Software Reverse Engineering Framework

Who am I ?

- ✓ Abdulrahman Al-Nimari
- ✓ Cyber Security Advisor, Architect, Consultant
- ✓ 25 Years IT & Cyber Security Experience
- ✓ Speaker : BSides, HITB, ICSC, AECT, ASC, MENA ISC
- ✓ Awarded Arab Cybersecurity Social Network Influencer Prize 2019
- ✓ Awarded Arab Cybersecurity Social Network Influencer Prize 2020
- ✓ CISSP, CISM, CCISO, PMP, GCIH, GCIA, GCUX, GREM, GSEC
- ✓ @nimari
- ✓ https://www.linkedin.com/in/alnimari/
- ✓ alnimari@gmail.com
- ✓ +966 (566) 465270

Agenda

- ✓ What is Software Reverse Engineering – SRE ?
- ✓ Tools of The Trade
- ✓ What is GHIDRA ?
- ✓ Installing and Using Ghidra
- ✓ Ghidra Key Features
- ✓ Demo

What is software reverse engineering (SRE) ?

- ✓ **“Reverse engineering**, also called **back engineering**, is the process by which a man-made object is deconstructed to reveal its designs, architecture, code or to extract knowledge from the object.”

https://en.wikipedia.org/wiki/Reverse_engineering

- ✓ **“Software reverse engineering (SRE)** is the practice of analyzing a software system, either in whole or in part, to extract design and implementation information.”

https://link.springer.com/chapter/10.1007/978-3-642-04117-4_31

Tools of The Trade in SRE

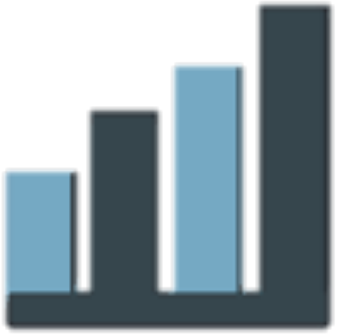
- ✓ IDA
- ✓ Binary Ninja
- ✓ Radare2
- ✓ Hopper
- ✓ GDB
- ✓ objdump !!
- ✓ GHIDRA

What is Ghidra ?

- ✓ Full-Featured SRE framework developed by the NSA.
- ✓ ~ 20 years of development.
- ✓ 1.2M lines of code.
- ✓ Primarily written in Java with some parts in C/C++
- ✓ Runs on Mac, Linux and Windows.
- ✓ Designed for customizability and extensibility.
- ✓ Publicly released in March 2019.
- ✓ Source code released on Github April 2019.
- ✓ www.ghidra-sre.org
- ✓ https://github.com/NationalSecurityAgency/ghidra

Ghidra is Being Actively Used

- ✓ www.ghidra-sre.org Stats (as of June 25)
  - ✓ 9.0.0: 302k downloads
  - ✓ 9.0.1: 36k downloads
  - ✓ 9.0.2: 100k downloads
  - ✓ 9.0.4: 42k downloads
  - ✓ Site views: 10.6M
  - ✓ Video hits: 751k
- ✓ Github Stats (as of June 25)
  - ✓ 16145 stars
  - ✓ 2019 forks
  - ✓ 718 watching
  - ✓ 608 issues, 272 open
  - ✓ 111 pull requests, 35 open

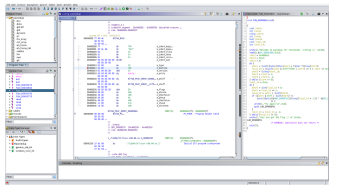


Using Ghidra

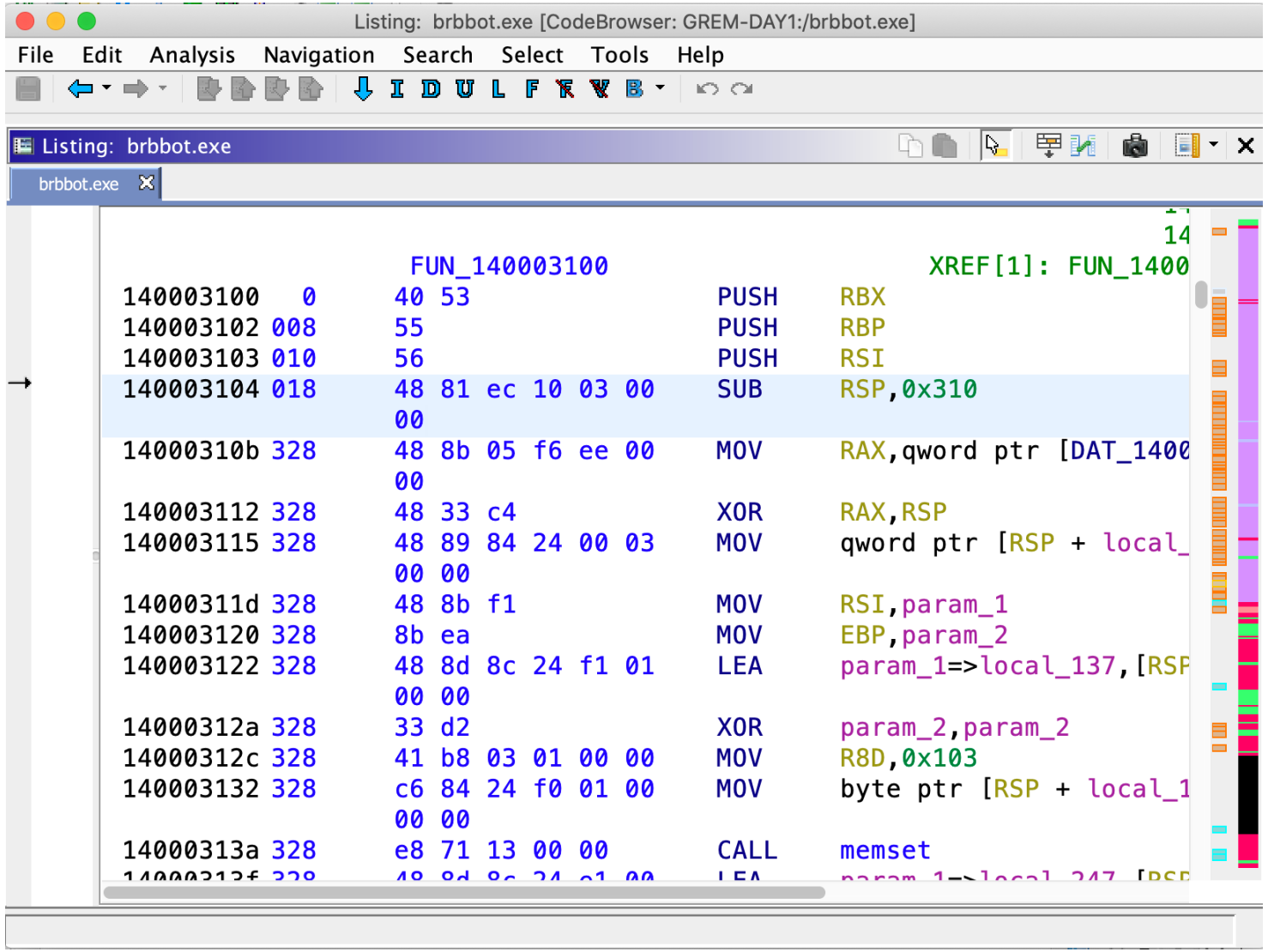
- ✓ Install OpenJDK 11
  - https://jdk.java.net/11
  - export PATH=$PATH:/opt/java-jdk/bin

