INVESTIGATIONS AND EVIDENCE RECOVERY PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://investigationsevidencerecovery.examzify.com

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

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.

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!

Questions

1. What is NOT a function of a forensic laboratory's Terms of Reference?

A. Measuring laboratory performance metrics

B. Defining the scope of forensic investigations

C. Establishing protocols for handling evidence

D. Controlling the budget of the laboratory

2. What is essential when utilizing GPS technology to trace a cell phone?

A. A built-in GPS chip

B. Access to the phone's call history

C. Continuous battery power

D. Cell tower connection

3. What type of files may contain information that can aid in investigations but were not directly part of the active data?

A. Cache files

B. Temporary files

C. System files

D. Hibernation files

4. What is required to legally monitor employee computer usage in most cases?

A. Written consent from employees

B. Public announcement of monitoring

C. Approval from a government agency

D. Complete transparency of actions

5. Where is a cellular phone customer's personal phonebook typically stored?

A. Flash drive

B. SIM

C. PUK

D. SSD

6. What does the Type Allocation Code on a telephone help identify?

A. Subscriber's name

B. Type of services purchased by the subscriber

C. Electronic serial number of the device

D. Model of the telephone

7. What type of documents is an attorney trying to protect when claiming work product during legal disputes?

A. Documents prepared while developing the product in dispute

B. Documents defining specifications for engineering the disputed product

C. Documents prepared by the legal team in anticipation of litigation

D. There is no work product privilege in a civil suit

8. In a typical Linux file system, where is the file owner information stored?

A. Dentry

B. Inode

C. Superblock

D. $MFT

9. Is Security as a Service one of the primary forms of service provided by cloud service providers?

A. True

B. False

C. Only for specific providers

D. Depends on the service agreement

10. What is referred to when providing internal and external training for the development of analysts?

A. Proficiency

B. Skills training

C. Employee Development

D. Employee Competency

Answers

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

Explanations

1. What is NOT a function of a forensic laboratory's Terms of Reference?

A. Measuring laboratory performance metrics

B. Defining the scope of forensic investigations

C. Establishing protocols for handling evidence

D. Controlling the budget of the laboratory

The function of a forensic laboratory's Terms of Reference is to outline the specific responsibilities and operational guidelines for the laboratory. This includes defining the scope of forensic investigations, which is crucial for ensuring that all parties involved understand what is included or excluded in particular cases. Establishing protocols for handling evidence is also significant, as it ensures that evidence is processed in a way that maintains its integrity and admissibility in court. Additionally, measuring laboratory performance metrics is vital, as it allows the laboratory to evaluate its effectiveness, efficiency, and adherence to standards over time. In contrast, controlling the budget of the laboratory is typically outside the purview of the Terms of Reference. Budget control is generally a function of administrative or financial management within the larger organizational structure, not a direct operational guideline for forensic investigations. Therefore, this aspect does not fit with the primary functions that the Terms of Reference are meant to address.

2. What is essential when utilizing GPS technology to trace a cell phone?

A. A built-in GPS chip

B. Access to the phone's call history

C. Continuous battery power

D. Cell tower connection

When utilizing GPS technology to trace a cell phone, having a built-in GPS chip is crucial because this component allows the device to receive signals from satellites to determine its precise location. The GPS chip utilizes a network of satellites to triangulate the phone's position, providing accurate and real-time location data. This functionality is foundational to GPS tracking; without it, the GPS system cannot operate, rendering tracing ineffective. While continuous battery power and a cell tower connection can play roles in maintaining device functionality and communication, respectively, they do not specifically pertain to the core requirement of GPS technology itself. Access to call history, although potentially useful for other investigative purposes, does not contribute directly to the GPS tracing capability. The presence of a built-in GPS chip is the key element that enables location tracking via GPS technology.

3. What type of files may contain information that can aid in investigations but were not directly part of the active data?

A. Cache files

B. Temporary files

C. System files

D. Hibernation files

Hibernation files are an essential type of file in the context of digital investigations because they contain a snapshot of the system's memory at the moment the computer was put into hibernation. This allows investigators to recover information about all running processes, open applications, and active user sessions at that point in time. Because the hibernation file captures the complete state of the system's memory, it holds valuable data that may not be available in the active data forms. Cache files, temporary files, and system files all play various roles in a computer's operations, but they don't encapsulate the entire memory state as hibernation files do. Cache files are often designed for efficiency in data retrieval and might not retain critical information about ongoing tasks. Temporary files may contain fragments of data that were in use but typically do not provide a comprehensive overview of system activity. System files are integral for the operation of the system but do not explicitly save user or operational states at the time of hibernation. Thus, hibernation files are particularly valuable for forensic analysis and investigations, making them the most relevant choice in this context.

4. What is required to legally monitor employee computer usage in most cases?

A. Written consent from employees

B. Public announcement of monitoring

C. Approval from a government agency

D. Complete transparency of actions

To legally monitor employee computer usage, obtaining written consent from employees is often necessary. This requirement stems from privacy laws and regulations designed to protect employees' rights and expectations of privacy in the workplace. When employees are informed and consent to monitoring, it establishes a clear understanding that their activities may be observed, thus creating a lawful basis for such actions. Written consent not only helps organizations comply with legal standards but also fosters trust and transparency between employers and employees. By having documentation of the employees' agreement, employers can defend their monitoring practices as being in accordance with established policies. The other options are not typically sufficient on their own to meet legal requirements. Public announcements may raise awareness about monitoring policies but do not provide the necessary consent. Approval from a government agency is generally not required for such monitoring unless specific legal or regulatory frameworks dictate otherwise. Lastly, complete transparency of actions might be ideal for fostering trust but does not replace the need for explicit consent within the legal context.

