Fas-Disassembler for Visuallisp 0.8

github.com/Hopfengetraenk/Fas-Disasm

Hopfengetraenk

Hopfengetraenk/
Fas-Disasm

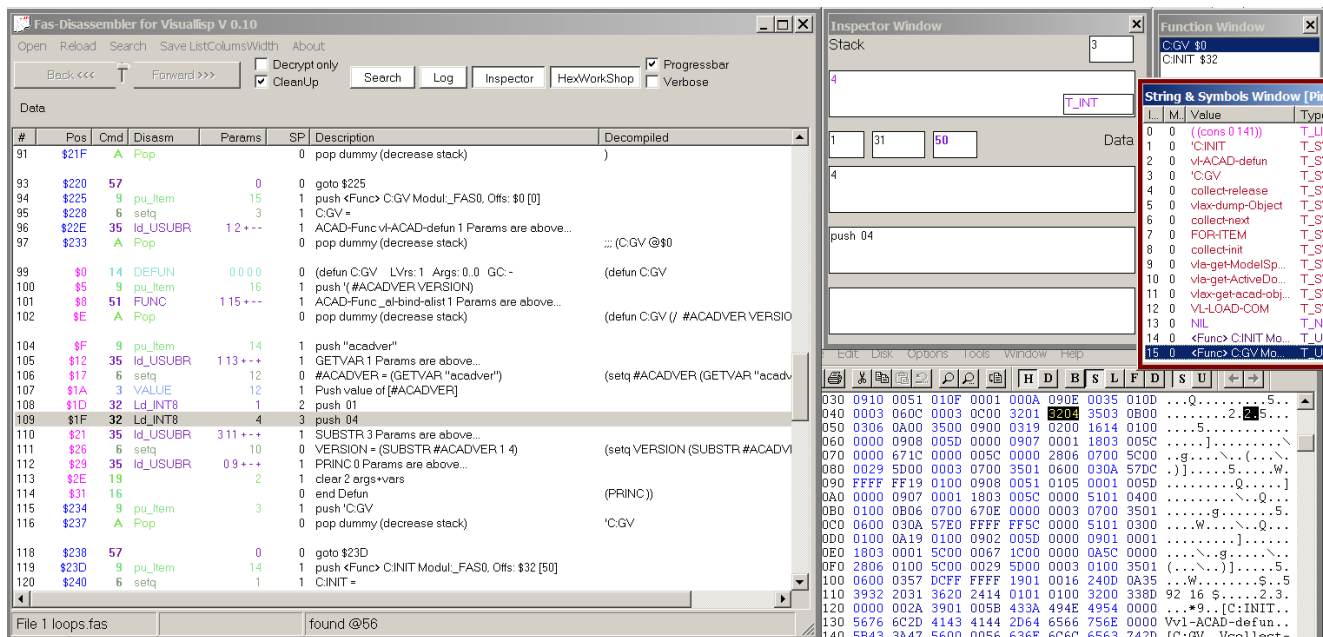Fas-Disassembler/Decompiler for AutoCAD Visual Lisp

👥 0	⊙ 5	☆ 19	⑂ 12
Contributors	Issues	Stars	Forks

=====================================

Autolisp is a programming language for AutoCAD. Lisp sourcecode files have the extension LSP and the compiled Lisp-scripts FAS. This program will decrypt the resource part of fas and fsl files (write it to disk) and disassemble the it. With help of the disassembling you can

see exactly :) what the program does, how thing are done and you can change some things with help of a Hexeditor.

Keys:

Enter, Space, double click on a line to jump to a offset that is in the Disasm Like "Goto 0213"

Backspace, Num'-' to go back to old offset

´(key beside Backspace), Num'+' to go forward

Getting FSL-Files

All internal lisp programs of Visuallisp are store in the resource section of vllib.dll (or vl.arx in Autocad LT). Use "Resource Hacker" or "Exescope" to dump these resources to disk and rename them to *.fsl.

FAS to LSP-Files

The data from the decompiler colum it written to some *_.lsp. However decompiler is far from being perfect. I really advice you to always also open the *.txt which contains all information.

Editing FAS-Files

For this purpose enable [HexWorkShop] and click some item. Fas-Dis will start HexWorkShop jump there in via sendkey. Sending keystrokes to another program is a little fragile. For best results place the HexWorkShop Window beside Fas-Dis's main window and avoid overlapping. Also take care for possible editing the fas file by error. When asked to 'Save changes'. Click NO! In HexWorkShop options enable 'Highlight changes' to better see unintented changes. Use HWorks UNDO to revert changes.

When hexediting fas-files maybe this two commands come in handy:

No Operation Good for deleting (= Nop out) unwanted instructions Bytecode: 20h (Just Space) [or 62 or 63] Parameters: none

short Jump to offset Good for jumping over unwanted instructions i.e. Fix Conditional Jump (=IF) Bytecode: 0Fh [57h for FAR Jump] Size: 3 Byte [5 Byte] Parameters: 1 Word 2 Bytes [Dword 4 Bytes] specify Bytes to Skip Example: '0F 0000' will point to the next instruction after jmp

When doing changes pay attention about the stack being embalenced. In case there are errors after editing - Decompiled the edited Fas again to check/fix possible stack corruptions.

At the moment there is no documentation file for fas-commands. To get more information about the command please look at the function 'InterpretStream()' in FasFile.cls and learn from the fas-disassembling.

Some specifications about the Fas-format are here: http://files.planet-dl.org/cw2k/Fas%20AutoLisp-Decompiler/fas-format.htm

Version history:

0.11 Feb 2018

- improved decompilation
  - support for local vars
  - started to manage/take care for types
  - branches cons, repeat
- added inspector tool
- colored output (Each command and type has it's own color)

0.10

- Uploaded to Git-hub
- Some bugfix (on reload content of *_.lsp was appended)

0.9 Dez 2013

Support for 'AutoCAD PROTECTED LISP file' *.lsp

0.8

- Support for vlx-files (vlx-splitter)
- forward backward buttons for navigation add

0.7

- opcodes names for fsl-disassembling improved
- add loop recognition
- decompilation column added

0.6

- added Quick jump function for Hexworkshop
- added Case in sensitiv search Checkbox

0.5

- FasCommand disassembling improved
- small bug's fixed

0.4 Nov 2005

First public Version

0.3..0.1

internal alpha-version (based on AutoLisp Resource Decrypter V0.9)