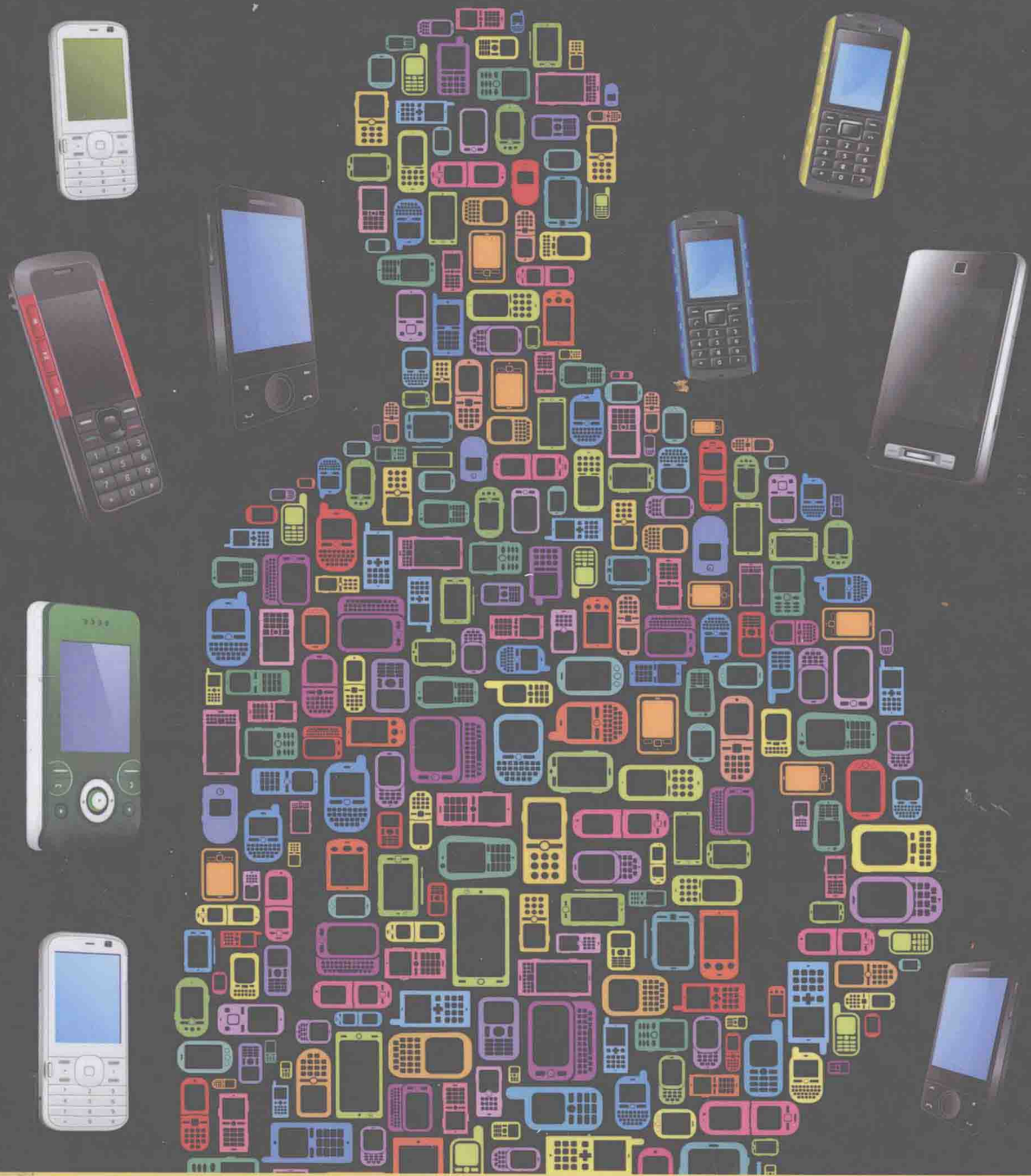
Digital Forensics for Handheld Devices



Eamon P. Doherty

CRC Press
Taylor & Francis Group

Digital Forensics for Handheld Devices

Eamon P. Doherty

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **Informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20120626

