# De-Confused-Ex

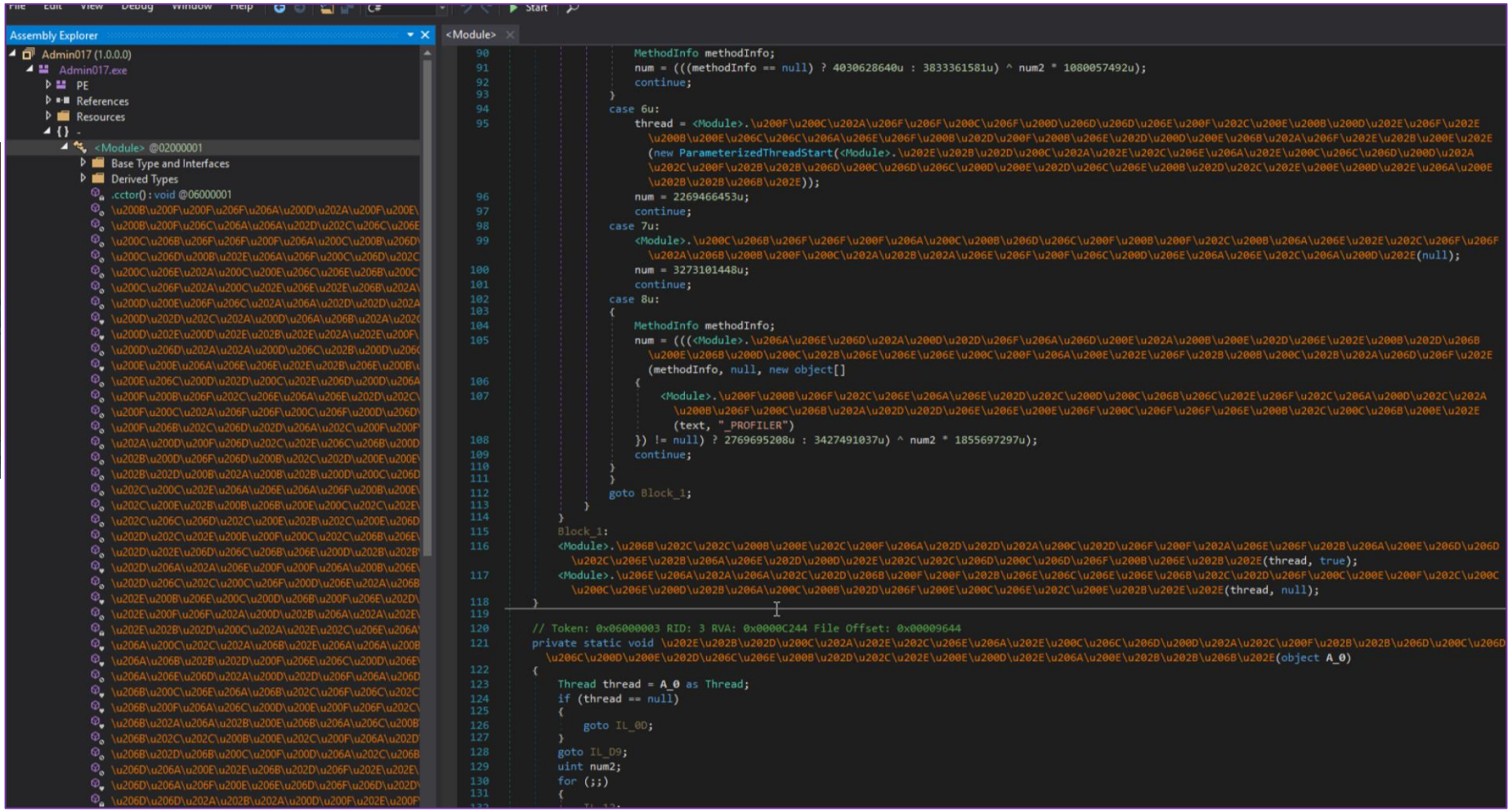
## Reversing ConfuserEx Obfuscated Binaries

Presenter: Shannon Lucas

# Agenda

- Confused
- Dumping Modules
- Header Reconstruction
- De-obfuscate
- Reflective Decryption
- Perseverance
- Issues

# Confused


Assembly Explorer
Admin017 (1.0.0.0)
Admin017.exe
PE
References
Resources
<Module> @02000001
Base Type and Interfaces
Derived Types
.cctor() : void @06000001
<Module>
// Token: 0x06000003 RID: 3 RVA: 0x0000C244 File Offset: 0x00009644
private static void
{
Thread thread = A_0 as Thread;
if (thread == null)
goto IL_0D;
goto IL_D9;
uint num2;
for (;;)

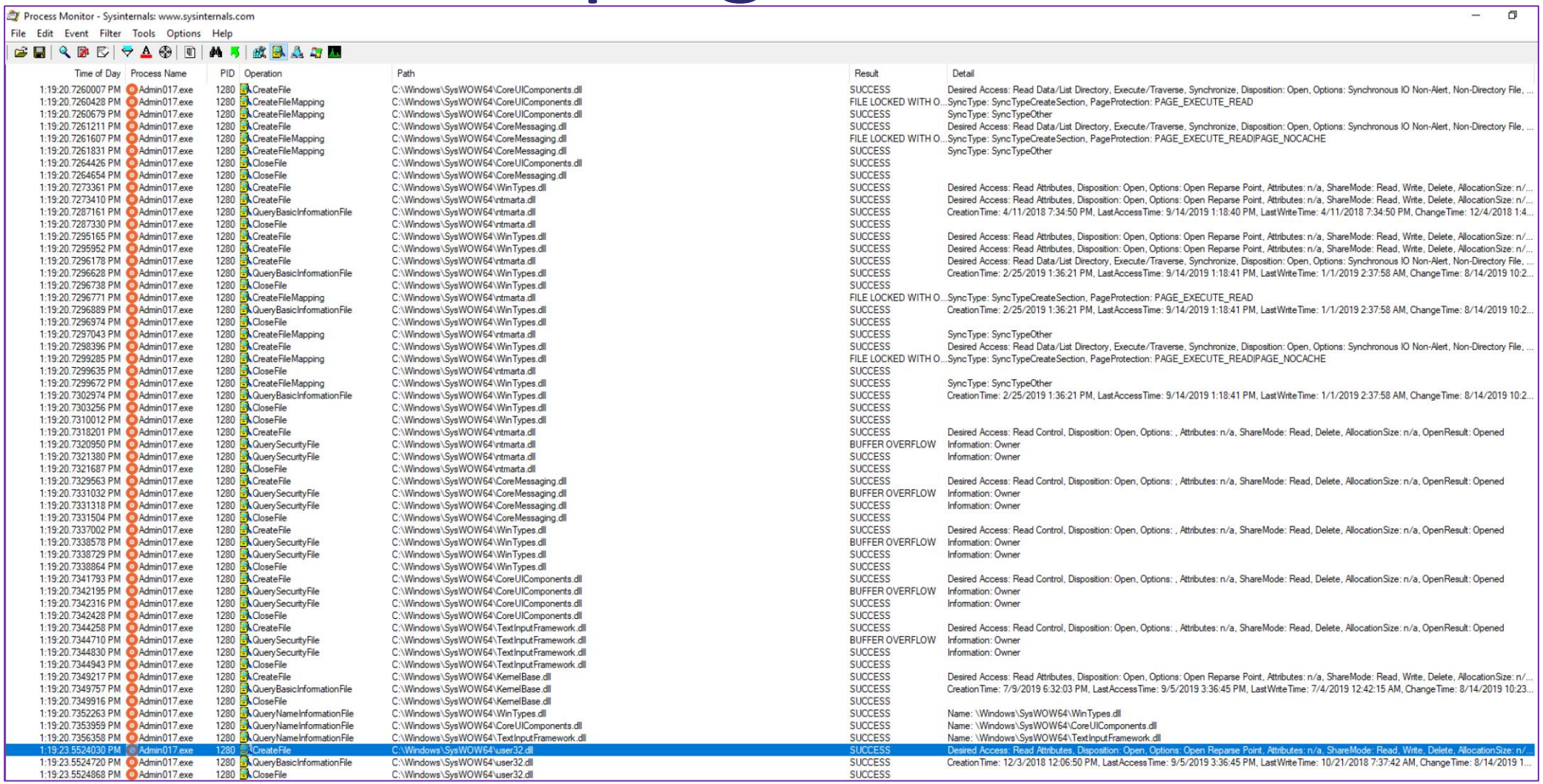
# Confused

Big shout out to Matt Graeber for explaining this black magic to me

# Dumping Modules

- Use Procmon to determine dlls that get loaded
- Load up executable with Windbg(x86)  (Binary is x86)
    - Or load binary with PowerShell and attach to PowerShell process with Windbg
- Break on a function that executes after Confuser has unpacked
- Dump module from memory
- Header Reconstruction

