Investigations and Evidence Recovery Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

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 aspect distinguishes a civil investigation from a criminal one?**

   A. The level of evidence required

   B. The location of the investigation

   C. The type of penalties involved

   D. All of the above

2. **Which of the following is NOT typically included in system metadata?**

   A. File creation date.

   B. Document content.

   C. Last modified date.

   D. File size.

3. **What is the consequence of obtaining evidence without a warrant?**

   A. The evidence is admissible in all cases.

   B. The evidence may be excluded from the trial.

   C. The evidence can be used if the crime is serious enough.

   D. This is never a concern in criminal cases.

4. **When a file occupying seven clusters is erased and another file of 610 bytes is saved in one cluster, how is that cluster described?**

   A. 610 bytes of data and 31,390 bytes of unallocated space.

   B. 610 bytes of data and 31,390 bytes of random zeroes and ones following the EOF marker.

   C. 610 bytes of data followed by 31,390 bytes of null space.

   D. 610 bytes of data followed by 31,390 bytes of the previous file in the slack space.

5. **Which piece of metadata is NOT stored in the $MFT file of the NTFS file system?**

   A. Create time

   B. File name

   C. Security descriptor

   D. Author's name

6. A false statement about evidence not conforming to Locard's Principle would be indicative of what?

A. Chain of custody issues.

B. Circumstantial evidence.

C. Hearsay concerns.

D. Authentication challenges.

7. What common feature found in files might suggest the innocence of a user suspected of collecting pornographic images?

A. All files appeared within moments of a single "TYPEDURL"

B. The HTTP headers indicate each file is the result of a REDIRECT

C. All files appear to have come from the same URL

D. Most files were PNG files and not JPEG files

8. 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

9. Does a DoD approved disk wiping utility erase information by applying a strong magnetic field to the disk surface?

A. True

B. False

10. What is the primary purpose of using a write blocker in digital investigations?

A. Improves the speed of the imaging process

B. Prevents accidental modification of evidence

C. Helps in decrypting encrypted files

D. Enhances the visibility of hidden files

Answers

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

Explanations

1. What aspect distinguishes a civil investigation from a criminal one?

A. The level of evidence required

B. The location of the investigation

C. The type of penalties involved

D. All of the above

A civil investigation is distinct from a criminal investigation primarily based on the level of evidence required to support claims or allegations. In civil cases, the standard is typically "preponderance of the evidence," meaning that it is more likely than not that the claim is true. This is a lower threshold compared to criminal cases, which require "beyond a reasonable doubt" to secure a conviction. The varying levels of evidence not only affect the outcome but also shape the approach taken by investigators in gathering and analyzing information. For instance, in civil investigations, evidence may be collected to establish liability or damages rather than to prove guilt in the same rigorous manner required for criminal investigations. While the other options address important characteristics of each type of investigation—such as location and type of penalties—none capture the fundamental difference in the level of evidence as clearly as this option does. Civil cases generally result in financial penalties or orders for action rather than criminal penalties like imprisonment. Thus, the emphasis on the evidentiary standards highlights the key distinction between civil and criminal investigations.

2. Which of the following is NOT typically included in system metadata?

A. File creation date.

B. Document content.

C. Last modified date.

D. File size.

The correct answer is that document content is not typically included in system metadata. System metadata refers to information created and maintained by the operating system or file management system that describes various attributes of a file or system resource. This can include details such as the file creation date, last modified date, and file size. File creation date and last modified date provide a timeline of when a file was created and last changed, which is crucial for organizing and retrieving files. File size indicates the amount of space the file takes up on the storage medium, which can be important for managing storage capacity. In contrast, document content encompasses the actual information or data contained within the file, such as text in a document or images in a photo. This content is not considered metadata because it is not descriptive of the file's attributes or characteristics; it is the subject of the file rather than information about the file itself. Therefore, document content does not fall under the definition of typical system metadata, making it the correct choice in this question.

3. What is the consequence of obtaining evidence without a warrant?

A. The evidence is admissible in all cases.

B. The evidence may be excluded from the trial.

C. The evidence can be used if the crime is serious enough.

D. This is never a concern in criminal cases.

Obtaining evidence without a warrant typically means that the evidence was collected in violation of an individual's Fourth Amendment rights, which protect against unreasonable searches and seizures. In the context of a legal proceeding, if the court determines that the evidence was obtained illegally, it is likely to be deemed inadmissible in court, which is often referred to as the "exclusionary rule." This rule is designed to deter law enforcement from conducting unlawful searches and ensures that individuals are protected from arbitrary governmental intrusion. The rationale behind this rule is rooted in the belief that allowing illegally obtained evidence would undermine the integrity of the judicial system. Therefore, when evidence is collected without a warrant and does not fall under any recognized exceptions (such as exigent circumstances), it faces the strong possibility of being excluded from prosecution, significantly impacting the case's outcome.

4. When a file occupying seven clusters is erased and another file of 610 bytes is saved in one cluster, how is that cluster described?

A. 610 bytes of data and 31,390 bytes of unallocated space.

B. 610 bytes of data and 31,390 bytes of random zeroes and ones following the EOF marker.

C. 610 bytes of data followed by 31,390 bytes of null space.

D. 610 bytes of data followed by 31,390 bytes of the previous file in the slack space.

The correct answer points to the concept of slack space, which refers to the unused space in a cluster after a file is saved. When a file that occupies seven clusters is erased, its data is no longer actively referenced by the file system, yet it may still physically exist on the disk until overwritten. In this case, when a new file of 610 bytes is saved in one cluster, it does not fully utilize the entire cluster capacity. Consequently, the remaining space in that cluster (after accounting for the 610 bytes) constitutes slack space. The total size of a cluster is typically larger than the file size, and any leftover space is still a part of that cluster. Because the prior file occupied seven clusters, the cluster now holding the 610-byte file could still contain remnants of the deleted file in the slack space, which is essentially leftover data not cleared when the prior file was erased. Therefore, the correct description includes not only the current data of 610 bytes but also the residual data from the previous file that remains in the slack space, thus constituting 31,390 bytes that reflect that leftover information.