International Standard Book Number: 978-1-4398-9877-2 (Hardback)

This book is dedicated to my lovely wife Ester, my mom, my sister-in-law Elly, and the memory of my dad, Edward T. Doherty

Preface

This book was written to teach someone about all the areas of mobile device forensics, which include topics from the legal, technical, academic, and social aspects of the discipline. It is hoped that the reader will now have an idea how to use a variety of digital forensic tools to examine flash drives, cell phones, PDAs, digital cameras, and netbooks. It is also hoped that the reader will understand the differences between a corporate investigation and a criminal investigation as well as some of the issues regarding privacy and the Fourth Amendment. The book ends with a discussion of the education and certifications that one needs for many possible careers in mobile device forensics.

Disclaimer

The views expressed in this book are Dr. Doherty's own views and ideas and do not necessarily represent the ideas and viewpoints of his employer or any organization he is associated with. This is an academic book that explores ideas, mobile device forensic techniques, and tools. This book is not a forensic manual or a legal manual. Dr. Doherty is not endorsing any products and was not paid to endorse any products. One should consult their organization's general counsel and follow the policies of the organization before attempting anything from the book.

Author

Eamon P. Doherty, PhD, CCE, SSCP, CPP, is an associate professor and the Cybercrime Training Lab director at Fairleigh Dickinson University (FDU), New Jersey. Dr. Doherty is a member of the High Tech Crimes Investigative Association, ASIS International, the FBI Infraguard, the American College of Forensic Examiners Institute, the FDU Digital Forensics Club, the IACSP, and the American Society of Digital Forensics & eDiscovery. Dr. Doherty has also assisted with some law enforcement cell phone investigations and is the chairman of the New Jersey Regional Homeland Security Technology Committee. Dr. Doherty previously worked for Morris County Government in their M.I.S./I.S.D. section. Presently, Dr. Doherty has developed and taught many continuing education classes for FDU on the subjects of cell phone forensics, PDA forensics, and digital camera forensics.

An environmentally friendly book printed and bound in England by www.printondemand-worldwide.com

This book is made entirely of sustainable materials; FSC paper for the cover and PEFC paper for the text pages.

#0371 - 050613 - C0 - 254/178/18 [20] - CB

Contents

	Preface	xxiii
	Disclaimer	xxv
	Author	xxvii
Chapter 1	The Cell Phone	1
	The Cell Phone Is Invented	1
	Cell Phone Models and Cell Phone Museums	2
	Cell Phone Protocols and Operating Systems	4
	Cell Phone Operating Systems: Finding the ESN and IMEI	4
	Cell Phone Operating Systems and Protocols: Synchronization	6
	Cell Phone Differences Worldwide	7
	Cell Phone Differences Worldwide: Various Bands	8
	Cell Phone Internal and External Storage	10
	Internal Cards: SIM Cards/Locked and Unlocking	12
	The Need for a Faraday Bag	13
	Survey of Tools to Investigate a Cell Phone	14
	Examining Cell Phones with Operating Systems Unsupported by Your Tools	15
	Cell Phone Forensic Tools: Mobil Edit	17
	Survey of Cell Phone Forensic Tools: Paraben Device Seizure	18
	Susteen Secure View	19
	Chinese Cell Phone Examination Tools	21
	Translation of Chinese Calling Codes and Documents within a Phone	22
	Validating Your Chinese Cell Phone Examination Tools	23
	Paraben's Deployable Device Seizure	23
	Paraben's SIM Card Seizure Version 3.1	25
	Replacing the USB Mini Port on a Cell Phone	26
	Paraben's Link2 V2.5	28
	Elcomsoft Phone Password Breaker	28

Investigative Computer and Precautions to Take 29
Precautions: Examining Phone—High-Profile Case 30
Precautions: Protecting Equipment from Static Electricity 31
GPS Camera Phones 32
GPS Data in Picture 32
GPS Data and Crimes 33
GPS Accuracy and Variables 34
Metadata: Linking Picture to Google Maps 35
Faking GPS Data Using Picasa 3 and Google Earth 36
Putting It All Together: Cell Phone Hardware 36
References 37