- ✓ Download Ghidra
  - https://ghidra-sre.org
  - https://github.com/NationalSecurityAgency/ghidra/releases.

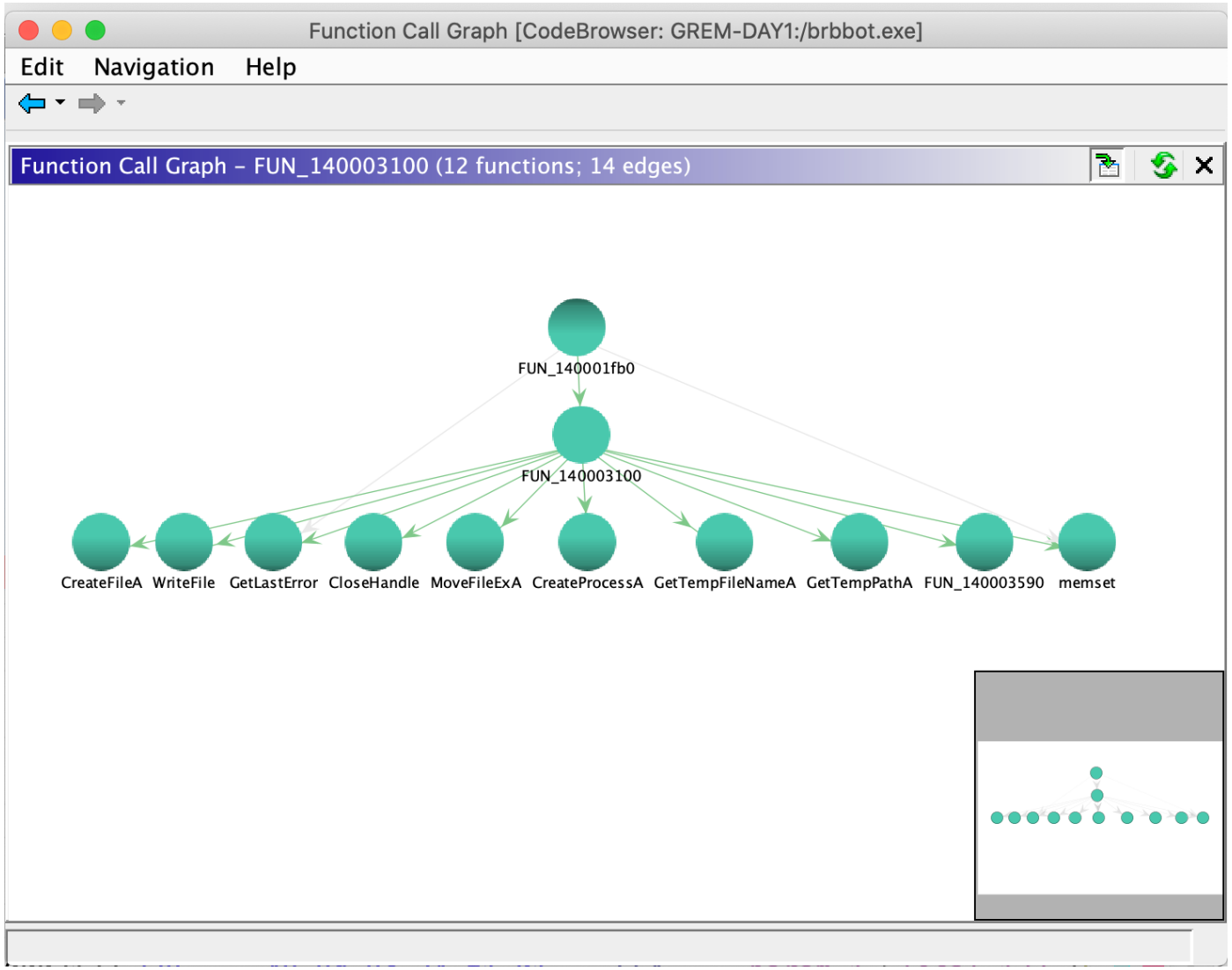
- ✓ Enjoy



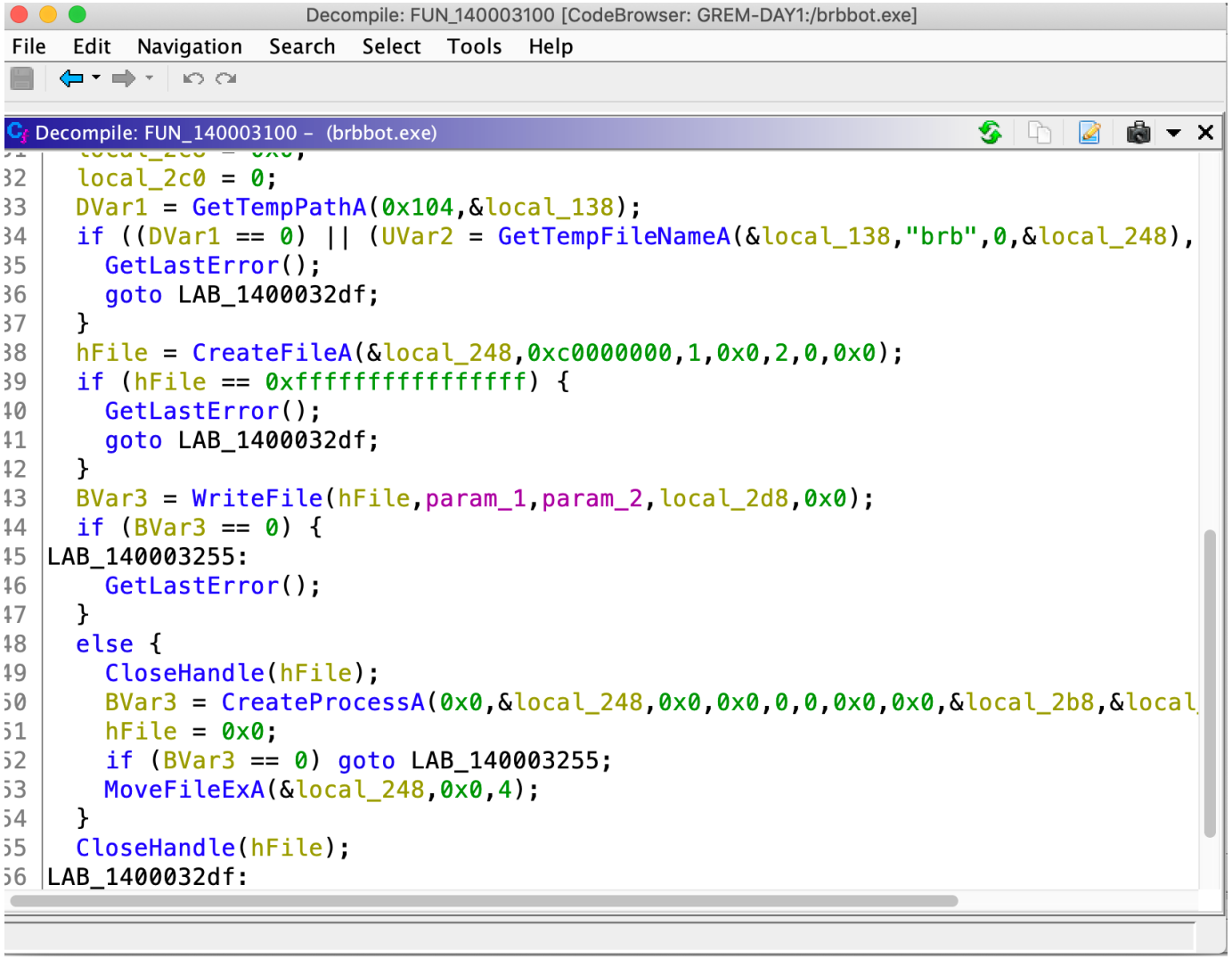
Ghidra Features - Listing Window (Disassembler)



