



ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно
&& видно?



Напишите в чат, если есть проблемы!

Ставьте если все хорошо

Программирование **Native** приложений

Таблица экспорта



1

Таблица экспорта

Описывается структурой `_IMAGE_EXPORT_DIRECTORY`

```
typedef struct _IMAGE_EXPORT_DIRECTORY {
    DWORD Characteristics;
    DWORD TimeDateStamp;
    WORD MajorVersion;
    WORD MinorVersion;
    DWORD Name;
    DWORD Base;
    DWORD NumberOfFunctions;
    DWORD NumberOfNames;
    /*+0x1C*/ DWORD AddressOfFunctions; // RVA from base of image
    DWORD AddressOfNames; // RVA from base of image
    DWORD AddressOfNameOrdinals; // RVA from base of image
} IMAGE_EXPORT_DIRECTORY, *PIMAGE_EXPORT_DIRECTORY;
```

```
} IMAGE_EXPORT_DIRECTORY, *PIMAGE_EXPORT_DIRECTORY;
    DWORD AddressOfNameOrdinals; // RVA from base of image
    DWORD AddressOfNames; // RVA from base of image
```

Получить указатель на `_IMAGE_DOS_HEADER`

По полю `_IMAGE_DOS_HEADER.e_lfanew (0x3C)`
получить смещение до `_IMAGE_NT_HEADERS`

По смещению `0x78` от `_IMAGE_NT_HEADERS`
читается смещение до таблицы экспорта

Читаются три указателя на массивы

AddressOfFunctions

AddressOfNames

AddressOfNameOrdinals

Из массива имён находится нужная функция по имени (или **хешу**) и запоминается её индекс N

Из массива ординалов читается N -ый элемент - M

Из массива адресов функций читается M -ый элемент - `address`

ИТОГ:

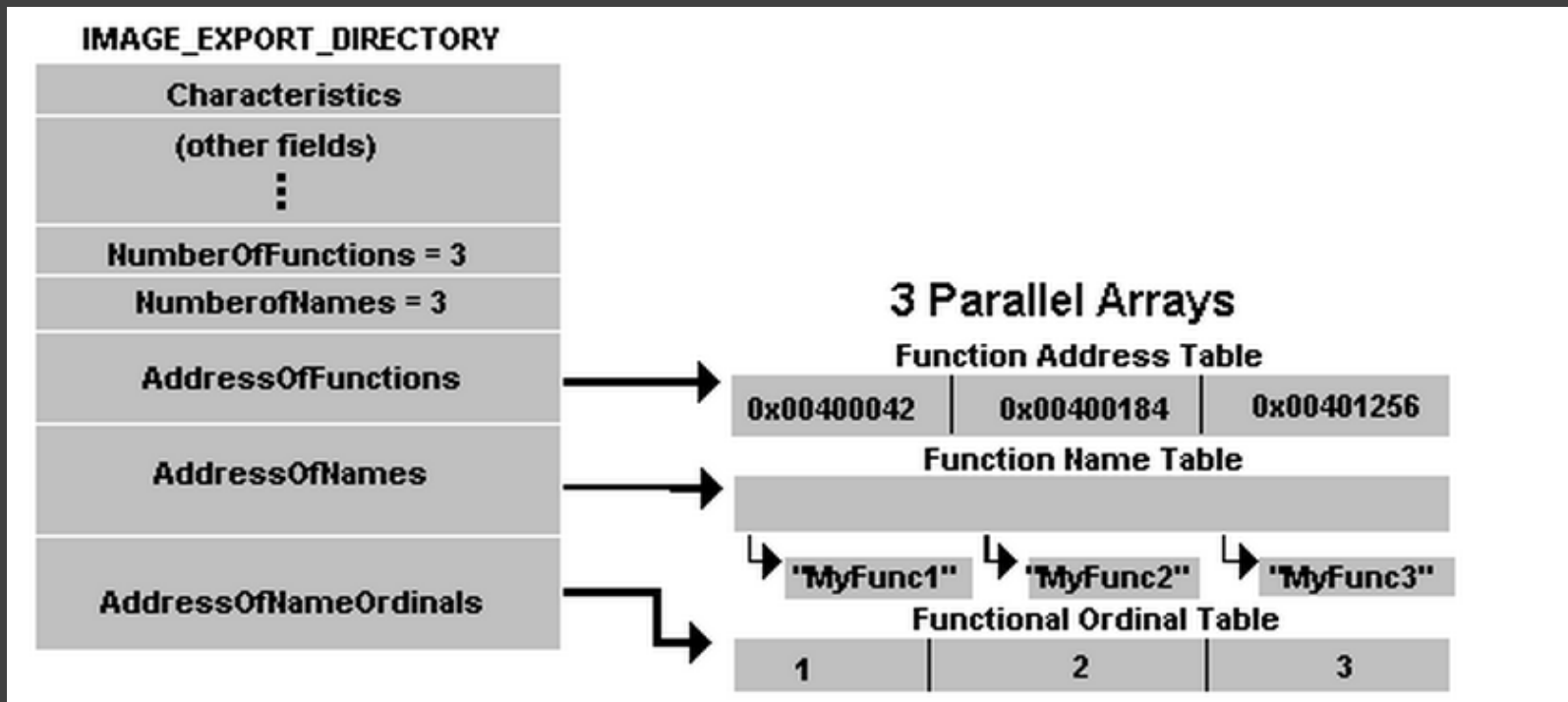


Figure 4. Export table layout

2

Программирование **Native** приложений

Windows Driver Kit Version 7.1.0 Native Development Kit

[скачать](#)[скачать](#)

Windows Driver Kit Version 7.1.0

Important! Selecting a language below will dynamically change the complete page content to that language.

Language: **English**

[Download](#)

The Windows Driver Kit (WDK) Version 7.1.0 is an update to the WDK 7.0.0 release and contains the tools, code samples, documentation, compilers, headers and libraries with which software developers create drivers for Windows 7, Windows Vista, Windows XP, Windows Server 2008 R2, Windows Server 2008, and Windows Server 2003.

Details

Version:

7.1.0

Date Published:

2/26/2010

File Name:

GRMWDK_EN_7600_1.ISO

File Size:

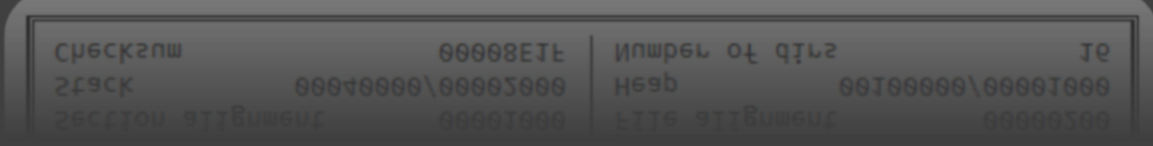
619.8 MB

The Windows Driver Kit (WDK) Version 7.1.0 is an update to the WDK 7.0.0 release and contains the tools, code samples, documentation, compilers, headers and libraries with which software developers create drivers for Windows 7, Windows Vista, Windows XP, Windows Server 2008 R2, Windows Server 2008, and Windows Server 2003. This development kit does not contain device drivers for your personal computer. If you are looking for drivers for your personal computer, go to Microsoft Update for downloads, or visit Windows Hardware Help for more information to find device drivers and hardware. A working knowledge of C programming is necessary to use this kit to develop Windows drivers.

Это программы, способные запускаться на раннем этапе загрузки Windows (до окна входа в систему)

Пример программы: [chkdsk](#)

```
Count of sections                2      Machine                Intel386
Symbol table 00000000[00000000]   Sat Apr 27 05:20:16 2019
Size of optional header          00E0   Magic optional header  010B
Linker version                   9.00   OS version              6.01
Image version                    6.01   Subsystem version      5.01
Entry point                      00001560 Size of code            00000800
Size of init data                00000200 Size of uninit data    00000000
Size of image                    00003000 Size of header         00000400
Base of code                     00001000 Base of data           00002000
Image base                      01000000 Subsystem           Native
Section alignment                00001000 File alignment         00000200
Stack 00040000/00002000         Heap 00100000/00001000
Checksum 00008E1F               Number of dirs        16
```