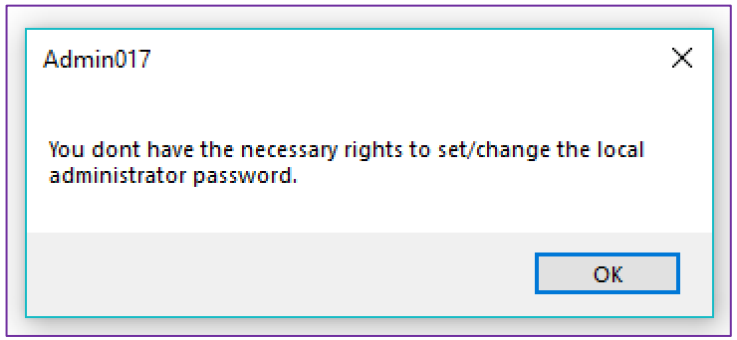
# Dumping Modules

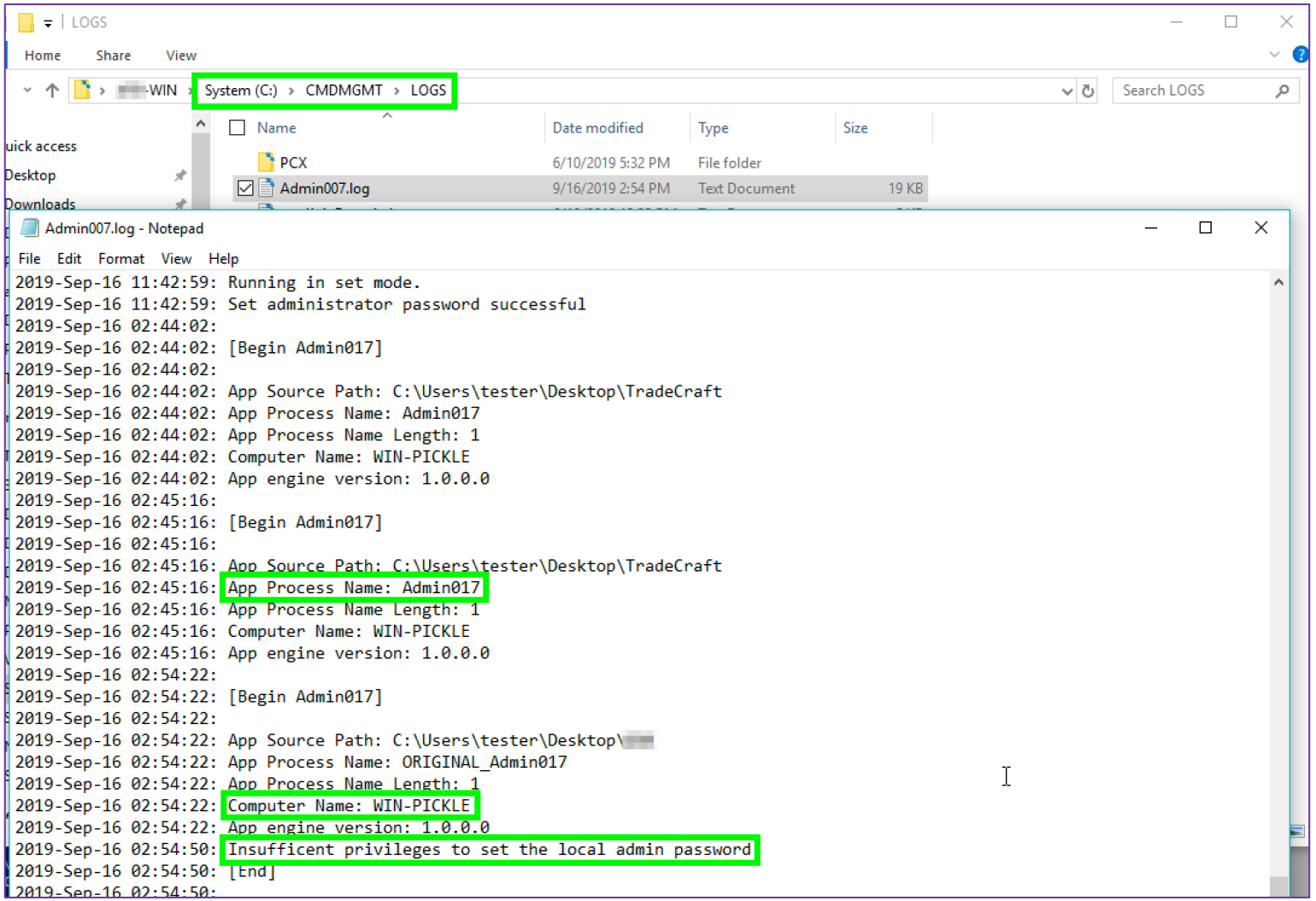



| Time of Day | Process Name | PID | Operation | Path | Result | Detail |
|---|---|---|---|---|---|---|
| 1:19:20.7260007 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\CoreUIComponents.dll | SUCCESS | Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, ... |
| 1:19:20.7260428 PM | Admin017.exe | 1280 | CreateFileMapping | C:\Windows\SysWOW64\CoreUIComponents.dll | FILE LOCKED WITH O... | SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READ |
| 1:19:20.7260679 PM | Admin017.exe | 1280 | CreateFileMapping | C:\Windows\SysWOW64\CoreUIComponents.dll | SUCCESS | SyncType: SyncTypeOther |
| 1:19:20.7261211 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\CoreMessaging.dll | SUCCESS | Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, ... |
| 1:19:20.7261607 PM | Admin017.exe | 1280 | CreateFileMapping | C:\Windows\SysWOW64\CoreMessaging.dll | FILE LOCKED WITH O... | SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READ\|PAGE_NOCACHE |
| 1:19:20.7261831 PM | Admin017.exe | 1280 | CreateFileMapping | C:\Windows\SysWOW64\CoreMessaging.dll | SUCCESS | SyncType: SyncTypeOther |
| 1:19:20.7264426 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\CoreUIComponents.dll | SUCCESS | |
| 1:19:20.7264654 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\CoreMessaging.dll | SUCCESS | |
| 1:19:20.7273361 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/... |
| 1:19:20.7273410 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\ntmarta.dll | SUCCESS | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/... |
| 1:19:20.7287161 PM | Admin017.exe | 1280 | QueryBasicInformationFile | C:\Windows\SysWOW64\ntmarta.dll | SUCCESS | CreationTime: 4/11/2018 7:34:50 PM, LastAccessTime: 9/14/2019 1:18:40 PM, LastWriteTime: 4/11/2018 7:34:50 PM, ChangeTime: 12/4/2018 1:4... |
| 1:19:20.7287330 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\ntmarta.dll | SUCCESS | |
| 1:19:20.7295165 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/... |
| 1:19:20.7295952 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/... |
| 1:19:20.7296178 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\ntmarta.dll | SUCCESS | Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, ... |
| 1:19:20.7296628 PM | Admin017.exe | 1280 | QueryBasicInformationFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | CreationTime: 2/25/2019 1:36:21 PM, LastAccessTime: 9/14/2019 1:18:41 PM, LastWriteTime: 1/1/2019 2:37:58 AM, ChangeTime: 8/14/2019 10:2... |
| 1:19:20.7296738 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | |
| 1:19:20.7296771 PM | Admin017.exe | 1280 | CreateFileMapping | C:\Windows\SysWOW64\ntmarta.dll | FILE LOCKED WITH O... | SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READ |
| 1:19:20.7296889 PM | Admin017.exe | 1280 | QueryBasicInformationFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | CreationTime: 2/25/2019 1:36:21 PM, LastAccessTime: 9/14/2019 1:18:41 PM, LastWriteTime: 1/1/2019 2:37:58 AM, ChangeTime: 8/14/2019 10:2... |
| 1:19:20.7296974 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | |
| 1:19:20.7297043 PM | Admin017.exe | 1280 | CreateFileMapping | C:\Windows\SysWOW64\ntmarta.dll | SUCCESS | SyncType: SyncTypeOther |
| 1:19:20.7298396 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, ... |
| 1:19:20.7299285 PM | Admin017.exe | 1280 | CreateFileMapping | C:\Windows\SysWOW64\WinTypes.dll | FILE LOCKED WITH O... | SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READ\|PAGE_NOCACHE |
| 1:19:20.7299635 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\ntmarta.dll | SUCCESS | |
| 1:19:20.7299672 PM | Admin017.exe | 1280 | CreateFileMapping | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | SyncType: SyncTypeOther |
| 1:19:20.7302974 PM | Admin017.exe | 1280 | QueryBasicInformationFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | CreationTime: 2/25/2019 1:36:21 PM, LastAccessTime: 9/14/2019 1:18:41 PM, LastWriteTime: 1/1/2019 2:37:58 AM, ChangeTime: 8/14/2019 10:2... |
| 1:19:20.7303256 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | |
| 1:19:20.7310012 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | |
| 1:19:20.7318201 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\ntmarta.dll | SUCCESS | Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: Opened |
| 1:19:20.7320950 PM | Admin017.exe | 1280 | QuerySecurityFile | C:\Windows\SysWOW64\ntmarta.dll | BUFFER OVERFLOW | Information: Owner |
| 1:19:20.7321380 PM | Admin017.exe | 1280 | QuerySecurityFile | C:\Windows\SysWOW64\ntmarta.dll | SUCCESS | Information: Owner |
| 1:19:20.7321687 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\ntmarta.dll | SUCCESS | |
| 1:19:20.7329563 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\CoreMessaging.dll | SUCCESS | Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: Opened |
| 1:19:20.7331032 PM | Admin017.exe | 1280 | QuerySecurityFile | C:\Windows\SysWOW64\CoreMessaging.dll | BUFFER OVERFLOW | Information: Owner |
| 1:19:20.7331318 PM | Admin017.exe | 1280 | QuerySecurityFile | C:\Windows\SysWOW64\CoreMessaging.dll | SUCCESS | Information: Owner |
| 1:19:20.7331504 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\CoreMessaging.dll | SUCCESS | |
| 1:19:20.7337002 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: Opened |
| 1:19:20.7338578 PM | Admin017.exe | 1280 | QuerySecurityFile | C:\Windows\SysWOW64\WinTypes.dll | BUFFER OVERFLOW | Information: Owner |
| 1:19:20.7338729 PM | Admin017.exe | 1280 | QuerySecurityFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | Information: Owner |
| 1:19:20.7338864 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | |
| 1:19:20.7341793 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\CoreUIComponents.dll | SUCCESS | Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: Opened |
| 1:19:20.7342195 PM | Admin017.exe | 1280 | QuerySecurityFile | C:\Windows\SysWOW64\CoreUIComponents.dll | BUFFER OVERFLOW | Information: Owner |
| 1:19:20.7342316 PM | Admin017.exe | 1280 | QuerySecurityFile | C:\Windows\SysWOW64\CoreUIComponents.dll | SUCCESS | Information: Owner |
| 1:19:20.7342428 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\CoreUIComponents.dll | SUCCESS | |
| 1:19:20.7344258 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\TextInputFramework.dll | SUCCESS | Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: Opened |
| 1:19:20.7344710 PM | Admin017.exe | 1280 | QuerySecurityFile | C:\Windows\SysWOW64\TextInputFramework.dll | BUFFER OVERFLOW | Information: Owner |
| 1:19:20.7344830 PM | Admin017.exe | 1280 | QuerySecurityFile | C:\Windows\SysWOW64\TextInputFramework.dll | SUCCESS | Information: Owner |
| 1:19:20.7344943 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\TextInputFramework.dll | SUCCESS | |
| 1:19:20.7349217 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\KernelBase.dll | SUCCESS | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/... |
| 1:19:20.7349757 PM | Admin017.exe | 1280 | QueryBasicInformationFile | C:\Windows\SysWOW64\KernelBase.dll | SUCCESS | CreationTime: 7/9/2019 6:32:03 PM, LastAccessTime: 9/5/2019 3:36:45 PM, LastWriteTime: 7/4/2019 12:42:15 AM, ChangeTime: 8/14/2019 10:23... |
| 1:19:20.7349916 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\KernelBase.dll | SUCCESS | |
| 1:19:20.7352263 PM | Admin017.exe | 1280 | QueryNameInformationFile | C:\Windows\SysWOW64\WinTypes.dll | SUCCESS | Name: \Windows\SysWOW64\WinTypes.dll |
| 1:19:20.7353959 PM | Admin017.exe | 1280 | QueryNameInformationFile | C:\Windows\SysWOW64\CoreUIComponents.dll | SUCCESS | Name: \Windows\SysWOW64\CoreUIComponents.dll |
| 1:19:20.7356358 PM | Admin017.exe | 1280 | QueryNameInformationFile | C:\Windows\SysWOW64\TextInputFramework.dll | SUCCESS | Name: \Windows\SysWOW64\TextInputFramework.dll |
| 1:19:23.5524030 PM | Admin017.exe | 1280 | CreateFile | C:\Windows\SysWOW64\user32.dll | SUCCESS | Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/... |
| 1:19:23.5524720 PM | Admin017.exe | 1280 | QueryBasicInformationFile | C:\Windows\SysWOW64\user32.dll | SUCCESS | CreationTime: 12/3/2018 12:06:50 PM, LastAccessTime: 9/5/2019 3:36:45 PM, LastWriteTime: 10/21/2018 7:37:42 AM, ChangeTime: 8/14/2019 1... |
| 1:19:23.5524868 PM | Admin017.exe | 1280 | CloseFile | C:\Windows\SysWOW64\user32.dll | SUCCESS | |

# Dumping Modules

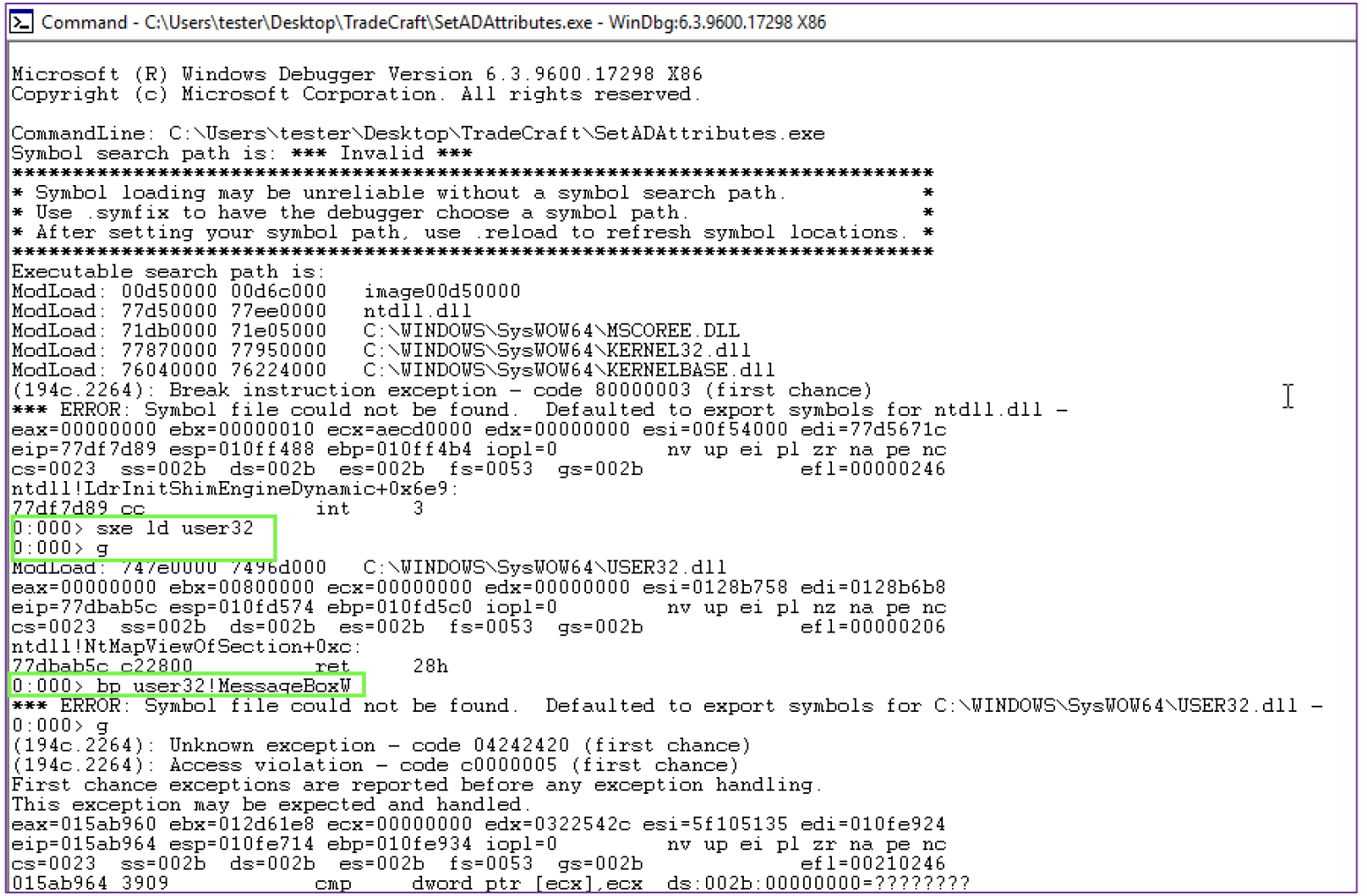
- Binary pops MessageBox if it's not run as admin.
- Creates Logs folder and log file
- Log file specifies App Process Name, Computer Name, and whether it successfully set the Admin password.