Ghidra Features - Function Call Graph

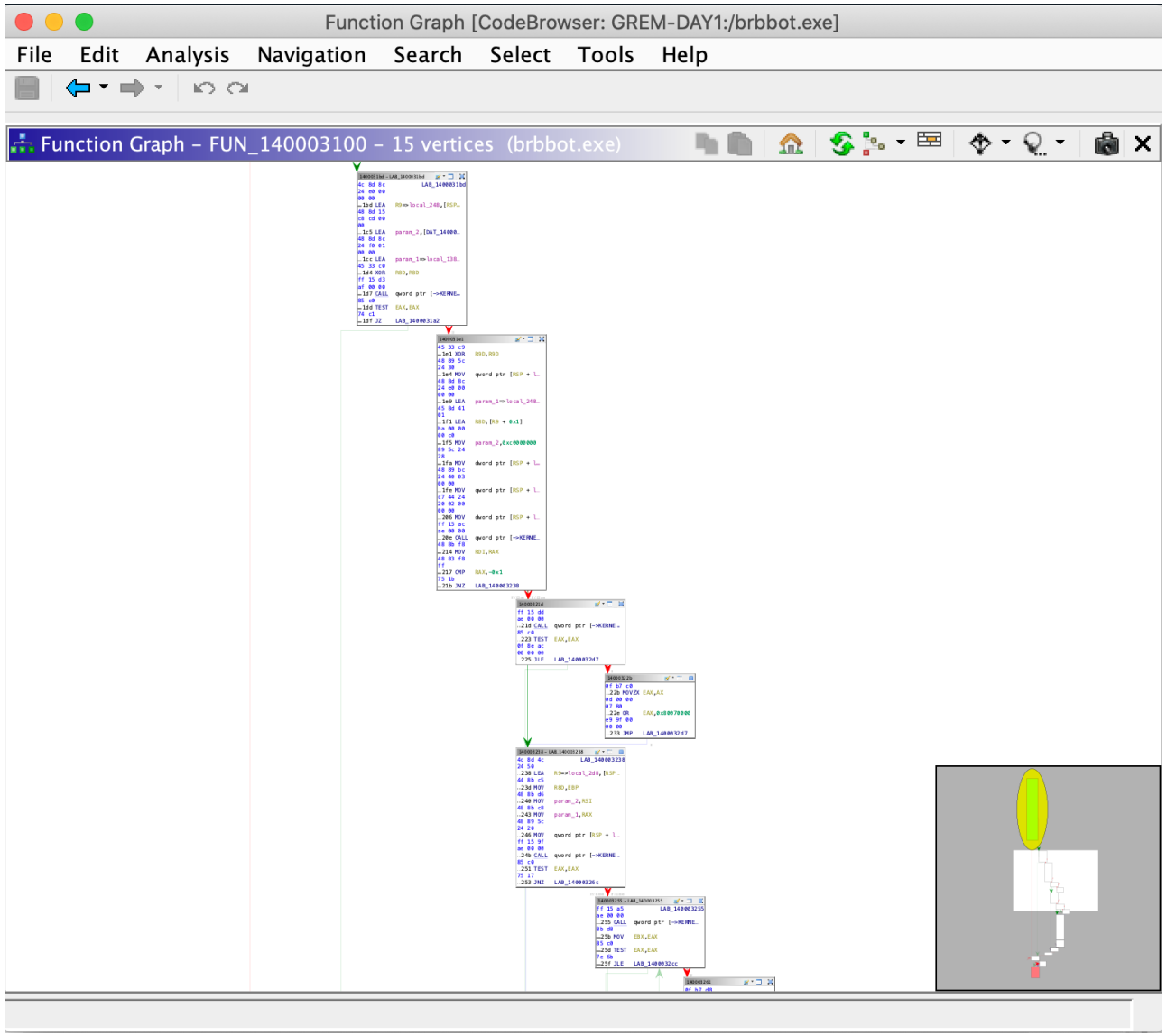


Ghidra Features - The Gold Feature: Decompiler

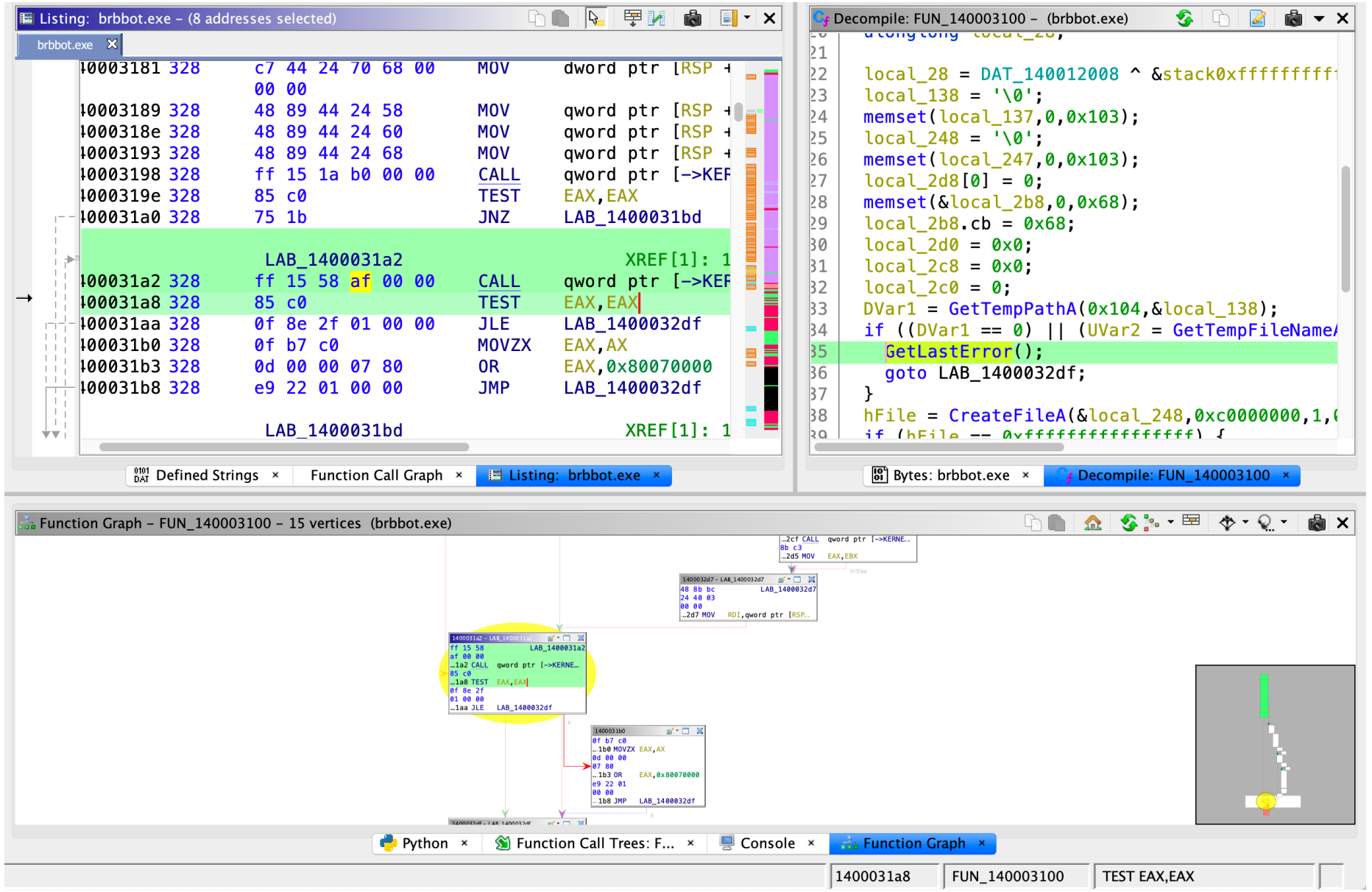



```
  local_2c0 = 0;
  DVar1 = GetTempPathA(0x104,&local_138);
  if ((DVar1 == 0) || (UVar2 = GetTempFileNameA(&local_138,"brb",0,&local_248),
    GetLastError();
    goto LAB_1400032df;
  }
  hFile = CreateFileA(&local_248,0xc0000000,1,0x0,2,0,0x0);
  if (hFile == 0xffffffffffffffff) {
    GetLastError();
    goto LAB_1400032df;
  }
  BVar3 = WriteFile(hFile,param_1,param_2,local_2d8,0x0);
  if (BVar3 == 0) {
LAB_140003255:
    GetLastError();
  }
  else {
    CloseHandle(hFile);
    BVar3 = CreateProcessA(0x0,&local_248,0x0,0x0,0,0,0x0,0x0,&local_2b8,&local
    hFile = 0x0;
    if (BVar3 == 0) goto LAB_140003255;
    MoveFileExA(&local_248,0x0,4);
  }
  CloseHandle(hFile);
LAB_1400032df:
```