Native приложения используют только функции, экспортируемые из библиотеки ntdll.dll, которые частично документированы

147	NtDisplayString	ntdll.dll
630	RtlInitUnicodeString	ntdll.dll
103	NtClose	ntdll.dll
358	NtWriteFile	ntdll.dll
265	NtReadFile	ntdll.dll
115	NtCreateFile	ntdll.dll
1268	memset	ntdll.dll
340	NtTerminateProcess	ntdll.dll
355	NtWaitForSingleObject	ntdll.dll
113	NtCreateEvent	ntdll.dll

Недокументированные функции можно подсмотреть [TVT](#)

Undocumented functions of NTDLL

NtDisplayString

```
NTSYSAPI
NTSTATUS
NTAPI

NtDisplayString(

    IN PUNICODE_STRING    String );
```

Function **NtDisplayString** display specified string in *text-mode* (typically: blue screen).
Warning: Trying to display string without previously switch to text-mode results as system hang.

- String Pointer to **UNICODE_STRING** contains string to display. Some basic control characters are implemented (like *CR*, *LF*).

Documented by:
Tomasz Nowak

Requirements:
Library: **ntdll.lib**
Privilege: **SE_TCB_PRIVILEGE**

See also:

Задача

Реализовать **Native** программу,
которая сдампит **MBR**

Описываем функции задержки и вывода на экран

```
void Sleep(DWORD mSec)
{
    LARGE_INTEGER interval;
    interval.QuadPart = -1 * (int)(mSec * 10000);
    NtDelayExecution(FALSE, &interval);
}

void WriteLn(LPWSTR Message)
{
    UNICODE_STRING string;
    RtlInitUnicodeString(&string, Message);
    NtDisplayString(&string);
}
```

```
}
Исходный код: https://github.com/0x00sec/0x00sec/blob/master/src/ntoskrnl/ntoskrnl.c#L10000
```

```
LARGE_INTEGER interval;  
  
interval.QuadPart = -1 * (int)(mSec * 10000);  
  
NtDelayExecution(FALSE, &interval);
```

- **Alertable** If set, execution can break in a result of [NtAlertThread](#) call.
 - **DelayInterval** Delay in 100-ns units. Negative value means delay relative to current.

$$10^3 * 100 * 10^{-9} * 10^4 = 10^3 * 10^{-7} * 10^4 =$$
$$= 10^0 = 1 \text{ sec}$$

Reads data from an open file

```
NTSTATUS NtReadFile(  
    _In_ HANDLE FileHandle,  
    _In_opt_ HANDLE Event,  
    _In_opt_ PIO_APC_ROUTINE ApcRoutine,  
    _In_opt_ PVOID ApcContext,  
    _Out_ PIO_STATUS_BLOCK IoStatusBlock,  
    _Out_ PVOID Buffer,  
    _In_ ULONG Length,  
    _In_opt_ PLARGE_INTEGER ByteOffset,  
    _In_opt_ PULONG Key  
);
```

Event [in, optional]

Optionally, a handle to an event object to set to the signaled state after the read operation completes. Device and intermediate drivers should set this parameter to **NULL**.

NtReadFile

```
RtlInitUnicodeString(&keyboard, L"\\Device\\KeyboardClass0");
InitializeObjectAttributes(&ObjectAttributes, &keyboard, OBJ_CASE_INSENSITIVE, NULL, NULL);

NtCreateFile(&hKeyBoard,
            SYNCHRONIZE | GENERIC_READ | FILE_READ_ATTRIBUTES,
            &ObjectAttributes,
            &Iosb,
            NULL,
            FILE_ATTRIBUTE_NORMAL,
            0,
            FILE_OPEN, FILE_DIRECTORY_FILE,
            NULL, 0);

InitializeObjectAttributes(&ObjectAttributes, NULL, 0, NULL, NULL);
NtCreateEvent(&hEvent, EVENT_ALL_ACCESS, &ObjectAttributes, 1, 0);

if (DumpMbr())
    WriteLn(L"Dump Created!\n");
else
    WriteLn(L"Dump Error!\n");
while (TRUE)
{
    NtReadFile(hKeyBoard, hEvent, NULL, NULL, &Iosb, &kbData, sizeof(KEYBOARD_INPUT_DATA), &ByteOffset, NULL);
    NtWaitForSingleObject(hEvent, TRUE, NULL);

    if (kbData.MakeCode == 0x01) //ESC
    {
        break;
    }
}
```

