



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)

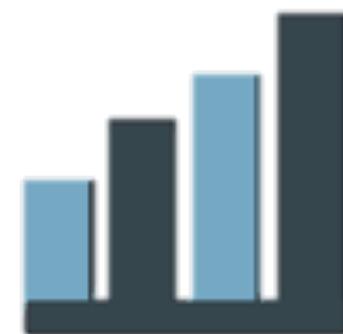
- ✓ 16145 stars

- ✓ 2019 forks

- ✓ 718 watching

- ✓ 608 issues, 272 open

- ✓ 111 pull requests, 35 open





Using Ghidra



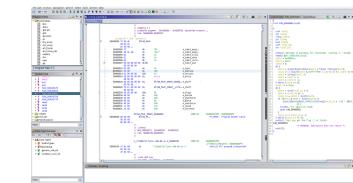
- ✓ Install OpenJDK 11
 - <https://jdk.java.net/11>
 - `export PATH=$PATH:/opt/java-jdk/bin`



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



- ✓ Enjoy



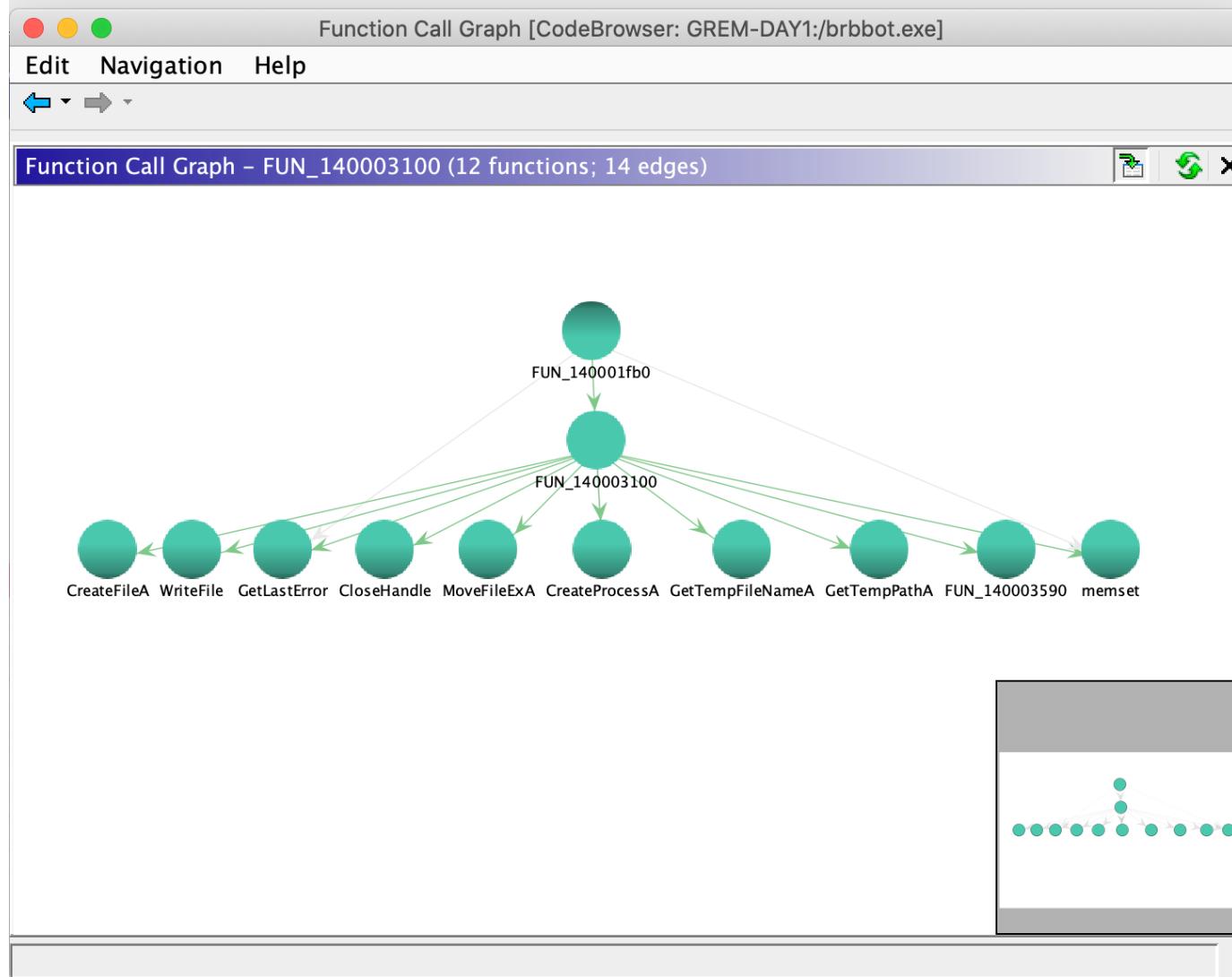


Ghidra Features - Listing Window (Disassembler)