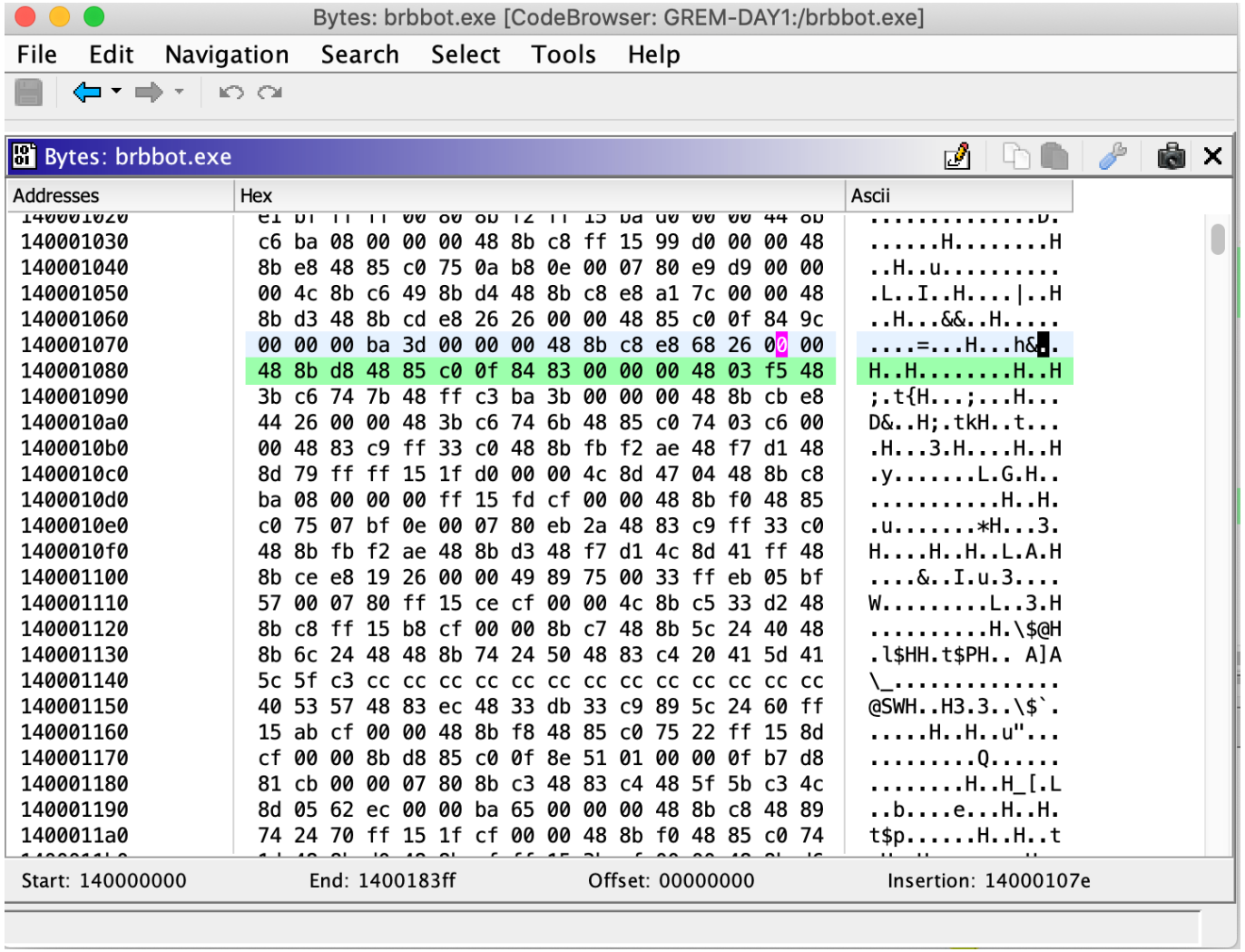
Ghidra Features - Function Graph



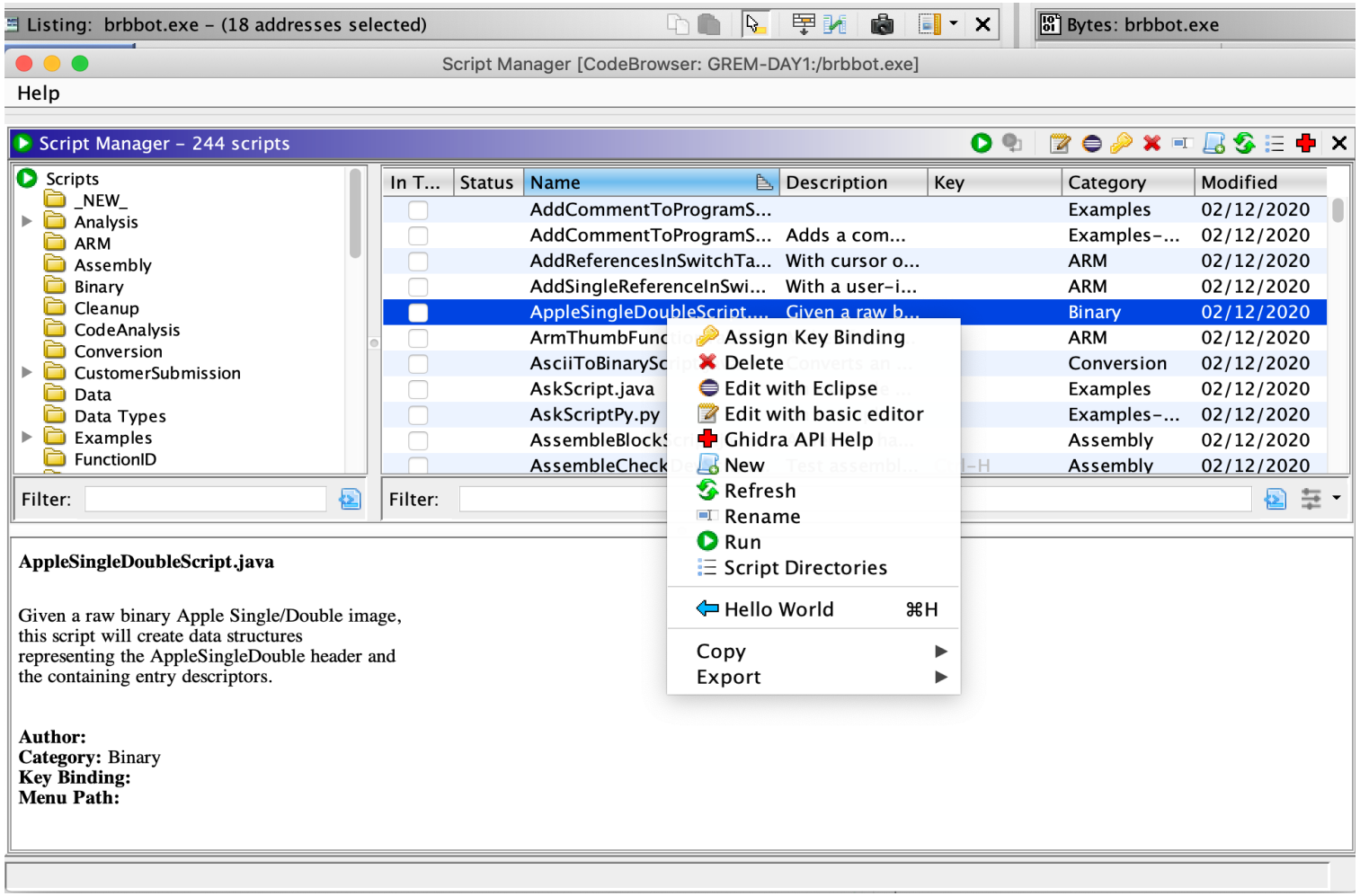
Ghidra Features - Synched Views



Ghidra Features - Bytes Window (Hex Editor)



