

Contents

Foreword.....	iii
Technical Working Group for Electronic Crime Scene Investigation	v
Acknowledgments	xiii
Overview	1
The Law Enforcement Response to Electronic Evidence.....	1
The Latent Nature of Electronic Evidence	2
The Forensic Process.....	2
Introduction	5
Who Is the Intended Audience for This Guide?	5
What is Electronic Evidence?	6
How Is Electronic Evidence Handled at the Crime Scene?	6
Is Your Agency Prepared to Handle Electronic Evidence?.....	7
Chapter 1. Electronic Devices: Types and Potential Evidence	9
Computer Systems.....	10
Components.....	12
Access Control Devices.....	12
Answering Machines.....	13
Digital Cameras.....	13
Handheld Devices (Personal Digital Assistants [PDAs], Electronic Organizers).....	14
Hard Drives	15
Memory Cards.....	15
Modems.....	16
Network Components	16
Pagers	18
Printers.....	18
Removable Storage Devices and Media	19
Scanners.....	19
Telephones.....	20
Miscellaneous Electronic Items	20

Chapter 2. Investigative Tools and Equipment	23
Tool Kit	23
Chapter 3. Securing and Evaluating the Scene	25
Chapter 4. Documenting the Scene	27
Chapter 5. Evidence Collection	29
Nonelectronic Evidence	29
Stand-Alone and Laptop Computer Evidence	30
Computers in a Complex Environment	32
Other Electronic Devices and Peripheral Evidence	33
Chapter 6. Packaging, Transportation, and Storage	35
Chapter 7. Forensic Examination by Crime Category	37
Auction Fraud (Online)	37
Child Exploitation/Abuse	37
Computer Intrusion	38
Death Investigation	38
Domestic Violence	38
Economic Fraud (Including Online Fraud, Counterfeiting)	38
E-Mail Threats/Harassment/Stalking	39
Extortion	39
Gambling	39
Identity Theft	39
Narcotics	40
Prostitution	40
Software Piracy	41
Telecommunications Fraud	41
Appendix A. Glossary	47
Appendix B. Legal Resources List	53
Appendix C. Technical Resources List	55
Appendix D. Training Resources List	73
Appendix E. References	77
Appendix F. List of Organizations	81