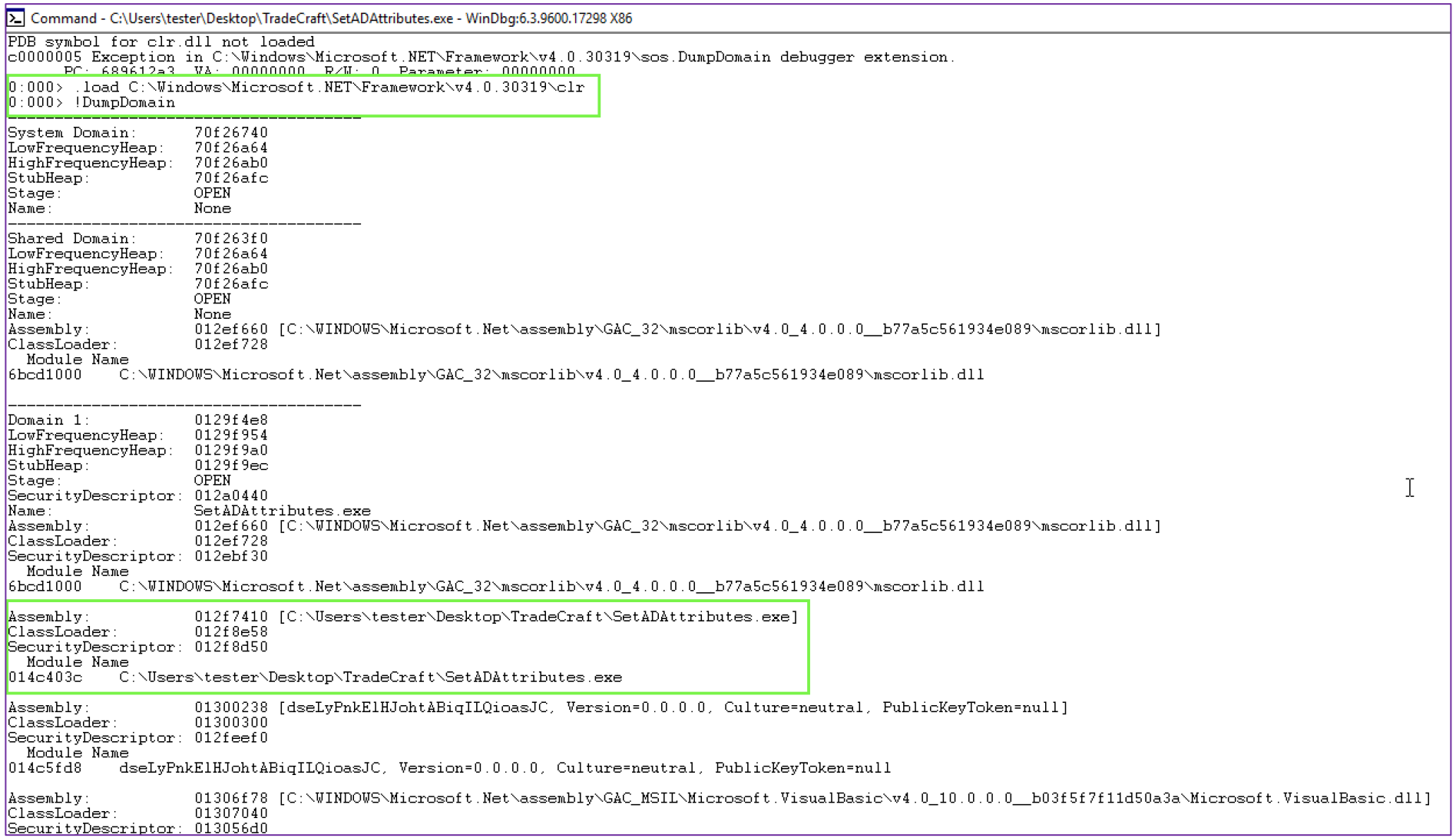
# Dumping Modules

- Break on user32 module load
- Continue
- Set breakpoint for MessageBoxW call from user32 module
- Continue



# Dumping Modules

- Load clr
- DumpDomain (list loaded assemblies in AppDomain with object address)



# Dumping Modules

```
ClassLoader:         0131e960
SecurityDescriptor: 0131eed0
  Module Name
65d31000    C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\System.Xml\v4.0_4.0.0.0__b77a5c561934e089\System.Xml.dll

Assembly:            0132cfd0 [C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remot
ClassLoader:         013292d0
SecurityDescriptor: 01328e98
  Module Name
5ddd1000    C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\System.Runtime.Remoting\v4.0_4.0.0.0__b77a5c561934e089\System.Runtime.Remoting.dll

Assembly:            01338d60 [C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\System.DirectoryServices.AccountManagement\v4.0_4.0.0.0__b77a5c561934e089\S
ClassLoader:         01338e28
SecurityDescriptor: 01338888
  Module Name
014cbcdc    C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\System.DirectoryServices.AccountManagement\v4.0_4.0.0.0__b77a5c561934e089\System.DirectorySer

Assembly:            0133c308 [C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\System.DirectoryServices\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.DirectorySer
ClassLoader:         0133c3d0
SecurityDescriptor: 0133b0b0
  Module Name
5f0c1000    C:\WINDOWS\Microsoft.Net\assembly\GAC_MSIL\System.DirectoryServices\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.DirectoryServices.dll

0:000> !SaveModule 014c403c C:\Users\tester\Desktop\TradeCraft\SetADAttributes_dumped.exe
5 sections in file
section 0 - VA=2000, VASize=7e78, FileAddr=400, FileSize=8000
section 1 - VA=a000, VASize=bb50, FileAddr=8400, FileSize=bc00
section 2 - VA=16000, VASize=600, FileAddr=14000, FileSize=600
section 3 - VA=18000, VASize=c, FileAddr=14600, FileSize=200
section 4 - VA=1a000, VASize=10, FileAddr=14800, FileSize=200

0:000>
```

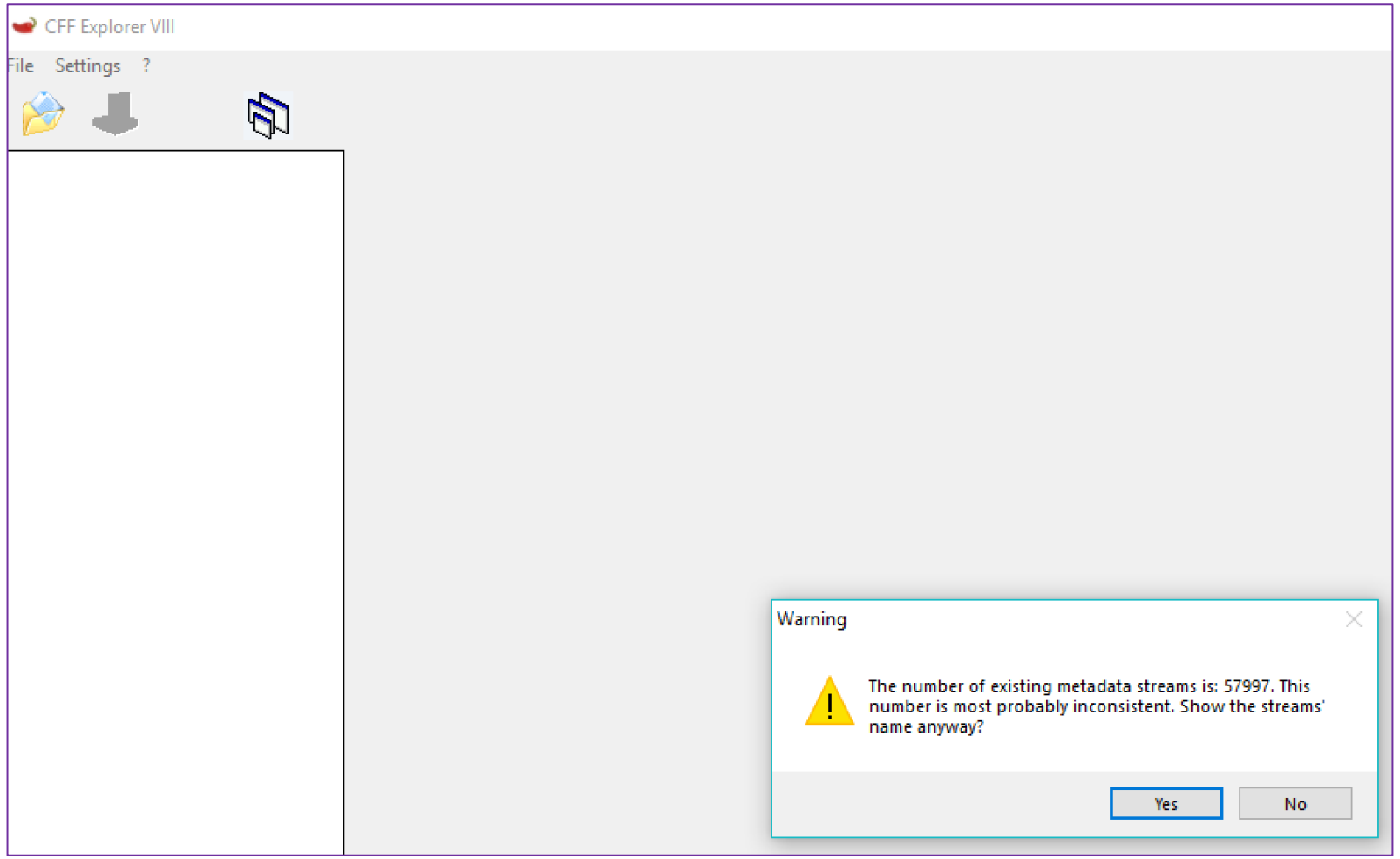
- SaveModule
  - Writes an image, which is loaded in memory at the specified address.
  - !SaveModule <object address> C:\path\to\new\binary.exe

# Header Reconstruction

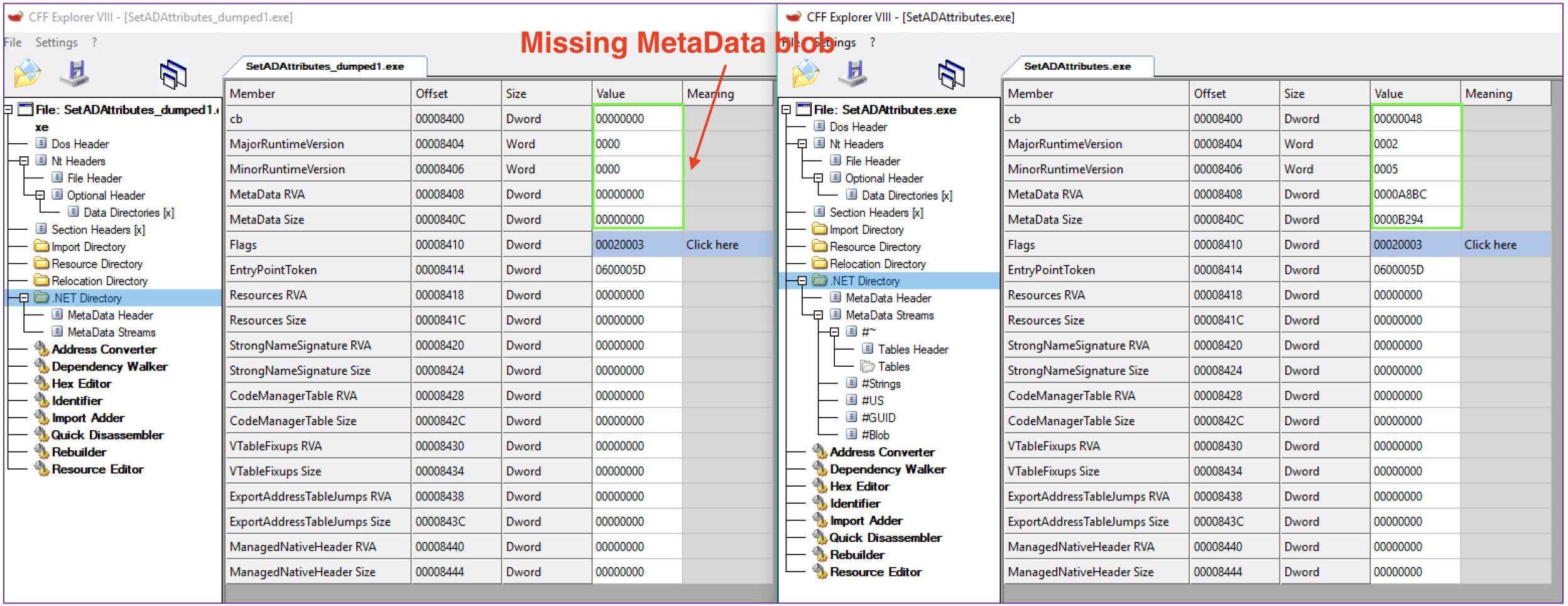
```
C:\Users\tester\Desktop\de4dot-net35>de4dot.exe C:\Users\tester\Desktop\TradeCraft\SetADAttributes_dumped1.exe

de4dot v3.1.41592.3405 Copyright (C) 2011-2015 de4dot@gmail.com
Latest version and source code: https://github.com/0xd4d/de4dot

WARNING: The file isn't a .NET PE file: C:\Users\tester\Desktop\TradeCraft\SetADAttributes_dumped1.exe
```

