User Manual

Virbox Protector Standalone

Version 1.0

Copyright & Trademarks

Disclaimer

All attempts have been made to make the information in this document complete and accurate. But we cannot guarantee everything is perfect, we will correct it in next version released in case some error has been found. SenseShield is not responsible for any direct or indirect damages or loss of business resulted from inaccuracies or omissions.

The specifications contained in this document are subject to change without notice.

Documentation Improvement

Any suggestion to this manual from you are welcome, We are glad to hear any feedback from you which will help us to continuously improve the documents quality and support and serve the developer to protect software products more efficiently.

Contact

Company: Beijing Senseshield Technology Co., Ltd

Address: Suite 510, Block C, Internet Innovation Center, Building 5, No.10, Xibeiwang East Road, Haidian District, Beijing China

Tel: +86-10-56730936

Fax: +86-10-56730936-8007

Sales: info@senselock.com;

Official Website: https://lm-global.virbox.com/

Virbox Developer Center (Virbox LM): https://developer.lm-global.virbox.com/

About this document

This document is designed to help Software Developer or Publisher to protect their Copyright or IP by protecting their software they would publish. And help the software resource supplier to protect their software resources.

Target User: The operation staff of Virbox Protector Standalone who is responsible for software copyright and IP protection.

Table of Contents

1 Overview 5

1.1 Virbox Protector Standalone Introduction 5

1.2 Advanced and Secured Protection Technology 6

1.3 Working Environment 6

1.4 Installation 8

1.5 License mode of Virbox Protector Standalone 8

1.5.1 License Verification with cloud license (For Trial User) 9

1.5.2 License Verification with soft license (For official user use soft license) 10

1.5.3 License Verification with El5 dongle (For official user use dongle license) 16

2 Getting Started 17

2.1 Main Menu of Virbox Protector Standalone 17

2. 2 Menu Bar 17

2.2.1 File 17

2.2.2 Protect 18

2.2.3 Plugin 19

2.2.4 Log 19

2.2.5 Setting 19

2.2.6 Help 20

2.3 File Panel and Protection Panel 20

2.3.1 File Panel 20

2.3.2 Protection Panel 21

3. The Principle of Software Protection 32

3.1 Protect the executable file and DLL lib 32

3.2 Protect the parse software and data resource file 32

3.3 Make the protection scheme for your software 33

4 Protection Example & Use Case 36

4.1 Windows Application .EXE or .DLL file protection 36

4.2 Java program, Jar archive, War archive Protection (Resources Protection) 38

4.2.1 Protect the .Jar archive. 42

4.3 Unity 3D Program Protection 44
4.3.1 Introduction 44
4.3.2 Protection Principle Overview 45
4.3.3 Source code Protection 45
4.3.4 Resources protection 46
4.4 Android Unity3D software protection 50
4.5 Software based on python protection process 51
4.6 Protect software in command line 53
5. SDK label 55
5.1 protect software by programming 55
5.2 How to encrypt and decrypt the string by SDK 56
6 Note 57
7 FAQ 58
7.1 What is the difference between the soft license version and dongle version? 58
7.2 What is the difference between the trial version and standard version? 58
7.3 How to generate a map file? 58

1 Overview

1.1 Virbox Protector Standalone Introduction

Virbox Protector Standalone, is the latest Protector and wrap tool to software developer to protect their software copyright and IP which integrated with multi encryption and protection technology: VM, Obfuscation, Smart compression, Data and resource protection, Anti-Hardware breakpoint, Anti-Memory breakpoint, Enable Memory Check, etc. It is the powerful protector for software developer to protect their software and critical code, algorithm without additional coding, with easy to use and effortless feature.

Virbox Protector Standalone is suitable for the following scenarios and software developers:

1. Software developer has established the third party license system or self-developed license system; with Virbox Protector Standalone, Developer may enhance the security level of software and integrated with existed license system;
2. The software program needs to be protected and distributed to software users without licensing to the software user. Developer just need use Virbox Protector Standalone to protect the software and distribute to targeted software user.
3. What is difference between Virbox Protector and Virbox Protector Standalone?

   Virbox Protector, to be a highly secured, easy to use and without code effort protection wrap tool, is one of critical component in Virbox LM solution, software developer use Virbox Protector to protect software and use Virbox LM (Virbox Developer Center) or Virbox Developer Utility to issue the license to the protected software and distribute the software and license to authorized software user.

   So, software developer may choose either Virbox Protector or Virbox Protector Standalone to protect software according to the software applied scenario.
4. Virbox Protector Standalone will only protect the software you currently protect. And would not have influence on the software execution or interrupt of lib you called, like the blow figure showing.

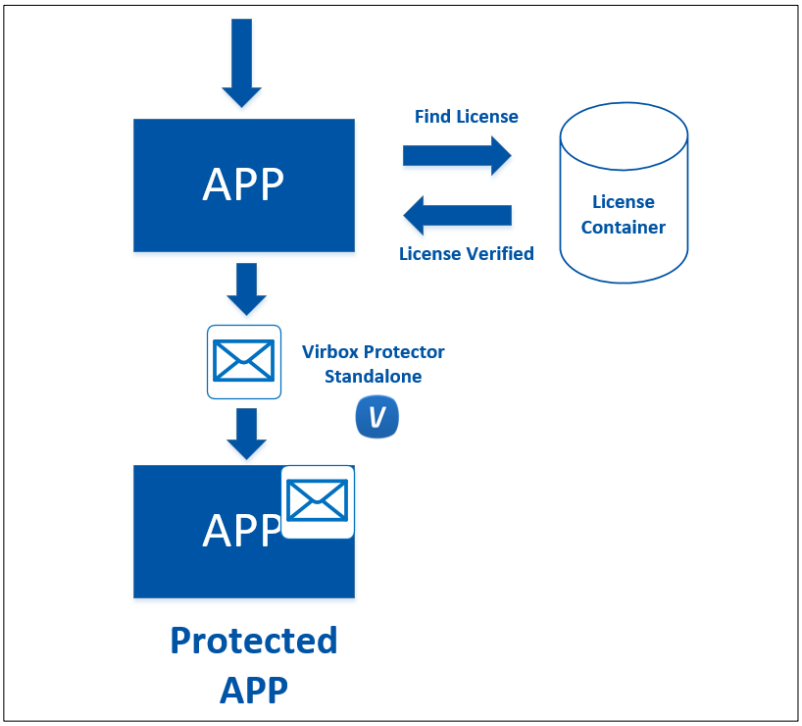


Figure 1

1.2 Advanced and Secured Protection Technology

- ***Advanced Obfuscation***: Advanced obfuscation functions supported to protect code, critical algorithm etc.
- ***Virtualization :*** Code Virtualization & Secured VM function available, the protected source code is translated into Secured Virtual Machine code and executed inside of VM; In combined with Obfuscation technology, it is effective way to defense static analysis tools to debug, reverse engineering the source code.
- ***Smart Compression:*** High efficiency Compression tools to developer with high performance, powerful shield to against hacker tools and effectively to prevents de-compilation of .NET, PE programs; effective to defense the crack tools and also keep small size of the program after protection.
- ***Multi Encryption Scheme*** to the selected functions, coding to be protected.

1.3 Working Environment

The Operation System we support

- Windows: Windows 7 and above version
- Linux: CentOS, Ubuntu, Debian-9.4.0

- Mac: OX 10.4 or above version
- Android System
- ARM Linux V7/V8

Virbox Protector Standalone has different version release and execute in above work environment. Please clarify your working environment with Virbox team before your apply trial license.

The Protected program language

C, C++, Java, Delphi XE7 or above version, PB, BCB, C#, VB6.0, Python, Lua, Perl, R, Ruby, PHP

The plugin and framework support:

AutoCAD ARX, Revit, Unity 3D, Unreal Engine 4, .NET

Development Tool support

MATLAB, LabView

Executable file & Driver support

32 bit/64 bit executable file and dynamic link library (DLL) & Driver program

Software Protection & Evaluation Process

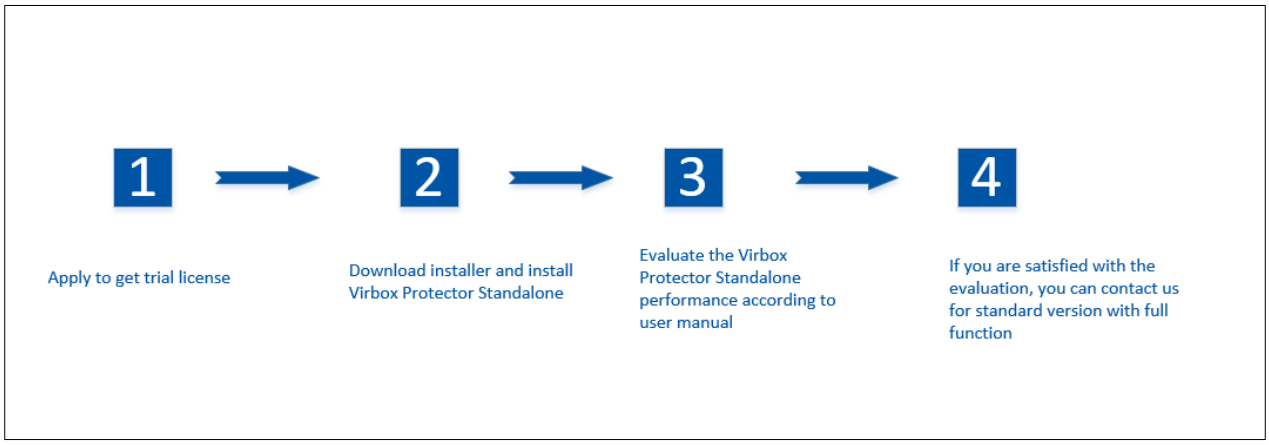


Figure 2

1. Apply to get trial license for Virbox Protector Standalone;
2. Download the installation package, and install trial version in your computer;
3. **Protection and Performance evaluation:** protect your software or data resource with Virbox Protector Standalone to evaluate the protection scheme and performance according to the instruction of User Manual;

4. If you are satisfied with the protection evaluation, you can purchase a standard version with complete package.

1.4 Installation

After the installation of the Virbox Protector Standalone, you will see two software are installed. **Virbox Protector Standalone & Virbox User License Tool**. Virbox User License Tool is the License Verification tool. You need to activate your Virbox Protector Standalone license and verify the license via Virbox User License Tool before protect your software/program.

Figure 3

1.5 License mode of Virbox Protector Standalone

Virbox Protector Standalone supports following license mode to software developer to choose when they apply trial and evaluate Virbox Protector Standalone performance or purchase Virbox Protector Standalone later:

Trial License: Cloud based license; which is most easier way to software developer to apply and get the Virbox Protector Standalone's trial license by sign up with your account ID via apply link;
Trial license for Virbox Protector Standalone will be valid within ***30 days***, The software protected by trial version would be expired in ***7*** days; Up to ***5 functions*** can be protected in the application by trial version, no limitation by standard version;

For official Virbox Protector Standalone user (software developer), they can select either soft license or dongle based license according to their requirement;

Soft license: Support both account based license and license code;
Dongle License: Use Virbox El5 to be the License container of Virbox Protector Standalone, developer can use Virbox Protector Standalone at designated computer which plug in EL5 Dongle;
Both License modes support subscription and perpetual license for Virbox Protector Standalone

1.5.1 License Verification with cloud license (For Trial User)

Open Virbox User License Tool, sign in your account to verify the Virbox Protector Standalone License, then you can open and use the Virbox Protector Standalone to test or evaluate software protection performance to your software.

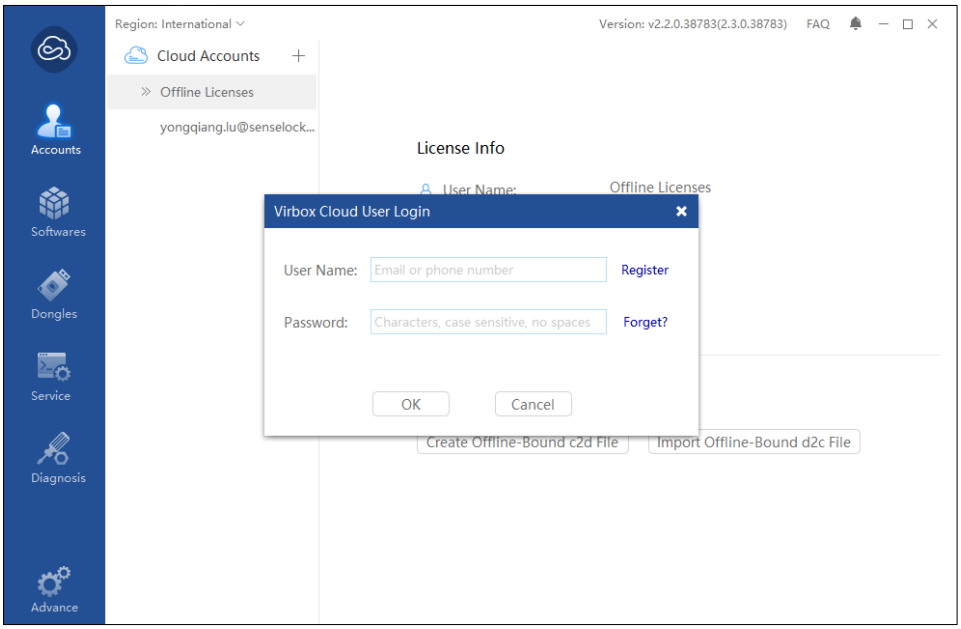


Figure 4

After sign in the account, you can check the detail information of the license here showing in the picture:

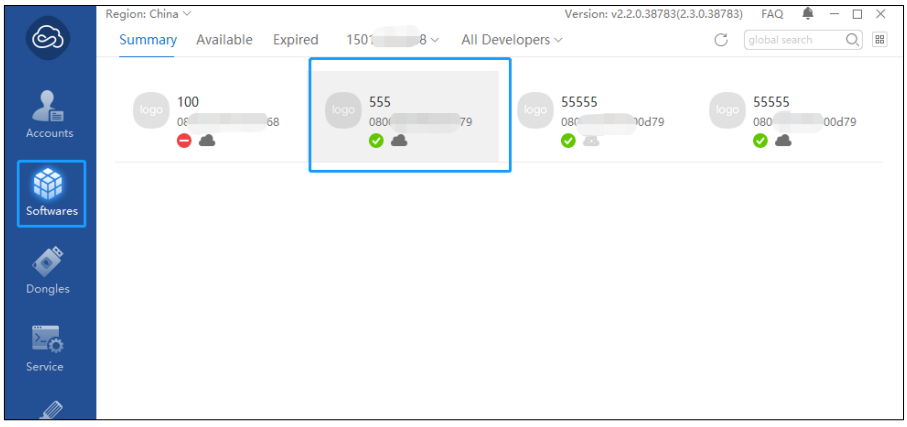


Figure 5

1.5.2 License Verification with soft license (For official user use soft license)

1.5.2.1 Use Virbox Protector Standalone in online environment

When you use the Virbox Protector Standalone in online environment, you can sign in the account that have already issued license. After you start Virbox Protector Standalone, the software license will bind to your hardware machine automatically.

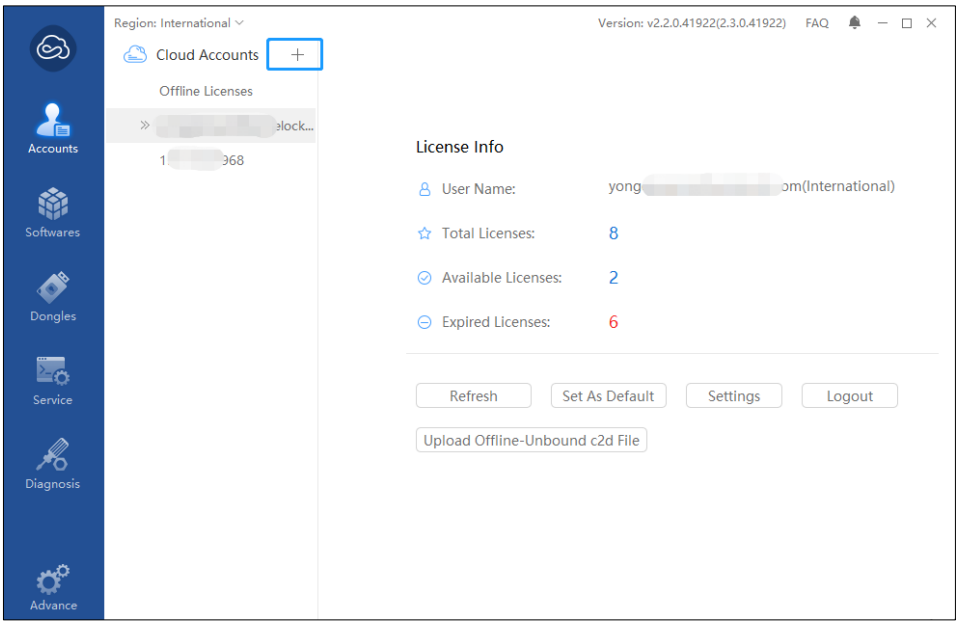


Figure 6

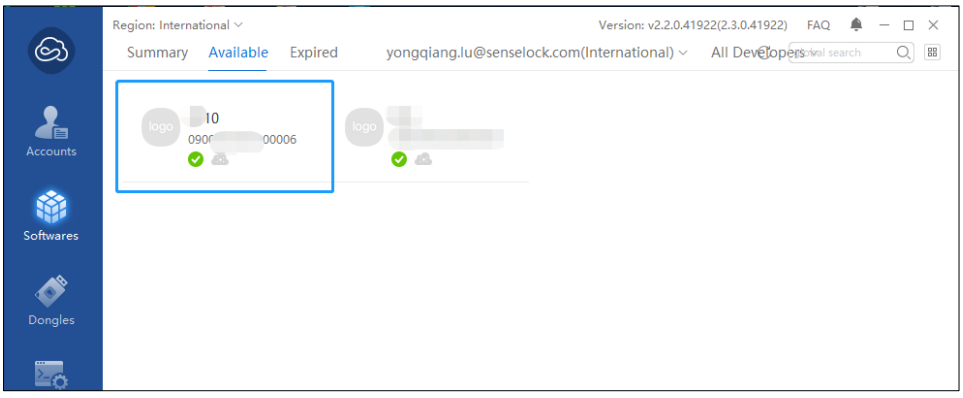


Figure 7

1.5.2.2 Use Virbox Protector Standalone in offline environment

If you use Virbox Protector Standalone in offline environment, you need to use the following step to bind the license to your offline machine with a computer that can connect to network (Online computer). Both computer need to install Virbox User License Tool.

- **Generate c2d file on the Offline computer**

Open Virbox User License Tool, click "**Accounts**",

Click "Offline",

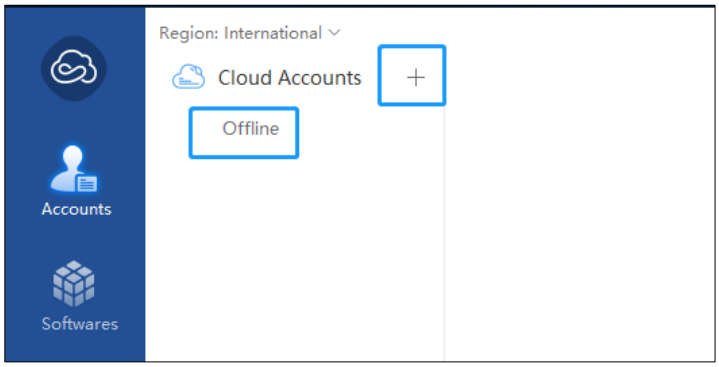


Figure 8

Generate offline bind c2d file, and save the .c2d file.

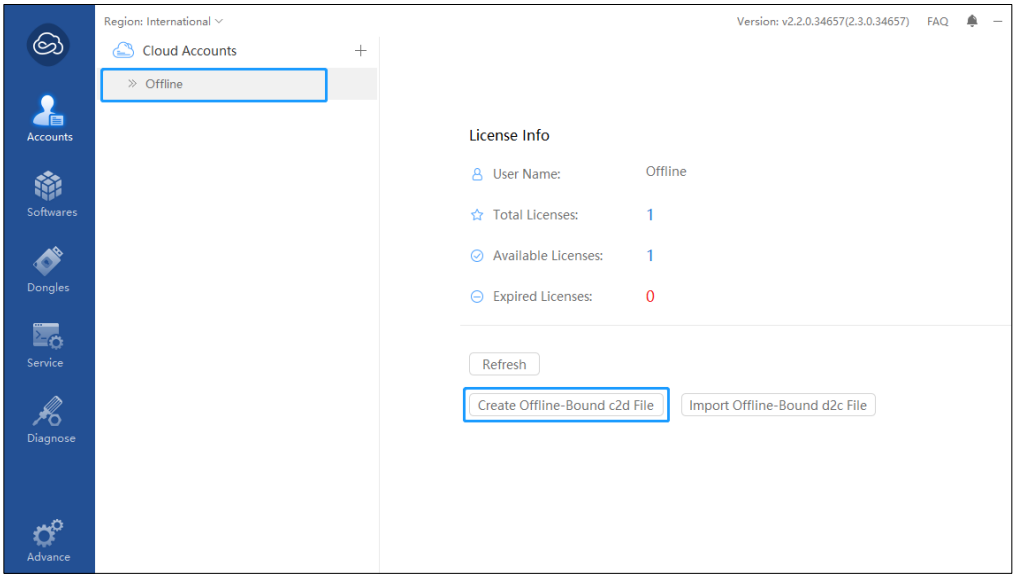


Figure 9

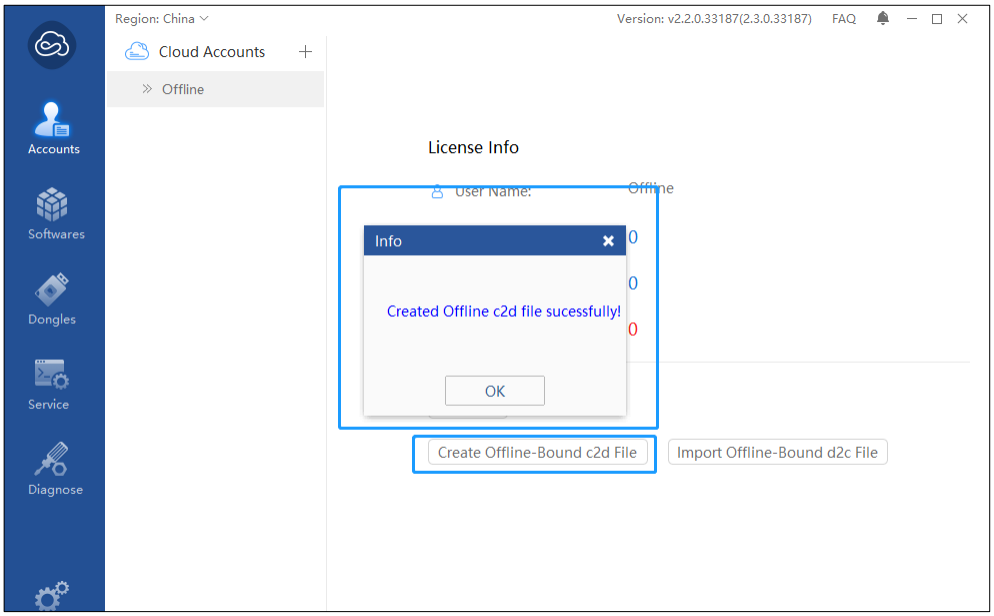


Figure 10

After you have created c2d file successfully. You need to copy this c2d file to online computer.

