EC-Council CHFI Practice Exam (Sample)

Study Guide

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit: https://eccouncilchfi.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

SAMPLE

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

Questions

SAMPLE

1. **How should an incident responder describe a situation where port 80 is confirmed open but necessary for the server’s function?**

   A. Possible risk

   B. An exception

   C. Critical vulnerability

   D. Unusual condition

2. **What are "metadata" in the context of digital files?**

   A. Information about a file's creation, modification, and access

   B. Data that is encrypted within a file

   C. Content that defines the size of a file

   D. Unique identifiers for hardware components

3. **Which of the following would be MOST important to verify while conducting a business continuity review of a forensic service provider?**

   A. Data encryption protocols

   B. Human safety procedures are in place

   C. Client confidentiality measures

   D. Backup storage locations

4. **Which area of physical security is the most crucial in a digital forensics facility according to a crime lab auditor's review?**

   A. The exit door is secured

   B. The exit door is blocked

   C. All windows are locked

   D. Access control is enforced

5. **Which standard is based on legal precedent regarding the admissibility of scientific examinations or experiments?**

   A. Daubert Standard

   B. Frye Standard

   C. Hearsay Rule

   D. Expert Testimony Rule

SAMPLE

6. Which of the following is a key principle in computer forensics?

- **A. The principle of maintaining a secure record of the evidence chain of custody**
- **B. The principle of conducting interviews with witnesses**
- **C. The principle of public disclosure of findings**
- **D. The principle of avoiding any technical restrictions**

7. What is the primary purpose of a digital forensics report?

- **A. To provide a summary of law enforcement procedures**
- **B. To document findings and methodology of the investigation**
- **C. To analyze the suspect's behavior**
- **D. To create a backup of digital evidence**

8. What is a common method for preventing data loss during an investigation?

- **A. Using unencrypted storage media**
- **B. Avoiding the use of data recovery tools**
- **C. Implementing proper handling techniques**
- **D. Storing evidence in cloud services**

9. Which term describes hacking that may not be malicious but violates laws or ethical standards?

- **A. Black hat hacking**
- **B. White hat hacking**
- **C. Gray hat hacking**
- **D. Red team hacking**

10. What is the difference between "active" and "passive" data collection?

- **A. Active collection uses physical devices, while passive does not**
- **B. Active collection involves using tools to extract data, while passive collection involves monitoring without intervention**
- **C. Active collection is more reliable than passive collection**
- **D. Active collection occurs in real-time, while passive is retrospective**

SAMPLE

Answers

SAMPLE

1. B
2. A
3. B
4. B
5. B
6. A
7. B
8. C
9. C
10. B

SAMPLE

Explanations

SAMPLE

1. How should an incident responder describe a situation where port 80 is confirmed open but necessary for the server’s function?

A. Possible risk

B. An exception

C. Critical vulnerability

D. Unusual condition

In the context of an incident responder evaluating the significance of an open port 80, which is typically used for HTTP traffic, describing it as an exception is the most appropriate approach. Port 80 being open is standard for web servers, as it allows users to access web applications and services. If port 80 is confirmed open and is necessary for the server's operational functionality, it indicates that this setup is expected and acceptable for the given context. Hence, it should be viewed as an exception to any general rules or policies that might flag open ports as potential risks. In cybersecurity, an exception implies that while there may be a general guideline regarding port security, this particular instance is justified due to the operational requirements of the server. The other choices may imply levels of risk or concern that are not applicable in this scenario since port 80 is intrinsic to the server's role, and thus, labeling it as a possible risk, critical vulnerability, or unusual condition does not accurately reflect the normative status of this port in a web server environment.

2. What are "metadata" in the context of digital files?

A. Information about a file's creation, modification, and access

B. Data that is encrypted within a file

C. Content that defines the size of a file

D. Unique identifiers for hardware components

Metadata refers to the supplementary information that describes various attributes of a digital file, such as its creation date, modification date, and access permissions. This information provides context about the file beyond just its content, enabling a deeper understanding of the file's origins and history. In digital forensics, metadata plays a crucial role in reconstructing events surrounding a file, such as when it was created or last altered, which can be essential in investigations. For example, when examining a document file, a forensic analyst can determine who created the file, when it was last modified, and even who accessed it. This capability allows investigators to piece together timelines and actions relevant to the case at hand. In contrast, the other options do not accurately describe metadata. Data that is encrypted within a file pertains to the security of that file rather than information about it. Content that defines the size of a file is related to the file's attributes but does not encompass the broader scope of metadata. Unique identifiers for hardware components relate to physical devices rather than digital files and their characteristics. Thus, the focus on creation, modification, and access information distinctly qualifies option A as the correct answer in the context of metadata in digital files.

