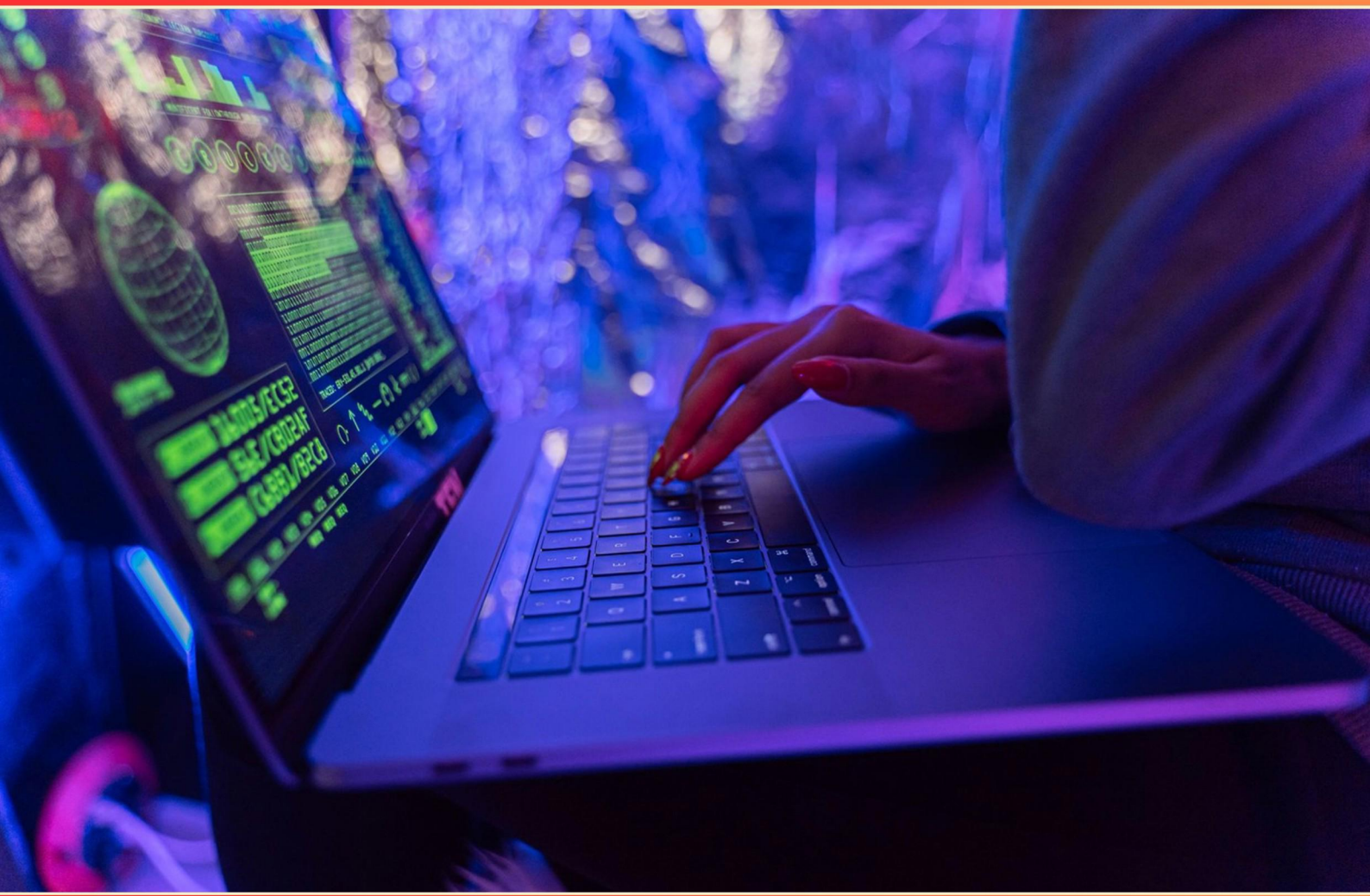
COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI) V11 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://chfiv11.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 15

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 primary purpose of an electronic crime scene checklist?**

   A. Locate and help the victim

   B. Transmit flash messages to other units

   C. Blog about the incident

   D. Advertise incident response services

2. **In a forensic ISO image, which artifact is most likely to indicate the source medium type?**

   A. Disc descriptor in the ISO9660 volume descriptor

   B. NTFS file creation times

   C. Master Boot Record on the host disk

   D. Slack space on a FAT32 partition

3. **Which statement about a forensic tool's capability is true?**

   A. EnCase can only search MFT

   B. EnCase cannot search Slack space

   C. EnCase primarily analyzes the registry

   D. EnCase can search NTFS MFT and Slack Space to recover files

4. **Temporal Key Integrity Protocol (TKIP) enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. Temporal keys are changed for every _____.**

   A. 5,000 packets

   B. 10,000 packets

   C. 15,000 packets

   D. 20,000 packets

5. **Technical Steganography is defined as steganography that uses which method to hide a message?**

   A. Linguistic Steganography uses natural language

   B. Technical Steganography uses physical or chemical means to hide messages

   C. Computer-based Steganography uses software only

   D. Visual Steganography uses colors only

SAMPLE

6. What is the outcome of executing a vulnerable login query that ends with DROP TABLE members;--' in the same batch as a SELECT query?

