



USA 2019

AUGUST 3-8, 2019

MANDALAY BAY / LAS VEGAS



GHIDRA

Software Reverse Engineering (SRE) Framework

Journey from Classified NSA Tool to Open Source

BRIAN KNIGHTON

- RESEARCHER
- GHIDRA DEVELOPER
- IoT VULNERABILITY RESEARCH

CHRIS DELIKAT

- RESEARCHER
- CYBER TEAM LEAD

- ABOUT NSA
- ABOUT GHIDRA
- BACKGROUND
- FEATURES
- FRAMEWORK
- OPEN SOURCE
- NEW FEATURES
- METRICS

- (S)RE - (Software) Reverse Engineering
- VR - Vulnerability Research
- Cyber - Cybersecurity
- CNO - Computer Network Operations
- IC - Intelligence Community
- U, Unclass - Unclassified
- NSA/Mission





GHIDRA is NSA's SRE Framework

In development for ~20 years

Public Release: March 2019 at RSA Conference

Open Source: April 2019

Created as a platform to solve hard cybersecurity problems

What's in your binary?

Needed SRE tool with:

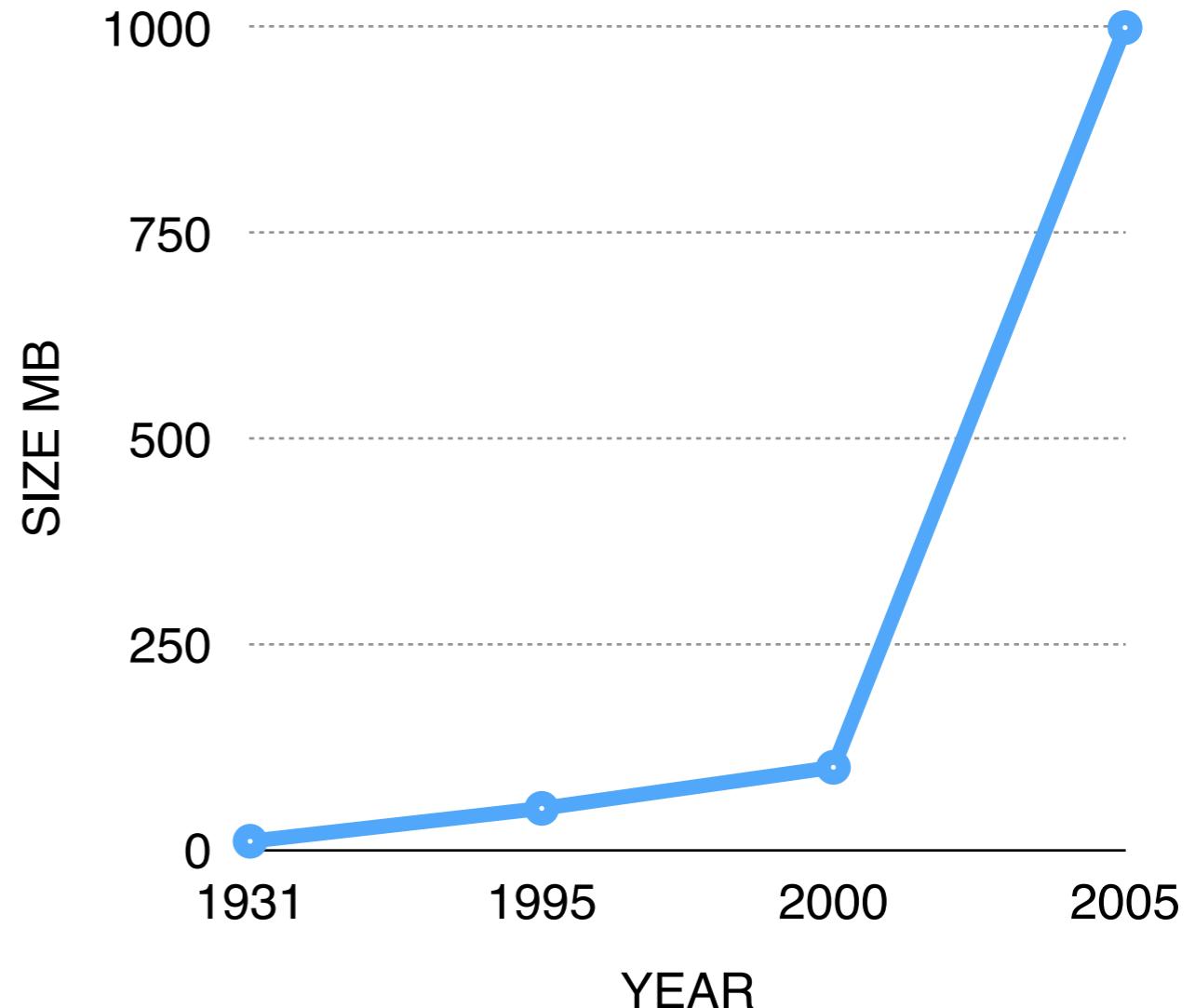
1. Scaling
2. Teaming
3. Extendability
4. Integration
5. Workflow
6. Undo/Redo
7. Headless, automated



BACKGROUND

Why?

- Software everywhere
 - Growing in size
- IoT Event Horizon
- Early IoT devices
 - PDA
 - Smart(ish) phones