SAMPLE

3. Which of the following would be MOST important to verify while conducting a business continuity review of a forensic service provider?

A. Data encryption protocols

B. Human safety procedures are in place

C. Client confidentiality measures

D. Backup storage locations

In the context of conducting a business continuity review of a forensic service provider, verifying human safety procedures is crucial because the primary focus of any business continuity plan is to ensure the safety and well-being of all personnel during and after an incident. This includes creating environments that protect employees from potential harm, especially in scenarios where investigations may involve hazardous materials or situations (such as cyber incidents leading to physical breaches). When a forensic service provider deals with evidence recovery, it is essential that all staff members can safely conduct their investigations without exposing themselves to risks. This includes comprehensive training and protocols for emergency situations, ensuring that human safety remains a top priority in the overall business continuity strategy. Additionally, a focus on human safety directly supports the operational integrity; without a safe workforce, the provider cannot effectively serve its clients or uphold its responsibilities. While other aspects, such as client confidentiality measures and data encryption protocols, are indeed important for the integrity and security of the data being handled, the immediate priority in a business continuity context is ensuring that personnel can work without risk to their safety. Likewise, backup storage locations are critical for data integrity but addressing human safety first ensures that the business can continue to function effectively in the face of challenges.

4. Which area of physical security is the most crucial in a digital forensics facility according to a crime lab auditor's review?

A. The exit door is secured

B. The exit door is blocked

C. All windows are locked

D. Access control is enforced

In a digital forensics facility, enforcing access control is paramount to maintaining the integrity of evidence and ensuring that only authorized personnel can enter sensitive areas. This aspect of physical security helps protect against unauthorized access, which could lead to tampering, contamination, or loss of critical data. Proper access control measures can include badge systems, biometric scanners, and visitor logs, which are essential for tracking who has entered and exited the facility. While securing exit doors and locking windows are also important components of physical security, they do not address the primary concern of access control that is critical to a forensic environment. Blocking an exit door, however, represents a breach of security protocol and could lead to serious safety hazards, making it an inappropriate choice in the context of a facility that strives to uphold the highest security standards. Access control ensures the chain of custody is maintained, which is vital for the validity of any forensic investigation.

SAMPLE

5. Which standard is based on legal precedent regarding the admissibility of scientific examinations or experiments?

A. Daubert Standard

B. Frye Standard

C. Hearsay Rule

D. Expert Testimony Rule

The Frye Standard is based on legal precedent and focuses on the admissibility of scientific examinations or experiments in court. Established in 1923 through the case Frye v. United States, this standard dictates that scientific evidence must be sufficiently established and accepted within the relevant scientific community to be considered admissible in court. According to this standard, if the methodology or techniques employed do not have widespread acceptance among experts in the field, the evidence may be deemed inadmissible. This principle emphasizes the importance of peer validation within the scientific community and serves to ensure that only reliable and proven scientific techniques underlie evidence presented during legal proceedings. The Frye Standard has been influential in shaping how courts interact with scientific evidence and has been used as a benchmark for determining its reliability and relevance. In contrast, the Daubert Standard, which evolved later, is more flexible and focuses on the reliability and relevance based on the specific circumstances of the evidence and its methodology, which may include factors like testability, peer review, and error rates. The Hearsay Rule and the Expert Testimony Rule deal with different aspects of law regarding witness statements and the qualifications of experts, respectively, rather than the foundational scientific acceptance necessary for evidence admissibility.

6. Which of the following is a key principle in computer forensics?

A. The principle of maintaining a secure record of the evidence chain of custody

B. The principle of conducting interviews with witnesses

C. The principle of public disclosure of findings

D. The principle of avoiding any technical restrictions

The principle of maintaining a secure record of the evidence chain of custody is fundamental in computer forensics because it ensures that all evidence collected during an investigation is preserved, authenticated, and verifiable. This chain of custody documentation provides a detailed account of who collected the evidence, how it was handled, and where it was stored, which is essential for maintaining the integrity of the evidence. If the chain of custody is compromised, the admissibility and reliability of the evidence in a legal context may be questioned, potentially impacting the outcome of investigations or legal proceedings. This principle is crucial for ensuring that findings are based on reliable evidence and that they can withstand scrutiny in court. Properly documenting the chain of custody allows forensic investigators to demonstrate that the evidence has not been tampered with or altered, thus upholding the standards of the forensic discipline. Other principles mentioned, such as conducting interviews and public disclosure of findings, do play roles in investigations and forensic work but do not have the same level of significance in terms of evidence integrity and legal compliance.

