



Index

@ character, 53, 55
= (“equals”), 313
/ (slash), 252
_ (underscore), 53, 55

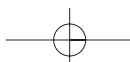
A

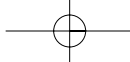
+a switch, 248-249
Address, 171
 base, 362-363, 367-372, 378
 computation, 71, 82-83
 driver load, 8
 exported names, 357-363
 FS, 173, 245-248
 indirect, 250
 linear, 171-177, 187-190, 278, 372
 load, 83
 logical, 171-174
 OMAP conversion, 84-92
 physical, 171-172, 176-178, 226-227, 278
 relative, 248-250
 TEB, 244
 virtual, 171-172
 See also Memory management
Advanced Server, 168
Alias, 115, 533-569
_allmu1 symbol, 95
Allocation bit array, 74, 77
ANSI character, 30
 CHAR type, 115

imagehlp.dll, 48
object tags, 428
PSTR and PWSTR types, 116
strings, 117-118, 399-401
w2k_img.dll, 60
API call. *See* Kernel API call; Native API call
Application descriptor, 192
Argument stack, 294-296, 310, 350-352, 391
Array
 allocation, 74, 77
 export, 361-362, 372
Asche, Ruediger R., 129
Assembly language (ASM), 25, 294-296,
 303, 309
At character (@), 53, 55

B

+b switch, 272, 275
Bad pointer, 351
Bang command, 11, 13-14, 434
Base address, 362-363, 367-372, 378
Bit array, 74, 77
Bit field, 178-179
Bit mask, 189, 192
Blink, 250
Block, memory, 232-236, 398
“Blue Screen Of Death” (BSOD), 2
Booth, Rick, 171
Branch prediction, 85

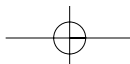


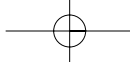


- Brown, R., 145
- Buffer
 - circular, 333
 - protocol, 336-339
 - size, 161, 164
 - string, 399-400
- Buffered I/O, 203, 207
- Bug, 12, 357, 382, 388
- “Bugslayer”, 85
- Build number, 285
- BYTE, 15

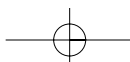
- C**
- C bit field, 178-179
- C language, 294, 296
- C runtime library, 110-111, 508-512
- C source file, 130
- Call interface function, 386-390
- Callback function, 46-47
- Category, object, 414-416
- CD contents
 - driver wizard, 129-134
 - hook viewer, 338
 - PDB stream reader, 81
 - service and driver browser, 164
 - SpySearch, 308
 - Utility Library, 149
 - w2k_call.c, 457
 - w2k_call.dll, 382
 - w2k_cv.exe, 60
 - w2k_dbg.dll, 30-34
 - w2k_def.h, 122-123, 413-414
 - w2k_dump.exe, 73
 - w2k_img.dll, 60, 71, 86-87
 - w2k_load.exe, 158
 - w2k_mem.exe, 238
 - w2k_obj.exe, 452
 - w2k_spy.h & w2k_spy.c, 297, 316
 - w2k_spy.sys, 195
 - w2k_sym.exe, 30
- _cdecl, 53, 295
 - internal symbols, 402
 - kernel-mode gate, 351, 355
- CHAR type, 115
- Charge, resource, 422-424
- Checkpoint file, 53
- Circular buffer, 333
- CLIENT_ID, 121
- Cloning, object, 455-458
- Code, IOCTL, 197
- CodeView, 60, 65-71
 - .dbg files, 72
 - .pdb files, 72
 - directories, 63, 67-68
- Cogswell, Bryce, 281-285, 293-294, 347
- CommandParse, 262
- Common Object File Format (COFF), 65
- Compound file, 74-75
- Configuration, kernel-mode driver, 132
- Constant, 527-531
 - Intel i386, 189-193
- Context
 - device, 142
 - thread/process, 443
- Control code, 146
- Control register, 227
- Copying memory blocks, 398
- CPU register, 351-352
- Crash dump, 2-8
- CreateFile, 261-262, 344
- Custer, H., 97, 432
- CV_PUBSYM, 69-71
- CV_SYMHASH, 69-71