G
H
I
D
R
A





GENERIC
HEXIDECIMAL
INTEGRATE
DECOMPILING
REVERSE-ENGINEERING
ARCHITECTURE

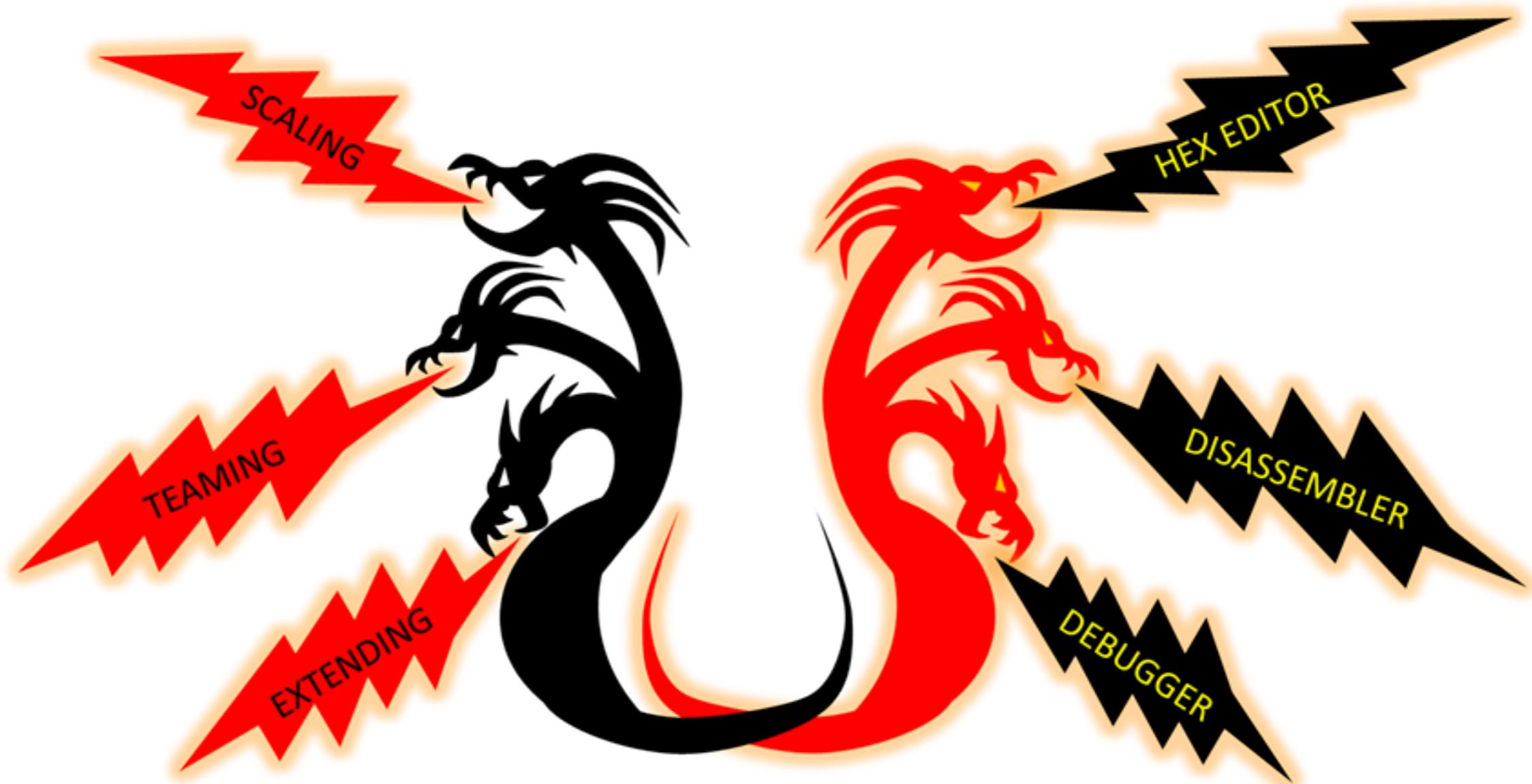




GENERIC
HEXIDECIMAL
INTEGRATED
DECOMPILING
REVERSE-ENGINEERING
Architecture

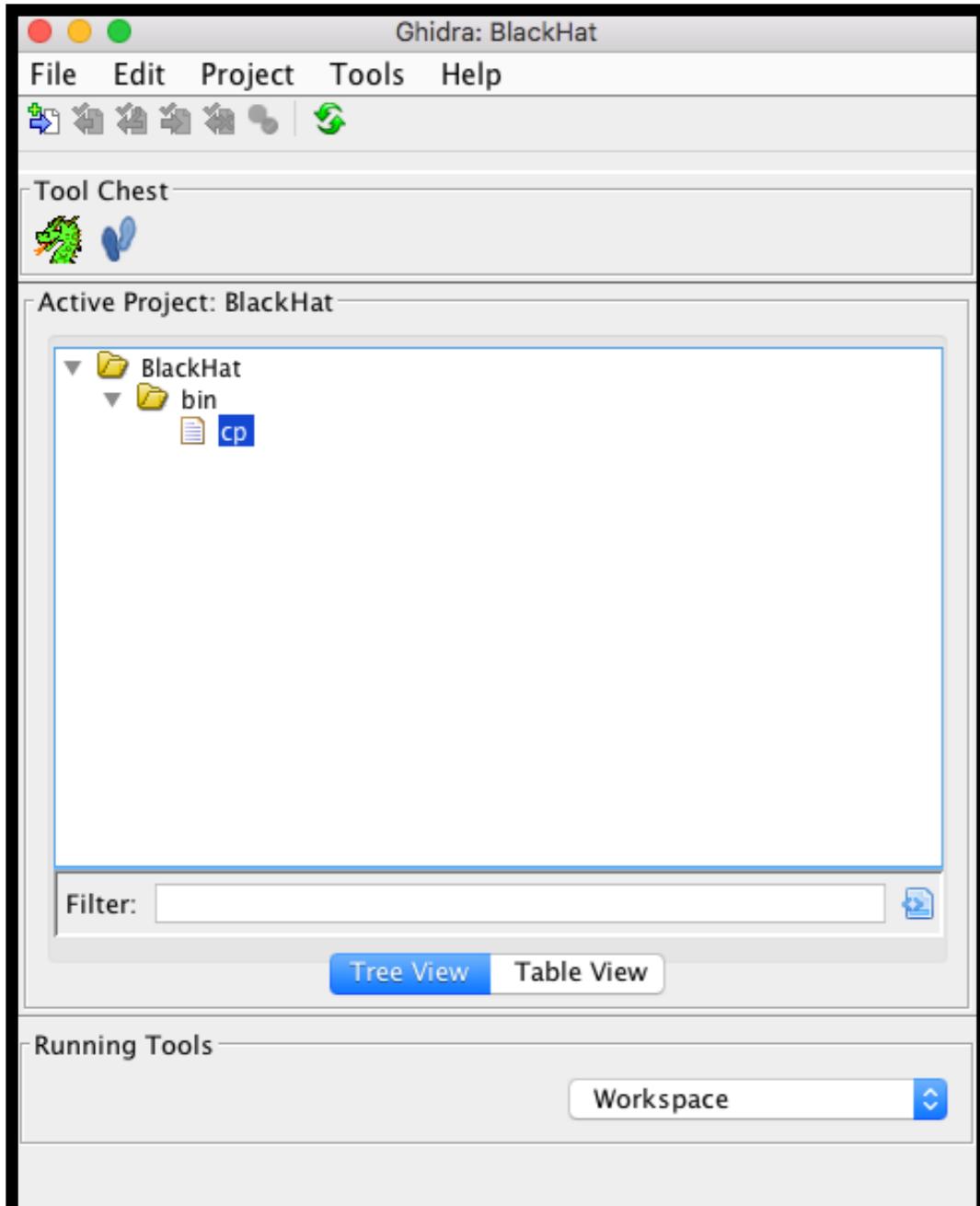


THE GHIDRA NAME



FEATURES

QUICK OVERVIEW OF MAJOR FEATURES



- Project Window
- aka Front End
- GHIDRA is project based

FEATURES

Listing: cp

* undefined FUNCTION
 undefined undefined [FUN_100001a1a\(\)](#)
 AL:1 <RETURN>
[FUN_100001a1a](#) XREF [3]:

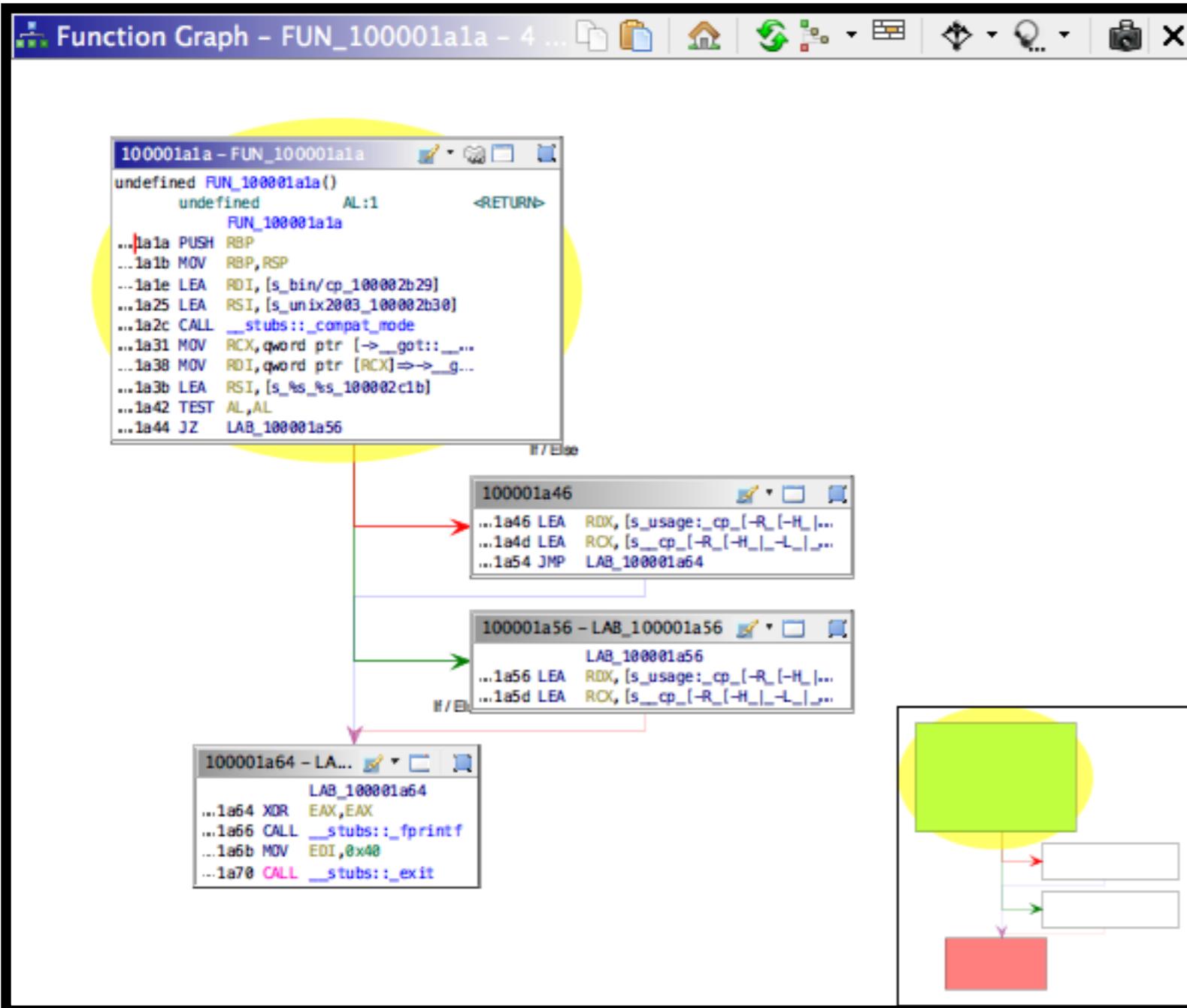
```

100001a1a 55      PUSH    RBP
100001a1b 48 89 e5 MOV     RBP,RSP
100001a1e 48 8d 3d LEA     RDI,[s_bin/cp_100002b29]
  04 11 00 00
100001a25 48 8d 35 LEA     RSI,[s_unix2003_100002b30]
  04 11 00 00
100001a2c e8 7b 0c CALL   __stubs::__compat_mode
  00 00
100001a31 48 8b 0d MOV    RCX,qword ptr [->__got::__stderrp]
  e0 15 00 00
100001a38 48 8b 39 MOV    RDI,qword ptr [RCX]=>->__got::__stderrp
100001a3b 48 8d 35 LEA     RSI,[s_%s_%s_100002c1b]
  d9 11 00 00
100001a42 84 c0 TEST   AL,AL
100001a44 74 10 JZ    LAB_100001a56
100001a46 48 8d 15 LEA     RDX,[s_usage:_cp_[ -R_[ -H_|_L_|_-P ] ]_[-10000:
  d5 11 00 00
100001a4d 48 8d 0d LEA     RCX,[s_cp_[ -R_[ -H_|_L_|_-P ] ]_[-fi_|_-10000:
  18 12 00 00
100001a54 eb 0e JMP   LAB_100001a54

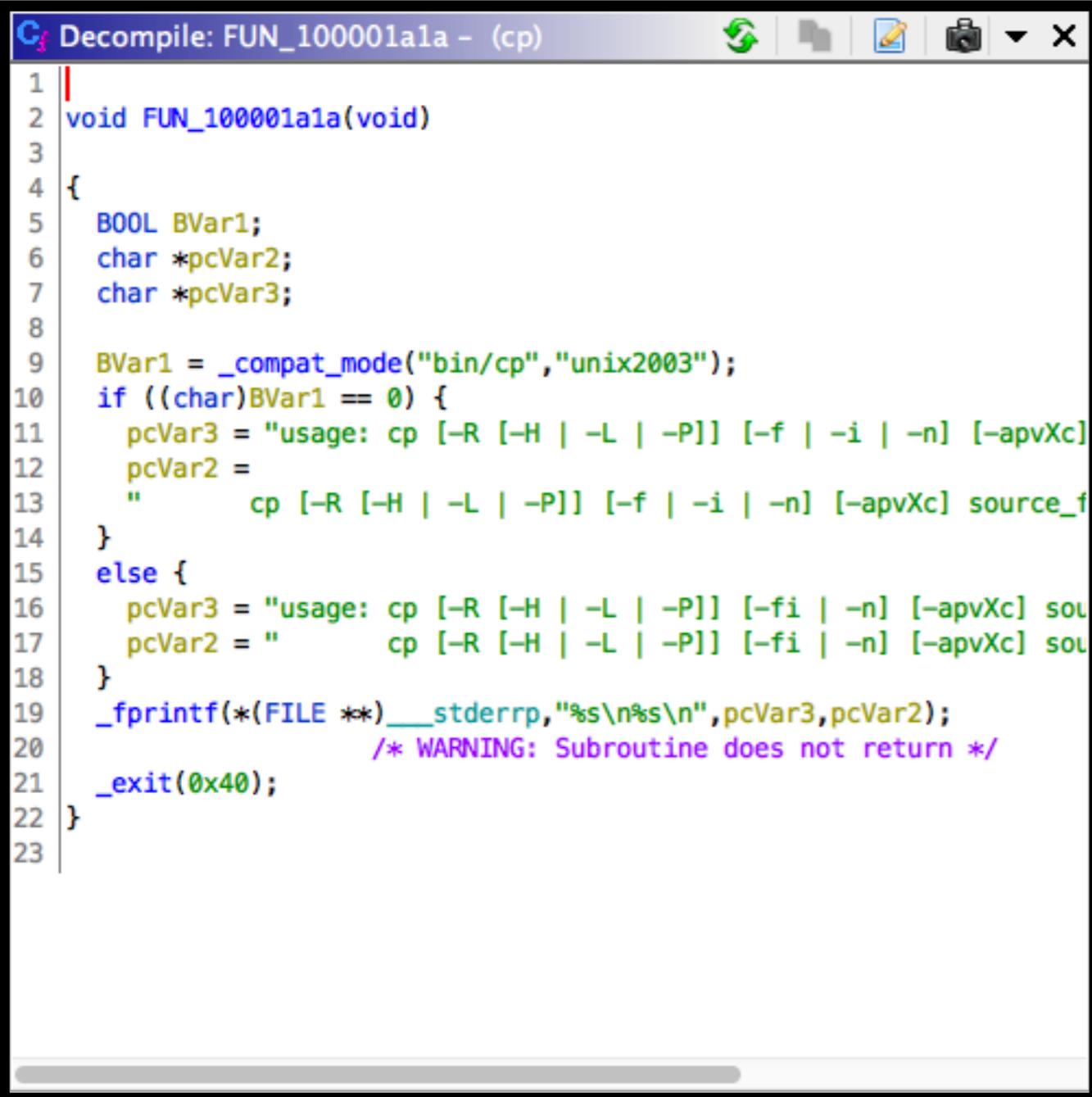
```

- Listing View
- Annotations
- Instructions
- Data
- Comments

FEATURES



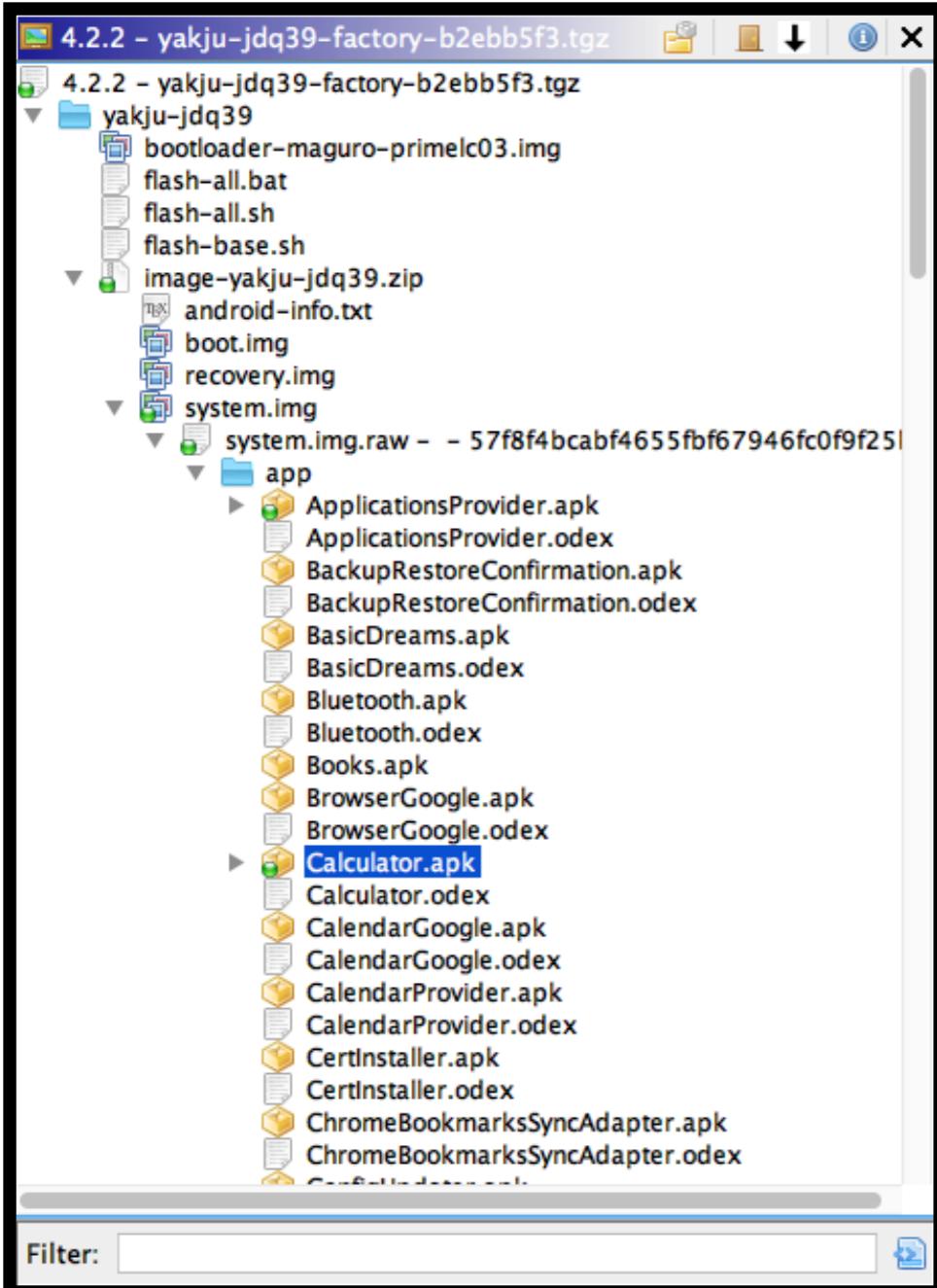
- Function Graph
- Displays functions as code blocks.



C & Decompile: FUN_100001a1a - (cp)

```
1
2 void FUN_100001a1a(void)
3 {
4     BOOL BVar1;
5     char *pcVar2;
6     char *pcVar3;
7
8     BVar1 = _compat_mode("bin/cp","unix2003");
9     if ((char)BVar1 == 0) {
10         pcVar3 = "usage: cp [-R [-H | -L | -P]] [-f | -i | -n] [-apvXc]"
11         pcVar2 =
12             "           cp [-R [-H | -L | -P]] [-f | -i | -n] [-apvXc] source_f"
13     }
14     else {
15         pcVar3 = "usage: cp [-R [-H | -L | -P]] [-fi | -n] [-apvXc] sou"
16         pcVar2 = "           cp [-R [-H | -L | -P]] [-fi | -n] [-apvXc] sou"
17     }
18     _fprintf(*(_FILE **)_stderrp,"%s\n%s\n",pcVar3,pcVar2);
19             /* WARNING: Subroutine does not return */
20     _exit(0x40);
21 }
22
23
```

- Decompiler
- Sleigh
- Works for all processors with Sleigh spec



- File System Browser
- Allows drilling down into firmware bundles
- Many formats supported
- tar, zip, etc

Script Manager - 43 scripts (of 238)

In T...	Status	Name	Description	Key	Category	Modified
		external_module_callee.py	Example of being imported by a G...		Examples-...	02/28/2019
		external_module_caller.py	Example of importing an external ...		Examples-...	02/28/2019
		FindChangedFunctionsScript.java	An example of how to use Version...		Examples-...	02/28/2019
		FindDataTypeScript.java	Shows how to find data types by n...		Examples	02/28/2019
		FormatExampleScript.java	An example using the printf()		Examples	02/28/2019
		FormatExampleScriptPy.py	An example using the Python strin...		Examples-...	02/28/2019
		GetAndSetAnalysisOptionsScript.j...	Shows examples of how to get, se...		Examples	02/28/2019
		ghidra_basics.py	Examples of basic Ghidra scriptin...		Examples-...	02/28/2019
		HelloWorldPopupScript.java	Writes "Hello World" in a popup di...		Examples	02/28/2019
		HelloWorldScript.java	Writes "Hello World" to console. Ctrl-Shif...		Examples	02/28/2019
		InnerClassScript.java	A script that uses inner classes.		Examples-...	02/28/2019
		jython_basics.py	Examples of Jython-specific funct...		Examples-...	02/28/2019
		MakeFuncsAtLabelsScript.java	Calculates the percentage of inst...		Examples	02/28/2019
		OpenVersionTrackingSessionScript...	An example of how to open an exi...		Examples-...	02/28/2019
		OverrideFunctionPrototypesOnAcc...	An example of how to use an exist...		Examples-...	02/28/2019
		PrintStructureScript.java	An example script that shows a fe...		Examples	02/28/2019
		ProgressExampleScript.java	Shows how to report progress to t...		Examples	02/28/2019
		python_basics.py	Examples of basic Python		Examples-...	02/28/2019
		RenameProgramsInProjectScript.java	Shows how to perform an operatio...		Examples	02/28/2019
		ReportDisassemblyErrors.java	Reports the the number of disasse...		Examples	02/28/2019

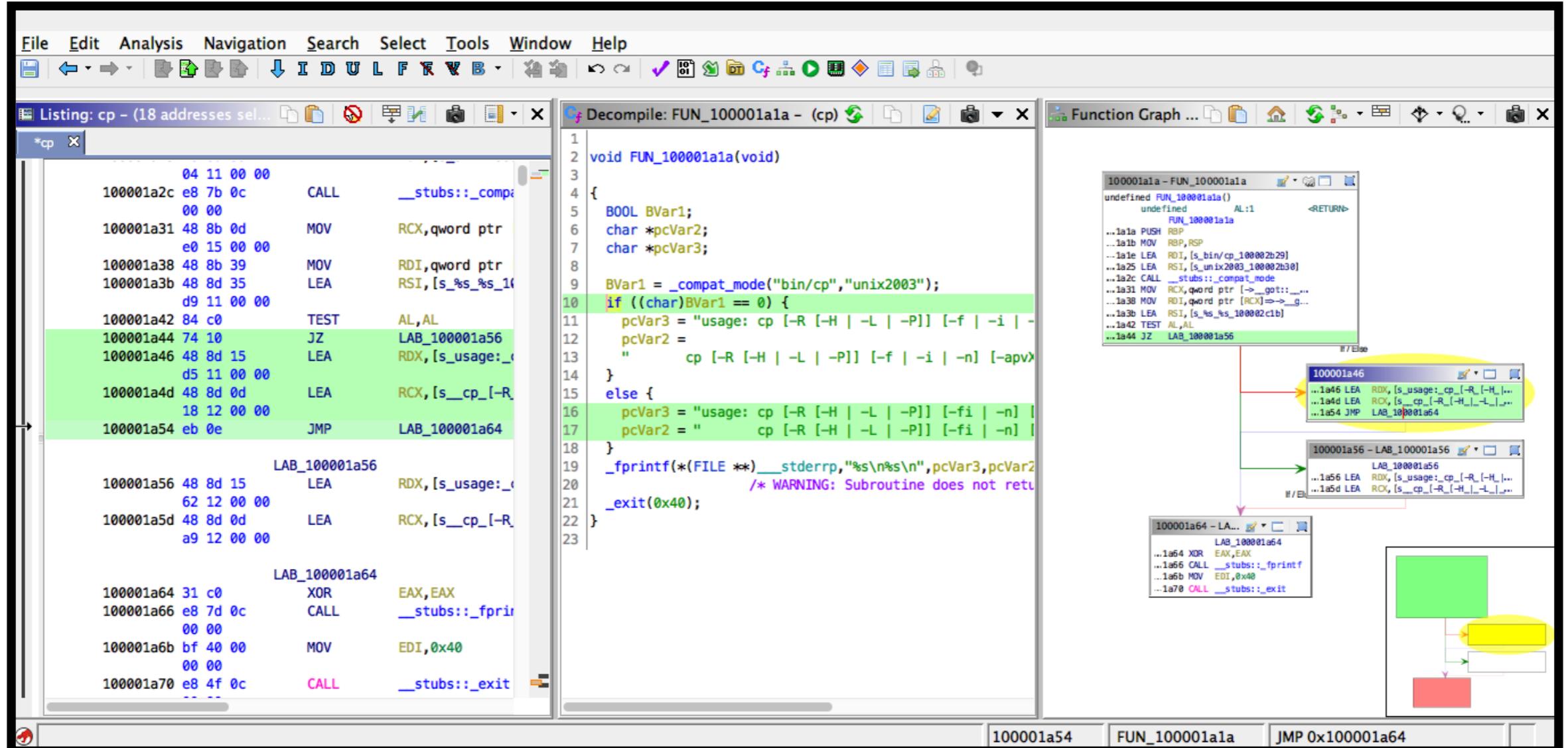
Filter: Filter:

HelloWorldScript.java

Writes "Hello World" to console.

Author:
Graham Cluley

- Script Manager
- Supports:
- Java
- Python



- All windows track selection and location changes

- Assembler
- Bookmarks
- Byte Viewer (Hex Editor)
- Data Type Manager
- Entropy
- Navigation
- Searching (bytes, strings, comments)
- Version Tracking
- Version Control (Multi-user)
- And more!

CODE BASE

QUICK OVERVIEW OF CODE BASE AND FRAMEWORK

Main Components

1. FRAMEWORK

- Generic GUI and Storage

2. FEATURES

- SRE Focused Plugins and Scripts

3. PROCESSORS

- Definitions of architectures and platforms
- Disassembler and Decompiler

Implementation of Design Requirements

Main Components

1. FRAMEWORK

- Generic GUI and Storage
- ### 2. FEATURES
- SRE Focused Plugins and Scripts
- ### 3. PROCESSORS
- Definitions of architectures and platforms
 - Disassembler and Decompiler

Let's dig into the Framework

Implementation of Design Requirements

Main Components:

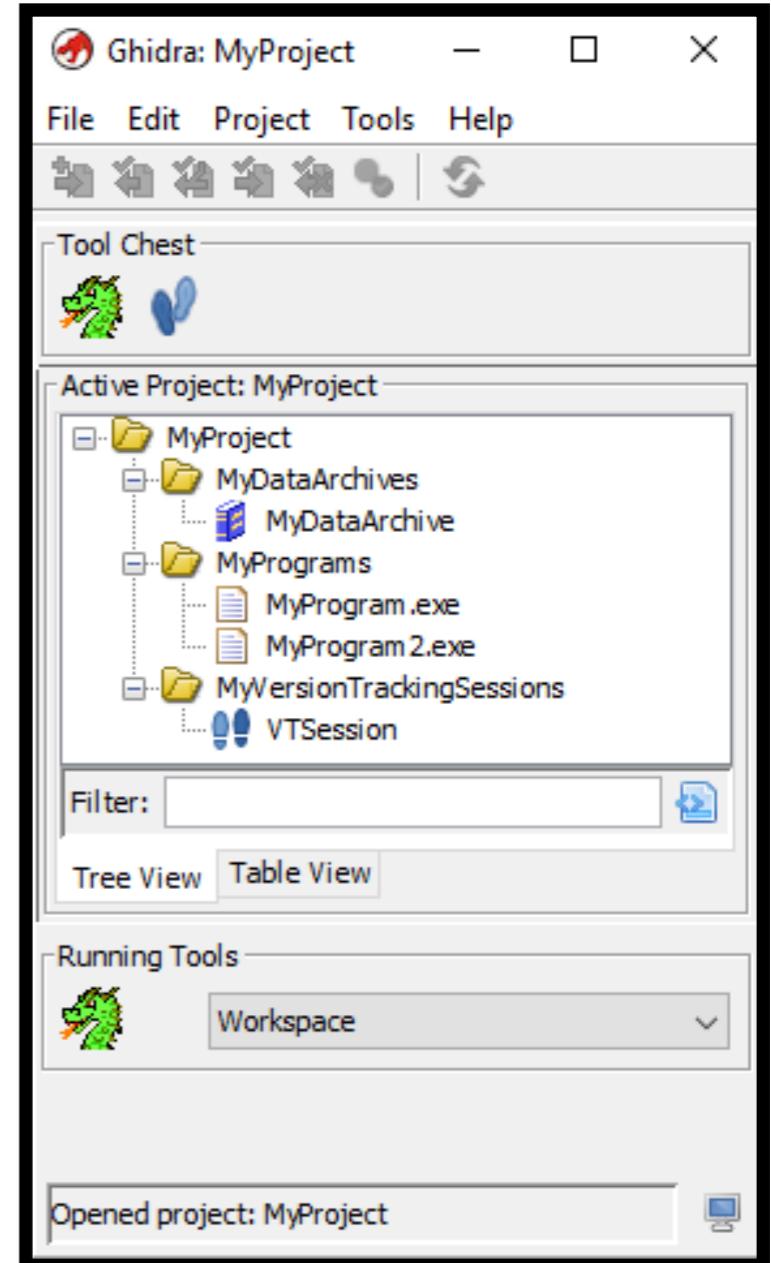
1. DB
2. Model
3. Software Modeling
4. Plugins
5. Docking Windows

1. DB

- Custom database to hold Domain Object data
- Tables, Rows, Cols
- Defined in package
 - db.*
- Created to support
 - Undo/Redo
 - Version Control (Multi-User)

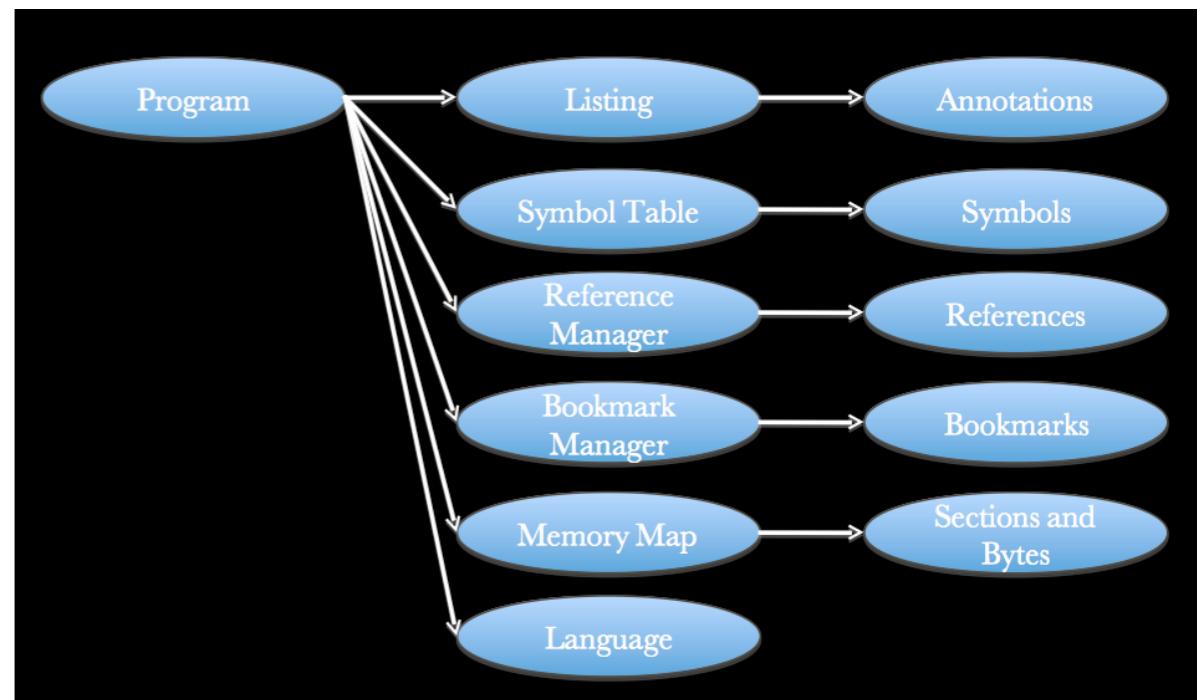
2. MODEL

- Data stored within the project
- Project
 - Domain Folder
 - Domain File
 - Domain Object
 - Implementations supported:
 - Program
 - Data Type Archive
 - Version Tracking Session



3. SOFTWARE MODELING

- Classes to represent a Program
- Program
 - Memory
 - Memory Blocks, Bytes
 - Symbol Table
 - Symbols
 - Listing
 - Instructions, Data
 - Bookmark Manager
 - Bookmarks



4. PLUGINS

- Extends “Plugin” base class
- Produces and Consumes
 - Events (PluginEvent)
 - Selections, Locations
 - Services
 - Goto, Program Manager
- Creates
 - Menu and button actions
 - GUI components

5. DOCKING WINDOWS

- Customized Java GUI components
 - GTree, GTable
- Improved TableModel and TreeModel
 - Generic Threaded Loading, Sorting, Filtering
- Uniform Look-and-Feel
- Overcome Java Swing limitations, issues, and general wonkiness

GTREE and GTABLE

Script Manager - 43 scripts (of 238)

