Contents

1 **The Initial Contact**

2 **Client Site Arrival**

3 **Evidence Collection Procedures**
Detailed Procedures for Obtaining a Bitstream Backup of a Hard Drive

4 **Evidence Collection and Analysis Tools**
SafeBack
GetTime
FileList, FileCnvt, and Excel
GetFree
Swap Files and GetSwap
GetSlack
Temporary Files
Filter_I
Key Word Generation
TextSearch Plus
CRCMD5
DiskSig
Doc
Mcrypt
Micro-Zap
Map
M-Sweep
Net Threat Analyzer
AnaDisk
Seized
Scrub
Spaces
NTFS FileList
NTFS GetFree
NTFS GetSlack
NTFS View
NTFS Check
NTIcopy

©2002 CRC Press LLC

Disk Search 32
EnCase
Analyst's Notebook, iBase, and iGlass
BackTracing

5 Password Recovery

6 Questions and Answers by Subject Area
Evidence Collection
Legal
Evidence Analysis
UNIX
Military
Hackers
BackTracing
Logs
Encryption
Government
Networking
E-Mail
Usenet and IRC (Chat)

7 Recommended Reference Materials
PERL and C Scripts
UNIX, Windows, NetWare, and Macintosh
Computer Internals
Computer Networking
Web Sites of Interest

8 Case Study
Recommendations

Appendix A: Glossary

Appendix B: Port Numbers Used by Malicious Trojan Horse Programs

Appendix C: Attack Signatures

Appendix D: UNIX/Linux Commands

Appendix E: Cisco PIX Firewall Commands

Appendix F: Discovering Unauthorized Access to Your Computer

Appendix G: U.S. Department of Justice Search and Seizure Guidelines
Searching and Seizing Computers without a Warrant
Searching and Seizing Computers with a Warrant
The Electronic Communications Privacy Act
Electronic Surveillance in Communications Networks
Evidence
Appendices
Appendix A: Sample Network Banner Language
Appendix B: Sample 18 U.S.C § 2703(d) Application and Order
Appendix C: Sample Language for Preservation Request Letters Under U.S.C. § 2703(f)

©2002 CRC Press LLC

Appendix D: Sample Pen Register/Trap and Trace Application and Order
Appendix E: Sample Subpoena Language
Appendix F: Sample Language for Search Warrants and Accompanying Affidavits to Search and Seize Computers
Index.
Footnotes

The Author

©2002 CRC Press LLC