

[9] Terminate the target process properly. How did you do that?

EndDialog

- 다이얼로그 창을 닫으려면 **EndDialog**가 실행되어야한다
- XREF 함수는 **FUN_14000a5a0** 이다.

```
*****
*                               *
*          POINTER to EXTERNAL FUNCTION          *
*                               *
*****
BOOL __fastcall EndDialog(HWND hDlg, INT_PTR nResult)
EAX:4      <RETURN>
RCX:8      hDlg
RDX:8      nResult
242 EndDialog <<not bound>>
PTR_EndDialog_14001f408      XREF[1]:  FUN_14000a5a0:14000a5be (R)
14001f408 be bf 02      addr  USER32.DLL:EndDialog
      00 00 00
      00 00
```

FUN_14000a5a0

- 이 함수의 XREF는 **FUN_140008a10** 이다.

FUN_140008a10

```
Decompile: FUN_140008a10 - (KU-RE{Final}.exe)
1
2 void FUN_140008a10(longlong param_1,undefined8 param_2,ushort param_3)
3
4 {
5     HANDLE hObject;
6     longlong lVar1;
7     wchar_t *pwVar2;
8     WCHAR *pWVar3;
9     undefined auStackY_c8 [32];
10    WCHAR local_78 [40];
11    ulonglong local_28;
12
13    local_28 = DAT_14002d080 ^ (ulonglong)auStackY_c8;
14    pwVar2 = L"KU-DFRC-ReverseMe2-Happy-New-Year.hdn";
15    pWVar3 = local_78;
16    for (lVar1 = 0x4c; lVar1 != 0; lVar1 = lVar1 + -1) {
17        *(undefined *)pWVar3 = *(undefined *)pwVar2;
18        pwVar2 = (wchar_t *) ((longlong)pwVar2 + 1);
19        pWVar3 = (WCHAR *) ((longlong)pWVar3 + 1);
20    }
21    hObject = CreateFileW(local_78,0x80000000,0,(LPSECURITY_ATTRIBUTES)0x0,3,0,(HANDLE)0x0);
22    if (hObject == (HANDLE)0xffffffff) {
23        FUN_14000a5a0(param_1,(uint)param_3);
24    }
25    else {
26        CloseHandle(hObject);
27    }
28    FUN_14000b800(local_28 ^ (ulonglong)auStackY_c8);
29    return;
30}
31
```

- 이 함수는 KU-DFRC-ReverseMe2-Happy-New-Year.hdn을 CreateFileW로 부르고 있다.
- 그리고 이 과정에서 오류가 나야지 EndDialog 함수로 들어가게 되어있다.
- CreateFile의 플래그 중 **dwCreationDisposition**: OPEN_EXISTING(0x3) 이 있으므로 이를 이용하면 될 것 같다.
 - 이 해당 파일이 만약 지워져있으면, OPEN_EXISTING 플래그에서 오류가 나게 된다. 존재하는 파일이 아니기 때문이다.
- 따라서 hidden 파일을 삭제하고, 닫기 창을 누르니까 잘 닫아졌다.

결과

KU-DFRC-ReverseMe2-Happy-New-Year.hdn 파일을 삭제하고, 닫는다.