

# Practitioner Series

---

Springer-Verlag London Ltd.

## Series Editor

Ray Paul *Brunel University, Uxbridge, UK*

## Editorial Board

Frank Bott *UWA, Aberystwyth, UK*  
Nic Holt *ICL, Manchester, UK*  
Kay Hughes *DERA, Malvern, UK*  
Elizabeth Hull *University of Ulster, Newtownabbey, N Ireland*  
Richard Nance *Virginia Tech, Blacksburg, USA*  
Russel Winder *Kings College London, UK*

---

## Other titles in this series:

The Project Management Paradigm <i>K. Burnett</i> 3-540-76238-8	Middleware <i>D. Serain (Translator: I. Craig)</i> 1-85233-011-2
The Politics of Usability <i>L. Trenner and J. Bawa</i> 3-540-76181-0	Java for Practitioners <i>J. Hunt</i> 1-85233-093-7
Electronic Commerce and Business Communications <i>M. Chesher and R. Kaura</i> 3-540-19930-6	Conceptual Modeling for User Interface Development <i>D. Benyon, T. Green and D. Bental</i> 1-85233-009-0
Key Java <i>J. Hunt and A. McManus</i> 3-540-76259-0	Computer-Based Diagnostic Systems <i>C. Price</i> 3-540-76198-5
Distributed Applications Engineering <i>I. Wijegunaratne and G. Fernandez</i> 3-540-76210-8	The Unified Process for Practitioners <i>J. Hunt</i> 1-85233-275-1
Finance for IT Decision Makers <i>M. Blackstaff</i> 3-540-76232-9	Managing Electronic Services <i>Å. Grönlund</i> 1-85233-281-6
The Renaissance of Legacy Systems <i>I. Warren</i> 1-85233-060-0	Real-Time and Multi-Agent Systems <i>A. Attoui (Translator: S. Ingram)</i> 1-85233-252-2

Tony Sammes and Brian Jenkinson

---

# **Forensic Computing**

## **A Practitioner's Guide**



Springer

A.J. Sammes, BSc, MPhil, PhD, FBCS, CEng  
Head, Department of Informatics and Simulation, Royal Military College of  
Science, Cranfield University, Shrivenham, Swindon, Wiltshire SN6 8LA, UK

B.L. Jenkinson, BA, BSc (hon), MBCS  
Forensic Computer Consultant. Detective Inspector (retired), former head of  
Cambridgeshire Constabulary Fraud Squad, Chairman of the Forensic  
Computer Group Training Committee and member of the ACPO Computer  
Crime Group.

ISSN 1439-9245

British Library Cataloguing in Publication Data  
Sammes, A. J.

Forensic Computing : a practitioner's guide. -  
(Practitioner series)  
1.Forensic science - Data processing 2.Microcomputers  
I.Title II.Jenkinson, B.  
363.2'5'0285416

Library of Congress Cataloging-in-Publication Data  
Sammes, A. J.

Forensic computing : a practitioner's guide / A.J. Sammes and B. Jenkinson.  
p. cm. -- (Practitioner series)  
Includes bibliographical references and index.

1. Forensic engineering--Data processing. I. Jenkinson, B., 1950- II. Title. III. Series.

TA219 .S36 2000  
363.25--dc21

00-037163

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.

ISBN 978-1-85233-299-0 ISBN 978-1-4471-3661-3 (eBook)  
DOI 10.1007/978-1-4471-3661-3

© Springer-Verlag London 2000

Originally published by Springer-Verlag London Limited in 2000.

2nd printing 2001  
3rd printing 2002  
4th printing 2003  
5th printing 2004

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.

Typesetting: Ian Kingston Editorial Services, Nottingham UK

34/3830-543 Printed on acid-free paper SPIN 11328063

# *Dedication*

---

*To Joan and Val*

# *Acknowledgements*

---

The authors would like to thank all the members and former members of the FCG Training Committee and all those law enforcement officers who have so generously given of their time for their kind support and the valuable contributions that they have made to this work. In particular our grateful thanks go to Steve Buddell (Inland Revenue), Tony Dearsley (Customs & Excise), Geoff Fellows (Northamptonshire Police), Paul Griffiths (Greater Manchester Police), Mike Hainey (Serious Fraud Office), Dave Honeyball (Thames Valley Police), Peter Lintern (Avon & Somerset Police), John McConnell (Greater Manchester Police), Keith McDonald (Customs & Excise), Geoff Morrison (Wiltshire Constabulary), Laurie Norton (Customs & Excise), Kathryn Owen (Serious Fraud Office) and Stewart Weston-Lewis (Inland Revenue). Our thanks also go to all the students of the seven Forensic Computing Foundation Courses that have so far run for their helpful comments and to the members of the DoIS staff who have provided such valuable support to us. Finally, a word of thanks for our publisher, our editor and our families who have all tolerated our intolerance as we have gone through the ups and downs of writing this book.

## *Series Editor's Foreword*

---

With the benefits of computing come the inevitable human misuses. This unique book, written by two authors with extensive practical experience, provides the reader with a sufficient depth of technical understanding to search for, find and confidently present any form of digital document as admissible evidence in a court of law. So the book has two classes of readership: a forensic computing analyst, and someone wanting to know the intrinsic technicalities of computers.

Chapters 2–5 provide the technical content, culminating with Disk Geometry in Chapter 5, the “real technical meat of the book”. Chapter 6 considers the issue of process as put forward by the Association of Chief Police Officers (ACPO) in their *Good Practice Guide for Computer Based Evidence*. Chapter 7 looks at personal organizers, which tend not to have hard disks and therefore make the analysis memory based. The final chapter is a look-ahead chapter, a springboard I would guess for future editions of this valuable book.

The material in this book has been tried and tested on students in Tony Sammes' department at the Royal Military College of Science at Shrivenham. Having been an external examiner there, I know how rigorous the material has to be. But more importantly, the experience distilled in this book has been gleaned and tested on numerous real cases by the authors. There can be no better evidence of its value.

*Ray Paul*

# Contents

---

<b>1 Forensic Computing</b> . . . . .	1
Origin of the Book . . . . .	2
Structure of the Book . . . . .	3
References . . . . .	5
<b>2 Understanding Information</b> . . . . .	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
<b>3 IT Systems Concepts</b> . . . . .	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
<b>4 PC Hardware and Inside the Box</b> . . . . .	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