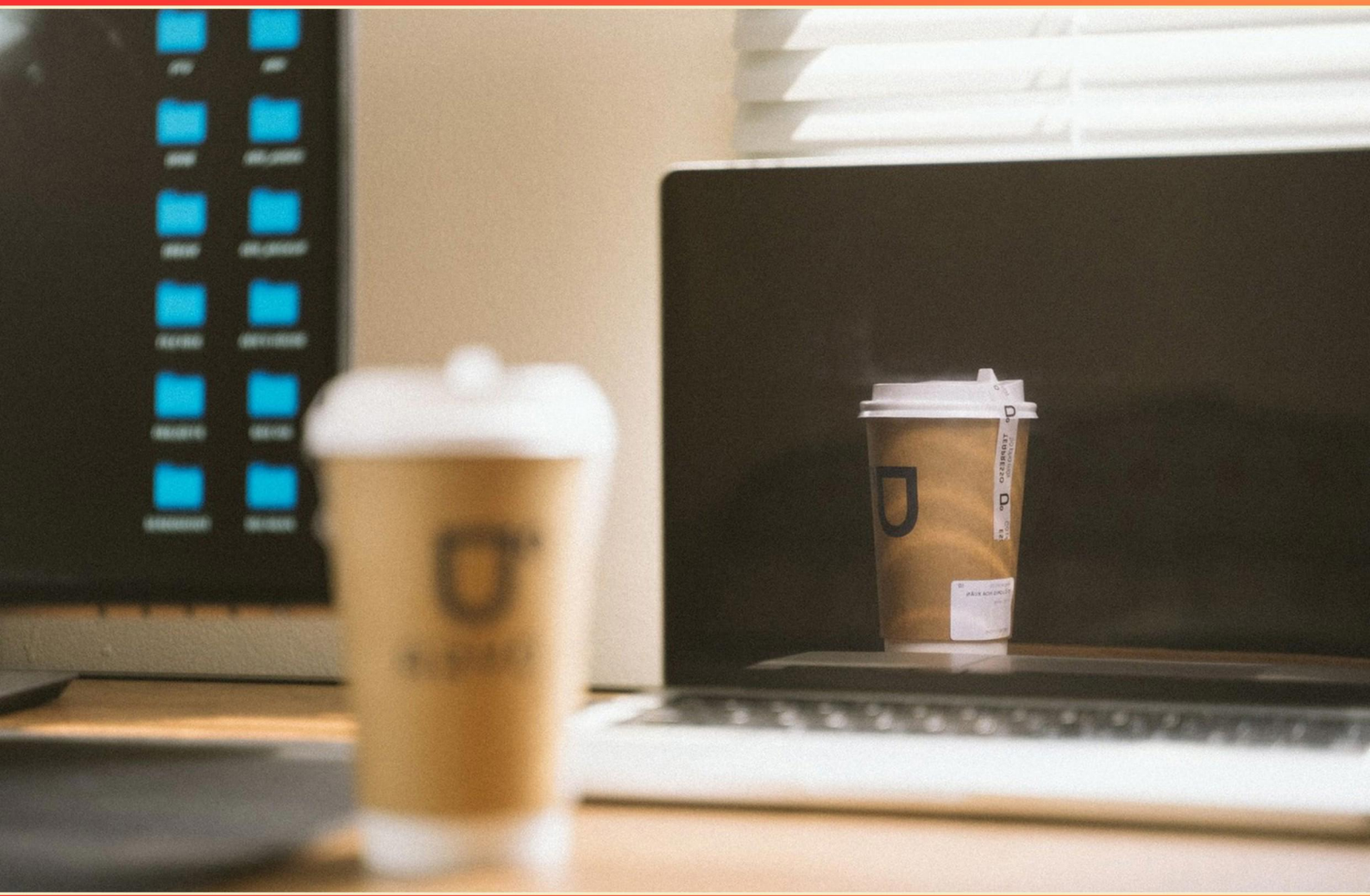
COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI) PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://chfi.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

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

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. What is the definition of a cold boot?

A. Starting a computer from a powered-down state

B. Restarting a computer already turned on

C. Shutting down a computer that is already on

D. Restarting a computer from sleep mode

2. In the logon event ID table, which event ID indicates a successful login?

A. 528

B. 529

C. 530

D. 531

3. Hard disk data addressing assigns addresses to each _____ of data on a hard disk.

A. Physical block

B. Logical block

C. Operating system block

D. Hard disk block

4. What is the purpose of MD5 checksum in forensic investigations?

A. To create an image of the disk

B. To verify the integrity of the evidence

C. To recover deleted files

D. To analyze network traffic

5. Which type of passwords are transmitted in clear text over networks?

A. Clear text passwords

B. Obfuscated passwords

C. Hashed passwords

D. Hex passwords

6. Which of the following describes the process of forensic investigation?

A. A systematic approach to identifying and collecting evidence

B. A random sampling of electronic data

C. An unstructured analysis of information

D. An assessment of potential security vulnerabilities

SAMPLE

7. Which of the following represents a common form of data encryption?

A. MD5 hashing

B. AES encryption

C. Base64 encoding

D. Hexadecimal conversion

8. Which statement is true about rogue access points?

A. They are authorized by the network provider

B. They pose a security risk as they are unauthorized

C. They operate within normal security protocols

D. They are only a concern on non-corporate devices

9. Which of the following best defines the purpose of session management in web applications?

A. To improve site performance

B. To manage visitor traffic

C. To maintain a user's state across interactions

D. To store user data securely

10. Which registry key should be checked to find values typed into the Run box in the Start menu?

A. UserAssist Key

B. MountedDevices key

C. RunMRU key

D. TypedURLs key

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the definition of a cold boot?

