

void \_\_thiscall sub\_4018E0(CWnd \*this)

* **의심스러운 루틴 1**

if ( ATL::CSimpleStringT<char,1>::GetLength(v4) <= 0 )

{

v3 = CWnd::GetDlgItem(this, 1);

CWnd::EnableWindow(v3, 0);

}

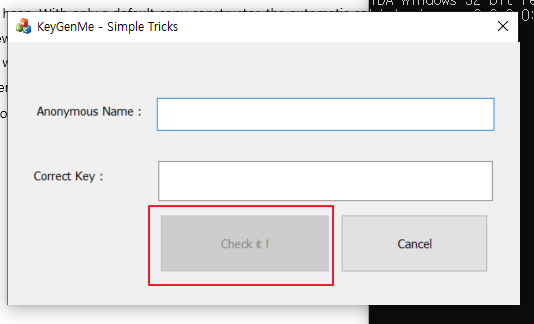
else

{

v2 = CWnd::GetDlgItem(this, 1);

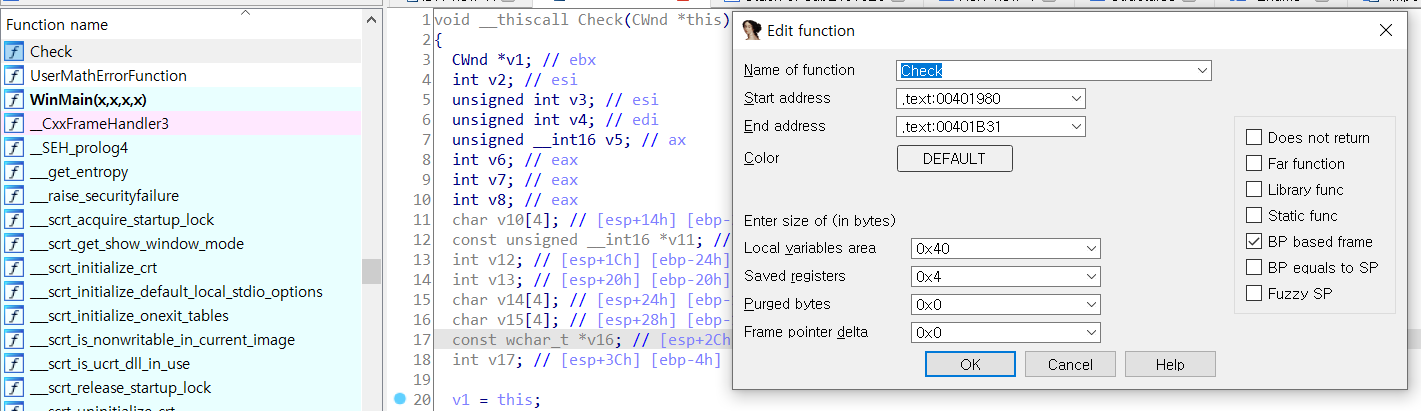
CWnd::EnableWindow(v2, 1);

}



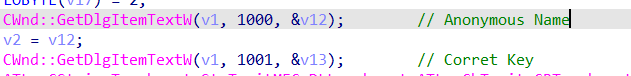
Check it ! 이라고 적힌 이부분 활성화 시키는 루틴 인듯합니다.

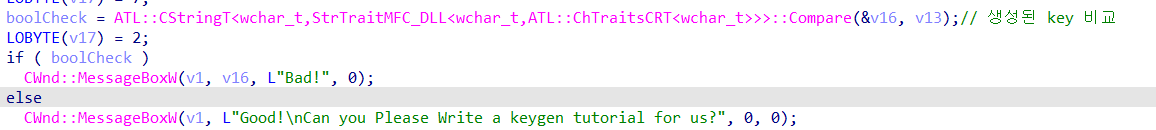
--------------------------------------------------------------------------------------------------------------