- **Create d2c file on the computer Online**

Also need open Virbox User license Tool on online computer.
Click "**+**" to login your account that have already have license.

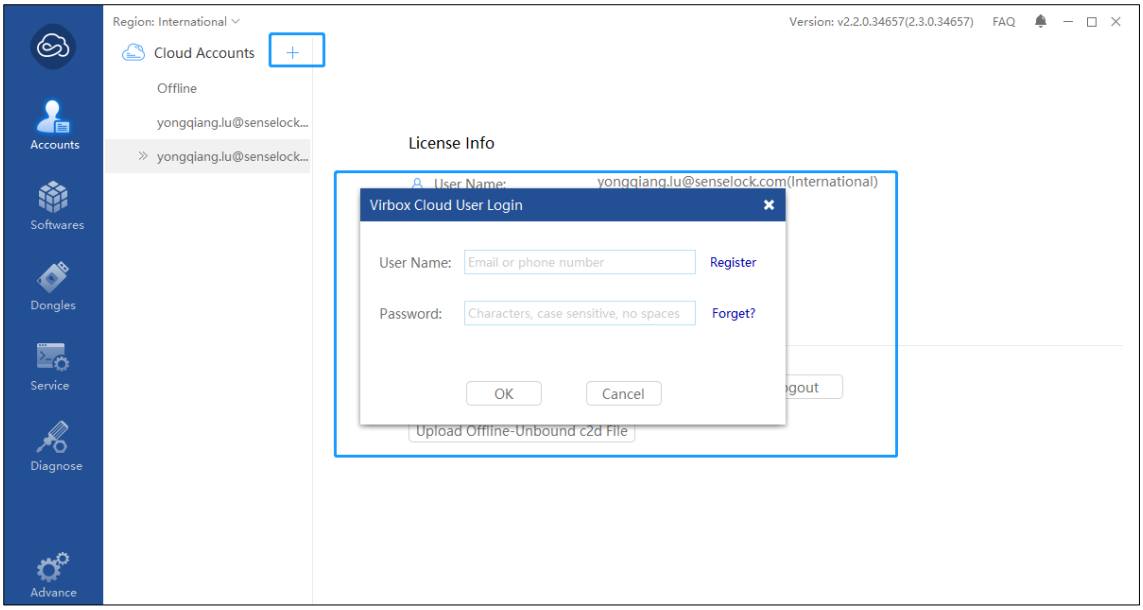


Figure 11

Click "**Software**",

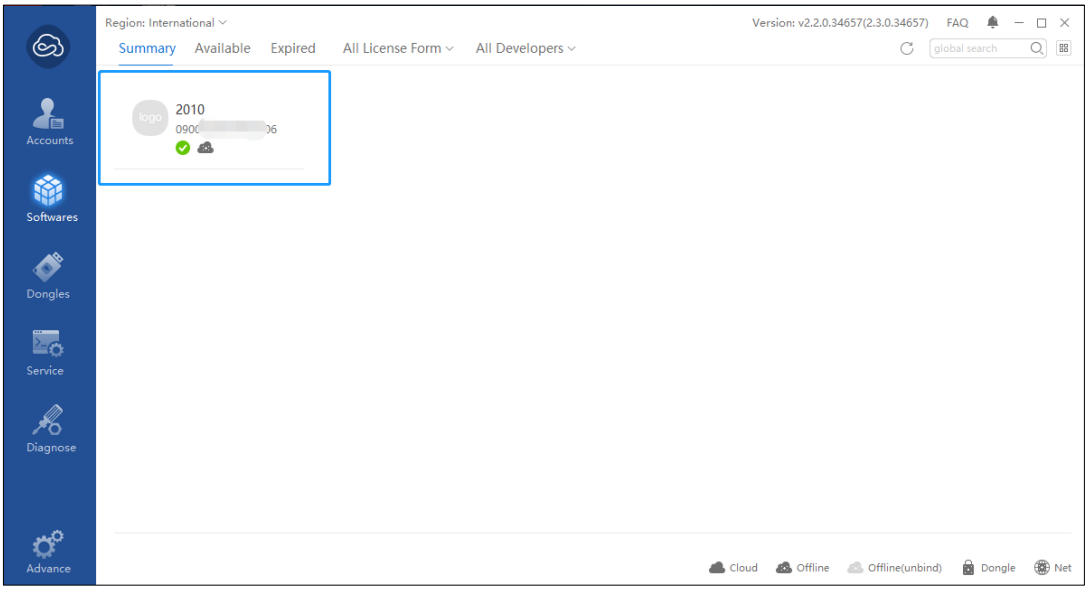


Figure 12

Double click the license, the detail information of the license will show:

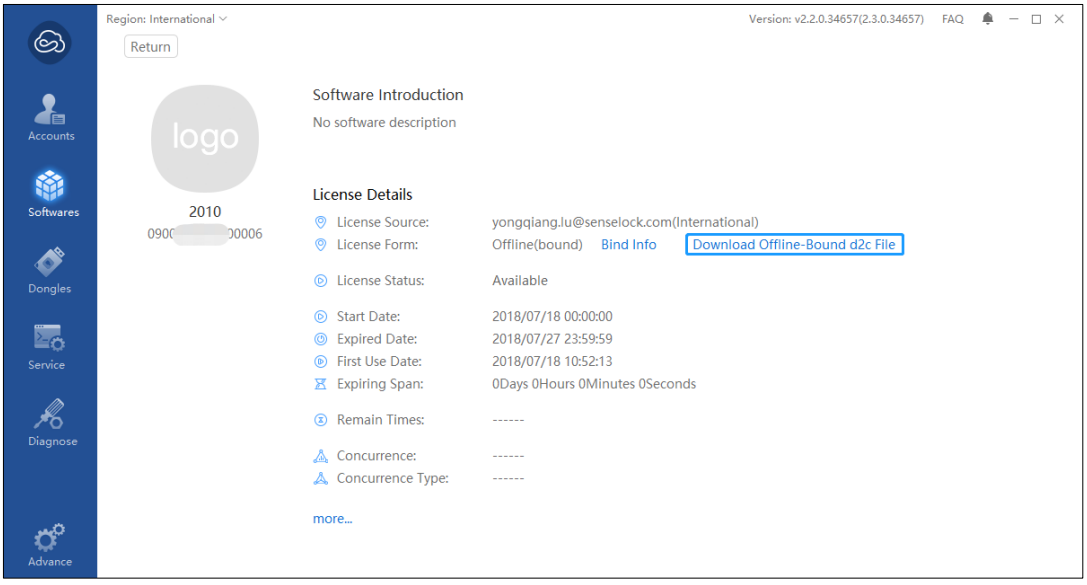


Figure 13

Click "**Download Offline Bound d2c file**"

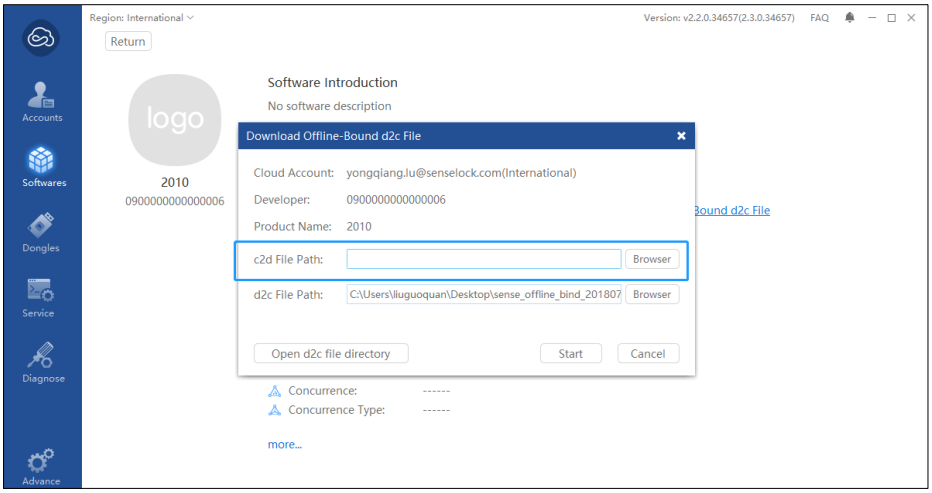


Figure 14

Selected the **c2d** file you generated from last step on the offline computer, software user need to copy it here. Click "**Start**",

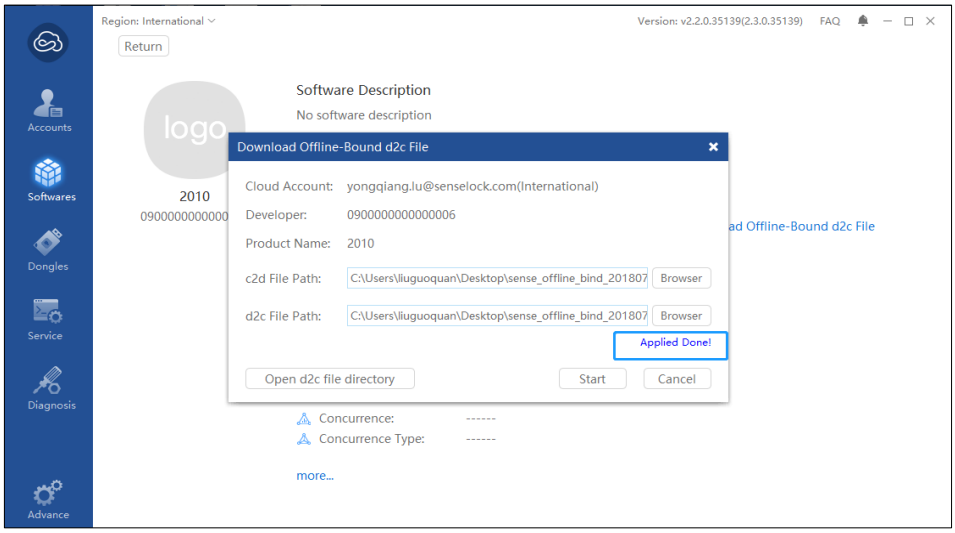


Figure 15

You can select the path to generate d2c file, here I put it to desktop. If the file is generated successfully, it will show "**Applied Done**" like in the picture above.

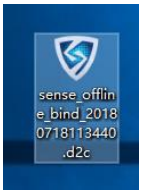


Figure 16

Note: 1. Click "**open d2c file directory**", also will show the path of the generated file. 2. The valid time of this d2c package is 24 hours, please complete binding timely.

- **Verify d2c file on the Offline computer**

Now we need to copy d2c file to the computer offline and complete license verification.

Copy the **d2c** file generated from the computer (Online computer).
Import it in to the offline computer.

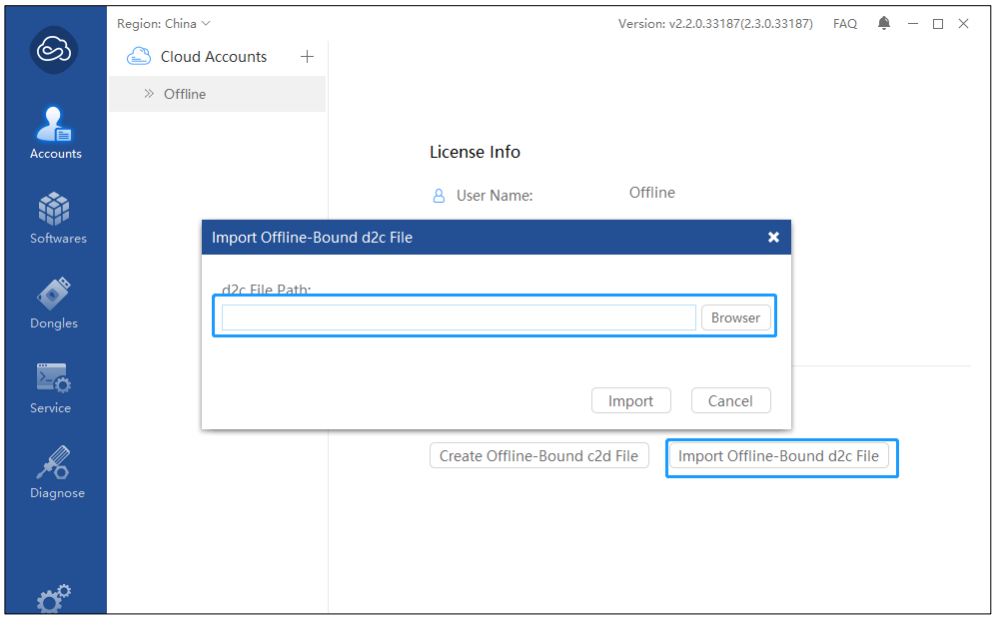


Figure 17

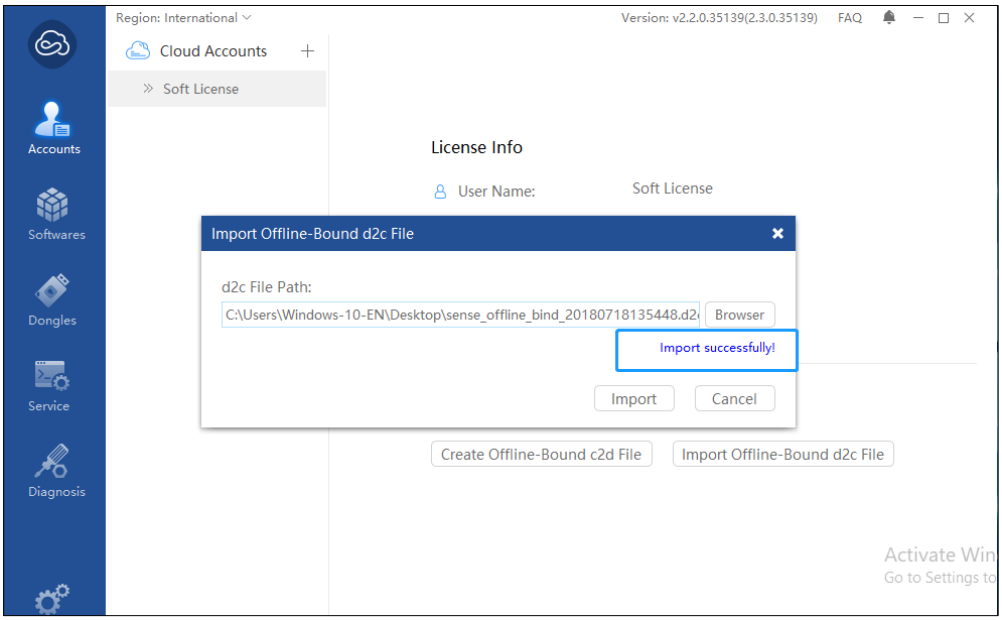


Figure 18

It will have "**Import successfully**" message after you imported the file successfully.

1.5.3 License Verification with El5 dongle (For official user use dongle license)

If you purchased the Virbox Protector Standalone with a Virbox El5 dongle, after installation you need to insert the dongle on your PC for license verification. Then you can use Virbox User License Tool to check the license you have subscripted. As the figure shown below:

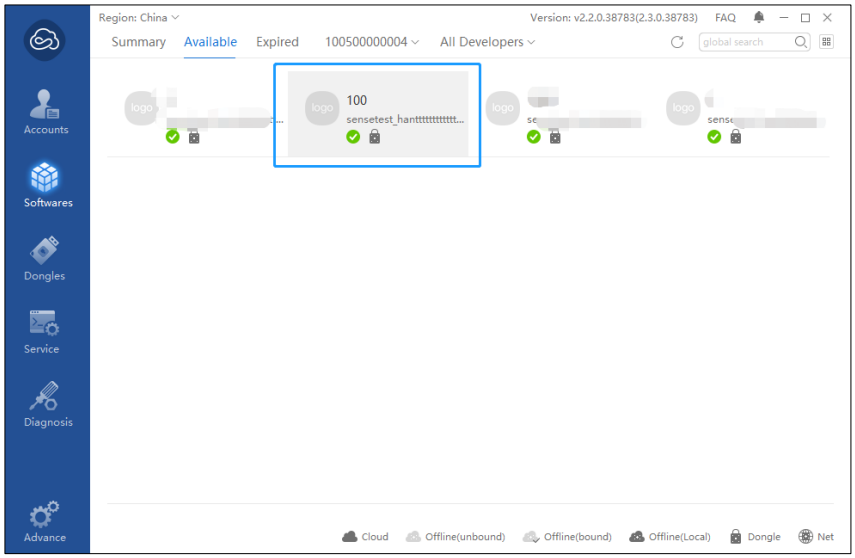


Figure 19

You can double click that dongle icon for license detail information.

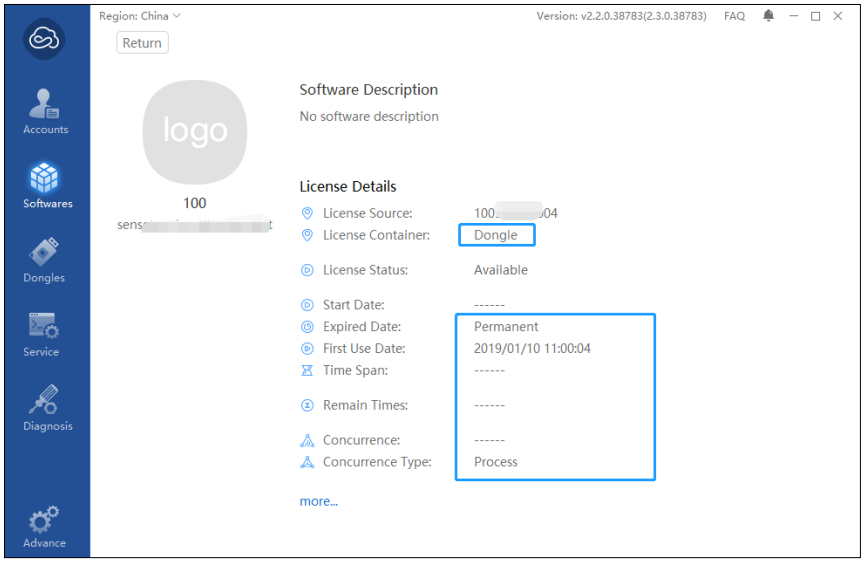


Figure 20

2 Getting Started

2.1 Main Menu of Virbox Protector Standalone

The main menus shown as below: includes 3 areas:

Menu Bar: consist of: File/Protect/Plug-in/Log/Setting/Help functions;

Tool Bar: Open File/ Save Selected Configuration/Save All Configuration/Protect Selected Projects/Protect All Projects;

File/Directory Panel and **Protection Panel**

These functions and options in the menu, Tab and Panels will be introduced and explained in this chapter.

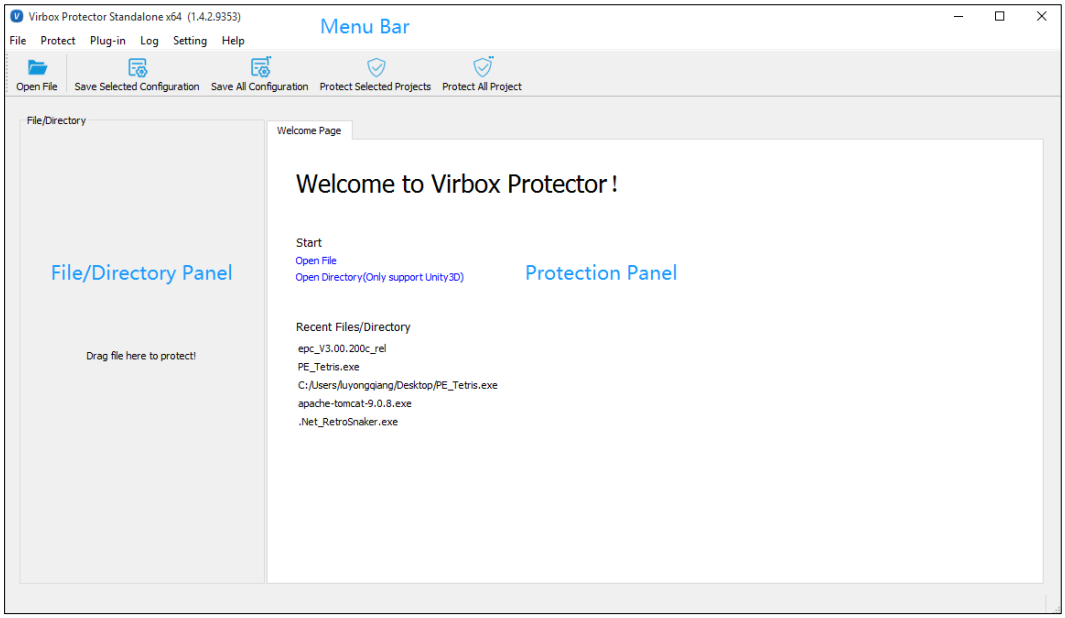


Figure 21

2. 2 Menu Bar

2.2.1 File

Open File: Click "**Open File**", you can select .Net, PE, ELF, MachO, Arm Linux and Android .so lib file. And load the selected files into the left panel, the File/Directory Panel.

