

Digital Forensics

Digital Evidence in Criminal Investigation

Angus M. Marshall

University of Teesside, UK

 **WILEY-BLACKWELL**

A John Wiley & Sons, Ltd., Publication

Digital Forensics

Digital Forensics

Digital Evidence in Criminal Investigation

Angus M. Marshall

University of Teesside, UK

 **WILEY-BLACKWELL**

A John Wiley & Sons, Ltd., Publication

This edition first published 2008
© 2008 John Wiley & Sons, Ltd

Wiley-Blackwell is an imprint of John Wiley & Sons, formed by the merger of Wiley's global Scientific, Technical and Medical business with Blackwell Publishing.

Registered office.

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

Other Editorial Offices:

9600 Garsington Road, Oxford, OX4 2DQ, UK
111 River Street, Hoboken, NJ 07030-5774, USA

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com/wiley-blackwell

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Library of Congress Cataloging-in-Publication Data

Marshall, Angus M.

Digital forensics : digital evidence in criminal investigation / Angus M. Marshall.
p. ; cm.

Includes bibliographical references and index.

ISBN 978-0-470-51774-1 (cloth)

1. Digital electronics. 2. Forensic engineering. I. Title.
[DNLM: 1. Forensic Medicine--methods. 2. Computers. 3. Forensic
Medicine--instrumentation. 4. Internet. W 626.5 M367d 2008]

TK7868.D5M3215 2008

363.25--dc22

2008033258

ISBN: 9780470517741 (HB)

ISBN: 9780470517758 (PB)

A catalogue record for this book is available from the British Library.

Typeset in 11/15pt Minion by Aptara Inc., New Delhi, India.
Printed in Singapore by Markono Pte Ltd
First impression – 2008

Contents

Preface	vii
Acknowledgments	xi
List of Tables	xii
List of Figures	xiii
1 Introduction	1
1.1 Key developments	1
1.2 Digital devices in society	5
1.3 Technology and culture	6
1.4 Comment	7
2 Evidential Potential of Digital Devices	9
2.1 Closed vs. open systems	10
2.2 Evaluating digital evidence potential	17
3 Device Handling	19
3.1 Seizure issues	21
3.2 Device identification	31
3.3 Networked devices	36
3.4 Contamination	40
4 Examination Principles	43
4.1 Previewing	43
4.2 Imaging	47
4.3 Continuity and hashing	48
4.4 Evidence locations	49
5 Evidence Creation	55
5.1 A seven-element security model	56
5.2 A developmental model of digital systems	60

5.3	Knowing	61
5.4	Unknowing	63
5.5	Audit and logs	68
6	Evidence Interpretation	69
6.1	Data content	69
6.2	Data context	83
7	Internet Activity	85
7.1	A little bit of history	85
7.2	The ISO/OSI model	86
7.3	The internet protocol suite	90
7.4	DNS	94
7.5	Internet applications	96
8	Mobile Devices	109
8.1	Mobile phones and PDAs	109
8.2	GPS	116
8.3	Other personal technology	118
9	Intelligence	119
9.1	Device usage	119
9.2	Profiling and cyberprofiling	121
9.3	Evaluating online crime: automating the model	124
9.4	Application of the formula to case studies	126
9.5	From success estimates to profiling	129
9.6	Comments	129
10	Case Studies and Examples	131
10.1	Introduction	131
10.2	Copyright violation	131
10.3	Missing person and murder	133
10.4	The view of a defence witness	137
Appendix A	The “Aircraft Carrier” PC	141
Appendix B	Additional Resources	145
B.1	Hard disc and storage laboratory tools	145
B.2	Mobile phone/PDA tools	146
B.3	Live CDs	146
B.4	Recommended reading	146
Appendix C	SIM Card Data Report	149
References		157
Index		161

Preface

A small auto-biography

For most of my life, I've been fascinated by computers. At school, one of my maths teachers, Mr. Brindle, had a Commodore PET (Personal Electronic Translator) which formed the nucleus of a computer club.