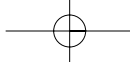
- D**
- Data access function, 398-401
- Data structure, 119-121, 533-569
 - Intel i386, 178-189
 - I/O system, 415-416
- Data type
 - integral, 114-116,
 - strings, 116-118
 - structures, 119-121
- Data-copying interface function, 390-393
- db command, 15
 - .dbg file, 57-64
 - header, 57-60
 - linkage, 72-73
 - OMAP, 63, 84
 - dbghelp.dll, 25-30
 - \DBG.HTM file, 9
 - dbgSymbolLoad, 48
- dd command, 15



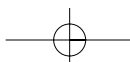


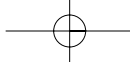
- Debugging, 1-95
 - crash dump, 2-8
 - i386kd.exe, 2
 - MFVDasm, 22-23
 - PEview, 24-25
 - postmortem, 2
 - support library, 30-34
 - WinDbg.exe, 2
 - See also* Interface, debugging; Kernel Debugger; Symbol file
 - Decoration, symbol, 53-56, 87, 95
 - .def file, 130, 132
 - Demand paging, 168-178
 - memory dump utility, 254-256
 - X86 data structures, 182-187
 - Descriptor
 - application, 192
 - system, 192-193
 - Descriptor Privilege Level (DPL), 265
 - Device context, 142
 - Device Driver Kit (DDK), 1, 98, 115
 - constants, 190
 - header files, 122-123, 126, 128, 204
 - kernel-mode drivers, 126-129
 - w2k_def.h, 413-414
 - Device I/O Control (IOCTL). *See* IOCTL
 - Directory
 - debug, 62-63
 - handle, 320
 - lock, 453
 - stream, 77-81
 - Dispatch ID
 - interrupt handler, 102, 107
 - Win32K, 108-110
 - Dispatcher
 - driver, 142-144
 - object, 414-416, 527
 - service, 99-102
 - spy, 197
 - DLL, 357-358, 381-384
 - DOS, 145
 - \DosDevices, 195
 - Driver
 - EnumDeviceDrivers, 34-37
 - exception, 194
 - w2k_kill.sys, 6-8
 - See also* Kernel-mode driver; Spy device
 - Driver skeleton, 135-144
 - !drivers, 18-20
 - .dsp file, 132
 - .dsw file, 129
 - Dump command, 15
 - See also* Memory dump utility
 - Dump Memory, 15
 - dw command, 15
 - DWORD, 15, 46
- ## E
- Entry point, driver, 139, 145
 - EnumDeviceDrivers, 34-37
 - Enumeration, 532-533
 - EnumProcesses, 38-40
 - EnumServicesStatus, 160-161, 164
 - Environment variable, 158
 - EPROCESS, 16-18, 434, 438-440, 438-442
 - “Equals” character (=), 313
 - ERESOURCE, 453
 - Error
 - bad arguments, 357
 - crash dump, 12
 - kernel API calls, 388
 - last-error code, 382
 - ETHREAD, 18-19, 434, 438-442, 446
 - ExAcquireResourceExclusive, 453
 - Examine Symbols, 15-16
 - Exception, 194
 - SEH, 316, 351, 356-357
 - Execute, 262, 344
 - Exported symbol
 - API thunks, 394
 - assigning, 353, 358-363
 - resolving, 369-373
 - SPY_IO_PE_EXPORT, 378
 - SPY_IO_PE_SYMBOL, 380
 - Extended kernel call interface, 402-412
 - Extended runtime library, 111-114, 513-525
 - Extension, debugger, 11, 13-14
- ## F
- +f switch, 245
 - _fastcall, 53, 55
 - ASM, 295
 - internal symbols, 402
 - kernel-mode gate, 351-352, 355