Note: If the xxx.map file located in the same directory of the program file being protected, these xxx.map file will be loaded with the program file automatically. And the name of the functions will also be loaded and listed in the File Panel. The map file generated by VS, VC, BCB, Delphi compiler is supported at present.

Open Directory: Here you can open a whole directory, to open Unity3D directory only.

Recent/Batch Projects: Here you can reopen the recent protection project quickly, or batch file protection project. Up to 5 recent projects can be recorded.

The recent protected program would be loaded and listed into the File Panel.

If you want to save the project setting and path of multiple file, you can save those configuration into a project file **xxx.vbpsln** by clicking "**Save Batch/project**". Then you can reload this project file later.

Save Batch Projects: You can use this function to save all of path of the file, but the configuration would not be saved. If you have changed the configuration and want to save them, you need to click "save the selected configuration" or "save all of the configuration".

When you reopen the Virbox Protector Standalone, you can drag in xxx.vbpsln to open the project, the saved file and configuration would be loaded if the location of the file haven't changed.

Exit:

Close Virbox Protector Standalone and exit.

2.2.2 Protect

Parse selected project (File):

Select one or multi file which listed in the File Panel, you can parse these file by clicking "**parse selected project**" button. The file need to be parsed correctly before protection.

Parse all project

Parse all of the files in the project, no matter how much you have selected.

The purpose of parsing is to reload the configuration status you saved.

Save selected configuration

Configuration means the function options, protection options, which you selected to the protected file,

You can save the configuration of the Function options, Protection options, Message by clicking "save selected configuration"

Save all configuration

Save all of the protection configuration of the project, no matter how many file you have selected. Corresponding error report or error code will show, if the configuration is not correct and you can't save the configuration.

Protect selected project

You can protect the selected file in the file list by clicking this option. If the configuration is not correct, it will

remind you corresponding error report or error code.

Protect all project:

No matter how much file you selected in the file list, you can protect all the file by clicking this option.

2.2.3 Plugin

Open DSProtector, which is the plugin tool for data resources protection, like jar archive, .py file, etc.

DSProtector is data security protection plugin unit (Hereinafter referred to as DS Protector) is plugin unit provided by Virbox, software developer may use DS Protector to protect data file and encrypt related data resources together with protected software program.

Please noted that DSProtector do not support the data resources protection which from Linux and Mac system currently.

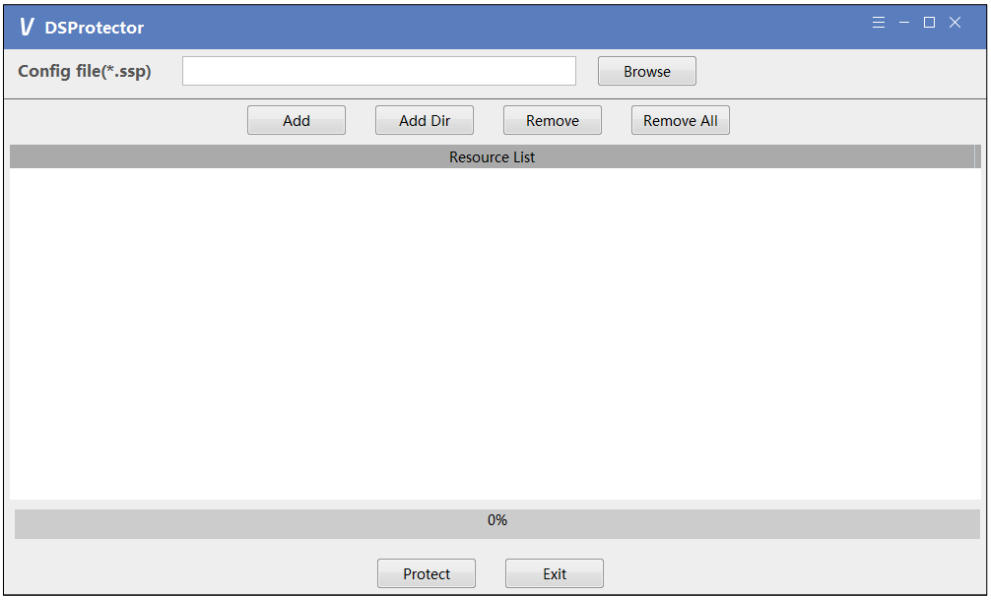


Figure 22

2.2.4 Log

Show log dialog

Log dialog will show the log file when you are protecting the software. You can save the log by clicking “save”, to save the log to other directory.

Open local log directory: Open the log directory.

2.2.5 Setting

Language setting:

Chinese and English is supported. To change the language of the interface of the software you need to restart the software. You can restart instantly or next time you open the software.

2.2.6 Help

About: It will show you the technical support email and website.

2.3 File Panel and Protection Panel

2.3.1 File Panel

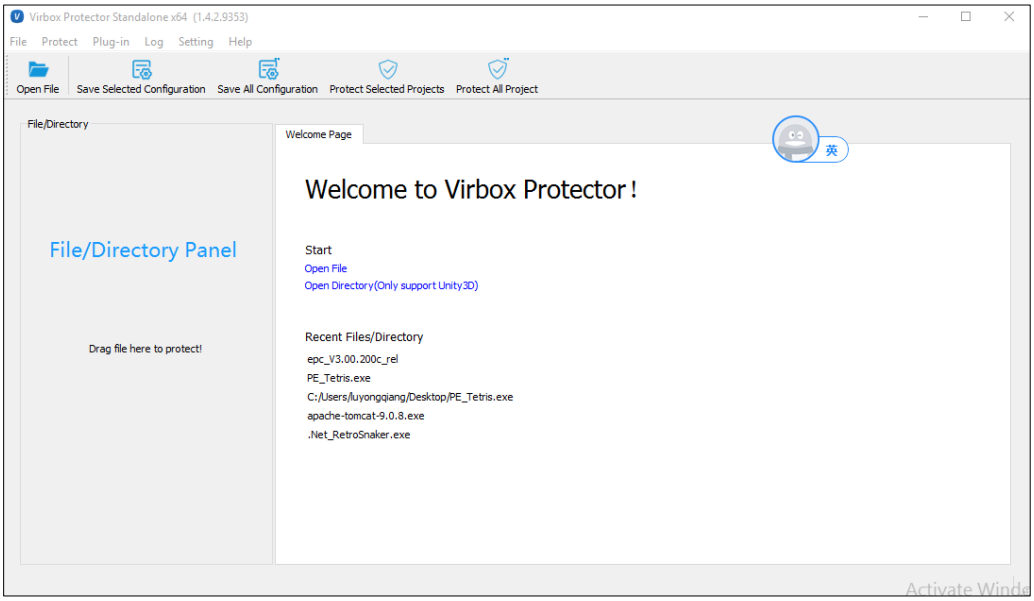


Figure 23

After you drag the software to be protected in to the file panel, the software basic information will show in the Basic info page.

You can select one or more software and right click the software to select the corresponding function.

- Parse (software or file)
- Save configuration
- Protect software
- Show contained sub folder
- Set output directory for protection
- Copy the protection option of this file to another selected files:

  Select 2 more software, right click software and choose “copy the protection option of this file to other selected files”, and use this setting to other software, the other software will have the same configuration.

- Close project:

  Right click the selected software, and choose close, you can close the program with saving the current configuration and also can exit without saving, or cancel the operation.

2.3.2 Protection Panel

- Basic info
- Function Option
- Protect Option

Basic Info

Basic info will show you the basic information of the loaded software, File/directory path, file creation time, Last configuration Modified Time, Last Accessed Time, Application Type (PE or .Net).

Function Option

Function Option page lists all the functions in your application, you can select and protect functions in your application or program in this page, you can select Virtualization, Obfuscation, Code Porting (Snippet) and Code encryption mode to protect the selected functions. When you click the function in the software, the protection type, function name, function address and assemble code will show in this page. And the total functions quantity and total protected functions and the quantity of every function protection type would also be shown in this page.

As shown the figure blow:

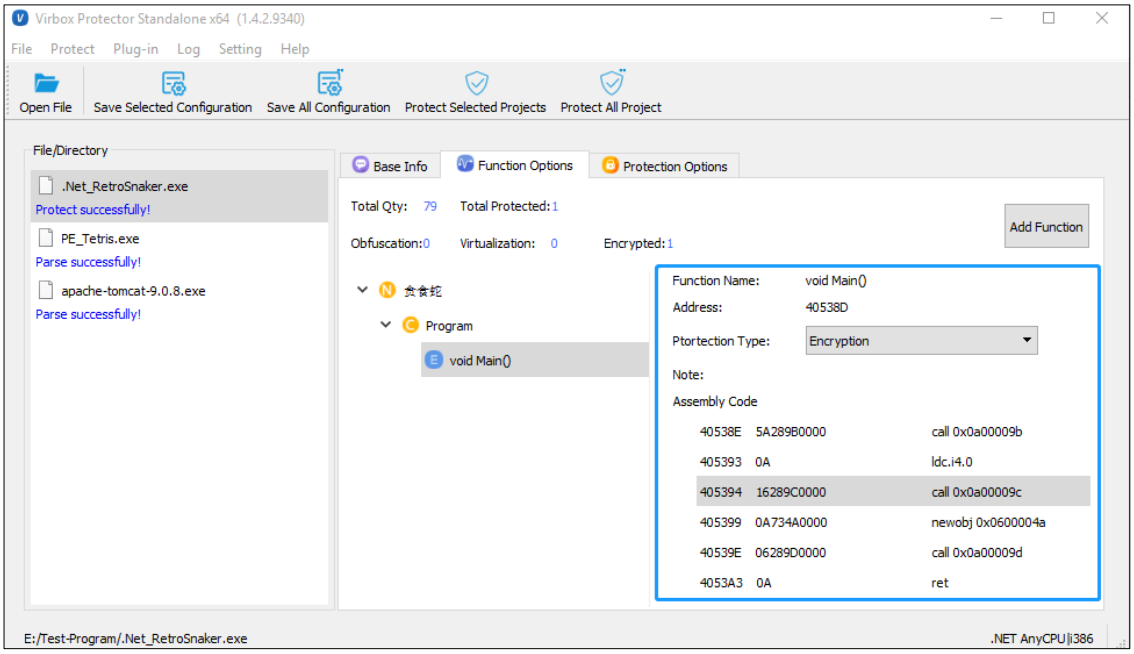


Figure 24

Following steps will describe how to set and select options for above setting:

Note: The functions be protected is limited within 5 functions for Virbox Protector Standalone **Trial version**, and no limitation to the No. of functions be protected to Standard version.

[Note: If xxx.map file existed in the same folder of software be protected, Virbox Protector Standalone will load this map file automatically and list functions in the main menu, currently the map file support be protected includes the map file created by VS, VC, BCB, Delphi compilers.]

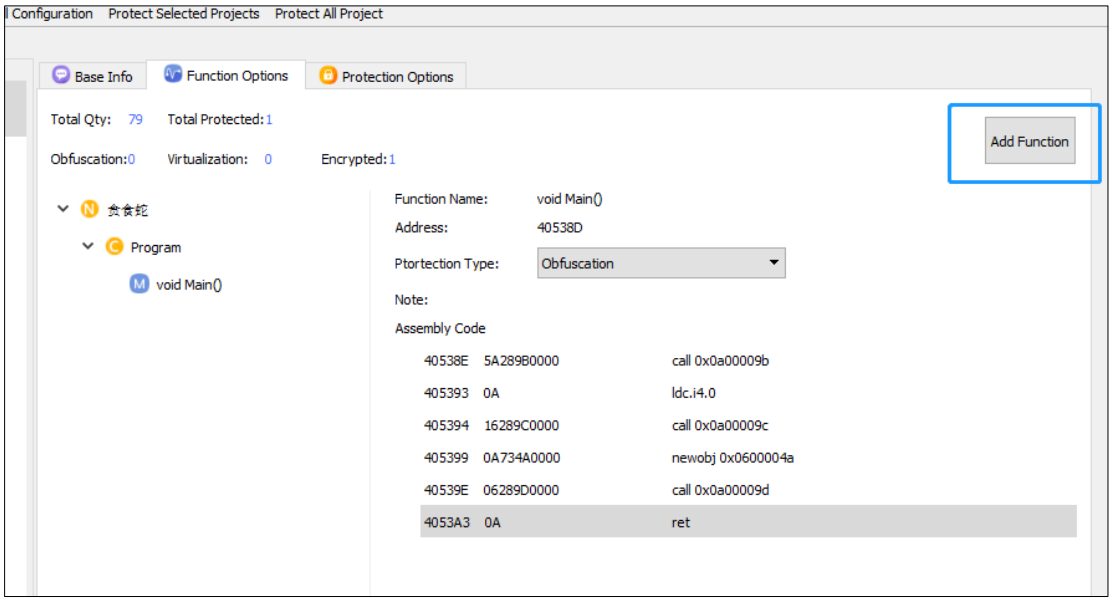


Figure 25

Note: Usually, software developer need to balance the software execution performance and protection level before software protection. Be careful to select and protect these frequently called functions, since it will decrease software execution performance after protection and encryption.

Click "**Add Function**" (See picture attached), the **Virbox Protector Standalone** will list all of the functions used in this software in the left panel. After you selected the protection mode (you can choose **Code Obfuscation**, **Virtualization, Encryption to code**) you can start to analysis functions details by clicking "**Analysis**" before protect software. The Analysis function will show you the direct running performance and the call times of the protected function. And after you completed analysis, the functions called times will be displayed in the middle of the panel. You can select corresponding technology to protect your software.

Function search is supported here:

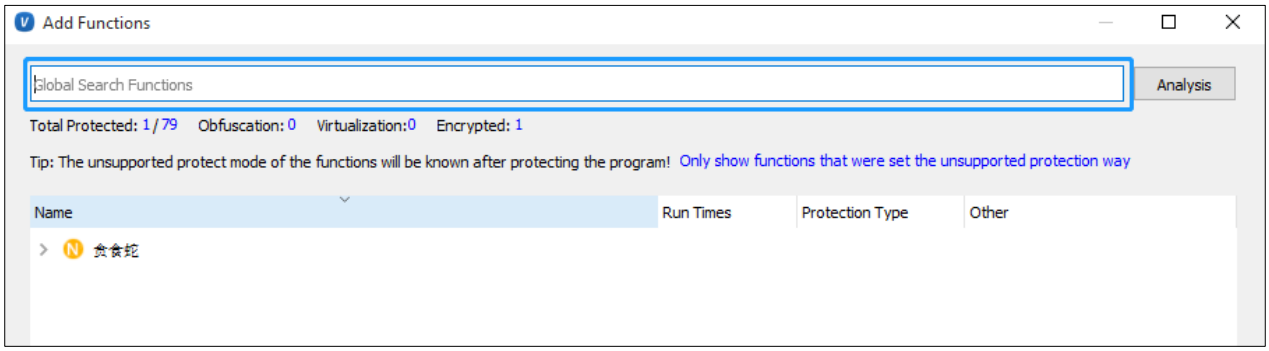


Figure 26

Note: If the program you are analyzing is **DLL** libs, please start the main program. We currently support EXE program and DLL library protection.

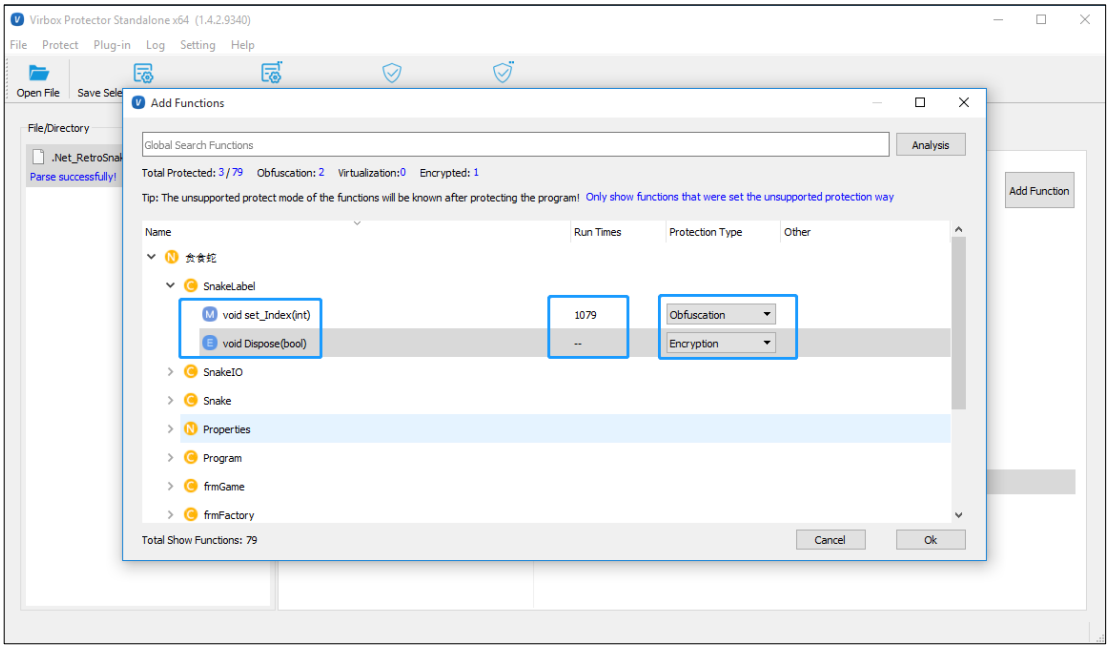


Figure 27

Run times: The functions called times during this analysis process, after you have run the program for some time (several minutes).

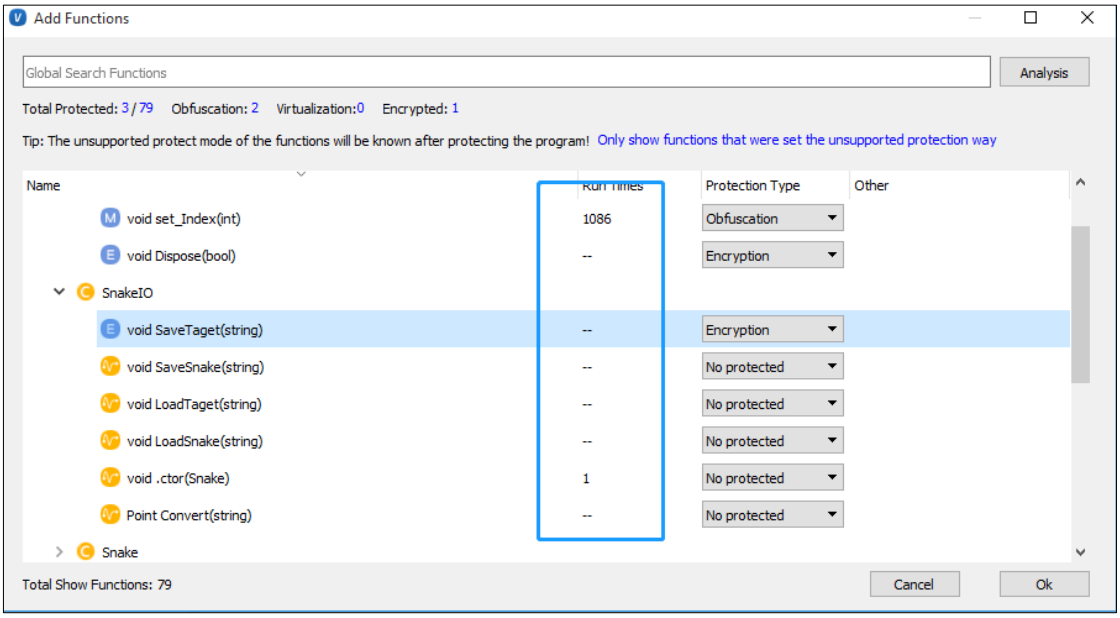


Figure 28

To protect the functions of the software, following functions protection mode can be selected: **No protected**, **Obfuscation**, and **Virtualization, Code Snippet (Code Port), Encryption to code.**

- For the function which is called frequently, select "**No Protection**" option, since if you protect the functions which is called frequently, it will decrease software's running performance when software

is executed;

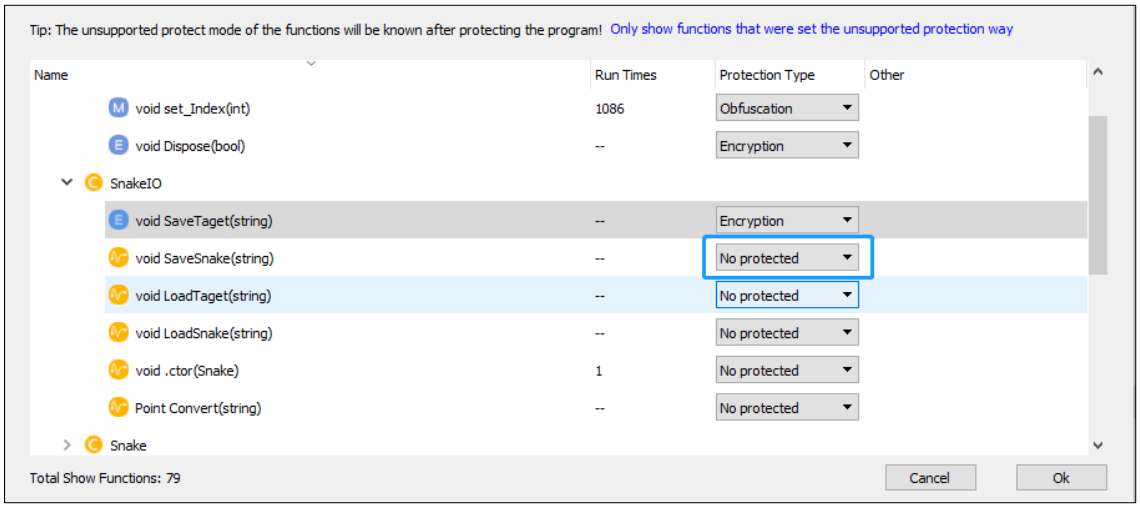


Figure 29

- Select "**Obfuscation**": **Virbox Protector Standalone** will translate the code instruction into a stream of pseudo-code that neither the machine nor the human can recognize. When the pseudo-code executed, the software will translate and interpret to restore the code into the original code. To let it executable when it is executed.