A. Starting a computer from a powered-down state

B. Restarting a computer already turned on

C. Shutting down a computer that is already on

D. Restarting a computer from sleep mode

The definition of a cold boot refers to the process of starting a computer from a powered-down state. This is the action taken when the machine is completely off and requires a full initialization of the hardware and operating system as it powers up. During a cold boot, the system undergoes a Power-On Self-Test (POST) to check for hardware functionality and then loads the operating system from the storage device. In contrast, restarting a computer already turned on, shutting down a computer that is already on, or restarting a computer from sleep mode all involve states where the system retains some level of operational readiness. These processes do not require reinitialization of the hardware in the same manner as a cold boot. Therefore, the essence of a cold boot lies in the fact that the computer is completely powered down prior to starting, contrasting with the other options that involve the machine being in an operational state.

2. In the logon event ID table, which event ID indicates a successful login?

A. 528

B. 529

C. 530

D. 531

In the context of event logging, a successful login is crucial for understanding user activity and security incidents. Event ID 528 is specifically designated to indicate a successful logon event in security audit logs on Windows systems. This identification helps system administrators and security professionals trace back actions taken by users, ensuring that only authorized personnel are accessing critical resources. When analyzing security logs, it's vital to monitor these successful login events carefully, as they form part of the overall audit trail necessary for validating user actions and detecting potential unauthorized access attempts. Understanding the event IDs associated with different login scenarios allows effective incident response and enhances security measures within an organization. The other event IDs (529, 530, and 531) describe different scenarios concerning login attempts, such as failed logins or logins with issues, thus underscoring the importance of distinguishing between successful and unsuccessful access events in security monitoring.

SAMPLE

3. Hard disk data addressing assigns addresses to each _____ of data on a hard disk.

A. Physical block

B. Logical block

C. Operating system block

D. Hard disk block

The correct answer is based on the fact that hard disk data addressing specifically refers to the way data is organized and accessed at the hardware level. Each physical block of data on a hard disk has a unique address that the disk controller uses to read or write data. These physical blocks are the actual locations on the disk platters where data is stored, and understanding this addressing scheme is crucial for forensic investigators when recovering or analyzing disk data. In contrast, logical blocks can refer to how the operating system views and interacts with the disk's data; while this abstraction simplifies data management for the user, it does not directly correspond to the physical arrangement of data on the hardware itself. Similarly, the term "operating system block" isn't a recognized term in the context of hard disk data addressing. Lastly, "hard disk block" sounds similar to physical block but isn't the standard terminology used to describe data addressing in the context of hard disk technology. Hence, the focus on physical blocks is essential for accurate data addressing and retrieval in computer forensics.

4. What is the purpose of MD5 checksum in forensic investigations?

A. To create an image of the disk

B. To verify the integrity of the evidence

C. To recover deleted files

D. To analyze network traffic

The purpose of the MD5 checksum in forensic investigations is primarily to verify the integrity of the evidence. When data is collected from digital devices, it is crucial to ensure that the data remains unchanged from the time of collection to the time of analysis and presentation in court. The MD5 checksum serves as a unique fingerprint for a specific set of data. By generating a checksum value for the original data and then calculating the checksum for the data later in the investigative process, forensic analysts can compare these values. If the MD5 checksum values match, it confirms that the data has not been altered or corrupted during collection, storage, or analysis. This process is critical in maintaining the chain of custody, establishing that the evidence presented is authentic and can be trusted. Thus, the use of MD5 checksums is a fundamental practice in digital forensics to uphold the integrity of the investigation.

SAMPLE

5. Which type of passwords are transmitted in clear text over networks?

A. Clear text passwords

B. Obfuscated passwords

C. Hashed passwords

D. Hex passwords

Clear text passwords are indeed transmitted in clear text over networks, meaning they are sent without any encryption or transformation that would obscure their content. This makes them vulnerable to interception by anyone monitoring the network traffic. When passwords are transmitted in this manner, any user with access to the communication channel can easily read and capture them, which poses a significant security risk. In contrast, obfuscated passwords typically involve some form of encoding or masking that makes them less readable, though not necessarily secure. Hashed passwords undergo a transformation to create a fixed-size string that obscures the original password, but they are not suitable for transmission as-is since they cannot be easily reversed unless additional information is provided. Hex passwords, while potentially part of a representation format, do not imply that the passwords are secure in transit and can also be vulnerable. Thus, the characteristic of clear text passwords being sent without any protective measures is what makes them the correct identification in this context.

