Отчет по лабораторной работе № 5

«Работа с объектами системы Windows»

7 вариант

Выполнил: студент группы P3317

Плюхин Д.А.

Преподаватель: Зинчик Александр Адольфович

# **Задание**

# Написать программу, позволяющая получить список всех загруженных модулей и позволяющая определить для каждого модуля процессы, использующие данный модуль.

# **Исходный код**

## Основная функция

freopen( "file.txt", "w", stdout );

DWORD aProcesses[1024];

DWORD cbNeeded;

DWORD cProcesses;

unsigned int i;

if ( !EnumProcesses( aProcesses, sizeof(aProcesses), &cbNeeded ) )

return 1;

cProcesses = cbNeeded / sizeof(DWORD);

for ( i = 0; i < cProcesses; i++ )

{

CollectModuleNames( aProcesses[i] );

}

std::cout << "Found " << current\_index\_modules << " loaded modules" << endl;

for ( i = 0; i < current\_index\_modules; i++){

\_tprintf( TEXT("Module %s is used by\n"),szModNames[i]);

for (int j = 0; j < cProcesses; j++ ){

PrintProcessesForModule(aProcesses[j], i);

}

}

return 0;

## Получение и сохранение загруженных модулей для конкретного процесса

int CollectModuleNames( DWORD processID )

{

HMODULE hMods[1024];

HANDLE hProcess;

DWORD cbNeeded;

unsigned int i;

hProcess = OpenProcess( PROCESS\_QUERY\_INFORMATION |

PROCESS\_VM\_READ,

FALSE, processID );

if (NULL == hProcess)

return 1;

if( EnumProcessModules(hProcess, hMods, sizeof(hMods), &cbNeeded))

{

for ( i = 0; i < (cbNeeded / sizeof(HMODULE)); i++ )

{

TCHAR szModName[MAX\_PATH];

if ( GetModuleFileNameEx( hProcess, hMods[i], szModName, sizeof(szModName) / sizeof(TCHAR)))

{

bool wasThisModule = false;

for (int j = 0; j < current\_index\_modules; j++){

if (strcmp(szModNames[j], szModName) == 0){

wasThisModule = true;

break;

}

}

if (!wasThisModule){

GetModuleFileNameEx( hProcess, hMods[i], szModNames[current\_index\_modules], sizeof(szModNames[current\_index\_modules]) / sizeof(TCHAR));

current\_index\_modules++;

}

}

}

}

CloseHandle( hProcess );

return 0;

}

## Вывод процессов, использующих конкретный модуль

int PrintProcessesForModule( DWORD processID, int module\_index )

{

HMODULE hMods[1024];

HANDLE hProcess;

DWORD cbNeeded;

unsigned int i;

hProcess = OpenProcess( PROCESS\_QUERY\_INFORMATION |

PROCESS\_VM\_READ,

FALSE, processID );

if( EnumProcessModules(hProcess, hMods, sizeof(hMods), &cbNeeded)){

for ( i = 0; i < (cbNeeded / sizeof(HMODULE)); i++ ){

TCHAR szModName[MAX\_PATH];

TCHAR szProcessName[MAX\_PATH];

if ( GetModuleFileNameEx( hProcess, hMods[i], szModName, sizeof(szModName) / sizeof(TCHAR)))

{

if (strcmp(szModNames[module\_index], szModName) == 0){

if (GetModuleFileNameEx(hProcess, 0, szProcessName, MAX\_PATH)){

\_tprintf( TEXT("\t%s\n"),szProcessName);

return 0;

}

}

}

}

}

return 0;

}

# **Пример фрагмента вывода**

Module C:\WINDOWS\SYSTEM32\ntdll.dll is used by

C:\Program Files (x86)\Lenovo\PowerDVD10\PDVD10Serv.exe

C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat\acrotray.exe

C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe

C:\Program Files (x86)\Jumpstart\jswtrayutil.exe

C:\Program Files\Lenovo\Lenovo Solution Center\LSCNotify.exe

C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Program Files (x86)\Microsoft Visual Studio 14.0\VC\bin\vctip.exe

C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

C:\Users\Zerbs\Desktop\interfaces\lab\_5\main.exe

Module C:\WINDOWS\System32\KERNEL32.DLL is used by

C:\Program Files (x86)\Lenovo\PowerDVD10\PDVD10Serv.exe

C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat\acrotray.exe

C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe

C:\Program Files (x86)\Jumpstart\jswtrayutil.exe

C:\Program Files\Lenovo\Lenovo Solution Center\LSCNotify.exe

C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

C:\Users\Zerbs\Desktop\interfaces\lab\_5\main.exe

Module C:\WINDOWS\System32\KERNELBASE.dll is used by

C:\Program Files (x86)\Lenovo\PowerDVD10\PDVD10Serv.exe

C:\Program Files (x86)\Adobe\Acrobat 11.0\Acrobat\acrotray.exe

C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe

C:\Program Files (x86)\Jumpstart\jswtrayutil.exe

C:\Program Files\Lenovo\Lenovo Solution Center\LSCNotify.exe

C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Users\Zerbs\AppData\Local\atom\app-1.22.1\atom.exe

C:\Program Files (x86)\Microsoft Visual Studio 14.0\VC\bin\vctip.exe

C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE

C:\Users\Zerbs\Desktop\interfaces\lab\_5\main.exe

# **Вывод**

Таким образом, получение списка загруженных модулей и соответствующих им процессов не сопряжено с большими трудности в случае программирования под Windows.