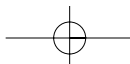


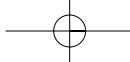
- File system, 74-75
 - Filter, garbage, 316-320, 332-333
 - Flag
 - file object, 419, 528
 - fOk, 215
 - object attribute, 531
 - object header, 530
 - Flat memory model, 172
 - Flink, 250
 - Floating point emulator, 111-113
 - fOk flag, 215
 - Format control ID, 307-309, 312, 320
 - Format string, 307-309, 312, 320
 - FS:[<base>]:addressing, 246-248
 - FS-relative addressing, 173, 245
 - Function
 - callback, 46-47
 - categories, 113-114
 - IOCTL, 205, 210-237, 257-259, 324-338
 - kernel API, 481-525
 - names, 156
 - wrapper, 149, 157, 257-259
 - Function set
 - imgTable*, 86-91
 - Nt* & Zw*, 97-98, 101, 364-365
- G**
- +g option, 266
 - Garbage filter, 316-320, 332-333
 - Gate
 - descriptor, 269-270
 - interrupt, 271-272
 - kernel-mode, 350-357
 - See also* Interrupt handler
 - GetModuleHandle, 358
 - GetProcAddress, 358
 - Gircys, G. R., 65
 - Global Descriptor Table (GDT), 174, 218, 221
 - selectors, 266-269
 - Graphics Device Interface (GDI), 108
 - kernel API functions, 489-509
- H**
- +h switch, 248
 - HalMakeBeep, 395
 - HalQueryRealTimeClock, 395-397
 - Handle, 317
 - API hook protocol, 316-324
 - directory, 320
 - handle count, 313-314
 - object, 248, 429-434
 - process, 40-43, 46
 - registered/unregistered, 317-320
 - Service Control, 148-149, 156-158
 - spy device, 259-262
 - Handle database, 421-422
 - HANDLE_TABLE, 429-431
 - Hardware, accessing, 6
 - Hardware Abstraction Layer (HAL), 395
 - Hash table, 454
 - Header file
 - .dbg, 57-60
 - DDK, 122-123, 126, 128, 204
 - DrvInfo.h, 141
 - ntddk.h/ntdef.h, 98
 - ntdll.lib, 122-123
 - object, 417-420
 - TestDrv.h, 135
 - w2k_spy.h, 195, 261, 297, 316
 - Hex dump viewer, 73
 - HMODULE, 40-42, 46
 - Hook, API
 - dispatcher, 296-311
 - handles, 316-324
 - management functions, 324-338
 - protocol, 311-316
 - reader, 338-348
 - system-wide, 282, 293-294
 - Hummel, Robert L., 113, 168, 193
- I**
- Icon file, 130
 - imagehlp.dll, 25-30
 - symbols, 45
 - undecoration, 54-55
 - ImageLoad, 47-48
 - IMG_DBG, 60
 - IMG_PUBSYM, 82
 - imgTable* function set, 86-91
 - Import library, 122-123
 - DDK, 126-128
 - Import thunk, 53-54, 95
 - Incremental updating, 80-81





- Index
 - object type, 428-429, 530
 - page-directory, 187
 - Indirect addressing, 250
 - Inline assembler, 294
 - Inner Loops*, 171
 - Input buffer, 203, 207
 - Inside Windows 2000*, 97
 - Inside Windows NT*, 6, 97
 - INT 2Eh service handler. *See* Interrupt handler
 - Integral data type, 114-116
 - Intel i386 memory management, 167-189
 - data structures, 178-189
 - 80286 CPU, 169
 - 80386 CPU, 112, 167-170
 - 80486 CPU, 170
 - layout, 168
 - macros/constants, 189-193
 - segmentation/demand paging, 168-178
 - Interface
 - GDI, 108
 - interface functions, 386-393
 - kernel API calls, 349-357, 402-412
 - Native API, 122-123
 - spy device, 257-262
 - Win32K kernel-mode, 108-110
 - Interface, debugging, 25-53
 - dbghelp.dll, 25-30
 - EnumDeviceDrivers, 34-37
 - EnumProcesses, 38-40
 - EnumProcessModules, 40-43
 - imagehlp.dll, 25-30, 45
 - process privileges, 43-45
 - psapi.dll, 25-30
 - Interrupt Descriptor Table (IDT), 100, 174, 266
 - gate descriptors, 269-270
 - SPY_IO_INTERRUPT, 222, 225
 - X86_GATE, 179-180
 - Interrupt handler, 100-102, 222
 - gates, 271-272
 - KiSystemService, 107, 282-284
 - Zw* functions, 364
 - I/O object, 415-416
 - I/O Request Packet (IRP), 142, 529
 - IOCTL, 145-146
 - code, 197
 - handler, 197, 203
 - hook management functions, 324-338
 - kernel API calls, 349-352, 373-386
 - spy device functions, 205, 210-237
 - spy device handle, 259-262
 - type codes, 529
 - wrapper functions, 257-259
 - IRP handler array, 142
 - i386kd.exe, 2, 11
- ## K
- +k switch, 246
 - Kernel API call, 349-411
 - calling conventions, 351
 - data access functions, 398-401
 - DLL encapsulation, 381-384
 - exported symbols, 357-363
 - interface functions, 386-393
 - internal symbols, 402-412
 - IOCTL, 349-352, 373-386
 - resolving symbols, 369-373, 380
 - retrieving module addresses, 364-369
 - SEH, 356-357
 - SpyCall, 352-356
 - thunks, 393-398
 - Kernel API functions, 481-525
 - Kernel Debugger, 2
 - commands, 11-22, 467-479
 - ln command, 16, 104-106
 - process and thread objects, 434, 446
 - setup, 11
 - symbol decoration, 54-55
 - Kernel-mode driver, 125-166
 - configuration, 132
 - enumerating services and drivers, 160-166
 - I/O control, 145-146
 - kernel API call, 350
 - management function, 149-160
 - Native API hooks, 293
 - nonexported structures, 452
 - ntoskrnl.exe, 99
 - privilege level, 194
 - SC Manager, 148-149
 - skeleton, 135-144
 - system crash, 6-8
 - wizard, 129-134
 - Kernel-mode interface, Win32, 108-110, 125-126

