

**THE INVESTIGATOR'S GUIDE
TO COMPUTER CRIME**

ABOUT THE AUTHOR

Carl J. Franklin has more than twenty years experience in the criminal justice profession. He spent almost thirteen of those years in a uniform working as a Community Service Officer, Police Officer, and in various roles as investigator and supervisor. He has worked in a uniform position with the University of Oklahoma, Norman, and Oklahoma City police departments. While a police officer, Franklin returned to the University of Oklahoma to complete a Bachelor's of Arts degree in Law Enforcement Administration. He later attended the Oklahoma University College of Law where he completed the Juris Doctor degree and was honored on three occasions with national awards for his writing in the areas of computers and constitutional law. He has also recently completed the Ph.D. in Business with an emphasis in Public Administration.

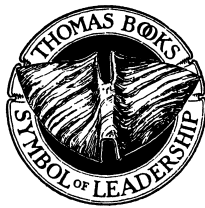
Franklin has also worked with the Oklahoma Court of Criminal Appeals, the Cleveland County District Attorney's Office, and as a private practitioner. He was appointed in three counties as the chief attorney for indigent defense, and maintained an active practice in criminal defense, police civil liability, and related areas.

He is the author of five books, including the *Police Officer's Guide to Civil Liability* (Charles Thomas) and more than forty professional and academic articles. Franklin currently works as an Assistant Professor (Tenure Track) at Southern Utah University where he teaches criminal and constitutional law, criminal procedure, ethics, and related classes.

THE INVESTIGATOR'S GUIDE TO COMPUTER CRIME

By

CARL J. FRANKLIN, J.D., PH.D.



CHARLES C THOMAS • PUBLISHER, LTD.
Springfield • Illinois • U.S.A.

Published and Distributed Throughout the World by

CHARLES C THOMAS • PUBLISHER, LTD.

2600 South First Street

Springfield, Illinois 62704

This book is protected by copyright. No part of
it may be reproduced in any manner without
written permission from the publisher.

© 2006 by CHARLES C THOMAS • PUBLISHER, LTD.

ISBN 0-398-07601-4 (hard)

ISBN 0-398-07602-2 (paper)

Library of Congress Catalog Card Number: 2005050873

*With THOMAS BOOKS careful attention is given to all details of manufacturing
and design. It is the Publisher's desire to present books that are satisfactory as to their
physical qualities and artistic possibilities and appropriate for their particular use.
THOMAS BOOKS will be true to those laws of quality that assure a good name
and good will.*

Printed in the United States of America

MM-R-3

Library of Congress Cataloging-in-Publication Data

Franklin, Carl J., 1958-

The investigator's guide to computer crime / by Carl J. Franklin.

p. cm.

Includes bibliographical references and index.

ISBN 0-398-07601-4 – ISBN 0-398-07602-2 (pbk.)

1. Computer crimes—Investigation—Handbooks, manuals, etc. I. Title.

HV8079.C65F73 2005

363.25'968—dc22

2005050873

*To Christopher, Michael, and Stacey.
You make me very proud.*

CONTENTS

	<i>Page</i>
<i>About the Author</i>ii

Section 1: Establishing Standards for the Computer Crime Investigation

Chapter 1: The Growing Trend of Computer Crime5
A. Introduction to Computer Crime5
B. Defining Computer and Technology Crime7
C. Establishing Parameters for Investigating Computer Crime10
D. Trends in Computer Crime13
Chapter 2: The Computer Crime Investigation Team17
A. Why Do We Need A Computer Crime Investigation Team?17
B. Who Should Be on the Team18
1. Case Supervisor19
2. Physical Search Team19
a. Guardian20
b. Crime Scene Manager21
c. Lead Investigator22
d. Search Coordinator22
e. Other Team Members23
3. Sketch and Photo Team23
4. Security and Arrest Team24
5. Technical Evidence Seizure Team25
6. Interview Team25
C. What if We Don't Have a Team?25
D. What Training and Education Do Team Members Need?26