A gang of us would gather at lunchtimes and after school, trying to devise new games and solve interesting problems. Soon, an Apple][was acquired and the club members had to relearn programming for this strange new creature. We even managed to get access to the holy mainframe (a DEC-20) at our local college and many evenings were spent exploring the capabilities of this magnificent beast.

Around this time, the Computer Misuse Act and the first Data Protection Act were being drafted and brought into legislation, defining specific offences relating to inappropriate and unauthorised use of computer systems. The first mobile phones started to appear and CD-players were a “must-have” gadget. Companies such as Commodore, Sinclair and Acorn enjoyed huge success with their home computers and Apple and IBM started production of personal computers aimed at businesses.

I was supposed to be a physicist, but an early introduction to the possibilities of computer networks led me into some experimentation with primitive “hacking” – nearly ruining my attempts to gain a BSc. Eventually, I did graduate with a degree in Computer Studies and Microsystems by forcing myself to concentrate on the challenge of getting hardware and software to work in harmony. My first real academic research dealt with the creation of neural networks on parallel processing systems, but I was developing more of an interest in a thing called the “Internet”, which seemed, to me, to

have great potential for information sharing and creating online communities. An emerging Internet service called the “World Wide Web” seemed to be a very accessible way of using the Internet, and combining it with my other passion (proper sports cars) led to a few years of collaboration with the Morgan Motor Company, where they gained a WWW presence, and my team gained a better understanding of how people navigate web sites.

Around 1992, I first became aware of the existence of “Forensic Computing” as an emerging discipline, concentrating on how data could be recovered from computers for use in criminal investigations.

For the following 10 years, or so, I continued as computer science lecturer in a number of British universities, finally landing at the Centre for Internet Computing in Scarborough where I was able to introduce some aspects of forensic computing into the curriculum, in the guise of modules dealing with computer security. I was also fortunate enough to have a colleague who shared some of my interests, and discovered that we made a good research team. So, we began writing and publishing papers, which were accepted by the general forensic science community to such an extent that it was suggested that I should register with the National Crime Faculty as an expert adviser on Internet activities.

Then, in 2003, I received a call from a police force asking if I could help them with a missing person enquiry. Soon, it transpired that we were dealing with a murder enquiry, and computer-originated evidence turned out to be almost essential in establishing patterns of behaviour and interests for the victim and more than one suspect.

Since then, I have acted as an expert witness for prosecution and defence in all manner of cases from fraud, through copyright violation to distribution of illegal images of children. The cases are always serious, but the work is never boring – with new challenges presented every time.

Now, I am a member of the Forensic and Crime Scene Sciences team at the University of Teesside where I am lucky enough to work with experts from a huge range of other disciplines.¹ My own group (Digital Evidence) is expanding steadily and we provide material for all of the forensic and crime scene science courses in our school. I also act as an external examiner and

¹Some of whom do their experiments in buckets.

adviser/consultant for other universities, and maintain links with business and industry wherever possible.

About this book

The world is full of digital devices. Without them, society as we know it would probably collapse. As a result, even the most innocuous device may contain information which is relevant in a criminal investigation. This book is intended to help investigators assess the potential of digital evidence sources, evaluate the huge and ever-changing range of technologies available, and introduce some of the main principles of digital evidence examination.

It does not go into excessive low-level detail of how files are deleted in the NTFS MFT, for example, but concentrates more on how those involved in criminal investigations can consider the potential of digital devices as sources of evidence; suggest possible lines of enquiry which can assist the investigator and, I hope, help them to understand the principles behind some of the more technical aspects of digital evidence examination.

Finally, an apology. To all my colleagues in the forensic science world: I know that “forensic” is an adjective relating to debating or courts and should never be used as a noun or, worse yet, a verb . . . but sometimes editors win arguments.