SAMPLE

7. What is the primary purpose of a digital forensics report?

A. To provide a summary of law enforcement procedures

B. To document findings and methodology of the investigation

C. To analyze the suspect's behavior

D. To create a backup of digital evidence

The primary purpose of a digital forensics report is to document findings and methodology of the investigation. This report serves as a comprehensive record of the evidence collected, the procedures followed during the investigation, and the analysis performed. It is crucial for ensuring that the investigation is transparent and reproducible, as well as for maintaining the integrity of the evidence in legal contexts. Such reports outline the steps taken during the analysis, the tools and techniques used, and the conclusions drawn from the data. This documentation is essential for legal proceedings, as it provides a clear account of how the evidence was handled, ensuring that it adheres to legal standards and can withstand scrutiny in court. Thus, the report plays a vital role in bridging the gap between technical findings and legal requirements, supporting the legitimacy of the investigative process. Other options do not encapsulate the primary function of a digital forensics report. Summarizing law enforcement procedures does not address the specific findings from the investigation or the methods used. Analyzing the suspect's behavior, while potentially relevant, is only a part of what may be covered in a digital forensics investigation but is not the core purpose of the report. Creating a backup of digital evidence pertains more to data preservation and management than to documenting the

8. What is a common method for preventing data loss during an investigation?

A. Using unencrypted storage media

B. Avoiding the use of data recovery tools

C. Implementing proper handling techniques

D. Storing evidence in cloud services

Implementing proper handling techniques is essential for preventing data loss during an investigation. This includes following a structured chain of custody, using write blockers when accessing storage media, and ensuring that evidence is stored securely and documented thoroughly. By adhering to these techniques, investigators can maintain the integrity of the data and reduce the risk of unintentional alteration or damage. The other options present methods that could lead to data loss rather than prevent it. Unencrypted storage media can expose sensitive information to unauthorized access or loss. Avoiding data recovery tools may hinder the ability to retrieve deleted files, which is critical in many investigations. Relying solely on cloud services for evidence storage could introduce risks related to data integrity and availability if the cloud service fails or is compromised. Overall, the emphasis on proper handling techniques is foundational for maintaining the reliability of evidence in digital investigations.

SAMPLE

9. Which term describes hacking that may not be malicious but violates laws or ethical standards?

A. Black hat hacking

B. White hat hacking

C. Gray hat hacking

D. Red team hacking

The term that describes hacking which may not be malicious but still violates laws or ethical standards is gray hat hacking. Gray hat hackers typically operate in a space between ethical (white hat) and unethical (black hat) hacking. They may exploit vulnerabilities in a system without permission, but their intent often is not to cause harm or steal information; rather, they might aim to highlight these vulnerabilities to the owner of the system, sometimes even without their knowledge, and may offer to fix the issues. This behavior creates a gray area—hence the name "gray hat"—where the hacker's actions are technically illegal (due to unauthorized access), yet the intention is often benign. For example, if a gray hat hacker discovers a security flaw in a website and informs the company about it, while their method of discovering the flaw might involve illegal access, their goal is to improve security, not to exploit it. Other terms in the options refer to different types of hacking with clearer motivations. Black hat hacking refers to malicious activities with the intent to steal or harm, while white hat hacking is ethical hacking for defensive purposes, often with permission. Red team hacking involves testing defense mechanisms through simulated attacks, generally in a controlled and authorized manner.

10. What is the difference between "active" and "passive" data collection?

A. Active collection uses physical devices, while passive does not

B. Active collection involves using tools to extract data, while passive collection involves monitoring without intervention

C. Active collection is more reliable than passive collection

D. Active collection occurs in real-time, while passive is retrospective

The distinction between "active" and "passive" data collection is primarily centered around the methodology employed to gather data. Active collection involves an intentional effort to extract information using specific tools or methods, which might include surveys, experiments, or direct querying of a database. This means that the data collector engages with the system or subjects to gather the desired information, often leading to more targeted and potentially richer data sets. In contrast, passive data collection refers to monitoring existing data without making any active intervention or inquiries. This method often relies on observing and recording data from a system or environment without influencing it. For example, logging network traffic or monitoring user behavior without asking for direct input from users would be considered passive collection. This approach provides insights based on what already exists, often enabling the gathering of large volumes of data without direct interaction. The other choices present common misunderstandings or oversimplifications of the concepts involved. While the reliability of data collection methods can vary, it's not inherently accurate to assert that one is categorically more reliable than the other; reliability depends on various factors including context and implementation. Additionally, the notion that active collection uses physical devices or that it occurs in real-time is not universally true, as both methods can utilize a range of tools and

SAMPLE

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://eccouncilchfi.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE