# TUTORIAL: HOW TO DEOBFUSCATE ASSEMBLY-CSHARP.DLL

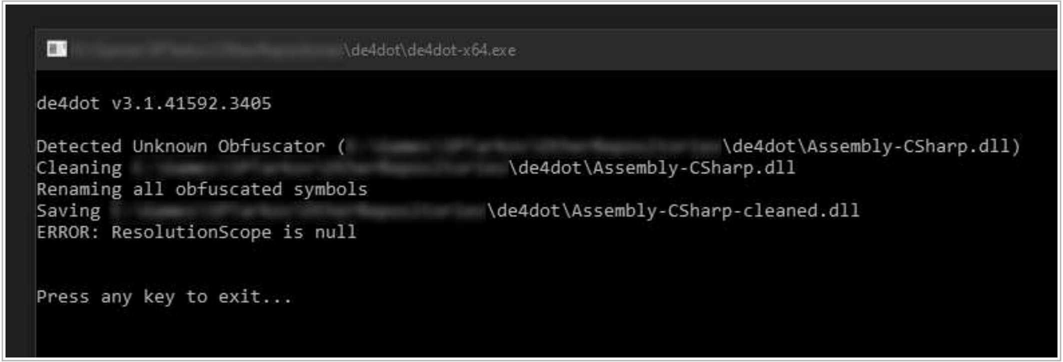
Terkoiz  Jul 26th 2021  Jan 13th 2022  3,861 times viewed

## Requirements:

- de4dot (specific version from Senko's dev repo - download here)
- dnSpy (download)

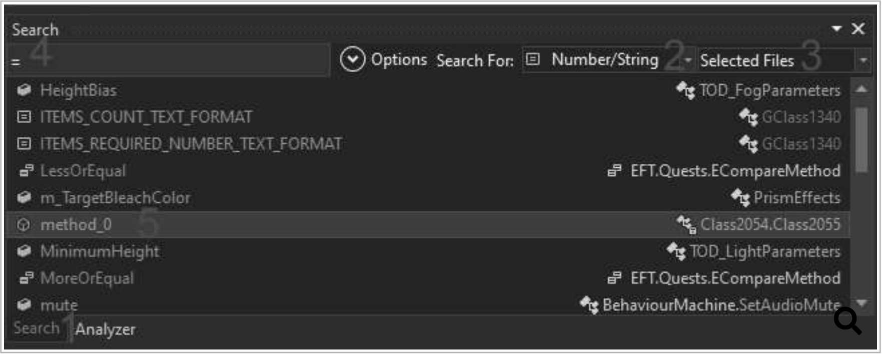
## 1 Deobfuscation

1. Copy-paste `EscapeFromTarkov_Data/Managed/Assembly-CSharp.dll` to where you extracted de4dot (same folder where `de4dot-x64.exe` is).
2. Drag and drop the `Assembly-CSharp.dll` on top of `de4dot-x64.exe`.
3. You should see the following:



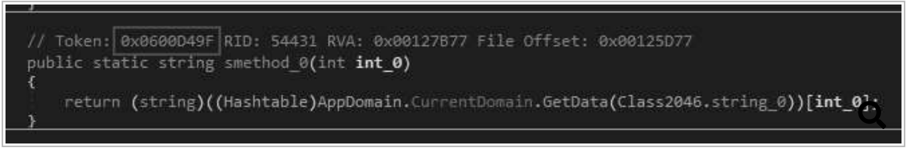
```
\de4dot\de4dot-x64.exe

de4dot v3.1.41592.3405

Detected Unknown Obfuscator (                    \de4dot\Assembly-CSharp.dll)
Cleaning                    \de4dot\Assembly-CSharp.dll
Renaming all obfuscated symbols
Saving                    \de4dot\Assembly-CSharp-cleaned.dll
ERROR: ResolutionScope is null


Press any key to exit...
```