In T...	Status	Name	Description	Key	Category	Modified
<input type="checkbox"/>		external_module_callee.py	Example of being imported by a G...		Examples...	02/28/2019
<input type="checkbox"/>		external_module_caller.py	Example of importing an external ...		Examples...	02/28/2019
<input type="checkbox"/>		FindChangedFunctionsScript.java	An example of how to use Version...		Examples...	02/28/2019
<input type="checkbox"/>		FindDataTypeScript.java	Shows how to find data types by n...		Examples	02/28/2019
<input type="checkbox"/>		FormatExampleScript.java	An example using the <code>printf()</code>		Examples	02/28/2019
<input type="checkbox"/>		FormatExampleScriptPy.py	An example using the Python strin...		Examples...	02/28/2019
<input type="checkbox"/>		GetAndSetAnalysisOptionsScript.j...	Shows examples of how to get, se...		Examples	02/28/2019
<input type="checkbox"/>		ghidra_basics.py	Examples of basic Ghidra scriptin...		Examples...	02/28/2019
<input type="checkbox"/>		HelloWorldPopupScript.java	Writes "Hello World" in a popup di...		Examples	02/28/2019
<input type="checkbox"/>		HelloWorldScript.java	Writes "Hello World" to console.	Ctrl-Shif...	Examples	02/28/2019
<input type="checkbox"/>		InnerClassScript.java	A script that uses inner classes.		Examples...	02/28/2019
<input type="checkbox"/>		jython_basics.py	Examples of Jython-specific funct...		Examples...	02/28/2019
<input type="checkbox"/>		MakeFuncsAtLabelsScript.java	Calculates the percentage of inst...		Examples	02/28/2019
<input type="checkbox"/>		OpenVersionTrackingSessionScript...	An example of how to open an exi...		Examples...	02/28/2019
<input type="checkbox"/>		OverrideFunctionPrototypesOnAcc...	An example of how to use an existi...		Examples...	02/28/2019
<input type="checkbox"/>		PrintStructureScript.java	An example script that shows a fe...		Examples	02/28/2019
<input type="checkbox"/>		ProgressExampleScript.java	Shows how to report progress to t...		Examples	02/28/2019
<input type="checkbox"/>		python_basics.py	Examples of basic Python		Examples...	02/28/2019
<input type="checkbox"/>		RenameProgramsInProjectScript.java	Shows how to perform an operatio...		Examples	02/28/2019
<input type="checkbox"/>		ReportDisassemblyErrors.java	Reports the the number of disasse...		Examples	02/28/2019

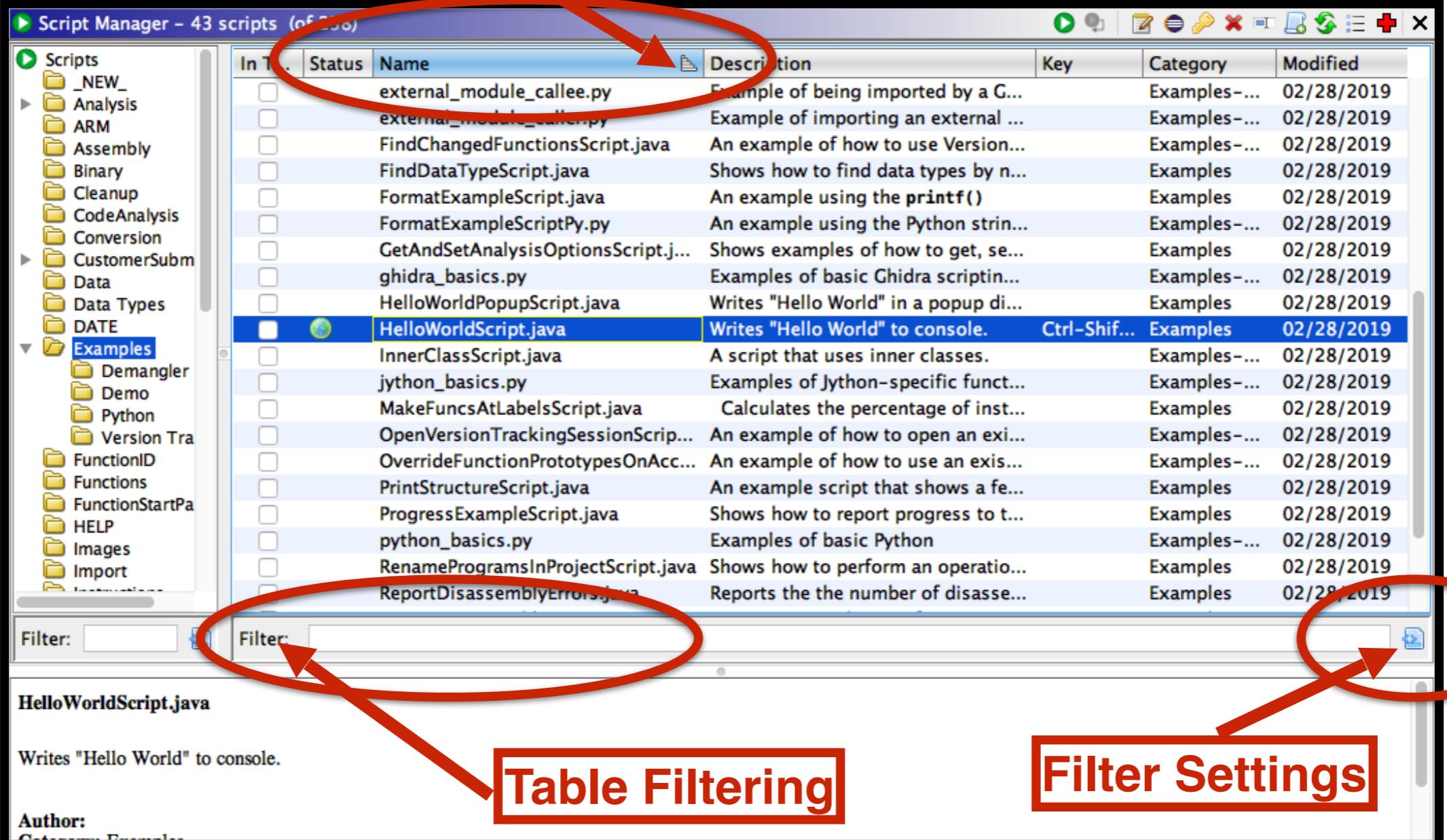
HelloWorldScript.java

Writes "Hello World" to console.

Author:
Ghidra Team

GTREE and GTABLE

Column Sorting



The screenshot shows the Script Manager interface with the title "Script Manager - 43 scripts (of 258)". On the left is a tree view of script categories. The main area is a table with columns: In Tr., Status, Name, Description, Key, Category, and Modified. A red arrow points from the "Name" header to the "Name" column. The "HelloWorldScript.java" row is selected. Red ovals highlight the "Filter:" input fields at the bottom left and right, and a red arrow points from the "Filter Settings" button at the bottom right to the rightmost "Filter:" field.

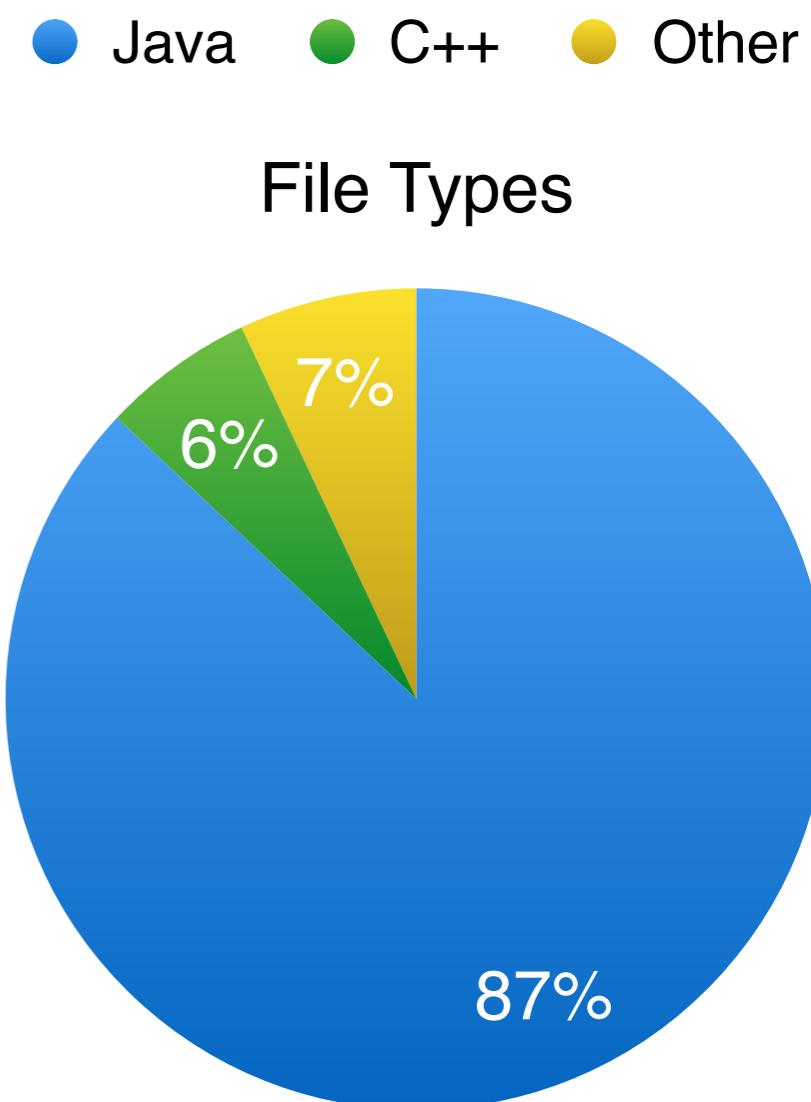
In Tr.	Status	Name	Description	Key	Category	Modified
		external_module_callee.py	Example of being imported by a G...		Examples...	02/28/2019
		external_module_caller.py	Example of importing an external ...		Examples...	02/28/2019
		FindChangedFunctionsScript.java	An example of how to use Version...		Examples...	02/28/2019
		FindDataTypeScript.java	Shows how to find data types by n...		Examples	02/28/2019
		FormatExampleScript.java	An example using the printf()		Examples	02/28/2019
		FormatExampleScriptPy.py	An example using the Python strin...		Examples...	02/28/2019
		GetAndSetAnalysisOptionsScript.j...	Shows examples of how to get, se...		Examples	02/28/2019
		ghidra_basics.py	Examples of basic Ghidra scriptin...		Examples...	02/28/2019
		HelloWorldPopupScript.java	Writes "Hello World" in a popup di...		Examples	02/28/2019
		HelloWorldScript.java	Writes "Hello World" to console. Ctrl-Shif...		Examples	02/28/2019
		InnerClassScript.java	A script that uses inner classes.		Examples...	02/28/2019
		jython_basics.py	Examples of Jython-specific funct...		Examples...	02/28/2019
		MakeFuncsAtLabelsScript.java	Calculates the percentage of inst...		Examples	02/28/2019
		OpenVersionTrackingSessionScript...	An example of how to open an exi...		Examples...	02/28/2019
		OverrideFunctionPrototypesOnAcc...	An example of how to use an exist...		Examples...	02/28/2019
		PrintStructureScript.java	An example script that shows a fe...		Examples	02/28/2019
		ProgressExampleScript.java	Shows how to report progress to t...		Examples	02/28/2019
		python_basics.py	Examples of basic Python		Examples...	02/28/2019
		RenameProgramsInProjectScript.java	Shows how to perform an operatio...		Examples	02/28/2019
		ReportDisassemblyErrors.java	Reports the the number of disasse...		Examples	02/28/2019

Filter: **Filter:**

HelloWorldScript.java
Writes "Hello World" to console.
Author: [Ghidra Team](#)

Table Filtering **Filter Settings**

- Early 2000's ... Java was hot
 - Tried C++
 - Platform independent
 - Dynamically load classes
 - Plugins, scripts, and other Extension points
 - Restart not required
 - Memory management (minimal)





OPEN SOURCE

THE PROCESS

RELEASE HISTORY

VERSION	YEAR	MAJOR FEATURES
1.x	2003	Classified version, Proof-of-concept, Framework
2.x	2004	DB, Docking Windows
3.x	2006	Sleigh, Decompiler, Version Control
4.x	2007	Scripting, Version Tracking
5.x	2010	File System Browser
6.x	2014	Unclassified version
7.x, 8.x	2015, 2016	Features, Improvements, Bug Fixes
9.x	2019	PUBLIC version (March 5 at RSA conference)

Executive Order 13691 Promoting Private Sector Cybersecurity Sharing

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to:

- Encourage the voluntary formation of such organizations
- Establish mechanisms to improve their capabilities and functions
- Enable voluntary partnering with the Federal Government

Federal Open Source Policy

sourcecode.cio.gov
code.gov

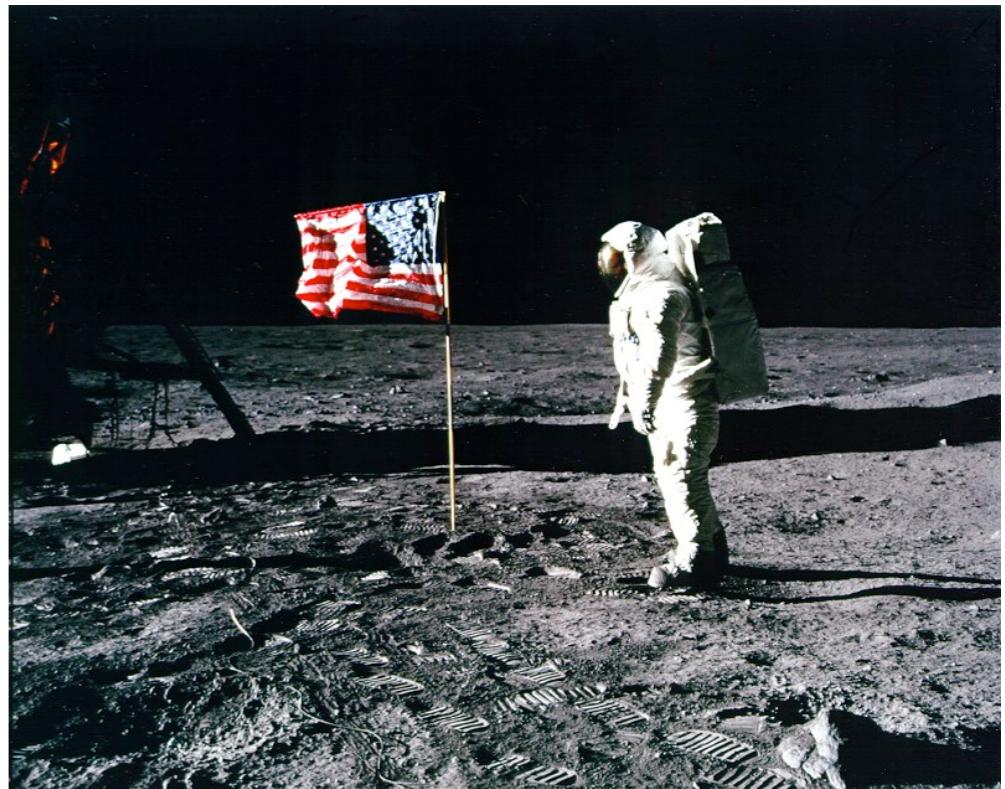
States that: "...challenges may result in duplicative acquisitions for substantially similar code and an inefficient use of taxpayer dollars. This policy seeks to address these challenges by ensuring that new custom-developed Federal source code be made broadly available for reuse across the Federal Government".

- Prepublication review of each line of text
 - 2 people per line
 - Code, HTML, Build Scripts, etc.
 - Took awhile
- Redesign build process
 - Make more open source centric
- Stand up infrastructure
- Huge Team Effort
 - Ghidra Team, PAO, OGC, Security

GHIDRA source code pushed to GitHub on April 5, 2019

BENEFITS

1. Cybersecurity is global issue
2. Collaboration
3. GHIDRA in college, school
4. NSA Recruitment!

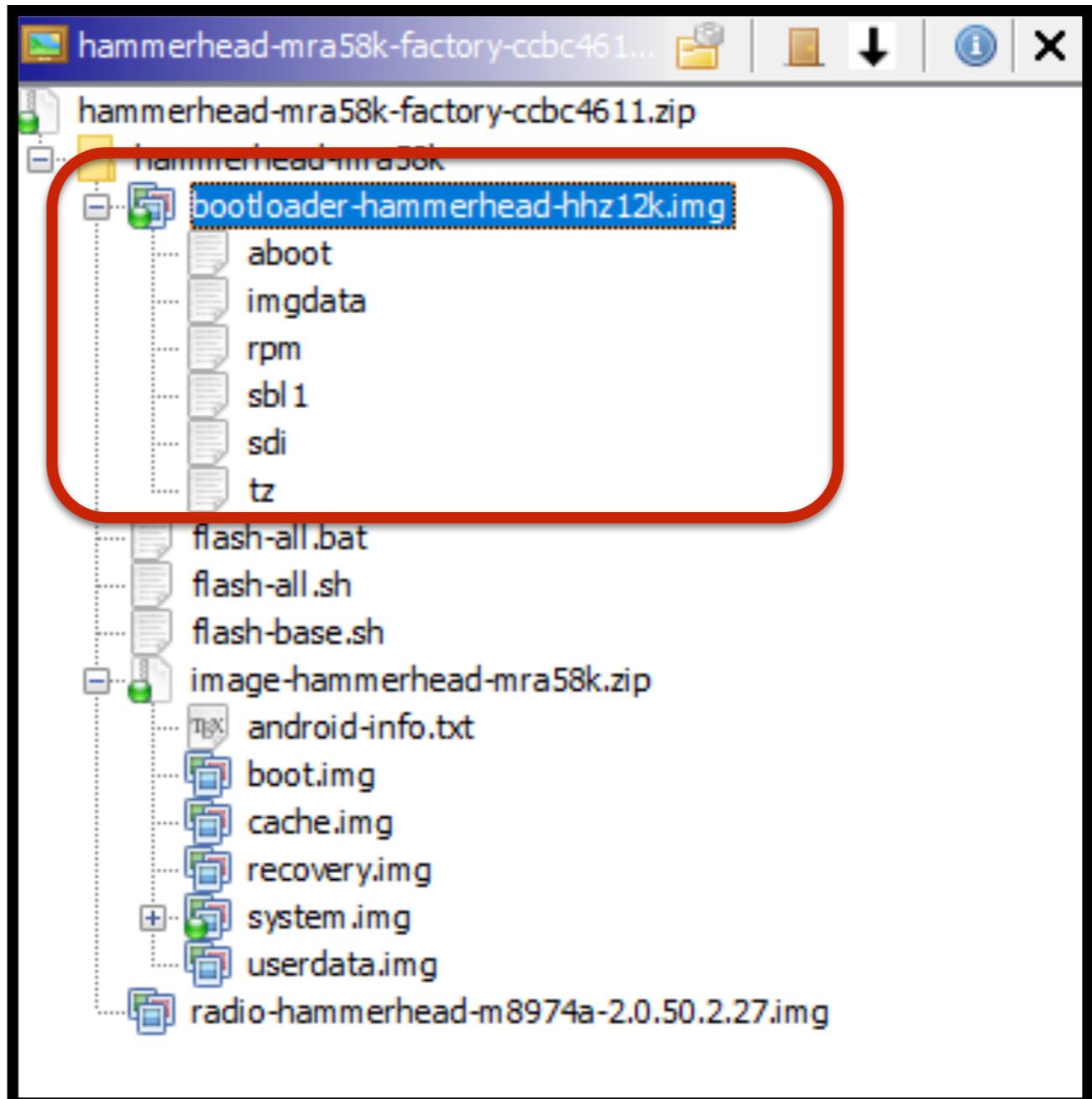


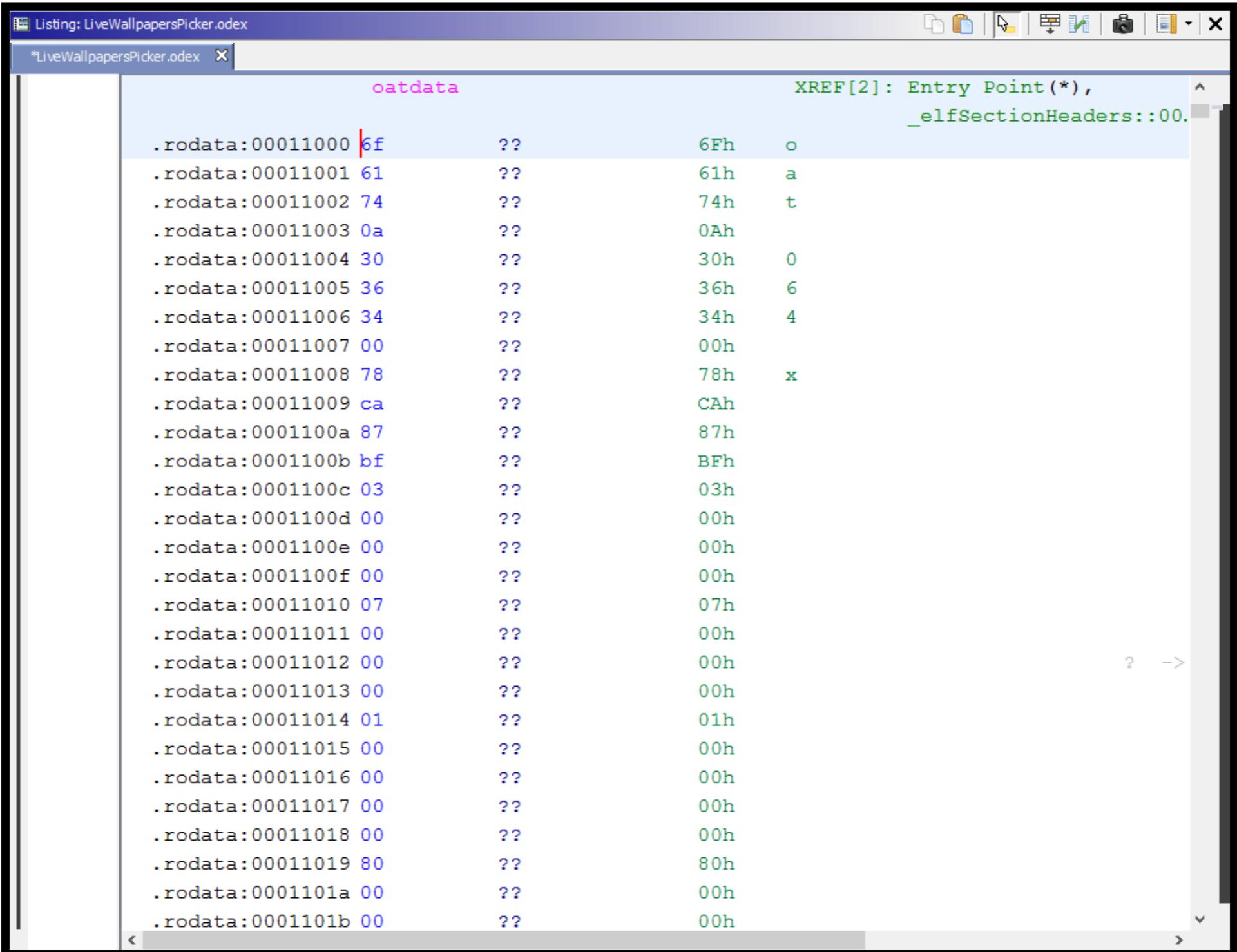
- 9.1
 - Additional Processor Modules
 - Data Type Bit Fields
 - SysCalls
 - Sleigh Editor
- Future
 - Android OAT/ART Support
 - Debugger (Alpha)
- External Engagements
- Bug Fixes