Ghidra Features - Script Window



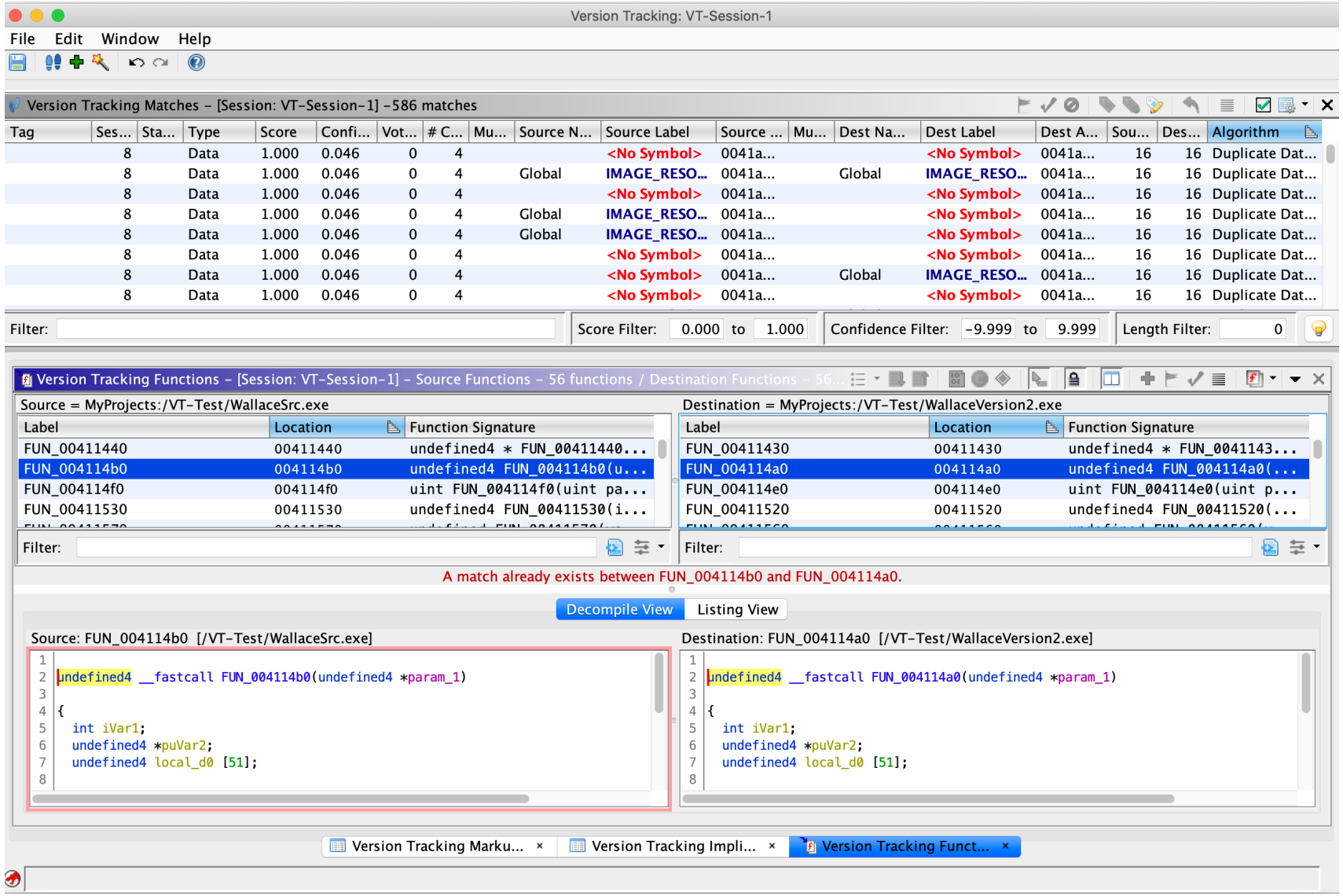
Java, Python and Eclipse Editor Integration

Ghidra Features - Version Tracking

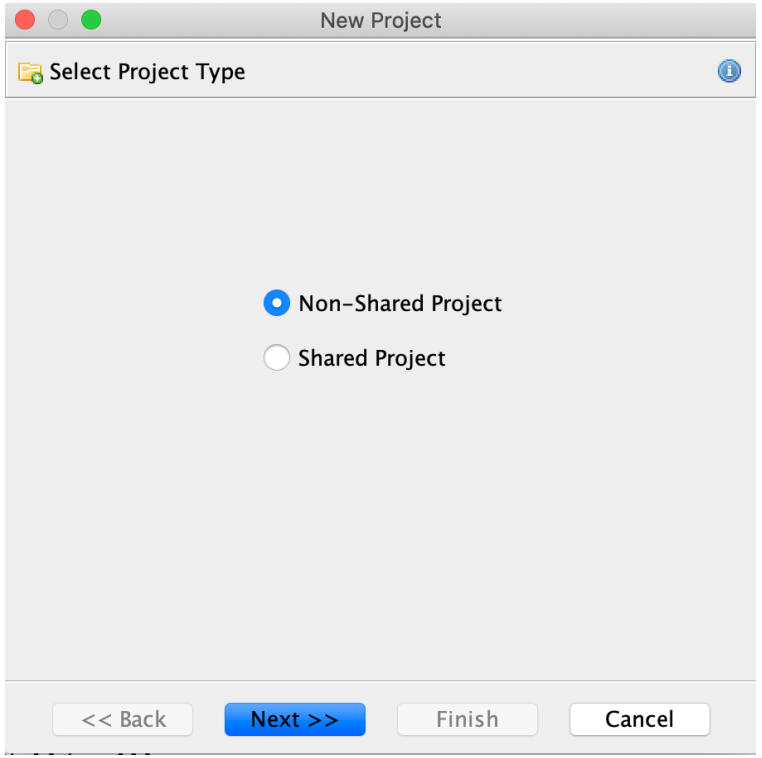
Matches functions and data from one version to another

