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

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

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

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

[1] Some 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

List of Figures

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 geeks[1] were interested in computers is long gone. Advances in computer usability have led to the development of digital

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

Digital Forensics: Digital Evidence in Criminal Investigation Angus M. Marshall

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 law[2] 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 activsting 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. 1982[4] 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.

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

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