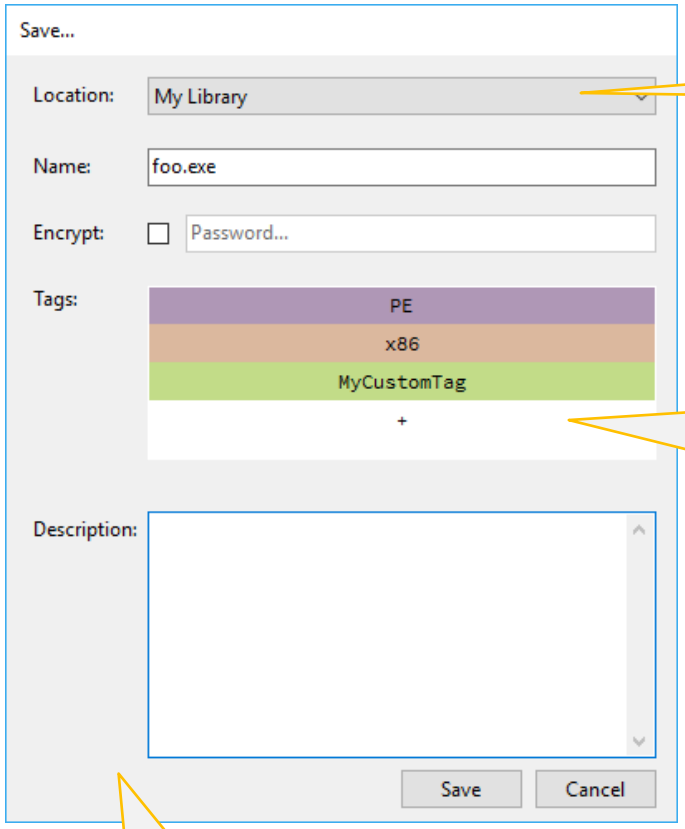


Select either a label or reference to a data block and then set its type via the right click menu or the default keyboard shortcut ‘T’.

Open the analysis options dialog via the analysis menu or the keyboard shortcut “F2”.

By default all addresses are displayed as Relative Virtual Addresses. You can select to use Virtual Addresses instead and optionally specify a custom base address to instantly rebase the analysis.