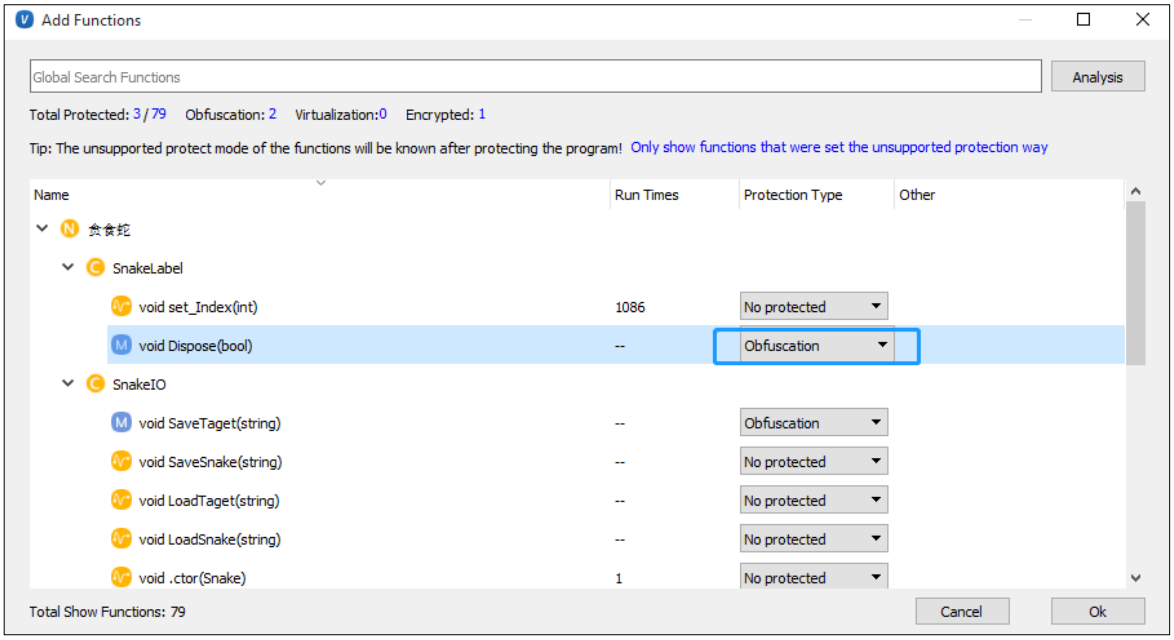


Figure 30

- Select "**Virtualization**": Virbox Protector Standalone will compiles instructions into virtual code and run them in the specified virtual machine. There are certain format requirements and limitation for instructions, and some functions may not be protected;

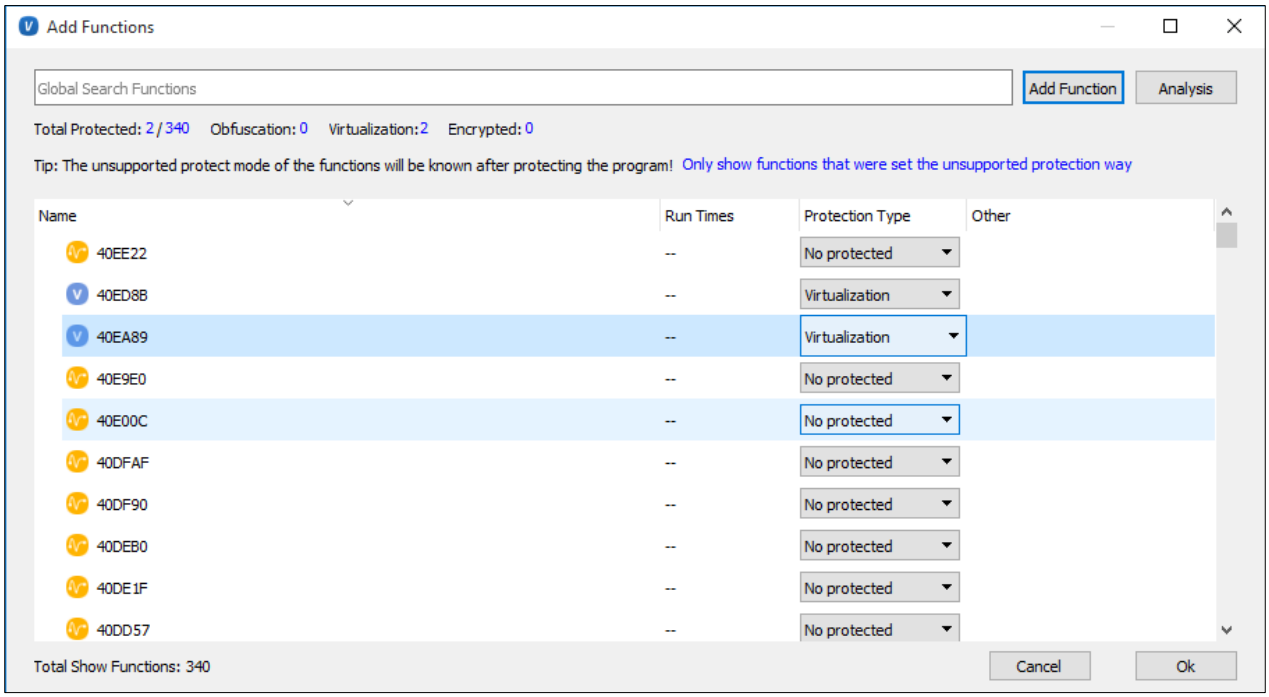


Figure 31

- **Code Encryption**: Select the code block (treat as data) and stored with encrypted function mode and verify with the license. When the program is executed to this encrypted function, the license is verified and decrypted. The complete code block is not exposed into the memory. Currently, part of functions cannot be added into the protection list and encrypted.

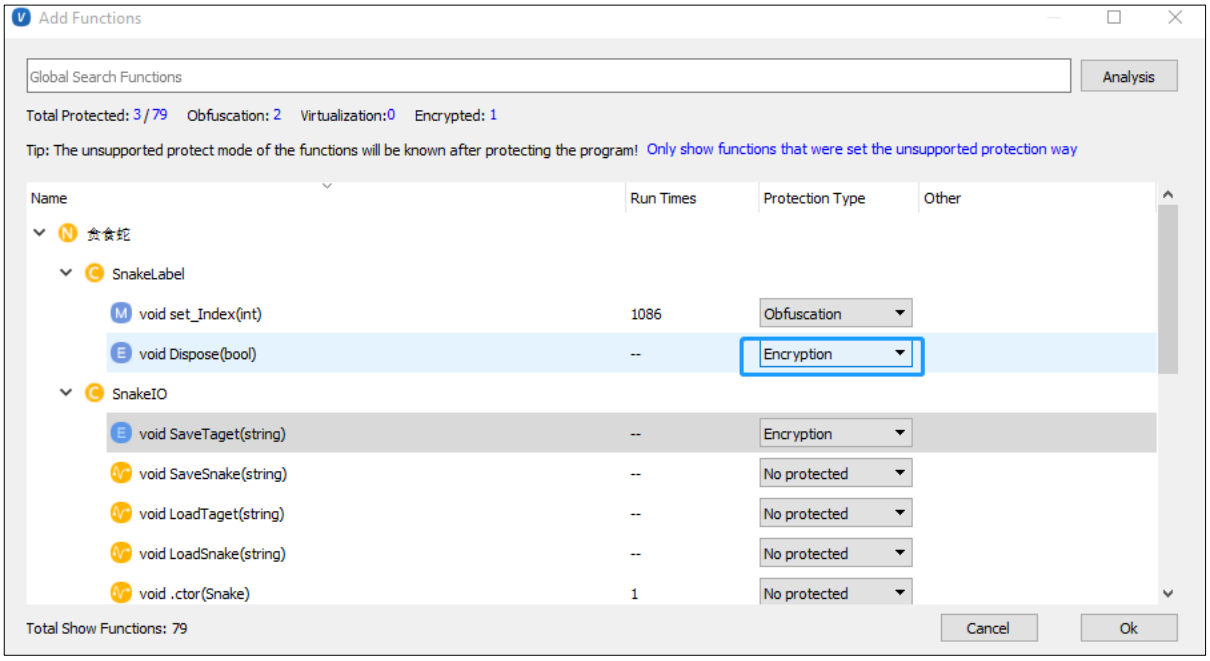


Figure 32

Note: For **.Net** Programs, Support function protection options includes: **No protect, Obfuscation, Encryption, Code snippet**;

For **Other** Programs (PE or local program): Support Function protection options: **No protect, Obfuscation and Virtualization, Encryption**.

Tips:

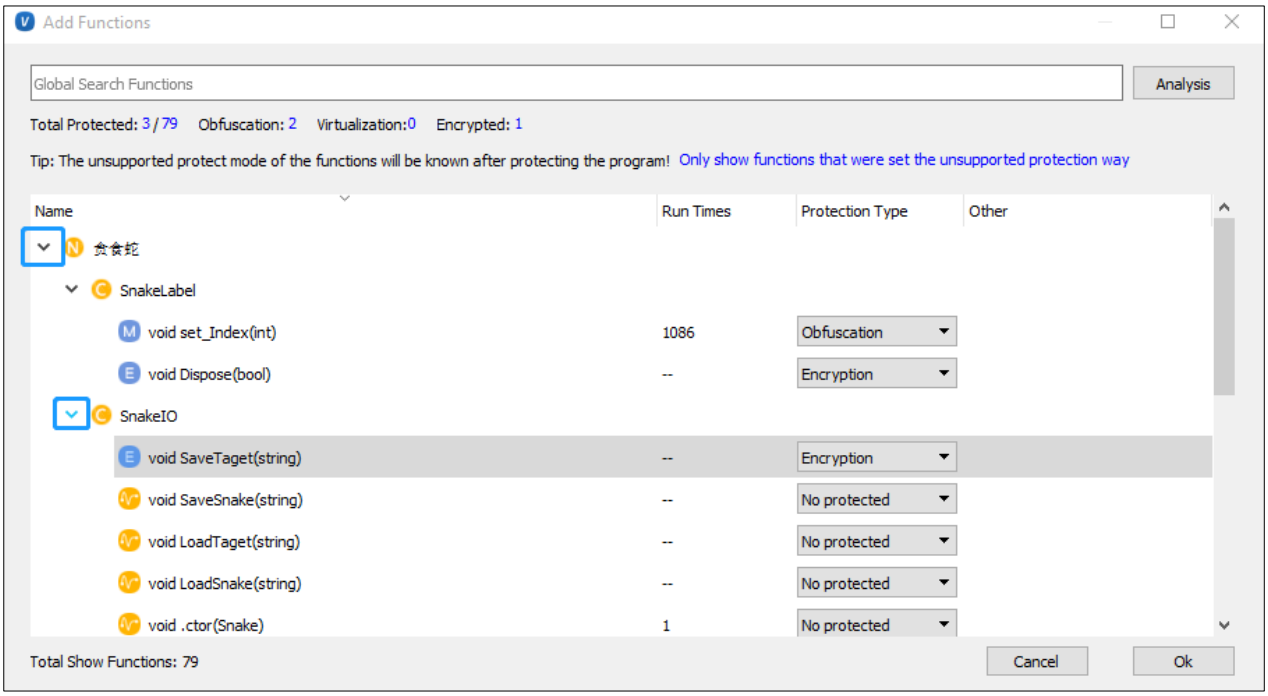


Figure 33

You can click the icon in the picture to open the function.

Protection Options

Protection Option setting will be different for different program, This "**Protection Option**" functions have little difference for PE (local program) and .NET application due to difference of PE and .NET technology and Gaming software based Unity3D. Developer can select and setup these "**Protection Option**" in actual project.

For **.NET program**, following options could be set and selected:

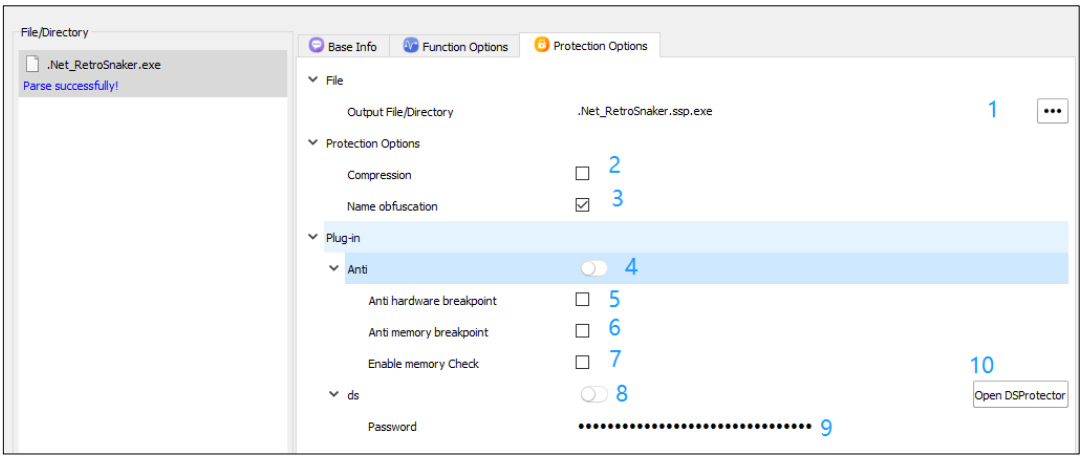


Figure 34

For **local program** (PE), following options could be set and selected:

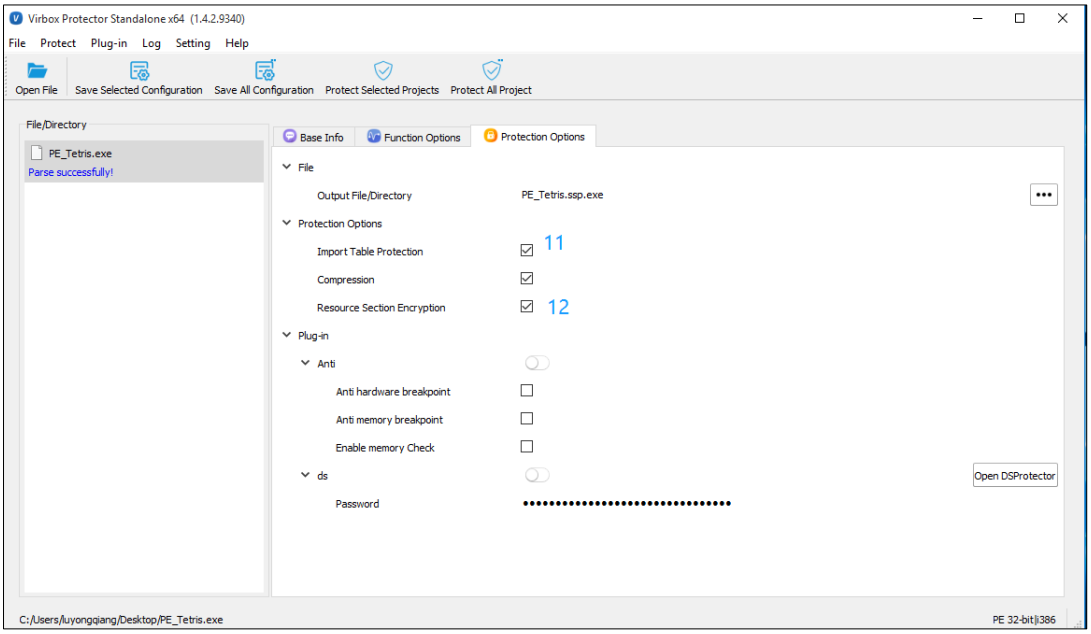


Figure 35

For Unity3D file following options will be displayed and selected:

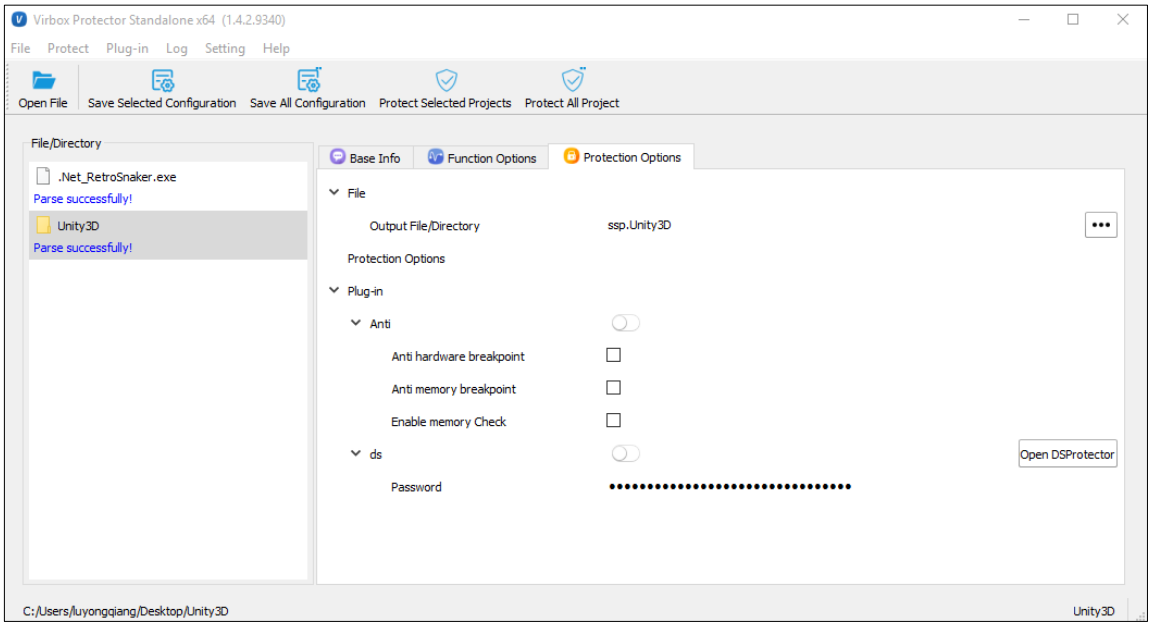


Figure 36

Press the "**Protection Option**"

1. **Output File**: Here you can change the output file path of the protected software.
2. **Compression**: Compression means to compress the application after protection and reduce size of application, it is also prevents static anti-compile the software application by hacker who use static anti-compiler tools. When you select Compression: It will keep and control the size of protected software application not too big size. Also will enhance protected software's security level after compression; for relatively big size program this function would be obvious to make the program smaller size.

Note: This function do not support .Net dynamic library, ARX library compression.

3. **Name Obfuscation:** Select this Option, developer can obfuscate the program file name and transforming software program name into the pseudo code which cannot be recognized by use of Static Anti Compiling Tools and then convert these Pseudo code into original program name when execute the protected software.

Note: Support .Net program only, not support IIS type program.

4. **Anti-Hack option button:** you can use the following anti-hack option by clicking this button.
   This is anti-debug function, including Anti-Hardware breakpoint, Anti-memory breakpoint, Enable memory check.
5. Anti-Hardware breakpoint: when you use this function when you protect the software, the program will stop execution if detect the protected software has been set the hardware breakpoint.
6. Anti-memory breakpoint: This function will protect your software by exit the program if the program has been detected to be setting memory breakpoint and write breakpoint into memory.
7. Enable memory check: when this function enabled, the program will be terminated execution if the

memory modification has been detected.

> Note: Code Encryption and DS are conflict with "Enable Memoy Check" and may not set at same time.

8. **Ds (Plugin):** Encrypts the resource section of the protected program, DS Protector is a data resource protection tool that encrypts the data resource files of the program. When you are using this function, you need to click the button to green.
9. **Password:** You can also set a password, letters and numbers are supported, but it should not be longer than 64 characters.
10. **DSProtector button:** You can open DSProtector by clicking this button.
11. **Import Table Protection:** Developer may select this option to protect "Import table" which imported to PE Program and encrypt this table, API list has been hidden and encrypted to enhance and increase the security level to the PE Program, recommend developer select this option.

> The Protection option of "Protect Import Table" support PE program only.

12. **Resource Section Encryption:** Encryption to Resource Section, select this option, Virbox Protector Standalone will encrypt resource section of the program be protected, relate resource section will be decrypted with valid license verification when program executed.

> Note: Encrypt the resource section. Only local programs currently supported.

Status bar

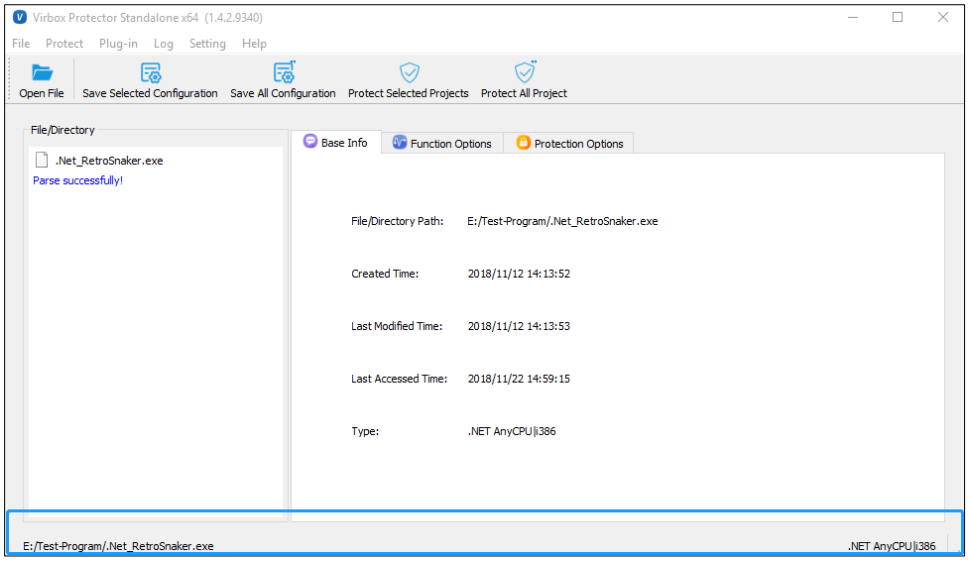


Figure 37

In the bottom of the window is the status bar, which will show the corresponding software location, software version, software type, and hardware type of the selected software.

To Complete the Protection:

Click the button of "Protect Selected Project" to complete the protection process, then prompt with "Protection Successful" means the software protection completed. Open the directory where the protected software located, you will find the file: xxx.ssp.exe or xxx.ssp.dll will be listed in this directory. The executable file that have ssp inside is the software application has been protected by Virbox Protector Standalone. Rename this file name to be original file name for further evaluation or distribute this protected software in future. Please keep the original software file in safety.

