# Cybersecurity and Digital Forensics 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. **Which VM format creates 'vmem' or 'vmsm' files for memory image collection?**

   **A. VMware**

   **B. VirtualBox**

   **C. Hyper-V**

   **D. KVM**

2. **What Windows artifact provides direct evidence of specific files opened by a user?**

   **A. Jump lists**

   **B. Event logs**

   **C. Registry**

   **D. Shortcuts**

3. **Which of the following is an anti-analysis technique?**

   **A. Secure file deletion**

   **B. Legacy media**

   **C. Post incident activity**

   **D. Visualization**

4. **What is an easy-to-use method for quick memory acquisition?**

   **A. Usermode tools**

   **B. Kernel drivers**

   **C. Full disk imaging**

   **D. Live CD**

5. **Which approach is described as easy for quick memory acquisition?**

   **A. Usermode tools**

   **B. Kernel drivers**

   **C. RAM freeze trick**

   **D. Memory dump writer**

**6. Which statement best describes what log data can help with security investigations?**

**A. Log data can reveal when a specific event or error occurred**

**B. Log data contains full user passwords**

**C. Log data is irrelevant to application behavior**

**D. Log data is only useful for billing**

**7. Which artifact can be used in place of a full memory image for memory forensics?**

**A. Pagefile and hibernation file only**

**B. Pagefile and system log**

**C. Hibernation file and RAM dump**

**D. Pagefile and picture files**

**8. According to CERT, must an incident be a real adverse event?**

**A. True**

**B. False**

**C. Not sure**

**D. It depends**

**9. Where is not a location to find information about application execution?**

**A. Recent files**

**B. Execution logs**

**C. System event logs**

**D. Application traces**

**10. What is a true statement about log creation in applications?**

**A. Logs can be created by explicit events or by periodic intervals**

**B. Logs are created only at system startup**

**C. Logs do not capture errors**

**D. Logs are stored only in memory**

# Answers

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

# Explanations

## 1. Which VM format creates 'vmem' or 'vmsm' files for memory image collection?

**A. VMware**

**B. VirtualBox**

**C. Hyper-V**

**D. KVM**

**Memory image collection hinges on how a hypervisor saves the RAM of a running or suspended VM. In VMware, the guest memory is written to a dedicated file with a .vmem extension, which stores the raw contents of the virtual machine's RAM. This is specifically the type of memory artifact you'd analyze for a memory image. Sometimes a related snapshot file is involved (often seen with a .vmsn extension for snapshot state), but the memory image itself is the .vmem file. Other hypervisors use different formats for memory artifacts, so the presence of .vmem (or related memory snapshot files) points to VMware.**

## 2. What Windows artifact provides direct evidence of specific files opened by a user?

**A. Jump lists**

**B. Event logs**

**C. Registry**

**D. Shortcuts**

**Jump lists are the Windows artifact that provides direct evidence of specific files opened by a user. When you open a document through a supported application, that item often appears in the app's jump list, showing the exact file name, path, and a timestamp of when it was accessed. This creates a concrete record of user activity—directly linking the user to particular files they opened. Other artifacts work differently. Event logs can capture related actions if auditing is enabled, but they're general logs of events and may not reliably enumerate every opened file. The registry stores settings and pointers, not a reliable record of opened documents. Shortcuts point to files but don't prove the files were actually opened. Remember also that jump lists can be cleared or disabled by privacy settings, so their presence isn't guaranteed in every case, but when they exist they give precise evidence of opened files.**

## 3. Which of the following is an anti-analysis technique?

**A. Secure file deletion**

**B. Legacy media**

**C. Post incident activity**

**D. Visualization**

**Anti-analysis techniques are methods that hinder investigators by destroying, obscuring, or concealing evidence so analysis and reconstruction of events become difficult. Secure file deletion directly fits this goal because it securely overwrites and removes data, making deleted information unrecoverable and erasing artifacts that analysts would rely on. The other options don't describe a focused method for thwarting analysis: legacy media is just older hardware, post-incident activity is a broad phase that can include many actions, and visualization is a way to present data rather than to obscure it.**

## 4. What is an easy-to-use method for quick memory acquisition?

**A. Usermode tools**

**B. Kernel drivers**

**C. Full disk imaging**

**D. Live CD**

**Capturing memory quickly is most practical when using tools that run in user mode inside the running operating system. These tools don't require installing kernel drivers or rebooting the machine, so you can start the memory dump right away and save the RAM image with minimal setup. They typically access memory through standard OS interfaces and write the dump to disk for analysis later, making the process fast and straightforward in the field. Keep in mind that while convenient, user-mode captures may not reach every memory nuance that kernel-mode or hardware methods can, and in some scenarios the contents can still change as the system runs. The other approaches involve more setup or disruption: kernel drivers require privileged installation, full-disk imaging targets storage rather than memory, and a Live CD needs you to reboot with external media, which slows you down.**