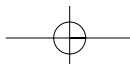


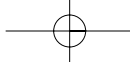


- Kernel's Processor Control Block (KPCB), 214, 443-444
- Kernel's Processor Control Region (KPCR), 214, 245, 444
- kernel32.dll, 97
- KeServiceDescriptorTable, 282-284, 394
- Keyboard poll, 345
- Killer device, 6-8, 146-147
- Kill.exe, 44
- KiSystemService, 107, 282-284
- KMUTEX, 453
- KPROCESS, 434-435, 434-437
- KTHREAD, 434-437, 446
- Kyle, J., 145

- L**
- LARGE_INTEGER, 172
- Least-recently-used (LRU) schedule, 170
- Library
 - C runtime, 110-111
 - DDK, 126-128
 - extended, 111-114, 513-525
 - ntdll.lib, 122-123
 - w2k_img.dll, 60, 71
- Linear address, 171-177, 187-190, 278, 372
- Linked list, 120
- List Nearest Symbols, 16
- LIST_ENTRY, 120
- In command, 16, 104-106
- Load address, 83
- Loading modules, 252-254
- LoadLibrary, 358
- Local Descriptor Table (LDT), 174, 218-221
- Lock
 - global, 452-453
 - handle table, 433
- Log file, 312
- Logical address, 171-174
- LONGLONG, 172

- M**
- Macro
 - Intel i386, 189-193
 - SpyHook, 297-305
- Macro Assembler (MASM), 25, 115, 294, 296
- Manager handle, 148-149, 157-158
- Map, memory, 277-279
- Mask, bit, 189, 192
- Mason, W. Anthony, 365
- Memory dump utility, 238-257
 - command options, 238-243, 256, 263-264
 - demand paging, 254-256
 - FS addressing, 245-248
 - handle/object resolution, 248
 - indirect addressing, 250
 - loading modules, 252-254
 - relative addressing, 248-250
 - TEB-relative addressing, 244
- Memory management, 167-279
 - descriptors, 264-272
 - dump commands, 15
 - Intel i386, 167-189
 - memory areas, 272-277
 - memory blocks, 232-236, 398
 - memory layout, 168
 - memory map, 277-279
 - selectors, 21-22
 - spy driver, 195-210
 - spy functions, 210-237
 - spy interface, 257-262
 - system information, 263-264
 - See also* Address
- Memory segmentation, 194, 264-272
 - Intel i386, 168-178
 - segment registers, 168-169, 216, 264-266
 - SPY_IO_SEGMENT, 215-221
- Microsoft Developer Network (MSDN) Library, 98
- MmGetPhysicalAddress, 178, 190, 226-227, 393-394
- MmIsAddressValid, 178, 190, 235, 393-394
- Module
 - handle, 40-43
 - loading, 252-254
 - relationships, 99
- Most recently used (MRU) algorithm, 424
- Multi-Format Visual Disassembler (MFVDasm), 22-23, 134
- Multithreaded environment, 310, 384
- Mutex, 206, 453