5. Where is a cellular phone customer's personal phonebook typically stored?

A. Flash drive

B. SIM

C. PUK

D. SSD

A cellular phone customer's personal phonebook is typically stored on the SIM (Subscriber Identity Module) card. The SIM card is a small removable card that contains the International Mobile Subscriber Identity (IMSI) and allows the phone to connect to the mobile network. In addition to storing user information necessary for network communication, the SIM card often holds the user's contacts, which can include phone numbers and related information. While other storage options exist, such as flash drives or solid-state drives (SSD), these are not typically used for storing a phone's contact list in the case of standard cellular phones. A PUK (Personal Unlocking Key) is specifically used to unlock a SIM card that has been locked due to incorrect PIN entries, and does not store any user data. Thus, the SIM card is the definitive location for storing a user's personal phonebook on a cellular device.

6. What does the Type Allocation Code on a telephone help identify?

A. Subscriber's name

B. Type of services purchased by the subscriber

C. Electronic serial number of the device

D. Model of the telephone

The Type Allocation Code (TAC) is a key component of the International Mobile Equipment Identity (IMEI) number, which is used to uniquely identify a mobile device. The first section of the IMEI, the TAC, specifically reveals the model of the telephone and the manufacturer. This code is crucial in distinguishing between different devices, as each manufacturer assigns a unique TAC to their products. Understanding the TAC's role is essential in investigations involving mobile devices, as it assists in determining the specific type of phone being used in various scenarios, such as tracking a device in criminal activity or ensuring compatibility with network services. Therefore, recognizing that the TAC helps identify the model of the telephone explains why this choice is correct. Other options suggest information that the TAC does not provide; for instance, it does not contain personal subscriber information, services purchased, or the electronic serial number, which are linked to different identifiers and aspects of mobile device management.

7. What type of documents is an attorney trying to protect when claiming work product during legal disputes?

A. Documents prepared while developing the product in dispute

B. Documents defining specifications for engineering the disputed product

C. Documents prepared by the legal team in anticipation of litigation

D. There is no work product privilege in a civil suit

The assertion that documents prepared by the legal team in anticipation of litigation are protected under the work product doctrine is fundamentally accurate. This doctrine is designed to protect the legal strategies, thoughts, and theories of a lawyer as they prepare for a case. When attorneys anticipate litigation, they often create various documents, including notes, memos, research, and strategy outlines, which are intended solely for their legal work. The privilege covers not just the documents directly submitted in court but also those that provide insights into the legal team's planning and analysis. This protection is crucial as it allows attorneys to work with a certain level of privacy, facilitating candid discussions and strategic planning without the fear of revealing their thought processes to opposing counsel. The other options do not encapsulate the essence of what the work product doctrine aims to protect. The first choice refers to materials created during product development, which aren't necessarily associated with legal anticipation. The second option deals with engineering specifications rather than legal documentation or strategies. Lastly, the assertion regarding the absence of a work product privilege in civil suits is incorrect; such a privilege does exist in civil litigation, specifically aimed at safeguarding the integrity of legal preparation.

8. In a typical Linux file system, where is the file owner information stored?

A. Dentry

B. Inode

C. Superblock

D. $MFT

The file owner information in a typical Linux file system is stored in the inode. An inode is a data structure used to represent a file or a directory. It contains essential metadata about the file, including the file's owner (user ID and group ID), access permissions, timestamps, and pointers to the actual data blocks on the disk where the file content is stored. The dentry, on the other hand, is used to cache the directory structure and has no ownership information of its own; rather, it serves as a mechanism for name resolution and linking names to inodes. The superblock contains metadata about the file system itself, such as its size, type, and status, but not per-file ownership details. The $MFT refers to the Master File Table used in NTFS (Windows file systems) and does not apply to Linux file systems. As such, the inode is the correct answer for where the file owner information is stored in a typical Linux file system.

9. Is Security as a Service one of the primary forms of service provided by cloud service providers?

A. True

B. False

C. Only for specific providers

D. Depends on the service agreement

The idea of Security as a Service refers to a model where companies outsource their security functions to third-party providers, primarily through cloud services. While many cloud service providers offer varying levels of security services, it cannot be definitively categorized as one of the primary forms of service. Cloud service offerings typically focus on infrastructure, platform, and software services—often referred to as IaaS, PaaS, and SaaS. Security services, though essential, are often considered supplementary or included as part of these offerings rather than standing as a primary model. Thus, the statement in question identifies Security as a Service as not being a central form of service offered by cloud providers, underlining that while it is relevant and frequently provided, it is not always categorized as a primary offering in the market.

10. What is referred to when providing internal and external training for the development of analysts?

A. Proficiency

B. Skills training

C. Employee Development

D. Employee Competency

The term that best captures the concept of providing internal and external training for the development of analysts is employee development. This encompasses a wide range of training programs and initiatives aimed at enhancing the skills, knowledge, and capabilities of employees within an organization. Employee development not only focuses on immediate skill enhancement but also on long-term career growth and professional advancement, which can include both structured training programs and informal learning opportunities. Skills training, while relevant, specifically refers to the acquisition of specific skills rather than the broader scope of career and personal growth that employee development embodies. Proficiency pertains to the level of skill or competence someone has in a particular area, and while it can be a goal of employee development, it does not directly define the training process itself. Employee competency refers to the demonstrated ability to perform job functions effectively, which can result from employee development efforts but does not encompass the training practices used to achieve that competency.

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://investigationsevidencerecovery.examzify.com

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