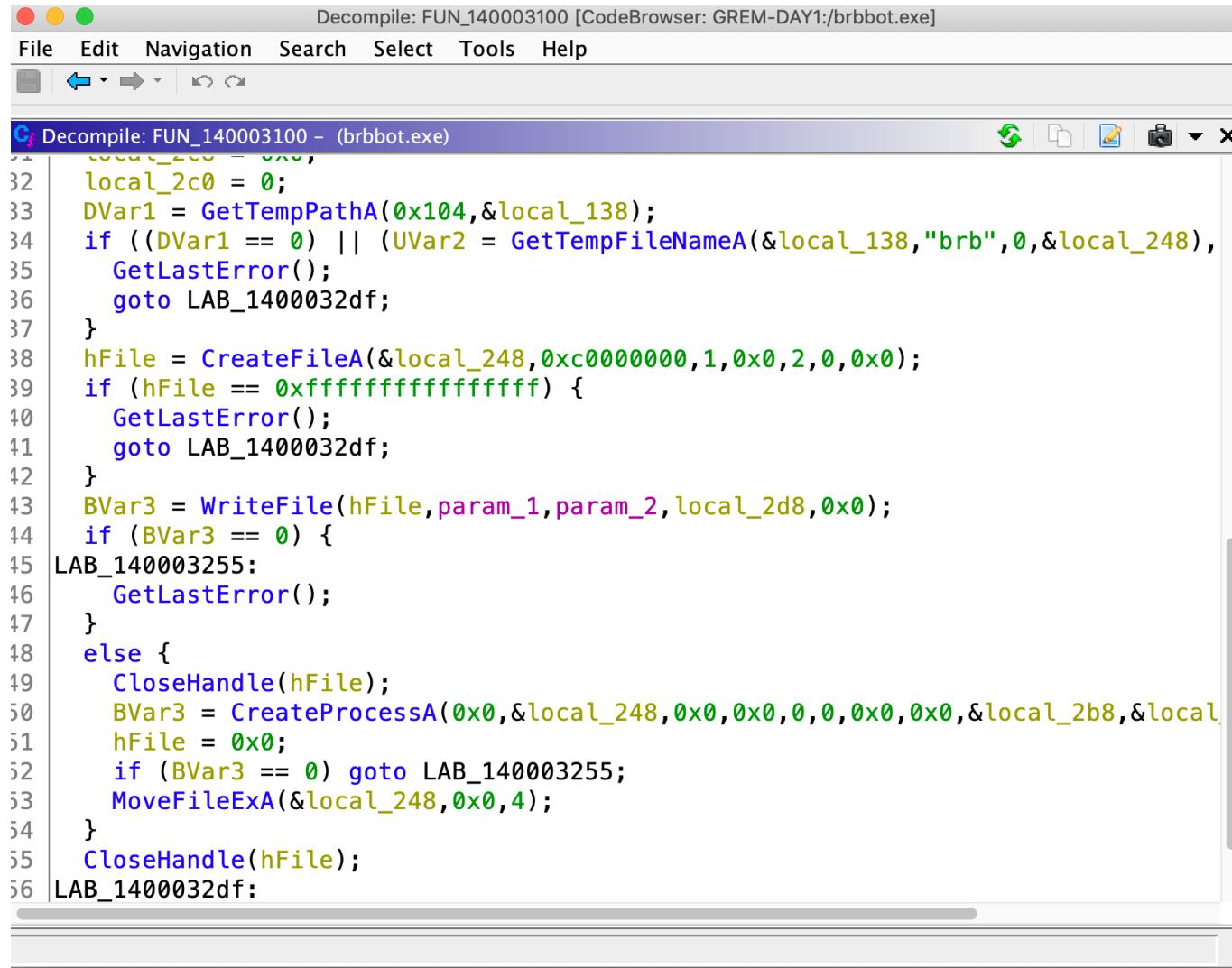


Ghidra Features - Function Call Graph





Ghidra Features - The Gold Feature: Decompiler



Decompile: FUN_140003100 [CodeBrowser: GREM-DAY1:/brbbot.exe]