Multiple algorithms for finding matches

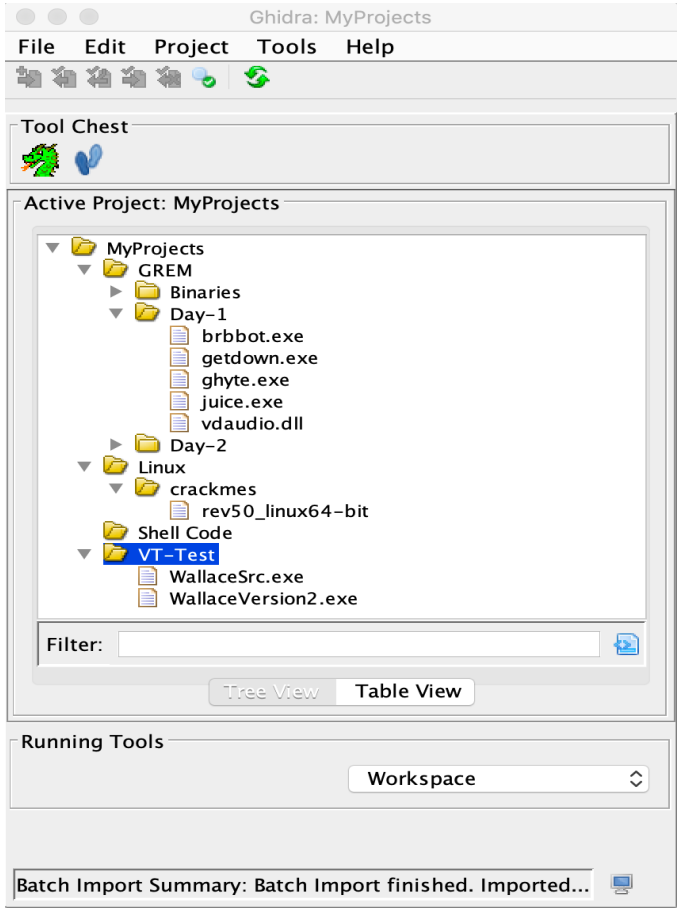
Easily port annotations and analysis from one version to another



Ghidra Features - Ghidra Projects



Multi User, Collaboration, Version Control
https://ghidra-server.org/
Or create your own ghidra server



Drag Your Binaries In

Ghidra Features - Processors Supported

- ✓ x86 16/32/64
- ✓ ARM/AARCH64
- ✓ PowerPC 32/64, VLE
- ✓ MIPS 16/32/64,micro
- ✓ 68k
- ✓ Java / DEXbytecode
- ✓ PA-RISC
- ✓ PIC 12/16/17/18/24
- ✓ Sparc32/64
- ✓ CR16C
- ✓ Z80
- ✓ 6502
- ✓ 8051
- ✓ MSP430
- ✓ AVR8, AVR32
- ✓ Others + variants

Your processor is not in the above list, you can implement a new CPU architecture using Sleigh Language

Ghidra Features - Ghidra Headless Mode

```
[support]$ ./analyzeHeadless /users/test/ghidra-projects project1 -import
/usr/bin/* -recursive -postScript MyScript.py
```

