REVERSE ENGINEERING 101

A very brief intro to using Ghidra

ABOUT THIS TALK

- Very VERY basic intro to reverse engineering
- Overview of Ghidra and some helpful tips
- Live Demo of extracting info from a simple program
- Please ask questions!

WHAT IS REVERSE ENGINEERING (RE)

- Trying to derive some level of understanding of a binary
- This can be done by trying to disassemble the binary's machine code to generate assembly and then convert that into a high level language

TOOLS

- New Hotness: Ghidra
  - Free, from the NSA (‘Murica!)
  - https://ghidra-sre.org
- Also awesome: radare2 & optional gui “Cutter”
  - Free, cross platform, CLI only unless using Cutter (GUI)
  - https://rada.re
  - https://github.com/radareorg/cutter/releases
- Old ’n Busted (not really, IDA is still the most popular RE tool): IDA / IDA Pro
  - https://www.hex-rays.com/products/ida/

ABOUT GHIDRA (GEE-DRUH)

キングギドラ KINGU GIDORA

- From Ghidorah, the Three-Headed Monster (1964)
- Developed by NSA, released at RSA San Francisco 2019
- Java Based
- Supported Architectures:
  - 16, 32 and 64 bit x86
  - ARM and AARCH64
  - PowerPC 32/64 and PowerPC VLE
  - MIPS 16/32/64
  - MicroMIPS
  - 68xxx
  - Java
  - DEX bytecode
  - PA-RISC
  - PIC 12/16/17/18/24
  - SPARC 32/64
  - CR16C
  - Z80
  - 6502
  - 8051
  - MSP430
  - AVR8
  - AVR32

BASIC WORKFLOW

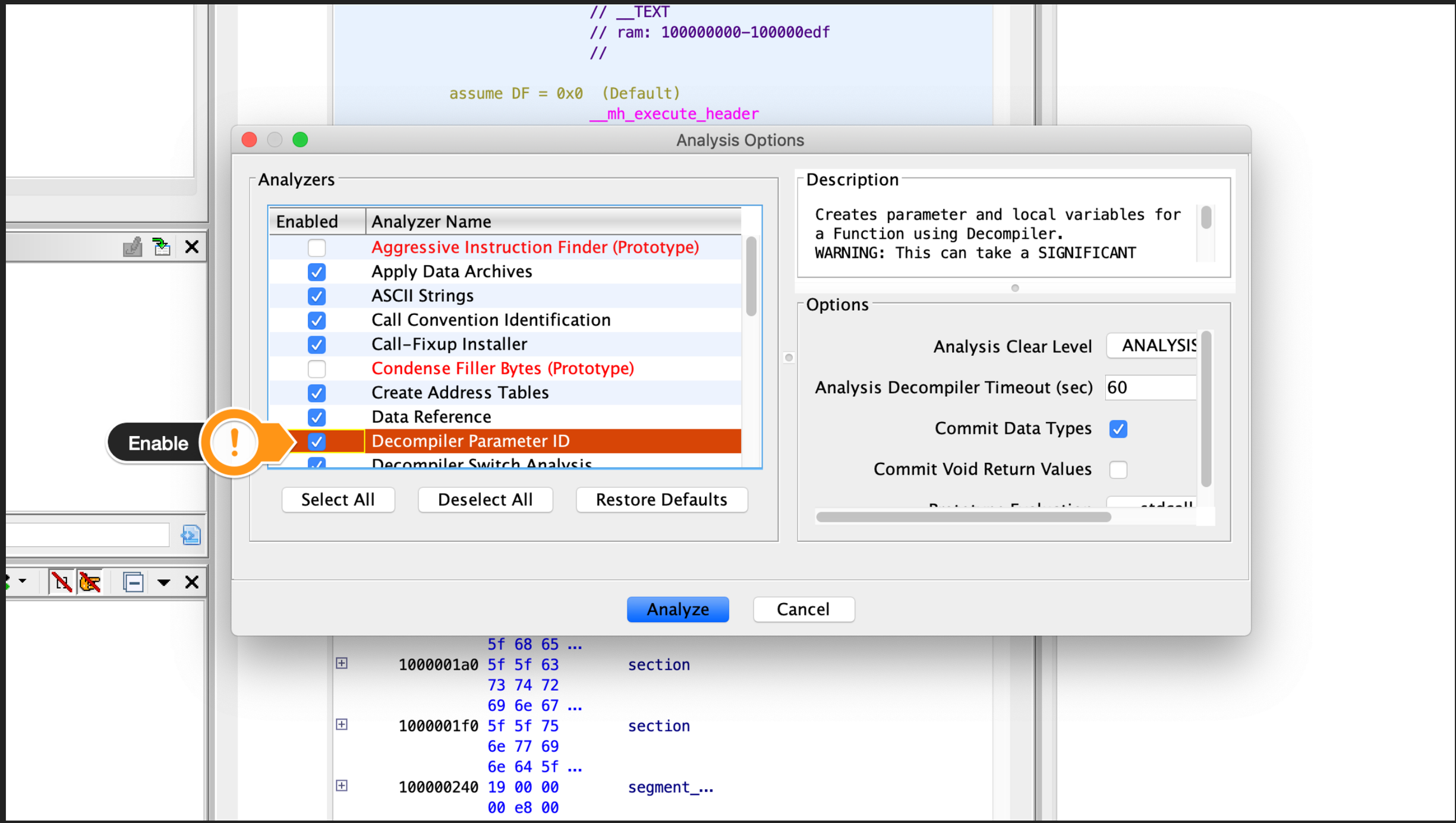
- First determine your goals
  - Learn more about something?
  - Search for exploits / vulns?
  - Set a target for yourself - don’t get lost in the rabbit hole
- Load binary into tool
- Analyze it
- Inspect the decompiled code. Try to gain insight into what it does
  - Start at entry point
  - Look at variables defined
  - Rename variables to make things clearer
  - Look at strings and other hard coded information

