SANS ADVANCED INCIDENT RESPONSE, THREAT HUNTING, AND DIGITAL FORENSICS (FOR508) PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://sansfor508.examzify.com

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 is Timesketch used for in FOR508 practice?

A. Visualizing and analyzing timelines

B. Managing incident tickets

C. Encrypting log files

D. Scanning for open ports

2. Memory-based forensics focuses on which data sources?

A. Disk-based file system metadata

B. Imaging the entire disk

C. Live processes, network connections, loaded modules, and memory-resident credentials

D. Printed documents from the case file

3. Which Windows artifact records changes to files and directories on NTFS volumes to aid timeline analysis?

A. Prefetch files

B. LSASS memory

C. USN Change Journal

D. Bash history

4. How do you validate that a memory capture is forensically sound and not tampered with before analysis?

A. Verify the memory dump hash, confirm the capture method used by a trusted tool, and document the chain-of-custody of the memory image

B. Run a virus scan on the memory image and treat any result as proof

C. Compare memory to a baseline from a different system

D. Reboot and re-capture to see if contents match

5. The combination of which two ASEP start values can each independently provide persistence for malicious code?

A. 0x02 and 0x00

B. 0x01 and 0x03

C. 0x04 and 0x08

D. 0x10 and 0x20

6. In the incident response lifecycle, which phase includes lessons learned, reporting, and improvements?

A. Preparation

B. Recovery

C. Response

D. Post-incident activities

7. What does NIST stand for in the context of standards organizations?

A. United States Institute of Standards and Technology

B. US National Institute for Standards and Technology

C. National Institute for Standards and Security

D. US National Security and Technology Institute

8. Which description best captures a key property STIX aims to provide?

A. A rigid, binary encoding scheme.

B. Fully expressive, flexible, extensible, automatable, and as human-readable as possible.

C. A collection of malware hashes.

D. A real-time network protocol analyzer.

9. What is the purpose of Sysmon in Windows incident response, and what kind of events should you collect?

A. Sysmon adds detailed process creation, network connections, and file/registry activity; collect Sysmon events and correlate with other logs.

B. Sysmon provides only antivirus scanning events.

C. Sysmon is a memory capture tool.

D. Sysmon logs only user logons.

10. Remediation events typically occur when?

A. During business hours on weekdays

B. Over a weekend

C. During annual maintenance window

D. Randomly any time

Answers

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

Explanations

1. What is Timesketch used for in FOR508 practice?

A. Visualizing and analyzing timelines

B. Managing incident tickets

C. Encrypting log files

D. Scanning for open ports

Timesketch is used to visualize and analyze timelines. It lets you bring together logs and artifacts from multiple sources and place every event on a common time axis, making it easy to see when things happened, how they relate, and how the incident unfolded. You can filter and group events by indicators like IP addresses, user IDs, or event types, which helps reveal the attacker's sequence of actions, identify correlations, and support reconstructing the incident step by step. It isn't a ticketing system for managing cases, nor a tool for encrypting logs, and it isn't a port-scanning utility—those functions belong to separate categories of software. In FOR508 practice, the strength of Timesketch lies in turning scattered data into an coherent timeline that guides investigation and response.

2. Memory-based forensics focuses on which data sources?

A. Disk-based file system metadata

B. Imaging the entire disk

C. Live processes, network connections, loaded modules, and memory-resident credentials

D. Printed documents from the case file

Memory-based forensics examines the volatile data held in RAM at the moment of capture. This means looking at what is actively in use by the system and running processes: the live processes and their threads, the open network connections and sockets, the modules loaded into memory (such as DLLs and kernel drivers), and credentials or other sensitive data that reside in memory during operation. This data is transient and can disappear if the system reboots, which is why capturing a memory image is crucial for understanding the exact state of the system at that moment and for uncovering artifacts that may not exist on disk. Disk-based data sources, like disk file system metadata or imaging the entire disk, reflect non-volatile storage and file system structures rather than the current execution state of the machine. Printed documents from the case file are outside digital memory forensics and do not represent volatile artifact data.

