Orange Heap

User Manual

Version 1.3

team.orangeheap@gmail.com

Contents

Introduction

Orange Heap software is intended for protecting internals of your applications from any unauthorized uses. It features advanced obfuscation techniques such as: name mangling, string encryption, assemblies merging, cross assembly obfuscation and much more.

To make usage of software more convenient it has been split up on two independent executable: Windows application (*OrangeHeap.exe*) and Command-Line tool (*ohc.exe*). Both of them can be used for protecting your .NET software. But only Windows application allows user to create and to manage configuration file, which is used during protection and must exist due to possibility to run protection process. Command-Line tool can only use such configuration file by referencing it via command line parameter.

Windows application can create and manage options of such configuration files. After configuration is ready the application can save it and if it necessary run protection process.

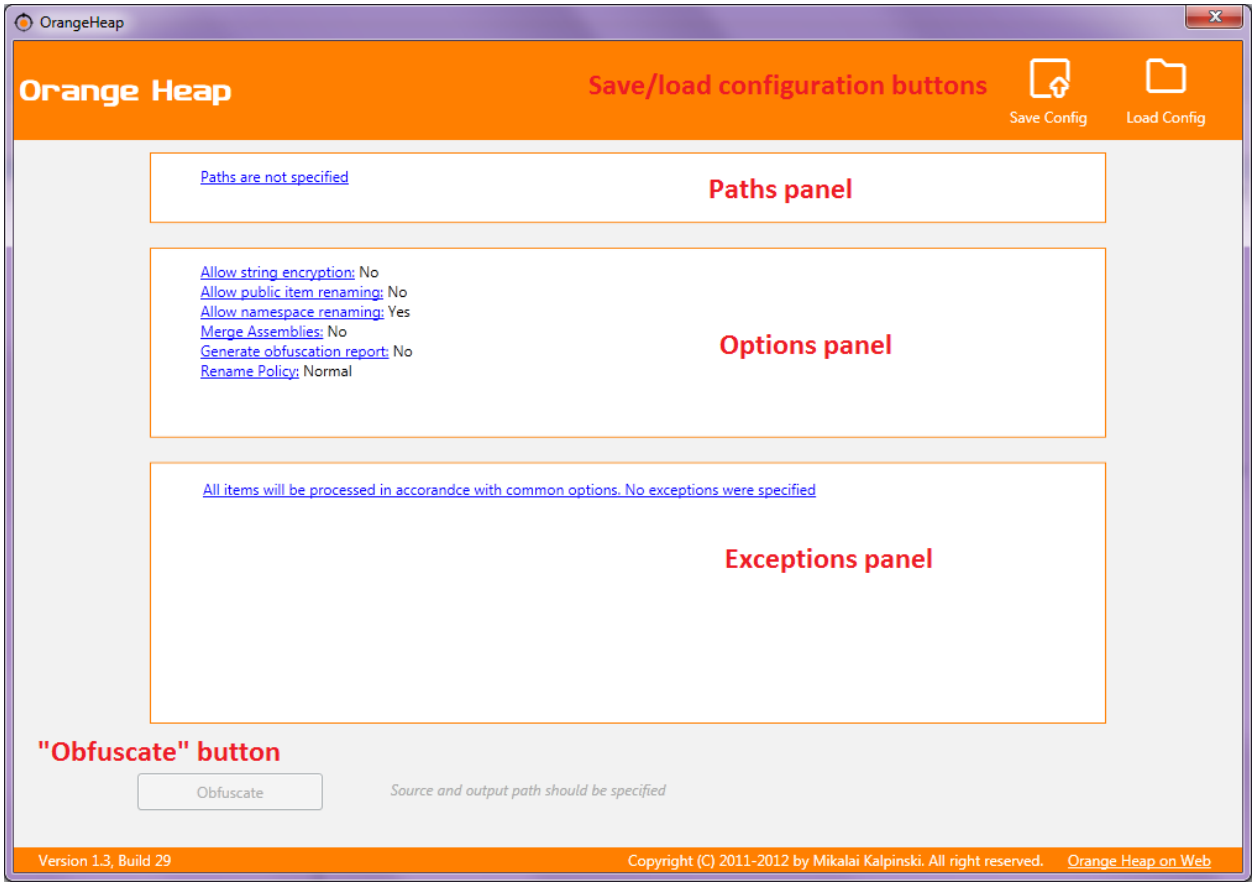
Command-Line tool can be used for automation protection process during the building the .NET solution or another batch process.