# Header Reconstruction

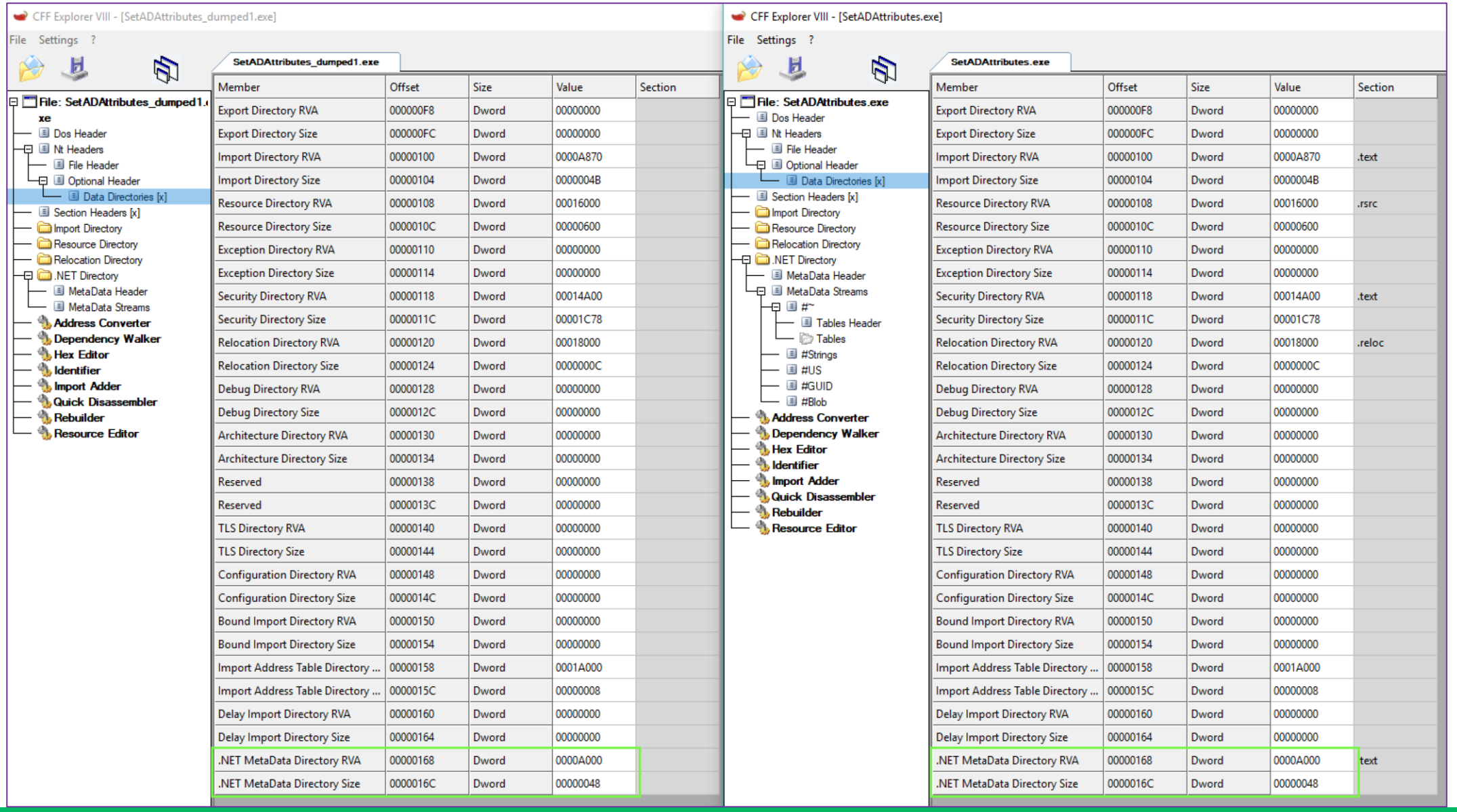
Issue with metadata?!



