Project Management Assignment 2 - ST2601 ITSP
Installation and Usage User Guide for GhOST
Group 6 - 3A/66 - Reverse Engineering ARM Binary

Members:

Admin No:	Name:
2003951	Haziq Bin Sanib
2003964	Tan Joven
2003782	Tee Kai Guan
2026130	Sree Vathsan
2025733	Toh Zheng Hong Shawn

Table of Contents

Table of Contents 1

Installation & Setup 2

- Linux 2
  - Using Docker 2
  - Manual Setup 3
- Windows 4
  - Using Docker 4
  - Manual Setup 4

Usage 8

- Using Docker 8
- Running Manually through Ghidra GUI 10

Installation & Setup

There are two ways to install and start using GhOST, either installing it and setting it up manually by installing Ghidra and Java or through the use of a docker.

Using a docker is recommended as it is easier to install and prevents any package pollution or conflicts with existing programs.

Linux

Using Docker

1) First update the system and install the necessary package

```
$ sudo apt-get update

$ sudo apt-get install \
    ca-certificates \
    curl \
    gnupg \
    lsb-release
```

2) Add Docker's official GPG key

```
$ sudo mkdir -p /etc/apt/keyrings
$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg |
sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
```

3) Set up repository

```
$ echo \ "deb [arch=$(dpkg --print-architecture)
signed-by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/ubuntu \ $(lsb_release
-cs) stable" | sudo tee
/etc/apt/sources.list.d/docker.list > /dev/null
```

4) Install docker engine

```
$ sudo apt-get update
$ sudo apt-get install docker-ce docker-ce-cli
containerd.io docker-compose-plugin
```

5) Create new user group and and add user to group

```
$ sudo groupadd docker
$ sudo usermod -aG docker $USER
```

6) Restart the system to ensure the group is added successfully

Manual Setup

1) Run the following command using sudo privileges to update the system and install Java version 17

   ```
   $ sudo apt update

   $ sudo apt install openjdk-17-jdk
   ```

2) Check Java is installed correctly using the following command

   ```
   $ java -version
   ```

   A similar output should be shown:

   ```
   openjdk version "17.0.1" 2021-04-14
   ```

3) Install python2 using the following command

   ```
   $ sudo apt install python2
   ```

   Verify python is working using the following command

   ```
   $ python2
   ```

   The following output should be shown:

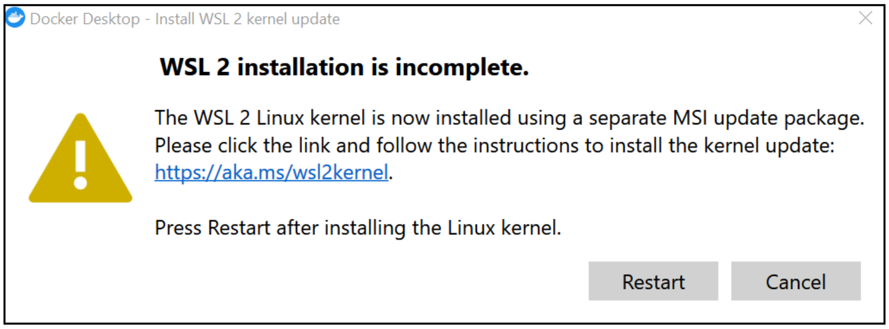
   ```
   $ Python 2.7.18 (default, Jul 14 2021, 08:11:37)
   [GCC 10.2.1 20210110] on linux2
   Type "help", "copyright", "credits" or "license" for more
   information.
   ```

4) Download the latest release of ghidra and extract it from the URL:
   Releases · NationalSecurityAgency/ghidra (github.com)

Windows

Using Docker

1) Download Docker Desktop from: https://desktop.docker.com/win/main/amd64/Docker%20Desktop%20Installer.exe
2) Run the installation file and select all default values, a restart should be prompted.
3) If the following pop up appears after the restart



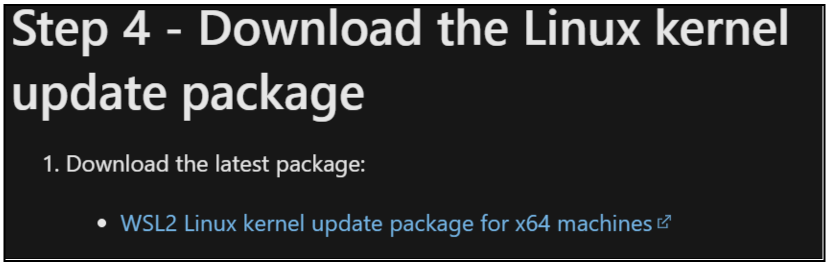
Docker Desktop - Install WSL 2 kernel update

WSL 2 installation is incomplete.

The WSL 2 Linux kernel is now installed using a separate MSI update package. Please click the link and follow the instructions to install the kernel update: https://aka.ms/wsl2kernel.

Press Restart after installing the Linux kernel.

Follow the link to download the WSL2 Linux kernel update package and run the installer



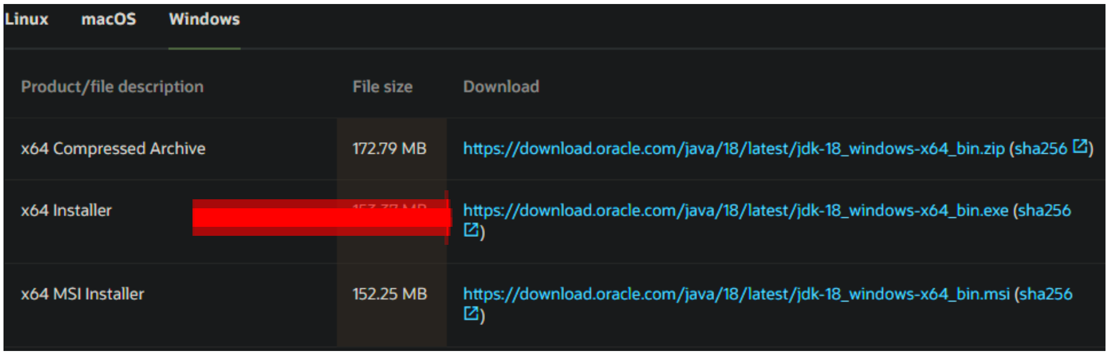
Step 4 - Download the Linux kernel update package

1. Download the latest package:
   - WSL2 Linux kernel update package for x64 machines

After successful install of the kernel update package, click on 'Restart' on the original prompt and Docker should now be running.