Windows application (*OrangeHeap.exe*)

Windows application can be used in the following cases:

1. Create/Update configuration file
2. Execute obfuscation process against the specified configuration file
3. Execute obfusction process against the configuration prepared on fly

Here is the Orange Heap main window as you can see on launching the application.



To continue you should specify paths:

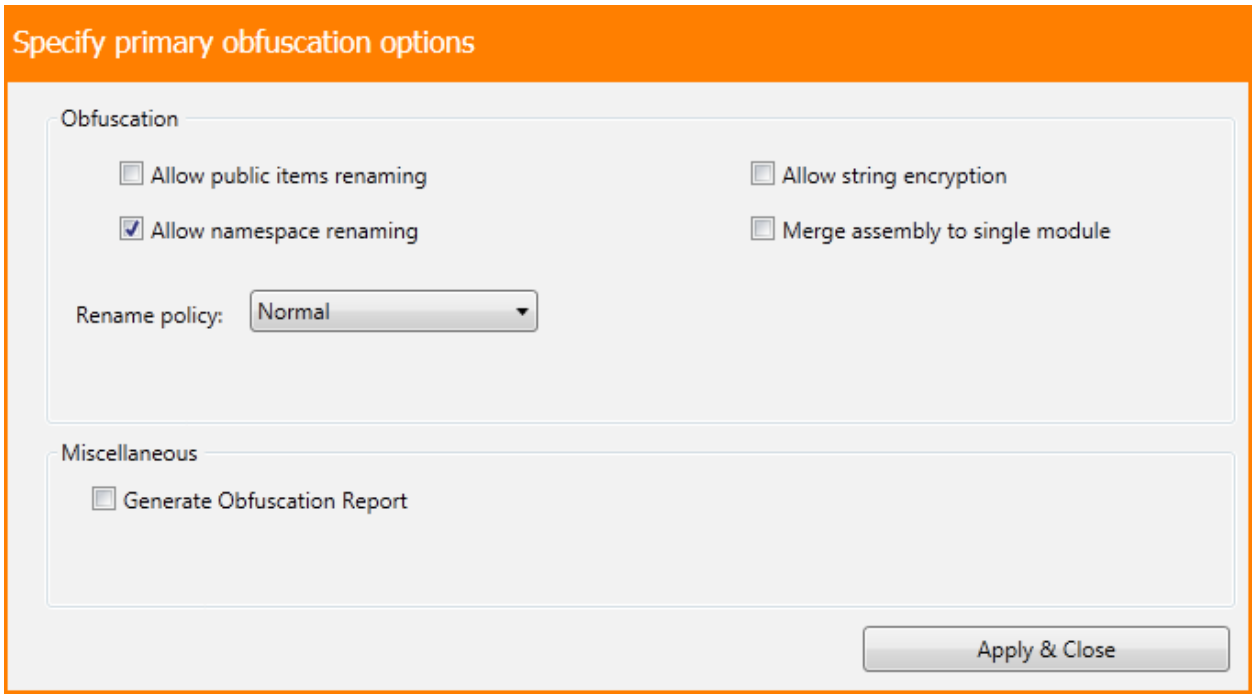
- source path – which files you want to obfuscate
- output path – where you want to put obfuscated files;

You can specify paths manually by clicking on "Paths are not specified" link on Paths panel, or by loading existent configuration file via "Load Config" button.

After you specified paths, all other options get enabled and you can set them appropriately.

Options dialog

Common options can be configured via Options dialog which will pop up on clicking on any item from Options panel.
Options dialog looks somehow like this:

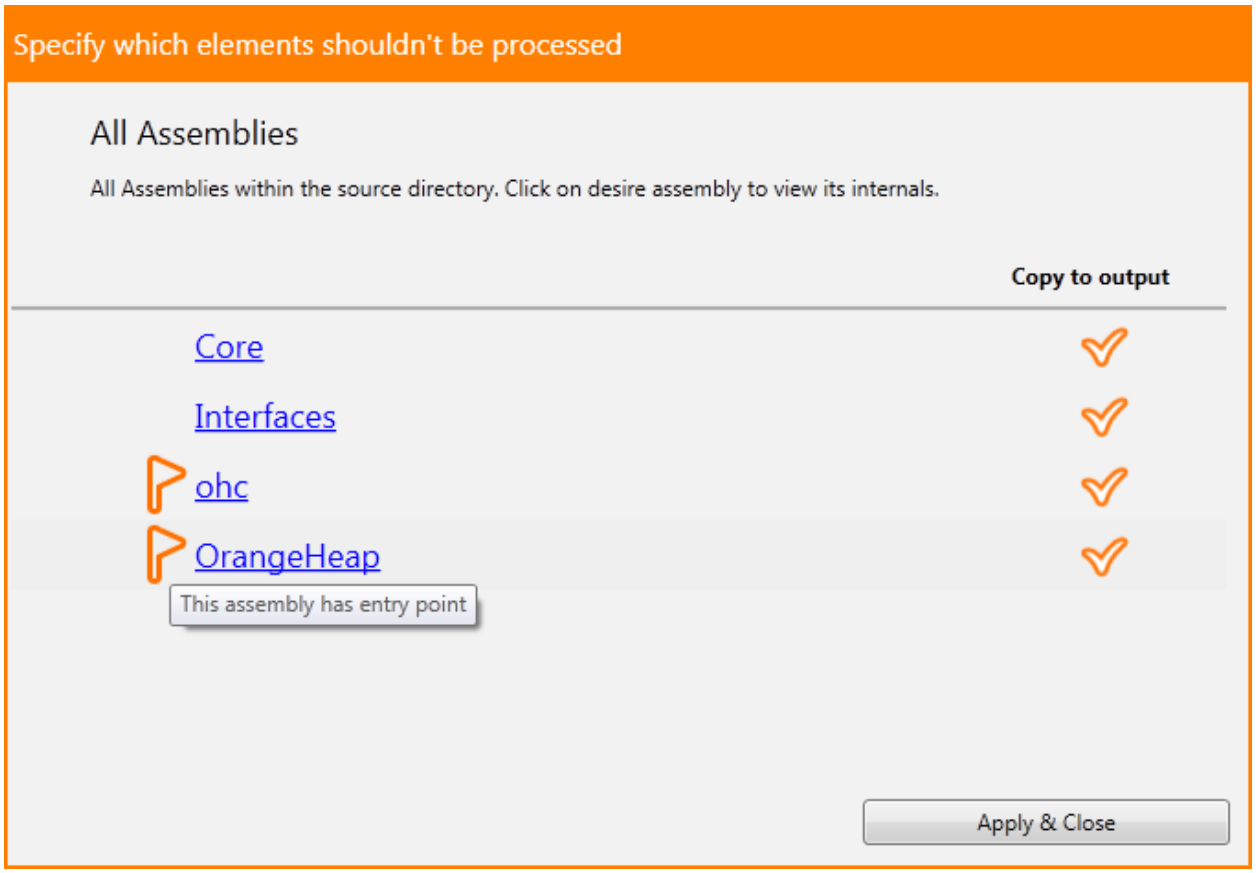


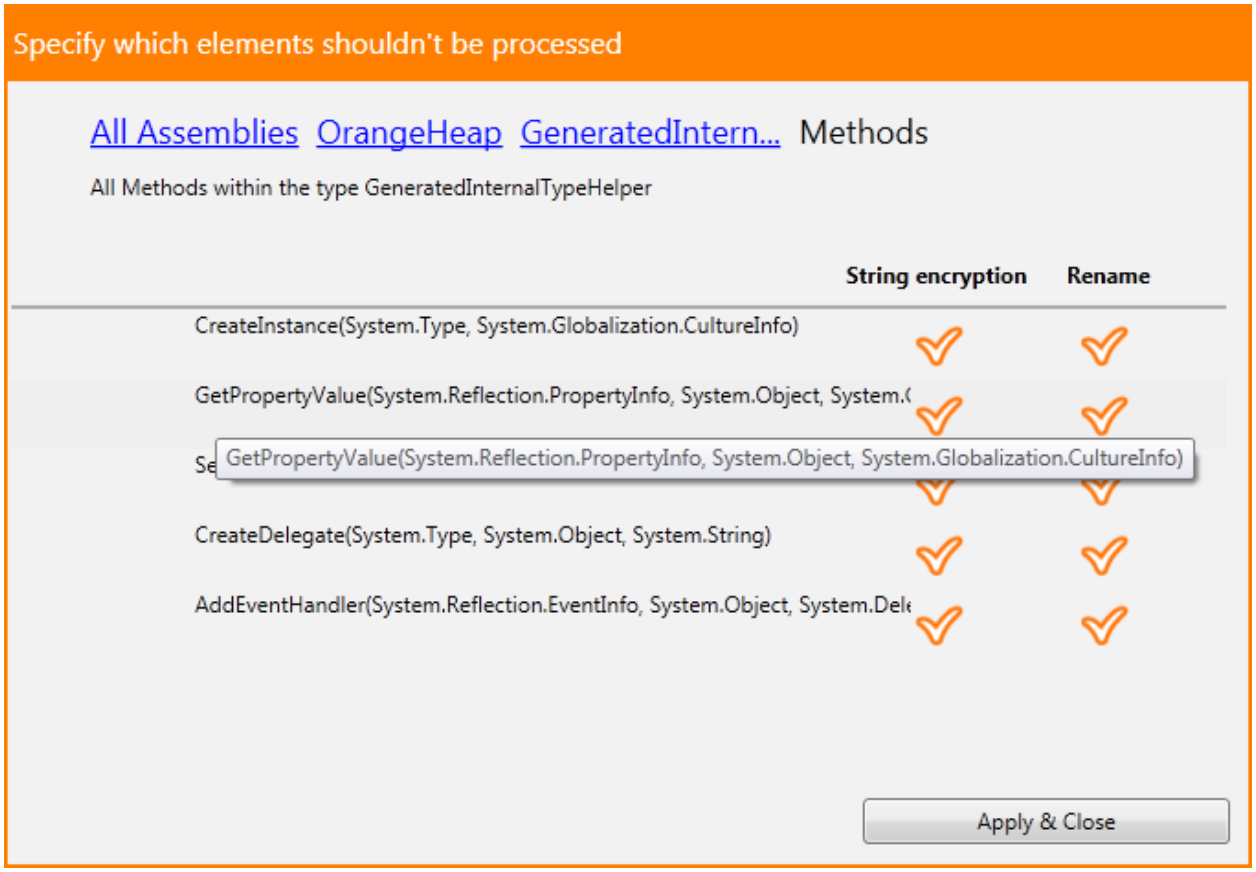
Options which can be configured here are the following:

- Allow public items renaming - If the option is enabled, then the public types and members will be obfuscated, otherwise only non-public items will be processed.
- Allow namespace renaming - If the option is enabled, then the namespaces will be obfuscated.
- Rename Policy - Specify how types and names will be obfuscated: *Developer* (using displayable symbols) or *Normal* (using non-displayable symbols).
- Allow string encryption - If the options is enabled, then the strings will be encrypted
- Merge assembly to single module - If the option is enabled, then all assemblies will be merged into the single assembly.
- Generate obfuscation report - If the option is enabled, then the obfuscation report will be generated. Report file will be named *report.xml* and placed to output directory on completing obfuscation process.

Exceptions dialog

By default all item (assemblies, types and theirs members) will be processed. But sometimes you will need to exclude some of them from processing. For example you may have requirements not to encrypt strings in some methods or not to rename some types. These are exceptions which can be configured via Exceptions dialog. It can be opened by clicking on any item from Exceptions panel. Exceptions dialog looks somehow like this:





Navigation between assemblies, types and their members can be performed by clicking on desire blue items. So you can easily navigate in forward (from assemblies to types and members) and backward (from members and types back to assemblies) directions.

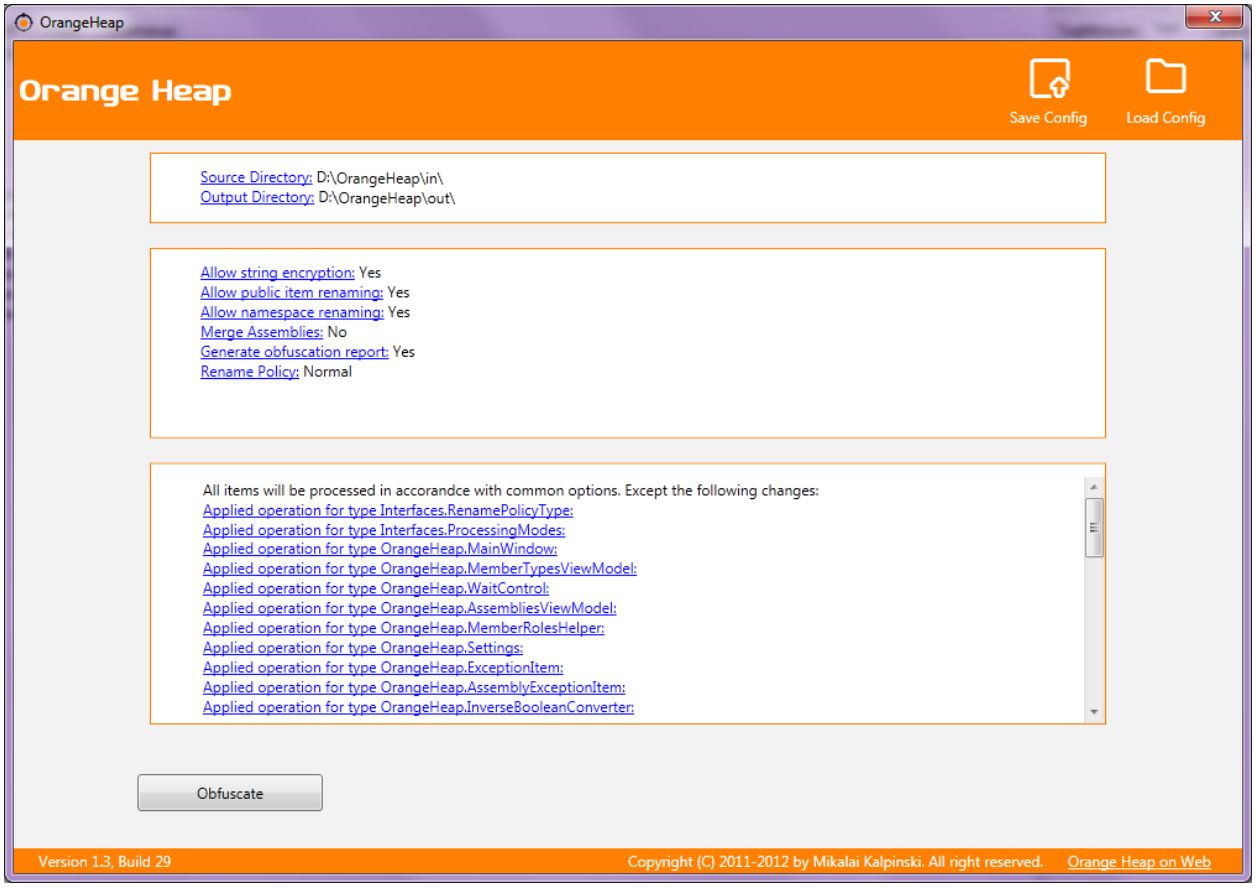
Here is the one rule – if item is blue – you can navigate to it by clicking on it.

While navigating through the assemblies, types and their member you can check/uncheck desire options for items as you wish. All this changes will be automatically taken into consideration on closing Exceptions dialog.

Execute obfuscation process and save configuration

Once you prepared your configuration you can briefly review all your options on main window.

Here, for example you can see options for obfuscating Orange binaries:

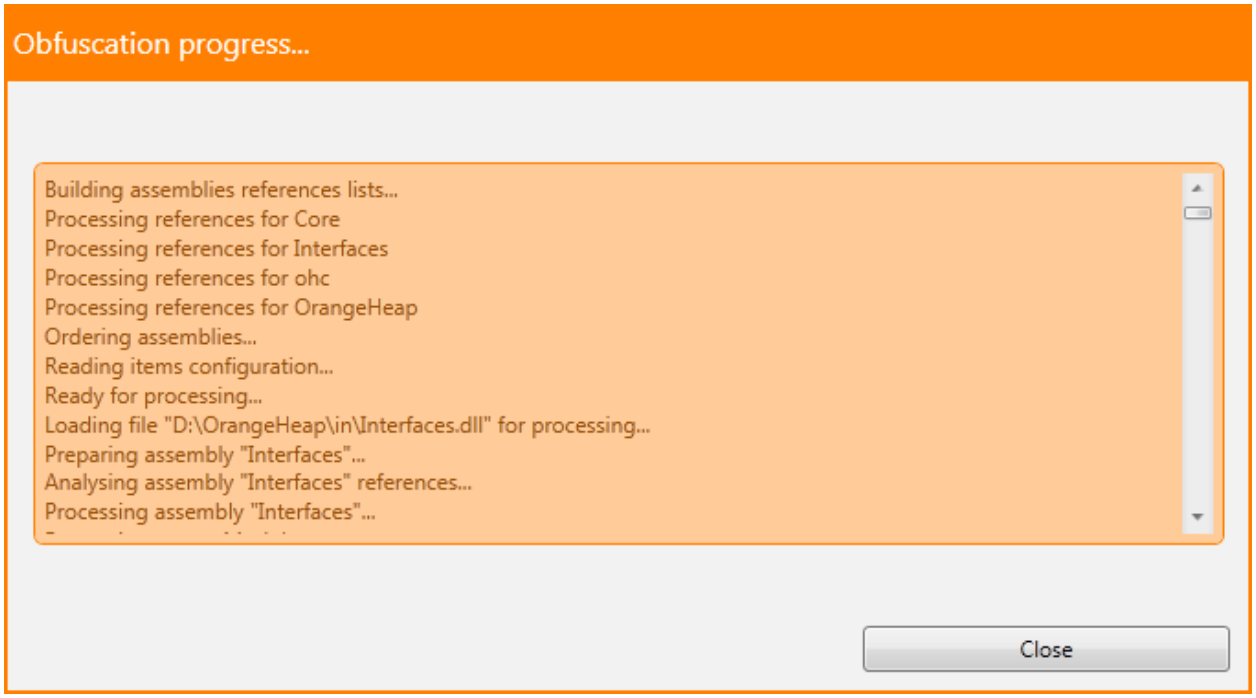


Now you can run obfuscation process against you configuration or save it into configuration file.