# Header Reconstruction

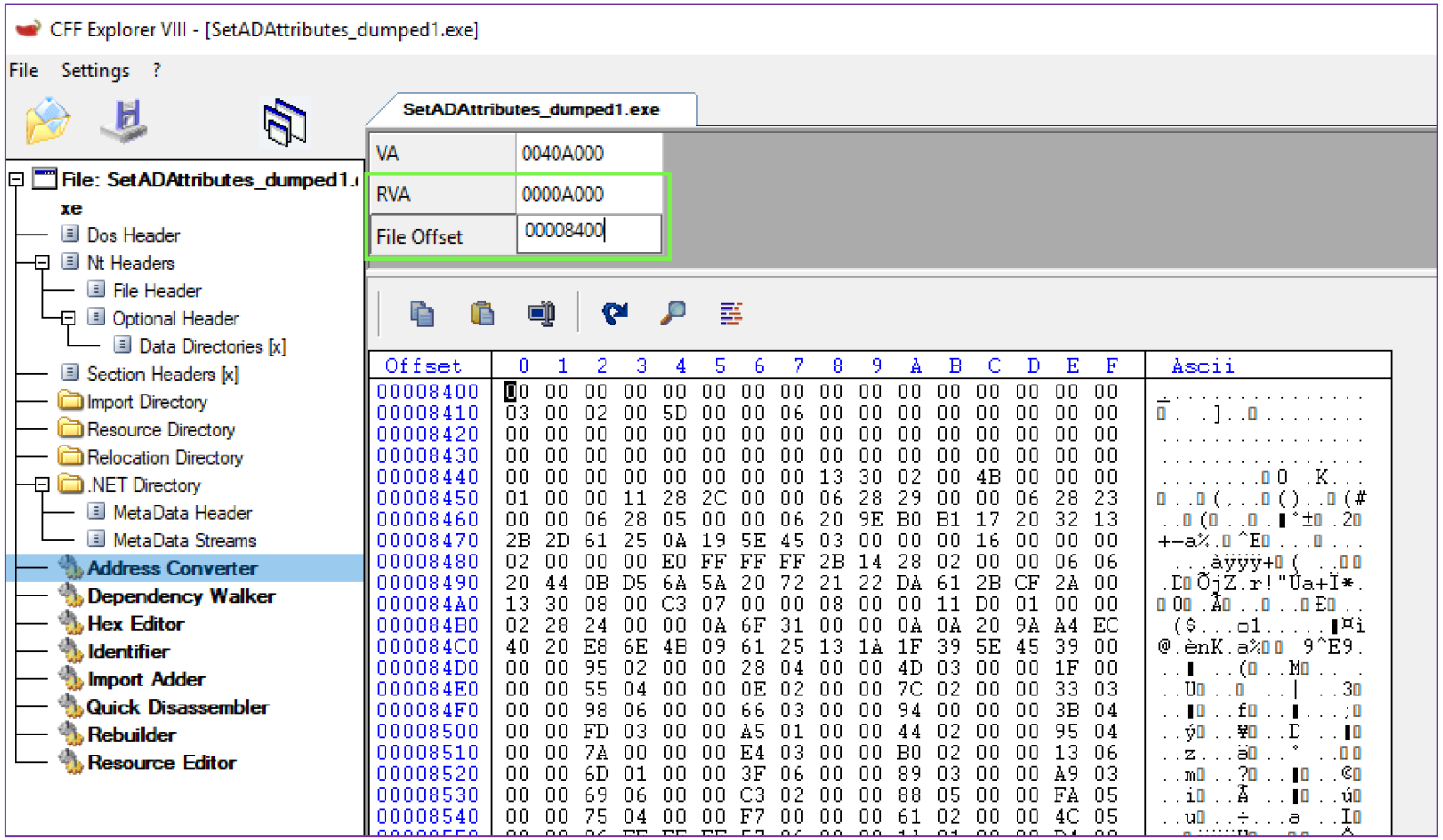


# Header Reconstruction

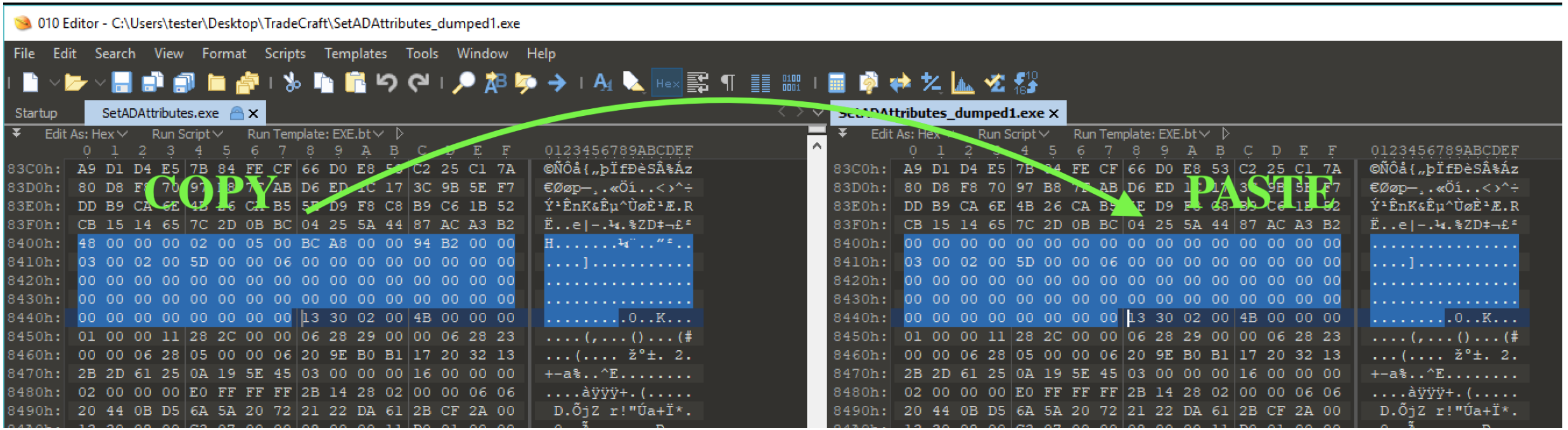


# Header Reconstruction

Use CFF Address Converter to convert RVA to file offset



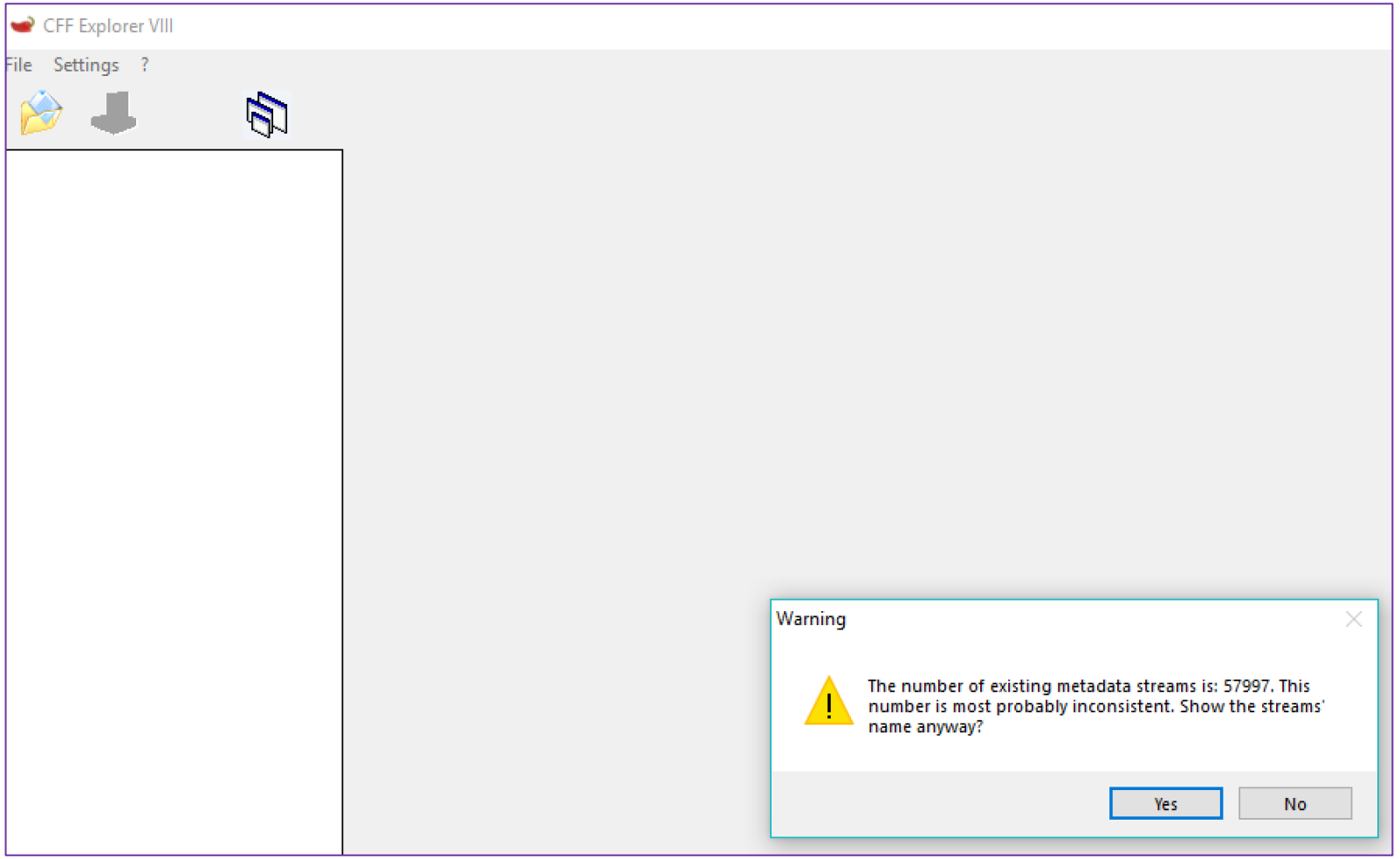
# Header Reconstruction




Copy MetaData header and paste in newly dumped binary

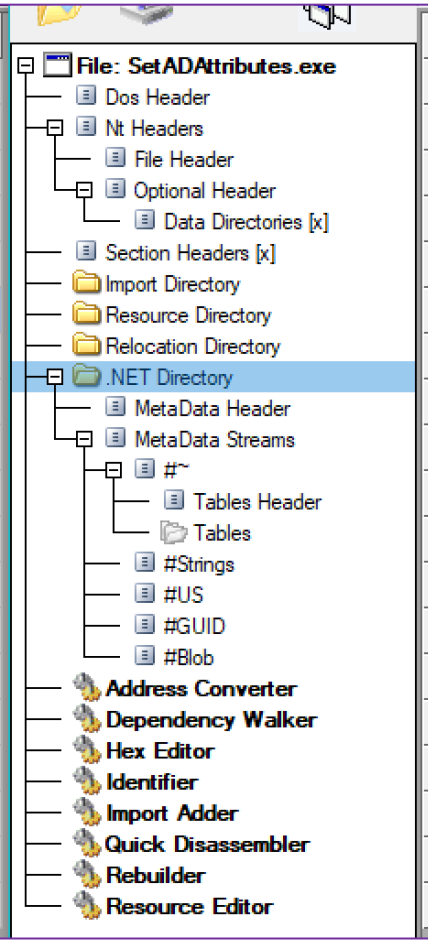
# Header Reconstruction

Still missing the metadata blob



# Header Reconstruction

| Member | Offset | Size | Value | Meaning |
|---|---|---|---|---|
| cb | 00008400 | Dword | 00000048 | |
| MajorRuntimeVersion | 00008404 | Word | 0002 | |
| MinorRuntimeVersion | 00008406 | Word | 0005 | |
| MetaData RVA | 00008408 | Dword | 0000A8BC | |
| MetaData Size | 0000840C | Dword | 0000B294 | |
| Flags | 00008410 | Dword | 00020003 | Click here |
| EntryPointToken | 00008414 | Dword | 0600005D | |
| Resources RVA | 00008418 | Dword | 00000000 | |
| Resources Size | 0000841C | Dword | 00000000 | |
| StrongNameSignature RVA | 00008420 | Dword | 00000000 | |
| StrongNameSignature Size | 00008424 | Dword | 00000000 | |
| CodeManagerTable RVA | 00008428 | Dword | 00000000 | |
| CodeManagerTable Size | 0000842C | Dword | 00000000 | |
| VTableFixups RVA | 00008430 | Dword | 00000000 | |
| VTableFixups Size | 00008434 | Dword | 00000000 | |
| ExportAddressTableJumps RVA | 00008438 | Dword | 00000000 | |
| ExportAddressTableJumps Size | 0000843C | Dword | 00000000 | |
| ManagedNativeHeader RVA | 00008440 | Dword | 00000000 | |
| ManagedNativeHeader Size | 00008444 | Dword | 00000000 | |

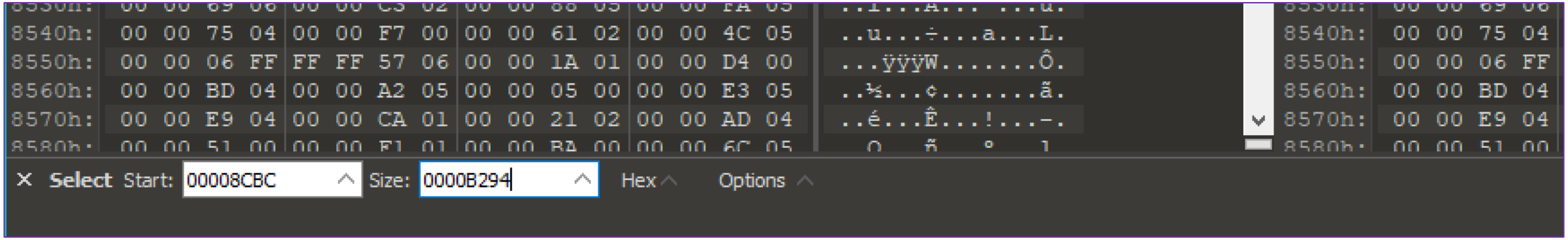




| Member | Offset | Size | Value | Meaning |
|---|---|---|---|---|
| cb | 00008400 | Dword | 00000048 | |
| MajorRuntimeVersion | 00008404 | Word | 0002 | |
| MinorRuntimeVersion | 00008406 | Word | 0005 | |
| MetaData RVA | 00008408 | Dword | 0000A8BC | |
| MetaData Size | 0000840C | Dword | 0000B294 | |
| Flags | 00008410 | Dword | 00020003 | Click here |
| EntryPointToken | 00008414 | Dword | 0600005D | |
| Resources RVA | 00008418 | Dword | 00000000 | |
| Resources Size | 0000841C | Dword | 00000000 | |
| StrongNameSignature RVA | 00008420 | Dword | 00000000 | |
| StrongNameSignature Size | 00008424 | Dword | 00000000 | |
| CodeManagerTable RVA | 00008428 | Dword | 00000000 | |
| CodeManagerTable Size | 0000842C | Dword | 00000000 | |
| VTableFixups RVA | 00008430 | Dword | 00000000 | |
| VTableFixups Size | 00008434 | Dword | 00000000 | |
| ExportAddressTableJumps RVA | 00008438 | Dword | 00000000 | |
| ExportAddressTableJumps Size | 0000843C | Dword | 00000000 | |
| ManagedNativeHeader RVA | 00008440 | Dword | 00000000 | |
| ManagedNativeHeader Size | 00008444 | Dword | 00000000 | |