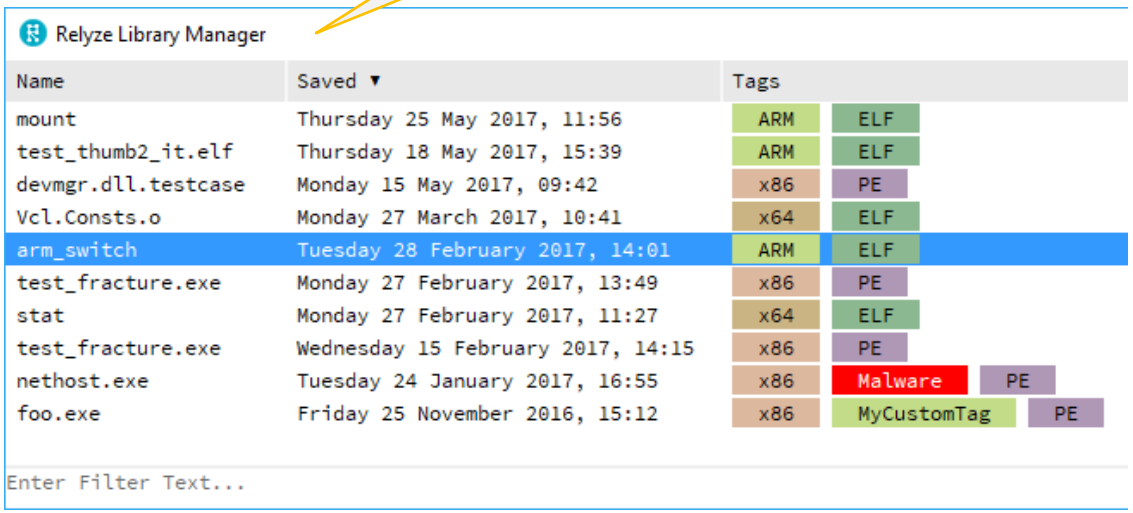


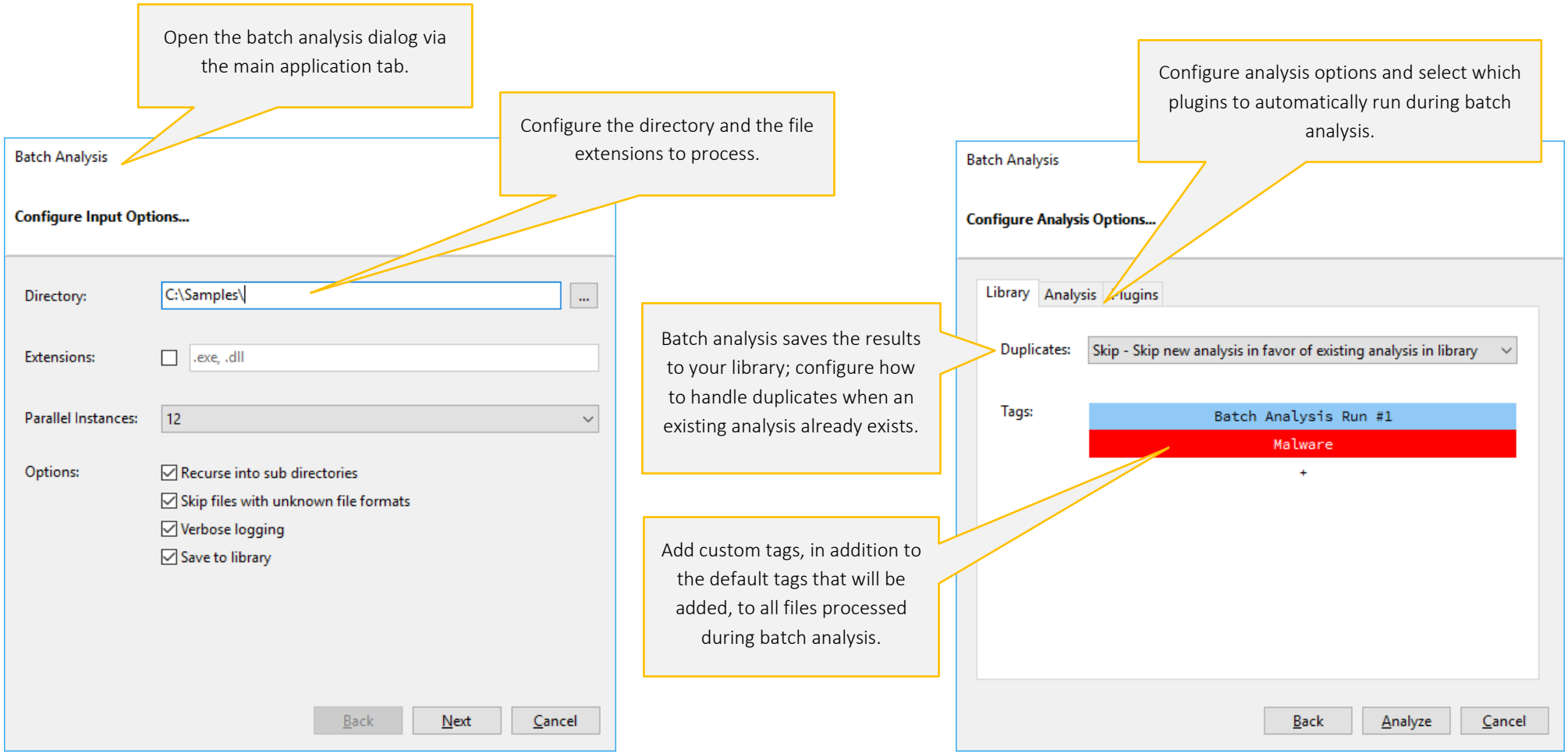
Save the analysis archive either to your library or to an external file.

Default tags will automatically be listed here. You can add in custom tags as needed. Right click to rename or re-colour a tag.

Access your library via the application main Tools menu. Double click on an item to open the analysis.