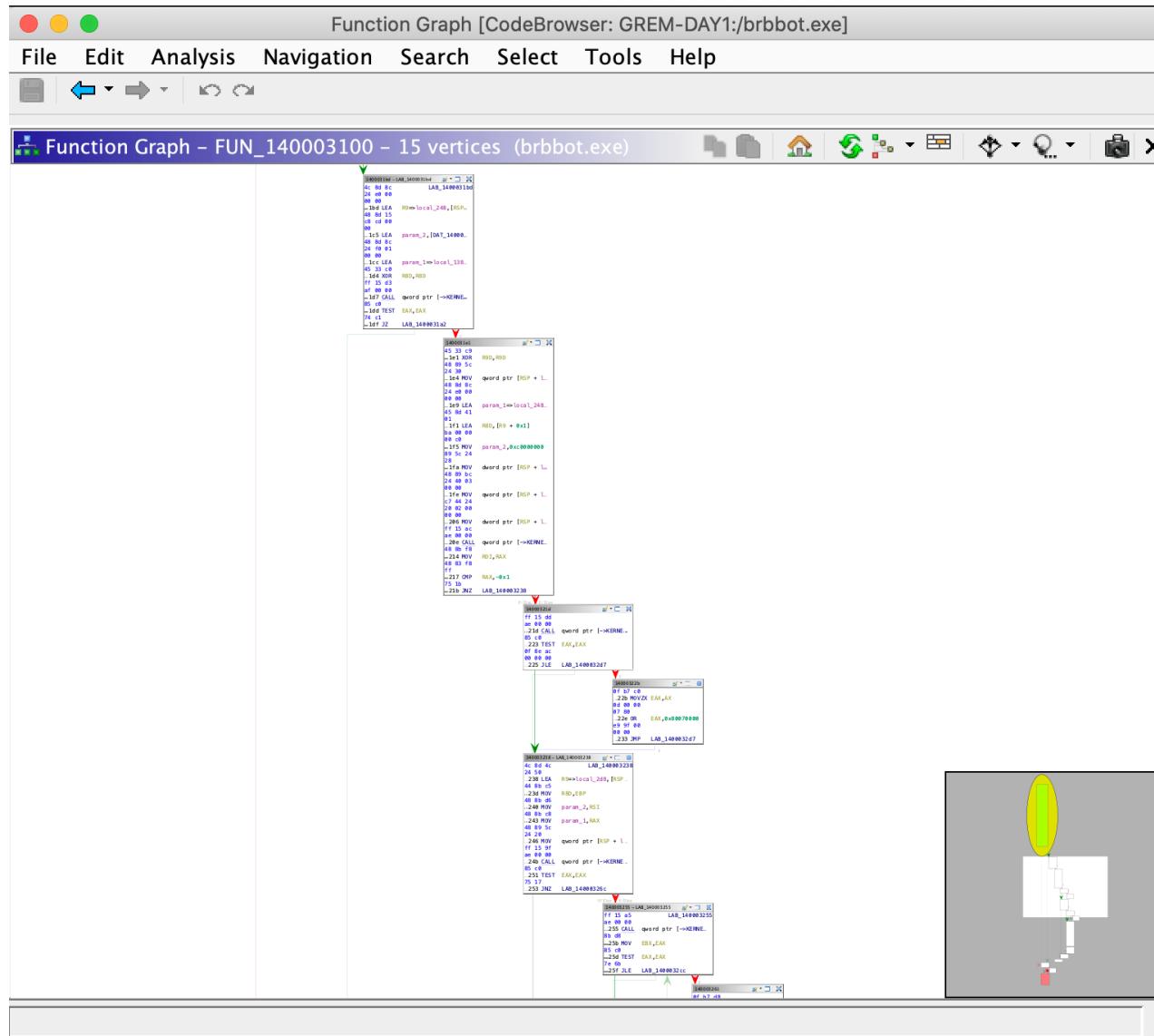
File Edit Navigation Search Select Tools Help

C: Decompile: FUN_140003100 - (brbbot.exe)

```
32 local_2c0 = 0;
33 DVar1 = GetTempPathA(0x104,&local_138);
34 if ((DVar1 == 0) || (UVar2 = GetTempFileNameA(&local_138,"brb",0,&local_248),
35     GetLastError());
36     goto LAB_1400032df;
37 }
38 hFile = CreateFileA(&local_248,0xc0000000,1,0x0,2,0,0x0);
39 if (hFile == 0xffffffffffff) {
40     GetLastError();
41     goto LAB_1400032df;
42 }
43 BVar3 = WriteFile(hFile,param_1,param_2,local_2d8,0x0);
44 if (BVar3 == 0) {
45 LAB_140003255:
46     GetLastError();
47 }
48 else {
49     CloseHandle(hFile);
50     BVar3 = CreateProcessA(0x0,&local_248,0x0,0x0,0,0,0x0,0x0,&local_2b8,&local
51     hFile = 0x0;
52     if (BVar3 == 0) goto LAB_140003255;
53     MoveFileExA(&local_248,0x0,4);
54 }
55 CloseHandle(hFile);
56 LAB_1400032df:
```



Ghidra Features - Function Graph





Ghidra Features - Synced Views



The screenshot displays the Ghidra interface with several windows open, illustrating its synchronized views feature.

