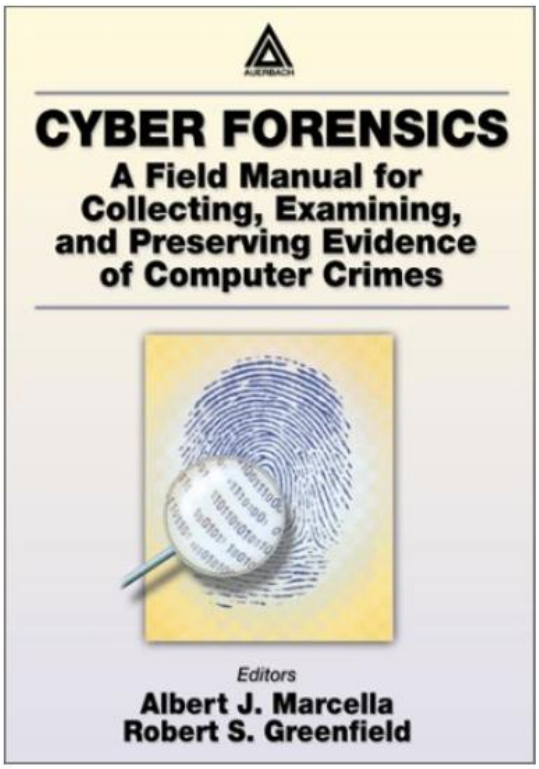

Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes

By Albert J. Marcella Jr & Robert S. Greenfield
Paperback / January 2002 / 0849309557
Link to Amazon

Table of Contents

Works Cited

Chapter 5: Tools of the Trade: Automated Tools Used to Secure a System Throughout the Stages of a Forensic Investigation
Overview
Detection Tools
Protection Tools
Analysis Tools

Chapter 6: Network Intrusion Management and Profiling
Overview
Common Intrusion Scenarios
Intrusion Profiling
Creating the Profile
Conclusion

Chapter 7: Cyber Forensics and the Legal System
Overview
How the System Works
Issues of Evidence
Hacker, Cracker, or Saboteur
Best Practices
Notes
Acknowledgments

Section II: Federal and International Guidelines
Chapter List
References

Chapter 8: Searching and Seizing Computers and Obtaining Electronic Evidence
Recognizing and Meeting Title III Concerns in Computer Investigations
Computer Records and the Federal Rules of Evidence
Proposed Standards for the Exchange of Digital Evidence
Recovering and Examining Computer Forensic Evidence
International Principles for Computer Evidence

Chapter 9: Computer Crime Policy and Programs
The National Infrastructure Protection Center Advisory 01.003
The National Information Infrastructure Protection Act of 1996
Distributed Denial of Service Attacks
The Melissa Virus
Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue

Chapter 10: International Aspects of Computer Crime
Council of Europe Convention on Cybercrime
Council of Europe Convention on Cybercrime Frequently Asked Questions
Internet as the Scene of Crime
Challenges Presented to Law Enforcement by High.Tech and Computer Criminals
Problems of Criminal Procedural Law Connected with Information Technology
Combating High.Tech and Computer.Related Crime
Vienna International Child Pornography Conference
OECD Guidelines for Cryptography Policy