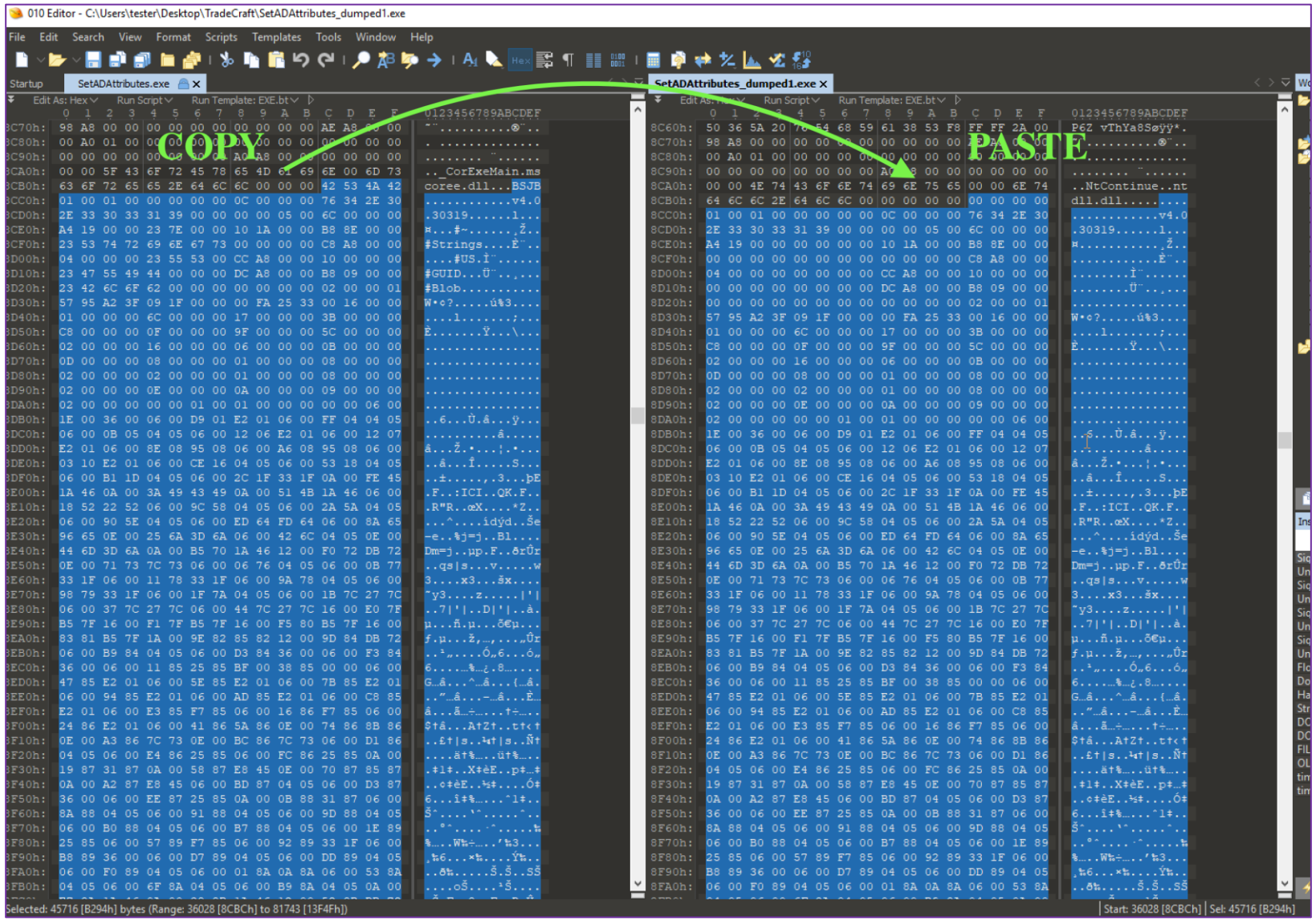

Use MetaData RVA offset and MetaData size to copy MetaData blob

# Header Reconstruction

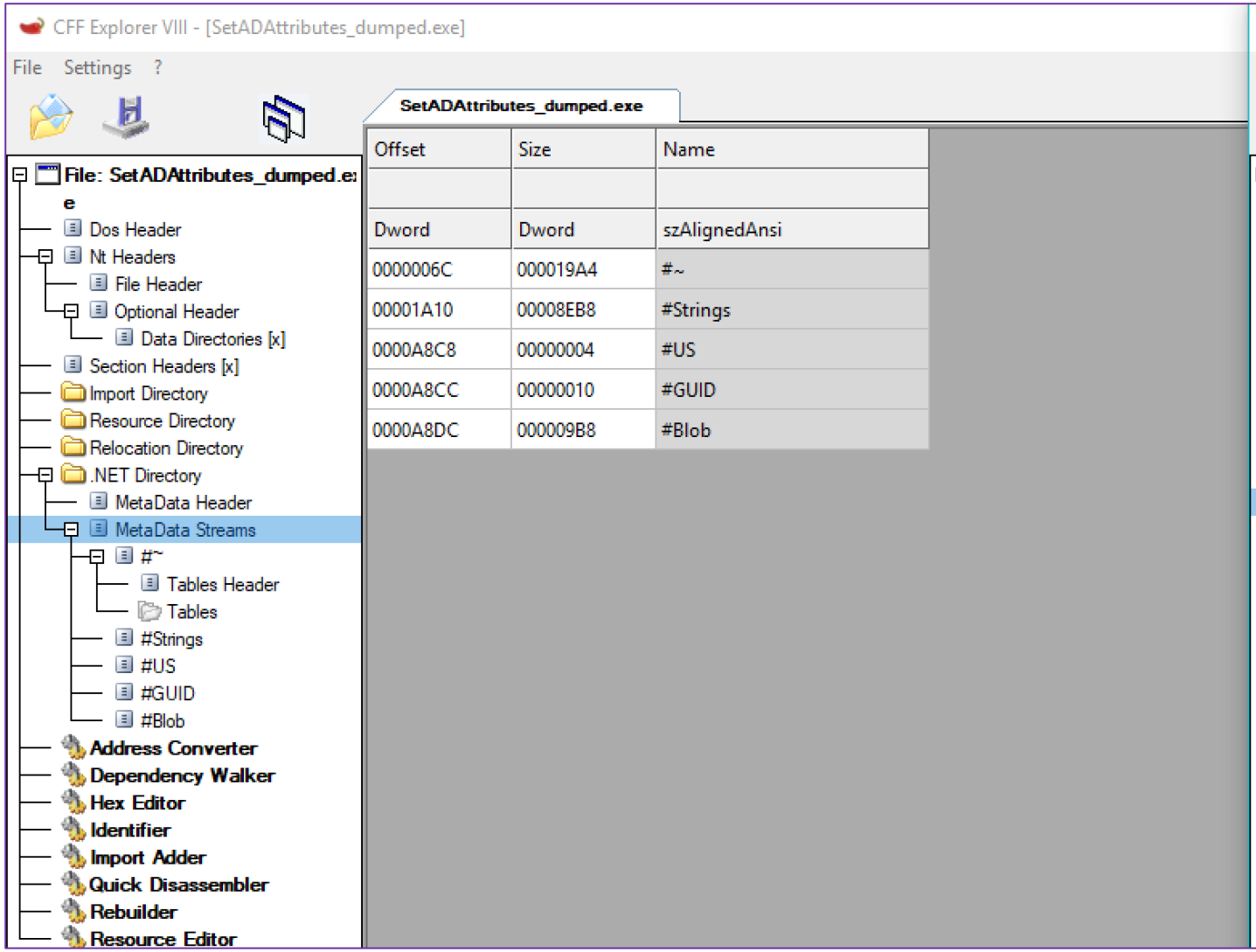


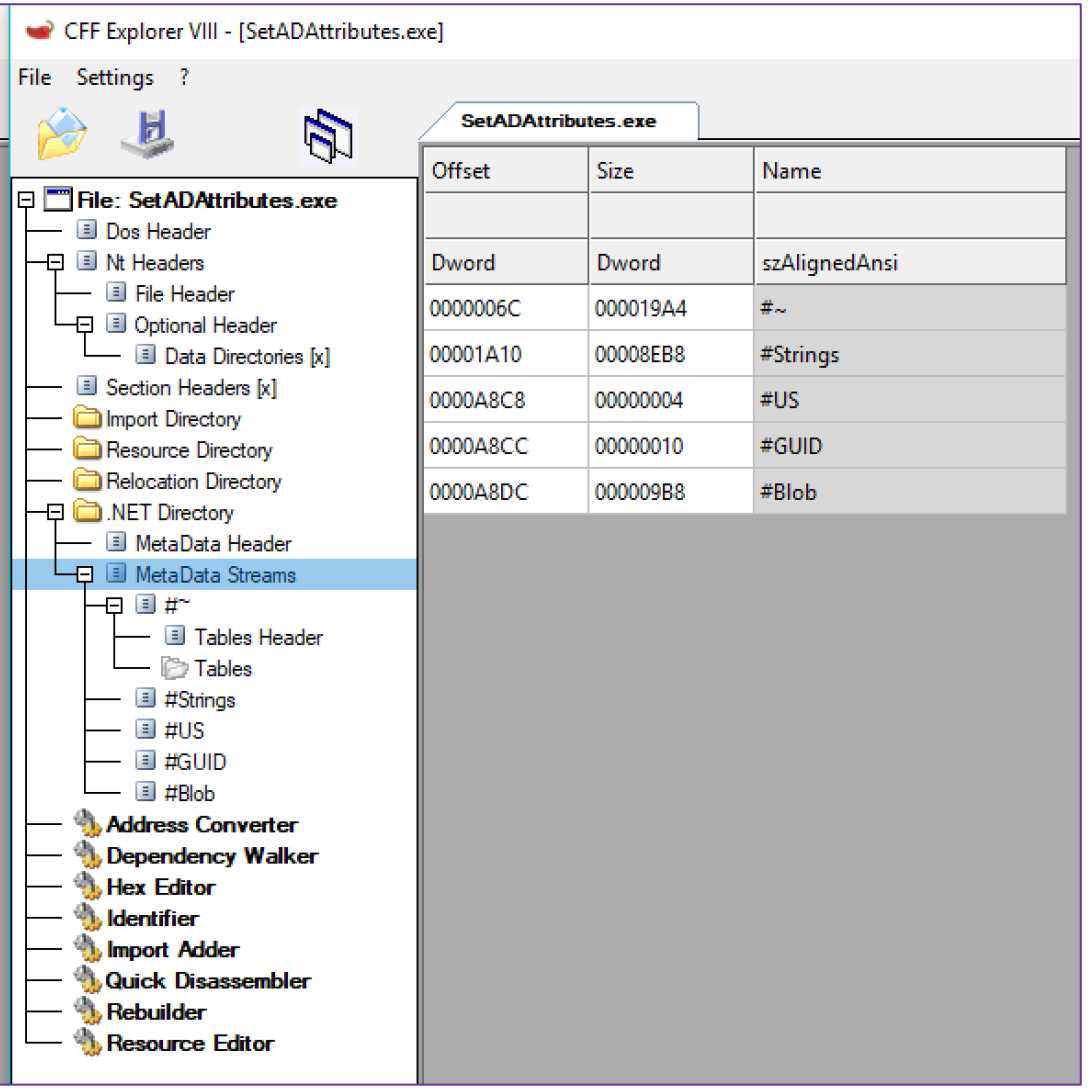

In hex editor select range by specifying start offset and size of MetaData blob

# Header Reconstruction



# Header Reconstruction



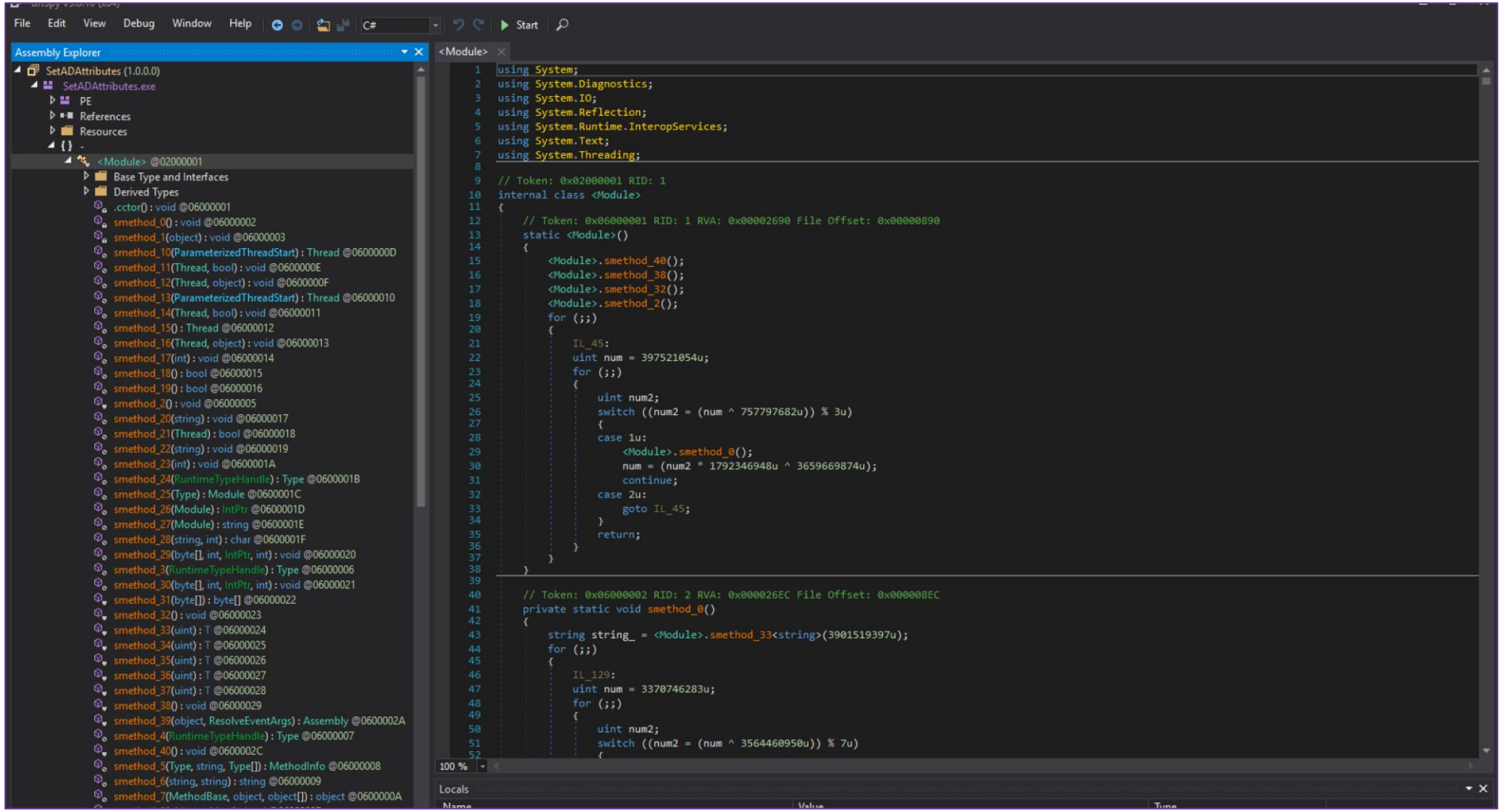



# De-Obfuscate

```
C:\Users\tester\Desktop\de4dot-net35>de4dot.exe C:\Users\tester\Desktop\TradeCraft\SetADAttributes_dumped.exe

de4dot v3.1.41592.3405 Copyright (C) 2011-2015 de4dot@gmail.com
Latest version and source code: https://github.com/0xd4d/de4dot

Detected Unknown Obfuscator (C:\Users\tester\Desktop\TradeCraft\SetADAttributes_dumped.exe)
Cleaning C:\Users\tester\Desktop\TradeCraft\SetADAttributes_dumped.exe
Renaming all obfuscated symbols
Saving C:\Users\tester\Desktop\TradeCraft\SetADAttributes_dumped-cleaned.exe
ERROR: Error calculating max stack value. If the method's obfuscated, set CilBody.KeepOldMaxStack or MetadataOptions.Fla
gs (KeepOldMaxStack, global option) to ignore this error. Otherwise fix your generated CIL code so it conforms to the EC
MA standard.
```

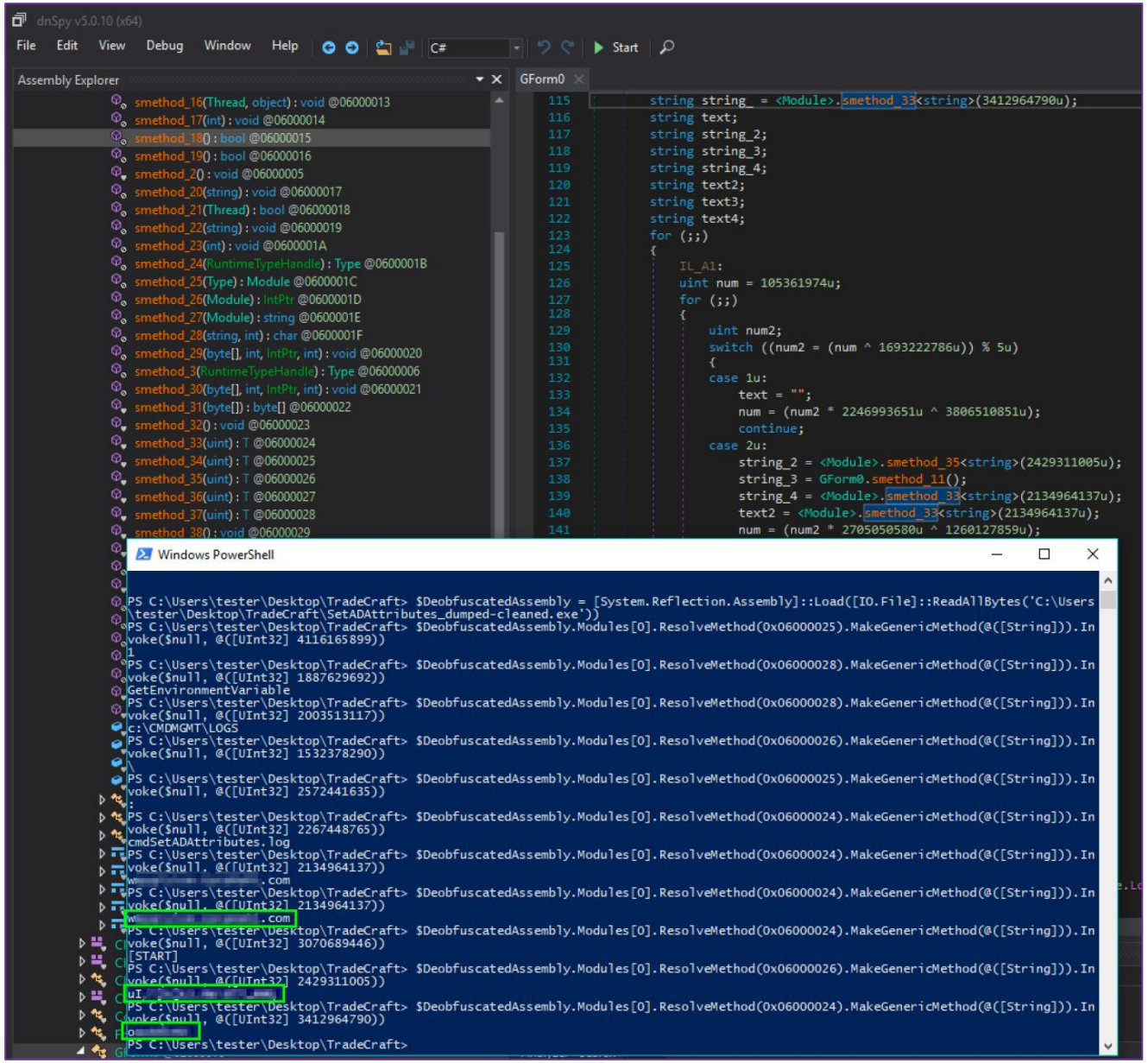
de4dot renames obfuscated symbols and helps with clean up