- Listing: brbbot.exe - (8 addresses selected)**: Shows assembly code for the selected addresses. The assembly code is:

```
10003181 328 c7 44 24 70 68 00 MOV dword ptr [RSP + 00 00]
10003189 328 48 89 44 24 58 MOV qword ptr [RSP + 00 00]
1000318e 328 48 89 44 24 60 MOV qword ptr [RSP + 00 00]
10003193 328 48 89 44 24 68 MOV qword ptr [RSP + 00 00]
10003198 328 ff 15 1a b0 00 00 CALL qword ptr [->KEF]
1000319e 328 85 c0 TEST EAX,EAX
100031a0 328 75 1b JNZ LAB_1400031bd

LAB_1400031a2
100031a2 328 ff 15 58 af 00 00 CALL qword ptr [->KEF]
100031a8 328 85 c0 TEST EAX,EAX
100031aa 328 0f 8e 2f 01 00 00 JLE LAB_1400032df
100031b0 328 0f b7 c0 MOVZX EAX,AX
100031b3 328 0d 00 00 07 80 OR EAX,0x80070000
100031b8 328 e9 22 01 00 00 JMP LAB_1400032df

LAB_1400031bd
XREF[1]: 1
```
- Decompile: FUN_140003100 - (brbbot.exe)**: Shows the decompiled C-like code for the selected function. The code is:

```
21 local_28 = DAT_140012008 ^ &stack0xffffffff;
22 local_138 = '\0';
23 memset(local_137,0,0x103);
24 local_248 = '\0';
25 memset(local_247,0,0x103);
26 local_2d8[0] = 0;
27 memset(&local_2b8,0,0x68);
28 local_2b8.cb = 0x68;
29 local_2d0 = 0x0;
30 local_2c8 = 0x0;
31 local_2c0 = 0;
32 DVar1 = GetTempPathA(0x104,&local_138);
33 if ((DVar1 == 0) || (UVar2 = GetTempFileName(
34 GetLastErrorMessage();
35 goto LAB_1400032df;
36
37 hFile = CreateFileA(&local_248,0xc0000000,1,
38 if (hFile == 0xffffffff) {
```
- Function Graph - FUN_140003100 - 15 vertices (brbbot.exe)**: Shows the control flow graph for the function. The graph highlights the flow from the entry point to the selected assembly code and decompiled code windows.
- Defined Strings**, **Function Call Graph**, **Listing: brbbot.exe**, **Bytes: brbbot.exe**, **Decompile: FUN_140003100**, **Python**, **Function Call Trees: F...**, **Console**, and **Function Graph** tabs are visible at the bottom.



Ghidra Features - Bytes Window (Hex Editor)



Bytes: brbbot.exe [CodeBrowser: GREM-DAY1:/brbbot.exe]