To save – click "Save Config" button and specify desire filename

To run obfuscation – click "Obfuscate" button. In this case Progress dialog will appear and will show you obfuscation progress.

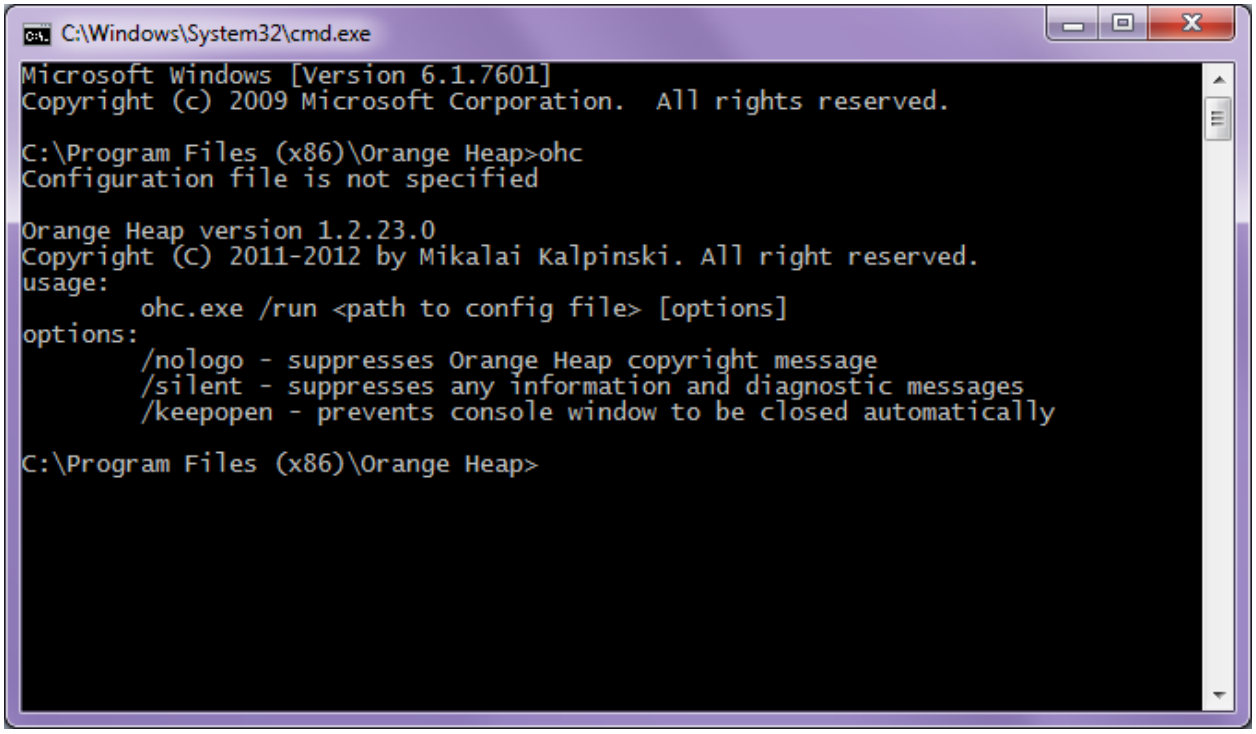
Progress dialog looks somehow like this:



Now all you need is to wait until Orange Heap software processes all you binaries.

Command-Line tool (*ohc.exe*)

The command-line tool can be used for executing protection process against the specified configuration file. Command-line tool and its usage are shown on the screenshot below.



Command Line Arguments:

/run *Config_filename*	Specifies full path to the file with configuration of the obfuscation process. See Configuration Structure File section more details. This is mandatory parameter.
/silent	Specifies that any information and diagnostic messages should not be displayed. This parameter is optional.
/nologo	Suppresses Orange Heap copyright message. This parameter is optional.
/keepopen	Prevents console window to be closed automatically. This parameter is optional.