3 The Principle of Software Protection

3.1 Protect the executable file and DLL lib.

Software Developer use Virbox Protector Standalone to protect the executable file and DLL lib, with the functions protections Option, Protection Options, "Anti-Hacker" plug-in feature and other Protection technology, as introduced in Chapter 2, Developer may flexible select these functions to protect the software functions, codes, critical algorithms and evaluate the software execution performance.

- Following protection process will be implemented:

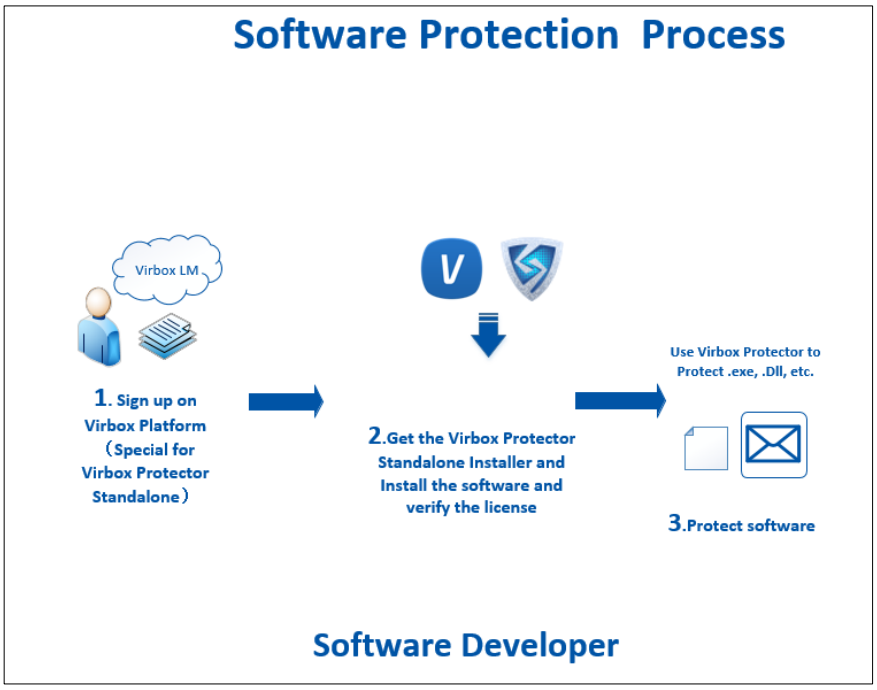


Figure 38

For example, you have created a python based exe executable file. When you are running this executable file, you don't have to build a running environment. You can use the above process to protect your software.

3.2 Protect the parse software and data resource file

Software developer use Virbox Protector Standalone and plug-in Unit (DS Protector) to protect the parse

software and related data resource files.

Software need to build an execution environment(executable environment), for example, install a python environment on your PC and execute the **.py** or **.pcy** file (Or execute an **Mp3, Mp4** file with a media player or run an **Jar archive** file, **War** file on an environment that have installed JDK or JRE).

- Following protection process will be implemented:
  - Use Virbox Protector Standalone to protect parse program (Java.exe, Python.exe, etc.);
  - Use DS Protector to protect the Data Resources (.Jar, .class, .py, etc.);

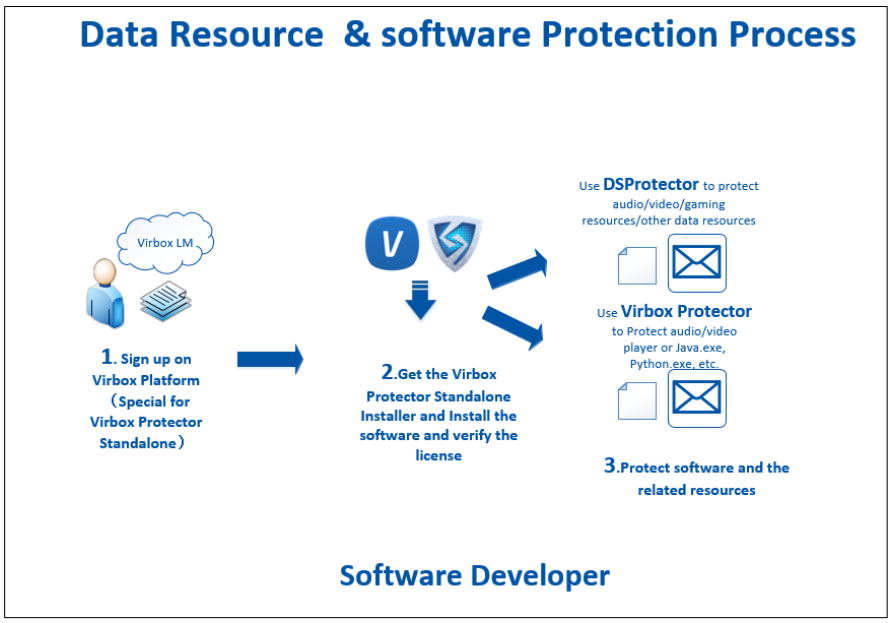


Figure 39

3.3 Make the protection scheme for your software

When you open the Virbox Protector Standalone, you can directly drag the windows Application to the Virbox Protector Standalone to protect, as shown in the figure below:

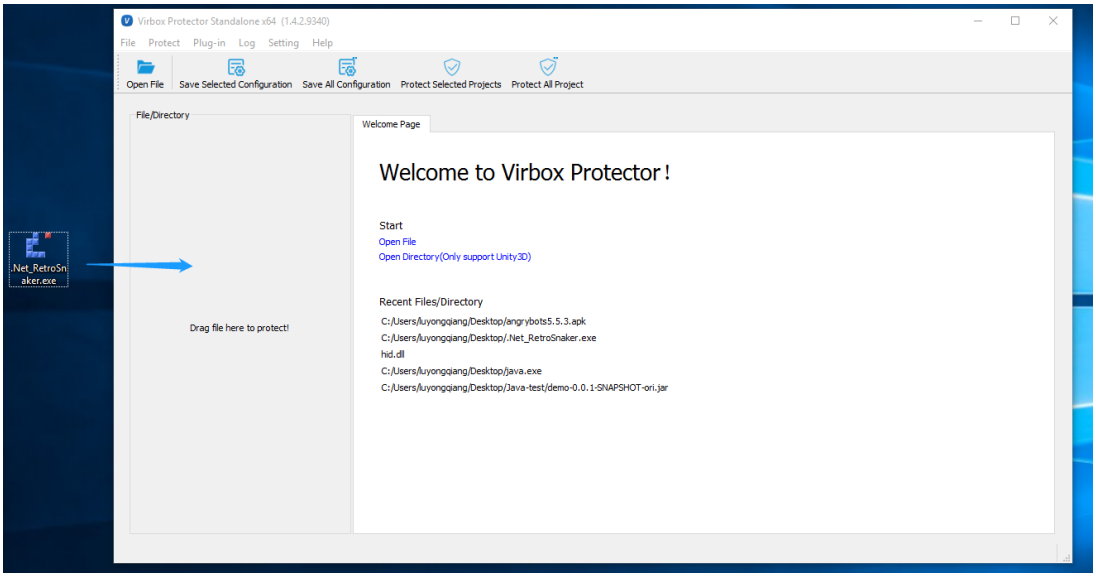


Figure 40

You can make your dedicated protection scheme and "configure" the protection options by select following Function Option and Protection Options as shown in below:

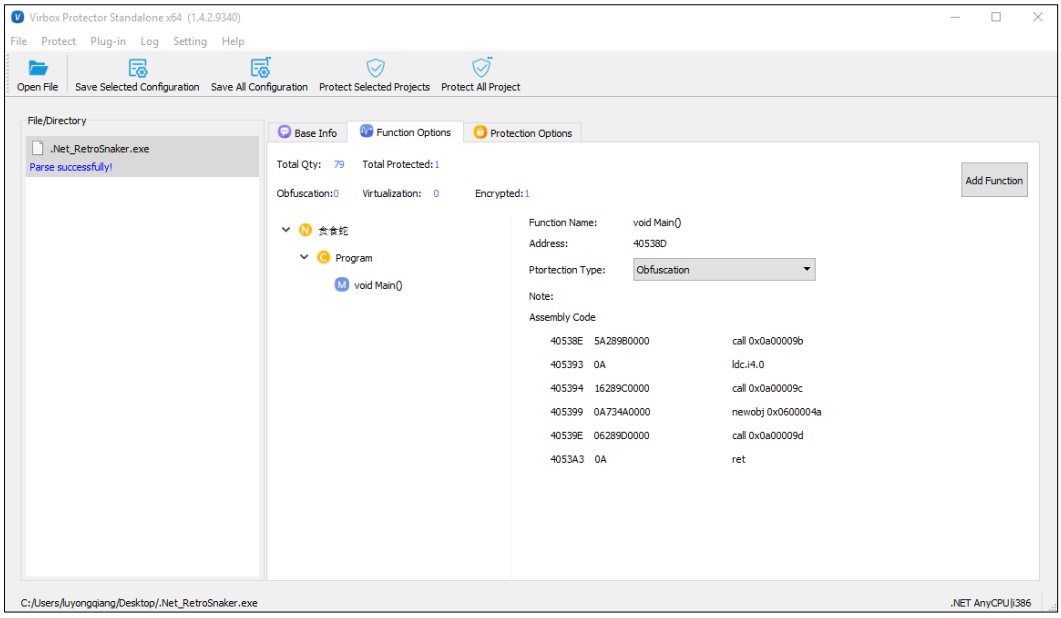


Figure 41

Note: You can also open the path of the executable file with "**Open File**" option; and use "**Save**" button to save the configuration you already made for one application; after clicked the "**Protect selected projects**" button, the application will be protected with your selected protection option.

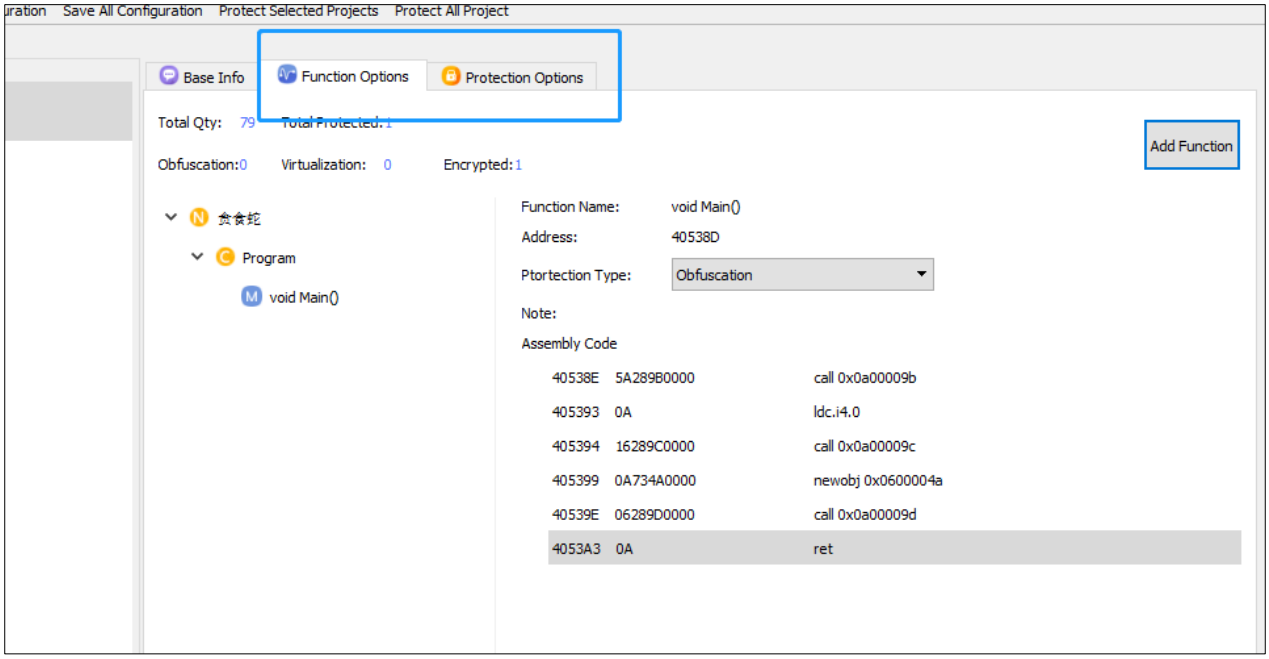


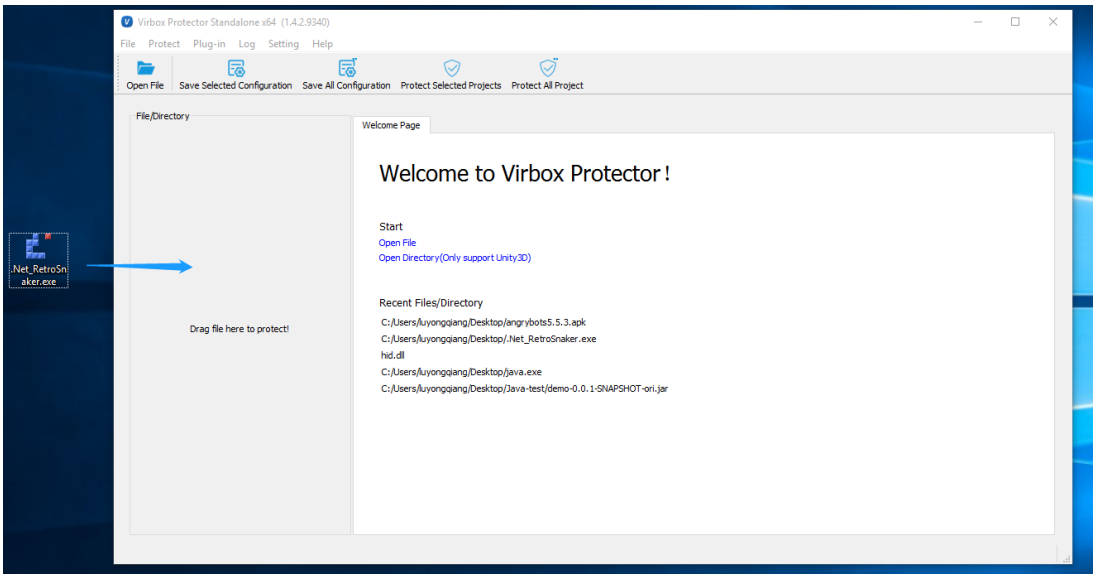
Figure 42

4 Protection Example & Use Case

4.1 Windows Application .EXE or .DLL file protection

In the example we use the setting shown as blow:

Drag the execute file you want to protect into Virbox Protector Standalone:



Function Option:

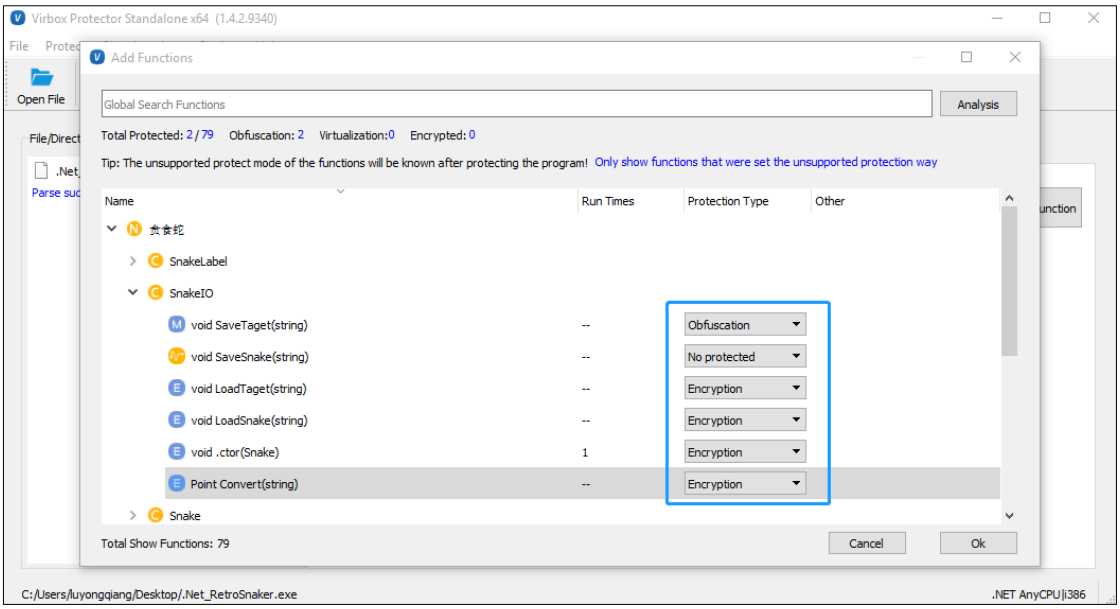


Figure 43

Protection Option:

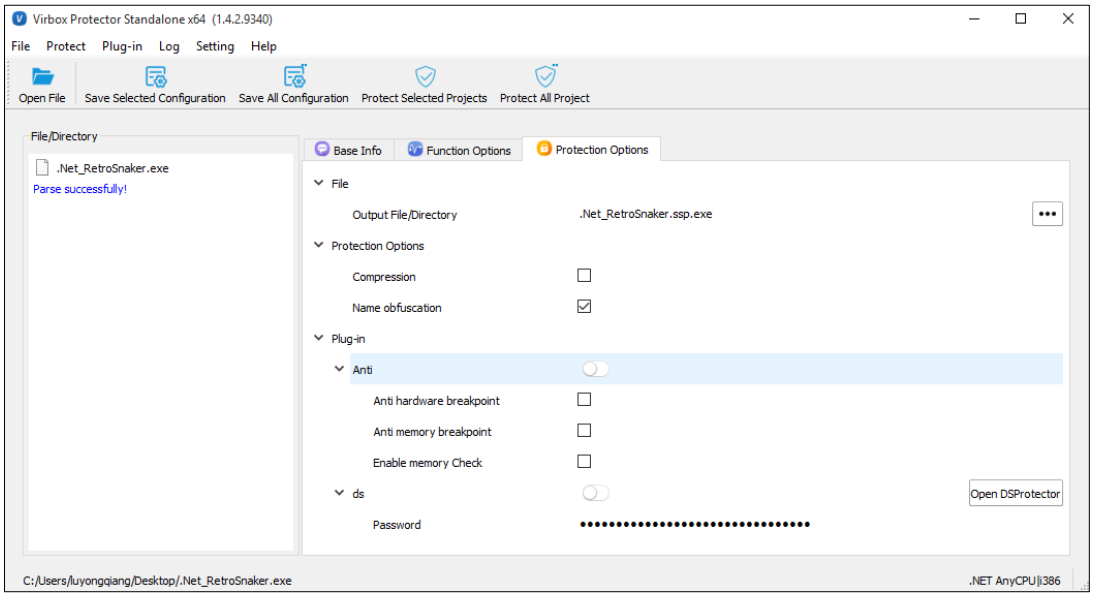


Figure 44

You can select the corresponding protection option according to the introduction of the function.

Then click "**Protect all project**" button **to complete** protection

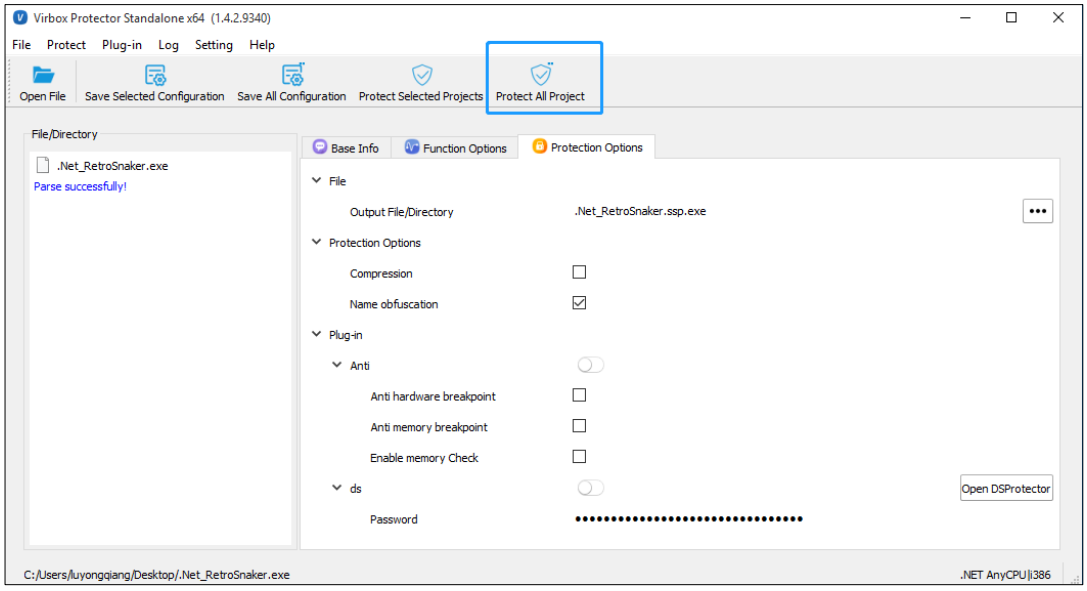


Figure 45

After Protection 2 more file will be created, **.Net.exe.ssp** and **.Net.ssp.exe**

.Net.exe.ssp is the configuration file that can be used to protect the data resources. If you do not need to protect the data resources like picture, video, Java archive file, you can delete this configuration file.

.Net.ssp.exe is the file after protection, please noted that the name of this file is different from the original file. You need to modify it to be the original one then you can distribute this file to software user. Because maybe an un-matched name would cause error.

[Note: Not all functions module can be listed in this panel.

1. The function module which program size less than 15 bytes will not be listed.
2. Some unconventional function modules are not listed ('.', '<', '>', '@', ':', '?', etc.) exist in the name.
3. **There are little difference between managed code and unmanaged code in the function list**
   For managed code: the function name would be" Namespace + Class name + Function name"
   The unmanaged code: Function name is the va value of the function.

After protection you can start to test the protection result before distribute the protected application to the software user.

4.2 Java program, Jar archive, War archive Protection (Resources Protection)

Introduction

Java program support cross platform operation which rely on the java execute in the Virtual machine environment as intermediate code, so the de-compilation to java code is much easier to implement than other languages. And the decompiled code is almost compatible with the source code after optimized. In order to against de-compilation tools and protect software copyright & intellectual property, the Java Obfuscator was developed and introduced.

