DIGITAL FORENSICS, INVESTIGATION, AND RESPONSE PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://digitalforensicsinvestresponse.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. Which term best describes an overarching plan to keep essential business operations operating during and after a disruptive event?

A. Incident Response Plan

B. Continuity of Operations Plan

C. Business Continuity Plan

D. Recovery Plan

2. An improvement on the Caesar cipher that uses more than one shift is called Multialphabet substitution.

A. Multialphabet substitution

B. Vigenère cipher

C. Polyalphabetic substitution

D. Monoalphabetic substitution

3. Logic bombs are often perpetrated by _____.

A. disgruntled employees

B. external hackers

C. customers

D. contractors

4. The .mbx extension is used by which email client?

A. Eudora

B. Outlook Express

C. Gmail

D. Mozilla Thunderbird

5. You are performing a forensic analysis on a cell phone. You have tried entering the PUK 6 times, all incorrectly. What does this mean for John's investigation?

A. The SIM is permanently locked

B. You can try the PUK 3 more times before the device is locked

C. Nothing; you can try the PUK 9 times before factory reset on the 10th

D. The phone will be restored to factory settings after the 7th attempt

SAMPLE

6. Which statement is false about evidence handling at a police station according to the provided guidelines?

A. Evidence need not be locked if it is at a police station.

B. Evidence must be secured and access controlled while stored

C. Evidence is typically handled with a documented chain of custody

D. Evidence should be stored in a controlled environment

7. Which product is described as recovering Inbox and Outbox data and all contacts data, with a free trial version available?

A. Data Doctor

B. XRY

C. Pwnage

D. Outlook Recovery Toolkit

8. Under the Wireless Communications and Public Safety Act of 1999, what type of data is described as 'empty' communications and may be collected?

A. Text messages and emails

B. Nonverbal and nontext communications such as GPS information

C. Voice calls

D. Video surveillance

9. Which application is commonly associated with creating OpenDocument Text files?

A. OpenOffice Writer

B. Microsoft Word

C. Google Docs

D. LibreOffice Calc

10. Which shell is described as the default for the macOS terminal, enabling command input in a Bash-like environment?

A. BASH

B. ZSH

C. SH

D. CSH

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which term best describes an overarching plan to keep essential business operations operating during and after a disruptive event?

A. Incident Response Plan

B. Continuity of Operations Plan

C. Business Continuity Plan

D. Recovery Plan

Maintaining essential operations during and after a disruption is what this term addresses. The Continuity of Operations Plan is built to ensure mission-critical functions stay active regardless of upheaval. It lays out who leads if key people are unavailable, the delegation of authority, alternate facilities, and the communications and vital records needed to keep those core functions running while normal operations are interrupted or restored. This focus on sustaining critical capabilities through the whole disruption life cycle makes it the best fit. In contrast, an Incident Response Plan centers on detecting and handling specific events like security incidents; a Recovery Plan tends to emphasize restoring IT systems after a disruption; and a Business Continuity Plan is broader, aiming to keep the business operating more generally, not solely the essential functions that must continue.

2. An improvement on the Caesar cipher that uses more than one shift is called Multialphabet substitution.

A. Multialphabet substitution

B. Vigenère cipher

C. Polyalphabetic substitution

D. Monoalphabetic substitution

Using more than one shift changes a Caesar-style encoding into a polyalphabetic substitution. A fixed shift maps every letter to the same counterpart, making it vulnerable to frequency analysis. When shifts vary across the message, you effectively use multiple alphabets, so the same plaintext letter can map to different ciphertext letters depending on its position. That description matches the idea of using multiple shifts directly. Among the options, Multialphabet substitution is the phrasing that conveys that concept most closely. In standard terms, this is called polyalphabetic substitution, with the Vigenère cipher being a well-known implementation that uses a keyword to determine the sequence of shifts. The monoalphabetic option, by contrast, relies on a single alphabet and a fixed mapping, which doesn't fit the "more than one shift" idea.

3. Logic bombs are often perpetrated by _____.

A. disgruntled employees

B. external hackers

C. customers

D. contractors

Logic bombs rely on the trusted access of someone inside the organization. A disgruntled employee already has legitimate login and system permissions, so they can conceal a dormant payload and trigger it later when a condition is met (such as a date or a specific event). External hackers, customers, or even contractors do not typically have the same ongoing access and insider positioning, making them less likely to plant a dormant bomb that activates quietly. While contractors could pose an insider risk, the most common scenario is a dissatisfied employee who can introduce the code and control its activation without immediate detection.

SAMPLE

4. The .mbx extension is used by which email client?

A. Eudora

B. Outlook Express

C. Gmail

D. Mozilla Thunderbird

The .mbx extension points to how Eudora stored its email. In Eudora, each mailbox was saved as a single file with the .mbx extension (often alongside a companion .toc index file). This makes .mbx a recognizable artifact for Eudora. In contrast, Outlook Express uses .dbx files for mailboxes, Gmail is a cloud-based service with no local .mbx files, and Mozilla Thunderbird uses the mbox format where mailbox files typically have no extension or use the mailbox name without an .mbx suffix. So, the .mbx extension is most closely tied to Eudora.

5. You are performing a forensic analysis on a cell phone. You have tried entering the PUK 6 times, all incorrectly. What does this mean for John's investigation?

A. The SIM is permanently locked

B. You can try the PUK 3 more times before the device is locked

C. Nothing; you can try the PUK 9 times before factory reset on the 10th

D. The phone will be restored to factory settings after the 7th attempt

The key idea is how the PUK (Personal Unblocking Key) works: it protects the SIM by giving you a limited number of attempts to unblock it after the PIN has been entered incorrectly too many times. The scenario here implies there is a final threshold (the 10th attempt) after which a drastic action—in this quiz's wording, a factory reset—would occur. Since you've already tried six times, there are still many chances left before that limit is reached. This means nothing has wiped the phone or its data yet, and the investigation can continue with the device accessible, aside from any loss of cellular service if the SIM becomes temporarily unusable. The important takeaway is that PUK attempts are finite and do not automatically erase the device; you still have the opportunity to unlock the SIM before reaching the final threshold.

6. Which statement is false about evidence handling at a police station according to the provided guidelines?

A. Evidence need not be locked if it is at a police station.

B. Evidence must be secured and access controlled while stored

C. Evidence is typically handled with a documented chain of custody

D. Evidence should be stored in a controlled environment

Secure, controlled handling of evidence is essential to preserve its integrity and admissibility. In a police station, evidence must be locked and secured when stored, with access strictly controlled to prevent tampering or unauthorized viewing. Every movement or transfer of evidence is recorded in a chain of custody, documenting who handled it, when, and for what purpose, so the trail remains intact. The storage environment should be controlled—temperature, humidity, light, and contamination risks minimized—to prevent degradation or alteration. Therefore, the statement that evidence does not need to be locked is false, because locking and securing storage is a fundamental baseline requirement. The other practices—keeping evidence secured and access-controlled, maintaining a documented chain of custody, and storing it in a controlled environment—reflect standard, necessary procedures.

SAMPLE

7. Which product is described as recovering Inbox and Outbox data and all contacts data, with a free trial version available?

A. Data Doctor

B. XRY

C. Pwnage

D. Outlook Recovery Toolkit

This item tests identifying a data recovery tool by the exact artifacts it promises to recover. The description mentions pulling back Inbox and Outbox data along with all contacts, and it also notes a free trial version. Data Doctor is described as a general data recovery utility capable of restoring email items (like Inbox and Outbox) and contact data, and it typically offers a free trial for evaluation. That combination—email artifacts plus contacts, plus a trial option—best matches the description. The other tools have different focuses: XRY is mainly a mobile-forensics extractor for a broad range of device data and isn't centered on Inbox/Outbox and contacts with a trial described in this way; Pwnage is a jailbreaking tool, not a data recovery product; Outlook Recovery Toolkit targets Outlook-specific PST/OST recovery, which is narrower and often described differently than a general Inbox/Outbox plus contacts recovery with a free trial.

8. Under the Wireless Communications and Public Safety Act of 1999, what type of data is described as 'empty' communications and may be collected?

A. Text messages and emails

B. Nonverbal and nontext communications such as GPS information

C. Voice calls

D. Video surveillance

The concept being tested is that some data collected in investigations is metadata—information about the communication rather than the content itself. "Empty" communications refer to nonverbal, nontext data that describes aspects of a communication, not what was said or written. GPS information is a prime example because it reveals where a device was and when, without exposing the actual message content. This type of data can be obtained to locate devices or track movements, often with fewer privacy hurdles than accessing the message content itself. Text messages and emails, by contrast, expose the actual words and content of the communication. Voice calls reveal spoken content. Video surveillance captures visual content. Each of these conveys substantive information about what happened, and they generally require different or stronger legal authorization to access.

9. Which application is commonly associated with creating OpenDocument Text files?

A. OpenOffice Writer

B. Microsoft Word

C. Google Docs

D. LibreOffice Calc

OpenDocument Text (.odt) is the standard text document format used by OpenDocument-compatible word processors. OpenOffice Writer is the classic application designed to create and save those .odt files, making it the most direct match for producing OpenDocument Text documents. The other options align with different document types or platforms—Calc is for spreadsheets (.ods), Word uses its own formats (.doc/.docx), and Google Docs is a web-based editor that can export to odt but isn't the native creator of OpenDocument Text files.

SAMPLE

10. Which shell is described as the default for the macOS terminal, enabling command input in a Bash-like environment?

A. BASH

B. ZSH

C. SH

D. CSH

macOS Terminal uses a shell as the command-line interface, and the default shell has shifted over time. Today, the default is zsh, which gives you a Bash-like command line experience while adding its own features and improvements. Bash is still available and can be used if you switch to it, but it's no longer the default on current macOS. The other shells listed (a traditional Bourne shell and the C shell) are separate options with different syntax and are not the macOS default. So the description of a Bash like environment as the standard macOS Terminal interface points to zsh.

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://digitalforensicsinvestresponse.examzify.com

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

SAMPLE