Contents

Introduction 1
Who Should Read This Book 1
What You Should Know to Use This Book 1
Sample Code 2

Chapter 1: Foundations 3
Windows Architecture Overview 3
Processes 4
Dynamic Link Libraries 6
Virtual Memory 7
Threads 8
General System Architecture 9
Windows Application Development 11
Your First Application 13
Working with Strings 18
Strings in the C/C++ Runtime 22
String Output Parameters 23
Safe String Functions 26
32-bit vs. 64-bit Development 28
Coding Conventions 30
C++ Usage 31
Handling API Errors 31
Defining Custom Error Codes 34
The Windows Version 35
Getting the Windows Version 39
Exercises 40
Summary 41

Chapter 2: Objects and Handles 43

Kernel Objects 43
Running a Single Instance Process 46
Handles 49
Pseudo Handles 58
RAII for Handles 59
Using WIL 61
Creating Objects 63
Object Names 65
Sharing Kernel Objects 68
Sharing by Name 69
Sharing by Handle Duplication 74
Private Object Namespaces 79
Bonus: WIL Wrappers for Private Namespaces 84
Other Objects and Handles 85
User Objects 86
GDI Objects 87
Summary 87

Chapter 3: Processes **89**
Process Basics 89
Processes in Process Explorer 96
Process Creation 100
The main Functions 109
Process Environment Variables 112
Creating Processes 116
Handle Inheritance 129
Process Drive Directories 134
Process (and Thread) Attributes 135
Protected and PPL Processes 144
UWP Processes 146
Minimal and Pico Processes 155
Process Termination 156
Enumerating Processes 158
Using `EnumProcesses` 158
Using the Toolhelp Functions 165
Using the WTS Functions 167
Using the Native API 173
Exercises 176

Summary 177
Chapter 4: Jobs 179
Introduction to Jobs 179
Creating Jobs 181
Nested Jobs 183
Querying Job Information 190
Job Accounting Information 191
Querying for Job Process List 198
Setting Job Limits 200
CPU Rate Limit 207
User Interface Limits 214
Job Notifications 217
Silos 222
Exercises 223
Summary 223
Chapter 5: Threads Basics 225
Introduction 225
Sockets, Cores and Logical Processors 227
Creating and Managing Threads 228
The Primes Counter Application 231
Running Primes Counter 237
Terminating Threads 241
A Thread's Stack 243
A Thread's Name 249
What About the C++ Standard Library? 250
Exercises 250
Summary 251
Chapter 6: Thread Scheduling 253
Priorities 253
Scheduling Basics 260
Single CPU Scheduling 260
The Quantum 266
Processor Groups 269
Multiprocessor Scheduling 270
Affinity 270
CPU Sets vs. Hard Affinity 278

System CPU Sets 279
Revised Scheduling Algorithm 279
Observing Scheduling 280
General Scheduling 281
Hard Affinity 287
CPU Sets 289
Background Mode 296
Priority Boosts 299
Completing I/O Operations 300
Foreground Process 300
GUI Thread Wakeup 301
Starvation Avoidance 301
Other Aspects of Scheduling 301
Suspend and Resume 301
Suspending and Resuming a Process 302
Sleeping and Yielding 303
Summary 304

Chapter 7: Thread Synchronization (Intra-Process) 305
Synchronization Basics 306
Atomic Operations 307
The Simple Increment Application 308
The `Interlocked` Family of Functions 310
Critical Sections 313
Locks and RAII 318
Deadlocks 321
The MD5 Calculator Application 321
Calculating MD5 Hash 324
The Hash Cache 326
Image Loads Notifications 328
Event Parsing 334
Putting it All Together 338
Reader Writer Locks 342
RAII Wrappers 343
MD5 Calculator 2 346
Condition Variables 348
The Queue Demo Application 351
Waiting on Address 361

Synchronization Barriers 362
What About the C++ Standard Library? 366
Exercises 367
Summary 367

Chapter 8: Thread Synchronization (Inter-Process) 369
Dispatcher Objects 369
Succeeding a Wait 372
The Mutex 372
The Mutex Demo Application 375
Abandoned Mutex 381
The Semaphore 382
The Queue Demo Application 384
The Event 388
Working with Events 390
The Waitable Timer 392
Other Wait Functions 400
Waiting in Alertable State 400
Waiting on GUI Threads 400
Waiting for an Idle GUI Thread 402
Signaling and Waiting Atomically 403
Exercises 404
Summary 405

Chapter 9: Thread Pools 407
Why Use a Thread Pool? 408
Thread Pool Work Callbacks 411
The Simple Work Application 412
Controlling a Work Item 417
The MD5 Calculator Application 419
Thread Pool Wait Callbacks 421
Thread Pool Timer Callbacks 424
The Simple Timer Sample 426
Thread Pool I/O Callbacks 427
Thread Pool Instance Operations 427
The Callback Environment 429
Private Thread Pools 431
Cleanup Groups 433

Exercises 435
Summary 435
Chapter 10: Advanced Threading 437
Thread Local Storage 437
Dynamic TLS 439
Static TLS 444
Remote Threads 446
The *Breakin* Application 448
Thread Enumeration 450
The *thlist* Application 451
Caches and Cache Lines 455
Wait Chain Traversal 464
The Deadlock Detector Application 469
Asynchronous WCT Sessions 475
User Mode Scheduling 475
Init Once Initialization 478
Debugging Multithreaded Applications 479
Breakpoints 480
Parallel Stacks 481
Parallel Watch 482
Thread Names 483
Exercises 483
Summary 483
Chapter 11: File and Device I/O 485
The I/O System 486
The `CreateFile` Function 487
Working with Symbolic Links 495
Path Length 501
Directories 502
Files 503
Setting File Information 508
Synchronous I/O 509
Asynchronous I/O 513
`ReadFileEx` and `WriteFileEx` 518
Manually Queued APC 519
I/O Completion Ports 520

The *Bulk Copy* Application 525
Using the Thread Pool for I/O Completion 535
The *Bulk Copy 2* Application 537
I/O Cancellation 541
Devices 542
Pipes and Mailslots 552
Pipes 553
Transactional NTFS 558
File Search and Enumeration 561
NTFS Streams 563
Summary 567

Chapter 12: Memory Management Fundamentals 569
Basic Concepts 569
Process Address Space 571
Page States 572
Address Space Layout 573
32-bit Systems 576
64-bit Systems 578
Address Space Usage 580
Memory Counters 584
Process Memory Counters 589
Process Memory Map 595
Page Protection 602
Enumerating Address Space Regions 603
The *Simple VMMap* Application 605
More Address Space Information 609
Sharing Memory 615
Page Files 620
WOW64 623
WOW64 Redirections 626
Virtual Address Translation 627
Summary 629