File Edit Navigation Search Select Tools Help

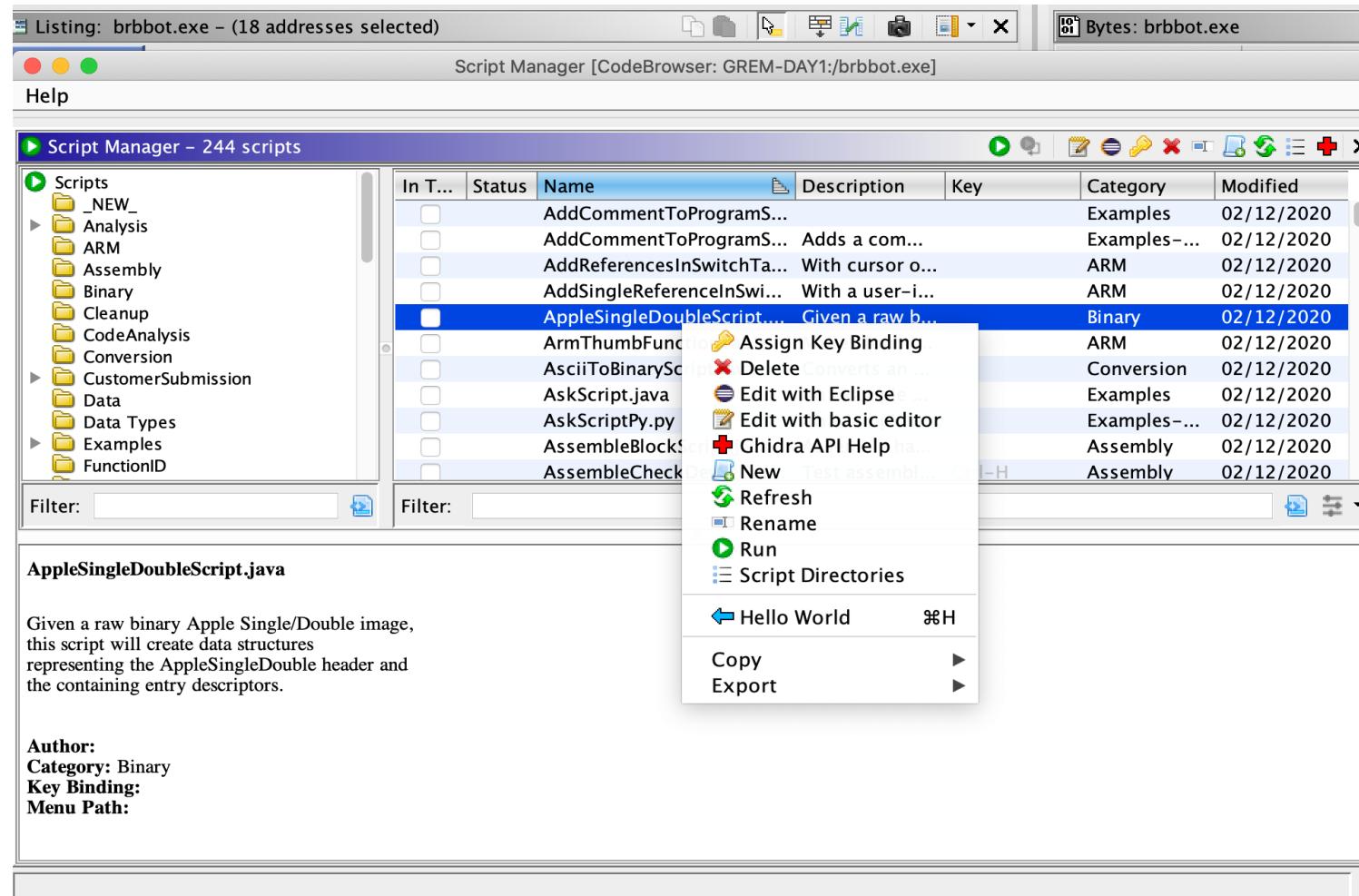
Bytes: brbbot.exe

Addresses	Hex	Ascii
140001030	c6 ba 08 00 00 00 48 8b c8 ff 15 99 d0 00 00 48H.....H
140001040	8b e8 48 85 c0 75 0a b8 0e 00 07 80 e9 d9 00 00	..H..u.....
140001050	00 4c 8b c6 49 8b d4 48 8b c8 e8 a1 7c 00 00 48	.L..I..H.... ..H
140001060	8b d3 48 8b cd e8 26 26 00 00 48 85 c0 0f 84 9c	..H...&&..H....
140001070	00 00 00 ba 3d 00 00 00 48 8b c8 e8 68 26 00 00=....H..h&..H
140001080	48 8b d8 48 85 c0 0f 84 83 00 00 00 48 03 f5 48	H..H.....H..H
140001090	3b c6 74 7b 48 ff c3 ba 3b 00 00 00 48 8b cb e8	;..t{H...;...H...
1400010a0	44 26 00 00 48 3b c6 74 6b 48 85 c0 74 03 c6 00	D&..H;.tkH..t...
1400010b0	00 48 83 c9 ff 33 c0 48 8b fb f2 ae 48 f7 d1 48	.H...3.H....H..H
1400010c0	8d 79 ff ff 15 1f d0 00 00 4c 8d 47 04 48 8b c8	.y.....L.G.H..
1400010d0	ba 08 00 00 00 ff 15 fd cf 00 00 48 8b f0 48 85H..H.
1400010e0	c0 75 07 bf 0e 00 07 80 eb 2a 48 83 c9 ff 33 c0	.u.....*H...3.
1400010f0	48 8b fb f2 ae 48 8b d3 48 f7 d1 4c 8d 41 ff 48	H....H..H..L.A.H
140001100	8b ce e8 19 26 00 00 49 89 75 00 33 ff eb 05 bf&..I.u.3....
140001110	57 00 07 80 ff 15 ce cf 00 00 4c 8b c5 33 d2 48	W.....L..3.H
140001120	8b c8 ff 15 b8 cf 00 00 8b c7 48 8b 5c 24 40 48H.\\$@H
140001130	8b 6c 24 48 48 8b 74 24 50 48 83 c4 20 41 5d 41	.l\$HH.t\$PH.. A]A
140001140	5c 5f c3 cc	\.....
140001150	40 53 57 48 83 ec 48 33 db 33 c9 89 5c 24 60 ff	@SWH..H3.3..\\$`.
140001160	15 ab cf 00 00 48 8b f8 48 85 c0 75 22 ff 15 8dH..H..u"...
140001170	cf 00 00 8b d8 85 c0 0f 8e 51 01 00 00 0f b7 d8Q.....
140001180	81 cb 00 00 07 80 8b c3 48 83 c4 48 5f 5b c3 4cH..H_[.L
140001190	8d 05 62 ec 00 00 ba 65 00 00 00 48 8b c8 48 89	..b....e....H..H.
1400011a0	74 24 70 ff 15 1f cf 00 00 48 8b f0 48 85 c0 74	t\$p.....H..H..t