- 9.1
 - Additional Processor Modules
 - Data Type Bit Fields
 - SysCalls
 - Sleigh Editor
 - Future
 - Android OAT/ART Support
 - Debugger (Alpha)
 - External Engagements
 - Bug Fixes
- Let's talk more about this**

- Current Format Support:
 - dex - Dalvik VM EXecutable
 - odex - Optimized Dalvik VM EXecutable
- New Format Support:
 - bootldr - Boot Loader binaries
 - odex - Natively Compiled (ELF)
 - oat - Ahead-Of-Time Compiled DEX
 - art - Android Run-Time
 - vdex, cdex
- OS Versions Supported: Lollipop (5.x) - Pie (9.x)

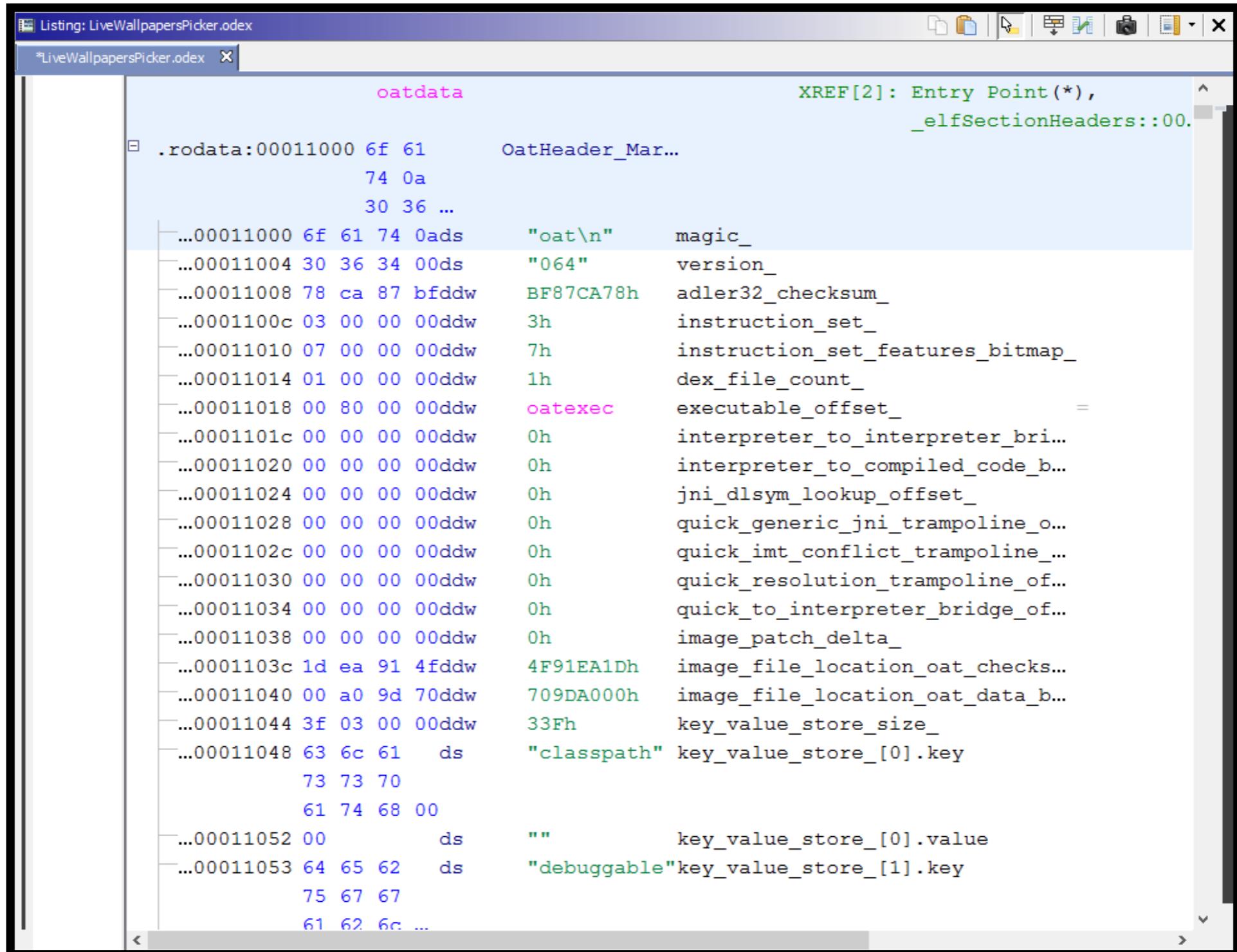
- GFileSystem to open Android Boot Loader format
- Displays contents within the “File System Browser”





The screenshot shows the CHIDRA tool interface with the title "Listing: LiveWallpapersPicker.odex". The main pane displays a table with columns for address, value, hex value, and offset. The table is titled "oatdata" and includes a header row with "XREF[2]: Entry Point(*), _elfSectionHeaders::00.". The data rows show various memory locations starting with ".rodata" and their corresponding values.

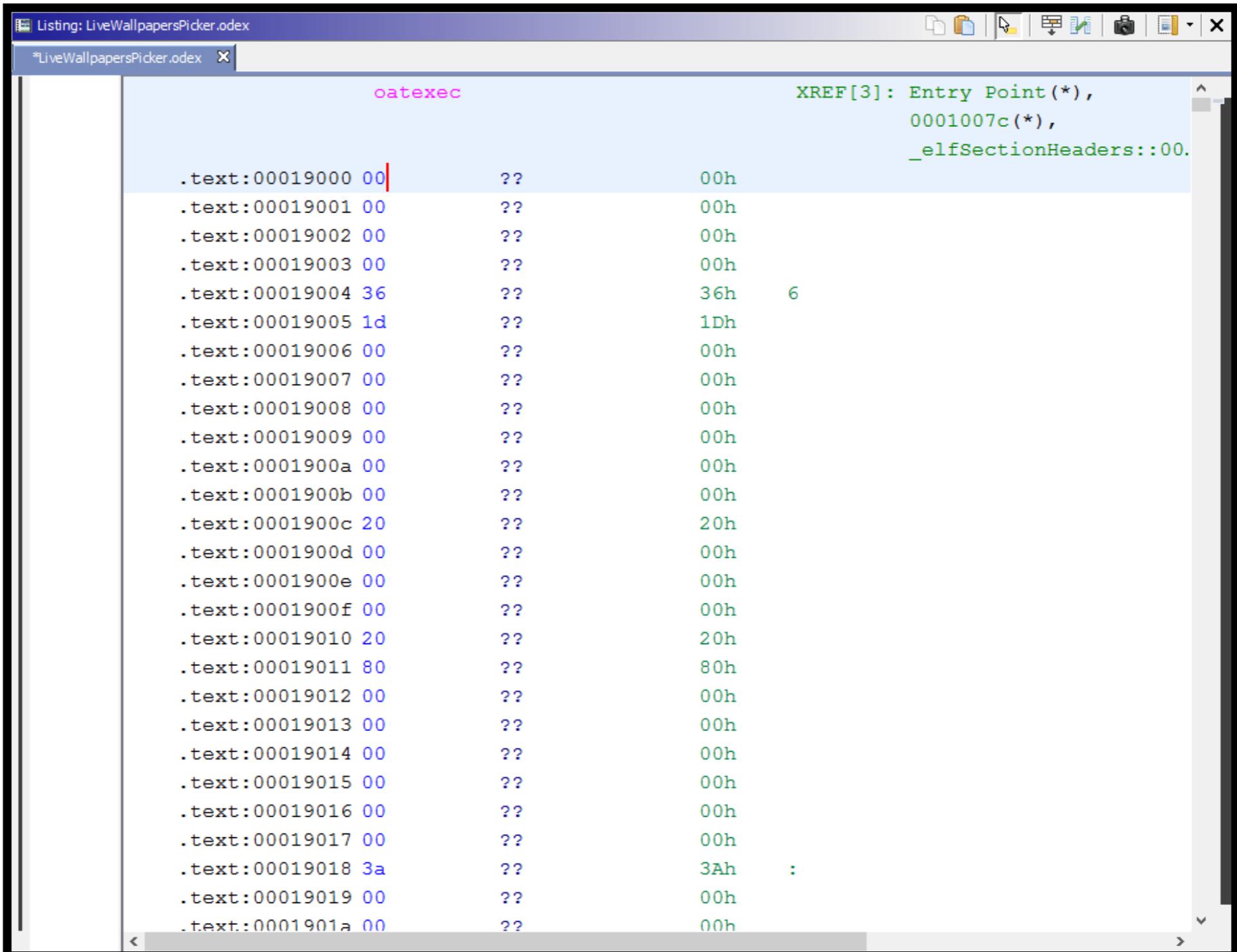
	oatdata		XREF[2]: Entry Point(*), _elfSectionHeaders::00.	
.rodata:00011000	6f	??	6Fh	o
.rodata:00011001	61	??	61h	a
.rodata:00011002	74	??	74h	t
.rodata:00011003	0a	??	0Ah	
.rodata:00011004	30	??	30h	0
.rodata:00011005	36	??	36h	6
.rodata:00011006	34	??	34h	4
.rodata:00011007	00	??	00h	
.rodata:00011008	78	??	78h	x
.rodata:00011009	ca	??	CAh	
.rodata:0001100a	87	??	87h	
.rodata:0001100b	bf	??	BFh	
.rodata:0001100c	03	??	03h	
.rodata:0001100d	00	??	00h	
.rodata:0001100e	00	??	00h	
.rodata:0001100f	00	??	00h	
.rodata:00011010	07	??	07h	
.rodata:00011011	00	??	00h	
.rodata:00011012	00	??	00h	
.rodata:00011013	00	??	00h	
.rodata:00011014	01	??	01h	
.rodata:00011015	00	??	00h	
.rodata:00011016	00	??	00h	
.rodata:00011017	00	??	00h	
.rodata:00011018	00	??	00h	
.rodata:00011019	80	??	80h	
.rodata:0001101a	00	??	00h	
.rodata:0001101b	00	??	00h	