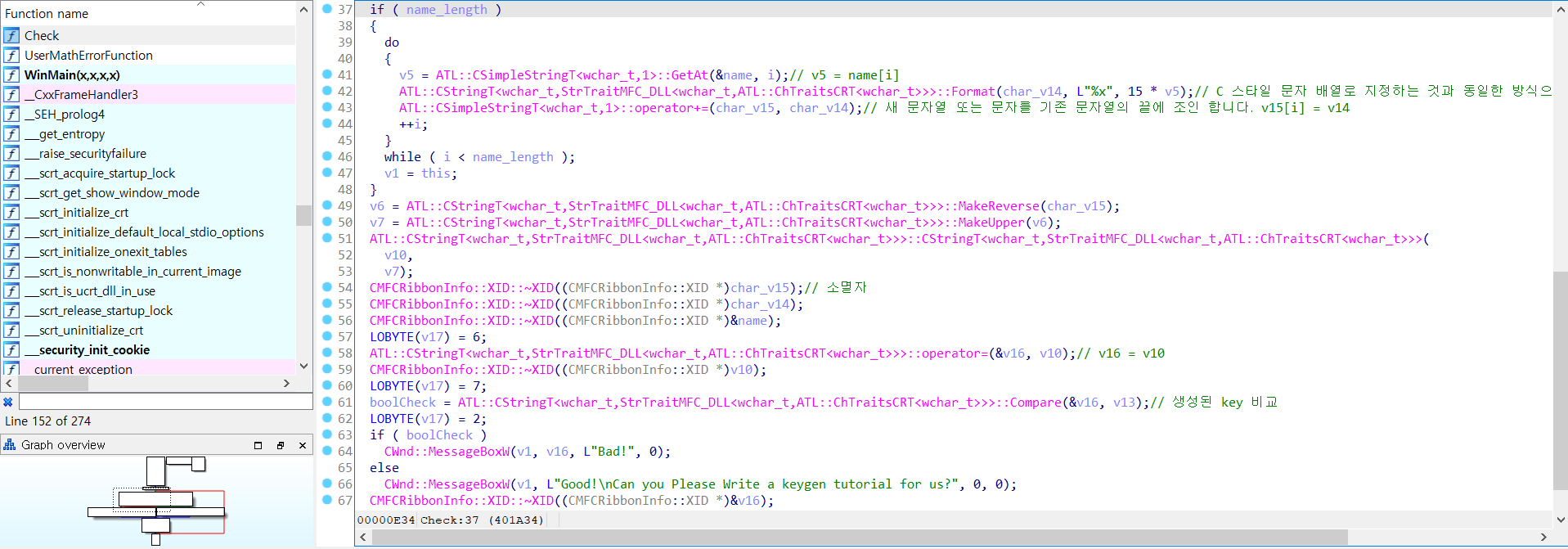
address: 0x00401980

* **키젠 루틴 발견**





* **생성된 key 비교**



void \_\_thiscall Check(CWnd \*this)

{

CWnd \*v1; // ebx

int v2; // esi

unsigned int name\_length; // esi

unsigned int i; // edi

unsigned \_\_int16 v5; // ax 16bit == 2byte == wchar\_t

int v6; // eax

int v7; // eax

int boolCheck; // eax

char v10[4]; // [esp+14h] [ebp-2Ch] BYREF

const unsigned \_\_int16 \*name; // [esp+18h] [ebp-28h] BYREF 16bit == 2byte == wchar\_t

int v12; // [esp+1Ch] [ebp-24h] BYREF

int v13; // [esp+20h] [ebp-20h] BYREF

char char\_v14[4]; // [esp+24h] [ebp-1Ch] BYREF

char char\_v15[4]; // [esp+28h] [ebp-18h] BYREF

const wchar\_t \*v16; // [esp+2Ch] [ebp-14h] BYREF

int v17; // [esp+3Ch] [ebp-4h]

v1 = this;

ATL::CStringT<char,StrTraitMFC\_DLL<char,ATL::ChTraitsCRT<char>>>::CStringT<char,StrTraitMFC\_DLL<char,ATL::ChTraitsCRT<char>>>(&v12);

v17 = 0;

ATL::CStringT<char,StrTraitMFC\_DLL<char,ATL::ChTraitsCRT<char>>>::CStringT<char,StrTraitMFC\_DLL<char,ATL::ChTraitsCRT<char>>>(&v13);

ATL::CStringT<char,StrTraitMFC\_DLL<char,ATL::ChTraitsCRT<char>>>::CStringT<char,StrTraitMFC\_DLL<char,ATL::ChTraitsCRT<char>>>(&v16);