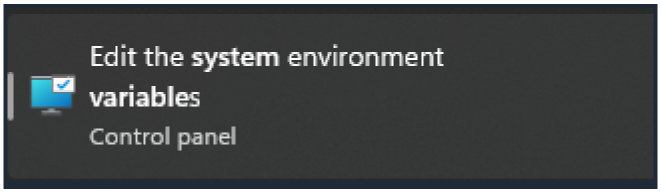
Manual Setup

1) Open the following webpage: https://www.oracle.com/java/technologies/downloads/#jdk17-windows
2) Click on windows and x64 installer



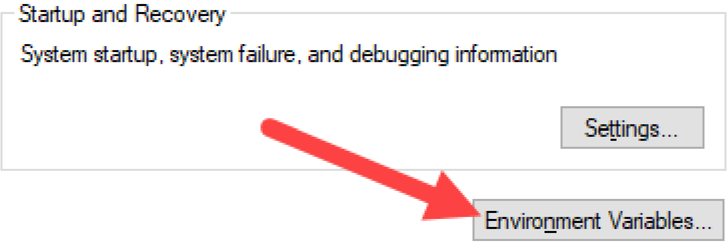
Product/file description	File size	Download
x64 Compressed Archive	172.79 MB	https://download.oracle.com/java/18/latest/jdk-18_windows-x64_bin.zip (sha256)
x64 Installer	[redacted]	https://download.oracle.com/java/18/latest/jdk-18_windows-x64_bin.exe (sha256)
x64 MSI Installer	152.25 MB	https://download.oracle.com/java/18/latest/jdk-18_windows-x64_bin.msi (sha256)

3) Run the downloaded file
4) Click next for all options and click close when done
5) Search for ‘System variables’ in the windows search bar and click the first option



Edit the **system** environment **variables**
Control panel

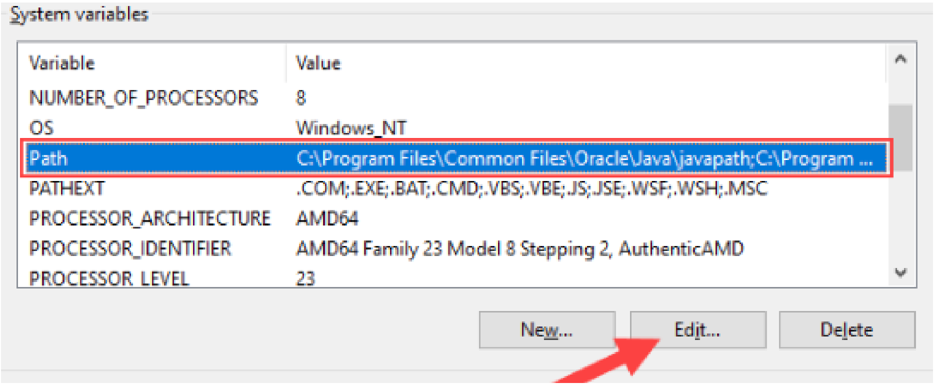
6) Click on environment variables



Startup and Recovery

System startup, system failure, and debugging information

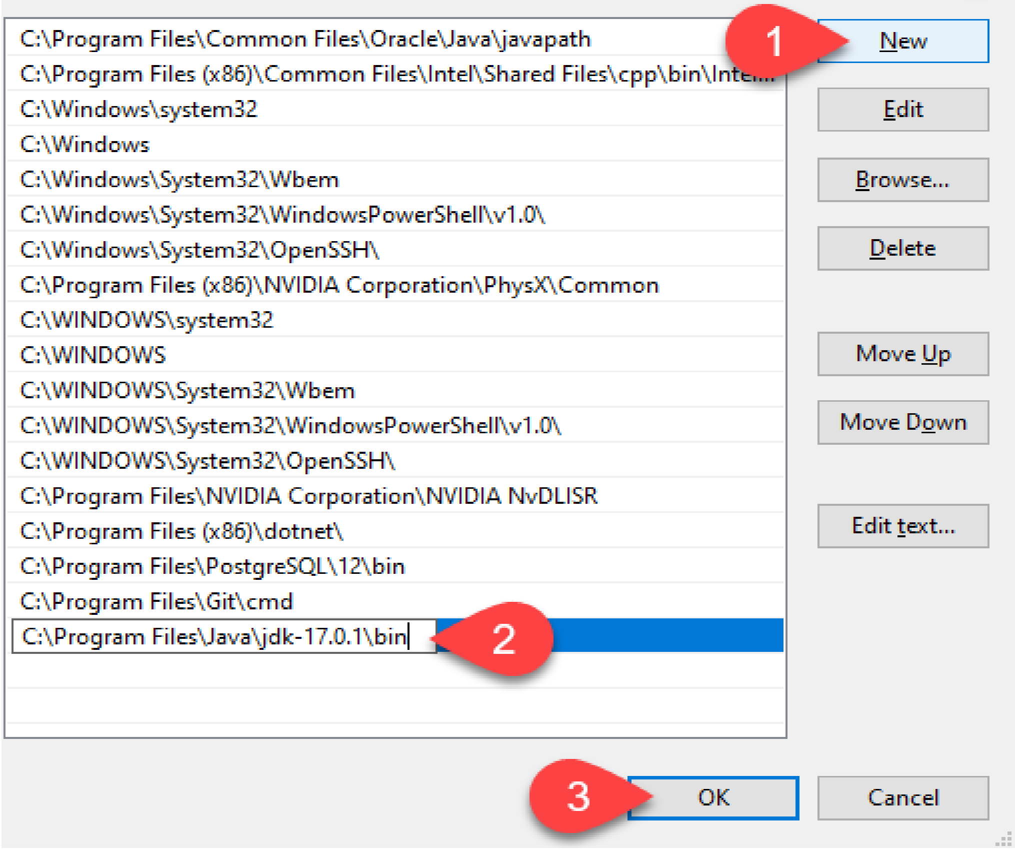
7) Select Path and click edit



System variables

Variable	Value
NUMBER_OF_PROCESSORS	8
OS	Windows_NT
Path	C:\Program Files\Common Files\Oracle\Java\javapath;C:\Program ...
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64
PROCESSOR_IDENTIFIER	AMD64 Family 23 Model 8 Stepping 2, AuthenticAMD
PROCESSOR_LEVEL	23

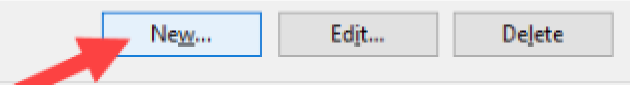
8) Click the New button and enter the path to the Java bin directory



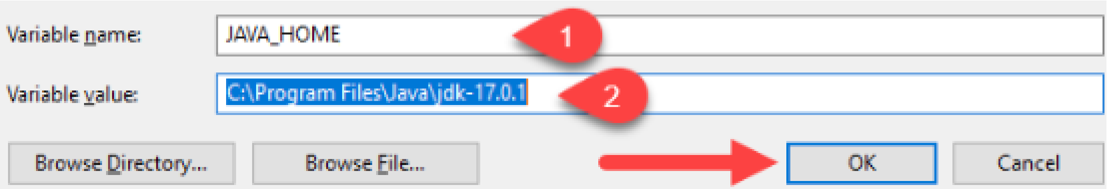
```
C:\Program Files\Common Files\Oracle\Java\javapath
C:\Program Files (x86)\Common Files\Intel\Shared Files\cpp\bin\Inte...
C:\Windows\system32
C:\Windows
C:\Windows\System32\Wbem
C:\Windows\System32\WindowsPowerShell\v1.0\
C:\Windows\System32\OpenSSH\
C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common
C:\WINDOWS\system32
C:\WINDOWS
C:\WINDOWS\System32\Wbem
C:\WINDOWS\System32\WindowsPowerShell\v1.0\
C:\WINDOWS\System32\OpenSSH\
C:\Program Files\NVIDIA Corporation\NVIDIA NvDLISR
C:\Program Files (x86)\dotnet\
C:\Program Files\PostgreSQL\12\bin
C:\Program Files\Git\cmd
C:\Program Files\Java\jdk-17.0.1\bin
```

9) Click ‘OK’ to save

10) In the Environment Variables window, under the System variables category, click the New… button to create a new variable