But the functionality of the Java obfuscator is obfuscate the compiled code, and makes the decompiled code difficulty to understand. The result by using java obfuscator is increasing the difficulty of reverse engineering. For the people who familiar to use the de-compilation tool. It is almost transparent. In addition, due to the multiple mappings in Java programs, the compatibility of most obfuscation tools is quite limited.

Following is an example to protect a Java program.

Usually, java project stored and saved in the //webapps directory, please start up the tomcat service and check if it start as usually, then the war archive will unzip a directory with same name of war archive name.

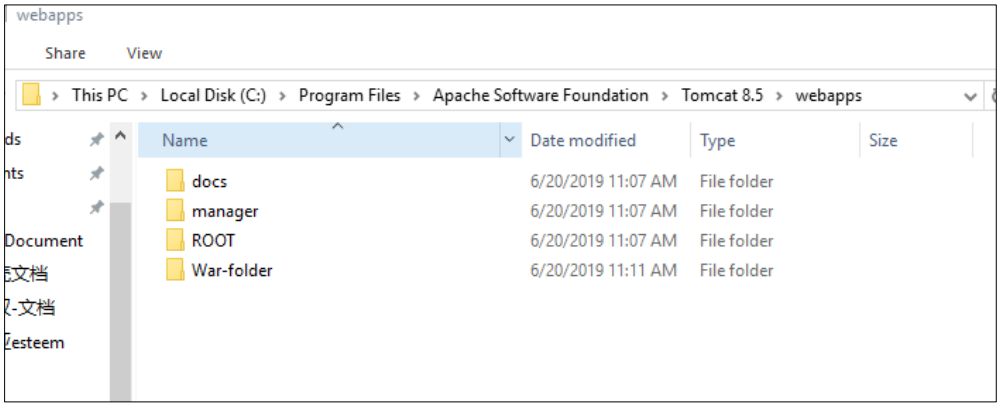


Figure 46

Startup tomcat service

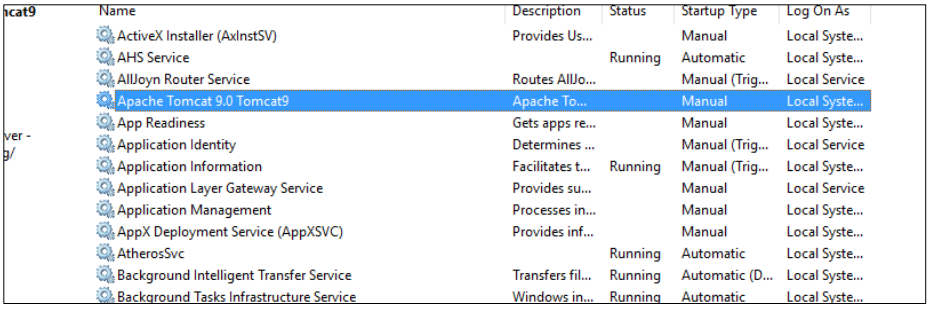


Figure 47

Find the interpreter

Open the task manager when startup the tomcat service and find the jvm file which associated with current project. Open the directory and find correspondent program and protect the program, see picture show as below.

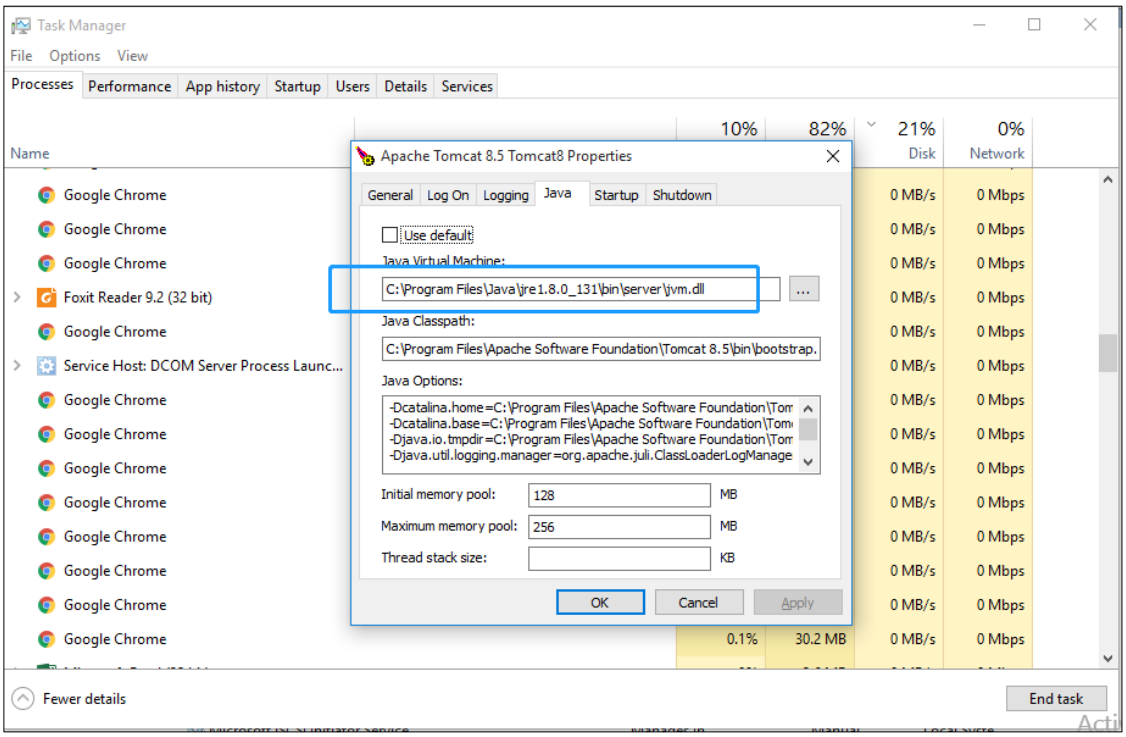


Figure 48

Find the "**Java.exe**" program installed on your machine, which located under the **JDK** installation directory.

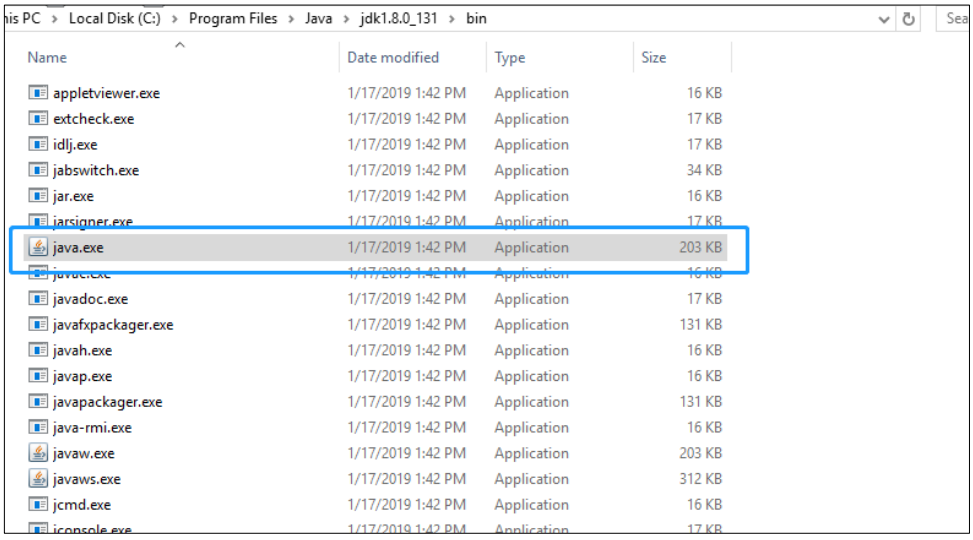


Figure 49

Create a folder for the "**Java.exe**", which is to avoid having influence on the original java environment

Open the "**Java.exe**" file with Virbox Protector Standalone.

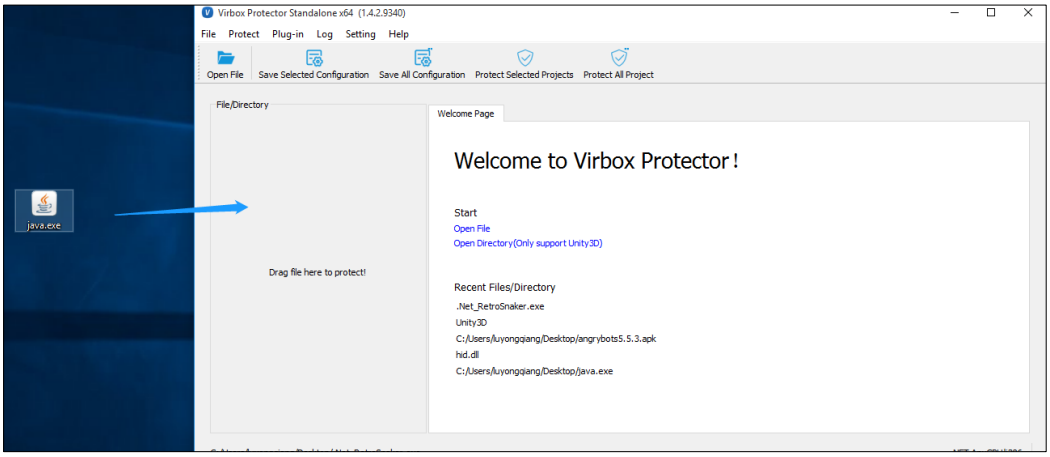


Figure 50

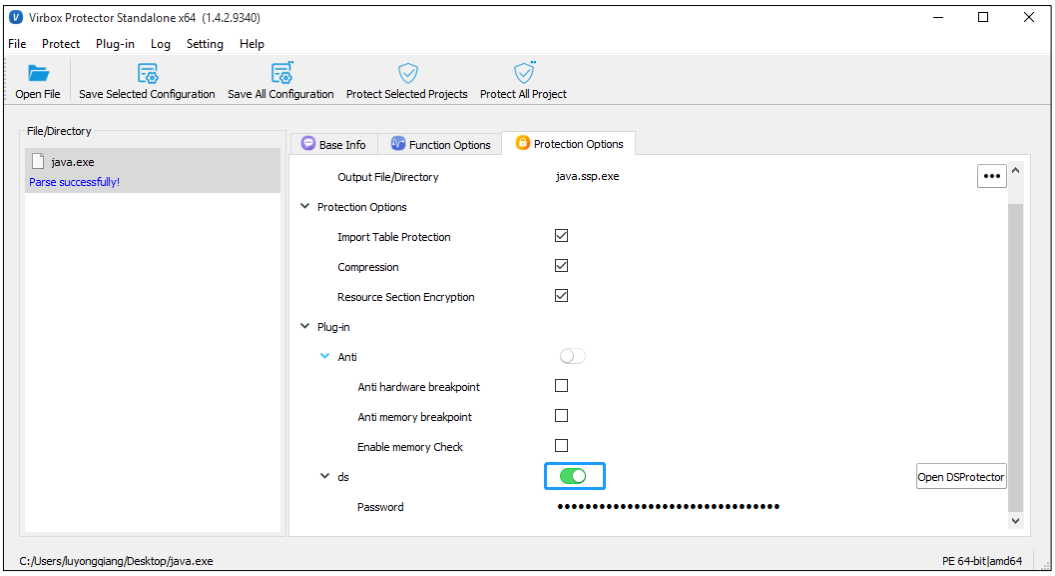


Figure 51

Open the ds protection button which will be used to protect the Jar archive file.

After protection, you can get 3 file.

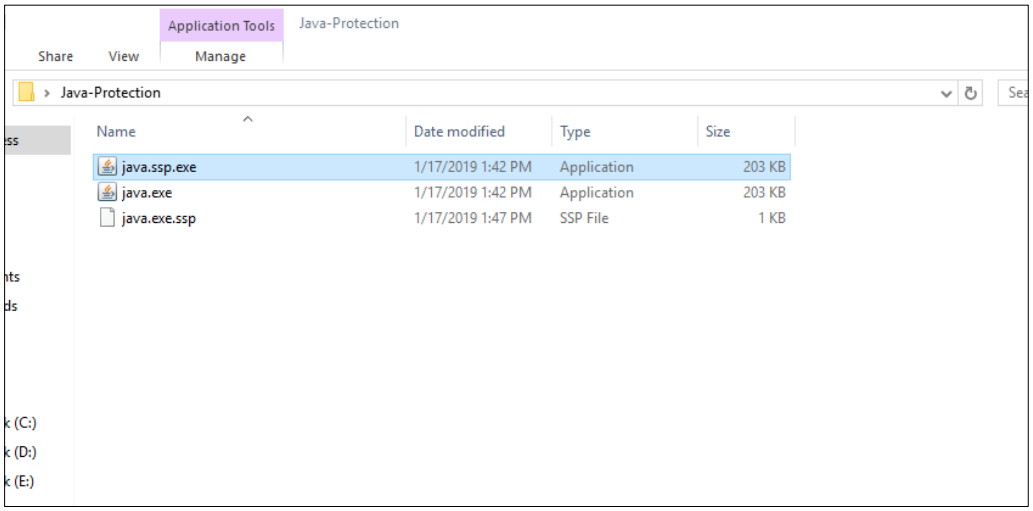


Figure 52

"**Java.exe**" is the original file without protection

"**java.exe.ssp**" is the resources protection configuration file, you would need to use this file for the **.War**, **.Jar**, **.Xml** file protection.

"**java.ssp.exe**" is the protected Java.exe file, this file can parse the protected .War, .Jar, .Xml file.

Before release the software, please modify the "**java.ssp.exe**" to be "**java.exe**" and copy the file to the original folder and make sure a same name as before.

4.2.1 Protect the .Jar archive.

Please note: this function is only supported on windows version Virbox Protector Standalone, Linux or Mac version is not supported.

Open the DSProtector by clicking the button "**Open DSProtector**"

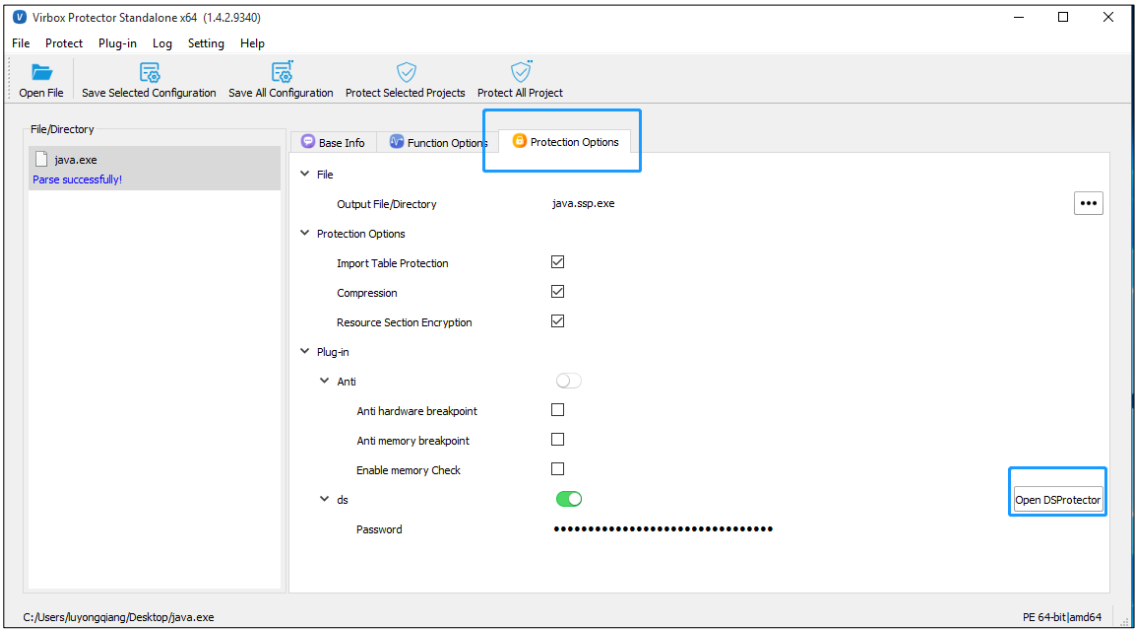


Figure 53

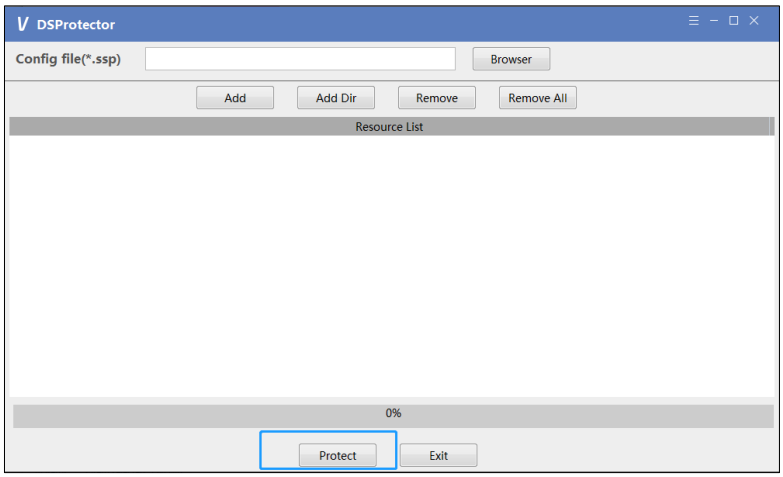


Figure 54

For the "**Config file (*.ssp)**"field, please choose the "**java.exe.ssp**" file you created in lase step.

For the Resource List area, you can directly drag in the "**xxx.jar**" file, in this document we use the "**demo-0.0.1-SNAPSHOT.jar**"file as an example.

Then click "**Protect**", the file would be protected.

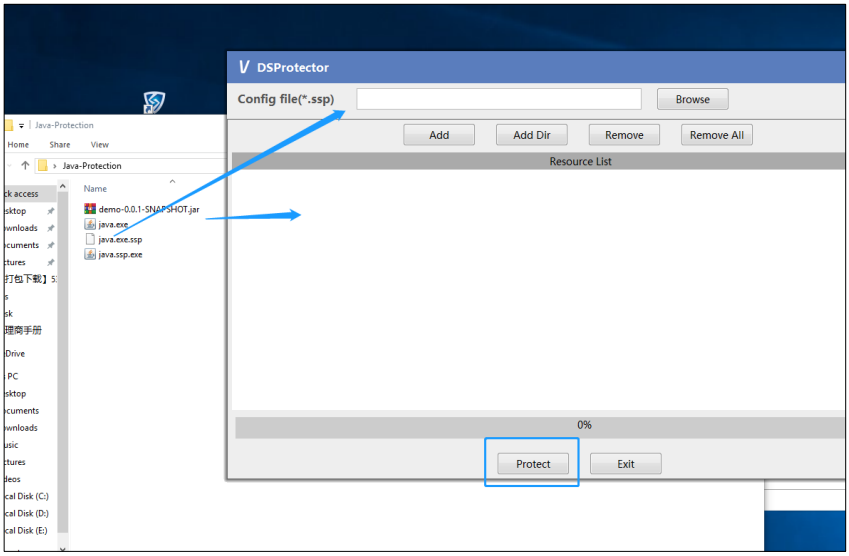


Figure 55

In this example, it is showing protect success.

After protection name of the original unprotected file will become a file that in bak format. The protected file name will be the original file name.

When you completed the protection of software on your side, you can distributed the protected file to the software user.

4.3 Unity 3D Program Protection

Why we need to protect the Gaming program based on Unity3D engine?

4.3.1 Introduction

The Unity 3D program mainly uses the C# and open source mono to execute the code logic and algorithm. All of the code is not compiled into the exe file and located at {APP}\build\game_Data\Managed\Assembly-CSharp.dll (note that the program with Unity-2017 is slightly different).

And the mono execution is compatible with the Microsoft .NET Framework but the execution principle is completely different. The traditional protection to .NET Framework will be invalid to protect the mono execution. Since Assembly-CSharp.dll is neither a dynamic library in PE format nor a dynamic library in .NET, it cannot be loaded from the .NET Framework. Instead, the mono.dll read the C# script inside of Assembly-CSharp.dll from mono.dll. Parse it and execute the program.

If you protect the Unity3D program with tradition software protection tool, it would not protect the main code

source. But Virbox Protector Standalone can not only protect the source code, but also would protect your resources (.resS). To protect your copyright and IP.

4.3.2 Protection Principle Overview

Virbox Protector Standalone protects the whole source directory of the **Unity3D** program with Virbox Protector Standalone, for the resource file, Virbox Protector Standalone will use DS Protector to protect it. In this way to protect your software main source code from being decompiled. And prevent your resources **(.resS**) from being extracted illegally. To protect the copyright and IP of the software developer.

