**How to reverse engineer (RE) the NMS exe.**

In this tutorial, we will look at how to use IDA to RE the NMS exe to discover the properties of the many structs used in game to be used to decompile and recompile mbin files.

First, open the exe with IDA and select what should be the first decompile option (making sure you have the 64-bit version of IDA open).

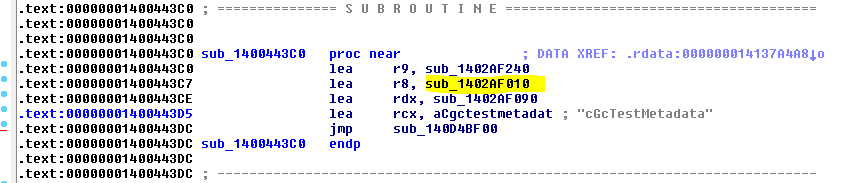
You will need to leave the program to run for a little while as it needs to parse the entire exe which takes some time (quite a few minutes. You can see the progress by the small triangle near the top of the screen. When it gets to the end, it has completed the first stage. The second stage the cursor will jump backwards and forwards quickly. Once the cursor stops moving, messages stop flashing up then the decompiling process is complete.)

When the process completes the main decompile window might be small, to increase the size, click on it and press the space bar key.

The first struct we will look for in the exe is the *GcTestMetadata* struct. We do this so that we can name several data types early on to assist us in the mapping of structs later.

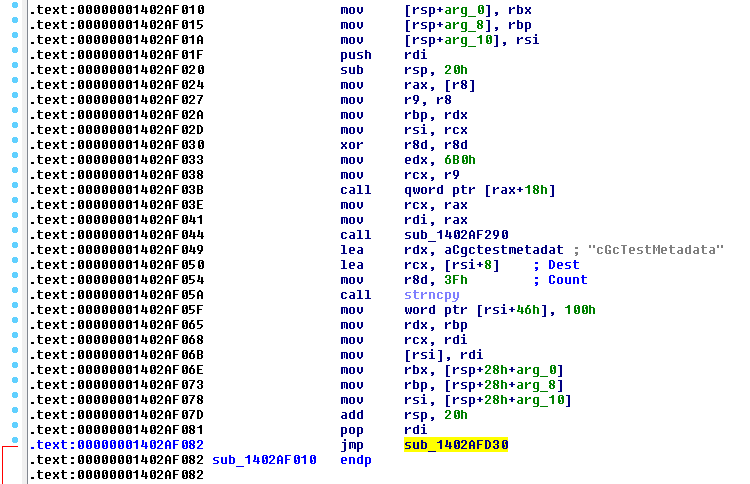
To search for a struct, go to the top of the exe and search (alt+T) for the string *GcTestMetadata*.  
We do not want to search for all the occurances, nor do we need it to be case sensitive.

The first result that appears should look something like



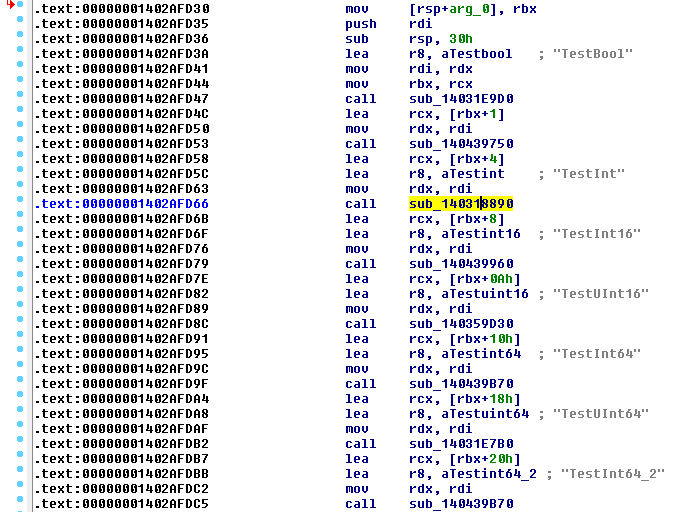
The locations will however vary depending on the version of the exe you are using.

In *most* cases, the steps you will want to do are as follows:

* Double click on the location (*sub\_<hex number>*) after the *r8* string (usually 2 above the *rcx* string). So in the case of my picture, you would click on the highlighted section.  
  This will take you to another screen. Note that to go back to the previous view easily you can press the Esc key.
* On this next view, right before the *endp* tag, there is a line with *jmp sub<hex number>*. Double click on this line.  
  