N

Name
 exported, 357-363
 object, 421, 428
 pattern, 347

Native API, 97-123
 data types, 114-118
 dispatch IDs, 108-110
 function handler, 310-311
 function sets, 97-98, 101, 364-365
 INT 2Eh handler, 107
 interfacing to, 122-123
 monitoring calls, 281
 nesting level, 310-311
 runtime library, 110-114
 SDTs, 102-106, 281-324
 service dispatcher, 99-102
 undocumentedness, 98-99
 Win32 kernel-mode interface, 108-110
 See also Spy device

Native API call, 281-348
 garbage filter, 316-320
 hook dispatcher, 296-311
 hook management functions, 324-338
 hook protocol, 311-316
 INT 2Eh handler, 282
 SDTs, 282-293

NB09 format, 65-66
NB10 format, 72

Nebbett, Gary, 36, 110, 123, 419-420, 433

Nesting level, 310-311

NT. *See* Windows NT

Nt* function set, 97-98, 101, 364-365

NT Insider, The, 12, 14

NtBuildNumber, 394

ntdll.dll library, 99-101, 110-114, 122-123

ntoskrnl.exe, 99-102, 110-114
 exported variables, 211
 handle tables, 433
 memory management, 178

NTPROC, 104

NtQuerySystemInformation, 35-36,
 39-40, 114
 address computation, 83
 handle tables, 433
 kernel API calls, 364-366
 strings, 117

NULL pointer, 6

O

ObCreateObject, 442

Object, 413-464
 body structure, 428-429
 categories, 414-416
 charges and quotas, 422-424
 creator information, 420-421
 directory, 424-425
 dispatcher, 414-416
 file flags, 528
 handle database, 421-422
 handle tables, 429-434
 header, 417-420
 I/O, 415-416
 mutex, 206
 name, 421, 428
 process/thread, 434-443
 type, 419, 425-429

Object browser, 452-464
 cloning structures and functions,
 455-458
 command help, 462
 global lock, 452-453
 object manager thunks, 452-453

Object Module Format (OMF), 65, 69

OBJECT_ATTRIBUTES, 119

OBJECT_CREATOR_INFO, 420

OBJECT_DIRECTORY, 424-425

OBJECT_HANDLE_DB, 422

OBJECT_NAME, 421

OBJECT_QUOTA_CHARGES, 423

OBJECT_TYPE, 425-427

ObReferenceObjectByHandle, 236-237

Offset
 .dbg files, 59-63
 export section, 378
 memory dump utility, 248-250
 object headers, 419, 421
 OMAP, 85-86