4.3.3 Source code Protection

Drag the whole directory to the Virbox Protector Standalone

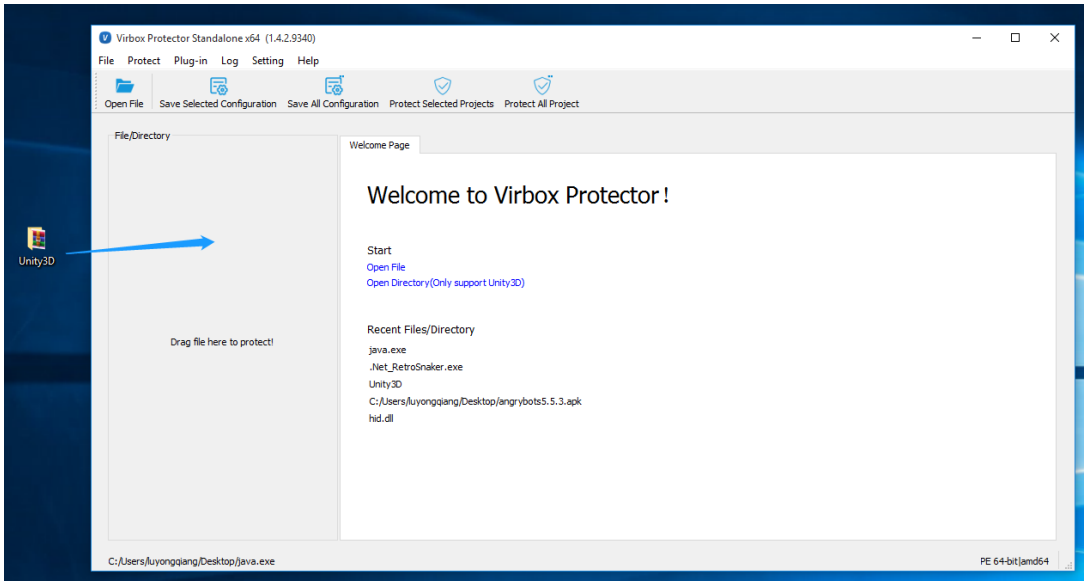


Figure 56

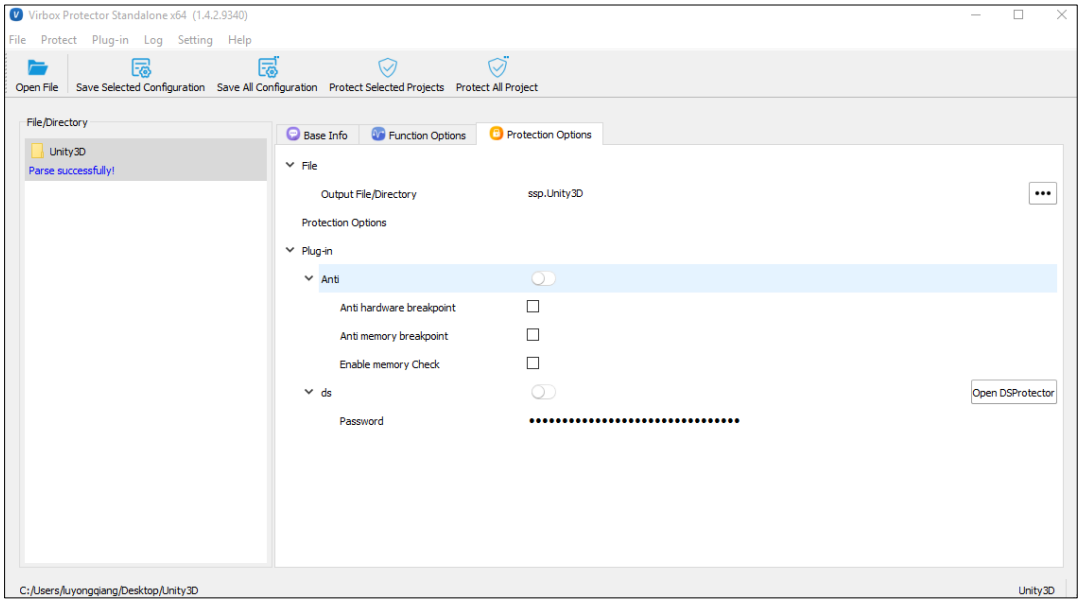


Figure 57

For the configuration of "**functions to be protected**", we do not need to set, Virbox Protector Standalone will protect all of the functions in "**mono.dll**", "**Assembly-CSharp.dll**" and "**Assembly-CSharp-firstpass.dll**".

For the configuration "**Protection Option**", no need to set, if you do not want to protect your gaming resources.

After protection, Virbox Protector Standalone will generate a new folder, same directory with the original folder named ssp.xxx (xxx is the original directory name), like the picture showing.

Two more files would be generated:

Figure 58

And it will remind you protection successful.

"**Unity3D-Test.ssp**" is the configuration file you may need to use for resources protection.

"**ssp.Unity3D-Test**" folder is the Unity3D program after protection, you can distribute this file to the software user.

4.3.4 Resources protection

For Unity3D resource protection, you need to:

1. Protect the whole directory with **Virbox Protector Standalone**

2. Protect the resources file with **DSProtector**. Before protection with DSProtector you need to import the "**ssp**" file

Blow will explain the detail steps:

Drag the whole directory to the Virbox Protector Standalone.

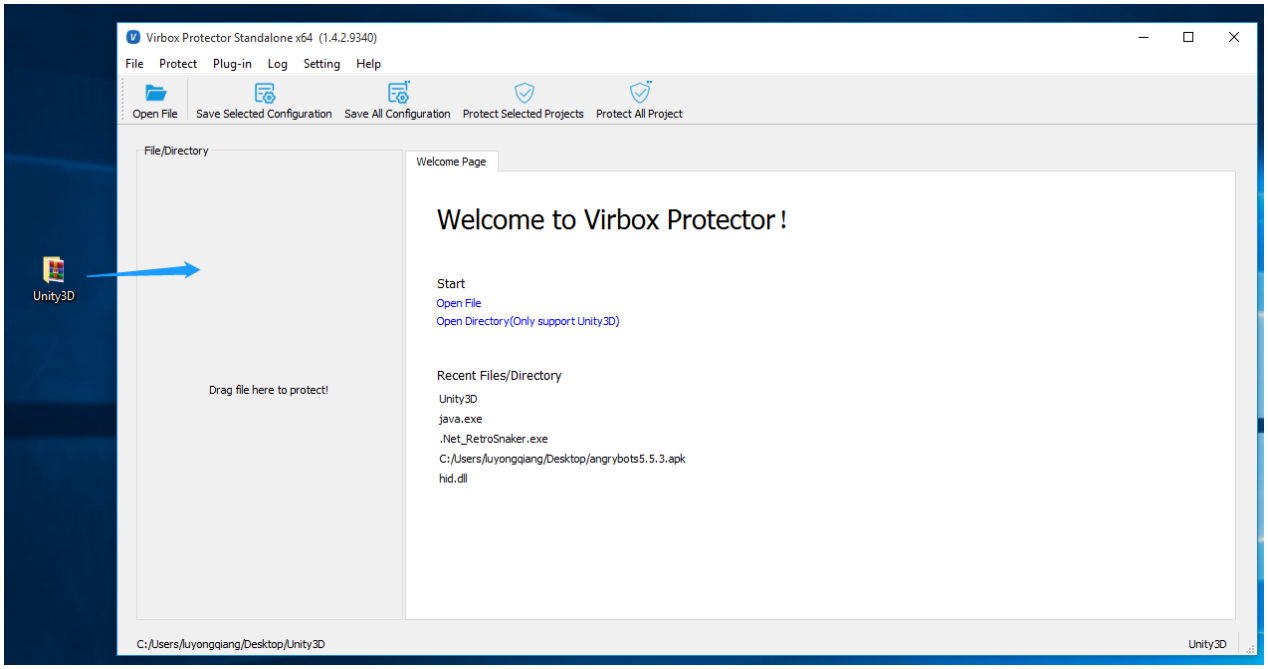


Figure 59

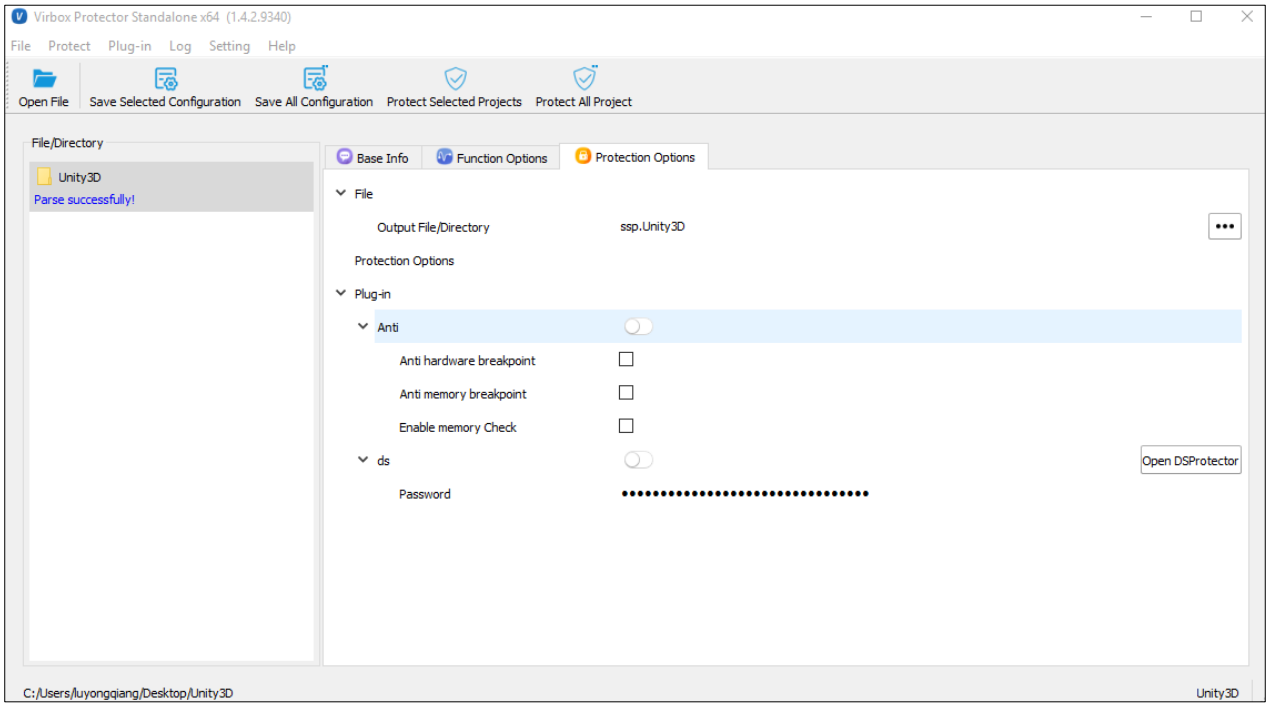


Figure 60

For the configuration of "**functions Option**", we do not need to set, Virbox Protector Standalone will protect all of the functions in "**mono.dll**"、"**Assembly-CSharp.dll**" and "**Assembly-CSharp-firstpass.dll**".

For the configuration "**Protection Option**", you need to open the "**ds**" button, like the picture showing.

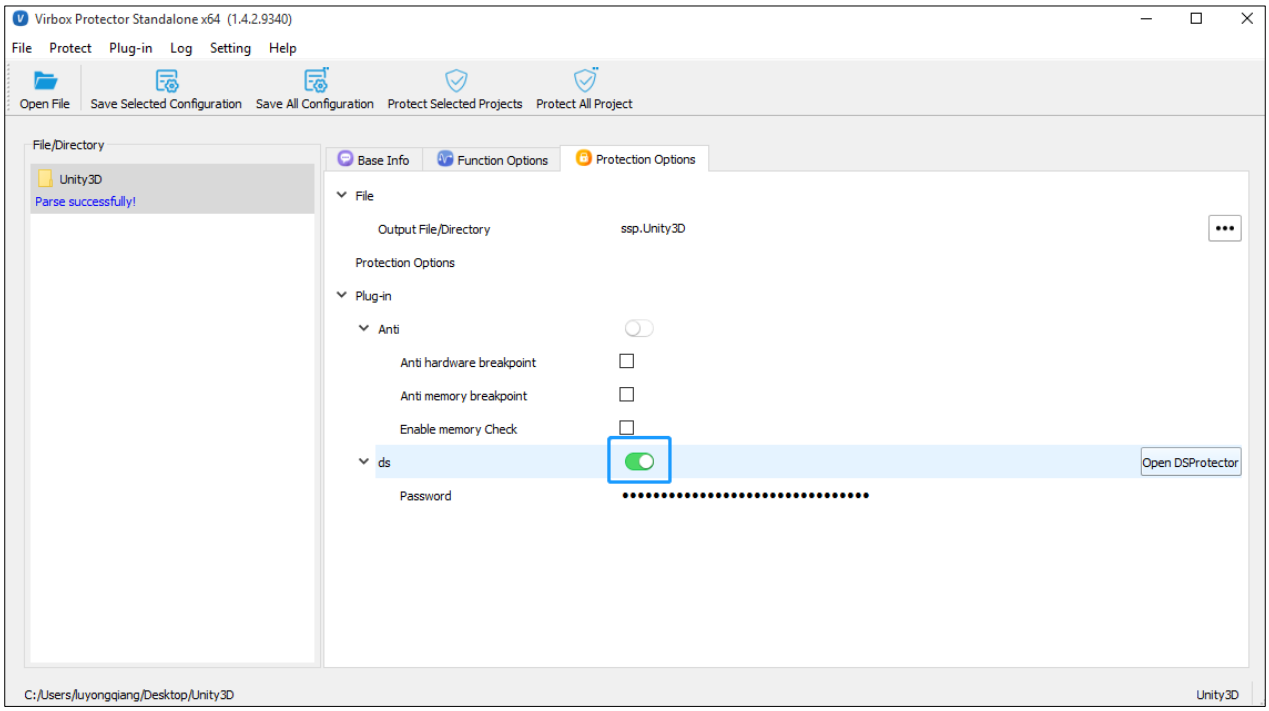


Figure 61

Note: When you are setting the Virbox Protector Standalone, you need to open the "**ds**" button.

After protection, Virbox Protector Standalone will generate a new directory, same directory with the original directory named ssp.xxx (xxx is the original directory name).

Figure 62

Next we will **protect the resource** file with **DSprotector**.

You have two way to Open **DSProtector,**

1. Click the button "**Open DSProtector**" to open DSProtector.

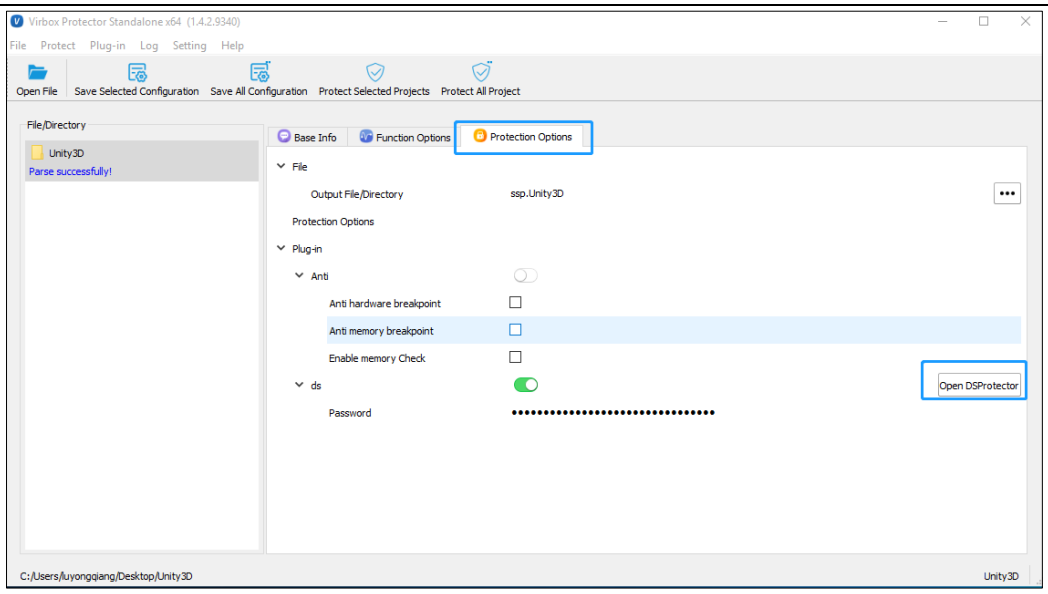


Figure 63

2. Also, you can open DSProtector in this installation path.

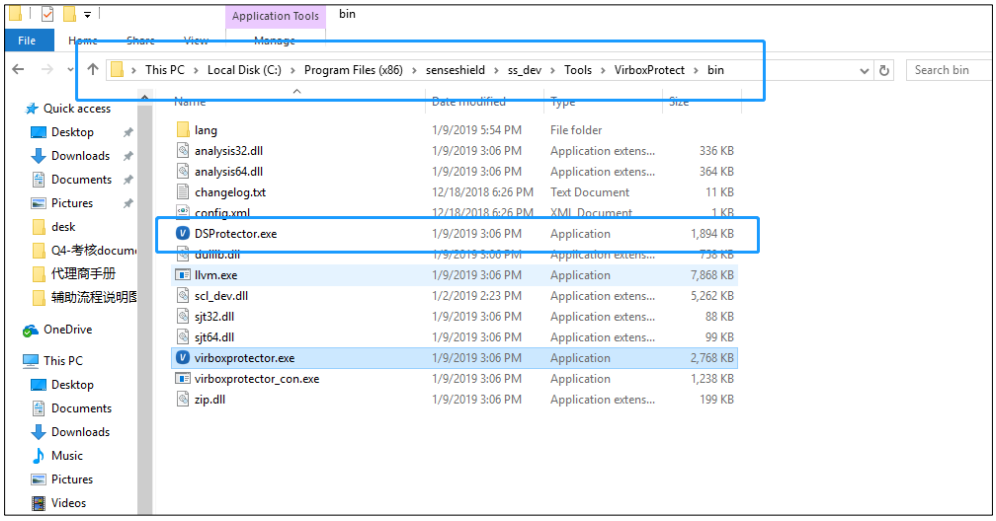


Figure 64

Choose the "**Unity3D-Test.ssp**" file you generated last step, and drag in the resources (.resS).

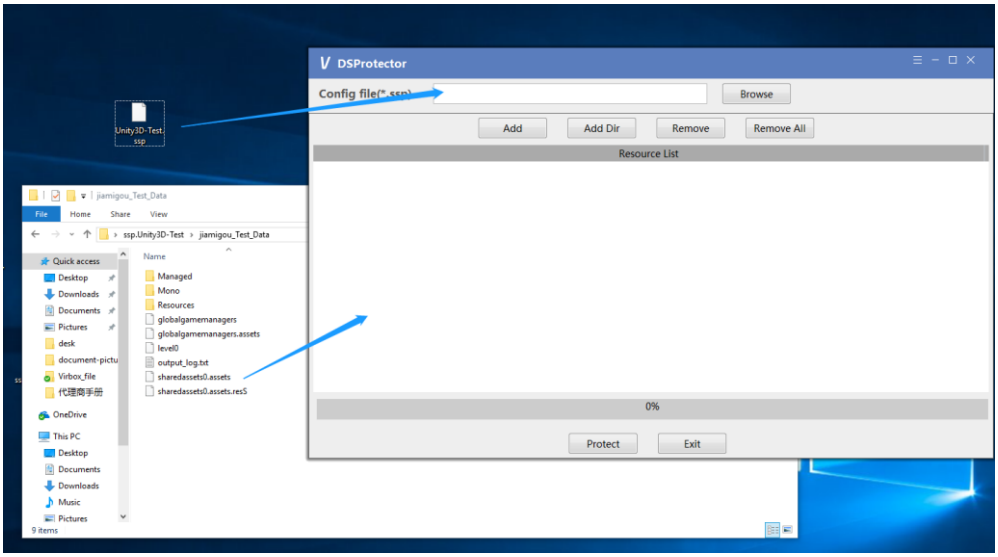


Figure 65

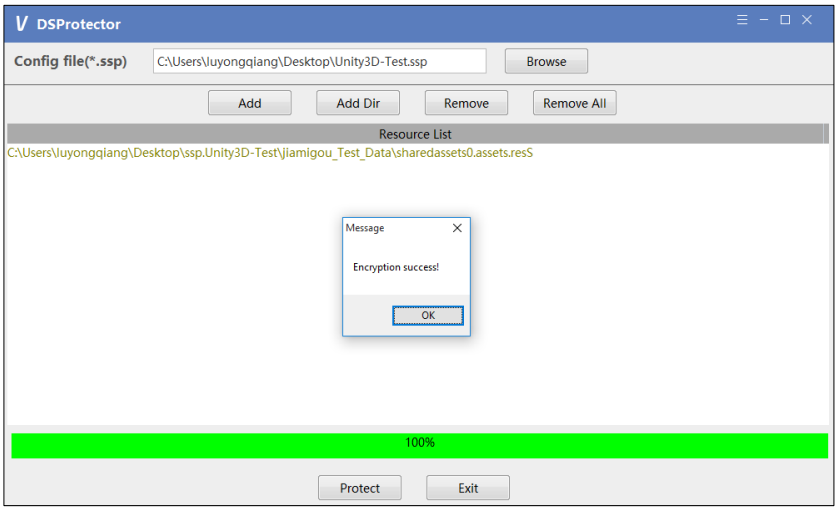


Figure 66

Click "**Protect**", to protect the resources file.

Till now the Unity3D file protection have been completed, this software can be used for further testing or distributed to software user later.

4.4 Android Unity3D software protection

1. Drag the apk of Android Unity3D in to the Virbox Protector Standalone, after protection a new file named xxx.ssp.apk would be created, Virbox Protector Standalone will protect the "**libmono.so**" and "**Assembly-CSharp.dll**".

Before protection:

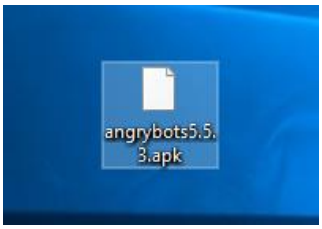


Figure 67

The un-protected file is named “angrybots5.5.3.apk”

After protection:

Figure 68

After protection,

“**angrybots5.5.3.ssp.apk**” is the file after protection. This could be released to software user.

“**angrybots5.5.3.apk.ssp**” is the configuration file. If you want to protect the data resources you need to use this file or this file can be deleted.

“**angrybots5.5.3.apk**” is the unprotected file. You can’t release this file.

4.5 Software based on python protection process

Source code protection

- Python.exe (parse) file based on python protection, the detail steps are same with Windows Application, please refer the steps above.

Resource Protection

- For resources protection, protect the python.exe with Virbox Protector Standalone first, and then protect the **.pyc** and **.py** file with DSProtector.

In this example, after protection, you will get 3 file

“**python.exe.ssp**” is the configuration file, and when you are protecting the **.py** and **.pyc** file, you would need this file.

“**ssp.python.exe**” is the **python.exe** file after protection, you need to use this file to parse the protected **.py**

and **.pyc** file. (The **.py** and **.pyc** file need to run with the **ssp.python.exe** file). When you run the protected .py and .pyc file.

Please modify the **python.ssp.exe** to be **python.exe,** in order not to influence the python environment.

"**python.exe**" is the file before protection.