Configuration file structure

```
<config name=”Project Name”>
	<options>
		<source path=”path” />
		<out path=”path” />
		<report path=”path” />
		<encryption enabled=”True | False” />
		<publicProcessing enabled=”True | False” />
		<merge enabled=”True | False” />
		<namespaceProcessing enabled="true" />
		<renameEngine name="Normal" />
	</options>
	<items mode=”Ignore | Accept”>
		<item assembly=”name” type=”name” member=” name”>
			<processing encryption=”True | False” renaming=”True | False” />
		</item>
		...
	</items>
</config>
```

The root element of the file is `config` node. The node can contain the following child sections:

Childs	Description
options	Contains common configuration for the processing. See section Options section configuration for more details.
items	Contains configuration for determining which items should be processed and how they should be processed. See section Items section configuration for more details.

Options sections configuration

This section is used for configuring the common options of the processing. See the table bellow for more details

Element	Attribute	Description
source	path	Specifies source folder with assemblies to obfuscate. All .NET assemblies within the folder will be processed by default. To ignore or not to process some assemblies the additional configuration via items section configuration.
out	path	Specifies destination folder for the obfuscated assemblies, rename report file and other results.
report	path	Creates report which contains information about renamed items. This report can be used for de-obfuscation in future. *Report_filename* should contain only filename with extension. File with specified name will be created in the destination folder
encryption	enabled	Specifies that string should be encrypted during processing .NET files from source folder. All string will be encrypted by default. To exclude some strings from the encryption the additional configuration via items section configuration.
publicProcessing	enabled	Specifies that all public types and members will be processed like other items. In this case it will be impossible to use the processed assemblies in another solutions as third-party because public contracts will be invalid.
namespaceProcessing	enabled	Specifies that namespaces will be renamed during the protection process.
renameEngine	name	"Normal" – uses non-displayed symbols for new names of the symbols, "Developer" – uses displayed symbols (i.e. "a1", "a314" and so on) for new names of the symbols
merge	enabled	Merges assemblies into the single module. Software automatically determines the main assembly and copies all type definitions from other assemblies into this one.

All elements from the table are mandatory.

Items section configuration

This section is used for configuring items (assemblies, types and members) to be processed, and strings of the items to be encrypted.

The root element of the section contains non-optional attribute `mode`. Available values of the attribute are the following:

Value	Description
Ignore	Determines, that all items from the source path (assemblies, types, members) by default are enabled for processing (processing includes copying to the output directory, taking part in merging, applying renaming and string encryption) except of items from the configuration file. In this mode configuration file specifies items which must be fully or partially (e.g. just copy to output without any renaming) ignored during the obfuscating process.
Accept	Determines, that all items from the source path by default are disabled for processing except of items from the configuration file. In this mode configuration file specifies items which must be fully or partially processed during the obfuscating.

Note: *If no configuration file provided or if the file doesn't contain `items` section, so mode of the processing is not defined, then software processes incoming files like "Ignore" mode is defined, i.e. all files from the source path being processed.*

The `items` element can contains one or more inner `item` elements which contain information about the target items (determining what definitely assemblies, types or members are going to be configured) and how these items should be processed or ignored depending on current mode.

Target items can be specified via the following attributes of the `item` element:

Attribute	Is Optional	Description
assembly	No	Specifies assembly name. All types from the assembly should be ignored or processed, depending on current mode.
type	Yes (*)	Specifies type name declared within the assembly. All members of the type should be ignored or processed, depending on current mode. This attribute can be skipped. (*) In the case when **member** is defined, the **type** attribute must be defined too.
member	Yes	Specifies member name of the type. All string within the member should be ignored or processed, depending on current mode. This attribute can be skipped.

Processing of the target items can be specified by the optional inner `processing` element and its attributes (`renaming` and `encryption`) which can be set to *True* or *False*.

Meaning of the `processing` element and its attributes varies depending on current mode. See the table below for more details.

	Ignore mode	Accept mode
processing element is not present	Target items should not be processed at all (i.e. do not copy to output, do not rename, do not encrypt strings of the target items). This situation is acceptable only for assembly-level, for type and members *processing* element should be always provided.	Target items should be fully processed at all (i.e. copied to output, renamed, encrypted strings of the target items) This situation is acceptable only for assembly-level, for type and members *processing* element should be always provided
processing element is present	Target items should be just copied to output	Used only for specifying values for attribute(s) of the element. If no attribute specified this situation is similar to previous one, when the element is not present
renaming = True	Target items should be only renamed	Doesn't make sense because it is set to True by default
renaming = False	Doesn't make sense because it is set to False by default	Target items should not be renamed
encryption = True	Only strings of target items should be encrypted	Doesn't make sense because it is set to True by default
encryption = False	Doesn't make sense because it is set to False by default	String of the target items should not be encrypted

See available samples of the configuration file with explanations for more details.

