Basic Malware RE

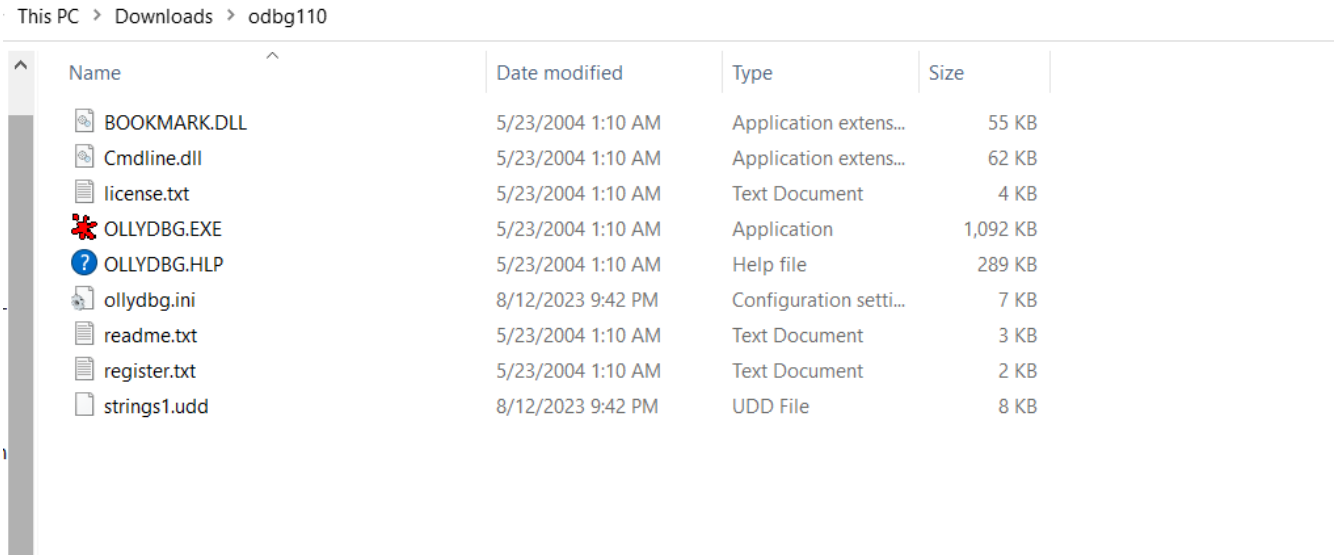
Task 1

Checking through Notepad+++ does not reveal much because there are too many options.

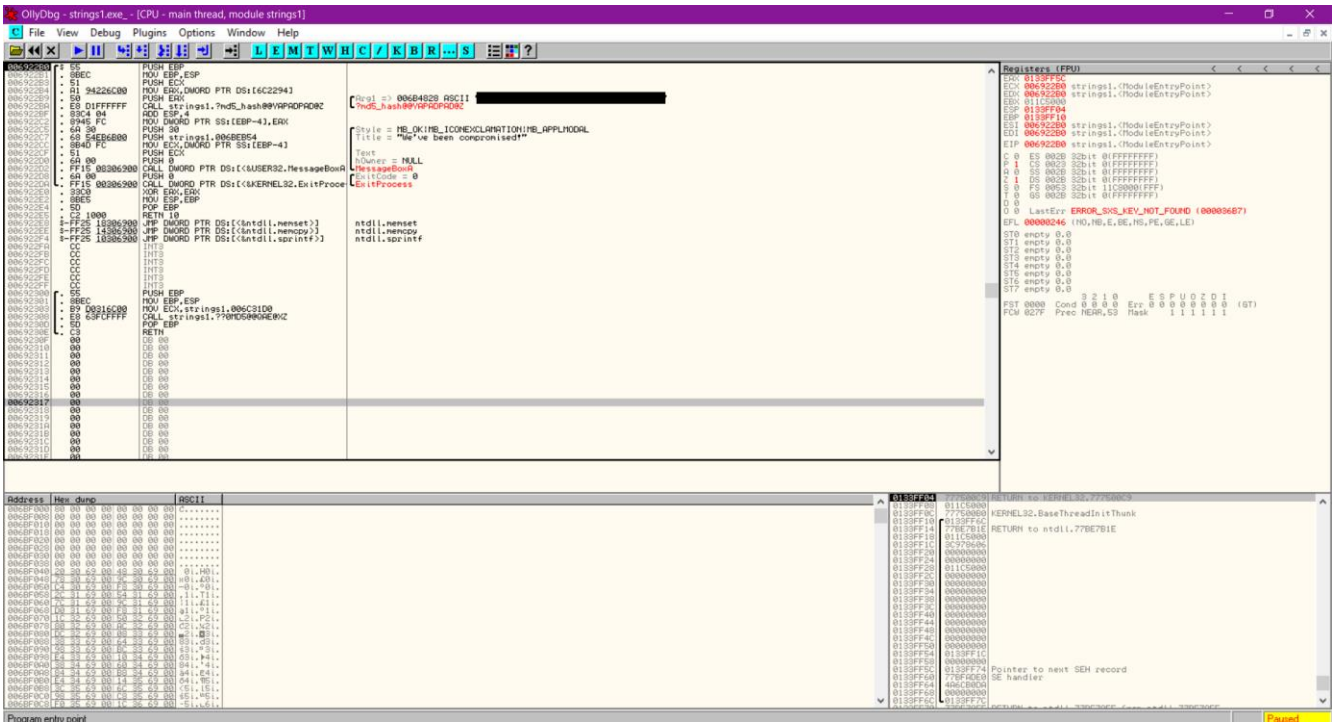
Screenshot below:

Now we go and try to use **OllyDBG** (similar tool to **IDA pro**) to check if we can get more information.

Shown below:

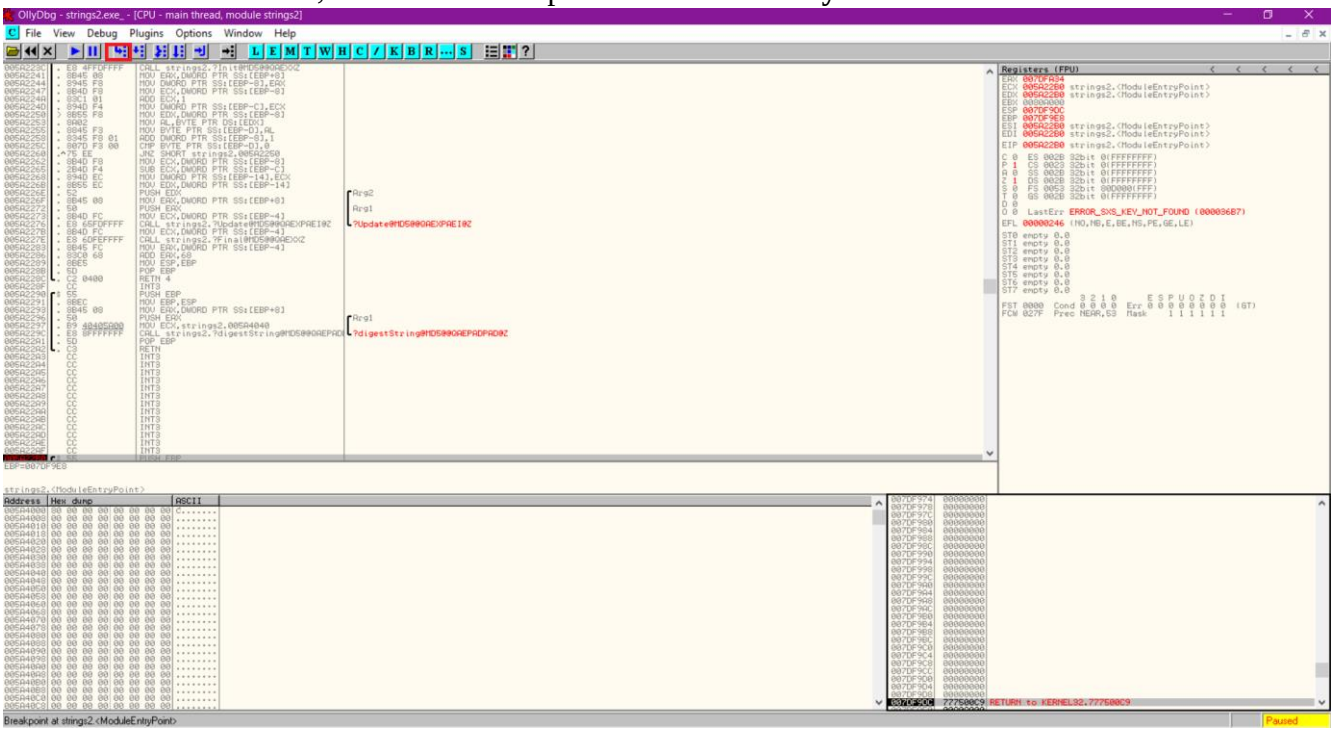


Using **OllyDBG** the flag is revealed right away.

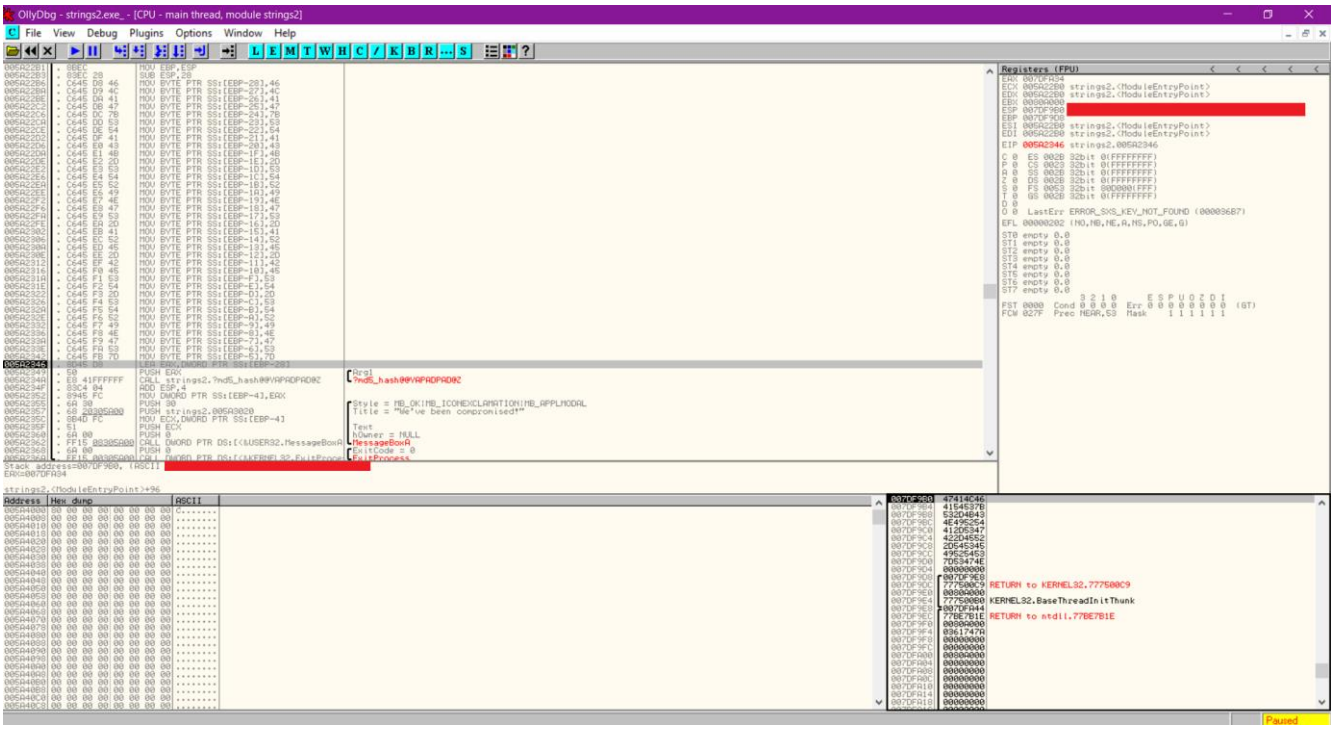


Task 2

Not so obvious this time, so we use the step into function of **OllyDBG**



After stepping through we find the flag



Task 3

After stepping through we notice rc.rc.

After noticing LoadStringA we add a breakpoint. After running the program breakpoint is triggered and we see the flag