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
K. Burnett
3-540-76238-8

The Politics of Usability
L. Trenner and J. Bawa
3-540-76181-0

Electronic Commerce and Business Communications
M. Chesher and R. Kaura
3-540-19930-6

Key Java
J. Hunt and A. McManus
3-540-76259-0

Distributed Applications Engineering
I. Wijegunaratne and G. Fernandez
3-540-76210-8

Finance for IT Decision Makers
M. Blackstaff
3-540-76232-9

The Renaissance of Legacy Systems
I. Warren
1-85233-060-0

Middleware
D. Serain (Translator: I. Craig)
1-85233-011-2

Java for Practitioners
J. Hunt
1-85233-093-7

Conceptual Modeling for User Interface Development
D. Benyon, T. Green and D. Bental
1-85233-009-0

Computer-Based Diagnostic Systems
C. Price
3-540-76198-5

The Unified Process for Practitioners
J. Hunt
1-85233-275-1

Managing Electronic Services
Å. Grönlund
1-85233-281-6

Real-Time and Multi-Agent Systems
A. Attoui (Translator: S. Ingram)
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 lookahead 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