DIGITAL FORENSIC CERTIFICATION PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://digitalforensic.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 a key requirement for tools used in the disk imaging process?**

   A. The tool must be affordable.

   B. The tool must have a user-friendly interface.

   C. The tool must alert if the destination is smaller than the source.

   D. The tool must be able to perform encryption.

2. **What step in forensic readiness involves deciding if full investigation is necessary?**

   A. Identify the sources of evidence

   B. Create a documentation process

   C. Identify if the incident requires full investigation

   D. Establish a legal advisory board

3. **What is defined as the number of bits per square inch on a hard disk platter?**

   A. Transfer speed

   B. Areal density

   C. Access time

   D. Seek rate

4. **What is recorded in the Windows Registry when the Tor browser is installed?**

   A. User activity logs

   B. Active network connections

   C. Browser execution pathways

   D. System performance metrics

5. **What command is used to retrieve important information about MAC times and timestamps in a Mac system?**

   A. stat [-FlLnqrsx] [-f format] [-t timefmt] [file ...]

   B. getinfo -t <file>

   C. macinfo <file>

   D. timestamp -v <file>

SAMPLE

6. What forensic tool does Richin utilize to conduct RAM dumps for viewing running processes and recently executed commands?

A. LiME

B. FTK Imager

C. Volatility Framework

D. EnCase

7. Which checksum algorithm does FastSum compute for file integrity?

A. SHA-1

B. CRC32

C. MD5

D. SHA-256

8. What term describes the fraudulent use of someone's identification for illegal transactions?

A. Whaling

B. Identity theft

C. Mail bombing

D. Cyberstalking

9. What is the purpose of Route Correlation in digital forensics?

A. To filter out irrelevant events

B. To determine user behavior patterns

C. To extract information about the attack route

D. To predict potential vulnerabilities

10. Which disk interface allows personal computers to communicate with various peripheral hardware?

A. SATA

B. USB

C. SCSI

D. IDE

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is a key requirement for tools used in the disk imaging process?

A. The tool must be affordable.

B. The tool must have a user-friendly interface.

C. The tool must alert if the destination is smaller than the source.

D. The tool must be able to perform encryption.

A crucial requirement for tools used in the disk imaging process is that they must alert if the destination is smaller than the source. This is essential because a successful disk image creation must ensure that all the data from the source device can fit onto the destination storage medium. When the destination is smaller, it can lead to data loss, corruption, or an incomplete image, which would negatively affect any subsequent forensic analysis or recovery efforts. Having this alert allows forensic professionals to make critical decisions about the imaging process, such as selecting a different destination that has adequate capacity or deleting unnecessary files from the source before imaging. This functionality is fundamental to maintaining the integrity of the forensic process, ensuring that all relevant data is captured and available for examination. While affordability and user-friendly interfaces might be desirable features of a disk imaging tool, they do not impact the technical functionality that ensures the successful imaging of disks. The ability to perform encryption is also important for security purposes, but it is not a primary requirement when considering the immediate need to successfully create an image that accurately represents the source medium without data loss.

2. What step in forensic readiness involves deciding if full investigation is necessary?

A. Identify the sources of evidence

B. Create a documentation process

C. Identify if the incident requires full investigation

D. Establish a legal advisory board

In the context of forensic readiness, determining whether a full investigation is necessary is a critical step. This process involves assessing the nature and severity of the incident to conclude if it warrants an extensive examination. This assessment allows organizations to allocate their resources effectively and make informed decisions about whether to proceed with a complete forensic investigation. When an organization identifies an incident, the decision on whether a full investigation is needed will depend on various factors, such as the potential impact of the incident, the sensitivity of the data involved, and the legal implications. By evaluating these factors early in the incident management process, organizations can ensure that they respond appropriately and minimize any potential risks or repercussions. Assessing the need for a full investigation is vital in the forensic readiness strategy, as it sets the stage for the subsequent steps, such as identifying the evidence sources or establishing documentation practices. Thus, this step is integral to managing the incident effectively and ensuring that appropriate actions are taken based on the situation's gravity.