OMAP address conversion, 84-92
 .dbg files, 63, 84

Open Systems Resources (OSR), 2

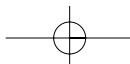
OpenProcess, 43

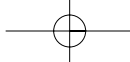
Optimization, 170-171

Ordinal number array, 372

Output buffer, 203, 207

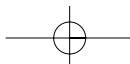
Overflow, 337-338

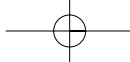




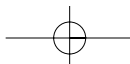
P

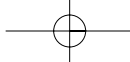
- +p switch, 250
 - Page entry, 183, 230-232
 - Page-Directory Base Register (PDBR), 175-176, 182, 230
 - Page-directory entry (PDE), 175-178, 183, 190
 - SPY_IO_PDE_ARRAY, 229-230
 - Page-directory index (PDI), 187, 189
 - Page-frame number (PFN), 175, 178, 182-183
 - Page-level write-through (PWT), 183
 - Page-not-present entry (PNPE), 183
 - Page-table entry (PTE), 175-178, 183, 189-190
 - Page-table index (PTI), 187, 189
 - Paging
 - charges and quotas, 423
 - crash dump, 3, 7
 - demand, 168-178, 182-187, 254-256
 - page fault, 170
 - swapping to pagefiles, 254-256
 - PASCAL string, 69
 - Pattern
 - name, 347
 - string, 345
 - Pcb, 434
 - .pdb file, 56, 72-82
 - header, 75-77
 - linkage, 72-73
 - stream directory, 77-81
 - PDB_PUBSYM, 81
 - Pentium CPU, 167-171
 - PEview, 22, 24-25, 134
 - Physical address, 171-172, 176-178, 278
 - Physical Address Extension (PAE), 168, 172, 226-227
 - Pietrek, Matt, 45, 57, 65, 72, 84, 281
 - Pointer
 - bad, 351
 - invalid, 316
 - KTHREAD/ETHREAD, 446-447
 - NULL, 6
 - object, 414
 - table, 284-285
 - Portable Executable (PE) file, 24-26, 353
 - directory IDs, 528
 - exported names, 357-363, 370-372
 - Postmortem debugging, 2
 - ppbFormats, 306
 - ppbSymbols, 306-308
 - pProcessorControlRegion, 214
 - #pragma directive, 144
 - Privilege level, 43-45
 - DPL, 265
 - kernel-mode drivers, 145, 227
 - memory segmentation, 194
 - module relationships, 99
 - Process
 - context, 443-447
 - handle, 40-43, 46
 - ID, 38-39, 43, 121, 421
 - module, 40-43
 - object, 434-443
 - Process Environment Block (PEB), 43, 447-451
 - !processfields, 16-18, 98, 434
 - Program Database (PDB) file. *See* .pdb file
 - Project template, 129
 - Protected Virtual Address Mode, 169
 - Protocol, API hook, 311-316
 - buffer, 336-339
 - entry format, 312-313
 - filter, 316-320, 332-333
 - reader, 338-348
 - Proxy, 393
 - psapi.dll, 25-31, 36
 - Pseudo handle, 46
 - PSTR type, 116
 - PTSTR type, 46
 - PWSTR type, 116
- ## Q
- q command, 22
 - Quota, resource, 422-424
- ## R
- Radburn, Wayne J., 22, 25
 - .rc file, 130
 - Read access right, 345
 - Real-Address Mode, 169
 - Registry key, 131
 - Relative addressing, 248-250
 - Requested Privilege Level (RPL), 179
 - Resource script, 144



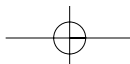


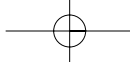
- Richter, Jeffrey, 281
 - Robbins, John, 85
 - Root stream, 77
 - RtlImageNtHeader, 358-359, 377
 - Runtime library, 110-114
 - Runtime linkage, 357
 - Russinovich, Mark, 97, 123, 281-285, 293-294, 347
- S**
- +s switch, 248-249
 - Security, system, 193-194, 398
 - Segmentation, memory. *See* Memory segmentation
 - Seigné, Jean-Louis, 22, 23
 - !sel, 21-22
 - Selector, 169, 179, 192
 - GDT, 266-269
 - spy device functions, 215-221
 - Service, 148
 - enumerating, 160-166
 - loading/unloading, 157-158
 - Service Control (SC) Manager, 148-149
 - Service Descriptor Table (SDT), 102-107, 169, 281-324
 - handles, 316-324
 - hook dispatcher, 296-311
 - hook protocol, 311-316
 - SpyHookExchange, 329-330
 - Windows 2000 vs. NT, 286-293
 - Service dispatcher, 99-102
 - Service handle, 148-149, 156-158
 - SharedUserData, 214, 285
 - Slash character (/), 252
 - Software Development Kit (SDK), 98
 - aliases, 115
 - header files, 122-123
 - Solomon, D. A., 6, 97, 432
 - Source file, C, 130
 - Spy device, 195-210
 - dump utility, 238-257
 - header files, 195, 204, 261
 - hook dispatcher, 296-311
 - hook management functions, 324-338
 - hook protocol, 311-316
 - interface, 257-262
 - internal symbols, 402
 - IOCTL functions, 205, 210-237, 257-259, 324-338
 - IOCTL handler, 197, 203
 - kernel API calls, 373-380
 - protocol reader, 338-348
 - SPY_CALL_INPUT, 351-352
 - SPY_CALL_OUTPUT, 351
 - SPY_IO_CALL, 380, 386
 - SPY_IO_CPU_INFO, 227-229, 245
 - SPY_IO_HANDLE_INFO, 236-237
 - SPY_IO_HOOK_FILTER, 332-333
 - SPY_IO_HOOK_INFO, 327-328
 - SPY_IO_HOOK_INSTALL, 328-330
 - SPY_IO_HOOK_PAUSE, 332
 - SPY_IO_HOOK_READ, 333-336
 - SPY_IO_HOOK_REMOVE, 330-332
 - SPY_IO_HOOK_RESET, 333
 - SPY_IO_HOOK_WRITE, 336-339
 - SPY_IO_MEMORY_BLOCK, 236, 398
 - SPY_IO_MEMORY_DATA, 232-236
 - SPY_IO_MODULE_INFO, 376-377
 - SPY_IO_OS_INFO, 211-214, 263
 - SPY_IO_PAGE_ENTRY, 230-232, 272
 - SPY_IO_PDE_ARRAY, 229-230
 - SPY_IO_PE_EXPORT, 378-379
 - SPY_IO_PE_HEADER, 377-378
 - SPY_IO_PE_SYMBOL, 380, 393
 - SPY_IO_PHYSICAL, 226-227
 - SPY_IO_SEGMENT, 215-221
 - SPY_IO_VERSION_INFO, 210
 - SpyCall, 352-356, 388
 - SpyHook macro, 297-305
 - SpyHookInitialize, 297-298
 - Stack frame, 295-296
 - _stdcall, 53, 55
 - ASM, 295
 - internal symbols, 402
 - kernel API calls, 388
 - kernel-mode gate, 351, 355
 - Stream directory, 77-81
 - String, 116-118
 - ANSI/Unicode, 117-118, 141
 - format, 307-309, 312, 320
 - kernel, 399-401
 - PASCAL, 69
 - pattern, 345
 - substitution, 130
 - zero-terminated, 316