Chapter 3: The Computer System in the Criminal Enterprise	30
A. Determining the Computer's Role in the Offense	30
B. Introduction to Computer Forensics	32
1. The Methodology of Computer Forensics	33
2. Establishing Policy and Procedures for Computer Cases	35
C. The Modus Operandi of Computer Crime:	
Motive and Technology	36
1. Entitlement	38
2. Compensatory	39
3. Anger or Retaliatory	39
4. Anger Excitation	40
Chapter 4: The Computer Crime Lab	43
A. Introduction	43
B. The Work Space	44
C. Basic Equipment Needs	47
1. The Computer Toolkit	47
2. Evidence Seizure Tools	55
3. Storage Containers	57
4. Computer-Oriented Items	59
D. Enhanced and Specialty Equipment	60
1. Magnetometer and Magnetic Compass	61
2. Portable Computer System	61
3. Software	62
4. Electronic Specialty Equipment	64
Chapter 5: Expert Assistance	66
A. Determining That an Expert is Needed	66
B. Finding Experts	70
1. Federal Sources	71
2. Private Experts	72
a. Professional Computer Organizations	73
b. Colleges and Universities	74
c. Computer and Telecommunications Industry Personnel	75
d. The Victim as Expert	75
C. What the Experts Can Do for Your Investigation	75

Section 2: Specific Computer Crimes

Chapter 6: Hardware and Software Crimes	79
A. Introduction	79
B. Classifying Hardware Involvement	80
1. Hardware as Contraband	80
2. Hardware as an Instrumentality of an Offense	81
3. Hardware as Evidence	83
C. Theft of Hardware or Software	84
1. Tracing Stolen Computer Components	84
a. Identifying Integrated Circuits	84
b. Computer Motherboards and Add-On Cards	89
c. Cases and Peripherals	91
2. Tracing Stolen Software	92
Chapter 7: Theft of Information	96
A. Introduction	96
B. Prioritizing the Investigation	98
1. Trade Secret	99
2. Proprietary Information	101
3. Confidential Information	103
C. The Value of Information	104
D. Identifying the Stolen Information	108
Chapter 8: Cyberstalking	110
A. What Is Cyberstalking?	111
B. Nature and Extent of Cyberstalking	113
C. Offline vs. Online Stalking—A Comparison	116
D. Evidence that Cyberstalking is a Growing Problem	119
E. Current Efforts to Address Cyberstalking	120
F. Jurisdictional and Statutory Limitations	122
G. Anonymity on the Internet	123
H. Law Enforcement Response	124
I. Industry Efforts	126
J. Cyberstalking Laws	127

Chapter 9: Identity Theft	129
A. The Nature of the Problem	129
B. How Does Identity Theft Occur?	132
C. Investigating the Identity Theft Case	134
D. Federal Criminal Laws for Identity Theft	136
E. Exemplary Federal Cases	139
F. State Criminal Laws	140
G. Steps to Help the Victim of Identity Theft	141

Section 3: The Computer Crime Investigation

Chapter 10: Initial Assessment and Response to the Computer Crime	147
A. Incident Notification and Response Protocol	147
B. The Initial Contact	151
C. Evaluating the Initial Scene	152
D. The Initial Interview	152
Chapter 11: Applying Forensic Science to Computers	157
A. Forensic Science Techniques	158
B. Recognition of Digital Evidence	159
C. Collecting and Preserving Hardware and Digital Evidence	161
D. Classification and Comparison of Digital Evidence	165
Chapter 12: Tracking the Offender	168
A. Basic Network Systems	169
B. The Basics of Tracking	171
1. The IP Address	172
2. The Internet Service Provider and Whois	173
3. The Route Through the System	174
4. Assigning Addresses	175
C. The Domain Name Service (DNS)	177
D. Using the DNS in the Track	178
1. Recursion	179
2. Other Addresses	181
E. Why are Addresses Important	181
F. The Art of the Track	182
G. Tracking the Mail Trail	184
H. SMTP Server Logs	185

Section 4: Search, Seizure, and Digital Evidence

Chapter 13: Computer-Related Evidence	189
A. Types of Computer-Related Evidence	189
1. Direct and Circumstantial Evidence	189
2. Applying Direct and Circumstantial Evidence	190
B. The Best Evidence Rule	191
C. Authenticating Electronic Documents	194
1. Distinctive Evidence	195
2. Chain of Custody	196
D. Electronic Processing of Evidence	197
E. Creation of Evidence from Computers	198
F. The Hearsay Rule	200
Chapter 14: Fourth Amendment Principles and	
Computer Searches	203
A. What Does the Fourth Amendment Protect?	204
B. Relevant Changes in the last Forty Years	206
C. Exceptions to the Warrant Requirement	207
1. Plain View	207
2. Exigent Circumstances	211
3. Border Searches	214
4. Consent Searches	214
a. Scope of the Consent	216
b. Third-Party Consent	217
c. General Rules of Consent	218
d. Spousal Consent	220
e. Parental Consent	221
f. Employer Consent	221
g. Networks: System Administrators	225
h. Informants and Undercover Operatives	226
i. Public Schools	228
<i>Appendix A: Identifying the Computer Components</i>	233
1. A Brief History of the Modern Computer	233
2. Advances in Computer Design	236
3. The Desktop IBM Compatible Computer System	241
a. System Architecture	242
b. System Components	244