## 5. Which approach is described as easy for quick memory acquisition?

**A. Usermode tools**

**B. Kernel drivers**

**C. RAM freeze trick**

**D. Memory dump writer**

**When you need memory quickly from a live system, the easiest option is to use usermode tools. They run in user space, so you can launch them without installing kernel drivers or rebooting the machine. Portable and simple to deploy, these tools can start a memory capture with minimal setup, making them ideal for a rapid initial acquisition. Kernel drivers, while more robust and capable of gathering a more complete and accurate dump, require you to install and load a driver with elevated privileges. That adds setup time, security checks, and risk, so it isn't as quick or easy as usermode approaches. The RAM freeze trick is a hardware/physical technique used to slow memory decay for later capture. It's not a routine or easy method for quick forensic collection and involves extra hardware and steps, making it ill-suited for rapid acquisition. A memory dump writer is a generic term for software that writes memory to disk, but without the context of how and where it runs (user mode vs. kernel mode) it doesn't inherently imply quick, easy access. It's not as clearly quick and straightforward as using usermode tools. So, the best fit for "easy for quick memory acquisition" is using usermode tools.**

## 6. Which statement best describes what log data can help with security investigations?

**A. Log data can reveal when a specific event or error occurred**

**B. Log data contains full user passwords**

**C. Log data is irrelevant to application behavior**

**D. Log data is only useful for billing**

**Logs provide a timeline of events that helps investigators reconstruct what happened during a security incident. Each log entry records something that occurred in the system along with a timestamp, such as a login attempt, access to a file, a service starting or stopping, an error, or a configuration change. That time-stamped sequence lets investigators place events in the correct order, see how a breach began, what actions followed, and which resources were affected. This temporal context is essential for understanding the scope of an incident, tracing attacker movements, and validating what happened. It's also important to recognize that security-friendly logging does not store full passwords; exposing secrets in logs is a major risk, so credentials and other sensitive data aren't kept in plain form. Logs are used to observe behavior and security-relevant activity, not for billing purposes, and they should be maintained and protected to preserve their integrity for investigations.**

## 7. Which artifact can be used in place of a full memory image for memory forensics?

**A. Pagefile and hibernation file only**

**B. Pagefile and system log**

**C. Hibernation file and RAM dump**

**D. Pagefile and picture files**

**In memory forensics, when you can't capture a full RAM image, certain on-disk artifacts can stand in for memory content. The hibernation file (hiberfil.sys) stores a complete snapshot of RAM at the moment the system enters hibernation, so it effectively provides a memory image on disk. The pagefile (pagefile.sys) contains swapped-out memory pages, which can reveal data that was resident in RAM and even reconstruct what processes were doing, what data they touched, and other artifacts. Using both together gives you the strongest approximation of volatile memory: the hibernation file provides a near-full RAM snapshot, while the pagefile adds additional swapped data that can fill gaps and recover more artifacts. Other options like system logs, isolated RAM dumps, or unrelated picture files don't capture memory contents in the same way, so they're not as effective as a substitute for a full memory image.**

## 8. According to CERT, must an incident be a real adverse event?

**A. True**

**B. False**

**C. Not sure**

**D. It depends**

**In CERT terms, an incident covers more than just events that cause real harm. A security incident is any event that violates or could violate computer security policies, including attempts or near-misses that are detected or blocked, as well as actual breaches. So an incident does not have to be a real adverse event; it can be an attempted intrusion, suspicious activity, or a policy violation that prompts investigation. That's why the statement is false: CERT recognizes incidents that may not result in realized damage but still require follow-up and containment. For example, a failed login, a port scan, or a malware alert that is blocked are all incidents, even though no harm occurred.**

## 9. Where is not a location to find information about application execution?

**A. Recent files**

**B. Execution logs**

**C. System event logs**

**D. Application traces**

**Understanding where to find information about how an application ran hinges on what each data source captures. Execution logs record what the program did, including start and stop times, errors, and significant events. They give a direct record of the application's activity. System event logs capture operating system–level events, such as process creation and termination, which helps establish a timeline that includes the application. Application traces provide even more detail, showing function calls, data flow, and timing, which is valuable for reconstructing the exact execution path. Recent files, on the other hand, is a user-interface history that lists documents or items recently opened. It does not reflect the actual execution of the application, and it can be cleared or manipulated without affecting how the program ran. Because of that, it isn't a reliable source for information about application execution.**

## 10. What is a true statement about log creation in applications?

**A. Logs can be created by explicit events or by periodic intervals**

**B. Logs are created only at system startup**

**C. Logs do not capture errors**

**D. Logs are stored only in memory**

**Logs are created in two common ways: when explicit events occur and on a regular schedule. In practice, an application writes a log entry immediately when something noteworthy happens—like an error, a failed login, or a completed process—so the record reflects that event as it occurs. At the same time, many systems also generate logs at periodic intervals to capture ongoing health, status, or batched activity, ensuring you have a consistent view over time even if individual events are sparse. This combination is why the statement is true: logging isn't tied only to startup or to a single moment. It happens throughout normal operation and can be driven by events or by time-based intervals. Logs are also intended to be stored persistently so they can be analyzed later, and they do capture errors, not just non-error information.**

# 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://cybersecdigiforensics.examzify.com**

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