5. Which piece of metadata is NOT stored in the $MFT file of the NTFS file system?

A. Create time

B. File name

C. Security descriptor

D. Author's name

The correct answer regarding metadata not stored in the $MFT (Master File Table) of the NTFS (New Technology File System) is the author's name. The $MFT is a critical component of NTFS that contains detailed information about every file and directory on the file system. This includes various attributes like the creation time, file name, and security descriptor. The create time captures when the file was first created, providing a timestamp that is essential for file management and tracking changes over time. The file name attribute contains the name of the file, which is fundamental for user interaction and file organization. A security descriptor is also included in the $MFT, detailing permissions and access control for files and directories, which is essential for managing security for users and processes accessing the data. However, the author's name is not a standard metadata field within the $MFT. While some file types may store an author's name within their specific file format or associated metadata elsewhere, such as embedded in documents or applications (like Microsoft Office files), it does not form part of the core attributes maintained in the $MFT itself. Therefore, it is this lack of inclusion that distinguishes the author's name from the other provided attributes.

6. A false statement about evidence not conforming to Locard's Principle would be indicative of what?

A. Chain of custody issues.

B. Circumstantial evidence.

C. Hearsay concerns.

D. Authentication challenges.

The assertion that a false statement about evidence not conforming to Locard's Principle would be indicative of chain of custody issues highlights the core principles of forensic science. Locard's Principle of Exchange states that the perpetrator of a crime will invariably bring something into the crime scene and leave with something from it, meaning that evidence is always transferred between the scene and the individuals involved. When evidence does not conform to this principle, it raises concerns about how that evidence was collected, handled, and transferred, ultimately leading to questions about its reliability and integrity. Chain of custody refers to the documentation and handling process that tracks the evidence from the time it is collected until it is presented in court. Any false statements involving this process suggest there may have been a breach in the way evidence was managed, which can undermine its credibility in an investigation. This focus on evidence handling is key in forensic investigations, as it ensures that the physical and digital evidence presented is the same as that which was originally collected. If evidence cannot be reliably traced back to the crime scene or the parties involved, it creates significant challenges for law enforcement and legal professionals trying to build a case.

7. What common feature found in files might suggest the innocence of a user suspected of collecting pornographic images?

A. All files appeared within moments of a single "TYPEDURL"

B. The HTTP headers indicate each file is the result of a REDIRECT

C. All files appear to have come from the same URL

D. Most files were PNG files and not JPEG files

The common feature that might suggest the innocence of a user suspected of collecting pornographic images is indicated by the HTTP headers showing that each file is the result of a REDIRECT. This is significant because when files are accessed via redirects, it typically suggests that the user did not directly seek out each individual file but was instead directed to them through another webpage or link. This behavior is often indicative of passive browsing or incidental exposure to content rather than active searching or collecting. If a user were intentionally seeking out pornographic content, we would expect to see files stemming directly from user-typed URLs or downloads from the same URL, which wouldn't involve the REDIRECT process. The presence of a redirect indicates that the user may have been led to the content unintentionally, perhaps by clicking on a link that took them elsewhere, suggesting a lack of intent regarding the collection of such files. This detail can be crucial in differentiating between someone who is innocently browsing and someone who is actively curating a collection of explicit material.

8. 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.

9. Does a DoD approved disk wiping utility erase information by applying a strong magnetic field to the disk surface?

A. True

B. False

A Department of Defense (DoD) approved disk wiping utility does not rely on applying a strong magnetic field to erase information from a disk surface. Instead, these utilities typically function by overwriting the existing data on the disk with a specific pattern of data multiple times, which makes the original data irretrievable. This method is in line with the DoD standards for data sanitization, which emphasize techniques that ensure data cannot be recovered by standard data recovery methods. Using a strong magnetic field is a method associated with degaussing, which is effective for certain types of storage media, such as magnetic tapes and hard drives. However, modern solid-state drives (SSDs) and some other storage technologies do not respond effectively to magnetic fields in the same way. The wiping utilities, which are software-based, focus on systematic overwriting rather than relying on physical destruction techniques like degaussing, thereby ensuring a broader applicability across different types of data storage.

10. What is the primary purpose of using a write blocker in digital investigations?

A. Improves the speed of the imaging process

B. Prevents accidental modification of evidence

C. Helps in decrypting encrypted files

D. Enhances the visibility of hidden files

The primary purpose of using a write blocker in digital investigations is to prevent accidental modification of evidence. Write blockers are critical tools that allow investigators to access and copy data from storage devices while ensuring that the original content remains unchanged. This is essential because any alteration to the original data could compromise the integrity of the evidence and invalidate its use in court. By using a write blocker, investigators can conduct their analyses and create forensic images without risking any changes to the data on the original device. This helps maintain a clear chain of custody and supports the legal admissibility of the evidence collected. The ability to securely and accurately preserve original data is foundational in building trust in the investigative process and ensuring that justice is served. The other options do not address the primary function of write blockers, as they focus on aspects like speed, decryption, and visibility, which are not the main goals of utilizing such tools in evidence recovery.

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!