i. The Case and CPU244
ii. The Motherboard247
iii. Bus Slots and I/O Cards251
iv. Peripherals255
v. Data Storage258
vi. Power Supply and Connectors260
<i>Appendix B: Understanding Software</i>261
A. Introduction to Software262
B. Operating Systems262
1. UNIX262
2. Linux265
3. Apple Mac OS267
4. Windows268
C. Application Programs269
1. Business Software269
a. Word Processors270
b. Spreadsheets271
c. Database271
d. Graphics272
e. Presentation273
f. Communication273
g. Other273
2. Entertainment Software274
a. Games274
b. Graphics274
c. Educational275
3. Utility Software275
a. System Maintenance275
b. Software Support275
c. Other276
<i>Appendix C: Networks and Communication Systems</i>277
A. Network Basics278
1. Clients and Servers280
2. Wiring and Cable281
3. Network Interface Cards282
4. Switches283
5. Bridges283

6. Routers	283
7. Modems	284
8. Network Management	284
B. Local-Area Networks: Ethernet, Fast Ethernet, and Gigabit Ethernet	285
1. Ethernet Basics	286
2. The 5-4-3 Rule	287
3. 10Base2	287
4. 10BaseT	287
5. 10BaseF	288
6. 100BaseT	288
7. 100BaseT4	289
8. 100BaseFx	289
9. 1000BaseX	289
10. CSMA/CD	289
11. I/G and U/L within the MAC address	290
12. Cisco's Inter-Switch Link (ISL)	291
13. Error Conditions	291
C. Token Ring	293
D. High-Speed LAN Technologies	293
E. Wireless Connections	294
F. Remote Access and Wide-Area Networks	295
G. Analog vs. Digital	295
H. ISDN	295
I. Leased Lines	296
J. Cable Modem/Router	296
K. Remote Access Servers	297
L. Digital Subscriber Line Service	297
M. Virtual Private Networks	298
N. Good Network Design: The 80/20 Rule	299
O. Understanding Network Protocols	299
<i>Appendix D: Computer Seizure Checklist</i>	302
<i>Glossary</i>	305
<i>Index</i>	309

FIGURES

	<i>Page</i>
4-1 Belkin small toolkit	48
4-2 Belkin 65-piece toolkit	49
4-3 Anti-static wrist strap	50
4-4 Jewelers screwdrivers	51
4-5 Torx diagram	52
4-6 Chip extractor	53
6-1 Integrated chip	87
6-2 Linksys Ethernet card	88
6-3 Mid-tower case with power supply and motherboard	90
6-4 Mid-tower case with identification label	91
Appendix A-1 Light bulb diagram	234
A-2 Light bulb (lit) diagram	234
A-3 Series of light bulbs	235
A-4 Series of light bulbs (lit)	235
A-5 Integrated chip	243
A-5a PC100 speed RAM Memory Module	248
Appendix C-1 Simple network	279
C-2 Network with hub	280

TABLES

Table 5-1 Sample checklist	69
Appendix A-1 Memory-addressing capabilities	246

**THE INVESTIGATOR'S GUIDE
TO COMPUTER CRIME**

Section 1

ESTABLISHING STANDARDS FOR THE COMPUTER CRIME INVESTIGATION

Chapter 1

THE GROWING TREND OF COMPUTER CRIME

-
- A. Introduction to Computer Crime
 - B. Defining Computer and Technology Crime
 - C. Establishing Parameters for Investigating Computer Crime
 - D. Trends in Computer Crime
-

A. INTRODUCTION TO COMPUTER CRIME

In the past half-century we have gone from a world where computers were science fiction to a world where computers are everyday fact. Just thirty years ago the computer that flew with the first astronauts to the moon had less computing power than the computer on the average student's desk today. Computers have grown in popularity, acceptance, and computing power. The average Personal Computer has doubled its computing capacity every eighteen months for more than a decade. Today, we find computers common in almost all parts of our life and there is no reason to believe that usage will decrease in the near future.

