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

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

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 term describes 'empty' communications such as GPS information that may be collected under the act?

A. Active data

B. Empty communications

C. Encrypted data

D. Metadata

2. Which Linux command can be used to generate a hash?

A. MD5sum

B. SHA1sum

C. Hashsum

D. Checksum

3. APFS was first announced at the Apple Developer Conference in 2016. Which choice best states the year?

A. 2014

B. 2016

C. 2018

D. 2020

4. Daubert standard is used by a trial judge to determine whether an expert's reasoning or methodology is scientifically valid and can be applied to the facts.

A. Admissibility of hearsay

B. Scientific validity of reasoning or methodology

C. Relevance to the facts

D. Authentication of documents

5. The .mbx extension is associated with which email client?

A. Eudora

B. Outlook Express

C. Thunderbird

D. Apple Mail

6. What file system is used in most modern Mac OS systems?

A. HFS+

B. APFS

C. NTFS

D. ext4

7. Network forensics primarily involves which activity?

A. Examining network traffic, transaction logs, and real-time monitoring using sniffers and tracing

B. Extracting data from mobile devices only

C. Email content analysis

D. Imaging hard drives

8. What is the recommended handling of the original evidence after creating copies and hashes?

A. Leave it untouched and store securely

B. Keep it connected to a live system

C. Use it for further testing in the field

D. Erase it after analysis

9. What does a 500 HTTP response indicate?

A. OK

B. Not Found

C. Server error

D. Unauthorized

10. In steganography, what is the payload?

A. The carrier file

B. The hidden message itself

C. The encryption key

D. The checksum

Answers

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

Explanations

1. What term describes 'empty' communications such as GPS information that may be collected under the act?

A. Active data

B. Empty communications

C. Encrypted data

D. Metadata

The main idea is recognizing data about a communication that doesn't include the actual message content. "Empty communications" is the label used for data that describes a communication without carrying its substance, such as GPS coordinates that show where someone was or when they connected, but not what they said or what was in the message itself. This type of data can be collected under certain legal authorities even though it doesn't contain the message payload. Why this fits best: GPS information reveals patterns, movements, and associations related to communications, but it doesn't disclose the content of those communications. The term "empty communications" specifically points to this non-content data category that the act allows investigators to access. In contrast, metadata is a broader term for data about communications, including times, participants, and location. The question uses the exact terminology associated with the act, which is why this option is the most precise fit in this context. Encrypted data implies the content is hidden, and active data isn't a standard label here, so they don't match the concept being asked about.

2. Which Linux command can be used to generate a hash?

A. MD5sum

B. SHA1sum

C. Hashsum

D. Checksum

Generating a hash means producing a fixed-length fingerprint of data using a hash algorithm. In Linux, md5sum is the standard utility to compute an MD5 hash of a file or from standard input. It outputs the hash value followed by the file name, which you can compare with a known digest to verify integrity. For example, running md5sum on a file will give you a 32-character hex string that represents its MD5 hash. You can verify against a stored digest by piping or using md5sum -c with a digest file. The other options aren't standard commands for generating hashes: there isn't a generic hashsum command, and checksum isn't a typical tool name. If you need a different algorithm, there are dedicated tools like sha1sum, sha256sum, and so on, with sha256sum becoming a common choice for stronger hashes due to MD5's weaknesses.

3. APFS was first announced at the Apple Developer Conference in 2016. Which choice best states the year?

A. 2014

B. 2016

C. 2018

D. 2020

APFS was introduced by Apple at the Worldwide Developers Conference in 2016. That event is where Apple first revealed the Apple File System as a successor to HFS+, marking 2016 as the year of the announcement. The other years don't align with when APFS was publicly unveiled.

4. Daubert standard is used by a trial judge to determine whether an expert's reasoning or methodology is scientifically valid and can be applied to the facts.

A. Admissibility of hearsay

B. Scientific validity of reasoning or methodology

C. Relevance to the facts

D. Authentication of documents

The Daubert standard acts as a gatekeeping test for expert testimony, focusing on the scientific validity of the reasoning or methodology the expert uses to reach conclusions and whether that approach can be appropriately applied to the case facts. It isn't just about whether the testimony relates to the facts; it's about whether the underlying methods are reliable and scientifically sound. In practice, it considers whether the technique can be tested, has undergone peer review, has known error rates, is governed by standards, and is generally accepted in the relevant scientific community. If these criteria are met, the testimony is admissible; if not, it's excluded. The other topics—hearsay admissibility, document authentication, and general relevance to the facts—are governed by different evidentiary rules and do not capture the Daubert gatekeeping focus.