- Structure, 119-121, 533-569
 - Intel i386, 178-189
 - I/O system, 415-416
 - Structured Exception Handling (SEH), 316, 351, 356-357
 - Symbol browser
 - w2k_sym.exe, 30, 51-53
 - w2k_sym2.exe, 93-95
 - Symbol file, 8-11, 53-95
 - address computation, 71, 82-83
 - CodeView, 65-71
 - .dbg, 57-64
 - decoration, 53-56, 87, 95
 - internal symbols, 402-412, 452
 - ln command, 16
 - OMAP, 84-92
 - path setup, 10-11
 - .pdb, 72-82
 - symbol table management functions, 86-87, 91-92, 407
 - See also* Exported symbol
 - SymEnumerateSymbols, 45-51
 - Synchronization object, 433
 - System crash, 6-8
 - System descriptor, 192-193
 - System Service Table (SST), 102, 107
- T**
- +t switch, 244
 - Table Indicator (TI), 218
 - Tag, object, 428, 531
 - Tagged record, 65
 - Task gate, 271-272
 - Task Register (TR), 227
 - Task-State Segment (TSS), 222-225, 264-265
 - TBYTE type, 115
 - Tcb, 434
 - .td file, 130, 132
 - TEB-relative addressing, 244
 - Template file, 129-131
 - TestDrv.c file, 135
 - Thread
 - context, 443-447
 - ID, 121, 311
 - initialization, 107
 - object, 434-443
 - Thread Environment Block (TEB), 244, 447-451
 - !threadfields, 18, 98, 434
 - Thunk, 53-54, 95
 - API, 393-398
 - function, 410-411
 - object manager, 452-453
 - .ti file, 130
 - Token handle, 44
 - Tomlinson, Paula, 148
 - .tp file, 129
 - Translation Lookaside Buffer (TLB), 176
 - Trap
 - gate, 271-272
 - handler, 222
 - .tw file, 129
 - Type ID, 415
 - Type object, 419, 425-429
- U**
- u becc3000 command, 12
 - +u switch, 246
 - Unassemble Machine Code, 14-15
 - Undecoration algorithm, 55
 - “Under the Hood”, 57, 84
 - Underscore (_), 53, 55
 - “Understanding NT”, 148
 - “Undocumentedness”, 98-99
 - Unicode character, 30
 - imagehlp.dll, 48
 - PSTR and PWSTR types, 116
 - strings, 117-118, 141, 399-401
 - w2k_img.dll, 60
 - WCHAR type, 115
 - zero-terminated strings, 316
 - UniqueProcessId, 421, 446
 - User-mode call, 350, 373
- V**
- Version number, 210
 - Virtual address, 171-172
 - Viscarola, Peter G., 365
 - Visual C/C++
 - ASM, 294
 - data types, 115
 - driver wizard, 129
 - ntdll.dll, 111
 - optimizer, 7, 25
 - .pdb files, 80-81