SAMPLE

3. What is defined as the number of bits per square inch on a hard disk platter?

A. Transfer speed

B. Areal density

C. Access time

D. Seek rate

The term that refers to the number of bits stored per square inch on a hard disk platter is areal density. Areal density is a critical metric in measuring the storage capacity of a hard drive, as it directly influences how much data can be stored within a given physical area of the disk. Higher areal density indicates that more bits are packed into a smaller area, allowing for increased data storage capacity without requiring a proportionate increase in the physical size of the disk. In contrast, transfer speed focuses on how quickly data can be read from or written to the disk but does not consider the actual data density. Access time pertains to the time it takes for the read/write heads to position themselves over the correct track, which is a performance characteristic rather than a measure of how data is stored physically. Lastly, seek rate refers to the speed at which the hard drive can move its read/write heads to different tracks on the disk, relating to operational efficiency rather than the storage characteristics defined by areal density.

4. What is recorded in the Windows Registry when the Tor browser is installed?

A. User activity logs

B. Active network connections

C. Browser execution pathways

D. System performance metrics

When the Tor browser is installed on a Windows system, the Windows Registry records details related to the installation and configuration of the browser, which includes the browser execution pathways. This information typically indicates where the Tor browser's executable files are located and how they should be run within the operating system. The purpose of recording this data is to ensure that the browser can launch correctly whenever the user initiates it, providing seamless access to its functionalities. The Registry keys for the Tor browser may also include settings related to its operation and integration with the system, such as file associations and default behaviors. The execution pathways specifically help the operating system understand where to find the necessary files for operational execution, which is essential for the software's functionality. Other options, like user activity logs or active network connections, are not stored in the Registry and instead may be found elsewhere in the system or managed by the application itself in its own data storage mechanisms. Likewise, system performance metrics are typically monitored through different system tools rather than through Registry entries related to a specific application like the Tor browser.

SAMPLE

5. What command is used to retrieve important information about MAC times and timestamps in a Mac system?

A. stat [-FlLnqrsx] [-f format] [-t timefmt] [file ...]

B. getinfo -t <file>

C. macinfo <file>

D. timestamp -v <file>

The command to retrieve important information about MAC times (Modification, Access, and Change timestamps) and other timestamps in a Mac system is "stat". This utility provides detailed information about file attributes, including timestamps that reflect various file states. Using "stat" allows users to examine the details associated with files directly from the command line. It can show the time of last access, last modification, and last metadata change. The various options available with "stat" such as -F, -f, and -t allow for customized output and formatting, catering to the needs of the user in a forensic context. This command is essential for digital forensic examiners who need accurate and detailed time-related information about files on macOS systems. The other commands mentioned do not serve the same purpose or lack the comprehensive attributes provided by "stat". Some may not even exist as standard commands on Mac systems. Thus, the ability of "stat" to provide a full spectrum of file time information solidifies it as the correct choice in this context.

6. What forensic tool does Richin utilize to conduct RAM dumps for viewing running processes and recently executed commands?

A. LiME

B. FTK Imager

C. Volatility Framework

D. EnCase

The correct answer is LiME, which stands for Linux Memory Extractor. LiME is specifically designed to facilitate memory acquisition on Linux systems by allowing forensic professionals to capture volatile memory. This includes information about running processes, recently executed commands, and other critical data that resides in RAM at the time of the analysis. LiME operates by creating a complete image of the RAM, which can then be analyzed to uncover various types of artifacts and data relevant to a forensic investigation. This capability is essential in cases where understanding the current state of the system is crucial, such as during an active attack or when examining malware behavior. The other tools mentioned have different primary functions. FTK Imager is primarily used for imaging hard drives and creating disk images rather than capturing RAM. The Volatility Framework is indeed used for analyzing memory dumps, but it does not perform the acquisition itself; rather, it is used after another tool has captured the RAM image. EnCase, while a powerful forensic tool that can aid in a wide range of forensic investigations, is more focused on filesystem analysis and managing disk images and evidence rather than specializing in RAM dumps specifically. Thus, LiME is the most appropriate tool for conducting RAM dumps and viewing the relevant information from volatile memory.

