Contents

1 **Forensic Computing** . . . 1

Origin of the Book . . . 2

Structure of the Book . . . 3

References . . . 5

2 **Understanding Information** . . . 7

Binary Systems and Memory . . . 8

Addressing . . . 9

Number Systems . . . 11

Characters . . . 22

Computer Programs . . . 23

Records and Files . . . 23

File Types and Signatures . . . 25

Use of Hexadecimal Listings . . . 25

Word Processing Formats . . . 26

Magic Numbers . . . 29

Graphic Formats . . . 30

Archive formats . . . 35

Other Applications . . . 37

Quick View Plus . . . 38

Exercises . . . 38

References . . . 40

3 **IT Systems Concepts** . . . 41

Two Black Boxes . . . 42

The Worked Example . . . 45

Program, Data, Rules and Objects . . . 53

Software Development . . . 55

Breaking Sequence . . . 57

An Information Processing System . . . 60

Exercises . . . 61

4 **PC Hardware and Inside the Box** . . . 65

The Black Box Model . . . 65

The Buses and the Motherboard . . . 67

Intel Processors and the Design of the PC . . . 74

The Pentium, Pentium Pro, Pentium II and Pentium III . . . 79

A Few Words about Memory 80
Backing Store Devices 83
External Peripherals 85
Expansion Cards 85
References 87

5 **Disk Geometry** 89
A Little Bit of History 89
Five Main Issues 90
Physical Construction of the Unit 90
Formation of Addressable Elements 92
Encoding Methods and Formats for Floppy Disks 93
Construction of Hard Disk Systems 98
Encoding Methods and Formats for Hard Disks 99
The Formatting Process 110
Hard Disk Interfaces 113
IDE/ATA Problems and Workarounds 122
The POST/Boot Sequence 133
The Master Boot Record and Partitions 144
FATs, Directories and File Systems 155
Hiding and Recovering Information 166
RAID 169
Exercises 170
References 171

6 **The Treatment of PCs** 175
The ACPO *Good Practice Guide* 176
Search and Seizure 177
Computer Examination – Initial Steps 185
Imaging and Copying 187
References 195

7 **The Treatment of Electronic Organizers** 197
Electronic Organizers 197
Application of the ACPO *Good Practice Guide* Principles 204
Examination of Organizers and What May Be Possible 206
A Final Word about Electronic Organizers 213
References 213

8 **Looking Ahead (Just a Little Bit)** 215
Bigger and Bigger Disks 216
Networked Systems Add to the Problems 218
Encryption 219
A Final Word 223
References 224

Bibliography 225

Appendices

1 Common Character Codes 233
2 Some Common File Format Signatures 237
3 A Typical Set of POST Codes 241
4 Typical BIOS Beep Codes and Error Messages 245
5 Disk Partition Types 249
6 Extended Partitions 253
7 Registers and Order Code for the Intel 8086 259

Answers to Exercises 267

Glossary 275

Index 289