Angus Marshall

Acknowledgments

The list of people who need to be thanked for their support in the production of this book is immense, but a few in particular deserve special thanks:

- Fiona and the team at Wiley: for tolerating my Adams-like attitude to deadlines.
- Allen Clarkson: for reading drafts and passing comments – always helpfully.
- Brian Tompsett and Natasha Semmens: my regular research partners and co-investigators in the Cyberprofiling project. Without their support, some of the ideas in this book could never have existed.
- Colleagues at the University of Teesside: who have taught me far too much about forensic and crime scene sciences and influenced my approach to casework.
- My students: for making me think much harder than I wanted to, sometimes. I hope I've done the same to you.
- My parents: for giving me a second chance all those years ago.

And, most importantly, my wife Shirley, who supported and encouraged me throughout this whole process.

List of Tables

2.1 Roles played by digital devices	13
2.2 Roles a PC plays in DVD copying	16
4.1 Hash values for strings which differ by one bit	49
5.1 Routes by which data/programs can arrive on a system	60
6.1 Possible meanings of some byte-length binary strings	70
6.2 Sample file signature "magic numbers"	71
6.3 The Alphabet in Morse Code	72

List of Figures

3.1	A typical uninterruptible power supply	25
3.2	A standard power connector on the rear of a Pc	27
3.3	Labelling the sockets and cables before disconnecting and packaging	28
3.4	A PDA in tamper-evident packaging	29
3.5	Front and rear of a sample evidence label, also know as a “CJA” (Criminal Justice Act) label	30
3.6	Sample from http://www.mini-itx.com/ showing a model aircraft carrier which contains a full PC (See Appendix A for more images)	32
3.7	“Standard” USB storage devices	33
3.8	A novelty/disguised USB storage devices (inset shows the USB connector visible when it is opened)	34
3.9	SD card (large) and micro-SD/TransFlash card (small) devices	35
3.10	A network socket on a PC and associated cable	36
3.11	A domestic broadband router with wireless antenna	37
3.12	A low-cost network switch used to connect multiple machines	37
3.13	A Standard RJ45 wall plate in the author’s bedroom	38
3.14	A network patch-panel in a domestic installation	39
4.1	A Tableau T8 USB write-blocker used to protect devices against accidental data writing	44
4.2	A typical SATA/IDE to USB hard disk adapter	45
4.3	Slack space	53
5.1	A seven element model of information security	56
6.1	Examples of txt-spk	72
6.2	Image to be compressed	73
6.3	“Raw” image in binary form	74
6.4	Compressed image using one bit per pixel	75
6.5	Original uncompressed image: File size 320 kilobytes	76

6.6	Image compressed using JFIF JPEG set at 50 per cent quality: File size 24 kilobytes	77
6.7	Image compressed using JFIF JPEG set at 10 per cent quality: occupies 4 kilobytes	78
6.8	An idealised sample segmented file structure for a word-processed document	78
6.9	A simple shift-substitution or “Caesar” cipher table	80
6.10	Application of the cipher table in Figure 6.9	80
7.1	The ISO/OSI seven-layer network model	86
7.2	The IP suite five-layer model	91
7.3	A DNS query in progress	95
7.4	A sample of HTML used to compose a web page	97
7.5	Contents of typical cookies from the author’s web browser	100
7.6	A sample e-mail showing full headers	102
8.1	A typical set of interface cables found in a mobile device examination kit	110
8.2	A multi-format removable memory card reader connected via a forensic bridge write-blocker	112
8.3	A standard small-format modern SIM card	113
8.4	A typical consumer GPS unit for use in-car	117
8.5	Personal media players	118
9.1	“Real world” crime	122
9.2	Internet model of crime	124
10.1	Suspicious file properties	136
A.1	The “aircraft carrier” PC	141
A.2	Detail showing the DVD-rewriter drawer extended	142
A.3	Connectors on the “rear”	142
A.4	Activity lights in aircraft on carrier deck	143

1

Introduction

The field of digital evidence, aka Forensic Computing, is unlike most other forensic sciences because the nature of the material under examination is determined, largely, by human ingenuity. Rather than looking for traces of material deposited by physical or biological entities, which tend to develop and evolve slowly, we deal with technology which is updated, enhanced and even created at an alarming rate.

Since the 1960s, the rate of development of digital technology has held true to Moore's law [32], which originally proposed that the density of transistors on a given area of silicon would double approximately every 18 months. Since the start of the 21st century, the rate has slowed slightly, but we still see a doubling in density every two years.

