CYBERSECURITY AND DIGITAL FORENSICS PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cybersecdigiforensics.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. **In VMware memory imaging, memory is typically stored in files with which extensions?**

   A. vmem and vmsm

   B. memdump and memcore

   C. vmcore and vmemdump

   D. memory.img and dump.mem

2. **Which statement reflects an advantage of plaintext logs enabling policy updates?**

   A. Easy to define and change

   B. Hard to standardize

   C. Requires binary format

   D. Not human-readable

3. **Which department is involved in computer security incident response?**

   A. IT

   B. Security

   C. Legal

   D. ALL

4. **Which statement best describes the difference between logical and physical disk imaging, and when would you use each?**

   A. Logical imaging copies the entire drive bit-for-bit; Physical imaging captures the file system view.

   B. Logical imaging collects the file system view; Physical imaging copies the entire drive bit-for-bit; use physical when unallocated space and deleted data matter, otherwise logical might suffice.

   C. Physical imaging requires a write blocker; logical imaging does not.

   D. Both methods are identical in scope and outcome.

5. **Forensic readiness and chain of custody.**

   A. Documenting who collected, when, and how evidence was handled throughout the investigation.

   B. Ensuring data is encrypted at rest.

   C. Deleting metadata to avoid leaks.

   D. Replacing old evidence with modern equivalents.

SAMPLE

6. Which of the following is an anti-analysis technique?

A. Metadata scrubbing

B. Encryption

C. Legacy media

D. Post incident activity

7. Why is chain of custody critical in a digital forensics examination?

A. It speeds up analysis

B. It ensures evidence integrity and admissibility

C. It guarantees the evidence is collected legally

D. It eliminates the need for chain documentation

8. Are events logged at the presentation tier good places to find evidence related to application domain specific logic?

A. True

B. False

C. Sometimes

D. Not sure

9. Which practices constitute common logging best practice?

A. Centralized logging; time-synchronization (NTP); integrity protection; secure storage; regular review.

B. Decentralized logs across machines; no integrity checks; local retention only.

C. Logs only for failed login attempts; no review.

D. Logs stored immediately in user desktops without centralization.

10. Which statement describes the process and components of a digital signature?

A. A password-protected file that encrypts the message.

B. Hash of message signed with private key; recipient uses public key to verify; components include digest, private key, public key, and certificate.

C. A symmetric key shared in advance.

D. A checksum only.

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. In VMware memory imaging, memory is typically stored in files with which extensions?

A. vmem and vmsm

B. memdump and memcore

C. vmcore and vmemdump

D. memory.img and dump.mem

VMware memory imaging uses a .vmem file to store the VM's RAM contents, and when a snapshot is taken, the memory state is captured in a companion file with a .vmsm extension. Together, these two files represent the in-memory state of a VM at a given moment: the .vmem holds the actual memory data, while the .vmsm records the memory state for the snapshot. That's why the pairing vmem and vmsm is the best answer. The other options don't reflect VMware's typical memory image naming conventions and would not accurately describe its memory image extensions.

2. Which statement reflects an advantage of plaintext logs enabling policy updates?

A. Easy to define and change

B. Hard to standardize

C. Requires binary format

D. Not human-readable

Plaintext logs are easy to define and change because their content is human-readable and editable. When policy processing relies on log data, you can inspect the entries, understand exactly what is captured, and modify the logging policy or the rules that act on those logs by editing a simple text file. This makes updates quick and collaborative: you can tweak what gets logged, adjust formats, or change alert thresholds and deploy those changes with minimal tooling. You can also use version control to track and roll back changes. If logs required binary formatting or were not readable, or if standardization was difficult, updating policies would be much slower and would demand more specialized tools.

3. Which department is involved in computer security incident response?

A. IT

B. Security

C. Legal

D. ALL

Incident response requires coordination across different parts of an organization. IT handles the technical side—detecting, containing, and restoring systems—while Security leads the analysis of the incident, determines scope, and helps implement remediation. Legal takes care of regulatory requirements, evidence handling, and notification obligations, ensuring that any disclosures or investigations comply with laws and contracts. Because these activities span technical, legal, and regulatory aspects, effective incident response isn't owned by a single department. The best answer reflects this cross-functional nature: all of them work together to manage and recover from an incident. In practice, teams run incident response plans that assign roles to IT, Security, and Legal (and often others) to ensure a swift, compliant, and well-documented response. For example, during a breach, IT may isolate affected systems, Security analyzes what happened and how it spread, and Legal coordinates any required notifications and preserves evidence. Relying on just one department risks missing critical steps, so involving all three is essential.

SAMPLE

4. Which statement best describes the difference between logical and physical disk imaging, and when would you use each?

A. Logical imaging copies the entire drive bit-for-bit; Physical imaging captures the file system view.

B. Logical imaging collects the file system view; Physical imaging copies the entire drive bit-for-bit; use physical when unallocated space and deleted data matter, otherwise logical might suffice.

C. Physical imaging requires a write blocker; logical imaging does not.

D. Both methods are identical in scope and outcome.

Understanding the difference between physical and logical imaging comes down to scope. A physical image copies the entire drive sector by sector, preserving every bit on the media—including unallocated space, slack space, and data that may have been deleted but still resides on the disk. A logical image, on the other hand, captures only what the file system presents: the files, folders, and their metadata as visible through the filesystem, not the free space or remnants that lie outside the active file structure. This is why physical imaging is used when evidence might be hidden in areas the file system doesn't expose, such as deleted data, remnants in unallocated sectors, or artifacts in slack space. Logical imaging is appropriate when you only need the existing files and their organization, and you can work with a smaller, faster image that doesn't include the drive's free space. Note that best practice in forensic work often involves using a write blocker during physical imaging to ensure the source isn't modified, but that requirement isn't what fundamentally differentiates the two methods. The key difference remains the scope: complete sector-by-sector capture versus file-system-level capture.

5. Forensic readiness and chain of custody.

A. Documenting who collected, when, and how evidence was handled throughout the investigation.

B. Ensuring data is encrypted at rest.

C. Deleting metadata to avoid leaks.

D. Replacing old evidence with modern equivalents.

The main idea here is establishing a solid chain of custody to prove the integrity and provenance of evidence. Documenting who collected the evidence, when it was collected, and exactly how it was handled keeps a transparent, auditable trail from seizure to presentation. This makes it possible to verify authenticity, detect any alterations, and defend admissibility in court. Forensic readiness hinges on having procedures and records in place so investigations can start quickly and evidence remains traceable and defensible. Other options miss the purpose: encrypting data at rest protects confidentiality but doesn't record who did what with the evidence or when, so it doesn't address provenance. Deleting metadata would remove important contextual information that helps establish timelines and authenticity. Replacing old evidence with newer equivalents is tampering and destroys the integrity of the evidentiary trail.

SAMPLE

6. Which of the following is an anti-analysis technique?

A. Metadata scrubbing

B. Encryption

C. Legacy media

D. Post incident activity

Anti-analysis techniques are ways attackers make it harder for security researchers to understand how a threat works, what it does, or what data it handles. Encryption fits this role strongly because it turns payloads, configuration data, or exfiltrated information into unreadable form without the correct key. When malware encrypts its payload or commands, analysts can't easily statically inspect what the code will do or what data it will exfiltrate; they must discover the key, observe decrypted in memory, or perform more complex runtime analysis to reveal the hidden content. This directly increases the difficulty and time required for analysis, which is the hallmark of an anti-analysis tactic. Other options don't target the analysis process in the same direct way. Metadata scrubbing aims to erase traces that might aid attribution rather than impede understanding of the malware's behavior, and legacy media or post-incident activity refer to artifacts or defender actions rather than techniques designed to thwart analysis of the threat itself.

7. Why is chain of custody critical in a digital forensics examination?

A. It speeds up analysis

B. It ensures evidence integrity and admissibility

C. It guarantees the evidence is collected legally

D. It eliminates the need for chain documentation

The main idea here is that chain of custody provides a verifiable, unbroken record of who handled the digital evidence, when, and for what purpose. In digital forensics, evidence such as disk images, memory captures, and log files often passes through multiple people, devices, and storage locations. Documenting every transfer, transformation, and storage condition keeps the data traceable and makes tampering detectable. By tying each stage to timestamps, personnel, and actions, and by verifying data integrity with hash values, you can show that the evidence remained authentic from seizure to presentation. This continuity is what makes the evidence admissible in court. If the chain is broken or unclear, questions can arise about whether the data were altered, corrupted, or substituted, which undermines the reliability of the forensic findings. Proper chain of custody thus directly supports the credibility and admissibility of the results. The other ideas—speeding up analysis, guaranteeing legal collection, or eliminating the need for chain documentation—don't capture the essential purpose. Chain of custody isn't primarily about faster work, nor does it on its own ensure that collection was legal. It also cannot exist without proper chain documentation; you can't have custody without documenting every step.

SAMPLE

8. Are events logged at the presentation tier good places to find evidence related to application domain specific logic?

A. True

B. False

C. Sometimes

D. Not sure

Events logged at the presentation tier are not reliable evidence of application domain-specific logic because the presentation layer focuses on UI and user interactions, not the business rules that govern data and processes. The domain logic is implemented in the application or service layer, and its evidence usually appears in server-side logs, audit trails, and database transaction records that capture decisions, state changes, validations, and data mutations. Presentation-tier logs can help reconstruct a timeline of what a user did, but they rarely reveal why a decision was made or what rules were applied, and they can be incomplete or subject to client-side tampering. So, while UI logs can supplement an investigation, they aren't the best primary source for domain-specific logic; server-side logs and related records provide more authoritative evidence.

9. Which practices constitute common logging best practice?

A. Centralized logging; time-synchronization (NTP); integrity protection; secure storage; regular review.

B. Decentralized logs across machines; no integrity checks; local retention only.

C. Logs only for failed login attempts; no review.

D. Logs stored immediately in user desktops without centralization.

The main idea is that solid logging practices create visibility, integrity, and accountability across the environment, which is essential for monitoring, incident response, and forensics. Centralized logging brings logs from many systems into one place, making it possible to search efficiently, correlate events, and retain data long enough to investigate incidents or meet compliance. Time-synchronization with a reliable NTP service ensures all devices stamp events with a consistent clock, so the order of actions across many hosts can be accurately reconstructed during investigations. Integrity protection, such as signing, tamper-evident or append-only storage, and protected transmission channels, helps ensure logs remain authentic and inviolate, which is crucial for reliable evidence. Secure storage adds access controls and encryption at rest to prevent unauthorized access or modification, safeguarding the logs from insider or external threats. Regular review means logs aren't collected and forgotten; they are actively analyzed, with alerts tuned and investigations initiated when anomalies appear, supporting proactive defense and compliance oversight. Log practices that decentralize logs, skip integrity checks, or rely on local retention only undermine visibility and trust. Without centralization, correlating events across systems becomes nearly impossible, and tampering can go undetected. Relying on local retention increases the risk of data loss if a host is compromised. Focusing only on failed logins or avoiding reviews leaves many relevant events unseen, and storing logs on user desktops removes central control and makes protection and collection difficult.

SAMPLE

10. Which statement describes the process and components of a digital signature?

A. A password-protected file that encrypts the message.

B. Hash of message signed with private key; recipient uses public key to verify; components include digest, private key, public key, and certificate.

C. A symmetric key shared in advance.

D. A checksum only.

Digital signatures authenticate who signed a message and ensure it hasn't been altered. The process starts by creating a hash (digest) of the message, then signing that digest with the sender's private key. The resulting digital signature travels with the message, and anyone who has the corresponding public key can verify the signature by re-hashing the received message and checking that the signature matches. If verification succeeds, the recipient gains confidence about the signer's identity and the message's integrity. The typical components involved are the digest, the private key used to create the signature, the public key used to verify it, and a certificate that ties the public key to the signer's identity within a trusted framework (PKI). The certificate helps establish that the public key truly belongs to the claimed sender. Other options describe different concepts that don't provide a signing and verification mechanism: encrypting a message with a password mainly aims at confidentiality, not authentication; sharing a symmetric key in advance is about secret communication, not non-repudiation or public-key verification; and a checksum is a simple integrity check without any cryptographic proof of origin or identity.

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://cybersecdigiforensics.examzify.com

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

SAMPLE