IX 222 Computer Forensics

Textbook

Title: Guide to Computer forensics and Investigations Sixth Edition
Publisher: Cengage
By: Bill Nelson, Amelia Phillips and Chris Steuart
ISBN: 978-1-337-56894-4

Chapter 1, Understanding the Computer Forensics Profession

- Digital forensics profession
- Understanding Law enforcement
- Private Sector Investigations
- Computer Crimes

Chapter 2, Investigator's Office and Laboratory

- The Forensics lab
- People
- Equipment

Chapter 3, Data Acquisition

- Types of data storage
- Acquisition Methods
- Types of Acquisition Tools

Chapter 4, Processing Crimes and Incident Scenes

- Identifying Digital Evidence
- Private-Sector Incident Scenes
- Law Enforcement Crime Scenes
- Seizing Digital Evidence at the scene

Chapter 5, Working with Windows and CLI systems

- PC hardware basics
- Windows Operating system
- Understanding the Windows files systems
- Understanding Disk Encryption

Chapter 7, Working with Linux and Macintosh

- Linux hardware basics
- Linux Operating system
- Understanding the Linux files systems
- Forensics Procedures for Linux Computers
- Macintosh hardware basics
- Macintosh Operating system
- Understanding the Macintosh files systems
- Forensics Procedures for Macintosh computers

Chapter 6, Current Digital Forensics Tools

- Digital Forensics Hardware Tools
- Digital Forensics Software Tools

Chapter 8, Recovering Graphic Files

- Types of Graphic files
- Types of Video files

Chapter 9, Digital Forensics Analysis and Validation

- Determining What Data to collect

Chapter 10, Virtual Servers and Network Forensics

- Virtual Server Hypervisor
- Investigating Virtual Networks

Chapter 11, E-Mail and Social Media Investigations

- How e-mail systems work
- Role of E-Mail investigations

- Types of E-Mail crimes
- E-Mail Forensic Tools

Chapter 12, Mobile Device Forensics

- Mobile Phones
- Acquisition of data from Mobile Phone

Chapter 13, Cloud Forensics

- How Cloud Services work
- Cloud Services Forensics
- Legal Challenges in cloud computing

Chapter 16, Ethics in investigations

- Applying Ethics and Code to witnesses
- Organizations with Code of Ethics
- Ethical Responsibilities owed to people

Textbook

Title: Computer Forensics and Cyber Crime and Introduction 3rd Edition
Publisher: Pearson
By: Marjiet T. Britz
ISBN: 10: 0-13-267771-7

Chapter 1, Introduction and Overview of computer Forensics and Cybercrime

- Computer Crimes
- Physical and Jurisdictional Concerns
- Prosecutions
- e-cash

Chapter 2, Computer Terminology

- Computer History
- Computer Hardware
- Computer Software and operating systems
- History of the Internet
- How the Internet works

Chapter 3, Traditional computer Crime and Hackers

- What is Computer Crime
- Hacking
- Theft of Intellectual Property

Chapter 4, Contemporary Computer Crime

- Web-Based Crime
- Malware
- Spam
- Terrorism

Chapter 5, Identity Theft and Identity Fraud

- Types of Identity Theft
- Types of Mail Theft

Chapter 6, Terrorism and Organized Crime

- Types of Terrorism
- Terrorism online
- Terrorism and Crime
- Organized Crime

Chapter 7, Avenues for Prosecution and Government

- New Laws for Computer Crimes
- Child Pornography Statues
- Law Enforcement Operations
- International Effort

Chapter 8, Applying the First Amendment to Computer-Related Crime

- Obscenity in General
- Traditional Notions of Decency
- Criminalizing child Pornography
- Technology-Specific Legislation

Chapter 9, The Fourth Amendment and Other Legal Issues

- The Fourth Amendment
- Searches with and without Warrants
- Electronics Surveillance and Right to Privacy
- Private verses Public Sector Searches
- The Patriot Act

Chapter 11, Searching and Seizing Computer-Related Evidence

- Pre-Search activities
- On-Scene Activities

Chapter 12 Processing of Evidence and Report

- Establish a Sterile Lab
- Physical Examination
- Getting into the computer Windows, Linux and MacOS
- Examining the files in the computer

XI 222 Agenda

Lesson 1:

Chapter 1, Understanding the Computer Forensics Profession

- Digital forensics profession
- Understanding Law enforcement
- Private Sector Investigations
- Computer Crimes

Chapter 1, Introduction and Overview of computer Forensics and Cybercrime

- Computer Crimes
- Physical and Jurisdictional Concerns
- Prosecutions
- e-cash

Lesson 2:

Chapter 2, Computer Terminology

- Computer History
- Computer Hardware
- Computer Software and operating systems
- History of the Internet
- How the Internet works

Chapter 5, Working with Windows and CLI systems

- PC hardware basics
- Windows Operating system
- Understanding the Windows files systems
- Understanding Disk Encryption

Lesson 3:

Chapter 3, Traditional computer Crime and Hackers

- What is Computer Crime
- Hacking
- Theft of Intellectual Property

Lesson 4:

Chapter 4, Contemporary Computer Crime

- Web-Based Crime
- Malware
- Spam
- Terrorism

Chapter 5, Identity Theft and Identity Fraud

- Types of Identity Theft
- Types of Mail Theft

Chapter 4, Processing Crimes and Incident Scenes

- Identifying Digital Evidence
- Private-Sector Incident Scenes
- Law Enforcement Crime Scenes
- Seizing Digital Evidence at the scene

Lesson 5:

Chapter 7, Avenues for Prosecution and Government

- New Laws for Computer Crimes

- Child Pornography Statues
- Law Enforcement Operations
- International Effort

Lesson 6:

Chapter 3, Data Acquisition

- Types of data storage
- Acquisition Methods
- Types of Acquisition Tools

Chapter 4, Processing Crimes and Incident Scenes

- Identifying Digital Evidence
- Private-Sector Incident Scenes
- Law Enforcement Crime Scenes
- Seizing Digital Evidence at the scene

Chapter 11, Searching and Seizing Computer-Related Evidence

- Pre-Search activities
- On-Scene Activities

Lesson 7:

Chapter 12, Mobile Device Forensics

- Mobile Phones
- Acquisition of data from Mobile Phone

Chapter 13, Cloud Forensics

- How Cloud Services work
- Cloud Services Forensics
- Legal Challenges in cloud computing

Chapter 4, Contemporary Computer Crime

- Web-Based Crime
- Malware
- Spam
- Terrorism

Chapter 5, Identity Theft and Identity Fraud

- Types of Identity Theft
- Types of Mail Theft

Lesson 8 Topics for Final Projects:

Chapter 9, The Fourth Amendment and Other Legal Issues

- The Fourth Amendment
- Searches with and without Warrants
- Electronics Surveillance and Right to Privacy
- Private verses Public Sector Searches
- The Patriot Act