

Contents

Introduction	i
Who is this series for?	i-1
How to use this book	i-2
Things to know before reading this book	i-2
Abbreviations.....	i-3
Definitions	i-5
What you will need to use this book	i-6
Installing the source code on your computer	i-6
What is on the disc	i-7
Prerequisite to using this book	i-8
What is not discussed in this book	i-8
Final word before we get started	i-8
Part 1	
Chapter 1. The System Core Overview.....	1
The design goal of this book	1-1
Other thing to know and consider.....	1-1
Simplicity of the Design	1-2
Tested devices	1-2
The BIOS	1-3
Real Mode versus Protected Mode	1-4
Wrap up	1-4
Chapter 2. The Boot Process	2
The Power-on Self-Test.....	2-1
The Boot Sector	2-3
The Master Boot Record.....	2-3
Extended partitions.....	2-5
LBA or CHS.....	2-7
Disk limits.....	2-9
MBR Code.....	2-10
Alternative to “Moving out of the way”	2-13
Wrap up	2-14
Chapter 3. Our Enhanced Master Boot Record	3
Full Control of the Drive.....	3-1
Introduction	3-2
The eMBR Partition Header.....	3-3
The eMBR Partiiion	3-6
The boot menu	3-7
Wrap up	3-8

Chapter 4. UEFI GUID Partition Tables.....	4
The GPT Header Block.....	4-2
The GPT Partition Entry.....	4-3
The Attributes field.....	4-4
The CRC fields.....	4-5
The creation of GUID's	4-5
Wrap up	4-5
Chapter 5. Our Booted Partition.....	5
The partition boot process	5-1
The BIOS Disk Extension services.....	5-2
Finding the Loader file	5-5
The Loader file	5-5
Boot Data	5-7
Original INT 1E address and floppy status	5-7
Current Time	5-9
Advanced Power Management.....	5-11
Keyboard Bits.....	5-13
BIOS Equipment Word	5-14
Memory Information.....	5-14
Get System Memory Map	5-15
Get Memory Size for 64+ Meg	5-18
Get Memory Info (Service 88/C0/C7)	5-19
Get CMOS Memory Info	5-22
Get Memory Info Results	5-23
VESA Video Information	5-24
Drive Parameter Block.....	5-29
Wrap Up.....	5-29
Chapter 6. Kernel Descriptors.....	6
Memory Access.....	6-1
Descriptor Table Types.....	6-3
Selectors	6-4
Interrupt Descriptors	6-5
Using Descriptors and Selectors	6-7
Wrap Up.....	6-11
Chapter 7. The A20 Line	7
Nothing is Standard	7-2
Testing the A20 Line.....	7-2
Method 1: Keyboard Controller Method.....	7-3
Method 2: Fast A20, Port 0x92	7-6
Method 3: Keyboard Controller, 0xDF	7-7
Method 4: Brute Force	7-8

Method 5: BIOS Services.....	7-9
Method 6: Port 0xEE	7-10
Wrap Up.....	7-10
Chapter 8. Finish the Loader	8
The System File Header	8-1
Before the Jump to Protected Mode.....	8-2
Read Time Stamp Counter Instruction	8-3
The Move to Protected Mode.....	8-5
Wrap Up.....	8-5
Chapter 9. The Kernel	9
The Memory Manager	9-1
Re-map the PIC.....	9-4
Set the Timer Tick	9-5
Set Our Clock.....	9-6
Set Our Screen Size.....	9-7
Set Our Interrupt Descriptor Table	9-8
Almost There.....	9-9
Our Round Robin Task Scheduler	9-9
Wrap Up.....	9-12
Chapter 10. Putting it All Together	10
Our Emulated Image	10-1
The Master Boot Record.....	10-2
The Extended Master Boot Record	10-2
The Kernel.sys File.....	10-3
The FYSFS File System	10-3
Running Your Code on an Emulator	10-4
Wrap Up.....	10-5
Chapter 11. Where to Go From Here.....	11
How to Use This List.....	11-2
Wrap Up.....	11-4
Part 2	
Chapter 12. The Paging Manager.....	12
Addressing Memory.....	12-1
Linear Addresses.....	12-2
Create a Page Directory and Page Tables	12-3
Finding Free Pages	12-6
Page Availability	12-6
Wrap Up.....	12-6

Chapter 13. The FYSOS Memory Allocator	13
Memory Layout	13-1
The Allocation Process	13-3
The Superblock	13-3
The Array List	13-5
The Allocation Sequence	13-9
Wrap Up	13-12
Chapter 14. The UEFI System BIOS.....	14
Advantages and Disadvantages	14-1
The EFI Overview	14-2
A Type EFI GUID Partitioned System	14-2
Booting Up	14-4
EFI Boot and Runtime Services	14-4
Console Out	14-5
Boot and Runtime Services	14-6
Getting the Video Modes	14-7
Getting the Memory Map	14-10
Reading a File	14-12
Exiting the Boot Services	14-14
Wrap Up.....	14-14
Part 3	
Chapter 15. The Real Time Clock.....	15
Accessing the RTC.....	15-1
The RTC Register Set	15-2
Status Register A	15-3
Status Register B	15-4
Status Register C	15-5
Status Register D	15-6
The Date and Time Registers	15-6
The Century	15-7
The Alarm	15-7
Wrap Up.....	15-7
Chapter 16. The Programmable Interval Timer	16
How the PIT Works	16-1
The PIT's Register Set	16-2
Operating Modes	16-3
Mode 0: Interrupt on Terminal	16-4
Mode 1: Re-triggerable One Shot	16-4
Mode 2: Rate Generator	16-4
Mode 3: Square Wave Generator	16-4

