

## Basic Malware RE

### Task 1

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

Screenshot below:



Normal text file length: 213,504 lines: 49 Ln: 16 Col: 570 Pos: 6,735 Macintosh (CR) ANSI INS

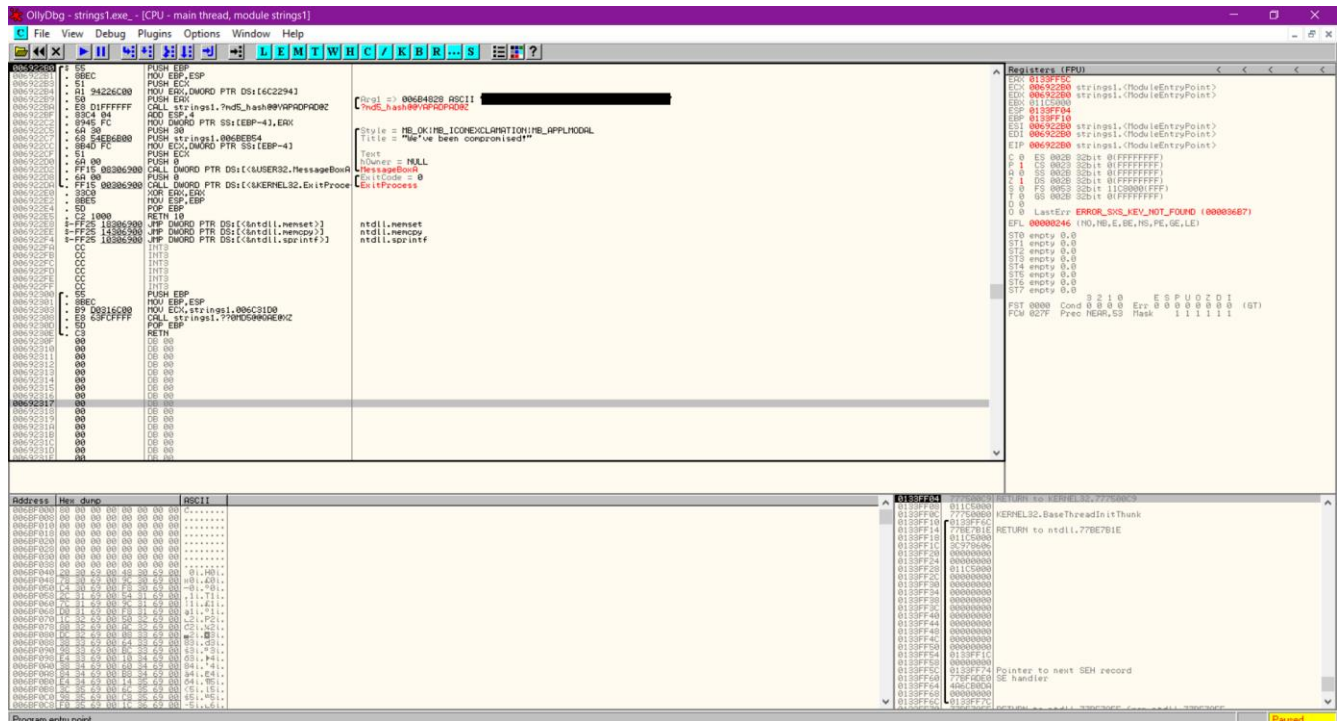
Now we go and try to use **OllyDBG** (similar tool to **IDA pro**) to check if we can get more information.

Shown below:

This PC > Downloads > odbg110

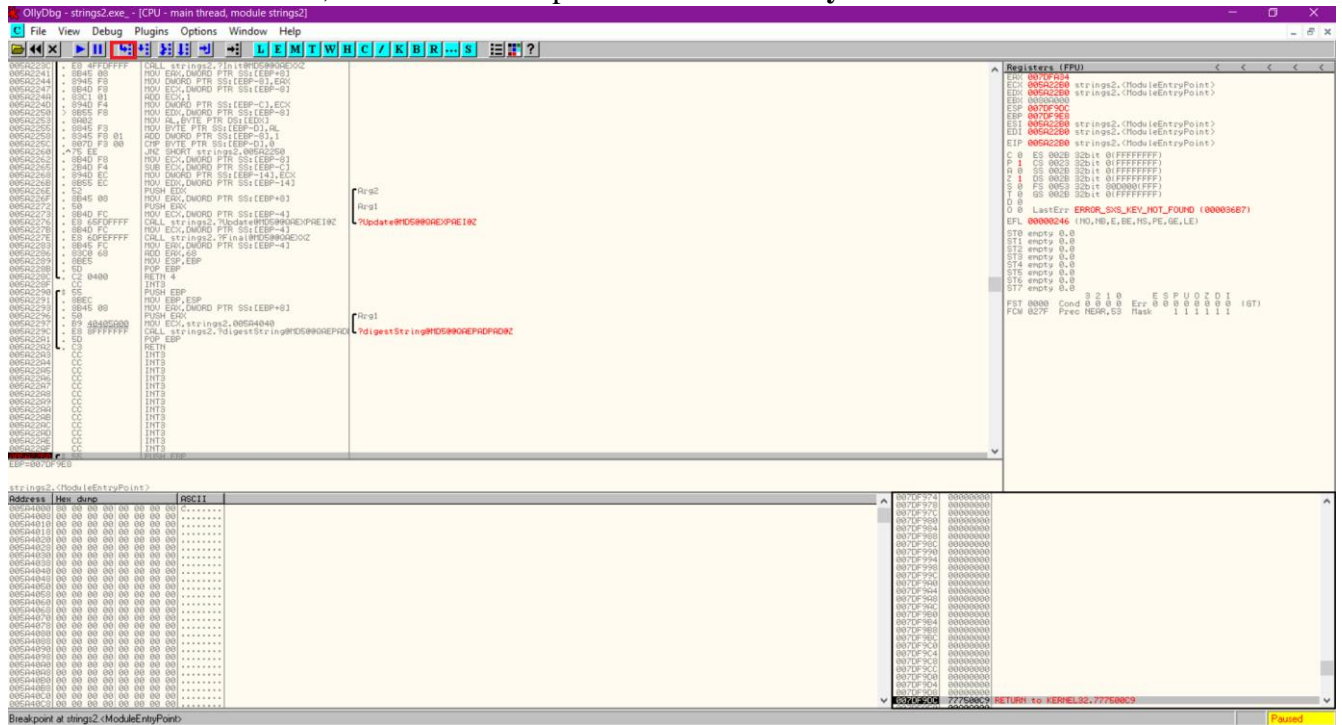
Name	Date modified	Type	Size
BOOKMARK.DLL	5/23/2004 1:10 AM	Application extens...	55 KB
Cmdline.dll	5/23/2004 1:10 AM	Application extens...	62 KB
license.txt	5/23/2004 1:10 AM	Text Document	4 KB
OLLYDBG.EXE	5/23/2004 1:10 AM	Application	1,092 KB
OLLYDBG.HLP	5/23/2004 1:10 AM	Help file	289 KB
ollydbg.ini	8/12/2023 9:42 PM	Configuration setti...	7 KB
readme.txt	5/23/2004 1:10 AM	Text Document	3 KB
register.txt	5/23/2004 1:10 AM	Text Document	2 KB
strings1.udd	8/12/2023 9:42 PM	UDD File	8 KB

Using OllyDBG the flag is revealed right away.

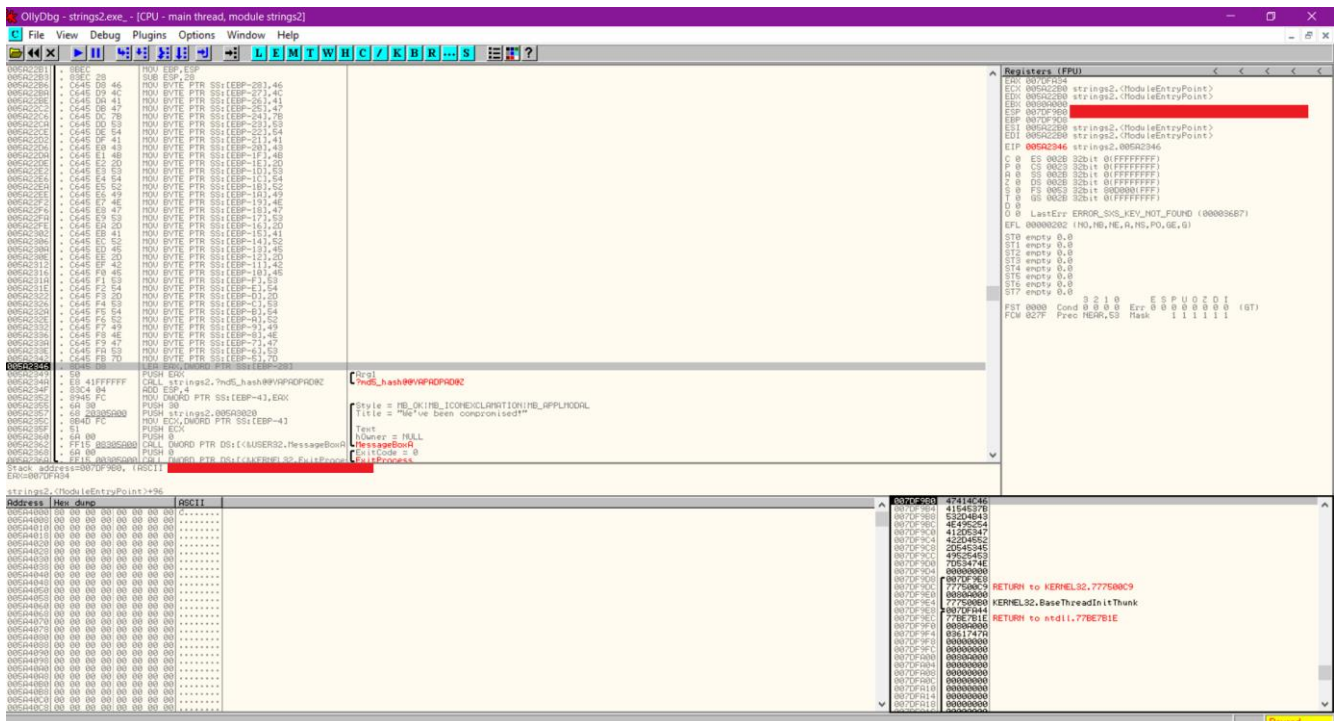


## Task 2

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