A. Deletes the entire members table

B. Retrieves the password for the first user in the members table

C. This command will not produce anything since the syntax is incorrect

D. Inserts the Error! Reference source not found. email address into the members table

7. Which of the following should a computer forensics lab used for investigations have?

A. isolation

B. restricted access

C. open access

D. an entry log

8. An image is an artifact that reproduces the likeness of some subject. These are produced by optical devices (i.e. cameras, mirrors, lenses, telescopes, and microscopes). Which property of the image shows you the number of colors available for each pixel in an image?

A. Pixel

B. Bit Depth

C. File Formats

D. Image File Size

9. Which statement does not support the case assessment?

A. Review the case investigator's request for service

B. Identify the legal authority for the forensic examination request

C. Do not document the chain of custody

D. Discuss whether other forensic processes need to be performed on the evidence

10. If a file of 2600 bytes on a hard disk uses 512-byte sectors, how many sectors are normally allocated to the file?

A. 4 Sectors

B. 5 Sectors

C. 7 Sectors

D. 6 Sectors

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the primary purpose of an electronic crime scene checklist?

A. Locate and help the victim

B. Transmit flash messages to other units

C. Blog about the incident

D. Advertise incident response services

The main idea is that an electronic crime scene checklist is a field tool used to guide responders to safely and systematically handle an incident, with locating and assisting anyone affected as the immediate priority. When responders arrive, the first steps focus on finding victims, assessing safety, and ensuring people are helped, before moving on to preserve and document digital evidence. That emphasis on helping people at the scene is why locating and helping the victim is the best answer. The other options describe activities (sending messages, blogging, advertising services) that aren't the primary purpose of the checklist.

2. In a forensic ISO image, which artifact is most likely to indicate the source medium type?

A. Disc descriptor in the ISO9660 volume descriptor

B. NTFS file creation times

C. Master Boot Record on the host disk

D. Slack space on a FAT32 partition

In an ISO 9660 image, the metadata stored in the volume descriptors describes the disc as it was created, including information about the medium. The disc descriptor within the ISO9660 volume descriptor directly encodes the type of medium (for example, CD-ROM, CD-R, DVD-ROM) and related characteristics. This makes it the most reliable artifact for inferring the source medium type when analyzing the image, because it is specifically designed to capture the nature of the physical disc that was used. Other artifacts don't serve this purpose as directly. NTFS file creation times pertain to a Windows file system and may not even be present in a standard ISO9660 image. The Master Boot Record on the host disk is outside the ISO image itself, so it won't reveal the image's source medium. Slack space on a FAT32 partition relates to a particular partition's unused space and isn't indicative of the medium that produced the ISO.

3. Which statement about a forensic tool's capability is true?

A. EnCase can only search MFT

B. EnCase cannot search Slack space

C. EnCase primarily analyzes the registry

D. EnCase can search NTFS MFT and Slack Space to recover files

NTFS stores file metadata in the Master File Table, and there's often data lingering in slack space—the unused portion of a cluster after a file has been written. A capable forensic tool like EnCase can search both the MFT and slack space to locate evidence and recover files, including those that have been deleted or partially overwritten. This dual capability is what makes the statement true: it isn't limited to one area but can systematically examine key NTFS structures to reconstruct or retrieve data. The other options misstate EnCase's scope, such as claiming it can only search MFT, that it cannot search slack space, or that its primary focus is registry analysis, which isn't its main role in most investigations.

SAMPLE

4. Temporal Key Integrity Protocol (TKIP) enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. Temporal keys are changed for every _____.

A. 5,000 packets

B. 10,000 packets

C. 15,000 packets

D. 20,000 packets

Temporal Key Integrity Protocol uses a rekeying mechanism to limit the amount of data encrypted with a single Temporal Key. After a set number of frames are processed, a new Temporal Key is generated and used for subsequent frames. That threshold is 10,000 packets, so temporal keys are changed after every 10,000 packets. This buffering helps contain potential key exposure by ensuring keys aren't reused for long stretches, improving resilience against certain attacks.

5. Technical Steganography is defined as steganography that uses which method to hide a message?

A. Linguistic Steganography uses natural language

B. Technical Steganography uses physical or chemical means to hide messages

C. Computer-based Steganography uses software only

D. Visual Steganography uses colors only

Technical Steganography hides a message by exploiting physical or chemical properties of materials, rather than by concealing data in text or digital files. This includes things like microdots, invisible or special inks, alterations to the material itself, or other methods that require physical or chemical manipulation to reveal the hidden information. Because its defining feature is the use of non-digital, tangible means, it stands apart from linguistic steganography (which hides in natural language), visual steganography (which hides in images or visuals), and computer-based steganography (which hides within digital data using software). That physical/chemical basis is why the description involving physical or chemical means is the best fit.

6. What is the outcome of executing a vulnerable login query that ends with DROP TABLE members;--' in the same batch as a SELECT query?

A. Deletes the entire members table

B. Retrieves the password for the first user in the members table

C. This command will not produce anything since the syntax is incorrect

D. Inserts the Error! Reference source not found. email address into the members table

This question tests how SQL injection can run multiple statements in one batch. In a vulnerable login query, an attacker can finish the first SELECT with a semicolon, then append a second statement. The "--" comments out the rest of the line, ensuring the injected part isn't rejected by trailing syntax. If the database user has permission and the API allows multiple statements per call, the second statement (DROP TABLE members) executes and deletes the entire table. That's why the outcome is the deletion of the members table.

SAMPLE

7. Which of the following should a computer forensics lab used for investigations have?

A. isolation

B. restricted access

C. open access

D. an entry log

Access control in a computer forensics lab is essential to preserve the integrity of evidence and maintain a solid chain of custody. By restricting entry to authorized personnel, only trained and vetted individuals can handle devices, access data, and perform procedures. This minimizes the risk of tampering, contamination, or accidental modification, and it makes it possible to clearly document who interacted with evidence and when. An entry log often accompanies restricted access, providing a verifiable record that supports the chain of custody. Isolation of the lab from external networks is important for security, but it addresses different risks than who is allowed inside. Open access would undermine the core need to protect evidence.

8. An image is an artifact that reproduces the likeness of some subject. These are produced by optical devices (i.e. cameras, mirrors, lenses, telescopes, and microscopes). Which property of the image shows you the number of colors available for each pixel in an image?

A. Pixel

B. Bit Depth

C. File Formats

D. Image File Size

Color information for each picture element is defined by bit depth. Bit depth is how many bits are used to represent the color of each pixel, so it determines how many distinct colors can appear per pixel. For example, 8 bits per channel in an RGB image means 8 bits for red, 8 for green, and 8 for blue, totaling 24 bits per pixel and about 16.7 million possible colors. Higher bit depth allows more colors and smoother color transitions. A pixel is simply a location in the image where color data is stored, not the amount of color information itself. File formats describe how data is encoded and stored, sometimes supporting different color depths, but the number of colors per pixel comes from bit depth. Image file size varies with resolution, color depth, and compression, and does not alone indicate how many colors per pixel are available.

SAMPLE

9. Which statement does not support the case assessment?

A. Review the case investigator's request for service

B. Identify the legal authority for the forensic examination request

C. Do not document the chain of custody

D. Discuss whether other forensic processes need to be performed on the evidence

In a case assessment, you're ensuring the investigation has a proper scope, proper authorization, and a plan that preserves evidence integrity. Reviewing the case investigator's request for service helps confirm what needs to be examined, what artifacts are relevant, and what deliverables are expected, so the assessment can be focused and accurate. Identifying the legal authority for the forensic examination request makes sure the actions are authorized by law or policy, preventing improper or unauthorized analysis. Discussing whether other forensic processes should be performed on the evidence supports a thorough, well-planned approach and helps avoid gaps or unnecessary duplication. Not documenting the chain of custody, however, undermines the whole assessment. The chain of custody records who handled the evidence, when, where, and what was done to it. Without that documentation, the integrity and admissibility of the evidence come into question, and the findings may be challenged in court.

10. If a file of 2600 bytes on a hard disk uses 512-byte sectors, how many sectors are normally allocated to the file?

A. 4 Sectors

B. 5 Sectors

C. 7 Sectors

D. 6 Sectors

Sectors are the basic units used to store data on a disk, and file systems allocate space in whole sectors (or larger units that are multiples of sectors). To find how many sectors a file needs, divide the file size by the sector size and round up to the next whole sector. Here, 2600 bytes divided by 512 bytes per sector equals 5.078125, so you round up to 6 sectors. Six sectors provide 3072 bytes of space, which is enough for the 2600-byte file, whereas five sectors would only offer 2560 bytes and would be insufficient. Therefore, six sectors are allocated.

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://chfiv11.examzify.com

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

SAMPLE