The following index is provided to help you easily identify the files associated with a particular example in 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 for that particular binary. This results in some long file names.

…regarding free-format coding vs book layout

When laying out code in a text, it sometimes requires some modification of the script, particularly with longer script examples. In *The Ghidra Book*, scripts occasionally required some modification (e.g., shorter variable names, fewer blank lines, fewer comments, rearranging declarations, etc.) to layout properly on a page. The scripts provided in this download maintain the 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 – Getting Started with Ghidra

Page 44 - 53	ch04/ch4_example.exe	(binary)

Chapter 05 – Ghidra Data Displays

Page 61	ch05/ch5_example1.exe	(binary)

Chapter 06 – Making Sense of a Ghidra Disassembly

Page 93	ch06/ch6_demo_stackframe_64	(binary)
Page 107	ch06/demo_stackframe_32	(binary)
Page 109	ch06/demo_stackframe_32	(binary)
Page 112	ch06/demo_stackframe_32	(binary)
Page 117	ch06/demo_stackframe_32	(binary)

Chapter 07 – Disassembly Manipulation

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

Page 121	ch06/demo_stackframe_32	(binary) **
Page 130	ch06/demo_stackframe_32	(binary) **
Page 131	ch06/demo_stackframe_32	(binary) **
Page 132	ch06/demo_stackframe_32	(binary) **
Page 143	ch06/demo_stackframe_32	(binary) **

Chapter 08 – Data Types and Data Structures

Page 149	ch08/http_get_example_x64	(binary)
Page 151	ch08/global_array_demo.c	(C Source)
Page 151	ch08/global_array_demo_x64_stripped	(binary)
Page 154	ch08/global_array_demo_x64_stripped	(binary)
Page 155	ch08/stack_array_demo.c	(C Source)
Page 155	ch08/stack_array_demo_x64_stripped	(binary)
Page 157	ch08/heap_array_demo.c	(C Source)
Page 157 - 158	ch08/heap_array_demo_x64_stripped	(binary)
Page 161	ch08/global_struct_demo.c	(C Source)
Page 161	ch08/global_struct_demo_x64_stripped	(binary)
Page 162	ch08/stack_struct_demo_x64_stripped	(binary)
Page 163	ch08/heap_struct_demo.c	(C Source)
Page 163	ch08/heap_struct_demo_x64_stripped	(binary)
Page 164	ch08/heap_packed_struct_demo_x64_stripped	(binary)
Page 164 - 165	ch08/global_array_demo.c	(C Source)
Page 165	ch08/global_array_demo_x64_stripped	(binary)
Page 167	ch08/global_struct_demo_x64_stripped	(binary)
Page 172	ch08/http_get_example_x86	(binary)
Page 175	ch08/call_vfunc.c	(C Source)
Page 176	ch08/call_vfunc.exe	(binary)

Chapter 09 – Cross-References

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

Page 185	ch06/demo_stackframe_32	(binary) **
Page 187	ch09/simple_flows.exe	(binary)
Page 188	ch09/simple_flows.c	(source)
Page 188	ch09/simple_flows.exe	(binary)
Page 189	ch09/simple_flows.exe	(binary)
Page 190	ch09/simple_flows.exe	(binary)
Page 192	ch08/call_vfunc.exe	(binary) **
Page 193	ch06/demo_stackframe_32	(binary) **
Page 195	ch08/call_vfunc_x86	(binary) **

Chapter 10 – Graphs

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

Page 198	ch08/global_array_demo.c	(C Source) **
Page 199	ch08/global_array_demo_x64	(binary) **
Page 206	ch10/rand_test_x64	(binary)
Page 209	ch10/call_tree_x64	(binary)
Page 213	ch10/call_tree_x64_static	(binary)

Chapter 11 – Collaborative SRE

Page 219	ch11/installGhidraServer.sh	(Bash script)

Chapter 12 – Customizing Ghidra

No example files required :)

Chapter 13 – Extending Ghidra's Worldview

Page 276	ch13/upx_demo1_x64_static.upx	(binary)
Page 278	ch13/upx_demo2_x64_static.upx	(binary)
Page 280	ch13/upx_demo1_x64_static_stripped.upx	(binary)
Page 281	ch13/libc.a	(library)

Chapter 14 – Basic Ghidra Scripting

Page 293	ch14/FindStringsByRegex.java	(script)
Page 295	ch14/FindStringsByRegex.py	(script)
Page 307	ch14/ch14_1_flat.java	(script)
Page 308	ch14/ch14_2_flat.java	(script)
Page 309	ch14/ch14_3_flat.java	(script)
Page 310	ch14/ch14_4_flat.java	(script)
Page 312	ch14/ch14_5_flat.java	(script)

Chapter 15 – Eclipse and GhidraDev

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

Page 331 - 337	ch15/SimpleROPAnalyzer.java	(analyzer module source)
Page 340	ch10/call_tree_x64_static	(binary) **

Chapter 16 – Ghidra in Headless Mode

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

Page 342	ch08/global_array_demo_x64	(binary) **
Page 344	ch08/global_array_demo_x64	(binary) **
Page 346	ch16/demo_stackframe_*	(subdirectory and binaries)
Page 349	ch16/CH16_subdirectory/demo_stackframe_32_sub	(binary)
Page 356	ch16_scripts/HeadlessSimpleROP.java	(script)
Page 359	ch13/libc.a	(library) **

Chapter 17 – Ghidra Loaders

Page 364	ch17/payload.linux.x86.bind_shell.bin	(binary)
Page 365	ch17/ch17_pe_raw.exe	(binary)
Page 377	ch17/payload.linux.x86.bind_shell.bin	(binary)
Page 380 - 384	ch17/SimpleShellcodeLoader.java	(loader module source)
Page 386	ch17/payload.linux.x86.bind_shell.bin	(binary)
Page 386	ch17/ch17_pe_raw.exe	(binary)
Page 388 - 389	ch17/SimpleShellcodeSourceLoader.java	(loader module source)
Page 390	ch17/payload.linux.x86.bind_shell.c	(C source file)
Page 391	ch17/elf_shellcode_min	(binary)
Page 392 - 396	ch17/SimpleELFShellcodeLoader.java	(loader module source)
Page 396	See Ghidra/Processors/x86/data/languages/x86.ldefs in your Ghidra installation	(language definition file)
Page 397	ch17/SimpleShellcode.opinion	(opinion file)
Page 398	ch17/elf_shellcode_min	(binary)

Chapter 18 – Ghidra 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 410	ch18/ia.sinc.01b_add_vmxplode	(SLEIGH)
Page 413	ch18/vmx_test_01a_vmxoff	(SLEIGH)
Page 414	ch18/vmx_test_01b_vmxplode	(SLEIGH)
Page 416	*ch18/ia.sinc.02a_set_eax_to_constant	(SLEIGH)
Page 416	ch18/vmx_test_01b_vmxplode	(SLEIGH)
Page 491	*ch18/ia.sinc.02b_set_reg_to_constant	(SLEIGH)
Page 423	ch18/vmx_test_02b_set_reg_to_constant	(SLEIGH)
Page 423	*ch18/ia.sinc.02c_set_reg_to_immediate	(SLEIGH)
Page 424	ch18/vmx_test_02c_set_reg_to_immediate	(SLEIGH)
Page 424 - 425	*ch18/ia.sinc.03a_add_vm_registers	(SLEIGH)
Page 425	ch18/vmx_test_03_add_vm_regs	(SLEIGH)

Chapter 19 – The Ghidra 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 Code Analysis

Page 492 - 494	ch21/burneye.java	(script)
Page 499 - 502	ch21/SimpleEmulator.java	(script)
Page 502	ch21/simplePack	(binary)

Chapter 22 – Patching Binaries

Page 509	ch22/search	(binary)
Page 513	ch22/patch_demo	(binary)
Page 515	ch22/patch.java	(script)
Page 520	ch22/patch_demo_64.exe	(binary)
Page 522	ch22/patch_demo_64	(binary)
Page 524 - 525	ch22/patch_file.java	(script)
Page 526	ch22/debug_check_x64	(binary)

Chapter 23 – Binary Differencing and Version Tracking

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

Page 531	ch22/debug_check_x64	(binary)
Page 531	ch23/debug_check_x64.patched	(binary)
Page 535	ch23/diff_sample1	(binary)
Page 535	ch23/diff_sample1a	(binary)
Page 538	ch22/debug_check_x64	(binary)
Page 538	ch23/debug_check_x64.patched	(binary)
Page 541	ch23/diff_sample2	(binary)
Page 545	ch23/diff_sample3	(binary)