# De-Obfuscate



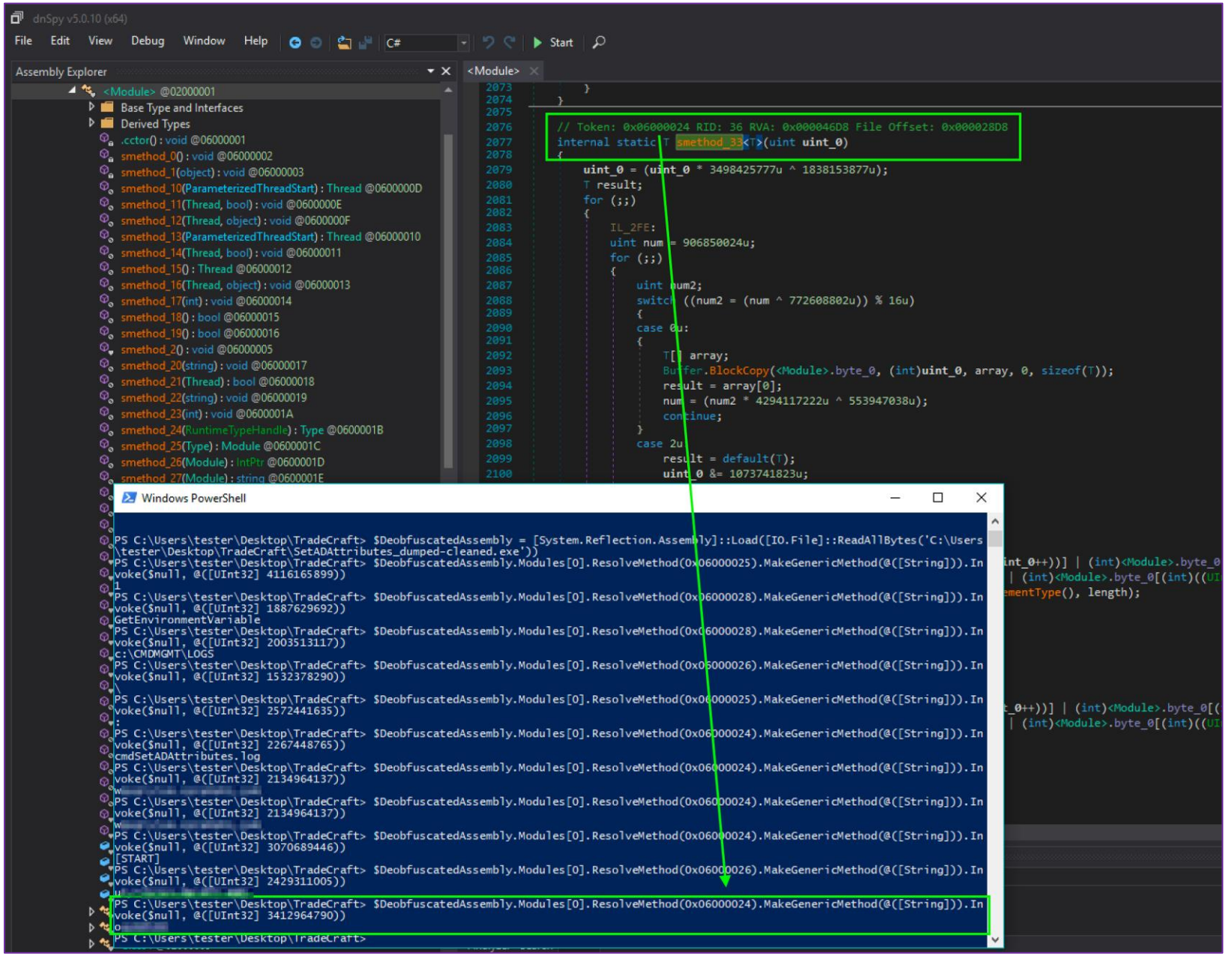
# Reflective Decryption

- Use PowerShell to reflectively load the reconstructed binary
- Reflection examines metadata and can invoke methods in the binary
- Modules.ResolveMethod() returns the method identified by the metadata token ID



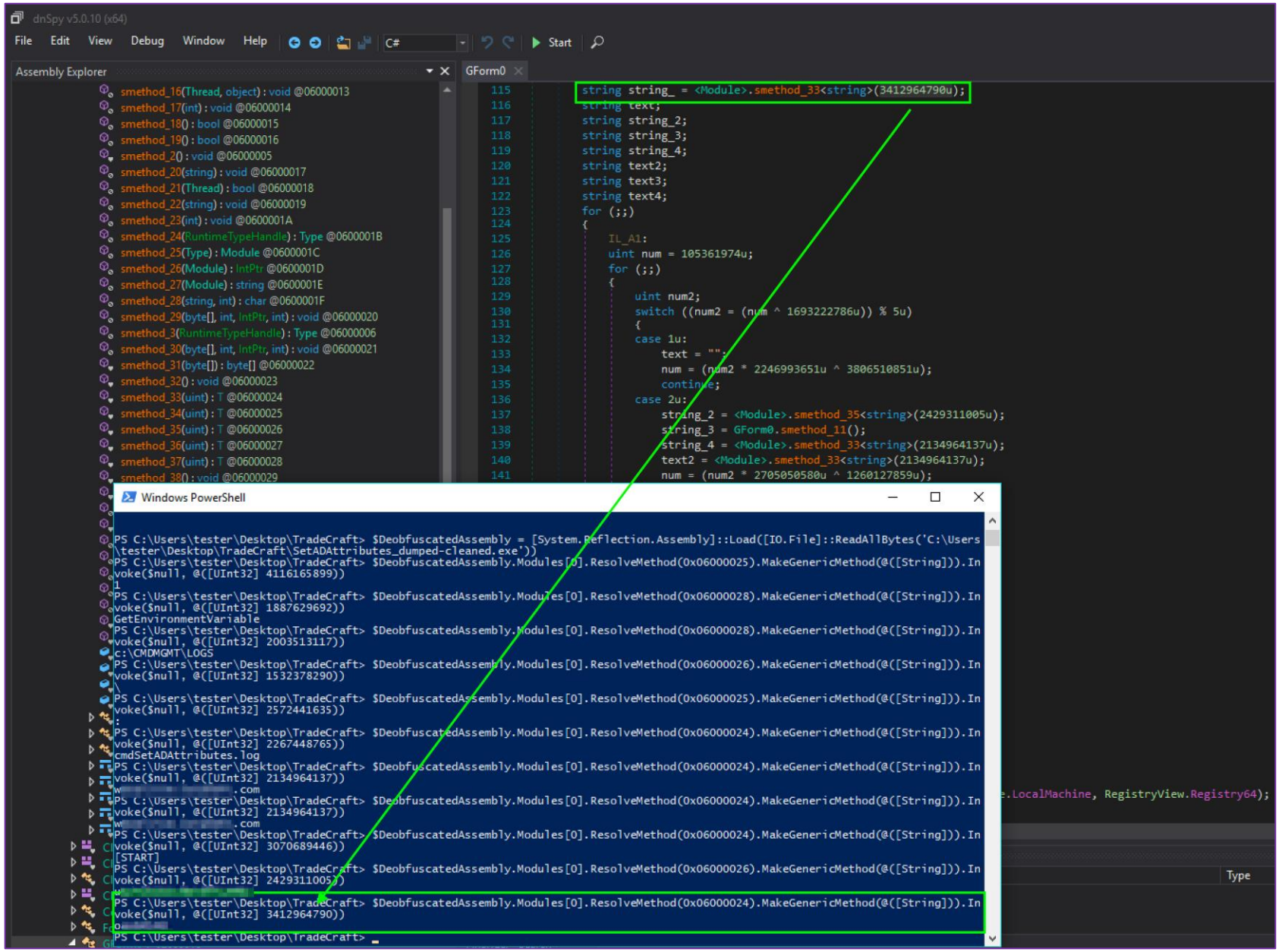
# Reflective Decryption

Trace smethod_XX to obtain Token ID for that decryption routine



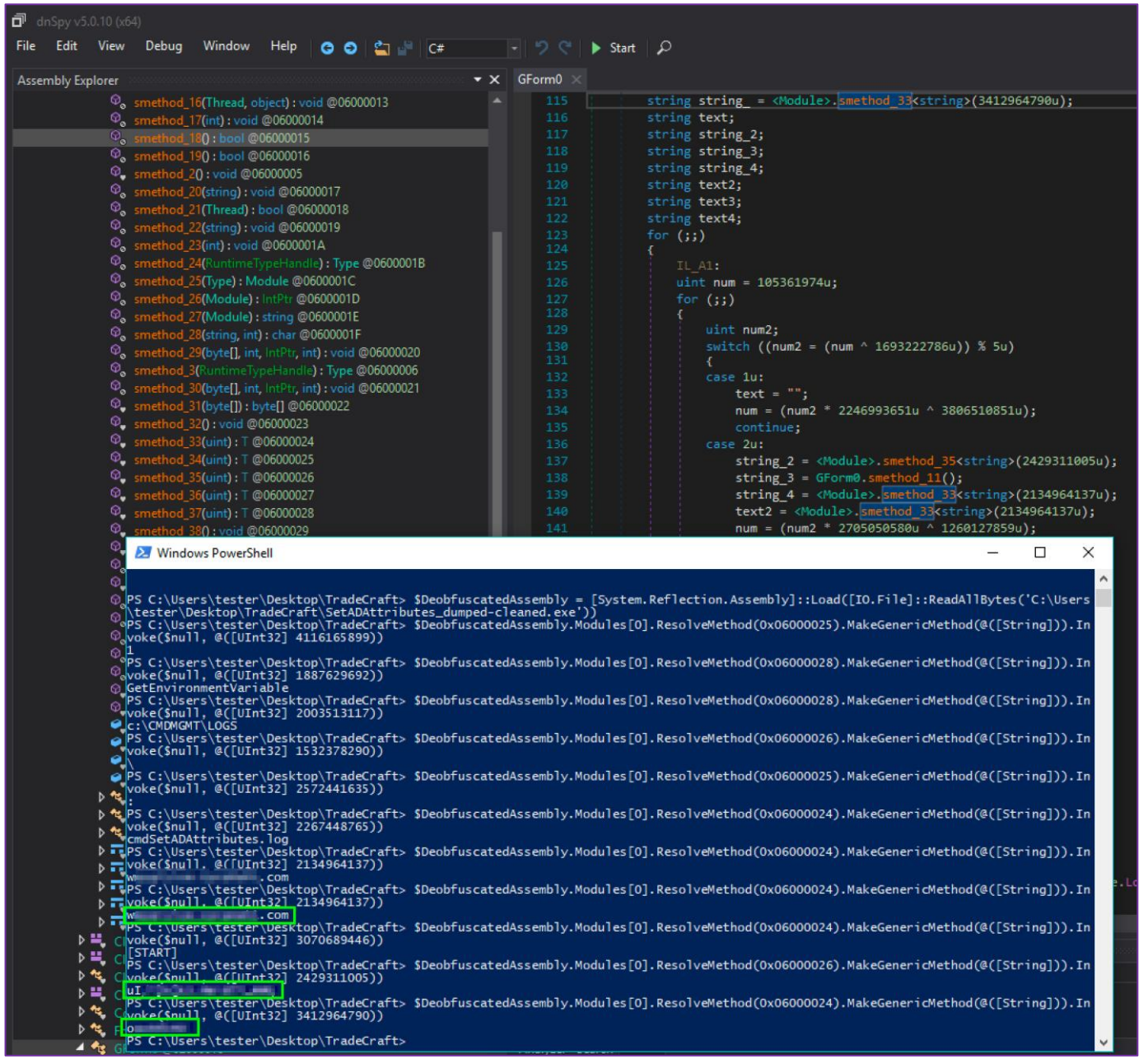
# Reflective Decryption

Call decryption routine on protected string resource

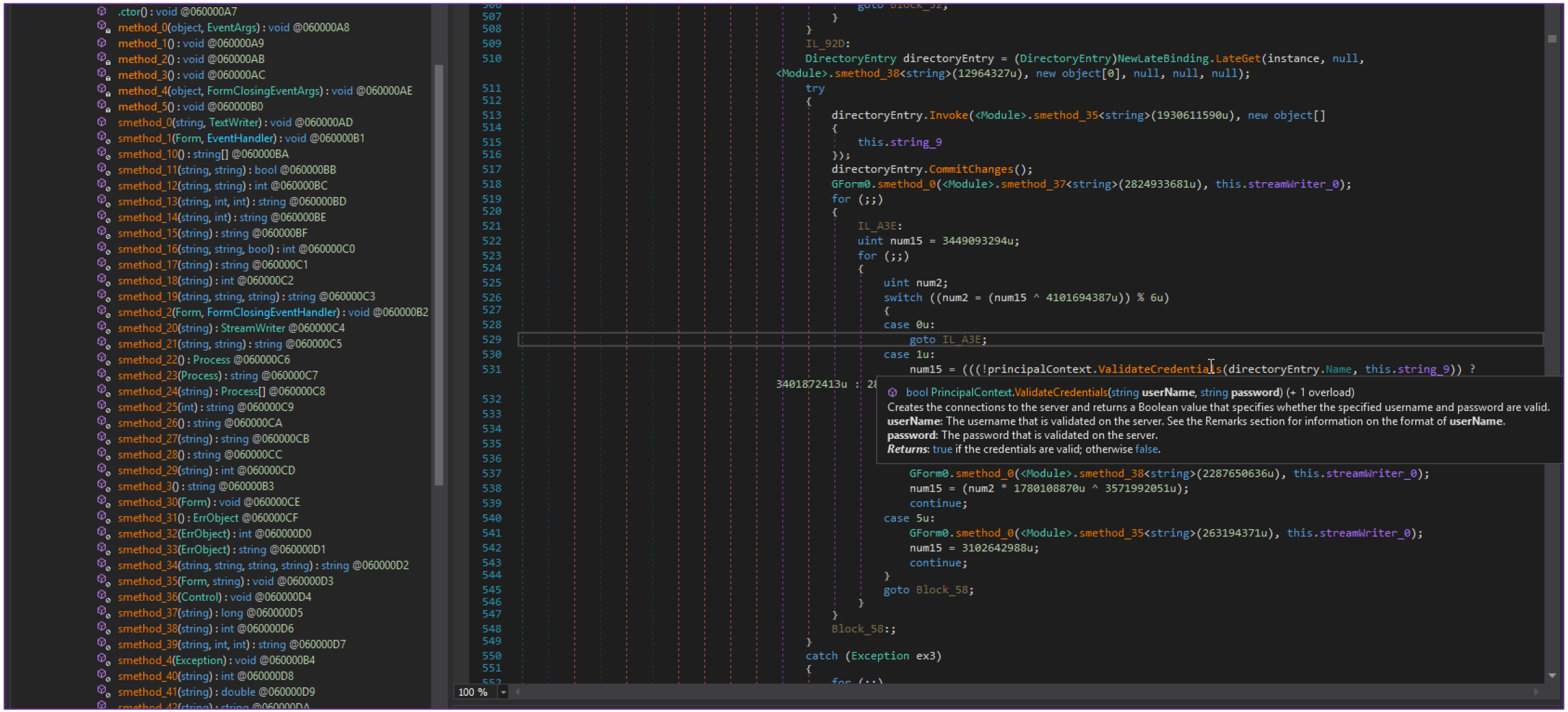


# Reflective Decryption

Valid domain creds!!