Chapter 2 Digital Camera Forensics 41
The History of the Digital Camera 41
Digital Camera History: Conversion of Analog Pictures to Digital Signals 41
Digital Camera History: The Transmission of Digital Images 42
Digital Camera History: Kodak's 1.4 Megapixel Sensor 42
Digital Camera History: The Apple Quick Take 100 42
Digital Camera History: The Webcam 42
Digital Camera History: dSLR 44
Getting to Understand Digital Camera Hardware 44
History of the Digital Camera: Criminal Activity 45
Digital Camera Operating Systems 46
Digital Camera File Systems: FAT 46
External Media 47
Survey of Tools to Investigate a Digital Camera 47
Survey of Tools: Forensic Professional Kiosk Card Reader EX-3U Read Only 48
New 3.5" All-in-One Internal Card Reader USB Flash Memory Metal Silver 50
The 26-in-1 USB Card Reader by DZ-Tech 51
Digital Image Recovery 51
Zero Assumption Recovery Toolkit 52
Disk Space Visualizer Version 1.2 52
Zero Assumption Recovery Tutorials 52
EXIF Data Standards 53
EXIF Field Types 53
GPS EXIF Data 54

EXIF Reader 54
PixelZap and PZapGui 54
Thumber 54
Framer 55
File Lister 55
MinUpTime 56
HideWin 56
FileMonitor 56
CamWork 56
CRead 57
Tools for the Camera Investigator: X-Ways "Forensic Software" 57
Tools for the Camera Investigator: Recover My Files 57
Tools for the Camera Investigator: ProDiscover Basic 57
Tools for the Digital Camera Phone Investigator: Susteen Secure View 58
Tools for the Digital Camera Phone Investigator: Guidance Software Encase 58
Tools for the Digital Camera Phone Investigator: ILook Investigator Software 58
Tools for the Digital Camera Phone Investigator: Paraben's Device Seizure 58
Survey of Tools: ABC Amber Image Converter 59
Thumbnails and Thumbnail Viewer: DM Thumbs 59
Survey of Tools to Investigate Camera: Case Study of Advanced Import Camera (2009) 59
Case Study: Data Carving with Data Lifter 2 61
Case Study: Determining the Level of Resolution Loss of the Recovered Pictures 61
Case Study: Survey of Tools to Investigate a Digital Camera 62
Case Study: Use of USB Write Blocker 62
Case Study: Access Data FTK 62
Case Study: Determining if a Picture Was Created with the Binocular Camera 63
Case Study: Each Camera Has Imperfections and Limitations That Impact the Picture 63
The Investigative Machine: Digital Camera Forensics 64
Black Hole Faraday Bag 66
Incident Response Tools and Services 67
CasesNotes Lite 67
FragView 67
GigaView 67

VideoTriage 67
My Thoughts on the Need for Time-Saving Video Investigation Tools 68
The Investigative Computer and Precautions to Take 68
Precautions: Be Prepared to Answer Most Basic Questions for a Deposition 68
Precautions: Get Certified (ACE, CCE, CISSP, etc.) 69
Precautions: Handling Evidence and Static Electricity 70
Precautions: Get a Good Image of the External Media and/or Internal Media 70
Precautions: Finding Experts for Specialized Old Digital Cameras 70
Precautions: Posting Questions on Blogs or List Servers 71
Precautions: Find Digital Pictures with Wrong File Extensions 71
Precautions: No Breaks of Custodianship of Evidence 72
Precautions: Do Not Just Rely on Automated Tools! 72
Precautions: Using Other Investigative Tools Such as Biometrics to Solve the Case 73
Precautions: Check HR for a Signed Camera Policy 73
Precautions: Know When to Invoke the Silver Platter Doctrine 73
Precautions: Check for Counterfeit American Money at Crime Scene 74
Precautions: Wet Batteries and Camera Phones/Digital Cameras 74
Why Steganography Is Important to Digital Camera Forensic Examiners 74
Precautions: Use the Best Evidence Rule 75
Precautions: Weeding Out the Wrong Types as Investigators 75
Precautions: Keeping Current on Digital Camera Forensics 76
References 76

