GSOC'18 - Cutter Debugging and Emulation support

r2con // September 8th 2018

mandlebro
Filipe Casal

Cutter

- radare2's GUI
- Supports most essential r2 features
- FOSS
- Developed in Qt C++
- https://github.com/radareorg/cutter

Google Summer of Code project

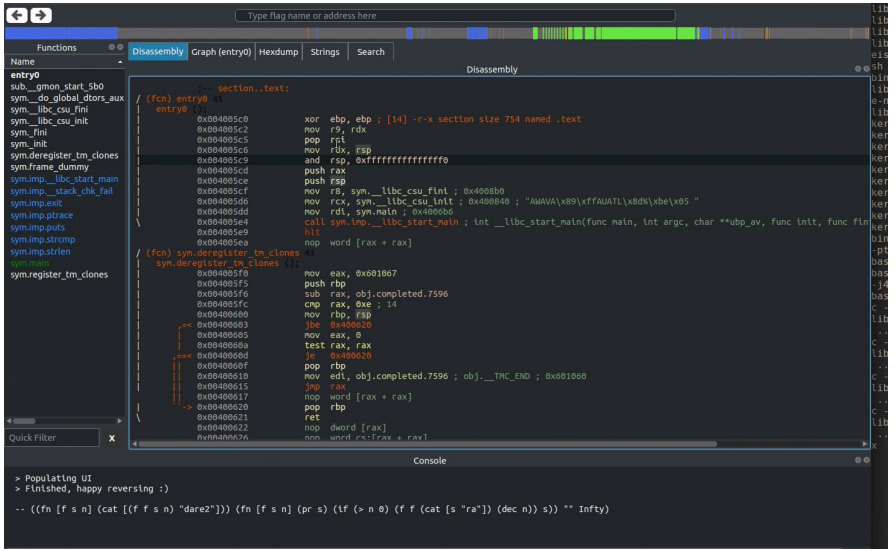
Implement Debugging and Emulation support in Cutter

Major goals:

- Independent seeks & Multiple widgets
- Debug & Emulation support

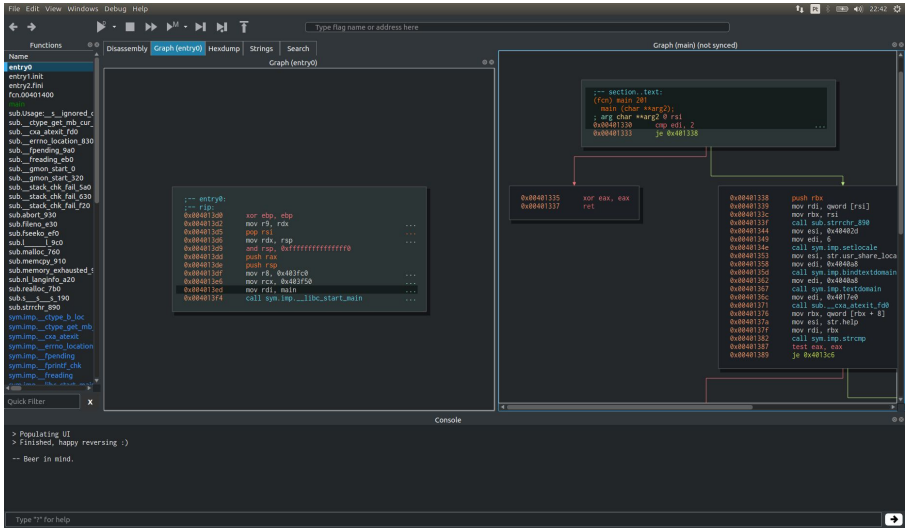
Independent seeks

You can now have different widgets with different seeks.



Multiple panels

You can now open more than one instance of the same widget



Debugging, Emulation & Attaching

Menus:

- Debug toolbar
- Context menu

Widgets:

- Registers
- Stack
- Breakpoints
- Backtrace
- Register references
- Memory maps

Debugging, Emulation & Attaching

Major Issues:

- Ptrace & multiple threads
- Handling stdin

ESIL

- Evaluable Strings Intermediate Language
- General intermediate representation
- Allows to **emulate** most architectures r2 supports!

Implemented features:

- Breakpoints now work in ESIL emulation
- ESIL continue until call: **aecc**
- Eval variable to break emulation on invalid instructions:

  e esil.breakoninvalid

Thank you!
Thanks to xarkes, Florian and Maijin for the support during the project!

Questions?

@fcasal

@filipe_casal