# Perseverance



# Perseverance

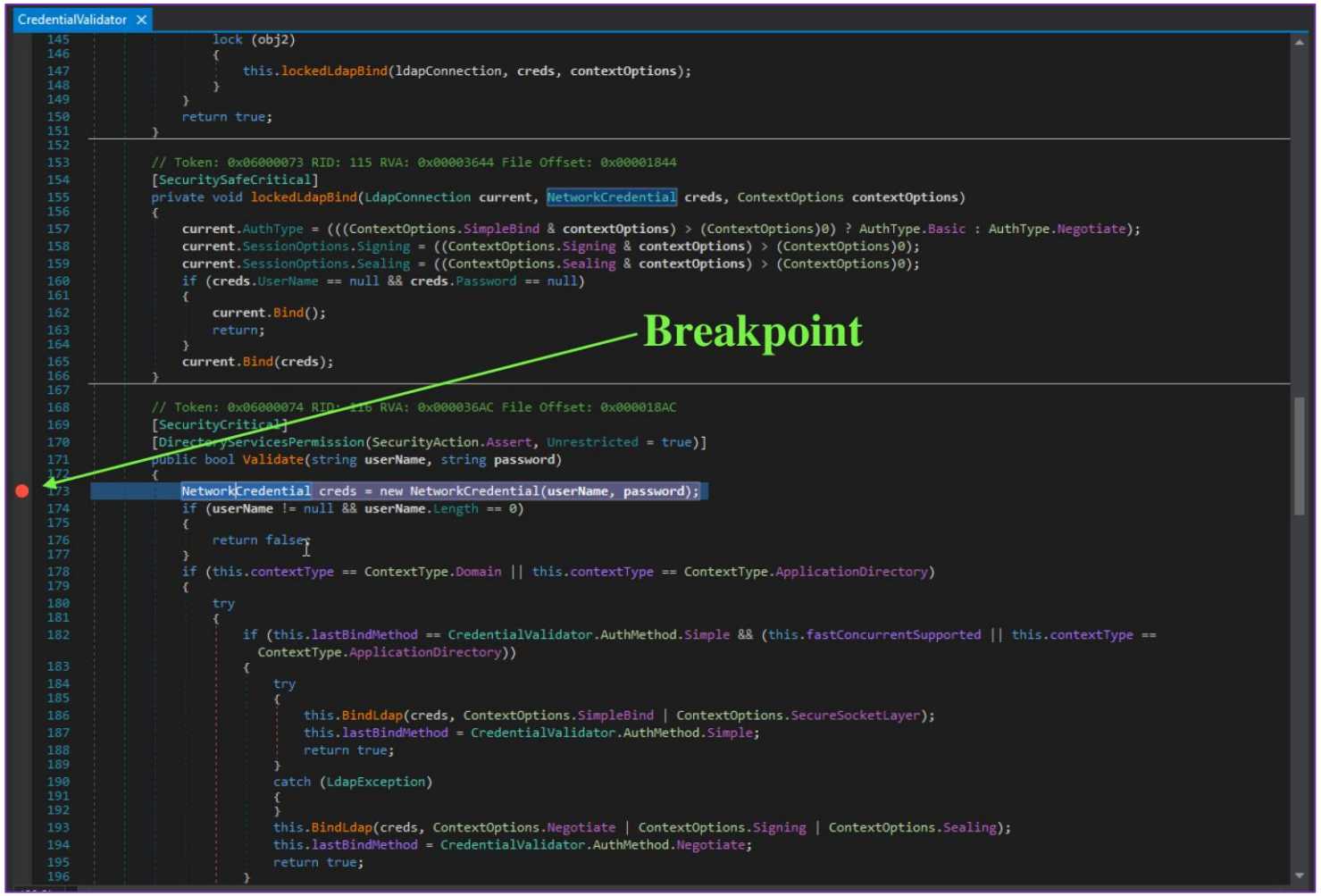
PrincipalContext

```
204         }
205
206         /// <summary>Gets the name of the server to which the principal context is connected. </summary>
207         /// <returns>The name of the server to which the principal context is connected or null if the principal context is not connected to a server. </
              returns>
208         // Token: 0x1700000D RID: 13
209         // (get) Token: 0x06000082 RID: 130 RVA: 0x000039FD File Offset: 0x00001BFD
210         public string ConnectedServer
211         {
212             get
213             {
214                 this.CheckDisposed();
215                 this.Initialize();
216                 return this.connectedServer;
217             }
218         }
219
220         /// <summary>Creates the connections to the server and returns a Boolean value that specifies whether the specified username and password are valid.
              </summary>
221         /// <param name="userName">The username that is validated on the server. See the Remarks section for information on the format of <paramref
              name="userName" />. </param>
222         /// <param name="password">The password that is validated on the server.</param>
223         /// <returns>
224         ///     <see langword="true" /> if the credentials are valid; otherwise <see langword="false" />. </returns>
225         // Token: 0x06000083 RID: 131 RVA: 0x00003A11 File Offset: 0x00001C11
226         public bool ValidateCredentials(string userName, string password)
227         {
228             this.CheckDisposed();
229             if ((userName == null && password != null) || (userName != null && password == null))
230             {
231                 throw new ArgumentException(StringResources.ContextBadUserPwdCombo);
232             }
233             return this.credValidate.Validate(userName, password);
234         }
235
236         /// <summary>Creates the connections to the server and returns a Boolean value that specifies whether the specified user name and password are
              valid. This method performs fast credential validation of the username and password. </summary>
237         /// <param name="userName">The username that is validated on the server. See the Remarks section for information on the format of <paramref
              name="userName" />. </param>
238         /// <param name="password">The password that is validated on the server.</param>
239         /// <param name="options">A combination of one or more <see cref="T:System.DirectoryServices.AccountManagement.ContextOptions" /> enumeration values
              that specify the options used to bind to the server. This parameter can only specify Simple bind with or without SSL, or Negotiate bind. </param>
240         /// <returns>
241         ///     <see langword="true" /> if the credentials are valid; otherwise <see langword="false" />. </returns>
242         /// <exception cref="T:System.ArgumentException">The <paramref name="options" /> parameter must specify <see
              cref="F:System.DirectoryServices.AccountManagement.ContextOptions.Negotiate" /> when the context type is <see
              cref="F:System.DirectoryServices.AccountManagement.ContextType.Machine" />. </exception>
243         // Token: 0x06000084 RID: 132 RVA: 0x00003A40 File Offset: 0x00001C40
244         public bool ValidateCredentials(string userName, string password, ContextOptions options)
245         {
246             this.CheckDisposed();
```

bool CredentialValidator.Validate(string userName, string password) (+ 1 overload)

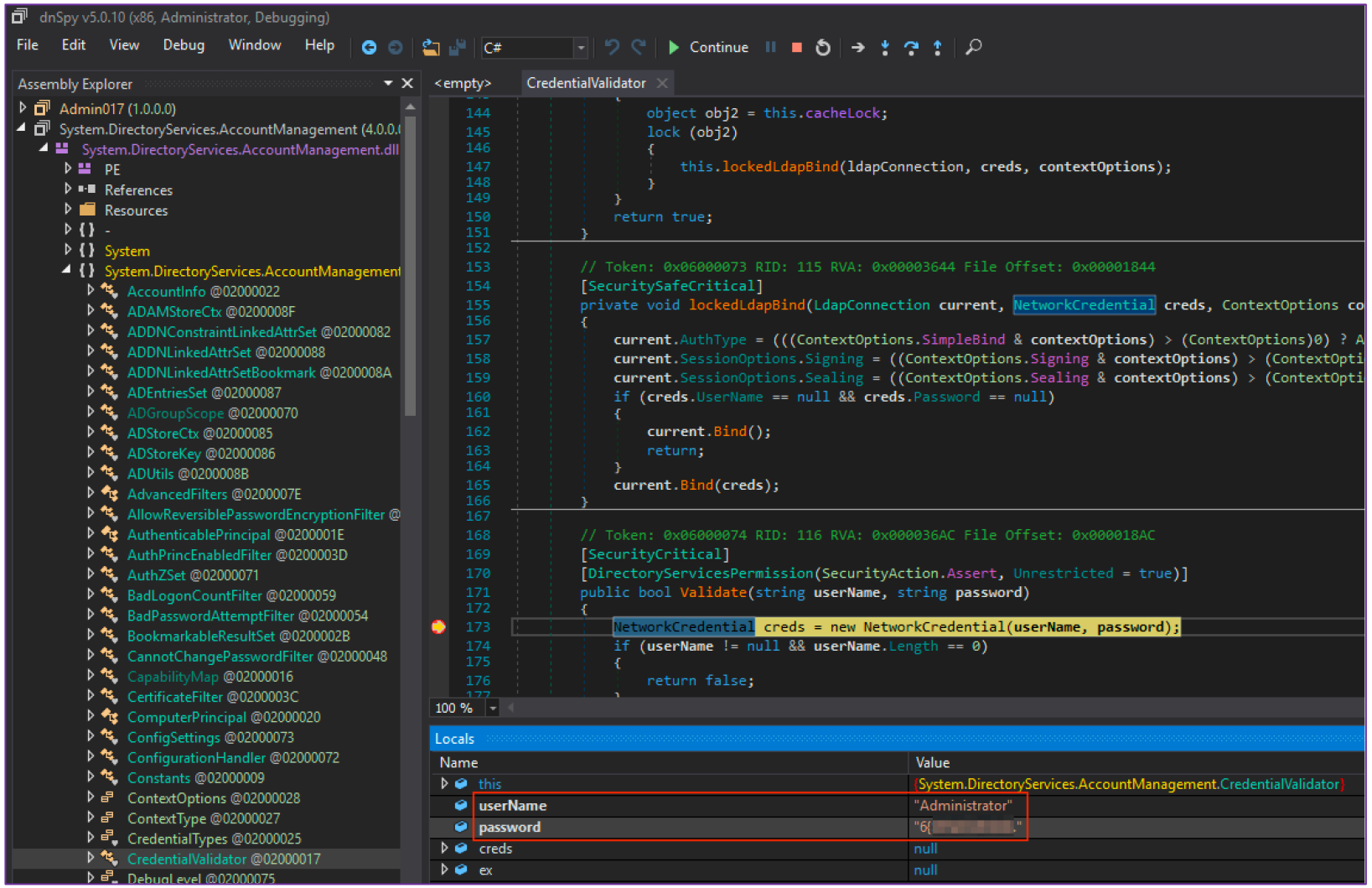
- After password creation, the credentials are tested against a domain server
- Validate Credentials method looks to send username and password as string args
- Trace Validate down one more level

# Perseverance




- NetworkCredential variable being set by calling NetworkCredential method with username and password string variables
- Set a breakpoint on this line
- Dnspy will need to be x86 version and run as Admin to reach this part of the code.
- Run it!!

# Perseverance




- Change VM hostname to any hostname in the environment
- Run this de-obfuscated binary in dnspy and hit this breakpoint
- Gain Local Admin credentials to any machine in the domain
- Confirmed by using PoC hostname and confirming password.

# Issues

- ConfuserEx on max settings adds anti-dumping protections that this workflow was not able to bypass
- ConfuserEx obfuscated binaries have been recently getting caught and removed by Windows Defender likely due to the unpacking method.
- ConfuserEx is used by actual threat actors in the wild

www.pickles.xyz
@_P1CKLES_
slucas@specterops.io