3. Which Windows artifact records changes to files and directories on NTFS volumes to aid timeline analysis?

A. Prefetch files

B. LSASS memory

C. USN Change Journal

D. Bash history

The main idea here is that the USN Change Journal on NTFS is a built-in audit log that records every change to files and directories on a volume, creating a chronological record that can be used to reconstruct what happened when. Each entry captures what changed (create, delete, modify, rename, attribute change, etc.), when it happened, and which file or directory was affected, including enough details to map actions across the timeline. Because this journal preserves a sequence of events directly from the file system, it provides a reliable backbone for timeline analysis, even if file timestamps are manipulated or multiple artifacts point to the same event. Prefetch files track program startup behavior, not file-system changes themselves. LSASS memory holds sensitive credentials, not a history of file activity. Bash history is Linux shell activity, not Windows NTFS changes.

4. How do you validate that a memory capture is forensically sound and not tampered with before analysis?

A. Verify the memory dump hash, confirm the capture method used by a trusted tool, and document the chain-of-custody of the memory image

B. Run a virus scan on the memory image and treat any result as proof

C. Compare memory to a baseline from a different system

D. Reboot and re-capture to see if contents match

Ensuring a memory capture is forensically sound hinges on three pillars: data integrity, trusted capture methods, and clear chain-of-custody. First, verifying the memory dump hash immediately after capture establishes that the exact bytes collected haven't been altered since the moment of acquisition. By computing a cryptographic hash (for example, SHA-256) and securely storing that value with the image, you can later confirm the image remains unchanged during handling and analysis. Second, using a capture method known to be trusted by the forensic community helps ensure the tool itself doesn't modify memory or introduce artifacts. This means selecting a reputable memory acquisition tool and following best practices that minimize disturbance to the system, such as documenting tool version, exact options used, and avoiding unnecessary writes to the source. The goal is reproducibility and verifiability of the capture process. Third, documenting chain-of-custody is essential. Every transfer, storage location, access control, and handling event should be recorded so the evidence can be traced from collection to analysis. This includes who performed the capture, when, where the image is stored, and how access is restricted, providing a verifiable history that supports admissibility and integrity. Why the other ideas don't fit: a virus scan on the memory image doesn't prove the image's integrity or authenticity and could be unreliable; comparing memory to a baseline from another system isn't a valid validity check due to hardware and configuration differences; rebooting and recapturing changes volatile data and can't prove that a prior capture was tampered with, since the memory contents aren't preserved between reboots.

5. The combination of which two ASEP start values can each independently provide persistence for malicious code?

A. 0x02 and 0x00

B. 0x01 and 0x03

C. 0x04 and 0x08

D. 0x10 and 0x20

In ASEP, each start value corresponds to a distinct persistence path. The requirement is that each start value, on its own, can maintain persistence for malicious code. The pair 0x00 and 0x02 fits this because each value maps to a separate, standalone persistence mechanism. This means an attacker could rely on either value independently to achieve persistence, and together they present two independent persistence vectors. The other options pair values where at least one does not provide a standalone persistence path, or the persistence outcome depends on combining values, so they don't meet the criterion of two independent persistence vectors. To defend, monitor and control changes to ASEP start values and block unauthorized persistence mechanisms at startup points.

6. In the incident response lifecycle, which phase includes lessons learned, reporting, and improvements?

A. Preparation

B. Recovery

C. Response

D. Post-incident activities

Post-incident activities focus on learning from the event and making the incident response program better. After containment and remediation, teams review what happened, document lessons learned, create or update after-action reports, and identify improvements to processes, playbooks, metrics, and controls. This closes the loop, ensuring findings lead to tangible changes in preparation, detection, and response for future incidents. The other phases serve different purposes: Preparation is about getting ready—training, policies, and ready-to-run tools; Response is the immediate actions to detect, contain, and eradicate the threat; Recovery is about restoring services and validating systems.