* This will take you to the actual data for the struct.

It should be noted that sometimes the *r8* sub location will take you straight to the struct, but normally you will need to follow the above simple process.  
This sub you are at you should rename the sub\_<~> to be whatever the actual struct name is. This can help later on when something in a different struct uses this struct, you will already know what the data type is!

Now that we have the struct, we can begin naming things. First, open up the GcTestMetadat.cs file either from a local clone of the MBINCompiler git repository, or open the file directly online. We will be comparing the structure of this file to the structure of the struct in the exe.



Comparing the highlighted sub in the above picture to the data type of the TestInt variable in the c# struct, we can see that it should be an int, thus we can rename (by pressing *N*) the sub.

Once we have renamed the sub’s it should look something like this:



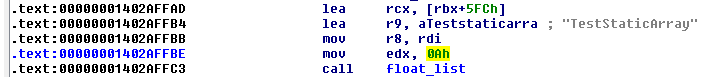
Note that I have added some extra things compared to the struct, namely the byte data type as it is missing (at time of writing) from the struct.

You can go through and name all the different data types.

Something to note is the *[rbx+20h]* (for example) above each of the names. This is the location of the variable within the struct.  
It is important to look at this value and think of whether it is what you expect it to be, because you can use it to both determine the size of the previous chunk of data, and use this to determine whether or not padding is potentially needed.

As you RE more and more of the exe you will get used to the sizes of different data types (eg, float is 0x4 (all numbers are generally in hex), Colour is 0x10, etc).

There are two more special types of data types that occur in the exe. One I will call a list, and the other an array (for lack of better names…)  
The list involves (unsurprisingly) a list of values of some certain length. We can see this in the exe by looking for example at the *TestStaticArray* variable.

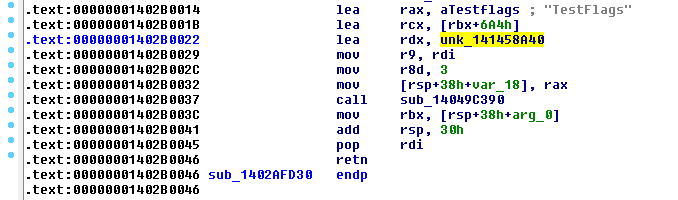


We see that this variable is located at 0x5FC, and is a list of floats (as seen in the c# struct). What is important to notice is that the exe tells us how long the list is. I have highlighted the length in the image (which is usually next to an *edx*) and you can compare this to the code in the struct.

You might ask, how do we know what the data type of the list is?! And this question isn’t always that easy to answer. If you scroll down past the struct there is another version of it (there are multiple versions of every struct in the exe, so sometimes it is required to check out these other versions to discern the data types of things) which can sometimes have more information of the problem. It also helps to have a look at the mbin and see what the data looks like at the location and see if it looks like anything familiar. Ultimately it sometimes just comes down to looking at the size of the struct that we are having a list of, and comparing that to other structs and just guessing by thinking about what data type it could possibly have. So a new struct to do with missions migh have a list of mission requirements, and there might be a mission requirements struct, so often you can work things out that way. In the end, lots of this comes down to practice and noticing patterns and understanding in a way how the structs work.

It should also be mentioned that there are dynamic length lists (as seen with the *TestDynamicArray* variable. The space taken up by each of these is 0x10, however in the mbin this will point to another location in the struct where the actual data is.

The next interesting data type is the array. The array is a list of values that can be chosen by the game, we will look at the *TestFlags* variable for this one.



If we double click on the *unk\_<hex number>* function, the view will change to a list of the possible options



These are the values in the list of strings that can be chosen and you can compare the code for these to the struct.

Once you have named at least most of the data types in this struct, you can start searching for other known structs and renaming any sub\_<~>’s.

Overall, this really is something that just take a bit of time to get used to doing. There are lots of little things to look out for, and there are plenty of little tricks. Things usch as pressing F5 when clicked on a sub will open up a window with a pseudocode view of the function, which can show you the data in a different way that is sometimes easier to analyse (I prefer the other view, but some prefer this pseudocode view).

Finally, a word on globals: Globals are *hard*. They do not obey the same rules as all the other structs (other than the debug globals for some odd reason…).  
Finding the data for the globals in the exe is reasonably hard, but do-able when there is string data, but even once you have the location of the struct in the exe, it is still a fair bit of work to write the c# code for the struct from this data. It is only recommended that you look at these once you already have a very firm grasp on how everything works.