5. The .mbx extension is associated with which email client?

A. Eudora

B. Outlook Express

C. Thunderbird

D. Apple Mail

The .mbx extension identifies a mailbox file format used by Eudora. In Eudora, each mailbox—the collection of messages for a folder like Inbox or Sent—was stored as a single file with the .mbx extension (for example, Inbox.mbx). This makes the extension a clear indicator of that client's storage style. Other email clients use different formats: Outlook Express uses .dbx files for its folders, Thunderbird uses the mbox format (typically stored as files named after the folder without a .mbx extension), and Apple Mail uses mailbox bundles that end with .mbox in a macOS environment. So the presence of .mbx most strongly points to Eudora.

6. What file system is used in most modern Mac OS systems?

A. HFS+

B. APFS

C. NTFS

D. ext4

APFS (Apple File System) is the file system used by modern macOS installations, especially on solid-state drives. It replaced HFS+ as the default starting with macOS High Sierra and remains the standard for current macOS versions, offering space sharing, copies-on-write, strong native encryption, and faster performance for modern storage. NTFS and ext4 are Windows and Linux filesystems, respectively, and aren't used by default on macOS. HFS+ (Mac OS Extended) was the previous default, but it's largely phased out on new systems.

7. Network forensics primarily involves which activity?

A. Examining network traffic, transaction logs, and real-time monitoring using sniffers and tracing

B. Extracting data from mobile devices only

C. Email content analysis

D. Imaging hard drives

Network forensics focuses on data in transit and the behavior of the network during an incident. The primary activity is examining network traffic, transaction logs, and real-time monitoring using sniffers and tracing. By capturing packets, reviewing protocol details, and inspecting logs from network devices, you can reconstruct what happened, when it occurred, and how an intrusion or data transfer unfolded. Sniffers provide the raw data of the communications, while tracing helps map the path of the traffic and correlate events across devices, making it possible to identify sources, destinations, and timelines. Other activities you might see in related fields—such as extracting data from mobile devices, imaging hard drives, or analyzing email content—focus on data at rest on endpoints or specific content, not on the live network activity and in-motion data that network forensics examines. This network-centered view is what enables investigators to understand how threats moved through the environment and what was exposed.

8. What is the recommended handling of the original evidence after creating copies and hashes?

A. Leave it untouched and store securely

B. Keep it connected to a live system

C. Use it for further testing in the field

D. Erase it after analysis

Preserving evidence integrity and maintaining a solid chain of custody require that the original media remain unchanged after imaging and hashing. Once you've created verified copies and computed hash values, those hashes prove the copies are exact reproductions of the original, so any modification to the original could invalidate the evidence and undermine admissibility. Therefore, the original should be left untouched and stored securely—in a controlled environment with tamper-evident seals, strict access controls, and proper logging. Keeping the original connected to a live system risks ongoing changes and potential tampering. Using the original for further testing in the field risks altering data. Erasing it would destroy the evidence entirely. In short, the best practice is to leave the original untouched and store it securely.

9. What does a 500 HTTP response indicate?

A. OK

B. Not Found

C. Server error

D. Unauthorized

A 500 HTTP response indicates a server-side error. It belongs to the 5xx family, which means something went wrong on the server while handling the request. The exact cause isn't specified by this code alone; it could be an unhandled exception in the application, a failed dependency, or a server misconfiguration. The key point is that the client's request was valid, but the server encountered an issue preventing it from fulfilling the request. This differs from a 200 OK (the request succeeded), a 404 Not Found (the resource isn't there), or a 401 Unauthorized (authentication is required or failed). In practice, diagnosing a 500 involves checking server logs, error traces, recent changes, and resource conditions to pinpoint the root cause.

10. In steganography, what is the payload?

A. The carrier file

B. The hidden message itself

C. The encryption key

D. The checksum

In steganography, the payload is the hidden data that is concealed inside another file. It's the actual secret content you want to hide, such as a text message, an image, or a small file, that gets embedded into a cover or carrier file like a PNG, WAV, or other media. The carrier file serves as the container that carries the payload without drawing attention to the embedded data. If the hidden data is encrypted before embedding, the encryption key is used to protect the payload, but it isn't the payload itself. A checksum is used for integrity verification and does not represent the concealed data.

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!