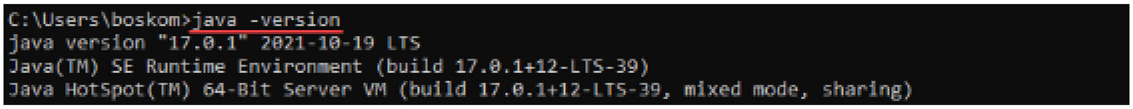
11) Name the variable as JAVA_HOME and In the variable value field, paste the path to your Java jdk directory and click OK



Variable name: JAVA_HOME

Variable value: C:\Program Files\Java\jdk-17.0.1

12) Run ‘java -version’ in the command prompt and ensures the output is similar



```
C:\Users\boskom>java -version
java version "17.0.1" 2021-10-19 LTS
Java(TM) SE Runtime Environment (build 17.0.1+12-LTS-39)
Java HotSpot(TM) 64-Bit Server VM (build 17.0.1+12-LTS-39, mixed mode, sharing)
```

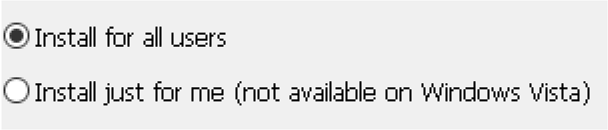
13) Visit the website: https://www.python.org/downloads/windows/

14) Click on ‘Late python 2 Release’

15) Select ‘Windows x86-64 MSI installer’

16) Run the downloaded file

17) Select ‘Install for all users’

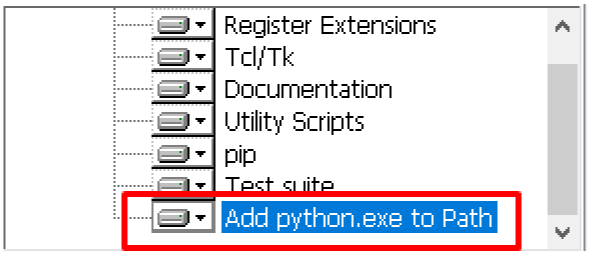


● Install for all users

○ Install just for me (not available on Windows Vista)

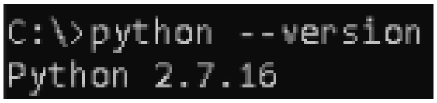
18) Select the default path and click Next

19) Then in the Customize Python screen click on ‘Add python.exe to Path’



Register Extensions
Tcl/Tk
Documentation
Utility Scripts
pip
Test suite
Add python.exe to Path

20) Ensure python is installed by running ‘python2 -version’ in the command line



```
C:\>python --version
Python 2.7.16
```

Usage

Using Docker

1. Ensure Docker is up and running on the system
2. Unzip the program.zip file into a folder
3. Open a command prompt or terminal with its location pointing to the folder containing the unzipped contents of the program.
4. Run the following command to build the GhOST docker image in **Linux**

   ```
   $ docker build -t ghost-image --build-arg USER_ID=$(id -u)
   --build-arg GROUP_ID=$(id -g) .
   ```

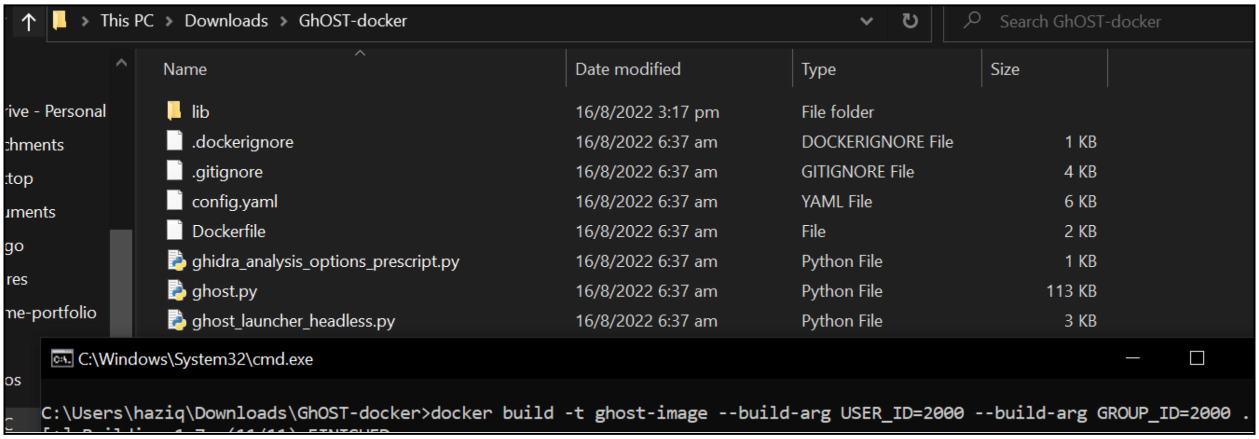
5. Run the following command to build the GhOST docker image in **Windows**

   ```
   $ docker build -t ghost-image --build-arg USER_ID=2000
   --build-arg GROUP_ID=2000 .
   ```

   The user and group ID arguments are only required for Linux. This was added to fix a permissions issue on Linux with the eventual output of the program.

   This is not needed for Windows. However docker is expecting the user and group id arguments. Thus, for Windows, simply defining a random ID such as 2000 is sufficient.

   Example is shown below for Windows.



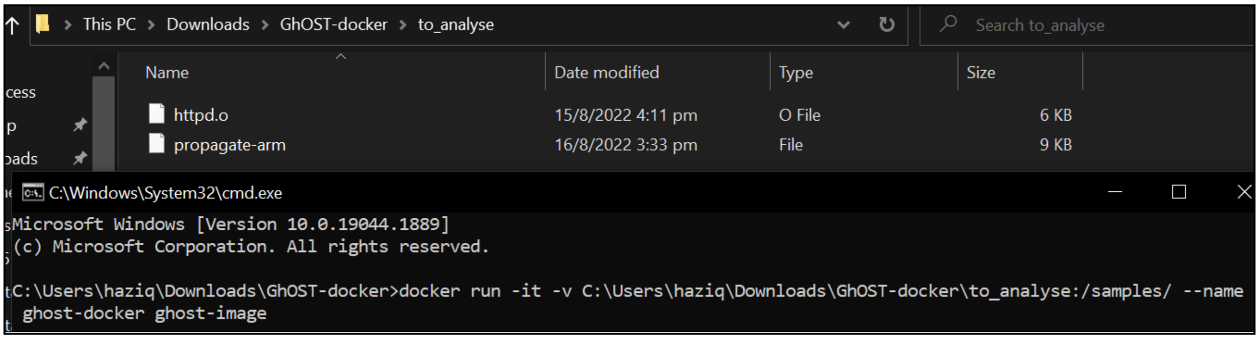
Name	Date modified	Type	Size
lib	16/8/2022 3:17 pm	File folder	
.dockerignore	16/8/2022 6:37 am	DOCKERIGNORE File	1 KB
.gitignore	16/8/2022 6:37 am	GITIGNORE File	4 KB
config.yaml	16/8/2022 6:37 am	YAML File	6 KB
Dockerfile	16/8/2022 6:37 am	File	2 KB
ghidra_analysis_options_prescript.py	16/8/2022 6:37 am	Python File	1 KB
ghost.py	16/8/2022 6:37 am	Python File	113 KB
ghost_launcher_headless.py	16/8/2022 6:37 am	Python File	3 KB

```
C:\Users\haziq\Downloads\GhOST-docker>docker build -t ghost-image --build-arg USER_ID=2000 --build-arg GROUP_ID=2000 .
```

