# Save the Dragon

# Author: - (Ayush Shende and Chirag Maski)

## Binary Exploitation (easy)

## Question description

Wizard Corbin has cast an evil spell on Ghidra, the dragon🐉. Your mission is to break the spell by casting your own spell and save the dragon. It shouldn’t be that difficult as the dragon has lent some of his powers to you.

### Hint (not to be given)

The counter spell can be found in \_/\_m/\_main

## Solution

If we run the .exe file in terminal we get a message “Cast your spell in Command Line as an argument.”.

So, now we try to give an argument:

```

> .\lock.exe aaaaaaa

Think Big !!!!

```

After some trials, we find that argument with length of 11 or more gives a different output, other than “Think Big”.

```

> .\lock.exe aaaaaaaaaaa

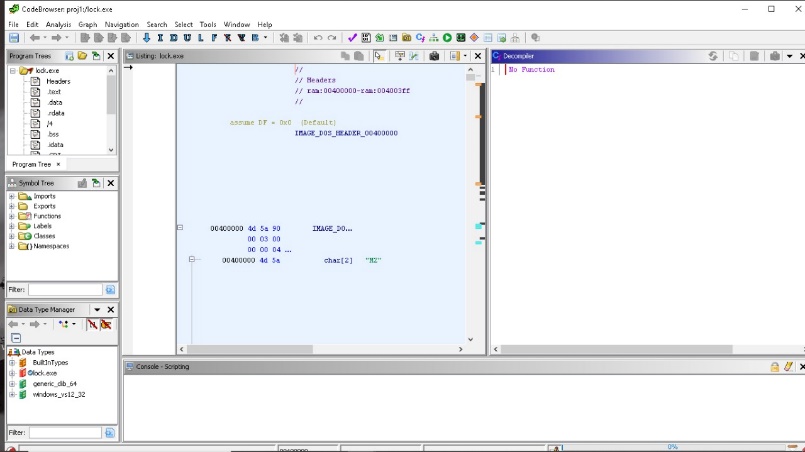
Wrong Spell