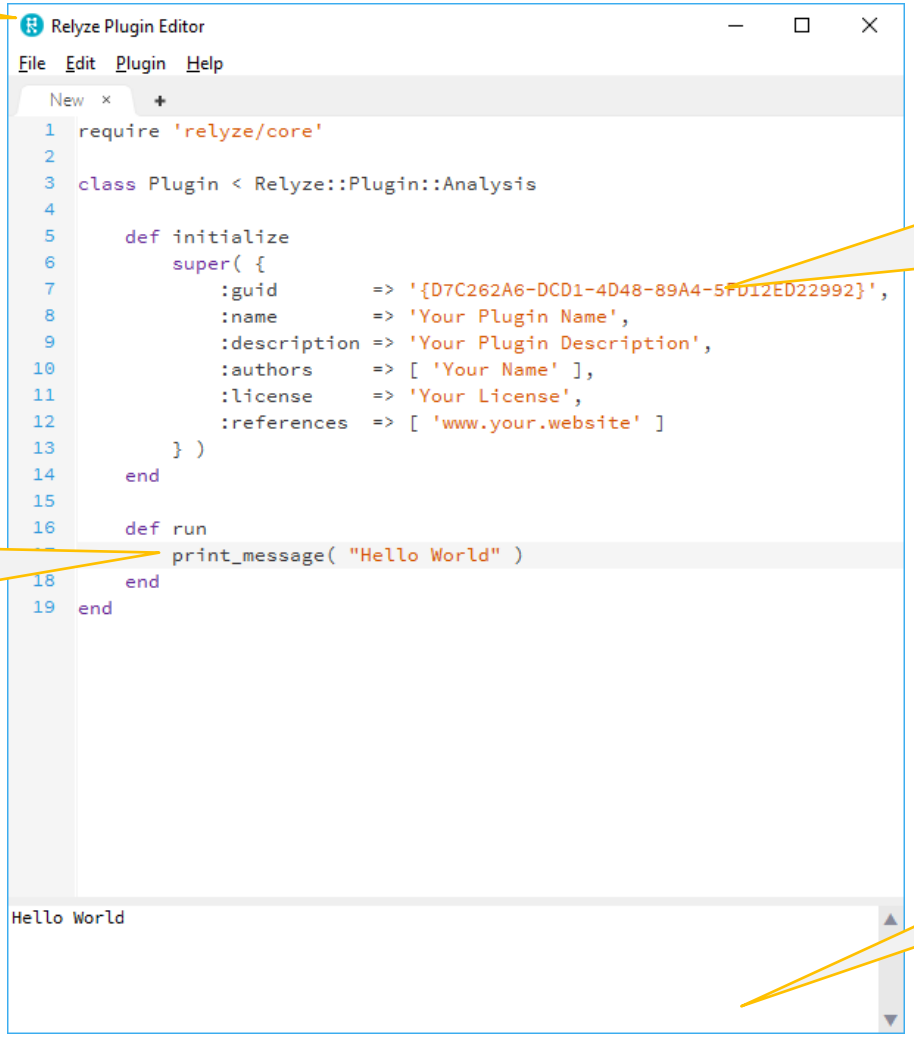
Use the application main menu or the keyboard shortcut “Ctrl-S” to save an analysis to your library.





Batch analysis is a convenient way to process many files at once. Every file successfully processed can be saved to your library. Custom plugins can be written to filter, modify and analyse files being processed during batch analysis. You can also run Relyze from the command line in a headless mode if you wish to perform any plugin based analysis without the GUI.

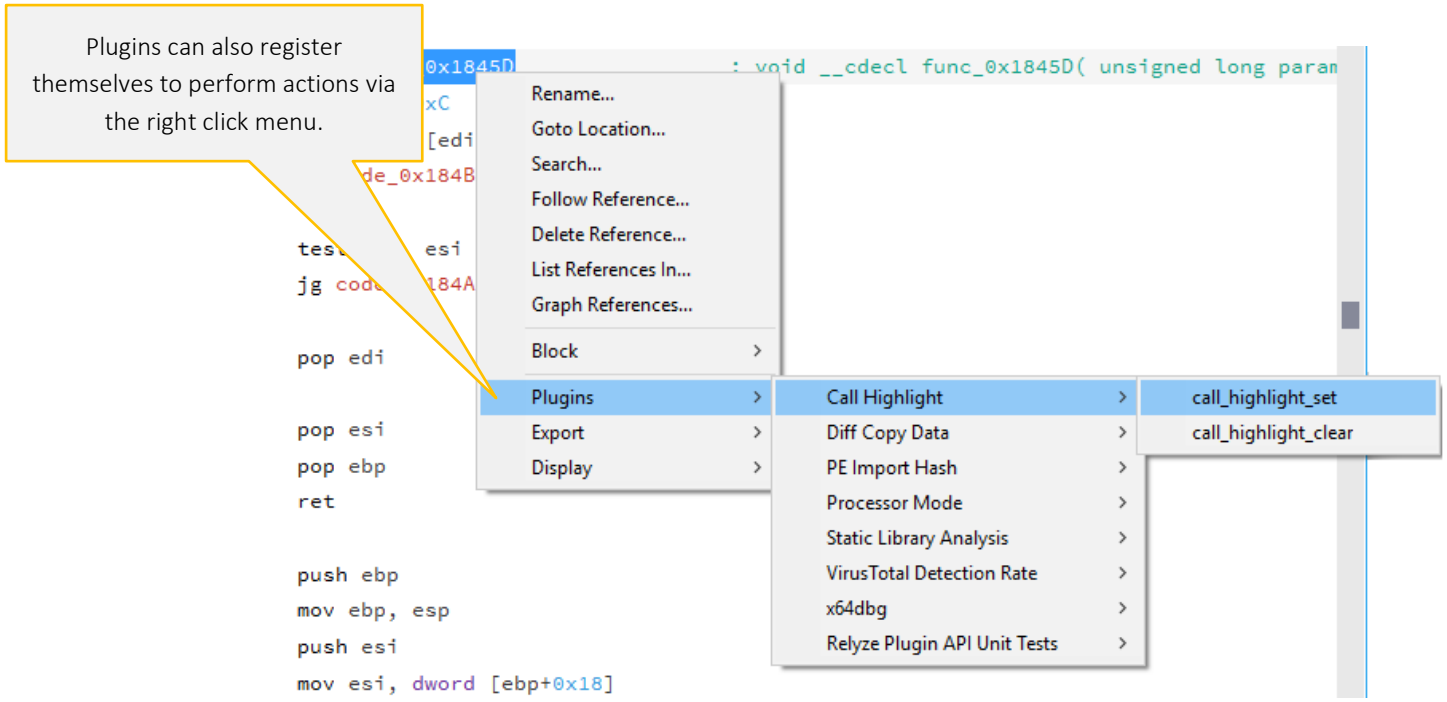
Press F1 at any time to display the Plugin Editor.



