

THE GHIDRA BOOK

THE DEFINITIVE GUIDE

KARA NANCE and CHRIS EAGLE

2nd Edition Handy Index!

The following index is provided to help you easily identify the files associated with a particular example in the second edition of the book. A few words to guide you as you explore these files:

...regarding reuse of files

In some cases, files are used in multiple locations throughout the text, so be sure to pay attention to the folder names to ensure you are loading the correct file.

...regarding file names

Most binary file names include meaningful indicators to better understand the compiler options used to build that binary. This results in some long file names. Don't be alarmed.

...regarding free-format coding vs book layout

When laying out code in a book, it sometimes requires some modification of the script, particularly with longer examples. In *The Ghidra Book*, scripts occasionally required changes (e.g., shorter variable names, fewer blank lines, fewer comments, rearranged declarations, etc.) to lay out properly on a page. The scripts provided in this download maintain the same functionality but should be more readable.

...example code vs robust production code

The example code written for this book was designed to demonstrate particular concepts or functionality. This generally requires a simplified scenario. We are very aware that this is not robust production code. These are toy examples to demonstrate and reinforce foundational concepts. 😊

If you have questions or comments, please feel free to contact:

questions@ghidrabook.com

Chapter 04 – Beginning Your Analysis

Page 44	ch04/ch4_example.exe	(binary)
---------	----------------------	----------

Chapter 05 – Exploring Ghidra’s Data Displays

Page 63	ch05/ch05_example1.exe	(binary)
---------	------------------------	----------

Chapter 06 – Making Sense of a Disassembly

Page 93 - 95	ch06/demo_stackframe_64	(binary)
Page 104 - 105	ch06/example1.c	(C source)
Page 104 - 105	ch06/example1	(binary)
Page 106 - 108	ch06/example2.c	(C source)
Page 106 - 108	ch06/example2	(binary)
Page 110 - 114	ch06/compute.c	(C source)
Page 110 - 114	ch06/compute	(binary)
Page 115 - 117	ch06/demo_stackframe_32	(binary)

Chapter 07 – Refining a Disassembly

** All examples in this chapter use files from previous chapters.

Page 122 - 139	ch06/demo_stackframe_32	(binary) **
Page 141 - 142	ch06/demo_stackframe_64	(binary) **
Page 144 - 145	ch06/demo_stackframe_32	(binary) **
Page 145	ch06/demo_stackframe_64	(binary) **

Chapter 08 – Working With Data Types and Data Structures

Page 149	ch08/http_get_example_x64	(binary)
Page 151 - 154	ch08/global_array_demo_x64_stripped	(binary)
Page 154 - 157	ch08/stack_array_demo_x64_stripped	(binary)
Page 157 - 159	ch08/heap_array_demo_x64_stripped	(binary)
Page 161	ch08/global_struct_demo_x64_stripped	(binary)
Page 162	ch08/stack_struct_demo_x64_stripped	(binary)
Page 163	ch08/heap_struct_demo_x64_stripped	(binary)
Page 164	ch08/heap_packed_struct_demo_x64_stripped	(binary)
Page 165	ch08/heap_struct_array_demo_x64_stripped	(binary)
Page 167 - 171	ch08/global_array_demo_x64_stripped	(binary)
Page 172	ch08/http_get_example_x86	(binary)
Page 176	ch08/call_vfunc.exe	(binary)

Chapter 09 – Understanding Cross-References

** Some examples in this chapter use files from previous chapters

Page 187	ch06/demo_stackframe_32	(binary) **
Page 190	ch09/simple_flows.c	(C source)
Page 190	ch09/simple_flows.exe	(binary)
Page 194	ch08/call_vfunc.exe	(binary) **
Page 195	ch06/demo_stackframe_32	(binary) **
Page 197	ch09/call_vfunc_x86	(binary) **

Chapter 10 – Using Graph Views

** Some examples in this chapter use files from previous chapters

Page 200	ch10/global_array_demo.c	(C source)
Page 201	ch10/global_array_demo_x64	(binary) **
Page 207	ch10/call_tree_x64	(binary)
Page 209	ch10/call_tree_x64_static	(binary)

Chapter 11 – Collaborative SRE

No example files required 😊

Chapter 12 – Customizing Ghidra

No example files required 😊

Chapter 13 – Extending Ghidra's Worldview

** Some examples in this chapter use files from previous chapters

Page 280 - 281	ch08/call_vfunc.exe	(binary) **
Page 282	ch10/global_array_demo_x64	(binary) **
Page 293	ch13/upx_demo1_x64_static.upx	(binary)
Page 296	ch13/upx_demo2_x64_static.upx	(binary)
Page 297	ch13/upx_demo1_x64_static_stripped.upx	(binary)
Page 298	ch13/libc.a	(library)

Chapter 14 – Basic Scripting with Ghidra and PyGhidra

Page 304	ch10/global_array_demo_x64	(binary) **
Page 309 - 313	ch14/FindStringsByRegex.java	(script)
Page 329	ch14/ch14_1_flat.java	(script)
Page 330	ch14/ch14_2_flat.java	(script)
Page 331	ch14/ch14_3_flat.java	(script)
Page 332	ch14/ch14_4_flat.java	(script)
Page 333	ch14/ch14_5_flat.java	(script)

Chapter 15 – Integrating Scripting with Eclipse and GhidraDev

** Some examples in this chapter use files from previous chapters

Page 352 - 362	ch15/SimpleROPAnalyzer.java	(analyzer module source)
Page 363	ch10/call_tree_x64_static	(binary) **

Chapter 16 – Running Ghidra in Headless Mode

** The directory structure and files in this folder are required to remain unchanged to achieve the same results as the text.

Page 367 - 377	ch16/global_array_demo_x64	(binary) **
Page 346	ch16/demo_stackframe_*	(subdirectory and binaries)
Page 349	ch16/CH16_subdirectory/demo_stackframe_32_sub	(binary)

Chapter 16a – Running Ghidra in Headless Mode

Page 378 - 383	ch16_scripts/HeadlessSimpleROP.java	(script)
Page 359	ch13/libc.a	(library) **

Chapter 17 – Loaders

** See shellcode_samples.README to learn more about these examples.

Page 387	ch17/payload.linux.x86.bind_shell.bin	(binary)
Page 389 - 398	ch17/ch17_pe_raw.exe	(binary)
Page 400 - 403	ch17/payload.linux.x86.bind_shell.bin	(binary)
Page 404 - 409	ch17/SimpleShellcodeLoader.java	(loader module source)
Page 410	ch17/payload.linux.x86.bind_shell.bin	(binary)
Page 410	ch17/ch17_pe_raw.exe	(binary)
Page 412 - 415	ch17/SimpleShellcodeSourceLoader.java	(loader module source)
Page 390	ch17/payload.linux.x86.bind_shell.c	(C source)
Page 391	ch17/elf_shellcode_min	(README)
Page 416 - 421	ch17/SimpleELFShellcodeLoader.java	(loader module source)
Page 422	See Ghidra/Processors/x86/data/languages/x86.ldefs in your Ghidra installation	(language definition file)
Page 423	ch17/SimpleShellcode.opinion	(opinion file)
Page 424 - 426	ch17/elf_shellcode_min	(README)

Chapter 18 – Processors

For those adventurous souls playing along with the home game for this chapter, the files marked with * contain the edited versions of the *ia.sinc* file used in each example. If you wish to use these files, you will need to rename each file to *ia.sinc* when you are using it. You can obtain the same results by modifying your *ia.sinc* file and using these files for reference should any issues arise. Regardless of your approach, be sure to save a copy of your original x86 *ia.sinc* file before replacing it during experimentation!

Page 435	ch18/ia.sinc.01b_add_vmxplode*	(SLEIGH)
Page 413	ch18/vmx_test_01a_vmxoff	(SLEIGH)
Page 414	ch18/vmx_test_01b_vmxplode	(SLEIGH)
Page 442 - 445	ch18/ia.sinc.02a_set_eax_to_constant*	(SLEIGH)
Page 442 - 445	ch18/vmx_test_01b_vmxplode	(SLEIGH)
Page 446 - 450	ch18/ia.sinc.02b_set_reg_to_constant*	(SLEIGH)
Page 446 - 450	ch18/vmx_test_02b_set_reg_to_constant	(SLEIGH)
Page 450	ch18/ia.sinc.02c_set_reg_to_immediate*	(SLEIGH)
Page 450	ch18/vmx_test_02c_set_reg_to_immediate	(SLEIGH)
Page 451 - 452	ch18/ia.sinc.03a_add_vm_registers*	(SLEIGH)
Page 451 - 452	ch18/vmx_test_03_add_vm_regs	(SLEIGH)

Chapter 19 – The Decompiler

Page 429 - 430	ch19/options	(binary)
Page 432	ch19/var_depends	(binary)
Page 438	ch19/structs	(binary)

Chapter 20 – Compiler Variations

Page 449	ch20/switch_demo_1_x86	(binary)
Page 450	ch20/switch_demo_1_Win32_Debug.exe	(binary)
Page 453	ch20/strange_math_x64_Debug.exe	(binary)
Page 453	ch20/strange_math_x64_Release.exe	(binary)
Page 454	ch20/strange_math_x64	(binary)
Page 455	ch20/idiom_x64	(binary)
Page 456	ch20/idiom_x64_Release.exe	(binary)
Page 456	ch20/idiom_x64_O2	(binary)
Page 457	ch20/functions_linux_x86	(binary)
Page 457	ch20/functions_linux_x86_O2	(binary)
Page 460	ch20/rtti_x64	(binary)
Page 461	ch20/rtti_x64_stripped	(binary)

Chapter 21 – Obfuscated and Emulation

Page 504 - 505	ch21/emulator_example_2	(binary)
Page 505 - 511	ch21/SimpleEmulator.java	(script)
Page 506	ch21/simplePack.c	(C source)
Page 511 - 512	ch21/simplePack	(binary)

Chapter 22 – Patching Binaries

Page 518	ch22/search.c	(C source)
Page 520	ch22/search	(binary)
Page 524	ch22/patch_demo	(binary)
Page 534	ch22/debug_check.c	(C source)
Page 522	ch22/debug_check_x64	(binary)
Page 526	ch22/debug_check_x64.patched	(binary)

Chapter 23 – BSim and Other Comparison Tools

****Some examples in this chapter use files from previous chapters**

Page 541	ch22/debug_check_x64	(binary) **
Page 541	ch22/debug_check_x64.patched	(binary) **
Page 545	ch23/diff_KN	(binary)
Page 545	ch23/diff_CS	(binary)
Page 550	ch22/debug_check_x64	(binary) **
Page 550	ch22/debug_check_x64.patched	(binary) **
Page 554	Ch23/diff_sample1	(binary)
Page 553	ch23/diff_sample2	(binary)
Page 556	ch23/diff_sample3	(binary)
Page 562	ch23/ransomware_v236	(binary)
Page 562	ch23/ransomware_new	(binary)
Page 564	ch23/ransomware_v236.c	(C source)
Page 565	ch23/ransomware_new.c	(C source)