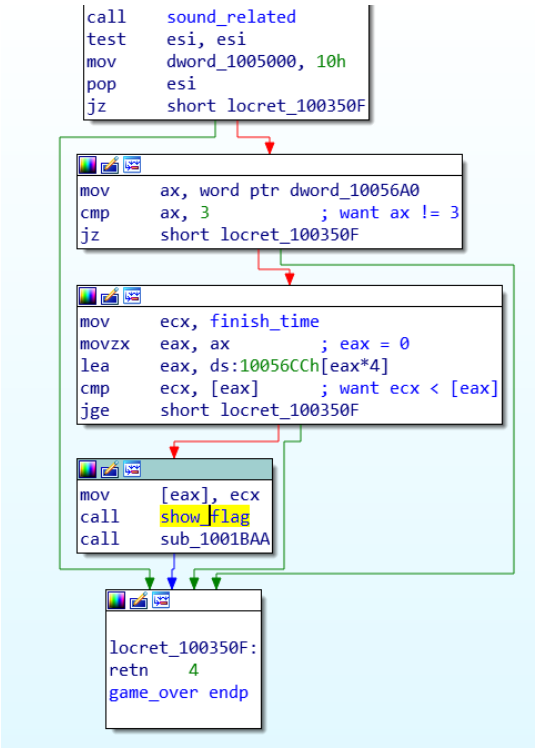
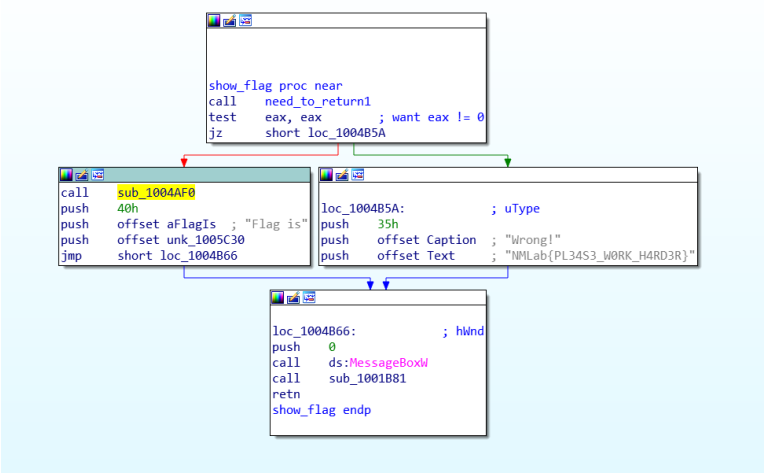
黃禹靖 電機四 b05901172

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。



3. 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。
4. 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。



5. 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。

```
signed int __spoils<ecx> need_to_return1()
{
  signed int result; // eax
  signed int v1; // ecx

  result = 0;
  if ( dword_1005C00[0] == 30 )
  {
    v1 = 8;
    while ( 1 )
    {
      dword_1005C00[v1] = ~dword_1005C00[v1];
      if ( dword_1004EFC[v1] != dword_1005C00[v1] )
        break;
      if ( !--v1 )
        return 1;
    }
  }
  return result;
}
```

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

Flag：

NMLab{You_are_good_at_mining_:D}