   Next, you'll need to locate a token to finish cleaning the assembly.
4. Open the cleaned `Assembly-CSharp.dll` file in dnSpy (`File > Open...` OR `Ctrl+O`).
5. In the search tab[1], choose to search for `Number/String`[2] and set the search scope to `Selected Files`[3]. Then, type `=`[4] and you will get a bunch of
   We're looking for a method called `method_0`[5], which should be inside of a nested class. Double click it.



```
HeightBias                              TOD_FogParameters
ITEMS_COUNT_TEXT_FORMAT                 GClass1340
ITEMS_REQUIRED_NUMBER_TEXT_FORMAT       GClass1340
LessOrEqual                             EFT.Quests.ECompareMethod
m_TargetBleachColor                     PrismEffects
method_0                                Class2054.Class2055
MinimumHeight                           TOD_LightParameters
MoreOrEqual                             EFT.Quests.ECompareMethod
mute                                    BehaviourMachine.SetAudioMute
```

6. From there, you should be able to locate a method called `smethod_0`, near the top of the class. You want to copy the `Token` value, displayed above th
   definition:



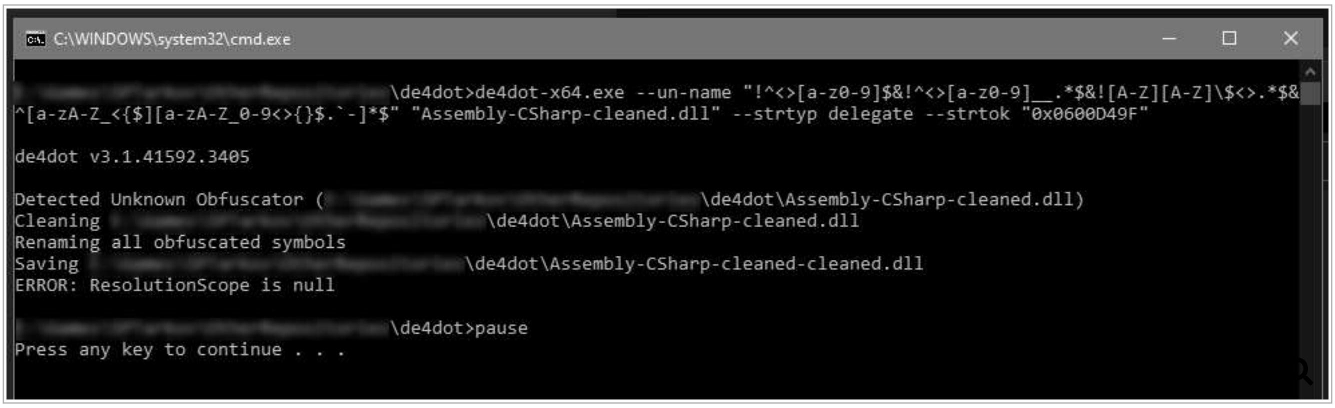
```
// Token: 0x0600D49F RID: 54431 RVA: 0x00127B77 File Offset: 0x00125D77
public static string smethod_0(int int_0)
{
    return (string)((Hashtable)AppDomain.CurrentDomain.GetData(Class2046.string_0))[int_0];
}
```

7. Now, create a .cmd file in the de4dot directory with the following contents:

```
de4dot-x64.exe --un-name "!^<>[a-z0-9]$&!^<>[a-z0-9]__.*$&![A-Z][A-Z]\$<>.*$&^[a-zA-Z_<{$][a-zA-Z_0-9<>{}$.`-]*$" "Assemb
-cleaned.dll" --strtyp delegate --strtok "YOUR TOKEN HERE"
pause
```

8. Replace the `YOUR TOKEN HERE` part with the token you copied (should look something like this: `--strtok "0x0600D49F"`).