6. Which of the following describes the process of forensic investigation?

A. A systematic approach to identifying and collecting evidence

B. A random sampling of electronic data

C. An unstructured analysis of information

D. An assessment of potential security vulnerabilities

The process of forensic investigation is fundamentally rooted in the principles of systematically identifying, preserving, and collecting evidence to ensure that it can be effectively analyzed and presented in a court of law. This methodical approach is crucial for maintaining the integrity of the evidence, as it minimizes the risk of contamination or loss, which can occur if a random or unstructured methodology is employed. Systematic procedures typically involve the establishment of a clear protocol for collecting digital evidence, including the use of specialized tools designed to preserve the data in its original state, and documenting each step taken during the investigation. This attention to detail is essential in ensuring that the findings can withstand legal scrutiny and are admissible in court. Random sampling, unstructured analysis, and assessments based on potential security vulnerabilities, while they may be elements of broader information security practices, do not capture the critical aspect of forensic investigation, which prioritizes accuracy, reliability, and adherence to legal standards. Therefore, the correct choice accurately reflects the structured nature of forensic investigations, highlighting the importance of thorough evidence handling.

SAMPLE

7. Which of the following represents a common form of data encryption?

A. MD5 hashing

B. AES encryption

C. Base64 encoding

D. Hexadecimal conversion

The correct choice represents a widely recognized and robust form of encryption. AES (Advanced Encryption Standard) is a symmetric encryption algorithm that encrypts data in fixed block sizes (typically 128 bits) using key sizes of 128, 192, or 256 bits. It uses the same key for both encryption and decryption, making it efficient for securing sensitive information. AES is widely adopted across various industries due to its security strength and performance, and it is often the encryption standard used for data protection in government, financial, and personal applications. While MD5 hashing is often mentioned in discussions about data security, it is actually a hashing algorithm rather than an encryption method, and it is not suitable for data encryption because it is a one-way function. Base64 encoding is primarily used for encoding binary data into ASCII text format and does not provide encryption; it merely allows for data representation. Hexadecimal conversion entails representing binary data in a human-readable format, which does not provide security or confidentiality. Thus, AES encryption stands out as an appropriate choice for data encryption, ensuring the confidentiality and integrity of data.

8. Which statement is true about rogue access points?

A. They are authorized by the network provider

B. They pose a security risk as they are unauthorized

C. They operate within normal security protocols

D. They are only a concern on non-corporate devices

Rogue access points pose a significant security risk because they are unauthorized devices that can connect to a legitimate network, bypassing normal security practices. These access points can be set up by malicious actors to intercept sensitive information, launch man-in-the-middle attacks, or allow unauthorized users to access the corporate network. Unlike authorized access points, rogue access points are not managed or monitored by the network provider, which prevents the organization from enforcing security measures effectively. By posing as legitimate access points, these rogue devices can trick users into connecting to them, often leading to data breaches or the compromise of network integrity. This risk is particularly prevalent in environments where users may unknowingly connect their devices to unfamiliar networks, making awareness and mitigation strategies essential for network security.

SAMPLE

9. Which of the following best defines the purpose of session management in web applications?

A. To improve site performance

B. To manage visitor traffic

C. To maintain a user's state across interactions

D. To store user data securely

The purpose of session management in web applications is primarily to maintain a user's state across interactions. This is essential because web applications are typically stateless, meaning that each request from a user is treated independently, without retaining information about previous interactions. Session management allows the application to remember user-specific data such as login status, preferences, and activities throughout their visit. For instance, when a user logs into a web application, session management creates a session that tracks that user's activities and behaviors. This session enables the application to identify the user in subsequent requests, allowing for a seamless experience, such as staying logged in, retaining user preferences, and maintaining a shopping cart in an e-commerce scenario. The other options represent important aspects of web application operation but do not define the core purpose of session management. While improving site performance and managing visitor traffic can enhance the overall user experience, these are not the primary goals of session management itself. Similarly, securely storing user data is crucial for application security, but it does not primarily encompass the functions of session management, which is more focused on maintaining state rather than data storage.

10. Which registry key should be checked to find values typed into the Run box in the Start menu?

A. UserAssist Key

B. MountedDevices key

C. RunMRU key

D. TypedURLs key

The RunMRU key is the correct choice because it specifically stores the Most Recently Used (MRU) list of commands that have been executed through the Run dialog box in the Windows operating system. When a user types a command into the Run box and executes it, that command is recorded within this registry key, allowing investigators to uncover what programs or paths a user has recently accessed. This information can be crucial in forensic investigations as it provides insights into user activity and can help establish patterns of behavior or intent. In contrast, the UserAssist key tracks applications that users have executed but does not specifically focus on the Run dialog entries. The MountedDevices key is related to devices that have been connected to the computer, not user activity through the Run command. The TypedURLs key tracks URLs entered into browsers, hence it is irrelevant when searching for commands used in the Run box. Understanding the specific purpose of these registry keys helps forensic analysts extract pertinent information during an investigation.

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://chfi.examzify.com

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

SAMPLE