```

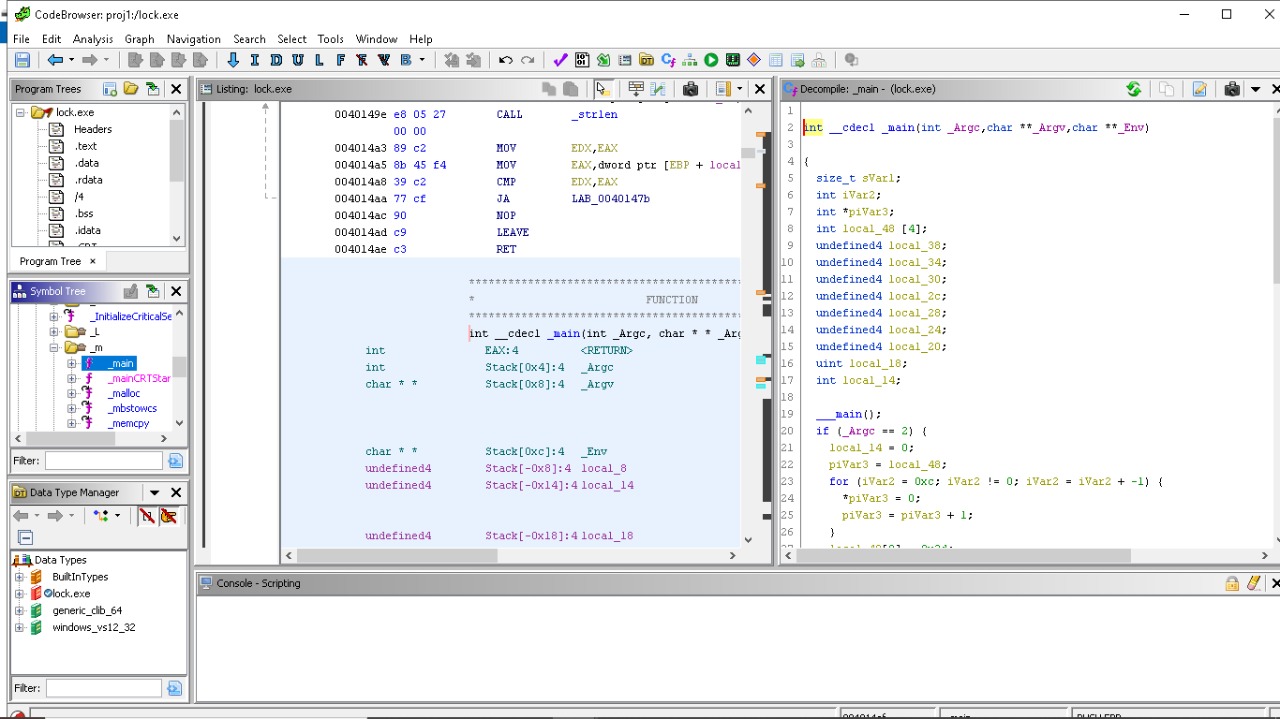
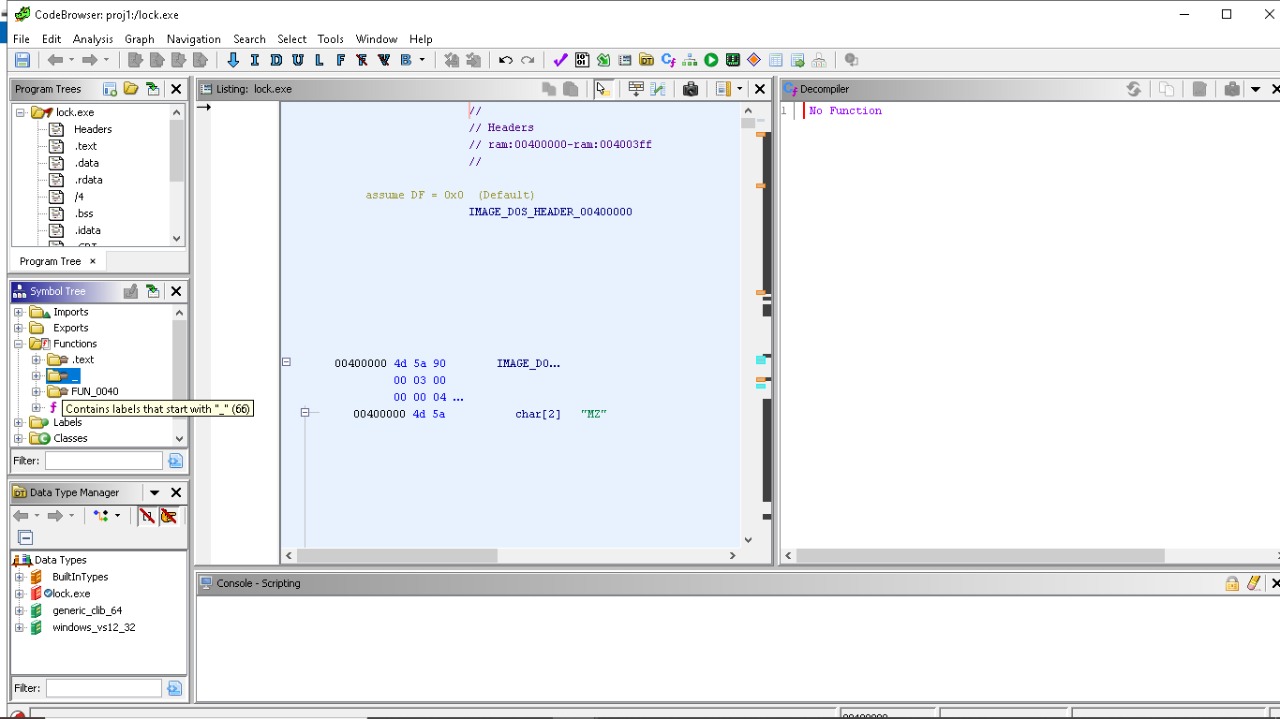
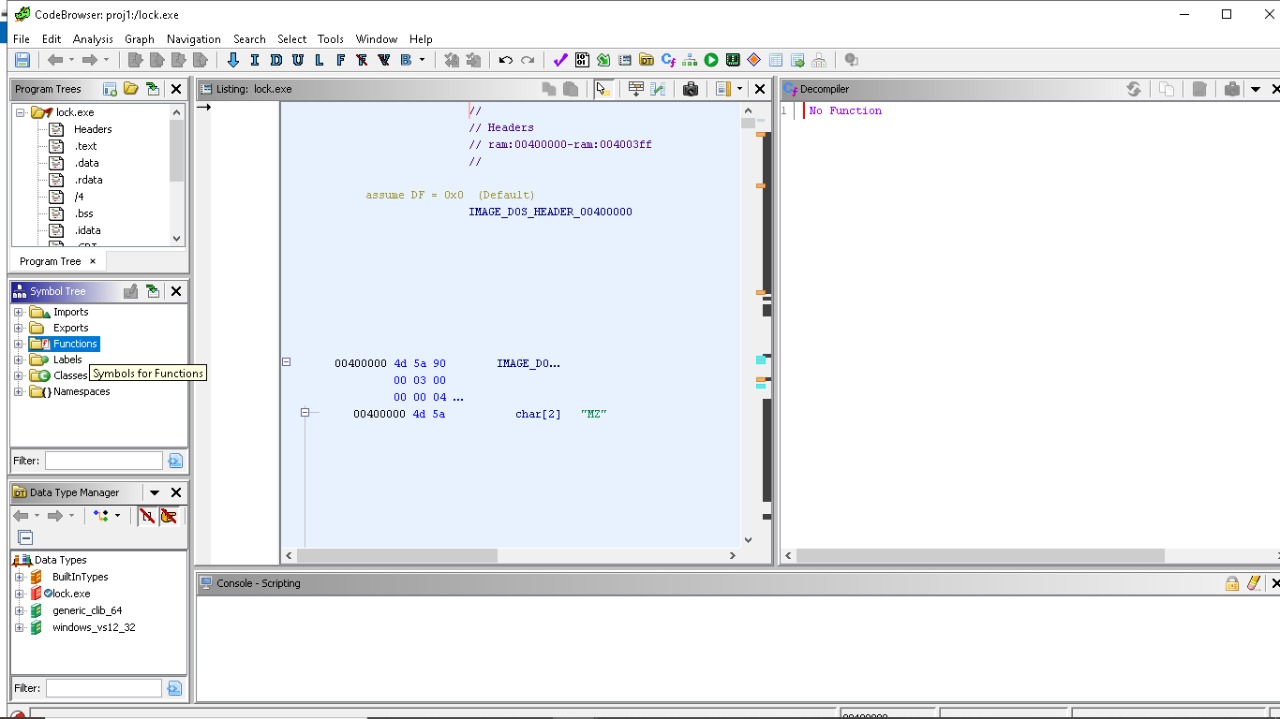
A big hint is given in the question description. The name of the dragon rings a bell of using Ghidra decompiler.

