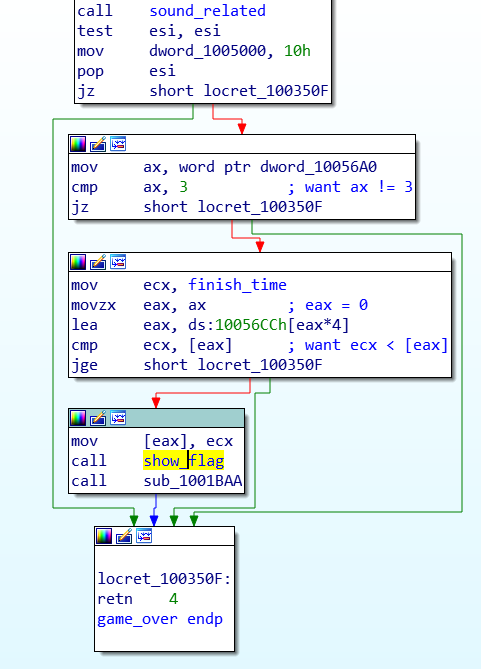
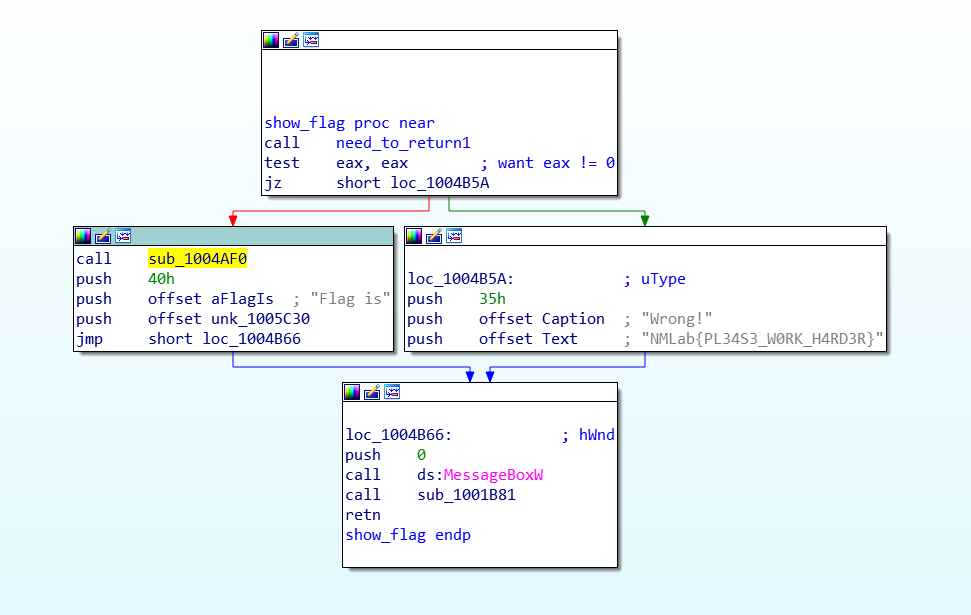
黃禹靖 電機四 b05901172

思路：

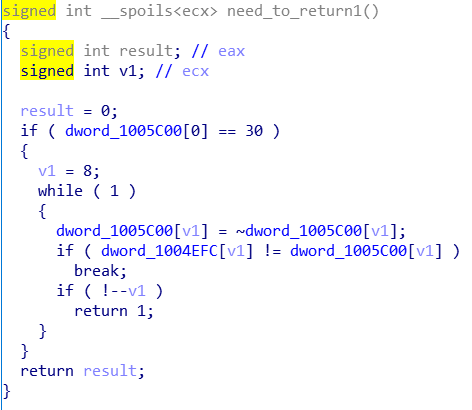
1. 如助教上課的步驟找到game over的function和裡面show\_flag的function。
2. 用debuger發現要採完地雷才有機會走到show\_flag的上面。如圖esi是1代表遊戲勝利，0代表踩到地雷。



1. 採完地雷後觀察發現dword\_100579C（圖中finish\_time）裡面是遊戲完成的時間，但是要小於1才會走到print flag，所以直接用debuger改成0。
2. 進入show\_flag裡發現第一個function必須回傳1，才會走左邊。所以進去看這個function。



1. 直接轉成c code發現他的架構是先一個if再比較dword\_1004EFC和dword\_1005C00兩個大小是8的陣列必須每個都相等才會回傳1。所以一樣用debuger改register讓他進入if裡。並且dword\_1005C00在show\_flag裡走左邊後的第一個function（sub\_1004AF0）有再被使用到，所以得知這個陣列可能跟印出flag有關，比較重要。因此把他的值都改成跟dword\_1004EFC裡的一樣。



1. 最後跑到 MessageBoxW這個library function就印出flag了。

Flag：

NMLab{You\_are\_good\_at\_mining\_:D}