9. Run your newly created .cmd file - if you copied the correct token, you should see this screen:



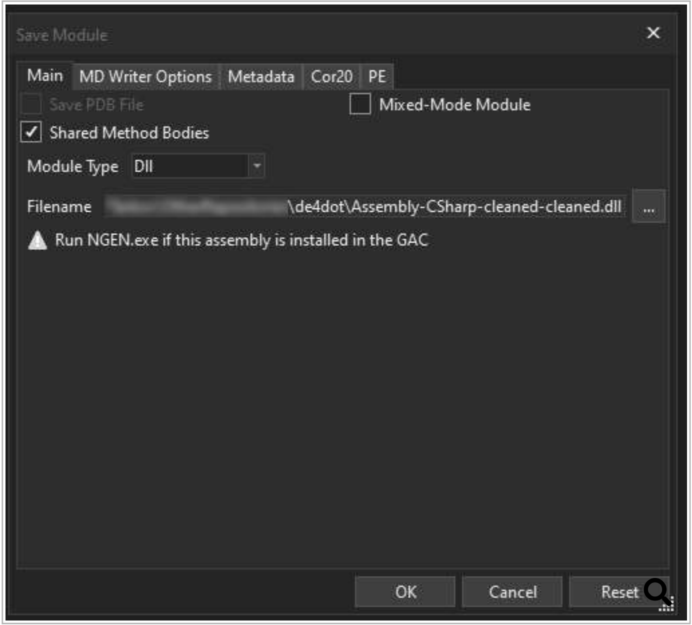
C:\WINDOWS\system32\cmd.exe

```
[redacted]\de4dot>de4dot-x64.exe --un-name "!^<>[a-z0-9]$&!^<>[a-z0-9]__.*$&![A-Z][A-Z]\$<>.*$&
^[a-zA-Z_<{$][a-zA-Z_0-9<>{}$.`-]*$" "Assembly-CSharp-cleaned.dll" --strtyp delegate --strtok "0x0600D49F"

de4dot v3.1.41592.3405

Detected Unknown Obfuscator ([redacted]\de4dot\Assembly-CSharp-cleaned.dll)
Cleaning [redacted]\de4dot\Assembly-CSharp-cleaned.dll
Renaming all obfuscated symbols
Saving [redacted]\de4dot\Assembly-CSharp-cleaned-cleaned.dll
ERROR: ResolutionScope is null

[redacted]\de4dot>pause
Press any key to continue . . .
```

If instead you get a screen with some `ERROR:` lines, where one of them ends with `Hmmmm... something didn't work` - you used the wrong token.

## 2 Fixing "ResolutionScope is null"

1. In dnSpy, clear your workspace (`File > Close All`)
2. Then, do `File > Open...` and go to your EFT install location, then `EscapeFromTarkov_Data/Managed/` and open **ALL** the files inside.
3. After that, do `File > Open...` once more, and go to wherever de4dot is located, and open `Assembly-CSharp-cleaned-cleaned.dll`.
4. While the file is still selected in the "Assembly Explorer", do `File > Save Module...`. The "filename" field should have `\Assembly-CSharp-cleanec` `dll` at the end. Click `Ok`.



Save Module

□ Save PDB File

□ Mixed-Mode Module

☑ Shared Method Bodies

Module Type: Dll

Filename: [redacted]\de4dot\Assembly-CSharp-cleaned-cleaned.dll

Run NGEN.exe if this assembly is installed in the GAC

That's it! You have a cleaned and deobfuscated assembly. Stay tuned for a guide on how to create .bpf patches, which can be used to update the assembly .bpf launcher with the assembly you just prepared.

## 3 Notes

If finding the token in the deobfuscation step fails, search manually through all ClassXXXX (**NOT GClassXXXX**) until you find a method that looks akin to this:

### Code

```
// Token: 0x0600D56B RID: 54635 RVA: 0x0012870F File Offset: 0x0012690F
// Note: Class2056 might look different
public static string smethod_0(int int_0)
{
    return (string)((Hashtable)AppDomain.CurrentDomain.GetData(Class2056.string_0))[int_0];
}
```

Use the token of the found method and continue from there.