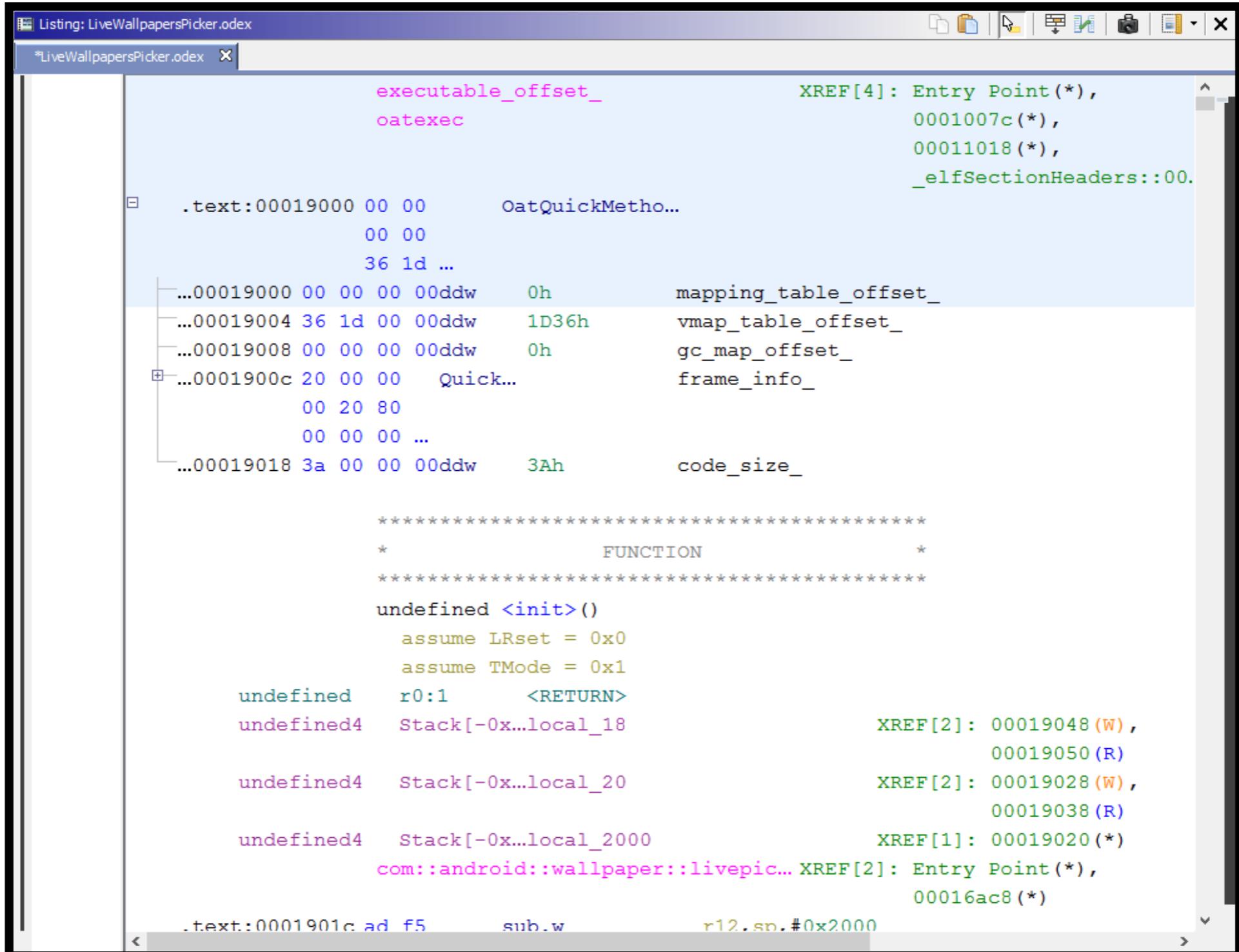
Listing: LiveWallpapersPicker.odex

*LiveWallpapersPicker.odex

	oatdata	XREF[2]: Entry Point (*), _elfSectionHeaders::00.
...	.rodata:00011000 6f 61 74 0a 30 36 ...	OatHeader_Mar...
...	...00011000 6f 61 74 0ads	"oat\n"
...	...00011004 30 36 34 00ds	magic_
...	...00011008 78 ca 87 bfddw	version_
...	...0001100c 03 00 00 00ddw	BF87CA78h adler32_checksum_
...	...00011010 07 00 00 00ddw	3h instruction_set_
...	...00011014 01 00 00 00ddw	7h instruction_set_features_bitmap_
...	...00011018 00 80 00 00ddw	1h dex_file_count_
...	...0001101c 00 00 00 00ddw	oatexec executable_offset_
...	...00011020 00 00 00 00ddw	0h interpreter_to_interpreter_bridge_offset_
...	...00011024 00 00 00 00ddw	0h interpreter_to_compiled_code_base_
...	...00011028 00 00 00 00ddw	jni_dlsym_lookup_offset_
...	...0001102c 00 00 00 00ddw	quick_generic_jni_trampoline_offset_
...	...00011030 00 00 00 00ddw	quick_imt_conflict_trampoline_offset_
...	...00011034 00 00 00 00ddw	quick_resolution_trampoline_offset_
...	...00011038 00 00 00 00ddw	quick_to_interpreter_bridge_offset_
...	...0001103c 1d ea 91 4fddw	image_patch_delta_
...	...00011040 00 a0 9d 70ddw	image_file_location_oat_checks...
...	...00011044 3f 03 00 00ddw	709DA000h image_file_location_oat_data_b...
...	...00011048 63 6c 61 ds	33Fh key_value_store_size_
		"classpath" key_value_store_[0].key
	73 73 70	
	61 74 68 00	
...	...00011052 00 ds	"" key_value_store_[0].value
...	...00011053 64 65 62 ds	"debuggable"key_value_store_[1].key
	75 67 67	
	61 62 6c ...	



	oatexec	XREF[3]: Entry Point(*), 0001007c(*), _elfSectionHeaders::00.
.text:00019000 00	??	00h
.text:00019001 00	??	00h
.text:00019002 00	??	00h
.text:00019003 00	??	00h
.text:00019004 36	??	36h 6
.text:00019005 1d	??	1Dh
.text:00019006 00	??	00h
.text:00019007 00	??	00h
.text:00019008 00	??	00h
.text:00019009 00	??	00h
.text:0001900a 00	??	00h
.text:0001900b 00	??	00h
.text:0001900c 20	??	20h
.text:0001900d 00	??	00h
.text:0001900e 00	??	00h
.text:0001900f 00	??	00h
.text:00019010 20	??	20h
.text:00019011 80	??	80h
.text:00019012 00	??	00h
.text:00019013 00	??	00h
.text:00019014 00	??	00h
.text:00019015 00	??	00h
.text:00019016 00	??	00h
.text:00019017 00	??	00h
.text:00019018 3a	??	3Ah :
.text:00019019 00	??	00h
.text:0001901a 00	??	00h



The screenshot shows the CHIDRA debugger interface with the following details:

- Title Bar:** Listing: LiveWallpapersPicker.odex
- Panel Headers:** executable_offset_, oatexec, XREF[4]: Entry Point (*), 0001007c (*), 00011018 (*), _elfSectionHeaders::00.
- Memory Dump Structure:**
 - .text:00019000 00 00 OatQuickMetho...
 - ...00019000 00 00 00ddw 0h mapping_table_offset_
 - ...00019004 36 1d 00 00ddw 1D36h vmap_table_offset_
 - ...00019008 00 00 00 00ddw 0h gc_map_offset_
 - ...0001900c 20 00 00 Quick... 00 20 80 frame_info_
 - ...00019018 3a 00 00 00ddw 3Ah code_size_
- FUNCTION Section:** **** FUNCTION ****
- Assembly Code:**

```
undefined <init>()
    assume LRset = 0x0
    assume TMode = 0x1
undefined    r0:1      <RETURN>
undefined4   Stack[-0x...local_18]           XREF[2]: 00019048 (W),
                                                       00019050 (R)
undefined4   Stack[-0x...local_20]           XREF[2]: 00019028 (W),
                                                       00019038 (R)
undefined4   Stack[-0x...local_2000]          XREF[1]: 00019020 (*)
com::android::wallpaper::livepic... XREF[2]: Entry Point (*),
                                         00016ac8 (*)
```
- Registers:** .text:0001901c ad f5, sub.w, r12.sp.#0x2000

Downloads:

- 9.0.0 : 302k
- 9.0.1 : 36k
- 9.0.2 : 102k
- 9.0.4 : 66k
- Video Views: 761k

GitHub:

- Stars : 16,518
- Forks : 2,076
- Watchers : 712
- Issues: 690
 - 290 open
- Pull Requests: 139
 - 29 open

As of ~22 July

- Bugs
 - Please report.
 - Provide
 - Source code
 - Relevant bytes from the binary
 - Stack trace(s)
 - Please don't send copyrighted binaries.
 - Improvements
 - New Features
-
- **Thanks to all those who contributed!**

- GHIDRA Team is only on GitHub
 - Not on Twitter, etc
- @NSAGov on Twitter announces new releases
- NSA Public Affairs Office (PAO)
 - mediarelations@nsa.gov

- Software
 - ghidra-sre.org
- Source Code
 - github.com/NationalSecurityAgency/ghidra
- All other sites are not official.

THANK YOU

Thank you!