Cengage Computer Forensics Practice Test (Sample)

Study Guide

BY EXAMZIFY

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 type of cards, consisting of a microprocessor and internal memory, are usually found in GSM devices?**

   A. SD Card

   B. NFC Tag

   C. SIM

   D. USB Flash Drive

2. **Which activity involves determining how much risk is acceptable for any process or operation?**

   A. Risk management

   B. Security auditing

   C. Compliance assessment

   D. Incident response

3. **What is PCAP data and how is it used in network forensics?**

   A. Public key certificates

   B. Packet capture data containing network traffic; analyzed to identify protocols, sessions, and indicators of compromise

   C. Password storage

   D. Personal configuration profile

4. **Which type of hypervisor is typically found loaded on a suspect machine?**

   A. Type 1

   B. Type 2

   C. No hypervisor

   D. KVM

5. **TDMA is a method used in digital networks to:**

   A. divide the radio frequency into frequency bands

   B. encrypt traffic

   C. divide the radio frequency into time slots

   D. compress data

6. What should you use to verify evidence and thus ensure its integrity?

A. Encryption

B. Checksums

C. Hash algorithms

D. Digital signatures

7. The lab manager is responsible for setting up processes for managing cases and reviewing them regularly.

A. False

B. Not True

C. Yes

D. True

8. Which tool enables acquiring a forensic image and processing it in one step?

A. EnCase

B. FTK

C. Magnet AXIOM

D. Autopsy

9. Which group often works as part of a team to secure an organization's computers and networks?

A. Incident responders

B. Forensics investigators

C. System administrators

D. Security analysts

10. What Windows artifact reveals program startup information and helps reconstruct execution flow?

A. Recycle Bin

B. Windows Registry

C. Prefetch files

D. Event Logs

Answers

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

Explanations

1. What type of cards, consisting of a microprocessor and internal memory, are usually found in GSM devices?

A. SD Card

B. NFC Tag

C. SIM

D. USB Flash Drive

In GSM networks, service access hinges on a SIM card, which is a small card that contains a microprocessor and memory to store the subscriber's identity and cryptographic keys. The SIM holds the IMSI (the subscriber's unique identifier) and authentication keys, and it runs the cryptographic processes needed to authenticate the device to the mobile network and authorize service. This enables roaming, billing, and secure access to network resources. Other options—SD cards, NFC tags, or USB flash drives—are mainly storage or tagging devices and do not carry the network authentication data or perform the mobile network's cryptographic checks, so they don't play the same role in GSM devices. Modern devices may use an embedded SIM (eSIM), but its fundamental function remains to provide identity and secure access to the cellular network.

2. Which activity involves determining how much risk is acceptable for any process or operation?

A. Risk management

B. Security auditing

C. Compliance assessment

D. Incident response

Determining how much risk is acceptable for any process or operation is a core function of risk management. This discipline sets the level of risk an organization is willing to accept, often described as risk appetite or risk tolerance, and uses that threshold to guide decisions about controls and investments. By identifying potential threats and their potential impact, evaluating how likely each risk is, and then deciding on how to treat each risk (avoid, mitigate, transfer, or accept), risk management aligns protection with cost, feasibility, and business goals. This makes it the best answer because it explicitly focuses on establishing acceptable risk levels across processes and operations. Security auditing, on the other hand, checks whether existing controls are effective and meet defined security standards. Compliance assessment looks at adherence to laws and regulations. Incident response is the set of actions taken after a security event to contain and recover. Each of these plays a critical role in cybersecurity, but they do not center on setting the acceptable level of risk itself the way risk management does.

3. What is PCAP data and how is it used in network forensics?

A. Public key certificates

B. Packet capture data containing network traffic; analyzed to identify protocols, sessions, and indicators of compromise

C. Password storage

D. Personal configuration profile

PCAP data is packet capture data that records the raw bytes of every network packet seen on a capture interface during a time window. In network forensics, this lets you see exactly how hosts communicated—what protocols were used, the sequence of packets, which IPs and ports talked, and when the traffic occurred. By analyzing a PCAP with a tool like Wireshark, you can filter to relevant conversations, reconstruct TCP streams to view complete dialogues, and spot indicators of compromise such as unusual destinations, beaconing patterns, or large data transfers. PCAPs also help establish a timeline by aligning packet timestamps with system logs or alerts, and they allow you to reproduce or validate events in a controlled setting. Keep in mind that PCAPs can be large and may contain encrypted payloads, so interpretation often relies on metadata, protocol behavior, and cross-checking with other evidence. Other items like public key certificates, password storage, or personal configuration profiles serve different purposes (authentication, credential protection, device setup) and are not raw network traffic captures.

4. Which type of hypervisor is typically found loaded on a suspect machine?

A. Type 1

B. Type 2

C. No hypervisor

D. KVM

Type 1 hypervisors are built to run directly on the hardware, without an underlying host operating system. That bare-metal placement makes them the typical virtualization layer you'd encounter on a suspect machine that's been prepared to run VMs covertly. Because there's no host OS to host a separate virtualization application, a Type 1 hypervisor can boot and operate more stealthily and persistently, which is why it's the most likely form to be found loaded in forensic scrutiny. In contrast, a Type 2 hypervisor sits on top of an existing OS, so you'd expect to see the host OS and the virtualization software as ordinary software artifacts within that OS. The option indicating no hypervisor would be incorrect if virtualization is actually present, and KVM is a specific implementation rather than a type; the classification you're looking for is the architecture—bare-metal, or Type 1.

5. TDMA is a method used in digital networks to:

A. divide the radio frequency into frequency bands

B. encrypt traffic

C. divide the radio frequency into time slots

D. compress data

TDMA uses time division to let multiple users share a single radio channel. The available frequency is divided into repeating time slots, and each user is assigned a specific slot in which they can transmit. This synchronization ensures transmissions don't collide, enabling efficient use of the channel. This approach is different from methods that share by frequency bands (where each user has a separate band) or by code, and it's not about encrypting data or compressing it. So dividing the radio frequency into time slots is what TDMA does.

6. What should you use to verify evidence and thus ensure its integrity?

A. Encryption

B. Checksums

C. Hash algorithms

D. Digital signatures

Verifying evidence integrity relies on a cryptographic hash function. You generate a digest (hash) of the original evidence and store it. Later, you recompute the hash on the copy or on the evidence after transport/storage; if the two digests match, the data hasn't changed. The reason this works is that good hash algorithms produce a fixed-size output that changes dramatically with any tiny modification—a property known as the avalanche effect—so any alteration yields a different digest. Encryption protects confidentiality, not integrity by itself. Checksums can detect simple errors but aren't cryptographically strong and can be bypassed or collided. Digital signatures can add authenticity by binding data to a signer, but for the straightforward task of verifying that evidence hasn't been altered, the hash alone is the most reliable and efficient method (often used in conjunction with signing the hash to prove provenance).

7. The lab manager is responsible for setting up processes for managing cases and reviewing them regularly.

A. False

B. Not True

C. Yes

D. True

Lab managers design and implement how cases are handled, including how cases are opened, tracked, assigned, documented, and archived. They establish workflows and standard operating procedures to ensure consistent handling, maintain chain of custody, preserve evidence integrity, and produce timely, defensible reports. Regular reviews of cases are essential to monitor progress, spot bottlenecks, verify that methods are followed, ensure QA/QC, stay aligned with accreditation requirements, and drive continuous improvement. Because setting up these processes and reviewing them regularly is a fundamental part of overseeing a forensic lab's operations, this statement is true.

8. Which tool enables acquiring a forensic image and processing it in one step?

A. EnCase

B. FTK

C. Magnet AXIOM

D. Autopsy

Integrated workflow where imaging and processing happen together is what Magnet AXIOM emphasizes. It lets you acquire a forensic image and start processing in the same session within the same project, so you can parse the file system, recover artifacts, index content, and build a searchable evidence set right away. This speed and simplicity come from its design to handle ingestion and analysis in one continuous flow, rather than requiring a separate imaging step followed by a distinct processing phase in another tool. Other options tend to separate imaging from analysis: some focus on creating the image first and then processing in a different module or tool, while Autopsy relies on data provided after imaging rather than performing the acquisition itself.

9. Which group often works as part of a team to secure an organization's computers and networks?

A. Incident responders

B. Forensics investigators

C. System administrators

D. Security analysts

When organizations defend their networks, collaborating across roles is essential, and forensic investigators often play a key part of that team. They bring specialized skills in preserving and analyzing digital evidence from breaches or suspicious activity, which helps the group understand exactly what happened, how attackers moved, and what data or systems were affected. This information guides containment and recovery actions and informs changes to prevent recurrence, such as improved logs, stricter access controls, and better incident playbooks. While other professionals focus on monitoring, maintenance, and immediate threat response, the forensic perspective is crucial for validating findings, preserving chain of custody, and driving lessons learned that strengthen future defenses.

10. What Windows artifact reveals program startup information and helps reconstruct execution flow?

A. Recycle Bin

B. Windows Registry

C. Prefetch files

D. Event Logs

Prefetch files are the artifact that reveals how a program starts and what happens during its launch. When a program is run, Windows creates a corresponding prefetch file that records the executable's path and the list of files the process opened during startup, including DLLs and other resources. It also notes how many times the program has run and the last run time. This snapshot lets an investigator understand the sequence of actions the program took as it started, including which modules loaded and in what order, which helps reconstruct the execution flow. Other options provide different kinds of information but not the same startup-level detail. The Recycle Bin only holds deleted items and doesn't reflect how an application started. The Windows Registry can show programs configured to run at startup, but it doesn't reveal the actual run-time sequence or loaded components. Event Logs capture system and application events, but they don't give a detailed view of the internal startup steps and files accessed by a program. So, the best artifact for uncovering startup activity and tracing execution is the prefetch file.

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://cengagecompforensics.examzify.com

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