6. Create a folder which will contain the programs to be analysed
7. Run the docker command to launch the image by replacing <path to programs to analyse folder > with the full path to the folder where the programs to be analysed are stored

   ```
   $ docker run -it -v <path to programs to analyse
   folder>:/samples/ --name ghost-docker ghost-image
   ```

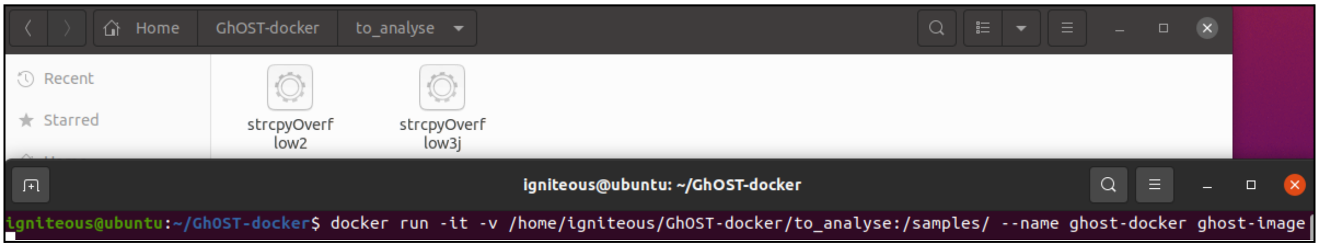
   Example is as shown below where the ‘to_analyse’ folder contains the programs to be analysed.


This PC > Downloads > GhOST-docker > to_analyse
Search to_analyse
C:\Windows\System32\cmd.exe

Name	Date modified	Type	Size
httpd.o	15/8/2022 4:11 pm	O File	6 KB
propagate-arm	16/8/2022 3:33 pm	File	9 KB

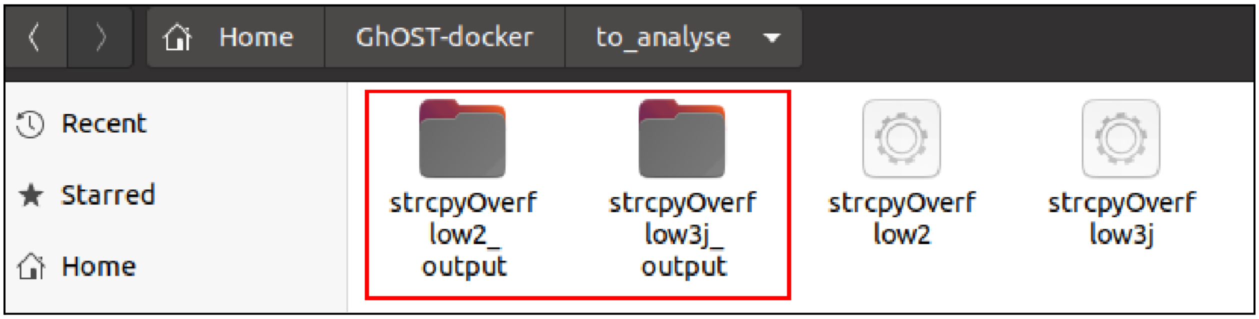
```
Microsoft Windows [Version 10.0.19044.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Users\haziq\Downloads\GhOST-docker>docker run -it -v C:\Users\haziq\Downloads\GhOST-docker\to_analyse:/samples/ --name
 ghost-docker ghost-image
```



```
igniteous@ubuntu:~/GhOST-docker$ docker run -it -v /home/igniteous/GhOST-docker/to_analyse:/samples/ --name ghost-docker ghost-image
```

8. The program should analyse all the files in the specified folder and store the output inside a new folder called <*program-name*>_output as shown below.



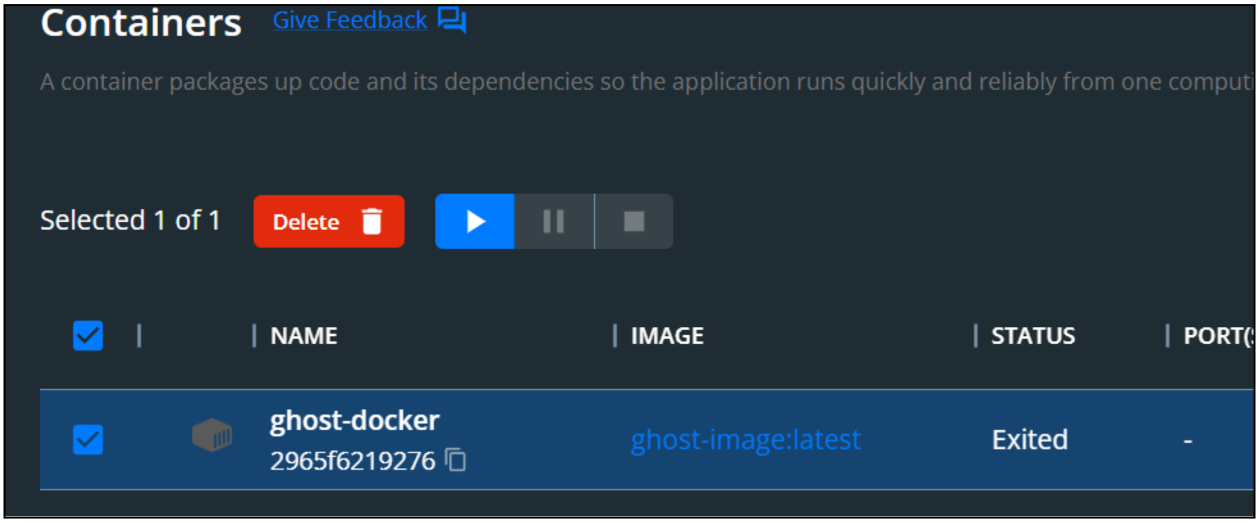
9. If you want to analyse programs again, run the command.
NOTE: If a program which was previously analysed is in the same folder, it will be re-analysed. Please remove such programs and the corresponding output folder before running the following command.

```
$ docker start -i ghost-docker
```

10. To stop the container, run the following command.

```
$ docker rm ghost-docker
```

Alternatively, if on Windows, the container can also be stopped using the Docker Desktop GUI.

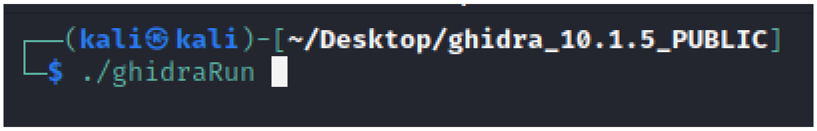


A container packages up code and its dependencies so the application runs quickly and reliably from one computi

☑		NAME	IMAGE	STATUS	PORT(
☑		ghost-docker 2965f6219276	ghost-image:latest	Exited	-

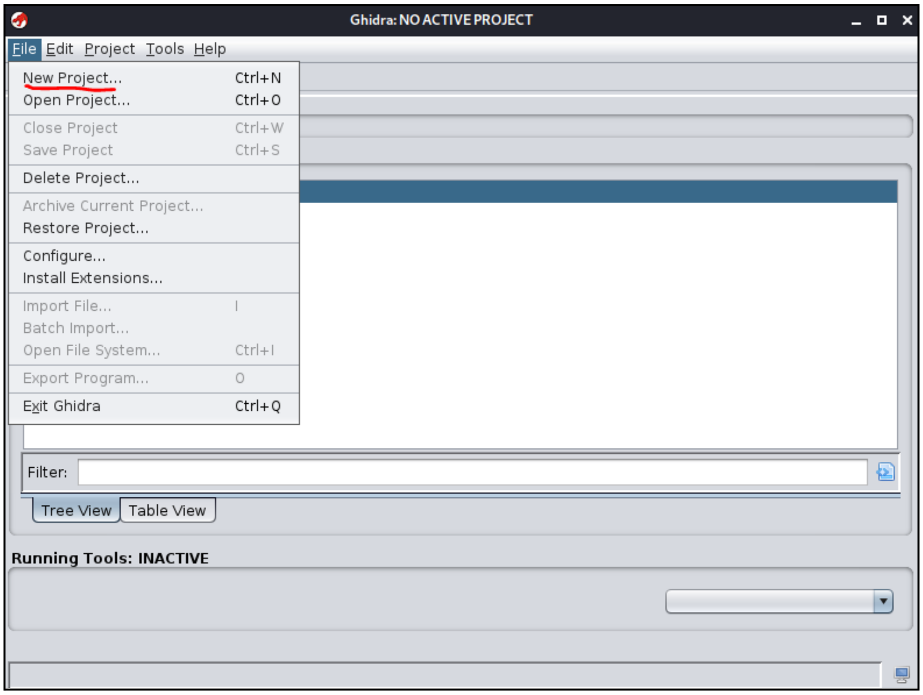
Running Manually through Ghidra GUI

1. Unzip the program.zip into a folder
2. Start Ghidra by running the ghidraRun.bat (**on Windows**)
   or
   ./ghidraRun program through the terminal (**on Linux**)

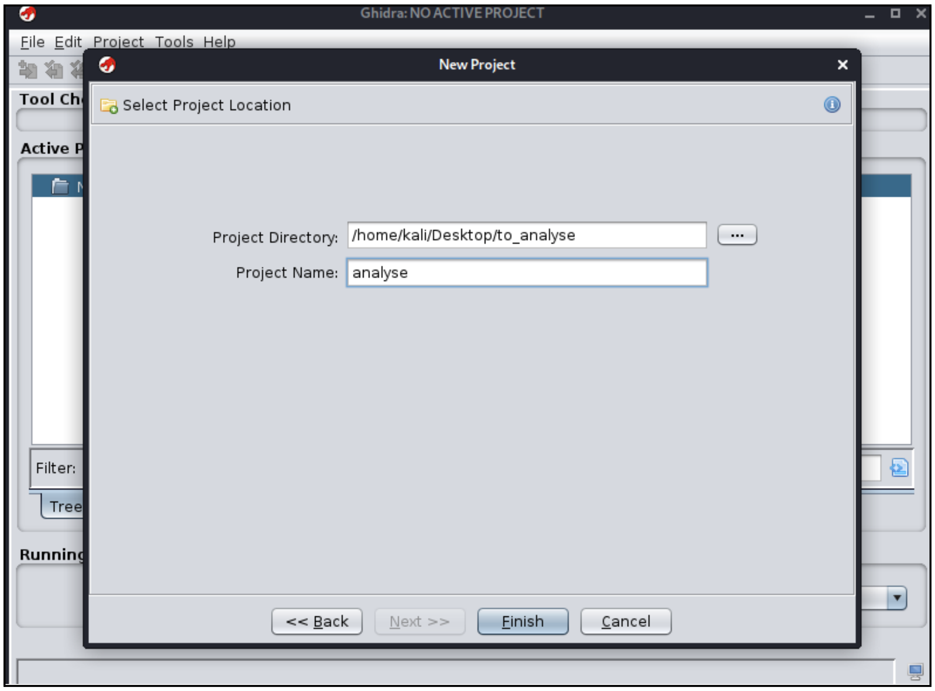


```
┌──(kali㉿kali)-[~/Desktop/ghidra_10.1.5_PUBLIC]
└─$ ./ghidraRun
```

3. Create a new project and import the files to be analysed



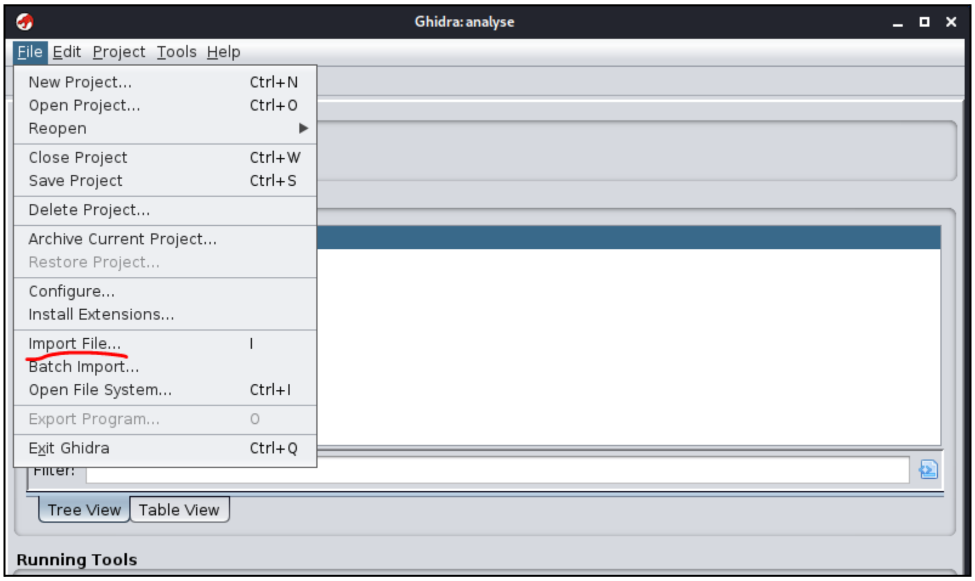
Enter a project directory and name when prompted.



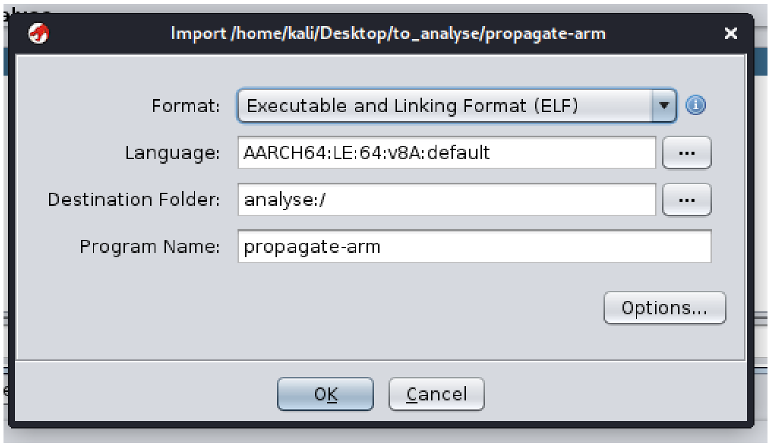
Project Directory: /home/kali/Desktop/to_analyse

Project Name: analyse

Import file which are the programs you want to analyse and run GhOST on.