Start: 1400000000 End: 1400183ff Offset: 00000000 Insertion: 14000107e



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

The screenshot shows the Ghidra interface for Version Tracking. At the top, a table titled "Version Tracking Matches" displays 586 matches between two sessions. The columns include Tag, Session, Status, Type, Score, Confidence, Votes, # C, Mu..., Source Name, Source Label, Source Address, Mu..., Dest Name, Dest Label, Dest Address, Sou..., Des..., and Algorithm. Below this is a "Version Tracking Functions" window comparing source and destination functions. The source functions are from "MyProjects:/VT-Test/WallaceSrc.exe" and the destination functions are from "MyProjects:/VT-Test/WallaceVersion2.exe". A message "A match already exists between FUN_004114b0 and FUN_004114a0." is shown. At the bottom, two decompiled code windows show the source code for "FUN_004114b0" and the destination code for "FUN_004114a0", with annotations and differences highlighted.

Tag	Ses...	Sta...	Type	Score	Confi...	Vot...	# C...	Mu...	Source N...	Source Label	Source ...	Mu...	Dest Na...	Dest Label	Dest A...	Sou...	Des...	Algorithm
8			Data	1.000	0.046	0	4			<No Symbol>	0041a...			<No Symbol>	0041a...	16	16	Duplicate Dat...
8			Data	1.000	0.046	0	4		Global	IMAGE_RESO...	0041a...		Global	IMAGE_RESO...	0041a...	16	16	Duplicate Dat...
8			Data	1.000	0.046	0	4			<No Symbol>	0041a...			<No Symbol>	0041a...	16	16	Duplicate Dat...
8			Data	1.000	0.046	0	4		Global	IMAGE_RESO...	0041a...			<No Symbol>	0041a...	16	16	Duplicate Dat...
8			Data	1.000	0.046	0	4		Global	IMAGE_RESO...	0041a...			<No Symbol>	0041a...	16	16	Duplicate Dat...
8			Data	1.000	0.046	0	4			<No Symbol>	0041a...			<No Symbol>	0041a...	16	16	Duplicate Dat...
8			Data	1.000	0.046	0	4			<No Symbol>	0041a...			<No Symbol>	0041a...	16	16	Duplicate Dat...
8			Data	1.000	0.046	0	4			<No Symbol>	0041a...			<No Symbol>	0041a...	16	16	Duplicate Dat...
8			Data	1.000	0.046	0	4			<No Symbol>	0041a...			<No Symbol>	0041a...	16	16	Duplicate Dat...

Filter: [] Score Filter: 0.000 to 1.000 Confidence Filter: -9.999 to 9.999 Length Filter: 0 []

Version Tracking Functions - [Session: VT-Session-1] - Source Functions - 56 functions / Destination Functions - 56...

Source = MyProjects:/VT-Test/WallaceSrc.exe

Label	Location	Function Signature
FUN_00411440	00411440	undefined4 * FUN_00411440(...)
FUN_004114b0	004114b0	undefined4 FUN_004114b0(u...
FUN_004114f0	004114f0	uint FUN_004114f0(uint pa...
FUN_00411530	00411530	undefined4 FUN_00411530(i...
FUN_00411570	00411570	... undefined4 FUN_00411570(...)

Destination = MyProjects:/VT-Test/WallaceVersion2.exe

Label	Location	Function Signature
FUN_00411430	00411430	undefined4 * FUN_00411430(...)
FUN_004114a0	004114a0	undefined4 FUN_004114a0(...)
FUN_004114e0	004114e0	uint FUN_004114e0(uint p...
FUN_00411520	00411520	undefined4 FUN_00411520(...)
FUN_00411560	00411560	... undefined4 FUN_00411560(...)

