

Forensic Computing

Tony Sammes and Brian Jenkinson

Forensic Computing

Second edition



Springer

Tony Sammes, BSc, MPhil, PhD, FBCS, CEng, CITP
The Centre for Forensic Computing
DCMT
Cranfield University
Shrivenham, Swindon, UK

Brian Jenkinson, BA, HSc (hon), MSc, FBCS, CITP
Forensic Computing Consultant

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2006927421

ISBN-13: 978-1-84628-397-0 e-ISBN-13: 978-1-84628-732-9
ISBN-10: 1-84628-397-3 e-ISBN 10: 1-84628-732-4
ISBN 1-85233-299-9 1st edition

Printed on acid-free paper

© Springer-Verlag London Limited 2007

First published 2000
Second edition 2007

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers.

The use of registered names, trademarks etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant laws and regulations and therefore free for general use.

The publisher makes no representation, express or implied, with regard to the accuracy of the information contained in this book and cannot accept any legal responsibility or liability for any errors or omissions that may be made.

9 8 7 6 5 4 3 2 1

Springer Science+Business Media
springer.com

Dedication

To Joan and Val

Acknowledgements

The authors would like to thank all the members and former members of the FCG Training Committee for the very valuable contributions that they made to the first edition of this book. In particular, our grateful thanks go to Steve Buddell, Tony Dearsley, Geoff Fellows, Paul Griffiths, Mike Hainey, Dave Honeyball, Peter Lintern, John McConnell, Keith McDonald, Geoff Morrison, Laurie Norton, Kathryn Owen and Stewart Weston-Lewis. For this second edition we would, in addition, like to thank Lindy Sheppard, Dr Tristan Jenkinson and John Hunter for their kind support. Our thanks also go to the students of the 30 or so Forensic Computing Foundation Courses that have now been run for all their helpful comments and suggestions. We would like to add a sincere word of thanks to our publisher and editors, to Catherine Brett, Wayne Wheeler, Helen Callaghan and Beverley Ford, all of Springer, who, after much chivvying, eventually managed to get us to put pen to paper for this second edition, and a most important thank you also to Ian Kingston of Ian Kingston Publishing Services, who has made the result look so good. Finally our contrite thanks go to our families, to whom we did sort of promise that the first edition would be the last.

Contents

1 Forensic Computing	1
Origin of the Book	2
Structure of the Book	3
References	6
2 Understanding Information	7
Binary Systems and Memory	8
Addressing	9
Number Systems	11
Characters	25
Computer Programs	27
Records and Files	27
File Types and Signatures	29
Use of Hexadecimal Listings	29
Word Processing Formats	30
Magic Numbers	35
Graphic Formats	36
Archive Formats	43
Other Applications	44
Quick View Plus	46
Exercises	46
References	48
3 IT Systems Concepts	49
Two Black Boxes	50
The Worked Example	53
Program, Data, Rules and Objects	62
Patterns Can Mean Whatever We Choose Them to Mean	63
Software Development	64
Breaking Sequence	67
An Information Processing System	70
References	72
Exercises	72
4 PC Hardware and Inside the Box	75
The Black Box Model	75
The Buses and the Motherboard	77

Intel Processors and the Design of the PC	86
A Few Words about Memory	93
Backing Store Devices	96
Floppy Disk Drive Units	98
External Peripherals	98
Expansion Cards	99
References	101
5 Disk Geometry	103
A Little Bit of History	103
Five Main Issues	104
Physical Construction of the Unit	104
Formation of Addressable Elements	106
Encoding Methods and Formats for Floppy Disks	107
Construction of Hard Disk Systems	112
Encoding Methods and Formats for Hard Disks	114
The Formatting Process	127
Hard Disk Interfaces	130
IDE/ATA Problems and Workarounds	141
Fast Drives and Big Drives	157
Serial ATA (SATA)	159
The POST/Boot Sequence	160
A Word About Other Systems	172
The Master Boot Record and Partitions	173
FATs, Directories and File Systems	189
RAID	207
Exercises	209
References	210
6 The New Technology File System	215
A Brief History	215
NTFS Features	216
NTFS – How it Works	217
The MFT in Detail	219
Analysis of a Sample MFT File Record with Resident Data	224
Analysis of a Sample MFT File Record with Non-Resident Data	240
Dealing with Directories	247
Analysis of a Sample MFT Directory Record with Resident Data	248
External Directory Listings – Creation of “INDX” Files	261
Analysis of an “INDX” File	268
Some Conclusions of Forensic Significance	270
7 The Treatment of PCs	277
The ACPO <i>Good Practice Guide</i>	278
Search and Seizure	279
Computer Examination – Initial Steps	288
Imaging and Copying	291

References	299
8 The Treatment of Electronic Organizers	301
Electronic Organizers	301
Application of the ACPO <i>Good Practice Guide</i> Principles	311
Examination of Organizers and What may be Possible	313
JTAG Boundary Scan	324
A Few Final Words about Electronic Organizers	324
References	325
9 Looking Ahead (Just a Little Bit More)	327
Bigger and Bigger Disks	328
Live System Analysis	332
Networked Systems Add to the Problems	333
Encryption	333
A Final Word	339
References	339
Bibliography	341
Appendices	
1 Common Character Codes	351
2 Some Common File Format Signatures	355
3 A Typical Set of POST Codes	359
4 Typical BIOS Beep Codes and Error Messages	363
5 Disk Partition Table Types	367
6 Extended Partitions	373
7 Registers and Order Code for the Intel 8086	379
8 NTFS Boot Sector and BIOS Parameter Block	387
9 MFT Header and Attribute Maps	389
10 The Relationship Between CHS and LBA Addressing	411
11 Alternate Data Streams – a Brief Explanation	415
Answers to Exercises	425
Glossary	435
Index	455