Click 'OK' when prompted whilst importing



Import /home/kali/Desktop/to_analyse/propagate-arm

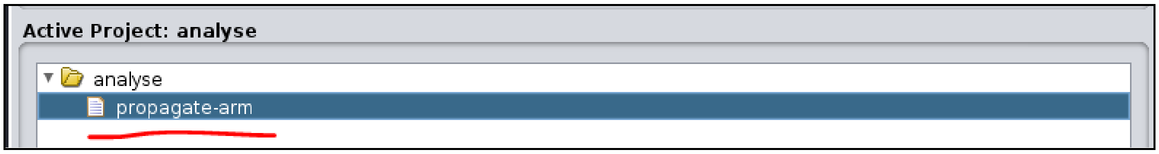
Format: Executable and Linking Format (ELF)

Language: AARCH64:LE:64:v8A:default

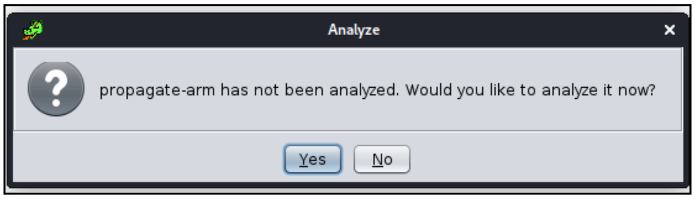
Destination Folder: analyse:/

Program Name: propagate-arm

After successful import, double click on the imported program to open it in Ghidra.

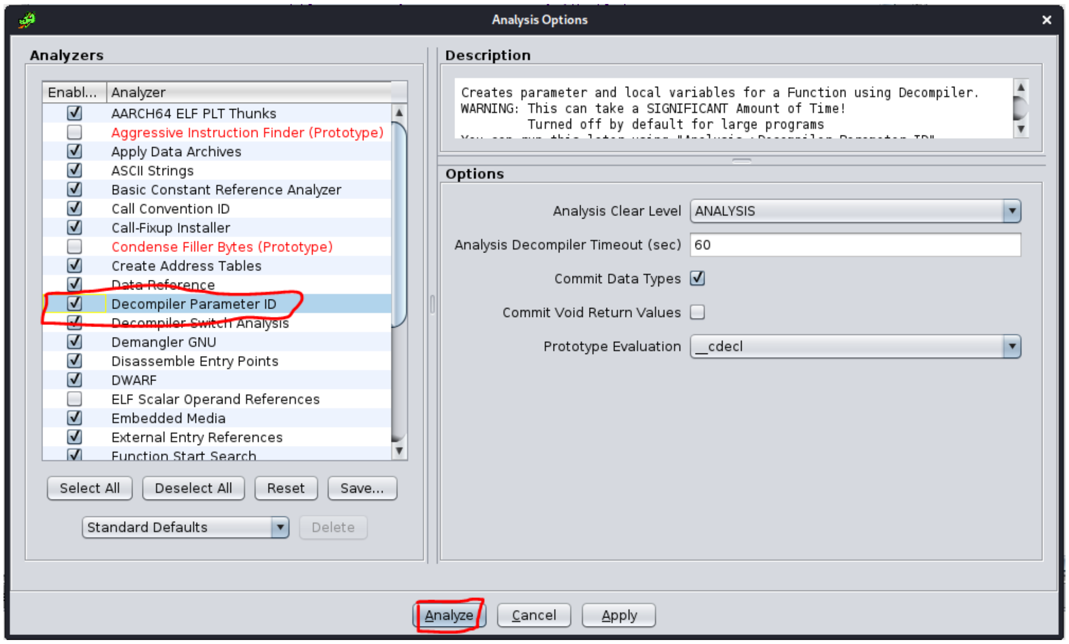


On first launch, it will prompt to analyse the program. Click 'Yes' and another prompt will appear. Enable 'Decompiler Parameter ID' before clicking 'Analyse'



Analyze

propagate-arm has not been analyzed. Would you like to analyze it now?



Analysis Options

Analyzers

Enabl...	Analyzer
☑	AARCH64 ELF PLT Thunks
□	Aggressive Instruction Finder (Prototype)
☑	Apply Data Archives
☑	ASCII Strings
☑	Basic Constant Reference Analyzer
☑	Call Convention ID
☑	Call-Fixup Installer
□	Condense Filler Bytes (Prototype)
☑	Create Address Tables
☑	Data Reference
☑	Decompiler Parameter ID
☑	Decompiler Switch Analysis
☑	Demangler GNU
☑	Disassemble Entry Points
☑	DWARF
□	ELF Scalar Operand References
☑	Embedded Media
☑	External Entry References
☑	Function Start Search

Description

```
Creates parameter and local variables for a Function using Decompiler.
WARNING: This can take a SIGNIFICANT Amount of Time!
         Turned off by default for large programs
You can run this later using "Analysis->Decompiler Parameter ID"
```

Options

Analysis Clear Level: ANALYSIS

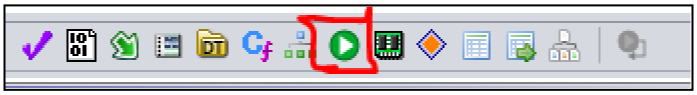
Analysis Decompiler Timeout (sec): 60

Commit Data Types ☑

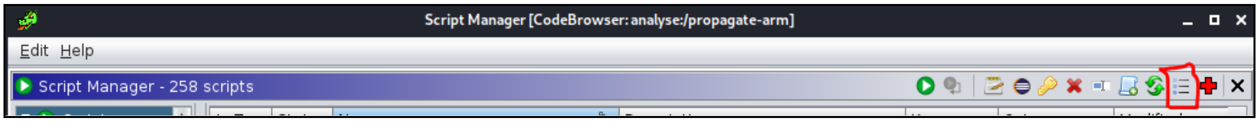
Commit Void Return Values □

Prototype Evaluation: __cdecl

4. Launch the Script Manager by clicking the green play button icon.



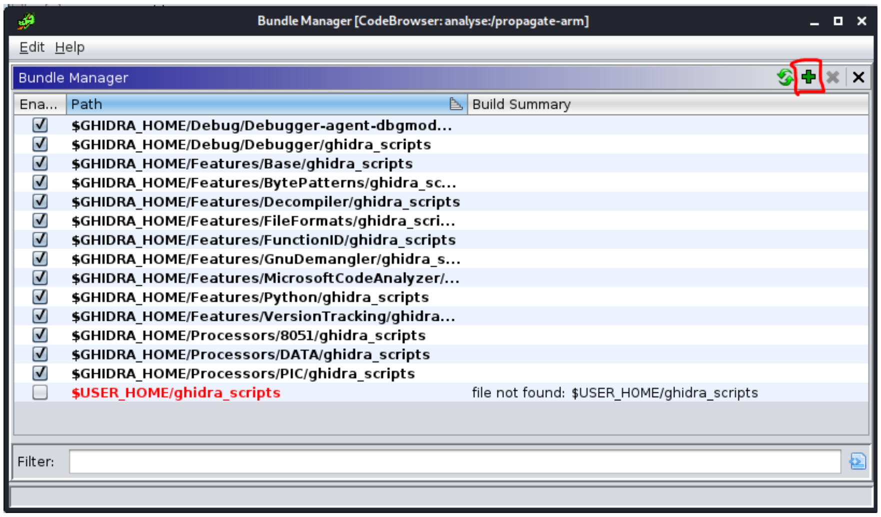
5. Inside the Script Manager, click the bullet point icon on the top bar to open the Bundle Manager