IMPORT SETTINGS

- Create Project
- Add files
  - Check “Import External Libraries"
- Analyze file
  - Enable “Decompile Paramater IDs”

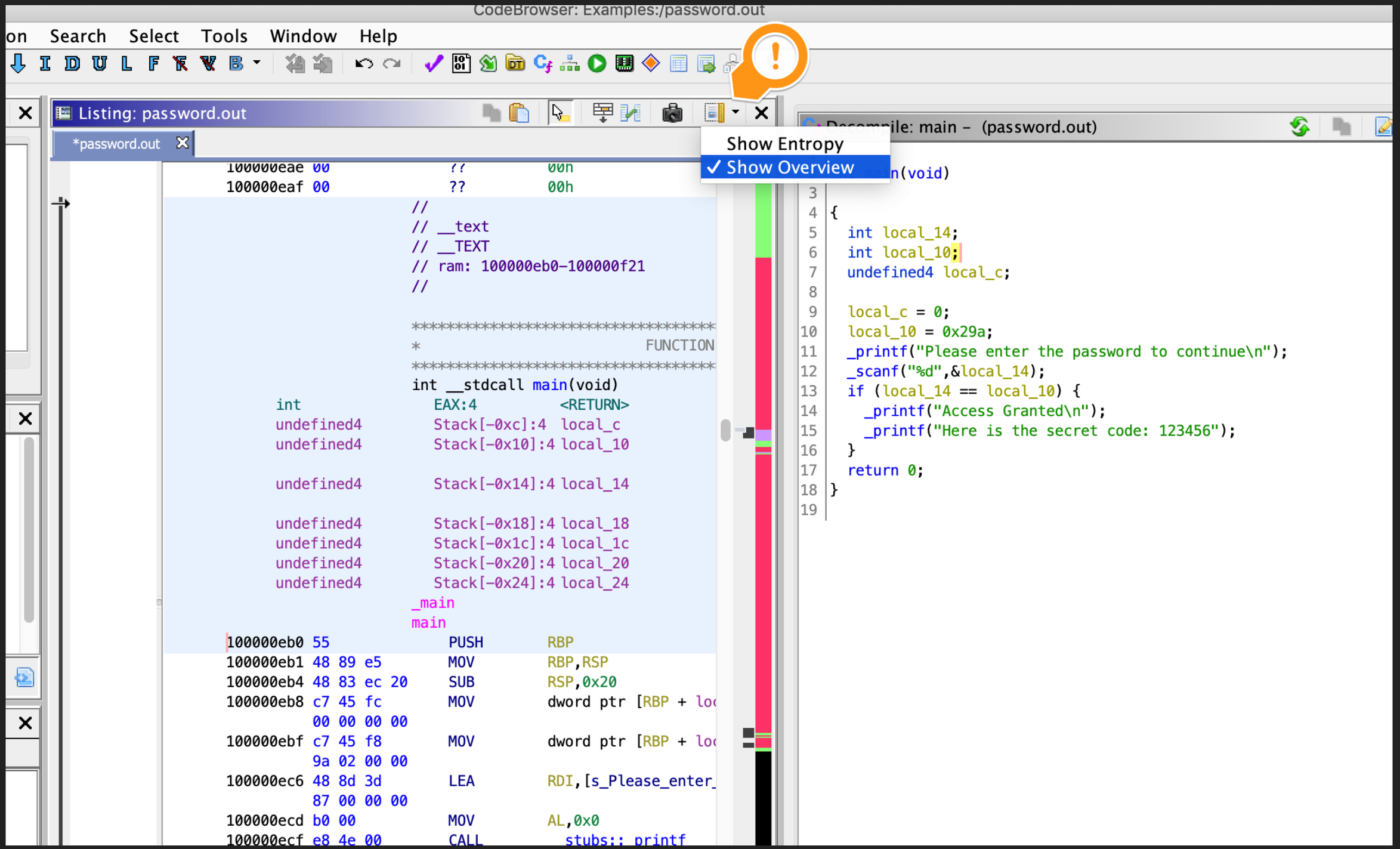
TIPS

Enable Decompiler Parameter ID



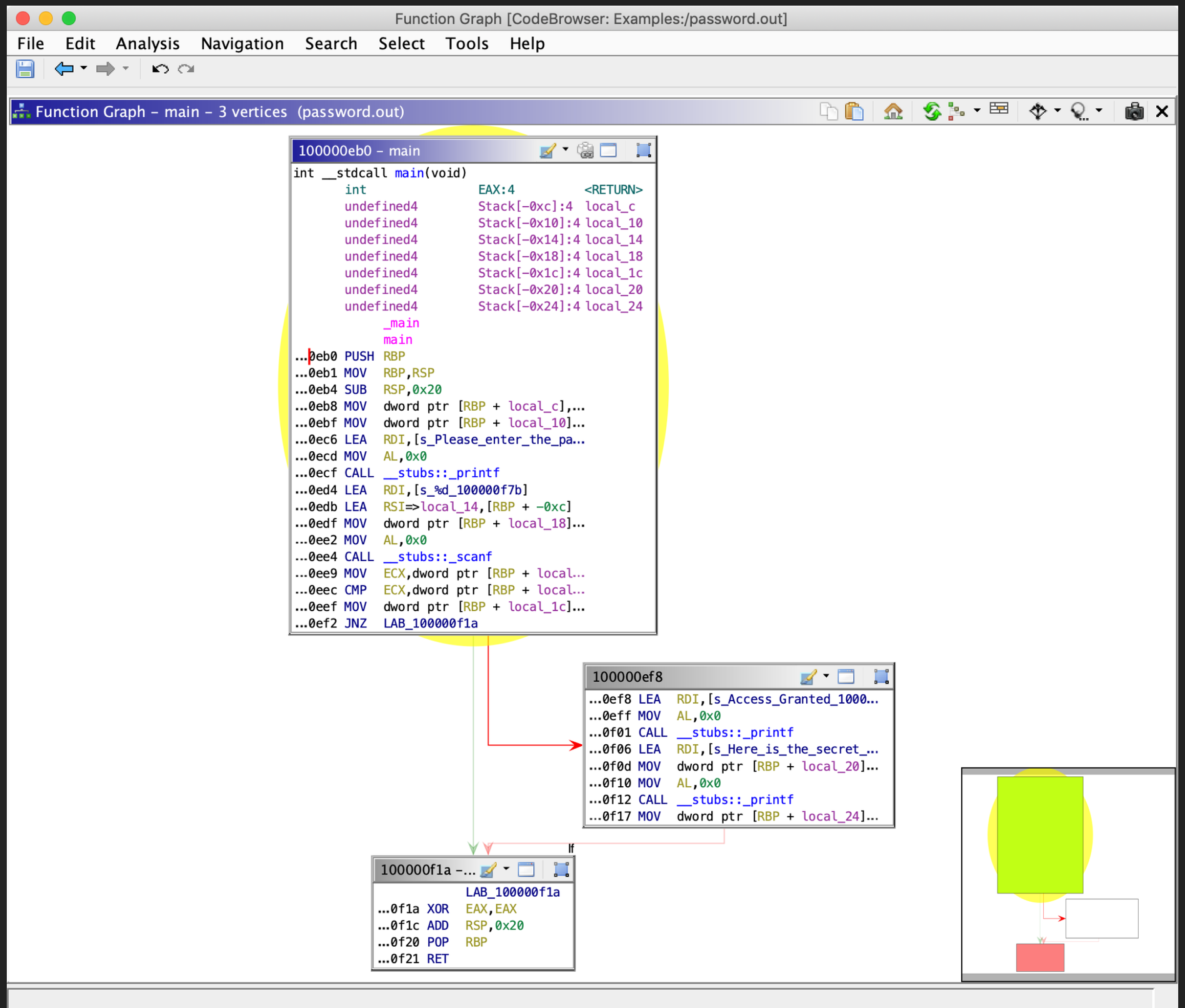
TIPS

Enable Binary Segment Overview



TIPS

Graph view provides a visual overview of program flow



HOTKEYS

- L - Rename
- G - Goto
- ; - Add comment

DEMOOOOOO

RESOURCES

- Microsoft PE Format overview - https://docs.microsoft.com/en-us/windows/win32/debug/pe-format
- Creating a simple C reverse shell - https://rastating.github.io/creating-a-reverse-tcp-shellcode/
- Ghidra Quick Tutorial - https://www.youtube.com/watch?v=fTGTnrgjuGA
- CrackMe's - Programs to test your RE skills - https://crackmes.one
- Ghidra Cheet Sheet - https://ghidra-sre.org/CheatSheet.html
- Amazon Coretto JDK 11 - https://docs.aws.amazon.com/corretto/latest/corretto-11-ug/downloads-list.html