Digital Forensics, Investigation, and Response 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. Steganography is defined as which of the following?

A. The art and science of encrypting messages.

B. The art and science of writing hidden messages.

C. The practice of deleting information to hide activity.

D. The technique of compressing data to save space.

2. Which port is IMAP commonly associated with by default?

A. 143

B. 25

C. 80

D. 443

3. 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

4. Which directory is commonly used to store configuration files on Unix-like systems?

A. /etc

B. /bin

C. /usr

D. /sbin

5. Which file extension is used to store Exchange mailbox databases?

A. .edb

B. .pst

C. .mbox

D. .dbx

6. OST files are used by which application to store offline mail data?

A. Microsoft Outlook

B. Mozilla Thunderbird

C. Eudora

D. OpenOffice

7. It is legal for employers to monitor work computers.

A. True

B. False

C. It depends on local laws

D. Only with employee consent

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. When seeking evidence of Ophcrack usage on a Windows Server 2008, which artifact is most likely to indicate its use?

A. A reboot event in the server logs

B. A new user account creation

C. A change in DNS entries

D. A hardware inventory update

10. AFF file format is used by which forensic software?

A. Autopsy and Sleuth Kit

B. EnCase

C. FTK

D. X-Ways

Answers

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

Explanations

1. Steganography is defined as which of the following?

A. The art and science of encrypting messages.

B. The art and science of writing hidden messages.

C. The practice of deleting information to hide activity.

D. The technique of compressing data to save space.

Steganography involves hiding a message inside another medium so that observers don't realize a secret message exists. The option that describes the art and science of writing hidden messages captures that idea by focusing on embedding the message within something ordinary. This differs from encryption, which aims to conceal the content of a message but not necessarily its presence; encryption can still signal that there is something to read. It also differs from deleting information to hide activity, which is about removing traces rather than embedding hidden data, and from compressing data to save space, which is about efficiency, not secrecy. A classic example is hiding a text message in the least significant bits of an image file so the image looks normal while carrying secret data.

2. Which port is IMAP commonly associated with by default?

A. 143

B. 25

C. 80

D. 443

IMAP is the protocol used to retrieve mail from a server, and its default listening port is 143 for unencrypted connections. This is defined in standard references for IMAP. When IMAP is secured with TLS/SSL, it typically uses port 993, but the common default for non-secure IMAP is 143. The other ports mentioned correspond to different services: 25 is for SMTP (sending mail), 80 is HTTP (web traffic), and 443 is HTTPS (encrypted web traffic). So seeing activity on port 143 is a strong indicator of an IMAP service handling mail retrieval.

3. 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.

4. Which directory is commonly used to store configuration files on Unix-like systems?

A. /etc

B. /bin

C. /usr

D. /sbin

Configuration files that control system behavior and service settings are traditionally stored in a dedicated location that is reserved for global, system-wide settings. On Unix-like systems, that place is /etc. You'll see files and subdirectories there for essential services and system configuration, such as /etc/hosts for host mappings, /etc/passwd for user accounts, and service-specific configs like /etc/ssh/sshd_config or /etc/nginx/nginx.conf. These files are usually owned by root and protected to prevent unintended changes, since altering them can affect how the entire system operates. It's helpful to contrast with other standard directories: /bin and /sbin contain executable programs needed for basic operation and system administration, not configuration data. /usr holds user-space programs and libraries, including many applications, rather than system-wide settings. While per-user preferences often live in a user's home directory (for example, hidden files or ~/.config), the central repository for global configuration remains /etc.

5. Which file extension is used to store Exchange mailbox databases?

A. .edb

B. .pst

C. .mbox

D. .dbx

Exchange stores its mailbox data in a database file created by the Extensible Storage Engine, and that file uses the .edb extension. This .edb file contains the actual mailbox data, including messages, folders, and indexing, and is managed by the server along with its transaction logs. The other extensions represent different mail systems or local client stores: .pst is a personal storage file used by Outlook on the client side, not the server mailbox store; .mbox is used by various Unix/macOS mail applications; .dbx comes from Outlook Express. Therefore, the .edb file is the correct designation for Exchange mailbox databases.

6. OST files are used by which application to store offline mail data?

A. Microsoft Outlook

B. Mozilla Thunderbird

C. Eudora

D. OpenOffice

Offline Storage Table (OST) files are the local cache Outlook creates for Exchange accounts so you can read, compose, and organize mail without being online. The OST keeps a complete copy of your mailbox on the device and stays synchronized with the server when you reconnect, so changes you make offline are uploaded and you see updates from others when online. This storage method is specific to Microsoft Outlook (in Cached Exchange Mode) and is why you'd see an OST file on a system using Outlook with Exchange. Other mail clients use different local formats—Thunderbird uses MBOX/Maildir-style storage, Eudora uses its own mailbox formats, and OpenOffice isn't an email client and doesn't manage offline mail data.

7. It is legal for employers to monitor work computers.

A. True

B. False

C. It depends on local laws

D. Only with employee consent

When a computer is provided by the employer and used for work, monitoring it is generally legal because the organization owns the hardware, network, and the data on them and has a legitimate business interest in protecting assets, enforcing policies, and investigating incidents. This can include logging user activity, reviewing emails and messages sent through company accounts, examining file access, analyzing network traffic, and, in some cases, screen or remote monitoring as part of security controls. The crucial factors are ownership, a legitimate business purpose, and alignment with the employer's stated policies; with clear policy and appropriate scope, such monitoring is commonly considered lawful. Keep in mind that notices or consent requirements and privacy protections may vary by jurisdiction and BYOD scenarios, so organizations usually publish an acceptable-use or monitoring policy that employees acknowledge.

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. When seeking evidence of Ophcrack usage on a Windows Server 2008, which artifact is most likely to indicate its use?

A. A reboot event in the server logs

B. A new user account creation

C. A change in DNS entries

D. A hardware inventory update

When password-cracking tools like Ophcrack are used on a Windows server, they're typically run from a bootable environment outside the normal Windows OS to access the SAM file offline. That requires restarting the machine. So the most telling artifact is a reboot event in the server logs, which captures the system starting up into a different environment rather than staying in the regular Windows session. The other options don't directly indicate this kind of activity: creating a new user might happen after passwords are cracked, but it's not what shows that Ophcrack was used; DNS changes or hardware inventory updates are unrelated to running a password-cracking tool.

10. AFF file format is used by which forensic software?

A. Autopsy and Sleuth Kit

B. EnCase

C. FTK

D. X-Ways

The Advanced Forensic File Format (AFF) is an open, flexible disk image container designed to store both the data and rich metadata needed for forensic analysis. Autopsy and The Sleuth Kit are the tools most closely associated with AFF, and they natively support opening and parsing AFF images to examine file systems, extract artifacts, and perform investigations. This native compatibility makes them the best match for AFF among common forensic software. Other tools like EnCase, FTK, or X-Ways typically rely on their own native or proprietary image formats (for example, EnCase often uses EWF or its own formats, FTK uses AD1, and X-Ways uses its own formats). While these tools may sometimes work with various image types, AFF is most strongly linked to Autopsy and Sleuth Kit.

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!