LOBYTE(v17) = 2;

CWnd::GetDlgItemTextW(v1, 1000, &v12); // Anonymous Name

v2 = v12;

CWnd::GetDlgItemTextW(v1, 1001, &v13); // Corret Key

ATL::CStringT<wchar\_t,StrTraitMFC\_DLL<wchar\_t,ATL::ChTraitsCRT<wchar\_t>>>::CStringT<wchar\_t,StrTraitMFC\_DLL<wchar\_t,ATL::ChTraitsCRT<wchar\_t>>>(

&name,

v2);

ATL::CStringT<char,StrTraitMFC\_DLL<char,ATL::ChTraitsCRT<char>>>::CStringT<char,StrTraitMFC\_DLL<char,ATL::ChTraitsCRT<char>>>(char\_v14);

ATL::CStringT<char,StrTraitMFC\_DLL<char,ATL::ChTraitsCRT<char>>>::CStringT<char,StrTraitMFC\_DLL<char,ATL::ChTraitsCRT<char>>>(char\_v15);

LOBYTE(v17) = 5;

name\_length = wcslen(name); // 입력받은 name

i = 0;

if ( name\_length )

{

do

{

v5 = ATL::CSimpleStringT<wchar\_t,1>::GetAt(&name, i);// v5 = name[i]

ATL::CStringT<wchar\_t,StrTraitMFC\_DLL<wchar\_t,ATL::ChTraitsCRT<wchar\_t>>>::Format(char\_v14, L"%x", 15 \* v5);// C 스타일 문자 배열로 지정하는 것과 동일한 방식으로 형식이 지정된 데이터를 씁니다.

ATL::CSimpleStringT<wchar\_t,1>::operator+=(char\_v15, char\_v14);// 새 문자열 또는 문자를 기존 문자열의 끝에 조인 합니다. v15[i] = v14

++i;

}

while ( i < name\_length );

v1 = this;

}

v6 = ATL::CStringT<wchar\_t,StrTraitMFC\_DLL<wchar\_t,ATL::ChTraitsCRT<wchar\_t>>>::MakeReverse(char\_v15);

v7 = ATL::CStringT<wchar\_t,StrTraitMFC\_DLL<wchar\_t,ATL::ChTraitsCRT<wchar\_t>>>::MakeUpper(v6);

ATL::CStringT<wchar\_t,StrTraitMFC\_DLL<wchar\_t,ATL::ChTraitsCRT<wchar\_t>>>::CStringT<wchar\_t,StrTraitMFC\_DLL<wchar\_t,ATL::ChTraitsCRT<wchar\_t>>>(

v10,

v7);

CMFCRibbonInfo::XID::~XID((CMFCRibbonInfo::XID \*)char\_v15);// 소멸자

CMFCRibbonInfo::XID::~XID((CMFCRibbonInfo::XID \*)char\_v14);

CMFCRibbonInfo::XID::~XID((CMFCRibbonInfo::XID \*)&name);

LOBYTE(v17) = 6;

ATL::CStringT<wchar\_t,StrTraitMFC\_DLL<wchar\_t,ATL::ChTraitsCRT<wchar\_t>>>::operator=(&v16, v10);// v16 = v10

CMFCRibbonInfo::XID::~XID((CMFCRibbonInfo::XID \*)v10);

LOBYTE(v17) = 7;

boolCheck = ATL::CStringT<wchar\_t,StrTraitMFC\_DLL<wchar\_t,ATL::ChTraitsCRT<wchar\_t>>>::Compare(&v16, v13);// 생성된 key 비교

LOBYTE(v17) = 2;

if ( boolCheck )

CWnd::MessageBoxW(v1, v16, L"Bad!", 0);

else

CWnd::MessageBoxW(v1, L"Good!\nCan you Please Write a keygen tutorial for us?", 0, 0);

CMFCRibbonInfo::XID::~XID((CMFCRibbonInfo::XID \*)&v16);

CMFCRibbonInfo::XID::~XID((CMFCRibbonInfo::XID \*)&v13);

CMFCRibbonInfo::XID::~XID((CMFCRibbonInfo::XID \*)&v12);

}



키젠 루틴을 찾았으니 즐거운 코딩시간~