Chapter 3 PDAs and Digital Forensics 79
PDA History 79
History of PDA and Pocket Size Organizer 80
PDA History: PDA Phone 81
Learning about PDAs/Museums 81
Learning about PDAs: PDA Hardware 82
PDA Protocols Connectivity and Operating Systems 83
PDA Connectivity: Infrared 83
PDA Connectivity: Wireless 84
PDA Connectivity: Bluetooth 85
PDA Connectivity: Cable 85
PDA Operating Systems: Microsoft Windows Mobile 5.0 Premium Edition 86

PDA Operating Systems: Palm 86
Learning about New Operating Systems 87
Investigative Computer and Precautions to Take 88
Investigative Computer and Policy Precautions to Take 88
Precaution: Use Forensic Sterile Media 89
Precaution: Get PDA Examiner Certifications 90
Precaution: What about Americans Taking Their PDAs to Other Countries? 91
Precaution: PDA Examination and Disease 92
Precaution: Encountering *Prima Facie* Evidence on the PDA 92
Survey of Tools to Investigate a PDA: Paraben Device Seizure 93
Survey of Tools to Investigate a PDA: Paraben PDA Seizure 94
Survey of Tools to Investigate a PDA: Avanquest's Data Recovery Professional 94
Survey of Tools to Investigate a PDA: Recover My Files 95
Survey of Tools to Investigate a PDA: Guidance Software's Encase 95
Survey of Tools to Investigate a PDA: Palm PDD 96
Survey of Tools to Investigate a PDA: XRY Forensics 96
PDA Forensics and Intelligence: Clearwell eDiscovery Software 97
e2Retrieve 97
e2fsck 98
Pilot Link 98
PPWDump 98
Hardware Write Blockers for USB Ports and PDAs 98
The Digital Forensics Framework 99
Write Blockers for PDAs with 9 Pin Serial Ports 100
Using Virtual Machines for Demonstrating the Accused's PDA in Court 101
Final Thoughts on PDA Investigation 101
Suggested Further Reading 101
References 101

Chapter 4 GPS Devices 105
Introduction 105
GPS Device History 105
GPS Device History: Multienvironment GPS Tracking Devices 106
GPS Device History: GPS Tracking and Warrants 107
GPS Device History: Braille GPS Devices 107
GPS Device History: Military-Grade GPS Jammers 108
GPS Device History: Civilian-Grade GPS Jammers 108

GPS Device History: Signal Jamming for Both GPS and Glonass Systems 108
GPS Device History: GPS Spoofing Devices and Truck Hijacking 109
GPS Device History: GPS Fishfinder Devices 109
GPS Operating Systems 109
Survey of Tools to Investigate GPS Navigation Devices 111
Need to Investigate GPS Tracking Devices 111
Need to Investigate GPS Navigation Devices 111
Example of Paraben Version 4 and a Garmin Nuvi 1300 111
Access Data FTK Imager and FTK 1.8 112
Helix 3 and TomTology and the Tom Tom 112
Blackthorn 2 GPS Forensic Software System 113
Porn Detection Stick 114
Survey of GPS Forensic Tools: Networking with GPS Forensic Investigators 115
GPS Tools and Education 115
Outfitting a Lab with GPS Forensic Tools 116
GPS Devices, Training Labs, and Privacy Issues 117
Learning about Low-Budget Tools for GPS Forensics 118
Map Send Lite 118
Easy GPS 118
GPS Utility 119
GPS Babel 119
QuakeMap 120
DSI USB Write Blocker 120
Virtual GPS 1.39: GPS Simulator 120
Discussion with a Mobile Device and Computer Forensic Investigator 120
Examining a Tom Tom Go 700 121
Best Practices for Seizing Electronic Evidence and Radio Signals 122
GPS Forensic Credentials 123
Geographic Information Systems Training 123
Mobile Forensics Certified Examiner 124
Graduate Certificate in Digital Forensics: RWU 124
Masters in Digital Forensics at the University of Central Florida 124
Certified Electronic Evidence Collection Specialist Certification 125
SANS: Mobile Device Forensics (Forensics 563)—Certificate of Attendance 125
Suggested Further Reading and Reference Sources for GPS 126
References 127