Every plugin has some associated metadata, including a unique GUID, a plugin name and description and information about the authors.

The main body of your plugin goes here. Plugins may also attach to the analysis pipeline to be invoked at different stages of analysis.

Press F5 to run the currently displayed plugin. The output console will display plugin output.



To learn more about how to create and run plugins, visit http://support.relyze.com/knowledge_base/categories/plugins-3 and https://www.relyze.com/docs/SDK/index.html

KEYBOARD SHORTCUTS

The default keyboard shortcuts are shown below. Additional keyboard shortcuts may be configured via the application options dialog.

Display Plugin Editor	F1	Block To Data	D
Display Analysis Options	F2	Block To Code	C
Display Analysis Task Manager	F3	Data Type Edit	T
Display Analysis Data Type Manager	F4	References In List	X
Plugin Editor - Run Plugin	F5	References Graph	Z
Analysis Save	Ctrl-S	Bookmark Edit	B
Navigate Back	ESCAPE	Comment Edit	;
Full Screen	F11	Jump Table Edit	J
Flash Instruction Analysis	Hold TAB	Copy Selected	Ctrl-C
Goto	G	Instruction Edit	E
Search	S	Cycle Between Flat and Flow Views	SPACE
Block Rename	N		

COMMAND LINE USAGE

You can run Relyze from the command line to analyze a file without bringing up the GUI by using the /analyze switch, for example:

```
RelyzeCLI.exe /analyze "c:\samples\foo.dll"
```

Additional command line options for /analyze are shown below:

/library <c:\path\to\library> - Specify a directory to use for the library. All saved analysis archives will be placed in this directory.
/tags "name1:hexcolor1,name2:hexcolor2" - Specify custom tags to apply to the saved analysis archive.
/nosave - Don't save the analysed file to the library.
/noflat - If the input file is not a recognised executable file format, don't process it as a flat binary file.
/skip - If a duplicate analysis archive exists in the library, don't analyse the new file.
/replace - If a duplicate analysis archive exists in the library, replace the existing archive with the newly analysed archive.
/add - Add the new analysis archive to the library, ignoring any duplicate archive that may exist.
/nosymbols - Don't try to retrieve or use symbols during analysis.
/decoder <GUID> - Run a given decoder plugin over the input file before analysis.
/plugin <File|GUID> - Run a given analysis plugin during analysis. To specify multiple plugins use a separate /plugin argument for each one.
/plugin_commandline "/opt1 /opt2=1234 /opt3=5678" - Specify any custom options to pass to all the plugins.

You can run a plugin directly from the command line via the /run switch, for example:

```
RelyzeCLI.exe /run /plugin "c:\samples\scripts\testing.rb"
```

Additional command line options for /run are shown below:

/plugin <File|GUID> - Run a given analysis plugin. To specify multiple plugins use a separate /plugin argument for each one.
/plugin_commandline "/opt1 /opt2=1234 /opt3=5678" - Specify any custom options to pass to all the plugins.
/log <c:\log.txt> - Log all plugin messages to a specific log file.
/library <c:\path\to\library> - Specify a directory to use for the library. All saved analysis archives will be placed in this directory.

SUPPORT

All online support options are available at https://www.relyze.com/support

The online plugin SDK documentation is available at https://www.relyze.com/docs/SDK/index.html

A repository of official and example plugins is available at https://github.com/relyze-ltd/plugins

For technical support please email support@relyze.com