**W**

WCHAR type, 115
Win32, 97-98, 169
 accessing hardware, 6
 ASM programming, 25
 hooks, 281-282
 kernel-mode interface, 108-110,
 125-126
 and Native API, 99-102
 SDK header file, 57
 w2k_def.h, 412-413
Win64, 30
Window Manager (USER), 108
Windows 3.x, 193
Windows NT, 169
 .dbg files, 57, 65-67
 DDK, 128
 debugging interfaces, 25-26
 4GT RAM Tuning, 168
 handle table, 432
 hooks, 282
 SDT comparison, 284-293
 system security, 193-194
 Win32K, 108
Windows NT/2000 Native API Reference,
 123, 419-420
WORD, 15
Workspace template, 129
Wrapper function, 149
 IOCTL, 257-259
 SC Manager, 157
Write access right, 206, 345
w2kCall, 386-390, 402
w2kCopy, 393
w2k_dbg.dll, 30-34
w2k_def.h, 122-123, 412-413
w2kDirectoryOpen, 453-455
w2kFilePath, 259-261

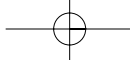
w2k_img.dll, 60, 71, 86-87, 91
w2k_kill.sys, 6-8, 146-147
w2k_mem.exe, 238-240
w2kObjectOpen, 455-456
w2kServiceList, 161, 164
w2kServiceLoad, 158, 259-261
w2kSpyClone, 454
w2kSpyControl, 382
w2kSpyRead, 398
w2k_sym.exe, 25, 30, 51-54
w2k_sym2.exe, 93-95

X

x command, 15-16
+x switch, 252, 254
X86 data structure, 178-189
 X86_DESCRIPTOR, 179, 192-193
 X86_GATE, 179-180
 X86_LINEAR, 187
 X86_OFFSET, 189
 X86_PAGE, 189-190
 X86_PAGES, 190
 X86_PDBR, 182-183
 X86_PDE, 183, 190
 X86_PDI, 189
 X86_PE, 183
 X86_PNPE, 183
 X86_PTE, 183, 190
 X86_PTI, 189
 X86_REGISTER, 179
 X86_SELECTOR, 179, 192
 X86_TABLE, 180

Z

Zbikowski, Mark, 34
Zw* function set, 97-98, 101, 364-365
ZwQuerySystemInformation, 364-366



CD-ROM Warranty

Addison-Wesley warrants the enclosed disc to be free of defects in materials and faulty workmanship under normal use for a period of ninety days after purchase. If a defect is discovered in the disc during this warranty period, a replacement disc can be obtained at no charge by sending the defective disc, postage prepaid, with proof of purchase to:

Editorial Department
Addison-Wesley Professional
Pearson Technology Group
75 Arlington Street, Suite 300
Boston, MA 02116
Email: AWPPro@awl.com

Addison-Wesley makes no warranty or representation, either expressed or implied, with respect to this software, its quality, performance, merchantability, or fitness for a particular purpose. In no event will Addison Wesley, its distributors, or dealers be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use the software. The exclusion of implied warranties is not permitted in some states. Therefore, the above exclusion may not apply to you. This warranty provides you with specific legal rights. There may be other rights that you may have that vary from state to state. The contents of this CD-ROM are intended for personal use only.

More information and updates are available at:
<http://www.awl.com/cseng/titles/0-201-72187-2>

Operating systems: Windows 2000, restricted compatibility to Windows NT 4.0, Windows 9x not supported.
CPU: x86 Pentium 90 and up.
RAM: 64 MB and up.
Compiler/Linker: MS Visual C/C++ 6.0.
Developer packages: MS Platform SDK, MS Device Driver Kit (DDK).
Document viewer: MS Internet Explorer 5.0 and up.