This means that a modern mobile phone can contain more processing power and storage capacity than the computers which NASA used to send man to the moon. In a device a fraction of the size. At a much lower price. And easier to use. With greater reliability. And a smaller power supply.

1.1 Key developments

The time when only nerds or geeks¹ were interested in computers is long gone. Advances in computer usability have led to the development of digital

¹A geek is a nerd with social skills, and an extrovert geek looks at *your* shoes when he/she is talking to you.

devices which are no longer the sole preserve of the white-coated “high priests” of computing (once known as the programmers and operators), but have become accessible to everyone capable of holding a mouse or using a keyboard.

Increasing dependence on computers can, arguably, be traced back to the late 1970s and early 1980s with the development of machines such as the Apple][, Lisa and Macintosh; Sinclair ZX81 and Spectrum; Commodore Vic20, 64 and Amiga and, finally, the IBM Personal Computer [8].

The IBM PC, with its standardised low-cost hardware, simple Microsoft Disc Operating System (PC-DOS or MS-DOS) and the backing of the world’s largest computer manufacturer, resulted in a host of imitators and compatible machines targeted mainly at business.

It seems that Pournelle’s law² was perceived to be true in business. The creation of low-cost machines that allowed users to perform common computing tasks on their desktops, without having to wait for time on the company mainframe or mini-computer, led to the first steps towards pervasive computing: “computing anywhere and everywhere”.

The success of these IBM-compatible PCs with Microsoft operating systems and applications created a de-facto standard, never before seen, which allowed free exchange of data and information between systems, people and organisations, thus eliminating one of the biggest barriers to information exchange.

Standardisation of software and data created opportunities for “paperless offices”, where every member of staff had access to computing resources on the desktop – often linked to a local area network – connecting machines within an office or building for even greater resource sharing and efficiency.

Meanwhile, since the 1960s, work had been progressing on what we know today as the Internet [43]. This wide area network began life as an academic project designed to allow data sharing between distant sites, but in a way which allowed the network to be scaled up to include millions of machines. Again, this created a de-facto international standard for networking through the creation of an easy to use system which allowed developers to

²“At least one CPU per user” – Jerry Pournelle, science fiction author and BYTE columnist, 1978.

add new features without compromising the existing network. In effect, the Internet provides a global “road network” which is capable of carrying any type of traffic which can be devised.

Prior to 1989, however, the Internet was largely the preserve of the technically minded, mostly because of the huge number of incompatible applications which existed on it. Tim Berners-Lee, a British physicist working at CERN, proposed a new information management system [5] for CERN to counter the problems of information loss, damage and confusion which the organisation was suffering at the time.

The proposal defined an information sharing system which allowed disparate information systems to be linked together via a common interface based around the concept of HyperText [4].³ In a HyperText system, the user can navigate around the text by activating links, which jump to other pieces of text. Berners-Lee’s innovation was to allow these links to reference documents and even applications external to the current document. In this way, the World Wide Web as we know it was born, with a single consistent interface to a range of different applications. Arguably, this is the single most important innovation in information systems in the 20th century. It has certainly led to the widespread adoption of Internet services as a part of everyday life.

Alongside, and slightly behind, the developments in desktop computing and internetworking, the continual shrinking of components created opportunities for smaller devices to be created. In the 1980s we saw the creation of the first analogue mobile telephony networks, with a proper launch in the UK in 1982. Although the devices in use were bulky with very limited battery life (typically a few hours), poor network coverage and susceptible to interference and eavesdropping, they were well-received and became essential tools for modern business. 1982⁴ also saw the launch of the compact disc (CD) by Philips, setting a new standard for audio and data storage. The thirst for increased capacity in this convenient disc format led to the later creation of the Digital Versatile Disc (DVD) and the current battles over High-Definition disc standards.

³The term HyperText was coined around 1965 by Ted Nelson, but the concept is older.

⁴A very good year – it also saw the launch of the author’s favourite car: the Lotus Excel.