Along with the acceptance of computers in our everyday life has emerged a new line of crime revolving around the computer. Just as computers make daily business transactions more efficient they have also made many crimes more efficient. Computers have given us many new advances in our lives and provided great improvement as a whole. This is also true of the criminal element; computers have created contemptible new crimes as well as modernized many of the old ones.

For the law enforcement officer the first major issue is the determination

of how much emphasis to put on the problem. Clearly, computers have become a growing part of our everyday work as criminal investigators, but does that mean they should become a specialization unto themselves? Should departments create a "computer crime" unit similar to our traditional homicide, robbery, and burglary units?

We know that computers have made a substantial impact on our society, but have computer crimes become so significant that they demand special attention? The short answer is that it has not; at least yet. While the number of computer-related crimes has increased over the last two decades the vast majority of police officers rarely are involved in a computer crime. What this means is that while we should be conscious of the increase in computer-related crime, we need not create entire new branches of investigative theory to deal with that crime. For the most part, focused education and training can prepare the majority of police investigators to handle almost any computer crime they encounter.

One should not infer from the above statement that computer crime is not a problem. The fact is that computer crime is on the increase, and there is firm evidence to believe that the growth trend will continue for some time to come. Investigators should also keep in mind the rise in computers as both a tool and potential element of crime. Just as computers have helped the police in becoming more efficient, so too, have they assisted wary criminals in perpetrating a wide variety of crimes. This trend is likely to continue, and for that reason alone police investigators should make themselves better prepared for computer-related crime investigations.

The obvious choice for most police agencies is a combination of upgrading our technology along with an increase of our knowledge so that we become more efficient in our pursuits. Of course, this will vary according to specific needs of the department or the investigative unit. It is clear that a vice unit does not need an advanced computer system when making routine prostitution arrests, but it is equally clear that an investigator will need some computer knowledge if he is to track money transactions stored by pimps on laptop computers. Simply stated, the increased use of computers by traditional criminals significantly increases the need for investigators to be computer competent.

The above example illustrates a crime which is not traditionally considered a computer crime but which does involve the use of a computer. Basic computer knowledge may be all that is needed to conduct this investigation, but what about crimes where the computer is a substantial part of the *modus operandi*? In coming chapters we will examine this issue in much more detail, but for now it is important to recognize that computer crime extends far beyond the original definitions set out by the industry.

Another, and sometimes more pressing issue, which often arises focuses

on the logistics of computer use in both crime and criminal detection. A nagging question facing the police community today is whether police agencies expend significant man-hours and resources preparing for crimes that are often difficult to detect and even more difficult to prosecute? A better way to look at this issue is to ask whether traditional investigative techniques, those that are used in less technologically advanced crimes, are enough to determine who has released the latest virus?

The potential for computer crime is almost limitless. As computers invade more of our everyday lives the need for competent investigators grows. For each of the issues set out above the answers all appear to be relatively the same. In each instance we can find a need for increased knowledge as well as better technology. In other words, to be effective, investigators in today's climate must move ahead both in understanding technology and in their preparedness to investigate computer-related crime.

To better prepare we must focus on training that will upgrade our knowledge and skills. That is the purpose of this book. To begin this task we must first establish some basic guidelines so that all readers will advance significantly in their knowledge and skills. We do this by first establishing basic principles, definitions, and techniques. The first of these is a definition of computers and computer crime.

B. DEFINING COMPUTER AND TECHNOLOGY CRIME

Defining computers and computer-related crime might seem simple on the surface, but therein lays the difficulty of the task. If we define both too broadly then we risk creating a menace that never appears. Define the terms too narrowly and we chance missing the real problem when it comes. In order to hit the proverbial nail on the head we should start with a simple definition, refine it, and then establish a usable working definition that will serve our purposes.

The simplest definition we can use is that "computer crime is any crime involving a computer." Almost immediately one can see that such a simple definition creates critical problems. In our highly mechanized and computerized world to define computer crime so broadly would be to catalog almost any crime as a computer crime. After all, consider the number of appliances in our homes that have some sort of computer system built into them. Today it is hard to buy a microwave, refrigerator, dishwasher, or any other major appliance without having it operate with a *Central Processing Unit* (CPU) of some type.

One of the problems with such a broad definition is that the investigator spends more time defining the crime than investigating it. Imagine for a