7. What does NIST stand for in the context of standards organizations?

A. United States Institute of Standards and Technology

B. US National Institute for Standards and Technology

C. National Institute for Standards and Security

D. US National Security and Technology Institute

Understanding what NIST stands for in standards contexts is about the official name of the organization. NIST is a U.S. federal agency that develops and maintains standards, guidelines, and measurement science. The correct expansion is National Institute of Standards and Technology. The word order matters: it uses "Standards and Technology," not "Standards for" or "Standards and Security." While you may see references that include a US prefix, the formal name does not insert extra words into the expansion itself. In practice, NIST publishes widely used standards and guidelines (such as the SP 800-series on security controls and the Cybersecurity Framework) that guide both government and industry.

8. Which description best captures a key property STIX aims to provide?

A. A rigid, binary encoding scheme.

B. Fully expressive, flexible, extensible, automatable, and as human-readable as possible.

C. A collection of malware hashes.

D. A real-time network protocol analyzer.

STIX is built to encode threat intelligence in a way that is both richly expressive and ready for automation, while still being understandable to humans. This means it can capture a wide range of concepts—indicators, tactics, techniques, procedures, campaigns, threat actors, relationships between objects, and more—within a single, consistent framework. The emphasis on expressiveness and extensibility allows analysts to describe complex threat scenarios and to expand the standard as new threats and contexts emerge. At the same time, STIX is designed to be machine-actionable: its JSON-based structure and defined object types enable automated ingestion, correlation, and sharing, often in conjunction with TAXII for transport. The human-readability aspect comes from the use of standardized vocabulary and patterns that help analysts interpret the data without needing to reverse-engineer the format. A rigid binary encoding would hinder evolution and collaboration. Focusing only on malware hashes narrows the scope far too much to be useful for comprehensive threat intelligence. A real-time network protocol analyzer serves a different purpose—traffic analysis—rather than describing and sharing threat intelligence.

9. What is the purpose of Sysmon in Windows incident response, and what kind of events should you collect?

A. Sysmon adds detailed process creation, network connections, and file/registry activity; collect Sysmon events and correlate with other logs.

B. Sysmon provides only antivirus scanning events.

C. Sysmon is a memory capture tool.

D. Sysmon logs only user logons.

Sysmon gives visibility into what ends up being hidden from standard Windows logs by logging detailed, structured events about system activity. In incident response, this means you get a clear view of the actions that processes take, how they communicate, and what files or registry keys they touch, all in a format that's easy to search and correlate with other data. Its purpose is to provide rich telemetry that goes beyond typical logging: detailed process creation (including the exact command line and the parent process), network connections (source and destination, ports, and protocol), and file and registry activity (such as file creation times and registry changes), plus other events like driver and image loads. This enables you to trace attacker techniques—like how a backdoor launches, what utilities it uses, where it moves laterally, or what persistence mechanisms it employs—and to assemble a coherent timeline of activity. You should collect Sysmon events and correlate them with other logs (security, network, application, and threat intel) to enhance detection and investigation. It's not an antivirus tool, nor a memory capture tool, nor limited to user logons, but a focused source of detailed behavioral telemetry that strengthens threat hunting and incident response.

10. Remediation events typically occur when?

A. During business hours on weekdays

B. Over a weekend

C. During annual maintenance window

D. Randomly any time

Remediation work is planned for times when impact to normal operations is minimized. Because remediation often requires taking systems offline, applying patches, cleaning up after incidents, or reconfiguring settings, teams schedule these tasks during off-peak periods so there's enough time to test changes and rollback if needed. Weekends are a common window for this, since user activity is typically lower and staff can work with less pressure, reducing disruption to business processes. So, remediation events typically occur over a weekend because this timing balances the need for careful, staged remediation with the goal of limiting impact to operations. Scheduling during business hours on weekdays would risk larger disruption, and while a dedicated annual maintenance window is a valid concept, it isn't as universally applicable or frequent as weekend off-hours. Random timing would lack planning and increase risk.

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://sansfor508.examzify.com

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