Exam 1 Topics:

- Chapter 1
  - What is the *Daubert standard*?
  - Explain the *chain of custody*.
  - What is *U.S. Federal Rule 702*?
  - What are some of the challenges related to computer system forensics?
  - List three types of digital system forensics analysis.
  - Can your roommate give consent to search your computer? Why or why not?

- Chapter 2
  - Explain what *cross-site scripting* is.
  - What is a *rainbow table* and how is it used in computer crime?
  - What is a *logic bomb* and how does this crime affect forensics?
  - Is *spyware* legal? Why or why not?

- Chapter 3
  - One forensic principle is *to handle original data as little as possible*. Why is this so important?
  - System forensics specialists must keep in mind three main technical data collection considerations. One of which is to consider the *life span of the information*. Explain why this is so important.
  - What is a *file slack* or *slack space*?
  - Why are *industry certifications* so important in digital forensics?
  - What is the purpose of the MD5 message-digest algorithm as it relates to digital forensics?

- Chapter 4
  - Explain the proper procedure when examining a suspect's machine. That is, describe the specific details to follow when collecting, seizing, and protecting evidence. Hint: think about (a) shutting down the computer, (b) what network connections the machine may have, (c) what open files or folder may be open and who has them open, (d) capturing what is in main memory, and (e) transporting the computer system to a secure location.
  - Describe how you can prove that you didn't alter any of the data on a storage device when conducting a forensic examination.
  - Describe the process of forensic imaging. Why is it important that you make a physical image of the drive before you begin your examination?

- Chapter 5
  - What is the difference between steganography and cryptography?

- One of the most common methods of hiding a message in a digital file is to use the least significant bit (LSB) method. Explain the LSB method and why it works so well.
- Explain which of these will be easier to perform steganalysis on (and why):
    a) A 10-kilobyte message in a 2-megabyte image file
    b) A 1-megabyte message in a 4-megabyte image file
- Explain what the Caesar Cipher is and how you might go about breaking this cipher.
- Describe the following cryptographic techniques:
    a) Known plaintext attack
    b) Chosen plaintext attack
    c) Ciphertext-only attack
- Modern cryptography is separated into two distinct groups: symmetric cryptography and asymmetric cryptography. Define and contrast each of these methods.
- Why will Quantum Computing have serious ramifications for widely used asymmetric cryptography algorithms?

Exam 2 Topics:

- Chapter 6
    - Explain what *File Carving* is.
    - What is *Zero-knowledge analysis*?
- Chapter 7
    - What is the relationship between incident response and forensics?
    - Describe what should be included in a *Business Continuity Plan* (BCP)?
    - Describe what should be included in a *Disaster Recovery Plan* (DRP)?
- Chapter 8
    - Describe what can be found in the *Windows Registry*? How many hives are in the Windows Registry?
- Chapter 11
    - What is the primary difference between *POP3* and *IMAP*?
    - What is *Anonymous Remailing*?
    - Describe some of the email headers that are not typically shown in simple email messages but are in the full header.
- Chapter 12
    - In mobile device forensics there are two primary types of extractions: *Logical Extractions* and *Physical Extractions.* Describe the difference between a Logical Extraction and a Physical Extraction.

- Chapter 13
  - The Honeynet Project is designed to help people learn the latest intrusion techniques that attackers are using. Conduct your own research to learn about the Honeynet Project and the tools and resources offered.
- Chapter 14
  - What is a DLL injection?