Automation and Scripting with Headless Analyzer From the Commandline

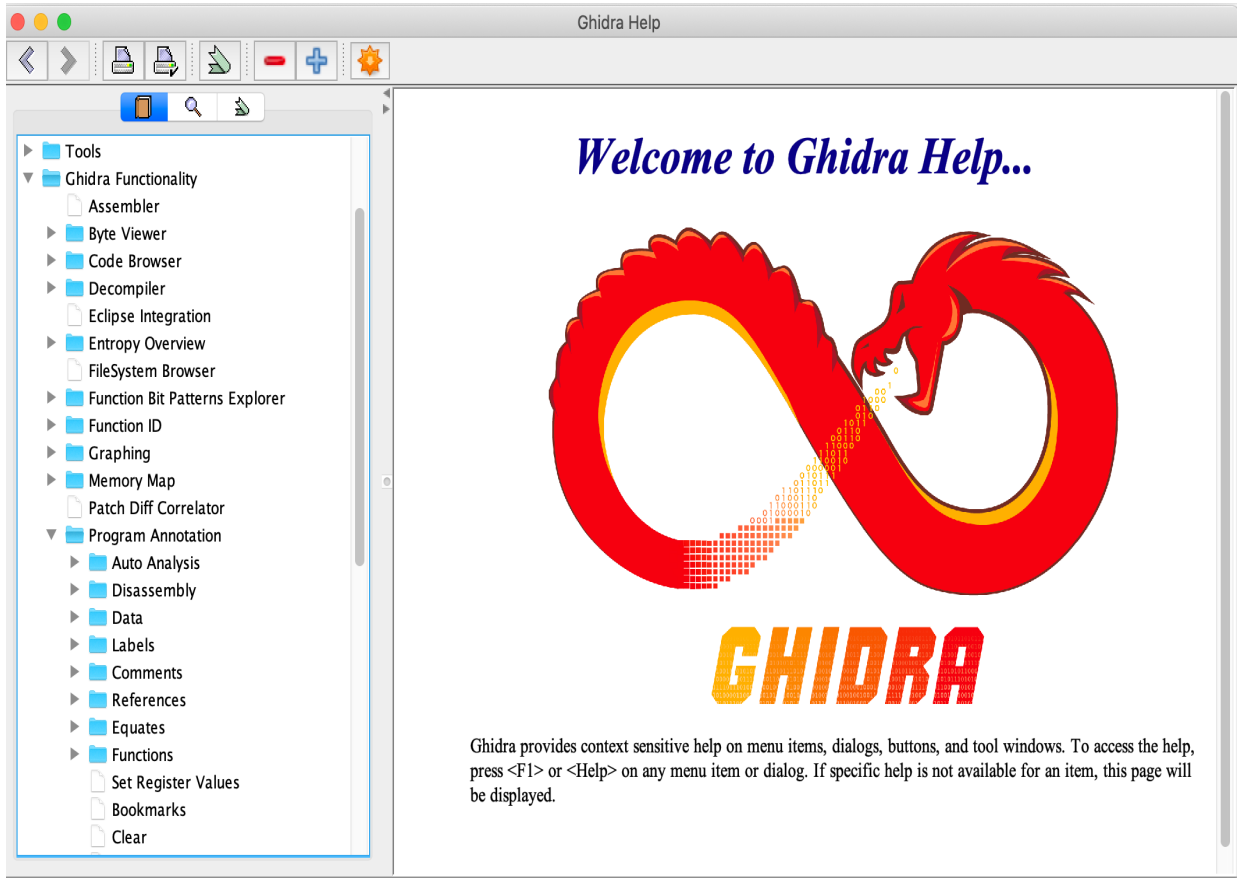
Ghidra Headless Mode Command Line Options

```
alnimari support >> ./analyzeHeadless --help
Java HotSpot(TM) 64-Bit Server VM warning: Archived non-system classes are disabled because the java.system.class.loader property is specified (value =
"ghidra.GhidraClassLoader"). To use archived non-system classes, this property must not be set
java version "13" 2019-09-17
Java(TM) SE Runtime Environment (build 13+33)
Java HotSpot(TM) 64-Bit Server VM (build 13+33, mixed mode, sharing)
Headless Analyzer Usage: analyzeHeadless
           <project_location> <project_name>[/<folder_path>]
             | ghidra://<server>[:<port>]/<repository_name>[/<folder_path>]
           [[-import [<directory>|<file>]+] | [-process [<project_file>]]]
           [-preScript <ScriptName>]
           [-postScript <ScriptName>]
           [-scriptPath "<path1>[;<path2>...]"]
           [-propertiesPath "<path1>[;<path2>...]"]
           [-scriptlog <path to script log file>]
           [-log <path to log file>]