Let’s load our file in Ghidra.

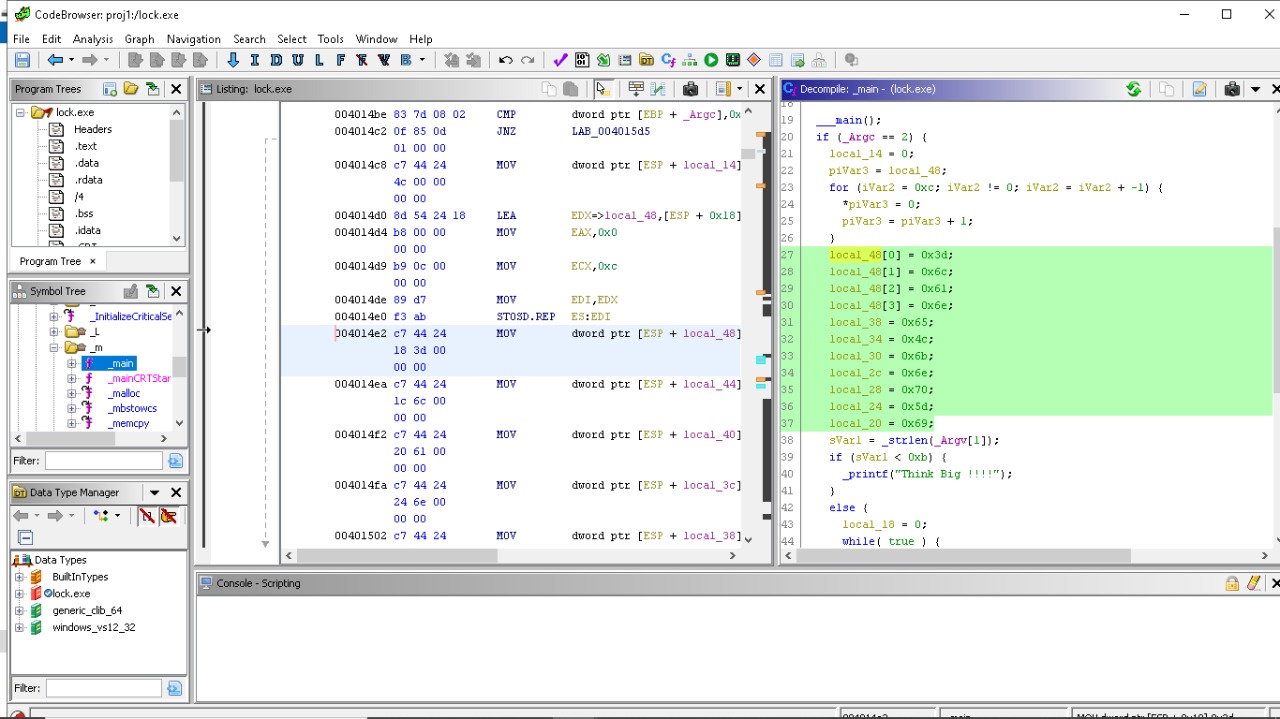
After analysing the file, we need to search for main function as the original file was written in C language.



On the left-hand side, we can find functions folder. There in “\_” subfolder, we will browse to “\_m” subfolder. In this subfolder we will find the main function as “\_\_main”.



On the right-hand side, in decompiled window, we can find the pseudo-C code of main function.



We have a simple array of 11 elements containing some hexadecimal values.

When we find the ASCII value of these hex numbers we get “=laneLknp]i”.

If we supply this string of 11 as our spell, Ghidra is rewards us with the flag.

```

> .\lock.exe =laneLknp]i

Ghidra is freed, he would like to reward you with a flag !!!

AperiPortam

```

### Flag

VishwaCTF{AperiPortam}