Filter: []

A match already exists between FUN_004114b0 and FUN_004114a0.

Decompile View Listing View

Source: FUN_004114b0 [/VT-Test/WallaceSrc.exe]

```
1
2 undefined4 __fastcall FUN_004114b0(undefined4 *param_1)
3
4 {
5     int iVar1;
6     undefined4 *puVar2;
7     undefined4 local_d0 [51];
8 }
```

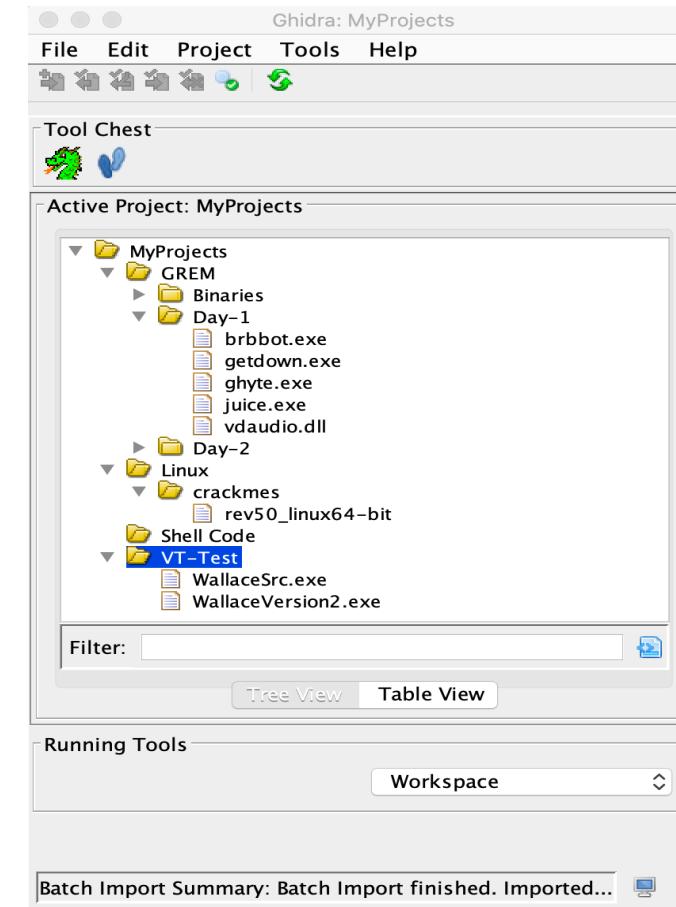
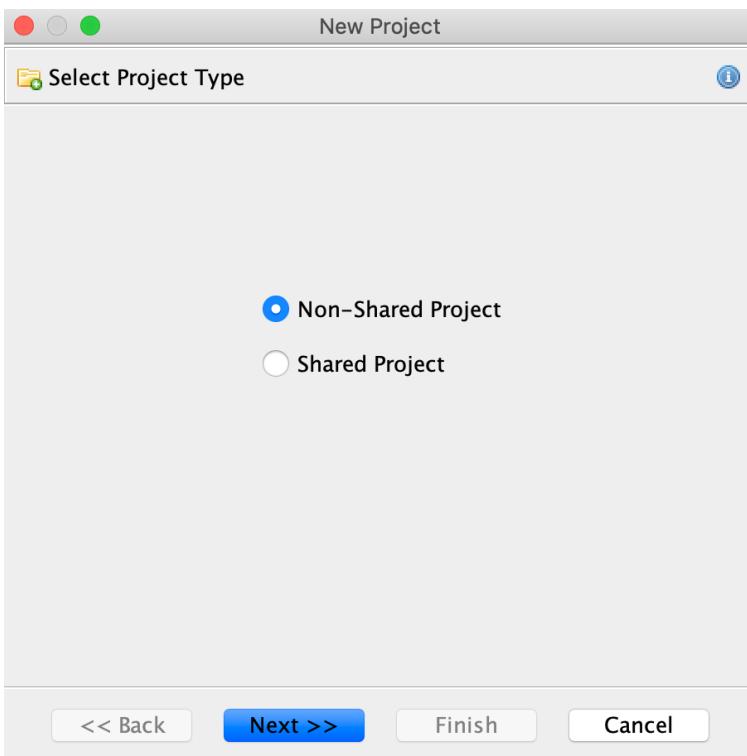
Destination: FUN_004114a0 [/VT-Test/WallaceVersion2.exe]

```
1
2 undefined4 __fastcall FUN_004114a0(undefined4 *param_1)
3
4 {
5     int iVar1;
6     undefined4 *puVar2;
7     undefined4 local_d0 [51];
8 }
```

Version Tracking Markup... Version Tracking Impli... Version Tracking Funct...