SAMPLE

7. Which checksum algorithm does FastSum compute for file integrity?

A. SHA-1

B. CRC32

C. MD5

D. SHA-256

FastSum is specifically designed to compute checksums to ensure file integrity, and it primarily uses the MD5 algorithm for this purpose. MD5 is recognized for its speed and efficiency when generating checksums, making it quite popular in various applications, including file verification. Although MD5 is not the most secure algorithm for cryptographic purposes due to vulnerabilities that can be exploited, it remains effective for integrity checking in many contexts. The other algorithms listed have distinct contexts and applications. For example, SHA-1 is more secure than MD5 but slower in performance, which isn't as ideal for a tool focused on rapid checksum generation like FastSum. CRC32 is more about error-checking in data transmission rather than generating a strong file integrity checksum, while SHA-256, although very secure, is computationally heavier and not typically associated with FastSum's primary functionality. Therefore, MD5 is the correct answer as it aligns with the FastSum program's intended use for quickly calculating file integrity checksums.

8. What term describes the fraudulent use of someone's identification for illegal transactions?

A. Whaling

B. Identity theft

C. Mail bombing

D. Cyberstalking

The term that describes the fraudulent use of someone's identification for illegal transactions is identity theft. This crime occurs when a person illegally acquires and uses someone else's personal information, such as their name, social security number, credit card details, or other financial information, typically to commit fraud or other crimes. Identity theft can lead to significant financial loss for victims, damage to their credit scores, and a long, complicated process to reclaim their identity. In contrast, whaling typically refers to targeting high-profile individuals within a company for phishing attacks, rather than stealing identities outright. Mail bombing is an attack aimed at overwhelming a mail server by flooding it with excessive messages. Cyberstalking involves using the internet to harass or threaten someone, which does not inherently involve using another person's identification for fraudulent purposes. Thus, identity theft is the clear and precise term for the fraudulent use of someone's identification for illegal transactions.

SAMPLE

9. What is the purpose of Route Correlation in digital forensics?

A. To filter out irrelevant events

B. To determine user behavior patterns

C. To extract information about the attack route

D. To predict potential vulnerabilities

The primary purpose of Route Correlation in digital forensics is to extract information about the attack route. This investigative technique involves analyzing data from various sources to reconstruct the path that an attacker took during a cyber incident. By correlating logs from different network devices, servers, and security tools, digital forensics professionals can identify how an attack was initiated, the various points of entry exploited, and how the attacker navigated through the system or network. Understanding the attack route is crucial for several reasons. It helps forensic analysts to ascertain the methods and tools used by the attacker, which can provide insights into their strategies and intentions. Furthermore, by mapping out the attack path, forensic teams can develop more effective defensive measures for the future, enhancing overall security posture. While filtering irrelevant events can help in narrowing down analysis, determining user behavior patterns, and predicting potential vulnerabilities are relevant forensic tasks, they serve different investigative purposes. The specific focus on attack routes is what makes this choice the most aligned with the concept of Route Correlation in digital forensics.

10. Which disk interface allows personal computers to communicate with various peripheral hardware?

A. SATA

B. USB

C. SCSI

D. IDE

The correct choice is SCSI, which stands for Small Computer System Interface. SCSI is a set of standards for connecting and transferring data between computers and peripheral devices like hard drives, scanners, and printers. It supports a wide range of devices, allowing multiple devices to communicate simultaneously over a single connection, making it a versatile option for personal computers. SCSI is known for its high performance and is often used in servers and workstations where speed and efficiency are critical. While other interfaces like SATA, USB, and IDE also allow communication between computers and peripherals, they have specific use cases and limitations. For instance, SATA is primarily designed for connecting storage devices like hard drives and SSDs, USB is widely used for various devices but has limitations in terms of speed and simultaneous connections, and IDE is an older interface that has largely been replaced by SATA for disk drives. SCSI, with its ability to handle multiple device types and support for high-speed data transfer, is particularly notable in environments where various peripherals need to connect and communicate effectively with personal computers.

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://digitalforensic.examzify.com

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

SAMPLE