ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»

Институт энергетики, информационных технологий и управляющих систем

Кафедра программного обеспечения вычислительной техники и

автоматизированных систем

Индивидуальное домашнее задание  
по дисциплине: «Архитектура вычислительных систем»  
на тему «Получение стека вызовов»

Выполнил: ст. группы ВТ-192

Федосеев Артём Дмитриевич

Проверил: Осипов О.В.

Белгород 2021

Получив адрес текущей вершины стека, мы можем начать исследовать стек на предмет наличия адресов возврата (а мы знаем, что адреса возврата при входе в функцию хранятся в стеке). В этом нам поможет стандартная WinAPI функция GetModuleHandleEx, которая возвращает начальный адрес модуля, в котором располагается инструкция с заданным адресом.

Далее, получив адрес модуля, мы можем узнать его имя с помощью функции GetModuleFileName. А имя самой функции, возврат которой мы нашли, поможет узнать функция SymFromAddr, обьявленная в библиотеке dbghelp.h

Функция, получающая стек вызовов:

#include "stdafx.h"

#include <Windows.h>

#include <iostream>

#include <string>

#include <winternl.h>

#include <cstdlib>

#include <dbghelp.h>

#define WIN32\_WINNT 0x0501

#pragma comment(lib, "dbghelp.lib")

using namespace std;

void AlienFunc() {

long long tmp;

DWORD\_PTR\* stack\_ptr = (DWORD\_PTR\*)&tmp;

DWORD\_PTR\* stack\_end = (DWORD\_PTR\*)((DWORD\_PTR)(stack\_ptr) | 0xFFFF);

HMODULE moduleHandle = NULL;

wchar\_t buffer[MAX\_PATH];

DWORD size = 2000;

HANDLE process = GetCurrentProcess();

SymInitialize(process, NULL, TRUE);

SYMBOL\_INFO\* sym = (SYMBOL\_INFO\*)calloc(sizeof(SYMBOL\_INFO) + 256 \* sizeof(char), 1);

sym->MaxNameLen = 255;

sym->SizeOfStruct = sizeof(SYMBOL\_INFO);

int i = 0;

while (stack\_ptr < stack\_end) {

if (GetModuleHandleEx(GET\_MODULE\_HANDLE\_EX\_FLAG\_FROM\_ADDRESS, (LPCTSTR)\*stack\_ptr, &moduleHandle))

{

cout << "Module address: 0x" << moduleHandle << endl;

if (GetModuleFileName(moduleHandle, buffer, size))

wprintf(L"Module name: %s\n", buffer);

SymFromAddr(process, (DWORD64)(\*stack\_ptr), 0, sym);

cout << sym->Name << " - " << sym->Address << endl;

}

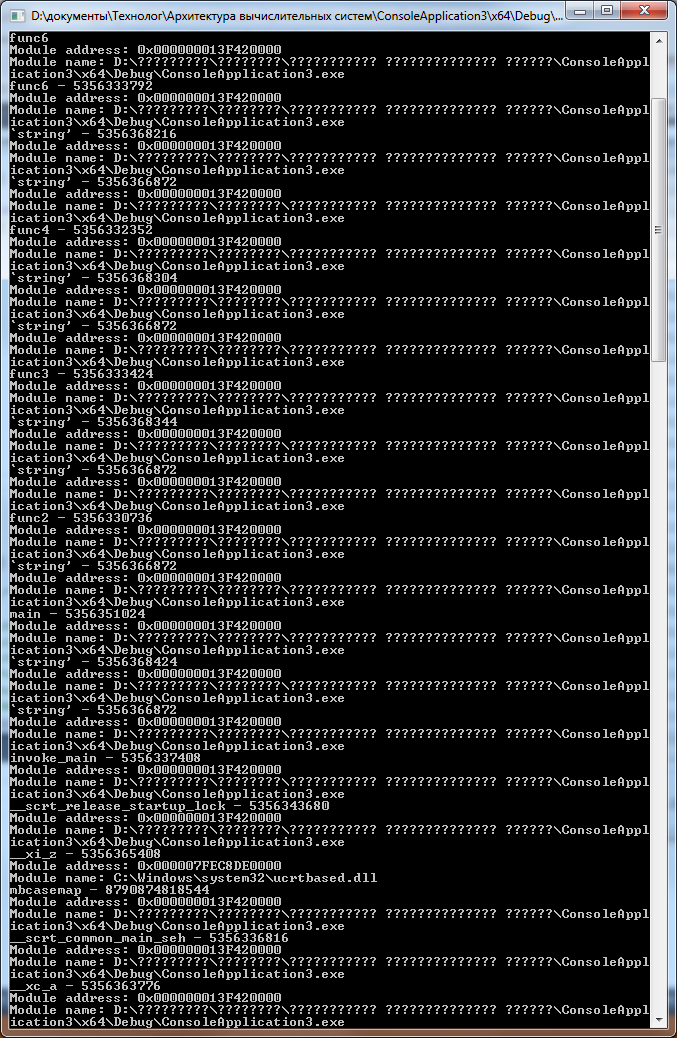
i++;

stack\_ptr++;

}

}

Демонстрация работы функции:



Как можно увидеть, функция получает информацию как о системных, так и пользовательских функциях внутри программы:

Полезные ссылки:

## https://firststeps.ru/mfc/winapi/r.php?22 - Вызов функций из DLL - GetModuleHandle и GetProcAddress

http://vsokovikov.narod.ru/New\_MSDN\_API/DLL/fn\_getmodulehandleex.htm   
http://vsokovikov.narod.ru/New\_MSDN\_API/DLL/fn\_getmodulefilename.htm

изложение работы функций получения дескриптора и имени

https://docs.microsoft.com/ru-ru/windows/win32/api/winternl/ns-winternl-peb  
https://docs.microsoft.com/en-us/windows/win32/api/winternl/ns-winternl-peb\_ldr\_data

описание структур процесса (Process Environment Block)

https://habr.com/ru/post/187226/ - получение PEB

https://www.codeproject.com/Articles/10438/Navigating-the-PEB - исследование PEB на предмет поиска процессов и их параметров ( АНГЛ)

https://eli.thegreenplace.net/2015/programmatic-access-to-the-call-stack-in-c/ - разбор дебаггинга и backtrace под линухсом

https://habr.com/ru/company/intel/blog/94340/ - про особенности и выгодность стиля вызова + стека в х64 приложениях

https://www.cyberforum.ru/post6242556.html - довольно подробно о выравнивании выделяемой памяти

https://www.sciencedirect.com/science/article/pii/S1742287618300458#fig2 - про построение StackTrace на х64 стеке (АНГЛ)