Script Manager [CodeBrowser: analyse:/propagate-arm]

Script Manager - 258 scripts

6. Inside the Bundle Manager, click the green '+' icon to add a new directory for Ghidra to search for scripts.

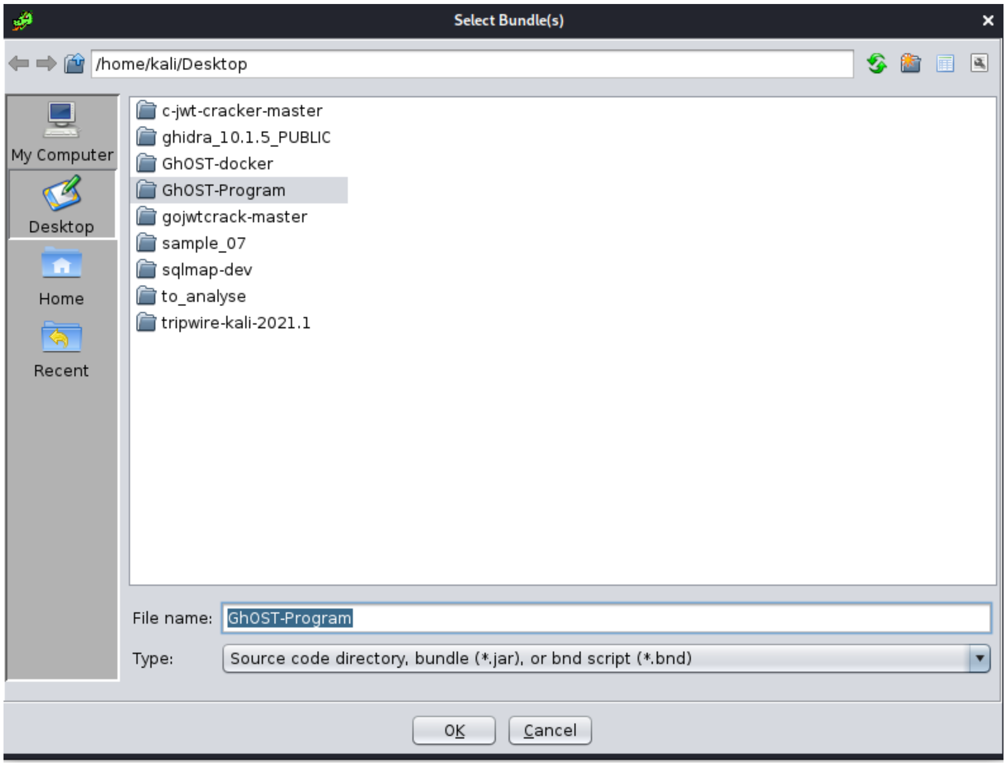


Bundle Manager [CodeBrowser: analyse:/propagate-arm]

Bundle Manager

Ena...	Path	Build Summary
☑	$GHIDRA_HOME/Debug/Debugger-agent-dbgmod...	
☑	$GHIDRA_HOME/Debug/Debugger/ghidra_scripts	
☑	$GHIDRA_HOME/Features/Base/ghidra_scripts	
☑	$GHIDRA_HOME/Features/BytePatterns/ghidra_sc...	
☑	$GHIDRA_HOME/Features/Decompiler/ghidra_scripts	
☑	$GHIDRA_HOME/Features/FileFormats/ghidra_scri...	
☑	$GHIDRA_HOME/Features/FunctionID/ghidra_scripts	
☑	$GHIDRA_HOME/Features/GnuDemangler/ghidra_s...	
☑	$GHIDRA_HOME/Features/MicrosoftCodeAnalyzer/...	
☑	$GHIDRA_HOME/Features/Python/ghidra_scripts	
☑	$GHIDRA_HOME/Features/VersionTracking/ghidra...	
☑	$GHIDRA_HOME/Processors/8051/ghidra_scripts	
☑	$GHIDRA_HOME/Processors/DATA/ghidra_scripts	
☑	$GHIDRA_HOME/Processors/PIC/ghidra_scripts	
□	$USER_HOME/ghidra_scripts	file not found: $USER_HOME/ghidra_scripts

Select the folder where the GhoST program was extracted to in Step 1 and click ‘Ok’



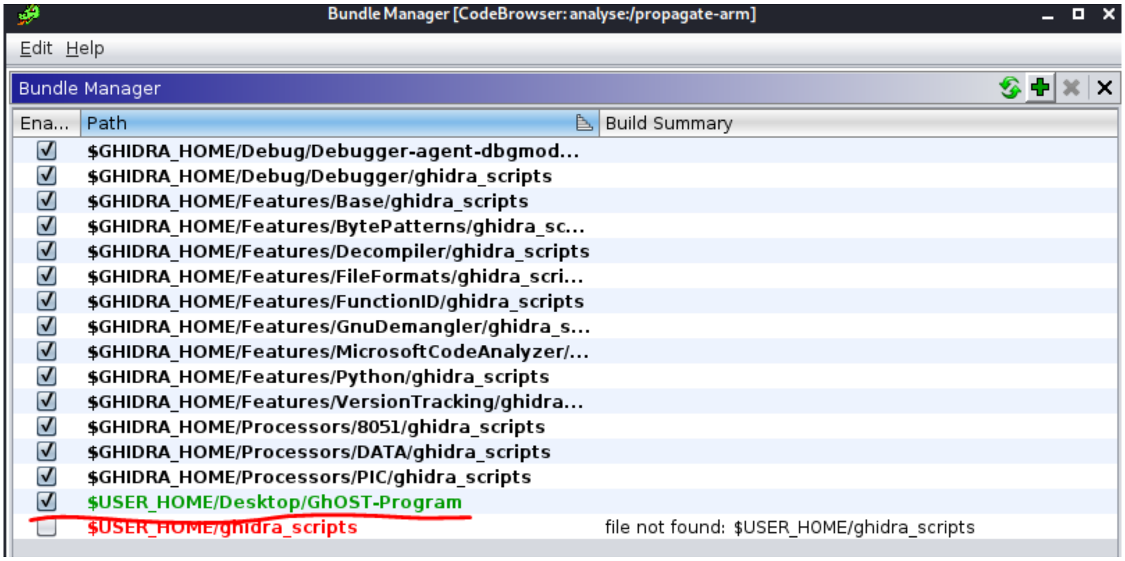
/home/kali/Desktop

- c-jwt-cracker-master
- ghidra_10.1.5_PUBLIC
- GhOST-docker
- GhOST-Program
- gojwtcrack-master
- sample_07
- sqlmap-dev
- to_analyse
- tripwire-kali-2021.1