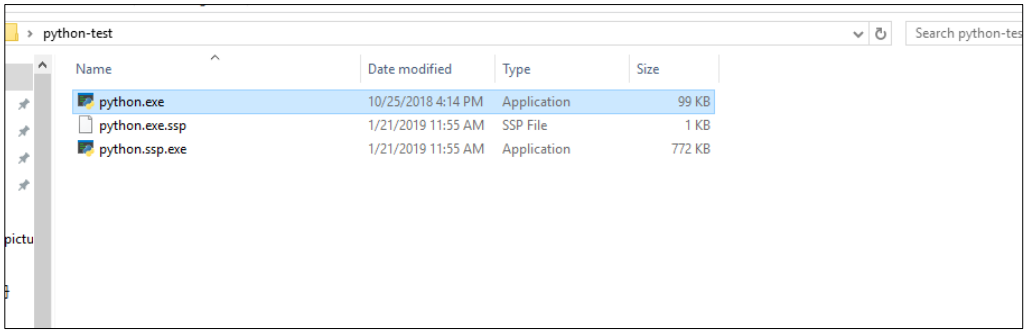


Figure 69

Open the DSProtector for .pcy and .py file protection,

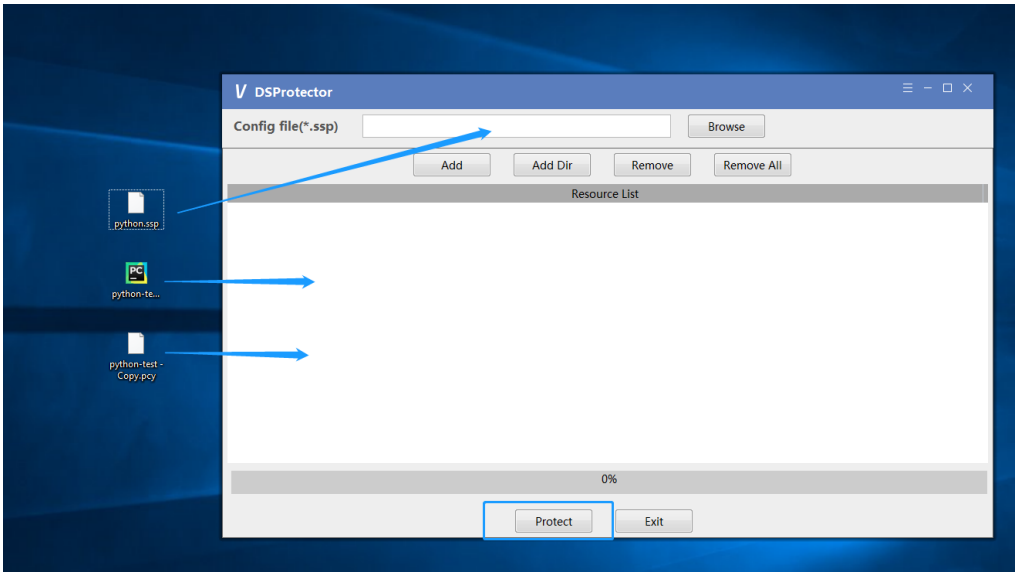


Figure 70

Choose the **ssp configuration file** created last step when you are protecting "**python.exe**"

Drag in the **.py** and **.pyc** file,

Click "**Protect**", it is showing "**protect success**"

The protected file name will use the original name, and the unprotected file will be in bak file format.

Till now the protection of **python resources** file has been completed, and please release the protected file to the customer.

4.6 Protect software in command line

1. Open com window in the start menu.
2. Input: *Virbox Protector_com.exe path*+ Virbox Protector_con.exe /?

   This command can get the help info.

Command line help info:

VirboxProtector_con <filename> [-o output]

-o output : output file name.

-? : show help information.

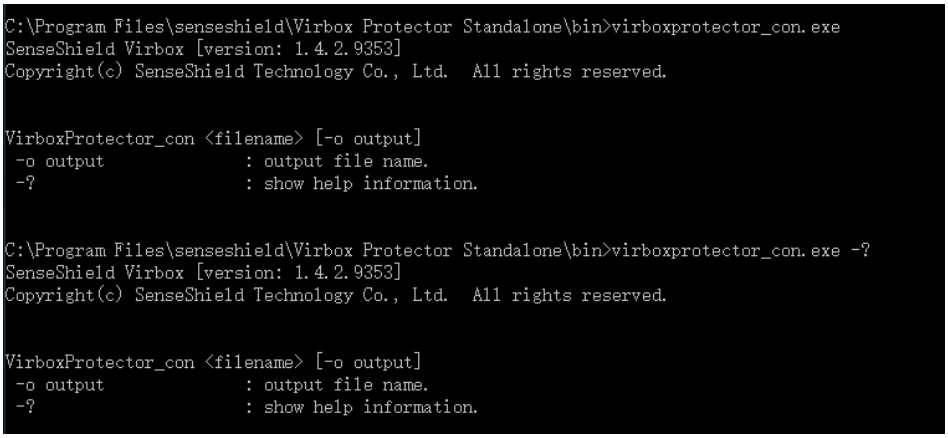


Figure 71

When you use the command without dongle, it will have this error report:

Figure 72

Plugin the dongle with license, you can complete protection.

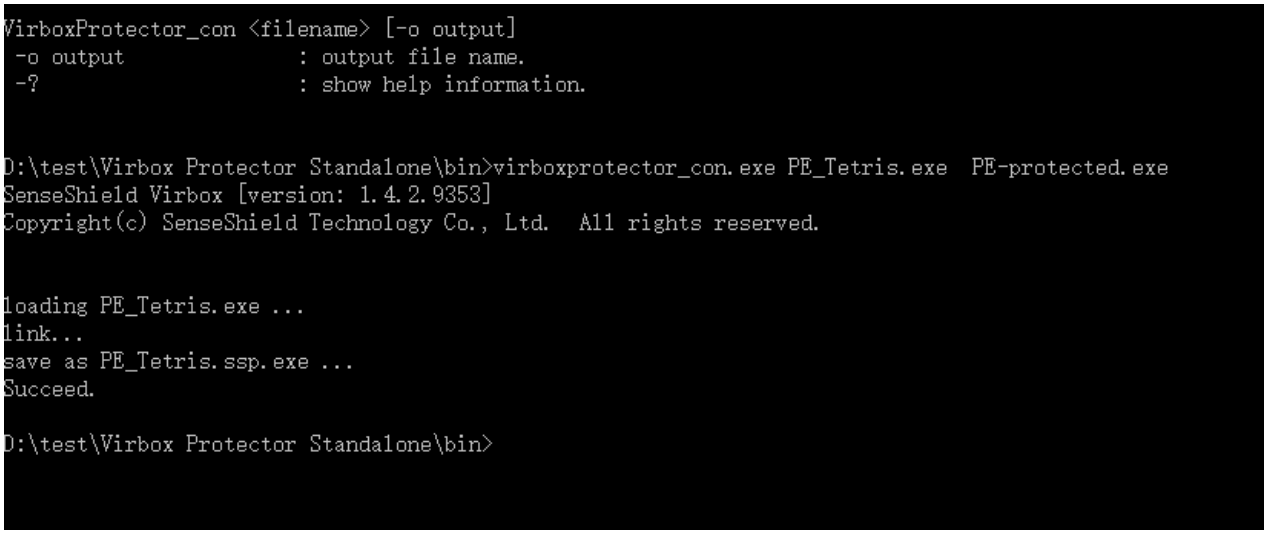


Figure 73

5 SDK label

This function is to locate the important function that need to be protected. When the program is written by C++ language, and you want to find the important function to protect. But only the address of the function would be shown. So this label will help you find the function you want to protect, and no need to find the function in thousands lines of code.

5.1 protect software by programming

Till now Virbox Protector Standalone supports to add those kind of label to the function:

VBProtectBegin: normal protection

VBVirtualizeBegin: Virtualization protection

VBMutateBegin: obfuscation protection

VBSnippetBegin: Code snippet protection

VBProtectDecrypt: License encryption and decryption function

Following is the guideline to use this function:

1. SDK can only be loaded statically and not supported to load dynamic link lib;
2. The parameter that imported by VBProtectBegin, VBVirtualizeBegin, VBSnippetBegin, VBMutateBegin can't be shared with other functions.
3. You need to make sure the imported parameter to be ASCII code, then the right function name would be shown, or it will show messy code.
4. Every begin will need to match an end, they need to use in pair, and only one pair is allowed in one function.
5. If the protection type in the label do not match with the protection type in Virbox Protector Standalone, the system will use the type of Virbox Protector Standalone
6. The code in between the Begin and End is better to more than 3 lines. To make sure the protected code be show correctly in the GUI of Virbox Protector Standalone.
7. SDK provides 32bit and 64bit dll, you do need to use the lib accordingly.
8. Not support Java, Unity3D.
9. Begin/end do not support nesting.
10. VBProtectDecrypt, the length of the encrypted string or buffer should be multi times of 16, i.e.:

char g_test_string[16] = {"test_decrypt"};

11. VBProtectDecrypt, the input buffer and output buffer can't be the same buffer.
12. VBProtectDecrypt, the buffer of input need to be out of the function, which means is a global variable. For detail how to use, please refer demo.
13. .Net program, is not supported by VBProtectDecrypt.

5.2 How to encrypt and decrypt the string by SDK

1. The encrypted string need to be a constant value.
2. VBDecryptData can be used to encrypt and decrypt the data, but the length and the data should be constant value.
3. The following type of string is supported:
   - String encryption:

     VBDecryptStringA("test_string");
   - Local static variable:

     static const char g_string[] = "test_string";
   - global variable:

     char g_test_string[] = "test_string";

     const char g_test_string[] = "test_string";

     static const char g_test_string[] = "test_string";

6 Note

Note:

- You can't use Virbox Protector Standalone to protect the protected software, any protected software can't be protected by Virbox Protector Standalone or third party Wrap tools to protect again.
- The protected .Net program only support Microsoft standard running lib, do not support third party running lib
- When you are protecting the command line to protect your software, the configuration file of the objective file should be exist.
- When you have used GetField("name", bindingAttr) in your program to be protected, if you use the obfuscation when protect software, the software may fail to run, and you need to remove the obfuscation protection.
- SDK label do not support the managed program that contain local source code.
- You may fail to protect the software with code snippet, this is because the too short instruction of the snippet code, maybe jump, and it can't be code ported.
- The name of the software after protection will change, please modify to be the original name. Maybe this will make the program can't be started.
- The ARX plugin of AutoCAD can only select "remote desk service dialog message box", and now only support win7 and server2008 or above version.
- If your Java program is based on spring framework, please use DSProtector to protect your program.
- Link is not supported by the program after compression
- Anti-varus AVAST may cause the start failed of the protected program, it will kill the thread of the thread of the protected software.
- Program with strong signature is not supported
- Anti-debug and code encryption & anti-memory break point is not supported at same time.
- DS plugin & Anti memory breakpoint is not supported at same time.

7 FAQ

7.1 What is the difference between the soft license version and dongle version?

For Virbox Protector Standalone with soft license mode: Only one device can use the license at one time, and you can use the license on up to 5 devices.

For Virbox Protector Standalone Dongle license mode: In addition to the software, you will also get a dongle that have license. You need to insert the dongle to the machine, and without device number limitation.

7.2 What is the difference between the trial version and standard version?

For a Trial version, you can only protect 5 of your functions to protect and evaluation.

If you want to protect more than 5 functions, the software will have prompt to remind you to buy a standard version.

When you run the protected software it will have the message pop up says:" **This application is protected with unregistered version of Virbox Protector Standalone**".

The protected Software program can be protected within 7 days for your internal testing and evaluation. You can extend the trial license if you can't complete testing within 7 days.

The trial version Virbox Protector Standalone will be expired after 30 days or 100 times usage.

For standard version, you can protect your functions without above limitation.

7.3 How to generate a map file?

1.1 Generate BCB Program Map, Project settings as shown below.

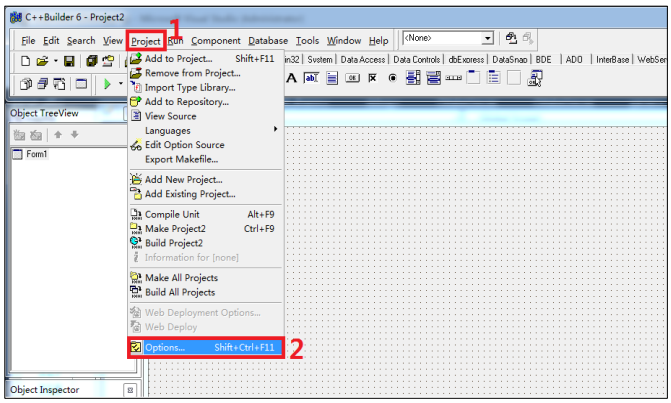


Figure 74

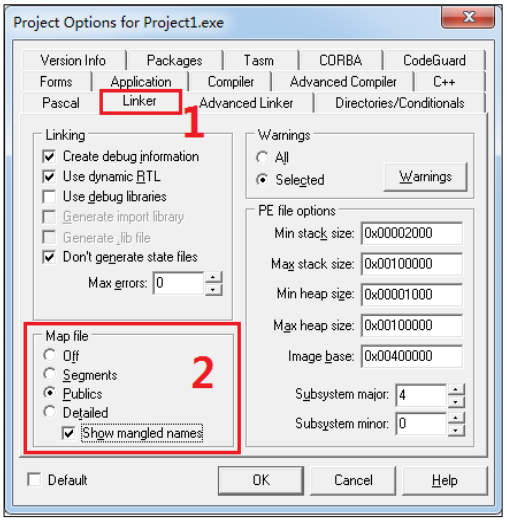


Figure 75

1.2 Generate vc program map, project settings as shown below.

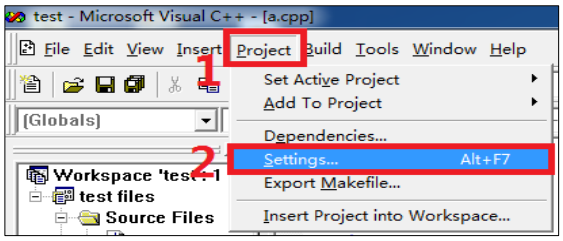


Figure 76

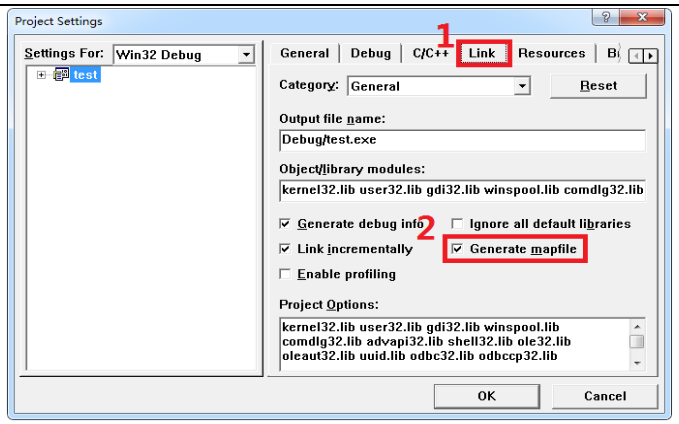


Figure 77

1.3 Generate VS program map, project settings as shown below.

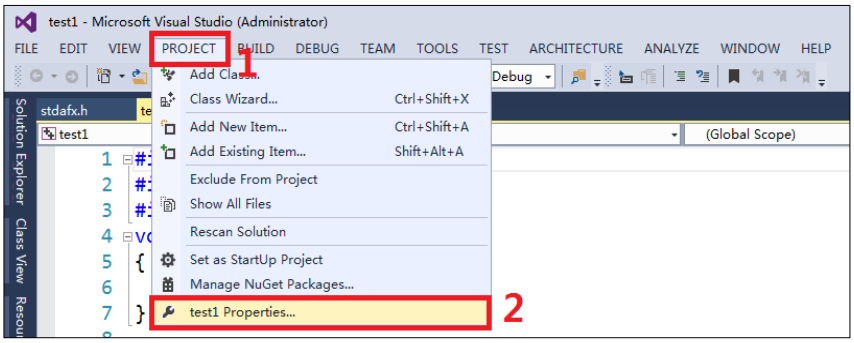


Figure 78

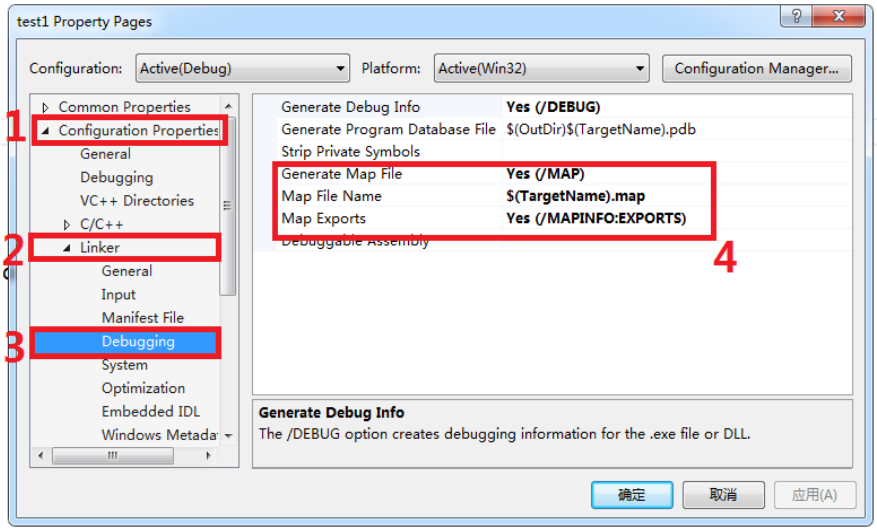


Figure 79

1.4 Generate Delphi program map, project settings as shown below.

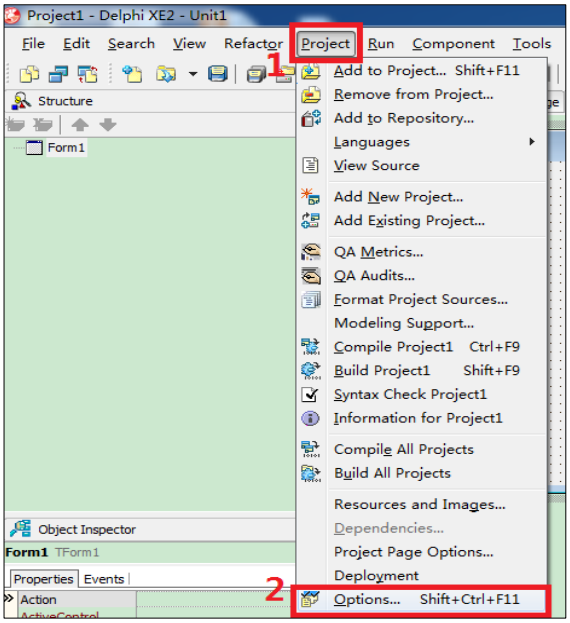


Figure 80

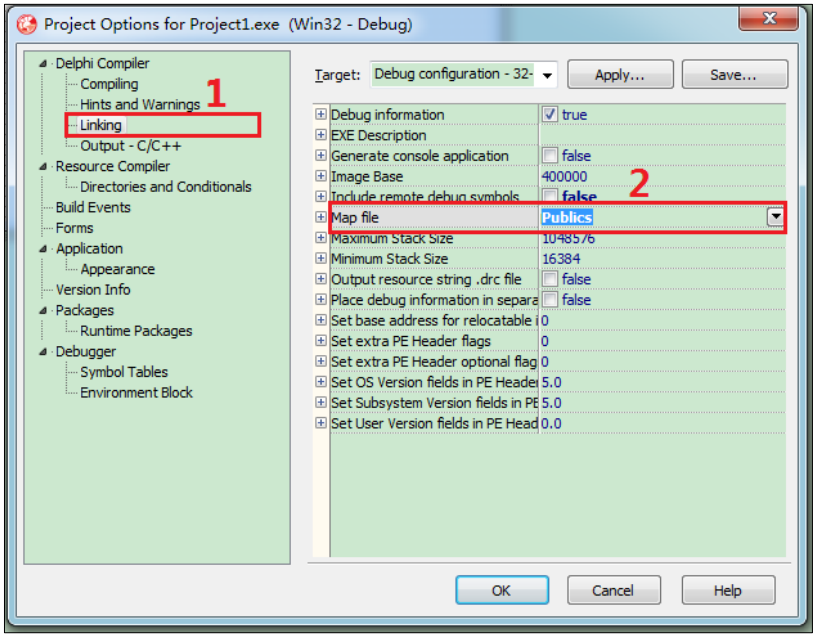


Figure 81

1.5 Generate a map of the vb6.0 program.

Add a "LINK" value to the system environment variable. The value is "/MAP". Restart the computer. This compiles and generates the exe program. The map file will not be automatically deleted, but will be retained.

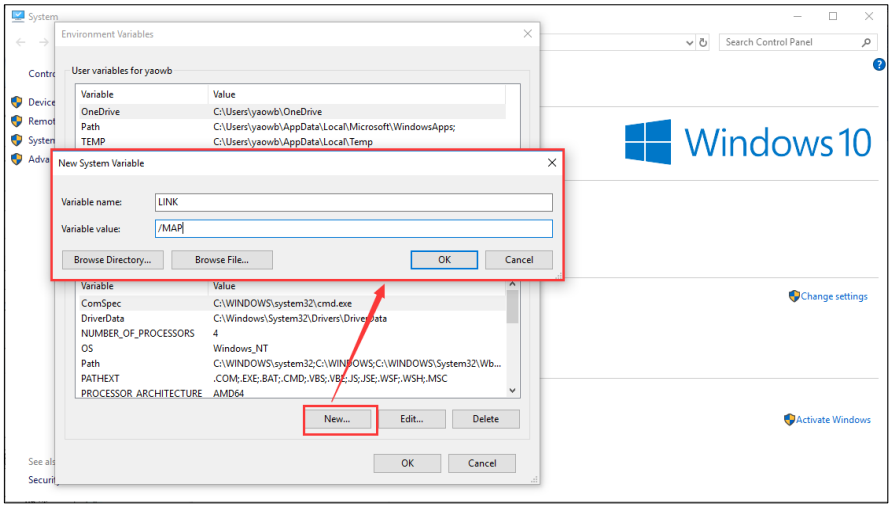


Figure 82

No matter which software area you come from, we have experts who understand the special challenges you are facing in your industry. We will help you solve those problem with what we have. And we have helped thousands of software enterprises from different industry to Protected the software and helped them realized software monetization. And we have established special Internet sales model and deeper customer relationships with our customer. We can also do this for you.