           [-overwrite]
           [-recursive]
           [-readOnly]
           [-deleteProject]
           [-noanalysis]
           [-processor <languageID>]
           [-cspec <compilerSpecID>]
           [-analysisTimeoutPerFile <timeout in seconds>]
           [-keystore <KeystorePath>]
           [-connect <userID>]
           [-p]
           [-commit ["<comment>"]]
           [-okToDelete]
           [-max-cpu <max cpu cores to use>]
           [-loader <desired loader name>]

     - All uses of $GHIDRA_HOME or $USER_HOME in script path must be preceded by '\'

Please refer to 'analyzeHeadlessREADME.html' for detailed usage examples and notes.
```

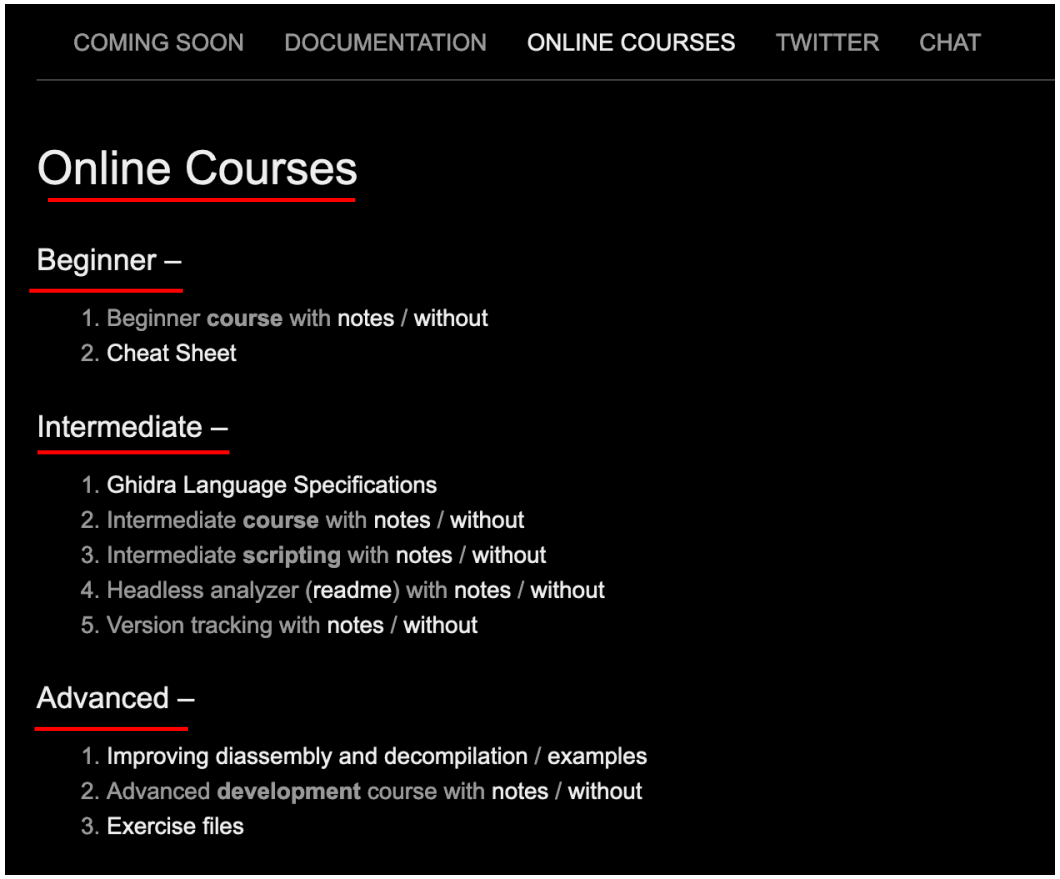
Ghidra Additional Features

- ✓ P-Code: (IR/IL) Don’t worry about CPU Architecture : x86, ARM, MIPS, SH4 ..
- ✓ Undo/Redo (up to 20 level)
- ✓ File System Support (zip, tar, tgz, dmg, apk ..)

Help, Documentation and Online Courses



Context Sesitive Help



https://ghidra.re/online-courses/

Demo

Fun Time

Q & A

Your Questions !?

End

سبحانك اللهم و بحمدك
أشهد أن لا إله إلا أنت
أستغفرك و أتوب إليك