Mode 4: Software Triggered Strobe	16-4
Mode 5: Hardware Triggered Strobe	16-4
Choosing a Mode	16-4
Using the Latch Command (Bits 5:4 = 00b)	16-5
Using the Read-back Command (Bits 7:6 = 11b)	16-5
Initializing a Channel	16-7
Wrap Up.....	16-9
Chapter 17. The Programmable Interrupt Controller.....	17
Interrupt Signals	17-2
Real Mode vs Protected Mode	17-2
Internal Registers	17-4
PIC Initialization	17-5
PIC Operation	17-9
Acknowledging and Interrupt	17-11
Spurious Interrupts	17-12
Interrupt Priority Level	17-12
Wrap Up.....	17-13
Chapter 18. The Multi-Processor Specification	18
The Item Entries	18-3
Processor (LAPIC) Entry	18-4
Bus Entry	18-4
I/O APIC Entry	18-5
Assignment Entries	18-5
Example	18-6
Wrap Up	18-9
Chapter 19. Advanced Configuration and Power Interface	19
Legacy BIOS vs UEFI	19-1
The RSDP.....	19-3
The ACPI Description Tables	19-4
The Root System Description Table (RSDT)	19-6
The Multiple APIC Description Table (MADT)	19-7
Processor Local APIC Entry	19-9
I/O APIC Entry	19-10
Interrupt Source Override Entry	19-10
First Part Wrap Up	19-11
The ACPI's Power Interface	19-12
The ACPI's Six Power States	19-13
Searching the AML Code	19-13
The PM1 Control Registers	19-14
Wrap Up.....	19-15

Chapter 20. The Advanced Programmable Interrupt Controller.....	20
In the Beginning	20-1
Enumeration	20-2
APIC Detection	20-3
The LAPIC's Base Address	20-3
The ACPI Way	20-4
The Multi-processor Specification Way	20-4
The Model Specific Way	20-4
The LAPIC's Address Space	20-5
The LAPIC ID Register	20-7
The LAPIC Version Register	20-7
The Task Priority Register	20-9
The Arbitration and Processor Priority Registers	20-9
The End of Interrupt	20-9
The Logical Destination and Destination Format Registers	20-10
The Spurious Interrupt Vector Register	20-10
The IRR, ISR, and TMR Registers	20-11
The Error Status Register	20-12
The Interrupt Command Register	20-12
The Processor Start-up Procedure	20-13
The Local Vector Table Registers	20-16
The LAPIC's Interrupt Timer	20-17
The I/O APIC.....	20-19
IOAPIC Detection	20-20
The IOAPIC's Base Address	20-20
The IOAPIC Address Space	20-20
The IOAPIC ID Register	20-21
The IOAPIC Version Register	20-22
The IOAPIC Arbitration Register	20-22
The IOAPIC I/O Redirection Table	20-23
Destination Modes	20-24
Wrap Up.....	20-25
Chapter 21. The High Precision Event Timer	21
The HPET Counter	21-1
The HPET Registers	21-4
The HPET General Register Set	21-4
The General Caps and ID Register	21-5
The General Configuration Register	21-6
The General Interrupt Status Register (ISR)	21-6
The Main Counter Register	21-7
The HPET Timer Register Set	21-7
The Config and Caps Register	21-7
Periodic vs One-shot Timers	21-9

The Comparator Register	21-9
Issues When Reading 64-bit Timers	21-10
Initializing a Periodic Timer	21-11
Wrap Up.....	21-12
Appendix A - Disc Contents	A
Contents of the disc/Disc layout.....	A-1
Installing the Source Code on your Computer.....	A-4
Finding the Specification Files	A-5
Appendix B - Included Utilities/Source Code	B
Obtaining a C/C++ Compiler.....	B-1
Obtaining the Newbasic C Compiler	B-1
Obtaining an Assembler	B-1
Obtaining the Flat Assembler.....	B-2
PKSFX(R) FAST! Self Extract Utility Version 2.50.....	B-2
A20 -- Finding the A20 Line technique	B-3
DiskInfo -- Getting the Information from a Hard Disk	B-4
List_MBR -- List the main and extended partitions.....	B-7
Make_Hdr -- Make the FYSOS System File Header.....	B-8
Mem_Info -- Getting the System Memory Information	B-8
MFYSFS -- Make a FYS File System Image	B-9
MGPTPart -- Make a GPT partitioned disk image.....	B-11
Mimage -- Make an empty disk image.....	B-12
MPart -- Create an image full of partitions.....	B-12
MPutImg -- Write a disk image to a floppy disk.....	B-15
MSectCpy -- Copy sectors from one image to another	B-16
RDTSC -- Read Time Stamp Counter demo	B-16
Vid_Info -- Getting the Video Information	B-16
Appendix C - Tables and Figures.....	C
Appendix D - NEC MS-DOS® 3.30 MBR's.....	D
Eight Partition Entries	D-1
Bug in DOS 3.30	D-4
Appendix E - Partition Identification Types	E
Appendix F - Finding the Boot Device.....	F
MBR Disk Signature	F-2
Appendix G - Processor Exceptions/Interrupts.....	G

Appendix H - Trusted Computing	H
Appendix I - Booting CD-ROM's.....	I
Appendix J - Segmented Addressing.....	J
Appendix K - The CPUID Instruction and the MSRs.....	K
Appendix X - For More Information	X
Where to get the CDROM that is included with this book.....	X-1
Where to find more information on this book	X-1
Where to get an erratum if one is needed	X-1
Where to get more examples.....	X-1
Bibliography	Bib