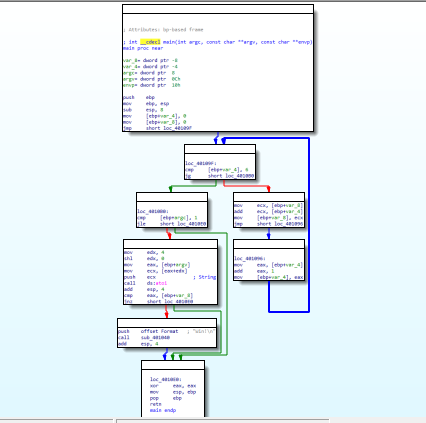
First we going to find the main:



We can see now the struct of the main program, we recognize a loop function(with 2 parameters) in the right part.

Now we trying to understand how its work. The loop func fill 2 bytes in the stack with ZERO.

If the first variable is less or equal to 6, we are still in a loop.

Inside the loop we add the value of var1 to var2:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

And increase by 1 var1 value.

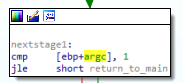
תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

Running example:

|  |  |  |
| --- | --- | --- |
| Var2 | Var1 | After Iteration |
| 0 | 0 | Begin: |
| 0+0=0 | 1 | 1 |
| 0+1=1 | 2 | 2 |
| 1+2=3 | 3 | 3 |
| 3+3=6 | 4 | 4 |
| 6+4=10 | 5 | 5 |
| 10+5=15 | 6 | 6 |
| 15+6=21 | 7 | 7 |

When var1 = 7 and var2=21 we break the loop,

We check if the value at stack in +8 bytes(this is not local variable, this one of the main params - argc) is less or equal to 1, if yes, exit main and end the program.

If it is grater then 1:

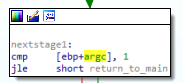
תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיEdx register get value of 8, eax get the value in the argv var, ecx get the value of argv+8, and push it to stack.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטיThe next func called is atoi who convert the value in the stack to int format, and return it to eax. Now we compare the eax value with var2 value(21), only if it equal we jump to "win" func who just print win string.

2.

To win the program we need to make that jump not work: 

To do it we need our argc big then 1. Each command line argument the user provides will cause argc to increase by 1.

So we need the arguments which are provided for the main to be 2 or more.

Here we need that the jump not work, to be zero.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

Eax get the pointer to the start of the arrays of the arguments.

Ecx get eax + 2 bytes.

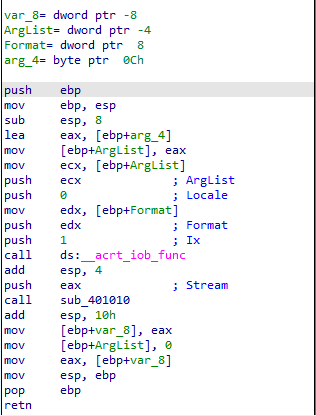
We turn it to int var and compare it to var\_8 – the second local var. if they equal – we good.

So we need the value at ecx will be 21.

Now we need to understand the obi func;

תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי

it gets the win word and create 2 local vars.

It take the arglist value and push to stack. Push 0, push win push1.

Now call the iob func and gets the stream to print.

The iob is cout in c++.