NtProcessStartup

```
void NtProcessStartup(void* StartupArgument)
{
    HANDLE hKeyBoard, hEvent;
    UNICODE_STRING skull, keyboard;
    OBJECT_ATTRIBUTES ObjectAttributes;
    IO_STATUS_BLOCK Iosb;
    LARGE_INTEGER ByteOffset;
    KEYBOARD_INPUT_DATA kbData;

    RtlInitUnicodeString(&keyboard, L"\\Device\\KeyboardClass0");
    InitializeObjectAttributes(&ObjectAttributes, &keyboard, OBJ_CASE_INSENSITIVE, NULL, NULL);

    NtCreateFile(&hKeyBoard,
                SYNCHRONIZE | GENERIC_READ | FILE_READ_ATTRIBUTES,
                &ObjectAttributes,
                &Iosb,
                NULL,
                FILE_ATTRIBUTE_NORMAL,
                0,
                FILE_OPEN, FILE_DIRECTORY_FILE,
                NULL, 0);
}
```

1. Установить WDK (например, на диск D)
2. Создать каталог MyNativeApps в
D:\WinDDK\7600.16385.1\
D:\WinDDK\7600.16385.1\
3. Скопировать в него каталог с исходниками dumpMbr
4. Запустить x86 Checked Build Environment
5. Cd MyNativeApps\dumpMbr
6. Build

Структура каталога

```
D:\WinDDK\7600.16385.1\MyNativeApps\dumpMbr
```

W	Name
..	
install	
objchk_wxp_x86	
buildchk_wxp_x86	log
sources	
dumpmbr	c
Makefile	

В случае успешной сборки:

```
D:\WinDDK\7600.16385.1\MyNativeApps\dumpMbr\objchk_wxp_x86\i386
```

W	Name
..	
dumpmbr	exe
dumpmbr	pdb
dumpmbr	obj
vc90	pdb
_objects	mac

В случае успешной сборки:

cmd Windows XP x86 Checked Build Environment

```
D:\WinDDK\7600.16385.1\MyNativeApps\dumpMbr>build
path contains nonexistant c:\program files (x86)\ati technologies\ati.ace\core-static, removing
path contains nonexistant c:\windows\system32\config\systemprofile\.dnx\bin, removing
path contains nonexistant c:\windows\system32\openssh, removing
BUILD: Compile and Link for x86
BUILD: Loading d:\winddk\7600.16385.1\build.dat...
BUILD: Computing Include file dependencies:
BUILD: Start time: Sat Apr 27 06:18:16 2019
BUILD: Examining d:\winddk\7600.16385.1\mynativeapps\dumpmbr directory for files to compile.
      d:\winddk\7600.16385.1\mynativeapps\dumpmbr Invalidating OACR warning log for 'WDKSamples:x86chk'
BUILD: Saving d:\winddk\7600.16385.1\build.dat...
BUILD: Compiling and Linking d:\winddk\7600.16385.1\mynativeapps\dumpmbr directory
Configuring OACR for 'WDKSamples:x86chk' - <OACR on>
_NT_TARGET_VERSION SET TO WINXP
Compiling - dumpmbr.c
Linking Executable - objchk_wxp_x86\i386\dumpmbr.exe
BUILD: Finish time: Sat Apr 27 06:18:17 2019
BUILD: Done
```

```
3 files compiled - 3 Warnings
1 executable built
```