File name: GhOST-Program

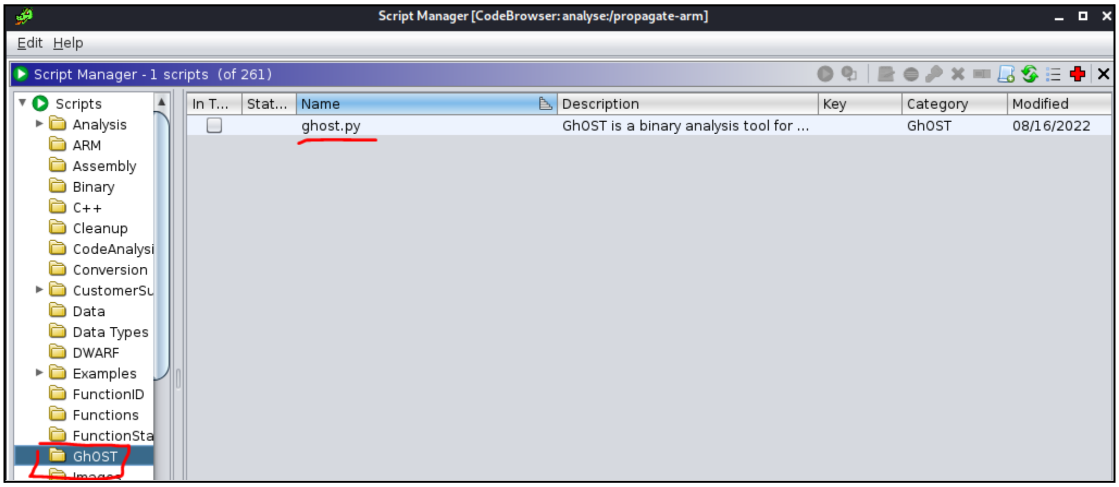
Type: Source code directory, bundle (*.jar), or bnd script (*.bnd)

It should now appear in the Bundle Manager.



Ena...	Path	Build Summary
☑	$GHIDRA_HOME/Debug/Debugger-agent-dbgmod...	
☑	$GHIDRA_HOME/Debug/Debugger/ghidra_scripts	
☑	$GHIDRA_HOME/Features/Base/ghidra_scripts	
☑	$GHIDRA_HOME/Features/BytePatterns/ghidra_sc...	
☑	$GHIDRA_HOME/Features/Decompiler/ghidra_scripts	
☑	$GHIDRA_HOME/Features/FileFormats/ghidra_scri...	
☑	$GHIDRA_HOME/Features/FunctionID/ghidra_scripts	
☑	$GHIDRA_HOME/Features/GnuDemangler/ghidra_s...	
☑	$GHIDRA_HOME/Features/MicrosoftCodeAnalyzer/...	
☑	$GHIDRA_HOME/Features/Python/ghidra_scripts	
☑	$GHIDRA_HOME/Features/VersionTracking/ghidra...	
☑	$GHIDRA_HOME/Processors/8051/ghidra_scripts	
☑	$GHIDRA_HOME/Processors/DATA/ghidra_scripts	
☑	$GHIDRA_HOME/Processors/PIC/ghidra_scripts	
☑	$USER_HOME/Desktop/GhOST-Program	
☐	$USER_HOME/ghidra_scripts	file not found: $USER_HOME/ghidra_scripts

7. Return to the Script Manager and find the program under the GhOST folder

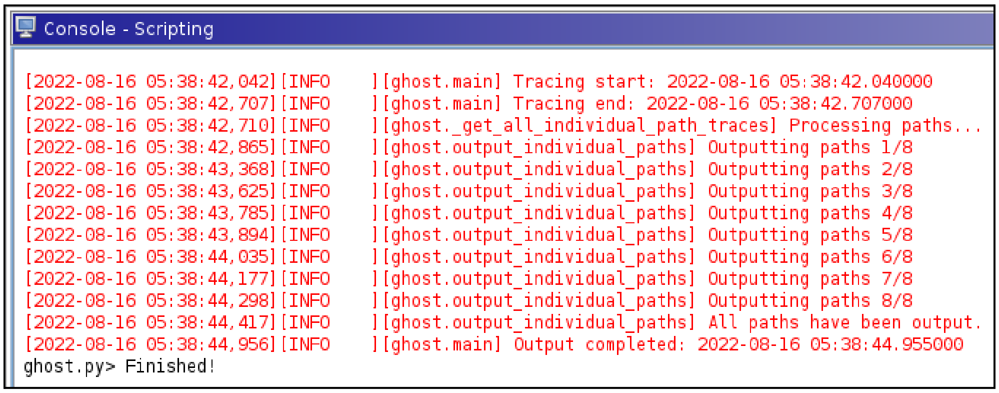


Script Manager [CodeBrowser: analyse:/propagate-arm]

Script Manager - 1 scripts (of 261)

In T...	Stat...	Name	Description	Key	Category	Modified
□		ghost.py	GhOST is a binary analysis tool for ...		GhOST	08/16/2022

8. Double click to run the program and start analysing the imported file.
   View the progress of the tracing on the console.

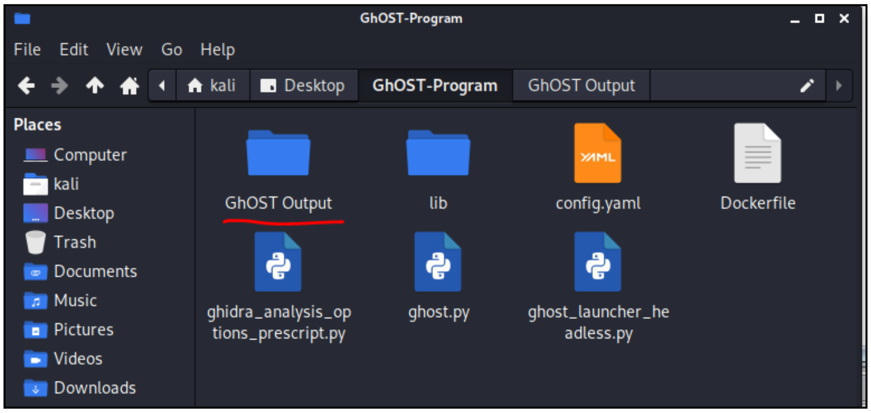


Console - Scripting

```
[2022-08-16 05:38:42,042][INFO    ][ghost.main] Tracing start: 2022-08-16 05:38:42.040000
[2022-08-16 05:38:42,707][INFO    ][ghost.main] Tracing end: 2022-08-16 05:38:42.707000
[2022-08-16 05:38:42,710][INFO    ][ghost._get_all_individual_path_traces] Processing paths...
[2022-08-16 05:38:42,865][INFO    ][ghost.output_individual_paths] Outputting paths 1/8
[2022-08-16 05:38:43,368][INFO    ][ghost.output_individual_paths] Outputting paths 2/8
[2022-08-16 05:38:43,625][INFO    ][ghost.output_individual_paths] Outputting paths 3/8
[2022-08-16 05:38:43,785][INFO    ][ghost.output_individual_paths] Outputting paths 4/8
[2022-08-16 05:38:43,894][INFO    ][ghost.output_individual_paths] Outputting paths 5/8
[2022-08-16 05:38:44,035][INFO    ][ghost.output_individual_paths] Outputting paths 6/8
[2022-08-16 05:38:44,177][INFO    ][ghost.output_individual_paths] Outputting paths 7/8
[2022-08-16 05:38:44,298][INFO    ][ghost.output_individual_paths] Outputting paths 8/8
[2022-08-16 05:38:44,417][INFO    ][ghost.output_individual_paths] All paths have been output.
[2022-08-16 05:38:44,956][INFO    ][ghost.main] Output completed: 2022-08-16 05:38:44.955000
ghost.py> Finished!
```

9. The output will be stored inside the folder where the script is.

   For example, in this case, the script running was stored in the GhOST-Program folder, hence the output will be generated there



GhOST-Program
File
Edit
View
Go
Help
kali
Desktop
GhOST-Program
GhOST Output
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
GhOST Output
lib
config.yaml
Dockerfile
ghidra_analysis_options_prescript.py
ghost.py
ghost_launcher_headless.py