Chapter 5 Corporate Investigations on a Netbook 129
Authorized Requestor Leads Investigations 129
AR Asks, "What Is a Netbook? Handtop? Subnotebook? Palmtop?" 130
HR, General Counsel, CIO 130
Incident Response Team 131
Incident Response Teams with Specializations 132
Incident Response Teams (Law Enforcement) and Dangerous Environments 133
Incident Response Teams Need a Photographer 135
Incident Response Teams (Resilience Training) 135
Incident Response Team Skills 136
Incident Response Team's Digital Forensics Lab 138
Incident Response Team's Toolkit 139
OSForensics: A Computer/Computer Media Forensic Analysis Tool 139
OSForensics as a Tool to Ensure Integrity of Examination Machine 140
Web-Based Training That Is "On Demand" for OSForensics 140
Password Recovery in OSForensics 140
OSForensics Case Management 141
Bootable Versions of OSForensics 141
OSFClone 141
cs2025 Forensic Software and Recovery Software for Unix, Linux, Windows, and Mac OS X 142
Network Miner 143
Mac-Robber 143
PLAC 143
Rdd Forensic Copy Program 143
AIR 143
TULP2G 143
ODESSA 143
Sleuth Kit 144
Maresware Linux Forensics 144
Drive Prophet 145
Elcomsoft: Advanced PDF Password Recovery 146
Advanced Sage Password Recovery 147
Elcomsoft Internet Password Breaker 147
Elcomsoft Wireless Security Auditor 148
Advanced Archive Password Recovery 149
Advanced Office Password Breaker 149

Instant Facebook Password Recovery 150
Zeitline 151
ProDiscover IR Smart Agent Version 6.7 151
ZeroView 151
X1 Professional Client 152
Windows Grep 152
WinFingerprint 152
Safari Books 152
Silent Runner Mobile 153
UnHide 154
Forensic Soft: Windows Forensic Boot Disk 154
Windows Forensic Tool Chest 156
Paraben's Shuttle 156
BackTrack 5 Forensic Tools 157
RkHunter: Backtrack Forensics Tools 157
Mork.Pl 158
HexEdit 158
ExifTool 158
Evtparse.pl 158
Missidentify 158
RegLookup 159
ReadPst 159
Pref.pl 159
Ptk 159
StegDetect 159
Vinetto 159
FatBack 160
Foremost 160
RecoverJPG 160
Safecopy 160
Scalpel 160
Scrounge-NTFS 160
TestDisk 160
HashDeep 161
MD5Deep 161
TigerDeep 161
ddRescue 161

EWFacquire 161
DriftNet 161
TcpReplay 162
WireShark 162
CmosPWD 162
fCrackZip 162
Samdump 162
PDF-ID 162
PDF-Parser 163
PeepDF 163
pdfbook.py 163
Pdgmail 163
Volatility 163
Paraben's Windows Breaker 163
LogicCube Forensic Talon Enhanced 164
Advanced EFS Data Recovery 165
PsLoggedOn (Incident Response Tool) 166
WebJob (Incident Response Tool) 166
AIR: Automated Image and Restore 167
Runtime Software 168
DriveLook Version 1 168
DriveImage XML V2.30 169
GetDataBack for NTFS V4.25 169
GetDataBack for FAT V4.25 169
Captain Nemo Pro V5.05 169
Disk Digger V1.0 169
ShadowCopy V2.0 170
RemoteByMail V1.01 170
Pythia V1.02 170
Ultimate Toolkit 170
eDiscovery Software 171
ChRootKit 172
Knoppix 173
Knoppix Security Tools Distribution 173
Password Recovery Toolkit 174
Distributed Network Attack 174
ISO Buster 175