Configuration file samples

Sample of configuration file for "Ignore" mode:

Let's assume we initially have five assemblies: *Fruits*, *Vegetables*, *Berries*, *Mushrooms and Juices*.

We want to configure software in such way, that not all assemblies being processed. Please review the configuration file below:

```
01. <config>
        ...
02. <items mode="Ignore">
03.     <item assembly="Fruits" type="Apple">
04.             <processing renaming="True" />
05.     </item>
06.     <item assembly="Fruits" type="Pear">
07.             <processing renaming="True" />
08.     </item>
09.     <item assembly="Vegetables">
10.             <processing renaming="True" />
11.     </item>
12.     <item assembly="Berries" />
13.     <item assembly="Juices">
14.             <processing />
15.     </item>
16. </items>
        ...
17. </config>
```

Items from the configuration file are described in "Ignore" mode, i.e. all items by default are enabled for processing except of items from the configuration file. All items from the configuration file by default have all processing attributes set to false, except explicit specified values. So in other words, the configuration file can be read as follow:

Line 2: All items are enabled to be processed except the items described below:
Line 3: All items from assemblies with name "Fruits" and types with name "Apple" should be only renamed and copied to output, other processing like string encryption should be disabled.
Line 6: All items from assemblies with name "Fruits" and types with name "Pear" should be only renamed and copied to output, other processing like string encryption should be disabled.
Line 9: All items from assemblies with name "Vegetables" should be only renamed and copied to output, other processing like string encryption should be disabled.
Line 12: All assemblies with name "Berries" and all items from them should not be processed at all.
Line 13: All items from assemblies with name "Juices" should be copied to output, but their strings should not be encrypted and their items should not be renamed.

NOTE: assembly with name "Mushrooms" is not mentioned in the configuration file, so it should be fully processed (copied to output, renamed, etc.).

The result of processing the items by the software according with the supplied configuration file is the following:

Assembly	Copied to Output	Processed	String Encrypted
Fruits	Yes	Yes	Partially, strings from types *Apple* and *Pear* wouldn't be encrypted
Vegetables	Yes	Yes	No
Berries	No	-	-
Mushrooms	Yes	Yes	Yes
Juices	Yes	No	No

Sample of configuration file for "Accept" mode.

Let's assume we initially have five assemblies: *Fruits*, *Vegetables*, *Berries*, *Mushrooms and Juices*.

We want to configure software in such way, that not all assemblies being processed. Please review the configuration file below:

```
01. <config>
        ...
02. <items mode="Accept">
03.     <item assembly="Fruits">
04.             <processing encryption="False" />
05.     </item>
06.     <item assembly="Fruits" type="Apple" />
07.     <item assembly="Fruits" type="Pear" />
08.     <item assembly="Vegetables" />
09.     <item assembly="Mushrooms">
10.             <processing encryption="False" />
11.     </item>
12.     <item assembly="Juices">
13.             <processing encryption="False" renaming="False" />
14.     </item>
15. </items>
        ...
16. </config>
```

Items from the configuration file are described in "Accept" mode, i.e. all items by default are disabled for processing except of items from the configuration file. All items from the configuration file by default have all processing attributes set to true, except explicit specified values. So in other words, the configuration file can be read as follow:

Line 2: All items are disabled to be processed except the items described below:
Line 3: All items from assemblies with name "Fruits" should be fully processed, but their strings should not be encrypted.
Line 6: All items from assemblies with name "Fruits" and types with name "Apple" should be fully processed, including encryption of their strings (overrides rule from line 3)
Line 7: All items from assemblies with name "Fruits" and types with name "Pear" should be fully processed, including encryption of their strings (overrides rule from line 3)
Line 8: All items from assemblies with name "Vegetables" should be fully processed.
Line 9: All items from assemblies with name "Mushrooms" should be fully processed, but their strings should not be encrypted.
Line 12: All items from assemblies with name "Juices" should be copied to output, but their strings should not be encrypted and their items should not be renamed.

NOTE: assembly with name "Berries" is not mentioned in the configuration file, so it should be absolutely ignored.

The result of processing the items by the software according with the supplied configuration file is the following:

Assembly	Copied to Output	Processed	String Encrypted
Fruits	Yes	Yes	Partially, strings from types *Apple* and *Pear* would be encrypted
Vegetables	Yes	Yes	Yes
Berries	No	-	-
Mushrooms	Yes	Yes	No
Juices	Yes	No	No