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



```
[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 '\'

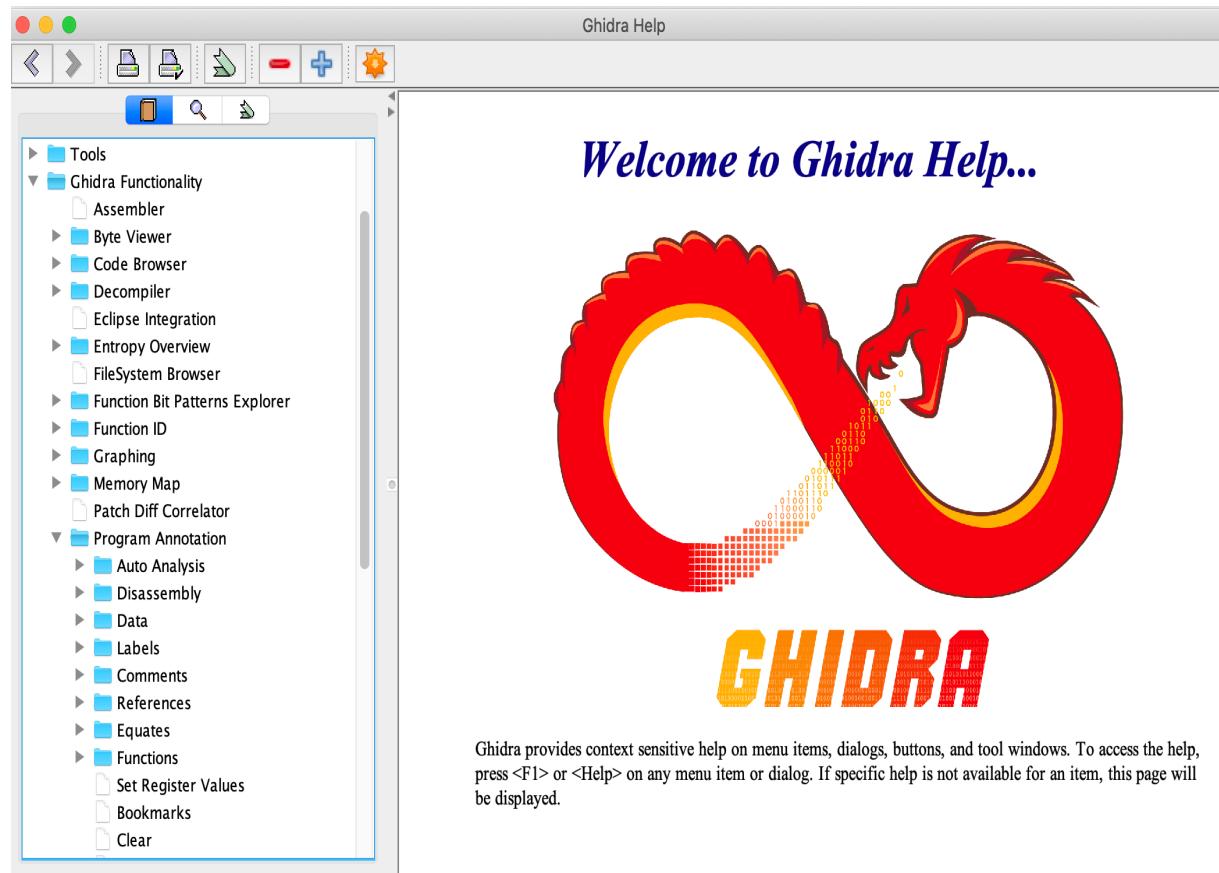
Please refer to 'analyzeHeadlessREADME.html' for detailed usage examples and notes.
```



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 ..)**



Context Sensitive Help

COMING SOON DOCUMENTATION ONLINE COURSES TWITTER CHAT

Online Courses

Beginner –

1. Beginner **course** with notes / without
2. Cheat Sheet

Intermediate –

1. Ghidra Language Specifications
2. Intermediate **course** with notes / without
3. Intermediate **scripting** with notes / without
4. Headless analyzer (readme) with notes / without
5. Version tracking with notes / without

Advanced –

1. Improving disassembly and decompilation / examples
2. Advanced **development** course with notes / without
3. Exercise files

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

Fun Time



Your Questions !?



سُبْحَانَكَ اللَّهُمَّ وَ بِحَمْدِكَ
أَشْهُدُ أَنْ لَا إِلَهَ إِلَّا أَنْتَ
أَسْتَغْفِرُكَ وَ أَتُوْبُ إِلَيْكَ