D:\WinDDK\7600.16385.1\MyNativeApps\dumpMbr>

D:\WinDDK\7600.16385.1\MyNativeApps\dumpMbr\objchk_wxp_x86\i386

W	Name	
..		
dumpmbr		exe
dumpmbr		pdb
dumpmbr		obj
vc90		pdb
_objects		mac

Для запуска Nativeприложения нужно его скопировать в system32 и прописать в реестре

```
HKLM\System\CurrentControlSet\Control\Session  
Manager\BootExecute
```

После строки «Autocheck Autochk *»

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager]  
"BootExecute"=hex(7):61,75,74,6f,63,68,65,63,6b,20,61,75,74,6f,63,68,6b,20,2a,  
\00,64,75,6d,70,6d,62,72,00,00
```

Recipe	Input
<p>From Charcode</p> <p>Delimiter Comma</p> <p>Base 16</p>	<p>61,75,74,6f,63,68,65,63,6b,20,61,75,74,6f,63,68,6b,20,2a</p> <p>Output</p> <p>autocheck autochk *</p>

```
Hiew: mbr.bin
<1> Hiew: mbr.bin
C:\mbr.bin
00000000: 33 C0 8E D0-BC 00 7C 8E-C0 8E D8 BE-00 7C BF 00 3  LÄU |Ä LÄU |  |
00000010: 06 B9 00 02-FC F3 A4 50-68 1C 06 CB-FB B9 04 00  |  |  |  |  |  |  |  |
00000020: BD BE 07 80-7E 00 00 7C-0B 0F 85 0E-01 83 C5 10  |  |  |  |  |  |  |  |
00000030: E2 F1 CD 18-88 56 00 55-C6 46 11 05-C6 46 10 00  |  |  |  |  |  |  |  |
00000040: B4 41 BB AA-55 CD 13 5D-72 0F 81 FB-55 AA 75 09  |  |  |  |  |  |  |  |
00000050: F7 C1 01 00-74 03 FE 46-10 66 60 80-7E 10 00 74  |  |  |  |  |  |  |  |
00000060: 26 66 68 00-00 00 00 66-FF 76 08 68-00 00 68 00  |  |  |  |  |  |  |  |
00000070: 7C 68 01 00-68 10 00 B4-42 8A 56 00-8B F4 CD 13  |  |  |  |  |  |  |  |
00000080: 05 82 C4 10-05 5B 14 B8-01 02 B8 00-7C 8A 56 00  |  |  |  |  |  |  |  |
00000160: 24 02 C3 49-6E 76 61 6C-69 64 20 70-61 72 74 69  |  |  |  |  |  |  |  |
00000170: 74 69 6F 6E-20 74 61 62-6C 65 00 45-72 72 6F 72  |  |  |  |  |  |  |  |
00000180: 20 6C 6F 61-64 69 6E 67-20 6F 70 65-72 61 74 69  |  |  |  |  |  |  |  |
00000190: 6E 67 20 73-79 73 74 65-6D 00 4D 69-73 73 69 6E  |  |  |  |  |  |  |  |
000001A0: 67 20 6F 70-65 72 61 74-69 6E 67 20-73 79 73 74  |  |  |  |  |  |  |  |
000001B0: 65 6D 00 00-00 63 7B 9A-2D 66 1F 38-01 01 80 20  |  |  |  |  |  |  |  |
000001C0: 21 00 07 FE-FF FF 00 08-00 00 00 F0-BF 03 00 00  |  |  |  |  |  |  |  |
000001D0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00  |  |  |  |  |  |  |  |
000001E0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00  |  |  |  |  |  |  |  |
000001F0: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 55 AA  |  |  |  |  |  |  |  |
```

```
+ Open PhysicalDrive0 STATUS_SUCCESS
+ Read MBR OK!
+ Open C:\mbr.bin STATUS_SUCCESS!
+ Dump MBR OK!
Dump Created!
```

```
Invalid partition table Error
loading operating system Missing operating system
c:\Ü-f▼800Ç
! ■ □ ≡▼
```

ДЗ

Собрать **DumpMBR** из
ИСХОДНИКОВ

Вопросы???





Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!

